CHAPTER 12

eigrp log-neighbor-changes コマンド～ functions（removed）コマンド

eigrp log-neighbor-changes

EIGRP ネイバーとの隣接関係の変更のロギングをイネーブルにするには、ルータ コンフィギュレーション モードで **eigrp log-neighbor-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eigrp log-neighbor-changes コマンドはデフォルトでイネーブルです。実行コンフィギュレーションには、コマンドの **no** 形式のみが表示されます。

例

次に、EIGRP ネイバーの変更のロギングをディセーブルにする例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# no eigrp log-neighbor-changes
```

関連コマンド

コマンド	説明
eigrp log-neighbor-warnings	ネイバー警告メッセージのロギングをイネーブルにします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp log-neighbor-warnings

EIGRP ネイバー警告メッセージのロギングをイネーブルにするには、ルータ コンフィギュレーション モードで **eigrp log-neighbor-warnings** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

構文の説明

seconds	（任意）ネイバー警告メッセージの反復間隔（秒数）。有効な値は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。すべてのネイバー警告メッセージがログに記録されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eigrp log-neighbor-warnings コマンドはデフォルトでイネーブルです。実行コンフィギュレーションには、コマンドの **no** 形式のみが表示されます。

例

次に、EIGRP ネイバーの警告メッセージのロギングをディセーブルにする例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# no eigrp log-neighbor-warnings
```

次に、EIGRP ネイバー警告メッセージをログに記録し、5 分（300 秒）間隔で警告メッセージを繰り返す例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# eigrp log-neighbor-warnings 300
```

関連コマンド

コマンド	説明
eigrp log-neighbor-messages	EIGRP ネイバーとの隣接関係に関する変更のロギングをイネーブルにします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp router-id

EIGRP ルーティング プロセスによって使用されるルータ ID を指定するには、ルータ コンフィギュレーション モードで **eigrp router-id** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

eigrp router-id *ip-addr*

no eigrp router-id [*ip-addr*]

構文の説明

ip-addr	IP アドレス形式（ドット付き 10 進形式）でのルータ ID。ルータ ID として 0.0.0.0 または 255.255.255.255 を使用することはできません。

デフォルト

指定しない場合、セキュリティ アプライアンス上で最上位の IP アドレスがルータ ID として使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eigrp router-id コマンドが設定されていない場合、EIGRP では、EIGRP プロセスの開始時に、セキュリティ アプライアンス上で最大の IP アドレスが自動的に選択されて、ルータ ID として使用されます。**no router eigrp** コマンドを使用して EIGRP プロセスを削除するか、または **eigrp router-id** コマンドを使用して手動でルータ ID を設定しない限り、ルータ ID は変更されません。

ルータ ID は、外部ルートの発信元ルータを識別するために使用されます。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。このような事態を回避するには、**eigrp router-id** コマンドを使用して、ルータ ID のグローバル アドレスを指定します。

各 EIGRP ルータには、一意の値を設定する必要があります。

例

次に、EIGRP ルーティング プロセスの固定ルータ ID として 172.16.1.3 を設定する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# eigrp router-id 172.16.1.3
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp stub

EIGRP ルーティング プロセスをスタブ ルーティング プロセスとして設定するには、ルータ コンフィギュレーション モードで **eigrp stub** コマンドを使用します。EIGRP スタブ ルーティングを削除するには、このコマンドの **no** 形式を使用します。

eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

no eigrp stub [receive-only] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

構文の説明

connected	（任意）接続ルートをアドバタイズします。
receive-only	（任意）セキュリティ アプライアンスを受信専用ネイバーとして設定します。
redistributed	（任意）他のルーティング プロトコルから再配布されたルートをアドバタイズします。
static	（任意）スタティック ルートをアドバタイズします。
summary	（任意）集約ルートをアドバタイズします。

デフォルト

スタブ ルーティングはイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eigrp stub コマンドを使用して、セキュリティ アプライアンスをスタブとして設定します。この場合、セキュリティ アプライアンスでは、すべての IP トラフィックがディストリビューション ルータに転送されます。

receive-only キーワードを使用すると、セキュリティ アプライアンスが自律システム内の他のどのルータともルートを共有しないように設定できます。セキュリティ アプライアンスは、EIGRP ネイバーからの更新のみを受信します。**receive-only** キーワードは他のキーワードと組み合わせて使用することはできません。

connected、**static**、**summary**、および **redistributed** の各キーワードは、1 つ以上を組み合わせて指定できます。これらのいずれかのキーワードを指定して **eigrp stub** コマンドを使用した場合、これらの特定のキーワードによって指定されたルート タイプのみが送信されます。

connected キーワードを指定すると、EIGRP スタブ ルーティング プロセスで接続ルートを送信できます。接続ルートが **network** ステートメントで指定されていない場合は、EIGRP プロセスで **redistribute** コマンドを使用して接続ルートの再配布が必要となることがあります。

static キーワードを指定すると、EIGRP スタブ ルーティング プロセスでスタティック ルートを送信できます。このオプションを設定しない場合、EIGRP ではスタティック ルートは送信されません。スタティック ルートが **network** ステートメントで指定されていない場合は、EIGRP プロセスで **redistribute** コマンドを使用してスタティック ルートの再配布が必要となることがあります。

summary キーワードを指定すると、EIGRP スタブ ルーティング プロセスで集約ルートを送信できます。集約ルートは、**summary-address eigrp** コマンドを使用して手動で作成することも、**auto-summary** コマンドをイネーブルにして自動的に作成することもできます（**auto-summary** はデフォルトでイネーブルになっています）。

redistributed キーワードを指定すると、EIGRP スタブ ルーティング プロセスで、他のルーティング プロトコルから EIGRP ルーティング プロセスに再配布されたルートを送信できます。このオプションを設定しない場合、再配布されたルートは EIGRP によってアドバタイズされません。

例

次に、**eigrp stub** コマンドを使用して、接続ルートおよび集約ルートをアドバタイズする EIGRP スタブとしてセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub connected summary
```

次に、**eigrp stub** コマンドを使用して、接続ルートおよびスタティック ルートをアドバタイズする EIGRP スタブとしてセキュリティ アプライアンスを設定する例を示します。集約ルートの送信は許可されません。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub connected static
```

次に、**eigrp stub** コマンドを使用して、EIGRP 更新の受信のみを行う EIGRP スタブとしてセキュリティ アプライアンスを設定する例を示します。接続ルート、集約ルート、およびスタティック ルートの情報は送信されません。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0 eigrp
hostname(config-router)# eigrp stub receive-only
```

次に、**eigrp stub** コマンドを使用して、他のルーティング プロトコルから EIGRP に再配布されたルートをアドバタイズする EIGRP スタブとしてセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub redistributed
```

次に、オプションの引数を指定しないで **eigrp stub** コマンドを使用する例を示します。引数なしで **eigrp stub** コマンドを使用すると、デフォルトで接続ルートおよびスタティック ルートがアドバタイズされます。

```
hostname(config)# router eigrp 100
hostname(config-router)# network 10.0.0.0
hostname(config-router)# eigrp stub
```

関連コマンド

コマンド	説明
router eigrp	実行コンフィギュレーションから EIGRP ルータ コンフィギュレーション モード コマンドをクリアします。
show running-config router eigrp	実行コンフィギュレーションの EIGRP ルータ コンフィギュレーション モード コマンドを表示します。

eject

ASA 5500 シリーズの外部コンパクト フラッシュ デバイスの取り外しをサポートするには、ユーザ EXEC モードで **eject** コマンドを使用します。

eject [/*noconfirm*] *disk1:*

構文の説明

disk1:	取り外すデバイスを指定します。
/noconfirm	セキュリティ アプライアンスから外部フラッシュ デバイスを物理的に取り外す前に、デバイスを取り外すかどうかの確認が必要ないことを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

eject コマンドを使用すると、ASA 5500 シリーズ セキュリティ アプライアンスからコンパクト フラッシュ デバイスを安全に取り外すことができます。

次に、**eject** コマンドを使用して、デバイスをセキュリティ アプライアンスから物理的に取り外す前に *disk1* を正常にシャットダウンする例を示します。

```
hostname# eject /noconfig disk1:
It is now safe to remove disk1:
hostname# show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34

Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"

wef5520 up 5 hours 36 mins

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

email

登録時に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **email** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

email *address*

no email

構文の説明

address	電子メール アドレスを指定します。*address* の最大長は 64 文字です。

デフォルト

デフォルト設定は設定されていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に電子メール アドレス user1@user.net を含める例を示します。

```
hostname(config)# crypto ca-trustpoint central
hostname(ca-trustpoint)# email user1@user.net
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca-trustpoint	トラストポイント コンフィギュレーション モードを開始します。

enable

特権 EXEC モードを開始するには、ユーザ EXEC モードで **enable** コマンドを使用します。

enable [*level*]

構文の説明

level	（任意）0 ～ 15 の特権レベル。enable 認証（**aaa authentication enable console** コマンド）では使用されません。

デフォルト

enable 認証（**aaa authentication enable console** コマンドを使用）を使用していない場合は、特権レベル 15 を開始します。enable 認証の場合、デフォルトのレベルは、ユーザ名に設定されているレベルに応じて異なります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

デフォルトのイネーブル パスワードはブランクです。パスワードの設定については、**enable password** コマンドを参照してください。

enable 認証を使用しない場合は、**enable** コマンドを入力すると、ユーザ名が enable_*level* に変更されます。デフォルトのレベルは 15 です。enable 認証を使用する場合（**aaa authentication enable console** コマンドを使用）、ユーザ名および関連するレベルは維持されます。ユーザ名の維持は、コマンド認可（ローカルまたは TACACS+ を使用した **aaa authorization command** コマンド）で重要です。

レベル 2 以上は特権 EXEC モードを開始します。レベル 0 およびレベル 1 は、ユーザ EXEC モードを開始します。中間のレベルを使用するには、ローカル コマンド認可（**aaa authorization command LOCAL** コマンド）をイネーブルにし、**privilege** コマンドを使用して異なる特権レベルにコマンドを設定します。TACACS+ コマンド認可では、セキュリティ アプライアンスに設定された特権レベルは使用されません。

現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

特権 EXEC モードを終了するには、**disable** コマンドを入力します。

例

次に、特権 EXEC モードを開始する例を示します。

```
hostname> enable
Password: Pa$$w0rd
```

```
hostname#
```

次に、レベル 10 の特権 EXEC モードを開始する例を示します。

```
hostname> enable 10
Password: Pa$$w0rd10
hostname#
```

関連コマンド

コマンド	説明
enable password	イネーブル パスワードを設定します。
disable	特権 EXEC モードを終了します。
aaa authorization command	コマンド認可を設定します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。

enable（webvpn）

以前に設定したインターフェイスで WebVPN または電子メール プロキシ アクセスをイネーブルにするには、enable コマンドを使用します。WebVPN の場合は、webvpn モードでこのコマンドを使用します。電子メール プロキシ（IMAP4S、POP3S、SMTPS）については、該当する電子メール プロキシ モードでこのコマンドを使用します。インターフェイスで WebVPN をディセーブルにするには、このコマンドの **no** バージョンを使用します。

enable *ifname*

no enable

構文の説明

ifname	以前に設定したインターフェイスを指定します。**nameif** コマンドを使用して、インターフェイスを設定します。

デフォルト

WebVPN は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	透過	シングル	コンテキスト	システム
webvpn	•	—	•	—	—
Imap4s	•	—	•	—	—
pop3s	•	—	•	—	—
SMTPS	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、Outside という名前のインターフェイスで WebVPN をイネーブルにする方法の例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# enable Outside
```

次に、Outside という名前のインターフェイスで POP3S 電子メール プロキシを設定する方法の例を示します。

```
hostname(config)# pop3s
hostname(config-pop3s)# enable Outside
```

enable gprs

RADIUS アカウンティングで GPRS をイネーブルにするには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **enable gprs** コマンドを使用します。このモードには、**inspect radius-accounting** コマンドを使用してアクセスします。セキュリティ アプライアンスは、セカンダリ PDP コンテキストを適切に処理するために、アカウンティング要求停止メッセージ内に 3GPP VSA 26-10415 があるかどうかをチェックします。このコマンドをディセーブルにするには、このコマンドの **no** 形式を使用します。

enable gprs

no enable gprs

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このオプションは、デフォルトで無効です。この機能をイネーブルにするには、GTP ライセンスが必要です。

例

次に、RADIUS アカウンティングで GPRS をイネーブルにする例を示します。

```
hostname(config)# policy-map type inspect radius-accounting ra
hostname(config-pmap)# parameters
hostname(config-pmap-p)# enable gprs
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
parameters	インスペクション ポリシー マップのパラメータを設定します。

enable password

特権 EXEC モードのイネーブル パスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。15 以外のレベルのパスワードを削除するには、このコマンドの **no** 形式を使用します。レベル 15 のパスワードは削除できません。

enable password *password* **[level** *level*] [**encrypted**]

no enable password level *level*

構文の説明

encrypted	（任意）パスワードが暗号化された形式であることを指定します。パスワードは暗号化された形式でコンフィギュレーションに保存されるため、パスワードの入力後に元のパスワードを表示することはできません。何らかの理由で別のセキュリティ アプライアンスにパスワードをコピーする必要があるが、元のパスワードを把握していない場合は、暗号化されたパスワードとこのキーワードを指定して **enable password** コマンドを入力できます。通常、**show running-config enable** コマンドを入力した場合にのみこのキーワードが表示されます。
level *level*	（任意）0 ～ 15 の特権レベルのパスワードを設定します。
password	3 ～ 32 文字の英数字および特殊文字から構成されるストリングとしてパスワードを設定します（大文字と小文字は区別されます）。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。

デフォルト

デフォルトのパスワードはブランクです。デフォルトのレベルは 15 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

イネーブル レベル 15（デフォルト レベル）のデフォルトのパスワードはブランクです。パスワードをブランクにリセットする場合は、*password* 引数にテキストを指定しません。

マルチ コンテキスト モードでは、システム コンフィギュレーションおよび各コンテキストに対してイネーブル パスワードを作成できます。

デフォルトの 15 以外の特権レベルを使用するには、ローカル コマンド認可（**aaa authorization command** コマンドを使用して **LOCAL** キーワードを指定）を設定し、**privilege** コマンドを使用して異なる特権レベルにコマンドを設定します。ローカル コマンド認可を設定しない場合、イネーブル レベルは無視されて、設定したレベルにかかわらずレベル 15 へのアクセスが可能になります。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードを開始します。レベル 0 およびレベル 1 は、ユーザ EXEC モードを開始します。

例

次に、イネーブル パスワードを Pa$$w0rd に設定する例を示します。

```
hostname(config)# enable password Pa$$w0rd
```

次に、レベル 10 のイネーブル パスワードを Pa$$w0rd10 に設定する例を示します。

```
hostname(config)# enable password Pa$$w0rd10 level 10
```

次に、イネーブル パスワードを、別のセキュリティ アプライアンスからコピーした暗号化されたパスワードに設定する例を示します。

```
hostname(config)# enable password jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
enable	特権 EXEC モードを開始します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。
show running-config enable	イネーブル パスワードを暗号化された形式で表示します。

endpoint

H.323 プロトコル インスペクションの HSI グループにエンドポイントを追加するには、HSI グループ コンフィギュレーション モードで **endpoint** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

構文の説明

if_name	エンドポイントがセキュリティ アプライアンスに接続するときに通過するインターフェイス。
ip_address	追加するエンドポイントの IP アドレス。HSI グループあたり最大で 10 のエンドポイントを設定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、H.323 インスペクション ポリシー マップの HSI グループにエンドポイントを追加する例を示します。

```
hostname(config-pmap-p)# hsi-group 10
hostname(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
hostname(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
hsi-group	HSI グループを作成します。
hsi	HSI を HSI グループに追加します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

endpoint-mapper

DCERPC インスペクションのエンドポイント マッパー オプションを設定するには、パラメータ コンフィギュレーション モードで **endpoint-mapper** コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

構文の説明

epm-service-only	バインディング時にエンドポイント マッパー サービスを適用することを指定します。
lookup-operation	エンドポイント マッパー サービスのルックアップ動作をイネーブルにすることを指定します。
timeout *value*	ルックアップ動作におけるピンホールのタイムアウトを指定します。範囲は、0:0:1 ～ 1193:0:0 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、DCERPC ポリシー マップにエンドポイント マッパーを設定する例を示します。

```
hostname(config)# policy-map type inspect dcerpc dcerpc_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# endpoint-mapper epm-service-only
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

enforcenextupdate

CRL の NextUpdate フィールドの処理方法を指定するには、ca-crl コンフィギュレーション モードで **enforcenextupdate** コマンドを使用します。期限が切れた NextUpdate フィールドがある場合や、NextUpdate フィールドがない場合を許容するには、このコマンドの **no** 形式を使用します。

enforcenextupdate

no enforcenextupdate

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定は強制（オン）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドが設定されている場合は、期限が切れていない NextUpdate フィールドが CRL に存在する必要があります。このコマンドが使用されていない場合、セキュリティ アプライアンスでは、CRL に NextUpdate フィールドがない場合や、期限が切れた NextUpdate フィールドがある場合が許容されます。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central に対して、期限が切れていない NextUpdate フィールドが CRL に存在することを必須とする例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# enforcenextupdate
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
cache-time	キャッシュのリフレッシュ時間を分単位で指定します。
crl configure	ca-crl コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。

enrollment-retrieval

登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定するには、ローカル CA サーバ コンフィギュレーション モードで **enrollment-retrieval** コマンドを使用します。期間をデフォルトの時間数（24）にリセットするには、このコマンドの **no** 形式を使用します。

enrollment-retrieval *timeout*

no enrollment-retrieval

構文の説明

timeout	何時間以内にユーザがローカル CA 登録 Web ページから発行された証明書を取得しなければならないかを指定します。有効なタイムアウト値の範囲は 1 ～ 720 時間です。

デフォルト

デフォルトでは、PKCS12 登録ファイルは 24 時間保存されて取得できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

PKCS12 登録ファイルには、発行された証明書とキー ペアが含まれています。ファイルはローカル CA サーバに保存され、**enrollment-retrieval** コマンドで指定された時間内は登録 Web ページから取得できます。

ユーザが登録可能とマークされている場合、そのユーザは **otp expiration** の時間内であればそのパスワードを使用して登録できます。ユーザが正常に登録すると、PKCS12 ファイルが生成および保存され、コピーが登録 Web ページを経由して返されます。何らかの理由でファイルのコピーが再度必要になった場合（登録しようとしてダウンロードに失敗した場合など）、ユーザは **enrollment-retrieval** コマンドで指定した時間内であれば新しくコピーを取得できます。

（注） この時間は、OTP の有効期限とは関係ありません。

例

次に、証明書の発行後 48 時間以内は PKCS12 登録ファイルをローカル CA サーバから取得できるように指定する例を示します。

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# enrollment-retrieval 48
hostname(config-ca-server)#
```

次に、取得可能時間をデフォルトの 24 時間にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no enrollment-retrieval
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
OTP expiration	CA 登録ページ用に発行されたワンタイム パスワードの有効期間を時間単位で指定します。
smtp from-address	CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示されるテキストを指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

enrollment retry count

再試行回数を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment retry count** コマンドを使用します。証明書を要求した後、セキュリティ アプライアンスは CA からの証明書の受信を待ちます。セキュリティ アプライアンスは、設定された再試行間隔内に証明書を受信できない場合、証明書要求を再度送信します。セキュリティ アプライアンスは、応答を受信するか、または設定されている再試行間隔が終了するまで、要求を繰り返し送信します。デフォルトの再試行回数設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry count *number*

no enrollment retry count

構文の説明

number	登録要求の送信を試行する最大回数。有効な範囲は、0、および 1 ～ 100 回の再試行です。

デフォルト

number のデフォルト設定は 0（無制限）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central 内の登録再試行回数を 20 回に設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry count 20
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。

enrollment retry period

再試行間隔を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment retry period** コマンドを使用します。証明書を要求した後、セキュリティ アプライアンスは CA からの証明書の受信を待ちます。セキュリティ アプライアンスは、指定された再試行間隔内に証明書を受信できない場合、証明書要求を再度送信します。デフォルトの再試行間隔設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry period *minutes*

no enrollment retry period

構文の説明

minutes	登録要求の送信を試行する間隔（分単位）。有効な範囲は、1 ～ 60 分です。

デフォルト

デフォルトの設定は 1 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central 内の登録再試行間隔を 10 分に設定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment retry period 10
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	すべての登録パラメータを、システムのデフォルト値に戻します。
enrollment retry count	登録要求の再試行回数を定義します。

enrollment terminal

このトラストポイントでカット アンド ペースト登録（手動登録とも呼ばれます）を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment terminal** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment terminal

no enrollment terminal

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の CA 登録にカット アンド ペースト方式を指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment terminal
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。
enrollment url	このトラストポイントに対して自動登録（SCEP）を指定して、URL を設定します。

enrollment url

このトラストポイントの登録に自動登録（SCEP）を指定して、登録 URL を設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment url** コマンドを使用します。このコマンドのデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment url *url*

no enrollment url

構文の説明

url	自動登録の URL の名前を指定します。最大の長さは 1000 文字です（実質的に無制限です）。

デフォルト

デフォルトの設定はオフです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central に URL https://enrollsite における SCEP 登録を指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# enrollment url https://enrollsite
hostname(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

enrollment-retrieval

登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定するには、ローカル CA サーバ コンフィギュレーション モードで **enrollment-retrieval** コマンドを使用します。期間をデフォルトの時間数（24）にリセットするには、このコマンドの **no** 形式を使用します。

enrollment-retrieval *timeout*

no enrollment-retrieval

構文の説明

timeout	何時間以内にユーザがローカル CA 登録 Web ページから発行された証明書を取得しなければならないかを指定します。有効なタイムアウト値の範囲は 1 ～ 720 時間です。

デフォルト

デフォルトでは、PKCS12 登録ファイルは 24 時間保存されて取得できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

PKCS12 登録ファイルには、発行された証明書とキー ペアが含まれています。ファイルはローカル CA サーバに保存され、**enrollment-retrieval** コマンドで指定された時間内は登録 Web ページから取得できます。

ユーザが登録可能とマークされている場合、そのユーザは **otp expiration** の時間内であればそのパスワードを使用して登録できます。ユーザが正常に登録すると、PKCS12 ファイルが生成および保存され、コピーが登録 Web ページを経由して返されます。何らかの理由でファイルのコピーが再度必要になった場合（登録しようとしてダウンロードに失敗した場合など）、ユーザは **enrollment-retrieval** コマンドで指定した時間内であれば新しくコピーを取得できます。

（注） この時間は、OTP の有効期限とは関係ありません。

例

次に、証明書の発行後 48 時間以内は PKCS12 登録ファイルをローカル CA サーバから取得できるように指定する例を示します。

```
hostname(config)# crypto ca server
```

```
hostname(config-ca-server)# enrollment-retrieval 48
hostname(config-ca-server)#
```

次に、取得可能時間をデフォルトの 24 時間にリセットする例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# no enrollment-retrieval
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
OTP expiration	CA 登録ページ用に発行されたワンタイム パスワードの有効期間を時間単位で指定します。
smtp from-address	CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示されるテキストを指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

eou allow

NAC フレームワーク コンフィギュレーションでクライアントレス認証をイネーブルにするには、グローバル コンフィギュレーション モードで **eou allow** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

eou allow {audit | clientless | none}

no eou allow {audit | clientless | none}

構文の説明

audit	監査サーバでクライアントレス認証を実行します。
clientless	Cisco ACS でクライアントレス認証を実行します。
none	クライアントレス認証をディセーブルにします。

デフォルト

デフォルトのコンフィギュレーションには、**eou allow clientless** コンフィギュレーションが含まれています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.3(0)	audit オプションを追加しました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、次の両方の条件が満たされている場合にのみこのコマンドが使用されます。

- NAC ポリシー タイプとして NAC フレームワークを使用するようにグループ ポリシーが設定されていること。
- セッションのホストが EAPoUDP 要求に応答しないこと。

例

次に、ACS を使用したクライアントレス認証の実行をイネーブルにする例を示します。

```
hostname(config)# eou allow clientless
hostname(config)#
```

次に、監査サーバを使用してクライアントレス認証を実行するようにセキュリティ アプライアンスを設定する例を示します。

```
hostname(config)# eou allow audit
hostname(config)#
```

次に、監査サーバの使用をディセーブルにする例を示します。

```
hostname(config)# no eou allow clientless
hostname(config)#
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou clientless	NAC フレームワーク コンフィギュレーションのクライアントレス認証で ACS に対して送信されるユーザ名およびパスワードを変更します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

eou clientless

NAC フレームワーク コンフィギュレーションにおけるクライアントレス認証でアクセス コントロール サーバに送信するユーザ名とパスワードを変更するには、グローバル コンフィギュレーション モードで **eou clientless** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou clientless username *username* **password** *password*

no eou clientless username *username* **password** *password*

構文の説明

password	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を取得するためにアクセス コントロール サーバに送信するパスワードを変更する場合に入力します。
password	クライアントレス ホストをサポートするためにアクセス コントロール サーバに設定されているパスワードを入力します。4 ～ 32 文字の ASCII 文字を入力します。
username	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を取得するためにアクセス コントロール サーバに送信するユーザ名を変更する場合に入力します。
username	クライアントレス ホストをサポートするためにアクセス コントロール サーバに設定されているユーザ名を入力します。先頭および末尾のスペース、シャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< および >）を除く、1 ～ 64 文字の ASCII 文字を入力します。

デフォルト

username 属性と password 属性のデフォルト値は、両方とも clientless です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、次の条件をすべて満たしている場合にのみ有効です。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上でクライアントレス認証がイネーブルになっている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、クライアントレス認証のユーザ名を sherlock に変更する例を示します。

```
hostname(config)# eou clientless username sherlock
hostname(config)#
```

次に、クライアントレス認証のユーザ名をデフォルト値である clientless に変更する例を示します。

```
hostname(config)# no eou clientless username
hostname(config)#
```

次に、クライアントレス認証のパスワードを secret に変更する例を示します。

```
hostname(config)# eou clientless password secret
hostname(config)#
```

次に、クライアントレス認証のパスワードをデフォルト値である clientless に変更する例を示します。

```
hostname(config)# no eou clientless password
hostname(config)#
```

関連コマンド

コマンド	説明
eou allow	NAC フレームワーク コンフィギュレーションでクライアントレス認証をイネーブルにします。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

eou initialize

1 つ以上の NAC フレームワーク セッションに割り当てられているリソースをクリアして、各セッションに対して新しい無条件のポスチャ検証を開始するには、特権 EXEC モードで **eou initialize** コマンドを使用します。

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

構文の説明

all	このセキュリティ アプライアンス上のすべての NAC フレームワーク セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC フレームワーク セッションを再確認します。
ip	単一の NAC フレームワーク セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

リモート ピアのポスチャが変更されたり、割り当てられているアクセス ポリシー（つまりダウンロードされた ACL）が変更されたりしたときに、セッションに割り当てられているリソースをクリアする場合は、このコマンドを使用します。このコマンドを入力すると、ポスチャ検証に使用される EAPoUDP アソシエーションおよびアクセス ポリシーが消去されます。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザ トラフィックに影響する場合があります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、すべての NAC フレームワーク セッションを初期化する例を示します。

```
hostname# eou initialize all
hostname
```

次に、tg1 というトンネル グループに割り当てられているすべての NAC フレームワーク セッションを初期化する例を示します。

```
hostname# eou initialize group tg1
hostname
```

次に、IP アドレス 209.165.200.225 を持つエンドポイントの NAC フレームワーク セッションを初期化する例を示します。

```
hostname# eou initialize 209.165.200.225
hostname
```

関連コマンド

コマンド	説明
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

eou max-retry

セキュリティ アプライアンスが EAP over UDP メッセージをリモート コンピュータに再送信する回数を変更するには、グローバル コンフィギュレーション モードで **eou max-retry** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou max-retry *retries*

no eou max-retry

構文の説明

retries	再送信タイマーが期限切れになった場合に再送信する回数を制限します。値は 1 ～ 3 の範囲で入力します。

デフォルト

デフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、次の条件をすべて満たしている場合にのみ有効です。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- セキュリティ アプライアンス上でクライアントレス認証がイネーブルになっている。
- セキュリティ アプライアンス上にネットワーク アドミッション コントロールが設定されている。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、EAP over UDP の再送信回数を 1 に制限する例を示します。

```
hostname(config)# eou max-retry 1
hostname(config)#
```

次に、EAP over UDP の再送信回数をデフォルト値である 3 に変更する例を示します。

```
hostname(config)# no eou max-retry
hostname(config)#
```

関連コマンド

eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

eou port

NAC フレームワーク コンフィギュレーションにおいて、Cisco Trust Agent との EAP over UDP 通信に使用するポート番号を変更するには、グローバル コンフィギュレーション モードで **eou port** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou port *port_number*

no eou port

構文の説明

port_number	EAP over UDP 通信用に指定するクライアント エンドポイントのポート番号。この番号は、Cisco Trust Agent に設定するポート番号です。値は 1024 ～ 65535 の範囲で入力します。

デフォルト

デフォルト値は 21862 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、EAP over UDP 通信のポート番号を 62445 に変更する例を示します。

```
hostname(config)# eou port 62445
hostname(config)#
```

次に、EAP over UDP 通信のポート番号をデフォルト値に変更する例を示します。

```
hostname(config)# no eou port
hostname(config)#
```

関連コマンド

debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou initialize	1 つ以上の NAC フレームワーク セッションに割り当てられているリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始します。

eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。
show vpn-session_summary.db	VLAN マッピング セッション データを含む、IPSec、Cisco AnyConnect、NAC の各セッションの数を表示します。
show vpn-session.db	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。

eou revalidate

1 つ以上の NAC フレームワーク セッションのポスチャ再検証をただちに実行するには、特権 EXEC モードで **eou revalidate** コマンドを使用します。

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

構文の説明

all	このセキュリティ アプライアンス上のすべての NAC フレームワーク セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC フレームワーク セッションを再確認します。
ip	単一の NAC フレームワーク セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ピアのポスチャ、または割り当てられているアクセス ポリシー（つまりダウンロードされた ACL が存在する場合その ACL）が変更された場合にこのコマンドを使用します。このコマンドは、新しい無条件のポスチャ検証を開始します。コマンド入力前に有効であったポスチャ検証および割り当てられているアクセス ポリシーは、新しいポスチャ検証に成功または失敗するまでは引き続き有効となります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、すべての NAC フレームワーク セッションを再検証する例を示します。

```
hostname# eou revalidate all
hostname
```

次に、tg-1 というトンネル グループに割り当てられているすべての NAC フレームワーク セッションを再検証する例を示します。

```
hostname# eou revalidate group tg-1
```

```
hostname
```

次に、IP アドレス 209.165.200.225 を持つエンドポイントの NAC フレームワーク セッションを初期化する例を示します。

```
hostname# eou revalidate ip 209.165.200.225
hostname
```

関連コマンド

コマンド	説明
eou initialize	1 つ以上の NAC フレームワーク セッションに割り当てられているリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始します。
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。

eou timeout

NAC フレームワーク コンフィギュレーションにおいて、リモート ホストに対して EAP over UDP メッセージを送信した後に待機する秒数を変更するには、グローバル コンフィギュレーション モードで **eou timeout** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou timeout {**hold-period | retransmit**} *seconds*

no eou timeout {**hold-period | retransmit**}

構文の説明

hold-period	EAPoUDP 再試行回数分の EAPoUDP メッセージを送信した後に待機する最大時間。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行した場合も、このタイマーがクリアされます。このタイマーが期限切れになった場合、セキュリティ アプライアンスはリモート ホストとの新しい EAP over UDP アソシエーションを開始します。
retransmit	1 回の EAPoUDP メッセージ送信後に待機する最大時間。リモート ホストから応答があると、このタイマーはクリアされます。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行した場合も、このタイマーがクリアされます。タイマーが期限切れになると、セキュリティ アプライアンスはリモート ホストに対して EAPoUDP メッセージを再送信します。
seconds	セキュリティ アプライアンスが待機する秒数。hold-period 属性には 60 ～ 86400 の範囲の値を、retransmit 属性には 1 ～ 60 の範囲の値を入力します。

デフォルト

hold-period 属性のデフォルト値は 180 です。

retransmit 属性のデフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、新しい EAP over UDP アソシエーションを開始するまでの待機時間を 120 秒に変更する例を示します。

```
hostname(config)# eou timeout hold-period 120
```

```
hostname(config)#
```

次に、新しい EAP over UDP アソシエーションを開始するまでの待機時間をデフォルト値に変更する例を示します。

```
hostname(config)# no eou timeout hold-period
hostname(config)#
```

次に、再送信タイマーを 6 秒に変更する例を示します。

```
hostname(config)# eou timeout retransmit 6
hostname(config)#
```

次に、再送信タイマーをデフォルト値に変更する例を示します。

```
hostname(config)# no eou timeout retransmit
hostname(config)#
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou max-retry	セキュリティ アプライアンスがリモート コンピュータに対して EAP over UDP メッセージを再送信する回数を変更します。

erase

ファイル システムを消去して再フォーマットするには、特権 EXEC モードで **erase** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むすべてのファイルを上書きしてファイル システムを消去し、ファイル システムを再インストールします。

erase [**disk0: | disk1: | flash:**]

構文の説明

disk0*:*	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	（任意）外部コンパクト フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	（任意）内部フラッシュ メモリを指定し、続けてコロンを入力します。 **注意** フラッシュ メモリを消去すると、フラッシュ メモリ内に保管されているライセンス情報も削除されます。フラッシュ メモリを消去する前に、ライセンス情報を保管してください。 ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

erase コマンドは、OxFF パターンを使用してフラッシュ メモリ上の全データを消去し、デバイスの空のファイル システム割り当てテーブルを再書き込みします。

（非表示のシステム ファイルを除く）表示されているすべてのファイルを削除する場合は、**erase** コマンドではなく **delete /recursive** コマンドを入力します。

（注） Cisco PIX セキュリティ アプライアンスでは、**erase** コマンドおよび **format** コマンドは両方とも、0xFF パターンを使用してユーザ データを破棄します。

（注）　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、**erase** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、**format** コマンドはファイル システムの制御構造をリセットするだけです。ロウ ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

例

次に、ファイル システムを消去して再フォーマットする例を示します。

```
hostname# erase flash:
```

関連コマンド

コマンド	説明
delete	非表示のシステム ファイルを除く表示されているすべてのファイルを削除します。
format	（非表示のシステム ファイルを含む）すべてのファイルを消去して、ファイル システムをフォーマットします。

esp

IPSec パススルー インスペクションで esp トンネルおよび AH トンネルのパラメータを指定するには、パラメータ コンフィギュレーション モードで **esp** コマンドを使用します。パラメータ コンフィギュレーション モードには、ポリシー マップ コンフィギュレーション モードからアクセスできます。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

{**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

構文の説明

esp	esp トンネルのパラメータを指定します。
ah	AH トンネルのパラメータを指定します。
per-client-max *num*	1 つのクライアントからの最大トンネル数を指定します。
timeout *time*	esp トンネルのアイドル タイムアウトを指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、UDP 500 のトラフィックを許可する例を示します。

```
hostname(config)# access-list test-udp-acl extended permit udp any any eq 500
hostname(config)# class-map test-udp-class
hostname(config-pmap-c)# match access-list test-udp-acl

hostname(config)# policy-map type inspect ipsec-pass-thru ipsec-map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# esp per-client-max 32 timeout 00:06:00
hostname(config-pmap-p)# ah per-client-max 16 timeout 00:05:00

hostname(config)# policy-map test-udp-policy
hostname(config-pmap)# class test-udp-class
hostname(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

established

確立された接続に基づく、ポートへの戻り接続を許可するには、グローバル コンフィギュレーション モードで **established** コマンドを使用します。**established** 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

構文の説明

est_protocol	確立された接続のルックアップに使用する IP プロトコル（UDP または TCP）を指定します。
dest_port	確立された接続のルックアップに使用する宛先ポートを指定します。
permitfrom	（任意）指定したポートから発信される戻りプロトコル接続を許可します。
permitto	（任意）指定したポートに着信する戻りプロトコル接続を許可します。
port [*-port*]	（任意）戻り接続の（UDP または TCP）宛先ポートを指定します。
protocol	（任意）戻り接続で使用される IP プロトコル（UDP または TCP）。
source_port	（任意）確立された接続のルックアップに使用する送信元ポートを指定します

デフォルト

デフォルトの設定は次のとおりです。

- *dest_port*：0（ワイルドカード）
- *source_port*：0（ワイルドカード）

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	キーワード **to** および **from** が CLI から削除されました。代わりにキーワード **permitto** および **permitfrom** を使用します。

使用上のガイドライン

established コマンドを使用すると、セキュリティ アプライアンス経由の発信接続の戻りアクセスを許可できます。このコマンドは、ネットワークから発信され、セキュリティ アプライアンスによって保護されている元の接続、および外部ホストからの同じ 2 つのデバイス間の着信戻り接続に対して動作します。**established** コマンドでは、接続のルックアップに使用する宛先ポートを指定できます。宛先

ポートを指定することによって、コマンドをより細かく制御でき、宛先ポートは既知であるが送信元ポートは不明であるプロトコルをサポートできます。**permitto** および **permitfrom** キーワードでは、リターン インバウンド接続を定義します。

注意　**established** コマンドでは、常に **permitto** キーワードおよび **permitfrom** キーワードを指定することを推奨します。これらのキーワードを指定しないで **established** コマンドを使用すると、外部システムに接続した場合にそれらのシステムから接続に関連する内部ホストに対して無制限に接続が可能となるため、セキュリティのリスクが発生します。このような状況は、内部システムの攻撃に悪用される可能性があります。

例

次に、**established** コマンドを正しく使用しない場合にセキュリティ違反が発生する可能性があることを示すいくつかの例を示します。

次に、内部システムから外部ホストのポート 4000 に TCP 接続を確立した場合に、外部ホストから任意のプロトコルを使用して任意のポートに戻り接続を確立できることを示す例を示します。

```
hostname(config)# established tcp 4000 0
```

プロトコルで使用されるポートが規定されていない場合は、送信元ポートおよび宛先ポートに **0** を指定できます。ワイルドカード ポート（0）は、必要な場合にのみ使用します。

```
hostname(config)# established tcp 0 0
```

（注）　**established** コマンドが正しく動作するためには、クライアントは **permitto** キーワードで指定されたポートでリッスンする必要があります。

established コマンドは、**nat 0** コマンドとともに使用できます（**global** コマンドがない場合）。

（注）　**established** コマンドは、PAT とともに使用することはできません。

セキュリティ アプライアンスでは、**established** コマンドを利用することによって XDMCP がサポートされます。

注意　セキュリティ アプライアンスを通して XWindows システム アプリケーションを使用すると、セキュリティのリスクが発生する可能性があります。

デフォルトで、XDMCP はオンになっていますが、次のように **established** コマンドを入力しないとセッションが完了しません。

```
hostname(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

established コマンドを入力すると、内部の XDMCP 実装ホスト（UNIX または Reflection X）から外部の XDMCP 実装 XWindows サーバにアクセスできます。UDP/177 ベースの XDMCP によって TCP ベースの XWindows セッションがネゴシエートされ、後続の TCP 戻り接続が許可されます。リターン トラフィックの送信元ポートは不明であるため、*source_port* フィールドには 0（ワイルドカード）を指定します。*dest_port* は 6000 + *n* となります。*n* は、ローカルのディスプレイ番号を表します。この値を変更するには、次の UNIX コマンドを使用します。

```
hostname(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

（ユーザ対話に基づいて）数多くの TCP 接続が生成され、これらの接続の送信元ポートが不明であるため、**established** コマンドが必要となります。宛先ポートのみがスタティックです。セキュリティ アプライアンスでは、XDMCP フィックスアップが透過的に実行されます。コンフィギュレーションは必要ありませんが、TCP セッションを確立できるように **established** コマンドを入力する必要があります。

次に、プロトコル A、宛先ポート B、送信元ポート C を使用した 2 つのホスト間の接続の例を示します。セキュリティ アプライアンス経由でプロトコル D（プロトコル D はプロトコル A とは異なっていてもかまいません）による戻り接続を許可するには、送信元ポートがポート F に、宛先ポートがポート E に対応している必要があります。

```
hostname(config)# established A B C permitto D E permitfrom D F
```

次に、TCP 宛先ポート 6060、および任意の送信元ポートを使用して、内部ホストから外部ホストに接続を開始する例を示します。セキュリティ アプライアンスでは、TCP 宛先ポート 6061 および任意の TCP 送信元ポートを使用したホスト間のリターン トラフィックが許可されます。

```
hostname(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

次に、UDP 宛先ポート 6060、および任意の送信元ポートを使用して、内部ホストから外部ホストに接続を開始する例を示します。セキュリティ アプライアンスでは、TCP 宛先ポート 6061 および TCP 送信元ポート 1024 ～ 65535 を使用したホスト間のリターン トラフィックが許可されます。

```
hostname(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

次に、ローカル ホストから外部ホストにポート 9999 への TCP 接続を開始する例を示します。この例では、外部ホストのポート 4242 からローカル ホストのポート 5454 へのパケットが許可されます。

```
hostname(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

関連コマンド

コマンド	説明
clear configure established	確立されたコマンドをすべて削除します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。

exceed-mss

スリーウェイ ハンドシェイクでピアによって設定された TCP 最大セグメント サイズを超えるデータ長のパケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

構文の説明

allow	MSS を超えるパケットを許可します。この設定は、デフォルトです。
drop	MSS を超えるパケットをドロップします。

デフォルト

パケットは、デフォルトで許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。
7.2(4)/8.0(4)	デフォルトが **drop** から **allow** に変更されました。

使用上のガイドライン

tcp-map コマンドはモジュラ ポリシー フレームワーク インフラストラクチャと一緒に使用されます。**class-map** コマンドを使用してトラフィックのクラスを定義し、**tcp-map** コマンドで TCP インスペクションをカスタマイズします。**policy-map** コマンドを使用して、新しい TCP マップを適用します。**service-policy** コマンドで、TCP インスペクションをアクティブにします。

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。スリーウェイ ハンドシェイクでピアによって設定された TCP 最大セグメント サイズを超えるデータ長の TCP パケットをドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。

例

次に、MSS を超えた場合にポート 21 のフローをドロップする例を示します。

```
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# exceed-mss drop
hostname(config)# class-map cmap
hostname(config-cmap)# match port tcp eq ftp
hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

```
hostname(config-pmap)# set connection advanced-options tmap
hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection advanced-options	TCP 正規化を含む、高度な接続機能を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

exempt-list

ポスチャ検証を免除されるリモート コンピュータ タイプのリストにエントリを追加するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **exempt-list** コマンドを使用します。免除リストからエントリを削除するには、このコマンドの **no** 形式を使用して、削除するエントリのオペレーティング システムおよび ACL を指定します。

exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

no exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

構文の説明

acl-name	セキュリティ アプライアンス コンフィギュレーションに存在する ACL の名前。指定する場合は、**filter** キーワードの後に指定する必要があります。
disable	次の 2 つの機能のいずれかを実行します。 • "os-name" の後に入力した場合、セキュリティ アプライアンスは、指定したオペレーティング システムを実行するリモート ホストで免除を行わず、NAC ポスチャ検証を適用します。 • *acl-name* の後に入力した場合、セキュリティ アプライアンスは指定したオペレーティング システムを免除しますが、関連するトラフィックに ACL を割り当てません。
filter	コンピュータのオペレーティング システムが *os name* に一致する場合にトラフィックをフィルタリングするための ACL を適用します。**filter** と *acl-name* のペアは省略可能です。
os	オペレーティング システムをポスチャ検証から免除します。
os name	オペレーティング システム名。名前にスペースが含まれている場合にのみ引用符が必要です（たとえば `"Windows XP"`）。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.3(0)	コマンド名が **vpn-nac-exempt** から **exempt-list** に変更されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

コマンドでオペレーティング システムを指定しても、例外リストに追加済みのエントリは上書きされません。免除する各オペレーティング システムおよび ACL に対して 1 つずつコマンドを入力します。

no exempt-list コマンドを入力すると、NAC フレームワーク ポリシーからすべての免除が削除されます。エントリを指定してこのコマンドの **no** 形式を発行すると、そのエントリが免除リストから削除されます。

NAC ポリシーに関連付けられている免除リストからすべてのエントリを削除するには、キーワードを指定しないでこのコマンドの **no** 形式を使用します。

例

次に、ポスチャ検証を免除するコンピュータのリストに Windows XP を実行するすべてのホストを追加する例を示します。

```
hostname(config-group-policy)# exempt-list os "Windows XP"
hostname(config-group-policy)
```

次に、Windows XP を実行するすべてのホストを免除して、これらのホストのトラフィックに ACL acl-1 を適用する例を示します。

```
hostname(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
hostname(config-nac-policy-nac-framework)
```

次に、免除リストから上記の例と同じエントリを削除する例を示します。

```
hostname(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
hostname(config-nac-policy-nac-framework)
```

次に、免除リストからすべてのエントリを削除する例を示します。

```
hostname(config-nac-policy-nac-framework)# no exempt-list
hostname(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
show vpn-session_summary.db	IPSec、Cisco AnyConnect、および NAC の各セッションの数を表示します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

exit

現在のコンフィギュレーション モードを終了するか、特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**exit** コマンドを使用します。

exit

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

キー シーケンス Ctrl+Z を使用して、グローバル コンフィギュレーション（および上位の）モードを終了することもできます。このキー シーケンスは、特権 EXEC モードまたはユーザ EXEC モードでは動作しません。

特権 EXEC モードまたはユーザ EXEC モードで **exit** コマンドを入力すると、セキュリティ アプライアンスからログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了して、セッションからログアウトする方法の例を示します。

```
hostname(config)# exit
hostname# exit

Logoff
```

次に、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後 **disable** コマンドを使用して特権 EXEC モードを終了する例を示します。

```
hostname(config)# exit
hostname# disable
hostname>
```

関連コマンド

コマンド	説明
quit	コンフィギュレーション モードを終了するか、または特権 EXEC モードやユーザ EXEC モードからログアウトします。

expiry-time

再検証しないでオブジェクトをキャッシュする有効期限を設定するには、キャッシュ コンフィギュレーション モードで **expiry-time** コマンドを使用します。コンフィギュレーションから有効期限を削除してデフォルト値に戻すには、このコマンドの **no** 形式を使用します。

expiry-time *time*

no expiry-time

構文の説明

time	セキュリティ アプライアンスが再検証しないでオブジェクトをキャッシュする時間（分）。

デフォルト

1 分。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

有効期限とは、セキュリティ アプライアンスが再検証しないでオブジェクトをキャッシュする時間（分）を指します。再検証では、内容が再度チェックされます。

例

次に、有効期限を 13 分に設定する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#expiry-time 13
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	WebVPN キャッシュ モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュをディセーブルにします。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。

コマンド	説明
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

export

証明書をクライアントにエクスポートすることを指定するには、CTL プロバイダー コンフィギュレーション モードで **export** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

export certificate *trustpoint_name*

no export certificate [*trustpoint_name*]

構文の説明

certificate *trustpoint_name*　クライアントにエクスポートする証明書を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CTL プロバイダー コンフィギュレーション モードで **export** コマンドを使用して、証明書をクライアントにエクスポートすることを指定します。トラストポイント名は、**crypto ca trustpoint** コマンドで定義します。証明書は、CTL クライアントで構成された証明書信頼リスト ファイルに追加されます。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
hostname(config)# ctl-provider my_ctl
hostname(config-ctl-provider)# client interface inside 172.23.45.1
hostname(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
hostname(config-ctl-provider)# export certificate ccm_proxy
hostname(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー モードで CTL プロバイダー インスタンスを設定します。

コマンド	説明
client	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードも指定します。
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

export webvpn customization

クライアントレス SSL VPN ユーザに表示される画面をカスタマイズするカスタマイゼーション オブジェクトをエクスポートするには、特権 EXEC モードで **export webvpn customization** コマンドを使用します。

export webvpn customization *name url*

構文の説明

name	カスタマイゼーション オブジェクトを識別する名前。最大 64 文字です。
url	XML カスタマイゼーション オブジェクトをエクスポートする *URL/filename* 形式のリモート パスとファイル名（最大 255 文字）。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

カスタマイゼーション オブジェクトとは、キャッシュ メモリ内にあり、クライアントレス SSL VPN ユーザに表示される画面（ログイン画面、ログアウト画面、ポータル ページ、使用可能な言語など）をカスタマイズする XML ファイルです。カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。

カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度セキュリティ アプライアンスにインポートできます。

Template の内容は、DfltCustomization オブジェクトの初期状態と同じです。

export webvpn customization コマンドを使用してカスタマイゼーション オブジェクトをエクスポートし、XML タグを変更し、**import webvpn customization** コマンドを使用して新しいオブジェクトとしてファイルをインポートできます。

例

次に、デフォルトのカスタマイゼーション オブジェクト（DfltCustomization）をエクスポートして、dflt_custom という名前の XML ファイルを作成する例を示します。

```
hostname# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
```

```
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
hostname#
```

関連コマンド

コマンド	説明
import webvpn customization	XML ファイルをカスタマイゼーション オブジェクトとしてキャッシュ メモリにインポートします。
revert webvpn customization	キャッシュ メモリからカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	キャッシュ メモリにあるカスタマイゼーション オブジェクトに関する情報を表示します。

export webvpn translation-table

SSL VPN 接続を確立するリモート ユーザに表示される用語を変換するために使用される変換テーブルをエクスポートするには、特権 EXEC モードで **export webvpn translation-table** コマンドを使用します。

export webvpn translation-table *translation_domain* {**language** *language* | **template**} *url*

構文の説明

language	事前にインポート済みの変換テーブル名を指定します。値は、ブラウザの言語オプションの表現に従って入力します。
translation_domain	機能エリアおよび関連するメッセージです。使用上のガイドラインのセクションに、使用可能な変換ドメインがリストされています。
url	オブジェクトの URL を指定します。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスでは、ブラウザベースのクライアントレス SSL VPN 接続を開始するユーザに表示されるポータルと画面、および AnyConnect VPN クライアント ユーザに表示されるユーザ インターフェイスで使用される言語を変換できます。

リモート ユーザに表示される各機能エリアとそのメッセージには独自の変換ドメインがあります。この変換ドメインは *translation_domain* 引数で指定します。次の表に、変換ドメインおよび、変換される機能領域を示します。

表 12-1　変換ドメインと影響を受ける機能エリア

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。

変換ドメイン	変換される機能エリア
banners	リモート ユーザに表示されるバナーと、VPN アクセスが拒否されたときのメッセージ。
PortForwarder	ポート フォワーディング ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。

変換テンプレートは変換テーブルと同じ形式の XML ファイルですが、変換内容はすべて空です。セキュリティ アプライアンスのソフトウェア イメージ パッケージには、標準機能の一部として各ドメイン用のテンプレートが含まれています。プラグインのテンプレートはプラグインに付属しており、独自の変換ドメインを定義します。クライアントレス ユーザのログインおよびログアウト ページ、ポータル ページ、および URL ブックマークはカスタマイズが可能なため、セキュリティ アプライアンスは **customization** および **url-list** 変換ドメイン テンプレートをダイナミックに生成し、テンプレートは変更内容をこれらの機能エリアに自動的に反映させます。

以前にインポートされた変換テーブルをエクスポートすると、URL の場所にそのテーブルの XML ファイルが作成されます。**show import webvpn translation-table** コマンドを使用して、使用可能なテンプレート、およびインポート済みのテーブルのリストを表示できます。

export webvpn translation-table コマンドを使用してテンプレートまたは変換テーブルをダウンロードし、メッセージを変更し、**import webvpn translation-table** コマンドを使用して変換テーブルをインポートします。

例

次に、変換ドメイン *customization* 用のテンプレートをエクスポートする例を示します。このドメインは、クライアントレス SSL VPN 接続を確立するリモート ユーザがカスタマイズおよび表示可能なログイン ページ、ログアウト ページ、ポータル ページ、およびすべてのメッセージを変換するために使用します。セキュリティ アプライアンスは、*Sales* という名前の XML ファイルを作成します。

```
hostname# export webvpn translation-table customization template
tftp://209.165.200.225/Sales
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

次に、*zh* という名前の、以前にインポートされた中国語用変換テーブルをエクスポートする例を示します。この短縮形 zh は、Microsoft Internet Explorer ブラウザの [Internet Options] で中国語に指定されている短縮形に準拠しています。セキュリティ アプライアンスは、*Chinese* という名前の XML ファイルを作成します。

```
hostname# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

関連コマンド

コマンド	説明
import webvpn translation-table	変換テーブルをインポートします。
revert	キャッシュ メモリから変換テーブルを削除します。
show import webvpn translation-table	インポートした変換テーブルに関する情報を表示します。

export webvpn url-list

URL リストをリモートの場所にエクスポートするには、特権 EXEC モードで **export webvpn url-list** コマンドを使用します。

export webvpn url-list *name url*

構文の説明

name	URL リストを識別する名前。最大 64 文字です。
URL	URL リストのソースへのリモート パス。最大 255 文字です。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

WebVPN には、デフォルトで URL リストはありません。

export webvpn url-list コマンドを使用して、Template というオブジェクトをダウンロードできます。Template は、変更または削除できません。Template の内容を編集してカスタム URL リストとして保存し、**import webvpn url-list** コマンドを使用してインポートし、カスタム URL リストを追加できます。

インポート済みの URL リストをエクスポートすると、URL の場所にそのリストの XML ファイルが作成されます。**show import webvpn url-list** コマンドを使用して、使用可能なテンプレート、およびインポート済みのテーブルのリストを表示できます。

例

次に、URL リスト *servers* をエクスポートする例を示します。

```
hostname# export webvpn url-list servers2 tftp://209.165.200.225
hostname#
```

関連コマンド

コマンド	説明
import webvpn url-list	URL リストをインポートします。

revert webvpn url-list	キャッシュ メモリから URL リストを削除します。
show import webvpn url-list	インポート済みの URL リストに関する情報を表示します。

export webvpn webcontent

リモートのクライアントレス SSL VPN ユーザに表示される、フラッシュ メモリ内のインポート済みコンテンツをエクスポートするには、特権 EXEC モードで **export webvpn webcontent** コマンドを使用します。

export webvpn webcontent <*source url*> <*destination url*>

構文の説明

<*source url*>	コンテンツがあるセキュリティ アプライアンスのフラッシュ メモリの URL。最大 64 文字です。
<*destination url*>	エクスポート先の URL。最大 255 文字です。

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

webcontent オプションを使用してエクスポートされるコンテンツは、リモートのクライアントレス ユーザに表示されるコンテンツです。これには、クライアントレス ポータルに表示されるインポート済みのヘルプ コンテンツや、カスタマイゼーション オブジェクトによって使用されるロゴなどがあります。

export webvpn webcontent コマンドの後に疑問符（**?**）を入力すると、エクスポート可能なコンテンツのリストを表示できます。次に例を示します。

```
hostname# export webvpn webcontent ?

Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

例

次に、tftp を使用してファイル *logo.gif* を、*logo_copy.gif* というファイル名で 209.165.200.225 にエクスポートする例を示します。

```
hostname# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

関連コマンド

コマンド	説明
import webvpn webcontent	クライアントレス SSL VPN ユーザに表示されるコンテンツをインポートします。
revert webvpn webcontent	コンテンツをフラッシュ メモリから削除します。
show import webvpn webcontent	インポートされたコンテンツに関する情報を表示します。

failover

フェールオーバーをイネーブルにするには、グローバル コンフィギュレーション モードで **failover** コマンドを使用します。フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

failover

no failover

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

フェールオーバーはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コンフィギュレーションでのフェールオーバーのイネーブルまたはディセーブルに限定されました（**failover active** コマンドを参照）。

使用上のガイドライン

フェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

ASA 5505 デバイスでは、ステートレス フェールオーバーのみが、Easy VPN ハードウェア クライアントとして動作していないときにのみ許可されます。

例

次に、フェールオーバーをディセーブルにする例を示します。

```
hostname(config)# no failover
hostname(config)#
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover active	スタンバイ ユニットをアクティブに切り替えます。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover active

スタンバイのセキュリティ アプライアンスまたはフェールオーバー グループをアクティブ ステートに切り替えるには、特権 EXEC モードで **failover active** コマンドを使用します。アクティブなセキュリティ アプライアンスまたはフェールオーバー グループをスタンバイに切り替えるには、このコマンドの **no** 形式を使用します。

failover active [**group** *group_id*]

no failover active [**group** *group_id*]

構文の説明

group *group_id*	（任意）アクティブにするフェールオーバー グループを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、フェールオーバー グループを含むように変更されました。

使用上のガイドライン

スタンバイ ユニットからのフェールオーバー切り替えを開始するには **failover active** コマンドを使用し、アクティブ ユニットからのフェールオーバー切り替えを開始するには **no failover active** コマンドを使用します。この機能を使用して、障害が発生したユニットを稼働させたり、メンテナンスのためにアクティブ ユニットをオフラインにしたりできます。ステートフル フェールオーバーを使用していない場合は、すべてのアクティブな接続がドロップされるため、フェールオーバー実行後にクライアントは接続を再確立する必要があります。

フェールオーバー グループの切り替えは、Active/Active フェールオーバーでのみ使用できます。Active/Active フェールオーバー ユニットでフェールオーバー グループを指定しないで **failover active** コマンドを入力すると、ユニットのすべてのグループがアクティブになります。

例

次に、スタンバイ グループ 1 をアクティブに切り替える例を示します。

```
hostname# failover active group 1
```

関連コマンド

コマンド	説明
failover reset	セキュリティ アプライアンスを障害発生状態からスタンバイに移行します。

failover exec

フェールオーバー ペアの特定のユニットに対してコマンドを実行するには、特権 EXEC モードまたはグローバル コンフィギュレーション モードで **failover exec** コマンドを使用します。

failover exec {**active** | **standby** | **mate**} *cmd_string*

構文の説明

active	コマンドをフェールオーバー ペアのアクティブ ユニットまたはフェールオーバー グループに対して実行することを指定します。アクティブ ユニットまたはフェールオーバー グループに対して入力されたコンフィギュレーション コマンドは、スタンバイ ユニットまたはフェールオーバー グループに複製されます。
cmd_string	実行するコマンド。show コマンド、コンフィギュレーション コマンド、および EXEC コマンドがサポートされています。
mate	コマンドをフェールオーバー ピアに対して実行することを指定します。
standby	コマンドをフェールオーバー ペアのスタンバイ ユニットまたはフェールオーバー グループに対して実行することを指定します。スタンバイ ユニットまたはフェールオーバー グループに対して実行されたコンフィギュレーション コマンドは、アクティブ ユニットまたはフェールオーバー グループには複製されません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

failover exec コマンドを使用して、フェールオーバー ペアの特定のユニットに対してコマンドを送信できます。

コンフィギュレーション コマンドはアクティブ ユニットまたはコンテキストからスタンバイ ユニットまたはコンテキストに複製されるため、いずれのユニットにログインしているかにかかわらず、**failover exec** コマンドを使用して正しいユニットにコンフィギュレーション コマンドを入力できます。たとえば、スタンバイ ユニットにログインしている場合、**failover exec active** コマンドを使用して、コンフィギュレーションの変更をアクティブ ユニットに送信できます。その後、これらの変更はスタンバイ装置に複製されます。スタンバイ装置またはコンテキストへのコンフィギュレーション コマンドの送信には、**failover exec** コマンドを使用しないでください。これらのコンフィギュレーションの変更はアクティブ装置に複製されないため、2 つのコンフィギュレーションが同期されなくなります。

コンフィギュレーション、exec、および **show** コマンドの出力は、現在のターミナル セッションで表示されます。したがって、**failover exec** コマンドを使用して、ピア装置で **show** コマンドを発行し、その結果を現在のターミナルに表示することができます。

ピア装置でコマンドを実行するには、ローカル装置でコマンドを実行できるだけの十分な権限を持っている必要があります。

コマンド モード

failover exec コマンドは、お使いのターミナル セッションのコマンド モードとは異なるコマンド モード状態を維持します。デフォルトで、**failover exec** のコマンド モードは、指定したデバイスに対するグローバル コンフィギュレーション モードです。このコマンド モードを変更するには、**failover exec** コマンドを使用して適切なコマンド（**interface** コマンドなど）を送信します。

指定されたデバイスの **failover exec** コマンド モードを変更しても、デバイスへのアクセスに使用しているセッションのコマンド モードは変更されません。たとえば、フェールオーバー ペアのアクティブ ユニットにログインしており、グローバル コンフィギュレーション モードで次のコマンドを発行した場合、セッションのコマンド モードはグローバル コンフィギュレーション モードのままですが、**failover exec** コマンドを使用して送信されるすべてのコマンドはインターフェイス コンフィギュレーション モードで実行されます。

```
hostname(config)# failover exec interface GigabitEthernet0/1
hostname(config)#
```

デバイスとの現在のセッションのコマンド モードを変更しても、**failover exec** コマンドで使用されるコマンド モードには影響しません。たとえば、アクティブ ユニットでインターフェイス コンフィギュレーション モードであるときに、**failover exec** のコマンド モードを変更していない場合、次のコマンドはグローバル コンフィギュレーション モードで実行されます。

```
hostname(config-if)# failover exec active router ospf 100
hostname(config-if)#
```

show failover exec コマンドを使用すると、指定したデバイスにコマンド モードが表示されます。**failover exec** コマンドを使用して送信されたコマンドは、このモードで実行されます。

セキュリティに関する注意事項

failover exec コマンドは、フェールオーバー リンクを使用してコマンドをピア装置に送信し、実行されたコマンドの出力をピア装置から受信します。盗聴や中間者攻撃を防止するには、**failover key** コマンドを使用してフェールオーバー リンクを暗号化する必要があります。

制限事項

- ゼロダウンタイム アップグレード手順を使用して 1 台の装置だけをアップグレードする場合は、機能するコマンドとして **failover exec** コマンドをサポートしているソフトウェアが両方の装置で動作している必要があります。
- コマンドの完成およびコンテキスト ヘルプは、*cmd_string* 引数のコマンドでは使用できません。
- マルチ コンテキスト モードでは、ピア装置のピア コンテキストだけにコマンドを送信できます。異なるコンテキストにコマンドを送信するには、まずログインしているユニットでそのコンテキストに変更する必要があります。
- 次のコマンドと **failover exec** コマンドを一緒に使用することはできません。
  - **changeto**
  - **debug**（**undebug**）
- スタンバイ装置が故障状態の場合、故障の原因がサービス カードの不具合であれば、**failover exec** コマンドからのコマンドは受信できます。それ以外の場合、リモート コマンドの実行は失敗します。

- **failover exec** コマンドを使用して、フェールオーバー ピアで特権 EXEC モードをグローバル コンフィギュレーション モードに切り替えることはできません。たとえば、現在の装置が特権 EXEC モードのときに **failover exec mate configure terminal** を入力すると、**show failover exec mate** の出力に、failover exec セッションがグローバル コンフィギュレーション モードであることが示されます。ただし、ピア装置で **failover exec** を使用してコンフィギュレーション コマンドを入力した場合、現在の装置でグローバル コンフィギュレーション モードを開始しない限り、その処理は失敗します。
- **failover exec mate failover exec mate** *コマンド*のような、再帰的な failover exec コマンドは入力できません。
- ユーザの入力または確認が必要なコマンドでは、**/nonconfirm** オプションを使用する必要があります。

例

次に、**failover exec** コマンドを使用して、アクティブ ユニットのフェールオーバー情報を表示する例を示します。コマンドはアクティブ ユニットで実行されるため、コマンドはローカルで実行されます。

```
hostname(config)# failover exec active show failover

Failover On
Failover unit Primary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:31:50 jst May 2 2004
        This host: Primary - Active
                Active time: 2483 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         328        0          328        0
        sys cmd         329        0          329        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       329
        Xmit Q:         0       1       329
hostname(config)#
```

次に、**failover exec** コマンドを使用して、ピア ユニットのフェールオーバー ステータスを表示する例を示します。コマンドはアクティブ ユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
hostname(config)# failover exec mate show failover

Failover On
Failover unit Secondary
Failover LAN Interface: failover GigabitEthernet0/3 (up)
Unit Poll frequency 1 seconds, holdtime 3 seconds
Interface Poll frequency 3 seconds, holdtime 15 seconds
Interface Policy 1
Monitored Interfaces 2 of 250 maximum
Version: Ours 8.0(2), Mate 8.0(2)
Last Failover at: 09:19:59 jst May 2 2004
        This host: Secondary - Standby Ready
                Active time: 0 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.111): Normal
                  admin Interface inside (192.168.0.11): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)
        Other host: Primary - Active
                Active time: 2604 (sec)
                slot 0: ASA5520 hw/sw rev (1.0/8.0(2)) status (Up Sys)
                  admin Interface outside (192.168.5.101): Normal
                  admin Interface inside (192.168.0.1): Normal
                slot 1: ASA-SSM-20 hw/sw rev (1.0/) status (Up/Up)

Stateful Failover Logical Update Statistics
        Link : failover GigabitEthernet0/3 (up)
        Stateful Obj    xmit       xerr       rcv        rerr
        General         344        0          344        0
        sys cmd         344        0          344        0
        up time         0          0          0          0
        RPC services    0          0          0          0
        TCP conn        0          0          0          0
        UDP conn        0          0          0          0
        ARP tbl         0          0          0          0
        Xlate_Timeout   0          0          0          0

        Logical Update Queue Information
                        Cur     Max     Total
        Recv Q:         0       1       344
        Xmit Q:         0       1       344
```

次に、**failover exec** コマンドを使用して、フェールオーバー ピアのフェールオーバー コンフィギュレーションを表示する例を示します。コマンドはアクティブ ユニットであるプライマリ ユニットで実行されるため、セカンダリのスタンバイ ユニットの情報が表示されます。

```
hostname(config)# failover exec mate show running-config failover

failover
failover lan interface failover GigabitEthernet0/3
failover polltime unit 1 holdtime 3
failover polltime interface 3 holdtime 15
failover link failover GigabitEthernet0/3
failover interface ip failover 10.0.5.1 255.255.255.0 standby 10.0.5.2
ciscoasa(config)#
```

次に、**failover exec** コマンドを使用して、スタンバイ ユニットからアクティブ ユニットにコンテキストを作成する例を示します。コマンドは、アクティブ ユニットからスタンバイ ユニットに複製されます。「Creating context」というメッセージが 2 回表示されていることに注意してください。1 回めは、コンテキスト作成時に **failover exec** コマンドによってピア ユニットから出力されたものであり、2 回めは複製されたコマンドによってローカルにコンテキストが作成されたときにローカル ユニットから出力されたものです。

```
hostname(config)# show context

Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1

Total active Security Contexts: 1

! The following is executed in the system execution space on the standby unit.

hostname(config)# failover exec active context text

Creating context 'text'... Done. (2)
Creating context 'text'... Done. (3)

hostname(config)# show context
Context Name      Class      Interfaces           URL
*admin            default    GigabitEthernet0/0,  disk0:/admin.cfg
                             GigabitEthernet0/1
 text             default                         (not entered)

Total active Security Contexts: 2
```

次に、**failover exec** コマンドを使用してスタンバイ ステートのフェールオーバー ピアにコンフィギュレーション コマンドを送信したときに警告が返され、その警告が表示される例を示します。

```
hostname# failover exec mate static (inside,outside) 192.168.5.241 192.168.0.241

        **** WARNING ****
        Configuration Replication is NOT performed from Standby unit to Active unit.
        Configurations are no longer synchronized.
hostname(config)#
```

次に、**failover exec** コマンドを使用して、**show interface** コマンドをスタンバイ ユニットに送信する例を示します。

```
hostname(config)# failover exec standby show interface

Interface GigabitEthernet0/0 "outside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
      Auto-Duplex(Half-duplex), Auto-Speed(100 Mbps)
      MAC address 000b.fcf8.c290, MTU 1500
      IP address 192.168.5.111, subnet mask 255.255.255.0
      216 packets input, 27030 bytes, 0 no buffer
      Received 2 broadcasts, 0 runts, 0 giants
      0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
      0 L2 decode drops
      284 packets output, 32124 bytes, 0 underruns
      0 output errors, 0 collisions
      0 late collisions, 0 deferred
      input queue (curr/max blocks): hardware (0/0) software (0/0)
      output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "outside":
      215 packets input, 23096 bytes
```

```
        284 packets output, 26976 bytes
        0 packets dropped
        1 minute input rate 0 pkts/sec,  21 bytes/sec
        1 minute output rate 0 pkts/sec,  23 bytes/sec
        1 minute drop rate, 0 pkts/sec
        5 minute input rate 0 pkts/sec,  21 bytes/sec
        5 minute output rate 0 pkts/sec,  24 bytes/sec
        5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/1 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Half-duplex), Auto-Speed(10 Mbps)
        MAC address 000b.fcf8.c291, MTU 1500
        IP address 192.168.0.11, subnet mask 255.255.255.0
        214 packets input, 26902 bytes, 0 no buffer
        Received 1 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        215 packets output, 27028 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/1) software (0/0)
  Traffic Statistics for "inside":
        214 packets input, 23050 bytes
        215 packets output, 23140 bytes
        0 packets dropped
        1 minute input rate 0 pkts/sec,  21 bytes/sec
        1 minute output rate 0 pkts/sec,  21 bytes/sec
        1 minute drop rate, 0 pkts/sec
        5 minute input rate 0 pkts/sec,  21 bytes/sec
        5 minute output rate 0 pkts/sec,  21 bytes/sec
        5 minute drop rate, 0 pkts/sec
Interface GigabitEthernet0/2 "failover", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps
        Auto-Duplex(Full-duplex), Auto-Speed(100 Mbps)
        Description: LAN/STATE Failover Interface
        MAC address 000b.fcf8.c293, MTU 1500
        IP address 10.0.5.2, subnet mask 255.255.255.0
        1991 packets input, 408734 bytes, 0 no buffer
        Received 1 broadcasts, 0 runts, 0 giants
        0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        0 L2 decode drops
        1835 packets output, 254114 bytes, 0 underruns
        0 output errors, 0 collisions
        0 late collisions, 0 deferred
        input queue (curr/max blocks): hardware (0/0) software (0/0)
        output queue (curr/max blocks): hardware (0/2) software (0/0)
  Traffic Statistics for "failover":
        1913 packets input, 345310 bytes
        1755 packets output, 212452 bytes
        0 packets dropped
        1 minute input rate 1 pkts/sec,  319 bytes/sec
        1 minute output rate 1 pkts/sec,  194 bytes/sec
        1 minute drop rate, 0 pkts/sec
        5 minute input rate 1 pkts/sec,  318 bytes/sec
        5 minute output rate 1 pkts/sec,  192 bytes/sec
        5 minute drop rate, 0 pkts/sec
.
.
.
```

次に、ピア ユニットに対して不正なコマンドを発行したときにエラー メッセージが返され、そのエラー メッセージが表示される例を示します。

```
hostname# failover exec mate bad command

bad command
  ^
ERROR: % Invalid input detected at '^' marker.
```

次に、フェールオーバーがディセーブルの場合に **failover exec** コマンドを使用してエラー メッセージが返され、そのエラー メッセージが表示される例を示します。

```
hostname(config)# failover exec mate show failover

ERROR: Cannot execute command on mate because failover is disabled
```

関連コマンド

コマンド	説明
debug fover	フェールオーバー関連のデバッグ メッセージを表示します。
debug xml	**failover exec** コマンドによって使用される XML パーサーのデバッグ メッセージを表示します。
show failover exec	**failover exec** のコマンド モードを表示します。

failover group

Active/Active フェールオーバー グループを設定するには、グローバル コンフィギュレーション モードで **failover group** コマンドを使用します。フェールオーバー グループを削除するには、このコマンドの **no** 形式を使用します。

failover group *num*

no failover group *num*

構文の説明

num	フェールオーバー グループの番号。有効な値は、1 または 2 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

最大 2 つのフェールオーバー グループを定義できます。**failover group** コマンドは、マルチ コンテキスト モードが設定されたデバイスのシステム コンテキストにのみ追加できます。フェールオーバー グループは、フェールオーバーがディセーブルになっているときに限り作成および削除できます。

このコマンドを入力すると、フェールオーバー グループ コマンド モードが開始されます。フェールオーバー グループ コンフィギュレーション モードでは、**primary**、**secondary**、**preempt**、**replication http**、**interface-policy**、**mac address**、および **polltime interface** コマンドを使用できます。グローバル コンフィギュレーション モードに戻るには、**exit** コマンドを使用します。

（注） **failover polltime interface**、**failover interface-policy**、**failover replication http**、および **failover mac address** コマンドは、Active/Active フェールオーバー コンフィギュレーションでは効果がありません。これらは、**polltime interface**、**interface-policy**、**replication http**、および **mac address** の各フェールオーバー グループ コンフィギュレーション モード コマンドによって上書きされます。

フェールオーバー グループを削除するときは、フェールオーバー グループ 1 を最後に削除する必要があります。フェールオーバー グループ 1 には、常に管理コンテキストが含まれています。フェールオーバー グループに割り当てられていないすべてのコンテキストは、デフォルトでフェールオーバー グループ 1 に割り当てられます。コンテキストが明示的に割り当てられているフェールオーバー グループは削除できません。

（注）　同じネットワーク上にアクティブ/アクティブ フェールオーバー ペアが複数ある場合は、あるペアのインターフェイスに割り当てられているものと同じデフォルト仮想 MAC アドレスが、他のペアのインターフェイスに割り当てられることがあります。これは、デフォルト仮想 MAC アドレスの決定方法に基づいた動作です。ネットワーク上に重複した MAC アドレスが存在しないようにするには、**mac address** コマンドを使用して、各物理インターフェイスに対して仮想アクティブ MAC アドレスおよび仮想スタンバイ MAC アドレスを割り当てる必要があります。

例

次に、2 つのフェールオーバー グループのコンフィギュレーションの例（抜粋）を示します。

```
hostname(config)# failover group 1
hostname(config-fover-group)# primary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)# failover group 2
hostname(config-fover-group)# secondary
hostname(config-fover-group)# preempt 100
hostname(config-fover-group)# exit
hostname(config)#
```

関連コマンド

コマンド	説明
asr-group	非対称ルーティング インターフェイス グループ ID を指定します。
interface-policy	モニタリングによってインターフェイスの障害が検出された場合のフェールオーバー ポリシーを指定します。
join-failover-group	コンテキストをフェールオーバー グループに割り当てます。
mac address	フェールオーバー グループ内のコンテキストに対して仮想 MAC アドレスを定義します。
polltime interface	モニタ対象インターフェイスに送信される hello メッセージ間の時間を指定します。
preempt	高いプライオリティを持つユニットが、リブート後にアクティブ ユニットとなることを指定します。
primary	フェールオーバー グループにおいて、プライマリ ユニットに対してより高いプライオリティを指定します。
replication http	選択したフェールオーバー グループに対して、HTTP セッションのレプリケーションを指定します。
secondary	フェールオーバー グループにおいて、セカンダリ ユニットに対してより高いプライオリティを指定します。

failover interface ip

フェールオーバー インターフェイスおよびステートフル フェールオーバー インターフェイスに対して IP アドレスおよびマスクを指定するには、グローバル コンフィギュレーション モードで **failover interface ip** コマンドを使用します。IP アドレスを削除するには、このコマンドの **no** 形式を使用します。

failover interface ip *if_name ip_address mask* **standby** *ip_address*

no failover interface ip *if_name ip_address mask* **standby** *ip_address*

構文の説明

if_name	フェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスのインターフェイス名。
ip_address mask	プライマリ モジュールのフェールオーバー インターフェイスまたはステートフル フェールオーバー インターフェイスに対して IP アドレスおよびマスクを指定します。
standby *ip_address*	セカンダリ モジュールがプライマリ モジュールと通信する場合に使用する IP アドレスを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバー インターフェイスおよびステートフル フェールオーバー インターフェイスは、セキュリティ アプライアンスがトランスペアレント ファイアウォール モードで動作している場合でもレイヤ 3 の機能であり、システムに対してグローバルです。

マルチ コンテキスト モードでは、システム コンテキストにフェールオーバーを設定します（**monitor-interface** コマンドを除く）。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときに、コンフィギュレーションの一部である必要があります。

例

次に、フェールオーバー インターフェイスの IP アドレスおよびマスクを指定する例を示します。

```
hostname(config)# failover interface ip lanlink 172.27.48.1 255.255.255.0 standby
172.27.48.2
```

関連コマンド

コマンド	説明
clear configure failover	**failover** コマンドを実行コンフィギュレーションから消去し、フェールオーバーのデフォルト値に戻します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover link	ステートフル フェールオーバーに使用するインターフェイスを指定します。
monitor-interface	指定したインターフェイスの状態をモニタします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover interface-policy

モニタリングによってインターフェイスの障害が検出された場合のフェールオーバーのポリシーを指定するには、グローバル コンフィギュレーション モードで **failover interface-policy** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

failover interface-policy *num*[**%**]

no failover interface-policy *num*[**%**]

構文の説明

num	パーセンテージとして使用される場合は 1 ～ 100 の数値を、数値として使用される場合は 1 ～インターフェイスの最大数を指定します。
%	（任意）*num* の数字が、モニタ対象インターフェイスのパーセンテージであることを指定します。

デフォルト

デフォルトの設定は次のとおりです。

- *num* は 1 です。
- 物理インターフェイスのモニタリングは、デフォルトでイネーブルになっています。論理インターフェイスのモニタリングは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

num 引数とオプションの **%** キーワードの間にはスペースを挿入しません。

障害が発生したインターフェイスの数が設定されているポリシーの基準を満たし、他方のセキュリティ アプライアンスが正しく機能している場合、セキュリティ アプライアンスは自身を障害発生状態とマークして、フェールオーバーが行われる可能性があります（アクティブなセキュリティ アプライアンスで障害が発生した場合）。ポリシーでカウントされるのは、**monitor-interface** コマンドでモニタ対象として指定したインターフェイスのみです。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードで **interface-policy** コマンドを使用して、各フェールオーバー グループのインターフェイス ポリシーを設定します。

例

次に、2 通りの方法でフェールオーバー ポリシーを指定する例を示します。

```
hostname(config)# failover interface-policy 20%

hostname(config)# failover interface-policy 5
```

関連コマンド

コマンド	説明
failover polltime	ユニットおよびインターフェイスのポーリング タイムを指定します。
failover reset	障害が発生したユニットを障害が発生していない状態に復元します。
monitor-interface	フェールオーバーのためにモニタ対象にするインターフェイスを指定します。
show failover	装置のフェールオーバー状態についての情報を表示します。

failover key

フェールオーバー ペアのユニット間での暗号化および認証された通信用のキーを指定するには、グローバル コンフィギュレーション モードで **failover key** コマンドを使用します。キーを削除するには、このコマンドの **no** 形式を使用します。

failover key {*secret* | **hex** *key*}

no failover key

構文の説明

hex *key*	暗号キーの 16 進数値を指定します。キーは、32 文字の 16 進数文字（0 ～ 9、a ～ f）である必要があります。
secret	英数字の共有秘密を指定します。秘密に使用できる文字数は、1 ～ 63 文字です。有効な文字は、数字、文字、または句読点の任意の組み合わせです。共有秘密は、暗号キーを生成するために使用されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover lan key** から **failover key** に変更されました。
7.0(4)	このコマンドが、**hex** *key* キーワードおよび引数を含むように変更されました。

使用上のガイドライン

ユニット間のフェールオーバー通信を暗号化および認証するには、両方のユニットに共有秘密または 16 進キーを設定する必要があります。フェールオーバー キーを指定しない場合、フェールオーバー通信はクリア テキストで送信されます。

（注） PIX セキュリティ アプライアンス プラットフォームでは、ユニットへの接続に専用のシリアル フェールオーバー ケーブルを使用している場合、フェールオーバー キーを設定しても、フェールオーバー リンク上の通信は暗号化されません。フェールオーバー キーでは、LAN ベースのフェールオーバー通信のみが暗号化されます。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、フェールオーバー ペアのユニット間でフェールオーバー通信をセキュリティ保護するための共有秘密を指定する例を示します。

```
hostname(config)# failover key abcdefg
```

次に、フェールオーバー ペアの 2 つのユニット間でフェールオーバー通信をセキュリティ保護するための 16 進キーを指定する例を示します。

```
hostname(config)# failover key hex 6a1ed228381cf5c68557cb0c32e614dc
```

関連コマンド

コマンド	説明
show running-config failover	実行コンフィギュレーション内の failover コマンドを表示します。

failover lan enable

PIX セキュリティ アプライアンスで LAN ベースのフェールオーバーをイネーブルにするには、グローバル コンフィギュレーション モードで **failover lan enable** コマンドを使用します。LAN ベースのフェールオーバーをディセーブルにするには、このコマンドの **no** 形式を使用します。

failover lan enable

no failover lan enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

イネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

このコマンドの **no** 形式を使用して LAN ベースのフェールオーバーがディセーブルになっている場合、フェールオーバー ケーブルが接続されていると、ケーブルベースのフェールオーバーが使用されます。このコマンドは、PIX セキュリティ アプライアンスでのみ使用できます。

注意　フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、LAN ベースのフェールオーバーをイネーブルにする例を示します。

```
hostname(config)# failover lan enable
```

関連コマンド

コマンド	説明
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover lan interface

フェールオーバー通信に使用されるインターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover lan interface** コマンドを使用します。フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover lan interface *if_name* {*phy_if*[*.sub_if*] | *vlan_if*]}

no failover lan interface [*if_name* {*phy_if*[*.sub_if*] | *vlan_if*]}]

構文の説明

if_name	フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	物理インターフェイスを指定します。
sub_if	（任意）サブインターフェイス番号を指定します。
vlan_if	ASA 5505 セキュリティ アプライアンスで、VLAN インターフェイスをフェールオーバー リンクとして指定するために使用されます。

デフォルト

設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、*phy_if* 引数を含めるように変更されました。
7.2(1)	このコマンドが、*vlan_if* 引数を含むように変更されました。

使用上のガイドライン

LAN フェールオーバーでは、フェールオーバー トラフィックを送受信するための専用のインターフェイスが必要です。ただし、LAN フェールオーバー インターフェイスをステートフル フェールオーバー リンクに使用することもできます。

（注） LAN フェールオーバーとステートフル フェールオーバーの両方で同じインターフェイスを使用する場合は、LAN ベースのフェールオーバーとステートフル フェールオーバーの両方のトラフィックを処理するのに十分な容量がインターフェイスに必要です。

デバイス上の任意の未使用のイーサネット インターフェイスをフェールオーバー インターフェイスとして使用できます。現在名前が設定されているインターフェイスは指定できません。フェールオーバー インターフェイスは、通常のネットワーキング インターフェイスとしては設定されず、フェールオー

バー通信専用となります。このインターフェイスは、フェールオーバー リンク専用である必要があります（ただしステート リンクとしても使用可能）。LAN ベースのフェールオーバー リンクは、リンクにホストまたはルータのない専用スイッチを使用するか、装置を直接リンクするためのクロスオーバー イーサネット ケーブルを使用して接続できます。

（注） VLAN を使用する場合は、フェールオーバー リンク専用の VLAN を使用します。フェールオーバー リンクの VLAN を他の VLAN と共有すると、断続的にトラフィックの問題が発生したり、ping や ARP の障害が発生したりすることがあります。フェールオーバー リンクの接続にスイッチを使用する場合は、スイッチおよびセキュリティ アプライアンスでフェールオーバー リンク専用のインターフェイスを使用します。インターフェイスを、通常のネットワーク トラフィックを伝送するサブインターフェイスと共有しないでください。

マルチ コンテキスト モードで動作するシステムでは、フェールオーバー リンクはシステム コンテキストにあります。システム コンテキストに設定できるインターフェイスは、このインターフェイス、および使用されている場合はステート リンクのみです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

（注） フェールオーバー リンクの IP アドレスおよび MAC アドレスは、フェールオーバー時に変更されません。

このコマンドの **no** 形式を使用すると、フェールオーバー インターフェイスの IP アドレス コンフィギュレーションもクリアされます。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときに、コンフィギュレーションの一部である必要があります。

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれています。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、PIX 500 シリーズセキュリティ アプライアンスでフェールオーバー LAN インターフェイスを設定する例を示します。

```
hostname(config)# failover lan interface folink Ethernet4
```

次に、ASA 5500 シリーズセキュリティ アプライアンス（ASA 5505 セキュリティ アプライアンスを除く）でサブインターフェイスを使用してフェールオーバー LAN インターフェイスを設定する例を示します。

```
hostname(config)# failover lan interface folink GigabitEthernet0/3.1
```

次に、ASA 5505 セキュリティ アプライアンスでフェールオーバー LAN インターフェイスを設定する例を示します。

```
hostname(config)# failover lan interface folink Vlan6
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan unit	LAN ベースのフェールオーバーでの、プライマリ装置またはセカンダリ装置を指定します。
failover link	ステートフル フェールオーバー インターフェイスを指定します。

failover lan unit

LAN フェールオーバー設定でセキュリティ アプライアンスをプライマリ装置またはセカンダリ装置のいずれかに設定するには、グローバル コンフィギュレーション モードで **failover lan unit** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

failover lan unit {**primary** | **secondary**}

no failover lan unit {**primary** | **secondary**}

構文の説明

primary	セキュリティ アプライアンスをプライマリ ユニットとして指定します。
secondary	セキュリティ アプライアンスをセカンダリ ユニットとして指定します。

デフォルト

セカンダリ

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Active/Standby フェールオーバーでは、フェールオーバー ユニットに対するプライマリとセカンダリの指定によって、起動時にどのユニットがアクティブになるかが決まります。次の場合に、起動時にプライマリ ユニットがアクティブ ユニットになります。

- 最初のフェールオーバー ポーリング チェックの間に、プライマリ ユニットとセカンダリ ユニットの両方がブート シーケンスを完了している。
- プライマリ ユニットがセカンダリ ユニットよりも前に起動している。

プライマリ ユニットの起動時にすでにセカンダリ ユニットがアクティブになっている場合、プライマリ ユニットはアクティブにはならずに、スタンバイ ユニットとなります。この場合、プライマリ ユニットを強制的にアクティブ ステータスに戻すには、セカンダリ（アクティブ）ユニットで **no failover active** コマンドを発行する必要があります。

Active/Active フェールオーバーでは、各フェールオーバー グループにプライマリまたはセカンダリのユニット プリファレンスが割り当てられます。このプリファレンスによって、両方のユニットが（フェールオーバー ポーリング期間内に）同時に起動されたときに、起動時にフェールオーバー ペアのどのユニットでフェールオーバー グループのコンテキストがアクティブになるかが決まります。

このコマンドは、セキュリティ アプライアンスを LAN フェールオーバー用にブートストラップするときに、コンフィギュレーションの一部である必要があります。

例

次に、セキュリティ アプライアンスを LAN ベースのフェールオーバーのプライマリ ユニットとして設定する例を示します。

```
hostname(config)# failover lan unit primary
```

関連コマンド

コマンド	説明
failover lan enable	PIX セキュリティ アプライアンス上で、LAN ベースのフェールオーバーをイネーブルにします。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover link

ステートフル フェールオーバー インターフェイスを指定するには、グローバル コンフィギュレーション モードで **failover link** コマンドを使用します。ステートフル フェールオーバー インターフェイスを削除するには、このコマンドの **no** 形式を使用します。

failover link *if_name* [*phy_if*]

no failover link

構文の説明

if_name	ステートフル フェールオーバー専用のセキュリティ アプライアンス インターフェイスの名前を指定します。
phy_if	（任意）物理インターフェイス ポートまたは論理インターフェイス ポートを指定します。ステートフル フェールオーバー インターフェイスが、フェールオーバー通信に割り当てられているインターフェイスを共有しているか、または標準ファイアウォール インターフェイスを共有している場合、この引数は必要ありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、*phy_if* 引数を含めるように変更されました。
7.0(4)	このコマンドが、標準ファイアウォール インターフェイスを受け入れるように変更されました。

使用上のガイドライン

このコマンドは、ステートフル フェールオーバーをサポートしない ASA 5505 シリーズセキュリティ アプライアンスでは使用できません。

物理または論理インターフェイス引数は、フェールオーバー通信または標準ファイアウォール インターフェイスを共有していない場合に必要となります。

failover link コマンドによって、ステートフル フェールオーバーがイネーブルになります。ステートフル フェールオーバーをディセーブルにするには、**no failover link** コマンドを入力します。専用のステートフル フェールオーバー インターフェイスを使用している場合は、**no failover link** コマンドによって、ステートフル フェールオーバー インターフェイスの IP アドレス コンフィギュレーションもクリアされます。

ステートフル フェールオーバーを使用するには、すべての状態情報を送信するためのステートフル フェールオーバー リンクを設定する必要があります。ステートフル フェールオーバー リンクを設定する方法としては、次の 3 つのオプションがあります。

- ステートフル フェールオーバー リンクに、専用のイーサネット インターフェイスを使用できます。
- LAN ベースのフェールオーバーを使用する場合は、フェールオーバー リンクを共有できます。
- 内部インターフェイスなど、通常のデータ インターフェイスを共有できます。しかし、このオプションはお勧めしません。

ステートフル フェールオーバー リンクに専用のイーサネット インターフェイスを使用する場合は、スイッチまたはクロス ケーブルを使用して、ユニットを直接接続できます。スイッチを使用する場合は、このリンク上に他のホストやルータを配置しないようにする必要があります。

（注） セキュリティ アプライアンスに直接接続されている Cisco スイッチ ポートの PortFast オプションをイネーブルにします。

ステートフル フェールオーバー リンクとしてフェールオーバー リンクを使用する場合は、使用可能なイーサネット インターフェイスのうち最も高速なインターフェイスを使用する必要があります。このインターフェイスでパフォーマンス上の問題が発生した場合は、別のインターフェイスをステートフル フェールオーバー インターフェイス専用にすることを検討してください。

ステートフル フェールオーバー リンクとしてデータ インターフェイスを使用する場合は、そのインターフェイスをステートフル フェールオーバー リンクとして指定したときに次の警告が表示されます。

```
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
  Sharing Stateful failover interface with regular data interface is not
  a recommended configuration due to performance and security concerns.
******* WARNING ***** WARNING ******* WARNING ****** WARNING  *********
```

データ インターフェイスとステートフル フェールオーバー インターフェイスを共有すると、リプレイ攻撃を受けやすくなる場合があります。さらに、大量のステートフル フェールオーバー トラフィックがインターフェイスで送信され、そのネットワーク セグメントでパフォーマンス上の問題が発生することがあります。

（注） データ インターフェイスは、シングル コンテキストのルーテッド モードでのみステートフル フェールオーバー インターフェイスとして使用できます。

マルチ コンテキスト モードでは、ステートフル フェールオーバー リンクはシステム コンテキストに存在します。このインターフェイスとフェールオーバー インターフェイスが、システム コンテキスト内にある唯一のインターフェイスです。他のインターフェイスは、すべてセキュリティ コンテキストに割り当てられ、セキュリティ コンテキスト内から設定されます。

（注） ステートフル フェールオーバー リンクが通常のデータ インターフェイスに設定されていない限り、ステートフル フェールオーバー リンクの IP アドレスと MAC アドレスは、フェールオーバー時に変更されません。

注意 フェールオーバー リンクおよびステートフル フェールオーバー リンク経由で送信される情報は、フェールオーバー キーを使用して通信をセキュリティで保護しない限り、すべてクリア テキストで送信されます。VPN トンネルの終端にセキュリティ アプライアンスを使用する場合、この情報には、トンネルの確立に使用されたすべてのユーザ名、パスワード、および事前共有キーが含まれて

います。この機密データをクリア テキストで転送することは、非常に大きなセキュリティ リスクになるおそれがあります。セキュリティ アプライアンスを使用して VPN トンネルを終端する場合は、フェールオーバー通信をフェールオーバー キーによってセキュリティで保護することをお勧めします。

例

次に、専用インターフェイスをステートフル フェールオーバー インターフェイスとして指定する例を示します。この例のインターフェイスには、既存のコンフィギュレーションはありません。

```
hostname(config)# failover link stateful_if e4
INFO: Non-failover interface config is cleared on Ethernet4 and its sub-interfaces
```

関連コマンド

コマンド	説明
failover interface ip	**failover** コマンドおよびステートフル フェールオーバー インターフェイスの IP アドレスを設定します。
failover lan interface	フェールオーバー通信に使用するインターフェイスを指定します。

failover mac address

物理インターフェイスのフェールオーバー仮想 MAC アドレスを指定するには、グローバル コンフィギュレーション モードで **failover mac address** コマンドを使用します。仮想 MAC アドレスを削除するには、このコマンドの **no** 形式を使用します。

failover mac address *phy_if active_mac standby_mac*

no failover mac address *phy_if active_mac standby_mac*

構文の説明

phy_if	MAC アドレスを設定するインターフェイスの物理名です。
active_mac	アクティブなセキュリティ アプライアンスの指定したインターフェイスに割り当てられた MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。
standby_mac	スタンバイのセキュリティ アプライアンスの指定したインターフェイスに割り当てられた MAC アドレス。MAC アドレスは h.h.h 形式で入力する必要があります。ここで、h は 16 ビットの 16 進数です。

デフォルト

設定されていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

failover mac address コマンドを使用すると、Active/Standby フェールオーバー ペアの仮想 MAC アドレスを設定できます。仮想 MAC アドレスが定義されていない場合は、各フェールオーバー ユニットが起動したときに、それらのユニットではインターフェイスのバーンドイン MAC アドレスが使用され、それらのアドレスがフェールオーバー ピアと交換されます。プライマリ ユニットのインターフェイスの MAC アドレスが、アクティブ ユニットのインターフェイスに使用されます。

ただし、両方のユニットが同時にオンラインにならず、セカンダリ ユニットが最初に起動してアクティブになった場合、セカンダリ ユニットは、自身のインターフェイスにバーンドイン MAC アドレスを使用します。その後プライマリ ユニットがオンラインになると、セカンダリ ユニットはプライマリ ユニットから MAC アドレスを取得します。この変更によりネットワーク トラフィックが中断される可能性があります。インターフェイスに仮想 MAC アドレスを設定すると、セカンダリ ユニットがプライマリ ユニットよりも前にオンラインになり、アクティブ ユニットとなった場合でも、正しい MAC アドレスが使用されるようになります。

failover lan interface コマンドでは、フェールオーバーが発生した場合に IP アドレスおよび MAC アドレスが変更されないため、LAN ベースのフェールオーバーに設定されたインターフェイスでは、**failover mac address** コマンドは不要であり、使用できません。このコマンドは、セキュリティ アプライアンスが Active/Active フェールオーバーに設定されている場合には効果がありません。

コンフィギュレーションに **failover mac address** コマンドを追加する場合は、仮想 MAC アドレスを設定し、コンフィギュレーションをフラッシュ メモリに保存して、フェールオーバー ペアをリロードすることを推奨します。アクティブな接続が存在するときに仮想 MAC アドレスを追加すると、これらの接続は停止します。また、仮想 MAC アドレス指定を有効にするには、**failover mac address** コマンドを含むコンフィギュレーション全体を、セカンダリセキュリティ アプライアンスのフラッシュ メモリに書き込む必要があります。

failover mac address がプライマリ ユニットのコンフィギュレーションに指定されている場合は、セカンダリ ユニットのブートストラップ コンフィギュレーションにも指定する必要があります。

（注） このコマンドが適用されるのは、Active/Standby フェールオーバーのみです。Active/Active フェールオーバーでは、フェールオーバー グループ コンフィギュレーション モードで **mac address** コマンドを使用して、フェールオーバー グループの各インターフェイスの仮想 MAC アドレスを設定します。

例

次に、intf2 という名前のインターフェイスのアクティブ MAC アドレスおよびスタンバイ MAC アドレスを設定する例を示します。

```
hostname(config)# failover mac address Ethernet0/2 00a0.c969.87c8 00a0.c918.95d8
```

関連コマンド

コマンド	説明
show interface	インターフェイスのステータス、コンフィギュレーション、および統計情報を表示します。

failover polltime

フェールオーバー ユニットのポーリング タイムおよびホールド タイムを指定するには、グローバル コンフィギュレーション モードで **failover polltime** コマンドを使用します。デフォルトのポーリング期間およびホールド タイムに戻すには、このコマンドの **no** 形式を使用します。

failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

no failover polltime [**unit**] [**msec**] *poll_time* [**holdtime** [**msec**] *time*]

構文の説明

holdtime *time*	（任意）ユニットが、フェールオーバー リンクで hello メッセージを受信する間隔を設定します。この時間を経過すると、ピア ユニットで障害が発生したと見なされます。 有効な値は 3 ～ 45 秒です。オプションの **msec** キーワードを使用した場合は、800 ～ 999 ミリ秒です。
msec	（任意）指定する時間がミリ秒単位であることを指定します。
poll_time	hello メッセージ間の時間。 有効な値は 1 ～ 15 秒です。オプションの **msec** キーワードを使用した場合は、200 ～ 999 ミリ秒です。
unit	（任意）コマンドがユニットのポーリング タイムおよびホールド タイムに使用されていることを示します。 このキーワードをコマンドに追加してもコマンドには影響がありませんが、コンフィギュレーションでこのコマンドを **failover polltime interface** コマンドと区別しやすくなります。

デフォルト

PIX セキュリティ アプライアンスのデフォルト値は次のとおりです。

- *poll_time* は 15 秒です。
- **holdtime** *time* は 45 秒です。

ASA セキュリティ アプライアンスのデフォルト値は次のとおりです。

- *poll_time* は 1 秒です。
- **holdtime** *time* は 15 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover poll** コマンドから **failover polltime** コマンドに変更され、**unit** キーワードおよび **holdtime** キーワードが含まれるようになりました。
7.2(1)	**holdtime** キーワードに **msec** キーワードが追加されました。**polltime** の最小値が 500 ミリ秒から 200 ミリ秒に引き下げられました。**holdtime** の最小値が 3 秒から 800 ミリ秒に引き下げられました。

使用上のガイドライン

ユニットのポーリング タイムの 3 倍未満の値を **holdtime** の値として入力することはできません。ポーリング時間が短いほど、セキュリティ アプライアンスは短時間で故障を検出し、フェールオーバーをトリガーできます。ただし、検出が速すぎると、ネットワークが一時的に輻輳したときに不要なスイッチオーバーが発生する可能性があります。

1 回のポーリング期間中にユニットがフェールオーバー通信インターフェイスまたはケーブルで hello パケットを受信しないと、残りのインターフェイス経由で追加のテストが行われます。それでも保持時間内にピア装置から応答がない場合、その装置は故障していると見なされ、故障した装置がアクティブ装置の場合は、スタンバイ装置がアクティブ装置を引き継ぎます。

failover polltime [**unit**] コマンドおよび **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスをパススルーする場合は、セキュリティ アプライアンスのフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次に、ユニットのポーリング タイムの頻度を 3 秒に変更する例を示します。

```
hostname(config)# failover polltime 3
```

次に、200 ミリ秒ごとに hello パケットを送信し、800 ミリ秒以内にフェールオーバー インターフェイスで hello パケットを受信しないとフェールオーバーを実行するようにセキュリティ アプライアンスを設定する例を示します。オプションの **unit** キーワードがコマンドに含まれています。

```
hostname(config)# failover polltime unit msec 200 holdtime msec 800
```

関連コマンド

コマンド	説明
failover polltime interface	Active/Standby フェールオーバー コンフィギュレーションのインターフェイス ポーリング期間およびホールド タイムを指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング タイムおよびホールド タイムを指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover polltime interface

Active/Standby フェールオーバー コンフィギュレーションのデータ インターフェイスのポーリング タイムおよびホールド タイムを指定するには、グローバル コンフィギュレーション モードで **failover polltime interface** コマンドを使用します。デフォルトのポーリング期間およびホールド タイムに戻すには、このコマンドの **no** 形式を使用します。

failover polltime interface [**msec**] *time* [**holdtime** *time*]

no failover polltime interface [**msec**] *time* [**holdtime** *time*]

構文の説明

holdtime *time*	（任意）データ インターフェイスが hello メッセージを受信する間隔を設定します。この時間を経過すると、ピアで障害が発生したと見なされます。有効な値は 5 ～ 75 秒です。
interface *time*	インターフェイス モニタリングのポーリング タイムを指定します。有効な値の範囲は、1 ～ 15 秒です。オプションの **msec** キーワードを使用した場合、有効な値は 500 ～ 999 ミリ秒です。
msec	（任意）指定する時間がミリ秒単位であることを指定します。

デフォルト

デフォルト値は次のとおりです。

- ポーリングの *time* は 5 秒です。
- **holdtime** *time* は、ポーリングの *time* の 5 倍です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが、**failover poll** コマンドから **failover polltime** コマンドに変更され、**unit** キーワード、**interface** キーワード、および **holdtime** キーワードが含まれるようになりました。
7.2(1)	オプションの **holdtime** *time* と、ミリ秒単位でポーリング タイムを指定する機能が追加されました。

使用上のガイドライン

データ インターフェイスで hello パケットが送信される頻度を変更するには、**failover polltime interface** コマンドを使用します。このコマンドは、Active/Standby フェールオーバーにのみ使用可能です。Active/Active フェールオーバーでは、**failover polltime interface** コマンドではなく、フェールオーバー グループ コンフィギュレーション モードで **polltime interface** コマンドを使用します。

ユニットのポーリング タイムの 5 倍未満の値を **holdtime** の値として入力することはできません。ポーリング時間が短いほど、セキュリティ アプライアンスは短時間で故障を検出し、フェールオーバーをトリガーできます。ただし短時間での検出は、ネットワークが一時的に輻輳した場合に不要な切り替えが行われる原因となります。ホールド タイムの半分が経過したときに、インターフェイスで hello パケットが受信されていない場合は、インターフェイスのテストが開始されます。

failover polltime unit コマンドと **failover polltime interface** コマンドの両方をコンフィギュレーションに含めることができます。

（注） CTIQBE トラフィックがフェールオーバー コンフィギュレーションのセキュリティ アプライアンスをパススルーする場合は、セキュリティ アプライアンスのフェールオーバー ホールド タイムを 30 秒未満に減らす必要があります。CTIQBE キープアライブ タイムアウトは 30 秒であるため、フェールオーバーの状況ではフェールオーバーが発生する前にタイムアウトする可能性があります。CTIQBE がタイムアウトした場合、Cisco CallManager への Cisco IP SoftPhone の接続はドロップされ、IP SoftPhone クライアントは CallManager に再登録する必要があります。

例

次に、インターフェイスのポーリング タイムの頻度を 15 秒に設定する例を示します。

```
hostname(config)# failover polltime interface 15
```

次に、インターフェイスのポーリング タイムの頻度を 500 ミリ秒に、ホールド タイムを 5 秒に設定する例を示します。

```
hostname(config)# failover polltime interface msec 500 holdtime 5
```

関連コマンド

コマンド	説明
failover polltime	装置のフェールオーバー ポーリング期間とホールド タイムを指定します。
polltime interface	Active/Active フェールオーバー コンフィギュレーションのインターフェイス ポーリング タイムを指定します。
show failover	フェールオーバー コンフィギュレーションの情報を表示します。

failover reload-standby

スタンバイ ユニットを強制的にリブートするには、特権 EXEC モードで **failover reload-standby** コマンドを使用します。

failover reload-standby

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

フェールオーバー ユニットが同期化されないときにこのコマンドを使用します。スタンバイ ユニットが再起動し、起動終了後にアクティブ ユニットと再同期化されます。

例

次に、アクティブ ユニットで **failover reload-standby** コマンドを使用して、スタンバイ ユニットを強制的にリブートする例を示します。

```
hostname# failover reload-standby
```

関連コマンド

コマンド	説明
write standby	実行コンフィギュレーションをスタンバイ ユニットのメモリに書き込みます。

failover replication http

HTTP（ポート 80）接続のレプリケーションをイネーブルにするには、グローバル コンフィギュレーション モードで **failover replication http** コマンドを使用します。HTTP 接続の複製をディセーブルにするには、このコマンドの **no** 形式を使用します。

failover replication http

no failover replication http

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

ディセーブル

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドが、**failover replicate http** から **failover replication http** に変更されました。

使用上のガイドライン

デフォルトでは、ステートフル フェールオーバーがイネーブルの場合、セキュリティ アプライアンスは HTTP セッション情報を複製しません。HTTP セッションは通常は存続期間が短く、また HTTP クライアントは接続試行が失敗すると通常は再試行するため、HTTP セッションの複製をしないことでシステムのパフォーマンスが向上します。複製をしなくても重要なデータや接続は失われません。**failover replication http** コマンドを使用すると、ステートフル フェールオーバー環境において HTTP セッションのステートフル レプリケーションが可能になりますが、システムのパフォーマンスに悪影響がある可能性があります。

Active/Active フェールオーバー コンフィギュレーションでは、フェールオーバー グループ コンフィギュレーション モードで **replication http** コマンドを使用して、フェールオーバー グループごとに HTTP セッションのレプリケーションを制御します。

例

次に、HTTP 接続のレプリケーションをイネーブルにする例を示します。

```
hostname(config)# failover replication http
```

関連コマンド

コマンド	説明
replication http	特定のフェールオーバー グループに対して、HTTP セッションのレプリケーションをイネーブルにします。
show running-config failover	実行コンフィギュレーションの **failover** コマンドを表示します。

failover reset

障害が発生したセキュリティ アプライアンスを障害が発生していない状態に復元するには、特権 EXEC モードで **failover reset** コマンドを使用します。

failover reset [**group** *group_id*]

構文の説明

group	（任意）フェールオーバー グループを指定します。**group** キーワードは、Active/Active フェールオーバーに対してのみ適用されます。
group_id	フェールオーバー グループの番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、オプションのフェールオーバー グループ ID を許可するように変更されました。

使用上のガイドライン

failover reset コマンドを使用すると、障害が発生したユニットまたはグループを、障害が発生していない状態に変更できます。**failover reset** コマンドはいずれのユニットでも入力できますが、常にアクティブ ユニットでコマンドを入力することを推奨します。アクティブ ユニットで **failover reset** コマンドを入力すると、スタンバイ ユニットが障害が発生していない状態に復元されます。

show failover コマンドまたは **show failover state** コマンドを使用して、ユニットのフェールオーバー ステータスを表示できます。

このコマンドには、**no** 形式はありません。

Active/Active フェールオーバーでは、**failover reset** を入力すると、ユニット全体がリセットされます。コマンドにフェールオーバー グループを指定すると、指定したグループのみがリセットされます。

例

次に、障害が発生したユニットを障害が発生していない状態に変更する例を示します。

```
hostname# failover reset
```

関連コマンド

コマンド	説明
failover interface-policy	モニタリングによってインターフェイスの障害が検出された場合のフェールオーバー ポリシーを指定します。
show failover	装置のフェールオーバー ステータスに関する情報を表示します。

failover timeout

非対称ルーテッド セッションのフェールオーバー再接続タイムアウト値を指定するには、グローバル コンフィギュレーション モードで **failover timeout** コマンドを使用します。デフォルトのタイムアウト値に戻すには、このコマンドの **no** 形式を使用します。

failover timeout *hh*[**:***mm*:[**:***ss*]

no failover timeout [*hh*[**:***mm*:[**:***ss*]]

構文の説明

hh	タイムアウト値の時間を指定します。有効な値の範囲は、-1 ～ 1193 です。デフォルトでは、この値は 0 に設定されています。 この値を -1 に設定すると、タイムアウトがディセーブルになり、任意の時間が経過したあとでも接続を再開できます。 この値を 0 に設定し、他のタイムアウト値を指定しないと、コマンドがデフォルト値に設定されて再接続ができなくなります。**no failover timeout** コマンドを入力しても、この値がデフォルト（0）に設定されます。 **（注）** デフォルト値に設定すると、このコマンドは実行コンフィギュレーションに表示されません。
mm	（任意）タイムアウト値の分を指定します。有効な値の範囲は 0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。
ss	（任意）タイムアウト値の秒を指定します。有効な値の範囲は 0 ～ 59 です。デフォルトでは、この値は 0 に設定されています。

デフォルト

デフォルトで、*hh*、*mm*、および *ss* は 0 であり、再接続はできないようになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、コマンド リストに表示されるように変更されました。

使用上のガイドライン

このコマンドは、**nailed** オプションを指定した **static** コマンドとともに使用されます。**nailed** オプションを指定すると、起動後、またはシステムがアクティブになった後、指定した時間内に接続を再確立できます。**failover timeout** コマンドでは、その時間を指定します。設定しない場合は、接続を再確立できません。**failover timeout** コマンドは、**asr-group** コマンドには影響しません。

（注）　**nailed** オプションを **static** コマンドに追加すると、その接続で TCP ステート トラッキングとシーケンス チェックがスキップされます。

このコマンドの **no** 形式を使用すると、デフォルト値に戻ります。**failover timeout 0** を入力しても、デフォルト値に戻ります。デフォルト値に設定すると、このコマンドは実行コンフィギュレーションに表示されません。

例

次に、スタンバイ グループ 1 をアクティブに切り替える例を示します。

```
hostname(config)# failover timeout 12:30
hostname(config)# show running-config failover
no failover
failover timeout 12:30:00
```

関連コマンド

コマンド	説明
static	ローカル IP アドレスをグローバル IP アドレスにマッピングすることによって、固定の 1 対 1 のアドレス変換ルールを設定します。

file-bookmarks

認証された WebVPN ユーザに表示される WebVPN ホームページの [File Bookmarks] タイトルまたは [File Bookmarks] リンクをカスタマイズするには、webvpn カスタマイゼーション コンフィギュレーション モードで **file-bookmarks** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

no file-bookmarks {**link** {**style** *value*} | **title** {**style** *value* | **text** *value*}}

構文の説明

link	リンクを変更することを指定します。
title	タイトルを変更することを指定します。
style	HTML スタイルを変更することを指定します。
text	テキストを変更することを指定します。
value	実際に表示するテキスト（最大 256 文字）、または CSS パラメータ（最大 256 文字）です。

デフォルト

デフォルトのリンクのスタイルは color:#669999;border-bottom: 1px solid #669999;text-decoration:none です。

デフォルトのタイトルのスタイルは color:#669999;background-color:#99CCCC;font-weight:bold です。

デフォルトのタイトル テキストは「File Folder Bookmarks」です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

style オプションは、任意の有効な CSS パラメータとして表されます。これらのパラメータについては、このマニュアルでは説明しません。CSS パラメータの詳細については、W3C の Web サイト（www.w3.org）の CSS 仕様を参照してください。『CSS 2.1 Specification』の「Appendix F」には、CSS パラメータの使いやすいリストがあります。この付録は www.w3.org/TR/CSS21/propidx.html で入手できます。

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

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。
- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

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

例

次に、[File Bookmarks] タイトルを「Corporate File Bookmarks」にカスタマイズする例を示します。

```
F1-asa1(config)# webvpn
F1-asa1(config-webvpn)# customization cisco
F1-asa1(config-webvpn-custom)# file-bookmarks title text Corporate File Bookmarks
```

関連コマンド

コマンド	説明
application-access	WebVPN ホームページの [Application Access] ボックスをカスタマイズします。
browse-networks	WebVPN ホームページの [Browse Networks] ボックスをカスタマイズします。
web-applications	WebVPN ホームページの [Web Application] ボックスをカスタマイズします。
web-bookmarks	WebVPN ホームページの [Web Bookmarks] タイトルまたはリンクをカスタマイズします。

file-browsing

ファイル サーバまたは共有の CIFS または FTP によるファイル ブラウジングをイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **file-browsing** コマンドを使用します。

file-browsing enable | disable

enable | disable	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

ファイル ブラウジングには、次の使用上の注意事項があります。

- ファイル ブラウジングでは、国際化はサポートされていません。
- ブラウズには、NBNS（マスター ブラウザまたは WINS）が必要です。NBNS に障害が発生した場合や、NBNS が設定されていない場合は、DNS を使用します。

セキュリティ アプライアンスは、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. トンネル グループのグループ ポリシー
5. デフォルトのグループ ポリシー

したがって、属性の DAP 値は、ユーザ、グループ ポリシー、またはトンネル グループに設定されたものよりも優先順位が高くなります。

DAP レコードの属性をイネーブルまたはディセーブルにすると、セキュリティ アプライアンスはその値を適用して実行します。たとえば、DAP webvpn モードでファイル ブラウジングをディセーブルにした場合、セキュリティ アプライアンスはそれ以上値を検索しません。ディセーブルにする代わりに **file-browsing** コマンドで no の値を設定した場合、属性は DAP レコードには存在しないため、セキュ

リティ アプライアンスはユーザ名の AAA 属性に移動し、必要に応じてグループ ポリシーにも移動して、適用する値を検索します。

例

次に、Finance という DAP レコードでファイル ブラウジングをイネーブルにする例を示します。

```
hostname (config)# config-dynamic-access-policy-record Finance
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# file-browsing enable
hostname(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-entry	アクセス先のファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。

file-encoding

Common Internet File System サーバからのページの文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **file-encoding** コマンドを使用します。file-encoding 属性の値を削除するには、このコマンドの **no** 形式を使用します。

file-encoding {server-name | server-ip-addr} *charset*

no file-encoding {server-name | server-ip-addr}

構文の説明

charset	最大 40 文字から成るストリングで、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 このストリングは、大文字と小文字が区別されません。セキュリティ アプライアンス コンフィギュレーション内では、コマンド インタプリタによって大文字が小文字に変換されます。
server-ip-addr	文字エンコーディングを指定する CIFS サーバの IP アドレス（ドット付き 10 進表記）。
server-name	文字エンコーディングを指定する CIFS サーバの名前。 セキュリティ アプライアンスでは、指定した大文字と小文字の区別が保持されますが、名前をサーバと照合するときには大文字と小文字は区別されません。

デフォルト

WebVPN コンフィギュレーションに明示的な file-encoding エントリがないすべての CIFS サーバからのページでは、character-encoding 属性の文字エンコーディング値が継承されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

WebVPN の character-encoding 属性の値とは異なる文字エンコーディングが必要なすべての CIFS サーバに対して、file-encoding エントリを入力します。

CIFS サーバから WebVPN ユーザにダウンロードされた WebVPN ポータル ページは、サーバを識別する WebVPN file-encoding 属性の値を符号化します。符号化が行われなかった場合は、character-encoding 属性の値を継承します。リモート ユーザのブラウザでは、ブラウザの文字エンコード セットのエントリにこの値がマップされ、使用する適切な文字セットが決定されます。WebVPN コンフィギュレーションで CIFS サーバ用の file-encoding エントリが指定されず、character-encoding 属性も設定されていない場合、WebVPN ポータル ページは値を指定しません。WebVPN ポータル ページが文字エンコーディングを指定しない場合、またはブラウザがサポートしていない文字エンコーディング値を指定した場合、リモート ブラウザはブラウザ自体のデフォルト エンコーディングを使用します。

CIFS サーバに適切な文字エンコーディングを、広域的には webvpn character-encoding 属性によって、個別的には file-encoding の上書きによってマッピングすることで、ページと同様にファイル名やディレクトリ パスを適切にレンダリングすることが必要な場合には、CIFS ページの正確な処理と表示が可能になります。

（注） character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。次の例に示すように日本語の Shift_JIS 文字エンコーディングを使用する場合などは、webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用してフォント ファミリを置換し、これらの値の設定を補足するか、または webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力してフォント ファミリを削除する必要があります。

例

次に、「CISCO-server-jp」という名前の CIFS サーバが日本語の Shift_JIS 文字をサポートするように file-encoding 属性を設定し、フォント ファミリを削除して、デフォルトの背景色を保持する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding CISCO-server-jp shift_jis
F1-asa1(config-webvpn)# customization DfltCustomization
F1-asa1(config-webvpn-custom)# page style background-color:white
F1-asa1(config-webvpn-custom)#
```

次に、CIFS サーバ 10.86.5.174 の file-encoding 属性を設定して、IBM860（エイリアス「CP860」）文字をサポートする例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# file-encoding 10.86.5.174 cp860
hostname(config-webvpn)
```

関連コマンド

コマンド	説明
character-encoding	WebVPN コンフィギュレーションの file-encoding エントリに指定されたサーバのページを除き、すべての WebVPN ポータル ページで使用されるグローバルな文字エンコーディングを指定します。
show running-config [all] webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルト コンフィギュレーションを組み込むには **all** キーワードを使用します。
debug webvpn cifs	Common Internet File System についてのデバッグ メッセージを表示します。

file-entry

アクセスするファイル サーバ名をユーザが入力できる機能をイネーブルまたはディセーブルにするには、DAP webvpn コンフィギュレーション モードで **file-entry** コマンドを使用します。

file-entry enable | disable

enable | disable	アクセス先のファイル サーバの名前を入力する機能をイネーブルまたはディセーブルにします。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、さまざまなソースからの属性値を適用できます。次の階層に従って、属性値を適用します。

1. DAP レコード
2. ユーザ名
3. グループ ポリシー
4. 接続プロファイル（トンネル グループ）のグループ ポリシー
5. デフォルトのグループ ポリシー

属性の DAP 値には、ユーザ、グループ ポリシー、または接続プロファイルよりも高いプライオリティが設定されています。

DAP レコードの属性をイネーブルまたはディセーブルにすると、セキュリティ アプライアンスはその値を適用して実行します。たとえば、DAP webvpn モードでファイル サーバ名の入力をディセーブルにした場合、セキュリティ アプライアンスはそれ以上値を検索しません。ディセーブルにする代わりに **file-entry** コマンドで no の値を設定した場合、属性は DAP レコードには存在しないため、セキュリティ アプライアンスはユーザ名の AAA 属性に移動し、必要に応じてグループ ポリシーにも移動して、適用する値を検索します。

例

次に、Finance という DAP レコードでファイル サーバ名の入力をイネーブルにする例を示します。

```
hostname (config)# config-dynamic-access-policy-record Finance
```

```
hostname(config-dynamic-access-policy-record)# webvpn
hostname(config-dap-webvpn)# file-entry enable
hostname(config-dap-webvpn)#
```

関連コマンド

コマンド	説明
dynamic-access-policy-record	DAP レコードを作成します。
file-browsing	ファイル サーバまたは共有のブラウズ機能をイネーブルまたはディセーブルにします。

filter

特定のグループ ポリシーまたはユーザ名の WebVPN 接続で使用するアクセス リストの名前を指定するには、webvpn コンフィギュレーション モードで **filter** コマンドを使用します。アクセス リスト（**filter none** コマンドを発行して作成されたヌル値を含む）を削除するには、このコマンドの **no** 形式を使用します。

filter {**value** *ACLname* | **none**}

no filter

構文の説明

none	**WebVPN タイプ**のアクセス リストがないことを示します。ヌル値を設定して、アクセス リストを使用できないようにします。アクセス リストを他のグループ ポリシーから継承しないようにします。
value *ACLname*	事前に設定済みのアクセス リストの名前を指定します。

デフォルト

WebVPN アクセス リストは、**filter** コマンドを使用してアクセス リストを指定するまでは適用されません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

no オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。フィルタ値を継承しないようにするには、**filter value none** コマンドを使用します。

このユーザまたはグループ ポリシーに対する、さまざまなタイプのトラフィックを許可または拒否するには、ACL を設定します。その後、**filter** コマンドを使用して、これらの WebVPN トラフィック用の ACL を適用します。

WebVPN では、**vpn-filter** コマンドで定義された ACL は使用されません。

例

次に、FirstGroup という名前のグループ ポリシーで *acl_in* という名前のアクセス リストを呼び出すフィルタを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# filter acl_in
```

関連コマンド

コマンド	説明
access-list	アクセス リストを作成するか、ダウンロード可能なアクセス リストを使用します。
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。

filter activex

セキュリティ アプライアンスを通過する HTTP トラフィック内の ActiveX オブジェクトを削除するには、グローバル コンフィギュレーション モードで **filter activex** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter activex | java **<***port***>** [**-**<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

no filter activex | java **<***port***>** [**-**<*port*>] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*>

構文の説明

port	フィルタリングが適用される TCP ポート。一般的に、これはポート 21 ですが、他の値も受け入れられます。ポート 21 の代わりに、**http** または **url** リテラルを使用できます。指定できる値の範囲は、0 ～ 65535 です。well-known ポートおよびそれらのリテラル値のリストについては、を参照してください。
-port	（任意）ポート範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

ActiveX オブジェクトには、保護されているネットワーク上のホストやサーバを攻撃することを目的とするコードが含まれている場合があるため、セキュリティのリスクが発生する可能性があります。**filter activex** コマンドを使用して、ActiveX オブジェクトをディセーブルにできます。

ActiveX コントロールは、以前は OLE コントロールまたは OCX コントロールと呼ばれていたもので、Web ページやその他のアプリケーションに挿入できるコンポーネントです。これらのコントロールにはカスタム フォームやカレンダーなど、情報の収集と表示に使用されるサードパーティ製の多様なフォームが含まれています。ActiveX は、技術的に、ネットワーク クライアントに対して多くの問題を発生させる可能性があります。たとえば、ワークステーションの障害の原因となる、ネットワーク セキュリティ問題を引き起こす、またはサーバへの攻撃に利用される、などのおそれがあります。

filter activex コマンドでは、HTML Web ページ内で HTML の <object> コマンドをコメントアウトすることによって、<object> コマンドがブロックされます。<APPLET> ～ </APPLET> タグおよび <OBJECT CLASSID> ～ </OBJECT> タグを選択的にコメントに置換することによって、HTML ファイルの ActiveX フィルタリングが実行されます。ネストされたタグのフィルタリングは、最上位タグをコメントに変換することによってサポートされています。

注意　<object> タグは、Java アプレット、画像ファイル、およびマルチメディア オブジェクトにも使用されます。この場合、これらもこのコマンドによってブロックされます。

<object> または </object> HTML タグが複数のネットワーク パケットに分割されている場合や、タグ内のコードが MTU のバイト数よりも長い場合は、セキュリティ アプライアンスでタグをブロックできません。

alias コマンドによって参照されている IP アドレスにユーザがアクセスした場合、または WebVPN トラフィックでは、ActiveX ブロッキングは行われません。

例

次に、すべての発信接続で ActiveX オブジェクトをブロックする例を示します。

```
hostname(config)# filter activex 80 0 0 0 0
```

このコマンドは、任意のローカル ホストから任意の外部ホストへの接続において、ポート 80 で Web トラフィックに対して ActiveX オブジェクト ブロッキングを適用することを指定します。

関連コマンド

コマンド	説明
filter url	トラフィックを URL フィルタリング サーバに送ります。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter ftp

Websense サーバまたは N2H2 サーバでフィルタリングする FTP トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter ftp** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter ftp <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

no filter ftp <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**interact-block**]

構文の説明

port	フィルタリングが適用される TCP ポート。一般的に、これはポート 21 ですが、他の値も受け入れられます。ポート 80 の代わりに、**ftp** リテラルを使用できます。
-*port*	（任意）ポート範囲を指定します。
except	先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
allow	（任意）サーバが利用できない場合に、フィルタリングなしで発信接続がセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、発信ポート 80（Web）トラフィックを停止します。
interact-block	（任意）ユーザが対話形式の FTP プログラムを使用して FTP サーバに接続することを禁止します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

filter ftp コマンドを使用すると、Websense サーバまたは N2H2 サーバでフィルタリングする FTP トラフィックを指定できます。

この機能をイネーブルにした後、ユーザがサーバに対して FTP GET 要求を発行すると、セキュリティ アプライアンスは、FTP サーバ、および Websense サーバまたは N2H2 サーバに対して同時に要求を送信します。Websense サーバまたは N2H2 サーバによって接続が許可されると、セキュリティ アプライアンスは成功の FTP リターン コードを変更しないでそのままユーザに返します。たとえば、成功のリターン コードは「250: CWD command successful」です。

Websense サーバまたは N2H2 サーバによって接続が拒否されると、セキュリティ アプライアンスは FTP リターン コードを変更して、接続が拒否されたことを示します。たとえば、セキュリティ アプライアンスは、コード 250 を「550 Requested file is prohibited by URL filtering policy」に変更します。Websense では、FTP GET コマンドのみがフィルタリングされ、FTP PUT コマンドはフィルタリングされません。

完全なディレクトリ パスを指定しない対話形式の FTP セッションを禁止するには、**interactive-block** オプションを使用します。対話形式の FTP クライアントを使用すると、ユーザは、完全なパスを入力しないでディレクトリを変更できます。たとえば、ユーザは、**cd /public/files** ではなく、**cd ./files** と入力できます。これらのコマンドを使用する前に、URL フィルタリング サーバを指定してイネーブルにする必要があります。

例

次に、FTP フィルタリングをイネーブルにする例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter ftp 21 0 0 0 0
hostname(config)# filter ftp except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter https	Websense サーバまたは N2H2 サーバによってフィルタリングされる HTTPS トラフィックを指定します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter https

N2H2 サーバまたは Websense サーバでフィルタリングする HTTPS トラフィックを指定するには、グローバル コンフィギュレーション モードで **filter https** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter https <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

no filter https <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**]

構文の説明

port	フィルタリングが適用される TCP ポート。一般的に、これはポート 443 ですが、他の値でも受け入れられます。ポート 443 の代わりに、**https** リテラルを使用できます。
-port	（任意）ポート範囲を指定します。
except	（任意）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
allow	（任意）サーバが利用できない場合に、フィルタリングなしで発信接続がセキュリティ アプライアンスを通過します。このオプションを省略した場合に、N2H2 サーバまたは Websense サーバがオフラインになると、セキュリティ アプライアンスは、N2H2 サーバまたは Websense サーバが再度オンラインになるまで、ポート 443 への発信トラフィックを停止します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

セキュリティ アプライアンスは、外部の Websense または N2H2 フィルタリング サーバを使用した HTTPS サイトおよび FTP サイトのフィルタリングをサポートしています。

サイトが許可されない場合、SSL 接続ネゴシエーションを完了させないことによって、HTTPS フィルタリングが行われます。ブラウザには、「The Page or the content cannot be displayed.」のようなエラーメッセージが表示されます。

HTTPS コンテンツは暗号化されているため、セキュリティ アプライアンスは、ディレクトリおよびファイル名の情報を付けずに URL ルックアップを送信します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTPS 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter https 443 0 0 0 0
hostname(config)# filter https except 10.0.2.54 255.255.255.255 0 0
```

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter java

セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除するには、グローバル コンフィギュレーション モードで **filter java** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

no filter java {[*port*[**-***port*] | **except** } *local_ip local_mask foreign_ip foreign_mask*]

構文の説明

port	フィルタリングが適用される TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には **http** または **url** リテラルを使用できます。
*port***-***port*	（任意）ポート範囲を指定します。
except	（任意）先行の **filter** 条件に対する例外を作成します。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

Java アプレットは、保護されたネットワーク上のホストとサーバを攻撃するコードを含むことがあるため、セキュリティ リスクを引き起こす可能性があります。Java アプレットは、**filter java** コマンドで取り除くことができます。

filter java コマンドは、発信接続からセキュリティ アプライアンスに返される Java アプレットをフィルタリングします。フィルタリングされてもユーザは HTML ページを受信できますが、アプレットの Web ページ ソースはコメントアウトされているため、アプレットは実行できません。**filter java** コマンドでは、WebVPN トラフィックはフィルタリングされません。

applet または /applet HTML タグが複数のネットワーク パケットに分割されている場合や、タグ内のコードが MTU のバイト数よりも長い場合は、セキュリティ アプライアンスでタグをブロックできません。Java アプレットが <object> タグ内にあることがわかっている場合は、**filter activex** コマンドを使用して削除します。

例

次の例では、すべての発信接続で Java アプレットをブロックすることを指定しています。

```
hostname(config)# filter java 80 0 0 0 0
```

このコマンドは、Java アプレット ブロックが、あらゆるローカル ホストからあらゆる外部ホストへのポート 80 の Web トラフィックに対して、適用されることを指定しています。

次の例では、保護されたネットワーク上のホストへの Java アプレットのダウンロードをブロックしています。

```
hostname(config)# filter java http 192.168.3.3 255.255.255.255 0 0
```

このコマンドは、ホスト 192.168.3.3 による Java アプレットのダウンロードをブロックします。

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter url	トラフィックを URL フィルタリング サーバに送ります。
show running-config filter	フィルタリング コンフィギュレーションを表示します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

filter url

トラフィックを URL フィルタリング サーバに転送するには、グローバル コンフィギュレーション モードで **filter url** コマンドを使用します。設定を削除するには、このコマンドの **no** 形式を使用します。

filter url <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

no filter url <*port***>** [**-<***port***>**] | **except** <*local_ip*> <*mask*> <*foreign_ip*> <*foreign_mask*> [**allow**] [**cgi-truncate**] [**longurl-truncate** | **longurl-deny**] [**proxy-block**]

構文の説明

allow	サーバが利用できない場合、発信接続はフィルタリングなしでセキュリティ アプライアンスを通過します。このオプションを省略した場合、および N2H2 サーバまたは Websense サーバがオフラインの場合、セキュリティ アプライアンスは、N2H2 サーバまたは Websense サーバがオンラインに戻るまで、発信ポート 80（Web）トラフィックを停止します。
cgi_truncate	CGI スクリプトのように、URL に疑問符（?）から始まるパラメータ リストがある場合は、フィルタリング サーバに送信する URL から、疑問符を含む疑問符以降のすべての文字を削除します。
except	先行の **filter** 条件に対する例外を作成します。
foreign_ip	セキュリティ レベルが最も低い、アクセスが要求されているインターフェイスの IP アドレス。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
foreign_mask	*foreign_ip* のネットワーク マスク。常に特定のマスク値を指定します。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
http	ポート 80 を指定します。80 の代わりに **http** または **www** と入力してポート 80 を指定することもできます。
local_ip	セキュリティ レベルが最も高い、アクセスが要求されているインターフェイスの IP アドレス。このアドレスに **0.0.0.0**（短縮形は **0**）を設定すると、すべてのホストを指定できます。
local_mask	*local_ip* のネットワーク マスク。**0.0.0.0**（短縮形は **0**）を使用すると、すべてのホストを指定できます。
longurl-deny	URL が URL バッファ サイズの制限を超える場合や、URL バッファが使用できない場合に URL 要求を拒否します。
longurl-truncate	URL が URL バッファの制限を超える場合は、N2H2 サーバまたは Websense サーバに対して元のホスト名または IP アドレスのみを送信します。
mask	任意のマスク。
-port	（任意）フィルタリングの適用対象となる TCP ポート。一般的に、これはポート 80 ですが、他の値でも受け入れられます。ポート 80 には **http** または **url** リテラルを使用できます。ハイフンの後にもう 1 つポートを追加すると、ポートの範囲を指定できます。
proxy-block	ユーザの HTTP プロキシ サーバへの接続を禁止します。
url	セキュリティ アプライアンス経由で伝送されるデータから URL をフィルタリングします。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン　**filter url** コマンドを使用すると、N2H2 または Websense フィルタリング アプリケーションを使用して指定した WWW 上の URL への発信ユーザのアクセスを禁止できます。

（注）　**filter url** コマンドを発行する前に、**url-server** コマンドを設定する必要があります。

filter url コマンドの **allow** オプションでは、N2H2 サーバまたは Websense サーバがオフラインになった場合のセキュリティ アプライアンスの動作が決定されます。**filter url** コマンドで **allow** オプションを使用し、N2H2 サーバまたは Websense サーバがオフラインになった場合、ポート 80 のトラフィックはフィルタリングなしでセキュリティ アプライアンスを通過します。**allow** オプションを指定しないでこのコマンドを使用し、サーバがオフラインになった場合、セキュリティ アプライアンスでは、サーバが再度オンラインになるまでポート 80（Web）への発信トラフィックが停止されるか、または別の URL サーバを使用できる場合は次の URL サーバに制御が渡されます。

（注）　**allow** オプションを設定した場合、セキュリティ アプライアンスでは、N2H2 サーバまたは Websense サーバがオフラインになると代替サーバに制御が渡されるようになりました。

N2H2 サーバまたは Websense サーバは、セキュリティ アプライアンスと連携して動作し、会社のセキュリティ ポリシーに基づいてユーザの Web サイトへのアクセスを拒否します。

フィルタリング サーバの使用方法

Websense プロトコル バージョン 4 では、ホストとセキュリティ アプライアンスとの間でのグループおよびユーザ名認証が可能です。セキュリティ アプライアンスは、ユーザ名ルックアップを実行し、その後 Websense サーバが URL フィルタリングおよびユーザ名のロギングを処理します。

N2H2 サーバは、IFP サーバを実行する Windows ワークステーション（2000、NT、または XP）である必要があります。512 MB 以上の RAM を推奨します。また、N2H2 サービスにおける長い URL のサポートは最大 3 KB までとなっており、Websense における制限よりも短くなっています。

Websense プロトコル バージョン 4 では、次の機能が拡張されました。

- URL フィルタリングにおいて、セキュリティ アプライアンスでは、Websense サーバに定義されているポリシーに対して発信 URL 要求をチェックできます。
- ユーザ名のロギングによって、Websense サーバでユーザ名、グループ、およびドメイン名が追跡されます。

- ユーザ名ルックアップによって、セキュリティ アプライアンスでは、ユーザ認証テーブルを使用して、ホストの IP アドレスをユーザ名にマッピングできます。

Websense についての情報は、次の Web サイトで入手できます。

http://www.websense.com/

設定手順

次の手順を実行して、URL フィルタリングを行います。

ステップ 1　ベンダー固有の適切な形式の **url-server** コマンドを使用して、N2H2 サーバまたは Websense サーバを指定します。

ステップ 2　**filter** コマンドを使用して、フィルタリングをイネーブルにします。

ステップ 3　必要に応じて **url-cache** コマンドを使用して、スループットを向上させます。ただし、このコマンドは Websense ログを更新しないため、Websense アカウンティング レポートに影響がある可能性があります。**url-cache** コマンドを使用する前に、Websense の実行ログを蓄積します。

ステップ 4　**show url-cache statistics** コマンドおよび **show perfmon** コマンドを使用して、実行情報を表示します。

長い URL の使用

Websense フィルタリング サーバでは 4 KB まで､N2H2 フィルタリング サーバでは 3 KB までの URL のフィルタリングがサポートされています。

許可されている最大サイズよりも長い URL 要求の処理を許可するには、**longurl-truncate** オプションおよび **cgi-truncate** オプションを使用します。

URL が最大長よりも長く、**longurl-truncate** オプションまたは **longurl-deny** オプションをイネーブルにしない場合、セキュリティ アプライアンスではパケットがドロップされます。

longurl-truncate オプションを指定すると、セキュリティ アプライアンスは URL が最大許容長よりも長い場合に、URL のホスト名または IP アドレス部分だけを、評価のためにフィルタリング サーバに送信します。**longurl-deny** オプションは、URL が最大許容長よりも長い場合、発信 URL トラフィックを拒否します。

パラメータは含まずに CGI スクリプトの場所とスクリプト名だけを含むよう CGI URL を切り捨てるには、**cgi-truncate** オプションを使用します。長い HTTP 要求のほとんどは、CGI 要求です。パラメータ リストが非常に長い場合、パラメータ リストを含む完全な CGI 要求を待機したり送信したりすると、大量のメモリ リソースが使用され、セキュリティ アプライアンスのパフォーマンスに影響を与える可能性があります。

HTTP 応答のバッファリング

デフォルトで、ユーザが特定の Web サイトに対する接続要求を発行すると、セキュリティ アプライアンスはその要求を Web サーバとフィルタリング サーバに同時に送信します。Web コンテンツ サーバよりも前にフィルタリング サーバが応答しない場合、Web サーバからの応答はドロップされます。このような場合、Web クライアントの観点からは、Web サーバの応答が遅延することになります。

HTTP 応答バッファをイネーブルにすることによって、Web コンテンツ サーバからの応答がバッファリングされ、フィルタリング サーバによって接続が許可された場合にその応答が要求元ユーザに転送されます。これにより、応答バッファをイネーブルにしない場合に発生する遅延を防止できます。

HTTP 応答バッファをイネーブルにするには、次のコマンドを入力します。

```
url-block block block-buffer-limit
```

block-buffer を、バッファリングする最大ブロック数で置き換えます。1 ～ 128 の値を指定できます。この値は、一度にバッファリング可能な 1550 バイトのブロック数を指定します。

例

次に、10.0.2.54 ホストからの接続を除く、すべての発信 HTTP 接続をフィルタリングする例を示します。

```
hostname(config)# url-server (perimeter) host 10.0.1.1
hostname(config)# filter url 80 0 0 0 0
hostname(config)# filter url except 10.0.2.54 255.255.255.255 0 0
```

次に、ポート 8080 でリッスンするプロキシ サーバ宛てのすべての発信 HTTP 接続をブロックする例を示します。

```
hostname(config)# filter url 8080 0 0 0 0 proxy-block
```

関連コマンド

コマンド	説明
filter activex	セキュリティ アプライアンスを通過する HTTP トラフィックから ActiveX オブジェクトを削除します。
filter java	セキュリティ アプライアンスを通過する HTTP トラフィックから Java アプレットを削除します。
url-block	フィルタリング サーバからのフィルタリング決定を待っている間、Web サーバの応答に使用される URL バッファを管理します。
url-cache	N2H2 サーバまたは Websense サーバからの応答を保留している間の URL キャッシングをイネーブルにし、キャッシュのサイズを設定します。
url-server	**filter** コマンドで使用する N2H2 サーバまたは Websense サーバを指定します。

fips enable

FIPS に準拠するためのポリシー チェックをイネーブルにするには、グローバル コンフィギュレーション モードで **fips enable** コマンドを使用します。ポリシー チェックをディセーブルにするには、このコマンドの **no** 形式を使用します。

fips enable

no fips enable

構文の説明

enable	FIPS に準拠するためのポリシー チェックをイネーブルまたはディセーブルにします。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

FIPS 準拠動作モードで実行するには、**fips enable** コマンドを適用し、セキュリティ ポリシーに指定されている適切なコンフィギュレーションを適用する必要があります。内部 API によって、実行時に、適切なコンフィギュレーションが適用されるようにデバイスを移行できます。

スタートアップ コンフィギュレーションに「fips enable」が存在する場合は、FIPS POST が実行されて、次のコンソール メッセージが表示されます。

```
Copyright (c) 1996-2005 by Cisco Systems, Inc.
Restricted Rights Legend

Use, duplication, or disclosure by the Government is subject to restrictions as set forth
in subparagraph (c) of the Commercial Computer Software - Restricted Rights clause at FAR
sec. 52.227-19 and subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer
Software clause at DFARS sec. 252.227-7013.

               Cisco Systems, Inc.
               170 West Tasman Drive
               San Jose, California 95134-1706

....
Cryptochecksum (unchanged): 6c6d2f77 ef13898e 682c9f94 9c2d5ba9
```

```
INFO: FIPS Power-On Self-Test in process.  Estimated completion in 90 seconds.
.................................................
INFO: FIPS Power-On Self-Test complete.
Type help or '?' for a list of available commands.
sw8-5520>
```

例

次に、FIPS に準拠するためのポリシー チェックをシステムでイネーブルにする例を示します。

```
sw8-ASA(config)# fips enable
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips self-test poweron	電源投入時自己診断テストを実行します。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

fips self-test poweron

電源オン セルフテストを実行するには、特権 EXEC モードで **fips self-test powereon** コマンドを使用します。

fips self-test poweron

構文の説明

poweron	電源オン セルフテストを実行します。

デフォルト

このコマンドには、デフォルト設定がありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが導入されました。

使用上のガイドライン

このコマンドを実行すると、デバイスで、FIPS 140-2 準拠に必要なすべてのセルフテストが実行されます。テストには、暗号化アルゴリズム テスト、ソフトウェア完全性テスト、および重要機能のテストがあります。

例

次に、システムで電源オン セルフテストを実行する例を示します。

```
sw8-5520(config)# fips self-test poweron
```

関連コマンド

コマンド	説明
clear configure fips	NVRAM に保存されているシステムまたはモジュールの FIPS コンフィギュレーション情報をクリアします。
crashinfo console disable	フラッシュに対するクラッシュ書き込み情報の読み取り、書き込み、およびコンフィギュレーションをディセーブルにします。
fips enable	システムまたはモジュールで FIPS 準拠を強制するためのポリシー チェックをイネーブルまたはディセーブルにします。
show crashinfo console	フラッシュに対するクラッシュ書き込みの読み取り、書き込み、および設定を行います。
show running-config fips	セキュリティ アプライアンスで実行されている FIPS コンフィギュレーションを表示します。

firewall transparent

ファイアウォール モードをトランスペアレント モードに設定するには、グローバル コンフィギュレーション モードで **firewall transparent** コマンドを使用します。ルーテッド モードに戻すには、このコマンドの **no** 形式を使用します。トランスペアレント ファイアウォールは、「Bump In The Wire」または「ステルス ファイアウォール」のように動作するレイヤ 2 のファイアウォールであり、接続デバイスにはルータ ホップとして認識されません。

firewall transparent

no firewall transparent

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

マルチ コンテキスト モードでは、すべてのコンテキストに対して 1 つのファイアウォール モードのみを使用できます。モードは、システム コンフィギュレーションで設定する必要があります。このコマンドは、各コンテキストのコンフィギュレーションにも情報提供の目的で表示されますが、このコマンドをコンテキストで入力することはできません。

多くのコマンドは両方のモードではサポートされていないため、モードを変更した場合は、セキュリティ アプライアンスによってコンフィギュレーションがクリアされます。設定済みのコンフィギュレーションがある場合は、モードを変更する前にコンフィギュレーションをバックアップしてください。新しいコンフィギュレーション作成時の参照としてこのバックアップを使用できます。

firewall transparent コマンドを使用してモードを変更するテキスト コンフィギュレーションをセキュリティ アプライアンスにダウンロードする場合は、このコマンドをコンフィギュレーションの先頭に配置します。先頭に配置することによって、セキュリティ アプライアンスでこのコマンドが読み込まれるとすぐにモードが変更され、その後引き続きダウンロードされたコンフィギュレーションが読み込まれます。コマンドをコンフィギュレーションの後の方に配置すると、コンフィギュレーション内のその位置よりも前にあるすべての行がセキュリティ アプライアンスによってクリアされます。

例

次に、ファイアウォール モードをトランスペアレントに変更する例を示します。

```
hostname(config)# firewall transparent
```

関連コマンド

コマンド	説明
arp-inspection	ARP パケットとスタティック ARP エントリを比較する ARP インスペクションをイネーブルにします。
mac-address-table static	MAC アドレス テーブルにスタティック MAC アドレス エントリを追加します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show firewall	ファイアウォール モードを表示します。
show mac-address-table	ダイナミック エントリおよびスタティック エントリを含む MAC アドレス テーブルを表示します。

flowcontrol

フロー制御のポーズ（XOFF）フレームを 10 ギガビット イーサネット インターフェイスでのみイネーブルにするには、インターフェイス コンフィギュレーション モードで **flowcontrol** コマンドを使用します。ポーズ フレームをディセーブルにするには、このコマンドの **no** 形式を使用します。

flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

no flowcontrol send on [*low_water high_water pause_time*] [**noconfirm**]

構文の説明

low_water	低基準値を 0 ～ 511 KB の範囲で設定します。Network Interface Controller（NIC; ネットワーク インターフェイス コントローラ）からポーズ フレームが送信された後、バッファの使用量が低基準値を下回ると、NIC から XON フレームが送信されます。リンク パートナーは、XON フレームを受信するとトラフィックを再開できます。デフォルトは、64 KB です。
pause_time	ポーズ リフレッシュのしきい値を 0 ～ 65535 の範囲で設定します。リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のこのタイマー値によって制御されます。バッファの使用量が継続的に高基準値を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが繰り返し送信されます。デフォルトは 26624 です。
noconfirm	確認なしでコマンドを適用します。このコマンドでは、インターフェイスがリセットされるため、このオプションを指定しない場合は、コンフィギュレーションの変更の確認を求められます。
high_water	高基準値を 0 ～ 511 KB の範囲で設定します。バッファの使用量が高基準値を超えると、NIC からポーズ フレームが送信されます。デフォルトは 128 KB です。

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

ポーズ フレームは、デフォルトではディセーブルになっています。

デフォルトの最高水準点は 128 KB です。

デフォルトの最低水準点は 64 KB です。

デフォルトのポーズ リフレッシュのしきい値は 26664 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、物理インターフェイスに対して入力します。

トラフィック バーストが発生している場合、バーストが NIC の FIFO バッファまたは受信リング バッファのバッファリング容量を超えると、パケットがドロップされる可能性があります。フロー制御用のポーズ フレームをイネーブルにすると、このような問題の発生を抑制できます。

このコマンドをイネーブルにすると、FIFO バッファの使用量に基づいて、NIC ハードウェアによってポーズ（XOFF）フレームおよび XON フレームが自動的に生成されます。

1. バッファの使用量が高基準値を超えると、NIC からポーズ フレームが送信されます。
2. ポーズが送信された後、バッファの使用量が低基準値を下回ると、NIC から XON フレームが送信されます。
3. リンク パートナーは、XON を受信した後、または XOFF の期限が切れた後、トラフィックを再開できます。XOFF の期限は、ポーズ フレーム内のタイマー値によって制御されます。
4. バッファの使用量が継続的に高基準値を超えている場合は、ポーズ リフレッシュのしきい値に指定された間隔でポーズ フレームが NIC から繰り返し送信されます。

このコマンドを使用すると、次の警告が表示されます。

```
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
```

プロンプトを表示しないでパラメータを変更するには、**noconfirm** キーワードを使用します。

（注） 802.3x に定義されているフロー制御フレームのみがサポートされています。プライオリティ ベースのフロー制御はサポートされていません。

例

次に、デフォルト設定を使用してポーズ フレームをイネーブルにする例を示します。

```
hostname(config)# interface tengigabitethernet 1/0
hostname(config-if)# flowcontrol send on
Changing flow-control parameters will reset the interface. Packets may be lost during the
reset.
Proceed with flow-control changes?
hostname(config-if)# y
```

関連コマンド

コマンド	説明
interface	インターフェイス コンフィギュレーション モードを開始します。

format

すべてのファイルを消去してファイル システムをフォーマットするには、特権 EXEC モードで **format** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去して、ファイル システムを再インストールします。

format {**disk0: | disk1: | flash:**}

構文の説明

disk0:	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

format コマンドは、指定したファイル システム上のすべてのデータを消去して、デバイスに FAT 情報を再書き込みします。

注意　**format** コマンドは、破損したフラッシュ メモリをクリーン アップするために必要な場合にのみ、細心の注意を払って使用してください。

（非表示のシステム ファイルを除く）表示されているすべてのファイルを削除する場合は、**format** コマンドではなく **delete /recursive** コマンドを入力します。

（注）　Cisco PIX セキュリティ アプライアンスでは、**erase** コマンドおよび **format** コマンドは両方とも、0xFF パターンを使用してユーザ データを破棄します。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** を入力します。

（注）　Cisco ASA 5500 シリーズのセキュリティ アプライアンスでは、**erase** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、**format** コマンドはファイル システムの制御構造をリセットするだけです。ロウ ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

破損したファイル システムを修復する場合は、**format** コマンドを入力する前に **fsck** を入力します。

例

次に、フラッシュ メモリをフォーマットする方法の例を示します。

```
hostname# format flash:
```

関連コマンド

コマンド	説明
delete	ユーザに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
fsck	破損したファイル システムを修復します。

forward interface

ASA 5505 適応型セキュリティ アプライアンスなどの組み込みのスイッチを備えたモデルにおいて、特定の VLAN で他の特定の VLAN への接続の開始を可能にするには、インターフェイス コンフィギュレーション モードで **forward interface** コマンドを使用します。特定の VLAN で他の特定の VLAN への接続が開始されないよう制限するには、このコマンドの **no** 形式を使用します。ライセンスでサポートされている VLAN 数に応じて、特定の VLAN の制限が必要となることがあります。

forward interface vlan *number*

no forward interface vlan *number*

構文の説明

vlan *number*	この VLAN インターフェイスでトラフィックの開始を禁止する先の VLAN ID を指定します。

デフォルト

デフォルトでは、すべてのインターフェイスから他のすべてのインターフェイスにトラフィックを開始できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

ルーテッド モードでは、ASA 5505 適応型セキュリティ アプライアンスの基本ライセンスで最大 3 つのアクティブ VLAN と Security Plus ライセンスで最大 5 つのアクティブ VLAN を設定できます。アクティブな VLAN とは、**nameif** コマンドが設定された VLAN のことです。いずれのライセンスでも、ASA 5505 適応型セキュリティ アプライアンスでは最大 5 つの非アクティブな VLAN を設定できますが、これらをアクティブにする場合は、ライセンスのガイドラインに従う必要があります。

基本ライセンスでは、3 つめの VLAN は **no forward interface** コマンドを使用して設定し、この VLAN から他の特定の VLAN への接続の開始を制限する必要があります。

たとえば、1 つめの VLAN がインターネット アクセス用の外部ネットワークに、2 つめの VLAN が内部の業務用ネットワークに、3 つめの VLAN が家庭用ネットワークにそれぞれ割り当てられているとします。家庭用ネットワークから業務用ネットワークにアクセスする必要はないため、家庭用 VLAN に対して **no forward interface** コマンドを使用できます。業務用ネットワークから家庭用ネットワークにはアクセスできますが、家庭用ネットワークから業務用ネットワークにはアクセスできません。

すでに 2 つの VLAN インターフェイスに **nameif** コマンドを設定している場合は、3 つめのインターフェイスに **nameif** コマンドを設定する前に **no forward interface** コマンドを入力する必要があります。セキュリティ アプライアンス（ASA 5505 適応型セキュリティ アプライアンス）の基本ライセンスでは、3 つの VLAN インターフェイスすべてを完全に動作させることは許可されていません。

例

次の例では、3 つの VLAN インターフェイスを設定します。3 つめの家庭用インターフェイスは、業務用インターフェイスにトラフィックを転送できません。

```
hostname(config)# interface vlan 100
hostname(config-if)# nameif outside
hostname(config-if)# security-level 0
hostname(config-if)# ip address dhcp
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 200
hostname(config-if)# nameif work
hostname(config-if)# security-level 100
hostname(config-if)# ip address 10.1.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface vlan 300
hostname(config-if)# no forward interface vlan 200
hostname(config-if)# nameif home
hostname(config-if)# security-level 50
hostname(config-if)# ip address 10.2.1.1 255.255.255.0
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/0
hostname(config-if)# switchport access vlan 100
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/1
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/2
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/3
hostname(config-if)# switchport access vlan 200
hostname(config-if)# no shutdown

hostname(config-if)# interface ethernet 0/4
hostname(config-if)# switchport access vlan 300
hostname(config-if)# no shutdown

...
```

関連コマンド

コマンド	説明
backup interface	たとえば、ISP へのバックアップ リンクとしてインターフェイスを割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
interface vlan	VLAN インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show interface	インターフェイスの実行時ステータスと統計情報を表示します。
switchport access vlan	スイッチ ポートを VLAN に割り当てます。

fqdn

登録時に、指定した FQDN を証明書のサブジェクト代替名の拡張に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **fqdn** コマンドを使用します。fqdn のデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

fqdn [*fqdn* | **none**]

no fqdn

構文の説明

fqdn	完全修飾ドメイン名を指定します。*fqdn* の最大長は 64 文字です。
none	完全修飾ドメイン名を指定しません。

デフォルト

デフォルトの設定には、FQDN は含まれていません。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

証明書を使用した Nokia VPN クライアントの認証をサポートするようにセキュリティ アプライアンスを設定する場合は、**none** キーワードを使用します。Nokia VPN クライアントの証明書認証のサポートの詳細については、**crypto isakmp identity** コマンドまたは **isakmp identity** コマンドを参照してください。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に FQDN engineering を含める例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# fqdn engineering
hostname(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。

コマンド	説明
enrollment retry period	登録要求の送信を試行するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

fragment

パケット フラグメンテーションの付加的な管理を提供して、NFS との互換性を向上させるには、グローバル コンフィギュレーション モードで **fragment** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

fragment {**size** | **chain** | **timeout** *limit*} [*interface*]

no fragment {**size** | **chain** | **timeout** *limit*} *interface*

構文の説明

chain *limit*	完全な IP パケットをフラグメント化できる最大フラグメント数を指定します。
interface	（任意）セキュリティ アプライアンスのインターフェイスを指定します。interface が指定されていない場合、このコマンドはすべてのインターフェイスに適用されます。
size *limit*	IP 再構築データベース内で再構築を待機可能な最大フラグメント数を設定します。 **（注）** セキュリティ アプライアンスでは、キューのサイズが 2/3 までいっぱいになると、既存のファブリック チェーンの一部ではないすべてのフラグメントが受け入れられなくなります。キューの残りの 1/3 は、すでに部分的にキューイングされている不完全なフラグメント チェーンと送信元 IP アドレス、宛先 IP アドレス、および IP ID 番号が同じであるフラグメントを受け入れるために使用されます。この制限は、フラグメント フラッディング攻撃が行われた場合でも、正規のフラグメント チェーンの再構築を可能にするための DoS 保護メカニズムです。
timeout *limit*	フラグメント化されたパケット全体が到着するまで待機する最大秒数を指定します。タイマーは、パケットの最初のフラグメントが到着したあとに開始します。指定した秒数までに到着しなかったパケット フラグメントがある場合、到着済みのすべてのパケット フラグメントが廃棄されます。

デフォルト

デフォルトの設定は次のとおりです。

- **chain** は 24 パケットです。
- *interface* はすべてのインターフェイスです。
- **size** は 200 です。
- **timeout** は 5 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドの引数が変更されました。**chain**、**size**、または **timeout** のいずれかの引数を選択する必要があります。ソフトウェアの以前のリリースではこれらの引数なしで **fragment** コマンドを入力できましたが、これらの引数なしでは入力できなくなりました。

使用上のガイドライン

デフォルトで、セキュリティ アプライアンスでは、完全な IP パケットを再構築するために最大で 24 のフラグメントを受け入れます。ネットワーク セキュリティ ポリシーに基づいて、各インターフェイスで **fragment chain 1** *interface* コマンドを入力して、フラグメント化されたパケットがセキュリティ アプライアンスを通過しないようにセキュリティ アプライアンスを設定することを検討する必要があります。limit を 1 に設定すると、すべてのパケットは完全なものである必要があります。つまり、フラグメント化されていない必要があります。

セキュリティ アプライアンスを通過するネットワーク トラフィックの多くが NFS である場合は、データベースのオーバーフローを回避するために追加の調整が必要となることがあります。

WAN インターフェイスなど、NFS サーバとクライアントとの間の MTU サイズが小さい環境では、**chain** キーワードに追加の調整が必要となる場合があります。この場合、効率性を向上させるために、NFS over TCP を使用することを推奨します。

size *limit* を大きな値に設定すると、セキュリティ アプライアンスがフラグメント フラッディングによる DoS 攻撃を受けやすくなります。**size** *limit* の値は、1550 または 16384 プールの合計ブロック数 以上には設定しないでください。

デフォルト値を使用すると、フラグメント フラッディングによる DoS 攻撃が抑制されます。

例

次に、外部インターフェイスおよび内部インターフェイスにおいてフラグメント化されたパケットの通過を禁止する例を示します。

```
hostname(config)# fragment chain 1 outside
hostname(config)# fragment chain 1 inside
```

引き続き、フラグメント化されたパケットの通過を禁止する追加の各インターフェイスに対して、**fragment chain 1** *interface* コマンドを入力します。

次に、外部インターフェイスのフラグメント データベースを、最大サイズ 2000、最大チェーン長 45、待機時間 10 秒に設定する例を示します。

```
hostname(config)# fragment size 2000 outside
hostname(config)# fragment chain 45 outside
hostname(config)# fragment timeout 10 outside
```

関連コマンド

コマンド	説明
clear configure fragment	すべての IP フラグメント再構成コンフィギュレーションを、デフォルトにリセットします。
clear fragment	IP フラグメント再構成モジュールの動作データをクリアします。
show fragment	IP フラグメント再構成モジュールの動作データを表示します。
show running-config fragment	IP フラグメント再構成コンフィギュレーションを表示します。

frequency

選択した SLA 動作の反復間隔を設定するには、SLA モニタ プロトコル コンフィギュレーション モードで **frequency** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

frequency *seconds*

no frequency

構文の説明

seconds	SLA プローブ間の秒数。有効な値は、1 ～ 604800 秒です。この値は、**timeout** の値未満にはできません。

デフォルト

デフォルトの頻度は、60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

使用上のガイドライン

SLA 動作は、動作のライフタイム中、指定された頻度で繰り返し実行されます。たとえば、60 秒の頻度に設定された **ipIcmpEcho** 動作は、動作のライフタイム中 60 秒ごとにエコー要求パケットを繰り返し送信します。たとえば、エコー動作のデフォルトのパケット数は 1 です。動作が開始されるとこのパケットが送信され、60 秒後に再度送信されます。

個別の SLA 動作において、指定された頻度の値よりも実行に時間がかかる場合は、動作がすぐに繰り返されるのではなく、「busy」という統計情報カウンタが増加します。

frequency コマンドには、**timeout** コマンドに指定された値未満の値は指定できません。

例

次の例では、ID が 123 の SLA 動作を設定し、ID が 1 のトラッキング エントリを作成して、SLA の到達可能性を追跡しています。SLA 動作の頻度が 3 秒に、タイムアウト値が 1000 ミリ秒に設定されています。

```
hostname(config)# sla monitor 123
hostname(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside
hostname(config-sla-monitor-echo)# timeout 1000
hostname(config-sla-monitor-echo)# frequency 3
hostname(config)# sla monitor schedule 123 life forever start-time now
hostname(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
sla monitor	SLA モニタリング動作を定義します。
timeout	SLA 動作が応答を待機する期間を定義します。

fsck

ファイル システムのチェックを実行して、破損を修復するには、特権 EXEC モードで **fsck** コマンドを使用します。

fsck [/no confirm]{**disk0: | disk1: | flash:**}

構文の説明

/noconfirm	任意。修復確認のためのプロンプトを表示しません。
disk0*:*	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

fsck コマンドは破損したファイル システムをチェックし、修復を試みます。他の方法を用いる前に、まずこのコマンドを使用してください。

/noconfirm キーワードは、最初に確認を求めずに破損を自動的に修復します。

例

次の例では、フラッシュ メモリのファイル システムのチェック方法を示しています。

```
hostname# fsck flash:
```

関連コマンド

コマンド	説明
delete	ユーザに表示されるすべてのファイルを削除します。
erase	すべてのファイルを削除し、フラッシュ メモリをフォーマットします。
format	非表示のシステム ファイルを含むファイル システム上のすべてのファイルを消去して、ファイル システムを再インストールします。

ftp mode passive

FTP モードをパッシブに設定するには、グローバル コンフィギュレーション モードで **ftp mode passive** コマンドを使用します。FTP クライアントをアクティブ モードにリセットするには、このコマンドの **no** 形式を使用します。

ftp mode passive

no ftp mode passive

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

ftp mode passive コマンドは、FTP モードをパッシブに設定します。セキュリティ アプライアンスでは、FTP を使用して、FTP サーバとの間でイメージ ファイルやコンフィギュレーション ファイルをアップロードまたはダウンロードできます。**ftp mode passive** コマンドは、セキュリティ アプライアンス上の FTP クライアントの FTP サーバとの通信方法を制御します。

パッシブ FTP では、クライアントは制御接続およびデータ接続の両方を開始します。パッシブ モードとはサーバの状態を指しており、クライアントが開始する制御接続およびデータ接続の両方をサーバが受動的に受け入れることを意味しています。

パッシブ モードでは、送信元ポートおよび宛先ポートの両方が 1023 よりも大きい一時ポートです。モードはクライアントによって設定されます。クライアントは、**passive** コマンドを発行して、パッシブ データ接続の設定を開始します。パッシブ モードではデータ接続の受け入れ側となるサーバは、今回の特定の接続においてリッスンするポート番号を応答として返します。

例

次に、FTP モードをパッシブに設定する例を示します。

```
hostname(config)# ftp mode passive
```

関連コマンド

copy	イメージ ファイルやコンフィギュレーション ファイルを FTP サーバとの間でアップロードまたはダウンロードします。

debug ftp client	FTP クライアントのアクティビティに関する詳細な情報を表示します。
show running-config ftp mode	FTP クライアントのコンフィギュレーションを表示します。

functions（削除）

functions コマンドは、リリース 8.0(2) では使用できません。このコマンドは廃止されており、下位互換性の目的でのみこのコマンド リファレンスに記載されています。Web サイトの URL リストの作成、ファイル アクセス、プラグイン、カスタマイゼーション、言語変換には、import コマンドおよび export コマンドを使用します。

特定のユーザまたはグループ ポリシーに対して、ポート フォワーディング Java アプレットの自動ダウンロード、ファイル アクセス、ファイル ブラウジング、ファイル サーバ名の入力、Web タイプ ACL の適用、HTTP プロキシ、ポート フォワーディング、または WebVPN 上での URL 入力を設定するには、webvpn コンフィギュレーション モードで **functions** コマンドを入力します。設定済みの機能を削除するには、このコマンドの **no** 形式を使用します。

functions {**auto-download | citrix | file-access | file-browsing | file-entry | filter | http-proxy | url-entry | port-forward | none**}

no functions [**auto-download | citrix | file-access | file-browsing | file-entry | filter | url-entry | port-forward**]

構文の説明

auto-download	WebVPN ログイン時のポート フォワーディング Java アプレットの自動ダウンロードをイネーブルまたはディセーブルにします。最初に、ポート フォワーディング、Outlook/Exchange プロキシ、または HTTP プロキシをイネーブルにする必要があります。
citrix	リモート ユーザに対して、MetaFrame Application Server からのターミナル サービスのサポートをイネーブルまたはディセーブルにします。このキーワードを指定すると、セキュリティ アプライアンスがセキュアな Citrix コンフィギュレーション内でセキュア ゲートウェイとして動作します。これらのサービスでは、ユーザは、標準的な Web ブラウザから MetaFrame アプリケーションにアクセスできます。
file-access	ファイル アクセスをイネーブルまたはディセーブルにします。イネーブルの場合、WebVPN ホームページには、サーバ リスト内のファイル サーバが一覧表示されます。ファイル ブラウジングまたはファイル サーバ名の入力をイネーブルにするには、ファイル アクセスをイネーブルにする必要があります。
file-browsing	ファイル サーバおよび共有のブラウジングをイネーブルまたはディセーブルにします。ユーザによるファイル サーバ名の入力を許可するには、ファイル ブラウジングをイネーブルにする必要があります。
file-entry	ユーザによるファイル サーバの名前の入力をイネーブルまたはディセーブルにします。
filter	Web タイプ ACL を適用します。イネーブルの場合、セキュリティ アプライアンスは、WebVPN の **filter** コマンドで定義された Web タイプ ACL を適用します。

http-proxy	リモート ユーザへの HTTP アプレット プロキシの転送をイネーブルまたはディセーブルにします。このプロキシは、Java、ActiveX、Flash などの、適切なマングリングに対して干渉するテクノロジーにおいて有用です。このプロキシによって、セキュリティ アプライアンスの使用を継続しながら、マングリングを回避できます。転送されたプロキシは、自動的にブラウザの古いプロキシ コンフィギュレーションを変更して、すべての HTTP および HTTPS 要求を新しいプロキシ コンフィギュレーションにリダイレクトします。HTTP アプレット プロキシでは、HTML、CSS、JavaScript、VBScript、ActiveX、Java など、ほとんどすべてのクライアント側テクノロジーがサポートされています。サポートされているブラウザは、Microsoft Internet Explorer だけです。
none	すべての WebVPN **functions** に対してヌル値を設定します。デフォルトまたは指定したグループ ポリシーから機能を継承しません。
port-forward	ポート フォワーディングをイネーブルにします。イネーブルの場合、セキュリティ アプライアンスは、WebVPN の **port-forward** コマンドで定義されたポート フォワーディング リストを使用します。
url-entry	ユーザによる URL の入力をイネーブルまたはディセーブルにします。イネーブルの場合でも、セキュリティ アプライアンスは引き続き設定されている URL またはネットワーク ACL に基づいて URL を制限します。URL 入力がディセーブルの場合、セキュリティ アプライアンスでは、WebVPN ユーザは、ホームページ上の URL に制限されます。

デフォルト

機能は、デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドは廃止されました。
7.1(1)	auto-download キーワードおよび citrix キーワードが追加されました。
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

functions none コマンドを発行することによって作成されたヌル値を含め、設定されているすべての機能を削除するには、引数を指定しないでこのコマンドの **no** 形式を使用します。**no** オプションを使用すると、値を別のグループ ポリシーから継承できるようになります。機能の値を継承しない場合は、**functions none** コマンドを使用します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、ファイル アクセスおよびファイル ブラウジングを設定する例を示します。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# functions file-access file-browsing
```

関連コマンド

コマンド	説明
webvpn	グループ ポリシー コンフィギュレーション モードまたはユーザ名コンフィギュレーション モードで使用します。webvpn モードを開始して、グループ ポリシーまたはユーザ名に適用するパラメータを設定できるようにします。
webvpn	グローバル コンフィギュレーション モードで使用します。WebVPN のグローバル設定を設定できます。