Cisco セキュリティ アプライアンス コマンド リファレンス

Cisco ASA 5500 シリーズ / Cisco PIX 500 シリーズ

Software Version 7.2(2)

Text Part Number: OL-10086-02-J

CONTENTS

このマニュアルについて

ここでは、『*Cisco セキュリティ アプライアンス コマンド リファレンス*』について紹介します。

この章には、次の項があります。

マニュアルの目的

このマニュアルでは、ネットワークの不正利用を防いだり、リモート サイトとユーザをネットワークに接続するバーチャル プライベート ネットワークを設定したりするための、セキュリティ アプライアンスで使用できるコマンドについて説明します。

Web ベースの GUI アプリケーションである ASDM を使用して、セキュリティ アプライアンスを設定したり、監視したりすることもできます。ASDM には、一般的なコンフィギュレーション シナリオで導くコンフィギュレーション ウィザードと、あまり一般的でないシナリオにはオンライン ヘルプがあります。詳細については、http://www.cisco.com/univercd/cc/td/doc/product/netsec/secmgmt/asdm/index.htm を参照してください。

このマニュアルは、Cisco PIX 500 シリーズ セキュリティ アプライアンス（PIX 515/515E、PIX 525、および PIX 535）および Cisco ASA 5500 シリーズ セキュリティ アプライアンス（ASA 5510、ASA 5520、および ASA 5540）に適用されます。このマニュアルを通じて、「セキュリティ アプライアンス」という語は、特に指定がなければ、一般的にサポートされているすべてのモデルに適用されます。PIX 501、PIX 506E、および PIX 520 セキュリティ アプライアンスは、Software Version 7.0(1) で、サポートされていません。

対象読者

このマニュアルは、次のタスクを実行するネットワーク管理者を対象としています。

- ネットワーク セキュリティの管理
- ファイアウォール / セキュリティ アプライアンスのインストールと設定
- VPN の設定
- 侵入検知ソフトウェアの設定

このマニュアルと『*Cisco Security Appliance Command Line Configuration Guide*』を併せて使用してください。

マニュアルの構成

このマニュアルは、次の章で構成されています。

- 第 1 章「コマンドライン インターフェイスの使用方法」では、セキュリティ アプライアンス コマンドとアクセス コマンドを紹介します。
- 第 2 章「aaa accounting command コマンド～ accounting-server-group コマンド」では、**aaa accounting** から **accounting-server-group** までのコマンドの詳細について説明します。
- 第 3 章「acl-netmask-convert コマンド～ auto-update timeout コマンド」では、**activation-key** から **auto-update timeout** までのコマンドの詳細について説明します。
- 第 4 章「backup interface コマンド～ browse-networks コマンド」では、**backup-servers** から **boot** までのコマンドの詳細について説明します。
- 第 5 章「cache コマンド～ clear compression コマンド」では、**cache-time** から **clear capture** までのコマンドの詳細について説明します。
- 第 6 章「clear configure コマンド～ clear configure zonelabs-integrity コマンド」では、**clear configure** から **clear configure virtual** までのコマンドの詳細について説明します。
- 第 7 章「clear console-output コマンド～ clear xlate コマンド」では、**clear console-output** から **clear xlate** までのコマンドの詳細について説明します。
- 第 8 章「client-access-rule コマンド～ crl configure コマンド」では、**client-access-rule** から **crl-configure** までのコマンドの詳細について説明します。
- 第 9 章「crypto ca authenticate コマンド～ customization コマンド」では、**crypto ca authenticate** から **crypto map set** までのコマンドの詳細について説明します。
- 第 10 章「ddns コマンド～ debug xdmcp コマンド」では、**debug aaa** から **debug xdmcp** までのコマンドの詳細について説明します。
- 第 11 章「default コマンド～ duplex コマンド」では、**default** から **duplex** までのコマンドの詳細について説明します。
- 第 12 章「email コマンド～ functions コマンド」では、**email** から **functions** までのコマンドの詳細について説明します。
- 第 13 章「gateway コマンド～ hw-module module shutdown コマンド」では、**gateway** から **hw-module module shutdown** までのコマンドの詳細について説明します。
- 第 14 章「icmp コマンド～ imap4s コマンド」では、**icmp** から **imap4s** までのコマンドの詳細について説明します。
- 第 15 章「inspect ctiqbe コマンド～ inspect xdmcp コマンド」では、**inspect ctiqbe** から **inspect xdmcp** までのコマンドの詳細について説明します。
- 第 16 章「interface-dhcp コマンド～ issuer-name コマンド」では、**interface-dhcp** から **issuer-name** までのコマンドの詳細について説明します。
- 第 17 章「java-trustpoint コマンド～ kill コマンド」では、**join-failover-group** から **kill** までのコマンドの詳細について説明します。
- 第 18 章「l2tp tunnel hello コマンド～ log-adj-changes コマンド」では、**l2tp tunnel hello** から **login** までのコマンドの詳細について説明します。
- 第 19 章「logging asdm コマンド～ logout message コマンド」では、**logging asdm** から **logout message** までのコマンドの詳細について説明します。
- 第 20 章「mac address コマンド～ multicast-routing コマンド」では、**mac-address** から **multicast-routing** までのコマンドの詳細について説明します。
- 第 21 章「nac コマンド～ override-account-disable コマンド」では、**name** から **outstanding** までのコマンドの詳細について説明します。
- 第 22 章「packet-tracer コマンド～ pwd コマンド」では、**participate** から **pwd** までのコマンドの詳細について説明します。
- 第 23 章「queue-limit コマンド～ rtp-conformance コマンド」では、**queue-limit** から **router ospf** までのコマンドの詳細について説明します。

- 第 24 章「same-security-traffic コマンド～ show asdm sessions コマンド」では、**same-security-traffic** から **show asdm sessions** までのコマンドの詳細について説明します。
- 第 25 章「show asp drop コマンド～ show curpriv コマンド」では、**show asp drop** から **show curpriv** までのコマンドの詳細について説明します。
- 第 26 章「show ddns update interface コマンド～ show ipv6 traffic コマンド」では、**show debug** から **show ipv6 traffic** までのコマンドの詳細について説明します。
- 第 27 章「show isakmp ipsec-over-tcp stats コマンド～ show route コマンド」では、**show isakmp sa** から **show route** までのコマンドの詳細について説明します。
- 第 28 章「show running-config コマンド～ show running-config isakmp コマンド」では、**show running-config** から **show running-config isakmp** までのコマンドの詳細について説明します。
- 第 29 章「show running-config ldap コマンド～ show running-config wccp コマンド」では、**show running-config logging** から **show running-config webvpn** までのコマンドの詳細について説明します。
- 第 30 章「show service-policy コマンド～ show webvpn svc コマンド」では、**show service-policy** から **show xlate** までのコマンドの詳細について説明します。
- 第 31 章「shun コマンド～ sysopt radius ignore-secret コマンド」では、**shun** から **sysopt uauth allow-http-cache** までのコマンドの詳細について説明します。
- 第 32 章「tcp-map コマンド～ type echo コマンド」では、**tcp-map** から **tunnel-limit** までのコマンドの詳細について説明します。
- 第 33 章「urgent-flag コマンド～ zonelabs integrity ssl-client-authentication コマンド」では、**urgent-flag** から **write terminal** までのコマンドの詳細について説明します。

マニュアルの表記法

コマンドの説明では、次の表記法を使用しています。

- 選択する必要があるものは、中カッコ ({ }) で囲んで示しています。
- オプションの要素は、大カッコ ([ ]) で囲んで示しています。
- どちらか選択する必要がある要素は、パイプ (|) で区切って示しています。
- 記載されているとおりに入力するコマンドおよびキーワードは、**Boldface** フォントで示しています。
- ユーザが値を指定する引数は、*Italics* フォントで示しています。

例では、次の表記法を使用しています。

- 画面に表示される情報は、`screen` フォントで示しています。
- ユーザが入力する情報は、**`boldface screen`** フォントで示しています。
- ユーザが値を指定する引数は、*`italic screen`* フォントで示しています。

(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。

モード、プロンプト、およびシンタックスの詳細については、第 1 章「コマンドライン インターフェイスの使用方法」を参照してください。

関連資料

詳細については、次のマニュアルを参照してください。

- *Cisco ASDM Release Notes*
- *Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*
- *Cisco ASA 5500 Series Hardware Installation Guide*
- *Cisco ASA 5500 Series Quick Start Guide*
- *Cisco ASA 5500 Series Release Notes*
- *Cisco PIX Security Appliance Release Notes*
- *Cisco PIX 515E Quick Start Guide*
- *Cisco Security Appliance Command Line Configuration Guide*
- *Cisco Security Appliance System Log Messages*
- *Guide for Cisco PIX 6.2 and 6.3 Users Upgrading to Cisco PIX Software Version 7.0*
- *Regulatory Compliance and Safety Information for the Cisco ASA 5500 Series*
- *Release Notes for Cisco Secure Desktop*
- *Migrating to ASA for VPN 3000 Concentrator Series Administrators*
- *Selected ASDM VPN Configuration Procedures for the Cisco ASA 5500 Series*

技術情報の入手方法

シスコの製品マニュアルやその他の資料は、Cisco.com でご利用いただけます。ここでは、シスコが提供する製品マニュアル リソースについて説明します。

Cisco.com

次の URL から、シスコ製品の最新資料を入手することができます。

http://www.cisco.com/techsupport

シスコの Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com

シスコの Web サイトの各国語版へは、次の URL からアクセスできます。

http://www.cisco.com/public/countries_languages.shtml

シスコ製品の最新資料の日本語版は、次の URL からアクセスしてください。

http://www.cisco.com/jp

Product Documentation DVD（英語版）

Product Documentation DVD は、技術情報を包含する製品マニュアルをポータブルなメディアに格納したライブラリです。この DVD を使用することにより、シスコ製の各ハードウェアやソフトウェアのインストール、コンフィギュレーション、およびコマンドに関するマニュアルにアクセスすることができます。また、この DVD を使用すると、次の URL のシスコの Web サイトに掲載されている HTML マニュアルおよび PDF ファイルにアクセスすることができます。

http://www.cisco.com/univercd/home/home.htm

Product Documentation DVD は、定期的に作成およびリリースされています。DVD は、1 回単位で入手することも、または定期購読することもできます。Cisco.com 登録ユーザの場合、Cisco Marketplace の Product Documentation Store から Product Documentation DVD（Product Number DOC-DOCDVD= または DOC-DOCDVD=SUB）を発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/docstore

マニュアルの発注方法（英語版）

Cisco Marketplace にアクセスするには、Cisco.com の登録ユーザとなる必要があります。登録ユーザの場合、Product Documentation Store からシスコ製品の英文マニュアルを発注できます。次の URL にアクセスしてください。

http://www.cisco.com/go/marketplace/docstore

ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

シスコシステムズマニュアルセンター

シスコシステムズマニュアルセンターでは、シスコ製品の日本語マニュアルの最新版を PDF 形式で公開しています。また、日本語マニュアル、および日本語マニュアル CD-ROM もオンラインで発注可能です。ご希望の方は、次の URL にアクセスしてください。

http://www2.hipri.com/cisco/

また、シスコシステムズマニュアルセンターでは、日本語マニュアル中の誤記、誤植に関するコメントをお受けしています。次の URL の「製品マニュアル内容不良報告」をクリックすると、コメント入力画面が表示されます。

http://www2.hipri.com/cisco/

なお、技術内容に関するお問い合せは、この Web サイトではお受けできませんので、製品を購入された各代理店へお問い合せください。

シスコ製品のセキュリティの概要

シスコでは、オンラインの Security Vulnerability Policy ポータル（英文のみ）を無料で提供しています。URL は次のとおりです。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このサイトは、次の目的に利用できます。

- シスコ製品のセキュリティ脆弱性を報告する。
- シスコ製品に伴うセキュリティ事象についてサポートを受ける。
- シスコからセキュリティ情報を受け取るための登録をする。

シスコ製品に関するセキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策の最新のリストには、次の URL からアクセスできます。

http://www.cisco.com/go/psirt

セキュリティ勧告、セキュリティ上の注意事項、およびセキュリティ対策がアップデートされた時点でリアルタイムに確認する場合は、次の URL から Product Security Incident Response Team Really Simple Syndication（PSIRT RSS）フィードに登録してください。PSIRT RSS フィードへの登録方法については、次の URL を参照してください。

http://www.cisco.com/en/US/products/products_psirt_rss_feed.html

シスコ製品のセキュリティ問題の報告

シスコでは、セキュアな製品を提供すべく全力を尽くしています。製品のリリース前には内部でテストを行い、すべての脆弱性を早急に修正するよう努力しています。万一、シスコ製品に脆弱性が見つかった場合は、PSIRT にご連絡ください。

- 緊急の場合：security-alert@cisco.com（英語のみ）

  緊急とは、システムがアクティブな攻撃を受けている場合、または至急の対応を要する重大なセキュリティ上の脆弱性が報告されている場合を指します。これに該当しない場合はすべて、緊急でないと見なされます。
- 緊急でない場合：psirt@cisco.com（英語のみ）

緊急の場合は、電話で PSIRT に連絡することもできます。

- 1 877 228-7302（英語のみ）
- 1 408 525-6532（英語のみ）

ヒント シスコに機密情報をお送りいただく際には、PGP（Pretty Good Privacy）または GnuPG などの互換製品を使用して、暗号化することをお勧めします。PSIRT は、PGP バージョン 2.*x* から 9.*x* を使用して暗号化された情報に対応しています。

無効になった、または有効期限が切れた暗号鍵は、絶対に使用しないでください。PSIRT に連絡する際に使用する正しい公開鍵には、Security Vulnerability Policy ページの Contact Summary セクションからリンクできます。次の URL にアクセスしてください。

http://www.cisco.com/en/US/products/products_security_vulnerability_policy.html

このページ上のリンクからは、現在使用されている最新の PGP 鍵の ID にアクセスできます。

PGP を持っていない、または使用していない場合は、機密情報を送信する前に PSIRT に問い合せ、他のデータ暗号化方法を確認してください。

Product Alerts および Field Notices

シスコ製品に対する変更やアップデートは、Cisco Product Alerts および Cisco Field Notices で通知されます。Cisco.com のプロダクト アラート ツールを使用すると、これらの通知を受け取ることができます。このツールを使用すれば、プロファイルを作成して、情報を受け取る製品を選択できます。

プロダクト アラート ツールにアクセスするには、Cisco.com の登録ユーザとなる必要があります。登録ユーザは、次の URL でこのツールを使用できます。

http://tools.cisco.com/Support/PAT/do/ViewMyProfiles.do?local=en

Cisco.com にユーザ登録するには、次の URL にアクセスします。

http://tools.cisco.com/RPF/register/register.do

テクニカル サポート

Cisco Technical Support では、24 時間テクニカル サポートを提供しています。Cisco.com の Cisco Technical Support Web サイトでは、多数のサポート リソースをオンラインで提供しています。また、シスコと正式なサービス契約を交わしているお客様には、Cisco Technical Assistance Center（TAC）のエンジニアが電話でのサポートにも対応します。シスコと正式なサービス契約を交わしていない場合は、代理店にお問い合せください。

Cisco Support Web サイト

Cisco Support Web サイトでは、シスコ製品やシスコの技術に関するトラブルシューティングにお役立ていただけるように、オンラインでマニュアルやツールを提供しています。この Web サイトは、24 時間、いつでも利用可能です。URL は次のとおりです。

http://www.cisco.com/en/US/support/index.html

Cisco Support Web サイトのツールにアクセスするには、Cisco.com のユーザ ID とパスワードが必要です。サービス契約が有効で、ユーザ ID またはパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://tools.cisco.com/RPF/register/register.do

（注） オンラインまたは電話でサービス リクエストを発行する前に、**Cisco Product Identification Tool** を使用して製品のシリアル番号を確認してください。Cisco Support Web サイトでこのツールを使用するには、**Get Tools & Resources** リンクをクリックし、**All Tools (A-Z)** タブをクリックした後、アルファベット順のリストから **Cisco Product Identification Tool** を選択します。このツールには、3 つの検索オプションがあります。製品 ID またはモデル名による検索、ツリー表示による検索、**show** コマンド出力のコピー アンド ペーストによる特定製品の検索です。検索結果では、製品が図示され、シリアル番号ラベルの位置が強調表示されます。ご使用の製品でシリアル番号ラベルを確認し、その情報を記録してからサービス コールをかけてください。

ヒント **Cisco.com での表示および検索**

ブラウザが Web ページをリフレッシュしていないと思われる場合は、Ctrl キーを押したまま **F5** を押すことで強制的にブラウザに Web ページを更新させます。

技術情報を検索する場合は、Cisco.com の Web サイト全体ではなく、技術マニュアルに検索対象を絞り込みます。Cisco.com のホームページで Search ボックスを使用した後、表示されたページで Search ボックスの隣の **Advanced Search** リンクをクリックし、**Technical Support & Documentation** オプション ボタンをオンにします。

Cisco.com の Web サイトまたは特定の技術マニュアルに関するフィードバックを送るには、Cisco.com のすべての Web ページの下部にある **Contacts & Feedback** をクリックします。

Japan TAC Web サイト

Japan TAC Web サイトでは、利用頻度の高い TAC Web サイト（http://www.cisco.com/tac）のドキュメントを日本語で提供しています。Japan TAC Web サイトには、次の URL からアクセスしてください。

http://www.cisco.com/jp/go/tac

サポート契約を結んでいない方は、「ゲスト」としてご登録いただくだけで、Japan TAC Web サイトのドキュメントにアクセスできます。Japan TAC Web サイトにアクセスするには、Cisco.com のログイン ID とパスワードが必要です。ログイン ID とパスワードを取得していない場合は、次の URL にアクセスして登録手続きを行ってください。

http://www.cisco.com/jp/register

サービス リクエストの発行

オンラインの TAC Service Request Tool を使用すると、S3 と S4 のサービス リクエストを短時間でオープンできます（S3：ネットワークに軽微な障害が発生した、S4：製品情報が必要である）。状況を入力すると、その状況を解決するための推奨手段が検索されます。これらの推奨手段で問題を解決できない場合は、シスコのエンジニアが対応します。TAC Service Request Tool には、次の URL からアクセスできます。

http://www.cisco.com/techsupport/servicerequest

S1 または S2 のサービス リクエストの場合、またはインターネットにアクセスできない場合は、Cisco TAC に電話でお問い合せください（S1：ネットワークがダウンした、S2：ネットワークの機能が著しく低下した）。S1 および S2 のサービス リクエストには、シスコのエンジニアがすぐに割り当てられ、業務を円滑に継続できるようサポートします。

Cisco TAC の連絡先については、次の URL を参照してください。

http://www.cisco.com/techsupport/contacts

サービス リクエストのシビラティの定義

シスコでは、報告されるサービス リクエストを標準化するために、シビラティを定義しています。

シビラティ 1（S1）：既存のネットワークが「ダウン」した状態か、業務に致命的な損害が発生した場合。お客様およびシスコが、24 時間体制でこの問題を解決する必要があると判断した場合。

シビラティ 2（S2）：既存のネットワーク動作が著しく低下したか、シスコ製品が十分に機能しないため、業務に重大な影響を及ぼした場合。お客様およびシスコが、通常の業務中の全時間を費やして、この問題を解決する必要があると判断した場合。

シビラティ 3（S3）：ネットワークの動作パフォーマンスが低下しているが、ほとんどの業務運用は継続できる場合。お客様およびシスコが、業務時間中にサービスを十分なレベルにまで復旧させる必要があると判断した場合。

シビラティ 4（S4）：シスコ製品の機能、インストレーション、コンフィギュレーションについて、情報または支援が必要な場合。業務の運用には、ほとんど影響がありません。

その他の資料および情報の入手

シスコの製品、テクノロジー、およびネットワーク ソリューションに関する情報について、さまざまな資料をオンラインおよび印刷物で入手できます。

- Cisco Online Subscription Center は、シスコのさまざまな E メール ニュースレターやその他の通信に登録できる Web サイトです。プロファイルを作成し、受信を希望する情報を選択してください。Cisco Online Subscription Center には、次の URL からアクセスできます。

  http://www.cisco.com/offer/subscribe

- 『*Cisco Product Quick Reference Guide*』は手軽でコンパクトな参照ツールです。チャネル パートナー経由で販売される多くのシスコ製品に関する簡単な製品概要、主要な機能、サンプル部品番号、および簡単な技術仕様を記載しています。年 2 回の更新の際には、シスコのチャネル製品の最新情報が収録されます。『*Cisco Product Quick Reference Guide*』の注文方法および詳細については、次の URL にアクセスしてください。

  http://www.cisco.com/go/guide

- Cisco Marketplace では、シスコの書籍やリファレンス ガイド、マニュアル、ロゴ製品を数多く提供しています。購入を希望される場合は、次の URL にアクセスしてください。

  http://www.cisco.com/go/marketplace/

- Cisco Press では、ネットワーク全般、トレーニング、および認定資格に関する出版物を幅広く発行しています。これらの出版物は、初級者にも上級者にも役立ちます。Cisco Press の最新の出版情報などについては、次の URL からアクセスしてください。

  http://www.ciscopress.com

- 『*Internet Protocol Journal*』は、インターネットおよびイントラネットの設計、開発、運用を担当するエンジニア向けに、シスコが発行する季刊誌です。『*Internet Protocol Journal*』には、次の URL からアクセスしてください。

  http://www.cisco.com/ipj

- シスコが提供するネットワーキング製品、および各種のカスタマー サポート サービスは、次の URL から入手できます。

  http://www.cisco.com/en/US/products/index.html

- Networking Professionals Connection は対話形式の Web サイトです。このサイトでは、ネットワーキング製品やテクノロジーに関する質問、提案、および情報をネットワーキング担当者がシスコの専門家や他のネットワーキング担当者と共有できます。次の URL にアクセスしてディスカッションに参加してください。

  http://www.cisco.com/discuss/networking

- 「What's New in Cisco Documentation」は、シスコ製品の最新のマニュアル リリースに関する情報を提供するオンライン出版物です。このオンライン出版物は毎月更新され、製品カテゴリ別に編成されているため、製品のマニュアルを簡単に検索できます。次の URL で「What's New in Cisco Documentation」の最新リリースを見ることができます。

  http://www.cisco.com/univercd/cc/td/doc/abtunicd/136957.htm

- シスコは、国際的なレベルのネットワーク関連トレーニングを実施しています。最新情報については、次の URL からアクセスしてください。

  http://www.cisco.com/en/US/learning/index.html

コマンドライン インターフェイスの使用方法

この章では、セキュリティ アプライアンスでの CLI の使用方法について説明します。この章は次の内容で構成されています。

（注） CLI のシンタックスおよび他の表記法は Cisco IOS CLI と同様ですが、セキュリティ アプライアンス オペレーティング システムは、Cisco IOS ソフトウェアのバージョンではありません。Cisco IOS CLI コマンドがセキュリティ アプライアンスで動作したり、同様の機能を持っているとは限りません。

ファイアウォール モードとセキュリティ コンテキスト モード

セキュリティ アプライアンスは次のモードの組み合せで動作します。

- 透過ファイアウォール モードまたはルーテッド ファイアウォール モード

  ファイアウォール モードは、セキュリティ アプライアンスがレイヤ 2 ファイアウォールまたはレイヤ 3 ファイアウォールとして動作するかどうかを判断します。

- マルチ コンテキスト モードまたはシングル コンテキスト モード

  セキュリティ コンテキスト モードは、セキュリティ アプライアンスがシングル デバイスとして動作するか、または仮想デバイスのようにマルチ セキュリティ コンテキストとして動作するかを決定します。

一部のコマンドは、特定のモードに限り使用可能です。

コマンド モードとプロンプト

セキュリティ アプライアンス CLI には、コマンド モードがあります。一部のコマンドは、特定のモードでのみ入力できます。たとえば、機密情報を表示するコマンドを入力する場合は、パスワードを入力して、さらに高い特権モードに入る必要があります。したがって、何らかの原因で設定の変更が入力されていないことを確認するには、コンフィギュレーション モードに入る必要があります。すべての下位コマンドは上位モードで入力できます。たとえば、グローバル コンフィギュレーション モードで特権 EXEC コマンドを入力できます。

システム コンフィギュレーション モードまたはシングル コンテキスト モードの場合、プロンプトは次のように hostname で開始されます。

```
hostname
```

コンテキスト内では、プロンプトはホスト名の後にコンテキスト名が表示されます。

```
hostname/context
```

プロンプトは、次のアクセス モードに応じて変わります。

- ユーザ EXEC モード

  ユーザ EXEC モードを使用すると、最低限のセキュリティ アプライアンス設定を確認できます。ユーザ EXEC モードのプロンプトは、初めてセキュリティ アプライアンスにアクセスしたときに次のように表示されます。

  ```
  hostname>

  hostname/context>
  ```

- 特権 EXEC モード

  特権 EXEC モードを使用すると、特権レベルまでの現在の設定をすべて表示できます。ユーザ EXEC モードのコマンドは、特権 EXEC モードで動作します。ユーザ EXEC モードで **enable** コマンドを入力して、特権 EXEC モードを起動するにはパスワードが必要です。プロンプトには、次のようにポンド記号（#）が含まれます。

  ```
  hostname#

  hostname/context#
  ```

- グローバル コンフィギュレーション モード

  グローバル コンフィギュレーション モードを使用すると、セキュリティ アプライアンス コンフィギュレーションを変更できます。このモードでは、すべてのユーザ EXEC、特権 EXEC、およびグローバル コンフィギュレーション コマンドが利用できます。特権 EXEC モードで **configure terminal** コマンドを入力して、グローバル コンフィギュレーション モードを開始します。プロンプトが次のように変化します。

  ```
  hostname(config)#

  hostname/context(config)#
  ```

- コマンド固有のコンフィギュレーション モード

  一部のコマンドは、グローバル コンフィギュレーション モードからコマンド固有のコンフィギュレーション モードに入ります。このモードでは、すべてのユーザ EXEC、特権 EXEC、グローバル コンフィギュレーション、およびコマンド固有のコンフィギュレーション コマンドが利用できます。たとえば、**interface** コマンドにより、インターフェイス コンフィギュレーション モードに入ります。プロンプトが次のように変化します。

  ```
  hostname(config-if)#

  hostname/context(config-if)#
  ```

シンタックスの書式

コマンド シンタックスの説明には、次の表記法を使用しています。

表 1-1　シンタックスの表記法

表記法	説明
太字	表示どおりに入力するコマンドおよびキーワードは、太字で示しています。
イタリック体	ユーザが値を指定する引数は、イタリック体で示しています。
[x]	省略可能な要素（キーワードまたは引数）は、角カッコで囲んで示しています。
|	省略可能または必須のキーワードや引数の中から選択する場合は、縦棒で区切って示しています。
[x | y]	どれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずどれか 1 つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。
[x {y | z}]	省略可能または必須の要素内に、さらに省略可能または必須の選択肢を含める場合は、角カッコや波カッコを入れ子にして示しています。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。

コマンドの省略

ほとんどのコマンドは、コマンド独自の最小限の文字に短縮して入力できます。たとえば、**write terminal** とコマンドを完全に入力する代わりに、**wr t** と入力すると、コンフィギュレーションを表示できます。または、**en** と入力すると、特権モードを開始し、**conf t** と入力すると、コンフィギュレーション モードを開始できます。さらに、**0** と入力して、**0.0.0.0** を表すこともできます。

コマンドラインの編集

セキュリティ アプライアンスは、Cisco IOS ソフトウェアと同様のコマンドライン編集の表記法を使用します。**show history** コマンドを使用してこれまでに入力したコマンドをすべて表示するか、または上向き矢印か **^p** コマンドで個別に表示することができます。これまでに入力したコマンドを確認したら、下向き矢印または **^n** コマンドでリスト内を移動できます。再使用するコマンドに到達したら、そのコマンドを編集したり、**Enter** キーを押して、コマンドを開始できます。**^w** を使用して、カーソルの左側の単語を削除したり、**^u** を使用して、行を削除することもできます。

セキュリティ アプライアンスを使用すると、コマンドに最大 512 文字を使用できます。それより多い文字は無視されます。

コマンドの完成

一部の文字列を入力した後で、コマンドまたはキーワードを完成するには、**Tab** キーを押します。セキュリティ アプライアンスは、一部の文字列が 1 つのコマンドまたはキーワードだけに一致した場合に限り、コマンドまたはキーワードを完成します。たとえば、**s** を入力して **Tab** キーを押すと、これに一致するコマンドが 2 つ以上あるため、セキュリティ アプライアンスはコマンドを完成しません。ただし、**dis** を入力して **Tab** キーを押すと、コマンド **disable** が完成します。

コマンドのヘルプ

次のコマンドを入力することにより、コマンドラインからヘルプ情報を利用できます。

- **help** *command_name*
  特定のコマンドに対するヘルプが表示されます。
- **help ?**
  ヘルプがあるコマンドが表示されます。
- *command_name* **?**
  利用可能な引数のリストが表示されます。
- *string***?**（スペースなし）
  文字列で始まる可能性があるコマンドを表示します。
- **?** および **+?**
  利用可能なコマンドをすべて表示します。**?** を入力すると、セキュリティ アプライアンスは現在のモードで利用可能なコマンドだけを表示します。下位モードのコマンドも含め、利用可能なコマンドをすべて表示するには、**+?** を入力します。

（注） コマンド文字列に疑問符（?）を含める場合は、不用意に CLI ヘルプが起動しないよう、疑問符を入力する前に **Ctrl+V** を押す必要があります。

show コマンド出力のフィルタリング

show コマンドと一緒に縦棒（|）を使用して、フィルタ オプションとフィルタリング表現を指定できます。フィルタリングは、Cisco IOS ソフトウェアと同様に、各出力行を正規表現に一致させることで実行されます。異なるフィルタ オプションを選択することで、表現と一致するすべての出力を表示または除外できます。また、表現と一致する行で開始される出力をすべて表示することもできます。

show コマンドでフィルタリング オプションを使用するシンタックスは、次のとおりです。

```
hostname# show command | {include | exclude | begin | grep [-v]} regexp
```

このコマンド文字列では、最初の縦棒（|）がコマンドに必要な演算子です。この演算子により、**show** コマンドの出力がフィルタに送られます。シンタックス内の他の縦棒（|）は代替オプションを示すもので、コマンドの一部ではありません。

include オプションでは、正規表現と一致するすべての出力行が含まれます。**-v** を指定しない **grep** オプションでも、同じ働きをします。**exclude** オプションでは、正規表現と一致するすべての出力が除外されます。**-v** を指定した **grep** オプションでも、同じ働きをします。**begin** オプションでは、正規表現と一致する行で開始されるすべての出力行が表示されます。

regexp には、任意の Cisco IOS の正規表現を指定します。正規表現は一重引用符または二重引用符で囲まれないため、末尾にスペースがついていないかどうか確認してください。スペースは正規表現の一部と解釈されます。

正規表現を作成する場合は、一致させる任意の文字または数字を使用できます。また、正規表現で使用されると、特別な意味を持つキーボード文字があります。表 1-2 に特別な意味を持つキーボード文字を示します。

表 1-2　正規表現での特殊文字の使用

文字の種類	文字	特別の意味
ピリオド	.	スペースを含む任意の単一文字と一致します。
アスタリスク	*	0 個またはそれ以上の連続するパターンに一致します。
プラス記号	+	1 個またはそれ以上の連続するパターンに一致します。
疑問符	?[1]	0 または 1 回のパターンと一致します。
キャレット	^	入力ストリングの先頭と一致します。
ドル記号	$	入力ストリングの末尾と一致します。
アンダースコア	_	カンマ（,）、左波カッコ（{）、右波カッコ（}）、左カッコ、右カッコ、入力ストリングの先頭、入力ストリングの末尾、またはスペースと一致します。
角カッコ	[]	単一文字のパターンの範囲を指定します。
ハイフン	-	範囲の終点を区切ります。

1. 疑問符の前に **Ctrl+V** を押すと、ヘルプ コマンドと解釈されません。

これらの特殊文字を単一文字パターンとして使用する場合は、各文字の前にバックスラッシュ（\）を置いて特別の意味を持たないようにしてください。

コマンド出力のページング

help または **?**、**show**、**show xlate** や、リストが長いその他のコマンドなどでは、画面に情報を表示して停止するか、完了するまでコマンドを実行させるかを指定できます。**pager** コマンドを使用すると、More プロンプトが表示される前に、表示する行数を選択できます。

ページングが有効になっているときには、次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトは UNIX の **more** コマンドと同様のシンタックスを使用します。

- 次の画面を表示するには、Space キーを押す。
- 次の行を表示するには、**Enter** キーを押す。
- コマンドラインに戻るには、**q** キーを押す。

コメントの追加

行の先頭にコロン（:）を入力すると、コメントを作成できます。ただし、コメントが表示されるのはコマンド履歴バッファ内だけで、コンフィギュレーションには表示されません。したがって、**show history** コマンドを使用してコメントを表示するか、矢印キーを押して前のコマンドを検索することでコメントを表示できます。ただし、コメントはコンフィギュレーションに入っていないため、**write terminal** コマンドを使用しても表示されません。

テキスト コンフィギュレーション ファイル

この項では、セキュリティ アプライアンスにダウンロードできるテキスト コンフィギュレーション ファイルをフォーマットする方法について説明します。この項は、次の内容で構成されています。

テキスト ファイル内の行とコマンドの対応

テキスト コンフィギュレーション ファイルには、このマニュアルで説明されているコマンドに対応する行が含まれています。

次の例では、コマンドが CLI プロンプトの後に来ます。次に、プロンプト「hostname(config)#」の例を示します。

```
hostname(config)# context a
```

テキスト コンフィギュレーション ファイルでは、コマンドの入力を求められないため、プロンプトは省略されます。

```
context a
```

コマンド固有のコンフィギュレーション モード コマンド

コマンドラインで入力する場合、コマンド固有のコンフィギュレーション モード コマンドは、メイン コマンドの下に字下げして表示されます。メイン コマンドのすぐ後にコマンドが表示されれば、テキスト ファイルの行を字下げする必要はありません。たとえば、次の字下げされていないテキストは、字下げされたテキストと同じように読み出されます。

```
interface gigabitethernet0/0
nameif inside
interface gigabitethernet0/1
    nameif outside
```

自動テキスト エントリ

コンフィギュレーションをセキュリティ アプライアンスにダウンロードすると、セキュリティ アプライアンスにより一部の行が自動的に挿入されます。たとえば、セキュリティ アプライアンスにより、デフォルト設定の行や、コンフィギュレーション変更時間の行が挿入されます。テキスト ファイルの作成時に、これらの自動エントリを入力する必要はありません。

行の順序

ほとんどのコマンドを任意の順序でファイルに入れることができます。ただし、ACE など一部の行は表示された順序で処理され、この順序がアクセス リストの機能に影響を与えます。他にも、順序の要件を持つコマンドがあります。たとえば、後続のコマンドの多くがインターフェイスの名前を使用するため、インターフェイスに **nameif** コマンドを最初に入力する必要があります。また、コマンド固有のコンフィギュレーション モードのコマンドも、メイン コマンドの直後に入力する必要があります。

テキスト コンフィギュレーションに含まれないコマンド

一部のコマンドでは、コンフィギュレーションに行が挿入されません。たとえば、**show running-config** などの実行時コマンドは、テキスト ファイル内に対応する行がありません。

パスワード

ログイン、イネーブル、およびユーザ パスワードは、コンフィギュレーションに保存される前に自動的に暗号化されます。たとえば、パスワード「cisco」の暗号化された形式は、jMorNbK0514fadBh のようになります。コンフィギュレーション パスワードは暗号化された形式で別のセキュリティ アプライアンスにコピーできますが、ユーザがそのパスワードの暗号を解読することはできません。

暗号化されていないパスワードをテキスト ファイルに入力した場合、コンフィギュレーションをセキュリティ アプライアンスにコピーしても、セキュリティ アプライアンスは自動的にパスワードを暗号化しません。セキュリティ アプライアンスがパスワードを暗号化するのは、**copy running-config startup-config** コマンドまたは **write memory** コマンドを使用して、コマンドラインから実行コンフィギュレーションを保存した場合のみです。

マルチ セキュリティ コンテキスト ファイル

マルチ セキュリティ コンテキストの場合、コンフィギュレーション全体は次に示す複数の部分で構成されます。

- セキュリティ コンテキストのコンフィギュレーション
- セキュリティ アプライアンスの基本設定を識別するシステム コンフィギュレーション（コンテキストのリストを含む）
- システム コンフィギュレーションのネットワーク インターフェイスを提供する管理コンテキスト

  システム コンフィギュレーション自体には、インターフェイスまたはネットワーク設定は含まれません。システムがネットワーク リソースにアクセスする必要がある（サーバからコンテキストをダウンロードするなど）場合に、システムは管理コンテキストとして指定されたコンテキストを使用します。

各コンテキストは、シングル コンテキスト モード コンフィギュレーションと同様です。システム コンフィギュレーションは、コンテキスト コンフィギュレーションとは異なります。システム コンフィギュレーションにはシステム専用コマンド（すべてのコンテキストのリストなど）が含まれますが、他の一般的なコマンド（多くのインターフェイス パラメータなど）は含まれません。

aaa accounting command コマンド～ accounting-server-group コマンド

aaa accounting command

CLI で **show** 以外のコマンドを入力したときに、TACACS+ アカウンティング サーバにアカウンティング メッセージを送信するには、グローバル コンフィギュレーション モードで **aaa accounting command** コマンドを使用します。コマンド アカウンティングのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

no aaa accounting command [**privilege** *level*] *tacacs+-server-tag*

シンタックスの説明

tacacs+-server-tag	**aaa-server protocol** コマンドで指定したように、アカウンティング レコードの送信先の TACACS+ サーバまたはサーバのグループを指定します。
privilege *level*	**privilege** コマンドを使用してコマンドの特権レベルをカスタマイズする場合は、特権の最低レベルを指定して、セキュリティ アプライアンスで処理の対象とするコマンドを制限できます。指定したレベルより下のコマンドは、セキュリティ アプライアンスで処理されません。

デフォルト

デフォルトの特権レベルは 0 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

aaa accounting command コマンドを設定すると、管理者が入力した **show** コマンド以外のコマンドが記録され、1 つまたは複数のアカウンティング サーバに送信されます。

例

次の例では、サポートされている全コマンドのアカウンティング レコードが生成され、そのレコードが adminserver というサーバ グループに送信されるように指定しています。

```
hostname(config)# aaa accounting command adminserver
```

関連コマンド

コマンド	説明
aaa accounting	**aaa-server** コマンドで指定したサーバ上の TACACS+ または RADIUS のユーザ アカウンティングをイネーブルまたはディセーブルにします。
clear configure aaa	設定済みの AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting console

管理者アクセス権の AAA アカウンティングのサポートをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting console** コマンドを使用します。管理者アクセス権の AAA アカウンティングのサポートをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting {**http | serial| telnet | ssh | enable**} **console** *server-tag*

no aaa accounting {**http | serial | telnet | ssh | enable**} **console** *server-tag*

シンタックスの説明

enable	特権 EXEC モードの開始および終了を示すアカウンティング レコードの生成をイネーブルにします。
http	HTTP 接続で作成される管理セッションの確立および終了を示すアカウンティング レコードの生成をイネーブルにします。
serial	シリアル コンソール インターフェイスを介して確立される管理セッションの確立および終了を示すアカウンティング レコードの生成をイネーブルにします。
server-tag	**aaa-server protocol** コマンドで定義したように、アカウンティング レコードの送信先のサーバ グループを指定します。有効なサーバ グループ プロトコルは、RADIUS および TACACS+ です。
ssh	SSH で作成される管理セッションの確立および終了を示すアカウンティング レコードの生成をイネーブルにします。
telnet	Telnet で作成される管理セッションの確立および終了を示すアカウンティング レコードの生成をイネーブルにします。

デフォルト

デフォルトでは、管理者アクセス権の AAA アカウンティングはディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

サーバ グループの名前（事前に **aaa-server** コマンドで指定したもの）を指定する必要があります。

例

次の例では、すべての HTTP トランザクションに対してアカウンティング レコードが生成され、そのレコードが adminserver という名前のサーバに送信されるよう指定しています。

```
hostname(config)# aaa accounting http console adminserver
```

関連コマンド

コマンド	説明
aaa accounting match	**aaa-server** コマンドで指定したサーバ上の TACACS+ または RADIUS のユーザ アカウンティングをイネーブルまたはディセーブルにします。
aaa accounting command	管理者（ユーザ）によって入力された、各コマンドまたは指定した特権レベル以上のコマンドを記録し、アカウンティング サーバ（複数可）に送信するよう指定します。
clear configure aaa	設定済みの AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting include、exclude

セキュリティ アプライアンス経由の TCP 接続または UDP 接続のアカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting include** コマンドを使用します。アカウンティングからアドレスを除外するには、**aaa accounting exclude** コマンドを使用します。アカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

no aaa accounting {**include** | **exclude**} *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] *server_tag*

シンタックスの説明

exclude	サービスとアドレスが **include** コマンドですでに指定されている場合に、指定されたサービスとアドレスをアカウンティングから除外します。
include	アカウンティングが必要なサービスと IP アドレスを指定します。**include** 文で指定されていないトラフィックは処理されません。
inside_ip	セキュリティの高いインターフェイスの IP アドレスを指定します。このコマンドを適用するインターフェイスに応じて、送信元アドレスまたは宛先アドレスを指定します。セキュリティの低いインターフェイスにこのコマンドを適用する場合は、宛先アドレスを指定します。セキュリティの高いインターフェイスにこのコマンドを適用する場合は、送信元アドレスを指定します。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を使用します。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
outside_ip	（オプション）セキュリティの低いインターフェイスの IP アドレスを指定します。このコマンドを適用するインターフェイスに応じて、送信元アドレスまたは宛先アドレスを指定します。セキュリティの低いインターフェイスにこのコマンドを適用する場合は、送信元アドレスを指定します。セキュリティの高いインターフェイスにこのコマンドを適用する場合は、宛先アドレスを指定します。すべてのホストを指定するには、0 を指定します。
outside_mask	（オプション）外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を使用します。
server_tag	**aaa-server host** コマンドで定義した AAA サーバ グループを指定します。
service	アカウンティングが必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定） • **ftp** • **http** • **https** • ***ssh*** • **telnet** • **tcp**/*port* • **udp**/*port*

デフォルト

デフォルトでは、管理者アクセス権の AAA アカウンティングはディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過するすべての TCP トラフィックおよび UDP トラフィックについて、アカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。このトラフィックが認証の対象にもなっている場合、AAA サーバはアカウンティング情報をユーザ名で管理できます。トラフィックが認証の対象になっていない場合、AAA サーバはアカウンティング情報を IP アドレスで管理できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、当該セッションでセキュリティ アプライアンスを通過したバイト数、使用されたサービス、および各セッションの継続時間が含まれています。

このコマンドを使用するには、**aaa-server** コマンドで AAA サーバを指定しておく必要があります。

アクセス リストで指定されているトラフィックのアカウンティングをイネーブルにするには、**aaa accounting match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションの中では使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することをお勧めします。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていないためです。

セキュリティ レベルが同じインターフェイス間で **aaa accounting include** および **exclude** コマンドを使用することはできません。この場合は、**aaa accounting match** コマンドを使用する必要があります。

例

次の例では、すべての TCP 接続でアカウンティングをイネーブルにしています。

```
hostname(config)# aaa-server mygroup protocol tacacs+
hostname(config)# aaa-server mygroup (inside) host 192.168.10.10 thekey timeout 20
hostname(config)# aaa accounting include any inside 0 0 0 0 mygroup
```

関連コマンド

コマンド	説明
aaa accounting match	アクセス リストで指定されているトラフィックに対するアカウンティングをイネーブルにします。
aaa accounting command	管理者アクセス権のアカウンティングをイネーブルにします。
aaa-server host	AAA サーバを設定します。
clear configure aaa	AAA コンフィギュレーションを消去します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa accounting match

セキュリティ アプライアンス経由の TCP 接続および UDP 接続のアカウンティングをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa accounting match** コマンドを使用します。トラフィックのアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa accounting match *acl_name interface_name server_tag*

no aaa accounting match *acl_name interface_name server_tag*

シンタックスの説明

acl_name	**access-list** 名の照合によるアカウンティングが必要なトラフィックを指定します。アクセス リスト内の permit エントリがアカウンティングの対象となり、deny エントリはアカウンティングから免除されます。このコマンドは、TCP トラフィックおよび UDP トラフィックに対してのみサポートされます。このコマンドを入力し、そのコマンドが他のプロトコルを許可するアクセス リストを参照している場合、警告メッセージが表示されます。
interface_name	ユーザがアカウンティングを要求するインターフェイスの名前を指定します。
server_tag	**aaa-server** コマンドで定義した AAA サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスは、セキュリティ アプライアンスを通過するすべての TCP トラフィックおよび UDP トラフィックについて、アカウンティング情報を RADIUS サーバまたは TACACS+ サーバに送信できます。このトラフィックが認証の対象にもなっている場合、AAA サーバはアカウンティング情報をユーザ名で管理できます。トラフィックが認証の対象になっていない場合、AAA サーバはアカウンティング情報を IP アドレスで管理できます。アカウンティング情報には、セッションの開始時刻と終了時刻、ユーザ名、当該セッションでセキュリティ アプライアンスを通過したバイト数、使用されたサービス、および各セッションの継続時間が含まれています。

このコマンドを使用するには、**aaa-server** コマンドで AAA サーバを指定しておく必要があります。

AAA サーバ プロトコル コンフィギュレーション モードで **accounting-mode** コマンドを使用して同時アカウンティングをイネーブルにしない限り、アカウンティング情報は、サーバ グループ内のアクティブなサーバだけに送信されます。

aaa accounting match コマンドは、**aaa accounting include** および **exclude** コマンドと同じコンフィギュレーションの中では使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することをお勧めします。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていないためです。

例

次の例では、特定のアクセス リスト acl2 と一致するトラフィックのアカウンティングをイネーブルにする方法を示します。

```
hostname(config)# access-list acl12 extended permit tcp any any
hostname(config)# aaa accounting match acl2 outside radserver1
```

関連コマンド

コマンド	説明
aaa accounting include、exclude	コマンド内で IP アドレスを直接指定することでアカウンティングをイネーブルにします。
access-list extended	アクセス リストを作成します。
clear configure aaa	AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication include、exclude

セキュリティ アプライアンスを経由する接続の認証をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication include** コマンドを使用します。認証からアドレスを除外するには、**aaa authentication exclude** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

no aaa authentication {include | **exclude}** *service interface_name inside_ip inside_mask* [*outside_ip outside_mask*] {*server_tag* | **LOCAL**}

シンタックスの説明

exclude	サービスとアドレスが **include** コマンドですでに指定されている場合に、指定されたサービスとアドレスを認証から除外します。
include	認証が必要なサービスと IP アドレスを指定します。**include** 文で指定されていないトラフィックは処理されません。
inside_ip	セキュリティの高いインターフェイスの IP アドレスを指定します。このコマンドを適用するインターフェイスに応じて、送信元アドレスまたは宛先アドレスを指定します。セキュリティの低いインターフェイスにこのコマンドを適用する場合は、宛先アドレスを指定します。セキュリティの高いインターフェイスにこのコマンドを適用する場合は、送信元アドレスを指定します。すべてのホストを指定するには、0 を指定します。
inside_mask	内部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を使用します。
interface_name	ユーザが認証を要求するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
outside_ip	（オプション）セキュリティの低いインターフェイスの IP アドレスを指定します。このコマンドを適用するインターフェイスに応じて、送信元アドレスまたは宛先アドレスを指定します。セキュリティの低いインターフェイスにこのコマンドを適用する場合は、送信元アドレスを指定します。セキュリティの高いインターフェイスにこのコマンドを適用する場合は、宛先アドレスを指定します。すべてのホストを指定するには、0 を指定します。
outside_mask	（オプション）外部 IP アドレスのネットワーク マスクを指定します。IP アドレスが 0 の場合は 0 を使用します。ホストには 255.255.255.255 を使用します。

server_tag	**aaa-server** コマンドで定義した AAA サーバ グループを指定します。
service	認証が必要なサービスを指定します。次のいずれかの値を指定できます。 • **any** または **tcp/0**（すべての TCP トラフィックを指定） • **ftp** • **http** • **https** • ***ssh*** • **telnet** • **tcp**/*port*[-*port*] • **udp**/*port*[-*port*] • **icmp**/*type* • *protocol*[/*port*[-*port*]] どのプロトコルまたはサービスへのネットワーク アクセスについても、認証を課すようにセキュリティ アプライアンスを設定することはできますが、ユーザは、HTTP、HTTPS、Telnet、または FTP のいずれかで認証を直接受けるだけで済みます。ユーザがこれらのサービスのいずれかで認証されると、セキュリティ アプライアンスは認証を必要とする別のトラフィックも許可します。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

アクセス リストで指定されているトラフィックの認証をイネーブルにするには、**aaa authentication match** コマンドを使用します。**match** コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションの中では使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することをお勧めします。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていないためです。

セキュリティ レベルが同じインターフェイス間で **aaa authentication include** および **exclude** コマンドを使用することはできません。この場合は、**aaa authentication match** コマンドを使用する必要があります。

TCP セッションのシーケンス番号は、シーケンス ランダム化をディセーブルにした場合でもランダム化されることがあります。この現象は、AAA サーバが TCP セッションを代行処理してユーザを認証し、アクセスを許可する場合に発生します。

ワンタイム認証

所定の IP アドレスを持つユーザは、認証セッションの期限が切れるまで、すべての規則およびタイプのいずれかで認証を 1 回受けるだけで済みます（タイムアウト値については、**timeout uauth** コマンドを参照してください）。たとえば、セキュリティ アプライアンスに Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションの継続中、FTP の認証を受ける必要がありません。

HTTP 認証または HTTPS 認証では、**timeout uauth** コマンドが非常に小さな値に設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」文字列をキャッシュして、当該サイトへの後続の接続すべてに使用するためです。この文字列が消去されるのは、ユーザが Web ブラウザのインスタンスをすべて終了し、再起動したときだけです。キャッシュをフラッシュしても意味がありません。

認証チャレンジの受信に必要なアプリケーション

どのプロトコルまたはサービスへのネットワーク アクセスについても、認証を課すようにセキュリティ アプライアンスを設定することはできますが、ユーザは、HTTP、HTTPS、Telnet、または FTP のいずれかで認証を直接受けるだけで済みます。ユーザがこれらのサービスのいずれかで認証されると、セキュリティ アプライアンスは認証を必要とする別のトラフィックも許可します。

セキュリティ アプライアンスが AAA 用にサポートしている認証ポートは、固定値です。

- FTP の場合はポート 21
- Telnet の場合はポート 23
- HTTP の場合はポート 80
- HTTPS の場合はポート 443

セキュリティ アプライアンスの認証プロンプト

Telnet および FTP では、セキュリティ アプライアンスが認証プロンプトを生成します。

HTTP では、セキュリティ アプライアンスはデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

HTTPS では、セキュリティ アプライアンスがカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

リダイレクションは基本方式を改良した機能です。リダイレクションを使用すると、認証時のユーザ エクスペリエンスが向上すると共に、Easy VPN モードとファイアウォール モードのどちらのモードでも HTTP および HTTPS に関して同質のユーザ エクスペリエンスが提供されます。セキュリティ アプライアンスでの直接認証もサポートされています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換規則を作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれているような非ブラウザ アプリケーションでは、基本認証との互換性が高い可能性があります。

正しく認証されると、セキュリティ アプライアンスによって元の宛先にリダイレクトされます。宛先サーバにも独自の認証手続きがある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

(注) **aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントからセキュリティ アプライアンスに送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することをお勧めします。

FTP では、ユーザがセキュリティ アプライアンスのユーザ名、アットマーク（@）、FTP ユーザ名（name1@name2 形式）を入力するオプションがあります。パスワードを入力するとき、ユーザはセキュリティ アプライアンスのパスワードに続けてアットマーク（@）を入力し、次に FTP パスワードを入力します（password1@password2）。たとえば、次のように入力します。

```
name> jamiec@jchrichton
password> letmein@he110
```

この機能が役立つのは、ファイアウォールをカスケードしていて、複数のログインが必要になる場合です。名前やパスワードが複数ある場合は、アットマーク（@）を複数使用して、それぞれを区切ります。

許可されるログイン試行の回数は、サポートされているプロトコルによって次のように異なります。

プロトコル	許可されるログイン試行の回数
FTP	間違ったパスワードを入力すると、接続がただちにドロップされる。
HTTP HTTPS	ログインが成功するまで、何回でもプロンプトが再表示される。
Telnet	4 回失敗すると接続がドロップされる。

スタティック PAT と HTTP

HTTP の認証では、スタティック PAT が設定されている場合、セキュリティ アプライアンスは実際のポートをチェックします。実際のポート 80 宛てのトラフィックを検出した場合、マッピング ポートが何番であるかにかかわらず、セキュリティ アプライアンスはその HTTP 接続を代行受信し、認証を強制します。

たとえば、外部 TCP ポート 889 が次のようにポート 80（www）に変換されていて、関係するすべてのアクセス リストでこのトラフィックが許可されているとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask
255.255.255.255
```

この場合、ユーザが 10.48.66.155 にポート 889 でアクセスしようとすると、セキュリティ アプライアンスがトラフィックを代行受信して HTTP 認証を強制します。セキュリティ アプライアンスが HTTP 接続の確立を許可する前に、ユーザの Web ブラウザに HTTP 認証ページが表示されます。

次の例のように、ローカル ポートが 80 以外になっているとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask
255.255.255.255
```

この場合、ユーザには認証ページが表示されません。代わりに、セキュリティ アプライアンスは Web ブラウザにエラー メッセージを送信して、要求されたサービスを使用するにはユーザが認証を受ける必要があることを通知します。

セキュリティ アプライアンスでの直接認証

HTTP、HTTPS、Telnet、または FTP がセキュリティ アプライアンスを通過することを許可せず、他のタイプのトラフィックに対しては認証を課す場合は、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用してセキュリティ アプライアンスで直接認証できます。

インターフェイスに対して AAA をイーブルにすると、セキュリティ アプライアンスでの直接認証が次の URL で可能になります。

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザはセキュリティ アプライアンス上で設定された所定の IP アドレスに Telnet で接続し、セキュリティ アプライアンスが Telnet プロンプトを提供します。

例

次の例は、外部インターフェイスで内部 IP アドレスが 192.168.0.0、ネットマスクが 255.255.0.0、すべてのホストの外部 IP アドレスの TCP トラフィックを tacacs+ というサーバ グループを使用して認証します。2 行目のコマンドでは、外部インターフェイスで、内部アドレスが 192.168.38.0、すべてのホストの外部 IP アドレスの Telnet トラフィックを認証から除外しています。

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.0.0 255.255.0.0 0 0
tacacs+
hostname(config)# aaa authentication exclude telnet outside 192.168.38.0 255.255.255.0
0 0 tacacs+
```

次の例は、*interface-name* パラメータの使用方法を示しています。セキュリティ アプライアンスには、内部ネットワーク　192.168.1.0、外部ネットワーク　209.165.201.0（サブネット　マスク 255.255.255.224）、および境界ネットワーク 209.165.202.128（サブネット マスク 255.255.255.224）が接続されています。

次の例では、内部ネットワークから外部ネットワーク宛てに送信される接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、内部ネットワークから境界ネットワーク宛てに送信される接続の認証をイネーブルにします。

```
hostname(config)#aaa authentication include tcp/0 inside 192.168.1.0 255.255.255.0
209.165.202.128 255.255.255.224 tacacs+
```

次の例では、外部ネットワークから内部ネットワーク宛てに送信される接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 outside 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224 tacacs+
```

次の例では、外部ネットワークから境界ネットワーク宛てに送信される接続の認証をイネーブルにします。

```
hostname(config)# aaa authentication include tcp/0 outside 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

次の例では、境界ネットワークから外部ネットワーク宛てに送信される接続の認証をイネーブルにします。

```
hostname(config)#aaa authentication include tcp/0 perimeter 209.165.202.128
255.255.255.224 209.165.201.0 255.255.255.224 tacacs+
```

関連コマンド

コマンド	説明
aaa authentication console	特権モードに入るときの認証をイネーブルまたはディセーブルにします。あるいは、指定した接続タイプでセキュリティ アプライアンスにアクセスする場合に、認証確認を要求します。
aaa authentication match	照合用のアクセス リストの名前（事前に **access-list** コマンドで定義したもの）を指定して、一致した場合に認証します。
aaa authentication secure-http-client	HTTP 要求がセキュリティ アプライアンスを通過することを許可する前に、セキュリティ アプライアンスに対してセキュアなユーザ認証方式を提供します。
aaa-server protocol	グループ関連のサーバ アトリビュートを設定します。
aaa-server host	ホスト関連のアトリビュートを設定します。

aaa authentication console

SSH、HTTP、Telnet 接続を介して、またはセキュリティ アプライアンスの Console コネクタからセキュリティ アプライアンス コンソールにアクセスするときの認証サービスをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication console** コマンドを使用します。このコマンドで、特権 EXEC モードへのアクセスもイネーブルになります。この認証サービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication {**serial** | **enable** | **telnet** | **ssh** | **http**} **console** {*server-tag* [**LOCAL**] | **LOCAL**}

no aaa authentication {**serial | enable | telnet | ssh | http**} **console** {*server-tag* [**LOCAL**] | **LOCAL**}

シンタックスの説明

enable	**enable** コマンドを使用して特権 EXEC モードで入力したエントリの認証をイネーブルにします。
http	HTTPS 接続の ASDM セッションの認証をイネーブルにします。HTTP の管理認証では、SDI サーバ グループのプロトコルをサポートしていません。
LOCAL	***LOCAL*** キーワードには、2 つの使用方法があります。ローカル データベースを使用するように指定する方法と、指定した認証サーバを利用できない場合にローカル データベースにフォールバックするように指定する方法です。
serial	シリアル コンソール インターフェイスで確立した管理セッションの認証をイネーブルにします。
server-tag	**aaa-server protocol** コマンドで定義した AAA サーバ グループ タグを指定します。 **LOCAL** というサーバ グループタグを指定すると、ローカルのユーザ データベースを使用できます。
ssh	SSH の管理セッションの認証をイネーブルにします。
telnet	Telnet 接続の管理セッションの認証をイネーブルにします。

デフォルト

デフォルトでは、ローカル データベースへのフォールバックはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

CLI 認証をイネーブルにした場合は、セキュリティ アプライアンスが、ログイン用のユーザ名とパスワードを入力するように求めるプロンプトを表示します。必要な情報を入力すると、ユーザ EXEC モードにアクセスできます。

特権 EXEC モードに入るには、**enable** コマンドか、**login** コマンド（ローカル データベースだけを使用している場合）を入力します。

イネーブル認証を設定した場合は、セキュリティ アプライアンスが、ユーザ名とパスワードを入力するように求めるプロンプトを表示します。イネーブル認証を設定していない場合は、**enable** コマンドを入力するときにシステム イネーブル パスワード（**enable password** コマンドで設定）を入力します。ただし、イネーブル認証を使用しないと、**enable** コマンドを入力した後で、特定のユーザとしてログインすることはありません。ユーザ名を維持したい場合は、イネーブル認証を使用してください。この機能は、コマンドの認証を行う場合、つまりユーザが入力できるコマンドを、ユーザ名で決める場合に特に便利です。

ローカル データベースを使って認証する場合は、**login** コマンドを使用できます。この場合は、ユーザ名が維持され、認証を有効にする設定は必要ありません。

セキュリティ アプライアンスで Telnet、SSH、または HTTP のユーザの認証を開始する前に、**telnet**、**ssh**、および **http** コマンドを使用してセキュリティ アプライアンスへのアクセスを設定する必要があります。これらのコマンドで、セキュリティ アプライアンスと通信できる IP アドレスが決まります。Telnet 接続では、内部インターフェイスおよび IPSec を設定した外部インターフェイスからセキュリティ アプライアンス コンソールにアクセスできます。SSH の場合は、どのインターフェイスからでもセキュリティ アプライアンス コンソールにアクセスできます。

http キーワードは、HTTPS を使用してセキュリティ アプライアンスにアクセスする ASDM クライアントを認証します。HTTP 認証は、AAA サーバを使用する場合だけ設定する必要があります。デフォルトでは、このコマンドを設定しなくても、ASDM は認証用にローカル データベースを使用します。HTTP 管理認証では、AAA サーバ グループ用に SDI プロトコルをサポートしていません。

認証用に AAA サーバ グループを使う場合は、セキュリティ アプライアンスで AAA サーバを利用できないときにローカル データベースをフォールバックとして使用するように設定できます。このためには、サーバ グループ名の次に **LOCAL** と入力します（**LOCAL** は必ず大文字で入力してください）。ローカル データベースのユーザ名とパスワードは、AAA サーバと同じものにすることをお勧めします。これは、セキュリティ アプライアンスのプロンプトには、どちらの方法で認証しているかが示されないからです。

ローカル データベースを主な認証方法（フォールバックなし）にすることもできます。この場合は、**LOCAL** だけを入力します。

HTTP 認証で要求できるユーザ名の最大長は、30 文字です。パスワードの最大長は 16 文字です。

次の表に、このコマンドで指定したオプションによって、セキュリティ アプライアンス コンソールへのアクセスを認証するときの処理がどのように異なるかを示します。

オプション	許可されるログイン試行の回数
Enable	3 回失敗するとアクセスが拒否される。
Serial	成功するまで何回でも試行できる。
SSH	3 回失敗するとアクセスが拒否される。
Telnet	成功するまで何回でも試行できる。
HTTP	成功するまで何回でも試行できる。

SSH での認証要求がタイムアウトになった（AAA サーバがダウンしているか利用できない）場合は、**pix** というユーザ名とイネーブル パスワード（**enable password** コマンドで設定）を使用してセキュリティ アプライアンスにアクセスできます。デフォルトでは、イネーブル パスワードはブラ

ンクです。この動作は、AAA が設定されていない状態でセキュリティ アプライアンスにログインする場合と異なります。AAA が設定されていない場合は、ログイン パスワード（**passwd** コマンドで設定）を使用します。

aaa authentication http console コマンド文を定義していない場合は、ASDM を使用して、ユーザ名とセキュリティ アプライアンスのイネーブル パスワード（**enable password** コマンドで設定）を入力しなくてもセキュリティ アプライアンスにアクセスできます。**aaa** コマンドを定義した場合でも、HTTP の認証要求がタイムアウトしたとき（AAA サーバがダウンしているか利用できない）は、デフォルトの管理者ユーザ名とイネーブル パスワードを使用してセキュリティ アプライアンスにアクセスできます。デフォルトでは、イネーブル パスワードは設定されていません。

例

次の例は、「radius」というサーバ タグの RADIUS サーバへの Telnet 接続で **aaa authentication console** コマンドを使用する方法を示しています。

```
hostname(config)# aaa authentication telnet console radius
```

次の例では、サーバ グループ「AuthIn」を管理認証用に指定しています。

```
hostname(config)# aaa authentication enable console AuthIn
```

次の例は、**aaa authentication console** コマンドを使用して、グループ「srvgrp1」内のすべてのサーバが利用できない場合に LOCAL ユーザ データベースにフォールバックするようにする方法を示しています。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config)# aaa authentication serial console srvgrp1 LOCAL
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	ユーザ認証用の AAA サーバ グループを指定します。
clear configure aaa	設定済みの AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication listener

ネットワーク ユーザを認証するために HTTP（S）リスニング ポートをイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authentication listener** コマンドを使用します。リスニング ポートをイネーブルにすると、セキュリティ アプライアンスは直接接続や通過トラフィックに対して認証ページを提供します。リスナーをディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

no aaa authentication listener http[**s**] *interface_name* [**port** *portnum*] [**redirect**]

シンタックスの説明

http[s]	リッスンするプロトコル（HTTP または HTTPS のいずれか）を指定します。このコマンドはプロトコルごとに入力します。
port *portnum*	セキュリティ アプライアンスがリッスンするポート番号を指定します。デフォルトは 80（HTTP）および 443（HTTPS）です。
redirect	セキュリティ アプライアンスによって提供される認証 Web ページに通過トラフィックをリダイレクトします。このキーワードを指定しないと、認証 Web ページにアクセスできるのはセキュリティ アプライアンス インターフェイス宛てのトラフィックだけとなります。
interface_name	リスナーをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトでは、イネーブルになっているリスナー サービスはなく、HTTP 接続は基本 HTTP 認証を使用します。リスナーをイネーブルにした場合、デフォルト ポートは 80（HTTP）および 443（HTTPS）です。

7.2(1) からアップグレードしている場合、リスナーはポート 1080（HTTP）および 1443（HTTPS）でイネーブルになります。**redirect** オプションもイネーブルになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

aaa authentication listener コマンドを使用しないと、**aaa authentication match** コマンドまたは **aaa authentication include** コマンドの設定後に HTTP（S）ユーザがセキュリティ アプライアンスで認証を受ける必要があるとき、セキュリティ アプライアンスは基本 HTTP 認証を使用します。HTTPS では、セキュリティ アプライアンスがカスタム ログイン画面を生成します。

aaa authentication listener コマンドを **redirect** キーワードと共に設定した場合、セキュリティ アプライアンスはすべての HTTP（S）認証要求を、セキュリティ アプライアンスが提供する Web ページにリダイレクトします。

リダイレクションは基本方式を改良した機能です。リダイレクションを使用すると、認証時のユーザ エクスペリエンスが向上すると共に、Easy VPN モードとファイアウォール モードのどちらのモードでも HTTP および HTTPS に関して同質のユーザ エクスペリエンスが提供されます。セキュリティ アプライアンスでの直接認証もサポートされています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換規則を作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれているような非ブラウザ アプリケーションでは、基本認証との互換性が高い可能性があります。

redirect オプションを *含めずに* **aaa authentication listener** コマンドを入力した場合は、セキュリティ アプライアンスでの直接認証だけがイネーブルになり、通過トラフィックは基本 HTTP 認証を使用することになります。**redirect** オプションを含めると、直接認証と通過トラフィック認証の両方がイネーブルになります。直接認証は、認証チャレンジをサポートしていないトラフィック タイプを認証する場合に役立ちます。他のサービスを使用する前に、各ユーザをセキュリティ アプライアンスで直接認証できます。

例

次の例では、HTTP 接続および HTTPS 接続をデフォルト ポートにリダイレクトするようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# aaa authentication http redirect
hostname(config)# aaa authentication https redirect
```

次の例では、直接セキュリティ アプライアンスに向かう認証要求を許可しています。通過トラフィックは基本 HTTP 認証を使用します。

```
hostname(config)# aaa authentication http
hostname(config)# aaa authentication https
```

次の例では、HTTP 接続および HTTPS 接続をデフォルトではないポートにリダイレクトするようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# aaa authentication http port 1100 redirect
hostname(config)# aaa authentication https port 1400 redirect
```

関連コマンド

コマンド	説明
aaa authentication match	通過トラフィックのユーザ認証を設定します。
aaa authentication secure-http-client	
clear configure aaa	設定済みの AAA コンフィギュレーションを削除します。
show running-config aaa	AAA コンフィギュレーションを表示します。
virtual http	

aaa authentication match

セキュリティ アプライアンス経由のトラフィックを認証するには、グローバル コンフィギュレーション モードで **aaa authentication match** コマンドを使用します。認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

no aaa authentication match *acl_name interface_name* {*server_tag* | **LOCAL**}

シンタックスの説明

acl_name	拡張アクセス リストの名前を指定します。
interface_name	ユーザを認証するインターフェイスの名前を指定します。
LOCAL	ローカル ユーザ データベースを指定します。
server_tag	**aaa-server** コマンドで定義した AAA サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

aaa authentication match コマンドは、**include** コマンドおよび **exclude** コマンドと同じコンフィギュレーションの中では使用できません。**include** コマンドおよび **exclude** コマンドの代わりに **match** コマンドを使用することをお勧めします。**include** コマンドおよび **exclude** コマンドは ASDM によってサポートされていないためです。

TCP セッションのシーケンス番号は、シーケンス ランダム化をディセーブルにした場合でもランダム化されることがあります。この現象は、AAA サーバが TCP セッションを代行処理してユーザを認証し、アクセスを許可する場合に発生します。

ワンタイム認証

所定の IP アドレスを持つユーザは、認証セッションの期限が切れるまで、すべての規則およびタイプのいずれかで認証を 1 回受けるだけで済みます（タイムアウト値については、**timeout uauth** コマンドを参照してください）。たとえば、セキュリティ アプライアンスに Telnet と FTP の認証を設定した場合、最初に Telnet の認証に成功したユーザは、その認証セッションの継続中、FTP の認証を受ける必要がありません。

HTTP 認証または HTTPS 認証では、**timeout uauth** コマンドが非常に小さな値に設定されている場合でも、一度認証されたユーザの再認証が必要になることはありません。これは、ブラウザが「Basic=Uuhjksdkfhk==」文字列をキャッシュして、当該サイトへの後続の接続すべてに使用するためです。この文字列が消去されるのは、ユーザが Web ブラウザのインスタンスをすべて終了し、再起動したときだけです。キャッシュをフラッシュしても意味がありません。

認証チャレンジの受信に必要なアプリケーション

どのプロトコルまたはサービスへのネットワーク アクセスについても、認証を課すようにセキュリティ アプライアンスを設定することはできますが、ユーザは、HTTP、HTTPS、Telnet、または FTP のいずれかで認証を直接受けるだけで済みます。ユーザがこれらのサービスのいずれかで認証されると、セキュリティ アプライアンスは認証を必要とする別のトラフィックも許可します。

セキュリティ アプライアンスが AAA 用にサポートしている認証ポートは、固定値です。

- FTP の場合はポート 21
- Telnet の場合はポート 23
- HTTP の場合はポート 80
- HTTPS の場合はポート 443

セキュリティ アプライアンスの認証プロンプト

Telnet および FTP では、セキュリティ アプライアンスが認証プロンプトを生成します。

HTTP では、セキュリティ アプライアンスはデフォルトで基本 HTTP 認証を使用し、認証プロンプトを提供します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

HTTPS では、セキュリティ アプライアンスがカスタム ログイン画面を生成します。ユーザがユーザ名とパスワードを入力できる内部 Web ページにユーザをリダイレクトするようにセキュリティ アプライアンスを設定することもできます（**aaa authentication listener** コマンドで設定します）。

リダイレクションは基本方式を改良した機能です。リダイレクションを使用すると、認証時のユーザ エクスペリエンスが向上すると共に、Easy VPN モードとファイアウォール モードのどちらのモードでも HTTP および HTTPS に関して同質のユーザ エクスペリエンスが提供されます。セキュリティ アプライアンスでの直接認証もサポートされています。

基本 HTTP 認証を使用し続けた方がよい場合もあります。セキュリティ アプライアンスでリスニング ポートを開く必要がない場合や、ルータ上の NAT を使用しているため、セキュリティ アプライアンスで提供される Web ページの変換規則を作成する必要がない場合、あるいは基本 HTTP 認証の方がネットワークで効果的に機能する場合です。たとえば、電子メールに URL が埋め込まれているような非ブラウザ アプリケーションでは、基本認証との互換性が高い可能性があります。

正しく認証されると、セキュリティ アプライアンスによって元の宛先にリダイレクトされます。宛先サーバにも独自の認証手続きがある場合、ユーザは別のユーザ名とパスワードを入力します。基本 HTTP 認証を使用していて、宛先サーバ用に別のユーザ名とパスワードを入力する必要がある場合は、**virtual http** コマンドを設定する必要があります。

（注） **aaa authentication secure-http-client** コマンドを使用しないまま HTTP 認証を使用すると、ユーザ名とパスワードはクリア テキストでクライアントからセキュリティ アプライアンスに送信されます。HTTP 認証をイネーブルにする場合は、必ず **aaa authentication secure-http-client** コマンドを使用することをお勧めします。

FTP では、ユーザがセキュリティ アプライアンスのユーザ名、アットマーク（@）、FTP ユーザ名（name1@name2 形式）を入力するオプションがあります。パスワードを入力するとき、ユーザはセキュリティ アプライアンスのパスワードに続けてアットマーク（@）を入力し、次に FTP パスワードを入力します（password1@password2）。たとえば、次のように入力します。

```
name> jamiec@jchrichton
password> letmein@he110
```

この機能が役立つのは、ファイアウォールをカスケードしていて、複数のログインが必要になる場合です。名前やパスワードが複数ある場合は、アットマーク（@）を複数使用して、それぞれを区切ります。

許可されるログイン試行の回数は、サポートされているプロトコルによって次のように異なります。

プロトコル	許可されるログイン試行の回数
FTP	間違ったパスワードを入力すると、接続がただちにドロップされる。
HTTP HTTPS	ログインが成功するまで、何回でもプロンプトが再表示される。
Telnet	4 回失敗すると接続がドロップされる。

スタティック PAT と HTTP

HTTP の認証では、スタティック PAT が設定されている場合、セキュリティ アプライアンスは実際のポートをチェックします。実際のポート 80 宛てのトラフィックを検出した場合、マッピング ポートが何番であるかにかかわらず、セキュリティ アプライアンスはその HTTP 接続を代行受信し、認証を強制します。

たとえば、外部 TCP ポート 889 が次のようにポート 80（www）に変換されていて、関係するすべてのアクセス リストでこのトラフィックが許可されているとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 www netmask
255.255.255.255
```

この場合、ユーザが 10.48.66.155 にポート 889 でアクセスしようとすると、セキュリティ アプライアンスがトラフィックを代行受信して HTTP 認証を強制します。セキュリティ アプライアンスが HTTP 接続の確立を許可する前に、ユーザの Web ブラウザに HTTP 認証ページが表示されます。

次の例のように、ローカル ポートが 80 以外になっているとします。

```
static (inside,outside) tcp 10.48.66.155 889 192.168.123.10 111 netmask
255.255.255.255
```

この場合、ユーザには認証ページが表示されません。代わりに、セキュリティ アプライアンスは Web ブラウザにエラー メッセージを送信して、要求されたサービスを使用するにはユーザが認証を受ける必要があることを通知します。

セキュリティ アプライアンスでの直接認証

HTTP、HTTPS、Telnet、または FTP がセキュリティ アプライアンスを通過することを許可せず、他のタイプのトラフィックに対しては認証を課す場合は、**aaa authentication listener** コマンドを設定することで、HTTP または HTTPS を使用してセキュリティ アプライアンスで直接認証できます。

インターフェイスに対して AAA をイーブルにすると、セキュリティ アプライアンスでの直接認証が次の URL で可能になります。

http://*interface_ip*[**:***port*]**/netaccess/connstatus.html**
https://*interface_ip*[**:***port*]**/netaccess/connstatus.html**

または、仮想 Telnet を設定する方法もあります（**virtual telnet** コマンドを使用）。仮想 Telnet を設定した場合、ユーザはセキュリティ アプライアンス上で設定された所定の IP アドレスに Telnet で接続し、セキュリティ アプライアンスが Telnet プロンプトを提供します。

例

次の一連の例は、**aaa authentication match** コマンドの使用方法を示しています。

```
hostname(config)# show access-list
access-list mylist permit tcp 10.0.0.0 255.255.255.0 192.168.2.0 255.255.255.0
(hitcnt=0) access-list yourlist permit tcp any any (hitcnt=0)

hostname(config)# show running-config aaa
aaa authentication match mylist outbound TACACS+
```

この場合、次の 2 つのコマンドは同じ意味になります。

```
hostname(config)# aaa authentication match yourlist outbound tacacs

hostname(config)# aaa authentication include TCP/0 outbound 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 tacacs
```

aaa コマンド内のリストでは、**access-list** コマンド文を参照している部分が指定した順に処理されます。ここで、次のコマンドを入力するとします。

```
hostname(config)# aaa authentication match mylist outbound TACACS+
```

上のコマンドの後に、次のコマンドを入力します。

```
hostname(config)# aaa authentication match yourlist outbound tacacs
```

セキュリティ アプライアンスは、まず **mylist** 内の **access-list** コマンド文グループにトラフィックが一致しているかどうかを確かめ、次に **yourlist** 内の **access-list** コマンド文グループに一致しているかどうかを確かめます。

関連コマンド

コマンド	説明
aaa authorization	LOCAL ユーザ認可サービスまたは TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。
access-list extended	アクセス リストを作成します。または、ダウンロード可能なアクセス リストを使用します。
clear configure aaa	設定済みの AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authentication secure-http-client

SSL をイネーブルにして、HTTP クライアントとセキュリティ アプライアンスの間でのユーザ名とパスワードの交換を保護するには、グローバル コンフィギュレーション モードで **aaa authentication secure-http-client** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。**aaa authentication secure-http-client** コマンドは、ユーザの HTTP ベース Web 要求がセキュリティ アプライアンスを通過することを許可する前に、セキュリティ アプライアンスに対してセキュアなユーザ認証方式を提供します。

aaa authentication secure-http-client

no aaa authentication secure-http-client

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

aaa authentication secure-http-client コマンドは、（SSL を介して）HTTP クライアント認証を保護します。このコマンドは、HTTP カットスルー プロキシ認証に使用されます。

次に、**aaa authentication secure-http-client** コマンドの制限事項を示します。

- 実行時、許可される HTTPS 認証プロセスは最大で 16 個です。16 個の HTTPS 認証プロセスがすべて実行中である場合、認証を要求する 17 番目の新しい HTTPS 接続は許可されません。
- **uauth timeout 0** が設定されている（**uauth timeout** が 0 に設定されている）場合は、HTTPS 認証が機能しません。HTTPS 認証を受けた後、ブラウザが複数の TCP 接続を開始して Web ページのロードを試みると、最初の接続はそのまま許可されますが、後続の接続に対しては認証が発生します。その結果、ユーザが認証ページに正しいユーザ名とパスワードを毎回入力しても、繰り返し認証ページが表示されます。この現象を回避するには、**timeout uauth 0:0:1** コマンドを使用して、**uauth timeout** を 1 秒に設定します。ただし、この回避策ではウィンドウが 1 秒間開かれるため、このウィンドウを利用して、同じ送信元 IP アドレスからアクセスしてくる未認証のユーザがファイアウォールを通過する可能性があります。

- HTTPS 認証は SSL ポート 443 で発生するため、HTTP クライアントから HTTP サーバに向かうポート 443 上のトラフィックをブロックするように **access-list** コマンド文を設定しないでください。また、ポート 80 上の Web トラフィックに対してスタティック PAT を設定する場合は、SSL ポートに対してもスタティック PAT を設定する必要があります。次の例では、1 行目で Web トラフィックに対してスタティック PAT を設定しているため、2 行目を追加して、HTTPS 認証コンフィギュレーションをサポートする必要があります。

```
static (inside,outside) tcp 10.132.16.200 www 10.130.16.10 www
static (inside,outside) tcp 10.132.16.200 443 10.130.16.10 443
```

例

次の例では、HTTP トラフィックがセキュアに認証されるように設定しています。

```
hostname(config)# aaa authentication secure-http-client
hostname(config)# aaa authentication include http...
```

「...」は、*authen_service if_name local_ip local_mask* [*foreign_ip foreign_mask*] *server_tag* に適切な値を指定することを表します。

次のコマンドでは、HTTPS トラフィックがセキュアに認証されるように設定しています。

```
hostname (config)# aaa authentication include https...
```

「...」は、*authentication -service interface-name local-ip local-mask* [*foreign-ip foreign-mask*] *server-tag* に適切な値を指定することを表します。

（注） HTTPS トラフィックの場合、**aaa authentication secure-https-client** コマンドは不要です。

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上の LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブルにします。
virtual telnet	セキュリティ アプライアンス仮想サーバにアクセスします。

aaa authorization

セキュリティ アプライアンス経由のトラフィックを TACACS+ サーバを使用したユーザ認可の対象にするか、対象から除外するかを指定するには、グローバル コンフィギュレーション モードで **aaa authorization** コマンドを ***include*** キーワードまたは ***exclude*** キーワードと共に使用します。認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization {**include** | **exclude**} *authorization-service interface-name inside-ip inside-mask* [*outside-ip outside-mask*] *tacacs+-server-tag*

no aaa authorization {**include** | **exclude**} *authorization-service interface-name inside-ip inside-mask* [*outside-ip outside-mask*] *tacacs+-server-tag*

シンタックスの説明

authorization-service	認可の対象にする、または対象から除外するトラフィックのタイプを指定します。次のタイプがあります。 • **any**：すべてのトラフィックを認可します。 • **telnet**：Telnet のトラフィックを認可します。 • **ssh**：SSH のトラフィックを認可します。 • **ftp**：FTP のトラフィックを認可します。 • **http**：HTTP のトラフィックを認可します。 • **https**：HTTPS のトラフィックを認可します。 • **icmp**/*type*：指定したタイプの ICMP トラフィックを認可します。 • *proto*：指定した値または名前（**ip** や **igmp** など）の IP プロトコルを認可します。 • **tcp**/*port*[-*port*]：指定したポートまたはポートの範囲の TCP トラフィックを認可します。すべての TCP トラフィックを認可するには、**0** に指定します。 • **udp**/*port*[-*port*]：指定したポートまたはポートの範囲の UDP トラフィックを認可します。すべての UDP トラフィックを認可するには、**0** に指定します。 **（注）** ポート範囲を指定すると、予期できない結果が認可サーバで生じる可能性があります。セキュリティ アプライアンスでは、サーバが文字列を解析してポート範囲に変換できることを前提としており、ポート範囲を文字列としてサーバに送信します。実際には、すべてのサーバがこのような変換を実行するとは限りません。また、ユーザに対して特定のサービスだけを認可する場合もあります。ポート範囲を指定すると、サービスを個別に認可できません。
exclude	指定したサービスを認可から除外して、前に指定した規則の例外を作成します。
include	規則に合致したトラフィックを認可します。
inside-ip	認可が必要な接続の発信元または宛先となる内部（セキュリティ レベルが高い）のホストまたはネットワークの IP アドレスを指定します。このアドレスを **0** に設定すると、すべてのホストを指定できます。このコマンドでは、認可の適用対象にするインターフェイスとは無関係に、常にセキュリティの高い IP アドレスからセキュリティの低い IP アドレスの順に指定します。
inside-mask	*inside-ip* のネットワーク マスクを指定します。
interface-name	接続の開始側になるインターフェイスを指定します。

outside-ip	（オプション）トラフィックを認可する対象となる、外部の（セキュリティ レベルの低い）IP アドレスを指定します。すべてのホストを指定するには、***0*** を指定します。このコマンドでは、認可の適用対象にするインターフェイスとは無関係に、常にセキュリティの高い IP アドレスからセキュリティの低い IP アドレスの順に指定します。
outside-mask	（オプション）*outside-ip* のネットワーク マスク。
tacacs+-server-tag	**aaa-server protocol** コマンドで定義した TACACS+ サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**exclude** パラメータにより、ユーザが、特定のホスト（複数可）宛てのポートを指定して除外できるようになりました。

使用上のガイドライン

セキュリティ アプライアンスでは、TACACS+ を使用してネットワーク アクセス認可を実行するように設定できます。

aaa authorization include コマンドや **exclude** コマンドの代わりに、**aaa authorization match** コマンドを使用することをお勧めします。**aaa authorization include** コマンドおよび **exclude** コマンドは、**aaa authorization match** コマンドと同じコンフィギュレーションの中では使用できません。**aaa authorization match** コマンドは、アクセス リストを使用してトラフィックの一致を調べるため、この目的で使用するものとしては堅牢性の高いコマンドです。

セキュリティ レベルが同じインターフェイス間で **aaa authorization** コマンドを使用することはできません。この場合は、**aaa authorization match** コマンドを使用する必要があります。

認証の文と認可の文は、互いに独立しています。ただし、認証されていないトラフィックは、認可文に一致した場合でも拒否されます。ユーザが認可を受けるには、まずセキュリティ アプライアンスに認証される必要があります。特定の認可規則では、それに対応する認証は必要ありません。認証が必要となるのは、FTP、HTTP、または Telnet の場合だけで、認可クレデンシャルを入力するための対話型の方法がユーザに提供されます。所定の IP アドレスを持つユーザが認証を受ける必要があるのは、認証セッションが期限切れになっていない場合、すべての規則およびタイプのいずれかで 1 回だけです。このため、トラフィックが認証文に一致した場合でも、認可は発生する可能性があります。

ユーザが認証されると、セキュリティ アプライアンスは認可規則をチェックして、一致するトラフィックがあるかどうかを調べます。トラフィックが認可文に一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバは、そのトラフィックを許可するか拒否するかをユーザ プロファイルに基づいて判定し、セキュリティ アプライアンスに応答します。セキュリティ アプライアンスは、応答に含まれている認可規則を適用します。

ユーザに対してネットワーク アクセス認可を設定する方法については、TACACS+ サーバのマニュアルを参照してください。

最初の認可試行が失敗し、2 番目の試行でタイムアウトが発生した場合は、認可されなかったクライアントを **service resetinbound** コマンドを使用してリセットし、そのクライアントが接続の再転送を行わないようにします。次の例は、Telnet の認可タイムアウト メッセージを示しています。

```
Unable to connect to remote host: Connection timed out
```

例

次の例では、TACACS+ プロトコルを使用しています。

```
hostname(config)# aaa-server tplus1 protocol tacacs+
hostname(config)# aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)# aaa authentication include any inside 0 0 0 0 tplus1
hostname(config)# aaa authorization include any inside 0 0 0 0
hostname(config)# aaa accounting include any inside 0 0 0 0 tplus1
hostname(config)# aaa authentication serial console tplus1
```

この例では、最初のコマンド文で tplus1 という名前のサーバ グループを作成し、このグループ用に TACACS+ プロトコルを指定しています。2 番目のコマンドでは、IP アドレス 10.1.1.10 の認証サーバが内部インターフェイス上にあること、および tplus1 サーバ グループに含まれていることを指定しています。その次の 3 つのコマンド文で指定しているのは、外部インターフェイスを経由する外部ホスト宛て接続を開始するユーザ全員を tplus1 サーバ グループで認証すること、正常に認証されたユーザに対してはどのサービスの使用も認可すること、およびすべての発信接続情報をアカウンティング データベースに記録することです。最後のコマンド文では、セキュリティ アプライアンスのシリアル コンソールにアクセスするには、tplus1 サーバ グループから認証を受ける必要があることを指定しています。

次の例では、外部インターフェイスからの DNS ルックアップに対する認可をイネーブルにします。

```
hostname(config)# aaa authorization include udp/53 outside 0.0.0.0 0.0.0.0
```

次の例では、内部ホストから内部インターフェイスに到着する、ICMP エコー応答パケットの認可をイネーブルにします。

```
hostname(config)# aaa authorization include 1/0 inside 0.0.0.0 0.0.0.0
```

このように設定すると、ユーザは Telnet、HTTP、または FTP を使用して認証を受けない限り、外部ホストを ping できなくなります。

次の例では、内部ホストから内部インターフェイスに到着する ICMP エコー（ping）についてだけ認可をイネーブルにします。

```
hostname(config)# aaa authorization include 1/8 inside 0.0.0.0 0.0.0.0
```

関連コマンド

コマンド	説明
aaa authorization command	コマンドの実行が認可の対象となるかどうかを指定します。または、指定したサーバ グループ内のすべてのサーバがディセーブルである場合にローカル ユーザ データベースにフォールバックするよう管理認可を設定します。
aaa authorization match	特定の access-list コマンド名に対して LOCAL または TACACS+ のユーザ認可サービスをイネーブルまたはディセーブルにします。
clear configure aaa	設定済みの AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization command

管理アクセスのコマンドの認可をイネーブルにするには、グローバル コンフィギュレーション モードで **aaa authorization command** コマンドを使用します。コマンド認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization command {**LOCAL** | *tacacs+-server-tag* [**LOCAL**]}

no aaa authorization command {**LOCAL** | *tacacs+-server-tag* [**LOCAL**]}

シンタックスの説明

LOCAL	ローカル コマンドの認可に、ローカル ユーザ データベースを使用することを指定します（特権レベルを使用）。TACACS+ サーバ グループ タグの後に **LOCAL** を指定すると、ローカル ユーザ データベースは、TACACS+ サーバ グループが利用できない場合のフォールバックとしてだけコマンド認可に使用されます。
tacacs+-server-tag	TACACS+ 認可サーバの定義済みのサーバ グループ タグを指定します。**aaa-server protocol** コマンドで定義した AAA サーバ グループ タグを指定します。

デフォルト

デフォルトでは、認可のためのローカル データベースへのフォールバックはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが変更され、指定したグループ内のすべてのサーバがディセーブルである場合にローカル ユーザ データベースにフォールバックするよう管理認可を設定できるようになりました。

使用上のガイドライン

デフォルトでは、ログインすると、必要最低限のコマンドだけを使用できるユーザ EXEC モードにアクセスできるようになっています。**enable** コマンド（ローカル データベースを使用している場合は **login** コマンド）を入力すると、特権 EXEC モードにアクセスして、コンフィギュレーション コマンドを含む各種コマンドを使用できます。コマンドへのアクセスを制御する場合は、セキュリティ アプライアンスでコマンドの認可を設定して、どのコマンドをユーザが利用できるかを決めます。

次のコマンド認可方法のうちのいずれか一方を使用できます。

- ローカル データベース：**privilege** コマンドを使用して、セキュリティ アプライアンスのコマンドの特権レベルを設定します。ローカル ユーザが **enable** コマンド（**aaa authenticate enable console** コマンドでイネーブルにする）で認証を受けるか、**login** コマンドを入力してログインする場合は、セキュリティ アプライアンスが、このユーザをローカル データベースで定義されている特権レベルに所属させます。ユーザは、その特権レベル以下のコマンドにアクセスできます。ローカルでのコマンド認可によって、それぞれのユーザが、ある特権レベルに置かれ、自分の特権レベル以下のコマンドを入力できるようになります。セキュリティ アプライアンスでは、コマンドに 16 レベル（0 ～ 15）のうちの 1 つを割り当てられます。デフォルトでは、各コマンドの特権レベルが 0 か 15 になっています。

（注） ローカルでのコマンド認可は、ローカル データベース内のユーザ、および CLI による認証やイネーブル認証なしで使用できます。この場合は、**enable** コマンドを入力するときにシステム イネーブル パスワードを入力します。セキュリティ アプライアンスによって、特権レベルが 15 に設定されます。次に、各レベルのイネーブル パスワードを作成し、**enable** *n*（2 ～ 15）と入力したときに、セキュリティ アプライアンスによって該当するレベル *n* に設定されるようにします。これらのレベルは、ローカルでのコマンド認可をオンにしない限り使用されません。

- TACACS+ サーバ：ユーザまたはグループが CLI によるアクセスの認証を受けた後に使用できるコマンドを、TACACS+ サーバで設定します。ユーザが CLI で入力するすべてのコマンドが TACACS+ サーバでチェックされます。TACACS+ によるコマンドの認可をイネーブルした場合に、ユーザが CLI でコマンドを入力すると、セキュリティ アプライアンスは、そのコマンドとユーザ名を TACACS+ サーバに送信し、そのコマンドが認可されているかどうかを確かめます。

  TACACS+ によるコマンドの認可をイネーブルにする前に、TACACS+ サーバで定義されているユーザとしてセキュリティ アプライアンスにログインしていることと、セキュリティ アプライアンスの設定を続けるのに必要なコマンドの使用が認可されていることを確認してください。たとえば、全コマンドの使用が認可されている管理ユーザとしてログインします。他のユーザでログインしていると、ロックアウトされることがあります。

  TACACS+ サーバによるコマンドの認可を設定するときは、意図したとおりに認可機能が動作することを確認してから設定を保存してください。ただし、設定間違いが原因でロックアウトされた場合は、通常セキュリティ アプライアンスを再起動すると元どおりアクセスできるようになります。

  TACACS+ システムが安定していて信頼できることを確認してください。これには、通常、TACACS+ サーバ システムが完全な冗長構成になっていることと、セキュリティ アプライアンスへの完全な冗長接続があることが必要です。たとえば、TACACS+ サーバ プールに、インターフェイス 1 に接続しているサーバと、インターフェイス 2 に接続している別のサーバを含め、TACACS+ サーバが利用できない場合にローカルでのコマンド認可をフォールバックとして設定しておきます。

例

次の例は、tplus1 という名前の TACACS+ サーバ グループによるコマンド認可をイネーブルにする方法を示しています。

```
hostname(config)#aaa authorization command tplus1
```

次の例は、tplus1 サーバ グループ内のすべてのサーバが利用できない場合に、ローカル ユーザ データベースにフォールバックするよう管理認可を設定する方法を示しています。

```
hostname(config)#aaa authorization command tplus1 LOCAL
```

関連コマンド

コマンド	説明
aaa authorization	**aaa-server** コマンドで指定した LOCAL または TACACS+ サーバのユーザ認可、あるいは ASDM ユーザ認証のユーザ認可をイネーブルまたはディセーブルにします。
aaa-server host	ホスト関連のアトリビュートを設定します。
aaa-server protocol	グループ関連のサーバ アトリビュートを設定します。
clear configure aaa	設定済みの AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa authorization match

セキュリティ アプライアンス経由のトラフィックの TACACS+ サーバによるユーザ認可をイネーブルにするには、**aaa authorization match** コマンドを使用します。認可をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa authorization match *acl-name interface-name server-tag*

no aaa authorization match *acl-name interface-name server-tag*

シンタックスの説明

acl-name	認可するトラフィックを特定するアクセス リストの名前を指定します。**access-list** コマンドを参照してください。**permit** の ACE は、一致したトラフィックを認可することを、**deny** のエントリは認可から除外することを示します。
interface-name	接続の開始側になるインターフェイスを指定します。
server-tag	**aaa-server protocol** コマンドで定義した TACACS+ サーバ グループ タグを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスでは、TACACS+ を使用してネットワーク アクセス認可を実行するように設定できます。

aaa authorization include コマンドや **exclude** コマンドの代わりに、**aaa authorization match** コマンドを使用することをお勧めします。**aaa authorization include** コマンドおよび **exclude** コマンドは、**aaa authorization match** コマンドと同じコンフィギュレーションの中では使用できません。**aaa authorization match** コマンドは、アクセス リストを使用してトラフィックの一致を調べるため、この目的で使用するものとしては堅牢性の高いコマンドです。

認証の文と認可の文は、互いに独立しています。ただし、認証されていないトラフィックは、認可文に一致した場合でも拒否されます。ユーザが認可を受けるには、まずセキュリティ アプライアンスに認証される必要があります。特定の認可規則では、それに対応する認証は必要ありません。認証が必要となるのは、FTP、HTTP、または Telnet の場合だけで、認可クレデンシャルを入力するための対話型の方法がユーザに提供されます。所定の IP アドレスを持つユーザが認証を受ける必要があるのは、認証セッションが期限切れになっていない場合、すべての規則およびタイプのいずれかで 1 回だけです。このため、トラフィックが認証文に一致した場合でも、認可は発生する可能性があります。

ユーザが認証されると、セキュリティ アプライアンスは認可規則をチェックして、一致するトラフィックがあるかどうかを調べます。トラフィックが認可文に一致した場合、セキュリティ アプライアンスはユーザ名を TACACS+ サーバに送信します。TACACS+ サーバは、そのトラフィックを許可するか拒否するかをユーザ プロファイルに基づいて判定し、セキュリティ アプライアンスに応答します。セキュリティ アプライアンスは、応答に含まれている認可規則を適用します。

ユーザに対してネットワーク アクセス認可を設定する方法については、TACACS+ サーバのマニュアルを参照してください。

最初の認可試行が失敗し、2 番目の試行でタイムアウトが発生した場合は、認可されなかったクライアントを **service resetinbound** コマンドを使用してリセットし、そのクライアントが接続の再転送を行わないようにします。次の例は、Telnet の認可タイムアウト メッセージを示しています。

```
Unable to connect to remote host: Connection timed out
```

例

次の例では、tplus1 サーバ グループを **aaa** コマンドで使用しています。

```
hostname(config)#aaa-server tplus1 protocol tacacs+
hostname(config)#aaa-server tplus1 (inside) host 10.1.1.10 thekey timeout 20
hostname(config)#aaa authentication match authen1 inside tplus1
hostname(config)#aaa accounting match acct1 inside tplus1
hostname(config)#aaa authorization match myacl inside tplus1
```

この例では、最初のコマンド文で、tplus1 サーバ グループを TACACS+ グループとして定義しています。2 番目のコマンドでは、IP アドレス 10.1.1.10 の認証サーバが内部インターフェイス上にあること、および tplus1 サーバ グループに含まれていることを指定しています。次の 2 つのコマンド文では、内部インターフェイスを通過する、任意の外部ホスト宛てのすべての接続が、tplus1 サーバ グループを使用して認証され、かつアカウンティング データベースに記録されるように指定しています。最後のコマンド文では、myacl 内の ACE に一致するすべての接続が tplus1 サーバ グループ内の AAA サーバによって認可されることを指定しています。

関連コマンド

コマンド	説明
aaa authorization	**aaa-server** コマンドで指定した LOCAL または TACACS+ サーバのユーザ認可、あるいは ASDM ユーザ認証のユーザ認可をイネーブルまたはディセーブルにします。
clear configure aaa	すべての aaa コンフィギュレーション パラメータをデフォルト値にリセットします。
clear uauth	1 人のユーザまたは全ユーザの AAA 認可キャッシュと AAA 認証キャッシュを削除して、ユーザが次回に接続を作成するときに再認証を強制します。
show running-config aaa	AAA コンフィギュレーションを表示します。
show uauth	認証および認可の目的で認可サーバに提供されたユーザ名を表示します。また、ユーザ名がバインドされている IP アドレス、ユーザが認証されただけであるか、キャッシュされたサービスを持っているかを表示します。

aaa local authentication attempts max-fail

セキュリティ アプライアンスが所定のユーザ アカウントに対して許可するローカル ログイン試行の連続失敗回数を制限するには、グローバル コンフィギュレーション モードで **aaa local authentication attempts max-fail** コマンドを使用します。このコマンドは、ローカル ユーザ データベースによる認証だけに影響を及ぼします。この機能をディセーブルにして、ローカル ログイン試行が連続して何回失敗してもよいようにするには、このコマンドの **no** 形式を使用します。

aaa local authentication attempts max-fail *number*

シンタックスの説明

number	ユーザが、ロックアウトされるまでに間違ったパスワードを入力できる最大回数。1 ～ 16 の数値を指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを省略すると、ユーザが何回でも間違ったパスワードを入力できるようになります。

間違ったパスワードによるユーザのログイン試行が設定回数に達すると、ユーザはロックアウトされ、管理者によってユーザ名がアンロックされるまで、ログインに成功しません。ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

管理者は、デバイスからロックアウトされません。

ユーザが正常に認証された場合、またはセキュリティ アプライアンスがリブートした場合は、失敗試行回数が 0 にリセットされ、ロックアウト ステータスが No にリセットされます。

例

次の例は、**aaa local authentication attempts max-limits** コマンドを使用して、許可される失敗試行の最大回数を 2 に設定する方法を示しています。

```
hostname(config)# aaa local authentication attempts max-limits 2
hostname(config)#
```

関連コマンド

コマンド	説明
clear aaa local user lockout	指定したユーザのロックアウト ステータスを消去し、失敗試行カウンタを 0 に設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更せずに、失敗したユーザ認証試行の回数を 0 にリセットします。
show aaa local user	現在ロックされているユーザ名のリストを表示します。

aaa mac-exempt

認証および認可の対象から免除する定義済みの MAC アドレス リストの使用を指定するには、グローバル コンフィギュレーション モードで **aaa mac-exempt** コマンドを使用します。**aaa mac-exempt** コマンドは、1 つだけ追加できます。MAC アドレスのリストの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

aaa mac-exempt match *id*

no aaa mac-exempt match *id*

シンタックスの説明

id	**mac-list** コマンドで設定した MAC アドレス リストの番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

aaa mac-exempt コマンドを使用するには、事前に **mac-list** コマンドを使用して MAC リストの番号を設定しておく必要があります。MAC リストにある permit のエントリは、その MAC アドレスの認証と認可を免除することを、deny のエントリは、認証と認可がイネーブルになっている場合に、その MAC アドレスを認証および認可する必要があることを示します。**aaa mac-exempt** コマンドは 1 回しか入力できないので、使用する MAC リストに、免除するすべての MAC アドレスが含まれていることを確認してください。

例

次の例では、1 つの MAC アドレスについて認証をバイパスします。

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

次のエントリでは、ハードウェア ID が 0003.E3 であるすべての Cisco IP Phone について、認証をバイパスしています。

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

次の例では、00a0.c95d.02b2 以外の MAC アドレスのグループの認証をバイパスしています。

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルにします。
aaa authorization	ユーザ認可サービスをイネーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から免除します。
show running-config mac-list	**mac-list** コマンドで指定されている MAC アドレスのリストを表示します。
mac-list	MAC アドレスの認証や認可を免除するために使用する MAC アドレスのリストを指定します。

aaa proxy-limit

ユーザ 1 人あたりに許可する同時プロキシ接続の最大数を設定することで、uauth セッションの制限値を手動で設定するには、グローバル コンフィギュレーション モードで **aaa proxy-limit** コマンドを使用します。プロキシをディセーブルにするには、**disable** パラメータを使用します。デフォルトのプロキシ制限値（16）に戻すには、このコマンドの **no** 形式を使用します。

aaa proxy-limit ***proxy_limit***

aaa proxy-limit disable

no aaa proxy-limit

シンタックスの説明

disable	プロキシは許可されません。
proxy_limit	ユーザ 1 人あたりに許可する同時プロキシ接続の数（1 ～ 128）を指定します。

デフォルト

デフォルトのプロキシ制限値は 16 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

送信元アドレスがプロキシ サーバである場合は、その IP アドレスを認証の対象から除外するか、許容可能な未処理 AAA 要求の数を増やすことを検討してください。

例

次の例は、ユーザ 1 人あたりに許容可能な未処理認証要求の最大数を設定する方法を示しています。

```
hostname(config)# aaa proxy-limit 6
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、または ASDM ユーザ認証をイネーブル化、ディセーブル化、または表示します。
aaa authorization	LOCAL または TACACS+ ユーザ認可サービスをイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバを指定します。
clear configure aaa	設定済みの AAA アカウンティングの値を削除またはリセットします。
show running-config aaa	AAA コンフィギュレーションを表示します。

aaa-server host

AAA サーバ グループの一部として AAA サーバを設定したり、ホスト固有の AAA サーバ パラメータを設定したりするには、グローバル コンフィギュレーション モードで **aaa-server host** コマンドを使用します。**aaa-server host** コマンドを使用すると、AAA サーバ ホスト コンフィギュレーション モードに入ります。このモードから、ホスト固有の AAA サーバ接続データを指定および管理できます。ホストのコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

aaa-server *server-tag* [**(***interface-name***)**] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

no aaa-server *server-tag* [**(***interface-name***)**] **host** {*server-ip* | *name*} [*key*] [**timeout** *seconds*]

シンタックスの説明

(*interface-name***)**	（オプション）認証サーバが常駐するネットワーク インターフェイスを指定します。このパラメータにはカッコが必要です。インターフェイスを何も指定しないと、デフォルトで **inside** になります（使用できる場合）。
key	（オプション）127 文字までの英数字のキーワードで、RADIUS サーバまたは TACACS+ サーバ上のキーと同じ値にします。アルファベットの大文字と小文字が区別されます。128 文字以降に入力された文字は、すべて無視されます。このキーは、セキュリティ アプライアンスとサーバの間でやり取りするデータを暗号化するために使用されます。このキーは、セキュリティ アプライアンス システムとサーバ システムの両方で同じにする必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。ホスト モードで **key** コマンドを使用して、キーを追加または変更できます。
name	**name** コマンドを使用してローカルで割り当てたサーバ名か、DNS 名を指定します。DNS 名の最大長は 128 文字、**name** コマンドで割り当てる名前の最大長は 63 文字です。
server-ip	AAA サーバの IP アドレスを指定します。
server-tag	サーバ グループのシンボリック名。**aaa-server protocol** コマンドで指定した名前と同じにします。
timeout *seconds*	（オプション）要求のタイムアウト間隔。この時間を超えると、セキュリティ アプライアンスは、プライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスは要求をそのバックアップ サーバに送信します。ホスト モードで **timeout** コマンドを使用して、タイムアウト間隔を変更できます。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

デフォルトのインターフェイスは、inside です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	DNS 名をサポートするようになりました。

使用上のガイドライン

AAA サーバのコンフィギュレーションを制御するには、**aaa-server protocol** コマンドで AAA サーバ グループ プロトコルを定義してから、**aaa-server host** コマンドを使用してサーバをグループに追加します。

シングルモードでは最大 15 個のサーバ グループ、マルチモードではコンテキストごとに 4 個のサーバ グループを持つことができます。各グループには、シングルモードで最大 16 台、マルチモードで最大 4 台のサーバを含めることができます。ユーザがログインするときは、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 台ずつアクセスされます。

aaa-server host コマンドを入力したら、次に、ホスト特有のパラメータを設定します。

例

次の例では、「watchdogs」という名前の Kerberos AAA サーバ グループを設定し、そのグループに AAA サーバを追加し、そのサーバの Kerberos レルムを定義します。

（注） Kerberos レルム名に使用できるのは、数字と大文字のアルファベットのみです。セキュリティ アプライアンスでは、レルム名に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。必ず大文字のアルファベットだけを使用してください。

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
```

次の例では、「svrgrp1」という名前の SDI AAA サーバ グループを設定し、そのグループに AAA サーバを追加し、タイムアウト間隔を 6 秒に、リトライ間隔を 7 秒に、SDI バージョンをバージョン 5 に設定しています。

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config-aaa-server-group)# exit
hostname(config)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 6
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# sdi-version sdi-5
```

関連コマンド

コマンド	説明
aaa-server protocol	AAA サーバ グループを作成および修正します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

aaa-server protocol

AAA サーバ グループを作成し、グループ固有および全グループのホストに共通した AAA サーバ パラメータを設定するには、グローバル コンフィギュレーション モードで **aaa-server protocol** コマンドを使用して、AAA サーバ グループ モードに入ります。このモードから、グループ パラメータを設定できます。指定したグループを削除するには、このコマンドの **no** 形式を使用します。

aaa-server *server-tag* **protocol** *server-protocol*

no aaa-server *server-tag* **protocol** *server-protocol*

シンタックスの説明

server-tag	サーバ グループの名前。**aaa-server host** コマンドで指定した名前と同じにします。他の AAA コマンドで、この AAA サーバ グループ名を参照します。
server-protocol	グループ内のサーバがサポートする AAA プロトコル。**kerberos**、**ldap**、**nt**、**radius**、**sdi**、または **tacacs+**。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

AAA サーバのコンフィギュレーションを制御するには、**aaa-server protocol** コマンドで AAA サーバ グループ プロトコルを定義してから、**aaa-server host** コマンドを使用してサーバをグループに追加します。

シングルモードでは最大 15 個のサーバ グループ、マルチモードではコンテキストごとに 4 個のサーバ グループを持つことができます。各グループには、シングルモードで最大 16 台、マルチモードで最大 4 台のサーバを含めることができます。ユーザがログインするときは、コンフィギュレーション内で指定されている最初のサーバから順に、サーバが応答するまでこれらのサーバが 1 台ずつアクセスされます。

aaa-server protocol コマンドを入力したら、次に、ホスト特有のパラメータを設定します。たとえば、AAA アカウンティングを行っている場合は、**accounting-mode** コマンドで同時アカウンティングを設定しない限り、アカウンティング情報はアクティブなサーバだけに送られます。

例

次の例は、**aaa-server protocol** コマンドを使用して、TACACS+ サーバ グループの詳細設定を変更する方法を示しています。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# reactivation mode timed
hostname(config-aaa-server-group)# max-failed attempts 2
```

関連コマンド

コマンド	説明
accounting-mode	アカウンティング メッセージが 1 台のサーバに送信されるか（シングルモード）、グループ内のすべてのサーバに送信されるか（同時モード）を指定します。
reactivation-mode	障害の発生したサーバを再度有効にする方式を指定します。
max-failed-attempts	サーバ グループ内の所定のサーバが無効になるまでに、そのサーバで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

absolute

時間範囲が有効である場合に絶対時間を定義するには、時間範囲コンフィギュレーション モードで ***absolute*** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

absolute [**end** *time date*] [**start** *time date*]

no absolute

シンタックスの説明

date	日付を day month year 形式で指定します（たとえば、1 January 2006）。年の有効範囲は 1993 ～ 2035 です。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。

デフォルト

開始日時を指定しない場合、permit 文または deny 文がただちに有効になります。最遅終了時刻は 23:59 31 December 2035 です。終了日時を指定しない場合、関連付けられている permit 文または deny 文はこの時刻まで有効です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
時間範囲コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間ベース ACL を実装するには、***time-range*** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。その後、**access-list extended time-range** コマンドを使用して、時間範囲を ACL にバインドします。

例

次の例では、2006 年 1 月 1 日午前 8 時に ACL が有効になります。

```
hostname(config-time-range)# absolute start 8:00 1 January 2006
```

終了日時が指定されていないので、関連する ACL は無期限に有効になります。

関連コマンド

コマンド	説明
access-list extended	セキュリティ アプライアンス経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	***time-range*** コマンドの ***absolute*** キーワードと ***periodic*** キーワードの設定をデフォルトに戻します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

accept-subordinates

装置にインストールされていない下位 CA 証明書がフェーズ 1 の IKE 交換で提供されたときに、その証明書を受け入れるようにセキュリティ アプライアンスを設定するには、暗号 CA トラストポイント コンフィギュレーション モードで **accept-subordinates** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

accept-subordinates

no accept-subordinates

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト設定はオンです（下位証明書は受け入れられます）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェーズ 1 の処理中、IKE ピアは下位証明書と ID 証明書の両方を渡すことがあります。渡された下位証明書は、セキュリティ アプライアンスにインストールされていないことがあります。このコマンドを使用すると、装置上にトラストポイントとして設定されていない下位 CA 証明書をサポートできます。確立されたすべてのトラストポイントのすべての下位 CA 証明書が受け入れ可能である必要はありません。つまり、このコマンドを使用すると、装置は、証明書チェーン全体をローカルにインストールすることなく、その証明書チェーンを認証できます。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入って、トラストポイント central での下位証明書の受け入れをセキュリティ アプライアンスに許可しています。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# accept-subordinates
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。

access-group

アクセス リストをインターフェイスにバインドするには、グローバル コンフィギュレーション モードで **access-group** コマンドを使用します。アクセス リストをインターフェイスからアンバインドするには、このコマンドの **no** 形式を使用します。

access-group *access-list* {***in*** | ***out***} ***interface*** *interface_name* [*per-user-override*]

no access-group *access-list* {***in*** | ***out***} ***interface*** *interface_name*

シンタックスの説明

access-list	アクセス リスト *ID*。
in	指定したインターフェイスで着信パケットをフィルタリングします。
interface *interface-name*	ネットワーク インターフェイスの名前。
out	指定したインターフェイスで発信パケットをフィルタリングします。
per-user-override	（オプション）ダウンロードしたユーザ アクセス リストが、インターフェイスに適用されているアクセス リストを上書きできるようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

access-group コマンドは、アクセス リストをインターフェイスにバインドします。アクセス リストは、インターフェイス宛ての着信トラフィックに適用されます。**access-list** コマンド文に ***permit*** オプションを入力した場合は、セキュリティ アプライアンスはパケットの処理を続行します。**access-list** コマンド文に ***deny*** オプションを入力した場合は、セキュリティ アプライアンスはパケットを廃棄して、次の syslog メッセージを生成します。

```
%hostname-4-106019: IP packet from source_addr to destination_addr, protocol
protocol received from interface interface_name deny by access-group id
```

per-user-override オプションを指定すると、ダウンロードしたアクセス リストが、インターフェイスに適用されているアクセス リストを上書きできます。*per-user-override* オプション引数を指定しないと、セキュリティ アプライアンスは既存のフィルタリング動作を維持します。*per-user-override* を指定すると、セキュリティ アプライアンスは、ユーザに関連付けられているユーザごとのアクセス リスト（ダウンロードされた場合）内の ***permit*** ステータスまたは ***deny*** ステータスで、**access-group** コマンドに関連付けられているアクセス リスト内の permit ステータスまたは deny ステータスを上書きできるようにします。さらに、次の規則が適用されます。

- パケットが到着した時点で、そのパケットに関連付けられているユーザごとのアクセス リストがない場合、インターフェイス アクセス リストが適用される。
- ユーザごとのアクセス リストは、***timeout*** コマンドの ***uauth*** オプションで指定されたタイムアウト値によって管理されるが、このタイムアウト値は、ユーザごとの AAA セッション タイムアウト値によって上書きできる。
- 既存のアクセス リスト ログ動作は同じである。たとえば、ユーザごとのアクセス リストによってユーザ トラフィックが拒否された場合、syslog メッセージ 109025 が記録されます。ユーザトラフィックが許可された場合、syslog メッセージは生成されません。ユーザごとのアクセス リストのログ オプションは、影響を及ぼしません。

access-list コマンドは、必ず **access-group** コマンドと共に使用してください。

access-group コマンドは、アクセス リストをインターフェイスにバインドします。***in*** キーワードは、アクセス リストを、指定したインターフェイス上のトラフィックに適用します。***out*** キーワードは、アクセス リストを発信トラフィックに適用します。

（注） 1 つまたは複数の **access-group** コマンドによって参照されるアクセス リストから、すべての機能エントリ（permit 文および deny 文）を削除すると、**access-group** コマンドがコンフィギュレーションから自動的に削除されます。**access-group** コマンドは、空のアクセス リストも、コメントだけを含むアクセス リストも参照できません。

no access-group コマンドは、アクセス リストをインターフェイス *interface_name* からアンバインドします。

show running config access-group コマンドは、インターフェイスにバインドされている現在のアクセス リストを表示します。

clear configure access-group コマンドは、インターフェイスからすべてのアクセス リストを削除します。

例

次の例は、**access-group** コマンドの使用方法を示しています。

```
hostname(config)# static (inside,outside) 209.165.201.3 10.1.1.3
hostname(config)# access-list acl_out permit tcp any host 209.165.201.3 eq 80
hostname(config)# access-group acl_out in interface outside
```

この **static** コマンドでは、Web サーバ 10.1.1.3 にグローバル アドレス 209.165.201.3 を付与しています。**access-list** コマンドでは、すべてのホストがポート 80 を使用してグローバル アドレスにアクセスすることを許可しています。**access-group** コマンドでは、外部インターフェイスで受信するトラフィックに **access-list** コマンドを適用することを指定しています。

関連コマンド

コマンド	説明
access-list extended	アクセス リストを作成します。または、ダウンロード可能なアクセス リストを使用します。
clear configure access-group	すべてのインターフェイスからアクセス グループを削除します。
show running-config access-group	コンテキスト グループのメンバーを表示します。

access-list alert-interval

拒否フロー最大値到達メッセージ間の時間間隔を指定するには、グローバル コンフィギュレーション モードで **access-list alert-interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-list alert-interval *secs*

no access-list alert-interval

シンタックスの説明

secs	拒否フロー最大値到達メッセージが生成される時間間隔。有効な値は 1 ～ 3600 秒です。

デフォルト

デフォルトは 300 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

access-list alert-interval コマンドは、syslog メッセージ 106101 を生成する時間間隔を設定します。syslog メッセージ 106101 は、セキュリティ アプライアンスが拒否フローの最大数に達したことを警告します。拒否フローの最大数に達したとき、前回の 106101 メッセージが生成されてから *secs* 秒以上経過していた場合は、さらに 106101 メッセージが生成されます。

拒否フロー最大値到達メッセージの生成については、**access-list deny-flow-max** コマンドを参照してください。

例

次の例は、拒否フロー最大値到達メッセージ間の時間間隔を指定する方法を示しています。

```
hostname(config)# access-list alert-interval 30
```

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリを番号別に表示します。

access-list deny-flow-max

作成できる同時拒否フローの最大数を指定するには、グローバル コンフィギュレーション モードで **access-list deny-flow-max** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

access-list deny-flow-max

no access-list deny-flow-max

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトは 4096 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスが ACL 拒否フローの最大数 *n* に達すると、syslog メッセージ 106101 が生成されます。

例

次の例は、作成できる同時拒否フローの最大数を指定する方法を示しています。

```
hostname(config)# access-list deny-flow-max 256
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリを番号別に表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list ethertype

EtherType に基づいてトラフィックを制御するアクセス リストを設定するには、グローバル コンフィギュレーション モードで **access-list ethertype** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **ethertype** {***deny*** | ***permit***} {***ipx*** | ***bpdu*** | ***mpls-unicast*** | ***mpls-multicast*** | ***any*** | *hex_number*}

no access-list *id* **ethertype** {***deny*** | ***permit***} {***ipx*** | ***bpdu*** | ***mpls-unicast*** | ***mpls-multicast*** | ***any*** | *hex_number*}

シンタックスの説明

any	すべてのものへのアクセスを指定します。
bpdu	ブリッジ プロトコル データ ユニットへのアクセスを指定します。デフォルトでは、BPDU は拒否されます。
deny	条件に合致している場合、アクセスを拒否します。
hex_number	EtherType を示す 0x600 以上の 16 ビット 16 進数値。
id	アクセス リストの名前または番号。
ipx	IPX へのアクセスを指定します。
mpls-multicast	MPLS マルチキャストへのアクセスを指定します。
mpls-unicast	MPLS ユニキャストへのアクセスを指定します。
permit	条件に合致している場合、アクセスを許可します。

デフォルト

デフォルトは次のとおりです。

- 特にアクセスを許可しない限り、セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについて syslog メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。

log オプション キーワードを指定したときの syslog メッセージ 106100 のデフォルト レベルは、6（情報）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、16 ビット 16 進数値で示された任意の EtherType を制御できます。EtherType ACL は、イーサネット V2 フレームをサポートしています。802.3 形式のフレームはタイプ フィールドではなく長さフィールドを使用するため、ACL によって処理されません。ブリッジ プロトコル データ ユニットだけは例外で、ACL によって処理されます。ブリッジ プロトコル データ ユニットは、SNAP 方式でカプセル化されており、セキュリティ アプライアンスは BPDU を処理するように設計されています。

EtherType はコネクションレス型であるため、両方向のトラフィックを通過させる場合は、両方のインターフェイスに ACL を適用する必要があります。

MPLS を許可する場合は、セキュリティ アプライアンスに接続されている両方の MPLS ルータが LDP セッションまたは TDP セッション用のルータ ID としてセキュリティ アプライアンス インターフェイス上の IP アドレスを使用するように設定することにより、LDP TCP 接続と TDP TCP 接続がセキュリティ アプライアンス経由で確立されるようにします（LDP および TDP では、MPLS ルータが、パケット転送用のラベル（アドレス）をネゴシエートできます）。

インターフェイスの方向ごとに、各タイプ（拡張または EtherType）の ACL を 1 つだけ適用できます。同じ ACL を複数のインターフェイスに適用することもできます。

（注） EtherType アクセス リストが ***deny all*** に設定されている場合、すべてのイーサネット フレームが廃棄されます。物理プロトコル トラフィック（オートネゴシエーションなど）だけが許可されます。

例

次の例は、EtherType アクセス リストを追加する方法を示しています。

```
hostname(config)# access-list ETHER ethertype permit ipx
hostname(config)# access-list ETHER ethertype permit bpdu
hostname(config)# access-list ETHER ethertype permit mpls-unicast
hostname(config)# access-group ETHER in interface inside
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
clear access-group	アクセス リスト カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリを番号別に表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list extended

アクセス コントロール エントリを追加するには、グローバル コンフィギュレーション モードで **access-list extended** コマンドを使用します。1 つのアクセス リストに、同じアクセス リスト ID を持つ 1 つまたは複数の ACE が入っています。アクセス リストを使って、ネットワークへのアクセスを制御したり、各種機能で処理するトラフィックを指定したりします。ACE を削除するには、このコマンドの **no** 形式を使用します。アクセス リスト全体を削除するには、**clear configure access-list** コマンドを使用します。

access-list *id* [***line*** *line-number*] [***extended***] {**deny** | **permit**}{*protocol* | **object-group** *protocol_obj_grp_id*}{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}[*operator port* | **object-group** *service_obj_grp_id*]{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*][***log*** [[*level*] [***interval*** *secs*] | ***disable*** | ***default***]] [***inactive*** | ***time-range*** *time_range_name*]

no access-list *id* [***line*** *line-number*] [***extended***] {**deny** | **permit**} {**tcp** | **udp**}{*src_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}[*operator port*] | **object-group** *service_obj_grp_id*]{*dest_ip mask* | **interface** *ifc_name* | **object-group** *network_obj_grp_id*}[*operator port* | **object-group** *service_obj_grp_id* | **object-group** *icmp_type_obj_grp_id*][***log*** [[*level*] [***interval*** *secs*] | ***disable*** | ***default***]][***inactive*** | ***time-range*** *time_range_name*]

シンタックスの説明

default	（オプション）ロギング方法をデフォルト（拒否パケットごとにシステム ログ メッセージ 106023 を送信）に設定します。
deny	条件を満たした場合に、パケットを拒否します。ネットワーク アクセスを制御する場合（**access-group** コマンドを使用）は、このキーワードでパケットがセキュリティ アプライアンスを通過しないようにします。クラスマップの検査を適用する場合（**class-map** と **inspect** コマンドを使用）は、このキーワードでトラフィックを検査の対象から免除します。機能の中には、ACE を拒否できないもの（NAT など）があります。詳しくは、アクセス リストを使用する各機能のコマンドの説明を参照してください。
dest_ip	パケットの送信先となるネットワークまたはホストの IP アドレスを指定します。単一の IP アドレスを指定するには、**host** キーワードに続けて IP アドレスを入力します。この場合は、マスクを入力しないでください。すべてのアドレスを指定するには、アドレスおよびマスクの代わりに **any** キーワードを入力します。
disable	（オプション）この ACE のロギングをディセーブルにします。
icmp_type	（オプション）使用するプロトコルが **icmp** の場合に、そのタイプを指定します。
id	アクセス リストの ID を 241 文字までの文字列または整数で指定します。大文字と小文字が区別されます。ヒント：コンフィギュレーション内で ID を区別しやすくするには、すべて大文字で指定します。
inactive	（オプション）ACE をディセーブルにします。イネーブルに戻すには、**inactive** キーワードなしで、ACE 全体を入力します。この機能を使うと、アクティブでない ACE のレコードをコンフィギュレーションに残しておけるので、イネーブルに戻しやすくなります。

interface *ifc_name*	送信元アドレスまたは宛先アドレスとしてのインターフェイス アドレスを指定します。 **（注）** トラフィックの宛先がデバイス インターフェイスである場合、アクセス リストに実際の IP アドレスを指定する代わりに interface キーワードを指定する必要があります。
interval *secs*	（オプション）システム ログ メッセージ 106100 を生成する間隔を指定します。有効な値は 1 ～ 600 秒です。デフォルトは 300 です。
level	（オプション）システム ログ メッセージ 106100 のレベル（0 ～ 7）を設定します。デフォルトは 6 です。
line *line-num*	（オプション）ACE の挿入先となる行の番号を指定します。行番号を指定しない場合、ACE はアクセス リストの末尾に追加されます。行番号は、コンフィギュレーションに保存されません。ACE を挿入する場所を指定するだけです。
log	（オプション）ネットワーク アクセスを制御（**access-group** コマンドでアクセス リストを適用）するときに、deny の ACE に一致するパケットのロギング オプションを設定します。引数なしで **log** キーワードを入力すると、デフォルトのレベル（6）のシステム ログ メッセージ 106100 がデフォルトの間隔（300 秒）で生成されます。log キーワードを入力しないと、システム ログ メッセージ 106023 のデフォルトのログが生成されます。
mask	IP アドレスのサブネット マスク。ネットワーク マスクを指定する方法は、Cisco IOS ソフトウェアの **access-list** コマンドと異なります。セキュリティ アプライアンスでは、ネットワーク マスク（たとえば、クラス C マスクは 255.255.255.0）を使用します。一方、Cisco IOS のマスクでは、ワイルドカード ビット（0.0.0.255 など）を使います。
object-group *icmp_type_obj_grp_id*	（オプション）使用するプロトコルが **icmp** の場合に、ICMP タイプのオブジェクト グループの ID を指定します。オブジェクト グループの追加については、**object-group icmp-type** コマンドを参照してください。
object-group *network_obj_grp_id*	ネットワーク オブジェクト グループの ID を指定します。オブジェクト グループの追加については、**object-group network** コマンドを参照してください。
object-group *protocol_obj_grp_id*	プロトコル オブジェクト グループの ID を指定します。オブジェクト グループの追加については、**object-group protocol** コマンドを参照してください。
object-group *service_obj_grp_id*	（オプション）プロトコルを **tcp** または **udp** に設定する場合に、サービス オブジェクト グループの ID を指定します。オブジェクト グループの追加については、**object-group service** コマンドを参照してください。
operator	（オプション）発信元または宛先のポート番号を照合します。使用できる演算子は次のとおりです。 • **lt**：より小さい • **gt**：より大きい • **eq**：等しい • **neq**：等しくない • **range**：値の範囲。この演算子を使うときは、次の例のように、ポート番号を 2 つ指定します。 `range 100 200`

permit	条件を満たした場合に、パケットを許可します。ネットワーク アクセスを制御する場合（**access-group** コマンドを使用）は、このキーワードでパケットがセキュリティ アプライアンスを通過するようにします。クラス マップの検査を適用（**class-map** と **inspect** コマンドを使用）する場合は、このキーワードでパケットを検査の対象に含めます。
port	（オプション）プロトコルを **tcp** または **udp** に設定する場合に、TCP ポートまたは UDP ポートの番号（整数）か名前を指定します。DNS、Discard、Echo、Ident、NTP、RPC、SUNRPC、Talk では、それぞれ TCP ポートを 1 つと UDP ポートを 1 つ定義する必要があります。TACACS+ では、TCP のポート 49 の定義が 1 つ必要です。
protocol	IP プロトコルの名前または番号を指定します。たとえば、UDP は 17、TCP は 6、EGP は 47 になります。
src_ip	パケットの送信元となるネットワークまたはホストの IP アドレスを指定します。単一の IP アドレスを指定するには、**host** キーワードに続けて IP アドレスを入力します。この場合は、マスクを入力しないでください。すべてのアドレスを指定するには、アドレスおよびマスクの代わりに **any** キーワードを入力します。
time-range *time_range_name*	（オプション）時間の範囲を決めて、各 ACE が特定の日時にアクティブになるようにします。時間範囲を定義する方法については、**time-range** コマンドを参照してください。

デフォルト

デフォルトは次のとおりです。

- ACE のログ機能によって、拒否パケットの syslog メッセージ 106023 が生成されます。拒否されたパケットを記録するには、deny の ACE が存在する必要があります。
- **log** キーワードを指定した場合は、syslog メッセージ 106100 のデフォルトのレベルは 6（情報）、間隔は 300 秒になります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

指定した名前のアクセス リスト用に入力した各 ACE は、ACE の行番号を指定しない限り、そのアクセス リストの最後に追加されます。

ACE の順番は重要です。セキュリティ アプライアンスがパケットを転送するかドロップするかを決めるときは、リストにある順番どおりに ACE を 1 つずつチェックしていきます。一致するものが見つかったら、残りの ACE はチェックされません。たとえば、アクセス リストの先頭にすべてのトラフィックを明示的に許可する ACE を作成した場合は、残りの ACE がまったくチェックされなくなります。

アクセス リストの最後には、暗黙的な拒否が設定されているので、明示的に許可しない限り、トラフィックを通過させることはできません。たとえば、セキュリティ アプライアンス経由で、特定のアドレスを除いた全ユーザにネットワークへのアクセスを許可するには、まず特定のアドレスの拒否を設定し、次に、他のすべてのアドレスを許可します。

NAT を使用する場合は、アクセス リストで指定する IP アドレスは、アクセス リストを関連付けているインターフェイスによって異なります。必ず、そのインターフェイスに接続するネットワークで有効なアドレスを使用してください。これは、着信と発信の両方のアクセス グループにあてはまります。使用するアドレスは、アクセスの方向ではなく、インターフェイスによって決まります。

TCP 接続と UDP 接続では、リターン トラフィックを許可するアクセス リストは必要ありません。これは、FWSM は、確立された双方向接続のすべてのトラフィックを許可するからです。一方、ICMP などのコネクションレス型のプロトコルでは、セキュリティ アプライアンスは、単方向のセッションを確立します。そのため、双方向の ICMP パケットを許可するアクセス リストを設定（発信元と宛先の両方のインターフェイスにアクセス リストを適用）するか、ICMP の検査エンジンをイネーブルにする必要があります。ICMP の検査エンジンは、ICMP セッションを双方向接続と見なします。

ICMP はコネクションレス型のプロトコルなので、双方向の ICMP パケットを許可するアクセス リストを設定（発信元と宛先の両方のインターフェイスにアクセス リストを適用）するか、ICMP の検査エンジンをイネーブルにする必要があります。ICMP 検査エンジンは、ICMP セッションをステートフル接続と見なします。ping を制御するには、**echo-reply (0)**（セキュリティ アプライアンスからホストへ）、または **echo (8)**（ホストからセキュリティ アプライアンスへ）を指定します。ICMP のタイプについては、表 2-1 を参照してください。

インターフェイスの方向ごとに、各タイプ（extended または EtherType）のアクセス リストを 1 つだけ適用できます。同じアクセス リストを複数のインターフェイスに適用できます。インターフェイスにアクセス リストを適用する方法については、**access-group** コマンドを参照してください。

（注） アクセス リストの設定を変更し、既存の接続がタイムアウトするのを待たずに新しいアクセス リスト情報を使用したい場合は、**clear local-host** コマンドを使用して接続を消去します。

表 2-1 に、使用できる ICMP タイプの値を示します。

表 2-1　ICMP タイプのリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply

表 2-1　ICMP タイプのリテラル（続き）

ICMP タイプ	リテラル
15	information-request
16	information-reply
17	mask-request
18	mask-reply
30	traceroute
31	conversion-error
32	mobile-redirect

例

次のアクセス リストは、このアクセス リストを適用するインターフェイスの全ホストからのセキュリティ アプライアンスへのアクセスを許可しています。

```
hostname(config)# access-list ACL_IN extended permit ip any any
```

次のアクセス リストは、192.168.1.0/24 のホストから 209.165.201.0/27 のネットワークにアクセスできないようにしています。他のアドレスはすべて許可しています。

```
hostname(config)# access-list ACL_IN extended deny tcp 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
hostname(config)# access-list ACL_IN extended permit ip any any
```

あるホストだけがアクセスできるようにする場合は、アクセスを限定する ACE を入力します。明示的に許可しない限り、デフォルトで他のすべてのトラフィックが拒否されます。

```
hostname(config)# access-list ACL_IN extended permit ip 192.168.1.0 255.255.255.0
209.165.201.0 255.255.255.224
```

次のアクセス リストは、このアクセス リストを適用するインターフェイスの全ホストが 209.165.201.29 というアドレスの Web サイトにアクセスできないようにしています。この他のトラフィックは、すべて許可されます。

```
hostname(config)# access-list ACL_IN extended deny tcp any host 209.165.201.29 eq www
hostname(config)# access-list ACL_IN extended permit ip any any
```

次のアクセス リストは、オブジェクト グループを使用して、内部ネットワークの数個のホストから、Web サーバのいくつかにアクセスできないようにしています。この他のトラフィックは、すべて許可されます。

```
hostname(config-network)# access-list ACL_IN extended deny tcp object-group denied
object-group web eq www
hostname(config)# access-list ACL_IN extended permit ip any any
hostname(config)# access-group ACL_IN in interface inside
```

あるネットワーク オブジェクト グループ（A）から別のネットワーク オブジェクト グループ（B）へのトラフィックを許可するアクセス リストを一時的にディセーブルにするには、次のように入力します。

```
hostname(config)# access-list 104 permit ip host object-group A object-group B
inactive
```

時間ベースアクセス リストを実装するには、***time-range*** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間の範囲をアクセス リストにバインドします。次の例では、「Sales」という名前のアクセス リストを「New_York_Minute」という名前の時間範囲にバインドしています。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

時間範囲を定義する方法の詳細については、**time-range** コマンドを参照してください。

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
clear access-group	アクセス リスト カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	ACE を番号別に表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list remark

access-list extended コマンドの前または後に追加するコメントのテキストを指定するには、グローバル コンフィギュレーション モードで **access-list remark** コマンドを使用します。コメントをディセーブルにするには、このコマンドの **no** 形式を使用します。

access-list *id* [***line*** *line-num*] **remark** *text*

no access-list *id* [***line*** *line-num*] **remark** [*text*]

シンタックスの説明

id	アクセス リストの名前。
line *line-num*	（オプション）コメントまたはアクセス コントロール エレメント（ACE）の挿入先となる行番号。
remark text	**access-list extended** コマンドの前または後に追加するコメントのテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

最大 100 文字（スペースや句読点を含む）をコメント テキストとして入力できます。コメント テキストには、スペース以外の文字を少なくとも 1 つ含める必要があります。空のコメントを入力することはできません。

コメントだけを含む ACL で **access-group** コマンドを使用することはできません。

例

次の例は、**access-list** コマンドの前または後に追加するコメントのテキストを指定する方法を示しています。

```
hostname(config)# access-list 77 remark checklist
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、セキュリティ アプライアンスを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリを番号別に表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list standard

アクセス リストを追加して、OSPF 再配布のルートマップに使用できる、OSPF ルートの宛先 IP アドレスを指定するには、グローバル コンフィギュレーション モードで **access-list standard** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **standard** [***line*** *line-num*] {***deny*** | ***permit***} {***any*** | ***host*** *ip_address* | *ip_address subnet_mask*}

no access-list *id* **standard** [***line*** *line-num*] {***deny*** | ***permit***} {***any*** | ***host*** *ip_address* | *ip_address subnet_mask*}

シンタックスの説明

any	すべてのものへのアクセスを指定します。
deny	条件に合致している場合、アクセスを拒否します。説明については、「使用上のガイドライン」を参照してください。
host *ip_address*	ホスト IP アドレスへのアクセスを指定します。
id	アクセス リストの名前または番号。
ip_address ip_mask	特定の IP アドレスおよびサブネット マスクへのアクセスを指定します。
line *line-num*	（オプション）ACE の挿入先となる行番号。
permit	条件に合致している場合、アクセスを許可します。説明については、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトは次のとおりです。

- 特にアクセスを許可しない限り、セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについて syslog メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-group コマンドと共に **deny** オプション キーワードを使用すると、パケットがセキュリティ アプライアンスを通過できなくなります。デフォルトでは、特にアクセスを許可しない限り、セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。

TCP や UDP など、すべてのインターネット プロトコルに一致するよう *protocol* を指定するには、**ip** キーワードを使用します。

オブジェクト グループの設定方法については、**object-group** コマンドの項を参照してください。

アクセス リストをグループ化するには、**object-group** コマンドを使用します。

送信元アドレス、ローカル アドレス、または宛先アドレスを指定する場合のガイドラインは、次のとおりです。

- 32 ビットの 4 分割ドット付き 10 進数形式を使用する。
- アドレスとマスクを 0.0.0.0 0.0.0.0 にする場合は、短縮形の ***any*** キーワードを使用する。このキーワードは、IPSec では使用しないことをお勧めします。

マスクを 255.255.255.255 にする場合は、短縮形の ***host*** *address* を使用します。

例

次の例は、ファイアウォール経由の IP トラフィックを拒否する方法を示しています。

```
hostname(config)# access-list 77 standard deny
```

次の例は、条件に合致している場合に、ファイアウォール経由の IP トラフィックを許可する方法を示しています。

```
hostname(config)# access-list 77 standard permit
```

関連コマンド

コマンド	説明
access-group	コンフィギュレーションの最適化に使用できるオブジェクト グループを定義します。
clear access-group	アクセス リスト カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリを番号別に表示します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

access-list webtype

WebVPN のフィルタリングをサポートするコンフィギュレーションにアクセス リストを追加するには、グローバル コンフィギュレーション モードで **access-list webtype** コマンドを使用します。アクセス リストを削除するには、このコマンドの **no** 形式を使用します。

access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | ***any***] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [***time_range*** *name*]]

no access-list *id* **webtype** {**deny** | **permit**} **url** [*url_string* | ***any***] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [***time_range*** *name*]]

access-list *id* **webtype** {**deny** | **permit**} **tcp** [***host*** *ip_address* | *ip_address subnet_mask* | ***any***] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [***time_range*** *name*]]

no **access-list** *id* **webtype** {**deny** | **permit**} **tcp** [***host*** *ip_address* | *ip_address subnet_mask* | ***any***] [*oper port* [*port*]] [**log** [[**disable** | **default**] | *level*] [**interval** *secs*] [***time_range*** *name*]]

シンタックスの説明

any	すべての IP アドレスを指定します。
any	（オプション）すべての URL を指定します。
deny	条件に合致している場合、アクセスを拒否します。
host *ip_address*	ホスト IP アドレスを指定します。
id	アクセス リストの名前または番号。
interval *secs*	（オプション）syslog メッセージ 106100 を生成する時間間隔を指定します。有効値の範囲は 1 ～ 600 秒です。
ip_address ip_mask	特定の IP アドレスおよびサブネット マスクを指定します。
log [[**disable** | **default**] | *level*]	（オプション）ACE 用に syslog メッセージ 106100 が生成されるように指定します。詳細については、**log** コマンドを参照してください。
oper	*ip_address* ポートを比較します。使用できる演算子は、lt（小なり）、gt（大なり）、eq（同値）、neq（非同値）、および range（範囲）です。
permit	条件に合致している場合、アクセスを許可します。
port	TCP ポートまたは UDP ポートの 10 進数または名前を指定します。
time_range *name*	（オプション）time-range オプションをこのアクセス リスト要素に付加するためのキーワードを指定します。
url	フィルタリングに URL を使用することを指定します。
url_string	（オプション）フィルタリングされる URL を指定します。

デフォルト

デフォルトは次のとおりです。

- 特にアクセスを許可しない限り、セキュリティ アプライアンスによって、発信元インターフェイス上のすべてのパケットが拒否されます。
- ACL ロギングでは、拒否されたパケットについて syslog メッセージ 106023 が生成されます。拒否されたパケットをログに記録するには、パケットを明示的に拒否する必要があります。
- **log** オプション キーワードを指定したときの syslog メッセージ 106100 のデフォルト レベルは、6（情報）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

access-list webtype コマンドは、WebVPN フィルタリングを設定するために使用されます。指定する URL は、全体でも一部（ファイル指定なし）でもよく、サーバを示すワイルドカードを含めることも、ポートを指定することもできます。

有効なプロトコル識別子は、http、https、cifs、imap4、pop3、および smtp です。URL に ***any*** キーワードを含めて、すべての URL を指すことができます。アスタリスクを使用して、DNS 名のサブコンポーネントを指すこともできます。

例

次の例は、特定の企業の URL へのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://*.company.com
```

次の例は、特定のファイルへのアクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_file webtype deny url
https://www.company.com/dir/file.html
```

次の例は、すべての場所へのポート 8080 経由の HTTP アクセスを拒否する方法を示しています。

```
hostname(config)# access-list acl_company webtype deny url http://my-server:8080/*
```

関連コマンド

コマンド	説明
access-group	コンフィギュレーションの最適化に使用できるオブジェクトグループを定義します。
access-list ethertype	トラフィックを EtherType に基づいて制御するためのアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
clear access-group	アクセス リスト カウンタを消去します。
show running-config access-list	セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示します。

accounting-mode

アカウンティング メッセージが 1 台のサーバに送信されるか（シングルモード）、グループ内のすべてのサーバに送信されるか（同時モード）を指定するには、AAA サーバ グループ モードで **accounting-mode** コマンドを使用します。アカウンティング モードの指定を削除するには、このコマンドの **no** 形式を使用します。

accounting-mode {**simultaneous** | **single**}

シンタックスの説明

simultaneous	グループ内のすべてのサーバにアカウンティング メッセージを送信します。
single	1 台のサーバにアカウンティング メッセージを送信します。

デフォルト

デフォルト値はシングルモードです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ グループ	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

1 台のサーバにアカウンティング メッセージを送信するには、***single*** キーワードを使用します。サーバ グループ内のすべてのサーバにアカウンティング メッセージを送信するには、***simultaneous*** キーワードを使用します。

このコマンドは、アカウンティング（RADIUS または TACACS+）にサーバ グループを使用する場合に限り有効です。

例

次の例は、**accounting-mode** コマンドを使用して、グループ内のすべてのサーバにアカウンティング メッセージを送信する方法を示しています。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# accounting-mode simultaneous
hostname(config-aaa-server-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa accounting	アカウンティング サービスをイネーブルまたはディセーブルにします。
aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードに入って、グループ内のすべてのホストに共通する、グループ固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-port

特定のホストの RADIUS アカウンティングに使用するポート番号を指定するには、AAA サーバ ホスト モードで **accounting-port** コマンドを使用します。認証ポートの指定を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、アカウンティング レコードの送信先となる、リモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定します。

accounting-port *port*

no accounting-port

シンタックスの説明

port	RADIUS アカウンティング用のポート番号（1 ～ 65535）。

デフォルト

デフォルトでは、デバイスはポート 1646 で RADIUS アカウンティングをリッスンします（RFC 2058 に準拠）。ポートを指定しない場合は、RADIUS アカウンティングのデフォルト ポート番号（1646）が使用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS アカウンティング サーバが 1646 以外のポートを使用する場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、セキュリティ アプライアンスで適切なポートを設定する必要があります。

このコマンドは、RADIUS に設定されているサーバ グループに限り有効です。

例

次の例では、ホスト「1.2.3.4」に対して「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒に、リトライ間隔を 7 秒に、アカウンティング ポートを 2222 に設定しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# accounting-port 2222
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa accounting	ユーザがアクセスしたネットワーク サービスのレコードを保持します。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入ります。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

accounting-server-group

アカウンティング レコード送信用の AAA サーバ グループを指定するには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **accounting-server-group** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの ***no*** 形式を使用します。

accounting-server-group *server-group*

no accounting-server-group

シンタックスの説明

server-group	AAA サーバ グループの名前を指定します。デフォルトでは ***NONE*** になっています。

デフォルト

デフォルトでは、このコマンドの設定は ***NONE*** になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドが、webvpn コンフィギュレーション モードからトンネル グループ一般アトリビュート コンフィギュレーション モードに変更されました。

使用上のガイドライン

すべてのトンネル グループ タイプにこのアトリビュートを適用できます。

例

トンネル グループ一般アトリビュート コンフィギュレーション モードに入る次の例では、IPSec LAN-to-LAN トンネル グループ「xyz」に「aaa-server123」という名前のアカウンティング サーバ グループを設定しています。

```
hostname(config)# tunnel-group xyz type IPSec_L2L
hostname(config)# tunnel-group xyz general-attributes
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般アトリビュートを指定します。

accounting-server-group（webvpn）

WebVPN または電子メール プロキシで使用するアカウンティング サーバ グループを指定するには、**accounting-server-group** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、このコマンドは該当する電子メール プロキシ モードで使用します。コンフィギュレーションからアカウンティング サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、アカウンティングを使用して、ユーザがアクセスするネットワーク リソースを追跡します。

accounting-server-group *group tag*

no accounting-server-group

シンタックスの説明

group tag	設定済みのアカウンティング サーバまたはサーバ グループを指定します。アカウンティング サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。

デフォルト

デフォルトでは、アカウンティング サーバは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	•	—	—	•
Imap4s	•	•	—	—	•
Pop3s	•	•	—	—	•
SMTPS	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは廃止されました。accounting-server-group コマンドは、トンネル グループ一般アトリビュート コンフィギュレーション モードで使用されるようになりました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

例

次の例は、WEBVPNACCT という名前のアカウンティング サーバ グループを使用するように WebVPN サービスを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# accounting-server-group WEBVPNACCT
```

次の例は、POP3SSVRS という名前のアカウンティング サーバ グループを使用するように POP3S 電子メール プロキシを設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# accounting-server-group POP3SSVRS
```

関連コマンド

コマンド	説明
aaa-server host	認証、認可、アカウンティング サーバを設定します。

CHAPTER 3

acl-netmask-convert コマンド～ auto-update timeout コマンド

acl-netmask-convert

RADIUS サーバから受信したダウンロード可能な ACL 内のネットマスクをセキュリティ アプライアンスがどのように扱うかを指定するには、AAA サーバ ホスト モードで **acl-netmask-convert** コマンドを使用します。このモードには、**aaa-server host** コマンドを使用してアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

acl-netmask-convert {**auto-detect** | **standard** | **wildcard**}

no acl-netmask-convert

シンタックスの説明

auto-detect	セキュリティ アプライアンスが、使用されているネットマスク表現のタイプを判断するように指定します。セキュリティ アプライアンスは、ワイルドカード ネットマスク表現を検出すると、標準ネットマスク表現に変換します。このキーワードの詳細については、「使用上のガイドライン」を参照してください。
standard	セキュリティ アプライアンスが、RADIUS サーバから受信したダウンロード可能な ACL に標準ネットマスク表現だけが含まれていると見なすように指定します。ワイルドカード ネットマスク表現からの変換は行われません。
wildcard	セキュリティ アプライアンスが、RADIUS サーバから受信したダウンロード可能な ACL にワイルドカード ネットマスク表現だけが含まれていると見なし、ACL のダウンロード時にその表現をすべて標準ネットマスク表現に変換するように指定します。

デフォルト

デフォルトでは、ワイルドカード ネットマスク表現からの変換は行われません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

RADIUS サーバがワイルドカード形式のネットマスクを含むダウンロード可能な ACL を提供する場合は、wildcard キーワードまたは auto-detect キーワードと共に **acl-netmask-convert** コマンドを使用します。セキュリティ アプライアンスは、ダウンロード可能な ACL に標準ネットマスク表現が含まれていると予想します。一方、Cisco Secure VPN 3000 シリーズ コンセントレータは、ダウンロード可能な ACL に、標準ネットマスク表現とは逆のワイルドカード ネットマスク表現が含まれていると予想します。ワイルドカード マスクでは、無視するビット位置には 1 が、一致する必要のあるビット位置には 0 が置かれます。**acl-netmask-convert** コマンドを使用すると、このような違いが、RADIUS サーバ上でダウンロード可能な ACL を設定する方法に及ぼす影響を最小限に抑えることができます。

auto-detect キーワードは、RADIUS サーバがどのように設定されているかわからない場合に役立ちます。ただし、ワイルドカード ネットマスク表現に「穴」があると、その表現が正しく検出されず、変換されません。たとえば、ワイルドカード ネットマスク 0.0.255.0 は、第 3 オクテットがどのような数値であっても許可し、Cisco VPN 3000 シリーズ コンセントレータで有効に使用できますが、セキュリティ アプライアンスはこの表現をワイルドカード ネットマスクとして検出できません。

例

次の例では、ホスト「192.168.3.4」に対して「srvgrp1」という名前の RADIUS AAA サーバを設定し、ダウンロード可能な ACL のネットマスク変換をイネーブルにして、タイムアウトを 9 秒に、リトライ間隔を 7 秒に、認証ポートを 1650 に設定しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# acl-netmask-convert wildcard
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、または ASDM ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入ります。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

action-uri

Web サーバの URI を指定してシングル サインオン認証用のユーザ名とパスワードを受信するには、AAA サーバ ホスト コンフィギュレーション モードで **action-uri** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

URI パラメータ値をリセットするには、このコマンドの **no** 形式を使用します。新しい値を入力するには、**action-uri** コマンドを再度使用します。

action-uri *string*

no action-uri

（注） HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

string	認証プログラムの URI。複数の行に入力できます。各行の最大文字数は 255 文字です。URI 全体の最大文字数は 2,048 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

URI（ユニフォーム リソース識別子）は、インターネット上のコンテンツの位置を特定するコンパクトな文字列です。URI で表されるコンテンツには、テキスト ページ、ビデオ クリップ、サウンド クリップ、静止画、動画、プログラムなどがあります。URI の最も一般的な形式は Web ページ アドレスです。Web ページ アドレスは、URI の特定の形式（つまりサブセット）で、Uniform Resource Locator（URL; ユニフォーム リソース ロケータ）と呼ばれます。

セキュリティ アプライアンスの WebVPN サーバは、POST 要求を使用してシングル サインオン認証要求を認証 Web サーバに送信します。この処理が実行されるようにするには、HTTP POST 要求を使用して認証 Web サーバ上のアクション URI にユーザ名とパスワードを渡すようにセキュリティ アプライアンスを設定します。**action-uri** コマンドは、セキュリティ アプライアンスが POST 要求を送信する先の Web サーバ上の認証プログラムの場所と名前を指定します。

認証 Web サーバ上のアクション URI は、認証 Web サーバのログイン ページにブラウザで直接接続するとわかります。ブラウザに表示されるログイン Web ページの URL が、認証 Web サーバのアクション URI です。

入力しやすいように、URI は連続する複数の行に入力できるようになっています。各行は入力と同時にセキュリティ アプライアンスによって連結され、URI が構成されます。action-uri 行の 1 行あたりの最大文字数は 255 文字ですが、それより少ない文字を各行に入力できます。

（注） 文字列に疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次の例では、認証データを受信する URI は次のとおりです。

http://www.example.com/auth/index.html/appdir/authc/forms/MCOlogin.fcc?TYPE=33554433&REALMOID=06-000a1311-a828-1185-ab41-8333b16a0008&GUID=&SMAUTHREASON=0&METHOD=GET&SMAGENTNAME=SM5FZmjnk3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6rB1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F%2Fauth.example.com

AAA サーバ ホスト コンフィギュレーション モードで入力した次の例では、www.example.com の上記の URI を指定しています。

```
hostname(config)# aaa-server testgrp1 host www.example.com
hostname(config-aaa-server-host)# action-uri http://www.example.com/auth/index.htm
hostname(config-aaa-server-host)# action-uri l/appdir/authc/forms/MCOlogin.fcc?TYP
hostname(config-aaa-server-host)# action-uri 554433&REALMOID=06-000a1311-a828-1185
hostname(config-aaa-server-host)# action-uri -ab41-8333b16a0008&GUID=&SMAUTHREASON
hostname(config-aaa-server-host)# action-uri =0&METHOD=GET&SMAGENTNAME=$SM$5FZmjnk
hostname(config-aaa-server-host)# action-uri 3DRNwNjk2KcqVCFbIrNT9%2bJ0H0KPshFtg6r
hostname(config-aaa-server-host)# action-uri B1UV2PxkHqLw%3d%3d&TARGET=https%3A%2F
hostname(config-aaa-server-host)# action-uri %2Fauth.example.com
hostname(config-aaa-server-host)#
```

（注） ホスト名とプロトコルをアクション URI に含める必要があります。上記の例では、URI の最初にある http://www.example.com にそれらが含まれています。

関連コマンド

コマンド	説明
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	SSO サーバとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求のパラメータの名前を指定します。
start-url	事前ログイン クッキーの取得先 URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

activation-key

セキュリティ アプライアンスのアクティベーション キーを変更し、セキュリティ アプライアンス上で運用されているアクティベーション キーをセキュリティ アプライアンスのフラッシュ パーティションに隠しファイルとして保存されているアクティベーション キーと比較してチェックするには、グローバル コンフィギュレーション モードで **activation-key** コマンドを使用します。

activation-key [*activation-key-four-tuple*| *activation-key-five-tuple*]

シンタックスの説明

activation-key-four-tuple	アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。
activation-key-five-tuple	アクティベーション キー。形式のガイドラインについては、「使用上のガイドライン」を参照してください。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•		•

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

各要素の間にスペースを 1 つ入れて、4 つの要素で構成される 16 進数文字列として *activation-key-four-tuple* を入力します。または、各要素の間にスペースを 1 つ入れて、5 つの要素で構成される 16 進数文字列として、*activation-key-five-tuple* を入力します。次に例を示します。

```
0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

先頭部分の 0x 指定子は省略できます。値は、すべて 16 進数であると見なされます。

キーはコンフィギュレーション ファイルに保存されず、シリアル番号に関連付けられます。

例

次の例は、セキュリティ アプライアンスのアクティベーション キーを変更する方法を示しています。

```
hostname(config)# activation-key 0xe02888da 0x4ba7bed6 0xf1c123ae 0xffd8624e
```

関連コマンド

コマンド	説明
show activation-key	アクティベーション キーを表示します。

address-pool

リモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定するには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **address-pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの ***no*** 形式を使用します。

address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

no address-pool [(*interface name*)] *address_pool1* [*...address_pool6*]

シンタックスの説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
interface name	（オプション）アドレス プールに使用するインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスを指定しない場合、このコマンドは、明示的に参照されていないすべてのインターフェイスのデフォルトを指定します。

グループ ポリシーの **address-pools** コマンドによるアドレス プールの設定で、トンネル グループの **address-pool** コマンドによるローカル プールの設定が上書きされます。

プールを指定する順序は重要です。セキュリティ アプライアンスは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスを割り当てます。

例

config-general コンフィギュレーション モードに入る次の例では、IPSec リモートアクセス トンネル グループ xyz のリモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定しています。

```
hostname(config)# tunnel-group xyz
hostname(config)# tunnel-group xyz general
hostname(config-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-general)#
```

関連コマンド

コマンド	説明
ip local pool	VPN リモートアクセス トンネルに使用する IP アドレス プールを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネル グループに関連付けます。

address-pools（グループ ポリシー）

リモート クライアントにアドレスを割り当てるためのアドレス プールのリストを指定するには、グループ ポリシーのアトリビュート コンフィギュレーション モードで **address-pools** コマンドを使用します。グループ ポリシーからアトリビュートを削除し、別のグループ ポリシーからの継承をイネーブルにするには、このコマンドの ***no*** 形式を使用します。

address-pools value *address_pool1* [*...address_pool6*]

no address-pools value *address_pool1* [*...address_pool6*]

address-pools none

no address-pools none

シンタックスの説明

address_pool	**ip local pool** コマンドで設定したアドレス プールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。
none	アドレス プールが何も設定されていないことを示し、他のグループ ポリシーからの継承をディセーブルにします。
value	アドレスの割り当てに使用するアドレス プールを 6 個まで指定します。

デフォルト

デフォルトでは、アドレス プールのアトリビュートを継承できるようになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドのアドレス プールの設定で、グループ内のローカル プールの設定が上書きされます。ローカル アドレスの割り当てに使用するローカル アドレス プールを 6 個まで指定できます。

プールを指定する順序は重要です。セキュリティ アプライアンスは、このコマンドでプールを指定した順序に従って、それらのプールからアドレスを割り当てます。

address-pools none コマンドは、このアトリビュートが他のポリシー（DefaultGrpPolicy など）から継承されることをディセーブルにします。**no address pools none** コマンドは、コンフィギュレーションから **address-pools none** コマンドを削除し、デフォルトの値（継承可能）に戻します。

例

次のコマンドは、config-general コンフィギュレーション モードで入力しています。この例では、GroupPolicy1 で、リモート クライアントにアドレスを割り当てるために pool 1 と pool20 を使用するように設定しています。

```
hostname(config)# ip local pool pool 192.168.10.1-192.168.10.100 mask 255.255.0.0
hostname(config)# ip local pool pool20 192.168.20.1-192.168.20.200 mask 255.255.0.0
hostname(config)# group-policy GroupPolicy1 attributes
hostname(config-group-policy)# address-pools value pool1 pool20
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
ip local pool	VPN のグループ ポリシーで使用する IP アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループ ポリシーを消去します。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

alias

アドレスを手動で変換し、DNS の応答を変更するには、グローバル コンフィギュレーション モードで **alias** コマンドを使用します。**alias** コマンドを削除するには、このコマンドの **no** 形式を使用します。このコマンドの代わりに、外部 NAT コマンド（**nat** コマンドと **static** コマンドを **dns** キーワードと一緒に使用）を使えるようになっています。**alias** コマンドではなく、外部 NAT コマンドを使用することをお勧めします。

alias *interface_name mapped_ip real_ip* [*netmask*]

[no] alias *interface_name mapped_ip real_ip* [*netmask*]

シンタックスの説明

interface_name	マップされた IP アドレスに向かうトラフィックの入力インターフェイス（またはマップされた IP アドレスからのトラフィックの出力インターフェイス）の名前を指定します。
mapped_ip	実際の IP アドレスの変換先の IP アドレスを指定します。
real_ip	実際の IP アドレスを指定します。
netmask	（オプション）両方の IP アドレスのサブネット マスクを指定します。ホストのマスクには、**255.255.255.255** と入力します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドで、宛先アドレスを変換することもできます。たとえば、ホストがパケットを 209.165.201.1 に送信する場合は、**alias** コマンドを使用することで、トラフィックを他のアドレス（209.165.201.30 など）にリダイレクトできます。

（注） ***alias*** コマンドを他のアドレスへの変換ではなく DNS の書き換えに使用する場合は、エイリアスがイネーブルなインターフェイス上で ***proxy-arp*** をディセーブルにします。***sysopt noproxyarp*** コマンドを使用して、セキュリティ アプライアンスが一般的な NAT 処理のために ***proxy-arp*** でトラフィックを自分自身にプルしないようにしてください。

alias コマンドを変更または削除した後は、**clear xlate** コマンドを使用します。

DNS ゾーン ファイルの中に、**alias** コマンドに含まれている「dnat」アドレスの A（アドレス）レコードが存在している必要があります。

alias コマンドには、2 つの使用方法があります。次に、その概要を示します。

- セキュリティ アプライアンスが *mapped_ip* 宛てのパケットを取得した場合、そのパケットを *real_ip* に送信するように **alias** コマンドを設定できる。
- セキュリティ アプライアンスが *real_ip* 宛てに DNS パケットを送信し、そのパケットがセキュリティ アプライアンスに戻ってきた場合、DNS パケットに変更を加えて、宛先ネットワーク アドレスを *mapped_ip* にするように **alias** コマンドを設定できる。

alias コマンドは、ネットワーク上の DNS サーバと自動的に対話して、エイリアスが設定された IP アドレスへのドメイン名によるアクセスを透過的に処理します。

real_ip IP アドレスと *mapped_ip* IP アドレスにネットワーク アドレスを使用すると、ネット エイリアスを指定できます。たとえば、**alias 192.168.201.0 209.165.201.0 255.255.255.224** コマンドを実行すると、209.165.201.1 ～ 209.165.201.30 の各 IP アドレスのエイリアスが作成されます。

static コマンドと **access-list** コマンドで **alias** コマンドの *mapped_ip* アドレスにアクセスするには、**access-list** コマンド内で、許可されるトラフィック送信元アドレスとして *mapped_ip* アドレスを指定します。次に例を示します。

```
hostname(config)# alias (inside) 192.168.201.1 209.165.201.1 255.255.255.255
hostname(config)# static (inside,outside) 209.165.201.1 192.168.201.1 netmask
255.255.255.255
hostname(config)# access-list acl_out permit tcp host 192.168.201.1 host 209.165.201.1
eq ftp-data
hostname(config)# access-group acl_out in interface outside
```

内部アドレス 192.168.201.1 を宛先アドレス 209.165.201.1 にマッピングして、エイリアスを指定しています。

内部ネットワーク クライアント 209.165.201.2 が example.com に接続すると、内部クライアントのクエリーに対する外部 DNS サーバからの DNS 応答は、セキュリティ アプライアンスによって 192.168.201.29 へと変更されます。セキュリティ アプライアンスで 209.165.200.225 ～ 209.165.200.254 をグローバル プール IP アドレスとして使用している場合、パケットはセキュリティ アプライアンスに SRC=209.165.201.2 および DST=192.168.201.29 として送信されます。セキュリティ アプライアンスは、アドレスを外部の SRC=209.165.200.254 および DST=209.165.201.29 に変換します。

例

次の例では、内部ネットワークに IP アドレス 209.165.201.29 が含まれています。このアドレスはインターネット上にあり、example.com に属しています。内部のクライアントが example.com にアクセスしても、パケットはセキュリティ　アプライアンスに到達しません。クライアントは、209.165.201.29 がローカルの内部ネットワーク上にあると判断するためです。

この動作を修正するには、**alias** コマンドを次のように使用します。

```
hostname(config)# alias (inside) 192.168.201.0 209.165.201.0 255.255.255.224

hostname(config)# show running-config alias
alias 192.168.201.0 209.165.201.0 255.255.255.224
```

次の例では、内部の 10.1.1.11 にある Web サーバ、および 209.165.201.11 で作成された **static** コマンドを示しています。送信元ホストは、外部のアドレス 209.165.201.7 にあります。外部の DNS サーバには、次に示すとおり、www.example.com のレコードが登録されています。

```
dns-server# www.example.com. IN A 209.165.201.11
```

ドメイン名 www.example.com. の末尾のピリオドは必要です。

次に、**alias** コマンドを使用する例を示します。

```
hostname(config)# alias 10.1.1.11 209.165.201.11 255.255.255.255
```

セキュリティ アプライアンスは、内部クライアント用のネーム サーバ応答を 10.1.1.11 に変更して、Web サーバに直接接続できるようにします。

アクセスを可能にするには、次のコマンドも必要です。

```
hostname(config)# static (inside,outside) 209.165.201.11 10.1.1.11

hostname(config)# access-list acl_grp permit tcp host 209.165.201.7 host
209.165.201.11 eq telnet
hostname(config)# access-list acl_grp permit tcp host 209.165.201.11 eq telnet host
209.165.201.7
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストを作成します。
clear configure alias	すべての **alias** コマンドをコンフィギュレーションから削除します。
show running-config alias	コンフィギュレーション内の、デュアル NAT コマンドで使用する重複アドレスを表示します。
static	ローカル IP アドレスをグローバル IP アドレスに、またはローカル ポートをグローバル ポートにマッピングすることによって、1 対 1 のアドレス変換規則を設定します。

allocate-interface

セキュリティ コンテキストにインターフェイスを割り当てるには、コンテキスト コンフィギュレーション モードで **allocate-interface** コマンドを使用します。コンテキストからインターフェイスを削除するには、このコマンドの **no** 形式を使用します。

allocate-interface *physical_interface* [*map_name*] [***visible*** | ***invisible***]

no allocate-interface *physical_interface*

allocate-interface *physical_interface.subinterface*[*-physical_interface.subinterface*] [*map_name*[*-map_name*]] [***visible*** | ***invisible***]

no allocate-interface *physical_interface.subinterface*[*-physical_interface.subinterface*]

シンタックスの説明

invisible	（デフォルト）コンテキスト ユーザが **show interface** コマンドで、マッピング名（設定されている場合）だけを表示できるようにします。

map_name	（オプション）マッピング名を設定します。
	
	map_name は、インターフェイス ID ではなく、インターフェイスを示す英数字のエイリアスで、コンテキスト内で使用できます。マッピング名を指定しない場合は、コンテキスト内でインターフェイス ID が使用されます。セキュリティを確保するため、コンテキストによって使用されているインターフェイスをコンテキスト管理者に知らせたくない場合があります。
	
	マッピング名はアルファベットで始まり、アルファベットまたは数字で終わる必要があります。その間の文字には、アルファベット、数字、または下線だけを使用できます。たとえば、次のような名前を使用できます。
	
	`int0`
	
	`inta`
	
	`int_0`
	
	サブインターフェイスの場合は、マッピング名の範囲を指定できます。
	
	範囲の詳細については、「使用上のガイドライン」を参照してください。

physical_interface	インターフェイス ID（***gigabit*ethernet0/1** など）を設定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	サブインターフェイス番号を設定します。サブインターフェイスの範囲を指定できます。
visible	（オプション）マッピング名を設定した場合でも、コンテキスト ユーザが **show interface** コマンドで、物理インターフェイスのプロパティを表示できるようにします。

デフォルト

デフォルトでは、マッピング名を設定した場合に **show interface** コマンドの出力にインターフェイス ID は表示されません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドを複数回入力して、異なる範囲を指定できます。マッピング名または表示の設定を変更するには、所定のインターフェイス ID でこのコマンドを再入力し、新しい値を設定します。**no allocate-interface** コマンドを入力して、最初からやり直す必要はありません。**allocate-interface** コマンドを削除すると、セキュリティ アプライアンスによって、コンテキスト内のインターフェイス関連のコンフィギュレーションがすべて削除されます。

透過ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 適応型セキュリティ アプライアンスでは、専用の管理インターフェイス Management 0/0（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。

（注）　透過モードの管理インターフェイスは、MAC アドレス テーブルにないパケットをそのインターフェイスを通してフラッドしません。

ルーテッド モードでは、必要に応じて、同じインターフェイスを複数のコンテキストに割り当てることができます。透過モードでは、インターフェイスを共有できません。

サブインターフェイスの範囲を指定する場合は、マッピング名の一致範囲を指定できます。範囲については、次のガイドラインに従ってください。

- マッピング名は、アルファベット部分と、それに続く数値部分で構成される必要がある。範囲の両端で、マッピング名のアルファベット部分が一致する必要があります。たとえば、次のような範囲を入力します。

  ```
  int0-int10
  ```

  たとえば、**gigabitethernet0/1.1-gigabitethernet0/1.5 happy1-sad5** と入力すると、コマンドが失敗します。

- マッピング名の数値部分には、サブインターフェイス範囲と同じ個数の数値が含まれる必要がある。たとえば、次の例では、両方の範囲に 100 個のインターフェイスが含まれています。

  ```
  gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int100
  ```

  たとえば、**gigabitethernet0/0.100-gigabitethernet0/0.199 int1-int15** と入力すると、コマンドが失敗します。

例

次の例は、gigabitethernet0/1.100、gigabitethernet0/1.200、および gigabitethernet0/2.300 ～ gigabitethernet0/1.305 をコンテキストに割り当てる方法を示しています。マッピング名は、int1 ～ int8 です。

```
hostname(config-ctx)# allocate-interface gigabitethernet0/1.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/2.300-gigabitethernet0/2.305
int3-int8
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

apcf

Application Profile Customization Framework プロファイルをイネーブルにするには、webvpn モードで **apcf** コマンドを使用します。特定の APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を使用します。すべての APCF スクリプトをディセーブルにするには、このコマンドの **no** 形式を引数なしで使用します。

apcf URL/filename.ext

no apcf [URL/filename.ext]

シンタックスの説明

URL	セキュリティ アプライアンス上にロードして使用する APCF プロファイルの場所を指定します。http://、https://、tftp://、ftp://、flash:/、disk#:/' のいずれかの URL を使用します。 URL には、サーバ、ポート、およびパスが含まれる場合があります。ファイル名だけを指定した場合、デフォルト URL は flash:/ です。**copy** コマンドを使用して、APCF プロファイルをフラッシュ メモリにコピーできます。
filename.extension	APCF カスタマイゼーション スクリプトの名前を指定します。これらのスクリプトは必ず XML 形式です。拡張子は、.xml、.txt、.doc などです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

Application Profile Customization Framework オプションでは、非標準の Web アプリケーションや Web リソースが WebVPN 接続で適切にレンダリングされるように、セキュリティ アプライアンスによってそれらの処理を可能にします。APCF プロファイルには、特定のアプリケーションに関して、いつ（事前、事後）、どこの（ヘッダー、本文、要求、応答）、どのデータを変換するかを指定するスクリプトがあります。

複数の APCF プロファイルをセキュリティ アプライアンス上で使用できます。そのようにした場合、セキュリティ アプライアンスは、それらを古いものから新しいものの順に 1 つずつ適用します。

apcf コマンドは、Cisco TAC のサポートがある場合に限り使用することをお勧めします。

例

次の例は、フラッシュ メモリの /apcf にある apcf1 という名前の APCF をイネーブルにする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf flash:/apcf/apcf1.xml
hostname(config-webvpn)#
```

次の例は、myserver という https サーバのポート 1440（パスは /apcf）にある apcf2.xml という名前の APCF をイネーブルにする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# apcf https://myserver:1440/apcf/apcf2.xml
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
proxy-bypass	特定のアプリケーションの最小限のコンテンツ リライトを設定します。
rewrite	トラフィックがセキュリティ アプライアンスを通過するかどうかを決定します。
show running config webvpn apcf	APCF コンフィギュレーションを表示します。

application-access

認証済みの WebVPN ユーザに表示される WebVPN ホームページの Application Access ボックス、およびそれらのユーザがアプリケーションを選択したときに開く Application Access ウィンドウをカスタマイズするには、webvpn カスタマイゼーション モードで **application-access** コマンドを使用します。

application-access {**title** | **message** | **window**} {**text** | **style**} *value*

[**no**] **application-access** {**title** | **message** | **window**} {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

title	Application Access ボックスのタイトルを変更することを指定します。
message	Application Access ボックスのタイトルの下に表示されるメッセージを変更することを指定します。
window	Application Access ウィンドウを変更することを指定します。
text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

Application Access ボックスのデフォルトのタイトル テキストは「Application Access」です。

Application Access ボックスのデフォルトのタイトル スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

Application Access ボックスのデフォルトのメッセージ テキストは「Start Application Client」です。

Application Access ボックスのデフォルトのメッセージ スタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller

Application Access ウィンドウのデフォルトのウィンドウ テキストは次のとおりです。

「Close this window when you finish using Application Access.Please wait for the table to be displayed before starting applications.」

Application Access ウィンドウのデフォルトのウィンドウ スタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、Application Access ボックスの背景色を RGB 16 進値 66FFFF（緑色の一種）にカスタマイズしています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# application-access title style background-color:#66FFFF
```

関連コマンド

コマンド	説明
application-access hide-details	Application Access ウィンドウでのアプリケーション詳細の表示をイネーブルまたはディセーブルにします。
browse-networks	WebVPN ホームページの Browse Networks ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの File Bookmarks タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの Web Application ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの Web Bookmarks タイトルまたはリンクをカスタマイズします。

application-access hide-details

WebVPN Applications Access ウィンドウに表示されるアプリケーション詳細を非表示にするには、WebVPN カスタマイゼーション モードで **application-access hide-details** コマンドを使用します。

application-access hide-details {**enable | disable**}

[**no**] **application-access hide-details** {**enable | disable**}

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

enable	Application Access ウィンドウのアプリケーション詳細を非表示にします。
disable	Application Access ウィンドウのアプリケーション詳細を非表示にしません。

デフォルト

デフォルトはディセーブルです。アプリケーション詳細は Application Access ウィンドウに表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次の例では、アプリケーション詳細の表示をディセーブルにしています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# application-access hide-details disable
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの Application Access ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの Browse Networks ボックスをカスタマイズします。
web-applications	WebVPN ホームページの Web Application ボックスをカスタマイズします。

area

OSPF エリアを作成するには、ルータ コンフィギュレーション モードで **area** コマンドを使用します。エリアを削除するには、このコマンドの **no** 形式を使用します。

area *area_id*

no area *area_id*

シンタックスの説明

area_id	作成するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

作成するエリアには、パラメータが設定されていません。関連する area コマンドを使用して、エリア パラメータを設定します。

例

次の例は、エリア ID 1 の OSPF エリアを作成する方法を示しています。

```
hostname(config-router)# area 1
hostname(config-router)#
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
area nssa	エリアを準スタブ エリアとして定義します。
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area authentication

OSPF エリアの認証をイネーブルにするには、ルータ コンフィギュレーション モードで **area authentication** コマンドを使用します。エリア認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

area *area_id* **authentication** [***message-digest***]

no area *area_id* **authentication** [***message-digest***]

シンタックスの説明

area_id	認証をイネーブルにするエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
message-digest	（オプション）*area_id* によって指定されたエリアでの Message Digest 5（MD5）認証をイネーブルにします。

デフォルト

エリア認証はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

指定した OSPF エリアが存在しない場合は、このコマンドの入力時にそのエリアが作成されます。***message-digest*** キーワードを付けずに **area authentication** コマンドを入力すると、簡易パスワード認証がイネーブルになります。***message-digest*** キーワードを付けると、MD5 認証がイネーブルになります。

例

次の例は、エリア 1 の MD5 認証をイネーブルにする方法を示しています。

```
hostname(config-router)# area 1 authentication message-digest
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area default-cost

スタブまたは NSSA に送信されるデフォルト サマリー ルートのコストを指定するには、ルータ コンフィギュレーション モードで **area default-cost** コマンドを使用します。デフォルトのコスト値に戻すには、このコマンドの **no** 形式を使用します。

area *area_id* ***default-cost*** *cost*

no area *area_id* ***default-cost***

シンタックスの説明

area_id	デフォルト コストを変更するスタブまたは NSSA の ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
cost	スタブまたは NSSA に使用されるデフォルト サマリー ルートのコストを指定します。有効な値は 0 ～ 65535 です。

デフォルト

cost のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

例

次の例は、スタブまたは NSSA に送信されるサマリー ルートのデフォルト コストを指定する方法を示しています。

```
hostname(config-router)# area 1 default-cost 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
area nssa	エリアを準スタブ エリアとして定義します。
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area filter-list prefix

ABR の OSPF エリア間のタイプ 3 LSA でアドバタイズされたプレフィックスをフィルタリングするには、ルータ コンフィギュレーション モードで **area filter-list prefix** コマンドを使用します。フィルタを変更またはキャンセルするには、このコマンドの **no** 形式を使用します。

area *area_id* **filter-list** ***prefix*** *list_name* {***in*** | ***out***}

no area *area_id* ***filter-list prefix*** *list_name* {***in*** | ***out***}

シンタックスの説明

area_id	フィルタリングを設定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
in	指定エリアに着信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。
list_name	プレフィックス リストの名前を指定します。
out	指定エリアから発信するアドバタイズされたプレフィックスに、設定済みプレフィックス リストを適用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

タイプ 3 LSA だけをフィルタリングできます。プライベート ネットワークに ASBR が設定されている場合は、ASBR がタイプ 5 LSA（プライベート ネットワークを記述）を送信します。この LSA は、パブリック エリアを含む AS 全体にフラッドされます。

例

次の例では、他のすべてのエリアからエリア 1 に送信されるプレフィックスをフィルタリングします。

```
hostname(config-router)# area 1 filter-list prefix-list AREA_1 in
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area nssa

エリアを NSSA として設定するには、ルータ コンフィギュレーション モードで **area nssa** コマンドを使用します。エリアから NSSA 指定を削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **nssa** [***no-redistribution***] [***default-information-originate*** [***metric-type*** {***1*** | ***2***}] [***metric*** *value*]] [***no-summary***]

no area *area_id* **nssa** [***no-redistribution***] [***default-information-originate*** [***metric-type*** {***1*** | ***2***}] [***metric*** *value*]] [***no-summary***]

シンタックスの説明

area_id	NSSA として指定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
default-information-originate	NSSA エリアでのタイプ 7 デフォルトの生成に使用します。このキーワードは、NSSA ABR 上または NSSA ASBR 上に限り有効です。
metric *metric_value*	（オプション）OSPF デフォルト メトリック値を指定します。有効な値は 0 ～ 16777214 です。
metric-type {***1*** | ***2***}	（オプション）デフォルト ルートの OSPF メトリック タイプ。有効な値は次のとおりです。 • ***1***：タイプ 1 • ***2***：タイプ 2 デフォルト値は 2 です。
no-redistribution	（オプション）ルータが NSSA ABR である場合に、**redistribute** コマンドで通常エリアだけにルートをインポートし、NSSA エリアにはインポートしないときに使用します。
no-summary	（オプション）エリアを、サマリー ルートが投入されない準スタブ エリアにします。

デフォルト

デフォルトは次のとおりです。

- NSSA エリアは定義されていません。
- ***metric-type*** は 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

あるオプションをエリアに設定した後、別のオプションを指定すると、両方のオプションが設定されます。たとえば、次の 2 つのコマンドを別々に入力すると、コンフィギュレーション内では、両方のオプションが設定された 1 つのコマンドになります。

```
area 1 nssa no-redistribution
area area_id nssa default-information-originate
```

例

次の例は、2 つのオプションを別々に設定すると、コンフィギュレーション内でどのように 1 つのコマンドになるかを示しています。

```
hostname(config-router)# area 1 nssa no-redistribution
hostname(config-router)# area 1 nssa default-information-originate
hostname(config-router)# exit
hostname(config-router)# show running-config router ospf 1
router ospf 1
 area 1 nssa no-redistribution default-information-originate
```

関連コマンド

コマンド	説明
area stub	エリアをスタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area range

エリアの境界でルートを統合および集約するには、ルータ コンフィギュレーション モードで **area range** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

area *area_id* **range** *address mask* [***advertise*** | ***not-advertise***]

no area *area_id* **range** *address mask* [***advertise*** | ***not-advertise***]

シンタックスの説明

address	サブネット範囲の IP アドレス。
advertise	（オプション）アドレス範囲ステータスを advertise に設定し、タイプ 3 要約リンクステート アドバタイズメント（LSA）を生成します。
area_id	範囲を設定するエリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
mask	IP アドレスのサブネット マスク。
not-advertise	（オプション）アドレス範囲ステータスを DoNotAdvertise に設定します。タイプ 3 要約 LSA の表示が抑止され、コンポーネント ネットワークは他のネットワークからは見えないままになります。

デフォルト

アドレス範囲ステータスは advertise に設定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

指定したエリアが以前に **area** コマンドで定義されていなかった場合は、このコマンドによって、指定したパラメータでそのエリアが作成されます。

area range コマンドは、ABR だけで使用されます。このコマンドによって、エリアのルートが統合または集約されます。その結果、1 つのサマリー ルートが ABR によって他のエリアにアドバタイズされます。エリアの境界でルーティング情報が凝縮されます。エリアの外部では、アドレス範囲ごとに 1 つのルートがアドバタイズされます。この動作は、「経路集約」と呼ばれます。1 つのエリアに複数の **area range** コマンドを設定できます。この設定により、OSPF は、多くの異なるアドレス範囲セットのアドレスを集約できます。

no area *area_id* **range** *ip_address netmask* ***not-advertise*** コマンドは、***not-advertise*** オプション キーワードだけを削除します。

例

次の例は、ネットワーク 10.0.0.0 上のすべてのサブネット対する 1 つのサマリー ルート、およびネットワーク 192.168.110.0 上のすべてのホストに対する 1 つのサマリー ルートが、ABR によって他のエリアにアドバタイズされるよう指定しています。

```
hostname(config-router)# area 10.0.0.0 range 10.0.0.0 255.0.0.0
hostname(config-router)# area 0 range 192.168.110.0 255.255.255.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area stub

エリアをスタブ エリアとして定義するには、ルータ コンフィギュレーション モードで **area stub** コマンドを使用します。スタブ エリア機能を削除するには、このコマンドの **no** 形式を使用します。

area *area_id* [***no-summary***]

no area *area_id* [***no-summary***]

シンタックスの説明

area_id	スタブ エリアの ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
no-summary	ABR がサマリー リンク アドバタイズメントをスタブ エリアに送信しないようにします。

デフォルト

デフォルトの動作は次のとおりです。

- スタブ エリアが定義されていません。
- サマリー リンク アドバタイズメントがスタブ エリアに送信されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、スタブまたは NSSA に接続されている ABR だけで使用できます。

area stub と **area default-cost** という 2 つのスタブ エリア ルータ コンフィギュレーション コマンドがあります。スタブ エリアに接続されているすべてのルータおよびアクセス サーバで、**area stub** コマンドを使用して、エリアをスタブ エリアとして設定する必要があります。スタブ エリアに接続されている ABR だけで **area default-cost** コマンドを使用します。**area default-cost** コマンドは、ABR によって生成されるサマリー デフォルト ルートのメトリックをスタブ エリアに提供します。

例

次の例では、指定したエリアをスタブ エリアとして設定しています。

```
hostname(config-router)# area 1 stub
hostname(config-router)#
```

関連コマンド

コマンド	説明
area default-cost	スタブまたは NSSA に送信されるデフォルト サマリー ルートのコストを指定します。
area nssa	エリアを準スタブ エリアとして定義します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

area virtual-link

OSPF 仮想リンクを定義するには、ルータ コンフィギュレーション モードで **area virtual-link** コマンドを使用します。オプションをリセットする、または仮想リンクを削除するには、このコマンドの **no** 形式を使用します。

area *area_id* **virtual-link** *router_id* [***authentication*** [***message-digest*** | ***null***]] [***hello-interval*** *seconds*] [***retransmit-interval*** seconds] [***transmit-delay*** *seconds*] [***dead-interval*** *seconds* [[***authentication-key*** *key*] | [***message-digest-key*** *key_id* ***md5*** *key*]]

no area *area_id* **virtual-link** *router_id* [***authentication*** [***message-digest*** | ***null***]] [***hello-interval*** *seconds*] [***retransmit-interval*** seconds] [***transmit-delay*** *seconds*] [***dead-interval*** *seconds* [[***authentication-key*** *key*] | [***message-digest-key*** *key_id* ***md5*** *key*]]

シンタックスの説明

area_id	仮想リンクの中継エリアのエリア ID。10 進数または IP アドレスを使用して ID を指定できます。有効な 10 進値は 0 ～ 4294967295 です。
authentication	（オプション）認証タイプを指定します。
authentication-key *key*	（オプション）隣接ルーティング デバイスで使用するための OSPF 認証パスワードを指定します。
dead-interval *seconds*	（オプション）hello パケットを 1 つも受信しない場合に、隣接ルーティング デバイスがダウンしたことを宣言する前の間隔を設定します。有効な値は 1 ～ 65535 秒です。
hello-interval *seconds*	（オプション）インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。
md5 *key*	（オプション）最大 16 バイトの英数字によるキーを指定します。
message-digest	（オプション）メッセージ ダイジェスト認証を使用することを指定します。
message-digest-key *key_id*	（オプション）Message Digest 5（MD5）認証をイネーブルにし、認証キー ID 番号を指定します。有効な値は 1 ～ 255 です。
null	（オプション）認証を使用しないことを指定します。パスワードまたはメッセージ ダイジェスト認証は、OSPF エリアに設定されていれば上書きされます。
retransmit-interval *seconds*	（オプション）インターフェイスに属する隣接ルータの LSA 再送間隔を指定します。有効な値は 1 ～ 65535 秒です。
router_id	仮想リンク ネイバーに関連付けられているルータ ID。ルータ ID は各ルータによって内部でインターフェイス IP アドレスから生成されます。この値は、IP アドレスの形式で入力する必要があります。デフォルトはありません。
transmit-delay *seconds*	（オプション）OSPF によるトポロジ変更の受信と最短パス優先（SPF）計算の開始との間の遅延時間（0 ～ 65535 秒）を指定します。デフォルトは 5 秒です。

デフォルト

デフォルトは次のとおりです。

- *area_id*：エリア ID は事前に定義されていません。
- *router_id*：ルータ ID は事前に定義されていません。
- ***hello-interval*** *seconds*：10 秒。
- ***retransmit-interval*** *seconds*：5 秒。
- ***transmit-delay*** *seconds*：1 秒。
- ***dead-interval*** *seconds*：40 秒。
- ***authentication-key*** *key*：キーは事前に定義されていません。
- ***message-digest-key*** *key_id* ***md5*** *key*：キーは事前に定義されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

OSPF では、すべてのエリアがバックボーン エリアに接続されている必要があります。バックボーンへの接続が失われた場合、仮想リンクを確立することで接続を修復できます。

hello 間隔を小さくすればするほど、トポロジ変更の検出が速くなりますが、ルーティング トラフィックが増加します。

再送間隔の設定値はあまり小さくしないでください。小さくすると、不要な再送信が行われます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

送信遅延の値では、インターフェイスの送信遅延と伝搬遅延を考慮に入れる必要があります。

指定した認証キーは、***area*** *area_id* ***authentication*** コマンドでバックボーンに対して認証がイネーブルにされている場合にだけ使用されます。

簡易テキスト認証と MD5 認証という 2 つの認証方式は、相互排他的です。どちらかを指定するか、または両方とも指定しないでください。***authentication-key*** *key* または ***message-digest-key*** *key_id* ***md5*** *key* の後に指定したキーワードと引数はすべて無視されます。したがって、オプションの引数はすべて、上記のキーワードと引数の組み合せの前に指定します。

インターフェイスに認証タイプが指定されていない場合、インターフェイスはエリアに指定されている認証タイプを使用します。エリアに認証タイプが指定されていない場合、エリアのデフォルトは null 認証です。

（注） 仮想リンクを正しく設定するには、各仮想リンク ネイバーに、中継エリア ID および対応する仮想リンク隣接ルータ ID が含まれている必要があります。ルータ ID を表示するには、**show ospf** コマンドを使用します。

仮想リンクからオプションを削除するには、削除するオプションを付けて、このコマンドの **no** 形式を使用します。仮想リンクを削除するには、**no area** *area_id* ***virtual-link*** コマンドを使用します。

例

次の例では、MD5 認証の仮想リンクを確立しています。

```
hostname(config-router)# area 10.0.0.0 virtual-link 10.3.4.5 message-digest-key 3 md5
sa5721bk47
```

関連コマンド

コマンド	説明
area authentication	OSPF エリアの認証をイネーブルにします。
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

arp

ARP テーブルにスタティック ARP エントリを追加するには、グローバル コンフィギュレーション モードで **arp** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。スタティック ARP エントリは MAC アドレスを IP アドレスにマッピングし、ホストに到達するまでに通過するインターフェイスを指定します。スタティック ARP エントリはタイムアウトしないため、ネットワーク問題の解決に役立つことがあります。透過ファイアウォール モードでは、ARP 検査でスタティック ARP テーブルが使用されます（**arp-inspection** コマンドを参照）。

arp *interface_name ip_address mac_address* [***alias***]

no arp *interface_name ip_address mac_address*

シンタックスの説明

alias	（オプション）このマッピングに対してプロキシ ARP をイネーブルにします。セキュリティ アプライアンスは、このコマンドで指定された IP アドレスに対する ARP 要求を受信すると、セキュリティ アプライアンスの MAC アドレスで応答します。その後、その IP アドレスを持つホスト宛てのトラフィックを受信すると、セキュリティ アプライアンスはこのコマンドで指定されたホスト MAC アドレスにそのトラフィックを転送します。このキーワードは、たとえば、ARP を実行しないデバイスがある場合に役立ちます。 透過ファイアウォール モードの場合、このキーワードは無視され、セキュリティ アプライアンスはプロキシ ARP を実行しません。
interface_name	ホスト ネットワークに接続されているインターフェイス。
ip_address	ホストの IP アドレス。
mac_address	ホストの MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ホストは IP アドレスによってパケットの宛先を指定しますが、イーサネット上での実際のパケット配信は、イーサネット MAC アドレスに依存しています。ルータまたはホストは、直接接続されているネットワーク上でパケットを配信する場合、IP アドレスに関連付けられている MAC アドレスを要求する ARP 要求を送信してから、その ARP 応答に従ってパケットを MAC アドレスに配信します。ホストまたはルータは ARP テーブルを保持しているため、配信する必要のあるパケットごとに ARP 要求を送信する必要がありません。ARP テーブルは、ネットワーク上で ARP 応答が送信されるたびに動的にアップデートされます。また、一定期間使用されなかったエントリは、タイムアウトになります。エントリが間違っている場合（たとえば、所定の IP アドレスの MAC アドレスが変更された場合）、アップデートされる前にそのエントリがタイムアウトになります。

（注） 透過ファイアウォール モードの場合、セキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）にはダイナミック ARP エントリが使用されます。

例

次の例では、外部インターフェイス上で、10.1.1.1 のスタティック ARP エントリを MAC アドレス 0009.7cbe.2100 で作成しています。

```
hostname(config)# arp outside 10.1.1.1 0009.7cbe.2100
```

関連コマンド

コマンド	説明
arp timeout	セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp timeout

セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定するには、グローバル コンフィギュレーション モードで **arp timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。ARP テーブルを再構築すると、自動的に、新しいホスト情報にアップデートされ、古いホスト情報が削除されます。ホスト情報が頻繁に変更されるため、タイムアウト値を小さくする必要がある場合もあります。

arp *timeout* *seconds*

no arp *timeout* *seconds*

シンタックスの説明

seconds	ARP テーブルを再構築する間隔の秒数（60 ～ 4294967）。

デフォルト

デフォルト値は 14,400 秒（4 時間）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、ARP タイムアウトを 5,000 秒に変更します。

```
hostname(config)# arp timeout 5000
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp timeout	ARP タイムアウトの現在のコンフィギュレーションを表示します。

arp-inspection

透過ファイアウォール モードで ARP 検査をイネーブルにするには、グローバル コンフィギュレーション モードで **arp-inspection** コマンドを使用します。ARP 検査をディセーブルにするには、このコマンドの **no** 形式を使用します。ARP 検査では、すべての ARP パケットがスタティック ARP エントリ（**arp** コマンドを参照）と比較され、一致しないパケットがブロックされます。この機能により、ARP スプーフィングを防止できます。

arp-inspection *interface_name* ***enable*** [***flood*** | ***no-flood***]

no arp-inspection *interface_name* ***enable***

シンタックスの説明

enable	ARP 検査をイネーブルにします。
flood	（デフォルト）スタティック ARP エントリのどの要素とも一致しないパケットが、発信元インターフェイスを除くすべてのインターフェイスにフラッドされるように指定します。MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、セキュリティ アプライアンスはパケットをドロップします。 **（注）** 管理専用のインターフェイス（存在する場合）では、このパラメータを flood に設定しても、パケットはフラッドされません。
interface_name	ARP 検査をイネーブルにするインターフェイス。
no-flood	（オプション）スタティック ARP エントリに正確に一致しないパケットがドロップされるように指定します。

デフォルト

デフォルトでは、すべてのインターフェイスで ARP 検査がディセーブルになっています。すべての ARP パケットがセキュリティ アプライアンスを通過できます。ARP 検査をイネーブルにすると、デフォルトでは、まったく一致しない ARP パケットがフラッドされます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ARP 検査をイネーブルにするには、事前に **arp** コマンドを使用してスタティック ARP エントリを設定しておく必要があります。

ARP 検査をイネーブルにすると、セキュリティ アプライアンスは、すべての ARP パケット内の MAC アドレス、IP アドレス、および送信元インターフェイスを ARP テーブル内のスタティック エントリと比較して、次のアクションを実行します。

- IP アドレス、MAC アドレス、および送信元インターフェイスが ARP エントリと一致した場合、パケットを通過させます。
- MAC アドレス、IP アドレス、またはインターフェイス間でミスマッチがある場合、セキュリティ アプライアンスはパケットをドロップします。
- ARP パケットのエントリがスタティック ARP テーブル内のどのエントリとも一致しなかった場合、パケットをすべてのインターフェイスに転送（フラッド）するように、またはドロップするように、セキュリティ アプライアンスを設定できます。

（注） 管理専用のインターフェイス（存在する場合）では、このパラメータを flood に設定しても、パケットはフラッドされません。

ARP 検査により、悪意のあるユーザが他のホストまたはルータになりすますこと（ARP スプーフィングと呼ばれる）を防止できます。ARP スプーフィングは、「man-in-the-middle」攻撃をイネーブルにすることができます。たとえば、ホストがゲートウェイ ルータに ARP 要求を送信すると、ゲートウェイ ルータはゲートウェイ ルータの MAC アドレスで応答します。ところが、攻撃者はホストに、ルータの MAC アドレスではなく、攻撃者の MAC アドレスを含む別の ARP 応答を送信します。これで、攻撃者は、ルータに転送する前に、ホストのトラフィックをすべて代行受信できるようになります。

ARP 検査により、正しい MAC アドレスと、それに関連付けられている IP アドレスがスタティック ARP テーブル内にある限り、攻撃者が攻撃者の MAC アドレスで ARP 応答を送信できないことが保証されます。

（注） 透過ファイアウォール モードの場合、セキュリティ アプライアンスとの間のトラフィック（管理トラフィックなど）にはダイナミック ARP エントリが使用されます。

例

次の例では、外部インターフェイス上で ARP 検査をイネーブルにし、スタティック ARP エントリに一致しないすべての ARP パケットをドロップするようセキュリティ アプライアンスを設定しています。

```
hostname(config)# arp outside 209.165.200.225 0009.7cbe.2100
hostname(config)# arp-inspection outside enable no-flood
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
clear configure arp-inspection	ARP 検査のコンフィギュレーションを消去します。
firewall transparent	ファイアウォール モードを透過に設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

asdm disconnect

アクティブな ASDM セッションを終了するには、特権 EXEC モードで **asdm disconnect** コマンドを使用します。

asdm disconnect *session*

シンタックスの説明

session	終了させるアクティブな ASDM セッションのセッション ID。すべてのアクティブな ASDM セッションのセッション ID を表示するには、**show asdm sessions** コマンドを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm disconnect** コマンドが **asdm disconnect** コマンドに変更されました。

使用上のガイドライン

アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm sessions** コマンドを使用します。特定のセッションを終了するには、**asdm disconnect** コマンドを使用します。

ASDM セッションを終了しても、残りのすべてのアクティブな ASDM セッションは、関連付けられている ID を保持します。たとえば、3 つのアクティブな ASDM セッションがあり、それぞれのセッション ID が 0、1、2 である場合、セッション 1 を終了しても、残りのアクティブな ASDM セッションはセッション ID 0 および 2 を保持します。この例では、次の新しい ASDM セッションにセッション ID 1 が割り当てられ、その後の新しいセッションには、セッション ID 3 から順番に ID が割り当てられます。

例

次の例では、セッション ID 0 の ASDM セッションを終了しています。**asdm disconnect** コマンドの入力前後に、**show asdm sessions** コマンドで、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm sessions	アクティブな ASDM セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm disconnect log_session

アクティブな ASDM ロギング セッションを終了するには、特権 EXEC モードで **asdm disconnect log_session** コマンドを使用します。

sdm disconnect log_session *session*

シンタックスの説明

session	終了させるアクティブな ASDM ロギング セッションのセッション ID。すべてのアクティブな ASDM セッションのセッション ID を表示するには、**show asdm log_sessions** コマンドを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示するには、**show asdm log_sessions** コマンドを使用します。特定のロギング セッションを終了するには、**asdm disconnect log_session** コマンドを使用します。

アクティブな各 ASDM セッションは、1 つまたは複数の ASDM ロギング セッションと関連付けられています。ASDM は、ロギング セッションを使用して、セキュリティ アプライアンスから syslog メッセージを取得します。ログ セッションを終了すると、アクティブな ASDM セッションに悪影響が及ぶことがあります。不要な ASDM セッションを終了するには、**asdm disconnect** コマンドを使用します。

（注） 各 ASDM セッションは、少なくとも 1 つの ASDM ロギング セッションを保持しているため、**show asdm sessions** と **show asdm log_sessions** の出力は同じ内容になることもあります。

ASDM ロギング セッションを終了しても、残りのすべてのアクティブな ASDM ロギング セッションは、関連付けられている ID を保持します。たとえば、3 つのアクティブな ASDM ロギング セッションがあり、それぞれのセッション ID が 0、1、2 である場合、セッション 1 を終了しても、残りのアクティブな ASDM ロギング セッションはセッション ID 0 および 2 を保持します。この例では、次の新しい ASDM ロギング セッションにセッション ID 1 が割り当てられ、その後の新しいロギング セッションには、セッション ID 3 から順番に ID が割り当てられます。

例

次の例では、セッション ID 0 の ASDM セッションを終了しています。**asdm disconnect log_sessions** コマンドの入力前後に、**show asdm log_sessions** コマンドで、アクティブな ASDM セッションを表示しています。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
hostname# asdm disconnect 0
hostname# show asdm log_sessions

1 192.168.1.2
```

関連コマンド

コマンド	説明
show asdm log_sessions	アクティブな ASDM ロギング セッションとそれに関連付けられているセッション ID のリストを表示します。

asdm group

注意　このコマンドを手動で設定しないでください。**asdm group** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部用に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

asdm group *real_grp_name real_if_name*

asdm group *ref_grp_name ref_if_name* ***reference*** *real_grp_name*

シンタックスの説明

real_grp_name	ASDM オブジェクト グループの名前。
real_if_name	指定のオブジェクト グループが関連付けられているインターフェイスの名前。
ref_grp_name	*real_grp_name* 引数で指定されたオブジェクト グループの変換された IP アドレスを含むオブジェクト グループの名前。
ref_if_name	着信トラフィックの宛先 IP アドレスが変換される元となるインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm group** コマンドが **asdm group** コマンドに変更されました。

使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

asdm history enable

ASDM 履歴トラッキングをイネーブルにするには、グローバル コンフィギュレーション モードで **asdm history enable** コマンドを使用します。ASDM 履歴トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

asdm history enable

no asdm history enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**pdm history enable** コマンドが **asdm history enable** コマンドに変更されました。

使用上のガイドライン

ASDM 履歴トラッキングをイネーブルにすることによって得られる情報は、ASDM 履歴バッファに格納されます。この情報を表示するには、**show asdm history** コマンドを使用します。この履歴情報は、ASDM によってデバイス モニタリングに使用されます。

例

次の例では、ASDM 履歴トラッキングをイネーブルにしています。

```
hostname(config)# asdm history enable
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

asdm image

フラッシュ メモリ内の ASDM ソフトウェア イメージの場所を指定するには、グローバル コンフィギュレーション モードで **asdm image** コマンドを使用します。イメージの場所の指定を削除するには、このコマンドの **no** 形式を使用します。

asdm image *url*

no asdm image [*url*]

シンタックスの説明

url　フラッシュ メモリ内の ASDM イメージの場所を設定します。次の URL シンタックスを参照してください。

- ***disk0:/*[*path/*]*filename***

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内蔵フラッシュ メモリを指します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。

- ***disk1:/*[*path/*]*filename***

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。

- ***flash:/*[*path/*]*filename***

  この URL は内蔵フラッシュ メモリを指します。

デフォルト

このコマンドをスタートアップ コンフィギュレーションに含めない場合、セキュリティ アプライアンスは最初に検出した ASDM イメージを起動時に使用します。内蔵フラッシュ メモリのルート ディレクトリ内を検索し、次に外部フラッシュ メモリを検索します。イメージを検出した場合、セキュリティ アプライアンスは **asdm image** コマンドを実行コンフィギュレーションに挿入します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フラッシュ メモリに複数の ASDM ソフトウェア イメージを格納できます。アクティブな ASDM セッションのある間に、**asdm image** コマンドを入力して新しい ASDM ソフトウェア イメージを指定しても、アクティブなセッションは中断しません。アクティブな ASDM セッションは、セッションを開始した ASDM ソフトウェア イメージを引き続き使用します。新しい ASDM セッションは、新しいソフトウェア イメージを使用します。**no asdm image** コマンドを入力すると、コンフィギュレーションからコマンドが削除されます。ただし、最後に設定したイメージの場所を使用して、セキュリティ アプライアンスから ASDM にアクセスできます。

このコマンドをスタートアップ コンフィギュレーションに含めない場合、セキュリティ アプライアンスは最初に検出した ASDM イメージを起動時に使用します。内蔵フラッシュ メモリのルート ディレクトリ内を検索し、次に外部フラッシュ メモリを検索します。イメージを検出した場合、セキュリティ アプライアンスは **asdm image** コマンドを実行コンフィギュレーションに挿入します。必ず **write memory** コマンドを使用して、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存してください。**asdm image** コマンドをスタートアップ コンフィギュレーションに保存しておかないと、再起動するたびにセキュリティ アプライアンスが ASDM イメージを探し、**asdm image** コマンドを実行コンフィギュレーションに挿入します。Auto Update を使用している場合は、起動時にこのコマンドが自動的に追加され、セキュリティ アプライアンスにあるコンフィギュレーションが Auto Update Server にあるコンフィギュレーションと一致しなくなります。そのため、セキュリティ アプライアンスは Auto Update Server からコンフィギュレーションをダウンロードします。この不必要な動作を防ぐには、**asdm image** コマンドをスタートアップ コンフィギュレーションに保存しておきます。

例

次の例では、ASDM イメージを asdm.bin に設定しています。

```
hostname(config)# asdm image flash:/asdm.bin
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm image	現在の ASDM イメージ ファイルを表示します。
boot	ソフトウェア イメージ ファイルとスタートアップ コンフィギュレーション ファイルを設定します。

asdm location

注意　このコマンドを手動で設定しないでください。**asdm location** コマンドは ASDM によって実行コンフィギュレーションに追加され、内部通信に使用されます。このコマンドは、情報提供のためだけにこのマニュアルに記載されています。

asdm location *ip_addr netmask if_name*

asdm location *ipv6_addr/prefix if_name*

シンタックスの説明

ip_addr	ネットワーク トポロジを定義するために ASDM によって内部で使用される IP アドレス。
netmask	*ip_addr* のサブネット マスク。
if_name	ASDM にアクセスするときに通過するインターフェイスの名前。
ipv6_addr/prefix	ネットワーク トポロジを定義するために ASDM によって内部で使用される IPv6 アドレスおよびプレフィックス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**pdm location** コマンドが **asdm location** コマンドに変更されました。

使用上のガイドライン

このコマンドを手動で設定または削除しないでください。

asr-group

非対称ルーティング インターフェイス グループ ID を指定するには、インターフェイス コンフィギュレーション モードで **asr-group** コマンドを使用します。この ID を削除するには、このコマンドの **no** 形式を使用します。

asr-group *group_id*

no asr-group *group_id*

シンタックスの説明

group_id	非対称ルーティング グループ ID。有効な値は 1 ～ 32 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	—	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

Active/Active フェールオーバーがイネーブルである場合、ロードバランシングのために、発信接続のリターン トラフィックがピア装置上のアクティブなコンテキストを介してルーティングされることがあります。このピア装置上で、発信接続のコンテキストはスタンバイ グループ内にあります。

asr-group コマンドでは、着信インターフェイスによるフローが見つからない場合、同じ asr グループのインターフェイスで着信パケットが再分類されます。再分類により、別のインターフェイスによるフローが見つかり、関連付けられているコンテキストがスタンバイ状態である場合、パケットは処理のためにアクティブ装置に転送されます。

このコマンドを有効にするには、ステートフル フェールオーバーがイネーブルである必要があります。

ASR 統計情報を表示するには、**show interface detail** コマンドを使用します。この統計情報には、インターフェイス上で送信、受信、およびドロップされた ASR パケットの数が含まれています。

例

次の例では、選択したインターフェイスを非対称ルーティング グループ 1 に割り当てています。

コンテキスト ctx1 のコンフィギュレーション

```
hostname/ctx1(config)# interface e2
hostname/ctx1(config-if)# nameif outside
hostname/ctx1(config-if)# ip address 192.168.1.11 255.255.255.0 standby 192.168.1.21
hostname/ctx1(config-if)# asr-group 1
```

コンテキスト ctx2 のコンフィギュレーション

```
hostname/ctx2(config)# interface e3
hostname/ctx2(config-if)# nameif outside
hostname/ctx2(config-if)# ip address 192.168.1.31 255.255.255.0 standby 192.168.1.41
hostname/ctx2(config-if)# asr-group 1
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイス統計情報を表示します。

auth-cookie-name

認証クッキーの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **auth-cookie-name** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

auth-cookie-name

シンタックスの説明

name	認証クッキーの名前。最大長は 128 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用してシングル サインオン認証要求を SSO サーバに送信します。認証が成功した場合、認証 Web サーバは、クライアント ブラウザに認証クッキーを返します。クライアント ブラウザは、その認証クッキーを提示することで、SSO ドメイン内の他の Web サーバに対して認証を行います。**auth-cookie-name** コマンドは、セキュリティ アプライアンスによって SSO で使用される認証クッキーの名前を設定します。

一般的な認証クッキーの形式は、Set-Cookie: < クッキー名 >=< クッキー値 > ［;< クッキー アトリビュート >］です。次の認証クッキーの例では、SMSESSION が **auth-cookie-name** コマンドで設定される名前です。

```
Set-Cookie:
SMSESSION=yN4Yp5hHVNDgs4FT8dn7+Rwev41hsE49XlKc+1twie0gqnjbhkTkUnR8XWP3hvDH6PZPbHIHtWLD
KTa8ngDB/lbYTjIxrbDx8WPWwaG3CxVa3adOxHFR8yjD55GevK3ZF4ujgU1lhO6fta0dSSOSepWvnsCb7IFxCw
+MGiw0o88uHa2t4l+SillqfJvcpuXfiIAO06D/dapWriHjNoi4llJOgCst33wEhxFxcWy2UWxs4EZSjsI5GyBn
efSQTPVfma5dc/emWor9vWr0HnTQaHP5rg5dTNqunkDEdMIHfbeP3F90cZejVzihM6igiS6P/CEJAjE;Domain
=.example.com;Path=/
```

AAA サーバ ホスト コンフィギュレーション モードで入力された次の例では、example.com という名前の Web サーバから受信した認証クッキーの認証クッキー名として SMSESSION を指定しています。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# auth-cookie-name SMSESSION
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名とパスワードを受信する Web サーバ URI を指定します。
hidden-parameter	認証 Web サーバとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求のパラメータの名前を指定します。
start-url	事前ログイン クッキーの取得先 URL を指定します。
user-parameter	SSO 認証で使用される HTTP POST 要求の一部としてユーザ名パラメータが送信される必要があることを指定します。

authentication

WebVPN または電子メール プロキシの認証方式を設定するには、**authentication** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、このコマンドは該当する電子メール プロキシ モードで使用します。デフォルトの AAA に戻すには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、ユーザを認証して、ユーザのアイデンティティを確認します。

authentication {**aaa** | **certificate** | **mailhost** | **piggyback**}

no authentication

シンタックスの説明

aaa	セキュリティ アプライアンスが設定済み AAA サーバに対してチェックするユーザ名とパスワードを提供します。
certificate	SSL ネゴシエーション中に証明書を提供します。
mailhost	リモート メール サーバを介した認証。mailhost を設定できるのは SMTPS だけです。IMAP4S および POP3S の場合、メールホスト認証は必須であり、設定可能なオプションとして表示されません。
piggyback	HTTPS WebVPN セッションがすでに存在する必要があります。ピギーバック認証は、電子メール プロキシだけで使用できます。

デフォルト

次の表は、WebVPN および電子メール プロキシのデフォルトの認証方式を示しています。

プロトコル	デフォルトの認証方式
WebVPN	AAA
IMAP4S	メールホスト（必須）
POP3S	メールホスト（必須）
SMTPS	AAA

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn モードでは廃止され、トンネル グループ webvpn アトリビュート モードに置き換えられました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn アトリビュート モードの同等のコマンドに変換されます。

WebVPN の場合、AAA 認証と証明書認証の両方を要求できます。その場合、ユーザは証明書およびユーザ名とパスワードを提供する必要があります。

電子メール プロキシ認証の場合、複数の認証方式を要求できます。

このコマンドを再び指定すると、現在のコンフィギュレーションが上書きされます。

例

次の例は、WebVPN ユーザに対して認証のために証明書の提供を要求する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication certificate
```

authentication（暗号 isakmp ポリシー コンフィギュレーション モード）

IKE ポリシー内の認証方式を指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **authentication** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

authentication {**crack** | **pre-share** | **rsa-sig**}

シンタックスの説明

crack	認証方式として、IKE Challenge/Response for Authenticated Cryptographic Keys（CRACK）を指定します。
pre-share	認証方式として、事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
rsa-sig	認証方式として、RSA シグニチャを指定します。 RSA シグニチャは、IKE ネゴシエーションに対する否認防止ができます。これは、基本的にユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。

デフォルト

デフォルトの ISAKMP ポリシー認証は、**pre-share** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 isakmp ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy authentication** コマンドは既存のものです。
7.2.(1)	**isakmp policy authentication** コマンドが、**authentication** コマンドに置き換えられました。

使用上のガイドライン

RSA シグニチャを指定する場合は、認証局（CA）から証明書を取得するようにセキュリティ アプライアンスとそのピアを設定する必要があります。事前共有キーを指定する場合は、セキュリティ アプライアンスとそのピアに、事前共有キーを別々に設定する必要があります。

例

次の例は、グローバル コンフィギュレーション モードで、**authentication** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーで RSA シグニチャの認証方式を使用するように設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

authentication（トンネル グループ webvpn コンフィギュレーション モード）

トンネル グループの認証方式を指定するには、トンネル グループ webvpn コンフィギュレーション モードで **authentication** コマンドを使用します。

authentication aaa [**certificate**]

authentication certificate [**aaa**]

シンタックスの説明

aaa	このトンネル グループの認証にユーザ名とパスワードを使用することを指定します。
certificate	認証にデジタル証明書を使用することを指定します。

デフォルト

デフォルトの認証方式は AAA です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードから、トンネル グループの webvpn アトリビュート コンフィギュレーション モードに移動しました。

使用上のガイドライン

認証方式は、少なくとも 1 つ必要です。AAA 認証、証明書認証、またはその両方を指定できます。これらは、どちらを先に指定してもかまいません。このコマンドを省略した場合、セキュリティ アプライアンスはデフォルトの認証方式である AAA を使用します。

WebVPN 証明書認証では、HTTPS ユーザ証明書を各インターフェイスに求める必要があります。つまり、この選択が機能するためには、証明書認証を指定する前に、**http authentication-certificate** コマンドでインターフェイスを指定しておく必要があります。

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn アトリビュート モードの同等のコマンドに変換されます。

例

次の例は、トンネル グループ webvpn コンフィギュレーション モードの **authentication** コマンドを示しています。トンネル グループ「test」のメンバーに対して、認証にユーザ名とパスワードを使用する必要があることを指定しています。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-webvpn)# authentication aaa
```

次の例は、**authentication** コマンドを示しています。トンネル グループ「docs」のメンバーに対して、認証にデジタル証明書を使用する必要があることを指定しています。

```
hostname(config)# tunnel-group docs type webvpn
hostname(config)# tunnel-group docs webvpn-attributes
hostname(config-webvpn)# authentication certificate
```

関連コマンド

コマンド	説明
clear configure tunnel-group	すべてのトンネル グループのコンフィギュレーションを削除します。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

authentication eap-proxy

L2TP over IPSec 接続で EAP をイネーブルにし、セキュリティ アプライアンスの PPP の認証プロセスを外部の RADIUS 認証サーバに代理させるには、トンネル グループの ppp アトリビュート コンフィギュレーション モードで **authentication eap-proxy** コマンドを使用します。

コマンドをデフォルト設定（CHAP および MS-CHAP を許可）に戻すには、このコマンドの ***no*** 形式を使用します。

authentication eap-proxy

no authentication eap-proxy

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトでは、EAP は認証プロトコルとして許可されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ PPP アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、L2TP/IPSec トンネル グループ タイプだけに適用できます。

例

次のコマンドは、config-ppp コンフィギュレーション モードで入力しています。この例では、ppremotegrp というトンネル グループの PPP 接続の EAP による認証を許可しています。

```
hostname(config)# tunnel-group ppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group ppremotegrp ppp-attributes
hostname(config-ppp)# authentication eap
hostname(config-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネル グループに関連付けます。

authentication ms-chap-v1

IPSec 接続を使用した L2TP において、PPP の Microsoft CHAP バージョン 1 認証をイネーブルにするには、トンネル グループ PPP アトリビュート コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。このプロトコルは CHAP と類似していますが、CHAP のようにサーバがクリアテキスト パスワードを格納および比較するのではなく、暗号化されたパスワードのみを格納および比較するため、セキュリティが高くなります。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

コマンドをデフォルト設定（CHAP および MS-CHAP を許可）に戻すには、このコマンドの ***no*** 形式を使用します。

Microsoft CHAP バージョン 1 をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication ms-chap-v1

no authentication ms-chap-v1

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ PPP アトリビュート	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、L2TP/IPSec トンネル グループ タイプだけに適用できます。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続に固有なレコードのデータベースを作成および管理します。

authentication ms-chap-v2

IPSec 接続を使用した L2TP において、PPP の Microsoft CHAP バージョン 2 認証をイネーブルにするには、トンネル グループ PPP アトリビュート コンフィギュレーション モードで **authentication ms-chap-v1** コマンドを使用します。このプロトコルは CHAP と類似していますが、CHAP のようにサーバがクリアテキスト パスワードを格納および比較するのではなく、暗号化されたパスワードのみを格納および比較するため、セキュリティが高くなります。また、このプロトコルはデータ暗号化のためのキーを MPPE によって生成します。

コマンドをデフォルト設定（CHAP および MS-CHAP を許可）に戻すには、このコマンドの ***no*** 形式を使用します。

Microsoft CHAP バージョン 2 をディセーブルにするには、このコマンドの **no** 形式を使用します。

authentication ms-chap-v1

no authentication ms-chap-v1

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ PPP アトリビュート	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、L2TP/IPSec トンネル グループ タイプだけに適用できます。

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続に固有なレコードのデータベースを作成および管理します。

authentication pap

L2TP over IPSec 接続で PPP の PAP による認証を許可するには、トンネル グループの ppp アトリビュート コンフィギュレーション モードで **authentication pap** コマンドを使用します。このプロトコルは、認証中にクリアテキストのユーザ名とパスワードを渡すので安全ではありません。

コマンドをデフォルト設定（CHAP および MS-CHAP を許可）に戻すには、このコマンドの ***no*** 形式を使用します。

authentication pap

no authentication pap

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトでは、PAP は認証プロトコルとして許可されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ PPP アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、L2TP/IPSec トンネル グループ タイプだけに適用できます。

例

次のコマンドは、config-ppp コンフィギュレーション モードで入力しています。この例では、ppremotegrps というトンネル グループの PPP 接続の PAP による認証を許可しています。

```
hostname(config)# tunnel-group ppremotegrp type IPSec/IPSec
hostname(config)# tunnel-group ppremotegrp ppp-attributes
hostname(config-ppp)# authentication pap
hostname(config-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group-map default-group	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネル グループに関連付けます。

authentication-port

特定のホストの RADIUS 認証に使用するポート番号を指定するには、AAA サーバ ホスト モードで **authentication-port** コマンドを使用します。認証ポートの指定を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、認証機能の割り当て先となる、リモート RADIUS サーバ ホストの宛先 TCP/UDP ポート番号を指定するものです。

authentication-port *port*

no authentication-port

シンタックスの説明

port	RADIUS 認証用のポート番号（1 ～ 65535）。

デフォルト

デフォルトでは、デバイスはポート 1645 で RADIUS をリッスンします（RFC 2058 に準拠）。ポートを指定しない場合は、RADIUS 認証のデフォルト ポート番号（1645）が使用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドのセマンティックが変更され、RADIUS サーバを含むサーバ グループでホストごとにサーバ ポートを指定できるようになりました。

使用上のガイドライン

RADIUS 認証サーバが 1645 以外のポートを使用する場合は、**aaa-server** コマンドで RADIUS サービスを開始する前に、セキュリティ アプライアンスに適切なポートを設定する必要があります。

このコマンドは、RADIUS に設定されているサーバ グループに限り有効です。

例

次の例では、ホスト「1.2.3.4」に対して「srvgrp1」という名前の RADIUS AAA サーバを設定し、タイムアウトを 9 秒に、リトライ間隔を 7 秒に、認証ポートを 1650 に設定しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定したサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、または ASDM ユーザ認証をイネーブルまたはディセーブルにします。
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入ります。このモードでは、ホストに固有の AAA サーバ パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

authentication-server-group

ユーザの認証で使用する AAA サーバ グループを指定するには、トンネル グループ一般アトリビュート モードで **authentication-server-group** コマンドを使用します。このアトリビュートをデフォルトに戻すには、このコマンドの ***no*** 形式を使用します。

authentication-server-group [(*interface_name*)] *server_group* [***LOCAL*** | ***NONE***]

no authentication-server-group [(*interface_name*)] *server_group*

シンタックスの説明

interface_name	（オプション）IPSec トンネルの終点となるインターフェイスを指定します。
LOCAL	（オプション）通信障害によってサーバ グループにあるすべてのサーバがアクティブでなくなった場合に、ローカル ユーザ データベースを使用して認証することを指定します。サーバ グループの名前が ***LOCAL*** か ***NONE*** の場合は、ここで ***LOCAL*** キーワードを使用しないでください。
NONE	（オプション）サーバ グループの名前を none に指定します。認証する必要がないことを示すには、***NONE*** キーワードをサーバ グループ名として使用します。
server_group	すでに設定済みの AAA サーバ グループの名前を指定します。

デフォルト

このコマンドのサーバ グループのデフォルト設定は、***LOCAL*** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート モードに移動しました。

使用上のガイドライン

認証サーバを設定するには、**aaa-server** コマンドを使用します。サーバ グループ名の最大長は 16 文字です。

このコマンドを入力する前に、AAA サーバ グループを設定しておく必要があります。

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。すべてのタイプのトンネル グループに、このアトリビュートを適用できるようになりました。

例

次のコマンドは、config-general コンフィギュレーション モードで入力しています。この例では、「remotegrp」という IPSec リモートアクセス トンネル グループ用に「aaa-server456」という認証サーバ グループを設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバのパラメータを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。

authentication-server-group（webvpn）

WebVPN またはいずれかの電子メール プロキシで使用する認証サーバ グループを指定するには、**authentication-server-group** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、このコマンドは該当する電子メール プロキシ モードで使用します。コンフィギュレーションから認証サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、ユーザを認証して、ユーザのアイデンティティを確認します。

authentication-server-group *group_tag*

no authentication-server-group

シンタックスの説明

group_tag	設定済みの認証サーバまたはサーバ グループを指定します。認証サーバを設定するには、**aaa-server** コマンドを使用します。グループ タグの最大長は 16 文字です。

デフォルト

デフォルトでは、認証サーバは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。
7.1(1)	このコマンドがトンネル グループ一般アトリビュート コンフィギュレーション モードに変更されました。

使用上のガイドライン

AAA 認証を設定する場合は、このアトリビュートも設定する必要があります。設定しないと、認証が必ず失敗します。

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

例

次の例は、「WEBVPNAUTH」という名前の認証サーバ グループを使用するように WebVPN サービスを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authentication-server-group WEBVPNAUTH
```

次の例は、「IMAP4SSVRS」という名前の認証サーバ グループを使用するように IMAP4S 電子メール プロキシを設定する方法を示しています。

```
hostname(config)# imap4s
hostname(config-imap4s)# authentication-server-group IMAP4SSVRS
```

関連コマンド

コマンド	説明
aaa-server host	認証、認可、アカウンティング サーバを設定します。

authorization-dn-attributes（トンネル グループ一般アトリビュート モード）

サブジェクト DN フィールドのどの部分を認可用のユーザ名として使用するかを指定するには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **authorization-dn-attributes** コマンドを使用します。これらのアトリビュートをデフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

authorization-dn-attributes {*primary-attr* [*secondary-attr*] | ***use-entire-name***}

no authorization-dn-attributes

シンタックスの説明

primary-attr	証明書から認可クエリー用の名前を生成するときに使用するアトリビュートを指定します。
secondary-attr	（オプション）プライマリ アトリビュートが存在しない場合に、証明書から認可クエリー用の名前を生成するときに使用する追加のアトリビュートを指定します。
use-entire-name	セキュリティ アプライアンスがサブジェクト DN（RFC1779）全体を使用して名前を生成するように指定します。

デフォルト

プライマリ アトリビュートのデフォルト値は CN（Common Name; 通常名）です。

セカンダリ アトリビュートのデフォルト値は OU（Organization Unit; 組織ユニット）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

プライマリ アトリビュートとセカンダリ アトリビュートには、次のようなものがあります。

アトリビュート	定義
CN	Common Name（通常名）：個人、システムなどの名前。
OU	Organizational Unit（組織ユニット）：組織（O）内のサブグループ。
O	Organization（組織）：会社、団体、機関、連合などの名前。
L	Locality（地名）：組織が置かれている市または町。
SP	State/Province（州または都道府県）：組織が置かれている州または都道府県。
C	Country（国または地域）：国または地域を示す 2 文字の短縮形。このコードは、ISO 3166 の国または地域の短縮形に準拠しています。
EA	E-mail address（電子メール アドレス）
T	Title（タイトル）
N	Name（名前）
GN	Given Name（名）
SN	Surname（姓）
I	Initials（イニシャル）
GENQ	Generational Qualifier（世代修飾子）
DNQ	Domain Name Qualifier（ドメイン名修飾子）
UID	User Identifier（ユーザ識別子）
UPN	User Principal Name（ユーザ プリンシパル名）
SER	Serial Number（シリアル番号）
use-entire-name	DN 名全体を使用

例

config-ipsec コンフィギュレーション モードに入る次の例では、「remotegrp」という名前のリモート アクセス トンネル グループ（ipsec_ra）を作成し、IPSec グループ アトリビュートを指定して、通常名が認可用のユーザ名として使用されるように定義しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-dn-attributes CN
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般アトリビュートを指定します。

authorization-dn-attributes（webvpn）

認可用のユーザ名として使用するプライマリ サブジェクト DN フィールドおよびセカンダリ サブジェクト DN フィールドを指定するには、**authorization-dn-attributes** コマンドを使用します。

WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、このコマンドは該当する電子メール プロキシ モードで使用します。このアトリビュートをコンフィギュレーションから削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

authorization-dn-attributes {*primary-attr***} [***secondary-attr***] | use-entire-name}**

no authorization-dn-attributes

シンタックスの説明

primary-attr	デジタル証明書から認可クエリー用の名前を生成するときに使用するアトリビュートを指定します。
secondary-attr	（オプション）デジタル証明書から認可クエリー用の名前を生成するときにプライマリ アトリビュートと共に使用する追加のアトリビュートを指定します。
use-entire-name	セキュリティ アプライアンスがサブジェクト DN 全体を使用して、デジタル証明書から認可クエリー用の名前を生成するように指定します。

デフォルト

プライマリ アトリビュートのデフォルト値は CN（Common Name; 通常名）です。

セカンダリ アトリビュートのデフォルト値は OU（Organization Unit; 組織ユニット）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。

使用上のガイドライン　次の表で、DN フィールドについて説明します。

DN フィールド	説明
C	Country（国または地域）
CN	Common Name（通常名）
DNQ	DN Qualifier（DN 修飾子）
EA	E-mail Address（電子メール アドレス）
GENQ	Generational Qualifier（世代修飾子）
GN	Given Name（名）
I	Initials（イニシャル）
L	Locality（地名）
N	Name（名前）
O	Organization（組織）
OU	Organizational Unit（組織ユニット）
SER	Serial Number（シリアル番号）
SN	Surname（姓）
SP	State/Province（州または都道府県）
T	Title（タイトル）
UID	User ID（ユーザ ID）
UPN	User Principal Name（ユーザ プリンシパル名）
use-entire-name	DN 名全体を使用

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

例　次の例は、WebVPN ユーザが電子メール アドレス（プライマリ アトリビュート）および組織ユニット（セカンダリ アトリビュート）に基づいて認可されるように指定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-dn-attributes EA OU
```

関連コマンド

コマンド	説明
authorization-required	ユーザが接続前に正常に認可されることを必須とします。

authorization-required（トンネル グループ一般アトリビュート モード）

ユーザが接続前に正常に認可されることを必須とするには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **authorization-required** コマンドを使用します。このアトリビュートをデフォルトに戻すには、このコマンドの ***no*** 形式を使用します。

authorization-required

no authorization-required

デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

シンタックスの説明

このコマンドには、引数もキーワードもありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

例

グローバル コンフィギュレーション モードに入る次の例では、「remotegrp」という名前のリモート アクセス トンネル グループを介して接続するユーザが、完全な DN に基づく認可を受けることを必須としています。最初のコマンドでは、「remotegrp」という名前のリモート グループのトンネル グループ タイプを ipsec_ra（IPSec リモートアクセス）と設定しています。2 番目のコマンドで、指定したトンネル グループのトンネル グループ一般アトリビュート コンフィギュレーション モードに入り、最後のコマンドで、指定したトンネル グループで認可が必要となるように指定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-required
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般アトリビュートを指定します。

authorization-required（webvpn）

WebVPN ユーザまたは電子メール プロキシ ユーザが接続前に正常に認可されることを必須とするには、**authorization-required** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、このコマンドは該当する電子メール プロキシ モードで使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

authorization-required

no authorization-required

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、authorization-required はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

例

次の例は、WebVPN ユーザが認可を受けることを必須とする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-required
```

関連コマンド

コマンド	説明
authorization-dn-attributes（webvpn）	認可用のユーザ名として使用するプライマリ サブジェクト DN フィールドおよびセカンダリ サブジェクト DN フィールドを指定します。

authorization-server-group（トンネル グループ一般アトリビュート モード）

ユーザ認可で使用する AAA サーバ グループ（およびオプションでインターフェイス）を指定するには、トンネル グループ一般アトリビュート モードで **authorization-server-group** コマンドを使用します。このコマンドをデフォルトに戻すには、このコマンドの ***no*** 形式を使用します。

authorization-server-group [(*interface-id*)] *server_group*

no authorization-server-group [(*interface-id*)]

シンタックスの説明

(*interface-id*)	（オプション）認可を実行するインターフェイスを指定します。このパラメータを指定する場合はカッコが必要です。
server_group	設定済みの認可サーバまたはサーバ グループの名前を指定します。

デフォルト

デフォルトでは、このコマンドの設定は ***no authorization-server-group*** になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。このコマンドは、すべてのトンネル グループ アトリビュート タイプに使用できるようになりました。
7.2(2)	インターフェイス単位で IPSec 接続の認可を行えるように機能が拡張されました。

使用上のガイドライン

VPN 認可が LOCAL と定義されている場合は、デフォルト グループ ポリシー DfltGrpPolicy に設定されているアトリビュートが適用されます。

認可サーバ グループを設定するには **aaa-server** コマンドを使用し、設定済みの aaa サーバ グループにサーバを追加するには **aaa-server-host** コマンドを使用します。

例

config-general コンフィギュレーション モードに入る次の例では、「remotegrp」という名前の IPSec リモートアクセス トンネル グループに「aaa-server78」という名前の認可サーバ グループを設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp general-attributes
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバのパラメータを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般アトリビュートを指定します。

authorization-server-group（webvpn）

WebVPN またはいずれかの電子メール プロキシで使用する認可サーバ グループを指定するには、**authorization-server-group** コマンドを使用します。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）の場合、このコマンドは該当する電子メール プロキシ モードで使用します。コンフィギュレーションから認可サーバを削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは、認可を使用して、ユーザがネットワーク リソースに対して許可されるアクセス レベルを確認します。

authorization-server-group *group_tag*

no authorization-server-group

シンタックスの説明

group_tag	設定済みの認可サーバまたはサーバ グループを指定します。認可サーバを設定するには、**aaa-server** コマンドを使用します。

デフォルト

デフォルトでは、認可サーバは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

例

次の例は、「WebVPNpermit」という名前の認可サーバ グループを使用するように WebVPN サービスを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# authorization-server-group WebVPNpermit
```

次の例は、「POP3Spermit」という名前の認可サーバ グループを使用するように POP3S 電子メール プロキシを設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# authorization-server-group POP3Spermit
```

関連コマンド

コマンド	説明
aaa-server host	認証、認可、アカウンティング サーバを設定します。

auth-prompt

セキュリティ アプライアンスを介したユーザ セッションの AAA チャレンジ テキストを指定または変更するには、グローバル コンフィギュレーション モードで **auth-prompt** コマンドを使用します。認証チャレンジ テキストを削除するには、このコマンドの **no** 形式を使用します。

auth-prompt prompt [**prompt** | **accept** | **reject**] *string*

no auth-prompt prompt [**prompt** | **accept** | **reject**]

シンタックスの説明

accept	Telnet 経由のユーザ認証を受け入れる場合に、プロンプトとして *string* を表示します。
prompt	このキーワードの後に、AAA チャレンジ プロンプトの文字列を入力します。
reject	Telnet 経由のユーザ認証を拒否する場合に、プロンプトとして *string* を表示します。
string	235 文字または 31 単語（どちらか最初に達した方）までの英数字で構成される文字列。特殊文字、スペース、および句読点を使用できます。文字列を終了するには、疑問符を入力するか、**Enter** キーを押します。疑問符は文字列に含まれます。

デフォルト

認証プロンプトを指定しない場合は、次のようになります。

- FTP ユーザには `FTP authentication` が表示される。
- HTTP ユーザには `HTTP Authentication` が表示される。
- Telnet ユーザにはチャレンジ テキストが表示されない。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	セマンティックの小さな変更。

使用上のガイドライン

auth-prompt コマンドを使用すると、TACACS+ サーバまたは RADIUS サーバからのユーザ認証が必要である場合に、セキュリティ アプライアンスを介した HTTP アクセス、FTP アクセス、および Telnet アクセスに対して表示される AAA チャレンジ テキストを指定できます。このテキストは飾りのようなもので、ユーザのログイン時に、ユーザ名プロンプトとパスワード プロンプトの上に表示されます。

ユーザ認証が Telnet から発生する場合は、**accept** オプションと **reject** オプションを使用すると、認証試行が AAA サーバで受け入れられたか拒否されたかを示す異なるステータス プロンプトを表示できます。

AAA サーバがユーザを認証すると、セキュリティ アプライアンスはユーザに **auth-prompt accept** テキストを表示します（指定されている場合）。認証に失敗すると、**reject** テキストを表示します（指定されている場合）。HTTP セッションおよび FTP セッションの認証では、プロンプトにチャレンジ テキストだけが表示されます。**accept** テキストも **reject** テキストも表示されません。

（注） Microsoft Internet Explorer では、認証プロンプトに最大 37 文字表示されます。Netscape Navigator では認証プロンプトに最大 120 文字、Telnet および FTP では最大 235 文字表示されます。

例

次の例では、認証プロンプトを「Please enter your username and password」という文字列に設定しています。

```
hostname(config)# auth-prompt prompt Please enter your username and password
```

コンフィギュレーションにこの文字列を追加すると、ユーザには次のプロンプトが表示されます。

```
Please enter your username and password
User Name:
Password:
```

Telnet ユーザに対しては、セキュリティ アプライアンスが認証試行を受け入れたときに表示するメッセージと、拒否したときに表示するメッセージを別々に指定することもできます。次に例を示します。

```
hostname(config)# auth-prompt reject Authentication failed. Try again.
hostname(config)# auth-prompt accept Authentication succeeded.
```

次の例では、認証が成功したときの認証プロンプトを「You’re OK.」という文字列に設定しています。

```
hostname(config)# auth-prompt accept You’re OK.
```

正常に認証されたユーザには、次のメッセージが表示されます。

```
You’re OK.
```

関連コマンド

コマンド	説明
clear configure auth-prompt	指定済みの認証プロンプト チャレンジ テキストがある場合、そのテキストを削除して、デフォルト値に戻します。
show running-config auth-prompt	現在の認証プロンプト チャレンジ テキストを表示します。

auto-signon

WebVPN ユーザ ログイン クレデンシャルを内部サーバに自動的に渡すようにセキュリティ アプライアンスを設定するには、webvpn コンフィギュレーション モード、webvpn グループ コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードのいずれかのモードで **auto-signon** コマンドを使用します。認証方式は、NTLM（NTLMv1）認証、HTTP Basic 認証、またはその両方が可能です。特定のサーバに対する auto-signon をディセーブルにするには、このコマンドの **no** 形式を元の **ip**、**uri**、および **auth-type** 引数と共に使用します。すべてのサーバに対する auto-signon をディセーブルにするには、このコマンドの **no** 形式を引数なしで指定します。

auto-signon allow {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ntlm** | **all**}

no auto-signon [**allow** {**ip** *ip-address ip-mask* | **uri** *resource-mask*} **auth-type** {**basic** | **ntlm** | **all**}]

シンタックスの説明

all	NTLM と HTTP Basic の両方の認証方式を指定します。
allow	特定のサーバに対する認証をイネーブルにします。
auth-type	認証方式の選択をイネーブルにします。
basic	HTTP Basic 認証方式を指定します。
ip	IP アドレスとマスクで認証先のサーバを特定することを指定します。
ip-address	*ip-mask* と共に、認証先のサーバの IP アドレス範囲を特定します。
ip-mask	*ip-address* と共に、認証先のサーバの IP アドレス範囲を特定します。
ntlm	NTLMv1 認証方式を指定します。
resource-mask	認証先のサーバの URI マスクを特定します。
uri	URI マスクで認証先のサーバを特定することを指定します。

デフォルト

デフォルトでは、この機能はすべてのサーバに対してディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN コンフィギュレーション	•	—	•	—	—
WebVPN グループ ポリシー コンフィギュレーション	•	—	•	—	—
WebVPN ユーザ名コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

auto-signon コマンドは、WebVPN ユーザのためのシングル サインオン方式です。このコマンドは、WebVPN ログイン クレデンシャル（ユーザ名とパスワード）を NTLM 認証、HTTP Basic 認証、またはその両方を使用する認証用の内部サーバに渡します。複数の auto-signon コマンドを入力でき、その際にはコマンドは入力順序に従って（最初に入力したコマンドが先に）処理されます。

auto-signon 機能は、webvpn コンフィギュレーション モード、webvpn グループ コンフィギュレーション モード、または webvpn ユーザ名コンフィギュレーション モードの 3 つのモードで使用できます。一般的な優先動作は、ユーザ名がグループに優先する場合、およびグループがグローバルに優先する場合に適用されます。どのモードを選択するかは、必要な認証範囲によって異なります。次の表を参照してください。

モード	範囲
WebVPN コンフィギュレーション	すべての WebVPN ユーザ（グローバル）
WebVPN グループ コンフィギュレーション	グループ ポリシーで定義されている WebVPN ユーザのサブセット
WebVPN ユーザ名コンフィギュレーション	個々の WebVPN ユーザ

例

次のコマンド例では、すべての WebVPN ユーザに対して、NTLM 認証を使用する auto-signon を設定しています。認証先のサーバの IP アドレスの範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
```

次のコマンド例では、すべての WebVPN ユーザに対して、HTTP Basic 認証を使用する auto-signon を設定しています。認証先のサーバは、URI マスク https://*.example.com/* で定義されています。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow uri https://*.example.com/* auth-type basic
```

次のコマンド例では、WebVPN ユーザ ExamplePolicy グループに対して、HTTP Basic 認証または NTLM 認証を使用する auto-signon を設定しています。認証先のサーバは、URI マスク https://*.example.com/* で定義されています。

```
hostname(config)# group-policy ExamplePolicy attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# auto-signon allow uri https://*.example.com/* auth-type
all
```

次のコマンド例では、Anyuser という名前のユーザに対して、HTTP Basic 認証を使用する auto-signon を設定しています。認証先のサーバの IP アドレスの範囲は、10.1.1.0 ～ 10.1.1.255 です。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0
auth-type basic
```

関連コマンド

コマンド	説明
show running-config webvpn auto-signon	実行コンフィギュレーションの auto-signon 割り当てを表示します。

auto-summary

RIP の経路集約を再度イネーブルにするには、ルータ コンフィギュレーション モードで **auto-summary** コマンドを使用します。RIP の経路集約をディセーブルにするには、このコマンドの **no** 形式を使用します。

auto-summary

no auto-summary

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

RIP バージョン 1 と 2 では、経路集約がイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

経路集約によって、ルーティング テーブル内のルーティング情報の量が少なくなります。

RIP バージョン 1 は、常に自動集約を使用します。RIP バージョン 1 の自動集約機能をディセーブルにすることはできません。

RIP バージョン 2 を使用している場合は、**no auto-summary** コマンドを指定して、自動集約をオフにすることができます。接続が切断されているサブネット間でルーティングする必要がある場合は、自動集約をディセーブルにします。自動集約をディセーブルにすると、サブネットがアドバタイズされます。

実行コンフィギュレーションに表示されるのは、このコマンドの **no** 形式のみです。

例

次の例では、RIP の経路集約をディセーブルにしています。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
hostname(config-router)# no auto-summary
```

関連コマンド

コマンド	説明
clear configure rip	実行コンフィギュレーションからすべての RIP コマンドを消去します。
router rip	RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードに入ります。
show running-config rip	実行コンフィギュレーション内の RIP コマンドを表示します。

auto-update device-id

Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定するには、グローバル コンフィギュレーション モードで **auto-update device-id** コマンドを使用します。デバイス ID を削除するには、このコマンドの **no** 形式を使用します。

auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

no auto-update device-id [**hardware-serial** | **hostname** | **ipaddress** [*if_name*] | **mac-address** [*if_name*] | **string** *text*]

シンタックスの説明

hardware-serial	セキュリティ アプライアンスのハードウェア シリアル番号を使用して、このデバイスを一意に識別します。
hostname	セキュリティ アプライアンスのホスト名を使用して、このデバイスを一意に識別します。
ipaddress [*if_name*]	セキュリティ アプライアンスの IP アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは、Auto Update Server との通信に使用するインターフェイスを使用します。別の IP アドレスを使用する場合は、*if_name* を指定します。
mac-address [*if_name*]	セキュリティ アプライアンスの MAC アドレスを使用して、セキュリティ アプライアンスを一意に識別します。デフォルトでは、セキュリティ アプライアンスは、Auto Update Server との通信に使用するインターフェイスの MAC アドレスを使用します。別の MAC アドレスを使用する場合は、*if_name* を指定します。
string *text*	デバイスを Auto Update Server に対して一意に識別するためのテキスト文字列を指定します。

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

デフォルト

デフォルトの ID はホスト名です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

例

次の例では、デバイス ID をシリアル番号に設定しています。

```
hostname(config)# auto-update device-id hardware-serial
```

関連コマンド

auto-update poll-period	セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update poll-at

セキュリティ アプライアンスで Auto Update Server をポーリングする特定の日時を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-at** コマンドを使用します。

auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

no auto-update poll-at *days-of-the-week time* [**randomize** *minutes*] [*retry_count* [*retry_period*]]

シンタックスの説明

days-of-the-week	Monday（月曜日）、Tuesday（火曜日）、Wednesday（水曜日）、Thursday（木曜日）、Friday（金曜日）、Saturday（土曜日）、および Sunday（日曜日）から曜日またはその組み合せを指定します。この他にも、daily（月曜日から日曜日まで）、weekdays（月曜日から金曜日まで）、weekend（土曜日と日曜日）を指定できます。
time	ポーリングを開始する時刻を HH:MM 形式で指定します。たとえば、8:00 は午前 8 時を、20:00 は午後 8 時を示します。
randomize *minutes*	指定した開始時刻以後、任意にポーリングする期間（1 ～ 1439 分）を指定します。
retry_count	Auto Update Server への最初の接続試行が失敗した後に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続を再試行する間隔を指定します。デフォルトは 5 分です。1 ～ 35791 分に指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

auto-update poll-at コマンドは、アップデートがあるかどうかを確認するためにポーリングするタイミングを指定します。**randomize** オプションをイネーブルにすると、*time* で指定した開始時刻以後、指定した時間（分単位）内の任意の時刻にポーリングされます。**auto-update poll-at** コマンドと **auto-update poll-period** コマンドは、互いに排他的です。設定できるのは、いずれか一方だけです。

例

次の例では、セキュリティ アプライアンスで毎週金曜日と土曜日の午後 10 時から 11 時の間、任意の時刻に Auto Update Server をポーリングするように設定しています。また、接続できなかった場合は、10 分間隔で 2 回再試行します。

```
hostname(config)# auto-update poll-at Friday Saturday 22:00 randomize 60 2 10
hostname(config)# auto-update server http://192.168.1.114/aus/autoupdate.asp
```

関連コマンド

auto-update device-id	Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。
auto-update poll-period	セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。
auto-update timeout	このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
management-access	セキュリティ アプライアンス上の内部管理インターフェイスにアクセスできるようにします。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update poll-period

セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定するには、グローバル コンフィギュレーション モードで **auto-update poll-period** コマンドを使用します。このパラメータをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

no auto-update poll-period *poll_period* [*retry_count* [*retry_period*]]

シンタックスの説明

poll_period	Auto Update Server をポーリングする頻度を分単位で指定します（1 ～ 35791）。デフォルトは 720 分（12 時間）です。
retry_count	Auto Update Server への最初の接続試行が失敗した後に、再接続を何回試行するかを指定します。デフォルトは 0 です。
retry_period	接続を試行する間隔を分単位で指定します（1 ～ 35791）。デフォルトは 5 分です。

デフォルト

デフォルトのポーリング間隔は 720 分（12 時間）です。

Auto Update Server への最初の接続試行が失敗した後に再接続を試行する回数は、デフォルトでは 0 です。

接続試行のデフォルト間隔は、5 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

auto-update poll-at コマンドと **auto-update poll-period** コマンドは、互いに排他的です。設定できるのは、いずれか一方だけです。

例

次の例では、ポーリング間隔を 360 分に、リトライ回数を 1 回に、リトライ間隔を 3 分に設定しています。

```
hostname(config)# auto-update poll-period 360 1 3
```

関連コマンド

auto-update device-id	Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。
auto-update server	Auto Update Server を指定します。
auto-update timeout	このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update server

Auto Update Server を指定するには、グローバル コンフィギュレーション モードで **auto-update server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、定期的に Auto Update Server にアクセスして、コンフィギュレーション、オペレーティング システム、および ASDM のアップデートがないか調べます。

auto-update server *url* [**source** *interface*] [*verify-certificate*]

no auto-update server *url* [**source** *interface*] [*verify-certificate*]

シンタックスの説明

url	Auto Update Server の場所を、シンタックス **http**[**s**]**:**[[*user:password@*]*location* [*:port*]] / *pathname* を使用して指定します。
interface	Auto Update Server に要求を送信する場合に使用するインターフェイスを指定します。
verify_certificate	Auto Update Server によって返される証明書を確認します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	複数のサーバをサポートできるようにコマンドが変更されました。

使用上のガイドライン

自動アップデート用に複数のサーバを設定できます。アップデートがあるかどうかをチェックするときは、まず 1 台目のサーバに接続しようとし、接続できなかった場合は、2 台目のサーバとの接続を試みます。この要領で、すべてのサーバとの接続が試みられます。どのサーバとも接続できないと、auto-update poll-period コマンドで再試行するように設定している場合は、最初のサーバに戻って再試行されます。

自動アップデート機能を正しく動作させるには、**boot system configuration** コマンドを使用して、有効なブート イメージを指定する必要があります。同様に、ASDM ソフトウェア イメージを自動アップデートするには、**asdm image** コマンドを使用する必要があります。

source *interface* 引数に指定したインターフェイスが、**management-access** コマンドで指定したインターフェイスと同じである場合、Auto Update Server への要求は VPN トンネル経由で送信されます。

例

次の例では、Auto Update Server の URL を設定し、インターフェイス outside を指定しています。

```
hostname(config)# auto-update server http://10.1.1.1:1741/ source outside
```

関連コマンド

auto-update device-id	Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。
auto-update poll-period	セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。
auto-update timeout	このタイムアウト期間内に Auto Update Server にアクセスしない場合、セキュリティ アプライアンスを通過するトラフィックを停止します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
management-access	セキュリティ アプライアンス上の内部管理インターフェイスにアクセスできるようにします。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

auto-update timeout

Auto Update Server へのアクセスに関するタイムアウト期間を設定するには、グローバル コンフィギュレーション モードで **auto-update timeout** コマンドを使用します。このタイムアウト期間内に Auto Update Server にアクセスしないと、セキュリティ アプライアンスは、セキュリティ アプライアンスを通過するすべてのトラフィックを停止させます。タイムアウトを設定することで、セキュリティ アプライアンスのイメージとコンフィギュレーションを常に最新の状態に保つことができます。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

auto-update timeout *period*

no auto-update timeout [*period*]

シンタックスの説明

period	タイムアウト期間を分単位で指定します（1 ～ 35791）。デフォルトは 0 で、タイムアウトはありません。タイムアウトを 0 に設定することはできません。タイムアウトを 0 にリセットするには、このコマンドの **no** 形式を使用します。

デフォルト

デフォルトのタイムアウトは 0 で、セキュリティ アプライアンスはタイムアウトしないように設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

タイムアウト状態は、システム ログ メッセージ 201008 で報告されます。

例

次の例では、タイムアウトを 24 時間に設定しています。

```
hostname(config)# auto-update timeout 1440
```

関連コマンド

auto-update device-id	Auto Update Server 用のセキュリティ アプライアンス デバイス ID を設定します。
auto-update poll-period	セキュリティ アプライアンスが Auto Update Server からのアップデートをチェックする頻度を設定します。
auto-update server	Auto Update Server を指定します。
clear configure auto-update	Auto Update Server のコンフィギュレーションを消去します。
show running-config auto-update	Auto Update Server のコンフィギュレーションを表示します。

CHAPTER 4

backup interface コマンド～ browse-networks コマンド

backup interface

組み込みスイッチを持つモデル（ASA 5505 適応型セキュリティ アプライアンスなど）では、インターフェイス コンフィギュレーション モードで **backup interface** コマンドを使用して、VLAN インターフェイスを ISP などのバックアップ用インターフェイスに指定します。このコマンドを入力できるのは、VLAN インターフェイスのインターフェイス コンフィギュレーション モードだけです。このコマンドは、プライマリ インターフェイスを通るデフォルトのルートがダウンしない限り、バックアップに指定したインターフェイスを通過しようとするトラフィックをすべてブロックします。通常の状態に戻すには、**no backup interface** コマンドを使用します。

backup interface vlan *number*

no backup interface vlan *number*

シンタックスの説明

vlan *number*	バックアップ インターフェイスの VLAN の ID を指定します。

デフォルト

デフォルトでは、**backup interface** コマンドはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
7.2(2)	Security Plus ライセンスでは、VLAN インターフェイスの数が通常のトラフィック用には 3 つ、バックアップ インターフェイス用には 1 つ、フェールオーバー用には 1 つと制限されていました。この制限がなくなり、最大 20 のインターフェイスを設定できるようになりました（これ以外の制限はありません）。したがって、**backup interface** コマンドは、4 つ以上のインターフェイスをイネーブルにするためには不要です。

使用上のガイドライン

backup interface コマンドで Easy VPN を設定すると、バックアップ インターフェイスがプライマリになった場合に、セキュリティ アプライアンスは VPN 規則を新しいプライマリ インターフェイスに移動します。バックアップ インターフェイスの状態を表示するには、**show interface** コマンドを参照してください。

プライマリ インターフェイスがダウンした場合にバックアップ インターフェイスを使用できるように、必ずプライマリとバックアップの両方のインターフェイスにデフォルト ルートを設定してください。たとえば、プライマリ インターフェイス用に管理ディスタンスの低いルート、バックアップ インターフェイス用に管理ディスタンスの高いルートの 2 つのデフォルト ルートを設定します。DHCP サーバから取得したデフォルト ルートの管理ディスタンスを上書きする方法については、**dhcp client route distance** コマンドを参照してください。ISP のデュアル サポートの設定について詳しくは、**sla monitor** コマンドと **track rtr** コマンドを参照してください。

management-only コマンドを設定しているインターフェイスをバックアップ インターフェイスに設定することはできません。

例

次の例では、4 つの LAN インターフェイスを設定しています。backup-ip インターフェイスでは、プライマリ インターフェイスがダウンしている場合に限り、通過トラフィックを許可します。**route** コマンドは、プライマリ インターフェイスおよびバックアップ インターフェイスのデフォルト ルートを作成しています。バックアップ ルートに低い管理ディスタンスが設定されています。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# backup interface vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# route outside 0 0 10.1.1.2 1
hostname(config)# route backup-isp 0 0 10.1.2.2 2
```

関連コマンド

コマンド	説明
forward interface	あるインターフェイスで、別のインターフェイスへのトラフィックを開始できないようにします。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードに入ります。
dhcp client route distance	DHCP サーバから取得したデフォルト ルートの管理ディスタンスを上書きします。
sla monitor	スタティック ルートのトラッキングの SLA 監視オペレーションを定義します。
track rtr	SLA 監視オペレーションの状況をトラッキングします。

backup-servers

バックアップ サーバを設定するには、グループ ポリシー コンフィギュレーション モードで **backup-servers** コマンドを使用します。バックアップ サーバを削除するには、このコマンドの **no** 形式を使用します。backup-servers アトリビュートを実行コンフィギュレーションから削除するには、引数を付けずにこのコマンドの **no** 形式を使用します。これで、backup-servers の値を別のグループ ポリシーから継承できます。

IPSec バックアップ サーバにより、VPN クライアントは、プライマリ セキュリティ アプライアンスが利用できない場合に中央のサイトに接続できます。バックアップ サーバを設定すると、IPSec トンネルが確立されるときにセキュリティ アプライアンスがクライアントにサーバ リストをプッシュします。

backup-servers {server1 server2.. . . server10 | clear-client-config | keep-client-config}

no backup-servers [server1 server2.. . . server10 | clear-client-config | keep-client-config]

シンタックスの説明

clear-client-config	クライアントがバックアップ サーバを使用しないように指定します。セキュリティ アプライアンスは、ヌルのサーバ リストをプッシュします。
keep-client-config	セキュリティ アプライアンスがバックアップ サーバ情報をクライアントに送信しないように指定します。クライアントは、独自のバックアップ サーバ リストを使用します（設定されている場合）。
server1 server 2.... server10	プライマリ セキュリティ アプライアンスが利用できない場合に VPN クライアントが使用するサーバのリストを入力します。各サーバをスペースで区切って優先度の高い順に並べます。サーバは、IP アドレスまたはホスト名で指定します。リストには 500 文字入力できますが、10 個のエントリしか含めることができません。

デフォルト

クライアントまたはプライマリ セキュリティ アプライアンス上にバックアップ サーバを設定しない限り、バックアップ サーバは存在しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

バックアップ サーバは、クライアントまたはプライマリ セキュリティ アプライアンス上に設定します。セキュリティ アプライアンス上にバックアップ サーバを設定すると、セキュリティ アプライアンスはバックアップ サーバ ポリシーをグループ内のクライアントにプッシュし、クライアント上にバックアップ サーバ リストが設定されている場合、そのリストを置き換えます。

(注) ホスト名を使用する場合は、バックアップ DNS サーバとバックアップ WINS サーバを、プライマリ DNS サーバとプライマリ WINS サーバとは別のネットワーク上に置くことをお勧めします。同一ネットワーク上に置くと、ハードウェア クライアントの背後のクライアントが DHCP を介してハードウェア クライアントから DNS 情報および WINS 情報を取得し、プライマリ サーバとの接続が失われ、バックアップ サーバに異なる DNS 情報および WINS 情報がある場合、DHCP リースが期限切れになるまでクライアントをアップデートできません。さらに、ホスト名を使用するときに DNS サーバが利用できないと、重大な遅延が発生することがあります。

例

次の例は、「FirstGroup」という名前のグループ ポリシーに IP アドレス 10.10.10.1 および 192.168.10.14 のバックアップ サーバを設定する方法を指定しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# backup-servers 10.10.10.1 192.168.10.14
```

banner

セッション バナー、ログイン バナー、または「今日のお知らせ」バナーを設定するには、グローバル コンフィギュレーション モードで ***banner*** コマンドを使用します。指定したバナー キーワード（**exec**、**login**、または **motd**）のすべての行を削除するには、**no banner** コマンドを使用します。

banner {**exec | login | motd** *text*}

[no] banner {**exec | login | motd** [*text*]}

シンタックスの説明

exec	イネーブル プロンプトを表示する前に、バナーを表示するようにシステムを設定します。
login	ユーザが Telnet を使用してセキュリティ アプライアンスにアクセスしたときに、パスワード ログイン プロンプトを表示する前にバナーを表示するようにシステムを設定します。
motd	初めて接続したときに「今日のお知らせ」バナーを表示するようにシステムを設定します。
text	表示するメッセージ テキスト行。

デフォルト

デフォルトでは、セッション バナー、ログイン バナー、および「今日のお知らせ」バナーは表示されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

banner コマンドは、指定したキーワードに対応するバナーを表示するように設定します。*text* 文字列は、最初の空白文字（スペース）の後に続く、行末（復帰または改行（LF））までのすべての文字で構成されます。テキスト内にあるスペースはそのまま表示されます。ただし、CLI ではタブを入力できません。

先に既存のバナーを消去しない限り、後続の *text* エントリはその末尾に追加されます。

（注） トークン $(domain) と $(hostname) を使用すると、それぞれセキュリティ アプライアンスのドメイン名とホスト名に置き換えられます。コンテキスト コンフィギュレーションで $(system) トークンを入力すると、コンテキストはシステム コンフィギュレーションに設定されているバナーを使用します。

バナーを複数行にするには、追加する 1 行ごとに banner コマンドを新しく入力します。入力した行は、既存バナーの末尾に追加されていきます。RAM およびフラッシュ メモリの容量による限界を除いて、バナーの長さに制限はありません。

Telnet または SSH でセキュリティ アプライアンスにアクセスする場合、バナー メッセージの処理に必要なシステム メモリが十分にないときや、TCP 書き込みエラーが発生したときは、セッションが閉じます。exec バナーと motd バナーだけが、SSH を介したセキュリティ アプライアンスへのアクセスをサポートしています。login バナーは SSH をサポートしていません。

バナーを置き換えるには、**no banner** コマンドを使用してから、新しい行を追加します。

no banner {**exec** | **login** | **motd**} コマンドは、指定したバナー キーワードのすべての行を削除します。

no banner コマンドでは、テキスト文字列の一部だけを削除できません。そのため、**no banner** コマンドの末尾に入力した *text* はすべて無視されます。

例

次の例は、**exec**、**login**、および **motd** の各バナーを設定する方法を示しています。

```
hostname(config)# banner motd Think on These Things
hostname(config)# banner exec Enter your password carefully
hostname(config)# banner login Enter your password to log in
hostname(config)# show running-config banner
exec:
Enter your password carefully

login:
Enter your password to log in

motd:
Think on These Things
```

次の例は、**motd** バナーにもう 1 行を追加する方法を示しています。

```
hostname(config)# banner motd and Enjoy Today
hostname(config)# show running-config banner motd
Think on These Things and Enjoy Today
```

関連コマンド

コマンド	説明
clear configure banner	すべてのバナーを削除します。
show running-config banner	すべてのバナーを表示します。

banner（グループ ポリシー）

リモート クライアントの接続時にリモート クライアント上でバナー（ウェルカム テキスト）を表示するには、グループ ポリシー コンフィギュレーション モードで **banner** コマンドを使用します。バナーを削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、バナーを別のグループ ポリシーから継承できます。バナーを継承しないようにするには、**banner none** コマンドを使用します。

banner {**value** *banner_string* | **none}**

no banner

（注） VPN グループ ポリシーで複数のバナーを設定し、いずれかのバナーを削除すると、すべてのバナーが削除されます。

シンタックスの説明

none	バナーにヌル値を設定して、バナーを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからバナーを継承しないようにします。
value *banner_string*	バナー テキストを設定します。文字列の最大サイズは 500 文字です。復帰を挿入するには、「\n」シーケンスを使用します。

デフォルト

デフォルトのバナーはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、「FirstGroup」という名前のグループ ポリシーにバナーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# banner value Welcome to Cisco Systems 7.0(1).
```

blocks

ブロック診断（**show blocks** コマンドで表示）に追加のメモリを割り当てるには、特権 EXEC モードで **blocks** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。割り当てられるメモリ量は最大 150 KB ですが、空きメモリの 50% を超えることはありません。オプションで、メモリ サイズを手動で指定できます。

blocks queue history enable [*memory_size*]

no blocks queue history enable [*memory_size*]

シンタックスの説明

memory_size	（オプション）動的な値を適用するのではなく、ブロック診断用のメモリ サイズをバイト単位で設定します。この値が空きメモリよりも大きい場合は、エラー メッセージが表示され、値は受け入れられません。この値が空きメモリの 50% を超える場合は、警告メッセージが表示されますが、値は受け入れられます。

デフォルト

ブロック診断の追跡に割り当てられるデフォルト メモリは 2136 バイトです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

現在割り当てられているメモリを表示するには、**show blocks queue history** コマンドを入力します。

セキュリティ アプライアンスをリロードすると、メモリ割り当てがデフォルトに戻ります。

例

次の例では、ブロック診断用のメモリ サイズを増やしています。

```
hostname# blocks queue history enable
```

次の例では、ブロック診断用のメモリ サイズを 3000 バイトに増やしています。

```
hostname# blocks queue history enable 3000
```

次の例では、ブロック診断用のメモリ サイズを 3000 バイトに増やそうとしていますが、値が空きメモリを上回っています。

```
hostname# blocks queue history enable 3000
ERROR: memory size exceeds current free memory
```

次の例では、ブロック診断用のメモリ サイズを 3000 バイトに増やしていますが、値が空きメモリの 50% を超えています。

```
hostname# blocks queue history enable 3000
WARNING: memory size exceeds 50% of current free memory
```

関連コマンド

コマンド	説明
clear blocks	システム バッファの統計情報を消去します。
show blocks	システム バッファの使用状況を表示します。

boot

システムが次回のリロードで使用するシステム イメージ、およびシステムが起動時に使用するコンフィギュレーション ファイルを指定するには、グローバル コンフィギュレーション モードで **boot** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

boot {**config** | ***system***} *url*

no boot {***config*** | ***system***} *url*

シンタックスの説明

config	システムがロードされるときに使用するコンフィギュレーション ファイルを指定します。
system	システムがロードされるときに使用するシステム イメージ ファイルを指定します。
url	イメージまたはコンフィギュレーションの場所を設定します。マルチ コンテキスト モードでは、管理コンテキストですべてのリモート URL にアクセスできる必要があります。次の URL シンタックスを参照してください。 • ***disk0:/***[*path/*]*filename* ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内蔵フラッシュ メモリを指します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。 • ***disk1:/***[*path/*]*filename* ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。 • ***flash:/***[*path/*]*filename* この URL は内蔵フラッシュ メモリを指します。 • ***tftp://***[*user*[**:***password*]**@**]*server*[*:port*]**/**[*path/*]*filename*[***;int=****interface_name*] サーバのアドレスへのルートを上書きする場合は、インターフェイス名を指定します。 このオプションは、ASA 5500 シリーズの適応型セキュリティ アプライアンスの **boot system** コマンドでしか使用できません。**boot config** コマンドを使用するには、セットアップ コンフィギュレーションがフラッシュ メモリになければなりません。 **boot system tftp:** コマンドは、1 つしか設定できず、最初に設定する必要があります。

デフォルト

boot config コマンドを指定しないと、スタートアップ コンフィギュレーションが非表示の場所に保存され、スタートアップ コンフィギュレーションを利用するコマンド（**show startup-config** コマンドや **copy startup-config** コマンド）だけで使用されます。

boot system コマンドにデフォルトはありません。場所を指定しないと、セキュリティ アプライアンスは、起動する有効なイメージを、まず内蔵フラッシュ メモリで探し、次に外部フラッシュ メモリで探します。有効なイメージが見つからない場合は、システム イメージがロードされず、セキュリティ アプライアンスは、ROMMON モードまたは Monitor モードに入るまでブート ループ状態になります。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドを、**write memory** コマンドを使用してスタートアップ コンフィギュレーションに保存すると、BOOT と CONFIG_FILE という環境変数にも設定が保存されます。この環境変数は、セキュリティ アプライアンスが再起動するときにスタートアップ コンフィギュレーションと起動するソフトウェア イメージを決めるために使用します。

最大 4 つの **boot system** コマンド エントリを入力し、異なるイメージを指定して、順番に起動を試みることができます。セキュリティ アプライアンスは、最初に見つけた有効なイメージを起動します。

現在の実行コンフィギュレーションとは別の場所のスタートアップ コンフィギュレーション ファイルを使用したい場合は、実行コンフィギュレーションを保存した後で、必ずスタートアップ コンフィギュレーション ファイルを新しい場所にコピーしてください。保存後にコピーしておかないと、新しいスタートアップ コンフィギュレーションが実行コンフィギュレーションで上書きされます。

ヒント　ASDM イメージ ファイルは、**asdm image** コマンドで指定します。

例　次の例は、起動時にセキュリティ アプライアンスが configuration.txt という名前のコンフィギュレーション ファイルをロードするように指定しています。

```
hostname(config)# boot config disk0:/configuration.txt
```

関連コマンド

コマンド	説明
asdm image	ASDM ソフトウェア イメージを指定します。
show bootvar	ブート ファイルおよびコンフィギュレーションの環境変数を表示します。

border style

認証された WebVPN ユーザに表示される WebVPN ホームページの境界線をカスタマイズするには、webvpn カスタマイゼーション モードで **border style** コマンドを使用します。

border style *value*

[**no**] **border style** *value*

コマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

value	Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

境界線のデフォルトのスタイルは background-color:#669999;color:white です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、境界線の背景色を RGB カラー #66FFFF（緑色の一種）にカスタマイズしています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# border style background-color:66FFFF
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの Application Access ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの Browse Networks ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの Web Bookmarks タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの File Bookmarks タイトルまたはリンクをカスタマイズします。

browse-networks

認証された WebVPN ユーザに表示される WebVPN ホームページの Browse Networks ボックスをカスタマイズするには、webvpn カスタマイゼーション モードで **browse-networks** コマンドを使用します。

browse-networks {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **browse-networks** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

コマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

title	タイトルを変更することを指定します。
message	タイトルの下に表示されるメッセージを変更することを指定します。
dropdown	ドロップダウン ボックスを変更することを指定します。
text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのテキストは「Browse Networks」です。

デフォルトのタイトルのスタイルは次のとおりです。

background-color:#99CCCC;color:black;font-weight:bold;text-transform:uppercase

デフォルトのメッセージのテキストは「Enter Network Path」です。

デフォルトのメッセージのスタイルは次のとおりです。

background-color:#99CCCC;color:maroon;font-size:smaller

デフォルトのドロップダウンのテキストは「File Folder Bookmarks」です。

デフォルトのドロップダウンのスタイルは次のとおりです。

border:1px solid black;font-weight:bold;color:black;font-size:80%

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、タイトルを「Browse Corporate Networks」に変更し、スタイル内のテキストを青色に変更しています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# browse-networks title text Browse Corporate Networks
F1-asa1(config-webvpn-custom)# browse-networks title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの Application Access ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの File Bookmarks タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの Web Application ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの Web Bookmarks タイトルまたはリンクをカスタマイズします。

CHAPTER 5

cache コマンド～ clear compression コマンド

cache

キャッシュ モードに入り、キャッシング アトリビュートの値を設定するには、webvpn モードで **cache** コマンドを入力します。キャッシュ関連のコマンドをすべてコンフィギュレーションから削除し、それらをデフォルト値に戻すには、同様に webvpn モードで、このコマンドの **no** 形式を使用します。

cache

no cache

デフォルト

各キャッシュ アトリビュートのデフォルト設定でイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシングは頻繁に再利用されるオブジェクトをシステム キャッシュに保存します。キャッシュに保存しておくことにより、リライトやコンテンツの圧縮を繰り返し実行する必要が少なくなります。WebVPN とリモート サーバの間および WebVPN とエンドユーザのブラウザとの間の両方でトラフィックを削減します。その結果、多くのアプリケーションがさらに効率よく実行されます。

例

次の例は、キャッシュ モードに入る方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシングをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

cache-compressed

WebVPN セッションの圧縮オブジェクトをキャッシュするには、webvpn モードで **cache-compressed** コマンドを使用します。圧縮コンテンツのキャッシングを禁止するには、このコマンドの **no** 形式を入力します。

cache-compressed enable

no cache-compressed

シンタックスの説明

enable	WebVPN セッションの圧縮コンテンツのキャッシングをイネーブルにします。

デフォルト

圧縮コンテンツのキャッシングはデフォルトでイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシングでは、頻繁に再利用されるオブジェクトがシステム キャッシュに保存されます。圧縮コンテンツのキャッシングがイネーブルの場合、セキュリティ アプライアンスは圧縮されたオブジェクトを保存します。圧縮コンテンツのキャッシングをディセーブルにすると、セキュリティ アプライアンスは圧縮ルーチンを呼び出す前にオブジェクトを保存します。

例

次の例は、圧縮コンテンツのキャッシングをディセーブルにする方法と、それを再度イネーブルにする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# no cache-compressed
hostname(config-webvpn-cache)# cache-compressed enable
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードに入ります。
disable	キャッシングをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

cache-time

CRL を期限切れと見なす前にキャッシュに残す時間を分単位で指定するには、ca-crl コンフィギュレーション モードで **cache-time** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

cache-time *refresh-time*

no cache-time

シンタックスの説明

refresh-time	CRL をキャッシュに残す時間（分）を指定します。範囲は 1 ～ 1,440 分です。CRL に NextUpdate フィールドがない場合、CRL はキャッシュされません。

デフォルト

デフォルト設定は 60 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、トラストポイント central に 10 分のキャッシュ時間のリフレッシュ値を指定します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# cache-time 10
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
enforcenextupdate	証明書で NextUpdate CRL フィールドを処理する方法を指定します。

call-agent

コール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **call-agent** コマンドを使用します。このモードには、**mgcp-map** コマンドを使用してアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

シンタックスの説明

ip_address	ゲートウェイの IP アドレス。
group_id	コール エージェント グループの ID（0 ～ 2147483647）。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

call-agent コマンドは、1 つまたは複数のゲートウェイを管理できるコール エージェントのグループを指定するために使用します。コール エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。*group_id* が同じコール エージェントは、同じグループに所属します。1 つのコール エージェントは複数のグループに所属できます。*group_id* オプションは 0 ～ 4294967295 の数字です。*ip_address* オプションでは、コール エージェントの IP アドレスを指定します。

例

次の例では、コール エージェント 10.10.11.5 と 10.10.11.6 がゲートウェイ 10.10.10.115 を制御できるようにし、コール エージェント 10.10.11.7 と 10.10.11.8 がゲートウェイ 10.10.10.116 と 10.10.10.117 の両方を制御できるようにしています。

```
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP に関するデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッション情報を表示します。

call-duration-limit

H.323 コール 1 回の制限時間を設定するには、パラメータ コンフィギュレーション モードで **call-duration-limit** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

call-duration-limit *hh:mm:ss*

no call-duration-limit *hh:mm:ss*

シンタックスの説明

hh:mm:ss	時、分、秒で時間を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 コール 1 回の制限時間を設定する方法を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-duration-limit 0:1:0
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

call-party-numbers

H.323 コールのセットアップ時に発信側の番号の送信を必須にするには、パラメータ コンフィギュレーション モードで **call-party-numbers** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

call-party-numbers

no call-party-numbers

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 コールのセットアップ時に発信側の番号の送信を必須にする方法を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-party-numbers
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

capture

パケット キャプチャ機能をイネーブルにして、パケットのスニッフィングやネットワーク障害を検出できるようにするには、**capture** コマンドを使用します。パケットのキャプチャ機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

capture *capture_name* [**type** {**asp-drop** [*drop-code*] | **raw-data** | **isakmp** | ***webvpn*** **user** *webvpn-user* [**url** *url*]}] [**access-list** *access_list_name*] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*] [**circular-buffer**][**trace** *trace_count*]

no capture *capture-name* [**access-list** *access_list_name*] [**circular-buffer**] [**interface** *interface_name*]

シンタックスの説明

access-list *access_list_name*	（オプション）アクセス リストに一致するトラフィックをキャプチャします。マルチ コンテキスト モードでは、1 つのコンテキスト内でのみ使用できます。
asp-drop [*drop-code***]**	（オプション）アクセラレーション セキュリティ パスでドロップされたパケットをキャプチャします。*drop-code* で、アクセラレーション セキュリティ パスでドロップされたトラフィックのタイプを指定します。ドロップ コードの一覧については、**show asp drop frame** コマンドを参照してください。*drop-code* 引数を入力しないと、ドロップされたパケットがすべてキャプチャされます。 このキーワードは、**packet-length**、**circular-buffer**、および **buffer** と一緒に入力できますが、**interface** や **ethernet** と一緒に入力することはできません。
buffer *buf_size*	（オプション）パケットの保存に使用するバッファのサイズをバイト単位で定義します。バッファがいっぱいになると、パケットのキャプチャが停止します。
capture_name	パケット キャプチャの名前を指定します。複数のタイプのトラフィックをキャプチャする場合は、複数の **capture** 文で同じ名前を使用します。**show capture** コマンドでキャプチャのコンフィギュレーションを表示すると、すべてのオプションが 1 行にまとめて示されます。
circular-buffer	（オプション）バッファがいっぱいになったときに、先頭部分からバッファを上書きしていきます。
ethernet-type *type*	（オプション）キャプチャするイーサネット タイプを選択します。デフォルトは、IP パケットです。802.1Q タイプと VLAN タイプでは例外が発生します。802.1Q タグは自動的にスキップされ、条件に一致しているかどうかの判定には内部イーサネット タイプが使用されます。
interface *interface_name*	パケットのキャプチャ機能を使用するインターフェイスの名前を設定します。パケットをキャプチャする場合は、インターフェイスを設定する必要があります。複数の **capture** コマンドで同じキャプチャ名を指定して、複数のインターフェイスを設定できます。ASA 5500 シリーズ適応型セキュリティ アプライアンスのデータプレーン上のパケットをキャプチャするには、***interface*** キーワードと、インターフェイスの名前として **asa_dataplane** を指定します。
isakmp	（オプション）ISAKMP トラフィックをキャプチャします。マルチ コンテキスト モードでは使用できません。ISAKMP サブシステムは、上位層のプロトコルにアクセスできません。キャプチャは、PCAP パーサーを満たすために物理層、IP 層、および UDP 層が組み合された擬似キャプチャです。ピア アドレスは SA 交換から取得され、IP 層に保存されます。

packet-length *bytes*	（オプション）キャプチャ バッファに保存する各パケットの最大サイズ（バイト数）を設定します。
raw-data	（オプション）着信パケットと発信パケットを 1 つまたは複数のインターフェイス上でキャプチャします。これがデフォルトです。
type	（オプション）キャプチャするデータのタイプを指定します。
url *url*	（オプション）データをキャプチャするときに照合する URL のプレフィックスを指定します。サーバへの HTTP トラフィックをキャプチャするには、URL http://*server*/*path* を使用します。サーバへの HTTPS トラフィックをキャプチャする場合は、https://*server*/*path* を使用します。
user ***webvpn-user***	（オプション）WebVPN キャプチャのユーザ名を指定します。
webvpn	（オプション）特定の WebVPN 接続の WebVPN データをキャプチャします。
trace *trace_count*	（オプション）パケットのトレース情報をキャプチャすることと、キャプチャするパケットの数を指定します。アクセス リストと共に使用し、パケットが正常に処理されたかどうかを確認するためにデータ パスにトレース パケットを挿入します。

デフォルト

デフォルトは次のとおりです。

- **type** は **raw-data**
- **buffer** *size* は 512 KB
- イーサネットのタイプは IP
- **packet-length** は 68 バイト

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
6.2(1)	このコマンドが導入されました。
7.0(1)	新しいキーワード、特に ***type asp-drop***、***type isakmp***、***type raw-data***、および ***type webvpn*** を含めるように変更されました。
7.2(1)	***trace*** キーワードを含めるように変更されました。

使用上のガイドライン

パケットのキャプチャは、接続上の問題のトラブルシューティングや疑わしいアクティビティのモニタリングを行う場合に役立ちます。複数のキャプチャを設定できます。パケットのキャプチャ情報を表示するには、**show capture** *name* コマンドを使用します。キャプチャ情報をファイルに保存するには、**copy capture** コマンドを使用します。パケットのキャプチャ情報を Web ブラウザで表示するには、**https://***security appliance-ip-address*/**capture/***capture_name*[/**pcap**] コマンドを使用します。**pcap** オプション キーワードを指定すると、libpcap 形式のファイルが Web ブラウザにダウンロードされるので、Web ブラウザを使用してファイルを保存できます。libcap ファイルは、TCPDUMP または Ethereal で表示できます。

バッファの内容を TFTP サーバに ASCII 形式でコピーする場合は、パケットの詳細や 16 進ダンプは表示されず、ヘッダーだけが表示されます。詳細や 16 進ダンプを表示するには、バッファを PCAP 形式で伝送し、TCPDUMP または Ethereal を使用して読み取る必要があります。

WebVPN のキャプチャをイネーブルにすると、セキュリティ アプライアンスが *capture_name*_ORIGINAL.000 と *capture_name*_MANGLED.000 というファイルのペアを作成します。後続のキャプチャごとに同様のペアを作成しますが、ファイル名の番号を順次増やしていきます。

（注） WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成した後は、キャプチャをディセーブルにしてください。

キャプチャが消去されないようにする場合は、**no capture** に **access-list** オプション キーワードまたは **interface** オプション キーワードのいずれかを付加して入力します。オプション キーワードを付加せずに **no capture** を入力すると、キャプチャが削除されます。**access-list** オプション キーワードを指定した場合は、キャプチャからアクセス リストが削除され、キャプチャは残されます。**interface** キーワードを指定した場合は、指定したインターフェイスからキャプチャが分離され、そのまま残ります。

（注） **capture** コマンドはコンフィギュレーションには保存されず、フェールオーバー中にスタンバイ装置にコピーされることもありません。

例

パケット キャプチャをイネーブルにするには、次のように入力します。

```
hostname# capture captest interface inside
hostname# capture captest interface outside
```

「captest」というキャプチャの内容を Web ブラウザで表示するには、次のアドレスを入力します。

```
https://171.69.38.95/capture/captest/pcap
```

Internet Explorer や Netscape Navigator などの Web ブラウザで使用される libcap ファイルをローカル マシンにダウンロードするには、次のアドレスを入力します。

```
https://171.69.38.95/capture/http/pcap
```

次の例では、外部ホスト 171.71.69.234 からキャプチャしたトラフィックが内部 HTTP サーバに伝送されます。

```
hostname# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
hostname# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
hostname# capture http access-list http packet-length 74 interface inside
```

次の例では、ARP パケットをキャプチャする方法を示します。

```
hostname# capture arp ethernet-type arp interface outside
```

次の例では、wwwin.abcd.com/hr/people という Web サイトにアクセスする user2 の HTTP トラフィックをキャプチャする、*hr* という WebVPN キャプチャを作成しています。

```
hostname# capture hr type webvpn user user2 url http://wwwin.abcd.com/hr/people
WebVPN capture started.
   capture name   hr
   user name      user2
   url            /http/0/wwwin.abcd.com/hr/people
```

次の例では、データ ストリームにトレース パケットを 5 つ挿入します。*access-list 101* は、TCP プロトコルが FTP であるトラフィックを定義しています。

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

上の例で **show capture ftptrace** コマンドを使用すると、トレースされたパケットと、パケットの処理に関する情報がわかりやすく表示されます。

関連コマンド

コマンド	説明
clear capture	キャプチャ バッファを消去します。
copy capture	キャプチャ ファイルをサーバにコピーします。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。

cd

現在の作業ディレクトリから指定したディレクトリに移動するには、特権 EXEC モードで ***cd*** コマンドを使用します。

cd [**disk0: | disk1: | flash:**] [*path*]

シンタックスの説明

disk0:	内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	取り外し可能な外部フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
flash:	内蔵フラッシュ メモリを指定し、続けてコロン(:)を入力します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。
path	（オプション）移動先ディレクトリの絶対パスです。

デフォルト

ディレクトリを指定しない場合、ルート ディレクトリに移動します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、「config」ディレクトリに移動する方法を示します。

```
hostname# cd flash:/config/
```

関連コマンド

コマンド	説明
pwd	現在の作業ディレクトリを表示します。

certificate

指定した証明書を追加するには、暗号 CA 証明書チェーン モードで **certificate** コマンドを使用します。このコマンドを使用する場合、セキュリティ アプライアンスは、コマンドに含まれているデータを 16 進形式の証明書として解釈します。**quit** 文字列は証明書の終わりを示します。

証明書を削除するには、このコマンドの **no** 形式を使用します。

certificate [***ca*** | ***ra-encrypt*** | ***ra-sign*** | ***ra-general***] *certificate-serial-number*

no certificate *certificate-serial-number*

シンタックスの説明

certificate-serial-number	quit で終わる 16 進形式の証明書のシリアル番号を指定します。
ca	証明書が certificate authority（CA; 認証局）発行の証明書であることを示します。
ra-encrypt	証明書が SCEP で使用される registration authority（RA; 登録局）の鍵暗号化証明書であることを示します。
ra-general	証明書が SCEP メッセージのデジタル署名および鍵暗号化に使用される登録局（RA）の証明書であることを示します。
ra-sign	証明書が SCEP メッセージで使用される登録局（RA）のデジタル署名証明書であることを示します。

デフォルト

このコマンドにデフォルト値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
証明書チェーン コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

認証局（CA）は、ネットワークにおいてセキュリティ クレデンシャルおよびメッセージ暗号化用の公開キーを発行、管理する組織です。公開キー インフラストラクチャの一部として、CA では登録局（RA）と共に、デジタル証明書の要求者から提供された情報を確認するためにチェックを行います。RA で要求者の情報が確認されると、CA は証明書を発行します。

例

次の例では、central という名前のトラストポイントの CA トラストポイント モードに入り、次に central の暗号 CA 証明書チェーン モードに入り、シリアル番号 29573D5FF010FE25B45 の CA を追加します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crypto ca certificate chain central
hostname(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
  0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
  16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
  0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
  6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
  6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
  301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
  30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
  03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
  3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
  73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
  732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
  01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
  181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
  1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
  04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
  14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
  3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
  2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
  63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
  72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
  312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
  0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
  DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
  BEA3C1FE 5EE2AB6D 91
  quit
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
crypto ca certificate chain	証明書暗号 CA 証明書チェーン モードに入ります。
crypto ca trustpoint	CA トラストポイント モードに入ります。
show running-config crypto map	すべての暗号マップのすべてのコンフィギュレーションを表示します。

chain

証明書チェーンの送信をイネーブルにするには、トンネル グループ ipsec アトリビュート コンフィギュレーション モードで **chain** コマンドを使用します。この操作には、ルート証明書および伝送のすべての下位 CA 証明書が含まれます。このコマンドをデフォルトに戻すには、このコマンドの ***no*** 形式を使用します。

chain

no chain

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、すべての IPSec トンネル グループ タイプに適用できます。

例

次の例では、トンネル グループ ipsec アトリビュート コンフィギュレーション モードに入り、ルート証明書およびすべての下位 CA 証明書を含む IP アドレス 209.165.200.225 の IPSec LAN-to-LAN トンネル グループのチェーンの送信をイネーブルにします。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# chain
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

changeto

セキュリティ コンテキストとシステムの間で切り替えを行うには、特権 EXEC モードで **changeto** コマンドを使用します。

changeto {**system** | **context** *name*}

シンタックスの説明

***context** name*	指定した名前を持つコンテキストに変更します。
system	システム実行スペースに変更します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

システム実行スペースまたは管理コンテキストにログインする場合は、各コンテキスト内でコンテキスト、実行コンフィギュレーション、モニタリング タスクを切り替えることができます。コンフィギュレーション モードで編集、あるいは **copy** または **write** コマンドで使用される「実行」コンフィギュレーションは、どの実行スペースにいるかによって異なります。システム実行スペースにいる場合、実行コンフィギュレーションはシステム コンフィギュレーションだけで構成されます。コンテキスト実行スペースにいる場合、実行コンフィギュレーションはそのコンテキストだけで構成されます。たとえば、**show running-config** コマンドを入力することで、実行コンフィギュレーションをすべて（システムとすべてのコンテキスト）表示することはできません。現在のコンフィギュレーションだけが表示されます。

例

次の例では、特権 EXEC モードでコンテキストとシステム間の切り替えを行います。

```
hostname/admin# changeto system
hostname# changeto context customerA
hostname/customerA#
```

次の例では、インターフェイス コンフィギュレーション モードでシステムと管理コンテキスト間の切り替えを行います。実行スペース間で切り替えを行い、コンフィギュレーション サブモードにいる場合、モードは新しい実行スペースでグローバル コンフィギュレーション モードに変わります。

```
hostname(config-if)# changeto context admin
hostname/admin(config)#
```

関連コマンド

コマンド	説明
admin-context	コンテキストを管理コンテキストに設定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

character-encoding

WebVPN ポータル ページでのグローバルな文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **character-encoding** コマンドを使用します。**no** 形式は、character-encoding アトリビュートの値を削除します。

character-encoding *charset*

no character-encoding [*charset***]**

シンタックスの説明

charset	最大 40 文字から成る文字列で、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。上記のページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 この文字列は、大文字と小文字が区別されません。コマンド インタプリタは、セキュリティ アプライアンス コンフィギュレーションで、大文字を小文字に変換します。

デフォルト

デフォルトの動作や値はありません。このアトリビュートに値がない場合、リモート ブラウザに設定された符号化タイプによって WebVPN ポータル ページの文字セットが決定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

文字エンコーディング（「文字コーディング」または「文字セット」ともいいます）は、未加工のデータ（0 と 1 からなるデータなど）と、そのデータを表す文字をペアにする方式です。使用する文字エンコーディング方式は、言語によって決まります。1 つの方式を使用する言語も、そうではない言語もあります。通常、ブラウザによって使用されるデフォルトのエンコーディング方式は、地理的な地域によって決まりますが、ユーザはそれを変更できます。ブラウザは、ページで指定さ

れているエンコーディングを検出し、それに応じて文書を表示することもできます。
character-encoding アトリビュートを使用すると、WebVPN ポータル ページ上に文字エンコーディング方式の値を指定し、ユーザがブラウザを使用している地域やブラウザに行った変更にかかわらず、ページがブラウザで適切に表示されるようにできます。

character-encoding アトリビュートは、デフォルトでは、すべての WebVPN ポータル ページに継承されるグローバルな設定です。ただし、character-encoding アトリビュートの値と異なる文字エンコーディングを使用する Common Internet File System サーバの file-encoding アトリビュートを上書きすることはできます。異なる文字エンコーディングを必要とする CIFS サーバ用に対して、異なる file-encoding 値を使用できます。

CIFS サーバから WebVPN ユーザにダウンロードされた WebVPN ポータル ページは、サーバを識別する WebVPN file-encoding アトリビュートの値を符号化します。符号化が行われなかった場合は、character-encoding アトリビュートの値を継承します。リモート ユーザのブラウザは、この値を文字エンコーディング セットのエントリにマッピングして、使用する適切な文字セットを決定します。WebVPN コンフィギュレーションで CIFS サーバ用の file-encoding エントリが指定されてなく、character-encoding アトリビュートも設定されていない場合、WebVPN ポータル ページは値を指定しません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自身のデフォルト エンコーディングを使用します。

CIFS サーバに適切な文字エンコーディングを、広域的には webvpn character-encoding アトリビュートによって、個別的には file-encoding の上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを適切にレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

（注） character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。日本語 Shift_JIS 文字エンコーディングを使用している場合、フォント ファミリを入れ替えるには、次の例で示すように webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してこれらの値の設定を含めるか、webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォント ファミリを削除する必要があります。

例

次の例では、日本語 Shift_JIS 文字をサポートするように character-encoding アトリビュートを設定し、フォント ファミリを削除し、デフォルトの背景色を保持しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# character-encoding shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

関連コマンド

コマンド	説明
file-encoding	このアトリビュートの値を上書きするために、CIFS サーバと、関連付ける文字エンコーディングを指定します。
show running-config [all] webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルトのコンフィギュレーションを含めるには、**all** キーワードを使用します。
debug webvpn cifs	CIFS についてのデバッグ メッセージを表示します。

checkheaps

チェックヒープ確認の間隔を設定するには、グローバル コンフィギュレーション モードで **checkheaps** コマンドを使用します。値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。チェックヒープは、ピープ メモリ バッファ（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられる）の健全性およびコード領域の完全性を確認する定期的なプロセスです。

checkheaps {check-interval | validate-checksum} *seconds*

no checkheaps {check-interval | validate-checksum} [*seconds*]

シンタックスの説明

check-interval	バッファ確認の間隔を設定します。バッファ確認のプロセスはヒープ（割り当てられ、解放されたメモリ バッファ）の健全性を確認します。プロセスをそれぞれ呼び出している間、セキュリティ アプライアンスは各メモリ バッファを確認し、ヒープ全体をチェックします。不一致がある場合、セキュリティ アプライアンスは「allocated buffer error」または「free buffer error」を発行します。エラーがある場合、セキュリティ アプライアンスは可能であればトレースバック情報をダンプし、リロードします。
validate-checksum	コード スペース チェックサム確認の間隔を設定します。セキュリティ アプライアンスは、最初の起動時にコード全体のハッシュを計算します。その後、定期チェックの間に、セキュリティ アプライアンスは新しいハッシュを生成し、最初のハッシュと比較します。ミスマッチがある場合、セキュリティ アプライアンスは「text checksum checkheaps error」を発行します。エラーがある場合、セキュリティ アプライアンスは可能であればトレースバック情報をダンプし、リロードします。
seconds	1 ～ 2,147,483 の間隔を秒単位で指定します。

デフォルト

デフォルトの間隔はそれぞれ 60 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、バッファ割り当ての間隔を 200 秒に設定し、コード スペース チェックサムの間隔を 500 秒に設定します。

```
hostname(config)# checkheaps check-interval 200
hostname(config)# checkheaps validate-checksum 500
```

関連コマンド

コマンド	説明
show checkheaps	チェックヒープ統計情報を表示します。

check-retransmission

TCP 再送信スタイルの攻撃を防止するには、tcp マップ コンフィギュレーション モードで **check-retransmission** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

check-retransmission

no check-retransmission

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトはディセーブルです。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　**tcp-map** コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP 検査をカスタマイズします。**policy-map** コマンドを使用して新しい TCP マップを適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。矛盾する再送信のエンド システムの解釈によって発生する TCP 再送信スタイルの攻撃を防止するには、tcp マップ コンフィギュレーション モードで **check-retransmission** コマンドを使用します。

セキュリティ アプライアンスは、再送信内のデータが元のデータと同じであるかどうかを確認しようとします。データが一致しない場合、接続はセキュリティ アプライアンスによってドロップされます。この機能がイネーブルの場合、TCP 接続上のパケットは、順番に許可されます。詳細については、**queue-limit** コマンドを参照してください。

例

次の例では、すべての TCP フロー上で、TCP check-retransmission 機能をイネーブルにします。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# check-retransmission
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map**、**class**、および **description** コマンドのシンタックス ヘルプを表示します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

checksum-verification

TCP チェックサムの確認をイネーブルまたはディセーブルにするには、tcp マップ コンフィギュレーション モードで **checksum-verification** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

checksum-verification

no checksum-verification

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

チェックサムの確認は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP 検査をカスタマイズします。**policy-map** コマンドを使用して新しい TCP マップを適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **checksum-verification** コマンドを使用して、TCP チェックサムの確認をイネーブルにします。チェックが失敗した場合、パケットはドロップされます。

例

次の例では、10.0.0.0 ～ 20.0.0.0 の TCP 接続上で TPC チェックサムの確認をイネーブルにします。

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# checksum-verification

hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1

hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap

hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map**、**class**、および **description** コマンドのシンタックス ヘルプを表示します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

class

セキュリティ コンテキストを割り当てるリソース クラスを作成するには、グローバル コンフィギュレーション モードで **class** コマンドを使用します。クラスを削除するには、このコマンドの **no** 形式を使用します。

class *name*

no class *name*

シンタックスの説明

name	クラスの名前を 20 文字までの文字列で指定します。デフォルト クラスの制限を設定する場合は、**default** という名前を入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、コンテキストごとの上限値が適用されていない限り、すべてのセキュリティ コンテキストがセキュリティ アプライアンスのリソースに無制限にアクセスできます。ただし、1 つまたは複数のコンテキストがリソースを大量に消費しているために、他のコンテキストで接続が拒否されていることが分かった場合などは、リソース管理を設定することによって、リソースの使用をコンテキストごとに制限できます。

セキュリティ アプライアンスでは、コンテキストをリソース クラスに割り当てることでリソースを管理します。各コンテキストは、クラスによって設定されるリソース制限値を使用します。

クラスを作成すると、セキュリティ アプライアンスによって、そのクラスに割り当てるそれぞれのコンテキスト分のリソースを確保するのではなく、使用できるリソースの上限が設定されます。リソースをオーバーサブスクライブした場合や、一部のリソースを無制限に許可した場合は、いくつかのコンテキストがそれらのリソースを使い果たして、他のコンテキストへのサービスに影響を及ぼす可能性があります。クラス用のリソースの制限を設定する方法については、**limit-resource** コマンドを参照してください。

すべてのコンテキストは、別のクラスに割り当てられていない場合、デフォルト クラスに属します。コンテキストをデフォルト クラスに割り当てる必要はありません。

コンテキストがデフォルト クラス以外に属している場合は、常にこのクラスの設定でデフォルト クラスの設定が上書きされます。ただし、そのデフォルト以外のクラスに一切の設定がない場合、そのクラスに属すコンテキストはデフォルト クラスの制限を使用します。たとえば、すべての同時接続についてリソースの上限を 2 パーセントとし、他の制限は設定しないでクラスを作成したとします。その他の制限についてはすべてデフォルト クラスから継承します。逆に、すべてのリソースの制限を設定したクラスを作成した場合は、デフォルト クラスの設定は何も使用されません。

デフォルトでは、次に示すコンテキストあたりの上限を除き、デフォルト クラスの全コンテキストからアクセスできるリソースに制限はありません。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

例

次の例では、conns に関するデフォルト クラスの制限値を、無制限から 10% に設定し直しています。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

他のリソースは、すべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

関連コマンド

コマンド	説明
clear configure class	クラス コンフィギュレーションを消去します。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスに対してリソース制限を設定します。
member	リソース クラスにコンテキストを割り当てます。
show class	クラスに割り当てられているコンテキストを表示します。

class（ポリシー マップ）

クラス マップのトラフィックに対するアクションを特定するポリシー マップにクラス マップを割り当てるには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。ポリシー マップからクラス マップを削除するには、このコマンドの **no** 形式を使用します。

class *classmap-name*

no class *classmap-name*

シンタックスの説明

classmap-name	クラス マップの名前を指定します。レイヤ 3/4 ポリシー マップ（**policy-map** コマンドを使用）の場合は、レイヤ 3/4 クラス マップの名前（**class-map** コマンドか **class-map type management** コマンドを使用）を指定する必要があります。検査ポリシー マップ（**policy-map type inspect** コマンドを使用）の場合は、検査クラス マップの名前（**class-map type inspect** コマンドを使用）を指定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

コンフィギュレーションは、すべてのトラフィックに一致する「class-default」というクラス マップを必ず含んでいます。どのレイヤ 3/4 ポリシー マップの末尾でも、アクションが何も定義されていない class-default クラス マップがコンフィギュレーションに含まれています。このマップは内部でのみ使用され、修正することはできません。

1 つのポリシー マップで、class-default を含め、**class** コマンドと **match** コマンドを 63 個まで設定できます。

class コマンドでポリシー マップにクラス マップを追加したなら、トラフィックへのアクション（複数可）を定義します。レイヤ 3/4 ポリシー マップのクラス コンフィギュレーション モードでサポートされている機能は、次のとおりです。

- TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化
- CSC
- アプリケーション検査
- IPS
- QoS ポリシング

- QoS プライオリティ キュー

検査ポリシー マップのクラス コンフィギュレーション モードでサポートされている機能は、次のとおりです。

- パケットのドロップ
- 接続のドロップ
- 接続のリセット
- ロギング
- メッセージのレートの制限
- コンテンツのマスク

例

次に、**class** コマンドを含む、接続ポリシーの **policy-map** コマンドの例を示します。ここでは、Web サーバ 10.1.1.1 にアクセスできる接続の数を制限しています。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次の例では、ポリシー マップで複数一致がどのように機能するかを示しています。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例では、使用可能な最初のクラス マップにトラフィックが一致し、同じ機能ドメインのアクションを指定している以降のどのクラス マップにも一致しない様子を示しています。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続を開始すると、**class telnet_traffic** が照合されます。同様に、FTP 接続を開始すると、**class ftp_traffic** が照合されます。Telnet と FTP 以外の TCP 接続では、**class tcp_traffic** が照合されます。Telnet 接続や FTP 接続を **class tcp_traffic** と照合できますが、すでに他のクラスと照合されているので、セキュリティ アプライアンスはこれらの接続を照合しません。

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
class-map type management	管理トラフィック用のレイヤ 3/4 クラス マップを作成します。
clear configure policy-map	service-policy コマンドで使用されているポリシー マップを除く、すべてのポリシー マップ コンフィギュレーションを削除します。
match	トラフィックの照合用パラメータを定義します。
policy-map	ポリシー（それぞれ 1 つまたは複数のアクションがある 1 つまたは複数のトラフィック クラスのアソシエーション）を設定します。

class-map

モジュラ ポリシー フレームワークを使用しているときに、アクションを適用するレイヤ 3 または 4 トラフィックを特定するには、グローバル コンフィギュレーション モードで **class-map** コマンドを **type** キーワードなしで使用します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map *class_map_name*

no class-map *class_map_name*

シンタックスの説明

class_map_name	最大 40 文字のクラス マップ名を指定します。「class-default」という名前と、「_internal」または「_default」で始まる名前は予約されています。すべてのタイプのクラス マップが同じネーム スペースを使用しているため、他のタイプのクラス マップですでに使用されている名前は再使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このタイプのクラス マップは、レイヤ 3/4 の通過トラフィック専用です。セキュリティ アプライアンス宛ての管理トラフィックのクラス マップについては、**class-map type management** コマンドを参照してください。

コンフィギュレーションは、すべてのトラフィックに一致する「class-default」というクラス マップを必ず含んでいます。どのレイヤ 3/4 ポリシー マップの末尾でも、アクションが何も定義されていない class-default クラス マップがコンフィギュレーションに含まれています。このマップは内部でのみ使用され、修正することはできません。

レイヤ 3/4 クラス マップでは、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。すべてのタイプのクラス マップの最大数は、シングルモードでは 255 個、マルチモードではコンテキストごとに 255 個です。このコンフィギュレーションは、セキュリティ アプライアンスがデフォルト グローバル ポリシーで使用するデフォルトのレイヤ 3/4 クラス マップを含みます。このクラス マップは **inspection_default** といい、デフォルトの検査トラフィックを照合します。

```
class-map inspection_default
 match default-inspection-traffic
```

各レイヤ 3/4 ポリシー マップに複数のレイヤ 3/4 クラス マップを作成できます。

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。
2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのための特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスに対するアクションを有効にします。

class-map コマンドを使用して、クラス マップ コンフィギュレーション モードに入ります。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。レイヤ 3/4 クラス マップには、**match tunnel-group** コマンドと **match default-inspection-traffic** コマンド以外に、クラス マップに含まれるトラフィックを特定する **match** コマンドを 1 つだけ指定できます。

例

次の例では、レイヤ 3/4 クラス マップを 4 つ作成します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server
10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

関連コマンド

コマンド	説明
class-map type management	セキュリティ アプライアンスに対するトラフィックのクラス マップを作成します。
policy-map	トラフィック クラスを 1 つまたは複数のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
service-policy	ポリシー マップを 1 つまたは複数のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type inspect

モジュラ ポリシー フレームワークの使用時に、検査アプリケーションに固有の照合基準を作成するには、グローバル コンフィギュレーション モードで **class-map type inspect** コマンドを使用します。検査のクラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type inspect *application* [**match-all]** *class_map_name*

no class-map [**type inspect** *application* [**match-all**]] *class_map_name*

シンタックスの説明

application	照合するアプリケーション トラフィックのタイプを指定します。指定できるタイプは、次のとおりです。 • **dns** • **ftp** • **h323** • **http** • **im** • **sip**
class_map_name	最大 40 文字のクラス マップ名を指定します。「class-default」という名前と、「_internal」または「_default」で始まる名前は予約されています。すべてのタイプのクラス マップが同じネーム スペースを使用しているため、他のタイプのクラス マップですでに使用されている名前は再使用できません。
match-all	（オプション）トラフィックがクラス マップと一致するには、すべての基準を満たす必要があることを指定します。**match-all** がデフォルトで、他にオプションはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを利用すると、数多くのアプリケーション検査のための特別なアクションを設定できます。レイヤ 3/4 ポリシー マップで検査エンジンをイネーブルにする場合は、*inspection policy map* で定義するアクションをイネーブルにすることもできます（**policy-map type inspect** コマンドを参照）。

検査ポリシー マップを設定するときに、検査クラス マップを作成することにより、処理の対象になるトラフィックを特定できます。クラス マップには、1 つまたは複数の **match** コマンドを含めます（1 つの検査ポリシー マップとアクションを対にする場合は、検査ポリシー マップ内で直接 **match** コマンドを使用します）。アプリケーションに固有の照合基準を指定できます。たとえば、DNS トラフィックでは、DNS クエリーのドメイン名を照合できます。

クラス マップは、トラフィックの複数の照合基準をグループにまとめたものです。トラフィックがクラス マップと一致するには、すべての **match** コマンドで指定した基準と一致しなければなりません。クラス マップを作成する場合と、検査ポリシー マップで直接トラフィックの照合を定義する場合の違いは、クラス マップでは複数の照合基準をグループにまとめられることと、クラス マップを再利用できることです。このクラス マップで特定されるトラフィックには、検査ポリシー マップで指定されている接続のドロップ、リセット、ログの記録などのアクションを指定できます。

例

次の例では、HTTP の検査クラス マップを作成します。

```
hostname(config)# class-map type inspect http match-all test
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request args regex regex1
```

関連コマンド

コマンド	説明
class-map	通過トラフィックのためのレイヤ 3/4 クラス マップを作成します。
policy-map	トラフィック クラスを 1 つまたは複数のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
service-policy	ポリシー マップを 1 つまたは複数のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type management

モジュラ ポリシー フレームワークを使用しているときに、セキュリティ アプライアンス宛てのレイヤ 3 または 4 のどの管理トラフィックにアクションを適用するかを指定するには、グローバル コンフィギュレーション モードで **class-map type management** コマンドを使用します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type management *class_map_name*

no class-map type management *class_map_name*

シンタックスの説明

class_map_name	最大 40 文字のクラス マップ名を指定します。「class-default」という名前と、「_internal」または「_default」で始まる名前は予約されています。すべてのタイプのクラス マップが同じネーム スペースを使用しているため、他のタイプのクラス マップですでに使用されている名前は再使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このタイプのクラス マップは、管理トラフィック専用です。通過トラフィックについては、**class-map** コマンド（**type** キーワードなし）を参照してください。

セキュリティ アプライアンスに対する管理トラフィックでは、この種類のトラフィック特有の処理が必要な場合があります。ポリシー マップの管理クラス マップに指定できるアクションは、管理トラフィック専用です。たとえば、RADIUS アカウンティング トラフィックを検査できます。

レイヤ 3/4 クラス マップでは、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。すべてのタイプのクラス マップの最大数は、シングルモードでは 255 個、マルチモードではコンテキストごとに 255 個です。

各レイヤ 3/4 ポリシー マップに複数のレイヤ 3/4 クラス マップ（管理トラフィックまたは通過トラフィック）を作成できます。

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。
2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのための特別なアクションを定義します。

3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスに対するアクションを有効にします。

class-map type management コマンドを使用して、クラス マップ コンフィギュレーション モードに入ります。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。TCP ポートまたは UDP ポートだけを照合する管理クラス マップを指定できます。レイヤ 3/4 クラス マップには、クラス マップに含めるトラフィックを特定する **match** コマンドを 1 つだけ指定できます。

例

次の例では、レイヤ 3/4 管理クラス マップを作成します。

```
hostname(config)# class-map type management radius_acct
hostname(config-cmap)# match port tcp eq 10000
```

関連コマンド

コマンド	説明
class-map	通過トラフィックのためのレイヤ 3/4 クラス マップを作成します。
policy-map	トラフィック クラスを 1 つまたは複数のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
service-policy	ポリシー マップを 1 つまたは複数のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type regex

モジュラ ポリシー フレームワークを使用しているときに、照合するテキストの正規表現をグループにまとめるには、グローバル コンフィギュレーション モードで **class-map type regex** コマンドを使用します。正規表現のクラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type regex match-any *class_map_name*

no class-map [**type regex match-any**] *class_map_name*

シンタックスの説明

class_map_name	最大 40 文字のクラス マップ名を指定します。「class-default」という名前と、「_internal」または「_default」で始まる名前は予約されています。すべてのタイプのクラス マップが同じネーム スペースを使用しているため、他のタイプのクラス マップですでに使用されている名前は再使用できません。
match-any	トラフィックが正規表現のいずれか 1 つにでも一致すると、クラス マップと一致したと見なすことを指定します。**match-any** が唯一のオプションです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを利用すると、数多くのアプリケーション検査のための特別なアクションを設定できます。レイヤ 3/4 ポリシー マップで検査エンジンをイネーブルにする場合は、*inspection policy map* で定義するアクションをイネーブルにすることもできます（**policy-map type inspect** コマンドを参照）。

検査ポリシー マップでは、1 つ以上の **match** コマンドを含んだ検査クラス マップを作成することで、アクションの実行対象となるトラフィックを指定できます。または、**match** コマンドを検査ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケットに含まれているテキストを正規表現を使用して識別できます。たとえば、HTTP パケットに含まれている URL 文字列と一致するかどうかを確認できます。正規表現は、正規表現クラス マップ内にグループにまとめます。

正規表現のクラス マップを作成する前に、**regex** コマンドを使用して正規表現を作成します。次に、クラス マップ コンフィギュレーション モードで **match regex** コマンドを使用して、指定の正規表現を特定します。

例

次の例では、正規表現を 2 つ作成し、1 つの正規表現クラス マップに追加します。トラフィックに「example.com」か「example2.com」という文字列が含まれていると、このトラフィックはクラス マップと一致します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックに一致するかどうかを調べるための検査クラス マップを作成します。
policy-map	トラフィック クラスを 1 つまたは複数のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
service-policy	ポリシー マップを 1 つまたは複数のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
regex	正規表現を作成します。

clear aaa local user fail-attempts

ユーザのロックアウト ステータスを変更せずに、失敗したユーザ認証試行の回数を 0 にリセットするには、特権 EXEC モードで **clear aaa local user fail-attempts** コマンドを使用します。

clear aaa local user authentication fail-attempts {**username** *name* | **all**}

シンタックスの説明

all	すべてのユーザの失敗試行カウンタを 0 にリセットします。
name	失敗試行カウンタが 0 にリセットされる特定のユーザ名を指定します。
username	後続のパラメータが、失敗試行カウンタが 0 にリセットされるユーザ名であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ユーザが数回認証に失敗した場合は、このコマンドを使用します。ただし、たとえば、コンフィギュレーションが最近変更された場合などは、カウンタを 0 にリセットします。

認証試行の失敗が設定された回数を超えると、ユーザはシステムからロックアウトされ、システム管理者がユーザ名をアンロックするか、システムをリブートするまで正常にログインできません。

ユーザが正常に認証された場合、またはセキュリティ アプライアンスがリブートした場合は、失敗試行回数が 0 にリセットされ、ロックアウト ステータスが No にリセットされます。

ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

特権レベル 15 のシステム管理者は、ロックアウトされません。

例

次の例では、**clear aaa local user authentication fail-attempts** コマンドを使用して、ユーザ名 anyuser の失敗試行カウンタを 0 にリセットする方法を示します。

```
hostname(config)# clear aaa local user authentication fail-attempts username anyuser
hostname(config)#
```

次の例では、**clear aaa local user authentication fail-attempts** コマンドを使用して、すべてのユーザの失敗試行カウンタを 0 にリセットする方法を示します。

```
hostname(config)# clear aaa local user authentication fail-attempts all
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	ユーザ認証試行の失敗が許可される回数の制限を設定します。
clear aaa local user lockout	ユーザのロックアウト ステータスを変更せずに、失敗したユーザ認証試行の回数を 0 にリセットします。
show aaa local user [locked]	現在ロックされているユーザ名のリストを表示します。

clear aaa local user lockout

指定したユーザのロックアウト ステータスを消去し、失敗試行カウンタを 0 にリセットするには、特権 EXEC モードで **clear aaa local user lockout** コマンドを使用します。

clear aaa local user lockout {**username** *name* | **all**}

シンタックスの説明

all	すべてのユーザの失敗試行カウンタを 0 にリセットします。
name	失敗試行カウンタが 0 にリセットされる特定のユーザ名を指定します。
username	後続のパラメータが、失敗試行カウンタが 0 にリセットされるユーザ名であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

username オプションを使用してユーザを 1 人だけ指定することも、***all*** オプションを使用してすべてのユーザを指定することもできます。

このコマンドは、ロックアウトされているユーザのステータスだけに影響を及ぼします。

管理者は、デバイスからロックアウトされません。

ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

例

次の例では、**clear aaa local user lockout** コマンドを使用してロックアウト状態を消去し、ユーザ名 anyuser の失敗試行カウンタを 0 にリセットする方法を示します。

```
hostname(config)# clear aaa local user lockout username anyuser
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	ユーザ認証試行の失敗が許可される回数の制限を設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更せずに、失敗したユーザ認証試行の回数を 0 にリセットします。
show aaa local user [locked]	現在ロックされているユーザ名のリストを表示します。

clear aaa-server statistics

AAA サーバの統計情報をリセットするには、特権 EXEC モードで **clear aaa-server statistics** コマンドを使用します。

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

シンタックスの説明

LOCAL	（オプション）LOCAL ユーザ データベースの統計情報を消去します。
groupname	（オプション）グループ内のサーバの統計情報を消去します。
host *hostname*	（オプション）グループ内の特定のサーバの統計情報を消去します。
protocol *protocol*	（オプション）次の特定のプロトコルのサーバの統計情報を消去します。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

すべてのグループのすべての AAA サーバ統計情報を削除します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。プロトコルの値の ***nt-domain*** が ***nt*** に、***rsa-ace*** が ***sdi*** に置き換えられました。

例

次のコマンドは、グループ内の特定のサーバの AAA 統計情報をリセットする方法を示しています。

```
hostname(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

次のコマンドは、1 つのサーバ グループ全体の AAA 統計情報をリセットする方法を示しています。

```
hostname(config)# clear aaa-server statistics svrgrp1
```

次のコマンドは、すべてのサーバ グループの AAA 統計情報をリセットする方法を示しています。

```
hostname(config)# clear aaa-server statistics
```

次のコマンドは、特定のプロトコル（この場合は TACACS+）の AAA 統計情報をリセットする方法を示しています。

```
hostname(config)# clear aaa-server statistics protocol tacacs+
```

関連コマンド

コマンド	説明
aaa-server protocol	AAA サーバ接続データのグループ化を指定および管理します。
clear configure aaa-server	デフォルト以外のすべての aaa サーバ グループを削除、または指定したグループを消去します。
show aaa-server	AAA サーバの統計情報を表示します。
show running-config aaa-server	現在の AAA サーバのコンフィギュレーション値を表示します。

clear access-group

すべてのインターフェイスからアクセス グループを削除するには、**clear access-group** コマンドを使用します。

clear access-group

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例　次の例では、すべてのアクセス グループを削除する方法を示します。

```
hostname(config)# clear access-group
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
show running-config access-group	現在のアクセス グループ コンフィギュレーションを表示します。

clear access-list

アクセス リスト カウンタを消去するには、グローバル コンフィギュレーション モードで **clear access-list** コマンドを使用します。

clear access-list [*id*] **counters**

シンタックスの説明

counters	アクセス リスト カウンタを消去します。
id	（オプション）アクセス リストの名前または番号。

デフォルト

すべてのアクセス リスト カウンタが消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear access-list コマンドを入力するときに *id* を指定しないと、すべてのアクセス リスト カウンタが消去されます。

例

次の例では、特定のアクセス リスト カウンタを消去する方法を示します。

```
hostname# clear access-list inbound counters
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list standard	アクセス リストを追加して、OSPF 再配布のルートマップに使用できる、OSPF ルートの宛先 IP アドレスを指定します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show access-list	アクセス リストのエントリを番号別に表示します。
show running-config access-list	セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示します。

clear arp

ダイナミック ARP エントリまたは ARP 統計情報を消去するには、特権 EXEC モードで **clear arp** コマンドを使用します。

clear arp [**statistics**]

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、ARP 統計情報をすべて消去します。

```
hostname# clear arp statistics
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear asp drop

アクセラレーション セキュリティ パスのドロップ統計情報を消去するには、特権 EXEC モードで **clear asp drop** コマンドを使用します。

clear asp drop [**flow** *type* | **frame** *type*]

シンタックスの説明

flow	（オプション）ドロップされたフロー統計情報を消去します。
frame	（オプション）ドロップされたパケット統計情報を消去します。
type	（オプション）特定のプロセスのドロップされたフローまたはパケットの統計情報を消去します。タイプのリストについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトでは、このコマンドはすべてのドロップ統計情報を消去します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　プロセス タイプには、次のものがあります。

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

例　次の例では、ドロップ統計情報をすべて消去します。

```
hostname# clear asp drop
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットのアクセラレーション セキュリティ パス カウンタを表示します。

clear blocks

最低水準点や履歴情報などのパケット バッファ カウンタをリセットするには、特権 EXEC モードで **clear blocks** コマンドを使用します。

clear blocks

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

最低水準点カウンタを各プール内で現在使用可能なブロックにリセットします。また、前回のバッファ割り当ての失敗時に保存された履歴情報も消去します。

例

次の例では、ブロックを消去します。

```
hostname# clear blocks
```

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられているメモリを増やします。
show blocks	システム バッファの使用状況を表示します。

clear-button

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示される WebVPN ページ ログイン ボックスの Clear ボタンをカスタマイズするには、webvpn カスタマイゼーション モードで **clear-button** コマンドを使用します。

clear-button {**text** | **style**} *value*

[**no**] **clear-button** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのテキストは「Clear」です。

デフォルトのスタイルは border:1px solid black;background-color:white;font-weight:bold;font-size:80% です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

(注)　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、Clear ボタンのデフォルトの背景色を黒から青に変更しています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# clear-button style background-color:blue
```

関連コマンド

コマンド	説明
login-button	WebVPN ページ Login ボックスのログイン ボタンをカスタマイズします。
login-title	WebVPN ページ Login ボックスのタイトルをカスタマイズします。
group-prompt	WebVPN ページ Login ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページ Login ボックスのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページ Login ボックスのユーザ名プロンプトをカスタマイズします。

clear capture

キャプチャ バッファを消去するには、**clear capture** *capture_name* コマンドを使用します。

clear capture *capture_name*

シンタックスの説明

capture_name	パケット キャプチャの名前。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドがサポートされるようになりました。

使用上のガイドライン

誤ってすべてのパケット キャプチャを消去することがないように、**clear capture** の短縮形（**cl cap** や **clear cap** など）はサポートされていません。

例

次の例では、キャプチャ バッファ「trudy」のキャプチャ バッファを消去する方法を示します。

```
hostname(config)# clear capture trudy
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能を有効にして、パケットのスニッフィングやネットワーク障害を検出できるようにします。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。

clear compression

すべての SVC および WebVPN 接続についての圧縮統計情報を消去するには、特権 EXEC モードで **clear compression** コマンドを使用します。

clear compression {**all** | **svc** | **http-comp**}

デフォルト

このコマンドには、デフォルトの動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次の例では、ユーザは圧縮コンフィギュレーションを消去します。

```
hostname#(config) clear configure compression
```

関連コマンド

コマンド	説明
compression	すべての SVC および WebVPN 接続の圧縮をイネーブルにします。
svc compression	SVC 接続上のデータの圧縮を特定のグループまたはユーザに対してイネーブルにします。

clear configure コマンド～ clear configure zonelabs-integrity コマンド

clear configure

実行コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure** コマンドを使用します。

clear configure {***primary*** | ***secondary*** | ***all*** | *command*}

シンタックスの説明

command	指定したコマンドのコンフィギュレーションを消去します。詳細については、このマニュアルの各 **clear configure** *command* コマンドの個々のエントリを参照してください。
primary	次のコマンドを含む、接続性に関連するコマンドを消去します。 • **tftp-server** • **shun** • **route** • **ip address** • **mtu** • **failover** • **monitor-interface** • **boot**
secondary	（***primary*** キーワードを使用して消去される）接続に関連するコマンド以外のコマンドを消去します。
all	実行コンフィギュレーション全体を消去します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　このコマンドをセキュリティ コンテキストで入力する場合は、コンテキスト コンフィギュレーションだけが消去されます。このコマンドをシステム実行スペースで入力する場合は、すべてのコンテキスト実行コンフィギュレーションに加えてシステム実行コンフィギュレーションも消去されます。システム コンフィギュレーション内のすべてのコンテキスト エントリが消去されるため（**context** コマンドを参照）、コンテキストは実行されず、コンテキスト実行スペースに移動できなくなります。

コンフィギュレーションを消去する前に、（スタートアップ コンフィギュレーションの場所を指定する）**boot config** コマンドへのすべての変更をスタートアップ コンフィギュレーションに保存します。スタートアップ コンフィギュレーションの場所を実行コンフィギュレーション内だけで変更した場合は、再起動時にコンフィギュレーションはデフォルト位置からロードされます。

例　次の例では、実行コンフィギュレーション全体を消去します。

```
hostname(config)# clear configure all
```

関連コマンド

コマンド	説明
configure http	指定した HTTP(S) URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure factory-default	CLI で入力するコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

clear configure aaa

aaa コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure aaa** コマンドを使用します。**clear configure aaa** コマンドは、コンフィギュレーションから AAA コマンド文を削除します。

clear configure aaa

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	CLI 内の一貫性のために、このコマンドが修正されました。

使用上のガイドライン

また、このコマンドは、AAA パラメータが存在する場合リセットしてデフォルト値にします。

元に戻すことはできません。

例

```
hostname(config)# clear configure aaa
```

関連コマンド

コマンド	説明
aaa accounting	ユーザがアクセスしたネットワーク サービスのレコードの保持をイネーブル化、ディセーブル化、または表示します。
aaa authentication	**aaa-server** コマンドで指定されたサーバ上での、LOCAL、TACACS+、または RADIUS のユーザ認証、または ASDM ユーザ認証をイネーブル化または表示します。
aaa authorization	**aaa-server** コマンドで指定した LOCAL または TACACS+ サーバのユーザ認可、あるいは ASDM ユーザ認証のユーザ認可をイネーブルまたはディセーブルにします。
show running-config aaa	AAA コンフィギュレーションを表示します。

clear configure aaa-server

すべての AAA サーバ グループを削除、または指定したグループを消去するには、グローバル コンフィギュレーション モードで **clear configure aaa-server** コマンドを使用します。

clear configure aaa-server [*server-tag*]

clear configure aaa-server [*server-tag*] **host** *server-ip*

シンタックスの説明

server-ip	AAA サーバの IP アドレス。
server-tag	（オプション）消去するサーバ グループの識別名。

デフォルト

すべての AAA サーバ グループを削除します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

特定の AAA サーバ グループ、またはデフォルトで、すべての AAA サーバ グループを指定できます。

サーバ グループ内の特定のサーバを指定するには、***host*** キーワードを使用します。

また、このコマンドは、AAA サーバ パラメータが存在する場合リセットしてデフォルト値にします。

例

```
hostname(config)# aaa-server svrgrp1 protocol sdi
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# sdi-version sdi-5
hostname(config-aaa-server)# exit
```

上記のコンフィギュレーションで、次のコマンドは、グループから特定のサーバを削除する方法を示しています。

```
hostname(config)# clear config aaa-server svrgrp1 host 1.2.3.4
```

次のコマンドは、1 つのサーバ グループを削除する方法を示しています。

```
hostname(config)# clear config aaa-server svrgrp1
```

次のコマンドは、すべてのサーバ グループを削除する方法を示しています。

```
hostname(config)# clear config aaa-server
```

関連コマンド

コマンド	説明
aaa-server host	ホスト固有の AAA サーバ接続データを指定および管理します。
aaa-server protocol	すべてのホストに共通する、グループ固有の AAA サーバ パラメータを設定できます。
show running-config aaa	他の AAA コンフィギュレーション値と共に、ユーザ 1 人あたりに許可する同時プロキシ接続の現在の最大数を表示します。

clear configure access-group

すべてのインターフェイスからアクセス グループを削除するには、**clear configure access-group** コマンドを使用します。

clear configure access-group

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

例　次の例では、すべてのアクセス グループを削除する方法を示します。

```
hostname(config)# clear configure access-group
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
show running-config access-group	現在のアクセス グループ コンフィギュレーションを表示します。

clear configure access-list

実行コンフィギュレーションからアクセス リストを消去するには、グローバル コンフィギュレーション モードで **clear configure access-list** コマンドを使用します。

clear configure access-list [*id*]

シンタックスの説明

id	（オプション）アクセス リストの名前または番号。

デフォルト

実行コンフィギュレーションからすべてのアクセス リストが消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear configure access-list コマンドを実行すると、**crypto map** コマンドまたはインターフェイスからアクセス リストが自動的にアンバインドされます。**crypto map** コマンドからアクセス リストをアンバインドすると、パケットがすべて廃棄される状態になる可能性があります。これは、アクセス リストを参照している **crypto map** コマンドが不完全なものになるためです。この状態を解消するには、別の **access-list** コマンドを定義して **crypto map** コマンドを完全なものにするか、**access-list** コマンドに関係する **crypto map** コマンドを削除します。詳細については、**crypto map client** コマンドの項を参照してください。

例

次の例では、実行コンフィギュレーションからアクセス リストを消去する方法を示します。

```
hostname(config)# clear configure access-list
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list standard	アクセス リストを追加して、OSPF 再配布のルートマップに使用できる、OSPF ルートの宛先 IP アドレスを指定します。
clear access-list	アクセス リスト カウンタを消去します。
show access-list	アクセス リストのカウンタを表示します。
show running-config access-list	セキュリティ アプライアンスで実行されているアクセス リスト コンフィギュレーションを表示します。

clear configure alias

コンフィギュレーションからすべての **alias** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure alias** コマンドを使用します。

clear configure alias

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、コンフィギュレーションからすべての **alias** コマンドを削除する方法を示します。

```
hostname(config)# clear configure alias
```

関連コマンド

コマンド	説明
alias	1 つのアドレスを別のアドレスに変換します。
show running-config alias	コンフィギュレーション内の、デュアル NAT コマンドで使用する重複アドレスを表示します。

clear configure arp

arp コマンドで追加したスタティック ARP エントリを消去するには、グローバル コンフィギュレーション モードで **clear configure arp** コマンドを使用します。

clear configure arp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、コンフィギュレーションからスタティック ARP エントリを消去します。

```
hostname# clear configure arp
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
firewall transparent	ファイアウォール モードを透過に設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear configure arp-inspection

ARP 検査のコンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure arp-inspection** コマンドを使用します。

clear configure arp-inspection

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ARP 検査のコンフィギュレーションを消去します。

```
hostname# clear configure arp-inspection
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
firewall transparent	ファイアウォール モードを透過に設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear configure asdm

実行コンフィギュレーションからすべての **asdm** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure asdm** コマンドを使用します。

clear configure asdm [*location* | *group* | *image*]

シンタックスの説明

group	（オプション）実行コンフィギュレーションから **asdm group** コマンドだけを消去します。
image	（オプション）実行コンフィギュレーションから **asdm image** コマンドだけを消去します。
location	（オプション）実行コンフィギュレーションから **asdm location** コマンドだけを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**clear pdm** コマンドが **clear configure asdm** コマンドに変更されました。

使用上のガイドライン

実行コンフィギュレーション内の **asdm** コマンドを表示するには、**show running-config asdm** コマンドを使用します。

コンフィギュレーションから **asdm image** コマンドを消去すると、ASDM アクセスがディセーブルになります。コンフィギュレーションから **asdm location** コマンドおよび **asdm group** コマンドを消去すると、次にアクセスされたときに ASDM によってこれらのコマンドが再生成されますが、アクティブな ASDM セッションが妨げられることがあります。

（注） マルチ コンテキスト モードで実行されているセキュリティ アプライアンスでは、**clear configure asdm image** コマンドはシステム実行スペースでのみ使用できます。一方、**clear configure asdm group** コマンドおよび **clear configure asdm location** コマンドは、ユーザ コンテキストでのみ使用できます。

例

次の例では、実行コンフィギュレーションから **asdm group** コマンドを消去します。

```
hostname(config)# clear configure asdm group
hostname(config)#
```

関連コマンド

コマンド	説明
asdm group	オブジェクト グループ名をインターフェイスに関連付けるために ASDM によって使用されます。
asdm image	ASDM イメージ ファイルを指定します。
asdm location	IP アドレスをインターフェイス アソシエーションに記録するために ASDM によって使用されます。
show running-config asdm	実行コンフィギュレーション内の **asdm** コマンドを表示します。

clear configure auth-prompt

指定済みの認証プロンプト チャレンジ テキストを削除し、デフォルト値に戻すには（存在する場合）、グローバル コンフィギュレーション モードで **clear configure auth-prompt** コマンドを使用します。

clear configure auth-prompt

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI 規格に適合するように、このコマンドが修正されました。

使用上のガイドライン

認証プロンプトを消去した後、ユーザのログイン時に表示されるプロンプトは、使用するプロトコルによって次のように異なります。

- HTTP を使用してログインするユーザの場合、`HTTP Authentication` が表示されます。
- FTP を使用してログインするユーザの場合、`FTP Authentication` が表示されます。
- Telnet を使用してログインするユーザの場合、プロンプトは表示されません。

例

次の例では、認証プロンプトを消去する方法を示します。

```
hostname(config)# clear configure auth-prompt
```

関連コマンド

auth-prompt	ユーザ認可プロンプトを設定します。
show running-config auth-prompt	ユーザ認可プロンプトを表示します。

clear configure banner

すべてのバナーを削除するには、グローバル コンフィギュレーション モードで **clear configure banner** コマンドを使用します。

clear configure banner

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、バナーを消去する方法を示します。

```
hostname(config)# clear configure banner
```

関連コマンド

コマンド	説明
banner	セッション バナー、ログイン バナー、および「今日のお知らせ」バナーを設定します。
show running-config banner	すべてのバナーを表示します。

clear configure ca certificate map

証明書マップ エントリをすべて削除、または指定した証明書マップ エントリを削除するには、グローバル コンフィギュレーション モードで **clear configure ca configurate map** コマンドを使用します。

clear configure ca certificate map [*sequence-number*]

シンタックスの説明

sequence-number	（オプション）削除する証明書マップ規則の番号を指定します。範囲は 1 ～ 65535 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、すべての証明書マップ エントリを削除します。

```
hostname(config)# clear configure ca certificate map
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードに入ります。

clear configure class

リソース クラスのコンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure class** コマンドを使用します。

clear configure class

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、クラス コンフィギュレーションを消去しています。

```
hostname(config)# clear configure class
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスに対してリソース制限を設定します。
member	リソース クラスにコンテキストを割り当てます。
show class	クラスに割り当てられているコンテキストを表示します。

clear configure class-map

すべてのクラス マップを削除するには、グローバル コンフィギュレーション モードで **clear configure class-map** コマンドを使用します。

clear configure class-map [**type** {**management** | **regex** | **inspect** [*protocol*]}

シンタックスの説明

inspect	（オプション）検査クラス マップを消去します。
management	（オプション）管理クラス マップを消去します。
protocol	（オプション）消去するアプリケーション マップのタイプを指定します。指定できるタイプは、次のとおりです。 • **dns** • **ftp** • **h323** • **http** • **im** • **p2p-donkey** • **sip**
regex	（オプション）正規表現クラス マップを消去します。
type	（オプション）消去するクラス マップのタイプを指定します。レイヤ 3/4 クラス マップを消去する場合は、タイプを指定しません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

特定のクラス マップ名のクラス マップを消去するには、**class-map** コマンドの **no** 形式を使用します。

例

次の例では、設定済みのクラス マップをすべて消去する方法を示します。

```
hostname(config)# clear configure class-map
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

clear configure client-update

クライアント アップデートを強制する機能をコンフィギュレーションから削除するには、グローバル コンフィギュレーション モードまたはトンネル グループ ipsec アトリビュート コンフィギュレーション モードで **clear configure client-update** コマンドを使用します。

clear config client-update

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec アトリビュート コンフィギュレーション モードが追加されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションから client-update 機能を削除します。

```
hostname(config)# clear config client-update
hostname(config)#
```

トンネル グループ ipsec アトリビュート コンフィギュレーション モードで入力した次の例では、test という名前のトンネル グループのコンフィギュレーションから client-update 機能を削除します。

```
hostname(config)# tunnel-group test ipsec-attributes
hostname(config-tunnel-ipsec)# clear config client-update
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
client-update	client-update を設定します。
show running-config client-update	現在の client-update コンフィギュレーションを表示します。

clear configure clock

クロック コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure clock** コマンドを使用します。

clear configure clock

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	**clear clock** がこのコマンドに変更されました。

使用上のガイドライン

このコマンドは、すべての **clock** コンフィギュレーション コマンドを消去します。**clock set** コマンドはコンフィギュレーション コマンドではないため、このコマンドではクロックはリセットされません。クロックをリセットするには、**clock set** コマンドに新しい時間を設定する必要があります。

例

次の例では、すべてのクロック コマンドを消去します。

```
hostname# clear configure clock
```

関連コマンド

コマンド	説明
clock set	時間を手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。

clear configure command-alias

デフォルト以外のコマンド エイリアスをすべて削除するには、グローバル コンフィギュレーション モードで ***clear configure command-alias*** コマンドを使用します。

clear configure command-alias

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

次の例では、デフォルト以外のコマンド エイリアスをすべて削除する方法を示します。

```
hostname(config)# clear configure command-alias
```

関連コマンド

コマンド	説明
command-alias	コマンド エイリアスを作成します。
show running-config command-alias	デフォルト以外のコマンド エイリアスをすべて表示します。

clear configure compression

グローバル圧縮コンフィギュレーションをデフォルト（すべての圧縮技術はイネーブル）にリセットするには、グローバル コンフィギュレーション モードで **clear configure compression** コマンドを使用します。

clear configure compression

デフォルト

このコマンドには、デフォルトの動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

例

次の例では、圧縮コンフィギュレーションが消去されます。

```
hostname#(config) clear configure compression
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続、WebVPN 接続、およびポート転送接続に対して圧縮をイネーブルにします。
svc compression	SVC 接続上の http データの圧縮を特定のグループまたはユーザに対してイネーブルにします。

clear configure console

コンソール接続の設定をデフォルトにリセットするには、グローバル コンフィギュレーション モードで **clear configure console** コマンドを使用します。

clear configure console

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、コンソール接続の設定をデフォルトにリセットする方法を示します。

```
hostname(config)# clear configure console
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定します。
show running-config console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを表示します。

clear configure context

システム コンフィギュレーションのすべてのコンテキスト コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure context** コマンドを使用します。

clear configure context [*noconfirm*]

シンタックスの説明

noconfirm	（オプション）確認を求めるプロンプトを表示せずにすべてのコンテキストを削除します。このオプションは、自動スクリプトに役立ちます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、管理コンテキストを含むすべてのコンテキストを削除できます。管理コンテキストは **no context** コマンドを使用して削除することはできませんが、**clear configure context** コマンドを使用して削除できます。

例

次の例では、システム コンフィギュレーションからすべてのコンテキストを削除し、削除を確認しません。

```
hostname(config)# clear configure context noconfirm
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
mode	コンテキスト モードをシングルまたはマルチに設定します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

clear configure crypto

IPSec、暗号マップ、ダイナミック暗号マップ、CA トラストポイント、すべての証明書、証明書マップ コンフィギュレーション、ISAKMP など、暗号コンフィギュレーション全体を削除するには、グローバル コンフィギュレーション モードで **clear configure crypto** コマンドを使用します。特定のコンフィギュレーションを削除するには、シンタックスに示されているように、このコマンドをキーワードと共に使用します。このコマンドは、慎重に使用してください。

clear configure crypto [**ca** | **dynamic-map** | **ipsec** | **iskmp** | **map**]

シンタックスの説明

ca	認証局のポリシーを削除します。
dynamic-map	ダイナミック暗号マップ コンフィギュレーションを削除します。
ipsec	IPSec コンフィギュレーションを削除します。
isakmp	ISAKMP コンフィギュレーションを削除します。
map	暗号マップ コンフィギュレーションを削除します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、セキュリティ アプライアンスからすべての暗号コンフィギュレーションを削除します。

```
hostname(config)# clear configure crypto
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのまたは指定したダイナミック暗号マップをコンフィギュレーションから消去します。
clear configure crypto map	すべてのまたは指定した暗号マップをコンフィギュレーションから消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
show running-config crypto	IPSec、暗号マップ、ダイナミック暗号マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear configure crypto ca trustpoint

コンフィギュレーションからすべてのトラストポイントを削除するには、グローバル コンフィギュレーション モードで **clear configure crypto ca trustpoint** コマンドを使用します。

clear configure crypto ca trustpoint

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションからすべてのトラストポイントを削除します。

```
hostname(config)# clear configure crypto ca trustpoint
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブコンフィギュレーション レベルに入ります。

clear configure crypto dynamic-map

コンフィギュレーションからすべてのまたは指定したダイナミック暗号マップを削除するには、グローバル コンフィギュレーション モードで **clear configure crypto dynamic-map** コマンドを使用します。

clear configure crypto dynamic-map *dynamic-map-name dynamic-seq-num*

シンタックスの説明

dynamic-map-name	特定のダイナミック暗号マップの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップのシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションからシーケンス番号 3 のダイナミック暗号マップ mymaps を削除します。

```
hostname(config)# clear configure crypto dynamic-map mymaps 3
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのまたは指定した暗号マップのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのアクティブなコンフィギュレーションを表示します。
show running-config crypto map	すべての暗号マップのすべてのアクティブなコンフィギュレーションを表示します。

clear configure crypto isakmp

すべての ISAKMP コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure crypto isakmp** コマンドを使用します。

clear configure crypto isakmp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear configure isakmp** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**clear configure crypto isakmp** コマンドに置き換えられました。

例

グローバル コンフィギュレーション モードで発行した次のコマンドは、セキュリティ アプライアンスからすべての ISAKMP コンフィギュレーションを削除します。

```
hostname(config)# clear configure crypto isakmp
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show crypto isakmp stats	実行時の統計情報を表示します。
show crypto isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure crypto isakmp policy

すべての ISAKMP ポリシー コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure isakmp policy** コマンドを使用します。

clear configure crypto isakmp policy *priority*

シンタックスの説明

priority	消去する ISAKMP ポリシーの優先順位を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear configure isakmp policy** コマンドが導入されました。
7.2(1)	**clear configure isakmp policy** コマンドが、**clear configure crypto isakmp policy** コマンドに置き換えられました。

例

次の例では、コンフィギュレーションから優先順位 3 の ISAKMP ポリシーを削除します。

```
hostname(config)# clear configure isakmp policy 3
hostname(config)#
```

関連コマンド

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時の統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure crypto map

コンフィギュレーションからすべてのまたは指定した暗号マップを削除するには、グローバル コンフィギュレーション モードで **clear configure crypto map** コマンドを使用します。

clear configure crypto map *map-name seq-num*

シンタックスの説明

map-name	特定の暗号マップの名前を指定します。
seq-num	暗号マップのシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションからシーケンス番号 3 の暗号マップ mymaps を削除します。

```
hostname(config)# clear configure crypto map mymaps 3
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのまたは指定したダイナミック暗号マップのコンフィギュレーションを消去します。
crypto map interface	暗号マップをインターフェイスに適用します。
show running-config crypto map	すべての暗号マップのアクティブなコンフィギュレーションを表示します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのアクティブなコンフィギュレーションを表示します。

clear configure ddns

すべての DDNS コマンドを消去するには、グローバル コンフィギュレーション モードで **clear configure ddns** コマンドを使用します。

clear configure ddns

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

例

次の例では、すべての DDNS コマンドを消去しています。

```
hostname(config)# clear configure ddns
```

関連コマンド

コマンド	説明
ddns（DDNS アップデート方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	セキュリティ アプライアンス インターフェイスを、DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
show ddns update interface	設定済みの各 DDNS 方式に関連付けられているインターフェイスを表示します。
show ddns update method	設定済みの各 DDNS 方式について、タイプおよび間隔を表示します。DDNS アップデートを実行する DHCP サーバ。
show running-config ddns	実行コンフィギュレーションに含まれている、設定済みのすべての DDNS 方式について、タイプおよび間隔を表示します。

clear configure dhcpd

DHCP サーバ コマンド、バインディング、および統計情報をすべて消去するには、グローバル コンフィギュレーション モードで **clear configure dhcpd** コマンドを使用します。

clear configure ***dhcpd***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear dhcpd** が **clear configure dhcpd** に変更されました。

使用上のガイドライン

clear configure dhcpd コマンドは、**dhcpd** コマンド、バインディング、および統計情報をすべて消去します。統計情報カウンタまたはバインディング情報だけを消去するには、**clear dhcpd** コマンドを使用します。

例

次の例では、すべての **dhcpd** コマンドを消去する方法を示します。

```
hostname(config)# clear configure dhcpd
```

関連コマンド

コマンド	説明
clear dhcpd	DHCP サーバのバインディングおよび統計情報カウンタを消去します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

clear configure dhcprelay

すべての DHCP リレー コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure dhcprelay** コマンドを使用します。

clear configure ***dhcprelay***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear dhcprelay** が **clear configure dhcprelay** に変更されました。

使用上のガイドライン

clear configure dhcprelay コマンドは、DHCP リレー統計情報およびコンフィギュレーションを消去します。DHCP 統計情報カウンタだけを消去するには、**clear dhcprelay statistics** コマンドを使用します。

例

次の例では、DHCP リレー コンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure dhcprelay
```

関連コマンド

コマンド	説明
clear dhcprelay statistics	DHCP リレー エージェント統計情報カウンタを消去します。
debug dhcprelay	DHCP リレー エージェントに関するデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

clear configure dns

すべての DNS コマンドを消去するには、グローバル コンフィギュレーション モードで **clear configure dns** コマンドを使用します。

clear configure dns

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、すべての DNS コマンドを消去します。

```
hostname(config)# clear configure dns
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear configure established

確立されたコマンドをすべて削除するには、グローバル コンフィギュレーション モードで **clear configure established** コマンドを使用します。

clear configure established

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

established コマンドで作成した確立されている接続を削除するには、***clear xlate*** コマンドを入力します。

例

次の例では、確立されたコマンドを削除する方法を示します。

```
hostname(config)# clear configure established
```

関連コマンド

コマンド	説明
established	確立されている接続に基づくポート上のリターン接続を許可します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。
clear xlate	現在の変換スロット情報および接続スロット情報を消去します。

clear configure failover

コンフィギュレーションから **failover** コマンドを削除してデフォルトに戻すには、グローバル コンフィギュレーション モードで **clear configure failover** コマンドを使用します。

clear configure failover

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが **clear failover** から **clear configure failover** に変更されました。

使用上のガイドライン

このコマンドは、すべての **failover** コマンドを実行コンフィギュレーションから消去し、デフォルトに戻します。***all*** キーワードを **show running-config failover** コマンドと共に使用すると、デフォルトのフェールオーバー コンフィギュレーションが表示されます。

clear configure failover コマンドは、マルチ コンフィギュレーション モードのセキュリティ コンテキストでは使用できません。このコマンドはシステム実行スペースで入力する必要があります。

例

次の例では、コンフィギュレーションからすべてのフェールオーバー コマンドを消去します。

```
hostname(config)# clear configure failover
hostname(config)# show running-configuration failover
no failover
```

関連コマンド

コマンド	説明
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

clear configure filter

URL、FTP、および HTTPS フィルタリング コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure filter** コマンドを使用します。

clear configure filter

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure filter コマンドは、URL、FTP、および HTTPS フィルタリング コンフィギュレーションを消去します。

例

次の例では、URL、FTP、および HTTPS フィルタリング コンフィギュレーションを消去します。

```
hostname# clear configure filter
```

関連コマンド

コマンド	説明
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure fips

NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去するには、**clear configure fips** コマンドを使用します。

clear configure fips

シンタックスの説明

fips	FIPS-2 準拠情報

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

例

```
sw8-ASA(config)# clear configure fips
```

関連コマンド

コマンド	説明
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールで FIPS に準拠するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

clear configure firewall

ファイアウォール モードをデフォルトのルーテッド モードに設定するには、グローバル コンフィギュレーション モードで **clear configure firewall** コマンドを使用します。

clear configure firewall

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ファイアウォール モードをデフォルトに設定します。

```
hostname(config)# clear configure firewall
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードを透過に設定します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear configure fixup

フィックスアップ コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure fixup** コマンドを使用します。

clear configure fixup

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear configure fixup コマンドは、フィックスアップ コンフィギュレーションを削除します。

例

次の例では、フィックスアップ コンフィギュレーションを消去します。

```
hostname# clear configure fixup
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

clear configure fragment

すべての IP フラグメント再構成コンフィギュレーションをデフォルトにリセットするには、グローバル コンフィギュレーション モードで **clear configure fragment** コマンドを使用します。

clear configure fragment [*interface*]

シンタックスの説明

interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	***configure*** キーワードおよびオプションの *interface* 引数が追加されました。また、このコマンドは、運用データの消去とコンフィギュレーション データの消去を区別するため、***clear fragment*** と ***clear configure fragment*** の 2 つのコマンドに分けられました。

使用上のガイドライン

clear configure fragment コマンドは、すべての IP フラグメント再構成コンフィギュレーションをデフォルトにリセットします。また、**chain**、**size**、および **timeout** キーワードが次のデフォルト値にリセットされます。

- ***chain*** は 24 パケットです。
- ***size*** は 200 です。
- ***timeout*** は 5 秒です。

例

次の例では、すべての IP フラグメント再構成コンフィギュレーションをデフォルトにリセットする方法を示します。

```
hostname(config)# clear configure fragment
```

関連コマンド

コマンド	説明
clear fragment	IP フラグメント再構成モジュールの運用データを消去します。
fragment	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
show fragment	IP フラグメント再構成モジュールの運用データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

clear configure ftp

FTP コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure ftp** コマンドを使用します。

clear configure ftp

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure ftp コマンドは、FTP コンフィギュレーションを消去します。

例

次の例では、FTP コンフィギュレーションを消去します。

```
hostname# clear configure filter
```

関連コマンド

コマンド	説明
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure global

コンフィギュレーションから **global** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure global** コマンドを使用します。

clear configure global

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

例

次の例では、コンフィギュレーションから **global** コマンドを削除する方法を示します。

```
hostname(config)# clear configure global
```

関連コマンド

コマンド	説明
global	グローバル アドレス プールに対してエントリを作成します。
show running-config global	コンフィギュレーション内の **global** コマンドを表示します。

clear config group-delimiter

トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するグループ デリミタをコンフィギュレーションから消去するには、グローバル コンフィギュレーション モードで **clear configure group-delimiter** コマンドを使用します。グループ名の解析がディセーブルになります。

clear config group-delimiter

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このデリミタは、トンネルのネゴシエーション中に、ユーザ名からトンネル グループ名を解析するために使用されます。デリミタを指定しないと、グループ名の解析がディセーブルになります。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションからグループ デリミタを削除します。

```
hostname(config)# clear config group-delimiter
hostname(config)#
```

関連コマンド

コマンド	説明
group-delimiter	グループ名の解析をイネーブルにし、IPSec リモートアクセス トンネル グループのグループ デリミタを指定します。
show running-config group-delimiter	現在の設定済みグループ デリミタを表示します。

clear configure group-policy

特定のグループ ポリシーのコンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure group-policy** コマンドを使用し、グループ ポリシーの名前を付加します。デフォルトのグループ ポリシー以外のすべての group-policy コマンドをコンフィギュレーションから削除するには、このコマンドを引数なしで使用します。

clear configure group-policy [*name*]

シンタックスの説明

name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトのグループ ポリシー以外のすべての group-policy コマンドをコンフィギュレーションから削除します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、FirstGroup という名前のグループ ポリシーのコンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーを作成、編集、または削除します。
group-policy attributes	指定したグループ ポリシーの AVP を設定できるグループ ポリシー アトリビュート モードに入ります。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。

clear configure hostname

ホスト名をデフォルトにリセットするには、グローバル コンフィギュレーション モードで **clear configure hostname** コマンドを使用します。

clear configure hostname

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト値はプラットフォームによって異なります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ホスト名を消去します。

```
hostname(config)# clear configure hostname
```

関連コマンド

コマンド	説明
banner	ログイン バナー、「今日のお知らせ」バナー、またはイネーブル バナーを設定します。
domain-name	デフォルトのドメイン名を設定します。
hostname	セキュリティ アプライアンスのホスト名を設定します。

clear configure http

HTTP サーバをディセーブルにし、HTTP サーバにアクセスできる設定済みホストを削除するには、グローバル コンフィギュレーション モードで **clear configure http** コマンドを使用します。

clear configure http

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、HTTP コンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure http
```

関連コマンド

コマンド	説明
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

clear configure icmp

ICMP トラフィックの設定済みアクセス規則を消去するには、グローバル コンフィギュレーション モードで **clear configure icmp** コマンドを使用します。

clear configure icmp

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure icmp コマンドは、ICMP トラフィックの設定済みアクセス規則を消去します。

例

次の例では、ICMP トラフィックの設定済みアクセス規則を消去します。

```
hostname# clear configure icmp
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションを消去します。
debug icmp	ICMP に関するデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

clear configure imap4s

コンフィギュレーションからすべての IMAP4S コマンドを削除してデフォルト値に戻すには、グローバル コンフィギュレーション モードで **clear configure imap4s** コマンドを使用します。

clear configure imap4s

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、IMAP4S コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure imap4s
hostname(config)#
```

関連コマンド

コマンド	説明
show running-configuration imap4s	IMAP4S の実行コンフィギュレーションを表示します。
imap4s	IMAP4S 電子メール プロキシのコンフィギュレーションを作成または編集します。

clear configure interface

インターフェイス コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure interface** コマンドを使用します。

clear configure interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドで割り当てた場合に、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイス コンフィギュレーションを消去します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**clear interface** がこのコマンドに変更されました。また、新しいインターフェイスの番号付け方式も含めるように修正されました。

使用上のガイドライン

メインの物理インターフェイスのインターフェイス コンフィギュレーションを消去する場合、セキュリティ アプライアンスではデフォルト設定が使用されます。

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内だけで使用できるからです。同様に、**allocate-interface** コマンドでインターフェイス ID をマッピング名にマップした場合は、そのマッピング名はコンテキスト内でしか使用できません。

例

次の例では、GigabitEthernet0/1 コンフィギュレーションを消去します。

```
hostname(config)# clear configure interface gigabitethernet0/1
```

次の例では、内部インターフェイス コンフィギュレーションを消去します。

```
hostname(config)# clear configure interface inside
```

次の例では、コンテキスト内で int1 インターフェイス コンフィギュレーションを消去します。「int1」はマッピング名です。

```
hostname/contexta(config)# clear configure interface int1
```

次の例では、すべてのインターフェイス コンフィギュレーションを消去します。

```
hostname(config)# clear configure interface
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear interface	**show interface** コマンドのカウンタを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

clear configure ip

ip address コマンドで設定したすべての IP アドレスを消去するには、グローバル コンフィギュレーション モードで **clear configure ip** コマンドを使用します。

clear configure ip

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

透過ファイアウォール モードでは、このコマンドは、管理 IP アドレスと Management 0/0 IP アドレス（設定している場合）を消去します。

古い IP アドレスを使用する現在の接続をすべて停止するには、**clear xlate** コマンドを入力します。入力しない場合、接続は通常どおりタイムアウトします。

例

次の例では、すべての IP アドレスを消去します。

```
hostname(config)# clear configure ip
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear configure interface	インターフェイスのコンフィギュレーションをすべて消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address	インターフェイスの IP アドレスを設定します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。

clear configure ip audit

監査ポリシー コンフィギュレーション全体を消去するには、グローバル コンフィギュレーション モードで **clear configure ip audit** コマンドを使用します。

clear configure ip audit [**configuration**]

シンタックスの説明

configuration	（オプション）このキーワードを入力できますが、使用しない場合も結果は同じです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが **clear ip audit** から変更されました。

例

次の例では、すべての **ip audit** コマンドを消去します。

```
hostname# clear configure ip audit
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

clear configure ip local pool

IP アドレス プールを削除するには、グローバル コンフィギュレーション モードで **clear configure ip local pool** コマンドを使用します。

clear ip local pool [*poolname*]

シンタックスの説明

poolname	（オプション）IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、実行コンフィギュレーションからすべての IP アドレス プールを削除します。

```
hostname(config)# clear config ip local pool
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
ip local pool	IP アドレス プールを設定します。

clear configure ip verify reverse-path

ip verify reverse-path コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure ip verify reverse-path** コマンドを使用します。

clear configure ip verify reverse-path

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear ip verify reverse-path** がこのコマンドに変更されました。

例

次の例では、すべてのインターフェイスの **ip verify reverse-path** コンフィギュレーションを消去します。

```
hostname(config)# clear configure ip verify reverse-path
```

関連コマンド

コマンド	説明
clear ip verify statistics	Unicast RPF の統計情報を消去します。
ip verify reverse-path	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
show ip verify statistics	Unicast RPF の統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear configure ipv6

実行コンフィギュレーションからグローバル IPv6 コマンドを消去するには、グローバル コンフィギュレーション モードで **clear configure ipv6** コマンドを使用します。

clear configure ipv6 [*route* | *access-list*]

シンタックスの説明

route	（オプション）実行コンフィギュレーションから IPv6 ルーティング テーブル内のルートをスタティックに定義するコマンドを消去します。
access-list	（オプション）実行コンフィギュレーションから IPv6 アクセス リスト コマンドを消去します。

デフォルト

キーワードを指定しない場合、このコマンドでは実行コンフィギュレーションからすべての IPv6 コマンドが消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドでは、実行コンフィギュレーションからグローバル IPv6 コマンドだけが消去されます。インターフェイス コンフィギュレーション モードで入力した IPv6 コマンドは消去されません。

例

次の例では、IPv6 ルーティング テーブルからスタティックに定義された IPv6 ルートを消去する方法を示します。

```
hostname(config)# clear configure ipv6 route
hostname(config)#
```

関連コマンド

コマンド	説明
ipv6 route	IPv6 ルーティング テーブル内のスタティック ルートを定義します。
show ipv6 route	IPv6 ルーティング テーブルの内容を表示します。
show running-config ipv6	実行コンフィギュレーション内の IPv6 コマンドを表示します。

clear configure isakmp

すべての ISAKMP コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure isakmp** コマンドを使用します。

clear configure isakmp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear configure isakmp** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**clear configure crypto isakmp** コマンドに置き換えられました。

例

グローバル コンフィギュレーション モードで発行した次の例では、セキュリティ アプライアンスからすべての ISAKMP コンフィギュレーションを削除します。

```
hostname(config)# clear configure isakmp
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時の統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure isakmp policy

すべての ISAKMP ポリシー コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure isakmp policy** コマンドを使用します。

clear configure isakmp policy *priority*

シンタックスの説明

priority	消去する ISAKMP ポリシーの優先順位を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear configure isakmp policy** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**clear configure crypto isakmp policy** コマンドに置き換えられました。

例

次の例では、コンフィギュレーションから優先順位 3 の ISAKMP ポリシーを削除します。

```
hostname(config)# clear configure isakmp policy 3
hostname(config)#
```

関連コマンド

コマンド	説明
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時の統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

clear configure ldap attribute-map

セキュリティ アプライアンスの実行コンフィギュレーションからすべての LDAP アトリビュート マップを削除するには、グローバル コンフィギュレーション モードで **clear configure ldap attribute-map** コマンドを使用します。

clear configure ldap attribute-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの実行コンフィギュレーションから LDAP アトリビュート マップを削除するには、このコマンドを使用します。

例

グローバル コンフィギュレーション モードで入力した次の例では、実行コンフィギュレーションからすべての LDAP アトリビュート マップを削除し、削除されたことを確認します。

```
hostname(config)# clear configuration ldap attribute-map
hostname(config)# show running-config ldap attribute-map
hostname(config)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP アトリビュート マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP アトリビュート名を、Cisco LDAP アトリビュート名にマッピングします。
map-value	ユーザ定義のアトリビュート値を、Cisco　アトリビュートにマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP アトリビュート マップまたはすべての実行アトリビュート マップを表示します。

clear configure logging

ロギング コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure logging** コマンドを使用します。

clear configure logging [***disabled*** | ***level***]

シンタックスの説明

disabled	（オプション）ディセーブルになっているすべてのシステム ログ メッセージを再度イネーブルにすることを指定します。このオプションを使用する場合、他のロギング コンフィギュレーションは消去されません。
level	（オプション）システム ログ メッセージへの重大度の割り当てをデフォルト値にリセットすることを指定します。このオプションを使用する場合、他のロギング コンフィギュレーションは消去されません。
（オプションが指定されていない場合）	すべてのコンフィギュレーション設定をデフォルト値に戻します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config logging コマンドを使用して、すべてのロギング コンフィギュレーションを表示できます。**clear configure logging** コマンドを disabled または level キーワードなしで使用した場合、すべてのロギング コンフィギュレーション設定が消去され、デフォルト値に戻ります。

例

次の例では、ロギング コンフィギュレーションを消去する方法を示します。**show logging** コマンドの出力は、すべてのロギング機能がディセーブルになっていることを示します。

```
hostname(config)# clear configure logging
hostname(config)# show logging
Syslog logging: disabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

clear configure logging rate-limit

ロギング レート制限をリセットするには、**clear configure logging rate-limit** コマンドを使用します。

clear configure logging rate-limit

シンタックスの説明こ このコマンドには、引数もキーワードもありません。

デフォルト　このコマンドにデフォルト設定はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

例　次の例では、ロギング レート制限をリセットする方法を示します。

```
hostname(config)# clear configure logging rate-limit
```

情報が消去されると、ホストが接続を再び確立するまで、何も表示されません。

関連コマンド

コマンド	説明
logging rate limit	システム ログ メッセージが生成されるレートを制限します。
show running config logging rate-limit	現在のロギング レート制限の設定を表示します。

clear configure mac-address-table

mac-address-table static および **mac-address-table aging-time** コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure mac-address-table** コマンドを使用します。

clear configure mac-address-table

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、**mac-address-table static** および **mac-address-table aging-time** コンフィギュレーションを消去します。

```
hostname# clear configure mac-address-table
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	インターフェイスの MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

clear configure mac-learn

mac-learn コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure mac-learn** コマンドを使用します。

clear configure mac-learn

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、**mac-learn** コンフィギュレーションを消去します。

```
hostname# clear configure mac-learn
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	インターフェイスの MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

clear configure mac-list

以前に **mac-list** コマンドで指定された MAC アドレスの指定したリストを削除するには、グローバル コンフィギュレーション モードで **clear configure mac-list** コマンドを使用します。

clear configure mac-list *id*

シンタックスの説明

id	MAC アドレス リスト名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI 規格に適合するように、このコマンドが修正されました。

使用上のガイドライン

MAC アドレスのリストを削除するには、**clear mac-list** コマンドを使用します。

例

次の例では、MAC アドレス リストを消去する方法を示します。

```
hostname(config)# clear configure mac-list firstmaclist
```

関連コマンド

コマンド	説明
mac-list	先頭一致検索を使用して MAC アドレスのリストを追加します。
show running-config mac-list	*id* で指定した MAC アドレスリストにある MAC アドレスを表示します。

clear configure management-access

セキュリティ アプライアンスの管理アクセスのための内部インターフェイスのコンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで ***clear configure management-access*** コマンドを使用します。

clear configure management-access

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます（インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 “ ” に囲まれて表示されます）。***clear configure management-access*** コマンドは、***management-access*** コマンドで指定した内部管理インターフェイスのコンフィギュレーションを削除します。

例

次の例では、セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。

```
hostname(config)# clear configure management-access
```

関連コマンド

コマンド	説明
management-access	管理アクセス用の内部インターフェイスを設定します。
show running-config management-access	管理アクセス用に設定されている内部インターフェイスの名前を表示します。

clear configure monitor-interface

実行コンフィギュレーションからすべての **monitor-interface** コマンドを削除し、デフォルトのインターフェイス ヘルス モニタリングに戻すには、グローバル コンフィギュレーション モードで **clear configure monitor-interface** コマンドを使用します。

clear configure monitor-interface

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、物理インターフェイスはフェールオーバーのために監視されます。**clear monitor-interface** コマンドを使用すると、実行コンフィギュレーションから **no monitor-interface** コマンドが消去され、デフォルトのインターフェイス ヘルス モニタリングに戻ります。実行コンフィギュレーション内の **monitor-interface** コマンドを表示するには、**show running-config all monitor-interface** コマンドを使用します。

例

次の例では、実行コンフィギュレーションから **monitor-interface** コマンドを消去します。

```
hostname(config)# clear configure monitor-interface
hostname(config)#
```

関連コマンド

コマンド	説明
monitor-interface	フェールオーバー用に指定されているインターフェイスのヘルス モニタリングをイネーブルにします。
show running-config monitor-interface	実行コンフィギュレーション内の **monitor-interface** コマンドを表示します。

clear configure mroute

実行コンフィギュレーションから **mroute** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure mroute** コマンドを使用します。

clear configure mroute

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、コンフィギュレーションから **mroute** コマンドを削除する方法を示します。

```
hostname(config)# clear configure mroute
hostname(config)#
```

関連コマンド

コマンド	説明
mroute	スタティック マルチキャスト ルートを設定します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	実行コンフィギュレーション内の **mroute** コマンドを表示します。

clear configure mtu

すべてのインターフェイスの設定済み Maximum Transmission Unit（MTU; 最大伝送ユニット）値を消去するには、グローバル コンフィギュレーション モードで **clear configure mtu** コマンドを使用します。

clear configure mtu

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

clear configure mtu コマンドを使用すると、すべてのイーサネット インターフェイスの最大伝送ユニットがデフォルトの 1500 に設定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、すべてのインターフェイスの現在の最大伝送ユニット値を消去します。

```
hostname(config)# clear configure mtu
```

関連コマンド

コマンド	説明
mtu	インターフェイスの最大伝送ユニットを指定します。
show running-config mtu	現在の最大伝送ユニットのブロック サイズを表示します。

clear configure multicast-routing

実行コンフィギュレーションから **multicast-routing** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure multicast-routing** コマンドを使用します。

clear configure *multicast-routing*

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure multicast-routing コマンドは、実行コンフィギュレーションから **multicast-routing** を削除します。**no multicast-routing** コマンドも、実行コンフィギュレーションから multicast-routing コマンドを削除します。

例

次の例では、実行コンフィギュレーションから **multicast-routing** コマンドを削除する方法を示します。

```
hostname(config)# clear configure multicast-routing
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

clear configure name

コンフィギュレーションから名前のリストを消去するには、グローバル コンフィギュレーション モードで **clear configure name** コマンドを使用します。

clear configure name

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

次の例では、名前のリストを消去する方法を示します。

```
hostname(config)# clear configure name
```

関連コマンド

コマンド	説明
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられている名前のリストを表示します。

clear configure nat

NAT コンフィギュレーションを削除するには、特権 EXEC モードで **clear configure nat** コマンドを使用します。

clear configure nat

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

透過ファイアウォール モードには、次の注意事項が適用されます。

（注） 透過ファイアウォール モードでは、NAT id 0 のみが有効です。

例

次の例では、NAT コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure nat
```

関連コマンド

コマンド	説明
nat	ネットワークをグローバル IP アドレス プールに関連付けます。
show running-config nat	ネットワークに関連付けられているグローバル IP アドレスのプールを表示します。

clear configure nat-control

NTP コンフィギュレーションの要件をディセーブルにするには、グローバル コンフィギュレーション モードで **clear configure nat-control** コマンドを使用します。

clear configure nat-control

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、NAT コンフィギュレーションの要件をディセーブルにしています。

```
hostname(config)# clear configure nat-control
```

関連コマンド

コマンド	説明
nat	他のインターフェイスのグローバル アドレスに変換される、1 つのインターフェイス上のアドレスを定義します。
nat-control	NAT コントロールを適用します。NAT コントロールをディセーブルにすると、NAT 規則を設定していない場合でも、内部ホストは外部ネットワークと通信することが許可されます。
show running-config nat-control	NAT コンフィギュレーションの要件を表示します。

clear configure ntp

NTP コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure ntp** コマンドを使用します。

clear configure ntp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	**clear ntp** がこのコマンドに変更されました。

例

次の例では、すべての **ntp** コマンドを消去します。

```
hostname# clear configure ntp
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP 認証キーを設定します。
ntp server	セキュリティ アプライアンスの時間を設定する NTP サーバを指定します。
ntp trusted-key	NTP の信頼できるキーを指定します。
show running-config ntp	NTP コンフィギュレーションを表示します。

clear configure object-group

コンフィギュレーションからすべての **object group** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure object-group** コマンドを使用します。

clear configure object-group [{**protocol** | **service** | **icmp-type** | **network**}]

シンタックスの説明

icmp-type	（オプション）すべての ICMP グループを消去します。
network	（オプション）すべてのネットワーク グループを消去します。
protocol	（オプション）すべてのプロトコル グループを消去します。
service	（オプション）すべてのサービス グループを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、コンフィギュレーションからすべての **object-group** コマンドを削除する方法を示します。

```
hostname(config)# clear configure object-group
```

関連コマンド

コマンド	説明
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

clear configure passwd

ログイン パスワード コンフィギュレーションを消去し、デフォルト設定の「cisco」に戻すには、グローバル コンフィギュレーション モードで **clear configure passwd** コマンドを使用します。

clear configure {**passwd** | **password**}

シンタックスの説明

***passwd*	*password***	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**clear passwd** がこのコマンドに変更されました。

例

次の例では、ログイン パスワードを消去し、デフォルトの「cisco」に戻します。

```
hostname(config)# clear configure passwd
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードに入ります。
enable password	イネーブル パスワードを設定します。
passwd	ログイン パスワードを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。
show running-config passwd	ログイン パスワードを暗号化された形で表示します。

clear configure pim

実行コンフィギュレーションからすべてのグローバル **pim** コマンドを消去するには、グローバル コンフィギュレーション モードで **clear configure pim** コマンドを使用します。

clear configure *pim*

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure pim コマンドは、実行コンフィギュレーションからすべての **pim** コマンドを消去します。PIM トラフィック カウンタおよびトポロジ情報を消去するには、**clear pim counters** コマンドおよび **clear pim topology** コマンドを使用します。

clear configure pim コマンドはグローバル コンフィギュレーション モードで入力された **pim** コマンドだけを消去します。インターフェイス固有の **pim** コマンドは消去しません。

例

次の例では、実行コンフィギュレーションからすべての **pim** コマンドを消去する方法を示します。

```
hostname(config)# clear configure pim
```

関連コマンド

コマンド	説明
clear pim topology	PIM トポロジ テーブルを消去します。
clear pim counters	PIM トラフィック カウンタを消去します。
show running-config pim	実行コンフィギュレーション内の **pim** コマンドを表示します。

clear configure policy-map

すべての **policy-map** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure policy-map** コマンドを使用します。

clear configure policy-map [**type inspect** [*protocol*]}

シンタックスの説明

type inspect	（オプション）検査ポリシー マップを消去します。
protocol	（オプション）消去する検査ポリシー マップのタイプを指定します。指定できるタイプは、次のとおりです。 • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **p2p** • **radius-accounting** • **sip** • **skinny** • **snmp**

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

特定の名前のポリシー マップを消去するには、**policy-map** コマンドの **no** 形式を使用します。

例

次に、**clear configure policy-map** コマンドの例を示します。

```
hostname(config)# clear configure policy-map
```

関連コマンド

コマンド	説明
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	ポリシー コンフィギュレーション全体を表示します。

clear configure pop3s

コンフィギュレーションからすべての POP3S コマンドを削除してデフォルト値に戻すには、グローバル コンフィギュレーション モードで **clear configure pop3s** コマンドを使用します。

clear configure pop3s

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例　次の例では、POP3S コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure pop3s
hostname(config)#
```

関連コマンド

コマンド	説明
show running-configuration pop3s	POP3S の実行コンフィギュレーションを表示します。
pop3s	POP3S 電子メール プロキシのコンフィギュレーションを作成または編集します。

clear configure port-forward

WebVPN ユーザが転送 TCP ポート経由でアクセスする設定済みのアプリケーションのセットを削除するには、グローバル コンフィギュレーション モードで **clear configure port-forward** コマンドを使用します。設定済みのアプリケーションをすべて削除するには、このコマンドを *listname* 引数なしで使用します。特定のリストのアプリケーションだけを削除するには、このコマンドに *listname* を付けて使用します。

clear configure port-forward [*listname***]**

シンタックスの説明

listname	WebVPN ユーザがアクセスできるアプリケーション（転送 TCP ポート）のセットをグループ化します。最大 64 文字です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、*SalesGroupPorts* という名前のポート転送リストを削除する方法を示します。

```
hostname(config)# clear configure port-forward SalesGroupPorts
```

関連コマンド

コマンド	説明
port-forward	WebVPN ユーザがアクセスできるアプリケーションのセットを設定するには、WebVPN コンフィギュレーション モードでこのコマンドを使用します。
port-forward	ユーザまたはグループ ポリシーの WebVPN アプリケーション　アクセスをイネーブルにするには、webvpn モードでこのコマンドを使用します。
show running-configuration port-forward	現在設定されている **port-forward** コマンドのセットを表示します。

clear configure prefix-list

実行コンフィギュレーションから **prefix-list** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure prefix-list** コマンドを使用します。

clear configure prefix-list [*prefix-list-name*]

シンタックスの説明

prefix-list-name	（オプション）プレフィックス リストの名前。プレフィックス リスト名を指定した場合は、そのプレフィックス リストのコマンドだけがコンフィギュレーションから削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear prefix-list** が **clear configure prefix-list** に変更されました。

使用上のガイドライン

clear configure prefix-list コマンドは、実行コンフィギュレーションから **prefix-list** コマンドおよび **prefix-list description** コマンドを削除します。プレフィックス リスト名を指定した場合は、実行コンフィギュレーションからそのプレフィックス リストの **prefix-list** コマンドと **prefix-list description** コマンド（存在する場合）だけが削除されます。

このコマンドは、実行コンフィギュレーションから **no prefix-list sequence** コマンドを削除しません。

例

次の例では、実行コンフィギュレーションから MyPrefixList という名前のプレフィックス リストのすべての **prefix-list** コマンドを削除します。

```
hostname# clear configure prefix-list MyPrefixList
```

関連コマンド

コマンド	説明
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

clear configure priority-queue

コンフィギュレーションからプライオリティ キューの指定を削除するには、グローバル コンフィギュレーション モードで **clear configure priority-queue** コマンドを使用します。

clear configure priority queue *interface-name*

シンタックスの説明

interface-name	プライオリティ キューの詳細を表示するインターフェイスの名前を指定します。

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、**clear configure priority-queue** コマンドを使用して、test という名前のインターフェイスでプライオリティ キュー コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure priority-queue test
```

関連コマンド

コマンド	説明
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

clear configure privilege

コマンドの設定済みの特権レベルを削除するには、グローバル コンフィギュレーション モードで **clear configure privilege** コマンドを使用します。

clear configure privilege

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

元に戻すことはできません。

例

次の例では、コマンドの設定済みの特権レベルをリセットする方法を示します。

```
hostname(config)# clear configure privilege
```

関連コマンド

コマンド	説明
privilege	コマンド特権レベルを設定します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

clear configure regex

すべての正規表現を削除するには、グローバル コンフィギュレーション モードで **clear configure regex** コマンドを使用します。

clear configure regex

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

特定の名前の正規表現を消去するには、**regex** コマンドの **no** 形式を使用します。

例

次の例では、設定済みの正規表現をすべて消去する方法を示します。

```
hostname(config)# clear configure regex
```

関連コマンド

コマンド	説明
class-map type regex	正規表現クラス マップを作成します。
regex	正規表現を作成します。
show running-config regex	すべての正規表現を表示します。
test regex	正規表現をテストします。

clear configure route

connect キーワードを含んでいないコンフィギュレーションから **route** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure route** コマンドを使用します。

clear configure route [*interface_name ip_address* [*netmask gateway_ip*]]

シンタックスの説明

gateway_ip	（オプション）ゲートウェイ ルータの IP アドレスを指定します（このルートのネクストホップ アドレス）。
interface_name	（オプション）内部または外部のネットワーク インターフェイス名。
ip_address	（オプション）内部または外部のネットワーク IP アドレス。
netmask	（オプション）*ip_address* に適用するネットワーク マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

使用上のガイドライン

デフォルト ルートを指定するには、**0.0.0.0** を使用します。0.0.0.0 IP アドレスは **0** に、0.0.0.0 *netmask* は **0** に省略できます。

例

次の例では、**connect** キーワードを含んでいないコンフィギュレーションから **route** コマンドを削除する方法を示します。

```
hostname(config)# clear configure route
```

関連コマンド

コマンド	説明
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear configure route-map

すべてのルートマップを削除するには、グローバル コンフィギュレーション モードで **clear configure route-map** コマンドを使用します。

clear configure route-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

コンフィギュレーション内のすべての **route-map** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure route-map** コマンドを使用します。**route-map** コマンドは、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を設定するために使用します。

個々の **route-map** コマンドを削除するには、**no route-map** コマンドを使用します。

例

次の例では、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を削除する方法を示します。

```
hostname(config)# clear configure route-map
```

関連コマンド

コマンド	説明
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。
show running-config route-map	ルートマップ コンフィギュレーションに関する情報を表示します。

clear configure router

実行コンフィギュレーションからすべてのルータ コンフィギュレーション コマンドを消去するには、グローバル コンフィギュレーション モードで **clear configure router** コマンドを使用します。

clear configure router [**ospf** [*id*] | ***rip***]

シンタックスの説明

id	（オプション）指定した OSPF プロセス ID のコンフィギュレーション コマンドを消去します。ID を指定しないと、すべての OSPF プロセスのコンフィギュレーション コマンドが消去されます。
ospf	（オプション）コンフィギュレーションから OSPF コンフィギュレーション コマンドだけを削除することを指定します。
rip	（オプション）コンフィギュレーションから RIP コンフィギュレーション コマンドだけを削除することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear router** コマンドが **clear configure router** コマンドに変更されました。
7.2(1)	コマンドに ***rip*** キーワードが追加されました。

例

次の例では、実行コンフィギュレーションから OSPF プロセス 1 に関連付けられたすべての OSPF コマンドを消去します。

```
hostname(config)# clear configure router ospf 1
```

次の例は、実行コンフィギュレーションから、RIP のルーティング プロセスに関連する、グローバル コンフィギュレーション モードのコマンドをすべて削除します。インターフェイス コンフィギュレーション モードで入力した RIP コマンドは消去されません。

```
hostname(config)# clear configure router rip
```

関連コマンド

コマンド	説明
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

clear configure same-security-traffic

same-security-traffic コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure same-security-traffic** コマンドを使用します。

clear configure same-security-traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、**same-security-traffic** コンフィギュレーションを消去します。

```
hostname(config)# clear configure same-security-traffic
```

関連コマンド

コマンド	説明
same-security-traffic	セキュリティ レベルの等しいインターフェイス間での通信を許可します。
show running-config same-security-traffic	**same-security-traffic** のコンフィギュレーションを表示します。

clear configure service-policy

サービス ポリシー コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで ***clear configure service-policy*** コマンドを使用します。

clear configure service-policy

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、***clear* configure *service-policy*** コマンドの例を示します。

```
hostname(config)# clear configure service-policy
```

関連コマンド

コマンド	説明
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
service-policy	サービス ポリシーを設定します。
clear service-policy	サービス ポリシーの統計情報を消去します。

clear configure sla monitor

実行コンフィギュレーションから **sla monitor** コマンドとサブコマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure sla monitor** コマンドを使用します。

clear configure sla monitor [*sla-id*]

シンタックスの説明

sla-id	（オプション）SLA オペレーションの ID。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id を指定しないと、SLA オペレーションのコンフィギュレーションがすべて消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**sla monitor** コマンド、および SLA モニタ コンフィギュレーション モードの関連するコマンドと **sla monitor schedule** コマンド（存在する場合）を消去します。**track rtr** コマンドは、コンフィギュレーションから削除されません。

実行コンフィギュレーション内の sla monitor コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次の例は、コンフィギュレーションからすべての **sla monitor** コマンドを消去します。

```
hostname(config)# clear configure sla monitor
```

次の例は、ID が 5 の SLA オペレーションに関連する **sla monitor** コマンドを消去します。

```
hostname(config)# clear configure sla monitor 5
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーション内の sla monitor コマンドを表示します。

clear configure smtps

コンフィギュレーションからすべての SMTPS コマンドを削除してデフォルト値に戻すには、グローバル コンフィギュレーション モードで **clear configure smtps** コマンドを使用します。

clear configure smtps

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、SMTPS コンフィギュレーションを削除する方法を示します。

```
hostname(config)# clear configure smtps
hostname(config)#
```

関連コマンド

コマンド	説明
show running-configuration smtps	SMTPS の実行コンフィギュレーションを表示します。
smtps	SMTPS 電子メール プロキシのコンフィギュレーションを作成または編集します。

clear configure smtp-server

SMTP サーバのコマンドと統計情報をすべて消去するには、グローバル コンフィギュレーション モードで **clear configure smtp-server** コマンドを使用します。

clear configure ***smtp-server***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドがサポートされるようになりました。

使用上のガイドライン

clear configure smtp-server コマンドは、**smtp** のコマンドと統計情報をすべて消去します。

例

次の例では、すべての **smtp-server** コマンドを消去する方法を示します。

```
hostname(config)# clear configure smtp-server
```

関連コマンド

コマンド	説明
show running-config smtp-server	現在の DHCP サーバ コンフィギュレーションを表示します。

clear configure snmp-map

SNMP マップ コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure snmp-map** コマンドを使用します。

clear configure snmp-map

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure snmp-map コマンドは、SNMP マップ コンフィギュレーションを削除します。

例

次の例では、SNMP マップ コンフィギュレーションを消去します。

```
hostname# clear configure snmp-map
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。

clear configure snmp-server

簡易ネットワーク管理プロトコル（SNMP）サーバをディセーブルにするには、グローバル コンフィギュレーション モードで **clear configure snmp-server** コマンドを使用します。

clear configure snmp-server

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

例

この例は、SNMP サーバをディセーブルにする方法を示しています。

```
hostname #clear snmp-server
```

関連コマンド

コマンド	説明
snmp-server	SNMP を介してセキュリティ アプライアンスのイベント情報を提供します。
show snmp-server statistics	SNMP サーバのコンフィギュレーションに関する情報を表示します。

clear configure ssh

実行コンフィギュレーションからすべての SSH コマンドを消去するには、グローバル コンフィギュレーション モードで **clear configure ssh** コマンドを使用します。

clear configure ***ssh***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear ssh** コマンドが **clear configure ssh** コマンドに変更されました。

使用上のガイドライン

このコマンドは、コンフィギュレーションからすべての SSH コマンドを消去します。特定のコマンドを消去するには、このコマンドの **no** 形式を使用します。

例

次の例では、コンフィギュレーションからすべての SSH コマンドを消去します。

```
hostname(config)# clear configure ssh
```

関連コマンド

コマンド	説明
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh scopy enable	セキュリティ アプライアンス上でセキュア コピー サーバをイネーブルにします。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

clear configure ssl

コンフィギュレーションからすべての SSL コマンドを削除してデフォルト値に戻すには、グローバル コンフィギュレーション モードで **clear config ssl** コマンドを使用します。

clear config ssl

デフォルト

デフォルトは次のとおりです。

- SSL クライアントおよび SSL サーバのバージョンは両方とも **any** です。
- SSL 暗号化は、3des-sha1 | des-sha1 | rc4-md5 の順序です。
- トラストポイント アソシエーションはありません。セキュリティ アプライアンスはデフォルトの RSA キー ペア証明書を使用します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、**clear config ssl** コマンドの使用方法を示します。

```
hostname(config)# clear config ssl
```

関連コマンド

コマンド	説明
show running-config ssl	現在設定されている ssl コマンドのセットを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

clear configure static

コンフィギュレーションからすべての **static** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure static** コマンドを使用します。

clear configure static

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

例

次の例では、コンフィギュレーションからすべての **static** コマンドを削除する方法を示します。

```
hostname(config)# clear configure static
```

関連コマンド

コマンド	説明
show running-config static	コンフィギュレーション内のすべての **static** コマンドを表示します。
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定します。

clear configure sunrpc-server

セキュリティ アプライアンスからリモート プロセッサ コール サービスを消去するには、グローバル コンフィギュレーション モードで **clear configure sunrpc-server** コマンドを使用します。

clear configure sunrpc-server [**active**]

シンタックスの説明

active	（オプション）セキュリティ アプライアンスで現在アクティブな SunRPC サービスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

sunrpc-server コマンドは、設定された **router ospf** コマンドを表示します。

（注） セキュリティ アプライアンス上で最上位の IP アドレスがプライベート アドレスの場合、このアドレスは hello パケットおよびデータベース定義で送信されます。このアクションを防止するには、**router-id** *ip_address* をグローバル アドレスに設定します。

例

次の例では、セキュリティ アプライアンスから SunRPC サービスを消去する方法を示します。

```
hostname(config)# clear configure sunrpc-server active
```

関連コマンド

コマンド	説明
sunrpc-server	SunRPC サービス テーブルを作成します。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

clear configure sysopt

すべての **sysopt** コマンドのコンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure sysopt** コマンドを使用します。

clear configure sysopt

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear sysopt** がこのコマンドに変更されました。

例

次の例では、すべての **sysopt** コマンドのコンフィギュレーションを消去します。

```
hostname(config)# clear configure sysopt
```

関連コマンド

コマンド	説明
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS の A レコード アドレスの変更をディセーブルにします。

clear configure tcp-map

tcp マップ コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure tcp-map** コマンドを使用します。

clear configure tcp-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、TCP マップ コンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure tcp-map
```

関連コマンド

コマンド	説明
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。
show running-config tcp-map	TCP マップ コンフィギュレーションに関する情報を表示します。

clear configure telnet

コンフィギュレーションから Telnet 接続およびアイドル タイムアウトを削除するには、グローバル コンフィギュレーション モードで **clear configure telnet** コマンドを使用します。

clear configure telnet

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***configure*** が追加されました。

例

次の例では、セキュリティ アプライアンスのコンフィギュレーションから Telnet 接続およびアイドル タイムアウトを削除する方法を示します。

```
hostname(config)# clear configure telnet
```

関連コマンド

コマンド	説明
show running-config telnet	セキュリティ アプライアンスへの Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
telnet	Telnet アクセスをコンソールに追加し、アイドル タイムアウトを設定します。

clear configure terminal

端末の表示幅設定を消去するには、グローバル コンフィギュレーション モードで ***clear configure terminal*** コマンドを使用します。

clear configure terminal

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	***configure*** キーワードが追加されました。

例

次の例では、表示幅を消去します。

```
hostname# clear configure terminal
```

関連コマンド

コマンド	説明
terminal	端末回線のパラメータを設定します。
terminal width	端末の表示幅を設定します。
show running-config terminal	現在の端末設定を表示します。

clear configure timeout

コンフィギュレーションのデフォルトのアイドル状態の継続時間に戻すには、グローバル コンフィギュレーション モードで **clear configure timeout** コマンドを使用します。

clear configure timeout

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、コンフィギュレーションからアイドル状態の最大継続時間を削除する方法を示します。

```
hostname(config)# clear configure timeout
```

関連コマンド

コマンド	説明
show running-config timeout	指定したプロトコルのタイムアウト値を表示します。
timeout	アイドル状態の最大継続時間を設定します。

clear configure time-range

設定されているすべての時間範囲を消去するには、グローバル コンフィギュレーション モードで **clear configure time-range** コマンドを使用します。

clear configure time-range

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、設定されているすべての時間範囲を消去します。

```
hostname(config)# clear configure time-range
```

関連コマンド

コマンド	説明
time-range	時間範囲コンフィギュレーション モードに入り、トラフィック規則または動作に添付できる時間範囲を定義します。

clear configure tunnel-group

コンフィギュレーションからすべてのまたは指定したトンネル グループを削除するには、グローバル コンフィギュレーション モードで **clear config tunnel-group** コマンドを使用します。

clear config tunnel-group [*name*]

シンタックスの説明

name	（オプション）トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、コンフィギュレーションから toengineering トンネル グループを削除します。

```
hostname(config)# clear config tunnel-group toengineering
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config tunnel-group	すべてのまたは選択したトンネル グループに関する情報を表示します。
tunnel-group	指定したタイプのトンネル グループ サブコンフィギュレーション モードに入ります。

clear configure tunnel-group-map

clear configure tunnel-group-map コマンドは、証明書のコンテンツからトンネル グループ名が生成されるときに使用されるポリシーおよび規則を消去します。

clear configure tunnel-group-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tunnel-group-map コマンドは、証明書ベースの IKE セッションをトンネル グループにマップするポリシーと規則を設定します。**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けるには、グローバル コンフィギュレーション モードで **tunnel-group-map** コマンドを使用します。各呼び出しが一意であり、マップ インデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。

crypto ca certificate map コマンドは、証明書マッピング規則の優先順位付きリストを管理します。定義できるマップは 1 つのみです。ただし、このマップで 65,535 個までの規則を保持できます。詳細については、**crypto ca certificate map** コマンドのマニュアルを参照してください。

証明書からトンネル グループ名を取得する処理は、トンネル グループに関連付けられていない証明書マップのエントリを無視します（どのマップ規則もこのコマンドでは識別されません）。

例

次の例はグローバル コンフィギュレーション モードで入力され、他の設定済みメソッドで名前を取得できない場合に使用されるデフォルトのトンネル グループを指定します。使用するトンネル グループの名前は、group1 です。

```
hostname(config)# clear configure tunnel-group-map
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	crypto ca 証明書マップ モードに入ります。
subject-name（暗号 CA 証明書マップ）	規則エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map default-group	既存のトンネル グループ名をデフォルト トンネル グループとして指定します。
tunnel-group-map enable	証明書ベースの IKE セッションをトンネル グループにマップするポリシーと規則を設定します。

clear configure url-block

URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure url-block** コマンドを使用します。

clear configure url-block

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-block コマンドは、URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションを消去します。

例

次の例では、URL 保留ブロック バッファおよび長い URL サポート コンフィギュレーションを消去します。

```
hostname# clear configure url-block
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用状況カウンタを消去します。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure url-cache

URL キャッシュを消去するには、グローバル コンフィギュレーション モードで **clear configure url-cache** コマンドを使用します。

clear configure url-cache

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-cache コマンドは、URL キャッシュを消去します。

例

次の例では、URL キャッシュを消去します。

```
hostname# clear configure url-cache
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**scsc** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

clear configure url-list

WebVPN ユーザがアクセスできる設定済みの URL のセットを削除するには、グローバル コンフィギュレーション モードで **clear configure url-list** コマンドを使用します。設定済みの URL をすべて削除するには、このコマンドを *listname* 引数なしで使用します。特定のリストの URL だけを削除するには、このコマンドに *listname* を付けて使用します。

clear configure url-list [*listname***]**

シンタックスの説明

listname	WebVPN ユーザがアクセスできる URL のセットをグループ化します。最大 64 文字です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、*Marketing URLs* という名前の URL リストを削除する方法を示します。

```
hostname(config)# clear configure url-list Marketing URLs
```

関連コマンド

コマンド	説明
show running-configuration url-list	現在設定されている **url-list** コマンドのセットを表示します。
url-list	WebVPN ユーザがアクセスできる URL のセットを設定するには、グローバル コンフィギュレーション モードでこのコマンドを使用します。
url-list	特定のグループ ポリシーまたはユーザの WebVPN URL アクセスをイネーブルにするには、グループ ポリシーまたはユーザ名モードからアクセスする WebVPN モードでこのコマンドを使用します。

clear configure url-server

URL フィルタリング サーバ コンフィギュレーションを消去するには、グローバル コンフィギュレーション モードで **clear configure url-server** コマンドを使用します。

clear configure url-server

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure url-server コマンドは、URL フィルタリング サーバ コンフィギュレーションを消去します。

例

次の例では、URL フィルタリング サーバ コンフィギュレーションを消去します。

```
hostname# clear configure url-server
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報を消去します。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear configure username

ユーザ名データベースを消去するには、**clear configure username** コマンドを使用します。特定のユーザのコンフィギュレーションを消去するには、このコマンドを使用し、ユーザ名を付加します。

clear configure username [*name*]

シンタックスの説明

name	（オプション）ユーザの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドを使用して入力されたユーザで構成されています。login コマンドは、このデータベースを認証用に使用します。

例

次の例では、anyuser という名前のユーザのコンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure username anyuser
```

関連コマンド

コマンド	説明
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username	ユーザをセキュリティ アプライアンスのデータベースに追加します。
username attributes	特定のユーザの AVP を設定できます。

clear configure virtual

コンフィギュレーションから認証仮想サーバを削除するには、グローバル コンフィギュレーション モードで **clear configure virtual** コマンドを使用します。

clear configure virtual

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

元に戻すことはできません。

例

次に、**clear configure virtual** コマンドの例を示します。

```
hostname(config)# clear configure virtual
```

関連コマンド

コマンド	説明
show running-config virtual	認証仮想サーバの IP アドレスを表示します。
virtual http	セキュリティ アプライアンスと HTTP サーバでの別々の認証を可能にします。
virtual telnet	セキュリティ アプライアンスが認証プロンプトを提供しないトラフィック タイプの仮想 Telnet サーバを使用してユーザを認証します。

clear configure vpdn group

コンフィギュレーションからすべての **vpdn group** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure vpdn group** コマンドを使用します。

clear configure vpdn group

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure vpdn group コマンドを入力しても、アクティブな PPPoE 接続には何も影響ありません。

例

次の例は、vpdn group コンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure vpdn group
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show running-config vpdn username	VPDN ユーザ名の現在のコンフィギュレーションを表示します。

clear configure vpdn username

コンフィギュレーションからすべての **vpdn username** コマンドを削除するには、グローバル コンフィギュレーション モードで **clear configure vpdn username** コマンドを使用します。

clear configure vpdn username

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure vpdn username コマンドを入力しても、アクティブな PPPoE 接続には影響がありません。

例

次の例は、vpdn username コンフィギュレーションを消去する方法を示します。

```
hostname(config)# clear configure vpdn username
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure vpdn group	コンフィギュレーションからすべての vpdn group コマンドを削除します。
show running-config vpdn username	VPDN ユーザ名の現在のコンフィギュレーションを表示します。

clear configure vpn-load-balancing

以前に指定した VPN ロードバランシング コンフィギュレーションを削除して、VPN ロードバランシングをディセーブルにするには、グローバル コンフィギュレーション モードで **clear configure vpn load-balancing** コマンドを使用します。

clear configure vpn load-balancing

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure vpn load-balancing コマンドは、**cluster encryption**、**cluster ip address**、**cluster key**、**cluster port**、**nat**、**participate**、および **priority** などの関連コマンドも消去します。

例

次のコマンドは、コンフィギュレーションから VPN ロードバランシング コンフィギュレーション文を削除します。

```
hostname(config)# clear configure vpn load-balancing
```

関連コマンド

show running-config load-balancing	現在の VPN ロードバランシング コンフィギュレーションを表示します。
vpn load-balancing	VPN ロードバランシング モードに入ります。

clear configure wccp

すべての WCCP コンフィギュレーションを削除するには、グローバル コンフィギュレーション モードで **clear configure wccp** コマンドを使用します。

clear configure wccp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、WCCP コンフィギュレーションを表示する方法を示しています。

```
hostname(config)# clear configure wccp
```

関連コマンド

コマンド	説明
show wccp	WCCP のコンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

clear configure zonelabs-integrity

実行コンフィギュレーションからすべての Zone Labs Integrity サーバを削除するには、グローバル コンフィギュレーション モードで **clear configure zonelabs-integrity** コマンドを使用します。

clear configure zonelabs-integrity

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

すべての Zone Lab Integrity サーバを削除します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2.(1)	このコマンドが導入されました。

使用上のガイドライン

clear configure zonelabs-integrity コマンドは、実行コンフィギュレーションからすべての Zone Labs Integrity サーバ（アクティブとスタンバイを含む）を削除します。

例

次の例では、2 つの設定済みの Zone Labs Integrity サーバを削除します。

```
hostname(config)# show running-config zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
hostname(config)# clear configure zonelabs-integrity
hostname(config)# show running-config zonelabs-integrity
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config [all] zonelabs-integrity	設定されている Zone Labs Integrity サーバを表示します。

clear console-output コマンド～ clear xlate コマンド

clear console-output

現在キャプチャされているコンソール出力を削除するには、特権 EXEC モードで **clear console-output** コマンドを使用します。

clear console-output

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例　次の例では、現在キャプチャされているコンソール出力を削除する方法を示します。

```
hostname# clear console-output
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定します。
show console-output	キャプチャされたコンソール出力を表示します。
show running-config console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを表示します。

clear counters

プロトコル スタック カウンタを消去するには、グローバル コンフィギュレーション モードで **clear counters** コマンドを使用します。

clear counters [all | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

シンタックスの説明

all	（オプション）すべてのフィルタの詳細を消去します。
context *context-name*	（オプション）コンテキスト名を指定します。
:*counter_name*	（オプション）カウンタの名前を指定します。
detail	（オプション）詳細なカウンタ情報を消去します。
protocol *protocol_name*	（オプション）指定したプロトコルのカウンタを消去します。
summary	（オプション）カウンタ情報を消去します。
threshold *N*	（オプション）指定したしきい値以上のカウンタを消去します。範囲は 1 ～ 4294967295 です。
top *N*	（オプション）指定したしきい値以上のカウンタを消去します。範囲は 1 ～ 4294967295 です。

デフォルト

clear counters summary detail

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、プロトコル スタック カウンタを消去する方法を示します。

```
hostname(config)# clear counters
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。

clear crashinfo

フラッシュ メモリ内のクラッシュ ファイルの内容を削除するには、特権 EXEC モードで ***clear crashinfo*** コマンドを入力します。

clear crashinfo

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

次のコマンドは、クラッシュ ファイルを削除する方法を示します。

```
hostname# clear crashinfo
```

関連コマンド

crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。
show crashinfo	フラッシュ メモリに保存されているクラッシュ ファイルの内容を表示します。

clear crypto accelerator statistics

暗号アクセラレータ MIB からグローバルな統計情報およびアクセラレータ固有の統計情報を消去するには、グローバル コンフィギュレーション モードおよび特権 EXEC モードで **clear crypto accelerator statistics** コマンドを使用します。

clear crypto accelerator statistics

シンタックスの説明

このコマンドには、キーワードも変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号アクセラレータの統計情報を表示します。

```
hostname(config)# clear crypto accelerator statistics
hostname(config)#
```

関連コマンド

コマンド	説明
clear crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去します。
show crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示します。

clear crypto ca crls

指定したトラストポイントに関連付けられたすべての CRL の CRL キャッシュを削除、またはすべての CRL の CRL キャッシュを削除するには、グローバル コンフィギュレーション モードで **clear crypto ca crls** コマンドを使用します。

clear crypto ca crls [*trustpointname*]

シンタックスの説明

trustpointname	（オプション）トラストポイントの名前。名前を指定しない場合、このコマンドはシステム上のキャッシュされた CRL をすべて消去します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、セキュリティ アプライアンスのすべての CRL からすべての CRL キャッシュを削除します。

```
hostname(config)# clear crypto ca crls
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca crl request	トラストポイントの CRL コンフィギュレーションに基づいて CRL をダウンロードします。
show crypto ca crls	キャッシュされたすべての CRL または指定したトラストポイントのキャッシュされた CRL を表示します。

clear [crypto] ipsec sa

IPSec SA のカウンタ、エントリ、暗号マップ、またはピア接続を削除するには、グローバル コンフィギュレーション モードで **clear [crypto] ipsec sa** コマンドを使用します。すべての IPSec SA を消去するには、このコマンドを引数なしで使用します。

clear [crypto] ipsec sa [counters | entry {*hostname* | *IP address***} {esp | ah} {***SPI***}| map {***map name***} | peer {***hostname* | *IP address***}]**

このコマンドは、慎重に使用してください。

シンタックスの説明

ah	認証ヘッダー。
counters	各 SA 統計情報のすべての IPSec を消去します。
entry	指定した IP アドレス、ホスト名、プロトコル、および SPI 値に一致するトンネルを削除します。
esp	暗号化セキュリティ プロトコル。
hostname	IP アドレスに割り当てられたホスト名を指定します。
IP address	IP アドレスを指定します。
map	マップ名で識別される指定した暗号マップに関連付けられたすべてのトンネルを削除します。
map name	暗号マップを識別する英数字の文字列。最大 64 文字です。
peer	指定したホスト名または IP アドレスによって識別されたピアへのすべての IPSec SA を削除します。
SPI	セキュリティ パラメータ インデックス（16 進数）を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、セキュリティ アプライアンスからすべての IPSec SA を削除します。

```
hostname(config)# clear ipsec sa
hostname(config)#
```

グローバル コンフィギュレーション モードで発行した次の例では、10.86.1.1 のピア IP アドレスを持つ SA を削除します。

```
hostname(config)# clear ipsec peer 10.86.1.1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのまたは指定した暗号マップをコンフィギュレーションから消去します。
clear configure isakmp	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
show ipsec sa	カウンタ、エントリ、マップ名、ピア IP アドレス、ホスト名などの IPSec SA に関する情報を表示します。
show running-config crypto	IPSec、暗号マップ、ダイナミック暗号マップ、ISAKMP など、暗号コンフィギュレーション全体を表示します。

clear crypto protocol statistics

暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear crypto protocol statistics** コマンドを使用します。

clear crypto protocol statistics *protocol*

シンタックスの説明

protocol	統計情報を消去するプロトコルの名前を指定します。指定できるプロトコルは、次のとおりです。 ***ikev1***：Internet Key Exchange バージョン 1 ***ipsec***：IP セキュリティ フェーズ 2 プロトコル ***ssl***：Secure Socket Layer ***other***：新しいプロトコルのために予約済み ***all***：現在サポートされているすべてのプロトコル このコマンドのオンライン ヘルプでは、今後のリリースでサポートされる他のプロトコルが表示される場合があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号アクセラレータの統計情報をすべて消去します。

```
hostname(config)# clear crypto protocol statistics all
hostname(config)#
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を消去します。
show crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を表示します。
show crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示します。

clear dhcpd

DHCP サーバのバインディングおよび統計情報を消去するには、**clear dhcp** コマンドを使用します。

clear dhcpd {***binding*** [*IP_address*] | ***statistics***}

シンタックスの説明

binding	すべてのクライアント アドレスのバインディングを消去します。
IP_address	指定した IP アドレスのバインディングを消去します。
statistics	統計情報カウンタを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear dhcpd binding コマンドに任意の IP アドレスを含めた場合、その IP アドレスのバインディングだけが消去されます。

すべての DHCP サーバ コマンドを消去するには、**clear configure dhcpd** コマンドを使用します。

例

次の例では、**dhcpd** 統計情報を消去する方法を示します。

```
hostname(config)# clear dhcpd statistics
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。

clear dhcprelay statistics

DHCP リレー統計情報カウンタを消去するには、特権 EXEC モードで **clear dhcprelay statistics** コマンドを使用します。

clear dhcprelay ***statistics***

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**clear dhcprelay statistics** コマンドは、DHCP リレー統計情報カウンタだけを消去します。DHCP リレー コンフィギュレーション全体を消去するには、**clear configure dhcprelay** コマンドを使用します。

例　次の例では、DHCP リレー統計情報を消去する方法を示します。

```
hostname# clear dhcprelay statistics
hostname#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcprelay	DHCP リレー エージェントに関するデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

clear dns-hosts cache

DNS キャッシュを消去するには、特権 EXEC モードで **clear dns-hosts cache** コマンドを使用します。このコマンドは、**name** コマンドで追加したスタティック エントリを消去しません。

clear dns-hosts cache

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、DNS キャッシュを消去します。

```
hostname# clear dns-hosts cache
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

clear failover statistics

フェールオーバー統計情報カウンタを消去するには、特権 EXEC モードで **clear failover statistics** コマンドを使用します。

clear failover statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**show failover statistics** コマンドで表示される統計情報および **show failover** コマンド出力の Stateful Failover Logical Update Statistics セクションのカウンタを消去します。フェールオーバー コンフィギュレーションを削除するには、**clear configure failover** コマンドを使用します。

例

次の例では、フェールオーバー統計情報カウンタを消去する方法を示します。

```
hostname# clear failover statistics
hostname#
```

関連コマンド

コマンド	説明
debug fover	フェールオーバーのデバッグ情報を表示します。
show failover	フェールオーバー コンフィギュレーションに関する情報および動作統計情報を表示します。

clear fragment

IP フラグメント再構成モジュールの運用データを消去するには、特権 EXEC モードで ***clear fragment*** コマンドを入力します。このコマンドは、現在キューに入っている再組み立てを待っているフラグメント（***queue*** キーワードが入力されている場合）またはすべての IP フラグメント再構成統計情報（***statistics*** キーワードが入力されている場合）のいずれかを消去します。統計情報は、再組み立てに成功したフラグメント チェーンの数、再組み立てに失敗したチェーンの数、および最大サイズの超過によってバッファのオーバーフローが発生した回数を示すカウンタです。

clear fragment {**queue** | **statistics**} [*interface*]

シンタックスの説明

interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。
queue	IP フラグメント再構成キューを消去します。
statistics	IP フラグメント再構成統計情報を消去します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、運用データの消去とコンフィギュレーション データの消去を区別するため、***clear fragment*** と ***clear configure fragment*** の 2 つのコマンドに分けられました。

例

次の例では、IP フラグメント再構成モジュールの運用データを消去する方法を示します。

```
hostname# clear fragment queue
```

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションを消去し、デフォルトにリセットします。
fragment	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
show fragment	IP フラグメント再構成モジュールの運用データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

clear gc

ガーベッジ コレクション プロセスの統計情報を削除するには、特権 EXEC モードで **clear gc** コマンドを使用します。

clear gc

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ガーベッジ コレクション プロセスの統計情報を削除する方法を示します。

```
hostname# clear gc
```

関連コマンド

コマンド	説明
show gc	ガーベッジ コレクション プロセスの統計情報を表示します。

clear igmp counters

すべての IGMP カウンタを消去するには、特権 EXEC モードで **clear igmp counters** コマンドを使用します。

clear igmp counters [*if_name*]

シンタックスの説明

if_name	**nameif** コマンドで指定されたインターフェイスの名前。このコマンドにインターフェイスの名前を含めると、指定したインターフェイスのカウンタだけが消去されます。

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、IGMP 統計情報カウンタを消去します。

```
hostname# clear igmp counters
```

関連コマンド

コマンド	説明
clear igmp group	検出されたグループを IGMP グループ キャッシュから消去します。
clear igmp traffic	IGMP トラフィック カウンタを消去します。

clear igmp group

IGMP グループ キャッシュから検出されたグループを消去するには、特権 EXEC モードで **clear igmp** コマンドを使用します。

clear igmp group [*group* | ***interface*** *name*]

シンタックスの説明

group	IGMP グループ アドレス。キャッシュから指定したグループを削除する特定のグループを指定します。
interface *name*	**namif** コマンドで指定されたインターフェイスの名前。指定した場合は、インターフェイスに関連付けられたすべてのグループが削除されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

グループまたはインターフェイスを指定しない場合は、すべてのインターフェイスからすべてのグループが消去されます。グループを指定した場合は、そのグループのエントリだけが消去されます。インターフェイスを指定した場合は、そのインターフェイスのすべてのグループが消去されます。グループとインターフェイスの両方を指定した場合は、指定したインターフェイスの指定したグループだけが消去されます。

このコマンドはスタティックに設定されたグループを消去しません。

例

次の例では、IGMP グループ キャッシュから検出されたすべての IGMP グループを消去する方法を示します。

```
hostname# clear igmp group
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP カウンタを消去します。
clear igmp traffic	IGMP トラフィック カウンタを消去します。

clear igmp traffic

IGMP トラフィック カウンタを消去するには、特権 EXEC モードで **clear igmp traffic** コマンドを使用します。

clear igmp traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、IGMP 統計情報トラフィック カウンタを消去します。

```
hostname# clear igmp traffic
```

関連コマンド

コマンド	説明
clear igmp group	検出されたグループを IGMP グループ キャッシュから消去します。
clear igmp counters	すべての IGMP カウンタを消去します。

clear interface

インターフェイス統計情報を消去するには、特権 EXEC モードで **clear interface** コマンドを使用します。

clear interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトでは、このコマンドはすべてのインターフェイス統計情報を消去します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear interface コマンドは、入力バイト数以外のインターフェイスの統計情報をすべて消去します。インターフェイス統計情報の詳細については、**show interface** コマンドを参照してください。

インターフェイスがコンテキスト間で共有されている場合にコンテキスト内でこのコマンドを入力すると、セキュリティ アプライアンスは現在のコンテキストの統計情報だけを消去します。システム実行スペースでこのコマンドを入力した場合、セキュリティ アプライアンスは結合された統計情報を消去します。

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内でのみ使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内でのみ使用できます。

例

次の例では、インターフェイス統計情報をすべて消去します。

```
hostname# clear interface
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイス コンフィギュレーションを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。

clear ip audit count

監査ポリシーの一致するシグニチャ数を消去するには、特権 EXEC モードで **clear ip audit count** コマンドを使用します。

clear ip audit count [**global** | **interface** *interface_name*]

シンタックスの説明

global	（デフォルト）すべてのインターフェイスの一致する数を消去します。
interface interface_name	（オプション）指定したインターフェイスの一致する数を消去します。

デフォルト

キーワードを指定しない場合、このコマンドはすべてのインターフェイスの一致を消去します（***global***）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、すべてのインターフェイスの数を消去します。

```
hostname# clear ip audit count
```

関連コマンド

コマンド	説明
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show ip audit count	監査ポリシーの一致するシグニチャの数を表示します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

clear ip verify statistics

Unicast RPF 統計情報を消去するには、特権 EXEC モードで **clear ip verify statistics** コマンドを使用します。Unicast RPF をイネーブルにするには、**ip verify reverse-path** コマンドを参照してください。

clear ip verify statistics [**interface** *interface_name*]

シンタックスの説明

interface *interface_name*	Unicast RPF 統計情報を消去するインターフェイスを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、Unicast RPF 統計情報を消去します。

```
hostname# clear ip verify statistics
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを消去します。
ip verify reverse-path	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
show ip verify statistics	Unicast RPF の統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

clear ipsec sa

IPSec SA を完全に消去、または指定したパラメータに基づいて消去するには、グローバル コンフィギュレーション モードおよび特権 EXEC モードで **clear ipsec sa** コマンドを使用します。代替の形式 **clear crypto ipsec sa** も使用できます。

clear ipsec sa [***counters*** **|** **entry** *peer-addr protocol spi* | **peer** *peer-addr* | **map** *map-name*]

シンタックスの説明

counters	（オプション）すべてのカウンタを消去します。
entry	（オプション）指定した IPSec ピア、プロトコル、および SPI の IPSec SA を消去します。
map *map-name*	（オプション）指定した暗号マップの IPSec SA を消去します。
peer	（オプション）指定したピアの IPSec SA を消去します。
peer-addr	IPSec ピアの IP アドレスを指定します。
protocol	IPSec プロトコル ***esp*** または **ah** を指定します。
spi	IPSec SPI を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

グローバル コンフィギュレーション モードで入力した次の例では、すべての IPSec SA カウンタを消去します。

```
hostname(config)# clear ipsec sa counters
hostname(config)#
```

関連コマンド

コマンド	説明
show ipsec sa	指定したパラメータに基づいて IPSec SA を表示します。
show ipsec stats	IPSec フロー MIB からのグローバル IPSec 統計情報を表示します。

clear ipv6 access-list counters

IPv6 アクセス リスト統計情報カウンタを消去するには、特権 EXEC モードで **clear ipv6 access-list counters** コマンドを使用します。

clear ipv6 access-list *id* ***counters***

シンタックスの説明

id	IPv6 アクセス リストの識別子。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、IPv6 アクセス リスト 2 の統計情報データを消去する方法を示します。

```
hostname# clear ipv6 access-list 2 counters
hostname#
```

関連コマンド

コマンド	説明
clear configure ipv6	現在のコンフィギュレーションから **ipv6 access-list** コマンドを消去します。
ipv6 access-list	IPv6 アクセス リストを設定します。
show ipv6 access-list	現在のコンフィギュレーションにある **ipv6 access-list** コマンドを表示します。

clear ipv6 neighbors

IPv6 近隣探索キャッシュを消去するには、特権 EXEC モードで **clear ipv6 neighbors** コマンドを使用します。

clear ipv6 neighbors

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、検出されたすべての IPv6 近隣をキャッシュから削除します。スタティック エントリは削除しません。

例

次の例では、スタティック エントリを除く、IPv6 近隣探索キャッシュ内のすべてのエントリを削除します。

```
hostname# clear ipv6 neighbors
hostname#
```

関連コマンド

コマンド	説明
ipv6 neighbor	IPv6 探索キャッシュにスタティック エントリを設定します。
show ipv6 neighbor	IPv6 近隣キャッシュ情報を表示します。

clear ipv6 traffic

IPv6 トラフィック カウンタをリセットするには、特権 EXEC モードで **clear ipv6 traffic** コマンドを使用します。

clear ipv6 traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、show ipv6 traffic コマンドからの出力のカウンタがリセットされます。

例

次の例では、IPv6 トラフィック カウンタをリセットします。**ipv6 traffic** コマンドからの出力は、カウンタがリセットされることを示します。

```
hostname# clear ipv6 traffic
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  1 total, 1 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         0 fragments, 0 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  1 generated, 0 forwarded
         0 fragmented into 0 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 0 received, 0 sent

ICMP statistics:
  Rcvd: 1 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert
  Sent: 1 output
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 0 router advert, 0 redirects
        0 neighbor solicit, 1 neighbor advert

UDP statistics:
  Rcvd: 0 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 0 output

TCP statistics:
  Rcvd: 0 input, 0 checksum errors
  Sent: 0 output, 0 retransmitted
```

関連コマンド

コマンド	説明
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

clear isakmp sa

すべての IKE ランタイム SA データベースを削除するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear isakmp sa** コマンドを使用します。

clear isakmp sa

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**clear isakmp sa** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**clear crypto isakmp sa** コマンドに置き換えられました。

例

次の例では、コンフィギュレーションから IKE ランタイム SA データベースを削除します。

```
hostname<config># clear isakmp sa
hostname<config>#
```

関連コマンド

コマンド	説明
clear isakmp	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp stats	実行時の統計情報を表示します。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

clear local-host

show local-host コマンドを入力することによって表示されるローカル ホストからネットワーク接続を解放するには、特権 EXEC モードで **clear local-host** コマンドを使用します。

clear local-host [*ip_address*] [**all**]

シンタックスの説明

all	（オプション）セキュリティ アプライアンスへの接続およびセキュリティ アプライアンスからの接続を含むローカル ホスト状態のホストが作成した接続を消去することを指定します。
ip_address	（オプション）ローカル ホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear local-host コマンドは、消去されたホストをライセンス制限から除外します。ライセンス制限にカウントされているホストの数は、**show local-host** コマンドを入力して表示できます。

注意　ローカル ホストのネットワーク状態を消去すると、ローカル ホストに関連するネットワーク接続と xlate がすべて停止します。

例

次の例では、**clear local-host** コマンドでローカル ホストに関する情報を消去する方法を示します。

```
hostname# clear local-host 10.1.1.15
```

情報が消去されると、ホストが接続を再び確立するまで、何も表示されません。

関連コマンド

コマンド	説明
show local-host	ローカル ホストのネットワーク状態を表示します。

clear logging asdm

ASDM ロギング バッファを消去するには、特権 EXEC モードで **clear logging asdm** コマンドを使用します。

clear logging asdm

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	**show pdm logging** コマンドが **show asdm log** コマンドに変更されました。

使用上のガイドライン

ASDM システム ログ メッセージは、セキュリティ アプライアンス システム ログ メッセージとは別のバッファに保存されます。ASDM ロギング バッファを消去すると、ASDM システム ログ メッセージだけが消去されます。セキュリティ アプライアンスのシステム ログ メッセージは消去されません。ASDM システム ログ メッセージを表示するには、**show asdm log** コマンドを使用します。

例

次の例では、ASDM ロギング バッファを消去します。

```
hostname(config)# clear logging asdm
hostname(config)#
```

関連コマンド

コマンド	説明
show asdm log_sessions	ASDM ロギング バッファの内容を表示します。

clear logging buffer

ロギング バッファを消去するには、グローバル コンフィギュレーション モードで **clear logging buffer** コマンドを使用します。

clear logging buffer

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

例

次の例は、ログ バッファの内容を消去する方法を示しています。

```
hostname # clear logging buffer
```

関連コマンド

コマンド	説明
logging buffered	ロギングを設定します。
show logging	ロギング情報を表示します。

clear mac-address-table

ダイナミック MAC アドレス テーブル エントリを消去するには、特権 EXEC モードで **clear mac-address-table** コマンドを使用します。

clear mac-address-table [*interface_name*]

シンタックスの説明

interface_name	（オプション）選択したインターフェイスの MAC アドレス テーブル エントリを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ダイナミック MAC アドレス テーブル エントリを消去します。

```
hostname# clear mac-address-table
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

clear memory delayed-free-poisoner

delayed free-memory poisoner ツールのキューと統計情報を消去するには、特権 EXEC モードで ***clear memory delayed-free-poisoner*** コマンドを使用します。

clear memory delayed-free-poisoner

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear memory delayed-free-poisoner コマンドは、delayed free-memory poisoner ツールのキューで保持されているメモリをすべて検証なしでシステムに戻し、関連のある統計情報カウンタを消去します。

例

次の例では、delayed free-memory poisoner ツールのキューと統計情報を消去します。

```
hostname# clear memory delayed-free-poisoner
```

関連コマンド

コマンド	説明
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキューを検証します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況について要約を表示します。

clear memory profile

メモリ プロファイリング機能によって保持されるメモリ バッファを消去するには、特権 EXEC コンフィギュレーション モードで ***clear memory profile*** コマンドを使用します。

clear memory profile [peak]

シンタックスの説明

peak	（オプション）ピーク メモリ バッファの内容を消去します。

デフォルト

デフォルトで現在「使用されている」プロファイル バッファを消去します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

clear memory profile コマンドはプロファイリング機能によって保持されるメモリ バッファを解放するため、消去する前にプロファイリングを停止する必要があります。

例

次の例では、プロファイリング機能によって保持されるメモリ バッファを消去します。

```
hostname# clear memory profile
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況のモニタリング（メモリ プロファイリング）をイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。

clear mfib counters

MFIB ルータ パケット カウンタを消去するには、特権 EXEC モードで **clear mfib counters** コマンドを使用します。

clear mfib counters [*group* [*source*]]

シンタックスの説明

group	（オプション）マルチキャスト グループの IP アドレス。
source	（オプション）マルチキャスト ルート送信元の IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。

デフォルト

このコマンドを引数なしで使用した場合、すべてのルートのルート カウンタが消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、すべての MFIB ルータ パケットのカウンタを消去します。

```
hostname# clear mfib counters
```

関連コマンド

コマンド	説明
show mfib count	MFIB ルートおよびパケット カウントのデータを表示します。

clear module recover

hw-module module recover コマンドで設定された AIP SSM のリカバリ ネットワーク設定を消去するには、特権 EXEC モードで **clear module recover** コマンドを使用します。

clear module 1 recover

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、AIP SSM のリカバリ設定を消去します。

```
hostname# clear module 1 recover
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、AIP SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	AIP SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

clear ospf

OSPF プロセス情報を消去するには、特権 EXEC モードで **clear ospf** コマンドを使用します。

clear ospf [*pid*] {***process*** | ***counters*** [***neighbor*** [*neighbor-intf*] [*neighbr-id*]]}

シンタックスの説明

counters	OSPF カウンタを消去します。
neighbor	OSPF 隣接カウンタを消去します。
neighbor-intf	（オプション）OSPF インターフェイス ルータ指定を消去します。
neighbr-id	（オプション）OSPF 隣接ルータ ID を消去します。
pid	（オプション）OSPF ルーティング プロセス用に内部的に使用される ID パラメータ。有効値は、1 ～ 65535 です。
process	OSPF ルーティング プロセスを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドはコンフィギュレーションのいずれの部分も削除しません。コンフィギュレーションから特定のコマンドを消去するには、コンフィギュレーション コマンドの **no** 形式を使用します。または、コンフィギュレーションからすべてのグローバル OSPF コマンドを削除するには、**clear configure router ospf** コマンドを使用します。

（注） **clear configure router ospf** コマンドは、インターフェイス コンフィギュレーション モードで入力された OSPF コマンドを消去しません。

例

次の例では、OSPF プロセス カウンタを消去する方法を示します。

```
hostname# clear ospf process
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべてのグローバル ルータ コマンドを消去します。

clear pc

PC 上に保持されている接続情報、xlate 情報、またはローカル ホスト情報を消去するには、グローバル コンフィギュレーション モードで **clear pc** コマンドを使用します。

clear pc

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、PC 情報を消去します。

```
hostname(config)# clear pc
```

関連コマンド

コマンド	説明
clear pclu	PC 論理アップデート統計情報を消去します。

clear pclu

PC 論理アップデート統計情報を消去するには、グローバル コンフィギュレーション モードで **clear pclu** コマンドを使用します。

clear pclu

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、PC 情報を消去します。

```
hostname(config)# clear pclu
```

関連コマンド

コマンド	説明
clear pc	PC 上に保持されている接続情報、xlate 情報、またはローカル ホスト情報を消去します。

clear pim counters

PIM トラフィック カウンタを消去するには、特権 EXEC モードで **clear pim counters** コマンドを使用します。

clear pim counters

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、トラフィック カウンタだけを消去します。PIM トポロジ テーブルを消去するには、**clear pim topology** コマンドを使用します。

例

次の例では、PIM トラフィック カウンタを消去します。

```
hostname# clear pim counters
```

関連コマンド

コマンド	説明
clear pim reset	リセットによって MRIB の同期化を強制します。
clear pim topology	PIM トポロジ テーブルを消去します。
show pim traffic	PIM トラフィック カウンタを表示します。

clear pim reset

リセットによって MRIB の同期化を強制するには、特権 EXEC モードで **clear pim reset** コマンドを使用します。

clear pim reset

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トポロジ テーブルからのすべての情報が消去され、MRIB 接続がリセットされます。このコマンドは、PIM トポロジ テーブルと MRIB データベース間の状態を同期化するために使用できます。

例

次の例では、トポロジ テーブルを消去し、MRIB 接続をリセットします。

```
hostname# clear pim reset
```

関連コマンド

コマンド	説明
clear pim counters	PIM のカウンタおよび統計情報を消去します。
clear pim topology	PIM トポロジ テーブルを消去します。
clear pim counters	PIM トラフィック カウンタを消去します。

clear pim topology

PIM トポロジ テーブルを消去するには、特権 EXEC モードで **clear pim topology** コマンドを使用します。

clear pim topology [*group*]

シンタックスの説明

group	（オプション）トポロジ テーブルから削除するマルチキャスト グループのアドレスまたは名前を指定します。

デフォルト

任意の *group* 引数を指定しない場合、トポロジ テーブルからすべてのエントリが消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルから既存の PIM ルートを消去します。IGMP ローカル メンバーシップなど、MRIB テーブルから取得した情報は保持されます。マルチキャスト グループを指定した場合は、それらのグループ エントリだけが消去されます。

例

次の例では、PIM トポロジ テーブルを消去します。

```
hostname# clear pim topology
```

関連コマンド

コマンド	説明
clear pim counters	PIM のカウンタおよび統計情報を消去します。
clear pim reset	リセットによって MRIB の同期化を強制します。
clear pim counters	PIM トラフィック カウンタを消去します。

clear priority-queue statistics

インターフェイスまたは設定されたすべてのインターフェイスのプライオリティ キュー統計情報カウンタを消去するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **clear priority-queue statistics** コマンドを使用します。

clear priority-queue statistics [*interface-name*]

シンタックスの説明

interface-name	（オプション）ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合、このコマンドは設定されたすべてのインターフェイスのプライオリティ キュー統計情報を消去します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、特権 EXEC モードで **clear priority-queue statistics** コマンドを使用して、「test」という名前のインターフェイスのプライオリティ キュー統計情報を削除します。

```
hostname# clear priority-queue statistics test
hostname#
```

関連コマンド

コマンド	説明
clear configure priority queue	指定したインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイスまたはすべてのインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

clear resource usage

リソース使用状況の統計情報を消去するには、特権 EXEC モードで **clear resource usage** コマンドを使用します。

clear resource usage [**context** *context_name* | **all** | **summary** | **system**] [**resource** {[**rate**] *resource_name* | **all**}]

シンタックスの説明

context *context_name*	（マルチモードのみ）統計情報を消去するコンテキスト名を指定します。すべてのコンテキストを対象にするには、**all**（デフォルト）を指定します。
resource [**rate**] *resource_name*	特定のリソースの使用状況を消去します。すべてのリソースを対象にするには、***all***（デフォルト）を指定します。**rate** で、消去するリソースの使用率を指定します。比率で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソース タイプを指定する場合は、**rate** キーワードを指定する必要があります。conns リソースは、同時接続としても測定されます。1 秒間あたりの接続を表示するには、**rate** キーワードのみを使用します。 リソースには、次のタイプがあります。 • **asdm**：ASDM の管理セッション。 • conns：1 つのホストと複数の他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • **inspects**：アプリケーション検査。 • **hosts**：セキュリティ アプライアンスを通じて接続可能なホスト。 • **mac-addresses**：透過ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。 • **ssh**：SSH セッション。 • **syslogs**：システム ログ メッセージ。 • **telnet**：Telnet セッション。 • **xlates**：NAT 変換。
summary	（マルチモードのみ）結合されたコンテキスト統計情報を消去します。
system	（マルチ モードのみ）システム全体（グローバル）の使用状況の統計情報を消去します。

デフォルト

マルチ コンテキスト モードの場合、デフォルトのコンテキストは **all** です。これを指定することにより、すべてのコンテキストのリソース使用状況が消去されます。シングルモードの場合、コンテキスト名は無視され、すべてのリソース統計情報が消去されます。

デフォルトのリソース名は **all** で、すべてのリソース タイプが消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、システム全体の使用状況の統計情報を除き、全コンテキストの全リソース使用状況の統計情報を消去します。

```
hostname# clear resource usage
```

次の例は、システム全体の使用状況の統計情報を消去します。

```
hostname# clear resource usage system
```

関連コマンド

コマンド	説明
context	セキュリティ コンテキストを追加します。
show resource types	リソース タイプのリストを表示します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

clear route

コンフィギュレーションからダイナミックにラーニングされたルートを削除するには、特権 EXEC モードで **clear route** コマンドを使用します。

clear route [*interface_name*]

シンタックスの説明

interface_name	（オプション）内部または外部のネットワーク インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、ダイナミックにラーニングされたルートを削除する方法を示します。

```
hostname# clear route
```

関連コマンド

コマンド	説明
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

clear service-policy

イネーブルになっているポリシーの運用データまたは統計情報（存在する場合）を消去するには、特権 EXEC モードで ***clear service-policy*** コマンドを使用します。検査エンジンのサービス ポリシーの統計情報を消去する方法については、**clear service-policy inspect** コマンドを参照してください。

clear service-policy [**global** | **interface** *intf*]

シンタックスの説明

global	（オプション）グローバル サービス ポリシーの統計情報を消去します。
interface *intf*	（オプション）特定のインターフェイスのサービス ポリシーの統計情報を消去します。

デフォルト

デフォルトでは、このコマンドはすべてのイネーブルなサービス ポリシーの統計情報をすべて消去します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、***clear service-policy*** コマンドのシンタックスを示します。

```
hostname(config)# clear service-policy outside_security_map interface outside
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	GTP 検査エンジンのサービス ポリシーの統計情報を消去します。
clear service-policy inspect radius-accounting	RADIUS アカウンティング検査エンジンのサービス ポリシーの統計情報を消去します。
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションを消去します。
service-policy	サービス ポリシーを設定します。

clear service-policy inspect gtp

グローバル GTP 統計情報を消去するには、特権 EXEC モードで **clear service-policy inspect gtp** コマンドを使用します。

clear service-policy inspect gtp {**pdp-context** [**all** | **apn** *ap_name* | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | **requests** | **statistics** [**gsn** *IP_address*] }

シンタックスの説明

all	すべての GTP PDP コンテキストを消去します。
apn	（オプション）指定した APN に基づいて PDP コンテキストを消去します。
ap_name	特定のアクセス ポイント名を指定します。
gsn	（オプション）GPRS 無線データ ネットワークと他のネットワーク間のインターフェイスである GPRS サポート ノードを指定します。
gtp	（オプション）GTP のサービス ポリシーを消去します。
imsi	（オプション）指定した IMSI に基づいて PDP コンテキストを消去します。
IMSI_value	特定の IMSI を識別する 16 進値。
interface	（オプション）特定のインターフェイスを指定します。
int	情報を消去するインターフェイスを指定します。
IP_address	統計情報を消去する IP アドレス。
ms-addr	（オプション）指定した MS アドレスに基づいて PDP コンテキストを消去します。
pdp-context	（オプション）パケット データ プロトコル コンテキストを指定します。
requests	（オプション）GTP 要求を消去します。
statistics	（オプション）**inspect gtp** コマンドの GTP 統計情報を消去します。
tid	（オプション）指定した TID に基づいて PDP コンテキストを消去します。
tunnel_ID	特定のトンネルを識別する 16 進値。
version	（オプション）GTP バージョンに基づいて PDP コンテキストを消去します。
version_num	PDP コンテキストのバージョンを指定します。有効な範囲は 0 ～ 255 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケット データ プロトコル コンテキストは、IMSI と NSAPI の組み合せであるトンネル ID によって識別されます。GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、パケットを外部パケット データ ネットワークとモバイル ステーション（MS）ユーザの間で転送するために必要なものです。

例

次の例では、GTP 統計情報を消去します。

```
hostname# clear service-policy inspect gtp statistics
```

関連コマンド

コマンド	説明
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査用に GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。
show running-config gtp-map	設定されている GTP マップを表示します。

clear service-policy inspect radius-accounting

RADIUS アカウンティングの統計情報を消去するには、特権 EXEC モードで **clear service-policy inspect radius-accounting** コマンドを使用します。

clear service-policy inspect radius-accounting { }

シンタックスの説明

all

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

例

次の例は、RADIUS アカウンティングの統計情報を消去します。

```
hostname# clear service-policy inspect radius-accounting statistics
```

関連コマンド

コマンド	説明

clear shun

現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去するには、特権 EXEC モードで **clear shun** コマンドを使用します。

clear shun [*statistics*]

シンタックスの説明

statistics	（オプション）インターフェイス カウンタだけを消去します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去する方法を示します。

```
hostname(config)# clear shun
```

関連コマンド

コマンド	説明
shun	新しい接続を阻止し、既存の接続からのパケットを拒否することによって、攻撃ホストへのダイナミックな応答をイネーブルにします。
show shun	排除情報を表示します。

clear startup-config errors

メモリからコンフィギュレーション エラー メッセージを消去するには、特権 EXEC モードで **clear startup-config errors** コマンドを使用します。

clear startup-config errors

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示するには、**show startup-config errors** コマンドを使用します。

例

次の例では、メモリからすべてのコンフィギュレーション エラーを消去します。

```
hostname# clear startup-config errors
```

関連コマンド

コマンド	説明
show startup-config errors	セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたコンフィギュレーション エラーを表示します。

clear sunrpc-server active

Sun RPC アプリケーション検査によって開けられたピンホールを消去するには、グローバル コンフィギュレーション モードで **clear sunrpc-server active** コマンドを使用します。

clear sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

Sun RPC アプリケーション検査によって開けられた、NFS や NIS などのサービス トラフィックがセキュリティ　アプライアンスを通過できるようにするピンホールを消去するには、**clear sunrpc-server active** コマンドを使用します。

例

次の例では、Sun RPC サービス テーブルを消去する方法を示します。

```
hostname(config)# clear sunrpc-server
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスから Sun リモート プロセッサ コール サービスを消去します。
inspect sunrpc	Sun RPC アプリケーション検査をイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	Sun RPC サービスのコンフィギュレーションに関する情報を表示します。
show sunrpc-server active	アクティブな Sun RPC サービスに関する情報を表示します。

clear traffic

送信アクティビティおよび受信アクティビティのカウンタをリセットするには、特権 EXEC モードで ***clear traffic*** コマンドを使用します。

clear traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear traffic コマンドは、***show traffic*** コマンドで表示される送信アクティビティおよび受信アクティビティのカウンタをリセットします。このカウンタは、最後に clear traffic コマンドが入力されてから、またはセキュリティ アプライアンスがオンラインになってから、各インターフェイスを通過したパケット数およびバイト数を示します。秒数は、最後にリブートされてからセキュリティ アプライアンスがオンラインである時間を示します。

例

次に、**clear traffic** コマンドの例を示します。

```
hostname# clear traffic
```

関連コマンド

コマンド	説明
show traffic	送信アクティビティおよび受信アクティビティのカウンタを表示します。

clear uauth

1 人のユーザまたはすべてのユーザのすべてのキャッシュされた認証および認可情報を削除するには、特権 EXEC モードで **clear uauth** コマンドを使用します。

clear uauth [*username*]

シンタックスの説明

username	（オプション）削除するユーザ認証情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認証および認可情報が削除されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear uauth コマンドは、1 人またはすべてのユーザの AAA 認可および認証のキャッシュを削除します。そのため、ユーザが次回接続を作成するときに、再認証が必要になります。

timeout コマンドと共に使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。ユーザが適切なホストから、キャッシュされたサービスにアクセスしようとすると、セキュリティ アプライアンスはユーザを認可済みであると見なし、すぐに接続を代理処理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、各イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。このプロセスにより、認可サーバ上でパフォーマンスが大幅に向上し、負荷も大幅に軽減されます。

ユーザ ホストごとにアドレスとサービスのペアを最大 16 個までキャッシュできます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能と共に Xauth を使用すると、ネットワーク間に IPSec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウンティング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、AAA コマンドを参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次の例では、ユーザ「Lee」が再認証されるようにする方法を示します。

```
hostname(config)# clear uauth lee
```

関連コマンド

コマンド	説明
aaa authentication	**aaa-server** コマンドで指定されたサーバ上の LOCAL、TACACS+、または RADIUS のユーザ認証をイネーブル化、ディセーブル化、または表示します。
aaa authorization	**aaa-server** コマンドで指定されたサーバ上の TACACS+ または RADIUS のユーザ認可をイネーブル化、ディセーブル化、または表示します。
show uauth	現在のユーザ認証および認可情報を表示します。
timeout	アイドル状態の最大継続時間を設定します。

clear url-block block statistics

ブロック バッファ使用状況カウンタを消去するには、特権 EXEC モードで **clear url-block block statistics** コマンドを使用します。

clear url-block block statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear url-block block statistics コマンドは、`Current number of packets held (global)` カウンタ以外のブロック バッファ使用状況カウンタを消去します。

例

次の例では、URL ブロック統計情報を消去し、消去後のカウンタの状態を表示します。

```
hostname# clear url-block block statistics
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  0
----------------------------------------------------
Cumulative number of packets held: | 0
Maximum number of packets held (per URL): | 0
Current number of packets held (global): | 38
Packets dropped due to
 | exceeding url-block buffer limit: | 0
 | HTTP server retransmission: | 0
Number of packets released back to client: | 0
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear url-cache statistics

コンフィギュレーションから **url-cache** コマンド文を削除するには、特権 EXEC モードで **clear url-cache** コマンドを使用します。

clear url-cache statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear url-cache コマンドは、コンフィギュレーションから **url-cache** 統計情報を削除します。

URL キャッシュを使用しても、Websense プロトコル Version 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル Version 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。セキュリティの要求に合致する使用状況プロファイルを取得した後、**| url-cache** コマンドを入力してスループットを向上させます。Websense プロトコル Version 4 および N2H2 URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログがアップデートされます。

例

次の例では、URL キャッシュ統計情報を消去します。

```
hostname# clear url-cache statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear url-server

URL フィルタリング サーバの統計情報を消去するには、特権 EXEC モードで **clear url-server** コマンドを使用します。

clear url-server statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear url-server コマンドは、コンフィギュレーションから URL フィルタリング サーバの統計情報を削除します。

例

次の例では、URL サーバの統計情報を消去します。

```
hostname# clear url-server statistics
```

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

clear wccp

WCCP 情報をリセットするには、特権 EXEC モードで **clear wccp** コマンドを使用します。

clear wccp [***web-cache*** | *service_number*]

シンタックスの説明

web-cache	Web キャッシュ サービスを指定します。
service-number	動的サービス ID。このサービスの定義は、キャッシュによって示されます。動的サービスの番号は 0 ～ 254 まで、最高 255 個です。***web-cache*** キーワードで指定する Web キャッシュ サービスを含め、256 個までに制限されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、Web キャッシュ サービスの WCCP 情報をリセットする方法を示しています。

```
hostname(config)# clear wccp web-cache
```

関連コマンド

コマンド	説明
show wccp	WCCP のコンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

clear xlate

現在の変換情報および接続情報を消去するには、特権 EXEC モードで **clear xlate** コマンドを使用します。

clear xlate [***global*** *ip1*[*-ip2*] [***netmask*** *mask*]] [***local*** *ip1*[*-ip2*] [***netmask*** *mask*]][***gport*** *port1*[*-port2*]] [***lport*** *port1*[*-port2*]] [***interface*** *if_name*] [***state*** *state*]

シンタックスの説明

global *ip1*[*-ip2*]	（オプション）アクティブな変換をグローバル IP アドレスまたはアドレスの範囲別に消去します。
gport *port1*[*-port2*]	（オプション）アクティブな変換をグローバル ポートまたはポートの範囲別に消去します。
interface *if_name*	（オプション）アクティブな変換をインターフェイス別に表示します。
local *ip1*[*-ip2*]	（オプション）アクティブな変換をローカル IP アドレスまたはアドレスの範囲別に消去します。
lport *port1*[*-port2*]	（オプション）アクティブな変換をローカル ポートまたはポートの範囲別に消去します。
netmask *mask*	（オプション）グローバル IP アドレスまたはローカル IP アドレスを限定するネットワーク マスクを指定します。
state *state*	（オプション）アクティブな変換を状態別に消去します。次の状態を 1 つまたは複数入力できます。 • ***static***：**スタティック**変換を指定します。 • ***portmap***：PAT グローバル変換を指定します。 • ***norandomseq***：***norandomseq*** 設定での **nat** またはスタティック変換を指定します。 • ***identity***：**nat 0** 識別アドレス変換を指定します。 複数の状態を指定する場合は、状態をスペースで区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clear xlate コマンドは、変換スロットの内容を消去します（「xlate」は変換スロットを意味します）。変換スロットは、キーの変更後も残ります。コンフィギュレーション内で **aaa-server**、**access-list**、**alias**、**global**、**nat**、**route**、または **static** コマンドを追加、変更、または削除した後には、必ず **clear xlate** コマンドを使用します。

xlate は、NAT または PAT セッションを示します。これらのセッションは、***detail*** オプションの **show xlate** コマンドで表示できます。xlate には、スタティックとダイナミックの 2 種類があります。

スタティック xlate は、**static** コマンドを使用して作成される固定の xlate です。スタティック xlate は、コンフィギュレーションから **static** コマンドを削除することによってのみ削除できます。**clear xlate** は、スタティック変換規則を削除しません。コンフィギュレーションから **static** コマンドを削除しても、スタティック規則を使用する既存の接続はトラフィックを転送できます。これらの接続を無効にするには、**clear local-host** を使用します。

ダイナミック xlate は、**nat** または **global** コマンドを使用して、トラフィック処理によってオンデマンドで作成されます。**clear xlate** は、ダイナミック xlate および関連付けられた接続を削除します。また、**clear local-host** コマンドを使用して、xlate および関連付けられた接続を消去することもできます。コンフィギュレーションから **nat** または **global** コマンドを削除しても、ダイナミック xlate および関連付けられた接続はアクティブのままとなる場合があります。これらの接続を削除するには、**clear xlate** または **clear local-host** コマンドを使用します。

例

次の例では、現在の変換スロット情報および接続スロット情報を消去する方法を示します。

```
hostname# clear xlate global
```

関連コマンド

コマンド	説明
clear local-host	ローカル ホストのネットワーク情報を消去します。
clear uauth	キャッシュされたユーザ認証および認可情報を消去します。
show conn	アクティブな接続をすべて表示します。
show local-host	ローカル ホストのネットワーク情報を表示します。
show xlate	現在の変換情報を表示します。

CHAPTER 8

client-access-rule コマンド～ crl configure コマンド

client-access-rule

リモートアクセス クライアントのタイプを制限する規則およびセキュリティ アプライアンスを通して IPSec 経由で接続できるバージョンを設定するには、グループ ポリシー コンフィギュレーション モードで **client-access-rule** コマンドを使用します。規則を削除するには、このコマンドの **no** 形式を使用します。

すべての規則を削除するには、**no client-access-rule** コマンドの priority 引数だけを指定して使用します。この指定により、**client-access-rule none** コマンドを入力して作成されたヌル規則を含む、設定されたすべての規則が削除されます。

クライアントのアクセス規則がない場合、ユーザはデフォルトのグループ ポリシー内に存在するすべての規則を継承します。ユーザがクライアントのアクセス規則を継承しないようにするには、**client-access-rule none** コマンドを使用します。クライアントのアクセス規則を継承しない場合、すべてのクライアント タイプおよびバージョンに接続できます。

client-access-rule *priority* **{permit | deny} type** *type* **version** *version* **| none**

no client-access-rule *priority* [**{permit | deny} type** *type* **version** *version*]

シンタックスの説明

deny	特定のタイプとバージョンの両方またはいずれか一方のデバイスの接続を拒否します。
none	クライアントのアクセス規則を許可しません。client-access-rule をヌル値に設定して、制限を許可しません。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
permit	特定のタイプとバージョンの両方またはいずれか一方のデバイスの接続を許可します。
priority	規則の優先順位を決定します。最も小さい整数の規則が、一番高い優先順位となります。したがって、クライアント タイプとバージョンの両方またはいずれか一方に一致する最も小さい整数の規則が、適用される規則です。優先順位の低い規則が矛盾している場合、セキュリティ アプライアンスはその規則を無視します。

type *type*	VPN 3002 などの自由形式の文字列を利用して、デバイス タイプを指定します。* 記号をワイルドカードとして使用できる場合を除き、文字列は **show vpn-sessiondb remote** 表示の外観と完全に一致する必要があります。
version *version*	7.0(1) などの自由形式の文字列を使用して、デバイス バージョンを指定します。* 記号をワイルドカードとして使用できる場合を除き、文字列は **show vpn-sessiondb remote** 表示の外観と完全に一致する必要があります。

デフォルト

デフォルトでは、アクセス規則はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

次の注意に従って規則を作成します。

- 規則を定義しない場合、セキュリティ アプライアンスはすべての接続タイプを許可します。
- クライアントが規則のいずれにも一致しない場合、セキュリティ アプライアンスは接続を拒否します。つまり deny 規則を定義する場合は、少なくとも 1 つの permit 規則も定義する必要があります。permit 規則を定義しないと、セキュリティ アプライアンスはすべての接続を拒否します。
- ソフトウェア クライアントとハードウェア クライアントのどちらも、タイプおよびバージョンが **show vpn-sessiondb remote** 表示の外観と完全に一致する必要があります。
- * 記号はワイルドカードで、各規則内で複数回使用できます。たとえば、**client-access-rule 3 deny type * version 3.*** は、リリース バージョン 3.x ソフトウェアを実行しているすべてのクライアント タイプを拒否する優先順位 3 のクライアントのアクセス規則を作成します。
- 1 つのグループ ポリシーにつき最大 25 の規則を作成できます。
- 一連の規則全体に 255 文字の制限があります。
- クライアント タイプとバージョンの両方またはいずれか一方を送信しないクライアントに n/a を使用できます。

例

次の例では、FirstGroup という名前のグループ ポリシーのクライアントのアクセス規則を作成する方法を示します。これらの規則は、ソフトウェア バージョン 4.1 を実行している VPN クライアントを許可する一方、すべての VPN 3002 ハードウェア クライアントを拒否します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-access-rule 1 d t VPN3002 v *
hostname(config-group-policy)# client-access-rule 2 p * v 4.1
```

client-firewall

セキュリティ アプライアンスが IKE トンネルのネゴシエーション中に VPN クライアントにプッシュするパーソナル ファイアウォール ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **client-firewall** コマンドを使用します。ファイアウォール ポリシーを削除するには、このコマンドの **no** 形式を使用します。

すべてのファイアウォール ポリシーを削除するには、引数を指定せずに **no client-firewall** コマンドを使用します。**client-firewall none** コマンドを発行して作成したヌル ポリシーを含む、すべての設定済みファイアウォール ポリシーが削除されます。

ファイアウォール ポリシーがなくなると、ユーザはデフォルトまたはその他のグループ ポリシー内に存在するファイアウォール ポリシーを継承します。ユーザがそれらのファイアウォール ポリシーを継承しないようにするには、**client-firewall none** コマンドを使用します。

client-firewall none

client-firewall {**opt** | **req**} **custom vendor-id** *num* **product-id** *num* **policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*} [**description** *string*]

client-firewall {**opt** | **req**} **zonelabs-integrity**

（注） ファイアウォールのタイプを **zonelabs-integrity** にする場合は、引数を指定しないでください。ポリシーは、Zone Labs Integrity サーバによって決められます。

client-firewall {**opt** | **req**} **zonelabs-zonealarm policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **zonelabs-zonealarmorpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **zonelabs-zonealarmpro policy** {**AYT** | **CPP acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **cisco-integrated acl-in** *acl* **acl-out** *acl*}

client-firewall {**opt** | **req**} **sygate-personal**

client-firewall {**opt** | **req**} **sygate-personal-pro**

client-firewall {**opt** | **req**} **sygate-personal-agent**

client-firewall {**opt** | **req**} **networkice-blackice**

client-firewall {**opt** | **req**} **cisco-security-agent**

シンタックスの説明

acl-in <*acl*>	クライアントが着信トラフィックに使用するポリシーを指定します。
acl-out <*acl*>	クライアントが発信トラフィックに使用するポリシーを指定します。
AYT	クライアント PC のファイアウォール アプリケーションがファイアウォール ポリシーを制御することを指定します。セキュリティ アプライアンスは、ファイアウォールが確実に実行されていることを確認します。「Are You There?」と表示され、応答がない場合、セキュリティ アプライアンスはトンネルを終了します。
cisco-integrated	Cisco Integrated ファイアウォール タイプを指定します。
cisco-security-agent	Cisco Intrusion Prevention Security Agent ファイアウォール タイプを指定します。

CPP	VPN クライアント ファイアウォール ポリシーのソースとしてプッシュされるポリシーを指定します。
custom	Custom ファイアウォール タイプを指定します。
description <*string*>	ファイアウォールについて説明します。
networkice-blackice	Network ICE Black ICE ファイアウォール タイプを指定します。
none	クライアント ファイアウォール ポリシーがないことを指定します。ファイアウォール ポリシーをヌル値に設定して、拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからファイアウォール ポリシーを継承しないようにします。
opt	オプションのファイアウォール タイプを指定します。
product-id	ファイアウォール製品を指定します。
req	必要なファイアウォール タイプを指定します。
sygate-personal	Sygate Personal ファイアウォール タイプを指定します。
sygate-personal-pro	Sygate Personal Pro ファイアウォール タイプを指定します。
sygate-security-agent	Sygate Security Agent ファイアウォール タイプを指定します。
vendor-id	ファイアウォールのベンダーを指定します。
zonelabs-integrity	Zone Labs Integrity サーバ ファイアウォール タイプを指定します。
zonelabs-zonealarm	Zone Labs Zone Alarm ファイアウォール タイプを指定します。
zonelabs-zonealarmorpro policy	Zone Labs Zone Alarm または Pro ファイアウォール タイプを指定します。
zonelabs-zonealarmpro policy	Zone Labs Zone Alarm Pro ファイアウォール タイプを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	**zonelabs-integrity** ファイアウォール タイプが追加されました。

使用上のガイドライン

このコマンドで設定できるインスタンスは 1 つだけです。

例

次の例では、FirstGroup という名前のグループ ポリシーの Cisco Intrusion Prevention Security Agent を必要とするクライアント ファイアウォール ポリシーを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# client-firewall req cisco-security-agent
```

client-update

全トンネル グループまたは特定のトンネル グループのアクティブなすべてのリモート VPN ソフトウェアとハードウェア クライアント、および Auto Update クライアントとして設定されているセキュリティ アプライアンス用のクライアント アップデートを発行するには、特権 EXEC モードで **client-update** コマンドを使用します。

クライアント アップデートのパラメータをグローバル レベル（VPN ソフトウェアとハードウェア クライアント、および Auto Update クライアントとして設定されているセキュリティ アプライアンスを含む）で設定および変更するには、グローバル コンフィギュレーション モードで **client-update** コマンドを使用します。

VPN ソフトウェアとハードウェア クライアント用のクライアント アップデート トンネル グループ IPSec アトリビュート パラメータを設定および変更するには、トンネル グループ ipsec アトリビュート コンフィギュレーション モードで **client-update** コマンドを使用します。

クライアントがリビジョン番号のリストにあるソフトウェア バージョンをすでに実行している場合は、ソフトウェアをアップデートする必要はありません。クライアントがリストにあるソフトウェア バージョンを実行していない場合は、アップデートする必要があります。

クライアント アップデートをディセーブルにするには、このコマンドの ***no*** 形式を使用します。

グローバル コンフィギュレーション モードのコマンドは、次のとおりです。

client-update {***enable*** | **component** {**asdm** | **image**} | **device-id** *dev_string* |**family** *family_name* | **type** *type*} ***url*** *url-string* ***rev-nums*** *rev-nums*}

no client-update {***enable*** | **component** {**asdm** | **image**} | **device-id** *dev_string* |**family** *family_name* | **type** *type*} ***url*** *url-string* ***rev-nums*** *rev-nums*}

トンネル グループ IPSec アトリビュート モードのコマンドは、次のとおりです。

client-update type *type* ***url*** *url-string* ***rev-nums*** *rev-nums*

no client-update type *type* ***url*** *url-string* ***rev-nums*** *rev-nums*

特権 EXEC モードのコマンドは、次のとおりです。

client-update {***all*** | *tunnel-group*}

no client-update *tunnel-group*

シンタックスの説明

all	（特権 EXEC モードでのみ使用可能）すべてのトンネル グループのすべてのアクティブ リモート クライアントにアクションを適用します。キーワード ***all*** をこのコマンドの ***no*** 形式で使用することはできません。
component {**asdm** | **image**}	Auto Update クライアントとして設定されているセキュリティ アプライアンスのソフトウェア コンポーネント。
device-id *dev_string*	Auto Update クライアント自体に固有の ID が付いている場合は、その文字列と同じものを指定します。最大長は 63 文字です。
enable	（グローバル コンフィギュレーション モードでのみ使用可能）リモート クライアントのソフトウェア アップデートをイネーブルにします。
family *family_name*	Auto Update クライアントをデバイス ファミリで識別するように設定している場合は、同じデバイス ファミリを指定します。これは、asa、pix、または 7 文字までの文字列です。

rev-nums *rev-nums*	（特権 EXEC モードでは使用不可）このクライアントのソフトウェア イメージまたはファームウェア イメージを指定します。Windows、WIN9X、WinNT、および vpn3002 クライアントは、任意の順番で 4 つまで、カンマで区切って指定できます。セキュリティ アプライアンスは、1 つしか指定できません。文字列の最大長は 127 文字です。
tunnel-group	（特権 EXEC モードでのみ使用可能）リモート クライアント アップデートの有効なトンネル グループの名前を指定します。
type *type*	（特権 EXEC モードでは使用不可）クライアントのアップデートを知らせるリモート PC のオペレーティング システムか、Auto Update として設定されているセキュリティ アプライアンスのタイプを指定します。次のものを指定できます。 • pix-515：Cisco PIX 515 Firewall • pix-515e：Cisco PIX 515E Firewall • pix-525：Cisco PIX 525 Firewall • pix-535：Cisco PIX 535 Firewall • asa5505：Cisco 5505 Adaptive Security Appliance • asa5510：Cisco 5510 Adaptive Security Appliance • asa5520：Cisco 5520 Adaptive Security Appliance • asa5540：Cisco Adaptive Security Appliance • Windows：Windows ベースのすべてのプラットフォーム • WIN9X：Windows 95、Windows 98、および Windows ME プラットフォーム • WinNT：Windows NT 4.0、Windows 2000、および Windows XP プラットフォーム • vpn3002：VPN 3002 ハードウェア クライアント • 15 文字までのテキスト文字列
url *url-string*	（特権 EXEC モードでは使用不可）ソフトウェア イメージまたはファームウェア イメージの URL を指定します。この URL は、このクライアントに応じたファイルを示す必要があります。URL の最大長は 255 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec アトリビュート コンフィギュレーション モードが追加されました。
7.2(1)	Auto Update サーバとして設定されたセキュリティ アプライアンスをサポートするために、**component**、**device-id**、および **family** キーワードとその引数が追加されました。

使用上のガイドライン

トンネル グループ ipsec アトリビュート コンフィギュレーション モードでは、このアトリビュートを IPSec リモートアクセス トンネル グループ タイプだけに適用できます。

client-update コマンドでは、アップデートのイネーブル化、アップデート適用先のクライアントのタイプとリビジョン番号の指定、アップデート取得先の URL または IP アドレスの指定が可能です。また、Windows クライアントの場合は、オプションで、VPN クライアント バージョンをアップデートする必要があることをユーザに通知できます。Windows クライアントに対しては、アップデートを実行するメカニズムをユーザに提供できます。VPN 3002 ハードウェア クライアント ユーザに対しては、アップデートは通知なしで自動的に実行されます。クライアントのタイプが別のセキュリティ アプライアンスの場合は、このセキュリティ アプライアンスが Auto Update サーバとして機能します。

クライアント アップデート メカニズムを設定するには、次の手順を実行します。

ステップ 1　グローバル コンフィギュレーション モードで、次のコマンドを入力してクライアント アップデートをイネーブルにします。

```
hostname(config)# client-update enable
hostname(config)#
```

ステップ 2　グローバル コンフィギュレーション モードで、特定のタイプのすべてのクライアントに適用するクライアント アップデート用のパラメータを設定します。つまり、クライアントのタイプと、最新イメージの取得先 URL または IP アドレスを指定します。Auto Update クライアントの場合は、ソフトウェア コンポーネントのタイプ（ASDM またはブート イメージ）を指定します。また、リビジョン番号も指定する必要があります。ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合は、そのクライアントをアップデートする必要はありません。このコマンドは、セキュリティ アプライアンス全体にわたって、指定したタイプのすべてのクライアントに適用されるクライアント アップデート パラメータを設定します。次の例を参考にしてください。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums
4.6.1
hostname(config)#
```

VPN 3002 ハードウェア クライアントのトンネル グループの設定については、「例」の項を参照してください。

（注）　すべての Windows クライアントと Auto Update クライアントで、URL のプレフィックスとして、「http://」または「https://」プロトコルを使用する必要があります。VPN3002 ハードウェア クライアントに対しては、代わりにプロトコル「tftp://」を指定する必要があります。

Windows クライアントと VPN3002 ハードウェア クライアントでは、特定のタイプの全クライアントではなく、個々のトンネル グループだけのクライアント アップデートを設定することもできます（ステップ 3 を参照）。

（注） ブラウザが自動的に起動されるように設定することができます。それには、URL の末尾にアプリケーション名を含めます（例：**https://support/updates/vpnclient.exe**）。

ステップ 3　クライアント アップデートをイネーブルにした後は、特定の ipsec-ra トンネル グループの一連のクライアント アップデート パラメータを定義できます。これを行うには、トンネル グループ ipsec アトリビュート モードで、トンネル グループの名前とタイプ、および最新イメージの取得先 URL または IP アドレスを指定します。また、リビジョン番号も指定する必要があります。ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合は、そのクライアントをアップデートする必要はありません。たとえば、すべての Windows クライアント用のクライアント アップデートを発行する必要はありません。

```
hostname(config)# tunnel-group remotegrp type ipsec-ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type windows url https://support/updates/
rev-nums 4.6.1
hostname(config-tunnel-ipsec)#
```

VPN 3002 ハードウェア クライアントのトンネル グループの設定については、「例」の項を参照してください。VPN 3002 クライアントは、ユーザの介入なしでアップデートされ、ユーザへの通知メッセージは送信されません。

ステップ 4　オプションで、古い Windows クライアントを使用しているアクティブ ユーザに、VPN クライアントをアップデートする必要があることを知らせる通知を送信できます。これらのユーザには、ポップアップ ウィンドウが表示されます。ユーザはこのポップアップ ウィンドウからブラウザを起動して、URL で指定されているサイトから最新のソフトウェアをダウンロードできます。このメッセージで設定可能な部分は URL だけです（ステップ 2 または 3 を参照）。アクティブでないユーザは、次回ログイン時に通知メッセージを受信します。この通知は、すべてのトンネル グループのすべてのアクティブ クライアントに送信することも、特定のトンネル グループのクライアントに送信することもできます。たとえば、すべてのトンネル グループのすべてのアクティブ クライアントに通知する場合は、次のコマンドを特権 EXEC モードで入力します。

```
hostname# client-update all
hostname#
```

ユーザのクライアント リビジョン番号が、指定したリビジョン番号のいずれかと一致する場合は、そのクライアントをアップデートする必要はありません。また、ユーザへの通知メッセージは送信されません。VPN 3002 クライアントは、ユーザの介入なしでアップデートされ、ユーザへの通知メッセージは送信されません。

（注） クライアント アップデートのタイプを ***windows***（Windows ベースの全プラットフォーム）に指定し、その後、同じエンティティに ***win9x*** タイプまたは ***winnt*** タイプを入力しなければならなくなった場合は、まずこのコマンドの **no** 形式で windows クライアント タイプを削除してから、新しい client-update コマンドを入力して新しいタイプのクライアントを指定してください。

例

グローバル コンフィギュレーション モードで入力した次の例では、すべてのトンネル グループのすべてのアクティブ リモート クライアントに対してクライアント アップデートをイネーブルにしています。

```
hostname(config)# client-update enable
hostname#
```

次の例は、Windows（win9x、winnt、または windows）にだけ適用されます。グローバル コンフィギュレーション モードで入力したこの例では、すべての Windows ベース クライアントのクライアント アップデート パラメータを設定します。リビジョン番号 4.7、および更新を取得する URL（https://support/updates）を指定します。

```
hostname(config)# client-update type windows url https://support/updates/ rev-nums 4.7
hostname(config)#
```

次の例は、VPN 3002 ハードウェア クライアントだけに適用されます。トンネル グループ ipsec アトリビュート コンフィギュレーション モードで入力されたこの例では、IPSec リモートアクセス トンネル グループ「salesgrp」のクライアント アップデート パラメータを設定します。リビジョン番号 4.7 を指定し、IP アドレス 192.168.1.1 を持つサイトからの最新ソフトウェアの取得に TFTP プロトコルを使用します。

```
hostname(config)# tunnel-group salesgrp type ipsec-ra
hostname(config)# tunnel-group salesgrp ipsec-attributes
hostname(config-tunnel-ipsec)# client-update type vpn3002 url tftp:192.168.1.1
rev-nums 4.7
hostname(config-tunnel-ipsec)#
```

次の例は、Auto Update クライアントとして設定されている Cisco 5520 Adaptive Security Appliance のクライアント アップデートを発行する方法を示します。

```
hostname(config)# client-update type asa5520 component asdm url
http://192.168.1.114/aus/asdm501.bin rev-nums 7.2(1)
```

特権 EXEC モードで入力した次の例では、「remotegrp」という名前のトンネル グループに属する、クライアント ソフトウェアをアップデートする必要のある接続中のすべてのリモート クライアントにクライアント アップデート通知を送信します。他のグループのクライアントには、アップデート通知は送信されません。

```
hostname# client-update remotegrp
hostname#
```

関連コマンド

コマンド	説明
clear configure client-update	client-update コンフィギュレーション全体を消去します。
show running-config client-update	現在の client-update コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

clock set

セキュリティ アプライアンスのクロックを手動で設定するには、特権 EXEC モードで **clock set** コマンドを使用します。

clock set *hh:mm:ss* {*month day* | *day month*} *year*

シンタックスの説明

day	1 ～ 31 の日を設定します。たとえば、標準の日付形式に応じて、月日を **april 1** や **1 april** のように入力できます。
hh:mm:ss	時、分、秒を 24 時間形式で設定します。たとえば、午後 8 時 54 分は **20:54:00** のように設定します。
month	月を設定します。標準の日付形式に応じて、月日を **april 1** や **1 april** のように入力できます。
year	4 桁で西暦年を設定します（たとえば、**2004**）。西暦年の範囲は 1993 ～ 2035 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

clock コンフィギュレーション コマンドを入力していない場合、**clock set** コマンドのデフォルトの時間帯は UTC です。**clock timezone** コマンドを使用して **clock set** コマンドを入力した後に時間帯を変更した場合、時間は自動的に新しい時間帯に調整されます。ただし、**clock timezone** コマンドを使用して時間帯を確立した後に **clock set** コマンドを入力した場合は、UTC ではなく新しい時間帯に応じた時間を入力します。同様に、**clock set** コマンドの後に **clock summer-time** コマンドを入力した場合、時間は夏時間に調整されます。**clock summer-time** コマンドの後に **clock set** コマンドを入力した場合は、夏時間の正しい時間を入力します。

このコマンドはハードウェア チップ内の時間を設定しますが、コンフィギュレーション ファイル内の時間は保存しません。この時間はリブート後も保持されます。他の **clock** コマンドとは異なり、このコマンドは特権 EXEC コマンドです。クロックをリセットするには、**clock set** コマンドに新しい時間を設定する必要があります。

例

次の例では、時間帯を MST に設定し、夏時間を米国のデフォルト期間に設定し、MDT の現在の時間を西暦 2004 年 7 月 27 日の午後 1 時 15 分に設定します。

```
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname(config)# exit
hostname# clock set 13:15:0 jul 27 2004
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

次の例では、クロックを UTC 時間帯で西暦 2004 年 7 月 27 日の 8 時 15 分に設定し、次に時間帯を MST に、夏時間を米国のデフォルト期間に設定します。終了時間（MDT の 1 時 15 分）は上記の例と同じです。

```
hostname# clock set 20:15:0 jul 27 2004
hostname# configure terminal
hostname(config)# clock timezone MST -7
hostname(config)# clock summer-time MDT recurring
hostname# show clock
13:15:00.652 MDT Tue Jul 27 2004
```

関連コマンド

コマンド	説明
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。
show clock	現在の時刻を表示します。

clock summer-time

セキュリティ アプライアンスの時間の表示用に夏時間の日付範囲を設定するには、グローバル コンフィギュレーション モードで **clock summer-time** コマンドを使用します。夏時間の日付をディセーブルにするには、このコマンドの **no** 形式を使用します。

clock summer-time *zone* ***recurring*** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*]

no clock summer-time [*zone* ***recurring*** [*week weekday month hh:mm week weekday month hh:mm*] [*offset*]]

clock summer-time *zone* ***date*** {*day month* | *month day*} *year hh:mm* {*day month* | *month day*} *year hh:mm* [*offset*]

no clock summer-time [*zone* ***date*** {*day month* | *month day*} *year hh:mm* {*day month* | *month day*} *year hh:mm* [*offset*]]

シンタックスの説明

date	夏時間の開始日と終了日を、特定の年の特定の日付として指定します。このキーワードを使用した場合は、日付を毎年リセットする必要があります。
day	1 ～ 31 の日を設定します。たとえば、標準の日付形式に応じて、月日を **April 1** や **1 April** のように入力できます。
hh:mm	時間と分を 24 時間形式で設定します。
month	月を文字列で設定します。***date*** コマンドでは、たとえば、標準の日付形式に応じて、月日を **April 1** や **1 April** のように入力できます。
offset	（オプション）夏時間の時間を変更する分数を設定します。この値は、デフォルトで 60 分です。
recurring	夏時間の開始日と終了日を、年の特定の日付ではなく、月の日と時間の形式で指定します。このキーワードを使用すると、毎年変更する必要がない定期的な日付範囲を設定できます。日付を指定しない場合、セキュリティ アプライアンスは、米国のデフォルトの日付範囲（4 月の最初の日曜日の午前 2 時～ 10 月の最後の日曜日の午前 2 時）を使用します。
week	（オプション）週を 1 ～ 4 の整数で、あるいは ***first*** または ***last*** の語で指定します。たとえば、日が 5 週目になった場合は、**last** を指定します。
weekday	（オプション）**Monday**、**Tuesday**、**Wednesday** など、曜日を指定します。
year	4 桁で西暦年を設定します（たとえば、**2004**）。西暦年の範囲は 1993 ～ 2035 です。
zone	たとえば、太平洋夏時間は **PDT** のように、時間帯を文字列で指定します。このコマンドで設定した日付範囲に従ってセキュリティ アプライアンスが夏時間を表示する場合、時間帯はここで設定した値に変更されます。基本の時間帯を UTC 以外の時間帯に設定するには、**clock timezone** を参照してください。

デフォルト

デフォルトのオフセットは 60 分です。

デフォルトの定期的な日付範囲は、4 月の最初の日曜日の午前 2 時から 10 月の最後の日曜日の午前 2 時です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

南半球の場合、セキュリティ アプライアンスは、たとえば 10 月から 3 月のように、開始月が終了月よりも後に来ることを受け入れます。

例

次の例では、オーストラリアの夏時間の範囲を設定します。

```
hostname(config)# clock summer-time PDT recurring last Sunday October 2:00 last Sunday
March 2:00
```

国によっては、夏時間は特定の日付に開始されます。次の例では、夏時間を西暦 2004 年 4 月 1 日午前 3 時に開始し、西暦 2004 年 10 月 1 日午前 4 時に終了するように設定します。

```
hostname(config)# clock summer-time UTC date 1 April 2004 3:00 1 October 2004 4:00
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show clock	現在の時刻を表示します。

clock timezone

セキュリティ アプライアンスのクロックの時間帯を設定するには、グローバル コンフィギュレーション モードで **clock timezone** コマンドを使用します。時間帯を UTC のデフォルトに戻すには、このコマンドの **no** 形式を使用します。**clock set** コマンドまたは NTP サーバから生成された時間は、時間を UTC で設定します。このコマンドを使用して、時間帯を UTC のオフセットとして設定する必要があります。

clock timezone *zone* [-]*hours* [*minutes*]

no clock timezone [*zone* [-]*hours* [*minutes*]]

シンタックスの説明

zone	たとえば、太平洋標準時間は **PST** のように、時間帯を文字列で指定します。
[-]*hours*	UTC からのオフセットの時間を設定します。たとえば、PST は **-8** 時間です。
minutes	（オプション）UTC からのオフセットの分数を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

夏時間を設定するには、**clock summer-time** コマンドを参照してください。

例

次の例では、時間帯を UTC から -8 時間の太平洋標準時間に設定します。

```
hostname(config)# clock timezone PST -8
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
ntp server	NTP サーバを指定します。
show clock	現在の時刻を表示します。

cluster encryption

仮想ロードバランシング クラスタ上で交換されるメッセージの暗号化をイネーブルにするには、VPN ロードバランシング モードで **cluster encryption** コマンドを使用します。暗号化をディセーブルにするには、このコマンドの **no** 形式を使用します。

cluster encryption

no cluster encryption

（注） VPN ロードバランシングには、アクティブな 3DES または AES ライセンスが必要です。セキュリティ アプライアンスは、ロードバランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。有効な 3DES ライセンスまたは AES ライセンスが検出されなかった場合、セキュリティ アプライアンスはロードバランシングをイネーブルにしません。また、ライセンスで許可されていない限り、ロードバランシング システムが 3DES の内部設定を行わないようにします。

シンタックスの説明

このコマンドには、引数も変数もありません。

デフォルト

暗号化は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、仮想ロードバランシング クラスタ上で交換されるメッセージの暗号化のオンとオフを切り替えます。

cluster encryption コマンドを設定する前に、まず **vpn load-balancing** コマンドを使用して VPN ロードバランシング モードに入る必要があります。また、クラスタの暗号化をイネーブルにする前に、**cluster key** コマンドを使用してクラスタ共有秘密鍵も設定する必要があります。

（注） 暗号化を使用する場合は、最初にコマンド **isakmp enable** *inside* を設定する必要があります。ここで、*inside* は、ロードバランシングの内部インターフェイスです。ロードバランシングの内部インターフェイスで isakmp がイネーブルでない場合は、クラスタの暗号化を設定しようとすると、エラー メッセージが表示されます。

例

次に、仮想ロードバランシング クラスタの暗号化をイネーブルにする **cluster encryption** コマンドを含む VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
cluster key	クラスタの共有秘密鍵を指定します。
vpn load-balancing	VPN ロードバランシング モードに入ります。

cluster ip address

仮想ロードバランシング クラスタの IP アドレスを設定するには、VPN ロードバランシング モードで **cluster ip address** コマンドを使用します。IP アドレスの指定を削除するには、このコマンドの **no** 形式を使用します。

cluster ip address *ip-address*

no cluster ip address [*ip-address*]

シンタックスの説明

ip-address	仮想ロードバランシング クラスタに割り当てる IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して VPN ロードバランシング モードに入り、仮想クラスタ IP アドレスが指すインターフェイスを設定する必要があります。

cluster ip address は、仮想クラスタを設定しているインターフェイスと同じサブネット上にある必要があります。

このコマンドの ***no*** 形式では、オプションの *ip-address* 値を指定した場合、その値は **no cluster ip address** コマンドが完了される前に、既存のクラスタの IP アドレスと一致する必要があります。

例

次に、仮想ロードバランシング クラスタの IP アドレスを 209.165.202.224 に設定する **cluster ip address** コマンドを含む VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
interface	デバイスのインターフェイスを設定します。
nameif	インターフェイスに名前を割り当てます。
vpn load-balancing	VPN ロードバランシング モードに入ります。

cluster key

仮想ロードバランシング クラスタ上で交換される IPSec サイトツーサイト トンネルの共有秘密を設定するには、VPN ロードバランシング モードで **cluster key** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

cluster key *shared-secret*

no cluster key [*shared-secret*]

シンタックスの説明

shared-secret	VPN ロードバランシング クラスタの共有秘密を定義する文字列。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。クラスタの暗号化には、**cluster key** コマンドで定義されたシークレットも使用されます。

共有秘密を設定するには、クラスタの暗号化をイネーブルにする前に **cluster key** コマンドを使用する必要があります。

このコマンドの **no cluster key** 形式で *shared-secret* の値を指定した場合、共有秘密の値は既存のコンフィギュレーションと一致する必要があります。

例

次に、仮想ロードバランシング クラスタの共有秘密を 123456789 に設定する **cluster key** コマンドを含む VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

cluster port

仮想ロードバランシング クラスタの UDP ポートを設定するには、VPN ロードバランシング モードで **cluster port** コマンドを使用します。ポートの指定を削除するには、このコマンドの **no** 形式を使用します。

cluster port *port*

no cluster port [*port*]

シンタックスの説明

port	仮想ロードバランシング クラスタに割り当てる UDP ポート。

デフォルト

デフォルトのクラスタ ポートは、9023 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。

任意の有効な UDP ポート番号を指定できます。範囲は 1 ～ 65535 です。

このコマンドの **no cluster port** 形式で *port* の値を指定した場合、指定したポート番号は既存の設定済みのポート番号と一致する必要があります。

例

次に、仮想ロードバランシング クラスタの UDP ポートを 9023 に設定する **cluster port address** コマンドを含む VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

command-alias

コマンドのエイリアスを作成するには、グローバル　コンフィギュレーション　モードで ***command-alias*** コマンドを使用します。エイリアスを削除するには、このコマンドの **no** 形式を使用します。コマンド エイリアスを入力すると、元のコマンドが実行されます。たとえば、コマンド エイリアスを作成して、長いコマンドのショートカットにすることもできます。

command-alias *mode command_alias original_command*

no command-alias *mode command_alias original_command*

シンタックスの説明

mode	たとえば、**exec**（ユーザおよび特権 EXEC モードの場合）、**configure**、**interface** などの、コマンド エイリアスを作成するコマンド モードを指定します。
command_alias	既存のコマンドに付ける新しい名前を指定します。
original_command	コマンド エイリアスを作成する既存のコマンドまたはキーワードがあるコマンドを指定します。

デフォルト

デフォルトでは、ユーザ EXEC モードで次のエイリアスが設定されています。

h（***help*** のエイリアス）

lo（***logout*** のエイリアス）

p（***ping*** のエイリアス）

s（***show*** のエイリアス）

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

任意のコマンドの最初の部分のエイリアスを作成し、さらに通常どおりキーワードと引数を入力できます。

CLI ヘルプを使用する場合、コマンド エイリアスはアスタリスク（*）で示され、次の形式で表示されます。

```
*command-alias=original-command
```

たとえば、**lo** コマンド エイリアスは、次のように、「lo」で始まる他の特権 EXEC モードのコマンドと共に表示されます。

```
hostname# lo?
*lo=logout login  logout
```

同じエイリアスを別のモードで使用できます。たとえば、次のように、「happy」を特権 EXEC モードとコンフィギュレーション モードで異なるコマンドのエイリアスに使用できます。

```
hostname(config)# happy?

configure mode commands/options:
*happy="username crichton password test"

exec mode commands/options:
*happy=enable
```

コマンドだけを表示し、エイリアスを省略するには、入力行の先頭にスペースを入力します。また、コマンド エイリアスを避けるには、コマンドを入力する前にスペースを使用します。次の例では、happy? コマンドの前にスペースがあるため、エイリアス happy は表示されません。

```
hostname(config)# alias exec test enable
hostname(config)# exit
hostname#   happy?
ERROR: % Unrecognized command
```

コマンドと同様に、CLI ヘルプを使用して、コマンド エイリアスの後に続く引数およびキーワードを表示できます。

完全なコマンド エイリアスを入力する必要があります。短縮されたエイリアスは使用できません。次の例では、パーサーはコマンド hap を、エイリアス happy を示しているとは認識しません。

```
hostname# hap
% Ambiguous command: "hap"
```

例

次の例では、***copy running-config startup-config*** コマンドに対して「***save***」という名前のコマンド エイリアスを作成する方法を示します。

```
hostname(config)# command-alias exec save copy running-config startup-config
hostname(config)# exit
hostname# save

Source filename [running-config]?
Cryptochecksum: 50d131d9 8626c515 0c698f7f 613ae54e

2209 bytes copied in 0.210 secs
hostname#
```

関連コマンド

コマンド	説明
clear configure command-alias	デフォルト以外のコマンド エイリアスをすべて消去します。
show running-config command-alias	デフォルト以外の設定済みのコマンド エイリアスをすべて表示します。

command-queue

応答を待つキューに入る MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

command-queue *limit*

no command-queue *limit*

シンタックスの説明

limit	キューに入るコマンドの最大数（1 ～ 2,147,483,647）を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

MGCP コマンド キューのデフォルトは 200 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

応答を待つキューに入る MGCP コマンドの最大数を指定するには、**command-queue** コマンドを使用します。許容値の範囲は、1 ～ 4,294,967,295 です。デフォルトは 200 です。限度に到達していて新しいコマンドが着信すると、最も長時間キューに入っているコマンドが削除されます。

例

次の例では、MGCP コマンド キューを 150 コマンドに制限します。

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)#command-queue 150
```

関連コマンド

コマンド	説明
debug mgcp	MGCP に関するデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッション情報を表示します。
timeout	MGCP メディア接続または MGCP PAT xlate 接続のアイドル タイムアウトを設定します。このタイムアウト後、その接続が終了します。

compatible rfc1583

RFC 1583 単位のサマリー ルート コスト計算で使用した方式に戻すには、ルータ コンフィギュレーション モードで **compatible rfc1583** コマンドを使用します。RFC 1583 互換性をディセーブルにするには、このコマンドの **no** 形式を使用します。

compatible rfc1583

no compatible rfc1583

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが表示されます。

例

次の例では、RFC 1583 互換ルート サマリー コスト計算をディセーブルにする方法を示します。

```
hostname(config-router)# no compatible rfc1583
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

compression

SVC 接続および WebVPN 接続に対して圧縮をイネーブルにするには、グローバル コンフィギュレーション モードで **compression** コマンドを使用します。

compression {**all** | **svc** | **http-comp**}

[**no**] **compression** {**all** | **svc** | **http-comp**}

このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

シンタックスの説明

all	使用可能なすべての圧縮技術をイネーブルにすることを指定します。
svc	SVC 接続に対する圧縮を指定します。
http-comp	WebVPN 接続に対する圧縮を指定します。

デフォルト

デフォルトは *all* です。使用可能なすべての圧縮技術がイネーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

SVC 接続の場合、グローバル コンフィギュレーション モードで設定した **compression** コマンドによって、グループ ポリシー webvpn モードおよびユーザ名 webvpn モードで設定した **svc compression** コマンドは上書きされます。

たとえば、グループ ポリシー webvpn モードで特定のグループに対する **svc compression** コマンドを入力し、グローバル コンフィギュレーション モードで **no compression** コマンドを入力した場合、そのグループに対して設定した **svc compression** コマンドの設定は上書きされます。

逆に、グローバル コンフィギュレーション モードで **compression** コマンドを使用して圧縮をオンに戻した場合は、グループ設定が有効となり、圧縮動作は最終的にグループ設定によって決定されます。

no compression コマンドを使用して圧縮をディセーブルにした場合、新しい接続だけが影響を受けます。アクティブな接続は影響を受けません。

例

次の例では、SVC 接続に対して圧縮をオンにしています。

```
hostname(config)# compression svc
```

次の例では、SVC 接続および WebVPN 接続に対して圧縮をディセーブルにしています。

```
hostname(config)# no compression svc http-comp
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについての情報を表示します。
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc compression	SVC 接続上の http データの圧縮を特定のグループまたはユーザに対してイネーブルにします。

config-register

次にセキュリティ アプライアンスをリロードするときに使用されるコンフィギュレーション レジスタ値を設定するには、グローバル コンフィギュレーション モードで **config-register** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、ASA 5500 適応型セキュリティ アプライアンスでのみサポートされています。コンフィギュレーション レジスタ値は、ブート イメージおよび他のブート パラメータを決定します。

config-register *hex_value*

no config-register

シンタックスの説明

hex_value	コンフィギュレーション レジスタ値を 0x0 ～ 0xFFFFFFFF の 16 進数値に設定します。この数は 32 ビットを表し、各 16 進文字は 4 ビットを表します。各ビットは異なる特性を制御します。ただし、ビット 32 ～ 20 は、将来の使用のために予約され、ユーザが設定できないか、または現在セキュリティ アプライアンスで使用されていません。したがって、それらのビットを表す 3 つの文字は常に 0 に設定されているため、無視できます。関連するビットは 5 桁の 16 進文字（0x*nnnnn*）で表されます。 文字の前の 0 は含める必要はありません。後続の 0 は含める必要があります。たとえば、0x2001 は 0x02001 と同じですが、0x10000 の 0 はすべて必要です。関連するビットに使用できる値の詳細については、表 8-1 を参照してください。

デフォルト

デフォルト値は 0x1 で、ローカル イメージおよびスタートアップ コンフィギュレーションからブートします。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

5 つの文字には、右から左へ 0 ～ 4 の番号が付けられています。これは、16 進数および 2 進数の規格です。各文字に対して 1 つの値を選択し、必要に応じて値を組み合せたり一致させたりできます。たとえば、文字番号 3 に対して 0 または 2 を選択できます。値によっては、他の値と競合した場合に優先するものがあります。たとえば、セキュリティ アプライアンスを TFTP サーバとローカル イメージの両方からブートするよう設定する 0x2011 を設定する場合、セキュリティ アプライアンスは TFTP サーバからブートします。この値は TFTP のブートが失敗した場合、セキュリティ アプライアンスが直接 ROMMON でブートすることも定めているため、デフォルト イメージからブートすることを指定したアクションは無視されます。

0 の値は、他に指定されていなければ、アクションを実行しないことを意味します。

表 8-1 に、各 16 進文字に関連付けられたアクションを一覧表示します。各文字に対して 1 つの値を選択します。

表 8-1　コンフィギュレーション レジスタ値

プレフィックス	16 進文字番号 4、3、2、1、および 0				
0x	**0**	**0**	**0**[1]	**0**[2]	**0**[2]
	1 起動中に ROMMON のカウントダウンを 10 秒間ディセーブルにします。通常は、カウントダウン中に Escape キーを押して ROMMON に入ることができます。	**2** セキュリティ アプライアンスを TFTP サーバからブートするように設定し、ブートが失敗した場合、この値は直接 ROMMON でブートします。		**1** ROMMON ブート パラメータ（存在する場合は、**boot system tftp** コマンドと同じ）で指定されたように TFTP サーバ イメージからブートします。この値は、文字 1 に設定された値に優先します。	**1** 最初の **boot system** *local_flash* コマンドで指定されたイメージをブートします。そのイメージが読み込まれない場合、セキュリティ アプライアンスは、正常にブートするまで後続の **boot system** コマンドで指定された各イメージのブートを試行します。
					3, **5**, **7**, **9** 特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値が 3 であると最初の **boot system** コマンドで指定されたイメージがブートされ、値が 5 であると 2 番目のイメージがブートされます（以降同様）。 イメージが正常にブートしない場合、セキュリティ アプライアンスは他の **boot system** コマンド イメージ（値 1 と値 3 の使用の違い）に戻ることを試行しません。ただし、セキュリティ アプライアンスには、ブートが失敗した場合に内蔵フラッシュ メモリのルート ディレクトリ内で検出されたいずれかのイメージからブートを試行するフェールセーフ機能があります。フェールセーフ機能を有効にしない場合は、ルート以外のディレクトリにイメージを保存します。
				4[3] スタートアップ コンフィギュレーションを無視してデフォルト コンフィギュレーションを読み込みます。	**2**, **4**, **6**, **8** ROMMON から、引数なしで **boot** コマンドを入力した場合、セキュリティ アプライアンスは特定の **boot system** *local_flash* コマンドで指定されたイメージをブートします。値が 3 であると最初の **boot system** コマンドで指定されたイメージがブートされ、値が 5 であると 2 番目のイメージがブートされます（以降同様）。この値はイメージを自動的にブートしません。
				5 上記の両方のアクションを実行します。	

1. 将来の使用のために予約されています。
2. 文字番号 0 および 1 がイメージを自動的にブートするように設定されていない場合は、セキュリティ アプライアンスが直接 ROMMON でブートします。
3. **service password-recovery** コマンドを使用してパスワードを回復できなくした場合は、スタートアップ コンフィギュレーションを無視するようにコンフィギュレーション レジスタを設定できません。

コンフィギュレーション レジスタ値はスタンバイ装置に複製されませんが、アクティブ装置にコンフィギュレーション レジスタを設定すると、次の警告が表示されます。

```
WARNING The configuration register is not synchronized with the standby, their values
may not match.
```

また、**confreg** コマンドを使用して、コンフィギュレーション レジスタ値を ROMMON で設定することもできます。

例

次の例では、デフォルト イメージからブートするようにコンフィギュレーション レジスタを設定します。

```
hostname(config)# config-register 0x1
```

関連コマンド

コマンド	説明
boot	ブート イメージおよびスタートアップ コンフィギュレーションを設定します。
service password-recovery	パスワードの回復をイネーブルまたはディセーブルにします。

configure factory-default

コンフィギュレーションを工場出荷時のデフォルトに戻すには、グローバル コンフィギュレーション モードで **configure factory-default** コマンドを使用します。工場出荷時のデフォルトは、シスコが新しいセキュリティ アプライアンスに適用しているコンフィギュレーションです。このコマンドは、PIX 525 と PIX 535 セキュリティ アプライアンスを除くすべてのプラットフォームでサポートされています。

configure factory-default [*ip_address* [*mask*]]

シンタックスの説明

ip_address	デフォルトのアドレス 192.168.1.1 を使用する代わりに、管理インターフェイスまたは内部インターフェイスの IP アドレスを設定します。各モデルで設定されるインターフェイスについては、「使用上のガイドライン」を参照してください。
mask	インターフェイスのサブネット マスクを設定します。マスクを設定しない場合、セキュリティ アプライアンスは IP アドレス クラスに適したマスクを使用します。

デフォルト

デフォルトの IP アドレスとマスクは 192.168.1.1 および 255.255.255.0 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	ASA 5505 適応型セキュリティ アプライアンスの工場出荷時にデフォルト コンフィギュレーションが追加されるようになりました。

使用上のガイドライン

PIX 515/515E、および ASA 5510 以上のセキュリティ アプライアンスでは、工場出荷時のデフォルト コンフィギュレーションによって、管理用のインターフェイスが自動的に設定されます。そのため、ASDM を使用してインターフェイスに接続し、残りの設定を行えます。ASA 5505 適応型セキュリティ アプライアンスでは、工場出荷時のデフォルト コンフィギュレーションによって、セキュリティ アプライアンスをネットワークですぐに使用できるように、インターフェイスと NAT が自動的に設定されます。

このコマンドは、ルーテッド ファイアウォール モードでのみ使用可能です。透過モードはインターフェイスの IP アドレスをサポートしていません。インターフェイス IP アドレスの設定は、このコマンドが行うアクションの 1 つです。また、このコマンドはシングル コンテキスト モードでのみ使用できます。コンフィギュレーションを消去されたセキュリティ アプライアンスには、このコマンドを使用して自動的に設定される定義済みのコンテキストはありません。

このコマンドは現在の実行コンフィギュレーションを消去してから、複数のコマンドを設定します。

configure factory-default コマンドで IP アドレスを設定した場合、**http** コマンドは指定したサブネットを使用します。同様に、**dhcpd address** コマンドの範囲は指定したサブネット内のアドレスで構成されます。

工場出荷時のデフォルト コンフィギュレーションに戻した後で、内蔵フラッシュ メモリに保存するには、**write memory** コマンドを使用します。**write memory** コマンドは、前に **boot config** コマンドでデフォルトの場所を設定していても、コンフィギュレーションを消去したときにこのパスも消去されているので、スタートアップ コンフィギュレーション用のデフォルトの場所に実行コンフィギュレーションを保存します。

(注)　このコマンドは、**boot system** コマンド（存在する場合）も、他のコンフィギュレーションと共に消去します。**boot system** コマンドを使用すると、外部フラッシュ メモリ カードのイメージを含む特定のイメージからブートできます。工場出荷時のコンフィギュレーションに戻した後、次にセキュリティ アプライアンスをリロードするとき、セキュリティ アプライアンスは内蔵フラッシュ メモリの最初のイメージからブートします。内蔵フラッシュ メモリにイメージがない場合はブートしません。

完全なコンフィギュレーションに有効な追加の設定を行うには、**setup** コマンドを参照してください。

ASA 5505 適応型セキュリティ アプライアンスのコンフィギュレーション

ASA 5505 適応型セキュリティ アプライアンスの工場出荷時のデフォルト コンフィギュレーションによって、次のように設定されます。

- イーサネット 0/1 ～ 0/7 スイッチ ポートを含む内部 VLAN 1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合は、IP アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- イーサネット 0/0 スイッチ ポートを含む外部 VLAN 2 インターフェイス。VLAN 2 は、DHCP を使用してその IP アドレスを割り当てます。
- デフォルトのルートも DHCP によって割り当てられる。
- すべての内部 IP アドレスが、外部にアクセスするときにインターフェイスの PAT によって変換される。
- デフォルトでは、内部のユーザの外部へのアクセスはアクセス リストによって制御され、外部のユーザは内部にアクセスできない。
- セキュリティ アプライアンスで DHCP サーバがイネーブルになっているため、VLAN 1 インターフェイスに接続している PC は、192.168.1.2 ～ 192.168.1.254 のアドレスを受け取る。
- HTTP サーバは ASDM 用にイネーブルになっており、192.168.1.0 ネットワーク上のユーザがアクセスできる。

このコンフィギュレーションは、次のコマンドで構成されています。

```
interface Ethernet 0/0
   switchport access vlan 2
   no shutdown
interface Ethernet 0/1
   switchport access vlan 1
   no shutdown
interface Ethernet 0/2
   switchport access vlan 1
   no shutdown
interface Ethernet 0/3
   switchport access vlan 1
   no shutdown
interface Ethernet 0/4
   switchport access vlan 1
   no shutdown
interface Ethernet 0/5
   switchport access vlan 1
   no shutdown
interface Ethernet 0/6
   switchport access vlan 1
   no shutdown
interface Ethernet 0/7
   switchport access vlan 1
   no shutdown
interface vlan2
   nameif outside
   no shutdown
   ip address dhcp setroute
interface vlan1
   nameif inside
   ip address 192.168.1.1 255.255.255.0
   security-level 100
   no shutdown
global (outside) 1 interface
nat (inside) 1 0 0
http server enable
http 192.168.1.0 255.255.255.0 inside
dhcpd address 192.168.1.2-192.168.1.254 inside
dhcpd auto_config outside
dhcpd enable inside
logging asdm informational
```

ASA 5510 以上の適応型セキュリティ アプライアンスのコンフィギュレーション

ASA 5510 以上の適応型セキュリティ アプライアンスの工場出荷時のデフォルト コンフィギュレーションによって、次のように設定されます。

- 管理用 Management 0/0 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- セキュリティ アプライアンスで DHCP サーバがイネーブルになっているため、インターフェイスに接続している PC は、192.168.1.2 ～ 192.168.1.254 のアドレスを受け取る。
- HTTP サーバは ASDM 用にイネーブルになっており、192.168.1.0 ネットワーク上のユーザがアクセスできる。

このコンフィギュレーションは、次のコマンドで構成されています。

```
interface management 0/0
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

PIX 515/515E セキュリティ アプライアンスのコンフィギュレーション

PIX 515/515E セキュリティ アプライアンスの工場出荷時のデフォルト コンフィギュレーションによって、次のように設定されます。

- 内部 Ethernet1 インターフェイス。**configure factory-default** コマンドで IP アドレスを設定しなかった場合、IP アドレスとマスクは、それぞれ 192.168.1.1 と 255.255.255.0 になります。
- セキュリティ アプライアンスで DHCP サーバがイネーブルになっているため、インターフェイスに接続している PC は、192.168.1.2 ～ 192.168.1.254 のアドレスを受け取る。
- HTTP サーバは ASDM 用にイネーブルになっており、192.168.1.0 ネットワーク上のユーザがアクセスできる。

このコンフィギュレーションは、次のコマンドで構成されています。

```
interface ethernet 1
   ip address 192.168.1.1 255.255.255.0
   nameif management
   security-level 100
   no shutdown
asdm logging informational 100
asdm history enable
http server enable
http 192.168.1.0 255.255.255.0 management
dhcpd address 192.168.1.2-192.168.1.254 management
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd enable management
```

例

次の例では、コンフィギュレーションを工場出荷時のデフォルトにリセットし、IP アドレス 10.1.1.1 をインターフェイスに割り当て、次に新しいコンフィギュレーションをスタートアップ コンフィギュレーションとして保存します。

```
hostname(config)# configure factory-default 10.1.1.1 255.255.255.0
Based on the inside IP address and mask, the DHCP address
pool size is reduced to 253 from the platform limit 256

WARNING: The boot system configuration will be cleared.
The first image found in disk0:/ will be used to boot the
system on the next reload.
Verify there is a valid image on disk0:/ or the system will
not boot.

Begin to apply factory-default configuration:
Clear all configuration
...
hostname(config)#
hostname(config)# copy running-config startup-config
```

関連コマンド

コマンド	説明
boot system	ブートするソフトウェア イメージを設定します。
clear configure	実行コンフィギュレーションを消去します。
copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
setup	セキュリティ アプライアンスの基本設定を設定するよう要求します。
show running-config	実行コンフィギュレーションを表示します。

configure http

HTTP（S）サーバからのコンフィギュレーション ファイルを実行コンフィギュレーションとマージするには、グローバル コンフィギュレーション モードで **configure http** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

configure *http*[*s*]*:*//[*user*[:***password*]**@**]*server*[:*port*]/[*path*/]*filename*

シンタックスの説明

*:*password	（オプション）HTTP(S) 認証の場合、パスワードを指定します。
:*port*	（オプション）ポートを指定します。HTTP の場合、デフォルトは 80 です。HTTPS の場合、デフォルトは 443 です。
@	（オプション）名前とパスワードの両方またはいずれか一方を入力する場合は、サーバの IP アドレスにアットマーク（@）を付けます。
filename	コンフィギュレーション ファイル名を指定します。
http[**s**]	HTTP または HTTPS を指定します。
path	（オプション）ファイル名へのパスを指定します。
server	サーバの IP アドレスまたは名前を指定します。IPv6 サーバ アドレスの場合、ポートを指定した場合は、IP アドレス内のコロンがポート番号の前のコロンと間違われないように、IP アドレスを角カッコで囲む必要があります。たとえば、アドレスとポートを次のように入力します。 `[fe80::2e0:b6ff:fe01:3b7a]:8080`
user	（オプション）HTTP(S) 認証の場合、ユーザ名を指定します。

デフォルト

HTTP の場合、デフォルト ポートは 80 です。HTTPS の場合、デフォルト ポートは 443 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

マージでは、新しいコンフィギュレーションのすべてのコマンドが実行コンフィギュレーションに追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

このコマンドは、**copy http running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドを使用できるのはシステム実行スペースに限られるため、**configure http** コマンドはコンテキスト内で使用するための代替です。

例

次の例では、コンフィギュレーション ファイルを HTTPS サーバから実行コンフィギュレーションにコピーします。

```
hostname(config)# configure https://user1:pa$$w0rd@10.1.1.1/configs/newconfig.cfg
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションを消去します。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure factory-default	CLI で入力するコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure memory

スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージするには、グローバル コンフィギュレーション モードで **configure memory** コマンドを使用します。

configure memory

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

マージでは、新しいコンフィギュレーションのすべてのコマンドが実行コンフィギュレーションに追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

コンフィギュレーションをマージしない場合は、セキュリティ アプライアンスを経由する通信を妨げる実行コンフィギュレーションを消去してから、**configure memory** コマンドを入力して新しいコンフィギュレーションを読み込むことができます。

このコマンドは **copy startup-config running-config** コマンドと同じです。

マルチ コンテキスト モードの場合、コンテキストのスタートアップ コンフィギュレーションは **config-url** コマンドで指定した場所にあります。

例

次の例では、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーします。

```
hostname(config)# configure memory
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションを消去します。
configure http	指定した HTTP(S) URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure factory-default	CLI で入力するコマンドを実行コンフィギュレーションに追加します。
show running-config	実行コンフィギュレーションを表示します。

configure net

TFTP サーバからのコンフィギュレーション ファイルを実行コンフィギュレーションとマージするには、グローバル コンフィギュレーション モードで **configure net** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

configure net [*server***:**[*filename*] | **:***filename*]

シンタックスの説明

:filename	パスとファイル名を指定します。**tftp-server** コマンドを使用してファイル名をすでに設定している場合、この引数はオプションです。 **tftp-server** コマンドで名前を指定したように、このコマンドでファイル名を指定すると、セキュリティ アプライアンスは **tftp-server** コマンド ファイル名をディレクトリとして扱い、***configure net*** コマンド ファイル名をディレクトリの下のファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ（//）が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。 **tftp-server** コマンドを使用して TFTP サーバのアドレスを指定した場合、コロン（:）の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。このアドレスが存在する場合は、**tftp-server** コマンドで設定したアドレスを上書きします。IPv6 サーバ アドレスの場合、IP アドレス内のコロンがファイル名の前のコロンと間違われないように、IP アドレスを角カッコで囲む必要があります。たとえば、アドレスを次のように入力します。 [fe80::2e0:b6ff:fe01:3b7a] デフォルト ゲートウェイ インターフェイスは最高レベルのセキュリティ インターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

マージでは、新しいコンフィギュレーションのすべてのコマンドが実行コンフィギュレーションに追加され、競合するすべてのコマンドが新しいバージョンで上書きされます。たとえば、コマンドが複数のインスタンスを許可している場合は、新しいコマンドが実行コンフィギュレーション内の既存のコマンドに追加されます。コマンドが 1 つのインスタンスしか許可していない場合は、実行コンフィギュレーション内のコマンドが新しいコマンドで上書きされます。実行コンフィギュレーション内に存在するが、新しいコンフィギュレーションには設定されていないコマンドは、マージによって削除されません。

このコマンドは、**copy tftp running-config** コマンドと同じです。マルチ コンテキスト モードの場合、このコマンドを使用できるのはシステム実行スペースに限られるため、**configure net** コマンドはコンテキスト内で使用するための代替です。

例

次の例では **tftp-server** コマンドにサーバとファイル名を設定した後、**configure net** コマンドを使用してサーバを上書きします。同じファイル名が使用されています。

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:
```

次の例では、サーバとファイル名を上書きします。ファイル名へのデフォルト パスは /tftpboot/configs/config1 です。ファイル名をスラッシュ（/）で始めない場合、パスの /tftpboot/ の部分はデフォルトで含まれます。このパスを上書きし、ファイルも tftpboot にある場合は、tftpboot パスを **configure net** コマンドに含めます。

```
hostname(config)# tftp-server inside 10.1.1.1 configs/config1
hostname(config)# configure net 10.2.2.2:/tftpboot/oldconfigs/config1
```

次の例では、サーバだけを **tftp-server** コマンドに設定します。**configure net** コマンドはファイル名だけを指定します。

```
hostname(config)# tftp-server inside 10.1.1.1
hostname(config)# configure net :configs/config1
```

関連コマンド

コマンド	説明
configure http	指定した HTTP(S) URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

configure terminal

実行コンフィギュレーションをコマンドラインで設定するには、特権 EXEC モードで **configure terminal** コマンドを使用します。このコマンドは、コンフィギュレーションを変更するコマンドを入力できるグローバル コンフィギュレーション モードに入ります。

configure terminal

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、グローバル コンフィギュレーション モードに入ります。

```
hostname# configure terminal
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure	実行コンフィギュレーションを消去します。
configure http	指定した HTTP(S) URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。

config-url

システムがコンテキスト コンフィギュレーションをダウンロードする URL を指定するには、コンテキスト コンフィギュレーション モードで **config-url** コマンドを使用します。

config-url *url*

シンタックスの説明

url　コンテキスト コンフィギュレーションの URL を設定します。すべてのリモート URL は、管理コンテキストからアクセスできる必要があります。次の URL シンタックスを参照してください。

- ***disk0:/***[*path/*]*filename*

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は内蔵フラッシュ メモリを指します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。
- ***disk1:/***[*path/*]*filename*

  ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、この URL は外部フラッシュ メモリ カードを指します。
- ***flash:/***[*path/*]*filename*

  この URL は内蔵フラッシュ メモリを指します。
- ***ftp://***[*user*[***:***password]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;type=***xx]

  type には、次のいずれかのキーワードを指定できます。
  - ***ap***：ASCII パッシブ モード
  - ***an***：ASCII 通常モード
  - ***ip***：（デフォルト）バイナリ パッシブ モード
  - ***in***：バイナリ通常モード
- ***http***[***s***]***://***[*user*[***:***password]***@***]*server*[*:port*]***/***[*path/*]*filename*
- ***tftp://***[*user*[***:***password]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;int=***interface_name]

  サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　コンテキスト URL を追加すると、システムはただちにコンテキストを読み込み実行中になります。

（注） **config-url** コマンドを入力する前に、**allocate-interface** コマンドを入力します。セキュリティ アプライアンスは、コンテキスト コンフィギュレーションを読み込む前に、コンテキストにインターフェイスを割り当てる必要があります。コンテキスト コンフィギュレーションには、インターフェイス（**interface**、**nat**、**global** など）を示すコマンドが含まれている場合があります。最初に **config-url** コマンドを入力した場合、セキュリティ アプライアンスはただちにコンテキスト コンフィギュレーションを読み込みます。コンテキストにインターフェイスを示すコマンドが含まれていない場合、それらのコマンドは失敗します。

ファイル名にファイル拡張子は必要ありませんが、「.cfg」を使用することを推奨します。

管理コンテキスト ファイルは、内蔵フラッシュ メモリに保存する必要があります。

HTTP または HTTPS サーバからコンテキスト コンフィギュレーションをダウンロードした場合、**copy running-config startup-config** コマンドを使用して変更内容をそれらのサーバに保存することはできません。ただし、**copy tftp** コマンドを使用して実行コンフィギュレーションを TFTP サーバにコピーできます。

サーバが利用できない、またはファイルがまだ存在しないためにシステムがコンテキスト コンフィギュレーション ファイルを取得できない場合、システムは、コマンドライン インターフェイスでただちに設定できるブランクのコンテキストを作成します。

URL を変更するには、新しい URL で **config-url** コマンドを再入力します。

セキュリティ アプライアンスは、新しいコンフィギュレーションを現在の実行コンフィギュレーションとマージします。同じ URL を再入力しても、保存されたコンフィギュレーションが実行コンフィギュレーションとマージされます。マージにより、新しいコンフィギュレーションのすべての新しいコマンドが実行コンフィギュレーションに追加されます。コンフィギュレーションが同じ場合、変更は行われません。コマンドが競合する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの効果はコマンドによって異なります。エラーが発生したり、予期しない結果が生じたりすることがあります。実行コンフィギュレーションがブランクの場合（たとえば、サーバが利用不可能でコンフィギュレーションがダウンロードされなかった場合）は、新しいコンフィギュレーションが使用されます。コンフィギュレーションをマージしない場合は、コンテキストを経由する通信を妨げる実行コンフィギュレーションを消去してから、新しい URL からコンフィギュレーションをリロードすることができます。

例

次の例では、管理コンテキストを「administrator」と設定し、内蔵フラッシュ メモリに「administrator」という名前のコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加しています。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

console timeout

セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **console timeout** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

console timeout *number*

no console timeout [*number*]

シンタックスの説明

number	コンソール セッションが終了するまでのアイドル時間を分単位（0 ～ 60）で指定します。

デフォルト

デフォルトのタイムアウトは 0 で、コンソール セッションはタイムアウトしません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

console timeout コマンドは、セキュリティ アプライアンスへの認証済みのすべてのイネーブル モード ユーザ セッションとコンフィギュレーション モード ユーザ セッションにタイムアウト値を設定します。**console timeout** コマンドによって、Telnet タイムアウトや SSH タイムアウトが変更されることはありません。これらのアクセス方式については、それぞれ独自のタイムアウト値が保持されています。

no console timeout コマンドは、コンソール タイムアウト値をデフォルトのタイムアウトの 0 にリセットします。この値は、コンソールがタイムアウトしないことを意味します。

例

次の例では、コンソール タイムアウトを 15 分に設定する方法を示します。

```
hostname(config)# console timeout 15
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
clear configure timeout	コンフィギュレーションにあるアイドル期間をデフォルトに戻します。
show running-config console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを表示します。

content-length

HTTP メッセージ本文の長さに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **content-length** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

no content-length { **min** *bytes* [**max** *bytes*] | **max** *bytes*] } **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこの検査に合格しなかったときに実行されるアクションを指定します。
allow	メッセージを許可します。
bytes	バイト数を指定します。許容される範囲は、**min** オプションでは 1 ～ 65,535、**max** オプションでは 1 ～ 50,000,000 です。
drop	接続を終了します。
log	（オプション）syslog を生成します。
max	（オプション）使用可能な最大コンテキスト長を指定します。
min	使用可能な最小コンテキスト長を指定します。
reset	TCP リセット メッセージをクライアントまたはサーバに送信します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

content-length コマンドをイネーブルにすると、セキュリティ アプライアンスは設定された範囲内のメッセージだけを許可し、許可しない場合は指定されたアクションを実行します。セキュリティ アプライアンスが TCP 接続をリセットして syslog エントリを作成するようにするには、**action** キーワードを使用します。

例

次の例では、HTTP トラフィックを 100 バイト以上 2,000 バイト以下のメッセージに制限しています。メッセージがこの範囲外の場合、セキュリティ アプライアンスは TCP 接続をリセットし、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

content-type-verification

HTTP メッセージのコンテキスト タイプに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **content-type-verification** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

no content-type-verification [**match-req-rsp**] **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがコマンド検査に合格しなかったときに実行されるアクションを指定します。
allow	メッセージを許可します。
drop	接続を終了します。
log	（オプション）syslog メッセージを生成します。
match-req-rsp	（オプション）HTTP 応答の content-type フィールドが、対応する HTTP 要求メッセージの accept フィールドに一致するかどうかを確認します。
reset	TCP リセット メッセージをクライアントまたはサーバに送信します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは次のチェックをイネーブルにします。

- ヘッダーの content-type の値が、サポートされているコンテンツ タイプの内部リストにあることを確認します。
- ヘッダーの content-type が、データ内の実際のコンテンツまたはメッセージのエンティティ本体の部分と一致していることを確認します。
- **match-req-rsp** キーワードは、HTTP 応答の content-type フィールドが、対応する HTTP 要求メッセージの **accept** フィールドに一致することを確認する追加のチェックをイネーブルにします。

メッセージが上記のいずれかのチェックに合格しなかった場合、セキュリティ アプライアンスは設定されたアクションを実行します。

次に、サポートされているコンテンツ タイプのリストを示します。

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

このリストの一部のコンテンツ タイプは、対応する正規表現（マジック ナンバー）がないためにメッセージの本体部分で確認できない場合があります。その場合、HTTP メッセージが許可されます。

例

次の例では、HTTP メッセージのコンテンツ タイプに基づいて HTTP トラフィックを制限します。サポートされていないコンテンツ タイプがメッセージに含まれている場合、セキュリティ アプライアンスは TCP 接続を制限し、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

context

システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **context** コマンドを使用します。コンテキストを削除するには、このコマンドの **no** 形式を使用します。コンテキスト コンフィギュレーション モードでは、コンテキストで使用できるコンフィギュレーション ファイルの URL とインターフェイスを指定できます。

context *name*

no context *name* [***noconfirm***]

シンタックスの説明

name	名前を最大 32 文字の文字列で指定します。この名前では大文字と小文字が区別されるため、たとえば、「customerA」と「CustomerA」という名前で 2 つのコンテキストを作成できます。文字、数字、またはハイフンを使用できますが、名前の先頭または末尾にハイフンを使用することはできません。 「System」および「Null」（大文字および小文字）は予約されている名前であるため、使用できません。
noconfirm	（オプション）確認を求めるプロンプトを表示せずにコンテキストを削除します。このオプションは、自動スクリプトに役立ちます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

管理コンテキストがない場合（たとえば、コンフィギュレーションを消去した場合）、追加する最初のコンテキストは管理コンテキストである必要があります。管理コンテキストを追加するには、**admin-context** コマンドを参照してください。管理コンテキストを指定した後、**context** コマンドを入力して管理コンテキストを設定します。

コンテキストは、システム コンフィギュレーションを編集することによってのみ削除できます。現在の管理コンテキストはこのコマンドの **no** 形式を使用して削除できません。**clear configure context** コマンドを使用してすべてのコンテキストを削除した場合のみ削除できます。

例

次の例では、管理コンテキストを「administrator」と設定し、内蔵フラッシュ メモリに「administrator」という名前のコンテキストを作成してから、FTP サーバから 2 つのコンテキストを追加しています。

```
hostname(config)# admin-context administrator
hostname(config)# context administrator
hostname(config-ctx)# allocate-interface gigabitethernet0/0.1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
hostname(config-ctx)# config-url flash:/admin.cfg

hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg

hostname(config-ctx)# context sample
hostname(config-ctx)# allocate-interface gigabitethernet0/1.200 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/1.212 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/1.230-gigabitethernet0/1.235
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/sample.cfg
```

関連コマンド

コマンド	説明
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
join-failover-group	フェールオーバー グループにコンテキストを割り当てます。
show context	コンテキスト情報を表示します。

copy

ファイルをある場所から別の場所にコピーするには、**copy** コマンドを使用します。

copy [**/noconfirm** | **/pcap**] {*url* | ***running-config*** | ***startup-config***} {***running-config*** | ***startup-config*** | *url*}

シンタックスの説明

/noconfirm	確認プロンプトなしでファイルをコピーします。
/pcap	事前に設定した TFTP サーバのデフォルトを指定します。デフォルトの TFTP サーバを設定するには、**tftp-server** コマンドを参照してください。
running-config	実行コンフィギュレーションを指定します。
startup-config	スタートアップ コンフィギュレーションを指定します。シングルモードのスタートアップ コンフィギュレーションまたはマルチ コンテキスト モードのシステムのスタートアップ コンフィギュレーションは、フラッシュ メモリ内の非表示のファイルです。スタートアップ コンフィギュレーションの場所は、コンテキスト内から **config-url** コマンドで指定します。たとえば、**config-url** コマンドで HTTP サーバを指定し、**copy startup-config running-config** コマンドを入力した場合、セキュリティ アプライアンスは管理コンテキスト インターフェイスを使用して、HTTP サーバからスタートアップ コンフィギュレーションをコピーします。

url	コピー元のファイルまたはコピー先のファイルを指定します。コピー元 URL とコピー先 URL の組み合せには、使用できないものもあります。たとえば、あるリモート サーバから別のリモート サーバにコピーすることはできません。このコマンドは、ローカルの場所とリモートの場所の間でのコピーに使用するためのものです。コンテキスト内では、コンテキスト インターフェイスを使用して、実行コンフィギュレーションまたはスタートアップ コンフィギュレーションを TFTP サーバまたは FTP サーバにコピーできますが、サーバから実行コンフィギュレーションまたはスタートアップ コンフィギュレーションをコピーすることはできません。他のオプションについては、**startup-config** キーワードを参照してください。また、TFTP サーバから実行コンテキスト コンフィギュレーションにダウンロードするには、**configure net** コマンドを参照してください。 次の URL シンタックスを参照してください。 • ***disk0:/***[*path/*]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみで使用でき、内蔵フラッシュ メモリを示します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。 • ***disk1:/***[*path/*]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみで使用でき、外部フラッシュ メモリ カードを示します。 • ***flash:/***[*path/*]*filename* このオプションは、内蔵フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、***flash*** は ***disk0*** のエイリアスです。 • ***ftp://***[*user*[***:****password*]***@***]*server*[*:port*]*/*[*path/*]*filename*[***;type=****xx*] ***type*** には、次のいずれかのキーワードを指定できます。 — ***ap***：ASCII パッシブ モード — ***an***：ASCII 通常モード — ***ip***：（デフォルト）バイナリ パッシブ モード — ***in***：バイナリ通常モード • ***http***[***s***]***://***[*user*[***:****password*]***@***]*server*[*:port*]*/*[*path/*]*filename* • ***tftp://***[*user*[***:****password*]***@***]*server*[*:port*]*/*[*path/*]*filename*[***;int=****interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 ただし、パス名にスペースを含めることはできません。パス名にスペースが含まれている場合は、**copy tftp** コマンドではなく **tftp-server** コマンドでパスを設定してください。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	DNS 名のサポートが追加されました。

使用上のガイドライン

コンフィギュレーションを実行コンフィギュレーションにコピーすると、2 つのコンフィギュレーションがマージされます。マージにより、新しいコンフィギュレーションのすべての新しいコマンドが実行コンフィギュレーションに追加されます。コンフィギュレーションが同じ場合、変更は行われません。コマンドが競合する場合、またはコマンドがコンテキストの実行に影響を与える場合、マージの効果はコマンドによって異なります。エラーが発生したり、予期しない結果が生じたりすることがあります。

例

次の例では、システム実行スペースでファイルをディスクから TFTP サーバにコピーする方法を示します。

```
hostname(config)# copy disk0:my_context/my_context.cfg
tftp://10.7.0.80/my_context/my_context.cfg
```

次に、ファイルをディスク上のある場所からディスク上の別の場所にコピーする方法を示します。宛先ファイルの名前は、コピー元のファイルの名前にすることも、別の名前することもできます。

```
hostname(config)# copy disk0:my_context.cfg disk:my_context/my_context.cfg
```

次の例では、ASDM ファイルを TFTP サーバから内蔵フラッシュ メモリにコピーする方法を示しています。

```
hostname(config)# copy tftp://10.7.0.80/asdm700.bin disk0:asdm700.bin
```

次の例では、コンテキスト内の実行コンフィギュレーションを TFTP サーバにコピーする方法を示しています。

```
hostname(config)# copy running-config tftp://10.7.0.80/my_context/my_context.cfg
```

copy コマンドでは、IP アドレス（上の例を参照）だけでなく、DNS 名も指定できます。

```
hostname(config)# copy running-config tftp://www.example.com/my_context/my_context.cfg
```

関連コマンド

コマンド	説明
configure net	ファイルを TFTP サーバから実行コンフィギュレーションにコピーします。
copy capture	キャプチャ ファイルを TFTP サーバにコピーします。
tftp-server	デフォルトの TFTP サーバを設定します。
write memory	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

copy capture

キャプチャ ファイルをサーバにコピーするには、グローバル コンフィギュレーション モードで **copy capture** コマンドを使用します。

copy [**/noconfirm**] [**/pcap**] **capture:** [*context_name/*]*buffer_name url*

シンタックスの説明

/noconfirm	確認プロンプトなしでファイルをコピーします。
/pcap	パケット キャプチャを未加工のデータとしてコピーします。
buffer_name	キャプチャを識別するための一意の名前。
context_name/	セキュリティ コンテキストで定義されたパケット キャプチャをコピーします。
url	パケット キャプチャ ファイルのコピー先を指定します。次の URL シンタックスを参照してください。 • ***disk0:/***[*path/*]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用でき、内蔵フラッシュ カードを示します。***disk0*** の代わりに ***flash*** を使用することもできます。これらは、エイリアス関係にあります。 • ***disk1:/***[*path/*]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスだけで使用でき、外部フラッシュ カードを示します。 • ***flash:/***[*path/*]*filename* このオプションは、内蔵フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合、***flash*** は ***disk0*** のエイリアスです。 • ***ftp://***[*user*[**:***password*]**@**]*server*[:*port*]**/**[*path/*]*filename*[**;*type*=***xx***] ***type*** には、次のいずれかのキーワードを指定できます。 — ***ap***：ASCII パッシブ モード — ***an***：ASCII 通常モード — ***ip***：（デフォルト）バイナリ パッシブ モード — ***in***：バイナリ通常モード • ***http***[***s***]***://***[*user*[**:***password*]**@**]*server*[:*port*]**/**[*path/*]*filename* • ***tftp://***[*user*[**:***password*]**@**]*server*[:*port*]**/**[*path/*]*filename*[**;*int*=***interface_name***] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 ただし、パス名にスペースを含めることはできません。パス名にスペースが含まれている場合は、**copy tftp** コマンドではなく **tftp-server** コマンドでパスを設定してください。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、フルパスを指定せずに **copy capture** コマンドを入力した場合に表示されるプロンプトを示します。

```
hostname(config)# copy capture:abc tftp
Address or name of remote host [171.68.11.129]?
Source file name [username/cdisk]?
copying capture to tftp://171.68.11.129/username/cdisk:
[yes|no|again]? y
!!!!!!!!!!!!!
```

次のようにフルパスを指定できます。

```
hostname(config)# copy capture:abc tftp:171.68.11.129/tftpboot/abc.cap
```

TFTP サーバを設定している場合は、次のようにファイルの位置や名前を省略できます。

```
hostname(config)# tftp-server outside 171.68.11.129 tftp/cdisk
hostname(config)# copy capture:abc tftp:/tftp/abc.cap
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能を有効にして、パケットのスニッフィングやネットワーク障害を検出できるようにします。
clear capture	キャプチャ バッファを消去します。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。

cpu profile activate

CPU プロファイル収集情報を開始するには、特権 EXEC モードで **cpu profile activate** コマンドを使用します。

cpu profile activate *n-samples*

シンタックスの説明

n-samples	n 個のサンプルを保存するためのメモリを割り当てます。値は 1 ～ 100000 です。デフォルトは 1000 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show cpu profile コマンドを **cpu profile activate** コマンドと組み合せて使用すると、TAC が CPU 問題のトラブルシューティングを支援するために収集および使用できる情報が表示されます。**show cpu profile** コマンドによって表示される情報は 16 進形式です。

例

次の例では、プロファイラを有効にし、5000 個のサンプルを格納するように指示します。

```
hostname# cpu profile activate 5000
Activated CPU profiling for 5000 samples.
```

show cpu profile コマンドを使用して、結果を確認します。

（注） **cpu profile activate** コマンドの実行中に **show cpu profile** コマンドを実行すると、進行状況が表示されます。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 CPU profiling currently in
progress, 1640 out of 5000 samples collected.
```

処理が完了すると、**show cpu profile** コマンド出力によって結果が表示されます。この情報をコピーし、TAC に提出します。TAC がこの情報をデコードします。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 Profiling finished, 5000
samples:
 00c483f5 00115283 002199d3 001151d1 002199e5 00116258 002199fc 00115230  0021984e
002198f6 00c48496 00219803 004a55b1 002198b1 00c484d9 00c48472
 00116258 00c48401 002199f3 00c48401 00c484b2 004a5580 0011520a 002198b4
 00116258 00219807 0011520a 00116258 002198a9 00116258 00219a2e 00112009  0021989c
00fff023 008be861 0011525e 002198be 0021984e 00115277 00219807  002199d0 00114a6d
002198af 0011520a 00115260 00115274 004a55a6 00c48472
 00c48472 00c48496 002199f9 002198ad 00c484c4 004a55a6 00115260 002198f4  0011528e
002198e0 00c484bb 00c48496 00c484a6 002199f3 00219810 001161d6 .
```

関連コマンド

コマンド	説明
show cpu profile	TAC で使用される CPU プロファイル アクティベーション情報を表示します。

crashinfo console disable

フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行うには、**crashinfo console disable** コマンドを使用します。

crashinfo console disable

[no] crashinfo console disable

シンタックスの説明

disable	クラッシュが発生した場合にコンソール出力を抑制します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用すると、crashinfo がコンソールに出力されないようにすることができます。crashinfo には、装置に接続されたすべてのユーザに対して表示されるのにふさわしくない機密情報が含まれている場合があります。このコマンドと共に、crashinfo がフラッシュに書き込まれていることも確認する必要があります。これは装置のリブート後に確認できます。このコマンドは、crashinfo および checkheaps の出力に影響を与えます。この出力はフラッシュに保存され、トラブルシューティングに十分に役立ちます。

例

```
hostname(config)# crashinfo console disable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
fips enable	システムまたはモジュールで FIPS に準拠するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

crashinfo force

セキュリティ アプライアンスを強制的にクラッシュさせるには、特権 EXEC モードで ***crashinfo force*** コマンドを使用します。

crashinfo force [**page-fault | watchdog**]

シンタックスの説明

page-fault	（オプション）ページ フォールトを利用して、セキュリティ アプライアンスを強制的にクラッシュさせます。
watchdog	（オプション）ウォッチドッグを利用して、セキュリティ アプライアンスを強制的にクラッシュさせます。

デフォルト

デフォルトでは、セキュリティ アプライアンスはフラッシュ メモリにクラッシュ情報ファイルを保存します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

crashinfo force コマンドを使用して、クラッシュ出力の生成をテストできます。クラッシュ出力では、本物のクラッシュと **crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドによって発生したクラッシュは区別できません。これは、コマンドによって実際にクラッシュが発生しているためです。セキュリティ アプライアンスは、クラッシュのダンプが完了するとリロードします。

注意　実稼働環境では **crashinfo force** コマンドを使用しないでください。**crashinfo force** コマンドはセキュリティ アプライアンスをクラッシュさせて、強制的にリロードを実行します。

例

次の例では、**crashinfo force page-fault** コマンドを入力したときに表示される警告を示します。

```
hostname# crashinfo force page-fault
WARNING: This command will force the XXX to crash and reboot.
    Do you wish to proceed? [confirm]:
```

キーボードの Return キーまたは Enter キーを押して復帰改行を入力するか、**Y** キーまたは **y** キーを押すと、セキュリティ アプライアンスがクラッシュしてリロードが実行されます。これらの応答は、いずれも操作に同意したものと解釈されます。その他の文字はすべて **no** と解釈され、セキュリティ アプライアンスはコマンドライン プロンプトに戻ります。

関連コマンド

clear crashinfo	クラッシュ情報ファイルの内容を消去します。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。
show crashinfo	クラッシュ情報ファイルの内容を表示します。

crashinfo save disable

フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにするには、グローバル コンフィギュレーション モードで ***crashinfo save*** コマンドを使用します。

crashinfo save disable

no crashinfo save disable

シンタックスの説明

このコマンドには、デフォルトの引数もキーワードもありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはフラッシュ メモリにクラッシュ情報ファイルを保存します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	***crashinfo save enable*** コマンドは廃止され、有効なオプションではなくなりました。代わりに、***no crashinfo save disable*** コマンドを使用します。

使用上のガイドライン

クラッシュ情報は、まずフラッシュ メモリに書き込まれ、次にコンソールに書き込まれます。

（注） セキュリティ　アプライアンスが起動中にクラッシュした場合、クラッシュ情報ファイルは保存されません。クラッシュ情報をフラッシュ メモリに保存するには、セキュリティ アプライアンスは完全に初期化されて、動作を開始している必要があります。

クラッシュ情報のフラッシュ メモリへの保存をもう一度イネーブルにするには、**no crashinfo save disable** コマンドを使用します。

例

```
hostname(config)# crashinfo save disable
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容を消去します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。
show crashinfo	クラッシュ ファイルの内容を表示します。

crashinfo test

セキュリティ アプライアンスの機能をテストして、フラッシュ メモリ内のファイルにクラッシュ情報を保存するには、グローバル コンフィギュレーション モードで ***crashinfo test*** コマンドを使用します。

crashinfo test

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

フラッシュ メモリ内に以前のクラッシュ情報ファイルがすでに存在する場合、そのファイルは上書きされます。

（注） **crashinfo test** コマンドを入力してもセキュリティ アプライアンスはクラッシュしません。

例

次の例では、クラッシュ情報ファイル テストの出力を示します。

```
hostname(config)# crashinfo test
```

関連コマンド

clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
show crashinfo	クラッシュ ファイルの内容を表示します。

crl

CRL コンフィギュレーション オプションを指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **crl** コマンドを使用します。

crl {**required | optional | nocheck**}

シンタックスの説明

required	必須の CRL は、検証されるピア証明書に対して使用できる必要があります。
optional	必須の CRL が使用できない場合にも、セキュリティ アプライアンスはピア証明書を受け入れることができます。
nocheck	CRL チェックを実行しないようにセキュリティ アプライアンスに指示します。

デフォルト

デフォルト値は、**nocheck** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。新しい **revocation-check** コマンドは、次のとおりです。 • **crl optional** は、**revocation-check crl none** に置き換えられました。 • **crl required** は、**revocation-check crl** に置き換えられました。 • **crl nocheck** は、**revocation-check none** に置き換えられました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、CRL がトラストポイント central の検証されるピア証明書に対して使用できることを要求します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl required
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca trustpoint	トラストポイント サブモードに入ります。
crl configure	crl コンフィギュレーション モードに入ります。

crl configure

CRL 設定コンフィギュレーション モードに入るには、暗号 CA トラストポイント コンフィギュレーション モードで **crl configure** コマンドを使用します。

crl configure

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central 内の crl コンフィギュレーション モードに入ります。

```
hostname<config># crypto ca trustpoint central
hostname<ca-trustpoint># crl configure
hostname<ca-crl>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca trustpoint	トラストポイント サブモードに入ります。

crypto ca authenticate コマンド～ customization コマンド

crypto ca authenticate

トラストポイントに関連付けられた CA 証明書をインストールおよび認証するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。CA 証明書を削除するには、このコマンドの **no** 形式を使用します。

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive]**

no crypto ca authenticate *trustpoint*

シンタックスの説明

fingerprint	セキュリティ アプライアンスが CA 証明書の認証に使用する、英数字で構成されたハッシュ値を指定します。フィンガープリントが提供されている場合、セキュリティ アプライアンスは CA 証明書の計算されたフィンガープリントと比較し、2 つの値が一致した場合のみその証明書を受け入れます。フィンガープリントがない場合、セキュリティ アプライアンスは計算されたフィンガープリントを表示し、証明書を受け入れるかどうか尋ねます。
hexvalue	フィンガープリントの 16 進値を指定します。
nointeractive	Device Manager 専用の非対話型モードを使用して、このトラストポイントの CA 証明書を取得します。そのとき、フィンガープリントがない場合、セキュリティ アプライアンスは確認せずに証明書を受け入れます。
trustpoint	CA 証明書を取得するトラストポイントを指定します。名前の最大長は 128 文字です。

デフォルト

このコマンドには、デフォルトの動作も値もありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン　トラストポイントが SCEP 登録用に設定されている場合、CA 証明書は SCEP 経由でダウンロードされます。トラストポイントが SCEP 登録用に設定されていない場合、セキュリティ アプライアンスは Base-64 形式の CA 証明書を端末に貼り付けるように要求します。

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例　次の例では、セキュリティ アプライアンスが CA の証明書を要求します。CA は証明書を送信し、セキュリティ アプライアンスは、管理者に CA 証明書のフィンガープリントをチェックして CA 証明書を確認するように要求します。セキュリティ アプライアンスの管理者は、表示されたフィンガープリントの値を既知の正しい値と照合する必要があります。セキュリティ アプライアンスによって表示されたフィンガープリントが正しい値と一致した場合は、その証明書を有効であるとして受け入れる必要があります。

```
hostname(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
hostname(config)#
```

次の例では、トラストポイント tp9 が端末ベース（手動）の登録用に設定されます。この場合、セキュリティ アプライアンスは管理者に CA 証明書を端末に貼り付けるように要求します。証明書のフィンガープリントを表示した後、セキュリティ アプライアンスは、管理者に証明書が保持されることを確認するように要求します。

```
hostname(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9Ccmlhbnl0DQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca enroll	CA への登録を開始します。
crypto ca import certificate	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入ります。

crypto ca certificate chain

指定したトラストポイントの証明書チェーン コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **crypto ca certificate chain** コマンドを使用します。グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用するか、**exit** コマンドを使用します。

crypto ca certificate chain *trustpoint*

シンタックスの説明

trustpoint	証明書チェーンを設定するトラストポイントを指定します。

デフォルト

このコマンドにデフォルト値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の CA 証明書チェーン サブモードに入ります。

```
hostname<config># crypto ca certificate chain central
hostname<config-cert-chain>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。

crypto ca certificate map

CA 証明書マップ モードに入るには、グローバル コンフィギュレーション モードで **crypto ca configuration map** コマンドを使用します。このコマンドを実行すると、CA 証明書マップ モードに入ります。証明書マッピング規則の優先順位付きリストを管理するには、このコマンドのグループを使用します。マッピング規則の順序はシーケンス番号によって決まります。

暗号 CA 証明書マップ規則を削除するには、このコマンドの **no** 形式を使用します。

crypto ca certificate map {*sequence-number* | *map-name sequence-number*}

no crypto ca certificate map {*sequence-number* | *map-name* [*sequence-number*]}

シンタックスの説明

map-name	certificate-to-group マップの名前を指定します。
sequence-number	作成する証明書マップ規則の番号を指定します。範囲は 1 ～ 65535 です。トンネル グループを証明書マップ規則にマッピングする tunnel-group-map を作成するときに、この番号を使用できます。

デフォルト

sequence-number のデフォルトの動作や値はありません。

map-name のデフォルトの値は、DefaultCertificateMap です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2	*map-name* キーワードが追加されました。

使用上のガイドライン

このコマンドを発行すると、セキュリティ アプライアンスは CA 証明書マップ コンフィギュレーション モードになります。このモードでは、証明書の発行者名およびサブジェクト認定者名（DN）に基づいて規則を設定できます。これらの規則の一般的な形式は次のとおりです。

DN match-criteria match-value

DN は、*subject-name* または *issuer-name* のいずれかです。DN は、ITU-T X.509 標準で定義されています。証明書フィールドのリストについては、関連コマンドを参照してください。

match-criteria は、次の表現または演算子で構成されます。

attr *tag*	比較を通常名（CN）などの特定の DN アトリビュートに制限します。
co	含む
eq	等しい
nc	含まない
ne	等しくない

DN の一致表現では大文字と小文字が区別されません。

例

次の例は、example-map というマップ名とシーケンス番号 1（規則番号 1）で CA 証明書マップ モードに入り、subject-name という通常名（CN）アトリビュートが Pat と一致する必要があることを指定しています。

```
hostname(config)# crypto ca certificate map example-map 1
hostname(ca-certificate-map)# subject-name attr cn eq pat
hostname(ca-certificate-map)#
```

次の例は、example-map というマップ名とシーケンス番号 1 で CA 証明書マップ モードに入り、subject-name 内のどこかに値 cisco が含まれることを指定しています。

```
hostname(config)# crypto ca certificate map example-map 1
hostname(ca-certificate-map)# subject-name co cisco
hostname(ca-certificate-map)#
```

関連コマンド

コマンド	説明
issuer-name	規則エントリが IPSec ピア証明書の発行者 DN に適用されることを指定します。
subject-name（暗号 CA 証明書マップ）	規則エントリが IPSec ピア証明書のサブジェクト DN に適用されることを指定します。
tunnel-group-map enable	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネル グループに関連付けます。

crypto ca crl request

指定したトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求するには、暗号 CA トラストポイント コンフィギュレーション モードで **crypto ca crl request** コマンドを使用します。

crypto ca crl request *trustpoint*

シンタックスの説明

trustpoint	トラストポイントを指定します。最大文字数は 128 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次の例では、central という名前のトラストポイントに基づいて CRL を要求します。

```
hostname(config)# crypto ca crl request central
hostname(config)#
```

関連コマンド

コマンド	説明
crl configure	crl 設定モードに入ります。

crypto ca enroll

CA との登録プロセスを開始するには、グローバル コンフィギュレーション モードで **crypto ca enroll** コマンドを使用します。このコマンドが正常に実行されるには、トラストポイントが正しく設定されている必要があります。

crypto ca enroll *trustpoint* [**noconfirm**]

シンタックスの説明

noconfirm	（オプション）すべてのプロンプトを表示しないようにします。要求されている場合がある登録オプションは、トラストポイントに事前設定されている必要があります。このオプションは、スクリプト、ASDM、または他の非対話型で使用するためのものです。
trustpoint	登録に使用するトラストポイントの名前を指定します。最大文字数は 128 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、セキュリティ アプライアンスはただちに CLI プロンプトを表示し、コンソールへのステータス メッセージを非同期的に表示します。トラストポイントが手動登録用に設定されている場合、セキュリティ アプライアンスは Base-64 符号化 PKCS10 認証要求をコンソールに書き込んでから、CLI プロンプトを表示します。

このコマンドは、参照されるトラストポイントの設定された状態に応じて異なる対話型のプロンプトを生成します。

例

次の例では、SCEP 登録を使用して、トラストポイント tp1 で ID 証明書を登録します。セキュリティ アプライアンスは、トラストポイント コンフィギュレーションで保存されていない情報を要求します。

```
hostname(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

hostname(config)#
```

次のコマンドは、CA 証明書の手動登録を示しています。

hostname(config)# **crypto ca enroll tp1**

```
% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca import pkcs12	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入ります。

crypto ca export

トラストポイント コンフィギュレーションに関連付けられたキーと証明書を PKCS12 形式でエクスポートするには、グローバル コンフィギュレーション モードで **crypto ca export** コマンドを使用します。

crypto ca export *trustpoint* ***pkcs12*** *passphrase*

シンタックスの説明

passphrase	エクスポートする PKCS12 ファイルの暗号化に使用するパスフレーズを指定します。
pkcs12	トラストポイント コンフィギュレーションのエクスポートに使用する公開キー暗号化標準を指定します。
trustpoint	証明書とキーをエクスポートするトラストポイントの名前を指定します。エクスポート時にトラストポイントが RSA キーを使用する場合、エクスポートされるキー ペアはトラストポイントと同じ名前を割り当てられます。

デフォルト

このコマンドにデフォルト値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。PKCS12 データは端末に書き込まれます。

例

次の例では、xxyyzz をパスコードとして使用して、トラストポイント central の PKCS12 データをエクスポートします。

```
hostname (config)# crypto ca export central pkcs12 xxyyzz

Exported pkcs12 follows:

[ PKCS12 data omitted ]

---End - This line not part of the pkcs12---

hostname (config)#
```

関連コマンド

コマンド	説明
crypto ca import pkcs12	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートします。
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入ります。

crypto ca import

手動登録要求への応答で CA から受信した証明書をインストール、または PKCS12 データを使用してトラストポイントの証明書とキー ペアをインポートするには、グローバル コンフィギュレーション モードで **crypto ca import** コマンドを使用します。セキュリティ アプライアンスは、Base-64 形式で端末にテキストを貼り付けるように要求します。

crypto ca import *trustpoint* **certificate** [**nointeractive**]

crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

シンタックスの説明

trustpoint	インポート アクションを関連付けるトラストポイントを指定します。最大文字数は 128 です。PKCS12 データをインポートし、トラストポイントが RSA キーを使用する場合、インポートされるキー ペアはトラストポイントと同じ名前を割り当てられます。
certificate	セキュリティ アプライアンスに、トラストポイントによって示される CA から証明書をインポートするように指示します。
pkcs12	セキュリティ アプライアンスに、PKCS12 形式を使用してトラストポイントの証明書とキー ペアをインポートするように指示します。
passphrase	PKCS12 データの暗号解除に使用するパスフレーズを指定します。
nointeractive	（オプション）非対話型モードを使用して証明書をインポートします。プロンプトをすべて表示しません。このオプションは、スクリプト、ASDM、または他の非対話型で使用するためのものです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント Main の証明書を手動でインポートします。

```
hostname (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
hostname (config)#
```

次の例では、PKCS12 データをトラストポイント central に手動でインポートします。

```
hostname (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
hostname (config)#
```

関連コマンド

コマンド	説明
crypto ca export	トラストポイントの証明書とキー ペアを PKCS12 形式でエクスポートします。
crypto ca authenticate	トラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入ります。

crypto ca trustpoint

指定したトラストポイントのトラストポイント サブモードに入るには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。指定したトラストポイントを削除するには、このコマンドの **no** 形式を使用します。このコマンドはトラストポイント情報を管理します。トラストポイントは、CA によって発行された証明書に基づいて CA の識別情報を表し、また、装置の識別情報を表すことがあります。トラストポイント サブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。このパラメータでは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが CA から証明書を取得する方法、および CA によって発行されるユーザ証明書の認証ポリシーを指定します。

crypto ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm***]*

シンタックスの説明

noconfirm	対話型のプロンプトをすべて表示しません。
trustpoint- name	管理するトラストポイントの名前を指定します。名前の最大長は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	Online Certificate Status Protocol（OSCP; オンライン証明書ステータス プロトコル）をサポートするためにサブコマンドが追加されました。**match certificate map**、**ocsp disable-nonce**、**ocsp url**、および **revocation-check** などのコマンドがあります。

使用上のガイドライン

CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。このコマンドを発行すると、暗号 CA トラストポイント コンフィギュレーション モードに入ります。

このマニュアルにアルファベット順に記載されている次のコマンドを使用して、トラストポイントの特性を指定できます。

- **accept-subordinates**：トラストポイントに関連付けられた CA に従属する CA 証明書が、装置にインストールされていない場合にフェーズ 1 の IKE 交換中に提供されたときに受け入れるかどうかを指定します。
- **crl required | optional | nocheck**：CRL コンフィギュレーション オプションを指定します。
- **crl configure**：CRL コンフィギュレーション サブモードに入ります（**crl** を参照）。

- **default enrollment**：すべての登録パラメータをシステム デフォルト値に戻します。このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。
- **email** *address*：登録中に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **enrollment retry period**：自動（SCEP）登録のリトライ期間を分単位で指定します。
- **enrollment retry count**：自動（SCEP）登録の許可されるリトライの最大回数を指定します。
- **enrollment terminal**：このトラストポイントを使用したカット アンド ペースト登録を指定します。
- **enrollment url** *url*：このトラストポイントを使用して登録する自動登録（SCEP）を指定し、登録 URL（*url*）を設定します。
- **exit**：サブモードを終了します。
- **fqdn** *fqdn*：登録中に、指定した完全修飾認定者名（FQDN）を証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **id-cert-issuer**：このトラストポイントに関連付けられた CA によって発行されるピア証明書をシステムが受け入れるかどうかを指定します。
- **ip-addr** *ip-address*：登録中に、セキュリティ アプライアンスの IP アドレスを証明書に含めるかどうかを CA に確認します。
- **keypair** *name*：公開キーを認証するキー ペアを指定します。
- **match certificate** *map-name* **override ocsp**：証明書マップを OCSP 上書き規則と照合します。
- **ocsp disable-nonce**：ナンス拡張子をディセーブルにします。この拡張子は、失効要求と応答を結び付けて暗号化して、リプレイ アタックを回避するためのものです。
- **ocsp url**：この URL の OCSP サーバで、このトラストポイントに関連するすべての証明書の失効ステータスをチェックすることを指定します。
- **exit**：サブモードを終了します。
- **password** *string*：登録中に CA に登録されるチャレンジ フレーズを指定します。CA は、通常、このフレーズを使用して、その後の失効要求を認証します。
- **revocation check**：失効ステータスをチェックする方法（CRL、OCSP、なし）を指定します。
- **serial-number**：登録中に、セキュリティ アプライアンスのシリアル番号を証明書に含めるかどうかを CA に確認します。
- **subject-name** *X.500 name*：登録中に、指定したサブジェクト DN を証明書に含めるかどうかを CA に確認します。
- **support-user-cert-validation**：イネーブルにした場合、トラストポイントがリモート証明書を発行した CA に対して認証されていれば、リモート ユーザ証明書を検証するコンフィギュレーション設定はこのトラストポイントから取得できます。このオプションは、サブコマンド **crl required | optional | nocheck** および CRL サブモードのすべての設定に関連付けられたコンフィギュレーション データに適用されます。

例

次の例では、central という名前のトラストポイントを管理するための CA トラストポイント モードに入ります。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca authenticate	このトラストポイントの CA 証明書を取得します。
crypto ca certificate map	暗号 CA 証明書マップ モードに入ります。証明書ベースの ACL を定義します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca import	手動登録要求への応答として CA から受信した証明書をインストールします。また、PKS12 データをトラストポイントにインポートします。

crypto dynamic-map match address

このコマンドの詳細については、crypto map match address コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

シンタックスの説明

acl-name	ダイナミック暗号マップ エントリに一致させるアクセス リストを指定します。
dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、aclist1 という名前のアクセス リストのアドレスに一致させる crypto dynamic-map コマンドの使用方法を示します。

```
hostname(config)# crypto dynamic-map mymap 10 match address aclist1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set nat-t-disable

接続の NAT-T をこの暗号マップ エントリに基づいてディセーブルにするには、グローバル コンフィギュレーション モードで **crypto dynamic-map set nat-t-disable** コマンドを使用します。この暗号マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルト設定はオフです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

isakmp nat-traversal コマンドを使用して、NAT-T をグローバルにイネーブルにします。その後、**crypto dynamic-map set nat-t-disable** コマンドを使用して、特定の暗号マップ エントリの NAT-T をディセーブルにできます。

例

次のコマンドは、mymap という名前のダイナミック暗号マップの NAT-T をディセーブルにします。

```
hostname(config)# crypto dynamic-map mymap 10 set nat-t-disable
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set peer

このコマンドの詳細については、**crypto map set peer** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。
ip_address	**name** コマンドで定義されているように、ダイナミック暗号マップ エントリのピアを IP アドレスで指定します。
hostname	**name** コマンドで定義されているように、ダイナミック暗号マップ エントリのピアをホスト名で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、mymap という名前のダイナミック マップのピアを IP アドレス 10.0.0.1 に設定します。

```
hostname(config)# crypto dynamic-map mymap 10 set peer 10.0.0.1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set pfs

このコマンドの詳細については、**crypto map set pfs** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5 | group 7]**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set pfs [group1 | group2 | group5 | group 7]**

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。
group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
set pfs	このダイナミック暗号マップ エントリ用の新しいセキュリティ アソシエーションの要求時に Perfect Forward Secrecy（PFS; 完全転送秘密）を要求するように IPSec を設定するか、または新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPSec を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更され、Diffie-Hellman group 7 が追加されました。

使用上のガイドライン

crypto dynamic-map コマンド（**match address**、**set peer**、**set pfs** など）については、**crypto map** コマンドの項で説明します。ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合は、ネゴシエーションに失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、セキュリティ アプライアンスはデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションで PFS が指定されていない場合は、ピアからの PFS のオファーがすべて受け入れられます。

セキュリティ アプライアンスは、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

次の例では、ダイナミック暗号マップ mymap 10 用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用することを指定します。指定されたグループはグループ 2 です。

```
hostname(config)# crypto dynamic-map mymap 10 set pfs group2
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set reverse route

このコマンドの詳細については、crypto map set reverse-route コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

シンタックスの説明

dynamic-map-name	暗号マップ セットの名前を指定します。
dynamic-seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、このコマンドの値はオフになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次のコマンドは、mymap という名前のダイナミック暗号マップの RRI をイネーブルにします。

```
hostname(config)# crypto dynamic-map mymap 10 set reverse route
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto dynamic-map	すべてのダイナミック暗号マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set transform-set

ダイナミック暗号マップ エントリで使用するトランスフォーム セットを指定するには、グローバル コンフィギュレーション モードで **crypto dynamic-map set transform-set** コマンドを使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

ダイナミック暗号マップ エントリからトランスフォーム セットを削除するには、このコマンドの **no** 形式で、削除するトランスフォーム セットの名前を指定します。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

すべてのトランスフォーム セットを指定するか、何も指定せずにこのコマンドの **no** 形式を使用すると、ダイナミック暗号マップ エントリが削除されます。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set transform-set**

シンタックスの説明

dynamic-map-name	ダイナミック暗号マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック暗号マップ エントリに対応するシーケンス番号を指定します。
transform-set-name1 *transform-set-name11*	トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドで定義されている必要があります。各暗号マップ エントリは、11 個までのトランスフォーム セットをサポートしています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	暗号マップ エントリにおけるトランスフォーム セットの最大数が変更されました。

使用上のガイドライン

ダイナミック暗号マップは、すべてのパラメータが設定されていない暗号マップです。ポリシーのテンプレートとして機能し、未設定のパラメータは、IPSec ネゴシエーションでピアに必要な条件を照合するときに動的にラーニングされます。セキュリティ アプライアンスは、スタティック暗号マップでピアの IP アドレスが特定されていない場合に、ピアでトンネルをネゴシエートさせるために動的マップを使用します。これは、次のようなピアに当てはまります。

- パブリック IP アドレスが動的に割り当てられる。

  LAN-to-LAN 接続のピアでも、リモート アクセスするピアでも、DHCP を使用してパブリック IP アドレスを取得します。セキュリティ アプライアンスは、このアドレスをトンネルを開始するときだけ使用します。
- プライベート IP アドレスが動的に割り当てられる。

  通常、リモート アクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられた IP アドレスを持っています。一般に、LAN-to-LAN トンネルには、事前に決定済みのプライベート ネットワークのセットがあり、スタティック マップを設定し、IPSec SA を確立するために使用されます。

管理者がスタティック暗号マップを設定するので、（DHCP または別の方法で）動的に割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。通常、VPN クライアントはスタティック IP アドレスを持たないので、IPSec ネゴシエーションを開始するには、ダイナミック暗号マップが必要です。たとえば、ヘッドセットが IKE のネゴシエーション中に Cisco VPN クライアントに IP アドレスを割り当て、クライアントはこのアドレスを IPSec SA のネゴシエーションで使用します。

ダイナミック暗号マップを使うと、IPSec の設定が簡単になります。ピアが常に事前に決定されていないネットワークで使用することをお勧めします。Cisco VPN クライアント（モバイル ユーザなど）や IP アドレスを動的に取得するルータがある場合に、ダイナミック暗号マップを使ってください。

ヒント　ダイナミック暗号マップの **permit** エントリに **any** キーワードを使うときは注意してください。マルチキャストやブロードキャストのトラフィックが **permit** エントリの対象となることもあるので、該当するアドレスの範囲について **deny** エントリをアクセス リストに挿入します。ネットワークとサブネットのブロードキャスト トラフィック、および IPSec で遮られない他のすべてのトラフィックについて **deny** エントリを挿入するようにしてください。

ダイナミック暗号マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。セキュリティ アプライアンスは、ダイナミック暗号マップを使用してリモート ピアと接続を開始することはできません。ダイナミック暗号マップを設定した場合は、発信トラフィックがアクセス リストで許可されていても、対応する SA が存在しないと、セキュリティ アプライアンスがトラフィックをドロップします。

暗号マップ セットには、ダイナミック暗号マップを含めることができます。ただし、ダイナミック暗号マップのセットには、一番低い優先度（優先度の数値が一番大きい）を設定し、セキュリティ アプライアンスがダイナミック暗号マップ以外のマップを先に評価するようにする必要があります。このように設定すると、他の（スタティック）マップのエントリが一致しない場合にだけ、ダイナミック暗号マップのセットを調べます。

スタティック暗号マップ セットと同様、ダイナミック暗号マップ セットにも、同じ dynamic-map-name を持つすべてのダイナミック暗号マップを含めます。dynamic-seq-num で、セット内のマップを区別します。ダイナミック暗号マップを設定する場合は、暗号アクセス リストに対して IPSec ピアのデータ フローを指示するために許可用の ACL を挿入してください。このように設定しないと、セキュリティ アプライアンスは、ピアが提示するデータ フローの ID をすべて受け入れることになります。

注意　ダイナミック暗号マップ セットを使用して設定されたセキュリティ アプライアンス インターフェイスに通じるトラフィックにスタティック ルート（デフォルト）を割り当てないでください。インターフェイスに通じるトラフィックを特定するには、ダイナミック暗号マップに ACL を追加します。リモート アクセス トンネル用の ACL を設定するときは、適切なアドレス プールを指定してください。トンネルがアップの状態になってから、逆ルート注入を使用してルートを指定します。

1 つの暗号マップ セットに、スタティックとダイナミックの両方のマップ エントリを含めることができます。

例

「crypto ipsec transform-set（トランスフォーム セットの作成または削除）」の項に、トランスフォーム セットに関するコマンド例を 10 例示しています。次の例では、その同じ 10 例のトランスフォーム セットからなる dynamic0 というダイナミック暗号マップ エントリを作成します。

```
hostname(config)# crypto dynamic-map dynamic0 1 set transform-set 3des-md5 3des-sha
56des-md5 56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec transform-set	トランスフォーム セットを設定します。
crypto map set transform-set	暗号マップ エントリで使用するトランスフォーム セットを指定します。
clear configure crypto dynamic-map	すべてのダイナミック暗号マップをコンフィギュレーションから消去します。
show running-config crypto dynamic-map	ダイナミック暗号マップのコンフィギュレーションを表示します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto ipsec df-bit

IPSec パケットの DF ビット ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec df-bit** コマンドを使用します。

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

シンタックスの説明

clear-df	（オプション）外部 IP ヘッダーは DF ビットを消去されること、およびセキュリティ アプライアンスはパケットをフラグメント化して IPSec カプセル化を追加する場合があることを指定します。
copy-df	（オプション）セキュリティ アプライアンスが外部 DF ビット設定を元のパケット内で探すことを指定します。
set-df	（オプション）外部 IP ヘッダーに DF ビットを設定することを指定します。しかし、元のパケットで DF ビットが消去されている場合、セキュリティ アプライアンスはパケットをフラグメント化することがあります。
interface	インターフェイス名を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。設定を指定せずにこのコマンドをイネーブルにすると、セキュリティ アプライアンスはデフォルトとして ***copy-df*** 設定を使用します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

DF ビットを IPSec トンネル機能と共に使用すると、セキュリティ アプライアンスがカプセル化されたヘッダーから Don't Fragment（DF）ビットを消去、設定、またはコピーできるかどうかが指定できます。IP ヘッダー内の DF ビットにより、装置がパケットをフラグメント化できるかどうかが決定されます。

カプセル化されたヘッダーに DF ビットを指定するようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **crypto *ipsec df-bit*** コマンドを使用します。

トンネル モードの IPSec トラフィックをカプセル化する場合は、DF ビットに ***clear-df*** 設定を使用します。この設定を使用すると、装置は使用可能な MTU のサイズよりも大きなパケットを送信できます。また、この設定は、使用可能な MTU のサイズが不明な場合にも適しています。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec DF ポリシーを **clear-df** に設定しています。

```
hostname(config)# crypto ipsec df-bit clear-df inside
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。
show crypto ipsec fragmentation	指定したインターフェイスのフラグメンテーション ポリシーを表示します。

crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec fragmentation** コマンドを使用します。

crypto ipsec fragmentation {**after-encryption** | **before-encryption**} *interface*

シンタックスの説明

after-encryption	暗号化の後で MTU の最大サイズに近い IPSec パケットをフラグメント化するようにセキュリティ アプライアンスに指定します(事前フラグメント化をディセーブルにします)。
before-encryption	暗号化の前に MTU の最大サイズに近い IPSec パケットをフラグメント化するようにセキュリティ アプライアンスに指定します(事前フラグメント化をイネーブルにします)。
interface	インターフェイス名を指定します。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

デフォルト

この機能はデフォルトでイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケットは、暗号化するセキュリティ アプライアンスの発信リンクの MTU のサイズに近い場合、IPSec ヘッダーを付けてカプセル化されると、発信リンクの MTU を超える可能性があります。MTU のサイズを超えると暗号化の後にパケットがフラグメント化され、このため暗号解除装置がプロセス パスで再組み立てされます。IPSec VPN の事前フラグメント化では、暗号解除装置はプロセス パスではなく高性能な CEF パスで動作するため、パフォーマンスが向上します。

IPSec VPN の事前フラグメント化では、暗号化装置は、IPSec SA の一部として設定されたトランスフォーム セットで使用可能な情報から、カプセル化されたパケット サイズを事前に設定します。装置でパケットが出力インターフェイスの MTU を超えることが事前に設定されている場合、装置は暗号化する前にそのパケットをフラグメント化します。これにより、暗号解除前のプロセス レベルの再組み立てが回避され、暗号解除のパフォーマンスおよび全体的な IPsec トラフィックのスループットの向上に役立ちます。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec パケットの事前フラグメント化を装置上でグローバルにイネーブルにします。

```
hostname(config)# crypto ipsec fragmentation before-encryption inside
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、IPSec パケットの事前フラグメント化をインターフェイス上でディセーブルにします。

```
hostname(config)# crypto ipsec fragmentation after-encryption inside
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPSec パケットの DF ビット ポリシーを設定します。
show crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを表示します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

crypto ipsec security-association lifetime

グローバル ライフタイム値を設定するには、グローバル コンフィギュレーション モードで **crypto ipsec security-association lifetime** コマンドを使用します。crypto ipsec エントリのライフタイム値をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto ipsec security-association lifetime {**seconds** *seconds* | **kilobytes** *kilobytes*}

シンタックスの説明

kilobytes	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。範囲は 10 ～ 2,147,483,647 KB です。デフォルトは 4,608,000 KB です。
seconds	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。範囲は 120 ～ 214783647 秒です。デフォルトは 28,800 秒（8 時間）です。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
1.1(1)	このコマンドが導入されました。

使用上のガイドライン

crypto ipsec security-association lifetime コマンドは、IPSec セキュリティ アソシエーションのネゴシエート時に使用されるグローバル ライフタイム値を変更します。

IPSec セキュリティ アソシエーションでは、共有秘密鍵を使用します。これらの鍵とセキュリティ アソシエーションは、両方同時にタイムアウトします。

個々の暗号マップ エントリでライフタイム値が設定されていない場合は、セキュリティ アソシエーションのネゴシエート中に新しいセキュリティ アソシエーションを要求するとき、セキュリティ アプライアンスは、ピアへの要求の中でグローバル ライフタイム値を指定します。この値を、新しいセキュリティ アソシエーションのライフタイムとして使用します。セキュリティ アプライアンスは、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定済みのライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します。

ライフタイムには、期間を指定するものとトラフィック量を指定するものの 2 つがあります。セキュリティ アソシエーションは、いずれかのライフタイムに最初に到達した時点で期限切れになります。

セキュリティ アプライアンスでは、暗号マップ、ダイナミック マップ、および ipsec 設定を動作中に変更できます。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ アプライアンスによって停止させられます。特に、アクセス リスト内のエントリを削除することによって、暗号マップに関連付けられている既存のアクセス リストを変更する場合は、関連する接続だけが停止させられます。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

グローバル期間ライフタイムを変更するには、**crypto ipsec security-association lifetime seconds** コマンドを使用します。期間ライフタイムを使用する場合は、指定した秒数が経過した時点でセキュリティ アソシエーションがタイムアウトします。

グローバル トラフィック量ライフタイムを変更するには、**crypto ipsec security-association lifetime kilobytes** コマンドを使用します。トラフィック量ライフタイムを使用する場合は、指定した量のトラフィック（KB 単位）がセキュリティ アソシエーション キーによって保護された時点で、セキュリティ アソシエーションがタイムアウトします。

ライフタイムを短くするほど、攻撃者がキー再現攻撃を成功させることが困難になります。攻撃者にとっては、解析の対象となる、同じキーで暗号化されたデータの量が少なくなるためです。ただし、ライフタイムを短くするほど、新しいセキュリティ アソシエーションの確立にかかる CPU 処理時間が長くなります。

セキュリティ アソシエーション（およびそれに対応するキー）は、指定した秒数または指定したトラフィック量（KB 単位）のうち、どちらかを超えた時点で有効期限が切れます。

例

次の例では、セキュリティ アソシエーションのグローバル期間ライフタイムを指定します。

```
hostname(config)# crypto ipsec-security association lifetime seconds 240
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての IPSec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）を消去します。
show running-config crypto map	すべての暗号マップのすべてのコンフィギュレーションを表示します。

crypto ipsec transform-set（トランスフォーム セットの作成または削除）

トランスフォーム セットを作成または削除するには、グローバル コンフィギュレーション モードで **crypto ipsec transform-set** コマンドを使用します。このコマンドを使用すると、トランスフォーム セットで使用される IPSec 暗号化およびハッシュ アルゴリズムを指定できます。トランスフォーム セットを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec transform-set *transform-set-name encryption* **[***authentication***]**

no crypto ipsec transform-set *transform-set-name encryption* **[***authentication***]**

シンタックスの説明

authentication	（オプション）IPSec のデータ フローの整合性を保証する認証方法を次の中から 1 つ指定します。 **esp-md5-hmac**：ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合 **esp-sha-hmac**：ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合 **esp-none**：HMAC 認証を使用しない場合
encryption	IPSec のデータ フローを保護する暗号化方法を次の中から 1 つ指定します。 **esp-aes**：128 ビット キーで AES を使用する場合 **esp-aes-192**：192 ビット キーで AES を使用する場合 **esp-aes-256**：256 ビット キーで AES を使用する場合 **esp-des**：56 ビットの DES-CBC を使用する場合 **esp-3des**：トリプル DES アルゴリズムを使用する場合 **esp-null**：暗号化を使用しない場合
transform-set-name	作成または変更するトランスフォーム セットの名前。すでにコンフィギュレーションに存在するトランスフォーム セットを表示するには、**show running-config ipsec** コマンドを入力します。

デフォルト

認証設定のデフォルトは、esp-none（認証しない）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	この項が改訂されました。

使用上のガイドライン

トランスフォーム セットを設定したら、そのセットを暗号マップに割り当てます。1 つの暗号マップにトランスフォーム セットを 6 つまで割り当てることができます。ピアが IPSec セッションを確立しようとする際、セキュリティ アプライアンスは、まず各暗号マップのアクセス リストとピアが一致するかどうかを調べます。次に、ピアがネゴシエートするすべてのプロトコル、アルゴリズム、その他の設定を、暗号マップに割り当てられているトランスフォーム セットと照合します。一致する設定が見つかった場合は、セキュリティ アプライアンスは、IPSec セキュリティ アソシエーションの一部としてその設定を、保護されたトラフィックに適用します。ピアがアクセス リストに一致しない場合や、暗号マップに割り当てられているトランスフォーム セット内に完全に一致するセキュリティ設定が見つからない場合、セキュリティ アプライアンスは IPSec セッションを終了します。

暗号化と認証のどちらを先に指定してもかまいません。また、認証を指定せずに暗号化を指定することもできます。作成しているトランスフォーム セットに認証を指定する場合は、暗号化も指定する必要があります。変更しているトランスフォーム セットに認証だけを指定した場合は、現在の暗号化設定がそのまま残ります。

AES 暗号化を指定する場合は、グローバル コンフィギュレーション モードでも **isakmp policy priority group 5** コマンドを使用して、AES の大きなサイズのキーを扱えるように Diffie-Hellman group 5 を割り当てることをお勧めします。

ヒント

暗号マップまたはダイナミック暗号マップにトランスフォーム セットを適用し、後でそのマップに割り当てられているトランスフォーム セットを表示する場合は、トランスフォーム セットに設定内容を表す名前を付けておくと便利です。たとえば、次に示す最初の例の 3des-md5 は、トランスフォーム セットで使用する暗号化と認証を示しています。その後に続く値は、トランスフォーム セットに割り当てる実際の暗号化と認証の設定です。

例

次のコマンドは、暗号化と認証をまったく設定しない場合を除く、すべてのオプションを示しています。

```
hostname(config)# crypto ipsec transform-set 3des-md5 esp-3des esp-md5-hmac
hostname(config)# crypto ipsec transform-set 3des-sha esp-3des esp-sha-hmac
hostname(config)# crypto ipsec transform-set 56des-md5 esp-des esp-md5-hmac
hostname(config)# crypto ipsec transform-set 56des-sha esp-des esp-sha-hmac
hostname(config)# crypto ipsec transform-set 128aes-md5 esp-aes esp-md5-hmac
hostname(config)# crypto ipsec transform-set 128aes-sha esp-aes esp-sha-hmac
hostname(config)# crypto ipsec transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
hostname(config)# crypto ipsec transform-set 192aes-sha esp-aes-192 esp-sha-hmac
hostname(config)# crypto ipsec transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
hostname(config)# crypto ipsec transform-set 256aes-sha esp-aes-256 esp-sha-hmac
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config ipsec	すべてのトランスフォーム セットの設定を表示します。
crypto map set transform-set	暗号マップ エントリで使用するトランスフォーム セットを指定します。
crypto dynamic-map set transform-set	ダイナミック暗号マップ エントリで使用するトランスフォーム セットを指定します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
show running-config crypto dynamic-map	ダイナミック暗号マップのコンフィギュレーションを表示します。

crypto ipsec transform-set mode transport

トランスフォーム セットの IPSec トランスポート モードを指定するには、グローバル コンフィギュレーション モードで **crypto ipsec transport-set mode transport** コマンドを使用します。トランスフォーム セットから IPSec トランスポート モードを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec transform-set *transform-set-name* **mode transport**

no crypto ipsec transform-set *transform-set-name* **mode transport**

シンタックスの説明

mode transport	トンネル モード要求に加えて、トランスポート モード要求を受け入れるためのトランスフォーム セットを指定します。
transform-set-name	変更するトランスフォーム セットの名前を指定します。トランスフォーム セットをすでに作成していることを前提としています。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

デフォルト

デフォルトはトンネル モードです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、トランスフォーム セットに対して IPSec トランスポート モードを指定します。Windows 2000 の L2TP/IPSec クライアントは IPSec トランスポート モードを使用するので、このトランスポート セットでトランスポート モードを選択する必要があります。デフォルトはトンネル モードです。

トンネル モードはトランスフォーム セットに対して自動的にイネーブルになります。セキュリティ アプライアンスは、Windows 2000 の L2TP/IPSec クライアントと通信する場合を除き（トランスポート モードを使用）、トンネル モードを使用します。

例

次の例では、暗号化に Triple DES を使用し、ハッシュ アルゴリズムに MD5/HMAC-128 を使用する transet5 という名前のトランスフォーム セットを設定してから、トランスフォーム セット transet5 に IPSec トランスポート モードを指定します。

```
hostname(config)# crypto ipsec transform-set transet5 esp-3des esp-md5-hmac
hostname(config)# crypto ipsec transform-set transet5 mode transport
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto	すべての ipsec コンフィギュレーション（たとえば、グローバル ライフタイムやトランスフォーム セット）を消去します。
clear configure crypto map	すべての暗号マップを消去します。
show running-config crypto map	すべての暗号マップのすべてのコンフィギュレーションを表示します。

crypto isakmp am-disable

アグレッシブ モードの着信接続をディセーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp am-disable** コマンドを使用します。アグレッシブ モードの着信接続をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp am-disable

no crypto isakmp am-disable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト値はイネーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp am-disable** コマンドが導入されました。
7.2.(1)	**isakmp am-disable** コマンドが、**crypto isakmp am-disable** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、アグレッシブ モードの着信接続をディセーブルにします。

```
hostname(config)# crypto isakmp am-disable
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp disconnect-notify

ピアに対する切断通知をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp disconnect-notify** コマンドを使用します。切断通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp disconnect-notify** コマンドが導入されました。
7.2.(1)	**isakmp disconnect-notify** コマンドが、**crypto isakmp disconnect-notify** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
hostname(config)# crypto isakmp disconnect-notify
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp enable

IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上で ISAKMP ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp enable** コマンドを使用します。インターフェイス上で ISAKMP ディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp enable *interface-name*

no crypto isakmp enable *interface-name*

シンタックスの説明

interface-name	ISAKMP ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	この **isakmp enable** コマンドは既存のものです。
7.2(1)	**isakmp enable** コマンドが、**crypto isakmp enable** コマンドに置き換えられました。

例

次の例は、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
hostname(config)# no crypto isakmp enable inside
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp identity

フェーズ 2 ID をピアに送信するように設定するには、グローバル コンフィギュレーション モードで **crypto isakmp identity** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

crypto isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

no crypto isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

シンタックスの説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	ISAKMP ネゴシエーションを、接続のタイプよって判別します（事前共有キーの IP アドレス、または証明書認証用の証明書 DN）。
hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用する文字列を指定します。

デフォルト

デフォルトの ISAKMP ID は、**crypto isakmp identity auto** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	**isakmp identity** コマンドは既存のものです。
7.2(1)	**isakmp identity** コマンドが、**crypto isakmp identity** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、IPSec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションを、接続タイプに応じてイネーブルにします。

```
hostname(config)# crypto isakmp identity auto
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp ipsec-over-tcp

IPSec over TCP をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto isakmp ipsec-over-tcp** コマンドを使用します。IPSec over TCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp ipsec-over-tcp [**port** *port1...port10*]

no crypto isakmp ipsec-over-tcp [**port** *port1...port10*]

シンタックスの説明

port *port1...port10*	（オプション）デバイスが IPSec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号の範囲は 1 ～ 65535 です。デフォルトのポート番号は 10000 です。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp ipsec-over-tcp** コマンドが導入されました。
7.2.(1)	**isakmpipsec-over-tcp** コマンドが、**crypto isakmpipsec-over-tcp** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、ポート 45 上で IPSec over TCP をイネーブルにします。

```
hostname(config)# crypto isakmp ipsec-over-tcp port 45
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp nat-traversal

NAT Traversal をグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP がイネーブルになっていることを確認し（イネーブルにするには **crypto isakmp enable** コマンドを使用します）、次に **crypto isakmp nat-traversal** コマンドを使用します。NAT Traversal がイネーブルのときに、これをディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

シンタックスの説明

natkeepalive	NAT キープアライブ間隔を 10 ～ 3,600 秒の範囲で設定します。デフォルトは 20 秒です。

デフォルト

デフォルトで、NAT Traversal（**crypto isakmp nat-traversal**）はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp nat-traversal** コマンドは既存のものです。
7.2.(1)	**isakmp nat-traversal** コマンドが、**crypto isakmp nat-traversal** コマンドに置き換えられました。

使用上のガイドライン

Network Address Translation（NAT; ネットワーク アドレス変換）は、Port Address Translation（PAT; ポート アドレス変換）も含め、IPSec も使用している多くのネットワークで使用されていますが、IPSec パケットが NAT デバイスを問題なく通過することを妨げる非互換性が数多くあります。NAT Traversal を使用すると、ESP パケットが 1 つまたは複数の NAT デバイスを通過できるようになります。

セキュリティ アプライアンスは、IETF の「UDP Encapsulation of IPsec Packets」ドラフトのバージョン 2 とバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に記述されているとおり NAT Traversal をサポートしています。NAT Traversal は、ダイナミックとスタティックの両方の暗号マップでサポートされています。

このコマンドは、セキュリティ アプライアンス上で NAT-T をグローバルにイネーブルにします。暗号マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次の例では、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、30 秒間隔で NAT Traversal をイネーブルにします。

```
hostname(config)# crypto isakmp enable
hostname(config)# crypto isakmp nat-traversal 30
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy

IKE ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

crypto isakmp policy *priority*

シンタックスの説明

priority	IKE ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2.(1)	このコマンドが導入されました。

使用上のガイドライン

crypto isakmp policy コマンドを使用すると、暗号 isakmp ポリシー モードに入って、認証、暗号化、グループ、ハッシュ、およびライフタイムの設定を行うことができます。

例

次の例は、グローバル コンフィギュレーション モードで、**crypto isakmp policy** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーで RSA シグニチャの認証方式を使用するように設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp reload-wait

すべてのアクティブなセッションが自主的が終了しないとセキュリティ アプライアンスをリブートできないようにするは、グローバル コンフィギュレーション モードで **crypto isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するのを待たずにセキュリティ アプライアンスをリブートするには、このコマンドの **no** 形式を使用します。

crypto isakmp reload-wait

no crypto isakmp reload-wait

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp reload-wait** コマンドが導入されました。
7.2.(1)	**isakmp reload-wait** コマンドが、**crypto isakmp reload-wait** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、すべてのアクティブなセッションが終了するまで待機してからリブートするように、セキュリティ アプライアンスに通知します。

```
hostname(config)# crypto isakmp reload-wait
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto key generate dsa

ID 証明書用の DSA キー ペアを生成するには、グローバル コンフィギュレーション モードで **crypto key generate dsa** コマンドを使用します。

crypto key generate dsa {**label** *key-pair-label*} [**modulus** *size*] [**noconfirm**]

シンタックスの説明

label *key-pair-label*	キー ペアに関連付ける名前を指定します。最大ラベル長は 128 文字です。DSA にはラベルが必要です。
modulus *size*	キー ペアのモジュール サイズ 512、768、または 1024 を指定します。デフォルトのモジュール サイズは 1024 です。
noconfirm	対話型のプロンプトをすべて表示しません。

デフォルト

デフォルトの係数サイズは 1024 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SSL、SSH、および IPSec 接続をサポートする DSA キー ペアを生成するには、**crypto key generate dsa** コマンドを使用します。生成されたキー ペアは、コマンド シンタックスの一部として指定したラベルで識別します。ラベルを指定しない場合、セキュリティ アプライアンスはエラー メッセージを表示します。

（注） DSA キーを生成するとき、遅延が発生する場合があります。Cisco PIX 515E Firewall では、この遅延が最大数分にわたることがあります。

例

グローバル コンフィギュレーション モードで入力した次の例では、mypubkey というラベルの DSA キー ペアを生成します。

```
hostname(config)# crypto key generate dsa label mypubkey
INFO: The name for the keys will be: mypubkey
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、誤って mypubkey というラベルの重複した DSA キー ペアを生成しようとしています。

```
hostname(config)# crypto key generate dsa label mypubkey
WARNING: You already have dSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new DSA keys named mypubkey
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key zeroize	DSA キー ペアを削除します。
show crypto key mypubkey	DSA キー ペアを表示します。

crypto key generate rsa

ID 証明書用の RSA キー ペアを生成するには、グローバル コンフィギュレーション モードで **crypto key generate rsa** コマンドを使用します。

crypto key generate rsa [**usage-keys | general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

シンタックスの説明

general-keys	一組の汎用キーを生成します。これはデフォルトのキー ペア タイプです。
label *key-pair-label*	キー ペアに関連付ける名前を指定します。このキー ペアのラベルは一意である必要があります。同じラベルで別のキー ペアを作成しようとすると、セキュリティ アプライアンスは警告メッセージを表示します。キーの生成時にラベルを指定しない場合、キー　　ペアはスタティックに <Default-RSA-Key> という名前が付けられます。
modulus *size*	キー ペアのモジュール サイズ 512、768、1024、または 2048 を指定します。デフォルトのモジュール サイズは 1024 です。
noconfirm	対話型のプロンプトをすべて表示しません。
usage-keys	シグニチャ用と暗号化用の 2 つのキー ペアを生成します。これは、対応する識別用に 2 通の証明書が必要なことを意味します。

デフォルト

デフォルトのキー ペア タイプは **general-keys** です。デフォルトの係数サイズは 1024 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SSL、SSH、および IPSec 接続をサポートする RSA キー ペアを生成するには、**crypto key generate rsa** コマンドを使用します。生成されたキー ペアは、コマンド シンタックスの一部として指定できるラベルで識別します。キー ペアを参照しないトラストポイントは、デフォルトの <Default-RSA-Key> を使用できます。SSH 接続では常にこのキーが使用されます。SSL は独自の証明書やキーをダイナミックに生成するため、トラストポイントに設定されていない限り、このことは SSL に影響を与えません。

例

グローバル コンフィギュレーション モードで入力した次の例では、mypubkey というラベルの RSA キー ペアを生成します。

```
hostname(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、誤って mypubkey というラベルの重複した RSA キー ペアを生成しようとしています。

```
hostname(config)# crypto key generate rsa label mypubkey
WARNING: You already have RSA keys defined named mypubkey
Do you really want to replace them? [yes/no] no
ERROR: Failed to create new RSA keys named mypubkey
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、デフォルト ラベルの RSA キー ペアを生成します。

```
hostname(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key zeroize	RSA キー ペアを削除します。
show crypto key mypubkey	RSA キー ペアを表示します。

crypto key zeroize

指定したタイプ（rsa または dsa）のキー ペアを削除するには、グローバル コンフィギュレーション モードで **crypto key zeroize** コマンドを使用します。

crypto key zeroize {**rsa** | **dsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

シンタックスの説明

default	ラベルがない RSA キー ペアを削除します。このキーワードは、RSA キー ペアに限り有効です。
dsa	キー タイプとして DSA を指定します。
label *key-pair-label*	指定したタイプ（rsa または dsa）のキー ペアを削除します。ラベルを指定しない場合、セキュリティ アプライアンスは指定したタイプのキー ペアをすべて削除します。
noconfirm	対話型のプロンプトをすべて表示しません。
rsa	キー タイプとして RSA を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

グローバル コンフィギュレーション モードで入力した次の例では、すべての RSA キー ペアを削除します。

```
hostname(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
hostname(config)#
```

関連コマンド

コマンド	説明
crypto key generate dsa	ID 証明書用の DSA キー ペアを生成します。
crypto key generate rsa	ID 証明書用の RSA キー ペアを生成します。

crypto map interface

定義済みの暗号マップ セットをインターフェイスに適用するには、グローバル コンフィギュレーション モードで **crypto map interface** コマンドを使用します。インターフェイスから暗号マップ セットを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name* **interface** *interface-name*

no crypto map *map-name* **interface** *interface-name*

シンタックスの説明

interface-name	セキュリティ アプライアンスが VPN ピアとのトンネルの確立に使用するインターフェイスを指定します。ISAKMP をイネーブルにしていて、認証局（CA）を使用して証明書を取得する場合には、CA 証明書内で指定されているアドレスを持つインターフェイスにする必要があります。
map-name	暗号マップ セットの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、暗号マップ セットをアクティブなセキュリティ アプライアンスのインターフェイスに割り当てるために使用します。セキュリティ アプライアンスでは、任意のアクティブ インターフェイスを IPSec の終端にできます。インターフェイスで IPSec サービスを提供するには、そのインターフェイスにまず暗号マップ セットを割り当てる必要があります。

インターフェイスに割り当てることができる暗号マップ セットは 1 つだけです。同じ *map-name* で *seq-num* が異なる暗号マップ エントリが複数ある場合、それらのエントリは同じセットの一部であり、そのインターフェイスにすべてが適用されます。セキュリティ アプライアンスは、*seq-num* が最も小さい暗号マップ エントリを最初に評価します。

（注） セキュリティ アプライアンスでは、暗号マップ、ダイナミック マップ、および ipsec 設定を動作中に変更できます。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ アプライアンスによって停止させられます。特に、アクセス リスト内のエントリを削除することによって、暗号マップに関連付けられている既存のアクセス リストを変更する場合は、関連する接続だけが停止させられます。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

（注） すべてのスタティック暗号マップは、アクセス リスト、トランスフォーム セット、および IPsec ピアの 3 つの部分を定義する必要があります。これらの 1 つが欠けている場合、暗号マップは不完全で、セキュリティ アプライアンスは次のエントリに進みます。しかし、暗号マップがアクセス リストでは一致するが、他の 2 つの要件のいずれかまたは両方で一致しない場合、このセキュリティ アプライアンスはトラフィックをドロップします。

すべての暗号マップが完全であることを確認するには、**show running-config crypto map** コマンドを使用します。不完全な暗号マップを修正するには、暗号マップを削除し、欠けているエントリを追加して再び適用します。

例

グローバル コンフィギュレーション モードで入力した次の例では、mymap という名前の暗号マップ セットを外部インターフェイスに割り当てます。トラフィックは、この外部インターフェイスを通過するとき、セキュリティ アプライアンスによって mymap セット内のすべての暗号マップ エントリと対照され、評価されます。発信トラフィックが mymap 暗号マップ エントリの 1 つのアクセス リストと一致する場合、セキュリティ アプライアンスはその暗号マップ エントリのコンフィギュレーションを使用して、セキュリティ アソシエーションを形成します。

```
hostname(config)# crypto map mymap interface outside
```

次の例は、必要な最小限の暗号マップ コンフィギュレーションを示しています。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap set transform-set my_t_set1
hostname(config)# crypto map mymap set peer 10.0.0.1
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map ipsec-isakmp dynamic

与えられた暗号マップ エントリに既存のダイナミック暗号マップを参照するように要求するには、グローバル コンフィギュレーション モードで **crypto map ipsec-isakmp dynamic** コマンドを使用します。相互参照を削除するには、このコマンドの **no** 形式を使用します。

ダイナミック暗号マップ エントリを作成するには、**crypto dynamic-map** コマンドを使用します。ダイナミック暗号マップ セットを作成したら、**crypto map ipsec-isakmp dynamic** コマンドを使用して、ダイナミック暗号マップ セットをスタティック暗号マップに追加します。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

シンタックスの説明

dynamic-map-name	既存のダイナミック暗号マップを参照する暗号マップ エントリの名前を指定します。
ipsec-isakmp	IKE がこの暗号マップ エントリの IPSec セキュリティ アソシエーションを確立することを指定します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが **ipsec-manual** キーワードを削除するように変更されました。

使用上のガイドライン

暗号マップ エントリを作成したら、**crypto map interface** コマンドを使用して、ダイナミック暗号マップ セットをインターフェイスに割り当てることができます。

ダイナミック暗号マップを使用することで、保護の対象となるトラフィックのフィルタリングと分類、そのトラフィックに適用するポリシーの定義という 2 つの機能を利用できます。最初の機能はインターフェイス上のトラフィック フローが対象となり、2 番目の機能は（IKE を通じた）そのトラフィックのためのネゴシエーションが対象となります。

IPSec ダイナミック暗号マップは次の 4 つを指定します。

- 保護するトラフィック
- セキュリティ アソシエーションを確立する IPSec ピア
- 保護対象のトラフィックと共に使用するトランスフォーム セット
- キーおよびセキュリティ アソシエーションの使用方法または管理方法

暗号マップ セットは、それぞれ異なるシーケンス番号（seq-num）を持ち、マップ名が共通している暗号マップ エントリの集合です。たとえば、所定のインターフェイスを介して、あるトラフィックには所定のセキュリティを適用してピアに転送し、その他のトラフィックには別の IPSec セキュリティを適用して同じまたは別個のピアに転送するとします。このような構成をセットアップするには、2 つの暗号マップ エントリを作成します。マップ名は同じ名前にし、シーケンス番号をそれぞれ別の番号にします。

シーケンス番号引数として割り当てる番号は、任意に決定しないようにしてください。この番号は、暗号マップ セットに含まれている複数の暗号マップ エントリにランクを付けます。シーケンス番号の小さい暗号マップ エントリが番号の大きいエントリよりも先に評価されます。つまり、番号の小さいマップ エントリは優先順位が高くなります。

（注） 暗号マップをダイナミック暗号マップにリンクする場合は、ダイナミック暗号マップを指定する必要があります。指定すると、**crypto dynamic-map** コマンドを使用して以前に定義した既存のダイナミック暗号マップに暗号マップがリンクされます。暗号マップ エントリが変換された後に加えた変更は、有効になりません。たとえば、set peer 設定への変更は有効になりません。しかし、セキュリティ アプライアンスは起動中に変更を保存します。ダイナミック暗号マップを暗号マップに変換して戻す場合、変更は有効で、**show running-config crypto map** コマンドの出力に表示されます。セキュリティ アプライアンスは、リブートされるまでこれらの設定を維持します。

例

グローバル コンフィギュレーション モードで入力した次のコマンドでは、暗号マップ mymap を test という名前のダイナミック暗号マップを参照するように設定します。

```
hostname(config)# crypto map mymap ipsec-isakmp dynamic test
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map match address

アクセス リストを暗号マップ エントリに割り当てるには、グローバル コンフィギュレーション モードで **crypto map match address** コマンドを使用します。暗号マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

シンタックスの説明

acl_name	暗号化アクセス リストの名前を指定します。この名前は、一致対象となる名前付き暗号化アクセス リストの名前引数と一致している必要があります。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、すべてのスタティック暗号マップに対して指定必須となるコマンドです。**crypto dynamic-map** コマンドでダイナミック暗号マップを定義する場合は、このコマンドは必須ではありませんが、使用することを強く推奨します。

アクセス リストを定義するには、**access-list** コマンドを使用します。

セキュリティ アプライアンスは、アクセ スリストを利用して、IPSec 暗号で保護するトラフィックと保護を必要としないトラフィックを区別します。また、許可 ACE に一致する発信パケットを保護し、許可 ACE に一致する着信パケットが保護されるようにします。

セキュリティ アプライアンスがパケットを deny 文と照合する場合、暗号マップ内の残りのアクセス コントロール エントリ（ACE）に対するパケットの評価を省略し、順番に次の暗号マップ内の ACE に対するパケットの評価を再開します。*ACL のカスケード処理*には、ACL 内の残りの ACE の評価をバイパスする拒否 ACE の使用、および暗号マップ セット内の次の暗号マップに割り当てられた ACL に対するトラフィックの評価の再開が含まれています。各暗号マップを別の IPSec 設定に関連付けることができるため、拒否 ACE を使用して対応する暗号マップの詳細な評価から特別なトラフィックを除外し、特別なトラフィックを別の暗号マップの permit 文と一致させて別のセキュリティを提供または要求できます。

(注)　暗号化用のアクセス　リストは、インターフェイスを通過するトラフィックを許可するかどうかを判定しません。このような判定には、**access-group** コマンドを使用してインターフェイスに直接適用されるアクセス リストが使用されます。

(注)　透過モードでは、宛先アドレスはセキュリティ アプライアンスの IP アドレス、管理アドレスである必要があります。透過モードでは、セキュリティ アプライアンスへのトンネルだけが許可されます。

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set connection-type

この暗号マップ エントリのバックアップ サイトツーサイト機能の接続タイプを指定するには、グローバル コンフィギュレーション モードで **crypto map set connection-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

no crypto map *map-name seq-num* **set connection-type {answer-only | originate-only | bidirectional}**

シンタックスの説明

answer-only	このピアが、適切な接続先ピアを決定するための初期の専用交換中に、最初は着信 IKE 接続だけに応答することを指定します。
bidirectional	このピアが、この暗号マップ エントリに基づいて接続を受け入れ、発信できることを指定します。これはすべてのサイトツーサイト接続のデフォルトの接続タイプです。
map-*name*	暗号マップ セットの名前を指定します。
originate-only	このピアが、適切な接続先ピアを決定するための最初の専用交換を開始することを指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
set connection-type	この暗号マップ エントリのバックアップ サイトツーサイト機能の接続タイプを指定します。answer-only、originate-only、および bidirectional の 3 タイプの接続があります。

デフォルト

デフォルト設定は bidirectional です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

* 透過ファイアウォール モードでは、このコマンドは表示されますが、インターフェイスに対応付けられた暗号マップに含まれる暗号マップ エントリでは、connection-type 値は answer-only 以外の値に設定できません。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

crypto map set connection-type コマンドは、バックアップ Lan-to-Lan 機能の接続タイプを指定します。接続の一方の側で複数のバックアップ ピアを指定することができます。

この機能は、次のプラットフォーム間のみで動作します。

- 2 つの Cisco ASA 5500 シリーズ セキュリティ アプライアンス
- Cisco ASA 5500 シリーズ セキュリティ アプライアンスと Cisco VPN 3000 コンセントレータ

- Cisco ASA 5500 シリーズ セキュリティ アプライアンスと、Cisco PIX セキュリティ アプライアンス ソフトウェア v7.0 以上を実行しているセキュリティ アプライアンス

バックアップ Lan-to-Lan 接続を設定するには、接続の一方の側を **originate-only** キーワードを使用して originate-only として設定し、複数のバックアップ ピアのある側を **answer-only** キーワードを使用して answer-only として設定することをお勧めします。originate-only 側では、**crypto map set peer** コマンドを使用してピアの優先順位を指定します。originate-only セキュリティ アプライアンスは、リストの最初のピアとネゴシエートしようとします。ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、リストにピアがなくなるまで下に向かってリストを検索します。

このように設定した場合、originate-only ピアは専用のトンネルを確立してピアとネゴシエートしようとします。その後は、いずれかのピアが通常の Lan-to-Lan 接続を確立することができ、いずれかの側からのデータがトンネル接続を開始できます。

表 9-1 に、サポートされるすべての設定を示します。これら以外の組み合せでは、予測できないルーティング問題が生じることがあります。

表 9-1　サポートされるバックアップ LAN-to-LAN 接続タイプ

リモート側	中央側
originate-only	answer-only
bidirectional	answer-only
bidirectional	bidirectional

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、接続タイプを originate-only に設定します。

```
hostname(config)# crypto map mymap 10 set connection-type originate-only
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set inheritance

この暗号マップ エントリ用に生成されるセキュリティ アソシエーションの精度（シングルまたはマルチ）を設定するには、グローバル コンフィギュレーション モードで **set inheritance** コマンドを使用します。この暗号マップ エントリの継承の設定を削除するには、このコマンドの no 形式を使用します。

crypto map *map-name seq-num* **set inheritance {data| rule}**

no crypto map *map-name seq-num* **set inheritance {data | rule}**

シンタックスの説明

data	規則で指定されているアドレス範囲内のすべてのアドレス ペアに 1 つのトンネルを指定します。
map-name	暗号マップ セットの名前を指定します。
rule	この暗号マップに関連付けられている各 ACL エントリに 1 つのトンネルを指定します。これはデフォルトの値です。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
set inheritance	継承のタイプを **data** または **rule** に指定します。継承では、各セキュリティ ポリシー データベース（SPD）規則に対して 1 つのセキュリティ アソシエーション（SA）を生成したり、範囲内の各アドレス ペアに対して複数のセキュリティ SA を生成したりすることができます。

デフォルト

デフォルト値は、***rule*** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、セキュリティ アプライアンスがトンネルに応答しているときではなく、トンネルを開始しているときのみ動作します。データ設定を使用すると、多数の IPSec SA が作成される可能性があります。この場合、メモリが消費され、全体的なトンネルが少なくなります。データ設定は、セキュリティ依存型のアプリケーションに対してのみ使用する必要があります。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、継承タイプを data に設定します。

```
hostname(config)# crypto map mymap 10 set inheritance data
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set nat-t-disable

接続の NAT-T をこの暗号マップ エントリに基づいてディセーブルにするには、グローバル コンフィギュレーション モードで **crypto map set nat-t-disable** コマンドを使用します。この暗号マップ エントリの NAT-T をイネーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* ***set nat-t-disable***

no crypto map *map-name seq-num* ***set nat-t-disable***

シンタックスの説明

map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

このコマンドのデフォルト設定はオンではありません（したがって、NAT-T はデフォルトでイネーブルです）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

isakmp nat-traversal コマンドを使用して、NAT-T をグローバルにイネーブルにします。その後、**crypto map set nat-t-disable** コマンドを使用して、特定の暗号マップ エントリの NAT-T をディセーブルにできます。

例

グローバル コンフィギュレーション モードで入力した次のコマンドは、mymap という名前の暗号マップ エントリの NAT-T をディセーブルにします。

```
hostname(config)# crypto map mymap 10 set nat-t-disable
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
isakmp nat-traversal	すべての接続の NAT-T をイネーブルにします。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set peer

暗号マップ エントリの IPSec ピアを指定するには、グローバル コンフィギュレーション モードで **crypto map set peer** コマンドを使用します。暗号マップ エントリから IPSec ピアを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address* | *hostname10*}

シンタックスの説明

hostname	ピアをセキュリティ アプライアンスの **name** コマンドで定義したホスト名で指定します。
ip_address	ピアを IP アドレスで指定します。
map-name	暗号マップ セットの名前を指定します。
peer	暗号マップ エントリの IPSec ピアをホスト名または IP アドレスで指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが、最大 10 のピア アドレスを許容するように変更されました。

使用上のガイドライン

このコマンドは、すべてのスタティック暗号マップに対して指定必須となるコマンドです。**crypto dynamic-map** コマンドでダイナミック暗号マップ エントリを定義する場合には、このコマンドは必須ではなく、ほとんど使用しません。これは、ピアが通常は未知のものであるためです。

複数のピアを設定することは、フォールバック リストを指定することと同じです。トンネルごとに、セキュリティ アプライアンスはリストの最初のピアとネゴシエートしようとします。ピアが応答しない場合、セキュリティ アプライアンスはピアが応答するか、リストにピアがなくなるまで下に向かってリストを検索します。バックアップ LAN-to-LAN 機能を使用している場合（つまり暗号マップ接続タイプが originate-only の場合）にのみ複数のピアを設定できます。詳細については、**crypto map set connection-type** コマンドを参照してください。

例

グローバル コンフィギュレーション モードで入力した次の例は、IKE を使用してセキュリティ アソシエーションを確立する暗号マップ コンフィギュレーションを示します。この例では、ピア 10.0.0.1 またはピア 10.0.0.2 に対するセキュリティ アソシエーションをセットアップできます。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 match address 101
hostname(config)# crypto map mymap 10 set transform-set my_t_set1
hostname(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set pfs

この暗号マップ エントリ用の新しいセキュリティ アソシエーションの要求時に完全転送秘密（PFS）を要求するように IPSec を設定するか、または新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPSec を設定するには、グローバル コンフィギュレーション モードで **crypto map set pfs** コマンドを使用します。IPSec が PFS を要求しないことを指定するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group7]**

no crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group7]**

シンタックスの説明

group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、PFS は設定されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが変更され、Diffie-Hellman group 7 が追加されました。

使用上のガイドライン

PFS を使用すると、新しいセキュリティ アソシエーションをネゴシエートするたびに新しい Diffie-Hellman 交換が発生します。この交換によって、処理にかかる時間が長くなります。PFS を使用すると、セキュリティがいっそう向上します。1 つのキーが攻撃者によってクラックされた場合でも、信頼性が損なわれるのはそのキーで送信されたデータだけになるためです。

このコマンドを使用すると、暗号マップ エントリ用の新しいセキュリティ アソシエーションを要求するとき、ネゴシエート中に IPSec が PFS を要求します。**set pfs** 文でグループが指定されていない場合、セキュリティ アプライアンスはデフォルト（group2）を送信します。

ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合は、ネゴシエーションに失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、セキュリティ アプライアンスはデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションで group2、group5、または group7 が指定されている場合は、そのグループがピアのオファーに含まれている必要があります。含まれていない場合は、ネゴシエーションに失敗します。

ネゴシエーションが成功するには、両端に PFS が設定されている必要があります。設定されている場合、グループは完全に一致する必要があります。セキュリティ アプライアンスは、ピアからの PFS のオファーをすべて受け入れません。

1536 ビットの Diffie-Hellman プライム モジュラス グループ group5 は、group1 や group2 よりも高いセキュリティを提供します。ただし、他のグループより処理時間が長くなります。

楕円曲線フィールドのサイズが 163 ビットである Diffie-Hellman Group 7 では、IPSec SA キーが生成されます。このオプションは、任意の暗号化アルゴリズムと共に使用できます。これは、movianVPN クライアントで使用するためのオプションですが、Group 7（ECC）をサポートしている任意のピアで使用できます。

セキュリティ アプライアンスは、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ「mymap 10」用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用することを指定します。

```
hostname(config)# crypto map mymap 10 ipsec-isakmp
hostname(config)# crypto map mymap 10 set pfs group2
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
tunnel-group	トンネル グループとそのパラメータを設定します。

crypto map set phase1 mode

メインまたはアグレッシブへの接続を開始する場合にフェーズ 1 の IKE モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set phase1mode** コマンドを使用します。フェーズ 1 IKE ネゴシエーションの設定を削除するには、このコマンドの **no** 形式を使用します。アグレッシブ モードの Diffie-Hellman グループを含めることはオプションです。含めない場合、セキュリティ アプライアンスは group 2 を使用します。

crypto map *map-name seq-num* **set phase1mode {main | aggressive [group1 | group2 | group5 | group7]}**

no crypto map *map-name seq-num* **set phase1mode {main | aggressive [group1 | group2 | group5 | group7]}**

シンタックスの説明

aggressive	フェーズ 1 IKE ネゴシエーションにアグレッシブ モードを指定します。
group1	IPSec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPSec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPSec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group7	IPSec が、たとえば movianVPN クライアントで、楕円曲線フィールドのサイズが 163 ビットである group7（ECC）を使用するように指定します。
main	フェーズ 1 IKE ネゴシエーションにメイン モードを指定します。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトのフェーズ 1 のモードは、**main** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、発信側モードでのみ動作します。応答側モードでは動作しません。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap を設定し、group2 を使用してフェーズ 1 のモードをアグレッシブに設定します。

```
hostname(config)# crypto map mymap 10 set phase1mode aggressive group2
hostname(config)#
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set reverse-route

この暗号マップ エントリに基づいて任意の接続の RRI をイネーブルにするには、グローバル コンフィギュレーション モードで **crypto map set reverse-route** コマンドを使用します。この暗号マップ エントリに基づいた任意の接続の逆ルート注入をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* ***set reverse-route***

no crypto map *map-name seq-num* ***set reverse-route***

シンタックスの説明

map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、このコマンドの設定はオフになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたは境界ルータに通知できます。

例

グローバル コンフィギュレーション モードで入力した次の例では、mymap という名前の暗号マップの RRI をイネーブルにします。

```
hostname(config)# crypto map mymap 10 set reverse-route
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set security-association lifetime

特定の暗号マップ エントリについて、IPSec セキュリティ アソシエーションをネゴシエートするときに使用されるグローバル ライフタイム値を上書きするには、グローバル コンフィギュレーション モードで **crypto map set security-association lifetime** コマンドを使用します。暗号マップ エントリのライフタイム値をグローバル値にリセットするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set security-association lifetime {seconds** *seconds* | **kilobytes** *kilobytes*}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *seconds* | **kilobytes** *kilobytes*}

シンタックスの説明

kilobytes	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。 デフォルトは 4,608,000 KB です。
map-name	暗号マップ セットの名前を指定します。
seconds	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。デフォルトは 28,800 秒（8 時間）です。
seq-num	暗号マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

暗号マップのセキュリティ アソシエーションは、グローバル ライフタイム値に基づいてネゴシエートされます。

IPSec セキュリティ アソシエーションでは、共有秘密鍵を使用します。これらの鍵とセキュリティ アソシエーションは、両方同時にタイムアウトします。

特定の暗号マップ エントリでライフタイム値が設定されている場合は、セキュリティ アソシエーションのネゴシエート中に新しいセキュリティ アソシエーションを要求するとき、セキュリティ アプライアンスは、ピアへの要求の中でこの暗号マップ ライフタイム値を利用します。この値を、新しいセキュリティ アソシエーションのライフタイムとして使用します。セキュリティ アプライアンスは、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定済みのライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します。

ライフタイムには、期間を指定するものとトラフィック量を指定するものの 2 つがあります。セッション キーとセキュリティ アソシエーションは、いずれかのライフタイムに最初に到達した時点で期限切れになります。1 つのコマンドで両方を指定できます。

（注） セキュリティ アプライアンスでは、暗号マップ、ダイナミック マップ、および ipsec 設定を動作中に変更できます。これを行う場合は、変更によって影響を受ける接続だけがセキュリティ アプライアンスによって停止させられます。特に、アクセス リスト内のエントリを削除することによって、暗号マップに関連付けられている既存のアクセス リストを変更する場合は、関連する接続だけが停止させられます。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

期間ライフタイムを変更するには、**crypto map set security-association lifetime seconds** コマンドを使用します。期間ライフタイムを使用する場合は、指定した秒数が経過した時点でキーおよびセキュリティ アソシエーションがタイムアウトします。

例

グローバル コンフィギュレーション モードで次のコマンドを入力すると、暗号マップ mymap のセキュリティ アソシエーション ライフタイムが秒単位および KB 単位で指定されます。

```
hostname(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set transform-set

暗号マップ エントリで使用するトランスフォーム セットを指定するには、グローバル コンフィギュレーション モードで **crypto map set transform-set** コマンドを使用します。

crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

暗号マップ エントリからトランスフォーム セットを削除するには、このコマンドの **no** 形式で、削除するトランスフォーム セットの名前を指定します。

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1* [*… transform-set-name11*]

すべてのトランスフォーム セットを指定するか何も指定せずにこのコマンドの **no** 形式を使用すると、暗号マップ エントリが削除されます。

no crypto map *map-name seq-num* **set transform-set**

シンタックスの説明

map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリのシーケンス番号を指定します。
transform-set-name1 *transform-set-name11*	トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドで定義されている必要があります。各暗号マップ エントリは、11 個までのトランスフォーム セットをサポートしています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.2(1)	暗号マップ エントリにおけるトランスフォーム セットの最大数が変更されました。

使用上のガイドライン

このコマンドは、すべての暗号マップ エントリに対して指定必須となるコマンドです。

IPSec 接続の開始側と反対側にあるピアは、最初に一致したトランスフォーム セットをセキュリティ アソシエーションで使用します。ローカルのセキュリティ アプライアンスがネゴシエーションを開始した場合は、**crypto map** コマンドで指定した順番どおりに、トランスフォームセットの内容をピアに提示します。ピアがネゴシエーションを開始すると、ローカルのセキュリティ アプライアンスは、暗号マップ エントリの中で、ピアから送られた IPSec パラメータと一致する最初のトランスフォーム セットを使用します。

IPSec 接続の開始側とは反対側にあるピアが、一致するトランスフォーム セットを見つけられない場合、セキュリティ アソシエーションは確立されません。トラフィックを保護するセキュリティ アソシエーションがないので、開始側はトラフィックをドロップします。

トランスフォーム セットのリストを変更するには、古いリストの代わりになる新しいリストを指定します。

このコマンドで暗号マップを変更する場合は、指定したシーケンス番号と同じ番号の暗号マップ エントリだけが変更されます。たとえば、次のコマンドを入力した場合、56des-sha というトランスフォーム セットがリストの最後に挿入されます。

```
hostname(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
hostname(config)# crypto map map1 1 transform-set 56des-sha
hostname(config)#
```

次のコマンドの応答は、上記の 2 つのコマンドで行った変更を合せたものになります。

```
hostname(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
hostname(config)#
```

暗号マップ エントリ内のトランスフォーム セットの順番を変えるには、まずエントリを削除し、マップ名とシーケンス番号の両方を指定してから、エントリを作成し直します。たとえば、次のコマンドは、シーケンス番号 3 の map2 という暗号マップ エントリを再設定します。

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

例

「crypto ipsec transform-set（トランスフォーム セットの作成または削除）」の項に、トランスフォーム セットに関するコマンド例を 10 例示しています。次の例では、その同じ 10 例のトランスフォーム セットからなる暗号マップ エントリ map2 を作成します。

```
hostname(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例は、セキュリティ アプライアンスが IKE を使用してセキュリティ アソシエーションを確立する場合に必要となる、最小限の暗号マップ コンフィギュレーションを示しています。

```
hostname(config)# crypto map map2 10 ipsec-isakmp
hostname(config)# crypto map map2 10 match address 101
hostname(config)# crypto map map2 set transform-set 3des-md5
hostname(config)# crypto map map2 set peer 10.0.0.1
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック暗号マップをコンフィギュレーションから消去します。
clear configure crypto map	すべての暗号マップをコンフィギュレーションから消去します。
crypto dynamic-map set transform-set	ダイナミック暗号マップ エントリで使用するトランスフォーム セットを指定します。
crypto ipsec transform-set	トランスフォーム セットを設定します。
show running-config crypto dynamic-map	ダイナミック暗号マップのコンフィギュレーションを表示します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。

crypto map set trustpoint

暗号マップ エントリのフェーズ 1 ネゴシエーション中に、認証用に送信する証明書を指定するトラストポイントを指定するには、グローバル コンフィギュレーション モードで **crypto map set trustpoint** コマンドを使用します。暗号マップ エントリからトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

nocrypto map *map-name seq-num* **set trustpoint** *trustpoint-name* **[chain]**

シンタックスの説明

chain	（オプション）証明書チェーンを送信します。CA 証明書チェーンには、ルート証明書から ID 証明書まで、証明書の階層内のすべての CA 証明書が含まれています。デフォルト値はディセーブル（チェーンなし）です。
map-name	暗号マップ セットの名前を指定します。
seq-num	暗号マップ エントリに割り当てる番号を指定します。
trustpoint- name	フェーズ 1 ネゴシエーション中に送信する証明書を指定します。デフォルトは none です。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

デフォルト

デフォルト値は none です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この暗号マップ コマンドは、接続の開始に限り有効です。応答側の情報については、**tunnel-group** コマンドを参照してください。

例

グローバル コンフィギュレーション モードで入力した次の例では、暗号マップ mymap に tpoint1 という名前のトラストポイントを指定し、証明書のチェーンを指定します。

```
hostname(config)# crypto map mymap 10 set trustpoint tpoint1 chain
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	すべての暗号マップのすべてのコンフィギュレーションを消去します。
show running-config crypto map	暗号マップのコンフィギュレーションを表示します。
tunnel-group	トンネル グループを設定します。

CSC

セキュリティ アプライアンスでネットワーク トラフィックを CSC SSM に送信するのをイネーブルにするには、クラス コンフィギュレーション モードで **csc** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

csc {***fail-open*** | ***fail-close***}

no csc

シンタックスの説明

fail-close	CSC SSM が失敗した場合、セキュリティ アプライアンスがトラフィックをブロックする必要があることを指定します。これは、クラス マップで選択されたトラフィックだけに適用します。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。
fail-open	CSC SSM が失敗した場合、セキュリティ アプライアンスがトラフィックを許可する必要があることを指定します。これは、クラス マップで選択されたトラフィックだけに適用します。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

csc コマンドは、該当するクラス マップによって照合されたトラフィックすべてを CSC SSM に送信するようにセキュリティ ポリシーを設定します。この設定の後、セキュリティ アプライアンスはトラフィックが宛先に進み続けるのを許可します。

CSC SSM がトラフィックをスキャンできない場合に、セキュリティ アプライアンスが一致しているトラフィックを取り扱う方法を指定できます。***fail-open*** キーワードは、CSC SSM が利用できない場合でも、トラフィックが宛先に進み続けるのをセキュリティ アプライアンスが許可するように指定します。***fail-close*** キーワードは、CSC SSM が使用できない場合に、一致しているトラフィックが宛先に進み続けるのをセキュリティ アプライアンスが許可しないように指定します。

CSC SSM は、HTTP、SMTP、POP3、および FTP トラフィックをスキャンできます。これは、接続を要求しているパケットの宛先ポートが、これらのプロトコルにとって既知のものである場合に限りサポートします。つまり、CSC SSM は次の接続に限りスキャンできます。

- TCP ポート 21 に対してオープンされている FTP 接続
- TCP ポート 80 に対してオープンされている HTTP 接続

- TCP ポート 110 に対してオープンされている POP3 接続
- TCP ポート 25 に対してオープンされている SMTP 接続

csc コマンドを使用しているポリシーが、他のプロトコルに対してこれらのポートを間違って使用している接続を選択している場合、セキュリティ アプライアンスはパケットを CSC SSM に渡しますが、CSC SSM はそれをスキャンせずに渡します。

CSC SSM の効率を最大限にするには、次のように **csc** コマンドを実装しているポリシーが使用するクラス マップを設定します。

- サポートされているプロトコルのうち CSC SSM がスキャンするプロトコルだけを選択します。たとえば、HTTP トラフィックをスキャンしない場合は、サービス ポリシーが絶対に HTTP トラフィックを CSC SSM に転送しないようにしてください。
- セキュリティ アプライアンスによって保護されている信頼できるホストを、危険にさらす接続だけを選択します。これらは、外部のネットワークまたは信頼できないネットワークから内部のネットワークへの接続です。次の接続をスキャンすることを推奨します。
  - 発信 HTTP 接続
  - セキュリティ アプライアンスの内部のクライアントからセキュリティ アプライアンスの外部のサーバへの FTP 接続
  - セキュリティ アプライアンスの内部のクライアントからセキュリティ アプライアンスの外部のサーバへの POP3 接続
  - 内部メール サーバ宛ての着信 SMTP 接続

FTP スキャン

CSC SSM は、FTP セッションのプライマリ チャネルが標準ポート（TCP ポート 21）を使用している場合に限り、FTP ファイル転送のスキャンをサポートします。

FTP 検査は、CSC SSM によりスキャンする FTP トラフィックに対してイネーブルである必要があります。これは、FTP が、データ転送用に動的に割り当てられたセカンダリ チャネルを使用するためです。セキュリティ アプライアンスは、セカンダリ チャネルに割り当てられるポートを決定し、データ転送の実行を許可するピンホールを空けます。CSC SSM が FTP データをスキャンするように設定されている場合、セキュリティ アプライアンスはデータ トラフィックを CSC SSM に転送します。

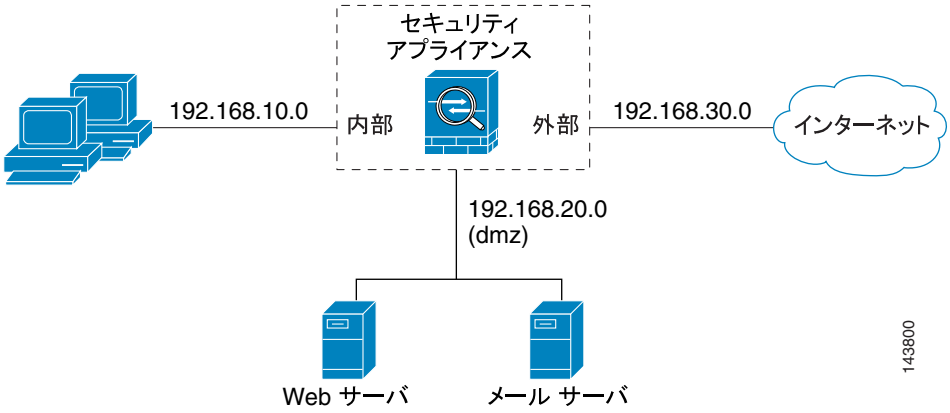
FTP 検査は、グローバル、または **csc** コマンドが適用される同じインターフェイスに適用できます。デフォルトでは、FTP 検査はグローバルにイネーブルにされています。デフォルトの検査コンフィギュレーションを変更していない場合は、CSC SSM により FTP スキャンをイネーブルにする際に、これ以上 FTP 検査コンフィギュレーションが必要になることはありません。

FTP 検査またはデフォルトの検査コンフィギュレーションの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

図 9-1 では、内部ネットワーク上のクライアントから HTTP、FTP、および POP3 接続で外部のネットワークに要求されたトラフィック、および外部のホストから dmz ネットワーク上のメール サーバに着信する SMTP 接続を CSC SSM に転送するように、セキュリティ アプライアンスを設定する必要があります。内部のネットワークから dmz ネットワーク上の Web サーバへの HTTP 要求は、スキャンしないでください。

図 9-1　CSC SSM スキャニングの一般的なネットワーク コンフィギュレーション



次のコンフィギュレーションは、2 つのサービス ポリシーを作成します。最初のポリシー csc_out_policy は、内部のインターフェイスに適用され、csc_out アクセス リストを使用して、FTP および POP3 に対するすべての発信要求が必ずスキャンされるようにします。csc_out アクセス リストは内部から外部インターフェイス上のネットワークへの HTTP 接続も必ずスキャンされるようにしますが、内部から dmz ネットワーク上のサーバへの HTTP 接続を除外する拒否 ACE を含んでいます。

2 番目のポリシーである csc_in_policy は、外部のインターフェイスに適用され、csc_in アクセス リストを使用して、外部インターフェイス上で dmz ネットワーク宛に送信される SMTP および HTTP に対する要求が CSC SSM によって必ずスキャンされるようにします。HTTP 要求をスキャンすることで、HTTP ファイルのアップロードから Web サーバを保護できます。

```
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
hostname(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
hostname(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

hostname(config)# class-map csc_outbound_class
hostname(config-cmap)# match access-list csc_out

hostname(config)# policy-map csc_out_policy
hostname(config-pmap)# class csc_outbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_out_policy interface inside

hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
hostname(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

hostname(config)# class-map csc_inbound_class
hostname(config-cmap)# match access-list csc_in

hostname(config)# policy-map csc_in_policy
hostname(config-pmap)# class csc_inbound_class
hostname(config-pmap-c)# csc fail-close

hostname(config)# service-policy csc_in_policy interface outside
```

（注） FTP により転送されたファイルを CSC SSM がスキャンするには、FTP 検査がイネーブルである必要があります。FTP 検査は、デフォルトでイネーブルです。

関連コマンド

コマンド	説明
class（ポリシー マップ）	トラフィックの分類に使用するクラス マップを指定します。
class-map	ポリシー マップで使用するトラフィック分類マップを作成します。
match port	宛先ポートを使用してトラフィックを照合します。
policy-map	トラフィック クラスを 1 つまたは複数のアクションと関連付けることによって、ポリシー マップを作成します。
service-policy	ポリシー マップを 1 つまたは複数のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。

csd enable

管理およびリモート ユーザ アクセスに対して Cisco Secure Desktop をイネーブルにするには、webvpn コンフィギュレーション モードで **csd enable** コマンドを使用します。CSD をディセーブルにするには、このコマンドの **no** 形式を使用します。

csd enable

no csd enable

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン　**csd enable** コマンドは、次の処理を実行します。

1. 以前の **csd image** *path* コマンドにより実行されたチェックを補足する有効性チェックを提供します。
2. disk0 上に sdesktop フォルダが存在しない場合は作成します。
3. sdesktop フォルダに data.xml（CSD コンフィギュレーション）ファイルが存在しない場合は挿入します。
4. フラッシュ デバイスから data.xml を実行コンフィギュレーションにロードします。
5. CSD をイネーブルにします。

show webvpn csd コマンドを入力して、CSD がイネーブルかどうかを判断します。

csd enable コマンドを入力する前に、実行コンフィギュレーション内に **csd image** *path* コマンドが存在する必要があります。

no csd enable コマンドは、実行コンフィギュレーションで CSD をディセーブルにします。CSD がディセーブルの場合、ユーザは Cisco Secure Desktop Manager にアクセスできず、リモート ユーザは CSD を使用できません。

data.xml ファイルを転送または交換する場合、CSD をディセーブルにした後、イネーブルにして実行コンフィギュレーションにこのファイルをロードします。

例

次のコマンドの例では、CSD イメージのステータスの表示方法とイネーブルにする方法を示します。

```
hostname(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
hostname(config-webvpn)# csd enable
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn csd	CSD がイネーブルである場合、そのバージョンを識別します。ディセーブルの場合、CLI は「Secure Desktop is not enabled.」と表示します。
csd image	コマンドで指定された CSD イメージを、パスで指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。

csd image

Cisco Secure Desktop 配布パッケージを検証して、実行コンフィギュレーションに追加するには、CSD を効率的にインストールし、webvpn コンフィギュレーション モードで **csd image** コマンドを使用します。CSD ディストリビューション パッケージを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

csd image *path*

no csd image [*path*]

シンタックスの説明

path	CSD パッケージのパスおよびファイル名を 255 文字以内で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを入力する前に、**show webvpn csd** コマンドを入力して、CSD イメージがイネーブルであるかどうかを判断します。CLI は、現在インストールされている CSD イメージがイネーブルである場合、そのバージョンを示します。

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop から新しい CSD イメージをコンピュータにダウンロードし、フラッシュ ドライブに転送してから、**csd image** コマンドを使用して、イメージをインストールするか既存のイメージをアップグレードします。必ず、使用しているセキュリティ アプライアンスに合ったファイルをダウンロードしてください。ファイルの形式は、**securedesktop_asa_**<*n*>**_**<*n*>***.pkg** です。

no csd image を入力すると、Cisco Secure Desktop Manager への管理アクセスと、CSD へのリモート ユーザ アクセスの両方を削除します。このコマンドを入力すると、セキュリティ アプライアンスは、CSD ソフトウェアとフラッシュ ドライブ上の CSD コンフィギュレーションに対してどのような変更も行いません。

（注） **write memory** コマンドを入力すると、次にセキュリティ アプライアンスをリブートしたときに CSD が使用できることを保証するために、実行コンフィギュレーションを保存します。

例

次のコマンド例は、現在の CSD 配布パッケージの表示方法、フラッシュ ファイル システムの内容の表示方法、および新しい CSD バージョンにアップグレードする方法について示しています。

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
hostname# config t
hostname(config)# webvpn
hostname(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
hostname(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
hostname(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn csd	CSD がイネーブルである場合、そのバージョンを識別します。ディセーブルの場合、CLI は「Secure Desktop is not enabled.」と表示します。
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。

customization

トンネル グループ、グループ、またはユーザ用のカスタマイゼーションを指定するには、次のモードで **customization** コマンドを使用します。

トンネル グループ webvpn コンフィギュレーション モード

customization *name*

no customization *name*

グループ ポリシー webvpn コンフィギュレーション モードとユーザ名 webvpn コンフィギュレーション モード

customization {**none** | **value** *name*}

no customization {**none** | **value** *name*}

シンタックスの説明

name	適用する WebVPN カスタマイゼーションの名前を指定します。
none	グループまたはユーザのカスタマイゼーションをディセーブルにし、デフォルトの WebVPN ページを表示します。
value *name*	グループ ポリシーまたはユーザに適用するカスタマイゼーションの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—
グループ ポリシー WebVPN コンフィギュレーション	•	—	•	—	—
ユーザ名の WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

トンネル グループ webvpn モードで **customization** コマンドを入力する前に、webvpn コンフィギュレーション モードで **customization** コマンドを使用したカスタマイゼーションの名前を付け、設定する必要があります。

モード別のコマンドのオプション

customization コマンドで使用できるキーワードは、モードによって異なります。グループ ポリシー webvpn コンフィギュレーション モードとユーザ名 webvpn コンフィギュレーション モードでは、追加の ***none*** キーワードと ***value*** キーワードがあります。これらのモードでの完全なシンタックスは、次のとおりです。

[**no**] **customization** {**none** | **value** *name*}

none は、グループまたはユーザのカスタマイゼーションをディセーブルにし、継承できないようにします。たとえば、ユーザ名 webvpn コンフィギュレーション モードで **customization none** コマンドを入力すると、セキュリティ アプライアンスは、グループ ポリシーやトンネル グループに含まれる値を検索しません。

name は、グループまたはユーザに適用するカスタマイゼーションの名前です。

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

例

次の例では、パスワード プロンプトを定義する「123」という名前の WebVPN カスタマイゼーションを最初に確立するコマンド シーケンスを示します。次に、「test」という WebVPN トンネル グループを定義し、**customization** コマンドを使用して、「123」という WebVPN カスタマイゼーションを使用することを指定しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization 123
hostname(config-webvpn-custom)# password-prompt Enter password
hostname(config-webvpn)# exit
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# customization 123
hostname(config-tunnel-webvpn)#
```

次の例では、「cisco」というカスタマイゼーションを「cisco_sales」というグループ ポリシーに適用する方法を示します。グループ ポリシー webvpn コンフィギュレーション モードでは、**customization** コマンドに **value** オプションを追加する必要があることに注意してください。

```
hostname(config)# group-policy cisco_sales attributes
hostname(config-group-policy)#  webvpn
hostname(config-group-webvpn)# customization value cisco
```

関連コマンド

コマンド	説明
clear configure tunnel-group	すべてのトンネル グループのコンフィギュレーションを削除します。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

CHAPTER 10

ddns コマンド～ debug xdmcp コマンド

ddns（DDNS アップデート方式）

DDNS アップデート方式のタイプを指定するには、DDNS アップデート方式モードで **ddns** コマンドを使用します。アップデート方式タイプを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ddns [**both**]

no ddns [**both**]

シンタックスの説明

both	（オプション）DNS A および PTR リソース レコード（RR）へのアップデートを指定します。

デフォルト

A RR のみをアップデートします。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DDNS アップデート方式	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ダイナミック DNS（DDNS）は、DNS で管理されている名前からアドレスへのマッピング、およびアドレスから名前へのマッピングをアップデートするものです。DDNS アップデートを実行するための 2 つの方式（RFC 2136 で定義されている IETF 標準、および一般的な HTTP 方式）のうち、セキュリティ アプライアンスのこのリリースでは、IETF 方式をサポートしています。

名前とアドレスのマッピングは、次の 2 タイプのリソース レコード（RR）に保持されます。

- A リソース レコードは、ドメイン名から IP アドレスへのマッピングを保持します。
- PTR リソース レコードは、IP アドレスからドメイン名へのマッピングを保持します。

DDNS アップデートを使用すると、A タイプの RR に保持される情報と、PTR タイプの RR に保持される情報との一貫性を維持できます。

DDNS アップデート方式のコンフィギュレーション モードで発行されると、**ddns** コマンドは A RR に対してのみアップデートするのか、A RR および PTR RR に対してアップデートするのかを定義します。

例

次の例は、ddns-2 という DDNS アップデート方式で A RR と PTR RR に対するアップデートを設定します。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# ddns both
```

関連コマンド

コマンド	説明
ddns update（インターフェイス コンフィギュレーション モード）	ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update（インターフェイス コンフィギュレーション）

ダイナミック DNS（DDNS）アップデート方式をセキュリティ アプライアンス インターフェイスまたはアップデート ホスト名と関連付けるには、インターフェイス コンフィギュレーション モードで **ddns update** コマンドを使用します。実行コンフィギュレーションから DDNS アップデート方式とインターフェイスまたはホスト名間の関連付けを削除するには、このコマンドの **no** 形式を使用します。

ddns update [***method-name*** **| hostname** *hostname*]

no ddns update [***method-name*** **| hostname** *hostname*]

シンタックスの説明

hostname	コマンド文字列において次に続く用語がホスト名であることを指定します。
hostname	アップデートに使用するホスト名を指定します。
method-name	設定するインターフェイスに関連付ける方式名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DDNS アップデート方式を定義したら、それをセキュリティ アプライアンス インターフェイスに関連付けて DDNS アップデートを有効にする必要があります。

ホスト名は、Fully Qualified Domain Name（FQDN; ドメイン名完全修飾子）またはホスト名のみを指定します。ホスト名のみの場合、セキュリティ アプライアンス ホスト名にドメイン名を付記してドメイン名完全修飾子を作成します。

例

次の例は、インターフェイス GigabitEthernet0/2 を ddns-2 という DDNS アップデート方式とホスト名 hostname1.example.com に関連付けます。

```
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# ddns update ddns-2
hostname(config-if)# ddns update hostname hostname1.example.com
```

関連コマンド

コマンド	説明
ddns（DDNS アップデート方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

ddns update method（グローバル コンフィギュレーション モード）

DNS リソース レコード（RR）をダイナミックにアップデートする方式を作成するには、グローバル コンフィギュレーション モードで **ddns update method** コマンドを使用します。実行コンフィギュレーションからダイナミック DNS（DDNS）アップデート方式を削除するには、このコマンドの **no** 形式を使用します。

ddns update method *name*

no ddns update method *name*

シンタックスの説明

name	DNS レコードをダイナミックにアップデートする方式名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ダイナミック DNS（DDNS）は、DNS で管理されている名前からアドレスへのマッピング、およびアドレスから名前へのマッピングをアップデートするものです。**ddns update method** コマンドにより設定されたアップデート方式は、いずれのダイナミック DNS アップデートをどれぐらいの頻度で実行するかを指定します。DDNS アップデートを実行するための 2 つの方式（RFC 2136 で定義されている IETF 標準、および一般的な HTTP 方式）のうち、セキュリティ アプライアンスのこのリリースでは、IETF 方式をサポートしています。

名前とアドレスのマッピングは、次の 2 タイプのリソース レコード（RR）に保持されます。

- A リソース レコードは、ドメイン名から IP アドレスへのマッピングを保持します。
- PTR リソース レコードは、IP アドレスからドメイン名へのマッピングを保持します。

DDNS アップデートを使用すると、A タイプの RR に保持される情報と、PTR タイプの RR に保持される情報との一貫性を維持できます。

（注） **ddns update method** を有効にするには、ドメイン ルックアップをインターフェイス上でイネーブルにしたまま **dns** コマンドを使用して到達可能なデフォルト DNS サーバを設定する必要があります。

例

次の例は、ddns-2 という DDNS アップデート方式を設定します。

```
hostname(config)# ddns update method ddns-2
```

関連コマンド

コマンド	説明
ddns（DDNS アップデート方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

debug aaa

AAA に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug aaa** コマンドを使用します。AAA メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug aaa [***accounting*** | ***authentication*** | ***authorization*** | ***internal*** | ***vpn*** [*level*]]

no debug aaa

シンタックスの説明

accounting	（オプション）アカウンティングに関するデバッグ メッセージだけを表示します。
authentication	（オプション）認証に関するデバッグ メッセージだけを表示します。
authorization	（オプション）認可に関するデバッグ メッセージだけを表示します。
internal	（オプション）ローカル データベースだけでサポートされる AAA 機能に関するデバッグ メッセージを表示します。
level	（オプション）デバッグ レベルを指定します。**vpn** キーワードと共に使用する場合だけ有効です。
vpn	（オプション）VPN 関連の AAA 機能に関するデバッグ メッセージだけを表示します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいキーワードを含めるように修正されました。

使用上のガイドライン

debug aaa コマンドは、AAA アクティビティに関する詳細な情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、ローカル データベースでサポートされる AAA 機能のデバッグをイネーブルにします。

```
hostname(config)# debug aaa internal
debug aaa internal enabled at level 1
hostname(config)# uap allocated. remote address: 10.42.15.172, Session_id: 2147483841
uap freed for user . remote address: 10.42.15.172, session id: 2147483841
```

関連コマンド

コマンド	説明
show running-config aaa	AAA に関連する実行コンフィギュレーションを表示します。

debug appfw

アプリケーション検査に関する詳細情報を表示するには、特権 EXEC モードで **debug appfw** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug appfw [**chunk** | **event** | **eventverb** | **regex**]

no debug appfw [**chunk** | **event** | **eventverb** | **regex**]

シンタックスの説明

chunk	（オプション）チャンク分割転送形式のパケットの処理に関するランタイム情報を表示します。
event	（オプション）パケット検査イベントのデバッグ情報を表示します。
eventverb	（オプション）イベントの応答でセキュリティ アプライアンスが取るアクションを表示します。
regex	（オプション）定義済みシグニチャに一致するパターンの情報を表示します。

デフォルト

デフォルトでは、すべてのオプションがイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug appfw コマンドは、HTTP アプリケーション検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、アプリケーション検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug appfw
```

関連コマンド

コマンド	説明
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。

debug arp

ARP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug arp** コマンドを使用します。ARP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug arp

no debug arp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、ARP に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug arp
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
show arp statistics	ARP 統計情報を表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug arp-inspection

ARP 検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug arp-inspection** コマンドを使用します。ARP 検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug arp-inspection

no debug arp-inspection

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、ARP 検査に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug arp-inspection
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show debug	イネーブルなデバッガをすべて表示します。

debug asdm history

ASDM のデバッグ情報を表示するには、特権 EXEC モードで **debug asdm history** コマンドを使用します。

debug asdm history *level*

シンタックスの説明

level	（オプション）デバッグ レベルを指定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**debug pdm history** コマンドから **debug asdm history** コマンドに変更されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、ASDM に関するレベル 1 のデバッグをイネーブルにします。

```
hostname# debug asdm history
debug asdm history enabled at level 1

hostname#
```

関連コマンド

コマンド	説明
show asdm history	ASDM 履歴バッファの内容を表示します。

debug context

セキュリティ コンテキストを追加または削除する際にデバッグ メッセージを表示するには、特権 EXEC モードで **debug context** コマンドを使用します。コンテキストに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug context [*level*]

no debug context [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、コンテキスト管理に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug context
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
show context	コンテキスト情報を表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug cplane

SSM に内部的に接続するコントロール プレーンに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug cplane** コマンドを使用します。制御プレーンに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug cplane [*level*]

no debug cplane [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、コントロール プレーンに関するデバッグ メッセージをイネーブルにします。

```
hostname# debug cplane
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

debug crypto ca

CA で使用する PKI アクティビティに関するデバッグ メッセージを表示するには、特権 EXEC モードで **ebug crypto ca** コマンドを使用します。PKI に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto ca [**messages** | **transactions**] [*level*]

no debug crypto ca [**messages** | **transactions**] [*level*]

シンタックスの説明

messages	（オプション）PKI の入力および出力メッセージに関するデバッグ メッセージだけを表示します。
transactions	（オプション）PKI トランザクションに関するデバッグ メッセージだけを表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。レベル 1（デフォルト）では、エラーが発生した場合にだけメッセージが表示されます。レベル 2 では、警告が表示されます。レベル 3 では、情報メッセージが表示されます。レベル 4 以上では、トラブルシューティングのための追加情報が表示されます。

デフォルト

デフォルトでは、このコマンドはすべてのデバッグ メッセージを表示します。デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、PKI に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug crypto ca
```

関連コマンド

コマンド	説明
debug crypto engine	暗号化エンジンに関するデバッグ メッセージを表示します。
debug crypto ipsec	IPSec に関するデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP に関するデバッグ メッセージを表示します。

debug crypto engine

暗号化エンジンに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto engine** コマンドを使用します。暗号化エンジンに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto engine [*level*]

no debug crypto engine [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、暗号化エンジンに関するデバッグ メッセージをイネーブルにします。

```
hostname# debug crypto engine
```

関連コマンド

コマンド	説明
debug crypto ca	CA に関するデバッグ メッセージを表示します。
debug crypto ipsec	IPSec に関するデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP に関するデバッグ メッセージを表示します。

debug crypto ipsec

IPSec に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto ipsec** コマンドを使用します。IPSec に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto ipsec [*level*]

no debug crypto ipsec [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、IPSec に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug crypto ipsec
```

関連コマンド

コマンド	説明
debug crypto ca	CA に関するデバッグ メッセージを表示します。
debug crypto engine	暗号化エンジンに関するデバッグ メッセージを表示します。
debug crypto isakmp	ISAKMP に関するデバッグ メッセージを表示します。

debug crypto isakmp

ISAKMP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug crypto isakmp** コマンドを使用します。ISAKMP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug crypto isakmp [**timers**] [*level*]

no debug crypto isakmp [**timers**] [*level*]

シンタックスの説明

timers	（オプション）ISAKMP タイマーの期限切れに関するデバッグ メッセージを表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。レベル 1（デフォルト）では、エラーが発生した場合にだけメッセージが表示されます。レベル 2 ～ 7 では、追加情報が表示されます。レベル 254 では、復号化された ISAKMP パケットが、人が読める形式で表示されます。レベル 255 では、復号化された ISAKMP パケットの 16 進形式のダンプが表示されます。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、ISAKMP に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug crypto isakmp
```

関連コマンド

コマンド	説明
debug crypto ca	CA に関するデバッグ メッセージを表示します。
debug crypto engine	暗号化エンジンに関するデバッグ メッセージを表示します。
debug crypto ipsec	IPSec に関するデバッグ メッセージを表示します。

debug ctiqbe

CTIQBE アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug ctiqbe** コマンドを使用します。CTIQBE アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ctiqbe [*level*]

no debug ctiqbe [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug ctiqbe** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、CTIQBE アプリケーション検査に関するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug ctiqbe
```

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
show ctiqbe	セキュリティ アプライアンスを介して確立された CTIQBE セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

debug ddns

DNS に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug dns** コマンドを使用します。デバッグ メッセージをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ddns

no debug ddns

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作または値が設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug http コマンドは、DDNS に関する詳細情報を表示します。**undebug ddns** は **no debug ddns** コマンドと同様、DDNS デバッグ情報をオフにします。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例は、DDNS デバッグ メッセージをイネーブルにする例を示します。

```
hostname# debug ddns
debug ddns enabled at level 1
```

関連コマンド

コマンド	説明
ddns（**DDNS** アップデート方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
show running-config ddns	実行コンフィギュレーションに含まれている、設定済みのすべての DDNS 方式について、タイプおよび間隔を表示します。

debug dhcpc

DHCP クライアントのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpc** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dhcpc {***detail*** | ***packet*** | ***error***} [*level*]

no debug dhcpc {***detail*** | ***packet*** | ***error***} [*level*]

シンタックスの説明

detail	DHCP クライアントに関連する詳細なイベント情報を表示します。
error	DHCP クライアントに関連するエラー メッセージを表示します。
level	（オプション）デバッグ レベルを指定します。有効な値は 1 ～ 255 です。
packet	DHCP クライアントに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

DHCP クライアントのデバッグ情報を表示します。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、DHCP クライアントに関するデバッグをイネーブルにする方法を示しています。

```
hostname# debug dhcpc detail 5
debug dhcpc detail enabled at level 5
```

関連コマンド

コマンド	説明
show ip address dhcp	インターフェイスの DHCP リースに関する詳細な情報を表示します。
show running-config interface	指定されたインターフェイスの実行コンフィギュレーションを表示します。

debug dhcpd

DHCP サーバのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpd** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dhcpd {***event*** | ***packet***} [*level*]

no debug dhcpd {***event*** | ***packet***} [*level*]

シンタックスの説明

event	DHCP サーバに関連するイベント情報を表示します。
level	（オプション）デバッグ レベルを指定します。有効な値は 1 ～ 255 です。
packet	DHCP サーバに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug dhcpd event コマンドは、DHCP サーバに関するイベント情報を表示します。**debug dhcpd packet** コマンドは、DHCP サーバに関するパケット情報を表示します。

debug dhcpd コマンドの **no** 形式を使用して、デバッグをディセーブルにします。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、DHCP イベント デバッグをイネーブルにする例を示します。

```
hostname# debug dhcpd event
debug dhcpd event enabled at level 1
```

関連コマンド

コマンド	説明
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

debug dhcpd ddns

DHCP DDNS のデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcpd** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dhcpd ddns [*level*]

no debug dhcpd ddns [*level*]

シンタックスの説明

level	（オプション）デバッグ レベルを指定します。有効な値は 1 ～ 255 です。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug dhcpd ddns コマンドは DHCP および DDNS に関する詳細を表示します。**undebug dhcpd ddns** コマンドは、**no debug dhcpd ddns** コマンドと同様、DHCP および DDNS デバッグ情報をオフにします。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、イネーブルである DHCP DDNS デバッグを示します。

```
hostname# debug dhcpd ddns
debug dhcpd ddns enabled at level 1
```

関連コマンド

コマンド	説明
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。
show running-config ddns	実行コンフィギュレーションの DDNS アップデート方式を表示します。

debug dhcprelay

DHCP リレー サーバのデバッグをイネーブルにするには、特権 EXEC モードで **debug dhcprelay** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug dhcprelay {***event*** | ***packet*** | ***error***} [*level*]

no debug dhcprelay {***event*** | ***packet*** | ***error***} [*level*]

シンタックスの説明

error	DHCP リレー エージェントに関連するエラー メッセージを表示します。
event	DHCP リレー エージェントに関連するイベント情報を表示します。
level	（オプション）デバッグ レベルを指定します。有効な値は 1 ～ 255 です。
packet	DHCP リレー エージェントに関連するパケット情報を表示します。

デフォルト

デフォルトのデバッグ レベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例は、DHCP リレー エージェントのエラー メッセージのデバッグをイネーブルにする方法を示しています。

```
hostname# debug dhcprelay error
debug dhcprelay error enabled at level 1
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェント統計情報カウンタを消去します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

debug disk

ファイル システムのデバッグ情報を表示するには、特権 EXEC モードで **debug disk** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug disk {***file*** | ***file-verbose*** | ***filesystem***} [*level*]

no debug disk {***file*** | ***file-verbose*** | ***filesystem***}

シンタックスの説明

file	ファイル レベルでのディスクのデバッグ メッセージをイネーブルにします。
file-verbose	ファイル レベルでの詳細なディスクのデバッグ メッセージをイネーブルにします。
filesystem	ファイル システムのデバッグ メッセージをイネーブルにします。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、ファイル レベルでのディスクのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、ファイル レベルでのディスク デバッグ メッセージがイネーブルになっていることを示します。**dir** コマンドを実行すると、いくつかのデバッグ メッセージが作成されます。

```
hostname# debug disk file
debug disk file enabled at level 1
hostname# show debug
debug vpn-sessiondb  enabled at level 1
hostname# dir
IFS: Opening: file flash:/, flags 1, mode 0
IFS: Opened: file flash:/ as fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3

Directory of flash:/
IFS: Close: fd 3
IFS: Opening: file flash:/, flags 1, mode 0

4      -rw-  5124096     14:42:27 Apr 04 2005  cdisk.binIFS: Opened: file flash:/ as
fd 3

9      -rw-  5919340     14:53:39 Apr 04 2005  ASDMIFS: Getdent: fd 3

11     drw-  0           15:18:56 Apr 21 2005  syslog
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Getdent: fd 3
IFS: Close: fd 3

16128000 bytes total (5047296 bytes free)
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug dns

DNS に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug dns** コマンドを使用します。DNS に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug dns [***resolver*** | ***all***] [*level*]

no debug dns [***resolver*** | ***all***] [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。
resolver	（オプション）DNS リゾルバ メッセージだけを表示します。
all	（デフォルト）DNS キャッシュに関するメッセージを含む、すべてのメッセージを表示します。

デフォルト

デフォルトのレベルは 1 です。キーワードを指定しない場合、セキュリティ アプライアンスはすべてのメッセージを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、DNS のデバッグ メッセージをイネーブルにします。

```
hostname# debug dns
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect dns	DNS アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

debug eap

ネットワーク アドミッション コントロール メッセージをデバッグするため、EAP イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug eap** コマンドを使用します。EAP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eap {***all*** | ***errors*** | ***events*** | ***packets*** | ***sm***}

no debug eap [***all*** | ***errors*** | ***events*** | ***packets*** | ***sm***]

シンタックスの説明

all	すべての EAP 情報に関するデバッグ メッセージのロギングをイネーブルにします。
errors	EAP パケット エラーのロギングをイネーブルにします。
events	EAP セッション イベントのロギングをイネーブルにします。
packets	EAP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
sm	EAP ステート マシーンの情報に関するデバッグ メッセージのロギングをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは EAP セッションの状態の変化とステータス クエリー イベントを記録し、16 進形式で EAP の完全なレコードとパケットの内容を生成します。

デバッグ出力に高優先順位を割り当てることで、システムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、すべての EAP セッション イベントのロギングをイネーブルにします。

```
hostname# debug eap events
hostname#
```

次の例では、すべての EAP デバッグ メッセージのロギングをイネーブルにします。

```
hostname# debug eap all
hostname#
```

次の例では、すべての EAP デバッグ メッセージのロギングをディセーブルにします。

```
hostname# no debug eap
hostname#
```

関連コマンド

コマンド	説明
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou initialize	1 つまたはそれ以上の NAC セッションに割り当てられているリソースを消去し、新しい無条件のポスチャ確認をセッションごとに開始します。
eou revalidate	1 つまたはそれ以上の NAC セッションのポスチャ再確認をただちに強制します。
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug entity

管理情報ベース（MIB）のデバッグ情報を表示するには、特権 EXEC モードで **debug entity** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug entity [*level*]

no debug entity

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、MIB デバッグ メッセージをイネーブルにします。**show debug** コマンドは、MIB デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug entity
debug entity  enabled at level 1
hostname# show debug
debug entity  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug eou

ネットワーク アドミッション コントロール メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug eou** コマンドを使用します。EAPoUDP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug eou {***all*** | ***eap*** | ***errors*** | ***events*** | ***packets*** | ***sm***}

no debug eou [***all*** | ***eap*** | ***errors*** | ***events*** | ***packets*** | ***sm***]

シンタックスの説明

all	すべての EAPoUDP 情報に関するデバッグ メッセージのロギングをイネーブルにします。
eap	EAPoUDP パケットに関するデバッグ メッセージのロギングをイネーブルにします。
errors	EAPoUDP パケット エラーのロギングをイネーブルにします。
events	EAPoUDP セッション イベントのロギングをイネーブルにします。
packets	EAPoUDP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
sm	EAPoUDP ステート マシン情報に関するデバッグ メッセージのロギングをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは EAPoUDP セッションの状態の変化とタイマー イベントを記録し、16 進形式で EAPoUDP ヘッダーの完全なレコードとパケットの内容を生成します。

デバッグ出力に高優先順位を割り当てることで、システムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、すべての EAPoUDP セッション イベントのロギングをイネーブルにします。

```
hostname# debug eou events
hostname#
```

次の例では、すべての EAPoUDP デバッグ メッセージのロギングをイネーブルにします。

```
hostname# debug eou all
hostname#
```

次の例では、すべての EAPoUDP デバッグ メッセージのロギングをディセーブルにします。

```
hostname# no debug eou
hostname#
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou initialize	1 つまたはそれ以上の NAC セッションに割り当てられているリソースを消去し、新しい無条件のポスチャ確認をセッションごとに開始します。
eou revalidate	1 つまたはそれ以上の NAC セッションのポスチャ再確認をただちに強制します。
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug esmtp

SMTP/ESMTP アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug smtp** コマンドを使用します。SMTP/ESMTP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug esmtp[*level*]

no debug esmtp [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug esmtp** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、SMTP/ESMTP アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug esmtp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect esmtp	ESMTP アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。
show conn	SMTP など、さまざまな接続タイプの接続状態を表示します。

debug fixup

アプリケーション検査に関する詳細情報を表示するには、特権 EXEC モードで **debug fixup** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug fixup

no debug fixup

デフォルト

デフォルトでは、すべてのオプションがイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug fixup コマンドは、アプリケーション検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、アプリケーション検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug fixup
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect *protocol*	特定のプロトコルに関するアプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

debug fover

フェールオーバーのデバッグ情報を表示するには、特権 EXEC モードで **debug fover** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug fover {***cable*** | ***fail*** | ***fmsg*** | ***ifc*** | ***open*** | ***rx*** | ***rxdmp*** | ***rxip*** | ***switch*** | ***sync*** | ***tx*** | ***txdmp*** | ***txip*** | ***verify***}

no debug fover {***cable*** | ***fail*** | ***fmsg*** | ***ifc*** | ***open*** | ***rx*** | ***rxdmp*** | ***rxip*** | ***switch*** | ***sync*** | ***tx*** | ***txdmp*** | ***txip*** | ***verify***}

シンタックスの説明

cable	フェールオーバーの LAN ステータスまたはシリアル ケーブル ステータス
fail	フェールオーバー内部例外
fmsg	フェールオーバー メッセージ
ifc	ネットワーク インターフェイス ステータス トレース
open	フェールオーバー デバイス オープン
rx	フェールオーバー メッセージ受信
rxdmp	フェールオーバー受信メッセージ ダンプ（シリアル コンソールのみ）
rxip	IP ネットワーク フェールオーバー パケット受信
switch	フェールオーバー スイッチング ステータス
sync	フェールオーバー コンフィギュレーション、またはコマンド複製
tx	フェールオーバー メッセージ送信
txdmp	フェールオーバー送信メッセージ ダンプ（シリアル コンソールのみ）
txip	IP ネットワーク フェールオーバー パケット送信
verify	フェールオーバー メッセージの確認

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。このコマンドには、追加のデバッグ キーワードが含まれています。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例は、フェールオーバー コマンド複製のデバッグ情報を表示する方法を示しています。

```
hostname# debug fover sync
fover event trace on
```

関連コマンド

コマンド	説明
show failover	フェールオーバー コンフィギュレーションに関する情報および動作統計情報を表示します。

debug fsm

FSM のデバッグ情報を表示するには、特権 EXEC モードで **debug fsm** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug fsm [*level*]

no debug fsm

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、FSM デバッグ メッセージをイネーブルにします。**show debug** コマンドは、FSM デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug fsm
debug fsm  enabled at level 1
hostname# show debug
debug fsm  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ftp client

FTP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug ftp client** コマンドを使用します。FTP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ftp client [*level*]

no debug ftp client [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug ftp client** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、FTP のデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug ftp client
```

関連コマンド

コマンド	説明
copy	イメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。
ftp mode passive	FTP セッションのモードを設定します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

debug generic

その他のデバッグ情報を表示するには、特権 EXEC モードで **debug generic** コマンドを使用します。その他のデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug generic [*level*]

no debug generic

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、その他のデバッグ メッセージをイネーブルにします。**show debug** コマンドは、その他のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug generic
debug generic  enabled at level 1
hostname# show debug
debug generic  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug gtp

GTP 検査に関する詳細情報を表示するには、特権 EXEC モードで **debug gtp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug gtp [**error** | **event** | **ha** | **parser**]

no debug gtp [**error** | **event** | **ha** | **parser**]

シンタックスの説明

error	GTP メッセージの処理中に発生したエラーのデバッグ情報を表示します。
event	GTP イベントのデバッグ情報を表示します。
ha option	GTP HA イベントに関する情報をデバッグします。
parser	GTP メッセージの解析のデバッグ情報を表示します。

デフォルト

デフォルトでは、すべてのオプションがイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug gtp コマンドは、GTP 検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

（注） GTP 検査には、特別なライセンスが必要です。

例

次の例では、GTP 検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug gtp
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査用に GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。
show running-config gtp-map	設定されている GTP マップを表示します。

debug h323

H.323 に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug h323** コマンドを使用します。H.323 に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug h323 {h225 | h245 | ras} [asn | event]

no debug h323 {h225 | h245 | ras} [asn | event]

シンタックスの説明

h225	H.225 シグナリングを指定します。
h245	H.245 シグナリングを指定します。
ras	登録、許可、およびステータスのプロトコルを指定します。
asn	（オプション）デコードされたプロトコル データ ユニット（PDU）の出力を表示します。
event	（オプション）シグナリングのイベントを表示するか、両方のトレースをオンにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug h323** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、H.225 シグナリングのデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug h323 h225
```

関連コマンド

コマンド	説明
inspect h323	H.323 アプリケーション検査をイネーブルにします。
show h225	セキュリティ アプライアンスを越えて確立された H.225 セッションの情報を表示します。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

debug http

HTTP トラフィックに関する詳細情報を表示するには、特権 EXEC モードで **debug http** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug http [*level*]

no debug http [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug http コマンドは、HTTP トラフィックに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、HTTP トラフィックに関する詳細情報の表示をイネーブルにします。

```
hostname# debug http
```

関連コマンド

コマンド	説明
http	セキュリティ アプライアンスの内部の HTTP サーバにアクセス可能なホストを指定します。
http-proxy	HTTP プロキシ サーバを設定します。
http redirect	HTTP トラフィックを HTTPS にリダイレクトします。
http server enable	セキュリティ アプライアンス HTTP サーバをイネーブルにします。

debug http-map

HTTP アプリケーション検査マップに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug http-map** コマンドを使用します。HTTP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug http-map

no debug http-map

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug http-map** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、HTTP アプリケーション検査のデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug http-map
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	HTTP アプリケーション検査に関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

debug icmp

ICMP 検査に関する詳細情報を表示するには、特権 EXEC モードで **debug icmp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug icmp trace [*level*]

no debug icmp trace [*level*]

シンタックスの説明

trace	ICMP トレース アクティビティのデバッグ情報を表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

すべてのオプションがイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug icmp コマンドは、ICMP 検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、ICMP 検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug icmp
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションを消去します。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
show conn	さまざまなプロトコルおよびセッション タイプについて、セキュリティ アプライアンスを介した接続状態を表示します。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

debug igmp

IGMP のデバッグ情報を表示するには、特権 EXEC モードで **debug igmp** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug igmp [***group*** *group_id* | ***interface*** *if_name*]

no debug igmp [***group*** *group_id* | ***interface*** *if_name*]

シンタックスの説明

group *group_id*	指定されたグループの IGMP デバッグ情報を表示します。
interface *if_name*	指定されたインターフェイスの IGMP デバッグ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug igmp** コマンドの出力例を示します。

```
hostname#debug igmp

IGMP debugging is on
IGMP: Received v2 Query on outside from 192.168.3.2
IGMP: Send v2 general Query on dmz
IGMP: Received v2 Query on dmz from 192.168.4.1
IGMP: Send v2 general Query on outside
IGMP: Received v2 Query on outside from 192.168.3.1
IGMP: Send v2 general Query on inside
IGMP: Received v2 Query on inside from 192.168.1.1
IGMP: Received v2 Report on inside from 192.168.1.6 for 224.1.1.1
IGMP: Updating EXCLUDE group timer for 224.1.1.1
```

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続されている受信者、および IGMP を通じてラーニングされた受信者を持つマルチキャスト グループを表示します。
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

debug ils

ILS に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug ils** コマンドを使用します。ILS に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ils [*level*]

no debug ils [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug ils** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、ILS アプリケーション検査のデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug ils
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect ils	ILS アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

debug imagemgr

Image Manager のデバッグ情報を表示するには、特権 EXEC モードで **debug imagemgr** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug imagemgr [*level*]

no debug imagemgr

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、Image Manager デバッグ メッセージをイネーブルにします。**show debug** コマンドは、Image Manager のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug imagemgr
debug imagemgr  enabled at level 1
hostname# show debug
debug imagemgr  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ipsec-over-tcp

IPSec-over-TCP のデバッグ情報を表示するには、特権 EXEC モードで **debug ipsec-over-tcp** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ipsec-over-tcp [*level*]

no debug ipsec-over-tcp

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、IPSec-over-TCP のデバッグ メッセージをイネーブルにします。**show debug** コマンドは、IPSec-over-TCP のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug ipsec-over-tcp
debug ipsec-over-tcp  enabled at level 1
hostname# show debug
debug ipsec-over-tcp  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ipv6

ipv6 のデバッグ メッセージを表示するには、特権 EXEC モードで **debug ipv6** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ipv6 {*icmp* | *interface* | *nd* | *packet* | *routing*}

no debug ipv6 {*icmp* | *interface* | *nd* | *packet* | *routing*}

シンタックスの説明

icmp	ICMPv6 近隣探索トランザクションを除外した、IPv6 ICMP トランザクションに関するデバッグ メッセージを表示します。
interface	IPv6 インターフェイスに関するデバッグ情報を表示します。
nd	ICMPv6 近隣探索トランザクションに関するデバッグ メッセージを表示します。
packet	IPv6 パケットに関するデバッグ メッセージを表示します。
routing	IPv6 のルーティング テーブル アップデートおよびルート キャッシュ アップデートに関するデバッグ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug ipv6 icmp** コマンドの出力例を示します。

```
hostname# debug ipv6 icmp
13:28:40:ICMPv6:Received ICMPv6 packet from 2000:0:0:3::2, type 136
13:28:45:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
13:28:50:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 136
13:28:55:ICMPv6:Received ICMPv6 packet from FE80::203:A0FF:FED6:1400, type 135
```

関連コマンド

コマンド	説明
ipv6 icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP メッセージのアクセス規則を設定します。
ipv6 address	IPv6 アドレスに対するインターフェイスを設定します。
ipv6 nd dad attempts	重複アドレスの検出中に実行される、近隣探索の試行回数を定義します。
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを定義します。

debug iua-proxy

個々のユーザ認証（IUA）プロキシのデバッグ情報を表示するには、特権 EXEC モードで **debug iua-proxy** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug iua-proxy [*level*]

no debug iua-proxy

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、IUA プロキシのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、IUA プロキシのデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug iua-proxy
debug iua-proxy  enabled at level 1
hostname# show debug
debug iua-proxy  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug kerberos

Kerberos 認証のデバッグ情報を表示するには、特権 EXEC モードで **debug kerberos** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug kerberos [*level*]

no debug kerberos

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、Kerberos のデバッグ メッセージをイネーブルにします。**show debug** コマンドは、Kerberos のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug kerberos
debug kerberos  enabled at level 1
hostname# show debug
debug kerberos  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug l2tp

L2TP のデバッグ情報を表示するには、特権 EXEC モードで **debug l2tp** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug l2tp {**data** | **error** | **event** | **packet**} *level*

no debug l2tp {**data** | **error** | **event** | **packet**} *level*

シンタックスの説明

data	データ パケット トレース情報を表示します。
error	エラー イベントを表示します。
event	L2TP 接続イベントを表示します。
packet	パケット トレース情報を表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では接続イベントの L2TP デバッグ メッセージをイネーブルにします。**show debug** コマンドは、L2TP のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug l2tp event 1
hostname# show debug
debug l2tp event enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ldap

LDAP のデバッグ情報を表示するには、特権 EXEC モードで **debug ldap** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ldap [*level*]

no debug ldap

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、LDAP のデバッグ メッセージをイネーブルにします。**show debug** コマンドは、LDAP のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug ldap
debug ldap  enabled at level 1
hostname# show debug
debug ldap  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug mac-address-table

MAC アドレス テーブルに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug mac-address-table** コマンドを使用します。MAC アドレス テーブルに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug mac-address-table [*level*]

no debug mac-address-table [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、MAC アドレス テーブルのデバッグ メッセージをイネーブルにします。

```
hostname# debug mac-address-table
```

関連コマンド

コマンド	説明
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show debug	イネーブルなデバッガをすべて表示します。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

debug menu

特定機能の詳細なデバッグ情報を表示するには、特権 EXEC モードで **debug menu** コマンドを使用します。

debug menu

注意　**debug menu** コマンドは、シスコのテクニカル サポート スタッフの指導の下で使用する必要があります。

シンタックスの説明

このコマンドは、シスコ テクニカル サポート スタッフの指導の下で使用する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

このコマンドは、シスコ テクニカル サポート スタッフの指導の下で使用する必要があります。

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug mfib

MFIB のデバッグ情報を表示するには、特権 EXEC モードで **debug mfib** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug mfib {***db*** | ***init*** | ***mrib*** | ***pak*** | ***ps*** | ***signal***} [*group*]

no debug mfib {***db*** | ***init*** | ***mrib*** | ***pak*** | ***ps*** | ***signal***} [*group*]

シンタックスの説明

db	（オプション）ルート データベース動作のデバッグ情報を表示します。
group	（オプション）マルチキャスト グループの IP アドレス。
init	（オプション）システムの初期化アクティビティを表示します。
mrib	（オプション）MRIB との通信のデバッグ情報を表示します。
pak	（オプション）パケット フォワーディング動作のデバッグ情報を表示します。
ps	（オプション）プロセス スイッチング動作のデバッグ情報を表示します。
signal	（オプション）ルーティング プロトコルへの MFIB シグナリングのデバッグ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、MFIB データベース動作のデバッグ情報を表示します。

```
hostname# debug mfib db
MFIB IPv4 db debugging enabled
```

関連コマンド

コマンド	説明
show mfib	MFIB の転送エントリおよびインターフェイスを表示します。

debug mgcp

MGCP アプリケーション検査に関する詳細情報を表示するには、特権 EXEC モードで **debug mgcp** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug mgcp {**messages** | **parser** | **sessions**}

no debug mgcp {**messages** | **parser** | **sessions**}

messages	MGCP メッセージのデバッグ情報を表示します。
parser	MGCP メッセージ解析のデバッグ情報を表示します。
sessions	MGCP セッションに関するデバッグ情報を表示します。

デフォルト

すべてのオプションがイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug mgcp コマンドは、mgcp 検査に関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例では、MGCP アプリケーション検査に関する詳細情報の表示をイネーブルにします。

```
hostname# debug mgcp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect mgcp	MGCP アプリケーション検査をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	セキュリティ アプライアンスを介して確立された MGCP セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。

debug module-boot

SSM ブーティング プロセスに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug module-boot** コマンドを使用します。SSM ブーティング プロセスに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug module-boot [*level*]

no debug module-boot [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、SSM ブーティング プロセスに関するデバッグ メッセージをイネーブルにします。

```
hostname# debug module-boot
```

関連コマンド

コマンド	説明
hw-module module recover	TFTP サーバからリカバリ イメージをロードすることにより、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

debug mrib

MRIB のデバッグ情報を表示するには、特権 EXEC モードで **debug mrib** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug mrib {***client*** | ***io*** | ***route*** [*group*] | ***table***}

no debug mrib {***client*** | ***io*** | ***route*** [*group*] | ***table***}

シンタックスの説明

client	MRIB クライアント管理アクティビティのデバッグをイネーブルにします。
io	MRIB I/O イベントのデバッグをイネーブルにします。
route	MRIB ルーティング エントリ アクティビティのデバッグをイネーブルにします。
group	指定グループでの MRIB ルーティング エントリ アクティビティのデバッグをイネーブルにします。
table	MRIB テーブル管理アクティビティのデバッグをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、MRIB I/O イベントのデバッグをイネーブルにする方法を示しています。

```
hostname# debug mrib io
IPv4 MRIB io debugging is on
```

関連コマンド

コマンド	説明
show mrib client	MRIB クライアント接続に関する情報を表示します。
show mrib route	MRIB テーブルのエントリを表示します。

debug nac

ネットワーク アドミッション コントロール イベントのロギングをイネーブルにするには、特権モードで、**debug nac** コマンドを使用します。NAC デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug nac {***all*** | ***auth*** | ***errors*** | ***events***}

no debug nac [***all*** | ***auth*** | ***errors*** | ***events***]

シンタックスの説明

all	すべての NAC 情報に関するデバッグ メッセージのロギングをイネーブルにします。
auth	NAC 認証要求と応答に関するデバッグ メッセージのロギングをイネーブルにします。
errors	NAC セッション エラーのロギングをイネーブルにします。
events	NAC セッション イベントのロギングをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、セキュリティ アプライアンスは次の NAC イベントのタイプ：初期化、例外リスト一致、ACS トランザクション、クライアントレス認証、デフォルト ACL の適用、および再確認をログに記録します。

デバッグ出力に高優先順位を割り当てることで、システムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、すべての NAC セッション イベントのロギングをイネーブルにします。

```
hostname# debug nac events
hostname#
```

次の例では、すべての NAC デバッグ メッセージのロギングをイネーブルにします。

```
hostname# debug nac all
hostname#
```

次の例では、すべての NAC デバッグ メッセージのロギングをディセーブルにします。

```
hostname# no debug nac
hostname#
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
eou initialize	1 つまたはそれ以上の NAC セッションに割り当てられているリソースを消去し、新しい無条件のポスチャ確認をセッションごとに開始します。
eou revalidate	1 つまたはそれ以上の NAC セッションのポスチャ再確認をただちに強制します。
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ntdomain

NT ドメイン認証のデバッグ情報を表示するには、特権 EXEC モードで **debug ntdomain** コマンドを使用します。NT ドメインのデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ntdomain [*level*]

no debug ntdomain

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、NT ドメインのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、NT ドメインのデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug ntdomain
debug ntdomain  enabled at level 1
hostname# show debug
debug ntdomain  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug ntp

NTP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug ntp** コマンドを使用します。NTP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug ntp {***adjust*** | ***authentication*** | ***events*** | ***loopfilter*** | ***packets*** | ***params*** | ***select*** | ***sync*** | ***validity***}

no debug ntp {***adjust*** | ***authentication*** | ***events*** | ***loopfilter*** | ***packets*** | ***params*** | ***select*** | ***sync*** | ***validity***}

シンタックスの説明

adjust	NTP クロック調整に関するメッセージを表示します。
authentication	NTP 認証に関するメッセージを表示します。
events	NTP イベントに関するメッセージを表示します。
loopfilter	NTP ループ フィルタに関するメッセージを表示します。
packets	NTP パケットに関するメッセージを表示します。
params	NTP クロック パラメータに関するメッセージを表示します。
select	NTP クロック セレクションに関するメッセージを表示します。
sync	NTP クロック同期に関するメッセージを表示します。
validity	NTP ピア クロックの有効性に関するメッセージを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、NTP に関するデバッグ メッセージをイネーブルにします。

```
hostname# debug ntp events
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバを指定します。
show debug	イネーブルなデバッガをすべて表示します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

debug ospf

OSPF ルーティング プロセスのデバッグ情報を表示するには、特権 EXEC モードで **debug ospf** コマンドを使用します。

debug ospf [***adj*** | ***database-timer*** | ***events*** | ***flood*** | ***lsa-generation*** | ***packet*** | ***retransmission*** | ***spf*** [***external*** | ***inter*** | ***intra***] | ***tree***]

no debug ospf [***adj*** | ***database-timer*** | ***events*** | ***flood*** | ***lsa-generation*** | ***packet*** | ***retransmission*** | ***spf*** [***external*** | ***inter*** | ***intra***] | ***tree***]

シンタックスの説明

adj	（オプション）OSPF 隣接イベントのデバッグをイネーブルにします。
database-timer	（オプション）OSPF タイマー イベントのデバッグをイネーブルにします。
events	（オプション）OSPF イベントのデバッグをイネーブルにします。
external	（オプション）SPF デバッグを外部イベントに制限します。
flood	（オプション）OSPF フラッディングのデバッグをイネーブルにします。
inter	（オプション）SPF デバッグをエリア間イベントに制限します。
intra	（オプション）SPF デバッグをエリア内イベントに制限します。
lsa-generation	（オプション）OSPF 集約 LSA 生成のデバッグをイネーブルにします。
packet	（オプション）受信した OSPF パケットのデバッグをイネーブルにします。
retransmission	（オプション）OSPF 再送信イベントのデバッグをイネーブルにします。
spf	（オプション）OSPF 最短パス優先計算のデバッグをイネーブルにします。SPF デバッグ情報は、***external***、***inter***、および ***intra*** のキーワードを使用することで制限できます。
tree	（オプション）OSPF データベース イベントのデバッグをイネーブルにします。

デフォルト

キーワードが提供されないときに、すべての OSPF デバッグ情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug ospf events** コマンドの出力例を示します。

```
hostname# debug ospf events
ospf event debugging is on

OSPF:hello with invalid timers on interface Ethernet0
hello interval received 10 configured 10
net mask received 255.255.255.0 configured 255.255.255.0
dead interval received 40 configured 30
```

関連コマンド

コマンド	説明
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

debug parser cache

CLI パーサーのデバッグ情報を表示するには、特権 EXEC モードで **debug parser cache** コマンドを使用します。CLI パーサーのデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug parser cache [*level*]

no debug parser cache

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、CLI パーサーのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、現在のデバッグ コンフィギュレーションを表示します。CLI パーサーのデバッグ メッセージは、**show debug** コマンドの出力の前後に表示されます。

```
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug pim

PIM のデバッグ情報を表示するには、特権 EXEC モードで **debug pim** コマンドを使用します。デバッグ情報の表示を停止するには、このコマンドの **no** 形式を使用します。

debug pim [***df-election*** [***interface*** *if_name* | ***rp*** *rp*] | ***group*** *group* | ***interface*** *if_name* | ***neighbor***]

no debug pim [***df-election*** [***interface*** *if_name* | ***rp*** *rp*] | ***group*** *group* | ***interface*** *if_name* | ***neighbor***]

シンタックスの説明

df-election	（オプション）PIM の双方向 DF 選定メッセージ プロセスに関するデバッグ メッセージを表示します。
group *group*	（オプション）指定されたグループのデバッグ情報を表示します。*group* の値は、次のいずれかです。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。
interface *if_name*	（オプション）***df-election*** キーワードと共に使用する場合は、DF 選定のデバッグ表示を、指定したインターフェイスに関する情報に制限します。 ***df-election*** キーワードと共に使用しない場合は、指定されたインターフェイスの PIM エラー メッセージを表示します。 **（注）** **debug pim *interface*** コマンドは、PIM プロトコル アクティビティ メッセージを表示せず、エラー メッセージだけを表示します。PIM プロトコル アクティビティのデバッグ情報を表示するには、***interface*** キーワードを使用せずに **debug pim** コマンドを使用します。***group*** キーワードを使用して、指定されたマルチキャスト グループに表示を制限することができます。
neighbor	（オプション）送信、または受信された PIM の HELLO メッセージだけを表示します。
rp *rp*	（オプション）次のいずれかを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

受信および送信された PIM パケットおよび PIM 関連のイベントを記録します。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug pim** コマンドの出力例を示します。

```
hostname# debug pim
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received RP-Reachable on Ethernet1 from 172.16.20.31
PIM: Update RP expiration timer for 224.2.0.1
PIM: Forward RP-reachability packet for 224.2.0.1 on Tunnel0
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Prune-list (10.221.196.51/32, 224.2.0.1)
PIM: Set join delay timer to 2 seconds for (10.221.0.0/16, 224.2.0.1) on Ethernet1
PIM: Received Join/Prune on Ethernet1 from 172.24.37.6
PIM: Received Join/Prune on Ethernet1 from 172.24.37.33
PIM: Received Join/Prune on Tunnel0 from 10.3.84.1
PIM: Join-list: (*, 224.2.0.1) RP 172.16.20.31
PIM: Add Tunnel0 to (*, 224.2.0.1), Forward state
PIM: Join-list: (10.0.0.0/8, 224.2.0.1)
PIM: Add Tunnel0 to (10.0.0.0/8, 224.2.0.1), Forward state
PIM: Join-list: (10.4.0.0/16, 224.2.0.1)
PIM: Prune-list (172.24.84.16/28, 224.2.0.1) RP-bit set RP 172.24.84.16
PIM: Send Prune on Ethernet1 to 172.24.37.6 for (172.24.84.16/28, 224.2.0.1), RP
PIM: For RP, Prune-list: 10.9.0.0/16
PIM: For RP, Prune-list: 10.16.0.0/16
PIM: For RP, Prune-list: 10.49.0.0/16
PIM: For RP, Prune-list: 10.84.0.0/16
PIM: For RP, Prune-list: 10.146.0.0/16
PIM: For 10.3.84.1, Join-list: 172.24.84.16/28
PIM: Send periodic Join/Prune to RP via 172.24.37.6 (Ethernet1)
```

関連コマンド

コマンド	説明
show pim group-map	グループからプロトコルへのマッピング テーブルを表示します。
show pim interface	PIM インターフェイス固有の情報を表示します。
show pim neighbor	PIM ネイバーテーブルのエントリを表示します。

debug pix pkt2pc

uauth コードに送信されたパケットをトレースし、uauth プロキシ セッションがデータ パスにカットスルーしたイベントをトレースするデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix pkt2pc** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix pkt2pc

no debug pix pkt2pc

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、uauth コードに送信されたパケットをトレースし、uauth プロキシ セッションがデータ パスにカットスルーしたイベントをトレースするデバッグ メッセージをイネーブルにします。

```
hostname# debug pix pkt2pc
```

関連コマンド

コマンド	説明
debug pix process	xlate およびセカンダリ接続プロセスに関するデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pix process

xlate およびセカンダリ接続プロセスに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug pix process** コマンドを使用します。デバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pix process

no debug pix process

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、xlate およびセカンダリ接続プロセスのデバッグ メッセージをイネーブルにします。

```
hostname# debug pix process
```

関連コマンド

コマンド	説明
debug pix pkt2pc	uauth コードに送信されたパケットをトレースし、uauth プロキシ セッションがデータ パスにカットスルーしたイベントをトレースするデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug pptp

PPTP に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug pptp** コマンドを使用します。PPTP に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug pptp [*level*]

no debug pptp [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug pptp** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、PPTP アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug pptp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect pptp	PPTP アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

debug radius

AAA に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug radius** コマンドを使用します。RADIUS メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug radius [***all*** | ***decode*** | ***session*** | ***user*** *username*]

no debug radius

シンタックスの説明

all	（オプション）デコードされた RADIUS メッセージを含む、すべてのユーザおよびセッションに関する RADIUS デバッグ メッセージを表示します。
decode	（オプション）RADIUS メッセージのデコードされたコンテンツを表示します。16 進値と、それらの値をデコードした読み取り可能なバージョンを含む、すべての RADIUS パケットのコンテンツが表示されます。
session	（オプション）セッション関連の RADIUS メッセージを表示します。送信および受信された RADIUS メッセージのパケット タイプは表示されますが、パケット コンテンツは表示されません。
user	（オプション）特定のユーザに関する RADIUS デバッグ メッセージを表示します。
username	メッセージを表示する対象のユーザを指定します。**user** キーワードと共に使用する場合だけ有効です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug radius コマンドは、セキュリティ アプライアンスと RADIUS AAA サーバの間の RADIUS メッセージに関する詳細情報を表示します。**no debug all** コマンドまたは **undebug all** コマンドは、イネーブルなデバッグをすべてオフにします。

例

次の例は、デコードされた RADIUS メッセージを示しています。これはアカウンティング パケットです。

```
hostname(config)# debug radius decode
hostname(config)# RADIUS packet decode (accounting request)

--------------------------------------
Raw packet data (length = 216).....
i
Parsed packet data.....
Radius: Code = 4 (0x04)
Radius: Identifier = 105 (0x69)
Radius: Length = 216 (0x00D8)
Radius: Vector: 842E0E99F44C00C05A0A19AB88A81312
Radius: Type = 40 (0x28) Acct-Status-Type
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x2
Radius: Type = 5 (0x05) NAS-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x1
Radius: Type = 4 (0x04) NAS-IP-Address
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.1.1.1 (0x0A010101)
Radius: Type = 14 (0x0E) Login-IP-Host
Radius: Length = 6 (0x06)
Radius: Value (IP Address) = 10.2.0.50 (0xD0FE1291)
Radius: Type = 16 (0x10) Login-TCP-Port
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x50
Radius: Type = 44 (0x2C) Acct-Session-Id
Radius: Length = 12 (0x0C)
Radius: Value (String) =
30 78 31 33 30 31 32 39 66 65                       |  0x130129fe
Radius: Type = 1 (0x01) User-Name
Radius: Length = 9 (0x09)
Radius: Value (String) =
62 72 6f 77 73 65 72                                |  browser
Radius: Type = 46 (0x2E) Acct-Session-Time
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x0
Radius: Type = 42 (0x2A) Acct-Input-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x256D
Radius: Type = 43 (0x2B) Acct-Output-Octets
Radius: Length = 6 (0x06)
Radius: Value (Hex) = 0x3E1
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 69 70 3d 31 30 2e     |  ip:source-ip=10.
31 2e 31 2e 31 30                                   |  1.1.10
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 27 (0x1B)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 21 (0x15)
Radius: Value (String) =
69 70 3a 73 6f 75 72 63 65 2d 70 6f 72 74 3d 33     |  ip:source-port=3
34 31 33                                            |  413
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 40 (0x28)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 34 (0x22)
Radius: Value (String) =
```

```
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 69    |  ip:destination-i
70 3d 32 30 38 2e 32 35 34 2e 31 38 2e 31 34 35    |  p=10.2.0.50
Radius: Type = 26 (0x1A) Vendor-Specific
Radius: Length = 30 (0x1E)
Radius: Vendor ID = 9 (0x00000009)
Radius: Type = 1 (0x01) Cisco-AV-pair
Radius: Length = 24 (0x18)
Radius: Value (String) =
69 70 3a 64 65 73 74 69 6e 61 74 69 6f 6e 2d 70    |  ip:destination-p
6f 72 74 3d 38 30                                  |  ort=80
```

関連コマンド

コマンド	説明
show running-config	セキュリティ アプライアンス上で実行されている設定を表示します。

debug rip

RIP のデバッグ情報を表示するには、特権 EXEC モードで **debug rip** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ***rip*** [***database*** | ***events***]

no debug ***rip*** [***database*** | ***events***]

シンタックスの説明

database	RIP データベース イベントを表示します。
events	RIP 処理イベントを表示します。

デフォルト

すべての RIP イベントがデバッグ出力に表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	***database*** キーワードと ***events*** キーワードが追加されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug rip** コマンドの出力例を示します。

```
hostname# debug rip

RIP: broadcasting general request on GigabitEthernet0/1
RIP: broadcasting general request on GigabitEthernet0/2
RIP: Received update from 10.89.80.28 on GigabitEthernet0/1
    10.89.95.0 in 1 hops
    10.89.81.0 in 1 hops
    10.89.66.0 in 2 hops
    172.31.0.0 in 16 hops (inaccessible)
    0.0.0.0 in 7 hops
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/1 (10.89.64.31)
    subnet 10.89.94.0, metric 1
    172.31.0.0 in 16 hops (inaccessible)
RIP: Sending update to 255.255.255.255 via GigabitEthernet0/2 (10.89.94.31)
    subnet 10.89.64.0, metric 1
    subnet 10.89.66.0, metric 3
    172.31.0.0 in 16 hops (inaccessible)
    default 0.0.0.0, metric 8
RIP: bad version 128 from 192.168.80.43
```

関連コマンド

コマンド	説明
router rip	RIP プロセスを設定します。
show running-config rip	実行コンフィギュレーション内の RIP コマンドを表示します。

debug rtp

H.323 検査および SIP 検査に関連する RTP パケットのデバッグ情報およびエラー メッセージを表示するには、特権 EXEC モードで **debug rtp** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug *rtp* [*level*]

no debug *rtp* [*level*]

シンタックスの説明

level	（オプション）デバッグのオプション レベルを指定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、**debug rtp** コマンドを使用して RTP パケットのデバッグをイネーブルにする方法を示しています。

```
hostname# debug rtp 255
debug rtp  enabled at level 255
```

関連コマンド

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
rtp-conformance	ピンホールを流れる RIP パケットの H.323 および SIP におけるプロトコル適合性を確認します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

debug rtsp

RTSP アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug rtsp** コマンドを使用します。RTSP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug rtsp [*level*]

no debug rtsp [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug rtsp** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、RTSP アプリケーション検査のデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug rtsp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect rtsp	RTSP アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

debug sdi

SDI 認証のデバッグ情報を表示するには、特権 EXEC モードで **debug sdi** コマンドを使用します。SDI デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sdi [*level*]

no debug sdi

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、SDI デバッグ メッセージをイネーブルにします。**show debug** コマンドは、SDI デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug sdi
debug sdi  enabled at level 1
hostname# show debug
debug sdi  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug sequence

すべてのデバッグ メッセージの最初にシーケンス番号を追加するには、特権 EXEC モードで **debug sequence** コマンドを使用します。デバッグ シーケンス番号の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sequence [*level*]

no debug sequence

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトは次のとおりです。

- デバッグ メッセージのシーケンス番号はディセーブルになっています。
- *level* のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、デバッグ メッセージのシーケンス番号をイネーブルにします。**debug parser cache** コマンドは、CLI パーサー デバッグ メッセージをイネーブルにします。**show debug** コマンドは、現在のデバッグ コンフィギュレーションを表示します。表示されている CLI パーサー デバッグ メッセージには、各メッセージの前にシーケンス番号が含まれます。

```
hostname# debug sequence
debug sequence  enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
0: parser cache: try to match 'show debug' in exec mode
debug parser cache enabled at level 1
debug sequence  enabled at level 1
1: parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug session-command

SSM へのセッションに対するデバッグ メッセージを表示するには、特権 EXEC モードで **debug session-command** コマンドを使用します。セッションに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug session-command [*level*]

no debug session-command [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、セッションのデバッグ メッセージをイネーブルにします。

```
hostname# debug session-command
```

関連コマンド

コマンド	説明
session	SSM へのセッションです。

debug sip

SIP アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug sip** コマンドを使用します。SIP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sip [*level*]

no debug sip [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug sip** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、SIP アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug sip
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect sip	SIP アプリケーション検査をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
show sip	セキュリティ アプライアンスを介して確立された SIP セッションに関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

debug skinny

SCCP（Skinny）アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug skinny** コマンドを使用します。SCCP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug skinny [*level*]

no debug skinny [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug skinny** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、SCCP アプリケーション検査に関するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug skinny
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect skinny	SCCP アプリケーション検査をイネーブルにします。
show skinny	セキュリティ アプライアンスを介して確立された SCCP セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

debug sla monitor

SLA モニタ オペレーションのデバッグ メッセージを表示するには、特権 EXEC モードで **debug sla monitor** コマンドを使用します。デバッグをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug sla monitor [***error*** | ***trace***] [*sla-id*]

no debug sla monitor [*sla-id*]

シンタックスの説明

error	（オプション）IP SLA モニタ エラー メッセージを出力します。
sla-id	（オプション）デバッグする SLA の ID を指定します。
trace	（オプション）IP SLA モニタ トレース メッセージを出力します。

デフォルト

エラー メッセージとトレース メッセージはデフォルトで表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

一度にデバッグできるのは 32 の SLA オペレーションのみです。

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、Cisco TAC とのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、SLA オペレーション エラーのデバッグをイネーブルにします。

```
hostname(config)# debug sla monitor error
```

次の例では、指定された SLA オペレーションの SLA オペレーション トレース メッセージの表示方法を示します。

```
hostname(config)# debug sla monitor trace 123
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。
clear route	RIP などのダイナミック ルーティング プロトコルを通じてラーニングされたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

debug sqlnet

SQL*Net アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug sqlnet** コマンドを使用します。SQL*Net アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sqlnet [*level*]

no debug sqlnet [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug sqlnet** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、SQL*Net アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug sqlnet
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect sqlnet	SQL*Net アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。
show conn	SQL*Net など、さまざまな接続タイプの接続状態を表示します。

debug ssh

SSH に関連するデバッグ情報およびエラー メッセージを表示するには、特権 EXEC モードで **debug ssh** コマンドを使用します。デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug *ssh* [*level*]

no debug *ssh* [*level*]

シンタックスの説明

level	（オプション）デバッグのオプション レベルを指定します。

デフォルト

デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次に、**debug ssh *255*** コマンドの出力例を示します。

```
hostname# debug ssh 255
debug ssh  enabled at level 255
SSH2 0: send: len 64 (includes padlen 17)
SSH2 0: done calc MAC out #239
SSH2 0: send: len 32 (includes padlen 7)
SSH2 0: done calc MAC out #240
SSH2 0: send: len 64 (includes padlen 15)
SSH2 0: done calc MAC out #241
SSH2 0: send: len 32 (includes padlen 16)
SSH2 0: done calc MAC out #242
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #243
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #244
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #245
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #246
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #247
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #248
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #249
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #250
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #251
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #252
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #253
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #254
SSH2 0: send: len 64 (includes padlen 8)
SSH2 0: done calc MAC out #255
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #256
SSH2 0: send: len 64 (includes padlen 7)
SSH2 0: done calc MAC out #257
SSH2 0: send: len 64 (includes padlen 18)
SSH2 0: done calc MAC out #258
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
show ssh sessions	セキュリティ アプライアンス上のアクティブな SSH セッションに関する情報を表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。

debug ssl

SSL のデバッグ情報を表示するには、特権 EXEC モードで **debug ssl** コマンドを使用します。SSL デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug ssl {***cipher*** | ***device***} [*level*]

no debug ssl {***cipher*** | ***device***}

シンタックスの説明

cipher	HTTP サーバとクライアント間の暗号ネゴシエーションに関する情報を表示します。
device	セッションの開始と進行中のステータスを含む SSL デバイスに関する情報を表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、特に暗号ネゴシエーションに対する SSL デバッグ メッセージをイネーブルにします。**show debug** コマンドは、SSL デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug ssl cipher
debug ssl cipher enabled at level 1
hostname# show debug
debug ssl cipher enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug sunrpc

RPC アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug sunrpc** コマンドを使用します。RPC アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug sunrpc [*level*]

no debug sunrpc [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug sunrpc** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、RPC アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug sunrpc
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect sunrpc	Sun RPC アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
show conn	RPC など、さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

debug switch ilpm

ASA 5505 適応型セキュリティ アプライアンスなどの内蔵スイッチが搭載されたモデルの場合、特権 EXEC モードで **debug switch ilpm** コマンドを使用して PoE のデバッグ メッセージを表示します。PoE に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug switch ilpm [**events** | **errors**] [*level*]

no debug switch ilpm [**events** | **errors**] [*level*]

シンタックスの説明

errors	（オプション）エラーがある場合に、トラブルシューティング情報を表示します。
events	（オプション）PoE イベントを表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

キーワードを指定しない場合、デフォルトではイベントとエラーの両方が表示されます。デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、PoE ポートのデバッグ メッセージをイネーブルにします。

```
hostname# debug switch ilpm
```

関連コマンド

コマンド	説明
interface vlan	VLAN インターフェイスを追加します。
debug switch manager	VLAN 割り当てのデバッグ メッセージと **switchport** コマンドにより発生したイベントとエラーを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug switch manager

ASA 5505 適応型セキュリティ アプライアンスなどの内蔵スイッチが搭載されたモデルの場合、特権 EXEC モードで **debug switch manager** コマンドを使用して、VLAN 割り当てのデバッグ メッセージと **switchport** コマンドにより発生したイベントとエラーを表示します。スイッチ ポートに関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug switch manager [**events** | **errors**] [*level*]

no debug switch manager [**events** | **errors**] [*level*]

シンタックスの説明

errors	（オプション）エラーがある場合に、トラブルシューティング情報を表示します。
events	（オプション）スイッチ マネージャ イベントを表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

キーワードを指定しない場合、デフォルトではイベントとエラーの両方が表示されます。デフォルトのレベルは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

debug コマンドを使用すると、通信量の多いネットワークのトラフィックが遅くなる可能性があります。

例

次の例では、スイッチ ポートのデバッグ メッセージをイネーブルにします。

```
hostname# debug switch manager
```

関連コマンド

コマンド	説明
interface vlan	VLAN インターフェイスを追加します。
debug switch ilpm	PoE に関するデバッグ メッセージを表示します。
show debug	イネーブルなデバッガをすべて表示します。

debug tacacs

TACACS+ のデバッグ情報を表示するには、特権 EXEC モードで **debug tacacs** コマンドを使用します。TACACS+ デバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug tacacs [***session*** | ***user*** *username*]

no debug tacacs [***session*** | ***user*** *username*]

シンタックスの説明

session	セッション関連の TACACS+ デバッグ メッセージを表示します。
user	ユーザ固有の TACACS+ デバッグ メッセージを表示します。一度に 1 人のユーザの TACACS+ デバッグ メッセージだけ表示できます。
username	TACACS+ デバッグ メッセージを表示するユーザを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、TACACS+ デバッグ メッセージをイネーブルにします。**show debug** コマンドは、TACACS+ デバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug tacacs user admin342
hostname# show debug
debug tacacs user admin342
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug tcp-map

TCP アプリケーション検査マップに関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug tcp-map** コマンドを使用します。TCP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug tcp-map

no debug tcp-map

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、TCP アプリケーション検査マップに対するデバッグ メッセージをイネーブルにします。**show debug** コマンドは、TCP アプリケーション検査マップのデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug tcp-map
debug tcp-map enabled at level 1.
hostname# show debug
debug tcp-map enabled at level 1.
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug timestamps

すべてのデバッグ メッセージの最初にタイムスタンプ情報を追加するには、特権 EXEC モードで **debug timestamps** コマンドを使用します。デバッグ タイムスタンプの使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug timestamps [*level*]

no debug timestamps

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

デフォルトは次のとおりです。

- デバッグ タイムスタンプ情報はディセーブルです。
- *level* のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、デバッグ メッセージのタイムスタンプをイネーブルにします。**debug parser cache** コマンドは、CLI パーサー デバッグ メッセージをイネーブルにします。**show debug** コマンドは、現在のデバッグ コンフィギュレーションを表示します。表示されている CLI パーサー デバッグ メッセージには、各メッセージの前にタイムスタンプが含まれています。

```
hostname# debug timestamps
debug timestamps  enabled at level 1
hostname# debug parser cache
debug parser cache enabled at level 1
hostname# show debug
1982769.770000000: parser cache: try to match 'show debug' in exec mode
1982769.770000000: parser cache: hit at index 8
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug vpn-sessiondb

VPN セッション データベースのデバッグ情報を表示するには、特権 EXEC モードで **debug vpn-sessiondb** コマンドを使用します。VPN セッション データベースに関するデバッグ情報の表示をディセーブルにするには、このコマンドの **no** 形式を使用します。

debug vpn-sessiondb [*level*]

no debug vpn-sessiondb

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力は CPU プロセスで高優先順位が割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、VPN セッション データベースのデバッグ メッセージをイネーブルにします。**show debug** コマンドは、VPN セッション データベースのデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug vpn-sessiondb
debug vpn-sessiondb  enabled at level 1
hostname# show debug
debug vpn-sessiondb  enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug wccp

WCCP イベントのロギングをイネーブルにするには、特権 EXEC モードで **debug wccp** コマンドを使用します。WCCP デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug wccp {***events*** | ***packets*** | ***subblocks***}

no debug wccp {***events*** | ***packets*** | ***subblocks***}

シンタックスの説明

events	WCCP セッション イベントのロギングをイネーブルにします。
packets	WCCP パケット情報に関するデバッグ メッセージのロギングをイネーブルにします。
subblocks	WCCP サブブロックに関するデバッグ メッセージのロギングをイネーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力に高優先順位を割り当てることで、システムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、すべての WCCP セッション イベントのロギングをイネーブルにします。

```
hostname# debug wccp events
hostname#
```

次の例では、WCCP パケット デバッグ メッセージのロギングをイネーブルにします。

```
hostname# debug wccp packets
hostname#
```

次の例では、WCCP デバッグ メッセージのロギングをディセーブルにします。

```
hostname# no debug wccp
hostname#
```

関連コマンド

コマンド	説明
wccp	WCCP のサポートをイネーブルにします。
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug webvpn

WebVPN デバッグ メッセージをログに記録するには、特権 EXEC モードで **debug webvpn** コマンドを使用します。WebVPN デバッグ メッセージのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

debug webvpn [***chunk*** | ***cifs*** | ***citrix*** | ***failover*** | ***html*** | ***javascript*** | ***request*** | ***response*** | ***svc*** | ***transformation*** | ***url*** | ***util*** | ***xml***] [*level*]

no debug webvpn [***chunk*** | ***cifs*** | ***citrix*** | ***failover*** | ***html*** | ***javascript*** | ***request*** | ***response*** | ***svc*** | ***transformation*** | ***url*** | ***util*** | ***xml***] [*level*]

シンタックスの説明

chunk	WebVPN 接続のサポートに使用されるメモリ ブロックのデバッグ メッセージを表示します。
cifs	Common Internet File System（CIFS）サーバと WebVPN ユーザの間の接続のデバッグ メッセージを表示します。
citrix	Citrix Metaframe サーバと Citrix ICA クライアントの間の、WebVPN を通した接続のデバッグ メッセージを表示します。
failover	WebVPN 接続に影響を与える機器のフェールオーバーのデバッグ メッセージを表示します。
html	WebVPN 接続を通して送信される HTML ページのデバッグ メッセージを表示します。
javascript	WebVPN 接続を通して送信される JavaScript のデバッグ メッセージを表示します。
request	WebVPN 接続を通して送信される要求のデバッグ メッセージを表示します。
response	WebVPN 接続を通して送信される応答のデバッグ メッセージを表示します。
svc	WebVPN を通した SSL VPN クライアントへの接続に関するデバッグ メッセージを表示します。
transformation	WebVPN の内容の変換に関するデバッグ メッセージを表示します。
url	WebVPN 接続を通して送信される Web サイト要求に関するデバッグ メッセージを表示します。
util	WebVPN リモート ユーザへの接続のサポートだけに使用される CPU の利用率に関するデバッグ メッセージを表示します。
xml	WebVPN 接続を通して送信される JavaScript のデバッグ メッセージを表示します。
level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ出力に高優先順位を割り当てることで、システムが使用できなくなることがあります。このため、特定の問題のトラブルシューティングを行う場合や、シスコのテクニカル サポート スタッフとのトラブルシューティング セッションの間に限り **debug** コマンドを使用してください。さらに、ネットワーク トラフィック量やユーザ数が少ない期間に **debug** コマンドを使用することをお勧めします。このような期間にデバッグを実行すると、**debug** コマンドの処理オーバーヘッドの増加によってシステムの使用に影響が生じる可能性が低くなります。

例

次の例では、特に CIFS に対する WebVPN デバッグ メッセージをイネーブルにします。**show debug** コマンドは、CIFS のデバッグ メッセージがイネーブルになっていることを示します。

```
hostname# debug webvpn cifs
INFO: debug webvpn cifs enabled at level 1.
hostname# show debug
debug webvpn cifs enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
show debug	現在のデバッグ コンフィギュレーションを表示します。

debug xdmcp

XDMCP アプリケーション検査に関するデバッグ メッセージを表示するには、特権 EXEC モードで **debug xdmcp** コマンドを使用します。XDMCP アプリケーション検査に関するデバッグ メッセージの表示を停止するには、このコマンドの **no** 形式を使用します。

debug xdmcp [*level*]

no debug xdmcp [*level*]

シンタックスの説明

level	（オプション）表示するデバッグ メッセージのレベル（1 ～ 255）を設定します。デフォルトは 1 です。高レベルの追加メッセージを表示するには、レベルを高い数値に設定します。

デフォルト

level のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

debug コマンドの現在の設定を表示するには、**show debug** コマンドを入力します。デバッグ出力を停止するには、**no debug** コマンドを入力します。デバッグ メッセージがすべて表示されないようにするには、**no debug all** コマンドを入力します。

（注） **debug xdmcp** コマンドをイネーブルにすると、通信量の多いネットワークでは、トラフィックの速度が遅くなります。

例

次の例では、XDMCP アプリケーション検査に対するデバッグ メッセージをデフォルトのレベル（1）でイネーブルにします。

```
hostname# debug xdmcp
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect xdmcp	XDMCP アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

CHAPTER 11

default コマンド～ duplex コマンド

default

time-range コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードのデフォルト設定を復元するには、時間範囲コンフィギュレーション モードで ***default*** コマンドを使用します。

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

シンタックスの説明

absolute	時間範囲が有効である絶対時間を定義します。
days-of-the-week	（オプション）最初の days-of-the-week 引数は、関連付けられている時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（monday（月曜日）、tuesday（火曜日）、wednesday（水曜日）、thursday（木曜日）、friday（金曜日）、saturday（土曜日）、および sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***to*** キーワードを入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ コンテキスト	システム
時間範囲コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、終了の days-of-the-week 値を省略できます。

time-range コマンドに ***absolute*** 値と ***periodic*** 値の両方が指定されている場合、***periodic*** コマンドは ***absolute start*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 機能はセキュリティ アプライアンスのシステム クロックに依存しています。しかし、この機能は、NTP 同期化により最適に動作します。

例

次の例は、***absolute*** キーワードのデフォルト動作を復元する方法を示しています。

```
hostname(config-time-range)# default absolute
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効である絶対時間を定義します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

default（crl 設定）

すべての CRL パラメータをシステムのデフォルト値に戻すには、crl 設定コンフィギュレーション モードで **default** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバが必要とする場合にだけ使用されます。

default

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•		•		

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。

例

次の例では、ca-crl コンフィギュレーション モードに入り、CRL コマンド値をデフォルトに戻します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# default
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol ldap	CRL の取得方法として LDAP を指定します。

default（時間範囲）

absolute コマンドおよび ***periodic*** コマンドのデフォルト設定を復元するには、時間範囲コンフィギュレーション モードで ***default*** コマンドを使用します。

default {**absolute** | **periodic** *days-of-the-week time* **to** [*days-of-the-week*] *time*}

シンタックスの説明

absolute	時間範囲が有効である絶対時間を定義します。
days-of-the-week	最初の days-of-the-week 引数は、関連付けられている時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（monday（月曜日）、tuesday（火曜日）、wednesday（水曜日）、thursday（木曜日）、friday（金曜日）、saturday（土曜日）、および sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***to*** キーワードを入力する必要があります。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
時間範囲コンフィギュレーション	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、終了の days-of-the-week 値を省略できます。

time-range コマンドに ***absolute*** 値と ***periodic*** 値の両方が指定されている場合、***periodic*** コマンドは ***absolute start*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 機能はセキュリティ アプライアンスのシステム クロックに依存しています。しかし、この機能は、NTP 同期化により最適に動作します。

例

次の例は、***absolute*** キーワードのデフォルト動作を復元する方法を示しています。

```
hostname(config-time-range)# default absolute
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効である絶対時間を定義します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

default enrollment

すべての登録パラメータをシステムのデフォルト値に戻すには、暗号 CA トラストポイント コンフィギュレーション モードで **default enrollment** コマンドを使用します。

default enrollment

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションの一部になりません。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、すべての登録パラメータをトラストポイント central 内のデフォルト値に戻します。

```
hostname<config># crypto ca trustpoint central
hostname<ca-trustpoint># default enrollment
hostname<ca-trustpoint>#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crl configure	crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。

default-domain

グループ ポリシーのユーザに対してデフォルトのドメイン名を設定するには、グループ ポリシー コンフィギュレーション モードで **default-domain** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

デフォルトのドメイン名をすべて削除するには、引数なしで **no default-domain** コマンドを使用します。**default-domain none** コマンドを発行して作成された null リストを含む設定済みのデフォルトのドメイン名がすべて削除されます。ユーザがドメイン名を継承しないようにするには、**default-domain none** コマンドを使用します。

セキュリティ アプライアンスは、ドメイン フィールドを省略した DNS クエリーに付加するために、デフォルト ドメイン名を IPSec クライアントに渡します。このドメイン名は、トンネル パケットにだけ適用されます。デフォルト ドメイン名がない場合、ユーザはデフォルト グループ ポリシーのデフォルト ドメイン名を継承します。

default-domain {value *domain-name* **| none}**

no default-domain [*domain-name***]**

シンタックスの説明

none	デフォルト ドメイン名がないことを指定します。デフォルト ドメイン名にヌル値を設定して、デフォルト ドメイン名を拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからデフォルトのドメイン名を継承しないようにします。
value *domain-name*	グループのデフォルト ドメイン名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトのドメイン名に使用できるのは、英数字、ハイフン（-）、およびピリオド（.）だけです。

例

次の例は、FirstGroup という名前のグループ ポリシーに対して FirstDomain のデフォルト ドメイン名を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# default-domain value FirstDomain
```

関連コマンド

コマンド	説明
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。
split-tunnel-policy	IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

default-group-policy

デフォルトでユーザが継承するアトリビュートのセットを指定するには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **default-group-policy** コマンドを使用します。デフォルトのグループ ポリシー名を削除するには、このコマンドの ***no*** 形式を使用します。

default-group-policy *group-name*

no default-group-policy *group-name*

シンタックスの説明

group-name	デフォルト グループの名前を指定します。

デフォルト

デフォルト グループ名は、DfltGrpPolicy です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn コンフィギュレーション モードの **default-group-policy** コマンドは廃止されました。トンネル グループ一般アトリビュート モードの **default-group-policy** コマンドで置き換えられています。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

デフォルトのグループ ポリシー DfltGrpPolicy では、セキュリティ アプライアンスが初期設定されています。すべてのトンネル グループ タイプにこのアトリビュートを適用できます。

例

次の例では、Config-general コンフィギュレーション モードに入り、「standard-policy」という名前の IPSec LAN-to-LAN トンネル グループで、ユーザがデフォルトで継承するアトリビュートのセットを指定します。このコマンドのセットは、アカウンティング サーバ、認証サーバ、認可サーバおよびアドレス プールを定義します。

```
hostname(config)# tunnel-group standard-policy type ipsec-ra
hostname(config)# tunnel-group standard-policy general-attributes
hostname(config-tunnel-general)# default-group-policy first-policy
hostname(config-tunnel-general)# accounting-server-group aaa-server123
hostname(config-tunnel-general)# address-pool (inside) addrpool1 addrpool2 addrpool3
hostname(config-tunnel-general)# authentication-server-group aaa-server456
hostname(config-tunnel-general)# authorization-server-group aaa-server78
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
group-policy	グループ ポリシーを作成または編集します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般アトリビュートを指定します。

default-group-policy（webvpn）

WebVPN または電子メールのプロキシ コンフィギュレーションがグループ ポリシーを指定していない場合に、使用するグループ ポリシー名を指定するには、**default-group-policy** コマンドを使用します。WebVPN、IMAP4S、POP3S、および SMTPS セッションは、指定されたグループ ポリシーまたはデフォルトのグループ ポリシーのいずれかを必要とします。WebVPN の場合、このコマンドは webvpn モードで使用します。電子メールの場合、このコマンドは、該当する電子メール プロキシ モードで使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

default-group-policy *groupname*

no default-group-policy

シンタックスの説明

groupname	デフォルトのグループ ポリシーとして使用する設定済みのグループ ポリシーを指定します。コンフィギュレーション モードで **group-policy** コマンドを使用し、グループ ポリシーを設定します。

デフォルト

DfltGrpPolicy という名前のデフォルト グループ ポリシーは、常にセキュリティ アプライアンスに存在します。**default-group-policy** コマンドを使用すると、作成したグループ ポリシーを、WebVPN および電子メール プロキシ セッション用のデフォルトのグループ ポリシーとして置き換えることができます。別の方法として、DfltGrpPolicy を編集することもできます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
Pop3s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、webvpn コンフィギュレーション モードでは廃止され、トンネル グループ一般アトリビュート コンフィギュレーション モードに置き換えられました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ一般アトリビュート モードの同等のコマンドに変換されます。

システムの DefaultGroupPolicy は編集できますが、削除できません。DefaultGroupPolicy の AVP は次のとおりです。

アトリビュート	デフォルト値
wins-server	none
dns-server	none
dhcp-network-scope	none
vpn-access-hours	unrestricted
vpn-simultaneous-logins	3
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-filter	none
vpn-tunnel-protocol	WebVPN
ip-comp	disable
re-xauth	disable
group-lock	none
pfs	disable
client-access-rules	none
banner	none
password-storage	disabled
ipsec-udp	disabled
ipsec-udp-port	0
backup-servers	keep-client-config
split-tunnel-policy	tunnelall
split-tunnel-network-list	none
default-domain	none
split-dns	none
intercept-dhcp	disable
client-firewall	none
secure-unit-authentication	disabled
user-authentication	disabled
user-authentication-idle-timeout	none
ip-phone-bypass	disabled
leap-bypass	disabled
nem	disabled
webvpn アトリビュート：	
filter	none
functions	disabled
homepage	none
html-content-filter	none
port-forward	disabled
port-forward-name	none
url-list	mpme

例

次の例は、WebVPN に WebVPN7 という名前のデフォルト グループ ポリシーを指定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# default-group-policy WebVPN7
```

default-idle-timeout

WebVPN ユーザに対するデフォルトのアイドル タイムアウト値を設定するには、webvpn モードで **default-idle-timeout** コマンドを使用します。デフォルトのアイドル タイムアウト値をコンフィギュレーションから削除してデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

デフォルトのアイドル タイムアウトを使用すると、セッションの失効を防ぐことができます。

default-idle-timeout *seconds*

no default-idle-timeout

シンタックスの説明

seconds	アイドル タイムアウトの秒数を指定します。最小値は 60 秒、最大値は 1 日（86,400 秒）です。

デフォルト

1,800 秒（30 分）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ユーザのアイドル タイムアウトが定義されていない場合、値が 0 の場合、または値が有効な範囲外である場合、セキュリティ アプライアンスはここで設定された値を使用します。

このコマンドに、短い時間を設定することをお勧めします。理由は、クッキーがディセーブルにされている（またはクッキーを要求され、それを拒否する）設定のブラウザにより、ユーザが接続していなくてもセッション データベースに表示される場合があるからです。許容する接続の最大数が 1 に設定されている場合は（**vpn-simultaneous-logins** コマンド）、すでに接続の最大数に達していることをデータベースが示すため、ユーザはログインし直すことができません。アイドル タイムアウトを低く設定すると、そのような実体のないセッションを迅速に削除し、ユーザは再度ログインできます。

例

次の例は、デフォルトのアイドル タイムアウトを 1,200 秒（20 分）に設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# default-idle-timeout 1200
```

関連コマンド

コマンド	説明
vpn-simultaneous-logins	許容する同時 VPN セッションの最大数を設定します。グループ ポリシーまたはユーザ名モードで使用します。

default-information originate（OSPF）

OSPF ルーティング ドメインへのデフォルトの外部ルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

default-information originate [***always***] [***metric*** *value*] [***metric-type*** {***1*** | ***2***}] [***route-map*** *name*]

no default-information originate [[***always***] [***metric*** *value*] [***metric-type*** {***1*** | ***2***}] [***route-map*** *name*]]

シンタックスの説明

always	（オプション）ソフトウェアでデフォルト ルートが設定されているかどうかかかわらず、常にデフォルト ルートをアドバタイズします。
metric *value*	（オプション）OSPF デフォルト メトリック値を指定します（0 ～ 16777214）。
metric-type {1 | 2}	（オプション）OSPF ルーティング ドメインにアドバタイズされたデフォルト ルートに関連する外部リンク タイプです。有効な値は次のとおりです。 • ***1***：タイプ 1 外部ルート • ***2***：タイプ 2 外部ルート
route-map *name*	（オプション）適用するルートマップの名前。

デフォルト

デフォルト値は次のとおりです。

- ***metric*** *value* は 1 です。
- ***metric-type*** は 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドの **no** 形式をオプションのキーワードおよび引数と共に使用すると、コマンドからオプションの情報だけが削除されます。たとえば、**no default-information originate** ***metric 3*** を入力すると、実行コンフィギュレーションのコマンドから ***metric 3*** オプションが削除されます。実行コンフィギュレーションからコマンド全体を削除するには、このコマンドの **no** 形式をオプションなしで使用します。つまり **no default-information originate** となります。

例

次の例は、オプションのメトリックおよびメトリック タイプと共に **default-information originate** コマンドを使用する方法を示しています。

```
hostname(config-router)# default-information originate always metric 3 metric-type 2
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

default-information originate（RIP）

RIP へのデフォルトのルートを生成するには、ルータ コンフィギュレーション モードで **default-information originate** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

default-information originate [***route-map*** *name*]

no default-information originate [***route-map*** *name*]

シンタックスの説明

route-map *name*	（オプション）適用するルートマップの名前。ルートマップが満たされると、ルーティング プロセスはデフォルトのルートを生成します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

default-information originate コマンドで参照されるルートマップは拡張アクセス リストを使用できません。標準のアクセス リストを使用します。

例

次の例では、デフォルト ルートを RIP に生成する方法を示します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# default-information originate
```

関連コマンド

コマンド	説明
router rip	RIP ルーティング プロセスのルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

delete

ディスク パーティションのファイルを削除するには、特権 EXEC モードで **delete** コマンドを使用します。

delete [**/noconfirm**] [**/recursive**] [**flash:**]*filename*

シンタックスの説明

/noconfirm	（オプション）確認のためのプロンプトを表示しないように指定します。
/recursive	（オプション）指定されたファイルをすべてのサブディレクトリで再帰的に削除します。
filename	削除するファイルの名前を指定します。
flash:	取り外しできない内蔵フラッシュを指定して、続けてコロン（:）を入力します。

デフォルト

ディレクトリを指定しない場合のデフォルトのディレクトリは、現在の作業ディレクトリです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

パスを指定しない場合、ファイルは現在の作業ディレクトリから削除されます。ファイルの削除では、ワイルドカードがサポートされています。ファイルを削除する場合、ファイル名のプロンプトが表示され、削除を確認する必要があります。

次の例は、現在の作業ディレクトリにある *test.cfg* という名前のファイルを削除する方法を示しています。

```
hostname# delete test.cfg
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに移動します。
rmdir	ファイルまたはディレクトリを削除します。
show file	指定されたファイルを表示します。

deny-message（グループ ポリシー webvpn コンフィギュレーション モード）

WebVPN に正常にログインしているが、VPN 権限を持たないリモート ユーザに配信されるメッセージを変更するには、トンネル グループ webvpn コンフィギュレーション モードで **deny-message value** コマンドを使用します。

no deny-message value コマンドは、文字列を削除するので、リモート ユーザはメッセージを受信できません。

no deny-message none コマンドは、トンネル グループ ポリシー コンフィギュレーションからアトリビュートを削除します。ポリシーはアトリビュート値を継承します。

deny-message value "*string***"**

no deny-message value

no deny-message none

シンタックスの説明

string	最大 491 文字の英数字で、特殊文字、スペース、および句読点を含みます。

デフォルト

デフォルトの拒否メッセージは次のとおりです。「ログインには成功しますが、特定の基準に適合しなかったり、一部の特定のグループ ポリシーがあったりする影響で、VPN 機能のいずれも使用する権限は与えられません。詳細については、IT 管理者にお問い合せください。」

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドはトンネル グループ webvpn コンフィギュレーション モードからグループ ポリシー webvpn コンフィギュレーション モードに移行しました。

使用上のガイドライン

このコマンドを入力する前に、グローバル コンフィギュレーション モードで **group-policy** *name* **attributes** を入力し、**webvpn** コマンドを入力します（すでに policy *name* を作成していることを前提としています）。

deny-message value コマンドで文字列を入力する場合は、コマンドが折り返しても続けて入力します。

VPN セッションで使用されるトンネル ポリシーとは別に、ログインの際にリモート ユーザのブラウザにこのテキストが表示されます。

例

次の例の最初のコマンドは group2 と呼ばれる内部グループ ポリシーを作成します。後続のコマンドは、そのポリシーに関連した拒否メッセージを変更します。

```
hostname(config)# group-policy group2 internal
hostname(config)# group-policy group2 attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# deny-message value "Your login credentials are OK.
However, you have not been granted rights to use the VPN features. Contact your
administrator for more information."
hostname(config-group-webvpn)
```

関連コマンド

コマンド	説明
clear configure group-policy	すべてのグループ ポリシー コンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成します。
group-policy attributes	グループ ポリシー コンフィギュレーション モードに入ります。
show running-config group-policy [*name*]	実行中のグループ ポリシー コンフィギュレーションを表示します（名前の付いたポリシーに対して）。
webvpn（グループ ポリシーまたはユーザ名コンフィギュレーション モード）	グループ ポリシー webvpn コンフィギュレーション モードに入ります。

deny version

SNMP トラフィックの特定のバージョンを拒否するには、SNMP マップ コンフィギュレーション モードで deny version コマンドを使用します。このモードには、グローバル コンフィギュレーション モードから snmp-map コマンドを入力してアクセスできます。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

deny version *version*

no deny version *version*

シンタックスの説明

version	セキュリティ アプライアンスがドロップする SNMP トラフィックのバージョンを指定します。許可される値は **1**、**2**、**2c**、および **3** です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SNMP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

deny version コマンドを使用して、SNMP トラフィックを、SNMP の特定のバージョンに制限します。SNMP の以前のバージョンはセキュリティが低いため、セキュリティ ポリシーで SNMP トラフィックを Version 2 に制限することができます。**snmp-map** コマンドを使用して設定する SNMP マップ内で **deny version** コマンドを使用します。SNMP マップを作成した後で、**inspect snmp** コマンドを使用してマップをイネーブルにし、次に **service-policy** コマンドを使用して 1 つまたは複数のインターフェイスに適用します。

例

次の例は、SNMP トラフィックを識別し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

description

指定したコンフィギュレーション ユニット（たとえば、コンテキストまたはオブジェクト グループ）に対する説明を追加するには、さまざまなコンフィギュレーション モードで **description** コマンドを使用します。この説明を削除するには、このコマンドの **no** 形式を使用します。説明により、役立つ情報がコンフィギュレーションに追加されます。

description *text*

no description

シンタックスの説明

text	説明に、最大 200 文字のテキスト文字列を設定します。文字列に疑問符（?）を含める場合は、不注意から CLI ヘルプを呼び出さないように、**Ctrl+V** を入力してから疑問符を入力する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—
コンテキスト コンフィギュレーション	•	•	—	—	•
Gtp マップ コンフィギュレーション	•	•	•	•	—
インターフェイス コンフィギュレーション	•	•	•	•	•
オブジェクト グループ コンフィギュレーション	•	•	•	•	—
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、複数の新しいコンフィギュレーション モードに追加されました。

例

次の例は、「アドミニストレーション」コンテキスト コンフィギュレーションに説明を追加したものです。

```
hostname(config)# context administrator
hostname(config-context)# description This is the admin context.
hostname(config-context)# allocate-interface gigabitethernet0/0.1
hostname(config-context)# allocate-interface gigabitethernet0/1.1
hostname(config-context)# config-url flash://admin.cfg
```

関連コマンド

コマンド	説明
class-map	**policy-map** コマンドでアクションを適用するトラフィックを指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
gtp-map	GTP 検査エンジンのパラメータを制御します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
object-group	**access-list** コマンドに含めるトラフィックを指定します。
policy-map	**class-map** コマンドで指定されたトラフィックに適用するアクションを指定します。

dhcp client route distance

DHCP を通じてラーニングしたルートの管理ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route distance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dhcp client route distance *distance*

no dhcp client route distance *distance*

シンタックスの説明

distance	DHCP を通じてラーニングしたルートに適用する管理ディスタンス。有効な値は 1 ～ 255 です。

デフォルト

DHCP を通じてラーニングしたルートには、デフォルトで管理ディスタンス 1 が割り当てられます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

dhcp client route distance コマンドは、ルートが DHCP を通じてラーニングされる場合にのみチェックされます。DHCP を通じてルートをラーニングした後に **dhcp client route distance** コマンドを入力した場合、指定された管理ディスタンスはラーニング済みの既存のルートには影響しません。指定した管理ディスタンスが与えられるのは、このコマンドの入力後にラーニングされたルートだけです。

DHCP を利用してルートを取得するには、**ip address dhcp** コマンドに ***setroute*** オプションを指定する必要があります。

複数のインターフェイスで DHCP を設定した場合は、各インターフェイスについて **dhcp client route distance** コマンドを使用して、インストール済みルートの優先順位を指定する必要があります。

例

次の例では、GigabitEthernet0/2 上で DHCP を利用してデフォルト ルートを取得します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA オペレーションによって、外部インターフェイスからの 10.1.1.1 ゲートウェイの可用性が監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で DHCP を通じて取得したバックアップ ルートが使用されます。バックアップ ルートには、管理ディスタンス 254 が割り当てられています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

関連コマンド

コマンド	説明
dhcp client route track	DHCP を通じてラーニングしたルートを、トラッキング エントリ オブジェクトに関連付けます。
ip address dhcp	DHCP を通じて取得した IP アドレスを使用して、指定したインターフェイスを設定します。
sla monitor	SLA 監視オペレーションを定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

dhcp client route track

追加ルートをトラッキング済みの指定オブジェクト番号に関連付けるように DHCP クライアントを設定するには、インターフェイス コンフィギュレーション モードで **dhcp client route track** コマンドを使用します。DHCP クライアント ルート トラッキングをディセーブルにするには、このコマンドの **no** 形式を使用します。

dhcp client route track *number*

no dhcp client route track

シンタックスの説明

number	トラッキング エントリのオブジェクト ID。有効な値は 1 ～ 500 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

dhcp client route track コマンドは、DHCP を通じてルートをラーニングする場合にのみチェックされます。DHCP を通じてルートをラーニングした後に **dhcp client route track** コマンドを入力した場合、ラーニングした既存のルートは、トラッキング オブジェクトには関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後にラーニングされたルートだけです。

DHCP を利用してルートを取得するには、**ip address dhcp** コマンドに ***setroute*** オプションを指定する必要があります。

複数のインターフェイスで DHCP を設定した場合は、各インターフェイスについて **dhcp client route distance** コマンドを使用して、インストール済みルートの優先順位を指定する必要があります。

例

次の例では、GigabitEthernet0/2 上で DHCP を利用してデフォルト ルートを取得します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA オペレーションによって、外部インターフェイスからの 10.1.1.1 ゲートウェイの可用性が監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で DHCP を通じて取得したバックアップ ルートが使用されます。バックアップ ルートには、管理ディスタンス 254 が割り当てられています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# dhcp client route track 1
hostname(config-if)# ip address dhcp setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# dhcp client route track 1
hostname(config-if)# dhcp client route distance 254
hostname(config-if)# ip address dhcp setroute
```

関連コマンド

コマンド	説明
dhcp client route distance	DHCP を通じてラーニングしたルートに管理ディスタンスを割り当てます。
ip address dhcp	DHCP を通じて取得した IP アドレスを使用して、指定したインターフェイスを設定します。
sla monitor	SLA 監視オペレーションを定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

dhcp-client update dns

DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定するには、グローバル コンフィギュレーション モードで **dhcp-client update dns** コマンドを使用します。DHCP クライアントが DHCP サーバに渡すパラメータを削除するには、このコマンドの **no** 形式を使用します。

dhcp-client update dns [**server** {**both** | **none**}]

no dhcp-client update dns [**server** {**both** | **none**}]

シンタックスの説明

both	クライアントは DHCP サーバが DNS A および PTR リソース レコードをアップデートするよう要求します。
none	クライアントは DHCP サーバが DDNS アップデートを実行しないよう要求します。
server	クライアントの要求を受信する DHCP サーバを指定します。

デフォルト

デフォルトでは、セキュリティ アプライアンスは DHCP サーバが PTR RR アップデートのみを実行するように要求します。クライアントはサーバに FQDN オプションを送信しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドはインターフェイス コンフィギュレーション モードでも入力できますが、ハイフンは使用しません。**dhcp client update dns** を参照してください。インターフェイス モードで入力した場合、**dhcp client update dns** コマンドはグローバル コンフィギュレーション モードでこのコマンドで設定した設定値を上書きします。

例

次の例では、DHCP サーバが A RR と PTR RR のどちらもアップデートしないことをクライアントが要求するよう設定します。

```
hostname(config)# dhcp-client update dns server none
```

次の例では、サーバが A RR と PTR RR をアップデートすることをクライアントが要求するよう設定します。

```
hostname(config)# dhcp-client update dns server both
```

関連コマンド

コマンド	説明
ddns（DDNS アップデート方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
dhcp-client update dns	
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcpd address

DHCP サーバで使用される IP アドレス プールを定義するには、グローバル コンフィギュレーション モードで **dhcpd address** コマンドを使用します。既存の DHCP アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

dhcpd address *IP_address1*[*-IP_address2*] *interface_name*

no dhcpd address *interface_name*

シンタックスの説明

interface_name	アドレス プールの割り当て先のインターフェイスです。
IP_address1	DHCP アドレス プールの開始アドレスです。
IP_address2	DHCP アドレス プールの終了アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd address *ip1*[*-ip2*] *interface_name* コマンドは、DHCP サーバのアドレス プールを指定します。セキュリティ アプライアンス DHCP サーバのアドレス プールは、そのプールがイネーブルにされたセキュリティ アプライアンス インターフェイスと同じサブネット内にある必要があり、*interface_name* を使用して関連するセキュリティ アプライアンス インターフェイスを指定する必要があります。

アドレス プールのサイズは、セキュリティ アプライアンスでプールあたり 256 に制限されています。アドレス プールの範囲が 253 アドレスよりも大きい場合、セキュリティ アプライアンス インターフェイスのネットマスクは、クラス C アドレス（たとえば、255.255.255.0）にはできないため、それよりいくらか大きく、たとえば、255.255.254.0 にする必要があります。

DHCP クライアントは、物理的にセキュリティ アプライアンス DHCP サーバ インターフェイスのサブネットに接続されている必要があります。

dhcpd address コマンドでは、「-」（ダッシュ）文字がオブジェクト名の一部ではなく範囲指定子と解釈されるため、「-」文字を含むインターフェイス名は使用できません。

no dhcpd address *interface_name* コマンドは、指定されたインターフェイスに設定されている DHCP サーバ アドレス プールを削除します。

DHCP サーバ機能をセキュリティ アプライアンスに実装する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例は、セキュリティ アプライアンスの **dmz** インターフェイスに DHCP クライアントに対するアドレス プールおよび DNS サーバを設定するため、**dhcpd address** コマンド、**dhcpd dns** コマンド、および **dhcpd enable** *interface_name* コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 209.165.200.226
hostname(config)# dhcpd enable dmz
```

次の例は、内部インターフェイスに DHCP サーバを設定する方法を示しています。その内部インターフェイスの DHCP サーバに IP アドレス 10 個のプールを割り当てるため、**dhcpd address** コマンドを使用します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd enable	指定したインターフェイス上で、DHCP サーバをイネーブルにします。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd auto_config

DHCP または PPPoE クライアントを実行しているインターフェイスから取得した値に基づいて、セキュリティ アプライアンスが DHCP サーバに対して DNS、WINS およびドメイン名を自動的に設定するのをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd auto_config** コマンドを使用します。DHCP パラメータの自動設定を解除するには、このコマンドの **no** 形式を使用します。

dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

no dhcpd auto_config *client_if_name* [[**vpnclient-wins-override**] **interface** *if_name*]

シンタックスの説明

client_if_name	DNS、WINS、およびドメイン名パラメータを提供する DHCP クライアントを実行している、インターフェイスを指定します。
interface *if_name*	アクションが適用されるインターフェイスを指定します。
vpnclient-wins-override	vpnclient パラメータにより、インターフェイス DHCP または PPPoE クライアント WINS パラメータを上書きします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

CLI コマンドを使用して DNS、WINS、またはドメイン名パラメータを指定した場合、自動設定によって取得されたパラメータは、CLI により設定されたパラメータに上書きされます。

例

次の例は、内部インターフェイス上で DHCP を設定する方法を示しています。外部インターフェイス上の DHCP クライアントから取得した DNS、WINS、およびドメイン情報を、内部インターフェイス上の DHCP クライアントに渡すには **dhcpd auto_config** コマンドを使用します。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd autoconfig outside
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd enable	指定したインターフェイス上で、DHCP サーバをイネーブルにします。
show ip address dhcp server	DHCP クライアントとして動作するインターフェイスに DHCP サーバから提供される、DHCP オプションに関する詳細情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd dns

DHCP クライアントに対して DNS サーバを定義するには、グローバル コンフィギュレーション モードで **dhcpd dns** コマンドを使用します。定義されたサーバを消去するには、このコマンドの **no** 形式を使用します。

dhcpd dns *dnsip1* [*dnsip2*] [**interface** *if_name*]

no dhcpd dns [*dnsip1* [*dnsip2*]] [**interface** *if_name*]

シンタックスの説明

dnsip1	DHCP クライアントに対するプライマリ DNS サーバの IP アドレスです。
dnsip2	（オプション）DHCP クライアントの代替 DNS サーバの IP アドレスです。
interface *if_name*	サーバに対して入力した値の適用対象となるインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd dns コマンドは、DHCP クライアントに対する DNS サーバの IP アドレスを指定します。2 つの DNS サーバを指定できます。**no dhcpd dns** コマンドは、コンフィギュレーションから DNS IP アドレスを削除します。

例

次の例は、セキュリティ アプライアンスの **dmz** インターフェイスに DHCP クライアントに対するアドレス プールおよび DNS サーバを設定するため、**dhcpd address** コマンド、**dhcpd dns** コマンド、および **dhcpd enable** *interface_name* コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.100-10.0.1.108 dmz
hostname(config)# dhcpd dns 192.168.1.2
hostname(config)# dhcpd enable dmz
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd address	指定したインターフェイス上で DHCP サーバが使用するアドレス プールを指定します。
dhcpd enable	指定したインターフェイス上で、DHCP サーバをイネーブルにします。
dhcpd wins	DHCP クライアントに対して WINS サーバを定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd domain

DHCP クライアントに対して DNS ドメイン名を定義するには、グローバル コンフィギュレーション モードで **dhcpd domain** コマンドを使用します。DNS ドメイン名を消去するには、このコマンドの **no** 形式を使用します。

dhcpd domain *domain_name* [**interface** *if_name*]

no dhcpd domain [*domain_name*] [**interface** *if_name*]

シンタックスの説明

domain_name	example.com などの DNS ドメイン名。
interface *if_name*	サーバに対して入力した値の適用対象となるインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd domain コマンドは、DHCP クライアントに対する DNS ドメイン名を指定します。**no dhcpd domain** コマンドは、コンフィギュレーションから DNS ドメイン サーバを削除します。

例

次の例は、セキュリティ アプライアンスで DHCP サーバにより DHCP クライアントに提供されるドメイン名を設定するために **dhcpd domain** コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd enable

DHCP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcpd enable** コマンドを使用します。DHCP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。DHCP サーバは、ネットワーク コンフィギュレーション パラメータを DHCP クライアントに提供します。セキュリティ アプライアンス内で DHCP サーバをサポートすることは、セキュリティ アプライアンスが DHCP を使用して、接続されているクライアントを設定できることを意味します。

dhcpd enable *interface*

no dhcpd enable *interface*

シンタックスの説明

interface	DHCP サーバをイネーブルにするインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd enable *interface* コマンドを使用すると、DHCP デーモンが DHCP 対応のインターフェイス上で DHCP クライアントの要求のリッスンを開始します。**no dhcpd enable** コマンドは、指定したインターフェイス上の DHCP サーバ機能をディセーブルにします。

（注） マルチ コンテキスト モードの場合、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP サーバをイネーブルにすることはできません。

セキュリティ アプライアンスが DHCP クライアント要求に応答する場合、要求を受信したインターフェイスの IP アドレスとサブネット マスクを、デフォルト ゲートウェイの IP アドレスとサブネット マスクとして応答で使用します。

（注） セキュリティ アプライアンス DHCP サーバ デーモンは、直接セキュリティ アプライアンス インターフェイスに接続されていないクライアントはサポートしません。

DHCP サーバ機能をセキュリティ アプライアンスに実装する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例は、DHCP サーバを内部インターフェイス上でイネーブルにするために **dhcpd enable** コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
debug dhcpd	DHCP サーバに対するデバッグ情報を表示します。
dhcpd address	指定したインターフェイス上で DHCP サーバが使用するアドレス プールを指定します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd lease

DHCP リース期間を指定するには、グローバル コンフィギュレーション モードで **dhcpd lease** コマンドを使用します。リースのデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dhcpd lease *lease_length* [**interface** *if_name*]

no dhcpd lease [*lease_length*] [**interface** *if_name*]

シンタックスの説明

interface *if_name*	サーバに対して入力した値の適用対象となるインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
lease_length	DHCP サーバから DHCP クライアントに与えられる、秒単位の、IP アドレスのリース期間です。有効値は 300 ～ 1,048,575 秒です。

デフォルト

デフォルトの *lease_length* は 3,600 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd lease コマンドは、DHCP クライアントに与えるリース期間を秒単位で指定します。このリース期間は、DHCP サーバが割り当てた IP アドレスを DHCP クライアントが使用できる期間を示します。

no dhcpd lease コマンドは、コンフィギュレーションから指定したリース長を削除して、この値をデフォルト値の 3,600 秒に置き換えます。

例

次の例は、DHCP クライアントに対する DHCP 情報のリース期間を指定するために **dhcpd lease** コマンドを使用する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd option

DHCP オプションを設定するには、グローバル コンフィギュレーション モードで **dhcpd option** コマンドを使用します。オプションを消去するには、このコマンドの **no** 形式を使用します。**dhcpd option** コマンドを使用して、TFTP サーバ情報を Cisco IP Phone およびルータに提供することができます。

dhcpd option *code* {***ascii*** *string*} | {***ip*** *IP_address* [*IP_address*]} | {***hex*** *hex_string*} [**interface** *if_name*]

no dhcpd option *code* [**interface** *if_name*]

シンタックスの説明

ascii	オプション パラメータが ASCII 文字列であることを指定します。
code	設定された DHCP オプションの番号を表します。有効値は 0 ～ 255 で、いくつかの例外があります。サポートしていない DHCP オプション コードのリストについては、下の「使用上のガイドライン」の項を参照してください。
hex	オプション パラメータが 16 進文字列であることを指定します。
hex_string	16 進文字列を、スペースのない偶数桁で指定します。0x プレフィックスを使用する必要はありません。
interface *if_name*	サーバに対して入力した値の適用対象となるインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
ip	オプション パラメータが IP アドレスであることを指定します。最大 2 つの IP アドレスを ***ip*** キーワードに指定できます。
IP_address	10 進数の IP アドレスを指定します。
string	スペースなしの ASCII 文字列を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

DHCP オプション要求がセキュリティ アプライアンス DHCP サーバに到着すると、セキュリティ アプライアンスは **dhcpd option** コマンドで指定された値を、クライアントに対する応答に入れます。

dhcpd option 66 コマンドおよび **dhcpd option 150** コマンドは、Cisco IP Phone およびルータがコンフィギュレーション ファイルをダウンロードするときに使用する TFTP サーバを指定します。次のようにコマンドを使用します。

- **dhcpd option 66 ascii** *string*。ここで、*string* は TFTP サーバの IP アドレスまたはホスト名です。オプション 66 には、TFTP サーバを 1 つだけ指定できます。
- **dhcpd option 150 ip** *IP_address* [*IP_address*]。ここで、*IP_address* は TFTP サーバの IP アドレスです。オプション 150 には、最大 2 つの IP アドレスを指定できます。

(注)　**dhcpd option 66** コマンドは ***ascii*** パラメータのみ受け付け、**dhcpd option 150** コマンドは ***ip*** パラメータのみ受け付けます。

dhcpd option 66 | 150 コマンドに IP アドレスを指定するときには、次のガイドラインに従ってください。

- TFTP サーバが DHCP サーバ インターフェイス上にある場合、TFTP サーバのローカル IP アドレスを使用します。
- TFTP サーバが DHCP サーバ インターフェイスよりもセキュリティが低いインターフェイス上にある場合は、一般の発信規則が適用されます。DHCP クライアント用の NAT エントリ、グローバル エントリ、および **access-list** エントリを作成し、TFTP サーバの実際の IP アドレスを使用します。
- TFTP サーバがよりセキュリティの高いインターフェイス上にある場合は、一般の受信規則が適用されます。TFTP サーバ用のスタティック文と **access-list** 文のグループを作成し、TFTP サーバのグローバル IP アドレスを使用します。

その他の DHCP オプションの詳細については、RFC2132 を参照してください。

(注)　セキュリティ アプライアンスは、与えられたオプション タイプおよび値が RFC 2132 に定義されているオプション コードの想定タイプおよび想定値と一致していることを確認しません。たとえば、**dhcpd option 46 ascii hello** と入力した場合、セキュリティ アプライアンスはその設定を受け入れますが、option 46 は 1 桁の 16 進値として RFC 2132 に定義されます。

dhcpd option コマンドで次の DHCP オプションは設定できません。

オプション コード	説明
0	DHCPOPT_PAD
1	HCPOPT_SUBNET_MASK
12	DHCPOPT_HOST_NAME
50	DHCPOPT_REQUESTED_ADDRESS
51	DHCPOPT_LEASE_TIME
52	DHCPOPT_OPTION_OVERLOAD
53	DHCPOPT_MESSAGE_TYPE
54	DHCPOPT_SERVER_IDENTIFIER
58	DHCPOPT_RENEWAL_TIME
59	DHCPOPT_REBINDING_TIME
61	DHCPOPT_CLIENT_IDENTIFIER
67	DHCPOPT_BOOT_FILE_NAME
82	DHCPOPT_RELAY_INFORMATION
255	DHCPOPT_END

例

次の例は、DHCP オプション 66 に TFTP サーバを指定する方法を示しています。

```
hostname(config)# dhcpd option 66 ascii MyTftpServer
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd ping_timeout

DHCP PING のデフォルト タイムアウトを変更するには、グローバル コンフィギュレーション モードで **dhcpd ping_timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。アドレスの競合を避けるため、DHCP サーバは、アドレスを DHCP クライアントに割り当てる前に 2 つの ICMP PING パケットをアドレスに送信します。このコマンドは、PING タイムアウトをミリ秒で指定します。

dhcpd ping_timeout *number* [**interface** *if_name*]

no dhcpd ping_timeout [**interface** *if_name*]

シンタックスの説明

interface *if_name*	サーバに対して入力した値の適用対象となるインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
number	ミリ秒単位の PING タイムアウト値です。最小値は 10、最大値は 10,000 です。デフォルトは 50 です。

デフォルト

number のデフォルトのミリ秒は 50 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスは、DHCP クライアントに IP アドレスを割り当てる前に、両方の ICMP PING パケットがタイムアウトになるのを待ちます。たとえば、デフォルト値が使用された場合、セキュリティ アプライアンスは IP アドレスを割り当てる前に、1,500 ミリ秒（各 ICMP PING パケットに対して 750 ミリ秒）待ちます。

PING のタイムアウト値が長いと、DHCP サーバのパフォーマンスに悪影響を及ぼす場合があります。

例

次の例は、**dhcpd ping_timeout** コマンドを使用して、DHCP サーバの PING タイムアウト値を変更する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcpd update dns

DHCP サーバによるダイナミック DNS アップデートを実行するには、グローバル コンフィギュレーション モードで **dhcpd update dns** コマンドを使用します。DHCP サーバによる DDNS をディセーブルにするには、このコマンドの **no** 形式を使用します。

dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

no dhcpd update dns [**both**] [**override**] [**interface** *srv_ifc_name*]

シンタックスの説明

both	DHCP サーバが A と PTR の両方の DNS リソース レコード（RR）をアップデートするように指定します。
interface	DDNS アップデートが適用されるセキュリティ アプライアンス インターフェイスを指定します。
override	DHCP サーバが DHCP クライアント要求を上書きするように指定します。
srv_ifc_name	このオプションを適用するインターフェイスを指定します。

デフォルト

デフォルトでは、DHCP サーバは PTR RR アップデートのみを実行します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ダイナミック DNS（DDNS）は、DNS で管理されている名前からアドレスへのマッピング、およびアドレスから名前へのマッピングをアップデートするものです。アップデートは DHCP サーバと連携して実行されます。**dhcpd update dns** コマンドはサーバによるアップデートをイネーブルにします。

名前とアドレスのマッピングは、次の 2 タイプのリソース レコード（RR）に保持されます。

- A リソース レコードは、ドメイン名から IP アドレスへのマッピングを保持します。
- PTR リソース レコードは、IP アドレスからドメイン名へのマッピングを保持します。

DDNS アップデートを使用すると、A タイプの RR に保持される情報と、PTR タイプの RR に保持される情報との一貫性を維持できます。

dhcpd update dns コマンドを使用すると、DHCP サーバが A RR と PRT RR の両方アップデート、または PTR RR アップデートのみを実行するように設定できます。DHCP クライアントからのアップデート要求を上書きするように設定することもできます。

例

次の例では、DDNS サーバが DHCP クライアントからの要求を上書きすると同時に、A と PTR の両方のアップデートを実行するよう設定します。

```
hostname(config)# dhcpd update dns both override
```

関連コマンド

コマンド	説明
ddns（DDNS アップデート方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
interval maximum	DDNS アップデート方式によるアップデート試行の最大間隔を設定します。

dhcpd wins

DHCP クライアント用の WINS サーバを定義するには、グローバル コンフィギュレーション モードで **dhcpd wins** コマンドを使用します。DHCP サーバから WINS サーバを削除するには、このコマンドの **no** 形式を使用します。

dhcpd wins *server1* [*server2*] [**interface** *if_name*]

no dhcpd wins [*server1* [*server2*]] [**interface** *if_name*]

シンタックスの説明

interface *if_name*	サーバに対して入力した値の適用対象となるインターフェイスを指定します。インターフェイスを指定しない場合、値はすべてのサーバに適用されます。
server1	プライマリの Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。
server2	（オプション）代替の Microsoft NetBIOS ネーム サーバ（WINS サーバ）の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcpd wins コマンドは、DHCP クライアント用の WINS サーバのアドレスを指定します。**no dhcpd wins** コマンドは、コンフィギュレーションから WINS サーバの IP アドレスを削除します。

例

次の例は、dhcpd wins コマンドを使用して、DHCP クライアントに送信された WINS サーバ情報を指定する方法を示しています。

```
hostname(config)# dhcpd address 10.0.1.101-10.0.1.110 inside
hostname(config)# dhcpd dns 198.162.1.2 198.162.1.3
hostname(config)# dhcpd wins 198.162.1.4
hostname(config)# dhcpd lease 3000
hostname(config)# dhcpd ping_timeout 1000
hostname(config)# dhcpd domain example.com
hostname(config)# dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
dhcpd address	指定したインターフェイス上で DHCP サーバが使用するアドレス プールを指定します。
dhcpd dns	DHCP クライアントに対して DNS サーバを定義します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

dhcprelay enable

DHCP リレー エージェントをイネーブルにするには、グローバル コンフィギュレーション モードで **dhcprelay enable** コマンドを使用します。DHCP リレー エージェントをディセーブルにするには、このコマンドの **no** 形式を使用します。DHCP リレー エージェントを使用すると、指定したセキュリティ アプライアンス インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

dhcprelay enable *interface_name*

no dhcprelay enable *interface_name*

シンタックスの説明

interface_name	DHCP リレー エージェントがクライアント要求を受け入れるインターフェイス名です。

デフォルト

DHCP リレー エージェントはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcprelay enable *interface_name* コマンドによってセキュリティ アプライアンスが DHCP リレー エージェントを開始するようにするには、**dhcprelay server** コマンドがコンフィギュレーションにすでに存在している必要があります。そのコマンドがなければ、セキュリティ アプライアンスは次に示すようなエラー メッセージを表示します。

```
DHCPRA: Warning - There are no DHCP servers configured!
        No relaying can be done without a server!
        Use the 'dhcprelay server <server_ip> <server_interface>' command
```

次の条件下では、DHCP リレーをイネーブルにできません。

- 同じインターフェイス上で DHCP リレーと DHCP リレー サーバをイネーブルにすることはできません。
- 同じインターフェイス上で DHCP リレーと DHCP サーバ（**dhcpd enable**）をイネーブルにすることはできません。
- 1 つのコンテキストの DHCP リレーを、DHCP サーバと同時にイネーブルにすることはできません。
- マルチ コンテキスト モードの場合、複数のコンテキストにより使用されているインターフェイス（共有 VLAN）で DHCP リレーをイネーブルにすることはできません。

no dhcprelay enable *interface_name* コマンドは、*interface_name* で指定されたインターフェイスの DHCP リレー エージェント コンフィギュレーションだけを削除します。

例

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイス上に設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイス上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

次の例は、DHCP リレー エージェントをディセーブルにする方法を示しています。

```
hostname(config)# no dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
debug dhcp relay	DHCP リレー エージェントに関するデバッグ情報を表示します。
dhcprelay server	DHCP リレー エージェントが、DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが、DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

dhcprelay server

DHCP 要求が転送される DHCP サーバを指定するには、グローバル コンフィギュレーション モードで **dhcpreplay server** コマンドを使用します。DHCP リレー コンフィギュレーションから DHCP サーバを削除するには、このコマンドの **no** 形式を使用します。DHCP リレー エージェントを使用すると、指定したセキュリティ アプライアンス インターフェイスから指定した DHCP サーバに DHCP 要求を転送できます。

dhcprelay server *IP_address interface_name*

no dhcprelay server *IP_address* [*interface_name*]

シンタックスの説明

interface_name	DHCP サーバが常駐するセキュリティ アプライアンス インターフェイス名です。
IP_address	DHCP リレー エージェントがクライアント DHCP 要求を転送する DHCP サーバの IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

インターフェイスあたり最大 4 つの DHCP リレー サーバを追加できます。**dhcprelay enable** コマンドを入力する前に、少なくとも 1 つの **dhcprelay server** コマンドをセキュリティ アプライアンス コンフィギュレーションに追加する必要があります。DHCP リレー サーバが設定されているインターフェイス上に、DHCP クライアントを設定することはできません。

dhcprelay server コマンドは、指定したインターフェイス上で UDP ポート 67 を開き、**dhcprelay enable** コマンドがコンフィギュレーションに追加されるとすぐに DHCP リレー タスクを開始します。

no dhcprelay server *IP_address* [*interface_name*] コマンドを使用すると、インターフェイスは DHCP パケットのそのサーバへの転送を停止します。

no dhcprelay server *IP_address* [*interface_name*] コマンドを使用すると、*IP_address* [*interface_name*] で指定された DHCP サーバ用の DHCP リレー エージェント コンフィギュレーションだけが削除されます。

例

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイス上に設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイス上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイス上で、DHCP リレー エージェントをイネーブルにします。
dhcprelay setroute	DHCP リレー エージェントが、DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

dhcprelay setroute

DHCP 応答にデフォルト ゲートウェイ アドレスを設定するには、グローバル コンフィギュレーション モードで **dhcprelay setroute** コマンドを使用します。デフォルト ルータを削除するには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、DHCP 応答のデフォルト IP アドレスは、指定されたセキュリティ アプライアンス インターフェイスのアドレスに置き換えられます。

dhcprelay setroute *interface*

no dhcprelay setroute *interface*

シンタックスの説明

interface	最初のデフォルト IP アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように DHCP リレー エージェントを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcprelay setroute *interface* コマンドを使用すると、DHCP リレー エージェントが最初のデフォルト ルータ アドレス（DHCP サーバから送信されるパケット内にある）を *interface* のアドレスに変更するように設定できます。

パケット内にデフォルトのルータ オプションがなければ、セキュリティ アプライアンスは、*interface* アドレスを含んでいるデフォルト ルータを追加します。その結果、クライアントは自分のデフォルト ルートがセキュリティ アプライアンスに向かうように設定できます。

dhcprelay setroute *interface* コマンドを設定しない場合（かつパケット内にデフォルトのルータ オプションがある場合）、パケットは、ルータ アドレスが変更されないままセキュリティ アプライアンスを通過します。

例

次の例は、**dhcprelay setroute** コマンドを使用して、DHCP 応答のデフォルト ゲートウェイを外部 DHCP サーバからセキュリティ アプライアンスの内部インターフェイスに設定する方法を示しています。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay setroute inside
hostname(config)# dhcprelay enable inside
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイス上で、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが、DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay timeout	DHCP リレー エージェントのタイムアウト値を指定します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

dhcprelay timeout

DHCP リレー エージェントのタイムアウト値を設定するには、グローバル コンフィギュレーション モードで **dhcprelay timeout** コマンドを使用します。タイムアウト値をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

dhcprelay timeout *seconds*

no dhcprelay timeout

シンタックスの説明

seconds	DHCP リレー アドレス ネゴシエーション用に許可されている時間（秒）を指定します。

デフォルト

dhcprelay タイムアウトのデフォルト値は 60 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

dhcprelay timeout コマンドは、DHCP サーバからの応答がリレー バインディング構造を通して DHCP クライアントに進むことが許されている時間を秒単位で設定します。

例

次の例は、10.1.1.1 という IP アドレスを持つ DHCP サーバ用の DHCP リレー エージェントをセキュリティ アプライアンスの外部インターフェイス上に設定し、クライアント要求をセキュリティ アプライアンスの内部インターフェイス上に設定して、さらにタイムアウト値を 90 秒に設定する方法を示しています。

```
hostname(config)# dhcprelay server 10.1.1.1 outside
hostname(config)# dhcprelay timeout 90
hostname(config)# dhcprelay enable inside
hostname(config)# show running-config dhcprelay
dhcprelay server 10.1.1.1 outside
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
dhcprelay enable	指定したインターフェイス上で、DHCP リレー エージェントをイネーブルにします。
dhcprelay server	DHCP リレー エージェントが、DHCP 要求の転送先にする DHCP サーバを指定します。
dhcprelay setroute	DHCP リレー エージェントが、DHCP 応答でデフォルト ルータ アドレスとして使用する IP アドレスを定義します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

dialog

WebVPN ユーザに表示するダイアログ メッセージをカスタマイズするには、webvpn カスタマイゼーション モードで **dialog** コマンドを使用します。

dialog {**title** | **message** | **border**} **style** *value*

[**no**] **dialog** {**title** | **message** | **border**} **style** *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

title	タイトルを変更することを指定します。
message	メッセージを変更することを指定します。
border	境界を変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのスタイルは background-color:#669999;color:white です。

デフォルトのメッセージのスタイルは background-color:#99CCCC;color:black です。

デフォルトの境界線のスタイルは border:1px solid black;border-collapse:collapse です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、ダイアログ メッセージの文字表示色を青色に変更するようにカスタマイズしています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# dialog message style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの Application Access ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの Browse Networks ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの Web Bookmarks タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの File Bookmarks タイトルまたはリンクをカスタマイズします。

dir

ディレクトリの内容を表示するには、特権 EXEC モードで **dir** コマンドを使用します。

dir ***[/all]*** [***all-filesystems***] [**/recursive**] [**flash:** | **system:**] [*path]*

シンタックスの説明

/all	（オプション）すべてのファイルを表示します。
all-filesystems	（オプション）すべてのファイル システムのファイルを表示します。
/recursive	（オプション）ディレクトリの内容を再帰的に表示します。
system:	（オプション）ファイル システムのディレクトリの内容を表示します。
flash:	（オプション）デフォルト フラッシュ パーティションのディレクトリの内容を表示します。
path	（オプション）特定のパスを指定します。

デフォルト

ディレクトリを指定しない場合のデフォルトのディレクトリは、現在の作業ディレクトリです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

キーワードまたは引数のない **dir** コマンドは、現在のディレクトリの内容を表示します。

例

次の例は、ディレクトリの内容を表示する方法を示しています。

```
hostname# dir
Directory of disk0:/

1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

次の例は、ファイル システム全体の内容を再帰的に表示する方法を示しています。

```
hostname# dir /recursive disk0:
Directory of disk0:/*
1      -rw-  1519        10:03:50 Jul 14 2003    my_context.cfg
2      -rw-  1516        10:04:02 Jul 14 2003    my_context.cfg
3      -rw-  1516        10:01:34 Jul 14 2003    admin.cfg
60985344 bytes total (60973056 bytes free)
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに移動します。
pwd	現在の作業ディレクトリを表示します。
mkdir	ディレクトリを作成します。
rmdir	ディレクトリを削除します。

disable

特権 EXEC モードを終了してユーザ EXEC モードに戻るには、特権 EXEC モードで **disable** コマンドを使用します。

disable

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**enable** コマンドを使用して、特権モードに入ります。**disable** コマンドは、特権モードを終了して、ユーザ モードに戻ります。

例　次の例は、特権モードに入る方法を示しています。

```
hostname> enable
hostname#
```

次の例は、特権モードを終了する方法を示しています。

```
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
enable	特権 EXEC モードをイネーブルにします。

disable（キャッシュ）

WebVPN に対するキャッシングをディセーブルにするには、キャッシュ モードで **disable** コマンドを使用します。キャッシングを再度イネーブルにするには、このコマンドの **no** 形式を使用します。

disable

no disable

デフォルト

キャッシングは、各キャッシュ アトリビュートに対するデフォルトの設定でイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシングは頻繁に再利用されるオブジェクトをシステム キャッシュに保存します。キャッシュに保存しておくことにより、リライトやコンテンツの圧縮を繰り返し実行する必要が少なくなります。WebVPN とリモート サーバの間および WebVPN とエンドユーザのブラウザとの間の両方でトラフィックを削減します。その結果、多くのアプリケーションがさらに効率よく実行されます。

例

次の例は、キャッシングをディセーブルにする方法と、それを再度イネーブルにする方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# disable
hostname(config-webvpn-cache)# no disable
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

distance ospf

ルート タイプに基づいて OSPF ルートの管理ディスタンスを定義するには、ルータ コンフィギュレーション モードで **distance ospf** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

distance ospf [***intra-area*** *d1*] [***inter-area*** *d2*] [***external*** *d3*]

no distance ospf

シンタックスの説明

d1、*d2*、*d3*	各ルート タイプの距離です。有効な値は 1 ～ 255 です。
external	（オプション）再配布によって取得した他のルーティング ドメインからのルートに距離を設定します。
inter-area	（オプション）あるエリアから別のエリアまでのルートすべての距離を設定します。
intra-area	（オプション）あるエリア内のすべてのルートの距離を設定します。

デフォルト

d1、*d2*、および *d3* のデフォルト値は 110 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

少なくとも 1 つのキーワードと引数を指定する必要があります。管理ディスタンスのタイプごとにコマンドを個別に入力することができますが、コンフィギュレーションでは 1 つのコマンドとして表示されます。管理ディスタンスを再入力する場合、対象ルート タイプの管理ディスタンスだけが変更されます。その他のルート タイプの管理ディスタンスは影響されません。

コマンドの **no** 形式には、キーワードも引数もありません。コマンドの **no** 形式を使用すると、すべてのルート タイプの管理ディスタンスがデフォルトに戻されます。複数のルート タイプを設定している場合、1 つのルートタイプをデフォルトの管理ディスタンスに戻すには、次のいずれかを実行します。

- ルート タイプを、手動でデフォルト値に設定します。
- コマンドの **no** 形式を使用してコンフィギュレーション全体を削除してから、保持するルート タイプのコンフィギュレーションを再入力します。

例

次の例では、外部ルートの管理ディスタンスを 150 に設定します。

```
hostname(config-router)# distance ospf external 105
hostname(config-router)#
```

次の例は、各ルート タイプに入力した個別のコマンドが、ルータ コンフィギュレーションで 1 つのコマンドとして表示される方法を示しています。

```
hostname(config-router)# distance ospf intra-area 105 inter-area 105
hostname(config-router)# distance ospf intra-area 105
hostname(config-router)# distance ospf external 105
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 105
!
hostname(config)#
```

次の例は、各管理ディスタンスを 105 に設定し、次に外部管理ディスタンスだけを 150 に変更する方法を示しています。**show running-config router ospf** コマンドは、外部ルート タイプの値だけが変更され、その他のルート タイプでは以前に設定された値が保持されている状況を示します。

```
hostname(config-router)# distance ospf external 105 intra-area 105 inter-area 105
hostname(config-router)# distance ospf external 150
hostname(config-router)# exit
hostname(config)# show running-config router ospf 1
!
router ospf 1
 distance ospf intra-area 105 inter-area 105 external 150
!
hostname(config)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

distribute-list in

アップデートを受信したネットワークをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list in** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式を使用します。

distribute-list *acl* ***in*** [***interface*** *if_name*]

no distribute-list *acl* ***in*** [***interface if_name***]

シンタックスの説明

acl	標準アクセス リストの名前。
if_name	（オプション）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイスを指定すると、そのインターフェイス上で受信されたルーティング アップデートだけにアクセス リストが適用されます。

デフォルト

着信アップデートの場合、ネットワークはフィルタリングされません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスが指定されていない場合、アクセス リストはすべての着信アップデートに適用されます。

例

次の例では、外部インターフェイスのルーティング アップデートのフィルタリングを制限します。10.0.0.0 ネットワークのルートを受け入れ、他はすべて拒否します。

```
hostname(config)# access-list ripfilter permit 10.0.0.0
hostname(config)# access-list ripfilter deny any
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter in interface outside
```

関連コマンド

コマンド	説明
distribute-list out	RIP アップデートでアドバタイズされるネットワークをフィルタリングします。
router rip	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

distribute-list out

RIP アップデートで特定のネットワークが送信されるのをフィルタリングするには、ルータ コンフィギュレーション モードで **distribute-list out** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式を使用します。

distribute-list *acl* ***out*** [***interface*** *if_name* | ***rip*** | ***ospf*** *pid* | ***static*** | ***connected***]

no distribute-list *acl* ***out*** [***interface if_name***]

シンタックスの説明

acl	標準アクセス リストの名前。
connected	（オプション）接続されたルートのみフィルタリングします。
interface *if_name*	（オプション）**nameif** コマンドで指定されたインターフェイスの名前。インターフェイスを指定すると、アクセス リストは指定されたインターフェイスに送信されたルーティング アップデートのみに適用されます。
ospf *pid*	（オプション）指定した OSPF プロセスにより検出された OSPF ルートのみフィルタリングします。
rip	（オプション）RIP ルートのみフィルタリングします。
static	（オプション）スタティック ルートのみフィルタリングします。

デフォルト

送信アップデートの場合、ネットワークはフィルタリングされません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスが指定されない場合、アクセス リストはすべての送信アップデートに適用されます。

例

次の例では、任意のインターフェイスから送信された RIP アップデートで 10.0.0.0 ネットワークがアドバタイズされないようにします。

```
hostname(config)# access-list ripfilter deny 10.0.0.0
hostname(config)# access-list ripfilter permit any
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# distribute-list ripfilter out
```

関連コマンド

コマンド	説明
distribute-list in	RIP アップデートで受信されるネットワークをフィルタリングします。
router rip	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

dns domain-lookup

サポートされているコマンドに対してネーム ルックアップを実行するために、セキュリティ アプライアンスが DNS サーバに DNS 要求を送信することをイネーブルにするには、グローバル コンフィギュレーション モードで **dns domain-lookup** コマンドを使用します。DNS lookup をディセーブルにするには、このコマンドの **no** 形式を使用します。

dns domain-lookup *interface_name*

no dns domain-lookup *interface_name*

シンタックスの説明

interface_name	DNS lookup をイネーブルにするインターフェイスを指定します。このコマンドを複数回入力して、DNS lookup を複数のインターフェイス上でイネーブルにする場合、セキュリティ アプライアンスは応答を受信するまで各インターフェイスを順番に試します。

デフォルト

デフォルトでは、DNS lookup はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

DNS 要求の送信先の DNS サーバ アドレスを設定するには、**dns name-server** コマンドを使用します。DNS lookup をサポートするコマンドのリストについては、**dns name-server** コマンドを参照してください。

セキュリティ アプライアンスは、ダイナミックにラーニングされたエントリで構成される名前解決のキャッシュを管理します。セキュリティ アプライアンスは、ホスト名から IP アドレスへの変換が必要になるたびに外部 DNS サーバにクエリーする代わりに、外部 DNS 要求から返された情報をキャッシュします。セキュリティ アプライアンスは、キャッシュにない名前に対してのみ要求を実行します。キャッシュのエントリは、DNS レコードの期限切れ、または 72 時間後のいずれか早い方に自動的にタイムアウトします。

例

次の例では、内部インターフェイス上で DNS lookup をイネーブルにします。

```
hostname(config)# dns domain-lookup inside
```

関連コマンド

コマンド	説明
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns-group（トンネル グループ webvpn コンフィギュレーション モード）

WebVPN トンネル グループに使用する DNS サーバを指定するには、トンネル グループ WebVPN コンフィギュレーション モードで **dns-group** コマンドを使用します。デフォルトの DNS グループを復元するには、このコマンドの **no** 形式を使用します。

dns-group *name*

no dns-group

シンタックスの説明

name	トンネル グループに使用する DNS サーバ グループ コンフィギュレーションの名前を指定します。

デフォルト

デフォルト値は DefaultDNS です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ WebVPN アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

名前には任意の DNS グループを指定できます。dns-group コマンドはホスト名をトンネル グループの適切な DNS サーバに解決します。

dns server-group コマンドを使用して DNS グループを設定します。

例

次の例は、「dnsgroup1」という名前の DNS グループの使用を指定するカスタマイゼーション コマンドを示しています。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# dns-group dnsgroup1
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードに入ります。
show running-config dns-server group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

dns-guard

クエリーごとに 1 つの DNS 応答を実行する DNS Guard 機能をイネーブルにするには、パラメータ コンフィギュレーション モードで **dns-guard** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

dns-guard

no dns-guard

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

DNS Guard はデフォルトでイネーブルです。このコマンドは、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定している場合はイネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションで **no dns-guard** を明示的に指定する必要があります。**inspect dns** が設定されていない場合、動作は **global dns-guard** コマンドにより指定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

DNS ヘッダーのインデックス フィールドを使用して、DNS 応答と DNS ヘッダーを一致させます。クエリーごとに 1 つの応答がセキュリティ アプライアンスを介して許可されます。

例

次の例では、DNS 検査ポリシー マップで DNS Guard をイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# dns-guard
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

dns name-server

1 つまたは複数の DNS サーバを指定するには、グローバル コンフィギュレーション モードで **dns name-server** コマンドを使用します。サーバを削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、WebVPN コンフィギュレーションまたは証明書コンフィギュレーションのサーバ名を解決するために DNS を使用します（サポートされるコマンドのリストについては、「使用上のガイドライン」を参照してください）。サーバ名を定義するその他の機能は（AAA など）、DNS 解決をサポートしていません。IP アドレスを入力するか、**name** コマンドを使用して手動により名前を IP アドレスに解決する必要があります。

dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

no dns name-server *ip_address* [*ip_address2*] [...] [*ip_address6*]

シンタックスの説明

ip_address	DNS サーバの IP アドレスを指定します。最大 6 個のアドレスを個別のコマンドとして指定するか、利便性のために、1 つのコマンド内で 6 つまでのアドレスをスペースで分けて指定できます。1 つのコマンドに複数のサーバを入力する場合、セキュリティ アプライアンスは、各サーバをコンフィギュレーションの個別のコマンドに保存します。セキュリティ アプライアンスは、応答を受信するまで各 DNS サーバを順番に試します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは廃止されました。DNS サーバ グループ コンフィギュレーション モードの **name-server** コマンドで置き換えられています。

使用上のガイドライン

DNS lookup をイネーブルにするには、DNS サーバ グループ コンフィギュレーション モードで **domain-name** コマンドを設定します。DNS lookup をイネーブルにしない場合、DNS サーバは使用されません。

DNS 解決をサポートする WebVPN コマンドには、次のコマンドが含まれます。

- **server (pop3s)**
- **server (imap4s)**
- **server (smtps)**
- **port-forward**
- **url-list**

DNS 解決をサポートする certificate コマンドには、次のコマンドが含まれます。

- **enrollment url**
- url

name コマンドを使用すると、名前と IP アドレスを手動で入力できます。

セキュリティ アプライアンスが一連の DNS サーバを再試行する回数を設定するには、**retries** コマンドを参照してください。

例

次の例では、3 つの DNS サーバを追加します。

```
hostname(config)# dns name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

セキュリティ アプライアンスは、次のようにコンフィギュレーションを個別のコマンドとして保存します。

```
dns name-server 10.1.1.1
dns name-server 10.2.3.4
dns name-server 192.168.5.5
```

2 つのサーバを追加するには、それらを 1 つのコマンドとして入力できます。

```
hostname(config)# dns name-server 10.5.1.1 10.8.3.8
hostname(config)# show running-config dns
dns name-server 10.1.1.1
dns name-server 10.2.3.4
dns name-server 192.168.5.5
dns name-server 10.5.1.1
dns name-server 10.8.3.8
...
```

それらを 2 つのコマンドとして入力することもできます。

```
hostname(config)# dns name-server 10.5.1.1
hostname(config)# dns name-server 10.8.3.8
```

複数のサーバを削除するには、それらのサーバを、次のように複数のコマンドとして、または 1 つのコマンドとして入力できます。

```
hostname(config)# no dns name-server 10.5.1.1 10.8.3.8
```

関連コマンド

コマンド	説明
domain-name（DNS サーバ グループ コンフィギュレーション モード）	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
name-server（DNS サーバ グループ コンフィギュレーション モード）	dns name-server コマンドの代わりに使用します。1 つ以上の DNS ネーム サーバを識別します。
retries（DNS サーバ グループ コンフィギュレーション モード）	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
timeout（DNS サーバ グループ コンフィギュレーション モード）	次の DNS サーバを試すまでに待つ時間を指定します。

dns retries

セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

dns retries *number*

no dns retries [*number*]

シンタックスの説明

number	再試行の回数を 0 ～ 10 の間で指定します。デフォルトは 2 です。

デフォルト

デフォルトでは、再試行の回数は 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、WebVPN 接続に対して廃止されました。

使用上のガイドライン

dns name-server コマンドを使用して DNS サーバを追加します。

例

次の例では、再試行の回数を 0 に設定します。セキュリティ アプライアンスは各サーバを 1 回ずつ試します。

```
hostname(config)# dns retries 0
hostname(config)#
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

dns-server

プライマリおよびセカンダリの DNS サーバの IP アドレスを設定するには、グループ ポリシー モードで **dns-server** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、DNS サーバを別のグループ ポリシーから継承できます。サーバを継承しないようにするには、**dns-server none** コマンドを使用します。

dns-server {**value** *ip_address* [*ip_address*] | none}

no dns-server

シンタックスの説明

none	dns サーバに、ヌル値を設定して DNS サーバを許可しません。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ DNS サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

dns-server コマンドを実行するたびに、既存の設定が上書きされます。たとえば、DNS サーバ x.x.x.x を設定し、次に DNS サーバ y.y.y.y を設定した場合、2 番目のコマンドは最初のコマンドを上書きし、y.y.y.y が唯一の DNS サーバになります。サーバを複数設定する場合も同様です。以前に設定された DNS サーバを上書きする代わりにサーバを追加するには、このコマンドを入力するときにすべての DNS サーバの IP アドレスを含めます。

例

次の例は、FirstGroup という名前のグループ ポリシーで、IP アドレスが 10.10.10.15、10.10.10.30、および 10.10.10.45 の DNS サーバを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# dns-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

dns server-group

トンネル グループに使用する DNS サーバのドメイン名、ネームサーバ、リトライ回数、タイムアウトの値を指定できる dns server-group モードに入るには、グローバル コンフィギュレーション モードで **dns server-group** コマンドを使用します。特定の DNS サーバ グループを削除するには、このコマンドの **no** 形式を使用します。

dns server -group *name*

no dns server-group

シンタックスの説明

name	トンネル グループに使用する DNS サーバ グループ コンフィギュレーションの名前を指定します。

デフォルト

デフォルト値は DefaultDNS です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

名前には任意の DNS グループを指定できます。**dns server-group** コマンドを使用して DNS グループを設定します。

例

次の例では、「eval」という名前の DNS サーバ グループを設定します。

```
hostname(config)# dns server-group eval
hostname(config-dns-server-group)# domain-name cisco.com
hostname(config-dns-server-group)# name-server 192.168.10.10
hostname(config-dns-server-group)# retries 5
hostname(config-dns-server-group)# timeout 7
hostname(config-dns-server-group)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
show running-config dns server-group	現在の実行 DNS サーバ グループ コンフィギュレーションを表示します。

dns timeout

次の DNS サーバを試すまで待機する時間を指定するには、グローバル コンフィギュレーション モードで **dns timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

dns timeout *seconds*

no dns timeout [*seconds*]

シンタックスの説明

seconds	タイムアウトを 1 ～ 30 の間の秒単位で指定します。デフォルトは 2 秒です。セキュリティ アプライアンスが一連のサーバを試すたびに、このタイムアウトは倍増します。試行回数を設定するには、**dns retries** コマンドを参照してください。

デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、タイムアウトを 1 秒に設定します。

```
hostname(config)# dns timeout 1
```

関連コマンド

コマンド	説明
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
domain-name	デフォルトのドメイン名を設定します。
show dns-hosts	DNS キャッシュを表示します。

domain-name

デフォルトのドメイン名を設定するには、グローバル コンフィギュレーション モードで **domain-name** コマンドを使用します。ドメイン名を削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、修飾子を持たない名前の拡張子として、ドメイン名を付加します。たとえば、ドメイン名を「example.com」と設定し、syslog サーバを、修飾子を持たない「jupiter」という名前で指定した場合、名前は、セキュリティ　　アプライアンスにより「jupiter.example.com.」と修飾されます。

domain-name *name*

no domain-name [*name*]

シンタックスの説明

name	ドメイン名を設定します。最大長は 63 文字です。

デフォルト

デフォルト ドメイン名は、default.domain.invalid です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

マルチ コンテキスト モードの場合、システム実行スペース内だけでなく、各コンテキストでもドメイン名を設定できます。

例

次の例では、ドメインを example.com に設定します。

```
hostname(config)# domain-name example.com
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
hostname	セキュリティ アプライアンスのホスト名を設定します。
show running-config domain-name	ドメイン名のコンフィギュレーションを表示します。

downgrade

オペレーティング システム ソフトウェア（ソフトウェア イメージ）の以前のバージョンにダウングレードするには、特権 EXEC モードで ***downgrade*** コマンドを使用します。

注意　PIX セキュリティ アプライアンスが現在 PIX バージョン 7.0 以降を実行している場合は、以前のバージョンのソフトウェアをロードしないでください。PIX バージョン 7.0 ファイル システムがインストールされている PIX セキュリティ アプライアンスに、モニタ モードからソフトウェア イメージをロードすることは、予測できない動作を発生させるため、サポートされていません。ダウングレード プロセスを簡単に行うために用意された、実行中の PIX バージョン 7.0 イメージから、***downgrade*** コマンドを使用することをお勧めします。

downgrade *image_url* **[activation-key [flash |** *4-part_key* **|** *file***]] [config** *start_config_url***]**

シンタックスの説明

4-part_key	（オプション）イメージに書き込むための 4 分割アクティベーション キーを指定します。 5 分割キーを使用する場合、4 分割キーに戻ることにより失われる可能性がある機能のリストと共に、警告が生成されます。 システム フラッシュが再フォーマットまたは消去された場合、ダウングレード用のデフォルト キーは使用できなくなります。その場合、CLI はコマンドラインにアクティベーション キーを入力するように求めます。これは、***activation-key*** キーワードがコマンドラインで指定されていない場合のデフォルトの動作です。
activation-key	（オプション）ダウングレードされたソフトウェア イメージで使用するアクティベーション キーを指定します。
config	（オプション）スタートアップ コンフィギュレーション ファイルを指定します。
file	（オプション）ダウングレード手順が完了した後で使用するパス /URL およびアクティベーション キー ファイルの名前を指定します。アップグレード プロセス中にフラッシュに保存されたファイルが、ソースのイメージ ファイルだった場合、このファイル内のアクティベーション キーがダウングレードで使用されます。
flash	（オプション）5 分割アクティベーション キーを使用する前にデバイスで使用されていた 4 分割アクティベーション キーをフラッシュ メモリで検索するように指定します。これは、***activation-key*** キーワードがコマンドラインで指定されていない場合のデフォルトの動作です。
image_url	ダウングレードするソフトウェア イメージのパス /URL および名前を指定します。ソフトウェア イメージは、7.0(1) 以前のバージョンである必要があります。
start_config_url	（オプション）ダウングレード手順が完了した後で使用するパス /URL およびコンフィギュレーション ファイルの名前を指定します。

デフォルト

activation-key キーワードが指定されていない場合、セキュリティ アプライアンスは最後に使用された 4 分割アクティベーション キーを試します。セキュリティ アプライアンスがフラッシュで 4 分割アクティベーション キーを検出できなかった場合、コマンドは拒否され、エラー メッセージが表示されます。この場合、次回にコマンドラインで有効な 4 分割アクティベーション キーを指定する必要があります。デフォルトのアクティベーション キーまたはユーザ指定のアクティベーション キーが、現在有効なアクティベーション キーと比較されます。選択されたアクティベーション キーを使用することで、機能を損失する可能性がある場合、ダウングレード後に、損失する可能性のある機能のリストと共に警告が表示されます。

スタートアップ コンフィギュレーション ファイルが指定されていない場合、セキュリティ アプライアンスはデフォルトで downgrade.cfg を使用します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•		

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ソフトウェア リリース 7.0(1) 以降を実行している Cisco PIX Firewall シリーズのセキュリティ アプライアンスに限り使用できます。このコマンドは、Cisco ASA 5500 シリーズのセキュリティ アプライアンスではサポートされていません。

注意

ダウングレード プロセス中に電源障害が発生すると、フラッシュ メモリが破損する場合があります。予防策として、ダウングレード プロセスを開始する前に、フラッシュ メモリ上のすべてのデータを外部デバイスにバックアップしてください。

破損したフラッシュ メモリを回復するには、コンソールへの直接アクセスが必要です。詳細については、***format*** コマンドを参照してください。

例

次の例では、ソフトウェアをリリース 6.3.3 にダウングレードします。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
32c261f3 062afe24 c94ef2ea 0e299a3f
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm]
Installing the correct file system for the image and saving the buffered data
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Flash downgrade succeeded







Rebooting....

Enter zero actkey:
```

次の例は、無効なアクティベーション キーを入力した場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
0 0 0 0
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!
Error: activation key entered is invalid.

Enter the file option when there is no actkey in the source image (happens if the
source is in tftp server).
```

次の例は、ソース イメージのアクティベーション キーを指定したときに、それが存在しなかった場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3 activation-key
file
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!
Activation key does not exist in the source image.
Please use the activation-key option to specify an activation key.
```

次の例は、最後のプロンプトでダウングレード手順を中止する方法を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!

Buffering startup config

All items have been buffered successfully.
If the flash reformat is interrupted or fails, data in flash will be lost
and the system might drop to monitor mode.
Do you wish to continue? [confirm] ===<typed n here>
Downgrade process terminated.
```

ダウングレードするには、ソフトウェア バージョンが 7.0 未満である必要があります。次の例は、ソフトウェアのダウングレードに失敗した試行を示しています。

```
hostname# downgrade tftp://17.13.2.25//scratch/views/test/target/sw/cdisk
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Error: Need to use an image with version less than 7-0-0-0.
```

次の例は、イメージを指定したときにアクティベーション キーを確認しなかった場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.4.4.1-rel
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image checksum has not been verified
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Warning: Activation key not verified.
Key 32c261f3 633fe24 c94ef2ea e299a3f might be incompatible with the image version
4-4-1-0.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

次の例は、4 分割アクティベーション キーに、現在の 5 分割アクティベーション キーのすべての機能が含まれていない場合の結果を示しています。

```
hostname# downgrade tftp://17.13.2.25//tftpboot/mananthr/cdisk.6.3.3
This command will reformat the flash and automatically reboot the system.
Do you wish to continue? [confirm]
Buffering image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!
!!!!
The following features available in current activation key in flash
are NOT available in 4 tuple activation key in flash:
VPN-3DES-AES
GTP/GPRS
5 Security Contexts
Failover is different:
current activation key in flash: UR(estricted)
4 tuple activation key in flash: R(estricted)
Some features might not work in the downgraded image if this key is used.
Do you wish to continue? [confirm]
Downgrade process terminated.
Please enter an activation-key in the command line.
```

関連コマンド

コマンド	説明
copy running-config startup-config	現在の実行コンフィギュレーションをフラッシュ メモリに保存します。

drop

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop** コマンドを使用して、**match** コマンドまたはクラス マップと一致するパケットをドロップします。この drop アクションは、アプリケーション トラフィックの検査ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションでこのアクションが許可されているわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

drop [**send-protocol-error**] [**log**]

no drop [**send-protocol-error**] [**log**]

シンタックスの説明

send-protocol-error	プロトコル エラー メッセージを送信します。
log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop** コマンドを入力して **match** コマンドまたは **class** コマンドと一致するすべてのパケットをドロップできます。

パケットをドロップすると、検査ポリシー マップで以降のアクションは実行されません。たとえば、最初のアクションでパケットをドロップした場合は、それ以降、**match** コマンドまたは **class** コマンドと一致しません。最初のアクションがパケットのロギングである場合は、パケットのドロップなどの 2 番目のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は検査ポリシー マップの名前です。

例

次の例では、パケットをドロップし、http-traffic クラス マップと一致した際にログを送信します。同じパケットが 2 番目の **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

drop-connection

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **drop-connection** コマンドを使用してパケットをドロップし、**match** コマンドまたはクラス マップと一致するトラフィックの接続を閉じます。接続は、セキュリティ アプライアンス上の接続データベースから削除されます。接続がドロップされた後で、引き続きセキュリティ アプライアンスに入るパケットは廃棄されます。この drop-connection アクションはアプリケーション トラフィックの検査ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションで、このアクションが許可されるわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

drop-connection [**send-protocol-error**] [**log**]

no drop-connection [**send-protocol-error**] [**log**]

シンタックスの説明

send-protocol-error	プロトコル エラー メッセージを送信します。
log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを識別（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを指す）した後は、**drop-connection** コマンドを入力してパケットをドロップし、**match** コマンドまたは **class** コマンドと一致するトラフィックの接続を閉じます。

パケットをドロップしたり接続を閉じると、それ以降は検査ポリシー マップではアクションは実行されません。たとえば、最初のアクションがパケットをドロップし接続を閉じることである場合、それ以降は **match** コマンドまたは **class** コマンドに対応しません。最初のアクションがパケットのロギングである場合は、パケットのドロップなどの 2 番目のアクションが発生する可能性があります。同じ **match** コマンドまたは **class** コマンドに対して **drop-connection** アクションと **log** アクションの両方を設定できます。その場合、パケットは所定の一致箇所でドロップされる前にロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は検査ポリシー マップの名前です。

例

次の例では、http-traffic クラス マップと一致する際には、パケットをドロップし、接続を閉じてログを送信します。同じパケットが 2 番目の **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

duplex

銅線イーサネット インターフェイス（RJ-45）のデュプレックス方式を設定するには、インターフェイス コンフィギュレーション モードで **duplex** コマンドを使用します。デュプレックス設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

duplex {***auto*** | ***full*** | ***half***}

no duplex

シンタックスの説明

auto	デュプレックス モードを自動検出します。
full	デュプレックス モードを全二重に設定します。
half	デュプレックス モードを半二重に設定します。

デフォルト

デフォルトは auto 検出です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

デュプレックス モードは、物理インターフェイス上にだけ設定します。

duplex コマンドは、ファイバ メディアでは使用できません。

ネットワークが自動検出をサポートしていない場合は、デュプレックス モードを特定の値に設定します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度またはデュプレックス方式のいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックス方式の両方に明示的に固定値を設定して、両方の設定に関するオートネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

PoE ポート上でデュプレックスを **auto** 以外に設定した場合は、IEEE 802.3af をサポートしない Cisco IP Phone およびシスコの無線アクセス ポイントは検出されず、電源が供給されません。

例

次の例では、デュプレックス モードを全二重に設定します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべて消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

CHAPTER 12

email コマンド～ functions コマンド

email

登録中に、指定された電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるには、暗号 CA トラストポイント コンフィギュレーション モードで **email** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

email *address*

no email

シンタックスの説明

address	電子メール アドレスを指定します。*address* の最大長は 64 文字です。

デフォルト

デフォルト値は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•		

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の登録要求に電子メールアドレスの jjh@nhf.net を含めます。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# email jjh@nhf.net
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。

enable

特権 EXEC モードに入るには、ユーザ EXEC モードで **enable** コマンドを使用します。

enable [*level*]

シンタックスの説明

level	（オプション）特権レベルは 0 ～ 15 の間です。

デフォルト

特権レベル 15 を入力します。ただし、コマンドの認可を使用している場合は、デフォルトのレベルはユーザ名に設定されたレベルによって異なります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

デフォルトのイネーブル パスワードはブランクです。パスワードを設定するには、**enable password** コマンドを参照してください。

デフォルトである 15 以外の特権レベルを使用するには、ローカル コマンド認可を設定し（**aaa authorization command** コマンドを参照。***LOCAL*** キーワードを指定する）、**privilege** コマンドを使用して、コマンドを別の特権レベルに設定します。ローカル コマンド認可を設定しない場合は、イネーブル レベルが無視され、設定したレベルにかかわらずレベル 15 にアクセスできます。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードに入ります。レベル 0 およびレベル 1 は、ユーザ EXEC モードに入ります。

disable コマンドを入力して、特権 EXEC モードを終了します。

例

次の例では、特権 EXEC モードに入ります。

```
hostname> enable
Password: Pa$$w0rd
hostname#
```

次の例では、レベル 10 の特権 EXEC モードに入ります。

```
hostname> enable 10
Password: Pa$$w0rd10
hostname#
```

関連コマンド

コマンド	説明
enable password	イネーブル パスワードを設定します。
disable	特権 EXEC モードを終了します。
aaa authorization command	コマンド認可を設定します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。

enable gprs

RADIUS アカウンティングにより GPRS をイネーブルにするには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **enable gprs** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。セキュリティ アプライアンスは、セカンダリ PDP コンテキストを適切に処理するために、アカウンティング要求停止メッセージの 3GPP VSA 26-10415 をチェックします。

このオプションは、デフォルトではディセーブルになっています。この機能をイネーブルにするには、GTP ライセンスが必要です。

enable gprs

no enable gprs

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、RADIUS アカウンティングにより GPRS をイネーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enable gprs
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングの検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

enable password

特権 EXEC モードのイネーブル パスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。15 以外のレベルのパスワードを削除するには、このコマンドの **no** 形式を使用します。レベル 15 のパスワードは削除できません。

enable password *password* **[level** *level*] [***encrypted***]

no enable password level *level*

シンタックスの説明

encrypted	（オプション）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由でパスワードを別のセキュリティ アプライアンスにコピーする必要があるが、元のパスワードを知らない場合、暗号化されたパスワードとこのキーワードを指定して、**enable password** コマンドを入力します。通常、このキーワードは、**show running-config enable** コマンドを入力したときにだけ表示されます。
level *level*	（オプション）特権レベル 0 ～ 15 のパスワードを設定します。
password	パスワードに、大文字と小文字が区別される最大 16 文字の英数字および特殊文字の文字列を設定します。パスワードには疑問符（?）とスペースを除く任意の文字を使用できます。

デフォルト

デフォルトのパスワードはブランクです。デフォルトのレベルは 15 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

イネーブル レベル 15（デフォルトのレベル）のデフォルトのパスワードは、ブランクです。パスワードをブランクにリセットする場合は、*password* にテキストを入力しないでください。

マルチ コンテキスト モードでは、各コンテキストだけでなく、システム コンフィギュレーションにもイネーブル パスワードを作成できます。

デフォルトである 15 以外の特権レベルを使用するには、ローカル コマンド認可を設定し（**aaa authorization command** コマンドを参照。***LOCAL*** キーワードを指定する）、**privilege** コマンドを使用して、コマンドを別の特権レベルに設定します。ローカル コマンド認可を設定しない場合は、イネーブル レベルが無視され、設定したレベルにかかわらずレベル 15 にアクセスできます。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードに入ります。レベル 0 およびレベル 1 は、ユーザ EXEC モードに入ります。

例

次の例では、イネーブル パスワードを Pa$$w0rd に設定します。

```
hostname(config)# enable password Pa$$w0rd
```

次の例では、レベル 10 のイネーブル パスワードを Pa$$w0rd10 に設定します。

```
hostname(config)# enable password Pa$$w0rd10 level 10
```

次の例では、イネーブル パスワードを別のセキュリティ アプライアンスからコピーした暗号化されたパスワードに設定します。

```
hostname(config)# enable password jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
enable	特権 EXEC モードに入ります。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。
show running-config enable	イネーブル パスワードを暗号化された形式で表示します。

encryption

IKE ポリシー内の暗号化アルゴリズムを指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** にリセットするには、このコマンドの **no** 形式を使用します。

encryption {**aes | aes-192| aes-256 | des | 3des**}

no encryption {**aes | aes-192| aes-256 | des | 3des**}

シンタックスの説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は **3des** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 isakmp ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy encryption** コマンドは既存のものです。
7.2.(1)	**isakmp policy encryption** コマンドが、**encryption** コマンドに置き換えられました。

例

次の例は、グローバル コンフィギュレーション モードで、**encryption** コマンドを使用する方法を示しています。この例では、優先順位番号 25 の IKE ポリシーに 128 ビット キーの AES 暗号化アルゴリズムを使用するように設定します。

```
hostname(config)# crypto isakmp policy 25
hostname(config-isakmp-policy)# encryption aes
```

次の例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシーに 3DES アルゴリズムを使用するように設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# encryption 3des
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

endpoint

H.323 プロトコル検査のために HSI グループにエンドポイントを追加するには、hsi グループ コンフィギュレーション モードで **endpoint** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

シンタックスの説明

ip_address	追加するエンドポイントの IP アドレス。HSI グループあたり最大で 10 のエンドポイントが許可されます。
if_name	エンドポイントがセキュリティ アプライアンスに接続されるインターフェイス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HSI グループ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査ポリシー マップでエンドポイントを HSI グループに追加する方法を示しています。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
hsi-group	HSI グループを作成します。
hsi	HSI を HSI グループに追加します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

endpoint-mapper

DCERPC 検査のためにエンドポイント マッパー オプションを設定するには、パラメータ コンフィギュレーション モードで **endpoint-mapper** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

endpoint-mapper [**epm-service only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service only**] [**lookup-operation** [**timeout** *value*]]

シンタックスの説明

epm-service only	バインディング時にエンドポイント マッパー サービスを適用します。
lookup-operation	エンドポイント マッパー サービスのルックアップ オペレーションをイネーブルにします。
timeout *value*	ルックアップ オペレーションからのピンホールのタイムアウトを指定します。範囲は 0:0:1 ～ 1193:0:0 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、DCERPC ポリシー マップにエンドポイント マッパーを設定する方法を示しています。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# endpoint-mapper epm-service-only
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

enforcenextupdate

NextUpdate CRL フィールドの処理方法を指定するには、ca-crl コンフィギュレーション モードで **enforcenextupdate** コマンドを使用します。これが設定された場合、このコマンドは CRL の NextUpdate フィールドを無効にしないことを要求します。使用されない場合、セキュリティ アプライアンスは、不明または無効な CRL の NextUpdate フィールドを許可します。

無効または不明な NextUpdate フィールドを許可するには、このコマンドの **no** 形式を使用します。

enforcenextupdate

no enforcenextupdate

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト設定は実行（オン）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、CRL の NextUpdate フィールドをトラストポイント central に対して期限切れにしないことを要求します

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# enforcenextupdate
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
cache-time	キャッシュのリフレッシュ時間を分単位で指定します。
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。

enrollment retry count

リトライ回数を指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **enrollment retry count** コマンドを使用します。セキュリティ アプライアンスは、証明書を要求した後、CA から証明書を受信するまで待機します。設定されたリトライ期間内にセキュリティ アプライアンスが証明書を受信しない場合、別の証明書要求が送信されます。セキュリティ アプライアンスが応答を受信するか、リトライ回数が設定回数に達するまで、要求は繰り返されます。

リトライ回数のデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry count *number*

no enrollment retry count

シンタックスの説明

number	登録要求の送信を再試行する最大回数です。有効な範囲は 0、1 ～ 100 リトライです。

デフォルト

number のデフォルト設定は、0（無制限）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central 内で登録のリトライ回数を 20 リトライに設定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry count 20
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry period	登録要求を再送信するまでの待機時間を、分単位で指定します。

enrollment retry period

リトライ期間を指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **enrollment retry period** コマンドを使用します。セキュリティ アプライアンスは、証明書を要求した後、CA から証明書を受信するまで待機します。指定されたリトライ期間内にセキュリティ アプライアンスが証明書を受信しない場合、別の証明書要求が送信されます。

リトライ期間のデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry period *minutes*

no enrollment retry period

シンタックスの説明

minutes	登録要求の送信を試行する分単位の間隔です。有効な範囲は 1 ～ 60 分です。

デフォルト

デフォルト設定は 1 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central 内で登録のリトライ期間を 10 分に設定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry period 10
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	すべての登録パラメータをシステムのデフォルト値に戻します。
enrollment retry count	登録を要求するリトライの回数を定義します。

enrollment terminal

このトラストポイントでのカット アンド ペースト登録を指定するには（手動登録とも呼ばれる）、暗号 CA トラストポイント コンフィギュレーション モードで **enrollment terminal** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment terminal

no enrollment terminal

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト設定はオフです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の CA 登録のカット アンド ペースト方式を指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment terminal
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求を再送信するまでの待機時間を、分単位で指定します。
enrollment url	このトラストポイントでの自動登録（SCEP）を指定し、URL を設定します。

enrollment url

このトラストポイントで登録し、登録 URL を設定するために自動登録（SCEP）を指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **enrollment url** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment url *url*

no enrollment url

シンタックスの説明

url	自動登録で使用する URL の名前を指定します。最大長は 1,000 文字（実質上の無制限）です。

デフォルト

デフォルト設定はオフです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の SCEP 登録を URL https://enrollsite で指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url https://enrollsite
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求を再送信するまでの待機時間を、分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

eou allow

クライアントレス認証をイネーブルにするには、グローバル コンフィギュレーション モードで **eou allow** コマンドを使用します。クライアントレス認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

eou allow clientless

no eou allow clientless

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

クライアントレス認証はデフォルトでイネーブルになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは EAPoUDP 要求に応答しないホストにのみ適用されます。このコマンドが有効になるのは、次の条件をすべて満たしている場合だけです。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

例

次の例はクライアントレス認証をイネーブルにします。

```
hostname(config)# eou allow clientless
hostname(config)#
```

次の例はクライアントレス認証をディセーブルにします。

```
hostname(config)# no eou allow clientless
hostname(config)#
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou clientless	クライアントレス認証に使用するユーザ名とパスワードを変更します。

eou clientless

クライアントレス認証用にアクセス コントロール サーバに送信するユーザ名とパスワードを変更するには、グローバル コンフィギュレーション モードで **eou clientless** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou clientless username *username*

eou clientless password *password*

デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

no eou clientless username

no eou clientless password

シンタックスの説明

username	EAPoUDP 要求に応答しないリモートホストのクライアントレス認証を得るためにアクセス コントロール サーバに送信したユーザ名を変更します。
username	クライアントレス ホストをサポートするために、アクセス コントロール サーバに設定したユーザ名を入力します。1 ～ 64 文字の ASCII 文字を入力します。前後のスペース、ポンド記号（#）、疑問符（?）、引用符（"）、アステリスク（*）、角括弧（< と >）は除きます。
password	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を得るためにアクセス コントロール サーバに送信したパスワードを変更します。
password	クライアントレス ホストをサポートするために、アクセス コントロール サーバに設定したパスワードを入力します。4 ～ 32 文字の ASCII 文字を入力します。

デフォルト

ユーザ名およびパスワード アトリビュートのデフォルト値は clientless です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効になるのは、次の条件をすべて満たしている場合のみです。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上でクライアントレス認証がイネーブルになっている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

例

次の例はクライアントレス認証のユーザ名を sherlock に変更します。

```
hostname(config)# eou clientless username sherlock
hostname(config)#
```

次の例はクライアントレス認証のユーザ名をデフォルト値である clientless に変更します。

```
hostname(config)# no eou clientless username
hostname(config)#
```

次の例はクライアントレス認証のパスワードを secret に変更します。

```
hostname(config)# eou clientless password secret
hostname(config)#
```

次の例はクライアントレス認証のパスワードをデフォルト値である clientless に変更します。

```
hostname(config)# no eou clientless password
hostname(config)#
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou allow	クライアントレス認証をイネーブルにします。

eou initialize

1 つ以上のネットワーク アドミッション コントロール セッションに割り当てられたリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始するには、EXEC モードで **eou initialize** コマンドを使用します。

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

シンタックスの説明

all	このセキュリティ アプライアンス上のすべての NAC セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC セッションを再確認します。
ip	単一の NAC セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

リモート ピアのポスチャが変更されたり、割り当てられたアクセス ポリシー（ダウンロードされた ACL）が変更された場合に、セッションに割り当てられたリソースを消去するには、このコマンドを使用します。このコマンドを入力すると、EAPoUDP アソシエーションとポスチャ確認に使用するアクセス ポリシー（ダウンロードされた ACL）が消去されます。NAC デフォルト ACL は再確認時には有効です。そのためセッションを初期化すると、ユーザのトラフィックが妨げられる可能性があります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

例

次の例では、すべての NAC セッションを初期化します。

```
hostname# eou initialize all
hostname
```

次の例では、tg1 というトンネル グループに割り当てられたすべての NAC セッションを初期化します。

```
hostname# eou initialize group tg1
hostname
```

次の例では、IP アドレス 209.165.200.225 が設定されているエンドポイントの NAC セッションを初期化します。

```
hostname# eou initialize 209.165.200.225
hostname
```

関連コマンド

コマンド	説明
eou revalidate	1 つまたはそれ以上の NAC セッションのポスチャ再確認をただちに強制します。
nac-reval-period	ネットワーク アドミッション コントロール セッションで正常に完了した各ポスチャ確認の間隔を指定します。
nac-sq-period	ネットワーク アドミッション コントロール セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。

eou max-retry

セキュリティ アプライアンスが EAP over UDP メッセージをリモート コンピュータに再送信する回数を変更するには、グローバル コンフィギュレーション モードで **eou max-retry** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou max-retry *retries*

no eou max-retry

シンタックスの説明

retries	再送信期限切れの応答で送信された再試行の回数を制限します。1 ～ 3 の値を入力します。

デフォルト

デフォルト値は 3 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効になるのは、次の条件をすべて満たしている場合のみです。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上でクライアントレス認証がイネーブルになっている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

例

次の例では、EAP over UDP 再送信の回数を 1 回に制限します。

```
hostname(config)# eou max-retry 1
hostname(config)#
```

次の例では、EAP over UDP 再送信の回数をデフォルト値の 3 回に変更します。

```
hostname(config)# no eou max-retry
hostname(config)#
```

関連コマンド

debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。

eou port

Cisco Trust Agent と通信する EAP over UDP のポート番号を変更するには、グローバル コンフィギュレーション モードで **eou port** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou port *port_number*

no eou port

シンタックスの説明

port_number	EAP over UDP 通信用に指定される、クライアント エンドポイント上のポート番号。この番号は Cisco Trust Agent 上で設定されるポート番号です。1024 ～ 65535 の値を入力します。

デフォルト

デフォルト値は 21862 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、EAP over UDP 通信用ポート番号を 62445 に変更します。

```
hostname(config)# eou port 62445
hostname(config)#
```

次の例では、EAP over UDP 通信用ポート番号をデフォルト値に変更します。

```
hostname(config)# no eou port
hostname(config)#
```

関連コマンド

debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou initialize	1 つまたはそれ以上の NAC セッションに割り当てられているリソースを消去し、新しい無条件のポスチャ確認をセッションごとに開始します。
eou revalidate	1 つまたはそれ以上の NAC セッションのポスチャ再確認をただちに強制します。

eou revalidate

1 つまたは複数のネットワーク アドミッション コントロール セッションについてポスチャの即時再確認を強制するには、EXEC モードで **eou revalidate** コマンドを使用します。

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

シンタックスの説明

all	このセキュリティ アプライアンス上のすべての NAC セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC セッションを再確認します。
ip	単一の NAC セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ピアのポスチャまたは割り当てられたアクセス ポリシー（ダウンロードされた ACL）が変更された場合、このコマンドを使用します。このコマンドは新しい、無条件のポスチャ確認を開始します。コマンドを入力する前に有効であったポスチャ確認と割り当てられたアクセス ポリシーは、新しいポスチャ確認が成功するか失敗するまで有効のままです。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

例

次の例では、すべての NAC セッションを再確認します。

```
hostname# eou revalidate all
hostname
```

次の例では、tg-1 というトンネル グループに割り当てられたすべての NAC セッションを再確認します。

```
hostname# eou revalidate group tg-1
hostname
```

次の例では、IP アドレス 209.165.200.225 が設定されているエンドポイントの NAC セッションを再確認します。

```
hostname# eou revalidate ip 209.165.200.225
hostname
```

関連コマンド

コマンド	説明
eou initialize	1 つまたはそれ以上の NAC セッションに割り当てられているリソースを消去し、新しい無条件のポスチャ確認をセッションごとに開始します。
nac-reval-period	ネットワーク アドミッション コントロール セッションで正常に完了した各ポスチャ確認の間隔を指定します。
nac-sq-period	ネットワーク アドミッション コントロール セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。

eou timeout

EAPoUDP メッセージをリモート ホストに送信した後の待機秒数を変更するには、グローバル コンフィギュレーション モードで **eou timeout** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou timeout {**hold-period | retransmit**} *seconds*

no eou timeout {**hold-period | retransmit**}

シンタックスの説明

hold-period	EAPoUDP メッセージ送信後の最長待機時間は EAPoUDP 再試行数と同じです。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行すると、この設定時間も消去されます。この設定時間が経過すると、セキュリティ アプライアンスは EAP over UDP とリモート ホストとの関連付けを新たに開始します。
retransmit	EAPoUDP メッセージ送信後の最長待機時間。リモート ホストからの応答により、この設定時間は消去されます。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行すると、この設定時間も消去されます。設定時間が経過すると、セキュリティ アプライアンスは EAPoUDP メッセージをリモート ホストに再送します。
seconds	セキュリティ アプライアンスが待機する秒数。hold-period アトリビュートには、範囲 60 ～ 86400 の値、retransmit アトリビュートには、範囲 1 ～ 60 の値をそれぞれ入力します。

デフォルト

hold-period アトリビュートのデフォルト値は 180 です。

retransmit アトリビュートのデフォルト値は 3 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、新しい EAP over UDP アソシエーションを開始するまでの待機時間を 120 秒に変更します。

```
hostname(config)# eou timeout hold-period 120
hostname(config)#
```

次の例では、新しい EAP over UDP アソシエーションを開始するまでの待機時間をデフォルト値に変更します。

```
hostname(config)# no eou timeout hold-period
hostname(config)#
```

次の例では、再送待機時間を 6 秒に変更します。

```
hostname(config)# eou timeout retransmit 6
hostname(config)#
```

次の例では、再送待機時間をデフォルト値に変更します。

```
hostname(config)# no eou timeout retransmit
hostname(config)#
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
eou max-retry	セキュリティ アプライアンスが EAP over UDP メッセージをリモート コンピュータに再送する回数を変更します。

erase

ファイル システムを消去して再フォーマットするには、特権 EXEC モードで ***erase*** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むすべてのファイルを上書きし、ファイル システムを消去してからファイル システムを再インストールします。

erase [**disk0: | disk1: | flash:**]

シンタックスの説明

disk0:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（オプション）外部のコンパクト フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
flash:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。 **注意** フラッシュ メモリを消去すると、フラッシュ メモリに保存されているライセンス情報も削除されます。フラッシュ メモリを消去する前に、ライセンス情報を保存してください。 ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

erase コマンドは、OxFF パターンを使用してフラッシュ メモリ上のすべてのデータを消去し、空のファイル システム割り当てテーブルをデバイスに書き直します。

すべての可視ファイル（非表示のシステム ファイルを除く）を削除するには、***erase*** コマンドではなく、***delete /recursive*** コマンドを使用します。

（注） Cisco PIX セキュリティ アプライアンスでは、***erase*** コマンドと ***format*** コマンドは同じ処理を実行します。ユーザ データを 0xFF パターンを使用して破棄します。

(注)　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、***erase*** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、***format*** コマンドはファイル システムの制御構造をリセットするだけです。生ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

例

次の例では、ファイル システムを消去して再フォーマットします。

```
hostname# erase flash:
```

関連コマンド

コマンド	説明
delete	非表示のシステム ファイルを除く、すべての可視ファイルを削除します。
format	すべてのファイル（非表示のシステム ファイルを含む）を消去して、ファイル システムをフォーマットします。

esp

IPSec Pass Thru 検査用に esp トンネルと AH トンネルのパラメータを指定するには、パラメータ コンフィギュレーション モードで **esp** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

{**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

シンタックスの説明

esp	esp トンネルのパラメータを指定します。
ah	AH トンネルのパラメータを指定します。
per-client-max *n*	1 つのクライアントから最大トンネルを指定します。
timeout *time*	esp トンネルにアイドルタイムを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、UDP 500 トラフィックを許可する方法を示しています。

```
hostname(config)# access-list test-udp-acl extended permit udp any any eq 500
hostname(config)# class-map test-udp-class
hostname(config-pmap-c)# match access-list test-udp-acl

hostname(config)# policy-map type inspect ipsec-pass-thru ipsec-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
hostname(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

hostname(config)# policy-map test-udp-policy
hostname(config-pmap)# class test-udp-class
hostname(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

established

確立されている接続に基づくポート上のリターン接続を許可するには、グローバル コンフィギュレーション モードで **established** コマンドを使用します。**established** 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

established *est_protocol dport* [*sport*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dport* [*sport*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

シンタックスの説明

est_protocol	確立されている接続のルックアップに使用する IP プロトコル（UDP または TCP）を指定します。
dport	確立されている接続のルックアップに使用する宛先ポートを指定します。
permitfrom	（オプション）指定されたポートから発信されるリターン プロトコル接続を許可します。
permitto	（オプション）指定されたポート宛のリターン プロトコル接続を許可します。
port [*-port*]	（オプション）リターン接続の（UDP または TCP）宛先ポートを指定します。
protocol	（オプション）リターン接続により使用される IP プロトコル（UDP または TCP）です。
sport	（オプション）確立されている接続のルックアップに使用する送信元ポートを指定します。

デフォルト

デフォルトは次のとおりです。

- *dport*：0（ワイルドカード）
- *sport*：0（ワイルドカード）

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	***to*** および ***from*** キーワードが、CLI から削除されました。代わりに ***permitto*** および ***permitfrom*** キーワードを使用してください。

使用上のガイドライン

established コマンドは、発信接続に対するリターン アクセスがセキュリティ アプライアンスを通るのを許可します。このコマンドは、ネットワークからの発信で、セキュリティ アプライアンスによって保護されている元の接続、および外部ホスト上の同じ 2 つのデバイス間の着信であるリターン接続を扱います。**established** コマンドを使用すると、接続のルックアップに使用する宛先ポートを指定できます。この追加によって、コマンドをさらに制御できるようになり、宛先ポートは既知であるが、送信元ポートは未知のプロトコルをサポートできます。**permitto** キーワードと **permitfrom** キーワードは、リターン着信接続を定義します。

注意　**established** コマンドには常に **permitto** キーワードと **permitfrom** キーワードを指定することを推奨します。この 2 つのキーワードを指定せずに **established** コマンドを使用すると、外部システムに接続したときに、その外部システムが接続に関係する内部ホストに無制限に接続できるため、セキュリティ リスクになるおそれがあります。この状況は、内部システムへの攻撃に利用される可能性があります。

次の例は、**established** コマンドを正しく使用しなかった場合に発生する可能性のあるセキュリティ違反を示しています。

この例は、内部システムがポート 4000 上の外部ホストに TCP 接続を作成した場合、外部ホストは、任意のプロトコルを使用して任意のポート上に戻れることを示しています。

```
hostname(config)# established tcp 0 4000
```

使用するポートをプロトコルが指定しない場合、送信元ポートおよび宛先ポートを **0** に指定できます。必要な場合に限り、ワイルドカード ポート（0）を使用します。

```
hostname(config)# established tcp 0 0
```

（注）　**established** コマンドが正しく動作するには、クライアントが **permitto** キーワードで指定したポート上でリッスンしている必要があります。

established コマンドは、**nat 0** コマンド（**global** コマンドがない）を付けて使用できます。

（注）　**established** コマンドを、PAT と共に使用することはできません。

セキュリティ アプライアンスは、**established** コマンドと連携して XDMCP をサポートしています。

注意　セキュリティ アプライアンスを介して XWindows システム アプリケーションを使用すると、セキュリティ リスクになる恐れがあります。

XDMCP は、デフォルトでオンになっていますが、**established** コマンドを次のように入力するまでセッションは確立されません。

```
hostname(config)# established tcp 0 6000 to tcp 6000 from tcp 1024-65535
```

established コマンドを入力すると、内部の XDMCP（UNIX または ReflectionX）搭載ホストが、外部の XDMCP 搭載 XWindows サーバにアクセスできます。UDP/177 ベースの XDMCP が TCP ベースの XWindows セッションをネゴシエートし、それに続く TCP リターン接続が許可されます。リターン トラフィックの送信元ポートが不明であるため、*sport* フィールドは 0（ワイルドカード）と指定する必要があります。*dport* は、6000 + *n* である必要があります。ここで、*n* は、ローカル ディスプレイ番号です。UNIX コマンドを使用して、この値を変更します。

```
hostname(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

established コマンドが必要な理由は、多くの TCP 接続が生成され（ユーザとの対話に基づき）、これらの接続に使用される送信元ポートが不明であるためです。宛先ポートだけがスタティックです。セキュリティ アプライアンスは、XDMCP フィックスアップを透過的に行います。設定は不要ですが、TCP セッションに対応するには **established** コマンドの入力が必要です。

例

次の例では、2 つのホスト間の、プロトコル A を使用した SRC ポート B からポート C を宛先とする接続を示しています。セキュリティ アプライアンスを通過するリターン接続でプロトコル D（プロトコル A はプロトコル D と異なる可能性がある）を許可するには、送信元ポートはポート F に対応し、宛先ポートはポート E に対応している必要があります。

```
hostname(config)# established A B C permitto D E permitfrom D F
```

この例は、内部ホストから外部ホストに対し、TCP 送信元ポート 6060 と任意の宛先ポートを使用して接続を開始する方法を示しています。セキュリティ アプライアンスは、このホスト間に TCP 宛先ポート 6061 と TCP 送信元ポート 6059 を経由するリターン トラフィックを許可します。

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 6059
```

この例は、内部ホストから外部ホストに対し、UPD 宛先ポート 6060 と任意の送信元ポートを使用して接続を開始する方法を示しています。セキュリティ アプライアンスは、このホスト間に TCP 宛先ポート 6061 と TCP 送信元ポート 1024-65535 を経由するリターン トラフィックを許可します。

```
hostname(config)# established udp 0 6060 permitto tcp 6061 permitfrom tcp 1024-65535
```

次の例は、ローカル ホスト 10.1.1.1 が外部のホスト 209.165.201.1 に対してポート 9999 上で TCP 接続を開始する方法を示しています。この例では、外部ホスト 209.165.201.1 のポート 4242 からのパケットがローカル ホスト 10.1.1.1 のポート 5454 に戻ることが許可されます。

```
hostname(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

次の例は、外部ホスト 209.165.201.1 の任意のポートからローカル ホスト 10.1.1.1 のポート 5454 に戻るパケットを許可する方法を示しています。

```
hostname(config)# established tcp 9999 permitto tcp 5454
```

関連コマンド

コマンド	説明
clear configure established	確立されたコマンドをすべて削除します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。

exceed-mss

スリーウェイ ハンドシェイクの間にピアによって設定された TCP の最大セグメント サイズを超えるデータ長のパケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

シンタックスの説明

allow	MSS を超えるパケットを許可します。
drop	MSS を超えるパケットをドロップします。

デフォルト

デフォルトでは、パケットはドロップされます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。スリーウェイ ハンドシェイクの間にピアによって設定された TCP の最大セグメント サイズを超えるデータ長の TCP パケットをドロップするには、tcp マップ コンフィギュレーション モードの **exceed-mss** コマンドを使用します。

例

次の例では、ポート 21 で MSS を超過するパケットを送信するフローを許可します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# exceed-mss allow
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq ftp
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンド シンタックスのヘルプを表示します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

exit

現在のコンフィギュレーション モードを終了するか、特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**exit** コマンドを使用します。

exit

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

キー シーケンス ***Ctrl+Z*** を使用しても、グローバル コンフィギュレーション（およびそれより上位の）モードを終了できます。このキー シーケンスは、特権 EXEC モードおよびユーザ EXEC モードでは機能しません。

特権 EXEC モードまたはユーザ EXEC モードで **exit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次の例は、**exit** コマンドを使用して、グローバル コンフィギュレーション モードを終了してセッションからログアウトする方法を示しています。

```
hostname(config)# exit
hostname# exit

Logoff
```

次の例は、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了する方法と、**disable** コマンドを使用して特権 EXEC モードを終了する方法を示しています。

```
hostname(config)# exit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
quit	コンフィギュレーション モードを終了します。または、特権 EXEC モードまたはユーザ EXEC モードからログアウトします。

expiry-time

オブジェクトのキャッシングが、オブジェクトの再確認なしで期限切れになる時刻を設定するには、キャッシュ モードで **expiry-time** コマンドを使用します。有効期限を新しい値で再設定するには、もう一度このコマンドを使用します。有効期限をコンフィギュレーションから削除してデフォルト値の 1 分にリセットするには、このコマンドの **no** 形式を使用します。

expiry-time *time*

no expiry-time

シンタックスの説明

time	セキュリティ アプライアンスがオブジェクトを再確認せずにキャッシュする場合に必要な時間を分単位で表します。

デフォルト

1 分。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

有効期限は、セキュリティ アプライアンスがオブジェクトを再確認せずにキャッシュする場合に必要な時間を分単位で表したものです。再確認は、コンテンツを再び確認することによって行われます。

例

次の例では、有効期限を 13 分に設定する方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#expiry-time 13
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシングをディセーブルにします。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

failover

フェールオーバーをイネーブルにするには、グローバル コンフィギュレーション モードで **failover** コマンドを使用します。フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

failover

no failover

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

フェールオーバーはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーションでフェールオーバーをイネーブルまたはディセーブルにすることに制限されています（**failover active** コマンドを参照してください）。
7.2(1)	ASA 5505 デバイスに固有のフェールオーバー機能のサポートが追加されました。

使用上のガイドライン

フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

注意

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

ASA 5505 デバイスではステートレス フェールオーバーのみ許可されます。さらに、Easy VPN ハードウェア クライアントとして機能していない場合に限ります。

例

次の例では、フェールオーバーをディセーブルにします。

```
hostname(config)# no failover
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	アクティブにするスタンバイ装置を切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover active

スタンバイ セキュリティ アプライアンスまたはフェールオーバー グループをアクティブ状態にするには、特権 EXEC モードで **failover active** コマンドを使用します。アクティブなセキュリティ アプライアンスまたはフェールオーバー グループをスタンバイに切り替えるには、このコマンドの **no** 形式を使用します。

failover active [***group*** *group_id*]

no failover active [***group*** *group_id*]

シンタックスの説明

group *group_id*	（オプション）アクティブにするフェールオーバー グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいフェールオーバー グループを含めるように修正されました。

使用上のガイドライン

failover active コマンドを使用して、スタンバイ装置からフェールオーバー スイッチを起動します。または、アクティブ装置から **no failover active** コマンドを使用して、フェールオーバー スイッチを起動します。この機能を使用して、障害が発生した装置をサービスに戻し、メンテナンスのため、アクティブ装置を強制的にオフラインにします。ステートフル フェールオーバーを使用していない場合、すべてのアクティブな接続はドロップされます。フェールオーバーが発生した後、クライアントはそれらの接続を再度確立する必要があります。

フェールオーバー グループの切り替えは、Active/Active フェールオーバーでのみ利用可能です。フェールオーバー グループを指定せずに Active/Active フェールオーバー装置に **failover active** コマンドを入力した場合、装置上のすべてのグループがアクティブになります。

例

次の例では、スタンバイ グループ 1 をアクティブにしています。

```
hostname# failover active group 1
```

関連コマンド

コマンド	説明
failover reset	セキュリティ アプライアンスを、障害が発生した状態からスタンバイに変更します。

failover group

Active/Active フェールオーバー グループを設定するには、グローバル コンフィギュレーション モードで **failover group** コマンドを使用します。フェールオーバー グループを削除するには、このコマンドの **no** 形式を使用します。

failover group *num*

no failover group *num*

シンタックスの説明

num	フェールオーバー グループの番号。有効値は、1 または 2 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

最大 2 つのフェールオーバー グループを定義できます。**failover group** コマンドは、マルチ コンテキスト モード用に設定されたデバイスのシステム コンテキストにだけ追加できます。フェールオーバー グループの作成と登録は、フェールオーバーがディセーブルにされている場合のみ可能です。

このコマンドを入力すると、フェールオーバー グループ コマンド モードに入ります。**primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、**mac address**、および **polltime interface** コマンドは、フェールオーバー グループ コンフィギュレーション モードで使用できます。グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

(注) **failover polltime interface**、**failover interface-policy**、**failover replication http**、および **failover mac address** コマンドは、Active/Active フェールオーバー コンフィギュレーションに影響を与えません。それらのコマンドは、フェールオーバー コンフィギュレーション モードの **polltime interface**、**interface-policy**、**replication http**、および **mac address** コマンドによって上書きされます。

フェールオーバー グループを削除するときは、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には、常に管理コンテキストが含まれています。フェールオーバー グループに割り当てられていないコンテキストは、デフォルトによりフェールオーバー グループ 1 に割り当てられます。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

（注） 同じネットワーク上に Active/Active フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上の MAC アドレスを重複させないためには、**mac address** コマンドを使用して、各物理インターフェイスに必ずアクティブとスタンバイの仮想 MAC アドレスを割り当てるようにしてください。

例

次の例（抜粋）は、2 つのフェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
asr-group	非対称のルーティング インターフェイス グループ ID を指定します。
interface-policy	モニタリングがインターフェイス障害を検出したときのフェールオーバー ポリシーを指定します。
join-failover-group	フェールオーバー グループにコンテキストを割り当てます。
mac address	フェールオーバー グループ内のコンテキストの仮想 MAC アドレスを定義します。
polltime interface	監視されているインターフェイスに送信される hello メッセージの間隔を指定します。
preempt	リブート後、優先順位がより高い装置がアクティブ装置になるように指定します。
primary	プライマリ装置に、フェールオーバー グループに対するより高い優先順位を指定します。
replication http	選択されたフェールオーバー グループに対して HTTP セッションの複製を指定します。
secondary	セカンダリ装置に、フェールオーバー グループに対するより高い優先順位を指定します。

failover interface ip

フェールオーバー インターフェイスとステートフル フェールオーバー インターフェイスに対して IP アドレスとマスクを指定するには、グローバル コンフィギュレーション モードで **failover interface ip** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

failover interface ip *if_name ip_address mask* ***standby*** *ip_address*

no failover interface ip *if_name ip_address mask* ***standby*** *ip_address*

シンタックスの説明

if_name	フェールオーバーまたはステートフル フェールオーバー インターフェイスのインターフェイス名です。
ip_address mask	プライマリ モジュール上のフェールオーバーまたはステートフル フェールオーバー インターフェイスに対して、IP アドレスとマスクを指定します。
standby *ip_address*	セカンダリ モジュールがプライマリ モジュールとの通信に使用する IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバーおよびステートフル フェールオーバー インターフェイスは、レイヤ 3 の機能です。そのことは、セキュリティ アプライアンスが透過的なファイアウォール モードで動作していても、インターフェイスがシステムにグローバルであっても変わりません。

マルチ コンテキスト モードでは、システム コンテキストでフェールオーバーを設定します（**monitor-interface** コマンドを除く）。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例は、フェールオーバー インターフェイスに対して IP アドレスとマスクを指定する方法を示しています。

```
hostname(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover link	ステートフル フェールオーバーに使用するインターフェイスを指定します。
monitor-interface	指定されたインターフェイスのヘルスを監視します。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover interface-policy

モニタリングがインターフェイス障害を検出したときのフェールオーバーのポリシーを指定するには、グローバル コンフィギュレーション モードで **failover interface-policy** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

failover interface-policy *num*[**%**]

no failover interface-policy *num*[**%**]

シンタックスの説明

num	パーセンテージとして使用されるときは 1 ～ 100 の数字を指定し、番号として使用されるときは 1 からインターフェイスの最大数の数字を指定します。
%	（オプション）*num* の数が監視対象インターフェイスのパーセンテージであることを指定します。

デフォルト

デフォルトは次のとおりです。

- *num* は 1 です。
- 物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトではディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にスペースを含めないでください。

障害が発生したインターフェイスの数が設定済みポリシーの基準を満たした場合、他のセキュリティ アプライアンスが正常に機能しているときは、セキュリティ アプライアンスは自身を障害としてマークし、場合によってはフェールオーバーが発生します（アクティブなセキュリティ アプライアンスに障害が発生した場合）。ポリシーでカウントされるのは、**monitor-interface** コマンドで監視対象として指定したインターフェイスのみです。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードの **interface-policy** コマンドを使用して、各フェールオーバー グループのインターフェイス ポリシーを設定します。

例

次の例では、フェールオーバー ポリシーを指定する 2 つの方法を示しています。

```
hostname(config)# failover interface-policy 20%

hostname(config)# failover interface-policy 5
```

関連コマンド

コマンド	説明
failover polltime	装置とインターフェイスのポーリング回数を指定します。
failover reset	障害が発生した装置を、障害が発生する前の状態に戻します。
monitor-interface	フェールオーバーのために監視対象にするインターフェイスを指定します。
show failover	装置のフェールオーバー状態に関する情報を表示します。

failover key

フェールオーバー ペアの装置間で暗号化および認証された通信のキーを指定するには、グローバル コンフィギュレーション モードで **failover key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

failover key {*secret* | ***hex*** *key*}

no failover key

シンタックスの説明

hex *key*	暗号キー用の 16 進値を指定します。キーは、32 個の 16 進文字（0-9、a-f）にする必要があります。
secret	英数字の共有秘密を指定します。秘密には 1 ～ 63 文字を設定できます。有効な文字は、番号、文字、または句読点の任意の組み合せです。共有秘密は、暗号キーを生成するために使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドは、**failover lan key** から **failover key** に修正されました。
7.0(4)	このコマンドは、***hex*** *key* キーワードおよび引数を含めるように変更されました。

使用上のガイドライン

装置間のフェールオーバー通信を暗号化して認証するには、共有秘密または 16 進キーを使用して両方の装置を設定する必要があります。フェールオーバー キーを指定しない場合、フェールオーバー通信はクリアで送信されます。

（注） PIX セキュリティ アプライアンス プラットフォームでは、装置を接続するために専用のシリアル フェールオーバー ケーブルを使用している場合、フェールオーバー キーが設定されていても、このフェールオーバー リンク経由の通信は暗号化されません。フェールオーバー キーは LAN ベースのフェールオーバー通信だけを暗号化します。

注意

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例は、フェールオーバー ペアの装置間のフェールオーバー通信を保護するために共有秘密を指定する方法を示しています。

```
hostname(config)# failover key abcdefg
```

次の例は、フェールオーバー ペアの装置間のフェールオーバー通信を保護するために 16 進キーを指定する方法を示しています。

```
hostname(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

関連コマンド

コマンド	説明
show running-config failover	実行コンフィギュレーション内の failover コマンドを表示します。

failover lan enable

LAN ベースのフェールオーバーを PIX セキュリティ アプライアンス上でイネーブルにするには、グローバル コンフィギュレーション モードで **failover lan enable** コマンドを使用します。LAN ベースのフェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

failover lan enable

no failover lan enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

イネーブルになっていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドの **no** 形式を使用して LAN ベースのフェールオーバーをディセーブルにした場合、フェールオーバー ケーブルがインストールされている場合はケーブル ベースのフェールオーバーが使用されます。このコマンドは、PIX セキュリティ アプライアンスでのみ使用できます。

注意

フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例では、LAN ベースのフェールオーバーをイネーブルにします。

```
hostname(config)# failover lan enable
```

関連コマンド

コマンド	説明
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover lan interface

フェールオーバー通信に使用されるインターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover lan interface** コマンドを使用します。フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover lan interface *if_name* {*phy_if*[*.sub_if*] | *vlan_if*}

no failover lan interface [*if_name* {*phy_if*[*.sub_if*] | *vlan_if*}]

シンタックスの説明

if_name	フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	物理インターフェイスを指定します。
sub_if	（オプション）サブインターフェイス番号を指定します。
vlan_if	ASA 5505 適応型セキュリティ アプライアンス上で使用され、フェールオーバー リンクとして VLAN インターフェイスを指定します。

デフォルト

設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドが、*phy_if* 引数を含めるように修正されました。
7.2(1)	このコマンドが、*vlan_if* 引数を含めるように修正されました。

使用上のガイドライン

LAN フェールオーバーでは、フェールオーバー トラフィックを送信するための専用のインターフェイスが必要です。ただし、ステートフル フェールオーバー リンクに対しては、LAN フェールオーバー インターフェイスを使用することもできます。

（注） LAN フェールオーバーとステートフル フェールオーバーの両方に対して同じインターフェイスを使用する場合、インターフェイスには LAN ベースのフェールオーバーとステートフル フェールオーバーの両方のトラフィックを処理するための十分な容量が必要です。

デバイス上の使用されていない任意のイーサネット インターフェイスを、フェールオーバー インターフェイスとして使用できます。現在名前で設定されているインターフェイスは指定できません。フェールオーバー インターフェイスは、通常のネットワーク インターフェイスとしては設定されません。フェールオーバー通信専用です。このインターフェイスは、フェールオーバー リンクのために（およびオプションで状態リンクのために）だけ使用する必要があります。LAN ベースのフェールオーバー リンクは、リンクにホストまたはルータのない専用スイッチを使用するか、装置を直接リンクするためのクロスオーバー イーサネット ケーブルを使用して接続できます。

(注)　VLAN を使用する場合は、フェールオーバー リンクのための専用 VLAN を使用します。フェールオーバー リンク VLAN を他の VLAN と共有すると、断続的なトラフィック障害や PING および ARP 障害が発生する場合があります。スイッチを使用してフェールオーバー リンクに接続する場合、スイッチ上の専用インターフェイスと、セキュリティ アプライアンス上の専用インターフェイスをフェールオーバー リンク用に使用してください。通常のネットワーク トラフィックを伝送するサブインターフェイスを持つインターフェイスを共有しないでください。

マルチ コンテキスト モードを実行しているシステム上では、フェールオーバー リンクはシステム コンテキスト内にあります。このインターフェイスと状態リンク（使用されている場合）が、システム コンテキスト内にある設定可能な唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

(注)　フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。

このコマンドの **no** 形式では、フェールオーバー インターフェイスの IP アドレス設定も消去されます。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例では、PIX 500 シリーズセキュリティ アプライアンス上にフェールオーバー LAN インターフェイスを設定します。

```
hostname(config)# failover lan interface folink Ethernet4
```

次の例では、ASA 5500 シリーズ適応型セキュリティ アプライアンス（ASA 5505 適応型セキュリティ アプライアンスを除く）上にサブインターフェイスを使用してフェールオーバー LAN インターフェイスを設定します。

```
hostname(config)# failover lan interface folink GigabitEthernet0/3.1
```

次の例では、ASA 5505 適応型セキュリティ アプライアンス上にフェールオーバー LAN インターフェイスを設定します。

```
hostname(config)# failover lan interface folink Vlan6
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
failover link	ステートフル フェールオーバー インターフェイスを指定します。

failover lan unit

LAN フェールオーバー設定でセキュリティ アプライアンスをプライマリ装置またはセカンダリ装置のいずれかに設定するには、グローバル コンフィギュレーション モードで **failover lan unit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

failover lan unit {***primary*** | ***secondary***}

no failover lan unit {***primary*** | ***secondary***}

シンタックスの説明

primary	セキュリティ アプライアンスをプライマリ装置として指定します。
secondary	セキュリティ アプライアンスをセカンダリ装置として指定します。

デフォルト

セカンダリです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

Active/Standby フェールオーバーの場合、フェールオーバー装置のプライマリ宛先およびセカンダリ宛先は、ブート時にどちらの装置がアクティブになるかを指定します。次の状態が発生すると、プライマリ装置がブート時にアクティブ装置になります。

- プライマリ装置およびセカンダリ装置の両方が、最初のフェールオーバー ポーリング チェック内にブート シーケンスを完了した。
- プライマリ装置がセカンダリ装置の前にブートした。

プライマリ装置がブートするときにセカンダリ装置がすでにアクティブであった場合、プライマリ装置はアクティブではなくスタンバイ装置になります。この場合、強制的にプライマリ装置をアクティブ ステータスに戻すために、**no failover active** コマンドをセカンダリ（アクティブ）装置に発行する必要があります。

Active/Active フェールオーバーに対して、各フェールオーバー グループにはプライマリ装置またはセカンダリ装置のプリファレンスが割り当てられます。このプリファレンスは、両方の装置が同時に起動する場合（フェールオーバー ポーリング期間内で）、フェールオーバー グループのコンテキストのフェールオーバー ペアのどの装置をアクティブにするかを決定します。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときにコンフィギュレーションに含める必要があります。

例

次の例では、LAN ベースのフェールオーバーでセキュリティ アプライアンスをプライマリ装置として設定します。

```
hostname(config)# failover lan unit primary
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover link

ステートフル フェールオーバー インターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover link** コマンドを使用します。ステートフル フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover link *if_name* [*phy_if*]

no failover link

シンタックスの説明

if_name	ステートフル フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	（オプション）物理インターフェイスまたは論理インターフェイスのポートを指定します。ステートフル フェールオーバー インターフェイスが、フェールオーバー通信に割り当てられたインターフェイスまたは標準ファイアウォール インターフェイスを共有している場合、この引数は必要ありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドが、*phy_if* 引数を含めるように修正されました。
7.0(4)	このコマンドは、標準ファイアウォール インターフェイスを受け入れるように修正されました。

使用上のガイドライン

このコマンドはステートフル フェールオーバーをサポートしない ASA 5505 シリーズ適応型セキュリティ アプライアンスでは利用できません。

物理インターフェイスまたは論理インターフェイスの引数は、フェールオーバー通信または標準ファイアウォール インターフェイスを共有していない場合に必要です。

failover link コマンドは、ステートフル フェールオーバーをイネーブルにします。ステートフル フェールオーバーをディセーブルにするには、**no failover link** コマンドを入力します。専用のステートフル フェールオーバー インターフェイスを使用している場合、**no failover link** コマンドを実行すると、ステートフル フェールオーバー インターフェイスの IP アドレス設定も消去されます。

ステートフル フェールオーバーを使用するには、すべての状態情報を渡すようにステートフル フェールオーバー リンクを設定する必要があります。ステートフル フェールオーバー リンクの設定には、次の 3 つのオプションがあります。

- ステートフル フェールオーバー リンク専用のイーサネット インターフェイスを使用できます。

- LAN ベースのフェールオーバーを使用している場合、フェールオーバー リンクを共有できます。
- 内部インターフェイスなどの通常のデータ インターフェイスを共有できます。ただし、このオプションは推奨されていません。

ステートフル フェールオーバー リンク専用のイーサネット インターフェイスを使用している場合、スイッチまたは装置を直接接続するクロスケーブルを使用できます。スイッチを使用する場合、このリンク上に他のホストまたはルータは設定できません。

(注)　セキュリティ アプライアンスに直接接続するシスコ スイッチ ポート上で PortFast オプションをイネーブルにします。

フェールオーバー リンクをステートフル フェールオーバー リンクとして使用している場合、利用可能な最速のイーサネット インターフェイスを使用する必要があります。インターフェイス上でパフォーマンスの低下が見られる場合は、別のインターフェイスをステートフル フェールオーバー インターフェイス専用にすることを検討してください。

ステートフル フェールオーバー リンクとしてデータ インターフェイスを使用する場合は、そのインターフェイスをステートフル フェールオーバー リンクとして指定しようとすると次の警告が表示されます。

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

データ インターフェイスをステートフル フェールオーバー インターフェイスと共有すると、リプレイ アタックを受けやすくなります。さらに、大容量のステートフル フェールオーバー トラフィックがインターフェイスに送信される可能性があり、そのネットワーク セグメントでパフォーマンスが低下する恐れがあります。

(注)　ステートフル フェールオーバー インターフェイスとしてデータ インターフェイスを使用することは、シングル コンテキスのルーテッド モードのみでサポートされています。

マルチ コンテキスト モードでは、ステートフル フェールオーバー リンクはシステム コンテキスト内にあります。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

マルチ コンテキスト モードでは、ステートフル フェールオーバー インターフェイスはシステム コンテキスト内にあります。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

(注)　ステートフル フェールオーバー リンクが通常のデータ インターフェイスで設定されている場合を除き、ステートフル フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバーで変更されません。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになる恐れがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次の例は、ステートフル フェールオーバー インターフェイスとして専用インターフェイスを指定する方法を示しています。次の例のインターフェイスには、既存のコンフィギュレーションはありません。

```
hostname(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

関連コマンド

コマンド	説明
failover interface ip	**failover** コマンドおよびステートフル フェールオーバー インターフェイスの IP アドレスを設定します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
mtu	インターフェイスの最大伝送ユニットを指定します。

failover mac address

物理インターフェイスのためのフェールオーバー仮想 MAC アドレスを指定するには、グローバル コンフィギュレーション モードで **failover mac address** コマンドを使用します。仮想 MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

シンタックスの説明

phy_if	MAC アドレスを設定するインターフェイスの物理名。
active_mac	アクティブなセキュリティ アプライアンスの、指定されたインターフェイスに割り当てられた MAC アドレス。MAC アドレスは、h.h.h 形式で入力する必要があります。h は、16 ビットの 16 進数値です。
standby_mac	スタンバイ セキュリティ アプライアンスの指定されたインターフェイスに割り当てられた MAC アドレス。MAC アドレスは、h.h.h 形式で入力する必要があります。h は、16 ビットの 16 進数値です。

デフォルト

設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

failover mac address コマンドは、Active/Standby フェールオーバー ペア用の仮想 MAC アドレスを設定します。仮想 MAC アドレスが定義されていない場合、各フェールオーバー装置はブート時にインターフェイスとしてバーンドイン MAC アドレスを使用し、それらのアドレスをフェールオーバー ピアと交換します。プライマリ装置上のインターフェイスの MAC アドレスは、アクティブ装置のインターフェイスに使用されます。

ただし、両方の装置が同時にオンラインにならず、セカンダリ装置が最初にブートしてアクティブになった場合は、独自のインターフェイスとしてバーンドイン MAC アドレスを使用します。プライマリ装置がオンラインになると、セカンダリ装置はプライマリ装置から MAC アドレスを取得します。この変更はネットワーク トラフィックを妨げる可能性があります。インターフェイスに仮想 MAC アドレスを設定すると、セカンダリ装置がプライマリ装置の前にオンラインになる場合でも、セカンダリ装置がアクティブ装置であるときに正しい MAC アドレスが使用されます。

LAN ベースのフェールオーバー用に設定されているインターフェイスには、**failover mac address** コマンドは、必要ありません（したがって、このコマンドは使用できません）。**failover lan interface** コマンドは、フェールオーバーが発生したときに IP アドレスおよび MAC アドレスのどちらも変更しないためです。セキュリティ アプライアンスが Active/Active フェールオーバーに対して設定されている場合、このコマンドは無効です。

failover mac address コマンドをコンフィギュレーションに追加する場合は、仮想 MAC アドレスを設定し、そのコンフィギュレーションをフラッシュ メモリに保存し、次にフェールオーバー ペアをリロードすることが最も良い方法です。アクティブ接続があるときに仮想 MAC アドレスが追加されると、そのアクティブ接続は停止します。また、**failover mac address** コマンドを含む完全なコンフィギュレーションをセカンダリ セキュリティ アプライアンスのフラッシュ メモリに書き込んで、仮想 MAC アドレッシングを有効にする必要があります。

failover mac address がプライマリ装置のコンフィギュレーションで指定された場合、それをセカンダリ装置のブートストラップ コンフィギュレーションでも指定する必要があります。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードの **mac address** コマンドを使用して、フェールオーバー グループのインターフェイスごとに仮想 MAC アドレスを設定します。

例

次の例では、intf2 という名前のインターフェイスに対してアクティブおよびスタンバイ MAC アドレスを設定します。

```
hostname(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

関連コマンド

コマンド	説明
show interface	インターフェイス ステータス、設定、および統計情報を表示します。

failover polltime

フェールオーバー装置のポーリング期間および待機期間を指定するには、グローバル コンフィギュレーション モードで **failover polltime** コマンドを使用します。デフォルトのポーリング期間および待機期間に戻すには、このコマンドの **no** 形式を使用します。

failover polltime [***unit***] [***msec***] *time* [***holdtime*** [***msec***] *time*]

no failover polltime [***unit***] [***msec***] *time* [***holdtime*** [***msec***] *time*]

シンタックスの説明

holdtime *time*	（オプション）、装置がフェールオーバー リンクで hello メッセージを受信する期間を設定します。この期間が経過すると、ピア装置は障害状態であると宣言されます。 有効な値の範囲は 3 ～ 45 秒ですが、オプションの ***msec*** キーワードが指定されている場合は 800 ～ 999 ミリ秒となります。
msec	（オプション）指定する時間がミリ秒単位であることを指定します。
time	hello メッセージの間隔。 有効な値の範囲は 1 ～ 15 秒ですが、オプションの ***msec*** キーワードが指定されている場合は 200 ～ 999 ミリ秒となります。
unit	（オプション）装置のポーリング期間および待機期間にコマンドを使用することを指定します。 コマンドにこのキーワードを追加してもコマンドに影響しませんが、コンフィギュレーションでこのコマンドと **failover polltime interface** コマンドとの識別が容易になります。

デフォルト

PIX セキュリティ アプライアンス上のデフォルト値は次のとおりです。

- ポーリングの *time* は 15 秒です。
- **holdtime** *time* は 45 秒です。

ASA セキュリティ アプライアンス上のデフォルト値は次のとおりです。

- ポーリングの *time* は 1 秒です。
- **holdtime** *time* は 15 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**failover poll** コマンドから **failover polltime** コマンドに変更され、***unit***、***interface***、および ***holdtime*** というキーワードを含むようになりました。
7.2(1)	***msec*** キーワードが ***holdtime*** キーワードに追加されました。***polltime*** 最短値が 500 ミリ秒から 200 ミリ秒に短縮されました。***holdtime*** 最短値が 3 秒から 800 ミリ秒に短縮されました。

使用上のガイドライン

装置のポーリング時間の 3 倍未満の ***holdtime*** 値は入力できません。ポーリング時間が短いほど、セキュリティ アプライアンスは、それだけ速く障害を検出して、フェールオーバーを起動できます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要な切り替えが発生する可能性があります。

hello パケットが、あるポーリング期間にフェールオーバー通信インターフェイスまたはケーブルで受信されない場合、追加テストが残りのインターフェイス全体で実施されます。待機期間内にピア装置から応答がない場合、この装置に障害が発生したと見なされ、障害が発生した装置がアクティブ装置であると、スタンドバイ装置が代わってアクティブ装置になります。

failover polltime [**unit**] コマンドと **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスを通過するときは、セキュリティ アプライアンスのフェールオーバー待機時間を 30 秒より低く設定する必要があります。CTIQBE キープアライブ タイムアウトは 30 秒で、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager を使用して再登録する必要があります。

例

次の例では、装置のポーリング間隔を 3 秒に設定します。

```
hostname(config)# failover polltime 3
```

次の例では、hello パケットがその時間内にフェールオーバー インターフェイスで受信されない場合、セキュリティ アプライアンスが 200 ミリ秒ごとに hello パケットを送信し、800 ミリ秒でフェールオーバーするよう設定します。次のコマンドには、オプションの ***unit*** キーワードが含まれます。

```
hostname(config)# failover polltime unit msec 200 holdtime msec 800
```

関連コマンド

コマンド	説明
failover polltime interface	Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間および待機期間を指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間および待機期間を指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover polltime interface

Active/Standby フェールオーバー コンフィギュレーションでデータ インターフェイスのポーリング期間と待機期間を指定するには、グローバル コンフィギュレーション モードで **failover polltime interface** コマンドを使用します。デフォルトのポーリング期間および待機期間に戻すには、このコマンドの **no** 形式を使用します。

failover polltime *interface* [***msec***] *time* [***holdtime*** *time*]

no failover polltime interface [***msec***] *time* [***holdtime*** *time*]

シンタックスの説明

holdtime *time*	（オプション）データ インターフェイスがデータ インターフェイスで hello メッセージを受信する期間を設定します。この期間が経過すると、ピアは障害状態であると宣言されます。有効な値は 5 ～ 75 秒です。
interface *time*	インターフェイス モニタリングのポーリング時間を指定します。有効となる値の範囲は、3 ～ 15 秒です。オプションの ***msec*** キーワードを使用した場合、有効となる値は 500 ～ 999 ミリ秒です。
msec	（オプション）指定する時間がミリ秒単位であることを指定します。

デフォルト

デフォルト値は次のとおりです。

- ポーリングの *time* は 5 秒です。
- **holdtime** *time* は、ポーリングの *time* の 5 倍の値です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**failover poll** コマンドから **failover polltime** コマンドに変更され、***unit***、***interface***、および ***holdtime*** というキーワードを含むようになりました。
7.2(1)	オプションの ***holdtime*** *time* とミリ秒でポーリング期間を指定する機能が追加されました。

使用上のガイドライン

failover polltime interface コマンドを使用して、hello パケットをデータ インターフェイスで送信する頻度を変更します。このコマンドは、Active/Active フェールオーバーに対してのみ使用できます。Active/Active フェールオーバーの場合、フェールオーバー グループ コンフィギュレーション モードの **polltime interface** コマンドを、**failover polltime interface** コマンドの代わりに使用します。

インターフェイスのポーリング時間の 5 倍未満の ***holdtime*** 値は入力できません。ポーリング時間が短いほど、セキュリティ アプライアンスは、それだけ速く障害を検出して、フェールオーバーを起動できます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要な切り替えが発生する可能性があります。インターフェイスのテストが開始されるのは、待機期間の半分が経過したときに、インターフェイス上で hello パケットが受信されていない場合です。

failover polltime unit および **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスを通過するときは、セキュリティ アプライアンスのフェールオーバー待機時間を 30 秒より低く設定する必要があります。CTIQBE キープアライブ タイムアウトは 30 秒で、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager を使用して再登録する必要があります。

例

次の例では、インターフェイスのポーリング間隔を 15 秒に設定します。

```
hostname(config)# failover polltime interface 15
```

次の例では、インターフェイスのポーリング間隔を 500 ミリ秒、待機期間を 5 秒にそれぞれ設定します。

```
hostname(config)# failover polltime interface msec 500 holdtime 5
```

関連コマンド

コマンド	説明
failover polltime	装置のフェールオーバー ポーリング期間と待機期間を指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間を指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover reload-standby

スタンバイ装置を強制的にリブートするには、特権 EXEC モードで **failover reload-standby** コマンドを使用します。

failover reload-standby

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、フェールオーバー装置が同期しない場合に使用します。スタンバイ装置は、ブーティングが終了した後で、再起動してアクティブ装置に再度同期します。

例

次の例は、スタンバイ装置を強制的にリブートするために、アクティブ装置で **failover reload-standby** コマンドを使用する方法を示しています。

```
hostname# failover reload-standby
```

関連コマンド

コマンド	説明
write standby	実行コンフィギュレーションを、スタンバイ装置のメモリに書き込みます。

failover replication http

HTTP（ポート 80）接続の複製をイネーブルにするには、グローバル コンフィギュレーション モードで **failover replication http** コマンドを使用します。HTTP 接続の複製をディセーブルにするには、このコマンドの **no** 形式を使用します。

failover replication http

no failover replication http

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

ディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドが、**failover replicate http** から **failover replication http** に変更されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常はリトライするため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**failover replication http** コマンドは、ステートフル フェールオーバーの環境で HTTP セッションのステートフル複製をイネーブルにしますが、システムのパフォーマンスに悪影響を及ぼす可能性があります。

Active/Active フェールオーバー コンフィギュレーションでは、フェールオーバー グループ コンフィギュレーション モードの **replication http** コマンドを使用して、各フェールオーバー グループの HTTP セッションの複製を設定します。

例

次の例は、HTTP 接続の複製をイネーブルにする方法を示しています。

```
hostname(config)# failover replication http
```

関連コマンド

コマンド	説明
replication http	特定のフェールオーバー グループでの HTTP セッションの複製をイネーブルにします。
show running-config failover	実行コンフィギュレーション内の **failover** コマンドを表示します。

failover reset

障害が発生したセキュリティ アプライアンスを障害が発生する前の状態に戻すには、特権 EXEC モードで **failover reset** コマンドを使用します。

failover reset [***group*** *group_id*]

シンタックスの説明

group	（オプション）フェールオーバー グループを指定します。
group_id	フェールオーバー グループの番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、オプションのフェールオーバー グループ ID を許可するように修正されました。

使用上のガイドライン

failover reset コマンドにより、障害が発生した装置またはグループを障害が発生する前の状態に変更できます。**failover reset** コマンドは、どちらの装置からでも入力できますが、常にアクティブ装置でコマンドを入力することをお勧めします。アクティブ装置で **failover reset** コマンドを入力すると、スタンバイ装置を「unfail」にします。

装置のフェールオーバー ステータスは、**show failover** または **show failover state** コマンドで表示できます。

このコマンドの **no** 形式はありません。

Active/Active フェールオーバーで **failover reset** を入力すると、装置全体がリセットされます。コマンドでフェールオーバー グループを指定すると、指定されたグループだけがリセットされます。

例

次の例は、障害が発生した装置を、障害が発生する前の状態に変更する方法を示しています。

```
hostname# failover reset
```

関連コマンド

コマンド	説明
failover interface-policy	モニタリングがインターフェイス障害を検出するときのフェールオーバー ポリシーを指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。

failover timeout

非対称ルーテッド セッションのフェールオーバーの再接続タイムアウト値を指定するには、グローバル コンフィギュレーション モードで **failover timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

failover timeout *hh*[**:***mm*:[**:***ss*]]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

シンタックスの説明

hh	タイムアウト値を時間単位で指定します。有効となる値の範囲は、-1 ～ 1,193 です。デフォルトでは、この値は 0 に設定されています。 この値を -1 に設定すると、タイムアウトがディセーブルにされ、任意の時間が経過した後でも接続を再開できます。 他のタイムアウト値を指定しないでこの値を 0 に設定すると、コマンドはデフォルト値に戻り、接続の再開はできません。**no failover timeout** コマンドも、この値をデフォルト（0）に設定します。 **(注)** デフォルト値に設定されている場合、このコマンドは実行コンフィギュレーション内に表示されません。
mm	（オプション）タイムアウト値を分単位で指定します。有効となる値の範囲は、0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。
ss	（オプション）タイムアウト値を秒単位で指定します。有効となる値の範囲は、0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。

デフォルト

デフォルトでは、*hh*、*mm*、および *ss* は 0 です。この設定では、再接続は行われません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドがコマンド リストに表示されるように修正されました。

使用上のガイドライン

このコマンドは、***nailed*** オプションを指定した **static** コマンドと共に使用します。***nailed*** オプションを使用すると、ブートアップ後またはシステムがアクティブになった後に、指定された時間内で接続を再確立できます。**failover timeout** コマンドは、その時間を指定します。設定しない場合は、接続を再確立できません。**failover timeout** コマンドは、**asr-group** コマンドに影響しません。

(注)　***nailed*** オプションを **static** コマンドに追加すると、その接続について、TCP のステート トラッキングおよびシーケンス チェッキングがスキップされます。

このコマンドの ***no*** 形式を入力すると、デフォルト値に戻ります。**failover timeout 0** を入力しても、デフォルト値に戻ります。デフォルト値に設定されている場合、このコマンドは実行コンフィギュレーション内に表示されません。

例

次の例では、スタンバイ グループ 1 をアクティブにしています。

```
hostname(config)# failover timeout 12:30
hostname(config)# show running-config failover
no failover
failover timeout 12:30:00
```

関連コマンド

コマンド	説明
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定します。

file-bookmarks

認証された WebVPN ユーザに対して表示される WebVPN ホームページの File Bookmarks タイトルまたは File Bookmarks リンクをカスタマイズするには、webvpn カスタマイゼーション モードで **file-bookmarks** コマンドを使用します。

file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **file-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトルのテキストは「File Folder Bookmarks」です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。

- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、File Bookmarks のタイトルを「Corporate File Bookmarks」にカスタマイズします。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの Application Access ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの Browse Networks ボックスをカスタマイズします。
web-applications	WebVPN ホームページの Web Application ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの Web Bookmarks タイトルまたはリンクをカスタマイズします。

file-encoding

Common Internet File System サーバからのページに対する文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **file-encoding** コマンドを使用します。**no** 形式は、file-encoding アトリビュートの値を削除します。

file-encoding {server-name | server-ip-addr} *charset*

no file-encoding {server-name | server-ip-addr}

シンタックスの説明

charset	最大 40 文字から成る文字列で、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。上記のページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 この文字列は、大文字と小文字が区別されません。コマンド インタプリタは、セキュリティ アプライアンス コンフィギュレーションで、大文字を小文字に変換します。
server-ip-addr	文字エンコーディングを指定する CIFS サーバの IP アドレス（ドット 10 進表記）。
server-name	文字エンコーディングを指定する CIFS サーバの名前。 セキュリティ アプライアンスは指定した大文字や小文字を保持しますが、名前をサーバと照合する場合は大文字と小文字の区別を無視します。

デフォルト

WebVPN コンフィギュレーションに file-encoding エントリを明示的に持たないすべての CIFS サーバからのページは、character-encoding アトリビュートから文字エンコーディング値を継承します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

webvpn character-encoding アトリビュートの値とは異なる文字エンコーディングが必要なすべての CIFS サーバに対する file-encoding エントリを入力します。

CIFS サーバから WebVPN ユーザにダウンロードされた WebVPN ポータル ページは、サーバを識別する WebVPN file-encoding アトリビュートの値を符号化します。符号化が行われなかった場合は、character-encoding アトリビュートの値を継承します。リモート ユーザのブラウザは、この値を文字エンコーディング セットのエントリにマッピングして、使用する適切な文字セットを決定します。WebVPN コンフィギュレーションで CIFS サーバ用の file-encoding エントリが指定されてなく、character-encoding アトリビュートも設定されていない場合、WebVPN ポータル ページは値を指定し

ません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自身のデフォルト エンコーディングを使用します。

CIFS サーバに適切な文字エンコーディングを、広域的には webvpn character-encoding アトリビュートによって、個別的には file-encoding の上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを適切にレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

（注） character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。日本語 Shift_JIS 文字エンコーディングを使用している場合、フォント ファミリを入れ替えるには、次の例で示すように webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してこれらの値の設定を含めるか、webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力して、フォント ファミリを削除する必要があります。

例

次の例では、「CISCO-server-jp」という名前の CIFS サーバの file-encoding アトリビュートが日本語 Shift_JIS 文字をサポートするように設定し、フォント ファミリを削除し、デフォルトの背景色を保持しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding CISCO-server-jp shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

次の例では、CIFS サーバ 10.86.5.174 の file-encoding アトリビュートが IBM860（エイリアス「CP860」）キャラクタをサポートするように設定します。

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)
```

関連コマンド

コマンド	説明
character-encoding	すべての WebVPN ポータル ページ（WebVPN コンフィギュレーションの file-encoding エントリで指定されたサーバからのページを除く）で使用されるグローバルな文字エンコーディングを指定します。
show running-config [all] webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルトのコンフィギュレーションを含めるには、**all** キーワードを使用します。
debug webvpn cifs	Common Internet File System に関するデバッグ メッセージを表示します。

filter

このグループ ポリシーまたはユーザ名の WebVPN 接続に使用するアクセス リストの名前を指定するには、webvpn モードで **filter** コマンドを使用します。**filter none** コマンドを発行して作成されたヌル値を含むアクセス リストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。フィルタ値を継承しないようにするには、**filter value none** コマンドを使用します。

ACL を設定して、このユーザまたはグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。次に、**filter** コマンドを使用して、これらの ACL を WebVPN トラフィックに適用します。

filter {**value** *ACLname* | **none**}

no filter

シンタックスの説明

none	**webvpntype** アクセス リストがないことを示します。ヌル値を設定して、アクセス リストを拒否します。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACLname*	設定済みアクセス リストの名前を指定します。

デフォルト

WebVPN アクセス リストは、**filter** コマンドを使用して指定するまで適用されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN は、**vpn-filter** コマンドで定義された ACL を使用しません。

例

次の例は、FirstGroup という名前のグループ ポリシーの *acl_in* という名前のアクセス リストを呼び出すフィルタを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成します。または、ダウンロード可能なアクセス リストを使用します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

filter activex

セキュリティ アプライアンスを通過する HTTP トラフィックの ActiveX オブジェクトを削除するには、グローバル コンフィギュレーション モードで **filter activex** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter activex | java <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

no filter activex | java <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 21 ですが、他の値でも受け入れられます。**http** または **url** リテラルをポート 21 に使用できます。許可される値の範囲は 0 ～ 65535 です。
-port	（オプション）ポートの範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ActiveX オブジェクトは、保護されたネットワーク上のホストやサーバを攻撃することを目的としたコードを含んでいる場合があるため、セキュリティ リスクになる恐れがあります。**filter activex** コマンドを使用して、ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロールは、以前は OLE コントロールまたは OCX コントロールと呼ばれており、web ページまたは他のアプリケーションに挿入できるコンポーネントです。これらのコントロールには、情報の収集や表示に使用するためのカスタム フォームや、カレンダ、多数のサードパーティ

フォームがあります。技術としては、ActiveX には、ネットワーク クライアントに対して起こる可能性のある問題、たとえば、ワークステーション障害の発生、ネットワーク セキュリティ問題の導入、またはサーバへの攻撃というような問題が数多く生じています。

filter activex コマンドは、HTML Web ページ内でコメント アウトすることにより HTML <object> コマンドをブロックします。HTML ファイルの ActiveX フィルタリングは、<APPLET> と </APPLET> および <OBJECT CLASSID> と </OBJECT> タグをコメントで選択的に置き換えることにより実行されます。入れ子タグのフィルタリングは、トップ レベルのタグをコメントに変換することでサポートされています。

注意　<object> タグは、Java アプレット、イメージ ファイル、およびマルチメディア オブジェクトでも使用されますが、これらも、このコマンドによってブロックされます。

<object> タグまたは </object> HTML タグがネットワーク パケット間で分割されている場合、またはタグ内のコードが MTU 内のバイト数よりも長い場合、セキュリティ アプライアンスはタグをブロックできません。

ActiveX ブロッキングは、***alias*** コマンドで参照されている IP アドレスにユーザがアクセスした場合、または WebVPN トラフィックの場合は実行されません。

（注）　ポート 80 に対して **filter activex** コマンドを **inspect im** コマンドと共に設定すると、**inspect im** コマンドはディセーブルになります。

例

次の例では、すべての発信接続で Activex オブジェクトがブロックされるように指定します。

```
hostname(config)# filter activex 80 0 0 0 0
```

このコマンドは、ポート 80 上において、あらゆるローカル ホストから来て、あらゆる外部ホスト接続へ向かう Web トラフィックに ActiveX オブジェクトのブロッキングが適用されることを指定します。

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter ftp

Websense サーバまたは N2H2 サーバによりフィルタリングされる FTP トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter ftp** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter ftp <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

no filter ftp <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 21 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**ftp** リテラルを使用できます。
-port	（オプション）ポートの範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
allow	（オプション）サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 80（Web）トラフィックを、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、停止します。
interact-block	（オプション）ユーザが対話型の FTP プログラムを使用して FTP サーバに接続しないようにします。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

filter ftp コマンドは、Websense サーバまたは N2H2 サーバによってフィルタリングされる FTP トラフィックを特定します。

この機能をイネーブルにした後で、ユーザが FTP GET 要求をサーバに発行すると、セキュリティ アプライアンスは FTP サーバと Websense サーバまたは N2H2 サーバに同時に要求を送信します。Websense サーバまたは N2H2 サーバが接続を許可する場合、セキュリティ アプライアンスは正常な FTP の戻りコードが変更されずにユーザに到達することを許します。たとえば、正常な戻りコードは「250: CWD command successful」です。

Websense サーバまたは N2H2 サーバが接続を拒否する場合、セキュリティ アプライアンスは、FTP の戻りコードを接続が拒否されたことを表示するように変更します。たとえば、セキュリティ アプライアンスはコード 250 を「550 Requested file is prohibited by URL filtering policy」に変更します（Websense は FTP GET コマンドだけをフィルタリングし、PUT コマンドはフィルタリングしません）。

interactive-block オプションを使用して、ディレクトリ パス全体を提供しない対話型 FTP セッションを防ぎます。対話型 FTP クライアントでは、ユーザはパス全体を入力せずにディレクトリを変更できます。たとえば、ユーザは **cd /public/files** の代わりに **cd ./files** を入力する可能性があります。これらのコマンドを使用する前に、URL フィルタリング サーバを指定してイネーブルにする必要があります。

例

次の例は、FTP フィルタリングをイネーブルにする方法を示しています。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter ftp 21 0 0 0 0
hostname(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter https	Websense サーバまたは N2H2 サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter https

N2H2 サーバまたは Websense サーバによりフィルタリングされる HTTPS トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter https** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter https <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

no filter https <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 443 ですが、他の値でも受け入れられます。ポート 443 の代わりに、**https** リテラルを使用できます。
-port	（オプション）ポートの範囲を指定します。
except	（オプション）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
allow	（オプション）サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 443 トラフィックを、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、停止します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスは、外部 Websense または N2H2 フィルタリング サーバを使用して、HTTPS サイトおよび FTP サイトのフィルタリングをサポートします。

HTTPS フィルタリングは、サイトが許可されない場合に SSL 接続ネゴシエーションの完了を防ぐことにより動作します。ブラウザには、「The Page or the content cannot be displayed」などのエラーメッセージが表示されます。

HTTPS のコンテンツは暗号化されているため、セキュリティ アプライアンスはディレクトリおよびファイル名の情報なしで URL ルックアップを送信します。

例

次の例では、10.0.2.54 ホストからの接続を除く、すべての発信 HTTPS 接続をフィルタリングします。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter https 443 0 0 0 0
hostname(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter java

セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除するには、グローバル コンフィギュレーション モードで **filter java** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter java {[*port*[*-port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[*-port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

シンタックスの説明

port	フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**http** または **url** リテラルを使用できます。
port-port	（オプション）ポートの範囲を指定します。
except	（オプション）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

Java アプレットは、保護されたネットワーク上のホストやサーバを攻撃することを目的としたコードを含んでいる場合があるため、セキュリティ リスクになる恐れがあります。**filter java** コマンドを使用して、Java アプレットを削除できます。

filter java コマンドは、発信接続からセキュリティ アプライアンスに返る Java アプレットをフィルタリングします。ユーザは、引き続き HTML ページを受信できますが、アプレットに対する Web ページのソースがコメント アウトされるため、アプレットは実行できません。**filter java** コマンドは WebVPN トラフィックをフィルタリングしません。

applet または /applet HTML タグがネットワーク パケット間で分割されている場合、またはタグ内のコードが MTU 内のバイト数よりも長い場合、セキュリティ アプライアンスはタグをブロックできません。Java アプレットは、<object> タグに含まれていることが分かっていれば、**filter activex** コマンドを使用して削除します。

（注） ポート 80 に対して **filter java** コマンドを **inspect im** コマンドと共に設定すると、**inspect im** コマンドはディセーブルになります。

例

次の例では、すべての発信接続で Java アプレットがブロックされるように指定します。

```
hostname(config)# filter java 80 0 0 0 0
```

このコマンドは、ポート 80 上において、あらゆるローカル ホストから来て、あらゆる外部ホスト接続へ向かう Web トラフィックに Java ブロッキングが適用されることを指定します。

次の例では、保護されたネットワーク上のホストに Java アプレットをダウンロードすることをブロックします。

```
hostname(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

このコマンドは、ホスト 192.168.3.3 が Java アプレットをダウンロードしないようにします。

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter url

トラフィックを URL フィルタリング サーバに向けて送るには、グローバル コンフィギュレーション モードで **filter url** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

filter url <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url <*port*> [-<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

シンタックスの説明

allow	サーバが利用できなければ、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは発信ポート 80（Web）トラフィックを、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、停止します。
cgi_truncate	URL のパラメータ リストに CGI スクリプトなどの疑問符（?）から始まるリストがある場合は、疑問符を含む疑問符以降のすべての文字を削除することにより、フィルタリング サーバに送信された URL を切り捨てます。
except	先行の **filter** 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
http	ポート 80 を指定します（ポート 80 を示す 80 の代わりに **http** または **www** を入力できます）。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定して、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用して、すべてのホストを指定できます。
longurl-deny	URL が URL バッファ サイズの制限を超えている場合、または URL バッファが利用できない場合に、URL 要求を拒否します。
longurl-truncate	URL が URL バッファの制限を超えている場合、発信ホスト名または発信 IP アドレスだけを N2H2 または Websense サーバに送信します。
mask	任意のマスク。
-port	（オプション）フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 の代わりに、**http** または **url** リテラルを使用できます。ハイフンの後に 2 番目のポートを追加すると、オプションでポートの範囲を指定します。
proxy-block	ユーザが HTTP プロキシ サーバに接続できないようにします。
url	セキュリティ アプライアンスを通過するデータから URL をフィルタリングします。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**filter url** コマンドを使用することで、N2H2 または Websense フィルタリング アプリケーションを使用して指示した World Wide Web URL に、発信ユーザがアクセスしないようにします。

（注） **filter url** コマンドを実行するには、事前に **url-server** コマンドを設定する必要があります。

filter url コマンドの **allow** オプションは、N2H2 サーバまたは Websense サーバがオフラインになった場合のセキュリティ アプライアンスの動作を決定します。**filter url** コマンドで **allow** オプションを使用している場合、N2H2 サーバまたは Websense サーバがオフラインになると、ポート 80 トラフィックはフィルタリングなしでセキュリティ アプライアンスを通過します。**allow** オプションなしの場合、サーバがオフラインになると、セキュリティ アプライアンスはサーバがオンラインに戻るまで発信ポート 80（Web）のトラフィックを停止するか、または他の URL サーバが利用できる場合は、次の URL サーバに制御を渡します。

（注） **allow** オプションが設定されている場合、N2H2 サーバまたは Websense サーバがオフラインになると、セキュリティ アプライアンスは制御を代替サーバに渡します。

N2H2 サーバまたは Websense サーバは、セキュリティ アプライアンスと共に動作して、企業のセキュリティ ポリシーに基づいて、ユーザが Web サイトにアクセスすることを拒否します。

フィルタリング サーバの使用

Websense プロトコル Version 4 は、グループとユーザ名の認証を、ホストとセキュリティ アプライアンスの間でイネーブルにします。セキュリティ アプライアンスがユーザ名のルックアップを実行し、次に、Websense サーバが URL フィルタリングとユーザ名ロギングを処理します。

N2H2 サーバは、IFP Server を実行している Windows ワークステーション（2000、NT、または XP）であり、推奨する最小メモリとして 512 MB RAM を搭載している必要があります。また、N2H2 サービス用の長い URL のサポートは、Websense の上限よりも少ない 3 KB に制限されます。

Websense プロトコルの Version 4 には、次の機能拡張があります。

- URL フィルタリングを使用すると、セキュリティ アプライアンスは、発信 URL 要求を Websense サーバ上に定義されているポリシーと照合してチェックします。
- ユーザ名ロギングは、Websense サーバ上のユーザ名、グループ、およびドメイン名を追跡します。

- ユーザ名ルックアップを使用すると、セキュリティ アプライアンスがユーザ認証テーブルを使用して、ホストの IP アドレスをユーザ名にマッピングできます。

Websense に関する情報は、次の Web サイトで利用できます。

http://www.websense.com/

設定手順

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　N2H2 サーバまたは Websense サーバに **url-server** コマンドの該当するベンダー固有の形式を指示します。

ステップ 2　**filter** コマンドでフィルタリングをイネーブルにします。

ステップ 3　必要に応じて、**url-cache** コマンドを使用して、スループットを改善します。ただし、このコマンドは Websense ログをアップデートしないため、Websense アカウンティング レポートに影響を与える可能性があります。**url-cache** コマンドを使用する前に Websense 実行ログを集めます。

ステップ 4　**show url-cache statistics** コマンドおよび **show perfmon** コマンドを使用して、実行情報を表示します。

長い URL の扱い

Websense フィルタリング サーバでは最大 4 KB の URL、N2H2 フィルタリング サーバでは最大 3 KB の URL がサポートされています。

最大の許可サイズよりも長い URL 要求を処理できるようにするには、***longurl-truncate*** および ***cgi-truncate*** オプションを使用します。

最大サイズよりも URL が長い場合、**longurl-truncate** オプションまたは **longurl-deny** オプションがイネーブルになっていないと、パケットはセキュリティ アプライアンスによりドロップされます。

longurl-truncate オプションを使用すると、許可された最大長よりも URL が長い場合、セキュリティ アプライアンスは URL のホスト名または IP アドレスの部分だけを評価のためにフィルタリング サーバに送信します。許可された最大長よりも URL が長い場合に発信 URL トラフィックを拒否するには、**longurl-deny** オプションを使用します。

パラメータなしで CGI スクリプトの場所とスクリプト名だけが含まれるように CGI URL を切り捨てるには、**cgi-truncate** オプションを使用します。長い HTTP 要求の多くは CGI 要求です。パラメータ リストが非常に長い場合、パラメータ リストを含む完全な CGI 要求を待機および送信すると、メモリ リソースがすべて使われてセキュリティ アプライアンスのパフォーマンスに影響します。

HTTP 応答のバッファリング

デフォルトでは、ユーザが特定の Web サイトに接続する要求を発行すると、セキュリティ アプライアンスは Web サーバとフィルタリング サーバに同時に要求を送信します。フィルタリング サーバが Web コンテンツ サーバの前に応答しない場合、Web サーバからの応答はドロップされます。これが原因で、Web クライアントからは Web サーバの応答が遅れているように見えます。

HTTP 応答バッファをイネーブルにすることにより、Web コンテンツ サーバからの応答はバッファされ、フィルタリング サーバが接続を許可すると、応答は要求したユーザに転送されます。これにより、発生する可能性のある遅延を防ぎます。

HTTP の応答バッファをイネーブルにするには、次のコマンドを入力します。

url-block block *block-buffer-limit*

block-buffer をバッファされるブロックの最大数で置き換えます。許可される値は、1 ～ 128 で、一度にバッファされることが可能な 1,550 バイトのブロック数を指定します。

（注） ポート 80 に対して **filter url** コマンドを **inspect im** コマンドと共に設定すると、**inspect im** コマンドはディセーブルになります。

例

次の例では、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングします。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter url 80 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次の例では、ポート 8080 上でリッスンするプロキシ サーバに向かう発信 HTTP 接続をすべてブロックします。

```
hostname(config)# filter url 8080 0 0 0 0 proxy-block
```

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

fips enable

システムまたはモジュールで FIPS に準拠するためのポリシー チェックをイネーブルまたはディセーブルにするには、**fips enable** コマンドまたは [**no**] **fips enable** コマンドを使用します。

fips enable

[no] fips enable

シンタックスの説明

enable	FIPS に準拠するためのポリシー チェックをイネーブルまたはディセーブルします。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 準拠の動作モードで実行するには、**fips enable** コマンドと、セキュリティ ポリシーに指定された正しい設定との両方を適用する必要があります。内部 API は、実行時に正しい設定を強制するためにデバイスが移行することを許可します。

「fips enable」がスタートアップ コンフィギュレーションにある場合、FIPS POST が実行されて、次のコンソール メッセージが表示されます。

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set
forth in subparagraph (c) of the Commercial Computer Software - Restricted Rights
clause at FAR sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical
Data and Computer Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9

INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

例

```
sw8-ASA(config)# fips enable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

fips self-test poweron

パワーオン セルフテストを実行するには、**fips self-test powereon** コマンドを使用します。

fips self-test poweron

シンタックスの説明

poweron	パワーオン セルフテストを実行します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行すると、デバイスは FIPS 140-2 準拠に要求されるすべてのセルフテストを実行します。テストは、暗号アルゴリズム テスト、ソフトウェア整合性テスト、およびクリティカル機能テストで構成されています。

例

```
sw8-5520(config)# fips self-test poweron
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールで FIPS に準拠するためのポリシーチェックをイネーブルまたはディセーブルにします。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示します。

firewall transparent

ファイアウォール モードを透過モードに設定するには、グローバル コンフィギュレーション モードで **firewall transparent** コマンドを使用します。ルーテッド モードに戻すには、このコマンドの **no** 形式を使用します。透過的なファイアウォールは、「bump in the wire」または「stealth firewall」の機能を果たすレイヤ 2 のファイアウォールで、接続装置に対するルータ ホップとしては見られません。

firewall ***transparent***

no firewall ***transparent***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのファイアウォール モードだけを使用できます。システム コンフィギュレーションでモードを設定する必要があります。このコマンドは、情報提供だけを目的として各コンテキスト コンフィギュレーションでも表示されますが、コンテキストにこのコマンドを入力することはできません。

コマンドの多くは両方のモードではサポートされていないため、モードを変更すると、セキュリティ アプライアンスによってコンフィギュレーションが消去されます。データが入力されたコンフィギュレーションがある場合、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーションを作成するときに、このバックアップを参照として使用できます。

firewall transparent コマンドを使用してモードを変更するように設定されているセキュリティ アプライアンスに、テキスト コンフィギュレーションをダウンロードする場合は、そのコマンドをコンフィギュレーションの先頭に置くようにしてください。セキュリティ アプライアンスはコマンドを読み込むとすぐにモードを変更してから、ダウンロードしたコンフィギュレーションの読み込みを継続します。このコマンドがコンフィギュレーションの後ろの方に置かれていると、コンフィギュレーションでコマンドより前に置かれているラインはセキュリティ アプライアンスによりすべて消去されます。

例

次の例では、ファイアウォール モードを透過的なモードに変更します。

```
hostname(config)# firewall transparent
```

関連コマンド

コマンド	説明
arp-inspection	ARP 検査をイネーブルにして、ARP パケットをスタティック ARP エントリと比較します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show firewall	ファイアウォール モードを示します。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

format

すべてのファイルを消去してファイル システムをフォーマットするには、特権 EXEC モードで **format** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去し、ファイル システムを再インストールします。

format {**disk0: | disk1: | flash:**}

シンタックスの説明

disk0:	後ろにコロンを付けて内蔵フラッシュ メモリを指定します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロン (:) を入力します。
flash:	後ろにコロンを付けて内蔵フラッシュ メモリを指定します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

format コマンドは、指定されたファイル システム上のすべてのデータを消去し、デバイスに FAT 情報を再度書き込みます。

注意　***format*** コマンドは、破損したフラッシュ メモリをクリーン アップするのに必要な場合のみ、細心の注意を払って使用してください。

すべての可視ファイル（非表示のシステム ファイルを除く）を削除するには、***format*** コマンドではなく、***delete /recursive*** コマンドを使用します。

（注）　Cisco PIX セキュリティ アプライアンスでは、***erase*** コマンドと ***format*** コマンドは同じ処理を実行します。ユーザ データを 0xFF パターンを使用して破棄します。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** コマンドを入力してみてください。

(注) Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、***erase*** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、***format*** コマンドはファイル システムの制御構造をリセットするだけです。生ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** コマンドを入力してみてください。

例

この例は、フラッシュ メモリをフォーマットする方法を示しています。

```
hostname# format flash:
```

関連コマンド

コマンド	説明
delete	ユーザから見えるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
fsck	破損したファイル システムを修復します。

forward interface

スイッチが組み込まれたモデル（ASA 5505 適応型セキュリティ アプライアンスなど）では、インターフェイス コンフィギュレーション モードで **no forward interface** コマンドを使用して、あるVLAN が別の VLAN にアクセスすることを制限します。このコマンドを入力できるのは、VLAN インターフェイスのインターフェイス コンフィギュレーション モードだけです。接続できるように戻すには、**forward interface** コマンドを使用します。ライセンスによってサポートされる VLAN の数によっては、1 つの VLAN だけに制限しなければならないことがあります。

forward interface vlan *number*

no forward interface vlan *number*

シンタックスの説明

vlan *number*	この VLAN インターフェイスがトラフィックを開始できない VLAN ID を指定します。

デフォルト

デフォルトでは、すべてのインターフェイスは他のいずれのインターフェイスに対してもトラフィックを開始できます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ルーテッド モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスの場合、アクティブな VLAN を 3 つまで、Security Plus ライセンスの場合は 5 つまで設定できます。アクティブな VLAN とは、**nameif** コマンドが設定されている VLAN です。どちらのライセンスでも、非アクティブな VLAN を ASA 5505 適応型セキュリティ アプライアンス上に 5 つまで設定できますが、それらの VLAN をアクティブにする場合は、ライセンスに関する次のガイドラインを遵守してください。

Base ライセンスの場合、3 つ目の VLAN を **no forward interface** コマンドで設定し、この VLAN による別の VLAN へのアクセスを制限する必要があります。

たとえば、インターネット アクセス用に外部に割り当てた VLAN が 1 つ、内部ワーク ネットワーク用に割り当てた VLAN が 1 つ、さらにホームネットワーク用に割り当てた 3 つ目の VLAN があるとします。ホーム ネットワークはワーク ネットワークにアクセスする必要はありません。そのためホーム VLAN には **no forward interface** コマンドを使用します。ワーク ネットワークはホームネットワークにアクセスできますが、ホームネットワークはワーク ネットワークにアクセスできません。

nameif コマンドで設定した VLAN インターフェイスがすでに 2 つある場合、**no forward interface** コマンドを入力してから、3 つ目のインターフェイスで **nameif** コマンドを入力します。セキュリティ アプライアンスでは、ASA 5505 適応型セキュリティ アプライアンスで Base ライセンスの場合、3 つの VLAN インターフェイスが完全に機能することを許可しません。

例

次の例では、3 つの LAN インターフェイスを設定しています。3 つ目のホーム インターフェイスはトラフィックをワーク インターフェイスに転送できません。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
backup interface	たとえば、インターフェイスをバックアップ リンクとして ISP に割り当てます。
clear interface	**show interface** コマンドのカウンタを消去します。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。

fqdn

登録中に、指定された FQDN を証明書のサブジェクト代替名の拡張に含めるには、暗号 CA トラストポイント コンフィギュレーション モードで **fqdn** コマンドを使用します。fqdn のデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

fqdn [*fqdn* | **none**]

no fqdn

シンタックスの説明

fqdn	完全修飾ドメイン名を指定します。*fqdn* の最大長は 64 文字です。
none	非完全修飾ドメイン名を指定します。

デフォルト

デフォルト設定では、FQDN は含まれません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

証明書を使用する Nokia VPN クライアントの認証をサポートするセキュリティ アプライアンスを設定する場合、**none** キーワードを使用します。Nokia VPN クライアントの証明書認証に関する詳細は、**crypto isakmp identity** コマンドまたは **isakmp identity** コマンドを参照してください。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、トラストポイント central の登録要求に FQDN エンジニアリングを含めます。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# fqdn engineering
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求の送信を試行するまでの待機時間を、分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

fragment

特別なパケット フラグメント化の管理を提供して NFS との互換性を向上させるには、グローバル コンフィギュレーション モードで **fragment** コマンドを使用します。

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} *interface*

シンタックスの説明

chain *limit*	完全な IP パケットがフラグメント化されるパケット数の最大値を示す。
interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。インターフェイスが指定されていなければ、このコマンドはすべてのインターフェイスに適用されます。
size *limit*	再構成のために待機している IP 再構成データベースに含めることができる、パケットの最大数を設定します。
timeout *limit*	フラグメント化されたパケット全体の到着を待つ最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着すると始動します。指定した秒数以内にパケットのすべてのフラグメントが到着しない場合、それまでに受信したパケット フラグメントはすべて廃棄されます。

デフォルト

デフォルトは次のとおりです。

- ***chain*** は 24 パケットです。
- *interface* はすべてのインターフェイスです。
- ***size*** は 200 です。
- ***timeout*** は 5 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、***chain***、***size***、または ***timeout*** のいずれかの引数を必ず選択するように変更されました。ソフトウェアの以前のリリースでサポートされていた、これらの引数を入力しない ***fragment*** コマンドは、入力できなくなりました。

使用上のガイドライン

デフォルトでは、セキュリティ アプライアンスは、完全な IP パケットの再構築をするために、最大 24 個のフラグメントを受け入れます。ネットワーク セキュリティ ポリシーに基づいて、各インターフェイスについて **fragment chain 1** *interface* コマンドを入力することで、フラグメント化されたパケットがセキュリティ アプライアンスを通過できなくするようにセキュリティ アプライアンスの設定を検討する必要があります。制限に 1 を設定すると、すべてのパケットが元のまま、つまり、フラグメント化されていない状態である必要があります。

セキュリティ アプライアンスを通過するネットワーク トラフィックのほとんどが NFS である場合、データベースのオーバーフローを防ぐため、さらに調整が必要になる可能性があります。

WAN インターフェイスなどのように NFS サーバとクライアントの間の MTU サイズが小さな環境では、**chain** キーワードをさらに調整する必要があります。この場合、効率を改善するには NFS over TCP の使用を推奨します。

size *limit* に大きな値を設定すると、セキュリティ アプライアンスは、さらにフラグメント フラッディングによる DoS 攻撃を受けやすくなります。***size limit*** に 1550 プールまたは 16384 プール内のブロックの総数以上の値を設定しないでください。

デフォルト値では、フラグメント フラッディングによって発生する DoS 攻撃が制限されます。

例

次の例は、フラグメント化したパケットを外部および内部のインターフェイスで防ぐ方法を示しています。

```
hostname(config)# fragment chain 1 outside
hostname(config)# fragment chain 1 inside
```

パケットのフラグメント化をさせない追加インターフェイスそれぞれに対して、続けて **fragment chain 1** *interface* コマンドを入力します。

次の例では、外部インターフェイスのフラグメント データベースを、最大サイズ 2000、最大チェイン長 45、待ち時間 10 秒に設定する方法を示しています。

```
hostname(config)# fragment size 2000 outside
hostname(config)# fragment chain 45 outside
hostname(config)# fragment timeout 10 outside
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの運用データを消去します。
show fragment	IP フラグメント再構成モジュールの運用データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

frequency

選択した SLA オペレーションが繰り返される頻度を設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **frequency** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

frequency *seconds*

no frequency

シンタックスの説明

seconds	SLA プローブ間の秒数。有効な値は 1 ～ 604,800 秒です。この値は **timeout** 値未満にはできません。

デフォルト

デフォルトの間隔は 60 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

SLA オペレーションは動作中、指定の頻度で繰り返し実行されます。たとえば、60 秒の頻度に設定した ***ipIcmpEcho*** オペレーションは動作中、エコー要求パケットの送信を 60 秒ごとに 1 度繰り返し実行します。たとえば、エコー オペレーションのデフォルトのパケット数は 1 です。このパケットは、オペレーションの開始時に送信され、60 秒後に再度送信されます。

個々の SLA オペレーションで、指定した頻度値より実行に時間がかかる場合、busy という統計カウンタの値が増え、オペレーションはすぐに繰り返されません。

frequency コマンドに指定する値は、**timeout** コマンドに指定した値未満にはできません。

例

次の例では、ID が 123 の SLA オペレーションを設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA オペレーションの頻度は 3 秒、タイムアウト値は 1000 ミリ秒に設定されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA 監視オペレーションを定義します。
timeout	SLA オペレーションが応答を待機する期間を定義します。

fsck

ファイル システムのチェックを実行し、破損を修復するには、特権 EXEC モードで **fsck** コマンドを使用します。

fsck [/no confirm]{disk0: | disk1: | flash:}

シンタックスの説明

/noconfirm	オプション。修復確認のためのプロンプトを表示しません。
disk0:	後ろにコロンを付けて内蔵フラッシュ メモリを指定します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロン (:) を入力します。
flash:	後ろにコロンを付けて内蔵フラッシュ メモリを指定します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

fsck コマンドは破損したファイル システムをチェックし、修復を試みます。他の方法を用いる前に、まずこのコマンドを使用してください。

/noconfirm キーワードは、最初に確認を求めずに破損を自動的に修復します。

例

次の例では、フラッシュ メモリのファイル システムのチェック方法を示しています。

```
hostname# fsck flash:
```

関連コマンド

コマンド	説明
delete	ユーザから見えるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
format	ファイル システム上にある非表示のシステム ファイルを含むすべてのファイルを削除し、ファイル システムを再インストールします。

ftp mode passive

FTP モードをパッシブに設定するには、グローバル コンフィギュレーション モードで **ftp mode passive** コマンドを使用します。FTP クライアントをアクティブ モードにリセットするには、このコマンドの **no** 形式を使用します。

ftp mode passive

no ftp mode passive

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ftp mode passive コマンドは、FTP モードをパッシブに設定します。セキュリティ アプライアンスは、イメージ ファイルまたはコンフィギュレーション ファイルの FTP サーバへのアップロードや FTP サーバからのダウンロードに FTP を使用できます。**ftp mode passive** コマンドは、セキュリティ アプライアンス上の FTP クライアントが FTP サーバと対話する方法を設定します。

パッシブ FTP では、クライアントが制御接続とデータ接続の両方を開始します。パッシブ モードはサーバ状態を参照します。つまり、サーバは、クライアントによって開始された制御接続とデータ接続の両方を受動的に受け入れます。

パッシブ モードでは、宛先ポートと送信元ポートの両方が一時ポートです（1023 より大きい）。クライアントが **passive** コマンドを発行してパッシブなデータ接続の設定を開始するため、このモードはクライアントにより設定されます。パッシブ モードでのデータ接続の受信者であるサーバは、特定の接続をリッスンしているポート番号で応答します。

例

次の例では、FTP モードをパッシブに設定します。

```
hostname(config)# ftp mode passive
```

関連コマンド

copy	イメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。
debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

functions

このユーザまたはグループ ポリシーに対して、WebVPN 経由でポート フォワーディング java アプレット、Citrix サポート、ファイル アクセス、ファイル ブラウジング、ファイル サーバ エントリ、webtype ACL のアプリケーション、HTTP プロキシ、MAPI プロキシ、ポート フォワーディング、または URL エントリに関する自動ダウンロードを設定するには、グループ ポリシーまたはユーザ名モードから入力する webvpn モードで **functions** コマンドを使用します。設定済み機能を削除するには、このコマンドの **no** 形式を使用します。

functions none コマンドを発行して作成されたヌル値を含むすべての設定済み機能を削除するには、このコマンドの **no** 形式を引数なしで使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。機能の値を継承しないようにするには、**functions none** コマンドを使用します。

functions {**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **http-proxy** | **url-entry** | **mapi** | **port-forward** | **none**}

no functions [**auto-download** | **citrix** | **file-access** | **file-browsing** | **file-entry** | **filter** | **url-entry** | **mapi** | **port-forward**]

シンタックスの説明

auto-download	WebVPN ログインの際に、ポート フォワーディング java アプレットの自動ダウンロードをイネーブルまたはディセーブルにします。最初にポート フォワーディング、Outlook/Exchange プロキシ、または HTTP プロキシをイネーブルにする必要があります。
citrix	MetaFrame アプリケーション サーバからリモート ユーザへの端末サービスのサポートを、イネーブルまたはディセーブルにします。このキーワードを使用すると、セキュリティ アプライアンスがセキュリティの高い Citrix コンフィギュレーション内でセキュアなゲートウェイとして動作できます。これらのサービスにより、ユーザは標準の Web ブラウザから MetaFrame アプリケーションにアクセスできます。
file-access	ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルの場合、WebVPN のホームページにはサーバ リスト内のファイル サーバが一覧表示されます。ファイル ブラウジングまたはファイル エントリをイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイル サーバおよび共有のブラウジングをイネーブルまたはディセーブルにします。ファイル サーバのユーザ エントリを許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ファイル サーバの名前を入力するユーザ機能をイネーブルまたはディセーブルにします。
filter	webtype ACL を適用します。イネーブルにすると、セキュリティ アプライアンスは webvpn の **filter** コマンドで定義された webtype ACL を適用します。
http-proxy	リモート ユーザへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。プロキシは、Java、ActiveX、および Flash などの独特のマングリングに干渉するテクノロジーに効果的です。プロキシを使用するとマングリングはバイパスされますが、セキュリティ アプライアンスの使用は確実に継続されます。転送されたプロキシはブラウザの古いプロキシ設定を自動的に変更し、すべての HTTP および HTTPS 要求を新しいプロキシ設定にリダイレクトします。HTML、CSS、JavaScript、VBScript、ActiveX、および Java を含む、すべてのクライアント側のテクノロジーを実質的にサポートします。サポートしているブラウザは、Microsoft Internet Explorer だけです。

mapi	Microsoft Outlook/Exchange のポート転送をイネーブルまたはディセーブルにします。
none	すべての WebVPN **functions** にヌル値を設定します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから機能を継承しないようにします。
port-forward	ポート転送をイネーブルにします。イネーブルにすると、セキュリティ アプライアンスは webvpn の **port-forward** コマンドで定義されたポート フォワーディング リストを使用します。
url-entry	URL のユーザ エントリをイネーブルまたはディセーブルにします。イネーブルになっても、セキュリティ アプライアンスは依然として URL を任意の設定された URL またはネットワーク ACL に制限します。URL エントリをディセーブルにすると、セキュリティ アプライアンスは WebVPN ユーザをホームページ上の URL に制限します。

デフォルト

デフォルトでは、この機能はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	auto-download キーワードと citrix キーワードが追加されました。
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup という名前のグループ ポリシーに対してファイル アクセス、ファイル ブラウジング、および MAPI プロキシを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions file-access file-browsing MAPI
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

CHAPTER 13

gateway コマンド～ hw-module module shutdown コマンド

gateway

特定のゲートウェイを管理しているコール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **gateway** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

gateway *ip_address* [*group_id*]

シンタックスの説明

gateway	特定のゲートウェイを管理しているコール エージェントのグループを指定します。
ip_address	ゲートウェイの IP アドレス。
group_id	コール エージェント グループの ID（0 ～ 2147483647）。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

gateway コマンドは、特定のゲートウェイを管理しているコール エージェントのグループを指定するために使用します。*ip_address* オプションを使用して、ゲートウェイの IP アドレスを指定します。*group_id* オプションは 0 ～ 4294967295 の数字です。この数字は、ゲートウェイを管理しているコール エージェントの *group_id* に対応している必要があります。1 つのゲートウェイは 1 つのグループだけに所属できます。

例

次の例では、コール エージェント 10.10.11.5 と 10.10.11.6 がゲートウェイ 10.10.10.115 を制御できるようにし、コール エージェント 10.10.11.7 と 10.10.11.8 がゲートウェイ 10.10.10.116 と 10.10.10.117 の両方を制御できるようにしています。

```
hostname(config)# mgcp-map mgcp_policy
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP に関するデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッション情報を表示します。

global

NAT 用のマッピング アドレスのプールを作成するには、グローバル コンフィギュレーション モードで **global** コマンドを使用します。アドレスのプールを削除するには、このコマンドの **no** 形式を使用します。

global (*mapped_ifc) nat_id* {*mapped_ip*[*-mapped_ip*] [**netmask** *mask*] | **interface**}

no global (*mapped_ifc) nat_id* {*mapped_ip*[*-mapped_ip*] [**netmask** *mask*] | **interface**}

シンタックスの説明

interface	インターフェイスの IP アドレスを、マッピング アドレスとして使用します。このキーワードを使用するのは、インターフェイス アドレスを使用しようとする場合に、アドレスが DHCP を使用して動的に割り当てられているときです。
mapped_ifc	マッピング IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
mapped_ip[*-mapped_ip*]	マッピングされているインターフェイスの終了時に実際のアドレスを変換する場合の変換先マッピング アドレス（複数可）を指定します。単一のアドレスを指定する場合は、PAT を設定します。アドレスの範囲を指定する場合は、ダイナミック NAT を設定します。 外部ネットワークがインターネットに接続されている場合は、各グローバル IP アドレスが Network Information Center（NIC）に登録されている必要があります。
nat_id	NAT ID の整数を指定します。この ID は、変換対象の実際のアドレスにマッピング プールを関連付けるときに **nat** コマンドによって参照されます。 通常の NAT の場合、この整数の範囲は 1 ～ 2147483647 となります。ポリシー NAT（**nat id access-list**）の場合、整数の範囲は 1 ～ 65535 となります。 **global** コマンドで NAT ID に 0 を指定しないでください。0 は、**global** コマンドを使用しないアイデンティティ NAT および NAT 免除用に予約されています。
netmask *mask*	（オプション）*mapped_ip* のネットワーク マスクを指定します。このマスクは、*mapped_ip* と組み合せた場合、ネットワークを指定しません。この場合は、*mapped_ip* をホストに割り当てるときに mapped_ip に割り当てたサブネット マスクを指定します。アドレスの範囲を設定する場合は、*mapped_ip-mapped_ip* を指定する必要があります。 マスクを指定しない場合は、アドレス クラスのデフォルト マスクが使用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ダイナミック NAT および PAT の場合は、最初に、変換対象となるインターフェイス上の実際のアドレスを指定する **nat** コマンドを設定します。次に、別のインターフェイスの終了時にマッピング アドレスを指定するための **global** コマンドを別途設定します（PAT の場合、マッピング アドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てられた番号である NAT ID の比較によって、**global** コマンドと一致します。

ダイナミック NAT および PAT の詳細については、**nat** コマンドを参照してください。

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするのを待たずに新しい NAT 情報を使用するときは、**clear xlate** コマンドを使用して変換テーブルを消去してもかまいません。ただし、変換テーブルを消去すると現在の接続がすべて切断されます。

例

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスと共に指定するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

関連コマンド

コマンド	説明
clear configure global	**global** コマンドをコンフィギュレーションから削除します。
nat	変換対象となる実際のアドレスを指定します。
show running-config global	コンフィギュレーション内の **global** コマンドを表示します。
static	1 対 1 の変換を設定します。

group

IKE ポリシーの Diffie-Hellman グループを指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **group** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。Diffie-Hellman グループ識別子をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

group {**1** | **2** | **5** | **7**}

no group

シンタックスの説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。768 ビットは、デフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1,536 ビットの Diffie-Hellman グループ 5 が使用されるように指定します。
group 7	IKE ポリシーで、Diffie-Hellman Group 7 を使用することを指定します。Group 7 は IPSec SA キーを生成します。楕円曲線フィールドのサイズは 163 ビットです。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトのグループ ポリシーは、group 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 isakmp ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy group** コマンドが導入されました。
7.2.(1)	**isakmp policy group** コマンドが、**group** コマンドに置き換えられました。

使用上のガイドライン

グループ オプションには、768 ビット（DH Group 1）、1,024 ビット（DH Group 2）、1,536 ビット（DH Group 5）、および DH Group 7 の 4 つがあります。1,024 ビットと 1,536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注） Cisco VPN クライアントのバージョン 3.x 以上では、ISAKMP ポリシーで DH グループ 2 を使用する必要があります（DH グループ 1 に設定すると接続できません）。

AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES のキーのサイズは非常に大きいので、ISAKMP ネゴシエーションで Diffie-Hellman（DH）グループ 1 や 2 ではなく、グループ 5 を使用する必要があります。この設定を行うには、**group 5** コマンドを使用します。

例

次の例は、グローバル コンフィギュレーション モードで、**group** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに、グループ 2、1024 ビット Diffie Hellman を使用するように設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# group 2
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

group-alias

ユーザがトンネル グループを参照できるように 1 つまたは複数の代替名を作成するには、トンネル グループ webvpn コンフィギュレーション モードで **group-alias** コマンドを使用します。リストからエイリアスを削除するには、このコマンドの **no** 形式を使用します。

group-alias *name* [***enable*** | ***disable]***

no group-alias *name*

シンタックスの説明

disable	グループ エイリアスをディセーブルにします。
enable	以前にディセーブルにしたグループ エイリアスをイネーブルにします。
name	トンネル グループ エイリアスの名前を指定します。名前には、スペースは使用できませんが、それ以外は任意の文字列を選択できます。

デフォルト

デフォルトのグループ エイリアスはありませんが、グループ エイリアスを指定すると、そのエイリアスがデフォルトでイネーブルになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ここで指定したグループ エイリアスは、ログイン ページのドロップダウン リストに表示されます。各グループはエイリアスを複数持ってもよいし、まったく持たなくてもかまいません。このコマンドは、同じグループが「Devtest」や「QA」などの複数の通常名で知られている場合に有用です。

例

次の例は、「devtest」という名前の webvpn トンネル グループを設定し、そのグループに対してエイリアス「QA」および「Fra-QA」を確立するコマンドを示しています。

```
hostname(config)# tunnel-group devtest type webvpn
hostname(config)# tunnel-group devtest webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias QA
hostname(config-tunnel-webvpn)# group-alias Fra-QA
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または名前の付いたトンネル グループ コンフィギュレーションを消去します。
show webvpn group-alias	指定したトンネル グループまたはすべてのトンネル グループに対するエイリアスを表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定するトンネル グループ webvpn コンフィギュレーション モードに入ります。

group-delimiter

グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定するには、グローバル コンフィギュレーション モードで **group-delimiter** コマンドを使用します。このグループ名の解析をディセーブルにするには、このコマンドの **no** 形式を使用します。

group-delimiter *delimiter*

no group-delimiter

シンタックスの説明

delimiter	グループ名のデリミタとして使用する文字を指定します。 有効値は、**@**、**#**、および **!** です。

デフォルト

デフォルトでは、デリミタは指定されておらず、グループ名の解析はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このデリミタは、トンネルのネゴシエーション中に、ユーザ名からトンネル グループ名を解析するために使用されます。デフォルトでは、デリミタは指定されておらず、グループ名の解析はディセーブルになっています。

例

次の例は、グループ デリミタを番号記号（#）に変更するための **group-delimiter** コマンドを示しています。

```
hostname(config)# group-delimiter #
```

関連コマンド

コマンド	説明
clear config group-delimiter	設定済みのグループ デリミタを消去します。
show running-config group-delimiter	現在の group-delimiter の値を表示します。
strip-group	strip-group の処理をイネーブルまたはディセーブルにします。

group-lock

リモート ユーザがトンネル グループだけからアクセスできるようにするには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **group-lock** コマンドを発行します。

group-lock アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループ ポリシーから継承できます。group-lock をディセーブルにするには、**group-lock none** コマンドを使用します。

group-lock はユーザを制限するときに、VPN Client に設定されているグループが、ユーザの割り当て先のトンネル グループと同じかどうかを確認します。同じでない場合、セキュリティ アプライアンスは、ユーザが接続できないようにします。group-lock を設定しない場合、セキュリティ アプライアンスは割り当てられているグループを考慮せずにユーザを認証します。

group-lock {value *tunnel-grp-name* **| none}**

no group-lock

シンタックスの説明

none	group-lock をヌル値に設定して、group-lock の制限を拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから group-lock の値を継承しないようにします。
value *tunnel-grp-name*	接続しようとするユーザ用にセキュリティ アプライアンスが必要とする既存のトンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup というグループ ポリシーにグループ ロックを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# group-lock value tunnel group name
```

group-object

ネットワーク オブジェクト グループを追加するには、プロトコル、ネットワーク、サービス、および icmp-type コンフィギュレーション モードで **group-object** コマンドを使用します。ネットワーク オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

group-object *obj_grp_id*

no group-object *obj_grp_id*

シンタックスの説明

obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。アルファベット、数字、アンダースコア（_）、ハイフン（-）、およびピリオド（.）を任意に組み合せることができます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プロトコル、ネットワーク、サービス、および icmp-type コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

group-object コマンドは、**object-group** コマンドと組み合せることで、それ自身がオブジェクト グループであるオブジェクトを定義します。このコマンドは、プロトコル、ネットワーク、サービス、および icmp-type コンフィギュレーション モードで使用されます。このサブコマンドを使用すると、同じタイプのオブジェクトを論理的にグループ化することや、構造化コンフィギュレーションの階層型オブジェクト グループを構築することができます。

グループ オブジェクトに限り、オブジェクトをオブジェクト グループ内で重複させることができます。たとえば、オブジェクト 1 がグループ A とグループ B の両方にある場合、A と B を両方含むグループ C を定義できます。ただし、グループ オブジェクトに含めることによってグループ階層が循環型になる場合は、含めることができません。たとえば、グループ A をグループ B に含め、同時にグループ B をグループ A に含めることはできません。

階層型オブジェクト グループの最大許容レベルは 10 です。

例

次の例は、ホストを重複させる必要がなくなるように、ネットワーク コンフィギュレーション モードで **group-object** コマンドを使用する方法を示しています。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit
hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit
hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit
hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)# access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)# access-list all permit tcp object-group all-hosts any eq w
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

group-policy

グループ ポリシーを作成または編集するには、グローバル コンフィギュレーション モードで **group-policy** コマンドを使用します。グループ ポリシーをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

group-policy *name* {**internal [from** *group-policy_name*] | **external server-group** *server_group* **password** *server_password*}

no group-policy *name*

シンタックスの説明

external server-group *server_group*	グループ ポリシーを外部として指定し、セキュリティ アプライアンスがアトリビュートをクエリーするための AAA サーバ グループを指定します。
from *group-policy_name*	この内部グループ ポリシーのアトリビュートを、既存のグループ ポリシーの値に初期化します。
internal	グループ ポリシーを内部として指定します。
name	グループ ポリシーの名前を指定します。この名前は最大 64 文字です。スペースを含めることはできません。
password *server_password*	外部 AAA サーバ グループからアトリビュートを取得するときに使用するパスワードを指定します。このパスワードは最大 128 文字です。スペースを含めることはできません。

デフォルト

デフォルトの動作や値はありません。使用上のガイドラインを参照してください。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

「DefaultGroupPolicy」というデフォルトのグループ ポリシーは、常にセキュリティ アプライアンス上に存在します。しかし、このデフォルトのグループ ポリシーを有効にするには、このポリシーを使用するようにセキュリティ アプライアンスを設定する必要があります。設定方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

group-policy attributes コマンドを使用して、任意のグループ ポリシー アトリビュート値ペアを設定できる config-group-policy モードに入ります。DefaultGroupPolicy には、次のアトリビュート値ペアが含まれています。

アトリビュート	デフォルト値
backup-servers	keep-client-config
banner	none
client-access-rules	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

さらに、config-group-policy モードで **webvpn** コマンドを入力するか、**group-policy attributes** コマンドを入力した後、config-group-webvpn モードで **webvpn** コマンドを入力することで、グループ ポリシーに対する webvpn-mode アトリビュートが設定できます。詳細については、**group-policy attributes** コマンドの説明を参照してください。

例

次の例は、「FirstGroup」という内部グループ ポリシーを作成する方法を示しています。

```
hostname(config)# group-policy FirstGroup internal
```

次の例は、「ExternalGroup」という外部グループ ポリシー、「BostonAAA」という AAA サーバ グループ、および「12345678」というパスワードを作成する方法を示しています。

```
hostname(config)# group-policy ExternalGroup external server-group BostonAAA password
12345678
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	config-group-policy モードに入ります。このモードでは、指定したグループ ポリシーのアトリビュートと値を設定したり、グループの webvpn アトリビュートを設定する webvpn モードに入ったりできます。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	config-group-webvpn モードに入ります。このモードで、指定したグループに対する WebVPN アトリビュートを設定できます。

group-policy attributes

config-group-policy モードに入るには、グローバル コンフィギュレーション モードで **group-policy attributes** コマンドを使用します。グループ ポリシーからすべてのアトリビュートを削除するには、このコマンドの **no** 形式を使用します。config-group-policy モードで、指定したグループ ポリシーのアトリビュート値ペアの設定、またはグループ ポリシー webvpn コンフィギュレーション モードでのグループの webvpn アトリビュートの設定ができます。

group-policy *name* **attributes**

no group-policy *name* **attributes**

シンタックスの説明

name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

アトリビュート モードのコマンドのシンタックスには、共通する次の特性があります。

- **no** 形式は、アトリビュートを実行コンフィギュレーションから削除し、値を別のグループ ポリシーから継承できるようにします。
- **none** キーワードは、実行コンフィギュレーションのアトリビュートをヌル値に設定して、値を継承できないようにします。
- ブール アトリビュートには、イネーブルまたはディセーブルになっている設定のための明示的なシンタックスがあります。

DefaultGroupPolicy という名前のデフォルト グループ ポリシーは、常にセキュリティ アプライアンスに存在します。しかし、このデフォルトのグループ ポリシーを有効にするには、このポリシーを使用するようにセキュリティ アプライアンスを設定する必要があります。設定方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

group-policy attributes コマンドは、任意のグループ ポリシー アトリビュート値ペアを設定できる config-group-policy モードに入ります。DefaultGroupPolicy には、次のアトリビュート値ペアが含まれています。

アトリビュート	デフォルト値
backup-servers	keep-client-config
banner	none
client-access-rule	none
client-firewall	none
default-domain	none
dns-server	none
group-lock	none
ip-comp	disable
ip-phone-bypass	disabled
ipsec-udp	disabled
ipsec-udp-port	10000
leap-bypass	disabled
nem	disabled
password-storage	disabled
pfs	disable
re-xauth	disable
secure-unit-authentication	disabled
split-dns	none
split-tunnel-network-list	none
split-tunnel-policy	tunnelall
user-authentication	disabled
user-authentication-idle-timeout	none
vpn-access-hours	unrestricted
vpn-filter	none
vpn-idle-timeout	30 minutes
vpn-session-timeout	none
vpn-simultaneous-logins	3
vpn-tunnel-protocol	IPSec WebVPN
wins-server	none

さらに、**group-policy attributes** コマンドを入力した後、config-group-policy モードで **webvpn** コマンドを入力することで、グループ ポリシーの webvpn-mode アトリビュートが設定できます。詳細については、**webvpn** コマンド（グループ ポリシー アトリビュートおよびユーザ名アトリビュート モード）の説明を参照してください。

例

次の例は、FirstGroup というグループ ポリシーのグループ ポリシー アトリビュート モードに入る方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy	グループ ポリシーを作成、編集、または削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn（グループ ポリシー アトリビュート モード）	config-group-webvpn モードに入ります。このモードで、指定したグループに対する WebVPN アトリビュートを設定できます。

group-prompt

WebVPN ユーザに対して、セキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログイン ボックスのグループ プロンプトをカスタマイズするには、webvpn カスタマイゼーション モードで **group-prompt** コマンドを使用します。

group-prompt {**text** | **style**} *value*

[**no**] **group-prompt** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

グループ プロンプトのデフォルトのテキストは「GROUP:」です。

グループ プロンプトのデフォルトのスタイルは、color:black;font-weight:bold;text-align:right です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、テキストを「Corporate Group:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更しています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# group-prompt text Corporate Group:
F1-asa1(config-webvpn-custom)# group-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページのユーザ名プロンプトをカスタマイズします。

group-url

グループに対する着信 URL または IP アドレスを指定するには、トンネル グループ WebVPN コンフィギュレーション モードで **group-url** コマンドを使用します。リストから URL を削除するには、このコマンドの **no** 形式を使用します。

group-url *url* [**enable** | **disable**]

no group-url *url*

シンタックスの説明

disable	URL をディセーブルにしますが、リストから削除はしません。
enable	URL をイネーブルにします。
url	このトンネル グループの URL または IP アドレスを指定します。

デフォルト

デフォルトの URL または IP アドレスはありませんが、URL または IP アドレスを指定すると、デフォルトでイネーブルになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

グループ URL または IP アドレスを指定することで、ログイン時にユーザがグループを選択する必要がなくなります。ユーザがログインすると、セキュリティ アプライアンスは tunnel-group-policy テーブル内のユーザの着信 URL またはアドレスを探します。着信 URL またはアドレスが検出され、さらにトンネル グループで group-url がイネーブルである場合、セキュリティ アプライアンスは関連するトンネル グループを自動的に選択し、ユーザに対してログイン ウィンドウでユーザ名フィールドとパスワード フィールドだけを表示します。このように表示することで、ユーザ インターフェイスが簡素化され、グループのリストがユーザの目に触れないようになるという利点が加わります。ユーザが見るログイン ウィンドウは、トンネル グループに対して設定されたカスタマイゼーションを使用します。

着信 URL またはアドレスがディセーブルで、グループ エイリアスが設定されている場合、グループのドロップダウン リストも表示されるので、ユーザは選択を行う必要があります。

1 つのグループに対して、複数の URL またはアドレスが設定できます（あるいは、何も設定しなくてもかまいません）。各 URL またはアドレスは、個別にイネーブルまたはディセーブルにできます。指定した URL およびアドレスそれぞれに対して、別個の **group-url** コマンドを使用する必要があります。http プロトコルか https プロトコルを含む、URL 全体またはアドレス全体を指定してください。

同じ URL およびアドレスを、複数のグループに関連付けることはできません。セキュリティ アプライアンスは、トンネル グループに対する URL またはアドレスを受け入れる前に、URL およびアドレスの一意性を確認します。

次の例は、「test」という名前の webvpn トンネル グループを設定し、そのグループに対して 2 つのグループ URL、「http://www.cisco.com」および「https://supplier.com」を確立するコマンドを示しています。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com
hostname(config-tunnel-webvpn)# group-url https://supplier.company.com
hostname(config-tunnel-webvpn)#
```

次の例では、RadiusServer という名前のトンネル グループに対してグループ URL の http://www.cisco.com および http://192.168.10.10 をイネーブルにします。

```
hostname(config)# tunnel-group RadiusServer type webvpn
hostname(config)# tunnel-group RadiusServer general-attributes
hostname(config-tunnel-general)# authentication server-group RADIUS
hostname(config-tunnel-general)# accounting-server-group RADIUS
hostname(config-tunnel-general)# tunnel-group RadiusServer webvpn-attributes
hostname(config-tunnel-webvpn)# group-alias "Cisco Remote Access" enable
hostname(config-tunnel-webvpn)# group-url http://www.cisco.com enable
hostname(config-tunnel-webvpn)# group-url http://192.168.10.10 enable
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または名前の付いたトンネル グループ コンフィギュレーションを消去します。
show webvpn group-url	指定したトンネル グループまたはすべてのトンネル グループに対する URL を表示します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

h245-tunnel-block

H.323 の H.245 トンネリングをブロックするには、パラメータ コンフィギュレーション モードで **h245-tunnel-block** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

h245-tunnel-block action [drop-connection | log]

no h245-tunnel-block action [drop-connection | log]

シンタックスの説明

drop-connection	H.245 トンネルが検出されたときにコール セットアップ接続をドロップします。
log	H.245 トンネルが検出されたときにログを発行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 コールの H.245 トンネリングをブロックする方法を示しています。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# h245-tunnel-block action drop-connection
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **hash** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

ハッシュ アルゴリズムをデフォルト値の SHA-1 にリセットするには、このコマンドの **no** 形式を使用します。

hash {**md5** | **sha**}

no hash

シンタックスの説明

md5	IKE ポリシーのハッシュ アルゴリズムを MD5（HMAC バリアント）に指定します。
priority	ポリシーの優先順位を示す固有の番号。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
sha	IKE ポリシーのハッシュ アルゴリズムを SHA-1（HMAC バリアント）に指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 isakmp ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy hash** コマンドは既存のものです。
7.2.(1)	**isakmp policy hash** コマンドが、**hash** コマンドに置き換えられました。

使用上のガイドライン

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。

例

次の例は、グローバル コンフィギュレーション モードで、**hash** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーで MD5 ハッシュ アルゴリズムを使用することを指定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# hash  md5
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

help

指定したコマンドのヘルプ情報を表示するには、ユーザ EXEC モードで **help** コマンドを使用します。

help {*command* | **?**}

シンタックスの説明

command	CLI ヘルプの表示対象となるコマンドを指定します。
?	現在の特権レベルとモードで利用できるコマンドをすべて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

help コマンドは、すべてのコマンドについてヘルプ情報を表示します。個々のコマンドについてのヘルプは、***help*** コマンドの後にコマンド名を入力することで、表示できます。コマンド名を指定しないで、代わりに **?** を入力すると、現在の特権レベルとモードで使用可能なコマンドがすべて表示されます。

pager コマンドがイネーブルになっている場合は、24 行が表示されたときに、表示が一時停止して次のプロンプトが表示されます。

```
<--- More --->
```

More プロンプトは UNIX の **more** コマンドと同様のシンタックスを使用します。このシンタックスを次に示します。

- 次のテキスト画面を表示するには、**Space** キーを押す。
- 次の行を表示するには、**Enter** キーを押す。
- コマンドラインに戻るには、**q** キーを押す。

例

次の例は、***rename*** コマンドのヘルプを表示する方法を示しています。

```
hostname# help rename

USAGE:

        rename /noconfirm [{disk0:|disk1:|flash:}] <source path> [{disk0:|disk1:
|flash:}] <destination path>

DESCRIPTION:

rename          Rename a file

SYNTAX:

/noconfirm                      No confirmation
{disk0:|disk1:|flash:} Optional parameter that specifies the filesystem
<source path>           Source file path
<destination path>      Destination file path

hostname#
```

次の例は、コマンド名と疑問符を入力してヘルプを表示する方法を示しています。

```
hostname(config)# enable ?
usage: enable password <pwd> [encrypted]
```

コア コマンド（**show**、**no**、**clear** 以外のコマンド）についてのヘルプは、コマンド プロンプトで **?** を入力します。

```
hostname(config)# ?
aaa             Enable, disable, or view TACACS+ or RADIUS
                user authentication, authorization and accounting
…
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

hic-fail-group-policy

グループ ポリシーを指定して、デフォルトのグループ ポリシーとは異なる WebVPN ユーザ アクセス権限を許可するには、トンネル グループ webvpn コンフィギュレーション モードで **hic-fail-group-policy** コマンドを使用します。このコマンドの **no** 形式は、グループ ポリシーにデフォルトのグループ ポリシーを使用します。

hic-fail-group-policy *name*

no hic-fail-group-policy

シンタックスの説明

name	グループ ポリシーの名前を指定します。

デフォルト

DfltGrpPolicy

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Cisco Secure Desktop がインストールされたセキュリティ アプライアンスだけで有効です。ホストの整合性確認（*System Detection* とも呼ばれる）には、VPN 機能ポリシーを適用するために満たす必要がある基準の最小セットに対するリモート PC のチェックが含まれます。セキュリティ アプライアンスは、リモート CSD ユーザへのアクセス権限を制限するために、hic-fail-group-policy アトリビュートの値を次のように使用します。

- VPN 機能ポリシーを「Use Failure Group-Policy」（失敗グループ ポリシーを使用する）に設定している場合は、常にこの値を使用します。
- VPN 機能ポリシーを「Use Success Group-Policy, if criteria match」（基準が一致する場合に成功グループ ポリシーを使用する）に設定している場合は、基準が一致しなかった時にこの値を使用します。

このアトリビュートは、失敗グループ ポリシーの名前を適用するよう指定します。グループ ポリシーを使用して、アクセス権限を、デフォルトのグループ ポリシーに関連付けられているアクセス権限と区別します。

（注） VPN 機能ポリシーを「Always use Success Group-Policy」（常に成功グループ ポリシーを使用する）に設定している場合、セキュリティ アプライアンスは、このアトリビュートを使用しません。

詳細については、『*Cisco Secure Desktop Configuration Guide for Cisco ASA 5500 Series Administrators*』を参照してください。

例

次の例は、「FirstGroup」という名前の WebVPN トンネル グループを作成し、「group2」という名前の失敗グループ ポリシーを指定しています。

```
hostname(config)# tunnel-group FirstGroup webvpn
hostname(config)# tunnel-group FirstGroup webvpn-attributes
hostname(config-tunnel-webvpn)# hic-fail-group-policy group2
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	名前付きのトンネル グループの WebVPN アトリビュートを指定します。

hidden-parameter

セキュリティ アプライアンスが SSO 認証用の認証 Web サーバに送信する HTTP POST 要求に非表示パラメータを指定するには、aaa-server-host コンフィギュレーション モードで **hidden-parameter** コマンドを使用します。

すべての非表示パラメータを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

これは HTTP Forms コマンドを使用した SSO です。

hidden-parameter *string*

no hidden-parameter

（注） HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

string	フォームに組み込まれ、SSO サーバに送信される非表示パラメータです。複数の行に入力できます。各行の最大文字数は、255 文字です。すべての行を一体とした、つまり完全な非表示パラメータの最大文字数は、2048 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、認証 Web サーバに対してシングル サインオン認証要求を送信するために HTTP POST 要求を使用します。その要求には、ユーザに見えない SSO HTML 形式に基づく固有の非表示パラメータが、ユーザ名とパスワード以外に、必要な場合があります。Web サーバから受信したフォームに対して HTTP ヘッダー アナライザを使用することで、POST 要求に含まれると Web サーバが予期している非表示パラメータを検出できます。

コマンド **hidden-parameter** を使用すると、Web サーバが必要とする非表示パラメータを認証 POST 要求に指定できます。ヘッダー アナライザを使用すると、任意の符号化 URL パラメータを含む非表示パラメータ文字列全体をコピー アンド ペーストできます。

入力を簡単にするため、1 つの非表示パラメータを複数の連続した行に入力できます。セキュリティ アプライアンスは、その複数の行を 1 つの非表示パラメータに連結します。非表示パラメータ 1 行の最大文字数は 255 文字ですが、各行にはそれより少ない数の文字を入力できます。

（注） 文字列に疑問符を含める場合は、疑問符の前に Ctrl+V のエスケープ シーケンスを使用する必要があります。

例

次の例は、& で区切られた 4 つのフォーム エントリ、およびその値で構成される 1 つの非表示パラメータを示しています。POST 要求から抜き出した 4 つのエントリとその値を次に示します。

- 値が ISO-8859-1 の SMENC
- 値が US-EN の SMLOCALE
- 値が https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG のターゲット
- 値が 0 の smauthreason

SMENC=ISO-8859-1&SMLOCALE=US-EN&target=https%3A%2F%2Ftools.cisco.com%2Femco%2Fappdir%2FAreaRoot.do%3FEMCOPageCode%3DENG&smauthreason=0

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# hidden-parameter
SMENC=ISO-8859-1&SMLOCALE=US-EN&targe
hostname(config-aaa-server-host)# hidden-parameter
t=https%3A%2F%2Ftools.cisco.com%2Femc
hostname(config-aaa-server-host)# hidden-parameter
o%2Fappdir%2FAreaRoot.do%3FEMCOPageCo
hostname(config-aaa-server-host)# hidden-parameter de%3DENG&smauthreason=0
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名とパスワードを受信する Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求のパラメータの名前を指定します。
start-url	事前ログイン クッキーの取得先 URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

homepage

この WebVPN ユーザまたはグループ ポリシーに対して、ログイン後すぐに表示する Web ページの URL を指定するには、WebVPN モードで **homepage** コマンドを使用します。WebVPN モードには、グループ ポリシー モードまたはユーザ名モードから入ります。設定済みのホーム ページ（**homepage none** コマンドを発行して作成されたヌル値を含む）を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。ホーム ページを継承しないようにするには、**homepage none** コマンドを使用します。

homepage {value *url-string* **| none}**

no homepage

シンタックスの説明

none	WebVPN ホーム ページを使用しないことを指定します。ヌル値を設定して、ホーム ページを拒否します。ホーム ページを継承しないようにします。
value *url-string*	ホーム ページの URL を指定します。文字列は、http:// または https:// で始まる必要があります。

デフォルト

デフォルトのホーム ページはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup というグループ ポリシーのホーム ページとして www.example.com を指定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# homepage value http://www.example.com
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。

host

RADIUS アカウンティングを使用して対話するホストを指定するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **host** コマンドを使用します。このモードには、ポリシー マップ タイプの検査 RADIUS アカウント サブモードで **parameters** コマンドを使用してアクセスできます。

このオプションは、デフォルトではディセーブルになっています。

host *address* [***key*** *secret*]

no host ***address*** [***key secret***]

シンタックスの説明

host	RADIUS アカウンティング メッセージを送信する単一のエンドポイントを指定します。
address	RADIUS アカウンティング メッセージを送信するクライアントまたはサーバの IP アドレス。
key	アカウンティング メッセージの無料コピーを送信するために、エンドポイントの秘密鍵を指定するオプションのキーワード。
secret	メッセージの検証に使用される、アカウンティング メッセージを送信するエンドポイントの共有秘密鍵。この鍵には最大 128 文字の英数字を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、インスタンスを複数設定することができます。

例

次の例では、RADIUS アカウンティングによるホストの指定方法を示しています。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# host 209.165.202.128 key cisco123
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングの検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

hostname

セキュリティ アプライアンスのホスト名を設定するには、グローバル コンフィギュレーション モードで **hostname** コマンドを使用します。デフォルトのホスト名に戻すには、このコマンドの **no** 形式を使用します。ホスト名はコマンドライン プロンプトとして表示されます。複数のデバイスに対してセッションを確立している場合は、ホスト名を見ることでコマンドの入力場所を把握できます。

hostname *name*

no hostname [*name*]

シンタックスの説明

name	最大 63 文字のホスト名を指定します。ホスト名の先頭と末尾はアルファベットまたは数字にする必要があります。それ以外の部分に使用できる文字はアルファベット、数字、またはハイフンのみです。

デフォルト

デフォルトのホスト名はプラットフォームによって異なります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	アルファベット以外の文字（ハイフンを除く）が使用不可になりました。

使用上のガイドライン

マルチ コンテキスト モードの場合、システム実行スペースに設定したホスト名は、すべてのコンテキストのコマンドライン プロンプトに表示されます。

コンテキスト内にオプションで設定したホスト名は、コマンドラインに表示されませんが、**banner** コマンドの **$(hostname)** トークンに使用できます。

例

次の例では、ホスト名を firewall1 に設定します。

```
hostname(config)# hostname firewall1
firewall1(config)#
```

関連コマンド

コマンド	説明
banner	ログイン バナー、「今日のお知らせ」バナー、またはイネーブル バナーを設定します。
domain-name	デフォルトのドメイン名を設定します。

hsi

H.323 プロトコルの検査のために HSI を HSI グループに追加するには、hsi グループ コンフィギュレーション モードで **hsi** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

hsi *ip_address*

no hsi *ip_address*

シンタックスの説明

ip_address	追加するホストの IP アドレス。1 つの HSI グループ当たり最大 5 つの HSI が許可されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HSI グループ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査ポリシー マップで HSI を HSI グループに追加する方法を示しています。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi-group	HSI グループを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

hsi-group

H.323 プロトコル検査用に HSI グループを定義し、hsi グループ コンフィギュレーション モードに入るには、パラメータ コンフィギュレーション モードで **hsi-group** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

hsi-group *group_id*

no hsi-group *group_id*

シンタックスの説明

group_id	HSI グループ ID 番号（0 ～ 2147483647）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査ポリシー マップで HSI グループを設定する方法を示します。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# hsi 10.10.15.11
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
endpoint	HSI グループにエンドポイントを追加します。
hsi	HSI を HSI グループに追加します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

html-content-filter

このユーザまたはグループ ポリシーに対して、WebVPN セッションの Java、ActiveX、イメージ、スクリプト、クッキーをフィルタリングするには、WebVPN モードで **html-content-filter** コマンドを使用します。WebVPN モードには、グループ ポリシー モードまたはユーザ名モードから入ります。コンテンツ フィルタを削除するには、このコマンドの **no** 形式を使用します。すべてのコンテンツ フィルタ（**html-content-filter none** コマンドを発行して作成されたヌル値を含む）を削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。html コンテンツ フィルタを継承しないようにするには、**html-content-filter none** コマンドを使用します。

html-content-filter {**java** | **images** | **scripts** | **cookies** | **none**}

no html-content-filter [**java** | **images** | **scripts** | **cookies** | **none**]

シンタックスの説明

cookies	イメージからクッキーを削除して、限定的な広告フィルタリングとプライバシーを実現します。
images	イメージへの参照を削除します（<IMG> タグを削除します）。
java	Java と ActiveX への参照を削除します（<EMBED>、<APPLET>、および <OBJECT> タグを削除します）。
none	フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
scripts	スクリプトへの参照を削除します（<SCRIPT> タグを削除します）。

デフォルト

フィルタリングは行われません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

コマンドを 2 回使用すると、先行する設定値が上書きされます。

例

次の例は、FirstGroup というグループ ポリシーに対して、JAVA、ActiveX、クッキー、およびイメージのフィルタリングを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# html-content-filter java cookies images
```

関連コマンド

コマンド	説明
webvpn（グループ ポリシー、ユーザ名）	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

http

セキュリティ アプライアンスの内部にある HTTP サーバにアクセスできるホストを指定するには、グローバル コンフィギュレーション モードで **http** コマンドを使用します。1 つまたは複数のホストを削除するには、このコマンドの **no** 形式を使用します。このアトリビュートをコンフィギュレーションから削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。

http *ip_address subnet_mask interface_name*

no http

シンタックスの説明

interface_name	ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスの名前を指定します。
ip_address	HTTP サーバにアクセスできるホストの IP アドレスを指定します。
subnet_mask	HTTP サーバにアクセスできるホストのサブネット マスクを指定します。

デフォルト

HTTP サーバにアクセスできるホストは指定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、IP アドレス 10.10.99.1 およびサブネット マスク 255.255.255.255 のホストが外部インターフェイス経由で HTTP サーバにアクセスできるようにする方法を示しています。

```
hostname(config)# http 10.10.99.1 255.255.255.255 outside
```

次の例は、すべてのホストが外部インターフェイス経由で HTTP サーバにアクセスできるようにする方法を示しています。

```
hostname(config)# http 0.0.0.0 0.0.0.0 outside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http authentication-certificate

HTTPS 接続を確立しようとするユーザに、証明書による認証を要求するには、グローバル コンフィギュレーション モードで **http authentication-certificate** コマンドを使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。コンフィギュレーションからすべての **http authentication-certificate** コマンドを削除するには、引数を指定しないで **no** 形式を使用します。

セキュリティ アプライアンスは、PKI トラストポイントに対して証明書を検証します。証明書が検証に合格しなかった場合、セキュリティ アプライアンスは SSL 接続を閉じます。

http authentication-certificate *interface*

no http authentication-certificate [*interface***]**

シンタックスの説明

interface	証明書認証を要求するセキュリティ アプライアンス上のインターフェイスを指定します。

デフォルト

HTTP 証明書認証はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

証明書認証はインターフェイスごとに設定できます。その結果、信頼できるインターフェイスまたは内部インターフェイス上の接続については証明書の提示が不要になります。コマンドを複数回使用すれば、複数のインターフェイス上で証明書認証をイネーブルにできます。

URL は検証後に判明します。そのため、検証は WebVPN と ASDM アクセスの両方に影響します。

ASDM は、この値のほかに、独自の認証方式を使用します。つまり、証明書認証とユーザ名 / パスワード認証の両方が設定されている場合は、両方の認証を要求し、証明書認証がディセーブルの場合は、ユーザ名 / パスワード認証のみを要求します。

例

次の例は、outside と external というインターフェイスに接続しようとするクライアントに証明書認証を要求する方法を示しています。

```
hostname(config)# http authentication-certificate inside
hostname(config)# http authentication-certificate external
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http-comp

特定のグループまたはユーザに対して WebVPN 接続を通して http データの圧縮をイネーブルにするには、グループ ポリシーまたはユーザ名の webvpn モードで **http-comp** コマンドを使用します。

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

http-comp {**gzip** | **none**}

no http-comp {**gzip** | **none**}

シンタックスの説明

gzip	グループまたはユーザに対して圧縮をイネーブルにすることを指定します。
none	グループまたはユーザに対して圧縮をディセーブルにすることを指定します。

デフォルト

デフォルトでは、圧縮は *gzip* に設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシーの WebVPN	•	—	•	—	—
ユーザ名の WebVPN	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

WebVPN 接続では、グローバル コンフィギュレーション モードで設定された **compression** コマンドは、グループ ポリシーまたはユーザ名の webvpn モードで設定された **http-comp** コマンドを上書きします。

例

次の例では、グループ ポリシー sales に対して圧縮がディセーブルにされます。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# http-comp none
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続、WebVPN 接続、IPSec VPN 接続に対して圧縮をイネーブルにします。

http-proxy

HTTP プロキシ サーバを設定するには、WebVPN モードで **http-proxy** コマンドを使用します。HTTP プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

このプロキシ サーバは、セキュリティ アプライアンスが HTTP 要求に使用する外部プロキシ サーバです。

http-proxy *address* [*port*]

no http-proxy

シンタックスの説明

address	外部 HTTP プロキシ サーバの IP アドレスを指定します。
port	HTTP プロキシ サーバが使用するポートを指定します。デフォルト ポートは 80 です。値を指定しない場合、セキュリティ アプライアンスはこのポートを使用します。

デフォルト

HTTP プロキシ サーバは、デフォルトでは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、ポート 80 を使用する IP アドレス 10.10.10.7 の HTTP プロキシ サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# http-proxy 10.10.10.7
hostname(config-webvpn)
```

http redirect

セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定するには、グローバル コンフィギュレーション モードで **http redirect** コマンドを使用します。指定した http redirect コマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。すべての http redirect コマンドをコンフィギュレーションから削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。

http redirect *interface* [*port*]

no http redirect [*interface*]

シンタックスの説明

interface	セキュリティ アプライアンスが HTTPS にリダイレクトする HTTP 要求を受信するインターフェイスを指定します。
port	セキュリティ アプライアンスが HTTP 要求をリッスンするポートを指定します。HTTP 要求は後で HTTPS にリダイレクトされます。デフォルトでは、ポート 80 上でリッスンします。

デフォルト

HTTP リダイレクトはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このインターフェイスが、HTTP を許可するアクセス リストを要求します。アクセス リストがない場合、セキュリティ アプライアンスは、ポート 80 も、HTTP 用に設定した他のどのポートもリッスンしません。

例

次の例は、デフォルト ポート 80 のままで、内部インターフェイスの HTTP リダイレクトを設定する方法を示しています。

```
hostname(config)# http redirect inside
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http server enable	HTTP サーバをイネーブルにします。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

http server enable

セキュリティ アプライアンス HTTP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **http server enable** コマンドを使用します。HTTP サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

http server enable [*port*]

シンタックスの説明

port	HTTP 接続に使用するポート。範囲は 1 ～ 65535 です。デフォルト ポートは 443 です。

デフォルト

HTTP サーバはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、HTTP サーバをイネーブルにする方法を示しています。

```
hostname(config)# http server enable
```

関連コマンド

コマンド	説明
clear configure http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
show running-config http	HTTP サーバにアクセスできるホストを表示し、さらに HTTP サーバがイネーブルであるかどうかを表示します。

https-proxy

HTTPS プロキシ サーバを設定するには、WebVPN モードで **https-proxy** コマンドを使用します。HTTPS プロキシ サーバをコンフィギュレーションから削除するには、このコマンドの no 形式を使用します。

このプロキシ サーバは、セキュリティ アプライアンスが HTTPS 要求に使用する外部プロキシ サーバです。

https-proxy *address* [*port*]

no https-proxy

シンタックスの説明

address	外部 HTTPS プロキシ サーバの IP アドレスを指定します。
port	HTTPS プロキシ サーバが使用するポートを指定します。デフォルト ポートは 443 です。値を指定しない場合、セキュリティ アプライアンスはこのポートを使用します。

デフォルト

HTTPS プロキシ サーバは、デフォルトでは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

例

次の例は、ポート 443 を使用する IP アドレス 10.10.10.1 の HTTPS プロキシ サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# https-proxy 10.10.10.1 443
```

hw-module module password-reset

ハードウェア モジュールのパスワードをデフォルト値「cisco」にリセットするには、特権 EXEC モードで **hw-module module password reset** コマンドを使用します。

hw-module module slot# ***password-reset***

シンタックスの説明

slot#	スロット番号を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効となるのは、ハードウェア モジュールが Up 状態にあり、パスワード リセットをサポートしている場合のみです。AIP SSM に対してこのコマンドを実行すると、AIP SSM はリブートします。このモジュールはリブートが完了するまでオフラインになります。これには数分間かかる場合があります。**show module** コマンドを実行すると、モジュールの状態を監視できます。

このコマンドは、確認のためのプロンプトを常に表示します。コマンドが正常に完了した場合、その他の出力は表示されません。コマンドが失敗した場合、障害が発生した理由を説明するエラー メッセージが表示されます。表示されるエラー メッセージを次に示します。

```
Unable to reset the password on the module in slot 1
Unable to reset the password on the module in slot 1 - unknown module state
Unable to reset the password on the module in slot 1 - no module installed
Failed to reset the password on the module in slot 1 - module not in Up state
Unable to reset the password on the module in slot 1 - unknown module type
The module is slot [n] does not support password reset
Unable to reset the password on the module in slot 1 - no application found
The SSM application version does not support password reset
Failed to reset the password on the module in slot 1
```

例

次の例では、slot 1 のハードウェア モジュールのパスワードをリセットします。

```
hostname (config)# hw-module module 1 password-reset
Reset the password on module in slot 1? [confirm] y
```

関連コマンド

コマンド	説明
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module reset	SSM ハードウェアをシャットダウンし、リセットします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module recover

TFTP サーバからインテリジェント SSM（たとえば、AIP SSM）にリカバリ ソフトウェア イメージをロードする場合や、TFTP サーバにアクセスするためのネットワーク設定値を設定する場合は、特権 EXEC モードで **hw-module module recover** コマンドを使用します。SSM でローカル イメージをロードできないような場合は、このコマンドを使用して SSM を回復することが必要となる場合があります。このコマンドは、インターフェイスの SSM（4GE SSM など）に対しては使用できません。

hw-module module 1 recover {***boot*** | ***stop*** | ***configure*** [***url*** *tfp_url* | ***ip*** *port_ip_address* | ***gateway*** *gateway_ip_address* | ***vlan*** *vlan_id*]}

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。
boot	この SSM のリカバリを開始し、***configure*** 設定に応じてリカバリ イメージをダウンロードします。その後、SSM が新しいイメージからリブートされます。
configure	リカバリ イメージをダウンロードするためのネットワーク パラメータを設定します。***configure*** キーワードの後ろにネットワーク パラメータを入力しない場合は、情報を入力するよう求められます。
gateway *gateway_ip_address*	（オプション）SSM 管理インターフェイスを通じて TFTP サーバにアクセスするためのゲートウェイ IP アドレス。
ip *port_ip_address*	（オプション）SSM 管理インターフェイスの IP アドレス。
stop	リカバリ アクションを停止し、リカバリ イメージのダウンロードを停止します。SSM　は元のイメージからブートします。このコマンドは、**hw-module module boot** コマンドを使用してリカバリを開始してから 30 ～ 45 秒以内に入力する必要があります。この期間を過ぎてから **stop** コマンドを発行すると、SSM が応答しなくなるなど、予期しない結果が生じる場合があります。
url *tfp_url*	（オプション）TFTP サーバ上のイメージの URL。この形式は次のとおりです。 ***tftp:****//server/*[*path/*]*filename*
vlan *vlan_id*	（オプション）管理インターフェイスの VLAN ID を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用できるのは、SSM が Up、Down、Unresponsive、または Recovery 状態にある場合のみです。状態については、**show module** コマンドを参照してください。

例

次の例では、TFTP サーバからイメージをダウンロードするように SSM を設定します。

```
hostname# hw-module module 1 recover configure
Image URL [tftp://127.0.0.1/myimage]: tftp://10.1.1.1/ids-newimg
Port IP Address [127.0.0.2]: 10.1.2.10
Port Mask [255.255.255.254]: 255.255.255.0
Gateway IP Address [1.1.2.10]: 10.1.2.254
VLAN ID [0]: 100
```

次の例では、SSM を回復します。

```
hostname# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may
erase all configuration and all data on that device and
attempt to download a new image for it.
Recover module in slot 1? [confirm]
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module reload

インテリジェント SSM ソフトウェア（たとえば、AIP SSM）をリロードするには、特権 EXEC モードで **hw-module module reload** コマンドを使用します。このコマンドは、インターフェイスの SSM（4GE SSM など）に対しては使用できません。

hw-module module 1 ***reload***

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効となるのは、SSM の状態が Up の場合のみです。状態については、**show module** コマンドを参照してください。

このコマンドは、同じくハードウェア リセットを実行する **hw-module module reset** コマンドとは異なります。

例

次の例では、スロット 1 の SSM をリロードします。

```
hostname# hw-module module 1 reload
Reload module in slot 1? [confirm] y
Reload issued for module in slot 1
%XXX-5-505002: Module in slot 1 is reloading.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module reset

SSM ハードウェアをシャットダウンし、リセットするには、特権 EXEC モードで **hw-module module reset** コマンドを使用します。

hw-module module 1 ***reset***

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドが有効となるのは、SSM の状態が Up、Down、Unresponsive、または Recover の場合のみです。状態については、**show module** コマンドを参照してください。

SSM が Up 状態にある場合、**hw-module module reset** コマンドを使用すると、リセットする前にソフトウェアをシャットダウンするよう求められます。

インテリジェント SSM（たとえば、AIP SSM）を回復するには、**hw-module module recover** コマンドを使用します。SSM が Recover 状態にあるときに **hw-module module reset** を入力しても、SSM はリカバリ プロセスを中断しません。**hw-module module reset** コマンドは、SSM のハードウェア リセットを実行します。ハードウェア リセット後に、SSM のリカバリが続行されます。SSM がハングした場合は、リカバリ中でも SSM をリセットできます。ハードウェア リセットにより、問題が解決する場合があります。

このコマンドは、ソフトウェアのリロードのみを行いハードウェア リセットを行わない **hw-module module reload** コマンドとは異なります。

例

次の例では、Up 状態にあるスロット 1 の SSM をリセットします。

```
hostname# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm] y
Reset issued for module in slot 1
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
%XXX-5-505003: Module in slot 1 is resetting.  Please wait...
%XXX-5-505006: Module in slot 1 is Up.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。
show module	SSM 情報を表示します。

hw-module module shutdown

SSM ソフトウェアをシャットダウンするには、特権 EXEC モードで **hw-module module shutdown** コマンドを使用します。

hw-module module 1 shutdown

シンタックスの説明

1	スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SSM ソフトウェアをシャットダウンすると、コンフィギュレーション データを失わずに SSM の電源を安全にオフにできる状態になります。

このコマンドが有効となるのは、SSM の状態が Up または Unresponsive の場合のみです。状態については、**show module** コマンドを参照してください。

例

次の例では、スロット 1 の SSM をシャットダウンします。

```
hostname# hw-module module 1 shutdown
Shutdown module in slot 1? [confirm] y
Shutdown issued for module in slot 1
hostname#
%XXX-5-505001: Module in slot 1 is shutting down.  Please wait...
%XXX-5-505004: Module in slot 1 shutdown is complete.
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
show module	SSM 情報を表示します。

CHAPTER 14

icmp コマンド～ imap4s コマンド

icmp

セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対してアクセス規則を設定するには、**icmp** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

no icmp {**permit** | **deny**} *ip_address net_mask* [*icmp_type*] *if_name*

シンタックスの説明

deny	条件に合致している場合、アクセスを拒否します。
icmp_type	（オプション）ICMP メッセージ タイプ（表 14-1 を参照）。
if_name	インターフェイス名。
ip_address	ICMP メッセージをインターフェイスに送信するホストの IP アドレス。
net_mask	*ip_address* に適用されるマスク。
permit	条件に合致している場合、アクセスを許可します。

デフォルト

デフォルトでは、セキュリティ アプライアンスは、セキュリティ アプライアンス インターフェイスへの ICMP トラフィックをすべて許可します。しかし、デフォルトでは、セキュリティ アプライアンスはブロードキャスト アドレス宛ての ICMP エコー要求には応答しません。また、セキュリティ アプライアンスは、保護されたインターフェイス上の宛先に対する、外部インターフェイスで受信した ICMP メッセージも拒否します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
6.0	このコマンドが導入されました。

使用上のガイドライン

icmp コマンドは、すべてのセキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックを制御します。ICMP コントロール リストが設定されていない場合、セキュリティ アプライアンスは、すべてのインターフェイス（外部インターフェイスを含む）で終端する ICMP トラフィックをすべて受け入れます。しかし、デフォルトでは、セキュリティ アプライアンスはブロードキャスト アドレス宛ての ICMP エコー要求には応答しません。

icmp deny コマンドは、インターフェイスへの ping をディセーブルにし、**icmp permit** コマンドは、インターフェイスへの ping をイネーブルにします。ping をディセーブルにすると、セキュリティ アプライアンスがネットワーク上で検出できなくなります。これは、設定可能なプロキシ ping とも呼ばれます。

保護されたインターフェイス上の宛先に向けてセキュリティ アプライアンス*経由でルーティング*される ICMP トラフィックに対しては、**access-list extended** または **access-group** コマンドを使用します。

ICMP 到達不能メッセージ タイプ（タイプ 3）は、許可することを推奨します。ICMP 到達不能メッセージを拒否すると、Path MTU Discovery がディセーブルになるため、IPSec トラフィックと PPTP のトラフィックが停止される場合があります。Path MTU Discovery の詳細については、RFC 1195 と RFC 1435 を参照してください。

ICMP コントロール リストがインターフェイスに設定されている場合、セキュリティ アプライアンスは、指定された ICMP トラフィックを最初に照合し、そのインターフェイス上のそれ以外の ICMP トラフィックをすべて暗黙的に拒否します。つまり、最初に一致したエントリが許可エントリの場合、その ICMP パケットは処理が続けられます。最初に一致したエントリが拒否エントリの場合、またはエントリが一致しなかった場合は、セキュリティ アプライアンスはその ICMP パケットを廃棄し、syslog メッセージを生成します。例外は、ICMP コントロール リストが設定されていない場合で、その場合は、**permit** ステートメントがあるものと見なされます。

表 14-1 に、使用できる ICMP タイプ値を示します。

表 14-1　ICMP タイプのリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
4	source-quench
5	redirect
6	alternate-address
8	echo
9	router-advertisement
10	router-solicitation
11	time-exceeded
12	parameter-problem
13	timestamp-request
14	timestamp-reply
15	information-request
16	information-reply

表 14-1　ICMP タイプのリテラル（続き）

ICMP タイプ	リテラル
17	mask-request
18	mask-reply
31	conversion-error
32	mobile-redirect

例

次の例では、外部インターフェイスで、すべての ping 要求を拒否し、すべての到達不能メッセージを許可します。

```
hostname(config)# icmp permit any unreachable outside
```

ICMP トラフィックを拒否する追加インターフェイスそれぞれに対して、続けて **icmp deny any** *interface* コマンドを入力します。

次の例では、ホスト 172.16.2.15 またはサブネット 172.22.1.0/16 上のホストに、外部インターフェイスへの ping を許可します。

```
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(config)# icmp permit any unreachable outside
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションを消去します。
debug icmp	ICMP に関するデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

icmp-object

icmp-type オブジェクト グループを追加するには、icmp-type コンフィギュレーション モードで **icmp-object** コマンドを使用します。ネットワーク オブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。

icmp-object *icmp_type*

no group-object *icmp_type*

シンタックスの説明

icmp_type	icmp-type の名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Icmp-type コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

icmp-object コマンドは、**object-group** コマンドと組み合せることで、icmp-type オブジェクトを定義します。このコマンドは、icmp-type コンフィギュレーション モードで使用されます。

ICMP タイプの番号と名前には、次のものがあります。

番号	ICMP タイプの名前
0	**echo-reply**
3	**unreachable**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
14	**timestamp-reply**
15	**information-request**

番号	ICMP タイプの名前
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

例

次の例は、icmp-type コンフィギュレーション モードで **icmp-object** コマンドを使用する方法を示しています。

```
hostname(config)# object-group icmp-type icmp_allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

id-cert-issuer

このトラストポイントに関連付けられている CA から発行されたピア証明書をシステムで受け入れるかどうかを示すには、暗号 CA トラストポイント コンフィギュレーション モードで **id-cert-issuer** コマンドを使用します。トラストポイントに関連付けられている CA から発行された証明書を拒否するには、このコマンドの **no** 形式を使用します。このコマンドは、広く使用されるルート CA を表すトラストポイントに対して有用です。

id-cert-issuer

no id-cert-issuer

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト設定はイネーブルです（ID 証明書は受け入れられます）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、広く使用されるルート CA の下位 CA から発行された証明書のみを受け入れるようにする場合に使用します。この機能を使用可能にしない場合は、セキュリティ アプライアンスが、この発行者によって署名された IKE ピア証明書をすべて拒否します。

例

次の例では、central トラストポイントの暗号 CA トラストポイント コンフィギュレーション モードに入り、central トラストポイントの発行者によって署名された ID 証明書の受け入れを管理者に許可します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# id-cert-issuer
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント サブモードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求の送信を試行するまでの待機時間を、分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

id-mismatch

過度の DNS ID ミスマッチのロギングをイネーブルにするには、パラメータ コンフィギュレーション モードで **id-mismatch** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

id-mismatch [**count** *number* **duration** *seconds*] **action log**

no id-mismatch [**count** *number* **duration** *seconds*] [**action log**]

シンタックスの説明

count *number*	システム メッセージ ログが送信される前のミスマッチ インスタンスの最大数。
duration *seconds*	監視する期間（秒）。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。コマンドがイネーブルで、オプションが指定されていない場合、デフォルト レートは最大数が 30 で、期間は 3 秒間です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ハイレートの DNS ID ミスマッチはキャッシュ ポイズニング攻撃を示す場合があります。このコマンドをイネーブルにすると、そうした試みを監視して警告します。ミスマッチ レートが設定値を超えると、システム メッセージの要約ログが出力されます。**id-mismatch** コマンドは通常のイベントベースのシステム メッセージ ログに関する詳細をシステム管理者に提供します。

例

次の例では、DNS 検査ポリシー マップで ID ミスマッチをイネーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-mismatch action log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

id-randomization

DNS クエリーの DNS ID をランダム化するには、パラメータ コンフィギュレーション モードで **id-randomization** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

id-randomization

no id-randomization

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトではディセーブルです。DNS クエリーからの DNS ID は変更されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ID のランダム化は、キャッシュ ポイズニング攻撃に対する保護に役立ちます。

例

次の例では、DNS 検査ポリシー マップで ID のランダム化をイネーブルにする方法を示しています。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# id-randomization
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

igmp

インターフェイス上で IGMP 処理を初期化するには、インターフェイス コンフィギュレーション モードで **igmp** コマンドを使用します。インターフェイス上で IGMP 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

igmp

no igmp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

イネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

実行コンフィギュレーションに表示されるのは、このコマンドの **no** 形式のみです。

例

次の例では、選択したインターフェイス上で IGMP 処理をディセーブルにします。

```
hostname(config-if)# no igmp
```

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続されている受信者、および IGMP を通じてラーニングされた受信者を持つマルチキャスト グループを表示します。
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp access-group

インターフェイスを利用するサブネット上のホストが加入できるマルチキャスト グループを制御するには、インターフェイス コンフィギュレーション モードで **igmp access-group** コマンドを使用します。インターフェイス上でグループをディセーブルにするには、このコマンドの **no** 形式を使用します。

igmp access-group *acl*

no igmp access-group *acl*

シンタックスの説明

acl	IP アクセス リストの名前。標準アクセス リスト、拡張アクセス リスト、またはその両方を指定できます。しかし、拡張アクセス リストを指定した場合、照合されるのは宛先アドレスのみです。そのため、送信元には **any** を指定する必要があります。

デフォルト

インターフェイス上ですべてのグループに加入できます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

例

次の例では、アクセス リスト 1 で許可されたホストだけがグループに加入できるようにします。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp access-group 1
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp forward interface

すべての IGMP ホスト レポートの転送をイネーブルにし、指定したインターフェイスでメッセージが受信される状態にするには、インターフェイス コンフィギュレーション モードで **igmp forward interface** コマンドを使用します。転送を解除するには、このコマンドの **no** 形式を使用します。

igmp forward interface *if-name*

no igmp forward interface *if-name*

シンタックスの説明

if-name	インターフェイスの論理名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドを入力インターフェイス上で入力します。このコマンドはスタブ マルチキャスト ルーティング用であるため、このコマンドに PIM を同時に設定することはできません。

例

次の例では、IGMP ホスト レポートを現在のインターフェイスから指定のインターフェイスに転送します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp forward interface outside
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp join-group

インターフェイスを、指定したグループのローカルに接続されたメンバーとして設定するには、インターフェイス コンフィギュレーション モードで **igmp join-group** コマンドを使用します。グループのメンバーシップをキャンセルするには、このコマンドの **no** 形式を使用します。

igmp join-group *group-address*

no igmp join-group *group-address*

シンタックスの説明

group-address	マルチキャスト グループの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドは、セキュリティ アプライアンス インターフェイスをマルチキャスト グループのメンバーとして設定します。**igmp join-group** コマンドを使用すると、セキュリティ アプライアンスは、指定されたマルチキャスト グループ宛てのマルチキャスト パケットを受け入れて、転送します。

マルチキャスト グループのメンバーにしないで、セキュリティ アプライアンスがマルチキャスト トラフィックを転送するように設定するには、**igmp static-group** コマンドを使用します。

例

次の例では、選択したインターフェイスが IGMP グループ 255.2.2.2 に加入するように設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp join-group 225.2.2.2
```

関連コマンド

コマンド	説明
igmp static-group	インターフェイスを、指定したマルチキャスト グループのスタティックに接続されたメンバーとして設定します。

igmp limit

IGMP の状態の数をインターフェイスごとに制限するには、インターフェイス コンフィギュレーション モードで **igmp limit** コマンドを使用します。デフォルトの制限に戻すには、このコマンドの **no** 形式を使用します。

igmp limit *number*

no igmp limit [*number*]

シンタックスの説明

number	インターフェイス上で許可する IGMP の状態の数。有効値の範囲は 0 ～ 500 です。デフォルト値は 500 です。値を 0 に設定すると、ラーニングされたグループが追加されなくなります。ただし、メンバーシップを手動で定義することは引き続き可能です（**igmp join-group** コマンドと **igmp static-group** コマンドを使用します）。

デフォルト

デフォルトは 500 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。このコマンドにより、**igmp max-groups** コマンドは置き換えられました。

例

次の例では、インターフェイスにおける IGMP の状態の数を 250 に制限します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp limit 250
```

関連コマンド

コマンド	説明
igmp	インターフェイス上で IGMP 処理を初期化します。
igmp join-group	インターフェイスを、指定したグループのローカルに接続されたメンバーとして設定します。
igmp static-group	インターフェイスを、指定したマルチキャスト グループのスタティックに接続されたメンバーとして設定します。

igmp query-interval

インターフェイスが IGMP ホスト クエリー メッセージを送信する頻度を設定するには、インターフェイス コンフィギュレーション モードで **igmp query-interval** コマンドを使用します。デフォルトの頻度に戻すには、このコマンドの **no** 形式を使用します。

igmp query-interval *seconds*

no igmp query-interval *seconds*

シンタックスの説明

seconds	IGMP ホスト クエリー メッセージを送信する頻度（秒単位）。有効となる値の範囲は、1 ～ 3,600 秒です。デフォルトは 125 秒です。

デフォルト

デフォルトのクエリー間隔は 125 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

マルチキャスト ルータは、ホスト クエリー メッセージを送信して、インターフェイスに接続されたネットワーク上のメンバーを含むマルチキャスト グループを検出します。ホストは、特定のグループ宛てのマルチキャスト パケットを受信する必要があることを示す IGMP レポート メッセージを使用して応答します。ホスト クエリー メッセージは、アドレス 224.0.0.1 および TTL 値 1 の all-hosts マルチキャスト グループに宛先指定されます。

IGMP ホスト クエリー メッセージを送信するルータは、LAN の指定ルータのみです。

- IGMP バージョン 1 の場合、指定ルータは、LAN 上で動作するマルチキャスト ルーティング プロトコルに応じて選定されます。
- IGMP バージョン 2 の場合、指定ルータは、サブネット上で最も低い IP アドレスを持つマルチキャスト ルータになります。

ルータがタイムアウト期間（期間は **igmp query-timeout** コマンドで制御される）にクエリーを受信しなかった場合は、そのルータがクエリー発行者になります。

注意　この値を変更すると、マルチキャスト転送に重大な影響を及ぼす場合があります。

例

次の例では、IGMP クエリー間隔を 120 秒に変更します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-interval 120
```

関連コマンド

コマンド	説明
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最長応答期間を設定します。
igmp query-timeout	前のクエリー発行者がクエリーを停止してから、ルータがインターフェイスのクエリー発行者を引き継ぐまでのタイムアウト期間を設定します。

igmp query-max-response-time

IGMP クエリーでアドバタイズされる最長応答期間を指定するには、インターフェイス コンフィギュレーション モードで **igmp query-max-response-time** コマンドを使用します。応答期間をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

igmp query-max-response-time *seconds*

no igmp query-max-response-time [*seconds*]

シンタックスの説明

seconds	IGMP クエリーでアドバタイズされる最長応答期間（秒単位）。有効な値は 1 ～ 25 秒です。デフォルト値は 10 秒です。

デフォルト

10 秒。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドが有効となるのは、IGMP バージョン 2 または 3 が動作している場合のみです。

このコマンドは、応答者が IGMP クエリー メッセージに応答できる期間を制御します。この期間を過ぎると、ルータがグループを削除します。

例

次の例では、最長クエリー応答期間を 8 秒に変更します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-max-response-time 8
```

関連コマンド

コマンド	説明
igmp query-interval	インターフェイスが IGMP ホスト クエリー メッセージを送信する頻度を設定します。
igmp query-timeout	前のクエリー発行者がクエリーを停止してから、ルータがインターフェイスのクエリー発行者を引き継ぐまでのタイムアウト期間を設定します。

igmp query-timeout

前のクエリー発行者がクエリーを停止してから、インターフェイスがクエリー発行者を引き継ぐまでのタイムアウト期間を設定するには、インターフェイス コンフィギュレーション モードで **igmp query-timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

igmp query-timeout *seconds*

no igmp query-timeout [*seconds*]

シンタックスの説明

seconds	前のクエリー発行者がクエリーを停止してから、ルータがクエリー発行者を引き継ぐまで待機する秒数。有効な値は 60 ～ 300 秒です。デフォルト値は 255 秒です。

デフォルト

デフォルトのクエリー間隔は 255 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドには IGMP バージョン 2 または 3 が必要です。

例

次の例では、最後にクエリーを受信してから、インターフェイスのクエリー発行者を引き継ぐまで 200 秒待機するようルータを設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp query-timeout 200
```

関連コマンド

コマンド	説明
igmp query-interval	インターフェイスが IGMP ホスト クエリー メッセージを送信する頻度を設定します。
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最長応答期間を設定します。

igmp static-group

インターフェイスを、指定したマルチキャスト グループのスタティックに接続されたメンバーとして設定するには、インターフェイス コンフィギュレーション モードで **igmp static-group** コマンドを使用します。スタティック グループ エントリを削除するには、このコマンドの **no** 形式を使用します。

igmp static-group *group*

no igmp static-group *group*

シンタックスの説明

group	IP マルチキャスト グループ アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

igmp static-group コマンドを使用して設定すると、セキュリティ アプライアンス インターフェイスは、指定されたグループそのものを宛先とするマルチキャスト パケットを受け入れずに、転送します。指定されたマルチキャスト グループ宛てのマルチキャスト パケットを受け入れて、転送するようにセキュリティ アプライアンスを設定するには、**igmp join-group** コマンドを使用します。**igmp join-group** コマンドに **igmp static-group** コマンドと同じグループ アドレスを設定した場合は、**igmp join-group** コマンドが優先され、グループはローカルに加入しているグループのように動作します。

例

次の例では、選択したインターフェイスをマルチキャスト グループ 239.100.100.101 に追加します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp static-group 239.100.100.101
```

関連コマンド

コマンド	説明
igmp join-group	インターフェイスを、指定したグループのローカルに接続されたメンバーとして設定します。

igmp version

インターフェイスが使用する IGMP のバージョンを設定するには、インターフェイス コンフィギュレーション モードで **igmp version** コマンドを使用します。バージョンをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

igmp version {***1*** | ***2***}

no igmp version [***1*** | ***2***]

シンタックスの説明

1	IGMP バージョン 1。
2	IGMP バージョン 2。

デフォルト

IGMP バージョン 2。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、インターフェイス コンフィギュレーション モードに変更されました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードに入る必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

サブネット上のルータはすべて、同じバージョンの IGMP をサポートする必要があります。ホストは任意の IGMP バージョン（1 または 2）を使用できます。また、セキュリティ アプライアンスは、ホストの存在を検出して、適切にクエリーします。

igmp query-max-response-time コマンドや **igmp query-timeout** コマンドなど、一部のコマンドでは IGMP バージョン 2 が必要です。

例

次の例では、選択したインターフェイスが IGMP バージョン 1 を使用するように設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# igmp version 1
```

関連コマンド

コマンド	説明
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最長応答期間を設定します。
igmp query-timeout	前のクエリー発行者がクエリーを停止してから、ルータがインターフェイスのクエリー発行者を引き継ぐまでのタイムアウト期間を設定します。

ignore lsa mospf

ルータが link-state advertisement（LSA; リンクステート アドバタイズメント）のタイプ 6 Multicast OSPF（MOSPF）パケットを受信した際に、syslog メッセージを送信しないようにするには、ルータ コンフィギュレーション モードで **ignore lsa mospf** コマンドを使用します。syslog メッセージを送信する設定に戻すには、このコマンドの **no** 形式を使用します。

ignore lsa mospf

no ignore lsa mospf

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

タイプ 6 MOSPF パケットはサポート対象外です。

例

次の例では、LSA タイプ 6 MOSPF パケットが無視されるようにします。

```
hostname(config-router)# ignore lsa mospf
```

関連コマンド

コマンド	説明
show running-config router ospf	OSPF ルータ コンフィギュレーションを表示します。

im

SIP 経由のインスタント メッセージをイネーブルにするには、パラメータ コンフィギュレーション モードで **im** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

im

no im

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、SIP 検査ポリシー マップで SIP 経由のインスタント メッセージをイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# im
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

imap4s

IMAP4S コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **imap4s** コマンドを使用します。IMAP4S コマンド モードで入力したコマンドをすべて削除するには、このコマンドの **no** 形式を使用します。

IMAP4 は、インターネット サーバがユーザ宛ての電子メールを受信および保管するためのクライアント / サーバ プロトコルです。ユーザ（または電子メール クライアント）は、メールのヘッダーおよび送信者のみを表示して、メールをダウンロードするかどうかを決めることができます。また、サーバ上に複数のフォルダやメールボックスを作成して操作する、メッセージを削除する、または特定部分やメッセージ全体を検索することもできます。メールを操作する間、IMAP はサーバに継続的にアクセスする必要があります。IMAP4S を使用すると、SSL 接続上で電子メールを受信できます。

imap4s

no imap4s

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、IMAP4S コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# imap4s
hostname(config-imap4s)#
```

関連コマンド

コマンド	説明
clear configure imap4s	IMAP4S コンフィギュレーションを削除します。
show running-config imap4s	IMAP4S の実行コンフィギュレーションを表示します。

CHAPTER 15

inspect ctiqbe コマンド～ inspect xdmcp コマンド

inspect ctiqbe

CTIQBE プロトコル検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect ctiqbe** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。検査をディセーブルにするには、このコマンドの **no** 形式を使用します。

inspect ctiqbe

no inspect ctiqbe

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは 7.0(1) で導入されました。このコマンドにより、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ctiqbe コマンドは、NAT、PAT、および双方向 NAT をサポートする CTIQBE プロトコル検査をイネーブルにします。イネーブルにすると、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と正常に連携動作して、セキュリティ アプライアンスを通じてコール セットアップを実行できるようになります。

Telephony Application Programming Interface（TAPI）と Java Telephony Application Programming Interface（JTAPI）は、多くの Cisco VoIP アプリケーションで使用されます。Computer Telephony Interface Quick Buffer Encoding（CTIQBE）は、Cisco TAPI Service Provider（TSP）が Cisco CallManager と通信するために使用します。

次に、CTIQBE アプリケーション検査を使用するときに適用される制限を要約します。

- CTIQBE アプリケーション検査では、**alias** コマンドを使用したコンフィギュレーションはサポートされません。
- CTIQBE コールのステートフル フェールオーバーはサポートされていません。
- **debug ctiqbe** コマンドを使用すると、メッセージ伝送が遅延する場合があります。その結果、リアルタイム環境ではパフォーマンスに影響が及ぶ場合があります。このデバッグまたはロギングをイネーブルにした結果、Cisco IP SoftPhone においてセキュリティ アプライアンスからのコール セットアップを完了できなくなったと思われる場合は、Cisco IP SoftPhone を実行するシステム上で Cisco TSP 設定のタイムアウト値を増やします。
- CTIQBE アプリケーション検査では、複数の TCP パケットにフラグメント化された CTIQBE メッセージはサポートされていません。

次に、特定のシナリオで CTIQBE アプリケーション検査を使用する場合に特に考慮が必要な事項を要約します。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されている場合、各 Cisco CallManager はセキュリティ アプライアンスの異なるインターフェイスに接続されているため、これら 2 つの電話間のコールは失敗します。
- Cisco CallManager が Cisco IP SoftPhone よりもセキュリティの高いインターフェイス上にあり、Cisco CallManager IP アドレスの NAT または外部 NAT が必要になる場合、Cisco IP SoftPhone では、Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定する必要があるため、マッピングはスタティックにする必要があります。
- PAT または外部 PAT を使用して、Cisco CallManager IP アドレスを変換する場合、Cisco IP SoftPhone の登録を成功させるには、その TCP ポート 2748 を PAT（インターフェイス）アドレスの**同じポート**にスタティックにマッピングする必要があります。CTIQBE リスニング ポート（TCP 2748）は固定されており、Cisco CallManager、Cisco IP SoftPhone、または Cisco TSP 上でユーザが設定変更することはできません。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect ctiqbe** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect ctiqbe** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect ctiqbe** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、CTIQBE 検査エンジンをイネーブルにします。この例では、デフォルト ポート（2748）上の CTIQBE トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map ctiqbe-port
hostname(config-cmap)# match port tcp eq 2748
hostname(config-cmap)# exit
hostname(config)# policy-map ctiqbe_policy
hostname(config-pmap)# class ctiqbe-port
hostname(config-pmap-c)# inspect ctiqbe
hostname(config-pmap-c)# exit
hostname(config)# service-policy ctiqbe_policy interface outside
```

すべてのインターフェイスに対して CTIQBE 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
show conn	さまざまな接続タイプの接続状態を表示します。
show ctiqbe	セキュリティ アプライアンスを越えて確立された CTIQBE セッションに関する情報を表示します。CTIQBE 検査エンジンによって割り当てられたメディア接続に関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect dcerpc

エンドポイント マッパー宛の DCERPC トラフィックの検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect dcerpc** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect dcerpc [*map_name*]

no inspect dceprc [*map_name*]

シンタックスの説明

map_name	（オプション）DCERPC マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

inspect dcerpc コマンドは、DCERPC プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。

例

次の例では、DCERPC ピンホールに設定されたタイムアウトを指定して、DCERPC 検査ポリシーを定義する方法を示します。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# timeout pinhole 0:10:00

hostname(config)# class-map dcerpc
hostname(config-cmap)# match port tcp eq 135

hostname(config)# policy-map global-policy
hostname(config-pmap)# class dcerpc
hostname(config-pmap-c)# inspect dcerpc dcerpc_map

hostname(config)# service-policy global-policy global
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
timeout pinhole	DCERPC ピンホールのタイムアウトを設定し、グローバル システム ピンホール タイムアウトを上書きします。

inspect dns

DNS 検査をイネーブルにするには（以前にディセーブルにした場合）、または、DNS 検査のパラメータを設定するには、クラス コンフィギュレーション モードで **inspect dns** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。DNS 検査をディセーブルにするには、このコマンドの **no** 形式を使用します。

inspect dns [*map_name*]

no inspect dns [*map_name*]

シンタックスの説明

map_name	（オプション）DNS マップの名前。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。
7.2(1)	さらに多くの DNS 検査パラメータを設定できるように、このコマンドが修正されました。

使用上のガイドライン

DNS guard は、DNS 応答がセキュリティ アプライアンスによって転送されると、DNS クエリーに関連付けられた DNS セッションをただちに停止します。DNS guard は、また、DNS 応答の ID が DNS クエリーの ID と一致していることを確認するために、メッセージ交換を監視します。

DNS 検査がイネーブルの場合（デフォルト）、セキュリティ アプライアンスは次の追加タスクを実行します。

- **alias** コマンド、**static** コマンド、および **nat** コマンドを使用して完成したコンフィギュレーションに基づいて、DNS レコードを変換する（DNS リライト）。変換が適用されるのは、DNS 応答の A レコードのみです。そのため、PTR レコードを要求する逆ルックアップは、DNS リライトの影響を受けません。

（注） DNS リライトは PAT には適用できません。これは、A レコードごとに複数の PAT 規則が適用可能であり、使用される PAT 規則があいまいになるためです。

- DNS メッセージの最大長を適用する（デフォルトは 512 バイト、最大長は 65,535 バイト）。必要に応じて再構成が実行され、パケット長が設定した最大長を超えていないことが確認されます。最大長を超えている場合、そのパケットはドロップされます。
- ドメイン名の長さとして 255 バイトを、ラベルの長さとして 63 バイトを適用する。
- DNS メッセージに圧縮ポインタが出現する場合、ポインタによって参照されるドメイン名の完全性を確認する。
- 圧縮ポインタのループが存在するかどうかを確認する。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つのみ作成されます。DNS の識別情報は、*app_id* によって追跡され、各 app_id のアイドル タイマーはそれぞれ独立して動作します。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内のみであり、リソースの継続使用はできません。しかし、**show conn** コマンドを入力すると、DNS 接続のアイドル タイマーが新しい DNS セッションによってリセットされることが示されます。これは共有 DNS 接続の性質によるものであり、仕様です。

DNS リライトの動作

DNS 検査がイネーブルの場合、DNS リライトは、任意のインターフェイスから発信される DNS メッセージの NAT をフル サポートします。

内部ネットワーク上のクライアントが内部アドレスの DNS 解決を外部インターフェイス上の DNS サーバに要求した場合、DNS A レコードは正しく変換されます。DNS 検査エンジンがディセーブルの場合、A レコードは変換されません。

DNS リライトは、次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイス上にある場合、*DNS 応答*内のパブリック アドレス（ルーティング可能なアドレスまたは「マッピングされた」アドレス）を、プライベート アドレス（「実」アドレス）に変換する。
- DNS クライアントがパブリック インターフェイス上にある場合、プライベート アドレスをパブリック アドレスに変換する。

DNS 検査がイネーブルであれば、**alias** コマンド、**static** コマンド、または **nat** コマンドを使用して DNS リライトを設定できます。これらのコマンドのシンタックスや機能の詳細については、該当するコマンドのページを参照してください。

注：アップグレード時に、コマンド シンタックスは現在のシンタックスに変換されます。

例

次の例では、DNS メッセージの最大長を設定する方法を示しています。

```
hostname(config)# policy-map type inspect dns dns-inspect
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 1024
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug dns	DNS のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect esmtp

SMTP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect esmtp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect esmtp

no inspect esmtp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ESMTP アプリケーション検査では、SMTP ベースの攻撃からの保護を強化するため、セキュリティ アプライアンスを通過できる SMTP コマンドのタイプを制限し、モニタリング機能を追加しています。

(注) ESMTP　検査ポリシーは、低セキュリティのインターフェイスから高セキュリティのインターフェイスに入ってくるトラフィック フローにのみ適用されます。高セキュリティのインターフェイスから低セキュリティのインターフェイスへのフローの場合は、検査は実行されません。

ESMTP は SMTP プロトコルの機能拡張であり、あらゆる点で SMTP と類似しています。便宜上、このドキュメントでは、SMTP という用語は SMTP と ESMTP の両方を指します。拡張 SMTP のアプリケーション検査プロセスは、SMTP アプリケーション検査と類似しており、SMTP セッションのサポートを備えています。拡張 SMTP セッションで使用されるコマンドのほとんどは、SMTP セッションで使用されるものと同じですが、ESMTP セッションは、動作がはるかに高速で、配信通知ステータスなど、信頼性とセキュリティに関するオプションをより多く備えています。

inspect esmtp コマンドには、**fixup smtp** コマンドで提供されていた機能が含まれています。また、一部の拡張 SMTP コマンドに対する追加サポートも含まれています。拡張 SMTP アプリケーション検査では、8 つの拡張 SMTP コマンド（AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、および VRFY）に対するサポートが追加されています。7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、および RSET）に対するサポートを合せると、セキュリティ アプライアンスは合計 15 の SMTP コマンドをサポートしています。

他の拡張 SMTP コマンド（ATRN、STARTLS、ONEX、VERB、CHUNKING など）やプライベート拡張はサポートされていません。サポート対象外のコマンドは、内部サーバにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、廃棄されます。

inspect esmtp コマンドは、SMTP バナーの文字を、「2」、「0」、「0」の文字を除いて、アスタリスクに変更します。復帰（CR）と改行（LF）は、無視されます。

SMTP 検査がイネーブルの場合、次の規則が順守されていないときは、対話型の SMTP に使用される Telnet セッションは有効なコマンドを待機し、ファイアウォール esmtp ステート マシンはセッションを正しい状態に保ちます。この規則とは、SMTP コマンドは少なくとも 4 文字の長さが必要である、SMTP コマンドは改行と復帰で終了する必要がある、次の返信を発行する前に応答を待つ必要がある、というものです。

SMTP サーバは、数値の応答コードと人が読めるオプションの文字列によって、クライアントの要求に応答します。SMTP アプリケーション検査は、ユーザが使用できるコマンドや、サーバが返すメッセージを制御および削減します。SMTP 検査は、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本的な SMTP コマンドと 8 つの拡張コマンドに制限する。
- SMTP コマンド応答シーケンスを監視する。
- 監査証跡を生成する。メール アドレスに埋め込まれていた無効な文字が置き換えられた場合、監査レコード 108002 が生成されます。詳細については、RFC 821 を参照してください。

SMTP 検査は、コマンドと応答のシーケンスを監視して、次の異常なシグニチャを検出します。

- 不完全なコマンド。
- コマンドの不正な終了（<CR><LR> で終了していない）。
- PIPE シグニチャが MAIL from コマンドまたは RCPT to コマンドへのパラメータとして検出された場合、セッションは閉じられます。ユーザは設定できません。
- SMTP サーバによる予期しない移行。
- 未知のコマンドがあると、セキュリティ アプライアンスはパケット内のすべての文字を X に変更します。この場合、サーバは、クライアントに対してエラー コードを生成します。パケット内が変更されるため、TCP チェックサムの再計算または調整が必要になります。
- TCP ストリームの編集。
- コマンドのパイプライン化。

例

次の例に示すように、SMTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（25）上の SMTP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map smtp-port
hostname(config-cmap)# match port tcp eq 25
hostname(config-cmap)# exit
hostname(config)# policy-map smtp_policy
hostname(config-pmap)# class smtp-port
hostname(config-pmap-c)# inspect esmtp
hostname(config-pmap-c)# exit
hostname(config)# service-policy smtp_policy interface outside
```

すべてのインターフェイスに対して SMTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug esmtp	SMTP のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。
show conn	SMTP など、さまざまな接続タイプの接続状態を表示します。

inspect ftp

FTP 検査用のポートを設定する場合、または高度な検査をイネーブルにする場合は、クラス コンフィギュレーション モードで **inspect ftp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect ftp [**strict** [*map_name*]]

no inspect ftp [**strict** [*map_name*]]

シンタックスの説明

map_name	FTP マップの名前。
strict	（オプション）FTP トラフィックの高度な検査をイネーブルにし、強制的に RFC 標準に準拠させます。

注意　FTP を上位のポートに移動する場合は、注意が必要です。たとえば、FTP ポートを 2021 に設定した場合、ポート 2021 に向けて開始する接続はすべて、データ ペイロードが FTP コマンドとして解釈されます。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、ポート 21 で FTP があるかどうかリッスンします。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。*map_name* オプションが追加されました。

使用上のガイドライン

FTP アプリケーション検査は、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックなセカンダリ データ接続を準備する。
- ***ftp*** コマンド応答シーケンスを追跡する。
- 監査証跡を生成する。
- 埋め込み IP アドレスの NAT を実行する。

（注）　バナーを除き、**inspect ftp** は FTP コマンドまたは応答をセグメント化する FTP サーバをサポートしていません。

FTP アプリケーション検査は、FTP データ転送用にセカンダリ チャネルを準備します。チャネルは、ファイルのアップロード、ファイルのダウンロード、またはディレクトリ一覧イベントの応答として割り当てられます。ただし、事前にネゴシエートされている必要があります。ポートは、PORT コマンドまたは PASV コマンドによってネゴシエートされます。

（注） **no inspect ftp** コマンドを使用して、FTP 検査エンジンをディセーブルにすると、発信ユーザはパッシブ モードだけで接続を開始でき、着信 FTP はすべてディセーブルになります。

strict オプションの使用方法

strict オプションは、Web ブラウザが FTP 要求内の埋め込みコマンドを送信しないようにします。各 ***ftp*** コマンドは、新しいコマンドが許可される前に確認される必要があります。埋め込みコマンドを送信する接続は、ドロップされます。**strict** オプションは、FTP サーバが 227 コマンドを生成することだけを許可し、FTP クライアントが PORT コマンドを生成することだけを許可します。227 コマンドと PORT コマンドはチェックして、エラー文字列内に表示されないようにします。

注意 ***strict*** オプションを使用すると、RFC 標準に準拠していない FTP クライアントが遮断されることがあります。

strict オプションがイネーブルの場合、次の異常なアクティビティについて、各 ***ftp*** コマンドと応答シーケンスが追跡されます。

- 不完全なコマンド：PORT および PASV 応答コマンド内のカンマの数が 5 つかどうかが確認されます。5 つ以外の場合、PORT コマンドは不完全であると見なされ、TCP 接続は終了します。
- 不正なコマンド：RFC に規定されているように、***ftp*** コマンドが <CR><LF> 文字で終了しているかどうかが確認されます。異なっている場合、接続は終了します。
- RETR コマンドと STOR コマンドのサイズ：固定値になっているかどうかが確認されます。サイズが固定値より大きい場合、エラー メッセージがログに記録され、接続は終了します。
- コマンド スプーフィング：PORT コマンドは常にクライアントから送信される必要があります。PORT コマンドがサーバから送信されている場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV　応答コマンド（227）は常にサーバから送信される必要があります。PASV 応答コマンドがクライアントから送信されている場合、TCP 接続は拒否されます。この拒否により、ユーザが「227 xxxxx a1, a2, a3, a4, p1, p2」を実行した場合のセキュリティ ホールが防止されます。
- TCP ストリームの編集。
- 無効なポートのネゴシエーション：ネゴシエートされたダイナミック ポートの値が 1024 未満かどうかが確認されます。1 ～ 1024 の範囲のポート番号は既知の接続用に予約されているため、ネゴシエートされたポートがこの範囲内の場合は、TCP 接続は開放されます。
- コマンドのパイプライン化：PORT および PASV 応答コマンド内のポート番号の後にある文字数が定数の 8 であるかどうかが相互確認されます。9 以上の場合、TCP 接続は終了します。
- セキュリティ アプライアンスが、SYST コマンドに対する FTP サーバの応答を一連の X に置き換え、サーバのシステム タイプが FTP クライアントに知られることを防止します。このデフォルト動作を無効にするには、FTP マップ コンフィギュレーション モードで **no mask-syst-reply** コマンドを使用します。

(注)　セキュリティ アプライアンスを通過させない特定の FTP コマンドを指定するには、FTP マップを指定し、**request-command deny** コマンドを使用します。詳細については、**ftp-map** コマンドと **request-command deny** コマンドのページを参照してください。

FTP ログ メッセージ

FTP アプリケーション検査は、次のログ メッセージを生成します。

- 取得またはアップロードされた各ファイルについて、監査レコード 302002 が生成されます。
- **ftp** コマンドが RETR または STOR であるかが確認され、取得コマンドと格納コマンドがログに記録されます。
- ユーザ名は、IP アドレスを提供するテーブルを検索することで取得されます。
- ユーザ名、送信元 IP アドレス、宛先 IP アドレス、NAT アドレス、およびファイル操作がログに記録されます。
- メモリ不足によってセカンダリ ダイナミック チャネルの準備に失敗した場合、監査レコード 201005 が生成されます。

FTP アプリケーション検査は、NAT と連携して、アプリケーション ペイロード内の IP アドレスを変換します。詳細については、RFC 959 を参照してください。

例

次の例では、FTP トラフィックを識別し、FTP マップを定義し、ポリシーを定義し、厳密な FTP 検査をイネーブルにして、そのポリシーを外部インターフェイスに適用します。

```
hostname(config)# class-map ftp-port
hostname(config-cmap)# match port tcp eq 21
hostname(config-cmap)# exit
hostname(config)# ftp-map inbound_ftp
hostname(config-inbound_ftp)# request-command deny put stou appe
hostname(config-ftp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class ftp-port
hostname(config-pmap-c)# inspect ftp strict inbound_ftp
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

すべてのインターフェイスに対して厳密な FTP アプリケーション検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

(注)　FTP 制御接続用のポートだけを指定して、データ接続用は指定しません。セキュリティ アプライアンス ステートフル検査エンジンは、必要に応じて、ダイナミックにデータ接続を用意します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
mask-syst-reply	FTP サーバ応答をクライアントから見えないようにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
request-command deny	禁止する FTP コマンドを指定します。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect gtp

GTP 検査をイネーブルまたはディセーブルにする場合、または GTP トラフィックまたはトンネルを制御するための GTP マップを定義する場合は、クラス コンフィギュレーション モードで **inspect gtp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

inspect gtp [*map_name*]

no inspect gtp [*map_name*]

（注） GTP 検査には、特別なライセンスが必要です。セキュリティ アプライアンス上で **inspect gtp** コマンドを入力する場合、必要なライセンスを持っていないときは、セキュリティ アプライアンスによってエラー メッセージが表示されます。

シンタックスの説明

map_name	（オプション）GTP マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

GTP は、GPRS 用のトンネリング プロトコルで、無線ネットワーク上のセキュアなアクセスを可能にします。GPRS は、既存の GSM ネットワークを統合するために設計されたデータ ネットワーク アーキテクチャです。モバイル ユーザに対して、企業ネットワークとインターネットにアクセスするためのパケット スイッチ データ サービスを中断なく提供します。GTP の概要については、『*Cisco Security Appliance Command Line Configuration Guide*』の「アプリケーション層プロトコル検査の適用」の章を参照してください。

GTP のパラメータの定義に使用する特定のマップを指定するには、**gtp-map** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。基準を満たさないメッセージに対して指定できるアクションは、**drop** と **rate-limit** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

GTP マップを定義したら、**inspect gtp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

GTP の既知のポートは、次のとおりです。

- 3386
- 2123

次の機能は 7.0(1) ではサポートされていません。

- NAT、PAT、外部 NAT、エイリアス、およびポリシー NAT
- 3386、2123、および 2152 以外のポート
- トンネリング IP パケットとその内容の検証

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect gtp** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect gtp** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect gtp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例は、アクセス リストを使用して GTP トラフィックを識別し、GTP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list gtp-acl permit udp any any eq 3386
hostname(config)# access-list gtp-acl permit udp any any eq 2123
hostname(config)# class-map gtp-traffic
hostname(config)# match access-list gtp-acl
hostname(config)# gtp-map gtp-policy
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class gtp-traffic
hostname(config-pmap-c)# inspect gtp gtp-policy
hostname(config)# service-policy inspection_policy interface outside
```

（注） 次の例では、デフォルト値を使用して GTP 検査をイネーブルにします。デフォルト値を変更するには、**gtp-map** コマンドのページと、GTP マップ コンフィギュレーション モードから入力する各コマンドのページを参照してください。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。
show service-policy inspect gtp	**inspect gtp** ポリシーのステータスと統計を示します。

inspect h323

H.323 アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect h323** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect h323 {**h225** | **ras**}

no inspect h323 {**h225** | **ras**}

シンタックスの説明

h225	H.225 シグナリング検査をイネーブルにします。
ras	RAS 検査をイネーブルにします。

デフォルト

デフォルトのポート割り当ては次のとおりです。

- h323 h225 1720
- h323 ras 1718-1719

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect h323 コマンドは、Cisco CallManager および VocalTec Gatekeeper などの H.323 に準拠したアプリケーションをサポートしています。H.323 は、International Telecommunication Union（ITU; 国際電気通信連合）が定義した LAN 上のマルチメディア会議用のプロトコル スイートです。セキュリティ アプライアンスは、One Call Signaling Channel 上の Multiple Calls の H.323 v3 機能など、バージョン 4 までの H.323 をサポートしています。

H.323 検査がイネーブルの場合、セキュリティ アプライアンスは、H.323 バージョン 3 で導入された機能である、同一のコール シグナリング チャネル上の複数のコールをサポートします。この機能を使用すると、コール セットアップ時間が短縮され、セキュリティ アプライアンス上のポートの使用も削減されます。

H.323 検査には、次の 2 つの主要な機能があります。

- H.225 および H.245 メッセージ内の必要な埋め込み IPv4 アドレスの NAT を実行する。H.323 メッセージは PER 符号化フォーマットで符号化されているため、セキュリティ アプライアンスは、ASN.1 デコーダを使用して H.323 メッセージをデコードします。
- ネゴシエートされた H.245 接続および RTP/RTCP 接続をダイナミックに割り当てる。

H.323 の動作

H.323 のプロトコル コレクションでは、集合的に、2 つまでの TCP 接続と 4 ～ 6 の UDP 接続を使用できます。FastStart は TCP 接続を 1 つだけ使用し、RAS は登録、許可、およびステータス用に 1 つの UDP 接続を使用します。

H.323 クライアントでは、最初に、TCP ポート 1720 を使用して H.323 サーバへの TCP 接続を確立し、Q.931 コールのセットアップを要求できます。コール セットアップ プロセスの一部として、H.323 端末は、H.245 TCP 接続に使用するポート番号をクライアントに提供します。H.245 接続は、コール ネゴシエーションとメディア チャネルのセットアップに使用されます。H.323 ゲートキーパーを使用している環境では、最初のパケットは UDP を使用して送信されます。

H.323 検査は、Q.931 TCP 接続を監視して、H.245 ポート番号を判別します。H.323 端末が FastStart を使用していない場合、セキュリティ アプライアンスは、H.225 メッセージの検査に基づいて、H.245 接続をダイナミックに割り当てます。

(注) H.225 接続は、RAS を使用してダイナミックに割り当てることもできます。

各 H.245 メッセージ内で、H.323 エンドポイントは、以降の UDP データ ストリームに使用するポート番号を交換します。H.323 検査は、H.245 メッセージを検査してこれらのポートを識別し、メディア交換用の接続をダイナミックに作成します。Real-Time Transport Protocol（RTP）は、ネゴシエートされたポート番号を使用しますが、RTP Control Protocol（RTCP）は、次の上位ポート番号を使用します。

H.323 コントロール チャネルは、H.225、H.245、および H.323 RAS を処理します。H.323 検査は、次のポートを使用します。

- 1718：ゲートキーパー検出に使用される UDP ポート
- 1719：RAS およびゲートキーパー検出に使用される UDP ポート
- 1720：TCP 制御ポート

ゲートキーパーからの ACF メッセージがセキュリティ アプライアンスを通過する場合は、H.225 接続用のピンホールが空けられます。H.245 シグナリング ポートは、H.225 シグナリングのエンドポイント間でネゴシエートされます。H.323 ゲートキーパーが使用される場合、セキュリティ アプライアンスは、ACF メッセージの検査に基づいて、H.225 接続を開きます。セキュリティ アプライアンスに ACF メッセージが表示されない場合は、H.225 コール シグナリング用に既知の H.323 ポート 1720 のアクセス リストを開くことが必要となる場合があります。

セキュリティ アプライアンスは、H.225 メッセージを検査した後で、H.245 チャネルをダイナミックに割り当て、同様に検査する H.245 チャネルに接続します。これは、セキュリティ アプライアンスを通過した H.245 メッセージはすべて、H.245 アプリケーション検査を通過し、埋め込み IP アドレスの NAT が実行され、ネゴシエートされたメディア チャネルが開かれることを意味します。

H.323 ITU 標準では、信頼できる接続に送信する前に、メッセージ長を定義する TPKT ヘッダーを H.225 および H.245 の前に配置することが規定されています。TPKT ヘッダーは H.225/H.245 メッセージと同じ TCP パケットで送信されない場合もあるため、メッセージを正しく処理およびデコードするには、セキュリティ アプライアンスで TPKT 長を保持しておく必要があります。セキュリティ アプライアンスは、各接続のデータ構造を保持し、このデータ構造には、次に受信されるメッセージの TPKT 長が含まれます。

セキュリティ アプライアンスで任意の IP アドレスの NAT を実行する必要がある場合は、チェックサム、UUIE（user-user information element）の長さ、および TPKT（H.225 メッセージの TCP パケットに含まれている場合）を変更する必要があります。TPKT が別の TCP パケットで送信される場合、セキュリティ アプライアンスは TPKT のプロキシ ACK を実行し、H.245 メッセージに新しい長さの新しい TPKT を付加します。

（注） セキュリティ アプライアンスによる TPKT のプロキシ ACK では、TCP オプションはサポートされません。

H.323 検査を通過するパケットを使用する各 UDP 接続は、H.323 接続としてマークされ、**timeout** コマンドを使用して設定された H.323 タイムアウトでタイムアウトします。

制限と制約事項

次に、H.323 アプリケーション検査を使用する上での既知の問題および制限の一部を示します。

- スタティック PAT は、H.323 メッセージ内のオプション フィールドに埋め込まれた IP アドレスを正しく変換しない場合があります。この種の問題が発生した場合は、H.323 に対してスタティック PAT を使用しないでください。
- H.323 アプリケーション検査は、セキュリティ レベルの等しいインターフェイス間の NAT ではサポートされていません。
- NetMeeting クライアントが、H.323 ゲートキーパーに登録されている状態で、同じく H.323 ゲートキーパーに登録されている H.323 ゲートウェイにコールを発信しようとする場合、接続は確立されますが、音声が双方向で聞こえない現象が報告されています。この問題は、セキュリティ アプライアンスとは無関係です。
- ネットワーク スタティックを設定する場合、そのネットワーク スタティックがサードパーティのネットマスクおよびアドレスと同じであるときは、すべての発信 H.323 接続が失敗します。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect h323** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect h323** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect h323** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、H.323 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1720）上の H.323 トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map h323-port
hostname(config-cmap)# match port tcp eq 1720
hostname(config-cmap)# exit
hostname(config)# policy-map h323_policy
hostname(config-pmap)# class h323-port
hostname(config-pmap-c)# inspect h323
hostname(config-pmap-c)# exit
hostname(config)# service-policy h323_policy interface outside
```

すべてのインターフェイスに対して H.323 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
show h225	セキュリティ アプライアンスを越えて確立された H.225 セッションの情報を表示します。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout {h225 | h323}	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

inspect http

HTTP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect http** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect http [*map_name*]

no inspect http [*map_name*]

シンタックスの説明

map_name	（オプション）HTTP マップの名前。

デフォルト

HTTP のデフォルト ポートは 80 です。

高度な HTTP 検査は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect http コマンドは、HTTP トラフィックに関連する可能性のある特定の攻撃やその他の脅威から保護します。HTTP 検査では、高度な HTTP 検査が実行されます。

高度な HTTP 検査は、HTTP メッセージが RFC 2616 に準拠していること、RFC で定義されている方式やサポートされている拡張方式を使用していること、および他のさまざまな基準を満たしていることを確認します。多くの場合、これらの基準と、その基準が満たされないときのシステムの応答を設定できます。基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

HTTP メッセージに適用できる基準には、次のものがあります。

- リスト（設定可能）に挙げられているメソッドを含んでいない。
- 特定の転送符号化方式またはアプリケーション タイプ。
- HTTP トランザクションが RFC 仕様に沿っている。
- メッセージ本文のサイズが、制限値（設定可能）以下である。
- 要求と応答のメッセージ ヘッダーのサイズが、制限値（設定可能）以下である。
- URI の長さが制限値（設定可能）以下である。

- メッセージ本文の content-type が、ヘッダーと一致している。
- 応答メッセージの content-type が、要求メッセージの *accept-type* フィールドと一致している。
- メッセージの content-type が、事前定義済みの内部リストに挙げられている。
- メッセージが、RFC による HTTP 形式の基準を満たしている。
- 選択したサポート可能アプリケーションが存在している（または、存在していない）。
- 選択した符号化タイプが存在している（または、存在していない）。

（注） 基準を満たさないメッセージに対して指定できるアクションは、**allow**、**reset**、**drop** などのさまざまなコンフィギュレーション コマンドを使用して設定します。これらのアクションに加えて、イベントをログに記録するかどうかも指定できます。

高度な HTTP 検査をイネーブルにするには、**inspect http** *http-map* コマンドを使用します。このコマンドが HTTP トラフィックに適用する規則は、特定の HTTP マップで定義されます。この HTTP マップを設定するには、**http-map** コマンドと HTTP マップ コンフィギュレーション モードのコマンドを入力します。

（注） HTTP マップを使用して HTTP 検査をイネーブルにすると、デフォルトでは、アクション reset および log を使用した厳密な HTTP 検査がイネーブルになります。検査に合格しない場合に実行されるアクションは変更できますが、HTTP マップがイネーブルのままである限り、厳密な検査をディセーブルにすることはできません。

inspect http コマンドは syslog メッセージ 304001 を介して、GET 要求のロギングをイネーブルまたはディセーブルにします。

（注） **inspect http** コマンドを **inspect im** コマンドと共に設定すると、**inspect im** コマンドはディセーブルになります。

例

次の例は、HTTP トラフィックを識別し、HTTP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# class-map http-port
hostname(config-cmap)# match port tcp eq 80
hostname(config-cmap)# exit
hostname(config)# http-map inbound_http
hostname(config-http-map)# content-length min 100 max 2000 action reset log
hostname(config-http-map)# content-type-verification match-req-rsp reset log
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class http-port
hostname(config-pmap-c)# inspect http inbound_http
hostname(config-pmap-c)# exit
hostname(config-pmap)# exit
hostname(config)# service-policy inbound_policy interface outside
```

この例では、次のコンテンツを含んでいるトラフィックをセキュリティ アプライアンスが検出したときに、接続をリセットして syslog エントリを作成します。

- 100 バイト未満または 2,000 バイトを超えるメッセージ
- サポートされていないコンテンツ タイプ
- 100 バイトを超える HTTP ヘッダー
- 100 バイトを超える URI

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	HTTP アプリケーション検査に関する詳細情報を表示します。
debug http-map	HTTP マップに関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

inspect icmp

ICMP 検査エンジンを設定するには、クラス コンフィギュレーション モードで **inspect icmp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。

inspect icmp

no inspect icmp

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

ICMP 検査エンジンを使用すると、ICMP トラフィックを TCP トラフィックおよび UDP トラフィックと同様に検査できます。ICMP 検査エンジンを使用しない場合は、ACL により ICMP がセキュリティ アプライアンスを通過しないようにすることをお勧めします。ステートフル検査が実行されない場合、ICMP はネットワークの攻撃に利用されることがあります。ICMP 検査エンジンは、各要求に対する応答が 1 つだけであり、シーケンス番号が正しいことを確認します。

ICMP 検査エンジンがディセーブルの場合（デフォルト設定）、低セキュリティ インターフェイスから高セキュリティ インターフェイスへの ICMP エコー応答メッセージは拒否されます。このメッセージが ICMP エコー要求への応答である場合も同様です。

例

次の例に示すように、ICMP アプリケーション検査をイネーブルにします。この例では、ICMP プロトコル ID（IPv4 は 1、IPv6 は 58）を使用して、ICMP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
policy-map	セキュリティ アクションを 1 つまたはそれ以上のトラフィック クラスに関連付けるためのポリシーを定義します。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect icmp error

ICMP エラー メッセージに対するアプリケーション検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect icmp error** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。

inspect icmp error

no inspect icmp error

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect icmp error コマンドは、スタティック /NAT のコンフィギュレーションに基づいて、ICMP エラー メッセージを送信する中間ホップの xlate を作成する場合に使用します。デフォルトでは、セキュリティ アプライアンスは中間ホップの IP アドレスを表示しません。ただし、**inspect icmp error** コマンドを使用すると、中間ホップの IP アドレスが表示されます。セキュリティ アプライアンスは、パケットを変換後の IP アドレスで上書きします。

イネーブルの場合、ICMP エラー検査エンジンは、ICMP パケットに次の変更を加えます。

- IP ヘッダーで、NAT IP が Client IP（宛先アドレスおよび中間ホップ アドレス）に変更され、IP チェックサムが変更されます。
- ICMP ヘッダーで、ICMP チェックサムが ICMP パケットの変更に応じて変更されます。

- ペイロードでは、次の変更が加えられます。
  - 元のパケットの NAT IP が Client IP に変更されます。
  - 元のパケットの NAT ポートが Client Port に変更されます。
  - 元のパケットの IP チェックサムが再計算されます。

ICMP エラー メッセージが取得されると、ICMP エラー検査がイネーブルかどうかに関係なく、ICMP ペイロードがスキャンされ、元のパケットから 5 つのタプル（src ip、dest ip、src port、dest port、および ip プロトコル）が取得されます。取得された 5 つのタプルを使用して検索が実行され、クライアントの元のアドレスが判別され、特定の 5 つのタプルに関連付けられた既存のセッションが検出されます。セッションが検出されない場合、ICMP エラー メッセージはドロップされます。

例

次の例に示すように、ICMP エラー アプリケーション検査をイネーブルにします。この例では、ICMP プロトコル ID（IPv4 は 1、IPv6 は 58）を使用して、ICMP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map icmp-class
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# exit
hostname(config)# policy-map icmp_policy
hostname(config-pmap)# class icmp-class
hostname(config-pmap-c)# inspect icmp error
hostname(config-pmap-c)# exit
hostname(config)# service-policy icmp_policy interface outside
```

すべてのインターフェイスに対して ICMP エラー検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
inspect icmp	ICMP 検査エンジンをイネーブルまたはディセーブルにします。
policy-map	セキュリティ アクションを 1 つまたはそれ以上のトラフィック クラスに関連付けるためのポリシーを定義します。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect ils

ILS アプリケーション検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect ils** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect ils

no inspect ils

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ils コマンドは、LDAP を使用して ILS サーバとディレクトリ情報を交換する Microsoft NetMeeting、SiteServer、および Active Directory 製品用の NAT をサポートします。

セキュリティ アプライアンスは ILS の NAT をサポートしています。ILS は、ILS または SiteServer Directory のエンドポイントの登録および検出に使用されます。LDAP データベースには IP アドレスだけが保管されるため、PAT はサポートできません。

LDAP サーバが外部にある場合、検索応答を実行するには、NAT を使用して、外部 LDAP サーバに登録されている内部ピア間のローカル通信を可能にすることを考慮する必要があります。このような検索応答では、xlate、DNAT エントリの順に検索され、正しいアドレスが取得されます。両方の検索に失敗した場合、アドレスは変更されません。NAT 0 を使用している（NAT を使用していない）サイトや、DNAT 対話を想定していないサイトについては、パフォーマンスを向上させるために、検査エンジンをオフにすることをお勧めします。

ILS サーバがセキュリティ アプライアンス境界の内側にある場合は、追加の設定が必要になることがあります。この場合は、指定ポート（通常は TCP 389）上で LDAP サーバにアクセスする外部クライアント用のホールが必要です。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は、TCP 非アクティビティ間隔が経過すると切断されます。デフォルトでは、この間隔は 60 分です。間隔を調整するには、**timeout** コマンドを使用します。

ILS/LDAP は、クライアント / サーバ モデルに基づいて、単一 TCP 接続上のセッションを処理します。これらのセッションの一部は、クライアントのアクションに応じて作成される場合があります。

接続のネゴシエーション中に、クライアントからサーバに対して BIND PDU が送信されます。サーバから BIND RESPONSE を正常に受信すると、他の操作メッセージ（ADD、DEL、SEARCH、または MODIFY など）が交換され、ILS Directory 上で処理が実行されます。ADD REQUEST および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される NetMeeting ピアの IP アドレスが含まれる場合があります。Microsoft NetMeeting v2.X および v3.X では、ILS がサポートされています。

ILS 検査は、次の処理を実行します。

- BER デコード機能を使用して、LDAP REQUEST/RESPONSE PDU をデコードする。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスで PDU を符号化する。
- 新しく符号化した PDU を TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号を差分的に調整する。

ILS 検査には、次の制限があります。

- 照会の要求および応答はサポートされません。
- 複数のディレクトリのユーザは統合されません。
- 複数のディレクトリに別々の ID を持つ単一ユーザは、NAT では認識できません。

（注） H225 コール シグナリング トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は、TCP **timeout** コマンドで指定された間隔が経過すると切断されます。この間隔は、デフォルトでは 60 分に設定されています。

例

次の例に示すように、ILS 検査エンジンをイネーブルにします。この例では、デフォルト ポート（389）上の ILS トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map ils-port
hostname(config-cmap)# match port tcp eq 389
hostname(config-cmap)# exit
hostname(config)# policy-map ils_policy
hostname(config-pmap)# class ils-port
hostname(config-pmap-c)# inspect ils
hostname(config-pmap-c)# exit
hostname(config)# service-policy ils_policy interface outside
```

すべてのインターフェイスに対して ILS 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug ils	ILS のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect im

IM トラフィックの検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect im** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect im [*map_name*]

no inspect im [*map_name*]

シンタックスの説明

map_name	（オプション）IM マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

inspect im コマンドは、IM プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。

（注） **inspect im** コマンドは、**inspect http** コマンドと共に設定した場合、またはポート 80 に対して **filter activex**、**filter java**、または **filter url** の各 **filter** コマンドと共に設定した場合にディセーブルになります。

例

次の例では、IM 検査ポリシー マップを定義する方法を示します。

```
hostname(config)# regex loginname1 "ying\@yahoo.com"
hostname(config)# regex loginname2 "Kevin\@yahoo.com"
hostname(config)# regex loginname3 "rahul\@yahoo.com"
hostname(config)# regex loginname3 "darshant\@yahoo.com"
hostname(config)# regex yhoo_version_regex "1\.0"

hostname(config)# class-map type regex match-any yahoo_src_login_name_regex
hostname(config-cmap)# match regex loginname1
hostname(config-cmap)# match regex loginname2

hostname(config)# class-map type regex match-any yahoo_dst_login_name_regex
hostname(config-cmap)# match regex loginname3
hostname(config-cmap)# match regex loginname4

hostname(config)# class-map type regex match-any yhoo_file_block_list
hostname(config-cmap)# match regex ".*\.gif"
hostname(config-cmap)# match regex ".*\.exe"

hostname(config)# class-map type regex match-any new_im_regexp
hostname(config-cmap)# match regexp "new_im_regexp"

hostname(config)# class-map type inspect im match-all yahoo_im_policy
hostname(config-cmap)# match login-name regex class yhoo_src_login_name_regex
hostname(config-cmap)# match peer-login-name regex class yhoo_dst_login_name_regex

hostname(config)# class-map type inspect im yahoo_im_policy2
hostname(config-cmap)# match version regex yahoo_version_regex

hostname(config)# class-map im_inspect_class_map
hostname(config-cmap)# match default-inspection-traffic

hostname(config)# policy-map type im im_policy_all
hostname(config-pmap)# class yahoo_in_file_xfer_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yhoo_im_policy
hostname(config-pmap-c)# drop-connection
hostname(config-pmap)# class yhoo_im_policy2
hostname(config-pmap-c)# reset
hostname(config-pmap)# match im-pattern regex class new_im_regexp
hostname(config-pmap-c)# action log
hostname(config)# policy-map global_policy_name
hostname(config-pmap)# class im_inspection_class_map
hostname(config-pmap-c)# inspect im im_policy_all
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
match protocol	検査クラス マップまたは検査ポリシー マップに含まれている、特定の IM プロトコルに一致するかどうかを調べます。

inspect ipsec-pass-thru

IPSec Pass Thru 検査をイネーブルにするには、クラス マップ コンフィギュレーション モードで **inspect ipsec-pass-thru** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect ipsec-pass-thru [*map_name*]

no inspect ipsec-pass-thru [*map_name*]

シンタックスの説明

map_name	（オプション）IPSec Pass Thru マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

inspect ipsec-pass-thru コマンドはアプリケーション検査をイネーブルまたはディセーブルにします。IPSec Pass Through アプリケーション検査では、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）トラフィックと AH（IP プロトコル 51）トラフィックの便利な Traversal が提供されます。これにより、ESP トラフィックと AH トラフィックを許可するためのアクセス リスト設定が長くなることを回避でき、タイムアウトと最大接続数を使用したセキュリティも実現できます。

検査のパラメータを定義するために使用する特定のマップを指定するには、IPSec Pass Through パラメータ マップを使用します。パラメータ コンフィギュレーションにアクセスするには、**policy-map type inspect** コマンドを使用します。その後、ESP トラフィックまたは AH トラフィックに対する制約を指定できます。パラメータ コンフィギュレーションでは、クライアントごとの最大接続数、およびアイドル タイムアウトを設定できます。

class-map、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。定義したパラメータ マップは、**inspect IPSec-pass-thru** コマンドと共に使用されたときにイネーブルになります。

NAT トラフィックおよび非 NAT トラフィックが許可されます。ただし、PAT はサポートされていません。

(注)　ASA 7.0 では、**inspect ipsec-pass-thru** コマンドは、ESP トラフィックだけに通過を許可していました。以降のバージョンでも同じ動作が保持されるように、引数なしで **inspect ipsec-pass-thru** コマンドを指定した場合は、ESP を許可するデフォルトのマップが作成されて対応付けられます。このマップは、**show running-config all** コマンドの出力で確認できます。

例

次の例は、アクセス リストを使用して IKE トラフィックを識別し、IPSec Pass Thru パラメータ マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list ipsecpassthruacl permit udp any any eq 500
hostname(config)# class-map ipsecpassthru-traffic
hostname(config-cmap)# match access-list ipsecpassthruacl
hostname(config)# policy-map type inspect ipsec-pass-thru iptmap
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
hostname(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
hostname(config)# policy-map inspection_policy
hostname(config-pmap)# class ipsecpassthru-traffic
hostname(config-pmap-c)# inspect ipsec-pass-thru iptmap
hostname(config)# service-policy inspection_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
match protocol	検査クラス マップまたは検査ポリシー マップに含まれている、特定の IM プロトコルに一致するかどうかを調べます。

inspect mgcp

MGCP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect mgcp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect mgcp [*map_name*]

no inspect mgcp [*map_name*]

シンタックスの説明

map_name	（オプション）MGCP マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

MGCP を使用する場合、通常、少なくとも 2 つの **inspect** コマンドを設定する必要があります。1 つはゲートウェイがコマンドを受信するポート用で、もう 1 つは Call Agent がコマンドを受信するポート用です。通常、Call Agent は、ゲートウェイのデフォルトの MGCP ポート 2427 にコマンドを送信し、ゲートウェイは、Call Agents のデフォルトの MGCP ポート 2727 にコマンドを送信します。

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部のコール制御要素からメディア ゲートウェイを制御するために使用されます。メディア ゲートウェイは、一般的に、電話回線上で伝送されるオーディオ信号と、インターネットまたは他のパケット ネットワーク上で伝送されるデータ パケットとの変換を行うネットワーク要素です。MGCP で NAT および PAT を使用すると、限られた数の外部（グローバル）アドレスで、内部ネットワーク上の多数のデバイスをサポートできます。

次に、メディア ゲートウェイの例を示します。

- トランキング ゲートウェイ。これは、電話網と Voice over IP ネットワーク間のインターフェイスです。このゲートウェイは、一般的に、多数のデジタル回線を管理します。
- レジデンシャル ゲートウェイ。これは、Voice over IP ネットワークに従来のアナログ（RJ11）インターフェイスを提供します。レジデンシャル ゲートウェイの例には、ケーブル モデム / ケーブル セットトップ ボックス、xDSL デバイス、ブロードバンド無線デバイスなどがあります。

- ビジネス ゲートウェイ。これは、Voice over IP ネットワークに従来のデジタル PBX インターフェイスまたは統合 *soft PBX* インターフェイスを提供します。

MGCP メッセージは、UDP 上で転送されます。応答は、コマンドの送信元アドレス（IP アドレスおよび UDP ポート番号）に返送されますが、コマンドの宛先と同じアドレスから返送されない場合があります。この状況が発生するのは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用され、コマンドを受信したコール エージェントからバックアップ コール エージェントに制御が渡された後で、バックアップ コール エージェントが応答を返送する場合です。

(注)　MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判別します。この結果、セキュリティ アプライアンスからのフローが確立され、MGCP エンドポイントがコール エージェントに登録できるようになります。

1 つ以上のコール エージェントおよびゲートウェイの IP アドレスを設定するには、MGCP マップ コンフィギュレーション モードで **call-agent** コマンドと **gateway** コマンドを使用します。コマンド キューに一度に入れることができる MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect mgcp** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect mgcp** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect mgcp** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例は、MGCP トラフィックを識別し、MGCP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。この例では、デフォルト ポート（2427 および 2727）上の MGCP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# access-list mgcp_acl permit tcp any any eq 2427
hostname(config)# access-list mgcp_acl permit tcp any any eq 2727
hostname(config)# class-map mgcp_port
hostname(config-cmap)# match access-list mgcp_acl
hostname(config-cmap)# exit
hostname(config)# mgcp-map inbound_mgcp
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
hostname(config-mgcp-map)# gateway 10.10.10.117 102
hostname(config-mgcp-map)# command-queue 150
hostname(config-mgcp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class mgcp_port
hostname(config-pmap-c)# inspect mgcp mgcp-map inbound_mgcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy inbound_policy interface outside
```

このコンフィギュレーションにより、コール エージェント 10.10.11.5 と 10.10.11.6 がゲートウェイ 10.10.10.115 を制御できるようになり、コール エージェント 10.10.11.7 と 10.10.11.8 がゲートウェイ 10.10.10.116 と 10.10.10.117 の両方を制御できるようになります。キューに入れることができる MGCP コマンドの最大数は、150 です。

すべてのインターフェイスの MGCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug mgcp	MGCP デバッグ情報をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	セキュリティ アプライアンスを介して確立された MGCP セッションに関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect netbios

NetBIOS アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect netbios コマンド**を使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect netbios [*map_name*]

no inspect netbios [*map_name*]

シンタックスの説明

map_name	（オプション）NetBIOS マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect netbios コマンドは、NetBIOS プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。

例

次の例では、NetBIOS 検査ポリシー マップを定義する方法を示しています。

```
hostname(config)# policy-map type inspect netbios netbios_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-violation drop
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect pptp

PPTP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect pptp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect pptp

no inspect pptp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Point-to-Point Tunneling Protocol（PPTP）は、PPP トラフィックをトンネリングするためのプロトコルです。PPTP セッションを構成するのは、1 つの TCP チャネルと、通常 2 つの PPTP GRE トンネルです。TCP チャネルは、PPTP GRE トンネルをネゴシエートおよび管理するためのコントロール チャネルです。GRE トンネルは、2 つのホスト間で PPP セッションを伝送します。

イネーブルの場合、PPTP アプリケーション検査は、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するのに必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 に定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP コントロール チャネルを越えてネゴシエートされる場合、GRE **[**RFC 2637**]** の修正版に対してだけ実行されます。Port Address Translation（PAT; ポート アドレス変換）は、修正前のバージョンの GRE **[**RFC 1701、RFC 1702**]** に対しては*実行されません*。

特に、セキュリティ アプライアンスは、PPTP バージョンのアナウンスメントと発信コールの要求 / 応答シーケンスを検査します。RFC 2637 に定義されている PPTP バージョン 1 だけが検査されます。どちらかの側でアナウンスされたバージョンがバージョン 1 でなければ、TCP コントロール チャネルはそれ以上検査されません。さらに、発信コール要求と応答シーケンスが追跡されます。接続と xlate は、必要に応じてダイナミックに割り当てられて、それ以後のセカンダリ GRE データ トラフィックを送ることが可能になります。

PPTP 検査エンジンは、PPTP トラフィックを PAT で変換するためにイネーブルにする必要があります。さらに、PAT は、GRE（RFC2637）の修正版に対してだけで実行されます。これは、PPTP TCP コントロール チャネルを越えてネゴシエートされる場合だけです。PAT は、修正前のバージョンの GRE（RFC 1701 と RFC 1702）に対しては実行されません。

RFC 2637 で規定されているように、PPTP プロトコルは、主に、モデム バンク PPTP Access Concentrator（PAC; PPTP アクセス コンセントレータ）から開始された PPP セッションをヘッドエンド PPTP Network Server（PNS; PPTP ネットワーク サーバ）へトンネリングするために使用されます。この使用方法では、PAC はリモート クライアントとなり、PNS はサーバとなります。

ただし、Windows によって VPN 用に使用される場合、対話関係は逆になります。PNS は、ヘッドエンド PAC への接続を開始して中央ネットワークにアクセスするリモート シングルユーザ PC です。

例

次の例に示すように、PPTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1723）上の PPTP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map pptp-port
hostname(config-cmap)# match port tcp eq 1723
hostname(config-cmap)# exit
hostname(config)# policy-map pptp_policy
hostname(config-pmap)# class pptp-port
hostname(config-pmap-c)# inspect pptp
hostname(config-pmap-c)# exit
hostname(config)# service-policy pptp_policy interface outside
```

すべてのインターフェイスに対して PPTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug pptp	PPTP のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect radius-accouting

RADIUS アカウンティング検査をイネーブルまたはディセーブルにする場合、またはトラフィックまたはトンネルを制御するためのマップを定義する場合は、クラス コンフィギュレーション モードで **inspect radius-accounting** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

inspect radius-accounting [*map_name*]

no inspect radius-accounting [*map_name*]

シンタックスの説明

map_name	（オプション）RADIUS アカウンティング マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RADIUS アカウンティングのパラメータの定義に使用する特定のマップを指定するには、**radius-accounting** コマンドを使用します。このコマンドを入力すると、システムがコンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。さまざまなコンフィギュレーション コマンドを使用して設定した基準を満たさないメッセージに対して指定できるアクションは、**send**、**host**、**validate-attribute**、**enable gprs**、**timeout users** などです。***parameter*** モードからこれらのコマンドにアクセスできます。

RADIUS アカウンティング マップを定義したら、**inspect gtp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

（注） **inspect radius-accounting** コマンドと共に使用できるのは **class-map type management** コマンドだけです。

例

次の例は、アクセス リストを使用して RADIUS アカウンティング トラフィックを識別し、RADIUS アカウンティングを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# policy-map type inspect radius-accountin ra
```

(注) 次の例では、デフォルト値を使用して RADIUS アカウンティング検査をイネーブルにします。デフォルト値を変更するには、**parameters** コマンドのページと、RADIUS アカウンティング コンフィギュレーション モードから入力する各コマンドのページを参照してください。

関連コマンド

コマンド	説明
parameters	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
class-map type management	アクションを適用するセキュリティ アプライアンスに宛てたレイヤ 3 またはレイヤ 4 の管理トラフィックを識別します。
show および **clear service-policy**	サービス ポリシーの設定を表示および消去します。
debug inspect radius-accounting	RADIUS アカウンティング検査をデバッグします。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect rsh

RSH アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect rsh** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect rsh

no inspect rsh

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RSH プロトコルは、TCP ポート 514 上で、RSH クライアントから RSH サーバへの TCP 接続を使用します。クライアントとサーバは、クライアントが STDERR 出力ストリームをリッスンする TCP ポート番号をネゴシエートします。RSH 検査は、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

例

次の例に示すように、RSH 検査エンジンをイネーブルにします。この例では、デフォルト ポート（514）上の RSH トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map rsh-port
hostname(config-cmap)# match port tcp eq 514
hostname(config-cmap)# exit
hostname(config)# policy-map rsh_policy
hostname(config-pmap)# class rsh-port
hostname(config-pmap-c)# inspect rsh
hostname(config-pmap-c)# exit
hostname(config)# service-policy rsh_policy interface outside
```

すべてのインターフェイスに対して RSH 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect rtsp

RTSP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect rtsp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect rtsp

no inspect rtsp

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　このコマンドは、デフォルトではディセーブルになっています。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン　**inspect rtsp** コマンドを使用すると、セキュリティ アプライアンスが RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV 接続が使用します。

（注）　Cisco IP/TV の場合は、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、コントロール チャネルとして、既知ポート 554 と TCP（まれに UDP）を使用します。セキュリティ アプライアンスは、RFC 2326 に準拠して、TCP だけをサポートしています。この TCP コントロール チャネルは、クライアント上で設定された転送モードに応じて、オーディオ/ビデオ トラフィックの伝送に使用するデータ チャネルをネゴシエートするために使用されます。

サポートされる RDT 転送は、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、および x-pn-tng/udp です。

セキュリティ アプライアンスは、Setup 応答メッセージをステータス コード 200 によって解析します。応答メッセージが内側へ進んでいる場合、サーバはセキュリティ アプライアンスの外側にあるため、サーバから内側へ来る接続用にダイナミック チャネルを開く必要があります。応答メッセージが発信の場合、セキュリティ アプライアンスでダイナミック チャネルを開く必要はありません。

RFC 2326 では、SETUP 応答メッセージにクライアント ポートとサーバのポートを含めることを規定していないため、セキュリティ アプライアンスで状態を保持し、SETUP メッセージ内のクライアント ポートを記憶しておく必要があります。QuickTime では、SETUP メッセージにクライアント ポートが設定され、サーバはサーバ ポートでのみ応答します。

RealPlayer の使用方法

RealPlayer を使用している場合、転送モードを正しく設定することが重要です。セキュリティ アプライアンスでは、**access-list** コマンド文は、サーバからクライアントへと、またはその逆で追加されます。RealPlayer の場合、**Options**>**Preferences**>**Transport**>**RTSPSettings** をクリックすることで、転送モードを変更します。

RealPlayer 上で TCP モードを使用している場合、**Use TCP to Connect to Server** チェックボックスと **Attempt to use TCP for all content** チェックボックスをオンにします。セキュリティ アプライアンス上では、検査エンジンを設定する必要はありません。

RealPlayer 上で UDP モードを使用している場合、**Use TCP to Connect to Server** チェックボックスと **Attempt to use UDP for all content** チェックボックスをオンにします。マルチキャスト経由で入手できないライブ コンテンツに対しても同様です。セキュリティ アプライアンス上で、**inspect rtsp** *port* コマンド文を追加します。

制約事項と制限

inspect rtsp コマンドには、次の制約事項が適用されます。

- セキュリティ アプライアンスは、UDP を介したマルチキャスト RTSP メッセージも RTSP メッセージもサポートしていません。
- **inspect rtsp** コマンドは、PAT をサポートしていません。
- セキュリティ アプライアンスには、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- セキュリティ アプライアンスは、RTSP メッセージについて NAT は実行できません。その理由は、埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として、SDP ファイルに含まれているからです。パケットはフラグメント化される可能性があり、セキュリティ アプライアンスは、フラグメント化されたパケットについて NAT は実行できません。
- Cisco IP/TV では、メッセージの SDP 部分についてセキュリティ アプライアンスが実行する NAT の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Viewer と Content Manager が外部ネットワークに、サーバが内部ネットワークにある場合、Cisco IP/TV は、NAT が使用できる場合に限り動作します。
- HTTP を介して配信されるメディア ストリームは、RTSP アプリケーション検査ではサポートされません。これは、RTSP 検査が HTTP クローキング（HTTP でラップされた RTSP）をサポートしていないためです。

例

次の例に示すように、RTSP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（554 および 8554）上の RTSP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# access-list rtsp-acl permit tcp any any eq 554
hostname(config)# access-list rtsp-acl permit tcp any any eq 8554
hostname(config)# class-map rtsp-traffic
hostname(config-cmap)# match access-list rtsp-acl
hostname(config-cmap)# exit
hostname(config)# policy-map rtsp_policy
hostname(config-pmap)# class rtsp-port
hostname(config-pmap-c)# inspect rtsp
hostname(config-pmap-c)# exit
hostname(config)# service-policy rtsp_policy interface outside
```

すべてのインターフェイスに対して RTSP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug rtsp	RTSP のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect sip

SIP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect sip** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sip

no inspect sip

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

SIP に対するデフォルトのポート割り当ては 5060 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SIP は、IETF で定義されているように、VoIP コールをイネーブルにします。SIP は SDP と連携して、コール シグナリングを処理します。SDP は、メディア ストリームの詳細を指定します。SIP を使用すると、セキュリティ アプライアンスは、あらゆる SIP Voice over IP（VoIP）ゲートウェイおよび VoIP プロキシ サーバをサポートできます。SIP と SDP は、次の RFC に定義されています。

- SIP：Session Initiation Protocol、RFC 2543
- SDP：Session Description Protocol、RFC 2327

セキュリティ アプライアンス経由の SIP コールをサポートするには、メディア接続アドレス宛のシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。これは、シグナリングが既知の宛先ポート（UDP/TCP 5060）を通じて送信されている間に、メディア ストリームがダイナミックに割り当てられるためです。また、SIP は、IP パケットのユーザデータ部分に IP アドレスを埋め込みます。SIP 検査は、これらの埋め込み IP アドレスに NAT を適用します。

(注)　リモート エンドポイントから、セキュリティ アプライアンスによって保護されたネットワーク上の SIP プロキシに登録する場合、ごく特殊な条件に合致すると登録が失敗します。この条件とは、PAT がリモート エンドポイントに対して設定されている場合、SIP レジストラ サーバが外部ネットワーク上にある場合、およびエンドポイントからプロキシ サーバに送信される REGISTER メッセージの contact フィールドにポートが指定されていない場合です。

インスタント メッセージ

インスタント メッセージとは、ほぼリアルタイムで行われるユーザ間のメッセージ転送を指します。MESSAGE/INFO 方式と 202 Accept 応答は、次の RFC で定義されている IM をサポートするために使用されます。

- Session Initiation Protocol (SIP)-Specific Event Notification、RFC 3265
- Session Initiation Protocol (SIP) Extension for Instant Messaging、RFC 3428

MESSAGE/INFO 要求は、登録 / 加入が完了するといつでも受信できます。たとえば、2 つのユーザはいつでもオンラインにできますが、何時間もチャットすることはできません。そのため、SIP 検査エンジンは、設定された SIP タイムアウト値に従ってタイムアウトするピンホールを空けます。この値には、加入期間より 5 分以上長い値を設定する必要があります。加入期間は、Contact Expires 値で定義されます。通常は、30 分にします。

MESSAGE/INFO 要求は、通常、ダイナミックに割り当てられたポート（ポート 5060 を除く）を使用して送信されるため、SIP 検査エンジンを通過する必要があります。

(注)　現在サポートされているのは、チャット機能のみです。ホワイトボード、ファイル転送、およびアプリケーション共有はサポートされていません。RTC Client 5.0 はサポートされていません。

技術的詳細

SIP 検査は、SIP のテキストベースのメッセージについて NAT を実行し、メッセージの SDP 部分に関するコンテンツの長さを再計算し、パケット長とチェックサムを再計算します。また、エンドポイントがリッスンするアドレス / ポートとして SIP メッセージの SDP 部分で指定されたポートに対して、メディア接続をダイナミックに開きます。

SIP 検査には、コールや送信元 / 宛先を識別する SIP ペイロードからの CALL_ID/FROM/TO インデックスに関するデータベースがあります。このデータベースには、SDP メディア情報フィールドに含まれていたメディア アドレスとメディア ポート、およびメディア タイプが保管されます。1 つのセッションに対して複数のメディア アドレスとポートを指定できます。RTP/RTCP 接続は、これらのメディア アドレス / ポートを使用して 2 つのエンドポイント間で開かれます。

初回のコール セットアップ（INVITE）メッセージには、既知ポート 5060 を使用する必要があります。ただし、以降のメッセージには、このポート番号を使用しなくてもかまいません。SIP 検査エンジンは、シグナリング接続のピンホールを空け、これらの接続を SIP 接続としてマークします。これは、メッセージを SIP アプリケーションに到達させ、メッセージに NAT を適用するためです。

コールがセットアップされると、SIP セッションは「一時的な」状態にあると見なされます。この状態は、宛先エンドポイントがリッスンしている RTP メディア アドレスおよびポートを示す Response メッセージが受信されるまで維持されます。1 分以内に応答メッセージが受信されなかった場合、シグナリング接続は切断されます。

最後のハンドシェイクが完了すると、コールの状態がアクティブに移行し、BYE メッセージを受信するまでシグナリング接続が維持されます。

内部エンドポイントから外部エンドポイントにコールを開始する場合は、内部エンドポイントからの INVITE メッセージに指定される内部エンドポイントのメディア アドレスおよびメディア ポートに RTP/RTCP UDP パケットが転送されるように、外部インターフェイスに対してメディア ホールが空けられます。内部インターフェイスへの非送信請求 RTP/RTCP UDP パケットは、セキュリティ アプライアンス コンフィギュレーションで特別に許可されている場合を除き、セキュリティ アプライアンスを通過しません。

メディア接続は、接続がアイドル状態になってから 2 分以内に切断されます。ただし、このタイムアウトは設定変更できるため、期間を増減して設定できます。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect sip** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect sip** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect sip** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SIP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（5060）上の SIP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sip-port
hostname(config-cmap)# match port tcp eq 5060
hostname(config-cmap)# exit
hostname(config)# policy-map sip_policy
hostname(config-pmap)# class sip-port
hostname(config-pmap-c)# inspect sip
hostname(config-pmap-c)# exit
hostname(config)# service-policy sip_policy interface outside
```

すべてのインターフェイスに対して SIP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
show sip	セキュリティ アプライアンスを介して確立された SIP セッションに関する情報を表示します。
debug sip	SIP のデバッグ情報をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect skinny

SCCP（Skinny）アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect skinny** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect skinny

no inspect skinny

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Skinny（または Simple）Client Control Protocol（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境で共存できます。Cisco CallManager を併用することで、SCCP クライアントは、H.323 準拠端末と相互運用できます。セキュリティ アプライアンスのアプリケーション レイヤ機能は、SCCP バージョン 3.3 を認識します。アプリケーション レイヤ ソフトウェアの機能により、SCCP シグナリング パケットの NAT を実行して、すべての SCCP シグナリングおよびメディア パケットがセキュリティ アプライアンスを通過できることが保証されます。

SCCP プロトコルのバージョンには、2.4、3.0.4、3.1.1、3.2、および 3.3.2 の 5 つがあります。セキュリティ アプライアンスは、バージョン 3.3.2 までのバージョンをすべてサポートします。また、SCCP の PAT および NAT を両方サポートします。IP Phone で使用するグローバル IP アドレスの数を制限している場合は、PAT が必要です。

Cisco CallManager と Cisco IP Phone 間の通常のトラフィックは、SCCP を使用します。また、特に設定しない限り、SCCP 検査によって処理されます。セキュリティ アプライアンスは、DHCP option 150 および DHCP option 66 もサポートしているため、TFTP サーバの場所を Cisco IP Phone や他の DHCP クライアントに送信できます。詳細については、**dhcp-server** コマンドを参照してください。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone よりもセキュリティの高いインターフェイス上にあるトポロジにおいて、Cisco CallManager IP アドレスの NAT が必要になる場合、Cisco IP Phone では Cisco CallManager IP アドレスをそのコンフィギュレーションで明示的に指定する必要があるため、マッピングは**スタティック**にする必要があります。ID スタティック エントリを使用した場合、高セキュリティ インターフェイス上の Cisco CallManager は Cisco IP Phone からの登録を受け入れることができます。

Cisco IP Phone は、TFTP サーバにアクセスして、Cisco CallManager サーバへの接続時に必要となるコンフィギュレーション情報ダウンロードする必要があります。

Cisco IP Phone が TFTP サーバよりもセキュリティの低いインターフェイス上にある場合は、アクセス リストを使用して、UDP ポート 69 上で保護された TFTP サーバに接続する必要があります。TFTP サーバにはスタティック エントリが必要ですが、「ID」スタティック エントリにする必要はありません。NAT を使用する場合、ID スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスおよびポートにマッピングされます。

Cisco IP Phone が TFTP サーバおよび Cisco CallManager よりもセキュリティの*高い*インターフェイス上にある場合、Cisco IP Phone で接続を開始できるようにするためのアクセス リストまたはスタティック エントリは必要ありません。

制約事項と制限

次に、SCCP に対する現行バージョンの PAT および NAT サポートに適用される制限を示します。

- PAT は、**alias** コマンドを使用するコンフィギュレーションは扱いません。
- 外部 NAT または PAT は**サポートされません**。

（注） 現在、SCCP コールのステートフル フェールオーバーは、コール セットアップ中のコールを除いて、サポートされています。

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートを設定している場合、セキュリティ アプライアンスは、現在のところ TFTP を経由して転送するファイルの内容に対して NAT または PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。セキュリティ アプライアンスは、TFTP メッセージの NAT をサポートしており、TFTP ファイル用のピンホールを空けて、セキュリティ アプライアンスを通過するようにしますが、電話機の登録中に TFTP を使用して転送される Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれている Cisco CallManager IP アドレスとポートは変換できません。

シグナリング メッセージの検査

シグナリング メッセージを検査する場合、**inspect skinny** コマンドでは、多くの場合、メディア エンドポイント（たとえば、IP 電話）の場所を正確に知る必要があります。

この情報は、メディア トラフィックのためのアクセス制御と NAT 状態を準備して、手作業での設定なしでメディア トラフィックを透過的にファイアウォールを通過させるために使用されます。

この場所を調べる場合、**inspect skinny** コマンドは、トンネル デフォルト ゲートウェイのルートを**使用しません**。トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPSec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect skinny** コマンドが必要となる場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例に示すように、SCCP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（2000）上の SCCP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map skinny-port
hostname(config-cmap)# match port tcp eq 2000
hostname(config-cmap)# exit
hostname(config)# policy-map skinny_policy
hostname(config-pmap)# class skinny-port
hostname(config-pmap-c)# inspect skinny
hostname(config-pmap-c)# exit
hostname(config)# service-policy skinny_policy interface outside
```

すべてのインターフェイスに対して SCCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug skinny	SCCP のデバッグ情報をイネーブルにします。
show skinny	セキュリティ アプライアンスを介して確立された SCCP セッションに関する情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect snmp

SNMP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect snmp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect snmp *map_name*

no inspect snmp *map_name*

シンタックスの説明

map_name	SNMP マップの名前。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

inspect snmp コマンドは、SNMP マップに関する設定値を使用して SNMP 検査をイネーブルにするために使用します。SNMP マップを作成するには、**snmp-map** コマンドを使用します。SNMP トラフィックを特定のバージョンの SNMP に制限するには、SNMP マップ コンフィギュレーション モードで **deny version** コマンドを使用します。

以前のバージョンの SNMP はセキュリティ レベルが低いため、セキュリティ ポリシーで SNMP トラフィックをバージョン 2 に制限することが必要となる場合があります。特定のバージョンの SNMP を拒否するには、SNMP マップ内で **deny version** コマンドを使用します。SNMP マップを作成するには、**snmp-map** コマンドを使用します。SNMP マップを設定したら、**inspect snmp** コマンドを使用してマップをイネーブルにします。次に、**service-policy** コマンドを使用して、1 つまたは複数のインターフェイスにマップを適用します。

例

次の例では、SNMP トラフィックを識別し、SNMP マップを定義し、ポリシーを定義し、SNMP 検査をイネーブルにして、そのポリシーを外部インターフェイスに適用します。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)# exit
```

すべてのインターフェイスに対して厳密な SNMP アプリケーション検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect sqlnet

Oracle SQL*Net アプリケーション検査をイネーブルにするには、クラス コンフィギュレーション モードで **inspect sqlnet** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sqlnet

no inspect sqlnet

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

デフォルトのポート割り当ては 1521 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

SQL*Net プロトコルは種々のパケット タイプで構成されています。セキュリティ アプライアンスは、セキュリティ アプライアンスの両側でデータ ストリームが Oracle アプリケーションに同一に見えるように、これらのパケット タイプを処理します。

SQL*Net のデフォルトのポート割り当ては 1521 です。この値は、Oracle for SQL*Net で使用されるものですが、Structured Query Language（SQL; 構造化照会言語）の IANA ポート割り当てとは一致しません。**class-map** コマンドを使用して、一定範囲のポート番号に SQL*Net 検査を適用します。

セキュリティ アプライアンスは、すべてのアドレスの NAT を実行し、パケット内の埋め込みポートをすべて検索して、SQL*Net バージョン 1 用に開きます。

SQL*Net バージョン 2 では、データ長が 0 の REDIRECT パケットの直後に続くすべての DATA または REDIRECT パケットがフィックスアップされます。

フィックスアップを必要とするパケットには、埋め込みホスト / ポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の TNSFrame タイプ（Connect、Accept、Refuse、Resend、および Marker）では、NAT 対象のアドレスを検出するためのスキャンは実行されません。また、検査によってパケット内の埋め込みポートに対してダイナミック接続が開かれることもありません。

SQL*Net バージョン 2 の TNSFrames パケット、Redirect パケット、および Data パケットは、直前に、ペイロードのデータ長が 0 である REDIRECT TNSFrame タイプがある場合は、開くポートおよび NAT 対象のアドレスを検出するためにスキャンされます。データ長が 0 の Redirect メッセージがセキュリティ アプライアンスを通過すると、次に到着する Data または Redirect メッセージが NAT 対象で、ポートがダイナミックに開かれることを示すために、接続データ構造にフラグが設定されます。前述の TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net 検査エンジンは、新しいメッセージと古いメッセージの長さのデータを使用して、チェックサムを再計算し、IP/TCP の長さを変更し、シーケンス番号と確認応答番号を再調整します。

その他すべてのケースでは、SQL*Net バージョン 1 の使用が前提となっています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、および Data）とすべてのパケットがスキャンされ、ポートとアドレスが検出されます。アドレスに NAT が適用され、ポート接続が開かれます。

例

次の例に示すように、SQL*Net 検査エンジンをイネーブルにします。この例では、デフォルト ポート（1521）上の SQL*Net トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sqlnet-port
hostname(config-cmap)# match port tcp eq 1521
hostname(config-cmap)# exit
hostname(config)# policy-map sqlnet_policy
hostname(config-pmap)# class sqlnet-port
hostname(config-pmap-c)# inspect sqlnet
hostname(config-pmap-c)# exit
hostname(config)# service-policy sqlnet_policy interface outside
```

すべてのインターフェイスに対して SQL*Net 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug sqlnet	SQL*Net のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。
show conn	SQL*Net など、さまざまな接続タイプの接続状態を表示します。

inspect sunrpc

Sun RPC アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc

no inspect sunrpc

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、**fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

Sun RPC アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、ポリシー マップ クラス コンフィギュレーション モードで **inspect sunrpc** コマンドを使用します。このモードには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用してアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect sunrpc コマンドは、Sun RPC プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスは、システム上のどのポートでも動作可能です。クライアントからサーバ上の Sun RPC サービスにアクセスする場合は、サービスが動作しているポートを検出する必要があります。検出するには、既知ポート 111 上のポートマッパー プロセスにクエリーします。

クライアントは、サービスの Sun RPC プログラム番号を送信して、ポート番号を取得します。この時点で、クライアント プログラムはその新しいポートに Sun RPC クエリーを送信します。サーバから応答が送信されると、セキュリティ アプライアンスはこのパケットを代行受信し、そのポート上で TCP および UDP の両方の初期接続を開きます。

（注） Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

例

次の例に示すように、RPC 検査エンジンをイネーブルにします。この例では、デフォルト ポート（111）上の RPC トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map sunrpc-port
hostname(config-cmap)# match port tcp eq 111
hostname(config-cmap)# exit
hostname(config)# policy-map sample_policy
hostname(config-pmap)# class sunrpc-port
hostname(config-pmap-c)# inspect sunrpc
hostname(config-pmap-c)# exit
hostname(config)# service-policy sample_policy interface outside
```

すべてのインターフェイスに対して RPC 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
clear configure sunrpc_server	**sunrpc-server** コマンドを使用して実行されたコンフィギュレーションを削除します。
clear sunrpc-server active	NFS や NIS など、特定のサービスの Sun RPC アプリケーション検査で空けられたピンホールを消去します。
show running-config sunrpc-server	Sun RPC サービス テーブル コンフィギュレーションに関する情報を表示します。
sunrpc-server	NFS や NIS などの Sun RPC サービスに対して、タイムアウトを指定してピンホールを作成できるようにします。
show sunrpc-server active	Sun RPC サービスに対して空けられたピンホールを表示します。

inspect tftp

TFTP アプリケーション検査をディセーブルにする場合、またはディセーブルの状態からイネーブルにする場合は、クラス コンフィギュレーション モードで **inspect tftp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect ftp

no inspect tftp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

デフォルトのポート割り当ては 69 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

RFC 1350 で規定されている Trivial File Transfer Protocol（TFTP）は、TFTP サーバとクライアント間でファイルの読み書きを行うための簡易プロトコルです。

セキュリティ アプライアンスは、TFTP トラフィックを検査し、必要に応じて接続と変換をダイナミックに作成して、TFTP クライアントとサーバ間のファイル転送を許可します。特に、検査エンジンは、TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）およびエラー通知（ERROR）を検査します。

有効な読み取り（RRQ）要求または書き込み（WRQ）要求が受信されると、必要に応じて、ダイナミック セカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、後で TFTP によってファイル転送またはエラー通知に使用されます。

セカンダリ チャネル上でトラフィックを開始できるのは、TFTP サーバのみです。また、TFTP クライアントとサーバ間に存在できる不完全なセカンダリ チャネルは最大で 1 つです。サーバからエラー通知が送信されると、セカンダリ チャネルは閉じられます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用される場合は、TFTP 検査をイネーブルにする必要があります。

例

次の例に示すように、TFTP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（69）上の TFTP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map tftp-port
hostname(config-cmap)# match port udp eq 69
hostname(config-cmap)# exit
hostname(config)# policy-map tftp_policy
hostname(config-pmap)# class tftp-port
hostname(config-pmap-c)# inspect tftp
hostname(config-pmap-c)# exit
hostname(config)# service-policy tftp_policy interface outside
```

すべてのインターフェイスに対して TFTP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

inspect xdmcp

XDMCP アプリケーション検査をイネーブルにする場合、またはセキュリティ アプライアンスがリッスンするポートを変更する場合は、クラス コンフィギュレーション モードで **inspect xdmcp** コマンドを使用します。クラス コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

inspect xdmcp

no inspect xdmcp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入され、既存の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect xdmcp コマンドは、XDMCP プロトコルのアプリケーション検査をイネーブルまたはディセーブルにします。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは、確立後は TCP を使用します。

ネゴシエーションを成功させ、XWindows セッションを正常に起動するには、セキュリティ アプライアンスは、Xhosted コンピュータからの TCP バック接続を許可する必要があります。バック接続を許可するには、セキュリティ アプライアンス上で **established** コマンドを使用します。XDMCP がディスプレイ送信用ポートをネゴシエートすると、**established** コマンドが参照され、このバック接続を許可する必要があるかどうかが確認されます。

XWindows セッション中は、管理者は既知ポート 6000 | n 上で Xserver ディスプレイと通信します。次の端末設定を行うと、各ディスプレイが Xserver に個別に接続されます。

```
setenv DISPLAY Xserver:n
```

ここで、*n* は、ディスプレイの番号です。

XDMCP を使用すると、ディスプレイが IP アドレスを使用してネゴシエートされます。この IP アドレスは、セキュリティ アプライアンスが必要に応じて NAT を実行できるものです。XDCMP 検査は、PAT をサポートしていません。

例

次の例に示すように、XDMCP 検査エンジンをイネーブルにします。この例では、デフォルト ポート（177）上の XDMCP トラフィックに一致するクラス マップを作成します。このサービス ポリシーが、外部インターフェイスに適用されます。

```
hostname(config)# class-map xdmcp-port
hostname(config-cmap)# match port tcp eq 177
hostname(config-cmap)# exit
hostname(config)# policy-map xdmcp_policy
hostname(config-pmap)# class xdmcp-port
hostname(config-pmap-c)# inspect xdmcp
hostname(config-pmap-c)# exit
hostname(config)# service-policy xdmcp_policy interface outside
```

すべてのインターフェイスに対して XDMCP 検査をイネーブルにするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug xdmcp	XDMCP のデバッグ情報をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。

CHAPTER 16

interface-dhcp コマンド～ issuer-name コマンド

intercept-dhcp

DHCP 代行受信をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **intercept-dhcp enable** コマンドを使用します。DHCP 代行受信をディセーブルにするには、**intercept-dhcp disable** コマンドを使用します。

intercept-dhcp アトリビュートを実行コンフィギュレーションから削除するには、**no intercept-dhcp** コマンドを使用します。このコマンドを使用すると、ユーザは、デフォルト グループ ポリシーまたは他のグループ ポリシーから DHCP 代行受信コンフィギュレーションを継承できます。

DHCP 代行受信を使用すると、Microsoft XP クライアントは、セキュリティ アプライアンスに対してスプリット トンネリングを使用できます。セキュリティ アプライアンスは、Microsoft Windows XP クライアントの DHCP Inform メッセージに直接応答し、そのクライアントにトンネル IP アドレスのサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。XP 以前の Windows クライアントに対しては、DHCP 代行受信は、ドメイン名とサブネット マスクを提供します。この機能は、DHCP サーバを使用することに利点がない環境に有用です。

intercept-dhcp *netmask* {**enable | disable**}

no intercept-dhcp

シンタックスの説明

disable	DHCP 代行受信をディセーブルにします。
enable	DHCP 代行受信をイネーブルにします。
netmask	トンネル IP アドレスのサブネット マスクを提供します。

デフォルト

DHCP 代行受信はディセーブルになっています。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　スプリット トンネル オプションが 225 バイトを超えていると、Microsoft XP に異常が発生し、ドメイン名が破損します。この問題を回避するには、セキュリティ アプライアンスで送信ルートの数を 27 ～ 40 ルートに制限します。ルートの数は、ルートのクラスによって異なります。

例　次の例は、FirstGroup というグループ ポリシーに DHCP 代行受信を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# intercept-dhcp enable
```

interface

インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **interface** コマンドを使用します。インターフェイス コンフィギュレーション モードでは、インターフェイスのタイプとセキュリティ コンテキスト モードに応じて、ハードウェア設定値を設定し、名前、VLAN、および IP アドレスを割り当て、その他多数の設定値を設定することができます。

すべてのモデルで、物理インターフェイスに対応したパラメータを設定できます。ASA 5505 適応型セキュリティ アプライアンスといった組み込みスイッチがあるモデルを除いて、すべてのモデルは、VLAN に割り当てられる論理サブインターフェイスを作成できます。組み込みスイッチがあるモデルには、VLAN インターフェイスに割り当てることができるスイッチ ポート（このコマンドの物理インターフェイスと呼ばれる）が用意されています。この場合、VLAN のサブインターフェイスは作成しませんが、物理インターフェイスとは別に VLAN インターフェイスを作成します。VLAN インターフェイスには、1 つまたは複数の物理インターフェイスを割り当てることができます。サブインターフェイスまたは VLAN インターフェイスを削除するには、このコマンドの **no** 形式を使用します。物理インターフェイスは削除できません。

物理インターフェイスの場合（すべてのモデル）：

interface {*physical_interface* | *mapped_name*}

サブインターフェイスの場合（組み込みスイッチがあるモデルには使用できません）：

interface {*physical_interface*.*subinterface* | *mapped_name*}

no interface *physical_interface*.*subinterface*

VLAN インターフェイスの場合（組み込みスイッチのあるモデル）：

interface vlan *number*

no interface vlan *number*

シンタックスの説明

mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	物理インターフェイスのタイプ、スロット、およびポート番号で、*type*[*slot*/]*port* として指定します。タイプとスロット / ポートの間にスペースを入れるかどうかは任意です。 物理インターフェイスのタイプには、次のものがあります。 • **ethernet** • **gigabitethernet** PIX 500 シリーズ セキュリティ アプライアンスの場合は、タイプに続けてポート番号を入力します（たとえば、**ethernet0**）。 ASA 5500 シリーズ適応型セキュリティ アプライアンスの場合は、タイプに続けてスロット / ポートを入力します（たとえば、**gigabitethernet0/1**）。シャーシに組み込まれたインターフェイスはスロット 0 に割り当てられ、4GE SSM 上のインターフェイス（または組み込まれた 4GE SSM）はスロット 1 に割り当てられます。 ASA 5510 以降の適応型セキュリティ アプライアンスには、次のタイプもあります。 • **management** 管理インターフェイスは、管理トラフィック専用に設計されたファースト イーサネット インターフェイスで、**management0/0** として指定されます。ただし、必要に応じて、通過トラフィックに使用することもできます（**management-only** コマンドを参照）。透過ファイアウォール モードでは、通過トラフィック用の 2 つのインターフェイスのほかに、管理インターフェイスを使用できます。また、管理インターフェイスにサブインターフェイスを追加して、マルチ コンテキスト モードのセキュリティ コンテキストごとに管理することができます。 インターフェイス タイプ、スロット、およびポート番号を特定するには、使用中のモデルに付属しているハードウェア ドキュメントを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。サブインターフェイスの最大数は、セキュリティ アプライアンスのモデルによって異なります。サブインターフェイスは ASA 5505 適応型セキュリティ アプライアンスといった組み込みスイッチがあるモデルには使用できません。プラットフォームごとのサブインターフェイス（または VLAN）の最大数については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。1 つまたは複数の VLAN サブインターフェイスを持つインターフェイスは、自動的に 802.1Q トランクとして設定されます。
vlan *number*	組み込みスイッチがあるモデルの場合、VLAN ID 番号を 1 ～ 1001 の範囲で指定します。

デフォルト

デフォルトでは、セキュリティ アプライアンスは、すべての物理インターフェイスに対して **interface** コマンドを自動的に生成します。

マルチ コンテキスト モードでは、セキュリティ アプライアンスは、**allocate-interface** コマンドを使用してコンテキストに割り当てられたインターフェイスすべてに対して、**interface** コマンドを自動的に生成します。

物理インターフェイスは、デフォルトではすべてシャットダウンされます。コンフィギュレーションでは、コンテキスト内の割り当て済みインターフェイスはシャットダウンされません。VLAN インターフェイスはデフォルトではシャットダウンされません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、新しいサブインターフェイスの命名規則が適用できるように、また、インターフェイス コンフィギュレーション モードで引数が独立したコマンドとなるように変更されました。
7.2(1)	**interface vlan** コマンドが、ASA 5505 適応型セキュリティ アプライアンスでの組み込みスイッチをサポートするために追加されました。

使用上のガイドライン

物理インターフェイスは、デフォルトではすべてシャットダウンされます。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。VLAN インターフェイスはデフォルトではイネーブルです。

イネーブルになっているインターフェイスをトラフィックが通過できるようにするには、インターフェイス コンフィギュレーション モードのコマンドである **nameif** および **ip address**（ルーテッド モード用）を設定します。サブインターフェイスの場合は、**vlan** コマンドを設定します。スイッチ物理インターフェイスの場合、**switchport access vlan** コマンド（アクセス ポート用）または **switchport trunk allowed vlan** コマンド（トランク ポート用）を使用して、物理インターフェイスを VLAN インターフェイスに割り当てます。セキュリティ レベルは、デフォルトでは 0（最低レベル）になっています。インターフェイスのデフォルト レベルについて調べる場合や、インターフェイスの相互通信を可能にするためにデフォルトの 0 から変更する場合は、**security-level** コマンドを参照してください。

マルチ コンテキスト モードでは、物理パラメータ、サブインターフェイス、および VLAN 割り当ては、システム コンフィギュレーションのみに設定します。それ以外のパラメータはすべて、コンテキスト コンフィギュレーションのみに設定します。

組み込みスイッチのあるモデルの場合、物理パラメータとスイッチ パラメータ（VLAN 割り当てを含む）を物理インターフェイスのみに設定できます。その他すべてのパラメータを VLAN インターフェイスに設定できます。

透過ファイアウォール モードでは、ASA 5505 適応型セキュリティ アプライアンスの場合、Base ライセンスでアクティブな VLAN を 2 つまで、Security Plus ライセンスでアクティブな VLAN を 3 つまで設定できます。その内のいずれかはフェールオーバー用にする必要があります。ルーテッド

モードでは、Base ライセンスの場合はアクティブな VLAN を 3 つまで、Security Plus ライセンスの場合は 20 まで設定できます。アクティブな VLAN とは、**nameif** コマンドが設定されている VLAN です。Base ライセンスの場合、3 つ目の VLAN のみが別の VLAN へのトラフィックを開始するように設定できます。**no forward interface** コマンドを使用して 3 つめの VLAN を制限します。

ASA 以降の適応型セキュリティ アプライアンスには、Management 0/0 と呼ばれる専用の管理インターフェイスが含まれており、このインターフェイスによってセキュリティ アプライアンスへのトラフィックをサポートします。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の管理専用モードをディセーブルにして、他のインターフェイスと同様にトラフィックを通過させることもできます。

(注) 透過ファイアウォール モードでは、2 つのインターフェイスのみがトラフィックを通過させることができます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスでは、専用の管理インターフェイス（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。モードはこの場合設定不能であり、常に管理専用にする必要があります。

インターフェイス設定を変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するときは、**clear local-host** コマンドを使用して接続を消去してもかまいません。

例

次の例では、シングルモードで、物理インターフェイスのパラメータを設定します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

次の例では、シングルモードで、サブインターフェイスのパラメータを設定します。

```
hostname(config)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次の例では、マルチ コンテキスト モードで、システム コンフィギュレーションのインターフェイス パラメータを設定し、gigabitethernet 0/1.1 サブインターフェイスを contextA に割り当てます。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1.1
hostname(config-subif)# vlan 101
hostname(config-subif)# no shutdown
hostname(config-subif)# context contextA
hostname(config-ctx)# ...
hostname(config-ctx)# allocate-interface gigabitethernet0/1.1
```

次の例では、マルチ コンテキスト モードで、コンテキスト コンフィギュレーションのパラメータを設定します。

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# no shutdown
```

次の例では、3 つの LAN インターフェイスを設定しています。3 つ目のホーム インターフェイスはトラフィックをワーク インターフェイスに転送できません。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

次の例では、5 つの VLAN インターフェイス（**failover lan** コマンドを使用して別々に設定されたフェールオーバー インターフェイスを含む）を設定しています。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# nameif dmz
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.3.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 400
hostname(config-if)# nameif backup-isp
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# failover lan faillink vlan500
hostname(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby
10.4.1.2 255.255.255.0

hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 400
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 500
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear configure interface	インターフェイスのコンフィギュレーションをすべて消去します。
clear interface	**show interface** コマンドのカウンタを消去します。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。

interface（VPN ロードバランシング）

VPN ロードバランシング仮想クラスタで VPN ロードバランシングのデフォルト以外のパブリックまたはプライベート インターフェイスを指定するには、VPN ロードバランシング モードで **interface** コマンドを使用します。インターフェイスの指定を削除して、デフォルト インターフェイスに戻すには、このコマンドの **no** 形式を使用します。

interface {**lbprivate** | **lbpublic}** *interface-name*]

no interface {**lbprivate** | **lbpublic**}

シンタックスの説明

interface-name	VPN ロードバランシング クラスタのパブリックまたはプライベート インターフェイスとして設定するインターフェイスの名前。
lbprivate	このコマンドが VPN ロードバランシングのプライベート インターフェイスを設定するように指定します。
lbpublic	このコマンドが VPN ロードバランシングのパブリック インターフェイスを設定するように指定します。

デフォルト

interface コマンドを省略した場合、デフォルトでは、***lbprivate*** インターフェイスは***内部***に、***lbpublic*** インターフェイスは***外部***に設定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。

また、事前に **interface**、**ip address**、および **nameif** コマンドを使用して、このコマンドで指定するインターフェイスを設定し、名前を割り当てておく必要があります。

このコマンドの no 形式を使用すると、インターフェイスがデフォルトに戻ります。

例

次に、**vpn load-balancing** コマンド シーケンスの例を示します。このコマンド シーケンスには、クラスタのパブリック インターフェイスを「test」として指定する **interface** コマンドと、クラスタのプライベート インターフェイスをデフォルト（内部）に戻す interface コマンドが含まれています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# no interface lbprivate
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

interface-policy

監視中にインターフェイスの障害が検出された場合のフェールオーバーのポリシーを指定するには、フェールオーバー グループ コンフィギュレーション モードで **interface-policy** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

interface-policy *num*[**%**]

no interface-policy *num*[**%**]

シンタックスの説明

num	1 ～ 100 の数を指定するか（パーセンテージとして使用する場合）、または 1 からインターフェイスの最大数までの数を指定します。
%	（オプション）*num* の数が監視対象インターフェイスのパーセンテージであることを指定します。

デフォルト

装置に対して **failover interface-policy** コマンドが設定されている場合は、その値が **interface-policy** フェールオーバー グループ コマンドのデフォルトと見なされます。設定されていなければ、*num* は 1 になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にスペースを含めないでください。

障害が発生したインターフェイスの数が設定済みポリシーの基準を満たした場合、他のセキュリティ アプライアンスが正常に機能しているときは、セキュリティ アプライアンスは自身を障害としてマークし、場合によってはフェールオーバーが発生します（アクティブなセキュリティ アプライアンスに障害が発生した場合）。ポリシーでカウントされるのは、**monitor-interface** コマンドで監視対象として指定したインターフェイスのみです。

例

次の例（抜粋）は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# interface-policy 25%
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバーグループを定義します。
failover interface-policy	インターフェイス モニタリング ポリシーを設定します。
monitor-interface	フェールオーバーのために監視対象にするインターフェイスを指定します。

interval maximum

DDNS アップデート方式によるアップデート試行間の最大間隔を設定するには、DDNS アップデート方式モードで **interval** コマンドを使用します。実行コンフィギュレーションから DDNS アップデート方式の間隔を削除するには、このコマンドの **no** 形式を使用します。

interval maximum *days hours minutes seconds*

no interval maximum *days hours minutes seconds*

シンタックスの説明

days	アップデート試行間の日数を 0 ～ 364 の範囲に指定します。
hours	アップデート試行間の時間数を 0 ～ 23 の範囲に指定します。
minutes	アップデート試行間の分数を 0 ～ 59 の範囲に指定します。
seconds	アップデート試行間の秒数を 0 ～ 59 の範囲に指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
DDNS アップデート方式コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

日数、時間数、分数、秒数がまとめて加算されて合計間隔が示されます。

例

次の例では 3 分 15 秒ごとにアップデートされる ddns-2 という方式が設定されます。

```
hostname(config)# ddns update method ddns-2
hostname(DDNS-update-method)# interval maximum 0 0 3 15
```

関連コマンド

コマンド	説明
ddns（DDNS アップデート方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	ダイナミック DNS（DDNS）のアップデート方式を、セキュリティ アプライアンス インターフェイスまたは DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによるダイナミック DNS アップデートの実行をイネーブルにします。

ip address

インターフェイスの IP アドレス（ルーテッド モード）または管理アドレスの IP アドレス（透過モード）を設定するには、**ip address** コマンドを使用します。ルーテッド モードの場合は、インターフェイス コンフィギュレーション モードでこのコマンドを入力します。透過モードの場合は、グローバル コンフィギュレーション モードでこのコマンドを入力します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。このコマンドは、また、フェールオーバー用のスタンバイ アドレスを設定します。

ip address *ip_address* [*mask*] [***standby*** *ip_address*]

no ip address [*ip_address*]

シンタックスの説明

ip_address	インターフェイスの IP アドレス（ルーテッド モード）、または管理 IP アドレス（透過モード）。
mask	（オプション）IP アドレスのサブネット マスク。マスクを設定しない場合、セキュリティ アプライアンスは IP アドレス クラスのデフォルト マスクを使用します。
standby *ip_address*	（オプション）フェールオーバー用のスタンバイ装置の IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	ルーテッド モードに関して、このコマンドが、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

シングル コンテキスト ルーテッド ファイアウォール モードでは、各インターフェイス アドレスは一意のサブネット上にある必要があります。マルチ コンテキスト モードでは、このインターフェイスが共有インターフェイス上にある場合、各 IP アドレスは一意で、同じサブネット上にある必要があります。インターフェイスが一意の場合、この IP アドレスは、必要に応じて他のコンテキストで使用することができます。

透過ファイアウォールは、IP ルーティングには参加しません。セキュリティ アプライアンスに必要な唯一の IP コンフィギュレーションは、管理 IP アドレスを設定することです。このアドレスが必要な理由は、セキュリティ アプライアンスがセキュリティ アプライアンス上で発信するトラフィック（システム メッセージや AAA サーバとの通信など）の送信元アドレスとして、このアドレスを使用するためです。また、このアドレスは、リモート管理アクセスに使用することもできます。このアドレスは、アップストリーム ルータおよびダウンストリーム ルータと同じサブネット上にある必要があります。マルチ コンテキスト モードの場合は、各コンテキスト内で管理 IP アドレスを設定します。

スタンバイ IP アドレスは、メイン IP アドレスと同じサブネット上にある必要があります。

例

次の例では、2 つのインターフェイスの IP アドレスとスタンバイ アドレスを設定します。

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/3
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
hostname(config-if)# no shutdown
```

次の例では、透過ファイアウォールの管理アドレスとスタンバイ アドレスを設定します。

```
hostname(config)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address dhcp	DHCP サーバから IP アドレスを取得するようにインターフェイスを設定します。
show ip address	インターフェイスに割り当てられた IP アドレスを表示します。

ip address dhcp

DHCP を使用してインターフェイスの IP アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ip address dhcp** コマンドを使用します。このインターフェイスの DHCP クライアントをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip address dhcp [*setroute*]

no ip address dhcp

シンタックスの説明

setroute	（オプション）DHCP サーバから提供されるデフォルト ルートをセキュリティ アプライアンスが使用できるようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。また、このコマンドが、外部インターフェイスだけでなく、すべてのインターフェイス上でイネーブルにできるようになりました。

使用上のガイドライン

DHCP リースをリセットして新しいリースを要求するには、このコマンドを再入力します。

no shutdown コマンドを使用してインターフェイスをイネーブルにしないで **ip address dhcp** コマンドを入力すると、一部の DHCP 要求が送信されない場合があります。

例

次の例では、gigabitethernet0/1 インターフェイス上で DHCP をイネーブルにします。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# no shutdown
hostname(config-if)# ip address dhcp
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address	インターフェイスの IP アドレスを設定します。または、透過ファイアウォールの管理 IP アドレスを設定します。
show ip address dhcp	DHCP サーバから取得した IP アドレスを表示します。

ip address pppoe

PPPoE をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ip address pppoe** コンドを使用します。PPPoE をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip address [*ip_address* [*mask*]] ***pppoe*** [***setroute***]

no ip address [*ip_address* [*mask*]] ***pppoe***

シンタックスの説明

ip_address	PPPoE サーバからアドレスを受信せずに、IP アドレスを手作業で設定します。
mask	IP アドレスのサブネット マスクを指定します。マスクを設定しない場合、セキュリティ アプライアンスは IP アドレス クラスのデフォルト マスクを使用します。
setroute	セキュリティ アプライアンスでは、PPPoE サーバから提供されるデフォルト ルートが使用されます。PPPoE サーバがデフォルト ルートを送信しない場合、セキュリティ アプライアンスはゲートウェイとしてアクセス コンセントレータのアドレスによりデフォルト ルートを作成します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

PPPoE では広く普及している規格である Ethernet と PPP を組み合せて、クライアント システムに認証方式で IP アドレスを割り当てます。ISP が PPPoE を導入している理由は、PPPoE が既存のリモート アクセス インフラストラクチャを使用する高速ブロードバンド アクセスをサポートしており、顧客が簡単に使用できるためです。

PPPoE を使用して IP アドレスを設定する前に、**vpdn** コマンドを使用してユーザ名、パスワード、認証プロトコルを設定します。複数のインターフェイスで、たとえば、ISP へのバックアップ リンクとして、このコマンドをイネーブルにする場合、必要に応じて **pppoe client vpdn group** コマンドを使用して、異なるグループに各インターフェイスを割り当てることができます。

Maximum Transmission Unit（MTU; 最大伝送ユニット）サイズは自動的に 1492 バイトに設定されます。この値は、イーサネット フレーム内で PPPoE 伝送を許可する正しい値です。

PPPoE セッションをリセットし再起動するには、このコマンドを再度入力します。

このコマンドは **ip address** コマンドまたは **ip address dhcp** コマンドと同時に設定できません。

例

次の例では、Gigabitethernet 0/1 インターフェイス上で PPPoE をイネーブルにします。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address pppoe
hostname(config-if)# no shutdown
```

次の例では、PPPoE インターフェイスに対して IP アドレスを手動で設定します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address	インターフェイスの IP アドレスを設定します。
pppoe client vpdn group	このインターフェイスを特定の VPDN グループに割り当てます。
show ip address pppoe	PPPoE サーバから取得した IP アドレスを表示します。
vpdn group	

ip-address-privacy

IP アドレスのプライバシーをイネーブルにするには、パラメータ コンフィギュレーション モードで **ip-address-privacy** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip-address-privacy

no ip-address-privacy

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、SIP 検査ポリシー マップにおいて、SIP 上での IP アドレスのプライバシーをイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# ip-address-privacy
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

ip audit attack

攻撃シグニチャに一致するパケットに対するデフォルト アクションを設定するには、グローバル コンフィギュレーション モードで **ip audit attack** コマンドを使用します。デフォルト アクションに戻す（接続をリセットする）には、このコマンドの **no** 形式を使用します。アクションは複数指定することも、一切指定しないこともできます。

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit attack

シンタックスの説明

action	（オプション）一連のデフォルト アクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。***action*** キーワードを入力しない場合、セキュリティ アプライアンスは入力したものと見なして ***action*** キーワードをコンフィギュレーションに記述します。
alarm	（デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
drop	（オプション）パケットをドロップします。
reset	（オプション）パケットをドロップし、接続を閉じます。

デフォルト

デフォルト アクションは、アラームの送信です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドにアクションを指定しない場合は、このコマンドで設定するアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次の例では、攻撃シグニチャに一致するパケットに対するデフォルト アクションを、alarm および reset に設定します。内部インターフェイスの監査ポリシーは、このデフォルトを無効にして alarm のみに設定します。一方、外部インターフェイスのポリシーは、**ip audit attack** コマンドで設定されたデフォルト設定を使用します。

```
hostname(config)# ip audit attack action alarm reset
hostname(config)# ip audit name insidepolicy attack action alarm
hostname(config)# ip audit name outsidepolicy attack
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

ip audit info

情報シグニチャに一致するパケットに対するデフォルト アクションを設定するには、グローバル コンフィギュレーション モードで **ip audit info** コマンドを使用します。デフォルト アクションに戻す（アラームを生成する）には、このコマンドの **no** 形式を使用します。アクションは複数指定することも、一切指定しないこともできます。

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit info

シンタックスの説明

action	（オプション）一連のデフォルト アクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。***action*** キーワードを入力しない場合、セキュリティ アプライアンスは入力したものと見なして ***action*** キーワードをコンフィギュレーションに記述します。
alarm	（デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
drop	（オプション）パケットをドロップします。
reset	（オプション）パケットをドロップし、接続を閉じます。

デフォルト

デフォルト アクションは、アラームの生成です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドにアクションを指定しない場合は、このコマンドで設定するアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次の例では、情報シグニチャに一致するパケットに対するデフォルト アクションを、alarm および reset に設定します。内部インターフェイスの監査ポリシーは、このデフォルトを無効にして alarm および drop に設定します。一方、外部インターフェイスのポリシーは、**ip audit info** コマンドで設定されたデフォルト設定を使用します。

```
hostname(config)# ip audit info action alarm reset
hostname(config)# ip audit name insidepolicy info action alarm drop
hostname(config)# ip audit name outsidepolicy info
hostname(config)# ip audit interface inside insidepolicy
hostname(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit info	**ip audit info** コマンドのコンフィギュレーションを表示します。

ip audit interface

インターフェイスに監査ポリシーを割り当てるには、グローバル コンフィギュレーション モードで **ip audit interface** コマンドを使用します。ポリシーをインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

ip audit interface *interface_name policy_name*

no ip audit interface *interface_name policy_name*

シンタックスの説明

interface_name	インターフェイス名を指定します。
policy_name	**ip audit name** コマンドで追加したポリシーの名前。各インターフェイスに ***info*** ポリシーと ***attack*** ポリシーを割り当てることができます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、監査ポリシーを内部インターフェイスと外部インターフェイスに適用します。

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit interface	**ip audit interface** コマンドのコンフィギュレーションを表示します。

ip audit name

パケットが定義済みの攻撃シグニチャまたは情報シグニチャに一致する場合に実行するアクションを識別する、名前付き監査ポリシーを作成するには、グローバル コンフィギュレーション モードで **ip audit name** コマンドを使用します。シグニチャは、既知の攻撃パターンに一致するアクティビティです。たとえば、DoS 攻撃（サービス拒絶攻撃）に一致するシグニチャがあります。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit name *name* {***info*** | ***attack***} [**action** [**alarm**] [**drop**] [**reset**]]

no ip audit name *name* {***info*** | ***attack***} [**action** [**alarm**] [**drop**] [**reset**]]

シンタックスの説明

action	（オプション）一連のアクションを定義することを指定します。このキーワードの後に何もアクションを指定しない場合、セキュリティ アプライアンスはアクションを実行しません。***action*** キーワードを入力しない場合、セキュリティ アプライアンスは、**ip audit attack** コマンドと **ip audit info** コマンドで設定されたデフォルト アクションを使用します。
alarm	（オプション）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。
attack	攻撃シグニチャの監査ポリシーを作成します。パケットは、DoS 攻撃や不正な FTP コマンドなど、ネットワークに対する攻撃の一部である可能性があります。
drop	（オプション）パケットをドロップします。
info	情報シグニチャの監査ポリシーを作成します。パケットは、現在のところ、ネットワークを攻撃することはありませんが、ポート スィープなど、情報収集アクティビティの一部である可能性があります。
name	ポリシーの名前を設定します。
reset	（オプション）パケットをドロップし、接続を閉じます。

デフォルト

ip audit attack コマンドと **ip audit info** コマンドを使用してデフォルト アクションを変更していなければ、攻撃シグニチャと情報シグニチャに対するデフォルト アクションは、アラームの生成になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ポリシーを適用するには、**ip audit interface** コマンドを使用してインターフェイスにポリシーを割り当てます。各インターフェイスに ***info*** ポリシーと ***attack*** ポリシーを割り当てることができます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

トラフィックがシグニチャに一致する場合、そのトラフィックに対してアクションを実行するときは、**shun** コマンドを使用して、攻撃ホストからの新しい接続を防止し、既存の接続からのパケットを拒否します。

例

次の例では、攻撃シグニチャと情報シグニチャに対してアラームを生成するように、内部インターフェイスの監査ポリシーを設定します。一方、外部インターフェイスのポリシーでは、攻撃の接続をリセットします。

```
hostname(config)# ip audit name insidepolicy1 attack action alarm
hostname(config)# ip audit name insidepolicy2 info action alarm
hostname(config)# ip audit name outsidepolicy1 attack action reset
hostname(config)# ip audit name outsidepolicy2 info action alarm
hostname(config)# ip audit interface inside insidepolicy1
hostname(config)# ip audit interface inside insidepolicy2
hostname(config)# ip audit interface outside outsidepolicy1
hostname(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit signature	シグニチャをディセーブルにします。
shun	特定の送信元アドレスと宛先アドレスが指定されたパケットをブロックします。

ip audit signature

監査ポリシーのシグニチャをディセーブルにするには、グローバル コンフィギュレーション モードで **ip audit signature** コマンドを使用します。シグニチャを再度イネーブルにするには、このコマンドの **no** 形式を使用します。正当なトラフィックがシグニチャに継続的に一致する場合、シグニチャをディセーブルにするリスクがあっても多数のアラームを回避することを考えているときは、ディセーブルにしてもかまいません。

ip audit signature *signature_number* ***disable***

no ip audit signature *signature_number*

シンタックスの説明

signature_number	ディセーブルにするシグニチャの番号を指定します。サポートされているシグニチャのリストについては、表 16-1 を参照してください。
disable	シグニチャをディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

表 16-1 に、サポートされているシグニチャとシステム メッセージ番号を示します。

表 16-1　シグニチャ ID とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP オプション：不良オプション リスト	情報	受信した IP データグラムの IP データグラム ヘッダーにある IP オプションのリストが不完全な場合や変造されている場合にトリガーされます。IP オプションのリストには、種々のネットワーク管理タスクやデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP オプション：記録パケット ルート	情報	受信した IP データグラムの IP オプション リストにオプション 7（記録パケット ルート）が含まれている場合にトリガーされます。
1002	400002	IP オプション：タイムスタンプ	情報	受信した IP データグラムの IP オプション リストにオプション 4（タイムスタンプ）が含まれている場合にトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1003	400003	IP オプション：セキュリティ	情報	受信した IP データグラムの IP オプション リストにオプション 2（セキュリティ オプション）が含まれている場合にトリガーされます。
1004	400004	IP オプション：発信元ルートの損失	情報	受信した IP データグラムの IP オプション リストにオプション 3（発信元ルートの損失）が含まれている場合にトリガーされます。
1005	400005	IP オプション：SATNET ID	情報	受信した IP データグラムの IP オプション リストにオプション 8（SATNET ストリーム ID）が含まれている場合にトリガーされます。
1006	400006	IP オプション：完全発信元ルート	情報	受信した IP データグラムの IP オプション リストにオプション 2（完全発信ルーティング）が含まれている場合にトリガーされます。
1100	400007	IP フラグメント攻撃	攻撃	受信した IP データグラムのオフセット フィールドに含まれているオフセット値が 0 より大きく 5 より小さい場合にトリガーされます。
1102	400008	IP 不可能パケット	攻撃	到着した IP パケットの送信元アドレスと宛先アドレスが一致している場合にトリガーされます。このシグニチャは、いわゆる Land 攻撃を捕捉します。
1103	400009	IP フラグメント重複（Teardrop）	攻撃	同じ IP データグラムに含まれている 2 つのフラグメントが、データグラム内で両フラグメントが位置決めを共有していることを示すオフセットを持っている場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味する場合があります。一部のオペレーティング システムは、このように重複するフラグメントを正しく処理しないため、重複フラグメントを受信したときに、例外を投げたり、不適切に動作したりする場合があります。このようにして、Teardrop 攻撃から DoS が引き起こされます。
2000	400010	ICMP エコー応答	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定されている場合にトリガーされます。
2001	400011	ICMP ホスト到達不能	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定されている場合にトリガーされます。
2002	400012	ICMP Source Quench	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（Source Quench）に設定されている場合にトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2003	400013	ICMP リダイレクト	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定されている場合にトリガーされます。
2004	400014	ICMP エコー要求	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定されている場合にトリガーされます。
2005	400015	データグラムの ICMP タイム超過	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムのタイム超過）に設定されている場合にトリガーされます。
2006	400016	データグラム上の ICMP パラメータ問題	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 12（データグラム上のパラメータ問題）に設定されている場合にトリガーされます。
2007	400017	ICMP タイムスタンプ要求	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 13（タイムスタンプ要求）に設定されている場合にトリガーされます。
2008	400018	ICMP タイムスタンプ応答	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 14（タイムスタンプ応答）に設定されている場合にトリガーされます。
2009	400019	ICMP 情報要求	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 15（情報要求）に設定されている場合にトリガーされます。
2010	400020	ICMP 情報応答	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 16（ICMP 情報応答）に設定されている場合にトリガーされます。
2011	400021	ICMP アドレス マスク要求	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 17（アドレス マスク要求）に設定されている場合にトリガーされます。
2012	400022	ICMP アドレス マスク応答	情報	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 18（アドレス マスク応答）に設定されている場合にトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2150	400023	フラグメント化された ICMP トラフィック	攻撃	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定されているほか、それ以外にも 1（ICMP）に設定されたフラグメント フラグがあるか、またはオフセット フィールドにオフセットが含まれている場合にトリガーされます。
2151	400024	大きい ICMP トラフィック	攻撃	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP の長さが 1024 より大きい場合にトリガーされます。
2154	400025	Ping of Death 攻撃	攻撃	受信した IP データグラムの IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、Last Fragment ビットが設定され、（IP オフセット * 8）+（IP データ長）> 65,535 の式が成り立つ場合にトリガーされます。この式は、IP オフセット（元のパケットにおけるこのフラグメントの開始位置で、8 バイト単位）と残りのパケットの合計が IP パケットの最大サイズを超えていることを意味します。
3040	400026	TCP NULL フラグ	攻撃	SYN、FIN、ACK、または RST フラグがいずれも設定されていない単一の TCP パケットが、特定のホストに送信された場合にトリガーされます。
3041	400027	TCP SYN+FIN フラグ	攻撃	SYN および FIN フラグが設定されている単一の TCP パケットが、特定のホストに送信された場合にトリガーされます。
3042	400028	TCP FIN のみのフラグ	攻撃	単一の身元不明 TCP FIN パケットが、特定のホスト上の特権ポート（ポート番号は 1024 より小さい）に送信された場合にトリガーされます。
3153	400029	FTP に誤ったアドレスを指定	情報	ポート コマンドが、要求元ホストとは異なるアドレスを使用して発行された場合にトリガーされます。
3154	400030	FTP に誤ったポートを指定	情報	ポート コマンドが、1024 未満または 65535 を超えるデータ ポートを指定して発行された場合にトリガーされます。
4050	400031	UDP Bomb 攻撃	攻撃	指定された UDP の長さが、指定された IP の長さより小さい場合にトリガーされます。この変造パケット タイプは、DoS 攻撃に関連付けられています。
4051	400032	UDP Snork 攻撃	攻撃	検出された UDP パケットの送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 の場合にトリガーされます。
4052	400033	UDP Chargen DoS 攻撃	攻撃	このシグニチャがトリガーされるのは、検出された UDP パケットの送信元ポートが 7 で、宛先ポートが 19 の場合です。
6050	400034	DNS HINFO 要求	情報	DNS サーバの HINFO レコードにアクセスする攻撃が発生した場合にトリガーされます。
6051	400035	DNS ゾーン転送	情報	通常の DNS ゾーン転送（送信元ポートは 53）が発生した場合にトリガーされます。

表 16-1　シグニチャ ID とシステム メッセージ番号（続き）

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6052	400036	ハイ ポートからの DNS ゾーン転送	情報	不正な DNS ゾーン転送（送信元ポートは 53 以外）が発生した場合にトリガーされます。
6053	400037	すべての記録の DNS 要求	攻撃	すべての記録の DNS 要求を受信した場合にトリガーされます。
6100	400038	RPC ポート登録	情報	ターゲット ホストに対して新しい RPC サービスを登録する攻撃が発生した場合にトリガーされます。
6101	400039	RPC ポート非登録	情報	ターゲット ホストに対して既存の RPC サービスを登録解除する攻撃が発生した場合にトリガーされます。
6102	400040	RPC Dump	情報	ターゲット ホストに RPC ダンプ要求が発行された場合にトリガーされます。
6103	400041	プロキシの RPC 要求	攻撃	ターゲット ホストのポートマッパーにプロキシの RPC 要求が送信された場合にトリガーされます。
6150	400042	ypserv（YP サーバ デーモン）Portmap 要求	情報	YP サーバ デーモン（ypserv）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6151	400043	ypbind（YP バインド デーモン）Portmap 要求	情報	YP バインド デーモン（ypbind）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6152	400044	yppasswdd（YP パスワード デーモン）Portmap 要求	情報	YP パスワード デーモン（yppasswdd）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6153	400045	ypupdated（YP アップデート デーモン）Portmap 要求	攻撃	YP アップデート デーモン（ypupdated）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6154	400046	ypxfrd（YP 転送デーモン）Portmap 要求	攻撃	YP 転送デーモン（ypxfrd）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6155	400047	mountd（マウント デーモン）Portmap 要求	情報	マウント デーモン（mountd）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6175	400048	rexd（リモート実行デーモン）Portmap 要求	情報	リモート実行デーモン（rexd）ポートのポートマッパーに要求が送信された場合にトリガーされます。
6180	400049	rexd（リモート実行デーモン）攻撃	情報	rexd プログラムが呼び出された場合にトリガーされます。リモート実行デーモンは、リモート プログラムの実行を担当するサーバです。これは、システム リソースに不正アクセスする攻撃の兆候である可能性があります。
6190	400050	statd バッファ オーバーフロー	攻撃	大規模な statd 要求が送信された場合にトリガーされます。これは、バッファをオーバーフローさせ、システム リソースにアクセスする攻撃である可能性があります。

例

次の例では、シグニチャ 6100 をディセーブルにします。

```
hostname(config)# ip audit signature 6100 disable
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit signature	**ip audit signature** コマンドのコンフィギュレーションを表示します。

ip-comp

LZS IP 圧縮をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ip-comp enable** コマンドを使用します。IP 圧縮をディセーブルにするには、**ip-comp disable** コマンドを使用します。

ip-comp アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループ ポリシーから継承できます。

ip-comp {**enable | disable**}

no ip-comp

シンタックスの説明

disable	IP 圧縮をディセーブルにします。
enable	IP 圧縮をイネーブルにします。

デフォルト

IP 圧縮はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

データ圧縮をイネーブルにすると、モデムで接続しているリモート ダイヤルイン ユーザのデータ伝送速度が向上する場合があります。

注意　データ圧縮を行うと、各ユーザ セッションのメモリ要件と CPU 使用率が増加するため、セキュリティ アプライアンスのスループット全体が低下します。このため、データ圧縮は、モデムで接続しているリモート ユーザに対してのみイネーブルにすることをお勧めします。モデム ユーザに固有のグループ ポリシーを設計し、このユーザに対してのみ圧縮をイネーブルにします。

例

次の例は、「FirstGroup」というグループ ポリシーに対して IP 圧縮をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-comp enable
```

ip local pool

VPN リモートアクセス トンネルに使用する IP アドレス プールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用します。アドレス プールを削除するには、このコマンドの **no** 形式を使用します。

ip local pool *poolname first-address—last-address* [***mask*** *mask*]

no ip local pool *poolname*

シンタックスの説明

first-address	IP アドレスの範囲の開始アドレスを指定します。
last-address	IP アドレスの範囲の最終アドレスを指定します。
mask *mask*	（オプション）アドレス プールのサブネット マスクを指定します。
poolname	IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

VPN クライアントに割り当てられた IP アドレスが非標準のネットワークに属する場合は、マスク値を指定する必要があります。デフォルト マスクを使用すると、データが誤ってルーティングされる可能性があります。一般的な例として、デフォルトでクラス A ネットワークになっている IP ローカル プールに 10.10.10.0/255.255.255.0 のアドレスが含まれている場合を考えます。この場合、VPN クライアントが複数のインターフェイス上で 10 ネットワーク内の複数のサブネットにアクセスしようとすると、ルーティングの問題が発生する可能性があります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェイス 2 経由で使用可能で、10.10.10.0 ネットワークが VPN トンネル上およびインターフェイス 1 経由で使用可能な場合、VPN クライアントでは、プリンタ宛のデータのルーティング先について混乱が生じます。10.10.10.0 と 10.10.100.0 のサブネットは両方とも 10.0.0.0 クラス A ネットワークに該当するため、プリンタのデータは VPN トンネル上で送信される場合があります。

例

次の例では、firstpool という IP アドレス プールを設定します。開始アドレスは 10.20.30.40 で、終了アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
hostname(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
show running-config ip local pool	ip プール コンフィギュレーションを表示します。特定の IP アドレス プールを指定するには、その名前をコマンドに含めます。

ip-phone-bypass

IP Phone Bypass をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ip-phone-bypass enable** コマンドを使用します。IP Phone Bypass をディセーブルにするには、**ip-phone-bypass disable** コマンドを使用します。IP phone Bypass アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、IP Phone Bypass の値を別のグループ ポリシーから継承できます。

IP Phone Bypass を使用すると、ハードウェア クライアントの背後にある IP 電話を接続するときに、ユーザ認証プロセスが不要になります。イネーブルの場合、Secure Unit Authentication は有効なままになります。

ip-phone-bypass {**enable** | **disable**}

no ip-phone-bypass

シンタックスの説明

disable	IP Phone Bypass をディセーブルにします。
enable	IP Phone Bypass をイネーブルにします。

デフォルト

IP Phone Bypass はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IP Phone Bypass を設定する必要があるのは、ユーザ認証をイネーブルにした場合のみです。

例

次の例は、FirstGroup というグループ ポリシーに対して IP Phone Bypass をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ip-phone-bypass enable
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

ips

ASA 5500 シリーズ適応型セキュリティ アプライアンスは、AIP SSM をサポートしています。AIP SSM は拡張 IPS ソフトウェアを実行して、インライン モードまたはプロミスキャス モードで詳細なセキュリティ検査を実行します。セキュリティ アプライアンスが AIP SSM にパケットを転送するのは、パケットが出力インターフェイスを通過する直前（または VPN 暗号化が設定されている場合は暗号化が行われる前）と、他のファイアウォール ポリシーが適用された後です。たとえば、アクセス リストによってブロックされたパケットは、AIP SSM に転送されません。

セキュリティ アプライアンスからのトラフィックを AIP SSM に割り当てるには、クラス コンフィギュレーション モードで **ips** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

ips {***inline*** | ***promiscuous***} {***fail-close*** | ***fail-open***}

no ips {***inline*** | ***promiscuous***} {***fail-close*** | ***fail-open***}

シンタックスの説明

fail-close	AIP SSM に障害が発生した場合にトラフィックをブロックします。
fail-open	AIP SSM に障害が発生した場合にトラフィックを許可します。
inline	AIP SSM にパケットを転送します。パケットは、IPS 動作の結果としてドロップされる場合があります。
promiscuous	AIP SSM に対するパケットを複製します。元のパケットを AIP SSM でドロップすることはできません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ips コマンドを設定するには、最初に、**class-map** コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

AIP SSM にトラフィックを転送するようにセキュリティ アプライアンスを設定したら、AIP SSM の検査と保護ポリシーを設定します。このポリシーは、トラフィックの検査方法と、進入が検知されたときの処理を決定します。セキュリティ アプライアンスから AIP SSM へのセッションを確立するか（**session** コマンド）、または管理インターフェイス上で SSH や Telnet を使用して AIP SSM に直接接続することができます。別の方法として、ASDM を使用することもできます。AIP SSM の設定の詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface*』を参照してください。

例

次の例では、プロミスキャス モードですべての IP トラフィックを AIP SSM に転送し、何らかの理由で AIP SSM カードに障害が発生した場合には、すべての IP トラフィックをブロックします。

```
hostname(config)# access-list IPS permit ip any any
hostname(config)# class-map my-ips-class
hostname(config-cmap)# match access-list IPS
hostname(config-cmap)# policy-map my-ips-policy
hostname(config-pmap)# class my-ips-class
hostname(config-pmap-c)# ips promiscuous fail-close
hostname(config-pmap-c)# service-policy my-ips-policy global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
class-map	ポリシー マップで使用するトラフィックを指定します。
clear configure policy-map	すべての**ポリシー マップ** コンフィギュレーションを削除します。ただし、ポリシー マップが **service-policy** コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	現在のすべての**ポリシー マップ** コンフィギュレーションを表示します。

ipsec-udp

IPSec over UDP をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp enable** コマンドを使用します。IPSec over UDP をディセーブルにするには、**ipsec-udp disable** コマンドを使用します。IPSec over UDP アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、IPSec over UDP の値を別のグループ ポリシーから継承できます。

IPSec over UDP（IPSec through NAT と呼ばれる場合もある）を使用すると、Cisco VPN Client またはハードウェア クライアントから、NAT を実行しているセキュリティ アプライアンスに UDP を介して接続できます。

ipsec-udp {enable | disable}

no ipsec-udp

シンタックスの説明

disable	IPSec over UDP をディセーブルにします。
enable	IPSec over UDP をイネーブルにします。

デフォルト

IPSec over UDP はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPSec over UDP を使用するには、**ipsec-udp-port** コマンドを設定する必要もあります。

また、Cisco VPN Client でも、IPSec over UDP を使用するように設定する必要があります（デフォルトでは、使用するように設定されています）。VPN 3002 では、IPSec over UDP を使用するように設定する必要はありません。

IPSec over UDP は独自の方式で、リモートアクセス接続のみに適用され、モード コンフィギュレーションを必要とします。これは、SA のネゴシエート中にセキュリティ アプライアンスがクライアントとコンフィギュレーション パラメータを交換することを意味します。

IPSec over UDP を使用すると、システム パフォーマンスがわずかに低下する場合があります。

例

次の例は、FirstGroup というグループ ポリシーに IPSec over UDP を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp enable
```

関連コマンド

コマンド	説明
ipsec-udp-port	セキュリティ アプライアンスが UDP トラフィックをリッスンするポートを指定します。

ipsec-udp-port

IPSec over UDP の UDP ポート番号を設定するには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドを使用します。UDP ポートをディセーブルにするには、このコマンドの **no** 形式を使用します。このオプションを使用すると、IPSec over UDP ポートの値を別のグループ ポリシーから継承できます。

IPSec ネゴシエーションでは、セキュリティ アプライアンスは、設定済みのポート上でリッスンし、そのポートに対する UDP トラフィックを転送します。これは、他のフィルタ規則によって UDP トラフィックがドロップされる場合でも同様です。

ipsec-udp-port *port*

no ipsec-udp-port

シンタックスの説明

port	4001 ～ 49151 の整数を使用して、UDP ポート番号を指定します。

デフォルト

デフォルト ポートは 10000 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この機能をイネーブルにした複数のグループ ポリシーを設定できます。グループ ポリシーごとに、別々のポート番号を使用できます。

例

次の例は、FirstGroup というグループ ポリシーの IPSec UDP ポートをポート 4025 に設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# ipsec-udp-port 4025
```

関連コマンド

コマンド	説明
ipsec-udp	Cisco VPN Client またはハードウェア クライアントから、NAT を実行しているセキュリティ アプライアンスに UDP を介して接続できるようにします。

ip verify reverse-path

Unicast RPF をイネーブルにするには、グローバル コンフィギュレーション モードで **ip verify reverse-path** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。Unicast RPF は、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用して実際の送信元を隠す）から保護します。この機能により、すべてのパケットの送信元 IP アドレスが、ルーティング テーブルに従って、正しい送信元インターフェイスに一致することが保証されます。

ip verify reverse-path interface *interface_name*

no ip verify reverse-path interface *interface_name*

シンタックスの説明

interface_name	Unicast RPF をイネーブルにするインターフェイス。

デフォルト

この機能は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

通常、セキュリティ アプライアンスは、パケットの転送先を決定するときは宛先アドレスだけを参照します。Unicast RPF は、送信元アドレスも参照するようにセキュリティ アプライアンスに指示します。この機能が Reverse Path Forwarding（RPF）と呼ばれるのはこのためです。セキュリティ アプライアンスを通過できるようにするすべてのトラフィックについて、送信元アドレスに戻るルートをセキュリティ アプライアンス ルーティング テーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックについては、セキュリティ アプライアンスはデフォルト ルートを使用して Unicast RPF 保護を機能させることができます。外部インターフェイスからトラフィックが着信した場合、送信元アドレスがルーティング テーブルにおいて未知のときは、セキュリティ アプライアンスはデフォルト ルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

ルーティング テーブルにおいて既知のアドレスから外部インターフェイスにトラフィックが着信した場合、そのアドレスが内部インターフェイスに関連付けられているときは、セキュリティ アプライアンスはパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが着信した場合、一致したルート（デフォルト ルート）は外部インターフェイスを示すため、セキュリティ アプライアンスはパケットをドロップします。

Unicast RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

例

次の例では、外部インターフェイス上で Unicast RPF をイネーブルにします。

```
hostname(config)# ip verify reverse-path interface outside
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを消去します。
clear ip verify statistics	Unicast RPF の統計情報を消去します。
show ip verify statistics	Unicast RPF の統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

ipv6 access-list

IPv6 アクセス リストを設定するには、グローバル コンフィギュレーション モードで **ipv6 access-list** コマンドを使用します。ACE を削除するには、このコマンドの **no** 形式を使用します。アクセス リストは、セキュリティ アプライアンスが通過させる、またはブロックするトラフィックを定義します。

ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} {*protocol* | ***object-group*** *protocol_obj_grp_id*} {*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*operator* {*port* [*port*] | ***object-group*** *service_obj_grp_id*}] {*destination-ipv6-prefix/prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [{*operator port* [*port*] | ***object-group*** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} {*protocol* | ***object-group*** *protocol_obj_grp_id*} {*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*operator* {*port* [*port*] | ***object-group*** *service_obj_grp_id*}] {*destination-ipv6-prefix/prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [{*operator port* [*port*] | ***object-group*** *service_obj_grp_id*}] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} ***icmp6*** {*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} {*destination-ipv6-prefix/prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*icmp_type* | ***object-group*** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

no ipv6 access-list *id* [***line*** *line-num*] {***deny*** | ***permit***} ***icmp6*** {*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address* | ***object-group*** *network_obj_grp_id*} {*destination-ipv6-prefix/prefix-length* | ***any*** | ***host*** *destination-ipv6-address* | ***object-group*** *network_obj_grp_id*} [*icmp_type* | ***object-group*** *icmp_type_obj_grp_id*] [**log** [[*level*] [**interval** *secs*] | **disable** | **default**]]

シンタックスの説明

any	IPv6 プレフィックス ::/0 の短縮形で、任意の IPv6 アドレスを示します。
default	（オプション）ACE 用に syslog メッセージ 106100 が生成されるように指定します。
deny	条件に合致している場合、アクセスを拒否します。
destination-ipv6-address	トラフィックを受信するホストの IPv6 アドレス。
destination-ipv6-prefix	トラフィックの宛先となる IPv6 ネットワーク アドレス。
disable	（オプション）syslog メッセージングをディセーブルにします。
host	アドレスが特定のホストを指していることを指定します。
icmp6	セキュリティ アプライアンスを通過する ICMPv6 トラフィックにアクセス規則が適用されるように指定します。

icmp_type	アクセス規則によってフィルタリングされる ICMP メッセージ タイプを指定します。値は、有効な ICMP タイプ番号（0 ～ 255）または次の ICMP タイプ リテラルのいずれかにできます。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect *icmp_type* 引数を省略すると、すべての ICMP タイプを示します。
icmp_type_obj_grp_id	（オプション）オブジェクト グループの ICMP タイプ ID を指定します。
id	アクセス リストの名前または番号。
interval *secs*	（オプション）syslog メッセージ 106100 を生成する時間間隔を指定します。有効値の範囲は 1 ～ 600 秒です。デフォルトの間隔は 300 秒です。この値は、非アクティブのフローを削除するためのタイムアウト値としても使用されます。
level	（オプション）メッセージ 106100 の syslog レベルを指定します。有効値の範囲は 0 ～ 7 です。デフォルト レベルは 6（情報）です。
line *line-num*	（オプション）アクセス規則を挿入するリスト内の行番号。行番号を指定しない場合、ACE はアクセス リストの末尾に追加されます。
log	（オプション）ACE のロギング アクションを指定します。**log** キーワードを指定しない場合や、**log default** キーワードを指定した場合、ACE によってパケットが拒否されると、メッセージ 106023 が生成されます。log キーワードを単独で指定した場合や、レベルまたは間隔と一緒に指定した場合、ACE によってパケットが拒否されると、メッセージ 106100 が生成されます。アクセス リストの末尾にある暗黙的な拒否によって拒否されるパケットについては、ログに記録されません。ロギングをイネーブルにするには、ACE でパケットを明示的に拒否する必要があります。
network_obj_grp_id	既存のネットワーク オブジェクト グループの ID。
object-group	（オプション）オブジェクト グループを指定します。
operator	（オプション）送信元 IP アドレスを宛先 IP アドレスと比較するための演算子を指定します。*operator* は、送信元 IP アドレスまたは宛先 IP アドレスのポートを比較します。使用できる演算子は、**lt**（小なり）、**gt**（大なり）**eq**（同値）、**neq**（非同値）、および **range**（範囲）です。すべてのポートを含めるには（デフォルト）、演算子およびポートを使用せずに **ipv6 access-list** コマンドを使用します。

permit	条件に合致している場合、アクセスを許可します。
port	（オプション）アクセスを許可または拒否するポートを指定します。*port* 引数を入力する場合は、0 ～ 65535 の数を使用するか、*protocol* が ***tcp*** または ***udp*** であればリテラル名を使用して、ポートを指定します。 使用可能な TCP リテラル名は、**aol**、**bgp**、**chargen**、**cifc**、**citrix-ica**、**cmd**、**ctiqbe**、**daytime**、**discard**、**domain**、**echo**、**exec**、**finger**、**ftp**、**ftp-data**、**gopher**、**h323**、**hostname**、**http**、**https**、**ident**、**irc**、**kerberos**、**klogin**、**kshell**、**ldap**、**ldaps**、**login**、**lotusnotes**、**lpd**、**netbios-ssn**、**nntp**、**pop2**、**pop3**、**pptp**、**rsh**、**rtsp**、**smtp**、**sqlnet**、**ssh**、**sunrpc**、**tacacs**、**talk**、**telnet**、**uucp**、**whois**、および **www** です。 使用可能な UDP リテラル名は、**biff**、**bootpc**、**bootps**、**cifs**、**discard**、**dnsix**、**domain**、**echo**、**http**、**isakmp**、**kerberos**、**mobile-ip**、**nameserver**、**netbios-dgm**、**netbios-ns**、**ntp**、**pcanywhere-status**、**pim-auto-rp**、**radius**、**radius-acct**、**rip**、**secureid-udp**、**snmp**、**snmptrap**、**sunrpc**、**syslog**、**tacacs**、**talk**、**tftp**、**time**、**who**、**www**、および **xdmcp** です。
prefix-length	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。
protocol	IP プロトコルの名前または番号。有効値は、**icmp**、**ip**、**tcp**、**udp** のいずれか、または IP プロトコル番号を表す 1 ～ 254 までの整数です。
protocol_obj_grp_id	既存のプロトコル オブジェクト グループの ID。
service_obj_grp_id	（オプション）オブジェクト グループを指定します。
source-ipv6-address	トラフィックを送信するホストの IPv6 アドレス。
source-ipv6-prefix	ネットワーク トラフィックの発信元の IPv6 ネットワーク アドレス。

デフォルト

log キーワードを指定したときの syslog メッセージ 106100 のデフォルト レベルは、6（情報）です。

デフォルトのロギング間隔は 300 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 access-list コマンドを使用すると、IPv6 アドレスがポートまたはプロトコルにアクセスすることを許可または拒否するかどうかを指定できます。各コマンドは、ACE と呼ばれます。同じアクセス リスト名を持つ 1 つまたは複数の ACE は、アクセス リストと呼ばれます。アクセス リストをインターフェイスに適用するには、**access-group** コマンドを使用します。

アクセス リストを使用してアクセスを特別に許可しない限り、セキュリティ アプライアンスは、外部インターフェイスから内部インターフェイスへのパケットをすべて拒否します。内部インターフェイスから外部インターフェイスへのすべてのパケットは、特にアクセスを拒否しない限り、デフォルトで許可されます。

ipv6 access-list コマンドは、IPv6 専用であるという点を除き、**access-list** コマンドと類似しています。アクセス リストの詳細については、**access-list extended** コマンドを参照してください。

ipv6 access-list icmp コマンドは、セキュリティ アプライアンスを通過する ICMPv6 メッセージをフィルタリングするために使用されます。特定のインターフェイスでの発信および着信を許可する ICMPv6 トラフィックを設定するには、**ipv6 icmp** コマンドを使用します。

オブジェクト グループの設定方法については、**object-group** コマンドの項を参照してください。

例

次の例では、TCP を使用するすべてのホストが 3001:1::203:A0FF:FED6:162D のサーバにアクセスできるようにします。

```
hostname(config)# ipv6 access-list acl_grp permit tcp any host
3001:1::203:A0FF:FED6:162D
```

次の例では、**eq** とポートを使用して、FTP へのアクセスのみを拒否します。

```
hostname(config)# ipv6 access-list acl_out deny tcp any host
3001:1::203:A0FF:FED6:162D eq ftp
hostname(config)# access-group acl_out in interface inside
```

次の例では、**lt** を使用して、ポート 2025 より小さいすべてのポートへのアクセスを許可します。その結果、既知ポート（1 ～ 1024）へのアクセスが許可されます。

```
hostname(config)# ipv6 access-list acl_dmz1 permit tcp any host
3001:1::203:A0FF:FED6:162D lt 1025
hostname(config)# access-group acl_dmz1 in interface dmz1
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスに割り当てます。
ipv6 icmp	セキュリティ アプライアンスのインターフェイスに着信する ICMP メッセージに対して、アクセス規則を設定します。
object-group	オブジェクト グループ（アドレス、ICMP タイプ、およびサービス）を作成します。

ipv6 address

IPv6 をイネーブルにし、インターフェイス上で IPv6 アドレスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 address** コマンドを使用します。IPv6 アドレスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 address {***autoconfig*** | *ipv6-prefix*/*prefix-length* [***eui-64***] | *ipv6-address* ***link-local***}

no ipv6 address {***autoconfig*** | *ipv6-prefix*/*prefix-length* [***eui-64***] | *ipv6-address* ***link-local***}

シンタックスの説明

autoconfig	インターフェイス上でステートレス自動設定を使用して、IPv6 アドレスの自動設定をイネーブルにします。
eui-64	（オプション）IPv6 アドレスの下位 64 ビットにインターフェイス ID を指定します。
ipv6-address	インターフェイスに割り当てられた IPv6 リンク ローカル アドレス。
ipv6-prefix	インターフェイスに割り当てられた IPv6 ネットワーク アドレス。
link-local	アドレスがリンク ローカル アドレスであることを指定します。
prefix-length	アドレスの高次の連続ビットのうち、何個が IPv6 プレフィックス（IPv6 アドレスのネットワーク部分）を構成しているかを指定します。

デフォルト

IPv6 はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス上で IPv6 アドレスを設定すると、IPv6 がそのインターフェイス上でイネーブルになります。IPv6 アドレスの指定後に **ipv6 enable** コマンドを使用する必要はありません。

ipv6 address ***autoconfig*** コマンドは、ステートレス自動設定を使用して、インターフェイス上で IPv6 アドレスの自動設定をイネーブルにするために使用されます。アドレスは、ルータ アドバタイズメント メッセージで受信されたプレフィックスに基づいて設定されます。リンク ローカル アドレスが設定されていなければ、このインターフェイス用に自動的に生成されます。そのリンク ローカル アドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

ipv6 address eui-64 コマンドは、インターフェイスの IPv6 アドレスを設定するために使用されます。オプションの **eui-64** が指定されている場合は、アドレスの下位 64 ビットに EUI-64 インターフェイス ID が使用されます。*prefix-length* 引数に指定した値が 64 ビットより大きい場合は、プレフィックス ビットがインターフェイス ID に優先します。指定されたアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

Modified EUI-64 形式のインターフェイス ID は、リンク レイヤ アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク レイヤ（MAC）アドレスから生成されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番目のビット（ユニバーサル / ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

ipv6 address *link-local* コマンドは、インターフェイスの IPv6 リンク ローカル アドレスを設定するために使用されます。このコマンドで指定する *ipv6-address* は、インターフェイス用に自動的に生成されるリンク ローカル アドレスを上書きします。リンク ローカル アドレスは、リンク ローカル プレフィックス FE80::/64 と、Modified EUI-64 形式のインターフェイス ID で構成されます。MAC アドレス 00E0.B601.3B7A のインターフェイスには、リンク ローカル アドレス FE80::2E0:B6FF:FE01:3B7A が指定されます。指定されたアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。

例

次の例では、選択したインターフェイスのグローバル アドレスとして 3FFE:C00:0:1::576/64 を割り当てます。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 address 3ffe:c00:0:1::576/64
```

次の例では、選択したインターフェイスに IPv6 アドレスを自動的に割り当てます。

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 address autoconfig
```

次の例では、選択したインターフェイスに IPv6 アドレス 3FFE:C00:0:1::/64 を割り当て、アドバイザーの下位 64 ビットに EUI-64 インターフェイス ID を指定します。

```
hostname(config)# interface gigabitethernet 0/2
hostname(onfig-if)# ipv6 address 3FFE:C00:0:1::/64 eui-64
```

次の例では、選択したインターフェイスのリンク レベル アドレスとして FE80::260:3EFF:FE11:6670 を割り当てます。

```
hostname(config)# interface gigabitethernet 0/3
hostname(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

関連コマンド

コマンド	説明
debug ipv6 interface	IPv6 インターフェイスに関するデバッグ情報を表示します。
show ipv6 interface	IPv6 用に設定したインターフェイスのステータスを表示します。

ipv6 enable

明示的な IPv6 アドレスが設定されていないインターフェイス上で IPv6 処理をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスが設定されていないインターフェイス上で IPv6 処理をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enable

no ipv6 enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

IPv6 はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 enable コマンドは、インターフェイス上で IPv6 リンク ローカル ユニキャスト アドレスを自動的に設定し、インターフェイスの IPv6 処理をイネーブルにします。

no ipv6 enable コマンドは、明示的な IPv6 アドレスが指定されているインターフェイス上では IPv6 処理をディセーブルにしません。

例

次の例では、選択したインターフェイス上で IPv6 処理をイネーブルにします。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 enable
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスの IPv6 アドレスを設定し、インターフェイス上で IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 enforce-eui64

ローカル リンク上で IPv6 アドレスに Modified EUI-64 形式インターフェイス ID を適用するには、グローバル コンフィギュレーション モードで **ipv6 enforce-eui64** コマンドを使用します。Modified EUI-64 アドレス形式の適用をディセーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 enforce-eui64 *if_name*

no ipv6 enforce-eui64 *if_name*

シンタックスの説明

if_name	**nameif** コマンドで指定したとおりに、インターフェイスの名前を指定して、Modified EUI-64 アドレス形式の適用をイネーブルにします。

デフォルト

Modified EUI-64 形式の適用はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドがあるインターフェイス上でイネーブルの場合、そのインターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスと照合され、インターフェイス ID に Modified EUI-64 形式が使用されていることが確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を使用していない場合、パケットはドロップされ、次のシステム ログ メッセージが生成されます。

```
%PIX|ASA-3-325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが生成された場合に限り行われます。既存のフローからのパケットはチェックされません。その他に、アドレスの確認はローカル リンク上のホストに限り行われます。ルータの背後にあるホストから受信したパケットはアドレス形式の確認に失敗し、ドロップされます。その送信元 MAC アドレスがルータの MAC アドレスであり、ホストの MAC アドレスではないためです。

Modified EUI-64 形式のインターフェイス ID は、リンク レイヤ アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク レイヤ（MAC）アドレスから生成されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番目のビット（ユニバーサル / ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

例

次の例では、内部インターフェイスで受信した IPv6 アドレスに対して Modified EUI-64 形式の適用をイネーブルにします。

```
hostname(config)# ipv6 enforce-eui64 inside
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスで IPv6 アドレスを設定します。
ipv6 enable	インターフェイスで IPv6 をイネーブルにします。

ipv6 icmp

インターフェイスの ICMP アクセス規則を設定するには、グローバル コンフィギュレーション モードで **ipv6 icmp** コマンドを使用します。ICMP アクセス規則を削除するには、このコマンドの **no** 形式を使用します。

ipv6 icmp {***permit*** | ***deny***} {*ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *ipv6-address*} [*icmp-type*] *if-name*

no ipv6 icmp {***permit*** | ***deny***} {*ipv6-prefix*/*prefix-length* | ***any*** | ***host*** *ipv6-address*} [*icmp-type*] *if-name*

シンタックスの説明

any	任意の IPv6 アドレスを指定するキーワード。IPv6 プレフィックス ::/0 の短縮形。
deny	選択したインターフェイス上で、指定した ICMP トラフィックを拒否します。
host	アドレスが特定のホストを指していることを指定します。
icmp-type	アクセス規則によってフィルタリングされる ICMP メッセージ タイプを指定します。値は、有効な ICMP タイプ番号（0 ～ 255）または次の ICMP タイプ リテラルのいずれかにできます。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	アクセス規則の適用先となるインターフェイスの名前（**nameif** コマンドで指定したもの）。
ipv6-address	ICMPv6 メッセージをインターフェイスに送信するホストの IPv6 アドレス。
ipv6-prefix	ICMPv6 メッセージをインターフェイスに送信する IPv6 ネットワーク。
permit	選択したインターフェイス上で、指定した ICMP トラフィックを許可します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力する必要があります。

デフォルト

ICMP アクセス規則が定義されていない場合、ICMP トラフィックはすべて許可されます。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　IPv6 機能の ICMP は、IPv4 の ICMP と同じです。ICMPv6 は、ICMP エコー要求メッセージおよび応答メッセージに類似した ICMP 宛先到達不能メッセージおよび情報メッセージなどのエラーメッセージを生成します。また、IPv6 の ICMP パケットは、IPv6 近隣探索プロセスとパス MTU 探索で使用されます。

インターフェイスに ICMP 規則が定義されていない場合、IPv6 ICMP トラフィックはすべて許可されます。

インターフェイスに ICMP 規則が定義されている場合は、最初に一致した規則が処理され、それ以降の規則はすべて暗黙的に拒否されます。たとえば、最初に一致した規則が許可規則の場合、その ICMP パケットは処理されます。最初に一致した規則が拒否規則の場合や、ICMP パケットがそのインターフェイス上のどの規則にも一致しなかった場合、セキュリティ アプライアンスはその ICMP パケットを廃棄し、syslog メッセージを生成します。

このため、ICMP 規則に入力する順序が重要になります。特定のネットワークからの ICMP トラフィックをすべて拒否する規則を入力してから、そのネットワーク上にある特定のホストからの ICMP トラフィックを許可する規則を入力した場合、そのホスト規則が処理されることはありません。ICMP トラフィックは、ネットワーク規則によってブロックされます。ただし、ホスト規則を入力してから、ネットワーク規則を入力した場合、ホストの ICMP トラフィックは許可されますが、それ以外の当該ネットワークからの ICMP トラフィックはすべてブロックされます。

ipv6 icmp コマンドは、セキュリティ アプライアンス インターフェイスに着信する ICMP トラフィックのアクセス規則を設定します。パススルー ICMP トラフィックのアクセス規則を設定するには、**ipv6 access-list** コマンドを参照してください。

例　次の例では、外部インターフェイスで、すべての ping 要求を拒否し、すべての Packet Too Big メッセージを許可します（パス MTU 探索をサポートするため）。

```
hostname(config)# ipv6 icmp deny any echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

次の例では、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに、外部インターフェイスへの ping を許可します。

```
hostname(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
hostname(config)# ipv6 icmp permit 2001::/64 echo-reply outside
hostname(config)# ipv6 icmp permit any packet-too-big outside
```

関連コマンド

コマンド	説明
ipv6 access-list	アクセス リストを設定します。

ipv6 nd dad attempts

重複アドレスの検出中にインターフェイス上で送信される連続的なネイバー送信要求メッセージの数を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd dad attempts** コマンドを使用します。送信される重複アドレス検出メッセージの数をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd dad attempts *value*

no ipv6 nd dad [**attempts** *value*]

シンタックスの説明

value	0 ～ 600 の数。0 を入力すると、指定されたインターフェイス上で重複アドレス検出がディセーブルになります。1 を入力すると、1 回だけ送信するように設定されます。デフォルト値は 1 つのメッセージです。

デフォルト

デフォルトの試行回数は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。ネイバー送信要求メッセージの送信頻度を設定するには、**ipv6 nd ns-interval** コマンドを使用します。

管理上のダウン状態にあるインターフェイスでは、重複アドレス検出は一時停止されます。インターフェイスが管理上のダウン状態にある場合、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。

インターフェイスが管理上のアップ状態に戻ると、インターフェイス上で重複アドレス検出が自動的に再開されます。管理上のアップ状態に戻っているインターフェイスでは、インターフェイス上のすべてのユニキャスト IPv6 アドレスに対して重複アドレス検出が再開されます。

（注） インターフェイスのリンク ローカル アドレスに対して重複アドレス検出が実行されている間、他の IPv6 アドレスは引き続き一時的な状態に設定されます。リンク ローカル アドレスに対する重複アドレス検出が完了すると、残りの IPv6 アドレスに対して重複アドレス検出が実行されます。

重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態は DUPLICATE に設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンク ローカル アドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。

```
%PIX-4-DUPLICATE: Duplicate address FE80::1 on outside
```

重複アドレスがインターフェイスのグローバル アドレスの場合、そのアドレスは使用されなくなり、次のようなエラー メッセージが発行されます。

```
%PIX-4-DUPLICATE: Duplicate address 3000::4 on outside
```

重複アドレスに関連付けられているコンフィギュレーション コマンドはすべて設定済みのままになりますが、アドレスの状態は DUPLICATE に設定されます。

インターフェイスのリンク ローカル アドレスが変更された場合は、新しいリンク ローカル アドレスに対して重複アドレス検出が実行され、そのインターフェイスに関連付けられている他の IPv6 アドレスがすべて再生成されます（重複アドレス検出は新しいリンク ローカル アドレスに対してのみ実行されます）。

例

次の例では、インターフェイスの一時的なユニキャスト IPv6 アドレスに対して重複アドレス検出が実行されている間に 5 つの連続したネイバー送信要求メッセージが送信されるように設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd dad attempts 5
```

次の例では、選択したインターフェイス上で重複アドレス検出をディセーブルにします。

```
hostname(config)# interface gigabitethernet 0/1
hostname(config-if)# ipv6 nd dad attempts 0
```

関連コマンド

コマンド	説明
ipv6 nd ns-interval	インターフェイス上でネイバー送信要求メッセージの送信間隔を設定します。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd ns-interval

インターフェイス上で IPv6 ネイバー送信要求メッセージの再送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ns-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ns-interval *value*

no ipv6 nd ns-interval [*value*]

シンタックスの説明

value	IPv6 ネイバー送信要求メッセージの送信間隔（ミリ秒単位）。有効となる値の範囲は 1,000 ～ 3,600,000 ミリ秒です。デフォルト値は 1,000 ミリ秒です。

デフォルト

ネイバー送信要求メッセージの送信間隔は 1,000 ミリ秒になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

この値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

例

次の例では、Gigabitethernet 0/0 に対して IPv6 ネイバー送信要求メッセージの送信間隔を 9,000 ミリ秒に設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ns-interval 9000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd prefix

IPv6 ルータ アドバタイズメントに含める IPv6 プレフィックスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd prefix** コマンドを使用します。プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd prefix *ipv6-prefix/prefix-length* | ***default*** [[*valid-lifetime preferred-lifetime*] | [***at*** *valid-date preferred-date*] | ***infinite*** | ***no-advertise*** | ***off-link*** | ***no-autoconfig***]

no ipv6 nd prefix *ipv6-prefix/prefix-length* | ***default*** [[*valid-lifetime preferred-lifetime*] | [***at*** *valid-date preferred-date*] | ***infinite*** | ***no-advertise*** | ***off-link*** | ***no-autoconfig***]

シンタックスの説明

at *valid-date preferred-date*	ライフタイムと優先順位が期限切れになる日付と時刻。プレフィックスは、この指定された日付と時刻に到達するまで有効になります。有効期限の形式は、*date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* です。
default	デフォルト値が使用されます。
infinite	（オプション）この有効ライフタイムは期限切れになりません。
ipv6-prefix	ルータ アドバタイズメントに含める IPv6 ネットワーク番号。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
no-advertise	（オプション）ローカル リンク上のホストに対して、指定されたプレフィックスが IPv6 自動設定に使用されないことを示します。
no-autoconfig	（オプション）ローカル リンク上のホストに対して、指定されたプレフィックスが IPv6 自動設定に使用不能であることを示します。
off-link	（オプション）指定されたプレフィックスがオンリンクの判別に使用されないことを示します。
preferred-lifetime	指定された IPv6 プレフィックスが優先されたものとしてアドバタイズされる期間（秒単位）。有効となる値の範囲は、0 ～ 4294967295 秒です。最大値は、無限を意味します。infinite で指定することもできます。デフォルトは 604,800（7 日）です。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力する必要があります。
valid-lifetime	指定された IPv6 プレフィックスが有効なものとしてアドバタイズされる期間。有効となる値の範囲は、0 ～ 4294967295 秒です。最大値は、無限を意味します。**infinite** として指定することもできます。デフォルトは 2,592,000（30 日）です。

デフォルト

IPv6 ルータ アドバタイズメントを発信するインターフェイス上で設定されたすべてのプレフィックスがアドバタイズされる場合、有効ライフタイム 2,592,000 秒（30 日）と優先ライフタイム 604,800 秒（7 日）が使用され、「onlink」フラグと「autoconfig」フラグの両方が設定されます。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドを使用すると、プレフィックスをアドバタイズするかどうかなど、個別のパラメータをプレフィックスごとに制御できます。

デフォルトでは、**ipv6 address** コマンドを使用してインターフェイス上のアドレスとして設定されたプレフィックスは、ルータ アドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してアドバタイズメントのプレフィックスを設定すると、そのプレフィックスだけがアドバタイズされます。

default キーワードを使用すると、すべてのプレフィックスのデフォルト パラメータを設定できます。

日付を設定してプレフィックスの有効期限を指定することができます。有効ライフタイムと優先ライフタイムは、リアルタイムでカウントダウンされます。有効期限に到達すると、プレフィックスはアドバタイズされなくなります。

onlink が「オン」（デフォルト）の場合、指定されたプレフィックスはリンクに割り当てられます。指定されたプレフィックスを含むアドレスにトラフィックを送信するノードでは、宛先をリンク上でローカルに到達可能なものと見なします。

autoconfig が「オン」（デフォルト）の場合、ローカル リンク上のホストには、指定されたプレフィックスが IPv6 自動設定に使用可能であることが示されます。

例　次の例では、指定されたインターフェイスから送信されるルータ アドバタイズメントに、IPv6 プレフィックス 2001:200::/35、有効ライフタイム 1,000 秒、および優先ライフタイム 900 秒を含めます。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

関連コマンド

コマンド	説明
ipv6 address	IPv6 アドレスを設定し、インターフェイス上で IPv6 処理をイネーブルにします。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd ra-interval

インターフェイス上で IPv6 ルータ アドバタイズメントの送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-interval [***msec***] *value*

no ipv6 nd ra-interval [[***msec***] *value*]

シンタックスの説明

msec	（オプション）指定された値がミリ秒単位であることを示します。このキーワードがない場合、指定された値は秒単位となります。
value	IPv6 ルータ アドバタイズメントの送信間隔。有効な値の範囲は 3 ～ 1,800 秒ですが、***msec*** キーワードが指定されている場合は 500 ～ 1,800,000 ミリ秒となります。デフォルトは 200 秒です。

デフォルト

200 秒。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 nd ra-lifetime コマンドを使用してセキュリティ アプライアンスをデフォルト ルータとして設定した場合、送信間隔は IPv6 ルータ アドバタイズメントのライフタイム以下にする必要があります。他の IPv6 ノードと同期させないようにするには、使用する実際の値を、指定された値の 20% 以内でランダムに調整します。

例

次の例では、選択したインターフェイスに対して IPv6 ルータ アドバタイズメントの送信間隔を 201 秒に設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-interval 201
```

関連コマンド

コマンド	説明
ipv6 nd ra-lifetime	IPv6 ルータ アドバタイズメントのライフタイムを設定します。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd ra-lifetime

インターフェイス上で IPv6 ルータ アドバタイズメントの「ルータ ライフタイム」を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-lifetime** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-lifetime *seconds*

no ipv6 nd ra-lifetime [*seconds*]

シンタックスの説明

seconds	このインターフェイスにおけるデフォルト ルータとしてのセキュリティ アプライアンスの有効期間。有効となる値の範囲は、0 ～ 9000 秒です。デフォルトは 1800 秒です。0 は、セキュリティ アプライアンスを、選択したインターフェイス上のデフォルト ルータと見なしてはならないことを示します。

デフォルト

1800 秒。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

「ルータ ライフタイム」値は、インターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。この値は、このインターフェイスにおけるデフォルト ルータとしてのセキュリティ アプライアンスの有効期間を示します。

値を 0 以外の値に設定することは、セキュリティ アプライアンスをこのインターフェイス上のデフォルト ルータと見なす必要があることを示します。「ルータ ライフタイム」値を 0 以外の値に設定する場合は、ルータ アドバタイズメントの送信間隔より小さくしないでください。

値を 0 に設定することは、セキュリティ アプライアンスをこのインターフェイス上のデフォルト ルータと見なしてはならないことを示します。

例

次の例では、選択したインターフェイスに対して IPv6 ルータ アドバタイズメントのライフタイムを 1,801 秒に設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd ra-lifetime 1801
```

関連コマンド

コマンド	説明
ipv6 nd ra-interval	インターフェイス上で IPv6 ルータ アドバタイズメントの送信間隔を設定します。
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd reachable-time

到達可能性の確認イベントが発生した後でリモート IPv6 ノードを到達可能と見なす期間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd reachable-time** コマンドを使用します。デフォルト期間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd reachable-time *value*

no ipv6 nd reachable-time [*value*]

シンタックスの説明

value	リモート IPv6 ノードを到達可能と見なす期間（ミリ秒単位）。有効となる値の範囲は 0 ～ 3,600,000 ミリ秒です。デフォルト値は 0 です。 *value* に 0 を設定した場合、到達可能な時間は不確定として送信されます。受信側のデバイスが、到達可能時間値を設定して追跡します。

デフォルト

0 ミリ秒。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

期間を設定すると、使用不可能なネイバーを検出できます。設定期間を短くすると、使用不可能なネイバーをより迅速に検出できます。ただし、期間を短くするほど、IPv6 ネットワークの帯域幅の消費量と、IPv6 ネットワーク デバイスすべての処理リソースの消費量が増加します。通常の IPv6 動作において、設定期間を大幅に短くすることはお勧めできません。

このコマンドを 0 に設定した場合にセキュリティ アプライアンスで使用される実際の値を含んだ到達可能時間を確認するには、**show ipv6 interface** コマンドを使用して、適用される ND 到達可能時間などの IPv6 インターフェイスの情報を表示します。

例

次の例では、選択したインターフェイスに対して IPv6 到達可能期間を 1,700,000 ミリ秒に設定します。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd reachable-time 1700000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 nd suppress-ra

LAN インターフェイス上で IPv6 ルータ アドバタイズメントを送信しないようにするには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN インターフェイス上で IPv6 ルータ アドバタイズメントの送信を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

IPv6 ユニキャスト ルーティングがイネーブルの場合は、LAN インターフェイス上でルータ アドバタイズメントが自動的に送信されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LAN 以外のタイプのインターフェイス（たとえば、シリアル インターフェイスやトンネル インターフェイス）上で IPv6 ルータ アドバタイズメントの送信をイネーブルにするには、**no ipv6 nd suppress-ra** コマンドを使用します。

例

次の例では、選択したインターフェイス上で IPv6 ルータ アドバタイズメントを送信しないようにします。

```
hostname(config)# interface gigabitethernet 0/0
hostname(config-if)# ipv6 nd suppress-ra
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 用に設定したインターフェイスのユーザビリティ ステータスを表示します。

ipv6 neighbor

IPv6 近隣探索キャッシュにスタティック エントリを設定するには、グローバル コンフィギュレーション モードで **ipv6 neighbor** コマンドを使用します。近隣探索キャッシュからスタティック エントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 neighbor *ipv6_address if_name mac_address*

no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

シンタックスの説明

if_name	**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。
ipv6_address	ローカルのデータリンク アドレスに対応する IPv6 アドレス。
mac_address	ローカルのデータライン（ハードウェア MAC）アドレス。

デフォルト

IPv6 近隣探索キャッシュにスタティック エントリは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ipv6 neighbor コマンドは、**arp** コマンドと類似しています。指定された IPv6 アドレスのエントリが近隣探索キャッシュにすでに存在する（IPv6 近隣探索プロセスからラーニングされた）場合、そのエントリはスタティック エントリに自動的に変換されます。**copy** コマンドを使用してコンフィギュレーションを格納すると、このエントリがコンフィギュレーションに格納されます。

IPv6 近隣探索キャッシュのスタティック エントリを表示するには、**show ipv6 neighbor** コマンドを使用します。

clear ipv6 neighbors コマンドは、IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。**no ipv6 neighbor** コマンドは、指定したスタティック エントリを近隣探索キャッシュから削除します。このコマンドによってダイナミック エントリ（IPv6 近隣探索プロセスからラーニングされたエントリ）がキャッシュから削除されることはありません。**no ipv6 enable** コマンドを使用してインターフェイス上で IPv6 をディセーブルにすると、そのインターフェイスに設定された IPv6 近隣探索キャッシュのすべてのエントリが、スタティック エントリを除いて削除されます（エントリの状態は INCMP [Incomplete] に変更されます）。

近隣探索プロセスによって IPv6 近隣探索キャッシュのスタティック エントリが変更されることはありません。

例

次の例では、IPv6 アドレス 3001:1::45A および MAC アドレス 0002.7D1A.9472 の内部ホストのスタティック エントリを近隣探索キャッシュに追加します。

```
hostname(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。
show ipv6 neighbor	IPv6 近隣キャッシュ情報を表示します。

ipv6 route

IPv6 ルーティング テーブルに IPv6 ルートを追加するには、グローバル コンフィギュレーション モードで **ipv6 route** コマンドを使用します。IPv6 デフォルト ルートを削除するには、このコマンドの **no** 形式を使用します。

ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance*]

no ipv6 route *if_name ipv6-prefix/prefix-length ipv6-address* [*administrative-distance*]

シンタックスの説明

administrative-distance	（オプション）ルートの管理ディスタンス。デフォルト値は 1 です。この場合、スタティック ルートは、接続済みルートを除く他のあらゆるタイプのルートに優先します。
if_name	ルートの設定対象となるインターフェイスの名前。
ipv6-address	特定のネットワークに到達するために使用できるネクストホップの IPv6 アドレス。
ipv6-prefix	スタティック ルートの宛先となる IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、何個がプレフィックス（ネットワーク部分）を構成しているかを指定します。プレフィックスの長さ値の前に、スラッシュ（/）を入力する必要があります。

デフォルト

デフォルトでは、*administrative-distance* は 1 になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IPv6 ルーティング テーブルの内容を表示するには、**show ipv6 route** コマンドを使用します。

例

次の例では、ネットワーク 7fff::0/32 に対するパケットを、管理ディスタンス 110 で、3FFE:1100:0:CC00::1 にある内部インターフェイス上のネットワーキング デバイスにルーティングします。

```
hostname(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 のルーティング テーブル アップデートおよびルート キャッシュ アップデートに関するデバッグ情報を表示します。
show ipv6 route	IPv6 ルーティング テーブルの現在の内容を表示します。

isakmp am-disable

アグレッシブ モードの着信接続をディセーブルにするには、グローバル コンフィギュレーション モードで **isakmp am-disable** コマンドを使用します。アグレッシブ モードの着信接続をイネーブルにするには、このコマンドの **no** 形式を使用します。

isakmp am-disable

no isakmp am-disable

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルト値はイネーブルです。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp am-disable** コマンドに置き換えられました。

例　次の例では、グローバル コンフィギュレーション モードで、アグレッシブ モードの着信接続をディセーブルにします。

```
hostname(config)# isakmp am-disable
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp disconnect-notify

ピアに対する切断通知をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp disconnect-notify** コマンドを使用します。切断通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp disconnect-notify

no isakmp disconnect-notify

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp disconnect-notify** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
hostname(config)# isakmp disconnect-notify
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp enable

IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上で ISAKMP ネゴシエーションをイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp enable** コマンドを使用します。インターフェイス上で ISAKMP ディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp enable *interface-name*

no isakmp enable *interface-name*

シンタックスの説明

interface-name	ISAKMP ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	このコマンドは廃止されました。**crypto isakmp enable** コマンドに置き換えられました。

例

次の例は、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
hostname(config)# no isakmp enable inside
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp identity

フェーズ 2 ID をピアに送信するように設定するには、グローバル コンフィギュレーション モードで **isakmp identity** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

no isakmp identity {address | hostname | key-id *key-id-string* | **auto}**

シンタックスの説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	ISKMP ネゴシエーションを、接続タイプよって判別します（事前共有キーの IP アドレス、または証明書認証用の証明書 DN）。
hostname	ISAKMP の識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用する文字列を指定します。

デフォルト

デフォルトの ISAKMP ID は、**isakmp identity hostname** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	このコマンドは廃止されました。**crypto isakmp identity** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、IPSec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションを、接続タイプに応じてイネーブルにします。

```
hostname(config)# isakmp identity auto
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp ikev1-user-authentication

IKE 中にハイブリッド認証を設定するには、トンネル グループ ipsec アトリビュート コンフィギュレーション モードで **isakmp ikev1-user-authentication** コマンドを使用します。ハイブリッド認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp ikev1-user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

no isakmp ikev1-user-authentication [*interface*] {**none** | **xauth** | **hybrid**}

シンタックスの説明

hybrid	IKE の使用時にハイブリッド XAUTH 認証を指定します。
interface	（オプション）ユーザ認証方式を設定するインターフェイスを指定します。
none	IKE の使用時にユーザ認証をディセーブルにします。
xauth	XAUTH（拡張ユーザ認証とも呼ばれる）を指定します。

デフォルト

デフォルトの認証方式は XAUTH（拡張ユーザ認証）です。デフォルトの *interface* はすべてのインターフェイスです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス認証や RADIUS、TACACS+、または SecurID といったリモート VPN ユーザ認証用の従来の手法にデジタル証明書を使用する場合は、このコマンドを使用します。このコマンドは、IKE のフェーズ 1 を次の 2 ステップに分けます。2 つのステップを合せてハイブリッド認証と呼びます。

1. セキュリティ アプライアンスは、リモート VPN ユーザに対して標準の公開キー技術を使用して認証を行います。この認証により単方向で認証される IKE セキュリティ アソシエーションを確立します。
2. そして、XAUTH 交換で、リモート VPN ユーザが認証されます。この拡張認証では、サポートされている従来の認証方式のいずれかが使用されます。

（注） 認証タイプをハイブリッドに設定するには、認証サーバを設定し、事前共有キーを作成して、トラストポイントを設定する必要があります。

オプションの **interface** パラメータを省略すると、コマンドはすべてのインターフェイスに適用され、インターフェイスごとにコマンドが指定されていない際にはバックアップとして機能します。トンネル グループに 2 つの **isakmp ikev1-user-authentication** コマンドを指定した場合、1 つは **interface** パラメータを使用し、2 つ目はそれを使用しません。インターフェイスを指定するコマンドはその特定のインターフェイスを優先します。

例

次のコマンド例は、example-group と呼ばれるトンネル グループの内部インターフェイスでハイブリッド XAUTH をイネーブルにします。

```
hostname(config)# tunnel-group example-group type ipsec-ra
hostname(config)# tunnel-group example-group ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp ikev1-user-authentication (inside) hybrid
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバを定義します。
pre-shared-key	IKE 接続をサポートする事前共有キーを作成します。
tunnel-group	IPSec、L2TP/IPSec、および WebVPN 接続に固有のレコードを含むデータベースを作成および管理します。

isakmp ipsec-over-tcp

IPSec over TCP をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp ipsec-over-tcp** コマンドを使用します。IPSec over TCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp ipsec-over-tcp [**port** *port1...port10*]

シンタックスの説明

port *port1...port10*	（オプション）デバイスが IPSec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号の範囲は 1 ～ 65535 です。デフォルトのポート番号は 10000 です。

デフォルト

デフォルト値はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp ipsec-over-tcp** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、ポート 45 上で IPSec over TCP をイネーブルにします。

```
hostname(config)# isakmp ipsec-over-tcp port 45
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp keepalive

IKE DPD を設定するには、トンネル グループ ipsec アトリビュート コンフィギュレーション モードで **isakmp keepalive** コマンドを使用します。デフォルトでは、すべてのトンネル グループで IKE キープアライブが、デフォルトのしきい値およびリトライ値を使用してイネーブルになっています。キープアライブ パラメータを、デフォルトのしきい値およびリトライ値を使用してイネーブルにした状態に戻すには、このコマンドの ***no*** 形式を使用します。

isakmp keepalive [***threshold*** *seconds*] [***retry*** *seconds*] [**disable**]

no isakmp keepalive disable

シンタックスの説明

disable	IKE キープアライブ処理をディセーブルにします。デフォルトではイネーブルになっています。
retry *seconds*	キープアライブ応答が受信されなくなった後のリトライ間の間隔を秒単位で指定します。範囲は 2 ～ 10 秒です。デフォルトは 2 秒です。
threshold *seconds*	キープアライブのモニタリングを開始するまでピアがアイドル状態を維持できる秒数を指定します。範囲は 10 ～ 3,600 秒です。LAN-to-LAN グループのデフォルトは 10 秒で、リモートアクセス グループのデフォルトは 300 秒です。

デフォルト

リモートアクセス グループのデフォルトは、しきい値が 300 秒で、リトライが 2 秒です。

LAN-to-LAN グループのデフォルトは、しきい値が 10 秒で、リトライが 2 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、IPSec リモートアクセスおよび IPSec LAN-to-LAN トンネル グループ タイプだけに適用できます。

例

次の例では、config-ipsec コンフィギュレーション モードで、209.165.200.225 という IP アドレスを持つ IPSec LAN-to-LAN トンネル グループに対して、IKE DPD を設定し、しきい値を 15 に設定し、リトライ間隔を 10 に指定します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

isakmp nat-traversal

NAT Traversal をグローバルにイネーブルにするには、グローバル コンフィギュレーション モードで ISAKMP をイネーブルにしたことを確認し（イネーブルにするには **isakmp enable** コマンドを使用します）、次に **isakmp nat-traversal** コマンドを使用します。NAT Traversal がイネーブルのときに、これをディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

シンタックスの説明

natkeepalive	NAT キープアライブ間隔を 10 ～ 3,600 秒の範囲で設定します。デフォルトは 20 秒です。

デフォルト

デフォルトで、NAT Traversal（**isakmp nat-traversal**）はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	このコマンドは廃止されました。**crypto isakmp nat-traversal** コマンドに置き換えられました。

使用上のガイドライン

Network Address Translation（NAT; ネットワーク アドレス変換）は、Port Address Translation（PAT; ポート アドレス変換）も含め、IPSec も使用している多くのネットワークで使用されていますが、IPSec パケットが NAT デバイスを問題なく通過することを妨げる非互換性が数多くあります。NAT Traversal を使用すると、ESP パケットが 1 つまたは複数の NAT デバイスを通過できるようになります。

セキュリティ アプライアンスは、IETF の「UDP Encapsulation of IPsec Packets」ドラフトのバージョン 2 とバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に記述されているとおり NAT Traversal をサポートしています。NAT Traversal は、ダイナミックとスタティックの両方の暗号マップについてサポートされています。

このコマンドは、セキュリティ アプライアンス上で NAT-T をグローバルにイネーブルにします。暗号マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次の例では、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、30 秒間隔で NAT Traversal をイネーブルにします。

```
hostname(config)# isakmp enable
hostname(config)# isakmp nat-traversal 30
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy authentication

IKE ポリシー内の認証方式を指定するには、グローバル コンフィギュレーション モードで **isakmp policy authentication** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

シンタックスの説明

crack	認証方式として、IKE Challenge/Response for Authenticated Cryptographic Keys（CRACK）を指定します。
pre-share	認証方式として、事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
rsa-sig	認証方式として、RSA シグニチャを指定します。 RSA シグニチャは、IKE ネゴシエーションに対する否認防止ができます。これは、基本的にユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。

デフォルト

デフォルトの ISAKMP ポリシー認証は、**pre-share** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。DSA-Sig が 7.0 で追加されました。

使用上のガイドライン

RSA シグニチャを指定する場合は、認証局（CA）から証明書を取得するようにセキュリティ アプライアンスとそのピアを設定する必要があります。事前共有キーを指定する場合は、セキュリティ アプライアンスとそのピアに、事前共有キーを別々に設定する必要があります。

例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy authentication** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに RSA シグニチャの認証方式を使用するように設定します。

```
hostname(config)# isakmp policy 40 authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy encryption

IKE ポリシー内の暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

no isakmp policy *priority* **encryption** {**aes | aes-192| aes-256 | des | 3des**}

シンタックスの説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は **3des** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy encryption** に置き換えられました。

例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy encryption** コマンドを使用する方法を示しています。この例では、優先順位番号 25 の IKE ポリシーに 128 ビット キーの AES 暗号化アルゴリズムを使用するように設定します。

```
hostname(config)# isakmp policy 25 encryption aes
```

次の例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシーに 3DES アルゴリズムを使用するように設定します。

```
hostname(config)# isakmp policy 40 encryption 3des
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy group

IKE ポリシーの Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **isakmp policy group** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。Diffie-Hellman グループ識別子をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **group** {**1** | **2** | **5** | **7**}

no isakmp policy *priority* **group**

シンタックスの説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。768 ビットは、デフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 が使用されるように指定します。
group 5	IKE ポリシーで、1536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。
group 7	IKE ポリシーで、Diffie-Hellman Group 7 を使用することを指定します。Group 7 は IPSec SA キーを生成します。楕円曲線フィールドのサイズは 163 ビットです。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。

デフォルト

デフォルトはグループ 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。Group 7 が追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy group** コマンドに置き換えられました。

使用上のガイドライン

グループ オプションには、768 ビット（DH Group 1）、1,024 ビット（DH Group 2）、1,536 ビット（DH Group 5）、および DH Group 7 の 4 つがあります。1,024 ビットと 1,536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

(注)　Cisco VPN Client Version 3.x 以降では、**isakmp policy** で DH **group 2** を設定する必要があります（DH **group 1** を設定した場合、Cisco VPN Client は接続できません）。

AES は、VPN-3DES のライセンスがあるセキュリティ アプライアンスに限りサポートされます。AES が提供するキーはサイズが大きいため、ISAKMP ネゴシエーションには、**group 1** や **group 2** ではなく、Diffie-Hellman（DH）**group 5** を使用する必要があります。この設定には、**isakmp policy priority group 5** コマンドを使用します。

例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy group** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに、グループ 2、1024 ビット Diffie Hellman を使用するように設定します。

```
hostname(config)# isakmp policy 40 group 2
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy hash** コマンドを使用します。IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

ハッシュ アルゴリズムをデフォルト値の SHA-1 にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **hash** {**md5 | sha**}

no isakmp policy *priority* **hash**

シンタックスの説明

md5	IKE ポリシーで使用するハッシュ アルゴリズムとして、MD5（HMAC バリアント）を指定します。
priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
sha	IKE ポリシーで使用するハッシュ アルゴリズムとして、SHA-1（HMAC バリアント）を指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy hash** コマンドに置き換えられました。

使用上のガイドライン

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 は、SHA-1 よりもダイジェストが小さく、わずかに速いとされています。

例

次の例は、グローバル コンフィギュレーション モードで、**isakmp policy hash** コマンドを使用する方法を示しています。この例では、優先順位番号 40 の IKE ポリシーに MD5 ハッシュ アルゴリズムを使用することを指定します。

```
hostname(config)# isakmp policy 40 hash md5
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy lifetime

IKE セキュリティ アソシエーションの期限が満了するまでのライフタイムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy lifetime** コマンドを使用します。ピアがライフタイムを提示していなければ、無限のライフタイムを指定できます。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）にリセットするには、このコマンドの **no** 形式を使用します。

isakmp policy *priority* **lifetime** *seconds*

no isakmp policy *priority* **lifetime**

シンタックスの説明

priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
seconds	各セキュリティ アソシエーションが期限満了するまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2,147,483,647 秒の整数を使用します。無限のライフタイムを提示するには、0 秒を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy lifetime** コマンドに置き換えられました。

使用上のガイドライン

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータを合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限満了するまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限満了するまでその後の IKE ネゴシエーションで利用できるため、新しい IPSec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限満了する前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、セキュリティ アプライアンスで以降の IPSec セキュリティ アソシエーションを設定する時間が節約されます。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することをお勧めします。

（注） IKE セキュリティ アソシエーションが無限のライフタイムに設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからのネゴシエートされた有限のライフタイムが使用されます。
次の例は、グローバル コンフィギュレーション モードで、**isakmp policy lifetime** コマンドを使用する方法を示します。この例では、優先順位番号 40 の IKE ポリシー内に IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定します。

例

この例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシー内に IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定します。

```
hostname(config)# isakmp policy 40 lifetime 50400
```

次の例では、グローバル コンフィギュレーション モードで、IKE セキュリティ アソシエーションを無限のライフタイムに設定します。

```
hostname(config)# isakmp policy 40 lifetime 0
```

関連コマンド

clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp reload-wait

すべてのアクティブなセッションが自主的に終了するまで待機してからセキュリティ アプライアンスをリブートできるようにするには、グローバル コンフィギュレーション モードで **isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するまで待機しないでセキュリティ アプライアンスのリブートを進めるには、このコマンドの **no** 形式を使用します。

isakmp reload-wait

no isakmp reload-wait

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp reload-wait** コマンドに置き換えられました。

例

次の例では、グローバル コンフィギュレーション モードで、すべてのアクティブなセッションが終了するまで待機してからリブートするように、セキュリティ アプライアンスに通知します。

```
hostname(config)# isakmp reload-wait
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

issuer-name

規則エントリ文字列との比較対象となる CA 証明書の DN を指定するには、CA 証明書マップ コンフィギュレーション モードで **issuer-name** コマンドを使用します。発行者名を削除するには、コマンドの **no** 形式を使用します。

issuer-name [**attr** *tag*] {**eq | ne | co | nc**} *string*

no issuer-name [**attr** *tag*] {**eq | ne | co | nc**} *string*

シンタックスの説明

attr tag	証明書の DN 文字列で、指定されているアトリビュート値だけが規則エントリ文字列と比較されることを示します。タグの値を次に示します。 DNQ = DN 修飾子 GENQ = 世代修飾子 I = イニシャル GN = 名 N = 名前 SN = 姓 IP = IP アドレス SER = シリアル番号 UNAME = 非構造化名 EA = 電子メール アドレス T = 役職 O = 組織名 L = 地名 SP = 州または都道府県 C = 国または地域 OU = 組織ユニット CN = 通常名
co	DN 文字列または指定されているアトリビュートが、規則エントリ文字列の部分文字列と一致する必要があることを指定します。
eq	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致する必要があることを指定します。
nc	DN 文字列または指定されているアトリビュートが、規則エントリ文字列の部分文字列と一致しない必要があることを指定します。
ne	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致しない必要があることを指定します。
string	規則エントリ情報を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、証明書マップ 4 の CA 証明書マップ モードに入り、発行者名を O = central として設定します。

```
hostname(config)# crypto ca certificate map 4
hostname(ca-certificate-map)# issuer-name attr o eq central
hostname(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードに入ります。
subject-name（暗号 CA 証明書マップ）	規則エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。

CHAPTER 17

java-trustpoint コマンド～ kill コマンド

java-trustpoint

指定したトラストポイントの場所から PKCS12 証明書とキー関連情報を使用する WebVPN Java オブジェクト署名機能を設定するには、Webvpn コンフィギュレーション モードで **java-trustpoint** コマンドを使用します。

Java オブジェクト署名のトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

java-trustpoint *trustpoint*

no java-trustpoint

シンタックスの説明

trustpoint	**crypto ca import** コマンドによって設定されたトラストポイントの場所を指定します。

デフォルト

デフォルトでは、Java オブジェクト署名のトラストポイントは none に設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(2)	このコマンドが導入されました。

使用上のガイドライン

トラストポイントは、certificate authority（CA; 認証局）または ID キー ペアを表します。java-trustpoint コマンドの場合、指定したトラストポイントにはアプリケーション署名エンティティの X.509 証明書、その証明書に対応する RSA 秘密鍵、ルート CA までの認証局チェーンを含める必要があります。そのためには通常、**crypto ca import** コマンドを使用して PKCS12 形式のバンドルをインポートします。PKCS12 バンドルは、信頼できる CA 認証局から入手するか、openssl といったオープンソース ツールを使用して既存の X.509 証明書と RSA 秘密鍵から手作業で作成できます。

例

次の例では、最初に新しいトラストポイントを設定してから、そのトラストポイントを WebVPN Java オブジェクト署名用に設定します。次のコマンドは、mytrustpoint という新しいトラストポイントを作成します。

```
hostname(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
hostname(config)#
```

次の例は、WebVPN Java オブジェクトに署名する新しいトラストポイントを設定します。

```
hostname(config)# webvpn
hostname(config)# java-trustpoint mytrustpoint
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca import	PKCS12 データを使用してトラストポイントの証明書とキーペアをインポートします。

join-failover-group

コンテキストをフェールオーバー グループに割り当てるには、コンテキスト コンフィギュレーション モードで **join-failover-group** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

join-failover-group *group_num*

no join-failover-group *group_num*

シンタックスの説明

group_num	フェールオーバー グループの番号を指定します。

デフォルト

フェールオーバー グループ 1。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

管理コンテキストは、常にフェールオーバー グループ 1 に割り当てられます。フェールオーバー グループとコンテキストの関連付けを表示するには、**show context detail** コマンドを使用します。

コンテキストをフェールオーバー グループに割り当てる前に、**failover group** コマンドを使用して、フェールオーバー グループをシステム コンテキスト内に作成する必要があります。このコマンドは、コンテキストがアクティブな状態になっている装置上で入力します。デフォルトでは、未割り当てのコンテキストは、フェールオーバー グループ 1 のメンバーになっています。そのため、コンテキストがまだフェールオーバー グループに割り当てられていない場合は、フェールオーバー グループ 1 がアクティブ状態になっている装置上で、このコマンドを入力する必要があります。

システムからフェールオーバー グループを削除するには、事前に **no join-failover-group** コマンドを使用して、フェールオーバー グループからコンテキストをすべて削除しておく必要があります。

例

次の例では、ctx1 というコンテキストをフェールオーバー グループ 2 に割り当てます。

```
hostname(config)# context ctx1
hostname(config-context)# join-failover-group 2
hostname(config-context)# exit
```

関連コマンド

コマンド	説明
context	指定したコンテキストのコンテキスト コンフィギュレーション モードに入ります。
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
show context detail	コンテキストの詳細情報（名前、クラス、インターフェイス、フェールオーバー グループの関連付け、およびコンフィギュレーション ファイルの URL など）を表示します。

kerberos-realm

この Kerberos サーバのレルム名を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **kerberos-realm** コマンドを使用します。レルム名を削除するには、このコマンドの **no** 形式を使用します。

kerberos-realm *string*

no kerberos-realm

シンタックスの説明

string	大文字と小文字が区別される最大 64 文字の英数字の文字列。文字列にスペースは使用できません。

（注） Kerberos レルム名に使用できるのは、数字と大文字のアルファベットのみです。セキュリティ アプライアンスでは、*string* 引数に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。必ず大文字のアルファベットだけを使用してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで導入されました。

使用上のガイドライン

このコマンドは、Kerberos サーバに対してのみ有効です。

Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レルムの Windows 2000 Active Directory サーバ上で実行する場合は、*string* 引数の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レルム名です。

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

string 引数には、数字と大文字のアルファベットのみを使用する必要があります。**kerberos-realm** コマンドでは、大文字と小文字が区別されます。また、セキュリティ アプライアンスでは、小文字は大文字に変換されません。

例

次のシーケンスは、AAA サーバ ホストの設定に関するコンテキストで Kerberos レルムを「EXAMPLE.COM」に設定するための **kerberos-realm** コマンドを示しています。

```
hostname(config)# aaa-server svrgrp1 protocol kerberos
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション サブモードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

key

AAA サーバに対して NAS を認証するために使用されるサーバ シークレットの値を指定するには、AAA サーバ ホスト モードで **key** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。キーを削除するには、このコマンドの **no** 形式を使用します。キー（サーバ シークレット）の値によって、セキュリティ アプライアンスが AAA サーバに対して認証されます。

key *key*

no key

シンタックスの説明

key	最大 127 文字の英数字キーワード。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

key の値は、127 文字までの英数字で構成されているキーワードで、TACACS+ サーバ上のキーと同じ値にします。アルファベットの大文字と小文字は区別されます。128 文字以降に入力された文字は、すべて無視されます。このキーは、クライアントとサーバの間でやり取りするデータを暗号化するために使用されます。キーは、クライアント システムとサーバ システムの両方で同一である必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。

このコマンドは、RADIUS サーバと TACACS+ サーバに対してのみ有効です。

以前の PIX Firewall のバージョンで使用されていた **aaa-server** コマンドの **key** パラメータは、対応する **key** コマンドに自動的に変換されます。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という TACACS+ AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、キーを「myexclusivemumblekey」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# key myexclusivemumblekey
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	AAA サーバのコンフィギュレーションを表示します。

keypair

証明する公開キーのキー ペアを指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **keypair** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

keypair *name*

no keypair

シンタックスの説明

name	キー ペアの名前を指定します。

デフォルト

デフォルト設定では、キー ペアは含まれません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、central トラストポイントの暗号 CA トラストポイント コンフィギュレーション モードに入り、central トラストポイント用に証明するキー ペアを指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# keypair exchange
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
crypto key generate dsa	DSA キーを生成します。
crypto key generate rsa	RSA キーを生成します。
default enrollment	登録パラメータをデフォルトに戻します。

kill

Telnet セッションを終了するには、特権 EXEC モードで **kill** コマンドを使用します。

kill *telnet_id*

シンタックスの説明

telnet_id	Telnet セッションの ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

kill コマンドを使用すると、Telnet セッションを終了できます。Telnet セッションの ID を表示するには、**who** コマンドを使用します。Telnet セッションを終了すると、セキュリティ アプライアンスは、警告することなく、すべてのアクティブなコマンドを終了して接続をドロップします。

例

次の例は、ID「2」の Telnet セッションを終了する方法を示しています。最初に、アクティブな Telnet セッションのリストを表示するため、**who** コマンドを入力します。次に、ID「2」の Telnet セッションを終了するため、**kill 2** コマンドを入力します。

```
hostname# who
2: From 10.10.54.0

hostname# kill 2
```

関連コマンド

コマンド	説明
telnet	セキュリティ アプライアンスへの Telnet アクセスを設定します。
who	アクティブな Telnet セッションのリストを表示します。

CHAPTER 18

l2tp tunnel hello コマンド～ log-adj-changes コマンド

l2tp tunnel hello

L2TP over IPSec 接続の hello メッセージ間の間隔を指定するには、グローバル コンフィギュレーション モードで **l2tp tunnel hello** コマンドを使用します。コマンドをコンフィギュレーションから削除してデフォルトを設定するには、このコマンドの no 形式を使用します。

l2tp tunnel hello *interval*

no l2tp tunnel hello *interval*

シンタックスの説明

interval	hello メッセージ間の間隔（秒）。デフォルトは 60 秒です。範囲は 10 ～ 300 秒です。

デフォルト

デフォルトは 60 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

l2tp tunnel hello コマンドは、セキュリティ アプライアンスによる L2TP 接続の物理レイヤに関する問題の検出をイネーブルにします。デフォルトは 60 秒です。それをより低い値に設定すると、問題の発生した接続はより早く解除されます。

例

次の例では、hello メッセージ間の間隔を 30 秒に設定します。

```
hostname(config)# l2tp tunnel hello 30
```

関連コマンド

コマンド	説明
show vpn-sessiondbdetail remote filter protocol L2TPOverIPSec	L2TP 接続の詳細を表示します。
vpn-tunnel-protocol l2tp-ipsec	特定のトンネル グループのトンネリング プロトコルとして L2TP をイネーブルにします。

ldap-attribute-map（AAA サーバ ホスト モード）

既存のマッピング コンフィギュレーションを LDAP ホストにバインドするには、AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用します。

バインディングを削除するには、このコマンドの **no** 形式を使用します。

ldap-attribute-map *map-name*

no ldap-attribute-map *map-name*

シンタックスの説明

map-name	LDAP アトリビュート マッピング コンフィギュレーションを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シスコ定義の LDAP アトリビュート名が使い勝手が悪い、または他の要件に合致しない場合は、独自のアトリビュート名を作成し、Cisco アトリビュートにマッピングしてから、得られたアトリビュート コンフィギュレーションを LDAP サーバにバインドすることができます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用して、何も入力されていないアトリビュート マップを作成します。このコマンドにより、ldap-attribute-map モードに入ります。このコマンドでは、「ldap」の後にハイフンがないことに注意してください。

2. ldap-attribute-map モードで **map-name** コマンドおよび **map-value** コマンドを使用して、アトリビュート マッピング コンフィギュレーションに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用して、アトリビュート マップ コンフィギュレーションを LDAP サーバにバインドします。

例

次のコマンド例では、AAA サーバ ホスト コンフィギュレーション モードに入り、myldapmap という名前の既存のアトリビュート マップを ldapsvr1 という名前の LDAP サーバにバインドします。

```
hostname(config)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-attribute-map myldapmap
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。
map-name	ユーザ定義の LDAP アトリビュート名を、Cisco LDAP アトリビュート名にマッピングします。
map-value	ユーザ定義のアトリビュート値を、Cisco　アトリビュートにマッピングします。
show running-config ldap attribute-map	特定の実行 ldap アトリビュート マッピング コンフィギュレーション、またはすべての実行アトリビュート マッピング コンフィギュレーションを表示します。
clear configure ldap attribute-map	すべての LDAP アトリビュート マップを削除します。

ldap attribute-map（グローバル コンフィギュレーション モード）

ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために LDAP アトリビュート マップを作成して名前をつけるには、グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用します。

マップを削除するには、このコマンドの **no** 形式を使用します。

ldap attribute-map *map-name*

no ldap attribute-map *map-name*

シンタックスの説明

map-name	LDAP アトリビュート マップにユーザ定義の名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ldap attribute-map コマンドを使用すると、独自のアトリビュート名と値を Cisco アトリビュート名にマッピングできます。作成されたアトリビュート マップは、LDAP サーバにバインドすることができます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用して、何も入力されていないアトリビュート マップを作成します。このコマンドにより、LDAP アトリビュート マップ コンフィギュレーション モードに入ります。
2. LDAP アトリビュート マップ コンフィギュレーション モードで **map-name** コマンドおよび **map-value** コマンドを使用して、アトリビュート マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用して、LDAP サーバにアトリビュート マップをバインドします。このコマンドでは、「ldap」の後にハイフンを入力してください。

（注） アトリビュート マッピング機能を正しく使用するには、Cisco LDAP アトリビュートの名前と値、およびユーザ定義アトリビュートの名前と値を理解しておく必要があります。

例

次の例では、コマンドをグローバル コンフィギュレーション モードで入力し、myldapmap という名前の LDAP アトリビュート マップを作成してから、情報の入力、または LDAP サーバへのバインドを行います。

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP アトリビュート マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP アトリビュート名を、Cisco LDAP アトリビュート名にマッピングします。
map-value	ユーザ定義のアトリビュート値を、Cisco　アトリビュート名にマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP アトリビュート マップまたはすべての実行アトリビュート マップを表示します。
clear configure ldap attribute-map	すべての LDAP アトリビュート マップを削除します。

ldap-base-dn

認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-base-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除して、検索の開始位置をリストの先頭にリセットするには、このコマンドの **no** 形式を使用します。

ldap-base-dn *string*

no ldap-base-dn

シンタックスの説明

string	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定する最大 128 文字の文字列で、大文字と小文字が区別されます（たとえば、OU=Cisco）。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

デフォルト

検索はリストの先頭から開始されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	既存のコマンドです。このリリースで修正されました。

使用上のガイドライン

このコマンドは、LDAP サーバに対してのみ有効です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ベース DN を「starthere」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-base-dn starthere
hostname(config-aaa-server-host)# exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。

ldap-defaults

LDAP のデフォルト値を定義するには、crl 設定コンフィギュレーション モードで **ldap-defaults** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのデフォルト値は、LDAP サーバが必要とする場合にだけ使用されます。LDAP デフォルトを指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-defaults *server* [*port*]

no ldap-defaults

シンタックスの説明

port	（オプション）LDAP サーバ ポートを指定します。このパラメータが指定されていない場合、セキュリティ アプライアンスは標準の LDAP ポート（389）を使用します。
server	LDAP サーバの IP アドレスまたはドメイン名を指定します。CRL 配布ポイント内にサーバが存在する場合、この値はそのサーバによって上書きされます。

デフォルト

デフォルト値は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、デフォルト ポート（389）上で LDAP デフォルト値を定義します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-defaults ldapdomain4 8389
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol ldap	LDAP を CRL 取得方法として指定します。

ldap-dn

CRL の取得時に認証を要求する LDAP サーバに X.500 認定者名とパスワードを渡すには、crl 設定コンフィギュレーション モードで **ldap-dn** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバが必要とする場合にだけ使用されます。

LDAP DN を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-dn *x.500-name password*

no ldap-dn

シンタックスの説明

password	この認定者名のパスワードを定義します。フィールドの最大長は 128 文字です。
x.500-name	この CRL データベースにアクセスするためのディレクトリ パスを定義します（たとえば、cn=crl,ou=certs,o=CAName,c=US）。フィールドの最大長は 128 文字です。

デフォルト

デフォルト値は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
crl 設定コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、X.500 の名前に CN=admin,OU=devtest,O=engineering を指定し、central トラストポイントのパスワードに xxzzyy を指定します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードに入ります。
crypto ca trustpoint	CA トラストポイント コンフィギュレーション モードに入ります。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-login-dn

システムがバインドするディレクトリ オブジェクトの名前を指定するには、AAA サーバ ホスト モードで **ldap-login-dn** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-login-dn *string*

no ldap-login-dn

シンタックスの説明

string	LDAP 階層内のディレクトリ オブジェクトの名前を指定する最大 128 文字の文字列で、大文字と小文字が区別されます。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0 (1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、LDAP サーバに対してのみ有効です。サポートされる文字列の最大長は 128 文字です。

Microsoft Active Directory サーバなどの LDAP サーバでは、他のすべての LDAP 動作に関する要求を受け入れる前に、セキュリティ アプライアンスが認証済みバインディングを介してハンドシェイクを確立している必要があります。セキュリティ アプライアンスは、認証済みバインディングに対して識別情報を示すときに、ユーザ認証要求に Login DN フィールドを付加します。Login DN フィールドは、セキュリティ アプライアンスの認証特性を説明します。この特性は、管理者特権を持つユーザの特性に対応している必要があります。

string 変数には、VPN コンセントレータの認証済みバインディングに関するディレクトリ オブジェクトの名前を入力します（たとえば、cn=Administrator、cn=users、ou=people、dc=XYZ Corporation、dc=com）。匿名アクセスの場合、このフィールドはブランクのままにします。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ログイン DN を「myobjectname」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-login-dn myobjectname
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-login-password

LDAP サーバのログイン パスワードを指定するには、AAA サーバ ホスト モードで **ldap-login-password** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。このパスワード指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-login-password *string*

no ldap-login-password

シンタックスの説明

string	大文字と小文字が区別される最大 64 文字の英数字のパスワード。パスワードにスペースは使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、LDAP サーバに対してのみ有効です。パスワード文字列の最大長は 64 文字です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP ログイン パスワードを「obscurepassword」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server)# timeout 9
hostname(config-aaa-server)# retry 7
hostname(config-aaa-server)# ldap-login-password obscurepassword
hostname(config-aaa-server)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。

ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-naming-attribute

相対認定者名アトリビュートを指定するには、AAA サーバ ホスト モードで **ldap-naming-attribute** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-naming-attribute *string*

no ldap-naming-attribute

シンタックスの説明

string	LDAP サーバ上のエントリを一意に識別するための相対認定者名アトリビュートで、大文字と小文字が区別される最大 128 文字の英数字です。文字列にスペースは使用できませんが、その他の特殊文字は使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
aaa-server host	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュートを入力します。共通の命名アトリビュートは、通常名（cn）とユーザ ID（uid）です。

このコマンドは、LDAP サーバに対してのみ有効です。サポートされる文字列の最大長は 128 文字です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP 命名アトリビュートを「cn」として設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-naming-attribute cn
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-scope	認可要求を受信したときに、サーバが実行する LDAP 階層内検索の範囲を指定します。

ldap-over-ssl

セキュリティ アプライアンスと LDAP サーバの間にセキュアな SSL 接続を確立するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-over-ssl** コマンドを使用します。

接続に対して SSL をディセーブルにするには、このコマンドの **no** 形式を使用します。

ldap-over-ssl enable

no ldap-over-ssl enable

シンタックスの説明

enable	SSL により LDAP サーバへの接続が保護されることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、セキュリティ アプライアンスと LDAP サーバ間の接続を SSL で保護することを指定するために使用します。

（注） 平文認証を使用している場合は、この機能をイネーブルにすることを推奨します。**sasl-mechanism** コマンドを参照してください。

例

次のコマンドを、AAA サーバ ホスト コンフィギュレーション モードで入力して、セキュリティ アプライアンスと、IP アドレスが 10.10.0.1 の ldapsvr1 という LDAP サーバとの間の接続に対して SSL をイネーブルにします。また、PLAIN SASL 認証メカニズムも設定します。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# ldap-over-ssl enable
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
sasl-mechanism	LDAP クライアントとサーバの間に SASL 認証を指定します。
server-type	LDAP サーバのベンダーを Microsoft または Sun として指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。

ldap-scope

認可要求を受信したときに、サーバが検索する LDAP 階層内の範囲を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **ldap-scope** コマンドを使用します。AAA サーバ ホスト コンフィギュレーション モードには、AAA サーバ プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除するには、このコマンドの **no** 形式を使用します。

ldap-scope *scope*

no ldap-scope

シンタックスの説明

scope	認可要求を受信したときに、サーバが検索する LDAP 階層のレベル番号を指定します。有効値は、次のとおりです。 • ***onelevel***：ベース DN の 1 つ下のレベルのみを検索します。 • ***subtree***：ベース DN の下にあるすべてのレベルを検索します。

デフォルト

デフォルト値は、***onelevel*** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	既存のコマンドです。このリリースで修正されました。

使用上のガイドライン

スコープを ***onelevel*** として指定すると、検索速度が向上します。これは、ベース DN の 1 つ下のレベルだけが検索されるためです。***subtree*** を指定すると速度が低下します。これは、ベース DN の下にあるすべてのレベルが検索されるためです。

このコマンドは、LDAP サーバに対してのみ有効です。

例

次の例では、ホスト「1.2.3.4」上で「srvgrp1」という LDAP AAA サーバを設定し、タイムアウトを 9 秒に設定し、リトライ間隔を 7 秒に設定し、LDAP スコープがサブツリー レベルを含むように設定します。

```
hostname(config)# aaa-server svrgrp1 protocol ldap
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# ldap-scope subtree
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
ldap-base-dn	認可要求を受信したときに、サーバが検索を開始する LDAP 階層内の位置を指定します。
ldap-login-dn	ディレクトリ オブジェクトの名前を指定します。システムは、オブジェクトをこの名前でバインドします。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは、LDAP サーバに対してのみ有効です。
ldap-naming-attribute	LDAP サーバ上のエントリを一意に識別するための、相対認定者名アトリビュート（複数可）を指定します。

leap-bypass

LEAP Bypass をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **leap-bypass enable** コマンドを使用します。LEAP Bypass をディセーブルにするには、**leap-bypass disable** コマンドを使用します。LEAP Bypass アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、LEAP Bypass の値を別のグループ ポリシーから継承できます。

LEAP Bypass をイネーブルにすると、VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットが、ユーザ認証の前に VPN トンネルを通過できるようになります。これにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。確立後、ワークステーションはユーザごとの認証をもう一度実行します。

leap-bypass {**enable | disable**}

no leap-bypass

シンタックスの説明

disable	LEAP Bypass をディセーブルにします。
enable	LEAP Bypass をイネーブルにします。

デフォルト

LEAP Bypass はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

対話型のハードウェア クライアント認証がイネーブルになっていると、この機能は正常に動作しません。

詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

（注） 認証されていないトラフィックがトンネルを通過できるようにすると、セキュリティ リスクが生じる場合があります。

例

次の例は、「FirstGroup」というグループ ポリシーに LEAP Bypass を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# leap-bypass enable
```

関連コマンド

コマンド	説明
secure-unit-authentication	VPN ハードウェア クライアントがトンネルを開始するたびに、クライアントにユーザ名とパスワードによる認証を要求します。
user-authentication	VPN ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

lifetime

IKE セキュリティ アソシエーションの期限が切れるまでのライフタイムを指定するには、暗号 isakmp ポリシー コンフィギュレーション モードで **lifetime** コマンドを使用します。ピアがライフタイムを提示していなければ、無限のライフタイムを指定できます。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）にリセットするには、このコマンドの **no** 形式を使用します。

lifetime *seconds*

no lifetime

シンタックスの説明

priority	Internet Key Exchange（IKE）ポリシーを一意に識別し、そのポリシーに優先順位を割り当てます。1 ～ 65534 の整数を使用します。1 は優先順位が最も高く、65534 が最も低くなります。
seconds	各セキュリティ アソシエーションが期限満了するまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2,147,483,647 秒の整数を使用します。無限のライフタイムを提示するには、0 秒を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 isakmp ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	**isakmp policy lifetime** コマンドは既存のものです。
7.2.(1)	**isakmp policy lifetime** コマンドが、**lifetime** コマンドに置き換えられました。

使用上のガイドライン

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータを合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限満了するまで、セキュリティ アソシエーションを保持します。セキュリティ アソシエーションは、期限満了するまでその後の IKE ネゴシエーションで利用できるため、新しい IPSec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限満了する前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、セキュリティ アプライアンスで以降の IPSec セキュリティ アソシエーションを設定する時間が節約されます。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することをお勧めします。

（注） IKE セキュリティ アソシエーションが無限のライフタイムに設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからのネゴシエートされた有限のライフタイムが使用されます。

例

この例では、グローバル コンフィギュレーション モードで、優先順位番号 40 の IKE ポリシー内に IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# lifetime 50400
```

次の例では、グローバル コンフィギュレーション モードで、IKE セキュリティ アソシエーションを無限のライフタイムに設定します。

```
hostname(config)# crypto isakmp policy 40
hostname(config-isakmp-policy)# lifetime 0
```

関連コマンド

clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

limit-resource

マルチ コンテキスト モードでクラスにリソース制限を指定するには、クラス コンフィギュレーション モードで **limit-resource** コマンドを使用します。制限をデフォルトに戻すには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスでは、コンテキストをリソース クラスに割り当てることでリソースを管理します。各コンテキストは、クラスによって設定されるリソース制限値を使用します。

limit-resource {**all 0** | [**rate**] *resource_name number*[**%**]}

no limit-resource {**all** | [**rate**] *resource_name*}

シンタックスの説明

all 0	すべてのリソースに対して制限を無制限として設定します。
number[**%**]	リソース制限を 1 以上の固定数として指定します。あるいは、パーセント記号（%）を使用して、1 ～ 100 までのシステム制限のパーセンテージとして指定します。無制限のリソースを示す場合は、制限を **0** に設定します。システム制限を持たないリソースの場合はパーセンテージ（%）を設定できません。絶対値のみ設定できます。
rate	リソースに対して秒単位でレートを設定することを指定します。秒単位でレートを設定可能なリソースについては、表 18-1 を参照してください。
resource_name	制限を設定するリソース名を指定します。この制限は、**all** に設定されている制限を上書きします。

デフォルト

すべてのリソースは、次に示す制限を除いて無制限に設定されています。これらの制限は、デフォルトではコンテキストごとに許可される最上限に設定されています。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- IPSec セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

クラスに対してリソース制限を設定する場合、セキュリティ アプライアンスはクラスに割り当てられた各コンテキストにリソースの一部を確保するのではなく、セキュリティ アプライアンスはコンテキストに上限を設定します。リソースをオーバーサブスクライブした場合や、一部のリソースを無制限に許可した場合は、いくつかのコンテキストがそれらのリソースを使い果たして、他のコンテキストへのサービスに影響を及ぼす可能性があります。

表 18-1 には、リソースのタイプと制限がリストされています。**show resource types** コマンドも参照してください。

表 18-1　リソース名と制限

リソース名	レートまたは同時接続数	コンテキスト単位の最少数と最大数	システム制限[1]	説明
mac-addresses	同時接続数	該当なし	65,535	透過ファイアウォール モードで、MAC アドレス テーブルに含められる MAC アドレスの数。
conns	同時接続数またはレート	該当なし	同時接続数：プラットフォームの接続制限については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。 レート：該当なし	1 つのホストと複数の他のホストとの間の接続を含む、2 つのホスト間の TCP または UDP 接続。
inspects	比率	該当なし	該当なし	アプリケーション検査。
hosts	同時接続数	該当なし	該当なし	セキュリティ アプライアンスを通じて接続可能なホスト。
asdm	同時接続数	最小値：1 最大値：5	32	ASDM 管理セッション。 **(注)** ASDM セッションでは 2 つの HTTPS 接続が使用されます。1 つは常に必要な監視用、もう 1 つは変更を加えたときにのみ必要となる設定の変更用です。たとえば、ASDM セッションのシステム制限が 32 である場合は、HTTPS セッション数が 64 に制限されることを示します。
ssh	同時接続数	最小値：1 最大値：5	100	SSH セッション。
syslogs	比率	該当なし	該当なし	System ログ メッセージ。
telnet	同時接続数	最小値：1 最大値：5	100	Telnet セッション。
xlates	同時接続数	該当なし	該当なし	アドレス変換。

1. このカラム値が該当なしの場合、リソースにハード システム制限がないため、リソースのパーセンテージを設定できません。

例

次の例では、conns に関するデフォルト クラスの制限値を、無制限から 10% に設定し直しています。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

他のリソースは、すべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
member	リソース クラスにコンテキストを割り当てます。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

lmfactor

他のサーバによって設定された有効期限値ではなく、最後に変更されたタイムスタンプのみを持つオブジェクトをキャッシュするように再検証ポリシーを設定するには、キャッシュ モードで **lmfactor** コマンドを使用します。このようなオブジェクトを再検証するために新しいポリシーを設定するには、このコマンドを再度使用します。このアトリビュートをデフォルト値の 20 にリセットするには、このコマンドの **no** 形式を入力します。

lmfactor *value*

no lmfactor

シンタックスの説明

value	0 ～ 100 の範囲の整数。

デフォルト

デフォルト値は 20 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、lmfactor の値を使用して、キャッシュされたオブジェクトに変化がないと見なす時間の長さを推定します。これが有効期限として認識されます。セキュリティ アプライアンスは有効期限を、最後の変更から経過した時間に lmfactor を乗算して推定します。

lmfactor をゼロに設定すると、再検証をただちに強制することになります。またこれを 100 に設定すると、再検証が強制されるまでの許容時間が最長になります。

例

次の例は、lmfactor を 30 に設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# lmfactor 30
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシングをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

log

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラス コンフィギュレーション モードで **log** コマンドを使用して **match** コマンドまたはクラス マップに一致するパケットをログに記録します。このログ アクションは、アプリケーション トラフィックの検査ポリシー マップで使用できます（**policy-map type inspect** コマンド）。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

log

no log

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。**match** または **class** コマンドを入力してアプリケーション トラフィックを識別してから（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを指す）、**log** コマンドを入力し、**match** コマンドまたは **class** コマンドに一致するパケットをすべてログに記録します。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は検査ポリシー マップの名前です。

例

次の例では、パケットが http-traffic クラス マップに一致する場合にログを送信します。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

log-adj-changes

OSPF 隣接ルータがアップ状態またはダウン状態になると syslog メッセージを送信するようにルータを設定するには、ルータ コンフィギュレーション モードで **log-adj-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

log-adj-changes [***detail***]

no log-adj-changes [***detail***]

シンタックスの説明

detail	（オプション）隣接ルータがアップ状態またはダウン状態になるときだけでなく、状態が変化するたびに syslog メッセージを送信します。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

log-adj-changes コマンドは、デフォルトでイネーブルになっており、コマンドの **no** 形式を使用して削除しない限り、実行コンフィギュレーションに表示されます。

例

次の例では、OSPF 隣接ルータがアップ状態またはダウン状態になったときに syslog メッセージを送信しないようにします。

```
hostname(config)# router ospf 5
hostname(config-router)# no log-adj-changes
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

CHAPTER 19

logging asdm コマンド～ logout message コマンド

logging asdm

ASDM ログ バッファにシステム ログ メッセージを送信するには、グローバル コンフィギュレーション モードで **logging asdm** コマンドを使用します。ASDM ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging asdm [*logging_list* | *level*]

no logging asdm [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	ASDM ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

ASDM のロギングは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ	
				コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用して、ロギングをイネーブルにしておく必要があります。

ASDM のログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。ASDM のログ バッファに保持されるシステム ログ メッセージの数を制御するには、**logging asdm-buffer-size** コマンドを使用します。

ASDM のログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは別のバッファです。

例

次の例は、ロギングをイネーブルにして、ASDM ログ バッファに重大度 0、1、および 2 のメッセージを送信する方法を示しています。また、ASDM ログ バッファのサイズを 200 メッセージに設定する方法も示しています。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログ バッファが保持しているメッセージをすべて消去します。
logging asdm-buffer-size	ASDM ログ バッファに保持される ASDM メッセージの数を指定します。
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	ロギングのコンフィギュレーションを表示します。

logging asdm-buffer-size

ASDM のログ バッファに保持されるシステム ログ メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用します。ASDM ログ バッファをデフォルト サイズの 100 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging asdm-buffer-size *num_of_msgs*

no logging asdm-buffer-size *num_of_msgs*

シンタックスの説明

num_of_msgs	セキュリティ アプライアンスが ASDM ログ バッファに保持するシステム ログ メッセージの数を指定します。

デフォルト

デフォルトの ASDM syslog バッファ サイズは 100 メッセージです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM のログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。ASDM ログ バッファへのロギングをイネーブルにするかどうかを制御する場合や、ASDM ログ バッファに保持されるシステム ログ メッセージの種類を制御する場合は、**logging asdm** コマンドを使用します。

ASDM のログ バッファは、**logging buffered** コマンドでイネーブルにするログ バッファとは別のバッファです。

例

次の例は、ロギングをイネーブルにして、ASDM ログ バッファに重大度 0、1、および 2 のメッセージを送信する方法を示しています。また、ASDM ログ バッファのサイズを 200 メッセージに設定する方法も示しています。

```
hostname(config)# logging enable
hostname(config)# logging asdm 2
hostname(config)# logging asdm-buffer-size 200
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログ バッファが保持しているメッセージをすべて消去します。
logging asdm	ASDM ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging buffered

セキュリティ アプライアンスがシステム ログ メッセージをログ バッファに送信できるようにするには、グローバル コンフィギュレーション モードで **logging buffered** コマンドを使用します。ログ バッファへのロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging buffered [*logging_list* | *level*]

no logging buffered [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- バッファのサイズは 4 KB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ログ バッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

新しいメッセージは、バッファの最後に追加されます。バッファがいっぱいになると、セキュリティ アプライアンスはバッファを消去してから、メッセージの追加を続行します。ログ バッファがいっぱいである場合、セキュリティ アプライアンスは最も古いメッセージを削除して、新しいメッセージ用の空き領域をバッファ内に確保します。バッファの内容が「ラップ」されるたびにバッファの内容を自動的に保存することができます。これは、最後に保存されてから追加されたすべてのメッセージが新しいメッセージに置き換えられることを意味します。詳細については、**logging flash-bufferwrap** コマンドと **logging ftp-bufferwrap** コマンドを参照してください。

バッファの内容は、いつでもフラッシュ メモリに保存できます。詳細については、**logging savelog** コマンドを参照してください。

バッファに送信されたシステム ログ メッセージは、**show logging** コマンドで表示できます。

例

次の例では、レベル 0 およびレベル 1 のイベントに対して、バッファへのロギングを設定します。

```
hostname(config)# logging buffered alerts
hostname(config)#
```

次の例では、最大ロギング レベル 7 の notif-list というリストを作成し、notif-list リストで識別されるシステム ログ メッセージに対して、バッファへのロギングを設定します。

```
hostname(config)# logging list notif-list level 7
hostname(config)# logging buffered notif-list
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging buffer-size

ログ バッファのサイズを指定するには、グローバル コンフィギュレーション モードで **logging buffer-size** コマンドを使用します。ログ バッファをデフォルト サイズの 4 KB にリセットするには、このコマンドの **no** 形式を使用します。

logging buffer-size *bytes*

no logging buffer-size *bytes*

シンタックスの説明

bytes	ログ バッファに使用するメモリ量をバイト単位で設定します。たとえば、8,192 を指定した場合、セキュリティ アプライアンスはログ バッファに 8 KB のメモリを使用します。

デフォルト

ログ バッファのメモリ サイズは 4KB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスが使用しているログ バッファのサイズがデフォルトのバッファ サイズと異なっているかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging buffer-size** コマンドが表示されない場合、セキュリティ アプライアンスが使用するログ バッファのサイズは 4 KB です。

セキュリティ アプライアンスによるバッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次の例では、ロギングとロギング バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファ用に 16 KB のメモリを使用するように指定します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging buffer-size 16384
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging class

メッセージ クラスに対して、ロギング先ごとの最大ロギング レベルを設定するには、グローバル コンフィギュレーション モードで **logging class** コマンドを使用します。メッセージ クラスのロギング レベル コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

logging class *class destination level* [*destination level . . .*]

no logging class ***class***

シンタックスの説明

class	設定するロギング先ごとの最大ロギング レベルの対象となるメッセージ クラスを指定します。クラスの有効値については、後述する「使用上のガイドライン」の項を参照してください。
destination	*class*　に対してロギング先を指定します。このロギング先についての、*destination* に送信される最大ロギング レベルは、*level* によって決まります。*destination* の有効値については、後述する「使用上のガイドライン」の項を参照してください。
level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL

デフォルト

デフォルトでは、セキュリティ アプライアンスは、ロギング先およびメッセージ クラスごとにロギング レベルを適用しないようになっています。代わりに、イネーブルになっている各ロギング先は、ロギング リストで指定されたロギング レベル、またはロギング先をイネーブルにするときに指定されたレベルで、すべてのクラスに対するメッセージを受信します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　*class* の有効値は、次のとおりです。

- **auth**：ユーザ認証。
- **bridge**：透過ファイアウォール。
- **ca**：PKI 認証局。
- **config**：コマンド インターフェイス。
- **eap**：Extensible Authentication Protocol（EAP）。ネットワーク アドミッション コントロールをサポートするために、EAP セッションの状態変化、EAP ステータス クエリー イベント、および EAP ヘッダーとパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：Extensible Authentication Protocol（EAP）over UDP。ネットワーク アドミッション コントロールをサポートするための EAPoUDP イベントをログに記録し、EAPoUDP ヘッダーとパケット内容の完全なレコードを生成します。
- **email**：電子メール プロキシ。
- **ha**：フェールオーバー。
- **ids**：侵入検知システム。
- **ip**：IP スタック。
- **nac**：ネットワーク アドミッション コントロール。初期化、例外リスト一致、ACS トランザクション、クライアントレス認証、デフォルト ACL の適用、および再検証の各イベントをログに記録します。
- **np**：ネットワーク プロセッサ。
- **ospf**：OSPF ルーティング。
- **rip**：RIP ルーティング。
- **session**：ユーザ セッション。
- **snmp**：SNMP。
- **sys**：システム。
- **vpn**：IKE および IPSec。
- **vpnc**：VPN クライアント。
- **vpnfo**：VPN フェールオーバー。
- **vpnlb**：VPN ロード バランシング。

有効なロギング先は、次のとおりです。

- **asdm**：このロギング先については、**logging asdm** コマンドを参照してください。
- **buffered**：このロギング先については、**logging buffered** コマンドを参照してください。
- **console**：このロギング先については、**logging console** コマンドを参照してください。
- **history**：このロギング先については、**logging history** コマンドを参照してください。
- **mail**：このロギング先については、**logging mail** コマンドを参照してください。
- **monitor**：このロギング先については、**logging monitor** コマンドを参照してください。
- **trap**：このロギング先については、**logging trap** コマンドを参照してください。

例　次の例では、フェールオーバー関連のメッセージに対して、ASDM ログ バッファの最大ロギング レベルが 2 で、システム ログ バッファの最大ロギング レベルが 7 であることを指定します。

```
hostname(config)# logging class ha asdm 2 buffered 7
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging console

セキュリティ アプライアンスがシステム ログ メッセージをコンソール セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。システム ログ メッセージをコンソール セッションに表示しないようにするには、このコマンドの **no** 形式を使用します。

logging console [*logging_list* | *level*]

no logging console

（注） このコマンドを使用すると、バッファ オーバーフローによって多数のシステム ログ メッセージがドロップされる可能性があるため、このコマンドの使用はお勧めできません。詳細については、後述する「使用上のガイドライン」の項を参照してください。

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	コンソール セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、システム ログ メッセージをコンソール セッションに表示しません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　コンソールにメッセージが送信される前に、**logging enable** コマンドを使用してロギングをイネーブルにしておく必要があります。

注意　**logging console** コマンドを使用すると、システム パフォーマンスが大幅に低下する可能性があります。代わりに、**logging buffered** を使用してロギングを開始し、**show logging** コマンドを使用してメッセージを表示してください。最新のメッセージをより簡単に表示するには、**clear logging** ***buffer*** コマンドを使用してバッファを消去します。

例　次の例は、レベル 0、1、2、および 3 のシステム ログ メッセージをコンソール セッションに表示できるようにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging console errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging debug-trace

デバッグ メッセージを、重大度 7 で発行された syslog メッセージ 711001 としてログにリダイレクトするには、グローバル コンフィギュレーション モードで **logging debug-trace** コマンドを使用します。ログへのデバッグ メッセージの送信を停止するには、このコマンドの **no** 形式を使用します。

logging debug-trace

no logging debug-trace

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはデバッグ出力をシステム ログ メッセージに含めません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

デバッグ メッセージは、重大度 7 のメッセージとして生成されます。このメッセージは、syslog メッセージ番号 711001 と一緒にログに表示されます。

例

次の例は、ロギングをイネーブルにし、ログ メッセージをシステム ログ バッファに送信し、デバッグ出力をログにリダイレクトし、ディスク アクティビティのデバッグをオンにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging debug-trace
hostname(config)# debug disk filesystem
```

ログに表示できるデバッグ メッセージの例を次に示します。

```
%PIX-7-711001: IFS: Read: fd 3, bytes 4096
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging device-id

EMBLEM 形式でないシステム ログ メッセージにデバイス ID を含めるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **logging device-id** コマンドを使用します。デバイス ID の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging device-id {***context-name*** | ***hostname*** | ***ipaddress*** *interface_name* | ***string*** *text*}

no logging device-id {***context-name*** | ***hostname*** | ***ipaddress*** *interface_name* | ***string*** *text*}

シンタックスの説明

context-name	デバイス ID として、現在のコンテキストの名前を使用します。
hostname	デバイス ID として、セキュリティ アプライアンスのホスト名を使用します。
ipaddress *interface_name*	デバイス ID として、*interface_name* で指定されたインターフェイスの IP アドレスを使用します。**ipaddress** キーワードを使用すると、セキュリティ アプライアンスがログ データを外部サーバに送信するために使用するインターフェイスに関係なく、外部サーバに送信されるシステム ログ メッセージに、指定されたインターフェイスの IP アドレスが含まれます。
string *text*	デバイス ID として、*text* に含まれている最大 16 文字の文字を使用します。*text* にスペースや次の文字は使用できません。 • &：アンパサンド • '：一重引用符 • "：二重引用符 • <：小なり • >：大なり • ?：疑問符

デフォルト

システム ログ メッセージにデフォルトのデバイス ID は使用されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ipaddress キーワードを使用すると、デバイス ID は、メッセージが送信されたインターフェイスに関係なく、指定したセキュリティ アプライアンス インターフェイスの IP アドレスとなります。このキーワードの使用により、そのデバイスから送信されるメッセージすべてに、1 つの同じデバイス ID が割り当てられます。

例

次の例は、secappl-1 というホストを設定する方法を示しています。

```
hostname(config)# logging device-id hostname
hostname(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

syslog メッセージでは、ホスト名 secappl-1 はメッセージの先頭に表示されます。メッセージの例を次に示します。

```
secappl-1 %PIX-5-111008: User 'enable_15' executed the 'logging buffer-size 4096'
command.
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging emblem

syslog サーバ以外のロギング先に送信されるシステム ログ メッセージに EMBLEM 形式を使用するには、グローバル コンフィギュレーション モードで **logging emblem** コマンドを使用します。EMBLEM 形式の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

logging emblem

no logging emblem

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、セキュリティ アプライアンスはシステム ログ メッセージに EMBLEM 形式を使用しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが **logging host** コマンドと無関係になるように変更されました。

使用上のガイドライン

logging emblem コマンドを使用すると、syslog サーバを除くすべてのロギング先に対して、EMBLEM 形式のロギングをイネーブルにできます。**logging timestamp** キーワードもイネーブルにすると、タイムスタンプ付きのメッセージが送信されます。

syslog サーバに対して EMBLEM 形式のロギングをイネーブルにするには、**logging host** コマンドに ***format emblem*** オプションを使用します。

例

次の例は、ロギングをイネーブルにし、syslog サーバを除くすべてのロギング先へのロギングに対して、EMBLEM 形式の使用をイネーブルにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging emblem
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging enable

設定済みの出力場所すべてに対してロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **logging enable** コマンドを使用します。ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging enable

no logging enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

ロギングは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが **logging on** コマンドから変更されました。

使用上のガイドライン

logging enable コマンドを使用すると、サポートされている任意のロギング先に対するシステム ログ メッセージの送信をイネーブルまたはディセーブルにできます。すべてのロギングを停止するには、**no logging enable** コマンドを使用します。

個別のロギング先へのロギングをイネーブルにするには、次のコマンドを使用します。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

例

次の例は、ロギングをイネーブルにする方法を示しています。**show logging** コマンドの出力は、使用可能な各ロギング先を個別にイネーブルにする必要がある状況を示しています。

```
hostname(config)# logging enable
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging facility

syslog サーバに送信されるメッセージに使用するロギング ファシリティを指定するには、グローバル コンフィギュレーション モードで **logging facility** コマンドを使用します。ロギング ファシリティをデフォルトの 20 にリセットするには、このコマンドの **no** 形式を使用します。

logging facility *facility*

no logging facility

シンタックスの説明

facility	syslog ファシリティを指定します。有効値は 16 ～ 23 です。

デフォルト

デフォルト ファシリティは 20（LOCAL4）です。

コマンド モード

次の表は、コマンドを入力できるモードを示しています。例外については、上記の「シンタックスの説明」の項を参照してください。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

syslog サーバは、メッセージの *facility* 番号をもとに、メッセージをファイルします。使用可能なファシリティには、16（LOCAL0）～ 23（LOCAL7）の 8 つがあります。

例

次の例は、セキュリティ アプライアンスがロギング ファシリティを 16 としてシステム ログ メッセージに指定するように設定する方法を示しています。**show logging** コマンドの出力には、セキュリティ アプライアンスによって使用されているファシリティが含まれます。

```
hostname(config)# logging facility 16
hostname(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: level errors, facility 16, 3607 messages logged
        Logging to infrastructure 10.1.2.3
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging flash-bufferwrap

バッファが未保存のメッセージでいっぱいになるたびに、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにするには、グローバル コンフィギュレーション モードで **logging flash-bufferwrap** コマンドを使用します。ログ バッファをフラッシュ メモリに書き込めないようにするには、このコマンドの **no** 形式を使用します。

logging flash-bufferwrap

no logging flash-bufferwrap

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- フラッシュ メモリへのログ バッファの書き込みはディセーブルです。
- バッファのサイズは 4 KB です。
- フラッシュ メモリの最小空き容量は 3 MB です。
- バッファ ロギング用のフラッシュ メモリ最大割当量は、1 MB です。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにするには、バッファへのロギングをイネーブルにする必要があります。このようにしないと、フラッシュ メモリに書き込むデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスは、ログ バッファの内容をフラッシュ メモリに書き込む間も、新しいイベント メッセージをログ バッファに継続的に格納します。

セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用した名前でログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

フラッシュ メモリの可用性により、セキュリティ アプライアンスが **logging flash-bufferwrap** コマンドを使用してシステム ログ メッセージを保存するときの方法が異なります。詳細については、**logging flash-maximum-allocation** コマンドと **logging flash-minimum-free** コマンドを参照してください。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにする方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
copy	ファイルを、ある位置から TFTP サーバや FTP サーバなどの別の位置にコピーします。
delete	保存済みログ ファイルなどのファイルを、ディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging flash-maximum-allocation	フラッシュ メモリについて、ログ バッファの内容を書き込むために使用できる最大量を指定します。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するときに、セキュリティ アプライアンスが使用できるようにしておく必要のある最小限のフラッシュ メモリ量を指定します。
show logging	イネーブルなロギング オプションを表示します。

logging flash-maximum-allocation

セキュリティ アプライアンスがログ データの格納に使用するフラッシュ メモリの最大量を指定するには、グローバル コンフィギュレーション モードで **logging flash-maximum-allocation** コマンドを使用します。このコマンドにより、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで使用できるフラッシュ メモリの最大量が決まります。この用途に使用するフラッシュ メモリの最大量をデフォルト サイズの 1 MB にリセットするには、このコマンドの **no** 形式を使用します。

logging flash-maximum-allocation *kbytes*

no logging flash-maximum-allocation *kbytes*

シンタックスの説明

kbytes	セキュリティ アプライアンスがログ バッファ データの保存に使用できるフラッシュ メモリの最大量（KB 単位）。

デフォルト

ログ データ用のデフォルトのフラッシュ メモリ最大割当量は、1 MB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

logging savelog または **logging flash-bufferwrap** によって保存されるログ ファイルが原因で、ログ ファイル用のフラッシュ メモリの使用量が、**logging flash-maximum-allocation** コマンドで指定された最大量を超える場合、セキュリティ アプライアンスは最も古いログ ファイルを削除して、新しいログ ファイル用に十分な量のメモリを開放します。削除するファイルがない場合や、古いファイルをすべて削除してもメモリの空き容量が新しいログ ファイル用には小さすぎる場合、セキュリティ アプライアンスは新しいログ ファイルを保存できません。

セキュリティ アプライアンスによるフラッシュ メモリの最大割当量がデフォルト サイズと異なっているかどうかを確認するには、**show running-config logging** コマンドを使用します。**logging flash-maximum-allocation** コマンドが表示されない場合、セキュリティ アプライアンスがログ バッファ データの保存に使用する最大サイズは 1 MB です。割り当てられたメモリは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドの両方に使用されます。

セキュリティ アプライアンスによるログ バッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにし、ログ ファイルの書き込みに使用するフラッシュ メモリの最大量を約 1.2 MB に設定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-maximum-allocation 1200
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-minimum-free	フラッシュ メモリへのログ バッファの書き込みを許可するときに、セキュリティ アプライアンスが使用できるようにしておく必要のある最小限のフラッシュ メモリ量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging flash-minimum-free

セキュリティ アプライアンスが新しいログ ファイルを保存する前に確保しておく必要のあるフラッシュ メモリの最小空き容量を指定するには、グローバル コンフィギュレーション モードで **logging flash-minimum-free** コマンドを使用します。このコマンドは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで作成されたログ ファイルをセキュリティ アプライアンスが保存する前に確保しておく必要のあるフラッシュ メモリの空き容量に影響を及ぼします。フラッシュ メモリの必要最小限の空き容量をデフォルト サイズの 3 MB にリセットするには、このコマンドの **no** 形式を使用します。

logging flash-minimum-free *kbytes*

no logging flash-minimum-free *kbytes*

シンタックスの説明

kbytes	セキュリティ アプライアンスが新しいログ ファイルを保存する前に使用可能にしておく必要のあるフラッシュ メモリの最小量（KB 単位）。

デフォルト

デフォルトのフラッシュ メモリの最小空き容量は 3 MB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

logging flash-minimum-free コマンドは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンド用に常に確保しておく必要のあるフラッシュ メモリ量を指定します。

logging savelog または **logging flash-bufferwrap** によって保存されるログ ファイルが原因で、フラッシュ メモリの空き容量が、**logging flash-minimum-free** コマンドで指定された限度を下回る場合、セキュリティ アプライアンスは最も古いログ ファイルを削除して、新しいログ ファイルの保存後もメモリの最小空き容量が保持されることを保証します。削除するファイルがない場合や、古いファイルをすべて削除してもメモリの空き容量が限度を下回る場合、セキュリティ アプライアンスは新しいログ ファイルを保存できません。

例

次の例は、ロギングとログ バッファをイネーブルにし、セキュリティ アプライアンスがログ バッファをフラッシュ メモリに書き込めるようにし、フラッシュ メモリの最小空き容量を 4,000 KB にする必要があることを指定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging flash-bufferwrap
hostname(config)# logging flash-minimum-free 4000
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファをフラッシュ メモリに書き込みます。
logging flash-maximum-allocation	フラッシュ メモリについて、ログ バッファの内容を書き込むために使用できる最大量を指定します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging from-address

セキュリティ アプライアンスによって電子メールで送信されるシステム ログ メッセージの送信者の電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging from-address** コマンドを使用します。電子メールで送信されるシステム ログ メッセージはすべて、指定したアドレスから送信されたように表示されます。送信者の電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。

logging from-address *from-email-address*

no logging from-address *from-email-address*

シンタックスの説明

from-email-address	送信元の電子メール アドレス（syslog 電子メールの送信元として表示される電子メール アドレス）。たとえば、cdb@example.com です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

システム ログ メッセージを電子メールで送信できるようにするには、**logging mail** コマンドを使用します。

このコマンドで指定するアドレスは、既存の電子メール アカウントに対応している必要はありません。

例

次の基準に従って、ロギングをイネーブルにし、システム ログ メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging enable
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging mail	セキュリティ アプライアンスがシステム ログ メッセージを電子メールで送信できるようにし、どのメッセージを電子メールで送信するかを決定します。
logging recipient-address	電子メールで送信されるシステム ログ メッセージの送信先となる電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging ftp-bufferwrap

バッファが未保存のメッセージでいっぱいになるたびに、セキュリティ アプライアンスがログ バッファを FTP サーバに送信できるようにするには、グローバル コンフィギュレーション モードで **logging ftp-bufferwrap** コマンドを使用します。ログ バッファを FTP サーバに送信しないようにするには、このコマンドの **no** 形式を使用します。

logging ftp-bufferwrap

no logging ftp-bufferwrap

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトは次のとおりです。

- バッファへのロギングはディセーブルです。
- FTP サーバへのログ バッファの送信はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

logging ftp-bufferwrap がイネーブルの場合、セキュリティ アプライアンスは、**logging ftp-server** コマンドで指定された FTP サーバにログ バッファ データを送信します。セキュリティ アプライアンスは、ログ データを FTP サーバに送信する間も、新しいイベント メッセージをログ バッファに継続的に格納します。

セキュリティ アプライアンスがログ バッファの内容を FTP サーバに送信できるようにするには、バッファへのロギングをイネーブルにする必要があります。このようにしないと、フラッシュ メモリに書き込むデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用した名前でログ ファイルを作成します。

LOG-*YYYY-MM-DD-HHMMSS*.TXT

YYYY は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

例

次の例は、ロギングとログ バッファをイネーブルにし、FTP サーバを指定し、セキュリティ アプライアンスがログ バッファを FTP サーバに書き込めるようにする方法を示しています。この例では、logserver-352 というホスト名の FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs を使用してアクセスできます。ログ ファイルは、/syslogs ディレクトリに保存されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-server	**logging ftp-bufferwrap** コマンドで使用する FTP サーバ パラメータを指定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging ftp-server

logging ftp-bufferwrap がイネーブルの場合にセキュリティ アプライアンスがログ バッファ データを送信する FTP サーバについての詳細を指定するには、グローバル コンフィギュレーション モードで **logging ftp-server** コマンドを使用します。FTP サーバについての詳細をすべて削除するには、このコマンドの **no** 形式を使用します。

logging ftp-server *ftp-server ftp_server path username password*

no logging ftp-server *ftp-server ftp_server path username password*

シンタックスの説明

ftp-server	外部 FTP サーバの IP アドレスまたはホスト名。 **(注)** ホスト名を指定する場合は、ネットワーク上で DNS が正しく動作していることを確認してください。
path	ログ バッファ データの保存先となる FTP サーバ上のディレクトリ パス。このパスは、FTP ルート ディレクトリに対する相対パスです。次の例を参考にしてください。 `/security_appliances/syslogs/appliance107`
username	FTP サーバへのロギングに有効なユーザ名。
password	指定したユーザ名に対応するパスワード。

デフォルト

FTP サーバは、デフォルトでは指定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

指定できる FTP サーバは 1 つのみです。ロギング FTP サーバがすでに指定されている場合、**logging ftp-server** コマンドを使用すると、その FTP サーバ コンフィギュレーションが、入力した新しいコンフィギュレーションに置き換えられます。

セキュリティ アプライアンスは、指定された FTP サーバ情報を確認しません。詳細を誤って設定した場合、セキュリティ アプライアンスはログ バッファ データを FTP サーバに送信できません。

例

次の例は、ロギングとログ バッファをイネーブルにし、FTP サーバを指定し、セキュリティ アプライアンスがログ バッファを FTP サーバに書き込めるようにする方法を示しています。この例では、logserver-352 というホスト名の FTP サーバを指定しています。このサーバには、ユーザ名 logsupervisor とパスワード 1luvMy10gs を使用してアクセスできます。ログ ファイルは、/syslogs ディレクトリに保存されます。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
hostname(config)# logging ftp-bufferwrap
hostname(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファのサイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバに送信します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging history

SNMP ロギングをイネーブルにし、SNMP サーバに送信されるメッセージを指定するには、グローバル コンフィギュレーション モードで **logging history** コマンドを使用します。SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging history [*logging_list* | *level*]

no logging history

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	SNMP サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは SNMP サーバにロギングしません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

logging history コマンドを使用すると、SNMP サーバへのロギングをイネーブルにし、SNMP メッセージ レベルまたはイベント リストを設定することができます。

例

次の例は、SNMP ロギングをイネーブルにし、レベル 0、1、2、および 3 のメッセージが設定済みの SNMP サーバに送信されるよう指定する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
hostname(config)# snmp-server enable traps syslog
hostname(config)# logging history errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。
snmp-server	SNMP サーバの詳細を指定します。

logging host

syslog サーバを定義するには、グローバル コンフィギュレーション モードで **logging host** コマンドを使用します。syslog サーバの定義を削除するには、このコマンドの **no** 形式を使用します。

logging host *interface_name syslog_ip* [***tcp****/port* | ***udp****/port*] [**format emblem**]

logging host *interface_name syslog_ip*

シンタックスの説明

format emblem	（オプション）syslog サーバに対して EMBLEM 形式のロギングをイネーブルにします。
interface_name	syslog サーバが常駐するインターフェイス。
syslog_ip	syslog サーバの IP アドレス。
tcp	メッセージを syslog サーバに送信するときに、セキュリティ アプライアンスが TCP を使用することを指定します。
udp	メッセージを syslog サーバに送信するときに、セキュリティ アプライアンスが TCP を使用することを指定します。
port	syslog サーバがメッセージをリッスンするポート。有効となるポート値の範囲は、どちらのプロトコルの場合も 1025 ～ 65535 です。

デフォルト

デフォルトは次のとおりです。

- デフォルトのポート番号は次のとおりです。
  - UDP ポートは 514
  - TCP ポートは 1470
- デフォルト プロトコルは UDP です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

logging host *ip_address* **format emblem** コマンドを使用すると、各 syslog サーバに対して EMBLEM 形式のロギングをイネーブルにできます。EMBLEM 形式のロギングは、UDP システム ログ メッセージに対してだけ利用できます。EMBLEM 形式のロギングを特定の syslog ホストに対してイネーブルにすると、メッセージがそのホストに送信されます。**logging timestamp** キーワードもイネーブルにすると、タイムスタンプ付きのメッセージが送信されます。

複数の **logging host** コマンドを使用して複数の追加サーバを指定すると、追加したサーバすべてがシステム ログ メッセージを受信します。ただし、サーバは UDP か TCP のどちらか一方を受信するように指定でき、両方を受信するようには指定できません。

(注)　*tcp* オプションが **logging host** コマンドで使用されている場合、syslog サーバに到達できないと、セキュリティ アプライアンスはファイアウォールを越える接続をドロップします。

以前入力した *port* と *protocol* の値のみを表示するには、**show running-config logging** コマンドを使用して、リストでコマンドを見つけます（TCP プロトコルは 6、UDP プロトコルは 17 として示されます）。TCP ポートは、セキュリティ アプライアンス syslog サーバに対してのみ動作します。*port* は、syslog サーバがリッスンするポートと一致している必要があります。

例

次の例は、内部インターフェイス上にあってデフォルトのプロトコルとポート番号を使用する syslog サーバに対して、レベル 0、1、2、および 3 のシステム ログ メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging list

各種の基準（ロギング レベル、イベント クラス、およびメッセージ ID）でメッセージを指定するため、他のコマンドで使用するロギング リストを作成するには、グローバル コンフィギュレーション モードで **logging list** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

logging list *name* {**level** *level* [**class** *event_class*] | **message** *start_id*[*-end_id*]}

no logging list *name*

シンタックスの説明

class *event_class*	（オプション）システム ログ メッセージのイベント クラスを設定します。指定されたレベルに対応する、指定されたクラスのシステム ログ メッセージのみが、コマンドによって特定されます。クラスのリストについては、「使用上のガイドライン」を参照してください。
level *level*	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
message *start_id*[*-end_id*]	メッセージ ID または ID の範囲を指定します。メッセージのデフォルト レベルを確認するには、**show logging** コマンドを使用するか、『*Cisco Security Appliance System Log Messages*』を参照してください。
name	ロギング リストの名前を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドがサポートされるようになりました。

使用上のガイドライン　リストを使用できるロギング コマンドは、次のとおりです。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

event_class に指定できる値は、次のとおりです。

- **auth**：ユーザ認証。
- **bridge**：透過ファイアウォール。
- **ca**：PKI 認証局。
- **config**：コマンド インターフェイス。
- **eap**：Extensible Authentication Protocol（EAP）。ネットワーク アドミッション コントロールをサポートするために、EAP セッションの状態変化、EAP ステータス クエリー イベント、および EAP ヘッダーとパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：Extensible Authentication Protocol（EAP）over UDP。ネットワーク アドミッション コントロールをサポートするための EAPoUDP イベントをログに記録し、EAPoUDP ヘッダーとパケット内容の完全なレコードを生成します。
- **email**：電子メール プロキシ。
- **ha**：フェールオーバー。
- **ids**：侵入検知システム。
- **ip**：IP スタック。
- **nac**：ネットワーク アドミッション コントロール。初期化、例外リスト一致、ACS トランザクション、クライアントレス認証、デフォルト ACL の適用、および再検証の各イベントをログに記録します。
- **np**：ネットワーク プロセッサ。
- **ospf**：OSPF ルーティング。
- **rip**：RIP ルーティング。
- **session**：ユーザ セッション。
- **snmp**：SNMP。
- **sys**：システム。
- **vpn**：IKE および IPSec。
- **vpnc**：VPN クライアント。
- **vpnfo**：VPN フェールオーバー。
- **vpnlb**：VPN ロード バランシング。

例　次の例は、logging list コマンドを使用する方法を示しています。

```
hostname(config)# logging list my-list 100100-100110
hostname(config)# logging list my-list level critical
hostname(config)# logging list my-list level warning class vpn
hostname(config)# logging buffered my-list
```

上記の例は、指定された基準に一致するシステム ログ メッセージがロギング バッファに送信されることを示しています。この例で指定されている基準は、次のとおりです。

1. 100100 ～ 100110 の範囲内にあるシステム ログ メッセージ ID
2. critical レベル以上（emergency、alert、または critical）にあるすべてのシステム ログ メッセージ
3. warning レベル以上（emergency、alert、critical、error、または warning）にある VPN クラスのすべてのシステム ログ メッセージ

システム ログ メッセージがこれらの条件のいずれかを満たしている場合、そのメッセージはバッファにロギングされます。

（注） リストの基準を設計する場合、メッセージを重複して指定する基準にしてもかまいません。複数の基準に一致するシステム ログ メッセージも正常にロギングされます。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging mail

セキュリティ アプライアンスがシステム ログ メッセージを電子メールで送信したり、電子メールで送信するメッセージを判別したりできるようにするには、グローバル コンフィギュレーション モードで **logging mail** コマンドを使用します。システム ログ メッセージを電子メールで送信しないようにするには、このコマンドの **no** 形式を使用します。

logging mail [*logging_list* | *level*]

no logging mail [*logging_list* | *level*]

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	電子メールの受信者に送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

電子メールへのロギングは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

電子メールで送信されたシステム ログ メッセージは、送信済み電子メールの件名欄に表示されます。

例

次の基準に従って、システム ログ メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	電子メールで送信されるシステム ログ メッセージの送信元として表示する電子メール アドレスを指定します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
logging recipient-address	電子メールで送信されるシステム ログ メッセージの送信先となる電子メール アドレスを指定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging message

システム ログ メッセージのロギング レベルを指定するには、グローバル コンフィギュレーション モードで **logging message** コマンドを ***level*** キーワードと組み合せて使用します。メッセージのロギング レベルをデフォルト レベルにリセットするには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスが特定のシステム ログ メッセージを生成しないようにするには、グローバル コンフィギュレーション モードで **logging message** コマンドの **no** 形式を使用します（***level*** キーワードは指定しません）。セキュリティ アプライアンスが特定のシステム ログ メッセージを生成できるようにするには、**logging message** コマンドを使用します（***level*** キーワードは指定しません）。これら 2 つの用途の **logging message** コマンドは、並行して実行できます。後述する「例」の項を参照してください。

logging message *syslog_id* **level** *level*

no logging message *syslog_id* **level** *level*

logging message *syslog_id*

no logging message *syslog_id*

シンタックスの説明

level *level*	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
syslog_id	イネーブルまたはディセーブルにするシステム ログ メッセージ、または重大度を変更するシステム ログ メッセージの ID。メッセージのデフォルト レベルを確認するには、**show logging** コマンドを使用するか、『*Cisco Security Appliance System Log Messages*』を参照してください。

デフォルト

デフォルトでは、システム ログ メッセージはすべてイネーブルになっており、すべてのメッセージの重大度はデフォルト レベルに設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

logging message コマンドは、次の 2 つの用途に使用できます。

- メッセージをイネーブルとディセーブルのどちらにするかを制御する。
- メッセージの重大度を制御する。

メッセージに現在割り当てられているレベルや、メッセージがイネーブルになっているかどうかを判別するには、**show logging** コマンドを使用します。

例

次の例にある一連のコマンドは、**logging message** コマンドを使用して、メッセージをイネーブルにするかどうか、およびメッセージの重大度の両方を制御する方法を示しています。

```
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)

hostname(config)# logging message 403503 level 1
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (disabled)

hostname(config)# logging message 403503
hostname(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)

hostname(config)# no logging message 403503 level 3
hostname(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

関連コマンド

コマンド	説明
clear configure logging	ロギング コンフィギュレーションすべてまたはメッセージ コンフィギュレーションのみを消去します。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging monitor

セキュリティ アプライアンスがシステム ログ メッセージを SSH および Telnet セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging monitor** コマンドを使用します。システム ログ メッセージを SSH および Telnet セッションに表示しないようにするには、このコマンドの **no** 形式を使用します。

logging monitor [*logging_list* | *level*]

no logging monitor

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	SSH または Telnet セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、システム ログ メッセージを SSH および Telnet セッションに表示しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

logging monitor コマンドを使用すると、現在のコンテキスト内のセッションすべてに対してシステム ログ メッセージをイネーブルにできます。ただし、セッションにシステム ログ メッセージを表示するかどうかは、セッションごとに **terminal** コマンドで制御します。

例

次の例は、システム ログ メッセージをコンソール セッションに表示できるようにする方法を示しています。***errors*** キーワードを使用することは、レベル 0、1、2、および 3 のメッセージを SSH および Telnet セッションに表示する必要があることを示しています。**terminal** コマンドを使用すると、現在のセッションにメッセージを表示できます。

```
hostname(config)# logging enable
hostname(config)# logging monitor errors
hostname(config)# terminal monitor
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。
terminal	端末回線のパラメータを設定します。

logging permit-hostdown

TCP ベースの syslog サーバの状態が新しいユーザ セッションとは無関係になるように指定するには、グローバル コンフィギュレーション モードで **logging permit-hostdown** コマンドを使用します。TCP ベースの syslog サーバが使用不能のときにセキュリティ アプライアンスが新しいユーザ セッションを拒否するように設定するには、このコマンドの **no** 形式を使用します。

logging permit-hostdown

no logging permit-hostdown

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、TCP 接続を使用する syslog サーバへのロギングをイネーブルにした場合、何らかの理由で syslog サーバが使用不能になったときは、セキュリティ アプライアンスは新しいネットワーク アクセス セッションを許可しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1) (1)	このコマンドが導入されました。

使用上のガイドライン

syslog サーバにメッセージを送信するためのロギング転送プロトコルとして TCP を使用する場合、セキュリティ アプライアンスは、syslog サーバに到達できないときは、セキュリティ保護手段として、新しいネットワーク アクセス セッションを拒否します。この制限を削除するには、**logging permit-hostdown** コマンドを使用します。

例

次の例では、TCP ベースの syslog サーバの状態が、セキュリティ アプライアンスが新しいセッションを許可するかどうかとは無関係になるように指定します。show running-config logging コマンドの出力に show running-config logging コマンドが含まれている場合、TCP ベースの syslog サーバの状態は新しいネットワーク アクセス セッションとは無関係になっています。

```
hostname(config)# logging permit-hostdown
hostname(config)# show running-config logging
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging trap	syslog サーバへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging queue

セキュリティ アプライアンスがロギング コンフィギュレーションに従って処理する前にシステム ログ メッセージ キューに保持できるシステム ログ メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging queue** コマンドを使用します。ロギング キューのサイズをデフォルトの 512 メッセージにリセットするには、このコマンドの **no** 形式を使用します。

logging queue *queue_size*

no logging queue *queue_size*

シンタックスの説明

queue_size	処理前に格納するためのキューに入れることができるシステム ログ メッセージの数。有効な値は 0 ～ 8,192 メッセージです。ロギング キューが 0 に設定されている場合、キューは設定可能な最大サイズ（8192 メッセージ）になります。

デフォルト

デフォルトのキュー サイズは 512 メッセージです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

トラフィックが重いためにキューがいっぱいになった場合、セキュリティ アプライアンスはメッセージを廃棄することがあります。

例

次の例は、**logging queue** コマンドと **show logging queue** コマンドの出力を表示する方法を示しています。

```
hostname(config)# logging queue 0
hostname(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

この例では、**logging queue** コマンドは 0 に設定されています。つまり、キューは最大サイズの 8192 に設定されています。キュー内のシステム ログ メッセージは、セキュリティ アプライアンスによって、ロギング コンフィギュレーションで指定される方法で処理されます。たとえば、システム ログ メッセージを電子メール受信者に送信する方法やフラッシュ メモリに保存する方法などがあります。

この例における **show logging queue** コマンドの出力は、キューにあるメッセージが 5 つ、セキュリティ アプライアンスが最後にブートされてから同時にキューに存在したメッセージの最大数が 3,513、廃棄されたメッセージが 1 つであることを表示しています。キューは無制限になるように設定されていましたが、メッセージをキューに追加するためのブロック メモリが使用できなかったため、メッセージは廃棄されました。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging rate-limit

システム ログ メッセージの生成レートを制限するには、特権 EXEC モードで **logging rate-limit** コマンドを使用します。レート制限をディセーブルにするには、特権 EXEC モードでこのコマンドの **no** 形式を使用します。

logging rate-limit {***unlimited*** | {*num* [*interval*]}} ***message*** *syslog_id* | ***level*** *severity_level*

[no] logging rate-limit [***unlimited*** | {*num* [*interval*]}} ***message*** *syslog_id*] ***level*** *severity_level*

シンタックスの説明

interval	（オプション）メッセージの生成レートの測定に使用される時間間隔（秒単位）。*interval* の有効値の範囲は 0 ～ 2,147,483,647 です。
level *severity_level*	設定されたレート制限を、特定の重大度に属するすべてのシステム ログ メッセージに適用します。指定された重大度のすべてのシステム ログ メッセージは、個別にレート制限されます。*severity_level* の有効な範囲は 1 ～ 7 です。
message	このシステム ログ メッセージのレポートを抑制します。
num	指定した時間間隔が経過するまでに生成できるシステム メッセージの数。*num* の有効値の範囲は 0 ～ 2,147,483,647 です。
syslog_id	抑制するシステム ログ メッセージの ID。*syslog_id* の有効値の範囲は 100000 ～ 999999 です。
unlimited	レート制限をディセーブルにします。これは、ロギング レートが制限されないことを意味します。

デフォルト

interval のデフォルト設定は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

システム メッセージの重大度は次のとおりです。

- 0：システムが使用不可
- 1：ただちに処置が必要
- 2：クリティカルな状態
- 3：エラー メッセージ
- 4：警告メッセージ
- 5：正常だが、注意が必要な状態

•6：情報

•7：デバッグ メッセージ

例

システム ログ メッセージの生成レートを制限するために、特定のメッセージ ID を入力できます。次の例は、特定のメッセージ ID および時間間隔を使用して、システム ログ メッセージの生成レートを制限する方法を示しています。

```
hostname(config)# logging rate-limit 100 600 message 302020
```

この例では、指定された 600 秒間隔でレート制限 100 に達すると、システム ログ メッセージ 302020 はホストに送信されなくなります。

システム ログ メッセージの生成レートを制限するために、特定の重大度を入力できます。次の例は、特定の重大度および時間間隔を使用して、システム ログ メッセージの生成レートを制限する方法を示しています。

```
hostname(config)# logging rate-limit 1000 600 level 6
```

この例では、重大度 6 のすべてのシステム ログ メッセージが、指定された 600 秒間隔で指定の生成レート 1000 に制限されます。重大度 6 の各システム ログ メッセージのレート制限は、1000 です。

関連コマンド

コマンド	説明
clear running-config logging rate-limit	ロギング レート制限の設定をデフォルトにリセットします。
show logging	内部バッファ内の現在のメッセージ、またはロギング コンフィギュレーションの設定を表示します。
show running-config logging rate-limit	現在のロギング レート制限の設定を表示します。

logging recipient-address

セキュリティ アプライアンスによって電子メールで送信されるシステム ログ メッセージの受信者の電子メール アドレスを指定するには、グローバル コンフィギュレーション モードで **logging recipient-address** コマンドを使用します。受信者の電子メール アドレスを削除するには、このコマンドの **no** 形式を使用します。受信者のアドレスは最大 5 つまで設定できます。必要に応じて、受信者のアドレスごとに、**logging mail** コマンドで指定されたメッセージ レベルとは別のレベルを指定できます。

logging recipient-address *address* [**level** *level*]

no logging recipient-address *address* [**level** *level*]

シンタックスの説明

address	システム ログ メッセージを電子メールで送信する場合の受信者の電子メール アドレスを指定します。
level	この後にロギング レベルが続くことを示します。
level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL **(注)** **logging recipient-address** コマンドでは、3 より大きなレベルを使用することはお勧めできません。ロギング レベルを高くすると、バッファ オーバーフローによってシステム ログ メッセージがドロップされることがあります。 **logging recipient-address** コマンドで指定されたメッセージ レベルは、**logging mail** コマンドで指定されたメッセージ レベルを上書きします。たとえば、**logging recipient-address** コマンドでレベル 7 が指定された場合、**logging mail** コマンドでレベル 3 が指定されていたときは、セキュリティ アプライアンスはレベル 4、5、6、および 7 のメッセージを含むすべてのメッセージを受信者に送信します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1) (1)	このコマンドが導入されました。

使用上のガイドライン

システム ログ メッセージを電子メールで送信できるようにするには、**logging mail** コマンドを使用します。

logging recipient-address コマンドは最大 5 つまで設定できます。コマンドごとに、別々のロギング レベルを指定できます。この方法は、緊急性の高いメッセージを緊急性の低いメッセージよりも多くの受信者に送信する場合に便利です。

例

次の基準に従って、システム ログ メッセージを電子メールで送信するようにセキュリティ アプライアンスを設定します。

- critical、alerts、および emergencies のメッセージを送信する。
- メッセージを送信するときに、ciscosecurityappliance@example.com を送信者のアドレスとして使用する。
- メッセージを admin@example.com に送信する。
- SMTP を使用して、メッセージをプライマリ サーバ pri-smtp-host およびセカンダリ サーバ sec-smtp-host に送信する。

次のコマンドを入力します。

```
hostname(config)# logging mail critical
hostname(config)# logging from-address ciscosecurityappliance@example.com
hostname(config)# logging recipient-address admin@example.com
hostname(config)# smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	電子メールで送信されるシステム ログ メッセージの送信元として表示する電子メール アドレスを指定します。
logging mail	セキュリティ アプライアンスがシステム ログ メッセージを電子メールで送信できるようにし、どのメッセージを電子メールで送信するかを決定します。
smtp-server	SMTP サーバを設定します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在動作しているロギング コンフィギュレーションを表示します。

logging savelog

ログ バッファをフラッシュ メモリに保存するには、特権 EXEC モードで **logging savelog** コマンドを使用します。

logging savelog [*savefile*]

シンタックスの説明

savefile	（オプション）保存するフラッシュ メモリ ファイルの名前。ファイル名が指定されない場合、セキュリティ アプライアンスは、次のように、デフォルトのタイムスタンプ形式を使用してファイルを保存します。 LOG-*YYYY-MM-DD-HHMMSS*.TXT *YYYY* は西暦年、*MM* は月、*DD* は日、*HHMMSS* は時刻の時、分、秒です。

デフォルト

デフォルトは次のとおりです。

- バッファのサイズは 4 KB です。
- フラッシュ メモリの最小空き容量は 3 MB です。
- バッファ ロギング用のフラッシュ メモリ最大割当量は、1 MB です。
- デフォルトのログ ファイル名は、上記の表のとおりです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1) (1)	このコマンドが導入されました。

使用上のガイドライン

ログ バッファをフラッシュ メモリに保存するには、事前にバッファへのロギングをイネーブルにしておく必要があります。このようにしないと、フラッシュ メモリに保存するデータがログ バッファに保持されません。バッファへのロギングをイネーブルにするには、**logging buffered** コマンドを使用します。

（注） **logging savelog** コマンドは、バッファを消去しません。バッファを消去するには、**clear logging buffer** コマンドを使用します。

例

次の例では、ロギングとログ バッファをイネーブルにし、グローバル コンフィギュレーション モードを終了し、latest-logfile.txt というファイル名を使用してログ バッファをフラッシュ メモリに保存します。

```
hostname(config)# logging enable
hostname(config)# logging buffered
hostname(config)# exit
hostname# logging savelog latest-logfile.txt
hostname#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持しているシステム ログ メッセージをすべて消去します。
copy	ファイルを、ある位置から TFTP サーバや FTP サーバなどの別の位置にコピーします。
delete	保存済みログ ファイルなどのファイルを、ディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。

logging standby

フェールオーバー スタンバイ セキュリティ アプライアンスがこのセキュリティ アプライアンスのシステム ログ メッセージをロギング先に送信できるようにするには、グローバル コンフィギュレーション モードで **logging standby** コマンドを使用します。syslog および SNMP ロギングをディセーブルにするには、このコマンドの **no** 形式を使用します。

logging standby

no logging standby

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

logging standby コマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

logging standby をイネーブルにすると、フェールオーバーが発生しても、フェールオーバー スタンバイ セキュリティ アプライアンスのシステム ログ メッセージが同期されたままになることが保証されます。

（注） **logging standby** コマンドを使用すると、syslog サーバ、SNMP サーバ、および FTP サーバなどの共有ロギング先に対するトラフィックが 2 倍になります。

例

次の例では、セキュリティ アプライアンスがシステム ログ メッセージをフェールオーバー スタンバイ セキュリティ アプライアンスに送信できるようにします。**show logging** コマンドの出力は、この機能がイネーブルになっていることを示しています。

```
hostname(config)# logging standby
hostname(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
failover	フェールオーバー機能をイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging timestamp

システム ログ メッセージにメッセージの生成日時を含めるよう指定するには、グローバル コンフィギュレーション モードで **logging timestamp** コマンドを使用します。システム ログ メッセージから日時を削除するには、このコマンドの **no** 形式を使用します。

logging timestamp

no logging timestamp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

セキュリティ アプライアンスは、デフォルトでは、日時をシステム ログ メッセージに含めません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

logging timestamp コマンドは、セキュリティ アプライアンスがすべてのシステム ログ メッセージにタイムスタンプを含めるように指定します。

例

次の例では、すべてのシステム ログ メッセージにタイムスタンプ情報を含めることをイネーブルにします。

```
hostname(config)# logging enable
hostname(config)# logging timestamp
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

logging trap

セキュリティ アプライアンスが syslog サーバに送信するシステム ログ メッセージを指定するには、グローバル コンフィギュレーション モードで **logging trap** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

logging trap [*logging_list* | *level*]

no logging trap

シンタックスの説明

level	システム ログ メッセージの最大レベルを設定します。たとえば、レベルを 3 に設定すると、セキュリティ アプライアンスはレベル 3、2、1、および 0 のシステム ログ メッセージを生成します。次の数値または名前で指定できます。 • **0** または **emergencies**：システムが使用不能 • **1** または **alerts**：ただちに処置が必要 • **2** または **critical**：クリティカルな状態 • **3** または **errors**：エラー • **4** または **warnings**：警告 • **5** または **notifications**：正常だが、注意が必要な状態 • **6** または **informational**：情報 • **7** または **debugging**：デバッグ メッセージ、ログ FTP コマンド、WWW URL
logging_list	syslog サーバに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

デフォルト

デフォルトの syslog トラップは定義されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ロギング転送プロトコルとして TCP を使用する場合、セキュリティ アプライアンスが syslog サーバに到達できないとき、syslog サーバが誤って設定されているとき、またはディスクがいっぱいのときは、セキュリティ アプライアンスはセキュリティ保護手段として、新しいネットワーク アクセス セッションを拒否します。

UDP ベースのロギングは、syslog サーバに障害が発生しても、セキュリティ アプライアンスによるトラフィックの送信を妨げません。

例

次の例は、内部インターフェイス上にあってデフォルトのプロトコルとポート番号を使用する syslog サーバに対して、レベル 0、1、2、および 3 のシステム ログ メッセージを送信する方法を示しています。

```
hostname(config)# logging enable
hostname(config)# logging host inside 10.2.2.3
hostname(config)# logging trap errors
hostname(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバを定義します。
logging list	再使用可能なメッセージ選択基準リストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのロギング関連の部分を表示します。

login

ローカル ユーザ データベースを使用して特権 EXEC モードに入る場合や、ユーザ名を変更する場合は、ユーザ EXEC モードで **login** コマンドを使用します。

login

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

login コマンドを使用すると、ユーザ EXEC モードから特権 EXEC モードに、ローカル データベース内の任意のユーザ名としてログインできます。イネーブル認証をオンにした場合、**login** コマンドは **enable** コマンドと類似したものになります（**aaa authentication console** コマンドを参照）。ただし、イネーブル認証とは異なり、**login** コマンドはローカル ユーザ名データベースのみを使用できます。このコマンドでは、常に認証が要求されます。また、**login** コマンドを使用すると、任意の CLI モードからユーザを変更できます。

ユーザがログイン時に特権 EXEC モード（およびすべてのコマンド）にアクセスできるようにするには、ユーザの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、**aaa authorization コマンド**を参照してください。

注意　CLI にアクセスできるユーザや特権 EXEC モードに入らせないようにするユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります。コマンド認可が設定されていない場合、ユーザは、特権レベルが 2 以上（2 がデフォルト）であれば、各自のパスワードを使用して CLI で特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、RADIUS または TACACS+ 認証を使用することもできます。あるいは、すべてのローカル ユーザをレベル 1 に設定して、システムのイネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザを制御することもできます。

例

次の例では、**login** コマンドを入力した後のプロンプトを示します。

```
hostname> login
Username:
```

関連コマンド

コマンド	説明
aaa authorization command	CLI アクセスのコマンド認可をイネーブルにします。
aaa authentication console	コンソール、Telnet、HTTP、SSH、または **enable** コマンド アクセスに対して認証を要求します。
logout	CLI からログアウトします。
username	ユーザをローカル データベースに追加します。

login-button

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン ボックスの Login ボタンをカスタマイズするには、webvpn カスタマイゼーション モードで **login-button** コマンドを使用します。

login-button {**text** | **style**} *value*

[**no**] **login-button** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトの Login ボタンのテキストは「Login」です。

デフォルトの Login ボタンのスタイルは、次のとおりです。

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、Login ボタンのテキストを「OK」にカスタマイズします。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-button text OK
```

関連コマンド

コマンド	説明
login-title	WebVPN ページのログイン ボックスのタイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。

login-message

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのログイン メッセージをカスタマイズするには、webvpn カスタマイゼーション モードで **login-message** コマンドを使用します。

login-message {**text** | **style**} *value*

[**no**] **login-message** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン メッセージは「Please enter your username and password」です。

デフォルトのログイン メッセージのスタイルは、background-color:#CCCCCC;color:black です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

(注)　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、ログイン メッセージのテキストを「username and password」に設定します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-message text username and password
```

関連コマンド

コマンド	説明
login-title	WebVPN ページのログイン ボックスのタイトルをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。

login-title

WebVPN ユーザに表示される WebVPN ページのログイン ボックスのタイトルをカスタマイズするには、webvpn カスタマイゼーション モードで **login-title** コマンドを使用します。

login-title {**text** | **style**} *value*

[**no**] **login-title** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログイン テキストは「Login」です。

ログイン タイトルのデフォルト HTML スタイルは、background-color: #666666; color: white です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

(注)　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、ログイン タイトルのスタイルを設定します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# login-title style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

関連コマンド

コマンド	説明
login-message	WebVPN ページのログイン メッセージをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。

logo

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページのロゴをカスタマイズするには、webvpn カスタマイゼーション モードで **logo** コマンドを使用します。

logo {**none** | **file** {*path value*}}

[**no**] **logo** {**none** | **file** {*path value*}}

シンタックスの説明

none	ロゴを使用しないことを指定します。ヌル値を設定して、ロゴを拒否します。ロゴを継承しないようにします。
file	ロゴを含むファイルを指定することを示します。
path	ファイル名のパス。可能なパスは disk0:、disk1:、または flash: です。
value	ロゴのファイル名を指定します。最大長は 255 文字です（スペースは含めません）。ファイル タイプには JPG、PNG、または GIF を指定し、サイズは 100 KB 未満にする必要があります。

デフォルト

デフォルトのロゴは、シスコのロゴです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

ロゴをコンフィギュレーションから削除してデフォルト（シスコのロゴ）にリセットするには、このコマンドの **no** 形式を使用します。

ロゴを削除するには、**logo none** コマンドを使用します。

指定したファイル名が存在しない場合は、エラー メッセージが表示されます。ロゴ ファイルを削除した場合、コンフィギュレーションが引き続きそのファイルを指していても、ロゴは表示されません。

ファイル名にスペースを含めることはできません。

例

次の例では、cisco_logo.gif というファイルにカスタム ロゴが含まれています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

関連コマンド

コマンド	説明
title	WebVPN ページのタイトルをカスタマイズします。
page style	Cascading Style Sheet（CSS）パラメータを使用して WebVPN ページをカスタマイズします。

logout

CLI を終了するには、ユーザ EXEC モードで **logout** コマンドを使用します。

logout

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**logout** コマンドを使用すると、セキュリティ アプライアンスからログアウトできます。ユーザ モードに戻るには、**exit** コマンドまたは **quit** コマンドを使用します。

例　次の例は、セキュリティ アプライアンスからログアウトする方法を示しています。

```
hostname> logout
```

関連コマンド

コマンド	説明
login	ログイン プロンプトを開始します。
exit	アクセス モードを終了します。
quit	コンフィギュレーション モードまたは特権モードを終了します。

logout-message

WebVPN ユーザが WebVPN サービスからログアウトするときに表示される WebVPN ログアウト画面のログアウト メッセージをカスタマイズするには、webvpn カスタマイゼーション モードで **logout-message** コマンドを使用します。

logout-message {**text** | **style**} *value*

[**no**] **logout-message** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのログアウト メッセージのテキストは「Goodbye」です。

デフォルトのログアウト メッセージのスタイルは、background-color:#999999;color:black です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

(注)　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、ログアウト メッセージのスタイルを設定します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# logout-message style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt;
font-style: italic; font-weight: bold
```

関連コマンド

コマンド	説明
logout-title	WebVPN ページのログアウト タイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザ名プロンプトをカスタマイズします。

CHAPTER 20

mac address コマンド～ multicast-routing コマンド

mac address

アクティブ装置およびスタンバイ装置の仮想 MAC アドレスを指定するには、フェールオーバー グループ コンフィギュレーション モードで **mac address** コマンドを使用します。デフォルトの仮想 MAC アドレスに戻すには、このコマンドの **no** 形式を使用します。

mac address *phy_if* [*active_mac*] [*standby_mac*]

no mac address *phy_if* [*active_mac*] [*standby_mac*]

シンタックスの説明

phy_if	MAC アドレスを設定するインターフェイスの物理名。
active_mac	アクティブ装置の仮想 MAC アドレス。MAC アドレスは、h.h.h 形式で入力する必要があります。h は、16 ビットの 16 進数値です。
standby_mac	スタンバイ装置の仮想 MAC アドレス。MAC アドレスは、h.h.h 形式で入力する必要があります。h は、16 ビットの 16 進数値です。

デフォルト

デフォルトは次のとおりです。

- アクティブ装置のデフォルト MAC アドレス：00a0.c9*physical_port_number.failover_group_id*01
- スタンバイ装置のデフォルト MAC アドレス：00a0.c9*physical_port_number.failover_group_id*02

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバー グループに仮想 MAC アドレスが定義されていない場合、デフォルト値が使用されます。

同じネットワーク上に Active/Active フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上の MAC アドレスを重複させないためには、各物理インターフェイスに必ずアクティブとスタンバイの仮想 MAC アドレスを割り当てるようにしてください。

例

次の例（抜粋）は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover mac address	物理インターフェイスの仮想 MAC アドレスを指定します。

mac-address

プライベート MAC アドレスをインターフェイスまたはサブインターフェイスに手作業で割り当てるには、インターフェイス コンフィギュレーション モードで **mac-address** コマンドを使用します。マルチ コンテキスト モードでは、このコマンドによって各コンテキストのインターフェイスに異なる MAC アドレスを割り当てることができます。MAC アドレスをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

mac-address *mac_address* [**standby** *mac_address*]

no mac-address [*mac_address* [**standby** *mac_address*]]

シンタックスの説明

mac_address	このインターフェイスの MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数値です。たとえば、MAC アドレス 00-0C-F1-42-4C-DE は、000C.F142.4CDE と入力します。フェールオーバーを使用する場合、この MAC アドレスはアクティブな MAC アドレスになります。
standby *mac_address*	（オプション）フェールオーバー用のスタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、この新たにアクティブになった装置がアクティブな MAC アドレスの使用を開始してネットワーク障害を最小限にする一方で、アクティブでなくなった方の装置はスタンバイ アドレスを使用します。

デフォルト

デフォルトの MAC アドレスは、物理インターフェイスのバーンドイン MAC アドレスです。サブインターフェイスは、物理インターフェイスの MAC アドレスを継承します。物理インターフェイスの MAC アドレスを設定するコマンドもある（シングル モードのこのコマンドを含む）ので、継承されるアドレスはそのコンフィギュレーションによって決定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードで、コンテキスト間のインターフェイスを共有する場合、一意の MAC アドレスを各コンテキストのインターフェイスに割り当てることができます。この機能により、セキュリティ アプライアンスではパケットを適切なコンテキストに分類しやすくなります。一意の MAC アドレスなしに共有インターフェイスを使用することは可能ですが、いくつかの制限があります。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

このコマンドを使用して各 MAC アドレスを手作業で割り当てるか、**mac-address auto** コンドを使用してコンテキストの共有インターフェイスの MAC アドレスを自動的に生成することができます。MAC アドレスを自動的に生成する場合、**mac-address** コマンドを使用して生成されたアドレスを上書きします。

シングル コンテキスト モードの場合、またはマルチ コンテキスト モードで共有されないインターフェイスの場合、一意の MAC アドレスをサブインターフェイスに割り当てることもできます。たとえば、サービス プロバイダーは MAC アドレスに基づいてアクセスを制御する場合もあります。

MAC アドレスは、他のコマンドや方法を使用して設定することもできます。MAC アドレスの設定方法には、次のような優先順位があります。

1. インターフェイス コンフィギュレーション モードの **mac-address** コマンド。

   このコマンドは、物理インターフェイスおよびサブインターフェイスに対して作用します。マルチ コンテキスト モードの場合は、各コンテキスト内で MAC アドレスを設定します。この機能を利用すると、同じインターフェイスに対して、複数のコンテキストでそれぞれ別の MAC アドレスを設定できます。

2. グローバル コンフィギュレーション モードの **failover mac address** コマンド（Active/Standby フェールオーバーの場合）。

   このコマンドは物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** コマンドまたは **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

3. フェールオーバー グループ コンフィギュレーション モードの **mac address** コマンド（Active/Active フェールオーバーの場合）。

   このコマンドは物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** コマンドまたは **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

4. グローバル コンフィギュレーション モードの **mac-address auto** コマンド（マルチ コンテキスト モードのみ）。

   このコマンドは、コンテキスト内の共有インターフェイスに適用されます。

5. Active/Active フェールオーバーにおける、物理インターフェイスのアクティブ MAC アドレスとスタンバイ MAC アドレスの自動生成。

   この方法は物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** コマンドまたは **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

6. バーンドイン MAC アドレス。この方法は物理インターフェイスに適用されます。

   サブインターフェイスは、**mac-address** コマンドまたは **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

例

次の例では、GigabitEthernet 0/1.1 の MAC アドレスを設定します。

```
hostname/contextA(config)# interface gigabitethernet0/1.1
hostname/contextA(config-if)# nameif inside
hostname/contextA(config-if)# security-level 100
hostname/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
hostname/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
hostname/contextA(config-if)# no shutdown
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address auto	マルチ コンテキスト モードの共有インターフェイスの MAC アドレス（アクティブおよびスタンバイ）を自動生成します。
mode	セキュリティ コンテキスト モードをシングルまたはマルチに設定します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

mac-address auto

プライベート MAC アドレスを各共有コンテキスト インターフェイスに自動的に割り当てるには、グローバル コンフィギュレーション モードで **mac-address auto** コマンドを使用します。MAC アドレスの自動割り当てをディセーブルにするには、このコマンドの **no** 形式を使用します。

mac-address auto

no mac-address auto

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

自動生成はデフォルトではディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

コンテキストでインターフェイスを共有するには、一意の MAC アドレスを各コンテキストのインターフェイスに割り当てることをお勧めします。MAC アドレスを使用してコンテキスト内のパケットを分類します。インターフェイスを共有する場合に、各コンテキストのインターフェイス用の MAC アドレスがないときには、宛先 IP アドレスを使用してパケットを分類します。宛先アドレスは、コンテキスト NAT コンフィギュレーションと照合されます。MAC アドレス方式と比較すると、この方式にはいくつかの制限があります。パケットの分類については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

デフォルトでは、物理インターフェイスはバーンドイン MAC アドレスを使用し、物理インターフェイスのサブインターフェイスはすべて同一のバーンドイン MAC アドレスを使用します。

フェールオーバーで使用する場合、セキュリティ アプライアンスは各インターフェイスに対してアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになる場合、この新たにアクティブになった装置はアクティブな MAC アドレスの使用を開始してネットワーク障害を最小限にします。**mac-address auto** コマンドは共有インターフェイスのみを設定するため、**mac-address** コマンドまたは **failover mac address** コマンドを使用して、Active/Standby コンフィギュレーションで非共有インターフェイスに仮想 MAC アドレスを依然として設定する必要があります（Active/Active フェールオーバーは仮想 MAC アドレスを物理インターフェイスに自動的に割り当てます）。

インターフェイスをコンテキストに割り当てると、新しい MAC アドレスがただちに生成されます。コンテキスト インターフェイスを生成した後にこのコマンドをイネーブルにした場合、このコマンドを入力するとただちに MAC アドレスがすべてのインターフェイスに生成されます。**no**

mac-address auto コマンドを使用すると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを再度使用します。

MAC アドレスは次の形式を使用して生成します。

- アクティブ装置の MAC アドレス：12*_slot.port_subid.contextid.*
- スタンバイ装置の MAC アドレス：02*_slot.port_subid.contextid.*

インターフェイス スロットのないプラットフォームの場合、スロットは常に 0 です。*port* はインターフェイス ポートです。*subid* はサブインターフェイスの内部 ID です。この ID は表示されません。*contextid* はコンテキストの内部 ID です。**show context detail** コマンドを使用して表示します。たとえば、ID 1 を持つコンテキストのインターフェイス GigabitEthernet 0/1.200 には次の生成された MAC アドレスが設定されています。サブインターフェイス 200 の内部 ID は 31 です。

- アクティブ：1200.0131.0001
- スタンバイ：0200.0131.0001

まれなケースですが、生成された MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合した場合は、コンテキスト内でインターフェイスの MAC アドレスを手作業で設定します。MAC アドレスを手作業で設定するには、**mac-address** コマンドを参照してください。

MAC アドレスは、他のコマンドや方法を使用して設定することもできます。MAC アドレスの設定方法には、次のような優先順位があります。

1. インターフェイス コンフィギュレーション モードの **mac-address** コマンド。

   このコマンドは、物理インターフェイスおよびサブインターフェイスに対して作用します。マルチ コンテキスト モードの場合は、各コンテキスト内で MAC アドレスを設定します。この機能を利用すると、同じインターフェイスに対して、複数のコンテキストでそれぞれ別の MAC アドレスを設定できます。

2. グローバル コンフィギュレーション モードの **failover mac address** コマンド（Active/Standby フェールオーバーの場合）。

   このコマンドは物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** コマンドまたは **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

3. フェールオーバー グループ コンフィギュレーション モードの **mac address** コマンド（Active/Active フェールオーバーの場合）。

   このコマンドは物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** コマンドまたは **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

4. グローバル コンフィギュレーション モードの **mac-address auto** コマンド（マルチ コンテキスト モードのみ）。

   このコマンドは、コンテキスト内の共有インターフェイスに適用されます。

5. Active/Active フェールオーバーにおける、物理インターフェイスのアクティブ MAC アドレスとスタンバイ MAC アドレスの自動生成。

   この方法は物理インターフェイスに適用されます。サブインターフェイスは、**mac-address** コマンドまたは **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

6. バーンドイン MAC アドレス。この方法は物理インターフェイスに適用されます。

   サブインターフェイスは、**mac-address** コマンドまたは **mac-address auto** コマンドを使用して個別に設定しない限り、物理インターフェイスの MAC アドレスを継承します。

例

次の例では、MAC アドレスの自動生成をイネーブルにします。

```
hostname(config)# mac-address auto
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address	物理インターフェイスまたはサブインターフェイスの MAC アドレス（アクティブおよびスタンバイ）を手動で設定します。マルチ コンテキスト モードでは、同じインターフェイスに対して、コンテキストごとにそれぞれ別の MAC アドレスを設定することができます。
mode	セキュリティ コンテキスト モードをシングルまたはマルチに設定します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

mac-address-table aging-time

MAC アドレス テーブル エントリのタイムアウトを設定するには、グローバル コンフィギュレーション モードで **mac-address-table aging-time** コマンドを使用します。5 分のデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

mac-address-table *aging-time* *timeout_value*

no mac-address-table *aging-time*

シンタックスの説明

timeout_value	タイムアウトになるまで MAC アドレス テーブルで MAC アドレス エントリを維持する時間は、5 ～ 720 分（12 時間）です。デフォルトは 5 分です。

デフォルト

デフォルトのタイムアウトは 5 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

使用上のガイドラインはありません。

例

次の例では、MAC アドレスのタイムアウトを 10 分に設定します。

```
hostname(config)# mac-address-timeout aging time 10
```

関連コマンド

コマンド	説明
arp-inspection	ARP 検査をイネーブルにして、ARP パケットをスタティック ARP エントリと比較します。
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

mac-address-table static

MAC アドレス テーブルにスタティック エントリを追加するには、グローバル コンフィギュレーション モードで **mac-address-table static** コマンドを使用します。スタティック エントリを削除するには、このコマンドの **no** 形式を使用します。通常、MAC アドレスは、特定の MAC アドレスからトラフィックがインターフェイスに届いたときに、MAC アドレス テーブルに動的に追加されます。MAC アドレス テーブルには、必要に応じてスタティック MAC アドレスを追加できます。スタティック エントリを追加する 1 つの利点は、MAC スプーフィングから保護できることです。スタティック エントリと同じ MAC アドレスを持つクライアントが、スタティック エントリに一致しないインターフェイスにトラフィックを送信しようとすると、セキュリティ アプライアンスはトラフィックをドロップし、システム メッセージを生成します。

mac-address-table static *interface_name mac_address*

no mac-address-table static *interface_name mac_address*

シンタックスの説明

interface_name	送信元インターフェイス。
mac_address	テーブルに追加する MAC アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。

```
hostname(config)# mac-address-table static inside 0010.7cbe.6101
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

mac-learn

インターフェイスの MAC アドレス ラーニングをディセーブルにするには、グローバル コンフィギュレーション モードで **mac-learn** コマンドを使用します。MAC アドレス ラーニングを再度イネーブルにするには、このコマンドの **no** 形式を使用します。デフォルトでは、受信するトラフィックの MAC アドレスを各インターフェイスが自動的にラーニングし、セキュリティ アプライアンスが対応するエントリを MAC アドレス テーブルに追加します。必要に応じて、MAC アドレス ラーニングをディセーブルにできます。

mac-learn *interface_name* ***disable***

no mac-learn *interface_name* ***disable***

シンタックスの説明

interface_name	MAC ラーニングをディセーブルにするインターフェイス。
disable	MAC ラーニングをディセーブルにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、外部インターフェイスの MAC ラーニングをディセーブルにします。

```
hostname(config)# mac-learn outside disable
```

関連コマンド

コマンド	説明
clear configure mac-learn	**mac-learn** コンフィギュレーションをデフォルトに設定します。
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。
show running-config mac-learn	**mac-learn** コンフィギュレーションを表示します。

mac-list

MAC アドレスの認証や認可を免除するために使用する MAC アドレスのリストを指定するには、グローバル コンフィギュレーション モードで **mac-list** コマンドを使用します。MAC リスト エントリを削除するには、このコマンドの **no** 形式を使用します。

mac-list *id* {**deny | permit**} *mac macmask*

no mac-list *id* {**deny | permit**} *mac macmask*

シンタックスの説明

deny	この MAC アドレスに一致するトラフィックが MAC リストに一致しないこと、**aaa mac-exempt** コマンドに指定された際に認証と認可の両方の対象となることを示します。ffff.ffff.0000 といった MAC アドレス マスクを使用する MAC アドレスの範囲を許可し、その範囲の MAC アドレスを認証と認可の対象とする場合は、deny（拒否）エントリを MAC リストに追加しなければならないことがあります。
id	16 進数の MAC アクセス リストの番号を指定します。MAC アドレスのセットをグループ化するには、同じ ID の値を使用して必要な数だけ **mac-list** コマンドを入力します。パケットは最も一致するシナリオではなく、最初に一致するエントリを使用するため、エントリの順序が重要です。permit（許可）エントリにおいては、permit エントリにより許可されたアドレスを拒否する場合、必ず permit エントリの前に deny エントリを入力します。
mac	12 桁の 16 進数形式（nnnn.nnnn.nnnn）で送信元 MAC アドレスを指定します。
macmask	マッチングに使用する MAC アドレスの一部を指定します。たとえば、ffff.ffff.ffff は MAC アドレスに完全に一致します。ffff.ffff.0000 は最初の 8 桁のみに一致します。
permit	この MAC アドレスに一致するトラフィックが MAC リストに一致することと、**aaa mac-exempt** コマンドに指定されたときに認証と認可の両方の対象から免除されることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

MAC アドレスを認証と認可の対象から免除するには、**aaa mac-exempt** コマンドを使用します。追加できる **aaa mac-exempt** コマンドのインスタンスは 1 つだけです。そのため、MAC リストに免除する MAC アドレスがすべて確実に含まれるようにしてください。複数の MAC リストを作成できますが、使用できるのは一度に 1 つだけです。

例

次の例では、1 つの MAC アドレスについて認証をバイパスします。

```
hostname(config)# mac-list abc permit 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# aaa mac-exempt match abc
```

次のエントリでは、ハードウェア ID が 0003.E3 であるすべての Cisco IP Phone について、認証をバイパスしています。

```
hostname(config)# mac-list acd permit 0003.E300.0000 FFFF.FF00.0000
hostname(config)# aaa mac-exempt match acd
```

次の例では、00a0.c95d.02b2 を除く MAC アドレスのグループについて認証をバイパスします。permit 文の前に deny 文を入力してください。00a0.c95d.02b2 は permit 文にも一致するため、permit 文が最初に来ると、deny 文には一致しないためです。

```
hostname(config)# mac-list 1 deny 00a0.c95d.0282 ffff.ffff.ffff
hostname(config)# mac-list 1 permit 00a0.c95d.0000 ffff.ffff.0000
hostname(config)# aaa mac-exempt match 1
```

関連コマンド

コマンド	説明
aaa authentication	ユーザ認証をイネーブルにします。
aaa authorization	ユーザ認可サービスをイネーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から免除します。
clear configure mac-list	**mac-list** コマンドで以前に指定されている MAC アドレスのリストを削除します。
show running-config mac-list	**mac-list** コマンドで指定されている MAC アドレスのリストを表示します。

mail-relay

ローカル ドメイン名を設定するには、パラメータ コンフィギュレーション モードで **mail-relay** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mail-relay *domain_name* **action** {**drop-connection** | **log**}

no mail-relay *domain_name* **action** {**drop-connection** | **log**}

シンタックスの説明

domain_name	ドメイン名を指定します。
drop-connection	接続を終了します。
log	システム ログ メッセージを生成します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、特定のドメインにメール リレーを設定する方法を示しています。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mail-relay mail action drop-connection
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

management-access

IPSec VPN の使用時にセキュリティ アプライアンスを実行するために使用したインターフェイス以外のインターフェイスへの管理アクセスを許可するには、グローバル コンフィギュレーション モードで ***management-access*** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

management-access *mgmt_if*

no management-access *mgmt_if*

シンタックスの説明

mgmt_if	別のインターフェイスからセキュリティ アプライアンスに入る際にアクセスする管理インターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドを使用すると、IPSec VPN の使用時にセキュリティ アプライアンスに入ったインターフェイス以外のインターフェイスに接続できます。たとえば、外部インターフェイスからセキュリティ アプライアンスに入った場合、このコマンドにより Telnet を使用して内部インターフェイスに接続できます。あるいは、外部インターフェイスから入ったときに、内部インターフェイスに対して ping を実行することができます。

定義できる管理アクセス用のインターフェイスは 1 つだけです。

例

次の例は、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定する方法を示しています。

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
show management-access	管理アクセス用に設定されている内部インターフェイスの名前を表示します。

management-only

管理トラフィックだけを受け入れるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **management-only** コマンドを使用します。トラフィックの通過を許可するには、このコマンドの **no** 形式を使用します。

management-only

no management-only

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

ASA 5510 以降の適応型セキュリティ アプライアンスの Management 0/0 インターフェイスは、デフォルトで管理専用モードに設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASA 5510 以降の適応型セキュリティ アプライアンスには、Management 0/0 と呼ばれる管理専用インターフェイスが含まれており、このインターフェイスによってセキュリティ アプライアンスへのトラフィックをサポートします。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。また、Management 0/0 の管理専用モードをディセーブルにして、他のインターフェイスと同様にトラフィックを通過させることもできます。

透過ファイアウォール モードでは、2 つのインターフェイスだけがトラフィックを通過できます。ただし、ASA 5510 以降の適応型セキュリティ アプライアンスでは、Management 0/0 インターフェイス（物理インターフェイスまたはサブインターフェイス）を管理トラフィック用の第 3 のインターフェイスとして使用できます。モードはこの場合設定不能であり、常に管理専用にする必要があります。このインターフェイスを管理 IP アドレスから異なるサブネット上に移行させる場合、透過モードでこのインターフェイスの IP アドレスを設定することもできます。個々のインターフェイスではなく、セキュリティ アプライアンスまたはコンテキストに対して割り当てます。

例

次の例では、管理インターフェイスの管理専用モードをディセーブルにします。

```
hostname(config)# interface management0/0
hostname(config-if)# no management-only
```

次の例では、サブインターフェイスの管理専用モードをイネーブルにします。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# management-only
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。

map-name

ユーザ定義のアトリビュート名を Cisco アトリビュート名にマッピングするには、LDAP アトリビュート マップ コンフィギュレーション モードで **map-name** コマンドを使用します。

このマッピングを削除するには、このコマンドの **no** 形式を使用します。

map-name *user-attribute-name Cisco-attribute-name*

no map-name *user-attribute-name Cisco-attribute-name*

シンタックスの説明

user-attribute-name	Cisco アトリビュートにマッピングする、ユーザ定義のアトリビュート名を指定します。
Cisco-attribute-name	ユーザ定義の名前にマッピングする、Cisco アトリビュート名を指定します。

デフォルト

デフォルトでは、名前のマッピングは存在しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
LDAP アトリビュート マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

map-name コマンドを使用して、独自のアトリビュート名を作成し、それを Cisco アトリビュート名にマッピングできます。作成されたアトリビュート マップは、LDAP サーバにバインドすることができます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用して、何も入力されていないアトリビュート マップを作成します。このコマンドにより、LDAP アトリビュート マップ コンフィギュレーション モードに入ります。
2. LDAP アトリビュート マップ コンフィギュレーション モードで **map-name** コマンドおよび **map-value** コマンドを使用して、アトリビュート マップに情報を入力します。

3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用して、LDAP サーバにアトリビュート マップをバインドします。このコマンドでは、「ldap」の後にハイフンを入力してください。

(注) アトリビュート マッピング機能を正しく使用するには、Cisco LDAP アトリビュートの名前と値、およびユーザ定義アトリビュートの名前と値を理解しておく必要があります。

例

次のコマンド例では、LDAP アトリビュート マップ「myldapmap」内で、ユーザ定義のアトリビュート名「Hours」を、Cisco アトリビュート名「cVPN3000-Access-Hours」にマッピングします。

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
hostname(config-ldap-attribute-map)#
```

LDAP アトリビュート マップ コンフィギュレーション モードでは、次の例に示すように、「?」を入力して Cisco LDAP アトリビュート名の完全なリストを表示できます。

```
hostname(config-ldap-attribute-map)# map-name ?
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
    :
    :
  cVPN3000-X509-Cert-Data
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP アトリビュート マップを LDAP サーバにバインドします。
map-value	ユーザ定義のアトリビュート値を、Cisco　アトリビュートにマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP アトリビュート マップまたはすべての実行アトリビュート マップを表示します。
clear configure ldap attribute-map	すべての LDAP アトリビュート マップを削除します。

map-value

Cisco LDAP アトリビュートにユーザ定義の値をマッピングするには、LDAP アトリビュート マップ コンフィギュレーション モードで **map-value** コマンドを使用します。

マップ内のエントリを削除するには、このコマンドの **no** 形式を使用します。

map-value *user-attribute-name user-value-string Cisco-value-string*

no map-value *user-attribute-name user-value-string Cisco-value-string*

シンタックスの説明

cisco-value-string	Cisco アトリビュートに対して Cisco 値の文字列を指定します。
user-attribute-name	Cisco アトリビュート名にマッピングする、ユーザ定義のアトリビュート名を指定します。
user-value-string	Cisco アトリビュート値にマッピングする、ユーザ定義の値文字列を指定します。

デフォルト

デフォルトでは、Cisco アトリビュートにマッピングされているユーザ定義の値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
LDAP アトリビュート マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

map-value コマンドを使用して、Cisco アトリビュート名と値に対して独自のアトリビュート値をマッピングできます。作成されたアトリビュート マップは、LDAP サーバにバインドすることができます。通常の手順は、次のとおりです。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用して、何も入力されていないアトリビュート マップを作成します。このコマンドにより、LDAP アトリビュート マップ コンフィギュレーション モードに入ります。
2. LDAP アトリビュート マップ コンフィギュレーション モードで **map-name** コマンドおよび **map-value** コマンドを使用して、アトリビュート マップに情報を入力します。
3. AAA サーバ ホスト モードで **ldap-attribute-map** コマンドを使用して、LDAP サーバにアトリビュート マップをバインドします。このコマンドでは、「ldap」の後にハイフンを入力してください。

（注） アトリビュート マッピング機能を正しく使用するには、Cisco LDAP アトリビュートの名前と値、およびユーザ定義アトリビュートの名前と値を理解しておく必要があります。

例

次の例は、LDAP アトリビュート マップ コンフィギュレーション モードで入力され、ユーザ アトリビュート「Hours」のユーザ定義値を、workDay というユーザ定義の時間ポリシーと Daytime というシスコ定義の時間ポリシーに設定します。

```
hostname(config)# ldap attribute-map myldapmap
hostname(config-ldap-attribute-map)# map-value Hours workDay Daytime
hostname(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP アトリビュート マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP アトリビュート名を、Cisco LDAP アトリビュート名にマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP アトリビュート マップまたはすべての実行アトリビュート マップを表示します。
clear configure ldap attribute-map	すべての LDAP マップを削除します。

mask

モジュラ ポリシー フレームワークを使用する場合、一致またはクラス コンフィギュレーション モードで **mask** コマンドを使用して **match** コマンドまたはクラス マップに一致するパケットの一部をマスクします。このマスク アクションはアプリケーション トラフィック用の検査ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリケーションがこのアクションを許可しているわけでありません。たとえば、セキュリティ アプライアンス経由のトラフィックを許可するには、DNS アプリケーション検査で **mask** コマンドを使用してヘッダー フラグをマスクします。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

mask [**log**]

no mask [**log**]

シンタックスの説明

log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。アプリケーション トラフィックを識別する **match** コマンドまたは **class** コマンド（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを指す）を入力してから、**mask** コマンドを使用して **match** コマンドまたは **class** コマンドに一致するパケットの一部をマスクします。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は検査ポリシー マップの名前です。

例

次の例では、セキュリティ アプライアンス経由でトラフィックを許可する前に、DNS ヘッダーの RD フラグと RA フラグをマスクします。

```
hostname(config-cmap)# policy-map type inspect dns dns-map1
hostname(config-pmap-c)# match header-flag RD
hostname(config-pmap-c)# mask log
hostname(config-pmap-c)# match header-flag RA
hostname(config-pmap-c)# mask log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

mask-banner

サーバのバナーを目立たないようにするには、パラメータ コンフィギュレーション モードで **mask-banner** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mask-banner

no mask-banner

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、サーバのバナーを隠す方法を示しています。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# mask-banner
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

mask-syst-reply

FTP サーバ応答をクライアントから見えないようにするには、FTP マップ コンフィギュレーション モードで **mask-syst-reply** コマンドを使用します。このモードには、**ftp-map** コマンドを使用してアクセスできます。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

mask-syst-reply

no mask-syst-reply

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
FTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

mask-syst-reply コマンドは、クライアントから FTP サーバ システムを保護するため、厳密な FTP 検査と併せて使用します。このコマンドをイネーブルにすると、**syst** コマンドへのサーバ応答は X の連続に置き換えられます。

例

次の例では、セキュリティ アプライアンスが syst コマンドへの FTP サーバ応答を X の連続に置き換えます。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# mask-syst-reply
hostname(config-ftp-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション検査用に特定の FTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。
request-command deny	禁止する FTP コマンドを指定します。

match access-list

モジュラ ポリシー フレームワークを使用する場合は、クラス マップ コンフィギュレーション モードで **match access-list** コマンドを使用し、アクションを適用するトラフィックをアクセス リストで識別します。**match access-list** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match access-list *access_list_name*

no match access-list *access_list_name*

シンタックスの説明

access_list_name	一致条件として使用するアクセス リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドを入力してから、**match access-list** コマンドを入力してトラフィックを識別します。また、**match port** コマンドなどの別のタイプの **match** コマンドを入力することもできます。クラス マップには **match access-list** コマンドを 1 つだけ含めることができます。それを別の種類の **match** コマンドと組み合せることはできません。例外としては、セキュリティ アプライアンスで検査可能なすべてのアプリケーションが使用するデフォルトの TCP ポートと UDP ポートに一致する **match default-inspection-traffic** コマンドを定義する場合、**match access-list** コマンドを使用してトラフィックを絞り込んで一致させることができます。**match default-inspection-traffic** コマンドは一致するポートを指定するため、アクセス リストに含まれるポートは無視されます。

2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのための特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスに対するアクションを有効にします。

例

次の例では、3 つのアクセス リストに一致する 3 つのレイヤ 3/4 クラス マップを作成します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server
10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match any

モジュラ ポリシー フレームワークを使用する場合、クラス マップ コンフィギュレーション モードで **match any** コマンドを使用してアクションを適用するすべてのトラフィックに一致させます。**match any** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match any

no match any

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドの入力後には、**match any** コマンドを入力してすべてのトラフィックを識別します。また、**match port** コマンドなどの別のタイプの **match** コマンドを入力することもできます。**match any** コマンドを別のタイプの **match** コマンドと組み合せることはできません。
2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのための特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスに対するアクションを有効にします。

例

次の例は、クラス マップおよび **match any** コマンドを使用して、トラフィック クラスを定義する方法を示しています。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match any
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match access-list	アクセス リストに従って、トラフィックを照合します。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match apn

GTP メッセージのアクセス ポイント名に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match apn** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **apn regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **apn regex** [*regex_name* | **class** *regex_class_name*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップ内で設定できます。GTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、GTP 検査クラス マップのアクセス ポイント名に関する一致条件を設定する方法を示します。

```
hostname(config-cmap)# match apn class gtp_regex_apn
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match body

ESMTP メッセージ本文の長さ、または行の長さに関する一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match body** コマンドを使用します。設定済みのセクションを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **body [length | line length] gt** *bytes*

no match [**not**] **body [length | line length] gt** *bytes*

シンタックスの説明

length	ESMTP メッセージ本文の長さを指定します。
line length	ESMTP メッセージ本文の行の長さを指定します。
bytes	バイト単位で一致する数字を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ESMTP 検査ポリシー マップで、特定の本文の行の長さに関して一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match body line length gt 1000
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match called-party

H.323 着信側に関する一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match called-party** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **called-party [regex** *regex***]**

no match [**not**] **match** [**not**] **called-party [regex** *regex***]**

シンタックスの説明

regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査クラス マップで着信側に関する一致条件を設定する方法を示します。

```
hostname(config-cmap)# match called-party regex caller1
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match calling-party

H.323 発信側に関する一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match calling-party** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **calling-party [regex** *regex***]**

no match [**not**] **match** [**not**] **calling-party [regex** *regex***]**

シンタックスの説明

regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査クラス マップで発信側に関する一致条件を設定する方法を示します。

```
hostname(config-cmap)# match calling-party regex caller1
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match certificate

PKI 証明書の検証プロセス時に、セキュリティ アプライアンスは証明書の失効ステータスをチェックし、セキュリティを維持します。このタスクを完了するために、CRL チェックまたは Online Certificate Status Protocol（OSCP; オンライン証明書ステータス プロトコル）が使用されます。CRL チェックの場合、セキュリティ アプライアンスは証明書の失効リストを取得し、解析してキャッシュします。このリストは失効した証明書の完全なリストを提供します。OCSP では、失効ステータスをよりスケーラブルな方法でチェックします。具体的には、証明書のステータスは、特定の証明書のステータスについて照会を行う検証機関によりローカライズされます。

証明書の一致規則を使用して、OCSP URL の上書きを設定できます。この上書きでは、リモートユーザ証明書の AIA フィールドの URL ではなく、失効ステータスをチェックする URL を指定します。一致規則により OCSP レスポンダ証明書の検証に使用するトラストポイントも設定されます。このトラストポイントにより、セキュリティ アプライアンスは自己署名証明書と、クライアント証明書の検証パスへの外部証明書を含む CA からのレスポンダ証明書を検証します。

証明書の一致規則を設定するには、暗号 CA トラストポイント モードで **match certificate** コマンドを使用します。この規則をコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

match certificate *map-name* **override ocsp [trustpoint** *trustpoint-name***]** *seq-num* **url** *URL*

no match certificate *map-name* **override ocsp**

シンタックスの説明

map-name	この規則に一致する証明書マップの名前を指定します。証明書マップを設定してから、一致規則を設定する必要があります。最大 65 文字です。
match certificate	この一致規則に証明書マップを指定します。
override ocsp	この規則は証明書の OCSP URL の上書きを目的とすることを指定します。
seq-num	この一致規則に優先順位を設定します。範囲は 1 ～ 10000 です。セキュリティ アプライアンスは、最初に一番小さいシーケンス番号を持つ一致規則を評価し、一致が見つかるまでより大きい番号を持つ一致規則を評価します。
trustpoint	（オプション）OCSP レスポンダ証明書の検証にトラストポイントを使用することを指定します。
trustpoint- name	（オプション）レスポンダ証明書を検証する上書きに使用するトラストポイントを指定します。
url	OCSP 失効ステータスの確認のために URL にアクセスすることを指定します。
URL	OCSP 失効ステータスを確認するためにアクセスする URL を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

OCSP を設定する際には、次のヒントに留意してください。

- トラストポイント コンフィギュレーション内に複数の一致規則を設定できますが、暗号 CA 証明書マップごとに設定できる一致規則は 1 つだけです。ただし、複数の暗号 CA 証明書マップを設定し、それらを同一のトラストポイントに関連付けることができます。
- 証明書マップを設定してから一致規則を設定する必要があります。
- 自己署名の OCSP レスポンダ証明書を検証するトラストポイントを設定するには、自己署名のレスポンダ証明書をそれ自体のトラストポイントに、信頼できる CA 証明書としてインポートします。次に、レスポンダ証明書の検証に、自己署名の OCSP レスポンダ証明書を含むトラストポイントを使用できるよう、トラストポイントを検証するクライアント証明書に **match certificate** コマンドを設定します。クライアント証明書の検証パスに含まれないレスポンダ証明書を検証する場合にも、同じように設定します。
- 同一の CA がクライアント証明書とレスポンダ証明書を発行する場合、トラストポイントは両方の証明書を検証できます。ただし、異なる CA がクライアント証明書とレスポンダ証明書を発行する場合は、各証明書に 1 つずつ、計 2 つのトラストポイントを設定する必要があります。
- OCSP サーバ（レスポンダ）証明書は通常、OCSP 応答に署名します。応答の受信後、セキュリティ アプライアンスはレスポンダ証明書を検証しようとします。CA は通常、OCSP レスポンダ証明書の期限を比較的短期間に設定して、その信用が失われる危険を最小限にします。また、CA のレスポンダ証明書には、証明書の失効ステータス確認が不要であることを示す ocsp-no-check 拡張も一般に含まれます。ただし、この拡張が含まれていない場合、セキュリティ アプライアンスはトラストポイントに指定したのと同じ方法で失効ステータスを確認します。レスポンダ証明書が検証できない場合は、失効チェックに失敗します。失効チェックが失敗しないようにするには、トラストポイントを検証するレスポンダ証明書に **revocation-check none** を設定すると同時に、クライアント証明書に **revocation-check ocsp** を設定します。
- セキュリティ アプライアンスは、一致しない場合に、**ocsp url** コマンドの URL を使用します。**ocsp url** コマンドを設定していない場合は、リモート ユーザ証明書の AIA フィールドが使用されます。証明書に AIA 拡張が含まれていない場合、失効ステータスのチェックは失敗します。

例

次の例では、newtrust というトラストポイントに証明書一致規則を作成する方法を示します。規則には mymap というマップ名、シーケンス番号 4、mytrust というトラストポイントが含まれ、URL 10.22.184.22 を指定します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint
mytrust 4 url 10.22.184.22
hostname(config-ca-trustpoint)#
```

次の例では、暗号 CA 証明書マップを設定後、一致証明書規則を設定して、CA 証明書が含まれるトラストポイントを指定し、レスポンダ証明書を検証する方法を段階的に示します。newtrust トラストポイントに指定された CA が OCSP レスポンダ証明書を発行しない場合に、この方法が必要になります。

ステップ 1　マップ規則が適用されるクライアント証明書を識別する証明書マップを設定します。次の例では、証明書マップの名前は mymap、シーケンス番号は 1 です。mycert と一致する CN アトリビュートが含まれるサブジェクト名を持つクライアント証明書は mymap エントリと一致します。

```
hostname(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
hostname(config-ca-cert-map)# subject-name attr cn eq mycert
hostname(config-ca-cert-map)#
```

ステップ 2　OCSP レスポンダ証明書を検証するための CA 証明書が含まれるトラストポイントを設定します。自己署名証明書の場合、これは自己署名証明書自体であり、インポート後にローカルに信頼されます。この目的で、外部の CA 登録を介して証明書を入手することもできます。プロンプトが表示されたら、CA 証明書に貼り付けます。

```
hostname(config-ca-cert-map)# exit
hostname(config)# crypto ca trustpoint mytrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint:     7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

ステップ 3　失効チェック方法として OCSP を使用して元のトラストポイント newtrust を設定します。次に、証明書マップ mymap、およびステップ 2 で設定した自己署名トラストポイント mytrust を含む一致規則を設定します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# enroll terminal
hostname(config-ca-trustpoint)# crypto ca authenticate newtrust

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint:     9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp
hostname(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint
mytrust 4 url 10.22.184.22
```

クライアント証明書の認証に newtrust トラストポイントを使用する接続では、クライアント証明書が mymap 証明書マップで指定したアトリビュート規則と一致するかどうかがチェックされます。その場合、セキュリティ アプライアンスは OCSP レスポンダ（10.22.184.22）にアクセスして、証明書の失効ステータスをチェックします。次に、mytrust トラストポイントを使用して、レスポンダ証明書が検証されます。

（注） newtrust トラストポイントを設定して、OCSP を介してクライアント証明書の有効性をチェックします。ただし、mytrust トラストポイントは失効チェックなし（デフォルト）に設定されているので、OCSP レスポンダ証明書に対して失効チェックは実行されません。

関連コマンド

コマンド	説明
crypto ca certificate map	暗号 CA 証明書マップを作成します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
crypto ca trustpoint	暗号 CA トラストポイント モードに入ります。このコマンドは、グローバル コンフィギュレーション モードで使用します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするための OCSP サーバを指定します。
revocation-check	失効のチェックに使用する方法（複数可）、およびその試行順序を指定します。

match cmd

ESMTP コマンド バーブに一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match cmd** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **cmd [verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

no match [**not**] **cmd [verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

シンタックスの説明

verb *verb*	ESMTP コマンド バーブを指定します。
line length gt *bytes*	行の長さを指定します。
RCPT count gt *recipients_number*	受信者の数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ESMTP 検査ポリシー マップに、ESMTP トランザクションで交換されるバーブ（メソッド）NOOP についての一致条件を設定する方法を示します。

```
hostname(config-pmap)# match cmd verb NOOP
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match default-inspection-traffic

クラス マップ内の inspect コマンドに対するデフォルトのトラフィックを指定するには、クラス マップ コンフィギュレーション モードで **match default-inspection-traffic** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match default-inspection-traffic

no match default-inspection-traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

各検査のデフォルトのトラフィックについては、「使用上のガイドライン」を参照してください。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** 文で定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに包含され、そのトラフィック クラスに関連付けられているアクションの対象になります。どのトラフィック クラスのどの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

match default-inspection-traffic コマンドを使用すると、個々の **inspect** コマンドのデフォルト トラフィックを一致させることができます。**match default-inspection-traffic** コマンドはその他の match コマンドの 1 つと併せて使用できます。このコマンドは、通常、***permit ip*** *src-ip dst-ip* 形式のアクセス リストです。

2 番目の **match** コマンドを **match default-inspection-traffic** コマンドと組み合せる際、**match default-inspection-traffic** コマンドを使用してプロトコルとポート情報を指定し、2 番目の **match** コマンドを使用して他のすべての情報（IP アドレスなど）を指定するという規則があります。2 番目の **match** コマンドで指定したプロトコルまたはポート情報は、**inspect** コマンドでは無視されます。

たとえば、次の例で指定するポート 65535 は無視されます。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)# match port 65535
```

検査用のデフォルトのトラフィックは次のとおりです。

検査タイプ	プロトコル タイプ	送信元ポート	宛先ポート
ctiqbe	tcp	該当なし	1748
dcerpc	tcp	該当なし	135
dns	udp	53	53
ftp	tcp	該当なし	21
gtp	udp	2123,3386	2123,3386
h323 h225	tcp	該当なし	1720
h323 ras	udp	該当なし	1718-1719
http	tcp	該当なし	80
icmp	icmp	該当なし	該当なし
ils	tcp	該当なし	389
im	tcp	該当なし	1-65539
ipsec-pass-thru	udp	該当なし	500
mgcp	udp	2427,2727	2427,2727
netbios	udp	137-138	該当なし
rpc	udp	111	111
rsh	tcp	該当なし	514
rtsp	tcp	該当なし	554
sip	tcp、udp	該当なし	5060
skinny	tcp	該当なし	2000
smtp	tcp	該当なし	25
sqlnet	tcp	該当なし	1521
tftp	udp	該当なし	69
xdmcp	udp	177	177

例

次の例は、クラス マップおよび **match default-inspection-traffic** コマンドを使用して、トラフィック クラスを定義する方法を示しています。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match default-inspection-traffic
hostname(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match any	すべてのトラフィックをクラス マップに含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dns-class

DNS Resource Record or Question（DNS リソース レコードまたはクエスチョン）セクションの Domain System Class（ドメイン システム クラス）に一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match dns-class** コマンドを使用します。設定済みのクラスを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

no match [**not**] **dns-class** {**eq** *c_well_known* | *c_val*} {**range** *c_val1 c_val2*}

シンタックスの説明

eq	完全一致を指定します。
c_well_known	既知の名前である IN により DNS クラスを指定します。
c_val	DNS クラス フィールドに任意の値（0 ～ 65535）を指定します。
range	範囲を指定します。
c_val1 c_val2	一致範囲を示す値を指定します。それぞれの値の範囲は、0 ～ 65535 です。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS メッセージのすべてのフィールド（クエスチョンと RR）を検査し、指定したクラスと照合します。DNS クエリーと DNS 応答の両方が確認されます。

一致対象は、**match not header-flag QR** と **match question** の 2 つのコマンドによって、DNS クエリーのクエスチョン部分にまで絞ることができます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップで、DNS クラスについての一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match dns-class eq IN
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dns-type

クエリー タイプと RR タイプを含む、DNS タイプの一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match dns-type** コマンドを使用します。設定した DNS タイプを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

no match [**not**] **dns-type** {**eq** *t_well_known* | *t_val*} {**range** *t_val1 t_val2*}

シンタックスの説明

eq	完全一致を指定します。
t_well_known	A、NS、CNAME、SOA、TSIG、IXFR、または AXFR といった既知の名前を使用して DNS タイプを指定します。
t_val	DNS タイプ フィールドに任意の値（0 ～ 65535）を指定します。
range	範囲を指定します。
t_val1 t_val2	一致範囲を示す値を指定します。それぞれの値の範囲は、0 ～ 65535 です。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS メッセージ（クエスチョンと RR）のすべてのセクションを検査し、指定したタイプと照合します。DNS クエリーと DNS 応答の両方が確認されます。

一致対象は、**match not header-flag QR** と **match question** の 2 つのコマンドによって、DNS クエリーのクエスチョン部分にまで絞ることができます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップで、DNS タイプの一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match dns-type eq a
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match domain-name

DNS メッセージ ドメイン名リストに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match domain-name** コマンドを使用します。設定済みのセクションを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **domain-name regex** *regex_id*

match [**not**] **domain-name regex class** *class_id*

no match [**not**] **domain-name regex** *regex_id*

no match [**not**] **domain-name regex class** *class_id*

シンタックスの説明

regex	正規表現を指定します。
regex_id	正規表現 ID を指定します。
class	複数の正規表現エントリを含むクラス マップを指定します。
class_id	正規表現クラス マップ ID を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは DNS メッセージのドメイン名と定義済みリストを照合します。圧縮されているドメイン名は拡張後、照合されます。他の DNS **match** コンドと組み合せて一致条件を特定のフィールドに絞り込みます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップの DNS ドメイン名を照合する方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match domain-name regex
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dscp

クラス マップ内の IETF 定義の DSCP 値（IP ヘッダー内）を指定するには、クラス マップ コンフィギュレーション モードで **match dscp** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match dscp {***values***}

no match dscp {***values***}

シンタックスの説明

values	IP ヘッダー内の最大 8 つの異なる IETF 定義の DSCP 値を指定します。範囲は 0 ～ 63 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** 文で定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに包含され、そのトラフィック クラスに関連付けられているアクションの対象になります。どのトラフィック クラスのどの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

match dscp コマンドを使用すると、IP ヘッダー内の IETF 定義の DSCP 値を一致させることができます。

例

次の例は、クラス マップおよび **match dscp** コマンドを使用して、トラフィック クラスを定義する方法を示しています。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match dscp af43 cs1 ef
hostname(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match port	該当するインターフェイスで受信されるパケットの比較基準として、TCP/UDP ポートを指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match ehlo-reply-parameter

ESMTP ehlo 応答パラメータに一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match ehlo-reply-parameter** コンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **ehlo-reply-parameter** *parameter*

no match [**not**] **ehlo-reply-parameter** *parameter*

シンタックスの説明

parameter	ehlo 応答パラメータを指定します。値には、8bitmime、auth、binarymime、checkpoint、dsn、etrn、others、pipelining、size、および vrfy が含まれます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ESMTP 検査ポリシー マップで、ehlo 応答パラメータに関する一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match ehlo-reply-parameter auth
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match filename

FTP 転送のファイル名に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match filename** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、FTP 検査クラス マップで、FTP 転送ファイル名に関する一致条件を設定する方法を示します。

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from
accessing /root
hostname(config-cmap)# match username regex class ftp_regex_user
hostname(config-cmap)# match filename regex ftp-file
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match filetype

FTP 転送のファイル タイプに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match filetype** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例は FTP 検査ポリシー マップで FTP 転送ファイル タイプに関する一致条件を設定する方法を示します。

```
hostname(config-pmap)# match filetype class regex ftp-regex-filetype
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match flow ip destination-address

クラス マップ内のフロー IP の宛先アドレスを指定するには、クラス マップ コンフィギュレーション モードで **match flow ip destination-address** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match flow ip destination-address

no match flow ip destination-address

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** 文で定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに包含され、そのトラフィック クラスに関連付けられているアクションの対象になります。どのトラフィック クラスのどの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

トンネル グループでフローベースのポリシー アクションをイネーブルにするには、**match flow ip destination-address** と **match tunnel-group** コマンドを **class-map**、**policy-map**、および **service-policy** コマンドと併せて使用します。フローを定義する基準は、宛先 IP アドレスです。一意の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。ポリシーのアクションは、トラフィック クラス全体ではなく各フローに適用されます。**match flow ip destination-address** コマンドを使用すると、QoS アクション ポリシングが適用されます。トンネル グループ内の各トンネルを、指定したレートにポリシングするには、**match tunnel-group** を使用します。

例

次の例は、トンネル グループ内でフロー ベースのポリシングをイネーブルにして、各トンネルを指定したレートに制限する方法を示しています。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match tunnel-group
hostname(config-cmap)# match flow ip destination-address
hostname(config-cmap)# exit
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# police 56000
hostname(config-pmap)# exit
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。
tunnel-group	VPN の接続固有レコードのデータベースを作成および管理します。

match header

ESMTP ヘッダーに一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match header** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **header [length gt** *bytes* | **to-fields count gt** *to_fields_number*]

no match [**not**] **header [length gt** *bytes* | **to-fields count gt** *to_fields_number*]

シンタックスの説明

length gt *bytes*	ESMTP ヘッダー メッセージの長さを照合することを指定します。
to-fields count gt *to_fields_number*	To：フィールドの数を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ESMTP 検査ポリシー マップで、ヘッダーに関して一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match header length gt 512
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match header-flag

DNS ヘッダー フラグに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match header-flag** コマンドを使用します。設定したヘッダー フラグを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **header-flag** [**eq**] {*f_well_known* | *f_value*}

no match [**not**] **header-flag** [**eq**] {*f_well_known* | *f_value*}

シンタックスの説明

eq	完全一致を指定します。設定されていない場合、**match-all** ビット マスク一致を指定します。
f_well_known	既知の名前を使用して DNS ヘッダー フラグ ビットを指定します。複数のフラグ ビットを入力でき、その場合は論理的に OR 関係になります。 QR（Query; クエリー）（注：QR=1 は、DNS 応答を示します） AA（Authoritative Answer; 権威ある回答） TC（TrunCation; 短縮） RD（Recursion Desired; 再帰要求） RA（Recursion Available; 再帰可能）
f_value	16 進数形式で任意の 16 ビット値を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、DNS クラス マップまたはポリシー マップ内で設定できます。DNS クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップで、DNS ヘッダー フラグに関する一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match header-flag AA
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match im-subscriber

SIP IM サブスクライバに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match im-subscriber** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、SIP 検査クラス マップで、SIP IM サブスクライバに関して一致条件を設定する方法を示します。

```
hostname(config-cmap)# match im-subscriber regex class im_sender
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match invalid-recipients

ESMTP の無効な受信者アドレスに関する一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match invalid-recipients** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **invalid-recipients count gt** *number*

no match [**not**] **invalid-recipients count gt** *number*

シンタックスの説明

count gt *number*	無効な受信者番号を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ESMTP 検査ポリシー マップで、無効な受信者数に関して一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match invalid-recipients count gt 1000
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match ip address

指定したいずれかのアクセス リストによって渡されたルート アドレスまたは一致パケットを持つ、すべてのルートを再配布するには、ルートマップ コンフィギュレーション モードで **match ip address** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

match ip address {*acl...*}

no match ip address {*acl...*}

シンタックスの説明

acl	アクセス リストの名前。複数のアクセス リストを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルートマップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、**match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する、個々の再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

例

次の例は、内部ルートを再配布する方法を示しています。

```
hostname(config)# route-map name
hostname(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したいずれかのアクセス リストによって渡されたネクストホップ ルータ アドレスを持つ、すべてのルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。
set metric	ルートマップの宛先ルーティング プロトコルのメトリック値を指定します。

match ip next-hop

指定したいずれかのアクセス リストによって渡されたネクストホップ ルータ アドレスを持つ、すべてのルートを再配布するには、ルートマップ コンフィギュレーション モードで **match ip next-hop** コマンドを使用します。ネクストホップ エントリを削除するには、このコマンドの **no** 形式を使用します。

match ip next-hop {*acl...*} | ***prefix-list prefix_list***

no match ip next-hop {*acl...*} | ***prefix-list prefix_list***

シンタックスの説明

acl	ACL の名前。複数の ACL を指定できます。
prefix-list *prefix_list*	プレフィックス リストの名前。

デフォルト

ネクストホップ アドレスに一致する必要なく、ルートが自由に配布されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルートマップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

コマンド シンタックスの省略形（...）は、コマンド入力で *acl* 引数に複数の値を含めることができることを示します。

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、**match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する、個々の再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

match ルートマップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートの再配布を実行するには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルートマップを通じてルートを渡す場合、ルートマップはいくつかの部分に分かれることがあります。**route-map** コマンドに関連付けられているどの match 節にも一致しないルートは、すべて無視されます。一部のデータのみを修正するには、2 番目のルートマップ セクションを設定して、正確に一致する基準を指定する必要があります。

例

次の例は、acl_dmz1 または acl_dmz2 のアクセス リストによって渡されたネクストホップ ルータ アドレスを持つルートを配布する方法を示しています。

```
hostname(config)# route-map name
hostname(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したいずれかのアクセス リストによって渡されたネクストホップ ルータ アドレスを持つ、すべてのルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。
set metric	ルートマップの宛先ルーティング プロトコルのメトリック値を指定します。

match ip route-source

ルータによってアドバタイジングされ、ACL で指定されたアドレスのサーバにアクセスするルートを再配布するには、ルートマップ コンフィギュレーション モードで **match ip route-source** コマンドを使用します。ネクストホップ エントリを削除するには、このコマンドの **no** 形式を使用します。

match ip route-source {*acl...*} | ***prefix-list prefix_list***

no match ip route-source {*acl...*}

シンタックスの説明

acl	ACL の名前。複数の ACL を指定できます。
prefix_list	プレフィックス リストの名前。

デフォルト

ルートの送信元では、フィルタリングは実行されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルートマップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

コマンド シンタックスの省略形（...）は、コマンド入力で access-list-name 引数に複数の値を含めることができることを示します。

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、**match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する、個々の再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

match ルートマップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートの再配布を実行するには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルートマップは、いくつかの部分に分かれることがあります。**route-map** コマンドに関連付けられているどの match 節にも一致しないルートは、すべて無視されます。一部のデータのみを修正するには、2 番目のルートマップ セクションを設定して、正確に一致する基準を指定する必要があります。ルートのネクストホップおよび送信元ルータのアドレスは、状況によって異なります。

例

次の例は、ルータによってアドバタイジングされ、acl_dmz1 および acl_dmz2 の ACL で指定されたアドレスのサーバにアクセスするルートを配布する方法を示しています。

```
hostname(config)# route-map name
hostname(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したいずれかの ACL によって渡されたネクストホップ ルータ アドレスを持つ、すべてのルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。
set metric	ルートマップの宛先ルーティング プロトコルのメトリック値を指定します。

match media-type

H.323 メディア タイプに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match media-type** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **media-type [audio | data | video]**

no match [**not**] **media-type [audio | data | video]**

シンタックスの説明

audio	オーディオ メディア タイプと照合することを指定します。
data	データ メディア タイプと照合することを指定します。
video	ビデオ メディア タイプと照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、H.323 検査クラス マップで、オーディオ メディア タイプに関して一致条件を設定する方法を示します。

```
hostname(config-cmap)# match media-type audio
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match message id

GTP メッセージ ID に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match message id** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message id [***message_id* | **range** *lower_range upper_range*]

no match [**not**] **message id [***message_id* | **range** *lower_range upper_range*]

シンタックスの説明

message_id	1 ～ 255 の範囲の英数字 ID を指定します。
range *lower_range upper_range*	ID の下位と上位を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップ内で設定できます。GTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、GTP 検査クラス マップで、メッセージ ID に関して一致条件を設定する方法を示します。

```
hostname(config-cmap)# match message id 33
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match message length

GTP メッセージ ID に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match message length** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message length min** *min_length* **max** *max_length*

no match [**not**] **message length min** *min_length* **max** *max_length*

シンタックスの説明

min *min_length*	メッセージ ID の最小の長さを指定します。値の範囲は、1 ～ 65536 です。
max *max_length*	メッセージ ID の最大長を指定します。値の範囲は、1 ～ 65536 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップ内で設定できます。GTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、GTP 検査クラス マップで、メッセージの長さに関して一致条件を設定する方法を示します。

```
hostname(config-cmap)# match message length min 8 max 200
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match message-path

Via ヘッダー フィールドでの指定のとおりに、SIP メッセージによって取得されるパスに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match message-path** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例は、SIP 検査クラス マップの SIP メッセージによって取得されるパスに関して、一致条件を設定する方法を示しています。

```
hostname(config-cmap)# match message-path regex class sip_message
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match mime

ESMTP mime エンコード タイプ、mime ファイル名の長さ、または mime ファイル タイプについて一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match mime** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **mime [encoding** *type* **| filename length gt** *bytes* **| filetype** *regex***]**

no match [**not**] **mime [encoding** *type* **| filename length gt** *bytes* **| filetype** *regex***]**

シンタックスの説明

encoding *type*	エンコード タイプを照合することを指定します。
filename length gt *bytes*	ファイル名の長さを照合することを指定します。
filetype *regex*	ファイル タイプを照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ESMTP 検査ポリシー マップで、mime ファイル名の長さに関して一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect esmtp esmtp_map
hostname(config-pmap)# match mime filename length gt 255
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match port

モジュラ ポリシー フレームワークを使用する場合、クラス マップ コンフィギュレーション モードで **match port** コマンドを使用して、アクションを適用する TCP ポートまたは UDP ポートを照合します。**match port** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

no match port {**tcp** | **udp**} {**eq** *port* | **range** *beg_port end_port*}

シンタックスの説明

eq port	ポート名または番号を 1 つ指定します。
range beg_port end_port	ポート範囲の開始値と終了値（1 ～ 65535）を指定します。
tcp	TCP ポートを指定します。
udp	UDP ポートを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。

   class-map コマンドの入力後に、**matchport** コマンドを入力してトラフィックを指定します。あるいは、**match access-list** コマンドなど、異なるタイプの **match** コマンドを入力します（**class-map type management** コマンドのみが match port コマンドを許可します）。クラス マップには、**match port** コマンドを 1 つだけ含めることができます。それを別のタイプの **match** コマンドと組み合せることはできません。
2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのための特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスに対するアクションを有効にします。

例

次の例は、クラス マップおよび **match port** コマンドを使用して、トラフィック クラスを定義する方法を示しています。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 8080
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match access-list	アクセス リストに従って、トラフィックを照合します。
match any	すべてのトラフィックをクラス マップに含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match precedence

クラス マップ内の優先順位値を指定するには、クラス マップ コンフィギュレーション モードで **match precedence** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match precedence *value*

no match precedence *value*

シンタックスの説明

value	スペースで区切った最大 4 つの優先順位値を指定します。範囲は 0 ～ 7 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** 文で定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに包含され、そのトラフィック クラスに関連付けられているアクションの対象になります。どのトラフィック クラスのどの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

IP ヘッダー内の TOS バイトで表現された値を指定するには、**match precedence** コマンドを使用します。

例

次の例は、クラス マップおよび **match precedence** コマンドを使用して、トラフィック クラスを定義する方法を示しています。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match precedence 1
hostname(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match any	すべてのトラフィックをクラス マップに含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match question

DNS クエスチョンまたはリソース レコードに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match question** コマンドを使用します。設定済みのセクションを削除するには、このコマンドの **no** 形式を使用します。

match {**question** | {**resource-record answer** | **authority** | **additional**}}

no match {**question** | {**resource-record answer** | **authority** | **additional**}}

シンタックスの説明

question	DNS メッセージのクエスチョン部分を指定します。
resource-record	DNS メッセージのリソース レコード部分を指定します。
answer	Answer（回答）RR セクションを指定します。
authority	Authority（権威）RR セクションを指定します。
additional	Additional（追加）RR セクションを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS ヘッダーを検査し、指定したフィールドと照合します。他の DNS **match** コマンドと組み合せて使用し、特定のクエスチョンまたは RR タイプの検査を定義します。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、DNS 検査ポリシー マップで、DNS クエスチョンに関して一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# match question
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request-command

特定の FTP コマンドを制限するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match request-command** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **request-command** *ftp_command* [*ftp_command...*]

no match [**not**] **request-command** *ftp_command* [*ftp_command...*]

シンタックスの説明

ftp_command	制限する 1 つまたは複数の FTP コマンドを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、FTP 検査ポリシー マップで、特定の FTP コマンドに関して一致条件を設定する方法を示します。

```
hostname(config)# policy-map type inspect ftp ftp_map1
hostname(config-pmap)# match request-command stou
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request-method

SIP メソッド タイプに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match request-method** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **request-method** *method_type*

no match [**not**] **request-method** *method_type*

シンタックスの説明

method_type	RFC 3261 とサポートされる拡張機能に応じてメソッド タイプを指定します。サポートされるメソッド タイプは、ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例は、SIP 検査クラス マップの SIP メッセージによって取得されるパスに関して、一致条件を設定する方法を示しています。

```
hostname(config-cmap)# match request-method ack
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match route-type

指定したタイプのルートを再配布するには、ルートマップ コンフィギュレーション モードで **match route-type** コマンドを使用します。ルート タイプ エントリを削除するには、このコマンドの **no** 形式を使用します。

match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

no match route-type {**local** | **internal** | {**external** [**type-1** | **type-2**]} | {**nssa-external** [**type-1** | **type-2**]}}

シンタックスの説明

local	ローカルに生成された BGP ルート。
internal	OSPF のエリア内ルートおよびエリア間ルート、または EIGRP の内部ルート。
external	OSPF の外部ルートまたは EIGRP の外部ルート。
type-1	（オプション）ルート タイプ 1 を指定します。
type-2	（オプション）ルート タイプ 2 を指定します。
nssa-external	外部 NSSA を指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルートマップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、**match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する、個々の再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

match ルートマップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートの再配布を実行するには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルートマップは、いくつかの部分に分かれることがあります。**route-map** コマンドに関連付けられているどの match 節にも一致しないルートは、すべて無視されます。一部のデータのみを修正するには、2 番目のルートマップ セクションを設定して、正確に一致する基準を指定する必要があります。

OSPF の場合、**external type-1** キーワードはタイプ 1 外部ルートにだけ一致し、**external type-2** キーワードはタイプ 2 外部ルートにだけ一致します。

例

次の例は、内部ルートを再配布する方法を示しています。

```
hostname(config)# route-map name
hostname(config-route-map)# match route-type internal
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したいずれかのアクセス リストによって渡されたネクストホップ ルータ アドレスを持つ、すべてのルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。
set metric	ルートマップの宛先ルーティング プロトコルのメトリック値を指定します。

match rtp

クラス マップ内の偶数ポートの UDP ポート範囲を指定するには、クラス マップ コンフィギュレーション モードで **match rtp** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match rtp *starting_port range*

no match rtp *starting_port range*

シンタックスの説明

starting_port	偶数の UDP 宛先ポートの下限を指定します。範囲は、2000 ～ 65535 です。
range	RTP ポートの範囲を指定します。範囲は、0 ～ 16383 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** 文で定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに包含され、そのトラフィック クラスに関連付けられているアクションの対象になります。どのトラフィック クラスのどの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

RTP ポート（*starting_port* ～ *starting_port* に *range* を加えた範囲の UDP の偶数ポート番号）に一致させるには、**match rtp** コマンドを使用します。

例

次の例は、クラス マップおよび **match rtp** コマンドを使用して、トラフィック クラスを定義する方法を示しています。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match rtp 20000 100
hostname(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
match any	すべてのトラフィックをクラス マップに含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match sender-address

ESMTP 送信者電子メール アドレスについて一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match sender-address** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

match [**not**] **sender-address [length gt** *bytes* **|** **regex** *regex***]**

no match [**not**] **sender-address [length gt** *bytes* **|** **regex** *regex***]**

シンタックスの説明

length gt *bytes*	送信者電子メール アドレスの長さを照合することを指定します。
regex *regex*	正規表現を照合することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ESMTP 検査ポリシー マップで、320 文字を超える長さの送信者電子メール アドレスに関して一致条件を設定する方法を示します。

```
hostname(config-pmap)# match sender-address length gt 320
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match server

FTP サーバに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match server** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、FTP 検査ポリシー マップで、FTP サーバに関して一致条件を設定する方法を示します。

```
hostname(config-pmap)# match server class regex ftp-server
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match third-party-registration

サード パーティー登録の要求者に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match third-party-registration** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップでは、入力できるエントリは 1 つのみです。

match third-party-registration コマンドは、SIP レジスタまたは SIP プロキシを使用して他のユーザを登録できるユーザを特定するために使用します。From 値と To 値が一致しない場合には、REGISTER メッセージの From ヘッダー フィールドにより特定されます。

例

次の例では、SIP 検査クラス マップで、サードパーティーの登録に関して一致条件を設定する方法を示します。

```
hostname(config-cmap)# match third-party-registration regex class sip_regist
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match tunnel-group

すでに定義されているトンネル グループに属するクラス マップ内のトラフィックに一致させるには、クラス マップ コンフィギュレーション モードで **match tunnel-group** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

match tunnel-group *name*

no match tunnel-group *name*

シンタックスの説明

name	トンネル グループ名のテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各種の **match** コマンドを使用して、クラス マップのトラフィック クラスに含まれるトラフィックを指定します。これらのコマンドは、クラス マップに含まれるトラフィックを定義するためのさまざまな基準を保持しています。トラフィック クラスは、モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定するときに、その一環として **class-map** グローバル コンフィギュレーション コマンドを使用して定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィック クラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラス マップの **match** 文で定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに包含され、そのトラフィック クラスに関連付けられているアクションの対象になります。どのトラフィック クラスのどの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

フローベースのポリシー アクションをイネーブルにするには、**match flow ip destination-address** と **match tunnel-group** コマンドを **class-map**、**policy-map**、および **service-policy** コマンドと併せて使用します。フローを定義する基準は、宛先 IP アドレスです。一意の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。ポリシーのアクションは、トラフィック クラス全体ではなく各フローに適用されます。**police** コマンドを使用すると、QoS アクション ポリシングが適用されます。トンネル グループ内の各トンネルを、指定したレートにポリシングするには、**match tunnel-group** を **match flow ip destination-address** と併せて使用します。

例

次の例は、トンネル グループ内でフロー ベースのポリシングをイネーブルにして、各トンネルを指定したレートに制限する方法を示しています。

```
hostname(config)# class-map cmap
hostname(config-cmap)# match tunnel-group
hostname(config-cmap)# match flow ip destination-address
hostname(config-cmap)# exit
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# police 56000
hostname(config-pmap)# exit
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラス マップ内のアクセス リスト トラフィックを指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。
tunnel-group	IPSec および L2TP の接続固有レコードのデータベースを作成および管理します。

match uri

SIP ヘッダーの URI に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match uri** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **uri** {**sip** | **tel**} **length gt** *gt_bytes*

no match [**not**] **uri** {**sip** | **tel**} **length gt** *gt_bytes*

シンタックスの説明

sip	SIP URI を指定します。
tel	TEL URI を指定します。
length gt *gt_bytes*	URI の最大長を指定します。値の範囲は、0 ～ 65536 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、SIP メッセージの URI に関して一致条件を設定する方法を示します。

```
hostname(config-cmap)# match uri sip length gt
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match username

FTP ユーザ名に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match username** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

no match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

シンタックスの説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現クラス マップを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、FTP 検査クラス マップで FTP ユーザ名に関して一致条件を設定する方法を示します。

```
hostname(config)# class-map type inspect ftp match-all ftp_class1
hostname(config-cmap)# match username regex class ftp_regex_user
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match version

GTP メッセージ ID に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match message length** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

no match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

シンタックスの説明

vresion_id	0 ～ 255 の範囲のバージョンを指定します。
range *lower_range upper_range*	バージョンの上位と下位の範囲を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーションまたはポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、GTP クラス マップまたは GTP ポリシー マップ内で設定できます。GTP クラス マップでは、入力できるエントリは 1 つのみです。

例

次の例では、GTP 検査クラス マップでメッセージ バージョンに関して一致条件を設定する方法を示します。

```
hostname(config-cmap)# match version 1
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
clear configure class-map	すべてのクラス マップを削除します。
match any	すべてのトラフィックをクラス マップに含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

max-failed-attempts

サーバ グループ内のある特定のサーバに対して許容される失敗数（失敗数がこれを超えるとそのサーバが無効になる）を指定するには、AAA サーバ グループ モードで **max-failed-attempts** コマンドを使用します。この指定を削除し、デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

max-failed-attempts *number*

no max-failed-attempts

シンタックスの説明

number	1 ～ 5 の範囲の整数。前の **aaa-server** コマンドで指定したサーバ グループ内の所定のサーバで許可される失敗数を指定します。

デフォルト

number のデフォルト値は 3 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ グループ	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行する前に、AAA サーバ / グループを設定しておく必要があります。

例

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-server-group)# max-failed-attempts 4
hostname(config-aaa-server-group)#
```

関連コマンド

コマンド	説明
aaa-server *server-tag* **protocol** *protocol*	AAA サーバ グループ コンフィギュレーション モードに入って、グループ内のすべてのホストに共通する、グループ固有の AAA パラメータを設定できるようにします。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

max-forwards-validation

Max-forwards ヘッダー フィールドが 0 であるかどうかのチェックをイネーブルにするには、パラメータ コンフィギュレーション モードで **max-forwards-validation** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

max-forwards-validation action {drop | drop-connection | reset | log} [log]

no max-forwards-validation action {drop | drop-connection | reset | log} [log]

シンタックスの説明

drop	違反が発生した場合、パケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
log	違反が発生した場合、独自または追加のログを記録することを指定します。このアクションは、任意のアクションに関連付けることができます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは宛先までのホップ数をカウントします。宛先に到達する前に、ホップ数が 0 になることはありません。

例

次の例では、SIP 検査ポリシー マップで max-forwards-validation をイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# max-forwards-validation action log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

max-header-length

HTTP ヘッダー長に基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **max-header-length** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

no max-header-length {**request** *bytes* [**response** *bytes*] | **response** *bytes*} **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクション。
allow	メッセージを許可します。
drop	接続を終了します。
bytes	バイト数（範囲は 1 ～ 65,535）。
log	（オプション）syslog を生成します。
request	要求メッセージ。
reset	TCP リセット メッセージをクライアントとサーバに送信します。
response	（オプション）応答メッセージ。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

max-header-length コマンドをイネーブルにすると、セキュリティ アプライアンスは、設定された制限内の HTTP ヘッダーを持つメッセージだけを許可します。それ以外の場合は、指定されたアクションを実施します。セキュリティ アプライアンスが TCP 接続をリセットして syslog エントリをオプションで作成するようにするには、**action** キーワードを使用します。

例

次の例では、HTTP 要求を 100 バイト以下の HTTP ヘッダーを持つものに限定します。ヘッダーが大きすぎる場合、セキュリティ アプライアンスが TCP 接続をリセットし、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-header-length request bytes 100 action log reset
hostname(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

max-object-size

セキュリティ アプライアンスが、WebVPN セッションに対してキャッシュできるオブジェクトの最大サイズを設定するには、キャッシュ モードで max-object-size コマンドを使用します。サイズを変更するには、このコマンドを再度使用します。

max-object-size *integer range*

シンタックスの説明

integer range	0 ～ 10000 KB

デフォルト

1000 KB

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

最大オブジェクト サイズは、最小オブジェクト サイズよりも大きくする必要があります。キャッシュ圧縮がイネーブルである場合、セキュリティ アプライアンスは、オブジェクト圧縮後のサイズを計算します。

例

次の例では、最大オブジェクト サイズである 4000 KB に設定する方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# max-object-size 4000
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシングをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再確認ポリシーを設定します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

max-uri-length

HTTP 要求メッセージの URI 長に基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **max-uri-length** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

no max-uri-length *bytes* **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクション。
allow	メッセージを許可します。
drop	接続を終了します。
bytes	バイト数（範囲は 1 ～ 65,535）。
log	（オプション）syslog を生成します。
reset	TCP リセット メッセージをクライアントとサーバに送信します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

max-uri-length コマンドをイネーブルにすると、セキュリティ アプライアンスは、設定された制限内の URI を持つメッセージだけを許可します。それ以外の場合は、指定されたアクションを実施します。セキュリティ アプライアンスが TCP 接続をリセットして syslog エントリを作成するようにするには、**action** キーワードを使用します。

設定した値以下の長さを持つ URI が許可されます。それ以外の場合は、指定されたアクションが実施されます。

例

次の例では、HTTP 要求を 100 バイト以下の URI を持つものに限定します。URI が大きすぎる場合、セキュリティ アプライアンスが TCP 接続をリセットし、syslog エントリを作成します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# max-uri-length 100 action reset log
hostname(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

mcc

IMSI プレフィックス フィルタリングのモバイル国番号とモバイル ネットワーク番号を指定するには、GTP マップ コンフィギュレーション モードで **mcc** コマンドを使用します。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

mcc *country_code* ***mnc*** *network_code*

no mcc *country_code* ***mnc*** *network_code*

シンタックスの説明

country_code	モバイル国番号を指定する 0（ゼロ）以外の 3 桁の値。1 桁または 2 桁のエントリは先頭に 0 が追加され、3 桁の値に生成されます。
network_code	ネットワーク番号を指定する 2 桁または 3 桁の値。

デフォルト

デフォルトでは、セキュリティ アプライアンスは有効な MCC/MNC の組み合せをチェックしません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、IMSI プレフィックス フィルタリング用に使用します。受信されたパケットの IMSI 内の MCC と MNC が、このコマンドで設定した MCC/MNC と比較され、一致しない場合にドロップされます。

IMSI プレフィックス フィルタリングをイネーブルにするには、このコマンドを使用する必要があります。許可された MCC と MNC の組み合せを指定するのに、複数のインスタンスを設定できます。デフォルトでは、セキュリティ アプライアンスが MNC と MCC の組み合せの有効性をチェックしないので、設定された組み合せの有効性を確認する必要があります。MCC と MNC 番号の詳細については、ITU E.212 の推奨事項である『*Identification Plan for Land Mobile Stations*』を参照してください。

例

次の例では、111 の MCC と 222 の MNC で IMSI プレフィックス フィルタリングのトラフィックを指定します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# mcc 111 mnc 222
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

media-type

メディア タイプを銅線またはファイバ ギガビット イーサネットに設定するには、インターフェイス コンフィギュレーション モードで **media-type** コマンドを使用します。ファイバ SFP コネクタは、ASA 5500 シリーズ適応型セキュリティ アプライアンスの 4GE SSM で使用できます。メディア タイプの設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

media-type {***rj45*** | ***sfp***}

no media-type [***rj45*** | ***sfp***]

シンタックスの説明

rj45	（デフォルト）メディア タイプを RJ-45 銅線コネクタに設定します。
sfp	メディア タイプをファイバ SFP コネクタに設定します。

デフォルト

デフォルトは **rj45** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)(4)	このコマンドが導入されました。

使用上のガイドライン

sfp 設定は固定速度（1,000 Mbps）を使用するので、**speed** コマンドを使用すると、インターフェイスがリンク パラメータをネゴシエートするかどうかを設定できます。**duplex** コマンドは、***sfp*** ではサポートされていません。

例

次の例では、メディア タイプを SFP に設定します。

```
hostname(config)# interface gigabitethernet1/1
hostname(config-if)# media-type sfp
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

member

コンテキストをリソース クラスに割り当てるには、コンテキスト コンフィギュレーション モードで **member** コマンドを使用します。コンテキストをクラスから削除するには、このコマンドの **no** 形式を使用します。

member *class_name*

no member *class_name*

シンタックスの説明

class_name	**class** コマンドを使用して作成したクラス名を指定します。

デフォルト

デフォルトでは、コンテキストはデフォルト クラスに割り当てられます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
コンテキスト コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、コンテキストごとの上限値が適用されていない限り、すべてのセキュリティ コンテキストがセキュリティ アプライアンスのリソースに無制限にアクセスできます。ただし、1 つまたは複数のコンテキストがリソースを大量に消費しているために、他のコンテキストで接続が拒否されていることが分かった場合などは、リソース管理を設定することによって、リソースの使用をコンテキストごとに制限できます。セキュリティ アプライアンスでは、コンテキストをリソース クラスに割り当てることでリソースを管理します。各コンテキストは、クラスによって設定されるリソース制限値を使用します。

例

次の例では、test というコンテキストを gold というクラスに割り当てます。

```
hostname(config-ctx)# context test
hostname(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
hostname(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
hostname(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
hostname(config-ctx)# config-url ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
hostname(config-ctx)# member gold
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
limit-resource	リソースに対して制限を設定します。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

memory caller-address

メモリ問題を分離できるように、コール トレース用のプログラム メモリの特定の範囲を設定するには、特権 EXEC モードで ***memory caller-address*** コマンドを使用します。発信者 PC は、メモリ割り当てプリミティブを呼び出したプログラムのアドレスです。アドレスの範囲を削除するには、このコマンドの **no** 形式を使用します。

memory caller-address *startPC endPC*

no memory caller-address

シンタックスの説明

endPC	メモリ ブロックの終了アドレス範囲を指定します。
startPC	メモリ ブロックの開始アドレス範囲を指定します。

デフォルト

実際の発信者 PC が、メモリ トレース用に記録されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

メモリ問題を特定のメモリ ブロックに分離するには、***memory caller-address*** コマンドを使用します。

場合によっては、メモリ割り当てプリミティブの実際の発信者 PC が、プログラムの多くの場所で使用されている既知のライブラリ機能になります。プログラムの個々の場所を分離するには、ライブラリ機能の開始および終了プログラム アドレスを設定して、ライブラリ機能のプログラムの発信者アドレスが記録されるようにします。

（注） 発信者アドレスのトレースをイネーブルにすると、セキュリティ　アプライアンスのパフォーマンスが一時的に低下することがあります。

例

次の例は、***memory caller-address*** コマンドで設定したアドレス範囲、および ***show memory-caller address*** コマンドによる表示結果を示しています。

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464

hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況のモニタリング（メモリ プロファイリング）をイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレスの範囲を表示します。

memory delayed-free-poisoner enable

delayed free-memory poisoner ツールをイネーブルにするには、特権 EXEC モードで **memory delayed-free-poisoner enable** コマンドを使用します。delayed free-memory poisoner ツールをディセーブルにするにするには、このコマンドの **no** 形式を使用します。delayed free-memory poisoner ツールを使用すると、アプリケーションに解放された後のメモリの変化を監視することができます。

memory delayed-free-poisoner enable

no memory delayed-free-poisoner enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

memory delayed-free-poisoner enable コマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

delayed free-memory poisoner ツールをイネーブルにすると、メモリ使用状況およびシステム パフォーマンスに重大な影響を及ぼします。このコマンドは、Cisco TAC の指導の下で使用する必要があります。システムの使用頻度が高いときは、実稼働環境でこのコマンドを使用しないでください。

このツールをイネーブルにすると、セキュリティ アプライアンスで実行中のアプリケーションからメモリを解放する要求が FIFO キューに書き込まれます。各要求が FIFO キューに書き込まれると、低レベルのメモリ管理に不要なメモリ中の関連付けられたバイトは、値 0xcc が書き込まれて「無効化」されます。

メモリ解放要求は、空きメモリ プールよりも多くのメモリがアプリケーションに必要になるまで、キューに保持されます。メモリが必要になると、最初のメモリ解放要求がキューから引き出され、無効化されたメモリが検証されます。

メモリが変更されなかった場合、このメモリは低レベル メモリ プールに戻され、delayed free-memory poisoner ツールは、最初の要求を行ったアプリケーションからメモリ要求を再発行します。このプロセスは、要求しているアプリケーションにとって十分なメモリが解放されるまで続行されます。

無効化されたメモリが変更済みの場合、クラッシュが発生し、クラッシュの原因を判断するための診断が出力されます。

delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。**memory delayed-free-poisoner validate** コマンドを使用して、手動で検証を開始することもできます。

このコマンドの **no** 形式を実行すると、キュー内の要求が参照しているすべてのメモリは空きメモリ プールに戻され、それらのメモリの検証および統計カウンタの消去は行われません。

例

次の例では、delayed free-memory poisoner ツールをイネーブルにしています。

```
hostname# memory delayed-free-poisoner enable
```

次に、delayed free-memory poisoner ツールが不正なメモリ再使用を検出した場合の出力例を示します。

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.

    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15

Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........

An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.

assertion "0" failed: file "delayfree.c", line 191
```

表 20-1 で、上記の出力の重要な部分を説明します。

表 20-1　不正なメモリ使用の出力に関する説明

フィールド	説明
heap region	要求を行っているアプリケーションが使用できるアドレス領域とメモリ領域のサイズ。これは要求されたサイズと同じではありません。要求されたサイズは、メモリ要求が行われた時点でシステムがメモリを区分したサイズよりも小さくなる場合があります。
memory address	メモリ中の異常が検出された場所。
byte offset	byte offset はヒープ領域の先頭からの相対位置で、実行結果を使用してこのアドレスから始まるデータ構造を格納した場合、変更されたフィールドの検索に使用できます。値が 0 の場合、またはヒープ領域バイト カウントよりも値が大きい場合、問題は低レベル ヒープ パッケージの予期しない値であることを示している可能性があります。
allocated by/freed by	特定のメモリ領域を対象にした最後の malloc/calloc/realloc および free コールが行われた命令アドレス。
Dumping...	検出された異常がヒープ メモリ領域の先頭からどれだけ近いかに応じて、1 つまたは 2 つのメモリ領域のダンプ。システム ヒープ ヘッダーの次の 8 バイトは、このツールがさまざまなシステム ヘッダー値のハッシュおよびキュー リンケージを格納するのに使用するメモリです。領域内のそれ以外のすべてのバイトには、システム ヒープ トレーラが発生するまで、0xcc が設定されている必要があります。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報を消去します。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内の要素を検証します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況について要約を表示します。

memory delayed-free-poisoner validate

memory delayed-free-poisoner キュー内のすべての要素を検証するには、特権 EXEC モードで ***memory delayed-free-poisoner validate*** コマンドを使用します。

memory delayed-free-poisoner validate

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

memory delayed-free-poisoner validate コマンドを発行する前に、**memory delayed-free-poisoner enable** コマンドを使用して delayed free-memory poisoner ツールをイネーブルにしておく必要があります。

memory delayed-free-poisoner validate コマンドを実行すると、**memory delayed-free-poisoner** キュー内の各要素が検証されます。要素に予期しない値が含まれている場合、クラッシュが発生し、クラッシュの原因を判断するための診断が出力されます。予期しない値が含まれていない場合は、要素はキューに保持されて正常に処理されます。**memory delayed-free-poisoner validate** コマンドを実行しても、キュー内のメモリはシステム メモリ プールに戻されません。

（注） delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。

例

次の例では、**memory delayed-free-poisoner** キュー内のすべての要素を検証します。

```
hostname# memory delayed-free-poisoner validate
```

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報を消去します。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況について要約を表示します。

memory profile enable

メモリ使用状況のモニタリング（メモリ プロファイリング）をイネーブルにするには、特権 EXEC モードで ***memory profile enable*** コマンドを使用します。メモリ プロファイリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

memory profile enable *peak* *peak_value*

no memory profile enable peak *peak_value*

シンタックスの説明

peak_value	メモリ使用状況のスナップショットがピーク使用状況のバッファに保存される、メモリ使用状況のしきい値を指定します。このバッファの内容は後で分析して、ピーク時のシステム メモリの必要量を判別できます。

デフォルト

メモリのプロファイリングは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

メモリ プロファイリングをイネーブルにする前に、***memory profile text*** コマンドを使用してメモリ テキストの範囲をプロファイルに設定する必要があります。

clear memory profile コマンドを入力するまで、メモリの一部はプロファイリング システムにより保持されます。***show memory status*** コマンドの出力を参照してください。

（注） メモリのプロファイリングをイネーブルにすると、セキュリティ　アプライアンスのパフォーマンスが一時的に低下することがあります。

次の例では、メモリ プロファイリングをイネーブルにします。

```
hostname# memory profile enable
```

関連コマンド

コマンド	説明
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。

memory profile text

プロファイルにメモリのプログラム テキスト範囲を設定するには、特権 EXEC モードで ***memory profile text*** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

memory profile text {*startPC endPC* | **all** *resolution*}

no memory profile text {*startPC endPC* | **all** *resolution*}

シンタックスの説明

all	メモリ ブロックのテキスト範囲全体を指定します。
endPC	メモリ ブロックのテキスト範囲終了点を指定します。
resolution	ソース テキスト領域に対するトレースの精度を指定します。
startPC	メモリ ブロックのテキスト範囲開始点を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

テキスト範囲が小さい場合、通常、「4」の精度で命令へのコールをトレースします。テキスト範囲が大きい場合、通常、最初のパスは粗精度で十分ですが、次のパスで範囲がより小さい領域セットに絞り込まれる可能性があります。

memory profile text コマンドにテキスト範囲を入力したら、***memory profile enable*** コマンドを入力して、メモリ プロファイリングを開始する必要があります。メモリのプロファイリングは、デフォルトではディセーブルになっています。

（注） メモリのプロファイリングをイネーブルにすると、セキュリティ　アプライアンスのパフォーマンスが一時的に低下することがあります。

例

次の例は、プロファイルにメモリのテキスト範囲を 4 の精度で設定する方法を示しています。

```
hostname# memory profile text 0x004018b4 0x004169d0 4
```

次の例では、テキスト範囲のコンフィギュレーションおよびメモリ プロファイリングのステータス（OFF）を表示します。

```
hostname# show memory profile
InUse profiling: OFF
Peak profiling: OFF
Profile:
0x004018b4-0x004169d0(00000004)
```

（注） メモリ プロファイリングを開始するには、***memory profile enable*** コマンドを入力する必要があります。メモリのプロファイリングは、デフォルトではディセーブルになっています。

関連コマンド

コマンド	説明
clear memory profile	メモリ プロファイリング機能によって保持されているバッファを消去します。
memory profile enable	メモリ使用状況のモニタリング（メモリ プロファイリング）をイネーブルにします。
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレスの範囲を表示します。

memory-size

WebVPN のさまざまなコンポーネントがアクセスするセキュリティ アプライアンス上にメモリ量を設定するには、WebVPN モードで **memory-size** コマンドを使用します。メモリ量は、KB 単位の設定量または全メモリのパーセンテージのいずれでも設定できます。設定されたメモリ サイズを削除するには、このコマンドの **no** 形式を使用します。

（注） 新しいメモリ サイズの設定を有効にするには、リブートが必要です。

memory-size {percent | kb} *size*

no memory-size [{percent | kb} *size***]**

シンタックスの説明

kb	メモリ量を KB 単位で指定します。
percent	メモリ量を、セキュリティ アプライアンス上の全メモリのパーセンテージとして指定します。
size	メモリ量を、KB 単位または全メモリのパーセンテージで指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次の例は、WebVPN のメモリ サイズを 30 パーセントに設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# memory-size percent 30
hostname(config-webvpn)#
hostname(config-webvpn)# reload
```

関連コマンド

コマンド	説明
show memory webvpn	WebVPN メモリ使用状況の統計情報を表示します。

message-length

設定した最大および最小の長さを満たしていない GTP パケットをフィルタリングするには、GTP マップ コンフィギュレーション モードで **message-length** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスできます。このコマンドを削除するには、**no** 形式を使用します。

message-length *min* *min_bytes* ***max*** *max_bytes*

no message-length *min* *min_bytes* ***max*** *max_bytes*

シンタックスの説明

max	UDP ペイロードで許可される最大バイト数を指定します。
max_bytes	UDP ペイロードの最大バイト数。範囲は、1 ～ 65,536 です。
min	UDP ペイロードで許可される最小バイト数を指定します。
min_bytes	UDP ペイロードの最小バイト数。範囲は、1 ～ 65,536 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	No

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドで指定される長さは、GTP ヘッダーと残りのメッセージ部分（UDP パケットのペイロード）を合せたものです。

例

次の例では、20 ～ 300 バイトの長さのメッセージを許可します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit message-length min 20 max 300
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

mfib forwarding

インターフェイス上で MFIB 転送を再度イネーブルにするには、インターフェイス コンフィギュレーション モードで **mfib forwarding** コマンドを使用します。インターフェイス上で MFIB 転送をディセーブルにするには、このコマンドの **no** 形式を使用します。

mfib forwarding

no mfib forwarding

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

multicast-routing コマンドは、デフォルトではすべてのインターフェイスの MFIB 転送をイネーブルにします。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

マルチキャスト ルーティングをイネーブルにすると、デフォルトでは、MFIB 転送はすべてのインターフェイスでイネーブルになります。特定のインターフェイス上で MFIB 転送をディセーブルにするには、このコマンドの **no** 形式を使用します。実行コンフィギュレーションに表示されるのは、このコマンドの **no** 形式のみです。

MFIB 転送をインターフェイス上でディセーブルにすると、他の方法で特別に設定しないかぎり、そのインターフェイスはマルチキャスト パケットを受け入れません。MFIB 転送がディセーブルになると、IGMP パケットも妨げられます。

例

次の例では、指定されたインターフェイスでの MFIB 転送をディセーブルにします。

```
hostname(config)# interface GigabitEthernet 0/0
hostname(config-if)# no mfib forwarding
```

関連コマンド

コマンド	説明
multicast-routing	マルチキャスト ルーティングをイネーブルにします。
pim	インターフェイスで PIM をイネーブルにします。

min-object-size

セキュリティ アプライアンスが、WebVPN セッションに対してキャッシュできるオブジェクトの最小サイズを設定するには、キャッシュ モードで min-object-size コマンドを使用します。サイズを変更するには、このコマンドを再度使用します。最小オブジェクト サイズを設定しない場合は、値としてゼロ（0）を入力します。

min-object-size *integer range*

シンタックスの説明

integer range	0 ～ 10000 KB

デフォルト

デフォルト サイズは 0 KB です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
キャッシュ モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

最小オブジェクト サイズは、最大オブジェクト サイズよりも小さくする必要があります。キャッシュ圧縮がイネーブルである場合、セキュリティ アプライアンスは、オブジェクト圧縮後のサイズを計算します。

例

次の例では、最大オブジェクト サイズである 40 KB に設定する方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)# min-object-size 40
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードに入ります。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシングをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシングに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。

mkdir

新しいディレクトリを作成するには、特権 EXEC モードで **mkdir** コマンドを使用します。

mkdir [**/noconfirm**] [**disk0: | disk1: | flash:**]*path*

シンタックスの説明

noconfirm	（オプション）確認プロンプトを表示しないようにします。
disk0:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。
disk1:	（オプション）外部フラッシュ メモリ カードを指定し、続けてコロン（:）を入力します。
flash:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。
path	作成するディレクトリの名前とパス。

デフォルト

パスを指定しない場合、ディレクトリは現在の作業ディレクトリに作成されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

同じ名前のディレクトリがすでに存在する場合、新しいディレクトリは作成されません。

例

次の例は、「backup」という新しいディレクトリを作成する方法を示しています。

```
hostname# mkdir backup
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに移動します。
dir	ディレクトリの内容を表示します。
rmdir	指定したディレクトリを削除します。
pwd	現在の作業ディレクトリを表示します。

mode

セキュリティ コンテキスト モードをシングルまたはマルチに設定するには、グローバル コンフィギュレーション モードで **mode** コマンドを使用します。1 つのセキュリティ アプライアンスを、セキュリティ コンテキストと呼ばれる複数の仮想装置に分割できます。各コンテキストは、独自のセキュリティ ポリシー、インターフェイス、および管理者を持つ独立した装置のように動作します。複数のコンテキストは、複数の独立型アプライアンスを持つことに相当します。シングル モードでは、セキュリティ アプライアンスは、1 つのコンフィギュレーションを保有し、1 つの装置のように動作します。マルチ モードでは、独自のコンフィギュレーションを持つ複数のコンテキストを作成できます。作成できるコンテキスト数は、ライセンスに応じて異なります。

mode {***single*** | ***multiple***} [***noconfirm***]

シンタックスの説明

multiple	マルチ コンテキスト モードを設定します。
noconfirm	（オプション）確認用のプロンプトを表示することなく、モードを設定します。このオプションは、自動スクリプトに役立ちます。
single	コンテキスト モードをシングルに設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、セキュリティ アプライアンスに、セキュリティ ポリシー、インターフェイス、および独立型装置で設定できるほとんどのオプションを指定するコンテキストごとのコンフィギュレーションが含まれます（コンテキスト コンフィギュレーションの場所の指定については、**config-url** コマンドを参照してください）。システム管理者は、システム コンフィギュレーションにコンテキストを設定することによって、コンテキストを追加したり管理したりします。これは、シングル モードの場合のコンフィギュレーションと同様、スタートアップ コンフィギュレーションです。システム コンフィギュレーションは、セキュリティ アプライアンスの基本的な設定を指定します。システム コンフィギュレーションには、システム自体のネットワーク インターフェイスまたはネットワークの設定は含まれません。ネットワーク リソースにアクセスする必要がある場合（サーバからコンテキストをダウンロードする場合など）、システム コンフィギュレーションは、管理コンテキストとして指定されているコンテキストの 1 つを使用します。

mode コマンドを使用してコンテキスト モードを変更する場合、リブートするためのプロンプトが表示されます。

コンテキスト モード（シングルまたはマルチ）は、リブート時も保持されますが、コンフィギュレーション ファイルには保存されません。別の装置にコンフィギュレーションをコピーする必要がある場合は、**mode** コマンドを使用して、新しい装置のモードが一致するように設定してください。

シングル モードからマルチ モードに変換すると、セキュリティ アプライアンスが実行コンフィギュレーションを 2 つのファイルに変換します。システム コンフィギュレーションを構成する新しいスタートアップ コンフィギュレーションと、管理コンテキストを構成する admin.cfg（内蔵フラッシュ メモリのルート ディレクトリ内）です。元の実行コンフィギュレーションは、old_running.cfg（内蔵フラッシュ メモリのルート ディレクトリ内）として保存されます。元のスタートアップ コンフィギュレーションは保存されません。セキュリティ アプライアンスは、システム コンフィギュレーションに「admin」という名前で管理コンテキストのエントリを自動的に追加します。

マルチ モードからシングル モードに変換する場合、必要に応じて、最初にスタートアップ コンフィギュレーション全体（可能な場合）をセキュリティ アプライアンスにコピーすることができます。マルチ モードから継承されたシステム コンフィギュレーションは、シングル モードの装置では完全に機能するコンフィギュレーションではありません。

マルチ コンテキスト モードでは、すべての機能はサポートされていません。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例では、モードをマルチに設定します。

```
hostname(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode

Rebooting....

Booting system, please wait...
```

次の例では、モードをシングルに設定します。

```
hostname(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single

***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode



Rebooting....

Booting system, please wait...
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードに入ります。
show mode	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

monitor-interface

特定のインターフェイスでヘルス モニタリングをイネーブルにするには、グローバル コンフィギュレーション モードで **monitor-interface** コマンドを使用します。インターフェイス モニタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

monitor-interface *if_name*

no monitor-interface *if_name*

シンタックスの説明

if_name	監視対象にするインターフェイスの名前を指定します。

デフォルト

物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトではディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスで監視できるインターフェイスの数は 250 です。hello メッセージは、各インターフェイスのポーリング間隔の間にセキュリティ アプライアンスのフェールオーバー ペア間で交換されます。フェールオーバー インターフェイスのポーリング間隔は、3 ～ 15 秒です。たとえば、ポーリング間隔が 5 秒に設定されている場合は、hello メッセージが 5 回続けて（25 秒）そのインターフェイスで聴取されないと、インターフェイスでテストが開始します。

監視対象のフェールオーバー インターフェイスのステータスは、次のいずれかになります。

- Unknown：初期ステータス。また、このステータスは、ステータスを判別できないことを意味します。
- Normal：インターフェイスがトラフィックを受信しています。
- Testing：5 ポーリング間隔の間、hello メッセージがインターフェイスで聴取されていません。
- Link Down：インターフェイスまたは VLAN が管理上ダウンしています。

- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスでトラフィックが受信されておらず、ピア インターフェイスでもトラフィックが聴取されていません。

Active/Active フェールオーバーでは、このコマンドはコンテキスト内でのみ有効です。

例

次の例では、「inside」という名前のインターフェイスでモニタリングをイネーブルにします。

```
hostname(config)# monitor-interface inside
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure monitor-interface	すべてのインターフェイスに対してデフォルトのインターフェイス ヘルス モニタリングを復元します。
failover interface-policy	フェールオーバーが発生する基準となる、監視対象のインターフェイスの障害数またはパーセンテージを指定します。
failover polltime	インターフェイスの hello メッセージ間の間隔を指定します（Active/Standby フェールオーバー）。
polltime interface	インターフェイスの hello メッセージ間の間隔を指定します（Active/Active フェールオーバー）。
show running-config monitor-interface	実行コンフィギュレーション内の **monitor-interface** コマンドを表示します。

more

ファイルの内容を表示するには、**more** コマンドを使用します。

more {**/ascii** | **/binary**| **/ebcdic** | **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **system:** | **tftp:**}*filename*

シンタックスの説明

/ascii	（オプション）バイナリ モードでバイナリ ファイルと ASCII ファイルを表示します。
/binary	（オプション）バイナリ モードでファイルを表示します。
/ebcdic	（オプション）EBCDIC のバイナリ ファイルを表示します。
disk0	（オプション）内蔵フラッシュ メモリのファイルを表示します。
disk1:	（オプション）外部フラッシュ メモリ カードのファイルを表示します。
flash:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。
ftp:	（オプション）FTP サーバのファイルを表示します。
http:	（オプション）Web サイトのファイルを表示します。
https:	（オプション）セキュア Web サイトのファイルを表示します。
system:	（オプション）ファイル システムを表示します。
tftp:	（オプション）TFTP サーバのファイルを表示します。
filename	表示するファイルの名前を指定します。

デフォルト

ACSII モード

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

more filesystem: コマンドは、ローカル ディレクトリまたはファイル システムのエイリアスを入力するためのプロンプトを表示します。

例

次の例は、「test.cfg」という名前のローカル ファイルの内容を表示する方法を示しています。

```
hostname# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005

XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
snmp-server contact admin@my_context.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

関連コマンド

コマンド	説明
cd	指定したディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。

mroute

スタティック マルチキャスト ルートを設定するには、グローバル コンフィギュレーション モードで **mroute** コマンドを使用します。スタティック マルチキャスト ルートを削除するには、このコマンドの **no** 形式を使用します。

mroute *src smask* {*in_if_name* [***dense*** *output_if_name*] | *rpf_addr*} [*distance*]

no mroute *src smask* {*in_if_name* [***dense*** *output_if_name*] | *rpf_addr*} [*distance*]

シンタックスの説明

dense *output_if_name*	（オプション）稠密モード出力用のインターフェイス名。 ***dense*** *output_if_name* キーワードと引数のペアは、SMR スタブ マルチキャスト ルーティング（IGMP フォワーディング）でのみサポートされています。
distance	（オプション）ルートの管理ディスタンス。より短い距離のルートが選択されます。デフォルトは 0 です。
in_if_name	mroute 用の着信インターフェイス名を指定します。
rpf_addr	mroute 用の着信インターフェイス名を指定します。RPF アドレスの PIM neighbor、PIM join、graft、prune の各メッセージがそのインターフェイスに送信されます。*rpf-addr* 引数には、直接接続されたシステムのホスト IP アドレス、またはネットワーク / サブネット番号を指定します。それがルートである場合、ユニキャスト ルーティング テーブルから再帰ルックアップが行われ、直接接続されたシステムを検索します。
smask	マルチキャスト送信元ネットワーク アドレス マスクを指定します。
src	マルチキャスト送信元の IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドを使用すると、マルチキャスト送信元の場所をスタティックに設定できます。セキュリティ アプライアンスは、特定の送信元にユニキャスト パケットを送信するときと同じインターフェイス上で、マルチキャスト パケットを受信すると予想します。マルチキャスト ルーティングをサポートしていないルートをバイパスする場合など、場合によっては、マルチキャスト パケットがユニキャスト パケットとは異なるパスを通ることがあります。

スタティック マルチキャスト ルートは、アドバタイジングまたは再配布されません。

マルチキャスト ルーティング テーブルの内容を表示するには、**show mroute** コマンドを使用します。実行コンフィギュレーションの mroute コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次の例は、**mroute** コマンドを使用して、スタティック マルチキャスト ルートを設定する方法を示しています。

```
hostname(config)# mroute 172.16.0.0 255.255.0.0 inside
```

関連コマンド

コマンド	説明
clear configure mroute	**mroute** コマンドをコンフィギュレーションから削除します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	コンフィギュレーション内の **mroute** コマンドを表示します。

msie-proxy except-list

クライアント PC 上でローカル バイパス用の Microsoft Internet Explorer ブラウザ プロキシ例外リスト設定値を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy except-list** コマンドを入力します。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

msie-proxy except-list {value *server*[*:port*] **| none}**

no msie-proxy except-list

シンタックスの説明

none	IP アドレス / ホスト名およびポートが存在しないことを示し、例外リストを継承しないようにします。
value *server:port*	IP アドレスまたは MSIE サーバの名前、およびこのクライアント PC に適用されるポートを指定します。ポート番号はオプションです。

デフォルト

デフォルトでは、msie-proxy except-list はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

例

次の例は、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ例外リスト（IP アドレス 192.168.20.1 のサーバで構成され、ポート 880 を使用）を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー アトリビュートの値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー アトリビュートを削除します。

msie-proxy local-bypass

クライアント PC に対して Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定値を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy local-bypass** コマンドを入力します。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

msie-proxy local-bypass {enable | disable}

no msie-proxy local-bypass {enable | disable}

シンタックスの説明

disable	クライアント PC に対して Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定をディセーブルにします。
enable	クライアント PC に対して Microsoft Internet Explorer ブラウザ プロキシ ローカル バイパス設定をイネーブルにします。

デフォルト

デフォルトでは、msie-proxy local-bypass はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ ローカル バイパスをイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy local-bypass enable
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー アトリビュートの値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー アトリビュートを削除します。

msie-proxy method

クライアント PC に対して Microsoft Internet Explorer ブラウザ プロキシ アクション（「方式」）を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy method** コマンドを入力します。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server**]

no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server**]

シンタックスの説明

auto-detect	クライアント PC に対して Internet Explorer の自動プロキシ サーバ検出の使用をイネーブルにします。
no-modify	このクライアント PC に対して Internet Explorer の HTTP ブラウザ プロキシ サーバ設定を変更しないようにします。
no-proxy	このクライアント PC に対して Interenet Explorer の HTTP プロキシ設定をディセーブルにします。
use-server	**msie-proxy server** コマンドで設定された値を使用するように Internet Explorer の HTTP プロキシ サーバ設定値を設定します。

デフォルト

デフォルトの方式は use-server です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

例

次の例は、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ設定値として自動検出を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy method auto-detect
hostname(config-group-policy)#
```

次の例では、クライアント PC のサーバとして QAserver サーバ、ポート 1001 を使用するように、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ設定値を設定しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server QAserver:port 1001
hostname(config-group-policy)# msie-proxy method use-server
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy server	クライアント PC に対して Microsoft Internet Explorer ブラウザ プロキシ サーバおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー アトリビュートの値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー アトリビュートを削除します。

msie-proxy server

クライアント PC に対して Microsoft Internet Explorer ブラウザ プロキシ サーバおよびポートを設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy server** コマンドを入力します。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

msie-proxy server {value *server*[*:port*] **| none}**

no msie-proxy server

シンタックスの説明

none	プロキシ サーバに指定されている IP アドレス / ホスト名またはポートが存在しないことを示し、サーバを継承しないようにします。
value *server:port*	IP アドレスまたは MSIE サーバの名前、およびこのクライアント PC に適用されるポートを指定します。ポート番号はオプションです。

デフォルト

デフォルトでは、msie-proxy サーバは指定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

例

次の例は、FirstGroup というグループ ポリシーに対して Microsoft Internet Explorer プロキシ サーバとして IP アドレス 192.168.10.1（ポート 880 を使用）を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# msie-proxy server value 192.168.21.1:880
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー アトリビュートの値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー アトリビュートを削除します。

mtu

インターフェイスの Maximum Transmission Unit（MTU; 最大伝送ユニット）を指定するには、グローバル コンフィギュレーション モードで **mtu** コマンドを使用します。イーサネット インターフェイスの MTU ブロック サイズを 1,500 にリセットするには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 トラフィックと IPv6 トラフィックをサポートしています。

mtu *interface_name bytes*

no mtu *interface_name bytes*

シンタックスの説明

bytes	MTU のバイト数を指定します。有効値は 64 ～ 65,535 バイトです。
interface_name	内部または外部のネットワーク インターフェイスの名前。

デフォルト

イーサネット インターフェイスの場合、デフォルトの *bytes* は 1500 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	—	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

mtu コマンドを使用すると、接続で送信されるデータのサイズを設定できます。MTU 値より大きなデータは、送信前にフラグメント化されます。

セキュリティ アプライアンスは RFC 1191 で定義されている IP Path MTU Discovery をサポートしています。IP Path MTU Discovery によって、ホストは、パスに沿ったさまざまなリンクの最大許容 MTU サイズでの相違を動的に検出して対応できます。パケットがインターフェイスに設定された MTU よりも大きいが、「don't fragment」（DF）ビットが設定されているため、セキュリティ アプライアンスがデータグラムを転送できないことがあります。ネットワーク ソフトウェアは、発信元ホストに対してこの問題を警告しながらメッセージを送信します。ホスト側では、宛先用にパケットをフラグメント化して、パスに沿ったリンクすべての最小パケット サイズに合せる必要があります。

イーサネット インターフェイスの場合、デフォルトの MTU は 1 ブロック 1,500 バイトで、これは最大値でもあります。これはほとんどのアプリケーションで十分な値ですが、ネットワークの条件で必要とされる場合はこれより低い数値を選択できます。

Layer 2 Tunneling Protocol（L2TP）を使用している場合は、MTU サイズを 1,380 に設定することを推奨します。このサイズは、L2TP ヘッダー長と IPSec ヘッダー長に相当するためです。

例

次の例は、インターフェイスの MTU を指定する方法を示しています。

```
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
hostname(config)# mtu inside 8192
hostname(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスの設定済み最大伝送ユニット値を消去します。
show running-config mtu	現在の最大伝送ユニットのブロック サイズを表示します。

multicast boundary

管理用マルチキャスト アドレスのマルチキャスト境界を設定するには、インターフェイス コンフィギュレーション モードで **multicast boundary** コマンドを使用します。境界を削除するには、このコマンドの **no** 形式を使用します。マルチキャスト境界はマルチキャスト データ パケット フローを制限し、異なる管理ドメインでの同一マルチキャスト グループ アドレスの再使用をイネーブルにします。

multicast boundary *acl* [***filter-autorp***]

no multicast boundary ***acl*** [***filter-autorp***]

シンタックスの説明

acl	アクセス リストの名前または番号を指定します。アクセス リストでは、境界によって影響を受けるアドレスの範囲が定義されます。このコマンドでは、標準 ACL だけを使用してください。拡張 ACL はサポートされていません。
filter-autorp	境界 ACL により拒否された Auto-RP メッセージをフィルタリングします。指定されない場合、Auto-RP メッセージはすべて渡されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用してインターフェイスに管理用の境界を設定し、*acl* 引数で定義された範囲内のマルチキャスト グループ アドレスをフィルタリングします。標準のアクセス リストは、対象となるアドレスの範囲を定義します。このコマンドを設定する場合、マルチキャスト データ パケットについては、いずれの方向においても境界をまたがってのフローは許可されません。マルチキャスト データ パケットを制限すると、異なる管理ドメインでの同一マルチキャスト グループ アドレスの再使用がイネーブルになります。

filter-autorp キーワードを設定すると、管理用の境界は Auto-RP の探索と通知のメッセージも検査し、境界 ACL により拒否された Auto-RP パケットから Auto-RP グループ範囲通知を削除します。Auto-RP グループ範囲内のすべてのアドレスが境界 ACL によって許可される場合に限り、Auto-RP グループ範囲通知は境界によって許可され、渡されます。アドレスが許可されない場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージから削除された後で、Auto-RP メッセージが転送されます。

例

次の例では、すべての管理用アドレスに境界を設定し、Auto-RP メッセージをフィルタリングします。

```
hostname(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
hostname(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# multicast boundary boundary_test filter-autorp
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

multicast-routing

セキュリティ アプライアンスの IP マルチキャスト ルーティングをイネーブルにするには、グローバル コンフィギュレーション モードで **multicast-routing** コマンドを使用します。IP マルチキャスト ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

multicast-routing

no multicast-routing

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

multicast-routing コマンドは、デフォルトではすべてのインターフェイスの PIM と IGMP をイネーブルにします。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

multicast-routing コマンドは、すべてのインターフェイスの PIM と IGMP をイネーブルにします。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

セキュリティ アプライアンスが PIM RP の場合は、セキュリティ アプライアンスの未変換の外部アドレスを、RP アドレスとして使用します。

マルチキャスト ルーティング テーブルのエントリ数は、システムの RAM 量によって制限されます。表 20-2 に、セキュリティ アプライアンスの RAM 量に基づいた特定のマルチキャスト テーブルの最大エントリ数を示します。これらの制限値に達すると、新しいエントリはすべて廃棄されます。

表 20-2　マルチキャスト テーブル エントリの制限値

テーブル	16 MB	128 MB	128 MB 以上
MFIB	1000	3000	5000
IGMP グループ	1000	3000	5000
PIM ルート	3000	7000	12000

例

次の例では、セキュリティ アプライアンスの IP マルチキャスト ルーティングをイネーブルにします。

```
hostname(config)# multicast-routing
```

関連コマンド

コマンド	説明
igmp	インターフェイスで IGMP をイネーブルにします。
pim	インターフェイスで PIM をイネーブルにします。

CHAPTER 21

nac コマンド～ override-account-disable コマンド

nac

ネットワーク アドミッション コントロールをイネーブルまたはディセーブルにするには、グループ ポリシー コンフィギュレーション モードで **nac** コマンドを使用します。デフォルトのグループ ポリシーから NAC 設定を継承するには、継承元となる別のグループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

nac {enable | disable}

no nac [enable | disable]

シンタックスの説明

enable	NAC をイネーブルにします。リモート アクセスにはポスチャ確認が必要です。リモート コンピュータが確認チェックをパスすると、ACS サーバはセキュリティ アプライアンスのアクセス ポリシーをダウンロードして施行します。
disable	NAC をディセーブルにします。

デフォルト

デフォルト設定はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　アクセス コントロール サーバがネットワーク上に存在する必要があります。

例

次の例では、グループ ポリシー用に NAC をイネーブルにします。

```
hostname(config-group-policy)# nac enable
hostname(config-group-policy)
```

次の例では、グループ ポリシー用に NAC をディセーブルにします。

```
hostname(config-group-policy)# nac disable
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーから NAC 設定を継承します。

```
hostname(config-group-policy)# no nac
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバまたは AAA サーバ グループのレコードを作成し、ホスト固有の AAA サーバ アトリビュートを設定します。
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac-authentication-server-group	認証サーバのグループがネットワーク アドミッション コントロールのポスチャ確認に使用されることを示します。

nac-authentication-server-group

ネットワーク アドミッション コントロールのポスチャ確認に使用される認証サーバのグループを特定するには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **nac-authentication-server-group** をコマンドを使用します。デフォルトのリモート アクセス グループから認証サーバを継承するには、継承元となる別のグループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

nac-authentication-server-group *server-group*

no nac-authentication-server-group

シンタックスの説明

server-group	**aaa-server host** コマンドを使用してセキュリティ アプライアンスで設定された、ポスチャ確認サーバ グループの名前です。この名前は、aaa-server host コマンドで指定した server-tag 変数と一致している必要があります。

デフォルト

このコマンドには、引数もキーワードもありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

NAC をサポートするために、アクセス コントロール サーバを少なくとも 1 つ設定します。**aaa-server** コマンドを使用して ACS グループに名前を付けます。
次に、**nac-authentication-server-group** コマンドを使用します。サーバ グループには同じ名前を使用します。

例

次の例では、acs-group1 を NAC のポスチャ確認に使用する認証サーバ グループとして指定します。

```
hostname(config-group-policy)# nac-authentication-server-group acs-group1
hostname(config-group-policy)
```

次の例では、デフォルトのリモート アクセス グループから認証グループを継承します。

```
hostname(config-group-policy)# no nac-authentication-server-group
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバまたは AAA サーバ グループのレコードを作成し、ホスト固有の AAA サーバ アトリビュートを設定します。
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac	グループ ポリシーでネットワーク アドミッション コントロールをイネーブルにします。

nac-default-acl

ポスチャ認証に失敗するネットワーク アドミッション コントロール セッションのデフォルト ACL として使用する ACL を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-default-acl** コマンドを使用します。

nac-default-acl value *acl-name*

nac-default-acl none

デフォルトのグループ ポリシーから ACL を継承するには、継承元となる別のグループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

no nac-default-acl

シンタックスの説明

acl-name	セキュリティ アプライアンスで設定されているとおりに、**aaa-server host** コマンドを使用してポスチャ確認サーバ グループに名前を付けます。この名前は、aaa-server host コマンドで指定した server-tag 変数と一致している必要があります。
none	デフォルトのグループ ポリシーからの ACL の継承をディセーブルにします。ポスチャ確認に失敗する NAC セッションに ACL を適用しません。

デフォルト

デフォルトは **none** です。

NAC はデフォルトでディセーブルになっているので、セキュリティ アプライアンスを経由する VPN トラフィックは、NAC がイネーブルになるまで NAC のデフォルト ACL の影響を受けません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ポスチャ確認の失敗時に適用される ACL として acl-1 を指定します。

```
hostname(config-group-policy)# nac-default-acl value acl-1
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーから ACL を継承します。

```
hostname(config-group-policy)# no nac-default-acl
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーからの ACL の継承をディセーブルにします。ポスチャ確認に失敗する NAC セッションに ACL は適用されません。

```
hostname(config-group-policy)# nac-default-acl none
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac	グループ ポリシーでネットワーク アドミッション コントロールをイネーブルにします。

nac-reval-period

ネットワーク アドミッション コントロール セッションでのポスチャ確認の成功後から次のポスチャ確認までの間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-reval-period** コマンドを使用します。デフォルトのグループ ポリシーから再確認のタイマーを継承するには、継承元となる別のグループ ポリシーにアクセスして、このコマンドの **no** 形式を使用します。

nac-reval-period *seconds*

no nac-reval-period [*seconds***]**

シンタックスの説明

seconds	正常に完了した各ポスチャ確認の間隔を示す秒数。範囲は 300 ～ 86400 です。

デフォルト

デフォルト値は 36000 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、ポスチャ確認が成功すると再確認のタイマーを開始します。このタイマーが切れると、無条件のポスチャ確認が開始されます。セキュリティ アプライアンスは再確認中、ポスチャ確認を維持します。デフォルトのグループ ポリシーは、アクセス コントロール サーバがポスチャ確認または再確認中に無効な場合に有効になります。

例

次の例では、再確認タイマーを 86400 秒に変更します。

```
hostname(config-group-policy)# nac-reval-period 86400
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーから再確認タイマーの値を継承します。

```
hostname(config-group-policy)# no nac-reval-period
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac	グループ ポリシーでネットワーク アドミッション コントロールをイネーブルにします。

nac-sq-period

ネットワーク アドミッション コントロール セッションでのポスチャ確認が成功してからホスト ポスチャの変更に関する次のクエリーまでの間隔を指定するには、グループ ポリシー コンフィギュレーション モードで **nac-sq-period** コマンドを使用します。デフォルトのグループ ポリシーからステータス クエリー タイマーの値を継承するには、継承元となる別のグループ ポリシーにアクセスし、このコマンドの **no** 形式を使用します。

nac-sq-period *seconds*

no nac-sq-period [*seconds***]**

シンタックスの説明

seconds	正常に完了した各ポスチャ確認の間隔を示す秒数。範囲は 300 ～ 1800 です。

デフォルト

デフォルト値は 300 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスはポスチャ確認とステータス クエリーの応答が正常に実行された後、ステータス クエリー タイマーを開始します。このタイマーが切れると、*ステータス クエリー*と呼ばれる、ホスト ポスチャの変更に関するクエリーが開始されます。

例

次の例では、ステータス クエリー タイマーの値を 1800 秒に変更します。

```
hostname(config-group-policy)# nac-sq-period 1800
hostname(config-group-policy)
```

次の例では、デフォルトのグループ ポリシーからステータス クエリー タイマーの値を継承します。

```
hostname(config-group-policy)# no nac-sq-period
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac	グループ ポリシーでネットワーク アドミッション コントロールをイネーブルにします。
nac-reval-period	ネットワーク アドミッション コントロール セッションで正常に完了した各ポスチャ確認の間隔を指定します。

name

名前を IP アドレスに関連付けるには、グローバル コンフィギュレーション モードで **name** コマンドを使用します。コンフィギュレーションから名前を削除することなく、テキスト名の使用をディセーブルにするには、このコマンドの **no** 形式を使用します。

name *ip_address name* [description *text*]]

no name *ip_address* **[***name* [description *text***]]**

シンタックスの説明

description	（オプション）IP アドレス名の説明を指定します。
ip_address	名前を付けるホストの IP アドレスを指定します。
name	IP アドレスに割り当てられる名前を指定します。a ～ z、A ～ Z、0 ～ 9、ダッシュ、およびアンダースコアの文字を使用します。*name* は、63 文字以下にする必要があります。また、*name* の先頭は数字にはできません。
text	この説明のテキストを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.0(4)	オプションとして description を使用できるように機能が拡張されました。

使用上のガイドライン

IP アドレスとの名前の関連付けをイネーブルにするには、***names*** コマンドを使用します。IP アドレスに関連付けることができるのは、1 つの名前だけです。

まず **names** コマンドを使用してから、**name** コマンドを使用する必要があります。**name** コマンドは、**names** コマンドの直後、かつ **write memory** コマンドの前に使用してください。

name コマンドを使用すると、ホストをテキスト名で識別し、テキスト文字列を IP アドレスにマッピングできます。**no name** コマンドを使用すると、テキスト名を使用できないようにできますが、コンフィギュレーションから名前は削除しません。名前のリストをコンフィギュレーションから消去するには、***clear configure name*** コマンドを使用します。

name 値の表示をディセーブルにするには、**no names** コマンドを使用します。

name コマンドと **names** コマンドは、両方ともコンフィギュレーションに保存されます。

name コマンドでは、ネットワーク マスクに名前を割り当てることはサポートされていません。たとえば、次のコマンドは拒否されます。

```
hostname(config)# name 255.255.255.0 class-C-mask
```

(注)　マスクを必要とするどのコマンドも、受け入れたネットワーク　マスクとして名前を処理できません。

例

次の例は、**names** コマンドによって、**name** コマンドの使用をイネーブルにする方法を示しています。**name** コマンドは、192.168.42.3 への参照の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用できるようにします。IP アドレスをネットワーク インターフェイスに割り当てる際に、**ip address** コマンドでこれらの名前を使用できます。**no names** コマンドは、**name** コマンド値の表示をディセーブルにします。その後で **names** コマンドを再度使用すると、**name** コマンド値の表示が元に戻ります。

```
hostname(config)# names
hostname(config)# name 192.168.42.3 sa_inside
hostname(config)# name 209.165.201.3 sa_outside

hostname(config-if)# ip address inside sa_inside 255.255.255.0
hostname(config-if)# ip address outside sa_outside 255.255.255.224

hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224

hostname(config)# no names
hostname(config)# show ip address
System IP Addresses:
    inside ip address 192.168.42.3 mask 255.255.255.0
    outside ip address 209.165.201.3 mask 255.255.255.224

hostname(config)# names
hostname(config)# show ip address
System IP Addresses:
    inside ip address sa_inside mask 255.255.255.0
    outside ip address sa_outside mask 255.255.255.224
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
names	IP アドレスとの名前の関連付けをイネーブルにします。
show running-config name	IP アドレスに関連付けられた名前を表示します。

nameif

インターフェイスに名前を付けるには、インターフェイス コンフィギュレーション モードで **nameif** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスのすべてのコンフィギュレーション コマンドで、インターフェイス タイプと ID（gigabitethernet0/1 など）ではなくインターフェイス名が使用されるので、トラフィックがインターフェイスを通過できるようにするにはインターフェイス名が必要です。

nameif *name*

no nameif

シンタックスの説明

name	最大 48 文字の名前を設定します。名前は大文字と小文字の区別がありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

サブインターフェイスの場合、**vlan** コマンドを使用して VLAN を割り当ててから、**nameif** コマンドを入力する必要があります。

新しい値でこのコマンドを再入力することによって、名前を変更できます。**no** 形式のコマンドは入力しないでください。このコマンドを入力すると、該当する名前に適用されるコマンドがすべて削除されます。

例

次の例では、2 つのインターフェイスの名前を「inside」と「outside」に設定します。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/0
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に関するすべての変換をリセットして、接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
security-level	インターフェイスのセキュリティ レベルを設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

names

name コマンドで設定可能な、IP アドレスから名前への変換をイネーブルにするには、グローバル コンフィギュレーション モードで **names** コマンドを使用します。アドレスから名前への変換をディセーブルにするには、このコマンドの **no** 形式を使用します。

names

no names

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

name コマンドで設定した IP アドレスとの名前の関連付けをイネーブルにするには、**names** コマンドを使用します。**name** または **names** コマンドを入力する順番は、重要ではありません。

例

次の例は、名前と IP アドレスとの関連付けをイネーブルにする方法を示してします。

```
hostname(config)# names
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられている名前のリストを表示します。
show running-config names	IP アドレスから名前への変換を表示します。

name-separator

電子メール、VPN ユーザ名、およびパスワード間のデリミタとして文字を指定するには、該当する電子メール プロキシ モードで **name-separator** コマンドを使用します。デフォルトの「:」に戻すには、このコマンドの **no** 形式を使用します。

name-separator [*symbol*]

no name-separator

シンタックスの説明

symbol	（オプション）電子メール、VPN ユーザ名、およびパスワード間を区切る文字。使用できるのは、アットマーク（@）、パイプ（|）、コロン（:）、番号記号（#）、カンマ（,）、およびセミコロン（;）です。

デフォルト

デフォルトは、「:」（コロン）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

名前セパレータには、サーバ セパレータと異なるものを指定する必要があります。

例

次の例は、POP3S の名前セパレータとしてハッシュ（#）を設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# name-separator #
```

関連コマンド

コマンド	説明
server-separator	電子メールとサーバ名を区切ります。

nat

別のインターフェイスのマッピング アドレスに変換される、1 つのインターフェイスのアドレスを指定するには、グローバル コンフィギュレーション モードで **nat** コマンドを使用します。このコマンドは、ダイナミック NAT または PAT を設定します。ダイナミック NAT または PAT では、アドレスをマッピング アドレスのいずれかのプールに変換します。**nat** コマンドを削除するには、このコマンドの **no** 形式を使用します。

標準ダイナミック NAT の場合：

nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

no nat (*real_ifc) nat_id real_ip* [*mask* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]]

ポリシー ダイナミック NAT と NAT 免除の場合：

nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

no nat (*real_ifc) nat_id* **access-list** *access_list_name* [**dns**] [**outside]** [[**tcp**] *tcp_max_conns* [*emb_limit*]] [**udp** *udp_max_conns*] [**norandomseq**]

シンタックスの説明

access-list *access_list_name*	拡張アクセス リスト（別名、ポリシー NAT）を使用して、ローカル アドレスと宛先アドレスを指定します。**access-list** コマンドを使用してアクセス リストを作成します。***eq*** 演算子を使用して、アクセス リストにローカル ポートと宛先ポートをオプションで指定できます。NAT ID が **0** の場合、アクセス リストは NAT から免除されたアドレスを指定します。NAT 免除はポリシー NAT とは異なります。たとえば、ポート アドレスを指定できません。 **(注)** アクセス リストのヒット カウント（**show access-list** コマンドを参照）は、NAT 免除アクセス リストの場合は増分されません。
dns	（オプション）このコマンドに一致する DNS 応答で、A レコード（アドレス レコード）を書き直します。マッピングされているインターフェイスから実際のインターフェイスに移動する DNS 応答では、A レコードが、マッピングされた値から実際の値に書き直されます。逆に、実際のインターフェイスからマッピングされているインターフェイスに移動する DNS 応答では、A レコードが、実際の値からマッピングされた値に書き直されます。 DNS サーバにエントリがあるホストのアドレスが NAT 文に含まれ、クライアントとは異なるインターフェイスに DNS サーバがある場合、クライアントと DNS サーバに必要なホスト アドレスはそれぞれ異なります。一方にはグローバル アドレスが必要で、もう一方にはローカル アドレスが必要です。変換対象のホストは、クライアントまたは DNS サーバのどちらかと同じインターフェイス上になければなりません。通常、他のインターフェイスからのアクセスを許可する必要があるホストがスタティック トランスレーションを使用するので、このオプションは **static** コマンドと併せて使用するのが一般的です。

emb_limit	（オプション）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実際のアドレスを指定します。**0.0.0.0**（または短縮形の **0**）を使用すると、すべてのアドレスを指定できます。
mask	（オプション）実際のアドレスのサブネット マスクを指定します。マスクを入力しない場合、IP アドレス クラスのデフォルト マスクが使用されます。
nat_id	NAT ID の整数を指定します。標準 NAT の場合、この整数は 1 ～ 2147483647 です。ポリシー NAT（nat id access-list）の場合、この整数は 1 ～ 65535 です。 アイデンティティ NAT（**nat 0**）と NAT 免除（**nat 0 access-list**）は、**0** の NAT ID を使用します。 **global** コマンドはこの ID を参照して、グローバル プールを *real_ip* に関連付けます。
norandomseq	（オプション）TCP ISN のランダム化保護をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの ISN があります。1 つはクライアントが生成し、1 つはサーバが生成します。セキュリティ アプライアンスは、ホストとサーバが生成する ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。 **norandomseq** キーワードは、外部 NAT には適用されません。ファイアウォールがランダム化するのは、セキュリティの高いインターフェイスに対してホストまたはサーバが生成する ISN のみです。外部 NAT に対して **norandomseq** を設定しても、その **norandomseq** キーワードは無視されます。
outside	（オプション）このインターフェイスのセキュリティ レベルが、**global** 文の一致で特定するインターフェイスより低い場合、**outside** を入力する必要があります。この機能は、外部 NAT または双方向 NAT と呼ばれます。
tcp *tcp_max_conns*	サブネット全体に関して、同時 TCP 接続の最大数を指定します。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。
udp *udp_max_conns*	（オプション）サブネット全体に関して、同時 UDP 接続の最大数を指定します。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は 0（無制限）です。この値は、最大使用可能値です。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　ダイナミック NAT と PAT の場合、最初に **nat** コマンドを設定し、変換する所定のインターフェイスの実アドレスを指定します。次に、別の **global** コマンドを設定して、別のインターフェイスから出るときのマッピング アドレスを指定します（PAT の場合、このアドレスは 1 つです）。各 **nat** コマンドは、各コマンドに割り当てられた番号である NAT ID の比較によって、1 つの **global** コマンドと一致します。

セキュリティ アプライアンスは、NAT 規則がトラフィックに一致する場合に、アドレスを変換します。NAT 規則が一致しない場合、パケットの処理が続行します。例外は、**nat-control** コマンドを使用して NAT コントロールをイネーブルにする場合です。NAT コントロールでは、セキュリティの高いインターフェイス（内部）からセキュリティの低いインターフェイス（外部）に移動するパケットが NAT 規則に一致する必要があります。一致していないと、パケットの処理が停止します。NAT コントロールをイネーブルにした場合でも、NAT は同一セキュリティ レベルのインターフェイスでは必要ありません。必要に応じて、オプションで NAT を設定できます。

ダイナミック NAT は、宛先ネットワークでルーティング可能なマッピング アドレスのプールに実際のアドレスのグループを変換します。マッピング プールは、実際のグループより少ないアドレスで構成されます。変換するホストが宛先ネットワークにアクセスするときに、セキュリティ アプライアンスがマッピング プールの IP アドレスをホストに割り当てます。実際のホストが接続を開始する場合にのみ、変換が追加されます。変換が有効なのは接続されている間だけなので、所定のユーザが変換のタイムアウト後も同じ IP アドレスを維持することはありません（**timeout xlate** コマンドを参照）。そのため、アクセス リストによって接続が許可されている場合でも、ダイナミック NAT（または PAT）を使用するホストに、宛先ネットワーク上のユーザから確実に接続を開始できません。また、実ホスト アドレスに直接接続しようとすると、セキュリティ アプライアンスが拒否します。ホストへの信頼できるアクセスについては、**static** コマンドを参照してください。

ダイナミック NAT には、次の短所があります。

- マッピング プール内のアドレスが実際のグループより少ない場合、トラフィック量が予想を超えるとアドレスが不足する可能性があります。

  PAT は単一アドレスのポートを使用して 64,000 を超える変換を実行できるので、この現象が頻繁に発生する場合は、PAT を使用してください。
- マッピング　プールで大量のルーティング可能なアドレスを使用しなければなりません。インターネットなどの登録アドレスが宛先ネットワークに必要な場合は、使用可能なアドレスが不足する可能性があります。

ダイナミック NAT の利点は、一部のプロトコルが PAT を使用できないということです。たとえば、GRE バージョン 0 のように、オーバーロードするポートを持たない IP プロトコルでは、PAT は動作しません。一部のマルチメディア アプリケーションのように、あるポートでデータ ストリームを流して別のポートで制御パスを提供するオープンスタンダードではない一部のアプリケーションでも、PAT は動作しません。

PAT では、複数の実アドレスを 1 つのマッピング IP アドレスに変換します。具体的には、セキュリティ アプライアンスが実アドレスと送信元ポート（実ソケット）をマッピング アドレスと一意なポート（マッピング ソケット）に変換します。送信元ポートが TCP/UDP の場合、送信元アドレスは PAT を使用して同じ範囲のアドレスに変換されます。範囲には、1 ～ 511、512 ～ 1023、および 1024 ～ 65535 が含まれます。送信元ポートはそれぞれの接続で異なるので、各接続には別個の変換が必要になります。たとえば、10.1.1.1:1025 には、10.1.1.1:1026 とは異なる変換が必要です。

接続の期限が切れると、ポートの変換も 30 秒の非アクティビティの後、期限切れになります。タイムアウトは、設定できません。

PAT で使用できるマッピング アドレスは 1 つなので、ルーティング可能なアドレスの節約になります。セキュリティ アプライアンスのインターフェイス IP アドレスを PAT アドレスとして使用することもできます。PAT は、データ ストリームが制御パスと異なる一部のマルチメディア アプリケーションでは動作しません。

（注） 変換中であれば、リモート ホストは、アクセス リストで許可されているかぎり変換対象のホストへの接続を開始できます。アドレスは（実際のアドレスとマッピング アドレスの両方とも）予測不能なので、ホストに接続できる可能性は非常に少なくなります。万一、接続が成功した場合は、アクセス リストのセキュリティに頼ることができます。

NAT コントロールをイネーブルにする場合、内部ホストは、外部ホストにアクセスするときに NAT 規則に一致する必要があります。一部のホストで NAT を実行しない場合は、それらのホストで NAT をバイパスできます（または、NAT コントロールをディセーブルにできます）。たとえば、NAT をサポートしていないアプリケーションを使用する場合に、NAT をバイパスすることになる可能性があります。**static** コマンドを使用して NAT をバイパスするか、次のいずれかのオプションを使用できます。

- アイデンティティ NAT（**nat 0** コマンド）：アイデンティティ NAT（ダイナミック NAT と類似）を設定する場合、特定のインターフェイスのホストの変換を制限しません。すべてのインターフェイスを通過する接続に、アイデンティティ NAT を使用する必要があります。そのため、インターフェイス A にアクセスするときに、実際のアドレスで標準変換を実行し、インターフェイス B にアクセスするときに、アイデンティティ NAT を使用するといった選択はできません。これに対して、標準ダイナミック NAT を使用した場合は、アドレスを変換する特定のインターフェイスを指定できます。アクセス リストに基づいて使用可能なすべてのネットワーク上で、アイデンティティ NAT を使用する実際のアドレスがルーティング可能でなければなりません。

  アイデンティティ NAT の場合、マッピング アドレスが実際のアドレスと同じでも、（アクセス リストで許可されている場合を含めて）外部から内部へ接続を開始することはできません。この機能では、スタティック アイデンティティ NAT または NAT 免除を使用してください。
- NAT 免除（**nat 0 access-list** コマンド）：NAT 免除を使用すると、変換対象のホストとリモート ホストの両方で接続を開始できます。アイデンティティ NAT と同様、特定のインターフェイスのホストに対する変換を制限しないでください。すべてのインターフェイスを通過する接続に NAT 免除を使用する必要があります。ただし、NAT 免除では、変換する実際のアドレスを決定するときに（ポリシー NAT と同様）、実際のアドレスと宛先アドレスを指定できるので、NAT 免除を使用すると詳細な制御が可能になります。一方、ポリシー NAT と異なり、NAT 免除ではアクセス リストのポートは考慮されません。

ポリシー NAT では、拡張アクセス リストで送信元アドレスと宛先アドレスを指定することによって、アドレス変換対象の実アドレスを指定できます。オプションで、送信元ポートと宛先ポートも指定できます。標準 NAT で考慮されるのは、実際のアドレスだけです。たとえば、実際のアドレスがサーバ A にアクセスするときはマッピング アドレス A に変換できますが、サーバ B にアクセスするときにはマッピング アドレス B に変換できます。

セカンダリ チャネルのアプリケーション検査を必要とするアプリケーション（FTP、VoIP など）に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリ ポートを変換します。

（注） NAT 免除を除くすべてのタイプの NAT がポリシー NAT をサポートしています。NAT 免除では、アクセス リストを使用して実際のアドレスを指定しますが、ポートが考慮されない点がポリシー NAT と異なります。ポリシー NAT をサポートしていない**スタティック** アイデンティティ NAT を使用すると、NAT 免除と同じ結果を得られます。

別の方法として、モジュラ ポリシー フレームワークを使用して接続制限（ただし初期接続制限はでない）を設定できます。詳細については、**set connection** コマンドを参照してください。NAT を使用する場合、初期接続制限のみが設定できます。同じトラフィックに対して両方の方法を使用してこれらの設定値を設定した場合、セキュリティ アプライアンスは小さい方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

NAT コンフィギュレーションを変更し、既存の変換のタイムアウトを待機せずに新しい NAT 情報が使用される場合、**clear xlate** コマンドを使用して、変換テーブルを消去できます。ただし、変換テーブルを消去すると現在の接続がすべて切断されます。

例

たとえば、内部インターフェイス上の 10.1.1.0/24 ネットワークを変換するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.1-209.165.201.30
```

ダイナミック NAT 用のアドレス プールを、NAT プールを使い果たしたときのための PAT アドレスと共に指定するには、次のコマンドを入力します。

```
hostname(config)# nat (inside) 1 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 1 209.165.201.5
hostname(config)# global (outside) 1 209.165.201.10-209.165.201.20
```

ルーティングの簡略化などのために、セキュリティの低い DMZ（非武装地帯）のネットワーク アドレスを変換して内部ネットワーク（10.1.1.0）と同じネットワーク上に表示するには、次のコマンドを入力します。

```
hostname(config)# nat (dmz) 1 10.1.2.0 255.255.255.0 outside dns
hostname(config)# global (inside) 1 10.1.1.45
```

ポリシー NAT を使用して、1 つの実際のアドレスに 2 つの異なる宛先アドレスを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list NET1 permit ip 10.1.2.0 255.255.255.0 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip 10.1.2.0 255.255.255.0 209.165.200.224
255.255.255.224
hostname(config)# nat (inside) 1 access-list NET1 tcp 0 2000 udp 10000
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list NET2 tcp 1000 500 udp 2000
hostname(config)# global (outside) 2 209.165.202.130
```

ポリシー NAT を使用して、それぞれが異なるポートを使用する、1 つの実際のアドレスと宛先アドレスのペアを指定するには、次のコマンドを入力します。

```
hostname(config)# access-list WEB permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 80
hostname(config)# access-list TELNET permit tcp 10.1.2.0 255.255.255.0 209.165.201.11
255.255.255.255 eq 23
hostname(config)# nat (inside) 1 access-list WEB
hostname(config)# global (outside) 1 209.165.202.129
hostname(config)# nat (inside) 2 access-list TELNET
hostname(config)# global (outside) 2 209.165.202.130
```

関連コマンド

コマンド	説明
access-list deny-flow-max	作成できる同時拒否フローの最大数を指定します。
clear configure nat	NAT コンフィギュレーションを削除します。
global	グローバル アドレス プールに対してエントリを作成します。
interface	インターフェイスを作成および設定します。
show running-config nat	ネットワークに関連付けられているグローバル IP アドレスのプールを表示します。

nat（VPN ロード バランシング）

この装置の IP アドレスが NAT で変換される先の IP アドレスを設定するには、VPN ロードバランシング モードで **nat** コマンドを使用します。この NAT 変換をディセーブルにするには、このコマンドの **no** 形式を使用します。

nat *ip-address*

no nat [*ip-adddress*]

シンタックスの説明

ip-address	この NAT で、この装置の IP アドレスを変換する先の IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。

このコマンドの **no nat** 形式では、オプションの *ip-address* 値を指定する場合、IP アドレスが実行コンフィギュレーションの既存の NAT IP アドレスと一致する必要があります。

例

次は、VPN ロードバランシング コマンド シーケンスの例です。NAT 変換のアドレスを 192.168.10.10 に設定する **nat** コマンドが含まれています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

nat-control

NAT コントロールを適用するには、グローバル コンフィギュレーション モードで **nat-control** コマンドを使用します。NAT コントロールでは、内部ホストが外部にアクセスする場合、内部ホストには NAT が必要になります。NAT コントロールをディセーブルにするには、このコマンドの **no** 形式を使用します。

nat-control

no nat-control

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

NAT コントロールは、デフォルトではディセーブルです（**no nat-control** コマンド）。ただし、ソフトウェアを以前のバージョンからアップグレードしたときに、以前のバージョンでデフォルトがイネーブルであった場合は、NAT コントロールがイネーブルになることがあります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

NAT コントロールでは、内部インターフェイスから外部インターフェイスに移動するパケットは、1 つの NAT 規則に一致している必要があります。外部ネットワークのホストにアクセスする内部ネットワークのホストではすべて、内部ホスト アドレスを変換するように NAT を設定してください。

同じセキュリティ レベルのインターフェイスでは、通信用に NAT を使用する必要はありません。ただし、NAT コントロールがイネーブルになっている状態で同じセキュリティ インターフェイスのダイナミック NAT または PAT を設定する場合、内部インターフェイスから同じセキュリティのインターフェイスあるいは外部インターフェイスへのトラフィックはすべて、NAT 規則に一致している必要があります。

同様に、NAT コントロールと共に外部のダイナミック NAT または PAT をイネーブルにする場合、内部インターフェイスへのアクセス時には、すべての外部トラフィックが 1 つの NAT 規則に一致している必要があります。

NAT コントロールを使用するスタティック NAT では、このような制限は発生しません。

デフォルトでは、NAT コントロールはディセーブルになっているため、NAT の実行を選択しないかぎり、ネットワーク上で NAT を実行する必要はありません。

NAT コントロールのセキュリティを強化する必要があるが、内部アドレスが変換されることを望まない場合は、これらのアドレスに NAT 免除（**nat 0 access-list**）またはアイデンティティ NAT（**nat 0** または **static**）規則が適用できます。

（注） マルチ コンテキスト モードでは、パケット分類子はパケットをコンテキストに割り当てるために、NAT 設定に依存する場合があります。NAT コントロールがディセーブルであるという理由で NAT を実行しない場合、分類子によってはネットワーク コンフィギュレーションの変更が必要になることがあります。

例

次の例では、NAT コントロールをイネーブルにします。

```
hostname(config)# nat-control
```

関連コマンド

コマンド	説明
nat	1 つのインターフェイス上のアドレスを他の 1 つのインターフェイス上のマッピング アドレスに変換することを定義します。
show running-config nat-control	NAT コンフィギュレーションの要件を表示します。
static	実アドレスをマッピング アドレスに変換します。

nat-rewrite

DNS 応答の A レコードに埋め込まれた IP アドレスに対して NAT リライトをイネーブルにするには、パラメータ コンフィギュレーション モードで **nat-rewrite** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

nat-rewrite

no nat-rewrite

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

NAT リライトはデフォルトでイネーブルになっています。このコマンドは、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定している場合はイネーブルにできます。このコマンドをディセーブルにするには、**no nat-rewrite** をポリシー マップ コンフィギュレーションで明示的に指定する必要があります。**inspect dns** を設定していない場合、NAT リライトは実行されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

この機能は、DNS 応答で A タイプのリソース レコード（RR）の NAT 変換を実行します。

例

次の例では、DNS 検査ポリシー マップで NAT リライトをイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# nat-rewrite
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

nbns-server（トンネル グループ webvpn アトリビュート モード）

NBNS サーバを設定するには、トンネル グループ webvpn コンフィギュレーション モードで **nbns-server** コマンドを使用します。NBNS サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは NBNS サーバに照会して、NetBIOS 名を IP アドレスにマッピングします。リモート システム上のファイルにアクセスしたり、ファイルを共有したりするため、WebVPN には NetBIOS が必要です。

nbns-server {*ipaddr* | *hostname***}** [***master***] [***timeout*** *timeout*] [***retry*** *retries*]

no nbns-server

シンタックスの説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバの照会をリトライする回数を指定します。セキュリティ アプライアンスは、ユーザが指定した回数、サーバのリストを循環した後で、エラー メッセージを送信します。デフォルト値は 2 です。有効な範囲は、1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	セキュリティ アプライアンスがクエリーを再送信する前の待機時間を指定します。NBNS サーバが 1 つのみの場合は同じサーバに、複数ある場合は別のサーバに送信します。デフォルトのタイムアウトは 2 秒です。有効な範囲は、1 ～ 30 秒です。

デフォルト

デフォルトでは、NBNS サーバは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn モードからトンネル グループ webvpn コンフィギュレーション モードに変更されました。

使用上のガイドライン

リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn アトリビュート モードの同等のコマンドに変換されます。

最大 3 つのサーバ エントリを設定できます。設定する最初のサーバはプライマリ サーバで、残りの 2 つのサーバは冗長構成用のバックアップになります。

一致するエントリをコンフィギュレーションから削除するには、**no** オプションを使用します。

例

次の例は、10.10.10.19 の IP アドレス、10 秒のタイムアウト値、および 8 回のリトライでマスターブラウザである NBNS サーバを設定して使用して、トンネル グループ「テスト」を設定する方法を示しています。また、10.10.10.24 の IP アドレス、15 秒のタイムアウト値、および 8 回のリトライで NBNS WINS サーバを設定する方法を示しています。

```
hostname(config)# tunnel-group test type webvpn
hostname(config)# tunnel-group test webvpn-attributes
hostname(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	名前付きのトンネル グループの WebVPN アトリビュートを指定します。

nbns-server（webvpn モード）

NBNS サーバを設定するには、トンネル グループ webvpn コンフィギュレーション モードで **nbns-server** コマンドを使用します。NBNS サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスは NBNS サーバに照会して、NetBIOS 名を IP アドレスにマッピングします。リモート システム上のファイルにアクセスしたり、ファイルを共有したりするため、WebVPN には NetBIOS が必要です。

nbns-server {*ipaddr* | *hostname***}** [***master***] [***timeout*** *timeout*] [***retry*** *retries*]

no nbns-server

シンタックスの説明

hostname	NBNS サーバのホスト名を指定します。
ipaddr	NBNS サーバの IP アドレスを指定します。
master	WINS サーバではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバの照会をリトライする回数を指定します。セキュリティ アプライアンスは、ユーザが指定した回数、サーバのリストを循環した後で、エラー メッセージを送信します。デフォルト値は 2 です。有効な範囲は、1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	セキュリティ アプライアンスがクエリーを再送信する前の待機時間を指定します。NBNS サーバが 1 つのみの場合は同じサーバに、複数ある場合は別のサーバに送信します。デフォルトのタイムアウトは 2 秒です。有効な範囲は、1 ～ 30 秒です。

デフォルト

デフォルトでは、NBNS サーバは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	webvpn モードからトンネル グループ webvpn コンフィギュレーション モードに変更されました。

使用上のガイドライン

このコマンドは、webvpn コンフィギュレーション モードでは廃止されました。トンネル グループ webvpn アトリビュート コンフィギュレーション モードの nbns-server コマンドで置き換えられています。リリース 7.1(1) では、このコマンドを webvpn コンフィギュレーション モードで入力すると、トンネル グループ webvpn アトリビュート モードの同等のコマンドに変換されます。

最大 3 つのサーバ エントリを設定できます。設定する最初のサーバはプライマリ サーバで、残りの 2 つのサーバは冗長構成用のバックアップになります。

一致するエントリをコンフィギュレーションから削除するには、**no** オプションを使用します。

例

次の例は、10.10.10.19 の IP アドレス、10 秒のタイムアウト値、および 8 回のリトライでマスターブラウザである NBNS サーバを設定する方法を示しています。また、10.10.10.24 の IP アドレス、15 秒のタイムアウト値、および 8 回のリトライで NBNS WINS サーバを設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
hostname(config-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
```

neighbor

ポイントツーポイントの非ブロードキャスト ネットワークにスタティック ネイバーを定義するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。スタティックに定義されたネイバーをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。**neighbor** コマンドは、VPN トンネルを介して OSPF ルートをアドバタイジングする場合に使用します。

neighbor *ip_address* [***interface*** *name*]

no neighbor *ip_address* [***interface*** *name*]

シンタックスの説明

interface *name*	（オプション）**nameif** コマンドで指定されるインターフェイス名。これを介して、ネイバーに到達できるようになります。
ip_address	隣接ルータの IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

既知の各非ブロードキャスト ネットワーク ネイバーに、ネイバー エントリが 1 つ含まれている必要があります。インターフェイスのプライマリ アドレスに、ネイバー アドレスが存在する必要があります。

システムに直接接続されているインターフェイスと同じネットワーク上にネイバーがない場合、***interface*** オプションが指定されている必要があります。さらに、ネイバーに到達するには、スタティック ルートが作成されている必要があります。

例

次の例では、192.168.1.1 のアドレスの隣接ルータを定義します。

```
hostname(config-router)# neighbor 192.168.1.1
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

nem

ハードウェア クライアントのネットワーク拡張モードをイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。NEM をディセーブルにするには、**nem disable** コマンドを使用します。NEM アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループ ポリシーから継承できます。

nem {**enable** | **disable**}

no nem

シンタックスの説明

disable	ネットワーク拡張モードをディセーブルにします。
enable	ネットワーク拡張モードをイネーブルにします。

デフォルト

ネットワーク拡張モードはディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

使用上のガイドライン

ネットワーク拡張モードにより、ハードウェア クライアントは、VPN トンネルを介したリモート プライベート ネットワークに対して、ルーティング可能なネットワークを 1 つ提示できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークからセキュリティ アプライアンスの背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、セキュリティ アプライアンスの背後にある装置は、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワークに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。ハードウェア クライアントがトンネルを開始する必要がありますが、トンネルがアップの状態になった後は、どちらの側からもデータ交換を開始できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup という名前のグループ ポリシーの NEM を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
```

network

RIP ルーティング プロセスのネットワーク リストを指定するには、ルータ コンフィギュレーション モードで **network** コンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

network *ip_addr*

no network *ip_addr*

シンタックスの説明

ip_addr	直接接続されたネットワークの IP アドレスを指定します。指定されたネットワークに接続されたインターフェイスは、RIP ルーティング プロセスに参加します。

デフォルト

指定されているネットワークはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

指定のネットワーク番号にサブネット情報を含めないようにしてください。ルータで使用できるネットワーク コマンドの数には制限がありません。RIP ルーティング アップデートは、指定されたネットワークのインターフェイスを経由してのみ送受信されます。また、インターフェイスのネットワークが指定されていない場合、そのインターフェイスは RIP アップデートでアドバタイズされません。

例

次の例では、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されたすべてのインターフェイスで使用されるルーティング プロトコルとして RIP を定義します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# network 192.168.7.0
```

関連コマンド

コマンド	説明
router rip	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

network area

OSPF が動作するインターフェイスを定義し、これらのインターフェイスのエリア ID を定義するには、ルータ コンフィギュレーション モードで **network area** コマンドを使用します。アドレス / ネットマスクのペアで定義したインターフェイスの OSPF ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

network *addr mask* ***area*** *area_id*

no network *addr mask* ***area*** *area_id*

シンタックスの説明

addr	IP アドレスを指定します。
area *area_id*	OSPF アドレス範囲に関連付けられるエリアを指定します。*area_id* は、IP アドレス形式または 10 進数形式のいずれかで指定できます。10 進数形式で指定した場合、有効値の範囲は 0 ～ 4294967295 です。
mask	ネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

インターフェイスで OSPF を動作させるには、**network area** コマンドでインターフェイスのアドレスが指定されている必要があります。**network area** コマンドでカバーされていないインターフェイスの IP アドレスがあれば、そのインターフェイス上では OSPF がイネーブルになりません。

セキュリティ アプライアンスで使用できる **network area** コンドの数には制限がありません。

例

次の例では、192.168.1.1 のインターフェイスで OSPF をイネーブルにし、エリア 2 に割り当てます。

```
hostname(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

network-object

ネットワーク オブジェクト グループにネットワーク オブジェクトを追加するには、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用します。ネットワーク オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

network-object host *host_addr* | *host_name*

no network-object host *host_addr* | *host_name*

network-object *net_addr netmask*

no network-object *net_addr netmask*

シンタックスの説明

host_addr	ホスト IP アドレス（**name** コマンドを使用してホスト名がまだ定義されていない場合）。
host_name	ホスト名（**name** コマンドを使用してホスト名が定義されている場合）。
net_addr	ネットワーク アドレス。*netmask* と共に使用してサブネット オブジェクトを定義します。
netmask	ネットマスク。*net_addr* と共に使用してサブネット オブジェクトを定義します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ネットワーク コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ネットワーク コンフィギュレーション モードでホストまたはサブネット オブジェクトを定義するには、**object-group** コマンドと共に **network-object** コマンドを使用します。

例

次の例は、ネットワーク コンフィギュレーション モードで **network-object** コマンドを使用して、新しいネットワーク オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network sjj_eng_ftp_servers
hostname(config-network)# network-object host sjj.eng.ftp
hostname(config-network)# network-object host 172.16.56.195
hostname(config-network)# network-object 192.168.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# quit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

nt-auth-domain-controller

このサーバの NT プライマリ ドメイン コントローラ名を指定するには、AAA サーバ ホスト モードで **nt-auth-domain-controller** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

nt-auth-domain-controller *string*

no nt-auth-domain-controller

シンタックスの説明

string	このサーバの、最大 16 文字のプライマリ ドメイン コントローラ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、NT 認証の AAA サーバでのみ有効です。最初に **aaa-server host** コマンドを使用して、ホスト コンフィギュレーション モードに入る必要があります。*string* 変数の名前は、サーバ自体の NT エントリに一致する必要があります。

例

次の例では、このサーバの NT プライマリ ドメイン コントローラ名を「primary1」に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol nt
hostname(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# nt-auth-domain-controller primary1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

ntp authenticate

NTP サーバを使用する認証をイネーブルにするには、グローバル コンフィギュレーション モードで **ntp authenticate** コマンドを使用します。NTP 認証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ntp authenticate

no ntp authenticate

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

認証をイネーブルにすると、セキュリティ アプライアンスは、NTP サーバが正しい信頼できるキーをパケットで使用している場合に限り、NTP サーバと通信します（**ntp trusted-key** コマンドを参照）。セキュリティ アプライアンスは、認証キーを NTP サーバと同期をとるためにも使用します（**ntp authentication-key** コマンドを参照）。

例

次の例では、NTP パケットで認証キー 42 を使用しているシステムのみと同期するようにセキュリティ アプライアンスを設定します。

```
hostname(config)# ntp authenticate
hostname(config)# ntp authentication-key 42 md5 aNiceKey
hostname(config)# ntp trusted-key 42
```

関連コマンド

コマンド	説明
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp authentication-key

NTP サーバを使用して認証を行うためのキーを設定するには、グローバル コンフィギュレーション モードで **ntp authentication-key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

ntp authentication-key *key_id* ***md5*** *key*

no ntp authentication-key *key_id* [***md5*** *key*]

シンタックスの説明

key_id	1 ～ 4294967295 のキー ID を指定します。**ntp trusted-key** コマンドを使用して、この ID を信頼できるキーとして指定する必要があります。
md5	MD5 として認証アルゴリズムを指定します。MD5 はサポートされている唯一のアルゴリズムです。
key	キーの値を、最大 32 文字の文字列として設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 と 2 を指定し、信頼できる各キー ID の認証キーを設定しています。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp server

セキュリティ アプライアンスの時刻を設定するために NTP サーバを指定するには、グローバル コンフィギュレーション モードで **ntp server** コマンドを使用します。Auto Update Server を削除するには、このコマンドの **no** 形式を使用します。複数のサーバを指定できます。セキュリティ アプライアンスは、最も正確なサーバを使用します。マルチ コンテキスト モードでは、システム コンフィギュレーションにのみ NTP サーバを設定します。

ntp server *ip_address* [***key*** *key_id*] [***source*** *interface_name*] [***prefer***]

no ntp server *ip_address* [***key*** *key_id*] [***source*** *interface_name*] [***prefer***]

シンタックスの説明

ip_address	NTP サーバの IP アドレスを設定します。
key *key_id*	**ntp authenticate** コマンドを使用して認証をイネーブルにする場合、このサーバの信頼できるキー ID を設定します。**ntp trusted-key** コマンドも参照してください。
source *interface_name*	ルーティング テーブルでデフォルトのインターフェイスを使用しない場合は、NTP パケットの発信インターフェイスを指定します。システムはマルチ コンテキスト モードのインターフェイスを包含しないので、管理コンテキストで定義されたインターフェイス名を指定します。
prefer	複数のサーバの正確性がほとんど変わらない場合、この NTP サーバを優先サーバとして設定します。NTP はアルゴリズムを使用して、最も正確なサーバを判別し、そのサーバと同期を取ります。複数のサーバの正確性がほとんど変わらない場合、***prefer*** キーワードが使用するサーバを指定します。しかし、特定のサーバの正確性が優先サーバより際立っている場合、セキュリティ アプライアンスはより正確なサーバを使用します。たとえば、セキュリティ アプライアンスは、優先された層 3 のサーバではなく、層 2 のサーバを使用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、送信元インターフェイスをオプションで使用するように修正されました。

例

次の例では、2 つの NTP サーバを指定し、キー ID 1 と 2 の認証をイネーブルにします。

```
hostname(config)# ntp server 10.1.1.1 key 1 prefer
hostname(config)# ntp server 10.2.1.1 key 2
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp trusted-key

信頼できるキー（NTP サーバを使用する認証に必要）として認証キー ID を指定するには、グローバル コンフィギュレーション モードで **ntp trusted-key** コマンドを使用します。信頼できるキーを削除するには、このコマンドの **no** 形式を使用します。複数のサーバで使用する、複数の信頼できるキーを入力できます。

ntp trusted-key *key_id*

no ntp trusted-key *key_id*

シンタックスの説明

key_id	1 ～ 4294967295 のキー ID を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドも設定します。サーバと同期を取るには、**ntp authentication-key** コマンドを使用して、キー ID の認証キーを設定します。

例

次の例では、認証をイネーブルにし、信頼できるキー ID 1 と 2 を指定し、信頼できる各キー ID の認証キーを設定しています。

```
hostname(config)# ntp authenticate
hostname(config)# ntp trusted-key 1
hostname(config)# ntp trusted-key 2
hostname(config)# ntp authentication-key 1 md5 aNiceKey
hostname(config)# ntp authentication-key 2 md5 aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

num-packets

SLA オペレーション中に送信される要求パケット数を指定するには、SLA モニタ プロトコル コンフィギュレーション モードで **num-packets** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

num-packets *number*

no num-packets *number*

シンタックスの説明

number	SLA オペレーション中に送信されるパケットの数を指定します。有効な値は 1 ～ 100 です。

デフォルト

送信されるエコー タイプのパケットのデフォルト数は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

パケット損失による正確でない到達情報を防止するために送信されるパケットのデフォルト数を増やします。

例

次の例では、ICMP エコー要求 / 応答時間プローブ オペレーションを使用する、ID が 123 の SLA オペレーションを設定しています。エコー要求パケットのペイロード サイズを 48 バイト、SLA オペレーション中に送信されるエコー要求の数を 5 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
request-data-size	要求パケットのペイロードのサイズを指定します。
sla monitor	SLA 監視オペレーションを定義します。
type echo	SLA オペレーションをエコー応答時間プローブ オペレーションとして設定します。

object-group

コンフィギュレーションの最適化に使用できるオブジェクト グループを定義するには、グローバル コンフィギュレーション モードで **object-group** コマンドを使用します。コンフィギュレーションからオブジェクト グループを削除するには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

no object-group {**protocol** | **network** | **icmp-type**} *obj_grp_id*

object-group service *obj_grp_id* {**tcp** | **udp** | **tcp-udp**}

no object-group service *obj_grp_id* {**tcp** | **udp** | **tcp-udp**}

シンタックスの説明

icmp-type	echo や echo-reply など、ICMP タイプのグループを定義します。メインの **object-group icmp-type** コマンドを入力した後、**icmp-object** コマンドと **group-object** コマンドを使用して ICMP オブジェクトを ICMP タイプ グループに追加します。
network	ホストまたはサブネット IP アドレスのグループを定義します。メインの **object-group network** コマンドを入力した後、**network-object** コマンドと **group-object** コマンドを使用してネットワーク オブジェクトをネットワーク グループに追加します。
obj_grp_id	オブジェクト グループ（1 ～ 64 文字）を指定します。アルファベット、数字、アンダースコア（_）、ハイフン（-）、およびピリオド（.）を任意に組み合せることができます。
protocol	TCP や UDP などのプロトコル グループを定義します。メインの **object-group protocol** コマンドを入力した後、**protocol-object** コマンドと **group-object** コマンドを使用してプロトコル オブジェクトをプロトコル グループに追加します。
service	「eq smtp」や「range 2000 2010」などの TCP/UDP ポート仕様のグループを定義します。メインの **object-group service** コマンドを入力した後、**port-object** コマンドと **group-object** コマンドを使用してポート オブジェクトをサービス グループに追加します。
tcp	サービス グループが TCP に使用されることを指定します。
tcp-udp	サービス グループが TCP および UDP に使用できることを指定します。
udp	サービス グループが UDP に使用されることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ホスト、プロトコル、サービスなどのオブジェクトはグループ化できます。グループ化をすると、グループ名を使用して 1 つのコマンドを発行してグループ内のすべての項目に適用できます。

object-group コマンドでグループを定義してから、任意のセキュリティ アプライアンス コマンドを使用すると、そのコマンドはグループ内のすべての項目に適用されます。この機能によってコンフィギュレーション サイズをかなり削減できます。

オブジェクト グループを定義したら、次のように、該当するすべてのセキュリティ アプライアンス コマンドで **object-group** キーワードの後にグループ名を使用する必要があります。

```
hostname# show running-config object-group group_name
```

group_name はグループの名前です。

次の例は、オブジェクト グループを定義した後で使用する方法を示しています。

```
hostname(config)# access-list access_list_name permit tcp any object-group group_name
```

また、**access list** コマンドの引数をグループ化できます。

個々の引数	代替用のオブジェクト グループ
protocol	**object-group** *protocol*
host and subnet	**object-group** *network*
service	**object-group** *service*
icmp_type	**object-group** *icmp_type*

コマンドは階層構造にグループ化できます。したがって、あるオブジェクト グループを別のオブジェクト グループのメンバーにできます。

オブジェクト グループを使用するには、次のことを実行する必要があります。

- **object-group** キーワードは、すべてのコマンドでオブジェクト グループ名の前に使用する。

  ```
  hostname(config)# access-list acl permit tcp object-group remotes object-group
  locals object-group eng_svc
  ```

  ここで、*remotes* および *locals* はオブジェクト グループ名です。
- オブジェクト グループを空にしない。
- 別のコマンドで現在使用されている場合は、オブジェクト グループを削除したり、空にしたりすることはできない。

メインの **object-group** コマンドが入力されると、コマンド モードは対応するモードに変わります。オブジェクト グループは新規のモードで定義されます。アクティブ モードがコマンド プロンプト形式で示されます。たとえば、コンフィギュレーション端末モードのプロンプトは次のように表示されます。

```
hostname(config)#
```

ここで、*hostname* はセキュリティ アプライアンスの名前です。

しかし、**object-group** コマンドを入力すると、プロンプトは次のように表示されます。

```
hostname(config-type)#
```

hostname はセキュリティ アプライアンスの名前、*type* は*オブジェクト グループのタイプ*です。

object-group モードを抜け、**object-group** メイン コマンドを終了するには、**exit** や **quit** コマンド、または **access-list** コマンドなどの有効な任意のコンフィギュレーション モードのコマンドを使用します。

show running-config object-group コマンドは、定義されているすべてのオブジェクト グループを表示します。このとき、**show running-config object-group** *grp_id* コマンドを入力した場合は *grp_id* ごとに、**show running-config object-group** *grp_type* コマンドを入力した場合はグループ タイプごとに表示されます。引数を指定せずに **show running-config object-group** コマンドを入力すると、定義されているすべてのオブジェクト グループが表示されます。

それまでに定義した **object-group** コマンドのグループを削除するには、**clear configure object-group** コマンドを使用します。引数を指定せずに **clear configure object-group** コマンドを使用すると、コマンドで使用中でない定義済のオブジェクト グループすべてが削除できます。*grp_type* 引数は、コマンドで使用中でない定義済のオブジェクト グループすべてのうち、そのグループ タイプだけを削除します。

object-group モードでは、**show running-config** および **clear configure** コマンドを含む他のすべてのセキュリティ アプライアンス コマンドを使用できます。

object-group モード内のコマンドは、**show running-config object-group** コマンド、**write** コマンド、または **config** コンドで表示または保存した場合は、字下げして表示されます。

object-group モード内のコマンドには、メイン コマンドと同じコマンド特権レベルがあります。

access-list コマンドで複数のオブジェクト グループを使用している場合、このコマンドで使用されるすべてのオブジェクト グループの要素は相互に連結されます。最初に 1 番目のグループ要素が 2 番目のグループ要素に連結され、1 番目と 2 番目のグループ要素が 3 番目のグループ要素に連結されるというようになります。

説明テキストの開始位置は、**description** キーワードに続く空白（ブランクまたはタブ）直後の文字です。

例

次の例は、**object-group icmp-type** モードを使用して新しい icmp-type オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group icmp-type icmp-allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(config-icmp-type)# exit
```

次の例は、**object-group network** コマンドを使用して新しいネットワーク オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network sjc_eng_ftp_servers
hostname(config-network)# network-object host sjc.eng.ftp.servcers
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object 192.1.1.0 255.255.255.224
hostname(config-network)# exit
```

次の例は、**object-group network** コマンドを使用して新しいネットワーク オブジェクト グループを作成し、既存のオブジェクト グループにマッピングする方法を示しています。

```
hostname(config)# object-group network sjc_ftp_servers
hostname(config-network)# network-object host sjc.ftp.servers
hostname(config-network)# network-object host 172.23.56.195
hostname(config-network)# network-object 193.1.1.0 255.255.255.224
hostname(config-network)# group-object sjc_eng_ftp_servers
hostname(config-network)# exit
```

次の例は、**object-group protocol** モードを使用して新しいプロトコル オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object ipsec
hostname(config-protocol)# exit

hostname(config)# object-group protocol proto_grp_2
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
```

次の例は、**object-group service** モードを使用して新しいポート（サービス）オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# group-object eng_www_service
hostname(config-service)# port-object eq ftp
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# exit
```

次の例は、テキスト説明をオブジェクト グループに追加およびオブジェクト グループから削除する方法を示しています。

```
hostname(config)# object-group protocol protos1
hostname(config-protocol)# description This group of protocols is for our internal
network

hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
description: This group of protocols is for our internal network

hostname(config-protocol)# no description
hostname(config-protocol)# show running-config object-group id protos1
object-group protocol protos1
```

次の例は、**group-object** モードを使用して、すでに定義済みのオブジェクトで構成される新しいオブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group network host_grp_1
hostname(config-network)# network-object host 192.168.1.1
hostname(config-network)# network-object host 192.168.1.2
hostname(config-network)# exit

hostname(config)# object-group network host_grp_2
hostname(config-network)# network-object host 172.23.56.1
hostname(config-network)# network-object host 172.23.56.2
hostname(config-network)# exit

hostname(config)# object-group network all_hosts
hostname(config-network)# group-object host_grp_1
hostname(config-network)# group-object host_grp_2
hostname(config-network)# exit

hostname(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
hostname(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
hostname(config)#access-list all permit tcp object-group all_hosts any eq www
```

group-object コマンドを使用しない場合は、*host_grp_1* と *host_grp_2* にすでに定義済みの IP アドレスをすべて含むように *all_hosts* グループを定義する必要があります。**group-object** コマンドを指定する場合は、重複してホストを定義する必要がなくなります。

次の例は、オブジェクト グループを使用してアクセス リストのコンフィギュレーションを簡略化する方法を示しています。

```
hostname(config)# object-group network remote
hostname(config-network)# network-object host kqk.suu.dri.ixx
hostname(config-network)# network-object host kqk.suu.pyl.gnl

hostname(config)# object-group network locals
hostname(config-network)# network-object host 172.23.56.10
hostname(config-network)# network-object host 172.23.56.20
hostname(config-network)# network-object host 172.23.56.194
hostname(config-network)# network-object host 172.23.56.195

hostname(config)# object-group service eng_svc ftp
hostname(config-service)# port-object eq www
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object range 25000 25100
```

このグループ化により、グループ化を使用しないと 24 行になるアクセス リストを 1 行で設定できます。その代わり、グループ化を使用するとアクセス リストのコンフィギュレーションは次のようになります。

```
hostname(config)# access-list acl permit tcp object-group remote object-group locals
object-group eng_svc
```

(注) **show running-config object-group** コマンドおよび **write** コマンドを使用すると、オブジェクト グループ名で設定されているようにアクセス リストを表示できます。**show access-list** コマンドは、オブジェクトをグループ化せずに、アクセス リスト エントリを個々のエントリに展開して表示します。

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

ocsp disable-nonce

デフォルトでは、OCSP 要求にナンス拡張子が含まれます。これは、要求を暗号でバインドしてリプレイ アタックを防ぐためのものです。ただし、一部の OCSP サーバは、この照合ナンス拡張子が含まれない、事前に生成された応答を使用します。これらのサーバで OCSP を使用するには、ナンス拡張子をディセーブルにする必要があります。

ナンス拡張子をディセーブルにするには、暗号 CA トラストポイント モードで **ocsp disable-nonce** コマンドを使用します。ナンス拡張子をもう一度イネーブルにするには、このコマンドの **no** 形式を使用します。

ocsp disable-nonce

no ocsp disable-nonce

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトでは、OCSP 要求にナンス拡張子が含まれます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、OCSP 要求には OCSP ナンス拡張子が含まれず、セキュリティ アプライアンスはチェックを行いません。

例

次の例では、newtrust というトラストポイントのナンス拡張子をディセーブルにする方法を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp disable-nonce
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードに入ります。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書き規則を設定します。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするための OCSP サーバを指定します。
revocation-check	失効のチェックに使用する方法（複数可）、およびその試行順序を指定します。

ocsp url

クライアント証明書の AIA 拡張子に指定されているサーバではなくトラストポイントに関連付けられているすべての証明書をチェックするよう、セキュリティ アプライアンスを使用して OCSP サーバを設定するには、暗号 CA トラストポイント モードで **ocsp url** コマンドを使用します。サーバをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

ocsp url *URL*

no ocsp url

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは HTTP URL のみサポートし、各トランスポイントに URL を 1 つだけ指定できます。

セキュリティ アプライアンスでは OCSP サーバ URL を定義する方法が 3 つあり、定義する方法に従って次の順序で OCSP サーバの使用を試みます。

- **match certificate** コマンドを使用して設定する OCSP サーバ
- **ocsp url** コマンドを使用して設定する OCSP サーバ
- クライアント証明書の AIA フィールドの OCSP サーバ

match certificate コマンド、または **ocsp url** コマンドを使用して OCSP URL を設定しない場合、セキュリティ アプライアンスはクライアント証明書の AIA 拡張子で OCSP サーバを使用します。証明書に AIA 拡張が含まれていない場合、失効ステータスのチェックは失敗します。

例

次の例では、URL http://10.1.124.22 で OCSP サーバを設定する方法を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# ocsp url http://10.1.124.22
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードに入ります。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書き規則を設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
revocation-check	失効のチェックに使用する方法（複数可）、およびその試行順序を指定します。

ospf authentication

OSPF 認証の使用をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ospf authentication** コマンドを使用します。デフォルトの認証スタンスに戻すには、このコマンドの **no** 形式を使用します。

ospf authentication [***message-digest*** | ***null***]

no ospf ***authentication***

シンタックスの説明

message-digest	（オプション）OSPF メッセージ ダイジェスト認証を使用するように指定します。
null	（オプション）OSPF 認証を使用しないように指定します。

デフォルト

デフォルトでは、OSPF 認証はイネーブルではありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf authentication コマンドを使用する前に、**ospf authentication-key** コマンドを使用してインターフェイスのパスワードを設定します。***message-digest*** キーワードを使用する場合、**ospf message-digest-key** コマンドを使用して、インターフェイスのメッセージ ダイジェスト キーを設定します。

下位互換性を維持するため、エリアの認証タイプが継続してサポートされます。認証タイプがインターフェイスに指定されていない場合、エリアの認証タイプが使用されます（エリアのデフォルトは null 認証です）。

オプションを指定せずにこのコマンドを使用する場合、簡易パスワード認証がイネーブルにされます。

例

次の例は、選択したインターフェイスで OSPF の簡易パスワード認証をイネーブルにする方法を示しています。

```
hostname(config-if)# ospf authentication
hostname(config-if)#
```

関連コマンド

コマンド	説明
ospf ***authentication-key***	隣接ルーティング デバイスで使用するためのパスワードを指定します。
ospf message-digest-key	MD5 認証をイネーブルにし、MD5 キーを指定します。

ospf authentication-key

隣接ルーティング デバイスで使用されるパスワードを指定するには、インターフェイス コンフィギュレーション モードで **ospf authentication-key** コマンドを使用します。パスワードを削除するには、このコマンドの **no** 形式を使用します。

ospf *authentication-key* *password*

no ospf authentication-key

シンタックスの説明

password	隣接ルーティング デバイスで使用するための OSPF 認証パスワードを割り当てます。パスワードは、9 文字未満にする必要があります。2 文字の間にブランク スペースを含めることができます。パスワードの最初または最後のスペースは無視されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドによって作成されたパスワードは、ルーティング プロトコル パケットが発信されるときに、OSPF ヘッダーに直接挿入されるキーとして使用されます。インターフェイス単位で、別個のパスワードを各ネットワークに割り当てることができます。同一ネットワーク上のすべての隣接ルータが、OSPF 情報を交換できる同じパスワードを持つ必要があります。

例

次の例は、OSPF 認証のパスワードを指定する方法を示しています。

```
hostname(config-if)# ospf authentication-key ThisMyPW
```

関連コマンド

コマンド	説明
area authentication	指定したエリアの OSPF 認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf cost

インターフェイスを介した 1 パケットの送信コストを指定するには、インターフェイス コンフィギュレーション モードで **ospf cost** コマンドを使用します。インターフェイス コストをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

ospf cost *interface_cost*

no ospf cost

シンタックスの説明

interface_cost	インターフェイスを介した 1 パケットの送信コスト（リンク状態メトリック）。これは 0 ～ 65535 の符号なし整数値です。0 は、インターフェイスに直接接続されているネットワークを表し、インターフェイスの帯域幅が高くなるほど、そのインターフェイスを通してパケットを送信する関連コストは低くなります。つまり、大きいコスト値は低い帯域幅のインターフェイスを表し、小さいコスト値は高い帯域幅のインターフェイスを表します。 セキュリティ アプライアンス上にある OSPF インターフェイスのデフォルト コストは 10 です。このデフォルトは Cisco IOS ソフトウェアのデフォルト コスト、ファースト イーサネットおよびギガビット イーサネットの場合の 1、10BaseT の場合の 10 とは異なります。ECMP をネットワークで使用している場合は、このことを考慮に入れておくことが重要です。

デフォルト

デフォルトの *interface_cost* は 10 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf cost コマンドを使用すると、インターフェイスでの 1 パケットの送信コストを明示的に指定できます。*interface_cost* パラメータは、0 ～ 65535 の符号なし整数値です。

no ospf cost コマンドを使用すると、パス コストをデフォルト値にリセットできます。

例

次の例は、選択したインターフェイスで 1 パケットの送信コストを指定する方法を示しています。

```
hostname(config-if)# ospf cost 4
```

関連コマンド

コマンド	説明
show running-config interface	指定したインターフェイスのコンフィギュレーションを表示します。

ospf database-filter

同期およびフラッディング中に OSPF インターフェイスへのすべての発信 LSA をフィルタリングするには、インターフェイス コンフィギュレーション モードで **ospf database-filter** コマンドを使用します。LSA を復元するには、このコマンドの **no** 形式を使用します。

ospf database-filter ***all out***

no ospf database-filter ***all out***

シンタックスの説明

all out	OSPF インターフェイスへのすべての発信 LSA をフィルタリングします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf database-filter コマンドは、OSPF インターフェイスへの発信 LSA をフィルタリングします。**no ospf database-filter all out** コマンドは、インターフェイスへの LSA のフォワーディングを復元します。

例

次の例は、**ospf database-filter** コマンドを使用して、発信 LSA をフィルタリングする方法を示しています。

```
hostname(config-if)# ospf database-filter all out
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf dead-interval

ネイバーがルータのダウンを宣言するまでの間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf dead-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf dead-interval *seconds*

no ospf dead-interval

シンタックスの説明

seconds	hello パケットを 1 つも受信しない時間。*seconds* のデフォルトは、**ospf hello-interval** コマンドで設定した間隔の 4 倍です（範囲は 1 ～ 65,535）。

デフォルト

seconds のデフォルト値は、**ospf hello-interval** コマンドで設定した間隔の 4 倍です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf dead-interval コマンドを使用すると、ネイバーがルータのダウンを宣言するまでのデッド間隔（hello パケットを 1 つも受信しない時間）を設定できます。*seconds* 引数はデッド間隔を指定します。この値はネットワーク上のすべてのノードで同じにする必要があります。*seconds* のフォルトは、**ospf hello-interval** コマンドで設定した間隔の 4 倍です（1 ～ 65,535）。

no ospf dead-interval コマンドを使用すると、デフォルトの間隔値に戻ります。

例

次の例では、OSPF デッド間隔を 1 分に設定します。

```
hostname(config-if)# ospf dead-interval 60
```

関連コマンド

コマンド	説明
ospf hello-interval	インターフェイスで hello パケットを送信する間隔を指定します。
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf hello-interval

インターフェイスで hello パケットを送信する間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf hello-interval** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf hello-interval *seconds*

no ospf hello-interval

シンタックスの説明

seconds	インターフェイスで hello パケットを送信する間隔を指定します。有効値は、1 ～ 65,535 秒です。

デフォルト

hello-interval *seconds* のデフォルト値は 10 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

この値は、hello パケットでアドバタイズされます。hello 間隔が短いほど、トポロジの変更が早急に検出されますが、より多くのルーティング トラフィックが結果として生じます。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバで同じにする必要があります。

例

次の例では、OSPF の hello 間隔を 5 秒に設定します。

```
hostname(config-if)# ospf hello-interval 5
```

関連コマンド

コマンド	説明
ospf dead-interval	ネイバーがルータのダウンを宣言するまでの間隔を指定します。
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf message-digest-key

OSPF の MD5 認証をイネーブルにするには、インターフェイス コンフィギュレーション モードで **ospf message-digest-key** コマンドを使用します。MD5 キーを削除するには、このコマンドの **no** 形式を使用します。

ospf message-digest-key *key-id* ***md5*** *key*

no ospf message-digest-key

シンタックスの説明

key-id	MD5 認証をイネーブルにし、数値による認証キー ID 番号を指定します。有効値は、1 ～ 255 です。
md5 *key*	最大 16 バイトの英数字によるパスワード。キー文字の間にスペースを含めることができます。キーの最初または最後のスペースは無視されます。MD5 認証は、通信整合性の検証、送信元の認証、および適時性の確認を行います。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ospf message-digest-key コマンドを使用すると、MD5 認証をイネーブルにできます。このコマンドの **no** 形式を使用すると、古い MD5 キーを削除できます。*key_id* は、1 ～ 255 の認証キー用数値 ID で、*key* は、最大 16 バイトの英数字によるパスワードです。MD5 は、通信整合性の検証、送信元の認証、および適時性の確認を行います。

例

次の例は、OSPF 認証の MD5 キーを指定する方法を示しています。

```
hostname(config-if)# ospf message-digest-key 3 md5 ThisIsMyMd5Key
```

関連コマンド

コマンド	説明
area authentication	OSPF エリア認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf mtu-ignore

データベース パケット受信時の OSPF の Maximum Transmission Unit（MTU; 最大伝送ユニット）ミスマッチ検出をディセーブルにするには、インターフェイス コンフィギュレーション モードで **ospf mtu-ignore** コマンドを使用します。MTU ミスマッチ検出を復元するには、このコマンドの **no** 形式を使用します。

ospf mtu-ignore

no ospf mtu-ignore

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、**ospf mtu-ignore** はイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

OSPF は、ネイバーが共通のインターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーが Database Descriptor（DBD）パケットを交換するときに実行されます。DBD パケット受信時の MTU が着信インターフェイスに設定された IP MTU より高い場合、OSPF の隣接関係が確立されません。**ospf mtu-ignore** コマンドは、DBD パケット受信時の OSPF MTU ミスマッチ検出をディセーブルにします。これは、デフォルトでイネーブルになっています。

例

次の例は、**ospf mtu-ignore** コマンドをディセーブルにする方法を示しています。

```
hostname(config-if)# ospf mtu-ignore
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス情報を表示します。

ospf network point-to-point non-broadcast

OSPF インターフェイスをポイントツーポイントの非ブロードキャスト ネットワークとして設定するには、インターフェイス コンフィギュレーション モードで **ospf network** ***point-to-point non-broadcast*** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。**ospf network** ***point-to-point non-broadcast*** コマンドを使用すると、VPN トンネルを介して OSPF ルートを送信できます。

ospf network ***point-to-point non-broadcast***

no ospf network ***point-to-point non-broadcast***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイスをポイントツーポイントとして指定する場合、OSPF ネイバーを手動で設定する必要があります。ダイナミック検出はできません。OSPF ネイバーを手動で設定するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。

インターフェイスをポイントツーポイントとして設定すると、次の制約事項が適用されます。

- 2 つ以上のネイバーをインターフェイスに定義できない。
- 暗号エンドポイントに向かうスタティック ルートを定義する必要がある。
- ネイバーを明示的に設定しないと、インターフェイスが隣接関係を形成できない。
- トンネルを介した OSPF がインターフェイスで実行されている場合、同じインターフェイス上で上流のルータによる標準 OSPF を実行できない。
- VPN トンネルを介して OSPF アップデートを受け渡すように OSPF ネイバーを指定する前に、インターフェイスに暗号マップをバインドする必要がある。OSPF ネイバーを指定した後、暗号マップをインターフェイスにバインドする場合、**clear local-host all** コマンドを使用して、OSPF 接続を消去し、OSPF の隣接関係が VPN トンネルを介して確立されるようにします。

例

次の例は、選択したインターフェイスをポイントツーポイントの非ブロードキャスト インターフェイスとして設定する方法を示しています。

```
hostname(config-if)# ospf network point-to-point non-broadcast
hostname(config-if)#
```

関連コマンド

コマンド	説明
neighbor	手動で設定された OSPF ネイバーを指定します。
show interface	インターフェイスのステータス情報を表示します。

ospf priority

OSPF ルータの優先順位を変更するには、インターフェイス コンフィギュレーション モードで **ospf priority** コマンドを使用します。デフォルトの優先順位に戻すには、このコマンドの **no** 形式を使用します。

ospf priority *number*

no ospf priority [*number*]

シンタックスの説明

number	ルータの優先順位を指定します。有効値は 0 ～ 255 です。

デフォルト

number のデフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ネットワークに接続されている 2 つのルータの両方が代表ルータになることを試行する場合、ルータの優先順位が高いルータが優先されます。両方のルータが同等である場合は、ルータ ID が高いルータが優先されます。ルータの優先順位が 0（ゼロ）に設定されているルータは、代表ルータまたはバックアップの代表ルータになる資格がありません。ルータの優先順位は、マルチアクセス ネットワーク（ポイントツーポイントではないネットワーク）へのインターフェイスにのみ設定されます。

例

次の例は、選択したインターフェイスで OSPF の優先順位を変更する方法を示しています。

```
hostname(config-if)# ospf priority 4
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf retransmit-interval

インターフェイスに属する隣接ルータの LSA 再送信間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf retransmit-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf retransmit-interval *seconds*

no ospf retransmit-interval [*seconds*]

シンタックスの説明

seconds	インターフェイスに属する隣接ルータの LSA 再送間隔を指定します。有効値は、1 ～ 65,535 秒です。

デフォルト

retransmit-interval *seconds* のデフォルト値は 5 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ルータは、LSA をネイバーに送信する場合に、確認応答メッセージを受信するまで LSA を保持します。確認応答を受信しない場合、ルータは LSA を再送信します。

このパラメータの設定を慎重に行う必要があります。そうしない場合、不要な再送信が生じます。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

例

次の例は、LSA の再送間隔を変更する方法を示しています。

```
hostname(config-if)# ospf retransmit-interval 15
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

ospf transmit-delay

インターフェイス上のリンクステート アップデート パケットを送信するのに必要な予想時間を設定するには、インターフェイス コンフィギュレーション モードで **ospf transmit-delay** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

ospf transmit-delay *seconds*

no ospf transmit-delay [*seconds*]

シンタックスの説明

seconds	インターフェイス上のリンクステート アップデート パケットを送信するのに必要な予想時間を設定します。デフォルト値は 1 秒で、範囲は 1 ～ 65,535 秒です。

デフォルト

seconds のデフォルト値は 1 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

アップデート パケットの LSA には、*seconds* 引数で指定された値ずつ加算された経過時間を格納してから送信する必要があります。値を割り当てるときは、インターフェイスの送信と伝搬遅延を考慮に入れる必要があります。

リンクを通じて送信される前に遅延が追加されていない場合、LSA がリンクを通じて伝播する時間が考慮されません。非常に低速のリンクでは、この設定は重要です。

例

次の例では、選択したインターフェイスの送信遅延を 3 秒に設定します。

```
hostname(config-if)# ospf restransmit-delay 3
hostname(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF 関連のインターフェイス情報を表示します。

outstanding

非認証の電子メール プロキシ セッションの数を制限するには、該当する電子メール プロキシ モードで **outstanding** コマンドを使用します。このアトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。これにより、非認証セッションは数が制限されずに許可されます。電子メール ポートに対する DoS 攻撃を制限するには、このコマンドを使用します。

電子メール プロキシ接続には、次の 3 つの状態があります。

1. 新しい電子メール接続は、「非認証」状態になります。
2. その接続でユーザ名が提示されると、「認証中」状態になります。
3. セキュリティ アプライアンスがその接続を認証すると、「認証済み」状態になります。

非認証状態の接続の数が、設定された限度を超えると、セキュリティ アプライアンスは、最も古い非認証接続を強制終了して、オーバーロードを防ぎます。認証済みの接続は、強制終了されません。

outstanding {*number*}

no outstanding

シンタックスの説明

number	許可される非認証セッション数。範囲は、1 ～ 1,000 です。

デフォルト

デフォルトは 20 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Pop3s	•	•	—	—	•
Imap4s	•	•	—	—	•
Smtps	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、POP3S 電子メール プロキシの非認証セッション数の限度を 12 に設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# outstanding 12
```

override-account-disable

AAA サーバからのアカウント ディセーブル表示を無効にするには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **override-account-disable** コマンドを使用します。表示の無効をディセーブルにするには、このコマンドの **no** 形式を使用します。

override-account-disable

no override-account-disable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

このコマンドは「account-disabled」という表示を返すサーバ、たとえば NT LDAP を使用する RADIUS や、Kerberos に対して有効です。

このアトリビュートは、IPSec RA トンネル グループおよび WebVPN トンネル グループに設定できます。

例

次の例では、WebVPN トンネル グループ「testgroup」に対して AAA サーバからの「account-disabled」表示を無効にするようにします。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

次の例では、IPSec リモート アクセス トンネル グループ「Agroup」に対して AAA サーバからの「account-disabled」表示を無効にするようにします。

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# override-account-disable
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	特定のトンネル グループのトンネル グループ データベースまたはコンフィギュレーションを消去します。
tunnel-group general-attributes	トンネル グループ一般アトリビュート値を設定します。

CHAPTER 22

packet-tracer コマンド～ pwd コマンド

packet-tracer

パケット トレース機能をイネーブルにして、パケットのスニッフィングやネットワーク障害切り離しを検出できるようにするには、**packet-tracer** コマンドを使用します。パケット キャプチャ機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

packet-tracer input [*src_int*] *protocol src_addr src_port dest_addr dest_port* [**detailed**] [**xml**]

no packet-tracer

シンタックスの説明

input *src_int*	パケット トレースの送信元インターフェイスを指定します。
protocol	パケット トレースのプロトコル タイプを指定します。利用できるプロトコル タイプのキーワードは、*icmp*、*rawip*、*tcp*、または *udp* です。
src_addr	パケット トレースの送信元アドレスを指定します。
src_port	パケット トレースの送信元ポートを指定します。
dest_addr	パケット トレースの宛先アドレスを指定します。
dest_port	パケット トレースの宛先ポートを指定します。
detailed	（オプション）詳細なパケット トレース情報を提供します。
xml	（オプション）XML 形式でトレース キャプチャを表示します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	—	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

パケットのキャプチャに加え、パケットが予想どおりに動作しているかどうか確認するために、セキュリティ アプライアンスを通してパケットの寿命をトレースすることができます。**packet-tracer** コマンドを使用すると、次の処理を実行できます。

- 実稼働ネットワークのすべてのパケット ドロップをデバッグする。
- 設定が目的どおりに動作しているかどうかを確認する。
- ルールの追加の原因となった CLI 行に沿ってパケットに適用されるすべてのルールを表示する。
- データ パスにパケット変更のタイム ラインを表示する。
- トレーサー パケットをデータ パスに挿入する。

packet-tracer コマンドはパケットと、パケットがセキュリティ アプライアンスによりどのように処理されたかを示す詳細情報を提供します。このコンフィギュレーションからのコマンドによりパケットがドロップしないインスタンスでは、**packet-tracer** コマンドはその原因に関する情報を簡単に読み取れる方法で提供します。たとえば、無効なヘッダー確認が原因でパケットがドロップした場合、「不正な IP ヘッダーによりパケットがドロップしました（原因）」というメッセージが表示されます。

例

内部ホスト 10.2.25.3 から詳細情報を持つ外部ホスト 209.165.202.158 に対するパケット トレースをイネーブルにするには、次のように入力します。

```
hostname# packet-tracer input inside tcp 10.2.25.3 www 209.165.202.158 aol detailed
```

関連コマンド

コマンド	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。

page style

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示される WebVPN ページをカスタマイズするには、webvpn カスタマイゼーション モードで **page style** コマンドを使用します。

page style *value*

[**no**] **page style** *value*

コマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

value	Cascading Style Sheet（CSS）パラメータ（最大 256 文字）。

デフォルト

デフォルトのページ スタイルは、background-color:white;font-family:Arial,Helv,sans-serif です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、ページ スタイルを large にカスタマイズします。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# page style font-size:large
```

関連コマンド

コマンド	説明
logo	WebVPN ページのロゴをカスタマイズします。
title	WebVPN ページのタイトルをカスタマイズします。

pager

Telnet セッションで「---more---」プロンプトが表示されるまでの 1 ページあたりのデフォルト行数を設定するには、グローバル コンフィギュレーション モードで **pager** コマンドを使用します。

pager [lines] *lines*

シンタックスの説明

[**lines**] *lines*	「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページが無制限であることを示します。範囲は 0 ～ 2,147,483,647 行です。**lines** キーワードはオプションです。このキーワードの有無にかかわらず、コマンドは同じです。

デフォルト

デフォルトは 24 行です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、特権 EXEC モード コマンドからグローバル コンフィギュレーション モード コマンドに変更されました。**terminal pager** コマンドが特権 EXEC モード コマンドとして追加されました。

使用上のガイドライン

このコマンドにより、Telnet セッションでのデフォルトの pager line 設定を変更します。現行セッションに対してのみ一時的に設定を変更する場合は、**terminal pager** コマンドを使用します。

管理コンテキストに Telnet 接続する場合、ある特定のコンテキスト内の **pager** コマンドに異なる設定があっても、他のコンテキストに移ったときには、pager line 設定はユーザのセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

例

次の例では、表示される行数を 20 に変更します。

```
hostname(config)# pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
show running-config terminal	現在の端末設定を表示します。
terminal	システム ログ メッセージが Telnet セッションで表示されるようにします。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードで端末の表示幅を設定します。

parameters

パラメータ コンフィギュレーション モードに入り、検査ポリシー マップのパラメータを設定するには、ポリシー マップ コンフィギュレーション モードで **parameters** コマンドを使用します。

parameters

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを利用すると、数多くのアプリケーション検査のための特別なアクションを設定できます。**inspect** コマンドを使用して、レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で検査エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成した検査ポリシー マップで定義するアクションをイネーブルにすることもできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は、検査ポリシー マップの名前です。

検査ポリシー マップは 1 つまたは複数の **parameters** コマンドをサポートできます。パラメータは検査エンジンの動作に影響します。パラメータ コンフィギュレーション モードで使用できるコマンドは、アプリケーションによって異なります。

例

次の例では、デフォルトの検査ポリシー マップ内に DNS パケットの最大メッセージ長を設定する方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# message-length maximum 512
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

participate

デバイスを仮想ロードバランシング クラスタに強制的に参加させるには、VPN ロードバランシング モードで **participate** コマンドを使用します。クラスタに参加した状態からデバイスを削除するには、このコマンドの **no** 形式を使用します。

participate

no participate

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルト動作では、デバイスは VPN ロードバランシング クラスタに参加しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

VPN ロードバランシング モードに入るには、**interface** コマンドおよび **nameif** コマンドを使用してインターフェイスを設定してから、**vpn load-balancing** コマンドを使用する必要があります。また、事前に **cluster ip** コマンドを使用してクラスタの IP アドレスを設定し、仮想クラスタの IP アドレスが参照するインターフェイスを設定する必要があります。

このコマンドは、このデバイスを仮想ロードバランシング クラスタに強制的に参加させます。デバイスの参加をイネーブルにするには、このコマンドを明示的に発行する必要があります。

1 つのクラスタに参加しているすべてのデバイスの IP アドレス、暗号化設定、暗号キー、およびポートの値は、クラスタ固有の同一の値である必要があります。

（注） 暗号化を使用する場合は、事前に **isakmp enable** *inside* コマンドを設定する必要があります。*inside* には、ロードバランシング内部インターフェイスを指定します。ロードバランシング内部インターフェイス上で isakmp がイネーブルになっていないと、クラスタ暗号化の設定を試みたときにエラー メッセージが表示されます。

cluster encryption コマンドを設定したときには isakmp がイネーブルであっても、**participate** コマンドを設定する前にディセーブルになった場合は、**participate** コマンドの入力時にエラー メッセージが表示され、そのローカル デバイスはクラスタに参加しません。

例

次に、VPN ロードバランシング コマンド シーケンスの例を示します。これには、現在のデバイスが VPN ロードバランシング クラスタに参加できるようにする **participate** コマンドが含まれています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
hostname(config-load-balancing)#
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

passive-interface

インターフェイスでの RIP ルーティング アップデートの伝送をディセーブルにするには、ルータ コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスでの RIP ルーティング アップデートをもう一度イネーブルにするには、このコマンドの **no** 形式を使用します。

passive-interface [***default*** | *if_name*]

no passive-interface {***default*** | *if_name*}

シンタックスの説明

default	（オプション）すべてのインターフェイスをパッシブ モードに設定します。
if_name	（オプション）RIP がパッシブ モードに設定されるインターフェイスです。

デフォルト

すべてのインターフェイスは RIP がイネーブルの場合にアクティブ RIP に対してイネーブルになります。

インターフェイスまたは **default** キーワードが指定されていない場合、コマンドは ***default*** がデフォルト設定となり、`passive-interface default` としてコンフィギュレーションに表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

パッシブ RIP をインターフェイスでイネーブルにします。インターフェイスは RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルに値を挿入しますが、ルーティング アップデートをブロードキャストしません。

例

次の例では、外部インターフェイスをパッシブ RIP に設定します。セキュリティ アプライアンスの他のインターフェイスは RIP アップデートを送受信します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# passive-interface outside
```

関連コマンド

コマンド	説明
clear configure rip	実行コンフィギュレーションからすべての RIP コマンドを消去します。
router rip	RIP ルーティング プロセスをイネーブルにし、RIP ルータ コンフィギュレーション モードに入ります。
show running-config rip	実行コンフィギュレーション内の RIP コマンドを表示します。

passwd

ログイン パスワードを設定するには、グローバル コンフィギュレーション モードで **passwd** コマンドを使用します。パスワードをデフォルトの「cisco」に戻すには、このコマンドの **no** 形式を使用します。Telnet または SSH を使用して、CLI にデフォルト ユーザとしてアクセスするときは、ログイン パスワードを入力するためのプロンプトが表示されます。ログイン パスワードを入力すると、ユーザ EXEC モードに入ります。

{**passwd** | **password**} *password* [***encrypted***]

no {**passwd** | **password**} *password*

シンタックスの説明

encrypted	（オプション）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由でパスワードを別のセキュリティ アプライアンスにコピーする必要があるのに元のパスワードがわからない場合、暗号化されたパスワードとこのキーワードを使用して **passwd** コマンドを入力します。通常、このキーワードは、**show running-config passwd** コマンドを入力したときにだけ表示されます。
passwd* | *password	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。
password	パスワードに、大文字と小文字が区別される最大 80 文字の文字列を設定します。パスワードにスペースを含めることはできません。

デフォルト

デフォルト パスワードは「cisco」です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このログイン パスワードはデフォルト ユーザ用です。**aaa authentication console** コマンドを使用して、Telnet または SSH のユーザごとに CLI 認証を設定した場合、このパスワードは使用されません。

例

次の例では、パスワードを Pa$$w0rd に設定します。

```
hostname(config)# passwd Pa$$w0rd
```

次の例では、別のセキュリティ アプライアンスからコピーした、暗号化されたパスワードをパスワードに設定します。

```
hostname(config)# passwd jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードを消去します。
enable	特権 EXEC モードに入ります。
enable password	イネーブル パスワードを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。
show running-config passwd	ログイン パスワードを暗号化された形で表示します。

password（暗号 CA トラストポイント）

登録中に CA に登録するチャレンジ フレーズを指定するには、暗号 CA トラストポイント コンフィギュレーション モードで **password** コマンドを使用します。CA は、通常、このフレーズを使用して、その後の失効要求を認証します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

password *string*

no password

シンタックスの説明

string	パスワードの名前を文字列として指定します。最初の文字を数字にすることはできません。文字列には、スペースを含む最大 80 文字の任意の英数字を使用できます。数字、スペース、任意の文字という形式のパスワードは指定できません。数字の後にスペースがあると、問題が発生します。たとえば、「hello 21」は適切なパスワードですが、「21 hello」は不適切です。パスワード チェックでは、大文字と小文字が区別されます。たとえば、「Secret」というパスワードと「secret」というパスワードは異なります。

デフォルト

デフォルトでは、パスワードを含めない設定になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、実際の証明書登録を開始する前に、証明書の失効パスワードを指定できます。指定したパスワードは、アップデートされたコンフィギュレーションがセキュリティ アプライアンスによって NVRAM に書き込まれるときに暗号化されます。

このコマンドがイネーブルになっていない場合、証明書登録中にパスワードの入力は求められません。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入り、CA に登録するチャレンジ フレーズをトラストポイント central の登録要求に含めています。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# password zzxxyy
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。

password-management

パスワード管理をイネーブルにするには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **password-management** コマンドを使用します。パスワード管理をディセーブルにするには、このコマンドの **no** 形式を使用します。日数をデフォルト値にリセットするには、***password-expire-in-days*** キーワードを指定してこのコマンドの **no** 形式を使用します。

password-management [***password-expire-in-days*** *days*]

no password-management

no password-management password-expire-in-days [*days*]

シンタックスの説明

days	現行のパスワードが期限切れになるまでの日数（0 ～ 180）を指定します。このパラメータは、***password-expire-in-days*** キーワードを指定する場合には必須です。
password-expire-in-days	（オプション）この直後のパラメータにより、現行のパスワードが期限切れになるまでの日数が指定され、セキュリティ アプライアンスが、ユーザにパスワードの期限が切れる時期が迫っていることを知らせる警告を開始します。このオプションは、LDAP サーバに対してのみ有効です。

デフォルト

このコマンドを指定しない場合、パスワード管理は行われません。***password-expire-in-days*** キーワードを指定しない場合、警告が開始されてから現行のパスワードが期限切れとなるまでのデフォルトの期間は 14 日間です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、IPSec リモート アクセスおよび WebVPN トンネル グループに設定できます。

このコマンドを設定すると、ログイン時にセキュリティ アプライアンスはリモート ユーザに、ユーザの現行のパスワードの期限が切れようとしている、またはパスワードが失効したということを通知します。ここでユーザは、セキュリティ アプライアンスにより、パスワードを変更する機会が与えられます。現行のパスワードがまだ失効していない場合、ユーザはそのパスワードを使用してログインできます。このコマンドは、このような通知をサポートする AAA サーバ（つまり、RADIUS サーバ、NT サーバを使用する RADIUS サーバ、および LDAP サーバ）に有効です。RADIUS または LDAP 認証が設定されていない場合、このコマンドはセキュリティ アプライアンスで無視されます。

このコマンドは、パスワードの期限が切れるまでの日数を変更するものではなく、セキュリティ アプライアンスがユーザにパスワードの期限が切れようとしているという警告を発した日から期限切れの日までの日数を変更するものであることに注意してください。

password-expire-in-days キーワードを指定する場合は、この日数も指定する必要があります。

この日数を 0 に設定してこのコマンドを指定すると、このコマンドはディセーブルになります。セキュリティ アプライアンスは、期限が迫っていることをユーザに通知しませんが、期限が切れた後で、ユーザはパスワードを変更できます。

例

次の例では、WebVPN トンネル グループ「testgroup」のパスワードの期限が切れる 90 日前になるとユーザに警告を開始するように設定します。

```
hostname(config)# tunnel-group testgroup type webvpn
hostname(config)# tunnel-group testgroup general-attributes
hostname(config-tunnel-general)# password-management password-expire-in-days 90
hostname(config-tunnel-general)#
```

次の例では、デフォルト値を使用して IPSec リモート アクセス トンネル グループ「QAgroup」のユーザにパスワードの期限が切れる 14 日前から警告を開始するようにします。

```
hostname(config)# tunnel-group QAgroup type ipsec-ra
hostname(config)# tunnel-group QAgroup general-attributes
hostname(config-tunnel-general)# password-management
hostname(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードを消去します。
passwd	ログイン パスワードを設定します。
radius-with-expiry	RADIUS 認証の間にパスワード アップデートのネゴシエーションをイネーブルにします（これは廃止されました）。
show running-config passwd	ログイン パスワードを暗号化された形で表示します。
tunnel-group general-attributes	トンネル グループ一般アトリビュート値を設定します。

password-parameter

SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求のパラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **password-parameter** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

password-parameter *string*

（注） HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

string	HTTP POST 要求に含まれるパスワード パラメータの名前です。パスワードの最大長は 128 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、認証 Web サーバに対してシングル サインオン認証要求を送信するために HTTP POST 要求を使用します。必要とされるコマンド **password-parameter** は、この POST 要求が SSO 認証用のユーザ パスワード パラメータを含める必要があることを指定します。

（注） ユーザはログイン時に、実際のパスワード値を入力します。このパスワードは POST 要求に入力されて認証 Web サーバに渡されます。

例

次の例では、AAA サーバ ホスト コンフィギュレーション モードで user_password という名前のパスワード パラメータを指定します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# password-parameter user_password
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名とパスワードを受信する Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバとの交換に使用する非表示パラメータを作成します。
start-url	事前ログイン クッキーの取得先 URL を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

password-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログインボックスのパスワード プロンプトをカスタマイズするには、webvpn カスタマイゼーション モードで **password-prompt** コマンドを使用します。

password-prompt {**text** | **style**} *value*

[**no**] **password-prompt** {**text** | **style**} *value*

コマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

パスワード プロンプトのデフォルトのテキストは「PASSWORD:」です。

パスワード プロンプトのデフォルトのスタイルは、color:black;font-weight:bold;text-align:right です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、テキストを「Corporate Password:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更しています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# password-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# password-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページのグループ プロンプトをカスタマイズします。
username-prompt	WebVPN ページのユーザ名プロンプトをカスタマイズします。

password-storage

クライアント システム上にログイン パスワードを保存することをユーザに許可するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **password-storage enable** コマンドを使用します。パスワードの保存をディセーブルにするには、**password-storage disable** コマンドを使用します。

password-storage アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。これにより、password-storage の値を別のグループ ポリシーから継承できるようになります。

password-storage {enable | disable}

no password-storage

シンタックスの説明

disable	パスワードの保存をディセーブルにします。
enable	パスワードの保存をイネーブルにします。

デフォルト

パスワードの保存はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュアなサイトにあることが判明しているシステムに限り、パスワードの保存をイネーブルにしてください。

このコマンドは、対話型ハードウェア クライアント認証またはハードウェア クライアントの個別ユーザ認証とは関係ありません。

例

次の例は、FirstGroup というグループ ポリシーのパスワードの保存をイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# password-storage enable
```

peer-id-validate

ピアの証明書を使用してピアのアイデンティティを確認するかどうかを指定するには、トンネル グループ ipsec アトリビュート モードで **peer-id-validate** コマンドを使用します。デフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

peer-id-validate *option*

no peer-id-validate

シンタックスの説明

option	次のオプションのいずれかを指定します。 • ***req***：必須 • ***cert***：証明書によってサポートされている場合 • ***nocheck***：確認しない

デフォルト

デフォルトでは、このコマンドの設定は ***req*** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ IPSec アトリビュート	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、すべての IPSec トンネル グループ タイプに適用できます。

例

config-ipsec コンフィギュレーション モードで入力された次の例は、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループのピアの証明書のアイデンティティを使用してのピアの確認を要求します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# peer-id-validate req
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

perfmon

パフォーマンス情報を表示するには、特権 EXEC モードで **perfmon** コマンドを使用します。

perfmon {**verbose** | **interval** *seconds* | **quiet** | **settings**} [***detail***]

シンタックスの説明

verbose	セキュリティ アプライアンス コンソールにパフォーマンス モニタ情報を表示します。
interval *seconds*	コンソールのパフォーマンス表示がリフレッシュされるまでの秒数を指定します。
quiet	パフォーマンス モニタの表示をディセーブルにします。
settings	interval を表示し、quiet と verbose のいずれであるかを表示します。
detail	パフォーマンスに関する詳細情報を表示します。

デフォルト

seconds は 120 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。
7.2(1)	***detail*** キーワードがサポートされるようになりました。

使用上のガイドライン

perfmon コマンドを使用すると、セキュリティ アプライアンスのパフォーマンスを監視できます。情報をすぐに表示するには、**show perfmon** コマンドを使用します。情報を 2 分間隔で表示し続けるには、**perfmon verbose** コマンドを使用します。指定した秒間隔で情報を表示し続けるには、**perfmon interval** *seconds* コマンドと **perfmon verbose** コマンドを併用します。

パフォーマンス情報は次のように表示されます。

PERFMON STATS:	Current	Average
Xlates	33/s	20/s
Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s
FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

この情報では、変換、接続、Websense 要求、アドレス変換（「フィックスアップ」と呼ばれる）、および AAA トランザクションについて、毎秒発生する数が表示されます。

例

次の例は、パフォーマンス モニタ統計情報を 30 秒間隔でセキュリティ アプライアンス コンソールに表示する方法を示しています。

```
hostname(config)# perfmon interval 120
hostname(config)# perfmon quiet
hostname(config)# perfmon settings
interval: 120 (seconds)
quiet
```

関連コマンド

コマンド	説明
show perfmon	パフォーマンス情報を表示します。

periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、時間範囲コンフィギュレーション モードで ***periodic*** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

no periodic *days-of-the-week time* **to** [*days-of-the-week*] *time*

シンタックスの説明

days-of-the-week	（オプション）最初の days-of-the-week 引数は、関連付けられている時間範囲が有効になる日または曜日です。2 番目の days-of-the-week 引数は、関連付けられている文の有効期間が終了する日または曜日です。 この引数は、任意の 1 つの曜日または曜日の組み合せです（monday（月曜日）、tuesday（火曜日）、wednesday（水曜日）、thursday（木曜日）、friday（金曜日）、saturday（土曜日）、および sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を完成させるには、***to*** キーワードを入力する必要があります。

デフォルト

periodic コマンドに値が入力されていない場合、***time-range*** コマンドによる定義に従ったセキュリティ アプライアンスへのアクセスがすぐに有効になり、常時オンとなります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
時間範囲コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間ベース ACL を実装するには、***time-range*** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。その後、**access-list extended time-range** コマンドを使用して、時間範囲を ACL にバインドします。

periodic コマンドは、時間範囲をいつ有効にするかを指定する方法の 1 つです。別の方法は、***absolute*** コマンドを使用して絶対時間範囲を指定する方法です。これらのコマンドのいずれかを、***time-range*** グローバル コンフィギュレーション コマンドの後に使用します。このコマンドは、時間範囲の名前を指定します。***time-range*** コマンドあたり複数の ***periodic*** 値を入力できます。

終了の days-of-the-week 値が開始の days-of-the-week 値と同じである場合は、終了の days-of-the-week 値を省略できます。

time-range コマンドに ***absolute*** 値と ***periodic*** 値の両方が指定されている場合、***periodic*** コマンドは ***absolute start*** 時刻に達した後にだけ評価され、***absolute end*** 時刻に達した後はそれ以上評価されません。

time-range 機能はセキュリティ アプライアンスのシステム クロックに依存しています。しかし、この機能は、NTP 同期化により最適に動作します。

例

次にいくつかの例を示します。

必要な設定	入力内容
月曜日から金曜日の午前 8 時～午後 6 時のみ	***periodic weekdays 8:00:00 to 18:00***
毎日午前 8 時～午後 6 時のみ	***periodic daily 8:00 to 18:00***
月曜日午前 8 時～金曜日午後 8 時の 1 分おき	***periodic monday 8:00 to friday 20:00***
週末、つまり土曜日の朝から日曜日の終わりまで	***periodic weekend 00:00:00 to 23:59***
土曜日および日曜日の正午～深夜	***periodic weekend 12:00:00 to 23:59***

次の例は、月曜日から金曜日の午前 8 時～午後 6 時にセキュリティ アプライアンスにアクセスすることを許可する方法を示しています。

```
hostname(config-time-range)# periodic weekdays 8:00 to 18:00
hostname(config-time-range)#
```

次の例は、特定の曜日（月曜日、火曜日、および金曜日）の午前 10 時 30 分～午後 12 時 30 分にセキュリティ アプライアンスにアクセスすることを許可する方法を示しています。

```
hostname(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
hostname(config-time-range)#
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効である絶対時間を定義します。
access-list extended	セキュリティ アプライアンスを通して IP トラフィックの許可または拒否に対するポリシーを設定します。
default	***time-range*** コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードのデフォルト設定を復元します。
time-range	時間に基づいてセキュリティ アプライアンスのアクセス コントロールを定義します。

permit errors

無効な GTP パケットを許可する、または許可しないと解析が失敗してドロップされるパケットを許可するには、GTP マップ コンフィギュレーション モードで **permit errors** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスできます。コマンドを削除するには、このコマンドの **no** 形式を使用します。

permit errors

no permit errors

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、無効なパケットまたは解析中に失敗したパケットは、すべてドロップされます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

無効なパケット、またはセキュリティ アプライアンスを通じて送信されるメッセージの検査中にエラーが発生したパケットを許可し、それらがドロップされないようにするには、GTP マップ コンフィギュレーション モードで **permit errors** コマンドを使用します。

例

次の例では、無効なパケットまたは解析中に失敗したパケットが含まれたトラフィックを許可します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit errors
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。
permit response	ロードバランシング GSN をサポートします。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

permit response

ロードバランシング GSN をサポートするには、GTP マップ コンフィギュレーション モードで **permit response** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスできます。permit response コマンドは、応答の送信先であった GSN とは異なる GSN からの GTP 応答を許可することにより、ロードバランシング GSN をサポートします。コマンドを削除するには、このコマンドの **no** 形式を使用します。

permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

no permit response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

シンタックスの説明

from-object-group *from_obj_group_id*	**object-group** コマンドにより設定された、*to_obj_group_id* 引数で指定したオブジェクト グループ内の GSN の集合に対して応答を送信できるオブジェクト グループの名前を指定します。セキュリティ アプライアンスがサポートしているのは、IPv4 アドレスを持つネットワーク オブジェクトを含んだオブジェクト グループのみです。IPv6 アドレスは、現時点では GTP でサポートされていません。
to-object-group *to_obj_group_id*	**object-group** コマンドにより設定された、*from_obj_group_id* 引数で指定したオブジェクト グループ内の GSN の集合から応答を受信できるオブジェクト グループの名前を指定します。セキュリティ アプライアンスがサポートしているのは、IPv4 アドレスを持つネットワーク オブジェクトを含んだオブジェクト グループのみです。IPv6 アドレスは、現時点では GTP でサポートされていません。

デフォルト

デフォルトでは、セキュリティ アプライアンスは、要求送信先のホスト以外の GSN からの GTP 応答をドロップします。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(4)	このコマンドが導入されました。

使用上のガイドライン

ロードバランシング GSN をサポートするには、GTP マップ コンフィギュレーション モードで **permit response** コマンドを使用します。**permit response** コマンドを使用して、応答の送信先であった GSN とは異なる GSN からの、GTP 応答を許可するように GTP マップを設定します。

ロードバランシング GSN のプールをネットワーク オブジェクトとして指定します。同様に、SGSN をネットワーク オブジェクトとして指定します。応答する GSN が、GTP 要求の送信先であった GSN と同じオブジェクト グループに属する場合、また応答する GSN が GTP 応答を送信できるオブジェクト グループに SGSN がある場合、セキュリティ アプライアンスはその応答を許可します。

例

次の例では、192.168.32.0 ネットワーク上の任意のホストから IP アドレス 192.168.112.57 を持つホストへの GTP 応答を許可します。

```
hostname(config)# object-group network gsnpool32
hostname(config-network)# network-object 192.168.32.0 255.255.255.0
hostname(config)# object-group network sgsn1
hostname(config-network)# network-object host 192.168.112.57
hostname(config-network)# exit
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# permit response to-object-group sgsn1 from-object-group
gsnpool32
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。
permit errors	無効な GTP パケットを許可します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

pfs

PFS をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **pfs enable** コマンドを使用します。PFS をディセーブルにするには、**pfs disable** コマンドを使用します。PFS アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、PFS の値を別のグループ ポリシーから継承できます。

IPSec ネゴシエーションで、PFS は新しい暗号鍵が以前のどの鍵とも無関係であることを保証します。

pfs {enable | disable}

no pfs

シンタックスの説明

disable	PFS をディセーブルにします。
enable	PFS をイネーブルにします。

デフォルト

PFS はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PFS 設定は、VPN クライアントとセキュリティ アプライアンスで一致している必要があります。

例

次の例は、FirstGroup というグループ ポリシーの PFS を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# pfs enable
```

pim

インターフェイス上の PIM を再度イネーブルにするには、インターフェイス コンフィギュレーション モードで **pim** コマンドを使用します。PIM をディセーブルにするには、このコマンドの **no** 形式を使用します。

pim

no pim

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

multicast-routing コマンドは、デフォルトではすべてのインターフェイスの PIM をイネーブルにします。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

multicast-routing コマンドは、デフォルトではすべてのインターフェイスの PIM をイネーブルにします。**no** 形式の **pim** コマンドだけがコンフィギュレーションに保存されます。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

例

次の例では、選択したインターフェイス上の PIM をディセーブルにします。

```
hostname(config-if)# no pim
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim accept-register

PIM 登録メッセージをフィルタリングするようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **pim accept-register** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式を使用します。

pim accept-register {***list*** *acl* | ***route-map*** *map-name*}

no pim accept-register

シンタックスの説明

list *acl*	アクセス リストの名前または番号を指定します。このコマンドでは、標準ホスト ACL だけを使用してください。拡張 ACL はサポートされていません。
route-map *map-name*	ルートマップ名を指定します。参照先のルートマップでは、標準ホスト ACL を使用してください。拡張 ACL はサポートされていません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

非認証の送信元が RP に登録されないようにするには、このコマンドを使用します。非認証の送信元が RP に登録メッセージを送信すると、セキュリティ アプライアンスはただちに登録中止メッセージを送信します。

例

次の例では、PIM 登録メッセージを、「no-ssm-range」というアクセス リストに定義されている送信元からのものに制限します。

```
hostname(config)# pim accept-register list no-ssm-range
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim bidir-neighbor-filter

どの双方向対応ネイバーが DF 選定に参加できるかを制御するには、インターフェイス コンフィギュレーション モードで **pim bidir-neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式を使用します。

pim bidir-neighbor-filter *acl*

no pim bidir-neighbor-filter ***acl***

シンタックスの説明

acl	アクセス リストの名前または番号を指定します。アクセス リストでは、双方向 DF 選定に参加できるネイバーを定義します。このコマンドでは、標準 ACL だけを使用してください。拡張 ACL はサポートされていません。

デフォルト

すべてのルータは双方向対応であると判断されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

双方向 PIM を使用すると、マルチキャスト ルータでは、情報を縮小して保持できます。セグメント内のすべてのマルチキャスト ルータは、bidir で DF を選定できるよう双方向にイネーブルになっていなければなりません。

pim bidir-neighbor-filter コマンドを使用すると、希薄モード専用ネットワークから双方向ネットワークへの移行が可能になります。この場合、すべてのルータの希薄モード ドメインへの参加を許可しながら、DF 選定へ参加しなければならないルータを指定します。双方向対応のルータは、セグメントに双方向非対応のルータがある場合でも、ルータの中から DF を選定できます。双方向非対応のルータのマルチキャスト境界は、双方向対応のグループからの PIM メッセージとデータが、双方向対応のサブセット クラウド内外に漏れることを防ぎます。

pim bidir-neighbor-filter コマンドがイネーブルになっていると、ACL により許可されているルータは双方向対応であると考えられます。したがって、次のような結果になります。

- 許可されたネイバーが双方向に対応しない場合、DF 選定は発生しません。
- 拒否されたネイバーが双方向に対応する場合、DF 選定は発生しません。
- 拒否されたネイバーが双方向に対応しない場合、DF 選定が発生します。

例

次の例では、10.1.1.1 が PIM 双方向対応ネイバーになります。

```
hostname(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
hostname(config)# access-list bidir_test deny any
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pim bidir-neighbor-filter bidir_test
```

関連コマンド

コマンド	説明
multicast boundary	管理用のマルチキャスト アドレスのマルチキャスト境界を定義します。
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim dr-priority

指定ルータの選定に使用されるネイバーの優先順位をセキュリティ アプライアンス上に設定するには、インターフェイス コンフィギュレーション モードで **pim dr-priority** コマンドを使用します。デフォルトの優先順位に戻すには、このコマンドの **no** 形式を使用します。

pim dr-priority *number*

no pim dr-priority

シンタックスの説明

number	0 ～ 4294967294 の任意の数字。この数字は、指定ルータを判別するときに、デバイスの優先順位を判別するために使用されます。0 に指定すると、セキュリティ アプライアンスは指定ルータに選定されません。

デフォルト

デフォルト値は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス上の優先順位値が最も大きいデバイスが、PIM 指定ルータになります。複数のデバイスで同じ指定ルータ優先順位値が設定されている場合、IP アドレスが最大のデバイスが指定ルータになります。デバイスの hello メッセージに DR-Priority Option（指定ルータ優先順位オプション）が含まれていない場合は、そのデバイスが最も優先順位の高いデバイスであると見なされ、指定ルータになります。hello メッセージにこのオプションが含まれていないデバイスが複数ある場合は、最大の IP アドレスを持つデバイスが指定ルータになります。

例

次の例は、インターフェイスの指定ルータ優先順位を 5 に設定します。

```
hostname(config-if)# pim dr-priority 5
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim hello-interval

PIM hello メッセージの頻度を設定するには、インターフェイス コンフィギュレーション モードで **pim hello-interval** コマンドを使用します。hello 間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim hello-interval *seconds*

no pim hello-interval [*seconds*]

シンタックスの説明

seconds	セキュリティ アプライアンスが hello メッセージを送信する前に待機する秒数。有効となる値の範囲は、1 ～ 3600 秒です。デフォルト値は 30 秒です。

デフォルト

30 秒。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、PIM hello 間隔を 1 分に設定します。

```
hostname(config-if)# pim hello-interval 60
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim join-prune-interval

PIM join/prune 間隔を設定するには、インターフェイス コンフィギュレーション モードで **pim join-prune-interval** コマンドを使用します。この間隔をデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim join-prune-interval *seconds*

no pim join-prune-interval [*seconds*]

シンタックスの説明

seconds	セキュリティ アプライアンスが join/prune メッセージを送信する前に待機する秒数。有効となる値の範囲は、10 ～ 600 秒です。デフォルトは、60 秒です。

デフォルト

60 秒

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、PIM join/prune 間隔を 2 分に設定します。

```
hostname(config-if)# pim join-prune-interval 120
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim neighbor-filter

どのネイバ ルータが PIM 選定に参加できるかを制御するには、インターフェイス コンフィギュレーション モードで **pim neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式を使用します。

pim neighbor-filter *acl*

no pim neighbor-filter ***acl***

シンタックスの説明

acl	アクセス リストの名前または番号を指定します。このコマンドでは、標準 ACL だけを使用してください。拡張 ACL はサポートされていません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、どのネイバー ルータが PIM に参加できるかを定義します。このコマンドがコンフィギュレーションに含まれていない場合、制限はありません。

このコマンドをコンフィギュレーション内に表示するには、マルチキャスト ルーティングと PIM がイネーブルでなければなりません。マルチキャスト ルーティングをディセーブルにすると、このコマンドはコンフィギュレーションから削除されます。

例

次の例では、IP アドレス 10.1.1.1 のルータが、GigabitEthernet0/2 インターフェイスで PIM ネイバーになるのを禁止します。

```
hostname(config)# access-list pim_filter deny 10.1.1.1 255.255.255.255
hostname(config)# interface gigabitEthernet0/2
hostname(config-if)# pim neighbor-filter pim_filter
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim old-register-checksum

古い登録チェックサム方法論を使用する Rendezvous Point（RP; ランデブー ポイント）上の下位互換性を許可するには、グローバル コンフィギュレーション モードで **pim old-register-checksum** コマンドを使用します。PIM RFC 準拠の登録を生成するには、このコマンドの **no** 形式を使用します。

pim old-register-checksum

no pim old-register-checksum

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

セキュリティ アプライアンスは、PIM RFC 準拠の登録を生成します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス ソフトウェアは、Cisco IOS 方式を使用せずに、PIM ヘッダー上のチェックサムを持つ登録メッセージと、それに続く 4 バイトだけを受け入れます。つまり、登録メッセージをすべての PIM メッセージ タイプ用の PIM メッセージ全体と共に受け入れます。**pim old-register-checksum** コマンドは、Cisco IOS ソフトウェアと互換性のある登録を生成します。

例

次の例では、古いチェックサム計算を使用するようにセキュリティ アプライアンスを設定します。

```
hostname(config)# pim old-register-checksum
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

pim rp-address

PIM Rendezvous Point（RP; ランデブー ポイント）のアドレスを設定するには、グローバル コンフィギュレーション モードで **pim rp-address** コマンドを使用します。RP アドレスを削除するには、このコマンドの **no** 形式を使用します。

pim rp-address *ip_address* [*acl*] [***bidir***]

no pim rp-address *ip_address*

シンタックスの説明

acl	（オプション）RP と共に使用するマルチキャスト グループを定義する、標準的なアクセス リストの名前または番号。このコマンドでホスト ACL を使用しないでください。
bidir	（オプション）指定したマルチキャスト グループが、双方向モードで動作することを示します。このオプションを使用しないでコマンドを設定した場合、指定したグループは PIM 希薄モードで動作します。
ip_address	PIM RP として使用するルータの IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。

このコマンドには、引数もキーワードもありません。

デフォルト

PIM RP アドレスは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

共通の PIM 希薄モード（PIM-SM）または双方向ドメイン内にあるすべてのルータは、周知の PIM RP アドレスの情報を必要とします。アドレスは、このコマンドを使用してスタティックに設定します。

（注） セキュリティ アプライアンスは、Auto-RP をサポートしていません。したがって、**pim rp-address** コマンドを使用して、RP アドレスを指定する必要があります。

1 つの RP で複数のグループが処理されるように設定できます。アクセス リストで指定されているグループ範囲により、PIM RP グループ マッピングが決まります。アクセス リストが指定されていない場合、グループの RP は、IP マルチキャスト グループ範囲全体（224.0.0.0/4）に適用されます。

（注） セキュリティ　アプライアンスは、実際の双方向コンフィギュレーションにかかわらず、常に、双方向機能を PIM hello メッセージ内でアドバタイズします。

例

次の例では、すべてのマルチキャスト グループの PIM RP アドレスに 10.0.0.1 を設定します。

```
hostname(config)# pim rp-address 10.0.0.1
```

関連コマンド

コマンド	説明
pim accept-register	PIM 登録メッセージをフィルタリングするように、候補 RP を設定します。

pim spt-threshold infinity

最後のホップ ルータの動作を、常に共有ツリーを使用し、Shortest-Path Tree（SPT; 最短パス ツリー）への切り替えを決して実行しないように変更するには、グローバル コンフィギュレーション モードで **pim spt-threshold infinity** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

pim spt-threshold infinity [***group-list*** *acl*]

no pim spt-threshold

シンタックスの説明

group-list *acl*	（オプション）アクセス リストで制限されている送信元グループを指定します。*acl* 引数には、標準 ACL を指定する必要があります。拡張 ACL はサポートされていません。

デフォルト

デフォルトでは、最後のホップ PIM ルータは最短パス送信元ツリーに切り替えます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

group-list キーワードを使用しない場合、このコマンドはすべてのマルチキャスト グループに適用されます。

例

次の例では、最短パス送信元ツリーに切り替えるのではなく、常に共有ツリーを使用するように最後のホップ PIM ルータを設定します。

```
hostname(config)# pim spt-threshold infinity
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

ping

セキュリティ アプライアンスから他の IP アドレスが可視であるかどうかを判断するには、特権 EXEC モードで **ping** コマンドを使用します。

ping [*if_name*] *host* [**data** *pattern*] [**repeat** *count*] [**size** *bytes*] [**timeout** *seconds*] [**validate**]

シンタックスの説明

***data** pattern*	（オプション）16 ビット データ パターンを 16 進数で指定します。
host	ping 対象のホストの IPv4 または IPv6 アドレス、または名前を指定します。この名前は DNS 名、または **name** コマンドで割り当てられた名前になります。DNA 名の最大文字数は 128 文字、**name** コマンドで作成した名前の最大文字数は 63 文字です。
if_name	（オプション）***nameif*** コマンドで設定され、*host* へのアクセスに使用できるインターフェイス名を指定します。指定しない場合、*host* は解決されて IP アドレスに変換され、その後で、宛先インターフェイスを確認するために、ルーティング テーブルが参照されます。
***repeat** count*	（オプション）ping 要求を繰り返す回数を指定します。
***size** bytes*	（オプション）データグラム サイズをバイト単位で指定します。
timeout *seconds*	（オプション）ping 要求がタイムアウトになるまでの秒数を指定します。
validate	（オプション）応答データを検証することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	DNS 名がサポートされるようになりました。

使用上のガイドライン

ping コマンドでは、セキュリティ アプライアンスに接続できるかどうか、またはホストがネットワークで利用可能であるかどうかが判断できます。セキュリティ アプライアンスに接続できる場合は、**icmp permit any** *interface* コマンドが設定されていることを確認します。このコンフィギュレーションは、***ping*** コマンドで生成されたメッセージの応答および受け入れをセキュリティ アプライアンスに許可するために必要です。***ping*** コマンドの出力には、応答が受信されたかどうかが示されます。**ping** コマンドを入力したとき、ホストが応答していない場合は、次のようなメッセージが表示されます。

```
hostname(config)# ping 10.1.1.1
Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

セキュリティ アプライアンスがネットワークに接続されていること、およびトラフィックの受け渡しを実行していることを確認するには、***show interface*** コマンドを使用します。指定した *if_name* のアドレスは ping の送信元アドレスとして使用されます。

内部ホストから外部ホストに ping を送信する場合は、次のいずれかを実行する必要があります。

- エコー応答用の ICMP ***access-list*** コマンドを作成します。たとえば、ping アクセスをすべてのホストに許可するには、***access-list acl_grp permit icmp any any*** コマンドを使用します。***access-group*** コマンドを使用して、テストの対象であるインターフェイスに ***access-list*** コマンドをバインドします。
- **inspect icmp** コマンドを使用して、ICMP 検査エンジンを設定します。たとえば、**inspect icmp** コマンドをグローバル サービス ポリシーの **class default_inspection** クラスに追加すると、内部ホストによって開始されたエコー要求に対して、セキュリティ アプライアンスを経由したエコー応答が許可されます。

拡張 ping を実行することもできます。拡張 ping では、キーワードを一度に 1 行ずつ入力できます。

ホスト間またはルータ間でセキュリティ アプライアンスを介して ping を実行するが、ping が成功しない場合は、**capture** コマンドを使用して ping の成功を監視できます。

セキュリティ アプライアンス **ping** コマンドでは、インターフェイス名は必須ではありません。インターフェイス名が指定されていない場合、セキュリティ アプライアンスは、ルーティング テーブルをチェックして指定されたアドレスを検索します。インターフェイス名を指定して、ICMP エコー要求が送信されるときに経由するインターフェイスを指示できます。

例

次の例は、他の IP アドレスがセキュリティ アプライアンスから可視であるかどうかを判断する方法を示しています。

```
hostname# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次の例は、DNS 名を使用するホストを指定します。

```
hostname# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、拡張 ping の例を示します。

```
hostname# ping
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

関連コマンド

コマンド	説明
capture	インターフェイスでパケットをキャプチャします。
icmp	インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
show interface	VLAN コンフィギュレーションについての情報を表示します。

police

厳密なスケジューリング優先順位をこのクラスに適用するには、クラス モードで **police** コマンドを使用します。レート制限要件を削除するには、このコマンドの **no** 形式を使用します。

police {**output** | **input**} *conform-rate* [*burst-size* **conform-action** {**drop** | **transmit**} **exceed-action** **{drop | transmit}**]

no police

シンタックスの説明

burst-size	1,000 ～ 512,000,000 の範囲の値。適合レート値にスロットリングするまでに持続的なバーストで許容される最大瞬間バイト数を指定します。
conform-action	レートが *burst-size* の値より小さいときに実行されるアクション（パケットのドロップまたは伝送）。
conform-rate	このトラフィック フローのレート限度。8,000 ～ 2,000,000,000 の任意の値で、許容される最大速度（ビット / 秒）を指定します。
drop	パケットをドロップします。
exceed-action	このアクションは、レートが conform-rate 値と conform-burst 値の間であるときに実行されます。
input	入力方向に流れるトラフィックのポリシングをイネーブルにします。
output	出力方向に流れるトラフィックのポリシングをイネーブルにします。
transmit	パケットを伝送します。

デフォルト

デフォルトの動作や変数はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	***input*** オプションが追加されました。着信方向のトラフィックのポリシングがサポートされます。コマンドの指定において、*conform rate* に続くコマンド内のすべてがオプションであることを示すシンタックスの表記方法が変更されました。

使用上のガイドライン

police コマンドを発行する前に、**policy-map** コマンドと **class** コマンドを設定しておく必要があります。

（注） **police** コマンドは、最大速度および最大バースト レートを強制し、それらの値を適合レート値に強制的に合せるだけです。***conform-action*** または ***exceed-action*** の指定は、存在する場合でも適用されません。

優先順位とポリシングを、両方ともイネーブルにすることはできません。

既存の VPN クライアント トラフィック、LAN-to-LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去（ドロップ）して再確立する必要があります。

例

次に、出力方向の **police** コマンドの例を示します。適合レート 100,000 ビット / 秒、バースト値 2,000,000 バイトを設定し、バースト レートを超過したトラフィックをドロップすることを指定しています。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class-map firstclass
hostname(config-cmap)# class localclass
hostname(config-pmap-c)# police output 100000 20000 exceed-action drop
hostname(config-cmap-c)# class class-default
hostname(config-pmap-c)#
```

次の例では、内部 Web サーバ宛のトラフィックに対してレート制限を設定する方法を示します。

```
hostname# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
hostname# class-map http_traffic
hostname(config-cmap)# match access-list http_traffic
hostname(config-cmap)# policy-map outside_policy
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# police input 56000
hostname(config-pmap-c)# service-policy outside_policy interface outside
hostname(config)#
```

関連コマンド

class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

policy

CRL を取得するための送信元を指定するには、ca-crl コンフィギュレーション モードで **policy** コマンドを使用します。

policy {***static*** | ***cdp*** | ***both***}

シンタックスの説明

both	CRL 配布ポイントを使用して CRL を取得することに失敗した場合は最大 5 つのスタティック CRL 配布ポイントを使用してリトライすることを、指定します。
cdp	チェック中の証明書に組み込まれた、CRL 配布ポイント拡張を使用します。この場合、セキュリティ アプライアンスは、チェック中の証明書の CRL 配布ポイント拡張から最大 5 つの CRL 配布ポイントを取得し、必要に応じて、設定されたデフォルト値で情報を増強します。セキュリティ アプライアンスは、プライマリ CRL 配布ポイントを使用して CRL を取得することに失敗した場合、リストにある次に利用可能な CRL 配布ポイントを使用してリトライします。これは、セキュリティ アプライアンスが CRL を取得するか、リストを使い果たすまで続行されます。
static	最大 5 つのスタティック CRL 配布ポイントを使用します。このオプションを指定する場合は、**protocol** コマンドで LDAP または HTTP URL も指定してください。

デフォルト

デフォルト設定は **cdp** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、チェック中の証明書内の CRL 配布ポイントを使用して CRL 取得を実行すること、それに失敗した場合は、スタティック CRL 配布ポイントを使用することを設定します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# policy both
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
url	CRL を取得するためのスタティック URL のリストを作成および維持します。

policy-map

モジュラ ポリシー フレームワークを使用する場合、グローバル コンフィギュレーション モードで **policy-map** コマンド（**type** キーワードなし）を使用し、レイヤ 3/4 クラス マップ（**class-map** コマンドまたは **class-map type management** コマンド）で特定したトラフィックにアクションを割り当てます。レイヤ 3/4 ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

policy-map *name*

no policy-map *name*

シンタックスの説明

name	このポリシー マップの名前を最大 40 文字で指定します。すべてのタイプのポリシー マップが同じネーム スペースを使用しているため、他のタイプのポリシー マップですでに使用されている名前は再使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。
2. （アプリケーション検査のみ）**policy-map type inspect** コマンドを使用して、アプリケーション検査トラフィックのための特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスに対するアクションを有効にします。

ポリシー マップの最大数は 64 です。レイヤ 3/4 ポリシー マップ内の複数のレイヤ 3/4 クラス マップを指定でき（**class** コマンドを参照）、各クラス マップに 1 つまたは複数の機能タイプから複数のアクションを割り当てることができます。

パケットは、各機能タイプのポリシー マップ内にある 1 つのクラス マップだけに一致します。パケットがある機能タイプのクラス マップと一致すると、セキュリティ アプライアンスはそのクラス マップを、その機能タイプの後続のクラス マップと照合しません。パケットが別の機能タイプの後続のクラス マップと一致すると、セキュリティ アプライアンスはそのクラス マップのアクションも適用します。たとえば、パケットが接続制限のクラス マップと一致し、アプリケーション検査のクラス マップにも一致する場合、両方のクラス マップのアクションが適用されます。パケットがアプリケーション検査のクラス マップと一致するが、アプリケーション検査の別のクラス マップとも一致する場合、2 番目のクラス マップのアクションは適用されません。

アクションは、機能に応じて双方向または単方向のトラフィックに適用されます。双方向に適用される機能については、トラフィックが双方向のクラス マップに一致する場合、ポリシー マップの適用先であるインターフェイスに入る、または出るすべてのトラフィックに影響します。

(注)　グローバル ポリシーを使用する場合、すべての機能は単方向です。1 つのインターフェイスに適用されるときに通常は双方向である機能は、グローバルに適用される際には各インターフェイスの入力にのみ適用されます。ポリシーはすべてのインターフェイスに適用されるため、ポリシーは双方向に適用されます。この場合の双方向性は冗長になります。

QoS など単方向に適用される機能の場合、ポリシーが適用されるインターフェイスを出るトラフィックのみ影響を受けます。各機能の方向性については、表 22-1 を参照してください。

表 22-1　機能の方向性

機能	一方向のインターフェイス	グローバルな方向
TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化	双方向	入力
CSC	双方向	入力
アプリケーション検査	双方向	入力
IPS	双方向	入力
QoS ポリシング	出力	出力
QoS プライオリティ キュー	出力	出力

ポリシー マップ内の各種アクションが実行される順序は、そのポリシー マップ内にアクションが出現する順序とは関係ありません。アクションは次の順序で実行されます。

- TCP 正規化、TCP 接続と UDP 接続の制限およびタイムアウト、TCP シーケンス番号のランダム化

(注)　セキュリティ アプライアンスがプロキシ サービス（AAA または CSC など）を実行する場合、または TCP ペイロード（FTP 検査など）を修正する場合、TCP ノーマライザはデュアル モードで動作します。このモードでは、ノーマライザはプロキシまたはペイロードの修正サービスの前後に適用されます。

- CSC
- アプリケーション検査
- IPS
- QoS ポリシング
- QoS プライオリティ キュー

各インターフェイスに割り当てられるポリシー マップは 1 つだけですが、複数のインターフェイスに同じポリシー マップを割り当てることができます。

コンフィギュレーションには、セキュリティ アプライアンスがデフォルトのグローバル ポリシーで使用するデフォルトのレイヤ 3/4 ポリシー マップが含まれています。このマップは **global_policy** と呼ばれ、デフォルトの検査トラフィックで検査を実行します。適用できるグローバル ポリシーは 1 つのみです。このため、グローバル ポリシーの内容を変更する場合は、デフォルトのポリシーを編集するか、ディセーブルにして新しいものを適用する必要があります。

デフォルトのポリシー マップ コンフィギュレーションには、次のコマンドが含まれています。

```
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
```

例

次に、接続ポリシーに対する **policy-map** コマンドの例を示します。ここでは、Web サーバ 10.1.1.1 にアクセスできる接続の数を制限しています。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次の例では、ポリシー マップで複数一致がどのように機能するかを示しています。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80

hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例では、使用可能な最初のクラス マップにトラフィックが一致し、同じ機能ドメインのアクションを指定している以降のどのクラス マップにも一致しない様子を示しています。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続が開始されると、**class telnet_traffic** と照合されます。同様に、FTP 接続が開始されると、**class ftp_traffic** と照合されます。Telnet と FTP 以外の TCP 接続の場合は、**class tcp_traffic** と照合されます。Telnet または FTP 接続が **class tcp_traffic** と一致する可能性があったとしても、すでに他のクラスと一致しているので、セキュリティ アプライアンスはこの照合を行いません。

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ポリシー マップが **service-policy** コマンドで使用中の場合、このポリシー マップは削除されません。
class-map	トラフィック クラス マップを定義します。
service-policy	ポリシー マップを 1 つのインターフェイスに割り当てるか、すべてのインターフェイスにグローバルに割り当てます。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

policy-map type inspect

モジュラ ポリシー フレームワークを使用する場合、グローバル コンフィギュレーション モードで **policy-map type inspect** コマンドを使用して検査アプリケーション トラフィックの特殊アクションを定義します。検査ポリシー マップの指定を削除するには、このコマンドの **no** 形式を使用します。

policy-map type inspect *application policy_map_name*

no policy-map [**type inspect** *application*] *policy_map_name*

シンタックスの説明

application	対象とするアプリケーション トラフィックのタイプを指定します。指定できるタイプは、次のとおりです。 • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **radius-accounting** • **sip** • **skinny** • **snmp**
policy_map_name	このポリシー マップの名前を最大 40 文字で指定します。「_internal」または「_default」で始まる名前は予約されるので、使用できません。すべてのタイプのポリシー マップが同じネーム スペースを使用しているため、他のタイプのポリシー マップですでに使用されている名前は再使用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを利用すると、数多くのアプリケーション検査のための特別なアクションを設定できます。**inspect** コマンドを使用して、レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で検査エンジンをイネーブルにする場合は、**policy-map type inspect** コマンドで作成した検査ポリシー マップで定義するアクションをイネーブルにすることもできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、検査ポリシー マップの名前です。

検査ポリシー マップは、ポリシー マップ コンフィギュレーション モードに入力された次のコマンドのうち 1 つまたは複数のコマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。

- **match** コマンド：**match** コマンドを直接検査ポリシー マップに定義できます。そうすることで、アプリケーション トラフィックを、URL 文字列などのこのアプリケーションに特有の基準と照合します。次に、一致コンフィギュレーション モードで **drop**、**reset**、**log** などのアクションをイネーブルにします。使用可能な **match** コマンドは、アプリケーションにより異なります。
- **class** コマンド：このコマンドは、ポリシー マップで検査クラス マップを特定します（検査クラス マップを作成する **class-map type inspect** コマンドを参照）。検査クラス マップには、URL 文字列などの、アプリケーション特有の基準によってアプリケーションのトラフィックを照合する複数の **match** コマンドが含まれます。それに応じて、ポリシー マップでアクションをイネーブルにします。クラス マップを作成することと、検査ポリシー マップに直接 **match** コマンドを使用することの違いは、複数の照合結果をグループ化できることと、クラス マップを再利用できることです。
- **parameters** コマンド：パラメータは、検査エンジンの動作に影響を与えます。パラメータ コンフィギュレーション モードで使用できるコマンドは、アプリケーションによって異なります。

ポリシー マップには複数の **class** コマンドまたは **match** コマンドを指定できます。

一部の **match** コマンドでは、パケット内のテキストに一致する正規表現を指定できます。複数の正規表現をグループ化する方法については、**regex** コマンドと **class-map type regex** コマンドを参照してください。

デフォルトの検査ポリシー マップ コンフィギュレーションには、DNS パケットのメッセージの最大長を 512 バイトに設定する次のコマンドが含まれます。

```
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
```

1 つのパケットで複数の異なる **match** コマンドまたは **class** コマンドが一致する場合、セキュリティ アプライアンスがアクションを適用する順番はセキュリティ アプライアンスの内部規則で決定されます。ポリシー マップに追加される順番ではありません。内部規則は、アプリケーションのタイプと、パケット解析の論理的な進行状況によって決定されます。ユーザは設定できません。たとえば、HTTP トラフィックの場合、Request Method フィールドは Header Host Length フィールドよりも先に解析されます。Request Method フィールドのアクションは Header Host Length フィールドのアクションの前に実行されます。たとえば、次の match コマンドは任意の順番で入力できますが、**match request method get** コマンドが最初に照合されます。

```
hostname(config-pmap)# match request header host length gt 100
hostname(config-pmap-c)# reset
hostname(config-pmap-c)# match request method get
hostname(config-pmap-c)# log
```

あるアクションがパケットをドロップすると、他のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合は、それ以降のどの **match** コマンドも照合されません。最初のアクションがパケットのロギングである場合は、接続のリセットなどの 2 番目のアクションが発生する可能性があります（同じ **match** コマンドに対して、**reset**（または **drop-connection** など）と **log** アクションを両方設定でできます。その場合、パケットは、指定の照合についてリセットされる前に記録されます）。

パケットが同一の複数の **match** コマンドまたは **class** コマンドと一致する場合、ポリシー マップに出現する順番で一致します。たとえば、ヘッダーの長さが 1001 のパケットの場合、その下にある最初のコマンドに一致し、記録され、次に 2 番目のコマンドと一致し、リセットされます。この 2 つの **match** コマンドの順番を逆にした場合、パケットはドロップされ、接続が 2 番目の **match** コマンドと一致する前にリセットされます。このパケットは記録されません。

```
hostname(config-pmap)# match request header length gt 100
hostname(config-pmap-c)# log
hostname(config-pmap-c)# match request header length gt 1000
hostname(config-pmap-c)# reset
```

あるクラス マップが別のクラス マップ、またはクラス マップ内で優先度の最も低い **match** コマンドに基づいた **match** コマンドと同じタイプであると判断されます（優先度は内部規則に基づきます）。クラス マップが他のクラス マップと同じ優先度の最も低いタイプの **match** コマンドである場合、このクラス マップはポリシー マップに追加される順番に従って照合されます。各クラス マップの優先度の最も低いコマンドが異なる場合、優先度の高い **match** コマンドを持つクラス マップが最初に照合されます。

例

次に、HTTP 検査ポリシー マップと関連するクラス マップの例を示します。このポリシー マップは、サービス ポリシーによってイネーブルになるレイヤ 3/4 ポリシー マップにより有効になります。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2

hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs

hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# drop-connection log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# parameters
hostname(config-pmap-p)# protocol-violation action log

hostname(config-pmap-p)# policy-map test
hostname(config-pmap)# class test (a Layer 3/4 class map not shown)
hostname(config-pmap-c)# inspect http http-map1

hostname(config-pmap-c)# service-policy inbound_policy interface outside
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
parameters	検査ポリシー マップのパラメータ コンフィギュレーション モードに入ります。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

policy-server-secret

SSO サーバへの認証要求を暗号化するために使用する秘密鍵を設定するには、webvpn-sso-siteminder コンフィギュレーション モードで **policy-server-secret** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

policy-server-secret *secret-key*

no policy-server-secret

（注） SSO 認証にはこのコマンドが必要です。

シンタックスの説明

secret-key	認証の通信内容を暗号化するための秘密鍵として使用される文字列。最小文字数にも最大文字数にも制限はありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn-sso-siteminder コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。最初に **sso-server** コマンドを使用して SSO サーバを作成します。次に、**policy-server-secret** コマンドを使用することにより、セキュリティ アプライアンスと SSO サーバ間の認証通信が保証されます。

コマンド引数、*secret-key* はパスワードと同様に作成、保存、および設定が可能です。秘密鍵は、セキュリティ アプライアンスでは `policy-server-secret` コマンドを使用して設定され、SiteMinder Policy Server では Cisco Java プラグイン認証スキームを使用して設定されます。

現在、セキュリティ アプライアンスは、Computer Associates の eTrust SiteMinder SSO サーバ（以前の Netegrity SiteMinder）をサポートしています。

例

次のコマンドは、webvpn-sso-siteminder コンフィギュレーション モードで入力され、ランダムな文字列を引数として含んでいます。このコマンドにより、SSO サーバの認証通信用の秘密鍵が作成されます。

```
hostname(config-webvpn)# sso-server my-sso-server type siteminder
hostname(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
request-timeout	失敗した SSO 認証試行がタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
test sso-server	テスト認証要求で SSO サーバをテストします。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

polltime interface

Active/Active フェールオーバー コンフィギュレーションのデータ インターフェイスのポーリング時間と待機時間を指定するには、フェールオーバー コンフィギュレーション モードで **polltime interface** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

polltime interface [***msec***] *time* [***holdtime*** *time*]

no polltime interface [***msec***] *time* [***holdtime*** *time*]

シンタックスの説明

holdtime *time*	（オプション）データ インターフェイスがピア インターフェイスから hello メッセージを受信する期限を設定します。この期限が経過すると、ピア インターフェイスは障害状態であると宣言されます。有効な値は 5 ～ 75 秒です。
interface *time*	データ インターフェイス ポーリング期間を指定します。有効な値は 3 ～ 15 秒です。オプションの ***msec*** キーワードを使用した場合、有効な値は 500 ～ 999 ミリ秒です。
msec	（オプション）指定する時間がミリ秒単位であることを指定します。

デフォルト

ポーリングの *time* は 5 秒です。

holdtime *time* は、ポーリングの *time* の 5 倍です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	オプションの ***holdtime*** *time* 値が追加され、ポーリング時間をミリ秒で指定できるように変更されました。

使用上のガイドライン

polltime interface コマンドを使用して、指定したフェールオーバー グループに関連付けられたインターフェイスで hello パケットが送信される周波数を変更します。このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。**failover polltime interface** コマンドは、Active/Standby フェールオーバー コンフィギュレーションで使用します。

装置のポーリング時間の 5 倍未満の ***holdtime*** 値は入力できません。ポーリング時間が短いほど、セキュリティ アプライアンスは、それだけ速く障害を検出して、フェールオーバーを起動できます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要な切り替えが発生する可能性があります。インターフェイスのテストが開始されるのは、待機期間の半分が経過したときに、インターフェイス上で hello パケットが受信されていない場合です。

failover polltime unit コマンドと **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスを通過するときは、セキュリティ アプライアンスのフェールオーバー待機時間を 30 秒より低く設定する必要があります。CTIQBE キープアライブ タイムアウトは 30 秒で、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager を使用して再登録する必要があります。

例

次の例（抜粋）は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。フェールオーバー グループ 1 のデータ インターフェイスに対して、インターフェイス ポーリング時間は 500 ミリ秒、待機時間は 5 秒に設定されます。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# polltime interface msec 500 holdtime 5
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover polltime	装置のフェールオーバー ポーリング期間と待機期間を指定します。
failover polltime interface	Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間および待機期間を指定します。

pop3s

POP3S コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **pop3s** コマンドを使用します。POP3S コマンド モードで入力したコマンドを削除するには、このコマンドの **no** 形式を使用します。

POP3 は、インターネット サーバが電子メールを受信し、保持するために使用するクライアント / サーバ プロトコルです。受信者（または受信者のクライアント電子メール レシーバー）は、サーバ上のメールボックスを定期的に確認し、電子メールがあればダウンロードします。この標準プロトコルは、一般的な電子メール製品に組み込まれています。POP3S を使用すると、SSL 接続で電子メールを受信できます。

pop3s

no pop3

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、POP3S コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)#
```

関連コマンド

コマンド	説明
clear configure pop3s	POP3S コンフィギュレーションを削除します。
show running-config pop3s	POP3S の実行コンフィギュレーションを表示します。

port

電子メール プロキシがリッスンするポートを指定するには、適切な電子メール プロキシ モードで **port** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

port {*portnum*}

no port

シンタックスの説明

portnum	電子メール プロキシが使用するポート。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

デフォルト

電子メール プロキシのデフォルト ポートは、次のとおりです。

電子メール プロキシ	デフォルト ポート
IMAP4S	993
POP3S	995
SMTPS	988

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

例

次の例は、IMAP4S 電子メール プロキシのポートを 1066 に設定する方法を示しています。

```
hostname(config)# imap4s
hostname(config-imap4s)# port 1066
```

port-forward

転送 TCP ポートを介して WebVPN ユーザがアクセスできるアプリケーションのセットを設定するには、グローバル コンフィギュレーション モードで **port-forward** コマンドを使用します。複数のアプリケーションへのアクセスを設定するには、このコマンドを同じ listname で複数回（アプリケーションごとに 1 回）使用します。設定したリスト全体を削除するには、**no port-forward** *listname* コマンドを使用します。設定したアプリケーションを削除するには、**no port-forward** *listname localport* コマンドを使用します（*remoteserver* パラメータおよび *remoteport* パラメータは含める必要はありません）。

port-forward {*listname localport remoteserver remoteport description***}**

no port-forward *listname*

no port-forward *listname localport*

シンタックスの説明

description	エンド ユーザのポート転送 Java アプレット画面に表示する、アプリケーション名または簡単な説明を入力します。最大 64 文字です。
listname	WebVPN ユーザがアクセスできるアプリケーション（転送 TCP ポート）のセットをグループ化します。最大 64 文字です。
localport	アプリケーションの TCP トラフィックをリッスンするローカル ポートを指定します。ローカル ポート番号は、1 つの *listname* に対して一度だけ使用できます。
remoteport	このアプリケーションが接続するリモート サーバ上のポートを指定します。
remoteserver	リモート サーバの DNS 名または IP アドレスをアプリケーション用に入力します。DNS 名を使用することをお勧めします。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

デフォルト

デフォルトのポート転送リストはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

特定の TCP ポート転送アプリケーションへのアクセスを特定のユーザまたはグループ ポリシーに許可するには、webvpn モードで、ここで作成した *listname* を **port-forward** コマンドと共に使用します。

例

次の例は、IMAP4S 電子メール、SMTPS 電子メール、DDTS、および Telnet へのアクセスを提供する *SalesGroupPorts* というポート転送リストを作成する方法を示しています。次の表に、この例で使用されている、各アプリケーションの値を示します。

アプリケーション	ローカル ポート	サーバ DNS 名	リモート ポート	説明
IMAP4S 電子メール	143	IMAP4Sserver	20143	Get Mail
SMTPS 電子メール	25	SMTPSserver	20025	Send Mail
DDTS over SSH	22	DDTSserver	20022	DDTS over SSH
Telnet	23	Telnetserver	20023	Telnet

```
hostname(config)# port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
hostname(config)# port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
hostname(config)# port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
hostname(config)# port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

関連コマンド

コマンド	説明
clear configuration port-forward [*listname*]	すべてのポート転送コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドだけを削除します。
port-forward	ユーザまたはグループ ポリシーの WebVPN アプリケーション アクセスをイネーブルにするには、webvpn モードでこのコマンドを使用します。
show running-config port-forward	現在設定されている **port-forward** コマンドのセットを表示します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

port-forward（webvpn）

WebVPN アプリケーション アクセスをこのユーザまたはグループ ポリシーに対してイネーブルにするには、webvpn モードで **port-forward** コマンドを使用します。このモードには、グループ ポリシー モードまたはユーザ名モードから入ります。**port-forward none** コマンドを発行することで作成されたヌル値を含む、ポート転送アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、リストを別のグループ ポリシーから継承できます。ポート転送リストを継承しないようにするには、**port-forward none** コマンドを使用します。

port-forward {**value** *listname* | **none**}

no port-forward

シンタックスの説明

none	フィルタリングを実行しないことを指定します。ヌル値を設定して、フィルタリングを拒否します。フィルタリングの値を継承しないようにします。
value listname	WebVPN ユーザがアクセスできるアプリケーションのリストを指定します。リストを定義するには、コンフィギュレーション モードで port-forward コマンドを使用します。

デフォルト

デフォルトでは、ポート転送はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

コマンドを 2 回使用すると、先行する設定値が上書きされます。

webvpn モードで **port-forward** コマンドを使用してアプリケーション アクセスをイネーブルにする前に、WebVPN 接続で使用することをユーザに許可するアプリケーションのリストを定義する必要があります。このリストを定義するには、グローバル コンフィギュレーション モードで **port-forward** コマンドを使用します。

例

次の例は、*ports1* というポート転送リストを FirstGroup というグループ ポリシーに対して設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward value ports1
```

関連コマンド

コマンド	説明
clear configuration port-forward [*listname*]	すべてのポート転送コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドだけを削除します。
port-forward	WebVPN ユーザがアクセスできるアプリケーション（転送ポート）を定義するには、コンフィギュレーション モードでこのコマンドを使用します。
show running-config port-forward	現在設定されている **port-forward** コマンドのセットを表示します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

port-forward-name

エンド ユーザが TCP ポート転送を識別できる表示名を、特定のユーザまたはグループ ポリシーに対して設定するには、webvpn モードで **port-forward-name** コマンドを使用します。このモードには、グループ ポリシー モードまたはユーザ名モードから入ります。**port-forward-name none** コマンドを使用することにより作成されたヌル値を含む表示名を削除するには、このコマンドの no 形式を使用します。**no** オプションを指定すると、デフォルト名の「Application Access」が復元されます。表示名を復元しないようにするには、**port-forward none** コマンドを使用します。

port-forward-name {**value** *name* | **none**}

no port-forward-name

シンタックスの説明

none	表示名がないことを指定します。ヌル値を設定して、表示名を拒否します。値を継承しないようにします。
value *name*	エンド ユーザに対してポート転送を説明します。最大 255 文字です。

デフォルト

デフォルト名は「Application Access」です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、「Remote Access TCP Applications」という名前を FirstGroup というグループ ポリシーに対して設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

port-object

ポート オブジェクトをサービス オブジェクト グループに追加するには、サービス コンフィギュレーション モードで **port-object** コマンドを使用します。ポート オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

port-object eq *service*

no port-object eq *service*

port-object range *begin_service end_service*

no port-object range *begin_service end_service*

シンタックスの説明

begin_service	サービス範囲の開始値である、TCP ポートまたは UDP ポートの 10 進数または名前を指定します。この値は、0 ～ 65535 で指定する必要があります。
end_service	サービス範囲の終了値である、TCP ポートまたは UDP ポートの 10 進数または名前を指定します。この値は、0 ～ 65535 で指定する必要があります。
eq service	サービス オブジェクトに TCP ポートまたは UDP ポートの 10 進数または名前を指定します。
range	ポートの範囲（包含）を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
サービス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

特定のサービス（ポート）またはサービス範囲（複数のポート）のいずれかのオブジェクトを定義するには、サービス コンフィギュレーション モードで **object-group** と共に **port-object** コマンドを使用します。

TCP サービスまたは UDP サービスの名前を指定する場合、その名前は、TCP、UDP、またはその両方でサポートされている名前のいずれかで、オブジェクト グループのプロトコル タイプと整合性を持つものである必要があります。たとえば、tcp、udp、tcp-udp の各プロトコル タイプの場合、名前はそれぞれ、有効な TCP サービス名、有効な UDP サービス名、TCP および UDP の有効なサービス名である必要があります。

番号を指定した場合、オブジェクトが表示されるときに、プロトコル タイプに基づいて、その番号が対応する名前（存在する場合）に変換されます。

次のサービス名がサポートされています。

表 22-2

TCP	UDP	TCP および UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
telnet		
uucp		
whois		
www		

例

次の例は、サービス コンフィギュレーション モードで **port-object** コマンドを使用して、新しいポート（サービス）オブジェクト グループを作成する方法を示しています。

```
hostname(config)# object-group service eng_service tcp
hostname(config-service)# port-object eq smtp
hostname(config-service)# port-object eq telnet
hostname(config)# object-group service eng_service udp
hostname(config-service)# port-object eq snmp
hostname(config)# object-group service eng_service tcp-udp
hostname(config-service)# port-object eq domain
hostname(config-service)# port-object range 2000 2005
hostname(config-service)# quit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

pppoe client route distance

PPPoE を通してラーニングされたルータの管理ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **pppoe client route distance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pppoe client route distance *distance*

no pppoe client route distance *distance*

シンタックスの説明

distance	PPPoE を通してラーニングされたルータに適用する管理ディスタンスです。有効な値は 1 ～ 255 です。

デフォルト

PPPoE を通してラーニングされたルータに指定されているデフォルトの管理ディスタンスは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

pppoe client route distance コマンドは、ルータが PPPoE からラーニングされた場合にのみチェックされます。ルータが PPPoE からラーニングされた後に **pppoe client route distance** コマンドが入力された場合、指定の管理ディスタンスは既存のラーニングされたルートに対して有効でなくなります。指定した管理ディスタンスが与えられるのは、このコマンドの入力後にラーニングされたルートだけです。

PPPoE を利用してルートを取得するには、**ip address pppoe** コマンドに ***setroute*** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートの優先順位を指定する必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングでのみサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次の例では、GigabitEthernet0/2 上で PPPoE を利用してデフォルト ルートを取得しています。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA オペレーションによって、外部インターフェイスからの 10.1.1.1 ゲートウェイの可用性が監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で PPPoE を通じて取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE を通じて取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route track	PPPoE を通じてラーニングしたルートを、トラッキング エントリ オブジェクトに関連付けます。
sla monitor	SLA 監視オペレーションを定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

pppoe client route track

PPPoE クライアントを設定して、追加されたルートを指定されたトラック済みオブジェクト番号に関連付けるには、インターフェイス コンフィギュレーション モードで **pppoe client route track** コマンドを使用します。PPPoE ルート トラッキングを削除するには、このコマンドの **no** 形式を使用します。

pppoe client route track *number*

no pppoe client route track

シンタックスの説明

number	トラッキング エントリのオブジェクト ID。有効な値は 1 ～ 500 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

pppoe client route track のチェックは、ルートを PPPoE からラーニングした場合にのみ行われます。PPPoE を通じてルートをラーニングした後に **pppoe client route track** コマンドを入力した場合、ラーニングした既存のルートは、トラッキング オブジェクトには関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後にラーニングされたルートだけです。

PPPoE を利用してルートを取得するには、**ip address pppoe** コマンドに ***setroute*** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートの優先順位を指定する必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングでのみサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次の例では、GigabitEthernet0/2 上で PPPoE を利用してデフォルト ルートを取得しています。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA オペレーションによって、外部インターフェイスからの 10.1.1.1 ゲートウェイの可用性が監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で PPPoE を通じて取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE を通じて取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route distance	PPPoE を通じてラーニングしたルートに管理ディスタンスを割り当てます。
sla monitor	SLA 監視オペレーションを定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

pppoe client secondary

PPPoE クライアントをトラック済みのオブジェクトのクライアントとして登録し、トラッキング状態に基づいて起動または終了するように設定するには、インターフェイス コンフィギュレーション モードで **pppoe client secondary** コマンドを使用します。クライアント登録を削除するには、このコマンドの **no** 形式を使用します。

pppoe client secondary track *number*

no pppoe client secondary track

シンタックスの説明

number	トラッキング エントリのオブジェクト ID。有効な値は 1 ～ 500 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

pppoe client secondary コマンドは、PPPoE セッションの起動時にのみチェックされます。PPPoE を通じてルートをラーニングした後に **pppoe client route track** コマンドを入力した場合、ラーニングした既存のルートは、トラッキング オブジェクトには関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後にラーニングされたルートだけです。

PPPoE を利用してルートを取得するには、**ip address pppoe** コマンドに ***setroute*** オプションを指定する必要があります。

複数のインターフェイスで PPPoE を設定した場合は、各インターフェイスについて **pppoe client route distance** コマンドを使用して、インストール済みルートの優先順位を指定する必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングでのみサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次の例では、GigabitEthernet0/2 上で PPPoE を利用してデフォルト ルートを取得しています。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA オペレーションによって、外部インターフェイスからの 10.1.1.1 ゲートウェイの可用性が監視されます。この SLA オペレーションが失敗した場合は、GigabitEthernet0/3 上で PPPoE を通じて取得したセカンダリ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# interface GigabitEthernet0/2
hostname(config-if)# pppoe client route track 1
hostname(config-if)# ip address pppoe setroute
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# pppoe client secondary track 1
hostname(config-if)# pppoe client route distance 254
hostname(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE を通じて取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route distance	PPPoE を通じてラーニングしたルートに管理ディスタンスを割り当てます。
pppoe client route track	PPPoE を通じてラーニングしたルートを、トラッキング エントリ オブジェクトに関連付けます。
sla monitor	SLA 監視オペレーションを定義します。

preempt

装置の優先順位が高い場合に、その装置をブート時にアクティブにするには、フェールオーバー グループ コンフィギュレーション モードで **preempt** コマンドを使用します。プリエンプションを削除するには、このコマンドの **no** 形式を使用します。

preempt [*delay*]

no preempt [*delay*]

シンタックスの説明

delay	ピアがプリエンプションされるまでの待ち時間（秒）。有効な値は 1 ～ 1200 秒です。

デフォルト

デフォルトでは、待ち時間はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プライマリまたはセカンダリの優先順位をフェールオーバー グループに割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートしたときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。ただし、ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方の装置がオンラインになると、優先順位として 2 番目の装置を持つフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドを使用して設定されているか、手作業で **no failover active** コマンドを使用してもう一方の装置に強制しない限り、2 番目の装置上ではアクティブになりません。フェールオーバー グループが **preempt** コマンドを使用して設定されている場合、そのフェールオーバー グループは、指定装置上で自動的にアクティブになります。

（注） ステートフル フェールオーバーがイネーブルの場合、フェールオーバー グループが現在アクティブである装置から接続が複製されるまで、プリエンプションは実行されません。

例

次の例では、優先順位の高いプライマリ装置を持つフェールオーバー グループ 1 と、優先順位の高いセカンダリ装置を持つフェールオーバー グループ 2 を設定しています。どちらのフェールオーバー グループも、**preempt** コマンドを使用して待ち時間 100 秒で設定されています。したがって、これらのグループは、優先する装置が利用可能になってから 100 秒後に、その装置上で自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
primary	設定しているフェールオーバー グループのフェールオーバー ペア優先順位における、プライマリ装置を指定します。
secondary	設定しているフェールオーバー グループのフェールオーバー ペア優先順位における、セカンダリ装置を指定します。

prefix-list

ABR タイプ 3 LSA フィルタリングのプレフィックス リストのエントリを作成するには、グローバル コンフィギュレーション モードで **prefix-list** コマンドを使用します。プレフィックス リスト エントリを削除するには、このコマンドの **no** 形式を使用します。

prefix-list *prefix-list-name* [***seq*** *seq_num*] {***permit*** | ***deny***} *network/len* [***ge*** *min_value*] [***le*** *max_value*]

no prefix-list *prefix-list-name* [***seq*** *seq_num*] {***permit*** | ***deny***} *network/len* [***ge*** *min_value*] [***le*** *max_value*]

シンタックスの説明

/	*network* 値と *len* 値の間に必要な区切り記号。
deny	一致した条件へのアクセスを拒否します。
ge *min_value*	（オプション）一致する必要のある最小プレフィックス長を指定します。*min_value* 引数の値は、*len* 引数の値より大きくする必要があります。また、*max_value* 引数が存在する場合は、それ以下にする必要があります。
le *max_value*	（オプション）一致する必要のある最大プレフィックス長を指定します。*max_value* 引数の値は、*min_value* 引数が存在する場合は、その値以上にする必要があり、*min_value* 引数が存在しない場合は、*len* 引数の値より大きくする必要があります。
len	ネットワーク マスクの長さ。有効な値は 0 ～ 32 です。
network	ネットワーク アドレス。
permit	一致した条件へのアクセスを許可します。
prefix-list-name	プレフィックス リストの名前。プレフィックス リスト名にスペースを含めることはできません。
seq *seq_num*	（オプション）指定したシーケンス番号を、作成中のプレフィックス リストに適用します。

デフォルト

シーケンス番号を指定しない場合、プレフィックス リストの最初のエントリにシーケンス番号 5 が割り当てられ、以降の各エントリには、5 ずつ増加するシーケンス番号が割り当てられます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

prefix-list コマンドは、ABR タイプ 3 LSA フィルタリング コマンドです。ABR タイプ 3 LSA フィルタリングによって OSPF 実行中の ABR 機能を拡張し、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されると、指定したプレフィックスだけが一方から他方のエリアに送信されます。その他のプレフィックスは、すべてそれぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアが終点または起点となるトラフィック、あるいはそのエリアの着信および発信両方のトラフィックに適用できます。

プレフィックス リストの複数のエントリが所定のプレフィックスに一致する場合、最も小さいシーケンス番号を持つエントリが使用されます。セキュリティ アプライアンスは、プレフィックス リストの最上部から、つまり最も小さいシーケンス番号を持つエントリから検索を開始します。一致が見つかると、セキュリティ アプライアンスは、リストの残りの部分を調べません。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

デフォルトでは、シーケンス番号は自動的に生成されます。それらは、**no prefix-list sequence-number** コマンドで抑制できます。シーケンス番号は、5 ずつ増分されます。プレフィックス リスト内に最初に生成されるシーケンス番号は 5 です。リスト内の次のエントリのシーケンス番号は 10 となり、以降も同様となります。あるエントリの値を指定し、後続のエントリの値を指定しない場合、生成されるシーケンス番号は、指定した値から 5 ずつ増分されます。たとえば、プレフィックス リストの最初のエントリのシーケンス番号を 3 と指定し、その後シーケンス番号を指定しないで 2 つのエントリを追加した場合、これら 2 つエントリに対して自動的に生成されるシーケンス番号は、8 および 13 となります。

ge キーワードおよび ***le*** キーワードを使用して、*network/len* 引数より具体的なプレフィックスと一致する必要のあるプレフィックスの長さの範囲を指定できます。***ge*** キーワードも ***le*** キーワードも指定しない場合は、完全一致が前提とされます。***ge*** キーワードだけを指定した場合の範囲は、*min_value* ～ 32 です。***le*** キーワードだけを指定した場合の範囲は、*len* ～ *max_value* です。

min_value 引数および *max_value* 引数の値は、次の条件を満たしている必要があります。

len < *min_value* <= *max_value* <= 32

特定のエントリをプレフィックス リストから削除するには、このコマンドの **no** 形式を使用します。プレフィックス リストを削除するには、**clear configure prefix-list** コマンドを使用します。**clear configure prefix-list** コマンドを使用すると、関連付けられた **prefix-list description** コマンドがある場合は、それもコンフィギュレーションから削除されます。

例

次の例では、デフォルト ルート 0.0.0.0/0 を拒否します。

```
hostname(config)# prefix-list abc deny 0.0.0.0/0
```

次の例では、プレフィックス 10.0.0.0/8 を許可します。

```
hostname(config)# prefix-list abc permit 10.0.0.0/8
```

次の例は、プレフィックス 192/8 を持つルートで最大 24 ビットのマスク長を受け入れる方法を示しています。

```
hostname(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

次の例は、プレフィックス 192/8 を持つルートで 25 ビットより大きいマスク長を拒否する方法を示しています。

```
hostname(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

次の例は、すべてのアドレス空間で 8 ～ 24 ビットのマスク長を許可する方法を示しています。

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

次の例は、すべてのアドレス空間で 25 ビットより大きいマスク長を拒否する方法を示しています。

```
hostname(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

次の例は、プレフィックス 10/8 を持つすべてのルートを拒否する方法を示しています。

```
hostname(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

次の例は、プレフィックス 192.168.1/24 を持つルートで長さが 25 ビットより大きいすべてのマスクを拒否する方法を示しています。

```
hostname(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

次の例は、プレフィックス 0/0 を持つすべてのルートを許可する方法を示しています。

```
hostname(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

関連コマンド

コマンド	説明
clear configure prefix-list	**prefix-list** コマンドを実行コンフィギュレーションから削除します。
prefix-list description	プレフィックス リストの説明を入力できます。
prefix-list sequence-number	プレフィックス リストのシーケンス番号付けをイネーブルにします。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

prefix-list description

プレフィックス リストに説明を追加するには、グローバル コンフィギュレーション モードで **prefix-list description** コマンドを使用します。プレフィックス リストの説明を削除するには、このコマンドの **no** 形式を使用します。

prefix-list *prefix-list-name* **description** *text*

no prefix-list *prefix-list-name* **description** [*text*]

シンタックスの説明

prefix-list-name	プレフィックス リストの名前。
text	プレフィックス リストの説明テキスト。最大で 80 文字入力できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

prefix-list コマンドおよび **prefix-list description** コマンドは、特定のプレフィックス リスト名に対して任意の順序で入力できます。つまり、プレフィックス リストの説明を入力する前に、プレフィックス リストを作成する必要はありません。**prefix-list description** コマンドは、コンフィギュレーション内で常に、関連付けられたプレフィックス リストの前の行に記述されます。これは、コマンドを入力した順序とは関係ありません。

すでに説明があるプレフィックス リスト エントリに対して **prefix-list description** コマンドを入力した場合、元の説明は新しい説明に置き換えられます。

このコマンドの **no** 形式を使用している場合、テキスト説明を入力する必要はありません。

例

次の例では、MyPrefixList という名前のプレフィックス リストの説明を追加します。**show running-config prefix-list** コマンドは、プレフィックス リストの説明が実行コンフィギュレーションにすでに追加されているものの、プレフィックスリスト自体は設定されていないことを示します。

```
hostname(config)# prefix-list MyPrefixList description A sample prefix list
description
hostname(config)# show running-config prefix-list

!
prefix-list MyPrefixList description A sample prefix list description
!
```

関連コマンド

コマンド	説明
clear configure prefix-list	**prefix-list** コマンドを実行コンフィギュレーションから削除します。
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

prefix-list sequence-number

プレフィックス リストのシーケンス番号付けをイネーブルにするには、グローバル コンフィギュレーション モードで **prefix-list sequence-number** コマンドを使用します。プレフィックス リストのシーケンス番号付けをディセーブルにするには、このコマンドの **no** 形式を使用します。

prefix-list sequence-number

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

プレフィックス リストのシーケンス番号付けは、デフォルトでイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。このコマンドの **no** 形式がコンフィギュレーションにある場合、シーケンス番号は、手動で設定したものも含めて、コンフィギュレーションの **prefix-list** コマンドから削除されます。また、新しいプレフィックス リスト エントリには、シーケンス番号が割り当てられません。

プレフィックス リストのシーケンス番号付けがイネーブルの場合、すべてのプレフィックス リスト エントリには、デフォルトの番号付け方式（開始値は 5 で、各番号は 5 ずつ増分される）で、シーケンス番号が割り当てられます。番号付けをディセーブルにする前に、シーケンス番号を手動でプレフィックス リスト エントリに割り当てた場合、手動で割り当てた番号が復元されます。自動番号付けがディセーブルになっているときに手動で割り当てたシーケンス番号も復元されます。ただし、番号付けがディセーブルの間、それらのシーケンス番号は表示されません。

例

次の例では、プレフィックス リストのシーケンス番号付けをディセーブルにします。

```
hostname(config)# no prefix-list sequence-number
```

関連コマンド

コマンド	説明
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーション内の **prefix-list** コマンドを表示します。

pre-shared-key

事前共有キーに基づく IKE 接続をサポートするために事前共有キーを指定するには、トンネル グループ ipsec アトリビュート コンフィギュレーション モードで **pre-shared-key** コマンドを使用します。デフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

pre-shared-key *key*

no pre-shared-key

シンタックスの説明

key	1 ～ 128 文字の英数字でキーを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、すべての IPSec トンネル グループ タイプに適用できます。

例

config-ipsec コンフィギュレーション モードで入力された次のコマンドは、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループの IKE 接続をサポートするため、事前共有キー XYZX を指定します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# pre-shared-key xyzx
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

primary

フェールオーバー グループに対するプライマリ装置の優先順位を高くするには、フェールオーバー グループ コンフィギュレーション モードで **primary** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

primary

no primary

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

フェールオーバー グループに対して **primary** または **secondary** を指定しない場合、そのフェールオーバー グループは、デフォルトでは **primary** に設定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プライマリまたはセカンダリの優先順位をフェールオーバー グループに割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートしたときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方の装置がオンラインになると、優先順位として 2 番目の装置を持つフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドを使用して設定されているか、手作業で **no failover active** コマンドを使用してもう一方の装置に強制しない限り、2 番目の装置上ではアクティブになりません。

例

次の例では、優先順位の高いプライマリ装置を持つフェールオーバー グループ 1 と、優先順位の高いセカンダリ装置を持つフェールオーバー グループ 2 を設定しています。どちらのフェールオーバー グループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先する装置が使用可能になったときにその装置上で自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
preempt	優先する装置が使用可能になったときに、フェールオーバー グループをその装置上で強制的にアクティブにします。
secondary	セカンダリ装置に、プライマリ装置より高い優先順位を設定します。

priority

厳密なスケジューリング優先順位をこのクラスに適用するには、クラス モードで **priority** コマンドを使用します。優先順位要件を削除するには、このコマンドの **no** 形式を使用します。

priority

no priority

シンタックスの説明

このコマンドには、パラメータも変数もありません。

デフォルト

デフォルトの動作や変数はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

priority コマンドを発行するには、**policy-map** コマンドと **class** コマンドをあらかじめ設定しておく必要があります。

例

次に、ポリシー マップ モードの **priority** コマンドの例を示します。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class firstclass
hostname(config-pmap-c)# priority
hostname(config-pmap-c)# class class-default
hostname(config-pmap-c)#
```

関連コマンド

class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

priority（VPN ロード バランシング）

仮想ロードバランシング クラスタに参加するローカル デバイスの優先順位を設定するには、VPN ロードバランシング モードで **priority** コマンドを使用します。デフォルトの優先順位指定に戻すには、このコマンドの **no** 形式を使用します。

priority *priority*

no priority

シンタックスの説明

priority	このデバイスに割り当てる優先順位（範囲は 1 ～ 10）。

デフォルト

デフォルトの優先順位は、デバイスのモデル番号によって異なります。

モデル番号	デフォルトの優先順位
5520	5
5540	7

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
VPN ロードバランシング	—	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシング モードに入る必要があります。

このコマンドは、仮想ロードバランシング クラスタに参加しているローカル デバイスの優先順位を設定します。

優先順位は、1（最低）～ 10（最高）の整数である必要があります。

優先順位は、マスター選定プロセスで、VPN ロードバランシング クラスタ内のどのデバイスがそのクラスタのマスター デバイスまたはプライマリ デバイスになるかを決定する方法の 1 つとして使用されます。マスター選定プロセスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

このコマンドの ***no*** 形式を使用すると、優先順位指定がデフォルト値に戻ります。

例

次に、VPN ロードバランシング コマンド シーケンスの例を示します。これには、現在のデバイスの優先順位を 9 に設定する **priority** コマンドが含まれています。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードに入ります。

priority-queue

インターフェイス上にプライオリティ キューイングを設定するには、グローバル コンフィギュレーション モードで priority-queue コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

priority-queue *interface-name*

no priority queue *interface-name*

シンタックスの説明

interface-name	プライオリティ キューイングをイネーブルにする物理インターフェイスの名前を指定します。

デフォルト

デフォルトでは、プライオリティ キューイングはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、次の 2 つのトラフィック クラスを使用できます。1 つは優先順位が高く、遅延に影響されやすいトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）で、もう 1 つは、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）です。セキュリティ アプライアンスは、優先トラフィックを認識し、適切な Quality of Service（QoS; サービス品質）ポリシーを適用します。プライオリティ キューのサイズと項目数を設定することで、トラフィック フローを微調整できます。

プライオリティ キューイングが発生するようにするには、名前付き物理インターフェイスに対してプライオリティ キューを作成する必要があります。プライオリティ キューを作成するには、グローバル コンフィギュレーション モードで **priority-queue** コマンドを使用します。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義された各物理インターフェイスに対して適用できます。**priority-queue** コマンドは、VLAN インターフェイスには適用できません。

priority-queue コマンドを使用すると、プライオリティ キュー モードに入ります。モードはプロンプトに表示されます。プライオリティ キュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびバッファに入れることのできる両タイプ（優先またはベストエフォート）のパケット数を設定できます（**queue-limit** コマンド）。queue-limit の数を超えると、以後のパケットはドロップされます。

指定する tx-ring-limit 値および queue-limit 値は、優先順位の高い低遅延キューとベストエフォートキューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両タイプのパケットの数です。このパケットの処理が終わると、ドライバは輻輳が解消するまで、インターフェイスの先頭にある、パケットをバッファしているキューの処理に戻ります。一般に、これらの 2 つのパラメータを調整することによって、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注） **queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。キューは、使用可能なメモリの量を超えることはできません。理論上の最大パケット数は、2,147,483,647（つまり、全二重時の回線速度が上限）です。

既存の VPN クライアント トラフィック、LAN-to-LAN トラフィック、または非トンネル トラフィックが確立されているインターフェイスを対象として、サービス ポリシーを適用または削除した場合、QoS ポリシーは適用されず、トラフィック ストリームから削除されません。このような接続を対象として QoS ポリシーを適用または削除するには、接続を消去（ドロップ）して再確立する必要があります。

優先順位とポリシングを、両方ともイネーブルにすることはできません。

例

次の例では、test というインターフェイスのプライオリティ キューを設定して、キューの上限を 30,000 パケット、送信キューの上限を 256 パケットと指定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
hostname(priority-queue)#
```

関連コマンド

コマンド	説明
queue-limit	プライオリティ キューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。
tx-ring-limit	イーサネット送信ドライバのキューにいつでも入れることができるパケットの最大数を設定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
clear configure priority-queue	現在のプライオリティ キュー コンフィギュレーションを削除します。
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、現在のすべてのプライオリティ キュー、および queue-limit と tx-ring-limit のコンフィギュレーション値が表示されます。

privilege

コマンド特権レベルを設定するには、グローバル コンフィギュレーション モードで **privilege** コマンドを使用します。この設定を取り消すには、このコマンドの **no** 形式を使用します。

privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

no privilege [**show | clear | configure**] **level** *level* [**mode** {**enable | configure**}] **command** *command*

シンタックスの説明

clear	（オプション）指定されたコマンドに対応する **clear** コマンドの特権レベルを設定します。
command *command*	特権レベルを設定する対象のコマンドを指定します。
configure	（オプション）指定したコマンドの特権レベルを設定します。
level *level*	特権レベルを指定します。有効値は 0 ～ 15 です。
mode enable	（オプション）コマンドのイネーブル モード用のレベルであることを指定します。
mode configure	（オプション）コマンドの設定モード用のレベルであることを指定します。
show	指定されたコマンドに対応する **show** コマンドの特権レベルを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

privilege コマンドを使用すると、セキュリティ アプライアンスのコマンドにユーザ定義の特権レベルを設定できます。このコマンドは、**show** コマンド、および **clear** コマンドという関連するコンフィギュレーションに異なる特権レベルを設定する場合に特に役立ちます。新しい特権レベルを使用する前に、セキュリティ ポリシーでコマンドの特権レベル変更を必ず検証してください。

コマンドおよびユーザに特権レベルが設定されている場合、両者は比較されて指定ユーザが指定コマンドを実行できるかどうかが判別されます。ユーザの特権レベルがコマンドの特権レベルよりも低い場合、ユーザはそのコマンドを実行できません。

特権レベルを切り替えるには、**login** コマンドを使用して別の特権レベルにアクセスし、適切な **logout** コマンド、**exit** コマンド、または **quit** コマンドを使用してそのレベルを終了します。

mode enable キーワードおよび **mode configure** キーワードは、イネーブル モードと設定モードの両方を持つコマンドで使用します。

特権レベルの数字が小さいほど、レベルは低くなります。

(注) **aaa authentication** コマンドと **aaa authorization** コマンドには、AAA サーバのコンフィギュレーションで使用する前に、定義する新しい特権レベルを入れる必要があります。

例

次の例は、個々のユーザに特権レベル「5」を設定する方法を示しています。

```
username intern1 password pass1 privilege 5
```

次の例は、特権レベル「5」の **show** コマンド セットを定義する方法を示しています。

```
hostname(config)# privilege show level 5 command alias
hostname(config)# privilege show level 5 command apply
hostname(config)# privilege show level 5 command arp
hostname(config)# privilege show level 5 command auth-prompt
hostname(config)# privilege show level 5 command blocks
hostname(config)#
```

次の例は、特権レベル 11 を AAA 許可コンフィギュレーション全体に適用する方法を示しています。

```
hostname(config)# privilege configure level 11 command aaa
hostname(config)# privilege configure level 11 command aaa-server
hostname(config)# privilege configure level 11 command access-group
hostname(config)# privilege configure level 11 command access-list
hostname(config)# privilege configure level 11 command activation-key
hostname(config)# privilege configure level 11 command age
hostname(config)# privilege configure level 11 command alias
hostname(config)# privilege configure level 11 command apply
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド文を削除します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

prompt

セッション プロンプト表示を設定するには、コンフィギュレーション モード（P_CONF）、複製（P_REP）、シングル モード、およびマルチモードのシステム コンテキストで **prompt** コマンドを使用します。設定されたプロンプトを表示できるのは、管理者だけです。ユーザ コンテキストでは、デフォルトのホスト名 / コンテキスト（コンフィギュレーション モード）プロンプトが表示されます。

prompt [<*keyword*> [*keyword*>] ...]

no prompt

シンタックスの説明

キーワード	説明
context	現在のコンテキストを表示するプロンプトを設定します（マルチモードのみ）。
domain	ドメインを表示するプロンプトを設定します。
hostname	ホスト名を表示するプロンプトを設定します。
priority	「failover lan unit」設定を表示するプロンプトを設定します。
state	現在のトラフィック処理の状態を表示するプロンプトを設定します。 *state* キーワードに対しては、次の値が表示されます。 *act*：装置は、トラフィックが通過している状態です（フェールオーバーがイネーブルになっている Active など）。 *stby*：装置は、トラフィックが通過している状態ではなく、スタンバイ、障害、またはその他の非アクティブ状態になっている可能性があります。 *actNoFailover*：装置は、非フェールオーバーで、トラフィックが通過できる状態です。

デフォルト

デフォルトはホスト名 / コンテキスト プロンプトです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

プロンプトに情報を追加できるため、複数のモジュールがある場合にどのモジュールにログインしているかを一目で判別できます。この機能は、フェールオーバーの発生時、2 つのモジュールのホスト名が同じ場合に重要になります。

例

次の例は、プロンプトを設定する方法を示しています。

```
asa (config)# prompt hostname context priority state
```

前提条件は次のとおりです。

```
hostname = myasa
context = admin
priority = failover lan unit primary
state = Active (with failover enabled)
```

プロンプトは次のように表示されます。

```
myasa/admin/pri/act>
myasa/admin/pri/act#
myasa/admin/pri/act(config)#
myasa/admin/pri/act(config-interface)#
```

ヘルプと使用方法は次のとおりです。

```
asa# help prompt

asa# prompt ?

configure mode commands/options:
hostname    Configures the prompt to display the hostname
domain       Configures the prompt to display the domain
context       Configures the prompt to display the current context (multimode only)
priority       Configures the prompt to display the 'failover lan unit' setting
state           Configures the prompt to display the current traffic handling state
```

関連コマンド

コマンド	説明
clear config prompt	設定されているプロンプトを消去します。
no prompt	プロンプトを完全に削除します。
show running-config prompt	設定されているプロンプトを表示します。

protocol-enforcement

圧縮およびループ ポインタ チェックを含む、ドメイン名、ラベルの長さ、形式のチェックをイネーブルにするには、パラメータ コンフィギュレーション モードで **protocol-enforcement** コマンドを使用します。プロトコル強制をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol-enforcement

no protocol-enforcement

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

プロトコル強制はデフォルトでイネーブルになっています。このコマンドは、**policy-map type inspect dns** を定義していなくても、**inspect dns** を設定している場合はイネーブルにできます。ディセーブルにするには、ポリシー マップ コンフィギュレーションで **no protocol-enforcement** を明示的に記述する必要があります。**inspect dns** を設定していない場合、NAT リライトは実行されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

特定の条件下では、このコマンドがディセーブルであってもプロトコル強制は行われます。たとえば、DNS リソース レコードの分類、NAT または TSIG チェックなど、DNS リソース レコードの解析が他の目的に必要な場合に行われます。

例

次の例では、プロトコル強制を DNS 検査ポリシー マップ内でイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# protocol-enforcement
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

protocol http

CRL を取得するために許可する配布ポイント プロトコルとして HTTP を指定するには、ca-crl コンフィギュレーション モードで **protocol http** コマンドを使用します。アクセス権があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した HTTP を削除するには、このコマンドの **no** 形式を使用します。

protocol http

no protocol http

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、HTTP を許可する設定になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する場合は、HTTP ルールを公開インターフェイス フィルタに必ず割り当ててください。

例

次の例では、ca-crl コンフィギュレーション モードに入り、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして HTTP を許可します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol http
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol ldap	CRL の取得方法として LDAP を指定します。
protocol scep	CRL の取得方法として SCEP を指定します。

protocol ldap

CRL を取得するための配布ポイント プロトコルとして LDAP を指定するには、ca-crl コンフィギュレーション モードで **protocol ldap** コマンドを使用します。アクセス権があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した LDAP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol ldap

no protocol ldap

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、LDAP を許可する設定になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして LDAP を許可します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol ldap
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol http	HTTP を CRL 取得方法として指定します。
protocol scep	SCEP を CRL 取得方法として指定します。

protocol scep

CRL を取得するための配布ポイント プロトコルとして SCEP を指定するには、crl 設定モードで **protocol scep** コマンドを使用します。アクセス権があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した SCEP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol scep

no protocol scep

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、SCEP を許可する設定になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次の例では、ca-crl コンフィギュレーション モードに入り、トラストポイント central の CRL を取得するための配布ポイント プロトコルとして SCEP を許可します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# protocol scep
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
protocol http	HTTP を CRL 取得方法として指定します。
protocol ldap	LDAP を CRL 取得方法として指定します。

protocol-object

プロトコル オブジェクトをプロトコル オブジェクト グループに追加するには、プロトコル コンフィギュレーション モードで **protocol-object** コマンドを使用します。ポート オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

protocol-object *protocol*

no protocol-object *protocol*

シンタックスの説明

protocol	プロトコルの名前または番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プロトコル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

プロトコル コンフィギュレーション モードでプロトコル オブジェクトを定義するには、**object-group** コマンドと共に **protocol-object** コマンドを使用します。

protocol 引数を使用して、IP プロトコルの名前または番号を指定できます。udp プロトコル番号は 17、tcp プロトコル番号は 6、egp プロトコル番号は 47 です。

例

次の例は、プロトコル オブジェクトを定義する方法を示しています。

```
hostname(config)# object-group protocol proto_grp_1
hostname(config-protocol)# protocol-object udp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# exit
hostname(config)# object-group protocol proto_grp
hostname(config-protocol)# protocol-object tcp
hostname(config-protocol)# group-object proto_grp_1
hostname(config-protocol)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

protocol-violation

プロトコル違反に対するアクションを定義するには、パラメータ コンフィギュレーション モードで **protocol-violation** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

protocol-violation action [drop | log]

no protocol-violation action [drop | log]

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ポリシー マップにおけるプロトコル違反に対するアクションを設定する方法を示します。

```
hostname(config-pmap-p)# protocol-violation action drop
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

proxy-bypass

コンテンツの最低限の書き換えを実行すると共に、書き換えるコンテンツのタイプとして、外部リンクと XML の両方またはいずれか一方を指定するようにセキュリティ アプライアンスを設定するには、webvpn モードで **proxy-bypass** コマンドを使用します。プロキシ バイパスをディセーブルにするには、このコマンドの **no** 形式を使用します。

proxy-bypass interface *interface name* **{port** *port number*| **path-mask** *path mask***} target** *url* **[rewrite {link | xml | none}]**

no proxy-bypass interface *interface name* **{port** *port number*| **path-mask** *path mask***} target** *url* **[rewrite {link | xml | none}]**

シンタックスの説明

host	トラフィックの転送先となるホストを指定します。ホスト IP アドレスまたはホスト名のいずれかを使用してください。
interface	プロキシ バイパス用の ASA インターフェイスを特定します。
interface name	ASA インターフェイスを名前で指定します。
link	絶対外部リンクの書き換えを指定します。
none	書き換えを指定しません。
path-mask	一致させるパターンを指定します。
path-mask	正規表現を含むことができるパターンと一致するよう、パターンを指定します。次のワイルドカードを使用できます。 *：すべてと一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列と共に使用する必要があります。 ?：任意の 1 文字と一致します。 [!seq]：シーケンスにない任意の文字に一致します。 [seq]：シーケンス内の任意の文字に一致します。 最大 128 バイトです。
port	プロキシ バイパス用に予約されているポートを特定します。
port number	プロキシ バイパス用に予約されている上位番号のポートを指定します。ポートの範囲は 20000 ～ -21000 です。1 つのプロキシ バイパスの規則に対してポートは 1 つだけ使用できます。
rewrite	（オプション）書き換えに対する追加規則を指定します（none、または XML と link の組み合せを付加）。
target	トラフィックの転送先となるリモート サーバを特定します。
url	URL を **http(s)://***fully_qualified_domain_name*[:*port*] という形式で入力します。最大 128 バイトです。ポートは、特に指定しない限り、HTTP の場合は 80、HTTPS の場合は 443 です。
xml	XML コンテンツの書き換えを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

プロキシ バイパスは、コンテンツの書き換えを最小限に実行して、アプリケーションおよび Web リソースの動作を向上させるために使用します。プロキシ バイパス コマンドにより、セキュリティ アプライアンスを通過する特定の Web アプリケーションの処理方法が決定されます。

このコマンドは複数回使用できます。エントリを設定する順序は重要でありません。プロキシ バイパス規則は、インターフェイスとパス マスクまたはインターフェイスとポートによって一意に特定されます。

パス マスクではなく、ポートを使用してプロキシ バイパスを設定する場合、ネットワーク コンフィギュレーションによっては、これらのポートのセキュリティ アプライアンスへのアクセスを許可するためにファイアウォール設定の変更が必要になることがあります。このような制限を回避するには、パス マスクを使用してください。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスとは、URL の .com または .org あるいはその他のタイプのドメイン名の後にあるものすべてをいいます。たとえば、www.mycompany.com/hrbenefits という URL では、*hrbenefits* がパスです。同様に、www.mycompany.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての「hr」サイトにプロキシ バイパスを使用する場合は、/hr* というようにワイルドカード * を使用すると、コマンドを複数回使用しないようにできます。

例

次の例は、HTTP とそのデフォルト ポート 80 を使用するセキュリティ アプライアンスが webvpn インターフェイス上でプロキシ　バイパス用のポート　20001　を使用してトラフィックを mycompany.site.com に転送し、XML コンテンツを書き換えるように設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface webvpn port 20001 target
http://mycompany.site.com rewrite xml
hostname(config-webvpn)#
```

次の例は、HTTPS とそのデフォルト ポート 443 を使用するセキュリティ アプライアンスが外部インターフェイスのプロキシ バイパス用パス マスク「mypath/*」を使用して、トラフィックを mycompany.site.com に転送し、XML およびリンク コンテンツを書き換えるように設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# proxy-bypass interface outside path-mask /mypath/* target
https://mycompany.site.com rewrite xml,link
hostname(config-webvpn)#
```

関連コマンド -

コマンド	説明
apcf	特定のアプリケーションに使用する非標準の規則を指定します。
rewrite	トラフィックがセキュリティ アプライアンスを通過するかどうかを決定します。

pwd

現在の作業ディレクトリを表示するには、特権 EXEC モードで **pwd** コマンドを使用します。

pwd

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトは、ルート ディレクトリ（/）です。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドは、機能の点で ***dir*** コマンドと類似しています。

例　次の例は、現在の作業ディレクトリを表示する方法を示しています。

```
hostname# pwd
flash:
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに移動します。
dir	ディレクトリの内容を表示します。
more	ファイルの内容を表示します。

CHAPTER 23

queue-limit コマンド～ rtp-conformance コマンド

queue-limit（プライオリティ キュー）

プライオリティ キューの深さを指定するには、プライオリティ キュー モードで **queue-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

シンタックスの説明

number-of-packets	インターフェイスがパケットのドロップを開始するまで、キューに入れる（つまり、バッファ処理する）ことができる低遅延パケットまたは通常の優先順位のパケットの最大数を指定します。指定可能な値の範囲については、「使用上の注意」の項を参照してください。

デフォルト

デフォルトでは、キューの上限は 1,024 パケットです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プライオリティ キュー	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、次の 2 つのトラフィック クラスを使用できます。1 つは優先順位が高く、遅延に影響されやすいトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）で、もう 1 つは、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）です。セキュリティ アプライアンスは、優先トラフィックを認識し、適切な Quality of Service（QoS; サービス品質）ポリシーを適用します。プライオリティ キューのサイズと項目数を設定することで、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にするには、**priority-queue** コマンドを使用して、インターフェイスのプライオリティ キューをあらかじめ作成しておく必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドを使用すると、プライオリティ キュー モードに入ります。モードはプロンプトに表示されます。プライオリティ キュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびバッファに入れることのできる両タイプ（優先またはベストエフォート）のパケット数を設定できます（**queue-limit** コマンド）。queue-limit の数を超えると、以後のパケットはドロップされます。

（注） インターフェイスのプライオリティ キューイングをイネーブルにするには、**priority-queue** コマンドを設定する必要があります。

指定する tx-ring-limit および queue-limit は、優先順位の高い低遅延キューとベストエフォート キューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両タイプのパケットの数です。このパケットの処理が終わると、ドライバは輻輳が解消するまで、インターフェイスの先頭にある、パケットをバッファしているキューの処理に戻ります。一般に、これらの 2 つのパラメータを調整することによって、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注） **queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。キューは、使用可能なメモリの量を超えることはできません。理論上の最大パケット数は 2,147,483,647 です。

例

次の例では、test というインターフェイスのプライオリティ キューを設定して、キューの上限を 30,000 パケット、送信キューの上限を 256 パケットと指定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 30000
hostname(priority-queue)# tx-ring-limit 256
hostname(priority-queue)#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、現在のすべてのプライオリティ キュー、および queue-limit と tx-ring-limit のコンフィギュレーション値が表示されます。
tx-ring-limit	イーサネット送信ドライバのキューにいつでも入れることができるパケットの最大数を設定します。

queue-limit（tcp マップ）

TCP ストリームのキューに入れることのできる順序付けされていないパケットの最大数を設定するには、tcp マップ コンフィギュレーション モードで **queue-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *pkt_num*

no queue-limit *pkt_num*

シンタックスの説明

pkt_num	順序付けされていないパケットがドロップされるまでに、TCP 接続のキューに入れることのできる、順序付けされていないパケットの最大数を指定します。範囲は 0 ～ 250 です。デフォルトは 0 です。

デフォルト

デフォルトの最大パケット数は 0 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **queue-limit** コマンドを使用すると、任意の TCP 接続の TCP パケットの順序付けをイネーブルにしたり、デフォルトで順序付けされている接続のキューの上限を変更したりできます。

検査、IDS 機能、または TCP check-retransmission のいずれかの機能がイネーブルになっている場合、パケットは TCP 接続上で順序付けされます。順序付けされている接続のパケット キューのデフォルトの上限は、1 フローにつき 2 つです。それ以外のすべての TCP 接続の場合、パケットは受信と同時に転送されます。これには、順序付けされていないパケットも含まれます。任意の TCP 接続の TCP パケットの順序付けをイネーブルにする、または順序付けされている接続のキューの上限を変更するには、**queue-limit** コマンドを使用します。この機能をイネーブルにすると、順序付けされていないパケットは、転送できるようになるまでキューに保持されるか、または一定の時間が経過するまでキューに保持されます。したがって、メモリ使用量は、パケットのバッファ処理により増加します。

例

次の例は、すべての Telnet 接続の TCP パケットの順序付けをイネーブルにする方法を示しています。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# queue-limit 8
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq telnet
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class-map	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

quit

現在のコンフィギュレーション モードを終了する、または特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**quit** コマンドを使用します。

quit

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

キー シーケンス ***Ctrl+Z*** を使用しても、グローバル コンフィギュレーション（およびそれより上位の）モードを終了できます。このキー シーケンスは、特権 EXEC モードおよびユーザ EXEC モードでは機能しません。

特権 EXEC モードまたはユーザ EXEC モードで **quit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次の例は、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、セッションからログアウトする方法を示しています。

```
hostname(config)# quit
hostname# quit

Logoff
```

次の例は、**quit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後、**disable** コマンドを使用して特権 EXEC モードを終了する方法を示しています。

```
hostname(config)# quit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
exit	コンフィギュレーション モードを終了します。または、特権 EXEC モードまたはユーザ EXEC モードからログアウトします。

radius-common-pw

セキュリティ アプライアンスを経由してこの RADIUS 認可サーバにアクセスするすべてのユーザが使用する共通のパスワードを指定するには、AAA サーバ ホスト モードで **radius-common-pw** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

radius-common-pw *string*

no radius-common-pw

シンタックスの説明

string	この RADIUS サーバとのすべての認可トランザクションで共通のパスワードとして使用される最大 127 文字の英数字のキーワード。大文字と小文字は区別されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このリリースで導入されました。

使用上のガイドライン

このコマンドは、RADIUS 認可サーバに対してのみ有効です。

RADIUS 認可サーバは、接続する各ユーザのパスワードとユーザ名を要求します。セキュリティ アプライアンスは、ユーザ名を自動的に入力します。ここでユーザは、パスワードを入力します。RADIUS サーバ管理者は、このパスワードを、このセキュリティ アプライアンスを経由してサーバに権限を与える各ユーザと関連付けるように、RADIUS サーバを設定する必要があります。この情報は、RADIUS サーバ管理者に必ず提供してください。

共通のユーザ パスワードを指定しない場合、各ユーザのパスワードは、ユーザ各自のユーザ名となります。たとえば、ユーザ名が「jsmith」のユーザは、「jsmith」と入力します。ユーザ名を共通のユーザ パスワードとして使用している場合は、セキュリティ対策として、この RADIUS サーバを使用ネットワーク外で認可用に使用しないでください。

（注） このフィールドは、基本的にスペースを埋めるためのものです。RADIUS サーバは、このフィールドを予期および要求しますが、使用することはありません。ユーザは、このフィールドを知っている必要はありません。

例

次の例では、ホスト「1.2.3.4」上に「svrgrp1」という RADIUS AAA サーバ グループを設定し、タイムアウト間隔を 9 秒に、リトライ間隔を 7 秒に設定します。さらに、RADIUS 共通パスワードを「allauthpw」に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry 7
hostname(config-aaa-server-host)# radius-common-pw allauthpw
hostname(config-aaa-server-host)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

radius-with-expiry

認証中に MS-CHAPv2 を使用してユーザとパスワード アップデートをネゴシエートするようにセキュリティ アプライアンスを設定するには、トンネル グループ ipsec アトリビュート コンフィギュレーション モードで **radius-with-expiry** コマンドを使用します。RADIUS 認証が設定されていない場合、このコマンドはセキュリティ アプライアンスで無視されます。

デフォルト値に戻すには、このコマンドの ***no*** 形式を使用します。

radius-with-expiry

no radius-with-expiry

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは廃止されました。**password-management** コマンドに置き換えられました。**radius-with-expiry** コマンドの **no** 形式はサポートされなくなりました。

使用上のガイドライン

このアトリビュートは、IPSec リモートアクセス トンネル グループ タイプだけに適用できます。

例

次の例では、config-ipsec コンフィギュレーション モードで入り、remotegrp というリモートアクセス トンネル グループの radius-with-expiry を設定しています。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)# radius-with-expiry
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
password-management	パスワードの管理をイネーブルにします。トンネル グループ一般アトリビュート コンフィギュレーション モードでは、**radius-with-expiry** コマンドはこのコマンドに置き換えられます。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

rate-limit

モジュラ ポリシー フレームワークを使用するとき、一致またはクラス コンフィギュレーション モードで **rate-limit** コマンドを使用して、**match** コマンドまたはクラス マップと一致するパケットのメッセージ レートを制限します。このレート制限アクションは、アプリケーション トラフィックの検査ポリシー マップ（**policy-map type inspect** コマンド）で有効です。ただし、すべてのアプリーションでこのアクションが許可されるわけではありません。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

rate-limit *messages_per_second*

no rate-limit *messages_per_second*

シンタックスの説明

messages_per_second	秒ごとにメッセージを制限します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを特定した後（**class** コマンドは、**match** コマンドを含む、既存の **class-map type inspect** コマンドを参照します）、メッセージのレートを制限する **rate-limit** コマンドを入力できます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにします。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は検査ポリシー マップの名前です。

例

次の例では、招待要求メッセージを毎秒 100 件までに制限します。

```
hostname(config-cmap)# policy-map type inspect sip sip-map1
hostname(config-pmap-c)# match request-method invite
hostname(config-pmap-c)# rate-limit 100
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

reactivation-mode

グループ内の障害のあるサーバを再度有効にする方法を指定するには、AAA サーバ グループ モードで **reactivation-mode** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

no reactivation-mode [**depletion** [**deadtime** *minutes*] | **timed**]

シンタックスの説明

deadtime *minutes*	（オプション）グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度イネーブルにするまでの時間の長さを、0 から 1440 分までの間で指定します。デフォルトは 10 分です。
depletion	グループ内のすべてのサーバが非アクティブになった場合のみ、障害のあるサーバを再度有効にします。
timed	30 秒のダウン時間が経過した後に、障害のあるサーバを再度有効にします。

デフォルト

デフォルトの再有効化モードは depletion で、デフォルトの deadtime 値は 10 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

各サーバ グループには、グループ内のサーバの再有効化ポリシーを指定するアトリビュートがあります。

depletion モードでは、あるサーバが無効になると、グループ内の他のすべてのサーバが非アクティブになるまで、そのサーバは非アクティブのままとなります。この事態が発生した場合、グループ内のすべてのサーバは再有効化されます。この方法で、障害のあるサーバが原因の接続遅延の発生が最小限に抑えられます。***depletion*** モードを使用している場合は、***deadtime*** パラメータも指定できます。***deadtime*** パラメータは、グループ内の最後のサーバをディセーブルにしてから、すべてのサーバを再度イネーブルにするまでの時間の長さ（分）を指定します。このパラメータは、サーバ グループがローカル フォールバック機能と連動して使用されている場合に限り、意味を持ちます。

timed モードでは、障害のあるサーバは、30 秒のダウン時間が経過した後に再有効化されます。これは、サーバ リスト内の最初のサーバをプライマリ サーバとして使用していて、可能な場合は常にそのサーバがオンラインであることが望ましい場合に役立ちます。このポリシーは、UDP サーバの場合は機能しません。UDP サーバへの接続は、たとえそのサーバが存在しない場合でも失敗しないため、UDP サーバは無条件にオンラインに戻ります。このモードでは、サーバ リストに到達不能なサーバが複数含まれている場合に、接続時間が長くなったり、接続が失敗したりする可能性があります。

同時アカウンティングがイネーブルになっているアカウンティング サーバ グループには、強制的に ***timed*** モードが適用されます。これは、所定のリスト内のすべてのサーバが同等であることを意味します。

例

次の例では、depletion 再有効化モードを使用するように、「srvgrp1」という aTACACS+ AAA サーバを設定します。deadtime は 15 分に設定します。

```
hostname(config)# aaa-server svrgrp1 protocol tacacs+
hostname(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
hostname(config-aaa-server)# exit
hostname(config)#
```

次の例では、timed 再有効化モードを使用するように、「srvgrp1」という aTACACS+ AAA サーバを設定します。

```
hostname(config)# aaa-server svrgrp2 protocol tacacs+
hostname(config-aaa-server)# reactivation-mode timed
hostname(config-aaa-server)#
```

関連コマンド

accounting-mode	アカウンティング メッセージを 1 つのサーバに送信するか、グループ内のすべてのサーバに送信するかを指定します。
aaa-server protocol	AAA サーバ グループ コンフィギュレーション モードに入って、グループ内のすべてのホストに共通する、グループ固有の AAA パラメータを設定できるようにします。
max-failed-attempts	サーバ グループ内の所定のサーバが無効になるまでに、そのサーバで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

redistribute（OSPF）

あるルーティング ドメインから OSPF ルーティング ドメインにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | **rip** | ***static*** | ***connected***} [***metric*** *metric_value*] [***metric-type*** *metric_type*] [***route-map*** *map_name*] [***tag*** *tag_value*] [***subnets***]

no redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | ***rip*** | ***static*** | ***connected***} [***metric*** *metric_value*] [***metric-type*** *metric_type*] [***route-map*** *map_name*] [***tag*** *tag_value*] [***subnets***]

シンタックスの説明

connected	インターフェイスに接続されているネットワークを OSPF ルーティング プロセスに再配布することを指定します。
external *type*	指定した自律システムの外部の OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システム内部の OSPF メトリック ルートを指定します。
match	（オプション）あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を指定します。
metric *metric_value*	（オプション）OSPF デフォルト メトリック値を指定します（0 ～ 16777214）。
metric-type *metric_type*	（オプション）OSPF ルーティング ドメインにアドバタイズされる、デフォルト ルートに関連付けられた外部リンク タイプ。2 つの値、つまり ***1***（タイプ 1 外部ルート）または ***2***（タイプ 2 外部ルート）のいずれかを使用できます。
nssa-external *type*	NSSA への外部のルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	OSPF ルーティング プロセスを現在の OSPF ルーティング プロセスに再配布するために使用されます。*pid* には、OSPF ルーティング プロセス用に内部的に使用される識別パラメータを指定します。有効な値は、1 ～ 65535 です。
rip	ネットワークを RIP ルーティング プロセスから現在の OSPF ルーティング プロセスに再配布するように指定します。
route-map *map_name*	（オプション）ソース ルーティング プロトコルから現在の OSPF ルーティング プロトコルへインポートされたルートをフィルタリングするために使用されるルート マップの名前です。指定しない場合、すべてのルートが再配布されます。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。
subnets	（オプション）ルートを OSPF に再配布する場合に、指定プロトコルの再配布を確認します。使用しない場合、クラスフル ルートだけが再配布されます。
tag *tag_value*	（オプション）各外部ルートに対応付けられた 32 ビットの 10 進値。この値は、OSPF 自体によって使用されることはありません。ASBR 間で情報を交換するために使用されます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効な値は 0 ～ 4294967295 です。

デフォルト

コマンドのデフォルト値は、次のとおりです。

- ***metric*** *metric-value*：0
- ***metric-type*** *type-value*：***2***
- ***match***：***Internal***、***external 1***、***external 2***
- ***tag*** *tag-value*：0

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	このコマンドが、***rip*** キーワードを含めるように修正されました。

例

次の例は、スタティック ルートを現在の OSPF プロセスに再配布する方法を示しています。

```
hostname(config)# router ospf 1
hostname(config-router)# redistribute static
```

関連コマンド

コマンド	説明
redistribute（RIP）	ルートを RIP ルーティング プロセスへ再配布します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

redistribute（RIP）

別のルーティング ドメインから RIP ルーティング プロセスにルートを再配布するには、ルータ コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | ***static*** | ***connected***} [***metric*** {*metric_value* | ***transparent***}] [***route-map*** *map_name*]

no redistribute {{***ospf*** *pid* [***match*** {***internal*** | ***external*** [***1*** | ***2***] | ***nssa-external*** [***1*** | ***2***]}]} | ***static*** | ***connected***} [***metric*** {*metric_value* | ***transparent***}] [***route-map*** *map_name*]

シンタックスの説明

connected	インターフェイスに接続されているネットワークを RIP ルーティング プロセスに再配布することを指定します。
external *type*	指定した自律システムの外部の OSPF メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システム内部の OSPF メトリック ルートを指定します。
match	（オプション）OSPF から RIP へルートを再配布するための条件を指定します。
metric {*metric_value* | ***transparent***}	（オプション）再配布されるルートの RIP メトリック値を指定します。*metric_value* として有効な値は 0 から 16 です。メトリックを ***transparent*** に設定すると、現在のルート メトリックが使用されます。
nssa-external *type*	not-so-stubby area（NSSA; 準スタブ エリア）外部のルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	OSPF ルーティング プロセスを RIP ルーティング プロセスに再配布するために使用されます。*pid* には、OSPF ルーティング プロセス用に内部的に使用される識別パラメータを指定します。有効な値は、1 ～ 65535 です。
route-map *map_name*	（オプション）ソース ルーティング プロセスから RIP ルーティング プロセスへインポートされたルートをフィルタリングするために使用されるルート マップの名前です。指定しない場合、すべてのルートが再配布されます。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。

デフォルト

コマンドのデフォルト値は、次のとおりです。

- ***metric*** *metric-value*：0
- ***match***：***Internal***、***external 1***、***external 2***

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、スタティック ルートを現在の RIP プロセスに再配布する方法を示しています。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# redistribute static metric 2
```

関連コマンド

コマンド	説明
redistribute（OSPF）	他のルーティング ドメインから OSPF へルートを再配布します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードに入ります。
show running-config router	グローバル ルータ コンフィギュレーション内のコマンドを表示します。

regex

テキストを照合するための正規表現を作成するには、グローバル コンフィギュレーション モードで **regex** コマンドを使用します。正規表現を削除するには、このコマンドの **no** 形式を使用します。

regex *name regular_expression*

no regex *name* [*regular_expression*]

シンタックスの説明

name	最大 40 文字の正規表現名を指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現に使用できるメタ文字のリストについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

regex コマンドは、テキストの照合が必要なさまざまな機能に使用できます。たとえば、モジュラ ポリシー フレームワークで*検査ポリシー マップ*を使用してアプリケーション検査に対する特殊なアクションを設定できます（**policy map type inspect** コマンドを参照）。検査ポリシー マップでは、1 つ以上の **match** コマンドを含んだ検査クラス マップを作成することで、アクションの実行対象となるトラフィックを指定できます。または、**match** コマンドを検査ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケットに含まれているテキストを正規表現を使用して識別できます。たとえば、HTTP パケットに含まれている URL 文字列と一致するかどうかを確認できます。正規表現クラス マップ内で正規表現をグループ化できます（**class-map type regex** コマンドを参照）。

正規表現では、完全に文字列と一致するようにテキスト文字列を照合するか、*メタ文字*を使用してテキスト文字列のさまざまな形を照合できます。特定のアプリケーション トラフィックの内容を照合するために正規表現を使用できます。たとえば、HTTP パケット内の本文を照合できます。

表 23-1 は、特殊な意味を持つメタ文字のリストです。

表 23-1　regex のメタ文字

文字	説明	注意事項
.	ドット	任意の 1 文字と一致します。たとえば、**d.g** は dog、dag、dtg、および doggonnit などの文字を含むすべての文字と一致します。
(*exp***)**	部分正規表現	部分正規表現によって文字を前後の文字と区別します。部分正規表現には他のメタ文字を使用できます。たとえば、**d(o|a)g** は dog と dag に一致しますが、**do|ag** は do と ag に一致します。また、部分正規表現は繰り返しを意味する文字を区別するために、繰り返し限定作用素と共に使用できます。たとえば、**ab(xy){3}z** は abxyxyxyz に一致します。
|	代用	この記号によって区切られた表現の一方と一致します。たとえば、**dog|cat** は dog または cat と一致します。
?	疑問符	直前の文字が含まれない場合と 1 つ含まれる場合があることを示す限定作用素です。たとえば、**lo?se** は、lse または lose と一致します。 **(注)** **Ctrl+V** キーを入力して疑問符を入力する必要があります。そうしないと、ヘルプ機能が起動されます。
*	アスタリスク	直前の文字が含まれない、1 つ含まれる、繰り返し含まれる場合があることを示す限定作用素です。たとえば、**lo*se** は lse、lose、loose などと一致します。
+	プラス記号	直前の文字が 1 つ以上含まれることを示す限定作用素です。たとえば、**lo+se** は lose と loose に一致しますが、lse とは一致しません。
{*x***}**	繰り返し限定作用素	表現が *x* 回、完全に繰り返された文字と一致します。たとえば、**ab(xy){3}z** は abxyxyxyz に一致します。
{*x***,}**	最小繰り返し限定作用素	表現が最低限 *x* 回繰り返された文字と一致します。たとえば、**ab(xy){2,}z** は abxyxyz、abxyxyxyz に一致します。
[*abc***]**	文字クラス	括弧内の任意の文字と一致します。たとえば、**[abc]** は a、b、または c と一致します。
[^*abc***]**	否定文字クラス	括弧内に含まれていない 1 つの文字と一致します。たとえば、**[^abc]** は a、b、または c 以外の 1 文字と一致します。**[^A-Z]** は大文字でない 1 文字と一致します。
[*a-c***]**	文字の範囲クラス	指定の範囲内の任意の文字と一致します。**[a-z]** は任意の小文字と一致します。文字と範囲を組み合せることができます。**[abcq-z]** は a、b、c、q、r、s、t、u、v、w、x、y、z と一致し、[**a-cq-z**] も同様です。 ダッシュ（-）記号は、括弧内の最後または最初の文字である場合にのみダッシュとして判断されます。たとえば、**[abc-]** または **[-abc]** などです。
""	引用符	文字列内の末尾と先頭に空いたスペースを保持します。たとえば、**" test"** と指定すると、照合時に先頭のスペースが保持されます。
^	キャレット	行頭を指定します。

表 23-1　regex のメタ文字（続き）

文字	説明	注意事項
\	エスケープ文字	メタ文字と共に使用した場合、表記どおりの文字と一致します。たとえば、**\[** は左角括弧（[）と一致します。
char	文字	文字がメタ文字でない場合、表記どおりの文字と一致します。
\r	キャリッジ リターン	キャリッジ リターン n 0x0d と一致します。
\n	改行	新行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	改ページ 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（2 桁）を使用する ASCII 文字と一致します。
NNN	エスケープされた 8 進数	ASCII 文字を 8 進数（3 桁）として照合します。たとえば、040 はスペースを表します。

一致させる対象の文字と完全に一致するかどうか正規表現をテストするには、**test regex** コマンドを入力します。

正規表現のパフォーマンスへの影響は、2 つの主要な要因によって決定されます。

- 正規表現を使用して検索するために必要なテキストの長さ。
  正規表現エンジンは、検索テキストが短い場合、セキュリティ アプライアンスのパフォーマンスにあまり影響を与えません。
- 正規表現を使用して検索するために必要な正規表現関連テーブルの数。

検索テキストの長さがパフォーマンスに与える影響

正規表現を使用した検索を設定する場合、検索するテキストのすべてのバイトは通常、正規表現データベースと照合され、一致する表現が検出されます。検索するテキストの長さに比例して検索時間も長くなります。この検索時間の変化を説明したパフォーマンス テスト ケースを次に示します。

- ある HTTP トランザクションには、300 バイト長の GET 要求と 3250 バイト長の応答が含まれる。
- URI の検索の正規表現が 445 件、要求本文検索の正規表現が 34 件。
- 応答本文検索の正規表現が 55 件。

HTTP GET 要求のみの URI と本文を検索するようポリシーが設定されると、スループットは次のようになります。

- 該当する正規表現データベースが検索されない場合は 420 mbps。
- 該当する正規表現データベースが検索された場合は 413 mbps（これは正規表現利用時のオーバーヘッドが比較的小さいことを示しています）。

しかし、HTTP 応答本文全体も検索するようにポリシーが設定されている場合は、長い応答本文（3250 バイト）を検索することになるので、スループットは 145 mbps に落ちます。

正規表現を使用した検索のテキストの長さが長くなる要因について次に示します。

- 正規表現を使用した検索は複数のさまざまなプロトコル フィールドで設定されます。たとえば、HTTP 検査では、URI だけが正規表現検索用に設定され、URI フィールドだけが正規表現検索の対象となる場合、検索テキストの長さは URI の長さに制限されます。ただし、ヘッダー、本文などの他のプロトコル フィールドも正規表現検索用に設定されている場合、ヘッダーと本文の長さを含めるために検索テキストの長さは長くなります。

- 検索対象のフィールドは長くなります。たとえば、URI が正規表現検索用に設定されると、GET 要求での長い URI の検索は長くなります。また、現在、HTTP 本文の長さは、デフォルトで 200 バイトまでに制限されています。ただし、本文を検索するようポリシーが設定され、本文検索テキストの長さが 5000 バイトに変更された場合、本文検索が長くなるためパフォーマンスに重大な影響が生じます。

関連する正規表現テーブルの数がパフォーマンスに与える影響

現在、URI のすべての正規表現など、同じプロトコル フィールドに設定されているすべての正規表現は、1 つまたは複数の正規表現関連テーブルから構成されるデータベースに保存されます。テーブルの数は、テーブルの構築時に必要なメモリの総容量とメモリの可用性により決定します。正規表現データベースは、次の条件に基づいて、複数のテーブルに分割されます。

- テーブルの最大サイズが 32 MB に制限されているために、必須メモリ総容量が 32 MB 以上であること。
- 隣接する最大メモリが完全な正規表現データベースの構築に不足している場合、サイズの小さい複数のテーブルが構築され、すべての正規表現を収容します。メモリのフラグメンテーションの程度は、相互に影響し合う多くの要因に応じて異なり、フラグメンテーションのレベルを予想することはできません。

複数の関連テーブルでは、各テーブルは正規表現を使用した検索で必ず対象となるので、検索時間は対象テーブルの数に比例して長くなります。

特定のタイプの正規表現は、テーブルのサイズを非常に大きくする傾向があります。ワイルドカードや繰り返しの使用を可能なかぎり避ける方法で正規表現を設計することを検討してください。次のメタ文字の説明については、表 23-1 を参照してください。

- ワイルドカードを使用した正規表現：
  - ドット（.）
- あるクラスの任意の文字と一致するさまざまな文字クラス：
  - [^a-z]
  - [a-z]
  - [abc]]
- 繰り返しを使用した正規表現：
  - *
  - +
  - {n,}
- ワイルドカードと繰り返しを組み合せた正規表現は、テーブルのサイズを劇的に増加させる可能性があります。例：
  - 123.*xyz
  - 123.+xyz
  - [^a-z]+
  - [^a-z]*
  - .*123.*（これは "123" の照合と同じなので実行されません）

次の例では、ワイルドカードと繰り返しの有無に応じて正規表現のメモリ消費量がどのように変化するかを示します。

- 次の 4 つの正規表現のデータベース サイズは、958,464 バイトです。

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

- 次の 4 つの正規表現のデータベース サイズは、10240 バイトだけです。

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

正規表現の数が多いと正規表現データベースに必要とされるメモリ総容量が増えるので、メモリが断片化されるとテーブルの数が増える可能性が高くなります。正規表現の数の変化に応じたメモリ消費量の例を次に示します。

- 100 個の URI をサンプリング：3,079,168 バイト
- 200 個の URI をサンプリング：7,156,224 バイト
- 500 個の URI をサンプリング：11,198,971 バイト

（注） コンテキストごとの正規表現の最大数は 2048 です。

debug menu regex 40 10 コマンドを使用して、各 regex データベースに関連テーブルがいくつあるかを表示できます。

例

次の例では、検査ポリシー マップで使用する 2 つの正規表現を作成します。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックに一致するかどうかを調べるための検査クラス マップを作成します。
policy-map	トラフィック クラスを 1 つまたは複数のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
test regex	正規表現をテストします。

reload

コンフィギュレーションをリブートおよびリロードするには、特権 EXEC モードで **reload** コマンドを使用します。

reload [**at** *hh*:*mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh*:]*mm*] [**max-hold-time** [*hh*:]*mm*] [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

シンタックスの説明

at *hh*:*mm*	（オプション）指定された時刻（24 時間方式のクロックを使用）で実行するように、ソフトウェアのリロードをスケジューリングします。月日を指定しなかった場合、リロードは当日の指定された時刻（指定された時刻が現在の時刻よりあとの場合）または翌日（指定された時刻が現在の時刻より前の場合）に実行されます。00:00 を指定すると、リロードは午前 0 時にスケジューリングされます。リロードは 24 時間以内に実行する必要があります。
cancel	（オプション）スケジューリングされたリロードをキャンセルします。
day	（オプション）日付の番号を指定します。範囲は 1 ～ 31 です。
in [*hh*:]*mm*]	（オプション）指定された時刻（分または時と分）に有効になるように、ソフトウェアのリロードをスケジューリングします。リロードは 24 時間以内に実行する必要があります。
max-hold-time [*hh*:]*mm*	（オプション）シャットダウンまたはリブートの前に、セキュリティ アプライアンスが他のサブシステムに通知するまで待機する最小待機期間を指定します。この時間が経過すると、クイック（強制）シャットダウンまたはリブートが実行されます。
month	（オプション）月名を指定します。月名を表す一意の文字列を作成するため、十分な文字を入力します。たとえば、「Ju」は「June」または「July」を表す可能性があるため一意ではありませんが、「Jul」と入力すれば、正確にこれらの 3 文字で始まる月は他にないので一意になります。
noconfirm	（オプション）ユーザによる確認がないセキュリティ アプライアンスのリロードを許可します。
quick	（オプション）通知したり、すべてのサブシステムを正常にシャットダウンしたりすることなく、クイック リロードを強制します。
reason *text*	（オプション）リロードの理由を 1 ～ 255 文字で指定します。理由テキストは、すべての IPSec VPN クライアント、端末、Tenet、SSH、および ASDM の接続またはセッションに送信されます。 **（注）** isakmp などの一部のアプリケーションで、IPSec VPN クライアントに理由テキストを送信するには、追加コンフィギュレーションが必要です。詳細については、ソフトウェア コンフィギュレーション マニュアルの適切な項を参照してください。
save-config	（オプション）シャットダウンする前に、実行コンフィギュレーションをメモリに保存します。***save-config*** キーワードを入力しない場合、コンフィギュレーションに対する未保存の変更はすべて、リロード後に失われます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、次の新しい引数およびキーワードを追加するために修正されました。*day*、*hh*、*mm*、*month*、***quick***、***save-config***、および *text*。

使用上のガイドライン　このコマンドを使用すると、セキュリティ アプライアンスをリブートし、コンフィギュレーションをフラッシュからリロードできます。

デフォルトでは、**reload** コマンドは対話型です。セキュリティ アプライアンスは、コンフィギュレーションが修正されていないかどうかを最初にチェックしますが、保存はしません。その場合、セキュリティ アプライアンスは、コンフィギュレーションを保存するためのプロンプトを表示します。マルチ コンテキスト モードでは、セキュリティ アプライアンスは、保存されていないコンフィギュレーションがあるコンテキストごとにプロンプトを表示します。***save-config*** パラメータを指定すると、プロンプトが表示されることなくコンフィギュレーションが保存されます。その場合、セキュリティ アプライアンスは、システムをリロードしてよいか確認するプロンプトを表示します。***y*** と応答するか、***Enter*** キーを押した場合のみ、リロードが開始されます。確認後、セキュリティ アプライアンスは、リロード プロセスを開始するか、スケジューリングします。どちらが実行されるかは、遅延パラメータ（***in*** または ***at***）の指定によって異なります。

デフォルトでは、リロード プロセスは「グレースフル」（「ナイス」とも呼ばれる）モードで動作します。リブートが実行される直前に、登録されているすべてのサブシステムには通知が行われます。この通知により、サブシステムはリブート前に正常にシャットダウンできます。このようなシャットダウンが実行されるまで待つことを避けるには、***max-hold-time*** パラメータで最大待ち時間を指定します。別の方法として、***quick*** パラメータを使用することでも、影響を受けるサブシステムに通知したり、グレースフル シャットダウンを待機したりすることなく、リロード プロセスを強制的に開始できます。

noconfirm パラメータを指定すると、**reload** コマンドの動作を強制的に非対話型にすることができます。この場合、***save-config*** パラメータが指定されていない限り、セキュリティ アプライアンスは、保存されていないコンフィギュレーションをチェックしません。セキュリティ アプライアンスは、システムをリブートする前に確認のプロンプトをユーザに表示しません。遅延パラメータを設定していない場合は、リロード プロセスはすぐに開始またはスケジューリングされます。ただし、***max-hold-time*** パラメータまたは ***quick*** パラメータを指定して、動作またはリロード プロセスを制御することはできます。

スケジューリングされたリロードをキャンセルするには、**reload cancel** を使用します。すでに進行中のリロードは、キャンセルできません。

（注）　フラッシュ パーティションに書き込まれていないコンフィギュレーションの変更は、リロードすると失われます。リブートする前に、**write memory** コマンドを入力して、現在のコンフィギュレーションをフラッシュ パーティションに保存してください。

例

次の例は、コンフィギュレーションをリブートおよびリロードする方法を示しています。

```
hostname# reload
Proceed with ?  [confirm] y

Rebooting...

XXX Bios VX.X
...
```

関連コマンド

コマンド	説明
show reload	セキュリティ アプライアンスのリロード ステータスを表示します。

remote-access threshold session-threshold-exceeded

しきい値を設定するには、グローバル コンフィギュレーション モードで **remote-access threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、アクティブなリモートアクセス セッションの数を指定します。この数に達した時点で、セキュリティ アプライアンスはトラップを送信します。

remote-access threshold session-threshold-exceeded {*threshold-value*}

no **remote-access threshold session-threshold-exceeded**

シンタックスの説明

threshold-value	セキュリティ アプライアンスがサポートしているセッション上限以下の整数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1) (1)	このコマンドが導入されました。

使用上のガイドライン

例

次の例は、しきい値として 1500 を設定する方法を示しています。

```
hostname# remote-access threshold session-threshold-exceeded 1500
```

関連コマンド

コマンド	説明
snmp-server enable trap remote-access	しきい値のトラッピングをイネーブルにします。

rename

コピー元ファイル名からコピー先ファイル名に、ファイルまたはディレクトリの名前を変更するには、特権 EXEC モードで **rename** コマンドを使用します。

rename ***[/noconfirm]*** ***[*****flash:*****]*** *source-path* **[flash:]** *destination-path*

シンタックスの説明

/noconfirm	（オプション）確認プロンプトを表示しないようにします。
destination-path	コピー先ファイルのパスを指定します。
flash:	（オプション）内蔵フラッシュ メモリを指定し、続けてコロン（:）を入力します。
source-path	コピー元ファイルのパスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

rename flash: flash: コマンドは、コピー元とコピー先のファイル名を入力するためのプロンプトを表示します。

ファイル システム全体で、ファイルまたはディレクトリの名前を変更することはできません。

次の例を参考にしてください。

```
hostname# rename flash: disk1:
Source filename []? new-config
Destination filename []? old-config
%Cannot rename between filesystems
```

例

次の例は、「test」という名前のファイルを「test1」に変更する方法を示しています。

```
hostname# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

関連コマンド

コマンド	説明
mkdir	新しいディレクトリを作成します。
rmdir	ディレクトリを削除します。
show file	ファイル システムに関する情報を表示します。

rename（クラス マップ）

クラス マップの名前を変更するには、クラス マップ コンフィギュレーション モードで **rename** コマンドを入力します。

rename *new_name*

シンタックスの説明

new_name	クラス マップの新しい名前の最大長は 40 文字です。class-default という名前は予約されています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、test から test2 にクラス マップ名を変更する方法を示します。

```
hostname(config)# class-map test
hostname(config-cmap)# rename test2
```

関連コマンド

コマンド	説明
class-map	クラス マップを作成します。

replication http

フェールオーバー グループの HTTP 接続の複製をイネーブルにするには、フェールオーバー グループ コンフィギュレーション モードで **replication http** コマンドを使用します。HTTP 接続の複製をディセーブルにするには、このコマンドの **no** 形式を使用します。

replication http

no replication http

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

ディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、HTTP クライアントは接続試行が失敗すると通常はリトライするため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**replication http** コマンドは、ステートフル フェールオーバー環境で HTTP セッションのステートフル複製をイネーブルにしますが、システム パフォーマンスには悪影響を与える可能性があります。

このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。このコマンドは、Active/Active フェールオーバー コンフィギュレーションのフェールオーバー グループを除く、Active/Standby フェールオーバーに対して **failover replication http** コマンドと同じ機能を提供します。

例

次の例は、フェールオーバー グループに対して適用可能なコンフィギュレーションを示しています。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# replication http
hostname(config-fover-group)# exit
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover replication http	HTTP 接続を複製するように、ステートフル フェールオーバーを設定します。

request-command deny

FTP 要求内で特定のコマンドを禁止するには、FTP マップ コンフィギュレーション モードで **request-command deny** コマンドを使用します。このモードには、**ftp-map** コマンドを使用してアクセスできます。コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }

no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

シンタックスの説明

appe	ファイルに対して付加を実行するコマンドを禁止します。
cdup	現在の作業ファイルの親ディレクトリに変更を加えるコマンドを禁止します。
dele	サーバ上のファイルを削除するコマンドを禁止します。
get	サーバからファイルを取得するクライアント コマンドを禁止します。
help	ヘルプ情報を提供するコマンドを禁止します。
mkd	サーバ上にディレクトリを作成するコマンドを禁止します。
put	サーバにファイルを送信するクライアント コマンドを禁止します。
rmd	サーバ上のディレクトリを削除するコマンドを禁止します。
rnfr	元のファイル名からの名前変更を指定するコマンドを禁止します。
rnto	新しいファイル名への名前変更を指定するコマンドを禁止します。
site	サーバ システム固有のコマンドを禁止します。通常は、リモート管理で使用されます。
stou	一意のファイル名を使用しているファイルを保存するコマンドを禁止します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
FTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドは、厳密な FTP 検査を使用するときに、セキュリティ アプライアンスを通過する FTP 要求内で許可されるコマンドを制御するために使用します。

例　次の例では、**stor** コマンド、**stou** コマンド、または **appe** コマンドが含まれている FTP 要求をドロップするように、セキュリティ アプライアンスを設定します。

```
hostname(config)# ftp-map inbound_ftp
hostname(config-ftp-map)# request-command deny put stou appe
hostname(config-ftp-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション検査用に特定の FTP マップを適用します。
mask-syst-reply	FTP サーバ応答をクライアントから見えないようにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

request-data-size

SLA オペレーション要求パケットのペイロードのサイズを設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **request-data-size** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

request-data-size *bytes*

no request-data-size

シンタックスの説明

bytes	要求パケット ペイロードのサイズ（バイト単位）。有効な値は 0 ～ 16384 です。最小値は、使用するプロトコルにより異なります。エコー タイプの場合、最小値は 28 バイトです。この値は、プロトコルまたは PMTU で許可されている最大値より大きい値に設定しないでください。

（注） セキュリティ アプライアンスは、8 バイトのタイムスタンプをペイロードに追加します。このため、実際のペイロードは *bytes* + 8 になります。

デフォルト

デフォルトのバイトは 28 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

到達可能性については、ソースとターゲット間での PMTU の変化を検出するため、デフォルトのデータ サイズを増やさなければならない場合があります。PMTU が低いとセッションのパフォーマンスに影響を与える傾向があります。低い PMTU が検出された場合、2 番目のパスが使用されることを示している可能性があります。

例

次の例では、ICMP エコー要求 / 応答時間プローブ オペレーションを使用する、ID が 123 の SLA オペレーションを設定しています。エコー要求パケットのペイロード サイズを 48 バイト、SLA オペレーション中に送信されるエコー要求の数を 5 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA オペレーション中に送信する要求パケットの数を指定します。
sla monitor	SLA 監視オペレーションを定義します。
type echo	SLA オペレーションをエコー応答時間プローブ オペレーションとして設定します。

request-method

HTTP 要求メソッドに基づいて HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **request-method** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

request-method {{ **ext** *ext_methods* | **default**} | { **rfc** *rfc_methods* | **default**}} **action** {**allow** | **reset** | **drop**} [**log**]

no request-method { **ext** *ext_methods* | **rfc** *rfc_methods* } **action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクションを指定します。
allow	メッセージを許可します。
default	サポートされている要求メソッドがトラフィックに含まれていて、そのメソッドが設定済みリストに記載されていない場合に、セキュリティ アプライアンスが実行するデフォルト アクションを指定します。
drop	接続を終了します。
ext	拡張メソッドを指定します。
ext-methods	セキュリティ アプライアンスを通過することを許可する拡張メソッドの 1 つを指定します。
log	（オプション）syslog を生成します。
reset	TCP リセット メッセージをクライアントまたはサーバに送信します。
rfc	RFC 2616 でサポートされているメソッドを指定します。
rfc-methods	セキュリティ アプライアンスを通過することを許可する RFC メソッドの 1 つを指定します（表 23-2 を参照）。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。このコマンドがイネーブルで、サポートされている要求メソッドが指定されていない場合、デフォルト アクションでは、ロギングなしで接続が許可されます。デフォルト アクションを変更するには、**default** キーワードを使用して別のデフォルト アクションを指定します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

request-method コマンドをイネーブルにすると、セキュリティ アプライアンスは、サポートおよび設定されている各要求メソッドの HTTP 接続に対して、指定されているアクションを適用します。

セキュリティ アプライアンスは、設定済みリストにある要求メソッドに一致しないすべてのトラフィックに対して、**default** アクションを適用します。**default** アクションでは、接続をロギングなしで **allow** します。事前設定済みのデフォルト アクションでは、**drop** および **log** というアクションを持つ 1 つまたは複数の要求メソッドを指定すると、セキュリティ アプライアンスは、設定済み要求メソッドが含まれている接続をドロップし、各接続をロギングし、サポートされているその他の要求メソッドが含まれているすべての接続を許可します。

より厳しいポリシーを設定する場合は、デフォルト アクションを **drop**（または **reset**）および **log** に変更します（イベントをログに記録する場合）。その後、**allow** アクションで、許可する各メソッドを設定します。

適用する設定ごとに 1 回、**request-method** コマンドを入力します。**request-method** コマンドのインスタンスを、デフォルト アクションを変更するために 1 つ、設定済みメソッドのリストに 1 つの要求メソッドを追加するために 1 つ使用します。

このコマンドの **no** 形式を使用して、要求メソッドを設定済みメソッドのリストから削除する場合、コマンドラインで要求メソッド キーワードの後にある文字はすべて無視されます。

RFC 2616 で定義されているメソッドで、設定済みメソッドのリストに追加できるものを表 23-2 に示します。

表 23-2　RFC 2616 メソッド

メソッド	説明
connect	トンネルに動的に切り替わることが可能なプロキシ（例、SSL トンネリング）と共に使用されます。
delete	Request-URI によって識別されたリソースをオリジン サーバが削除することを要求します。
get	Request-URI によって識別された情報またはオブジェクトをすべて取得します。
head	サーバが応答でメッセージ本文を返さないこと以外は、GET と同じです。
options	Request-URI によって識別されたサーバで使用できる、通信オプションについての情報の要求を表します。
post	要求に含まれているオブジェクトを、Request-Line 内の Request-URI によって識別されたリソースの新しい下位リソースとしてオリジン サーバが受け入れることを要求します。
put	含まれているオブジェクトを指定した Request-URI の下に保存することを要求します。
trace	リモートのアプリケーション層の要求メッセージのループバックを起動します。

例

次の例では、事前設定済みのデフォルトを使用して、緩やかなポリシーを指定しています。サポートされているすべての要求メソッドを、個別に拒否されていない限り許可します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc options drop log
hostname(config-http-map)# request-method rfc post drop log
hostname(config-http-map)
```

この例では、**options** 要求メソッドおよび **post** 要求メソッドだけがドロップされ、イベントが記録されます。

次の例では、厳しいポリシーを設定します。デフォルト アクションは、個別に許可されていないすべての要求メソッドの接続を **reset** し、イベントを **log** するように変更されています。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# request-method rfc default action reset log
hostname(config-http-map)# request-method rfc get allow
hostname(config-http-map)# request-method rfc put allow
hostname(config-http-map)#
```

この場合、**get** 要求メソッドおよび **put** 要求メソッドが許可されます。その他のメソッドを使用するトラフィックが検出された場合、セキュリティ アプライアンスは接続をリセットし、syslog エントリを作成します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

request-queue

応答待ちでキュー入れられる GTP 要求の最大数を指定するには、GTP マップ コンフィギュレーション モードで **request-queue** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスできます。この数をデフォルトの 200 に戻すには、このコマンドの **no** 形式を使用します。

request-queue *max_requests*

no request-queue *max_requests*

シンタックスの説明

max_requests	応答待ちでキューに入れられる GTP 要求の最大数。範囲は、1 ～ 4,294,967,295 です。

デフォルト

max_requests のデフォルトは 200 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

gtp request-queue コマンドは、応答待ちでキューに入れられる GTP 要求の最大数を指定します。限度に到達していて新しい要求が着信すると、最も長時間キューに入っている要求が削除されます。Error Indication、Version Not Supported、および SGSN Context Acknowledge の各メッセージは要求と見なされないため、応答を待つために要求キューに入れられることはありません。

例

次の例では、要求キューの最大サイズを 300 バイトに指定します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# request-queue-size 300
hostname(config-gtpmap)#
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

request-timeout

失敗した SSO 認証の試行がタイムアウトになるまでの秒数を設定するには、webvpn-sso-siteminder コンフィギュレーション モードで **request-timeout** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

request-timeout *seconds*

no request-timeout

シンタックスの説明

seconds	失敗した SSO 認証試行がタイムアウトになるまでの秒数です。範囲は 1 ～ 30 秒です。端数はサポートされていません。

デフォルト

デフォルトでは、このコマンドの値は 5 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn-sso-siteminder コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。現在、セキュリティ アプライアンスは、Computer Associates の eTrust SiteMinder SSO サーバ（以前の Netegrity SiteMinder）をサポートしています。

セキュリティ アプライアンスが SSO 認証をサポートするように設定したら、次の 2 つのタイムアウト パラメータをオプションで調整できます。

- 失敗した SSO 認証試行がタイムアウトになるまでの秒数。これには **request-timeout** コマンドを使用します。
- セキュリティ アプライアンスが失敗した SSO 認証を再試行する回数（**max-retry-attempts** コマンドを参照）。

例

webvpn-sso-siteminder コンフィギュレーション モードで入力された次の例では、SiteMinder SSO サーバ「example」の認証タイムアウトを 10 秒に設定しています。

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# request-timeout 10
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
test sso-server	テスト認証要求で SSO サーバをテストします。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

reserved-bits

TCP ヘッダーの予約済みビットを消去するには、または、予約済みビットが設定されたパケットをドロップするには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

reserved-bits {**allow** | **clear** | **drop**}

no reserved-bits {**allow** | **clear** | **drop**}

シンタックスの説明

allow	TCP ヘッダー内に予約済みビットを持つパケットを許可します。
clear	TCP ヘッダー内の予約済みビットを消去してから、そのパケットを許可します。
drop	TCP ヘッダー内に予約済みビットを持つパケットをドロップします。

デフォルト

デフォルトでは、予約済みビットが許可されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。予約済みビットのあるパケットがエンド ホストで処理される方法についてのあいまいさを排除するには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。あいまいさがあると、セキュリティ アプライアンスの非同期につながる場合があります。TCP ヘッダー内の予約済みビットを消去することを選択できます。さらには、予約済みビットが設定されたパケットをドロップすることも選択できます。

例

次の例は、予約済みビットが設定されたすべての TCP フローのパケットを消去する方法を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# reserved-bits clear
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

reset

モジュラ ポリシー フレームワークを使用する場合、パケットをドロップして接続を終了し、一致またはクラス コンフィギュレーション モードで **reset** コマンドを使用して、**match** コマンドまたはクラス マップと一致するトラフィックに対して TCP のリセットを送信します。このリセット アクションは、アプリケーション トラフィックの検査ポリシー マップ（**policy-map type inspect** コマンド）で有効です。このアクションをディセーブルにするには、このコマンドの **no** 形式を使用します。

reset [**log**]

no reset [**log**]

シンタックスの説明

log	一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

検査ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。検査ポリシー マップで使用できるコマンド自体は、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを特定した後（**class** コマンドは、**match** コマンドを含む、既存の **class-map type inspect** コマンドを参照します）、**reset** コマンドを入力してパケットをドロップし、**match** コマンドまたは **class** コマンドと一致するトラフィックの接続を終了します。

接続をリセットすると、検査ポリシー マップのそれ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** コマンドまたは **class** コマンドとは一致しません。最初のアクションがパケットのロギングである場合は、接続のリセットなどの 2 番目のアクションが発生する可能性があります。同じ **match** または **class** コマンドに対して、**reset** と **log** アクションを両方を設定できます。その場合、パケットは、指定の一致によってリセットされるまでロギングされます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション検査をイネーブルにするときは、このアクションを含んでいる検査ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は検査ポリシー マップの名前です。

例

次の例では、接続をリセットして、http-traffic クラス マップと一致するとログを送信します。同じパケットが 2 番目の **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
hostname(config-cmap)# policy-map type inspect http http-map1
hostname(config-pmap)# class http-traffic
hostname(config-pmap-c)# reset log
hostname(config-pmap-c)# match req-resp content-type mismatch
hostname(config-pmap-c)# reset log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

retries

セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

retries *number*

no retries [*number*]

シンタックスの説明

number	再試行の回数を 0 ～ 10 の間で指定します。デフォルトは 2 です。

デフォルト

デフォルトでは、再試行の回数は 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

name-server コマンドを使用して DNS サーバを追加します。

dns name-server コマンドは、このコマンドに置き換えられます。

例

次の例では、再試行の回数を 0 に設定します。セキュリティ アプライアンスは各サーバを 1 回だけ試します。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns retries 0
hostname(config-dns-server-group)#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	dns サーバ グループ モードに入ります。
show running-config dns server-group	既存の DNS サーバ グループ コンフィギュレーションを 1 つまたはすべて表示します。

retry-interval

aaa-server host コマンドで以前に指定した特定の AAA サーバに対するリトライ間隔（時間の長さ）を設定するには、AAA サーバ ホスト モードで **retry-interval** コマンドを使用します。このリトライ間隔をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

retry-interval *seconds*

no retry-interval

シンタックスの説明

seconds	要求をリトライする間隔を指定します（1 ～ 10 秒）。セキュリティ アプライアンスが接続要求をリトライするまでに待つ時間です。

デフォルト

デフォルトのリトライ間隔は 10 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

セキュリティ アプライアンスが接続試行を実行する間隔（秒数）を指定またはリセットするには、**retry-interval** コマンドを使用します。**timeout** コマンドを使用して、セキュリティ アプライアンスが AAA サーバへの接続を試みる時間の長さを指定します。

例

次の例は、コンテキスト内の **retry-interval** コマンドを示しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 7
hostname(config-aaa-server-host)# retry-interval 9
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。
timeout	セキュリティ アプライアンスが AAA サーバへの接続確立の試行を継続する時間の長さを指定します。

revocation-check

失効チェックの方法を 1 つまたは複数設定するには、暗号 CA トラストポイント モードで **revocation-check** コマンドを使用します。セキュリティ アプライアンスは設定された順番でその方法を試行します。2 番目、3 番目の方法は、ステータスが失効として検出された場合とは反対に、直前の方法がエラー（サーバ ダウンなど）になった場合にのみ実行されます。

失効チェックの方法は、トラストポイントを検証するクライアント証明書に設定できます。また、トラストポイントを検証する応答側証明書に失効チェックなし（**revocation-check none**）を設定することもできます。**match certificate** コマンドのマニュアルには、手順に沿って示したコンフィギュレーション例が含まれています。

デフォルトの失効チェック方法（*none*）に戻すには、このコマンドの **no** 形式を使用します。

revocation-check {[**crl**] [**none**] [**ocsp**]}

no revocation-check

シンタックスの説明

crl	セキュリティ アプライアンスで失効チェック方法として CRL を使用することを指定します。
none	セキュリティ アプライアンスはすべての方法でエラーが返されても、証明書の状況を有効であると解釈することを指定します。
ocsp	セキュリティ アプライアンスで OCSP を失効チェック方法として使用することを指定します。

デフォルト

デフォルト値は *none* です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。次のように各コマンドが置き換えられました。 • **crl optional** は、**revocation-check crl none** に置き換えられました。 • **crl required** は、**revocation-check crl** に置き換えられました。 • **crl nocheck** は、**revocation-check none** に置き換えられました。

使用上のガイドライン

OCSP 応答の署名者は通常、OCSP サーバ（レスポンダ）証明書です。この応答の受信後、デバイスはレスポンダ証明書を確認します。

通常、CA は OCSP レスポンダ証明書の寿命を比較的短期間に設定して、セキュリティが脅かされる機会を最小限に抑えます。CA では、レスポンダ証明書内に失効状況を確認する必要がないことを示す ocsp-no-check 拡張機能を含みます。ただし、この拡張機能が含まれていない場合、デバイスはこの **revocation-check** コマンドでトラストポイントに設定する失効方法を使用して証明書の失効状況を確認しようとします。状況チェックを無視する *none* オプションも設定しないと OCSP 失効チェックは失敗するので、OCSP レスポンダ証明書は、ocsp-no-check 拡張機能が含まれていない場合に検証可能である必要があります。

例

次に例では、newtrust というトラストポイントに対して、OCSP と CRL の失効方法をこの順番で設定する方法を示します。

```
hostname(config)# crypto ca trustpoint newtrust
hostname(config-ca-trustpoint)# revocation-check ocsp crl
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	暗号 CA トラストポイント モードに入ります。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書き規則を設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするための OCSP サーバを指定します。

rewrite

特定のアプリケーションまたは WebVPN 接続のトラフィックのタイプのコンテンツ リライトをディセーブルにするには、WebVPN モードで **rewrite** コマンドを使用します。リライト規則を削除するには、このコマンドの **no** 形式を、規則を一意に識別する規則番号を付けて使用します。リライト規則をすべて削除するには、コマンドの **no** 形式を、規則番号を付けずに使用します。

デフォルトでは、セキュリティ アプライアンスはすべての WebVPN トラフィックのリライトまたは変換を行います。

rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

no rewrite order *integer* **{enable | disable} resource-mask** *string* **[name** *resource name***]**

シンタックスの説明

disable	リライト規則を、指定されたトラフィックに対するコンテンツ リライトをディセーブルにする規則として定義します。コンテンツ リライトをディセーブルにすると、トラフィックはセキュリティ アプライアンスを通過しません。
enable	リライト規則を、指定されたトラフィックに対するコンテンツ リライトをイネーブルにする規則として定義します。
integer	設定済みのすべての規則の順序を設定します。範囲は 1 ～ 65534 です。
name	（オプション）規則を適用するアプリケーションまたはリソースの名前を指定します。
order	セキュリティ アプライアンスが規則を適用する順序を定義します。
resource-mask	規則のアプリケーションまたはリソースを指定します。
resource name	（オプション）規則を適用するアプリケーションまたはリソースを指定します。最大 128 バイトです。
string	正規表現を含むことができるアプリケーションまたはリソースと一致するよう、アプリケーションまたはリソースの名前を指定します。次のワイルドカードを使用できます。 正規表現を含むことができるパターンと一致するよう、パターンを指定します。次のワイルドカードを使用できます。 * ：すべてと一致します。このワイルドカードはこれだけでは使用できません。英数字の文字列と共に使用する必要があります。 ? ：任意の 1 文字と一致します。 [!seq]：シーケンスにない任意の文字に一致します。 [seq]：シーケンス内の任意の文字に一致します。 最大 300 バイトです。

デフォルト

デフォルトでは、すべてリライトします。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン　セキュリティ アプライアンスは、WebVPN 接続上でアプリケーションが正しく動作するよう、アプリケーションのコンテンツ リライトを行います。外部の公的 Web サイトなど、コンテンツ リライトが不要なアプリケーションもあります。このようなアプリケーションには、コンテンツ リライトをオフにすることもできます。

コンテンツ リライトを選択的にオフにするには、disable オプションで rewrite コマンドを使用し、ユーザがセキュリティ アプライアンスを介さずに直接特定のサイトを閲覧できるようにします。これは、IPSec VPN 接続のスプリット トンネリングと類似しています。

このコマンドは複数回使用できます。セキュリティ アプライアンスはリライト規則を順番に検索し、一致した最初の規則を適用するため、エントリを設定する順序は重要です。

例　次の例は、cisco.com ドメインの URL のコンテンツ リライトをオフにする、1 番目のリライト規則を設定する方法を示しています。

```
hostname(config-webpn)# rewrite order 2 disable resource-mask *cisco.com/*
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
apcf	特定のアプリケーションに使用する非標準の規則を指定します。
proxy-bypass	特定のアプリケーションの最小限のコンテンツ リライトを設定します。

re-xauth

ユーザが IKE キー再生成で再認証を受けることを必須とするには、グループ ポリシー コンフィギュレーション モードで **re-xauth enable** コマンドを使用します。IKE キー再生成でのユーザ認証をディセーブルにするには、**re-xauth disable** コマンドを使用します。

re-xauth アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。これにより、IKE キー再生成での再認証の値を別のグループ ポリシーから継承できるようになります。

re-xauth {**enable** | **disable**}

no re-xauth

シンタックスの説明

disable	IKE キー再生成での再認証をディセーブルにします。
enable	IKE キー再生成での再認証をイネーブルにします。

デフォルト

IKE キー再生成での再認証は、ディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IKE キー再生成での再認証をイネーブルにすると、セキュリティ アプライアンスは、フェーズ 1 IKE ネゴシエーション中にユーザ名とパスワードの入力を求めるプロンプトを表示します。また、IKE キー再生成が実行されるたびに、ユーザ認証を求めるプロンプトを表示します。再認証により、セキュリティが向上します。

設定されているキー再生成間隔が極端に短い場合、ユーザは認証を繰り返し求められることに不便を感じることがあります。その場合は、再認証をディセーブルにしてください。設定されているキー再生成間隔を確認するには、モニタリング モードで **show crypto ipsec sa** コマンドを発行して、セキュリティ結合のライフタイムの秒単位データおよび KB 単位データを表示します。

（注） 接続相手側にユーザが存在しない場合、再認証は失敗します。

例

次の例は、FirstGroup というグループ ポリシーのキー再生成での再認証をイネーブルにする方法を示しています。

```
hostname(config) #group-policy FirstGroup attributes
hostname(config-group-policy)# re-xauth enable
```

rip authentication key

RIP バージョン 2 パケットの認証をイネーブルにし、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication key** コマンドを使用します。RIP バージョン 2 をディセーブルにするには、このコマンドの **no** 形式を使用します。

rip authentication key *key* ***key_id*** *key_id*

no rip authentication key

シンタックスの説明

key	RIP アップデートを認証するキー。このキーの最大長は 16 文字です。
key_id	キー ID 値：有効な値は 1 ～ 255 です。

デフォルト

RIP 認証はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用することで、RIP アップデートを認証できます。ネイバー認証をイネーブルにする場合、*key* 引数と *key_id* 引数は、RIP バージョン 2 アップデートを提供するネイバー デバイスによって使用される引数と同じでなければなりません。*key* は、最大 16 文字のテキスト文字列です。

特定のインターフェイスについて **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次の例では、インターフェイス GigabitEthernet0/3 に対して設定されている RIP 認証を表示しています。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

関連コマンド

コマンド	説明
rip authentication mode	RIP バージョン 2 パケットで使用される認証タイプを指定します。
rip receive version	指定したインターフェイス上でアップデートを受信するときに、受け入れる RIP バージョンを指定します。
rip send version	特定のインターフェイスからアップデートを送信するときに、使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip authentication mode

RIP バージョン 2 パケットで使用される認証タイプを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication mode** コマンドを使用します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

rip authentication mode {***text*** | ***md5***}

no rip authentication mode

シンタックスの説明

md5	RIP メッセージ認証には MD5 を使用します。
text	RIP メッセージ認証にはクリア テキストを使用します（推奨しません）。

デフォルト

クリア テキスト認証はデフォルトでは使用されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用することで、RIP アップデートを認証できます。

特定のインターフェイスについて **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次の例では、インターフェイス GigabitEthernet0/3 に対して設定されている RIP 認証を表示しています。

```
hostname(config)# interface Gigabit0/3
hostname(config-if)# rip authentication mode md5
hostname(config-if)# rip authentication key thisismykey key_id 5
```

関連コマンド

コマンド	説明
rip authentication key	RIP バージョン 2 認証をイネーブルにして、認証キーを指定します。
rip receive version	指定したインターフェイス上でアップデートを受信するときに、受け入れる RIP バージョンを指定します。
rip send version	特定のインターフェイスからアップデートを送信するときに、使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip receive version

インターフェイスで受け入れる RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip receive version** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

version {[*1*] [*2*]}

no version

シンタックスの説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは、バージョン 1 とバージョン 2 のパケットを受け入れます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスに対して **rip receive version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用することで、RIP アップデートを認証できます。

例

次の例では、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを受信するようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに、使用する RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードに入ります。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rip send version

インターフェイスで RIP アップデートを送信するために使用される RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip send version** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

rip send version {[*1*] [*2*]}

no rip send version

シンタックスの説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは RIP バージョン 1 パケットを送信します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP 送信バージョンのグローバル設定をインターフェイスごとに上書きするには、インターフェイスに対して **rip send version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用することで、RIP アップデートを認証できます。

例

次の例では、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを送受信するようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# interface GigabitEthernet0/3
hostname(config-if)# rip send version 1 2
hostname(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip receive version	指定したインターフェイス上でアップデートを受信するときに、受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードに入ります。
version	セキュリティ アプライアンスでグローバルに使用される RIP のバージョンを指定します。

rmdir

既存のディレクトリを削除するには、特権 EXEC モードで **rmdir** コマンドを使用します。

rmdir [**/noconfirm**] [**flash:**]*path*

シンタックスの説明

noconfirm	（オプション）確認プロンプトを表示しないようにします。
flash:	（オプション）取り外しできない内蔵フラッシュを指定し、続けてコロン（:）を入力します。
path	（オプション）削除するディレクトリの絶対パスまたは相対パス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ディレクトリが空でない場合、***rmdir*** コマンドは失敗します。

例

次の例は、「test」という名前の既存のディレクトリを削除する方法を示しています。

```
hostname# rmdir test
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
mkdir	新しいディレクトリを作成します。
pwd	現在の作業ディレクトリを表示します。
show file	ファイル システムに関する情報を表示します。

route

指定したインターフェイスのスタティック ルートまたはデフォルト ルートを入力するには、グローバル コンフィギュレーション モードで **route** コマンドを使用します。指定したインターフェイスからルートを削除するには、このコマンドの **no** 形式を使用します。

route *interface_name ip_address netmask gateway_ip* [[*metric*] [***track*** *number*] | ***tunneled***]

no route *interface_name ip_address netmask gateway_ip* [[*metric*] [***track*** *number*] | ***tunneled***]

シンタックスの説明

gateway_ip	ゲートウェイ ルータの IP アドレスを指定します（このルートのネクストホップ アドレス）。 **（注）** *gateway_ip* 引数は、透過モードでのオプションです。
interface_name	内部または外部のネットワーク インターフェイスの名前。
ip_address	内部または外部のネットワーク IP アドレス。
metric	（オプション）このルートの管理ディスタンス。有効な値は、1 ～ 255 です。デフォルト値は 1 です。
netmask	*ip_address* に適用するネットワーク マスクを指定します。
track *number*	（オプション）トラッキング エントリとこのルートを関連付けます。有効な値は 1 ～ 500 です。 **（注）** ***track*** オプションは、単独のルーテッド モードでのみ有効です。
tunneled	VPN トラフィックのデフォルト トンネル ゲートウェイとして、ルートを指定します。

デフォルト

metric のデフォルトは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	***track*** *number* 値が追加されました。

使用上のガイドライン

インターフェイスのデフォルト ルートまたはスタティック ルートを入力するには、**route** コマンドを使用します。デフォルト ルートを入力するには、*ip_address* と *netmask* を **0.0.0.0** に設定するか、短縮形の **0** を使用します。**route** コマンドを使用して入力したすべてのルートは、保存時にコンフィギュレーションに格納されます。

標準のデフォルト ルートに加えて、トンネル トラフィック用の別のデフォルト ルートを定義できます。***tunneled*** オプションを使用してデフォルト ルートを作成すると、セキュリティ アプライアンスに到達する暗号化されたトラフィックで、ラーニングされたルートまたはスタティック ルートのいずれでもルーティングできないトラフィックは、すべてこのルートに送信されます。トラフィックが暗号化されていない場合、標準のデフォルト ルート エントリが使用されます。***tunneled*** オプションで複数のデフォルト ルートを定義することはできません。トンネル トラフィックの ECMP はサポートされていません。

任意のインターフェイスでルータの外部に接続されているネットワークにアクセスするには、スタティック ルートを作成します。たとえば、セキュリティ アプライアンスはこのスタティック **route** コマンドを使用し、192.168.42.0 ネットワークに向けて 192.168.1.5 ルータ経由ですべてのパケットを送信します。

```
hostname(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

各インターフェイスの IP アドレスを入力すると、セキュリティ アプライアンスは、ルート テーブルに CONNECT ルートを作成します。このエントリは、**clear route** コマンドまたは **clear configure route** コマンドを使用しても削除できません。

route コマンドがセキュリティ アプライアンスのインターフェイスいずれか 1 つの IP アドレスをゲートウェイ IP アドレスとして使用する場合、セキュリティ アプライアンスはゲートウェイ IP アドレスに対して ARP を実行するのではなく、パケット内の宛先 IP アドレスに対して ARP を実行します。

例

次の例は、外部インターフェイスに対して 1 つのデフォルト **route** コマンドを指定する方法を示しています。

```
hostname(config)# route outside 0 0 209.165.201.1 1
```

次の例は、次のスタティック **route** コマンドを追加して、ネットワークへのアクセスを提供する方法を示しています。

```
hostname(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
hostname(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

次の例は、デフォルト ルートを外部インターフェイスの 10.1.1.1 ゲートウェイにインストールするために SLA オペレーションを使用します。SLA オペレーションはゲートウェイの可用性を監視します。SLA 操作が失敗すると、dmz インターフェイスでバックアップ ルートが使用されます。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
hostname(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
hostname(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。
clear route	RIP などのダイナミック ルーティング プロトコルを通じてラーニングされたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

route-map

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義するには、グローバル コンフィギュレーション モードで **route-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

route-map *map_tag* [**permit** | **deny**] [*seq_num*]

no route-map *map_tag* [**permit** | **deny**] [*seq_num*]

シンタックスの説明

deny	（オプション）このルートマップが一致基準に適合した場合は、このルートを再配布しないことを指定します。
map_tag	ルートマップ タグのテキスト。テキストの長さは最大 57 文字です。
permit	（オプション）このルートマップが一致基準に適合した場合は、このルートを、設定アクションによる制御に従って再配布することを指定します。
seq_num	（オプション）ルートマップのシーケンス番号。有効な値は 0 ～ 65535 です。すでに同じ名前で設定されているルートマップのリストにおける新しいルートマップの位置を示します。

デフォルト

デフォルトは次のとおりです。

- **permit**
- *seq_num* を指定しない場合、*seq_num* の値 10 が最初のルートマップに割り当てられます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

route-map コマンドを使用すると、ルートを再配布できます。

route-map グローバル コンフィギュレーション コマンド、**match** コンフィギュレーション コマンド、および **set** コンフィギュレーション コマンドは、あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。各 **route-map** コマンドには、**match** コマンドと **set** コマンドが関連付けられます。**match** コマンドは、一致基準、つまり現在の **route-map** コマンドについて再配布を許可する条件を指定します。**set** コマンドには、設定アクション、つまり **match** コマンドで指定した基準を満たしている場合に実行する再配布アクションを指定します。**no route-map** コマンドを実行すると、ルートマップが削除されます。

match route-map コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。また、**set** コマンドで指定した設定アクションに従ってルートの再配布を実行するには、すべての **match** コマンドに一致する必要があります。**match** コマンドを **no** 形式で実行すると、指定した一致基準が削除されます。

ルーティング プロセス間のルート再配布方法を細かく制御するには、ルートマップを使用します。宛先ルーティング プロトコルは、**router ospf** グローバル コンフィギュレーション コマンドで指定します。送信元ルーティング プロトコルは、**redistribute** ルータ コンフィギュレーション コマンドで指定します。

ルートマップを通じてルートを渡すとき、ルートマップはいくつかの部分に分かれることがあります。**route-map** コマンドと関連する 1 つ以上の match 節と一致しないルートは、無視されます。そのルートが、発信ルートマップのためにアドバタイズされるか、着信ルートマップのために受け入れられることはありません。一部のデータのみを修正するには、正確に一致する基準を指定した 2 番目のルートマップ セクションを設定する必要があります。

seq_number 引数については、次のとおりです。

1. 提供されたタグでエントリを定義しない場合、*seq_number* 引数に 10 が設定されたエントリが作成されます。
2. 提供されたタグで 1 つだけエントリを定義した場合、そのエントリは、その後に続く **route-map** コマンドのデフォルト エントリとなります。このエントリの *seq_number* 引数は変更されません。
3. 提供されたタグで 2 つ以上のエントリを定義した場合、*seq_number* 引数が必要であることを示すエラー メッセージが出力されます。

no route-map *map-tag* コマンドを（*seq-num* 引数なしで）指定した場合、ルートマップ全体（同じ *map-tag* テキストを持つすべての **route-map** エントリ）が削除されます。

一致基準に適合しない場合に **permit** キーワードを指定してあれば、同じ *map_tag* を持つ次のルートマップがテストされます。ルートは、同じ名前を共有するルートマップ セットの一致基準に 1 つも一致しなかった場合、そのセットによって再配布されません。

例

次の例は、OSPF ルーティングで使用するルートマップを設定する方法を示しています。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show running-config route-map
route-map maptag1 permit 8
    set metric 5
    match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を削除します。
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
router ospf	OSPF ルーティング プロセスを開始および設定します。
set metric	ルートマップの宛先ルーティング プロトコルのメトリック値を指定します。
show running-config route-map	ルートマップ コンフィギュレーションに関する情報を表示します。

router-id

固定ルータ ID を使用するには、ルータ コンフィギュレーション モードで **router-id** コマンドを使用します。先行の OSPF ルータ ID 動作を使用するように OSPF をリセットするには、このコマンドの **no** 形式を使用します。

router-id *addr*

no router-id [*addr*]

シンタックスの説明

addr	IP アドレス形式のルータ ID。

デフォルト

指定しない場合、セキュリティ アプライアンス上で最上位の IP アドレスがルータ ID として使用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンス上で最上位の IP アドレスがプライベート アドレスの場合、このアドレスは hello パケットおよびデータベース定義で送信されます。この状況を回避するには、**router-id** コマンドを使用してルータ ID のグローバル アドレスを指定します。

例

次の例では、ルータ ID を 192.168.1.1 に設定します。

```
hostname(config-router)# router-id 192.168.1.1
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

router ospf

OSPF ルーティング プロセスを開始し、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router ospf** コマンドを使用します。OSPF ルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

router ospf *pid*

no router ospf *pid*

シンタックスの説明

pid	OSPF ルーティング プロセス用に内部的に使用される識別パラメータ。有効な値は、1 ～ 65535 です。*pid* は、他のルータ上の OSPF プロセスの ID と一致する必要はありません。

デフォルト

OSPF ルーティングはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

router ospf コマンドは、セキュリティ アプライアンス上で実行している OSPF ルーティング プロセスのグローバル コンフィギュレーション コマンドです。**router ospf** コマンドを入力すると、コマンド プロンプトは (config-router)# と表示されます。これは、ルータ コンフィギュレーション モードに入ったことを示しています。

no router ospf コマンドを使用する場合、必要な情報を提供するものでない限り、オプションの引数を使用する必要はありません。**no router ospf** コマンドは、*pid* で指定された OSPF ルーティング プロセスを終了します。*pid* をセキュリティ アプライアンス上でローカルに割り当てることができます。OSPF ルーティング プロセスごとに固有の値を割り当てる必要があります。

router ospf コマンドは、OSPF 固有の次のコマンドと共に使用され、OSPF ルーティング プロセスを設定します。

- **area**：通常の OSPF エリアを設定します。
- **compatible rfc1583**：RFC 1583 準拠のサマリー ルート コストの計算に使用される方式に戻します。
- **default-information originate**：OSPF ルーティング ドメイン内へのデフォルトの外部ルートを生成します。
- **distance**：ルート タイプに基づいて、OSPF ルートの管理ディスタンスを定義します。
- **ignore**：タイプ 6 Multicast OSPF（MOSPF）パケットの link-state advertisement（LSA; リンクステート アドバタイズメント）を受信した際に、syslog メッセージを送信しないようにします。

- **log-adj-changes**：OSPF 隣接ルータがアップ状態またはダウン状態になると syslog メッセージを送信するように、ルータを設定します。
- **neighbor**：隣接ルータを指定します。VPN トンネル経由での隣接関係の確立を可能にするために使用されます。
- **network**：OSPF を実行するインターフェイス、およびそれらのインターフェイスのエリア ID を定義します。
- **redistribute**：指定されたパラメータに基づく、あるルーティング ドメインから別のルーティング ドメインへのルートの再配布を設定します。
- **router-id**：固定ルータ ID を作成します。
- **summary-address**：OSPF の集約アドレスを作成します。
- **timers lsa-group-pacing**：OSPF LSA グループ間隔タイマー（リフレッシュまたは最大限にエージングされている LSA グループの間隔）。
- **timers spf**：SPF 計算に対する変更を受信する間隔。

セキュリティ アプライアンスで RIP が設定されている場合は、OSPF を設定できません。

例

次の例は、5 番の OSPF ルーティング プロセスのコンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# router ospf 5
hostname(config-router)#
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションから OSPF ルータ コマンドを消去します。
show running-config router ospf	実行コンフィギュレーション内の OSPF ルータ コマンドを表示します。

router rip

RIP ルーティング プロセスを開始し、そのプロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router rip** コマンドを使用します。RIP ルーティング プロセスをディセーブルにするには、このコマンドの **no** 形式を使用します。

router rip

no router rip

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

RIP ルーティングはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

router rip コマンドは、セキュリティ アプライアンス上で実行している RIP ルーティング プロセスのグローバル コンフィギュレーション コマンドです。セキュリティ アプライアンスで RIP プロセスを 1 つだけ設定できます。**no router rip** コマンドは RIP ルーティング プロセスを停止し、その処理のためのすべてのルータ コンフィギュレーションを削除します。

router rip コマンドを入力すると、コマンド プロンプトは `hostname(config-router)#` に変更されます。これは、ルータ コンフィギュレーション モードに入ったことを示しています。

router rip コマンドは、次のルータ コンフィギュレーション コマンドと共に使用され、RIP ルーティング プロセスを設定します。

- **auto-summary**：ルートの自動集約をイネーブル / ディセーブルにします。
- **default-information originate**：デフォルト ルートを配布します。
- **distribute-list in**：着信するルーティング アップデートのネットワークをフィルタリングします。
- **distribute-list out**：送信するルーティング アップデートのネットワークをフィルタリングします。
- **network**：ルーティング プロセスからインターフェイスを追加 / 削除します。
- **passive-interface**：特定のインターフェイスをパッシブ モードに設定します。
- **redistribute**：他のルーティング プロセスからのルートを RIP ルーティング プロセスに再配布します。
- **version**：セキュリティ アプライアンスで使用される RIP プロトコル バージョンを設定します。

さらに、次のコマンドをインターフェイス コンフィギュレーション モードで使用して、RIP プロパティをインターフェイスごとに設定できます。

- **rip authentication key**：認証キーを設定します。
- **rip authentication mode**：RIP バージョン 2 で使用される認証タイプを設定します。
- **rip send version**：インターフェイス外にアップデートを送信するために使用される RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。
- **rip receive version**：インターフェイスによって受け入れられる RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。

RIP は、透過モードではサポートされません。デフォルトで、セキュリティ アプライアンスはすべての RIP ブロードキャストおよびマルチキャスト パケットを拒否します。これらの RIP メッセージが透過モードで動作するセキュリティ アプライアンスを通過することを許可するには、このトラフィックを許可するようアクセス リストのエントリを定義する必要があります。たとえば、RIP バージョン 2 トラフィックのセキュリティ アプライアンス通過を許可するには、`access-list myriplist extended permit ip any host 224.0.0.9` などのアクセス リスト エントリを作成します。RIP バージョン 1 ブロードキャストを許可するには、`access-list myriplist extended permit udp any any eq rip` などのアクセス リスト エントリを作成します。アクセス リスト エントリをインターフェイスに適用するには、**access-group** コマンドを使用します。

RIP と OSPF ルーティングをセキュリティ アプライアンスで同時にイネーブルにできます。

例

次の例は、5 番の OSPF ルーティング プロセスのコンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

関連コマンド

コマンド	説明
clear configure router rip	実行コンフィギュレーションから RIP ルータ コマンドを消去します。
show running-config router rip	実行コンフィギュレーション内の RIP ルータ コマンドを表示します。

rtp-conformance

ピンホールを流れる RIP パケットの H.323 および SIP におけるプロトコル適合性を確認するには、パラメータ コンフィギュレーション モードで **rtp-conformance** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

rtp-conformance [enforce-payloadtype]

no rtp-conformance [enforce-payloadtype]

シンタックスの説明

enforce-payloadtype	シグナリング交換に基づいてペイロード タイプをオーディオ/ビデオに分類します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、ピンホールを流れる RIP パケットの H.323 コールにおけるプロトコル適合性を確認する方法を示しています。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# rtp-conformance
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
debug rtp	H.323 および SIP 検査に関連付けられた RTP パケットのデバッグ情報およびエラー メッセージを表示します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

CHAPTER 24

same-security-traffic コマンド～ show asdm sessions コマンド

same-security-traffic

セキュリティ レベルが等しいインターフェイス間での通信を許可する、またはトラフィックが同じインターフェイスへ入る、または出るのを許可するには、グローバル コンフィギュレーション モードで **same-security-traffic** コマンドを使用します。セキュリティの等しいトラフィック間での通信をディセーブルにするには、このコマンドの **no** 形式を使用します。

same-security-traffic permit {**inter-interface | intra-interface**}

no same-security-traffic permit {**inter-interface | intra-interface**}

シンタックスの説明

inter-interface	セキュリティ レベルの等しい複数のインターフェイス間での通信を許可します。
intra-interface	同じインターフェイスの通信のインおよびアウトを許可します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。
7.2(1)	このバージョン以降は、**intra-interface** キーワードを使用すると、IPSec トラフィックだけでなく、すべてのトラフィックが同じインターフェイスに出入りできます。

使用上のガイドライン

セキュリティ レベルが等しいインターフェイス間での通信を許可（**same-security-traffic inter-interface** コマンドを使用）すると、次の利点があります。

- 101 個を超える通信インターフェイスを設定できる。インターフェイスごとにそれぞれ別のレベルを使用する場合、設定できるインターフェイスは各レベル（0 ～ 100）に 1 つのみです。
- セキュリティ レベルの等しいすべてのインターフェイス間で、アクセス リストとは無関係に、トラフィックを自由に送受信できる。

same-security-traffic intra-interface コマンドを使用すると、通常は許可されていない、トラフィックによる同一インターフェイスへの出入りが可能になります。この機能は、あるインターフェイスに入り、同じインターフェイスから出る VPN トラフィックに役立ちます。この場合、VPN トラフィックの暗号化は解除されるか、別の VPN 接続に対して再暗号化されます。たとえば、ハブまたはスポークの VPN ネットワークがあるとします。セキュリティ アプライアンスがハブで、リモート VPN ネットワークがスポークであり、一方のスポークが別のスポークと通信する場合、トラフィックはセキュリティ アプライアンスに入り、その後別のスポークに向けて出て行かなければなりません。

例

次の例は、セキュリティ レベルの等しいインターフェイス間での通信をイネーブルにする方法を示しています。

```
hostname(config)# same-security-traffic permit inter-interface
```

次の例では、トラフィックが同じインターフェイスに入り、出て来るようにする方法を示します。

```
hostname(config)# same-security-traffic permit intra-interface
```

関連コマンド

コマンド	説明
show running-config same-security-traffic	**same-security-traffic** のコンフィギュレーションを表示します。

sasl-mechanism

LDAP サーバに対する LDAP クライアントの認証に SASL（Simple Authentication and Security Layer）メカニズムを指定するには、AAA サーバ ホスト コンフィギュレーション モードで **sasl-mechanism** コマンドを使用します。SASL 認証メカニズムのオプションは、**digest-md5** および **kerberos** です。

認証メカニズムをディセーブルにするには、このコマンドの **no** 形式を使用します。

sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

no sasl-mechanism {**digest-md5** | **kerberos** *server-group-name*}

（注） VPN ユーザにとってセキュリティ アプライアンスは、LDAP サーバに対するクライアント プロキシとして機能するため、ここでいう LDAP クライアントとは、セキュリティ アプライアンスのことです。

シンタックスの説明

digest-md5	セキュリティ アプライアンスは、ユーザ名とパスワードから計算された MD5 の値で応答します。
kerberos	セキュリティ アプライアンスは、GSSAPI（Generic Security Services Application Programming Interface）Kerberos メカニズムを使用してユーザ名とレルムを送信することで応答します。
server-group-name	Kerberos AAA サーバ グループを指定します（最大 64 文字）。

デフォルト

デフォルトの動作や値はありません。セキュリティ アプライアンスは、認証パラメータをプレーンテキスト形式で LDAP サーバに渡します。

（注） SASL を設定していない場合は、**ldap-over-ssl** コマンドを使用して SSL で LDAP 通信を保護することをお勧めします。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、LDAP サーバに対するセキュリティ アプライアンスの認証に SASL メカニズムを使用するよう指定します。

セキュリティ アプライアンスも LDAP サーバも、複数の SASL 認証メカニズムをサポートできます。SASL 認証のネゴシエート時には、セキュリティ アプライアンスはサーバ上に設定されている SASL メカニズムのリストを取得し、セキュリティ アプライアンスとサーバの両方で設定されている最も強固なメカニズムとして SASL 認証メカニズムを設定します。Kerberos メカニズムは Digest-MD5 メカニズムよりも強固です。たとえば、LDAP サーバもセキュリティ アプライアンスも両方のメカニズムをサポートしている場合、セキュリティ アプライアンスはより強固なメカニズムである Kerberos を選択します。

SASL メカニズムをディセーブルにする場合、これらのメカニズムは個別に設定されるため、ディセーブルにするメカニズムごとに **no** コマンドを入力する必要があります。明確にディセーブルにしないと、メカニズムは有効になったままです。たとえば、両方の SASL メカニズムをディセーブルにするには、次のコマンドを両方とも入力する必要があります。

no sasl-mechanism digest-md5

no sasl-mechanism kerberos <*server-group-name*>

例

次の例は、AAA サーバ ホスト コンフィギュレーション モードに入り、IP アドレスが 10.10.0.1 で ldapsvr1 という名前の LDAP サーバに対する認証として、SASL メカニズムをイネーブルにしています。この例は、SASL digest-md5 認証メカニズムをイネーブルにしています。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism digest-md5
hostname(config-aaa-server-host)#
```

次の例は、SASL Kerberos 認証メカニズムをイネーブルにし、Kerberos AAA サーバとして kerb-servr1 を指定しています。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# sasl-mechanism kerberos kerbsvr1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL によって LDAP クライアントとサーバの接続を保護するよう指定します。
server-type	LDAP サーバのベンダーを Microsoft または Sun として指定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。

secondary

フェールオーバー グループ内のセカンダリ装置に高い優先順位を与えるには、フェールオーバー グループ コンフィギュレーション モードで **secondary** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

secondary

no secondary

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

フェールオーバー グループに対して **primary** または **secondary** を指定しない場合、そのフェールオーバー グループは、デフォルトでは **primary** に設定されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プライマリまたはセカンダリの優先順位をフェールオーバー グループに割り当てると、両方の装置が（装置のポーリング時間内で）同時にブートしたときに、フェールオーバー グループがどの装置上でアクティブになるかが指定されます。ある装置がもう一方の装置よりも先にブートした場合、どちらのフェールオーバー グループもその装置上でアクティブになります。もう一方の装置がオンラインになると、優先順位として 2 番目の装置を持つフェールオーバー グループは、そのフェールオーバー グループが **preempt** コマンドを使用して設定されているか、手作業で **no failover active** コマンドを使用してもう一方の装置に強制しない限り、2 番目の装置上ではアクティブになりません。

例

次の例では、優先順位の高いプライマリ装置を持つフェールオーバー グループ 1 と、優先順位の高いセカンダリ装置を持つフェールオーバー グループ 2 を設定しています。どちらのフェールオーバー グループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先する装置が使用可能になったときにその装置上で自動的にアクティブになります。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
preempt	優先する装置が使用可能になったときに、フェールオーバー グループをその装置上で強制的にアクティブにします。
primary	プライマリ装置に対して、セカンダリ装置よりも高い優先順位を与えます。

secondary-color

WebVPN のログイン ページ、ホーム ページ、およびファイル アクセス ページに 2 番目の色を設定するには、WebVPN モードで **secondary-color** コマンドを使用します。色をコンフィギュレーションから削除してデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

secondary-color [*color***]**

no secondary-color

シンタックスの説明

color	（オプション）色を指定します。カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。 • RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。 • HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。 • 名前の長さは、最大で 32 文字です。

デフォルト

デフォルトの 2 番目の色は、HTML の #CCCCFF（薄紫色）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

RGB 値を使用する場合、推奨値は 216 です。推奨色は、数学的にあり得る数よりはるかに少なくなります。多くのディスプレイは 256 色しか処理できず、その中の 40 色は、Macintosh と PC では別の色が表示されます。最適な表示結果を得るには、各所で公開されている RGB テーブルを確認してください。RGB テーブルをオンラインで見つけるには、検索エンジンで RGB と入力します。

例

次の例は、HTML 色値 #5F9EAO（灰青色）を設定する方法を示しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-color #5F9EAO
```

関連コマンド

コマンド	説明
title-color	ログイン ページ、ホーム ページ、およびファイル アクセス ページの WebVPN タイトルバーに色を設定します。

secondary-text-color

WebVPN のログイン ページ、ホーム ページ、およびファイル アクセス ページでテキストの 2 番目の色を設定するには、WebVPN モードで **secondary-text-color** コマンドを使用します。色をコンフィギュレーションから削除してデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

secondary-text-color [*black* | *white*]

no secondary-text-color

シンタックスの説明

auto	text-color コマンドの設定に基づいて黒または白を選択します。つまり、最初の色が黒の場合、この値は白となります。
black	デフォルトのテキストの 2 番目の色は黒です。
white	テキストの色を白に変更できます。

デフォルト

デフォルトのテキストの 2 番目の色は黒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、テキストの 2 番目の色を白に設定する方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# secondary-text-color white
```

関連コマンド

コマンド	説明
text-color	ログイン ページ、ホーム ページ、およびファイル アクセス ページの WebVPN タイトルバーのテキストに色を設定します。

secure-unit-authentication

Secure Unit Authentication（SUA）をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **secure-unit-authentication enable** コマンドを使用します。Secure Unit Authentication をディセーブルにするには、**secure-unit-authentication disable** コマンドを使用します。Secure Unit Authentication アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、Secure Unit Authentication の値を別のグループ ポリシーから継承できます。

Secure Unit Authentication は、VPN ハードウェア クライアントがトンネルを開始するたびに、ユーザ名とパスワードを使用して認証を受けるように要求して、セキュリティを強化します。この機能がイネーブルになっている場合、ハードウェア クライアントは保存されているユーザ名とパスワードを使用できません。

（注） この機能がイネーブルになっているときに VPN トンネルを確立するには、ユーザ名とパスワードを入力するユーザがいる必要があります。

secure-unit-authentication {**enable** | **disable**}

no secure-unit-authentication

シンタックスの説明

disable	Secure Unit Authentication をディセーブルにします。
enable	Secure Unit Authentication をイネーブルにします。

デフォルト

Secure Unit Authentication はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

Secure Unit Authentication を使用するには、ハードウェア クライアントの使用するトンネル グループ用に認証サーバグループを設定しておく必要があります。

プライマリ セキュリティ アプライアンス上で Secure Unit Authentication を要求する場合は、すべてのバックアップ サーバ上でも認証サーバグループを設定する必要があります。

例

次の例は、Secure Unit Authentication を FirstGroup というグループ ポリシーに対してイネーブルにする方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# secure-unit-authentication enable
```

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を受けずに IP 電話を接続できるようにします。Secure Unit Authentication は有効なままになります。
leap-bypass	VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットが、ユーザ認証（有効になっている場合）前に VPN トンネルを通過することを許可します。これにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。確立後、ワークステーションはユーザごとの認証をもう一度実行します。
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

security-level

インターフェイスのセキュリティ レベルを設定するには、インターフェイス コンフィギュレーション モードで **security-level** コマンドを使用します。セキュリティ レベルをデフォルトに設定するには、このコマンドの **no** 形式を使用します。セキュリティ レベルとは、2 つのネットワーク間に保護手段を追加して、セキュリティの高いネットワークをセキュリティの低いネットワークから保護するものです。

security-level *number*

no security-level

シンタックスの説明

number	0（最低）～ 100（最高）の整数。

デフォルト

デフォルトでは、セキュリティ レベルは 0 です。

インターフェイスに「inside」という名前を付けて、セキュリティ レベルを明示的に設定しなかった場合、セキュリティ アプライアンスはセキュリティ レベルを 100 に設定します（**nameif** コマンドを参照）。このレベルは必要に応じて変更できます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**nameif** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

セキュリティ レベルによって、次の動作が制御されます。

- ネットワーク アクセス：デフォルトでは、セキュリティの高いインターフェイスからセキュリティの低いインターフェイスへのアクセス（発信）は暗黙的に許可されます。セキュリティの高いインターフェイス上にあるホストは、セキュリティの低いインターフェイス上にあるすべてのホストにアクセスできます。アクセスを制限するには、インターフェイスにアクセス リストを適用します。

  セキュリティ レベルの等しいインターフェイスが複数ある場合、セキュリティ レベルが同等またはそれ以下である他のインターフェイスへのアクセスは、暗黙的に許可されます。
- 検査エンジン：一部の検査エンジンは、セキュリティ レベルに依存します。セキュリティ レベルの等しいインターフェイスが複数ある場合、検査エンジンは双方向のトラフィックに適用されます。
  - NetBIOS 検査エンジン：発信接続にのみ適用されます。
  - OraServ 検査エンジン：2 つのホスト間で OraServ ポートの制御接続が存在する場合、セキュリティ アプライアンスでは着信データ接続のみが許可されます。

- フィルタリング：HTTP（S）と FTP のフィルタリングは、（高レベルから低レベルへの）発信接続にのみ適用されます。

  セキュリティ レベルの等しいインターフェイスが複数ある場合は、双方向のトラフィックをフィルタリングできます。

- NAT 制御：NAT 制御をイネーブルにする場合、セキュリティの高いインターフェイス（内部）上にあるホストがセキュリティの低いインターフェイス（外部）上にあるホストにアクセスする場合は、セキュリティの高いインターフェイス上にあるホストに対して NAT を設定する必要があります。

  NAT 制御を使用しない場合や、セキュリティ レベルの等しい複数のインターフェイス間では、任意のインターフェイス間に NAT を使用することも、NAT を使用しないこともできます。外部インターフェイスに対して NAT を設定する場合は、特殊なキーワードが必要になることがあります。

- **established** コマンド：このコマンドは、セキュリティ レベルの高いホストから低いホストに向かう接続がすでに確立されている場合に、セキュリティの低いホストからセキュリティの高いホストへのリターン接続を許可します。

  セキュリティ レベルの等しいインターフェイスが複数ある場合は、双方向に対して **established** コマンドを設定できます。

通常、セキュリティ レベルの等しいインターフェイス間では通信できません。セキュリティ レベルの等しいインターフェイス間で通信する必要がある場合は、**same-security-traffic** コマンドを参照してください。101 個を超える通信インターフェイスを作成する場合や、2 つのインターフェイス間で発生するトラフィックに対して同等に保護機能を適用する場合は、2 つのインターフェイスに同じセキュリティ レベルを割り当てて、通信を許可することがあります。たとえば、同等のセキュリティを必要とする 2 つの部署がある場合などです。

インターフェイスのセキュリティ レベルを変更する場合、既存の接続がタイムアウトするのを待たずに新しいセキュリティ情報を使用するには、**clear local-host** コマンドを使用して接続を消去します。

例

次の例では、2 つのインターフェイスのセキュリティ レベルを 100 と 0 に設定しています。

```
hostname(config)# interface gigabitethernet0/0
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
hostname(config-if)# interface gigabitethernet0/1
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address 10.1.2.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear local-host	すべての接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
nameif	インターフェイス名を設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

send response

RADIUS Accounting-Response Start および Stop メッセージを RADIUS Accounting-Request Start および Stop メッセージの送信者に送信するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **send response** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。

このオプションは、デフォルトではディセーブルになっています。

send response

no send response

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、RADIUS アカウンティングを指定した応答を送信する方法を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# send response
hostname(config-pmap-p)# send response
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングの検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

serial-number

セキュリティ アプライアンスのシリアル番号を登録時に証明書に含めるには、暗号 CA トラストポイント コンフィギュレーション モードで **serial-number** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

serial-number

no serial-number

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、シリアル番号を含めない設定になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、central というトラストポイントの暗号 CA トラストポイント コンフィギュレーション モードに入って、セキュリティ アプライアンスのシリアル番号をトラストポイント central の登録要求に含めています。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# serial-number
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。

server

デフォルトの電子メールプロキシ サーバを指定するには、適切な電子メールプロキシ モードで **server** コマンドを使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。セキュリティ アプライアンスは、ユーザがサーバを指定せずに電子メールプロキシに接続すると、要求をデフォルト電子メール サーバに送信します。デフォルト サーバを設定しない場合、ユーザもサーバを指定しなかったときは、セキュリティ アプライアンスはエラーを返します。

server {*ipaddr or hostname***}**

no server

シンタックスの説明

hostname	デフォルト電子メールプロキシ サーバの DNS 名。
ipaddr	デフォルト電子メールプロキシ サーバの IP アドレス。

デフォルト

デフォルトでは、デフォルト電子メールプロキシ サーバはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Pop3s	•	•	—	—	•
Imap4s	•	•	—	—	•
Smtps	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、デフォルト POP3S 電子メール サーバの IP アドレスを 10.1.1.7 に設定する方法を示しています。

```
hostname(config)# pop3s
hostname(config-pop3s)# server 10.1.1.7
```

server-port

ホストの AAA サーバ ポートを設定するには、AAA サーバ ホスト モードで **server-port** コマンドを使用します。指定したサーバ ポートを削除するには、このコマンドの **no** 形式を使用します。

server-port *port-number*

no server-port

シンタックスの説明

port-number	0 ～ 65535 のポート番号。

デフォルト

デフォルトのサーバ ポートは次のとおりです。

- SDI：5500
- LDAP：389
- Kerberos：88
- NT：139
- TACACS+：49

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ グループ	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、「srvgrp1」という名前の SDI AAA サーバでサーバ ポート番号 8888 を使用するように設定しています。

```
hostname(config)# aaa-server srvgrp1 protocol sdi
hostname(config-aaa-server-group)# aaa-server srvgrp1 host 192.168.10.10
hostname(config-aaa-server-host)# server-port 8888
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	ホスト固有の AAA サーバ パラメータを設定します。
clear configure aaa-server	AAA サーバのコンフィギュレーションをすべて削除します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

server-separator

電子メール サーバ名と VPN サーバ名のデリミタとなる文字を指定するには、適切な電子メールプロキシ モードで **server-separator** コマンドを使用します。デフォルトのコロン（:）に戻すには、このコマンドの no 形式を使用します。

server-separator {*symbol***}**

no server-separator

シンタックスの説明

symbol	電子メール サーバ名と VPN サーバ名を区切る文字。使用できるのは、アットマーク（@）、パイプ（|）、コロン（:）、番号記号（#）、カンマ（,）、およびセミコロン（;）です。

デフォルト

デフォルトは、アットマーク（@）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Pop3s	•	—	•	—	—
Imap4s	•	—	•	—	—
Smtps	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

サーバ セパレータは、名前セパレータとは別の文字にする必要があります。

例

次の例は、パイプ（|）を IMAP4S のサーバ セパレータとして設定する方法を示しています。

```
hostname(config)# imap4s
hostname(config-imap4s)# server-separator |
```

関連コマンド

コマンド	説明
name-separator	電子メールおよび VPN のユーザ名と、パスワードを区切る文字を指定します。

server-type

LDAP サーバ モデルを手動で設定するには、AAA サーバ ホスト コンフィギュレーション モードで **server-type** コマンドを使用します。セキュリティ アプライアンスは次のサーバ モデルをサポートしています。

- Microsoft Active Directory
- Sun Microsystems JAVA System Directory Server（以前は Sun ONE Directory Server と呼ばれていた）

このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

server-type {**auto-detect| microsoft** | **sun**}

no server-type {**auto-detect| microsoft** | **sun**}

シンタックスの説明

auto-detect	セキュリティ アプライアンスが自動検出によって LDAP サーバ タイプを決定するように指定します。
microsoft	LDAP サーバが Microsoft Active Directory であることを指定します。
sun	LDAP サーバが Sun Microsystems JAVA System Directory Server であることを指定します。

デフォルト

デフォルトでは、自動検出によりサーバ タイプを決定するようになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは LDAP バージョン 3 をサポートし、Sun Microsystems JAVA System Directory Server および Microsoft Active Directory のみと互換性があります。

（注）

- Sun：Sun のディレクトリ サーバにアクセスするためにセキュリティ アプライアンスで設定された DN は、そのサーバのデフォルト パスワード ポリシーにアクセスできなければなりません。DN としてディレクトリ管理者か、ディレクトリ管理者権限を持つユーザを使用することを推奨します。または、デフォルト パスワード ポリシーに ACI を置くことができます。
- Microsoft：Microsoft Active Directory を使用してパスワードを管理できるように、SSL で LDAP を設定する必要があります。

デフォルトでは、セキュリティ アプライアンスは、接続先が Microsoft または Sun の LDAP ディレクトリ サーバであるかどうかを自動検出します。ただし、自動検出による LDAP サーバ タイプの決定が失敗した場合でも、LDAP サーバが Microsoft または Sun のどちらであるかがわかっている場合は、**server-type** コマンドを使用して、サーバを Microsoft または Sun Microsystems の LDAP サーバに手動で設定できます。

例

次の例では、AAA サーバ ホスト コンフィギュレーション モードに入り、サーバ タイプを IP アドレス 10.10.0.1 の LDAP サーバ ldapsvr1 に設定します。最初の例では、Sun Microsystems LDAP サーバを設定しています。

```
hostname(config)# aaa-server ldapsvr1 protocol ldap
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type sun
hostname(config-aaa-server-host)#
```

次の例では、セキュリティ アプライアンスが自動検出によってサーバ タイプを決定するように指定しています。

```
hostname(config)# aaa-server ldapsvr1 protocol LDAP
hostname(config-aaa-server-group)# aaa-server ldapsvr1 host 10.10.0.1
hostname(config-aaa-server-host)# server-type auto-detect
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap-over-ssl	SSL によって LDAP クライアントとサーバの接続を保護するよう指定します。
sasl-mechanism	LDAP クライアントとサーバ間の SASL 認証を設定します。
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。

service

拒否された TCP 接続のリセットをイネーブルにするには、グローバル コンフィギュレーション モードで **service** コマンドを使用します。リセットをディセーブルにするには、このコマンドの **no** 形式を使用します。

service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

no service {**resetinbound** [**interface** *interface_name*] | **resetoutbound** [**interface** *interface_name*] | **resetoutside**}

シンタックスの説明

interface *interface_name*	指定されたインターフェイスのリセットをイネーブルまたはディセーブルにします。
resetinbound	セキュリティ アプライアンスを通過しようとしたが、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスに拒否されたすべての着信 TCP セッションの TCP リセットを送信します。セキュリティ レベルが同じインターフェイス間のトラフィックにも影響します。このオプションがイネーブルになっていないと、セキュリティ アプライアンスは拒否されたパケットを通知なしで廃棄します。インターフェイスが指定されていない場合、この設定はすべてのインターフェイスに適用されます。
resetoutbound	セキュリティ アプライアンスを通過しようとしたが、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスに拒否されたすべての発信 TCP セッションの TCP リセットを送信します。セキュリティ レベルが同じインターフェイス間のトラフィックにも影響します。このオプションがイネーブルになっていないと、セキュリティ アプライアンスは拒否されたパケットを通知なしで廃棄します。このオプションは、デフォルトではイネーブルになっています。たとえば、トラフィック ストームなどで CPU の負荷を軽減するために、発信リセットをディセーブルにすることもできます。
resetoutside	セキュリティ レベルが最も低いインターフェイスで終了し、アクセス リストまたは AAA 設定に基づいてセキュリティ アプライアンスに拒否された TCP パケットのリセットをイネーブルにします。このオプションがイネーブルになっていないと、セキュリティ アプライアンスは拒否されたパケットを通知なしで廃棄します。インターフェイス PAT では、**resetoutside** キーワードを使用することをお勧めします。このキーワードを使用すると、外部の SMTP サーバまたは FTP サーバからの IDENT をセキュリティ アプライアンスで終端することができます。接続をアクティブにリセットすることにより、30 秒のタイムアウト遅延が回避されます。

デフォルト

デフォルトでは、**service resetoutbound** はすべてのインターフェイスでイネーブルになっています。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	**interface** キーワードおよび **resetoutbound** コマンドが追加されました。

使用上のガイドライン　識別要求（IDENT）接続をリセットする必要がある場合、着信トラフィックのリセットを明示的に送信することもできます。TCP RST（TCP ヘッダー内のリセット フラグ）を拒否されたホストに送信すると、RST により着信 IDENT プロセスが停止し、IDENT がタイムアウトになるまで待つ必要がなくなります。IDENT のタイムアウトを待っていると、トラフィックが遅くなることがあります。これは、IDENT がタイムアウトになるまで外部ホストが SYN の再送信を続けるためで、**service resetinbound** コマンドを使用するとパフォーマンスが向上することがあります。

例　次の例では、内部インターフェイスを除くすべてのインターフェイスで発信リセットをディセーブルにしています。

```
hostname(config)# no service resetoutbound
hostname(config)# service resetoutbound interface inside
```

次の例では、DMZ インターフェイスを除くすべてのインターフェイスで着信リセットをイネーブルにしています。

```
hostname(config)# service resetinbound
hostname(config)# no service resetinbound interface dmz
```

次の例では、外部インターフェイス上で終了した接続のリセットをイネーブルにしています。

```
hostname(config)# service resetoutside
```

関連コマンド

コマンド	説明
show running-config service	サービス コンフィギュレーションを表示します。

service password-recovery

パスワードの回復をイネーブルにするには、グローバル コンフィギュレーション モードで **service password-recovery** コマンドを使用します。パスワードの回復をディセーブルにするには、このコマンドの **no** 形式を使用します。パスワードの回復は、デフォルトではイネーブルになっています。ただし、不正なユーザがパスワードの回復メカニズムを利用してセキュリティ アプライアンスのセキュリティを侵害しないようにするために、この機能はディセーブルにすることをお勧めします。

service password-recovery

no service password-recovery

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

パスワードの回復は、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、パスワードを忘れた場合、起動中にプロンプトに従って端末キーボードの **Esc** キーを押すことで、セキュリティ アプライアンスで ROMMON に入ることができます。次に、コンフィギュレーション レジスタを変更して、スタートアップ コンフィギュレーションを無視するようにセキュリティ アプライアンスを設定します（**config-register** コマンドを参照）。たとえば、コンフィギュレーション レジスタがデフォルトの 0x1 である場合は、**confreg 0x41** コマンドを入力して、値を 0x41 に変更します。セキュリティ アプライアンスをリロードするとデフォルト コンフィギュレーションがロードされるので、デフォルトのパスワードを使用して特権 EXEC モードに入ることができます。次に、スタートアップ コンフィギュレーションを実行コンフィギュレーションにコピーして、スタートアップ コンフィギュレーションをロードし、パスワードをリセットします。最後に、コンフィギュレーション レジスタを元の設定に戻して、以前と同様にブートするようにセキュリティ アプライアンスを設定します。たとえば、グローバル コンフィギュレーション モードで **config-register 0x1** コマンドを入力します。

PIX 500 シリーズ セキュリティ アプライアンスの場合は、起動中にプロンプトに従って端末キーボードの **Esc** キーを押して、セキュリティ アプライアンスで監視モードに入ります。次に、PIX パスワード ツールをセキュリティ アプライアンスにダウンロードします。このツールは、すべてのパスワードと **aaa authentication** コマンドを消去します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、**no service password-recovery** コマンドを使用すると、ユーザが設定目的で ROMMON に入ることを防止できます。ユーザが ROMMON に入ると、セキュリティ アプライアンスはすべてのフラッシュ ファイル システムを消去するようにユーザに要求します。ユーザは、最初にこの消去操作を実行しない限り、ROMMON に入ることができません。ユーザがフラッシュ ファイル システムを消去しない場合、セキュリティ アプライアンスはリロードします。パスワードの回復では、ROMMON を使用すること、および既存のコンフィギュレーションを維持することが必要になるため、この消去操作を実行するとパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態まで回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。**service password-recovery** コマンドがコンフィギュレーション ファイルに表示されるのは、情報の提供のみを目的としています。このコマンドを CLI プロンプトで入力すると、設定は NVRAM に保存されます。この設定を変更する唯一の方法は、このコマンドを CLI プロンプトで入力することです。このコマンドの別のバージョンを使用する新しいコンフィギュレーションをロードしても、設定は変更されません。（パスワードの回復に備えて）起動時にスタートアップ コンフィギュレーションを無視するようにセキュリティ アプライアンスを設定している場合は、パスワードの回復をディセーブルにすると、セキュリティ アプライアンスは設定を変更してスタートアップ コンフィギュレーションを通常どおりブートします。フェールオーバーを使用している場合、スタートアップ コンフィギュレーションを無視するようにスタンバイ装置を設定すると、**no service password recovery** コマンドがスタンバイ装置に複製されるときに、同じ変更がコンフィギュレーション レジスタに対して行われます。

PIX 500 シリーズ セキュリティ アプライアンス上で **no service password-recovery** コマンドを使用した場合は、PIX パスワード ツールを実行すると、ユーザはすべてのフラッシュ ファイル システムを消去するように要求されます。ユーザは、最初にこの消去操作を実行しない限り、PIX パスワード ツールを使用することができません。ユーザがフラッシュ ファイル システムを消去しない場合、セキュリティ アプライアンスはリロードします。パスワードの回復では、既存のコンフィギュレーションを維持することが必要になるため、この消去操作を実行するとパスワードを回復できなくなります。ただし、パスワードを回復できなくすることで、不正なユーザがコンフィギュレーションを表示したり、別のパスワードを挿入したりすることがなくなります。この場合、システムを動作可能な状態まで回復するには、新しいイメージとバックアップ コンフィギュレーション ファイル（入手できる場合）をロードします。

例

次の例では、ASA 5500 シリーズ適応型セキュリティ アプライアンスでパスワードの回復をディセーブルにしています。

```
hostname(config)# no service password-recovery
WARNING: Executing "no service password-recovery" has disabled the password recovery
mechanism and disabled access to ROMMON.  The only means of recovering from lost or
forgotten passwords will be for ROMMON to erase all file systems including
configuration files and images.  You should make a backup of your configuration and
have a mechanism to restore images from the ROMMON command line.
```

次の例では、PIX 500 シリーズ セキュリティ アプライアンスでパスワードの回復をディセーブルにしています。

```
hostname(config)# no service password-recovery
WARNING: Saving "no service password-recovery" in the startup-config will disable
password recovery via the npdisk application.  The only means of recovering from lost
or forgotten passwords will be for npdisk to erase all file systems including
configuration files and images.  You should make a backup of your configuration and
have a mechanism to restore images from the Monitor Mode command line.
```

次の例は、ASA 5500 シリーズ適応型セキュリティ アプライアンス上で起動時に ROMMON に入るタイミングと、パスワードの回復操作を完了する方法を示しています。

```
Use BREAK or ESC to interrupt boot.
Use SPACE to begin boot immediately.
Boot interrupted.


Use ? for help.
rommon #0> confreg

Current Configuration Register: 0x00000001
Configuration Summary:
  boot default image from Flash

Do you wish to change this configuration? y/n [n]: n

rommon #1> confreg 0x41

Update Config Register (0x41) in NVRAM...

rommon #2> boot
Launching BootLoader...
Boot configuration file contains 1 entry.


Loading disk0:/ASA_7.0.bin... Booting...
####################
...
Ignoring startup configuration as instructed by configuration register.
Type help or '?' for a list of available commands.
hostname> enable
Password:
hostname# configure terminal
hostname(config)# copy startup-config running-config

Destination filename [running-config]?
Cryptochecksum(unchanged): 7708b94c e0e3f0d5 c94dde05 594fbee9

892 bytes copied in 6.300 secs (148 bytes/sec)
hostname(config)# enable password NewPassword
hostname(config)# config-register 0x1
```

関連コマンド

コマンド	説明
config-register	リロード時にスタートアップ コンフィギュレーションを無視するようにセキュリティ アプライアンスを設定します。
enable password	イネーブル パスワードを設定します。
password	ログイン パスワードを設定します。

service-policy

すべてのインターフェイス上でグローバルに、または必要なインターフェイス上でポリシー マップをアクティブにするには、グローバル コンフィギュレーション モードで ***service-policy*** コマンドを使用します。サーバ ポリシーをディセーブルにするには、このコマンドの **no** 形式を使用します。インターフェイス上で一連のポリシーをイネーブルにするには、***service-policy*** コマンドを使用します。

service-policy *policymap_name* [**global** | **interface** *intf*]

no service-policy *policymap_name* [**global** | **interface** *intf*]

シンタックスの説明

policymap_name	**policy-map** コマンドで設定したポリシー マップ名を指定します。レイヤ 3/4 ポリシー マップのみ指定でき、検査ポリシー マップは指定できません（**policy-map type inspect**）。
global	ポリシー マップをすべてのインターフェイスに適用します。
interface *intf*	ポリシー マップを特定のインターフェイスに適用します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス サービス ポリシーはグローバル サービス ポリシーよりも優先されます。

デフォルトでは、コンフィギュレーションに、すべてのデフォルト アプリケーション検査トラフィックと一致し、検査をグローバルにトラフィックに適用するグローバル ポリシーが含まれます。適用できるグローバル ポリシーは 1 つのみです。このため、グローバル ポリシーの内容を変更する場合は、デフォルトのポリシーを編集するか、ディセーブルにして新しいものを適用する必要があります。

デフォルトのサービス ポリシーには、次のコマンドが含まれます。

```
service-policy global_policy global
```

例

次の例では、inbound_policy ポリシー マップを外部インターフェイスでイネーブルにする方法を示します。

```
hostname(config)# service-policy inbound_policy interface outside
```

次のコマンドは、デフォルトのグローバル ポリシーをディセーブルにし、new_global_policy という新しいポリシーを他のすべてのセキュリティ アプライアンス インターフェイスでイネーブルにします。

```
hostname(config)# no service-policy global_policy global
hostname(config)# service-policy new_global_policy global
```

関連コマンド

コマンド	説明
show service-policy	サービス ポリシーを表示します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。
clear service-policy	サービス ポリシーの統計情報を消去します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションを消去します。

session

AIP SSM または CSC SSM などのインテリジェント SSM への Telnet セッションを確立するには、特権 EXEC モードで **session** コマンドを使用します。

session *slot* [***do*** | ***ip***]

シンタックスの説明

do	*slot* 引数で指定された SSM 上でコマンドを実行します。Cisco TAC から指示がない限り、***do*** キーワードは使用しないでください。
ip	*slot* 引数で指定された SSM の IP アドレスのロギングを設定します。Cisco TAC から指示がない限り、***ip*** キーワードは使用しないでください。
slot	SSM スロット番号を指定します。これは、常に 1 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	***do*** キーワードと ***ip*** キーワードが追加されました。これらのキーワードは、Cisco TAC から指示された場合にのみ使用します。

使用上のガイドライン

このコマンドは、SSM がアップ状態のときにのみ使用できます。状態については、**show module** コマンドを参照してください。

セッションを終了するには、**exit** と入力するか、**Ctrl+Shift+6** キーを押してから **X** キーを押します。

例

次の例では、スロット 1 で SSM へのセッションを確立しています。

```
hostname# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

関連コマンド

コマンド	説明
debug session-command	セッションに関するデバッグ メッセージを表示します。

set connection

トラフィック クラスに関する接続値をポリシー マップ内で指定するには、クラス モードで **set connection** コマンドを使用します。このコマンドは、同時接続の最大数を指定するために、および TCP シーケンス番号のランダム化をイネーブルにするかどうかを指定するために使用します。これらの指定を削除して接続数を無制限にするには、このコマンドの **no** 形式を使用します。

set connection {***conn-max*** *n* | ***embryonic-conn-max*** *n* | ***per-client-embryonic-max*** *n* | ***per-client-max*** *n* | ***random-sequence-number*** {***enable*** | ***disable***}}. . . . .

no set connection {***conn-max*** *n* | ***embryonic-conn-max*** *n* | ***per-client-embryonic-max*** *n* | ***per-client-max*** *n* | ***random-sequence-number*** {***enable*** | ***disable***}}. . . . .

シンタックスの説明

conn-max *n*	（オプション）許容される同時 TCP 接続または同時 UDP 接続の最大数。
disable	TCP シーケンス番号のランダム化をオフにします。
enable	TCP シーケンス番号のランダム化をオンにします。
embryonic-conn-max *n*	（オプション）許容される同時初期接続の最大数。
per-client-embryonic-max *n*	（オプション）許容される同時初期接続の最大数。
per-client-max *n*	（オプション）クライアントごとに許容される同時接続の最大数。
random-sequence-number	（オプション）TCP シーケンス番号のランダム化をイネーブルまたはディセーブルにします。

デフォルト

conn-max、***embryonic-conn-max***、***per-client-embryonic-max***、***per-client-max*** の各パラメータの *n* のデフォルト値は 0 で、接続数は無制限になります。

シーケンス番号のランダム化は、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	***per-client-embryonic-max*** および ***per-client-max*** キーワードが追加されました。

使用上のガイドライン

conn-max、***embryonic-conn-max***、***per-client-embryonic-max***、***per-client-max, random-sequence-number*** キーワードはいずれもオプションですが、少なくとも 1 つは指定する必要があります。

このコマンドに複数のパラメータを入力するか、個別のコマンドに各パラメータを入力することができます。セキュリティ アプライアンスは、実行コンフィギュレーションでこれらのコマンドを 1 行に結合します。たとえば、クラス コンフィギュレーション モードで次の 2 つのコマンドを入力したとします。

```
hostname(config-pmap-c)# set connection conn-max 600
hostname(config-pmap-c)# set connection embryonic-conn-max 50
```

show running-config policy-map コマンドの出力には、2 つのコマンドが 1 つの結合されたコマンドという形で表示されます。

```
set connection conn-max 600 embryonic-conn-max 50
```

set connection コマンドのパラメータ（***conn-max***、***embryonic-conn-max***、***per-client-embryonic-max***、***per-client-max***、***random-sequence-number***）は、任意の **nat** コマンドまたは **static** コマンドと共存できます。つまり、接続パラメータは **nat**/**static** コマンドで ***max-conn***、***emb_limit***、***noramdomseq*** の各パラメータを使用して設定することも、MPC の **set connection** コマンドで ***conn-max***、***embryonic-conn-max***、***per-client-embryonic-max***、***per-client-max***、***random-sequence-number*** の各パラメータを使用して設定することもできます。混合コンフィギュレーションはお勧めしませんが、実際に使用した場合の動作は次のようになります。

- MPC の **set connection** コマンドと **nat**/**static** コマンドの両方でトラフィック クラスが接続制限または初期接続制限を課されている場合は、いずれか一方の制限値に達したときに、その制限値が適用されます。
- MPC の **set connection** コマンドまたは **nat**/**static** コマンドのいずれかで、シーケンス番号のランダム化をディセーブルにするように TCP トラフィック クラスが設定されている場合、シーケンス番号のランダム化はディセーブルになります。

per-client-embryonic-max パラメータおよび ***per-client-max*** パラメータは、クライアントが開くことのできる最大接続数を制限します。特定のクライアントが必要以上に多くのネットワーク リソースを同時に使用する場合、これらのパラメータを使用して、セキュリティ アプライアンスが特定のクライアントに許可する接続数を制限することができます。DoS 攻撃は、基幹ホストに対し接続や接続要求といった過剰な負荷をかけることにより、ネットワークを妨害しようとします。***per-client-embryonic-max*** パラメータおよび ***per-client-max*** パラメータを使用して、DoS 攻撃を防止することができます。攻撃を受ける可能性のあるホストがサポートできる、クライアントごとの最大接続数を設定すると、悪意のあるクライアントは保護されたネットワーク上のホストを攻撃できなくなります。

例

次の例では、**set connection** コマンドを使用して、同時接続の最大数を 256 に、TCP シーケンス番号のランダム化をディセーブルにするように設定しています。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection conn-max 256 random-sequence-number disable
hostname(config-pmap-c)#
```

次の例では、トラフィックを Cisco Content Security and Control（CSC）SSM に転送するサービス ポリシーで **set connection** コマンドを使用しています。**set connection** コマンドは、CSC SSM にトラフィックをスキャンされる各クライアントの接続を最大 5 つに制限します。

```
hostname(config)# policy-map csc_policy
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection per-client-max 5
hostname(config-pmap-c)# csc fail-close
hostname(config-pmap-c)#
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
show service-policy	サービス ポリシーのコンフィギュレーションを表示します。**set connection** コマンドを含むポリシーを表示するには、***set connection*** キーワードを使用します。

set connection advanced-options

トラフィック クラスに関する高度な TCP 接続オプションをポリシー マップ内で指定するには、クラス モードで **set connection advanced-options** コマンドを使用します。トラフィック クラスに関する高度な TCP 接続オプションをポリシー マップから削除するには、クラス モードで、このコマンドの **no** 形式を使用します。

set connection advanced-options *tcp-mapname*

no set connection advanced-options *tcp-mapname*

シンタックスの説明

tcp-mapname	高度な TCP 接続オプションの設定対象となる TCP マップの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを発行するには、TCP マップ名に加えて、**policy-map** コマンドと **class** コマンドをあらかじめ設定しておく必要があります。詳細については、**tcp-map** コマンドの説明を参照してください。

例

次の例では、**set connection advanced-options** コマンドを使用して、localmap という TCP マップを使用することを指定しています。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit
hostname(config)# tcp-map localmap
hostname(config)# policy-map global_policy global
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection advanced-options localmap
hostname(config-pmap-c)#
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
class-map	クラス マップ モードで、多くとも 1 つの match コマンド（tunnel-group と default-inspection-traffic は除く）を発行し、一致基準を指定することによって、トラフィック クラスを設定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

set connection timeout

アイドル状態の TCP 接続が切断されるまでのタイムアウト期間を設定するには、クラス コンフィギュレーション モードで **set connection timeout** コマンドを使用します。タイムアウトを削除するには、このコマンドの **no** 形式を使用します。

set connection timeout {**tcp** <*value*> [reset]] [**half-close** <*value*>] [**embryonic** <*value*>] [**dcd** [<retry-interval> [max-retries]]]}

no set connection timeout {**tcp** <*value*> [reset]] [**half-close** <*value*>] [**embryonic** <*value*>] [**dcd** [<retry-interval> [max-retries]]]}

シンタックスの説明

dcd	アイドル タイムアウトになると、DCD プローブを接続エンド ホストに送信して、接続の有効性を判断します。設定されている数の DCD プローブが設定されている間隔で送信された後、エンド ホストのいずれかが応答に失敗した場合、その接続は解放されます。両方のエンド ホストが接続が有効であると応答した場合、アクティビティ タイムアウトが現在の時刻に更新され、それに応じてアイドル タイムアウトのスケジュールも再設定されます。
embryonic	TCP 初期接続が終了するまでの絶対時間を設定します。1 ～ 255（秒）を設定します。この値を 0 に設定して、接続がタイムアウトしないようにすることもできます。
half-closed	TCP ハーフクローズ接続が解放されるまでのアイドル時間を設定します。5 ～ 255（分）を設定します。この値を 0 に設定して、接続がタイムアウトしないようにすることもできます。
max-retries	接続が「無効」と宣言されるまでに連続して失敗したリトライ数です。最小値は 1、最大値は 255 です。
reset	TCP アイドル接続が削除された後に、両端のシステムに TCP RST パケットを送信します。
retry-interval	非応答 DCD プローブ間の待機時間は <hh:mm:ss> 形式で表示します。最小値は 1 秒、最大値は 24 時間です。
tcp	確立済みの接続が終了するまでのアイドル時間です。
value	0:0:5 から 1192:59:59 までの時間（*hh*:*mm*:*ss* 形式）。この値を 0 に設定して、接続がタイムアウトしないようにすることもできます。

デフォルト

デフォルトの ***embryonic*** 値は 30 秒です。

デフォルトの ***half-closed*** 値は 10 分です。

デフォルトの **max-retries** 値は 5 です。

デフォルトの **retry-interval** 値は 15 秒です。

デフォルトの ***tcp*** 値は 1 時間です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
クラス コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	DCD のサポートが追加されました。

使用上のガイドライン

このコマンドを発行するには、**policy-map** コマンドと **class** コマンドをあらかじめ設定しておく必要があります。

「初期」接続とは、3 ウェイ ハンドシェイクの完了していない TCP 接続です。***embryonic*** 接続タイムアウト値には、***0:0:0*** を使用して接続がタイムアウトしないことを指定します。このように指定しない場合は、タイムアウト期間を 5 秒以上に設定する必要があります。

TCP 接続が終了中（CLOSING）状態のときは、half-closed パラメータを使用して、接続が解放されるまでの時間の長さを設定します。接続がタイムアウトしないように指定するには、***0:0:0*** を使用します。最短のタイムアウト期間は 5 分です。

tcp 非アクティブ接続のタイムアウトには、確立済み状態でアイドルになっている TCP 接続が切断されるまでの期間を設定します。接続がタイムアウトしないように指定するには、***0:0:0*** を使用します。最短のタイムアウト期間は 5 分です。

reset キーワードは、アイドル TCP 接続がタイムアウトしたときに両端のシステムに TCP RST パケットを送信する場合に使用します。アプリケーションの中には、タイムアウト後に TCP RST を送信しないと適切に動作しないものがあります。

DCD をイネーブルにすると、TCP ノーマライザにおけるアイドル タイムアウト処理の動作が変わります。Dead Connection Detection（DCD; デッド接続検出）プローブにより、**show conn** コマンドで表示される接続のアイドル タイムアウトがリセットされます。timeout コマンドで設定されているタイムアウト値を超えても、DCD プローブによって接続が維持される期間を判断するために、**show service-policy** コマンドには、DCD からアクティビティ量を表示するためのカウンタがあります。

例

次の **set connection timeout** コマンドの例では、初期接続のタイムアウトとして 2 分を指定しています。

```
ASA Version 7.2(0)80
!
hostname ciscoasa
domain-name default.domain.invalid
enable password 8Ry2YjIyt7RRXU24 encrypted
names
!
interface Vlan1
 nameif inside
 security-level 100
 ip address 192.168.0.1 255.255.0.0 standby 192.168.0.2
!
interface Vlan2
 backup interface Vlan4
 nameif outside
 security-level 0
 ip address 17.12.9.1 255.255.0.0 standby 17.12.9.2
!
interface Vlan4
 nameif backifx
 security-level 0
 ip address 172.23.62.137 255.255.255.0 standby 172.23.62.136
!
interface Vlan150
 description LAN Failover Interface
!
interface Vlan160
 nameif dmz
 security-level 50
 ip address 172.16.0.1 255.255.0.0 standby 172.16.0.2
!
interface Ethernet0/0
 switchport access vlan 2
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/1
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/2
 switchport access vlan 160
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/3
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/4
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/5
 switchport access vlan 150
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/6
```

```
 switchport access vlan 4
 no nameif
 no security-level
 no ip address
!
interface Ethernet0/7
 switchport access vlan 4
 no nameif
 no security-level
 no ip address
!
passwd 2KFQnbNIdI.2KYOU encrypted
boot system disk0:/cdisk.7.2.0.80
ftp mode passive
dns server-group DefaultDNS
 domain-name default.domain.invalid
access-list outside-acl extended permit ip any any
access-list inside_nat0_outbound extended permit ip any 192.168.0.128 255.255.25
5.192
access-list outside_cryptomap extended permit ip any 192.168.0.128 255.255.255.1
92
pager lines 24
logging enable
logging buffered debugging
logging asdm informational
mtu inside 1500
mtu outside 1500
mtu backifx 1500
mtu dmz 1500
ip local pool vpnpool 192.168.0.150-192.168.0.160 mask 255.255.0.0
no failover
failover lan unit primary
failover lan interface fover Vlan150
failover interface ip fover 150.1.1.1 255.255.255.0 standby 150.1.1.2
asdm image disk0:/asdm-5211.bin
no asdm history enable
arp timeout 14400
nat-control
global (outside) 1 interface
nat (inside) 1 0.0.0.0 0.0.0.0
static (inside,outside) 17.12.9.51 192.168.0.3 netmask 255.255.255.255
static (inside,outside) 17.12.9.52 192.168.0.10 netmask 255.255.255.255
static (inside,outside) 17.12.9.54 192.168.0.4 netmask 255.255.255.255
static (inside,dmz) 172.16.0.13 192.168.0.3 netmask 255.255.255.255
static (inside,dmz) 172.16.0.14 192.168.0.100 netmask 255.255.255.255
static (dmz,outside) 17.12.9.53 172.16.0.20 netmask 255.255.255.255
access-group outside-acl in interface outside
access-group outside-acl in interface dmz
route outside 0.0.0.0 0.0.0.0 17.12.0.1 1 track 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02      ------------>
ramain same
timeout sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00
timeout sip 0:30:00 sip_media 0:02:00 sip-invite 0:03:00 sip-disconnect 0:02:00
timeout uauth 0:05:00 absolute
group-policy vpngroup internal
group-policy vpngroup attributes
 wins-server value 171.69.2.87
 dns-server value 171.70.168.183
 vpn-tunnel-protocol IPSec
 default-domain value cisco.com
username snoopy password wQO7//ZyQYDXv5q. encrypted privilege 15
aaa authentication telnet console LOCAL
http server enable
http 0.0.0.0 0.0.0.0 outside
http 0.0.0.0 0.0.0.0 inside
http 192.168.0.0 255.255.0.0 inside
no snmp-server location
no snmp-server contact
```

```
snmp-server enable traps snmp authentication linkup linkdown coldstart
sla monitor 10
 type echo protocol ipIcmpEcho 17.12.0.1 interface outside
 frequency 5
sla monitor schedule 10 life forever start-time now
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-sha-hmac
crypto dynamic-map outside0 20 set transform-set ESP-3DES-SHA
crypto map outside 20 ipsec-isakmp dynamic outside0
crypto map outside interface outside
crypto isakmp enable outside
crypto isakmp policy 10
 authentication pre-share
 encryption 3des
 hash sha
 group 2
 lifetime 86400
!
track 1 rtr 10 reachability
tunnel-group vpngroup type ipsec-ra
tunnel-group vpngroup general-attributes
 address-pool vpnpool
 default-group-policy vpngroup
tunnel-group vpngroup ipsec-attributes
 pre-shared-key *
telnet 0.0.0.0 0.0.0.0 inside
telnet 0.0.0.0 0.0.0.0 outside
telnet timeout 5
ssh timeout 5
console timeout 0

!
class-map dcd
 match access-list outside-acl
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map type inspect dns preset_dns_map
 parameters
  message-length maximum 512
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect rsh
  inspect rtsp
  inspect esmtp
  inspect sqlnet
  inspect skinny
  inspect sunrpc
  inspect xdmcp
  inspect sip
  inspect netbios
  inspect tftp
  inspect icmp
 class dcd
  set connection timeout dcd
!
service-policy global_policy global
tftp-server outside 17.12.9.152 test1.cfg
prompt hostname context
Cryptochecksum:dc412a5fe2003621d7d723420da6e8d5
: end
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。
show service-policy	DCD のカウンタおよびその他のサービス アクティビティを表示します。

set metric

ルーティング プロトコルにメトリック値を設定するには、ルートマップ コンフィギュレーション モードで **set metric** コマンドを使用します。デフォルトのメトリック値に戻すには、このコマンドの **no** 形式を使用します。

set metric *value*

no set metric *value*

シンタックスの説明

value	メトリック値。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルートマップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

no set metric *value* コマンドを使用すると、デフォルトのメトリック値に戻すことができます。この場合の *value* は、0 ～ 4294967295 の整数です。

例

次の例は、OSPF ルーティングで使用するルートマップを設定する方法を示しています。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
set metric 5
match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したいずれかのアクセス リストによって渡されたネクストホップ ルータ アドレスを持つ、すべてのルートを配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。

set metric-type

OSPF メトリック ルートのタイプを指定するには、ルートマップ コンフィギュレーション モードで **set metric-type** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

set metric-type {**type-1** | **type-2**}

no set metric-type

シンタックスの説明

type-1	指定した自律システム外部の OSPF メトリック ルートのタイプを指定します。
type-2	指定した自律システム外部の OSPF メトリック ルートのタイプを指定します。

デフォルト

デフォルトは **type-2** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルートマップ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、OSPF ルーティングで使用するルートマップを設定する方法を示しています。

```
hostname(config)# route-map maptag1 permit 8
hostname(config-route-map)# set metric 5
hostname(config-route-map)# match metric 5
hostname(config-route-map)# set metric-type type-2
hostname(config-route-map)# show route-map
route-map maptag1 permit 8
  set metric 5
  set metric-type type-2
  match metric 5
hostname(config-route-map)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクストホップを持つ、すべてのルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。
set metric	ルートマップの宛先ルーティング プロトコルのメトリック値を指定します。

setup

対話型のプロンプトを使用して、セキュリティ アプライアンスの最小限のコンフィギュレーションを設定するには、グローバル コンフィギュレーション モードで **setup** コマンドを入力します。このコンフィギュレーションによって、ASDM を使用するための接続が提供されます。デフォルトのコンフィギュレーションに戻すには、**configure factory-default** コマンドも参照してください。

setup

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

フラッシュ メモリ内にスタートアップ コンフィギュレーションが存在しない場合、ブート時にセットアップ ダイアログが自動的に表示されます。

setup コマンドを使用するには、内部インターフェイスをあらかじめ設定しておく必要があります。PIX 500 シリーズのデフォルト コンフィギュレーションには、内部インターフェイス（Ethernet 1）が含まれていますが、ASA 550 シリーズのデフォルト コンフィギュレーションには含まれていません。**setup** コマンドを使用する前に、内部インターフェイスにするインターフェイスについて、**interface** コマンドを入力し、次に **nameif inside** コマンドを入力しておく必要があります。

マルチ コンテキスト モードでは、システム実行スペース内で、および各コンテキストに対して **setup** コマンドを使用できます。

setup コマンドを入力すると、表 24-1 に示す情報の入力を要求されます。システムの **setup** コマンドには、これらのプロンプトのサブセットが含まれています。要求されたパラメータに対するコンフィギュレーションがすでに存在している場合は、そのコンフィギュレーションが（）で囲まれて表示されます。このコンフィギュレーションをデフォルトとして受け入れることも、新しいコンフィギュレーションを入力して上書きすることもできます。

表 24-1　setup のプロンプト

プロンプト	説明
`Pre-configure Firewall now through interactive prompts [yes]?`	***yes*** または ***no*** を入力します。**yes** を入力すると、セットアップ ダイアログが続行されます。***no*** を入力した場合、セットアップ ダイアログは停止して、グローバル コンフィギュレーション プロンプト（`hostname(config)#`）が表示されます。
`Firewall Mode [Routed]:`	***routed*** または ***transparent*** を入力します。
`Enable password:`	イネーブル パスワードを入力します。このパスワードは、3 文字以上にする必要があります。
`Allow password recovery [yes]?`	***yes*** または ***no*** を入力します。
`Clock (UTC):`	このフィールドには一切入力できません。デフォルトの UTC 時刻が使用されます。
`Year:`	西暦年を 4 桁で入力します（たとえば、2005）。年の範囲は 1993 ～ 2035 です。
`Month:`	月を表す英単語の先頭 3 文字を使用して、月を入力します。たとえば、**Sep** は 9 月を表します。
`Day:`	1 ～ 31 の日を入力します。
`Time:`	時、分、秒を 24 時間形式で入力します。たとえば、午後 8 時 54 分 44 秒の場合は **20:54:44** と入力します。
`Inside IP address:`	内部インターフェイスの IP アドレスを入力します。
`Inside network mask:`	内部 IP アドレスに適用するネットワーク マスクを入力します。255.0.0.0 や 255.255.0.0 など、有効なネットワーク マスクを指定する必要があります。
`Host name:`	コマンドライン プロンプトに表示するホスト名を入力します。
`Domain name:`	セキュリティ アプライアンスが実行されるネットワークのドメイン名を入力します。
`IP address of host running Device Manager:`	ASDM にアクセスする必要のあるホストの IP アドレスを入力します。
`Use this configuration and write to flash?`	***yes*** または ***no*** を入力します。**yes** と入力すると、内部インターフェイスがイネーブルとなり、要求したコンフィギュレーションがフラッシュ パーティションに書き込まれます。 ***no*** と入力すると、セットアップ ダイアログが繰り返され、最初の質問が開始されます。 `Pre-configure Firewall now through interactive prompts [yes]?` ***no*** を入力してセットアップ ダイアログを終了するか、***yes*** を入力してセットアップ ダイアログを繰り返します。

例

次の例は、**setup** コマンド プロンプトで最後まで作業する方法を示しています。

```
hostname(config)# setup
Pre-configure Firewall now through interactive prompts [yes]? yes
Firewall Mode [Routed]: routed
Enable password [<use current password>]: writer
Allow password recovery [yes]? yes
Clock (UTC):
   Year: 2005
   Month: Nov
   Day: 15
   Time: 10:0:0
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

The following configuration will be used:
Enable password: writer
Allow password recovery: yes
Clock (UTC): 20:54:44 Sep 17 2005
Firewall Mode: Routed
Inside IP address: 192.168.1.1
Inside network mask: 255.255.255.0
Host name: tech_pubs
Domain name: your_company.com
IP address of host running Device Manager: 10.1.1.1

Use this configuration and write to flash? yes
```

関連コマンド

コマンド	説明
configure factory-default	デフォルトのコンフィギュレーションに戻します。

show aaa local user

現在ロックされているユーザ名のリスト、またはユーザ名に関する詳細を表示するには、グローバル コンフィギュレーション モードで **show aaa local user** コマンドを使用します。

show aaa local user [locked]

シンタックスの説明

locked	（オプション）現在ロックされているユーザ名のリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

オプションのキーワード ***locked*** を省略すると、セキュリティ アプライアンスは、すべての AAA ローカル ユーザについて、失敗した試行とロックアウト ステータスの詳細を表示します。

username オプションを使用してユーザを 1 人のみ指定することも、***all*** オプションを使用してすべてのユーザを指定することもできます。

このコマンドは、ロックアウトされているユーザのステータスだけに影響を及ぼします。

管理者は、デバイスからロックアウトされません。

例

次の例では、**show aaa local user** コマンドを使用して、すべてのユーザ名のロックアウト ステータスを表示しています。

この例では、認証失敗の上限を 5 回に設定した後で、**show aaa local user** コマンドを使用して、すべての AAA ローカル ユーザについて認証の失敗回数とロックアウト ステータスの詳細を表示しています。

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
    -                   2       N       mona
    -                   1       N       cisco
    -                   4       N       newuser
hostname(config)#
```

次の例では、認証失敗の上限を 5 回に設定した後で、**show aaa local user** コマンドを ***lockout*** キーワード付きで使用して、ロックアウトされたすべての AAA ローカル ユーザについて、認証の失敗回数とロックアウト ステータスの詳細を表示しています。

```
hostname(config)# aaa local authentication attempts max-fail 5
hostname(config)# show aaa local user
Lock-time  Failed-attempts      Locked  User
    -                   6       Y       test
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	正しくないパスワードの入力を何回まで許容するかを設定します。この回数を超えると、ユーザはロックアウトされます。
clear aaa local user fail-attempts	試行の失敗回数を 0 にリセットします。ロックアウト ステータスは変更しません。
clear aaa local user lockout	指定したユーザまたはすべてのユーザのロックアウト ステータスを消去し、試行失敗のカウンタを 0 に設定します。

show aaa-server

AAA サーバに関する統計情報を表示するには、特権 EXEC モードで **show aaa-server** コマンドを使用します。

show aaa-server [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

シンタックスの説明

LOCAL	（オプション）LOCAL ユーザ データベースの統計情報を表示します。
groupname	（オプション）グループに含まれているサーバの統計情報を表示します。
host *hostname*	（オプション）グループに含まれている特定のサーバの統計情報を表示します。
protocol *protocol*	（オプション）指定したプロトコルのサーバの統計情報を表示します。 • **http form** • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

デフォルトでは、すべての AAA サーバの統計情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.1(1)	http 形式のプロトコルが追加されました。

例

次の例では、**show aaa-server** コマンドを使用して、サーバグループ group1 に含まれている特定のホストの統計情報を表示しています。

```
hostname(config)# show aaa-server group1 host 192.68.125.60
Server Group:          group1
Server Protocol:       RADIUS
Server Address:       192.68.125.60
Server port:        1645
Server status:     ACTIVE/FAILED. Last transaction (success) at 11:10:08 UTC  Fri Aug 22
Number of pending requests 20
Average round trip time4ms
Number of authentication requests20
Number of authorization requests 0
Number of accounting requests 0
Number of retransmissions1
Number of accepts  16
Number of rejects  4
Number of challenges   5
Number of malformed responses0
Number of bad authenticators0
Number of pending requests0
Number of timeouts 0
Number of unrecognized responses0
hostname(config)#
```

次の例では、**show aaa-server** コマンドを使用して、非アクティブな小規模システムに含まれているすべてのホストの統計情報を表示しています。

```
hostname(config)# show aaa-server
Server Group:      LOCAL
Server Protocol:   Local database
Server Address:    None
Server port:       None
Server status:     ACTIVE, Last transaction at unknown
Number of pending requests        0
Average round trip time           0ms
Number of authentication requests 0
Number of authorization requests  0
Number of accounting requests     0
Number of retransmissions         0
Number of accepts                 0
Number of rejects                 0
Number of challenges              0
Number of malformed responses     0
Number of bad authenticators      0
Number of timeouts                0
Number of unrecognized responses  0
hostname(config)#
```

関連コマンド

show running-config aaa-server	指定したサーバグループに含まれているすべてのサーバ、または特定のサーバの統計情報を表示します。
clear aaa-server statistics	AAA サーバの統計情報を消去します。

show access-list

アクセス リストのカウンタを表示するには、特権 EXEC モードで **show access-list** コマンドを使用します。

show access-list *id*

シンタックスの説明

id	アクセス リストを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show access-list** コマンドの出力例を示します。

```
hostname# show access-list
access-list cached ACL log flows: total 0, denied 0 (deny-flow-max 4096)
             alert-interval 300
access-list 101; 10 elements
access-list 101 line 1 extended permit tcp any eq www any (hitcnt=0) 0xa14fc533
access-list 101 line 2 extended permit tcp any eq www any eq www (hitcnt=0) 0xaa73834e
access-list 101 line 3 extended permit tcp any eq www any range telnet www (hitcnt=0)
0x49ac02e6
access-list 101 line 4 extended permit tcp any range telnet www any range telnet www
(hitcnt=0) 0xa0021a9f
access-list 101 line 5 extended permit udp any range biff www any (hitcnt=0)
0xf89a7328
access-list 101 line 6 extended permit udp any lt ntp any (hitcnt=0) 0x8983c43
access-list 101 line 7 extended permit udp any any lt ntp (hitcnt=0) 0xf361ffb6
access-list 101 line 8 extended permit udp any any range ntp biff (hitcnt=0) 0x219581
access-list 101 line 9 extended permit icmp any any (hitcnt=0) 0xe8fa08e1
access-list 101 line 10 extended permit icmp any any echo (hitcnt=0) 0x2eb8deea
access-list 102; 1 elements access-list 102 line 1 extended permit icmp any any echo
(hitcnt=0) 0x59e2fea8
```

この出力では、各行の最後に個々のアクセス コントロール エントリに対する独自の 16 進数の識別子が含まれています。

関連コマンド

コマンド	説明
access-list ethertype	トラフィックを EtherType に基づいて制御するためのアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
clear access-list	アクセス リスト カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。
show running-config access-list	現在実行しているアクセス リスト コンフィギュレーションを表示します。

show activation-key

アクティベーション キーによってイネーブルになった機能のコンフィギュレーションに含まれているコマンドを、許容されているコンテキストの数を含めて表示するには、特権 EXEC モードで **show activation-key** コマンドを使用します。

show activation-key

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
PIX バージョン 7.0	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

show activation-key コマンドの出力で示されるアクティベーション キーのステータスは、次のとおりです。

- セキュリティ アプライアンスのフラッシュ ファイル システムにあるアクティベーション キーが、セキュリティ アプライアンスで機能しているアクティベーション キーと同じものである場合、**show activation-key** コマンドの出力は次のようになります。

```
The flash activation key is the SAME as the running key.
```

- セキュリティ アプライアンスのフラッシュ ファイル システムにあるアクティベーション キーが、セキュリティ アプライアンスで機能しているアクティベーション キーと異なるものである場合、**show activation-key** コマンドの出力は次のようになります。

```
The flash activation key is DIFFERENT from the running key.
The flash activation key takes effect after the next reload.
```

- アクティベーション キーをダウングレードする場合は、機能しているキー（古いキー）が、フラッシュに格納されているキー（新しいキー）と異なっていることが表示されます。セキュリティ アプライアンスを再起動すると、新しいキーが使用されます。
- キーをアップグレードして追加の機能をイネーブルにする場合、新しいキーはすぐに機能し始めます。再起動する必要はありません。
- PIX Firewall プラットフォームでは、新しいキーと古いキーでフェールオーバー機能（R/UR/FO）に違いがある場合、確認するように要求されます。ユーザが ***n*** を入力すると、変更内容は破棄されます。その他の場合は、フラッシュ ファイル システムに格納されているキーがアップデートされます。セキュリティ アプライアンスを再起動すると、新しいキーが使用されます。

例

次の例は、アクティベーション キーによってイネーブルになった機能のコンフィギュレーションに含まれているコマンドを表示する方法を示しています。

```
hostname(config)# show activation-key
Serial Number:  P3000000134 Running Activation Key: 0xyadayada 0xyadayada 0xyadayada
0xyadayada 0xyadayada

License Features for this Platform:
Maximum Physical Interfaces : Unlimited
Maximum VLANs               : 50
Inside Hosts                : Unlimited
Failover                    : Enabled
VPN-DES                     : Enabled
VPN-3DES-AES                : Disabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL-filtering               : Enabled
Security Contexts           : 20
GTP/GPRS                    : Disabled
VPN Peers                   : 5000

The flash activation key is the SAME as the running key.
hostname(config)#
```

関連コマンド

コマンド	説明
activation-key	アクティベーション キーを変更します。

show admin-context

管理コンテキストとして現在割り当てられているコンテキストの名前を表示するには、特権 EXEC モードで **show admin-context** コマンドを使用します。

show admin-context

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show admin-context** コマンドの出力例を示します。この例では、flash のルート ディレクトリに格納されている「admin」という管理コンテキストが表示されています。

```
hostname# show admin-context
Admin: admin flash:/admin.cfg
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
clear configure context	すべてのコンテキストを削除します。
mode	コンテキスト モードをシングルまたはマルチに設定します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

show arp

アドレス解決プロトコル（ARP）テーブルを表示するには、特権 EXEC モードで **show arp** コマンドを使用します。このコマンドは、ダイナミック ARP エントリと手作業で設定した ARP エントリを表示しますが、各エントリの作成元は示しません。

show arp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show arp** コマンドの出力例を示します。

```
hostname# show arp
        inside 10.86.195.205 0008.023b.9892
        inside 10.86.194.170 0001.023a.952d
        inside 10.86.194.172 0001.03cf.9e79
        inside 10.86.194.1 00b0.64ea.91a2
        inside 10.86.194.146 000b.fcf8.c4ad
        inside 10.86.194.168 000c.ce6f.9b7e
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報を消去します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp-inspection

各インターフェイスの ARP 検査設定を表示するには、特権 EXEC モードで **show arp-inspection** コマンドを使用します。

show arp-inspection

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show arp-inspection** コマンドの出力例を示します。

```
hostname# show arp-inspection
interface                arp-inspection         miss
-----------------------------------------------------
inside1                  enabled                flood
outside                  disabled                -
```

miss カラムは、ARP 検査がイネーブルになっている場合に、一致しないパケットに対して実行するデフォルト アクション（flood または no-flood）を示しています。

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報を消去します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show arp statistics

ARP 統計情報を表示するには、特権 EXEC モードで show arp statistics コマンドを使用します。

show arp statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show arp statistics** コマンドの出力例を示します。

```
hostname# show arp statistics
        Number of ARP entries:
        ASA : 6
        Dropped blocks in ARP: 6
        Maximum Queued blocks: 3
        Queued blocks: 1
        Interface collision ARPs Received: 5
        ARP-defense Gratuitous ARPS sent: 4
        Total ARP retries: 15
        Unresolved hosts: 1
        Maximum Unresolved hosts: 2
```

表 24-2 に、各フィールドの説明を示します。

表 24-2　show arp statistics のフィールド

フィールド	説明
Number of ARP entries	ARP テーブル エントリの合計数。
Dropped blocks in ARP	IP アドレスが対応するハードウェア アドレスに解決されている間に、ドロップされたブロックの数。
Maximum queued blocks	IP アドレスが解決されるまで待機している間に、ARP モジュールのキューに入れられたブロックの最大数。
Queued blocks	ARP モジュールのキューに現在入っているブロックの数。
Interface collision ARPs received	すべてのセキュリティ アプライアンス インターフェイス上で、セキュリティ アプライアンス インターフェイスと同じ IP アドレスから受信した ARP パケットの数。

表 24-2　show arp statistics のフィールド（続き）

フィールド	説明
ARP-defense gratuitous ARPs sent	セキュリティ アプライアンスによって、ARP 防御メカニズムの一部として送信された gratuitous ARP の数。
Total ARP retries	最初の ARP 要求でアドレスが解決されなかった場合に、ARP モジュールによって送信された ARP 要求の合計数。
Unresolved hosts	ARP モジュールによってまだ ARP 要求が送信されている、未解決ホストの数。
Maximum unresolved hosts	未解決ホストが最後に消去された時点、またはセキュリティ アプライアンスがブートアップされた時点から、ARP モジュール内で未解決となったホスト数の最大値。

関連コマンド

コマンド	説明
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
clear arp statistics	ARP 統計情報を消去し、値を 0 にリセットします。
show arp	ARP テーブルを表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

show asdm history

ASDM 履歴バッファの内容を表示するには、特権 EXEC モードで **show asdm history** コマンドを使用します。

show asdm history [***view*** *timeframe*] [***snapshot***] [***feature*** *feature*] [***asdmclient***]

シンタックスの説明

asdmclient	（オプション）ASDM クライアント用に整形された ASDM 履歴データを表示します。
feature *feature*	（オプション）履歴の表示対象を指定された機能に限定します。次に、*feature* 引数で有効となる値を示します。 • ***all***：すべての機能の履歴を表示します（デフォルト）。 • ***blocks***：システム バッファの履歴を表示します。 • ***cpu***：CPU 使用率の履歴を表示します。 • ***failover***：フェールオーバーの履歴を表示します。 • ***ids***：IDS の履歴を表示します。 • ***interface*** *if_name*：指定したインターフェイスの履歴を表示します。*if_name* 引数は、**nameif** コマンドで指定したインターフェイス名です。 • ***memory***：メモリ使用率の履歴を表示します。 • ***perfmon***：パフォーマンスの履歴を表示します。 • ***sas***：セキュリティ結合の履歴を表示します。 • ***tunnels***：トンネルの履歴を表示します。 • ***xlates***：変換スロットの履歴を表示します。
snapshot	（オプション）ASDM 履歴の最新データ ポイントだけを表示します。
view *timeframe*	（オプション）履歴の表示対象を指定された期間に限定します。次に、*timeframe* 引数で有効となる値を示します。 • ***all***：履歴バッファのすべての内容（デフォルト） • ***12h***：12 時間 • ***5d***：5 日間 • ***60m***：60 分間 • ***10m***：10 分間

デフォルト

引数もキーワードも指定しない場合は、すべての機能のすべての履歴情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm history** コマンドから **show asdm history** コマンドに変更されました。

使用上のガイドライン

show asdm history コマンドは、ASDM 履歴バッファの内容を表示します。ASDM 履歴情報を表示するには、**asdm history enable** コマンドを使用して、ASDM 履歴のトラッキングをあらかじめイネーブルにしておく必要があります。

例

次に、**show asdm history** コマンドの出力例を示します。ここでは、出力する内容を外部インターフェイスに関する最近 10 分間に収集されたデータに限定しています。

```
hostname# show asdm history view 10m feature interface outside

Input KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 62640 62636 62633 62628 62622 62616 62609
Output KByte Count:
        [  10s:12:46:41 Mar 1 2005  ] 25178 25169 25165 25161 25157 25151 25147
Input KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]   752   752   751   751   751   751   751
Output KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]    55    55    55    55    55    55    55
Input Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  3397  2843  3764  4515  4932  5728  4186
Output Bit Rate:
        [  10s:12:46:41 Mar 1 2005  ]  7316  3292  3349  3298  5212  3349  3301
Input Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     5     4     6     7     6     8     6
Output Packet Rate:
        [  10s:12:46:41 Mar 1 2005  ]     1     0     0     0     0     0     0
Input Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
No Buffer:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Received Broadcasts:
        [  10s:12:46:41 Mar 1 2005  ] 375974 375954 375935 375902 375863 375833 375794
Runts:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Giants:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
CRC:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Frames:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Overruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Underruns:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Output Error Packet Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Collisions:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
LCOLL:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Reset:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Deferred:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Lost Carrier:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]   128   128   128   128   128   128   128
Software Input Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Hardware Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Software Output Queue:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
Drop KPacket Count:
        [  10s:12:46:41 Mar 1 2005  ]     0     0     0     0     0     0     0
hostname#
```

次に、**show asdm history** コマンドの出力例を示します。上の例と同様に、出力する内容を外部インターフェイスに関する最近 10 分間に収集されたデータに限定しています。ただし、この例では出力を ASDM クライアント用に整形しています。

```
hostname# show asdm history view 10m feature interface outside asdmclient

MH|IBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|62439|62445|62453|62457|624
64|62469|62474|62486|62489|62496|62501|62506|62511|62518|62522|62530|62534|62539|62542
|62547|62553|62556|62562|62568|62574|62581|62585|62593|62598|62604|62609|62616|62622|6
2628|62633|62636|62640|62653|62657|62665|62672|62678|62681|62686|62691|62695|62700|627
04|62711|62718|62723|62728|62733|62738|62742|62747|62751|62761|62770|62775|
MH|OBC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|25023|25023|25025|25025|250
25|25026|25026|25032|25038|25044|25052|25056|25060|25064|25070|25076|25083|25087|25091
|25096|25102|25106|25110|25114|25118|25122|25128|25133|25137|25143|25147|25151|25157|2
5161|25165|25169|25178|25321|25327|25332|25336|25341|25345|25349|25355|25359|25363|253
67|25371|25375|25381|25386|25390|25395|25399|25403|25410|25414|25418|25422|
MH|IPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|749|749|749|749|749|750|750
|750|750|750|750|750|750|750|750|750|750|750|750|750|751|751|751|751|751|751|751|751|7
51|751|751|751|751|751|751|752|752|752|752|752|752|752|752|752|752|752|752|752|752|753
|753|753|753|753|753|753|753|753|753|753|
MH|OPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|55|55|55|55|55|55|55|55|55|
55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55|55
|55|55|55|55|55|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|56|
MH|IBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|7127|5155|6202|3545|5408|39
79|4381|9492|3033|4962|4571|4226|3760|5923|3265|6494|3441|3542|3162|4076|4744|2726|484
7|4292|5401|5166|3735|6659|3837|5260|4186|5728|4932|4515|3764|2843|3397|10768|3080|630
9|5969|4472|2780|4492|3540|3664|3800|3002|6258|5567|4044|4059|4548|3713|3265|4159|3630
|8235|6934|4298|
MH|OBR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|82791|57|1410|588|57|639|0|
4698|5068|4992|6495|3292|3292|3352|5061|4808|5205|3931|3298|3349|5064|3439|3356|3292|3
343|3349|5067|3883|3356|4500|3301|3349|5212|3298|3349|3292|7316|116896|5072|3881|3356|
3931|3298|3349|5064|3292|3349|3292|3292|3349|5061|3883|3356|3931|3452|3356|5064|3292|3
349|3292|
MH|IPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|8|6|5|7|5|6|14|5|7|7|5|6
|9|5|8|6|5|5|7|6|5|6|5|6|7|6|8|6|6|6|8|6|7|6|4|5|19|5|8|7|6|4|7|5|6|6|5|7|8|6|6|7|5|5|
7|6|9|7|6|
MH|OPR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|12|0|1|0|0|0|0|4|0|2|2|0|0|
0|0|1|1|0|0|0|0|0|0|0|0|0|0|0|0|0|1|0|0|0|0|0|0|1|28|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|
MH|IERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|
MH|NB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|
MH|RB|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|374874|374911|374943|374967|
375010|375038|375073|375113|375140|375160|375181|375211|375243|375289|375316|375350|37
5373|375395|375422|375446|375481|375498|375535|375561|375591|375622|375654|375701|3757
38|375761|375794|375833|375863|375902|375935|375954|375974|375999|376027|376075|376115
|376147|376168|376200|376224|376253|376289|376315|376365|376400|376436|376463|376508|3
76530|376553|376583|376614|376668|376714|376749|
MH|RNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|GNT|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|CRC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|FRM|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|OR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|
```

```
MH|UR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|
MH|OERR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|
MH|COLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|
0|0|0|0|
MH|LCOLL|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|
MH|RST|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|DEF|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|LCR|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|HIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|1
28|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128|128
|128|128|128|128|128|128|128|128|128|128|
MH|SIQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|HOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|SOQ|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
MH|DPC|10|CURFACT|0|CURVAL|0|TIME|1109703031|MAX|60|NUM|60|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0|0
|0|0|0|
hostname#
```

次に、*snapshot* キーワードを使用した **show asdm history** コマンドの出力例を示します。

```
hostname# show asdm history view 10m snapshot

Available 4 byte Blocks:  [  10s] : 100
Used 4 byte Blocks:  [  10s] : 0
Available 80 byte Blocks:  [  10s] : 100
Used 80 byte Blocks:  [  10s] : 0
Available 256 byte Blocks:  [  10s] : 2100
Used 256 byte Blocks:  [  10s] : 0
Available 1550 byte Blocks:  [  10s] : 7425
Used 1550 byte Blocks:  [  10s] : 1279
Available 2560 byte Blocks:  [  10s] : 40
Used 2560 byte Blocks:  [  10s] : 0
Available 4096 byte Blocks:  [  10s] : 30
Used 4096 byte Blocks:  [  10s] : 0
Available 8192 byte Blocks:  [  10s] : 60
Used 8192 byte Blocks:  [  10s] : 0
Available 16384 byte Blocks:  [  10s] : 100
Used 16384 byte Blocks:  [  10s] : 0
Available 65536 byte Blocks:  [  10s] : 10
Used 65536 byte Blocks:  [  10s] : 0
CPU Utilization:  [  10s] : 31
Input KByte Count:  [  10s] : 62930
Output KByte Count:  [  10s] : 26620
Input KPacket Count:  [  10s] : 755
Output KPacket Count:  [  10s] : 58
Input Bit Rate:  [  10s] : 24561
Output Bit Rate:  [  10s] : 518897
Input Packet Rate:  [  10s] : 48
Output Packet Rate:  [  10s] : 114
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 377331
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 3672
Output KByte Count:  [  10s] : 4051
Input KPacket Count:  [  10s] : 19
Output KPacket Count:  [  10s] : 20
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 1458
Runts:  [  10s] : 1
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
```

```
Collisions:  [  10s] : 63
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 15
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Input KByte Count:  [  10s] : 0
Output KByte Count:  [  10s] : 0
Input KPacket Count:  [  10s] : 0
Output KPacket Count:  [  10s] : 0
Input Bit Rate:  [  10s] : 0
Output Bit Rate:  [  10s] : 0
Input Packet Rate:  [  10s] : 0
Output Packet Rate:  [  10s] : 0
Input Error Packet Count:  [  10s] : 0
No Buffer:  [  10s] : 0
Received Broadcasts:  [  10s] : 0
Runts:  [  10s] : 0
Giants:  [  10s] : 0
CRC:  [  10s] : 0
Frames:  [  10s] : 0
Overruns:  [  10s] : 0
Underruns:  [  10s] : 0
Output Error Packet Count:  [  10s] : 0
Collisions:  [  10s] : 0
LCOLL:  [  10s] : 0
Reset:  [  10s] : 0
Deferred:  [  10s] : 0
Lost Carrier:  [  10s] : 0
Hardware Input Queue:  [  10s] : 128
Software Input Queue:  [  10s] : 0
Hardware Output Queue:  [  10s] : 0
Software Output Queue:  [  10s] : 0
Drop KPacket Count:  [  10s] : 0
Available Memory:  [  10s] : 205149944
Used Memory:  [  10s] : 63285512
Xlate Count:  [  10s] : 0
```

```
Connection Count:  [  10s] : 0
TCP Connection Count:  [  10s] : 0
UDP Connection Count:  [  10s] : 0
URL Filtering Count:  [  10s] : 0
URL Server Filtering Count:  [  10s] : 0
TCP Fixup Count:  [  10s] : 0
TCP Intercept Count:  [  10s] : 0
HTTP Fixup Count:  [  10s] : 0
FTP Fixup Count:  [  10s] : 0
AAA Authentication Count:  [  10s] : 0
AAA Authorzation Count:  [  10s] : 0
AAA Accounting Count:  [  10s] : 0
Current Xlates:  [  10s] : 0
Max Xlates:  [  10s] : 0
ISAKMP SAs:  [  10s] : 0
IPSec SAs:  [  10s] : 0
L2TP Sessions:  [  10s] : 0
L2TP Tunnels:  [  10s] : 0
hostname#
```

関連コマンド

コマンド	説明
asdm history enable	ASDM 履歴のトラッキングをイネーブルにします。

show asdm image

現在の ASDM ソフトウェア イメージ ファイルを表示するには、特権 EXEC モードで **show asdm image** コマンドを使用します。

show asdm image

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm image** コマンドから **show asdm image** コマンドに変更されました。

例

次に、**show asdm image** コマンドの出力例を示します。

```
hostname# show asdm image

Device Manager image file, flash:/ASDM
```

関連コマンド

コマンド	説明
asdm image	現在の ASDM イメージ ファイルを指定します。

show asdm log_sessions

アクティブな ASDM ロギング セッションのリスト、およびそれらのセッションに関連付けられているセッション ID を表示するには、特権 EXEC モードで **show asdm log_sessions** コマンドを使用します。

show asdm log_sessions

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

アクティブな各 ASDM セッションは、1 つまたは複数の ASDM ロギング セッションと関連付けられています。ASDM は、このロギング セッションを使用してセキュリティ アプライアンスから syslog メッセージを取得します。各 ASDM ロギング セッションには、一意のセッション ID が割り当てられています。このセッション ID を **asdm disconnect log_session** コマンドで使用すると、指定したセッションを終了することができます。

（注） 各 ASDM セッションは、少なくとも 1 つの ASDM ロギング セッションを保持しているため、**show asdm sessions** と **show asdm log_sessions** の出力は同じ内容になることもあります。

例

次に、**show asdm log_sessions** コマンドの出力例を示します。

```
hostname# show asdm log_sessions

0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect log_session	アクティブな ASDM ロギング セッションを終了します。

show asdm sessions

アクティブな ASDM セッションのリスト、およびそれらに関連付けられているセッション ID を表示するには、特権 EXEC モードで **show asdm sessions** コマンドを使用します。

show asdm sessions

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show pdm sessions** コマンドから **show asdm sessions** コマンドに変更されました。

使用上のガイドライン

アクティブな各 ASDM セッションには、一意のセッション ID が割り当てられています。このセッション ID を **asdm disconnect** コマンドで使用すると、指定したセッションを終了することができます。

例

次に、**show asdm sessions** コマンドの出力例を示します。

```
hostname# show asdm sessions

0 192.168.1.1
1 192.168.1.2
```

関連コマンド

コマンド	説明
asdm disconnect	アクティブな ASDM セッションを終了します。

CHAPTER 25

show asp drop コマンド～ show curpriv コマンド

show asp drop

アクセラレーション セキュリティ パスによってドロップされたパケットまたは接続をデバッグするには、特権 EXEC モードで **show asp drop** コマンドを使用します。

show asp drop [**flow [***flow_drop_reason***]** | **frame [***frame_drop_reason***]**]

シンタックスの説明

flow [*flow_drop_reason*]	（オプション）ドロップされたフロー（接続）を表示します。*flow_drop_reason* 引数を使用して、特定の理由を指定できます。*flow_drop_reason* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。
frame [***frame_drop_reason***]	（オプション）ドロップされたパケットを表示します。*frame_drop_reason* 引数を使用して、特定の理由を指定できます。*frame_drop_reason* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	他のドロップ理由が追加されました。

使用上のガイドライン

show asp drop コマンドは、アクセラレーション セキュリティ パスによってドロップされたパケットまたは接続を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。この情報はデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

表 25-2 はドロップされたフローの *flow_drop_reason* 引数に有効な値を一覧表示しています。表 25-1 はドロップされたフレームの *frame_drop_reason* 引数に有効な値を一覧表示しています。

表 25-1　フレーム ドロップの理由

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
acl-drop	アクセス規則によってフローが拒否されます。	パケットがセキュリティ アプライアンスに拒否された場合、このカウンタが増分します。拒否規則は、セキュリティ アプライアンスの起動時、さまざまな機能がオンまたはオフにされたとき、アクセス リストがインターフェイスに適用されたとき、またはその他の機能で作成されたデフォルトの規則の可能性があります。デフォルトの規則のドロップを除き、フローが拒否される理由は次のとおりです。 • インターフェイス上にアクセス リストが設定されている。 • アクセス リストが AAA 用に設定されていて、AAA がユーザを拒否した。 • トラフィックを通過して管理専用インターフェイスに到達した。 • IPSec がイネーブルになっているインターフェイスに、暗号化されていないトラフィックが到達した。 **推奨事項**：次のシステム ログ メッセージが参照するアクセス リストをチェックします。 **システム ログ メッセージ**：106023、106100、106004
bad-crypto	不良暗号がパケットで戻ります。	セキュリティ アプライアンスがパケットの暗号化を試みましたが、暗号化が失敗した場合、このカウンタが増分します。これは正常な状態ではなく、セキュリティ アプライアンスに関するソフトウェアまたはハードウェアに問題がある可能性を示しています。 **推奨事項**：不良暗号の表示を何度も受信する場合は、セキュリティ アプライアンスの点検が必要である可能性があります。システム メッセージ 402123 をイネーブルにして、暗号不良がハードウェアのエラーなのかソフトウェアのエラーなのかを判断してください。また、**show ipsec stats** コマンドを使用して、グローバル IPSec 統計情報にあるエラー カウンタをチェックしてください。これらのエラーを引き起こす IPSec SA が既知である場合は、**show ipsec sa detail** コマンドから出力される SA 統計情報も問題の診断に役立ちます。 **システム ログ メッセージ**：402123

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
bad-ipsec-natt	不良 IPSEC NATT パケット。	セキュリティ アプライアンスが IPSec 接続上で NAT-T とネゴシエートしたパケットを受信したが、パケットのアドレスが NAT-T UDP の宛先ポートである 4500 になっていない、またはパケットのペイロード長が無効である場合、このカウンタが増分します。 **推奨事項**：ネットワーク トラフィックを分析し、NAT-T トラフィックの送信元を特定します。 **システム ログ メッセージ**：なし。
bad-ipsec-prot	AH または ESP ではない IPSEC。	セキュリティ アプライアンスが IPSec 接続上で AH または ESP プロトコル パケットではないパケットを受信した場合、このカウンタが増分します。これは正常な状態ではありません。 **推奨事項**：AH または ESP ではない IPSec 表示が何度もセキュリティ アプライアンスに表示される場合は、ネットワーク トラフィックを分析し、トラフィックの送信元を特定します。 **システム ログ メッセージ**：402115
bad-ipsec-udp	不良 IPSEC UDP パケット。	セキュリティ アプライアンスが、IPSec over UDP とネゴシエート済みの IPSec 接続上でパケットを受信したが、このパケットのペイロード長が無効だった場合、このカウンタが増分します。 **推奨事項**：ネットワーク トラフィックを分析し、NAT-T トラフィックの送信元を特定します。 **システム ログ メッセージ**：なし。
bad-tcp-cksum	不良 TCP チェックサム。	セキュリティ アプライアンスが、算出された TCP チェックサムと TCP ヘッダーに記録されているチェックサムが一致しない TCP パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。不適切な TCP チェックサムを持つパケットを許可するには、**checksum-verification** 機能をディセーブルにします。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
bad-tcp-flags	不良 TCP フラグ。	セキュリティ アプライアンスが、TCP ヘッダー内の TCP フラグが無効な TCP パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。たとえば、SYN フラグと FIN TCP フラグの両方がセットされているパケットは、ドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
conn-limit	接続制限値に到達しました。	この理由は、接続制限値またはホスト接続制限値を超えたためにパケットがドロップされたことによるものです。このパケットが、接続制限値により TCP 接続設定フェーズ中にドロップされた TCP パケットの場合は、ドロップ理由「TCP connection limit reached（TCP 接続制限値に到達しました。）」も報告されます。 **推奨事項**：カウンタが急速に増分する場合は、システム メッセージをチェックし、どのホストが接続制限値に到達したのかを判断します。トラフィックが正常な場合、またはホストが攻撃を受けている場合は、接続制限値を増分する必要があることもあります。 **システム ログ メッセージ**：201011
ctm-error	CTM がエラーを返しました。	セキュリティ アプライアンスがパケットの暗号化を試みましたが、暗号化が失敗した場合、このカウンタが増分します。これは正常な状態ではなく、セキュリティ アプライアンスに関するソフトウェアまたはハードウェアに問題がある可能性を示しています。 **推奨事項**：不良暗号の表示を何度も受信する場合は、セキュリティ アプライアンスの点検が必要である可能性があります。システム メッセージ 402123 をイネーブルにして、暗号不良がハードウェアのエラーなのかソフトウェアのエラーなのかを判断してください。また、**show ipsec stats** コマンドを使用して、グローバル IPSec 統計情報にあるエラー カウンタをチェックしてください。これらのエラーを引き起こす IPSec SA が既知である場合は、**show ipsec sa detail** コマンドから出力される SA 統計情報も問題の診断に役立ちます。 **システム ログ メッセージ**：402123

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
dns-guard-id-not-matched	DNS Guard id が一致しません。	DNS 応答メッセージの ID が、同じ接続上で先にセキュリティ アプライアンスを通過した DNS クエリーのいずれにも一致しなかった場合、このカウンタが増分します。このカウンタは、DNS Guard 機能により増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：なし。
dns-guard-out-of-app-id	app id 以外の DNS Guard。	DNS Guard 機能が DNS メッセージの ID を保存するためのデータ構造の割り当てに失敗した場合、このカウンタが増分します。 **推奨事項**：システム メモリの使用状況をチェックします。通常このイベントは、システムがメモリ不足になった場合に発生します。 **システム ログ メッセージ**：なし。
dst-l2_lookup-fail	Dst MAC L2 検索が失敗しました。	セキュリティ アプライアンスが透過モードに設定され、セキュリティ アプライアンスがレイヤ 2 の宛先 MAC アドレスの検索に失敗した場合、このカウンタが増分します。検索に失敗すると、セキュリティ アプライアンスは宛先 MAC 探索プロセスを開始し、ARP/ICMP メッセージからホストの場所を探そうとします。 **推奨事項**：セキュリティ アプライアンスが透過モードに設定されている場合、これは正常な状態です。**show mac-address-table** コマンドを実行して、現在セキュリティ アプライアンスによって検出されているレイヤ 2 MAC アドレスの場所をリストすることもできます。 **システム ログ メッセージ**：なし。
flow-expired	期限切れのフロー。	セキュリティ アプライアンスが新しいパケットまたはキャッシュされたパケットを投入しようとしたが、そのパケットがすでに期限切れのフローに属している場合、このカウンタが増分します。また、セキュリティ アプライアンスがすでに期限切れの TCP フロー上で RST を送信しようとした場合、または AIP SSM からパケットが返されてもそのフローがすでに期限切れの場合にも増分します。このパケットはドロップされます。 **推奨事項**：有効なアプリケーションが優先されている場合、タイムアウトを増分する必要があるかどうか調べます。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
fo-standby	スタンバイ装置によってドロップされました。	スタンバイ状態のセキュリティ アプライアンスまたはコンテキストに through-the-box パケットが届き、フローが作成されると、そのパケットはドロップされ、作成されたフローは削除されます。パケットがこの方法でドロップされるたびに、このカウンタが増分します。 **推奨事項**：アクティブなセキュリティ アプライアンスまたはコンテキスト上では、このカウンタが増分することはありません。ただし、スタンバイ アプライアンスまたはセキュリティ アプライアンス上では、増分するのが普通です。 **システム ログ メッセージ**：302014、302016、302018
fragment-reassembly-failed	フラグメントの再構成が失敗しました。	このカウンタは、セキュリティ アプライアンスが一連の断片化されたパケットを 1 つのパケットに再構成できなかった場合に増分します。一連のフラグメント パケットはすべてドロップされます。これは、再構成されたパケットにメモリを配分中にエラーが発生したことが原因であると考えられます。 **推奨事項**：**show blocks** コマンドを使用して、現在のブロック メモリを監視します。 **システム ログ メッセージ**：なし。
host-move-pkt	FP ホスト移動パケット。	セキュリティ アプライアンスまたはコンテキストが透過モードに設定されていて、既知のレイヤ 2 MAC アドレスの発信元インターフェイスが異なるインターフェイス上で検出された場合、このカウンタが増分します。 **推奨事項**：これは、ホストがあるインターフェイス（たとえば LAN セグメント）から別のインターフェイスに移動したことを示しています。実際にホストが移動している場合、透過モードではこれは正常な状態です。ただし、ホストがインターフェイス間であちこち移動する場合は、ネットワーク ループが存在している可能性があります。 **システム ログ メッセージ**：412001、412002、322001
ifc-classify	仮想ファイアウォール分類が失敗しました。	パケットが共有インターフェイスに到着しましたが、特定のコンテキスト インターフェイスへの分類が失敗しました。 **推奨事項**：**global** コマンドまたは **static** コマンドを使用して、各コンテキスト インターフェイスに属している IPv4 アドレスを指定します。 **システム ログ メッセージ**：なし。
inspect-dns-id-not-matched	DNS Inspect id が一致しません。	DNS 応答メッセージの ID が、同じ接続上で先にセキュリティ アプライアンスを通過した DNS クエリーのいずれにも一致しなかった場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
inspect-dns-invalid-domain-label	DNS Inspect 無効ドメイン ラベル。	セキュリティ アプライアンスが無効な DNS ドメイン名またはラベルを検出した場合、このカウンタが増分します。DNS ドメイン名とラベルのチェックは、RFC 1035 ごとに行われます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
inspect-dns-invalid-pak	DNS Inspect 無効パケット。	セキュリティ アプライアンスが無効な DNS パケットを検出した場合、このカウンタが増分します。たとえば、DNS パケットに DNS ヘッダーがない場合や、DNS リソース レコード数がヘッダー内のカウンタと一致しない場合などです。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
inspect-dns-out-of-app-id	app id 以外の DNS Inspect。	DNS 検査エンジンが、DNS メッセージの ID を保存するためのデータ構造の割り当てに失敗した場合、このカウンタが増分します。 **推奨事項**：システム メモリの使用状況をチェックします。通常このイベントは、システムがメモリ不足になった場合に発生します。 **システム ログ メッセージ**：なし。
inspect-dns-pak-too-long	DNS Inspect パケットが長すぎます。	DNS メッセージ長が設定されている最大値を超えると、このカウンタが増分します。 **推奨事項**：アクションは不要です。DNS メッセージ長のチェックが必要でない場合は、**inspect dns maximum-length** オプションを指定せずに DNS 検査をイネーブルにします。 **システム ログ メッセージ**：410001
inspect-icmp-error-different-embedded-conn	ICMP Error Inspect の組み込み接続が異なります。	ICMP エラー メッセージに埋め込まれたフレームが、ICMP 接続の作成時に識別された確立済みの接続と一致しない場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：313005
inspect-icmp-error-no-existing-conn	ICMP Error Inspect に既存の接続がありません。	セキュリティ アプライアンスが、ICMP エラー メッセージに埋め込まれたフレームに関連する確立済みの接続を見つけられなかった場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：313005

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
inspect-icmp-out-of-app-id	app id 以外の ICMP Inspect。	ICMP 検査エンジンが App ID データ構造の割り当てに失敗した場合、このカウンタが増分します。このデータ構造は、ICMP パケットのシーケンス番号を保存するのに使用します。 **推奨事項**：システム メモリの使用状況をチェックします。通常このイベントは、システムがメモリ不足になった場合に発生します。 **システム ログ メッセージ**：なし。
inspect-icmp-seq-num-not-matched	ICMP Inspect シーケンス番号が一致しません。	ICMP エコー応答メッセージ内のシーケンス番号が、同じ接続上で先にセキュリティ アプライアンスを通過した ICMP エコー メッセージのいずれにも一致しない場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：313004
inspect-icmpv6-error-invalid-pak	ICMPv6 Error Inspect 無効パケット。	セキュリティ アプライアンスが ICMPv6 パケットに埋め込まれた無効なフレームを検出した場合、このカウンタが増分します。このチェックは IPv6 パケットと同じものです。たとえば、不完全な IPv6 ヘッダーや変造された IPv6 Next Header などです。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
inspect-icmpv6-error-no-existing-conn	ICMPv6 Error Inspect に既存の接続がありません。	セキュリティ アプライアンスが、ICMPv6 エラー メッセージに埋め込まれたフレームに関連する確立済みの接続を見つけられなかった場合、このカウンタが増分します。 **推奨事項**：これが断続的なイベントの場合、アクションは不要です。攻撃が原因の場合、ホストがアクセス リストを使用できないようにします。 **システム ログ メッセージ**：313005
inspect-rtcp-invalid-length	無効な RTCP パケット長。	このカウンタは、UDP パケット長が RTCP ヘッダーのサイズよりも短い場合に増分します。 **推奨事項**：アクションは不要です。キャプチャを利用すると、不適切なパケットを送信している RTP 送信元を特定できるので、アクセス リストを使用してそのホストを拒否できます。 **システム ログ メッセージ**：なし。
inspect-rtcp-invalid-payload-type	無効な RTCP ペイロード タイプ フィールド。	このカウンタは、RTCP ペイロード タイプ フィールドに 200 から 204 の値が含まれていない場合に増分します。 **推奨事項**：RTP のソースを検証して、RFC 1889 で推奨される範囲外のペイロード タイプが送信された理由を確認する必要があります。 **システム ログ メッセージ**：431002

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
inspect-rtcp-invalid-version	無効な RTCP バージョン フィールド。	このカウンタは、RTCP バージョン フィールドが 2 以外のバージョンを含む場合に増分します。 **推奨事項**：ネットワーク内の RTP ソースが RFC 1889 に適合する RTCP パケットを送信していないようです。アクセス リストを使用するホストを要求に応じて拒否できるよう、この理由を特定する必要があります。 **システム ログ メッセージ**：431002
inspect-rtp-invalid-length	無効な RTP パケット長。	このカウンタは、UDP パケット長が RTP ヘッダーのサイズより短いと増分します。 **推奨事項**：アクションは不要です。キャプチャを利用すると、不適切なパケットを送信している RTP 送信元を特定できるので、アクセス リストを使用してそのホストを拒否できます。 **システム ログ メッセージ**：なし。
inspect-rtp-invalid-payload-type	無効な RTP ペイロード タイプ フィールド。	このカウンタは、信号を発信しているチャンネルが RTP セカンダリ接続の自動メディア タイプについてネゴシエートしているときに、RTP ペイロード タイプ フィールドにオーディオ ペイロード タイプが含まれていないと増分します。カウンタは、ビデオ ペイロード タイプの場合と同じように増分します。 **推奨事項**：ネットワーク内の RTP ソースはオーディオ RTP セカンダリ接続を使用してビデオを送信しています（逆の場合も同じ）。この操作が行われないようにする場合は、アクセス リストを使用するホストを拒否できます。 **システム ログ メッセージ**：431001
inspect-rtp-invalid-version	無効な RTP バージョン フィールド。	このカウンタは、RTP バージョン フィールドが 2 以外のバージョンを含む場合に増分します。 **推奨事項**：ネットワーク内の RTP ソースは RFC 1889 に適合する RTCP パケットを送信していないようです。この理由を特定する必要があり、必要な場合はアクセス リストを使用するホストを拒否できます。 **システム ログ メッセージ**：431001
inspect-rtp-max-outofseq-paks-probation	検査期間中の順番どおりでない RTP パケット。	このカウンタは、RTP ソースを確認中に、順番どおりでない RTP パケットの数が 20 を超えると増分します。検査では、順番どおりの 5 つのパケットを検出すると、ソースが確認済みであると判断されます。 **推奨事項**：RTP ソースを調べて、最初のいくつかのパケットが順番どおりに着信しない理由を確認し、RTP ソースを訂正します。 **システム ログ メッセージ**：431001

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
inspect-rtp-sequence-num-outofrange	範囲外の RTP シーケンス番号。	このカウンタは、パケット内の RTP シーケンス番号が検査により予想された範囲内にないと増分します。 **推奨事項**：RTP ソースからシーケンス番号が順番どおりでない場合、検査によって復元され、新しいシーケンス番号からトラッキングが開始されるので、アクションは必要ありません。 **システム ログ メッセージ**：431001
inspect-rtp-ssrc-mismatch	無効な RTP 同期ソース フィールド。	このカウンタは、パケット内の RTP SSRC フィールドが、すべての RTP パケット内の RTP ソースからの、検査により確認された SSRC と一致しないと増分します。 **推奨事項**：これは、ネットワーク内の RTP ソースがリブートして SSRC を変更したためか、またはネットワーク上の別のホストがファイアウォール上で開かれているセカンダリ RTP 接続を使用して RTP パケットを送信しようとしているために生じます。問題があるかどうか確認するために、さらに調べる必要があります。 **システム ログ メッセージ**：431001
intercept-unexpected	予期しないパケットを代行受信します。	セキュリティ アプライアンスが、サーバからの SYNACK を待機中にクライアントからデータを受信した、または特定の TCP 代行受信状態では処理できないパケットを受信しました。 **推奨事項**：このドロップが接続の失敗の原因である場合、接続のクライアント側およびサーバ側のスニファ トレースを実行し、この問題を報告してください。セキュリティ アプライアンスが攻撃を受けている可能性があり、スニファ トレースまたはスニファ キャプチャが原因の特定に役立ちます。 **システム ログ メッセージ**：なし。
interface-down	インターフェイスがダウンしています。	**shutdown** コマンドを使用して、シャットダウンしているインターフェイス上でパケットを受信するたびに、このカウンタが増分します。入トラフィックでは、セキュリティ コンテキスト分類が行われ、そのコンテキストに関連付けられたインターフェイスがシャットダウンしている場合、このパケットはドロップされます。出トラフィックでは、出トラフィックがシャットダウンしている場合、パケットがドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
invalid-app-length	無効な app 長。	セキュリティ アプライアンスがパケット内にレイヤ 7 ペイロードの無効な長さを検出した場合、このカウンタが増分します。現在は、DNS Guard 機能のみによるドロップをカウントします。たとえば、不完全な DNS ヘッダーなどです。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
invalid-encap	無効なカプセル化。	セキュリティ アプライアンスが、サポートされていないリンクレベルのプロトコルに属するフレームを受信した場合、またはフレームに指定されている L3 タイプがセキュリティ アプライアンスによってサポートされていない場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：直接接続されているホストのリンクレベル プロトコルの設定が正しいことを確認します。 **システム ログ メッセージ**：なし。
invalid-ethertype	無効な ethertype。	セキュリティ アプライアンス上のフラグメンテーション モジュールが、IP バージョン 4 またはバージョン 6 に属さないフラグメント化されたパケットを受信した場合、または送信しようとした場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：セキュリティ アプライアンスやネットワークに接続されている他のデバイスの MTU を確認し、セキュリティ アプライアンスがなぜそのようなフラグメントを処理しているのかを判断します。 **システム ログ メッセージ**：なし。
invalid-ip-header	無効な IP ヘッダー。	セキュリティ アプライアンスが、IP ヘッダーの算出されたチェックサムとヘッダーに記録されているチェックサムが一致しない IP パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、ピアから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
invalid-ip-length	無効な IP 長。	セキュリティ アプライアンスが IPv4 または IPv6 パケットを受信し、そのパケットの IP ヘッダー内のヘッダー長フィールドまたは全長フィールドが有効でない、または受信したパケット長と矛盾する場合、このカウンタが増分します。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
invalid-ip-option	設定された IP オプションはドロップされます。	ユニキャスト パケットまたはマルチキャスト パケットに対して IP オプションを受信するように設定されていないのに、セキュリティ アプライアンスが受信した場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：IP オプションを指定されたパケットが送信者から送信された理由を調査します。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
invalid-tcp-hdr-length	無効な tcp 長。	セキュリティ アプライアンスが、パケット サイズが許可されている最小ヘッダー長よりも小さい TCP パケット、または受信したパケット長と矛盾する TCP パケットを受信した場合、このカウンタが増分します。 **推奨事項**：無効なパケットは、攻撃者から送信された偽造パケットの可能性があります。次のシステム メッセージ内の送信元からのトラフィックを調査します。 **システム ログ メッセージ**：500003
invalid-udp-length	無効な udp 長。	セキュリティ アプライアンスが受信した UDP パケットのサイズが、ヘッダー内のフィールドから計算されたサイズと、ネットワークから受信したときに測定されたサイズで異なる場合、このカウンタが増分します。 **推奨事項**：無効なパケットは、攻撃者から送信された偽造パケットの可能性があります。 **システム ログ メッセージ**：なし。
ipsec-clearpkt-notun	トンネルなしの IPSEC Clear Pkt。	セキュリティ アプライアンスが、暗号化されているはずなのに実際には暗号化されていないパケットを受信した場合、このカウンタが増分します。このパケットは、セキュリティ アプライアンス上で設定され確立された IPSec 接続の内部ヘッダー セキュリティ ポリシー チェックに一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**：ネットワーク トラフィックを分析し、スプーフィングされた IPSec トラフィックの送信元を特定します。 **システム ログ メッセージ**：402117
ipsec-ipv6	IPV6 経由の IPSEC。	セキュリティ アプライアンスが、IPv6 ヘッダーでカプセル化された IPSec ESP パケット、IPSec NAT-T ESP パケット、または IPSec over UDP ESP パケットを受信した場合、このカウンタが増分します。現在セキュリティ アプライアンスは、IPv6 でカプセル化された IPSec セッションをサポートしていません。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
ipsec-need-sa	IPSEC SA がまだネゴシエートされていません。	セキュリティ アプライアンスが、暗号化の必要があるのに IPSec セキュリティ アソシエーションを確立していないパケットを受信した場合、このカウンタが増分します。通常 LAN-to-LAN IPSec コンフィギュレーションでは、これは正常な状態です。これが表示されると、セキュリティ アプライアンスは宛先ピアとの ISAKMP ネゴシエーションを開始します。 **推奨事項**：セキュリティ アプライアンス上で IPSec LAN-to-LAN を設定している場合は、この表示は正常なもので、問題を示すものではありません。ただし、このカウンタが急速に増分する場合は、**crypto** の設定エラーまたはネットワーク エラーにより、ISAKMP ネゴシエーションが完了できないことを示している可能性があります。宛先ピアと通信可能であることを確認し、**show running-config** コマンドを使用して **crypto** 設定を確認します。 **システム ログ メッセージ**：なし。
ipsec-spoof	IPSEC Spoof が検出されました。	セキュリティ アプライアンスが、暗号化されているはずなのに実際には暗号化されていないパケットを受信した場合、このカウンタが増分します。このパケットは、セキュリティ アプライアンス上で設定され確立された IPSec 接続の内部ヘッダー セキュリティ ポリシー チェックに一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**：ネットワーク トラフィックを分析し、スプーフィングされた IPSec トラフィックの送信元を特定します。 **システム ログ メッセージ**：402117
ipsec-tun-down	IPSEC トンネルがダウンしています。	セキュリティ アプライアンスが、削除中の IPSec 接続に関連付けられたパケットを受信した場合、このカウンタが増分します。 **推奨事項**：IPSec トンネルが何らかの理由で切断された場合、これは正常な状態です。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
ipsecudp-keepalive	IPSEC/UDP キープアライブ メッセージ。	セキュリティ アプライアンスが IPSec over UDP キープアライブ メッセージを受信した場合、このカウンタが増分します。IPSec over UDP キープアライブ メッセージは、IPSec over UDP ピアとセキュリティ アプライアンスの間にあるネットワーク デバイスで NAT/PAT フロー情報を常に最新のものにするために、IPSec ピアからセキュリティ アプライアンスに送信されます。 **（注）** UDP 経由でも伝送され UDP ポート 4500 にアドレス指定される、業界標準の NAT-T キープアライブ メッセージはありません。 **推奨事項**：セキュリティ アプライアンス上で IPSec over UDP を設定している場合は、この表示は正常なもので、問題を示すものではありません。セキュリティ アプライアンス上で IPSec over UDP を設定していない場合は、ネットワーク トラフィックを分析し、IPSec over UDP トラフィックの発信元を特定します。 **システム ログ メッセージ**：なし。
ips-fail-close	IPS カードがダウンしています。	AIP SSM がダウンしている状態で、IPS 検査で **fail-close** オプションが使用された場合、このカウンタが増分します。 **推奨事項**：AIP SSM をチェックしてから起動します。 **システム ログ メッセージ**：420001
ips-request	要求された IPS モジュールはドロップされます。	パケットが IPS エンジンのシグニチャと一致した場合、このカウンタが増分し、このパケットは AIP SSM の要求どおりにドロップされます。 **推奨事項**：システム ログ メッセージと AIP SSM 上の警告をチェックします。 **システム ログ メッセージ**：420002
ipv6_sp-security-failed	IPv6 低速パス セキュリティ チェックが失敗しました。	次のいずれかの理由により、このカウンタが増分し、パケットがドロップされます。 • IPv6 through-the-box パケットの送信元アドレスと宛先アドレスが同じである。 • IPv6 through-the-box パケットにリンク ローカル送信元アドレスまたは宛先アドレスがある。 • IPv6 through-the-box パケットの宛先アドレスがマルチキャストである。 **推奨事項**：上記のようなパケットは、悪意のあるアクティビティを示しているか、IPv6 ホストの設定が誤っている結果である可能性があります。パケット キャプチャ機能を使用して type asp パケットをキャプチャし、送信元 MAC アドレスを使用して送信元を特定します。 **システム ログ メッセージ**：送信元アドレスと宛先アドレスが同じ場合、システム メッセージ 106016。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
l2_acl	FP L2 規則がドロップされます。	EtherType アクセス リストによりセキュリティ アプライアンスがパケットを拒否した場合、このカウンタが増分します。デフォルトの場合、ルーテッド モードではセキュリティ アプライアンスは次のものを許可します。 • IPv4 パケット • IPv6 パケット • ARP パケット • FFFF:FFFF:FFFF のレイヤ 2 宛先 MAC（ブロードキャスト） • レイヤ 2 宛先が 0100:5E00:0000-0100:5EFE:FFFF の IPv4 MCAST パケット • レイヤ 2 宛先が 3333:0000:0000-3333:FFFF:FFFF の IPv6 MCAST パケット デフォルトの場合、透過モードではセキュリティ アプライアンスはルーテッド モード アクセス リストおよび次のものを許可します。 • レイヤ 2 宛先が 0100:0CCC:CCCD の BPDU パケット • レイヤ 2 宛先が 0900:0700:0000-0900:07FF:FFFF の Appletalk パケット また、EtherType アクセス リストを設定してインターフェイスに適用することにより、その他のタイプのレイヤ 2 トラフィックを許可することもできます。 **（注）** EtherType アクセス リストに許可されるパケットが、レイヤ 3 またはレイヤ 4 アクセス リストにドロップされる場合もあります。 **推奨事項**：セキュリティ アプライアンスまたはコンテキストを透過モードで実行していて、IP 以外のパケットがセキュリティ アプライアンスにドロップされる場合は、EtherType アクセス リストを設定してこのアクセス リストをアクセス グループに適用することができます。 **（注）** セキュリティ アプライアンスの EtherType アクセス リストは、EtherTypes のみをサポートし、レイヤ 2 宛先 MAC アドレスはサポートしません。 **システム ログ メッセージ**：106026、106027

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
l2_same-lan-port	L2 Src/Dst が同じ LAN ポートです。	セキュリティ アプライアンスまたはコンテキストが透過モードに設定されていて、宛先インターフェイスの L2 MAC アドレスが入力インターフェイスと同じであるとセキュリティ アプライアンスが判断した場合、このカウンタが増分します。 **推奨事項**：セキュリティ アプライアンスまたはコンテキストが透過モードに設定されている場合、これは正常な状態です。セキュリティ アプライアンスが無差別モードで動作しているため、セキュリティ アプライアンスまたはコンテキストはローカル LAN セグメント上のすべてのパケットを受信します。 **システム ログ メッセージ**：なし。
loopback-buffer-full	ループバック バッファがいっぱいです。	セキュリティ アプライアンスのあるコンテキストから別のコンテキストに、共有インターフェイスを介してパケットが送信されたが、ループバック キューにバッファの空き領域がない場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：システム CPU をチェックして、過負荷になっていないかどうか確認します。 **システム ログ メッセージ**：なし。
lu-invalid-pkt	無効な LU パケット。	スタンバイ装置が破損した Logical Update パケットを受信しました。 **推奨事項**：ケーブル不良、回線上のノイズ、またはソフトウェアの欠陥により、パケットが破損した可能性があります。インターフェイスが正しく機能しているように見えても、この問題を Cisco TAC に報告してください。 **システム ログ メッセージ**：なし。
mp-pf-queue-full	ポート転送キューがいっぱいです。	このカウンタは、ポート転送アプリケーションの内部キューがいっぱいである際に、別の伝送パケットを受信した場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-addr-renew-response	SVC モジュールがアドレス更新応答データ フレームを受信しました。	このカウンタは、セキュリティ アプライアンスが SVC から Address Renew Response メッセージを受信すると増分します。SVC はこのメッセージを送信しません。 **推奨事項**：これは、SVC ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
mp-svc-bad-framing	SVC モジュールが不正にフレーム化されたデータを受信しました。	このカウンタは、セキュリティ アプライアンスが SVC から、またはデコードできないコントロール ソフトウェアからパケットを受信すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。SVC またはセキュリティ アプライアンスで、障害が発生している可能性があります。 **システム ログ メッセージ**：722037（SVC の受信したデータのみ）
mp-svc-bad-length	SVC モジュールが不正なデータ長を受信しました。	このカウンタは、セキュリティ アプライアンスが SVC から、または計算された指定の長さが一致しないコントロール ソフトウェアからパケットを受信すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。SVC またはセキュリティ アプライアンスで、障害が発生している可能性があります。 **システム ログ メッセージ**：722037（SVC の受信したデータのみ）
mp-svc-compress-error	SVC モジュール圧縮エラー。	このカウンタは、セキュリティ アプライアンスが、SVC に対してデータを圧縮中にエラーを検出すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。SVC またはセキュリティ アプライアンスで、障害が発生している可能性があります。 **システム ログ メッセージ**：722037
mp-svc-decompres-error	SVC モジュール圧縮解除エラー。	このカウンタは、セキュリティ アプライアンスが SVC からのデータを圧縮解除中にエラーを検出すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。SVC またはセキュリティ アプライアンスで、障害が発生している可能性があります。 **システム ログ メッセージ**：722037
mp-svc-delete-in-progress	接続の削除中に SVC モジュールがデータを受信しました。	このカウンタは、セキュリティ アプライアンスが、削除中の SVC 接続に関連付けられたパケットを受信すると増分します。 **推奨事項**：SVC トンネルが何らかの理由で切断された場合、これは正常な状態です。このエラーが繰り返し何度も発生する場合は、クライアントのネットワーク接続に問題があると考えられます。 **システム ログ メッセージ**：なし。
mp-svc-flow-control	SVC セッションがフローを制御しています。	このカウンタは、SVC が一時的にこれ以上データを受信できないため、セキュリティ アプライアンスがデータをドロップする必要がある場合に増分します。 **推奨事項**：クライアントがこれ以上データを受信できないことを示します。クライアントは受信するトラフィックの量を減らす必要があります。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
mp-svc-invalid-mac	SVC モジュールがフレーム内の無効な L2 データを検出しました。	このカウンタは、セキュリティ アプライアンスが SVC から受信したデータに添付された L2 MAC ヘッダーが無効であると検出した場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-invalid-mac-len	SVC モジュールがフレーム内の無効な L2 データ長を検出しました。	このカウンタは、セキュリティ アプライアンスが SVC から受信したデータに添付された L2 MAC 長が無効であると検出した場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-no-channel	SVC モジュールに再注入のためのチャネルがありません。	このカウンタは、暗号化データを受信したインターフェイスが、復号化データを注入する際に検出されないと増分します。 **推奨事項**：インターフェイスが接続中にシャットダウンすると、この現象が発生します。インターフェイスを再イネーブルにしてチェックしてください。接続中にシャットダウンしたのでない場合は、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-no-mac	SVC モジュールがフレームの L2 データを検出できません。	このカウンタは、セキュリティ アプライアンスが SVC から受信したデータの L2 MAC ヘッダーを検出できない場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-no-prepend	SVC　モジュールにヘッダーを挿入するためのスペースがありません。	このカウンタは、ネットワークにパケットを配置するために、パケット データの前に Mac ヘッダーを付加する十分なスペースがない場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
mp-svc-no-session	SVC　モジュールにセッションがありません。	このカウンタは、セキュリティ アプライアンスがこのデータを送信しなければならない SVC セッションを決定できない場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
mp-svc-unknown-type	SVC モジュールが不明なデータ フレームを受信しました。	このカウンタは、セキュリティ アプライアンスがデータのタイプが不明な SVC からパケットを受信すると増分します。 **推奨事項**：クライアントが使用している SVC がセキュリティ アプライアンス ソフトウェアのバージョンと適合しているかどうかを確認します。 **システム ログ メッセージ**：なし。
natt-keepalive	NAT-T キープアライブ メッセージ。	セキュリティ アプライアンスが IPSec NAT-T キープアライブ メッセージを受信した場合、このカウンタが増分します。NAT-T キープアライブ メッセージは、NAT-T IPSec ピアとセキュリティ アプライアンスの間にあるネットワーク デバイスで NAT/PAT フロー情報を常に最新のものにするために、IPSec ピアからセキュリティ アプライアンスに送信されます。 **推奨事項**：セキュリティ アプライアンス上で IPSec NAT-T を設定している場合は、この表示は正常なもので、問題を示すものではありません。セキュリティ アプライアンス上で NAT-T を設定していない場合は、ネットワーク トラフィックを分析し、NAT-T トラフィックの発信元を特定します。 **システム ログ メッセージ**：なし。
no-adjacency	有効な隣接情報がありません。	セキュリティ アプライアンスが隣接情報を取得しようとしましたが、ネクストホップの MAC アドレスを取得できなかった場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：このドロップ理由のキャプチャを設定し、指定された宛先アドレスのホストが、接続されたネットワーク上に存在するかどうか、またはセキュリティ アプライアンスからルーティング可能かどうかをチェックします。 **システム ログ メッセージ**：なし。
no-mcast-entry	FP に mcast エントリがありません。	次のいずれかの理由により、このカウンタが増分します。 • マルチキャスト　フローに一致するパケットが着信したが、マルチキャスト サービスがイネーブルでなくなっていた、またはマルチキャスト フローが作成された後で再度イネーブルにされた。 **推奨事項**：マルチキャストがディセーブルの場合は、再度イネーブルにします。 **システム ログ メッセージ**：なし。 • パケットが CP にパントされた後にマルチキャスト エントリの変更が検出され、エントリが存在しないために NP がパケットを転送できない。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
no-mcast-intrf	FP に mcast 出力インターフェイスがありません。	次のいずれかの理由により、このカウンタが増分します。 • すべての出力インターフェイスがマルチキャスト エントリから削除された。 **推奨事項**: このグループに受信者が存在しないことを確認します。 **システム ログ メッセージ**：なし。 • マルチキャスト パケットを転送できなかった。 **推奨事項**: このパケットにフローが存在することを確認します。 **システム ログ メッセージ**：なし。
non-ip-pkt-in-routed-mode	非 IP パケットがルーテッド モードで受信されました。	セキュリティ アプライアンスが受信したパケットが IPv4 パケット、IPv6 パケット、ARP パケットのいずれでもなく、セキュリティ アプライアンスまたはコンテキストがルーテッド モードに設定されている場合、このカウンタが増分します。通常の動作では、そのようなパケットはドロップされます。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：106026、106027
no-route	ホストへのルートがありません。	セキュリティ アプライアンスがパケットをインターフェイスから送信しようとしましたが、そのためのルートがルーティング テーブルで見つからなかった場合、このカウンタが増分します。 **推奨事項**：生成されたシステム メッセージから取得した宛先アドレスのルートが存在することを確認します。 **システム ログ メッセージ**：110001
np-socket-closed	終了したソケット内の保留パケットがドロップされました。	ソケットがユーザまたはソフトウェアにより突然終了すると、そのソケットのパイプライン中にある保留中のパケットもドロップします。このカウンタは、パイプライン中にある各ソケットがドロップするたびに増分します。 **推奨事項**：このカウンタは、一般的に、通常の動作の一部として増分していきます。ただし、カウンタが急速に増分している場合や、ソケット ベースのアプリケーションに著しい不適切動作が見られる場合は、ソフトウェアの欠陥によって発生している可能性があります。Cisco TAC に連絡して、問題を詳しく調査してください。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
np-sp-invalid-spi	無効な SPI。	セキュリティ アプライアンスが、現在既知ではない SPI（security parameter index; セキュリティ パラメータ インデックス）を指定するセキュリティ アプライアンスにアドレス変換される IPSec ESP パケットを受信した場合、このカウンタが増分します。 **推奨事項**：無効な SPI が時折表示されるのは珍しいことではなく、特にキーの再生成処理中にはよく起こります。無効な SPI が何度も表示される場合は、何らかの問題または DoS 攻撃を示している可能性があります。無効な SPI が頻繁に表示される場合は、ネットワーク トラフィックを分析して ESP トラフィックの送信元を特定します。 **システム ログ メッセージ**：402114
punt-rate-limit	パントのレート制限を超えました。	セキュリティ アプライアンスがレイヤ 2 パケットをレート制限されたコントロール ポイント サービス ルーチンに転送しようとしたが、レート制限（毎秒）を超えている場合、このカウンタが増分します。現在、レート制限されているコントロール ポイント サービス ルーチン宛てのレイヤ 2 パケットは、ARP パケットだけです。ARP パケットのレート制限は、インターフェイスあたり毎秒 500 ARP です。 **推奨事項**：ネットワーク トラフィックを分析し、ARP パケットのレート制限を超えた理由を判断します。 **システム ログ メッセージ**：322002、322003
queue-removed	キューに入っているパケットがドロップされました。	QoS 設定が変更または削除されると、出力キューで送信の待機をしていた既存のパケットはドロップされ、このカウンタが増分します。 **推奨事項**：正常な状態では、ユーザが QoS 設定を変更した場合に、このような状況が見られます。QoS 設定が何も変更されていないのにこの状況が発生した場合は、Cisco TAC に連絡してください。 **システム ログ メッセージ**：なし。
rate-exceeded	QoS レートを超えました。	レート制限（ポリシング）が出力 / 入力インターフェイスに設定され、出力 / 入力トラフィック レートが設定されたバースト レートを超えた場合、このカウンタが増分します。パケットがドロップされるたび、このカウンタが増分します。 **推奨事項**：インターフェイスから送信されるトラフィックのレートがなぜ設定されたレートを超えたのかを調査し、原因を特定します。正常な状態の場合もあれば、ウイルスの感染や攻撃を示している可能性もあります。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
rm-conn-limit	RM 接続制限に達しました。	このカウンタは、コンテキストまたはシステムの最大接続数に達して新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321001
rm-conn-rate-limit	RM 接続レート制限に達しました。	このカウンタは、コンテキストまたはシステムの最大接続レートに達して新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321002
rpf-violated	逆パス確認が失敗しました。	**ip verify reverse-path** がインターフェイス上に設定されていて、セキュリティ アプライアンスが受信したパケットの発信元 IP ルート検索から得られたインターフェイスが、このパケットが受信されたインターフェイスと異なる場合、このカウンタが増分します。 **推奨事項**：次のシステム メッセージに示されている発信元 IP に基づいてトラフィックの発信元をトレースし、なぜスプーフィングされたトラフィックが送信されているのかを調査します。 **システム ログ メッセージ**：106021
security-failed	早期セキュリティ チェックが失敗しました。	セキュリティ アプライアンスが次のような場合、このカウンタが増分し、パケットはドロップされます。 • IPv4 マルチキャスト パケットを受信したが、パケットのマルチキャスト MAC アドレスがパケットのマルチキャスト宛先 IP アドレスと一致しない。 • オフセットの小さいフラグメントまたは重複するフラグメントが含まれている IPv6 または IPv4 teardrop フラグメントを受信した。 • IP 監査シグニチャと一致する IPv4 パケットを受信した。 **推奨事項**：リモート ピアの管理者に連絡する、またはセキュリティ ポリシーに従ってこの問題の危険度を高くします。IP 監査攻撃チェックの詳細な説明とシステム メッセージについては、**ip audit signature** コマンドを参照してください。 **システム メッセージ**：106020、400xx（IP 監査チェックの場合）
send-ctm-error	CTM　への送信がエラーを返しました。	このカウンタはセキュリティ アプライアンスでは廃止され、増分することはありません。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
sp-security-failed	低速パス　セキュリティ チェックが失敗しました。	セキュリティ アプライアンスが次のような場合、このカウンタが増分し、パケットはドロップされます。 • ルーテッド モードで、次の through-the-box パケットを受信した。 — L2 ブロードキャスト パケット — 宛先 IP アドレスが 0.0.0.0 の IPv4 パケット — 送信元 IP アドレスが 0.0.0.0 の IPv4 パケット **推奨事項**：外部ユーザが、保護されたネットワークを侵害しようとしているかどうか判断します。設定に誤りのあるクライアントをチェックします。 **システム ログ メッセージ**：106016 • ルーテッド モードまたは透過モードで、次の through-the-box IPv4 パケットを受信した。 — 送信元 IP アドレスの最初のオクテットがゼロ。 — 送信元 IP アドレスがループバック IP アドレスと等しい。 — 送信元 IP アドレスのネットワーク部分がすべて 0。 — 送信元 IP アドレスのネットワーク部分がすべて 1。 — 送信元 IP アドレスのホスト部分がすべて 0 またはすべて 1。 **推奨事項**：外部ユーザが、保護されたネットワークを侵害しようとしているかどうか判断します。設定に誤りのあるクライアントをチェックします。 **システム ログ メッセージ**：106016 • ルーテッド モードまたは透過モードで、送信元と宛先の IP アドレスが同じ IPv4 パケットまたは IPv6 パケットを受信した。 **推奨事項**：このメッセージ カウンタが急速に増分する場合は、攻撃を受けている可能性があります。パケット キャプチャ機能を使用して type asp パケットをキャプチャし、パケット内の送信元 MAC アドレスをチェックして送信元を特定します。 **システム ログ メッセージ**：106017

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
ssm-app-fail	サービス モジュールがダウンしています。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。SSM により検査されるパケットが、SSM が使用不可になったためにドロップすると増分します。たとえば、ソフトウェアまたはハードウェアの欠陥、ソフトウェアまたはシグナチャのアップグレード、またはシャットダウンするモジュールなどです。 **推奨事項**：セキュリティ アプライアンスのコントロール プレーンで実行する SSM マネージャ プロセスは、システム メッセージと CLI 警告を発行してその障害を通知します。SSM 障害のトラブルシューティングについては、SSM に付属するマニュアルを参照してください。必要な場合は、Cisco TAC にお問い合せください。 **システム ログ メッセージ**：なし。
ssm-app-request	サービス モジュールがドロップを要求しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。このカウンタは、SSM で実行するアプリケーションが、セキュリティ アプライアンスがパケットをドロップすることを要求すると増分します。 **推奨事項**：詳細については、事故レポート、または SSM により生成されるシステム メッセージを照会することで取得することができます。手順については、SSM に付属のマニュアルを参照してください。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
ssm-asdp-invalid	SSM カードから無効な ASDP パケットを受信しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。セキュリティ アプライアンスが内部データ プレーン インターフェイスから ASA SSM Dataplane Protocol（ASDP）パケットを受信したが、このパケットを解析してドライバに問題が生じると増分します。ASDP は、CSC SSM と同様に、特定のタイプの SSM と通信するためにセキュリティ アプライアンスが使用するプロトコルです。この現象は、さまざまな理由により生じます。たとえば、ASDP プロトコルのバージョンがセキュリティ アプライアンスと SSM 間で適合しなかった場合、コントロール プレーン内の SSM マネージャ プロセスがシステム メッセージと CLI 警告を送信して、インストールする適切なバージョンのイメージを通知します。ASDP パケットがセキュリティ アプライアンス側ですでに終了している接続に属している場合もあります。セキュリティ アプライアンスがスタンバイ状態に切り替わっている場合（フェールオーバーがイネーブルになっている場合）には、これ以降トラフィックを通過させることができません。また、ASDP ヘッダーとペイロードの解析時に予期しない値があった場合もあります。 **推奨事項**：カウンタは通常 0 または非常に小さい数値です。ただし、カウンタが長期わたって少しずつ増分した場合、特にフェールオーバーがあったときや、CLI 経由でセキュリティ アプライアンスの接続を手動で消去したときは考慮する必要がありません。カウントが通常動作時に急激に増分した場合は、Cisco TAC に連絡してください。 システム ログ メッセージ：421003、421004
ssm-dpp-invalid	SSM カードから無効なパケットを受信しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。セキュリティ アプライアンスが内部データ プレーン インターフェイスから ASA SSM Dataplane Protocol（ASDP）パケットを受信するが、それを解析する適切なドライバを検出できない場合に増分します。 **推奨事項**：データ プレーン ドライバは、システムにインストールされた SSM のタイプに応じて動的に登録されます。したがって、この現象は、セキュリティ アプライアンスが完全に初期化される前にデータ プレーン パケットが到着すると発生する可能性があります。このカウンタの値は通常 0 です。ドロップが若干あっても気にする必要はありません。ただし、システムが起動して稼働中であるときにこのカウンタの値が上昇し続ける場合は、問題があることを示している可能性があります。これがセキュリティ アプライアンスの正常な動作に影響を与えると思われる場合は、Cisco TAC に連絡してください。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp_xmit_partial	TCP 再送信が不完全です。	**check-retransmission** 機能がイネーブルになっていて、不完全な TCP 再送信を受信した場合、このカウンタが増分し、パケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-3whs-failed	TCP が 3 ウェイ ハンドシェイクに失敗しました。	セキュリティ アプライアンスがスリーウェイ ハンドシェイク中に無効な TCP パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。たとえば、クライアントからの SYN-ACK は、この理由でドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-acked	TCP DUP が確認されました。	セキュリティ アプライアンスが再送信されたデータ パケットを受信し、このデータがピア TCP エンドポイントにより確認応答された場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-ack-syn-diff	SYNACK 内の TCP ACK が無効です。	セキュリティ アプライアンスがスリーウェイ ハンドシェイク中に不適切な TCP 確認応答番号によって SYN-ACK パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-bad-option-len	TCP 内のオプション長が不正です。	セキュリティ アプライアンスが TCP オプションが設定されている TCP パケットを受信しましたが、このオプションの長さが TCP RFC で定義されているオプションの長さと一致しない場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tcp-bad-option-list	TCP オプション リストが無効です。	セキュリティ アプライアンスが受信した TCP パケットの TCP ヘッダーに非標準の TCP ヘッダー オプションが付属していた場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのような TCP パケットを許可する、または非標準の TCP ヘッダー オプションを消去してこのパケットを許可するには、**tcp-options** コマンドを使用します。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp-bad-sack-allow	TCP SACK ALLOW オプションが不正です。	セキュリティ アプライアンスが受信した TCP パケットに選択的な確認応答オプションが指定されているのに、SYN フラグがセットされていない場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tcp-bad-winscale	TCP ウィンドウ スケール値が不正です。	セキュリティ アプライアンスが受信した TCP パケットに 14 より大きい window-scale オプションが指定されている場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tcp-buffer-full	TCP パケット バッファがいっぱいです。	セキュリティ アプライアンスが接続上で順序が乱れた TCP パケットを受信したが、このパケットを保存するバッファがない場合、このカウンタが増分し、このパケットはドロップされます。通常 TCP パケットは、順番に接続上に配置されてセキュリティ アプライアンスによって検査されるか、またはパケットが SSM に送信されて検査されます。デフォルトのキュー サイズがあり、このデフォルトのキュー サイズを超えるパケットを受信すると、ドロップされます。 **推奨事項**：ASA プラットフォームでは、**queue-size** コマンドを使用してキュー サイズを増分できます。 **システム ログ メッセージ**：なし。
tcp-conn-limit	TCP 接続制限値に到達しました。	この理由は、TCP 接続設定フェーズ中に接続制限値を超えたため、TCP パケットがドロップされたことによるものです。接続制限値は、**set connection conn-max** コマンドを使用して設定します。 **推奨事項**：カウンタが急速に増分する場合は、システム メッセージをチェックし、どのホストが接続制限値に到達したのかを判断します。トラフィックが正常な場合、またはホストが攻撃を受けている場合は、接続制限値を増分する必要があることもあります。 **システム ログ メッセージ**：201011

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp-data-past-fin	FIN 後に TCP データが送信されました。	FIN を送信済みで接続を終了したエンドポイントから、セキュリティ アプライアンスが新しい TCP データ パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-discarded-ooo	3 方向ハンドシェイクで TCP ACK が無効です。	このカウンタは、セキュリティ アプライアンスが 3 方向ハンドシェイク中にクライアントから TCP ACK パケットを受信し、シーケンス番号が次に予想されるシーケンス番号でない場合に増分し、パケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-dual-open	TCP デュアル オープンが拒否されました。	セキュリティ アプライアンスがサーバから TCP SYN パケットを受信したが、初期 TCP 接続がすでに開始している場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-fo-drop	TCP の複製されたフロー pak がドロップされました。	このカウンタは、セキュリティ アプライアンスがアクティブ装置となった直後に、確立した接続上でセキュリティ アプライアンスが SYN、FIN、または RST などのコントロール フラグを持つ TCP パケットを受信すると増分し、パケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-invalid-ack	TCP の無効な ACK。	セキュリティ アプライアンスが受信した TCP パケットの確認応答番号が、ピア TCP エンドポイントから送信されたデータよりも大きい場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-mss-exceeded	TCP データが MSS を超過。	セキュリティ アプライアンスが受信した TCP パケットのデータの長さが、ピア TCP エンドポイントから通知された MSS よりも大きい場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのような TCP パケットを許可するには、**exceed-mss** コマンドを使用します。 **システム ログ メッセージ**：4419001

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcpnorm-rexmit-bad	TCP の不正な再送信。	**check-retransmission** 機能がイネーブルになっていて、元のパケットと異なるデータを持つ TCP 再送信を受信した場合、このカウンタが増分し、パケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcpnorm-win-variation	TCP の予期しない、さまざまなウィンドウ サイズ。	TCP エンドポイントにアドバタイズされたウィンドウ サイズが、大量のデータを受け取ることもなく激変した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのようなパケットを許可するには、**window-variation** コマンドを使用します。 **システム ログ メッセージ**：なし。
tcp-not-syn	最初の TCP パケットが SYN ではありません。	セキュリティ アプライアンスが、代行受信でもなくネイリングもされていない接続の最初のパケットとして、SYN ではないパケットを受信しました。 **推奨事項**：正常な状態では、セキュリティ アプライアンスがすでに接続を終了したのに、クライアントまたはサーバ側がまだ接続が続いていると見なしてデータ転送を続けている場合に、このような現象が見られます。**clear local-host** コマンドまたは **clear xlate** コマンドを発行した直後に、このような状況が発生することがあります。接続が削除された直後でもないのに、このカウンタが急速に増分する場合は、セキュリティ アプライアンスが攻撃を受けている可能性もあります。原因を特定するためには、スニファ トレースを取り込みます。 **システム ログ メッセージ**：6106015
tcp-paws-fail	TCP パケットが PAWS テストに失敗しました。	タイムスタンプ ヘッダー オプションが指定されている TCP パケットが、PAWS（Protect Against Wrapped Sequences）テストに失敗した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのような接続の続行を許可するには、**tcp-options** コマンドを使用してタイムスタンプ オプションを消去します。 **システム ログ メッセージ**：なし。
tcp-reserved-set	TCP の予約済みフラグが設定されました。	セキュリティ アプライアンスが受信した TCP パケットの TCP ヘッダーに予約済みのフラグが設定されていた場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。そのような TCP パケットを許可するか予約済みフラグを消去して、このパケットを渡すには、**reserved-bits** コマンドを使用します。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp-rstfin-ooo	順序が異なる TCP RST/FIN。	セキュリティ アプライアンスが受信した RST パケットまたは FIN パケットの TCP シーケンス番号が不適切な場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-rst-syn-in-win	TCP RST/SYN がウィンドウ内にあります。	セキュリティ アプライアンスが確立された接続上で受信した TCP SYN パケットまたは TCP RST パケットのシーケンス番号が、ウィンドウ内にはあるが次に予測されるシーケンス番号ではなかった場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-seq-past-win	TCP パケットの SEQ がウィンドウを超えています。	セキュリティ アプライアンスが受信した TCP データ パケットのシーケンス番号が、ピア TCP エンドポイントで許可されているウィンドウを超えている場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-seq-syn-diff	SYN/SYNACK　内の TCP SEQ が無効です。	セキュリティ アプライアンスがスリーウェイ ハンドシェイク中に不適切な TCP シーケンス番号によって SYN パケットまたは SYN-ACK パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-synack-data	TCP SYNACK にデータがあります。	セキュリティ アプライアンスが受信した TCP SYN-ACK パケットにデータがある場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tcp-synack-ooo	TCP SYNACK が確立された接続上にあります。	セキュリティ アプライアンスが確立された TCP 接続上で TCP SYN-ACK パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
tcp-syn-data	TCP SYN にデータがあります。	セキュリティ アプライアンスが受信した TCP SYN パケットにデータがある場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：そのような TCP パケットを許可するには、**syn-data** コマンドを使用します。 **システム ログ メッセージ**：なし。
tcp-syn-ooo	TCP SYN が確立された接続上にあります。	セキュリティ アプライアンスが確立された TCP 接続上で TCP SYN パケットを受信した場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
tcp-winscale-no-syn	TCP ウィンドウ スケールが非 SYN 上にあります。	セキュリティ アプライアンスが受信した TCP パケットが、SYN フラグが設定されずに window-scale TCP オプションが指定されていた場合、このカウンタが増分し、このパケットはドロップされます。 **推奨事項**：ケーブル不良または回線上のノイズにより、パケットが破損した可能性があります。また、TCP エンドポイントから破損したパケットが送信され、攻撃を受けている可能性もあります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：なし。
tfw-no-mgmt-ip-config	TFW に管理 IP アドレスが設定されていません。	セキュリティ アプライアンスが透過モードで IP パケットを受信したが、管理 IP アドレスが定義されていない場合、このカウンタが増分します。このパケットはドロップされます。 **推奨事項**：セキュリティ アプライアンスに管理 IP アドレスとマスク値を設定します。 **システム ログ メッセージ**：322004
unable-to-add-flow	フロー ハッシュがいっぱいです。	新しく作成されたフローがフロー ハッシュ テーブルに挿入されましたが、フロー ハッシュ テーブルがいっぱいだったために挿入が失敗した場合、このカウンタが増分します。フローとパケットはドロップされます。このカウンタは、最大接続数の制限値に到達した場合に増分するカウンタとは異なります。 **推奨事項**：このメッセージは、セキュリティ アプライアンスがリソース不足で、操作が成功しなかったことを示しています。**show conn** 出力内の接続が、設定されたアイドル タイムアウト値を超えているかどうかチェックしてください。超えている場合は、Cisco TAC に連絡してください。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
unable-to-create-flow	リソース制限により拒否されたフロー	このカウンタは、システム リソースが制限されているため、フローの作成が失敗すると増分し、パケットはドロップされます。リソースの制限は、次のとおりです。 • システム メモリ • パケット ブロック拡張メモリ • システムの接続制限 最初の 2 つの原因は、「No memory to complete flow（フローを完了するメモリがない）」というフローのドロップ理由で同時に発生します。 **推奨事項**： • システム メモリの空き容量が少ないかどうか確認します。 • 「No memory to complete flow（フローを完了するメモリがない）」というフローのドロップ理由が発生するかどうか確認します。 • **show resource usage** コマンドを使用して、接続カウントがシステム接続制限に達しているかどうか確認します。 **システム ログ メッセージ**：なし。
unexpected-packet	予測されないパケット。	このカウンタは、透過モードでセキュリティ アプライアンスが MAC アドレス宛の非 IP パケットを受信するが、このパケットを処理するための該当するサービスがセキュリティ アプライアンス上にない場合に増分します。 推奨事項：セキュリティ アプライアンスが攻撃を受けているかどうか確認します。疑わしいパケットがない場合、またはセキュリティ アプライアンスが透過モードでない場合、このカウンタは、ソフトウェア エラーが原因で増分していると考えられます。カウンタの増分の原因であるトラフィックを把握し、Cisco TAC に連絡してください。 **システム ログ メッセージ**：なし。
unsupported-ip-version	サポートされていない IP バージョン。	セキュリティ アプライアンスが受信した IP パケットの IP ヘッダー内のバージョン フィールドに、サポートされていないバージョンが入っている場合、このカウンタが増分します。特に、このパケットがバージョン 4 またはバージョン 6 に属していない場合、パケットはドロップされます。 **推奨事項**：ネットワークに接続されている他のデバイスが、バージョン 4 または 6 のみに属する IP パケットを送信するように設定されていることを確認します。 **システム ログ メッセージ**：なし。

表 25-1　フレーム ドロップの理由（続き）

フレーム ドロップのキーワード	フレーム ドロップの理由の表示	説明
unsupport-ipv6-hdr	サポートされていない IPV6 ヘッダー。	サポートされていない IPv6 拡張ヘッダーが付いた IPv6 パケットを受信した場合、このカウンタが増分し、そのパケットはドロップされます。サポートされている IPv6 拡張ヘッダーは、TCP、UDP、ICMPv6、ESP、AH、Hop オプション、Destination オプション、および Fragment です。IPv6 ルーティング拡張ヘッダーはサポートされていません。また、上記以外の拡張ヘッダーもサポートされていません。IPv6 ESP ヘッダーと AH ヘッダーは、パケットが through-the-box の場合にのみサポートされます。To-the-box の IPv6 ESP パケットと AH パケットはサポートされず、ドロップされます。 **推奨事項**：このエラーは、ホスト設定の誤りが原因である可能性があります。このエラーが再発する場合、または何度も発生する場合は、DoS 攻撃など偽のアクティビティや悪意のあるアクティビティを示している可能性があります。 **システム ログ メッセージ**：なし。
vpn-context-expired	期限が切れた VPN コンテキスト。	このカウンタは、暗号化または復号化を必要とするパケットをセキュリティ アプライアンスが受信する場合、または操作を実行するために必要な ASP VPN が有効でなくなる場合に増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
wccp-redirect-no-route	キャッシュ エンジンへのルートはありません。	このカウンタは、セキュリティ アプライアンスがパケットのリダイレクトを試行し、キャッシュ エンジンへのルートを検出できない場合に増分します。 **推奨事項**：キャッシュ エンジンへのルートが存在することを確認してください。 **システム ログ メッセージ**：なし。
wccp-return-no-route	WCCP　が戻したパケットのホストへのルートがありません。	このカウンタは、パケットがキャッシュ エンジンから戻され、セキュリティ アプライアンスがこのパケットの元のソースのルートを検出できない場合に増分します。 **推奨事項**：キャッシュ エンジンから戻されたパケットのソース IP アドレスのルートが存在することを確認します。 **システム ログ メッセージ**：なし。

表 25-2 は、ドロップされたフローの *flow_drop_reason* 引数の有効な値を示しています。

表 25-2　フロー ドロップの理由

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
acl-drop	アクセス規則によってフローが拒否されます。	このカウンタは、パケットがセキュリティ アプライアンスに拒否された場合に増分し、フローの作成は拒否されます。拒否規則は、セキュリティ アプライアンスの起動時、さまざまな機能がオンまたはオフにされたとき、アクセス リストがインターフェイスに適用されたとき、またはその他の機能で作成されたデフォルトの規則の可能性があります。デフォルトの規則のドロップを除き、フローが拒否される理由は次のとおりです。 • インターフェイス上にアクセス リストが設定されている。 • アクセス リストが AAA 用に設定されていて、AAA がユーザを拒否した。 • トラフィックを通過して管理専用インターフェイスに到達した。 • IPSec がイネーブルになっているインターフェイスに、暗号化されていないトラフィックが到達した。 • アクセス リストの末尾に暗黙的な拒否がある。 **推奨事項**：パケットのドロップに関連するシステム メッセージが表示されるかどうか確認します。フロー ドロップにより対応するパケットもドロップされ、必要なシステム メッセージが表示されます。 **システム ログ メッセージ**：なし。
audit-failure	監査が失敗しました。	関連付けられたアクションとしてリセットした **ip audit** シグニチャと一致した後、フローは解放されました。 **推奨事項**:このシグニチャと一致したときにフローの削除を望まない場合は、**ip audit** コマンドからリセット アクションを削除します。 **システム ログ メッセージ**：なし。
closed-by-inspection	検査によりフローが終了しました。	この理由は、アプリケーション検査中にエラーが検出されたためにフローが終了したことによるものです。たとえば、H323 メッセージの検査中にエラーが検出された場合、この理由により対応する H323 フローが終了します。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
conn-limit-exceeded	接続制限値を超えました。	この理由は、接続制限値を超えたためにフローが終了したことによるものです。接続制限値は、**set connection conn-max** コマンドを使用して設定します。 **推奨事項**：なし。 **システム ログ メッセージ**：201011

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
fin-timeout	FIN のタイムアウト。	この理由は、ハーフクローズ タイマーが時間切れになったためにTCP フローが終了したことによるものです。 **推奨事項**：TCP フローの終了よりも時間のかかる有効なセッションがある場合は、ハーフクローズ タイムアウトを増分します。 **システム ログ メッセージ**：302014
flow-reclaimed	tcp/udp 以外のフローが新しい要求を再要求しました。	再要求可能なフローが削除されて新しいフローの要求が可能になると、このカウンタが増分します。これは、セキュリティ アプライアンスを通過するフロー数がソフトウェアの制限で許可された最大数と等しくなり、新しいフロー要求が受信された場合にのみ発生します。この状況が発生すると、再要求可能なフロー数がセキュリティ アプライアンスで許可されている VPN トンネル数を超えた場合、最も古い再要求可能なフローが削除され、新しいフローが可能になります。すべてのフローが再要求可能とされていますが、次のフローは除きます。 • TCP、UDP、GRE およびフェールオーバー フロー • ICMP フロー（ICMP ステートフル検査がイネーブルの場合） • セキュリティ アプライアンスへの ESP フロー **推奨事項**：このカウンタが徐々に増分する場合は、アクションは不要です。このカウンタが急速に増分する場合は、セキュリティ アプライアンスが攻撃を受けていて、セキュリティ アプライアンスのフロー再作成と再要求に時間がかかっていることを示している可能性があります。 **システム ログ メッセージ**：302021
fo-primary-closed	フェールオーバー プライマリが終了しました。	スタンバイ装置がアクティブ装置からフロー削除メッセージを受信し、フローを終了しました。 **推奨事項**：セキュリティ アプライアンスがステートフル フェールオーバーを実行している場合は、スタンバイ アプライアンス上で切断された接続が複製されるたびに、このカウンタが増分します。 **システム ログ メッセージ**：302014、302016、302018
fo-standby	フェールオーバー スタンバイによりフローが終了しました。	スタンバイ状態のセキュリティ アプライアンスまたはコンテキストに through-the-box パケットが届くと、フローが作成され、そのパケットはドロップされ、作成されたフローは削除されます。このカウンタは、この方法でフローが削除されるたびに増分します。 **推奨事項**：アクティブなセキュリティ アプライアンスまたはコンテキスト上では、このカウンタが増分することはありません。ただし、スタンバイしているセキュリティ アプライアンスまたはコンテキスト上では、増分するのが普通です。 **システム ログ メッセージ**：302014、302016、302018

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
fo_rep_err	スタンバイ フローの複製エラー。	スタンバイ装置がフローの複製に失敗しました。 **推奨事項**：セキュリティ アプライアンスが VPN トラフィックを処理している場合は、IKE SA 情報よりも先にフローが複製されるため、このカウンタはスタンバイ装置上で常に増分しています。この場合、アクションは不要です。セキュリティ アプライアンスが VPN トラフィックを処理していない場合は、この表示はソフトウェアの検出を示しています。スタンバイ装置上で **debug fover fail** コマンドを実行し、デバッグ出力を収集し、この問題を Cisco TAC に報告してください。 **システム ログ メッセージ**：302014、302016、302018
host-removed	ホストが削除されました。	**clear local-host** コマンドに応答して、フローが削除されました。 **推奨事項**：これは情報カウンタです。 **システム ログ メッセージ**：302014、302016、302018、302021、305010、305012、609002
inspect-fail	検査が失敗しました。	セキュリティ アプライアンスが、接続のために NP によって行われるプロトコル検査をイネーブルにできなかった場合、このカウンタが増分します。原因として考えられるのは、メモリ割り当てが失敗したこと、または ICMP エラー メッセージの場合は、この ICMP エラー メッセージに埋め込まれているフレームに関連した確立済みの接続をセキュリティ アプライアンスが検出できなかったことです。 **推奨事項**：システム メモリの使用状況をチェックします。ICMP エラー メッセージに関しては、攻撃が原因の場合、ホストに対してアクセス リストを使用させないようにすることができます。 **システム ログ メッセージ**：ICMP エラーの場合 313004 です。
ips-fail-close	IPS が失敗して終了しました。	この理由は、AIP SSM がダウンしている状態で、fail-close オプションが IPS 検査で使用されたためにフローが終了したことによるものです。 **推奨事項**：AIP SSM をチェックしてから起動します。 **システム ログ メッセージ**：420001
ips-request	IPS によりフローが終了しました。	この理由は、AIP SSM の要求どおりにフローが終了したことによるものです。 **推奨事項**：システム ログ メッセージと AIP SSM 上の警告をチェックします。 **システム ログ メッセージ**：420002

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
ipsec-spoof-detect	IPsec スプーフ パケットが検出されました。	セキュリティ アプライアンスが、暗号化されているはずなのに実際には暗号化されていないパケットを受信した場合、このカウンタが増分します。このパケットは、セキュリティ アプライアンス上で設定され確立された IPSec 接続の内部ヘッダー セキュリティ ポリシー チェックに一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**：ネットワーク トラフィックを分析し、スプーフィングされた IPSec トラフィックの送信元を特定します。 **システム ログ メッセージ**：402117
loopback	フローがループバックしています。	この理由は、次のいずれかの状況により、フローが終了したことによるものです。 • U-turn トラフィックがフローに存在する。 • **same-security-traffic permit intra-interface** が設定されていない。 **推奨事項**：インターフェイス上で U-turn トラフィックを許可するには、そのインターフェイスを **same-security-traffic permit intra-interface** コマンドで設定します。 **システム ログ メッセージ**：なし。
mcast-entry-removed	マルチキャスト エントリが削除されました。	この理由は、次のいずれかの場合によるものです。 • マルチキャスト フローに一致するパケットが着信したが、マルチキャスト サービスがイネーブルでなくなっていた、またはマルチキャスト フローが作成された後で再度イネーブルにされた。 **推奨事項**：マルチキャストがディセーブルの場合は、再度イネーブルにします。 **システム ログ メッセージ**：なし。 • マルチキャスト エントリが削除されたのでフローもクリーンアップされるが、パケットはデータ パスに再び挿入される。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
mcast-intrf-removed	マルチキャスト インターフェイスが削除されました。	この理由は、次のいずれかの場合によるものです。 • 出力インターフェイスがマルチキャスト エントリから削除された。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。 • すべての出力インターフェイスがマルチキャスト エントリから削除された。 **推奨事項**：このグループに受信者が存在しないことを確認します。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
nat-failed	NAT が失敗しました。	IP を変換する、またはヘッダーを転送するための xlate の作成が失敗しました。 **推奨事項**：NAT が必要でない場合は、**nat-control** をディセーブルにします。そうでない場合は、**static**、**nat**、**global** のいずれかのコマンドを使用して、ドロップされたフローに NAT ポリシーを設定します。ダイナミック NAT では、各 **nat** コマンドが少なくとも 1 つの **global** コマンドとペアになっていることを確認します。NAT 規則を確認するには、**show running-config nat** と **debug pix process** を使用します。 **システム ログ メッセージ**：305005、305006、305009、305010、305011、305012
nat-rpf-failed	NAT 逆パスが失敗しました。	マッピングされたホストの実際のアドレスを使用してそのホストに接続しようとしましたが、拒否されました。 **推奨事項**：NAT を実施しているホストと同じインターフェイス上にない場合は、実際のアドレスの代わりにマッピング アドレスを使用してホストに接続します。また、アプリケーションが IP アドレスを埋め込む場合は、適切な **inspect** コマンドをイネーブルにします。 **システム ログ メッセージ**：305005
need-ike	IKE ネゴシエーションを開始する必要があります。	セキュリティ アプライアンスが、暗号化の必要があるのに IPSec セキュリティ アソシエーションを確立していないパケットを受信した場合、このカウンタが増分します。通常 LAN-to-LAN IPSec コンフィギュレーションでは、これは正常な状態です。これが表示されると、セキュリティ アプライアンスは宛先ピアとの ISAKMP ネゴシエーションを開始します。 **推奨事項**：セキュリティ アプライアンス上で IPSec LAN-to-LAN を設定している場合は、この表示は正常なもので、問題を示すものではありません。ただし、このカウンタが急速に増分する場合は、**crypto** の設定エラーまたはネットワーク エラーにより、ISAKMP ネゴシエーションが完了できないことを示している可能性があります。 宛先ピアと通信可能であることを確認し、**show running-config** コマンドを使用して **crypto** 設定を確認します。 **システム ログ メッセージ**：なし。
no-inspect	検査の割り当てに失敗。	このカウンタは、接続が確立されたときにセキュリティ アプライアンスがランタイム検査のデータ構造の割り当てに失敗すると増分します。接続はドロップされます。 **推奨事項**：このエラーの条件は、セキュリティ アプライアンスがシステム メモリを使い切ると発生します。**show memory** コマンドを発行して、使用可能な空きメモリをチェックします。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
no-ipv6-ipsec	IPsec over IPv6 はサポートされていません。	セキュリティ アプライアンスが、IPv6 ヘッダーでカプセル化された IPSec ESP パケット、IPSec NAT-T ESP パケット、または IPSec over UDP ESP パケットを受信した場合、このカウンタが増分します。現在セキュリティ アプライアンスは、IPv6 でカプセル化された IPSec セッションをサポートしていません。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
non_tcp_syn	TCP が SYN 以外です。	この理由は、最初のパケットが SYN パケットではなかったために TCP フローが終了したことによるものです。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
out-of-memory	フローを完了するためのメモリがありません。	セキュリティ アプライアンスがメモリ不足のためにフローを作成できない場合、このカウンタが増分します。 **推奨事項**：現在の接続をチェックして、セキュリティ アプライアンスが攻撃を受けていないことを確認します。また、設定したタイムアウト値が大きすぎるために、アイドル状態のフローがメモリに長時間常駐していないかどうかも確認します。**show memory** コマンドを発行して、使用可能な空きメモリをチェックします。空きメモリが少ない場合は、**show processes memory** コマンドを発行し、メモリを大量に使用しているプロセスを特定します。 **システム ログ メッセージ**：なし。
parent-closed	親フローが終了しています。	下位フローの親フローが終了すると、その下位フローも終了します。たとえば、FTP データ制御フロー（親フロー）が終了すると、この理由により FTP データ フロー（下位フロー）も終了します。また、この理由は、制御アプリケーションによってセカンダリ フロー（pin-hole）が終了した場合にも該当します。たとえば、BYE メッセージを受信すると、SIP 検査エンジン（制御アプリケーション）は対応する SIP RTP フロー（セカンダリ フロー）を終了します。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
pinhole-timeout	Pinhole のタイムアウト。	セキュリティ アプライアンスがセカンダリ フローを開始しましたが、タイムアウト間隔内にこのフローにパケットが渡されなかったためにフローが削除されたことを報告する場合、このカウンタが増分します。セカンダリ フローの例としては、FTP コントロール チャネル上でネゴシエーションの成功後に作成される FTP データ チャネルがあります。 **推奨事項**：なし。 **システム ログ メッセージ**：302014、302016

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
recurse	再帰的フローを終了します。	フローが再帰的に解放されました。この理由はペア フローとマルチキャスト スレーブ フローに該当し、これらの各下位フローに対するシステム メッセージは発行されません。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
reinject-punt	パント アクションによりフローが終了しました。	検査や AAA などの強化されたサービスによって、処理のための例外パスにパケットがパントされた場合、このカウンタが増分します。このサービス ルーチンは、フロー上を流れるトラフィック内に違反を検出すると、そのフローをドロップするよう要求します。このフローはただちにドロップされます。 **推奨事項**：サービス ルーチンによってトリガーされるシステム メッセージに注意してください。フロー ドロップにより、対応する接続も終了します。 **システム ログ メッセージ**：なし。
reset-by-ips	IPS によりフローがリセットされました。	この理由は、AIP SSM の要求どおりに TCP フローが終了したことによるものです。 **推奨事項**: システム ログ メッセージと AIP SSM 上の警告をチェックします。 **システム ログ メッセージ**：420003
reset-in	TCP リセット I。	この理由は、（セキュリティが低いインターフェイスからセキュリティが同じまたは高いインターフェイスへの）発信フロー上で TCP リセットを受信して、そのフローが終了したことによるものです。 **推奨事項**：なし。 **システム ログ メッセージ**：302014
reset-out	TCP リセット O。	この理由は、（セキュリティが高いインターフェイスからセキュリティが低いインターフェイスへの）着信フロー上で TCP リセットを受信して、そのフローが終了したことによるものです。 **推奨事項**：なし。 **システム ログ メッセージ**：302014
shunned	フローが排除されました。	排除データベース内にあるホストと一致する送信元 IP アドレスを持つパケットを受信した場合、このカウンタが増分します。**shun** コマンドが適用される場合、それぞれの既存のフローが **shun** コマンドに一致するたびに増分します。 **推奨事項**：なし。 **システム ログ メッセージ**：401004

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
ssl-bad-record-detect	SSL 不良レコードが検出されました。	このカウンタは、リモート ピアから不明の SSL レコード タイプを受信するたびに増分します。ピアから受信した不明のレコード タイプはすべて重大エラーとして処理され、このエラーが検出された SSL 接続は終了しなければなりません。 **推奨事項**：このカウンタが増分するのはどんなときでも正常でありません。このカウンタが増分する場合、通常、SSL プロトコルの状態がクライアント ソフトウェアと同期していないこと示します。この問題の原因として最も可能性があるのは、クライアント ソフトウェア内のソフトウェアの欠陥です。Cisco TAC にそのクライアント ソフトウェアまたは Web ブラウザのバージョンについて問い合せ、この問題を解決するために SSL データ交換のネットワーク トレースを提供してください。 **システム ログ メッセージ**：なし。
ssl-handshake-failed	SSL ハンドシェイクが失敗しました。	このカウンタは、SSL ハンドシェイクの失敗により TCP 接続がドロップすると増分します。 **推奨事項**：このカウンタは、SSL ハンドシェイクの失敗により TCP 接続がドロップしたことを示します。ハンドシェイク障害状況により生成されたシステム ログ メッセージ情報に基づいて問題が解決できない場合は、Cisco TAC に問い合せる際に、関連するシステム ログ メッセージ情報を提供してください。 **システム ログ メッセージ**：725006、725014
rm-xlate-limit	RM xlate 制限に達しました。	このカウンタは、あるコンテキストまたはシステムの xlate が最大数に達し、新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321001
rm-host-limit	RM ホスト制限に達しました。	このカウンタは、あるコンテキストまたはシステムのホストが最大数に達し、新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321001
rm-inspect-rate-limit	RM 検査レート制限に達しました。	このカウンタは、コンテキストまたはシステムの検査レートが最大数に達し、新しい接続が試行されると増分します。 **推奨事項**：デバイスの管理者は、**show resource usage** コマンドおよび **show resource usage system** コマンドを使用して、コンテキストやシステムのリソース制限値と「Denied」の回数を確認し、必要に応じてリソース制限値を調整できます。 **システム ログ メッセージ**：321002

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
ctm-crypto-request-error	CTM 暗号要求エラー。	このカウンタは、CTM が暗号要求を受け入れない場合に、その都度増分します。これは通常、暗号ハードウェア要求のキューがいっぱいになっていることを示します。 **推奨事項**：show crypto protocol statistics ssl コマンドを発行し、この情報を Cisco TAC に提供してください。 **システム ログ メッセージ**：なし。
ssl-record-decrypt-error	SSL レコード復号化が失敗しました。	このカウンタは、SSL データを受信中に復号化エラーが発生すると増分します。これは通常、ASA またはピアの SSL コードにバグがある場合、または攻撃者がデータ ストリームを変更している可能があることを示します。SSL 接続は終了されます。 **推奨事項**：ASA に対する SSL データ ストリームを検証します。攻撃者がいない場合は、Cisco TAC へ報告すべきソフトウェア エラーがあることを示します。 **システム ログ メッセージ**：なし。
np-socket-conn-not-accepted	新規のソケット接続が受け入れられませんでした。	このカウンタは、セキュリティ アプライアンスによって新規のソケット接続が受け入れられない場合に増分します。 **推奨事項**：このカウンタは、通常の動作が行われる過程で増分していく可能性があります。ただし、カウンタが急速に増分している場合や、ソケット ベースのアプリケーションに著しい不適切動作が見られる場合は、ソフトウェアの欠陥によって発生している可能性があります。Cisco TAC に連絡して、問題を詳しく調査してください。 **システム ログ メッセージ**：なし。
np-socket-failure	NP ソケットの欠陥。	これは、重大なソケット処理エラーに対する一般的なカウンタです。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
np-socket-data-move-failure	NP ソケット データ移動エラー。	このカウンタは、ソケット データの移動時にエラーがあると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
np-socket-new-conn-failure	NP ソケットの新規接続エラー。	このカウンタは、ソケットの新規接続が失敗すると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
np-socket-transport-closed	NP ソケット転送が終了しました。	このカウンタは、ソケットに関連する転送が異常終了すると増分します。 **推奨事項**：このカウンタは、通常の動作が行われる過程で増分していく可能性があります。ただし、カウンタが急速に増分している場合や、ソケット ベースのアプリケーションに著しい不適切動作が見られる場合は、ソフトウェアの欠陥によって発生している可能性があります。Cisco TAC に連絡して、問題を詳しく調査してください。 **システム ログ メッセージ**：なし。
np-socket-block-conv-failure	NP ソケット ブロック変換エラー。	このカウンタは、ソケット ブロック変換エラーがあると増分します。 **推奨事項**：これは、ソフトウェアのエラーを Cisco TAC に報告する必要があることを示しています。 **システム ログ メッセージ**：なし。
ssl-received-close-alert	SSL が終了アラートを受信しました。	このカウンタは、セキュリティ アプライアンスがリモート クライアントから終了アラートを受信すると増分します。これは、クライアントが接続をドロップしようとしていることを通知したことを示します。通常の接続切断プロセスの一部です。 **推奨事項**：なし。 **システム ログ メッセージ**：725007
tracer-flow	packet-tracer がフローのドロップをトレースしました。	このカウンタは、トレースが完了して解放されたフローについて、packet-tracer により内部的に使用されます。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
ssl-malloc-error	SSL の malloc のエラー。	このカウンタは、SSL ライブラリ内で malloc のエラーが発生すると増分します。これは、SSL がメモリ バッファまたはパケット ブロックを割り当てることができないメモリ不足状態であることを示します。 **推奨事項**：セキュリティ アプライアンスのメモリとパケット ブロックの状態を調べ、このメモリ情報を Cisco the TAC に連絡してください。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
ssm-app-fail	サービス モジュールが失敗しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。このカウンタは、SSM により検査中の接続が、SSM にエラーが生じたために終了すると増分します。 **推奨事項**：セキュリティ アプライアンスのコントロール プレーン内で動作しているカード マネージャ プロセスが、システム メッセージと CLI 警告を発行してこのエラーを通知します。SSM エラーの問題解決については、SSM に付属のマニュアルを参照してください。必要な場合は、Cisco TAC に連絡してください。 **システム ログ メッセージ**：421001
ssm-app-incompetent	サービス モジュールが機能しませんでした。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。SSM による接続の検査が予定されているが、SSM が検査できない場合に増分します。このカウンタは将来使用するために予約されます。現在のリリースでは常に 0 である必要があります。 **推奨事項**：なし。 **システム ログ メッセージ**：なし。
ssm-app-request	サービス モジュールによりフローが終了しました。	このカウンタが適用されるのは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみです。カウンタは、SSM で実行するアプリケーションがセキュリティ アプライアンスに接続を終了するよう要求すると増分します。 **推奨事項**：SSM によって生成された事故レポートまたはシステム メッセージを照会して、詳細情報を取得することができます。手順については、SSM に付属のマニュアルを参照してください。 **システム ログ メッセージ**：なし。
svc-failover	SVC ソケット接続がスタンバイ装置側で切断中です。	このカウンタは、アクティブ装置がフェールオーバー変遷の一部としてスタンバイ状態に移行するときに新規の SVC ソケット接続が切断されると増分します。 **推奨事項**：なし。これは、現在のデバイスがアクティブからスタンバイに移行する際の SVC 接続の通常のクリーンアップの一部です。デバイスでの既存の SVC 接続は有効でなるので、削除する必要があります。 **システム ログ メッセージ**：なし。
svc-spoof-detect	SVC スプーフ パケットが検出されました。	このカウンタは、暗号化されているはずが暗号化されていないパケットをセキュリティ アプライアンスが受信すると増分します。このパケットは、セキュリティ アプライアンスで設定、確立された SVC 接続の内部ヘッダー セキュリティ ポリシー チェックに一致しましたが、暗号化されずに受信されました。これはセキュリティの問題です。 **推奨事項**：ネットワーク トラフィックを分析し、スプーフィングされた SVC トラフィックの送信元を特定します。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
syn-timeout	SYN のタイムアウト。	この理由は、初期タイマーが時間切れになったために TCP フローが終了したことによるものです。 **推奨事項**:接続の確立に時間のかかる有効なセッションがある場合は、初期タイムアウトを増分します。 **システム ログ メッセージ**：302014
tcp-fins	TCP FIN。	この理由は、TCP FIN パケットを受信した時に TCP フローが終了したことによるものです。 **推奨事項**：各 TCP 接続が FIN で正常に終了した場合、このカウンタが増分します。 **システム ログ メッセージ**：302014
tcp-intercept-no-response	TCP 代行受信サーバが応答しませんでした。	SYN 再送信は、1 秒に 1 回の割合で 3 回試行した後にタイムアウトになります。サーバが到達不能のため、接続が切断されました。 **推奨事項**：サーバがセキュリティ アプライアンスから到達可能であるかどうかをチェックします。 **システム ログ メッセージ**：なし。
tcp-intercept-kill	TCP 代行受信によりフローが終了しました。	次の理由により、TCP 代行受信が接続を切断しました。 1. これは最初の SYN である。 2. 接続が SYN 用に作成されている。 3. TCP 代行受信が SYN クッキーで応答した。または TCP 代行受信が SYN をサーバに送信し、サーバがクライアントからの有効な ACK を確認した後、RST で応答した。 **推奨事項**：ネイリング規則がある、パケットが VPN トンネル経由で着信する、またはクライアントに到達するネクストホップ ゲートウェイ アドレスが解決されない場合を除き、通常 TCP 代行受信では最初の SYN に対する接続は作成されません。そのため、これは最初の SYN に対して接続が作成されたことを示しています。TCP 代行受信がサーバから RST を受信すると、そのサーバ上の対応するポートが閉じる可能性があります。 **システム ログ メッセージ**：なし。
tcp-intercept-unexpected	TCP 代行受信の予期しない状態。	TCP 代行受信モジュールの論理エラーです。このようなことは発生しないようになっています。 **推奨事項**：メモリの破損、または TCP 代行受信モジュールの論理エラーを示しています。 **システム ログ メッセージ**：なし。
tcpmod-connect-clash	TCP モジュール ポート衝突がクライアントとサーバの間で発生しました。	TCP 接続ソケットは、既存のリッスン接続と衝突します。これは、内部システムのエラーです **推奨事項**：TAC に連絡してください。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
tcpnorm-invalid-syn	TCP の無効な SYN。	この理由は、SYN パケットが無効の場合に TCP フローが終了したことによるものです。 **推奨事項**：チェックサムや TCP ヘッダーが無効な場合など、さまざまな理由で SYN パケットが無効になる可能性があります。なぜ SYN パケットが無効になるかを理解するには、パケット キャプチャ機能を使用してください。これらの接続を許可する場合は、**tcp-map** 設定を使用してチェックをバイパスします。 **システム ログ メッセージ**：302014
tcpnorm-rexmit-bad	TCP の不正な再送信。	この理由は、**check-retransmission** 機能がイネーブルになっている時に、TCP エンドポイントから元のパケットと異なるデータが再送信されて TCP フローが終了したことによるものです。 **推奨事項**：TCP の再送信の際に異なるデータを送信するという方法で、TCP エンドポイントが攻撃を加えている可能性があります。パケット キャプチャ機能を使用して、パケットの発信元の詳細を確認してください。 **システム ログ メッセージ**：302014
tcpnorm-win-variation	TCP の予期しない、さまざまなウィンドウ サイズ。	この理由は、TCP エンドポイントにアドバタイズされたウィンドウ サイズが、大量のデータを受け取ることもなく激変し、TCP フローが終了したことによるものです。 **推奨事項**：この接続を許可するために、**window-variation** コマンドを使用します。 **システム ログ メッセージ**：302014
timeout	接続のタイムアウト。	非アクティビティ タイマーの期限切れのためフローが終了した場合、このカウンタが増分します。 **推奨事項**：なし。 **システム ログ メッセージ**：302014、302016、302018、302021
tunnel-pending	トンネルを確立または切断しています。	セキュリティ アプライアンスがセキュリティ ポリシー データベース（たとえば **crypto map**）のエントリに一致するパケットを受信したが、セキュリティ アソシエーションがネゴシエーションの途中でまだ完了していない場合、このカウンタが増分します。 また、セキュリティ アプライアンスがセキュリティ ポリシー データベースのエントリに一致するパケットを受信したが、セキュリティ アソシエーションが削除された、または削除中である場合にも、このカウンタが増分します。この表示と「Tunnel has been torn down（トンネルが切断されました。）」表示の違いは、「Tunnel has been torn down（トンネルが切断されました。）」表示は確立済みのフロー用であるということです。 **推奨事項**：IPSec トンネルがネゴシエーション中または削除中の場合、これは正常な状態です。 **システム ログ メッセージ**：なし。

表 25-2　フロー ドロップの理由（続き）

フロー ドロップのキーワード	フロー ドロップの理由の表示	説明
tunnel-torn-down	トンネルが切断されました。	セキュリティ アプライアンスが、IPSec セキュリティ アソシエーションが削除中の確立済みフローに関連付けられたパケットを受信した場合、このカウンタが増分します。 **推奨事項**：IPSec トンネルが何らかの理由で切断された場合、これは正常な状態です。 **システム ログ メッセージ**：なし。
xlate-removed	Xlate の消去。	**clear xlate** コマンドまたは **clear local-host** コマンドに応答して、フローが削除されました。 **推奨事項**：これは情報カウンタです。 **システム ログ メッセージ**：302014、302016、302018、302021、305010、305012、609002

例

次に、**show asp drop** コマンドの出力例を示します。

```
hostname# show asp drop

Frame drop:
  Invalid encapsulation                                10897
  Invalid tcp length                                    9382
  Invalid udp length                                      10
  No valid adjacency                                    5594
  No route to host                                      1009
  Reverse-path verify failed                              15
  Flow is denied by access rule                       25247101
  First TCP packet not SYN                              36888
  Bad TCP flags                                         67148
  Bad option length in TCP                                731
  TCP MSS was too large                                 10942
  TCP Window scale on non-SYN                            2591
  Bad TCP SACK ALLOW option                               224
  TCP Dual open denied                                     11
  TCP data send after FIN                                  62
  TCP failed 3 way handshake                           328859
  TCP RST/FIN out of order                             258871
  TCP SEQ in SYN/SYNACK invalid                           142
  TCP ACK in SYNACK invalid                               278
  TCP packet SEQ past window                            46331
  TCP invalid ACK                                     1234749
  TCP packet buffer full                             90009943
  TCP RST/SYN in window                                 43136
  TCP DUP and has been ACKed                           927075
  TCP packet failed PAWS test                            9907
  Early security checks failed                              3
  Slowpath security checks failed                          19
  DNS Inspect invalid packet                             1097
  DNS Inspect invalid domain label                         10
  DNS Inspect packet too long                               5
  DNS Inspect id not matched                             8270
  FP L2 rule drop                                         783
  FP no mcast output intrf                                  5
  Interface is down                                      3881
  Non-IP packet received in routed mode                   158

Flow drop:
  Flow is denied by access rule                            24
  NAT failed                                            28739
  NAT reverse path failed                               22266
  Inspection failure                                    19433
```

関連コマンド

コマンド	説明
capture	パケットをキャプチャします。asp ドロップ コードに基づいてパケットをキャプチャするオプションも含まれています。
clear asp drop	アクセラレーション セキュリティ パスのドロップ統計情報を消去します。
show conn	接続に関する情報を表示します。

show asp table arp

アクセラレーション セキュリティ パスの ARP テーブルをデバッグするには、特権 EXEC モードで **show asp table arp** コマンドを使用します。

show asp table arp [**interface** *interface_name*] [**address** *ip_address* [**netmask** *mask*]]

シンタックスの説明

address*ip_address*	（オプション）ARP テーブル エントリを表示する IP アドレスを指定します。
interface *interface_name*	（オプション）ARP テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	（オプション）IP アドレスのサブネット マスクを設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show arp コマンドが制御プレーンの内容を表示するのに対して、**show asp table arp** コマンドはアクセラレーション セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table arp** コマンドの出力例を示します。

```
hostname# show asp table arp

Context: single_vf, Interface: inside
  10.86.194.50                            Active   000f.66ce.5d46 hits 0
  10.86.194.1                             Active   00b0.64ea.91a2 hits 638
  10.86.194.172                           Active   0001.03cf.9e79 hits 0
  10.86.194.204                           Active   000f.66ce.5d3c hits 0
  10.86.194.188                           Active   000f.904b.80d7 hits 0

Context: single_vf, Interface: identity
  ::                                      Active   0000.0000.0000 hits 0
  0.0.0.0                                 Active   0000.0000.0000 hits 50208
```

関連コマンド

コマンド	説明
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show asp table classify

アクセラレーション セキュリティ パスの分類子テーブルをデバッグするには、特権 EXEC モードで **show asp table classify** コマンドを使用します。分類子は、着信パケットのプロパティ（プロトコル、送信元アドレス、宛先アドレスなど）を検査して、各パケットを適切な分類規則と対応付けます。それぞれの規則には、パケットのドロップや通過の許可など、どのタイプのアクションを実行するかを規定した分類ドメインのラベルが付けられます。

show asp table classify [**crypto** | **domain** *domain_name* | **interface** *interface_name*]

シンタックスの説明

domain *domain_name*	（オプション）特定の分類子ドメインのエントリを表示します。ドメインのリストについては、「使用上のガイドライン」を参照してください。
interface *interface_name*	（オプション）分類子テーブルを表示する特定のインターフェイスを指定します。
crypto	（オプション）encrypt ドメイン、decrypt ドメイン、および ipsec-tunnel-flow ドメインのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table classify コマンドは、アクセラレーション セキュリティ パスの分類子の内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

分類子ドメインには、次のものがあります。

```
aaa-acct
aaa-auth
aaa-user
accounting
arp
capture
capture
conn-nailed
conn-set
ctcp
decrypt
encrypt
established
filter-activex
filter-ftp
filter-https
filter-java
filter-url
host
ids
inspect
inspect-ctiqbe
inspect-dns
inspect-dns-ids
inspect-ftp
inspect-ftp-data
inspect-gtp
inspect-h323
inspect-http
inspect-icmp
inspect-icmp-error
inspect-ils
inspect-mgcp
inspect-netbios
inspect-pptp
inspect-rsh
inspect-rtsp
inspect-sip
inspect-skinny
inspect-smtp
inspect-snmp
inspect-sqlnet
inspect-sqlnet-plus
inspect-sunrpc
inspect-tftp
inspect-xdmcp
ipsec-natt
ipsec-tunnel-flow
ipsec-user
l2tp
l2tp-ppp
limits
lu
mac-permit
mgmt-lockdown
mgmt-tcp-intercept
multicast
nat
nat-exempt
nat-exempt-reverse
nat-reverse
null
permit
permit-ip-option
permit-log
pim
ppp
```

```
priority-q
punt
punt-l2
punt-root
qos
qos-per-class
qos-per-dest
qos-per-flow
qos-per-source
shun
tcp-intercept
```

例

次に、**show asp table classify** コマンドの出力例を示します。

```
hostname# show asp table classify

Interface test:
in  id=0x36f3800, priority=10, domain=punt, deny=false
        hits=0, user_data=0x0, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=10.86.194.60, mask=255.255.255.255, port=0
in  id=0x33d3508, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=0
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
in  id=0x33d3978, priority=99, domain=inspect, deny=false
        hits=0, user_data=0x0, use_real_addr, flags=0x0
        src ip=0.0.0.0, mask=0.0.0.0, port=53
        dst ip=0.0.0.0, mask=0.0.0.0, port=0
...
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットのアクセラレーション セキュリティ パス カウンタを表示します。

show asp table interfaces

アクセラレーション セキュリティ パスのインターフェイス テーブルをデバッグするには、特権 EXEC モードで **show asp table interfaces** コマンドを使用します。

show asp table interfaces

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table interfaces コマンドは、アクセラレーション セキュリティ パスのインターフェイス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table interfaces** コマンドの出力例を示します。

```
hostname# show asp table interfaces

** Flags: 0x0001-DHCP, 0x0002-VMAC, 0x0010-Ident Ifc, 0x0020-HDB Initd,
   0x0040-RPF Enabled
Soft-np interface 'dmz' is up
    context single_vf, nicnum 0, mtu 1500
        vlan 300, Not shared, seclvl 50
        0 packets input, 1 packets output
        flags 0x20

Soft-np interface 'foo' is down
    context single_vf, nicnum 2, mtu 1500
        vlan <None>, Not shared, seclvl 0
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'outside' is down
    context single_vf, nicnum 1, mtu 1500
        vlan <None>, Not shared, seclvl 50
        0 packets input, 0 packets output
        flags 0x20

Soft-np interface 'inside' is up
    context single_vf, nicnum 0, mtu 1500
        vlan <None>, Not shared, seclvl 100
        680277 packets input, 92501 packets output
        flags 0x20
...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show asp table mac-address-table

アクセラレーション セキュリティ パスの MAC アドレス テーブルをデバッグするには、特権 EXEC モードで **show asp table mac-address-table** コマンドを使用します。

show asp table mac-address-table [**interface** *interface_name*]

シンタックスの説明

interface *interface_name*	（オプション）特定のインターフェイスの MAC アドレス テーブルを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table mac-address-table コマンドは、アクセラレーション セキュリティ パスの MAC アドレス テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table mac-address-table** コマンドの出力例を示します。

```
hostname# show asp table mac-address-table

interface                mac  address       flags
------------------------------------------------------------
    inside1                     0009.b74d.3800     None
    inside1                     0007.e903.ad6e     None
    inside1                     0007.e950.2067     None
    inside1                     0050.0499.3749     None
    inside1                     0012.d96f.e200     None
    inside1                     0001.02a7.f4ec     None
    inside1                     0001.032c.6477     None
    inside1                     0004.5a2d.a1c8     None
    inside1                     0003.4773.c87b     None
    inside1                     000d.88ef.5d1c     None
    inside1                     00c0.b766.adce     None
    inside1                     0050.5640.450d     None
    inside1                     0001.03cf.0431     None
...
```

関連コマンド

コマンド	説明
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

show asp table routing

アクセラレーション セキュリティ パスのルーティング テーブルをデバッグするには、特権 EXEC モードで **show asp table routing** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

show asp table routing [**input** | **output**] [**address** *ip_address* [***netmask*** *mask*] | **interface** *interface_name*]

シンタックスの説明

address *ip_address*	ルーティング エントリを表示する IP アドレスを設定します。IPv6 アドレスの場合は、サブネット マスクを含めることができます。スラッシュ（/）に続けて、プレフィックス（0 ～ 128）を入力します。たとえば、次のように入力します。 `fe80::2e0:b6ff:fe01:3b7a/128`
input	入力ルート テーブルにあるエントリを表示します。
interface *interface_name*	（オプション）ルーティング テーブルを表示する特定のインターフェイスを指定します。
netmask *mask*	IPv4 アドレスの場合に、サブネット マスクを指定します。
output	出力ルート テーブルにあるエントリを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table routing コマンドは、アクセラレーション セキュリティ パスのルーティング テーブルの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table routing** コマンドの出力例を示します。

```
hostname# show asp table routing

in   255.255.255.255 255.255.255.255 identity
in   224.0.0.9       255.255.255.255 identity
in   10.86.194.60    255.255.255.255 identity
in   10.86.195.255   255.255.255.255 identity
in   10.86.194.0     255.255.255.255 identity
in   209.165.202.159 255.255.255.255 identity
in   209.165.202.255 255.255.255.255 identity
in   209.165.201.30  255.255.255.255 identity
in   209.165.201.0   255.255.255.255 identity
in   10.86.194.0     255.255.254.0   inside
in   224.0.0.0       240.0.0.0       identity
in   0.0.0.0         0.0.0.0         inside
out  255.255.255.255 255.255.255.255 foo
out  224.0.0.0       240.0.0.0       foo
out  255.255.255.255 255.255.255.255 test
out  224.0.0.0       240.0.0.0       test
out  255.255.255.255 255.255.255.255 inside
out  10.86.194.0     255.255.254.0   inside
out  224.0.0.0       240.0.0.0       inside
out  0.0.0.0         0.0.0.0         via 10.86.194.1, inside
out  0.0.0.0         0.0.0.0         via 0.0.0.0, identity
out  ::              ::              via 0.0.0.0, identity
```

関連コマンド

コマンド	説明
show route	制御プレーン内のルーティング テーブルを表示します。

show asp table vpn-context

アクセラレーション セキュリティ パスの VPN コンテキスト テーブルをデバッグするには、特権 EXEC モードで **show asp table vpn-context** コマンドを使用します。

show asp table vpn-context [**detail**]

シンタックスの説明

detail	（オプション）VPN コンテキスト テーブルに関する追加の詳細情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show asp table vpn-context コマンドは、アクセラレーション セキュリティ パスの VPN コンテキストの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。アクセラレーション セキュリティ パスの詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。これらのテーブルはデバッグのみを目的として使用するものであり、出力される情報は変更されることがあります。このコマンドを使用したシステム デバッグについて支援が必要な場合は、Cisco TAC にお問い合せください。

例

次に、**show asp table vpn-context** コマンドの出力例を示します。

```
hostname# show asp table vpn-context

VPN ID=0058070576, DECR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058193920, ENCR+ESP, UP, pk=0000000000, rk=0000000000, gc=0
VPN ID=0058168568, DECR+ESP, UP, pk=0000299627, rk=0000000061, gc=2
VPN ID=0058161168, ENCR+ESP, UP, pk=0000305043, rk=0000000061, gc=1
VPN ID=0058153728, DECR+ESP, UP, pk=0000271432, rk=0000000061, gc=2
VPN ID=0058150440, ENCR+ESP, UP, pk=0000285328, rk=0000000061, gc=1
VPN ID=0058102088, DECR+ESP, UP, pk=0000268550, rk=0000000061, gc=2
VPN ID=0058134088, ENCR+ESP, UP, pk=0000274673, rk=0000000061, gc=1
VPN ID=0058103216, DECR+ESP, UP, pk=0000252854, rk=0000000061, gc=2
...
```

次に、**show asp table vpn-context detail** コマンドの出力例を示します。

```
hostname# show asp table vpn-context detail

VPN Ctx  = 0058070576 [0x03761630]
State    = UP
Flags    = DECR+ESP
SA       = 0x037928F0
SPI      = 0xEA0F21F0
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0

VPN Ctx  = 0058193920 [0x0377F800]
State    = UP
Flags    = ENCR+ESP
SA       = 0x037B4B70
SPI      = 0x900FDC32
Group    = 0
Pkts     = 0
Bad Pkts = 0
Bad SPI  = 0
Spoof    = 0
Bad Crypto = 0
Rekey Pkt  = 0
Rekey Call = 0
...
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットのアクセラレーション セキュリティ パス カウンタを表示します。

show blocks

パケット バッファの使用状況を表示するには、特権 EXEC モードで **show blocks** コマンドを使用します。

show blocks [{***address*** *hex* | ***all*** | ***assigned*** | ***free*** | ***old*** | ***pool*** *size* [***summary***]} [**diagnostics** | ***dump*** | ***header*** | ***packet***] | ***queue history*** [***detail***]]

シンタックスの説明

address *hex*	（オプション）このアドレスに対応するブロックを 16 進形式で表示します。
all	（オプション）すべてのブロックを表示します。
assigned	（オプション）アプリケーションによって割り当てられ、使用されているブロックを表示します。
detail	（オプション）一意の各キュー タイプの最初のブロックの一部（128 バイト）を表示します。
dump	（オプション）ヘッダーとパケットの情報を含めて、ブロックの内容全体を表示します。dump と packet の相違点は、dump の場合、ヘッダーとパケットに関する追加情報が含まれることです。
diagnostics	（オプション）ブロックに関する診断を表示します。
free	（オプション）使用可能なブロックを表示します。
header	（オプション）ブロックのヘッダーを表示します。
old	（オプション）1 分より前に割り当てられたブロックを表示します。
packet	（オプション）パケットの内容をブロックのヘッダーと共に表示します。
pool *size*	（オプション）特定のサイズのブロックを表示します。
queue history	（オプション）セキュリティ アプライアンスがブロックを使い果たしたときに、ブロックが割り当てられる位置を表示します。ブロックはプールから割り当てられますが、一度もキューに割り当てられないことがあります。この場合に表示される位置は、ブロックを割り当てたコードのアドレスです。
summary	（オプション）ブロックの使用状況に関する詳細情報を表示します。この情報は、このクラスにブロックを割り当てたアプリケーションのプログラム アドレス、このクラスのブロックを解放したアプリケーションのプログラム アドレス、およびこのクラスの有効なブロックが属しているキューを基準としてソートされています。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	**pool summary** オプションが追加されました。

使用上のガイドライン

show blocks コマンドは、セキュリティ アプライアンスが過負荷になっているかどうかを判断する場合に役立ちます。このコマンドは、事前割り当て済みのシステム バッファの使用状況を表示します。トラフィックがセキュリティ アプライアンスを経由して移動している限り、メモリがすべて使用されている状態は問題にはなりません。**show conn** コマンドを使用すると、トラフィックが移動しているかどうかを確認できます。トラフィックが移動していないで、かつメモリがすべて使用されている場合は、問題がある可能性があります。

この情報は、SNMP を使用して表示することもできます。

セキュリティ コンテキスト内で表示される情報には、使用中のブロック、およびブロック使用状況の最高水準点について、コンテキスト固有の情報と共にシステム全体の情報も含まれています。

表示される出力については、「例」の項を参照してください。

例

次に、シングルモードでの **show blocks** コマンドの出力例を示します。

```
hostname# show blocks
  SIZE     MAX    LOW     CNT
     4    1600   1598    1599
    80     400    398     399
   256    3600   3540    3542
  1550    4716   3177    3184
 16384      10     10      10
  2048    1000   1000    1000
```

表 25-3 に、各フィールドの説明を示します。

表 25-3　show blocks のフィールド

フィールド	説明
SIZE	ブロック プールのサイズ（バイト単位）。それぞれのサイズは、特定のタイプを表しています。下に例を示します。
4	DNS モジュール、ISAKMP モジュール、URL フィルタリング モジュール、uauth モジュール、TFTP モジュール、TCP モジュールなどのアプリケーションの既存ブロックを複製します。
80	TCP 代行受信で確認応答パケットを生成するために、およびフェールオーバー hello メッセージに使用されます。

表 25-3　show blocks のフィールド（続き）

フィールド	説明
256	ステートフル フェールオーバーのアップデート、syslog 処理、およびその他の TCP 機能に使用されます。 これらのブロックは、主にステートフル フェールオーバーのメッセージに使用されます。アクティブなセキュリティ アプライアンスは、パケットを生成してスタンバイ セキュリティ アプライアンスに送信し、変換と接続のテーブルをアップデートします。接続が頻繁に作成または切断されるバースト トラフィックが発生すると、使用可能なブロックの数が 0 まで低下することがあります。この状況は、1 つまたはそれ以上の接続がスタンバイ セキュリティ アプライアンスに対してアップデートされなかったことを示しています。ステートフル フェールオーバー プロトコルは、不明な変換または接続を次回に捕捉します。256 バイト ブロックの CNT カラムが長時間にわたって 0 またはその付近で停滞している場合は、セキュリティ アプライアンスの処理している 1 秒あたりの接続数が非常に多いために、変換テーブルと接続テーブルの同期が取れている状態をセキュリティ アプライアンスが維持できない問題が発生しています。 セキュリティ アプライアンスから送信される syslog メッセージも 256 バイト ブロックを使用しますが、256 バイト ブロック プールが枯渇するような量が発行されることは通常ありません。CNT カラムの示す 256 バイト ブロックの数が 0 に近い場合は、Debugging（レベル 7）のログを syslog サーバに記録していないことを確認してください。この情報は、セキュリティ アプライアンス コンフィギュレーションの logging trap 行に示されています。ロギングは、デバッグのために詳細な情報が必要となる場合を除いて、Notification（レベル 5）以下に設定することをお勧めします。
1550	セキュリティ アプライアンスで処理するイーサネット パケットを格納するために使用されます。 パケットは、セキュリティ アプライアンス インターフェイスに入ると入力インターフェイス キューに配置され、次にオペレーティング システムに渡されてブロックに配置されます。セキュリティ アプライアンスは、パケットを許可するか拒否するかをセキュリティ ポリシーに基づいて決定し、パケットを出力インターフェイス上の出力キューに配置します。セキュリティ アプライアンスがトラフィックの負荷に対応できていない場合は、使用可能なブロックの数が 0 付近で停滞します（このコマンドの出力の CNT カラムに示されます）。CNT カラムが 0 になると、セキュリティ アプライアンスはさらにブロックを確保しようとします（最大で 8,192 個まで）。使用可能なブロックがなくなった場合、セキュリティ アプライアンスはパケットをドロップします。
16384	64 ビット 66 MHz のギガビット イーサネット カード（i82543）にのみ使用されます。 イーサネット パケットの詳細については、1550 の説明を参照してください。
2048	制御アップデートに使用される制御フレームまたはガイド付きフレーム。
MAX	指定したバイト ブロックのプールで使用可能なブロックの最大数。ブロックの最大数は、ブートアップ時にメモリに基づいて配分されます。ブロックの最大数は、通常は変化しません。例外は 256 バイト ブロックと 1,550 バイト ブロックで、セキュリティ アプライアンスはこれらのブロックを必要に応じて動的に作成できます（最大で 8,192 個まで）。

表 25-3　show blocks のフィールド（続き）

フィールド	説明
LOW	最低水準点。この数は、セキュリティ アプライアンスの電源がオンになった時点、またはブロックの内容が（**clear blocks** コマンドで）最後に消去された時点から、このサイズの使用可能なブロックが最も少なくなったときの数を示しています。LOW カラムが 0 である場合は、先行のイベントでメモリがすべて使用されたことを示します。
CNT	指定したサイズのブロック プールで現在使用可能なブロックの数。CNT カラムが 0 である場合は、メモリが現在すべて使用されていることを意味します。

次に、**show blocks all** コマンドの出力例を示します。

```
hostname# show blocks all
Class 0, size 4
     Block   allocd_by    freed_by  data size    alloccnt     dup_cnt  oper location
0x01799940  0x00000000  0x00101603          0           0           0 alloc
not_specified
0x01798e80  0x00000000  0x00101603          0           0           0 alloc
not_specified
0x017983c0  0x00000000  0x00101603          0           0           0 alloc
not_specified

...

    Found 1000 of 1000 blocks
    Displaying 1000 of 1000 blocks
```

表 25-4 に、各フィールドの説明を示します。

表 25-4　show blocks all のフィールド

フィールド	説明
Block	ブロックのアドレス。
allocd_by	ブロックを最後に使用したアプリケーションのプログラム アドレス（使用されていない場合は 0）。
freed_by	ブロックを最後に解放したアプリケーションのプログラム アドレス。
data size	ブロック内部のアプリケーション バッファまたはパケット データのサイズ。
alloccnt	このブロックが作成されてから使用された回数。
dup_cnt	このブロックに対する現時点での参照回数（このブロックが使用されている場合）。0 は 1 回の参照、1 は 2 回の参照を意味します。
oper	ブロックに対して最後に実行された操作。割り当て、取得、入力、解放の 4 つのいずれかです。
location	ブロックを使用しているアプリケーション。または、ブロックを最後に割り当てたアプリケーションのプログラム アドレス（allocd_by フィールドと同じ）。

次に、コンテキスト内での **show blocks** コマンドの出力例を示します。

```
hostname/contexta# show blocks
  SIZE    MAX    LOW    CNT  INUSE   HIGH
     4   1600   1599   1599      0      0
    80    400    400    400      0      0
   256   3600   3538   3540      0      1
  1550   4616   3077   3085      0      0
```

次に、**show blocks queue history** コマンドの出力例を示します。

```
hostname# show blocks queue history
Each Summary for User and Queue_type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    200     1 alloc   ip_rx             tcp       contexta
    108     1 get     ip_rx             udp       contexta
     85     1 free    fixup             h323_ras  contextb
     42     1 put     fixup             skinny    contextb

Block Size: 1550
Summary for User "http", Queue "tcp_unp_c_in", Blocks 1595, Queues 1000
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
...
```

次に、**show blocks queue history detail** コマンドの出力例を示します。

```
hostname# show blocks queue history detail
History buffer memory usage: 2136 bytes (default)
Each Summary for User and Queue type is followed its top 5 individual queues
Block Size: 4
Summary for User "http", Queue_Type "tcp_unp_c_in", Blocks 1595, Queues 1396
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
    186     1 put                               contexta
     15     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...

Summary for User "aaa", Queue "tcp_unp_c_in", Blocks 220, Queues 200
Blk_cnt Q_cnt Last_Op Queue_Type        User      Context
     21     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contexta
      1     1 put                               contextb
      1     1 put                               contextc
 First Block information for Block at 0x.....
  dup_count 0, flags 0x8000000, alloc_pc 0x43ea2a,
  start_addr 0xefb1074, read_addr 0xefb118c, write_addr 0xefb1193
  urgent_addr 0xefb118c, end_addr 0xefb17b2
  0efb1150: 00 00 00 03 47 c5 61 c5 00 05 9a 38 76 80 a3 00  |  ....G.a....8v...
  0efb1160: 00 0a 08 00 45 00 05 dc 9b c9 00 00 ff 06 f8 f3  |  ....E...........
  0efb1170: 0a 07 0d 01 0a 07 00 50 00 17 cb 3d c7 e5 60 62  |  .......P...=..`b
  0efb1180: 7e 73 55 82 50 18 10 00 45 ca 00 00 2d 2d 20 49  |  ~sU.P...E...-- I
  0efb1190: 50 20 2d 2d 0d 0a 31 30 2e 37 2e 31 33 2e 31 09  |  P --..10.7.13.1.
  0efb11a0: 3d 3d 3e 09 31 30 2e 37 2e 30 2e 38 30 0d 0a 0d  |  ==>.10.7.0.80...
...

total_count: total buffers in this class
```

次に、**show blocks pool summary** コマンドの出力例を示します。

```
hostname# show blocks pool 1550 summary
Class 3, size 1550

================================================
         total_count=1531    miss_count=0
Alloc_pc        valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000012
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
         total_count=9716    miss_count=0
Freed_pc        valid_cnt       invalid_cnt
0x9a81f3        00000104        00000007
         0x05006140 0x05000380 0x04fffa20 0x04ffde00 00000000 0x00000000
0x9a0326        00000053        00000033
         0x05006aa0 0x050057e0 0x05004e80 0x05003260 00000000 0x00000000
0x4605a2        00000005        00000000
         0x04ff5ac0 0x01e8e2e0 0x01e2eac0 0x01e17d20 00000000 0x00000000
...
================================================
         total_count=1531    miss_count=0
Queue   valid_cnt       invalid_cnt
0x3b0a18        00000256        00000000  Invalid Bad qtype
         0x01ad0760 0x01acfe00 0x01acf4a0 0x01aceb40 00000000 0x00000000
0x3a8f6b        00001275        00000000  Invalid Bad qtype
         0x05006aa0 0x05006140 0x050057e0 0x05004520 00000000
0x00000000

================================================
free_cnt=8185  fails=0  actual_free=8185  hash_miss=0
   03a8d3e0  03a8b7c0  03a7fc40  03a6ff20  03a6f5c0  03a6ec60 kao-f1#
```

表 25-5 に、各フィールドの説明を示します。

表 25-5　show blocks pool summary のフィールド

フィールド	説明
total_count	指定したクラスのブロックの数。
miss_count	技術的な理由により、指定したカテゴリで報告されなかったブロックの数。
Freed_pc	このクラスのブロックを解放したアプリケーションのプログラム アドレス。
Alloc_pc	このクラスにブロックを割り当てたアプリケーションのプログラム アドレス。
Queue	このクラスの有効なブロックが属しているキュー。
valid_cnt	現時点で割り当てられているブロックの数。
invalid_cnt	現時点では割り当てられていないブロックの数。
Invalid Bad qtype	このキューが解放されてコンテンツが無効になっているか、このキューは初期化されていませんでした。
Valid tcp_usr_conn_inp	キューは有効です。

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てられているメモリを増やします。
clear blocks	システム バッファの統計情報を消去します。
show conn	アクティブな接続を表示します。

show bootvar

ブート ファイルとコンフィギュレーションのプロパティを表示するには、特権コンフィギュレーション モードで ***show bootvar*** コマンドを使用します。

show bootvar

シンタックスの説明

show bootvar	システムのブート プロパティ。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

BOOT 変数は、さまざまなデバイス上の起動イメージのリストを指定するものです。CONFIG_FILE 変数は、システム初期化中に使用されるコンフィギュレーション ファイルを指定します。これらの変数は、それぞれ ***boot system*** コマンドと ***boot config*** コマンドで設定します。

例

次の例では、BOOT 変数が disk0:/f1_image を保持しています。これは、システムのリロード時にブートされるイメージです。BOOT の現在の値は、disk0:/f1_image; disk0:f1_backupimage です。これは、BOOT 変数が boot system コマンドで変更されているものの、実行コンフィギュレーションがまだ ***write memory*** コマンドで保存されていないことを意味しています。実行コンフィギュレーションを保存すると、BOOT 変数と現在の BOOT 変数が両方とも disk0:/f1_image; disk0:f1_backupimage になります。実行コンフィギュレーションが保存済みである場合、ブート ローダーは BOOT 変数の内容をロードしようとします。つまり、disk0:/f1image を起動します。このイメージが存在しないか無効である場合は、disk0:/f1_backupimage をブートしようとします。

CONFIG_FILE 変数は、システムのスタートアップ コンフィギュレーションをポイントします。この例ではこの変数が設定されていないため、スタートアップ コンフィギュレーション ファイルは、***boot config*** コマンドで指定したデフォルトです。現在の CONFIG_FILE 変数は、***boot config*** コマンドで変更して、***write memory*** コマンドで保存することができます。

```
hostname# show bootvar
BOOT variable = disk0:/f1_image
Current BOOT variable = disk0:/f1_image; disk0:/f1_backupimage
CONFIG_FILE variable =
Current CONFIG_FILE variable =
hostname#
```

関連コマンド

コマンド	説明
boot	起動時に使用されるコンフィギュレーション ファイルまたはイメージ ファイルを指定します。

show capture

キャプチャのコンフィギュレーションを表示するには、オプションを指定せずに **show capture** コマンドを使用します。

show capture [*capture_name*] [**access-list** *access_list_name*] [**count** *number*] [**decode**] [**detail**] [**dump**] [**packet-number** *number*]

シンタックスの説明

capture_name	（オプション）パケット キャプチャの名前。
access-list *access_list_name*	（オプション）特定のアクセス リストの IP フィールドまたはより高位のフィールドに基づいて、パケットに関する情報を表示します。
count *number*	（オプション）指定したパケットの数に関するデータを表示します。
decode	このオプションは、isakmp タイプのキャプチャがインターフェイスに適用されている場合に役立ちます。当該のインターフェイスを通過する isakmp データは、復号化の後にすべてキャプチャされ、フィールドをデコードした後にその他の情報と共に表示されます。
detail	（オプション）各パケットの詳細なプロトコル情報を表示します。
dump	（オプション）データ リンク トランスポート経由で伝送されるパケットの 16 進ダンプを表示します。
packet-number *number*	指定したパケット番号から表示を開始します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

セキュリティ コンテキスト モード：シングル コンテキスト モードおよびマルチ コンテキスト モード

アクセス場所：システムおよびコンテキストのコマンドライン

コマンド モード：特権モード

ファイアウォール モード：ルーテッド ファイアウォール モードおよび透過ファイアウォール モード

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

capture_name を指定した場合は、そのキャプチャのキャプチャ バッファの内容が表示されます。

dump キーワードを指定しても、MAC に関する情報は 16 進ダンプに表示されません。

パケットのデコード出力は、パケットのプロトコルによって形式が異なります。表 25-6 で [ ] に囲まれている出力は、**detail** キーワードを指定した場合に表示されます。

表 25-6　パケット キャプチャの出力形式

パケットのタイプ	キャプチャの出力形式
802.1Q	*HH:MM:SS.ms* [ether-hdr] *VLAN-info encap-ether-packet*
ARP	*HH:MM:SS.ms* [ether-hdr] *arp-type arp-info*

表 25-6　パケット キャプチャの出力形式（続き）

パケットのタイプ	キャプチャの出力形式
IP/ICMP	*HH:MM:SS.ms* [ether-hdr] *ip-source* > *ip-destination:* icmp: *icmp-type icmp-code* [checksum-failure]
IP/UDP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port dest-addr.dst-port*: [checksum-info] udp *payload-len*
IP/TCP	*HH:MM:SS.ms* [ether-hdr] *src-addr.src-port* d*est-addr.dst-port*: *tcp-flags* [header-check] [checksum-info] *sequence-number ack-number tcp-window urgent-info tcp-options*
IP/ その他	*HH:MM:SS.ms* [ether-hdr] *src-addr dest-addr*: *ip-protocol ip-length*
その他	*HH:MM:SS.ms ether-hdr*: *hex-dump*

例

次の例は、キャプチャのコンフィギュレーションを表示する方法を示しています。

```
hostname(config)# show capture
capture arp ethernet-type arp interface outside
capture http access-list http packet-length 74 interface inside
```

次の例は、ARP キャプチャによってキャプチャされたパケットを表示する方法を示しています。

```
hostname(config)# show capture arp
2 packets captured
19:12:23.478429 arp who-has 171.69.38.89 tell 171.69.38.10
19:12:26.784294 arp who-has 171.69.38.89 tell 171.69.38.10
2 packets shown
```

関連コマンド

コマンド	説明
capture	パケット キャプチャ機能を有効にして、パケットのスニッフィングやネットワーク障害を検出できるようにします。
clear capture	キャプチャ バッファを消去します。
copy capture	キャプチャ ファイルをサーバにコピーします。

show chardrop

シリアル コンソールからドロップされた文字の数を表示するには、特権 EXEC モードで **show chardrop** コマンドを使用します。

show chardrop

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show chardrop** コマンドの出力例を示します。

```
hostname# show chardrop
```

Chars dropped pre-TxTimeouts: 0, post-TxTimeouts: 0

関連コマンド

コマンド	説明
show running-config	現在の実行コンフィギュレーションを表示します。

show checkheaps

チェックヒープに関する統計情報を表示するには、特権 EXEC モードで **show checkheaps** コマンドを使用します。チェックヒープは、ピープ メモリ バッファ（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられる）の健全性およびコード領域の完全性を確認する定期的なプロセスです。

show checkheaps

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show checkheapls** コマンドの出力例を示します。

```
hostname# show checkheaps

Checkheaps stats from buffer validation runs
--------------------------------------------
Time elapsed since last run     : 42 secs
Duration of last run            : 0 millisecs
Number of buffers created       : 8082
Number of buffers allocated     : 7808
Number of buffers free          : 274
Total memory in use             : 43570344 bytes
Total memory in free buffers    : 87000 bytes
Total number of runs            : 310
```

関連コマンド

コマンド	説明
checkheaps	チェックヒープの確認間隔を設定します。

show checksum

コンフィギュレーションのチェックサムを表示するには、特権 EXEC モードで **show checksum** コマンドを使用します。

show checksum

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

show checksum コマンドを使用すると、コンフィギュレーションの内容のデジタル サマリーとして機能する 16 進数の 4 つのグループを表示できます。このチェックサムが計算されるのは、コンフィギュレーションをフラッシュ メモリに格納するときのみです。

show config コマンドまたは **show checksum** コマンドの出力でチェックサムの前にドット「.」が表示された場合、この出力は、通常のコンフィギュレーション読み込みまたは書き込みモードのインジケータを示しています（セキュリティ アプライアンス フラッシュ パーティションからの読み込み、またはセキュリティ アプライアンス フラッシュ パーティションへの書き込み時）。「.」は、セキュリティ アプライアンスが処理に占有されているが「ハングアップ」していないことを示しています。このメッセージは、「system processing, please wait」メッセージと同様です。

例

次の例は、コンフィギュレーションまたはチェックサムを表示する方法を示しています。

```
hostname(config)# show checksum
Cryptochecksum: 1a2833c0 129ac70b 1a88df85 650dbb81
```

show chunkstat

チャンクに関する統計情報を表示するには、特権 EXEC モードで **show chunkstat** コマンドを使用します。

show chunkstat

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、チャンクに関する統計情報を表示する方法を示しています。

```
hostname# show chunkstat
Global chunk statistics: created 181, destroyed 34, siblings created 94, siblings
destroyed 34

Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01edb4cc, name "Managed Chunk Queue Elements", data start @ 01edbd24,
end @ 01eddc54
next: 01eddc8c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 499, elt size: 16, index first free 498
# chunks in use: 1, HWM of total used: 1, alignment: 0
Per-chunk statistics: siblings created 0, siblings trimmed 0
Dump of chunk at 01eddc8c, name "Registry Function List", data start @ 01eddea4, end @
01ede348
next: 01ede37c, next_sibling: 00000000, prev_sibling: 00000000
flags 00000001
maximum chunk elt's: 99, elt size: 12, index first free 42
# chunks in use: 57, HWM of total used: 57, alignment: 0
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
show cpu	CPU の使用状況に関する情報を表示します。

show class

クラスに割り当てられたコンテキストを表示するには、特権 EXEC モードで **show class** コマンドを使用します。

show class *name*

シンタックスの説明

name	20 文字までの長さの文字列として名前を指定します。デフォルト クラスを表示するには、名前として **default** と入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show class default** コマンドの出力例を示します。

```
hostname# show class default

Class Name           Members    ID   Flags
default                All       1    0001
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス コンフィギュレーションを消去します。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスに対してリソース制限を設定します。
member	リソース クラスにコンテキストを割り当てます。

show clock

セキュリティ アプライアンス上の時刻を表示するには、ユーザ EXEC モードで **show clock** コマンドを使用します。

show clock [**detail**]

シンタックスの説明

detail	（オプション）クロックのソース（NTP またはユーザ設定）と現在のサマータイム設定（存在する場合）を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show clock** コマンドの出力例を示します。

```
hostname> show clock
12:35:45.205 EDT Tue Jul 27 2004
```

次に、**show clock detail** コマンドの出力例を示します。

```
hostname> show clock detail
12:35:45.205 EDT Tue Jul 27 2004
Time source is user configuration
Summer time starts 02:00:00 EST Sun Apr 4 2004
Summer time ends 02:00:00 EDT Sun Oct 31 2004
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。
ntp server	NTP サーバを指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show compression svc

SVC 接続の圧縮統計情報をセキュリティ アプライアンス上に表示するには、特権 EXEC モードで **show compression svc** コマンドを使用します。

show compression svc

デフォルト

このコマンドには、デフォルトの動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、**show compression svc** コマンドの出力例を示します。

```
hostname# show compression svc
Compression SVC Sessions                        1
Compressed Frames                          249756
Compressed Data In (bytes)                0048042
Compressed Data Out (bytes)               4859704
Expanded Frames                                 1
Compression Errors                              0
Compression Resets                              0
Compression Output Buf Too Small                0
Compression Ratio                            2.06
Decompressed Frames                        876687
Decompressed Data In                    279300233
```

関連コマンド

コマンド	説明
compression	すべての SVC および WebVPN 接続の圧縮をイネーブルにします。
svc compression	SVC 接続上の http データの圧縮を特定のグループまたはユーザに対してイネーブルにします。

show conn

指定した接続タイプの接続状態を表示するには、特権 EXEC モードで **show conn** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

show conn [**all** | **count**] [**state** *state_type*] | [{{**foreign** | **local**} *ip* [*-ip2*] **netmask** *mask*}] | [**long** | ***detail***] | [{{**lport** | **fport**} *port1*} [*-port2*]] | [**protocol** {**tcp** | **udp**}]

シンタックスの説明

all	デバイスを通過するトラフィックの接続に加えて、デバイスへの接続とデバイスからの接続を表示します。
count	（オプション）アクティブな接続の数を表示します。
detail	変換タイプとインターフェイスの情報を含めて、接続の詳細を表示します。
foreign	指定した外部 IP アドレスとの接続を表示します。
fport	指定した外部ポートとの接続を表示します。
ip	ドット付き 10 進表記の IP アドレス。または、IP アドレス範囲の開始アドレス。
-ip2	（オプション）IP アドレス範囲の終了 IP アドレス。
local	指定したローカル IP アドレスとの接続を表示します。
long	（オプション）接続をロング フォーマットで表示します。
lport	指定したローカル ポートとの接続を表示します。
netmask	指定した IP アドレスに使用するサブネット マスクを指定します。
mask	ドット付き 10 進表記のサブネット マスク。
port1	ポート番号。または、ポート番号範囲の開始ポート番号。
-port2	（オプション）ポート番号範囲の終了ポート番号。
protocol	（オプション）接続プロトコルを指定します。
state	（オプション）指定した接続の状態を表示します。
state_type	接続状態タイプを指定します。接続状態タイプに使用できるキーワードのリストについては、表 25-7 を参照してください。
tcp	TCP プロトコル接続を表示します。
udp	UDP プロトコル接続を表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show conn コマンドは、アクティブな TCP 接続の数を表示し、さまざまなタイプの接続に関する情報を提供します。接続のテーブル全体を参照するには、**show conn all** コマンドを使用します。

(注)　セカンダリ接続を可能にするためのピンホールをセキュリティ アプライアンスが作成するとき、この接続は **show conn** コマンドでは不完全な接続として表示されます。この不完全な接続を消去するには、**clear local** コマンドを使用します。

表 25-7 に、**show conn state** コマンドを使用するときに指定できる接続タイプを示します。複数の接続タイプを指定する場合は、キーワードをカンマで区切り、スペースは入れません。

表 25-7　接続状態のタイプ

キーワード	表示される接続タイプ
up	アップ状態の接続
conn_inbound	着信接続
ctiqbe	CTIQBE 接続
data_in	着信データ接続
data_out	発信データ接続
finin	FIN 着信接続
finout	FIN 発信接続
h225	H.225 接続
h323	H.323 接続
http_get	HTTP get 接続
mgcp	MGCP 接続
nojava	Java アプレットへのアクセスを拒否する接続
rpc	RPC 接続
service_module	SSM によってスキャンされる接続
sip	SIP 接続
skinny	SCCP 接続
smtp_data	SMTP メール データ接続
sqlnet_fixup_data	SQL*Net データ検査エンジン接続

detail オプションを使用すると、表 25-8 に示した接続フラグを使用して、変換タイプとインターフェイスに関する情報が表示されます。

表 25-8　接続フラグ

フラグ	説明
a	SYN に対する外部 ACK（確認応答）を待機
A	SYN に対する内部 ACK（確認応答）を待機
B	外部からの初期 SYN
C	Computer Telephony Interface Quick Buffer Encoding（CTIQBE）メディア接続
d	ダンプ
D	DNS
E	外部バック接続
f	内部 FIN
F	外部 FIN

表 25-8　接続フラグ（続き）

フラグ	説明
g	Media Gateway Control Protocol（MGCP）接続
G	接続がグループの一部[1]
h	H.225
H	H.323
i	不完全な TCP または UDP 接続
I	着信データ
k	Skinny Client Control Protocol（SCCP）メディア接続
K	GTP t3 応答
m	SIP メディア接続
M	SMTP データ
O	発信データ
p	複製（未使用）
P	内部バック接続
q	SQL*Net データ
r	確認応答された内部 FIN
R	TCP 接続に対する、確認応答された外部 FIN
R	UDP RPC[2]
s	外部 SYN を待機
S	内部 SYN を待機
t	SIP 一時接続[3]
T	SIP 接続[4]
U	アップ
X	CSC SSM などのサービス モジュールに検査される。

1. G フラグは、接続がグループの一部であることを示します。GRE および FTP の Strict フィックスアップによって設定され、制御接続と関連するすべてのセカンダリ接続を指定します。制御接続が終了すると、関連するすべてのセカンダリ接続も終了します。
2. **show conn** コマンド出力の各行は 1 つの接続（TCP または UDP）を表すため、1 行に 1 つの R フラグだけが存在します。
3. UDP 接続の場合、値 t は接続が 1 分後にタイムアウトすることを示しています。
4. UDP 接続の場合、値 T は、**timeout sip** コマンドを使用して指定した値に従って接続がタイムアウトすることを示しています。

（注） DNS サーバを使用する接続の場合、**show conn** コマンドの出力で、接続の送信元ポートが DNS サーバの IP アドレスに置き換えられることがあります。

複数の DNS セッションが同じ 2 つのホスト間で発生し、それらのセッションの 5 つのタプル（送信元 / 宛先 IP アドレス、送信元 / 宛先ポート、およびプロトコル）が同じものである場合、それらのセッションに対しては接続が 1 つのみ作成されます。DNS の識別情報は、*app_id* によって追跡され、各 app_id のアイドル タイマーはそれぞれ独立して動作します。

app_id の有効期限はそれぞれ独立して満了するため、正当な DNS 応答がセキュリティ アプライアンスを通過できるのは、限られた期間内のみであり、リソースの継続使用はできません。ただし、**show conn** コマンドを入力すると、DNS 接続のアイドル タイマーが新しい DNS セッションによってリセットされているように見えます。これは共有 DNS 接続の性質によるものであり、仕様です。

（注） **conn timeout** コマンドで定義した非アクティブ期間（デフォルトは 01:00:00）中に TCP トラフィックがまったく発生しなかった場合は、接続が終了し、対応する接続フラグ エントリも表示されなくなります。

例

複数の接続タイプを指定する場合は、キーワードをカンマで区切り、スペースは入れません。次の例では、アップ状態の RPC 接続、H.323 接続、および SIP 接続に関する情報を表示しています。

```
hostname# show conn state up,rpc,h323,sip
```

次の例は、内部ホスト 10.1.1.15 から 192.168.49.10 の外部 Telnet サーバへの TCP セッション接続を示しています。B フラグが存在しないため、接続は内部から開始されています。「U」フラグ、「I」フラグ、および「O」フラグは、接続がアクティブであり、着信データと発信データを受信したことを示しています。

```
hostname# show conn
2 in use, 2 most used
TCP out 192.168.49.10:23 in 10.1.1.15:1026 idle 0:00:22
Bytes 1774 flags UIO
UDP out 192.168.49.10:31649 in 10.1.1.15:1028 idle 0:00:14
flags D-
```

次の例には、接続が SSM によってスキャンされていることを示す「X」フラグが含まれています。

```
hostname(config)# show conn local 10.0.0.122 state service_module
TCP out 10.1.0.121:22 in 10.0.0.122:34446 idle 0:00:03 bytes 2733 flags UIOX
```

次の例は、外部ホスト 192.168.49.10 から内部ホスト 10.1.1.15 への UDP 接続を示しています。D フラグは、DNS 接続であることを示しています。1028 は、接続上の DNS ID です。

```
hostname(config)# show conn detail
2 in use, 2 most used
Flags: A - awaiting inside ACK to SYN, a - awaiting outside ACK to SYN,
       B - initial SYN from outside, C - CTIBQE media, D - DNS, d - dump,
       E - outside back connection, f - inside FIN, F - outside FIN,
       G - group, g - MGCP, H - H.323, h - H.255.0, I - inbound data, i - incomplete,
       k - Skinny media, M - SMTP data, m - SIP media
       O - outbound data, P - inside back connection,
       q - SQL*Net data, R - outside acknowledged FIN,
       R - UDP RPC, r - inside acknowledged FIN, S - awaiting inside SYN,
       s - awaiting outside SYN, T - SIP, t - SIP transient, U - up
       X - inspected by service module
TCP outside:192.168.49.10/23 inside:10.1.1.15/1026 flags UIO
UDP outside:192.168.49.10/31649 inside:10.1.1.15/1028 flags dD
```

次に、**show conn all** コマンドの出力例を示します。

```
hostname# show conn all
6 in use, 6 most used
  TCP out 209.165.201.1:80 in 10.3.3.4:1404 idle 0:00:00 Bytes 11391
  TCP out 209.165.201.1:80 in 10.3.3.4:1405 idle 0:00:00 Bytes 3709
  TCP out 209.165.201.1:80 in 10.3.3.4:1406 idle 0:00:01 Bytes 2685
  TCP out 209.165.201.1:80 in 10.3.3.4:1407 idle 0:00:01 Bytes 2683
  TCP out 209.165.201.1:80 in 10.3.3.4:1403 idle 0:00:00 Bytes 15199
  TCP out 209.165.201.1:80 in 10.3.3.4:1408 idle 0:00:00 Bytes 2688
  UDP out 209.165.201.7:24 in 10.3.3.4:1402 idle 0:01:30
  UDP out 209.165.201.7:23 in 10.3.3.4:1397 idle 0:01:30
  UDP out 209.165.201.7:22 in 10.3.3.4:1395 idle 0:01:30
```

例では、内部のホスト 10.3.3.4 が 209.165.201.1 の Web サイトにアクセスしています。外部インターフェイス上のグローバル アドレスは、209.165.201.7 です。

関連コマンド

コマンド	説明
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
inspect mgcp	MGCP アプリケーション検査をイネーブルにします。
inspect sip	Java アプレットを HTTP トラフィックから削除します。
inspect skinny	SCCP アプリケーション検査をイネーブルにします。

show console-output

現在キャプチャされているコンソール出力を表示するには、特権 EXEC モードで **show console-output** コマンドを使用します。

show console-output

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、コンソール出力がない場合に表示されるメッセージを示しています。

```
hostname# show console-output
Sorry, there are no messages to display
```

関連コマンド

コマンド	説明
clear configure console	デフォルトのコンソール接続設定に戻します。
clear configure timeout	コンフィギュレーションにあるアイドル期間をデフォルトに戻します。
console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定します。
show running-config console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを表示します。

show context

割り当てられているインターフェイス、コンフィギュレーション ファイルの URL、および設定済みコンテキストの数を含めてコンテキスト情報を表示するには（または、システム実行スペースからすべてのコンテキストのリストを表示するには）、特権 EXEC モードで **show context** コマンドを使用します。

show context [*name* | ***detail*** | ***count***]

シンタックスの説明

count	（オプション）設定済みコンテキストの数を表示します。
detail	（オプション）実行状態および内部使用のための情報を含めて、コンテキストに関する詳細な情報を表示します。
name	（オプション）コンテキスト名を設定します。名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。コンテキスト内で入力できるのは、現在のコンテキスト名のみです。

デフォルト

システム実行スペースでは、名前を指定しない場合、セキュリティ アプライアンスはすべてのコンテキストを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

次に、**show context** コマンドの出力例を示します。この表示例では、3 つのコンテキストが表示されています。

```
hostname# show context

Context Name      Interfaces                  URL
*admin            GigabitEthernet0/1.100      flash:/admin.cfg
                  GigabitEthernet0/1.101
contexta          GigabitEthernet0/1.200      flash:/contexta.cfg
                  GigabitEthernet0/1.201
contextb          GigabitEthernet0/1.300      flash:/contextb.cfg
                  GigabitEthernet0/1.301
Total active Security Contexts: 3
```

表 25-9 に、各フィールドの説明を示します。

表 25-9　show context のフィールド

フィールド	説明
Context Name	すべてのコンテキスト名が一覧表示されます。アスタリスク（*）の付いているコンテキスト名は、管理コンテキストです。
Interfaces	コンテキストに割り当てられるインターフェイス。
URL	セキュリティ アプライアンスがコンテキストのコンフィギュレーションをロードする URL。

次に、**show context detail** コマンドの出力例を示します。

```
hostname# show context detail

Context "admin", has been created, but initial ACL rules not complete
  Config URL: flash:/admin.cfg
  Real Interfaces: Management0/0
  Mapped Interfaces: Management0/0
  Flags: 0x00000013, ID: 1

Context "ctx", has been created, but initial ACL rules not complete
  Config URL: ctx.cfg
  Real Interfaces: GigabitEthernet0/0.10, GigabitEthernet0/1.20,
     GigabitEthernet0/2.30
  Mapped Interfaces: int1, int2, int3
  Flags: 0x00000011, ID: 2

Context "system", is a system resource
  Config URL: startup-config
  Real Interfaces:
  Mapped Interfaces: Control0/0, GigabitEthernet0/0,
     GigabitEthernet0/0.10, GigabitEthernet0/1, GigabitEthernet0/1.10,
     GigabitEthernet0/1.20, GigabitEthernet0/2, GigabitEthernet0/2.30,
     GigabitEthernet0/3, Management0/0, Management0/0.1
  Flags: 0x00000019, ID: 257

Context "null", is a system resource
  Config URL: ... null ...
  Real Interfaces:
  Mapped Interfaces:
  Flags: 0x00000009, ID: 258
```

表 25-10 に、各フィールドの説明を示します。

表 25-10　コンテキストの状態

フィールド	説明
コンテキスト	コンテキストの名前。ヌル コンテキストの情報は内部でのみ使用されます。system というコンテキストは、システム実行スペースを表しています。
（状態メッセージ）	コンテキストの状態。次に、表示される可能性のあるメッセージを示します。

表 25-10　コンテキストの状態（続き）

フィールド	説明
Has been created, but initial ACL rules not complete	セキュリティ アプライアンスはコンフィギュレーションを解析しましたが、デフォルト セキュリティ ポリシーを確立するためのデフォルト ACL をまだダウンロードしていません。デフォルト セキュリティ ポリシーは、すべてのコンテキストに対して最初に適用されるもので、セキュリティ レベルの低い方から高い方に向かうトラフィックを拒否し、アプリケーション検査およびその他のパラメータをイネーブルにします。このセキュリティ ポリシーによって、コンフィギュレーションが解析されてからコンフィギュレーションの ACL がコンパイルされるまでの間に、トラフィックがセキュリティ アプライアンスを一切通過しないことが保証されます。コンフィギュレーションの ACL は非常に高速でコンパイルされるため、この状態が表示されることはほとんどありません。
Has been created, but not initialized	**context** *name* コマンドを入力しましたが、まだ **config-url** コマンドを入力していません。
Has been created, but the config hasn't been parsed	デフォルトの ACL がダウンロードされましたが、まだセキュリティ アプライアンスがコンフィギュレーションを解析していません。この状態が表示される場合は、ネットワーク接続に問題があるために、コンフィギュレーションのダウンロードが失敗した可能性があります。または、**config-url** コマンドをまだ入力していません。コンフィギュレーションをリロードするには、コンテキスト内から **copy startup-config running-config** を入力します。システムから、**config-url** コマンドを再度入力します。または、空白の実行コンフィギュレーションの設定を開始します。
Is a system resource	この状態に該当するのは、システム実行スペースとヌル コンテキストのみです。ヌル コンテキストはシステムによって使用され、この情報は内部でのみ使用されます。
Is a zombie	**no context** コマンドまたは **clear context** コマンドを使用してコンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Is active	このコンテキストは現在実行中であり、コンテキスト コンフィギュレーションのセキュリティ ポリシーに従ってトラフィックを通過させることができます。
Is ADMIN and active	このコンテキストは管理コンテキストであり、現在実行中です。
Was a former ADMIN, but is now a zombie	**clear configure context** コマンドを使用して管理コンテキストを削除しましたが、コンテキストの情報は、セキュリティ アプライアンスがコンテキスト ID を新しいコンテキストに再利用するか、セキュリティ アプライアンスを再起動するまでメモリに保持されます。
Real Interfaces	コンテキストに割り当てられるインターフェイス。インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、この表示内容はインターフェイスの実際の名前を示しています。システム実行スペースは、すべてのインターフェイスを含んでいます。

表 25-10　コンテキストの状態（続き）

フィールド	説明
Mapped Interfaces	インターフェイスの ID を **allocate-interface** コマンドでマッピングした場合、この表示内容はマッピングされた名前を示しています。インターフェイスをマッピングしなかった場合は、実際の名前がもう一度表示されます。
Flag	内部でのみ使用されます。
ID	このコンテキストの内部 ID。

次に、**show context count** コマンドの出力例を示します。

```
hostname# show context count
Total active contexts: 2
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。

show controller

ASA 5505 適応型セキュリティ アプライアンスのシステムに存在するすべてのインターフェイスのコントローラ固有の情報を表示するには、特権 EXEC モードで **show controller** コマンドを使用します。

show controller [*switch_port*]

シンタックスの説明

switch_port	（オプション）インターフェイス ID を特定します（**ethernet0/0** ～ **ethernet0/7**）。

デフォルト

スイッチ ポートを特定しない場合、このコマンドはすべてのインターフェイスの情報を表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

Cisco TAC では、このコマンドを使用して内部で見つかった欠陥や、顧客が見つけた欠陥を調査する際にコントローラに関するデバッグ情報を収集します。

例

次に、**show controller** コマンドの出力例を示します。

```
hostname# show controller

Ethernet0/0:
   Marvell 88E6095 revision 2, switch port 7
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x40a1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x4c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0907  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0074
         Port Ctrl-1:   0x0000  Vlan Map:      0x077f
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0080
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

     Global Registers:
         Control:       0x0482
```

```
-------------------------------------------------------------------
Number of VLANs: 1
-------------------------------------------------------------------
Vlan[db]\Port|  0 |  1 |  2 |  3 |  4 |  5 |  6 |  7 |  8 |  9 | 10 |
-------------------------------------------------------------------
  <0001[01]> | EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUT| EUM| NM | NM |
-------------------------------------------------------------------

Ethernet0/1:
   Marvell 88E6095 revision 2, switch port 6
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x0130
         PHY Status:    0x0040  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07bf
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0040
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/2:
   Marvell 88E6095 revision 2, switch port 5
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x41e1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x6c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0d07  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07df
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0020
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/3:
   Marvell 88E6095 revision 2, switch port 4
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x41e1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x6c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0d07  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07ef
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0010
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
```

```
Ethernet0/4:
   Marvell 88E6095 revision 2, switch port 3
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x41e1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x6c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0d07  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07f7
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0008
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/5:
   Marvell 88E6095 revision 2, switch port 2
     PHY Register:
         Control:       0x3000  Status:        0x786d
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x41e1
         Auto Neg Ex:   0x0005  PHY Spec Ctrl: 0x0130
         PHY Status:    0x6c00  PHY Intr En:   0x0400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0d07  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fb
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0004
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000

Ethernet0/6:
   Marvell 88E6095 revision 2, switch port 1
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fd
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0002
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
```

```
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

Ethernet0/7:
   Marvell 88E6095 revision 2, switch port 0
     PHY Register:
         Control:       0x3000  Status:        0x7849
         Identifier1:   0x0141  Identifier2:   0x0c85
         Auto Neg:      0x01e1  LP Ability:    0x0000
         Auto Neg Ex:   0x0004  PHY Spec Ctrl: 0x8130
         PHY Status:    0x0040  PHY Intr En:   0x8400
         Int Port Sum:  0x0000  Rcv Err Cnt:   0x0000
         Led select:    0x1a34
         Reg 29:        0x0003  Reg 30:        0x0000
     Port Registers:
         Status:        0x0007  PCS Ctrl:      0x0003
         Identifier:    0x0952  Port Ctrl:     0x0077
         Port Ctrl-1:   0x0000  Vlan Map:      0x07fe
         VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
         Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
         Port Asc Vt:   0x0001
         In Discard Lo: 0x0000  In Discard Hi: 0x0000
         In Filtered:   0x0000  Out Filtered:  0x0000
   ----Inline power related counters and registers----
   Power on fault: 0  Power off fault: 0
   Detect enable fault: 0  Detect disable fault: 0
   Faults: 0
   Driver counters:
   I2C Read Fail: 0   I2C Write Fail: 0
   Resets: 1  Initialized: 1
   PHY reset error: 0
   LTC4259 registers:
   INTRPT STATUS = 0x88  INTRPT MASK   = 0x00  POWER EVENT   = 0x00
   DETECT EVENT  = 0x03  FAULT EVENT   = 0x00  TSTART EVENT  = 0x00
   SUPPLY EVENT  = 0x02  PORT1 STATUS  = 0x06  PORT2 STATUS  = 0x06
   PORT3 STATUS  = 0x00  PORT4 STATUS  = 0x00  POWER STATUS  = 0x00
   OPERATE MODE  = 0x0f  DISC. ENABLE  = 0x30  DT/CLASS ENBL = 0x33
   TIMING CONFIG = 0x00  MISC. CONFIG  = 0x00

Internal-Data0/0:
   Y88ACS06 Register settings:
    rap                           0xe0004000 = 0x00000000
    ctrl_status                   0xe0004004 = 0x5501064a
    irq_src                       0xe0004008 = 0x00000000
    irq_msk                       0xe000400c = 0x00000000
    irq_hw_err_src                0xe0004010 = 0x00000000
    irq_hw_err_msk                0xe0004014 = 0x00001000
    bmu_cs_rxq                    0xe0004060 = 0x002aaa80
    bmu_cs_stxq                   0xe0004068 = 0x01155540
    bmu_cs_atxq                   0xe000406c = 0x012aaa80

   Bank 2: MAC address registers:
    mac_addr1_lo                  0xe0004100 = 0x00000000
    mac_addr1_hi                  0xe0004104 = 0x00000000
    mac_addr2_lo                  0xe0004108 = 0x00000000
    mac_addr2_hi                  0xe000410c = 0x00000000
    mac_addr3_lo                  0xe0004110 = 0x00000000
    mac_addr3_hi                  0xe0004114 = 0x00000000
    chip_info                     0xe0004118 = 0xb0110000
    eprom                         0xe000411c = 0x00000000
    flash_addr_reg                0xe0004120 = 0x0001fffe
    flash_data_port               0xe0004124 = 0x000000ff
```

```
 loader                          0xe0004128 = 0x00000400
 timer_init_val                  0xe0004130 = 0x00000000
 timer_val                       0xe0004134 = 0x00000000
 timer_ctrl                      0xe0004138 = 0x00000202
 irq_mod_timer_init_val          0xe0004140 = 0x00000000
 irq_mod_timer                   0xe0004144 = 0x00000000
 irq_mod_timer_ctrl              0xe0004148 = 0x00000202
 irq_mod_msk                     0xe000414c = 0x00000000
 irq_hw_err_mod_mask             0xe0004150 = 0x00000000
 tst_ctrl                        0xe0004158 = 0x00000001
 gp_io                           0xe000415c = 0x0000000f
 i2c_ctrl                        0xe0004160 = 0x00000000
 i2c_data                        0xe0004164 = 0x00000000
 i2c_irq                         0xe0004168 = 0x00000000
 i2c_sw                          0xe000416c = 0x00000003

RAM Random Registers:
 ram_addr                        0xe0004180 = 0x00000000
 ram_data_port_lo                0xe0004184 = 0x00000000
 ram_data_port_hi                0xe0004188 = 0x00000000

Ram Interface Registers:
 ram_if_to_lo                    0xe0004190 = 0x24242424
 ram_if_to_hi                    0xe0004194 = 0x00002424
 ram_if_timeout_val              0xe000419c = 0x00000000
 ram_if_ctrl                     0xe00041a0 = 0x000a0002

Transmit Arbiter MAC:
 tx_arb_iti_init                 0xe0004200 = 0x00000000
 tx_arb_iti_val                  0xe0004204 = 0x00000000
 tx_arb_lim_init                 0xe0004208 = 0x00000000
 tx_arb_lim_val                  0xe000420c = 0x00000000
 tx_arb_ctrl_tst_status          0xe0004210 = 0x00001256

Bank 8: Receive queue registers:
 rx_qregs.buf_ctrl               0xe0004400 = 0xc8550800
 rx_qregs.next_desc_addr_lo      0xe0004404 = 0x016d4020
 rx_qregs.buf_addr_lo            0xe0004408 = 0x019acd00
 rx_qregs.buf_addr_hi            0xe000440c = 0x00000000
 rx_qregs.frame_sw               0xe0004410 = 0x00000000
 rx_qregs.time_stamp             0xe0004414 = 0x00000000
 rx_qregs.tcp_csum               0xe0004418 = 0x00000000
 rx_qregs.tcp_csum_start         0xe000441c = 0x00000000
 rx_qregs.desc_addr_lo           0xe0004420 = 0x016d4000
 rx_qregs.desc_addr_hi           0xe0004424 = 0x00000000
 rx_qregs.addr_cntr_lo           0xe0004428 = 0x016d4020
 rx_qregs.addr_cntr_hi           0xe000442c = 0x00000000
 rx_qregs.byte_cntr              0xe0004430 = 0x00000000
 rx_qregs.bmu_cs                 0xe0004434 = 0x002aaa80
 rx_qregs.flag                   0xe0004438 = 0x00000600
 rx_qregs.tst1                   0xe000443c = 0xd2020202
 rx_qregs.tst2                   0xe0004440 = 0x00000050
 rx_qregs.tst3                   0xe0004444 = 0x00000000

Bank 12: Synchronous transmit queue registers:
 stx_qregs.buf_ctrl              0xe0004600 = 0x00000000
 stx_qregs.next_desc_addr_lo     0xe0004604 = 0x00000000
 stx_qregs.buf_addr_lo           0xe0004608 = 0x00000000
 stx_qregs.buf_addr_hi           0xe000460c = 0x00000000
 stx_qregs.frame_sw              0xe0004610 = 0x00000000
 stx_qregs.time_stamp            0xe0004614 = 0x00000000
 stx_qregs.tcp_csum              0xe0004618 = 0x00000000
 stx_qregs.tcp_csum_start        0xe000461c = 0x00000000
 stx_qregs.desc_addr_lo          0xe0004620 = 0x00000000
 stx_qregs.desc_addr_hi          0xe0004624 = 0x00000000
 stx_qregs.addr_cntr_lo          0xe0004628 = 0x00000000
 stx_qregs.addr_cntr_hi          0xe000462c = 0x00000000
 stx_qregs.byte_cntr             0xe0004630 = 0x00000000
 stx_qregs.bmu_cs                0xe0004634 = 0x01155540
```

```
 stx_qregs.flag                0xe0004638 = 0x0a000600
 stx_qregs.tst1                0xe000463c = 0x02020202
 stx_qregs.tst2                0xe0004640 = 0x00000050
 stx_qregs.tst3                0xe0004644 = 0x00000000

Bank 13: Asynchronous transmit queue registers:
 atx_qregs.buf_ctrl            0xe0004680 = 0x00000000
 atx_qregs.next_desc_addr_lo   0xe0004684 = 0x00000000
 atx_qregs.buf_addr_lo         0xe0004688 = 0x00000000
 atx_qregs.buf_addr_hi         0xe000468c = 0x00000000
 atx_qregs.frame_sw            0xe0004690 = 0x00000000
 atx_qregs.time_stamp          0xe0004694 = 0x00000000
 atx_qregs.tcp_csum            0xe0004698 = 0x00000000
 atx_qregs.tcp_csum_start      0xe000469c = 0x00000000
 atx_qregs.desc_addr_lo        0xe00046a0 = 0x016d9000
 atx_qregs.desc_addr_hi        0xe00046a4 = 0x00000000
 atx_qregs.addr_cntr_lo        0xe00046a8 = 0x016d901c
 atx_qregs.addr_cntr_hi        0xe00046ac = 0x00000000
 atx_qregs.byte_cntr           0xe00046b0 = 0x00000000
 atx_qregs.bmu_cs              0xe00046b4 = 0x012aaa80
 atx_qregs.flag                0xe00046b8 = 0x0a000600
 atx_qregs.tst1                0xe00046bc = 0x02020202
 atx_qregs.tst2                0xe00046c0 = 0x00000050
 atx_qregs.tst3                0xe00046c4 = 0x00000000

Bank 16: Receive RAM buffer registers:
 rx_ram_buf_regs.start_addr    0xe0004800 = 0x00000000
 rx_ram_buf_regs.end_addr      0xe0004804 = 0x000017ff
 rx_ram_buf_regs.wr_ptr        0xe0004808 = 0x00000000
 rx_ram_buf_regs.rd_ptr        0xe000480c = 0x00000000
 rx_ram_buf_regs.up_thres_pp   0xe0004810 = 0x00001400
 rx_ram_buf_regs.lo_thres_pp   0xe0004814 = 0x00001000
 rx_ram_buf_regs.up_thres_hp   0xe0004818 = 0x00000000
 rx_ram_buf_regs.lo_thres_hp   0xe000481c = 0x00000000
 rx_ram_buf_regs.pak_cnt       0xe0004820 = 0x00000000
 rx_ram_buf_regs.level         0xe0004824 = 0x00000000
 rx_ram_buf_regs.ctrl          0xe0004828 = 0x0002222a

Bank 20: Synchronous transmit RAM buffer registers:
 stx_ram_buf_regs.start_addr   0xe0004a00 = 0x00000000
 stx_ram_buf_regs.end_addr     0xe0004a04 = 0x00000000
 stx_ram_buf_regs.wr_ptr       0xe0004a08 = 0x00000000
 stx_ram_buf_regs.rd_ptr       0xe0004a0c = 0x00000000
 stx_ram_buf_regs.pak_cnt      0xe0004a20 = 0x00000000
 stx_ram_buf_regs.level        0xe0004a24 = 0x00000000
 stx_ram_buf_regs.ctrl         0xe0004a28 = 0x00022215

Bank 21: Asynchronous transmit RAM buffer registers:
 atx_ram_buf_regs.start_addr   0xe0004a80 = 0x00001800
 atx_ram_buf_regs.end_addr     0xe0004a84 = 0x00002fff
 atx_ram_buf_regs.wr_ptr       0xe0004a88 = 0x00001800
 atx_ram_buf_regs.rd_ptr       0xe0004a8c = 0x00001800
 atx_ram_buf_regs.up_thres_pp  0xe0004a90 = 0x00000000
 atx_ram_buf_regs.lo_thres_pp  0xe0004a94 = 0x00000000
 atx_ram_buf_regs.up_thres_hp  0xe0004a98 = 0x00000000
 atx_ram_buf_regs.lo_thres_hp  0xe0004a9c = 0x00000000
 atx_ram_buf_regs.pak_cnt      0xe0004aa0 = 0x00000000
 atx_ram_buf_regs.level        0xe0004aa4 = 0x00000000
 atx_ram_buf_regs.ctrl         0xe0004aa8 = 0x0002222a

Bank 24: Receive GMAC FIFO registers:
 rx_gmfifo_regs.end_addr       0xe0004c40 = 0x0000007f
 rx_gmfifo_regs.thr            0xe0004c44 = 0x00000070
 rx_gmfifo_regs.ctrl           0xe0004c48 = 0x0000224a

Bank 26: Transmit GMAC FIFO registers:
 tx_gmfifo_regs.end_addr       0xe0004d40 = 0x0000007f
 tx_gmfifo_regs.thr            0xe0004d44 = 0x00000010
 tx_gmfifo_regs.ctrl           0xe0004d48 = 0x0002220a
```

```
    tx_gmfifo_regs.wr_ptr          0xe0004d60 = 0x00000000
    tx_gmfifo_regs.wr_shdw_ptr     0xe0004d64 = 0x00000000
    tx_gmfifo_regs.wr_level        0xe0004d68 = 0x00000000
    tx_gmfifo_regs.rd_ptr          0xe0004d70 = 0x00000000
    tx_gmfifo_regs.restart_ptr     0xe0004d74 = 0x00000000
    tx_gmfifo_regs.rd_level        0xe0004d78 = 0x00000000

  Descriptor poll timer registers:
    dpt_init_val                   0xe0004e00 = 0x00000000
    dpt_val                        0xe0004e04 = 0x00000000
    dpt_ctrl                       0xe0004e08 = 0x00020001

  Timestamp timer register:
    ts_timer_val                   0xe0004e14 = 0x00000000
    ts_timer_ctrl                  0xe0004e18 = 0x00000202

  GMAC and GPHY control registers:
    gmac_ctrl                      0xe0004f00 = 0x00000056
    gphy_ctrl                      0xe0004f04 = 0x0b7de002
    gmac_irq_src                   0xe0004f08 = 0x00000000
    gmac_irq_msk                   0xe0004f0c = 0x0000003a
    gmac_link_ctrl                 0xe0004f10 = 0x00000002

  Wake on LAN control registers:
    wol_ctrl                       0xe0004f20 = 0x00000555
    wol_mac_addr_lo                0xe0004f24 = 0x00000000
    wol_mac_addr_hi                0xe0004f28 = 0x00000000
    wol_patt_rd_ptr                0xe0004f2c = 0x00000000
    wol_patt_len_lo                0xe0004f30 = 0x3b3b3b3b
    wol_patt_len_hi                0xe0004f34 = 0x003b3b3b
    wol_patt_cnt_lo                0xe0004f38 = 0x00000000
    wol_patt_cnt_hi                0xe0004f3c = 0x00000000

  Bank 80 (0x50): GMAC registers:
    gmac_gpsr                      0xe0006800 = 0x0000f014
    gmac_gpcr                      0xe0006804 = 0x000038ff
    gmac_tx_ctrl                   0xe0006808 = 0x00001c00
    gmac_rx_ctrl                   0xe000680c = 0x0000a000
    gmac_tx_fctrl                  0xe0006810 = 0x0000ffff
    gmac_tx_parm                   0xe0006814 = 0x0000c000
    gmac_smod                      0xe0006818 = 0x00002306
    gmac_sa1_lo                    0xe000681c = 0x0000d000
    gmac_sa1_md                    0xe0006820 = 0x0000ff2b
    gmac_sa1_hi                    0xe0006824 = 0x00009f44
    gmac_sa2_lo                    0xe0006828 = 0x0000d000
    gmac_sa2_md                    0xe000682c = 0x0000ff2b
    gmac_sa2_hi                    0xe0006830 = 0x00009f44
    gmac_mcast_addr_hash1          0xe0006834 = 0x00000000
    gmac_mcast_addr_hash2          0xe0006838 = 0x00000000
    gmac_mcast_addr_hash3          0xe000683c = 0x00000000
    gmac_mcast_addr_hash4          0xe0006840 = 0x00000000
    gmac_tx_irq_src                0xe0006844 = 0x00000000
    gmac_rx_irq_src                0xe0006848 = 0x00000000
    gmac_tr_irq_src                0xe000684c = 0x00000000
    gmac_tx_irq_msk                0xe0006850 = 0x00000000
    gmac_rx_irq_msk                0xe0006854 = 0x00000000
    gmac_tr_irq_msk                0xe0006858 = 0x00000000

Internal-Data0/1:
  Marvell 88E6095 revision 2, switch port 8
    Port Registers:
        Status:        0x0e84  PCS Ctrl:      0xc13e
        Identifier:    0x0952  Port Ctrl:     0x0177
        Port Ctrl-1:   0x0000  Vlan Map:      0x06ff
        VID and PRI:   0x0001  Port Ctrl-2:   0x0cc8
        Rate Ctrl:     0x0000  Rate Ctrl-2:   0x3000
        Port Asc Vt:   0x0100
        In Discard Lo: 0x0000  In Discard Hi: 0x0000
        In Filtered:   0x0000  Out Filtered:  0x0000
```

関連コマンド

コマンド	説明
show interface	インターフェイスの統計を表示します。
show tech-support	Cisco TAC が問題を診断できるように情報を表示します。

show counters

プロトコル スタック カウンタを表示するには、特権 EXEC モードで **show counters** コマンドを使用します。

show counters [all | **context** *context-name* | **summary** | **top** *N*] [**detail**] [**protocol** *protocol_name* [**:***counter_name*]] [**threshold** *N*]

シンタックスの説明

all	フィルタの詳細を表示します。
context *context-name*	コンテキスト名を指定します。
:*counter_name*	カウンタを名前で指定します。
detail	詳細なカウンタ情報を表示します。
protocol *protocol_name*	指定したプロトコルのカウンタを表示します。
summary	カウンタの要約を表示します。
threshold *N*	指定したしきい値以上のカウンタのみ表示します。範囲は 1 ～ 4294967295 です。
top *N*	指定したしきい値以上のカウンタを表示します。範囲は 1 ～ 4294967295 です。

デフォルト

show counters summary detail threshold 1

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、すべてのカウンタを表示する方法を示しています。

```
hostname# show counters all
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   single_vf
IOS_IPC       OUT_PKTS              2   single_vf

hostname# show counters
Protocol      Counter           Value   Context
NPCP          IN_PKTS            7195   Summary
NPCP          OUT_PKTS           7603   Summary
IOS_IPC       IN_PKTS             869   Summary
IOS_IPC       OUT_PKTS            865   Summary
IP            IN_PKTS             380   Summary
IP            OUT_PKTS            411   Summary
IP            TO_ARP              105   Summary
IP            TO_UDP                9   Summary
UDP           IN_PKTS               9   Summary
UDP           DROP_NO_APP           9   Summary
FIXUP         IN_PKTS             202   Summary
```

次の例は、カウンタの要約を表示する方法を示しています。

```
hostname# show counters summary
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               2   Summary
IOS_IPC       OUT_PKTS              2   Summary
```

次の例は、コンテキストのカウンタを表示する方法を示しています。

```
hostname# show counters context single_vf
Protocol      Counter           Value   Context
IOS_IPC       IN_PKTS               4   single_vf
IOS_IPC       OUT_PKTS              4   single_vf
```

関連コマンド

コマンド	説明
clear counters	プロトコル スタック カウンタを消去します。

show cpu

CPU の使用状況に関する情報を表示するには、特権 EXEC モードで **show cpu usage** コマンドを使用します。

show cpu [**usage | profile**]

マルチ コンテキスト モードでは、システム コンフィギュレーションから次のように入力します。

show cpu [**usage**] [**context** {**all** | *context_name*}]

シンタックスの説明

all	すべてのコンテキストを表示の対象にすることを指定します。
context	1 つのコンテキストを表示の対象にすることを指定します。
context_name	表示の対象にするコンテキストの名前を指定します。
profile	CPU プロファイルの使用状況を表示します。表示された情報は、トラブルシューティングの目的で TAC が使用することがあります。
usage	（オプション）CPU 使用状況を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

CPU の使用状況は、負荷の近似値を使用して 5 秒ごとに算出されます。この近似値は、次回と次々回の移動平均に提供されます。

show cpu コマンドを使用すると、負荷に関係しているプロセス（つまり、シングルモードで実行した ***show process*** コマンドと、マルチ コンテキスト モードのシステム コンフィギュレーションから実行した ***show process*** コマンドの両方の出力に表示されている項目のためのアクティビティ）を発見できます。

さらに、マルチ コンテキスト モードでは、いずれかの設定済みコンテキストが CPU に負荷をかけている場合、その負荷に関係しているプロセスを中断するように要求できます。このためには、各コンテキストに移動して ***show cpu*** コマンドを入力するか、このコマンドの変化型である ***show cpu context*** を入力します。

プロセスに関係する負荷は、直近の整数に四捨五入されます。それに対して、コンテキストに関係する負荷には小数点第 1 位が含まれています。たとえば、***show cpu*** をシステム コンテキストから入力すると、***show cpu context system*** コマンドを入力したときとは別の数値が示されます。前者は ***show cpu context all*** のすべての要素の近似的な要約であり、後者はその要約の一部にすぎません。

show cpu profile コマンドを **cpu profile activate** コマンドと組み合せて使用すると、TAC が CPU 問題のトラブルシューティングを支援するために収集および使用できる情報が表示されます。**show cpu profile** コマンドによって表示される情報は 16 進形式です。

例

次の例は、CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu usage
CPU utilization for 5 seconds = 18%; 1 minute: 18%; 5 minutes: 18%
```

次の例は、マルチモードでシステム コンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu context system
CPU utilization for 5 seconds = 9.1%; 1 minute: 9.2%; 5 minutes: 9.1%
```

次の例は、すべてのコンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname# show cpu usage context all
5 sec  1 min  5 min  Context Name
9.1%   9.2%   9.1%  system
0.0%   0.0%   0.0%  admin
5.0%   5.0%   5.0%  one
4.2%   4.3%   4.2%  two
```

次の例は、one というコンテキストの CPU 使用状況を表示する方法を示しています。

```
hostname/one# show cpu usage
CPU utilization for 5 seconds = 5.0%; 1 minute: 5.0%; 5 minutes: 5.0%
```

次の例では、プロファイラを有効にし、5000 個のサンプルを格納するように指示します。

```
hostname# cpu profile activate 5000
Activated CPU profiling for 5000 samples.
```

show cpu profile コマンドを使用して、結果を確認します。

(注) **cpu profile activate** コマンドの実行中に **show cpu profile** コマンドを実行すると、進行状況が表示されます。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 CPU profiling currently in
progress, 1640 out of 5000 samples collected.
```

処理が完了すると、**show cpu profile** コマンド出力によって結果が表示されます。この情報をコピーし、TAC に提出します。TAC がこの情報をデコードします。

```
hostname# show cpu profile
CPU profiling started: 07:54:40.888 PDT Fri Sep 1 2006 Profiling finished, 5000
samples:
 00c483f5 00115283 002199d3 001151d1 002199e5 00116258 002199fc 00115230  0021984e
002198f6 00c48496 00219803 004a55b1 002198b1 00c484d9 00c48472
 00116258 00c48401 002199f3 00c48401 00c484b2 004a5580 0011520a 002198b4
 00116258 00219807 0011520a 00116258 002198a9 00116258 00219a2e 00112009  0021989c
00fff023 008be861 0011525e 002198be 0021984e 00115277 00219807  002199d0 00114a6d
002198af 0011520a 00115260 00115274 004a55a6 00c48472
 00c48472 00c48496 002199f9 002198ad 00c484c4 004a55a6 00115260 002198f4  0011528e
002198e0 00c484bb 00c48496 00c484a6 002199f3 00219810 001161d6 .
```

関連コマンド

コマンド	説明
show counters	プロトコル スタック カウンタを表示します。
cpu profile activate	CPU プロファイリングを有効にします。

show crashinfo

フラッシュ メモリに格納されているクラッシュ ファイルの内容を表示するには、特権 EXEC モードで ***show crashinfo*** コマンドを入力します。

show crashinfo [**save**]

シンタックスの説明

save	（オプション）クラッシュ情報をフラッシュ メモリに保存するようにセキュリティ アプライアンスが設定されているかどうかを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

クラッシュ ファイルがテスト クラッシュ（**crashinfo test** コマンドで生成）のものである場合、クラッシュ ファイルの最初の文字列は「**: Saved_Test_Crash**」であり、最後の文字列は「**: End_Test_Crash**」です。クラッシュ ファイルが実際のクラッシュのものである場合、クラッシュ ファイルの最初の文字列は「**: Saved_Crash**」であり、最後の文字列は「**: End_Crash**」です（**crashinfo force page-fault** コマンドまたは **crashinfo force watchdog** コマンドを使用して発生させたクラッシュを含む）。

クラッシュ データがフラッシュにまったく保存されていない場合や、**clear crashinfo** コマンドを入力してクラッシュ データを消去していた場合は、**show crashinfo** コマンドを実行するとエラー メッセージが表示されます。

例

次の例は、現在のクラッシュ情報コンフィギュレーションを表示する方法を示しています。

```
hostname# show crashinfo save
crashinfo save enable
```

次の例は、クラッシュ ファイル テストの出力を示しています（このテストによって、セキュリティ アプライアンスが実際にクラッシュすることはありません。このテストで生成されるのは、擬似的なサンプル ファイルです）。

```
hostname(config)# crashinfo test
hostname(config)# exit
hostname# show crashinfo
: Saved_Test_Crash

Thread Name: ci/console (Old pc 0x001a6ff5 ebp 0x00e88920)

Traceback:
0: 00323143
1: 0032321b
2: 0010885c
3: 0010763c
4: 001078db
5: 00103585
6: 00000000
    vector 0x000000ff (user defined)
       edi 0x004f20c4
       esi 0x00000000
       ebp 0x00e88c20
       esp 0x00e88bd8
       ebx 0x00000001
       edx 0x00000074
       ecx 0x00322f8b
       eax 0x00322f8b
error code n/a
       eip 0x0010318c
        cs 0x00000008
    eflags 0x00000000
       CR2 0x00000000
Stack dump: base:0x00e8511c size:16384, active:1476
0x00e89118: 0x004f1bb4
0x00e89114: 0x001078b4
0x00e89110-0x00e8910c: 0x00000000
0x00e89108-0x00e890ec: 0x12345678
0x00e890e8: 0x004f1bb4
0x00e890e4: 0x00103585
0x00e890e0: 0x00e8910c
0x00e890dc-0x00e890cc: 0x12345678
0x00e890c8: 0x00000000
0x00e890c4-0x00e890bc: 0x12345678
0x00e890b8: 0x004f1bb4
0x00e890b4: 0x001078db
0x00e890b0: 0x00e890e0
0x00e890ac-0x00e890a8: 0x12345678
0x00e890a4: 0x001179b3
0x00e890a0: 0x00e890b0
0x00e8909c-0x00e89064: 0x12345678
0x00e89060: 0x12345600
0x00e8905c: 0x20232970
0x00e89058: 0x616d2d65
0x00e89054: 0x74002023
0x00e89050: 0x29676966
0x00e8904c: 0x6e6f6328
0x00e89048: 0x31636573
0x00e89044: 0x7069636f
0x00e89040: 0x64786970
0x00e8903c-0x00e88e50: 0x00000000
0x00e88e4c: 0x000a7473
0x00e88e48: 0x6574206f
0x00e88e44: 0x666e6968
0x00e88e40: 0x73617263
0x00e88e3c-0x00e88e38: 0x00000000
0x00e88e34: 0x12345600
0x00e88e30-0x00e88dfc: 0x00000000
```

```
0x00e88df8: 0x00316761
0x00e88df4: 0x74706100
0x00e88df0: 0x12345600
0x00e88dec-0x00e88ddc: 0x00000000
0x00e88dd8: 0x00000070
0x00e88dd4: 0x616d2d65
0x00e88dd0: 0x74756f00
0x00e88dcc: 0x00000000
0x00e88dc8: 0x00e88e40
0x00e88dc4: 0x004f20c4
0x00e88dc0: 0x12345600
0x00e88dbc: 0x00000000
0x00e88db8: 0x00000035
0x00e88db4: 0x315f656c
0x00e88db0: 0x62616e65
0x00e88dac: 0x0030fcf0
0x00e88da8: 0x3011111f
0x00e88da4: 0x004df43c
0x00e88da0: 0x0053fef0
0x00e88d9c: 0x004f1bb4
0x00e88d98: 0x12345600
0x00e88d94: 0x00000000
0x00e88d90: 0x00000035
0x00e88d8c: 0x315f656c
0x00e88d88: 0x62616e65
0x00e88d84: 0x00000000
0x00e88d80: 0x004f20c4
0x00e88d7c: 0x00000001
0x00e88d78: 0x01345678
0x00e88d74: 0x00f53854
0x00e88d70: 0x00f7f754
0x00e88d6c: 0x00e88db0
0x00e88d68: 0x00e88d7b
0x00e88d64: 0x00f53874
0x00e88d60: 0x00e89040
0x00e88d5c-0x00e88d54: 0x12345678
0x00e88d50-0x00e88d4c: 0x00000000
0x00e88d48: 0x004f1bb4
0x00e88d44: 0x00e88d7c
0x00e88d40: 0x00e88e40
0x00e88d3c: 0x00f53874
0x00e88d38: 0x004f1bb4
0x00e88d34: 0x0010763c
0x00e88d30: 0x00e890b0
0x00e88d2c: 0x00e88db0
0x00e88d28: 0x00e88d88
0x00e88d24: 0x0010761a
0x00e88d20: 0x00e890b0
0x00e88d1c: 0x00e88e40
0x00e88d18: 0x00f53874
0x00e88d14: 0x0010166d
0x00e88d10: 0x0000000e
0x00e88d0c: 0x00f53874
0x00e88d08: 0x00f53854
0x00e88d04: 0x0048b301
0x00e88d00: 0x00e88d30
0x00e88cfc: 0x0000000e
0x00e88cf8: 0x00f53854
0x00e88cf4: 0x0048a401
0x00e88cf0: 0x00f53854
0x00e88cec: 0x00f53874
0x00e88ce8: 0x0000000e
0x00e88ce4: 0x0048a64b
0x00e88ce0: 0x0000000e
0x00e88cdc: 0x00f53874
0x00e88cd8: 0x00f7f96c
0x00e88cd4: 0x0048b4f8
0x00e88cd0: 0x00e88d00
0x00e88ccc: 0x0000000f
```

```
0x00e88cc8: 0x00f7f96c
0x00e88cc4-0x00e88cc0: 0x0000000e
0x00e88cbc: 0x00e89040
0x00e88cb8: 0x00000000
0x00e88cb4: 0x00f5387e
0x00e88cb0: 0x00f53874
0x00e88cac: 0x00000002
0x00e88ca8: 0x00000001
0x00e88ca4: 0x00000009
0x00e88ca0-0x00e88c9c: 0x00000001
0x00e88c98: 0x00e88cb0
0x00e88c94: 0x004f20c4
0x00e88c90: 0x0000003a
0x00e88c8c: 0x00000000
0x00e88c88: 0x0000000a
0x00e88c84: 0x00489f3a
0x00e88c80: 0x00e88d88
0x00e88c7c: 0x00e88e40
0x00e88c78: 0x00e88d7c
0x00e88c74: 0x001087ed
0x00e88c70: 0x00000001
0x00e88c6c: 0x00e88cb0
0x00e88c68: 0x00000002
0x00e88c64: 0x0010885c
0x00e88c60: 0x00e88d30
0x00e88c5c: 0x00727334
0x00e88c58: 0xa0ffffff
0x00e88c54: 0x00e88cb0
0x00e88c50: 0x00000001
0x00e88c4c: 0x00e88cb0
0x00e88c48: 0x00000002
0x00e88c44: 0x0032321b
0x00e88c40: 0x00e88c60
0x00e88c3c: 0x00e88c7f
0x00e88c38: 0x00e88c5c
0x00e88c34: 0x004b1ad5
0x00e88c30: 0x00e88c60
0x00e88c2c: 0x00e88e40
0x00e88c28: 0xa0ffffff
0x00e88c24: 0x00323143
0x00e88c20: 0x00e88c40
0x00e88c1c: 0x00000000
0x00e88c18: 0x00000008
0x00e88c14: 0x0010318c
0x00e88c10-0x00e88c0c: 0x00322f8b
0x00e88c08: 0x00000074
0x00e88c04: 0x00000001
0x00e88c00: 0x00e88bd8
0x00e88bfc: 0x00e88c20
0x00e88bf8: 0x00000000
0x00e88bf4: 0x004f20c4
0x00e88bf0: 0x000000ff
0x00e88bec: 0x00322f87
0x00e88be8: 0x00f5387e
0x00e88be4: 0x00323021
0x00e88be0: 0x00e88c10
0x00e88bdc: 0x004f20c4
0x00e88bd8: 0x00000000 *
0x00e88bd4: 0x004eabb0
0x00e88bd0: 0x00000001
0x00e88bcc: 0x00f5387e
0x00e88bc8-0x00e88bc4: 0x00000000
0x00e88bc0: 0x00000008
0x00e88bbc: 0x0010318c
0x00e88bb8-0x00e88bb4: 0x00322f8b
0x00e88bb0: 0x00000074
0x00e88bac: 0x00000001
0x00e88ba8: 0x00e88bd8
0x00e88ba4: 0x00e88c20
```

```
0x00e88ba0: 0x00000000
0x00e88b9c: 0x004f20c4
0x00e88b98: 0x000000ff
0x00e88b94: 0x001031f2
0x00e88b90: 0x00e88c20
0x00e88b8c: 0xffffffff
0x00e88b88: 0x00e88cb0
0x00e88b84: 0x00320032
0x00e88b80: 0x37303133
0x00e88b7c: 0x312f6574
0x00e88b78: 0x6972772f
0x00e88b74: 0x342f7665
0x00e88b70: 0x64736666
0x00e88b6c: 0x00020000
0x00e88b68: 0x00000010
0x00e88b64: 0x00000001
0x00e88b60: 0x123456cd
0x00e88b5c: 0x00000000
0x00e88b58: 0x00000008

Cisco XXX Firewall Version X.X
Cisco XXX Device Manager Version X.X

Compiled on Fri 15-Nov-04 14:35 by root

hostname up 10 days 0 hours

Hardware:   XXX-XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 13:49:42.148 UTC Wed Nov 20 2004

------------------ show clock ------------------

15:34:28.129 UTC Sun Nov 24 2004

------------------ show memory ------------------

Free memory:        50444824 bytes
Used memory:        16664040 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------
```

```
0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    927

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        6139 packets input, 830375 bytes, 0 no buffer
        Received 5990 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        90 packets output, 6160 bytes, 0 underruns
        0 output errors, 13 collisions, 0 interface resets
        0 babbles, 0 late collisions, 47 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (5/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show process ------------------


     PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3792/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mrd 002e3a17 00c8f8d4 0053e600          0 00c8d93c 7908/8192 tcp_intercept_times
```

```
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 PIX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6904/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 pix/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 pix/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 pix/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 pix/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 pix/intf2
H*  001a6ff5 0009ff2c 0053e5b0       4820 00e8511c 12860/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  508286220 00f310fc 3688/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48        120 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc         10 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3456/4096 tcp_thread/0
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 865565.090 secs):
                6139 packets    830375 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                90 packets      6160 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 865565.090 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------
```

```
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
: End_Test_Crash
```

関連コマンド

コマンド	説明
clear crashinfo	クラッシュ ファイルの内容を削除します。
crashinfo force	セキュリティ アプライアンスを強制的にクラッシュさせます。
crashinfo save disable	フラッシュ メモリへのクラッシュ情報の書き込みをディセーブルにします。
crashinfo test	フラッシュ メモリ内のファイルにクラッシュ情報を保存する、セキュリティ アプライアンスの機能をテストします。

show crashinfo console

フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行うには、**crashinfo console disable** コマンドを使用します。このコマンドは、クラッシュを強制的に発生させます。

show crashinfo console

シンタックスの説明

console	クラッシュ情報をコンソールに出力するかどうかを制御します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 140-2 に準拠すると、キーやパスワードなどのクリティカル セキュリティ パラメータを暗号境界（シャーシ）の外側に配布することができません。アサートまたはチェックヒープのエラーによってデバイスがクラッシュしたとき、コンソールにダンプされるスタック領域やメモリ領域は、機密データを含んでいることがあります。この出力は、FIPS モードでは表示されないようにする必要があります。

例

```
sw8-5520(config)# show crashinfo console
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールで FIPS に準拠するためのポリシーチェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

show crypto accelerator statistics

ハードウェア暗号アクセラレータ MIB 内のグローバルな統計情報またはアクセラレータ固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto accelerator statistics** コマンドを使用します。

show crypto accelerator statistics

シンタックスの説明

このコマンドには、キーワードも変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、グローバルな暗号アクセラレータ統計情報を表示しています。

```
hostname # show crypto accelerator statistics

Crypto Accelerator Status
-------------------------
[Capacity]
   Supports hardware crypto: True
   Supports modular hardware crypto: False
   Max accelerators: 1
   Max crypto throughput: 100 Mbps
   Max crypto connections: 750
[Global Statistics]
   Number of active accelerators: 1
   Number of non-operational accelerators: 0
   Input packets: 700
   Input bytes: 753488
   Output packets: 700
   Output error packets: 0
   Output bytes: 767496
[Accelerator 0]
   Status: Active
   Software crypto engine
   Slot: 0
   Active time: 167 seconds
   Total crypto transforms: 7
   Total dropped packets: 0
   [Input statistics]
      Input packets: 0
      Input bytes: 0
      Input hashed packets: 0
      Input hashed bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [Output statistics]
      Output packets: 0
      Output bad packets: 0
      Output bytes: 0
      Output hashed packets: 0
      Output hashed bytes: 0
      Encrypted packets: 0
      Encrypted bytes: 0
   [Diffie-Hellman statistics]
      Keys generated: 0
      Secret keys derived: 0
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 98
      Random number request failures: 0
[Accelerator 1]
   Status: Active
   Encryption hardware device : Cisco ASA-55x0 on-board accelerator
(revision 0x0)
```

```
                                Boot microcode   : CNlite-MC-Boot-Cisco-1.2
                                SSL/IKE microcode: CNlite-MC-IPSEC-Admin-3.03
                                IPSec microcode  : CNlite-MC-IPSECm-MAIN-2.03
   Slot: 1
   Active time: 170 seconds
   Total crypto transforms: 1534
   Total dropped packets: 0
   [Input statistics]
      Input packets: 700
      Input bytes: 753544
      Input hashed packets: 700
      Input hashed bytes: 736400
      Decrypted packets: 700
      Decrypted bytes: 719944
   [Output statistics]
      Output packets: 700
      Output bad packets: 0
      Output bytes: 767552
      Output hashed packets: 700
      Output hashed bytes: 744800
      Encrypted packets: 700
      Encrypted bytes: 728352
   [Diffie-Hellman statistics]
      Keys generated: 97
      Secret keys derived: 1
   [RSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
      Encrypted packets: 0
      Encrypted bytes: 0
      Decrypted packets: 0
      Decrypted bytes: 0
   [DSA statistics]
      Keys generated: 0
      Signatures: 0
      Verifications: 0
   [SSL statistics]
      Outbound records: 0
      Inbound records: 0
   [RNG statistics]
      Random number requests: 1
      Random number request failures: 0
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を消去します。
clear crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去します。
show crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示します。

show crypto ca certificates

特定のトラストポイントに関連付けられている証明書、またはシステムにインストールされているすべての証明書を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates [*trustpointname*]

シンタックスの説明

trustpointname	（オプション）トラストポイントの名前。名前を指定しない場合は、システムにインストールされているすべての証明書が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、tp1 というトラストポイントの CA 証明書を表示しています。

```
hostname(config)# show crypto ca certificates tp1
CA Certificate
    Status: Available
    Certificate Serial Number 2957A3FF296EF854FD0D6732FE25B45
    Certificate Usage: Signature
    Issuer:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST - massachusetts
        C = US
        EA = a@b.con
    Subject:
        CN = ms-root-sha-06-2004
        OU = rootou
        O = cisco
        L = franklin
        ST = massachusetts
        C = US
        EA = a@b.com
    CRL Distribution Point
        ldap://w2kadvancedsrv/CertEnroll/ms-root-sha-06-2004.crl
    Validity Date:
        start date: 14:11:40 UTC Jun 26 2004
        end date: 14:01:30 UTC Jun 4 2022
    Associated Trustpoints: tp2 tp1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定したトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca enroll	CA との登録プロセスを開始します。
crypto ca import	指定したトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント モードに入ります。

show crypto ca crls

キャッシュされているすべての CRL、または指定したトラストポイントでキャッシュされているすべての CRL を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ca crls** コマンドを使用します。

show crypto ca crls [*trustpointname*]

シンタックスの説明

trustpointname	（オプション）トラストポイントの名前。名前を指定しない場合は、システムにキャッシュされているすべての CRL が表示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、tp1 というトラストポイントの CRL を表示しています。

```
hostname(config)# show crypto ca crls tp1
CRL Issuer Name:
    cn=ms-sub1-ca-5-2004,ou=Franklin DevTest,o=Cisco
Systems,l=Franklin,st=MA,c=US,ea=user@cisco.com
    LastUpdate: 19:45:53 UTC Dec 24 2004
    NextUpdate: 08:05:53 UTC Jan 1 2005
    Retrieved from CRL Distribution Point:
      http://win2k-ad2.frk-ms-pki.cisco.com/CertEnroll/ms-sub1-ca-5-2004.crl
    Associated Trustpoints: tp1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca authenticate	指定したトラストポイントの CA 証明書を取得します。
crypto ca crl request	指定したトラストポイントのコンフィギュレーション パラメータに基づいて、CRL を要求します。
crypto ca enroll	CA との登録プロセスを開始します。
crypto ca import	指定したトラストポイントに証明書をインポートします。
crypto ca trustpoint	指定したトラストポイントのトラストポイント モードに入ります。

show crypto ipsec df-bit

指定したインターフェイスの IPSec パケットの IPSec DF ビット ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec df-bit** コマンドを使用します。

show crypto ipsec df-bit *interface*

シンタックスの説明

interface	インターフェイス名を指定します。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、inside というインターフェイスの IPSec DF ビット ポリシーを表示しています。

```
hostname(config)# show crypto ipsec df-bit inside
df-bit inside copy
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPSec パケットの IPSec DF ビット ポリシーを設定します。
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを表示します。

show crypto ipsec fragmentation

IPSec パケットのフラグメンテーション ポリシーを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec fragmentation** コマンドを使用します。

show crypto ipsec fragmentation *interface*

シンタックスの説明

interface	インターフェイス名を指定します。
token	ユーザ認証にトークン ベースのサーバを使用することを指定します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、inside というインターフェイスの IPSec フラグメンテーション ポリシーを表示しています。

```
hostname(config)# show crypto ipsec fragmentation inside
fragmentation inside before-encryption
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPSec パケットのフラグメンテーション ポリシーを設定します。
crypto ipsec df-bit	IPSec パケットの DF ビット ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

show crypto ipsec sa

IPSec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec sa** コマンドを使用します。このコマンドの別の形式である、**show ipsec sa** を使用することもできます。

show crypto ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

シンタックスの説明

detail	（オプション）表示対象に関する詳細なエラー情報を表示します。
entry	（オプション）IPSec SA をピア アドレスでソートして表示します。
identity	（オプション）IPSec SA を ID でソートして、ESP を除いて表示します。これは圧縮された形式です。
***map** map-name*	（オプション）指定した暗号マップの IPSec SA を表示します。
***peer**peer-addr*	（オプション）指定したピア IP アドレスの IPSec SA を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

（注） 断片化の統計は、IPSec 処理前に断片化が発生することを IPSec SA ポリシーが記述している場合は、断片化前の統計になります。断片化後の統計は、IPSec 処理後に断片化が発生することを SA ポリシーが記述している場合に表示されます。

グローバル コンフィギュレーション モードで入力した次の例では、def という暗号マップの IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
```

```
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード ***entry*** を指定して IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

```
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード ***entry detail*** を指定して IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
```

```
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

次の例では、キーワード ***identity*** を指定して IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次の例では、キーワード ***identity*** と ***detail*** を指定して IPSec SA を表示しています。

```
hostname(config)# show crypto ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto ipsec stats

一連の IPSec 統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto ipsec stats** コマンドを使用します。

show crypto ipsec stats

シンタックスの説明

このコマンドには、キーワードも変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec 統計情報を表示しています。

```
hostname(config)# show crypto ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPSec SA またはカウンタを、指定したパラメータに基づいて消去します。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定したパラメータに基づいて IPSec SA を表示します。
show ipsec sa summary	IPSec SA の要約を表示します。

show crypto isakmp stats

実行時の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが導入されました。
7.2(1)	**show isakmp stats** コマンドが廃止されました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects

- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP 統計情報を表示しています。

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp sa** コマンドを使用します。

show crypto isakmp sa [**detail**]

シンタックスの説明

detail	SA データベースに関する詳細な出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp sa** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合：

表 25-11

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合：

表 25-12

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

グローバル コンフィギュレーション モードで入力した次の例では、SA データベースに関する詳細な情報を表示しています。

```
hostname(config)# show crypto isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto isakmp stats

実行時の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto isakmp stats** コマンドを使用します。

show crypto isakmp stats

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが導入されました。
7.2(1)	**show isakmp stats** コマンドが廃止されました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects

- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP 統計情報を表示しています。

```
hostname(config)# show crypto isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show crypto protocol statistics

暗号アクセラレータ MIB 内のプロトコル固有の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show crypto protocol statistics** コマンドを使用します。

show crypto protocol statistics *protocol*

シンタックスの説明

protocol	統計情報を表示するプロトコルの名前を指定します。指定できるプロトコルは、次のとおりです。 ***ikev1***：Internet Key Exchange バージョン 1 ***ipsec***：IP セキュリティ フェーズ 2 プロトコル ***ssl***：Secure Socket Layer ***other***：新しいプロトコルのために予約済み ***all***：現在サポートされているすべてのプロトコル

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、指定したプロトコルに関する暗号アクセラレータ統計情報を表示しています。

```
hostname # show crypto protocol statistics ikev1
[IKEv1 statistics]
   Encrypt packet requests: 39
   Encapsulate packet requests: 39
   Decrypt packet requests: 35
   Decapsulate packet requests: 35
   HMAC calculation requests: 84
   SA creation requests: 1
   SA rekey requests: 3
    SA deletion requests: 2
   Next phase key allocation requests: 2
   Random number generation requests: 0
    Failed requests: 0

hostname # show crypto protocol statistics ipsec
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
   Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics ssl
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0

hostname # show crypto protocol statistics other
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0

hostname # show crypto protocol statistics all
[IKEv1 statistics]
   Encrypt packet requests: 46
   Encapsulate packet requests: 46
   Decrypt packet requests: 40
   Decapsulate packet requests: 40
   HMAC calculation requests: 91
    SA creation requests: 1
   SA rekey requests: 3
```

```
   SA deletion requests: 3
   Next phase key allocation requests: 2
   Random number generation requests: 0
   Failed requests: 0
[IKEv2 statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
    Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[IPsec statistics]
   Encrypt packet requests: 700
   Encapsulate packet requests: 700
    Decrypt packet requests: 700
   Decapsulate packet requests: 700
   HMAC calculation requests: 1400
   SA creation requests: 2
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSL statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
   HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 0
   Failed requests: 0
[SSH statistics are not supported]
[SRTP statistics are not supported]
[Other statistics]
   Encrypt packet requests: 0
   Encapsulate packet requests: 0
   Decrypt packet requests: 0
   Decapsulate packet requests: 0
    HMAC calculation requests: 0
   SA creation requests: 0
   SA rekey requests: 0
   SA deletion requests: 0
   Next phase key allocation requests: 0
   Random number generation requests: 99
   Failed requests: 0
hostname #
```

関連コマンド

コマンド	説明
clear crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を消去します。
clear crypto protocol statistics	暗号アクセラレータ MIB 内のプロトコル固有の統計情報を消去します。
show crypto accelerator statistics	暗号アクセラレータ MIB 内のグローバルな統計情報およびアクセラレータ固有の統計情報を表示します。

show csc node-count

ノードとは、固有のソース IP アドレス、またはセキュリティ アプライアンスにより保護されているネットワーク上のデバイスのアドレスです。セキュリティ アプライアンスは、毎日のノード カウントをトラッキングし、ユーザ ライセンス管理を目的に CSC SSM に伝えます。CSC SSM がスキャンしたトラフィックのノード数を表示するには、特権 EXEC モードで **show csc node-count** コマンドを使用します。

show csc node-count [**yesterday**]

シンタックスの説明

yesterday	（オプション）CSC SSM が前日の 24 時間（午前零時から翌日の午前零時まで）スキャンしたトラフィックのノード数を表示します。

デフォルト

デフォルトで表示されるノード カウントは、午前零時からスキャンされたノード数です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

この例では、**show csc node-count** コマンドを使用して、CSC SSM が午前零時からスキャンしたトラフィックのノード数を表示する方法を示します。

```
hostname# show csc node-count
```

この例では、**show csc node-count** コマンドを使用して、CSC SSM が前日の 24 時間（午前零時から翌日の午前零時まで）スキャンしたトラフィックのノード数を表示する方法を示します。

```
hostname(config)# show csc node-count yesterday
```

関連コマンド

csc	ネットワーク トラフィックを CSC SSM に送信して、CSC SSM で設定されているとおりに FTP、HTTP、POP3、および SMTP をスキャンします。
show running-config class-map	現在のクラス マップ コンフィギュレーションを表示します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションを表示します。
show running-config service-policy	現在のサービス マップ コンフィギュレーションを表示します。

show ctiqbe

セキュリティ アプライアンスを越えて確立されている CTIQBE セッションの情報を表示するには、特権 EXEC モードで **show ctiqbe** コマンドを使用します。

show ctiqbe

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show ctiqbe コマンドは、セキュリティ アプライアンスを越えて確立されている CTIQBE セッションの情報を表示します。**debug ctiqbe** や **show local-host** と共に、このコマンドは、CTIQBE 検査エンジンの問題のトラブルシューティングに使用されます。

（注） **show ctiqbe** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの CTIQBE セッションが存在し、**pager** コマンドが設定されていない場合、**show ctiqbe** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例

次の条件における **show ctiqbe** コマンドの出力例を示します。セキュリティ アプライアンスを越えてセットアップされているアクティブ CTIQBE セッションは 1 つだけです。そのセッションは、ローカル アドレス 10.0.0.99 の内部 CTI デバイス（たとえば、Cisco IP SoftPhone）と 172.29.1.77 の外部 Cisco CallManager の間で確立されています。ここで、TCP ポート 2748 は、Cisco CallManager です。このセッションのハートビート間隔は 120 秒です。

```
hostname# show ctiqbe

Total: 1
  | LOCAL | FOREIGN | STATE | HEARTBEAT
------------------------------------------------------------
1 | 10.0.0.99/1117  172.29.1.77/2748 | 1 | 120
  | RTP/RTCP: PAT xlates: mapped to 172.29.1.99(1028 | 1029)
  | MEDIA: Device ID 27 | Call ID 0
  | Foreign 172.29.1.99 | (1028 | 1029)
  | Local | 172.29.1.88 | (26822 | 26823)
  | ------------------------------------------
```

CTI デバイスは、すでに CallManager に登録されています。デバイスの内部アドレスと RTP リスニング ポートは、172.29.1.99 UDP ポート 1028 に PAT 変換されています。その RTCP リスニング ポートは、UDP 1029 に PAT 変換されています。

`RTP/RTCP: PAT xlates:` で始まる行は、内部 CTI デバイスが外部 CallManager に登録され、CTI デバイスのアドレスとポートは、その外部インターフェイスに PAT 変換されている場合に限り表示されます。この行は、CallManager が内部インターフェイス上に位置する場合、または内部 CTI デバイスのアドレスとポートが、CallManager が使用しているのと同じ外部インターフェイスに NAT 変換されている場合は、表示されません。

この出力は、コールがこの CTI デバイスと 172.29.1.88 にある別の電話機の間に確立されていることを示します。他の電話機の RTP および RTCP リスニング ポートは、UDP 26822 および 26823 です。セキュリティ アプライアンスは 2 番目の電話機と CallManager に関連する CTIQBE セッション レコードを維持できないので、他の電話機は、CallManager と同じインターフェイス上にあります。CTI デバイス側のアクティブ コール レグは、Device ID 27 および Call ID 0 で確認できます。

次に、これらの CTIBQE 接続に対する xlate 情報を示します。

```
hostname# show xlate debug
3 in use, 3 most used
Flags: D | DNS, d | dump, I | identity, i | inside, n | no random,
 | o | outside, r | portmap, s | static
TCP PAT from inside:10.0.0.99/1117 to outside:172.29.1.99/1025 flags ri idle 0:00:22
timeout 0:00:30
UDP PAT from inside:10.0.0.99/16908 to outside:172.29.1.99/1028 flags ri idle 0:00:00
timeout 0:04:10
UDP PAT from inside:10.0.0.99/16909 to outside:172.29.1.99/1029 flags ri idle 0:00:23
timeout 0:04:10
hostname#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
inspect ctiqbe	CTIQBE アプリケーション検査をイネーブルにします。
service-policy	1 つまたは複数のインターフェイスにポリシー マップを適用します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show curpriv

現在のユーザ特権を表示するには、**show curpriv** コマンドを使用します。

show curpriv

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•
特権 EXEC	•	•	—	—	•
ユーザ	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに準拠するように修正されました。

使用上のガイドライン

show curpriv コマンドは、現在の特権レベルを表示します。特権レベルの数値が小さいほど、特権レベルが低いことを示しています。

例

次の例は、enable_15 という名前のユーザが異なる特権レベルにある場合の **show curpriv** コマンドの出力を示しています。ユーザ名はログイン時にユーザが入力した名前を示し、P_PRIV はユーザが **enable** コマンドを入力したことを示し、P_CONF は **config terminal** コマンドを入力したことを示します。

```
hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV P_CONF
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_15
Current privilege level : 15
Current Mode/s : P_PRIV
hostname(config)# exit

hostname(config)# show curpriv
Username : enable_1
Current privilege level : 1
Current Mode/s : P_UNPR
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド文を削除します。
show running-config privilege	コマンドの特権レベルを表示します。

CHAPTER 26

show ddns update interface コマンド ～ show ipv6 traffic コマンド

show ddns update interface

セキュリティ アプライアンス インターフェイスに指定された DDNS 方式を表示するには、特権 EXEC モードで **show ddns update interface** コマンドを表示します。

show ddns update interface [*interface-name*]

シンタックスの説明

interface-name	（オプション）ネットワーク インターフェイスの名前。

デフォルト

interface-name 文字列を省略すると、各インターフェイスに指定された DDNS 方式が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、内部インターフェイスに指定された DDNS 方式を表示します。

```
hostname# show ddns update interface inside
Dynamic DNS Update on inside:
  Update Method Name            Update Destination
  ddns-2                        not available
hostname#
```

関連コマンド

コマンド	説明
ddns（DDNS アップデート方式モード）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	セキュリティ アプライアンス インターフェイスを、DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
show ddns update method	設定済みの各 DDNS 方式について、タイプおよび間隔を表示します。DDNS アップデートを実行する DHCP サーバ。
show running-config ddns	実行コンフィギュレーションに含まれている、設定済みのすべての DDNS 方式について、タイプおよび間隔を表示します。

show ddns update method

実行コンフィギュレーションに含まれている DDNS アップデート方式を表示するには、特権 EXEC モードで **show ddns update method** コマンドを使用します。

show ddns update method [*method-name***]**

シンタックスの説明

method-name	（オプション）設定されている DDNS アップデート方式の名前です。

デフォルト

method-name 文字列を省略すると、設定されたすべての DDNS アップデート方式が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ddns-2 という名前の DDNS 方式を表示します。

```
hostname(config)# show ddns update method ddns-2

Dynamic DNS Update Method: ddns-2
  IETF standardized Dynamic DNS 'A' and 'PTR' records update
  Maximum update interval: 0 days 0 hours 10 minutes 0 seconds
hostname(config)#
```

関連コマンド

コマンド	説明
ddns（**DDNS アップデート方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	セキュリティ アプライアンス インターフェイスを、ダイナミック DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
show ddns update interface	設定済みの各 DDNS 方式に関連付けられているインターフェイスを表示します。
show running-config ddns	実行コンフィギュレーションに含まれている、設定済みのすべての DDNS 方式について、タイプおよび間隔を表示します。

show debug

現在のデバッグ コンフィギュレーションを表示するには、**show debug** コマンドを使用します。

show debug [*command* [*keywords*]]

シンタックスの説明

command	（オプション）現在のコンフィギュレーションを表示するデバッグ コマンドを指定します。*command* 以降のシンタックスは、各 *command* の関連 **debug** コマンドでサポートされているシンタックスと同じです。たとえば、**show debug aaa** 以降で有効となる *keywords* は、**debug aaa** コマンドで有効となるキーワードと同じです。つまり、**show debug *aaa*** の場合は ***accounting*** キーワードをサポートしています。このキーワードを使用すると、AAA デバッグの当該部分のデバッグ コンフィギュレーションを表示することを指定できます。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

有効となる *command* 値は、次のとおりです。*command* 以降で有効となるシンタックスについては、該当する **debug** *command* のエントリを参照してください。

（注） それぞれの *command* 値を入力できるかどうかは、該当する **debug** コマンドをサポートしているコマンド モードによって異なります。

- **aaa**
- **appfw**
- **arp**
- **asdm**
- **context**
- **crypto**
- **ctiqbe**
- **ctm**
- **dhcpc**
- **dhcpd**

- **dhcprelay**
- **disk**
- **dns**
- **email**
- **entity**
- **fixup**
- **fover**
- **fsm**
- **ftp**
- **generic**
- **gtp**
- **h323**
- **http**
- **http-map**
- **icmp**
- **igmp**
- **ils**
- **imagemgr**
- **ipsec-over-tcp**
- **ipv6**
- **iua-proxy**
- **kerberos**
- **ldap**
- **mfib**
- **mgcp**
- **mrib**
- **ntdomain**
- **ntp**
- **ospf**
- **parser**
- **pim**
- **pix**
- **pptp**
- **radius**
- **rip**
- **rtsp**
- **sdi**
- **sequence**
- **sip**
- **skinny**
- **smtp**
- **sqlnet**
- **ssh**

- **ssl**
- **sunrpc**
- **tacacs**
- **timestamps**
- **vpn-sessiondb**
- **webvpn**
- **xdmcp**

例

次のコマンドでは、認証、アカウンティング、およびフラッシュ メモリについてデバッグをイネーブルにしています。**show debug** コマンドを 3 つの方法で使用して、すべてのデバッグ コンフィギュレーション、特定の機能のデバッグ コンフィギュレーション、および機能のサブセットのデバッグ コンフィギュレーションを表示する方法を示しています。

```
hostname# debug aaa authentication
debug aaa authentication enabled at level 1
hostname# debug aaa accounting
debug aaa accounting enabled at level 1
hostname# debug disk filesystem
debug disk filesystem enabled at level 1
hostname# show debug
debug aaa authentication enabled at level 1
debug aaa accounting enabled at level 1
debug disk filesystem enabled at level 1
hostname# show debug aaa
debug aaa authentication enabled at level 1
debug aaa authorization is disabled.
debug aaa accounting enabled at level 1
debug aaa internal is disabled.
debug aaa vpn is disabled.
hostname# show debug aaa accounting
debug aaa accounting enabled at level 1
hostname#
```

関連コマンド

コマンド	説明
debug	すべての **debug** コマンドを参照してください。

show dhcpd

DHCP のバインディング、状態、および統計情報を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcpd** コマンドを使用します。

show dhcpd {***binding*** [*IP_address*] | ***state*** | ***statistics***}

シンタックスの説明

binding	与えられたサーバの IP アドレスとそれに関連付けられているクライアント ハードウェア アドレスとリース期間に対するバインディング情報を表示します。
IP_address	指定した IP アドレスのバインディング情報を表示します。
state	DHCP サーバの状態を表示します。たとえば、現在のコンテキストでイネーブルになっているかどうか、各インターフェイスでイネーブルになっているかどうかなどです。
statistics	アドレス プール、バインディング、有効期限切れのバインディング、形式が誤っているメッセージ、送信済みメッセージ、および受信済みメッセージの数などの統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show dhcpd binding コマンドにオプションの IP アドレスを含めると、その IP アドレスのバインディングのみが表示されます。

show dhcpd binding | state | statistics コマンドは、グローバル コンフィギュレーション モードでも使用できます。

例

次に、**show dhcpd binding** コマンドの出力例を示します。

```
hostname# show dhcpd binding
IP Address Hardware Address Lease Expiration Type
10.0.1.100 0100.a0c9.868e.43 84985 seconds automatic
```

次に、**show dhcpd state** コマンドの出力例を示します。

```
hostname# show dhcpd state
Context Not Configured for DHCP
Interface outside, Not Configured for DHCP
Interface inside, Not Configured for DHCP
```

次に、**show dhcpd statistics** コマンドの出力例を示します。

```
hostname# show dhcpd statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Address pools        1
Automatic bindings   1
Expired bindings     1
Malformed messages   0

Message              Received
BOOTREQUEST          0
DHCPDISCOVER         1
DHCPREQUEST          2
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

Message              Sent
BOOTREPLY            0
DHCPOFFER            1
DHCPACK              1
DHCPNAK              1
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
clear dhcpd	DHCP サーバのバインディングおよび統計情報カウンタを消去します。
dhcpd lease	クライアントに与える DHCP 情報のリース期間を定義します。
show running-config dhcpd	現在の DHCP サーバ コンフィギュレーションを表示します。

show dhcprelay state

DHCP リレー エージェントの状態を表示するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **show dhcprelay state** コマンドを使用します。

show dhcprelay state

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、現在のコンテキストおよび各インターフェイスの DHCP リレー エージェントの状態情報を表示します。

例

次に、**show dhcprelay state** コマンドの出力例を示します。

```
hostname# show dhcprelay state

Context  Configured as DHCP Relay
Interface outside, Not Configured for DHCP
Interface infrastructure, Configured for DHCP RELAY SERVER
Interface inside, Configured for DHCP RELAY
```

関連コマンド

コマンド	説明
show dhcpd	DHCP サーバの統計情報と状態情報を表示します。
show dhcprelay statistics	DHCP リレーの統計情報を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

show dhcprelay statistics

DHCP リレーの統計情報を表示するには、特権 EXEC モードで **show dhcprelay statistics** コマンドを使用します。

show dhcprelay ***statistics***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show dhcprelay statistics コマンドの出力は、**clear dhcprelay satistics** コマンドを入力するまでは増分します。

例

次に、**show dhcprelay statistics** コマンドの出力例を示します。

```
hostname# show dhcprelay statistics

DHCP UDP Unreachable Errors: 0
DHCP Other UDP Errors: 0

Packets Relayed
BOOTREQUEST          0
DHCPDISCOVER         7
DHCPREQUEST          3
DHCPDECLINE          0
DHCPRELEASE          0
DHCPINFORM           0

BOOTREPLY            0
DHCPOFFER            7
DHCPACK              3
DHCPNAK              0
FeralPix(config)#
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェント統計情報カウンタを消去します。
debug dhcprelay	DHCP リレー エージェントに関するデバッグ情報を表示します。
show dhcprelay state	DHCP リレー エージェントの状態を表示します。
show running-config dhcprelay	現在の DHCP リレー エージェント コンフィギュレーションを表示します。

show disk

フラッシュ メモリの内容を表示するには、特権 EXEC モードで **show disk** コマンドを使用します。PIX セキュリティ アプライアンスのフラッシュ メモリを表示するには、**show flash** コマンドを参照してください。

show disk[**0** | **1**] [**filesys** | **all**]

シンタックスの説明

0	**1**	内蔵フラッシュ メモリ（0。デフォルト）または外部フラッシュメモリ（1）を指定します。
filesys	コンパクト フラッシュ カードに関する情報を表示します。
all	フラッシュ メモリの内容に加えてファイル システム情報を表示します。

デフォルト

デフォルトでは、内蔵フラッシュ メモリが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、**show disk** コマンドの出力例を示します。

```
hostname# show disk
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 test1.cfg
 13 2551       Jan 06 2005 10:07:36 test2.cfg
 14 609223     Jan 21 2005 07:14:18 test3.cfg
 15 1619       Jul 16 2004 16:06:48 test4.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 test5.cfg
 20 1792       Jan 21 2005 07:29:24 test6.cfg
 21 7765184    Mar 07 2005 19:38:30 test7.cfg
 22 1674       Nov 11 2004 02:47:52 test8.cfg
 23 1863       Jan 21 2005 07:29:18 test9.cfg
 24 1197       Jan 19 2005 08:17:48 test10.cfg
 25 608554     Jan 13 2005 06:20:54 backupconfig.cfg
 26 5124096    Feb 20 2005 08:49:28 cdisk1
 27 5124096    Mar 01 2005 17:59:56 cdisk2
 28 2074       Jan 13 2005 08:13:26 test11.cfg
 29 5124096    Mar 07 2005 19:56:58 cdisk3
 30 1276       Jan 28 2005 08:31:58 lead
 31 7756788    Feb 24 2005 12:59:46 asdmfile.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile1.dbg
 33 7764344    Mar 04 2005 12:17:46 asdmfile2.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk4
 35 15322      Mar 04 2005 12:30:24 hs_err.log

10170368 bytes available (52711424 bytes used)
```

次に、**show disk filesys** コマンドの出力例を示します。

```
hostname# show disk filesys
******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
show flash	内蔵フラッシュ メモリの内容を表示します。

show dns-hosts

DNS キャッシュを表示するには、特権 EXEC モードで **show dns-hosts** コマンドを使用します。DNS キャッシュには、DNS サーバから動的にラーニングしたエントリと共に、**name** コマンドを使用して手作業で入力した名前および IP アドレスが保持されています。

show dns-hosts

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

次に、**show dns-hosts** コマンドの出力例を示します。

```
hostname# show dns-hosts
Host                        Flags      Age Type   Address(es)
ns2.example.com             (temp, OK) 0    IP    10.102.255.44
ns1.example.com             (temp, OK) 0    IP    192.168.241.185
snowmass.example.com        (temp, OK) 0    IP    10.94.146.101
server.example.com          (temp, OK) 0    IP    10.94.146.80
```

表 26-1 に、各フィールドの説明を示します。

表 26-1　show dns-hosts のフィールド

フィールド	説明
Host	ホスト名を表示します。
Flags	次のフラグを組み合せて、エントリのステータスを表示します。 • temp：このエントリは、DNS サーバから取得した一時的なものです。セキュリティ アプライアンスは、非アクティブ状態が 72 時間を過ぎるとこのエントリを削除します。 • perm：このエントリは、**name** コマンドで追加された永続的なものです。 • OK：このエントリは有効です。 • ??：このエントリは問題のある可能性があり、再確認が必要です。 • EX：このエントリは、有効期限が切れています。
Age	このエントリが最後に参照された時点からの経過時間を表示します。
Type	DNS レコードのタイプを表示します。この値は、常に IP です。
Address(es)	IP アドレス。

関連コマンド

コマンド	説明
clear dns-hosts	DNS キャッシュを消去します。
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。

show failover

装置のフェールオーバー ステータスに関する情報を表示するには、特権 EXEC モードで **show failover** コマンドを使用します。

show failover [***group*** *num* | ***history*** | ***interface*** | ***state*** | ***statistics***]

シンタックスの説明

group	指定したフェールオーバー グループの動作状態を表示します。
history	フェールオーバーの履歴を表示します。フェールオーバーの履歴には、過去のフェールオーバーの状態変化、および状態変化の理由が表示されます。デバイスがリブートされると、履歴情報は消去されます。
interface	フェールオーバー コマンドとステートフル リンクの情報を表示します。
num	フェールオーバー グループの番号。
state	両方のフェールオーバー装置のフェールオーバー状態を表示します。表示される情報には、装置のプライマリ状態またはセカンダリ状態、装置の Active/Standby ステータス、および最後に報告されたフェールオーバーの理由が含まれます。障害の原因が解決した場合でも、出力には障害理由が保持されます。
statistics	フェールオーバー コマンド インターフェイスの送信パケットと受信パケットの数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。出力に含まれる情報を追加しています。

使用上のガイドライン

show failover コマンドは、ダイナミック フェールオーバーの情報、インターフェイスのステータス、およびステートフル フェールオーバーの統計情報を表示します。Stateful Failover Logical Update Statistics の出力は、ステートフル フェールオーバーがイネーブルになっている場合のみ表示されます。「xerr」値と「rerr」値は、フェールオーバーのエラーではなく、パケットの送信エラーまたは受信エラーの数を示します。

（注） ステートフル フェールオーバー（ステートフル フェールオーバー統計出力）は、ASA 5505 シリーズ適応型セキュリティ アプライアンスでは使用できません。

show failover コマンドの出力で、Stateful Failover フィールドに表示される値は次のとおりです。

- Stateful Obj には、次の値が表示されます。
  - xmit：送信したパケット数を示します。
  - xerr：送信エラーの数を示します。
  - rcv：受信したパケット数を示します。
  - rerr：受信エラーの数を示します。
- 各行は、次に示す特定オブジェクトのスタティック カウント用です。
  - General：ステートフル オブジェクト全部の合計を示します。
  - sys cmd：論理アップデート システム コマンド、たとえば、**login** または **stay alive** を参照します。
  - up time：アクティブ セキュリティ アプライアンスがスタンバイ セキュリティ アプライアンスに渡すセキュリティ アプライアンス アップタイムの値を示します。
  - RPC services：リモート プロシージャ コール接続の情報。
  - TCP conn：ダイナミック TCP 接続の情報。
  - UDP conn：ダイナミック UDP 接続の情報。
  - ARP tbl：ダイナミック ARP テーブルの情報。
  - Xlate_Timeout：接続変換タイムアウトの情報を示します。
  - VPN IKE upd：IKE 接続の情報。
  - VPN IPSEC upd：IPSec 接続の情報。
  - VPN CTCP upd：cTCP トンネル接続の情報。
  - VPN SDI upd：SDI AAA 接続の情報。
  - VPN DHCP upd：トンネリングされた DHCP 接続の情報。

フェールオーバー IP アドレスを入力していなければ、**show failover** コマンドは IP アドレスに対して 0.0.0.0 を表示し、インターフェイスのモニタリングは、「waiting」状態のままになります。フェールオーバーが動作するためには、フェールオーバー IP アドレスを設定する必要があります。

マルチ コンフィギュレーション モードでは、セキュリティ コンテキストで使用できるのは **show failover** コマンドのみです。オプションのキーワードは入力できません。

例

次に、Active/Standby フェールオーバーでの **show failover** コマンドの出力例を示します。セキュリティ アプライアンスは ASA 5500 シリーズ適応型セキュリティ アプライアンスです。詳細に示されているように、各セキュリティ アプライアンスのスロット 1 にはそれぞれ CSC SSM が搭載されています。

```
hostname# show failover

Failover On
Cable status: N/A - LAN-based failover enabled
Failover unit Primary
Failover LAN Interface: fover Ethernet2 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
failover replication http
Last Failover at: 22:44:03 UTC Dec 8 2004
        This host: Primary - Active
                Active time: 13434 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.3): Normal
                  Interface outside (10.132.9.3): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status
(Up/Up)
                  Logging port IP: 10.0.0.3/24
                  CSC-SSM, 5.0 (Build#1176)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/7.1(0)10) status (Up Sys)
                  Interface inside (10.130.9.4): Normal
                  Interface outside (10.132.9.4): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/CSC-SSM 5.0 (Build#1176)) status
(Up/Up)
                  Logging port IP: 10.0.0.4/24
                  CSC-SSM, 5.0 (Build#1176)

Stateful Failover Logical Update Statistics
        Link : fover Ethernet2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         1733       0          1733       0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        6          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         106        0          0          0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       2       1733
        Xmit Q:         0       2       15225
```

次に、Active/Active フェールオーバーでの **show failover** コマンドの出力例を示します。

```
hostname# show failover

Failover On
Failover unit Primary
Failover LAN Interface: third GigabitEthernet0/2 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 4 seconds
Interface Policy 1
Monitored Interfaces 8 of 250 maximum
failover replication http
Group 1 last failover at: 13:40:18 UTC Dec 9 2004
Group 2 last failover at: 13:40:06 UTC Dec 9 2004

  This host:    Primary
  Group 1       State:          Active
                Active time:    2896 (sec)
  Group 2       State:          Standby Ready
                Active time:    0 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.11)S91(0.11)) status (Up)
                admin Interface outside (10.132.8.5): Normal
                admin Interface third (10.132.9.5): Normal
                admin Interface inside (10.130.8.5): Normal
                admin Interface fourth (10.130.9.5): Normal
                ctx1 Interface outside (10.1.1.1): Normal
                ctx1 Interface inside (10.2.2.1): Normal
                ctx2 Interface outside (10.3.3.2): Normal
                ctx2 Interface inside (10.4.4.2): Normal

  Other host:   Secondary
  Group 1       State:          Standby Ready
                Active time:    190 (sec)
  Group 2       State:          Active
                Active time:    3322 (sec)

                slot 0: ASA-5530 hw/sw rev (1.0/7.0(0)79) status (Up Sys)
                slot 1: SSM-IDS-20 hw/sw rev (1.0/5.0(0.1)S91(0.1)) status (Up)
                admin Interface outside (10.132.8.6): Normal
                admin Interface third (10.132.9.6): Normal
                admin Interface inside (10.130.8.6): Normal
                admin Interface fourth (10.130.9.6): Normal
                ctx1 Interface outside (10.1.1.2): Normal
                ctx1 Interface inside (10.2.2.2): Normal
                ctx2 Interface outside (10.3.3.1): Normal
                ctx2 Interface inside (10.4.4.1): Normal

Stateful Failover Logical Update Statistics
        Link : third GigabitEthernet0/2 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         0          0          0          0
        sys cmd         380        0          380        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        1435       0          1450       0
        UDP conn        0          0          0          0
        ARP tbl         124        0          65         0
        Xlate_Timeout   0          0          0          0
        VPN IKE upd     15         0          0          0
        VPN IPSEC upd   90         0          0          0
        VPN CTCP upd    0          0          0          0
        VPN SDI upd     0          0          0          0
        VPN DHCP upd    0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       1895
        Xmit Q:         0       0       1940
```

次に、ASA 5505 適応型セキュリティ アプライアンスでの **show failover** コマンドの出力例を示します。

```
Failover On
Failover unit Primary
Failover LAN Interface: fover Vlan150 (up)
Unit Poll frequency 1 seconds, holdtime 15 seconds
Interface Poll frequency 5 seconds, holdtime 25 seconds
Interface Policy 1
Monitored Interfaces 4 of 250 maximum
Version: Ours 7.2(0)55, Mate 7.2(0)55
Last Failover at: 19:59:58 PST Apr 6 2006

        This host: Primary - Active
                Active time: 34 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.1): Normal
                  Interface outside (192.168.2.201): Normal
                  Interface dmz (172.16.0.1): Normal
                  Interface test (172.23.62.138): Normal
                slot 1: empty

        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5505 hw/sw rev (1.0/7.2(0)55) status (Up Sys)
                  Interface inside (192.168.1.2): Normal
                  Interface outside (192.168.2.211): Normal
                  Interface dmz (172.16.0.2): Normal
                  Interface test (172.23.62.137): Normal
                slot 1: empty
```

次に、**show failover state** コマンドの出力例を示します。

```
hostname# show failover state

====My State===
Primary | Active |
====Other State===
Secondary | Standby |
====Configuration State===
        Sync Done
====Communication State===
        Mac set
=========Failed Reason==============
My Fail Reason:
Other Fail Reason:
        Service Card Failure
```

表 26-2 に **show failover state** コマンドの出力を示します。

表 26-2　show failover state 出力の説明

フィールド	説明
My State	装置の Primary/Secondary ステータスおよび Active/Standby ステータスを表示します。
Other State	ピア装置の Primary/Secondary ステータスおよび Active/Standby ステータスを表示します。

表 26-2　show failover state 出力の説明（続き）

フィールド	説明
Configuration State	コンフィギュレーションの同期化の状態を表示します。 次に、スタンバイ装置について表示される可能性のあるコンフィギュレーション状態を示します。 • **Config Syncing - STANDBY**：コンフィギュレーションの同期化の実行中に設定されます。 • **Sync Done - STANDBY**：スタンバイ装置がアクティブ装置からのコンフィギュレーションの同期化を完了したときに設定されます。 次に、アクティブ装置について表示される可能性のあるコンフィギュレーション状態を示します。 • **Config Syncing**：アクティブ装置がスタンバイ装置へのコンフィギュレーションの同期化を実行中に、アクティブ装置に設定されます。 • **Sync Done**：アクティブ装置がスタンバイ装置へのコンフィギュレーションの同期化を正常に終了したときに設定されます。 • **Ready for Config Sync**：スタンバイ装置がコンフィギュレーションの同期化を受信する準備ができたという信号を送信したときに、アクティブ装置に設定されます。
Communication State	MAC アドレスの同期化の状態を表示します。 • **Mac set**：MAC アドレスがピア装置からこの装置に同期されました。 • **Updated Mac**：MAC アドレスが更新され、他の装置と同期する必要がある場合に使用されます。また、この装置がピア装置から同期されたローカル MAC アドレスを更新している移行期間中にも使用されます。
Failed Reason	最後に報告された障害の原因を表示します。障害状態が解決した場合でも、この情報は消去されません。この情報は、フェールオーバーが発生した場合にのみ変更されます。 次に、障害を引き起こす可能性のある原因を示します。 • **Ifc Failure**：障害が発生したインターフェイスの数がフェールオーバー基準を満たした結果、フェールオーバーが発生した。 • **Comm Failure**：フェールオーバー リンクに障害が発生したか、またはピアがダウンしている。 • **Service card Failure**：SSM カードに障害が発生した（ASA のみ）。

次に、**show failover history** コマンドの出力例を示します。

```
hostname# show failover history

==============================================================================
From State                 To State                   Reason
==============================================================================
Not Detected               Negotiation                No Error

Negotiation                Cold Standby               Detected an Active mate

Cold Standby               Sync Config                Detected an Active mate

Sync Config                Sync File System           Detected an Active mate

Sync File System           Bulk Sync                  Detected an Active mate

Bulk Sync                  Standby Ready              Detected an Active mate

Standby Ready              Just Active                Set by the CI config cmd

Just Active                Active Drain               Set by the CI config cmd

Active Drain               Active Applying Config     Set by the CI config cmd

Active Applying Config     Active Config Applied      Set by the CI config cmd

Active Config Applied      Active                     Set by the CI config cmd

Active                     Disabled                   Set by the CI config cmd

==============================================================================
```

各エントリは、状態変化が発生した日時、最初の状態、最終の状態、および状態変化の原因を示します。最新のエントリは、下部に表示されます。古いエントリは上部に表示されます。最大 60 のエントリを表示できます。エントリが最大数に達すると、最も古いエントリが出力の上部から削除され、新しいエントリが下部に追加されます。

表 26-3 にフェールオーバーの状態を示します。状態には、安定状態と過渡状態の 2 種類があります。安定状態は、障害などによって状態変化が発生するまで装置が維持できる状態です。過渡状態は、装置が安定状態に到達する途上にある状態です。

表 26-3　フェールオーバーの状態

状態	説明
Initialization	この装置はプラットフォームの機能およびコンフィギュレーションをチェックし、フェールオーバー通信チャネルの準備をしています。これは過渡状態です。
Disabled	フェールオーバーはディセーブルになっています。これは安定状態です。
Negotiation	この装置はピアとの接続を確立し、ピアとネゴシエートしてソフトウェアバージョンの互換性および Active/Standby ロールを判断します。ネゴシエーションされているロールに応じて、この装置は Standby Unit States または Active Unit States に移行するか、または障害が発生した状態に入ります。これは過渡状態です。
Failed	この装置は、障害が発生した状態です。これは安定状態です。
Standby Unit States	
Cold Standby	この装置は、ピアが Active 状態になるのを待っています。ピア装置が Active 状態になると、この装置は Standby Config 状態に進みます。これは過渡状態です。

表 26-3　フェールオーバーの状態（続き）

状態	説明
Sync Config	この装置は、ピア装置に実行コンフィギュレーションを要求しています。コンフィギュレーションの同期化中にエラーが発生した場合、この装置は Initialization 状態に戻ります。これは過渡状態です。
Sync File System	この装置は、ピア装置とファイル システムを同期しています。これは過渡状態です。
Bulk Sync	この装置は、ピア装置から状態の情報を受信しています。この状態が発生するのは、ステートフル フェールオーバーがイネーブルになっている場合のみです。これは過渡状態です。
Standby Ready	この装置は、アクティブ装置に障害が発生した場合に引き継ぐ準備ができています。これは安定状態です。
Active Unit States	
Just Active	この装置がアクティブ装置になったときの最初の状態。この状態のとき、メッセージがピアに送信され、この装置がアクティブになり、IP アドレスと MAC アドレスがインターフェイス用に設定されたことがピアに通知されます。これは過渡状態です。
Active Drain	ピアのキュー メッセージは廃棄されます。これは過渡状態です。
Active Applying Config	この装置は、システム コンフィギュレーションを適用しています。これは過渡状態です。
Active Config Applied	この装置は、システム コンフィギュレーションの適用を終了しました。これは過渡状態です。
Active	この装置はアクティブで、トラフィックを処理しています。これは安定状態です。

各状態変化の後に、状態変化の原因が示されます。通常、状態変化の原因は、装置が過渡状態から安定状態へ移行する原因と同じです。次に、状態変化をもたらす可能性のある原因を示します。

- エラーなし
- CI config cmd によって設定されている
- フェールオーバー状態チェック
- フェールオーバー インターフェイスの準備ができた
- HELLO が受信されない
- 他の装置のソフトウェア バージョンが異なっている
- 他の装置の動作モードが異なっている
- 他の装置のライセンスが異なっている
- 他の装置のシャーシ設定が異なっている
- 他の装置のカード設定が異なっている
- 他の装置が、この装置にアクティブ状態になるよう要求した
- 他の装置が、この装置にスタンバイ状態になるよう要求した
- 他の装置が、この装置に障害が発生したことを報告した
- 他の装置が、その装置自体に障害が発生したことを報告した
- コンフィギュレーションのミスマッチ
- アクティブ装置が検出された
- アクティブ装置が検出されなかった
- コンフィギュレーションの同期化が行われた

- 通信障害から回復した
- 他の装置の VLAN コンフィギュレーションが異なっている
- VLAN コンフィギュレーションを確認できない
- コンフィギュレーションの同期化が不完全である
- コンフィギュレーションの同期化に失敗した
- インターフェイス チェック
- この装置で通信に障害が発生した
- ACK がフェールオーバー メッセージを受信しなかった
- 他の装置が、同期化後にラーニング状態で動作しなくなった
- ピアの電源が検出されなかった
- フェールオーバー ケーブルがない
- HA 状態の移行に失敗した
- サービス カード障害が検出された
- 他の装置のサービス カードに障害が発生した
- この装置のサービス カードがピアと同様である
- LAN インターフェイスが未設定状態になった
- ピア装置がリロードされた
- シリアル ケーブルから LAN ベース fover に切り替わった
- コンフィギュレーションの同期化の状態を確認できない
- 原因不明

関連コマンド

コマンド	説明
show running-config failover	現在のコンフィギュレーション内の **failover** コマンドを表示します。

show file

ファイル システムに関する情報を表示するには、特権 EXEC モードで **show file** コマンドを使用します。

show file descriptors | system | information *filename*

シンタックスの説明

descriptors	開かれているファイル記述子をすべて表示します。
information	特定のファイルに関する情報を表示します。
filename	ファイル名を指定します。
system	ディスク ファイル システムについて、サイズ、利用可能なバイト数、メディアのタイプ、フラグ、およびプレフィックス情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、ファイル システムに関する情報を表示する方法を示しています。

```
hostname# show file descriptors
No open file descriptors
hostname# show file system
File Systems:
   Size(b)     Free(b)    Type  Flags  Prefixes
* 60985344    60973056    disk    rw     disk:
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
pwd	現在の作業ディレクトリを表示します。

show firewall

現在のファイアウォール モード（ルーテッドまたは透過）を表示するには、特権 EXEC モードで **show firewall** コマンドを使用します。

show firewall

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show firewall** コマンドの出力例を示します。

```
hostname# show firewall
Firewall mode: Router
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを設定します。
show mode	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

show flash

内蔵フラッシュ メモリの内容を表示するには、特権 EXEC モードで **show flash:** コマンドを使用します。

show flash:

（注） ASA 5500 シリーズでは、***flash*** キーワードは ***disk0*** のエイリアスです。

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、内蔵フラッシュ メモリの内容を表示する方法を示しています。

```
hostname# show flash:
-#- --length-- -----date/time------ path
 11 1301       Feb 21 2005 18:01:34 test.cfg
 12 1949       Feb 21 2005 20:13:36 pepsi.cfg
 13 2551       Jan 06 2005 10:07:36 Leo.cfg
 14 609223     Jan 21 2005 07:14:18 rr.cfg
 15 1619       Jul 16 2004 16:06:48 hackers.cfg
 16 3184       Aug 03 2004 07:07:00 old_running.cfg
 17 4787       Mar 04 2005 12:32:18 admin.cfg
 20 1792       Jan 21 2005 07:29:24 Marketing.cfg
 21 7765184    Mar 07 2005 19:38:30 asdmfile-RLK
 22 1674       Nov 11 2004 02:47:52 potts.cfg
 23 1863       Jan 21 2005 07:29:18 r.cfg
 24 1197       Jan 19 2005 08:17:48 tst.cfg
 25 608554     Jan 13 2005 06:20:54 500kconfig
 26 5124096    Feb 20 2005 08:49:28 cdisk70102
 27 5124096    Mar 01 2005 17:59:56 cdisk70104
 28 2074       Jan 13 2005 08:13:26 negateACL
 29 5124096    Mar 07 2005 19:56:58 cdisk70105
 30 1276       Jan 28 2005 08:31:58 steel
 31 7756788    Feb 24 2005 12:59:46 asdmfile.50074.dbg
 32 7579792    Mar 08 2005 11:06:56 asdmfile.gusingh
 33 7764344    Mar 04 2005 12:17:46 asdmfile.50075.dbg
 34 5124096    Feb 24 2005 11:50:50 cdisk70103
 35 15322      Mar 04 2005 12:30:24 hs_err_pid2240.log

10170368 bytes available (52711424 bytes used)
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
show disk0	内蔵フラッシュ メモリの内容を表示します。
show disk1	外部フラッシュ メモリ カードの内容を表示します。

show fragment

IP フラグメント再構成モジュールの運用データを表示するには、特権 EXEC モードで ***show fragment*** コマンドを入力します。

show fragment [*interface*]

シンタックスの説明

interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
イネーブル EXEC モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	コンフィギュレーション データを運用データから分離するために、コマンドが ***show fragment*** と ***show running-config fragment*** の 2 つのコマンドに分割されました。

例

次の例は、IP フラグメント再構成モジュールの運用データを表示する方法を示しています。

```
hostname# show fragment
Interface: inside
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: outside1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test1
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
Interface: test2
    Size: 200, Chain: 24, Timeout: 5, Threshold: 133
    Queue: 0, Assembled: 0, Fail: 0, Overflow: 0
```

関連コマンド

コマンド	説明
clear configure fragment	IP フラグメント再構成コンフィギュレーションを消去し、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの運用データを消去します。
fragment	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

show gc

ガーベッジ コレクション プロセスに関する統計情報を表示するには、特権 EXEC モードで **show gc** コマンドを使用します。

show gc

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show gc** コマンドの出力例を示します。

```
hostname# show gc

Garbage collection process stats:
Total tcp conn delete response             :            0
Total udp conn delete response             :            0
Total number of zombie cleaned             :            0
Total number of embryonic conn cleaned     :            0
Total error response                       :            0
Total queries generated                    :            0
Total queries with conn present response   :            0
Total number of sweeps                     :          946
Total number of invalid vcid               :            0
Total number of zombie vcid                :            0
```

関連コマンド

コマンド	説明
clear gc	ガーベッジ コレクション プロセスに関する統計情報を削除します。

show h225

セキュリティ アプライアンスを越えて確立されている H.225 セッションの情報を表示するには、特権 EXEC モードで **show h225** コマンドを使用します。

show h225

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show h225 コマンドは、セキュリティ アプライアンスを越えて確立されている H.225 セッションの情報を表示します。**debug h323 h225 event**、**debug h323 h245 event**、および **show local-host** コマンドと共に、このコマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用されます。

show h225、**show h245**、または **show h323-ras** コマンドを使用する前に、**pager** コマンドを設定することを推奨します。多くのセッション レコードが存在し、**pager** コマンドが設定されていない場合、**show** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。異常なほど多くの接続が存在する場合は、デフォルトのタイムアウト値または設定した値を基づいてセッションがタイムアウトしているかどうか確認します。タイムアウトしていなければ問題があるので、調査が必要です。

例

次に、**show h225** コマンドの出力例を示します。

```
hostname# show h225
Total H.323 Calls: 1
1 Concurrent Call(s) for
 | Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
 | 1. CRV 9861
 | Local: | 10.130.56.3/1040 | Foreign: 172.30.254.203/1720
0 Concurrent Call(s) for
 | Local: | 10.130.56.4/1050 | Foreign: 172.30.254.205/1720
```

この出力は、現在セキュリティ アプライアンスを通過しているアクティブ H.323 コールが 1 つ、ローカル エンドポイント 10.130.56.3 と外部のホスト 172.30.254.203 の間にあることを示しています。また、これらの特定のエンドポイントの間に、同時コールが 1 つあり、そのコールの CRV（Call Reference Value）が 9861 であることを示しています。

ローカル エンドポイント 10.130.56.4 と外部ホスト 172.30.254.205 に対して、同時コールは 0 です。つまり H.225 セッションがまだ存在しているものの、このエンドポイント間にはアクティブ コールがないことを意味します。この状況は、**show h225** コマンドを実行したときに、コールはすでに終了しているが、H.225 セッションがまだ削除されていない場合に発生する可能性があります。または、2 つのエンドポイントが、「maintainConnection」を TRUE に設定しているため、TCP 接続をまだ開いたままにしていることを意味する可能性もあります。したがって、「maintainConnection」を再度 FALSE に設定するまで、またはコンフィギュレーション内の H.225 タイムアウト値に基づくセッションのタイムアウトが起こるまで、セッションは開いたままになります。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show h245

スロー スタートを使用しているエンドポイントによって、セキュリティ アプライアンスを越えて確立されている H.245 セッションの情報を表示するには、特権 EXEC モードで **show h245** コマンドを使用します。

show h245

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show h245 コマンドは、スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します（スロースタートは、コールの 2 つのエンドポイントが H.245 用の別の TCP コントロール チャネルを開いた場合です。ファースト スタートは、H.245 メッセージが H.225 コントロール チャネル上の H.225 メッセージの一部として交換された場合です）。**debug h323 h245 event**、**debug h323 h225 event**、および **show local-host** コマンドと共に、このコマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用されます。

例

次に、**show h245** コマンドの出力例を示します。

```
hostname# show h245
Total: 1
  | LOCAL | TPKT | FOREIGN | TPKT
1 | 10.130.56.3/1041 | 0 | 172.30.254.203/1245 | 0
  | MEDIA: LCN 258 Foreign 172.30.254.203 RTP 49608 RTCP 49609
  | Local | 10.130.56.3 RTP 49608 RTCP 49609
  | MEDIA: LCN 259 Foreign 172.30.254.203 RTP 49606 RTCP 49607
  | Local | 10.130.56.3 RTP 49606 RTCP 49607
```

セキュリティ アプライアンスを越えているアクティブな H.245 コントロール セッションが、現在 1 つあります。ローカル エンドポイントは、10.130.56.3 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します（TKTP ヘッダーは、各 H.225/H.245 メッセージの前に送られる 4 バイトのヘッダーです。このヘッダーで、この 4 バイトのヘッダーを含むメッセージの長さが分かります）。外部のホストのエンドポイントは、172.30.254.203 であり、TPKT 値が 0 であることから、このエンドポイントからの次のパケットには TPKT ヘッダーがあると予測します。

これらのエンドポイント間でネゴシエートされたメディアには、258 という LCN（論理チャネル番号）があり、外部に 172.30.254.203/49608 という RTP IP アドレス / ポート ペアと 172.30.254.203/49609 という RTCP IP アドレス / ポート ペアを持ち、ローカルに 10.130.56.3/49608 という RTP IP アドレス / ポート ペアと 49609 という RTCP ポートを持っています。

259 という 2 番目の LCN には、外部に 172.30.254.203/49606 という RTP IP アドレス / ポート ペアと 172.30.254.203/49607 という RTCP IP アドレス / ポート ペアがあり、ローカルに 10.130.56.3/49606 という RTP IP アドレス / ポート ペアと 49607 という RTCP ポートを持っています。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show h323-ras

ゲートキーパーとその H.323 エンドポイントの間でセキュリティ アプライアンスを越えて確立されている H.323 RAS セッションの情報を表示するには、特権 EXEC モードで **show h323-ras** コマンドを使用します。

show h323-ras

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show h323-ras コマンドは、セキュリティ アプライアンスを越えてゲートキーパーとその H.323 エンドポイントの間に確立されている H.323 RAS セッションの情報を表示します。**debug h323 ras event** および **show local-host** コマンドと共に、このコマンドは、H.323 RAS 検査エンジンの問題のトラブルシューティングに使用されます。

show h323-ras コマンドは、H.323 検査エンジンの問題のトラブルシューティングに使用される接続情報を表示します。詳細については、**inspect protocol h323 {h225 | ras}** コマンドのページを参照してください。

例

次に、**show h323-ras** コマンドの出力例を示します。

```
hostname# show h323-ras
Total: 1
 | GK | Caller
 | 172.30.254.214 10.130.56.14
hostname#
```

この出力は、ゲートキーパー 172.30.254.214 とそのクライアント 10.130.56.14 の間にアクティブな登録が 1 つあることを示しています。

関連コマンド

コマンド	説明
debug h323	H.323 のデバッグ情報の表示をイネーブルにします。
inspect h323	H.323 アプリケーション検査をイネーブルにします。
show h245	スロースタートを使用しているエンドポイントがセキュリティ アプライアンスを越えて確立した H.245 セッションの情報を表示します。
show h323-ras	セキュリティ アプライアンスを越えて確立された H.323 RAS セッションの情報を表示します。
timeout h225 | h323	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

show history

以前に入力したコマンドを表示するには、ユーザ EXEC モードで **show history** コマンドを使用します。

show history

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**show history** コマンドを使用すると、以前に入力したコマンドを表示できます。上矢印キーと下矢印キーを使用したり、**^p** を入力して入力済みの行を表示したり、**^n** を入力して次の行を表示したりして、コマンドを個々に調べることができます。

例　次の例は、以前に入力したコマンドをユーザ EXEC モードに入っているときに表示する方法を示しています。

```
hostname> show history
    show history
    help
    show history
```

次の例は、以前に入力したコマンドを特権 EXEC モードに入っているときに表示する方法を示しています。

```
hostname# show history
    show history
    help
    show history
    enable
    show history
```

次の例は、以前に入力したコマンドをグローバル コンフィギュレーション モードに入っているときに表示する方法を示しています。

```
hostname(config)# show history
    show history
    help
    show history
    enable
    show history
    config t
    show history
```

関連コマンド

コマンド	説明
help	指定したコマンドのヘルプを表示します。

show icmp

ICMP コンフィギュレーションを表示するには、特権 EXEC モードで **show icmp** コマンドを使用します。

show icmp

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show icmp コマンドは、ICMP コンフィギュレーションを表示します。

例

次の例では、ICMP コンフィギュレーションを表示しています。

```
hostname# show icmp
```

関連コマンド

clear configure icmp	ICMP コンフィギュレーションを消去します。
debug icmp	ICMP に関するデバッグ情報の表示をイネーブルにします。
icmp	セキュリティ アプライアンス インターフェイスで終端する ICMP トラフィックに対して、アクセス規則を設定します。
inspect icmp	ICMP 検査エンジンをイネーブルまたはディセーブルにします。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show idb

インターフェイス記述子ブロックのステータスに関する情報を表示するには、特権 EXEC モードで **show idb** コマンドを使用します。

show idb

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

IDB は、インターフェイスのリソースを表現するための内部データ構造です。表示される出力については、「例」の項を参照してください。

例

次に、**show idb** コマンドの出力例を示します。

```
hostname# show idb
Maximum number of Software IDBs 280.  In use 23.

                    HWIDBs     SWIDBs
             Active 6          21
           Inactive 1          2
         Total IDBs 7          23
 Size each (bytes) 116        212
        Total bytes 812        4876

HWIDB#   1 0xbb68ebc  Control0/0
HWIDB#   2 0xcd47d84  GigabitEthernet0/0
HWIDB#   3 0xcd4c1dc  GigabitEthernet0/1
HWIDB#   4 0xcd5063c  GigabitEthernet0/2
HWIDB#   5 0xcd54a9c  GigabitEthernet0/3
HWIDB#   6 0xcd58f04  Management0/0

SWIDB#   1 0x0bb68f54 0x01010001 Control0/0
SWIDB#   2 0x0cd47e1c 0xffffffff GigabitEthernet0/0
SWIDB#   3 0x0cd772b4 0xffffffff GigabitEthernet0/0.1
  PEER IDB#   1 0x0d44109c 0xffffffff      3  GigabitEthernet0/0.1
  PEER IDB#   2 0x0d2c0674 0x00020002      2  GigabitEthernet0/0.1
  PEER IDB#   3 0x0d05a084 0x00010001      1  GigabitEthernet0/0.1
SWIDB#   4 0x0bb7501c 0xffffffff GigabitEthernet0/0.2
SWIDB#   5 0x0cd4c274 0xffffffff GigabitEthernet0/1
SWIDB#   6 0x0bb75704 0xffffffff GigabitEthernet0/1.1
  PEER IDB#   1 0x0cf8686c 0x00020003      2  GigabitEthernet0/1.1
SWIDB#   7 0x0bb75dec 0xffffffff GigabitEthernet0/1.2
  PEER IDB#   1 0x0d2c08ac 0xffffffff      2  GigabitEthernet0/1.2
SWIDB#   8 0x0bb764d4 0xffffffff GigabitEthernet0/1.3
  PEER IDB#   1 0x0d441294 0x00030001      3  GigabitEthernet0/1.3
SWIDB#   9 0x0cd506d4 0x01010002 GigabitEthernet0/2
SWIDB#  10 0x0cd54b34 0xffffffff GigabitEthernet0/3
  PEER IDB#   1 0x0d3291ec 0x00030002      3  GigabitEthernet0/3
  PEER IDB#   2 0x0d2c0aa4 0x00020001      2  GigabitEthernet0/3
  PEER IDB#   3 0x0d05a474 0x00010002      1  GigabitEthernet0/3
SWIDB#  11 0x0cd58f9c 0xffffffff Management0/0
  PEER IDB#   1 0x0d05a65c 0x00010003      1  Management0/0
```

表 26-4 に、各フィールドの説明を示します。

表 26-4　show idb stats のフィールド

フィールド	説明
HWIDBs	すべての HWIDB の統計情報を表示します。HWIDB は、システムのハードウェア ポートごとに作成されます。
SWIDBs	すべての SWIDB の統計情報を表示します。SWIDB は、システムのメイン インターフェイスとサブインターフェイスごと、およびコンテキストに割り当てられているインターフェイスごとに作成されます。 他の一部の内部ソフトウェア モジュールも IDB を作成します。
HWIDB#	ハードウェア インターフェイスのエントリを示します。IDB シーケンス番号、アドレス、およびインターフェイス名が各行に表示されます。
SWIDB#	ソフトウェア インターフェイスのエントリを示します。IDB シーケンス番号、アドレス、対応する vPif ID、およびインターフェイス名が各行に表示されます。
PEER IDB#	コンテキストに割り当てられているインターフェイスを示します。IDB シーケンス番号、アドレス、対応する vPif ID、コンテキスト ID、およびインターフェイス名が各行に表示されます。

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show igmp groups

セキュリティ アプライアンスに直接接続し、IGMP によってラーニングされたレシーバーがあるマルチキャスト グループを表示するには、特権 EXEC モードで **show igmp groups** コマンドを使用します。

show igmp groups [[***reserved*** | *group*] [*if_name*] [***detail***]] | ***summary***]

シンタックスの説明

detail	（オプション）送信元の詳細な説明を表示します。
group	（オプション）IGMP グループのアドレス。このオプション引数を指定すると、表示される情報は指定したグループに関するものだけになります。
if_name	（オプション）指定したインターフェイスのグループ情報を表示します。
reserved	（オプション）予約済みグループに関する情報を表示します。
summary	（オプション）グループ加入の要約情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

オプションの引数とキーワードをすべて省略した場合、**show igmp groups** コマンドは、直接接続しているすべてのマルチキャスト グループをグループ アドレス、インターフェイス タイプ、およびインターフェイス番号別に表示します。

例

次に、**show igmp groups** コマンドの出力例を示します。

```
hostname#show igmp groups

IGMP Connected Group Membership
Group Address    Interface            Uptime    Expires   Last Reporter
224.1.1.1        inside               00:00:53  00:03:26  192.168.1.6
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

show igmp interface

インターフェイスのマルチキャスト情報を表示するには、特権 EXEC モードで **show igmp interface** コマンドを使用します。

show igmp *interface* [*if_name*]

シンタックスの説明

if_name	（オプション）選択したインターフェイスの IGMP グループ情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。***detail*** キーワードが削除されました。

使用上のガイドライン

オプションの *if_name* 引数を省略した場合、**show igmp interface** コマンドはすべてのインターフェイスの情報を表示します。

例

次に、**show igmp interface** コマンドの出力例を示します。

```
hostname# show igmp interface inside

inside is up, line protocol is up
 Internet address is 192.168.37.6, subnet mask is 255.255.255.0
 IGMP is enabled on interface
 IGMP query interval is 60 seconds
 Inbound IGMP access group is not set
 Multicast routing is enabled on interface
 Multicast TTL threshold is 0
 Multicast designated router (DR) is 192.168.37.33
 No multicast groups joined
```

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンスに直接接続されている受信者、および IGMP を通じてラーニングされた受信者を持つマルチキャスト グループを表示します。

show igmp traffic

IGMP トラフィックに関する統計情報を表示するには、特権 EXEC モードで **show igmp traffic** コマンドを使用します。

show igmp traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show igmp traffic** コマンドの出力例を示します。

```
hostname# show igmp traffic

IGMP Traffic Counters
Elapsed time since counters cleared: 00:02:30
                               Received     Sent
Valid IGMP Packets                3           6
Queries                           2           6
Reports                           1           0
Leaves                            0           0
Mtrace packets                    0           0
DVMRP packets                     0           0
PIM packets                       0           0

Errors:
Malformed Packets                 0
Martian source                    0
Bad Checksums                     0
```

関連コマンド

コマンド	説明
clear igmp counters	すべての IGMP 統計情報カウンタを消去します。
clear igmp traffic	IGMP トラフィック カウンタを消去します。

show interface

インターフェイスに関する統計情報を表示するには、ユーザ EXEC モードで **show interface** コマンドを使用します。

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] [***stats*** | ***detail***]

シンタックスの説明

detail	（オプション）インターフェイスの詳細な情報を表示します。この情報には、インターフェイスが追加された順序、設定されている状態、実際の状態が含まれ、非対称ルーティングが **asr-group** コマンドによってイネーブルになっている場合は、非対称ルーティングの統計情報も含まれています。すべてのインターフェイスを表示する場合、SSM 用の内部インターフェイスが ASA 5500 シリーズ適応型セキュリティ アプライアンスにインストールされているときは、それらのインターフェイスに関する情報が表示されます。内部インターフェイスは、ユーザが設定することはできません。この情報は、デバッグのみを目的としたものです。
interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
stats	（デフォルト）インターフェイスに関する情報と統計情報を表示します。このキーワードはデフォルトであるため、入力を省略できます。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（オプション）組み込みスイッチを持つ ASA 5505 適応型セキュリティ アプライアンスなどのモデルに対して、VLAN インターフェイスを指定します。

デフォルト

オプションを指定しない場合は、すべてのインターフェイスに関する基本的な統計情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが、新しいインターフェイス番号付け方式を取り入れるように修正され、明示的な指定をするための ***stats*** キーワード、および ***detail*** キーワードが追加されました。
7.0(4)	このコマンドに 4GE SSM インターフェイスのサポートが追加されました。
7.2(1)	このコマンドにスイッチ インターフェイスのサポートが追加されました。

使用上のガイドライン

インターフェイスが複数のコンテキストで共有されている場合は、コンテキスト内でこのコマンドを入力すると、セキュリティ アプライアンスは現在のコンテキストに関する統計情報のみ表示します。このコマンドをシステム実行スペースで物理インターフェイスに関して入力すると、セキュリティ アプライアンスはすべてのコンテキストの合算統計情報を表示します。

サブインターフェイスに関して表示される統計情報の数は、物理インターフェイスに関して表示される統計情報の数のサブセットです。

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内でのみ使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内でのみ使用できます。**allocate-interface** コマンドで ***visible*** キーワードを設定した場合、セキュリティ アプライアンスは **show interface** コマンドの出力にインターフェイスの ID を表示します。

表示される出力については、「例」の項を参照してください。

例

次に、**show interface** コマンドの出力例を示します。

```
hostname> show interface
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1328522 packets input, 124426545 bytes, 0 no buffer
        Received 1215464 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124606 packets output, 86803402 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/7) software (0/0)
        output queue (curr/max blocks): hardware (0/13) software (0/0)
  Traffic Statistics for "outside":
        1328509 packets input, 99873203 bytes
        124606 packets output, 84502975 bytes
        524605 packets dropped
Interface GigabitEthernet0/1 "inside", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        MAC address 000b.fcf8.c44f, MTU 1500
        IP address 10.10.0.1, subnet mask 255.255.0.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
Interface GigabitEthernet0/2 "faillink", is administratively down, line protocol is
down
```

```
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c450, MTU 1500
        IP address 192.168.1.1, subnet mask 255.255.255.0
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
  Traffic Statistics for "faillink":
        0 packets input, 0 bytes
        1 packets output, 28 bytes
        0 packets dropped
Interface GigabitEthernet0/3 "", is administratively down, line protocol is down
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c451, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
Interface Management0/0 "", is administratively down, line protocol is down
  Hardware is i82557, BW 100 Mbps
        Auto-Duplex, Auto-Speed
        Available but not configured via nameif
        MAC address 000b.fcf8.c44d, MTU not set
        IP address unassigned
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
```

表 26-5 に、各フィールドの説明を示します。

表 26-5　show interface のフィールド

フィールド	説明
Interface *ID*	インターフェイス ID。コンテキスト内では、**allocate-interface** コマンドで ***visible*** キーワードを設定しない限り、セキュリティ アプライアンスはマッピング名（設定されている場合）を表示します。
“*interface_name*”	**nameif** コマンドで設定したインターフェイス名。システム内でこの名前を設定することはできないため、システム実行スペースでは、このフィールドは空白です。名前を設定していない場合は、Hardware 行の後に次のメッセージが表示されます。 `Available but not configured via nameif`

表 26-5　show interface のフィールド（続き）

フィールド	説明
is *state*	管理状態。次のいずれかです。 • up：インターフェイスはシャットダウンされていません。 • administratively down：インターフェイスは **shutdown** コマンドでシャットダウンされています。
Line protocol is *state*	回線の状態。次のいずれかです。 • up：使用しているケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが誤っているか、インターフェイス コネクタに接続されていません。
VLAN identifier	サブインターフェイスの VLAN ID。
Hardware	インターフェイスのタイプ、最大帯域幅、デュプレックス方式、および速度。リンクがダウンしている場合は、デュプレックス方式と速度は設定値が表示されます。リンクが動作している場合、これらのフィールドには実際の設定がカッコ（ ）で囲まれて設定値と共に表示されます。次に、一般的なハードウェア タイプを示します。 • i82542：PIX プラットフォームで使用される Intel PCI ファイバ ギガビット カード • i82543：PIX プラットフォームで使用される Intel PCI-X ファイバ ギガビット カード • i82546GB：ASA プラットフォームで使用される Intel PCI-X 銅線ギガビット • i82547GI：ASA プラットフォームでバックプレーンとして使用される Intel CSA 銅線ギガビット • i82557：ASA プラットフォームで使用される Intel PCI 銅線ファースト イーサネット • i82559：PIX プラットフォームで使用される Intel PCI 銅線ファースト イーサネット VCS7380：SSM-4GE で使用される Vitesse Four Port ギガビット スイッチ
Media-type	（4GE SSM インターフェイスのみ）インターフェイスが RJ-45 または SFP のいずれとして設定されているかを表示します。

message area	特定の状況下で、メッセージが表示されることがあります。次の例を参照してください。
	• システム実行スペースでは、次のメッセージが表示されることがあります。
	`Available for allocation to a context`
	• 名前を設定していない場合は、次のメッセージが表示されます。
	`Available but not configured via nameif`

MAC address	インターフェイスの MAC アドレス。
MTU	このインターフェイスで許容されるパケットの最大サイズ（バイト単位）。インターフェイス名を設定していない場合、このフィールドには「MTU not set」と表示されます。

表 26-5　show interface のフィールド（続き）

フィールド	説明
IP address	**ip address** コマンドを使用して設定した、または DHCP サーバから受信したインターフェイス IP アドレス。システム内で IP アドレスを設定することはできないため、システム実行スペースでは、このフィールドに「IP address unassigned」と表示されます。
Subnet mask	IP アドレスのサブネット マスク。
Packets input	このインターフェイスで受信されたパケット数。
Bytes	このインターフェイスで受信されたバイト数。
No buffer	メイン システムのバッファ スペースがなかったために、廃棄された受信済みパケットの数。この数を、無視された数と比較してください。イーサネット ネットワーク上のブロードキャスト ストームは、多くの場合、入力バッファ イベントがないことに原因があります。
Received:	
Broadcasts	受信されたブロードキャストの数。
Runts	最小限のパケット サイズ（64 バイト）よりも小さいために廃棄されたパケットの数。ラントの原因は、通常は衝突です。不適切な配線や電気干渉が原因となって発生することもあります。
Giants	最大パケット サイズを超えているために廃棄されたパケットの数。たとえば、1,518 バイトを超えるイーサネット パケットはすべてジャイアントと見なされます。
Input errors	下に示したタイプを含めた、入力エラーの総数。入力に関係しているこの他のエラーも、入力エラーの数が増加する原因になります。また、一部のデータグラムは複数のエラーを包含していることもあります。したがって、この合計数は下に示したタイプについて表示されるエラーの数を超える場合があります。
CRC	巡回冗長検査エラーの数。ステーションは、フレームを送信するときにフレーム末尾に CRC を付加します。この CRC は、フレームに含まれているデータに基づいて、アルゴリズムに従って生成されます。送信元と宛先の中間でフレームが改変された場合、セキュリティ アプライアンスは、CRC が一致しないことを指摘します。CRC の値が大きくなる原因は、通常は衝突か、不良データを転送しているステーションです。
Frame	フレーム エラーの数。不良フレームには、長さが不適切なパケット、またはフレーム チェックサムの正しくないパケットが含まれています。このエラーが発生する原因は、通常は衝突か、故障しているイーサネット デバイスです。
Overrun	入力レートがセキュリティ アプライアンスのデータ処理能力を超えたために、受信したデータをセキュリティ アプライアンスがハードウェア バッファに渡すことができなかった回数。
Ignored	インターフェイス ハードウェアの内部バッファが不足したために、インターフェイスによって無視された受信パケットの数。これらのバッファは、バッファの説明で前に述べたシステム バッファとは別のものです。無視される数は、ブロードキャスト ストームとバースト雑音が原因となって増加する場合もあります。
Abort	このフィールドは使用されません。この値は常に 0 です。
L2 decode drops	名前が（**nameif** コマンドで）設定されていないため、または無効な VLAN ID を持つフレームを受信したために、ドロップされたパケットの数。

表 26-5　show interface のフィールド（続き）

フィールド	説明
Packets output	このインターフェイスで送信されたパケット数。
Bytes	このインターフェイスで送信されたバイト数。
Underruns	トランスミッタの動作速度がセキュリティ アプライアンスの処理速度を上回った回数。
Output Errors	衝突が設定されている最大数を超えたために伝送されなかったフレーム数。このカウンタは、ネットワーク トラフィックが大きい間は増加します。
Collisions	イーサネット衝突（1 つまたは複数の衝突）が原因で、再送されたメッセージ数。これは、通常、拡張しすぎた LAN（イーサネット ケーブルまたはトランシーバ ケーブルが長すぎる、ステーション間にリピータが 3 つ以上ある、またはカスケード接続されたマルチポート トランシーバが多すぎる）で発生します。衝突したパケットは、出力パケットによって一度だけカウントされます。
Interface resets	インターフェイスがリセットされた回数。インターフェイスが 3 秒間伝送できない場合、セキュリティ アプライアンスはインターフェイスをリセットして、伝送を再開します。この間隔の間も、接続状態は保持されます。インターフェイスのリセットは、インターフェイスがループバックされた場合、またはシャットダウンされた場合にも起こります。
Babbles	未使用（「babble」は、トランスミッタがインターフェイス上に留まっている時間が、最大長のフレームの伝送に要する時間を超えたことを意味します）。
Late collisions	衝突が表示される通常のウィンドウに表示されない衝突が発生したために伝送されなかったフレーム数。遅延衝突は、パケットの伝送で遅れて検出される衝突です。通常は、このようなことは起こらないようになっています。2 つのイーサネット ホストが同時に伝送を試みた場合、両ホストが早期にパケットの衝突を起こして両方がバックオフするか、2 番目のホストが 1 番目のホストの伝送に気付いて待機します。 遅延衝突が発生した場合、デバイスが割り込んでイーサネット上でパケットの送信を試み、同時にセキュリティ アプライアンスがパケットの送信を一部終了します。セキュリティ アプライアンスは、パケットの最初の部分が入ったバッファをすでに解放してしまっている可能性があるため、パケットを再送信しません。ネットワーキング プロトコルは、パケットを再送信することで衝突に対処するように設計されているため、これは大きな問題ではありません。しかし、遅延衝突はネットワークに問題が存在することを示します。よくある問題は、リピータを何台も使用して拡張したネットワーク、および仕様範囲外で動作しているイーサネット ネットワークです。
Deferred	リンク上のアクティビティが原因で、伝送前に延期されたフレーム数。
Rate limit drops	（4GE SSM インターフェイスのみ）転送速度がギガビットではないインターフェイスを設定して、10Mbps を超える速度で転送しようとした場合に、ドロップされたパケットの数。
Lost carrier	伝送中に搬送信号が消失した回数。
No carrier	未使用。
Input queue (curr/max blocks):	入力キューに入っているパケットの数（現在値と最大値）。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。

表 26-5　show interface のフィールド（続き）

フィールド	説明
Output queue (curr/max blocks):	出力キューに入っているパケットの数（現在値と最大値）。
Hardware	ハードウェア キュー内のパケットの数。
Software	ソフトウェア キュー内のパケットの数。
Traffic Statistics:	受信、送信、またはドロップされたパケットの数。
Packets input	受信されたパケットの数とバイトの数。
Packets output	送信されたパケットの数とバイトの数。
Packets dropped	ドロップしたパケットの数。

次に、ASA 5505 適応型セキュリティ アプライアンスでの **show interface** コマンドの出力例を示します。スイッチ ポートが含まれます。

```
hostname# show interface
Interface Vlan1 "inside", is up, line protocol is up
  Hardware is EtherSVI
        MAC address 00d0.2bff.449f, MTU 1500
        IP address 1.1.1.1, subnet mask 255.0.0.0
  Traffic Statistics for "inside":
        0 packets input, 0 bytes
        0 packets output, 0 bytes
        0 packets dropped
      1 minute input rate 0 pkts/sec,  0 bytes/sec
      1 minute output rate 0 pkts/sec,  0 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 0 pkts/sec,  0 bytes/sec
      5 minute output rate 0 pkts/sec,  0 bytes/sec
      5 minute drop rate, 0 pkts/sec

    Interface Ethernet0/0 "", is up, line protocol is up
      Hardware is 88E6095, BW 100 Mbps
            Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
            Available but not configured via nameif
            MAC address 00d0.2bfd.6ec5, MTU not set
            IP address unassigned
            407 packets input, 53587 bytes, 0 no buffer
            Received 103 broadcasts, 0 runts, 0 giants
            0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
            0 L2 decode drops
            43 switch ingress policy drops
            0 packets output, 0 bytes, 0 underruns
            0 output errors, 0 collisions, 0 interface resets
            0 babbles, 0 late collisions, 0 deferred
            0 lost carrier, 0 no carrier
            0 rate limit drops
            0 switch egress policy drops
```

表 26-6 に、ASA 5505 適応型セキュリティ アプライアンスなどのスイッチ インターフェイスに関する **show interface** コマンドの各フィールドの説明を示します。**show interface** コマンドで表示されるフィールドについては、表 26-5 を参照してください。

表 26-6　スイッチ インターフェイスに関する show interface のフィールド

フィールド	説明
switch ingress policy drops	このドロップは通常、ポートが正常に設定されていない場合に表示されます。このドロップは、デフォルトまたはユーザ定義のスイッチ ポート設定の結果として、パケットがスイッチ ポート内で正常に転送されない場合に増分します。次のようなコンフィギュレーションがこのドロップの原因と考えられます。 • **nameif** コマンドが VLAN インターフェイスで設定されませんでした。 **（注）** 同じ VLAN のインターフェイスとして、**nameif** コマンドが設定されていなかった場合でも、VLAN 内でスイッチングが正常であれば、このカウンタは増分しません。 • VLAN がシャットダウンします。 • アクセス ポートが 802.1Q タグ付きパケットを受信しました。 • トランク ポートが、許可されていないタグ、またはタグ付きでないパケットを受信しました。
switch egress policy drops	現在使用されていません。

次に、**show interface detail** コマンドの出力例を示します。次の例では、すべてのインターフェイスに関する詳細なインターフェイス統計情報を表示しています。この情報には、内部インターフェイス（プラットフォームに存在する場合）が含まれ、非対称ルーティングが **asr-group** コマンドによってイネーブルになっている場合は、非対称ルーティングの統計情報も含まれています。

```
hostname> show interface detail
Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        MAC address 000b.fcf8.c44e, MTU 1500
        IP address 10.86.194.60, subnet mask 255.255.254.0
        1330214 packets input, 124580214 bytes, 0 no buffer
        Received 1216917 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        9 L2 decode drops
        124863 packets output, 86956597 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/7) software (0/0)
        output queue (curr/max blocks): hardware (0/13) software (0/0)
  Traffic Statistics for "outside":
        1330201 packets input, 99995120 bytes
        124863 packets output, 84651382 bytes
        525233 packets dropped
  Control Point Interface States:
        Interface number is 1
        Interface config status is active
        Interface state is active
Interface Internal-Data0/0 "", is up, line protocol is up
  Hardware is i82547GI rev00, BW 1000 Mbps
        (Full-duplex), (1000 Mbps)
        MAC address 0000.0001.0002, MTU not set
        IP address unassigned
        6 packets input, 1094 bytes, 0 no buffer
        Received 6 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops, 0 demux drops
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/2) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)
   Control Point Interface States:
        Interface number is unassigned
...
```

表 26-7 に、**show interface** ***detail*** コマンドの各フィールドの説明を示します。**show interface** コマンドで表示されるフィールドについては、表 26-5 を参照してください。

表 26-7　show interface detail のフィールド

フィールド	説明
Demux drops	（内部データ インターフェイスのみ）SSM インターフェイスからのパケットをセキュリティ アプライアンスが逆多重化できなかったために、ドロップされたパケットの数。SSM インターフェイスは、バックプレーンを経由してネイティブ インターフェイスと通信し、どの SSM インターフェイスからのパケットもバックプレーン上で多重化されます。
Control Point Interface States:	
Interface number	このインターフェイスが作成された順序を示す、デバッグに使用される番号。0 から開始されます。
Interface config status	管理状態。次のいずれかです。 • active：インターフェイスはシャットダウンされていません。 • not active：インターフェイスは **shutdown** コマンドでシャットダウンされています。
Interface state	インターフェイスの実際の状態。ほとんどの場合、この状態は上の config status と一致しています。ハイ アベイラビリティを設定した場合には、セキュリティ アプライアンスは必要に応じてインターフェイスを起動またはシャットダウンするため、一致しない場合があります。
Asymmetrical Routing Statistics:	
Received X1 packets	このインターフェイスで受信された ASR パケット数。
Transmitted X2 packets	このインターフェイスで送信された ASR パケット数。
Dropped X3 packets	このインターフェイスでドロップされた ASR パケット数。パケットがドロップされるのは、パケットを転送しようとしたときにインターフェイスがダウンしている場合です。

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear interface	**show interface** コマンドのカウンタを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show interface ip brief

インターフェイスの IP アドレスとステータスを表示するには、特権 EXEC モードで **show interface ip brief** コマンドを使用します。

show interface [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*] ***ip brief***

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ　コンテキスト　モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（オプション）組み込みスイッチを持つ ASA 5505 適応型セキュリティ アプライアンスなどのモデルに対して、VLAN インターフェイスを指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイスを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過[1]	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

1. Management 0/0 インターフェイスまたはサブインターフェイスに対してのみ使用可能。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	このコマンドに、VLAN インターフェイスのサポート、および Management 0/0 インターフェイスまたはサブインターフェイスのサポート（透過モード）が追加されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名またはインターフェイス名はコンテキスト内でのみ指定できます。

表示される出力については、「例」の項を参照してください。

例

次に、**show interface ip brief** コマンドの出力例を示します。

```
hostname# show interface ip brief
    Interface                  IP-Address      OK? Method  Status
Protocol
    Control0/0                 127.0.1.1       YES CONFIG  up                    up
    GigabitEthernet0/0         209.165.200.226 YES CONFIG  up                    up
    GigabitEthernet0/1         unassigned      YES unset   administratively down down
    GigabitEthernet0/2         10.1.1.50       YES manual  administratively down down
    GigabitEthernet0/3         192.168.2.6     YES DHCP    administratively down down
    Management0/0              209.165.201.3   YES CONFIG  up
```

表 26-8 に、各フィールドの説明を示します。

表 26-8　show interface ip brief のフィールド

フィールド	説明
Interface	インターフェイス ID。マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してマッピング名を設定した場合は、その名前。すべてのインターフェイスを表示する場合、AIP SSM 用の内部インターフェイスが ASA 適応型セキュリティ アプライアンスにインストールされているときは、それらのインターフェイスに関する情報も表示されます。内部インターフェイスは、ユーザが設定することはできません。この情報は、デバッグのみを目的としたものです。
IP-Address	インターフェイスの IP アドレス。
OK?	このカラムは、現在は使用されていません。常に「Yes」が表示されます。
Method	インターフェイスが IP アドレスを受信したときの方法。値には、次のものがあります。 • unset：IP アドレスが設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。
Status	管理状態。次のいずれかです。 • up：インターフェイスはシャットダウンされていません。 • administratively down：インターフェイスは **shutdown** コマンドでシャットダウンされています。
Protocol	回線の状態。次のいずれかです。 • up：使用しているケーブルがネットワーク インターフェイスに接続されています。 • down：ケーブルが誤っているか、インターフェイス コネクタに接続されていません。

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address	インターフェイスの IP アドレスを設定します。または、透過ファイアウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show inventory

ネットワーク デバイスにインストールされ、製品 ID（PID）、バージョン ID（VID）、シリアル番号（SN）を割り当てられているすべてのシスコ製品に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show inventory** コマンドを使用します。シスコ エンティティに PID が割り当てられていない場合、そのエンティティは取得されず、表示されません。

show inventory [**slot**]

シンタックスの説明

slot	（オプション）SSM スロット番号を指定します（システムはスロット 0）。

デフォルト

インベントリを表示するスロットを指定しない場合は、次のように処理されます。

- 電源を含めて、すべての SSM のインベントリ情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	セマンティックの小さな変更。

使用上のガイドライン

show inventory コマンドは、各シスコ製品のインベントリ情報を UDI 形式で取得し、表示します。UDI は、製品 ID（PID）、バージョン ID（VID）、シリアル番号（SN）という 3 つの別個のデータ要素を結合したものです。

PID は、製品をご注文いただく際の名称で、従来は「製品名」または「製品番号」と呼ばれていたものです。これは、交換部品を間違いなくご注文いただくために使用する識別子です。

VID は、製品のバージョンです。製品が改良されると、VID が増分します。VID は、製品変更通知（PCN）について規定した業界ガイドラインである Telcordia GR-209-CORE に基づいた、厳格なプロセスに従って増分されます。

SN は、製品に対するベンダー独自の連続番号です。製造される各製品は、製造時に割り当てられる一意のシリアル番号を保持しており、この番号は現場では変更できません。この番号は、製品の特定のインスタンスを個々に識別するための手段です。

UDI では、各製品をエンティティと呼びます。シャーシなどの一部のエンティティは、スロットなどの下位エンティティを保持しています。各エンティティは、シスコ エンティティ別に階層構造で整理された論理的な表示順に従って、1 行に 1 つずつ表示されます。

show inventory コマンドをオプションなしで使用すると、ネットワーク デバイスにインストールされた、PID を割り当てられているシスコ エンティティのリストが表示されます。

例

次に、キーワードと引数を指定しない場合の **show inventory** コマンドの出力例を示します。この出力例では、ルータにインストールされた、PID を割り当てられているシスコ エンティティのリストが表示されています。

```
ciscoasa# show inventory
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540            , VID:V01 , SN:P3000000998

Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20         , VID:V01 , SN:P0000000999

Name:"power supply", DESCR:"ASA 5500 Series 180W AC Power Supply"
PID:ASA-180W-PWR-AC    , VID:V01 , SN:123456789AB

ciscoasa# show inventory 0
Name:"Chassis", DESCR:"ASA 5540 Adaptive Security Appliance"
PID:ASA5540            , VID:V01 , SN:P3000000998

ciscoasa# show inventory 1
Name:"slot 1", DESCR:"ASA 5500 Series Security Services Module-20"
PID:ASA-SSM-20         , VID:V01 , SN:P0000000999
```

表 26-9 は、この出力に表示されるフィールドについて説明しています。

表 26-9　show inventory のフィールドの説明

フィールド	説明
Name	シスコ エンティティに割り当てられている物理名（テキスト文字列）。たとえば、デバイスの物理コンポーネント名前付けシンタックスに基づいた、「1」などのコンソール番号または単純なコンポーネント番号（ポート番号やモジュール番号）です。RFC 2737 の entPhysicalName MIB 変数に相当します。
DESCR	オブジェクトの特徴を示す、シスコ エンティティの物理的な説明。RFC 2737 の entPhysicalDesc MIB 変数に相当します。
PID	エンティティの製品 ID。RFC 2737 の entPhysicalModeName MIB 変数に相当します。
VID	エンティティのバージョン ID。RFC 2737 の entPhysicalHardwareRev MIB 変数に相当します。
SN	製品のシリアル番号。RFC 2737 の entPhysicalSerialNum MIB 変数に相当します。

関連コマンド

コマンド	説明
show diag	ネットワーク デバイスについて、コントローラ、インターフェイス プロセッサ、ポート アダプタの診断情報を表示します。
show tech-support	ルータが問題を報告したときに、ルータに関する一般情報を表示します。

show ip address

インターフェイスの IP アドレスまたは透過モードの管理 IP アドレスを表示するには、特権 EXEC モードで **show ip address** コマンドを使用します。

show ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*]

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（オプション）組み込みスイッチを持つ ASA 5505 適応型セキュリティ アプライアンスなどのモデルに対して、VLAN インターフェイスを指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイスの IP アドレスを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドに VLAN インターフェイスのサポートが追加されました。

使用上のガイドライン

ハイ アベイラビリティを設定した場合は、現在の IP アドレスと共にプライマリ IP アドレス（表示には「System」と示されます）が表示されます。装置がアクティブになっている場合、システム IP アドレスと現在の IP アドレスは一致します。装置がスタンバイになっている場合、現在の IP アドレスにはスタンバイ アドレスが表示されます。

例

次に、**show ip address** コマンドの出力例を示します。

```
hostname# show ip address
System IP Addresses:
Interface                Name         IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
Current IP Addresses:
Interface                Name         IP address      Subnet mask       Method
GigabitEthernet0/0       mgmt         10.7.12.100     255.255.255.0     CONFIG
GigabitEthernet0/1       inside       10.1.1.100      255.255.255.0     CONFIG
GigabitEthernet0/2.40    outside      209.165.201.2   255.255.255.224   DHCP
GigabitEthernet0/3       dmz          209.165.200.225 255.255.255.224   manual
```

表 26-10 に、各フィールドの説明を示します。

表 26-10　show ip address のフィールド

フィールド	説明
Interface	インターフェイス ID。マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してマッピング名を設定した場合は、その名前。
Name	**nameif** コマンドで設定したインターフェイス名。
IP address	インターフェイスの IP アドレス。
Subnet mask	IP アドレスとサブネット マスク。
Method	インターフェイスが IP アドレスを受信したときの方法。値には、次のものがあります。 • unset：IP アドレスが設定されていません。 • manual：実行コンフィギュレーションを設定しました。 • CONFIG：スタートアップ コンフィギュレーションからロードしました。 • DHCP：DHCP サーバから受信しました。

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
nameif	インターフェイス名を設定します。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show ip address dhcp

インターフェイスの DHCP リースまたは DHCP サーバに関する詳細情報を表示するには、特権 EXEC モードで **show ip address dhcp** コマンドを使用します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*} ***dhcp*** {***lease*** | ***server***}

シンタックスの説明

interface_name	**nameif** コマンドで設定したインターフェイス名を指定します。
lease	DHCP リースに関する情報を表示します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
server	DHCP サーバに関する情報を表示します。
subinterface	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過[1]	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

1. Management 0/0 インターフェイスまたはサブインターフェイスに対してのみ使用可能。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、新しいサーバ機能に対応するための ***lease*** キーワードと ***server*** キーワードを含むように変更されました。
7.2(1)	このコマンドに、VLAN インターフェイスのサポート、および Management 0/0 インターフェイスまたはサブインターフェイスのサポート（透過モード）が追加されました。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

次に、**show ip address dhcp lease** コマンドの出力例を示します。

```
hostname# show ip address outside dhcp lease
Temp IP Addr:209.165.201.57 for peer on interface:outside
Temp sub net mask:255.255.255.224
   DHCP Lease server:209.165.200.225, state:3 Bound
   DHCP Transaction id:0x4123
   Lease:259200 secs, Renewal:129600 secs, Rebind:226800 secs
   Temp default-gateway addr:209.165.201.1
   Temp ip static route0: dest 10.9.0.0 router 10.7.12.255
   Next timer fires after:111797 secs
   Retry count:0, Client-ID:cisco-0000.0000.0000-outside
   Proxy: TRUE  Proxy Network: 10.1.1.1
   Hostname: device1
```

表 26-11 に、各フィールドの説明を示します。

表 26-11　show ip address dhcp lease のフィールド

フィールド	説明
Temp IP Addr	インターフェイスに割り当てられている IP アドレス。
Temp sub net mask	インターフェイスに割り当てられているサブネット マスク。
DHCP Lease server	DHCP サーバのアドレス。
state	DHCP リースの状態。次のいずれかです。 • Initial：初期化状態。セキュリティ アプライアンスがリース取得プロセスを開始します。この状態は、リースが終了したときとリースのネゴシエーションが失敗したときも表示されます。 • Selecting：セキュリティ アプライアンスは、1 つまたはそれ以上の DHCP サーバから DHCPOFFER メッセージを受信して、いずれかを選択できる状態になるのを待っています。 • Requesting：セキュリティ アプライアンスは、要求の送信先となったサーバからの応答を待っています。 • Purging：セキュリティ アプライアンスは、クライアントが IP アドレスを解放したか、その他の何らかのエラーが発生したために、リースを削除しています。 • Bound：セキュリティ アプライアンスは有効なリースを保持し、正常に動作しています。 • Renewing：セキュリティ　アプライアンスは、リースを更新しようとしています。DHCPREQUEST メッセージを現在の DHCP サーバに定期的に送信して、応答を待ちます。 • Rebinding：セキュリティ　アプライアンスは元のサーバとの間でリースの更新に失敗したため、いずれかのサーバから応答があるか、リースが終了するまで DHCPREQUEST メッセージを送信します。 • Holddown：セキュリティ アプライアンスは、リースを削除するプロセスを開始しました。 • Releasing：セキュリティ アプライアンスは、IP アドレスが不要になったことを示す解放メッセージをサーバに送信します。
DHCP transaction id	クライアントが選択したランダムな数値。要求メッセージに関連付けるためにクライアントとサーバが使用します。
Lease	DHCP サーバが指定した、インターフェイスがこの IP アドレスを使用できる期間。

表 26-11　show ip address dhcp lease のフィールド（続き）

フィールド	説明
Renewal	インターフェイスがこのリースを自動的に更新しようとするまでの期間。
Rebind	セキュリティ アプライアンスが DHCP サーバに再バインドしようとするまでの期間。再バインドが発生するのは、セキュリティ アプライアンスが元の DHCP サーバと通信できないまま、リース期間の 87.5% が経過した場合です。この場合、セキュリティ アプライアンスは DHCP 要求をブロードキャストして、使用可能ないずれかの DHCP サーバと通信しようとします。
Temp default-gateway addr	DHCP サーバが提供したデフォルト ゲートウェイ アドレス。
Temp ip static route0	デフォルトのスタティック ルート。
Next timer fires after	内部タイマーが始動するまでの秒数。
Retry count	セキュリティ アプライアンスがリースを確立しようとしている場合、このフィールドはセキュリティ アプライアンスが DHCP メッセージの送信を試行した回数を示しています。たとえば、セキュリティ アプライアンスが Selecting 状態になっている場合、この値はセキュリティ アプライアンスが検出メッセージを送信した回数を示しています。セキュリティ アプライアンスが Requesting 状態になっている場合は、セキュリティ アプライアンスが要求メッセージを送信した回数を示しています。
Client-ID	サーバとのすべての通信で使用されるクライアント ID。
Proxy	このインターフェイスが、VPN クライアントのプロキシ DHCP クライアントであるかどうかを示します（True または False）。
Proxy Network	要求されたネットワーク。
Hostname	クライアントのホスト名。

次に、**show ip address dhcp server** コマンドの出力例を示します。

```
hostname# show ip address outside dhcp server

   DHCP server: ANY (255.255.255.255)
    Leases:   0
    Offers:   0      Requests: 0     Acks: 0     Naks: 0
    Declines: 0      Releases: 0     Bad:  0

   DHCP server: 40.7.12.6
    Leases:   1
    Offers:   1      Requests: 17     Acks: 17     Naks: 0
    Declines: 0      Releases: 0     Bad:  0
    DNS0:   171.69.161.23,   DNS1:  171.69.161.24
    WINS0:  172.69.161.23,   WINS1: 172.69.161.23
    Subnet: 255.255.0.0   DNS Domain: cisco.com
```

表 26-12 に、各フィールドの説明を示します。

表 26-12　show ip address dhcp server のフィールド

フィールド	説明
DHCP server	このインターフェイスがリースを取得した DHCP サーバのアドレス。最初のエントリ（「ANY」）はデフォルト サーバで、常に表示されます。
Leases	サーバから取得したリースの数。インターフェイスの場合、リースの数は通常は 1 です。VPN のプロキシとして動作しているインターフェイスに対してサーバがアドレスを提供している場合は、リースが複数になります。
Offers	サーバからのオファーの数。
Requests	サーバに送信した要求の数。
Acks	サーバから受信した確認応答の数。
Naks	サーバから受信した否定応答の数。
Declines	サーバから受信した辞退の数。
Releases	サーバに送信したリリースの数。
Bad	サーバから受信した不良パケットの数。
DNS0	DHCP サーバから取得したプライマリ DNS サーバ アドレス。
DNS1	DHCP サーバから取得したセカンダリ DNS サーバ アドレス。
WINS0	DHCP サーバから取得したプライマリ WINS サーバ アドレス。
WINS1	DHCP サーバから取得したセカンダリ WINS サーバ アドレス。
Subnet	DHCP サーバから取得したサブネット アドレス。
DNS Domain	DHCP サーバから取得したドメイン。

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address dhcp	DHCP サーバから IP アドレスを取得するようにインターフェイスを設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip address pppoe

PPPoE 接続に関する詳細情報を表示するには、特権 EXEC モードで **show ip address pppoe** コマンドを実行します。

show ip address {*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name* | **vlan** *number*} ***pppoe***

シンタックスの説明

interface_name	**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。
vlan *number*	（オプション）組み込みスイッチを持つ ASA 5505 適応型セキュリティ アプライアンスなどのモデルに対して、VLAN インターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過[1]	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

1. Management 0/0 インターフェイスまたはサブインターフェイスに対してのみ使用可能。

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

次に、**show ip address pppoe** コマンドの出力例を示します。

```
hostname# show ip address outside pppoe
```

表 26-13 に、各フィールドの説明を示します。

表 26-13　show ip address dhcp lease のフィールド

フィールド	説明
	•

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address ppoe	PPPoE サーバから IP アドレスを取得するようにインターフェイスを設定します。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。
show ip address	インターフェイスの IP アドレスを表示します。

show ip audit count

インターフェイスに監査ポリシーを適用した場合に、一致したシグニチャの数を表示するには、特権 EXEC モードで **show ip audit count** コマンドを使用します。

show ip audit count [**global** | **interface** *interface_name*

シンタックスの説明

global	（デフォルト）すべてのインターフェイスについて、一致した件数を表示します。
interface *interface_name*	（オプション）指定したインターフェイスについて、一致した件数を表示します。

デフォルト

キーワードを指定しない場合は、すべてのインターフェイスについて一致件数が表示されます（***global***）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

監査ポリシーを作成するには **ip audit name** コマンドを使用し、ポリシーを適用するには **ip audit interface** コマンドを使用します。

例

次に、**show ip audit count** コマンドの出力例を示します。

```
hostname# show ip audit count
IP AUDIT GLOBAL COUNTERS

1000 I Bad IP Options List        0
1001 I Record Packet Route        0
1002 I Timestamp                  0
1003 I Provide s,c,h,tcc          0
1004 I Loose Source Route         0
1005 I SATNET ID                  0
1006 I Strict Source Route        0
1100 A IP Fragment Attack         0
1102 A Impossible IP Packet       0
1103 A IP Teardrop                0
2000 I ICMP Echo Reply            0
2001 I ICMP Unreachable           0
2002 I ICMP Source Quench         0
2003 I ICMP Redirect              0
2004 I ICMP Echo Request          10
2005 I ICMP Time Exceed           0
2006 I ICMP Parameter Problem     0
2007 I ICMP Time Request          0
2008 I ICMP Time Reply            0
2009 I ICMP Info Request          0
2010 I ICMP Info Reply            0
2011 I ICMP Address Mask Request  0
2012 I ICMP Address Mask Reply    0
2150 A Fragmented ICMP            0
2151 A Large ICMP                 0
2154 A Ping of Death              0
3040 A TCP No Flags               0
3041 A TCP SYN & FIN Flags Only   0
3042 A TCP FIN Flag Only          0
3153 A FTP Improper Address       0
3154 A FTP Improper Port          0
4050 A Bomb                       0
4051 A Snork                      0
4052 A Chargen                    0
6050 A DNS Host Info              0
6051 A DNS Zone Xfer              0
6052 A DNS Zone Xfer High Port    0
6053 A DNS All Records            0
6100 I RPC Port Registration      0
6101 I RPC Port Unregistration    0
6102 I RPC Dump                   0
6103 A Proxied RPC                0
6150 I ypserv Portmap Request     0
6151 I ypbind Portmap Request     0
6152 I yppasswdd Portmap Request  0
6153 I ypupdated Portmap Request  0
6154 I ypxfrd Portmap Request     0
6155 I mountd Portmap Request     0
6175 I rexd Portmap Request       0
6180 I rexd Attempt               0
6190 A statd Buffer Overflow      0

IP AUDIT INTERFACE COUNTERS: inside
...
```

関連コマンド

コマンド	説明
clear ip audit count	監査ポリシーのシグニチャ一致件数を消去します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit attack	**ip audit attack** コマンドのコンフィギュレーションを表示します。

show ip verify statistics

Unicast RPF 機能によってドロップされたパケットの数を表示するには、特権 EXEC モードで **show ip verify statistics** コマンドを使用します。Unicast RPF をイネーブルにするには、**ip verify reverse-path** コマンドを使用します。

show ip verify statistics [interface *interface_name*]

シンタックスの説明

interface ***interface_name***	（オプション）指定したインターフェイスに関する統計情報を表示します。

デフォルト

このコマンドは、すべてのインターフェイスに関する統計情報を表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show ip verify statistics** コマンドの出力例を示します。

```
hostname# show ip verify statistics
interface outside: 2 unicast rpf drops
interface inside: 1 unicast rpf drops
interface intf2: 3 unicast rpf drops
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを消去します。
clear ip verify statistics	Unicast RPF の統計情報を消去します。
ip verify reverse-path	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
show running-config ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを表示します。

show ipsec sa

IPSec SA のリストを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa** コマンドを使用します。このコマンドの別の形式である、**show crypto ipsec sa** を使用することもできます。

show ipsec sa [**entry** | **identity** | **map** *map-name* | **peer** *peer-addr*] [**detail**]

シンタックスの説明

detail	（オプション）表示対象に関する詳細なエラー情報を表示します。
entry	（オプション）IPSec SA をピア アドレスでソートして表示します。
identity	（オプション）IPSec SA を ID でソートして、ESP を除いて表示します。これは圧縮された形式です。
map map-name	（オプション）指定した暗号マップの IPSec SA を表示します。
peer peer-addr	（オプション）指定したピア IP アドレスの IPSec SA を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec SA を表示しています。

```
hostname(config)# show ipsec sa
interface: outside2
    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (172.20.0.21/255.255.255.255/0/0)
      current_peer: 172.20.0.21
      dynamic allocated peer ip: 10.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1145, #pkts decrypt: 1145, #pkts verify: 1145
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pre-frag successes: 2, #pre-frag failures: 1, #fragments created: 10
      #PMTUs sent: 5, #PMTUs rcvd: 2, #decapstulated frags needing reassembly: 1
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 10.132.0.17, remote crypto endpt.: 172.20.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 548
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 10.132.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
hostname(config)#
```

（注） 断片化の統計は、IPSec 処理前に断片化が発生することを IPSec SA ポリシーが記述している場合は、断片化前の統計になります。断片化後の統計は、IPSec 処理後に断片化が発生することを SA ポリシーが記述している場合に表示されます。

グローバル コンフィギュレーション モードで入力した次の例では、def という暗号マップの IPSec SA を表示しています。

```
hostname(config)# show ipsec sa map def
cryptomap: def
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1146, #pkts decrypt: 1146, #pkts verify: 1146
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 480
         IV size: 8 bytes
         replay detection support: Y

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73672, #pkts encrypt: 73672, #pkts digest: 73672
      #pkts decaps: 78824, #pkts decrypt: 78824, #pkts verify: 78824
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73672, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
```

```
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 263
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード ***entry*** を指定して IPSec SA を表示しています。

```
hostname(config)# show ipsec sa entry
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 429
         IV size: 8 bytes
         replay detection support: Y

peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73723, #pkts encrypt: 73723, #pkts digest: 73723
      #pkts decaps: 78878, #pkts decrypt: 78878, #pkts verify: 78878
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73723, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

```
    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 212
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

グローバル コンフィギュレーション モードで入力した次の例では、キーワード ***entry detail*** を指定して IPSec SA を表示しています。

```
hostname(config)# show ipsec sa entry detail
peer address: 10.132.0.21
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1148, #pkts decrypt: 1148, #pkts verify: 1148
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    inbound esp sas:
      spi: 0x1E8246FC (511854332)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0xDC15BF68 (3692412776)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 3, crypto-map: def
         sa timing: remaining key lifetime (sec): 322
         IV size: 8 bytes
         replay detection support: Y
```

```
peer address: 10.135.1.8
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73831, #pkts encrypt: 73831, #pkts digest: 73831
      #pkts decaps: 78989, #pkts decrypt: 78989, #pkts verify: 78989
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73831, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35

    inbound esp sas:
      spi: 0xB32CF0BD (3006066877)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
    outbound esp sas:
      spi: 0x3B6F6A35 (997157429)
         transform: esp-3des esp-md5-hmac
         in use settings ={RA, Tunnel, }
         slot: 0, conn_id: 4, crypto-map: def
         sa timing: remaining key lifetime (sec): 104
         IV size: 8 bytes
         replay detection support: Y
hostname(config)#
```

次の例では、キーワード ***identity*** を指定して IPSec SA を表示しています。

```
hostname(config)# show ipsec sa identity
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73756, #pkts encrypt: 73756, #pkts digest: 73756
      #pkts decaps: 78911, #pkts decrypt: 78911, #pkts verify: 78911
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73756, #pkts comp failed: 0, #pkts decomp failed: 0
      #send errors: 0, #recv errors: 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

次の例では、キーワード ***identity*** と ***detail*** を指定して IPSec SA を表示しています。

```
hostname(config)# show ipsec sa identity detail
interface: outside2
    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (10.132.0.21/255.255.255.255/0/0)
      current_peer: 10.132.0.21
      dynamic allocated peer ip: 90.135.1.5

      #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
      #pkts decaps: 1147, #pkts decrypt: 1147, #pkts verify: 1147
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.132.0.21

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: DC15BF68

    Crypto map tag: def, local addr: 172.20.0.17

      local ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
      remote ident (addr/mask/prot/port): (192.168.132.0/255.255.255.0/0/0)
      current_peer: 10.135.1.8
      dynamic allocated peer ip: 0.0.0.0

      #pkts encaps: 73771, #pkts encrypt: 73771, #pkts digest: 73771
      #pkts decaps: 78926, #pkts decrypt: 78926, #pkts verify: 78926
      #pkts compressed: 0, #pkts decompressed: 0
      #pkts not compressed: 73771, #pkts comp failed: 0, #pkts decomp failed: 0
      #pkts no sa (send): 0, #pkts invalid sa (rcv): 0
      #pkts encaps failed (send): 0, #pkts decaps failed (rcv): 0
      #pkts invalid prot (rcv): 0, #pkts verify failed: 0
      #pkts invalid identity (rcv): 0, #pkts invalid len (rcv): 0
      #pkts replay rollover (send): 0, #pkts replay rollover (rcv): 0
      #pkts replay failed (rcv): 0
      #pkts internal err (send): 0, #pkts internal err (rcv): 0

      local crypto endpt.: 172.20.0.17, remote crypto endpt.: 10.135.1.8

      path mtu 1500, ipsec overhead 60, media mtu 1500
      current outbound spi: 3B6F6A35
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show ipsec sa summary

IPSec SA の要約を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec sa summary** コマンドを使用します。

show ipsec sa summary

シンタックスの説明

このコマンドには、引数も変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、次の接続タイプごとに IPSec SA の要約を表示しています。

- IPSec
- IPSec over UDP
- IPSec over NAT-T
- IPSec over TCP
- IPSec VPN ロードバランシング

```
hostname(config)# show ipsec sa summary

Current IPSec SA's:             Peak IPSec SA's:
IPSec              :     2          Peak Concurrent SA  :    14
IPSec over UDP     :     2          Peak Concurrent L2L :     0
IPSec over NAT-T   :     4          Peak Concurrent RA  :    14
IPSec over TCP     :     6
IPSec VPN LB       :     0
Total              :    14
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPSec SA 全体を削除します。または、指定したパラメータに基づいて削除します。
show ipsec sa	IPSec SA のリストを表示します。
show ipsec stats	IPSec に関する一連の統計情報を表示します。

show ipsec stats

一連の IPSec 統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show ipsec stats** コマンドを使用します。

show ipsec stats

シンタックスの説明　このコマンドには、キーワードも変数もありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、IPSec 統計情報を表示しています。

```
hostname(config)# show ipsec stats

IPsec Global Statistics
-----------------------
Active tunnels: 2
Previous tunnels: 9
Inbound
    Bytes: 4933013
    Decompressed bytes: 4933013
    Packets: 80348
    Dropped packets: 0
    Replay failures: 0
    Authentications: 80348
    Authentication failures: 0
    Decryptions: 80348
    Decryption failures: 0
    Decapsulated fragments needing reassembly: 0
Outbound
    Bytes: 4441740
    Uncompressed bytes: 4441740
    Packets: 74029
    Dropped packets: 0
    Authentications: 74029
    Authentication failures: 0
    Encryptions: 74029
    Encryption failures: 0
    Fragmentation successes: 3
        Pre-fragmentation successes:2
        Post-fragmentation successes: 1
    Fragmentation failures: 2
        Pre-fragmentation failures:1
        Post-fragmentation failures: 1
    Fragments created: 10
    PMTUs sent: 1
    PMTUs recvd: 2
Protocol failures: 0
Missing SA failures: 0
System capacity failures: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear ipsec sa	IPSec SA またはカウンタを、指定したパラメータに基づいて消去します。
crypto ipsec transform-set	トランスフォーム セットを定義します。
show ipsec sa	指定したパラメータに基づいて IPSec SA を表示します。
show ipsec sa summary	IPSec SA の要約を表示します。

show ipv6 access-list

IPv6 アクセス リストを表示するには、特権 EXEC モードで **show ipv6 access-list** コマンドを使用します。IPv6 アクセス リストは、どの IPv6 トラフィックがセキュリティ アプライアンスを通過できるかを規定するものです。

show ipv6 access-list [*id* [*source-ipv6-prefix/prefix-length* | ***any*** | ***host*** *source-ipv6-address*]]

シンタックスの説明

any	（オプション）IPv6 プレフィックス ::/0 の短縮形です。
host *source-ipv6-address*	（オプション）特定のホストの IPv6 アドレス。指定した場合は、指定したホストに関するアクセス規則のみが表示されます。
id	（オプション）アクセス リスト名。指定した場合は、指定したアクセス リストのみが表示されます。
source-ipv6-prefix /prefix-length	（オプション）IPv6 ネットワーク アドレスとプレフィックス。指定した場合は、指定した IPv6 ネットワークに関するアクセス規則のみが表示されます。

デフォルト

すべての IPv6 アクセス リストを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show ipv6 access-list コマンドは、IPv6 固有のものであることを除けば、**show ip access-list** コマンドと同様の出力を提供します。

例

次に、**show ipv6 access-list** コマンドの出力例を示します。inbound、tcptraffic、および outbound という名前の IPv6 アクセス リストが表示されています。

```
hostname# show ipv6 access-list
IPv6 access list inbound
    permit tcp any any eq bgp reflect tcptraffic (8 matches) sequence 10
    permit tcp any any eq telnet reflect tcptraffic (15 matches) sequence 20
    permit udp any any reflect udptraffic sequence 30
IPv6 access list tcptraffic (reflexive) (per-user)
    permit tcp host 2001:0DB8:1::1 eq bgp host 2001:0DB8:1::2 eq 11000 timeout 300
(time
        left 243) sequence 1
    permit tcp host 2001:0DB8:1::1 eq telnet host 2001:0DB8:1::2 eq 11001 timeout 300
        (time left 296) sequence 2
IPv6 access list outbound
    evaluate udptraffic
    evaluate tcptraffic
```

関連コマンド

コマンド	説明
ipv6 access-list	IPv6 アクセス リストを作成します。

show ipv6 interface

IPv6 用に設定されているインターフェイスのステータスを表示するには、特権 EXEC モードで **show ipv6 interface** コマンドを使用します。

show ipv6 interface [***brief***] [*if_name* [***prefix***]]

シンタックスの説明

brief	各インターフェイスの IPv6 ステータスとコンフィギュレーションについて、簡単な要約を表示します。
if_name	（オプション）**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。指定したインターフェイスについてのみ、ステータスとコンフィギュレーションが表示されます。
prefix	（オプション）ローカル IPv6 プレフィックス プールから生成されたプレフィックス。

デフォルト

すべての IPv6 インターフェイスを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show ipv6 interface コマンドは、IPv6 固有のものであることを除けば、**show interface** コマンドと同様の出力を提供します。インターフェイス ハードウェアが使用可能な場合、そのインターフェイスは *up* とマークされます。インターフェイスが双方向通信を提供できる場合、回線プロトコルは *up* とマークされます。

インターフェイス名を指定しない場合は、すべての IPv6 インターフェイスに関する情報が表示されます。インターフェイス名を指定すると、指定したインターフェイスに関する情報が表示されます。

例

次に、**show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface outside
interface ethernet0 "outside" is up, line protocol is up
  IPv6 is enabled, link-local address is 2001:0DB8::/29 [TENTATIVE]
  Global unicast address(es):
    2000::2, subnet is 2000::/64
  Joined group address(es):
    FF02::1
    FF02::1:FF11:6770
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

次に、***brief*** キーワードを指定して入力した **show ipv6 interface** コマンドの出力例を示します。

```
hostname# show ipv6 interface brief
outside [up/up]
    unassigned
inside [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::a:0:0:a0a:a70
vlan101 [up/up]
    fe80::20d:29ff:fe1d:69f0
    fec0::65:0:0:a0a:6570
dmz-ca [up/up]
    unassigned
```

次に、**show ipv6 interface** コマンドの出力例を示します。アドレスからプレフィックスを生成したインターフェイスの特性が表示されています。

```
hostname# show ipv6 interface inside prefix
IPv6 Prefix Advertisements inside
Codes: A - Address, P - Prefix-Advertisement, O - Pool
       U - Per-user prefix, D - Default       N - Not advertised, C - Calendar

AD      fec0:0:0:a::/64 [LA] Valid lifetime 2592000, preferred lifetime 604800
```

show ipv6 neighbor

IPv6 近隣探索キャッシュ情報を表示するには、特権 EXEC モードで **show ipv6 neighbor** コマンドを使用します。

show ipv6 neighbor [*if_name* | *address*]

シンタックスの説明

address	（オプション）指定した IPv6 アドレスの近隣探索キャッシュ情報だけを表示します。
if_name	（オプション）指定したインターフェイス名（**nameif** コマンドによって設定）のキャッシュ情報だけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

次に、**show ipv6 neighbor** コマンドによって提供される情報を示します。

- **IPv6 Address**：ネイバーまたはインターフェイスの IPv6 アドレス。
- **Age**：アドレスが到達可能と確認された時点からの経過時間（分単位）。ハイフン（-）は、スタティック エントリであることを示します。
- **Link-layer Addr**：MAC アドレス。アドレスが不明な場合は、ハイフン（-）が表示されます。
- **State**：近隣キャッシュ エントリの状態。

（注） 到達可能性の検出は、IPv6 近隣探索キャッシュのスタティック エントリには適用されません。したがって、**INCMP**（不完全）状態と **REACH**（到達可能）状態の説明は、ダイナミック キャッシュ エントリとスタティック キャッシュ エントリで異なります。

次に、IPv6 近隣探索キャッシュのダイナミック エントリについて表示される可能性のある状態を示します。

- **INCMP**：（不完全）このエントリのアドレス解決を実行中です。ネイバー送信要求メッセージがターゲットの送信要求ノード マルチキャスト アドレスに送信されましたが、対応するネイバー アドバタイズメント メッセージをまだ受信していません。
- **REACH**：（到達可能）ネイバーへの転送パスが正常に機能していることを示す肯定確認が、直近の ReachableTime ミリ秒以内に受信されました。**REACH** 状態になっている間は、パケットが送信されるときにデバイスは特に操作を実行しません。

- **STALE**：転送パスが正常に機能していることを示す最後の肯定確認を受信してから、ReachableTime ミリ秒を超える時間が経過しました。**STALE** 状態になっている間は、パケットが送信されるまで、デバイスは操作を一切実行しません。
- **DELAY**：転送パスが正常に機能していることを示す最後の肯定確認を受信してから、ReachableTime ミリ秒を超える時間が経過しました。パケットは、直近の DELAY_FIRST_PROBE_TIME 秒以内に送信されました。**DELAY** 状態に入ってから DELAY_FIRST_PROBE_TIME 秒以内に到達可能性確認が受信できない場合は、ネイバー送信要求メッセージが送信され、状態が **PROBE** に変更されます。
- **PROBE**：到達可能性確認が受信されるまで、RetransTime ミリ秒ごとにネイバー送信要求メッセージを再送信して、到達可能性確認を要求し続けます。
- **????**：不明な状態。

次に、IPv6 近隣探索キャッシュのスタティック エントリについて表示される可能性のある状態を示します。

- **INCMP**：（不完全）このエントリのインターフェイスはダウンしています。
- **REACH**：（到達可能）このエントリのインターフェイスは動作しています。

- Interface

  アドレスに到達可能であったインターフェイス。

例

次に、インターフェイスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
hostname# show ipv6 neighbor inside
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
FE80::203:A0FF:FED6:141E                    0 0003.a0d6.141e  REACH inside
3001:1::45a                                 - 0002.7d1a.9472  REACH inside
```

次に、IPv6 アドレスを指定して入力した **show ipv6 neighbor** コマンドの出力例を示します。

```
hostname# show ipv6 neighbor 2000:0:0:4::2
IPv6 Address                              Age Link-layer Addr State Interface
2000:0:0:4::2                               0 0003.a0d6.141e  REACH inside
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	IPv6 近隣探索キャッシュのすべてのエントリを、スタティック エントリを除いて削除します。
ipv6 neighbor	IPv6 近隣探索キャッシュ内にスタティック エントリを設定します。

show ipv6 route

IPv6 ルーティング テーブルの内容を表示するには、特権 EXEC モードで **show ipv6 route** コマンドを使用します。

show ipv6 route

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show ipv6 route コマンドは、情報が IPv6 固有のものであることを除けば、**show route** コマンドと同様の出力を提供します。

次に、IPv6 ルーティング テーブルに表示される情報を示します。

- **Codes**：ルートを生成したプロトコルを示します。表示される値は次のとおりです。
  - **C**：接続済み
  - **L**：ローカル
  - **S**：スタティック
  - **R**：RIP 生成
  - **B**：BGP 生成
  - **I1**：ISIS L1：統合 IS-IS Level 1 生成
  - **I2**：ISIS L2：統合 IS-IS Level 2 生成
  - **IA**：ISIS エリア間：統合 IS-IS エリア間生成
- **fe80::/10**：リモート ネットワークの IPv6 プレフィックスを示します。
- **[0/0]**：カッコ内の最初の数値は、情報ソースの管理ディスタンスです。2 番目の数値はルートのメトリックです。
- **via ::**：リモート ネットワークに到達するための次のルータのアドレスを示します。
- **inside**：示されているネットワークへの次のルータに到達できるインターフェイスを示します。

例

次に、**show ipv6 route** コマンドの出力例を示します。

```
hostname# show ipv6 route

IPv6 Routing Table - 7 entries
Codes: C - Connected, L - Local, S - Static, R - RIP, B - BGP
       U - Per-user Static route
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea
       O - OSPF intra, OI - OSPF inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
L   fe80::/10 [0/0]
     via ::, inside
     via ::, vlan101
L   fec0::a:0:0:a0a:a70/128 [0/0]
     via ::, inside
C   fec0:0:0:a::/64 [0/0]
     via ::, inside
L   fec0::65:0:0:a0a:6570/128 [0/0]
     via ::, vlan101
C   fec0:0:0:65::/64 [0/0]
     via ::, vlan101
L   ff00::/8 [0/0]
     via ::, inside
     via ::, vlan101
S   ::/0 [0/0]
     via fec0::65:0:0:a0a:6575, vlan101
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 のルーティング テーブル アップデートおよびルート キャッシュ アップデートに関するデバッグ情報を表示します。
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 routers

オンリンク ルータから受信した IPv6 ルータ アドバタイズメント情報を表示するには、特権 EXEC モードで **show ipv6 routers** コマンドを使用します。

show ipv6 routers [*if_name*]

シンタックスの説明

if_name	（オプション）情報を表示する対象となる、**nameif** コマンドによって指定される内部インターフェイス名または外部インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス名を指定しない場合は、すべての IPv6 インターフェイスに関する情報が表示されます。インターフェイス名を指定すると、指定したインターフェイスに関する情報が表示されます。

例

次に、インターフェイス名を指定せずに入力した **show ipv6 routers** コマンドの出力例を示します。

```
hostname# show ipv6 routers
Router FE80::83B3:60A4 on outside, last update 3 min
  Hops 0, Lifetime 6000 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
  Prefix 3FFE:C00:8007::800:207C:4E37/96 autoconfig
    Valid lifetime -1, preferred lifetime -1
Router FE80::290:27FF:FE8C:B709 on inside, last update 0 min
  Hops 64, Lifetime 1800 sec, AddrFlag=0, OtherFlag=0
  Reachable time 0 msec, Retransmit time 0 msec
```

関連コマンド

コマンド	説明
ipv6 route	IPv6 ルーティング テーブルにスタティック エントリを追加します。

show ipv6 traffic

IPv6 トラフィックに関する統計情報を表示するには、特権 EXEC モードで **show ipv6 traffic** コマンドを使用します。

show ipv6 traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

トラフィック カウンタを消去するには、**clear ipv6 traffic** コマンドを使用します。

例

次に、**show ipv6 traffic** コマンドの出力例を示します。

```
hostname# show ipv6 traffic
IPv6 statistics:
  Rcvd:  545 total, 545 local destination
         0 source-routed, 0 truncated
         0 format errors, 0 hop count exceeded
         0 bad header, 0 unknown option, 0 bad source
         0 unknown protocol, 0 not a router
         218 fragments, 109 total reassembled
         0 reassembly timeouts, 0 reassembly failures
  Sent:  228 generated, 0 forwarded
         1 fragmented into 2 fragments, 0 failed
         0 encapsulation failed, 0 no route, 0 too big
  Mcast: 168 received, 70 sent

ICMP statistics:
  Rcvd: 116 input, 0 checksum errors, 0 too short
        0 unknown info type, 0 unknown error type
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 60 router advert, 0 redirects
        31 neighbor solicit, 25 neighbor advert
  Sent: 85 output, 0 rate-limited
        unreach: 0 routing, 0 admin, 0 neighbor, 0 address, 0 port
        parameter: 0 error, 0 header, 0 option
        0 hopcount expired, 0 reassembly timeout,0 too big
        0 echo request, 0 echo reply
        0 group query, 0 group report, 0 group reduce
        0 router solicit, 18 router advert, 0 redirects
        33 neighbor solicit, 34 neighbor advert

UDP statistics:
  Rcvd: 109 input, 0 checksum errors, 0 length errors
        0 no port, 0 dropped
  Sent: 37 output

TCP statistics:
  Rcvd: 85 input, 0 checksum errors
  Sent: 103 output, 0 retransmitted
```

関連コマンド

コマンド	説明
clear ipv6 traffic	IPv6 トラフィック カウンタを消去します。

CHAPTER 27

show isakmp ipsec-over-tcp stats コマンド～ show route コマンド

show isakmp ipsec-over-tcp stats

IPsec over TCP の実行時の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp ipsec-over tcp stats** コマンドを使用します。

show isakmp ipsec-over-tcp stats

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp ipsec-over-tcp stats** コマンドが導入されました。
7.2(1)	**show isakmp ipsec-over-tcp stats** コマンドが廃止されました。**show crypto isakmp ipsec-over-tcp stats** コマンドに置き換えられました。

使用上のガイドライン　このコマンドの出力には、次のフィールドが含まれています。

- Embryonic connections
- Active connections
- Previous connections
- Inbound packets
- Inbound dropped packets
- Outbound packets
- Outbound dropped packets
- RST packets
- Received ACK heart-beat packets
- Bad headers
- Bad trailers
- Timer failures
- Checksum errors
- Internal errors

例　グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP 統計情報を表示しています。

```
hostname(config)# show isakmp ipsec-over-tcp stats
Global IPSec over TCP Statistics
-------------------------------
Embryonic connections: 2
Active connections: 132
Previous connections: 146
Inbound packets: 6000
Inbound dropped packets: 30
Outbound packets: 0
Outbound dropped packets: 0
RST packets: 260
Received ACK heart-beat packets: 10
Bad headers: 0
Bad trailers: 0
Timer failures: 0
Checksum errors: 0
Internal errors: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config crypto isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp sa

IKE ランタイム SA データベースを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp sa** コマンドを使用します。

show isakmp sa [**detail**]

シンタックスの説明

detail	SA データベースに関する詳細な出力を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp sa** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp sa** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

detail オプションを指定しない場合：

表 27-1

IKE Peer	Type	Dir	Rky	State
209.165.200.225	L2L	Init	No	MM_Active

detail オプションを指定した場合：

表 27-2

IKE Peer	Type	Dir	Rky	State	Encrypt	Hash	Auth	Lifetime
209.165.200.225	L2L	Init	No	MM_Active	3des	md5	preshrd	86400

例

グローバル コンフィギュレーション モードで入力した次の例では、SA データベースに関する詳細な情報を表示しています。

```
hostname(config)# show isakmp sa detail
hostname(config)# sho isakmp sa detail

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
1 209.165.200.225 User  Resp  No   AM_Active  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
2 209.165.200.226 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
3 209.165.200.227 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

IKE Peer  Type  Dir   Rky  State      Encrypt Hash  Auth    Lifetime
4 209.165.200.228 User  Resp  No   AM_ACTIVE  3des    SHA   preshrd 86400

hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show isakmp stats

実行時の統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show isakmp stats** コマンドを使用します。

show isakmp stats

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show isakmp stats** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**show crypto isakmp stats** コマンドに置き換えられました。

使用上のガイドライン

このコマンドの出力には、次のフィールドが含まれています。

- Global IKE Statistics
- Active Tunnels
- In Octets
- In Packets
- In Drop Packets
- In Notifys
- In P2 Exchanges
- In P2 Exchange Invalids
- In P2 Exchange Rejects
- In P2 Sa Delete Requests
- Out Octets
- Out Packets
- Out Drop Packets
- Out Notifys
- Out P2 Exchanges
- Out P2 Exchange Invalids
- Out P2 Exchange Rejects

- Out P2 Sa Delete Requests
- Initiator Tunnels
- Initiator Fails
- Responder Fails
- System Capacity Fails
- Auth Fails
- Decrypt Fails
- Hash Valid Fails
- No Sa Fails

例

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP 統計情報を表示しています。

```
hostname(config)# show isakmp stats
Global IKE Statistics
Active Tunnels: 132
Previous Tunnels: 132
In Octets: 195471
In Packets: 1854
In Drop Packets: 925
In Notifys: 0
In P2 Exchanges: 132
In P2 Exchange Invalids: 0
In P2 Exchange Rejects: 0
In P2 Sa Delete Requests: 0
Out Octets: 119029
Out Packets: 796
Out Drop Packets: 0
Out Notifys: 264
Out P2 Exchanges: 0
Out P2 Exchange Invalids: 0
Out P2 Exchange Rejects: 0
Out P2 Sa Delete Requests: 0
Initiator Tunnels: 0
Initiator Fails: 0
Responder Fails: 0
System Capacity Fails: 0
Auth Fails: 0
Decrypt Fails: 0
Hash Valid Fails: 0
No Sa Fails: 0
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show running-config isakmp	アクティブな ISAKMP コンフィギュレーションをすべて表示します。

show local-host

ローカル ホストのネットワーク状態を表示するには、特権 EXEC モードで **show local-host** コマンドを使用します。

show local-host [*ip_address*] [**detail**] [**all**]

シンタックスの説明

all	（オプション）セキュリティ アプライアンスに接続するローカル ホストとセキュリティ アプライアンスから接続するローカル ホストを含みます。
detail	（オプション）アクティブな xlate とネットワーク接続の情報を含む、ローカル ホストの詳細なネットワーク状態情報を表示します。
ip_address	（オプション）ローカル ホストの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	ホスト制限があるモデルの場合、このコマンドにより外部インターフェイスと見なされるインターフェイスが表示されるようになりました。

使用上のガイドライン

show local-host コマンドを使用すると、ローカル ホストのネットワーク状態を表示できます。ローカル ホストは、トラフィックをセキュリティ アプライアンスに転送するか、セキュリティ アプライアンスを通じて転送するすべてのホストに対して作成されます。

このコマンドを使用すると、ローカル ホストの変換スロットと接続スロットを表示できます。また、標準の変換状態および接続状態が適用されない場合、**nat 0** ***access-list*** コマンドで設定されたホストの情報を提供します。

このコマンドは、接続制限値も表示します。接続制限を設定していない場合、この値には 0 が表示され、制限は適用されません。

ホスト制限があるモデルの場合、ルーテッド モードで、内部のホスト（ワーク ゾーンとホーム ゾーン）は、外部（インターネット ゾーン）と通信するときのみ制限されます。インターネット ホストは制限されません。ワークとホーム間のトラフィックを開始するホストも制限されません。デフォルト ルートに関連付けられているインターフェイスは、インターネット インターフェイスと見なされます。デフォルト ルートがない場合、すべてのインターフェイスのホストは制限されます。透過モードでは、ホストの数が最も少ないインターフェイスは、ホスト制限の対象です。

TCP 代行受信を設定した場合は、SYN 攻撃が発生すると、代行受信された接続の数が **show local-host** コマンドの出力の使用状況カウントに含まれます。このフィールドには、通常は完全にオープンな接続のみが表示されます。

show local-host コマンドの出力で TCP embryonic count to host counter が使用されるのは、スタティック接続を使用するホストに対して最大初期接続数の制限（TCP 代行受信の水準点）を設定した場合です。このカウンタは、他のホストからこのホストに向かう初期接続の合計数を示しています。この合計数が設定済みの制限値を超えると、このホストに向かう新しい接続に TCP 代行受信が適用されます。

例

次の出力例は、**show local-host** コマンドによって表示されます。

```
hostname# show local-host
Interface inside: 0 active, 0 maximum active, 0 denied
Interface outside: 1 active, 2 maximum active, 0 denied
```

次の出力例は、ホスト制限のあるセキュリティ アプライアンス上で **show local-host** コマンドを実行すると表示されます。

```
hostname# show local-host
Detected interface 'outside' as the Internet interface. Host limit applies to all
other interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface inside: 1 active, 1 maximum active, 0 denied
Interface outside: 0 active, 0 maximum active, 0 denied
```

次の出力例は、ホスト制限のあるセキュリティ アプライアンス上で **show local-host** コマンドを実行すると表示されますが、デフォルト ルートがない場合、ホスト制限がすべてのインターフェイスに適用されます。デフォルト ルート、またはデフォルト ルートが使用しているインターフェイスがダウンしている場合、デフォルトのルート インターフェイスが検出されないことがあります。

```
hostname# show local-host
Unable to determine Internet interface from default route. Host limit applied to all
interfaces.

Current host count: 3, towards licensed host limit of: 50

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

次の出力例は、無制限ホストがあるセキュリティ アプライアンス上で **show local-host** コマンドを実行すると表示されます。

```
hostname# show local-host
Licensed host limit: Unlimited

Interface c1in: 1 active, 1 maximum active, 0 denied
Interface c1out: 0 active, 0 maximum active, 0 denied
```

次の例は、ローカル ホストのネットワーク状態を表示する方法を示しています。

```
hostname# show local-host all
Interface outside: 1 active, 2 maximum active, 0 denied
local host: <11.0.0.4>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
Interface inside: 1 active, 2 maximum active, 0 denied
local host: <17.3.8.2>,
```

```
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
Interface NP Identity Ifc: 2 active, 4 maximum active, 0 denied
local host: <11.0.0.3>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:44 bytes 4464
105 out 11.0.0.4 in 11.0.0.3 idle 0:01:42 bytes 4464
local host: <17.3.8.1>,
TCP flow count/limit = 0/unlimited
TCP embryonic count to host = 0
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited
Conn:
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:44 bytes 4464
105 out 17.3.8.2 in 17.3.8.1 idle 0:01:42 bytes 4464

hostname# show local-host 10.1.1.91
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
PAT Global 192.150.49.1(1024) Local 10.1.1.91(4984)

Conn:
TCP out 192.150.49.10:21 in 10.1.1.91:4984 idle 0:00:07 bytes 75 flags UI Interface
outside: 1 active, 1 maximum active, 0 denied

hostname# show local-host 10.1.1.91 detail
Interface third: 0 active, 0 maximum active, 0 denied
Interface inside: 1 active, 1 maximum active, 0 denied
local host: <10.1.1.91>,
TCP flow count/limit = 1/unlimited
TCP embryonic count to (from) host = 0 (0)
TCP intercept watermark = unlimited
UDP flow count/limit = 0/unlimited

Xlate:
TCP PAT from inside:10.1.1.91/4984 to outside:192.150.49.1/1024 flags ri

Conn:
TCP outside:192.150.49.10/21 inside:10.1.1.91/4984 flags UI Interface outside: 1
active, 1 maximum active, 0 denied
```

関連コマンド

コマンド	説明
clear local-host	***show local-host*** コマンドで表示された、ローカル ホストからのネットワーク接続を解放します。
nat	ネットワークをグローバル IP アドレス プールに関連付けます。

show logging

バッファに保持されているログ、またはその他のロギング設定を表示するには、**show logging** コマンドを使用します。

show logging [**message** [*syslog_id* | **all**] | **asdm** | ***queue*** | ***setting***]

シンタックスの説明

message	（オプション）デフォルト以外のレベルのメッセージを表示します。メッセージ レベルを設定するには、**logging message** コマンドを参照してください。
syslog_id	（オプション）表示するメッセージ番号を指定します。
all	（オプション）イネーブルまたはディセーブルのどちらになっているかを含めて、すべてのシステム ログ メッセージ ID を表示します。
setting	（オプション）ロギング設定を表示します。ロギング バッファは表示しません。
asdm	（オプション）ASDM ロギング バッファの内容を表示します。
queue	（オプション）システム ログ メッセージ キューを表示します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

logging buffered コマンドを使用している場合は、キーワードを指定せずに **show logging** コマンドを実行すると、現在のメッセージ バッファと設定が表示されます。

show logging queue コマンドを使用すると、次の情報を表示できます。

- キュー内のメッセージ数
- キューに記録されたメッセージの最大数
- 処理に利用できるブロック メモリがなかったために廃棄されたメッセージ数

例

次に、**show logging** コマンドの出力例を示します。

```
hostname(config)# show logging
Syslog logging: enabled
    Timestamp logging: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: level debugging, 37 messages logged
    Trap logging: disabled
305001: Portmapped translation built for gaddr 209.165.201.5/0 laddr 192.168.1.2/256
...
```

次に、**show logging message all** コマンドの出力例を示します。

```
hostname(config)# show logging message all

syslog 111111: default-level alerts (enabled)
syslog 101001: default-level alerts (enabled)
syslog 101002: default-level alerts (enabled)
syslog 101003: default-level alerts (enabled)
syslog 101004: default-level alerts (enabled)
syslog 101005: default-level alerts (enabled)
syslog 102001: default-level alerts (enabled)
syslog 103001: default-level alerts (enabled)
syslog 103002: default-level alerts (enabled)
syslog 103003: default-level alerts (enabled)
syslog 103004: default-level alerts (enabled)
syslog 103005: default-level alerts (enabled)
syslog 103011: default-level alerts (enabled)
syslog 103012: default-level informational (enabled)
```

関連コマンド

コマンド	説明
logging asdm	ASDM へのロギングをイネーブルにします。
logging buffered	バッファへのロギングをイネーブルにします。
logging message	メッセージ レベルを設定します。または、メッセージをディセーブルにします。
logging queue	ロギング キューを設定します。

show logging rate-limit

禁止されたメッセージを元の設定で表示するには、**show logging rate-limit** コマンドを使用します。

show logging rate-limit

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。

使用上のガイドライン

情報が消去されると、ホストが接続を再び確立するまで、何も表示されません。

例

次の例は、禁止されたメッセージを表示する方法を示しています。

```
hostname(config)# show logging rate-limit
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。

show mac-address-table

MAC アドレス テーブルを表示するには、特権 EXEC モードで **show mac-address-table** コマンドを使用します。

show mac-address-table [*interface_name* | **count** | **static**]

シンタックスの説明

count	（オプション）ダイナミック エントリとスタティック エントリの総数を表示します。
interface_name	（オプション）MAC アドレス テーブル エントリを表示するインターフェイス名を指定します。
static	（オプション）スタティック エントリのみ表示します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスの MAC アドレス エントリが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table
interface          mac address       type      Time Left
-----------------------------------------------------------------------
outside            0009.7cbe.2100    static      -
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

次に、inside というインターフェイスに関する **show mac-address-table** コマンドの出力例を示します。

```
hostname# show mac-address-table inside
interface          mac address       type      Time Left
-----------------------------------------------------------------------
inside             0010.7cbe.6101    static      -
inside             0009.7cbe.5101    dynamic     10
```

次に、**show mac-address-table count** コマンドの出力例を示します。

```
hostname# show mac-address-table count
Static     mac-address bridges (curr/max): 0/65535
Dynamic    mac-address bridges (curr/max): 103/65535
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。

show management-access

管理アクセス用に設定されている内部インターフェイスの名前を表示するには、特権 EXEC モードで show management-access コマンドを使用します。

show management-access

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます（インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 “ ” に囲まれて表示されます）。

例

次の例は、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定し、結果を表示する方法を示しています。

```
hostname(config)# management-access inside
hostname(config)# show management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
management-access	管理アクセス用の内部インターフェイスを設定します。

show memory

物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示するには、特権 EXEC モードで **show memory** コマンドを使用します。

show memory [**detail**]

シンタックスの説明

detail	（オプション）空きシステム メモリと割り当て済みシステム メモリの詳細を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show memory コマンドを使用すると、オペレーティング システムで使用できる最大物理メモリと現在の空きメモリの要約を表示することができます。メモリは、必要に応じて割り当てられます。

show memory detail コマンドの出力を **show memory binsize** コマンドで利用すると、メモリ リークをデバッグすることができます。

また、SNMP を使用して **show memory** コマンドからの情報を表示することもできます。

例

次の例は、使用できる最大物理メモリと現在の空きメモリの要約を表示する方法を示しています。

```
hostname# show memory
Free memory:       845044716 bytes (79%)
Used memory:       228697108 bytes (21%)
-------------     ----------------
Total memory:     1073741824 bytes (100%)
```

次の例は、メモリに関する詳細な出力を示しています。

```
hostname# show memory detail
Free memory: 15958088 bytes (24%)
Used memory:
Allocated memory in use: 29680332 bytes (44%)
Reserved memory: 21470444 bytes (32%)
---------------------------- ----------------
Total memory: 67108864 bytes (100%)

Least free memory: 4551716 bytes ( 7%)
Most used memory: 62557148 bytes (93%)

----- fragmented memory statistics -----
```

```
fragment size count total
(bytes) (bytes)
---------------- ---------- --------------
16 8 128
24 4 96
32 2 64
40 5 200
64 3 192
88 1 88
168 1 168
224 1 224
256 1 256
296 2 592
392 1 392
400 1 400
1816 1 1816*
4435968 1 4435968**
11517504 1 11517504

* - top most releasable chunk.
** - contiguous memory on top of heap.


----- allocated memory statistics -----

fragment size count total
(bytes) (bytes)
---------------- ---------- --------------
40 50 2000
48 144 6912
56 24957 1397592
64 101 6464
72 99 7128
80 1032 82560
88 18 1584
96 64 6144
104 57 5928
112 6 672
120 112 13440
128 15 1920
136 87 11832
144 22 3168
152 31 4712
160 90 14400
168 65 10920
176 74 13024
184 11 2024
192 8 1536
200 1 200
< 以下省略 >
```

関連コマンド

コマンド	説明
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。

show memory binsize

特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示するには、特権 EXEC モードで ***show memory binsize*** コマンドを使用します。

show memory binsize *size*

シンタックスの説明

size	（オプション）特定のバイナリ サイズのチャンク（メモリ ブロック）を表示します。バイナリ サイズは、***show memory detail*** コマンドの出力の「fragment size」カラムに示されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

次の例では、バイナリ サイズ 500 が割り当てられているチャンクに関する要約情報を表示しています。

```
hostname# show memory binsize 500
pc = 0x00b33657, size = 460      , count = 1
```

関連コマンド

コマンド	説明
show memory-caller address	セキュリティ アプライアンス上に設定されているアドレスの範囲を表示します。
show memory profile	セキュリティ アプライアンスのメモリ使用状況に関する情報（プロファイリング）を表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。

show memory delayed-free-poisoner

memory delayed-free-poisoner キューの使用状況の要約を表示するには、特権 EXEC モードで **show memory delayed-free-poisoner** コマンドを使用します。

show memory delayed-free-poisoner

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

キューおよび統計情報を消去するには、**clear memory delayed-free-poisoner** コマンドを使用します。

例

次に、**show memory delayed-free-poisoner** コマンドの出力例を示します。

```
hostname# show memory delayed-free-poisoner
delayed-free-poisoner statistics:
         3335600:  memory held in queue
            6095:  current queue count
               0:  elements dequeued
               3:  frees ignored by size
            1530:  frees ignored by locking
              27:  successful validate runs
               0:  aborted validate runs
        01:09:36:  local time of last validate
```

表 27-3 に、**show memory delayed-free-poisoner** コマンド出力において重要なフィールドの説明を示します。

表 27-3　show memory delayed-free-poisoner コマンド出力の説明

フィールド	説明
memory held in queue	delayed free-memory poisoner ツールのキューに保持されるメモリ。通常このようなメモリは、delayed free-memory poisoner ツールがイネーブルになっていない場合、**show memory** 出力では「空き」容量になります。
current queue count	キュー内の要素の数。

表 27-3　show memory delayed-free-poisoner コマンド出力の説明（続き）

フィールド	説明
elements dequeued	キューから削除された要素の数。この数が増加し始めるのは、最終的にシステム内の他の空きメモリの大部分またはすべてがキューに保持されることになった場合です。
frees ignored by size	要求が小さ過ぎて必要なトラッキング情報を保持できなかったため、キューに配置されなかった解放要求の数。
frees ignored by locking	複数のアプリケーションがメモリを使用しているため、キューに配置されずに、ツールによって代行受信された解放要求の数。最後にメモリを解放してシステムに戻したアプリケーションが、このメモリ領域をキューに割り当てます。
successful validate runs	**clear memory delayed-free-poisoner** コマンドを使用して、モニタリングがイネーブルにされた後、または消去された後で、キュー コンテンツが（自動的に、または **memory delayed-free-poisoner validate** コマンドによって）検証された回数。
aborted validate runs	**clear memory delayed-free-poisoner** コマンドを使用して、モニタリングがイネーブルにされた後、または消去された後で、複数のタスク（定期的な実行または CLI からの検証要求）が同時にキューを使用しようとしたため、キュー コンテンツをチェックする要求が中止された回数。
local time of last validate	最後の検証の実行が完了したときのローカル システムの時刻。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報を消去します。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内の要素を検証します。

show memory profile

セキュリティ アプライアンスのメモリ使用状況（プロファイリング）に関する情報を表示するには、特権 EXEC モードで ***show memory profile*** コマンドを使用します。

show memory profile [peak] [detail | collated | status]

シンタックスの説明

collated	（オプション）表示されるメモリ情報を整形します。
detail	（オプション）メモリの詳細情報を表示します。
peak	（オプション）「使用中の」バッファではなく、ピーク キャプチャ バッファを表示します。
status	（オプション）メモリ プロファイリングの現在の状態とピーク キャプチャ バッファを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show memory profile コマンドは、メモリ使用状況レベルとメモリ リークをトラブルシューティングするために使用します。プロファイル バッファの内容は、プロファイリングを停止した場合でもまだ参照できます。プロファイリングを開始すると、バッファは自動的に消去されます。

（注） メモリのプロファイリングをイネーブルにすると、セキュリティ　アプライアンスのパフォーマンスが一時的に低下することがあります。

例

次のように表示されます。

```
hostname# show memory profile
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 0
```

次に示す **show memory profile detail** コマンドの出力は、6 つのデータ カラムと 1 つのヘッダー カラムに区分され、左揃えで表示されています。ヘッダー カラムには、先頭のデータ カラムのメモリ バケットのアドレスが表示されます（16 進値）。データ自体は、バケット アドレスにあるテキストまたはコードが保持しているバイト数です。データ カラム内のピリオド（.）は、このバケットのテキストによってメモリが保持されていないことを意味します。行内の他のカラムは、前のカラムから増分値に従って増分したバケット アドレスを表しています。たとえば、最初の行の先頭の

データ カラムのアドレス バケットは 0x001069e0 です。最初の行の 2 番目のデータ カラムのアドレス バケットは 0x001069e4 で、以降も同様に増分していきます。通常は、ヘッダー カラムにあるアドレスが次のバケット アドレスです。これは、前の行の最後のデータ カラムのアドレスに増分値を加算したものです。使用状況を含んでいない行は、一切表示されません。このような非表示になる行が、複数連続していることもあります。この場合は、ヘッダー カラムに 3 個のピリオド（...）で示されます。

```
hostname# show memory profile detail
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
...
0x001069e0 . 24462 . . . .
...
0x00106d88 . 1865870 . . . .
...
0x0010adf0 . 7788 . . . .
...
0x00113640 . . . . 433152 .
...
0x00116790 2480 . . . . .
< 省略 >
```

次に、整形された出力の例を示します。

```
hostname# show memory profile collated
Range: start = 0x00100020, end = 0x00e006e0, increment = 00000004
Total = 48941152
24462 0x001069e4
1865870 0x00106d8c
7788 0x0010adf4
433152 0x00113650
2480 0x00116790
< 省略 >
```

次の例では、ピーク キャプチャ バッファを表示しています。

```
hostname# show memory profile peak
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
```

次の例では、ピーク キャプチャ バッファ、および当該バケット アドレスにあるテキストまたはコードが保持しているバイト数を表示しています。

```
hostname# show memory profile peak detail
Range: start = 0x004018b4, end = 0x004169d0, increment = 00000004
Total = 102400
...
0x00404c8c . . 102400 . . .
```

次の例では、メモリ プロファイリングの現在の状態とピーク キャプチャ バッファを表示しています。

```
hostname# show memory profile status
InUse profiling: ON
Peak profiling: OFF
Memory used by profile buffers: 11518860 bytes
Profile:
0x00100020-0x00bfc3a8(00000004)
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況のモニタリング（メモリ プロファイリング）をイネーブルにします。
memory profile text	プロファイルするメモリのプログラム テキスト範囲を設定します。
clear memory profile	メモリ プロファイリング機能が保持しているメモリ バッファを消去します。

show memory webvpn

webvpn メモリ使用状況の統計情報を生成するには、特権 EXEC モードで **show memory webvpn** コマンドを使用します。

show memory webvpn [allobjects | blocks | dumpstate [cache | disk0 | disk1 | flash | ftp | system | tftp]| pools | profile [clear | dump | start | stop] | usedobjects {{begin | exclude | grep | include} line *line***}]**

シンタックスの説明

allobjects	プール、ブロック、使用中オブジェクトおよび解放済みオブジェクトに対する webvpn メモリ使用量の詳細を表示します。
begin	一致する行から開始します。
blocks	メモリ ブロックに対する webvpn メモリ使用量の詳細を表示します。
cache	webvpn メモリ キャッシュ状態のダンプ ファイル名を指定します。
clear	webvpn メモリ プロファイルを消去します。
disk0	webvpn メモリの disk0 状態のダンプ ファイル名を指定します。
disk1	webvpn メモリの disk1 状態のダンプ ファイル名を指定します。
dump	webvpn メモリ プロファイルをファイルに書き込みます。
dumpstate	webvpn メモリ状態をファイルに書き込みます。
exclude	一致する行を除外します。
flash	webvpn メモリ フラッシュ状態のダンプ ファイル名を指定します。
ftp	webvpn メモリ ftp 状態のダンプ ファイル名を指定します。
grep	一致する行を含めるか、または除外します。
include	一致する行を含めます。
line	一致する行を識別します。
line	一致する行を指定します。
pools	メモリ プールに対する webvpn メモリ使用量の詳細を表示します。
profile	webvpn メモリ プロファイルを収集してファイルに書き込みます。
system	webvpn メモリ システム状態のダンプ ファイル名を指定します。
start	webvpn メモリ プロファイルの収集を開始します。
stop	webvpn メモリ プロファイルの収集を停止します。
tftp	webvpn メモリ tftp 状態のダンプ ファイル名を指定します。
usedobjects	使用中のオブジェクトに対する webvpn メモリ使用量の詳細を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、**show memory webvpn allobjects** コマンドの出力例を示します。

```
hostname# show memory webvpn allobjects
Arena 0x36b14f8 of 4094744 bytes (61 blocks of size 66048), maximum 134195200
130100456 free bytes (97%; 1969 blocks, zone 0)
Arena is dynamically allocated, not contiguous
Features: GroupMgmt: SET, MemDebugLog: unset
Pool 0xd719a78 ("cp_entries" => "pool for class cpool entries") (next 0xd6d91d8)
Size: 66040 (1% of current, 0% of limit)
Object frame size: 32
Load related limits: 70/50/30
Callbacks: !init/!prep/!f2ca/!dstr/!dump
Blocks in use:
Block 0xd719ac0..0xd729cb8 (size 66040), pool "cp_entries"
Watermarks { 0xd7098f8 <= 0xd70bb60 <= 0xd719a60 } = 57088 ready
Block size 66040 not equal to arena block 66048 (realigned-to-8)
Used objects: 0
Top allocated count: 275
Objects dump:
0. Object 0xd70bb50: FREED (by "jvclass_pool_free")
```

関連コマンド

コマンド	説明
memory-size	WebVPN サービスが使用できるセキュリティ アプライアンス上のメモリ量を設定します。

show memory-caller address

セキュリティ アプライアンス上に設定されているアドレス範囲を表示するには、特権 EXEC モードで ***show memory-caller address*** コマンドを使用します。

show memory-caller address

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show memory-caller address コマンドを使用してアドレス範囲を表示するには、***memory caller-address*** コマンドを使用して、アドレス範囲をあらかじめ設定しておく必要があります。

例

次の例は、***memory caller-address*** コマンドで設定したアドレス範囲、および ***show memory-caller address*** コマンドによる表示結果を示しています。

```
hostname# memory caller-address 0x00109d5c 0x00109e08
hostname# memory caller-address 0x009b0ef0 0x009b0f14
hostname# memory caller-address 0x00cf211c 0x00cf4464

hostname# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

アドレス範囲を設定する前に ***show memory-caller addresss*** コマンドを入力した場合、アドレスは表示されません。

```
hostname# show memory-caller address
Move down stack frame for the addresses:
```

関連コマンド

コマンド	説明
memory caller-address	呼び出し側 PC のメモリ ブロックを設定します。

show mfib

転送する側のエントリおよびインターフェイスに関する MFIB を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib** コマンドを使用します。

show mfib [*group* [*source*]] [***verbose***]

シンタックスの説明

group	（オプション）マルチキャスト グループの IP アドレス。
source	（オプション）マルチキャスト ルート送信元の IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。
verbose	（オプション）エントリの詳細な情報を表示します。

デフォルト

オプションの引数を指定しない場合は、すべてのグループの情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib** コマンドの出力例を示します。

```
hostname# show mfib 224.0.2.39
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib verbose	転送する側のエントリおよびインターフェイスに関する詳細な情報を表示します。

show mfib active

アクティブなマルチキャスト送信元を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib active** コマンドを使用します。

show mfib [*group*] **active** [*kbps*]

シンタックスの説明

group	（オプション）マルチキャスト グループの IP アドレス。
kbps	（オプション）この値以上のレートで送信されているマルチキャスト ストリームのみを表示します。

このコマンドには、引数もキーワードもありません。

デフォルト

kbps のデフォルト値は 4 です。*group* を指定しない場合は、すべてのグループが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show mfib active コマンドの出力では、PPS のレートに正または負の数値が表示されます。セキュリティ アプライアンスが負の数値を表示するのは、RPF パケットが失敗した場合か、ルータが発信インターフェイス（OIF）リストを使用して RPF パケットを監視している場合です。このような現象が発生している場合は、マルチキャスト ルーティングに問題がある可能性があります。

例

次に、**show mfib active** コマンドの出力例を示します。

```
hostname# show mfib active
Active IP Multicast Sources - sending >= 4 kbps

Group: 224.2.127.254, (sdr.cisco.com)
   Source: 192.168.28.69 (mbone.ipd.anl.gov)
     Rate: 1 pps/4 kbps(1sec), 4 kbps(last 1 secs), 4 kbps(life avg)

Group: 224.2.201.241, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 9 pps/93 kbps(1sec), 145 kbps(last 20 secs), 85 kbps(life avg)

Group: 224.2.207.215, ACM 97
   Source: 192.168.52.160 (webcast3-e1.acm97.interop.net)
     Rate: 3 pps/31 kbps(1sec), 63 kbps(last 19 secs), 65 kbps(life avg)
```

関連コマンド

コマンド	説明
show mroute active	アクティブなマルチキャスト ストリームを表示します。

show mfib count

MFIB ルートおよびパケットの数に関するデータを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib count** コマンドを使用します。

show mfib [*group* [*source*]] **count**

シンタックスの説明

group	（オプション）マルチキャスト グループの IP アドレス。
source	（オプション）マルチキャスト ルート送信元の IP アドレス。これは、4 分割ドット 10 進表記のユニキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、パケットのドロップに関する統計情報を表示します。

例

次に、**show mfib count** コマンドの出力例を示します。

```
hostname# show mfib count
MFIB global counters are :
* Packets [no input idb] : 0
* Packets [failed route lookup] : 0
* Packets [Failed idb lookup] : 0
* Packets [Mcast disabled on input I/F] : 0
```

関連コマンド

コマンド	説明
clear mfib counters	MFIB ルータ パケットのウンタを消去します。
show mroute count	マルチキャスト ルートのカウンタを表示します。

show mfib interface

MFIB プロセスに関係しているインターフェイスのパケット統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib interface** コマンドを使用します。

show mfib interface [*interface*]

シンタックスの説明

interface	（オプション）インターフェイス名を指定します。指定したインターフェイスに関する情報のみを表示します。

デフォルト

すべての MFIB インターフェイスに関する情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib interface** コマンドの出力例を示します。

```
hostname# show mfib interface
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
MFIB interface       status    CEF-based output
                               [configured,available]
           Ethernet0   up    [        no,       no]
           Ethernet1   up    [        no,       no]
           Ethernet2   up    [        no,       no]
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib reserved

予約済みグループを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib reserved** コマンドを使用します。

show mfib reserved [***count*** | ***verbose*** | ***active*** [*kpbs*]]

シンタックスの説明

count	（オプション）パケットおよびルートの数に関するデータを表示します。
verbose	（オプション）詳細な情報を表示します。
active	（オプション）アクティブなマルチキャスト送信元を表示します。
kpbs	（オプション）この値以上のレートで送信を実行している、アクティブなマルチキャスト送信元のみを表示します。

デフォルト

kbps のデフォルト値は 4 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、224.0.0.0 ～ 224.0.0.225 の範囲にある MFIB エントリを表示します。

例

次に、**show mfib reserved** コマンドの出力例を示します。

```
hostname# command example
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop Forwarding Counts: Pkt Count/Pkts per
second/Avg Pkt Size/Kbits per second Other counts: Total/RPF failed/Other drops
Interface Flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.0.0/4) Flags: C K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/24) Flags: K
   Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.1) Flags:
   Forwarding: 0/0/0/0, Other: 0/0/0
   outside Flags: IC
   dmz Flags: IC
   inside Flags: IC
```

関連コマンド

コマンド	説明
show mfib active	アクティブなマルチキャスト ストリームを表示します。

show mfib status

MFIB の全般的なコンフィギュレーションと動作ステータスを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib status** コマンドを使用します。

show mfib status

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例　次に、**show mfib status** コマンドの出力例を示します。

```
hostname# show mfib status
IP Multicast Forwarding (MFIB) status:
    Configuration Status: enabled
    Operational Status: running
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。

show mfib summary

MFIB のエントリおよびインターフェイスの数に関する要約情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib summary** コマンドを使用します。

show mfib summary

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib summary** コマンドの出力例を示します。

```
hostname# show mfib summary
IPv6 MFIB summary:

  54     total entries [1 (S,G), 7 (*,G), 46 (*,G/m)]

  17     total MFIB interfaces
```

関連コマンド

コマンド	説明
show mroute summary	マルチキャスト ルーティング テーブルの要約情報を表示します。

show mfib verbose

転送する側のエントリおよびインターフェイスに関する詳細情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mfib verbose** コマンドを使用します。

show mfib verbose

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mfib verbose** コマンドの出力例を示します。

```
hostname# show mfib verbose
Entry Flags: C - Directly Connected, S - Signal, IA - Inherit A flag,
             AR - Activity Required, D - Drop
Forwarding counts: Pkt Count/Pkts per second/Avg Pkt Size/Kbits per second
Other counts: Total/RPF failed/Other drops
Interface flags: A - Accept, F - Forward, NS - Negate Signalling
             IC - Internal Copy, NP - Not platform switched
             SP - Signal Present
Interface Counts: FS Pkt Count/PS Pkt Count
(*,224.0.1.39) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.1.40) Flags: S K
  Forwarding: 0/0/0/0, Other: 0/0/0
(*,224.0.0.0/8) Flags: K
  Forwarding: 0/0/0/0, Other: 0/0/0
```

関連コマンド

コマンド	説明
show mfib	転送する側のエントリおよびインターフェイスに関する MFIB 情報を表示します。
show mfib summary	MFIB のエントリおよびインターフェイスの数に関する要約情報を表示します。

show mgcp

MGCP のコンフィギュレーションとセッション情報を表示するには、特権 EXEC モードで **show mgcp** コマンドを使用します。

show mgcp {***commands*** | ***sessions***} [***detail***]

シンタックスの説明

コマンド	コマンド キューに含まれている MGCP コマンドの数を表示します。
sessions	既存の MGCP セッションの数を表示します。
detail	（オプション）各コマンド（またはセッション）に関する追加情報を出力に含めます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show mgcp commands コマンドは、コマンド キュー内の MGCP コマンド数を表示します。**show mgcp sessions** コマンドは、既存の MGCP セッション数を表示します。**detail** オプションは、各コマンド（またはセッション）に関する追加情報を出力に含めます。

例

次に、**show mgcp** コマンド オプションの例を示します。

```
hostname# show mgcp commands
1 in use, 1 most used, 200 maximum allowed
CRCX, gateway IP: host-pc-2, transaction ID: 2052, idle: 0:00:07
hostname#

hostname# show mgcp commands detail
1 in use, 1 most used, 200 maximum allowed
CRCX, idle: 0:00:10
        Gateway IP | host-pc-2
        Transaction ID  2052
        Endpoint name | aaln/1
        Call ID | 9876543210abcdef
        Connection ID |
        Media IP | 192.168.5.7
        Media port | 6058
hostname#

hostname# show mgcp sessions
1 in use, 1 most used
Gateway IP host-pc-2, connection ID 6789af54c9, active 0:00:11
hostname#

hostname# show mgcp sessions detail
1 in use, 1 most used
Session active 0:00:14
        Gateway IP | host-pc-2
        Call ID | 9876543210abcdef
        Connection ID | 6789af54c9
        Endpoint name | aaln/1
        Media lcl port  6166
        Media rmt IP | 192.168.5.7
        Media rmt port  6058
hostname#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug mgcp	MGCP デバッグ情報をイネーブルにします。
inspect mgcp	MGCP アプリケーション検査をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。

show mode

実行中のソフトウェア イメージおよびフラッシュ メモリに保持されている任意のイメージについて、セキュリティ コンテキスト モードを表示するには、特権 EXEC モードで **show mode** コマンドを使用します。

show mode

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show mode** コマンドの出力例を示します。ここでは、現在のモード、および実行されていないイメージ「image.bin」のモードを表示しています。

```
hostname# show mode flash:/image.bin
Firewall mode: multiple
```

モードは、マルチまたはシングルのいずれかです。

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。
mode	コンテキスト モードをシングルまたはマルチに設定します。

show module

ASA 5500 シリーズ適応型セキュリティ アプライアンス上の SSM に関する情報をシステム情報と共に表示するには、ユーザ EXEC モードで **show module** コマンドを使用します。

show module [all | *slot* [***details*** | ***recover***]]]

シンタックスの説明

all	（デフォルト）スロット 1 の SSM およびスロット 0 のシステムに関する情報を表示します。
details	（オプション）インテリジェント SSM（ASA-SSM-*x*0 など）のリモート管理コンフィギュレーションを含めて、詳細な情報を表示します。
recover	（オプション）インテリジェント SSM について、**hw-module module recover** コマンドの設定を表示します。 **(注)** ***recover*** キーワードが有効になるのは、**hw-module module recover** コマンドに ***configure*** キーワードを使用して SSM のリカバリ コンフィギュレーションを設定した場合のみです。
slot	（オプション）スロット番号（0 または 1）を指定します。スロット 0 は、セキュリティ アプライアンスの基本システムです。

デフォルト

両方のスロットの情報を表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト[1]	システム
ユーザ EXEC	•	•	•	•	•

1. **show module recover** コマンドを使用できるのは、システム実行スペース内のみです。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドは、より多くの詳細情報を出力するように変更されました。

使用上のガイドライン

このコマンドは、SSM に関する情報をシステムおよび組み込みインターフェイスの情報と共に表示します。

表示される出力については、次の「例」の項を参照してください。

例

次に、**show module** コマンドの出力例を示します。スロット 0 は基本システムで、スロット 1 は CSC SSM です。

```
hostname> show module
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P3000000034
  1 ASA 5500 Series Security Services Module-20  ASA-SSM-20         0

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.c30d to 000b.fcf8.c311  1.0          1.0(10)0     7.1(0)5
  1 000b.fcf8.012c to 000b.fcf8.012c  1.0          1.0(10)0     CSC SSM 5.0
(Build#1187)

Mod SSM Application Name           SSM Application Version
--- ------------------------------ --------------------------
  1 CSC SSM scan services are not
  1 CSC SSM                        5.0 (Build#1187)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  0 Up Sys             Not Applicable
  1 Up                 Up
```

表 27-4 に、各フィールドの説明を示します。

表 27-4　show module のフィールド

フィールド	説明
Mod	スロット番号（0 または 1）。
Card Type	スロット 0 にあるシステムの場合、タイプはプラットフォーム モデルです。スロット 1 にある SSM の場合は、SSM のタイプです。
Model	このスロットのモデル。
Serial No.	シリアル番号。
MAC Address Range	この SSM 上のインターフェイス、システム、または組み込みインターフェイスの MAC アドレス範囲。
Hw Version	ハードウェアのバージョン。
Fw Version	ファームウェアのバージョン。
Sw Version	ソフトウェアのバージョン。
SSM Application Name	SSM 上で実行しているアプリケーションの名前。
SSM Application Version	SSM 上で実行しているアプリケーションのバージョン。

表 27-4　show module のフィールド

フィールド	説明
Status	スロット 1 にあるシステムの場合、ステータスは Up Sys です。スロット 1 にある SSM のステータスは、次のいずれかです。 • Initializing：SSM は検出中で、制御接続はシステムによって初期化中です。 • Up：SSM は、システムによる初期化が完了しています。 • Unresponsive：システムがこの SSM と通信しているときに、エラーが発生しました。 • Reloading：インテリジェント SSM である場合に、SSM がリロード中です。 • Shutting Down：SSM はシャットダウン中です。 • Down：SSM はシャットダウンしました。 • Recover：インテリジェント SSM である場合に、SSM がリカバリ イメージをダウンロードしようとしています。
Data Plane Status	SSM へのデータ プレーンの現在の状態。
Compatibility	システムの他の部分に対する SSM の互換性。

show module details コマンドの出力は、SSM がどちらのスロットにあるかによって異なります。たとえば、CSC SSM の出力には、CSC SSM ソフトウェアのコンポーネントに関するフィールドが含まれます。これらのフィールドは、スロットに AIP SSM がある場合は表示されません。次に、**show module details** コマンドの一般的な出力例を示します。

```
hostname> show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   V1.0
Serial Number:      12345678
Firmware version:   1.0(7)2
Software version:   4.1(1.1)S47(0.1)
MAC Address Range:  000b.fcf8.0156 to 000b.fcf8.0156
Data plane Status:  Up
Status:             Up
Mgmt IP addr:       10.89.147.13
Mgmt web ports:     443
Mgmt TLS enabled:   true
```

表 27-5 に、各フィールドの説明を示します。**show module** コマンドで表示されるフィールドについては、表 27-4 を参照してください。

表 27-5　show module details のフィールド

フィールド	説明
Mgmt IP addr	インテリジェント SSM について、SSM 管理インターフェイスの IP アドレスを表示します。
Mgmt web ports	インテリジェント SSM について、管理インターフェイス用に設定されているポートを表示します。
Mgmt TLS enabled	インテリジェント SSM について、SSM の管理インターフェイスへの接続でトランスポート レイヤ セキュリティがイネーブルになっているかどうかを表示します（true または false）。

次に、**show module** コマンドに ***recover*** キーワードが使用された場合の出力例を示します。

```
hostname> show module 1 recover
Module 1 recover parameters. . .
Boot Recovery Image: Yes
Image URL:           tftp://10.21.18.1/ids-oldimg
Port IP Address:     10.1.2.10
Port Mask :          255.255.255.0
Gateway IP Address:  10.1.2.254
```

関連コマンド

コマンド	説明
debug module-boot	SSM のブート プロセスに関するデバッグ メッセージを表示します。
hw-module module recover	リカバリ イメージを TFTP サーバからロードして、インテリジェント SSM を回復します。
hw-module module reset	SSM をシャットダウンし、ハードウェア リセットを実行します。
hw-module module reload	インテリジェント SSM ソフトウェアをリロードします。
hw-module module shutdown	コンフィギュレーション データを失わずに電源を切るため、SSM ソフトウェアをシャットダウンします。

show mrib client

MRIB クライアント接続に関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib client** コマンドを使用します。

show mrib client [***filter***] [***name*** *client_name*]

シンタックスの説明

filter	（オプション）クライアント フィルタを表示します。各クライアントの所有する MRIB フラグ、および各クライアントと関連のあるフラグに関する情報を表示するために使用します。
name *client_name*	（オプション）MRIB のクライアントとして機能する、PIM や IGMP などのマルチキャスト ルーティング プロトコルの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

filter オプションは、さまざまな MRIB クライアントが登録した、ルートおよびインターフェイス レベルのフラグの変化を表示するために使用します。このコマンド オプションを指定すると、どのフラグが MRIB クライアントによって所有されているかも表示されます。

例

次に、*filter* キーワードを使用した **show mrib client** コマンドの出力例を示します。

```
hostname# show mrib client filter
MFWD:0 (connection id 0)
interest filter:
entry attributes: S C IA D
interface attributes: F A IC NS DP SP
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
groups:
include 0.0.0.0/0
interfaces:
include All
igmp:77964 (connection id 1)
ownership filter:
interface attributes: II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
pim:49287 (connection id 5)
interest filter:
entry attributes: E
interface attributes: SP II ID LI LD
groups:
include 0.0.0.0/0
interfaces:
include All
ownership filter:
entry attributes: L S C IA D
interface attributes: F A IC NS DP
groups:
include 0.0.0.0/0
interfaces:
include All
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルのエントリを表示します。

show mrib route

MRIB テーブルに含まれているエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show mrib route** コマンドを使用します。

show mrib route [[*source* | *****] [*group*[/*prefix-length*]]]

シンタックスの説明

*****	（オプション）共有ツリー エントリを表示します。
/prefix-length	（オプション）MRIB ルートのプレフィックスの長さ。アドレスの上位連続ビットの数を示す 10 進値がプレフィックスになります（アドレスのネットワーク部分）。10 進値の前にスラッシュを付ける必要があります。
group	（オプション）グループの IP アドレスまたは名前。
source	（オプション）ルート送信元の IP アドレスまたは名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

MFIB テーブルは、MRIB からアップデートされるエントリとフラグのサブセットを管理します。フラグは、マルチキャスト パケットに関する一連の転送規則に従って、転送とシグナリングの動作を決定するものです。

インターフェイスとフラグのリストに加えて、ルート エントリごとにさまざまなカウンタも表示されます。バイト数は、転送された総バイト数です。パケット数は、このエントリで受信したパケットの数です。**show mfib count** コマンドは、ルートとは無関係にグローバルなカウンタを表示します。

例

次に、**show mrib route** コマンドの出力例を示します。

```
hostname# show mrib route
IP Multicast Routing Information Base
Entry flags: L - Domain-Local Source, E - External Source to the Domain,
    C - Directly-Connected Check, S - Signal, IA - Inherit Accept, D - Drop
Interface flags: F - Forward, A - Accept, IC - Internal Copy,
    NS - Negate Signal, DP - Don't Preserve, SP - Signal Present,
    II - Internal Interest, ID - Internal Disinterest, LI - Local Interest,
LD - Local Disinterest
(*,224.0.0.0/4) RPF nbr: 10.11.1.20 Flags: L C
   Decapstunnel0 Flags: NS

(*,224.0.0.0/24) Flags: D

(*,224.0.1.39) Flags: S

(*,224.0.1.40) Flags: S
   POS0/3/0/0 Flags: II LI

(*,238.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS LI
   Decapstunnel0 Flags: A

(*,239.1.1.1) RPF nbr: 10.11.1.20 Flags: C
   POS0/3/0/0 Flags: F NS
   Decapstunnel0 Flags: A
```

関連コマンド

コマンド	説明
show mfib count	MFIB テーブルのルートおよびパケットの数に関するデータを表示します。
show mrib route summary	MRIB テーブル エントリの要約を表示します。

show mroute

IPv4 マルチキャスト ルーティング テーブルを表示するには、特権 EXEC モードで **show mroute** コマンドを使用します。

show mroute [*group* [*source*] | ***reserved***] [***active*** [*rate*] | ***count*** | ***pruned*** | ***summary***]

シンタックスの説明

active *rate*	（オプション）アクティブなマルチキャスト送信元のみを表示します。アクティブな送信元とは、指定した *rate* 以上で送信を実行している送信元です。*rate* を指定しない場合、アクティブな送信元は 4 Kbps 以上のレートで送信を実行している送信元です。
count	（オプション）グループと送信元に関する統計情報を表示します。この情報には、パケットの数、1 秒あたりのパケット数、パケットの平均サイズ、および 1 秒あたりのビット数が含まれています。
group	（オプション）DNS（ドメイン ネーム システム）ホスト テーブルで定義されているマルチキャスト グループの IP アドレスまたは名前。
pruned	（オプション）プルーニングされたルートを表示します。
reserved	（オプション）予約済みグループを表示します。
source	（オプション）送信元のホスト名または IP アドレス。
summary	（オプション）マルチキャスト ルーティング テーブル内の各エントリの要約を 1 行で表示します。

デフォルト

rate 引数を指定しない場合、デフォルトでは 4 Kbps になります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show mroute コマンドは、マルチキャスト ルーティング テーブルの内容を表示します。セキュリティ アプライアンスは、PIM プロトコル メッセージ、IGMP レポート、およびトラフィックに基づいて (S,G) エントリと (*,G) エントリを作成し、マルチキャスト ルーティング テーブルにデータを入力します。アスタリスク（*）はすべての送信元アドレス、「S」は単一の送信元アドレス、「G」は宛先マルチキャスト グループ アドレスを意味します。(S,G) エントリを作成する場合、ソフトウェアはユニキャスト ルーティング テーブル内で（RPF を経由して）見つかった該当する宛先グループへの最適パスを使用します。

実行コンフィギュレーションに含まれている **mroute** コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**show mroute** コマンドの出力例を示します。

```
hostname(config)# show mroute

Multicast Routing Table
Flags: D - Dense, S - Sparse, B - Bidir Group, s - SSM Group,
       C - Connected, L - Local, I - Received Source Specific Host Report,
       P - Pruned, R - RP-bit set, F - Register flag, T - SPT-bit set,
       J - Join SPT
Timers: Uptime/Expires
Interface state: Interface, State

(*, 239.1.1.40), 08:07:24/never, RP 0.0.0.0, flags: DPC
  Incoming interface: Null
  RPF nbr: 0.0.0.0
  Outgoing interface list:
    inside, Null, 08:05:45/never
    tftp, Null, 08:07:24/never

(*, 239.2.2.1), 08:07:44/never, RP 140.0.0.70, flags: SCJ
  Incoming interface: outside
  RPF nbr: 140.0.0.70
  Outgoing interface list:
    inside, Forward, 08:07:44/never
```

show mroute の出力には、次のフィールドが含まれています。

- **Flags**：エントリに関する情報を提供します。
  - **D（Dense）**：エントリは稠密モードで動作しています。
  - **S（Sparse）**：エントリは希薄モードで動作しています。
  - **B：(Bidir Group)**：マルチキャスト グループが双方向モードで動作していることを示します。
  - **s（SSM Group）**：マルチキャスト グループが SSM の IP アドレス範囲に入っていることを示します。このフラグは、SSM の範囲が変更されるとリセットされます。
  - **C（Connected）**：マルチキャスト グループのメンバーは、直接接続されたインターフェイス上に存在します。
  - **L（Local）**：セキュリティ アプライアンス自体が、マルチキャスト グループのメンバーです。グループは、（設定済みのグループに対する）**igmp join-group** コマンドによってローカルに加入されています。
  - **I（Received Source Specific Host Report）**：(S,G) エントリが (S,G) レポートによって作成されたことを示します。この (S,G) レポートは IGMP によって作成された可能性があります。このフラグが設定されるのは、DR に対してのみです。
  - **P（Pruned）**：ルートがプルーニングされています。ソフトウェアは、この情報を保持して、ダウンストリーム メンバーが送信元に加入できるようにします。
  - **R（RP-bit set）**：(S,G) エントリが RP をポイントしていることを示します。
  - **F(Register flag)**：ソフトウェアがマルチキャスト送信元に登録されていることを示します。
  - **T（SPT-bit set）**：パケットが最短パス送信元ツリーで受信されていることを示します。
  - **J（Join SPT）**：(*,G) エントリの場合、共有ツリーの下方向に流れるトラフィックの速度が、グループの SPT しきい値設定を超えていることを示します（デフォルトの SPT しきい値設定は 0 Kbps です）。J - Join 最短パス ツリー（SPT）フラグが設定されている場合に、共有ツリーの下流で次の (S,G) パケットが受信されると、送信元の方向に (S,G) join メッセージがトリガーされます。これにより、セキュリティ アプライアンスは送信元ツリーに加入します。

    (S,G) エントリの場合、グループの SPT しきい値を超過したためにエントリが作成されたことを示します。(S,G) エントリに J - Join SPT フラグが設定されている場合、セキュリティ アプライアンスは送信元ツリー上のトラフィック速度を監視します。送信元ツリーのトラフィック速度がグループの SPT しきい値を下回っている状況が 1 分以上継続した場合、ルータはこの送信元の共有ツリーに再び切り替えようとします。

(注) セキュリティ アプライアンスは共有ツリー上のトラフィック速度を測定し、この速度とグループの SPT しきい値を 1 秒ごとに比較します。トラフィック速度が SPT しきい値を超えた場合は、トラフィック速度の次の測定が行われるまで、(*,G) エントリに J - Join SPT フラグが設定されます。共有ツリーに次のパケットが着信し、新しい測定間隔が開始されると、フラグが解除されます。

グループにデフォルトの SPT しきい値（0 Kbps）が使用されている場合、(*,G) エントリには常に J - Join SPT フラグが設定され、解除されません。デフォルトの SPT しきい値が使用されている場合に、新しい送信元からトラフィックを受信すると、セキュリティ アプライアンスは最短パス送信元ツリーにただちに切り替えます。

- **Timers:Uptime/Expires**：Uptime は、エントリが IP マルチキャスト ルーティング テーブルに格納されていた期間（時間、分、秒）をインターフェイスごとに示します。Expires は、IP マルチキャスト ルーティング テーブルからエントリが削除されるまでの期間（時間、分、秒）をインターフェイスごとに示します。
- **Interface state**：着信インターフェイスまたは発信インターフェイスの状態を示します。
  - **Interface**：着信インターフェイスまたは発信インターフェイスのリストに表示されるインターフェイス名。
  - **State**：アクセス リストまたは Time to Live（TTL）しきい値による制限があるかどうかに応じて、インターフェイス上で転送、プルーニング、ヌル値化のいずれの処理がパケットに対して実行されるかを示します。
- **(*, 239.1.1.40)** と **(* , 239.2.2.1)**：IP マルチキャスト ルーティング テーブルのエントリ。エントリは、送信元の IP アドレスと、それに続くマルチキャスト グループの IP アドレスで構成されます。送信元の位置に置かれたアスタリスク（*）は、すべての送信元を意味します。
- **RP**：RP のアドレス。希薄モードで動作するルータおよびアクセス サーバの場合、このアドレスは常に 224.0.0.0 です。
- **Incoming interface**：送信元からのマルチキャスト パケットが着信する予定のインターフェイス。パケットがこのインターフェイスに着信しなかった場合、廃棄されます。
- **RPF nbr**：送信元に対するアップストリーム ルータの IP アドレス。
- **Outgoing interface list**：パケット転送時に使用されるインターフェイス。

関連コマンド

コマンド	説明
clear configure mroute	**mroute** コマンドを実行コンフィギュレーションから削除します。
mroute	スタティック マルチキャスト ルートを設定します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	設定されているマルチキャスト ルートを表示します。

show nameif

nameif コマンドを使用して設定されているインターフェイス名を表示するには、特権 EXEC モードで show nameif コマンドを使用します。

show nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

シンタックスの説明

mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合、セキュリティ アプライアンスはすべてのインターフェイス名を表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名はコンテキスト内でのみ指定できます。このコマンドの出力では、Interface カラムにはマッピング名のみが示されます。

例

次に、**show nameif** コマンドの出力例を示します。

```
hostname# show nameif
Interface               Name                    Security
GigabitEthernet0/0      outside                 0
GigabitEthernet0/1      inside                  100
GigabitEthernet0/2      test2                   50
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
nameif	インターフェイス名を設定します。
show interface ip brief	インターフェイスの IP アドレスとステータスを表示します。

show ntp associations

NTP アソシエーションの情報を表示するには、ユーザ EXEC モードで **show ntp associations** コマンドを使用します。

show ntp associations [**detail**]

シンタックスの説明

detail	（オプション）各アソシエーションの詳細な情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

次に、***show ntp associations*** コマンドの出力例を示します。

```
hostname> show ntp associations
     address         ref clock      st  when  poll  reach  delay  offset    disp
 ~172.31.32.2      172.31.32.1       5    29  1024  377     4.2   -8.59     1.6
+~192.168.13.33    192.168.1.111     3    69   128  377     4.1    3.48     2.3
*~192.168.13.57    192.168.1.111     3    32   128  377     7.9   11.18     3.6
* master (synced), # master (unsynced), + selected, - candidate, ~ configured
```

表 27-6 に、各フィールドの説明を示します。

表 27-6　show ntp associations のフィールド

フィールド	説明
（表示行の行頭の文字）	表示行の行頭には、次の文字が 1 つまたはそれ以上表示されます。 • *：このピアに同期しています。 • #：このピアに対してほぼ同期しています。 • +：ピアは同期可能な対象として選択されています。 • -：ピアが選択候補です。 • ~：ピアがスタティックに設定されていますが、同期していません。
address	NTP ピアのアドレス。
ref clock	ピアのリファレンス クロックのアドレス。
st	ピアの層。

表 27-6　show ntp associations のフィールド（続き）

フィールド	説明
when	ピアから最終 NTP パケットが受信されてからの時間。
poll	ポーリング間隔（秒）。
reach	ピアの到達可能性（8 進のビット文字列）。
delay	ピアまでのラウンド トリップ遅延（ミリ秒）。
offset	ローカル クロックに対するピア クロックの相対時間（ミリ秒）。
disp	分散値。

次に、***show ntp associations detail*** コマンドの出力例を示します。

```
hostname> show ntp associations detail
172.23.56.249 configured, our_master, sane, valid, stratum 4
ref ID 172.23.56.225, time c0212639.2ecfc9e0 (20:19:05.182 UTC Fri Feb 22 2002)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 38.04 msec, root disp 9.55, reach 177, sync dist 156.021
delay 4.47 msec, offset -0.2403 msec, dispersion 125.21
precision 2**19, version 3
org time c02128a9.731f127b (20:29:29.449 UTC Fri Feb 22 2002)
rcv time c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
xmt time c02128a9.6b3f729e (20:29:29.418 UTC Fri Feb 22 2002)
filtdelay =     4.47    4.58    4.97    5.63    4.79    5.52    5.87    0.00
filtoffset =   -0.24   -0.36   -0.37    0.30   -0.17    0.57   -0.74    0.00
filterror =     0.02    0.99    1.71    2.69    3.66    4.64    5.62    16000.0
```

表 27-7 に、各フィールドの説明を示します。

表 27-7　show ntp associations detail のフィールド

フィールド	説明
IP-address configured	サーバ（ピア）の IP アドレス。
（ステータス）	• our_master：セキュリティ アプライアンスがこのピアに対して同期しています。 • selected：ピアは同期可能な対象として選択されています。 • candidate：ピアが選択候補です。
（健全性）	• sane：ピアが基本健全性チェックをパスしました。 • insane：ピアが基本健全性チェックで失敗しました。
（有効性）	• valid：ピア時間は有効であると見なされています。 • invalid：ピア時間は無効であると見なされています。 • leap_add：ピアが、うるう秒が加算されることをシグナリングしています。 • leap-sub：ピアが、うるう秒が減算されることをシグナリングしています。
stratum	ピアの層。
（リファレンス ピア）	unsynced：ピアは、他のどのマシンにも同期されていません。 ref ID：ピアの同期対象となるマシンのアドレス。
time	ピアがマスターから受信した最終タイムスタンプ。
our mode client	ピアに対する相対的なモード。常に「クライアント」です。
peer mode server	ピアの相対的なモード。常に「サーバ」です。
our poll intvl	ピアに対するポーリング間隔。

表 27-7　show ntp associations detail のフィールド（続き）

フィールド	説明
peer poll intvl	ピアからのポーリング間隔。
root delay	ルートへのパスに沿った遅延（最上位層 1 のタイム ソース）。
root disp	ルートへのパスの分散。
reach	ピアの到達可能性（8 進のビット文字列）。
sync dist	ピアの同期間隔。
delay	ピアまでのラウンド トリップ遅延。
offset	クロックに対するピア クロックのオフセット。
dispersion	ピア クロックの分散。
precision	ピア クロックの精度（ヘルツ）。
version	ピアが使用中の NTP バージョン番号。
org time	開始時のタイムスタンプ。
rcv time	受信時のタイムスタンプ。
xmt time	送信時のタイムスタンプ。
filtdelay	各サンプルのラウンドトリップ遅延（ミリ秒）。
filtoffset	各サンプルのクロック オフセット（ミリ秒）。
filterror	各サンプルの誤差の概算値。

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show ntp status

各 NTP アソシエーションのステータスを表示するには、ユーザ EXEC モードで **show ntp status** コマンドを使用します。

show ntp status

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

表示される出力については、「例」の項を参照してください。

例

次に、***show ntp status*** コマンドの出力例を示します。

```
hostname> show ntp status
Clock is synchronized, stratum 5, reference is 172.23.56.249
nominal freq is 99.9984 Hz, actual freq is 100.0266 Hz, precision is 2**6
reference time is c02128a9.73c1954b (20:29:29.452 UTC Fri Feb 22 2002)
clock offset is -0.2403 msec, root delay is 42.51 msec
root dispersion is 135.01 msec, peer dispersion is 125.21 msec
```

表 27-8 に、各フィールドの説明を示します。

表 27-8　show ntp status のフィールド

フィールド	説明
Clock	• synchronized：セキュリティ アプライアンスが NTP サーバに対して同期しています。 • unsynchronized：セキュリティ アプライアンスが NTP サーバに対して同期していません。
stratum	このシステムの NTP 層。
reference	セキュリティ アプライアンスの同期対象になる NTP サーバのアドレス。
nominal freq	システム ハードウェア クロックの公称周波数。
actual freq	システム ハードウェア クロックの測定周波数。
precision	このシステムのクロックの精度（ヘルツ）。

表 27-8　show ntp status のフィールド（続き）

フィールド	説明
reference time	参照時のタイムスタンプ。
clock offset	同期されたピアに対するシステム クロックのオフセット。
root delay	ルート クロックまでのパスに沿った合計遅延。
root dispersion	ルート パスの分散。
peer dispersion	同期されたピアの分散。

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp associations	セキュリティ アプライアンスが関連付けられている NTP サーバを表示します。

show ospf

OSPF ルーティング プロセスに関する一般情報を表示するには、特権 EXEC モードで **show ospf** コマンドを使用します。

show ospf [*pid* **[***area_id***]**]

シンタックスの説明

area_id	（オプション）OSPF アドレス範囲に関連付けられているエリアの ID。
pid	（オプション）OSPF プロセスの ID。

デフォルト

pid を指定しない場合は、すべての OSPF プロセスが一覧表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

pid を指定すると、指定したルーティング プロセスの情報だけが表示されます。

例

次に、**show ospf** コマンドの出力例を示します。この例は、特定の OSPF ルーティング プロセスに関する一般情報を表示する方法を示しています。

```
hostname# show ospf 5
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

次の **show ospf** コマンドの出力例は、すべての OSPF ルーティング プロセスに関する一般情報を表示する方法を示しています。

```
hostname# show ospf
 Routing Process "ospf 5" with ID 127.0.0.1 and Domain ID 0.0.0.5
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0

 Routing Process "ospf 12" with ID 172.23.59.232 and Domain ID 0.0.0.12
 Supports only single TOS(TOS0) routes
 Supports opaque LSA
 SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
 Minimum LSA interval 5 secs. Minimum LSA arrival 1 secs
 Number of external LSA 0. Checksum Sum 0x     0
 Number of opaque AS LSA 0. Checksum Sum 0x     0
 Number of DCbitless external and opaque AS LSA 0
 Number of DoNotAge external and opaque AS LSA 0
 Number of areas in this router is 0. 0 normal 0 stub 0 nssa
 External flood list length 0
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf border-routers

ABR および ASBR に対する内部 OSPF ルーティング テーブル エントリを表示するには、特権 EXEC モードで **show ospf border-routers** コマンドを使用します。

show ospf border-routers

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show ospf border-routers** コマンドの出力例を示します。

```
hostname# show ospf border-routers

OSPF Process 109 internal Routing Table

Codes: i - Intra-area route, I - Inter-area route

i 192.168.97.53 [10] via 192.168.1.53, fifth, ABR, Area 0, SPF 20
i 192.168.103.51 [10] via 192.168.96.51, outside, ASBR, Area 192.168.12.0, SPF 14
i 192.168.103.52 [10] via 192.168.96.51, outside, ABR/ASBR, Area 192.168.12.0, SPF 14
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf database

セキュリティ アプライアンス上の OSPF トポロジ データベースに格納されている情報を表示するには、特権 EXEC モードで **show ospf database** コマンドを使用します。

show ospf [*pid* [*area_id*]] **database** [***router*** | ***network*** | ***summary*** | ***asbr-summary*** | ***external*** | ***nssa-external***] [*lsid*] [***internal***] [***self-originat***e | ***adv-router*** *addr*]

show ospf [*pid* [*area_id*]] **database database-summary**

シンタックスの説明

addr	（オプション）ルータのアドレス。
adv-router	（オプション）アドバタイズされたルータ。
area_id	（オプション）OSPF アドレス範囲に関連付けられているエリアの ID。
asbr-summary	（オプション）ASBR リストの要約を表示します。
database	データベース情報を表示します。
database-summary	（オプション）データベース全体の要約リストを表示します。
external	（オプション）指定した自律システムの外部のルートを表示します。
internal	（オプション）指定した自律システム内部のルート。
lsid	（オプション）LSA ID。
network	（オプション）ネットワークに関する OSPF データベース情報を表示します。
nssa-external	（オプション）外部準スタブ エリアのリストを表示します。
pid	（オプション）OSPF プロセスの ID。
router	（オプション）ルータを表示します。
self-originate	（オプション）指定した自律システムに関する情報を表示します。
summary	（オプション）リストの要約を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

例

次に、**show ospf database** コマンドの出力例を示します。

```
hostname# show ospf database
OSPF Router with ID(192.168.1.11) (Process ID 1)

                Router Link States(Area 0)
Link ID   ADV Router   Age   Seq# Checksum Link count
192.168.1.8 192.168.1.8 1381 0x8000010D    0xEF60 2
192.168.1.11 192.168.1.11 1460 0x800002FE    0xEB3D 4
192.168.1.12 192.168.1.12 2027 0x80000090    0x875D 3
192.168.1.27 192.168.1.27 1323 0x800001D6    0x12CC 3

                Net Link States(Area 0)
Link ID ADV Router   Age   Seq# Checksum
172.16.1.27 192.168.1.27 1323 0x8000005B    0xA8EE
172.17.1.11 192.168.1.11 1461 0x8000005B    0x7AC

                Type-10 Opaque Link Area Link States (Area 0)
Link ID ADV Router   Age Seq# Checksum Opaque ID
10.0.0.0 192.168.1.11 1461 0x800002C8    0x8483   0
10.0.0.0 192.168.1.12 2027 0x80000080    0xF858   0
10.0.0.0 192.168.1.27 1323 0x800001BC    0x919B   0
10.0.0.1 192.168.1.11 1461 0x8000005E    0x5B43   1
```

次に、**show ospf database asbr-summary** コマンドの出力例を示します。

```
hostname# show ospf database asbr-summary
OSPF Router with ID(192.168.239.66) (Process ID 300)
Summary ASB Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1463
Options: (No TOS-capability)
LS Type: Summary Links(AS Boundary Router)
Link State ID: 172.16.245.1 (AS Boundary Router address)
Advertising Router: 172.16.241.5
LS Seq Number: 80000072
Checksum: 0x3548
Length: 28
Network Mask: 0.0.0.0
TOS: 0 Metric: 1
```

次に、**show ospf database router** コマンドの出力例を示します。

```
hostname# show ospf database router
OSPF Router with id(192.168.239.66) (Process ID 300)
Router Link States(Area 0.0.0.0)
Routing Bit Set on this LSA
LS age: 1176
Options: (No TOS-capability)
LS Type: Router Links
Link State ID: 10.187.21.6
Advertising Router: 10.187.21.6
LS Seq Number: 80002CF6
Checksum: 0x73B7
Length: 120
AS Boundary Router
Number of Links: 8
Link connected to: another Router (point-to-point)
(link ID) Neighboring Router ID: 10.187.21.5
(Link Data) Router Interface address: 10.187.21.6
Number of TOS metrics: 0
TOS 0 Metrics: 2
```

次に、**show ospf database network** コマンドの出力例を示します。

```
hostname# show ospf database network
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Net Link States(Area 0.0.0.0)
LS age: 1367
Options: (No TOS-capability)
LS Type: Network Links
Link State ID: 10.187.1.3 (address of Designated Router)
Advertising Router: 192.168.239.66
LS Seq Number: 800000E7
Checksum: 0x1229
Length: 52
Network Mask: 255.255.255.0
Attached Router: 192.168.239.66
Attached Router: 10.187.241.5
Attached Router: 10.187.1.1
Attached Router: 10.187.54.5
Attached Router: 10.187.1.5
```

次に、**show ospf database summary** コマンドの出力例を示します。

```
hostname# show ospf database summary
OSPF Router with id(192.168.239.66) (Process ID 300)
Displaying Summary Net Link States(Area 0.0.0.0)
LS age: 1401
Options: (No TOS-capability)
LS Type: Summary Links(Network)
Link State ID: 10.187.240.0 (summary Network Number)
Advertising Router: 10.187.241.5
LS Seq Number: 80000072
Checksum: 0x84FF
Length: 28
Network Mask: 255.255.255.0 TOS: 0 Metric: 1
```

次に、**show ospf database external** コマンドの出力例を示します。

```
hostname# show ospf database external
OSPF Router with id(192.168.239.66) (Autonomous system 300)

                  Displaying AS External Link States
LS age: 280
Options: (No TOS-capability)
LS Type: AS External Link
Link State ID: 172.16.0.0 (External Network Number)
Advertising Router: 10.187.70.6
LS Seq Number: 80000AFD
Checksum: 0xC3A
Length: 36
Network Mask: 255.255.0.0

      Metric Type: 2 (Larger than any link state path)
TOS: 0
Metric: 1
Forward Address: 0.0.0.0
External Route Tag: 0
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf flood-list

インターフェイスを介してフラッドされるのを待機している OSPF LSA のリストを表示するには、特権 EXEC モードで **show ospf flood-list** コマンドを使用します。

show ospf flood-list *interface_name*

シンタックスの説明

interface_name	ネイバー情報を表示するインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

例

次に、**show ospf flood-list** コマンドの出力例を示します。

```
hostname# show ospf flood-list outside

  Interface outside, Queue length 20
  Link state flooding due in 12 msec

  Type  LS ID          ADV RTR          Seq NO       Age   Checksum
     5  10.2.195.0     192.168.0.163    0x80000009   0     0xFB61
     5  10.1.192.0     192.168.0.163    0x80000009   0     0x2938
     5  10.2.194.0     192.168.0.163    0x80000009   0     0x757
     5  10.1.193.0     192.168.0.163    0x80000009   0     0x1E42
     5  10.2.193.0     192.168.0.163    0x80000009   0     0x124D
     5  10.1.194.0     192.168.0.163    0x80000009   0     0x134C
```

関連コマンド

コマンド	説明
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf interface

OSPF 関連のインターフェイス情報を表示するには、特権 EXEC モードで **show ospf interface** コマンドを使用します。

show ospf interface [*interface_name*]

シンタックスの説明

interface_name	（オプション）OSPF 関連の情報を表示するインターフェイスの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

interface_name 引数を指定せずに使用すると、すべてのインターフェイスの OSPF 情報が表示されます。

例

次に、**show ospf interface** コマンドの出力例を示します。

```
hostname# show ospf interface inside
inside is up, line protocol is up
Internet Address 192.168.254.202, Mask 255.255.255.0, Area 0.0.0.0
AS 201, Router ID 192.77.99.1, Network Type BROADCAST, Cost: 10
Transmit Delay is 1 sec, State OTHER, Priority 1
Designated Router id 192.168.254.10, Interface address 192.168.254.10
Backup Designated router id 192.168.254.28, Interface addr 192.168.254.28
Timer intervals configured, Hello 10, Dead 60, Wait 40, Retransmit 5
Hello due in 0:00:05
Neighbor Count is 8, Adjacent neighbor count is 2
  Adjacent with neighbor 192.168.254.28 (Backup Designated Router)
  Adjacent with neighbor 192.168.254.10 (Designated Router)
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開きます。

show ospf neighbor

インターフェイスごとの OSPF ネイバー情報を表示するには、特権 EXEC モードで **show ospf neighbor** コマンドを使用します。

show ospf neighbor [***detail*** | *interface_name* [*nbr_router_id*]]

シンタックスの説明

detail	（オプション）指定したルータに関する詳細な情報を表示します。
interface_name	（オプション）ネイバー情報を表示するインターフェイスの名前。
nbr_router_id	（オプション）隣接ルータのルータ ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show ospf neighbor** コマンドの出力例を示します。この例は、インターフェイスごとの OSPF ネイバー情報を表示する方法を示しています。

```
hostname# show ospf neighbor outside

Neighbor 192.168.5.2, interface address 10.225.200.28
    In the area 0 via interface outside
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 10.225.200.28 BDR is 10.225.200.30
    Options is 0x42
    Dead timer due in 00:00:36
    Neighbor is up for 00:09:46
  Index 1/1, retransmission queue length 0, number of retransmission 1
    First 0x0(0)/0x0(0) Next 0x0(0)/0x0(0)
    Last retransmission scan length is 1, maximum is 1
    Last retransmission scan time is 0 msec, maximum is 0 msec
```

関連コマンド

コマンド	説明
neighbor	非ブロードキャスト ネットワークに相互接続する OSPF ルータを設定します。
router ospf	OSPF ルーティングをイネーブルにし、グローバル OSPF ルーティング パラメータを設定します。

show ospf request-list

ルータによって要求されたすべての LSA のリストを表示するには、特権 EXEC モードで **show ospf request-list** コマンドを使用します。

show ospf request-list *nbr_router_id interface_name*

シンタックスの説明

interface_name	ネイバー情報を表示するインターフェイスの名前。このインターフェイスからルータによって要求されたすべての LSA のリストを表示します。
nbr_router_id	隣接ルータのルータ ID。このネイバーからルータによって要求されたすべての LSA のリストを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show ospf request-list** コマンドの出力例を示します。

```
hostname# show ospf request-list 192.168.1.12 inside

          OSPF Router with ID (192.168.1.11) (Process ID 1)

  Neighbor 192.168.1.12, interface inside address 172.16.1.12

  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x8000020D   8     0x6572
```

関連コマンド

コマンド	説明
show ospf retransmission-list	再送信されるのを待機しているすべての LSA のリストを表示します。

show ospf retransmission-list

再送信されるのを待機しているすべての LSA のリストを表示するには、特権 EXEC モードで **show ospf retransmission-list** コマンドを使用します。

show ospf retransmission-list *nbr_router_id interface_name*

シンタックスの説明

interface_name	ネイバー情報を表示するインターフェイスの名前。
nbr_router_id	隣接ルータのルータ ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

OSPF ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。OSPF 関連の **show** コマンドを使用するには、OSPF コンフィギュレーション モードである必要はありません。

nbr_router_id 引数を指定すると、この隣接ルータの、再送信されるのを待機しているすべての LSA のリストが表示されます。

interface_name 引数を指定すると、このインターフェイスの、再送信されるのを待機しているすべての LSA のリストが表示されます。

例

次に、**show ospf retransmission-list** コマンドの出力例を示します。例では、*nbr_router_id* 引数は 192.168.1.11 で、*if_name* 引数は outside です。

```
hostname# show ospf retransmission-list 192.168.1.11 outside

          OSPF Router with ID (192.168.1.12) (Process ID 1)

  Neighbor 192.168.1.11, interface outside address 172.16.1.11
  Link state retransmission due in 3764 msec, Queue length 2


  Type   LS ID          ADV RTR        Seq NO       Age   Checksum
     1   192.168.1.12   192.168.1.12   0x80000210   0     0xB196
```

関連コマンド

コマンド	説明
show ospf request-list	ルータによって要求されたすべての LSA のリストを表示します。

show ospf summary-address

OSPF プロセスに対して設定されたすべてのサマリー アドレス再配布情報のリストを表示するには、特権 EXEC モードで **show ospf summary-address** コマンドを使用します。

show ospf summary-address

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show ospf summary-address** コマンドの出力例を示します。この例は、ID が 5 である OSPF プロセスに対してサマリー アドレスが設定される前に、すべてのサマリー アドレス再配布情報のリストを表示する方法を示しています。

```
hostname# show ospf 5 summary-address

OSPF Process 2, Summary-address

10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 0
10.2.0.0/255.255.0.0 Metric -1, Type 0, Tag 10
```

関連コマンド

コマンド	説明
summary-address	OSPF の集約アドレスを作成します。

show ospf virtual-links

OSPF 仮想リンクのパラメータと現在の状態を表示するには、特権 EXEC モードで **show ospf virtual-links** コマンドを使用します。

show ospf virtual-links

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show ospf virtual-links** コマンドの出力例を示します。

```
hostname# show ospf virtual-links

Virtual Link to router 192.168.101.2 is up
Transit area 0.0.0.1, via interface Ethernet0, Cost of using 10
Transmit Delay is 1 sec, State POINT_TO_POINT
Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
Hello due in 0:00:08
Adjacency State FULL
```

関連コマンド

コマンド	説明
area virtual-link	OSPF 仮想リンクを定義します。

show perfmon

セキュリティ アプライアンスのパフォーマンスに関する情報を表示するには、**show perfmon** コマンドを使用します。

show perfmon [**detail**]

シンタックスの説明

detail	（オプション）追加の統計情報を表示します。これらの統計情報は Cisco Unified Firewall MIB のグローバル接続オブジェクトとプロトコルごとの接続オブジェクトにより収集された情報と一致します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	セキュリティ アプライアンスでこのコマンドがサポートされるようになりました。
7.2(1)	**detail** キーワードが追加されました。

使用上のガイドライン

このコマンドの出力は、Telnet セッションには表示されません。

perfmon コマンドは指定した間隔でパフォーマンス統計情報を連続的に表示します。**show perfmon** コマンドを使用すると、すぐに情報を表示できます。

例

次に、**show perfmon** コマンドの出力例を示します。

```
hostname(config)# show perfmon
Context: my_context
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
WebSns Req           0/s          0/s
TCP Fixup            0/s          0/s
TCP Intercept        0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

次に、**show perfmon detail** コマンドの出力例を示します。

```
hostname(config)# show perfmon detail
PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
TCP Intercept        0/s          0/s

SETUP RATES:
Connections for 1 minute = 0/s; 5 minutes = 0/s
TCP Conns for 1 minute = 0/s; 5 minutes = 0/s
UDP Conns for 1 minute = 0/s; 5 minutes = 0/s
```

関連コマンド

コマンド	説明
perfmon	指定した間隔で詳細なパフォーマンス モニタ情報を表示します。

show pim df

ランデブー ポイント（RP）またはインターフェイスについて、双方向 DF の「勝者」を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim df** コマンドを使用します。

show pim df [**winner**] [*rp_address* | *if_name*]

シンタックスの説明

rp_address	次のいずれか 1 つを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。
if_name	インターフェイスの物理名または論理名。
winner	（オプション）DF 選択の勝者をインターフェイスごと、RP ごとに表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、RP への勝者のメトリックも表示します。

例

次に、**show pim df** コマンドの出力例を示します。

```
hostname# show df winner inside
RP           Interface   DF Winner   Metrics

172.16.1.3   Loopback3   172.17.3.2  [110/2]
172.16.1.3   Loopback2   172.17.2.2  [110/2]
172.16.1.3   Loopback1   172.17.1.2  [110/2]
172.16.1.3   inside      10.10.2.3   [0/0]
172.16.1.3   inside      10.10.1.2   [110/2]
```

show pim group-map

グループからプロトコルへのマッピング テーブルを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim group-map** コマンドを使用します。

show pim group-map [***info-source***] [*group*]

シンタックスの説明

group	（オプション）次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。
info-source	（オプション）グループ範囲情報の情報源を表示します。

デフォルト

すべてのグループについて、グループからプロトコルへのマッピングを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、RP について、グループとプロトコルとのアドレス マッピングをすべて表示します。マッピングは、セキュリティ アプライアンス上でさまざまなクライアントからラーニングされます。

セキュリティ アプライアンスの PIM 実装は、さまざまな特殊エントリをマッピング テーブルで保持しています。Auto-RP グループ範囲は、希薄モード グループ範囲から明確に拒否されます。SSM グループ範囲も希薄モードには入りません。リンク ローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.225。224.0.0.0/24 として定義）も、希薄モード グループ範囲から拒否されます。最後のエントリは、所定の RP で希薄モードに入っている残りすべてのグループを示します。

pim rp-address コマンドで複数の RP を設定した場合は、適切なグループ範囲が対応する RP と共に表示されます。

例

次に、**show pim group-map** コマンドの出力例を示します。

```
hostname# show pim group-map
Group Range      Proto   Client Groups   RP address   Info

224.0.1.39/32*   DM      static 1        0.0.0.0
224.0.1.40/32*   DM      static 1        0.0.0.0
224.0.0.0/24*    NO      static 0        0.0.0.0
232.0.0.0/8*     SSM     config 0        0.0.0.0
224.0.0.0/4*     SM      autorp 1        10.10.2.2    RPF: POS01/0/3,10.10.3.2
```

1 行目と 2 行目で、Auto-RP グループ範囲が希薄モード グループ範囲から明確に拒否されています。

3 行目では、リンク ローカル マルチキャスト グループ（224.0.0.0 ～ 224.0.0.225。224.0.0.0/24 として定義）も希薄モード グループ範囲から拒否されています。

4 行目では、PIM 送信元特定マルチキャスト（PIM-SSM）グループ範囲が 232.0.0.0/8 にマッピングされています。

最後のエントリは、残りすべてのグループが希薄モードに入って、RP 10.10.3.2 にマッピングされたことを示しています。

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。
pim rp-address	PIM ランデブー ポイント（RP）のアドレスを設定します。

show pim interface

PIM に関するインターフェイス固有の情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim interface** コマンドを使用します。

show pim interface [*if_name* | ***state-off*** | ***state-on***]

シンタックスの説明

if_name	（オプション）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。
state-off	（オプション）PIM がディセーブルになっているインターフェイスを表示します。
state-on	（オプション）PIM がイネーブルになっているインターフェイスを表示します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスに関する PIM 情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの PIM 実装は、セキュリティ アプライアンス自体を PIM ネイバーと見なします。したがって、このコマンドの出力にあるネイバー数カラムでは、ネイバー数が実際の数よりも 1 つ多く表示されます。

例

次の例では、内部インターフェイスに関する PIM 情報を表示しています。

```
hostname# show pim interface inside
Address    Interface      Ver/     Nbr     Query      DR     DR
                          Mode     Count   Intvl      Prior
172.16.1.4 inside         v2/S     2       100 ms     1      172.16.1.4
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

show pim join-prune statistic

PIM の加入とプルーニングに関する集約的な統計情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim join-prune statistics** コマンドを使用します。

show pim join-prune statistics [*if_name*]

シンタックスの説明

if_name	（オプション）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて、加入とプルーニングに関する統計情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PIM の加入とプルーニングに関する統計情報を消去するには、**clear pim counters** コマンドを使用します。

例

次に、**show pim join-prune statistic** コマンドの出力例を示します。

```
hostname# show pim join-prune statistic

PIM Average Join/Prune Aggregation for last (1K/10K/50K) packets
Interface          Transmitted             Received

             inside   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet1   0 /    0 /    0         0 /    0 /    0
         Ethernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet3   0 /    0 /    0         0 /    0 /    0
  GigabitEthernet0   0 /    0 /    0         0 /    0 /    0
         Ethernet2   0 /    0 /    0         0 /    0 /    0
```

関連コマンド

コマンド	説明
clear pim counters	PIM トラフィック カウンタを消去します。

show pim neighbor

PIM ネイバー テーブルに含まれているエントリを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim neighbor** コマンドを使用します。

show pim neighbor [***count*** | ***detail***] [*interface*]

シンタックスの説明

interface	（オプション）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。
count	（オプション）PIM ネイバーの合計数、および各インターフェイスの PIM ネイバーの数を表示します。
detail	（オプション）upstream-detection hello オプションを通じてラーニングした、ネイバーの追加アドレスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、このルータが PIM の hello メッセージを通じてラーニングした PIM ネイバーを特定するために使用します。また、このコマンドは、インターフェイスが指定ルータ（DR）であること、およびネイバーで双方向処理が可能になるタイミングも示します。

セキュリティ アプライアンスの PIM 実装は、セキュリティ アプライアンス自体を PIM ネイバーと見なします。したがって、セキュリティ アプライアンス インターフェイスがこのコマンドの出力に表示されます。セキュリティ アプライアンスの IP アドレスは、アドレスの次にアスタリスク（*）を付けて示されています。

例

次に、**show pim neighbor** コマンドの出力例を示します。

```
hostname# show pim neighbor inside
Neighbor Address    Interface    Uptime     Expires   DR  pri  Bidir
10.10.1.1           inside       03:40:36   00:01:41  1        B
10.10.1.2*          inside       03:41:28   00:01:32  1   (DR) B
```

関連コマンド

コマンド	説明
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

show pim range-list

PIM の範囲リストの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim range-list** コマンドを使用します。

show pim range-list [*rp_address*]

シンタックスの説明

rp_address	次のいずれか 1 つを指定できます。 • RP の名前。ドメイン ネーム システム（DNS）の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • RP の IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、マルチキャスト転送モードからグループへのマッピングを特定するために使用します。出力には、この範囲のランデブー ポイント（RP）のアドレスも示されます（該当する場合）。

例

次に、**show pim range-list** コマンドの出力例を示します。

```
hostname# show pim range-list
config SSM Exp: never Src: 0.0.0.0
  230.0.0.0/8 Up: 03:47:09
config BD RP: 172.16.1.3 Exp: never Src: 0.0.0.0
  239.0.0.0/8 Up: 03:47:16
config BD RP: 172.18.1.6 Exp: never Src: 0.0.0.0
  239.100.0.0/16 Up: 03:47:10
config SM RP: 172.18.2.6 Exp: never Src: 0.0.0.0
  235.0.0.0/8 Up: 03:47:09
```

関連コマンド

コマンド	説明
show pim group-map	グループから PIM モードへのマッピング、およびアクティブな RP の情報を表示します。

show pim topology

PIM トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology** コマンドを使用します。

show pim topology [*group*] [*source*]

シンタックスの説明

group	（オプション）次のいずれかを指定できます。 • マルチキャスト グループの名前。DNS の hosts テーブルに定義されているものか、ドメインの **ipv4 host** コマンドで定義したものです。 • マルチキャスト グループの IP アドレス。これは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。
source	（オプション）次のいずれかを指定できます。 • マルチキャスト送信元の名前。DNS の hosts テーブルに定義されているものか、**domain ipv4 host** コマンドで定義したものです。 • マルチキャスト送信元の IP アドレスこれは、4 分割ドット 10 進表記のマルチキャスト IP アドレスです。

デフォルト

すべてのグループと送信元のトポロジ情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PIM トポロジ テーブルは、所定のグループのさまざまなエントリ、(*,G)、(S,G)、(S,G)RPT をそれぞれのインターフェイス リストと共に表示するために使用します。

PIM は、これらのエントリの内容を MRIB を通じてやり取りします。MRIB は、PIM などのマルチキャスト ルーティング プロトコルと、インターネット グループ管理プロトコル（IGMP）などのローカル メンバーシップ プロトコルとの通信における仲介手段であり、システムのマルチキャスト転送エンジンです。

MRIB は、所定の (S,G) エントリについて、どのインターフェイスでデータ パケットを受け取る必要があるか、どのインターフェイスでデータ パケットを転送する必要があるかを示します。また、転送時にはマルチキャスト転送情報ベース（MFIB）テーブルを使用して、パケットごとの転送アクションを決定します。

（注） 転送情報を表示するには、**show mfib route** コマンドを使用します。

例

次に、**show pim topology** コマンドの出力例を示します。

```
hostname# show pim topology

IP PIM Multicast Topology Table
Entry state: (*/S,G)[RPT/SPT] Protocol Uptime Info
Entry flags: KAT - Keep Alive Timer, AA - Assume Alive, PA - Probe Alive,
    RA - Really Alive, LH - Last Hop, DSS - Don't Signal Sources,
    RR - Register Received, SR
(*,224.0.1.40) DM Up: 15:57:24 RP: 0.0.0.0
JP: Null(never) RPF: ,0.0.0.0 Flags: LH DSS
  outside            15:57:24  off LI LH

(*,224.0.1.24) SM Up: 15:57:20 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:20  fwd LI LH

(*,224.0.1.60) SM Up: 15:57:16 RP: 0.0.0.0
JP: Join(00:00:32) RPF: ,0.0.0.0 Flags: LH
  outside            15:57:16  fwd LI LH
```

関連コマンド

コマンド	説明
show mrib route	MRIB テーブルを表示します。

show pim topology reserved

予約済みグループに関する PIM トポロジ テーブルの情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology reserved** コマンドを使用します。

show pim topology reserved

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

なし。

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show pim topology route-count

PIM トポロジ テーブルのエントリの数を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim topology route-count** コマンドを使用します。

show pim topology route-count [***detail***]

シンタックスの説明

detail	（オプション）グループごとに、数に関する詳細な情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、PIM トポロジ テーブルに保持されているエントリの数を表示します。エントリに関する詳細な情報を表示するには、**show pim topology** コマンドを使用します。

例

次に、**show pim topology route-count** コマンドの出力例を示します。

```
hostname# show pim topology route-count

PIM Topology Table Summary
  No. of group ranges = 5
  No. of (*,G) routes = 0
  No. of (S,G) routes = 0
  No. of (S,G)RPT routes = 0
```

関連コマンド

コマンド	説明
show pim topology	PIM トポロジ テーブルを表示します。

show pim traffic

PIM トラフィックのカウンタを表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim traffic** コマンドを使用します。

show pim traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PIM トラフィックのカウンタを消去するには、**clear pim counters** コマンドを使用します。

例

次に、**show pim traffic** コマンドの出力例を示します。

```
hostname# show pim traffic

PIM Traffic Counters
Elapsed time since counters cleared: 3d06h

                                Received     Sent
Valid PIM Packets                      0        9485
Hello                                  0        9485
Join-Prune                             0           0
Register                               0           0
Register Stop                          0           0
Assert                                 0           0
Bidir DF Election                      0           0

Errors:
Malformed Packets                                  0
Bad Checksums                                      0
Send Errors                                        0
Packet Sent on Loopback Errors                     0
Packets Received on PIM-disabled Interface         0
Packets Received with Unknown PIM Version          0
```

関連コマンド

コマンド	説明
clear pim counters	PIM トラフィック カウンタを消去します。

show pim tunnel

PIM トンネル インターフェイスに関する情報を表示するには、ユーザ EXEC モードまたは特権 EXEC モードで **show pim tunnels** コマンドを使用します。

show pim tunnels [*if_name*]

シンタックスの説明

if_name	（オプション）インターフェイスの名前。この引数を指定すると、表示される情報は指定したインターフェイスに関するものだけになります。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスについて PIM トンネル情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC または特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

PIM レジスタ パケットは、仮想カプセル化トンネル インターフェイスを経由して、送信元の最初のホップ DR ルータから RP に送信されます。RP では、仮想カプセル化解除トンネルを使用して、PIM レジスタ パケットの受信インターフェイスを表現します。このコマンドは、両方のタイプのインターフェイスについてトンネル情報を表示します。

レジスタ トンネルは、（PIM レジスタ メッセージ内に）カプセル化された、送信元からのマルチキャスト パケットです。送信元は、共有ツリーを経由して、配布のために RP に送信されます。登録が適用されるのは、SM に対してのみです。SSM および双方向 PIM には適用されません。

例

次に、**show pim tunnel** コマンドの出力例を示します。

```
hostname# show pim tunnel

Interface     RP Address Source Address


Encapstunnel0 10.1.1.1   10.1.1.1

Decapstunnel0 10.1.1.1   -
```

show power inline

ASA 5505 適応型セキュリティ アプライアンスなどの PoE インターフェイスを持つモデルの場合、インターフェイス上で電源のステータスを表示するには、**show power inline** コマンドを使用します。

show power inline

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

PoE インターフェイスを使用して、IP Phone または無線アクセス ポイントなどの電源を必要するデバイスを接続します。

例

次に、**show power inline** コマンドの出力例を示します。

```
hostname> show power inline

  Interface     Power   Device
  -----------   -----   ------
  Ethernet0/0    n/a    n/a
  Ethernet0/1    n/a    n/a
  Ethernet0/2    n/a    n/a
  Ethernet0/3    n/a    n/a
  Ethernet0/4    n/a    n/a
  Ethernet0/5    n/a    n/a
  Ethernet0/6    On     Cisco
  Ethernet0/7    Off    n/a
```

表 27-9 に、各フィールドの説明を示します。

表 27-9　show power inline のフィールド

フィールド	説明
Interface	セキュリティ アプライアンス上のすべてのインターフェイスを表示します。PoE が使用できないインターフェイスも含みます。
Power	電源がオンかオフかを示します。デバイスに電源が必要でない場合、インターフェイスにデバイスがない場合、またはインターフェイスがシャットダウンしている場合、値はオフになります。インターフェイスが PoE をサポートしていない場合、値は n/a（該当なし）になります。
Device	給電されるデバイスのタイプを表示します。Cisco または IEEE のいずれかです。デバイスが給電されていない場合、値は n/a（該当なし）です。デバイスの給電が Cisco の場合、ディスプレイには Cisco と表示されます。IEEE は、デバイスの給電が IEEE 802.3af 準拠であることを示します。

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべて消去します。
clear interface	**show interface** コマンドのカウンタを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show priority-queue statistics

インターフェイスのプライオリティ キューに関する統計情報を表示するには、特権 EXEC モードで **show priority-queue statistics** コマンドを使用します。

show priority-queue statistics [*interface-name*]

シンタックスの説明

interface-name	（オプション）ベストエフォート キューおよび低遅延キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

インターフェイス名を省略した場合は、すべての設定済みインターフェイスについてプライオリティ キュー統計情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、test というインターフェイスについて **show priority-queue statistics** コマンドを使用した場合のコマンド出力を示しています。この出力で、BE はベストエフォート キュー、LLQ は低遅延キューを表しています。

```
hostname# show priority-queue statistics test

Priority-Queue Statistics interface test

Queue Type      = BE
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0

Queue Type      = LLQ
Packets Dropped   = 0
Packets Transmit  = 0
Packets Enqueued  = 0
Current Q Length  = 0
Max Q Length      = 0
hostname#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
clear priority-queue statistics	特定のインターフェイス、またはすべての設定済みインターフェイスに関するプライオリティ キュー統計情報のカウンタを消去します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show running-config priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを表示します。

show processes

セキュリティ アプライアンス上で動作しているプロセスのリストを表示するには、特権 EXEC モードで **show processes** コマンドを使用します。

show processes [cpu-hog | memory | internals]

デフォルト

デフォルトでは、このコマンドはセキュリティ アプライアンス上で動作しているプロセスを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドがサポートされるようになりました。
7.0(4)	Runtime 値を 1 ミリ秒以内の精度で表示するように強化されました。
7.2(1)	出力表示が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。

使用上のガイドライン

show processes コマンドを使用すると、セキュリティ アプライアンス上で動作しているプロセスのリストを表示できます。

また、オプションの **cpu-hog** 引数を指定して実行すると、CPU を使用しているプロセスを特定するのに役立ちます。プロセスには、CPU を占有している期間が 100 ミリ秒を超えている場合、フラグが付けられます。**show process cpu-hog** コマンドを実行すると、次のカラムが表示されます。

- MAXHOG：CPU 占有実行の最長期間（ミリ秒単位）
- NUMHOG：CPU 占有実行の回数
- LASTHOG：最後の CPU 占有実行の期間（ミリ秒単位）
- PC：CPU 占有プロセスの命令ポインタ

- Traceback：CPU 占有プロセスのスタック トレース

プロセスは、数個の命令だけを必要とする軽量スレッドです。リスト内で、PC はプログラム カウンタ、SP はスタック ポインタ、STATE はスレッド キューのアドレス、Runtime はスレッドが実行されている（CPU クロックのサイクルに基づく）時間（ミリ秒）、SBASE はスタックのベース アドレス、Stack はスタックの現在使用されているバイト数と合計サイズであり、Process はスレッドの機能を示します。

ランタイム値を 1 ミリ秒以内の精度で表示するように強化され、クロック ティック（精度 10 ミリ秒）の代わりに CPU クロック サイクル（最大精度 10 ナノ秒）に基づいた CPU 使用状況のプロセスのアカウンティングが正確で完全になりました。

Traceback には最大で 14 のアドレスを設定できます。

スケジューラと合計サマリー行で、**show proccess** コマンドを 2 回連続で実行し、その出力を比較して次のことを判断できます。

- CPU 時間がどこで 100% 使用されたか。
- 各スレッドが CPU を何 % 使用しているか。これは、スレッドのランタイム差分を合計ランタイム差分と比較して判断します。

オプションの **memory** 引数を指定すると、各プロセスによって割り当てられたメモリが表示されます。この情報は、プロセスによるメモリ使用状況を追跡するのに役立ちます。

オプションの **internals** 引数を指定すると、起動されたコールの数とギブアップの数が表示されます。Invoked は、スケジューラがプロセスを起動した（実行した）回数です。Giveups は、プロセスが CPU をスケジューラに返還した回数です。

例

次の例は、セキュリティ アプライアンス上で動作しているプロセスのリストを表示する方法を示しています。

```
hostname(config)# show processes

    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 00102aa0 0a63f288 0089b068     117460 0a63e2d4 3600/4096 arp_timer
Lsi 00102aa0 0a6423b4 0089b068         10 0a64140c 3824/4096 FragDBGC
Hwe 004257c8 0a7cacd4 0082dfd8          0 0a7c9d1c 3972/4096 udp_timer
Lwe 0011751a 0a7cc438 008ea5d0         20 0a7cb474 3560/4096 dbgtrace
<--- More --->

-     -        -         -        638515    -         -     scheduler
-     -        -         -       2625389    -         -     total
hostname(config)# show processes cpu

Process: ci/console, NUMHOG: 1, MAXHOG: 210, LASTHOG: 210 LASTHOG At:  01:08:24 UTC
Jul 24 2005
PC:          153412
Traceback:    1532de  15352a  14b66d  14ba61 148c30 14930e  1125d1

Process: fover_parse, NUMHOG: 2, MAXHOG: 200, LASTHOG: 200
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           6ff434
Traceback:    6ff838  6fe3a7  6fe424  6fe5ab 7060b7 3bfa44  1125d1

hostname(config)# show processes memory

-------------------------------------------------------------
Allocs   Allocated       Frees         Freed         Process
          (bytes)                      (bytes)
-------------------------------------------------------------
23512    13471545        6             180           *System Main*
0        0               0             0             lu_rx
2        8324            16            19488         vpnlb_thread
(other lines deleted for brevity)

hostname# sho proc internals

     Invoked      Giveups  Process
           1            0  block_diag
    19108445     19108445  Dispatch Unit
           1            0  CF OIR
           1            0  Reload Control Thread
           1            0  aaa
           2            0  CMGR Server Process
           1            0  CMGR Timer Process
           2            0  dbgtrace
          69            0  557mcfix
    19108019     19108018  557poll
           2            0  557statspoll
           1            0  Chunk Manager
         135            0  PIX Garbage Collector
           6            0  route_process
           1            0  IP Address Assign
           1            0  QoS Support Module
           1            0  Client Update Task
        8973         8968  Checkheaps
           6            0  Session Manager
         237          235  uauth
(other lines deleted for brevity)
```

show reload

セキュリティ アプライアンスのリロードのステータスを表示するには、特権 EXEC モードで ***show reload*** コマンドを使用します。

show reload

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

次の例は、リロードが 4 月 20 日、日曜日の午前 0 時（夜の 12 時）にスケジューリングされていることを示しています。

```
hostname# show reload
Reload scheduled for 00:00:00 PDT Sat April 20 (in 12 hours and 12 minutes)
```

関連コマンド

コマンド	説明
reload	コンフィギュレーションをリブートおよびリロードします。

show resource allocation

すべてのクラスとクラス メンバーにまたがってリソースごとにリソース割り当てを表示するには、特権 EXEC モードで **show resource allocation** コマンドを使用します。

show resource allocation [*detail*]

シンタックスの説明

detail	追加情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、リソース割り当てを表示しますが、実際に使用されているリソースは表示しません。実際のリソース使用状況を表示するには、**show resource usage** コマンドを使用します。

例

次に、**show resource allocation** コマンドの出力例を示します。ディスプレイには、各リソースの合計割り当て値が、絶対値および使用可能なシステム リソースのパーセンテージとして表示されます。

```
hostname# show resource allocation
Resource                  Total       % of Avail
 Conns [rate]             35000           N/A
 Inspects [rate]          35000           N/A
 Syslogs [rate]           10500           N/A
 Conns                   305000           30.50%
 Hosts                    78842           N/A
 SSH                         35           35.00%
 Telnet                      35           35.00%
 Xlates                   91749           N/A
 All                  unlimited
```

表 27-10 に、各フィールドの説明を示します。

表 27-10　show resource allocation のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Total	すべてのコンテキストで割り当てられるリソースの総量。この数量は、同時発生インスタンスまたは 1 秒間あたりのインスタンスの絶対数です。クラス定義でパーセンテージを指定した場合、セキュリティ アプライアンスはこの表示のためにパーセンテージを絶対数に変換します。
% of Avail	使用できる場合は、すべてのコンテキストで割り当てられるシステム リソース総量のパーセンテージ。リソースにシステム制限がない場合、このカラムには N/A（該当なし）と表示されます。

次に、**show resource allocation detail** コマンドの出力例を示します。

```
hostname# show resource allocation detail
Resource Origin:
    A    Value was derived from the resource 'all'
    C    Value set in the definition of this class
    D    Value set in default class
Resource         Class          Mmbrs  Origin      Limit      Total    Total %
Conns [rate]     default          all      CA  unlimited
                 gold               1       C      34000      34000     N/A
                 silver             1      CA      17000      17000     N/A
                 bronze             0      CA       8500
                 All Contexts:      3                         51000     N/A

Inspects [rate]  default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      10000      10000     N/A
                 bronze             0      CA       5000
                 All Contexts:      3                         10000     N/A

Syslogs [rate]   default          all      CA  unlimited
                 gold               1       C       6000       6000     N/A
                 silver             1      CA       3000       3000     N/A
                 bronze             0      CA       1500
                 All Contexts:      3                          9000     N/A

Conns            default          all      CA  unlimited
                 gold               1       C     200000     200000     20.00%
                 silver             1      CA     100000     100000     10.00%
                 bronze             0      CA      50000
                 All Contexts:      3                        300000     30.00%

Hosts            default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      26214      26214      N/A
                 bronze             0      CA      13107
                 All Contexts:      3                         26214      N/A

SSH              default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                           20     20.00%

Telnet           default          all       C          5
                 gold               1       D          5          5      5.00%
                 silver             1      CA         10         10     10.00%
                 bronze             0      CA          5
                 All Contexts:      3                           20     20.00%

Xlates           default          all      CA  unlimited
                 gold               1      DA  unlimited
                 silver             1      CA      23040      23040     N/A
                 bronze             0      CA      11520
                 All Contexts:      3                         23040     N/A

mac-addresses    default          all       C      65535
                 gold               1       D      65535      65535    100.00%
                 silver             1      CA       6553       6553      9.99%
                 bronze             0      CA       3276
                 All Contexts:      3                        137623    209.99%
```

表 27-11 に、各フィールドの説明を示します。

表 27-11　show resource allocation detail のフィールド

フィールド	説明
Resource	制限を課すことのできるリソースの名前。
Class	デフォルト クラスを含む、各クラスの名前。 すべてのコンテキスト フィールドには、すべてのクラスを含む合計値が表示されます。
Mmbrs	各クラスに割り当てられるコンテキストの数。
Origin	リソース制限の生成元。値は次のとおりです。 • A：この制限を個々のリソースとしてではなく、**すべて**のオプションを使用して設定します。 • C：この制限はメンバー クラスから生成されます。 • D：この制限はメンバー クラスでは定義されたのではなく、デフォルト クラスから生成されました。デフォルト クラスに割り当てられたコンテキストの場合、値は「D」ではなく「C」になります。 セキュリティ アプライアンスでは、「A」を「C」または「D」と組み合せることができます。
Limit	コンテキストごとのリソース制限（絶対数として）。クラス定義でパーセンテージを指定した場合、セキュリティ アプライアンスはこの表示のためにパーセンテージを絶対数に変換します。
Total	クラス内のすべてのコンテキストにわたって割り当てられているリソースの合計数。この数量は、同時発生インスタンスまたは 1 秒間あたりのインスタンスの絶対数です。リソースが無制限の場合、この表示はブランクです。
% of Avail	使用できる場合、クラス内のすべてのコンテキストにわたって割り当てられるシステム リソースの合計数のパーセンテージ。リソースが無制限の場合、この表示はブランクです。リソースにシステム制限がない場合、このカラムには N/A（該当なし）と表示されます。

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを追加します。
limit-resource	クラスに対してリソース制限を設定します。
show resource types	制限を設定できるリソース タイプを表示します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

show resource types

セキュリティ アプライアンスが使用状況の追跡対象にしているリソース タイプを表示するには、特権 EXEC モードで **show resource types** コマンドを使用します。

show resource types

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。
7.2(1)	このコマンドは、コンテキストごとに管理できる追加のリソース タイプを表示するように変更されました。

例

次の例では、リソース タイプを表示しています。

```
hostname# show resource types

Rate limited resource types:
  Conns           Connections/sec
  Inspects        Inspects/sec
  Syslogs         Syslogs/sec

Absolute limit types:
  Conns           Connections
  Hosts           Hosts
  Mac-addresses   MAC Address table entries
  ASDM            ASDM Connections
  SSH             SSH Sessions
  Telnet          Telnet Sessions
  Xlates          XLATE Objects
  All             All Resources
```

関連コマンド

コマンド	説明
clear resource usage	リソース使用状況の統計情報を消去します。
context	セキュリティ コンテキストを追加します。
show resource usage	セキュリティ アプライアンスのリソース使用状況を表示します。

show resource usage

セキュリティ アプライアンスまたはマルチモードの各コンテキストのリソース使用状況を表示するには、特権 EXEC モードで **show resource usage** コマンドを使用します。

show resource usage [**context** *context_name* | **top** *n* | **all** | **summary** | **system** | **detail**] [**resource** {[**rate**] *resource_name* | **all**}] [**counter** *counter_name* [*count_threshold*]]

シンタックスの説明

context *context_name*	（マルチモードのみ）統計情報を表示するコンテキストの名前を指定します。すべてのコンテキストを対象にするには、**all** を指定します。セキュリティ アプライアンスは、各コンテキストのリソース使用状況を一覧表示します。
count_threshold	使用回数を設定します。この回数以上に使用されているリソースが表示の対象になります。デフォルトは 1 です。リソースの使用状況がここで設定する回数を下回っている場合、そのリソースは表示されません。カウンタ名に **all** を指定した場合、*current_threshold* は現在の使用状況に適用されます。 **（注）** すべてのリソースを表示するには、*count_threshold* を **0** に設定します。
counter *counter_name*	次のカウンタ タイプの数を表示します。 • **current**：リソースのアクティブな同時発生インスタンス数、またはリソースの現在のレートを表示します。 • **peak**：ピーク時のリソースの同時発生インスタンス数、またはピーク時のリソースのレートを表示します。これは、統計情報が **clear resource usage** コマンドまたはデバイスのリブートによって最後に消去された時点から計測されます。 • **denied**：制限カラムに示されるリソース制限を越えたため拒否されたインスタンスの数を表示します。 • **all**：（デフォルト）すべての統計情報を表示します。
detail	管理できないリソースを含むすべてのリソースのリソース使用状況を表示します。たとえば、TCP 代行受信の数を表示できます。

resource [**rate**] *resource_name*	特定のリソースの使用状況を表示します。すべてのリソースを対象にするには、***all***（デフォルト）を指定します。リソースの使用状況を表示するには、**rate** を指定します。比率で測定されるリソースには、**conns**、**inspects**、および **syslogs** があります。これらのリソース タイプを指定する場合は、**rate** キーワードを指定する必要があります。conns リソースは、同時接続としても測定されます。1 秒間あたりの接続を表示するには、**rate** キーワードのみを使用します。 リソースには、次のタイプがあります。 • **asdm**：ASDM 管理セッション。 • **conns**：1 つのホストと複数の他のホスト間の接続を含む 2 つのホスト間の TCP または UDP 接続。 • **inspects**：アプリケーション検査。 • **hosts**：セキュリティ アプライアンスを通じて接続可能なホスト。 • **mac-addresses**：透過ファイアウォール モードの場合、MAC アドレス テーブルで許可された MAC アドレスの数。 • **ssh**：SSH セッション。 • **syslogs**：システム ログ メッセージ。 • **telnet**：Telnet セッション。 • **xlates**：NAT 変換。
summary	（マルチモードのみ）すべてのコンテキストの合算使用状況を表示します。
system	（マルチモードのみ）すべてのコンテキストの合算使用状況を表示します。ただし、コンテキストの合算制限値ではなくシステムのリソース制限値を表示します。
top *n*	（マルチモードのみ）指定したリソースの上位 *n* 人のユーザのコンテキストを表示します。このオプションでは、**resource all** ではなくリソース タイプを 1 つのみ指定する必要があります。

デフォルト

マルチ コンテキスト モードでは、デフォルト コンテキストは **all** です。すべてのコンテキストのリソース使用状況が表示されます。シングルモードの場合、コンテキスト名は無視され、出力では「context」は「System」として表示されます。

デフォルトのリソース名は、**all** です。すべてのリソース タイプが表示されます。

デフォルトのカウンタ名は、**all** です。すべての統計情報が表示されます。

デフォルトのカウントしきい値は、**1** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(1)	コンテキストごとにリソースを制限できるようになったため、このコマンドは現在では拒否されたリソースを表示します。

例

次に、**show resource usage context** コマンドの出力例を示します。この例では、admin コンテキストのリソース使用状況を表示しています。

```
hostname# show resource usage context admin

Resource              Current         Peak      Limit    Denied  Context
Telnet                      1            1          5         0  admin
Conns                      44           55        N/A         0  admin
Hosts                      45           56        N/A         0  admin
```

次に、**show resource usage summary** コマンドの出力例を示します。この例では、すべてのコンテキストとすべてのリソースのリソース使用状況が表示されます。ここでは、6 コンテキスト分の制限値が表示されています。

```
hostname# show resource usage summary

Resource              Current         Peak      Limit     Denied Context
Syslogs [rate]           1743         2132      12000(U)       0 Summary
Conns                     584          763     100000(S)       0 Summary
Xlates                   8526         8966      93400          0 Summary
Hosts                     254          254     262144          0 Summary
Conns [rate]              270          535      42200       1704 Summary
Inspects [rate]           270          535     100000(S)       0 Summary
U = Some contexts are unlimited and are not included in the total.
S = System: Combined context limits exceed the system limit; the system limit is
shown.
```

次に、**show resource usage system** コマンドの出力例を示します。この例では、すべてのコンテキストのリソース使用状況が表示されますが、合算のコンテキスト制限値ではなくシステム制限値が表示されています。

```
hostname# show resource usage system

Resource              Current         Peak      Limit    Denied  Context
Telnet                      3            5        100         0  System
SSH                         5            7        100         0  System
Conns                      40           55        N/A         0  System
Hosts                      44           56        N/A         0  System
```

次に、**show resource usage detail counter all 0** コマンドの出力例を示します。このコマンドは、ユーザが管理できるリソースだけでなく、すべてのリソースを表示します。

```
hostname# show resource usage detail counter all 0

Resource              Current         Peak      Limit        Denied Context
memory                1012028      1538428  unlimited             0 admin
chunk:aaa                   0            0  unlimited             0 admin
chunk:aaa_queue             0            0  unlimited             0 admin
chunk:acct                  0            0  unlimited             0 admin
chunk:channels             25           39  unlimited             0 admin
chunk:CIFS                  0            0  unlimited             0 admin
chunk:conn                  0            0  unlimited             0 admin
chunk:crypto-conn           0            0  unlimited             0 admin
chunk:dbgtrace              1            2  unlimited             0 admin
chunk:dhcpd-radix           0            0  unlimited             0 admin
chunk:dhcp-relay-r          0            0  unlimited             0 admin
chunk:dhcp-lease-s          0            0  unlimited             0 admin
chunk:dnat                  0            0  unlimited             0 admin
chunk:ether                 0            0  unlimited             0 admin
chunk:est                   0            0  unlimited             0 admin

...

Telnet                      0            0          5             0 admin
SSH                         1            1          5             0 admin
ASDM                        0            1          5             0 admin
Syslogs [rate]              0           68  unlimited             0 admin
aaa rate                    0            0  unlimited             0 admin
url filter rate             0            0  unlimited             0 admin
Conns                       1            6  unlimited             0 admin
Xlates                      0            0  unlimited             0 admin
tcp conns                   0            0  unlimited             0 admin
Hosts                       2            3  unlimited             0 admin
udp conns                   0            0  unlimited             0 admin
smtp-fixups                 0            0  unlimited             0 admin
Conns [rate]                0            7  unlimited             0 admin
establisheds                0            0  unlimited             0 admin
pps                         0            0  unlimited             0 admin
syslog rate                 0            0  unlimited             0 admin
bps                         0            0  unlimited             0 admin
Fixups [rate]               0            0  unlimited             0 admin
non tcp/udp conns           0            0  unlimited             0 admin
tcp-intercepts              0            0  unlimited             0 admin
globals                     0            0  unlimited             0 admin
np-statics                  0            0  unlimited             0 admin
statics                     0            0  unlimited             0 admin
nats                        0            0  unlimited             0 admin
ace-rules                   0            0        N/A             0 admin
aaa-user-aces               0            0        N/A             0 admin
filter-rules                0            0        N/A             0 admin
est-rules                   0            0        N/A             0 admin
aaa-rules                   0            0        N/A             0 admin
console-access-rul          0            0        N/A             0 admin
policy-nat-rules            0            0        N/A             0 admin
fixup-rules                 0            0        N/A             0 admin
aaa-uxlates                 0            0  unlimited             0 admin
CP-Traffic:IP               0            0  unlimited             0 admin
CP-Traffic:ARP              0            0  unlimited             0 admin
CP-Traffic:Fixup            0            0  unlimited             0 admin
CP-Traffic:NPCP             0            0  unlimited             0 admin
CP-Traffic:Unknown          0            0  unlimited             0 admin
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
clear resource usage	リソース使用状況の統計情報を消去します。
context	セキュリティ コンテキストを追加します。
limit-resource	クラスに対してリソース制限を設定します。
show resource types	リソース タイプのリストを表示します。

show rip database

RIP トポロジ データベースに格納されている情報を表示するには、特権 EXEC モードで **show rip database** コマンドを使用します。

show rip database [*ip_addr* [*mask*]]

シンタックスの説明

ip_addr	（オプション）指定したネットワーク アドレスの表示ルートを制限します。
mask	（オプション）オプションのネットワーク アドレスのネットワーク マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

RIP ルーティング関連の **show** コマンドは、セキュリティ アプライアンス上で特権モードで使用できます。RIP 関連の **show** コマンドを使用するには、RIP コンフィギュレーション モードである必要はありません。

RIP データベースには RIP を通じてラーニングされたルートがすべて含まれます。このデータベースに表示されるルートはルーティング テーブルには必ずしも表示されません。ルーティング テーブルにルーティング プロトコル データベースから値を挿入する方法については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次に、**show rip database** コマンドの出力例を示します。

```
hostname# show rip database

10.0.0.0/8    auto-summary
10.11.11.0/24    directly connected, GigabitEthernet0/2
10.1.0.0/8    auto-summary
10.11.0.0/16    int-summary
10.11.10.0/24    directly connected, GigabitEthernet0/3
192.168.1.1/24
    [2] via 10.11.10.5, 00:00:14, GigabitEthernet0/3
```

次に、ネットワーク アドレスとマスクを指定した、**show rip database** コマンドの出力例を示します。

```
Router# show rip database 172.19.86.0 255.255.255.0

172.19.86.0/24
    [1] via 172.19.67.38, 00:00:25, GigabitEthernet0/2
    [2] via 172.19.70.36, 00:00:14, GigabitEthernet0/3
```

関連コマンド

コマンド	説明
router rip	RIP ルーティングをイネーブルにし、グローバル RIP ルーティング パラメータを設定します。

show route

ルーティング テーブルを表示するには、特権 EXEC モードで **show route** コマンドを使用します。

show route [*interface_name* [*ip_address* [*netmask* [***static***]]]]

シンタックスの説明

static	（オプション）表示対象をスタティック ルートに限定します。
interface_name	（オプション）表示対象を指定のインターフェイスを使用するルート エントリに限定します。
ip_address	（オプション）表示対象を指定の宛先へのルートに限定します。
netmask	（オプション）*ip_address* に適用するネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show route** コマンドの出力例を示します。

```
hostname# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    10.86.194.0 255.255.255.0 is directly connected, outside
C    10.40.10.0 255.255.255.0 is directly connected, inside
C    192.168.2.0 255.255.255.0 is directly connected, faillink
C    192.168.3.0 255.255.255.0 is directly connected, statelink
```

次に、ASA5505 適応型セキュリティ アプライアンスの show route コマンドの出力例を示します。この例には、個々のユーザ認証用に VPN ハードウェア クライアントが使用する内部ループバック アドレスが表示されます。

```
hostname(config)# show route

Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 10.86.194.1 to network 0.0.0.0

C    127.1.0.0 255.255.0.0 is directly connected, _internal_loopback
C    10.86.194.0 255.255.254.0 is directly connected, outside
S*   0.0.0.0 0.0.0.0 [1/0] via 10.86.194.1, outside
```

関連コマンド

コマンド	説明
clear configure route	**connect** キーワードを含んでいない **route** コマンドをコンフィギュレーションから削除します。
route	スタティックまたはデフォルト ルートを作成します。
show running-config route	実行コンフィギュレーションの route コマンドを表示します。

CHAPTER 28

show running-config コマンド～ show running-config isakmp コマンド

show running-config

セキュリティ アプライアンス上で実行されているコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config** コマンドを使用します。

show running-config [**all**] [*command*]

シンタックスの説明

all	デフォルト値を含めて、実行コンフィギュレーション全体を表示します。
command	特定のコマンドに関連付けられているコンフィギュレーションを表示します。

デフォルト

引数もキーワードも指定しない場合は、デフォルト以外に設定されているセキュリティ アプライアンス コンフィギュレーション全体が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されました。

使用上のガイドライン

show running-config コマンドは、セキュリティ アプライアンス上の現在の実行コンフィギュレーションを表示します。

running-config キーワードは、**show running-config** コマンド内だけで使用できます。このキーワードを **no** および **clear** と共に使用することはできません。また、スタンドアロン コマンドとして使用することもできません。CLI ではサポートされないコマンドとして処理されます。**?**、**no ?**、または **clear ?** のいずれかのキーワードを入力した場合、**running-config** キーワードはコマンド リストに表示されません。

(注) デバイス　マネージャのコマンドを使用してセキュリティ　アプライアンスに接続するかセキュリティ アプライアンスを設定した後は、デバイス マネージャのコマンドがコンフィギュレーションに表示されます。

例

次の例は、セキュリティ アプライアンス上で実行されているコンフィギュレーションを表示する方法を示しています。

```
hostname# show running-config
: Saved
:
XXX Version X.X(X)
names
!
interface Ethernet0
 nameif test
 security-level 10
 ip address 10.10.88.50 255.255.255.254
!
interface Ethernet1
 nameif inside
 security-level 100
 ip address 10.86.194.176 255.255.254.0
!
interface Ethernet2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet4
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Ethernet5
 shutdown
 no nameif
 security-level 0
 no ip address
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname XXX
domain-name XXX.com
boot system flash:/cdisk.bin
ftp mode passive
pager lines 24
mtu test 1500
mtu inside 1500
```

```
monitor-interface test
monitor-interface inside
ASDM image flash:ASDM
no ASDM history enable
arp timeout 14400
route inside 0.0.0.0 0.0.0.0 10.86.194.1 1
timeout xlate 3:00:00
timeout conn 2:00:00 half-closed 1:00:00 udp 0:02:00 icmp 1:00:00 rpc 1:00:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
http server enable
http 0.0.0.0 0.0.0.0 inside
no snmp-server location
no snmp-server contact
snmp-server enable traps snmp
fragment size 200 test
fragment chain 24 test
fragment timeout 5 test
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
telnet 0.0.0.0 0.0.0.0 inside
telnet timeout 1440
ssh timeout 5
console timeout 0
group-policy todd internal
!
class-map inspection_default
 match default-inspection-traffic
!
!
policy-map xxx_global_fw_policy
 class inspection_default
  inspect dns
  inspect ftp
  inspect h323 h225
  inspect h323 ras
  inspect http
  inspect ils
  inspect mgcp
  inspect netbios
  inspect rpc
  inspect rsh
  inspect rtsp
  inspect sip
  inspect skinny
  inspect sqlnet
  inspect tftp
  inspect xdmcp
  inspect ctiqbe
  inspect cuseeme
  inspect icmp
!
terminal width 80
service-policy xxx_global_fw_policy global
Cryptochecksum:bfecf4b9d1b98b7e8d97434851f57e14
: end
```

関連コマンド

コマンド	説明
configure	セキュリティ アプライアンスを端末から設定します。

show running-config aaa

実行コンフィギュレーションの AAA コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config aaa** コマンドを使用します。

show running-config aaa [***accounting*** | ***authentication*** | ***authorization*** | ***mac-exempt*** | ***proxy-limit***]

シンタックスの説明

accounting	（オプション）アカウンティング関連の AAA コンフィギュレーションを表示します。
authentication	（オプション）認証関連の AAA コンフィギュレーションを表示します。
authorization	（オプション）認可関連の AAA コンフィギュレーションを表示します。
mac-exempt	（オプション）MAC アドレス免除の AAA コンフィギュレーションを表示します。
proxy-limit	（オプション）ユーザ 1 人あたりに許可されている同時プロキシ接続の数を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config aaa** コマンドの出力例を示します。

```
hostname# show running-config aaa
aaa authentication match infrastructure_authentication_radiusvrs infrastructure
radiusvrs
aaa accounting match infrastructure_authentication_radiusvrs infrastructure radiusvrs
aaa authentication secure-http-client
aaa local authentication attempts max-fail 16
hostname#
```

関連コマンド

コマンド	説明
aaa authentication match	アクセス リストによって識別されるトラフィックに対する認証をイネーブルにします。
aaa authorization match	アクセス リストによって識別されるトラフィックに対する認可をイネーブルにします。
aaa accounting match	アクセス リストによって識別されるトラフィックに対するアカウンティングをイネーブルにします。
aaa mac-exempt	認証と認可を免除される MAC アドレスの事前定義済みリストを使用することを指定します。
aaa proxy-limit	ユーザ 1 人あたりに許可する同時プロキシ接続の最大数を設定して、uauth セッション制限を設定します。

show running-config aaa-server

AAA サーバのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config aaa-server** コマンドを使用します。

show running-config [**all**] **aaa-server** [*server-tag*] [**(***interface-name***)**] [**host** *hostname*]

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。
host *hostname*	（オプション）AAA サーバ統計情報の表示対象となる、特定のホストのシンボリック名または IP アドレス。
(interface-name)	（オプション）AAA サーバが常駐するネットワーク インターフェイス。
server-tag	（オプション）サーバグループのシンボリック名。

デフォルト

server-tag 値を省略すると、すべての AAA サーバのコンフィギュレーションが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

このコマンドは、特定のサーバグループの設定を表示するために使用します。明示的に設定されている値に加えてデフォルト値も表示するには、**all** パラメータを使用します。

例

デフォルト AAA サーバグループの実行コンフィギュレーションを表示するには、次のコマンドを使用します。

```
hostname(config)# show running-config default aaa-server

aaa-server group1 protocol tacacs+ accounting-mode simultaneous
reactivation-mode depletion deadtime 10
max-failed-attempts 4
hostname(config)#
```

関連コマンド

コマンド	説明
show aaa-server	AAA サーバの統計情報を表示します。
clear configure aaa-server	AAA サーバのコンフィギュレーションを消去します。

show running-config aaa-server host

特定のサーバの AAA サーバ統計情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config aaa-server** コマンドを使用します。

show/clear aaa-server

show running-config [**all**] **aaa-server** *server-tag* [(*interface-name*)] **host** *hostname*

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。
server-tag	サーバグループのシンボリック名。

デフォルト

default キーワードを省略すると、明示的に設定されているコンフィギュレーション値のみが表示され、デフォルト値は表示されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

このコマンドは、特定のサーバグループの統計情報を表示するために使用します。明示的に設定されている値に加えてデフォルト値も表示するには、default パラメータを使用します。

例

サーバグループ svrgrp1 の実行コンフィギュレーションを表示するには、次のコマンドを使用します。

```
hostname(config)# show running-config default aaa-server svrgrp1
hostname(config)#
```

関連コマンド

コマンド	説明
show running-config aaa-server	指定したサーバ、グループ、またはプロトコルの AAA サーバ設定を表示します。
clear configure aaa	すべてのグループのすべての AAA サーバの設定を削除します。

show running-config access-group

アクセス グループの情報を表示するには、特権 EXEC モードで **show running-config access-group** コマンドを使用します。

show running-config access-group

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show running-config access-group** コマンドの出力例を示します。

```
hostname# show running-config access-group
access-group 100 in interface outside
```

関連コマンド

コマンド	説明
access-group	アクセス リストをインターフェイスにバインドします。
clear configure access-group	すべてのインターフェイスからアクセス グループを削除します。

show running-config access-list

セキュリティ アプライアンス上で実行されているアクセス リストのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config access-list** コマンドを使用します。

show running-config [***default***] **access-list** [**alert-interval** | **deny-flow-max**]

show running-config [***default***] **access-list** *id* [*saddr_ip***]**

シンタックスの説明

alert-interval	syslog メッセージ 106001 を生成する警告間隔を表示します。このメッセージは、システムが拒否フローの最大数に達したことを警告するものです。
deny-flow-max	作成できる同時拒否フローの最大数を表示します。
id	表示するアクセス リストを指定します。
saddr_ip	指定した送信元 IP アドレスを保持しているアクセス リスト要素を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

show running-config access-list コマンドを使用すると、セキュリティ アプライアンス上の現在のアクセス リスト実行コンフィギュレーションを表示できます。

例

次に、**show running-config access-list** コマンドの出力例を示します。

```
hostname# show running-config access-list
access-list allow-all extended permit ip any any
```

関連コマンド

コマンド	説明
access-list ethertype	トラフィックを EtherType に基づいて制御するためのアクセス リストを設定します。
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list ethertype	トラフィックを EtherType に基づいて制御するためのアクセス リストを設定します。
clear access-list	アクセス リスト カウンタを消去します。
clear configure access-list	実行コンフィギュレーションからアクセス リストを消去します。

show running-config alias

コンフィギュレーションに含まれている、デュアル NAT コマンドで使用する重複アドレスを表示するには、特権 EXEC モードで **show running-config alias** コマンドを使用します。

show running-config alias {*interface_name***}**

シンタックスの説明

interface_name	destination_ip が上書きする、内部ネットワーク インターフェイス名。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例は、エイリアス情報を表示する方法を示しています。

```
hostname# show running-config alias
```

関連コマンド

コマンド	説明
alias	エイリアスを作成します。
clear configure alias	エイリアスを削除します。

show running-config arp

arp コマンドで作成し、実行コンフィギュレーションに含まれているスタティック ARP エントリを表示するには、特権 EXEC モードで **show running-config arp** コマンドを使用します。

show running-config arp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config arp** コマンドの出力例を示します。

```
hostname# show running-config arp
arp inside 10.86.195.11 0008.023b.9893
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show arp	ARP テーブルを表示します。
show arp statistics	ARP 統計情報を表示します。

show running-config arp timeout

実行コンフィギュレーションの ARP タイムアウト コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config arp timeout** コマンドを使用します。

show running-config arp timeout

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show arp timeout** から変更されました。

例

次に、**show running-config arp timeout** コマンドの出力例を示します。

```
hostname# show running-config arp timeout
arp timeout 20000 seconds
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp timeout	セキュリティ アプライアンスが ARP テーブルを再構築するまでの時間を設定します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。

show running-config arp-inspection

実行コンフィギュレーションの ARP 検査コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config arp-inspection** コマンドを使用します。

show running-config arp-inspection

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show arp timeout** から変更されました。

例

次に、**show running-config arp-inspection** コマンドの出力例を示します。

```
hostname# show running-config arp-inspection

arp-inspection inside1 enable no-flood
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	透過ファイアウォール モードで、ARP パケットを調べて ARP スプーフィングを防止します。
clear configure arp-inspection	ARP 検査のコンフィギュレーションを消去します。
firewall transparent	ファイアウォール モードを透過に設定します。
show arp statistics	ARP 統計情報を表示します。

show running-config asdm

実行コンフィギュレーションに含まれている **asdm** コマンドを表示するには、特権 EXEC モードで **show running-config asdm** コマンドを使用します。

show running-config asdm [**group** | **location**]

シンタックスの説明

group	（オプション）実行コンフィギュレーションに含まれている **asdm group** コマンドだけを表示します。
location	（オプション）実行コンフィギュレーションに含まれている **asdm location** コマンドだけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show running-config pdm** コマンドから **show running-config asdm** コマンドに変更されました。

使用上のガイドライン

asdm コマンドをコンフィギュレーションから削除するには、**clear configure asdm** コマンドを使用します。

（注） マルチ コンテキスト モードで動作しているセキュリティ アプライアンスでは、**show running-config asdm group** コマンドと **show running-config asdm location** コマンドを使用できるのはシステム実行スペース内だけです。

例

次に、**show running-config asdm** コマンドの出力例を示します。

```
hostname# show running-config asdm
asdm image flash:/ASDM
asdm history enable
hostname#
```

関連コマンド

コマンド	説明
show asdm image	現在の ASDM イメージ ファイルを表示します。

show running-config auth-prompt

現在の認証プロンプト チャレンジ テキストを表示するには、グローバル コンフィギュレーション モードで show running-config auth-prompt コマンドを使用します。

show running-config [default] auth-prompt

シンタックスの説明

default	（オプション）デフォルトの認証プロンプト チャレンジ テキストを表示します。

デフォルト

設定されている認証プロンプト チャレンジ テキストを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、CLI ガイドラインに準拠するようにこのリリースで修正されました。

使用上のガイドライン

show running-config auth-prompt コマンドは、**auth-prompt** コマンドで認証プロンプトを設定した後に、現在のプロンプト テキストを表示するために使用します。

例

次に、**show running-config auth-prompt** コマンドの出力例を示します。

```
hostname(config)# show running-config auth-prompt
auth-prompt prompt Please login:
auth-prompt accept You're in!
auth-prompt reject Try again.
hostname(config)#
```

関連コマンド

auth-prompt	ユーザ認可プロンプトを設定します。
clear configure auth-prompt	ユーザ認可プロンプトをデフォルト値にリセットします。

show running-config banner

指定したバナー、およびそのバナーに設定されているすべての行を表示するには、特権 EXEC モードで **show running-config banner** コマンドを使用します。

show running-config banner [**exec | login | motd**]

シンタックスの説明

exec	（オプション）イネーブル プロンプトを表示する前にバナーを表示します。
login	（オプション）ユーザが Telnet を使用してセキュリティ アプライアンスにアクセスしたときに、パスワード ログイン プロンプトを表示する前にバナーを表示します。
motd	（オプション）「今日のお知らせ」バナーを表示します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	***running-config*** キーワードが追加されました。

使用上のガイドライン

show running-config banner コマンドは、キーワードで指定したバナー、およびそのバナーに設定されているすべての行を表示します。キーワードを指定しない場合は、すべてのバナーが表示されます。

例

次の例は、「今日のお知らせ」（motd）バナーを表示する方法を示しています。

```
hostname# show running-config banner motd
```

関連コマンド

コマンド	説明
banner	バナーを作成します。
clear configure banner	バナーを削除します。

show running-config class

リソース クラス コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config class** コマンドを使用します。

show running-config class

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show running-config class** コマンドの出力例を示します。

```
hostname# show running-config class

class default
  limit-resource All 0
  limit-resource Mac-addresses 65535
  limit-resource ASDM 5
  limit-resource SSH 5
  limit-resource Telnet 5
```

関連コマンド

コマンド	説明
class	リソース クラスを設定します。
clear configure class	クラス コンフィギュレーションを消去します。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスに対してリソース制限を設定します。
member	リソース クラスにコンテキストを割り当てます。

show running-config class-map

クラス マップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config class-map** コマンドを使用します。

show running-config [***all***] **class-map** [*class_map_name* | **type** {**management** | **regex** | **inspect** [*protocol*]}]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべてのコマンドを表示します。
class_map_name	（オプション）クラス マップ名の実行コンフィギュレーションを表示します。
inspect	（オプション）検査クラス マップを表示します。
management	（オプション）管理クラス マップを表示します。
protocol	（オプション）表示するアプリケーション マップのタイプを指定します。指定できるタイプは、次のとおりです。 • **dns** • **ftp** • **h323** • **http** • **im** • **p2p-donkey** • **sip**
regex	（オプション）正規表現クラス マップを表示します。
type	（オプション）表示するクラス マップのタイプを指定します。レイヤ 3/4 クラス マップを表示する場合は、タイプを指定しないでください。

デフォルト

match any コマンドを 1 つだけ含んでいる **class-map class-default** コマンドが、デフォルトのクラス マップです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

例

次に、**show running-config class-map** コマンドの出力例を示します。

```
hostname# show running-config class-map
class-map tcp-port
  match port tcp eq ftp
hostname#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。

show running-config client-update

グローバル クライアント アップデート コンフィギュレーション情報を表示するには、グローバル コンフィギュレーション モード、またはトンネル グループ ipsec アトリビュート コンフィギュレーション モードで **show running-config client-update** コマンドを使用します。

show running-config client-update

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec アトリビュート コンフィギュレーション モードが追加されました。

使用上のガイドライン

グローバル クライアント アップデート コンフィギュレーション情報を表示するには、このコマンドを使用します。

例

次の例は、グローバル コンフィギュレーション モードでの **show running-config client-update** コマンドと、クライアント アップデートがイネーブルにされたコンフィギュレーションの出力を示しています。

```
hostname(config)# show running-config client-update
hostname(config)# client-update enable
```

関連コマンド

コマンド	説明
clear configure client-update	client-update コンフィギュレーション全体を消去します。
client-update	client-update を設定します。

show running-config clock

実行コンフィギュレーションのクロック コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config clock** コマンドを使用します。

show running-config [**all**] **clock**

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての **clock** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

all キーワードを指定した場合は、**clock summer-time** コマンドの正確な日時もオフセットのデフォルト設定（オフセットを設定しなかった場合）と共に表示されます。

例

次に、**show running-config clock** コマンドの出力例を示します。**clock summer-time** コマンドのみ設定されていました。

```
hostname# show running-config clock
clock summer-time EDT recurring
```

次に、**show running-config all clock** コマンドの出力例を示します。設定されていない **clock timezone** コマンドについてはデフォルト設定が表示され、**clock summer-time** コマンドについては詳細な情報が表示されています。

```
hostname# show running-config all clock
clock timezone UTC 0
clock summer-time EDT recurring 1 Sun Apr 2:00 last Sun Oct 2:00 60
```

関連コマンド

コマンド	説明
clock set	セキュリティ アプライアンスのクロックを手動で設定します。
clock summer-time	夏時間を表示する日付範囲を設定します。
clock timezone	時間帯を設定します。

show running-config command-alias

設定されているコマンド エイリアスを表示するには、特権 EXEC モードで ***show running-config command-alias*** コマンドを使用します。

show running-config [**all**] **command-alias**

シンタックスの説明

all	（オプション）デフォルト値を含めて、設定されているすべてのコマンド エイリアスを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

all キーワードを入力しない場合は、デフォルト以外のコマンド エイリアスのみが表示されます。

例

次の例では、デフォルト値を「含めて」、セキュリティ アプライアンス上に設定されているすべてのコマンド エイリアスを表示しています。

```
hostname# show running-config all command-alias
command-alias exec h help
command-alias exec lo logout
command-alias exec p ping
command-alias exec s show
command-alias exec save copy running-config startup-config
```

次の例では、デフォルト値を「除いて」、セキュリティ アプライアンス上に設定されているすべてのコマンド エイリアスを表示しています。

```
hostname# show running-config command-alias
command-alias exec save copy running-config startup-config
hostname#
```

関連コマンド

コマンド	説明
command-alias	コマンド エイリアスを作成します。
clear configure command-alias	デフォルト以外のコマンド エイリアスをすべて削除します。

show running-config compression

実行コンフィギュレーションに含まれている圧縮コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config compression** コマンドを使用します。

show running-config compression

デフォルト

このコマンドには、デフォルトの動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

例

この例では、実行コンフィギュレーション内の圧縮コンフィギュレーションを表示しています。

```
hostname# show running-config compression
compression svc http-comp
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続、WebVPN 接続、およびポート転送接続に対して圧縮をイネーブルにします。

show running-config console timeout

コンソール接続のタイムアウト値を表示するには、特権 EXEC モードで **show running-config console timeout** コマンドを使用します。

show running-config console timeout

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、コンソール接続のタイムアウト設定を表示する方法を示しています。

```
hostname# show running-config console timeout
console timeout 0
```

関連コマンド

コマンド	説明
console timeout	セキュリティ アプライアンスへのコンソール接続のアイドル タイムアウトを設定します。
clear configure console	コンソール接続の設定をデフォルトにリセットします。

show running-config context

システム実行スペースのコンテキスト コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config context** コマンドを使用します。

show running-config context

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config context** コマンドの出力例を示します。

```
hostname# show running-config context

admin-context admin
context admin
  allocate-interface GigabitEthernet0/0
  config-url flash:/admin.cfg
!

context A
  allocate-interface GigabitEthernet0/1
  config-url flash:/A.cfg
!
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
allocate-interface	コンテキストにインターフェイスを割り当てます。
changeto	コンテキスト間またはコンテキストとシステム実行スペースの間で切り替えを行います。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードに入ります。

show running-config crypto

IPSec、暗号マップ、ダイナミック暗号マップ、および ISAKMP を含めた暗号コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto** コマンドを使用します。

show running-config crypto

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

特権 EXEC モードで入力した次の例では、すべての暗号コンフィギュレーション情報を表示しています。

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto dynamic-map

ダイナミック暗号マップを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto dynamic-map** コマンドを使用します。

show running-config crypto dynamic-map

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、ダイナミック暗号マップに関するすべてのコンフィギュレーション情報を表示しています。

```
hostname(config)# show running-config crypto dynamic-map

Crypto Map Template "dyn1" 10

        access-list 152 permit ip host 172.21.114.67 any
        Current peer: 0.0.0.0
        Security association lifetime: 4608000 kilobytes/120 seconds
        PFS (Y/N): N
        Transform sets={ tauth, t1, }
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto ipsec

IPSec コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto ipsec** コマンドを使用します。

show running-config crypto ipsec

シンタックスの説明

このコマンドには、デフォルトの動作も値もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで発行した次の例では、IPSec コンフィギュレーションに関する情報を表示しています。

```
hostname(config)# show running-config crypto ipsec
crypto ipsec transform-set ttt esp-3des esp-md5-hmac
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto isakmp

ISAKMP コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto isakmp** コマンドを使用します。

show running-config crypto isakmp

シンタックスの説明

このコマンドには、デフォルトの動作も値もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show running-config isakmp** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**show running-config crypto isakmp** コマンドに置き換えられました。

例

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP コンフィギュレーションに関する情報を表示しています。

```
hostname<config># show running-config crypto isakmp
crypto isakmp enable inside
crypto isakmp policy 1 authentication pre-share
crypto isakmp policy 1 encryption 3des
crypto isakmp policy 1 hash md5
crypto isakmp policy 1 group 2
crypto isakmp policy 1 lifetime 86400
hostname<config>#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure crypto isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear crypto isakmp sa	IKE ランタイム SA データベースを消去します。
crypto isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show crypto isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config crypto map

すべての暗号マップのすべてのコンフィギュレーションを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config crypto map** コマンドを使用します。

show running-config crypto map

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

特権 EXEC モードで入力した次の例では、すべての暗号マップのすべてのコンフィギュレーション情報を表示しています。

```
hostname# show running-config crypto map
crypto map abc 1 match address xyz
crypto map abc 1 set peer 209.165.200.225
crypto map abc 1 set transform-set ttt
crypto map abc interface test
hostname#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

show running-config ddns

実行コンフィギュレーションの DDNS アップデート方式を表示するには、特権 EXEC モードで **show running-config ddns** コマンドを使用します。

show running-config [**all**] **ddns** [**update**]

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。
update	（オプション）DDNS アップデート方式の情報を表示することを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、名前に test を持つ実行コンフィギュレーションの DDNS 方式を表示します。

```
hostname# show running-config all ddns | grep test
ddns update method test
hostname#
```

関連コマンド

コマンド	説明
ddns（**DDNS アップデート方式モード**）	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update（インターフェイス コンフィギュレーション モード）	セキュリティ アプライアンス インターフェイスを、DDNS アップデート方式または DDNS アップデート ホスト名に関連付けます。
ddns update method（グローバル コンフィギュレーション モード）	DNS のリソース レコードを動的にアップデートするための方式を作成します。
show ddns update interface	設定済みの各 DDNS 方式に関連付けられているインターフェイスを表示します。
show ddns update method	設定済みの各 DDNS 方式について、タイプおよび間隔を表示します。DDNS アップデートを実行する DHCP サーバ。

show running-config dhcp-client

実行コンフィギュレーションの DHCP クライアント アップデート パラメータを表示するには、特権 EXEC モードで **show running-config dhcp-client** コマンドを使用します。

show running-config [**all**] **dhcp-client**

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、A レコードと PTR レコードの両方のアップデートを指定する実行コンフィギュレーションの DHCP クライアント アップデート パラメータを表示します。

```
hostname# show running-config all dhcp-client | grep both
dhcp-client update dns server both
hostname#
```

関連コマンド

コマンド	説明
dhcp-client update dns	DHCP クライアントが DHCP サーバに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバによる DDNS アップデートの実行をイネーブルにします。
clear configure dhcp-client	DHCP クライアント コンフィギュレーションを消去します。

show running-config dhcpd

DHCP コンフィギュレーションを表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config dhcpd** コマンドを使用します。

show running-config ***dhcpd***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show dhcpd** コマンドから **show running-config dhcpd** コマンドに変更されました。

使用上のガイドライン

show running-config dhcpd コマンドは、実行コンフィギュレーションに入力されている DHCP のコマンドを表示します。DHCP のバインディング、状態、および統計情報を表示するには、**show dhcpd** コマンドを使用します。

例

次に、**show running-config dhcpd** コマンドの出力例を示します。

```
hostname# show running-config dhcpd

dhcpd address 10.0.1.100-10.0.1.108 inside
dhcpd lease 3600
dhcpd ping_timeout 750
dhcpd dns 209.165.201.2 209.165.202.129
dhcpd enable inside
```

関連コマンド

コマンド	説明
clear configure dhcpd	DHCP サーバの設定をすべて削除します。
debug dhcpd	DHCP サーバに対するデバッグ情報を表示します。
show dhcpd	DHCP のバインディング、統計情報、または状態情報を表示します。

show running-config dhcprelay

現在の DHCP リレー エージェント コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config dhcprelay** コマンドを使用します。

show running-config *dhcprelay*

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config dhcprelay コマンドは、現在の DHCP リレー エージェント コンフィギュレーションを表示します。DHCP リレー エージェントのパケット統計情報を表示するには、**show dhcprelay statistics** コマンドを使用します。

例

次に、**show running-config dhcprelay** コマンドの出力例を示します。

```
hostname(config)# show running-config dhcprelay

dhcprelay server 10.1.1.1
dhcprelay enable inside
dhcprelay timeout 90
```

関連コマンド

コマンド	説明
clear configure dhcprelay	DHCP リレー エージェントの設定をすべて削除します。
clear dhcprelay statistics	DHCP リレー エージェント統計情報カウンタを消去します。
debug dhcprelay	DHCP リレー エージェントに関するデバッグ情報を表示します。
show dhcprelay statistics	DHCP リレー エージェントの統計情報を表示します。

show running-config dns

実行コンフィギュレーションの DNS コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config dns** コマンドを使用します。

show running-config dns

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config dns** コマンドの出力例を示します。

```
hostname# show running-config dns
dns domain-lookup inside
dns name-server
dns retries 2
dns timeout 15
dns name-server 10.1.1.1
```

関連コマンド

コマンド	説明
dns domain-lookup	セキュリティ アプライアンスがネーム ルックアップを実行できるようにします。
dns name-server	DNS サーバのアドレスを設定します。
dns retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
dns timeout	次の DNS サーバを試すまでに待つ時間を指定します。
show dns-hosts	DNS キャッシュを表示します。

show running-config dns server-group

実行コンフィギュレーションの DNS コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config dns** コマンドを使用します。

show [**all**] **running-config dns server-group** [*name*]

シンタックスの説明

all	1 つまたはすべての dns サーバ グループのデフォルトおよび明示的に設定されたコンフィギュレーション情報を表示します。
name	コンフィギュレーション情報を表示する dns サーバ グループの名前を指定します。

デフォルト

dns サーバ グループ名を省略すると、このコマンドは既存の dns サーバ グループ コンフィギュレーションをすべて表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1	このコマンドが導入されました。

例

次に、**show running-config dns server-group** コマンドの出力例を示します。

```
hostname# show running-config dns server-group
dns domain-lookup inside
dns server-group DefaultDNS
 name-server 90.1.1.22
 domain-name frqa.cisco.com
dns server-group writers1
 retries 10
 timeout 3
 name-server 10.86.194.61
 domain-name doc-group
hostname#
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバ グループを設定できる DNS サーバ グループ モードに入ります。

show running-config domain-name

実行コンフィギュレーションのドメイン名コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config domain-name** コマンドを使用します。

show running-config domain-name

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show domain-name** から変更されました。

例

次に、**show running-config domain-name** コマンドの出力例を示します。

```
hostname# show running-config domain-name
example.com
```

関連コマンド

コマンド	説明
domain-name	デフォルトのドメイン名を設定します。
hostname	セキュリティ アプライアンスのホスト名を設定します。

show running-config enable

暗号化されたイネーブル パスワードを表示するには、特権 EXEC モードで **show running-config enable** コマンドを使用します。

show running-config enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show enable** コマンドから変更されました。

使用上のガイドライン

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードは ***encrypted*** キーワードと共に表示され、パスワードが暗号化されていることが示されます。

例

次に、**show running-config enable** コマンドの出力例を示します。

```
hostname# show running-config enable
enable password 2AfK9Kjr3BE2/J2r level 10 encrypted
enable password 8Ry2YjIyt7RRXU24 encrypted
```

関連コマンド

コマンド	説明
disable	特権 EXEC モードを終了します。
enable	特権 EXEC モードに入ります。
enable password	イネーブル パスワードを設定します。

show running-config established

確立済みの接続に基づいて許可されている着信接続を表示するには、特権 EXEC モードで **show running-config established** コマンドを使用します。

show running-config established

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

このコマンドに使用上のガイドラインはありません。

例

この例は、確立済みの接続に基づいて許可されている着信接続を表示する方法を示しています。

```
hostname# show running-config established
```

関連コマンド

コマンド	説明
established	確立されている接続に基づくポート上のリターン接続を許可します。
clear configure established	確立されたコマンドをすべて削除します。

show running-config failover

コンフィギュレーションに含まれている **failover** コマンドを表示するには、特権 EXEC モードで **show running-config failover** コマンドを使用します。

show running-config [***all***] **failover**

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての failover コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config failover コマンドは、実行コンフィギュレーションに含まれている **failover** コマンドを表示します。**monitor-interface** コマンドおよび **join-failover-group** コマンドは表示しません。

例

次の例では、フェールオーバーを設定する前のデフォルト フェールオーバー コンフィギュレーションを表示しています。

```
hostname# show running-config all failover
no failover
failover lan unit secondary
failover polltime unit 15 holdtime 45
failover polltime interface 15
failover interface policy 1
hostname#
```

関連コマンド

コマンド	説明
show failover	フェールオーバーの状態と統計情報を表示します。

show running-config filter

フィルタリング コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config filter** コマンドを使用します。

show running-config filter

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config filter コマンドは、セキュリティ アプライアンスのフィルタリング コンフィギュレーションを表示します。

例

次に、**show running-config filter** コマンドの出力例を示します。セキュリティ アプライアンスのフィルタリング コンフィギュレーションが表示されています。

```
hostname# show running-config filter
!
filter activex 80 10.86.194.170 255.255.255.255 10.1.1.0 255.255.255.224
!
```

この例では、アドレス 10.86.194.170 について、ポート 80 で ActiveX フィルタリングがイネーブルになっています。

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter ftp	URL フィルタリング サーバによってフィルタリングされる FTP トラフィックを指定します。
filter https	Websense サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。

show running-config fips

セキュリティ アプライアンス上で実行されている FIPS コンフィギュレーションを表示するには、**show running-config fips** コマンドを使用します。

show running-config fips

シンタックスの説明

fips	FIPS-2 準拠情報

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

show running-config fips コマンドを使用すると、現在の実行 FIPS コンフィギュレーションを表示できます。**running-config** キーワードは、**show running-config fips** コマンド内だけで使用します。このキーワードを no または clear と共に使用することはできません。また、スタンドアロン コマンドとして使用することもできません。そのような使用方法はサポートされていません。また、**?**、**no ?**、または **clear ?** のいずれかのキーワードを入力した場合、**running-config** キーワードはコマンド リストに表示されません。

例

```
sw8-ASA(config)# show running-config fips
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に格納されているシステムまたはモジュールの FIPS コンフィギュレーション情報を消去します。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、および設定をディセーブルにします。
fips enable	システムまたはモジュールで FIPS に準拠するためのポリシー チェックをイネーブルまたはディセーブルにします。
fips self-test poweron	パワーオン セルフテストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。

show running-config fragment

フラグメント データベースの現在のコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config fragment** コマンドを使用します。

show running-config fragment [*interface*]

シンタックスの説明

interface	（オプション）セキュリティ アプライアンスのインターフェイスを指定します。

デフォルト

インターフェイスが指定されていなければ、このコマンドはすべてのインターフェイスに適用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config fragment コマンドは、フラグメント データベースの現在のコンフィギュレーションを表示します。インターフェイス名が指定されていれば、指定したインターフェイスに常駐するデータベースの情報だけを表示します。インターフェイス名が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。

show running-config fragment コマンドは、次の情報を表示するために使用します。

- Size：**size** キーワードで設定されるパケットの最大数。この値は、インターフェイス上で許容されるフラグメントの最大数です。
- Chain：**chain** キーワードで設定される 1 つのパケットのフラグメントの最大数。
- Timeout：**timeout** キーワードで設定される最大秒数。これは、フラグメント化されたパケット全体が到着するのを待つ最大秒数です。タイマーは、パケットの最初のフラグメントが到着すると始動します。指定した秒数以内にパケットのすべてのフラグメントが到着しない場合、それまでに受信したパケット フラグメントはすべて廃棄されます。

例

次の例は、すべてのインターフェイス上のフラグメント データベースの状態を表示する方法を示しています。

```
hostname# show running-config fragment
fragment size 200 inside
fragment chain 24 inside
fragment timeout 5 inside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

次の例は、名前が「outside」で始まるインターフェイス上にあるフラグメント データベースの状態を表示する方法を示しています。

(注) この例では、「outside1」、「outside2」、および「outside3」という名前のインターフェイスが表示されています。

```
hostname# show running-config fragment outside
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
fragment size 200 outside2
fragment chain 24 outside2
fragment timeout 5 outside2
fragment size 200 outside3
fragment chain 24 outside3
fragment timeout 5 outside3
```

次の例は、「outside1」というインターフェイス上にあるフラグメント データベースについてのみ、状態を表示する方法を示しています。

```
hostname# show running-config fragment outside1
fragment size 200 outside1
fragment chain 24 outside1
fragment timeout 5 outside1
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの運用データを消去します。
fragment	特別なパケット フラグメント化の管理を提供して、NFS との互換性を改善します。
show fragment	IP フラグメント再構成モジュールの運用データを表示します。

show running-config ftp mode

FTP に関して設定されているクライアント モードを表示するには、特権 EXEC モードで **show running-config ftp mode** コマンドを使用します。

show running-config ftp mode

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config ftp mode コマンドは、FTP サーバにアクセスするときにセキュリティ アプライアンスが使用するクライアント モードを表示します。

例

次に、**show running-config ftp-mode** コマンドの出力例を示します。

```
hostname# show running-config ftp-mode
!
ftp-mode passive
!
```

関連コマンド

コマンド	説明
copy	イメージ ファイルまたはコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。
debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
ftp mode passive	FTP サーバにアクセスするときにセキュリティ アプライアンスが使用する FTP クライアント モードを設定します。

show running-config global

コンフィギュレーションに含まれている **global** コマンドを表示するには、特権 EXEC モードで **show running-config global** コマンドを使用します。

show running-config global

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

例

次に、**show running-config global** コマンドの出力例を示します。

```
hostname# show running-config global
global (outside1) 10 interface
```

関連コマンド

コマンド	説明
clear configure global	コンフィギュレーションから **global** コマンドを削除します。
global	グローバル アドレス プールに対してエントリを作成します。

show running-config group-delimiter

トンネルのネゴシエーション中に受信したユーザ名に基づいてグループ名を解析するときに使用する、現在のデリミタを表示するには、グローバル コンフィギュレーション モード、またはトンネル グループ ipsec アトリビュート コンフィギュレーション モードで **show running-config group-delimiter** コマンドを使用します。

show running-config group-delimiter

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•
トンネル グループ ipsec アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	トンネル グループ ipsec アトリビュート コンフィギュレーション モードが追加されました。

使用上のガイドライン

このコマンドは、現在設定されているグループデリミタを表示するために使用します。

例

次の例は、**show running-config group-delimiter** コマンドおよびその出力を示しています。

```
hostname(config)# show running-config group-delimiter
group-delimiter @
```

関連コマンド

コマンド	説明
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定します。

show running-config group-policy

特定のグループ ポリシーの実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config group-policy** コマンドを使用するときに、グループ ポリシーの名前を付加します。すべてのグループ ポリシーの実行コンフィギュレーションを表示するには、特定のグループ ポリシーを指定せずにこのコマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] group-policy [*name***]**

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルト値を含めて表示します。
name	（オプション）グループ ポリシーの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、FirstGroup というグループ ポリシーの実行コンフィギュレーションをデフォルト値を含めて表示する方法を示しています。

```
hostname# show running-config all group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーを作成、編集、または削除します。
group-policy attributes	指定したグループ ポリシーの AVP を設定できるグループ ポリシー アトリビュート モードに入ります。
clear config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。

show running-config http

現在の一連の設定済み http コマンドを表示するには、特権 EXEC モードで **show running-config http** コマンドを使用します。

show running-config http

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

例

次の出力例は、**show running-config http** コマンドを使用する方法を示しています。

```
hostname# show running-config http
http server enabled
0.0.0.0 0.0.0.0 inside
```

関連コマンド

コマンド	説明
clear http	HTTP コンフィギュレーションを削除します。HTTP サーバをディセーブルにし、HTTP サーバにアクセスできるホストを削除します。
http	IP アドレスとサブネット マスクによって、HTTP サーバにアクセスできるホストを指定します。ホストが HTTP サーバにアクセスするときに通過するセキュリティ アプライアンス インターフェイスを指定します。
http authentication-certificate	セキュリティ アプライアンスへの HTTPS 接続を確立するユーザに証明書による認証を要求します。
http redirect	セキュリティ アプライアンスが HTTP 接続を HTTPS にリダイレクトするように指定します。
http server enable	HTTP サーバをイネーブルにします。

show running-config icmp

ICMP トラフィックに対して設定されているアクセス規則を表示するには、特権 EXEC モードで **show running-config icmp** コマンドを使用します。

show running-config icmp *map_name*

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config icmp コマンドは、ICMP トラフィックに対して設定されているアクセス規則を表示します。

例

次に、**show running-config icmp** コマンドの出力例を示します。

```
hostname# show running-config icmp
!
icmp permit host 172.16.2.15 echo-reply outside
icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
icmp permit any unreachable outside
!
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションを消去します。
debug icmp	ICMP に関するデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

show running-config imap4s

IMAP4S の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config imap4s** コマンドを使用します。

show running-config [all] imap4s

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルト値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
Webvpn	•	—	•	—	—

例

次に、**show running-config imap4s** コマンドの出力例を示します。

```
hostname# show running-config imap4s

imap4s
 server 10.160.105.2
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all imap4s

imap4s
 port 993
 server 10.160.105.2
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

関連コマンド

コマンド	説明
clear configure imap4s	IMAP4S コンフィギュレーションを削除します。
imap4s	IMAP4S 電子メール プロキシのコンフィギュレーションを作成または編集します。

show running-config interface

実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config interface** コマンドを使用します。

show running-config [**all**] **interface** [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての **interface** コマンドを表示します。
interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ　コンテキスト　モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスのコンフィギュレーションが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

インターフェイス名をシステム実行スペースで使用することはできません。これは、**nameif** コマンドはコンテキスト内でのみ使用できるためです。同様に、**allocate-interface** コマンドを使用してインターフェイス ID をマッピング名にマッピングした場合、そのマッピング名はコンテキスト内でのみ使用できます。

例

次に、**show running-config interface** コマンドの出力例を示します。この例では、すべてのインターフェイスの実行コンフィギュレーションを表示しています。GigabitEthernet0/2 インターフェイスと GigabitEthernet0/3 インターフェイスはまだ設定されていないため、デフォルトのコンフィギュレーションが表示されます。Management0/0 インターフェイスについても、デフォルトの設定が表示されています。

```
hostname# show running-config interface
!
interface GigabitEthernet0/0
 no shutdown
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 no shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
interface GigabitEthernet0/1.1
 vlan 101
 no shutdown
 nameif dmz
 security-level 50
 ip address 10.50.1.1 255.255.255.0
 mac-address 000C.F142.4CDE standby 020C.F142.4CDE
!
interface GigabitEthernet0/2
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface GigabitEthernet0/3
 shutdown
 no nameif
 security-level 0
 no ip address
!
interface Management0/0
 shutdown
 no nameif
 security-level 0
 no ip address
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear configure interface	インターフェイス コンフィギュレーションを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
nameif	インターフェイス名を設定します。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show running-config ip address

実行コンフィギュレーションの IP アドレス コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip address** コマンドを使用します。

show running-config ip address [*physical_interface*[**.***subinterface*] | *mapped_name* | *interface_name*]

シンタックスの説明

interface_name	（オプション）**nameif** コマンドで設定したインターフェイス名を指定します。
mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスの IP アドレス コンフィギュレーションが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名またはインターフェイス名はコンテキスト内でのみ指定できます。

透過ファイアウォール モードの場合は、インターフェイスを指定しないでください。このコマンドは、管理 IP アドレスのみを表示するものであり、透過ファイアウォールではインターフェイスに IP アドレスが関連付けられていないためです。

このコマンドの表示内容では、**nameif** コマンドと **security-level** コマンドのコンフィギュレーションも示されます。

例

次に、**show running-config ip address** コマンドの出力例を示します。

```
hostname# show running-config ip address
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイス コンフィギュレーションを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
ip address	インターフェイスの IP アドレスを設定します。または、透過ファイアウォールの管理 IP アドレスを設定します。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。

show running-config ip audit attack

実行コンフィギュレーションの **ip audit attack** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit attack** コマンドを使用します。

show running-config ip audit attack

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show ip audit attack** から変更されました。

例

次に、**show running-config ip audit attack** コマンドの出力例を示します。

```
hostname# show running-config ip audit attack
ip audit attack action drop
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit info

実行コンフィギュレーションの **ip audit info** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit info** コマンドを使用します。

show running-config ip audit info

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show ip audit info** から変更されました。

例

次に、**show running-config ip audit info** コマンドの出力例を示します。

```
hostname# show running-config ip audit info
ip audit info action drop
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit interface

実行コンフィギュレーションの **ip audit interface** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit interface** コマンドを使用します。

show running-config ip audit interface [*interface_name*]

シンタックスの説明

interface_name	（オプション）インターフェイス名を指定します。

デフォルト

インターフェイス名を指定しない場合は、すべてのインターフェイスのコンフィギュレーションが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show ip audit interface** から変更されました。

例

次に、**show running-config ip audit interface** コマンドの出力例を示します。

```
hostname# show running-config ip audit interface
ip audit interface inside insidepolicy
ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit name

実行コンフィギュレーションの **ip audit name** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit name** コマンドを使用します。

show running-config ip audit name [*name* [***info*** | ***attack***]]

シンタックスの説明

attack	（オプション）攻撃シグニチャに対する名前付き監査ポリシーのコンフィギュレーションを表示します。
info	（オプション）情報シグニチャに対する名前付き監査ポリシーのコンフィギュレーションを表示します。
name	（オプション）**ip audit name** コマンドを使用して作成した監査ポリシー名のコンフィギュレーションを表示します。

デフォルト

名前を指定しない場合は、すべての監査ポリシーのコンフィギュレーションが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show ip audit name** から変更されました。

例

次に、**show running-config ip audit name** コマンドの出力例を示します。

```
hostname# show running-config ip audit name
ip audit name insidepolicy1 attack action alarm
ip audit name insidepolicy2 info action alarm
ip audit name outsidepolicy1 attack action reset
ip audit name outsidepolicy2 info action alarm
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip audit signature

実行コンフィギュレーションの **ip audit signature** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip audit signature** コマンドを使用します。

show running-config ip audit signature [*signature_number*]

シンタックスの説明

signature_number	（オプション）このシグニチャ番号に対応するコンフィギュレーションが存在する場合は、表示します。サポートされているシグニチャのリストについては、**ip audit signature** コマンドを参照してください。

デフォルト

番号を指定しない場合は、すべてのシグニチャのコンフィギュレーションが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show ip audit signature** から変更されました。

例

次に、**show running-config ip audit signature** コマンドの出力例を示します。

```
hostname# show running-config ip audit signature
ip audit signature 1000 disable
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	インターフェイスに監査ポリシーを割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。

show running-config ip local pool

IP アドレス プールを表示するには、特権 EXEC モードで **show running-config ip local pool** コマンドを使用します。

show running-config ip local pool [*poolname*]

シンタックスの説明

poolname	（オプション）IP アドレス プールの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config ip local pool** コマンドの出力例を示します。

```
hostname(config)# show running-config ip local pool firstpool

Pool             Begin           End             Mask            Free    In use
firstpool               10.20.30.40     10.20.30.50     255.255.255.0      11
    0
Available Addresses:
10.20.30.40
10.20.30.41
10.20.30.42
10.20.30.43
10.20.30.44
10.20.30.45
10.20.30.46
10.20.30.47
10.20.30.48
10.20.30.49
10.20.30.50

hostname(config)#
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
ip local pool	IP アドレス プールを設定します。

show running-config ip verify reverse-path

実行コンフィギュレーションの **ip verify reverse-path** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ip verify reverse-path** コマンドを使用します。

show running-config ip verify reverse-path [interface *interface_name*]

シンタックスの説明

interface *interface_name*	（オプション）指定したインターフェイスのコンフィギュレーションを表示します。

デフォルト

このコマンドは、すべてのインターフェイスのコンフィギュレーションを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show ip verify reverse-path** から変更されました。

例

次に、**show ip verify statistics** コマンドの出力例を示します。

```
hostname# show running-config ip verify reverse-path
ip verify reverse-path interface inside
ip verify reverse-path interface outside
ip verify reverse-path interface dmz
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コンフィギュレーションを消去します。
clear ip verify statistics	Unicast RPF の統計情報を消去します。
ip verify reverse-path	Unicast Reverse Path Forwarding 機能をイネーブルにして IP スプーフィングを防止します。
show ip verify statistics	Unicast RPF の統計情報を表示します。

show running-config ipv6

実行コンフィギュレーションに含まれている IPv6 のコマンドを表示するには、特権 EXEC モードで **show running-config ipv6** コマンドを使用します。

show running-config [**all**] **ipv6**

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、実行コンフィギュレーションに含まれているすべての **ipv6** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config ipv6** コマンドの出力例を示します。

```
hostname# show running-config ipv6
ipv6 unicast-routing
ipv6 route vlan101 ::/0 fec0::65:0:0:a0a:6575
ipv6 access-list outside_inbound_ipv6 permit ip any any
ipv6 access-list vlan101_inbound_ipv6 permit ip any any
hostname#
```

関連コマンド

コマンド	説明
debug ipv6	IPv6 デバッグ メッセージを表示します。
show ipv6 access-list	IPv6 アクセス リストを表示します。
show ipv6 interface	IPv6 インターフェイスのステータスを表示します。
show ipv6 route	IPv6 ルーティング テーブルの内容を表示します。
show ipv6 traffic	IPv6 トラフィックの統計情報を表示します。

show running-config isakmp

ISAKMP コンフィギュレーション全体を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config isakmp** コマンドを使用します。

show running-config isakmp

シンタックスの説明

このコマンドには、デフォルトの動作も値もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**show running-config isakmp** コマンドが導入されました。
7.2(1)	このコマンドは廃止されました。**show running-config crypto isakmp** コマンドに置き換えられました。

例

グローバル コンフィギュレーション モードで発行した次の例では、ISAKMP コンフィギュレーションに関する情報を表示しています。

```
hostname(config)# show running-config isakmp
isakmp enable inside
isakmp policy 1 authentication pre-share
isakmp policy 1 encryption 3des
isakmp policy 1 hash md5
isakmp policy 1 group 2
isakmp policy 1 lifetime 86400
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションを消去します。
clear configure isakmp policy	ISAKMP ポリシー コンフィギュレーションをすべて消去します。
clear isakmp sa	IKE ランタイム SA データベースを消去します。
isakmp enable	IPSec ピアがセキュリティ アプライアンスと通信するインターフェイス上の ISAKMP ネゴシエーションをイネーブルにします。
show isakmp sa	追加情報を含め、IKE ランタイム SA データベースを表示します。

CHAPTER 29

show running-config ldap コマンド～ show running-config wccp コマンド

show running-config ldap

実行 LDAP アトリビュート マップ内の LDAP アトリビュート名と値マッピングを表示するには、特権 EXEC モードで **show running-config ldap** コマンドを使用します。

show running-config [**all**] **ldap attribute-map** *name*

シンタックスの説明

all	すべての LDAP アトリビュート マップを表示します。
name	表示する個々の LDAP アトリビュート マップを指定します。

デフォルト

デフォルトでは、すべてのアトリビュート マップ、マッピング名、およびマッピング値が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンス上で実行されているアトリビュート マップに含まれる LDAP のアトリビュート名と値マッピングを表示するには、このコマンドを使用します。**all** オプションを使用してすべてのアトリビュート マップを表示するか、マップ名を指定して単一のアトリビュート マップを表示できます。**all** オプションも LDAP アトリビュート マップ名も入力しない場合は、すべてのアトリビュート マップ、マッピング名、およびマッピング値が表示されます。

例

特権 EXEC モードで入力した次の例では、指定された実行アトリビュート マップ「myldapmap」のアトリビュート名と値マッピングが表示されています。

```
hostname# show running-config ldap attribute-map myldapmap
map-name Hours cVPN3000-Access-Hours
map-value Hours workDay Daytime
```

次のコマンドは、すべての実行アトリビュート マップ内のすべてのアトリビュート名と値マッピングを表示します。

```
hostname# show running-config all ldap attribute-map
```

関連コマンド

コマンド	説明
ldap attribute-map（グローバル コンフィギュレーション モード）	ユーザ定義のアトリビュート名を Cisco LDAP アトリビュート名にマッピングするために、LDAP アトリビュート マップを作成し、名前を付けます。
ldap-attribute-map（AAA サーバ ホスト モード）	LDAP アトリビュート マップを LDAP サーバにバインドします。
map-name	ユーザ定義の LDAP アトリビュート名を、Cisco LDAP アトリビュート名にマッピングします。
map-value	ユーザ定義のアトリビュート値を、Cisco アトリビュートにマッピングします。
clear configure ldap attribute-map	すべての LDAP アトリビュート マップを削除します。

show running-config logging

現在実行されているすべてのロギング コンフィギュレーションを表示するには、特権 EXEC モードで ***show running-config logging*** コマンドを使用します。

show running-config [all] logging [level | disabled]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、ロギング コンフィギュレーションを表示します。
disabled	（オプション）ディセーブルになっているシステム ログ メッセージのコンフィギュレーションのみを表示します。
level	（オプション）デフォルト以外のセキュリティ レベルを持つシステム ログ メッセージのコンフィギュレーションのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1) (1)	このコマンドが、**show logging** コマンドから変更されました。

例

次に、***show running-config logging disabled*** コマンドの例を示します。

```
hostname# show running-config logging disabled

no logging message 720067
```

関連コマンド

コマンド	説明
logging message	ロギングを設定します。
show logging	ログ バッファおよびその他のロギング設定を表示します。

show running-config mac-address

実行コンフィギュレーションの **mac-address auto** コンフィギュレーションを表示するには、特権 EXEC モードで **how running-config mac-address** コマンドを使用します。

show running-config mac-address

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show running-config mac-address** コマンドの出力例を示します。

```
hostname# show running-config mac-address
no mac-address auto
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address	物理インターフェイスまたはサブインターフェイスの MAC アドレス（アクティブおよびスタンバイ）を手動で設定します。マルチ コンテキスト モードでは、同じインターフェイスに対して、コンテキストごとにそれぞれ別の MAC アドレスを設定することができます。
mac-address auto	マルチ コンテキスト モードの共有インターフェイスの MAC アドレス（アクティブおよびスタンバイ）を自動生成します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

show running-config mac-address-table

実行コンフィギュレーションの **mac-address-table static** および **mac-address-table aging-time** のコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config mac-address-table** コマンドを使用します。

show running-config mac-address-table

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config mac-learn** コマンドの出力例を示します。

```
hostname# show running-config mac-address-table
mac-address-table aging-time 50
mac-address-table static inside1 0010.7cbe.6101
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

show running-config mac-learn

実行コンフィギュレーションの **mac-learn** コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config mac-learn** コマンドを使用します。

show running-config mac-learn

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config mac-learn** コマンドの出力例を示します。

```
hostname# show running-config mac-learn
mac-learn disable
```

関連コマンド

コマンド	説明
firewall transparent	ファイアウォール モードを透過に設定します。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	ダイナミック エントリとスタティック エントリを含め、MAC アドレス テーブルを表示します。

show running-config mac-list

以前に **mac-list** コマンドで指定した MAC アドレスのリストを MAC リスト番号で指定して表示するには、特権 EXEC モードで **show running-config mac-list** コマンドを使用します。

show running-config mac-list *id*

シンタックスの説明

id	16 進形式の MAC アドレス リスト番号です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

show running-config aaa コマンドは、AAA コンフィギュレーションの一部として **mac-list** コマンド文を表示します。

例

次の例は、*id* が adc と等しい MAC アドレス リストを表示する方法を示しています。

```
hostname(config)# show running-config mac-list adc
mac-list adc permit 00a0.cp5d.0282 ffff.ffff.ffff
mac-list adc deny 00a1.cp5d.0282 ffff.ffff.ffff
mac-list ac permit 0050.54ff.0000 ffff.ffff.0000
mac-list ac deny 0061.54ff.b440 ffff.ffff.ffff
mac-list ac deny 0072.54ff.b440 ffff.ffff.ffff
```

関連コマンド

コマンド	説明
mac-list	先頭一致検索を使用して MAC アドレスのリストを追加します。
clear configure mac-list	指定した **mac-list** コマンド文を削除します。
show running-config aaa	実行されている AAA コンフィギュレーションの値を表示します。

show running-config management-access

管理アクセス用に設定されている内部インターフェイスの名前を表示するには、特権 EXEC モードで ***show running-config management-access*** コマンドを使用します。

show running-config management-access

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

management-access コマンドを使用すると、*mgmt_if* で指定したファイアウォール インターフェイスの IP アドレスを使用して、内部管理インターフェイスを定義できます（インターフェイス名は **nameif** コマンドによって定義され、**show interface** コマンドの出力で引用符 " " に囲まれて表示されます）。

例

次の例は、「inside」という名前のファイアウォール インターフェイスを管理アクセス インターフェイスとして設定し、結果を表示する方法を示しています。

```
hostname# management-access inside
hostname# show running-config management-access
management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	セキュリティ アプライアンスの管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
management-access	管理アクセス用の内部インターフェイスを設定します。

show running-config monitor-interface

実行コンフィギュレーションに含まれているすべての **monitor-interface** コマンドを表示するには、特権 EXEC モードで **show running-config monitor-interface** コマンドを使用します。

show running-config [all] monitor-interface

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての **monitor-interface** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

monitor-interface コマンドは、デフォルトではすべての物理インターフェイスでイネーブルになっています。このデフォルト設定を表示するには、このコマンドと共に ***all*** キーワードを使用する必要があります。

例

次に、**show running-config monitor-interface** コマンドの出力例を示します。最初の例では ***all*** キーワードを使用しないでコマンドが入力されているため、モニタリングがイネーブルのインターフェイスだけが出力に表示されます。2 番目の例では ***all*** キーワードを使用してコマンドが入力されているため、デフォルトの **monitor-interface** コンフィギュレーションも表示されます。

```
hostname# show running-config monitor-interface
no monitor-interface outside
hostname#
hostname# show running-config all monitor-interface
monitor-interface inside
no monitor-interface outside
hostname#
```

関連コマンド

コマンド	説明
monitor-interface	フェールオーバー用に指定されているインターフェイスのヘルス モニタリングをイネーブルにします。
clear configure monitor-interface	実行コンフィギュレーション内の **no monitor-interface** コマンドを削除し、デフォルトのインターフェイス ヘルス モニタリング状態に戻します。

show running-config mroute

実行コンフィギュレーションに含まれているスタティック マルチキャスト ルート テーブルを表示するには、特権 EXEC モードで **show running-config mroute** コマンドを使用します。

show running-config mroute [*dst* [*src*]]

シンタックスの説明

dst	マルチキャスト グループの Class D アドレス。
src	マルチキャスト送信元の IP アドレス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

例

次に、**show running-config mroute** コマンドの出力例を示します。

```
hostname# show running-config mroute
```

関連コマンド

コマンド	説明
mroute	スタティック マルチキャスト ルートを設定します。

show running-config mtu

Maximum Transmission Unit（MTU; 最大伝送ユニット）の現在のブロック サイズを表示するには、特権 EXEC モードで **show running-config mtu** コマンドを使用します。

show running-config mtu [*interface_name*]

シンタックスの説明

interface_name	（オプション）内部または外部のネットワーク インターフェイス名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	—	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show running-config mtu** コマンドの出力例を示します。

```
hostname# show running-config mtu
mtu outside 1500
mtu inside 1500
mtu dmz 1500
hostname# show running-config mtu outside
mtu outside 1500
```

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスの設定済み最大伝送ユニット値を消去します。
mtu	インターフェイスの最大伝送ユニットを指定します。

show running-config multicast-routing

実行コンフィギュレーションに **multicast-routing** コマンドが含まれている場合に、それらのコマンドを表示するには、特権 EXEC モードで **show running-config multicast-routing** コマンドを使用します。

show running-config ***multicast-routing***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config multicast-routing コマンドは、実行コンフィギュレーションに含まれている **multicast-routing** コマンドを表示します。**multicast-routing** コマンドを実行コンフィギュレーションから削除するには、**clear configure multicast-routing** コマンドを入力します。

例

次に、**show running-config multicast-routing** コマンドの出力例を示します。

```
hostname# show running-config multicast-routing

multicast-routing
```

関連コマンド

コマンド	説明
clear configure multicast-routing	**multicast-routing** コマンドを実行コンフィギュレーションから削除します。
multicast-routing	セキュリティ アプライアンス上のマルチキャスト ルーティングをイネーブルにします。

show running-config name

IP アドレスに関連付けられている（**name** コマンドで設定した）名前のリストを表示するには、特権 EXEC モードで **show running-config name** コマンドを使用します。

show running-config name

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、IP アドレスに関連付けられている名前のリストを表示する方法を示しています。

```
hostname# show running-config name
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
name	名前を IP アドレスに関連付けます。

show running-config nameif

実行コンフィギュレーションのインターフェイス名コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config nameif** コマンドを使用します。

show running-config nameif [*physical_interface*[**.***subinterface*] | *mapped_name*]

シンタックスの説明

mapped_name	（オプション）マルチ コンテキスト モードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	（オプション）インターフェイス ID（***gigabit*ethernet0/1** など）を指定します。使用できる値については、**interface** コマンドを参照してください。
subinterface	（オプション）論理サブインターフェイスを示す 1 ～ 4294967293 の整数を指定します。

デフォルト

インターフェイスを指定しない場合は、すべてのインターフェイスのインターフェイス名コンフィギュレーションが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show nameif** から変更されました。

使用上のガイドライン

マルチ コンテキスト モードで、**allocate-interface** コマンドを使用してインターフェイス ID をマッピングした場合、そのマッピング名はコンテキスト内でだけ指定できます。

このコマンドの表示内容では、**security-level** コマンドのコンフィギュレーションも示されます。

例

次に、**show running-config nameif** コマンドの出力例を示します。

```
hostname# show running-config nameif
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
!
interface GigabitEthernet0/1
 nameif test
 security-level 0
!
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
clear configure interface	インターフェイス コンフィギュレーションを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
nameif	インターフェイス名を設定します。
security-level	インターフェイスのセキュリティ レベルを設定します。

show running-config names

IP アドレスから名前への変換を表示するには、特権 EXEC モードで **show running-config names** コマンドを使用します。

show running-config names

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　***names*** コマンドと共に使用します。

例　次の例は、IP アドレスから名前への変換を表示する方法を示しています。

```
hostname# show running-config names
name 192.168.42.3 sa_inside
name 209.165.201.3 sa_outside
```

関連コマンド

コマンド	説明
clear configure name	名前のリストをコンフィギュレーションから消去します。
name	名前を IP アドレスに関連付けます。
names	IP アドレスから名前への変換をイネーブルにします。変換の内容は、**name** コマンドで設定できます。
show running-config name	IP アドレスに関連付けられている名前のリストを表示します。

show running-config nat

ネットワークに関連付けられているグローバル IP アドレスのプールを表示するには、特権 EXEC モードで **show running-config nat** コマンドを使用します。

show running-config nat [*interface_name*] [*nat_id*]

シンタックスの説明

interface_name	（オプション）ネットワーク インターフェイスの名前。
nat_id	（オプション）ホスト グループまたはネットワークの ID。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

このコマンドは、UDP プロトコルの最大接続値を表示します。UDP 最大接続値が設定されていない場合、この値はデフォルトでは常に 0 と表示され、適用されません。

（注） 透過モードでは、有効となる NAT ID は 0 のみです。

例

次の例は、ネットワークに関連付けられているグローバル IP アドレスのプールを表示する方法を示しています。

```
hostname# show running-config nat
nat (inside) 1001 10.7.2.0 255.255.255.224 0 0
nat (inside) 1001 10.7.2.32 255.255.255.224 0 0
nat (inside) 1001 10.7.2.64 255.255.255.224 0 0
nat (inside) 1002 10.7.2.96 255.255.255.224 0 0
nat (inside) 1002 10.7.2.128 255.255.255.224 0 0
nat (inside) 1002 10.7.2.160 255.255.255.224 0 0
nat (inside) 1003 10.7.2.192 255.255.255.224 0 0
nat (inside) 1003 10.7.2.224 255.255.255.224 0 0
```

関連コマンド

コマンド	説明
clear configure nat	NAT コンフィギュレーションを削除します。
nat	ネットワークをグローバル IP アドレス プールに関連付けます。

show running-config nat-control

NAT コンフィギュレーションの要件を表示するには、特権 EXEC モードで **show running-config nat-control** コマンドを使用します。

show running-config nat-control

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config nat-control** コマンドの出力例を示します。

```
hostname# show running-config nat-control
no nat-control
```

関連コマンド

コマンド	説明
nat	他のインターフェイスのグローバル アドレスに変換される、1 つのインターフェイス上のアドレスを定義します。
nat-control	NAT 規則を設定していない場合でも、内部ホストが外部ネットワークと通信することを許可します。

show running-config ntp

実行コンフィギュレーションの NTP コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config ntp** コマンドを使用します。

show running-config ntp

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config ntp** コマンドの出力例を示します。

```
hostname# show running-config ntp
ntp authentication-key 1 md5 test2
ntp authentication-key 2 md5 test
ntp trusted-key 1
ntp trusted-key 2
ntp server 10.1.1.1 key 1
ntp server 10.2.1.1 key 2 prefer
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバと同期するための暗号化認証キーを設定します。
ntp server	NTP サーバを指定します。
ntp trusted-key	NTP サーバとの認証で、パケット内で使用するセキュリティ アプライアンスのキー ID を指定します。
show ntp status	NTP アソシエーションのステータスを表示します。

show running-config object-group

現在のオブジェクト グループを表示するには、特権 EXEC モードで **show running-config object-group** コマンドを使用します。

show running-config [**all**] **object-group** [**protocol** | **service** | **network** | **icmp-type** | **id** *obj_grp_id*]

シンタックスの説明

icmp-type	（オプション）ICMP タイプ オブジェクト グループを表示します。
id obj_grp_id	（オプション）指定したオブジェクト グループを表示します。
network	（オプション）ネットワーク オブジェクト グループを表示します。
protocol	（オプション）プロトコル オブジェクト グループを表示します。
service	（オプション）サービス オブジェクト グループを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show running-config object-group** コマンドの出力例を示します。

```
hostname# show running-config object-group
object-group protocol proto_grp_1
    protocol-object udp
    protocol-object tcp
object-group service eng_service tcp
    port-object eq smtp
    port-object eq telnet
object-group icmp-type icmp-allowed
    icmp-object echo
    icmp-object time-exceeded
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。

show running-config passwd

暗号化されたログイン パスワードを表示するには、特権 EXEC モードで **show running-config passwd** コマンドを使用します。

show running-config {**passwd** | **password**}

シンタックスの説明

***passwd*	*password***	どちらのコマンドでも入力できます。これらは互いにエイリアス関係にあります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show passwd** コマンドから変更されました。

使用上のガイドライン

パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。パスワードは ***encrypted*** キーワードと共に表示され、パスワードが暗号化されていることが示されます。

例

次に、**show running-config passwd** コマンドの出力例を示します。

```
hostname# show running-config passwd
passwd 2AfK9Kjr3BE2/J2r encrypted
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードを消去します。
enable	特権 EXEC モードに入ります。
enable password	イネーブル パスワードを設定します。
passwd	ログイン パスワードを設定します。
show curpriv	現在ログインしているユーザの名前および特権レベルを表示します。

show running-config pim

実行コンフィギュレーションに含まれている PIM のコマンドを表示するには、特権 EXEC モードで **show running-config pim** コマンドを使用します。

show running-config ***pim***

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config pim コマンドは、グローバル コンフィギュレーション モードで入力された **pim** コマンドを表示します。インターフェイス コンフィギュレーション モードで入力された **pim** コマンドは表示しません。インターフェイス コンフィギュレーション モードで入力された **pim** コマンドを表示するには、**show running-config interface** コマンドを入力します。

例

次に、**show running-config pim** コマンドの出力例を示します。

```
hostname# show running-config pim

pim old-register-checksum
pim spt-threshold infinity
```

関連コマンド

コマンド	説明
clear configure pim	**pim** コマンドを実行コンフィギュレーションから削除します。
show running-config interface	インターフェイス コンフィギュレーション モードで入力されたインターフェイス コンフィギュレーション コマンドを表示します。

show running-config policy-map

すべてまたはデフォルトのポリシー マップ コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config policy-map** コマンドを使用します。

show running-config [all] policy-map [*policy_map_name* | **type inspect** [*protocol*]]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべてのコマンドを表示します。
policy_map_name	（オプション）ポリシー マップ名の実行コンフィギュレーションを表示します。
protocol	（オプション）表示する検査ポリシー マップのタイプを指定します。指定できるタイプは、次のとおりです。 • **dcerpc** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **mgcp** • **netbios** • **p2p** • **radius-accounting** • **sip** • **skinny** • **snmp**
type inspect	（オプション）検査ポリシー マップを表示します。

デフォルト

all キーワードを省略すると、明示的に設定したポリシー マップ コンフィギュレーションだけが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

all キーワードを指定すると、明示的に設定したポリシー マップ コンフィギュレーションに加えて、デフォルトのポリシー マップ コンフィギュレーションも表示されます。

例

次に、**show running-config policy-map** コマンドの出力例を示します。

```
hostname# show running-config policy-map
!
policy-map localmap1
    description this is a test.
    class firstclass
    priority
    ids promiscuous fail0close
    set connection random-seq# enable
    class class-default
!
```

関連コマンド

コマンド	説明
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
clear configure policy-map	ポリシー コンフィギュレーション全体を削除します。

show running-config pop3s

POP3S の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config pop3s** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] pop3s

シンタックスの説明

all	実行コンフィギュレーションを、デフォルト値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
Webvpn	•	—	•	—	—

例

次に、**show running-config pop3s** コマンドの出力例を示します。

```
hostname# show running-config pop3s

pop3s
 server 10.160.102.188
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all pop3s

pop3s
 port 995
 server 10.160.102.188
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
```

関連コマンド

コマンド	説明
clear configure pop3s	POP3S コンフィギュレーションを削除します。
pop3s	POP3S 電子メール プロキシのコンフィギュレーションを作成または編集します。

show running-config port-forward

転送された TCP ポートを通じて WebVPN ユーザがアクセスできるアプリケーションのセットを表示するには、特権 EXEC モードで **show running-config port-forward** コマンドを使用します。

show running-config [all] port-forward

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルト値を含めて表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次に、**show running-config port-forward** コマンドの出力例を示します。

```
hostname# show running-config port-forward

port-forward Telnet 3500 10.148.1.5 23
port-forward Telnet 3501 10.148.1.81 23
port-forward Telnet 3502 10.148.1.82 23
port-forward SSH2 4976 10.148.1.81 22
port-forward SSH2 4977 10.148.1.85 22
port-forward Apps1 10143 flask.CompanyA.com 143
port-forward Apps1 10110 flask.CompanyA.com 110
port-forward Apps1 10025 flask.CompanyA.com 25
port-forward Apps1 11533 sametime-im.CompanyA.com 1533
port-forward Apps1 10022 ddts.CompanyA.com 22
port-forward Apps1 54000 10.148.1.5 23
port-forward Apps1 58000 vpn3060-1 23
port-forward Apps1 58001 vpn3005-1 23
hostname#
```

関連コマンド

コマンド	説明
clear configure port-forward	すべてのポート転送コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドだけを削除します。
port-forward	WebVPN ユーザがアクセスできるアプリケーションのセットを設定します。
port-forward（webvpn）	ユーザまたはグループ ポリシーの WebVPN アプリケーション アクセスをイネーブルにします。

show running-config prefix-list

実行コンフィギュレーションに含まれている **prefix-list** コマンドを表示するには、特権 EXEC モードで **show running-config prefix-list** コマンドを使用します。

show running-config prefix-list

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show prefix-list** コマンドから **show running-config prefix-list** コマンドに変更されました。

使用上のガイドライン

実行コンフィギュレーションに含まれている **prefix-list description** コマンドは、常に関連する **prefix-list** コマンドの前に表示されます。コマンドを入力した順序は関係しません。

例

次に、**show running-config prefix-list** コマンドの出力例を示します。

```
hostname# show running-config prefix-list

!
prefix-list abc description A sample prefix list
prefix-list abc seq 5 permit 192.168.0.0/8 le 24
prefix-list abc seq 10 deny 10.0.0.0/8 le 32
!
```

関連コマンド

コマンド	説明
clear configure prefix-list	**prefix-list** コマンドを実行コンフィギュレーションから消去します。

show running-config priority-queue

インターフェイスのプライオリティ キュー コンフィギュレーションの詳細を表示するには、特権 EXEC モードで **show running-config priority-queue** コマンドを使用します。

show running-config priority-queue *interface-name*

シンタックスの説明

interface-name	プライオリティ キューの詳細を表示するインターフェイスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、test というインターフェイスについて show running-config priority-queue コマンドを使用した場合のコマンド出力を示しています。

```
hostname# show running-config priority-queue test
priority-queue test
  queue-limit   50
  tx-ring-limit 10
hostname#
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスからプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
show priority-queue statistics	指定したインターフェイス上に設定されているプライオリティ キューの統計情報を表示します。

show running-config privilege

コマンドまたはコマンド セットの特権を表示するには、特権 EXEC モードで **show running-config privilege** コマンドを使用します。

show running-config [all] privilege [**all** | **command** *command* | **level** *level*]

シンタックスの説明

all	（オプション。最初の引数）デフォルトの特権レベルを表示します。
all	（オプション。2 番目の引数）すべてのコマンドの特権レベルを表示します。
command *command*	（オプション）特定のコマンドの特権レベルを表示します。
level *level*	（オプション）指定したレベルに設定されているコマンドを表示します。有効値は 0 ～ 15 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、CLI ガイドラインに準拠するようにこのリリースで修正されました。

使用上のガイドライン

show running-config privilege コマンドは、現在の特権レベルを表示するために使用します。

例

```
hostname(config)# show running-config privilege level 0
privilege show level 0 command checksum
privilege show level 0 command curpriv
privilege configure level 0 mode enable command enable
privilege show level 0 command history
privilege configure level 0 command login
privilege configure level 0 command logout
privilege show level 0 command pager
privilege clear level 0 command pager
privilege configure level 0 command pager
privilege configure level 0 command quit
privilege show level 0 command version
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド文を削除します。
privilege	コマンドの特権レベルを設定します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

show running-config regex

regex コマンドを使用して設定したすべての正規表現を表示するには、特権 EXEC モードで **show running-config regex** コマンドを使用します。

show running-config regex

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config regex** コマンドの出力例を示します。この例にはすべての正規表現が表示されています。

```
hostname# show running-config regex
regex test "string"
```

関連コマンド

コマンド	説明
class-map type regex	正規表現クラス マップを作成します。
clear configure regex	すべての正規表現を消去します。
regex	正規表現を作成します。
test regex	正規表現をテストします。

show running-config route

セキュリティ アプライアンス上で実行されているルート コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config route** コマンドを使用します。

show running-config [***all***] **route**

シンタックスの説明

デフォルトの動作や値はありません。

デフォルト

このコマンドには、引数もキーワードもありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

例

次に、**show running-config route** コマンドの出力例を示します。

```
hostname# show running-config route
route outside 10.30.10.0 255.255.255.0 1
```

関連コマンド

コマンド	説明
clear configure route	**connect** キーワードを含んでいない **route** コマンドをコンフィギュレーションから削除します。
route	インターフェイスのスタティック ルートまたはデフォルト ルートを指定します。
show route	ルート情報を表示します。

show running-config route-map

ルートマップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config route-map** コマンドを使用します。

show running-config route-map [*map_tag*]

シンタックスの説明

map_tag	（オプション）ルートマップ タグのテキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

show running-config route-map コマンドは、コンフィギュレーション内に定義されているすべてのルートマップを表示するために使用します。名前を指定して個々のルートマップを表示するには、**show running-config route-map** *map_tag* コマンドを使用します。*map_tag* は、ルートマップの名前です。複数のルートマップで同じマップ タグ名を共有できます。

例

次に、**show running-config route-map** コマンドの出力例を示します。

```
hostname# show running-config route-map
route-map maptag1 permit sequence 10
    set metric 5
    match metric 3
route-map maptag1 permit sequence 12
    set metric 5
    match interface backup
    match metric 3
route-map maptag2 deny sequence 10
    match interface dmz
```

関連コマンド

コマンド	説明
clear configure route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を削除します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を定義します。

show running-config router

指定したルーティング プロトコルのグローバル コンフィギュレーション コマンドを表示するには、特権 EXEC モードで **show running-config router** コマンドを使用します。

show running-config [all] **router** [**ospf** [*process_id*] | ***rip***]

シンタックスの説明

all	デフォルトから変更していないコマンドを含めて、すべての router コマンドを表示します。
ospf	（オプション）グローバル OSPF コンフィギュレーション コマンドを表示します。
process_id	（オプション）選択した OSPF プロセスに関するコマンドを表示します。
rip	（オプション）グローバル RIP コンフィギュレーション コマンドを表示します。

デフォルト

ルーティング プロトコルが指定されていない場合、設定済みのルーティング プロトコルがすべて表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show router** コマンドから **show running-config router** コマンドに変更されました。

例

次に、**show running-config router ospf** コマンドの出力例を示します。

```
hostname# show running-config router ospf 1

router ospf 1
  log-adj-changes detail
  ignore lsa mospf
  no compatible rfc1583
  distance ospf external 200
  timers spf 10 20
  timers lsa-group-pacing 60
```

次に、**show running-config router rip** コマンドの出力例を示します。

```
router rip
    network 10.0.0.0
    version 2
    no auto-summary
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションからすべての router コマンドを消去します。
router ospf	OSPF ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードに入ります。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードに入ります。

show running-config same-security-traffic

セキュリティ レベルの等しいインターフェイス間での通信を表示するには、特権 EXEC モードで **show running-config same-security-traffic** コマンドを使用します。

show running-config same-security-traffic

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例　次に、**show running-config same-security-traffic** コマンドの出力例を示します。

```
hostname# show running-config same-security-traffic
```

関連コマンド

コマンド	説明
same-security-traffic	セキュリティ レベルの等しいインターフェイス間での通信を許可します。

show running-config service

システム サービスを表示するには、特権 EXEC モードで **show running-config service** コマンドを使用します。

show running-config service

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

例

次のコマンドは、システム サービスを表示する方法を示しています。

```
hostname# show running-config service
service resetoutside
```

関連コマンド

コマンド	説明
service	システム サービスをイネーブルにします。

show running-config service-policy

現在実行されているすべてのサービス ポリシー コンフィギュレーションを表示するには、特権 EXEC モードで ***show running-config service-policy*** コマンドを使用します。

show running-config [all] service-policy

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含む、すべてのサービス ポリシー コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、***show running-config service-policy*** コマンドの出力例を示します。

```
hostname# show running-config service-policy
```

関連コマンド

コマンド	説明
show service-policy	サービス ポリシーを表示します。
service-policy	サービス ポリシーを設定します。
clear service-policy	すべてのサービス ポリシーのコンフィギュレーションを消去します。
clear configure service-policy	サービス ポリシーのコンフィギュレーションを消去します。

show running-config sla monitor

実行コンフィギュレーションの SLA オペレーション コマンドを表示するには、特権 EXEC モードで **show running-config sla monitor** コマンドを使用します。

show running-config sla monitor [*sla-id*]

シンタックスの説明

sla_id	表示する **sla monitor** コマンドの SLA ID を指定します。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id を指定しない場合、すべての SLA オペレーションの **sla monitor** コマンドが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、**sla monitor** コマンド、関連付けられた SLA モニタ コンフィギュレーション モード コマンド、関連付けられた **sla monitor** スケジュール コマンド（存在する場合）を表示します。コンフィギュレーションの **track rtr** コマンドは表示しません。

例

次に、**show running-config sla monitor 5** コマンドの出力例を示します。SLA ID が 5 である SLA オペレーションの SLA モニタ コンフィギュレーションを表示します。

```
hostname# show running-config sla monitor 5

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

関連コマンド

コマンド	説明
clear configure sla monitor	**sla monitor** と、関連するコマンドを実行コンフィギュレーションから削除します。
show sla monitor configuration	指定した SLA オペレーションのコンフィギュレーション値を表示します。

show running-config snmp-map

設定済みの SNMP マップを表示するには、特権 EXEC モードで **show running-config snmp-map** コマンドを使用します。

show running-config snmp-map *map_name*

シンタックスの説明

map_name	指定した SNMP マップのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config snmp-map コマンドは、設定済みの SNMP マップを表示します。

例

次に、**show running-config snmp-map** コマンドの出力例を示します。

```
hostname# show running-config snmp-map snmp-policy
!
snmp-map snmp-policy
deny version 1
!
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。

show running-config snmp-server

現在実行されているすべての SNMP サーバのコンフィギュレーションを表示するには、グローバル コンフィギュレーション モードで ***show running-config snmp-server*** コマンドを使用します。

show running-config [default] snmp-server

シンタックスの説明

default	デフォルト SNMP サーバのコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、***show running-config snmp-server*** コマンドの例を示します。

```
hostname# show running-config snmp-server
```

関連コマンド

コマンド	説明
snmp-server	SNMP サーバを設定します。
clear snmp-server	SNMP サーバのコンフィギュレーションを消去します。
show snmp-server statistics	SNMP サーバのコンフィギュレーションを表示します。

show running-config ssh

現在のコンフィギュレーションに含まれている SSH のコマンドを表示するには、特権 EXEC モードで **show running-config ssh** コマンドを使用します。

show running-config [***default***] ***ssh*** [***timeout*** | ***version***]

show run [***default***] ***ssh*** [***timeout***]

シンタックスの説明

default	（オプション）設定済みの SSH コンフィギュレーション値に加えて、デフォルトの値も表示します。
timeout	（オプション）現在の SSH セッション タイムアウト値を表示します。
version	（オプション）現在サポートされている SSH のバージョンを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show ssh** コマンドから **show running-config ssh** コマンドに変更されました。

使用上のガイドライン

このコマンドは、現在の SSH コンフィギュレーションを表示します。SSH セッション タイムアウト値だけを表示するには、***timeout*** オプションを使用します。アクティブな SSH セッションのリストを表示するには、**show ssh sessions** コマンドを使用します。

例

次の例では、SSH セッション タイムアウトを表示しています。

```
hostname# show running-config timeout
ssh timeout 5 minutes
hostname#
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh scopy enable	セキュリティ アプライアンス上でセキュア コピー サーバをイネーブルにします。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

show running-config ssl

現在の一連の設定済み ssl コマンドを表示するには、特権 EXEC モードで **show running-config ssl** コマンドを使用します。

show running-config ssl

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次に、`show running-config ssl` コマンドの出力例を示します。

```
hostname# show running-config ssl
ssl server-version  tlsv1
ssl client-version tlsv1-only
ssl encryption 3des-sha1
ssl trust-point Firstcert
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

show running-config static

コンフィギュレーションに含まれているすべての **static** コマンドを表示するには、特権 EXEC モードで **show running-config static** コマンドを使用します。

show running-config static

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

使用上のガイドライン

このコマンドは、UDP プロトコルの最大接続値を表示します。UDP 最大接続値が「0」の場合、または設定されていない場合、制限の適用はディセーブルになります。

例

次の例は、コンフィギュレーションに含まれているすべての static コマンドを表示する方法を示しています。

```
hostname# show running-config static
static (inside,outside) 192.150.49.91 10.1.1.91 netmask 255.255.255.255
static (inside,outside) 192.150.49.200 10.1.1.200 netmask 255.255.255.255 tcp 255 0
```

（注） UDP 接続の制限値は表示されません。

関連コマンド

コマンド	説明
clear configure static	すべての **static** コマンドをコンフィギュレーションから削除します。
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定します。

show running-config sunrpc-server

SunRPC コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config sunrpc-server** コマンドを使用します。

show running-config sunrpc-server *interface_name ip_addr mask* **service** *service_type* **protocol** [**TCP** | **UDP**] **port** *port* [**-** *port*] **timeout** *hh:mm:ss*

シンタックスの説明

interface_name	サーバのインターフェイス。
ip_addr	サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* - *port*	SunRPC プロトコルのポート範囲。または、2 番目のポートを指定します。
protocol	SunRPC 転送プロトコル。
service	サービスを指定します。
service_type	SunRPC サービス プログラム タイプを設定します。
timeout *hh:mm:ss*	SunRPC サービス トラフィックへのアクセスが終了するまでのタイムアウト アイドル時間を指定します。
TCP	（オプション）TCP を指定します。
UDP	（オプション）UDP を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

service_type は、**sunrpcinfo** コマンドで指定したものです。

例

次に、**show running-config sunrpc-server** コマンドの出力例を示します。

```
hostname# show running-config sunrpc-server
inside 30.26.0.23 255.255.0.0 service 2147483647 protocol TCP port 2222 timeout
0:03:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	SunRPC サービスをセキュリティ アプライアンスから消去します。
debug sunrpc	SunRPC のデバッグ情報をイネーブルにします。
show conn	SunRPC など、さまざまな接続タイプの接続状態を表示します。
sunrpc-server	SunRPC サービス テーブルを作成します。
timeout	SunRPC を含む、さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show running-config sysopt

実行コンフィギュレーションの **sysopt** コマンド コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config sysopt** コマンドを使用します。

show running-config sysopt

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**show sysopt** コマンドから変更されました。

例

次に、**show running-config sysopt** コマンドの出力例を示します。

```
hostname# show running-config sysopt
no sysopt connection timewait
sysopt connection tcpmss 1200
sysopt connection tcpmss minimum 400
no sysopt nodnsalias inbound
no sysopt nodnsalias outbound
no sysopt radius ignore-secret
sysopt connection permit-ipsec
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS の A レコード アドレスの変更をディセーブルにします。

show running-config tcp-map

TCP マップ コンフィギュレーションに関する情報を表示するには、特権 EXEC モードで **show running-config tcp-map** コマンドを使用します。

show running-config tcp-map [*tcp_map_name*]

シンタックスの説明

tcp_map_name	（オプション）TCP マップ名のテキスト。テキストの長さは、58 文字までです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**show running-config tcp-map** コマンドの出力例を示します。

```
hostname# show running-config tcp-map
tcp-map localmap
```

関連コマンド

コマンド	説明
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。
clear configure tcp-map	TCP マップのコンフィギュレーションを消去します。

show running-config telnet

セキュリティ アプライアンスへの Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示するには、特権 EXEC モードで **show running-config telnet** コマンドを使用します。また、このコマンドを使用して、Telnet セッションに許容されるアイドル時間（分）を表示することもできます。このアイドル時間が経過すると、その Telnet セッションはセキュリティ アプライアンスが終了します。

show running-config telnet [**timeout**]

シンタックスの説明

timeout	（オプション）Telnet セッションに許容されるアイドル時間（分）で、アイドル時間が経過すると、その Telnet セッションはセキュリティ アプライアンスが終了します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	キーワード ***running-config*** が追加されました。

例

次の例は、セキュリティ アプライアンスへの Telnet 接続で使用することを認可されている IP アドレスの現在のリストを表示する方法を示しています。

```
hostname# show running-config telnet
2003 Jul 15 14:49:36 %MGMT-5-LOGIN_FAIL:User  failed to
log in from 128.107.183.22 through Telnet
2003 Jul 15 14:50:27 %MGMT-5-LOGIN_FAIL:User  failed to log in from 128.107.183.
22 through Telnet
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
telnet	Telnet アクセスをコンソールに追加し、アイドル タイムアウトを設定します。

show running-config terminal

現在の端末設定を表示するには、特権 EXEC モードで ***show running-config terminal*** コマンドを使用します。

show running-config terminal

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、ページの長さの設定が消去されます。

```
hostname# show running-config terminal

Width = 80, no monitor
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
terminal	端末回線のパラメータを設定します。
terminal width	端末の表示幅を設定します。

show running-config tftp-server

デフォルト TFTP サーバのアドレスとディレクトリを表示するには、グローバル コンフィギュレーション モードで **show running-config tftp-server** コマンドを使用します。

show running-config tftp-server

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	***running-config*** キーワードが追加されました。

例

次の例は、デフォルト TFTP サーバの IP/IPv6 アドレスとコンフィギュレーション ファイルのディレクトリを表示する方法を示しています。

```
hostname(config)# show running-config tftp-server
tftp-server inside 10.1.1.42 /temp/config/test_config
```

関連コマンド

コマンド	説明
configure net	コンフィギュレーションを TFTP サーバ上の指定パスからロードします。
tftp-server	デフォルト TFTP サーバのアドレスとコンフィギュレーション ファイルのディレクトリを設定します。

show running-config timeout

すべてまたは特定のプロトコルのタイムアウト値を表示するには、特権 EXEC モードで **show running-config timeout** コマンドを使用します。

show running-config timeout *protocol*

シンタックスの説明

protocol	（オプション）指定したプロトコルのタイムアウト値を表示します。サポートされているプロトコルは、**xlate**、**conn**、**udp**、**icmp**、**rpc**、**h323**、**h225**、**mgcp**、***mgcp-pat***、**sip**、**sip_media**、および **uauth** です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	***running-config*** キーワードと ***mgcp-pat*** キーワードが追加されました。

例

次の例は、システムのタイムアウト値を表示する方法を示しています。

```
hostname(config)# show timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02
:00
timeout uauth 0:00:00 absolute
```

関連コマンド

コマンド	説明
clear configure timeout	デフォルトのアイドル期間に戻します。
timeout	アイドル状態の最大継続時間を設定します。

show running-config track

実行コンフィギュレーションの **track rtr** コマンドを表示するには、特権 EXEC モードで **show running-config track** コマンドを使用します。

show running-config track [*track-id*]

シンタックスの説明

track-id	（オプション）表示対象を、指定のトラッキング オブジェクト ID を持つ **track rtr** コマンドに限定します。

デフォルト

track-id が指定されない場合、実行コンフィギュレーションのすべての **track rtr** コマンドが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show running-config track** コマンドの出力例を示します。

```
hostname# show running-config track 5

track 5 rtr 124 reachability
```

関連コマンド

コマンド	説明
clear configure track	**track rtr** コマンドを実行コンフィギュレーションから削除します。
show track	追跡するオブジェクトに関する情報を表示します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

show running-config tunnel-group

すべてまたは特定のトンネル グループおよびトンネル グループ アトリビュートについて、コンフィギュレーション情報を表示するには、グローバル コンフィギュレーション モードまたは特権 EXEC モードで **show running-config tunnel-group** コマンドを使用します。

show running-config [**all**] ***tunnel-group*** [*name* [**general-attributes | ipsec-attributes | ppp-attributes**]]

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての tunnel-group コマンドを表示します。
general-attributes	一般アトリビュートのコンフィギュレーション情報を表示します。
ipsec-attributes	IPSec アトリビュートのコンフィギュレーション情報を表示します。
name	トンネル グループの名前を指定します。
ppp-attributes	PPP アトリビュートのコンフィギュレーション情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•		•		
特権 EXEC	•		•		

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

グローバル コンフィギュレーション モードで入力した次の例では、すべてのトンネル グループの現在のコンフィギュレーションを表示しています。

```
hostname<config># show running-config tunnel-group
tunnel-group 209.165.200.225 type IPSec_L2L
tunnel-group 209.165.200.225 ipsec-attributes
    pre-shared-key xyzx
hostname<config>#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループのコンフィギュレーションを削除します。
tunnel-group general-attributes	指定したトンネル グループの一般アトリビュートを指定するための、サブコンフィギュレーション モードに入ります。
tunnel-group ipsec-attributes	指定したトンネル グループの IPSec アトリビュートを指定するための、サブコンフィギュレーション モードに入ります。
tunnel-group	指定したタイプのトンネル グループ サブコンフィギュレーション モードに入ります。

show running-config url-block

URL フィルタリングで使用されるバッファとメモリ割り当てのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-block** コマンドを使用します。

show running-config url-block [block | url-mempool | url-size]

シンタックスの説明

block	バッファされるブロックの最大数に関するコンフィギュレーションを表示します。
url-mempool	許容される最大の URL サイズ（KB 単位）に関するコンフィギュレーションを表示します。
url-size	長い URL のバッファに割り当てられるメモリ リソース（KB 単位）に関するコンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config url-block コマンドは、URL フィルタリングで使用されるバッファとメモリ割り当てのコンフィギュレーションを表示します。

例

次に、**show running-config url-block** コマンドの出力例を示します。

```
hostname# show running-config url-block
!
url-block block 56
!
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用状況カウンタを消去します。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-config url-cache

URL フィルタリングで使用されるキャッシュのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-cache** コマンドを使用します。

show running-config url-cache

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config url-cache コマンドは、URL フィルタリングで使用されるキャッシュのコンフィギュレーションを表示します。

例

次に、**show running-config url-cache** コマンドの出力例を示します。

```
hostname# show running-config url-cache
!
url-cache src_dst 128
!
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-configuration url-list

WebVPN ユーザがアクセスできる URL のセットを表示するには、特権 EXEC モードで **show running-configuration url-list** コマンドを使用します。

show running-configuration url-list

シンタックスの説明

このコマンドには、引数もキーワードもありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
Webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次に、**show running-configuration url-list** コマンドの出力例を示します。

```
hostname# show running-configuration url-list
url-list userURL "SW Engineering" http://10.1.1.2
url-list userURL "My Company" http://www.mycompany.com
url-list userURL "401K Program" https://401k.com
url-list userURL "Exchange5.5 Mail" http://10.1.1.11/exchange
url-list URLlist2 "OWA-2000" http://10.1.1.7/exchange
```

関連コマンド

コマンド	説明
clear configuration url-list	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドだけを削除します。
url-list	WebVPN ユーザがアクセスできる URL のセットを設定します。
url-list	特定のグループ ポリシーまたはユーザの WebVPN URL アクセスをイネーブルにします。

show running-config url-server

URL フィルタリング サーバのコンフィギュレーションを表示するには、特権 EXEC モードで **show running-config url-server** コマンドを使用します。

show running-config url-server

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show running-config url-server コマンドは、URL フィルタリング サーバのコンフィギュレーションを表示します。

例

次に、**show running-config url-server** コマンドの出力例を示します。

```
hostname# show running-config url-server
!
url-server (perimeter) vendor websense host 10.0.1.1
!
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報を消去します。
show url-server	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show running-config username

特定のユーザの実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config username** コマンドをユーザ名を付加して使用します。すべてのユーザの実行コンフィギュレーションを表示するには、ユーザ名を指定せずにこのコマンドを使用します。

show running-config [**all**] **username** [*name*] [**attributes**]]

シンタックスの説明

attributes	ユーザの特定の AVP を表示します。
all	（オプション）デフォルトから変更していないコマンドを含めて、すべてのユーザ名についてコマンドを表示します。
name	ユーザの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、anyuser というユーザについての show running-config username コマンドの出力例を示します。

```
hostname# show running-config username anyuser
username anyuser password .8T1d6ik58/lzXS5 encrypted privilege 3
username anyuser attributes
vpn-group-policy DefaultGroupPolicy
vpn-idle-timeout 10
vpn-session-timeout 120
vpn-tunnel-protocol IPSec
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースを消去します。
username	ユーザをセキュリティ アプライアンスのデータベースに追加します。
username attributes	特定のユーザのアトリビュートを設定できます。

show running-config virtual

セキュリティ アプライアンス仮想サーバの IP アドレスを表示するには、特権 EXEC モードで **show running-config virtual** コマンドを使用します。

show running-config [**all**] **virtual**

シンタックスの説明

all	すべての仮想サーバの仮想サーバ IP アドレスを表示します。

デフォルト

all キーワードを省略すると、現在の仮想サーバ（複数の場合あり）に対して明示的に設定した IP アドレスだけが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。

使用上のガイドライン

このコマンドを使用するには、特権 EXEC モードに入っている必要があります。

例

次に、設定済みの HTTP 仮想サーバが存在する場合の **show running-config virtual** コマンドの出力例を示します。

```
hostname(config)# show running-config virtual
virtual http 192.168.201.1
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド文を削除します。
virtual	認証仮想サーバのアドレスを表示します。

show running-config vpn load-balancing

現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示するには、グローバル コンフィギュレーション モード、特権 EXEC モード、または VPN ロードバランシング モードで **show running-config vpn load-balancing** コマンドを使用します。

show running-config [**all**] **vpn load-balancing**

シンタックスの説明

all	デフォルトおよび明示的に設定した VPN ロードバランシング コンフィギュレーションを両方とも表示します。

デフォルト

all キーワードを省略すると、明示的に設定した VPN ロードバランシング コンフィギュレーションが表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—
VPN ロードバランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

show running-config vpn load-balancing コマンドは、関連コマンドである **cluster encryption**、**cluster ip address**、**cluster key**、**cluster port**、**nat**、**participate**、および **priority** に関するコンフィギュレーション情報も表示します。

例

次に、***all*** オプションをイネーブルにした **show running-config vpn load-balancing** コマンドとその出力例を示します。

```
hostname(config)# show running-config all vpn load-balancing
vpn load-balancing
 no nat
 priority 9
 interface lbpublic test
 interface lbprivate inside
 no cluster ip address
 no cluster encryption
 cluster port 9023
 no participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	コンフィギュレーションから **vpn load-balancing** コマンド文を削除します。
show vpn load-balancing	VPN ロードバランシングの実行時の統計情報を表示します。
vpn load-balancing	VPN ロードバランシング モードに入ります。

show running-config webvpn

webvpn の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config webvpn** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] webvpn [apcf | auto-signon | cache | proxy-bypass | rewrite | sso-server | url-list]

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルト値を含めて表示します。
apcf	（オプション）WebVPN APCF の実行コンフィギュレーションを表示します。
auto-signon	（オプション）WebVPN 自動サインオンの実行コンフィギュレーションを表示します。
cache	（オプション）WebVPN キャッシングの実行コンフィギュレーションを表示します。
proxy-bypass	（オプション）WebVPN プロキシ バイパスの実行コンフィギュレーションを表示します。
rewrite	（オプション）WebVPN コンテンツ変換の実行コンフィギュレーションを表示します。
sso-server	（オプション）シングル サインオンの実行コンフィギュレーションを表示します。
url-list	（オプション）WebVPN による URL へのアクセスの実行コンフィギュレーションを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。
7.1(1)	このコマンドが変更されました。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—
WebVPN	•	—	•	—	—

例

次に、**show running-config webvpn** コマンドの出力例を示します。

```
hostname# show running-configuration webvpn
webvpn
 title WebVPN Services for ASA-4
 title-color green
 default-idle-timeout 0
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 authorization-dn-attributes CN
```

次に、**show running-config all webvpn** コマンドの出力例を示します。

```
hostname#(config-webvpn)# show running-config all webvpn

webvpn
 title WebVPN Services for ASA-4
 username-prompt Username
 password-prompt Password
 login-message Please enter your username and password
 logout-message Goodbye
 no logo
 title-color green
 secondary-color #CCCCFF
 text-color white
 secondary-text-color black
 default-idle-timeout 0
 no http-proxy
 no https-proxy
 nbns-server 10.148.1.28 master timeout 2 retry 2
 accounting-server-group RadiusACS1
 authentication-server-group RadiusACS2
 no authorization-server-group
 default-group-policy DfltGrpPolicy
 authentication aaa
 no authorization-required
 authorization-dn-attributes CN
hostname#
```

次に、**show running-config webvpn sso-server** コマンドの出力例を示します。

```
hostname#(config-webvpn)# show running-config webvpn sso-server
sso-server
sso-server bxbsvr type siteminder
web-agent-url http://bxb-netegrity.demo.com/vpnauth/
policy-server-secret cisco1234
sso-server policysvr type siteminder
web-agent-url http://webagent1.mysiteminder.com/ciscoauth/
policy-server-secret Cisco1234
max-retry-attempts 4
request-timeout 10
hostname#(config-webvpn)#
```

関連コマンド

コマンド	説明
clear configure webvpn	デフォルト以外の WebVPN コンフィギュレーション アトリビュートを削除します。
debug webvpn	WebVPN セッションに関するデバッグ情報を表示します。
show webvpn	WebVPN セッションに関する統計情報を表示します。

show running-config webvpn auto-signon

実行コンフィギュレーション内のすべての WebVPN 自動サインオン割り当てを表示するには、グローバル コンフィギュレーション モードで **show running-config webvpn auto-signon** コマンドを使用します。

show running-config webvpn auto-signon

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、**show running-config webvpn auto-signon** の出力例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
hostname(config-webvpn)# auto-signon allow uri *.example.com/* auth-type basic
hostname(config-webvpn)# show running-config webvpn auto-signon
auto-signon allow ip 10.1.1.0 255.255.255.0 auth-type ntlm
auto-signon allow uri *.example.com/* auth-type basic
```

関連コマンド

auto-signon	セキュリティ アプライアンスが WebVPN ログイン クレデンシャルを自動的に内部サーバに渡すように設定します。

show running-config zonelabs-integrity

Zone Labs Integrity サーバ コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config zonelabs-integrity** コマンドを使用します。

show running-config [**all**] **zonelabs-integrity**

シンタックスの説明

all	（オプション）実行コンフィギュレーションを、デフォルトのコンフィギュレーション値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用して、すべての Zone Labs Integrity サーバのアドレスと、アクティブな Zone Labs Integrity サーバの設定値を表示します。明示的に設定されている値に加えてデフォルト値も表示するには、**all** パラメータを使用します。

例

次に、**show running-config zonelabs-integrity** コマンドの出力例を示します。

```
hostname# show running-config zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
zonelabs-integrity port 300
hostname#
```

次に、**show running-config all zonelabs-integrity** コマンドの出力例を示します。

```
hostname# show running-config all zonelabs-integrity
zonelabs-integrity server-address 10.0.9.1 10.0.9.2
zonelabs-integrity port 300
zonelabs-integrity interface none
zonelabs-integrity fail-open
zonelabs-integrity fail-timeout 10
zonelabs-integrity ssl-client-authentication disable
zonelabs-integrity ssl-certificate-port 80
hostname#
```

関連コマンド

コマンド	説明
clear configure zonelabs-integrity	Zone Labs Integrity サーバのコンフィギュレーションを消去します。

show running-config smtps

SMTPS の実行コンフィギュレーションを表示するには、特権 EXEC モードで **show running-configuration smtps** コマンドを使用します。表示内容にデフォルト コンフィギュレーションを含めるには、**all** キーワードを使用します。

show running-config [all] smtps

シンタックスの説明

all	実行コンフィギュレーションを、デフォルト値を含めて表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次に、**show running-config smtps** コマンドの出力例を示します。

```
hostname# show running-config smtps

smtps
server 10.1.1.21
 authentication-server-group KerbSvr
 authentication aaa

hostname# show running-config all smtps

smtps
 port 995
 server 10.1.1.21
 outstanding 20
 name-separator :
 server-separator @
 authentication-server-group KerbSvr
 no authorization-server-group
 no accounting-server-group
 no default-group-policy
 authentication aaa
hostname#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
smtps	SMTPS 電子メール プロキシのコンフィギュレーションを作成または編集します。

show running-config vpdn

PPPoE 接続に使用する VPDN コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config vpdn** コマンドを使用します。

show running-config vpdn

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドには、デフォルトの動作も値もありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、show running-config vpdn コマンドの使用方法とそのコマンド出力を示します。

```
hostname# show running-config vpdn
vpdn group telecommuters ppp authentication mschap
vpdn username tomm password ********* store-local
```

関連コマンド

コマンド	説明
show running-config vpdn group	VPDN グループの現在のコンフィギュレーションを表示します。
show running-config vpdn username	VPDN ユーザ名の現在のコンフィギュレーションを表示します。

show running-configuration vpn-sessiondb

現在の一連の設定済み vpn-sessiondb コマンドを表示するには、特権 EXEC モードで **show running-configuration vpn-sessiondb** コマンドを使用します。

show running-configuration [all] vpn-sessiondb

シンタックスの説明

all	（オプション）デフォルトから変更していないコマンドを含めて、すべての **vpn-sessiondb** コマンドを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

リリース 7.0 以降では、このコマンドは VPN 最大セッション制限のみを表示します（設定されている場合）。

例

次に、**show running-configuration vpn-sessiondb** コマンドの出力例を示します。

```
hostname# show running-configuration vpn-sessiondb
```

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb summary	セッションの要約を表示します。現在のセッションの合計数、各タイプの現在のセッション数、ピーク時の数および累積合計数、最大同時セッション数を含んでいます。

show running-config wccp

実行コンフィギュレーションの WCCP コンフィギュレーションを表示するには、特権 EXEC モードで **show running-config wccp** コマンドを使用します。

show [**all**] **running-config wccp**

シンタックスの説明

all	1 つまたはすべての WCCP コマンドについて、デフォルトと、明示的に設定されたコンフィギュレーション情報を表示します。

デフォルト

このコマンドには、引数もキーワードもありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show running-config wccp** コマンドの出力例を示します。

```
hostname# show running-config wccp
wccp web-cache redirect-list wooster group-list jeeves password whatho
hostname#
```

関連コマンド

コマンド	説明
wccp	WCCP のサポートをイネーブルにします。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

CHAPTER 30

show service-policy コマンド～ show webvpn svc コマンド

show service-policy

設定済みのサービス ポリシーを表示するには、グローバル コンフィギュレーション モードで ***show service-policy*** コマンドを使用します。

show service-policy [**global** | ***interface*** *intf*] [***csc*** | ***inspect*** | ***ips*** | ***police*** | ***priority***]

show service-policy [**global** | ***interface*** *intf*] [***set connection*** [***details***]]

show service-policy [**global** | ***interface*** *intf*] [***flow*** *protocol* {***host*** *src_host* | *src_ip src_mask*} [***eq*** *src_port*] {***host*** *dest_host* | *dest_ip dest_mask*} [***eq*** *dest_port*] [*icmp_number* | *icmp_control_message*]]

シンタックスの説明

csc	（オプション）***csc*** コマンドを含んでいるポリシーだけを出力します。
dest_ip	トラフィック フローの宛先 IP アドレス。
dest_mask	トラフィック フローの宛先 IP アドレスのサブネット マスク。
dest_port	（オプション）トラフィック フローで使用されている宛先ポート。
details	（オプション）クライアントごとの接続制限がイネーブルになっている場合は、クライアントごとの接続制限情報を表示します。
eq	（オプション）等号。送信元または宛先のポートが、以降に指定するポート番号と一致することを要求します。
flow	（オプション）セキュリティ アプライアンスでポリシーの適用対象となるトラフィック フローを指定します。このフローに適用されるポリシーが表示されます。***flow*** キーワードに続いて指定する引数とキーワードでは、フローを IP 5 タプル形式で指定します。
global	（オプション）すべてのインターフェイスに適用されるグローバル ポリシーのみを出力します。
host *dest_host*	トラフィック フローの宛先ホストの IP アドレス。
host *src_host*	トラフィック フローの送信元ホストの IP アドレス。
icmp_control_message	（オプション）トラフィック フローの ICMP 制御メッセージを指定します。*icmp_control_message* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。
icmp_number	（オプション）トラフィック フローの ICMP プロトコル番号を指定します。
inspect	（オプション）**inspect** コマンドを含んでいるポリシーだけを出力します。

***interface** intf*	（オプション）*intf* 引数で指定したインターフェイスに適用されるポリシーを表示します。*intf* は、**nameif** コマンドで定義したインターフェイス名です。
ips	**ips** コマンドを含んでいるポリシーだけを出力します。
police	**police** コマンドを含んでいるポリシーだけを出力します。
priority	**priority** コマンドを含んでいるポリシーだけを出力します。
set connection	**set connection** コマンドを含んでいるポリシーだけを出力します。
protocol	トラフィック フローで使用されているプロトコル。*protocol* 引数で有効となる値については、下の「使用上のガイドライン」に示しています。
src_ip	トラフィック フローで使用されている送信元 IP アドレス。
src_mask	トラフィック フローで使用されている送信元 IP ネットマスク。
src_port	トラフィック フローで使用されている送信元ポート。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	このコマンドが ***csc*** キーワードを追加するように変更されました。

使用上のガイドライン

flow キーワードを使用すると、記述可能な任意のフローについて、セキュリティ アプライアンスがそのフローに適用するポリシーを特定できます。この情報を利用すると、必要なサービスがこのサービス ポリシー コンフィギュレーションによって特定の接続に提供されるかどうかを確認できます。***flow*** キーワード以降に指定する引数とキーワードでは、オブジェクト グループ化をしていないフローを IP 5 タプル形式で指定します。

フローを IP 5 タプル形式で記述するため、すべての一致基準がサポートされるわけではありません。次に、フローの検索でサポートされている一致基準のリストを示します。

- ***match access-list***
- ***match port***
- ***match rtp***
- ***match default-inspection-traffic***

priority キーワードは、インターフェイスを経由して転送されたパケットの集約カウンタ値を表示するために使用します。

show service-policy コマンドの出力に表示される初期接続の数は、**class-map** コマンドで定義したトラフィック マッチングと一致したインターフェイスに向かう現在の初期接続の数を示しています。`embryonic-conn-max` フィールドは、モジュラ ポリシー フレームワークを使用するトラフィック クラスに対して設定した最大初期接続数の制限値を示しています。表示される現在の初期接続数が最大値と等しい場合、または最大値を超えている場合は、新しい TCP 接続が **class-map** コマンドで定義したトラフィック タイプと一致すると、その接続に対して TCP 代行受信が適用されます。

protocol 引数の値

次に、*protocol* 引数で有効となる値を示します。

- *number*：プロトコル番号（0 ～ 255）
- ***ah***
- ***eigrp***
- ***esp***
- ***gre***
- ***icmp***
- ***icmp6***
- ***igmp***
- ***igrp***
- ***ip***
- ***ipinip***
- ***ipsec***
- ***nos***
- ***ospf***
- ***pcp***
- ***pim***
- ***pptp***
- ***snp***
- ***tcp***
- ***udp***

icmp_control_message 引数の値

次に、*icmp_control_message* 引数で有効となる値を示します。

- ***alternate-address***
- ***conversion-error***
- ***echo***
- ***echo-reply***
- ***information-reply***
- ***information-request***
- ***mask-reply***
- ***mask-request***
- ***mobile-redirect***
- ***parameter-problem***
- ***redirect***
- ***router-advertisement***
- ***router-solicitation***
- ***source-quench***
- ***time-exceeded***
- ***timestamp-reply***
- ***timestamp-request***
- ***traceroute***

- *unreachable*

例

次の例は、*show service-policy* コマンドのシンタックスを示しています。

```
hostname# show service-policy global

Global policy:
  Service-policy: inbound_policy
    Class-map: ftp-port
      Inspect: ftp strict inbound_ftp, packet 0, drop 0, reset-drop 0
hostname# show service-policy priority

Interface outside:

Global policy:
  Service-policy: sa_global_fw_policy

Interface outside:
  Service-policy: ramap
    Class-map: clientmap
      Priority:
        Interface outside: aggregate drop 0, aggregate transmit 5207048
    Class-map: udpmap
      Priority:
        Interface outside: aggregate drop 0,  aggregate transmit 5207048
    Class-map: cmap


hostname# show service-policy flow udp host 209.165.200.229 host 209.165.202.158 eq
5060

Global policy:
  Service-policy: f1_global_fw_policy
    Class-map: inspection_default
      Match: default-inspection-traffic
      Action:
        Input flow:  inspect sip

Interface outside:
  Service-policy: test
    Class-map: test
      Match: access-list test
        Access rule: permit ip 209.165.200.229 255.255.255.224 209.165.202.158
255.255.255.224
      Action:
        Input flow:  ids inline
        Input flow:  set connection conn-max 10 embryonic-conn-max 20
```

関連コマンド

コマンド	説明
clear configure service-policy	サービス ポリシーのコンフィギュレーションを消去します。
clear service-policy	すべてのサービス ポリシーのコンフィギュレーションを消去します。
service-policy	サービス ポリシーを設定します。
show running-config service-policy	実行コンフィギュレーションに設定されているサービス ポリシーを表示します。

show service-policy inspect gtp

GTP コンフィギュレーションを表示するには、特権 EXEC モードで **show service-policy inspect gtp** コマンドを使用します。

show service-policy [**interface** *int*] **inspect gtp** {**pdp-context** [**apn** *ap_name* | **detail** | **imsi** *IMSI_value* | **ms-addr** *IP_address* | **tid** *tunnel_ID* | **version** *version_num*] | ***pdpmcb*** | **requests** | **statistics** [**gsn** *IP_address*] }

シンタックスの説明

apn	（オプション）指定した APN に基づいて、PDP コンテキストの詳細な出力を表示します。
ap_name	統計情報を表示する特定のアクセス ポイント名を指定します。
detail	（オプション）PDP コンテキストの詳細な出力を表示します。
imsi	指定した IMSI に基づいて、PDP コンテキストの詳細な出力を表示します。
IMSI_value	統計情報を表示する特定の IMSI を指定するための 16 進値。
interface	（オプション）特定のインターフェイスを指定します。
int	情報を表示するインターフェイスを指定します。
gsn	（オプション）GPRS サポート ノードを指定します。このノードは、GPRS 無線データ ネットワークとその他のネットワークの間にあるインターフェイスです。
gtp	（オプション）GTP のサービス ポリシーを表示します。
IP_address	統計情報を表示する IP アドレス。
ms-addr	（オプション）指定したモバイル ステーション（MS）アドレスに基づいて、PDP コンテキストの詳細な出力を表示します。
pdp-context	（オプション）パケット データ プロトコル コンテキストを指定します。
pdpmcb	（オプション）PDP マスター制御ブロックのステータスを表示します。
requests	（オプション）GTP 要求のステータスを表示します。
statistics	（オプション）GTP 統計情報を表示します。
tid	（オプション）指定した TID に基づいて、PDP コンテキストの詳細な出力を表示します。
tunnel_ID	統計情報を表示する特定のトンネルを指定するための 16 進値。
version	（オプション）GTP バージョンに基づいて、PDP コンテキストの詳細な出力を表示します。
version_num	統計情報を表示する PDP コンテキストのバージョンを指定します。有効な範囲は 0 ～ 255 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

縦線（|）を使用すると、表示内容をフィルタリングできます。表示フィルタリング オプションの詳細については、| を入力してください。

show pdp-context コマンドは、PDP コンテキストに関する情報を表示します。

パケット データ プロトコル コンテキストは、IMSI と NSAPI の組み合せであるトンネル ID によって識別されます。GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、パケットを外部パケット データ ネットワークとモバイル ステーション ユーザの間で転送するために必要なものです。

show gtp requests コマンドは、要求キューに入っている現在の要求を表示します。

例

次に、**show gtp requests** コマンドの出力例を示します。

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

次の例のように縦線（|）を使用すると、表示内容をフィルタリングできます。

```
hostname# show service-policy gtp statistics | grep gsn
```

この例では、出力に gsn という語が含まれている GTP 統計情報が表示されます。

次のコマンドでは、GTP 検査の統計情報を表示しています。

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

次のコマンドでは、PDP コンテキストに関する情報を表示しています。

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

表 30-1 に、**show service-policy inspect gtp pdp-context** コマンドの出力に含まれている各カラムの説明を示します。

表 30-1　PDP コンテキスト

カラムのヘッダー	説明
Version	GTP のバージョンを表示します。
TID	トンネル識別子を表示します。
MS Addr	モバイル ステーションのアドレスを表示します。
SGSN Addr	サービス提供ゲートウェイ サービス ノードを表示します。
Idle	PDP コンテキストが使用されていない期間を表示します。
APN	アクセス ポイント名を表示します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。

show service-policy inspect radius-accounting

GTP コンフィギュレーションを表示するには、特権 EXEC モードで **show service-policy inspect radius-accounting** コマンドを使用します。

show service-policy [**interface** *int*] **inspect radius-accounting**

シンタックスの説明

interface *int*	（オプション）特定のインターフェイスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

例

次に、**show gtp requests** コマンドの出力例を示します。

```
hostname# show gtp requests
0 in use, 0 most used, 200 maximum allowed
```

次の例のように縦線（|）を使用すると、表示内容をフィルタリングできます。

```
hostname# show service-policy gtp statistics | grep gsn
```

この例では、出力に gsn という語が含まれている GTP 統計情報が表示されます。

次のコマンドでは、GTP 検査の統計情報を表示しています。

```
hostname# show service-policy inspect gtp statistics
GPRS GTP Statistics:
  version_not_support | 0 | msg_too_short | 0
  unknown_msg | 0 | unexpected_sig_msg | 0
  unexpected_data_msg | 0 | ie_duplicated | 0
  mandatory_ie_missing | 0 | mandatory_ie_incorrect | 0
  optional_ie_incorrect | 0 | ie_unknown | 0
  ie_out_of_order | 0 | ie_unexpected | 0
  total_forwarded | 0 | total_dropped | 0
  signalling_msg_dropped | 0 | data_msg_dropped | 0
  signalling_msg_forwarded | 0 | data_msg_forwarded | 0
  total created_pdp | 0 | total deleted_pdp | 0
  total created_pdpmcb | 0 | total deleted_pdpmcb | 0
  pdp_non_existent | 0
```

次のコマンドでは、PDP コンテキストに関する情報を表示しています。

```
hostname# show service-policy inspect gtp pdp-context
1 in use, 1 most used, timeout 0:00:00

Version TID | MS Addr | SGSN Addr | Idle | APN
v1 | 1234567890123425 | 1.1.1.1 | 11.0.0.2 0:00:13  gprs.cisco.com

 | user_name (IMSI): 214365870921435 | MS address: | 1.1.1.1
 | primary pdp: Y | nsapi: 2
 | sgsn_addr_signal: | 11.0.0.2 | sgsn_addr_data: | 11.0.0.2
 | ggsn_addr_signal: | 9.9.9.9 | ggsn_addr_data: | 9.9.9.9
 | sgsn control teid: | 0x000001d1 | sgsn data teid: | 0x000001d3
 | ggsn control teid: | 0x6306ffa0 | ggsn data teid: | 0x6305f9fc
 | seq_tpdu_up: | 0 | seq_tpdu_down: | 0
 | signal_sequence: | 0
 | upstream_signal_flow: | 0 | upstream_data_flow: | 0
 | downstream_signal_flow: | 0 | downstream_data_flow: | 0
 | RAupdate_flow: | 0
```

表 30-2 に、**show service-policy inspect gtp pdp-context** コマンドの出力に含まれている各カラムの説明を示します。

表 30-2　PDP コンテキスト

カラムのヘッダー	説明
Version	GTP のバージョンを表示します。
TID	トンネル識別子を表示します。
MS Addr	モバイル ステーションのアドレスを表示します。
SGSN Addr	サービス提供ゲートウェイ サービス ノードを表示します。
Idle	PDP コンテキストが使用されていない期間を表示します。
APN	アクセス ポイント名を表示します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。

show shun

排除情報を表示するには、特権 EXEC モードで **show shun** コマンドを使用します。

show shun [*src_ip* | *statistics*]

シンタックスの説明

src_ip	（オプション）このアドレスに関する情報を表示します。
statistics	（オプション）インターフェイスのカウンタのみを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次に、**show shun** コマンドの出力例を示します。

```
hostname# show shun
shun (outside) 10.1.1.27 10.2.2.89 555 666 6
shun (inside1) 10.1.1.27 10.2.2.89 555 666 6
```

関連コマンド

コマンド	説明
clear shun	現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去します。
shun	新しい接続を阻止し、既存の接続からのパケットを拒否することによって、攻撃ホストへのダイナミックな応答をイネーブルにします。

show sip

SIP セッションを表示するには、特権 EXEC モードで **show sip** コマンドを使用します。

show sip

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**show sip** コマンドは、SIP 検査エンジンの問題のトラブルシューティングに役立ちます。説明は、**inspect protocol sip udp 5060** コマンドと一緒にします。**show timeout sip** コマンドは、指示されているプロトコルのタイムアウト値を表示します。

show sip コマンドは、セキュリティ アプライアンスを越えて確立されている SIP セッションの情報を表示します。**debug sip** と **show local-host** コマンドと共に、このコマンドは、SIP 検査エンジンの問題のトラブルシューティングに使用されます。

（注）　**show sip** コマンドを使用する前に **pager** コマンドを設定することを推奨します。多くの SIP セッション レコードが存在し、**pager** コマンドが設定されていない場合、**show sip** コマンドの出力が最後まで到達するには、しばらく時間がかかることがあります。

例　次に、**show sip** コマンドの出力例を示します。

```
hostname# show sip
Total: 2
call-id c3943000-960ca-2e43-228f@10.130.56.44
 | state Call init, idle 0:00:01
call-id c3943000-860ca-7e1f-11f7@10.130.56.45
 | state Active, idle 0:00:06
```

この例は、セキュリティ アプライアンス上の 2 つのアクティブな SIP セッションを示しています（`Total` フィールドで示されているように）。各 `call-id` は、コールを表わしています。

最初のセッションは、call-id c3943000-960ca-2e43-228f@10.130.56.44 で、Call Init 状態にあります。これは、このセッションはまだコール セットアップ中であることを示しています。コール セットアップが完了するのは、ACK が確認されたときのみです。このセッションは、1 秒間アイドル状態でした。

2 番目のセッションは、Active 状態です。ここでは、コール セットアップは完了して、エンドポイントはメディアを交換しています。このセッションは、6 秒間アイドル状態でした。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug sip	SIP のデバッグ情報をイネーブルにします。
inspect sip	SIP アプリケーション検査をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show skinny

SCCP（Skinny）検査エンジンの問題をトラブルシューティングするには、特権 EXEC モードで **show skinny** コマンドを使用します。

show skinny

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show skinny コマンドは、SCCP（Skinny）検査エンジンの問題のトラブルシューティングに役立ちます。

例

次の条件での **show skinny** コマンドの出力例を示します。セキュリティ アプライアンスを越えて 2 つのアクティブな Skinny セッションがセットアップされています。最初の Skinny セッションは、ローカル アドレス 10.0.0.11 にある内部 Cisco IP Phone と 172.18.1.33 にある外部 Cisco CallManager の間に確立されています。TCP ポート 2000 は、CallManager です。2 番目の Skinny セッションは、ローカル アドレス 10.0.0.22 にある別の内部 Cisco IP Phone と同じ Cisco CallManager の間に確立されています。

```
hostname# show skinny

        LOCAL                   FOREIGN                 STATE

----------------------------------------------------------------

1       10.0.0.11/52238         172.18.1.33/2000                1

  MEDIA 10.0.0.11/22948         172.18.1.22/20798

2       10.0.0.22/52232         172.18.1.33/2000                1

  MEDIA 10.0.0.22/20798         172.18.1.11/22948
```

この出力は、両方の内部 Cisco IP Phone 間でコールが確立されていることを示します。最初と 2 番目の電話機の RTP リスニング ポートは、それぞれ UDP 22948 と 20798 です。

次に、これらの Skinny 接続に対する xlate 情報を示します。

```
hostname# show xlate debug
2 in use, 2 most used
Flags: D | DNS, d | dump, I | identity, i | inside, n | no random,
 | o | outside, r | portmap, s | static
NAT from inside:10.0.0.11 to outside:172.18.1.11 flags si idle 0:00:16 timeout 0:05:00
NAT from inside:10.0.0.22 to outside:172.18.1.22 flags si idle 0:00:14 timeout 0:05:00
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug skinny	SCCP のデバッグ情報をイネーブルにします。
inspect skinny	SCCP アプリケーション検査をイネーブルにします。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

show sla monitor configuration

SLA オペレーションのデフォルトを含むコンフィギュレーション値を表示するには、ユーザ EXEC モードで **show sla monitor configuration** コマンドを使用します。

show sla monitor configuration [*sla-id*]

シンタックスの説明

sla-id	（オプション）SLA オペレーションの ID 番号。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合、すべての SLA オペレーションのコンフィギュレーション値が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

実行コンフィギュレーションの SLA オペレーション コマンドを表示するには、**show running config sla monitor** コマンドを使用します。

例

次に、**show sla monitor** コマンドの出力例を示します。SLA オペレーション 123 のコンフィギュレーション値が表示されます。**show sla monitor** コマンドの出力に続いて、同じ SLA オペレーションの **show running-config sla monitor** コマンドが出力されます。

```
hostname> show sla monitor 124

SA Agent, Infrastructure Engine-II
Entry number: 124
Owner:
Tag:
Type of operation to perform: echo
Target address: 10.1.1.1
Interface: outside
Number of packets: 1
Request size (ARR data portion): 28
Operation timeout (milliseconds): 1000
Type Of Service parameters: 0x0
Verify data: No
Operation frequency (seconds): 3
Next Scheduled Start Time: Start Time already passed
Group Scheduled : FALSE
Life (seconds): Forever
Entry Ageout (seconds): never
Recurring (Starting Everyday): FALSE
Status of entry (SNMP RowStatus): Active
Enhanced History:

hostname# show running-config sla monitor 124

sla monitor 124
 type echo protocol ipIcmpEcho 10.1.1.1 interface outside
 timeout 1000
 frequency 3
sla monitor schedule 124 life forever start-time now
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーションの SLA オペレーション コンフィギュレーション コマンドを表示します。
sla monitor	SLA 監視オペレーションを定義します。

show sla monitor operational-state

SLA オペレーションの操作状態を表示するには、ユーザ EXEC モードで **show sla monitor operational-state** コマンドを使用します。

show sla monitor operational-state [*sla-id*]

シンタックスの説明

sla-id	（オプション）SLA オペレーションの ID 番号。有効な値は 1 ～ 2147483647 です。

デフォルト

sla-id が指定されていない場合、すべての SLA オペレーションの統計情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

実行コンフィギュレーションの SLA オペレーション コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次に、**show sla monitor operational-state** コマンドの出力例を示します。

```
hostname> show sla monitor operationl-state

Entry number: 124
Modification time: 14:42:23.607 EST Wed Mar 22 2006
Number of Octets Used by this Entry: 1480
Number of operations attempted: 4043
Number of operations skipped: 0
Current seconds left in Life: Forever
Operational state of entry: Active
Last time this entry was reset: Never
Connection loss occurred: FALSE
Timeout occurred: TRUE
Over thresholds occurred: FALSE
Latest RTT (milliseconds): NoConnection/Busy/Timeout
Latest operation start time: 18:04:26.609 EST Wed Mar 22 2006
Latest operation return code: Timeout
RTT Values:
RTTAvg: 0       RTTMin: 0       RTTMax: 0
NumOfRTT: 0     RTTSum: 0       RTTSum2: 0
```

関連コマンド

コマンド	説明
show running-config sla monitor	実行コンフィギュレーションの SLA オペレーション コンフィギュレーション コマンドを表示します。
sla monitor	SLA 監視オペレーションを定義します。

show snmp-server statistics

SNMP サーバに関する統計情報を表示するには、特権 EXEC モードで **show snmp-server statistics** コマンドを使用します。

show snmp-server statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

この例は、SNMP サーバ統計情報を表示する方法を示しています。

```
hostname# show snmp-server statistics
0 SNMP packets input
    0 Bad SNMP version errors
    0 Unknown community name
    0 Illegal operation for community name supplied
    0 Encoding errors
    0 Number of requested variables
    0 Number of altered variables
    0 Get-request PDUs
    0 Get-next PDUs
    0 Get-bulk PDUs
    0 Set-request PDUs (Not supported)
0 SNMP packets output
    0 Too big errors (Maximum packet size 512)
    0 No such name errors
    0 Bad values errors
    0 General errors
    0 Response PDUs
    0 Trap PDUs
```

関連コマンド

コマンド	説明
snmp-server	SNMP を介してセキュリティ アプライアンスのイベント情報を提供します。
clear configure snmp-server	簡易ネットワーク管理プロトコル(SNMP)サーバをディセーブルにします。
show running-config snmp-server	SNMP サーバのコンフィギュレーションを表示します。

show ssh sessions

セキュリティ アプライアンス上のアクティブな SSH セッションの情報を表示するには、特権 EXEC モードで **show ssh sessions** コマンドを使用します。

show ssh *sessions* [*ip_address*]

シンタックスの説明

ip_address	（オプション）指定した IP アドレスのセッション情報だけを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

SID は、SSH セッションを識別する一意な番号です。Client IP は、SSH クライアントを実行しているシステムの IP アドレスです。Version は、SSH クライアントがサポートしているプロトコル バージョン番号です。SSH が SSH バージョン 1 のみサポートしている場合、Version カラムには 1.5 が表示されます。SSH クライアントが SSH バージョン 1 と SSH バージョン 2 の両方をサポートしている場合、Version カラムには 1.99 が表示されます。SSH クライアントが SSH バージョン 2 のみサポートしている場合、Version カラムには 2.0 が表示されます。Encryption カラムには、SSH クライアントが使用している暗号化のタイプが表示されます。State カラムには、クライアントとセキュリティ アプライアンスとの対話の進行状況が表示されます。Username カラムには、セッションで認証されているログイン ユーザ名が表示されます。

例

次に、**show ssh sessions** コマンドの出力例を示します。

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
```

関連コマンド

コマンド	説明
ssh disconnect	アクティブな SSH セッションを切断します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

show startup-config

スタートアップ コンフィギュレーションを表示するか、スタートアップ コンフィギュレーションがロードされたときのエラーを表示するには、特権 EXEC モードで **show startup-config** コマンドを使用します。

show startup-config [errors]

シンタックスの説明

errors	（オプション）セキュリティ アプライアンスがスタートアップ コンフィギュレーションをロードしたときに生成されたエラーを表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム[1]
特権 EXEC	•	•	•	•	•

1. **errors** キーワードは、シングルモードでシステム実行スペースでだけ使用できます。

コマンド履歴

リリース	変更内容
7.0(1)	**errors** キーワードが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、このコマンドは現在の実行スペース（システム コンフィギュレーションまたはセキュリティ コンテキスト）のスタートアップ コンフィギュレーションを表示します。

メモリからスタートアップ エラーを消去するには、**clear startup-config errors** コマンドを使用します。

例

次に、**show startup-config** コマンドの出力例を示します。

```
hostname# show startup-config
: Saved
: Written by enable_15 at 01:44:55.598 UTC Thu Apr 17 2003

Version 7.0(0)28
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
!
interface GigabitEthernet0/1
 shutdown
 nameif test
 security-level 0
 ip address 10.10.4.200 255.255.0.0
!

...
!
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
hostname firewall1
domain-name example.com
boot system disk0:/cdisk.bin
ftp mode passive
names
name 10.10.4.200 outside
access-list xyz extended permit ip host 192.168.0.4 host 150.150.0.3
!
ftp-map ftp_map
!
ftp-map inbound_ftp
 deny-request-cmd appe stor stou
!

...

Cryptochecksum:4edf97923899e712ed0da8c338e07e63
```

次に、**show startup-config errors** コマンドの出力例を示します。

```
hostname# show startup-config errors

ERROR: 'Mac-addresses': invalid resource name
*** Output from config line 18, "  limit-resource Mac-add..."
INFO: Admin context is required to get the interfaces
*** Output from config line 30, "arp timeout 14400"
Creating context 'admin'... WARNING: Invoked the stub function ibm_4gs3_context_
set_max_mgmt_sess
WARNING: Invoked the stub function ibm_4gs3_context_set_max_mgmt_sess
Done. (1)
*** Output from config line 33, "admin-context admin"
WARNING: VLAN *24* is not configured.
*** Output from config line 12, context 'admin', " nameif inside"
.....
*** Output from config line 37, "  config-url disk:/admin..."
```

関連コマンド

コマンド	説明
clear startup-config errors	メモリからスタートアップ エラーを消去します。
show running-config	実行コンフィギュレーションを表示します。

show sunrpc-server active

Sun RPC サービス用に開いているピンホールを表示するには、特権 EXEC モードで **show sunrpc-server active** コマンドを使用します。

show sunrpc-server active

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show sunrpc-server active コマンドは、NFS や NIS などの Sun RPC サービス用に開いているピンホールを表示するために使用します。

例

Sun RPC サービス用に開いているピンホールを表示するには、**show sunrpc-server active** コマンドを入力します。次に、**show sunrpc-server active** コマンドの出力例を示します。

```
hostname# show sunrpc-server active
        LOCAL           FOREIGN                 SERVICE TIMEOUT
        -----------------------------------------------
        192.168.100.2/0 209.165.200.5/32780     100005 00:10:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスから Sun リモート プロセッサ コール サービスを消去します。
clear sunrpc-server active	NFS や NIS などの Sun RPC サービス用に開いているピンホールを消去します。
inspect sunrpc	Sun RPC アプリケーション検査をイネーブルまたはディセーブルにし、使用されるポートを設定します。
show running-config sunrpc-server	Sun RPC サービスのコンフィギュレーションに関する情報を表示します。

show switch mac-address-table

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、特権 EXEC モードで **show switch mac-address-table** コマンドを使用してスイッチ MAC アドレス テーブルを表示します。

show switch mac-address-table

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、組み込みスイッチを持つモデル専用です。スイッチ MAC アドレス テーブルでは、スイッチ ハードウェアの各 VLAN 内にトラフィック用の MAC アドレス対スイッチ ポートのマッピングが維持されます。透過ファイアウォール モードの場合、**show mac-address-table** コマンドを使用して ASA ソフトウェアのブリッジ MAC アドレス テーブルを表示します。ブリッジ MAC アドレス テーブルでは、VLAN 間を通過するトラフィック用の MAC アドレス対 VLAN のインターフェイス マッピングが維持されます。

MAC アドレス エントリは 5 分間で無効になります。

例

次に、**show switch mac-address-table** コマンドの出力例を示します。

```
hostname# show switch mac-address-table
Legend: Age - entry expiration time in seconds

   Mac Address  | VLAN |       Type        | Age | Port
------------------------------------------------------
 000e.0c4e.2aa4 | 0001 |     dynamic       | 287 | Et0/0
 0012.d927.fb03 | 0001 |     dynamic       | 287 | Et0/0
 0013.c4ca.8a8c | 0001 |     dynamic       | 287 | Et0/0
 00b0.6486.0c14 | 0001 |     dynamic       | 287 | Et0/0
 00d0.2bff.449f | 0001 |     static        |  -  | In0/1
 0100.5e00.000d | 0001 | static multicast  |  -  | In0/1,Et0/0-7
Total Entries: 6
```

表 30-3 に、各フィールドの説明を示します。

表 30-3　show switch mac-address-table のフィールド

フィールド	説明
Mac Address	MAC アドレスを表示します。
VLAN	MAC アドレスに関連付けられている VLAN を表示します。
Type	MAC アドレスが、スタティック マルチキャスト アドレスとしてダイナミックにラーニングされたか、スタティックにラーニングされたかを示します。内部バックプレーン インターフェイスの場合にのみスタティック エントリになります。
Age	MAC アドレス テーブルにダイナミック エントリの経過時間を表示します。
:port	MAC アドレスを持つホストに到達できるスイッチ ポートを表示します。

関連コマンド

コマンド	説明
show mac-address-table	組み込みスイッチを持たないモデルの MAC アドレス テーブルを表示します。
show switch vlan	VLAN と物理 MAC アドレスの関連付けを表示します。

show switch vlan

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、特権 EXEC モードで **show switch vlan** コマンドを使用して VLAN と、関連付けられたスイッチ ポートを表示します。

show switch vlan

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、組み込みスイッチを持つモデル専用です。他のモデルでは、**show vlan** コマンドを使用します。

例

次に、**show switch vlan** コマンドの出力例を示します。

```
hostname# show switch vlan

VLAN Name                            Status    Ports
---- --------------------------------- --------- -------------
100  inside                          up        Et0/0, Et0/1
200  outside                         up        Et0/7
300  -                               down      Et0/1, Et0/2
400  backup                          down      Et0/3
```

表 30-4 に、各フィールドの説明を示します。

表 30-4　show switch vlan のフィールド

フィールド	説明
VLAN	VLAN 番号を表示します。
Name	VLAN インターフェイスの名前を表示します。名前が **nameif** コマンドを使用して設定されていない場合、または **interface vlan** コマンドがない場合、ダッシュ（-）が表示されます。
Status	up ステータスまたは down ステータスで、スイッチの VLAN からトラフィックを受信するか、スイッチの VLAN にトラフィックを送信するかを示します。VLAN が up ステータスになるには、VLAN のスイッチ ポートが最低でも 1 つ up 状態でなければなりません。
:port	各 VLAN に割り当てられたスイッチ ポートを表示します。1 つのスイッチ ポートが複数の VLAN についてリストされている場合、そのスイッチ ポートはトランク ポートです。上記の出力例は、Ethernet 0/1 が VLAN 100 および 300 を伝送するトランク ポートであることを示します。

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタを消去します。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show vlan	組み込みスイッチを持たないモデルの VLAN を表示します。
switchport mode	スイッチ ポートのモードをアクセスまたはトランク モードに設定します。

show tcpstat

セキュリティ アプライアンスの TCP スタックおよびセキュリティ アプライアンスで終端している TCP 接続のステータスを（デバッグのために）表示するには、特権 EXEC モードで **show tcpstat** コマンドを使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

show tcpstat

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show tcpstat コマンドを使用すると、TCP スタックおよびセキュリティ アプライアンスで終端している TCP 接続のステータスを表示できます。表 30-5 は、表示される TCP 統計情報を説明しています。

表 30-5　show tcpstat コマンドでの TCP 統計情報

統計情報	説明
tcb_cnt	TCP ユーザの数。
proxy_cnt	TCP プロキシの数。TCP プロキシは、ユーザ認可によって使用されます。
tcp_xmt pkts	TCP スタックによって送信されたパケットの数。
tcp_rcv good pkts	TCP スタックによって受信された正常なパケットの数。
tcp_rcv drop pkts	TCP スタックがドロップした受信パケットの数。
tcp bad chksum	不良チェックサムを保持していた受信パケットの数。
tcp user hash add	ハッシュ テーブルに追加された TCP ユーザの数。
tcp user hash add dup	新しい TCP ユーザを追加しようとしたときに、ユーザがすでにハッシュ テーブル内に存在していた回数。
tcp user srch hash hit	検索時に TCP ユーザがハッシュ テーブル内で検出された回数。
tcp user srch hash miss	検索時に TCP ユーザがハッシュ テーブル内で検出されなかった回数。
tcp user hash delete	TCP ユーザがハッシュ テーブルから削除された回数。
tcp user hash delete miss	TCP ユーザを削除しようとしたときに、ユーザがハッシュ テーブル内で検出されなかった回数。

表 30-5　show tcpstat コマンドでの TCP 統計情報（続き）

統計情報	説明
lip	TCP ユーザのローカル IP アドレス。
fip	TCP ユーザの外部 IP アドレス。
lp	TCP ユーザのローカル ポート。
fp	TCP ユーザの外部ポート。
st	TCP ユーザの状態（RFC 793 を参照）。表示される値を次に示します。 1　CLOSED 2　LISTEN 3　SYN_SENT 4　SYN_RCVD 5　ESTABLISHED 6　FIN_WAIT_1 7　FIN_WAIT_2 8　CLOSE_WAIT 9　CLOSING 10　LAST_ACK 11　TIME_WAIT
rexqlen	TCP ユーザの再送信キューの長さ。
inqlen	TCP ユーザの入力キューの長さ。
tw_timer	TCP ユーザの time_wait タイマーの値（ミリ秒）。
to_timer	TCP ユーザの非活動タイムアウト タイマーの値（ミリ秒）。
cl_timer	TCP ユーザのクローズ要求タイマーの値（ミリ秒）。
per_timer	TCP ユーザの持続タイマーの値（ミリ秒）。
rt_timer	TCP ユーザの再送信タイマーの値（ミリ秒）。
tries	TCP ユーザの再送信カウント。

例

次の例は、セキュリティ アプライアンスの TCP スタックのステータスを表示する方法を示しています。

```
hostname# show tcpstat
                CURRENT MAX     TOTAL
tcb_cnt         2       12      320
proxy_cnt       0       0       160

tcp_xmt pkts = 540591
tcp_rcv good pkts = 6583
tcp_rcv drop pkts = 2
tcp bad chksum = 0
tcp user hash add = 2028
tcp user hash add dup = 0
tcp user srch hash hit = 316753
tcp user srch hash miss = 6663
tcp user hash delete = 2027
tcp user hash delete miss = 0

lip = 172.23.59.230 fip = 10.21.96.254 lp = 443 fp = 2567 st = 4 rexqlen = 0
in0
  tw_timer = 0 to_timer = 179000 cl_timer = 0 per_timer = 0
rt_timer = 0
tries 0
```

関連コマンド

コマンド	説明
show conn	使用されている接続と使用可能な接続を表示します。

show tech-support

テクニカル サポート アナリストが診断時に使用する情報を表示するには、特権 EXEC モードで **show tech-support** コマンドを使用します。

show tech-support [**detail** | **file** | **no-config**]

シンタックスの説明

detail	（オプション）詳細情報を表示します。
file	（オプション）コマンドの出力をファイルに書き込みます。
no-config	（オプション）実行コンフィギュレーションの出力を除外します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	***detail*** キーワードと ***file*** キーワードが追加されました。
7.2(1)	出力表示が拡張され、CPU を占有しているプロセスに関して、さらに詳細な情報が表示されるようになりました。

使用上のガイドライン

show tech-support コマンドでは、テクニカル サポート アナリストが問題を診断する場合に役立つ情報が表示されます。**show** コマンドからの出力を組み合せて、テクニカル サポート アナリストに対して最も多くの情報を提供します。

例

次の例は、テクニカル サポートで分析に使用する情報を、実行コンフィギュレーションの出力を除外して表示する方法を示しています。

```
hostname# show tech-support no-config

Cisco XXX Firewall Version X.X(X)
Cisco Device Manager Version X.X(X)

Compiled on Fri 15-Apr-05 14:35 by root

XXX up 2 days 8 hours

Hardware:   XXX, 64 MB RAM, CPU Pentium 200 MHz
Flash i28F640J5 @ 0x300, 16MB
BIOS Flash AT29C257 @ 0xfffd8000, 32KB

0: ethernet0: address is 0003.e300.73fd, irq 10
1: ethernet1: address is 0003.e300.73fe, irq 7
2: ethernet2: address is 00d0.b7c8.139e, irq 9
```

```
Licensed Features:
Failover:           Disabled
VPN-DES:            Enabled
VPN-3DES-AES:       Disabled
Maximum Interfaces: 3
Cut-through Proxy:  Enabled
Guards:             Enabled
URL-filtering:      Enabled
Inside Hosts:       Unlimited
Throughput:         Unlimited
IKE peers:          Unlimited

This XXX has a Restricted (R) license.

Serial Number: 480430455 (0x1ca2c977)
Running Activation Key: 0xc2e94182 0xc21d8206 0x15353200 0x633f6734
Configuration last modified by enable_15 at 23:05:24.264 UTC Sat Nov 16 2002

------------------ show clock ------------------

00:08:14.911 UTC Sun Apr 17 2005

------------------ show memory ------------------

Free memory:        50708168 bytes
Used memory:        16400696 bytes
-------------     ----------------
Total memory:       67108864 bytes

------------------ show conn count ------------------

0 in use, 0 most used

------------------ show xlate count ------------------

0 in use, 0 most used

------------------ show blocks ------------------

  SIZE    MAX    LOW    CNT
     4   1600   1600   1600
    80    400    400    400
   256    500    499    500
  1550   1188    795    919

------------------ show interface ------------------

interface ethernet0 "outside" is up, line protocol is up
  Hardware is i82559 ethernet, address is 0003.e300.73fd
  IP address 172.23.59.232, subnet mask 255.255.0.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        1267 packets input, 185042 bytes, 0 no buffer
        Received 1248 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        20 packets output, 1352 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 9 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (13/128) software (0/2)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet1 "inside" is up, line protocol is down
  Hardware is i82559 ethernet, address is 0003.e300.73fe
  IP address 10.1.1.1, subnet mask 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        1 packets output, 60 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
```

```
        0 babbles, 0 late collisions, 0 deferred
        1 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/1)
interface ethernet2 "intf2" is administratively down, line protocol is down
  Hardware is i82559 ethernet, address is 00d0.b7c8.139e
  IP address 127.0.0.1, subnet mask 255.255.255.255
  MTU 1500 bytes, BW 10000 Kbit half duplex
        0 packets input, 0 bytes, 0 no buffer
        Received 0 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 packets output, 0 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 babbles, 0 late collisions, 0 deferred
        0 lost carrier, 0 no carrier
        input queue (curr/max blocks): hardware (128/128) software (0/0)
        output queue (curr/max blocks): hardware (0/0) software (0/0)

------------------ show cpu usage ------------------

CPU utilization for 5 seconds = 0%; 1 minute: 0%; 5 minutes: 0%

------------------ show cpu hogging process ------------------

Process:      fover_parse, NUMHOG: 2, MAXHOG: 280, LASTHOG: 140
LASTHOG At:   02:08:24 UTC Jul 24 2005
PC:           11a4d5
Traceback:    12135e  121893  121822  a10d8b  9fd061  114de6 113e56f
              777135  7a3858  7a3f59  700b7f  701fbf  14b984

------------------ show process ------------------


    PC       SP       STATE       Runtime    SBASE     Stack Process
Hsi 001e3329 00763e7c 0053e5c8          0 00762ef4 3784/4096 arp_timer
Lsi 001e80e9 00807074 0053e5c8          0 008060fc 3832/4096 FragDBGC
Lwe 00117e3a 009dc2e4 00541d18          0 009db46c 3704/4096 dbgtrace
Lwe 003cee95 009de464 00537718          0 009dc51c 8008/8192 Logger
Hwe 003d2d18 009e155c 005379c8          0 009df5e4 8008/8192 tcp_fast
Hwe 003d2c91 009e360c 005379c8          0 009e1694 8008/8192 tcp_slow
Lsi 002ec97d 00b1a464 0053e5c8          0 00b194dc 3928/4096 xlate clean
Lsi 002ec88b 00b1b504 0053e5c8          0 00b1a58c 3888/4096 uxlate clean
Mwe 002e3a17 00c8f8d4 0053e5c8          0 00c8d93c 7908/8192 tcp_intercept_times
Lsi 00423dd5 00d3a22c 0053e5c8          0 00d392a4 3900/4096 route_process
Hsi 002d59fc 00d3b2bc 0053e5c8          0 00d3a354 3780/4096 XXX Garbage Collecr
Hwe 0020e301 00d5957c 0053e5c8          0 00d55614 16048/16384 isakmp_time_keepr
Lsi 002d377c 00d7292c 0053e5c8          0 00d719a4 3928/4096 perfmon
Hwe 0020bd07 00d9c12c 0050bb90          0 00d9b1c4 3944/4096 IPSec
Mwe 00205e25 00d9e1ec 0053e5c8          0 00d9c274 7860/8192 IPsec timer handler
Hwe 003864e3 00db26bc 00557920          0 00db0764 6952/8192 qos_metric_daemon
Mwe 00255a65 00dc9244 0053e5c8          0 00dc8adc 1436/2048 IP Background
Lwe 002e450e 00e7bb94 00552c30          0 00e7ad1c 3704/4096 XXX/trace
Lwe 002e471e 00e7cc44 00553368          0 00e7bdcc 3704/4096 XXX/tconsole
Hwe 001e5368 00e7ed44 00730674          0 00e7ce9c 7228/8192 XXX/intf0
Hwe 001e5368 00e80e14 007305d4          0 00e7ef6c 7228/8192 XXX/intf1
Hwe 001e5368 00e82ee4 00730534       2470 00e8103c 4892/8192 XXX/intf2
H*  0011d7f7 0009ff2c 0053e5b0        780 00e8511c 13004/16384 ci/console
Csi 002dd8ab 00e8a124 0053e5c8          0 00e891cc 3396/4096 update_cpu_usage
Hwe 002cb4d1 00f2bfbc 0051e360          0 00f2a134 7692/8192 uauth_in
Hwe 003d17d1 00f2e0bc 00828cf0          0 00f2c1e4 7896/8192 uauth_thread
Hwe 003e71d4 00f2f20c 00537d20          0 00f2e294 3960/4096 udp_timer
Hsi 001db3ca 00f30fc4 0053e5c8          0 00f3004c 3784/4096 557mcfix
Crd 001db37f 00f32084 0053ea40  121094970 00f310fc 3744/4096 557poll
Lsi 001db435 00f33124 0053e5c8          0 00f321ac 3700/4096 557timer
Hwe 001e5398 00f441dc 008121e0          0 00f43294 3912/4096 fover_ip0
Cwe 001dcdad 00f4523c 00872b48         20 00f44344 3528/4096 ip/0:0
Hwe 001e5398 00f4633c 008121bc          0 00f453f4 3532/4096 icmp0
Hwe 001e5398 00f47404 00812198          0 00f464cc 3896/4096 udp_thread/0
Hwe 001e5398 00f4849c 00812174          0 00f475a4 3832/4096 tcp_thread/0
```

```
Hwe 001e5398 00f495bc 00812150          0 00f48674 3912/4096 fover_ip1
Cwe 001dcdad 00f4a61c 008ea850          0 00f49724 3832/4096 ip/1:1
Hwe 001e5398 00f4b71c 0081212c          0 00f4a7d4 3912/4096 icmp1
Hwe 001e5398 00f4c7e4 00812108          0 00f4b8ac 3896/4096 udp_thread/1
Hwe 001e5398 00f4d87c 008120e4          0 00f4c984 3832/4096 tcp_thread/1
Hwe 001e5398 00f4e99c 008120c0          0 00f4da54 3912/4096 fover_ip2
Cwe 001e542d 00f4fa6c 00730534          0 00f4eb04 3944/4096 ip/2:2
Hwe 001e5398 00f50afc 0081209c          0 00f4fbb4 3912/4096 icmp2
Hwe 001e5398 00f51bc4 00812078          0 00f50c8c 3896/4096 udp_thread/2
Hwe 001e5398 00f52c5c 00812054          0 00f51d64 3832/4096 tcp_thread/2
Hwe 003d1a65 00f78284 008140f8          0 00f77fdc  300/1024 listen/http1
Mwe 0035cafa 00f7a63c 0053e5c8          0 00f786c4 7640/8192 Crypto CA

------------------ show failover ------------------

No license for Failover

------------------ show traffic ------------------

outside:
        received (in 205213.390 secs):
                1267 packets    185042 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205213.390 secs):
                20 packets      1352 bytes
                0 pkts/sec      0 bytes/sec
inside:
        received (in 205215.800 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.800 secs):
                1 packets       60 bytes
                0 pkts/sec      0 bytes/sec
intf2:
        received (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec
        transmitted (in 205215.810 secs):
                0 packets       0 bytes
                0 pkts/sec      0 bytes/sec

------------------ show perfmon ------------------


PERFMON STATS:    Current      Average
Xlates               0/s          0/s
Connections          0/s          0/s
TCP Conns            0/s          0/s
UDP Conns            0/s          0/s
URL Access           0/s          0/s
URL Server Req       0/s          0/s
TCP Fixup            0/s          0/s
TCPIntercept         0/s          0/s
HTTP Fixup           0/s          0/s
FTP Fixup            0/s          0/s
AAA Authen           0/s          0/s
AAA Author           0/s          0/s
AAA Account          0/s          0/s
```

関連コマンド

コマンド	説明
show clock	Syslog Server（PFSS）と公開キー インフラストラクチャ（PKI）プロトコルで使用されるクロックを表示します。
show conn count	使用されている接続と使用可能な接続を表示します。
show cpu	CPU の使用状況に関する情報を表示します。
show failover	接続のステータス、およびどのセキュリティ アプライアンスがアクティブになっているかを表示します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について、要約を表示します。
show perfmon	セキュリティ アプライアンスのパフォーマンスに関する情報を表示します。
show processes	動作しているプロセスのリストを表示します。
show running-config	セキュリティ アプライアンス上で現在実行されているコンフィギュレーションを表示します。
show xlate	変換スロットに関する情報を表示します。

show track

トラッキング プロセスにより追跡されたオブジェクトに関する情報を表示するには、ユーザ EXEC モードで **show track** コマンドを使用します。

show track [*track-id*]

シンタックスの説明

track-id	トラッキング エントリのオブジェクト ID。有効な値は 1 ～ 500 です。

デフォルト

track-id が提供されない場合、すべてのトラッキング オブジェクトに関する情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show track** コマンドの出力例を示します。

```
hostname(config)# show track

Track 5
    Response Time Reporter 124 reachability
    Reachability is UP
    2 changes, last change 03:41:16
    Latest operation return code: OK
    Tracked by:
        STATIC-IP-ROUTING 0
```

関連コマンド

コマンド	説明
show running-config track	実行コンフィギュレーションの **track rtr** コマンドを表示します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

show traffic

インターフェイスの送信アクティビティと受信アクティビティを表示するには、特権 EXEC モードで ***show traffic*** コマンドを使用します。

show traffic

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	ASA 5550 適応型セキュリティ アプライアンスのための特別な表示が追加されました。

使用上のガイドライン

show traffic コマンドは、show traffic コマンドが最後に入力された時点またはセキュリティ アプライアンスがオンラインになった時点以降に、各インターフェイスを通過したパケットの数とバイト数を表示します。秒数は、セキュリティ アプライアンスが直前のリブート以降、オンラインになってからの経過時間です（直前のリブート以降に **clear traffic** コマンドが入力されていない場合）。このコマンドが入力されていた場合、この秒数は、コマンドが入力された時点からの経過時間です。

ASA 5550 適応型セキュリティ アプライアンスの場合、**show traffic** コマンドはスロットごとの集約スループットも表示します。ASA 5550 適応型セキュリティ アプライアンスではスループットを最大限にするためにトラフィックが均一に配布されることが求められますが、この集約スループットの表示により、トラフィックが均一に配布されていることを簡単に判別できます。

例

次に、**show traffic** コマンドの出力例を示します。

```
hostname# show traffic
outside:
        received (in 102.080 secs):
                2048 packets 204295 bytes
                20 pkts/sec 2001 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 204056 bytes
                20 pkts/sec 1998 bytes/sec

Ethernet0:
        received (in 102.080 secs):
                2049 packets 233027 bytes
                20 pkts/sec 2282 bytes/sec
        transmitted (in 102.080 secs):
                2048 packets 232750 bytes
                20 pkts/sec 2280 bytes/sec
```

ASA 5550 適応型セキュリティ アプライアンスの場合、次のテキストが最後に表示されます。

```
---------------------------------------
        Per Slot Throughput Profile
---------------------------------------
  Packets-per-second profile:
    Slot 0:       3148  50%|***************
    Slot 1:       3149  50%|***************

  Bytes-per-second profile:
    Slot 0:     427044  50%|***************
    Slot 1:     427094  50%|***************
```

関連コマンド

コマンド	説明
clear traffic	送信アクティビティと受信アクティビティのカウンタをリセットします。

show uauth

現在認証されている 1 人またはすべてのユーザ、ユーザがバインドされているホスト IP、キャッシュされた IP およびポート認可情報を表示するには、特権 EXEC モードで **show uauth** コマンドを使用します。

show uauth [*username*]

シンタックスの説明

username	（オプション）表示するユーザ認証情報とユーザ認可情報をユーザ名で指定します。

デフォルト

ユーザ名を省略すると、すべてのユーザの認可情報が表示されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show uauth コマンドは、1 人またはすべてのユーザの AAA 認可キャッシュと AAA 認証キャッシュを表示します。

timeout コマンドと共に使用します。

各ユーザ ホストの IP アドレスには、認可キャッシュが付加されます。ユーザ ホストごとにアドレスとサービスのペアを最大 16 個までキャッシュできます。ユーザが適切なホストから、キャッシュされたサービスにアクセスしようとすると、セキュリティ アプライアンスはユーザを認可済みであると見なし、すぐに接続を代理処理します。ある Web サイトへのアクセスを一度認可されると、たとえば、イメージを読み込むときに、各イメージごとに認可サーバと通信しません（イメージが同じ IP アドレスからであると想定されます）。このプロセスにより、認可サーバ上でパフォーマンスが大幅に向上し、負荷も大幅に軽減されます。

show uauth コマンドの出力では、認証および認可の目的で認可サーバに提供されたユーザ名が表示されます。また、ユーザ名がバインドされている IP アドレス、ユーザが認証されただけであるか、キャッシュされたサービスを持っているかが表示されます。

（注） Xauth をイネーブルにすると、クライアントに割り当てられている IP アドレスのエントリが uauth テーブル（**show uauth** コマンドで表示できます）に追加されます。ただし、ネットワーク拡張モードで Easy VPN Remote 機能と共に Xauth を使用すると、ネットワーク間に IPSec トンネルが作成されるため、ファイアウォールの向こう側にいるユーザを 1 つの IP アドレスに関連付けることができません。したがって、Xauth の完了時に uauth エントリが作成されません。AAA 認可またはアカウンティング サービスが必要となる場合は、AAA 認証プロキシをイネーブルにして、ファイアウォールの向こう側にいるユーザを認証します。AAA 認証プロキシの詳細については、**aaa** コマンドの項を参照してください。

ユーザの接続がアイドルになった後にキャッシュを保持する期間を指定するには、**timeout uauth** コマンドを使用します。すべてのユーザのすべての認可キャッシュを削除するには、**clear uauth** コマンドを使用します。次回接続を作成するときには再認証される必要が生じます。

例

次に、ユーザが認証されておらず、1 人のユーザの認証が進行中である場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
                        Current    Most Seen
Authenticated Users       0          0
Authen In Progress        0          1
```

次に、3 人のユーザが認証され、セキュリティ アプライアンスを介してサービスを使用することを認可されている場合の **show uauth** コマンドの出力例を示します。

```
hostname(config)# show uauth
user 'pat' from 209.165.201.2 authenticated
user 'robin' from 209.165.201.4 authorized to:
   port 192.168.67.34/telnet    192.168.67.11/http     192.168.67.33/tcp/8001
        192.168.67.56/tcp/25    192.168.67.42/ftp
user 'terry' from 209.165.201.7 authorized to:
   port 192.168.1.50/http     209.165.201.8/http
```

関連コマンド

コマンド	説明
clear uauth	現在のユーザの認証情報と認可情報を削除します。
timeout	アイドル状態の最大継続時間を設定します。

show url-block

url-block バッファにあるパケット数、およびバッファ上限を超えたためまたは再送信のためにドロップされたパケット数（ある場合）を表示するには、特権 EXEC モードで **show url-block** コマンドを使用します。

show url-block [**block statistics**]

シンタックスの説明

block statistics	（オプション）ブロック バッファ使用状況の統計情報を表示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show url-block block statistics コマンドは、url-block バッファにあるパケット数、およびバッファ上限を超えたためまたは再送信のためにドロップされたパケット数（ある場合）を表示します。

例

次に、**show url-block** コマンドの出力例を示します。

```
hostname# show url-block
 | url-block url-mempool 128 | url-block url-size 4 | url-block block 128
```

URL ブロック バッファのコンフィギュレーションが表示されています。

次に、**show url-block block statistics** コマンドの出力例を示します。

```
hostname# show url-block block statistics

URL Pending Packet Buffer Stats with max block  128 |
Cumulative number of packets held: | 896
Maximum number of packets held (per URL): | 3
Current number of packets held (global): | 38
Packets dropped due to
 | exceeding url-block buffer limit: | 7546
 | HTTP server retransmission: | 10
Number of packets released back to client: | 0
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用状況カウンタを消去します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show url-cache statistics

N2H2 フィルタリング サーバまたは Websense フィルタリング サーバから受信された URL 応答に使用される、URL キャッシュに関する情報を表示するには、特権 EXEC モードで **show url-cache statistics** コマンドを使用します。

show url-cache statistics

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　**show url-cache statistics** コマンドは、次のエントリを表示します。

- Size：KB 単位で表したキャッシュ サイズ。**url-cache** *size* オプションを使用して設定します。
- Entries：キャッシュ サイズに基づくキャッシュ エントリの最大数。
- In Use：現在キャッシュにあるエントリ数。
- Lookups：セキュリティ アプライアンスがキャッシュ エントリを検索した回数。
- Hits：セキュリティ アプライアンスがキャッシュ内でエントリを検出した回数。

show perfmon コマンドを使用して、N2H2 Sentian または Websense フィルタリング アクティビティに関する追加情報を表示できます。

例

次に、**show url-cache statistics** コマンドの出力例を示します。

```
hostname# show url-cache statistics

URL Filter Cache Stats
----------------------
 | Size :     1KB
 Entries :     36
  In Use :     30
 Lookups :     300
 | Hits :     290
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバから受信した応答の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show url-server

URL フィルタリング サーバに関する情報を表示するには、特権 EXEC モードで **show url-server** コマンドを使用します。

show url-server statistics

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

show url-server statistics コマンドは、URL サーバ ベンダー、URL の合計数、許可された数、拒否された数、HTTPS 接続の合計数、許可された数、拒否された数、TCP 接続の合計数、許可された数、拒否された数、および URL サーバ ステータスを表示します。

show url-server コマンドは、次の情報を表示します。

- N2H2 の場合：**url-server (***if_name***) vendor n2h2 host** *local_ip* **port** *number* **timeout** *seconds* **protocol [{TCP | UDP}{version 1 | 4}]**
- Websense の場合：**url-server (***if_name***) vendor websense host** *local_ip* **timeout** *seconds* **protocol [{TCP | UDP}]**

例

次に、**show url-server statistics** コマンドの出力例を示します。

```
hostname## show url-server statistics
Global Statistics:
------------------
URLs total/allowed/denied         994387/155648/838739
URLs allowed by cache/server      70483/85165
URLs denied by cache/server       801920/36819
HTTPSs total/allowed/denied       994387/155648/838739
HTTPs allowed by cache/server     70483/85165
HTTPs denied by cache/server      801920/36819
FTPs total/allowed/denied         994387/155648/838739
FTPs allowed by cache/server      70483/85165
FTPs denied by cache/server       801920/36819
Requests dropped                  28715
Server timeouts/retries           567/1350
Processed rate average 60s/300s   1524/1344 requests/second
Denied rate average 60s/300s      35648/33022 requests/second
Dropped rate average 60s/300s     156/189 requests/second

URL Server Statistics:
----------------------
192.168.0.1                       UP
Vendor                            websense
Port                              17035
Requests total/allowed/denied     366519/255495/110457
Server timeouts/retries           567/1350
Responses received                365952
Response time average 60s/300s    2/1 seconds/request
192.168.0.2                       DOWN
Vendor                            websense
Port                              17035
Requests total/allowed/denied     0/0/0
Server timeouts/retries           0/0
Responses received                0
Response time average 60s/300s    0/0 seconds/request
. . .
URL Packets Sent and Received Stats:
------------------------------------
Message                 Sent    Received
STATUS_REQUEST          411     0
LOOKUP_REQUEST          366519  365952
LOG_REQUEST             0       NA

Errors:
-------
RFC noncompliant GET method     0
URL buffer update failure       0

Semantics:
This command allows the operator to display url-server statistics organized on a
global and per-server basis.  The output is reformatted to provide: more-detailed
information and per-server organization.

Supported Modes:
privileged
router || transparent
single || multi/context

Privilege:
ATTR_ES_CHECK_CONTEXT

Debug support:
N/A

Migration Strategy (if any):
N/A
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報を消去します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
url-block	Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

show version

ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンス キー、および関連する稼働時間データを表示するには、特権 EXEC モードで **show version** コマンドを使用します。

show version

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。
7.2(1)	ステートフル フェールオーバー モードでは、クラスタの稼働時間を示す行が表示されるように変更されました。

使用上のガイドライン　**show version** コマンドを使用すると、ソフトウェア バージョン、最後にリブートされて以降の動作時間、プロセッサ タイプ、フラッシュ パーティション タイプ、インターフェイス ボード、シリアル番号（BIOS ID）、アクティベーション キー値、ライセンス タイプ（R または UR）、および、コンフィギュレーションが最後に変更されたときのタイムスタンプを表示できます。

show version コマンドで表示されるシリアル番号は、フラッシュ パーティション BIOS のものです。シャーシのシリアル番号とは異なります。ソフトウェア アップグレードを取得する場合は、シャーシ番号ではなく、**show version** コマンドで表示されるシリアル番号が必要です。

(注)　稼働時間の値は、フェールオーバー セットが動作している期間の長さを示しています。1 台の装置が動作を停止した場合、他の装置が動作を継続している限り、稼働時間の値は増加していきます。

例

次の例は、ソフトウェア バージョン、ハードウェア コンフィギュレーション、ライセンスキー、および関連する稼働時間データを表示する方法を示しています。ステートフル フェールオーバーが設定されている環境では、フェールオーバー クラスタの稼働時間を示す追加の行が表示されます。フェールオーバーが設定されていない場合、この行は表示されません。

```
hostname# show version

Cisco PIX Security Appliance Software Version 7.0(4)
Device Manager Version 5.0(4)

Compiled on Tue 27-Sep-05 10:41 by root
System image file is "flash:/cdisk.bin"
Config file at boot was "startup-config"

pix2 up 7 days 7 hours
failover cluster up 2 mins 44 secs


Hardware:   PIX-515E, 128 MB RAM, CPU Pentium II 433 MHz
Flash E28F128J3 @ 0xfff00000, 16MB
BIOS Flash AM29F400B @ 0xfffd8000, 32KB

 0: Ext: Ethernet0           : address is 0011.2094.1d2b, irq 10
 1: Ext: Ethernet1           : address is 0011.2094.1d2c, irq 11

Licensed features for this platform:
Maximum Physical Interfaces : 6
Maximum VLANs               : 25
Inside Hosts                : Unlimited
Failover                    : Active/Active
VPN-DES                     : Enabled
VPN-3DES-AES                : Enabled
Cut-through Proxy           : Enabled
Guards                      : Enabled
URL Filtering               : Enabled
Security Contexts           : 5
GTP/GPRS                    : Enabled
VPN Peers                   : Unlimited

This platform has an Unrestricted (UR) license.

Serial Number: 808184143
Running Activation Key: 0xcf22f25d 0xec1c3174 0x8cb138a0 0xaad8b878 0x4f32fd90
Configuration last modified by enable_15 at 14:18:26.103 UTC Thu Oct 6 2005
hostname#
```

関連コマンド

コマンド	説明
show hardware	ハードウェアの詳細情報を表示します。
show serial	ハードウェアのシリアル情報を表示します。
show uptime	セキュリティ アプライアンスが動作している期間の長さを表示します。

show vlan

セキュリティ アプライアンスに設定されているすべての VLAN を表示するには、特権 EXEC モードで **show vlan** コマンドを使用します。

show vlan

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、設定されている VLAN を表示します。

```
hostname# show vlan
10-11, 30, 40, 300
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタを消去します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。

show vpn load-balancing

VPN ロードバランシング仮想クラスタのコンフィギュレーションに関する実行時統計情報を表示するには、グローバル コンフィギュレーション モード、特権 EXEC モード、または VPN ロードバランシング モードで **show vpn load-balancing** コマンドを使用します。

show vpn load-balancing

シンタックスの説明

このコマンドには、引数も変数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—
特権 EXEC	•	—	•	—	—
VPN ロードバランシング	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.1(1)	出力例の Load (%) 表示および Session 表示に、個別の IPSec カラムおよび SSL カラムが追加されました。

使用上のガイドライン

show vpn load-balancing コマンドは、仮想 VPN ロードバランシング クラスタに関する統計情報を表示します。ローカル デバイスが VPN ロードバランシング クラスタに参加していない場合、このコマンドは、このデバイスには VPN ロードバランシングが設定されていないことを通知します。

出力のアスタリスク（*）は、接続しているセキュリティ アプライアンスの IP アドレスを示します。

例

次の例は、ローカル デバイスが VPN ロードバランシング クラスタに参加している場合の **show vpn load-balancing** コマンドおよびその出力を示しています。

```
hostname(config-load-balancing)# show vpn load-balancing

Status: enabled
Role: Master
Failover: n/a
Encryption: enabled
Cluster IP: 192.168.1.100
Peers: 1
                                          Load (%)          Sessions
Public IP       Role   Pri     Model      IPSec  SSL       IPSec   SSL
------------------------------------------------------------------------------
* 192.168.1.40  Master 10      PIX-515      0       0         0       0
  192.168.1.110  Backup   5 PIX-515        0       0         0       0
hostname(config-load-balancing)#
```

ローカル デバイスが VPN ロードバランシング クラスタに参加していない場合、**show vpn load-balancing** コマンドは、上とは異なる次のような結果を表示します。

```
hostname(config)# show vpn load-balancing
VPN Load Balancing has not been configured.
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	コンフィギュレーションから **vpn load-balancing** コマンド文を削除します。
show running-config vpn load-balancing	現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示します。
vpn load-balancing	VPN ロードバランシング モードに入ります。

show vpn-sessiondb

VPN セッションに関する情報を表示するには、特権 EXEC モードで **show vpn-sessiondb** コマンドを使用します。このコマンドには、情報を完全または詳細に表示するためのオプションが含まれています。表示するセッションのタイプを指定できるほか、情報をフィルタリングおよびソートするためのオプションが用意されています。「シンタックスの説明」の表と「使用上のガイドライン」で、それぞれの使用可能なオプションについて説明しています。

show vpn-sessiondb [detail] [full] {remote | l2l | index *indexnumber* | **webvpn | email-proxy} [filter {name** *username* **| ipaddress** *IPaddr* **| a-ipaddress** *IPaddr* **| p-ipaddress** *IPaddr* **| tunnel-group** *groupname* **| protocol** *protocol-name* **| encryption** *encryption-algo***}] [sort {name | ipaddress | a-ipaddress | p-ip address | tunnel-group | protocol | encryption}]**

シンタックスの説明

表示の詳細度	
detail	セッションに関する詳細な情報を表示します。たとえば、IPSec セッションに対して **detail** オプションを使用すると、IKE ハッシュ アルゴリズム、認証モード、キー再生成間隔などの追加の詳細情報が表示されます。 **detail** と **full** オプションを指定すると、セキュリティ アプライアンスはマシンで読み取り可能な形式で詳細出力を表示します。
filter	1 つ以上のフィルタ オプションを使用して、指定する情報のみを表示するように出力をフィルタリングします。詳細については、使用上の注意を参照してください。
full	連続した、短縮されていない出力を表示します。出力の各レコード間は、| 記号と || 文字列で区切られます。
sort	指定するソート オプションに従って出力をソートします。詳細については、使用上の注意を参照してください。
表示するセッション タイプ	
email-proxy	電子メールプロキシ セッションを表示します。電子メールプロキシ セッションに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**（接続名）、**ipaddress**（クライアント）、**encryption** を使用して情報をフィルタリングすることもできます。
index *indexnumber*	インデックス番号を指定して、単一のセッションを表示します。セッションのインデックス番号（1 ～ 750）を指定します。フィルタ オプションとソート オプションは適用されません。
l2l	VPN の LAN-to-LAN セッション情報を表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**、**ipaddress**、**protocol**、**encryption** を使用して情報をフィルタリングすることもできます。
remote	リモートアクセス セッションを表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションである **name**、**a-ipaddress**、**p-ipaddress**、**tunnel-group**、**protocol**、**encryption** を使用して情報をフィルタリングすることもできます。
webvpn	WebVPN セッションに関する情報を表示します。すべてのグループに関するこの情報をそのまま表示することも、フィルタ オプションとソート オプションである **name**、**ipaddress**、**encryption** を使用して情報をフィルタリングすることもできます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　次のオプションを使用して、セッションに関する表示内容をフィルタリングおよびソートできます。

フィルタ / ソート オプション	意味
filter a-ipaddress *IPaddr*	出力をフィルタリングして、指定した割り当て済み IP アドレス（複数可）についてのみ情報を表示します。
sort a-ipaddress	割り当て済み IP アドレスを基準として、表示内容をソートします。
filter encryption *encryption-algo*	出力をフィルタリングして、指定した暗号化アルゴリズム（複数可）を使用しているセッションについてのみ情報を表示します。
sort encryption	暗号化アルゴリズムを基準として、表示内容をソートします。暗号化アルゴリズムには、aes128、aes192、aes256、des、3des、rc4 が含まれます。
filter ipadddress *IPaddr*	出力をフィルタリングして、指定した内部 IP アドレス（複数可）についてのみ情報を表示します。
sort ipaddress	内部 IP アドレスを基準として、表示内容をソートします。
filter name *username*	出力をフィルタリングして、指定したユーザ名（複数可）に関するセッションを表示します。
sort name	ユーザ名を基準として、表示内容をアルファベット順でソートします。
filter p-address *IPaddr*	出力をフィルタリングして、指定した外部 IP アドレスについてのみ情報を表示します。
sort p-address	指定した外部 IP アドレス（複数可）を基準として、表示内容をソートします。
filter protocol *protocol-name*	出力をフィルタリングして、指定したプロトコル（複数可）を使用しているセッションについてのみ情報を表示します。
sort protocol	プロトコルを基準として、表示内容をソートします。プロトコルには、IKE、IMAP4S、IPSec、IPSecLAN2LAN、IPSecLAN2LANOverNatT、IPSecOverNatT、IPSecoverTCP、IPSecOverUDP、SMTPS、userHTTPS、vcaLAN2LAN が含まれます。

フィルタ / ソート オプション	意味
filter tunnel-group *groupname*	出力をフィルタリングして、指定したトンネル グループ（複数可）についてのみ情報を表示します。
sort tunnel-group	トンネル グループを基準として、表示内容をソートします。
| 記号	引数 {begin | include | exclude | grep | [-v]} {reg_exp} を使用して、出力を修正します。
<cr>	出力をコンソールに送信します。

特権 EXEC モードで入力した次の例では、LAN-to-LAN セッションに関する詳細な情報を表示しています。

```
hostname# show vpn-sessiondb detail l2l
Session Type: LAN-to-LAN Detailed
Connection   : 172.16.0.1
Index        : 1                     IP Addr      : 172.16.0.1
Protocol     : IPSecLAN2LAN          Encryption   : AES256
Bytes Tx     : 48484156              Bytes Rx     : 875049248
Login Time   : 09:32:03 est Mon Aug 2 2004
Duration     : 6:16:26
Filter Name  :

IKE Sessions: 1 IPSec Sessions: 2

IKE:
  Session ID   : 1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Main                  Auth Mode    : preSharedKeys
  Encryption   : AES256                Hashing      : SHA1
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 63814 Seconds
  D/H Group    : 5

IPSec:
  Session ID   : 2
  Local Addr   : 10.0.0.0/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel                PFS Group    : 5
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 10903 Seconds
  Bytes Tx     : 46865224              Bytes Rx     : 2639672
  Pkts Tx      : 1635314               Pkts Rx      : 37526


IPSec:
  Session ID   : 3
  Local Addr   : 10.0.0.1/255.255.255.0
  Remote Addr  : 209.165.201.30/255.255.255.0
  Encryption   : AES256                Hashing      : SHA1
  Encapsulation: Tunnel                PFS Group    : 5
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 6282 Seconds
  Bytes Tx     : 1619268               Bytes Rx     : 872409912
  Pkts Tx      : 19277                 Pkts Rx      : 1596809

hostname#
```

次の例は単一セッションの詳細を示します。

```
AsaNacDev# show vpn-sessiondb detail full index 4
Session Type: Remote Detailed |

Index: 1 | Username: dbrownhi | Tunnel Group: bxbvpnlab | IP Addr: 192.168.2.70 |
Public IP: 10.86.5.114 | Protocol: IPSec | Encryption: AES128 | Login Time: 15:22:46
EDT Tue May 10 2005 |Duration: 6h:57m:40s | Bytes Tx: 0 | Bytes Rx: 598357 | Client
Type: WinNT | Client Ver: 4.6.00.0049 | Filter Name: | NAC Result: Accepted | Posture
Token: Healthy ||

IKE Sessions: 1  | IPSec Sessions: 1  |  NAC Sessions: 1  |

Type: IKE | Session ID: 1 | Authentication Mode: preSharedKeysXauth | UDP Source Port:
500 | UDP Destination Port: 500 | IKE Negotiation Mode: Aggressive | Encryption: 3DES
| Hashing: MD5 | Diffie-Hellman Group: 2 | Rekey Time Interval: 86400 Seconds| Rekey
Left(T): 61341 Seconds ||

Type: IPSec | Session ID: 2 | Local IP Addr: 0.0.0.0 | Remote IP Addr: 192.168.2.70 |
Encryption: AES128 | Hashing: SHA1 | Encapsulation: Tunnel | Rekey Time Interval:
28800 Seconds | Rekey Left(T): 26794 Seconds | Bytes Tx: 0 | Bytes Rx: 598357 |
Packets Tx: 0 | Packets Rx: 8044 | ||

Type: NAC | Revalidation Time Interval: 3000 Seconds | Time Until Next Revalidation:
286 Seconds | Status Query Time Interval: 600 Seconds | EAPoUDP Session Age: 2714
Seconds | Hold-Off Time Remaining: 0 Seconds | Posture Token: Healthy | Redirect URL:
www.cisco.com ||

AsaNacDev# show vpn-sessiondb detail index 1

Session Type: Remote Detailed

Username     : dbrownhi
Index        : 1
Assigned IP  : 192.168.2.70          Public IP    : 10.86.5.114
Protocol     : IPSec                 Encryption   : AES128
Hashing      : SHA1
Bytes Tx     : 0                     Bytes Rx     : 604533
Client Type  : WinNT                 Client Ver   : 4.6.00.0049
Tunnel Group : bxbvpnlab
Login Time   : 15:22:46 EDT Tue May 10 2005
Duration     : 7h:02m:03s
Filter Name  :
NAC Result   : Accepted
Posture Token: Healthy

IKE Sessions: 1 IPSec Sessions: 1 NAC Sessions: 1

IKE:
  Session ID   : 1
  UDP Src Port : 500                   UDP Dst Port : 500
  IKE Neg Mode : Aggressive            Auth Mode    : preSharedKeysXauth
  Encryption   : 3DES                  Hashing      : MD5
  Rekey Int (T): 86400 Seconds         Rekey Left(T): 61078 Seconds
  D/H Group    : 2

IPSec:
  Session ID   : 2
  Local Addr   : 0.0.0.0
  Remote Addr  : 192.168.2.70
  Encryption   : AES128                Hashing      : SHA1
  Encapsulation: Tunnel
  Rekey Int (T): 28800 Seconds         Rekey Left(T): 26531 Seconds
  Bytes Tx     : 0                     Bytes Rx     : 604533
  Pkts Tx      : 0                     Pkts Rx      : 8126

NAC:
  Reval Int (T): 3000 Seconds          Reval Left(T): 286 Seconds
  SQ Int (T)   : 600 Seconds           EoU Age (T)  : 2714 Seconds
  Hold Left (T): 0 Seconds             Posture Token: Healthy
  Redirect URL : www.cisco.com
```

例に示されているように、**show vpn-sessiondb** コマンドに応答して表示されるフィールドは、入力するキーワードにより異なります。表 30-6 では、これらのフィールドについて説明しています。

表 30-6　show vpn-sessiondb コマンドのフィールド

フィールド	説明
Auth Mode	このセッションを認証するためのプロトコルまたはモード。
Bytes Rx	セキュリティ アプライアンスによりリモートのピアまたはクライアントから受信した合計バイト数。
Bytes Tx	セキュリティ アプライアンスによりリモートのピアまたはクライアントへ送信されたバイト数。
Client Type	リモート ピア上で実行されるクライアント ソフトウェア（可能な場合）。
Client Ver	リモート ピア上で実行されるクライアント ソフトウェアのバージョン。
Connection	接続名またはプライベート IP アドレス。
D/H Group	Diffie-Hellman グループ。IPSec SA 暗号キーを生成するためのアルゴリズムとキー サイズ。
Duration	セッション ログイン時刻から直前の画面リフレッシュまでの経過時間（HH:MM:SS）。
EAPoUDP Session Age	正常に完了した直前のポスチャ確認からの経過秒数。
Encapsulation	IPSec ESP（カプセル化セキュリティ ペイロード プロトコル）の暗号化と認証（つまり、ESP を適用した元の IP パケットの一部）を適用するためのモード。
Encryption	このセッションが使用しているデータ暗号化アルゴリズム（存在する場合）。
Encryption	このセッションが使用しているデータ暗号化アルゴリズム。
EoU Age (T)	EAPoUDP セッション経過時間。正常に完了した直前のポスチャ確認からの経過秒数。
Filter Name	セッション情報の表示を制限するよう指定されたユーザ名。
Hashing	パケットのハッシュを生成するためのアルゴリズムで、IPSec データ認証に使用されます。
Hold Left (T)	Hold-Off Time Remaining の略です。直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
Hold-Off Time Remaining	直前のポスチャ確認が正常に完了した場合は、0 秒です。それ以外の場合は、次回のポスチャ確認試行までの秒数です。
IKE Neg Mode	キー情報を交換し、SA を設定するための IKE（IPSec フェーズ 1）モード（アグレッシブまたはメイン）。
IKE Sessions	IKE（IPSec フェーズ 1）セッションの数で、通常は 1 です。これらのセッションは IPSec トラフィックのトンネルを確立します。
Index	このレコードの一意の ID。
IP Addr	このセッション用にリモート クライアントに割り当てられたプライベート IP アドレス。このアドレスは、内部 IP アドレスまたは仮想 IP アドレスとも呼ばれます。このアドレスにより、クライアントはプライベート ネットワークでホストと見なされます。

表 30-6　show vpn-sessiondb コマンドのフィールド

フィールド	説明
IPSec Sessions	IPSec（フェーズ 2）セッション（トンネル経由のデータ トラフィック セッション）の数。各 IPSec リモートアクセス セッションには 2 つの IPSec セッションがあります。1 つはトンネル エンドポイントで構成されるセッション、もう 1 つはトンネル経由で到達可能なプライベート ネットワークで構成されるセッションです。
Local IP Addr	トンネルのローカル エンドポイント（セキュリティ アプライアンス上のインターフェイス）に割り当てられた IP アドレス。
Login Time	セッションがログインした日付と時刻（MMM DD HH:MM:SS）。時刻は 24 時間表示です。
NAC Result	ネットワーク アドミッション コントロール ポスチャ確認の状態。状態は次のいずれかになります。 • Accepted：ACS は正常にリモート ホストのポスチャを確認しました。 • Rejected：ACS はリモート ホストの確認に失敗しました。 • Exempted：セキュリティ アプライアンスで設定されたポスチャ確認免除リストに従い、リモート ホストはポスチャ確認を免除されました。 • Non-Responsive：リモート ホストは EAPoUDP Hello メッセージに応答しませんでした。 • Hold-off：セキュリティ アプライアンスで、ポスチャ確認に成功した後、リモート ホストと EAPoUDP の通信が途絶えました。 • N/A：NAC は VPN NAC グループ ポリシーに応じてリモート ホストに対してディセーブルになります。 • Unknown：ポスチャ確認が進行中です。
NAC Sessions	ネットワーク アドミッション コントロール（EAPoUDP）セッションの数。
Packets Rx	セキュリティ アプライアンスによりリモート ピアから受信したパケット数。
Packets Tx	セキュリティ アプライアンスによりリモート ピアに送信されたパケット数。
PFS Group	完全転送秘密グループ数。
Posture Token	アクセス コントロール サーバ上で設定可能な情報テキスト文字列。ACS は、ポスチャ トークンを情報提供の目的でセキュリティ アプライアンスにダウンロードし、システムのモニタリング、レポート、デバッグ、およびロギングに使用します。通常のポスチャ トークンは、Healthy、Checkup、Quarantine、Infected、または Unknown です。
Protocol	セッションが使用しているプロトコル。
Public IP	クライアントに割り当てられた、パブリックにルーティング可能な IP アドレス。

表 30-6　show vpn-sessiondb コマンドのフィールド

フィールド	説明
Redirect URL	ポスチャ確認またはクライアントレス認証に続いて、ACS はセッションのアクセス ポリシーをセキュリティ アプライアンスにダウンロードします。Redirect URL は、アクセス ポリシー ペイロードのオプションの一部です。セキュリティ アプライアンスはリモート ホストのすべての HTTP（ポート 80）要求と HTTPS（ポート 443）要求を Redirect URL（存在する場合）にリダイレクトします。アクセス ポリシーに Redirect URL が含まれていない場合、セキュリティ アプライアンスはリモート ホストからの HTTP 要求と HTTPS 要求をリダイレクトしません。 Redirect URL は、IPSec セッションが終了するか、ポスチャ確認が実行されるまで有効です。ACS は、異なる Redirect URL が含まれるか、Redirect URL が含まれない新しいアクセス ポリシーを Redirect URL にダウンロードします。
Rekey Int (T)	IPSec（IKE）SA 暗号キーの有効期限。
Rekey Left (T)	IPSec（IKE）SA 暗号キーの残り有効期限。
Rekey Time Interval	IPSec（IKE）SA 暗号キーの有効期限。
Remote IP Addr	トンネルのリモート エンドポイントに割り当てられた IP アドレス（リモート ピア上のインターフェイス）。
Reval Int (T)	Revalidation Time Interval の略です。正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
Reval Left (T)	Time Until Next Revalidation の略です。直前のポスチャ確認試行が正常に完了しなかった場合は、0 秒です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Revalidation Time Interval	正常に完了した各ポスチャ確認間に、設ける必要のある間隔（秒単位）。
Session ID	セッション コンポーネント（サブセッション）の ID。各 SA には独自の ID があります。
Session Type	セッションのタイプ：LAN-to-LAN または Remote。
SQ Int (T)	Status Query Time Interval の略です。正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、セキュリティ アプライアンスがリモート ホストに発行する要求です。
Status Query Time Interval	正常に完了した各ポスチャ確認またはステータス クエリー応答から、次回のステータス クエリー応答までの間に空けることができる秒数です。ステータス クエリーは、直前のポスチャ確認以降にホストでポスチャが変化したかどうかを確認するために、セキュリティ アプライアンスがリモート ホストに発行する要求です。
Time Until Next Revalidation	直前のポスチャ確認試行が正常に完了しなかった場合は、0 秒です。それ以外の場合は、Revalidation Time Interval と、正常に完了した直前のポスチャ確認からの経過秒数との差です。
Tunnel Group	アトリビュート値を求めるために、このトンネルが参照するトンネル グループ名。

表 30-6　show vpn-sessiondb コマンドのフィールド

フィールド	説明
UDP Dst Port または UDP Destination Port	UDP についてリモート ピアが使用するポート番号。
UDP Src Port または UDP Source Port	UDP についてセキュリティ アプライアンスが使用するポート番号。
Username	セッションを確立するために使用したユーザのログイン名。

関連コマンド

コマンド	説明
show running-configuration vpn-sessiondb	VPN セッション データベースの実行コンフィギュレーションを表示します。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。
show vpn-sessiondb summary	すべての VPN セッションの要約を表示します。

show vpn-sessiondb ratio

現在のセッションについて、プロトコルまたは暗号化アルゴリズムごとの比率（%）を表示するには、特権 EXEC モードで **show vpn-sessiondb ratio** コマンドを使用します。

show vpn-sessiondb ratio {protocol | encryption} [filter *groupname***]**

シンタックスの説明

encryption	表示する暗号化プロトコルを指定します。フェーズ 2 暗号化について指定します。暗号化アルゴリズムには、次の種類があります。 aes128 / des aes192 / 3des aes256 / rc4
filter *groupname*	出力をフィルタリングして、指定するトンネル グループについてのみセッション比率を表示します。
protocol	表示するプロトコルを指定します。プロトコルには、次の種類があります。 IKE / SMTPS IMAP4S / userHTTPS IPSec / vcaLAN2LAN IPSecLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、**encryption** を引数として指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb ratio enc
Filter Group         : All
Total Active Sessions: 5
Cumulative Sessions  : 9

Encryption               Sessions        Percent
none                     0                0%
DES                      1               20%
3DES                     0                0%
AES128                   4        80%
AES192                   0                0%
AES256                   0                0%
```

次に、**protocol** を引数として指定した場合の **show vpn-sessiondb ratio** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb ratio protocol
Filter Group         : All
Total Active Sessions: 6
Cumulative Sessions  : 10

Protocol                 Sessions        Percent
IKE                      0                0%
IPSec                    1               20%
IPSecLAN2LAN             0                0%
IPSecLAN2LANOverNatT     0                0%
IPSecOverNatT            0                0%
IPSecOverTCP             1 20%
IPSecOverUDP             0                0%
L2TP                     0                0%
L2TPOverIPSec            0                0%
L2TPOverIPSecOverNatT    0                0%
PPPoE                    0                0%
vpnLoadBalanceMgmt       0                0%
userHTTPS                0                0%
IMAP4S                   3 30%
POP3S                    0                0%
SMTPS                    3 30%
```

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb summary	セッションの要約を表示します。現在のセッションの合計数、各タイプの現在のセッション数、ピーク時の数および累積合計数、最大同時セッション数を含んでいます。

show vpn-sessiondb summary

IPSec セッション、WebVPN セッション、およびネットワーク アドミッション コントロール セッションの要約を表示するには、特権 EXEC モードで **show vpn-sessiondb summary** コマンドを使用します。

show vpn-sessiondb summary

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ コンテキスト	システム
特権 EXEC	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、**show vpn-sessiondb summary** コマンドの出力例を示します。

```
hostname# show vpn-sessiondb summary

Active Sessions:                          Session Information:
  IPSec LAN-to-LAN       : 0                  Peak Concurrent        : 0
  IPSec Remote Access    : 0                  IPSec Limit            : 750
  WebVPN                 : 0                  WebVPN Limit           : 500
  SSL VPN Client (SVC)   : 0                  Cumulative Sessions    : 0
  Email Proxy            : 0
  Total Active Sessions  : 0                  Percent Session Load   : 0%
                                              VPN LB Mgmt Sessions   : 0

Active NAC Sessions:                      Cumulative NAC Sessions:
  Accepted               : 0                  Accepted               : 0
  Rejected               : 0                  Rejected               : 0
  Exempted               : 0                  Exempted               : 0
  Non-responsive         : 0                  Non-responsive         : 0
  Hold-off               : 0                  Hold-off               : 0
  N/A                    : 0                  N/A                    : 0
F1-asa1#
```

セッションとは、特定のピアで確立された VPN トンネルです。IPSec LAN-to-LAN トンネルは 1 つのセッションとしてカウントされ、トンネル経由で多くのホスト間接続が許可されます。IPSec リモート アクセス セッションは、1 つのユーザ接続をサポートする 1 つのリモート アクセス トンネルです。

表 30-7 では、アクティブ セッション テーブルとセッション情報テーブルのフィールドを説明します。

表 30-7　show vpn-sessiondb summary コマンド：アクティブ セッションとセッション情報のフィールド

フィールド	説明
Concurrent Limit	このセキュリティ アプライアンスで許可された、同時にアクティブなセッションの最大数。
Cumulative Sessions	セキュリティ アプライアンスが最後にブートまたはリセットされてからのすべてのタイプのセッション数。
LAN-to-LAN	現在アクティブな IPSec LAN-to-LAN セッション数。
Peak Concurrent	セキュリティ アプライアンスが最後にブートまたはリセットされてから、同時にアクティブであったすべてのタイプのセッションの最大数。
Percent Session Load	使用中の vpn セッション割り当てのパーセンテージ。この値は、Total Active Sessions を使用可能なセッションの最大数で割った値に等しく、パーセンテージで表示されます。使用可能なセッションの最大数は、次のいずれかの値です。 • ライセンスがある IPSec セッションと WebVPN セッションの最大数。 • 次のコマンドを使用して設定されたセッションの最大数。 — **vpn-sessiondb max-session-limit** — **vpn-sessiondb max-webvpn-session-limit**
Remote Access	現在アクティブな PPTP、L2TP、IPSec リモートアクセス ユーザ、L2TP over IPSec、IPSec through NAT セッション数。
Total Active Sessions	現在アクティブなすべてのタイプのセッション数。

アクティブな NAC セッション テーブルには、ポスチャ確認の対象であるリモート ピアに関する一般的な統計情報が表示されます。

NAC 累積セッション テーブルには、ポスチャ確認の対象である、あるいは以前から対象であったリモート ピアに関する一般的な統計情報が表示されます。

表 30-8 では、アクティブな NAC セッション テーブルと NAC 累積合計セッション テーブルのフィールドについて説明します。

表 30-8　show vpn-sessiondb summary コマンド：アクティブな NAC セッション テーブルと NAC 累積合計セッション テーブルのフィールド

フィールド	説明
Accepted	ポスチャ確認が成功し、アクセス コントロール サーバによりアクセス ポリシーが供与されたピアの数。
Exempted	セキュリティ アプライアンス上で設定されたポスチャ確認免除リストのエントリに一致しているため、ポスチャ確認の対象とならないピアの数。
Hold-off	セキュリティ アプライアンスがポスチャ確認に成功した後、EAPoUDP との通信が途絶えたピアの数。NAC Hold Timer アトリビュート（コンフィギュレーション > VPN > NAC）は、このタイプのイベントと、ピアごとの次のポスチャ確認試行間の遅延を指定します。
N/A	VPN NAC グループ ポリシーに応じて NAC がディセーブルになるピアの数。

表 30-8　show vpn-sessiondb summary コマンド：アクティブな NAC セッション テーブルと NAC 累積合計セッション テーブルのフィールド（続き）

フィールド	説明
Non-responsive	ポスチャ確認の際の EAP over UDP 要求に応答しないピアの数。CTA が実行されていないピアは、これらの要求に応答しません。セキュリティ アプライアンス コンフィギュレーションがクライアントレス ホストをサポートする場合、アクセス コントロール サーバはクライアントレス ホストに関連付けられているアクセス ポリシーをこれらのピアのセキュリティ アプライアンスにダウンロードします。クライアントレス ホストをサポートしない場合、セキュリティ アプライアンスは NAC デフォルト ポリシーを割り当てます。
Rejected	ポスチャ確認に失敗したか、アクセス コントロール サーバによりアクセス ポリシーを供与されなかったピアの数。

関連コマンド

コマンド	説明
show vpn-sessiondb	セッションを詳細情報付きまたは詳細情報なしで表示します。指定する基準に従って、フィルタリングおよびソートすることもできます。
show vpn-sessiondb ratio	VPN セッションの暗号化またはプロトコルの比率を表示します。

show wccp

Web Cache Communication Protocol（WCCP; Web キャッシュ通信プロトコル）に関連するグローバル統計情報を表示するには、特権 EXEC モードで **show wccp** コマンドを使用します。

show wccp {**web-cache** | *service-number*}[***detail*** | ***view***]

シンタックスの説明

web-cache	Web キャッシュ サービスの統計情報を指定します。
service-number	（オプション）キャッシュが制御する Web キャッシュ サービス グループの ID 番号。番号は 0 ～ 256 の範囲です。Cisco Cache Engine を使用する Web キャッシュの場合、逆プロキシ サービスは値 99 で示されます。
detail	（オプション）ルータとすべての Web キャッシュに関する情報を表示します。
view	（オプション）特定のサービス グループの他のメンバーが検出されたかどうかを表示します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、WCCP 情報を表示する方法を示します。

```
hostname(config)# show wccp
Global WCCP information:
    Router information:
        Router Identifier:                   -not yet determined-
        Protocol Version:                    2.0

    Service Identifier: web-cache
        Number of Cache Engines:             0
        Number of routers:                   0
        Total Packets Redirected:            0
        Redirect access-list:                foo
        Total Connections Denied Redirect:   0
        Total Packets Unassigned:            0
        Group access-list:                   foobar
        Total Messages Denied to Group:      0
        Total Authentication failures:       0
        Total Bypassed Packets Received:     0
asa1(config)#
```

関連コマンド

コマンド	説明
wccp	サービス グループを使用して、WCCP のサポートをイネーブルにします。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

show webvpn csd

CSD がイネーブルになっているかどうかを判別し、イネーブルであった場合に、実行コンフィギュレーションの CSD バージョンを表示するか、または CSD の配布パッケージが有効かどうかを確認するためにファイルをテストするには、特権 EXEC モードで **show webvpn csd** コマンドを使用します。

show webvpn csd [**image** *filename*]

シンタックスの説明

filename	CSD 配布パッケージとしての有効性をテストするファイル名を指定します。これは securedesktop_asa_<*n*>_<*n*>*.pkg の形式にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

CSD の動作ステータスを確認するには、**show webvpn csd** コマンドを使用します。このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- `Secure Desktop is not enabled.`

  CSD は実行コンフィギュレーション内にありますが、ディセーブルにされています。CSD をイネーブルにするには、webvpn コンフィギュレーション モードに入って **csd enable** コマンドを入力します。

- `Secure Desktop version n.n.n.n is currently installed and enabled.`

  CSD はイネーブルです。フラッシュ デバイスから読み込まれた配布パッケージがバージョン番号を判別します。Cisco Secure Desktop Manager には、ASDM Configuration > CSD のメニュー パスからアクセスできます。ユーザが CSD にアクセスできるのは、CSD コンフィギュレーションに場所が含まれる場合だけです。

ファイルが有効な CSD 配布パッケージであるかどうかをテストして確認するには、**show webvpn csd image** コマンドを使用します。同様に、webvpn コンフィギュレーション モードで **csd image** コマンドが入力された場合は、コマンドで指定したファイルが有効な CSD 配布パッケージである場合に限り、CSD がインストールされます。ファイルが無効である場合は、「ERROR: Unable to use CSD image」のメッセージが表示されます。

show webvpn csd image コマンドは、有効な CSD 配布パッケージであるかどうかを確認するためにファイルをテストしますが、ファイルが有効な場合でも、自動的に CSD がインストールされることはありません。このコマンドが入力されると、CLI は次のいずれかのメッセージで応答します。

- `ERROR: This is not a valid Secure Desktop image file.`

ファイル名が securedesktop_asa_<*n*>_<n>*.pkg の形式になっていることを確認します。形式が正しい場合は、ファイルを次の Web サイトから新たに取得したファイルで置き換えます。

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop

次に **show webvpn csd image** コマンドを再入力します。イメージが有効である場合は、webvpn コンフィギュレーション モードで **csd image** および **csd enable** コマンドを使用して、CSD をインストールしてイネーブルにします。

- This is a valid Cisco Secure Desktop image:
  Version ：3.1.0.25
  Built on : Wed 10/19/2005 14:51:23.82

  ファイルが有効な場合、CLI の応答にはバージョンと日付スタンプが含まれることに注意してください。

例

次の例は、CSD が実行コンフィギュレーションにインストールされてイネーブルにされたことを示しています。

```
hostname# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
hostname#
```

次の例は、指定されたファイルが有効な CSD イメージであることを示しています。

```
hostname#show webvpn csd image securedesktop_asa_3_1_0_25.pkg

This is a valid Cisco Secure Desktop image:
  Version  : 3.1.0.25
  Built on : Wed 10/19/2005 14:51:23.82

hostname#
```

関連コマンド

コマンド	説明
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。
csd image	コマンドで指定された CSD イメージを、パスで指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。

show webvpn group-alias

特定のトンネル グループまたはすべてのトンネル グループのエイリアスを表示するには、特権 EXEC モードで **group-alias** コマンドを使用します。

show webvpn group-alias [*tunnel-group*]

シンタックスの説明

tunnel-group	（オプション）グループ エイリアスを表示する特定のトンネル グループを指定します。

デフォルト

トンネル グループ名を入力しない場合、このコマンドはすべてのトンネル グループのすべてのエイリアスを表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1	このコマンドが導入されました。

使用上のガイドライン

show webvpn group-alias コマンドを入力するときには、WebVPN が実行されている必要があります。

各トンネル グループは、エイリアスを複数持つことも、まったく持たないこともあります。

例

次の例は、トンネル グループ「devtest」のエイリアスを表示する **show webvpn group-alias** コマンドと、そのコマンドの出力を示しています。

```
hostname# show webvpn group-alias devtest
QA
Fra-QA
```

関連コマンド

コマンド	説明
group-alias	グループに対して 1 つまたは複数の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

show webvpn group-url

特定のトンネル グループまたはすべてのトンネル グループの URL を表示するには、特権 EXEC モードで **group-url** コマンドを使用します。

show webvpn group-url [*tunnel-group*]

シンタックスの説明

tunnel-group	（オプション）URL を表示する特定のトンネル グループを指定します。

デフォルト

トンネル グループ名を入力しない場合、このコマンドはすべてのトンネル グループのすべての URL を表示します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

show webvpn group-url コマンドを入力するときには、WebVPN が実行されている必要があります。各グループは、エイリアスを複数持つことも、まったく持たないこともあります。

例

次の例は、トンネル グループ「frn-eng1」の URL を表示する **show webvpn group-url** コマンドと、そのコマンドの出力を示しています。

```
hostname# show webvpn group-url
http://www.cisco.com
https://fra1.vpn.com
https://fra2.vpn.com
```

関連コマンド

コマンド	説明
group-url	グループに対して 1 つまたは複数の URL を指定します。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

show webvpn sso-server

シングル サインオン サーバに関する動作統計情報を表示するには、特権 EXEC モードで **show webvpn sso-server** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

show webvpn sso-server *name*

シンタックスの説明

name	SSO サーバの名前を指定します。文字数は最小 4 文字から最大 32 文字までです。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。**show webvpn sso-server** コマンドは、設定済みである任意の SSO サーバまたはすべての SSO サーバの動作統計情報を表示します。

SSO サーバ名の引数が入力されない場合は、すべての SSO サーバの統計情報が表示されます。

例

特権 EXEC モードで入力した次の例では、example という名前の SSO サーバの統計情報が表示されます。

```
hostname# show webvpn sso-server example
Name: example
Type: SiteMinder
Authentication Scheme Version: 1.0
Web Agent URL: http://www.example.com/webvpn
Number of pending requests:         0
Number of auth requests:            0
Number of retransmissions:          0
Number of accepts:                  0
Number of rejects:                  0
Number of timeouts:                 0
Number of unrecognized responses:   0
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
request-timeout	失敗した SSO 認証試行がタイムアウトになるまでの秒数を指定します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

show webvpn svc

SVC インストレーションを表示するか、有効な SVC ファイルかどうかを確認するためにファイルをテストするには、特権 EXEC モードで **show webvpn svc** コマンドを使用します。

show webvpn svc [**image** *filename*]

シンタックスの説明

image *filename*	SVC イメージ ファイルとしての有効性をテストするファイル名を指定します。

デフォルト

このコマンドには、デフォルトの動作も値もありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

使用するために設定された既存の SVC イメージに関する情報を表示するには、**show webvpn svc** コマンドを使用します。

ファイルが有効な SVC イメージかどうかをテストして確認するには、**image** *filename* オプションを使用します。ファイルが有効な SVC イメージでない場合は、次のメッセージが表示されます。

```
ERROR: This is not a valid SSL VPN Client image file.
```

例

次の例は、現在インストールされている SVC イメージに対する **show webvpn svc** コマンドの出力を示しています。

```
hostname# show webvpn svc
1. windows.pkg 1
SSL VPN Client
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
2. window2.pkg 15
CISCO STC win2k+ 1.1.0
1,1,0,107
Thu 04/14/2005 09:27:54.43
```

次の例は、有効な SVC イメージに対する **show webvpn svc image** *filename* コマンドの出力を示しています。

```
F1(config-webvpn)# show webvpn svc image sslclient-win-1.0.2.127.pkg

This is a valid SSL VPN Client image:
  CISCO STC win2k+ 1.0.0
  1,0,2,127
  Fri 07/22/2005 12:14:45.43
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc enable	SVC ファイルをリモート コンピュータにダウンロードするためにセキュリティ アプライアンスをイネーブルにします。
svc image	セキュリティ アプライアンスが SVC ファイルをフラッシュ メモリから RAM にロードするように指定し、さらにセキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定します。

CHAPTER 31

shun コマンド～ sysopt radius ignore-secret コマンド

shun

新しい接続を阻止し、既存の接続からのパケットを拒否することによって、攻撃ホストへのダイナミックな応答をイネーブルにするには、特権 EXEC モードで **shun** コマンドを使用します。セキュリティ アプライアンスが排除のルックアップに使用する実際のアドレス（*src_ip*）に基づく排除をディセーブルにするには、このコマンドの **no** 形式を使用します。

shun *src_ip* [*dst_ip src_port dest_port* [*protocol*]] [**vlan** *vlan_id*]

no shun *src_ip* [**vlan** *vlan_id*]

シンタックスの説明

dest_port	（オプション）排除を引き起こす接続の宛先ポート。
dst_ip	（オプション）ターゲット ホストのアドレス。
protocol	（オプション）UDP や TCP などの IP プロトコル。*dst_ip* を指定する場合は必須です。
src_ip	攻撃ホストのアドレス。
src_port	（オプション）排除を引き起こす接続の送信元ポート。
vlan_id	（オプション）VLAN ID を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

shun コマンドを使用すると、攻撃を受けるインターフェイスにブロッキング機能を適用できます。攻撃ホストの IP 送信元アドレスを含むパケットは、ブロッキング機能が手動でまたは Cisco IPS マスター モジュールによって削除されるまで、ドロップされ記録されます。IP 送信元アドレスからのトラフィックはセキュリティ アプライアンスを通過できません。残っている接続はすべて、標準アーキテクチャの一部としてタイムアウトになります。**shun** コマンドのブロッキング機能は、指定したホスト アドレスとの接続が現在アクティブであるかどうかに関らず適用されます。

ホストの送信元 IP アドレスだけを指定して **shun** コマンドを使用する場合、デフォルトは 0 となります。攻撃ホストからのトラフィックは許可されません。

shun コマンドは、攻撃のダイナミックなブロックに使用されるため、セキュリティ アプライアンス コンフィギュレーションには表示されません。

インターフェイスを削除すると、そのインターフェイスに適用されている排除もすべて削除されます。新しいインターフェイスを追加する場合や、同じインターフェイス（同じ名前）を置き換える場合、そのインターフェイスを IPS センサーで監視するときは、そのインターフェイスを IPS センサーに追加する必要があります。

例

次の例は、攻撃ホスト（10.1.1.27）が TCP で攻撃対象（10.2.2.89）との接続を作成していることを示しています。接続は、セキュリティ アプライアンス接続テーブル内で次のように記載されています。

```
10.1.1.27, 555-> 10.2.2.89, 666 PROT TCP
```

shun コマンドを次のように適用したとします。

```
hostname# shun 10.1.1.27 10.2.2.89 555 666 tcp
```

上のコマンドにより、セキュリティ アプライアンス接続テーブルから接続が削除され、10.1.1.27 からのパケットがセキュリティ アプライアンスを通過できなくなります。攻撃ホストは、セキュリティ アプライアンスの内部にある場合も、外部にある場合もあります。

関連コマンド

コマンド	説明
clear shun	現在イネーブルであるすべての排除をディセーブルにして、排除統計情報を消去します。
show shun	排除情報を表示します。

shutdown

インターフェイスをディセーブルにするには、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを使用します。インターフェイスをイネーブルにするには、このコマンドの **no** 形式を使用します。

shutdown

no shutdown

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

物理インターフェイスは、デフォルトではすべてシャットダウンされます。セキュリティ コンテキスト内の割り当て済みインターフェイスは、コンフィギュレーション内ではシャットダウンされません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

物理インターフェイスは、デフォルトではすべてシャットダウンされます。イネーブルになっているサブインターフェイスをトラフィックが通過できるようにするには、物理インターフェイスを事前にイネーブルにしておく必要があります。マルチ コンテキスト モードの場合、物理インターフェイスまたはサブインターフェイスをコンテキストに割り当てると、インターフェイスはデフォルトではそのコンテキスト内でイネーブルになります。ただし、トラフィックがコンテキスト インターフェイスを通過するためには、そのインターフェイスをシステム コンフィギュレーションでもイネーブルにする必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、そのインターフェイスを共有しているすべてのコンテキストでダウンします。

例

次の例では、メインのインターフェイスをイネーブルにしています。

```
hostname(config)# interface gigabitethernet0/2
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

次の例では、サブインターフェイスをイネーブルにしています。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次の例では、サブインターフェイスをシャットダウンしています。

```
hostname(config)# interface gigabitethernet0/2.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に関するすべての変換をリセットして、接続をリセットします。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。

sla monitor

SLA オペレーションを作成するには、グローバル コンフィギュレーション モードで **sla monitor** コマンドを使用します。SLA オペレーションを削除するには、このコマンドの **no** 形式を使用します。

sla monitor *sla_id*

no sla monitor *sla_id*

シンタックスの説明

sla_id	設定する SLA の ID を指定します。SLA がまだ存在しない場合は、SLA が作成されます。有効な値は 1 ～ 2147483647 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

sla monitor コマンドを使用すると、SLA オペレーションを作成し、SLA モニタ コンフィギュレーション モードに入ります。このコマンドを入力すると、コマンド プロンプトが、SLA モニタ コンフィギュレーション モードに入っていることを示す `hostname(config-sla-monitor)#` に変更されます。SLA オペレーションがすでに存在していて、タイプがすでに SLA オペレーションに定義されている場合、プロンプトは `hostname(config-sla-monitor-echo)#` と表示されます。最大で 2000 の SLA オペレーションを作成できます。常時デバッグ可能な SLA オペレーションは 32 だけです。

no sla monitor コマンドは、指定した SLA オペレーションとそのオペレーションの設定に使用したコマンドを削除します。

SLA オペレーションの設定後に、**sla monitor schedule** コマンドを使用してそのオペレーションのスケジュールを設定する必要があります。SLA オペレーションのコンフィギュレーションは、オペレーションのスケジュールを設定した後は修正できません。スケジュールを設定した SLA オペレーションのコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して選択済みの SLA オペレーションを完全に削除する必要があります。SLA オペレーションを削除すると、関連付けられている **sla monitor schedule** コマンドも削除されます。この後に、SLA オペレーションのコンフィギュレーションを再度入力できます。

オペレーションの現在のコンフィギュレーション設定を表示するには、**show sla monitor configuration** コマンドを使用します。SLA オペレーションの操作統計情報を表示するには、**show sla monitor operation-state** コマンドを使用します。コンフィギュレーションの SLA コマンドを表示するには、**show running-config sla monitor** コマンドを使用します。

例

次の例では、ID が 123 の SLA オペレーションを設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA オペレーションを繰り返す頻度を指定します。
show sla monitor configuration	SLA コンフィギュレーションの設定を表示します。
sla monitor schedule	SLA オペレーションのスケジュールを設定します。
timeout	SLA オペレーションが応答を待機する期間を設定します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

sla monitor schedule

SLA オペレーションのスケジュールを設定するには、グローバル コンフィギュレーション モードで **sla monitor schedule** コマンドを使用します。SLA オペレーションのスケジュールの設定を削除し、保留状態にするには、このコマンドの **no** 形式を使用します。

sla monitor schedule *sla-id* [***life*** {***forever*** | *seconds*}] [***start-time*** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | ***pending*** | ***now*** | ***after*** *hh*:*mm*:*ss*}] [***ageout*** *seconds*] [***recurring***]

no sla monitor schedule *sla-id*

シンタックスの説明

after *hh*:*mm*:*ss*	コマンド入力後に、指定した時刻（時 : 分 : 秒）にオペレーションが開始されることを示します。
ageout *seconds*	（オプション）オペレーションが情報を収集していないときに、そのオペレーションをメモリに保存する秒数を指定します。SLA オペレーションは、無効になると、実行コンフィギュレーションから削除されます。
day	オペレーションを開始する日。有効値は 1 ～ 31 です。日が指定されていない場合、現在の日が使用されます。日を指定する場合、月も指定する必要があります。
hh:*mm*[:*ss*]	24 時間制で絶対開始時間を指定します。秒はオプションです。*month* と *day* を指定しない場合、次にこの指定した時間が来るとオペレーションが開始されます。
life forever	（オプション）オペレーションを無期限に実行するようにスケジュールを設定します。
life *seconds*	（オプション）オペレーションが情報を収集する秒数を指定します。
month	（オプション）オペレーションを開始する月。月が指定されない場合、現在の月が使用されます。月を指定する場合、日も指定する必要があります。 月の英語名を完全に入力するか、最初の 3 文字だけ入力します。
now	コマンドの入力と同時に、オペレーションを開始することを示します。
pending	情報を収集しないことを示します。これはデフォルトの状態です。
recurring	（オプション）オペレーションが毎日、指定の時刻に自動的に開始し、指定の期間実行されることを示します。
sla-id	スケジュールを設定する SLA オペレーションの ID。
start-time	SLA オペレーションを開始する時間を設定します。

デフォルト

デフォルトは次のとおりです。

- SLA オペレーションは、スケジュールされた時間になるまで、***pending*** 状態です。この状態では、オペレーションはイネーブルだが、データを収集しません。
- デフォルトの ***ageout*** 時間は 0 秒です（無効になりません）。
- デフォルトの ***life*** は 3600 秒（1 時間）です。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
	ルーテッド	透過	シングル	マルチ コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　SLA オペレーションがアクティブな状態の場合、ただちに情報を収集します。次の点線と W、X、Y、Z は、オペレーションが無効になるまでの段階を示しています。

```
W--------------------X--------------------Y--------------------Z
```

- W は、**sla monitor** コマンドを使用して、SLA オペレーションを設定した時間です。
- X は、SLA オペレーションの開始時間です。ここでオペレーションは「アクティブ」になります。
- Y は、**sla monitor schedule** コマンドによって設定された有効期間の終わりを示します（***life*** 秒は 0 になります）。
- Z は、オペレーションが無効になったことを示します。

オペレーションが無効になるまでの段階として、W が開始時点で、X と Y の間は中断、Y で設定サイズにリセットされて再開されます。SLA オペレーションが無効になると、SLA オペレーションのコンフィギュレーションは実行コンフィギュレーションから削除されます。オペレーションは実行される前に無効になる可能性があります（つまり、Z は X の前に発生する可能性があります）。オペレーションが実行前に無効にならないようにするには、設定時間（X）と開始時間（W）の差異は、無効にならない秒数にする必要があります。

recurring キーワードは、単一の SLA オペレーションのスケジュール設定でのみ使用できます。1 回 **sla monitor schedule** コマンドを実行するだけで、複数の SLA オペレーションのスケジュールを設定することはできません。繰り返し行われる SLA オペレーションの ***life*** 値は、1 日未満にする必要があります。繰り返し行われるオペレーションの ***ageout*** 値を「無期限」（値 0 で指定）にするか、***life*** 値と ***ageout*** 値の合計を 1 日より大きい値にする必要があります。recurring オプションを指定しない場合、オペレーションは既存の通常のスケジューリング モードで開始されます。

SLA オペレーションのコンフィギュレーションは、オペレーションのスケジュールを設定した後は修正できません。スケジュールされた SLA オペレーションのコンフィギュレーションを変更するには、**no sla monitor** コマンドを使用して、選択した SLA オペレーションを完全に削除します。SLA オペレーションを削除すると、関連付けられている **sla monitor schedule** コマンドも削除されます。この後に、SLA オペレーションのコンフィギュレーションを再度入力できます。

例　次の例では、4 月 5 日午後 3:00 にデータ収集を開始するようスケジュール設定した SLA オペレーション 25 を示します。このオペレーションは、アクティブでない状態で 12 時間経過すると無効になります。この SLA オペレーションが無効になると、SLA オペレーションのすべてのコンフィギュレーション情報が実行コンフィギュレーションから削除されます。

```
hostname(config)# sla monitor schedule 25 life 43200 start-time 15:00 apr 5 ageout
43200
```

次の例では、5 分間の遅延の後に、データ収集を開始するようスケジュール設定した SLA オペレーション 1 を示します。1 時間のデフォルトの有効時間が適用されます。

```
hostname(config)# sla monitor schedule 1 start after 00:05:00
```

次の例では、データ収集をただちに開始し、無期限に実行するようスケジュール設定された SLA オペレーション 3 を示します。

```
hostname(config)# sla monitor schedule 3 life forever start-time now
```

次の例では、毎日午前 1:30 にデータ収集を自動的に開始するようスケジュール設定された SLA オペレーション 15 を示します。

```
hostname(config)# sla monitor schedule 15 start-time 01:30:00 recurring
```

関連コマンド

コマンド	説明
show sla monitor configuration	SLA コンフィギュレーションの設定を表示します。
sla monitor	SLA 監視オペレーションを定義します。

smtps

SMTPS コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **smtps** コマンドを使用します。SMTPS コマンド モードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。SMTPS は、SSL 接続を通じた電子メール送信を可能にする TCP/IP プロトコルです。

smtps

no smtps

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例は、SMTPS コンフィギュレーション モードに入る方法を示しています。

```
hostname(config)# smtps
hostname(config-smtps)#
```

関連コマンド

コマンド	説明
clear configure smtps	SMTPS コンフィギュレーションを削除します。
show running-config smtps	SMTPS の実行コンフィギュレーションを表示します。

smtp-server

SMTP サーバを設定するには、グローバル コンフィギュレーション モードで **smtp-server** コマンドを使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

セキュリティ アプライアンスには、特定のイベントが発生したことを外部エンティティに通知するときにイベント システムが使用できる、内部 SMTP クライアントが含まれています。これらのイベント通知を SMTP サーバで受信して、指定した電子メール アドレスに転送するように SMTP サーバを設定することができます。SMTP ファシリティがアクティブになるのは、セキュリティ アプライアンスで電子メール イベントをイネーブルにしている場合だけです。

smtp-server {*primary_server*} [*backup_server*]

no smtp-server

シンタックスの説明

primary_server	プライマリ SMTP サーバを指定します。IP アドレスまたは DNS 名のいずれかを使用します。
backup_server	プライマリ SMTP サーバが使用不能になった場合に、イベント メッセージのリレー先となるバックアップ SMTP サーバを指定します。IP アドレスまたは DNS 名のいずれかを使用します。

デフォルト

デフォルトでは、SMTP サーバは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	—	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

例

次の例は、SMTP サーバの IP アドレスとして 10.1.1.24 を設定し、バックアップ SMTP サーバの IP アドレスとして 10.1.1.34 を設定する方法を示しています。

```
hostname(config)# smtp-server 10.1.1.24 10.1.1.34
```

関連コマンド

コマンド	説明

snmp-map

SNMP 検査のパラメータを定義している特定のマップを指定するには、グローバル コンフィギュレーション モードで **snmp-map** コマンドを使用します。マップを削除するには、このコマンドの **no** 形式を使用します。

snmp-map *map_name*

no snmp-map *map_name*

シンタックスの説明

map_name	SNMP マップの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

snmp-map コマンドは、SNMP 検査のパラメータを定義している特定のマップを指定するために使用します。このコマンドを入力すると、システムが SNMP マップ コンフィギュレーション モードに入って、個々のマップを定義するためのさまざまなコマンドを入力できるようになります。SNMP マップを定義した後は、**inspect snmp** コマンドを使用してマップをイネーブルにします。**class-map**、**policy-map**、および **service-policy** の各コマンドを使用して、トラフィックのクラスを定義し、**inspect** コマンドをクラスに適用し、ポリシーを 1 つまたはそれ以上のインターフェイスに適用します。

例

次の例は、SNMP トラフィックを識別し、SNMP マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する方法を示しています。

```
hostname(config)# access-list snmp-acl permit tcp any any eq 161
hostname(config)# access-list snmp-acl permit tcp any any eq 162
hostname(config)# class-map snmp-port
hostname(config-cmap)# match access-list snmp-acl
hostname(config-cmap)# exit
hostname(config)# snmp-map inbound_snmp
hostname(config-snmp-map)# deny version 1
hostname(config-snmp-map)# exit
hostname(config)# policy-map inbound_policy
hostname(config-pmap)# class snmp-port
hostname(config-pmap-c)# inspect snmp inbound_snmp
hostname(config-pmap-c)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用するトラフィックを拒否します。
inspect snmp	SNMP アプリケーション検査をイネーブルにします。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

snmp-server community

SNMP コミュニティ ストリングを設定するには、グローバル コンフィギュレーション モードで **snmp-server community** コマンドを使用します。コミュニティ ストリングを削除するには、このコマンドの **no** 形式を使用します。

snmp-server community *text*

no snmp-server community [*text*]

シンタックスの説明

text	コミュニティ ストリングを設定します。

デフォルト

デフォルトのコミュニティ ストリングは **public** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

SNMP コミュニティ ストリングは、SNMP 管理ステーションと、管理されているネットワーク ノードとの間での共有秘密です。セキュリティ アプライアンスは、キーを使用して、着信 SNMP 要求が有効であるかどうかを判断します。たとえば、サイトにコミュニティ ストリングを指定してから、ルータ、セキュリティ アプライアンス、および管理ステーションに同じストリングを設定できます。セキュリティ アプライアンスはこのストリングを使用しますが、無効なコミュニティ ストリングを持つ要求には応答しません。

例

次の例では、コミュニティ ストリングを wallawallabingbang に設定します。

```
hostname(config)# snmp-server community wallawallabingbang
```

関連コマンド

コマンド	説明
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホストのアドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server contact

SNMP の連絡先名を設定するには、グローバル コンフィギュレーション モードで **snmp-server contact** コマンドを使用します。連絡先名を削除するには、このコマンドの **no** 形式を使用します。

snmp-server contact *text*

no snmp-server contact [*text*]

シンタックスの説明

text	連絡先の担当者またはセキュリティ アプライアンスのシステム管理者の名前を指定します。名前は大文字と小文字が区別されます。最大 127 文字までです。スペースを使用できますが、複数のスペースは 1 つのスペースに短縮されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、連絡先として Pat Johnson を設定します。

```
hostname(config)# snmp-server contact Pat Johnson
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server enable	セキュリティ アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホストのアドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable

セキュリティ アプライアンス上で SNMP サーバをイネーブルにするには、グローバル コンフィギュレーション モードで **snmp-server enable** コマンドを使用します。SNMP をディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable

no snmp-server enable

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、SNMP サーバはイネーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用すると、SNMP トラップやその他のコンフィギュレーションを設定、再設定せずに、SNMP を簡単にイネーブル / ディセーブルにできます。

例

次の例では、SNMP をイネーブルにし、SNMP のホストとトラップを設定してから、トラップをシステム メッセージとして送信しています。

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホストのアドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server enable traps

セキュリティ アプライアンスをイネーブルにしてトラップを NMS に送信するには、グローバル コンフィギュレーション モードで **snmp-server enable traps** コマンドを使用します。トラップをディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

no snmp-server enable traps [**all** | **syslog** | **snmp** [*trap*] [...] | **entity** [*trap*] [...] | **ipsec** [*trap*] [...] | **remote-access** [*trap*]]

シンタックスの説明

all	すべてのトラップをイネーブルにします。
entity [*trap*]	エンティティ トラップをイネーブルにします。**entity** のトラップは次のとおりです。 • **config-change** • **fru-insert** • **fru-remove**
ipsec [*trap*]	IPSec トラップをイネーブルにします。**ipsec** のトラップは次のとおりです。 • **start** • **stop**
remote-access [*trap*]	リモート アクセス トラップをイネーブルにします。リモート アクセス トラップは次のとおりです。 • **session-threshold-exceeded**
snmp [*trap*]	SNMP トラップをイネーブルにします。デフォルトでは、SNMP トラップはすべてイネーブルです。**snmp** のトラップは次のとおりです。 • **authentication** • **linkup** • **linkdown** • **coldstart**
syslog	syslog トラップをイネーブルにします。

デフォルト

デフォルトのコンフィギュレーションでは、**snmp** トラップはすべてイネーブルです（**snmp-server enable traps snmp authentication linkup linkdown coldstart**）。これらのトラップをディセーブルにするには、**snmp** キーワードを指定してこのコマンドの **no** 形式を使用します。ただし、**clear configure snmp-server** コマンドは、SNMP トラップをデフォルトのイネーブルに戻します。

このコマンドを入力し、トラップのタイプを指定しない場合、デフォルトは **syslog** になります（デフォルトの **snmp** トラップは、**syslog** トラップと共に引き続きイネーブルのままです）。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン　機能タイプごとにこのコマンドを入力して、個々のトラップまたはトラップのセットをイネーブルにするか、**all** キーワードを入力してすべてのトラップをイネーブルにします。

トラップを NMS に送信するには、**logging history** コマンドを入力し、**logging enable** コマンドを使用してロギングをイネーブルにします。

例　次の例では、SNMP をイネーブルにし、SNMP のホストとトラップを設定してから、トラップをシステム メッセージとして送信しています。

```
hostname(config)# snmp-server enable
hostname(config)# snmp-server community wallawallabingbang
hostname(config)# snmp-server location Building 42, Sector 54
hostname(config)# snmp-server contact Sherlock Holmes
hostname(config)# snmp-server host perimeter 10.1.2.42
hostname(config)# snmp-server enable traps all
hostname(config)# logging history 7
hostname(config)# logging enable
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンス上で SNMP をイネーブルにします。
snmp-server host	SNMP ホストのアドレスを設定します。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server host

セキュリティ アプライアンス上で SNMP を使用できる NMS を指定するには、グローバル コンフィギュレーション モードで **snmp-server host** コマンドを使用します。NSM をディセーブルにするには、このコマンドの **no** 形式を使用します。

snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community** *text*] [**version** {**1** | **2c**}] [**udp-port** *port*]

no snmp-server host *interface_name ip_address* [**trap** | **poll**] [**community** *text*] [**version** {**1** | **2c**}] [**udp-port** *port*]

シンタックスの説明

community *text*	この NMS のコミュニティ ストリングを設定します。
host	トラップが送信される NMS の IP アドレス、または SNMP 要求の送信元の NMS の IP アドレスを指定します。
interface_name	NMS がセキュリティ アプライアンスと通信するインターフェイス名を指定します。
ip_address	SNMP トラップの送信先または SNMP 要求の送信元である NMS の IP アドレスを指定します。
trap	（オプション）トラップのみが送信され、このホストはブラウジング（ポーリング）を実行できないことを指定します。
poll	（オプション）このホストはブラウジング（ポーリング）を実行できるが、トラップは送信されないことを指定します。
udp-port *udp_port*	（オプション）通知の送信先とする UDP ポートを設定します。SNMP トラップは、デフォルトで UDP ポート 162 を使用して送信されます。
version {**1** | **2c**}	（オプション）SNMP 通知バージョンをバージョン 1 または 2c に設定します。

デフォルト

デフォルトの UDP ポートは 162 です。

デフォルトのバージョンは 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

最大で 32 の NMS を指定できます。

例

次の例では、ホストを境界インターフェイスに接続されている 10.1.2.42 に設定します。

```
hostname(config)# snmp-server host perimeter 10.1.2.42
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server listen-port

SNMP 要求のリッスン ポートを設定するには、グローバル コンフィギュレーション モードで **snmp-server listen-port** コマンドを使用します。デフォルト ポートに戻すには、このコマンドの **no** 形式を使用します。

snmp-server listen-port *lport*

no snmp-server listen-port *lport*

シンタックスの説明

lport	着信要求を受け入れるポート。デフォルト ポートは 161 です。[1]

1. **snmp-server *listen-port*** コマンドは、システム コンテキストでは使用できないため、管理テキストでのみ使用できます。

デフォルト

デフォルト ポートは 161 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例はリッスン ポートを 192 に設定します。

```
hostname(config)# snmp-server listen-port 192
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server location	SNMP サーバのロケーション文字列を設定します。

snmp-server location

SNMP にセキュリティ アプライアンスの場所を設定するには、グローバル コンフィギュレーション モードで **snmp-server location** コマンドを使用します。場所を削除するには、このコマンドの **no** 形式を使用します。

snmp-server location *text*

no snmp-server location [*text*]

シンタックスの説明

location *text*	セキュリティ アプライアンスの場所を指定します。**location** *text* は、大文字と小文字が区別される最大 127 文字の値です。スペースを使用できますが、複数のスペースは 1 つのスペースに短縮されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、場所を Building 42、Sector 54 として設定します。

```
hostname(config)# snmp-server location Building 42, Sector 54
```

関連コマンド

コマンド	説明
snmp-server community	SNMP コミュニティ ストリングを設定します。
snmp-server contact	SNMP の連絡先名を設定します。
snmp-server enable	セキュリティ アプライアンス上で SNMP をイネーブルにします。
snmp-server enable traps	SNMP トラップをイネーブルにします。
snmp-server host	SNMP ホストのアドレスを設定します。

software-version

サーバまたはエンド ポイントのソフトウェア バージョンを表示するサーバおよびユーザ エージェント ヘッダー フィールドを指定するには、パラメータ コンフィギュレーション モードで **software-version** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

software-version action {mask | log} [log]

no software-version action {mask | log} [log]

シンタックスの説明

mask	ソフトウェア バージョンに SIP メッセージ マスクを設定します。
log	違反が発生した場合、独自または追加のログを記録することを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は SIP 検査ポリシー マップでソフトウェア バージョンを識別する方法を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# software-version action log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

speed

銅線（RJ-45）イーサネット インターフェイスの速度を設定するには、インターフェイス コンフィギュレーション モードで **speed** コマンドを使用します。速度の設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

speed {***auto*** | ***10*** | ***100*** | ***1000*** | ***nonegotiate***}

no speed [***auto*** | ***10*** | ***100*** | ***1000*** | ***nonegotiate***]

シンタックスの説明

10	速度を 10BASE-T に設定します。
100	速度を 100BASE-T に設定します。
1000	速度を 1000BASE-T に設定します(銅線ギガビット イーサネットの場合のみ)。
auto	速度を自動検出します。
nonegotiate	ファイバ インターフェイスの場合は、速度を 1000 Mbps に設定し、リンク パラメータはネゴシエートしないでください。ファイバ インターフェイスに対して使用できる設定は、このコマンド、およびこのコマンドの **no** 形式だけです。この値を **no speed nonegotiate**（デフォルト）に設定すると、インターフェイスはリンクのネゴシエーションをイネーブルにして、フロー制御パラメータとリモート障害情報を交換します。

デフォルト

銅線インターフェイスの場合、デフォルトは **speed auto** です。

ファイバ インターフェイスの場合、デフォルトは **no speed nonegotiate** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

速度は、物理インターフェイスに対してのみ設定します。

ネットワークが自動検出をサポートしていない場合は、速度を特定の値に設定します。

ASA 5500 シリーズ適応型セキュリティ アプライアンスの RJ-45 インターフェイスでは、デフォルトのオートネゴシエーション設定に Auto-MDI/MDIX 機能も含まれています。Auto-MDI/MDIX は、オートネゴシエーション フェーズでストレート ケーブルが検出されると、内部クロスオーバーを実行して、クロス ケーブルによる接続を不要にします。インターフェイスで Auto-MDI/MDIX をイネーブルにするには、速度またはデュプレックス方式のいずれかをオートネゴシエーションに設定する必要があります。速度とデュプレックス方式の両方に明示的に固定値を設定して、両方の設定に関するオートネゴシエーションをディセーブルにすると、Auto-MDI/MDIX もディセーブルになります。

PoE ポートの速度を **auto** 以外に設定する場合（可能な場合）、IEEE 802.3af をサポートしない Cisco IP Phone とシスコの無線アクセス ポイントは検出されず給電されません。

例

次の例では、速度を 1000BASE-T に設定しています。

```
hostname(config)# interface gigabitethernet0/1
hostname(config-if)# speed 1000
hostname(config-if)# duplex full
hostname(config-if)# nameif inside
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear configure interface	インターフェイスのコンフィギュレーションをすべて消去します。
duplex	デュプレックス モードを設定します。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show interface	インターフェイスのランタイム ステータスと統計情報を表示します。
show running-config interface	インターフェイスのコンフィギュレーションを表示します。

split-dns

スプリット トンネルを介して解決されるドメインのリストを入力するには、グループ ポリシー コンフィギュレーション モードで **split-dns** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ドメインのリストをすべて削除するには、**no split-dns** コマンドを引数なしで使用します。**split-dns none** コマンドを発行して作成されたヌル リストを含めて、設定済みのスプリット トンネリング ドメインのリストがすべて削除されます。

スプリット トンネリング ドメインのリストがない場合、ユーザはデフォルト グループ ポリシーに含まれているリストを継承します。ユーザがこれらのスプリット トンネリング ドメイン リストを継承しないようにするには、**split-dns none** コマンドを使用します。

split-dns {**value** *domain-name1 domain-name2 domain-nameN* | **none**}

no split-dns [*domain-name domain-name2 domain-nameN*]

シンタックスの説明

value *domain-name*	スプリット トンネルを介してセキュリティ アプライアンスが解決するドメインの名前を提供します。
none	スプリット DNS リストがないことを指定します。スプリット DNS リストにヌル値を設定して、スプリット DNS リストを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからスプリット DNS リストを継承しないようにします。

デフォルト

スプリット DNS はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ドメインのリストに記述する各エントリは、1 個のスペースを使用して区切ります。エントリの数に制限はありませんが、エントリ文字列の長さは、255 文字を超えることはできません。使用できるのは、英数字、ハイフン（-）、およびピリオド（.）のみです。

no spilit-dns コマンドを引数なしで使用すると、**split-dns none** コマンドを発行して作成されたヌル値を含めて、現在の値がすべて削除されます。

例

次の例は、FirstGroup というグループ ポリシーに対して、スプリット トンネリングを介して解決されるドメイン Domain1、Domain2、Domain3、および Domain4 を設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-dns value Domain1 Domain2 Domain3 Domain4
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトのドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。
split-tunnel-policy	IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

split-tunnel-network-list

スプリット トンネリング用のネットワークのリストを作成するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-network-list** コマンドを使用します。ネットワークのリストを削除するには、このコマンドの **no** 形式を使用します。

スプリット トンネリング ネットワークのリストをすべて削除するには、**no split-tunnel-network-list** コマンドを引数なしで使用します。**split-tunnel-network-list none** コマンドを発行して作成されたヌル リストを含めて、設定済みのネットワーク リストがすべて削除されます。

スプリット トンネリング ネットワークのリストがない場合、ユーザは、デフォルト グループ ポリシーまたは指定したグループ ポリシーに含まれているネットワーク リストを継承します。ユーザがこれらのネットワーク リストを継承しないようにするには、**split-tunnel-network-list none** コマンドを使用します。

スプリット トンネリング ネットワークのリストは、トラフィックにトンネルの通過を要求するネットワークと、トンネリングを要求しないネットワークとを区別するためのものです。

split-tunnel-network-list {value *access-list name* **| none}**

no split-tunnel-network-list value [*access-list name*]

シンタックスの説明

value *access-list name*	トンネリングするネットワークまたはトンネリングしないネットワークを列挙したアクセス リストを指定します。
none	スプリット トンネリング用のネットワークのリストが存在しないことを指定します。セキュリティ アプライアンスは、すべてのトラフィックをトンネリングします。 スプリット トンネリング ネットワークのリストにヌル値を設定して、スプリット トンネリングを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから、スプリット トンネリング ネットワークのデフォルトのリストを継承しないようにします。

デフォルト

デフォルトでは、スプリット トンネリング ネットワークのリストはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、スプリット トンネリングを実行するかどうかをネットワーク リストに基づいて判断します。このリストは、プライベート ネットワーク上にあるアドレスのリストで構成される、標準的な ACL です。

no spilit-tunnel-network-list コマンドを引数なしで使用すると、**split-tunnel-network-list none** コマンドを発行して作成されたヌル値を含めて、現在のネットワーク リストがすべて削除されます。

例

次の例は、FirstGroup というグループ ポリシーに対して、FirstList というネットワーク リストを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-network-list FirstList
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成します。または、ダウンロード可能なアクセス リストを使用します。
default-domain	ドメイン フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトのドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-policy	IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようにします。

split-tunnel-policy

スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **split-tunnel-policy** コマンドを使用します。split-tunnel-policy のアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、スプリット トンネリングの値を別のグループ ポリシーから継承できます。

スプリット トンネリングを利用すると、リモートアクセス IPSec クライアントが、条件に応じて、パケットを暗号化された形式で IPSec トンネルを介して誘導したり、クリアテキスト形式でネットワーク インターフェイスに誘導したりできるようになります。スプリット トンネリングがイネーブルになっている場合、宛先が IPSec トンネルの向こう側ではないパケットについては、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングが不要です。

このコマンドは、このようなスプリット トンネリング ポリシーを特定のネットワークに適用するものです。

split-tunnel-policy {tunnelall | tunnelspecified | excludespecified}

no split-tunnel-policy

シンタックスの説明

excludespecified	トラフィックを暗号化なしで送信する宛先ネットワークのリストを定義します。この機能が役立つのは、企業ネットワークにトンネル経由で接続しながら、ローカル ネットワーク上のプリンタなどのデバイスにアクセスしようとするリモート ユーザです。このオプションが適用されるのは、Cisco VPN Client のみです。
split-tunnel-policy	トラフィックのトンネリング規則を設定することを指定します。
tunnelall	トラフィックを暗号化なしでは送信しないこと、またはセキュリティ アプライアンス以外の宛先に送信しないことを指定します。リモート ユーザは、インターネット ネットワークには企業ネットワークを通じて到達し、ローカル ネットワークにはアクセスできません。
tunnelspecified	指定したネットワークからのトラフィック、または指定したネットワークに向かうトラフィックをすべてトンネリングします。このオプションを指定すると、スプリット トンネリングがイネーブルになります。これによって、トンネリングの対象となるネットワークのアドレス リストを作成できるようになります。他のアドレス宛てのデータは、すべて暗号化なしで送信され、リモート ユーザのインターネット サービス プロバイダーによってルーティングされます。

デフォルト

デフォルト（tunnelall）では、スプリット トンネリングはディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

スプリット トンネリングは、本来はセキュリティ機能ではなくトラフィック管理機能です。最適なセキュリティを確保するには、スプリット トンネリングをイネーブルにしないことをお勧めします。

例

次の例は、FirstGroup というグループ ポリシーに対して、指定したネットワークのみトンネリングするスプリット トンネリング ポリシーを設定する方法を示しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# split-tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
default-domain	ドメイン フィールドを省略した DNS クエリーに対して、IPSec クライアントが使用するデフォルトのドメイン名を指定します。
split-dns	スプリット トンネルを介して解決されるドメインのリストを提供します。
split-tunnel-network-list none	スプリット トンネリング用のアクセス リストが存在しないことを指定します。トラフィックは、すべてトンネルを通過します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために、セキュリティ アプライアンスが使用するアクセス リストを指定します。

spoof-server

HTTP プロトコル検査のために、サーバ ヘッダー フィールドの文字列を置き換えるには、パラメータ コンフィギュレーション モードで **spoof-server** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

spoof-server *string*

no spoof-server *string*

シンタックスの説明

string	サーバ ヘッダー フィールドに代入する文字列。最大 82 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN ストリームは **spoof-server** コマンドの対象になりません。

例

次の例では、HTTP 検査ポリシー マップでサーバ ヘッダー フィールドの文字列を置き換える方法を示します。

```
hostname(config-pmap-p)# spoof-server string
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

ssh

セキュリティ アプライアンスへの SSH アクセスを追加するには、グローバル コンフィギュレーション モードで **ssh** コマンドを使用します。セキュリティ アプライアンスへの SSH アクセスをディセーブルにするには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

ssh {*ip_address mask* | *ipv6_address/prefix*} *interface*

no ssh {*ip_address mask* | *ipv6_address/prefix*} *interface*

シンタックスの説明

interface	SSH をイネーブルにするセキュリティ アプライアンス インターフェイス。指定しない場合は、外部インターフェイスを除くすべてのインターフェイスで SSH がイネーブルになります。
ip_address	セキュリティ アプライアンスへの SSH 接続の開始が認可されるホストまたはネットワークの IPv4 アドレス。ホストの場合は、ホスト名を入力することもできます。
ipv6_address/prefix	セキュリティ アプライアンスへの SSH 接続の開始が認可されるホストまたはネットワークの IPv6 アドレスとプレフィックス。
mask	*ip_address* のネットワーク マスク。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ssh *ip_address* コマンドは、セキュリティ アプライアンスへの SSH 接続の開始を認可するホストまたはネットワークを指定します。複数の ssh コマンドをコンフィギュレーションに含めることができます。このコマンドの **no** 形式は、特定の ssh コマンドをコンフィギュレーションから削除します。すべての ssh コマンドを削除するには、**clear configure ssh** コマンドを使用します。

SSH を使用してセキュリティ アプライアンスに接続するには、**crypto key generate rsa** コマンドを使用して、デフォルトの RSA キーをあらかじめ生成しておく必要があります。

セキュリティ アプライアンスでは、次のセキュリティ アルゴリズムと暗号がサポートされています。

- データ暗号化のための 3DES 暗号と AES 暗号
- パケットの完全性を保証するための HMAC-SHA アルゴリズムと HMAC-MD5 アルゴリズム
- ホスト認証のための RSA 公開キー アルゴリズム

- キー交換のための Diffie-Hellman Group 1 アルゴリズム

セキュリティ アプライアンスでは、次の SSH バージョン 2 機能はサポートされていません。

- X11 転送
- ポート転送
- SFTP サポート
- Kerberos と AFS のチケットの引き渡し
- データ圧縮

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
crypto key generate rsa	ID 証明書のための RSA キー ペアを生成します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
ssh scopy enable	セキュリティ アプライアンス上でセキュア コピー サーバをイネーブルにします。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

ssh disconnect

アクティブな SSH セッションを切断するには、特権 EXEC モードで **ssh disconnect** コマンドを使用します。

ssh disconnect *session_id*

シンタックスの説明

session_id	ID 番号で指定した SSH セッションを切断します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セッション ID を指定する必要があります。切断する SSH セッションの ID を取得するには、**show ssh sessions** コマンドを使用します。

例

次の例は、SSH セッションが切断される様子を示しています。

```
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.39    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
2   172.69.39.29    1.99    IN   3des-cbc   sha1     SessionStarted  pat
                            OUT  3des-cbc   sha1     SessionStarted  pat
hostname# ssh disconnect 2
hostname# show ssh sessions
SID Client IP       Version Mode Encryption Hmac     State           Username
0   172.69.39.29    1.99    IN   aes128-cbc md5      SessionStarted  pat
                            OUT  aes128-cbc md5      SessionStarted  pat
1   172.23.56.236   1.5     -    3DES       -        SessionStarted  pat
```

関連コマンド

コマンド	説明
show ssh sessions	セキュリティ アプライアンス上のアクティブな SSH セッションに関する情報を表示します。
ssh timeout	アイドル状態の SSH セッションのタイムアウト値を設定します。

ssh scopy enable

セキュリティ アプライアンス上でセキュア コピー（SCP）をイネーブルにするには、グローバル コンフィギュレーション モードで **ssh scopy enable** コマンドを使用します。SCP をディセーブルにするには、このコマンドの **no** 形式を使用します。

ssh scopy enable

no ssh scopy enable

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SCP は、サーバ専用の実装です。SCP のための接続を受け入れること、および終了することはできますが、開始することはできません。セキュリティ アプライアンスでは、次の制限事項があります。

- SCP のこの実装では、ディレクトリをサポートしていないため、セキュリティ アプライアンスの内部ファイルへのリモート クライアント アクセスだけを実行できます。
- SCP 使用時は、バナーをサポートしていません。
- SCP はワイルドカードをサポートしません。
- SSH バージョン 2 接続をサポートするには、セキュリティ アプライアンスのライセンスに VPN-3DES-AES 機能が含まれている必要があります。

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。
ssh version	セキュリティ アプライアンスが SSH Version 1 または SSH Version 2 のいずれかだけを使用するように制限します。

ssh timeout

デフォルトの SSH セッション アイドル タイムアウト値を変更するには、グローバル コンフィギュレーション モードで **ssh timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

ssh timeout *number*

no ssh timeout

シンタックスの説明

number	SSH セッションが切断されるまでに非アクティブ状態を維持する時間（分）を指定します。有効な値は 1 ～ 60 分です。

デフォルト

デフォルトのセッション タイムアウト値は 5 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ssh timeout コマンドは、セッションが切断されるまでにアイドル状態を維持する時間（分）を指定します。デフォルトの時間は 5 分です。

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続のみを受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
show ssh sessions	セキュリティ アプライアンス上のアクティブな SSH セッションに関する情報を表示します。
ssh disconnect	アクティブな SSH セッションを切断します。

ssh version

セキュリティ アプライアンスが受け入れる SSH のバージョンを制限するには、グローバル コンフィギュレーション モードで **ssh version** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。デフォルト値では、セキュリティ アプライアンスへの SSH バージョン 1 接続と SSH バージョン 2 接続が許可されます。

ssh version {***1*** | ***2***}

no ssh version [***1*** | ***2***]

シンタックスの説明

1	SSH バージョン 1 接続のみをサポートすることを指定します。
2	SSH バージョン 2 接続のみをサポートすることを指定します。

デフォルト

デフォルトでは、SSH バージョン 1 と SSH バージョン 2 の両方がサポートされます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

1 と 2 は、セキュリティ アプライアンスが使用する SSH のバージョンをいずれかに限定するように指定します。このコマンドの **no** 形式は、セキュリティ アプライアンスをデフォルトの状態である互換モード（両方のバージョンを使用可能）に戻します。

例

次の例は、IP アドレスが 10.1.1.1 である管理コンソールからの SSH バージョン 2 接続を受け入れるように内部インターフェイスを設定する方法を示しています。アイドル セッション タイムアウトを 60 分に設定し、SCP をイネーブルにしています。

```
hostname(config)# ssh 10.1.1.1 255.255.255.0 inside
hostname(config)# ssh version 2
hostname(config)# ssh copy enable
hostname(config)# ssh timeout 60
```

関連コマンド

コマンド	説明
clear configure ssh	実行コンフィギュレーションからすべての SSH コマンドを消去します。
debug ssh	SSH コマンドのデバッグ情報とエラー メッセージを表示します。
show running-config ssh	実行コンフィギュレーション内の現在の SSH コマンドを表示します。
ssh	指定したクライアントまたはネットワークからセキュリティ アプライアンスへの SSH 接続を許可します。

ssl client-version

セキュリティ アプライアンスがクライアントとして動作するときに使用する SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl client-version** コマンドを使用します。デフォルトの **any** に戻すには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、セキュリティ アプライアンスが送信する SSL/TLS のバージョンを限定できます。

ssl client-version [*any* | *sslv3-only* | *tlsv1-only*]

no ssl client-version

シンタックスの説明

any	セキュリティ アプライアンスは、SSL バージョン 3 の hello を送信し、SSL バージョン 3 または TLS バージョン 1 のいずれかをネゴシエートします。
sslv3-only	セキュリティ アプライアンスは、SSL バージョン 3 の hello を送信し、SSL バージョン 3 のみを受け入れます。
tlsv1-only	セキュリティ アプライアンスは、TLS バージョン 1 クライアントの hello を送信し、TLS バージョン 1 のみを受け入れます。

デフォルト

デフォルト値は、**any** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

TCP ポート転送は、WebVPN ユーザが一部の SSL バージョンを使用して接続している場合には機能しません。次に説明を示します。

Negotiate SSLv3	Java がダウンロードされる
Negotiate SSLv3/TLSv1	Java がダウンロードされる
Negotiate TLSv1	Java がダウンロードされない
TLSv1Only	Java がダウンロードされない
SSLv3Only	Java がダウンロードされない

問題となるのは、ポート転送アプリケーションを起動したときに、Java はクライアントの Hello パケットで SSLv3 のみをネゴシエートする点です。

例

次の例は、SSL クライアントとして動作するときに、TLSv1 だけを使用して通信するようにセキュリティ アプライアンスを設定する方法を示しています。

```
hostname(config)# ssl client-version tlsv1-only
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作するときに使用する、SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl encryption

SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **ssl encryption** コマンドを使用します。このコマンドをもう一度発行すると、直前の設定が上書きされます。アルゴリズムを使用する優先順位は、アルゴリズムの順序によって決まります。アルゴリズムを追加または削除して、使用している環境での要件を満たすようにしてください。デフォルト（すべての暗号化アルゴリズムが使用可能）に戻すには、このコマンドの **no** 形式を使用します。

ssl encryption [*3des-sha1*] [*des-sha1*] [*rc4-md5*] [*aes128-sha1*] [*aes256-sha1*] [*possibly others*]

no ssl encryption

シンタックスの説明

3des-sha1	Secure Hash Algorithm 1 を使用する Triple DES 暗号化を指定します。
des-sha1	Secure Hash Algorithm 1 を使用する DES 暗号化を指定します。
rc4-md5	MD5 ハッシュ関数を使用する RC4 暗号化を指定します。
aes128-sha1	Secure Hash Algorithm 1 を使用する Triple AES 128 ビット暗号化を指定します。
aes256-sha1	Secure Hash Algorithm 1 を使用する Triple AES 256 ビット暗号化を指定します。
possibly others	暗号化アルゴリズムが、将来のリリースで追加される可能性があることを示します。

デフォルト

デフォルトでは、すべてのアルゴリズムが次の順序で使用可能になっています。

[*3des-sha1***] [***des-sha1***] [***rc4-md5***] [***possibly others***]**

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

ASDM のライセンス タブでは、設定する値ではなく、ライセンスがサポートする暗号化の最大レベルが反映されます。

例

次の例は、3des-sha1 暗号化アルゴリズムと des-sha1 暗号化アルゴリズムを使用するようにセキュリティ アプライアンスを設定する方法を示しています。

```
hostname(config)# ssl encryption 3des-sha1 des-sha1
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作するときに使用する、SSL/TLS プロトコルのバージョンを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl server-version

セキュリティ アプライアンスがサーバとして動作するときに使用する SSL/TLS プロトコルのバージョンを指定するには、グローバル コンフィギュレーション モードで **ssl server-version** コマンドを使用します。デフォルトの any に戻すには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、セキュリティ アプライアンスが受け入れる SSL/TLS のバージョンを限定できます。

ssl server-version [*any* | *sslv3* | *tlsv1* | *sslv3-only* | *tlsv1-only*]

no ssl server-version

シンタックスの説明

any	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、SSL バージョン 3 または TLS バージョン 1 のいずれかをネゴシエートします。
sslv3	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、SSL バージョン 3 をネゴシエートします。
sslv3-only	セキュリティ アプライアンスは、SSL バージョン 3 クライアントの hello のみを受け入れ、SSL バージョン 3 のみを使用します。
tlsv1	セキュリティ アプライアンスは、SSL バージョン 2 クライアントの hello を受け入れ、TLS バージョン 1 をネゴシエートします。
tlsv1-only	セキュリティ アプライアンスは、TLSv1 クライアントの hello のみを受け入れ、TLS バージョン 1 のみを使用します。

デフォルト

デフォルト値は、**any** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

TCP ポート転送は、WebVPN ユーザが一部の SSL バージョンを使用して接続している場合には機能しません。次に説明を示します。

Negotiate SSLv3	Java がダウンロードされる
Negotiate SSLv3/TLSv1	Java がダウンロードされる
Negotiate TLSv1	Java がダウンロードされない
TLSv1Only	Java がダウンロードされない
SSLv3Only	Java がダウンロードされない

電子メールプロキシを設定する場合は、SSL バージョンを tlsv1-only に設定しないでください。Outlook と Outlook Express は、TLS をサポートしていません。

例

次の例は、SSL サーバとして動作するときに、TLSv1 だけを使用して通信するようにセキュリティ アプライアンスを設定する方法を示しています。

```
hostname(config)# ssl server-version tlsv1-only
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
show running-config ssl	現在設定されている ssl コマンドのセットを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl trust-point	インターフェイスの SSL 証明書を表す証明書トラストポイントを指定します。

ssl trust-point

インターフェイスの SSL 証明書を表す証明書トラストポイントを指定するには、グローバル コンフィギュレーション モードで **ssl trust-point** コマンドを *interface* 引数を指定して使用します。インターフェイスを指定しない場合は、トラストポイントが設定されていないすべてのインターフェイスに使用される、フォールバック トラストポイントが作成されます。インターフェイスの指定がない SSL トラストポイントをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。インターフェイスの指定がないエントリを削除するには、このコマンドの **no ssl trust-point {***trustpoint [interface]***}** 形式を使用します。

ssl trust-point {*trustpoint [interface]***}**

no ssl trust-point

シンタックスの説明

interface	トラストポイントを適用するインターフェイス名。このインターフェイス名は、**nameif** コマンドで指定したものです。
trustpoint	**crypto ca trustpoint** {*name*} コマンドで設定した、CA トラストポイントの *name*。

デフォルト

トラストポイントの関連付けはありません。セキュリティ アプライアンスは、デフォルトの自己生成 RSA キー ペア証明書を使用します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを使用する場合は、次の注意事項に従ってください。

- *trustpoint* の値は、**crypto ca trustpoint {*name*}** コマンドで設定した CA トラストポイントの名前にする必要があります。
- *interface* の値は、事前設定済みのインターフェイスの *nameif* 名にする必要があります。
- トラストポイントを削除すると、そのトラストポイントを参照している **ssl trust-point** エントリもすべて削除されます。
- **ssl trustpoint** エントリは、インターフェイスごとに 1 つずつ、およびインターフェイスの指定がないもの 1 つを保持できます。
- 同じトラストポイントを複数のエントリで再利用できます。

次の例は、このコマンドの **no** 形式を使用する方法を示しています。

このコンフィギュレーションには、次の SSL トラストポイントが含まれています。

```
ssl trust-point tp1
ssl trust-point tp2 outside
```

次のコマンドを発行します。

```
no ssl trust-point
```

show run ssl を実行すると、次のように表示されます。

```
ssl trust-point tp2 outside
```

例

次の例は、内部インターフェイス用の FirstTrust という SSL トラストポイント、および関連するインターフェイスを持たない DefaultTrust というトラストポイントを設定する方法を示しています。

```
hostname(config)# ssl trust-point FirstTrust inside
hostname(config)# ssl trust-point DefaultTrust
```

次の例は、このコマンドの **no** 形式を使用して、関連するインターフェイスを持たないトラストポイントを削除する方法を示しています。

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
```

次の例は、インターフェイスが関連付けられているトラストポイントを削除する方法を示しています。

```
hostname(config)# show running-configuration ssl
ssl trust-point FirstTrust inside
ssl trust-point DefaultTrust
hostname(config)# no ssl trust-point FirstTrust inside
hostname(config)# show running-configuration ssl
ssl trust-point DefaultTrust
```

関連コマンド

コマンド	説明
clear config ssl	すべての SSL コマンドをコンフィギュレーションから削除して、デフォルト値に戻します。
show running-config ssl	現在設定されている一連の SSL コマンドを表示します。
ssl client-version	セキュリティ アプライアンスがクライアントとして動作する場合に使用する SSL プロトコルおよび TLS プロトコルのバージョンを指定します。
ssl encryption	SSL/TLS プロトコルで使用する暗号化アルゴリズムを指定します。
ssl server-version	セキュリティ アプライアンスがサーバとして動作するときに使用する、SSL/TLS プロトコルのバージョンを指定します。

sso-server

セキュリティ アプライアンスのユーザ認証のためにシングル サインオン サーバを作成するには、webvpn コンフィギュレーション モードで **sso-server** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

SSO サーバを削除するには、このコマンドの **no** 形式を使用します。

sso-server *name* **type** *siteminder*

no sso-server *name* **type** *siteminder*

（注） SSO 認証にはこのコマンドが必要です。

シンタックスの説明

name	SSO サーバの名前を指定します。文字数は最小 4 文字から最大 31 文字までです。
siteminder	セキュリティ アプライアンスは CA SiteMinder と互換性があるため、使用できる引数は *siteminder* だけです。
type	SSO サーバのタイプを指定します。使用できるタイプは SiteMinder だけです。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。**sso-server** コマンドを使用して SSO サーバを作成できます。SSO サーバを作成したら、認証 URL（**web-agent-url** コマンドを参照）、およびサーバとのコミュニケーションを保護するための秘密鍵（**policy-server-secret** コマンドを参照）を任意の順序で設定する必要があります。

認証では、セキュリティ アプライアンスは SSO サーバへの WebVPN ユーザのプロキシとして動作します。現在、セキュリティ アプライアンスは、Computer Associates の eTrust SiteMinder SSO サーバ（以前の Netegrity SiteMinder）をサポートしています。したがって、タイプのオプションに使用できる引数は *siteminder* です。

例

webvpn コンフィギュレーション モードで入力した次の例では、「example」という名前の SSO サーバを作成しています。

```
hostname(config)# webvpn
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
request-timeout	失敗した SSO 認証試行がタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
test sso-server	テスト認証要求で SSO サーバをテストします。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

sso-server value（グループ ポリシー webvpn コンフィギュレーション）

グループ ポリシーに SSO サーバを割り当てるには、グループ ポリシーの webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

割り当てを削除してデフォルト ポリシーを使用するには、このコマンドの **no** 形式を使用します。

デフォルト ポリシーを継承しないようにするには、**sso-server none** コマンドを使用します。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

シンタックスの説明

name	グループ ポリシーに割り当てられる SSO サーバの名前を指定します。

デフォルト

グループに割り当てられたデフォルト ポリシーは DfltGrpPolicy です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループの WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。グループ ポリシーの webvpn モードで **sso-server value** コマンドを入力すると、SSO サーバをグループ ポリシーに割り当てることができます。

（注） 同じコマンド（**sso-server value**）をユーザ名の webvpn コンフィギュレーション モードで入力すると、SSO サーバをユーザ ポリシーに割り当てることができます。

例

次の例は、コマンドによって my-sso-grp-pol という名前のグループ ポリシーを作成し、そのグループ ポリシーを example という名前の SSO サーバに割り当てます。

```
hostname(config)# group-policy my-sso-grp-pol internal
hostname(config)# group-policy my-sso-grp-pol attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# sso-server value example
hostname(config-group-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
sso-server value（ユーザ名 **webvpn** コンフィギュレーション）	SSO サーバをユーザ ポリシーに割り当てます。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

sso-server value（ユーザ名 webvpn コンフィギュレーション）

ユーザ ポリシーに SSO サーバを割り当てるには、ユーザ名 webvpn コンフィギュレーション モードで **sso-server value** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

ユーザへの SSO サーバ割り当てを削除するには、このコマンドの **no** 形式を使用します。

ユーザ ポリシーがグループ ポリシーから不要な SSO サーバ割り当てを継承した場合は、**sso-server none** コマンドを使用して割り当てを削除します。

sso-server {**value** *name* | **none**}

[**no**] **sso-server value** *name*

シンタックスの説明

name	ユーザ ポリシーに割り当てられる SSO サーバの名前を指定します。

デフォルト

デフォルトでは、ユーザ ポリシーはグループ ポリシーの SSO サーバ割り当てを使用します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名の WebVPN コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。**sso-server value** コマンドを使用すると、SSO サーバをユーザ ポリシーに割り当てることができます。

（注）　同じコマンド（**sso-server value**）をグループの webvpn コンフィギュレーション モードで入力すると、SSO サーバをグループ ポリシーに割り当てることができます。

例

次のコマンドの例では、my-sso-server という名前の SSO サーバを、Anyuser というユーザ名の WebVPN ユーザのユーザ ポリシーに割り当てています。

```
hostname(config)# username Anyuser attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# sso-server value my-sso-server
hostname(config-username-webvpn)#
```

関連コマンド

コマンド	説明
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
sso-server value（グループ ポリシー **webvpn** コンフィギュレーション）	SSO サーバをグループ ポリシーに割り当てます。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

start-url

オプションの事前ログイン クッキーを取得する URL を入力するには、AAA サーバ ホスト コンフィギュレーション モードで **start-url** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

start-url *string*

（注） HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

string	SSO サーバの URL です。URL の最大長は 1024 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、認証 Web サーバにシングル サインオン認証要求を送信するために HTTP POST 要求を使用できます。認証 Web サーバは、Set-Cookie ヘッダーをログイン ページのコンテンツと共に送信することにより、事前ログイン シーケンスを実行できます。ブラウザで認証 Web サーバのログイン ページに直接接続すると、この実行を検出できます。ログイン ページがロードされるときに Web サーバがクッキーを設定し、そのクッキーが次のログイン セッションに関連している場合は、クッキーが取得される URL に入るために **start-url** コマンドを使用する必要があります。実際のログイン シーケンスは、事前ログイン クッキー シーケンスの後で、認証 Web サーバへのフォーム提出により開始されます。

（注） **start-url** コマンドは、事前ログインのクッキー交換が存在する場合にだけ必要です。

例

AAA サーバ ホスト コンフィギュレーション モードで入力された次の例では、https://example.com/east/Area.do?Page-Grp1 の事前ログイン クッキーを取得するための URL を指定しています。

```
hostname(config)# aaa-server testgrp1 (inside) host example.com
hostname(config-aaa-server-host)# start-url https://example.com/east/Area.do?Page=Grp1
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名とパスワードを受信する Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求のパラメータの名前を指定します。
user-parameter	SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

state-checking

H.323 の状態チェックを実行するには、パラメータ コンフィギュレーション モードで **state-checking** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

state-checking [h225 | ras]

no state-checking [h225 | ras]

シンタックスの説明

h225	H.225 の状態チェックを実行します。
ras	RAS の状態チェックを実行します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例は、H.323 コールで RAS の状態チェックを実行する方法を示しています。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# state-checking ras
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

static

実際の IP アドレスをマッピング IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換規則を設定するには、グローバル コンフィギュレーション モードで **static** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

スタティック NAT の場合：

static (*real_ifc*,*mapped_ifc***)** *mapped_ip* {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name* | **interface**} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

no static (*real_ifc*,*mapped_ifc***)** *mapped_ip* {*real_ip* [**netmask** *mask*] | **access-list** *access_list_name* | **interface**} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

スタティック PAT の場合：

static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} *mapped_ip mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name* | | **interface**} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

no static (*real_ifc*,*mapped_ifc*) {**tcp** | **udp**} *mapped_ip mapped_port* {*real_ip real_port* [**netmask** *mask*] | **access-list** *access_list_name* | **interface**} [**dns**] [[**tcp**] *max_conns* [*emb_lim*]] [**udp** *udp_max_conns*] [**norandomseq [nailed]**]

シンタックスの説明

access-list *access_list_name*	実際のアドレスと宛先アドレス（またはポート）を指定して、NAT 用の実際のアドレスを指定できます。この機能は、ポリシー NAT と呼ばれます。 アクセス リストで使用されるサブネット マスクは、*mapped_ip* でも使用されます。 アクセス リストには、**permit** 文だけを含めることができます。**eq** 演算子を使用して、実際のポートと宛先ポートをアクセス リスト内で指定することもできます。ポリシー NAT の場合、**inactive** キーワードと **time-range** キーワードは考慮されません。ポリシー NAT のコンフィギュレーションでは、すべての ACE はアクティブであるものと見なされます。
dns	（オプション）DNS 応答に含まれていて、このスタティック エントリと一致する A レコード（アドレス レコード）を書き換えます。マッピングされているインターフェイスから実際のインターフェイスに移動する DNS 応答では、A レコードが、マッピングされた値から実際の値に書き直されます。逆に、実際のインターフェイスからマッピングされているインターフェイスに移動する DNS 応答では、A レコードが、実際の値からマッピングされた値に書き直されます。 **（注）** この機能をサポートするには、DNS 検査をイネーブルにする必要があります。
emb_lim	（オプション）ホストごとの初期接続の最大数を指定します。デフォルトは 0 で、初期接続に制限がないことを意味します。 初期接続の数を制限することで、DoS 攻撃（サービス拒絶攻撃）から保護されます。セキュリティ アプライアンスでは、初期接続の制限を利用して TCP 代行受信を発生させます。代行受信によって、TCP SYN パケットを使用してインターフェイスをフラッディングする DoS 攻撃から内部システムを保護します。初期接続とは、送信元と宛先の間で必要になるハンドシェイクを完了していない接続要求のことです。

interface	インターフェイスの IP アドレスを、マッピング アドレスとして使用します。このキーワードを使用するのは、インターフェイス アドレスを使用しようとする場合に、アドレスが DHCP を使用して動的に割り当てられているときです。 **（注）** インターフェイスの IP アドレスをスタティック PAT エントリに含める場合は、実際の IP アドレスを指定するのではなく、interface キーワードを使用する必要があります。
mapped_ifc	マッピング IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
mapped_ip	実際のアドレスの変換後のアドレスを指定します。
mapped_port	マッピング TCP ポートまたは UDP ポートを指定します。ポートは、リテラル名または番号（0 ～ 65535）のどちらでも指定できます。 有効なポート番号は、次の Web サイトで確認できます。 http://www.iana.org/assignments/port-numbers
nailed	（オプション）非対称ルーティング トラフィックの TCP セッションを許容します。このオプションを指定すると、着信トラフィックは、対応する発信接続の状態が確立されていなくてもセキュリティ アプライアンスを通過することができます。**failover timeout** コマンドと共に使用します。**failover timeout** コマンドは、システムがブートしたときまたはアクティブになったときを起点として、ネイリングされたセッションが受け入れられる期間を指定するものです。設定しない場合は、接続を再確立できません。 **（注）** **static** コマンドに ***nailed*** オプションを付加すると、当該の接続については TCP の状態追跡とシーケンス確認が省略されます。非対称ルーティングのサポートを設定する場合は、**asr-group** コマンドを使用する方が **static** コマンドに ***nailed*** オプションを付加して使用するよりもセキュリティ上安全であり、非対称ルーティングのサポートの設定にはこの方法をお勧めします。
netmask *mask*	実際のアドレスとマッピング アドレスのサブネット マスクを指定します。単一ホストの場合は、255.255.255.255 を使用します。マスクを入力しない場合は、IP アドレス クラスのデフォルト マスクが使用されます。ただし、例外が 1 つあります。マスク後のホストビットが 0 でない場合は、ホスト マスクの 255.255.255.255 が使用されます。*real_ip* の代わりに **access-list** キーワードを使用すると、アクセス リストで使用されるサブネット マスクが *mapped_ip* にも使用されます。

norandomseq	（オプション）TCP ISN のランダム化保護をディセーブルにします。TCP シーケンスのランダム化をディセーブルにするのは、別のインライン ファイアウォールもシーケンス番号をランダム化していて、結果としてデータ順序が変わる場合だけにします。各 TCP 接続には、2 つの ISN があります。1 つはクライアントが生成し、1 つはサーバが生成します。セキュリティ アプライアンスは、ホストとサーバが生成する ISN をランダム化します。少なくとも 1 つの ISN をランダムに生成して、攻撃者が次の ISN を予想してセッションを乗っ取ることができないようにする必要があります。 **norandomseq** キーワードは外部 NAT に適用されません。ファイアウォールは、セキュリティの高いインターフェイスのホスト / サーバが生成する ISN だけをランダム化します。外部 NAT に対して **norandomseq** を設定しても、**norandomseq** キーワードは無視されます。
real_ifc	実際の IP アドレス ネットワークに接続されているインターフェイスの名前を指定します。
real_ip	変換の対象となる実際のアドレスを指定します。
real_port	実際の TCP ポートまたは UDP ポートを指定します。ポートは、リテラル名または番号（0 ～ 65535）のどちらでも指定できます。 有効なポート番号は、次の Web サイトで確認できます。 http://www.iana.org/assignments/port-numbers
tcp	スタティック PAT の場合に、プロトコルを TCP として指定します。
tcp *max_conns*	サブネット全体に関して、同時 TCP 接続の最大数を指定します。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。
udp	スタティック PAT の場合に、プロトコルを UDP として指定します。
udp *udp_max_conns*	（オプション）サブネット全体に関して、同時 UDP 接続の最大数を指定します。デフォルトは 0 です。接続数の制限がないことを意味します（アイドル接続は、**timeout conn** コマンドで指定したアイドル タイムアウトの経過後に閉じられます）。

デフォルト

tcp_max_conns、*emb_limit*、および *udp_max_conns* のデフォルト値は 0（無制限）です。この値は、最大使用可能値です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	**ルーテッド**	**透過**	**シングル**	**コンテキスト**	**システム**
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

スタティック NAT では、実際のアドレス（複数可）からマッピング アドレス（複数可）への固定的な変換を作成します。ダイナミック NAT およびダイナミック PAT の場合、後続の変換では、各ホストはそれぞれ別のアドレスまたはポートを使用します。スタティック NAT では、マッピング アドレスは連続する各接続で同じであり、恒久的な変換規則が存在します。このため、スタティック NAT を利用する場合は、宛先ネットワーク上のホストが変換後のホストに向かうトラフィックを開始できます（この処理を許可するアクセス リストが存在する場合）。

ダイナミック NAT と、スタティック NAT のアドレス範囲との主な違いは、スタティック NAT を利用する場合、変換後のホストに向かう接続をリモート ホストが開始できることです（この処理を許可するアクセス リストが存在する場合）。ダイナミック NAT の場合はできません。また、スタティック NAT では、実際のアドレスと同じ数のマッピング アドレスが必要になります。

スタティック PAT はスタティック NAT と同じですが、実際のアドレスおよびマッピング アドレスに対して、プロトコル（TCP または UDP）とポートを指定できる点が異なります。

この機能を使用すると、同じマッピング アドレスを複数のさまざまな static 文に対して指定できます。ただし、それぞれの文でポートが異なっている必要があります（複数のスタティック NAT 文に対して同じマッピング アドレスを使用することはできません）。

同じ実際のアドレスまたはマッピング アドレスを、複数の **static** コマンド内で同じ 2 つのインターフェイスに関して使用することはできません。同じマッピング インターフェイスに対して **global** コマンドでも定義されているマッピング アドレスは、**static** コマンドの中では使用しないでください。

セカンダリ チャネルのアプリケーション検査を必要とするアプリケーション（FTP、VoIP など）に対してポリシー NAT のポートを指定すると、セキュリティ アプライアンスは自動的にセカンダリ ポートを変換します。

NAT は、従来の意味では、透過ファイアウォール モードで使用できません。透過ファイアウォール モードでは、***static*** コマンドを使用することによって、最大接続数、最大初期接続数、および TCP シーケンスのランダム化を設定できます。この場合、実際の IP アドレスとマッピング IP アドレスは両方とも同じです。

別の方法として、**set connection** コマンドを使用して、最大接続数、最大初期接続数、および TCP シーケンス ランダム化を設定できます。同じトラフィックに対して両方の方法でこれらの設定値を設定した場合、セキュリティ アプライアンスは小さい方の制限値を使用します。TCP シーケンスのランダム化がいずれかの方法でディセーブルにされている場合、セキュリティ アプライアンスは TCP シーケンスのランダム化をディセーブルにします。

変換のためのネットワークを指定すると（10.1.1.0 255.255.255.0 など）、セキュリティ アプライアンスは .0 と .255 のアドレスを変換します。これらのアドレスへのアクセスを禁止する場合は、アクセスを拒否するようにアクセス リストを設定する必要があります。

static コマンド文を変更または削除した後は、**clear xlate** コマンドを使用して変換を消去してください。

例

スタティック NAT の例

次のポリシー スタティック NAT の例は、宛先アドレスに応じて 2 つのマッピング アドレスに変換される 1 つの実際のアドレスを示しています。

```
hostname(config)# access-list NET1 permit ip host 10.1.2.27 209.165.201.0
255.255.255.224
hostname(config)# access-list NET2 permit ip host 10.1.2.27 209.165.200.224
255.255.255.224
hostname(config)# static (inside,outside) 209.165.202.129 access-list NET1
hostname(config)# static (inside,outside) 209.165.202.130 access-list NET2
```

次のコマンドでは、内部 IP アドレス（10.1.1.3）を外部 IP アドレス（209.165.201.12）にマッピングしています。

```
hostname(config)# static (inside,outside) 209.165.201.12 10.1.1.3 netmask
255.255.255.255
```

次のコマンドでは、外部 IP アドレス（209.165.201.15）を内部 IP アドレス（10.1.1.6）にマッピングしています。

```
hostname(config)# static (outside,inside) 10.1.1.6 209.165.201.15 netmask
255.255.255.255
```

次のコマンドでは、サブネット全体をスタティックにマッピングしています。

```
hostname(config)# static (inside,dmz) 10.1.1.0 10.1.2.0 netmask 255.255.255.0
```

次の例は、限定された数のユーザが、Intel Internet Phone、CU-SeeMe、CU-SeeMe Pro、MeetingPoint、または Microsoft NetMeeting を使用して、H.323 経由でコール インできるようにする方法を示しています。**static** コマンドでは、アドレス 209.165.201.0 ～ 209.165.201.30 がローカル アドレス 10.1.1.1 ～ 10.1.1.30 にマッピングされます（209.165.201.1 は 10.1.1.1 にマッピングされ、209.165.201.10 は 10.1.1.10 にマッピングされ、他も同様にマッピングされます）。

```
hostname(config)# static (inside, outside) 209.165.201.0 10.1.1.0 netmask
255.255.255.224
hostname(config)# access-list acl_out permit tcp any 209.165.201.0 255.255.255.224 eq
h323
hostname(config)# access-group acl_out in interface outside
```

次の例は、Mail Guard をディセーブルにするためのコマンドを示しています。

```
hostname(config)# static (dmz1,outside) 209.165.201.1 10.1.1.1 netmask 255.255.255.255
hostname(config)# access-list acl_out permit tcp any host 209.165.201.1 eq smtp
hostname(config)# access-group acl_out in interface outside
hostname(config)# no fixup protocol smtp 25
```

この例では、**static** コマンドでグローバル アドレスをセットアップして、外部のホストが dmz1 インターフェイス上の 10.1.1.1 メール サーバ ホストにアクセスすることを許可します。DNS 用の MX レコードが 209.165.201.1 アドレスを指すように設定する必要があり、これによってメールはこのアドレスに送信されます。**access-list** コマンドによって、外側ユーザが SMTP ポート（25）を経由して、グローバル アドレスにアクセスできるようにしています。**no fixup protocol** コマンドにより、Mail Guard がディセーブルになります。

スタティック PAT の例

たとえば、10.1.3.0 ネットワーク上のホストから開始されてセキュリティ アプライアンスの外部インターフェイス（10.1.2.14）に向かう Telnet トラフィックは、次のコマンドを入力することで内部のホスト（10.1.1.15）にリダイレクトできます。

```
hostname(config)# access-list TELNET permit tcp host 10.1.1.15 eq telnet 10.1.3.0
255.255.255.0 eq telnet
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet access-list TELNET
```

10.1.3.0 ネットワーク上のホストから開始されてセキュリティ アプライアンスの外部インターフェイス（10.1.2.14）に向かう HTTP トラフィックは、次のコマンドを入力することで内部のホスト（10.1.1.15）にリダイレクトできます。

```
hostname(config)# access-list HTTP permit tcp host 10.1.1.15 eq http 10.1.3.0
255.255.255.0 eq http
hostname(config)# static (inside,outside) tcp 10.1.2.14 http access-list HTTP
```

セキュリティ アプライアンスの外部インターフェイス（10.1.2.14）からの Telnet トラフィックを内部ホスト 10.1.1.15 にリダイレクトするには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
```

上の実際の Telnet サーバが接続を開始することを許可するには、変換を追加する必要があります。たとえば、他のすべてのタイプのトラフィックを変換するには、次のコマンドを入力します。元のままの **static** コマンドは、このサーバに向かう Telnet に関する変換を定義しています。それに対して、**nat** コマンドと **global** コマンドでは、このサーバからの発信接続に関する PAT を定義しています。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
```

すべての内部トラフィックに独自の変換を定義していて、内部ホストが Telnet サーバとは別のマッピング アドレスを使用している場合でも、Telnet サーバから開始されるトラフィックについては、サーバに向かう Telnet トラフィックを許可する **static** 文と同じマッピング アドレスを使用するように設定することができます。Telnet サーバにだけ適用する、より限定的な **nat** コマンドを作成する必要があります。**nat** 文は、最もよく一致しているものが読み取られます。このため、限定的な **nat** コマンドは汎用の文よりも先に一致します。次の例は、Telnet に関する **static** 文、Telnet サーバから開始されるトラフィックに関する限定的な **nat** 文、および別のマッピング アドレスを使用するその他の内部ホストに関する文を示しています。

```
hostname(config)# static (inside,outside) tcp 10.1.2.14 telnet 10.1.1.15 telnet
netmask 255.255.255.255
hostname(config)# nat (inside) 1 10.1.1.15 255.255.255.255
hostname(config)# global (outside) 1 10.1.2.14
hostname(config)# nat (inside) 2 10.1.1.0 255.255.255.0
hostname(config)# global (outside) 2 10.1.2.78
```

既知のポート（80）を別のポート（8080）に変換するには、次のコマンドを入力します。

```
hostname(config)# static (inside,outside) tcp 10.1.2.45 80 10.1.1.16 8080 netmask
255.255.255.255
```

関連コマンド

コマンド	説明
clear configure static	コンフィギュレーションから **static** コマンドを削除します。
clear xlate	すべての変換を消去します。
nat	ダイナミック NAT を設定します。
show running-config static	コンフィギュレーションに含まれているすべての **static** コマンドを表示します。
timeout conn	接続のタイムアウトを設定します。

strict-header-validation

RFC 3261 に従って、SIP メッセージのヘッダー フィールドの厳密な検証をイネーブルにするには、パラメータ コンフィギュレーション モードで **strict-header-validation** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

no strict-header-validation action {**drop** | **drop-connection** | **reset** | **log**} [**log**}

シンタックスの説明

drop	違反が発生した場合、パケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
log	違反が発生した場合、独自または追加のログを記録することを指定します。このアクションは、任意のアクションに関連付けることができます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、SIP 検査ポリシー マップで SIP ヘッダー フィールドの厳密な検証をイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# strict-header-validation action log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

strict-http

HTTP に準拠しないトラフィックの転送を許可するには、HTTP マップ コンフィギュレーション モードで **strict-http** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。この機能の動作をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

strict-http action {**allow** | **reset** | **drop**} [**log**]

no **strict-http action** {**allow** | **reset** | **drop**} [**log**]

シンタックスの説明

action	メッセージがこのコマンド検査に合格しなかったときに実行されるアクション。
allow	メッセージを許可します。
drop	接続を終了します。
log	（オプション）syslog を生成します。
reset	クライアントとサーバに TCP リセット メッセージを送信して、接続を終了します。

デフォルト

このコマンドは、デフォルトではイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

厳密な HTTP 検査をディセーブルにすることはできませんが、**strict-http action allow** コマンドを使用すると、HTTP に準拠しないトラフィックの転送をセキュリティ アプライアンスで許可することができます。このコマンドは、デフォルトの動作（HTTP に準拠しないトラフィックの転送を拒否）を上書きします。

例

次の例では、HTTP に準拠しないトラフィックの転送を許可しています。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# strict-http allow
hostname(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

strip-group

このコマンドが適用されるのは、user@realm の形式で受信したユーザ名のみです。レルムは、@ デリミタを使用してユーザ名に付加される管理ドメインです（たとえば、juser@abc）。

グループ除去処理をイネーブルまたはディセーブルにするには、トンネル グループ一般アトリビュート モードで **strip-group** コマンドを使用します。セキュリティ アプライアンスは、VPN クライアントが提示するユーザ名からグループ名を取得して、IPSec 接続用のトンネル グループを選択します。グループ除去処理をイネーブルにすると、セキュリティ アプライアンスは、ユーザ名のユーザ部分だけを認可と認証用に送信します。これ以外の場合（ディセーブルにした場合）、セキュリティ アプライアンスはレルムを含めてユーザ名全体を送信します。

グループ除去処理をディセーブルにするには、このコマンドの ***no*** 形式を使用します。

strip-group

no strip-group

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトでは、このコマンドの設定はディセーブルになっています。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン　このアトリビュートは、IPSec リモートアクセス トンネルタイプだけに適用できます。

例

次の例では、IPSec リモートアクセス タイプ用に「remotegrp」という名前のリモートアクセス トンネル グループを設定し、次に一般コンフィギュレーション モードに入って、「remotegrp」という名前のトンネル グループをデフォルト グループ ポリシーとして設定し、次にこのトンネル グループについてグループ除去をイネーブルにしています。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-group
hostname(config-tunnel-general)
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
group-delimiter	グループ名の解析をイネーブルにし、トンネルのネゴシエーション中に受信したユーザ名からグループ名を解析するときに使用するデリミタを指定します。
show running-config tunnel group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般アトリビュートを指定します。

strip-realm

レルム除去処理をイネーブルまたはディセーブルにするには、トンネル グループ一般アトリビュート コンフィギュレーション モードで **strip-realm** コマンドを使用します。レルム除去処理は、ユーザ名を認証サーバまたは認可サーバに送信するときに、ユーザ名からレルムを削除するものです。レルムは、@　デリミタを使用してユーザ名に付加される管理ドメインです（たとえば、username@realm）。このコマンドをイネーブルにすると、セキュリティ アプライアンスは、ユーザ名のユーザ部分だけを認可と認証用に送信します。ディセーブルにした場合には、セキュリティ アプライアンスはユーザ名全体を送信します。

レルム除去処理をディセーブルにするには、このコマンドの ***no*** 形式を使用します。

strip-realm

no strip-realm

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、このコマンドの設定はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ一般アトリビュート　コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、IPSec リモートアクセス トンネルタイプだけに適用できます。

例

次の例では、IPSec リモートアクセス タイプ用に「remotegrp」という名前のリモートアクセス トンネル グループを設定し、次に一般コンフィギュレーション モードに入って、「remotegrp」という名前のトンネル グループをデフォルト グループ ポリシーとして設定し、次にこのトンネル グループについてレルム除去をイネーブルにしています。

```
hostname(config)# tunnel-group remotegrp type IPSec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)# default-group-policy remotegrp
hostname(config-tunnel-general)# strip-realm
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されたすべてのトンネル グループまたは指定されたトンネル グループを消去します。
show running-config tunnel-group	現在のトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般アトリビュートを指定します。

subject-name（暗号 CA 証明書マップ）

規則エントリを IPSec ピア証明書のサブジェクト DN に適用することを指定するには、CA 証明書マップ コンフィギュレーション モードで **subject-name** コマンドを使用します。サブジェクト名を削除するには、このコマンドの **no** 形式を使用します。

subject-name [**attr** *tag*] **eq | ne |co | nc** *string*

no subject-name [**attr** *tag*] **eq | ne |co | nc** *string*

シンタックスの説明

attr tag	証明書 DN にある、指定したアトリビュート値のみを規則エントリ文字列と比較することを指定します。タグの値を次に示します。 DNQ = DN 修飾子 GENQ = 世代修飾子 I = イニシャル GN = 名 N = 名前 SN = 姓 IP = IP アドレス SER = シリアル番号 UNAME = 非構造化名 EA = 電子メール アドレス T = 役職 O = 組織名 L = 地名 SP = 州または都道府県 C = 国または地域 OU = 組織ユニット CN = 通常名
co	規則エントリ文字列が、DN 文字列または指定されているアトリビュートのサブストリングになる必要があることを指定します。
eq	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致する必要があることを指定します。
nc	規則エントリ文字列が、DN 文字列または指定されているアトリビュートのサブストリングにならない必要があることを指定します。
ne	DN 文字列または指定されているアトリビュートが、規則の文字列全体と一致しない必要があることを指定します。
string	一致するかどうかの確認対象となる値を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA 証明書マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、証明書マップ 1 の CA 証明書マップ モードに入って、証明書サブジェクト名の Organization アトリビュートが Central と等しくなる必要があると指定する規則エントリを作成しています。

```
hostname(config)# crypto ca certificate map 1
hostname(ca-certificate-map)# subject-name attr o eq central
hostname(ca-certificate-map)# exit
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードに入ります。
issuer-name	規則エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map	**crypto ca certificate map** コマンドで作成された証明書マップ エントリをトンネル グループに関連付けます。

subject-name（暗号 CA トラストポイント）

指定したサブジェクト DN を登録時に証明書に含めるには、暗号 CA トラストポイント コンフィギュレーション モードで **subject-name** コマンドを使用します。これは、証明書を使用する人物またはシステムです。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

subject-name *X.500_name*

no subject-name

シンタックスの説明

X.500_name	X.500 認定者名（たとえば、cn=crl,ou=certs,o=CAName,c=US）を定義します。最大長は 1,000 文字（実質上の無制限）です。

デフォルト

デフォルトでは、サブジェクト名を含めない設定になっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入って、URL https//:frog.phoobin.com での自動登録をセットアップし、サブジェクト DN OU tiedye.com をトラストポイント central の登録要求に含めています。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url http://frog.phoobin.com/
hostname(ca-trustpoint)# subject-name ou=tiedye.com
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。
enrollment url	CA への登録用の URL を指定します。

summary-address

OSPF の集約アドレスを作成するには、ルータ コンフィギュレーション モードで **summary-address** コマンドを使用します。サマリー アドレスまたは特定のサマリー アドレス オプションを削除するには、このコマンドの **no** 形式を使用します。

summary-address *addr mask* [***not-advertise***] [***tag*** *tag_value*]

no summary-address *addr mask* [***not-advertise***] [***tag*** *tag_value*]

シンタックスの説明

addr	一定範囲のアドレスに指定されたサマリー アドレスの値。
mask	サマリー ルートに使用される IP サブネット マスク。
not-advertise	（オプション）指定されたプレフィックスとマスクのペアに一致するルートを抑止します。
tag *tag_value*	（オプション）各外部ルートに対応付けられた 32 ビットの 10 進値。この値は、OSPF 自体によって使用されることはありません。ASBR 間で情報を交換するために使用されます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効な値は 0 ～ 4294967295 です。

デフォルト

デフォルトは次のとおりです。

- *tag_value* は 0 です。
- 指定されたプレフィックスとマスクのペアに一致するルートは、抑止されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

他のルーティング プロトコルからラーニングしたルートは、要約することができます。このコマンドを OSPF に対して使用すると、OSPF 自律システム境界ルータ（ASBR）は、当該アドレスの対象となる再配布されるすべてのルートの要約として、1 つの外部ルートをアドバタイズします。このコマンドが要約するのは、他のルーティング プロトコルからラーニングした、OSPF に再配布されているルートのみです。OSPF エリア間の経路集約には、**area range** コマンドを使用します。

summary-address コマンドをコンフィギュレーションから削除するには、このコマンドの no 形式を他のオプション キーワードや引数を指定せずに使用します。オプションをコンフィギュレーション内の summary コマンドから削除するには、削除するオプションを付加してこのコマンドの **no** 形式を使用します。詳細については、「例」を参照してください。

例

次の例では、*tag* を 3 に設定して経路集約を設定しています。

```
hostname(config-router)# summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次の例は、デフォルト値に戻す対象オプションを指定して **summary-address** コマンドの **no** 形式を使用する方法を示しています。この例では、前の例で 3 に設定した *tag* の値を **summary-address** コマンドから削除しています。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0 tag 3
hostname(config-router)#
```

次の例では、**summary-address** コマンドをコンフィギュレーションから削除しています。

```
hostname(config-router)# no summary-address 1.1.0.0 255.255.0.0
hostname(config-router)#
```

関連コマンド

コマンド	説明
area range	エリアの境界でルートを統合および要約します。
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf summary-address	各 OSPF ルーティング プロセスのサマリー アドレス設定を表示します。

sunrpc-server

SunRPC サービス テーブル内にエントリを作成するには、グローバル コンフィギュレーション モードで **sunrpc-server** コマンドを使用します。SunRPC サービス テーブルのエントリをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* **[-** *port* **]**
timeout *hh:mm:ss*

no sunrpc-server *ifc_name ip_addr mask* **service** *service_type* **protocol** [**tcp** | **udp**] **port** *port* [**-** *port]*
timeout *hh:mm:ss*

no sunrpc-server active service *service_type* **server** *ip_addr*

シンタックスの説明

ifc_name	サーバのインターフェイス名。
ip_addr	SunRPC サーバの IP アドレス。
mask	ネットワーク マスク。
port *port* [**-** *port*]	SunRPC プロトコルのポート範囲を指定します。
port- *port*	（オプション）SunRPC プロトコルのポート範囲を指定します。
protocol tcp	SunRPC 転送プロトコルを指定します。
protocol udp	SunRPC 転送プロトコルを指定します。
service	サービスを指定します。
service_type	**sunrpcinfo** コマンドで指定した SunRPC サービス プログラム番号を設定します。
timeout *hh:mm:ss*	SunRPC サービス トラフィックへのアクセスが終了するまでのタイムアウト アイドル時間を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

SunRPC サービス テーブルは、タイムアウトで指定した期間中に、SunRPC トラフィックが確立済み SunRPC セッションに基づいてセキュリティ アプライアンスを通過することを許可するために使用します。

例

次の例は、SunRPC サービス テーブルを作成する方法を示しています。

```
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100003 protocol TCP
port 111 timeout 0:11:00
hostname(config)# sunrpc-server outside 10.0.0.1 255.0.0.0 service 100005 protocol TCP
port 111 timeout 0:11:00
```

関連コマンド

コマンド	説明
clear configure sunrpc-server	セキュリティ アプライアンスから Sun リモート プロセッサ コール サービスを消去します。
show running-config sunrpc-server	SunRPC コンフィギュレーションに関する情報を表示します。

support-user-cert-validation

現在のトラストポイントが、リモート ユーザ証明書を発行した CA に認証されている場合に、リモート ユーザ証明書をそのトラストポイントに基づいて検証するには、暗号 CA トラストポイント コンフィギュレーション モードで **support-user-cert-validation** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

support-user-cert-validation

no support-user-cert-validation

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、ユーザ証明書の検証をサポートするように設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
暗号 CA トラストポイント コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、同じ CA に対して 2 つのトラストポイントを保持できます。このため、同じ CA から 2 つの異なる ID 証明書が発行されることがあります。あるトラストポイントが、この機能をイネーブルにしている別のトラストポイントにすでに関連付けられている CA の認証を受ける場合、このオプションは自動的にディセーブルになります。したがって、パス検証パラメータの選択であいまいさが生じることはありません。あるトラストポイントが、この機能をイネーブルにしている別のトラストポイントにすでに関連付けられている CA の認証を受けた場合は、ユーザが当該トラストポイント上でこの機能をアクティブにしようとしても、その操作は許可されません。2 つのトラストポイント上でこの設定をイネーブルにして、同じ CA の認証を受けることはできません。

例

次の例では、トラストポイント central の暗号 CA トラストポイント コンフィギュレーション モードに入って、トラストポイント central でのユーザ検証の受け入れをイネーブルにしています。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# support-user-cert-validation
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
default enrollment	登録パラメータをデフォルトに戻します。

SVC

特定のグループまたはユーザの SVC をイネーブルにするか、または要求するには、グループ ポリシーまたはユーザ名の webvpn モードで **svc** コマンドを使用します。

コンフィギュレーションから **svc** コマンドを削除するには、このコマンドの **no** 形式を使用します。

svc {**none** | **enable** | **required**}

no svc

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

none	このグループまたはユーザの SVC をディセーブルにします。
enable	このグループまたはユーザの SVC をイネーブルにします。
required	このグループまたはユーザには SVC が必要です。

デフォルト

デフォルトは **none** です。SVC はグループ ポリシーまたはユーザ ポリシーでディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシーの WebVPN	•	—	•	—	—
ユーザ名の WebVPN	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

例

次の例では、ユーザは、SVC を必要とするように既存のグループ ポリシー *sales* を設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc required
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについての情報を表示します。
svc enable	SVC ファイルをリモート コンピュータにダウンロードするためにセキュリティ アプライアンスをイネーブルにします。
svc image	セキュリティ アプライアンスが SVC ファイルをフラッシュ メモリから RAM にロードするように指定し、さらにセキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定します。

svc compression

特定のグループまたはユーザの SVC 接続で、http データの圧縮をイネーブルにするには、グループ ポリシーまたはユーザ名の webvpn モードで **svc compression** コマンドを使用します。

コンフィギュレーションから **svc compression** コマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

svc compression {**deflate** | **none**}

no svc compression {**deflate** | **none**}

シンタックスの説明

deflate	グループまたはユーザに対して圧縮をイネーブルにすることを指定します。
none	グループまたはユーザに対して圧縮をディセーブルにすることを指定します。

デフォルト

デフォルトでは、SVC 圧縮は *deflate*（イネーブル）に設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシーの WebVPN	•	—	•	—	—
ユーザ名の WebVPN	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

SVC 接続では、グローバル コンフィギュレーション モードで設定された **compression** コマンドが、グループ ポリシーまたはユーザ名の webvpn モードで設定された **svc compression** コマンドを上書きします。

例

次の例では、グループ ポリシー sales の SVC 圧縮はディセーブルになっています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc compression none
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続、WebVPN 接続、および IPSec VPN 接続に対して圧縮をイネーブルにします。
show webvpn svc	SVC インストレーションについての情報を表示します。

svc dpd-interval

セキュリティ アプライアンスの DPD をイネーブルにして、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定するには、グループ ポリシー またはユーザ名の webvpn モードで **svc dpd-interval** コマンドを使用します。

svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

no svc dpd-interval {[**gateway** {*seconds* | **none**}] | [**client** {*seconds* | **none**}]}

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

gateway *seconds*	セキュリティ アプライアンスが DPD を実行する間隔を 30 ～ 3,600 秒の範囲で指定します。
gateway none	セキュリティ アプライアンスが実行する DPD をディセーブルにします。
client *seconds*	SVC が DPD を実行する間隔を 30 ～ 3,600 秒の範囲で指定します。
client none	SVC が実行する DPD をディセーブルにします。

デフォルト

デフォルトは none です。SVC およびセキュリティ アプライアンスの DPD はディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN グループ ポリシー	•	—	•	—	—
WebVPN ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次の例では、既存の Sales という名前のグループ ポリシーに対して、セキュリティ アプライアンス（ゲートウェイ）が実行する DPD の間隔を 3,000 秒に設定し、クライアントが実行する DPD の間隔を 1,000 秒に設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc dpd-interval gateway 3000
hostname(config-group-webvpn)# svc dpd-interval client 1000
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc keepalive	リモート コンピュータの SVC が、セキュリティ アプライアンスにキープアライブ メッセージを送信する頻度を指定します。
svc keep-installer	リモート コンピュータへの SVC の永続的なインストールをイネーブルにします。
svc rekey	SVC セッションで SVC がキーの再生成を実行することをイネーブルにします。

svc enable

セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードすることをイネーブルにするには、webvpn モードで **svc enable** コマンドを使用します。

コンフィギュレーションから **svc enable** コマンドを削除するには、このコマンドの **no** 形式を使用します。

svc enable

no svc enable

デフォルト

デフォルトでは、このコマンドはディセーブルになっています。セキュリティ アプライアンスは SVC ファイルをダウンロードしません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

no svc enable コマンドを入力しても、アクティブな SVC セッションは終了しません。

例

次の例では、セキュリティ アプライアンスによる SVC ファイルのダウンロードをイネーブルにしています。

```
(config)# webvpn
(config-webvpn)# svc enable
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについての情報を表示します。
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc image	セキュリティ アプライアンスが SVC ファイルをフラッシュ メモリから RAM にロードするように指定し、さらにセキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定します。

svc image

セキュリティ アプライアンスが SVC ファイルをフラッシュ メモリから RAM にロードするように指定し、さらにセキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定するには、webvpn モードで **svc image** コマンドを使用します。

コンフィギュレーションから **svc image** コマンドを削除するには、このコマンドの **no** 形式を使用します。

svc image *filename order*

no svc image *filename order*

シンタックスの説明

filename	SVC ファイルのファイル名を最大 255 文字で指定します。
order	ファイル間の相対的な位置を示す番号を 1 ～ 65,535 の間で指定します。

デフォルト

デフォルトの順序は 1 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

SVC ファイルに番号を付けると、セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序が確立されます。セキュリティ アプライアンスは、最も小さい番号の SVC ファイルを最初にダウンロードします。したがって、オペレーティング システムで最も一般的に使用されるファイルに最小の番号を割り当てる必要があります。

ファイルは任意の順序で設定できます。たとえば、2 を 1 の前に設定することが可能です。

例

次の例で、**show webvpn svc** コマンドの出力は、windows.pkg ファイルが順序番号 1、windows2.pkg ファイルが順序番号 15 であることを示しています。リモート コンピュータが SVC 接続を確立しようとすると、windows.pkg ファイルが最初にダウンロードされます。ファイルがオペレーティング システムに一致しない場合は、windows2.pkg ファイルがダウンロードされます。

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows.pkg 1
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows2.pkg 15
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

次に、**svc image** コマンドを使用して SVC アーカイブ ファイルの順序を変更し、リモート PC に最初にダウンロードされるファイルを windows2.pkg ファイルとして、2 番目にダウンードされるファイルを windows.pkg としています。

```
hostname(config-webvpn)# svc image windows2.pkg 10
hostname(config-webvpn)# svc image windows.pkg 20
```

show webvpn svc コマンドを再度入力すると、新しい順序でファイルが表示されます。

```
hostname(config-webvpn)# show webvpn svc
1. disk0:/windows2.pkg 10
  CISCO STC win2k+ 1.0.0
  1,0,2,132
  Thu 08/25/2005 21:51:30.43

2. disk0:/windows.pkg 20
  CISCO STC win2k+ 1.0.0
  1,0,0,164
  Thu 02/17/2005 20:09:22.43

2 SSL VPN Client(s) installed
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについての情報を表示します。
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc enable	SVC ファイルをリモート コンピュータにダウンロードするためにセキュリティ アプライアンスをイネーブルにします。

svc keepalive

リモート コンピュータの SVC が、セキュリティ アプライアンスにキープアライブ メッセージを送信する頻度を設定するには、**svc keepalive** コマンドを使用します。

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

svc keepalive {**none** | *seconds*}

no svc keepalive {**none** | *seconds*}

シンタックスの説明

none	SVC のキープアライブ メッセージをディセーブルにします。
seconds	SVC がキープアライブ メッセージを送信することをイネーブルにし、15 ～ 600 秒の範囲でメッセージの間隔を指定します。

デフォルト

デフォルトは none（ディセーブル）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN グループ ポリシー	•	—	•	—	—
WebVPN ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

アイドル状態での接続時間をデバイスが制限している場合でも、プロキシ、ファイアウォール、または NAT デバイスを介した SVC 接続を維持するように、キープアライブ メッセージの頻度（*seconds* で指定された）を調整できます。

頻度を調整することにより、Microsoft Outlook や Microsoft Internet Explorer などのソケット ベースのアプリケーションをユーザがアクティブに実行していないときに、SVC の切断や再接続が発生しないようにします。

例

次の例では、ユーザは、既存の Sales という名前のグループ ポリシーに対して、SVC がキープアライブ メッセージを 300 秒（5 分）の間隔で送信することをイネーブルにするようにセキュリティ アプライアンスを設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc keepalive 300
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc dpd-interval	セキュリティ アプライアンスの Dead Peer Detection（DPD）をイネーブルにし、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定します。
svc keep-installer	リモート コンピュータへの SVC の永続的なインストールをイネーブルにします。
svc rekey	SVC セッションで SVC がキーの再生成を実行することをイネーブルにします。

svc keep-installer

リモート コンピュータへの SVC の永続的なインストレーションをイネーブルにするには、グループ ポリシー またはユーザ名の webvpn モードで **svc keep-installer** を使用します。

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

svc keep-installer {**installed** | **none**}

no svc keep-installer {**installed** | **none**}

シンタックスの説明

installed	リモート コンピュータに SVC が永続的にインストールされることを指定します。
none	アクティブな SVC 接続が終了した後で、リモート コンピュータから SVC をアンインストールするように指定します。

デフォルト

デフォルトでは、SVC の永続的なインストレーションはディセーブルになっています。SVC は SVC セッションの終了時にリモート コンピュータからアンインストールされます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN グループ ポリシー	•	—	•	—	—
WebVPN ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次の例では、ユーザはグループ ポリシーがリモート コンピュータへの SVC のインストールを維持するように設定しています。

```
hostname(config-group-policy)# svc keep-installer installed
hostname(config-group-policy)#
```

関連コマンド

コマンド	説明
show webvpn svc	SVC インストレーションについての情報を表示します。
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc enable	セキュリティ アプライアンスに対して、SVC ファイルをフラッシュ メモリから RAM にダウンロードさせます。
svc image	セキュリティ アプライアンスが SVC ファイルをリモート コンピュータにダウンロードする順序を指定します。

svc rekey

SVC がキーの再生成を SVC セッションで実行することをイネーブルにするには、グループ ポリシーまたはユーザ名の webvpn モードで **svc rekey** コマンドを使用します。

コンフィギュレーションからコマンドを削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

no svc rekey {**method** {**ssl** | **new-tunnel**} | **time** *minutes* | **none**}

シンタックスの説明

method ssl	SSL の再ネゴシエーションが SVC のキー再生成の間に行われることを指定します。
method new-tunnel	SVC が SVC のキー再生成の間に新しいトンネルを確立することを指定します。
time *minutes*	セッションの開始からキー再生成が行われるまでの分数を、4 ～ 10,080（1 週間）の範囲で指定します。
method none	SVC のキー再生成をディセーブルにします。

デフォルト

デフォルトは none（ディセーブル）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN グループ ポリシー	•	—	•	—	—
WebVPN ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キー再生成の方式として SSL を設定することをお勧めします。

例

次の例では、既存の Sales という名前のグループ ポリシーに対して、キーの再生成の間に SSL が SVC と再ネゴシエーションするように設定し、キー再生成がセッションの開始後 30 分で発生するように設定しています。

```
hostname(config)# group-policy sales attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# svc rekey method ssl
hostname(config-group-webvpn)# svc rekey time 30
```

関連コマンド

コマンド	説明
svc	特定のグループまたはユーザに対して SVC をイネーブルまたは必須にします。
svc dpd-interval	セキュリティ アプライアンスの Dead Peer Detection（DPD）をイネーブルにし、SVC またはセキュリティ アプライアンスが DPD を実行する頻度を設定します。
svc keepalive	リモート コンピュータの SVC が、セキュリティ アプライアンスにキープアライブ メッセージを送信する頻度を指定します。
svc keep-installer	リモート コンピュータへの SVC の永続的なインストールをイネーブルにします。

switchport access vlan

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、インターフェイス コンフィギュレーション モードで **switchport access vlan** コマンドを使用してスイッチ ポートを VLAN に割り当てます。

switchport access vlan *number*

no switchport access vlan *number*

シンタックスの説明

vlan *number*	このスイッチ ポートを割り当てる VLAN ID を指定します。VLAN ID は 1 ～ 1001 です。

デフォルト

デフォルトでは、スイッチ ポートはすべて VLAN 1 に割り当てられます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

透過ファイアウォール モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスの場合はアクティブな VLAN を 2 つ、Security Plus ライセンスの場合は 3 つ設定できます。その内の 1 つはフェールオーバー用にする必要があります。

ルーテッド モードでは、ASA 5505 適応型セキュリティ アプライアンスの Base ライセンスの場合、アクティブな VLAN を 3 つまで、Security Plus ライセンスの場合は 20 まで設定できます。

アクティブな VLAN とは、**nameif** コマンドが設定されている VLAN です。

switchport access vlan コマンドを使用して、各 VLAN に 1 つまたは複数の物理インターフェイスを割り当てることができます。デフォルトでは、そのインターフェイスの VLAN モードがアクセス ポートになります（インターフェイスに関連付けられた 1 つの VLAN）。インターフェイス上で複数の VLAN を通過させるトランク ポートを作成する場合は、**switchport mode access trunk** コマンドを使用してモードをトランク モードに変更してから、**switchport trunk allowed vlan** コマンドを使用します。

例

次の例では、5 つの物理インターフェイスを 3 つの VLAN インターフェイスに割り当てます。

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	同じ VLAN 上でスイッチ ポートが他のスイッチ ポートと通信することを禁止して、セキュリティを大幅に強化します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport mode

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルの場合、インターフェイス コンフィギュレーション モードで **switchport mode** コマンドを使用して VLAN モードをアクセス（デフォルト）またはトランクに設定します。

switchport mode {**access** | **trunk**}

no switchport mode {**access** | **trunk**}

シンタックスの説明

access	スイッチ ポートをアクセス モードに設定します。このモードでは、スイッチ ポートで 1 つの VLAN だけのトラフィックを通過させることができます。パケットは、802.1Q VLAN タグなしでスイッチ ポートから出ます。パケットがタグ付きでスイッチ ポートに入ると、パケットはドロップされます。
trunk	スイッチ ポートをトランク モードに設定します。このモードでは、複数の VLAN のトラフィックを通過させることができます。パケットは、802.1Q VLAN タグ付きでスイッチ ポートから出ます。パケットがタグなしでスイッチ ポートに入ると、パケットはドロップされます。

デフォルト

デフォルトのモードは access です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
7.2(2)	今までトランクは 1 つに制限されていましたが、複数のトランク ポートを設定できるようになりました。

使用上のガイドライン

デフォルトでは、スイッチ ポートの VLAN モードはアクセス ポートになります（スイッチ ポートに関連付けられた 1 つの VLAN）。アクセス モードでは、**switchport access vlan** コマンドを使用してスイッチ ポートを VLAN に割り当てます。複数の VLAN が通過するトランク ポートをスイッチ ポート上に作成する場合は、モードをトランク モードに設定してから、**switchport trunk allowed vlan** コマンドを使用して、複数の VLAN をトランクに割り当てます。モードをトランク モードに設定し、**switchport trunk allowed vlan** コマンドを設定していない場合、スイッチ ポートは「line protocol down」状態のままになり、トラフィックの転送には参加できません。トランク モードを使用できるのは、Security Plus ライセンスの場合のみです。

switchport vlan access コマンドは、モードをアクセス モードに設定しない限り有効になりません。**switchport trunk allowed vlan** コマンドは、モードをトランク モードに設定しない限り有効になりません。

例

次の例では、アクセス モードのスイッチ ポート（VLAN 100 を割り当て）、およびトランク モードのスイッチ ポート（VLAN 200 と 300 を割り当て）を設定しています。

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200,300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport protected	同じ VLAN 上でスイッチ ポートが他のスイッチ ポートと通信することを禁止して、セキュリティを大幅に強化します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport protected

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、インターフェイス コンフィギュレーション モードで **switchport protected** コマンドを使用して同じ VLAN 上でスイッチ ポートが他の保護されたスイッチ ポートと通信することを禁止します。あるスイッチ ポートの安全性が確保されていない場合、この機能により VLAN 上の他のスイッチ ポートのセキュリティを向上させることができます。

switchport protected

no switchport protected

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、インターフェイスは保護されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

スイッチ ポート上のデバイスが主に別の VLAN からアクセスされ、VLAN 内アクセスを許可する必要がなく、感染やその他のセキュリティ障害のときに各デバイスを隔離する場合は、スイッチ ポートが相互に通信することを禁止できます。たとえば、3 つの Web サーバをホスティングする DMZ が設定されている場合、**switchport protected** コマンドを各スイッチ ポートに適用する際には、各 Web サーバを隔離できます。内部と外部のネットワークはいずれも 3 つの Web サーバすべてと相互に通信できますが、Web サーバは相互に通信できません。

保護されていないポートへの通信とそのポートからの通信は、このコマンドによって制限されません。

例

次の例では、7 つのスイッチ ポートが設定されます。イーサネット 0/4、0/5、および 0/6 は、DMZ ネットワークに割り当てられ、相互に保護されています。

```
hostname(config)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/5
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/6
hostname(config-if)# switchport access vlan 300
hostname(config-if)# switchport protected
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport trunk allowed vlan	VLAN をトランク ポートに割り当てます。

switchport trunk allowed vlans

組み込みスイッチの付いた ASA 5505 適応型セキュリティ アプライアンスなどのモデルでは、インターフェイス コンフィギュレーション モードで **switchport trunk allowed vlans** コマンドを使用して、VLAN をトランク ポートに割り当てます。1 つまたは複数の VLAN をトランクから削除するには、このコマンドの **no** 形式を使用します。

switchport trunk allowed vlans *vlan_range*

no switchport trunk allowed vlans *vlan_range*

シンタックスの説明

vlan_range	トランク ポートに割り当て可能な 1 つまたは複数の VLAN を指定します。VLAN ID は 1 ～ 1001 です。 *vlan_range* は、次のいずれかの方法で指定できます。 • 単一の番号（n） • 範囲（n-x） 番号および範囲は、カンマで区切ります。たとえば、次のように指定します。 5,7-10,13,45-100 カンマの代わりにスペースを使用できますが、コマンドはカンマ付きでコンフィギュレーションに保存されます。

デフォルト

デフォルトでは VLAN はトランクに割り当てられません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
7.2(2)	このコマンドは、スイッチ ポートごとに 3 つ以上の VLAN を割り当てられるように修正されました。また、今までは 1 つのトランク ポートに限定されていましたが、複数のトランク ポートを設定できるようになりました。このコマンドでは、スペースの代わりにカンマを使用して VLAN ID を区切ることもできます。

使用上のガイドライン

複数の VLAN が通過するトランク ポートをスイッチ ポート上に作成する場合は、モードをトランク モードに設定してから、**switchport trunk allowed vlan** コマンドを使用して、複数の VLAN をトランクに割り当てます。このスイッチ ポートについては、少なくとも 1 つの VLAN が割り当てられるまでは、トラフィックを通過させることができません。モードをトランク モードに設定し、

switchport trunk allowed vlan コマンドを設定していない場合、スイッチ ポートは「line protocol down」状態のままになり、トラフィックの転送には参加できません。トランク モードを使用できるのは、Security Plus ライセンスの場合のみです。

switchport trunk allowed vlan コマンドは、モードをトランク モードに設定しない限り有効になりません。

トランク ポートはタグのないパケットをサポートしません。ネイティブ VLAN はサポートされず、セキュリティ アプライアンスはこのコマンドで指定したタグを含んでいないパケットをすべてドロップします。

no switchport trunk allowed vlan コマンドを使用すると、すべての VLAN または VLAN のサブセットをトランクから削除できます。

（注） このコマンドは、バージョン 7.2(1) との下位互換性はなく、VLAN を区切るためのカンマは 7.2(1) では認識されません。ダウングレードした場合は、必ずスペースで VLAN を区切り、4 つ以上の VLAN を指定しないでください。

例

次の例では、アクセス モードのスイッチ ポートに VLAN 100 を割り当て、トランク モードのスイッチ ポートに VLAN 200、201、および 202 を割り当て、もう 1 つのトランク モードのスイッチ ポートに VLAN 300、301、および 305 を割り当てています。

```
hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 200-202
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport mode trunk
hostname(config-if)# switchport trunk allowed vlan 300,301,305
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show running-config interface	実行コンフィギュレーションのインターフェイス コンフィギュレーションを表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。
switchport mode	VLAN モードをアクセスまたはトランクに設定します。
switchport protected	同じ VLAN 上でスイッチ ポートが他のスイッチ ポートと通信することを禁止して、セキュリティを大幅に強化します。

syn-data

データを含んでいる SYN パケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

syn-data {**allow** | **drop**}

no syn-data {**allow** | **drop**}

シンタックスの説明

allow	データを含んでいる SYN パケットを許可します。
drop	データを含んでいる SYN パケットをドロップします。

デフォルト

デフォルトでは、データを含んでいる SYN パケットは許可されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **syn-data** コマンドを使用して、データを含んでいる SYN パケットをドロップします。

TCP の仕様によると、TCP 実装は、SYN パケットに含まれているデータを受け入れることが要件になっています。これは仕様の微妙かつあいまいな点であり、実装の中には、このパケットを適切に処理しないものもあります。不適切なエンドシステム実装を標的にする挿入攻撃に対して、脆弱にならないようにするには、データを含んでいる SYN パケットをドロップすることをお勧めします。

例

次の例は、データを含んでいる SYN パケットをすべての TCP フローでドロップする方法を示しています。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# syn-data drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

sysopt connection permit-vpn

VPN トンネルを通してセキュリティ アプライアンスに入り、復号化されるトラフィックに対して、トラフィックがインターフェイス アクセス リストをバイパスできるように、グローバル コンフィギュレーション モードで **sysopt connection permit-vpn** コマンドを使用します。グループ ポリシーおよびユーザごとの認可アクセス リストは、引き続きトラフィックに適用されます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sysopt connection permit-vpn

no sysopt connection permit-vpn

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

この機能はデフォルトでイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが、デフォルトでイネーブルになりました。また、バイパスされるのはインターフェイスのアクセス リストのみです。グループ ポリシーおよびユーザごとのアクセス リストは有効なままです。
7.1(1)	このコマンドが、**sysopt connection permit-ipsec** から変更されました。

使用上のガイドライン

デフォルトでは、セキュリティ アプライアンスは VPN トラフィックがセキュリティ アプライアンスのインターフェイスで終端することを許可しています。したがって、IKE または ESP（またはその他のタイプの VPN パケット）をインターフェイス アクセス リストに含める必要はありません。デフォルトでは、復号化された VPN パケットのローカル IP アドレスに対するインターフェイス アクセス リストも必要ありません。VPN トンネルは VPN セキュリティ メカニズムを使用して正常に終端するため、この機能によりコンフィギュレーションが簡略化され、セキュリティ アプライアンスのパフォーマンスもセキュリティ リスクを負うことなく最大化されます（グループ ポリシーおよびユーザごとの認可アクセス リストは、引き続きトラフィックに適用されます）。

インターフェイス アクセス リストをローカル IP アドレスに適用するには、**no sysopt connection permit-vpn** コマンドを入力します。アクセス リストの作成およびアクセス リストのインターフェイスへの適用については、**access-list** コマンドおよび **access-group** コマンドを参照してください。アクセス リストはローカル IP アドレスに適用されますが、VPN パケットが復号化される前に使用された元のクライアント IP アドレスには適用されません。

例

次の例では、復号化された VPN トラフィックがインターフェイス アクセス リストに従う必要があります。

```
hostname(config)# no sysopt connection permit-vpn
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、最大サイズが指定したサイズよりも小さくならないようにします。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection tcpmss

TCP セグメントの最大サイズが設定した値を超えないようにし、指定したサイズよりも小さくならないようにするには、グローバル コンフィギュレーション モードで **sysopt connection tcpmss** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

sysopt connection tcpmss [***minimum***] *bytes*

no sysopt connection tcpmss [***minimum***] [*bytes*]

シンタックスの説明

bytes	TCP セグメントの最大サイズをバイト単位で設定します（48 ～任意の最大値）。デフォルト値は 1,380 バイトです。*bytes* を 0 に設定することによって、この機能をディセーブルにできます。 ***minimum*** キーワードの場合、*bytes* は許容される最も小さい最大値を表します。
minimum	セグメントの最大サイズを上書きして、*bytes* 未満（48 ～ 65,535 バイト）にならないようにします。この機能は、デフォルトではディセーブルになっています（0 に設定されています）。

デフォルト

デフォルトの最大値は 1,380 バイトです。minimum 機能は、デフォルトではディセーブルになっています（0 に設定されています）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

ホストとサーバが接続を最初に確立するときは、ホストとサーバの両方でセグメントの最大サイズを設定できます。どちらかの最大サイズが **sysopt connection tcpmss** コマンドで設定した値を超えている場合、セキュリティ アプライアンスはその最大サイズを無効にして、設定した値を挿入します。どちらかの最大サイズが **sysopt connection tcpmss minimum** コマンドで設定した値よりも小さくなっている場合、セキュリティ アプライアンスはその最大サイズを無効にして、設定した「minimum」値を挿入します（minimum 値は、許容される最も小さい最大サイズです）。たとえば、最大サイズを 1,200 バイト、最小サイズを 400 バイトに設定した場合、ホストが最大サイズとして 1,300 バイトを要求しているときは、1,200 バイト（最大サイズ）を要求するようにセキュリティ アプライアンスがパケットを変更します。別のホストが最大値として 300 バイトを要求している場合、セキュリティ アプライアンスは 400 バイト（最小サイズ）を要求するようにパケットを変更します。

デフォルトの 1,380 バイトにしておくと、ヘッダー情報用の余裕ができるため、パケット全体のサイズが 1,500 バイトを超えることがなくなります。1,500 バイトは、イーサネットのデフォルト Maximum Transmission Unit（MTU; 最大伝送ユニット）です。次の計算式を参照してください。

1,380 データ + 20 TCP + 20 IP + 24 AH + 24 ESP_CIPHER + 12 ESP_AUTH + 20 IP = 1,500 バイト

ホストまたはサーバが最大セグメント サイズを要求しない場合、セキュリティ アプライアンスは、RFC 793 のデフォルト値である 536 バイトが有効であると想定します。

最大サイズを 1,380 バイトよりも大きい値に設定すると、MTU のサイズ（デフォルトは 1,500 バイト）によってはパケットがフラグメント化される可能性があります。フラグメントが大量に発生すると、セキュリティ アプライアンスが Frag Guard 機能を使用している場合にパフォーマンスに影響する可能性があります。最小サイズを設定しておくと、TCP サーバが小さな TCP データ パケットをクライアントに大量に送信して、サーバとネットワークのパフォーマンスに影響を与えることを防止できます。

（注） この機能を普通に使用する場合にはお勧めしませんが、syslog IPFRAG メッセージ 209001 および 209002 が発生する場合は、*bytes* 値を大きくできます。

例

次の例では、最大サイズを 1,200 バイト、最小サイズを 400 バイトに設定しています。

```
hostname(config)# sysopt connection tcpmss 1200
hostname(config)# sysopt connection tcpmss minimum 400
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection timewait	最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が短縮 TIME_WAIT 状態を保持するようにします。

sysopt connection timewait

最後の標準 TCP クローズダウン シーケンスの後、各 TCP 接続が少なくとも 15 秒の短縮 TIME_WAIT 状態を保持するようにするには、グローバル コンフィギュレーション モードで **sysopt connection timewait** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。エンド ホスト アプリケーションのデフォルト TCP 終了シーケンスが同時クローズである場合は、この機能を使用することをお勧めします。

sysopt connection timewait

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

この機能は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

セキュリティ アプライアンスのデフォルトの動作では、シャットダウン シーケンスが追跡され、2 つの FIN と最後の FIN セグメントの ACK の後、接続が解放されます。この即時解放ヒューリスティックにより、セキュリティ アプライアンスは、標準クローズ シーケンスと呼ばれる一般的なクロージング シーケンスに基づいて、高接続率を保つことができます。ただし、一方のエンドがクローズし、もう一方のエンドは確認応答してからクロージング シーケンスを開始する標準クローズ シーケンスとは対照的に、同時クローズでは、トランザクションの両エンドがクロージング シーケンスを開始します（RFC 793 を参照）。したがって、同時クローズでは、即時解放により、接続の 1 つのサイドで CLOSING 状態が保持されます。CLOSING 状態の多くのソケットがある場合は、エンド ホストのパフォーマンスが低下することがあります。たとえば、一部の WinSock メインフレーム クライアントは、このような動作を示し、メインフレーム サーバのパフォーマンスを低下させることが確認されています。**sysopt connection timewait** コマンドを使用すると、同時クローズ ダウン シーケンスを完了するためのウィンドウが作成されます。

例

次の例では、timewait（一時停止）機能をイネーブルにしています。

```
hostname(config)# sysopt connection timewait
```

関連コマンド

コマンド	説明
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt connection permit-ipsec	ACL でインターフェイスをチェックせずに IPSec トンネルからのすべてのパケットを許可します。
sysopt connection tcpmss	TCP セグメントの最大サイズを上書きします。または、最大サイズが指定したサイズよりも小さくならないようにします。

sysopt nodnsalias

alias コマンドを使用する場合に、DNS の A レコード アドレスを変更する DNS 検査をディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt nodnsalias** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。**alias** コマンドで NAT だけを実行して、DNS パケットの変更が不要な場合には、DNS アプリケーション検査をディセーブルにすることをお勧めします。

sysopt nodnsalias {***inbound*** | ***outbound***}

no sysopt nodnsalias {***inbound*** | ***outbound***}

シンタックスの説明

inbound	セキュリティの低いインターフェイスから、**alias** コマンドで指定したセキュリティの高いインターフェイスに向かうパケットの DNS レコード変更をディセーブルにします。
outbound	**alias** コマンドで指定したセキュリティの高いインターフェイスから、セキュリティの低いインターフェイスに向かうパケットの DNS レコード変更をディセーブルにします。

デフォルト

この機能は、デフォルトではディセーブルになっています。つまり、DNS レコードのアドレス変更がイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

alias コマンドは、NAT、および DNS の A レコードのアドレス変更を実行します。DNS レコードの変更は、特定の状況下ではディセーブルにした方がよい場合もあります。

例

次の例では、着信パケットについて DNS アドレスの変更をディセーブルにしています。

```
hostname(config)# sysopt nodnsalias inbound
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に対応するように DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt noproxyarp	インターフェイス上でのプロキシ ARP をディセーブルにします。

sysopt noproxyarp

NAT グローバル アドレスに対するインターフェイス上でのプロキシ ARP をディセーブルにするには、グローバル コンフィギュレーション モードで **sysopt noproxyarp** コマンドを使用します。グローバル アドレスに対するプロキシ ARP を再度イネーブルにするには、このコマンドの **no** 形式を使用します。

sysopt noproxyarp *interface_name*

no sysopt noproxyarp *interface_name*

シンタックスの説明

interface_name	プロキシ ARP をディセーブルにするインターフェイス名。

デフォルト

デフォルトでは、グローバル アドレスに対するプロキシ ARP はイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

まれに、グローバル アドレスに対するプロキシ ARP をディセーブルにした方がよい場合もあります。

ホストが IP トラフィックを同じイーサネット ネットワーク上の別のデバイスに送信するとき、ホストはデバイスの MAC アドレスを知っている必要があります。ARP は、IP アドレスを MAC アドレスに解決するレイヤ 2 プロトコルです。ホストは、「この IP アドレスは誰なのか」という ARP 要求を送信します。当該の IP アドレスを所有しているデバイスは、「その IP アドレスを所有している。これが私の MAC アドレスだ」という応答を返します。

プロキシ ARP は、デバイスが当該の IP アドレスを所有していない場合でも、デバイスが自身の MAC アドレスで ARP 要求に応答する動作です。NAT を設定して、セキュリティ アプライアンス インターフェイスと同じネットワーク上にあるグローバル アドレスを指定すると、セキュリティ アプライアンスはプロキシ ARP を使用します。トラフィックがホストに到達する唯一の方法は、セキュリティ アプライアンスがプロキシ ARP を使用して、セキュリティ アプライアンスの MAC アドレスが宛先グローバル アドレスに割り当てられていると主張することです。

例

次の例では、内部インターフェイス上でのプロキシ ARP をディセーブルにしています。

```
hostname(config)# sysopt noproxyarp inside
```

関連コマンド

コマンド	説明
alias	外部アドレスを変換し、変換に対応するように DNS レコードを変更します。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。
sysopt nodnsalias	**alias** コマンドを使用するときに、DNS の A レコード アドレスの変更をディセーブルにします。

sysopt radius ignore-secret

RADIUS アカウンティング応答に含まれている認証キーを無視するには、グローバル コンフィギュレーション モードで **sysopt radius ignore-secret** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。一部の RADIUS サーバとの互換性を維持するには、このキーを無視する必要があります。

sysopt radius ignore-secret

no sysopt radius ignore-secret

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

この機能は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

Livingston Version 1.16 など、一部の RADIUS サーバでは、アカウンティング確認応答の認証ハッシュ内にキーが含まれていないという使用上の注意点があります。このような場合、セキュリティ アプライアンスがアカウンティング要求を継続的に再送信することがあります。**sysopt radius ignore-secret** コマンドは、アカウンティング確認応答の認証キーを無視して、再送信の問題を回避するために使用します。ここで説明しているキーとは、**aaa-server host** コマンドで設定するキーです。

例

次の例では、アカウンティング応答に含まれている認証キーを無視しています。

```
hostname(config)# sysopt radius ignore-secret
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバを指定します。
clear configure sysopt	**sysopt** コマンドのコンフィギュレーションを消去します。
show running-config sysopt	**sysopt** コマンドのコンフィギュレーションを表示します。

CHAPTER 32

tcp-map コマンド～ type echo コマンド

tcp-map

TCP フローの検査をカスタマイズするには、グローバル コンフィギュレーション モードで **tcp-map** コマンドを使用します。TCP マップの指定を削除するには、このコマンドの **no** 形式を使用します。

tcp-map *map_name*

no tcp-map *map_name*

シンタックスの説明

map_name	モジュラ ポリシー CLI モードで TCP マップを適用するために使用する TCP マップ名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用して、高度な TCP 接続設定を設定します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。次のコマンドを tcp マップ コンフィギュレーション モードで使用できます。

check-retransmission	再転送データのチェックをイネーブルおよびディセーブルにします。
checksum-verification	チェックサムの確認をイネーブルおよびディセーブルにします。
exceed-mss	ピアにより設定された MSS を超過したパケットを許可またはドロップします。
queue-limit	TCP 接続のキューに入れることができる順序付けされていないパケットの最大数を設定します。このコマンドは、ASA 5500 シリーズ適応型セキュリティ アプライアンスでのみ使用できます。PIX 500 シリーズのセキュリティ アプライアンスでは、キューに入れられるパケットは 3 つまでで、この数を変更することはできません。
reserved-bits	セキュリティ アプライアンスに予約済みフラグ ポリシーを設定します。
syn-data	データを持つ SYN パケットを許可またはドロップします。
tcp-options	selective-ack、timestamp、window-scale の各 TCP オプションを許可または消去します。
ttl-evasion-protection	セキュリティ アプライアンスにより提供された TTL 回避保護をイネーブルまたはディセーブルにします。
urgent-flag	セキュリティ アプライアンスを通して URG ポインタを許可または消去します。
window-variation	突然ウィンドウ サイズが変更された接続をドロップします。

例

次の例では、localmap という名前の TCP マップの使用を指定するための **tcp-map** コマンドの使用方法を示します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server
hostname(config-cmap)# exit

hostname(config)# tcp-map localmap

hostname(config)# policy-map global_policy global
hostname(config-pmap)# description This policy map defines a policy concerning
connection to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection advanced-options localmap
hostname(config-pmap-c)#
```

関連コマンド

コマンド	説明
class（ポリシー マップ）	トラフィック分類に使用するクラス マップを指定します。
clear configure tcp-map	TCP マップのコンフィギュレーションを消去します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
show running-config tcp-map	TCP マップ コンフィギュレーションに関する情報を表示します。
tcp-options	selective-ack、timestamp、window-scale の各 TCP オプションを許可または消去します。

tcp-options

セキュリティ アプライアンスを通して TCP オプションを許可または消去するには、tcp マップ コンフィギュレーション モードで **tcp-options** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

no tcp-options {**selective-ack** | **timestamp** | **window-scale**} {**allow** | **clear**}

tcp-options range *lower upper* {**allow** | **clear** | **drop**}

no tcp-options range *lower upper* {**allow** | **clear** | **drop**}

シンタックスの説明

allow	TCP ノーマライザを通して TCP オプションを許可します。
clear	TCP ノーマライザを通して TCP オプションを消去し、パケットを許可します。
drop	パケットをドロップします。
lower	下位バインド範囲（6 ～ 7）および（9 ～ 255）です。
selective-ack	選択的な確認応答メカニズム（SACK）オプションを設定します。デフォルトでは、SACK オプションを許可します。
timestamp	timestamp オプションを設定します。timestamp オプションを消去すると、PAWS および RTT がディセーブルとなります。デフォルトでは、timestamp オプションを許可します。
upper	上位バインド範囲（6 ～ 7）および（9 ～ 255）です。
window-scale	window scale mechanism オプションを設定します。デフォルトでは、window scale mechanism オプションを許可します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **tcp-options** コマンドを使用して、selective-acknowledgement オプション、window-scale オプション、および timestamp TCP オプションを消去します。また、明確に定義されていないオプションを持つパケットも消去またはドロップできます。

例

次の例では、TCP オプションが 6 ～ 7 および 9 ～ 255 の範囲にあるすべてのパケットをドロップする方法を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# tcp-options range 6 7 drop
hostname(config-tcp-map)# tcp-options range 9 255 drop
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
hostname(config)#
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

telnet

コンソールへの Telnet アクセスを追加して、アイドル タイムアウトを設定するには、グローバル コンフィギュレーション モードで **telnet** コマンドを使用します。あらかじめ設定された IP アドレスから Telnet アクセスを削除するには、このコマンドの **no** 形式を使用します。

telnet {{*hostname* | *IP_address mask interface_name*} | {*IPv6_address interface_name*} | {**timeout** *number*}}

no telnet {{*hostname* | *IP_address mask interface_name***} | {***IPv6_address interface_name***} | {timeout** *number*}**}**

シンタックスの説明

hostname	セキュリティ アプライアンスの Telnet コンソールにアクセスできるホストの名前を指定します。
interface_name	Telnet へのネットワーク インターフェイスの名前を指定します。
IP_address	セキュリティ アプライアンスへのログインを認可するホストまたはネットワークの IP アドレスを指定します。
IPv6_address	セキュリティ アプライアンスへのログインを認可する IPv6 アドレスおよびプレフィックスを指定します。
mask	IP アドレスに関連付けられているネットマスクを指定します。
timeout *number*	Telnet セッションがセキュリティ アプライアンスによって停止されるまでにアイドル状態を維持する時間（分）。有効な値は 1 ～ 1,440 分です。

デフォルト

デフォルトでは、Telnet セッションのアイドル状態が 5 分間続くと、セキュリティ アプライアンスによって停止されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	変数 *IPv6_address* が追加されました。また、**no telnet timeout** コマンドも追加されました。

使用上のガイドライン

telnet コマンドでは、Telnet でセキュリティ アプライアンス コンソールにアクセスできるホストを指定できます。セキュリティ アプライアンスへの Telnet 接続は、すべてのインターフェイスでイネーブルにできます。ただし、セキュリティ アプライアンスでは、外部インターフェイスへの Telnet トラフィックがすべて、必ず IPSec で保護されます。外部インターフェイスへの Telnet セッションをイネーブルにするには、まず外部インターフェイス上で、IPSec がセキュリティ アプライアンスの生成する IP トラフィックを含むように設定した後、外部インターフェイスで Telnet をイネーブルにします。

no telnet コマンドを使用すると、それまでに設定した IP アドレスから Telnet アクセスが削除されます。**telnet timeout** コマンドを使用すると、コンソールの Telnet セッションの最大アイドル時間を設定して、その時間が経過すると、セキュリティ アプライアンスがログオフするようにできます。**no telnet** コマンドは、**telnet timeout** コマンドと共に使用できません。

IP アドレスを入力した場合、ネットマスクも入力する必要があります。デフォルトのネットマスクはありません。内部ネットワークのサブネットワーク マスクを使用しないでください。*netmask* は、IP アドレスのビット マスクだけです。アクセスを IP アドレス 1 つに制限するには、255.255.255.255 のように各オクテットに 255 を使用します。

IPSec が動作中の場合に、アンセキュアなインターフェイス名（通常、外部インターフェイス）を指定できます。**telnet** コマンドでインターフェイス名を指定するには、少なくとも、**crypto map** コマンドを設定する必要があります。

passwd コマンドを使用して、コンソールへの Telnet アクセスで使用するパスワードを設定します。デフォルトは **cisco** です。**who** コマンドを使用して、現在セキュリティ アプライアンス コンソールにアクセスしている IP アドレスを表示します。**kill** コマンドを使用して、アクティブな Telnet コンソール セッションを終了します。

aaa コマンドを **console** キーワードと共に使用する場合は、Telnet コンソール アクセスを認証サーバで認証する必要があります。

（注） **aaa** コマンドを設定して、セキュリティ アプライアンス Telnet コンソール アクセスに認証を要求した場合に、コンソール ログイン要求がタイムアウトしたときは、セキュリティ アプライアンス ユーザ名と **enable password** コマンドで設定したパスワードを入力して、シリアル コンソールからセキュリティ アプライアンスにアクセスできます。

例

次の例では、ホスト 192.168.1.3 および 192.168.1.4 が Telnet を通してセキュリティ アプライアンス コンソールへのアクセス許可を得る方法を示します。さらに、192.168.2.0 ネットワーク上のすべてのホストがアクセスを許可されます。

```
hostname(config)# telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# telnet 192.168.1.4 255.255.255.255 inside
hostname(config)# telnet 192.168.2.0 255.255.255.0 inside
hostname(config)# show running-config telnet
192.168.1.3 255.255.255.255 inside
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside
```

次の例では、セッションの最大アイドル継続時間を変更する方法を示します。

```
hostname(config)# telnet timeout 10
hostname(config)# show running-config telnet timeout
telnet timeout 10 minutes
```

次の例では、Telnet コンソール ログイン セッションを示します（パスワードは入力時には表示されません）。

```
hostname# passwd: cisco

Welcome to the XXX
…
Type help or '?' for a list of available commands.
hostname>
```

no telnet コマンドを使用して個々のエントリを削除することも、すべての telnet コマンド文を clear configure telnet コマンドで削除することもできます。

```
hostname(config)# no telnet 192.168.1.3 255.255.255.255 inside
hostname(config)# show running-config telnet
192.168.1.4 255.255.255.255 inside
192.168.2.0 255.255.255.0 inside

hostname(config)# clear configure telnet
```

関連コマンド

コマンド	説明
clear configure telnet	コンフィギュレーションから Telnet 接続を削除します。
kill	Telnet セッションを終了します。
show running-config telnet	セキュリティ アプライアンスへの Telnet 接続の使用を認可されている IP アドレスの現在のリストを表示します。
who	セキュリティ アプライアンス上のアクティブな Telnet 管理セッションを表示します。

terminal

現在の Telnet セッションでシステム ログ メッセージの表示を許可するには、特権 EXEC モードで **terminal monitor** コマンドを使用します。システム ログ メッセージをディセーブルにするには、**terminal no monitor** コマンドを使用します。

terminal {**monitor** | **no monitor**}

シンタックスの説明

monitor	現在の Telnet セッションでシステム ログ メッセージの表示をイネーブルにします。
no monitor	現在の Telnet セッションでシステム ログ メッセージの表示をディセーブルにします。

デフォルト

システム ログ メッセージは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、ロギングをイネーブルにしてから、現在のセッションだけでロギングをディセーブルにする方法を示します。

```
hostname# terminal monitor
hostname# terminal no monitor
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードで端末の表示幅を設定します。

terminal pager

Telnet セッションで「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定するには、特権 EXEC モードで **terminal pager** コマンドを使用します。

terminal pager [lines] *lines*

シンタックスの説明

[**lines**] *lines*	「---more---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページが無制限であることを示します。範囲は 0 ～ 2,147,483,647 行です。**lines** キーワードはオプションです。このキーワードの有無にかかわらず、コマンドは同じです。

デフォルト

デフォルトは 24 行です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、現在の Telnet セッションに対してだけ pager line 設定を変更します。新しいデフォルトの pager 設定をコンフィギュレーションに保存するには、**pager** コマンドを使用します。

管理コンテキストに Telnet 接続する場合、ある特定のコンテキスト内の **pager** コマンドに異なる設定があっても、他のコンテキストに移ったときには、pager line 設定はユーザのセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

例

次の例では、表示される行数を 20 に変更します。

```
hostname# terminal pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されます。
show running-config terminal	現在の端末設定を表示します。
terminal	システム ログ メッセージが Telnet セッションで表示されるようにします。
terminal width	グローバル コンフィギュレーション モードで端末の表示幅を設定します。

terminal width

コンソール セッション中に情報を表示する幅を設定するには、グローバル コンフィギュレーション モードで **terminal** ***width*** コマンドを使用します。ディセーブルにするには、このコマンドの ***no*** 形式を使用します。

terminal ***width columns***

no terminal ***width columns***

シンタックスの説明

columns	端末の幅をカラム単位で指定します。デフォルトは 80 です。範囲は 40 ～ 511 です。

デフォルト

デフォルトの表示幅は 80 カラムです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

例

次の例では、端末の表示幅を 100 カラムにする方法を示します。

```
hostname# terminal width 100
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定を消去します。
show running-config terminal	現在の端末設定を表示します。
terminal	特権 EXEC モードで端末回線のパラメータを設定します。

test aaa-server

test aaa-server コマンドを使用して、セキュリティ アプライアンスが特定の AAA サーバでユーザを認証または認可できるかどうかを確認します。AAA サーバへの到達に失敗する場合、セキュリティ アプライアンスのコンフィギュレーションが誤っているか、他の理由（ネットワーク コンフィギュレーションまたはサーバのダウンタイムが制限されているなど）で到達不能になっている可能性があります。

test aaa-server {authentication | authorization} *server-tag* **[host** *server-ip*] **[username** *username*] **[password** *password*]

シンタックスの説明

authentication	セキュリティ アプライアンスはテスト認証要求を送信する必要があることを指定します。
authorization	セキュリティ アプライアンスはテスト認可要求を送信する必要があることを指定します。
host *server-ip*	AAA サーバの IP アドレスを指定します。
password *password*	所定のユーザ名のパスワードを指定します。**password** 引数は認証テストの場合にだけ使用できます。入力されたユーザ名に対してパスワードが正しいことを確認します。正しくない場合、認証テストは失敗します。
server-tag	**aaa-server protocol** コマンドで定義されているサーバ グループの識別名を指定します。
username *username*	AAA サーバ設定のテストに使用されるアカウントのユーザ名を指定します。AAA サーバ上にそのユーザ名が存在することを確認します。存在しない場合、テストは失敗します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

test aaa-server コマンドを使用して、セキュリティ アプライアンスが特定の AAA サーバでユーザを認証または認可できるかどうかを確認します。このコマンドを使用すると、実際のサプリカントでテストする必要がないため、セキュリティ アプライアンス上のコンフィギュレーションの確認が簡略化されます。また、認証および認可の失敗が、AAA サーバ パラメータの設定の誤り、AAA サーバへの接続の問題、またはセキュリティ アプライアンスでのその他のコンフィギュレーション エラーに起因するものかどうかを識別できます。

このコマンドを入力すると、***host*** および ***password*** キーワードと引数のペアを省略できます。セキュリティ アプライアンスは、これらの値を入力するようにプロンプトを表示します。認証テストを実行している場合、***password*** キーワードと引数のペアを省略して、セキュリティ アプライアンスがプロンプトを表示しているときにパスワードを入力できます。

例

次の例では、ホスト 192.168.3.4 の srvgrp1 という名前の RADIUS AAA サーバに対して、タイムアウト 9 秒、リトライ間隔 7 秒、認証ポート 1650 を設定します。AAA サーバ パラメータの設定に続く **test aaa-server** コマンドは、認証テストがサーバに到達できずに失敗したことを示しています。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 192.168.3.4
hostname(config-aaa-server-host)# timeout 9
hostname(config-aaa-server-host)# retry-interval 7
hostname(config-aaa-server-host)# authentication-port 1650
hostname(config-aaa-server-host)# exit
hostname(config)# test aaa-server authentication svrgrp1
Server IP Address or name: 192.168.3.4
Username: bogus
Password: ******
INFO: Attempting Authentication test to IP address <192.168.3.4> (timeout: 10 seconds)
ERROR: Authentication Server not responding: No error
```

関連コマンド

コマンド	説明
aaa-server host	特定の AAA サーバのパラメータを指定します。
show running-config aaa-server	すべての AAA サーバ、特定のサーバ グループ、特定のグループ内の特定のサーバ、または特定のプロトコルの AAA サーバ統計情報を表示します。

test regex

正規表現をテストするには、特権 EXEC モードで **test regex** コマンドを使用します。

test regex *input_text regular_expression*

シンタックスの説明

input_text	正規表現と照合するテキストを指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現で使用できるメタ文字のリストについては、**regex** コマンドを参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

test regex コマンドは、正規表現が一致すべきものと一致するかどうかをテストします。

入力したテキストと正規表現が一致すると、次のメッセージが表示されます。

```
INFO: Regular expression match succeeded.
```

一致しない場合は、次のメッセージが表示されます。

```
INFO: Regular expression match failed.
```

例

次の例は、入力したテキストと正規表現が一致するかどうかをテストします。

```
hostname# test regex farscape scape
INFO: Regular expression match succeeded.

hostname# test regex farscape scaper

INFO: Regular expression match failed.
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	トラフィック クラスを 1 つまたは複数のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション検査のための特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
regex	正規表現を作成します。

test sso-server

テスト認証要求で SSO サーバをテストするには、特権 EXEC モードで **test sso-server** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

test sso-server *server-name* **username** *user-name*

シンタックスの説明

server-name	テストされる SSO サーバの名前を指定します。
user-name	テストされる SSO サーバ上のユーザ名を指定します。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザはユーザ名とパスワードを 1 度入力すると、再入力しなくてもさまざまなサーバで各種のセキュアなサービスにアクセスできます。**test sso-server** コマンドは、SSO サーバが認識されるかどうか、および認証要求に応答するかどうかをテストします。

server-name 引数により指定された SSO サーバが検出されない場合は、次のエラーが表示されます。

```
ERROR: sso-server server-name does not exist
```

SSO サーバが検出されても *user-name* 引数によって指定されたユーザが検出されない場合、認証は拒否されます。

例

特権 EXEC モードで入力された次の例では、my-sso-server という名前の SSO サーバが Anyuser というユーザ名を使用して正常にテストされています。

```
hostname# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Success
hostname#
```

次の例は同じサーバのテストを示していますが、Anyuser というユーザ名は認識されず、認証は失敗しています。

```
hostname# test sso-server my-sso-server username Anyuser
INFO: Attempting authentication request to sso-server my-sso-server for user Anyuser
INFO: STATUS: Failed
hostname#
```

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
request-timeout	失敗した SSO 認証試行がタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
web-agent-url	セキュリティ アプライアンスが SSO 認証を要求する SSO サーバの URL を指定します。

text-color

ログイン ページ、ホーム ページ、およびファイル アクセス ページの WebVPN タイトルバーのテキストに色を設定するには、WebVPN モードで **text-color** コマンドを使用します。テキストの色をコンフィギュレーションから削除してデフォルトにリセットするには、このコマンドの no 形式を使用します。

text-color [*black* | *white* | *auto***]**

no text-color

シンタックスの説明

auto	secondary-color コマンドの設定に基づいて黒または白を選択します。つまり、2 番目の色が黒の場合、この値は白となります。
black	タイトルバーのテキストのデフォルト色は白です。
white	色を黒に変更できます。

デフォルト

タイトルバーのテキストのデフォルト色は白です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次の例では、タイトルバーのテキストの色を黒に設定する方法を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# text-color black
```

関連コマンド

コマンド	説明
secondary-text-color	WebVPN ログイン ページ、ホーム ページ、およびファイル アクセス ページの 2 番目のテキストの色を設定します。

tftp-server

configure net コマンドまたは **write net** コマンドで使用するデフォルトの TFTP サーバおよびパスとファイル名を指定するには、グローバル コンフィギュレーション モードで **tftp-server** コマンドを使用します。サーバ コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 アドレスと IPv6 アドレスをサポートしています。

tftp-server *interface_name server filename*

no tftp-server [*interface_name server filename*]

シンタックスの説明

interface_name	ゲートウェイ インターフェイス名を指定します。最高のセキュリティ インターフェイス以外のインターフェイスを指定した場合、このインターフェイスがアンセキュアなことを示す警告メッセージが表示されます。
server	TFTP サーバの IP アドレスまたは名前を設定します。IPv4 アドレスまたは IPv6 アドレスを入力できます。
filename	パスとファイル名を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	現在ではゲートウェイ インターフェイスが必要です。

使用上のガイドライン

tftp-server コマンドを使用すると、**configure net** コマンドと **write net** コマンドの入力が容易になります。**configure net** コマンドや **write net** コマンドを入力するときに、**tftp-server** コマンドで指定した TFTP サーバを継承するか、独自の値を指定できます。また、**tftp-server** コマンドのパスをそのまま継承したり、**tftp-server** コマンド値の末尾にパスとファイル名を追加したり、**tftp-server** コマンド値を上書きすることもできます。

セキュリティ アプライアンスがサポートする **tftp-server** コマンドは 1 つだけです。

例

次の例では、TFTP サーバを指定し、コンフィギュレーションを /temp/config/test_config ディレクトリから読み取る方法を示します。

```
hostname(config)# tftp-server inside 10.1.1.42 /temp/config/test_config
hostname(config)# configure net
```

関連コマンド

コマンド	説明
configure net	コンフィギュレーションを TFTP サーバ上の指定パスからロードします。
show running-config tftp-server	デフォルトの TFTP サーバ アドレスとコンフィギュレーション ファイルのディレクトリを表示します。

threshold

SLA 監視オペレーションのしきい値超過イベントを決めるしきい値を設定するには、SLA モニタ コンフィギュレーション モードで **threshold** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

threshold *milliseconds*

no threshold

シンタックスの説明

milliseconds	宣言する上限値をミリ秒で指定します。有効な値は 0 ～ 2147483647 です。ただし、タイムアウトに設定された値よりも大きな値にすることはできません。

デフォルト

デフォルトのしきい値は 5000 ミリ秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

しきい値は、しきい値超過イベントを示すためだけに使われます。このイベントは、到達可能性には影響しませんが、**timeout** コマンドの設定が正しいかどうかを調べるために使用できます。

例

次の例では、ID が 123 の SLA オペレーションを設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA オペレーションの頻度を 10 秒、しきい値を 2,500 ミリ秒、タイムアウト値を 4,000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA 監視オペレーションを定義します。
timeout	SLA オペレーションが応答を待機する期間を定義します。

timeout

アイドル状態の最大継続時間を設定するには、グローバル コンフィギュレーション モードで **timeout** コマンドを使用します。

timeout {xlate | **conn** | **udp** | **icmp** | **rpc** | **h225** | **h323** | **mgcp** | ***mgcp-pat*** | **sip** | **sip-disconnect** | **sip-invite** | **sip_media**} *hh*:*mm*:*ss*

timeout uauth *hh*:*mm*:*ss* [**absolute** | **inactivity**]

シンタックスの説明

absolute	（オプション）タイムアウトになった場合は、無条件に再認証を求めます。
conn	（オプション）接続が終了するまでのアイドル時間を指定します。最短時間は 5 分です。
hh:*mm*:*ss*	タイムアウト時間を指定します。
h225 *hh*:*mm*:*ss*	（オプション）H.225 シグナリング接続が終了するまでのアイドル時間を指定します。
h323	（オプション）H.245（TCP）および H.323（UDP）メディア接続が終了するまでのアイドル時間を指定します。デフォルトは 5 分です。 **（注）** H.245 および H.323 メディア接続の両方に同じ接続フラグが設定されるため、H.245（TCP）接続は H.323（RTP および RTCP）メディア接続とアイドル タイムアウトを共有します。
half-closed	（オプション）TCP ハーフクローズ接続が解放されるまでのアイドル時間を指定します。
icmp	（オプション）ICMP のアイドル時間を指定します。
inactivity	（オプション）無活動タイムアウトになった場合は、再認証を求めます。
mgcp *hh:mm:ss*	（オプション）MGCP メディア接続が削除されるまでのアイドル時間を指定します。
mgcp-pat *hh:mm:ss*	（オプション）MGCP PAT 変換が削除されるまでの絶対間隔を設定します。
rpc	（オプション）RPC スロットが解放されるまでのアイドル時間を指定します。最短時間は 1 分です。
sip	（オプション）SIP タイマーを修正します。
sip-disconnect	（オプション）メディアが削除され、メディア xlate が終了するまでのアイドル時間を設定します。範囲は 1 ～ 10 分です。デフォルトは 2 分です。
sip-invite	（オプション）暫定応答のピンホールおよびメディア xlate が終了するまでのアイドル時間を設定します。範囲は 1 ～ 30 分です。デフォルトは 3 分です。
sip_media	（オプション）SIP メディア タイマーを修正します。メディア タイマーは、UDP 非アクティビティ タイムアウトの代わりに、SIP UDP メディア パケットを扱う SIP RTP/RTCP で使用されます。
sunrpc	（オプション）SUNRPC スロットが終了するまでアイドル時間を指定します。
uauth	（オプション）認証および認可キャッシュがタイムアウトするまでの継続時間を設定します。ユーザは次回の接続時に再認証を必要とします。
udp	（オプション）UDP スロットが解放されるまでのアイドル時間を指定します。最短時間は 1 分です。
xlate	（オプション）変換スロットが解放されるまでのアイドル時間を指定します。最短時間は 1 分です。

デフォルト

デフォルトは次のとおりです。

- **conn** *hh*:*mm*:*ss* は、1 時間（**01:00:00**）です。
- **h225** *hh*:*mm*:*ss* は、1 時間（**01:00:00**）です。
- **h323** *hh*:*mm*:*ss* は、5 分（**00:05:00**）です。
- **half-closed** *hh*:*mm*:*ss* は、10 分（**00:10:00**）です。
- **icmp** *hh:mm:ss* は、2 分（**00:00:0***2*）です。
- **mgcp** *hh:mm:ss* は、5 分（**00:05:00**）です。
- **mgcp-pat** *hh:mm:ss* は、5 分（**00:05:00**）です。
- **rpc** *hh*:*mm*:*ss* は、10 分（**00:10:00**）です。
- **sip** *hh:mm:* は、30 分（**00:30:00**）です。
- **sip-disconnect** *hh:mm:ss* は、2 分（**00:02:00**）です。
- **sip-invite** *hh:mm:ss* は、3 分（**00:03:00**）です。
- **sip_media** *hh:mm:ss* は、2 分（**00:02:00**）です。
- **sunrpc** *hh:mm:ss* は、10 分（**00:10:00**）です。
- **uauth** *hh:mm:ss* は、5 分（**00:5:00 absolute**）です。
- **udp** *hh*:*mm*:*ss* は、2 分（**00:02:00**）です。
- **xlate** *hh*:*mm*:*ss* は、3 時間（**03:00:00**）です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	キーワード ***mgcp-pat***、**sip-disconnect**、および **sip-invite** が追加されました。

使用上のガイドライン

timeout コマンドは、接続、変換 UDP、および RPC の各スロットに許容されるアイドル時間を設定します。指定されたアイドル時間内に、そのスロットが使用されていなければ、リソースがフリープールに戻されます。TCP 接続スロットは、通常の接続終了シーケンスの約 60 秒後に解放されます。

（注） 接続に受動 FTP を使用している場合、または Web 認証に **virtual** コマンドを使用している場合は、**timeout uauth 0:0:0** コマンドは使用しないでください。

timeout コマンドの後ろにキーワードと値を複数入力できます。

接続タイマーは、変換タイマーに優先します。つまり、変換タイマーは、すべての接続がタイムアウトした後に初めて動作します。

conn *hh*:*mm*:*ss* を設定する場合、**0:0:0** を使用すると、接続がタイムアウトしません。

half-closed *hh*:*mm*:*ss* を設定する場合、**0:0:0** を使用すると、ハーフクローズ接続がタイムアウトしません。

h255 *hh*:*mm*:*ss* を設定する場合、**h225 00:00:00** を使用すると、H.225 シグナリング接続が絶対に終了しません。タイムアウト値を **h225 00:00:01** に設定すると、タイマーがディセーブルになり、すべてのコールが消去された後、TCP 接続がすぐに終了します。

uauth *hh*:*mm*:*ss* 時間は、**xlate** キーワードより短く設定する必要があります。キャッシュをディセーブルにするには、**0** に設定します。接続上で受動 FTP が使用されている場合は、0 には設定しないでください。

absolute キーワードをディセーブルにするには、uauth タイマーに 0（ゼロ）を設定します。

例

次の例では、アイドル状態の最大継続時間を設定する方法を示します。

```
hostname(config)# timeout uauth 0:5:00 absolute uauth 0:4:00 inactivity
hostname(config)# show running-config timeout
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 rpc 0:10:00 h323 0:05:00
sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute uauth 0:04:00 inactivity
```

関連コマンド

コマンド	説明
show running-config timeout	指定したプロトコルのタイムアウト値を表示します。

timeout（AAA サーバ ホスト）

AAA サーバとの接続の確立を中止するまでの、ホスト固有の最大応答時間を秒単位で設定するには、AAA サーバ ホスト モードで **timeout** コマンドを使用します。タイムアウト値を削除して、タイムアウト時間をデフォルト値の 10 秒にリセットするには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout

シンタックスの説明

seconds	要求に対するタイムアウト間隔（1 ～ 60 秒）を指定します。この時間を超えると、セキュリティ アプライアンスは、プライマリ AAA サーバへの要求を断念します。スタンバイ AAA サーバが存在する場合、セキュリティ アプライアンスは要求をそのバックアップ サーバに送信します。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、すべての AAA サーバ プロトコル タイプに有効です。

timeout コマンドを使用して、セキュリティ アプライアンスが AAA サーバへの接続を試みる時間の長さを指定します。**retry-interval** コマンドを使用して、セキュリティ アプライアンスが接続を試行する間隔を指定します。

タイムアウトは、セキュリティ アプライアンスがサーバとのトランザクションの完了に必要となる合計所要時間です。リトライ間隔は、タイムアウト期間中に通信が再試行される頻度を決定します。したがって、リトライ間隔がタイムアウト値以上の場合、再試行されません。再試行する場合は、リトライ間隔をタイムアウト値よりも小さくする必要があります。

例

次の例では、ホスト 1.2.3.4 上の「svrgrp1」という名前の RADIUS AAA サーバに、タイムアウト値 30 秒、リトライ間隔 10 秒を設定します。したがって、セキュリティ アプライアンスは、30 秒後に中止するまで通信を 3 度試行します。

```
hostname(config)# aaa-server svrgrp1 protocol radius
hostname(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
hostname(config-aaa-server-host)# timeout 30
hostname(config-aaa-server-host)# retry-interval 10
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ ホスト コンフィギュレーション モードに入って、ホスト固有の AAA サーバ パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド文をコンフィギュレーションから削除します。
show running-config aaa	現在の AAA コンフィギュレーション値を表示します。

timeout（DNS サーバ グループ コンフィギュレーション モード）

次の DNS サーバを試すまで待機する時間を指定するには、dns サーバ グループ コンフィギュレーション モードで **timeout** コマンドを使用します。デフォルトのタイムアウトに戻すには、このコマンドの **no** 形式を使用します。

timeout *seconds*

no timeout [*seconds*]

シンタックスの説明

seconds	タイムアウトを 1 ～ 30 の間の秒単位で指定します。デフォルトは 2 秒です。セキュリティ アプライアンスが一連のサーバを試すたびに、このタイムアウトは倍増します。再試行の回数を設定するには、dns サーバ グループ コンフィギュレーション モードで **retries** コマンドを使用します。

デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.1	このコマンドが導入されました。

例

次の例では、DNS サーバ グループの「dnsgroup1」に対してタイムアウトを 1 秒に設定しています。

```
hostname(config)# dns server-group dnsgroup1
hostname(config-dns-server-group)# dns timeout 1
```

関連コマンド

コマンド	説明
clear configure dns	ユーザが作成したすべての DNS サーバ グループを削除して、デフォルトのサーバ グループのアトリビュートをデフォルト値にリセットします。
domain-name	デフォルトのドメイン名を設定します。
retries	セキュリティ アプライアンスが応答を受信しないときに、一連の DNS サーバへのアクセスを再試行する回数を指定します。
show running-config dns server-group	現在の実行 DNS サーバ グループ コンフィギュレーションを表示します。

timeout（GTP マップ）

GTP セッションの非アクティビティ タイマーを変更するには、GTP マップ コンフィギュレーション モードで **timeout** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスできます。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout {**gsn** | ***pdp-context*** | ***request*** | **signaling** | ***t3-response*** | ***tunnel*** } *hh*:*mm*:*ss*

no timeout {**gsn** | ***pdp-context*** | ***request*** | **signaling** | ***t3-response*** | ***tunnel*** } *hh*:*mm*:*ss*

シンタックスの説明

hh:*mm*:*ss*	これはタイムアウトで、*hh* は時間、*mm* は分、*ss* は秒を示し、これら 3 つの要素はコロン（:）で分けられます。値 0 は、すぐには絶対に終了しないことを意味します。
gsn	GSN が削除されるまでの非アクティビティの継続時間を指定します。
pdp-context	PDP コンテキストの受信を開始するまでの、許可される最大時間を指定します。
request	GTP メッセージの受信を開始するまでの､許可される最大時間を指定します。
signaling	GTP シグナリングが削除されるまでの非アクティビティの継続時間を指定します。
t3-response	GTP 接続が削除されるまでに応答を待つ最長時間を指定します。
tunnel	GTP トンネルが終了するまでの非アクティビティの継続時間を指定します。

デフォルト

デフォルトは、**gsn**、**pdp-context**、および **signaling** に対して 30 分です。

request のデフォルトは 1 分です。

tunnel のデフォルトは 1 時間です（Delete PDP Context Request を受信していない場合）。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	No

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

パケット データ プロトコル（PDP）コンテキストは、IMSI と NSAPI の組み合せであるトンネル識別子（TID）によって識別されます。各 MS は最大 15 の NSAPI を持つことができ、様々な QoS レベルのアプリケーション要件に基づいて、それぞれが異なる NSAPI を持つ複数の PDP コンテキストを作成できます。

GTP トンネルは、それぞれ別個の GSN ノードにある、2 つの関連する PDP コンテキストによって定義され、トンネル ID によって識別されます。GTP トンネルは、パケットを外部パケット データ ネットワークとモバイル ステーション ユーザの間で転送するために必要なものです。

例

次の例では、要求キューに対して 2 分のタイムアウト値を設定します。

```
hostname(config)# gtp-map gtp-policy
hostname(config-gtpmap)# timeout request 00:02:00
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

timeout（RADIUS アカウンティング）

RADIUS アカウンティングのユーザの非アクティビティ タイマーを変更するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **timeout** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。これらの間隔にデフォルト値を設定するには、このコマンドの **no** 形式を使用します。

timeout users *hh*:*mm*:*ss*

no timeout users *hh*:*mm*:*ss*

シンタックスの説明

hh:*mm*:*ss*	これはタイムアウトで、*hh* は時間、*mm* は分、*ss* は秒を示し、これら 3 つの要素はコロン（:）で分けられます。値 0 は、すぐには絶対に終了しないことを意味します。デフォルトは 1 時間です。
users	ユーザのタイムアウト値を指定します。

デフォルト

ユーザのデフォルトのタイムアウト値は 1 時間です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	•	•	•	•	No

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、ユーザのタイムアウト値を 10 分に設定します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout user 00:10:00
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングの検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

timeout（SLA モニタ）

SLA オペレーションで要求パケットへの応答を待つ時間を設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **timeout** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timeout *milliseconds*

no timeout

シンタックスの説明

milliseconds	0 ～ 604800000

デフォルト

デフォルトのタイムアウト値は 5000 ミリ秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

SLA オペレーションで要求パケットを送信する頻度を設定するには **frequency** コマンドを使用し、要求への応答を受信するために待機時間を設定するには **timeout** コマンドを使用します。**timeout** コマンドで指定する値は、**frequency** コマンドで指定する値より大きくすることはできません。

例

次の例では、ID が 123 の SLA オペレーションを設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA オペレーションの頻度を 10 秒、しきい値を 2,500 ミリ秒、タイムアウト値を 4,000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
frequency	SLA オペレーションを繰り返す頻度を指定します。
sla monitor	SLA 監視オペレーションを定義します。

timeout pinhole

DCERPC ピンホールのタイムアウト値を設定し、グローバルなシステム ピンホール タイムアウト値である 2 分を上書きするには、パラメータ コンフィギュレーション モードで **timeout pinhole** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

timeout pinhole *hh:mm:ss*

no timeout pinhole

シンタックスの説明

hh:mm:ss	ピンホール接続のタイムアウト値。0:0:1 ～ 1193:0:0 の値を指定できます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、DCERPC 検査ポリシー マップのピンホール接続のタイムアウト値を設定する方法を示します。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# timeout pinhole 0:10:00
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

time-range

時間範囲コンフィギュレーション モードに入り、トラフィックの規則、またはアクションに関連付ける時間範囲を定義するには、グローバル コンフィギュレーション モードで ***time-range*** コマンドを使用します。ディセーブルにするには、このコマンドの **no** 形式を使用します。

time-range *name*

no time-range *name*

シンタックスの説明

name	時間範囲の名前。64 文字以下にする必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

時間範囲を作成しても、デバイスへのアクセスは制限されません。**time-range** コマンドは、時間範囲だけを定義します。時間範囲を定義したら、トラフィックの規則かアクションに関連付けます。

時間ベース ACL を実装するには、***time-range*** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended time-range** コマンドと共に使用して、時間範囲を ACL にバインドします。

時間範囲は、セキュリティ アプライアンスのシステム クロックによって決まりますが、NTP で同期を取れます。

例

次の例では、New_York_Minute という時間範囲を作成し、時間範囲コンフィギュレーション モードに入ります。

```
hostname(config)# time-range New_York_Minute
hostname(config-time-range)#
```

時間範囲を作成し、時間範囲コンフィギュレーション モードに入ったら、**absolute** キーワードと **periodic** キーワードを使用して時間範囲のパラメータを定義できます。***time-range*** コマンドの ***absolute*** キーワードおよび ***periodic*** キーワードの設定をデフォルトに戻すには、時間範囲コンフィギュレーション モードで ***default*** コマンドを使用します。

時間ベース ACL を実装するには、***time-range*** コマンドを使用して、週および 1 日の中の特定の時刻を定義します。次に、**access-list extended** コマンドを使用して、時間範囲を ACL にバインドします。次の例では、Sales という ACL を New_York_Minute という時間範囲にバインドします。

```
hostname(config)# access-list Sales line 1 extended deny tcp host 209.165.200.225 host
209.165.201.1 time-range New_York_Minute
hostname(config)#
```

ACL の詳細については、**access-list extended** コマンドを参照してください。

関連コマンド

コマンド	説明
absolute	時間範囲が有効である絶対時間を定義します。
access-list extended	セキュリティ アプライアンス経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	***time-range*** コマンドの ***absolute*** キーワードと ***periodic*** キーワードの設定をデフォルトに戻します。
periodic	時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定します。

timers spf

最短パス優先（SPF）計算の遅延時間と待機時間を指定するには、ルータ コンフィギュレーション モードで **timers spf** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

timers spf *delay holdtime*

no timers spf [*delay holdtime*]

シンタックスの説明

delay	OSPF によるトポロジ変更の受信と最短パス優先（SPF）計算の開始との間の遅延時間（1 ～ 65,535 秒）を指定します。
holdtime	2 つの連続した SPF 計算の間の待機時間（秒）で、有効な値は 1 ～ 65,535 秒です。

デフォルト

デフォルトは次のとおりです。

- *delay* は 5 秒です。
- *holdtime* は 10 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

OSPF プロトコルによるトポロジ変更受信と計算開始との間の遅延時間、および 2 つの連続した SPF 計算での待機時間を設定するには、**timers spf** コマンドを使用します。デフォルトのタイマー値に戻すには、**no timers spf** コマンドを使用します。

例

次の例では、SPF 計算の遅延時間に 10 秒、SPF 計算の待機時間に 20 秒を設定します。

```
hostname(config-router)# timers spf 10 20
hostname(config-router)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードに入ります。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。
timers lsa-group-pacing	OSPF リンクステート アドバタイズメント（LSA）が収集されてリフレッシュ、チェックサム、またはエージングされる間隔を指定します。

title

WebVPN ユーザがセキュリティ アプライアンスに接続するときに WebVPN のページに表示されるタイトルをカスタマイズするには、webvpn カスタマイゼーション モードで **title** コマンドを使用します。

title {**text** | **style**} *value*

[**no**] **title** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのテキストは「WebVPN Service」です。

デフォルトのタイトルのスタイルは次のとおりです。

background-color:white;color:maroon;border-bottom:5px groove #669999;font-size:larger;
vertical-align:middle;text-align:left;font-weight:bold

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

タイトルを入れない場合は、*value* の引数なしで **title text** コマンドを使用します。

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、タイトルを「Cisco WebVPN Service」というテキストでカスタマイズします。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# title text Cisco WebVPN Service
```

関連コマンド

コマンド	説明
logo	WebVPN ページのロゴをカスタマイズします。
page style	Cascading Style Sheet（CSS）パラメータを使用して WebVPN ページをカスタマイズします。

tos

SLA オペレーションの要求パケットの IP ヘッダーでタイプ オブ サービス（ToS）バイトを定義するには、SLS モニタ プロトコル コンフィギュレーション モードで **tos** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

tos *number*

no tos

シンタックスの説明

number	IP ヘッダーで使用するサービス タイプの値。有効な値は 0 ～ 255 です。

デフォルト

デフォルトは 0 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ プロトコル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このフィールドには、遅延、優先度、信頼性などの情報が入っています。ネットワークにある他のルータのポリシー ルーティングや、専用アクセス レートなどの機能で使用されます。

例

次の例では、ICMP エコー要求 / 応答時間プローブ オペレーションを使用する、ID が 123 の SLA オペレーションを設定しています。また、エコー要求パケットのペイロード サイズを 48 バイト、SLA オペレーション中に送信するエコー要求の数を 5、タイプ オブ サービス バイトを 80 に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# num-packets 5
hostname(config-sla-monitor-echo)# request-data-size 48
hostname(config-sla-monitor-echo)# tos 80
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA オペレーション中に送信する要求パケットの数を指定します。
request-data-size	要求パケットのペイロードのサイズを指定します。
sla monitor	SLA 監視オペレーションを定義します。
type echo	SLA オペレーションをエコー応答時間プローブ オペレーションとして設定します。

traceroute

パケットが宛先に到達するまでにたどるルートを調査するには、**traceroute** コマンドを使用します。

traceroute *destination_ip* | *hostname* [***source*** *source_ip* | *source-interface*] [***numeric***] [***timeout*** *timeout_value*] [***probe*** *probe_num*] [***ttl*** *min_ttl max_ttl*] [***port*** *port_value*] [***use-icmp***]

シンタックスの説明

destination_ip	traceroute の宛先 IP アドレスを指定します。
hostname	ルートをトレースする先のホストのホスト名。ホスト名を指定する場合は、***name*** コマンドを使用して定義するか、DNS サーバを設定して traceroute がホスト名を IP アドレスに名前解決できるようにします。www.example.com などの DNS ドメイン名がサポートされています。
source	トレース パケットの送信元となる IP アドレスまたはインターフェイスを指定します。
source_ip	パケット トレースの送信元の IP アドレスを指定します。この IP アドレスは、送信元インターフェイスの IP アドレスでなければなりません。透過モードでは、セキュリティ アプライアンスの管理 IP アドレスを指定する必要があります。
source_interface	パケット トレースの送信元インターフェイスを指定します。指定した場合は、送信元のインターフェイスの IP アドレスが使用されます。
numeric	このコマンドの出力に、中間のゲートウェイの IP アドレスだけが表示されるようにします。このキーワードを指定しないと、トレース中に到達したゲートウェイのホスト名が検索されます。
timeout	使用するタイムアウト値を指定します。
timeout_value	接続がタイムアウトになるまでに、応答を待つ時間を秒単位で指定します。デフォルトは 3 秒です。
probe *probe_num*	TTL の各レベルで送信するプローブの数。デフォルトは 3 です。
ttl	プローブで使用する Time To Live（TTL; 存続可能時間）の範囲を指定するキーワード。
min_ttl	最初のプローブの TTL の値。デフォルトは 1 ですが、高い値に設定して、既知のホップが表示されないようにすることもできます。
max-ttl	使用できる TTL の最大値。デフォルトは 30 です。トレースするパケットが宛先に到達するか、TTL がこの値になるとコマンドは終了します。
port *port_value*	User Datagram Protocol（UDP; ユーザ データグラム プロトコル）プローブ メッセージで使用する宛先ポート。デフォルトは 33434 です。
use-icmp	UDP プローブ パケットではなく、ICMP プローブ パケットを使用することを指定します。

デフォルト

このコマンドにデフォルト設定はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権モード	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

traceroute コマンドは、送信された各プローブの結果を出力します。出力の各行が 1 つの TTL 値に対応します（昇順）。次の表に、このコマンドの出力で使われる記号を示します。

出力に示される記号	説明
*	タイムアウトの期間内にプローブへの応答を受信しませんでした。
nn msec	各ノードで、指定した数のプローブのラウンドトリップにかかる時間（ミリ秒）。
!N.	ICMP ネットワークに到達できません。
!H	ICMP のホストに到達できません。
!P	ICMP プロトコルが見つかりません。
!A	ICMP が設定によって禁止されています。
?	ICMP の原因不明のエラーが発生しました。

例

次の例では、traceroute コマンドで宛先 IP アドレスを指定した場合の出力を示します。

```
hostname# traceroute 209.165.200.225

Tracing the route to 209.165.200.225

 1  10.83.194.1 0 msec 10 msec 0 msec
 2  10.83.193.65 0 msec 0 msec 0 msec
 3  10.88.193.101 0 msec 10 msec 0 msec
 4  10.88.193.97 0 msec 0 msec 10 msec
 5  10.88.239.9 0 msec 10 msec 0 msec
 6  10.88.238.65 10 msec 10 msec 0 msec
 7 172.16.7.221 70 msec 70 msec 80 msec
 8 209.165.200.225 70 msec 70 msec 70 msec
```

関連コマンド

コマンド	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが何も指定されていない場合は、キャプチャのコンフィギュレーションを表示します。
packet-tracer	パケットのトレース機能をイネーブルにします。

track rtr

SLA オペレーションの到達可能性を調べるには、グローバル コンフィギュレーション モードで **track rtr** コマンドを使用します。SLA のトラッキングを削除するには、このコマンドの **no** 形式を使用します。

track *track-id* ***rtr*** *sla-id* ***reachabilitity***

no track *track-id* ***rtr*** *sla-id* ***reachabilitity***

シンタックスの説明

reachability	オブジェクトの到達可能性を追跡することを指定します。
sla-id	トラッキング エントリで使用する SLA の ID。
track-id	トラッキング エントリのオブジェクト ID を作成します。有効な値は 1 ～ 500 です。

デフォルト

SLA のトラッキングはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

track rtr コマンドで、トラッキング エントリのオブジェクト ID を作成し、そのエントリで使用する SLA を指定します。

SLA オペレーションごとに、オペレーション戻りコード値が保持されます。この値は、トラッキング プロセスで解釈されます。OK、Over Threshold、および他のいくつかの戻りコードがあります。表 32-1 に、戻りコードが意味するオブジェクトの到達可能性の状態を示します。

表 32-1　SLA トラッキングの戻りコード

トラッキング	戻りコード	トラッキング状態
到達可能性	OK または Over Threshold	アップ
	その他のコード	ダウン

例

次の例では、ID が 123 の SLA オペレーションを設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
route	スタティック ルートを設定します。
sla monitor	SLA 監視オペレーションを定義します。

traffic-non-sip

既知の SIP シグナリング ポートを使用して SIP 以外のトラフィックを許可するには、パラメータ コンフィギュレーション モードで **traffic-non-sip** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

traffic-non-sip

no traffic-non-sip

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、SIP 検査ポリシー マップで、既知の SIP シグナリング ポートを使用した SIP 以外のトラフィックを許可する方法を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# traffic-non-sip
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

transfer-encoding

転送符号化タイプを指定することで HTTP トラフィックを制限するには、HTTP マップ コンフィギュレーション モードで **transfer-encoding** コマンドを使用します。このモードには、**http-map** コマンドを使用してアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

transfer-encoding type {***chunked*** | ***compress*** | ***deflate*** | ***gzip*** | ***identity*** | ***default***} ***action*** {***allow*** | ***reset*** | ***drop***} [***log***]

no transfer-encoding type {***chunked*** | ***compress*** | ***deflate*** | ***gzip*** | ***identity*** | ***default***} ***action*** {***allow*** | ***reset*** | ***drop***} [***log***]

シンタックスの説明

action	指定した転送符号化タイプを使用している接続が検出された場合に実行されるアクションを指定します。
allow	メッセージを許可します。
chunked	メッセージ本文が一連のチャンクとして転送される転送符号化タイプを識別します。
compress	UNIX ファイル圧縮を使用してメッセージ本文が転送される転送符号化タイプを識別します。
default	サポートされている要求メソッドがトラフィックに含まれていて、そのメソッドが設定済みリストに記載されていない場合に、セキュリティ アプライアンスが実行するデフォルト アクションを指定します。
deflate	zlib 形式（RFC 1950）およびデフレート圧縮（RFC 1951）を使用して、メッセージ本文が転送される転送符号化タイプを識別します。
drop	接続を終了します。
gzip	GNU zip（RFC 1952）を使用してメッセージ本文が転送される転送符号化タイプを識別します。
identity	転送符号化が実行されていないメッセージ本文の接続を識別します。
log	（オプション）syslog を生成します。
reset	TCP リセット メッセージをクライアントまたはサーバに送信します。
type	HTTP アプリケーション検査を通して制御される転送符号化タイプを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。コマンドがイネーブルで、サポートされる転送符号化タイプが指定されていない場合、デフォルトのアクションは接続をロギングなしで許可します。デフォルト アクションを変更するには、**default** キーワードを使用して別のデフォルト アクションを指定します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
HTTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

transfer-encoding コマンドをイネーブルにする場合、セキュリティ アプライアンスは、サポートおよび設定された各転送符号化タイプの HTTP 接続に、指定したアクションを適用します。

セキュリティ アプライアンスは、設定したリストの転送符号化タイプに一致しないすべてのトラフィックに、**default** アクションを適用します。事前設定済みの **default** アクションでは、接続をロギングなしで **allow** します。

たとえば、事前設定済みのデフォルトのアクションが与えられ、**drop** および **log** のアクションを伴う符号化タイプを 1 つ以上指定する場合、セキュリティ アプライアンスは設定済みの符号化タイプを含む接続をドロップして、各接続のログを記録し、サポートされるその他の符号化タイプに対してすべての接続を許可します。

より厳しいポリシーを設定する場合は、デフォルト アクションを **drop**（または **reset**）および **log** に変更します（イベントをログに記録する場合）。次に、**allow** アクションを使用して、許容される符号化タイプをそれぞれ設定します。

適用する各設定に対して、**transfer-encoding** コマンドを 1 度入力します。**transfer-encoding** コマンドの 1 つのインスタンスはデフォルト アクションの変更に使用し、もう 1 つのインスタンスは設定済みの転送符号化タイプのリストに各符号化タイプを追加するために使用します。

このコマンドの **no** 形式を使用して、設定済みのアプリケーション タイプのリストからアプリケーション カテゴリを削除する場合は、アプリケーション カテゴリのキーワードの後ろに入力した文字がすべて無視されます。

例

次の例では、事前設定済みのデフォルトを使用して、緩やかなポリシーを指定しています。サポートされているすべてのアプリケーション タイプを、個別に拒否されていない限り許可します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# transfer-encoding gzip drop log
hostname(config-http-map)#
```

この場合、GNU zip を使用した接続だけがドロップされ、イベントのログが記録されます。

次の例では、特に許可されていない任意の符号化タイプに対し、接続をリセットしてイベントをログに記録するようにデフォルト アクションを変更した厳しいポリシーを指定します。

```
hostname(config)# http-map inbound_http
hostname(config-http-map)# port-misuse default action reset log
hostname(config-http-map)# port-misuse identity allow
hostname(config-http-map)#
```

この場合、転送符号化を使用していない接続だけが許可されます。サポートされるその他の符号化タイプの HTTP トラフィックを受信した場合、セキュリティ アプライアンスは接続をリセットして、syslog エントリを作成します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用する先のトラフィック クラスを定義します。
debug appfw	高度な HTTP 検査に関連付けられているトラフィックに関する詳細情報を表示します。
http-map	高度な HTTP 検査を設定するための HTTP マップを定義します。
inspect http	アプリケーション検査用に特定の HTTP マップを適用します。
policy-map	クラス マップを特定のセキュリティ アクションに関連付けます。

trust-point

IKE ピアに送信される証明書を識別するトラストポイントの名前を指定するには、トンネル グループ IPSec アトリビュート モードで **trust-point** コマンドを使用します。トラストポイント仕様を削除するには、このコマンドの ***no*** 形式を使用します。

trust-point *trust-point-name*

no trust-point *trust-point-name*

シンタックスの説明

trust-point-name	使用するトラストポイントの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
トンネル グループ IPSec アトリビュート	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

このアトリビュートは、すべての IPSec トンネル グループ タイプに適用できます。

例

次の例は config-ipsec コンフィギュレーション モードで入力され、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループの IKE ペアに送られる証明書を識別するためのトラストポイントを設定します。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# trust-point mytrustpoint
hostname(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec アトリビュートを設定します。

tsig enforced

TSIG リソース レコードを必須とするには、パラメータ コンフィギュレーション モードで **tsig enforced** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

tsig enforced action {**drop** [**log**] | **log**}

no tsig enforced [**action** {**drop** [**log**] | **log**}]

シンタックスの説明

drop	TSIG が存在しない場合に、パケットをドロップします。
log	システム メッセージ ログを生成します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、DNS トランザクションにおいて、TSIG の監視をイネーブルにし、TSIG が必ず存在することを要求します。

例

次の例では、DNS 検査ポリシー マップで TSIG 強制をイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# tsig enforced action log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

ttl-evasion-protection

Time-To-Live 回避保護をディセーブルにするには、tcp マップ コンフィギュレーション モードで **ttl-evasion-protection** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

ttl-evasion-protection

no ttl-evasion-protection

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

セキュリティ アプライアンスが提供する TTL 回避保護は、デフォルトでイネーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **ttl-evasion-protection** コマンドを使用して、セキュリティ ポリシーを回避しようとした攻撃を防止します。

たとえば、攻撃者は非常に短い TTL を持つポリシーを通過するパケットを送信できます。TTL が 0 になると、セキュリティ アプライアンスとエンドポイントの間のルータはパケットをドロップします。攻撃者は、この時点で長い TTL を持つ悪意のあるパケットを送信できます。セキュリティ アプライアンスはこのパケットを再送と見なし、通過させます。ただし、エンドポイントのホストでは、このパケットが攻撃者より受信した最初のパケットとなります。このような場合、攻撃者は攻撃を防ぐセキュリティがなくても成功します。この機能をイネーブルにすると、このような攻撃を防ぐことができます。

例

次の例では、ネットワーク 10.0.0.0 から 20.0.0.0 へのフローで TTL 回避保護をディセーブルにする方法を示します。

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# ttl-evasion-protection disable
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

tunnel-group

IPSec および WebVPN トンネルに対する接続固有のレコードのデータベースを作成し、管理するには、グローバル コンフィギュレーション モードで **tunnel-group** コマンドを使用します。トンネル グループを削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* ***type*** *type*

no tunnel-group *name*

シンタックスの説明

name	トンネル グループの名前を指定します。これには、任意の文字列を選択できます。名前が IP アドレスの場合は、通常、ピアの IP アドレスとなります。
type	トンネル グループのタイプを次のように指定します。 ipsec-ra：IPSec リモートアクセス ipsec-l2l：IPsec LAN-to-LAN webvpn：WebVPN

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	注を参照してください。	•	—	—

（注） tunnel-group コマンドは、透過ファイアウォール モードで使用して、LAN-to-LAN トンネル グループのコンフィギュレーションを許可できますが、リモートアクセス グループまたは WebVPN グループは許可できません。また、LAN-to-LAN で使用できるすべての tunnel-group コマンドは、透過ファイアウォール モードでも使用できます。

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。
7.1	webvpn タイプが追加されました。

使用上のガイドライン

セキュリティ アプライアンスには、次のデフォルト トンネル グループがあります。

- DefaultRAGroup：デフォルトの IPSec リモート アクセス トンネル グループ
- DefaultL2LGroup：デフォルトの IPSec LAN-to-LAN トンネル グループ
- DefaultWEBVPNGroup：デフォルトの WebVPN トンネル グループ

これらのグループの変更はできますが、削除はできません。セキュリティ アプライアンスは、トンネル ネゴシエーション中に特定のトンネル グループが識別されない場合、これらのグループを使用して、リモートアクセスおよび LAN-to-LAN トンネル グループに対してデフォルトのトンネル パラメータを設定します。

tunnel-group コマンドを入力した後､特定のトンネル グループに特定のアトリビュートを設定するには、次のコマンドから適切なものを入力します。それぞれのコマンドは、トンネル グループ アトリビュートを設定するためのコンフィギュレーション モードに入ります。

- **tunnel-group general-attributes**
- **tunnel-group ipsec-attributes**
- **tunnel-group webvpn-attributes**
- **tunnel-group ppp-attributes**

例

次の例は、グローバル コンフィギュレーション モードで入力されています。最初のコマンドは、IPSec リモート アクセス トンネル グループを設定します。グループ名は「group1」です。

```
hostname(config)# tunnel-group group1 type ipsec-ra
hostname(config)#
```

次の例では、IPSec LAN-to-LAN トンネル グループを設定します。名前は、LAN-to-LAN ピアの IP アドレスです。

```
hostname(config)# tunnel-group 209.165.200.225 type ipsec-l2l
hostname(config)#
```

次の例では、「group1」という名前の webvpn トンネル グループを設定する tunnel-group コマンドを示します。このコマンドはグローバル コンフィギュレーション モードで入力します。

```
hostname(config)# tunnel-group group1 type webvpn
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループを消去します。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	一般トンネル グループ アトリビュートを設定する config-general モードに入ります。
tunnel-group ipsec-attributes	IPSec トンネル グループ アトリビュートを設定する config-ipsec モードに入ります。
tunnel-group ppp-attributes	L2TP 接続の PPP を設定する config-ppp モードに入ります。
tunnel-group webvpn-attributes	WebVPN トンネル グループ アトリビュートを設定する config-webvpn モードに入ります。

tunnel-group general-attributes

一般アトリビュート コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **tunnel-group general-attributes** コマンドを使用します。このモードは、サポートされるすべてのトンネリング プロトコルに共通の値を設定するために使用されます。

一般アトリビュートをすべて削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* ***general-attributes***

no tunnel-group *name* ***general*-attributes**

シンタックスの説明

***general*-attributes**	このトンネル グループのアトリビュートを指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。
7.1.1	さまざまなアトリビュートが他のトンネル グループ タイプから一般トンネル グループ アトリビュート リストに移され、トンネル グループ一般アトリビュート モードのプロンプトが変更されました。

使用上のガイドライン

次の表は、このグループに属しているコマンドと、コマンドを設定できるトンネル グループのタイプを示しています。

一般アトリビュート	設定できるトンネル グループのタイプ
accounting-server-group	IPSec RA、IPSec L2L、WebVPN
address-pool	IPSec RA
authentication-server-group	IPSec RA、WebVPN
authorization-dn-attributes	IPSec RA、WebVPN
authorization-required	WebVPN
authorization-server-group	IPSec RA
default-group-policy	IPSec RA、IPSec L2L
dhcp-server	IPSec RA
override-account-disabled	IPSec RA、WebVPN
password-management	IPSec RA、WebVPN

一般アトリビュート	設定できるトンネル グループのタイプ
strip-group	IPSec RA、WebVPN
strip-realm	IPSec RA、WebVPN

例

次の例はグローバル コンフィギュレーション モードで入力され、LAN-to-LAN ピアの IP アドレスを使用して IPSec LAN-to-LAN 接続用のトンネル グループを作成してから一般コンフィギュレーション　モードに入り、一般アトリビュートを設定します。トンネル　グループの名前は、209.165.200.225 です。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 general
hostname(config-tunnel-general)#
```

次の例はグローバル コンフィギュレーション モードで入力され、IPSec リモートアクセス接続用の「remotegrp」という名前のトンネル グループを作成してから一般コンフィギュレーション モードに入り、「remotegrp」という名前のトンネル グループ用の一般アトリビュートを設定します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp general
hostname(config-tunnel-general)
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続に固有なレコードのデータベースを作成および管理します。

tunnel-group ipsec-attributes

ipsec アトリビュート コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **tunnel-group ipsec-attributes** コマンドを使用します。このモードは、IPSec トンネリング プロトコルに限定される値を設定するために使用されます。

IPSec アトリビュートをすべて削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* ***ipsec-attributes***

no tunnel-group *name* ***ipsec*-attributes**

シンタックスの説明

***ipsec*-attributes**	このトンネル グループのアトリビュートを指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。
7.1.1	さまざまな IPSec トンネル グループ アトリビュートが一般トンネル グループ アトリビュート リストに移され、トンネル グループ ipsec アトリビュート モードのプロンプトが変更されました。

使用上のガイドライン

次のコマンドは、このグループに所属しています。

IPSec アトリビュート	設定できるトンネル グループのタイプ
chain	IPSec RA、IPSec L2L
client-update	IPSec RA
isakmp keepalive	IPSec RA
peer-id-validate	IPSec RA、IPSec L2L
pre-shared-key	IPSec RA、IPSec L2L
radius-with-expiry	IPSec RA
trust-point	IPSec RA、IPSec L2L

例

次の例はグローバル コンフィギュレーションで入力され、remotegrp という名前の IPSec リモート アクセス トンネル グループ用のトンネル グループを作成してから、IPSec グループ アトリビュートを指定します。

```
hostname(config)# tunnel-group remotegrp type ipsec_ra
hostname(config)# tunnel-group remotegrp ipsec-attributes
hostname(config-tunnel-ipsec)
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続に固有なレコードのデータベースを作成および管理します。

tunnel-group ppp-attributes

PPP アトリビュート コンフィギュレーション モードに入り、L2TP over IPSec 接続で使用する PPP を設定するには、グローバル コンフィギュレーション モードで **tunnel-group ppp-attributes** コマンドを使用します。

PPP アトリビュートをすべて削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* ***ppp-attributes***

no tunnel-group *name* ***ppp*-attributes**

シンタックスの説明

name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2.1	このコマンドが導入されました。

使用上のガイドライン

PPP 設定は、Layer 2 Tunneling Protocol（L2TP）で使用されます。これは、リモート クライアントがパブリック IP ネットワークにダイヤルアップ接続して、企業のプライベート ネットワーク サーバと安全に通信できるようにする VPN トンネリング プロトコルです。L2TP は、クライアント / サーバ モデルに基づいており、PPP over UDP（ポート 1701）を使用してデータをトンネリングします。

次の表は、このグループに属しているコマンドと、コマンドを設定できるトンネル グループのタイプを示しています。

PPPoE アトリビュート	設定できるトンネル グループのタイプ
authentication chap	PPPoE
authentication eap-proxy	PPPoE
authentication ms-chap-v1	PPPoE
authentication ms-chap-v2	PPPoE
authentication-pap	PPPoE

例

次の例では、*telecommuters* というトンネル グループを作成し、PPP アトリビュート コンフィギュレーション モードに入ります。

```
hostname(config)# tunnel-group telecommuters type pppoe
hostname(config)# tunnel-group telecommuters ppp-attributes
hostname(tunnel-group-ppp)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続に固有なレコードのデータベースを作成および管理します。

tunnel-group webvpn-attributes

WebVPN アトリビュート コンフィギュレーション モードに入るには、グローバル コンフィギュレーション モードで **tunnel-group webvpn-attributes** コマンドを使用します。このモードは WebVPN トンネリングに共通した値を設定します。

WebVPN アトリビュートをすべて削除するには、このコマンドの **no** 形式を使用します。

tunnel-group *name* ***webvpn-attributes***

no tunnel-group *name* ***webvpn*-attributes**

シンタックスの説明

***webvpn*-attributes**	このトンネル グループの WebVPN アトリビュートを指定します。
name	トンネル グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが導入されました。

使用上のガイドライン

一般アトリビュートに加えて、WebVPN 接続に固有の次のアトリビュートを WebVPN アトリビュート モードで設定できます。

- authentication
- customization
- dns-group
- group-alias
- group-url
- hic-fail-group-policy
- nbns-server-name

これらのアトリビュートの設定に関する詳細については、個々のコマンドの説明を参照してください。

例

次の例はグローバル コンフィギュレーション モードで入力され、LAN-to-LAN ピアの IP アドレスを使用して WebVPN 接続用のトンネル グループを作成してから webvpn コンフィギュレーション モードに入り、WebVPN アトリビュートを設定します。トンネル グループの名前は、209.165.200.225 です。

```
hostname(config)# tunnel-group 209.165.200.225 type webvpn
hostname(config)# tunnel-group 209.165.200.225 webvpn-attributes
hostname(config-tunnel-webvpn)#
```

次の例はグローバル コンフィギュレーション モードで入力され、WebVPN 接続用の「remotegrp」という名前のトンネル グループを作成してから webvpn コンフィギュレーション モードに入り、「remotegrp」という名前のトンネル グループ用の WebVPN アトリビュートを設定します。

```
hostname(config)# tunnel-group remotegrp type webvpn
hostname(config)# tunnel-group remotegrp webvpn-attributes
hostname(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	トンネル グループ データベース全体、または特定のトンネル グループのみを消去します。
show running-config tunnel-group	指定したトンネル グループまたはすべてのトンネル グループの現在の実行トンネル グループ コンフィギュレーションを表示します。
tunnel-group	IPSec および WebVPN トンネルの接続に固有なレコードのデータベースを作成および管理します。

tunnel-group-map default-group

tunnel-group-map default-group コマンドは、他の設定済みの方法でトンネル グループ名を判別できなかった場合に、使用するデフォルトのトンネル グループ名を指定します。

tunnel-group-map を削除するには、このコマンドの **no** 形式を使用します。

tunnel-group-map [*rule-index*] **default-group** *tunnel-group-name*

no *tunnel-group-map*

シンタックスの説明

default-group *tunnel-group-name*	他の設定済みメソッドで名前を取得できない場合に使用されるデフォルトのトンネル グループを指定します。*tunnel-group name* は、既存である必要があります。
rule index	オプション。**crypto ca certificate map** コマンドで指定したパラメータを参照します。値は、1 ～ 65535 です。

デフォルト

tunnel-group-map default-group のデフォルト値は、DefaultRAGroup です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tunnel-group-map コマンドは、証明書ベースの IKE セッションをトンネル グループにマップするポリシーと規則を設定します。**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けるには、グローバル コンフィギュレーション モードで **tunnel-group-map** コマンドを使用します。各呼び出しが一意であり、マップ インデックスを 2 回以上参照しない限り、このコマンドを複数回実行できます。

crypto ca certificate map コマンドは、証明書マッピング規則の優先順位付きリストを管理します。定義できるマップは 1 つのみです。ただし、このマップで 65,535 個までの規則を保持できます。詳細については、**crypto ca certificate map** コマンドのマニュアルを参照してください。

証明書からトンネル グループ名を取得する処理は、トンネル グループに関連付けられていない証明書マップのエントリを無視します（どのマップ規則もこのコマンドでは識別されません）。

例

次の例はグローバル コンフィギュレーション モードで入力され、他の設定済みメソッドで名前を取得できない場合に使用されるデフォルトのトンネル グループを指定します。使用するトンネル グループの名前は、group1 です。

```
hostname(config)# tunnel-group-map default-group group1
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	crypto ca 証明書マップ モードに入ります。
subject-name（暗号 CA 証明書マップ）	規則エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map enable	証明書ベースの IKE セッションをトンネル グループにマップするポリシーと規則を設定します。

tunnel-group-map enable

tunnel-group-map enable コマンドは、証明書ベースの IKE セッションをトンネル グループにマップするポリシーと規則を設定します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

tunnel-group-map [*rule-index*] ***enable*** *policy*

no *tunnel-group-map enable* [*rule-index*]

シンタックスの説明

policy	証明書からトンネル グループ名を取得するポリシーを指定します。*policy* は、次のいずれかになります。 **ike-id**：トンネル グループが規則の検索に基づいて決定されない、または ou から取得されない場合、証明書ベースの IKE セッションはフェーズ 1 IKE ID のコンテンツに基づいたトンネル グループにマップされることを示します。 **ou**：トンネル グループが規則の検索に基づいて決定されない場合、サブジェクト認定者名（DN）の組織ユニット（OU）の値を使用することを示します。 **peer-ip**：トンネル グループが規則の検索に基づいて決定されないか、ou または ike-id メソッドから取得されない場合、確立されたピア IP アドレスを使用することを示します。 **rules**：証明書ベースの IKE セッションは、このコマンドにより設定された証明書マップ結合に基づいてトンネル グループにマップされることを示します。
rule index	オプション。**crypto ca certificate map** コマンドで指定したパラメータを参照します。値は、1 ～ 65535 です。

デフォルト

tunnel-group-map コマンドのデフォルト値は、**enable ou** で、**default-group** は、DefaultRAGroup に設定されています。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン　**crypto ca certificate map** コマンドは、証明書マッピング規則の優先順位付きリストを管理します。定義できるマップは 1 つのみです。ただし、このマップで 65,535 個までの規則を保持できます。詳細については、**crypto ca certificate map** コマンドのマニュアルを参照してください。

例　次の例では、フェーズ 1 IKE ID のコンテンツに基づいて、トンネル グループへの証明書ベースの IKE セッションのマッピングをイネーブルにします。

```
hostname(config)# tunnel-group-map enable ike-id
hostname(config)#
```

次の例では、確立されたピアの IP アドレスに基づいて、トンネル グループへの証明書ベースの IKE セッションのマッピングをイネーブルにします。

```
hostname(config)# tunnel-group-map enable peer-ip
hostname(config)#
```

次の例では、サブジェクト認定者名（DN）の組織ユニット（OU）に基づいて証明書ベースの IKE セッションのマッピングをイネーブルにします。

```
hostname(config)# tunnel-group-map enable ou
hostname(config)#
```

次の例では、確立した規則に基づいて、証明書ベースの IKE セッションのマッピングをイネーブルにします。

```
hostname(config)# tunnel-group-map enable rules
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	CA 証明書マップ モードに入ります。
subject-name（暗号 CA 証明書マップ）	規則エントリ文字列との比較対象となる、CA 証明書に含まれている DN を指定します。
tunnel-group-map default-group	既存のトンネル グループ名をデフォルト トンネル グループとして指定します。

tunnel-limit

セキュリティ アプライアンスでアクティブになることを許可されている GTP トンネルの最大数を指定するには、GTP マップ コンフィギュレーション モードで **tunnel limit** コマンドを使用します。このモードには、**gtp-map** コマンドを使用してアクセスできます。トンネル制限をデフォルトに戻すには、**no** を使用します。

tunnel-limit *max_tunnels*

no tunnel-limit *max_tunnels*

シンタックスの説明

max_tunnels	これは、トンネルの許容最大数です。グローバルなトンネル制限全体の範囲は、1 ～ 4,294,967,295 です。

デフォルト

トンネル制限のデフォルトは 500 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
GTP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドで指定されたトンネル数に到達すると、新しい要求はドロップされます。

例

次の例では、GTP トラフィックに最大 10,000 トンネルを指定します。

```
hostname(config)# gtp-map qtp-policy
hostname(config-gtpmap)# tunnel-limit 10000
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバル GTP 統計情報を消去します。
debug gtp	GTP 検査に関する詳細情報を表示します。
gtp-map	GTP マップを定義し、GTP マップ コンフィギュレーション モードをイネーブルにします。
inspect gtp	アプリケーション検査に使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

tx-ring-limit

プライオリティ キューの項目数を指定するには、プライオリティ キュー モードで **tx-ring-limit** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

tx-ring-limit *number-of-packets*

no tx-ring-limit *number-of-packets*

シンタックスの説明

number-of-packets	イーサネット送信ドライバが許容できる低遅延パケットまたは標準の優先順位のパケットの最大数を指定します。このパケットの処理が終わると、イーサネット送信ドライバは輻輳が解消するまで、インターフェイス上のパケットをバッファしているキューの処理に戻ります。**tx-ring-limit** 値の範囲は、PIX プラットフォームでは 3 ～ 128 パケット、ASA プラットフォームでは 3 ～ 256 パケットです。

デフォルト

デフォルトの **tx-ring-limit** は、128 パケットです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
プライオリティ キュー	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、2 つのクラスのトラフィックを許可します。1 つは優先順位が高く、遅延に影響されやすいトラフィック（音声およびビデオなど）用の Low-Latency Queuing（LLQ; 低遅延キューイング）で、もう 1 つは、それ以外のすべてのトラフィック用のベストエフォート（デフォルト）です。セキュリティ アプライアンスは、優先トラフィックを認識し、適切な Quality of Service（QoS; サービス品質）ポリシーを適用します。プライオリティ キューのサイズと項目数を設定することで、トラフィック フローを微調整できます。

プライオリティ キューイングを有効にするには、**priority-queue** コマンドを使用して、インターフェイスのプライオリティ キューをあらかじめ作成しておく必要があります。1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドを使用すると、プライオリティ キュー モードに入ります。モードはプロンプトに表示されます。プライオリティ キュー モードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびバッファに入れることのできる両タイプ（優先またはベストエフォート）のパケット数を設定できます（**queue-limit** コマンド）。queue-limit の数を超えると、以後のパケットはドロップされます。

（注） インターフェイスでプライオリティ キューイングをイネーブルにするには、**priority-queue** コマンドを設定する必要があります。

指定する tx-ring-limit および queue-limit は、優先順位の高い低遅延キューとベストエフォート キューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両タイプのパケットの数です。このパケットの処理が終わると、ドライバは輻輳が解消するまで、インターフェイスの先頭にある、パケットをバッファしているキューの処理に戻ります。一般に、これらの 2 つのパラメータを調整することによって、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これが「テール ドロップ」です。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファ サイズを大きくします。

（注） **queue-limit** コマンドと **tx-ring-limit** コマンドの値の範囲の上限は、実行時に動的に決まります。この上限値を表示するには、コマンドラインで **help** または **?** と入力します。主な決定要素は、キューのサポートに必要となるメモリと、デバイス上で使用可能なメモリの量です。**queue-limit** 値の範囲は、0 ～ 2,048 パケットです。**tx-ring-limit** 値の範囲は、PIX プラットフォームでは 3 ～ 128 パケット、ASA プラットフォームでは 3 ～ 256 パケットです。

例

次の例では、test というインターフェイスのプライオリティ キューを設定して、キューの上限を 2048 パケット、送信キューの上限を 256 パケットと指定しています。

```
hostname(config)# priority-queue test
hostname(priority-queue)# queue-limit 2048
hostname(priority-queue)# tx-ring-limit 256
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。
queue-limit	プライオリティ キューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。
show priority-queue statistics	指定したインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、このコマンドは現在のすべての **priority-queue**、**queue-limit**、および **tx-ring-limit** コマンドのコンフィギュレーション値を表示します。

type echo

SLA オペレーションをエコー応答時間プローブ オペレーションとして設定するには、SLA モニタ コンフィギュレーション モードで **type echo** コマンドを使用します。このタイプのオペレーションを SLA コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

type echo *protocol ipIcmpEcho* *target* interface *if-name*

no type echo *protocol ipIcmpEcho* *target* interface *if-name*

シンタックスの説明

interface *if-name*	**nameif** コマンドで指定したように、エコー要求パケットを送信するインターフェイスの名前を指定します。インターフェイスの送信元アドレスが、エコー要求パケットで送信元アドレスとして使用されます。
protocol	プロトコルを指定するキーワード。***ipIcmpEcho*** という値しか指定できません。この値は、エコー オペレーションで IP/ICMP エコー要求を使用することを指定します。
target	監視するオブジェクトの IP アドレスまたはホスト名。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
SLA モニタ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ICMP パケットのペイロードのデフォルト サイズは 28 バイトです。ICMP パケットの合計サイズは 64 バイトになります。ペイロードのサイズを変更するには、**request-data-size** コマンドを使用します。

例

次の例では、ICMP エコー要求 / 応答時間プローブ オペレーションを使用する、ID が 123 の SLA オペレーションを設定しています。ID が 1 のトラッキング エントリを作成し、SLA の到達可能性を追跡します。SLA オペレーションの頻度を 10 秒、しきい値を 2,500 ミリ秒、タイムアウト値を 4,000 ミリ秒に設定しています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# threshold 2500
hostname(config-sla-monitor-echo)# timeout 4000
hostname(config-sla-monitor-echo)# frequency 10
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA オペレーション中に送信する要求パケットの数を指定します。
request-data-size	SLA オペレーションの要求パケットのペイロードのサイズを指定します。
sla monitor	SLA 監視オペレーションを定義します。

CHAPTER 33

urgent-flag コマンド～ zonelabs integrity ssl-client-authentication コマンド

urgent-flag

TCP ノーマライザを通して URG ポインタを許可または消去するには、tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

urgent-flag {**allow** | **clear**}

no urgent-flag {**allow** | **clear**}

シンタックスの説明

allow	TCP ノーマライザを通して URG ポインタを許可します。
clear	TCP ノーマライザを通して URG ポインタを消去します。

デフォルト

緊急フラグおよび緊急オフセットはデフォルトで消去されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **urgent-flag** コマンドを使用して、緊急フラグを許可します。

URG フラグは、ストリーム内の他のデータよりも高い優先順位の情報を含むパケットを示すために使用されます。TCP RFC は、URG フラグの正確な解釈を明確化していません。したがって、エンド システムは緊急オフセットをさまざまな方法で処理します。このため、エンド システムが攻撃を受け易くなります。デフォルトの動作は、URG フラグとオフセットを消去します。

例

次の例では、緊急フラグを許可する方法を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# urgent-flag allow
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq 513
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

uri-non-sip

Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別するには、パラメータ コンフィギュレーション モードで **uri-non-sip** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

uri-non-sip action {**mask** | **log**} [**log**}

no uri-non-sip action {**mask** | **log**} [**log**}

シンタックスの説明

mask	SIP 以外の URI をマスクします。
log	違反が発生した場合、独自または追加のログを記録することを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、SIP 検査ポリシー マップの Alert-Info ヘッダー フィールドと Call-Info ヘッダー フィールドにある SIP 以外の URI を識別する方法を示します。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# uri-non-sip action log
```

関連コマンド

コマンド	説明
class	ポリシー マップに含めるクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するための検査クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のすべてのポリシー マップ コンフィギュレーションを表示します。

url

CRL を検索するためのスタティック URL のリストを維持するには、crl 設定コンフィギュレーション モードで **url** コマンドを使用します。crl 設定コンフィギュレーション モードには、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。既存の URL を削除するには、このコマンドの **no** 形式を使用します。

url *index url*

no url *index url*

シンタックスの説明

index	リスト内の各 URL のランクを決定する 1 ～ 5 の値を指定します。セキュリティ アプライアンスは、インデックス 1 から URL を試行します。
url	CRL の検索元となる URL を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
CRL　設定コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

既存の URL は上書きできません。既存の URL を置き換えるには、まずそれを削除して、このコマンドの **no** 形式を使用します。

例

次の例では、ca-crl コンフィギュレーション モードに入り、CRL 検索用の URL のリストを作成し、維持するためにインデックス 3 を設定して、CRL の検索元となる URL https://foobin.com を設定します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# url 3 https://foobin.com
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードに入ります。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードに入ります。
policy	CRL の検索元を指定します。

url-block

フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答に使用される URL バッファを管理するには、**url-block** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

url-block block *block_buffer*

no url-block block *block_buffer*

url-block mempool-size *memory_pool_size*

no url-block mempool-size *memory_pool_size*

url-block url-size *long_url_size*

no url-block url-size *long_url_size*

シンタックスの説明

block *block_buffer*	フィルタリング サーバからのフィルタリング決定を待っている間に Web サーバの応答を保存する HTTP 応答バッファを作成します。許容される値は 1 ～ 128 です。これは、1,550 バイトのブロック数を指定します。
mempool-size *memory_pool_size*	URL バッファ メモリ プールの最大サイズ（KB）を設定します。指定できる値は、2 ～ 10,240（2 KB ～ 10,240 KB）です。
url-size *long_url_size*	バッファする各 URL の最大サイズを KB 単位で設定します。指定できる値は、Websense では 2、3、4（2 KB、3 KB、4KB）、Secure Computing では 2 または 3（2 KB または 3 KB）です。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

Websense フィルタリング サーバの場合、**url-block url-size** コマンドを使用すると、最大 4 KB の長さの URL のフィルタリングが可能です。Secure Computing の場合は、**url-block url-size** コマンドを使用して最大 3 KB の長さの URL をフィルタリングできます。Websense フィルタリング サーバおよび N2H2 フィルタリング サーバの両方の場合、**url-block block** コマンドは、URL フィルタリング サーバからの応答を待つ間の Web クライアント要求に応じて Web サーバから受信したパケットをセキュリティ アプライアンスにバッファします。この処理により、デフォルトのセキュリティ アプライアンスの動作と比較して、Web クライアントのパフォーマンスが改善されます。デフォルトの動作はパケットをドロップし、接続が許可された場合は Web サーバにパケットの再転送を要求します。

url-block block コマンドを使用し、フィルタリング サーバが接続を許可した場合、セキュリティ アプライアンスは、HTTP 応答バッファから Web クライアントにブロックを送信して、バッファからブロックを削除します。フィルタリング サーバが接続を拒否した場合、セキュリティ アプライアンスは拒否メッセージを Web クライアントに送信して、HTTP 応答バッファからブロックを削除します。

url-block block コマンドを使用して、フィルタリング サーバからフィルタリングの決定を待っている間に Web サーバの応答のバッファリングに使用するブロックの数を指定します。

url-block url-mempool-size コマンドと共に **url-block url-size** コマンドを使用して、フィルタリングする URL の最大長と、URL のバッファに割り当てる最大メモリを指定します。これらのコマンドを使用して、1,159 バイトより長く 4,096 バイト以下の URL を Websense サーバまたは Secure Computing サーバに渡します。**url-block url-size** コマンドは、1,159 バイトより長い URL をバッファに保存した後、その URL を Websense サーバまたは Secure Computing サーバに渡します（TCP パケット ストリームを使用して）。その結果、サーバがその URL へのアクセスを許可または拒否できます。

例

次の例では、1,550 バイトのブロックを 56 個、URL フィルタリング サーバからの応答のバッファリングに割り当てます。

```
hostname#(config)# url-block block 56
```

関連コマンド

コマンド	説明
clear url-block block statistics	ブロック バッファ使用状況カウンタを消去します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバからの応答を待っている間の URL バッファリングに使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

url-cache

N2H2 サーバまたは Websense サーバから受信した URL 応答の URL キャッシングをイネーブルにして、キャッシュのサイズを設定するには、グローバル コンフィギュレーション モードで **url-cache** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

url-cache {**dst** | **src_dst**} *kbytes* **[kb]**

no url-cache {**dst** | **src_dst**} *kbytes* **[kb]**

シンタックスの説明

dst	URL 宛先アドレスに基づくキャッシュ エントリ。このモードは、N2H2 サーバまたは Websense サーバ上で、すべてのユーザが同じ URL フィルタリング ポリシーを共有する場合に選択します。
size *kbytes*	キャッシュ サイズの値を 1 ～ 128 KB の範囲で指定します。
src_dst	URL 要求を発信している送信元アドレスと URL 宛先アドレスの両方に基づくキャッシュ エントリ。このモードは、N2H2 サーバまたは Websense サーバ上で、ユーザが同じ URL フィルタリング ポリシーを共有していない場合に選択します。
statistics	**statistics** オプションを使用すると、追加の URL キャッシュ統計情報、たとえば、キャッシュ ルックアップの回数やヒット率が表示されます。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

url-cache コマンドには、URL サーバから応答をキャッシュするコンフィギュレーション オプションが用意されています。

url-cache コマンドは、URL キャッシュをイネーブルにし、キャッシュ サイズを設定し、キャッシュの統計情報を表示する場合に使用します。

キャッシュによって URL アクセス特権が、セキュリティ アプライアンス上のメモリに保存されます。ホストが接続を要求すると、セキュリティ アプライアンスは要求を N2H2 または Websense サーバに転送するのではなく、まず一致するアクセス特権を URL キャッシュ内で探します。キャッシュをディセーブルにするには、**no url-cache** コマンドを使用します。

(注) N2H2 サーバまたは Websense サーバで設定を変更した場合は、**no url-cache** コマンドでキャッシュをディセーブルにした後、**url-cache** コマンドで再度イネーブルにします。

URL キャッシュを使用しても、Websense プロトコル Version 1 の Websense アカウンティング ログはアップデートされません。Websense プロトコル Version 1 を使用している場合は、Websense を実行してログを記録し、Websense アカウンティング情報を表示できるようにします。セキュリティの要求に合致する使用状況プロファイルを取得した後、**url-cache** をイネーブルにしてスループットを向上させます。Websense プロトコル Version 4 および N2H2 URL フィルタリングでは、**url-cache** コマンドの使用時にアカウンティング ログがアップデートされます。

例

次の例では、送信元アドレスと宛先アドレスに基づいて、すべての発信 HTTP 接続をキャッシュします。

```
hostname(config)# url-cache src_dst 128
```

関連コマンド

コマンド	説明
clear url-cache statistics	コンフィギュレーションから **url-cache** コマンド文を削除します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-cache statistics	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-server	**filter** コマンド用の N2H2 サーバまたは Websense サーバを指定します。

url-list

WebVPN ユーザがアクセスする URL のセットを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。複数の URL でリストを設定するには、各 URL に対して 1 回、同じリスト名でこのコマンドを複数回使用します。設定済みリスト全体を削除するには、**no url-list** *listname* コマンドを使用します。設定済みの URL を削除するには、**no url-list** *listname url* コマンドを使用します。

複数のリストを設定するには、このコマンドを複数回使用して、各リストに固有の *listname* を割り当てます。

url-list {*listname displayname url***}**

no url-list *listname*

no url-list *listname url*

シンタックスの説明

displayname	WebVPN エンド ユーザ インターフェイスに表示されるテキストを入力して、URL を識別します。最大 64 文字です。リストごとに固有の名前でなければなりません。スペースを使用できます。
listname	WebVPN ユーザがアクセスできる URL のセットをグループ化します。最大 64 文字です。最大 64 文字です。セミコロン（;）、アンパサンド（&）、小なり（<）記号は使用できません。
url	リンクを指定します。サポートされる URL タイプは http、https、および cifs です。

デフォルト

デフォルトの URL リストはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードで url-list コマンドを使用して、URL のリストを 1 つ以上作成します。特定のグループ ポリシーまたはユーザがリスト内の URL にアクセスできるようにするには、WebVPN モードで、ここで作成した *listname* を **url-list** コマンドと共に使用します。

例

次の例は、www.cisco.com、www.example.com、および www.example.org にアクセスする *Marketing URLs* という URL リストを作成する方法を示しています。次の表に、各 URL の設定で使用する値を示します。

listname	displayname	url
Marketing URLs	Cisco Systems	http://www.cisco.com
Marketing URLs	Example Company, Inc.	http://www.example.com
Marketing URLs	Example Organization	http://www.example.org

```
hostname(config)# url-list Marketing URLs Cisco Systems http://www.cisco.com
hostname(config)# url-list Marketing URLs Example Company, Inc. http://www.example.com
hostname(config)# url-list Marketing URLs Example Organization http://www.example.org
```

関連コマンド

コマンド	説明
clear configuration url-list	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドのみ削除します。
url-list	WebVPN モードでこのコマンドを使用すると、グループ ポリシーまたはユーザが URL の設定済みリストにアクセスできます。
show running-configuration url-list	現在設定されている URL のセットを表示します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。WebVPN モードに入って、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル コンフィギュレーション値を設定できます。

url-list（webvpn）

WebVPN サーバのリストと URL を特定のユーザまたはグループ ポリシーに適用するには、グループ ポリシー webvpn コンフィギュレーション モードまたはユーザ名 webvpn コンフィギュレーション モードで **url-list** コマンドを使用します。**url-list none** コマンドを使用して作成したヌル値を含むリストを削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。URL リストを継承しないようにするには、**url-list none** コマンドを使用します。コマンドを 2 回使用すると、先行する設定値が上書きされます。

url-list {***value*** *name* | **none**} [*index*]

no url-list

シンタックスの説明

index	ホームページ上で表示される優先順位を示します。
none	URL リストにヌル値を設定します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからリストを継承しないようにします。
value *name*	URL の設定済みリストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

デフォルト

デフォルトの URL リストはありません。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
WebVPN モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

コマンドを 2 回使用すると、先行する設定値が上書きされます。

WebVPN モードで **url-list** コマンドを使用して、ユーザまたはグループ ポリシー用の WebVPN ホームページに表示する URL リストを識別する前に、リストを作成する必要があります。グローバル コンフィギュレーション モードで **url-list** コマンドを使用して、1 つ以上のリストを作成します。

例

次の例では、FirstGroupURLs という URL リストを FirstGroup というグループ ポリシーに適用し、このリストを 1 番目の URL リストに指定しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# url-list value FirstGroupURLs 1
```

関連コマンド

コマンド	説明
clear configure url-list [*listname*]	すべての url-list コマンドをコンフィギュレーションから削除します。listname を含めると、セキュリティ アプライアンスはそのリストのコマンドのみ削除します。
show running-configuration url-list	現在設定されている **url-list** コマンドのセットを表示します。
url-list	WebVPN ユーザがアクセスできる URL のセットを設定するには、グローバル コンフィギュレーション モードでアクセスできる WebVPN モードでこのコマンドを使用します。
webvpn	webvpn モードに入ります。これは、webvpn コンフィギュレーション モード、グループ ポリシー webvpn コンフィギュレーション モード（特定のグループ ポリシーに対する webvpn の値を設定するため）、またはユーザ名 webvpn コンフィギュレーション モード（特定のユーザに対する webvpn の値を設定するため）のいずれかです。

url-server

filter コマンドで使用する N2H2 または Websense サーバを指定するには、グローバル コンフィギュレーション モードで **url-server** コマンドを使用します。このコンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

N2H2

url-server [<(*if_name*)>]　vendor {smartfilter | n2h2} host <*local_ip*> [port <*number*>] [timeout <seconds>] [protocol {TCP [connections <*number*>]} | UDP]

no url-server [<(*if_name*)>]　vendor {smartfilter | n2h2} host <*local_ip*> [port <*number*>] [timeout <seconds>] [protocol {TCP [connections <*number*>]} | UDP]

Websense

url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** | **connections** *num_conns*] | *version*]

no url-server (*if_name***) vendor websense host** *local_ip* [**timeout** *seconds*] [**protocol** {**TCP** | **UDP** [**connections** *num_conns*] | *version*]

シンタックスの説明

N2H2

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに向かって作成される TCP 接続の最大数を指定します。これはサーバごとの数であるため、複数のサーバに対して、それぞれ別の接続値を指定することができます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	（オプション）認証サーバが常駐するネットワーク インターフェイス。指定しない場合、デフォルトは内部インターフェイスです。
port *number*	N2H2 サーバ ポート。セキュリティ アプライアンスは、UDP 返答のリッスンもこのポート上で行います。デフォルトのポート番号は 4005 です。
protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP です。
timeout *seconds*	許容される最大アイドル時間で、経過後にセキュリティ アプライアンスは指定した次のサーバに切り替わります。デフォルトは 30 秒です。
vendor	smartfilter または n2h2（下位互換性を保つため）を使用して、URL フィルタリング サービスを指定します。ただし、smartfilter はベンダー文字列として保存されます。

Websense

connections	許容する TCP 接続の最大数を制限します。
num_conns	セキュリティ アプライアンスから URL サーバに向かって作成される TCP 接続の最大数を指定します。これはサーバごとの数であるため、複数のサーバに対して、それぞれ別の接続値を指定することができます。
host *local_ip*	URL フィルタリング アプリケーションを実行するサーバ。
if_name	認証サーバが常駐するネットワーク インターフェイス。指定しない場合、デフォルトは内部インターフェイスです。
timeout *seconds*	許容される最大アイドル時間で、経過後にセキュリティ アプライアンスは指定した次のサーバに切り替わります。デフォルトは 30 秒です。

protocol	プロトコルは、**TCP** キーワードまたは **UDP** キーワードを使用して設定できます。デフォルトは TCP プロトコル、Version 1 です。
vendor websense	URL フィルタリング サービス ベンダーが Websense であることを示します。
version	プロトコル Version **1** または Version **4** を指定します。デフォルトは TCP プロトコル Version 1 です。TCP は、Version 1 または Version 4 を使用して設定できます。UDP の設定に使用できるのは、Version 4 だけです。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

url-server コマンドでは、N2H2 または Websense URL フィルタリング アプリケーションを実行しているサーバを指定します。ただし、URL サーバ数の上限は、シングル コンテキスト モードでは 16、マルチ コンテキスト モードですが、一度に使用できるアプリケーションは、N2H2 または Websense のどちらか 1 つだけです。さらに、セキュリティ アプライアンス上でコンフィギュレーションを変更しても、アプリケーション サーバ上のコンフィギュレーションはアップデートされないため、ベンダーの指示に従って別途アップデートする必要があります。

HTTPS および FTP に対して **filter** コマンドを実行するには、事前に **url-server** コマンドを設定する必要があります。すべての URL サーバがサーバ リストから削除されると、URL フィルタリングに関連する **filter** コマンドもすべて削除されます。

サーバを指示した後、**filter url** コマンドを使用して、URL フィルタリング サービスをイネーブルにします。

サーバの統計情報（到達できないサーバも含む）を表示するには、**show url-server statistics** コマンドを使用します。

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　ベンダー固有の **url-server** コマンドを適切な形式で使用して、URL フィルタリング アプリケーション サーバを指示します。

ステップ 2　**filter** コマンドで、URL フィルタリングをイネーブルにします。

ステップ 3　（オプション）**url-cache** コマンドを使用して、URL キャッシュをイネーブルにし、認識される応答時間を改善します。

ステップ 4　（オプション）**url-block** コマンドを使用して、長い URL および HTTP のバッファリングのサポートをイネーブルにします。

ステップ 5　**show url-block block statistics**、**show url-cache statistics**、または **show url-server statistics** の各コマンドを使用して、実行情報を表示します。

N2H2 によるフィルタリングの詳細については、次の N2H2 の Web サイトを参照してください。

http://www.n2h2.com

Websense フィルタリングの詳細については、次の Web サイトを参照してください。

http://www.websense.com/

例

次の例では、N2H2 を使用している場合に、10.0.2.54 ホストからの接続を除く、発信 HTTP 接続をすべてフィルタリングします。

```
hostname(config)# url-server (perimeter) vendor n2h2 host 10.0.1.1
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次の例では、Websense を使用している場合に、10.0.2.54 ホストからの接続を除く、発信 HTTP 接続をすべてフィルタリングします。

```
hostname(config)# url-server (perimeter) vendor websense host 10.0.1.1 protocol TCP
version 4
hostname(config)# filter url http 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
clear url-server	URL フィルタリング サーバの統計情報を消去します。
filter url	トラフィックを URL フィルタリング サーバに向けて送ります。
show url-block	N2H2 フィルタリング サーバまたは Websense フィルタリング サーバから受信した URL 応答に使用される URL キャッシュに関する情報を表示します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。

user-authentication

ユーザ認証をイネーブルにするには、グループ ポリシー コンフィギュレーション モードで **user-authentication enable** コマンドを使用します。ユーザ認証をディセーブルにするには、**user-authentication disable** コマンドを使用します。ユーザ認証アトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、ユーザ認証の値を別のグループ ポリシーから継承できます。

イネーブルの場合、ユーザ認証ではハードウェア クライアントの背後にいる個々のユーザが、トンネルを越えてネットワークへのアクセスを取得するように認証する必要があります。

user-authentication {**enable | disable**}

no user-authentication

シンタックスの説明

disable	ユーザ認証をディセーブルにします。
enable	ユーザ認証をイネーブルにします。

デフォルト

ユーザ認証はディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

個々のユーザは設定した認証サーバの順序に従って認証します。

プライマリ セキュリティ アプライアンスでのユーザ認証が必要な場合は、バックアップ サーバでも同様に設定されていることを確認します。

例

次の例は、「FirstGroup」というグループ ポリシーのユーザ認証をイネーブルにする方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication enable
```

関連コマンド

コマンド	説明
ip-phone-bypass	ユーザ認証を受けずに IP 電話を接続できるようにします。Secure Unit Authentication は有効なままになります。
leap-bypass	イネーブルの場合、LEAP パケットが VPN クライアントの背後にある無線デバイスから VPN トンネルを通過した後でユーザ認証を行います。これにより、シスコの無線アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できます。確立後、ワークステーションはユーザごとの認証をもう一度実行します。
secure-unit-authentication	クライアントがトンネルを開始するたびに VPN クライアントがユーザ名とパスワードを使用した認証を要求することにより、さらにセキュリティが向上します。
user-authentication-idle-timeout	個々のユーザのアイドル タイムアウトを設定します。アイドル タイムアウト期間中にユーザ接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

user-authentication-idle-timeout

ハードウェア クライアントの背後にいる個々のユーザに対してアイドル タイムアウトを設定するには、グループ ポリシー コンフィギュレーション モードで **user-authentication-idle-timeout** コマンドを使用します。アイドル タイムアウト値を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、アイドル タイムアウト値を別のグループ ポリシーから継承できます。アイドル タイムアウト値を継承しないようにするには、**user-authentication-idle-timeout none** コマンドを使用します。

アイドル タイムアウト期間中にハードウェア クライアントの背後にいるユーザによる通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

user-authentication-idle-timeout {*minutes* | **none**}

no user-authentication-idle-timeout

シンタックスの説明

minutes	アイドル タイムアウト期間を分単位で指定します。範囲は、1 ～ 35791394 分です。
none	無制限のアイドル タイムアウト期間を許容します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーからユーザ認証のアイドル タイムアウト値を継承しないようにします。

デフォルト

30 分。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

最小値は 1 分、デフォルトは 30 分、最大値は 10,080 分です。

例

次の例は、「FirstGroup」というグループ ポリシーに 45 分のアイドル タイムアウト値を設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# user-authentication-idle-timeout 45
```

関連コマンド

コマンド	説明
user-authentication	ハードウェア クライアントの背後にいるユーザに対して、接続前にセキュリティ アプライアンスに識別情報を示すように要求します。

username

セキュリティ アプライアンス データベースにユーザを追加するには、グローバル コンフィギュレーション モードで **username** コマンドを入力します。ユーザを削除するには、削除するユーザ名で、このコマンドの **no** 形式を使用します。すべてのユーザ名を削除するには、ユーザ名を付加せずに、このコマンドの **no** 形式を使用します。

username *name* {**nopassword** | **password** *password* [**mschap** | **encrypted** | **nt-encrypted**]} [**privilege** *priv_level*]

no username *name*

シンタックスの説明

encrypted	パスワードを暗号化することを示します（**mschap** を指定しなかった場合）。**username** コマンドで定義するパスワードは、セキュリティを維持するため、コンフィギュレーションに保存されるときに暗号化されます。**show running-config** コマンドを入力したときに、**username** コマンドで実際のパスワードは表示されません。暗号化されたパスワードと、その後に **encrypted** キーワードが表示されます。たとえば、「test」というパスワードを入力した場合は、**show running-config** を実行すると次のように表示されます。 `username pat password rvEdRh0xPC8bel7s encrypted` CLI で実際に **encrypted** キーワードを入力するのは、別のセキュリティ アプライアンスにコンフィギュレーションをカット アンド ペーストして同じパスワードを使用する場合だけです。
mschap	入力したパスワードを unicode に変換し、MD4 でハッシュすることを指定します。ユーザを MSCHAPv1 または MSCHAPv2 を使用して認証している場合に、このキーワードを使用します。
name	ユーザの名前を 4 ～ 15 文字で指定します。
nopassword	このユーザにはパスワードが不要であることを示します。
nt-encrypted	パスワードを MSCHAPv1 または MSCHAPv2 での認証用に暗号化することを指定します。ユーザを追加するときに **mschap** キーワードを指定すると、**show running-config** コマンドでコンフィギュレーションを表示したときに、**encrypted** キーワードではなく、このキーワードが表示されます。 **username** コマンドで定義するパスワードは、セキュリティを維持するため、コンフィギュレーションに保存されるときに暗号化されます。**show running-config** コマンドを入力したときに、**username** コマンドで実際のパスワードは表示されません。暗号化されたパスワードと、その後に **nt-encrypted** キーワードが表示されます。たとえば、「test」というパスワードを入力した場合は、**show running-config** を実行すると次のように表示されます。 `username pat password DLaUiAX3l78qgoB5c7iVNw== nt-encrypted` CLI で実際に **nt-encrypted** キーワードを入力するのは、別のセキュリティ アプライアンスにコンフィギュレーションをカット アンド ペーストして同じパスワードを使用する場合だけです。
password *password*	3 ～ 16 文字のパスワードを設定します。
privilege *priv_level*	使用する特権レベルを 0（最低）～ 15（最高）に指定します。デフォルトの特権レベルは 2 です。この特権レベルは、コマンドの認可で使用されます。

デフォルト

デフォルトの特権レベルは 2 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	**mschap** キーワードと **nt-encrypted** キーワードが追加されました。

使用上のガイドライン

login コマンドを入力したときに、このデータベースが認証用に使われます。

CLI にアクセスできるユーザや特権 EXEC モードに入れないユーザをローカル データベースに追加する場合は、コマンド認可を設定する必要があります（**aaa authorization command** コマンドを参照）。コマンド認可を設定しないと、ユーザの特権レベルが 2（デフォルト）以上であれば、CLI で自分のパスワードを使って特権 EXEC モード（およびすべてのコマンド）にアクセスできるようになります。または、AAA 認証を使用して、ユーザが **login** コマンドを使えないようにするか、全ローカル ユーザの特権レベルを 1 に設定して、どのユーザが **enable** パスワードで特権 EXEC モードにアクセスできるかを制御します。

デフォルトでは、このコマンドを使用して追加した VPN ユーザには、アトリビュートまたはグループ ポリシーのアソシエーションはありません。**username attributes** コマンドを使用して、すべての値を明示的に設定する必要があります。

例

次の例では、12345678 というパスワードと、特権レベル 12 を持つ anyuser というユーザを設定する方法を示します。

```
hostname(config)# username anyuser password 12345678 privilege 12
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
clear config username	特定のユーザまたはすべてのユーザのコンフィギュレーションを消去します。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username attributes	ユーザ名アトリビュート モードに入って、個々のユーザのアトリビュートを設定できるようにします。
webvpn	config-group-webvpn モードに入ります。このモードで、指定したグループに対する WebVPN アトリビュートを設定できます。

username attributes

ユーザ名アトリビュート モードに入るには、ユーザ名コンフィギュレーション モードで **username attributes** コマンドを使用します。特定のユーザのすべてのアトリビュートを削除するには、このコマンドの **no** 形式を使用して、ユーザ名を付加します。すべてのユーザのアトリビュートを削除するには、ユーザ名を付加せずに、このコマンドの **no** 形式を使用します。アトリビュート モードを使用すると、指定したユーザに対してアトリビュート値ペアを設定できます。

username {*name*} **attributes**

no username [*name*] **attributes**

シンタックスの説明

name	ユーザの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0.1	このコマンドが導入されました。

使用上のガイドライン

内部ユーザ認証データベースは、username コマンドを使用して入力されたユーザで構成されています。login コマンドは、このデータベースを認証用に使用します。ユーザ名アトリビュートは、**username** コマンドまたは **username attributes** コマンドのいずれかを使用して設定します。

ユーザ名コンフィギュレーション モードのコマンドのシンタックスには、共通する次の特性があります。

- **no** 形式は、実行コンフィギュレーションからアトリビュートを削除します。
- **none** キーワードも、実行コンフィギュレーションからアトリビュートを削除します。ただし、アトリビュートにヌル値を設定することにより削除され、継承しないようにします。
- ブール アトリビュートには、イネーブルまたはディセーブルになっている設定のための明示的なシンタックスがあります。

username attributes コマンドでユーザ名コンフィギュレーション モードに入ると、次のアトリビュートを設定できます。

アトリビュート	機能
group-lock	ユーザが接続する必要がある既存のトンネル グループを指定します。
password-storage	クライアント システムでのログイン パスワードの保管をイネーブルまたはディセーブルにします。
vpn-access-hours	設定済みの時間範囲ポリシーの名前を指定します。

アトリビュート	機能
vpn-filter	ユーザ固有の ACL の名前を指定します。
vpn-framed-ip-address	クライアントに割り当てられる IP アドレスとネット マスクを指定します。
vpn-group-policy	アトリビュートの継承元になるグループ ポリシーの名前を指定します。
vpn-idle-timeout	アイドル タイムアウト期間を分で指定するか、または ***none*** を使用してディセーブルにします。
vpn-session-timeout	ユーザの最長接続時間を分単位で指定するか、***none*** を使用して無制限にします。
vpn-simultaneous-logins	使用可能な同時ログインの最大数を指定します。
vpn-tunnel-protocol	許可されたトンネリング プロトコルを指定します。
webvpn	webvpn アトリビュートを設定する webvpn モードに入ります。

ユーザ名に対する webvpn モード アトリビュートは、ユーザ名の webvpn コンフィギュレーション モードで **username attributes** コマンドを入力してから **webvpn** コマンドを入力して設定します。詳細については、**webvpn** コマンド（グループ ポリシー アトリビュートおよびユーザ名アトリビュート モード）の説明を参照してください。

例

次の例では、「anyuser」という名前のユーザのユーザ名アトリビュート コンフィギュレーション モードに入る方法を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)#
```

関連コマンド

コマンド	説明
clear config username	ユーザ名データベースを消去します。
show running-config username	特定のユーザまたはすべてのユーザの実行コンフィギュレーションを表示します。
username	ユーザをセキュリティ アプライアンスのデータベースに追加します。
webvpn	指定されたグループの WebVPN アトリビュートを設定するユーザ名の webvpn コンフィギュレーション モードに入ります。

username-prompt

WebVPN ユーザがセキュリティ アプライアンスに接続するときに表示される WebVPN ページ ログイン ボックスのユーザ名プロンプトをカスタマイズするには、webvpn カスタマイゼーション モードで **username-prompt** コマンドを使用します。

username-prompt {**text** | **style**} *value*

[**no**] **username-prompt** {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

text	テキストを変更することを指定します。
style	スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

ユーザ名プロンプトのデフォルトのテキストは「USERNAME」です。

ユーザ名プロンプトのデフォルトのスタイルは color:black;font-weight:bold;text-align:right です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

(注)　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、テキストを「Corporate Username:」に変更し、デフォルト スタイルのフォント ウェイトを bolder に変更しています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# username-prompt text Corporate Username:
F1-asa1(config-webvpn-custom)# username-prompt style font-weight:bolder
```

関連コマンド

コマンド	説明
group-prompt	WebVPN ページのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのパスワード プロンプトをカスタマイズします。

user-parameter

SSO 認証用にユーザ名を送信する必要がある HTTP POST 要求のパラメータの名前を指定するには、AAA サーバ ホスト コンフィギュレーション モードで **user-parameter** コマンドを使用します。これは HTTP Forms コマンドを使用した SSO です。

user-parameter *name*

（注） HTTP プロトコルで SSO を適切に設定するには、認証と HTTP プロトコル交換についての十分な実用知識が必要です。

シンタックスの説明

name	HTTP POST 要求に含まれるユーザ名パラメータの名前です。最大長は 128 文字です。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
AAA サーバ ホスト コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスの WebVPN サーバは、HTTP POST 要求を使用して、シングル サインオン認証要求を SSO サーバに送信します。要求されたコマンド **user-parameter** は、この HTTP POST 要求が SSO 認証用のユーザ名パラメータを含める必要があることを指定します。

（注） ログイン時に、ユーザは実際の名前の値を入力します。この値は HTTP POST 要求に入力されて、認証 web サーバに渡されます。

例

AAA サーバ ホスト コンフィギュレーション モードで入力された次の例では、ユーザ名パラメータの userid が SSO 認証で使用される HTTP POST 要求に含まれることを指定します。

```
hostname(config)# aaa-server testgrp1 host example.com
hostname(config-aaa-server-host)# user-parameter userid
hostname(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザ名とパスワードを受信する Web サーバ URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバとの交換に使用する非表示パラメータを作成します。
password-parameter	SSO 認証用にユーザ パスワードを送信する必要がある HTTP POST 要求のパラメータの名前を指定します。
start-url	事前ログイン クッキーの取得先 URL を指定します。

validate-attribute

RADIUS アカウンティングを使用する際に RADIUS アトリビュートを検証するには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで、**validate attribute** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスできます。

このオプションは、デフォルトではディセーブルになっています。

validate-attribute [*attribute_number*]

no validate-attribute [*attribute_number*]

シンタックスの説明

attribute_number	RADIUS アカウンティングで検証する RADIUS アトリビュート。有効な範囲は 1 ～ 191 です。ベンダー固有のアトリビュートはサポートされていません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
RADIUS アカウンティング パラメータ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを設定すると、セキュリティ アプライアンスでは、Framed IP アトリビュートに加えて RADIUS アトリビュートも照合します。このコマンドは、インスタンスを複数設定することができます。

RADIUS アトリビュートのタイプのリストを見るには、次のサイトにアクセスしてください。

http://www.iana.org/assignments/radius-types

例

次の例では、ユーザ名 RADIUS アトリビュートの RADIUS アカウンティングをイネーブルにする方法を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# validate attribute 1
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングの検査を設定します。
parameters	検査ポリシー マップのパラメータを設定します。

verify

ファイルのチェックサムを検証するには、特権 EXEC モードで **verify** コマンドを使用します。

verify *path*

verify ***/md5*** *path* [*md5-value*]

シンタックスの説明

/md5	（オプション）指定したソフトウェア イメージの MD5 値を計算して表示します。この値を、Cisco.com で入手できるこのイメージの値と比較します。
md5-value	（オプション）指定したイメージの既知の MD5 値。このコマンドで MD5 値を指定すると、指定したイメージの MD5 値が計算され、MD5 値が一致するかどうかを示すメッセージが表示されます。
path	• ***disk0:/***[*path/*]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみで使用でき、内蔵フラッシュ メモリを示します。***disk0*** ではなく ***flash*** を使用することもできます。これらは、エイリアス関係にあります。 • ***disk1:/***[*path/*]*filename* このオプションは、ASA 5500 シリーズ適応型セキュリティ アプライアンスのみで使用でき、外部フラッシュ メモリ カードを示します。 • ***flash:/***[*path/*]*filename* このオプションは、内蔵フラッシュ カードを示します。ASA 5500 シリーズ適応型セキュリティ アプライアンスでは、***flash*** は ***disk0*** のエイリアスです。 • ***ftp://***[*user*[***:***password*]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;type=***xx*] ***type*** には、次のいずれかのキーワードを指定できます。 — ***ap***：ASCII パッシブ モード — ***an***：ASCII 通常モード — ***ip***：（デフォルト）バイナリ パッシブ モード — ***in***：バイナリ通常モード • ***http***[***s***]***://***[*user*[***:***password*]***@***]*server*[*:port*]***/***[*path/*]*filename* • ***tftp://***[*user*[***:***password*]***@***]*server*[*:port*]***/***[*path/*]*filename*[***;int=***interface_name*] サーバ アドレスへのルートを上書きする場合は、インターフェイス名を指定します。 ただし、パス名にスペースを含めることはできません。パス名にスペースが含まれている場合は、**verify** コマンドではなく **tftp-server** コマンドでパスを設定してください。

デフォルト

現在のフラッシュ デバイスが、デフォルトのファイル システムです。

（注） ***/md5*** オプションを指定する場合に、ftp、http、tftp などのネットワークのファイルをソースとして指定できます。***/md5*** オプションを指定せずに **verify** コマンドを使用すると、フラッシュ メモリにあるローカル イメージしか検証できません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　**verify** コマンドを使用して、ファイルを使う前にそのチェックサムを検証します。

ディスクで配布されるソフトウェア イメージごとに、イメージ全体用のチェックサムが 1 つあります。このチェックサムは、イメージをフラッシュ メモリにコピーした場合にだけ表示されます。あるディスクから別のディスクにコピーした場合には表示されません。

新しいイメージをロードまたは複製する前に、そのチェックサムと MD5 情報を記録しておき、イメージをフラッシュ メモリやサーバにコピーしたときにチェックサムを検証できるようにしてください。Cisco.com には、イメージのさまざまな情報が掲載されています。

フラッシュ メモリの内容を表示する場合は、**show flash** コマンドを使用します。表示される内容に、個々のファイルのチェックサムは含まれていません。イメージをフラッシュ メモリにコピーした後で、そのチェックサムを再度計算して検証するには、**verify** コマンドを使用します。ただし、**verify** コマンドは、ファイルがファイル システムに保存されている場合にのみ、整合性のチェックを行うことに注意してください。そのため、壊れたイメージがセキュリティ アプライアンスに転送され、検出されずにファイル システムに保存されている可能性があります。セキュリティ アプライアンスに壊れたイメージが転送された場合、ソフトウェアは、イメージが壊れていることを検出できず、ファイルの検証が問題なく完了します。

Message Digest 5（MD5）ハッシュ アルゴリズムを使ってファイルを検証する場合は、**verify** コマンドと共に ***/md5*** オプションを使用します。MD5（RFC 1321 で規定）は、128 ビットの固有のメッセージ ダイジェストを作成してデータの整合性を検証するアルゴリズムです。**verify** コマンドの ***/md5*** オプションは、セキュリティ アプライアンスのソフトウェア イメージの MD5 チェックサムの値を、その既知の MD5 チェックサム値と比較することにより、イメージの整合性を確認します。Cisco.com では、ローカル システム イメージ値との比較用に、すべてのセキュリティ アプライアンスのソフトウェア イメージの MD5 値を取得できます。

MD5 による整合性の確認を行うには、***/md5*** キーワードを使用して **verify** コマンドを発行します。たとえば、**verify /md5 flash:cdisk.bin** コマンドを発行すると、ソフトウェア イメージの MD5 値が計算されて表示されます。この値を、Cisco.com で入手できるこのイメージの値と比較します。

または、先に Cisco.com から MD5 値を取得しておき、その値をコマンドのシンタックスで指定できます。たとえば、**verify /md5 flash:cdisk.bin 8b5f3062c4cacdbae72571440e962233** コマンドを発行すると、MD5 値が一致するかどうかを示すメッセージが表示されます。MD5 値が一致しないというのは、イメージが壊れているか、入力された MD5 値が間違っているという意味です。

例

次の例では、cdisk.bin というイメージ ファイルを検証します。ただし、わかりやすいように、テキストの一部が省略されています。

```
hostname# verify cdisk.bin
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!Done!
Embedded Hash MD5: af5a155f3d5c128a271282c33277069b
Computed Hash MD5: af5a155f3d5c128a271282c33277069b
CCO Hash      MD5: b569fff8bbf8087f355aaf22ef46b782
Signature Verified
Verified disk0:/cdisk.bin
hostname#
```

関連コマンド

コマンド	説明
copy	ファイルをコピーします。
dir	システム内のファイルを一覧表示します。

version

セキュリティ アプライアンスでグローバルに使用する RIP のバージョンを指定するには、ルータ コンフィギュレーション モードで **version** コマンドを使用します。デフォルトに戻すには、このコマンドの **no** 形式を使用します。

version {***1*** | ***2***}

no version

シンタックスの説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

デフォルト

セキュリティ アプライアンスは、バージョン 1 と 2 の両方のパケットを受け取れますが、バージョン 1 のパケットしか送信しません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ルータ コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドと **rip receive version** コマンドを指定します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用することで、RIP アップデートを認証できます。

例

次の例では、すべてのインターフェイスで RIP バージョン 2 のパケットを送受信するようにセキュリティ アプライアンスを設定します。

```
hostname(config)# router rip
hostname(config-router)# network 10.0.0.0
hostname(config-router)# version 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに、使用する RIP バージョンを指定します。
rip receive version	指定したインターフェイス上でアップデートを受信するときに、受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードに入ります。

virtual http

仮想 HTTP サーバを設定するには、グローバル コンフィギュレーション モードで **virtual http** コマンドを使用します。仮想サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

virtual http *ip_address* [**warning**]

no virtual http *ip_address* [**warning**]

シンタックスの説明

ip_address	セキュリティ アプライアンス上の仮想 HTTP サーバの IP アドレスを設定します。このアドレスが、セキュリティ アプライアンスに向かってルーティングされる未使用アドレスであることを確認してください。たとえば、外部にアクセスするときに内部アドレスの NAT を実行し、仮想 HTTP サーバへの外部アクセスを提供する場合は、仮想 HTTP サーバ アドレスに対して、グローバル NAT アドレスの 1 つを使用できます。
warning	（オプション）HTTP 接続をセキュリティ アプライアンスにリダイレクトする必要があることをユーザに通知します。このキーワードは、リダイレクトが自動的に発生しないテキストベースのブラウザのみに適用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	前のリリースで使用されていたインライン基本 HTTP 認証方式がリダイレクション方式に置き換えられたため、このコマンドは必要なくなり、廃止されました。
7.2(2)	基本 HTTP 認証（デフォルト）を使用するか、**aaa authentication listener** コマンドによる HTTP リダイレクションを使用するかを選択できるようになったため、このコマンドが復活しました。リダイレクション方式では、HTTP 認証をカスケードする際に特別なコマンドを必要としません。

使用上のガイドライン

セキュリティ アプライアンスで HTTP 認証を使用する場合（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）、セキュリティ アプライアンスではデフォルトで基本 HTTP 認証が使用されます。セキュリティ アプライアンスが Web ページ（**aaa authentication listener** コマンドに **redirect** キーワードを指定してセキュリティ アプライアンス自身によって生成された Web ページ）に HTTP 接続をリダイレクトするように、認証方式を変更できます。

ただし、基本 HTTP 認証を使用し続ける場合、HTTP 認証をカスケードするときに **virtual http** コマンドが必要になることがあります。

セキュリティ アプライアンスに加えて宛先 HTTP サーバでも認証が必要な場合、**virtual http** コマンドを使用すると、セキュリティ アプライアンス（AAA サーバ経由）と宛先 HTTP サーバで別々に認証することができます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。AAA サーバおよび HTTP サーバのユーザ名およびパスワードが同じでない場合、HTTP 認証は失敗します。

このコマンドは、セキュリティ アプライアンス上の仮想 HTTP サーバへの AAA 認証を必要とするすべての HTTP 接続をリダイレクトします。セキュリティ アプライアンスは、AAA サーバのユーザ名およびパスワードを要求します。AAA サーバがユーザを認証すると、セキュリティ アプライアンスは HTTP 接続を元のサーバにリダイレクトしますが、AAA サーバのユーザ名およびパスワードは含まれません。HTTP パケットにユーザ名およびパスワードが含まれていないため、HTTP サーバは個々のユーザに HTTP サーバのユーザ名およびパスワードを要求します。

(注) **virtual http** コマンドを使用する場合は、**timeout uauth** コマンドの継続時間を 0 秒に設定しないでください。このように設定すると、実際の Web サーバへの HTTP 接続ができなくなります。

例

次の例は、AAA 認証と共に仮想 HTTP 認証をイネーブルにする方法を示しています。

```
hostname(config)# access-list HTTP-ACL extended permit tcp 10.1.1.0 any eq 80
hostname(config)# aaa authentication match HTTP-ACL inside tacacs+
hostname(config)# virtual http 10.1.2.1
```

関連コマンド

コマンド	説明
aaa authentication listener http	セキュリティ アプライアンスで認証に使用される方式を設定します。
clear configure virtual	コンフィギュレーションから **virtual** コマンド文を削除します。
show running-config virtual	セキュリティ アプライアンス仮想サーバの IP アドレスを表示します。
sysopt uauth allow-http-cache	**virtual http** コマンドをイネーブルにすると、ブラウザ キャッシュにあるユーザ名およびパスワードを使用して仮想サーバに再接続できます。
virtual telnet	セキュリティ アプライアンス上に仮想 Telnet サーバを設定することで、認証が必要な他のタイプの接続を開始する前にセキュリティ アプライアンスでユーザを認証できるようにします。

virtual telnet

セキュリティ アプライアンスで仮想 Telnet サーバを設定するには、グローバル コンフィギュレーション モードで **virtual telnet** コマンドを使用します。セキュリティ アプライアンスで認証プロンプトが表示されない別のタイプのトラフィックを認証する必要がある場合は、仮想 Telnet サーバでユーザを認証しなければならないことがあります。サーバをディセーブルにするには、このコマンドの **no** 形式を使用します。

virtual telnet *ip-address*

no virtual telnet *ip-address*

シンタックスの説明

ip_address	セキュリティ アプライアンス上の仮想 Telnet サーバの IP アドレスを設定します。このアドレスが、セキュリティ アプライアンスに向かってルーティングされる未使用アドレスであることを確認してください。たとえば、外部にアクセスするときに内部アドレスの NAT を実行し、仮想 Telnet サーバへの外部アクセスを提供する場合は、仮想 Telnet サーバ アドレスに対して、グローバル NAT アドレスの 1 つを使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

任意のプロトコルまたはサービス（**aaa authentication match** コマンドまたは **aaa authentication include** コマンドを参照）に対してネットワーク アクセス認証を設定できますが、直接 HTTP、Telnet、または FTP だけで認証することもできます。ユーザは認証を必要とする別のトラフィックが許可される前に、これらのサービスの 1 つで先に認証する必要があります。セキュリティ アプライアンスを通して HTTP、Telnet、または FTP を許可せずに、別のタイプのトラフィックを認証する場合は、セキュリティ アプライアンスで設定された所定の IP アドレスにユーザが Telnet 接続し、セキュリティ アプライアンスが Telnet プロンプトを表示するように、仮想 Telnet を設定できます。

権限のないユーザが仮想 Telnet IP アドレスに接続したとき、ユーザ名とパスワードが要求され、AAA サーバによって認証されます。認証されると、「Authentication Successful.」というメッセージが表示されます。その後、ユーザは認証を必要とするその他のサービスに正常にアクセスできるようになります。

例

次の例では、他のサービスに対する AAA 認証と共に仮想 Telnet をイネーブルにする方法を示します。

```
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 10.1.2.1 eq
telnet
hostname(config)# access-list AUTH extended permit tcp 10.1.1.0 host 209.165.200.225
eq smtp
hostname(config)# aaa authentication match AUTH inside tacacs+
hostname(config)# virtual telnet 10.1.2.1
```

関連コマンド

コマンド	説明
clear configure virtual	コンフィギュレーションから **virtual** コマンド文を削除します。
show running-config virtual	セキュリティ アプライアンス仮想サーバの IP アドレスを表示します。
virtual http	セキュリティ アプライアンス上で HTTP 認証を使用し、HTTP サーバも認証を要求している場合、このコマンドを使用すると、セキュリティ アプライアンスと HTTP サーバで別々に認証を実行できます。仮想 HTTP を使用しない場合は、セキュリティ アプライアンスに対する認証で使用したものと同じユーザ名とパスワードが HTTP サーバに送信されます。HTTP サーバのユーザ名とパスワードを別に入力するように求められることはありません。

vlan

VLAN ID をサブインターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **vlan** コマンドを使用します。VLAN ID を削除するには、このコマンドの **no** 形式を使用します。サブインターフェイスには、トラフィックを渡す VLAN ID が必要です。VLAN サブインターフェイスを使用すると、1 つの物理インターフェイスに複数の論理インターフェイスを設定できます。VLAN を使用すると、所定の物理インターフェイス（たとえば複数のセキュリティ コンテキスト）にトラフィックを別に保存できます。

vlan *id*

no vlan

シンタックスの説明

id	1 ～ 4094 の整数を指定します。一部の VLAN ID には、接続されたスイッチで予約されているものもあります。詳細については、スイッチのマニュアルを参照してください。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
インターフェイス コンフィギュレーション	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**interface** コマンドのキーワードからインターフェイス コンフィギュレーション モードのコマンドに変更されました。

使用上のガイドライン

1 つの VLAN だけを、物理インターフェイスではなく、サブインターフェイスに割り当てることができます。各サブインターフェイスは、トラフィックを通過する前に VLAN ID を持つ必要があります。VLAN ID を変更するには、**no** オプションで古い VLAN ID を削除する必要はありません。別の VLAN ID を使用して **vlan** コマンドを入力すると、セキュリティ アプライアンスは古い ID を変更します。

サブインターフェイスをイネーブルにするために、**no shutdown** コマンドで物理インターフェイスをイネーブルにする必要があります。サブインターフェイスをイネーブルにする場合、物理インターフェイスはタグの付かないパケットを通過させるため、一般的には物理インターフェイスがトラフィックを通過させないようにします。したがって、インターフェイスを停止することで物理インターフェイスを介してトラフィックが通過しないようにすることはできません。代わりに、**nameif** コマンドを省略することで、物理インターフェイスがトラフィックを通過させないことを確認します。物理インターフェイスがタグの付かないパケットを通過させるようにする場合は、通常通り **nameif** コマンドを設定できます。

サブインターフェイスの最大数は、プラットフォームによって変わります。プラットフォームごとのサブインターフェイスの最大数については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

例

次の例では、サブインターフェイスに VLAN 101 を割り当てます。

```
hostname(config)# interface gigabitethernet0/0.1
hostname(config-subif)# vlan 101
hostname(config-subif)# nameif dmz1
hostname(config-subif)# security-level 50
hostname(config-subif)# ip address 10.1.2.1 255.255.255.0
hostname(config-subif)# no shutdown
```

次の例では、VLAN を 102 に変更します。

```
hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 101
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0

hostname(config)# interface gigabitethernet0/0.1
hostname(config-interface)# vlan 102

hostname(config)# show running-config interface gigabitethernet0/0.1
interface GigabitEthernet0/0.1
   vlan 102
   nameif dmz1
   security-level 50
   ip address 10.1.2.1 255.255.255.0
```

関連コマンド

コマンド	説明
allocate-interface	セキュリティ コンテキストにインターフェイスおよびサブインターフェイスを割り当てます。
interface	インターフェイスを設定し、インターフェイス コンフィギュレーション モードに入ります。
show running-config interface	インターフェイスの現在のコンフィギュレーションを表示します。

vpdn group

VPDN グループを作成または編集し、PPPoE クライアントを設定するには、グローバル コンフィギュレーション モードで **vpdn group** コマンドを使用します。グループ ポリシーをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpdn group *group_name* {**localname** ***username*** | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

no vpdn group *group_name* {**localname** ***name*** | **request dialout pppoe | ppp authentication** {**chap** | **mschap** | **pap**}}

（注） PPPoE は、セキュリティ アプライアンスでフェールオーバーを設定している場合、およびマルチ コンテキスト モードや透過モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングルモードかつルーテッド モードの場合のみです。

シンタックスの説明

vpdn group *group_name*	VPDN グループの名前を指定します。
localname *username*	認証するユーザ名を VPDN グループにリンクします。この名前は、**vpdn username** コマンドで設定した名前と一致する必要があります。
request dialout pppoe	PPPoE のダイヤルアウト要求を許可することを指定します。
ppp authentication {chap | mschap | pap}	Point-to-Point Protocol（PPP; ポイントツーポイント プロトコル）接続で使用する認証プロトコルを指定します。Windows クライアントのダイヤルアップ ネットワークを設定するときに、どの認証プロトコル（PAP、CHAP、または MS-CHAP）を使用するかを選択します。クライアントで選択したプロトコルと同じものをセキュリティ アプライアンスでも使用する必要があります。Password Authentication Protocol（PAP; パスワード認証プロトコル）では、PPP のピアがお互いに認証し合います。このとき、クリア テキストのホスト名とユーザ名を渡します。Challenge Handshake Authentication Protocol（CHAP; チャレンジ ハンドシェーク認証プロトコル）の場合は、PPP のピアがアクセス サーバと通信して不正なアクセスを防ぎます。MS-CHAP は、CHAP を Microsoft が独自に拡張したものです。PIX Firewall は、MS-CHAP バージョン 1 だけをサポートしています(バージョン 2.0 はサポートしていません)。 ホストで認証プロトコルが設定されていない場合は、コンフィギュレーションに **ppp authentication** オプションを指定しないでください。

デフォルト

デフォルトの動作や値はありません。使用上のガイドラインを参照してください。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2.1	このコマンドが導入されました。

使用上のガイドライン

Virtual Private Dial-up Networking（VPDN; バーチャル プライベート ダイヤルアップ ネットワーク）は、遠く離れたダイヤルイン ユーザとプライベート ネットワークを結ぶときに使用するポイントツーポイント接続です。セキュリティ アプライアンスの VDPN は、レイヤ 2 トンネリング技術である PPPoE を使用して、リモート ユーザがパブリック ネットワークを経由してプライベート ネットワークにダイヤルアップ接続できるようにします。

PPPoE とは、Point-to-Point Protocol（PPP）over Ethernet の略です。PPP は、IP、IPX、ARA などのネットワーク レイヤ プロトコルと併用できるように設計されています。また、CHAP と PAP がセキュリティ メカニズムとして組み込まれています。

PPPoE 接続のセッション情報を表示するには、**show vpdn session pppoe** コマンドを使用します。**clear configure vpdn group** コマンドは、コンフィギュレーションからすべての **vpdn group** コマンドを削除して、アクティブな L2TP トンネルと PPPoE トンネルを停止します。**clear configure vpdn username** コマンドは、すべての **vpdn username** コマンドをコンフィギュレーションから削除します。

PPPoE は、PPP をカプセル化するので、PPP が認証を行うことと、VPN トンネル内で動作するクライアントのセッションで ECP と CCP が機能することが必要です。また、PPPoE では、PPP によって IP アドレスが割り当てられるので、DHCP を使用することはできません。

（注） PPPoE 用の VPDN グループを設定しないと、PPPoE では接続を確立できません。

PPPoE 用の VPDN グループを定義するには、まず **vpdn group** *group_name* **request dialout pppoe** コマンドを使用します。次に、インターフェイス コンフィギュレーション モードで **pppoe client vpdn group** コマンドを使用して、VPDN グループを特定のインターフェイスの PPPoE クライアントに関連付けます。

利用している ISP が認証を必要とする場合は、**vpdn group** *group_name* **ppp authentication** {**chap** | **mschap** | **pap**} コマンドで、ISP で使用されている認証プロトコルを選択します。

ISP が割り当てたユーザ名を VPDN グループと関連付けるには、**vpdn group** *group_name* **localname** *username* コマンドを使用します。

PPPoE 接続用のユーザ名とパスワードのペアを作成するには、**vpdn username** *username* password *password* コマンドを使用します。PPPoE 用に設定した VPDN グループのユーザ名と同じものを指定してください。

（注） ISP が CHAP または MS-CHAP を使用している場合は、ユーザ名のことをリモート システム名、パスワードのことを CHAP シークレットということがあります。

PPPoE クライアントの機能は、デフォルトでオフになっています。そのため、VPDN を設定したら、**ip address** *if_name* **pppoe** [**setroute**] コマンドで、PPPoE をイネーブルにしてください。**setroute** オプションは、デフォルトのルートがない場合に、デフォルト ルートを作成します。

PPPoE を設定するとすぐに、セキュリティ アプライアンスが、通信する PPPoE アクセス コンセントレータを探します。PPPoE 接続が正常、異常を問わず切断されると、セキュリティ アプライアンスは、通信する新しいアクセス コンセントレータを見つけようとします。

いったん PPPoE セッションを開始したら、次の **ip address** コマンドは使用しないでください。使用すると、PPPoE セッションが終了されます。

- **ip address outside pppoe**：新しい PPPoE セッションを開始しようとします。
- **ip address outside dhcp**：インターフェイスが DHCP コンフィギュレーションを取得するまでディセーブルになります。
- **ip address outside** *address netmask*：インターフェイスを、通常どおり初期化されたインターフェイスとして起動します。

例

次の例では、*telecommuters* という VPDN グループを作成し、PPPoE クライアントを設定します。

```
F1(config)# vpdn group telecommuters request dialout pppoe
F1(config)# vpdn group telecommuters localname user1
F1(config)# vpdn group telecommuters ppp authentication pap
F1(config)# vpdn username user1 password test1
F1(config)# interface GigabitEthernet 0/1
F1(config-subif)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての vpdn group コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show vpdn group *group_name*	VPDN グループのコンフィギュレーションを表示します。
vpdn username	PPPoE 接続用のユーザ名とパスワードのペアを作成します。

vpdn username

PPPoE 接続用のユーザ名とパスワードのペアを作成するには、グローバル コンフィギュレーション モードで **vpdn username** コマンドを使用します。

vpdn username *username* **password** *password* [**store-local**]

no vpdn username *username* **password** *password* [**store-local**]

（注） PPPoE は、セキュリティ アプライアンスでフェールオーバーを設定している場合、およびマルチ コンテキスト モードや透過モードではサポートされません。PPPoE がサポートされるのは、フェールオーバーを設定していない、シングルモードかつルーテッド モードの場合のみです。

シンタックスの説明

username	ユーザ名を指定します。
password	パスワードを指定します。
store-local	ユーザ名とパスワードをセキュリティ アプライアンスの NVRAM の特別な場所に保存します。Auto Update Server がセキュリティ アプライアンスにコンフィギュレーションを消去するコマンドを送信した後で接続が中断した場合に、セキュリティ アプライアンスが NVRAM のこの場所からユーザ名とパスワードを読み取って、アクセス コンセントレータとの認証をやり直します。

デフォルト

デフォルトの動作や値はありません。使用上のガイドラインを参照してください。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

VPDN のユーザ名は、**vpdn group** *group_name* **localname** *username* コマンドで指定した VPDN グループのユーザ名と同じでなければなりません。

clear configure vpdn username コマンドは、すべての **vpdn username** コマンドをコンフィギュレーションから削除します。

例

次の例では、*bob_smith* というユーザ名と *telecommuter*9/8 というパスワードを作成します。

```
F1(config)# vpdn username bob_smith password telecommuter9/8
```

関連コマンド

コマンド	説明
clear configure vpdn group	すべての vpdn group コマンドをコンフィギュレーションから削除します。
clear configure vpdn username	すべての vpdn username コマンドをコンフィギュレーションから削除します。
show vpdn group	VPDN グループのコンフィギュレーションを表示します。
vpdn group	VPDN グループを作成し、PPPoE クライアントを設定します。

vpn-access-hours

設定済みの時間範囲ポリシーをグループ ポリシーに関連付けるには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-access-hours** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、時間範囲値を別のグループ ポリシーから継承できます。値を継承しないようにするには、**vpn-access-hours none** コマンドを使用します。

vpn-access hours value {*time-range*} **| none**

no vpn-access hours

シンタックスの説明

none	VPN アクセス時間にヌル値を設定することで、時間範囲ポリシーを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
time-range	設定済みの時間範囲ポリシーの名前を指定します。

デフォルト

無制限です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

例

次の例では、824 と呼ばれる時間範囲ポリシーに FirstGroup という名前のグループ ポリシーを関連付ける方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-access-hours 824
```

関連コマンド

コマンド	説明
time-range	ネットワークにアクセスする曜日および 1 日の時間を設定します（開始日と終了日を含む）。

vpn-addr-assign

IP アドレスをリモートアクセス クライアントに割り当てる方法を指定するには、グローバル コンフィギュレーション モードで **vpn-addr-assign** コマンドを使用します。アトリビュートをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。設定されている Vpn アドレスの割り当て方法をセキュリティ アプライアンスからすべて削除するには、引数なしで、このコマンドの **no** 形式を使用します。

vpn-addr-assign {**aaa | dhcp | local**}

no vpn-addr-assign [**aaa | dhcp | local**]

シンタックスの説明

aaa	外部 AAA 認証サーバから IP アドレスを取得します。
dhcp	DHCP 経由で IP アドレスを取得します。
local	内部認証サーバから IP アドレスを割り当て、トンネル グループに関連付けます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

DHCP を選択する場合は、**dhcp-network-scope** コマンドを使用して、DHCP サーバが使用できる IP アドレスの範囲を定義する必要があります。

ローカルを選択する場合は、**ip-local-pool** コマンドを使用して、使用する IP アドレスの範囲を定義する必要があります。**vpn-framed-ip-address** コマンドおよび **vpn-framed-netmask** コマンドを使用して、個々のユーザに IP アドレスとネットマスクを割り当てます。

AAA を選択する場合、設定済みの RADIUS サーバのいずれかから IP アドレスを取得します。

例

次の例では、アドレスの割り当て方法として DHCP を設定する方法を示します。

```
hostname(config)# vpn-addr-assign dhcp
```

関連コマンド

コマンド	説明
dhcp-network-scope	セキュリティ アプライアンス DHCP サーバがグループ ポリシーのユーザにアドレスを割り当てるときに使用する必要がある IP アドレスの範囲を指定します。
ip-local-pool	ローカル IP アドレス プールを作成します。
vpn-framed-ip-address	IP アドレスを指定して、特定のユーザに割り当てます。
vpn-framed-ip-netmask	ネットマスクを指定して、特定のユーザに割り当てます。

vpn-filter

VPN 接続に使用する ACL の名前を指定するには、グループ ポリシーまたはユーザ名モードで **vpn-filter** コマンドを使用します。**vpn-filter none** コマンドを発行して作成したヌル値を含む ACL を削除するには、このコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できます。値を継承しないようにするには、**vpn-filter none** コマンドを使用します。

ACL を設定して、このユーザまたはグループ ポリシーについて、さまざまなタイプのトラフィックを許可または拒否します。**vpn-filter** コマンドを使用して、これらの ACL を適用します。

vpn-filter {**value** *ACL name* | **none**}

no vpn-filter

シンタックスの説明

none	アクセス リストがないことを指定します。ヌル値を設定して、アクセス リストを拒否します。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACL name*	設定済みアクセス リストの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN は、**vpn-filter** コマンドで定義された ACL を使用しません。

例

次の例では、FirstGroup という名前のグループ ポリシーの acl_vpn と呼ばれるアクセス リスト名を実行するフィルタを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-filter value acl_vpn
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成します。または、ダウンロード可能なアクセス リストを使用します。

vpn-framed-ip-address

特定のユーザに割り当てる IP アドレスを指定するには、ユーザ名モードで **vpn-framed-ip-address** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip-address {*ip_address*}

no vpn-framed-ip-address

シンタックスの説明

ip_address	このユーザの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、anyuser という名前のユーザに 10.92.166.7 という IP アドレスを設定する方法を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-address 10.92.166.7
```

関連コマンド

コマンド	説明
vpn-framed-ip-netmask	このユーザのサブネット マスクを指定します。

vpn-framed-ip-netmask

特定のユーザに割り当てるサブネット マスクを指定するには、ユーザ名モードで **vpn-framed-ip-netmask** コマンドを使用します。サブネットマスクを削除するには、このコマンドの **no** 形式を使用します。

vpn-framed-ip-netmask {*netmask*}

no vpn-framed-ip-netmask

シンタックスの説明

netmask	このユーザのサブネット マスクを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、anyuser という名前のユーザに 255.255.255. 254 というサブネット マスクを設定する方法を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-framed-ip-netmask 255.255.255.254
```

（注） RADIUS がサブネット マスクだけを返す場合、認証は独自のサブネット ネットマスクを持つローカル プールからの IP アドレスを使用します。RADIUS からのマスクは使用しません。これを防止するには、RADIUS からネットマスクと IP アドレスの両方を返します。

関連コマンド

コマンド	説明
vpn-framed-ip-address	このユーザの IP アドレスを指定します。

vpn-group-policy

ユーザに設定済みのグループ ポリシーからアトリビュートを継承させるには、ユーザ名コンフィギュレーション モードで **vpn-group-policy** コマンドを使用します。ユーザ コンフィギュレーションからグループ ポリシーを削除するには、このコマンドの **no** 形式を使用します。このコマンドを使用すると、ユーザがユーザ名レベルで設定していないアトリビュートを継承できます。

vpn-group-policy {*group-policy name*}

no vpn-group-policy {*group-policy name*}

シンタックスの説明

group-policy name	グループ ポリシーの名前を指定します。

デフォルト

デフォルトでは、VPN ユーザにはグループ ポリシーのアソシエーションはありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

アトリビュートをユーザ名モードで利用できる場合、ユーザ名モードで設定することにより、特定のユーザに対するグループ ポリシーのアトリビュートの値を上書きできます。

例

次の例では、FirstGroup という名前のグループ ポリシーからアトリビュートを使用するように anyuser という名前のユーザを設定する方法を示します。

```
hostname(config)# username anyuser attributes
hostname(config-username)# vpn-group-policy FirstGroup
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーをセキュリティ アプライアンスのデータベースに追加します。
group-policy attributes	グループ ポリシーの AVP を設定できるグループ ポリシー アトリビュート モードに入ります。
username	ユーザをセキュリティ アプライアンスのデータベースに追加します。
username attributes	ユーザ名アトリビュート モードに入って、個々のユーザの AVP を設定できるようにします。

vpn-idle-timeout

ユーザのタイムアウト期間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-idle-timeout** コマンドを使用します。この期間中に接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、タイムアウト値を別のグループ ポリシーから継承できます。値を継承しないようにするには、**vpn-idle-timeout none** コマンドを使用します。

vpn-idle-timeout {*minutes* **| none}**

no vpn-idle-timeout

シンタックスの説明

minutes	タイムアウト期間を分単位で指定します。1 ～ 35791394 の整数を使用します。
none	無制限のアイドル タイムアウト期間を許容します。アイドル タイムアウトにヌル値を設定して、アイドル タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

デフォルト

30 分。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、「FirstGroup」という名前のグループ ポリシーに対して 15 分の VPN アイドル タイムアウトを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-idle-timeout 30
```

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-session-timeout	VPN 接続に許可されている最大時間を設定します。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

vpn load-balancing

VPN ロードバランシングおよび関連機能を設定できる VPN ロードバランシング モードに入るには、グローバル コンフィギュレーション モードで **vpn load-balancing** コマンドを使用します。

vpn load-balancing

（注） ASA Models 5540 および 5520 だけが、VPN ロードバランシングをサポートします。VPN ロードバランシングには、有効な 3DES ライセンスまたは AES ライセンスも必要です。セキュリティ アプライアンスは、ロードバランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。有効な 3DES ライセンスまたは AES ライセンスが検出されなかった場合、セキュリティ アプライアンスはロードバランシングをイネーブルにしません。また、ライセンスで許可されていない限り、ロードバランシング システムが 3DES の内部設定を行わないようにします。

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション モード	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

vpn load-balancing コマンドを使用して、VPN ロードバランシング モードに入ります。次のコマンドは、VPN ロードバランシング モードで使用できます。

cluster encryption

cluster ip address

cluster key

cluster port

interface

nat

participate

priority

詳細については、個々のコマンドの説明を参照してください。

例

次に **vpn load-balancing** コマンドの例を示します。プロンプト内の変化に注意してください。

```
hostname(config)# vpn load-balancing
hostname(config-load-balancing)#
```

次に、クラスタのパブリック インターフェイスを「test」として、クラスタのプライベート インターフェイスを「foo」として指定するインターフェイス コマンドを含む、VPN ロードバランシング コマンド シーケンスの例を示します。

```
hostname(config)# interface GigabitEthernet 0/1
hostname(config-if)# ip address 209.165.202.159 255.255.255.0
hostname(config)# nameif test
hostname(config)# interface GigabitEthernet 0/2
hostname(config-if)# ip address 209.165.201.30 255.255.255.0
hostname(config)# nameif foo
hostname(config)# vpn load-balancing
hostname(config-load-balancing)# nat 192.168.10.10
hostname(config-load-balancing)# priority 9
hostname(config-load-balancing)# interface lbpublic test
hostname(config-load-balancing)# interface lbprivate foo
hostname(config-load-balancing)# cluster ip address 209.165.202.224
hostname(config-load-balancing)# cluster key 123456789
hostname(config-load-balancing)# cluster encryption
hostname(config-load-balancing)# cluster port 9023
hostname(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	ロードバランシング実行時のコンフィギュレーションを削除して、ロードバランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示します。
show vpn load-balancing	VPN ロードバランシング実行時の統計情報を表示します。

vpn-nac-exempt

ポスチャ確認を免除するリモート コンピュータのタイプのリストにエントリを追加するには、グループ ポリシー コンフィギュレーション モードで **vpn-nac-exempt** コマンドを使用します。

vpn-nac-exempt os "*os name*" [**filter** {*acl-name* | **none**}] [**disable**]

継承をディセーブルにし、すべてのホストをポスチャ確認の対象にするには、**vpn-nac-exempt** のすぐ後ろに **none** キーワードを入力します。

vpn-nac-exempt none

免除リストからエントリを削除するには、このコマンドの **no** 形式を使用し、削除するエントリのオペレーティング システム（および ACL）を指定します。

no vpn-nac-exempt [os "*os name*"] [**filter** {*acl-name* | **none**}] [**disable**]

このグループ ポリシーの免除リストにある全エントリを削除し、デフォルトのグループ ポリシーの免除リストを継承するには、キーワードを指定せずにこのコマンドの **no** 形式を使用します。

no vpn-nac-exempt

シンタックスの説明

acl-name	セキュリティ アプライアンスのコンフィギュレーションに含まれる ACL の名前。
disable	免除リストのエントリを削除せずにディセーブルにします。
filter	コンピュータのオペレーティング システムの名前が *os name* に一致したときに、トラフィックをフィルタリングするために ACL を適用します。
none	このキーワードを **vpn-nac-exempt** のすぐ後ろに入力した場合は、継承がディセーブルになり、すべてのホストがポスチャ確認の対象になります。 **filter** のすぐ後ろに入力した場合は、ACL を指定しないことを示します。
OS	オペレーティング システムのポスチャ確認を免除します。
os name	オペレーティング システムの名前。引用符は、オペレーティング システムの名前にスペースが入っている場合のみ必要です（Windows XP など）。

デフォルト

デフォルトでは、免除リストは空になっています。

フィルタ アトリビュートのデフォルトの値は none です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　ポスチャ確認を免除するリモート ホストのオペレーティング システム（および ACL）ごとに **vpn-nac-exempt** を 1 回入力します。

例

次の例では、Windows XP を実行しているすべてのホストを、ポスチャ確認を免除するコンピュータのリストに追加します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows XP"
hostname(config-group-policy)
```

次の例では、Windows 98 を実行しているホストをすべて免除し、これらのホストからのトラフィックに acl-1 という ACL を適用します。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次の例では、上と同じエントリを免除リストに追加していますが、ディセーブルにしています。

```
hostname(config-group-policy)# vpn-nac-exempt os "Windows 98" filter acl-1 disable
hostname(config-group-policy)
```

次の例では、同じエントリを、ディセーブルかどうかにかかわらず、免除リストから削除しています。

```
hostname(config-group-policy)# no vpn-nac-exempt os "Windows 98" filter acl-1
hostname(config-group-policy)
```

次の例では、継承をディセーブルにして、すべてのホストをポスチャ確認の対象にしています。

```
hostname(config-group-policy)# no vpn-nac-exempt none
hostname(config-group-policy)
```

次の例では、免除リストからすべてのエントリを削除しています。

```
hostname(config-group-policy)# no vpn-nac-exempt
hostname(config-group-policy)
```

関連コマンド

コマンド	説明
debug eap	NAC メッセージをデバッグするための EAP イベントのロギングをイネーブルにします。
debug eou	NAC メッセージをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac	グループ ポリシーでネットワーク アドミッション コントロールをイネーブルにします。

vpn-sessiondb logoff

すべての VPN セッションまたは選択した VPN セッションをログオフするには、グローバル コンフィギュレーション モードで **vpn-sessiondb logoff** コマンドを使用します。

vpn-sessiondb logoff {**remote | l2l | webvpn | email-proxy | protocol** *protocol-name* | **name** *username* | **ipaddress** *IPaddr* | **tunnel-group** *groupname* | **index** *indexnumber* | **all**}

シンタックスの説明

all	すべての VPN セッションをログオフします。
email-proxy	すべての電子メール プロキシ セッションをログオフします。
index *indexnumber*	インデックス番号ごとにシングル セッションをログオフします。セッションのインデックス番号を指定します。
ipaddress *IPaddr*	指定した IP アドレスのセッションをログオフします。
l2l	すべての LAN-to-LAN セッションをログオフします。
name *username*	指定したユーザ名のセッションをログオフします。
protocol *protocol-name*	指定したプロトコルのセッションをログオフします。プロトコルには、次の種類があります。 IKE　POP3S IMAP4S　SMTPS IPSec　userHTTPS IPSecLAN2LAN　vcaLAN2LAN IPSecLAN2LANOverNatT IPSecOverNatT IPSecoverTCP IPSecOverUDP
remote	すべてのリモートアクセス セッションをログオフします。
tunnel-group *groupname*	指定したトンネル グループのセッションをログオフします。
webvpn	すべての WebVPN セッションをログオフします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、すべてのリモートアクセス セッションをログオフする方法を示します。

```
hostname# vpn-sessiondb logoff remote
```

次の例では、すべての IPSec セッションをログオフする方法を示します。

```
hostname# vpn-sessiondb logoff protocol IPSec
```

vpn-sessiondb max-session-limit

VPN セッションをセキュリティ アプライアンスが許可しているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-session-limit** コマンドを使用します。セッションの制限値を削除するには、このコマンドの **no** 形式を使用します。現在の設定を上書きするには、このコマンドを再度使用します。

vpn-sessiondb max-session-limit {*session-limit*}

no **vpn-sessiondb max-session-limit**

シンタックスの説明

session-limit	許容する VPN セッションの最大数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは IPSec VPN セッションに適用されます。

例

次の例では、VPN セッションの最大制限値である 450 に設定する方法を示します。

```
hostname# vpn-sessiondb max-session-limit 450
```

関連コマンド

コマンド	説明
vpn-sessiondb logoff	IPsec VPN セッションおよび WebVPN セッションのすべてまたは特定のタイプをログオフします。
vpn-sessiondb max-webvpn-session-limit	WebVPN セッションの最大数を設定します。

vpn-sessiondb max-webvpn-session-limit

WebVPN セッションをセキュリティ アプライアンスが許可しているよりも小さい値に制限するには、グローバル コンフィギュレーション モードで **vpn-sessiondb max-webvpn-session-limit** コマンドを使用します。セッションの制限値を削除するには、このコマンドの **no** 形式を使用します。現在の設定を上書きするには、このコマンドを再度使用します。

vpn-sessiondb max-webvpn-session-limit {*session-limit*}

no vpn-sessiondb max-webvpn-session-limit

シンタックスの説明

session-limit	許容する WebVPN セッションの最大数を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは WebVPN セッションに適用されます。

例

次の例では、WebVPN セッションの最大制限値である 75 に設定する方法を示します。

```
hostname (config)# vpn-sessiondb max-webvpn-session-limit 75
```

関連コマンド

コマンド	説明
vpn-sessiondb logoff	IPsec VPN セッションおよび WebVPN セッションのすべてまたは特定のタイプをログオフします。
vpn-sessiondb max-vpn-session-limit	VPN セッションの最大数を設定します。

vpn-session-timeout

VPN 接続に許可される最大時間を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-session-timeout** コマンドを使用します。この期間が終了すると、セキュリティ アプライアンスは接続を終了します。

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、タイムアウト値を別のグループ ポリシーから継承できます。値を継承しないようにするには、**vpn-session-timeout none** コマンドを使用します。

vpn-session-timeout {*minutes* **| none}**

no vpn-session-timeout

シンタックスの説明

minutes	タイムアウト期間を分単位で指定します。1 ～ 35791394 の整数を使用します。
none	無制限のセッション タイムアウト期間を許容します。セッション タイムアウトにヌル値を設定して、セッション タイムアウトを拒否します。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

例

次の例では、FirstGroup という名前のグループ ポリシーに対して 180 分の VPN セッション タイムアウトを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-session-timeout 180
```

関連コマンド

group-policy	グループ ポリシーを作成または編集します。
vpn-idle-timeout	ユーザ タイムアウト期間を設定します。この期間中に接続上で通信アクティビティがまったくなかった場合、セキュリティ アプライアンスは接続を終了します。

vpn-simultaneous-logins

ユーザに許容される同時ログイン数を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-simultaneous-logins** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、値を別のグループ ポリシーから継承できます。ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

vpn-simultaneous-logins {*integer***}**

no vpn-simultaneous-logins

シンタックスの説明

integer	0 ～ 2147483647 の数値です。

デフォルト

デフォルトの同時ログイン数は 3 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。

使用上のガイドライン

ログインをディセーブルにしてユーザのアクセスを禁止するには、0 を入力します。

例

次の例では、FirstGroup という名前のグループ ポリシーに対して最大 4 つの同時ログインを許可する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-simultaneous-logins 4
```

vpn-tunnel-protocol

VPN トンネルのタイプ（IPSec、L2TP over IPSec、または WebVPN）を設定するには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **vpn-tunnel-protocol** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpn-tunnel-protocol {webvpn | l2tp-ipsec | IPSec}

no vpn-tunnel-protocol [webvpn | l2tp-ipsec | IPSec]

シンタックスの説明

IPSec	2 つのピア間（リモートアクセス クライアントまたはその他のセキュアなゲートウェイ）で IPSec トンネルをネゴシエートします。認証、暗号化、カプセル化、およびキー管理を管理するセキュリティ結合を作成します。
l2tp-ipsec	L2TP 接続のために IPSec トンネルをネゴシエートします。
webvpn	HTTPS 対応の Web ブラウザを経由してリモート ユーザに VPN サービスを提供します。クライアントは不要です。

デフォルト

IPSec です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)(1)	このコマンドが導入されました。
7.2(1)	**l2tp-ipsec** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用して 1 つ以上のトンネリング モードを設定します。VPN トンネルを越えて接続するには、ユーザに対して少なくとも 1 つのトンネリング モードを設定する必要があります。

例

次の例では、「FirstGroup」という名前のグループ ポリシーに対して WebVPN および IPSec トンネリング モードを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# vpn-tunnel-protocol webvpn
hostname(config-group-policy)# vpn-tunnel-protocol IPSec
```

vpnclient connect

設定済みサーバへの Easy VPN Remote 接続の確立を試行するには、グローバル コンフィギュレーション モードで **vpnclient connect** コマンドを使用します。

vpnclient connect

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA モデル 5505 のみに適用されます。

例

次の例は、設定済み EasyVPN サーバへの Easy VPN Remote 接続の確立を試行する方法を示しています。

```
hostname(config)# vpnclient connect
hostname(config)#
```

vpnclient disconnect

Easy VPN Remote 接続を切断するには、グローバル コンフィギュレーション モードで **vpnclient disconnect** コマンドを使用します。

vpnclient disconnect

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
EXEC	•	—	•	—	—
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA モデル 5505 のみに適用されます。

例

次の例は、Easy VPN Remote 接続を切断する方法を示しています。

```
hostname(config)# vpnclient disconnect
hostname(config)#
```

vpnclient enable

Easy VPN Remote 機能をイネーブルにするには、グローバル コンフィギュレーション モードで **vpnclient enable** コマンドを使用します。Easy VPN Remote 機能をディセーブルにするには、このコマンドの ***no*** 形式を使用します。

vpnclient enable

no vpnclient enable

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA 5505 のみに適用されます。

vpnclient enable コマンドを入力すると、ASA 5505 は Easy VPN ハードウェア クライアント（「Easy VPN Remote」とも呼ばれる）として機能します。**no vpnclient enable** コマンドを入力すると、Easy VPN サーバ（「ヘッドエンド」とも呼ばれる）として機能します。クライアントまたはサーバとしてのみ機能します。

例

次の例は、Easy VPN Remote 機能をイネーブルにする方法を示しています。

```
hostname(config)# vpnclient enable
hostname(config)#
```

次の例は、Easy VPN Remote 機能をディセーブルにする方法を示しています。

```
hostname(config)# no vpnclient enable
hostname(config)#
```

vpnclient ipsec-over-tcp

TCP カプセル化 IPSec を使用するように、Easy VPN ハードウェア クライアントとして稼働している ASA 5505 を設定するには、グローバル コンフィギュレーション モードで **vpnclient ipsec-over-tcp** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient ipsec-over-tcp [**port** *tcp_port*]

no vpnclient ipsec-over-tcp

シンタックスの説明

port	（オプション）特定のポートを使用するように指定します。
tcp_port	（***port*** キーワードを指定した場合は必須）TCP カプセル化 IPSec トンネルに使用する TCP ポート番号を指定します。

デフォルト

このコマンドでポート番号が指定されていない場合、Easy VPN Remote 接続ではポート 10000 が使用されます。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN ハードウェア クライアント（「Easy VPN Remote」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。

デフォルトでは、Easy VPN クライアントおよびサーバは、User Datagram Protocol（UDP; ユーザ データグラム プロトコル）パケットをカプセル化します。特定のファイアウォール規則が設定されているような環境や、NAT デバイスおよび PAT デバイスでは、UDP が禁止されています。そのような環境で標準の Encapsulating Security Protocol（ESP、プロトコル 50）または Internet Key Exchange（IKE; インターネット キー エクスチェンジ、UDP 500）を使用するには、TCP パケット内の IPSec をカプセル化してセキュアなトンネリングをイネーブルにするように、クライアントとサーバを設定する必要があります。ただし、UDP が許可されている環境では、IPSec over TCP を設定すると、不要なオーバーヘッドが発生します。

TCP カプセル化 IPSec を使用するように ASA 5505 を設定する場合は、次のコマンドを入力して、大きいパケットを外部インターフェイスに送信するようにします。

```
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

このコマンドは、カプセル化されたヘッダーから Don't Fragment（DF）ビットを消去します。DF ビットとは、パケットのフラグメント化が可能かどうかを判断する、IP ヘッダー内のビットです。このコマンドにより、Easy VPN ハードウェア クライアントは、MTU サイズよりも大きいパケットを送信できます。

例

次の例では、デフォルト ポート 10000 を使用して TCP カプセル化 IPSec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きいパケットを送信できるようにする方法を示しています。

```
hostname(config)# vpnclient ipsec-over-tcp
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

次の例では、ポート 10501 を使用して TCP カプセル化 IPSec を使用するように Easy VPN ハードウェア クライアントを設定し、外部インターフェイスを介して大きいパケットを送信できるようにする方法を示しています。

```
hostname(config)# vpnclient ipsec-over-tcp port 10501
hostname(config)# crypto ipsec df-bit clear-df outside
hostname(config)#
```

vpnclient mac-exempt

Easy VPN Remote 接続の背後にあるデバイスに対して個々のユーザ認証要件を免除するには、グローバル コンフィギュレーション モードで **vpnclient mac-exempt** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient mac-exempt *mac_addr_1 mac_mask_1* [*mac_addr_2 mac_mask_2...mac_addr_n mac_mask_n*]

no vpnclient mac-exempt

シンタックスの説明

mac_addr_1	ドット付き 16 進表記の MAC アドレスで、個々のユーザ認証を免除するデバイスのメーカーおよびシリアル番号を指定します。デバイスが複数の場合は、各 MAC アドレスをスペースで区切り、対応するネットワーク マスクを指定します。 MAC アドレスの最初の 6 文字はデバイスのメーカーを識別し、最後の 6 文字はシリアル番号です。最後の 24 ビットは、16 進形式での装置のシリアル番号です。
mac_mask_1	MAC アドレスに対応するネットワーク マスク。ネットワーク マスクと後続の MAC アドレスおよびネットワーク マスクのペアは、スペースで区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA モデル 5505 のみに適用されます。

Cisco IP Phone、無線アクセス ポイント、プリンタなどのデバイスは認証を実行できないため、個々の装置認証がイネーブルになっている場合でも認証しません。個々のユーザ認証がイネーブルになっている場合は、このコマンドを使用して、これらのデバイスの認証を免除できます。デバイスに対する個々のユーザ認証の免除は、「デバイス パススルー」とも呼ばれます。

このコマンドでは、MAC アドレスと MAC マスクは、3 桁の 16 進数をピリオドで区切って指定します。たとえば、MAC マスク ffff.ffff.ffff は、指定された MAC アドレスに対応します。すべてゼロの MAC マスクは対応する MAC アドレスがないことを示します。また、ffff.ff00.0000 という MAC マスクは同じメーカーで製造されたすべてのデバイスに対応します。

例

Cisco IP Phone のメーカー ID は 00036b です。したがって、次のコマンドでは、すべての Cisco IP Phone（今後追加する Cisco IP Phone も含む）が免除されます。

```
hostname(config)# vpnclient mac-exempt 0003.6b00.0000 ffff.ff00.0000
hostname(config)#
```

次の例では、特定の Cisco IP Phone が免除されるため、セキュリティは向上しますが、柔軟性は低下します。

```
hostname(config)# vpnclient mac-exempt 0003.6b54.b213 ffff.ffff.ffff
hostname(config)#
```

vpnclient management

管理アクセス用に Easy VPN ハードウェア クライアントへの IPSec トンネルを生成するには、グローバル コンフィギュレーション モードで **vpnclient management** コマンドを使用します。

vpnclient management tunnel *ip_addr_1 ip_mask_1* [*ip_addr_2 ip_mask_2...ip_addr_n ip_mask_n*]

vpnclient management ***clear***

このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。この形式では、**split-tunnel-policy** コマンドと **split-tunnel-network-list** コマンドに従って、管理専用の IPSec トンネルが設定されます。

no vpnclient management

シンタックスの説明

clear	通常のルーティングを使用して、企業ネットワークから ASA 5505（Easy VPN クライアントとして稼働）の外部インターフェイスへの管理アクセスを可能にします。このオプションでは、管理トンネルは作成されません。 **(注)** クライアントとインターネットとの間で NAT デバイスが動作している場合に、このオプションを使用します。
ip_addr	ホストまたはネットワークの IP アドレス。Easy VPN ハードウェア クライアントからこの IP アドレスへの管理トンネルを構築します。この引数は **tunnel** キーワードと共に使用します。1 つまたは複数の IP アドレスおよび対応するネットワーク マスクを指定します。複数の場合は、各 IP アドレスをスペースで区切ります。
ip_mask	IP アドレスに対応するネットワーク マスク。ネットワーク マスクと後続の IP アドレスおよびネットワーク マスクのペアは、スペースで区切ります。
tunnel	企業ネットワークから ASA 5505（Easy VPN クライアントとして稼働）の外部インターフェイスへの管理アクセス専用の IPSec トンネルを自動的にセットアップします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン　このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。次の各コマンドが ASA 5505 コンフィギュレーションに含まれていることを前提としています。

vpnclient server コマンド（ピアを指定する）

vpnclient mode コマンド（クライアント モード（PAT）またはネットワーク拡張モードを指定する）

次のいずれかのコマンド

- **vpnclient vpngroup** コマンド（Easy VPN サーバで認証に使用するトンネル グループと IKE 事前共有キーを指定する）
- **vpnclient trustpoint** コマンド（認証に使用する RSA 証明書を識別するトラストポイントを指定する）

vpnclient enable コマンド（ASA 5505 を Easy VPN クライアントとしてイネーブルにする）

（注）　NAT デバイス上でスタティック NAT マッピングを追加しないと、NAT デバイスの背後にある ASA 5505 のパブリック アドレスにはアクセスできません。

例　次の例は、ASA 5505 の外部インターフェイスからホスト（IP アドレス / マスクが 192.168.10.10 255.255.255.0 というの組み合せのホスト）への IPSec トンネルを生成する方法を示しています。

```
hostname(config)# vpnclient management tunnel 192.168.10.0 255.255.255.0
hostname(config)#
```

次の例は、IPSec を使用せずに、ASA 5505 の外部インターフェイスへの管理アクセスを可能にする方法を示しています。

```
hostname(config)# vpnclient management clear
hostname(config)#
```

vpnclient mode

クライアント モードまたはネットワーク拡張モードの Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient mode** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient mode {**client-mode** | **network-extension-mode**}

no vpnclient mode

シンタックスの説明

client-mode	クライアント モード（PAT）を使用するように Easy VPN Remote 接続を設定します。
network-extension-mode	Network Extension Mode（NEM; ネットワーク拡張モード）を使用するように Easy VPN Remote 接続を設定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。Easy VPN クライアントは、クライアント モードまたは NEM のいずれかの動作モードをサポートします。動作モードは、企業ネットワークからトンネル経由で内部ホスト（Easy VPN クライアントから見た場合の内部ホスト）にアクセスできるかどうかによって決まります。Easy VPN クライアントにはデフォルトのモードがないので、接続を行う前に必ず動作モードを指定します。

- クライアント モードでは、Easy VPN クライアントは内部ホストからのすべての VPN トラフィックに対して Port Address Translation（PAT; ポート アドレス変換）を実行します。このモードでは、ハードウェア クライアント（デフォルトの RFC 1918 アドレスが割り当てられている）の内部アドレスまたは内部ホストに対する IP アドレス管理は必要ありません。PAT により、企業ネットワークから内部ホストにアクセスすることはできません。
- NEM では、内部ネットワークおよび内部インターフェイス上のすべてのノードに、企業ネットワークでルーティング可能なアドレスが割り当てられます。企業ネットワークからトンネル経由で内部ホストにアクセスできます。内部ネットワーク上のホストには、アクセス可能なサブネットからの IP アドレスが（スタティックに、または DHCP によって）割り当てられます。ネットワーク拡張モードでは、PAT は VPN トラフィックに適用されません。

（注） Easy VPN ハードウェア クライアントが NEM を使用し、セカンダリ サーバに接続している場合は、各ヘッドエンド デバイスで **crypto map set reverse-route** コマンドを使用して、Reverse Route Injection（RRI; 逆ルート注入）によるリモート ネットワークのダイナミックな通知を設定します。

例

次の例は、クライアント モードで Easy VPN Remote 接続を設定する方法を示しています。

```
hostname(config)# vpnclient mode client-mode
hostname(config)#
```

次の例は、NEM で Easy VPN Remote 接続を設定する方法を示しています。

```
hostname(config)# vpnclient mode network-extension-mode
hostname(config)#
```

vpnclient nem-st-autoconnect

NEM およびスプリット トンネリングが設定されている場合、IPSec データ トンネルを自動的に開始するように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient nem-st-autoconnect** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient nem-st-autoconnect

no vpnclient nem-st-autoconnect

シンタックスの説明

このコマンドには、キーワードも引数もありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。

vpnclient nem-st-autoconnect コマンドを入力する前に、ハードウェア クライアントのネットワーク拡張モードがイネーブルになっていることを確認します。ネットワーク拡張モードにより、ハードウェア クライアントは、VPN トンネルを介したリモート プライベート ネットワークに対して、ルーティング可能なネットワークを 1 つ提示できます。IPSec は、ハードウェア クライアントの背後にあるプライベート ネットワークからセキュリティ アプライアンスの背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、セキュリティ アプライアンスの背後にある装置は、ハードウェア クライアントの背後にある、トンネルを介したプライベート ネットワークに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。ハードウェア クライアントがトンネルを開始する必要があります。トンネルがアップの状態になった後は、どちらの側からもデータ交換を開始できます。

（注） また、ネットワーク拡張モードをイネーブルにするように Easy VPN サーバを設定する必要があります。そのためには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。

ネットワーク拡張モードでは、スプリット トンネリングが設定されている場合を除き、IPSec データ トンネルが自動的に開始されて持続します。

例

次の例は、スプリット トンネリングが設定されたネットワーク拡張モードで自動的に接続するように Easy VPN Remote 接続を設定する方法を示しています。グループ ポリシー FirstGroup のネットワーク拡張モードはイネーブルになっています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# nem enable
hostname(config)# vpnclient nem-st-autoconnect
hostname(config)#
```

関連コマンド

コマンド	説明
nem	ハードウェア クライアントのネットワーク拡張モードをイネーブルにします。

vpnclient server-certificate

証明書マップで指定された特定の証明書を持つ Easy VPN サーバへの接続のみを受け入れるように Easy VPN Remote 接続を設定するには、グローバル コンフィギュレーション モードで **vpnclient server-certificate** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient server-certificate *certmap_name*

no vpnclient server-certificate

シンタックスの説明

certmap_name	受け入れ可能な Easy VPN サーバ証明書を特定するための証明書マップの名前を指定します。最大長は 64 文字です。

デフォルト

デフォルトでは、Easy VPN サーバ証明書のフィルタリングはディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA モデル 5505 のみに適用されます。

このコマンドを使用して、Easy VPN サーバ証明書のフィルタリングをイネーブルにします。証明書マップ自体は、crypto ca certificate map コマンドおよび crypto ca certificate chain コマンドを使用して定義します。

例

次の例は、homeservers という名前の証明書マップを持つ Easy VPN サーバへの接続のみをサポートするように Easy VPN Remote 接続を設定する方法を示しています。

```
hostname(config)# vpnclient server-certificate homeservers
hostname(config)#
```

関連コマンド

コマンド	説明
certificate	指定された証明書を追加します。
vpnclient trustpoint	Easy VPN Remote 接続で使用する RSA ID 証明書を設定します。

vpnclient server

Easy VPN Remote 接続でプライマリおよびセカンダリ IPSec サーバを設定するには、グローバル コンフィギュレーション モードで **vpnclient server** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient server *ip_primary_address* [*ip_secondary_address_1 ... ipsecondary_address_10*]

no vpnclient server

シンタックスの説明

ip_primary_address	プライマリ Easy VPN（IPSec）サーバの IP アドレスまたは DSN 名。すべての ASA または VPN 3000 コンセントレータ シリーズが Easy VPN サーバとして機能できます。
ip_secondary_address_n	（オプション）最大 10 台のバックアップ Easy VPN サーバの IP アドレスまたは DNS 名のリスト。スペースを使用して、リスト内の項目を区切ります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA モデル 5505 のみに適用されます。

接続を確立する前に、サーバを設定しておく必要があります。**vpnclient server** コマンドは、IPv4 アドレス、名前データベース、または DNS 名をサポートし、この順序でアドレスを解決します。

サーバの IP アドレスまたはホスト名のいずれかを使用できます。

例

次の例では、名前 headend-1 をアドレス 10.10.10.10 に関連付け、**vpnclient server** コマンドを使用して headend-dns.domain.com（プライマリ）、headend-1（セカンダリ）、および 192.168.10.10（セカンダリ）の 3 台のサーバを指定しています。

```
hostname(config)# names
hostname(config)# 10.10.10.10 headend-1
hostname(config)# vpnclient server headend-dns.domain.com headend-1 192.168.10.10
hostname(config)#
```

次の例は、VPN クライアントに対し、IP アドレスが 10.10.10.15 のプライマリ IPSec サーバ、IP アドレスが 10.10.10.30 および 192.168.10.45 のセカンダリ サーバを設定する方法を示しています。

```
hostname(config)# vpnclient server 10.10.10.15 10.10.10.30 192.168.10.10
hostname(config)#
```

vpnclient trustpoint

Easy VPN Remote 接続で使用する RSA ID 証明書を設定するには、グローバル コンフィギュレーション モードで **vpnclient trustpoint** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient trustpoint *trustpoint_name* [***chain***]

no vpnclient trustpoint

シンタックスの説明

chain	証明書チェーン全体を送信します。
trustpoint_name	認証に使用する RSA 証明書を識別するトラストポイントの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA モデル 5505 のみに適用されます。また、このコマンドが適用されるのは、デジタル証明書を使用している場合だけです。

crypto ca trustpoint コマンドを使用してトラストポイントを定義します。トラストポイントは、CA によって発行された証明書に基づいて CA の識別情報を表し、また、装置の識別情報を表すことがあります。トラストポイント サブモード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。このパラメータでは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが CA から証明書を取得する方法、および CA によって発行されるユーザ証明書の認証ポリシーを指定します。

例

次の例は、central という名前の ID 証明書を使用し、証明書チェーン全体を送信するように Easy VPN Remote 接続を設定する方法を示しています。

```
hostname(config)# crypto ca trustpoint central
hostname(config)# vpnclient trustpoint central chain
hostname(config)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	指定したトラストポイントのトラストポイント サブモードに入り、トラストポイント情報を管理します。

vpnclient username

Easy VPN Remote 接続用の VPN ユーザ名およびパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient username** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient username *xauth_username* ***password*** *xauth password*

no vpnclient username

シンタックスの説明

xauth_password	XAUTH に使用するパスワードを指定します。最大長は 64 文字です。
xauth_username	XAUTH に使用するユーザ名を指定します。最大長は 64 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ASA モデル 5505 のみに適用されます。

XAUTH ユーザ名およびパスワードのパラメータは、セキュアな装置認証がディセーブルになっていて、サーバが XAUTH クレデンシャルを要求する場合に使用されます。セキュアな装置認証がイネーブルになっている場合、これらのパラメータは無視され、セキュリティ アプライアンスはユーザにユーザ名およびパスワードを要求します。

例

次の例は、XAUTH ユーザ名 testuser とパスワード ppurkm1 を使用するように Easy VPN Remote 接続を設定する方法を示しています。

```
hostname(config)# vpnclient username testuser password ppurkm1
hostname(config)#
```

vpnclient vpngroup

Easy VPN Remote 接続用の VPN トンネル グループ名およびパスワードを設定するには、グローバル コンフィギュレーション モードで **vpnclient vpngroup** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

vpnclient vpngroup *group_name* ***password*** *preshared_key*

no vpnclient vpngroup

シンタックスの説明

group_name	Easy VPN サーバ上で設定されている VPN トンネル グループの名前を指定します。最大長は 64 文字で、スペースは使用できません。
preshared_key	Easy VPN サーバが認証に使用する IKE 事前共有キー。最大長は 128 文字です。

デフォルト

Easy VPN クライアントとして稼働している ASA 5505 のコンフィギュレーションでトンネル グループが指定されていない場合、クライアントは RSA 証明書の使用を試行します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、Easy VPN クライアント（「Easy VPN Remote」とも呼ばれる）として稼働している ASA 5505 のみに適用されます。

パスワードとして事前共有キーを使用します。接続を確立する前に、サーバを設定しておく必要があります。

例

次の例は、VPN トンネル グループ名 TestGroup1 とパスワード my_key123 を使用するように、VPN トンネル グループとの Easy VPN Remote 接続を設定する方法を示しています。

```
hostname(config)# vpnclient vpngroup TestGroup1 password my_key123
hostname(config)#
```

関連コマンド

コマンド	説明
vpnclient trustpoint	Easy VPN 接続で使用する RSA ID 証明書を設定します。

wccp

容量を割り当て、指定した Web Cache Communication Protocol（WCCP）サービスのサポートをイネーブルにして、サービス グループに参加できるようにするには、グローバル コンフィギュレーション モードで **wccp** コマンドを使用します。サービス グループをディセーブルにして、容量の割り当てを解除するには、このコマンドの no 形式を使用します。

wccp {**web-cache** | ***service-number***} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** password]

no wccp {**web-cache** | ***service-number***} [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** password [**0** | **7**]]

シンタックスの説明

web-cache	Web キャッシュ サービスを指定します。 **（注）** Web キャッシュは、1 つのサービスとして数えます。サービスの最大数は、service-number 引数で指定したものも含め、256 個です。
service-number	動的サービス ID。このサービスの定義は、キャッシュによって示されます。動的サービス数は 0 ～ 254 までの範囲で、255 個です。***web-cache*** キーワードで指定する Web キャッシュ サービスを含め、256 個までに制限されます。
redirect-list	（オプション）このサービス グループにリダイレクトするトラフィックをコントロールするアクセス リストと共に使用します。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。
access-list	アクセス リストの名前を指定します。
group-list	（オプション）サービス グループに参加する Web キャッシュを決めるアクセス リスト。access-list 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で構成する必要があります。
password	（オプション）サービス グループから受信するメッセージを Message Digest 5（MD5）で認証することを指定します。認証できなかったメッセージは廃棄されます。
password	認証で使用するパスワードを指定します。最大長は 7 文字です。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、WCCP のサービス グループへの参加をイネーブルにする方法を示します。

```
hostname(config)# wccp web-cache redirect-list jeeves group-list wooster password
whatho
```

関連コマンド

コマンド	説明
show wccp	WCCP のコンフィギュレーションを表示します。
wccp redirect	WCCP リダイレクションのサポートをイネーブルにします。

wccp redirect

Web Cache Communication Protocol（WCCP）を使用して、インターフェイスの入り口でパケットのリダイレクトをイネーブルにするには、**wccp redirect** コマンドを使用します。WCCP のリダイレクションをディセーブルにするには、このコマンドの no 形式を使用します。

wccp interface *interface_name service* **redirect in**

no wccp interface *interface_name service* **redirect in**

シンタックスの説明

interface_name	パケットをリダイレクトするインターフェイスの名前。
service	サービス グループを指定します。***web-cache*** キーワードか、サービスの ID 番号（0 ～ 99）を指定できます。
in	パケットがこのインターフェイスに入ろうとしたときにリダイレクトすることを指定します。

デフォルト

このコマンドは、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、Web キャッシュ サービスの内部インターフェイスで WCCP リダイレクションをイネーブルにする方法を示します。

```
hostname(config)# wccp interface inside web-cache redirect in
```

関連コマンド

コマンド	説明
show wccp	WCCP のコンフィギュレーションを表示します。
wccp	サービス グループを使用して、WCCP のサポートをイネーブルにします。

web-agent-url

セキュリティ アプライアンスが SSO 認証要求を行う SSO サーバの URL を指定するには、webvpn-sso-siteminder コンフィギュレーション モードで **web-agent-url** コマンドを使用します。これは CA SiteMinder コマンドによる SSO です。

SSO サーバの認証 URL を削除するには、このコマンドの **no** 形式を使用します。

web-agent-url *url*

no web-agent-url *url*

（注） SSO 認証にはこのコマンドが必要です。

シンタックスの説明

url	SSO サーバの認証 URL を指定します。http:// または https:// を含める必要があります。

デフォルト

デフォルトでは、認証 URL は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn-sso-siteminder コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN だけで使用できるシングル サインオンのサポートは、ユーザが、異なるサーバ上の異なるセキュア サービスにユーザ名とパスワードを複数回入力することなくアクセスできるようにします。SSO サーバには、認証要求を処理する URL があります。

この URL に認証を送信するようにセキュリティ アプライアンスを設定するには、**web-agent-url** コマンドを使用します。認証 URL を設定する前に、**sso-server** コマンドを使用して SSO サーバを作成する必要があります。

例

webvpn-sso-siteminder コンフィギュレーション モードで入力された次の例では、認証 URL に http://www.example.com/webvpn を指定しています。

```
hostname(config-webvpn)# sso-server example type siteminder
hostname(config-webvpn-sso-siteminder)# web-agent-url http://www.example.com/webvpn
hostname(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	失敗した SSO 認証に対して、セキュリティ アプライアンスが認証を再試行する回数を設定します。
policy-server-secret	SSO サーバへの認証要求の暗号化に使用する秘密鍵を作成します。
request-timeout	失敗した SSO 認証試行がタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	SSO サーバの動作統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。

web-applications

認証された WebVPN ユーザに対して表示される WebVPN ホームページの Web Application ボックスをカスタマイズするには、webvpn カスタマイゼーション モードで **web-applications** コマンドを使用します。

web-applications {**title** | **message** | **dropdown**} {**text** | **style**} *value*

[**no**] **web-applications** {**title** | **message** | **dropdown**} {**text** | **style**} *value*

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

title	タイトルを変更することを指定します。
message	タイトルの下に表示されるメッセージを変更することを指定します。
dropdown	ドロップダウン ボックスを変更することを指定します。
text	テキストを変更することを指定します。
style	HTML スタイルを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのタイトルのテキストは「Web Application」です。

デフォルトのタイトルのスタイルは
background-color:#99CCCC;color:black;font-weight:bold;text-transform です。
uppercase

デフォルトのメッセージのテキストは「Enter Web Address（URL）」です。

デフォルトのメッセージのスタイルは
background-color:#99CCCC;color:maroon;font-size:smaller です。

デフォルトのドロップダウンのテキストは「Web Bookmarks」です。

デフォルトのドロップダウンのスタイルは
border:1px solid black;font-weight:bold;color:black;font-size:80% です。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン　**style** オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注）　WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例　次の例では、タイトルを「Applications」に変更し、テキストの色を青に変更しています。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-applications title text Applications
F1-asa1(config-webvpn-custom)# web-applications title style color:blue
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの Application Access ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの Browse Networks ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの Web Bookmarks タイトルまたはリンクをカスタマイズします。
file-bookmarks	WebVPN ホームページの File Bookmarks タイトルまたはリンクをカスタマイズします。

web-bookmarks

認証された WebVPN ユーザに表示される WebVPN ホームページの Web Bookmarks のタイトルまたはリンクをカスタマイズするには、webvpn カスタマイゼーション モードで **web-bookmarks** コマンドを使用します。

web-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

[**no**] **web-bookmarks** {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

このコマンドをコンフィギュレーションから削除し、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

シンタックスの説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトルのテキストは「Web Bookmarks」です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
Webvpn カスタマイゼーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、有効な Cascading Style Sheet（CSS）パラメータとして表現されます。このパラメータの説明は、このマニュアルでは取り扱いません。CSS パラメータの詳細については、World Wide Web Consortium（W3C）の Web サイト www.w3.org の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手可能です。

ここでは、WebVPN ページに対する変更で最もよく行われるページの配色を変更するためのヒントを紹介します。

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）について 0 ～ 255 の範囲で 10 進値を入力します。このカンマ区切りのエントリは、他の 2 色と混合する各色の輝度のレベルを示しています。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番目は赤を、3 番目と 4 番目は緑を、5 番目と 6 番目は青を表しています。

（注） WebVPN ページを簡単にカスタマイズするには、ASDM を使用することをお勧めします。ASDM には、色見本やプレビュー機能など、スタイルの要素を設定するのに便利な機能があります。

例

次の例では、Web Bookmarks のタイトルを「Corporate Web Bookmarks」に変更します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# web-bookmarks title text Corporate Web Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの Application Access ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの Browse Networks ボックスをカスタマイズします。
file-bookmarks	WebVPN ホームページの File Bookmarks タイトルまたはリンクをカスタマイズします。
web-applications	WebVPN ホームページの Web Application ボックスをカスタマイズします。

webvpn（グループ ポリシー モードおよびユーザ名モード）

この WebVPN モードに入るには、グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで **webvpn** コマンドを使用します。WebVPN モードで入力したコマンドをすべて削除するには、このコマンドの **no** 形式を使用します。これらの webvpn コマンドは、設定するユーザ名またはグループ ポリシーに適用されます。

グループ ポリシーおよびユーザ名に対する webvpn コマンドにより、WebVPN を超えたファイル、MAPI プロキシ、URL および TCP アプリケーションへのアクセスが定義されます。また、ACL およびフィルタリングするトラフィックのタイプも識別されます。

webvpn

no webvpn

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

WebVPN は、デフォルトではディセーブルになっています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—
ユーザ名	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

グローバル コンフィギュレーション モードから入って WebVPN モードを使用すると、WebVPN のグローバル設定値を設定できます。グループ ポリシー アトリビュート コンフィギュレーション モード、またはユーザ名アトリビュート コンフィギュレーション モードの **webvpn** コマンドは、webvpn コマンドで指定された設定を親コマンドで指定されたグループまたはユーザに適用します。つまり、この項で説明したように、グループ ポリシー モードまたはユーザ名モードから入って WebVPN モードを使用すると、特定のユーザ ポリシーまたはグループ ポリシーの WebVPN コンフィギュレーションをカスタマイズできます。

特定のグループ ポリシーに対してグループ ポリシー アトリビュート モードで適用した webvpn アトリビュートは、デフォルトのグループ ポリシーで指定された webvpn アトリビュートを上書きします。ユーザ名アトリビュート モードで特定のユーザに対して適用した webvpn アトリビュートは、デフォルト グループ ポリシーおよび、当該ユーザが所属するグループ ポリシーの両方で webvpn アトリビュートを上書きします。基本的に、これらのコマンドを使用すると、デフォルトのグループまたは特定のグループ ポリシーから継承される設定を微調整できます。WebVPN 設定の詳細については、グローバル コンフィギュレーション モードの **webvpn** コマンドの説明を参照してください。

次の表は、webvpn グループ ポリシー アトリビュート モードおよびユーザ名アトリビュート モードで設定できるアトリビュートを示しています。詳細については、個々のコマンドの説明を参照してください。

アトリビュート	説明
auto-signon	WebVPN ユーザのログイン クレデンシャルを内部サーバに自動的に渡すようにセキュリティ アプライアンスを設定して、WebVPN ユーザにシングル サインオン方式を提供します。
customization	適用する事前設定済みの WebVPN カスタマイゼーションを指定します。
deny-message	アクセスが拒否されたときにユーザに表示するメッセージを指定します。
filter	WebVPN 接続で使用するアクセス リストを指定します。
functions	ファイル アクセスとファイル ブラウジング、MAPI プロキシ、および WebVPN を超える URL エントリを設定します。
homepage	WebVPN ユーザがログインしたときに表示する Web ページの URL を設定します。
html-content-filter	WebVPN セッションに対してフィルタリングする Java、ActiveX、イメージ、スクリプト、およびクッキーを指定します。
http-comp	使用する HTTP 圧縮アルゴリズムを指定します。
keep-alive-ignore	セッションのアップデートで無視する最大オブジェクト サイズを指定します。
port-forward	WebVPN アプリケーション アクセスをイネーブルにします。
port-forward-name	エンド ユーザに転送する TCP ポートを識別する表示名を設定します。
sso-server	SSO サーバ名を設定します。
svc	SSL VPN Client のアトリビュートを設定します。
url-list	ユーザが WebVPN 経由でアクセスできるサーバおよび URL のリストを指定します。

例

次の例は、「FirstGroup」というグループ ポリシーで WebVPN モードに入る方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-webvpn)#
```

次の例は、「test」というユーザ名で WebVPN モードに入る方法を示します。

```
hostname(config)# group-policy test attributes
hostname(config-username)# webvpn
hostname(config-webvpn)#
```

関連コマンド

clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
group-policy attributes	config-group-policy モードに入ります。このモードでは、指定したグループ ポリシーのアトリビュートと値を設定したり、グループの webvpn アトリビュートを設定する webvpn モードに入ったりできます。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
webvpn	config-group-webvpn モードに入ります。このモードで、指定したグループに対する WebVPN アトリビュートを設定できます。

who

セキュリティ アプライアンス上のアクティブな Telnet 管理セッションを表示するには、特権 EXEC モードで **who** コマンドを使用します。

who [*local_ip*]

シンタックスの説明

local_ip	（オプション）リストを 1 つの内部 IP アドレスまたはネットワーク アドレス（IPv4 または IPv6）に制限するために指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

who コマンドを使用すると、現在セキュリティ アプライアンスにログインしている各 Telnet クライアントの TTY_ID および IP アドレスを表示できます。

例

次の例では、クライアントが Telnet セッションを通してセキュリティ アプライアンスにログインした場合の ***who*** コマンドの出力を示します。

```
hostname# who
0: 100.0.0.2
hostname# who 100.0.0.2
0: 100.0.0.2
hostname#
```

関連コマンド

コマンド	説明
kill	Telnet セッションを終了します。
telnet	Telnet アクセスをセキュリティ アプライアンス コンソールに追加し、アイドル タイムアウトを設定します。

window-variation

さまざまなウィンドウ サイズの接続をドロップするには、tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

window variation {**allow-connection** | **drop-connection**}

no window variation {**allow-connection** | **drop-connection**}

シンタックスの説明

allow-connection	接続を許可します。
drop-connection	接続をドロップします。

デフォルト

デフォルト アクションは、接続を許可します。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
tcp マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

tcp-map コマンドをモジュラ ポリシー フレームワーク インフラストラクチャと共に使用します。トラフィックのクラスを **class-map** コマンドを使用して定義し、TCP 検査を **tcp-map** コマンドを使用してカスタマイズします。その新しい TCP マップを **policy-map** コマンドを使用して適用します。TCP 検査を **service-policy** コマンドを使用して有効にします。

tcp-map コマンドを使用して、tcp マップ コンフィギュレーション モードに入ります。tcp マップ コンフィギュレーション モードで **window-variation** コマンドを使用して、縮小されたウィンドウ サイズの接続をすべてドロップします。

ウィンドウ サイズ メカニズムを使用すると、TCP は大きなウィンドウをアドバタイズした後、多すぎるデータを受信することなく、小さなウィンドウにアドバタイズできます。TCP の仕様では、「ウィンドウの縮小」は推奨されていません。この状態が検出されると、接続をドロップできます。

例

次の例では、さまざまなウィンドウ サイズの接続をすべてドロップする方法を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# window-variation drop-connection
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシー（トラフィック クラスと 1 つまたは複数のアクションのアソシエーション）を設定します。
set connection	接続値を設定します。
tcp-map	TCP マップを作成し、tcp マップ コンフィギュレーション モードにアクセスできるようにします。

wins-server

プライマリおよびセカンダリ WINS サーバの IP アドレスを設定するには、グループ ポリシー コンフィギュレーション モードで **wins-server** コマンドを使用します。このアトリビュートを実行コンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、WINS サーバを別のグループ ポリシーから継承できます。サーバを継承しないようにするには、**wins-server none** コマンドを使用します。

wins-server value {*ip_address*} [*ip_address*] | none

no wins-server

シンタックスの説明

none	WINS サーバにヌル値を設定して、WINS サーバを許可しないようにします。デフォルトのグループ ポリシーまたは指定されているグループ ポリシーから値を継承しないようにします。
value *ip_address*	プライマリおよびセカンダリ WINS サーバの IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グループ ポリシー	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

wins-server コマンドを発行するたびに、既存の設定を上書きします。たとえば、WINS サーバ x.x.x.x を設定してから WINS サーバ y.y.y.y を設定すると、2 番目のコマンドが最初のコマンドを上書きします。したがって、y.y.y.y は唯一の WINS サーバになります。サーバを複数設定する場合も同様です。設定済みのサーバを上書きするのではなく、WINS サーバを追加するには、このコマンドを入力するときにすべての WINS サーバの IP アドレスを含めます。

例

次の例では、FirstGroup という名前のグループ ポリシーに対して IP アドレス 10.10.10.15、10.10.10.30、および 10.10.10.45 で WINS サーバを設定する方法を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# wins-server value 10.10.10.15 10.10.10.30 10.10.10.45
```

write erase

スタートアップ コンフィギュレーションを消去するには、特権 EXEC モードで **write erase** コマンドを使用します。実行コンフィギュレーションはそのまま残ります。

write erase

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、セキュリティ コンテキスト内ではサポートされません。コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで識別します。コンテキストのコンフィギュレーションを削除する場合は、リモート サーバ（指定されている場合）からファイルを手作業で削除するか、システム実行スペースで **delete** コマンドを使用してフラッシュ メモリからファイルを消去します。

例

次の例では、スタートアップ コンフィギュレーションを消去します。

```
hostname# write erase
Erase configuration in flash memory? [confirm] y
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
delete	フラッシュ メモリからファイルを削除します。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write memory

スタートアップ コンフィギュレーションに実行コンフィギュレーションを保存するには、特権 EXEC モードで **write memory** コマンドを使用します。

write memory [**all** [**/noconfirm**]]

シンタックスの説明

/noconfirm	**all** キーワードを使用するときに、確認プロンプトをなくします。
all	マルチ コンテキスト モードのシステム実行スペースで、すべてのコンテキスト コンフィギュレーションとシステム コンフィギュレーションを保存します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.2(1)	**all** キーワードで、すべてのコンテキスト コンフィギュレーションを保存できるようになりました。

使用上のガイドライン

実行コンフィギュレーションは、メモリ内で現在実行されているコンフィギュレーションです。コマンドラインで行った変更がすべて含まれています。変更をスタートアップ コンフィギュレーションに保存する場合は、リブートの間だけ保存されます。これは起動時に実行中のメモリにロードされるコンフィギュレーションです。シングル コンテキスト モード、およびマルチ コンテキスト モードのシステムのスタートアップ コンフィギュレーションの場所は、**boot config** コマンドを使用して、デフォルトの場所（隠しファイル）から別の場所に変更できます。マルチ コンテキスト モードの場合は、コンテキストのスタートアップ コンフィギュレーションは、システム コンフィギュレーションの **config-url** コマンドで指定した場所にあります。

マルチ コンテキスト モードでは、各コンテキストで **write memory** コマンドを入力して、現在のコンテキストのコンフィギュレーションを保存できます。すべてのコンテキストのコンフィギュレーションを保存するには、システム実行スペースで **write memory all** コマンドを入力します。コンテキストのスタートアップ コンフィギュレーションは外部サーバ上に配置できます。この場合、セキュリティ アプライアンスは、コンフィギュレーションをサーバに戻して保存できない HTTP と HTTPS の URL を除き、**config-url** コマンドで指定したサーバにコンフィギュレーションを戻して保存します。**write memory all** コマンドで各コンテキストを保存すると、次のメッセージが表示されます。

```
'Saving context 'b' ... ( 1/3 contexts saved ) '
```

エラーが発生して、コンテキストを保存できないことがあります。次に、そのエラーについて説明します。

- メモリが不足しているためコンテキストを保存できない場合は、次のメッセージが表示されます。

```
The context 'context a' could not be saved due to Unavailability of resources
```

- リモートの宛先に到達できないためコンテキストを保存できない場合は、次のメッセージが表示されます。

```
The context 'context a' could not be saved due to non-reachability of destination
```

- コンテキストがロックされているため保存できない場合は、次のメッセージが表示されます。

```
Unable to save the configuration for the following contexts as these contexts are
locked.
context ‘a’ , context ‘x’ , context ‘z’ .
```

  コンテキストがロックされるのは、別のユーザがすでにコンフィギュレーションを保存しているか、コンテキストを削除している場合だけです。

- スタートアップ コンフィギュレーションが読み取り専用（HTTP サーバの場合など）のため保存できない場合は、他のメッセージの最後に次のメッセージが表示されます。

```
Unable to save the configuration for the following contexts as these contexts have
read-only config-urls:
context ‘a’ , context ‘b’ , context ‘c’ .
```

- フラッシュ メモリのセクターが壊れているためコンテキストを保存できない場合は、次のメッセージが表示されます。

```
The context 'context a' could not be saved due to Unknown errors
```

システムは管理コンテキスト インターフェイスを使用して、コンテキストのスタートアップ コンフィギュレーションにアクセスするため、**write memory** コマンドも管理コンテキスト インターフェイスを使用します。ただし、**write net** コマンドは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。

write memory コマンドは、**copy running-config startup-config** コマンドと同じです。

例

次の例では、スタートアップ コンフィギュレーションに実行コンフィギュレーションを保存します。

```
hostname# write memory
Building configuration...
Cryptochecksum: e43e0621 9772bebe b685e74f 748e4454

19319 bytes copied in 3.570 secs (6439 bytes/sec)
[OK]
hostname#
```

関連コマンド

コマンド	説明
admin-context	管理コンテキストを設定します。
configure memory	スタートアップ コンフィギュレーションを実行コンフィギュレーションとマージします。
config-url	コンテキスト コンフィギュレーションの場所を指定します。
copy running-config startup-config	実行コンフィギュレーションをスタートアップ コンフィギュレーションにコピーします。
write net	実行コンフィギュレーションを TFTP サーバにコピーします。

write net

TFTP サーバに実行コンフィギュレーションを保存するには、特権 EXEC モードで **write net** コマンドを使用します。

write net [*server:***[***filename***] | *:filename***]**

シンタックスの説明

:filename	パスとファイル名を指定します。**tftp-server** コマンドですでにファイル名を設定している場合は、この引数はオプションです。 **tftp-server** コマンドとこのコマンドの両方でファイル名を指定すると、セキュリティ アプライアンスは **tftp-server** コマンドのファイル名をディレクトリとして扱い、***write net*** コマンドのファイル名をそのディレクトリの下にファイルとして追加します。 **tftp-server** コマンドの値を上書きするには、パスとファイル名の前にスラッシュを入力します。スラッシュは、パスが tftpboot ディレクトリに対する相対パスではなく、絶対パスであることを示します。このファイル用に生成される URL には、ファイル名パスの前にダブル スラッシュ（//）が含まれます。必要なファイルが tftpboot ディレクトリにある場合は、ファイル名パスに tftpboot ディレクトリへのパスを含めることができます。TFTP サーバがこのタイプの URL をサポートしていない場合は、代わりに **copy running-config tftp** コマンドを使用します。 **tftp-server** コマンドで TFTP サーバのアドレスを指定した場合は、コロン（:）の後にファイル名だけを入力できます。
server:	TFTP サーバの IP アドレスまたは名前を設定します。このアドレスが存在する場合は、**tftp-server** コマンドで設定したアドレスが上書きされます。 デフォルトのゲートウェイ インターフェイスはセキュリティが最高のインターフェイスですが、**tftp-server** コマンドを使用して別のインターフェイス名を設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

実行コンフィギュレーションは、メモリ内で現在実行されているコンフィギュレーションです。コマンドラインで行った変更がすべて含まれています。

マルチ コンテキスト モードでこのコマンドを実行すると、現在のコンフィギュレーションのみ保存されます。1 回のコマンドですべてのコンテキストを保存することはできません。システムおよび各コンテキストについて、このコマンドを個別に入力する必要があります。**write net** コマンドは、コンテキスト インターフェイスを使用してコンフィギュレーションを TFTP サーバに書き込みます。ただし、システムは管理コンテキスト インターフェイスを使用して、コンテキストのスタートアップ コンフィギュレーションにアクセスするため、**write memory** コマンドは管理コンテキスト インターフェイスを使用して、スタートアップ コンフィギュレーションに保存します。

write net コマンドは、**copy running-config tftp** コマンドと同じです。

例

次の例では、**tftp-server** コマンドに TFTP サーバとファイル名を設定しています。

```
hostname# tftp-server inside 10.1.1.1 /configs/contextbackup.cfg
hostname# write net
```

次の例では、**write net** コマンドにサーバとファイル名を設定しています。**tftp-server** コマンドは入力されません。

```
hostname# write net 10.1.1.1:/configs/contextbackup.cfg
```

次の例では、**write net** コマンドにサーバとファイル名を設定しています。**tftp-server** コマンドはディレクトリ名を示し、サーバ アドレスは上書きされます。

```
hostname# tftp-server 10.1.1.1 configs
hostname# write net 10.1.2.1:context.cfg
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
copy running-config tftp	実行コンフィギュレーションを TFTP サーバにコピーします。
show running-config	実行コンフィギュレーションを表示します。
tftp-server	他のコマンドで使用するためのデフォルトの TFTP サーバおよびパスを設定します。
write memory	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

write standby

フェールオーバー スタンバイ装置にセキュリティ アプライアンスまたはコンテキストの実行コンフィギュレーションをコピーするには、特権 EXEC モードで **write standby** コマンドを使用します。

write standby

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

Active/Standby フェールオーバーの場合、**write standby** コマンドは、アクティブなフェールオーバー装置の RAM に保存されているコンフィギュレーションを、スタンバイ装置の RAM に書き込みます。プライマリ装置とセカンダリ装置のコンフィギュレーションの情報が異なる場合は、**write standby** コマンドを使用します。このコマンドをアクティブ装置に入力します。

Active/Active フェールオーバーの場合、**write standby** コマンドは次のように動作します。

- システム実行スペースで **write standby** コマンドを入力すると、システム コンフィギュレーションおよびセキュリティ アプライアンス上のセキュリティ コンテキストのすべてのコンフィギュレーションはピア装置に書き込まれます。これは、スタンバイ状態にあるセキュリティ コンテキストのコンフィギュレーション情報を含みます。アクティブ状態のフェールオーバー グループ 1 を持つ装置のシステム実行スペースに、このコマンドを入力する必要があります。
- セキュリティ コンテキストに **write standby** コマンドを入力する場合、セキュリティ コンテキストのコンフィギュレーションだけがピア装置に書き込まれます。セキュリティ コンテキストがアクティブ状態で表示される装置のセキュリティ コンテキストに、このコマンドを入力する必要があります。

（注） **write standby** コマンドはコンフィギュレーションをピア装置の実行コンフィギュレーションに複製します。コンフィギュレーションはスタートアップ コンフィギュレーションには保存されません。コンフィギュレーションの変更をスタートアップ コンフィギュレーションに保存するには、**write standby** コマンドを入力したのと同じ装置で **copy running-config startup-config** コマンドを使用します。コマンドはピア装置に複製され、コンフィギュレーションはスタートアップ コンフィギュレーションに保存されます。

例

次の例では、現在の実行コンフィギュレーションをスタンバイ装置に書き込みます。

```
hostname# write standby
Building configuration...
[OK]
hostname#
```

関連コマンド

コマンド	説明
failover reload-standby	スタンバイ装置を強制的にリブートします。

write terminal

端末に実行コンフィギュレーションを表示するには、特権 EXEC モードで **write terminal** コマンドを使用します。

write terminal

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
既存	このコマンドは既存のものです。

使用上のガイドライン

このコマンドは、**show running-config** コマンドと同じです。

例

次の例では、端末に実行コンフィギュレーションを書き込みます。

```
hostname# write terminal
: Saved
:
ASA Version 7.0(0)61
multicast-routing
names
name 10.10.4.200 outside
!
interface GigabitEthernet0/0
 nameif inside
 security-level 100
 ip address 10.86.194.60 255.255.254.0
 webvpn enable
...
```

関連コマンド

コマンド	説明
configure net	指定した TFTP URL からのコンフィギュレーション ファイルを実行コンフィギュレーションとマージします。
show running-config	実行コンフィギュレーションを表示します。
write memory	実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。

zonelabs-integrity fail-close

セキュリティ アプライアンスが Zone Labs Integrity ファイアウォール サーバに接続できなかった場合に、VPN クライアントへの接続を閉じるようにセキュリティ アプライアンスを設定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-close** コマンドを使用します。Zone Labs に接続できなかった場合に VPN 接続を開いたままにするデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-close

no zonelabs-integrity fail-close

シンタックスの説明

このコマンドには、引数もキーワードもありません。

デフォルト

デフォルトでは、サーバに障害が発生しても、VPN 接続が開いたままになります。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバがセキュリティ アプライアンスに応答しない場合でも、セキュリティ アプライアンスはプライベート ネットワークに向かう VPN クライアント接続を必要に応じて確立します。また、既存の開いた接続も維持します。これにより、ファイアウォール サーバに障害が発生しても、企業の VPN 接続が中断されないようにします。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態で維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。

Zone Labs Integrity ファイアウォール サーバに接続できなくなってもクライアントの VPN 接続を維持するデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドを使用します。

例

次の例では、Zone Labs Integrity ファイアウォール サーバが応答しない場合や、サーバとの接続が中断した場合に、VPN クライアントの接続を閉じるようにセキュリティ アプライアンスを設定します。

```
hostname(config)# zonelabs-integrity fail-close
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、セキュリティ アプライアンスへの VPN クライアント接続を開いたままにすることを指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイウォール サーバをセキュリティ アプライアンスが到達不能と見なすまでの秒数を指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。

zonelabs-integrity fail-open

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバの接続が中断した後も、リモート VPN クライアントからセキュリティ アプライアンスへの接続を開いたままにするには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-open** コマンドを使用します。Zone Labs サーバとの接続が中断した場合に、VPN クライアントの接続を閉じる場合は、このコマンドの **no** 形式を使用します。

zonelabs-integrity fail-open

no zonelabs-integrity fail-open

シンタックスの説明　このコマンドには、引数もキーワードもありません。

デフォルト　デフォルトでは、セキュリティ アプライアンスが Zone Labs Integrity ファイアウォール サーバに接続できない場合や接続が中断した場合でも、リモート VPN 接続が開いたままになります。

コマンド モード　次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

デフォルトでは、プライマリの Zone Labs Integrity ファイアウォール サーバがセキュリティ アプライアンスに応答しない場合でも、セキュリティ アプライアンスはプライベート ネットワークに向かう VPN クライアント接続を必要に応じて確立します。また、既存の開いた接続も維持します。これにより、ファイアウォール サーバに障害が発生しても、企業の VPN 接続が中断されないようにします。ただし、Zone Labs Integrity ファイアウォール サーバで障害が発生した場合に、VPN 接続を運用可能な状態で維持しないようにするには、**zonelabs-integrity fail-close** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバに接続できなくなってもクライアントの VPN 接続を維持するデフォルト状態に戻すには、**zonelabs-integrity fail-open** コマンドか、**no zonelabs-integrity fail-open** コマンドを使用します。

例

次の例では、Zone Labs Integrity ファイアウォール サーバに接続できなくなっても VPN クライアントの接続が開いたままになるデフォルト状態に戻します。

```
hostname(config)# zonelabs-integrity fail-open
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスで VPN クライアント接続を閉じることを指定します。
zonelabs-integrity fail-timeout	応答しない Zone Labs Integrity ファイウォール サーバをセキュリティ アプライアンスが到達不能と見なすまでの秒数を指定します。

zonelabs-integrity fail-timeout

セキュリティ アプライアンスが応答しない Zone Labs Integrity ファイアウォール サーバを到達不能と見なすまでの時間（秒単位）を指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity fail-timeout** コマンドを使用します。デフォルトのタイムアウト値 10 秒に戻すには、引数を指定せずにこのコマンドの **no** 形式を使用します。

zonelabs-integrity fail-timeout *timeout*

no zonelabs-integrity fail-timeout

シンタックスの説明

timeout	セキュリティ アプライアンスが、応答しない Zone Labs Integrity ファイウォール サーバを到達不能と見なすまでの秒数を指定します。5 ～ 20 秒に指定できます。

デフォルト

デフォルトのタイムアウト値は 10 秒です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスが指定した秒数待っても Zone Labs サーバから応答がないと、サーバを到達不能と見なします。VPN クライアントへの接続は、デフォルトまたは **zonelabs-integrity fail-open** コマンドの設定に従って開いたままになります。ただし、**zonelabs-integrity fail-close** コマンドを発行している場合は、セキュリティ アプライアンスが Zone Labs Integrity ファイアウォール サーバを到達不能と見なした時点で、VPN クライアントの接続が閉じられます。

例

次の例では、12 秒経過すると、アクティブな Zone Labs Intergity ファイアウォール サーバを到達不能と見なすようにセキュリティ アプライアンスを設定します。

```
hostname(config)# zonelabs-integrity fail-timeout 12
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-open	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生した後も、セキュリティ アプライアンスへの VPN クライアント接続を開いたままにすることを指定します。
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスで VPN クライアント接続を閉じることを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。

zonelabs-integrity interface

Zone Labs Integrity ファイアウォール サーバと通信するセキュリティ アプライアンスのインターフェイスを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity interface** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバとのインターフェイスをデフォルトのインターフェイスなしに戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity interface *interface*

no zonelabs-integrity interface

シンタックスの説明

interface	Zone Labs Integrity ファイアウォール サーバと通信するセキュリティ アプライアンスのインターフェイスを指定します。**nameif** コマンドで作成したインターフェイスの名前をよく使用します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバとのインターフェイスは設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次の例では、IP アドレスが 10.0.0.5 ～ 10.0.0.7 の Zone Labs Intergity ファイアウォール サーバを 3 台設定します。さらに、ポート 300 で、また inside というインターフェイスで、サーバからの通信をリッスンするようにセキュリティ アプライアンスを設定します。

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5 10.0.0.6 10.0.0.7
hostname(config)# zonelabs-integrity port 300
hostname(config)# zonelabs-integrity interface inside
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity port

セキュリティ アプライアンスが Zone Labs Integrity ファイアウォール サーバとの通信に使用するポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity port** コマンドを使用します。デフォルト ポート 5054 に戻すには、このコマンドの **no** 形式を使用します。

zonelabs-integrity port *port_number*

no zonelabs-integrity port *port_number*

シンタックスの説明

port	セキュリティ アプライアンスの Zone Labs Integrity ファイアウォール サーバ用のポートを指定します。
port_number	Zone Labs Integrity ファイアウォール サーバ用のポートの番号。10 ～ 10000 の範囲になります。

デフォルト

Zone Labs Integrity ファイアウォール サーバ用のデフォルト ポートは 5054 です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、**zonelabs-integrity port** コマンドと **zonelabs-integrity interface** コマンドで設定したポートとインターフェイスで、Zone Labs Integrity ファイアウォール サーバからの接続をリッスンします。

（注） セキュリティ アプライアンスの現在のリリースでは、ユーザ インターフェイスで Integrity サーバを 5 台まで設定できますが、同時にサポートできる Integrity サーバは 1 台です。アクティブなサーバに障害が発生した場合は、セキュリティ アプライアンス上で別の Integrity サーバを設定してから、クライアント VPN セッションを再確立してください。

例

次の例では、IP アドレスが 10.0.0.5 の Zone Labs Integrity ファイアウォール サーバを設定します。さらに、デフォルト ポート 5054 ではなくポート 300 で、アクティブな Zone Labs サーバをリッスンするようにセキュリティ アプライアンスを設定します。

```
hostname(config)# zonelabs-integrity server-address 10.0.0.5
hostname(config)# zonelabs-integrity port 300
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity server-address

セキュリティ アプライアンスのコンフィギュレーションに Zone Labs Integrity ファイアウォール サーバを追加するには、グローバル コンフィギュレーション モードで **zonelabs-integrity server-address** コマンドを使用します。Zone Labs Integrity ファイアウォール サーバの IP アドレスまたはホスト名を指定します。

実行コンフィギュレーションから Zone Labs Integrity ファイアウォール サーバを削除するには、引数を指定せずにこのコマンドの **no** 形式を使用します。

zonelabs-integrity server-address {*hostname1* | *ip-address1*}

no zonelabs-integrity server-address

(注) セキュリティ アプライアンスのユーザ インターフェイスは、複数の Zone Labs Integrity ファイアウォール サーバを含むコンフィギュレーションをサポートしているように見えますが、現在のリリースでは一度に 1 台のサーバにしか接続できません。

シンタックスの説明

hostname	Zone Labs Integrity ファイアウォール サーバのホスト名を指定します。ホスト名の指定方法については、**name** コマンドを参照してください。
ip-address	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。

コマンドのデフォルト設定

デフォルトでは、Zone Labs Integrity ファイアウォール サーバは設定されません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このリリースでは、Zone Labs Integrity ファイアウォール サーバを 1 台だけ設定できます。設定したサーバに障害が発生した場合は、別のサーバを設定してからクライアントの VPN セッションを確立し直してください。

ホスト名でサーバを指定するには、まず **name** コマンドを使用して、Zone Labs サーバの名前を指定する必要があります。このとき、**name** コマンドを使用する前に **names** コマンドを使用してコマンドをイネーブルにします。

（注） セキュリティ アプライアンスの現在のリリースでは、ユーザ インターフェイスで Integrity サーバを 5 台まで設定できますが、同時にサポートできる Integrity サーバは 1 台です。アクティブなサーバに障害が発生した場合は、セキュリティ アプライアンス上で別の Integrity サーバを設定してから、クライアント VPN セッションを再確立してください。

例

次の例は、IP アドレス 10.0.0.5 に ZL-Integrity-Svr というサーバ名を割り当ててから、この名前を使用して Zone Labs Intergity ファイアウォール サーバを設定しています。

```
hostname(config)# names
hostname(config)# name 10.0.0.5 ZL-Integrity-Svr
hostname(config)# zonelabs-integrity server-address ZL-Integrity-Svr
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity fail-close	セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの接続で障害が発生したとき、セキュリティ アプライアンスで VPN クライアント接続を閉じることを指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-certificate-port

Zone Labs Integrity ファイアウォール サーバが、SSL 証明書を取得するときに接続するセキュリティ アプライアンスのポートを指定するには、グローバル コンフィギュレーション モードで **zonelabs-integrity ssl-certificate-port** コマンドを使用します。デフォルトのポート番号（80）に戻すには、引数を指定せずにこのコマンドの **no** 形式を使用します。

zonelabs-integrity ssl-certificate-port *cert-port-number*

no zonelabs-integrity ssl-certificate-port

シンタックスの説明

cert-port-number	Zone Labs Integrity ファイアウォール サーバが SSL 証明書を要求するときに接続するセキュリティ アプライアンスのポートの番号を指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバがセキュリティ アプライアンスのポート 80 で SSL 証明書を要求するように設定されています。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの SSL 接続では、セキュリティ アプライアンスが SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始するときは、SSL サーバ（セキュリティ アプライアンス）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。**zonelabs-integrity ssl-certificate-port** コマンドで、Zone Labs サーバが SSL サーバ証明書を要求するときに接続するポートを指定します。

例

次の例では、セキュリティ アプライアンスのポート 30 で、Zone Labs Integrity サーバからの SSL 証明書要求を受信するように設定します。

```
hostname(config)# zonelabs-integrity ssl-certificate-port 30
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-client-authentication	セキュリティ アプライアンスによる、Zone Labs Integrity ファイアウォール サーバ SSL 証明書の認証をイネーブルにします。

zonelabs-integrity ssl-client-authentication

Zone Labs Integrity ファイアウォール サーバの SSL 証明書をセキュリティ アプライアンスで認証できるようにするには、グローバル　コンフィギュレーション　モードで　**zonelabs-integrity ssl-client-authentication** コマンドを *enable* 引数を指定して使用します。Zone Labs の SSL 証明書の認証をディセーブルにするには、*disable* 引数を使用するか、引数を指定せずにこのコマンドの **no** 形式を使用します。

zonelabs-integrity ssl-client-authentication {*enable* | *disable*}

no zonelabs-integrity ssl-client-authentication

シンタックスの説明

enable	セキュリティ アプライアンスで Zone Labs Integrity ファイアウォール サーバの SSL 証明書を認証することを指定します。
disable	Zone Labs Integrity ファイアウォール サーバの IP アドレスを指定します。

デフォルト

デフォルトでは、Zone Labs Integrity ファイアウォール サーバの SSL 証明書のセキュリティ アプライアンスによる認証は、ディセーブルです。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
グローバル コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスと Zone Labs Integrity ファイアウォール サーバとの SSL 接続では、セキュリティ アプライアンスが SSL サーバであり、Zone Labs サーバは SSL クライアントです。SSL 接続を開始するときは、SSL サーバ（セキュリティ アプライアンス）の証明書がクライアント（Zone Labs サーバ）によって認証される必要があります。ただし、クライアント証明書の認証はオプションです。Zone Lab サーバ（SSL クライアント）証明書のセキュリティ アプライアンス認証をイネーブルまたはディセーブルにするには、**zonelabs-integrity ssl-client-authentication** コマンドを使用します。

例

次の例では、Zone Labs Integrity ファイアウォール サーバの SSL 証明書を認証するようにセキュリティ アプライアンスを設定します。

```
hostname(config)# zonelabs-integrity ssl-client-authentication enable
hostname(config)#
```

関連コマンド

コマンド	説明
zonelabs-integrity interface	アクティブな Zone Labs Integrity サーバと通信するためのセキュリティ アプライアンス インターフェイスを指定します。
zonelabs-integrity port	Zone Labs Integrity ファイアウォール サーバと通信するためのセキュリティ アプライアンス上のポートを指定します。
zonelabs-integrity server-address	Zone Labs Integrity ファイアウォール サーバをセキュリティ アプライアンスのコンフィギュレーションに追加します。
zonelabs-integrity ssl-certificate-port	SSL 証明書を取得するときに、Zone Labs Integrity ファイアウォール サーバが接続するセキュリティ アプライアンスのポートを指定します。

Symbols

Numerics

A

C

D

E

F

H

I

J

L

M

N

P

Q

R

S

T

U

V

W

あ

い

え

お

か

き

け

こ

さ

し

す

せ

そ

た

て

と

に

ね

は

ひ

ふ

へ

ほ

ま

も

ゆ

ら

り

る

れ

ろ