Cisco Secure Firewall ASA シリーズ コマンドリファレンス、I ～ R コマンド

最終更新：2023 年 5 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

第 I 部

I コマンド

ia – inr

icmp

Cisco Secure Firewall ASA インターフェイスで終了する ICMP トラフィックのアクセスルールを設定するには、**icmp** 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。

icmp { **permit** | **deny** } *ip_address net_mask* [*icmp_type*] *if_name*
no icmp { **permit** | **deny** } *ip_address net_mask* [*icmp_type*] *if_name*

構文の説明

deny	条件に合致している場合、アクセスを拒否します。
icmp_type	（任意）ICMP メッセージタイプ（表 1-1 を参照）。
if_name	インターフェイス名。
ip_address	ICMP メッセージをインターフェイスに送信しているホストの IP アドレス。
net_mask	ホストの IP アドレスに適用するネットワーク マスク。
permit	条件に合致している場合、アクセスを許可します。

コマンド デフォルト

ASA のデフォルトの動作は、ASA インターフェイス宛てのすべての ICMP トラフィックを許可することです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

icmp コマンドは、ASA インターフェイスで終了する ICMP トラフィックを制御します。ICMP コントロールリストが設定されていない場合、ASA は外部インターフェイスを含め任意のインターフェイスで終了するすべての ICMP トラフィックを受け付けます。ただし、デフォルトでは、ASA はブロードキャストアドレスに送信される ICMP エコー要求に応答しません。

ASAは、トラフィックが着信するインターフェイス宛てのICMPトラフィックにのみ応答します。ICMP トラフィックは、離れたインターフェイスにインターフェイス経由で送信できません。

ASA への通過ルートとなるインターフェイス以外のインターフェイスへの VPN アクセスはサポートされません。たとえば、VPN アクセスが外部インターフェイスにある場合、外部インターフェイスへの直接接続のみ開始できます。複数のアドレスを覚える必要がないように、ASAの直接アクセス可能インターフェイスのVPNを有効にし、名前解決を使用してください。

icmp deny コマンドはインターフェイスへの ping の実行をディセーブルにし、icmp permit コマンドはインターフェイスへの ping の実行をイネーブルにします。ping の実行が無効になっている場合、ASA はネットワーク上で検出できません。これは、設定可能なプロキシ ping とも呼ばれます。

宛先が保護されたインターフェイスにある場合、access-list extended コマンドまたは access-group コマンドは ASA 経由でルーティングされる ICMP トラフィックに対して使用します。

ICMP 到達不能メッセージ タイプ（タイプ 3）の権限を付与することを推奨します。ICMP 到達不能メッセージを拒否すると、ICMPパスMTUディスカバリがディセーブルになって、IPSec および PPTP トラフィックが停止することがあります。パス MTU ディスカバリの詳細については、RFC 1195 および RFC 1435 を参照してください。

インターフェイスのICMPコントロールリストが設定されている場合、ASAは指定されたICMPトラフィックを照合し、そのインターフェイス上の他のすべてのICMPトラフィックに関して暗黙拒否を適用します。つまり、最初に一致したエントリが許可エントリである場合、ICMP パケットは引き続き処理されます。最初に一致したエントリが拒否エントリであるか、エントリが一致しない場合、ASAによってICMPパケットは破棄され、syslogメッセージが生成されます。例外は、ICMP コントロール リストが設定されていない場合です。その場合、permit ステートメントがあるものと見なされます。

次の表に、サポートされている ICMP タイプの値を示します。

表 *1: ICMP* タイプおよびリテラル

ICMP タイプ	リテラル
0	echo-reply
3	unreachable
8	echo
11	time-exceeded

例

次に、到達不能メッセージを除き、外部インターフェイスで、一般的なすべての ping 要求とすべての着信 ICMP 接続を拒否する例を示します。

```
ciscoasa(config)# icmp permit any unreachable outside
```

ICMP トラフィックを拒否するその他のインターフェイスごとに **icmp deny any** *interface* コマンドの入力を続けます。

次に、ホスト 172.16.2.15 またはサブネット 172.22.1.0/16 上のホストに外部インターフェイスへの ping の実行を許可する例を示します。

```
ciscoasa(config)# icmp permit host 172.16.2.15 echo outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo outside
ciscoasa(config)# icmp permit any unreachable outside
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

icmp-object

ICMP オブジェクト グループに ICMP タイプを追加するには、ICMP タイプ コンフィギュレーション モードで icmp-object コマンドを使用します。ICMP タイプを削除するには、このコマンドの **no** 形式を使用します。

icmp-object*icmp_type*
no icmp-object *icmp_type*

構文の説明

icmp_type	ICMP タイプの名前または番号（0 ～ 255）を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ICMP タイプ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

icmp-object コマンドは、ICMP オブジェクトを定義するために、**object-group icmp-type** コマンドとともに使用されます。また、ICMP タイプ コンフィギュレーション モードで使用されます。

ICMP タイプを含むサービス グループを作成する場合は、このコマンドではなく、**object-group service** コマンドと **service-group** コマンドを使用します。サービス グループには ICMP6 および ICMP のコードを含めることができますが、ICMP オブジェクトにはそれらのコードを含めることはできません。

ICMP タイプの番号と名前には、次のものがあります。

番号	ICMP タイプ名
0	**echo-reply**
3	**unreachable**

番号	ICMP タイプ名
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**
13	**timestamp-request**
18	**timestamp-reply**
15	**information-request**
16	**information-reply**
17	**address-mask-request**
18	**address-mask-reply**
31	**conversion-error**
32	**mobile-redirect**

例

次に、ICMP タイプ コンフィギュレーション モードで **icmp-object** コマンドを使用する例を示します。

```
ciscoasa(config)# object-group icmp-type icmp_allowed
ciscoasa(config-icmp-type)# icmp-object echo
ciscoasa(config-icmp-type)# icmp-object time-exceeded
ciscoasa(config-icmp-type)# exit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

icmp unreachable

ASA インターフェイスで終端する ICMP トラフィックに到達不能な ICMP メッセージレート制限を設定するには、**icmp unreachable** 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。

icmp unreachable rate-limit *rate* **burst-size** *size*
no icmp unreachable rate-limit *rate* **burst-size** *size*

構文の説明

rate-limit *rate*	到達不能メッセージのレート制限を 1 秒あたり 1 ～ 100 メッセージに設定します。デフォルトは、1 秒あたり 1 メッセージです。
burst-size *size*	バースト レートを 1 ～ 10 に設定します。応答のバーストサイズ数が送信されますが、後続の応答は、レート制限に達するまで送信されません。

コマンド デフォルト

デフォルトのレート制限は、1 秒あたり 1 メッセージです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが追加されました。

使用上のガイドライン

到達不能メッセージなどの ICMP メッセージに ASA インターフェイスへの送信を許可する（**icmp** コマンドを参照）場合は、到達不能メッセージのレートを制御できます。

このコマンド、および **set connection decrement-ttl** コマンドは、ASA をホップの 1 つとして表示する ASA 経由の traceroute を可能とするために必要です。

例

次の例では、存続時間のデクリメントをイネーブルにして、ICMP 到達不能レート制限を設定します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class local_server
ciscoasa(config-pmap-c)# set connection decrement-ttl
```

```
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# icmp permit host 172.16.2.15 echo-reply outside
ciscoasa(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
ciscoasa(config)# icmp permit any unreachable outside
ciscoasa(config)# icmp unreachable rate-limit 50 burst-size 10
```

関連コマンド

コマンド	説明
clear configure icmp	ICMP コンフィギュレーションをクリアします。
debug icmp	ICMP のデバッグ情報の表示をイネーブルにします。
set connection decrement-ttl	パケットの存続可能時間の値をデクリメントします。
show icmp	ICMP コンフィギュレーションを表示します。
timeout icmp	ICMP のアイドル タイムアウトを設定します。

id-cert-issuer

システムがこのトラストポイントに関連付けられた CA が発行したピア証明書を受け付けるかどうかを示すには、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 **id-cert-issuer** コマンドを使用します。トラストポイントに関連付けられた CA によって発行された証明書を拒否するには、このコマンドの **no** 形式を使用します。これは、広く使用されているルート CA を表すトラストポイントに便利です。

id-cert-issuer
no id-cert-issuer

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。

コマンド デフォルト

デフォルト設定はイネーブルになっています（アイデンティティ証明書は受け付けられます）。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、広く使用されているルート証明書の下位証明書が発行した証明書に限って受け付けることができます。この機能を許可しないと、ASA はこの発行者によって署名された IKE ピア証明書を拒否します。

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、管理者がトラストポイント central の発行者によって署名されたアイデンティティ証明書を受け付ける例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# id-cert-issuer
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	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。

id-mismatch

過度の DNS ID 不一致のロギングを有効にするには、パラメータ コンフィギュレーション モードで **id-mismatch** 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。

id-mismatch [**count** *number* **duration** *seconds*] **action log**
id-mismatch [**count** *number* **duration** *seconds*] **action log**]

構文の説明

count number	不一致の最大数。この数を超えると、システム メッセージ ログが送信されます。
duration seconds	モニタする期間（秒単位）。

コマンド 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。コマンドがイネーブルで、オプションが指定されていない場合、デフォルトのレートは 3 秒間で 30 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

DNS ID 不一致のレートが高い場合、キャッシュ侵害攻撃が発生している可能性があります。このコマンドをイネーブルにすると、このような攻撃をモニターし、警告を発することができます。不一致レートが設定値を超えた場合、システム メッセージ ログを要約したものが印刷されます。**id-mismatch** コマンドは、通常のイベントベースのシステムメッセージログに加え、追加の情報をシステム管理者に提供します。

例

次に、DNS インスペクション ポリシー マップで ID 不一致をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# id-mismatch action log
```

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。

id-randomization

DNS クエリの DNS 識別子をランダム化するには、パラメータ コンフィギュレーション モードで **id-randomization** 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。

id-randomization
no id-randomization

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。

コマンド デフォルト

デフォルトでは、ディセーブルです。DNS クエリーからの DNS 識別子は変更されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

ID のランダム化は、キャッシュ侵害攻撃からの保護に役立ちます。

例

次に、DNS インスペクション ポリシー マップで ID のランダム化をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# id-randomization
```

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。

id-usage

証明書の登録済み ID を使用できることを指定するには、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 **id-usage** コマンドを使用します。証明書の使用をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

id-usage { **ssl-ipsec** | **code-signer** }
no id-usage { **ssl-ipsec code-signer** }

構文の説明

code-signer	この証明書で表されるデバイスの ID は、リモート ユーザーに提供されるアプレットを検証する際に Java コード署名者として使用されます。
ssl-ipsec	（デフォルト）この証明書で表されるデバイスの ID は、SSL 接続または IPsec-encrypted 接続のサーバー側 ID として使用できます。

コマンド デフォルト

id-usage コマンドのデフォルトは **ssl-ipsec** 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

リモート アクセス VPN では、配置要件に応じて SSL、IPsec、またはその両方のプロトコルを使用して、ほとんどすべてのネットワーク アプリケーションまたはリソースへのアクセスを許可できます。**id-usage** コマンドを使用すると、証明書で保護されたさまざまなリソースへのアクセスのタイプを指定できます。

CA の ID と、場合によってはデバイスの ID は、CA が発行した証明書に基づいています。クリプト CA トラストポイント コンフィギュレーション モードのコマンドはすべて、ASA が CA 証明書を取得する方法、CA から自身の証明書を取得する方法、および CA によって発行され

るユーザー証明書の認証ポリシーを指定するCA固有のコンフィギュレーションパラメータを制御します。

id-usage コマンドは、1 つのトラストポイント コンフィギュレーションに 1 回のみ指定できます。**code-signer** や **ssl-ipsec** オプションのトラストポイントを有効にするには、コマンドを 1 回使用して、いずれか一方または両方のオプションを指定できます。

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、トラストポイント central をコード署名者の証明書として指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer
ciscoasa(config-ca-trustpoint)#
```

次に、トラストポイント general 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、トラストポイント general をコード署名者の証明書として、かつ SSL 接続または IPsec 接続のサーバー側 ID として指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)# id-usage code-signer ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

次に、トラストポイント checkin1 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、トラストポイント checkin1 の使用を SSL 接続または IPsec 接続に制限するようにトラストポイント checkin1 をリセットする例を示します。

```
ciscoasa(config)# crypto ca trustpoint checkin1
ciscoasa(config-ca-trustpoint)# no
 id-usage ssl-ipsec
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	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ます。
java-trustpoint	指定されたトラストポイントの場所から PKCS12 証明書およびキー関連情報を使用するように WebVPN Java オブジェクト署名機能を設定します。
ssl trust-point	インターフェイスのSSL証明書を表す証明書を指定します。
trust-point (tunnel-group ipsec-attributes mode)	IKE ピアに送信される証明書を識別する名前を指定します。
validation-policy	ユーザー接続に関連付けられた証明書を検証する条件を指定します。

igmp

インターフェイスでのIGMP処理を元の状態に戻すには、インターフェイス コンフィギュレーション モードで **igmp** コマンドを使用します。インターフェイスでIGMP処理を無効にするには、このコマンドの **no** 形式を使用します。

igmp
no igmp

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。

コマンド デフォルト

イネーブル

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

実行コンフィギュレーションではこのコマンドの **no** 形式のみが表示されます。

例

次に、選択したインターフェイス上のIGMP処理をディセーブルにする例を示します。

```
ciscoasa(config-if)# no igmp
```

関連コマンド

コマンド	説明
show igmp groups	ASA に直接接続されている受信者、および IGMP を通じて学習された受信者を含むマルチキャストグループを表示します。
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp access-group

インターフェイスからサービスを提供されているサブネット上のホストが参加できるマルチキャストグループを制御するには、インターフェイス コンフィギュレーション モードで **igmp access-group** コマンドを使用します。インターフェイスでグループを無効にするには、このコマンドの **no** 形式を使用します。

igmp access-group *acl*
no igmp access-group *acl*

構文の説明

acl	IP アクセス リスト名。標準のアクセス リストまたは拡張アクセス リストを指定できます。ただし、拡張アクセスリストを指定した場合は、宛先アドレスのみが照合されるため、送信元には **any** を指定する必要があります。

コマンド デフォルト

すべてのグループがインターフェイスでの参加を許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	こ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 モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

例

次に、アクセス リスト 1 でグループへの参加を許可するホストを制限する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp access-group 1
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp forward interface

すべてのIGMPホストレポートの転送を有効にし、受信したメッセージを指定されたインターフェイスに残しておくには、インターフェイス コンフィギュレーション モードで**igmp forward interface** コマンドを使用します。転送を削除するには、このコマンドの**no**形式を使用します。

igmp forward interface *if-name*
no igmp forward interface *if-name*

構文の説明

if-name インターフェイスの論理名。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	こ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 モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

入力インターフェイスでこのコマンドを入力します。このコマンドは、スタブ マルチキャスト ルーティングに使用されるため、PIM と同時には設定できません。

例

次に、IGMP ホスト レポートを現在のインターフェイスから指定したインターフェイスに転送する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp forward interface outside
```

関連コマンド

コマンド	説明
show igmp interface	インターフェイスのマルチキャスト情報を表示します。

igmp join-group

指定したグループのローカルに接続されたメンバーになるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **igmp join-group** コマンドを使用します。グループのメンバーシップをキャンセルするには、このコマンドの **no** 形式を使用します。

igmp join-group *group-address*
no igmp join-group *group-address*

構文の説明

group-address	マルチキャスト グループの IP アドレス。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	こ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 モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドは、マルチキャストグループのメンバーとなるように ASA インターフェイスを設定します。 **igmp join-group** コマンドを使用すると、ASA は指定したマルチキャストグループ宛てのマルチキャストパケット受け付けて転送します。

（注） **igmp join-group** コマンドは、ASA がインターフェイスの指定ルーター（DR）である場合にのみ有効です。

マルチキャストグループのメンバーにならずにマルチキャストトラフィックを転送するように ASA を設定するには、**igmp static-group** コマンドを使用します。

例

次に、IGMP グループ 255.2.2.2 に参加するように、選択したインターフェイスを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp join-group 225.2.2.2
```

関連コマンド

コマンド	説明
igmp static-group	指定したマルチキャスト グループのスタティックに接続されたメンバーになるように、インターフェイスを設定します。

igmp limit

インターフェイス単位でIGMP状態の数を制限するには、インターフェイス コンフィギュレーション モードで**igmp limit** コマンドを使用します。デフォルトの制限に戻すには、このコマンドの **no** 形式を使用します。

igmp limit *number*
no igmp limit [*number*]

構文の説明

number インターフェイスで許可されている IGMP 状態の数。有効な値の範囲は 0 ～ 5000 です。デフォルト値は5000です。この値を0に設定すると、学習したグループが追加されなくなりますが、手動で定義したメンバーシップ（**igmp join-group** and **igmp static-group** コマンドを使用）は引き続き許可されます。

コマンド デフォルト

デフォルトは 5000 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドは、 **igmp max-groups** コマンドに置き換えられました。
9.15(1) *9.12(4)* でも同様	igmp limit が 500 から 5000 に増加しました。

使用上のガイドライン

このコマンドは、IGMP 状態の制限を設定します。設定された上限を超過したメンバーシップ報告はIGMPキャッシュに入力されず、超過した分のメンバーシップ報告のトラフィックは転送されません。

アクティブな結合があるインターフェイスでIGMP制限を変更した場合、新しい制限は既存のグループには適用されません。ASAでは、新しいグループがインターフェイスに追加されたときと IGMP join タイマーが期限切れになったときにのみ制限を検証します。新しい制限をすぐ

に適用するには、インターフェイスで IGMP を無効にしてから再度有効にする必要があります。

例

次に、インターフェイス上の IGMP 状態の数を 250 に制限する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp limit 250
```

関連コマンド

コマンド	説明
igmp	インターフェイス上の IGMP 処理を元の状態に戻します。
igmp join-group	指定したグループのローカルに接続されたメンバーになるようにインターフェイスを設定します。
igmp static-group	指定したマルチキャスト グループのスタティックに接続されたメンバーになるように、インターフェイスを設定します。

igmp query-interval

IGMP ホストクエリメッセージがインターフェイスによって送信される頻度を設定するには、インターフェイス コンフィギュレーション モードで **igmp query-interval** コマンドを使用します。デフォルトの頻度に戻すには、このコマンドの **no** 形式を使用します。

igmp query-interval *seconds*
no igmp query-interval *seconds*

構文の説明

seconds IGMP ホスト クエリー メッセージを送信する頻度（秒単位）。有効な値の範囲は、1 ～ 3600 です。デフォルト値は 125 秒です。

コマンド デフォルト

デフォルトのクエリー間隔は 125 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	こ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 モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

マルチキャストルータは、ホストクエリーメッセージを送信して、インターフェイスにアタッチされているネットワークでどのマルチキャストグループがメンバーを持っているかを検出します。ホストは、特定のグループのマルチキャスト パケットを受信することを示す IGMP レポート メッセージで応答します。ホスト クエリー メッセージは、アドレスが 224.0.0.1 で、TTL 値が 1 である all-hosts マルチキャスト グループ宛てに送信されます。

LAN の指定ルータが、IGMP ホスト クエリー メッセージを送信する唯一のルータです。

- IGMP バージョン 1 の場合、指定ルータは LAN で稼働するマルチキャスト ルーティング プロトコルに従って選択されます。

- IGMP バージョン 2 の場合、指定ルータはサブネットで最も小さな IP アドレスが指定されたマルチキャスト ルータです。

ルータがタイムアウト時間（**igmp query-timeout** コマンドによって制御されます）にクエリーを受信しないと、そのルータがクエリアになります。

注意 この値を変更すると、マルチキャスト転送に深刻な影響が及ぶ可能性があります。

例

次に、IGMP クエリー間隔を 120 秒に変更する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-interval 120
```

関連コマンド

コマンド	説明
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最大応答時間を設定します。
igmp query-timeout	前のクエリアがクエリーを停止した後、ルータがインターフェイスのクエリアとして引き継ぐまでのタイムアウト期間を設定します。

igmp query-max-response-time

IGMP クエリでアドバタイズされる最大応答時間を指定するには、インターフェイス コンフィギュレーション モードで **igmp query-max-response-time** コマンドを使用します。デフォルトの応答時間に戻すには、このコマンドの **no** 形式を使用します。

igmpquery-max-response-time *seconds*
no igmp query-max-response-time *seconds*

構文の説明

seconds IGMP クエリーでアドバタイズされる最大応答時間（秒単位）。有効な値は、1 ～ 25 です。デフォルト値は 10 秒です。

コマンド デフォルト

10 秒。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	こ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 モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

このコマンドは、IGMP バージョン 2 または 3 が実行されているときにだけ有効です。

このコマンドは、応答側が IGMP クエリー メッセージに応答できる期間を制御します。この期間を過ぎると、ルータはグループを削除します。

例

次に、最大クエリー応答時間を 8 秒に変更する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-max-response-time 8
```

関連コマンド

コマンド	説明
igmp query-interval	IGMP ホスト クエリー メッセージがインターフェイスによって送信される頻度を設定します。
igmp query-timeout	前のクエリアがクエリーを停止した後、ルータがインターフェイスのクエリアとして引き継ぐまでのタイムアウト期間を設定します。

igmp query-timeout

前のクエリアがクエリを停止した後でインターフェイスがクエリアを引き継ぐまでのタイムアウト期間を設定するには、インターフェイス コンフィギュレーション モードで **igmp query-timeout** 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。

igmpquery-timeout *seconds*
no igmp query-timeout *seconds*

構文の説明

seconds	前のクエリアがクエリーを停止した後でルータがクエリアを引き継ぐまでの秒数。有効な値は、60 ～ 300 秒です。デフォルト値は 255 秒です。

コマンド デフォルト

デフォルトのクエリー間隔は 255 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、IGMP バージョン 2 または 3 が必要です。

例

次に、最後のクエリーを受信してからインターフェイスのクエリアを引き継ぐまで200秒待機するようにルータを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp query-timeout 200
```

関連コマンド

コマンド	説明
igmp query-interval	IGMP ホストクエリーメッセージがインターフェイスによって送信される頻度を設定します。
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最大応答時間を設定します。

igmp static-group

指定したマルチキャストグループの静的に接続されたメンバーになるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **igmp static-group** コマンドを使用します。スタティック グループ エントリを削除するには、このコマンドの **no** 形式を使用します。

igmp static-group *group*
no igmp static-group *group*

構文の説明

group	IP マルチキャスト グループ アドレス。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

igmp static-group コマンドで設定された場合、ASA インターフェイスは指定されたグループ自体宛てのマルチキャストパケットを受け付けず、転送だけします。特定のマルチキャストグループのマルチキャストパケットを受け付けて転送するように ASA を設定するには、**igmp join-group** コマンドを使用します。**igmp static-group** コマンドと同じグループアドレスに対して **igmp join-group** コマンドが設定されている場合、**igmp join-group** コマンドが優先され、グループはローカルに参加したグループのように動作します。

（注） **igmp static-group** コマンドは、ASA がインターフェイスの指定ルーター（DR）である場合にのみ有効です。

例

次に、選択したインターフェイスをマルチキャスト グループ 239.100.100.101 に追加する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp static-group 239.100.100.101
```

関連コマンド

コマンド	説明
igmp join-group	指定したグループのローカルに接続されたメンバーになるようにインターフェイスを設定します。

igmp version

インターフェイスが使用するIGMPのバージョンを設定するには、インターフェイス コンフィギュレーション モードで **igmp version** コマンドを使用します。バージョンをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

igmp version { **1** | **2** }
no igmp version [**1** | **2**]

構文の説明

1	IGMP バージョン 1。
2	IGMP バージョン 2。

コマンド デフォルト

IGMP バージョン 2。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	こ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 モードに移動しました。以前のバージョンでは、マルチキャスト インターフェイス コンフィギュレーション モードを開始する必要がありましたが、このモードは使用できなくなりました。

使用上のガイドライン

サブネット上のすべてのルータが、同じバージョンのIGMPをサポートする必要があります。ホストは任意の IGMP バージョン（1 または 2）を搭載でき、ASA はホストの存在を正しく検出して適切にホストをクエリできます。

igmp query-max-response-time や **igmp query-timeout** など一部のコマンドでは、IGMP バージョン 2 が必要です。

例

次に、IGMP バージョン 1 を使用するように、選択したインターフェイスを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# igmp version 1
```

関連コマンド

コマンド	説明
igmp query-max-response-time	IGMP クエリーでアドバタイズされる最大応答時間を設定します。
igmp query-timeout	前のクエリアがクエリーを停止した後、ルータがインターフェイスのクエリアとして引き継ぐまでのタイムアウト期間を設定します。

ignore-ipsec-keyusage（廃止）

IPsec クライアント証明書でキー使用状況チェックを実行しないようにするには、CA トラストポイント コンフィギュレーション モードで **ignore-ipsec-keyusage** コマンドを使用します。キー使用状況チェックを再開するには、このコマンドの **no** 形式を使用します。

ignore-ipsec-keyusage
no ignore-ipsec-keyusage

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA トラストポイント コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドは安全対策として追加されましたが、すぐに廃止されました。今後のリリースでは、キー使用状況チェックの停止が提供されない可能性があることに注意してください。

使用上のガイドライン

このコマンドを使用すると、IPsec リモートクライアント証明書のキー使用状況および拡張キー使用状況の値が検証されなくなります。このコマンドはキー使用状況チェックを無視し、非準拠の配置に便利です。

例

次に、キー使用状況チェックの結果を無視する例を示します。

```
ciscoasa(config)#
crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ipsec-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

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

ignore lsa mospf

ルータが LSA Type 6 MOSPF パケットを受信したときには syslog メッセージの送信を行わないようにするには、ルータ コンフィギュレーション モードで **ignore lsa mospf** コマンドを使用します。syslog メッセージの送信を復元するには、このコマンドの **no** 形式を使用します。

ignore lsa mospf
no ignore lsa mospf

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Type 6 MOSPF パケットはサポートされていません。

例

次に、LSA Type 6 MOSPF パケットを無視する例を示します。

```
ciscoasa(config-router)# ignore lsa mospf
```

関連コマンド

コマンド	説明
show running-config router ospf	OSPF ルータ コンフィギュレーションを表示します。

ignore-lsp-errors

ASA が内部チェックサムエラーのある IS-IS リンクステートパケットを受信した場合、パージするのではなく無視できるようにするには、ルータ ISIS コンフィギュレーション モードで **ignore-lsp-errors** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ignore-lsp-errors
no ignore-lsp-errors

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。

コマンド 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。つまり、ネットワークの安定性のために、破損した LSP は除去されるのではなくドロップ

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

IS-IS プロトコル定義では、データリンク チェックサムが不正な受信リンクステート パケットを受信側が除去することになっています。これにより、パケットの発信側はLSP を再生成します。ただし、正しいデータリンク チェックサムによってリンクステート パケットを配信中にデータの破損を引き起こすリンクがネットワークに含まれている場合、大量のパケットの除去と再生成を繰り返す連続サイクルが発生する可能性があります。

その結果、ネットワークが機能しなくなる可能性があるため、**ignore-lsp-errors** コマンドを使用して、リンクステートパケットを除去せずに、無視します。受信側ルータは、リンクステート パケットを使用してルーティング テーブルのメンテナンスを行います。

破損した LSP を明示的に除去するには、**no ignore-lsp-errors** コマンドを発行します。

例

次に、内部チェックサムを持つリンクステート パケットを無視するようにルータに指示する例を示します。

エラー：

ciscoasa(config)# **router isis**

```
ciscoasa(config-router)# ignore-lsp-errors
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。

コマンド	説明
isis authentication mode	インターフェイスごとに、インスタンスに対してIS-ISパケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-ISパケットに対してのみ認証を実行するように、インターフェイスごとのIS-ISインスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャストインターフェイス上で定期的にCSNPパケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS helloをインターフェイスごとのフルMTUサイズに設定します。
isis lsp-interval	インターフェイスごとの連続するIS-ISLSP送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定されたASAのプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各IS-ISLSPの再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各IS-ISLSPの再送信間の時間を設定します。
isis tag	IPプレフィックスがLSPに挿入されたときに、インターフェイスに設定されたIPアドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASAがログメッセージを生成できるようにします。

コマンド	説明
lsp-full suppress	PDUがフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSPが更新されずにASAのデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべてのIS-ISインターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成してLSPデータベースをクリアすることができないように、IS-ISプロトコルをグローバルで無効にします。
redistribute isis	特にレベル1からレベル2へ、またはレベル2からレベル1へ、IS-IS ルートを再配布します。
route priority high	IS-IS IPプレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。

コマンド	説明
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

ignore-ssl-keyusage（廃止）

SSL クライアント証明書でキー使用状況チェックを実行しないようにするには、CA トラストポイント コンフィギュレーション モードで **ignore-ssl-keyusage** コマンドを使用します。キー使用状況チェックを再開するには、このコマンドの **no** 形式を使用します。

ignore-ssl-keyusage
no ignore-ssl-keyusage

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA トラストポイント コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドは安全対策として追加されましたが、すぐに廃止されました。今後のリリースでは、キー使用状況チェックの停止が提供されない可能性があることに注意してください。

使用上のガイドライン

このコマンドを使用すると、IPsec リモートクライアント証明書のキー使用状況および拡張キー使用状況の値が検証されなくなります。このコマンドはキー使用状況チェックを無視し、非準拠の配置に便利です。

例

次に、キー使用状況チェックの結果を無視する例を示します。

```
ciscoasa(config)#
crypto ca trustpoint central
ciscoasa(config-ca-trustpoint)#
ciscoasa(config-ca-trustpoint)# ignore-ssl-keyusage
Notice: This command has been deprecated
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

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

ike-retry-count

SSL による接続試行に戻るまでに、Cisco AnyConnect VPN Client が IKE を使用して接続を再試行できる最大数を設定するには、グループ ポリシー webvpn コンフィギュレーション モード、またはユーザー名 webvpn コンフィギュレーション モードで **ike-retry-count** コマンドを使用します。構成からこのコマンドを削除し、再試行の最大数をデフォルト値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。

ike-retry-count { **none** | *value* }
no ike-retry-count { **none** | *value* }

構文の説明

none	再試行を許可しないことを指定します。
value	初期接続障害の後、Cisco AnyConnect VPN クライアントが接続を再試行できる最大数（1 ～ 10）を指定します。

コマンド デフォルト

許可されている再試行のデフォルトの回数は 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名 webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco AnyConnect VPN Client が IKE を使用して接続を試行できる回数を制御するには、**ike-retry-count** コマンドを使用します。IKE を使用して接続に失敗した回数がこのコマンドに指定された再試行数を上回ると、SSL による接続試行に戻ります。この値は、Cisco AnyConnect VPN クライアントに存在する値を上書きします。

（注） IPsec から SSL へのフォールバックをサポートするには、**vpn-tunnel-protocol** コマンドに **svc** 引数と **ipsec** 引数の両方を設定する必要があります。

例

次に、FirstGroup というグループ ポリシーの IKE 再試行回数を 7 に設定する例を示します。

```
ciscoasa
(config)# group-policy FirstGroup attributes
ciscoasa
(config-group-policy)# webvpn
ciscoasa
(config-group-webvpn)# ike-retry-count 7
ciscoasa
(config-group-webvpn)#
```

次に、ユーザー名 Finance の IKE 再試行回数を 9 に設定する例を示します。

```
ciscoasa
(config)#
username
Finance attributes
ciscoasa
(config-username)# webvpn
ciscoasa
(config-username-webvpn)# ike-retry-count 9
ciscoasa
(config-group-webvpn)#
```

関連コマンド

コマンド	説明
group-policy	グループ ポリシーを作成または編集します。
ike-retry-timeout	IKE 再試行間の秒数を指定します。
username	ASA データベースにユーザーを追加します。
vpn-tunnel-protocol	VPN トンネル タイプ（IPsec、L2TP over IPsec、または WebVPN）を設定します。
webvpn	グループ ポリシー webvpn コンフィギュレーション モードまたはユーザー名 webvpn コンフィギュレーション モードを開始します。

ikev1 pre-shared-key

事前共有キーを指定して、事前共有キーに基づいたIKEv1接続をサポートするには、トンネルグループIPSec属性コンフィギュレーション モードで **pre-shared-key** 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。

pre-shared-key*key*
no pre-shared-key

構文の説明

key	1 ～ 128 文字の英数字キーを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	コマンド名が pre-shared-key から ikev1 pre-shared-key に変更されました。

使用上のガイドライン

この属性は、すべての IPsec トンネル グループ タイプに適用できます。

例

次に、設定 IPSec コンフィギュレーション モードで、209.165.200.225 という名前の IPSec LAN-to-LAN トンネル グループの IKE 接続をサポートするように事前共有キー XYZX を指定する例を示します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# pre-shared-key xyzx
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ IPsec 属性を設定します。

ikev1 trust-point

IKEv1 ピアに送信する証明書を識別するトラストポイントの名前を指定するには、トンネルグループ ipsec 属性モードで **trust-point** コマンドを使用します。トラストポイント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。

trust-point*trust-point-name*
no trust-point *trust-point-name*

構文の説明

trust-point-name	使用するトラストポイントの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(1)	コマンド名が trust-point から ikev1 trust-point に変更されました。

使用上のガイドライン

この属性は、すべての IPsec トンネル グループ タイプに適用できます。

例

次に、トンネル ipsec コンフィギュレーション モードを開始し、IPsec LAN-to-LAN トンネル グループ 209.165.200.225 の IKEv1 ピアに送信される証明書を識別するためのトラストポイントを設定する例を示します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 trust-point mytrustpoint
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネルグループをクリアします。

コマンド	説明
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ IPsec 属性を設定します。

ikev1 user-authentication

IKE時にハイブリッド認証を設定するには、トンネルグループipsec属性コンフィギュレーション モードで **ikev1 user-authentication** コマンドを使用します。ハイブリッド認証を無効にするには、このコマンドの **no** 形式を使用します。

ikev1 user-authentication [*interface*] { **none** | **xauth** | **hybrid** }
no ikev1 user-authentication [*interface*] { **none** | **xauth** | **hybrid** }

構文の説明

hybrid	IKE 時にハイブリッド XAUTH 認証を指定します。
interface	（任意）ユーザー認証方式が設定されているインターフェイスを指定します。
none	IKE 時にユーザー認証をディセーブルにします。
xauth	拡張ユーザ認証とも呼ばれる XAUTH を指定します。

コマンド デフォルト

デフォルトの認証方式は XAUTH、つまり拡張ユーザー認証です。デフォルトは、すべてのインターフェイスです。

（注） 確立されている L2TP over IPsec セッションが切断されないようにするには、デフォルト値の XAUTH のままにする必要があります。トンネル グループが他の値（isakmp ikev1-user-authentication none など）に設定されている場合、L2TP over IPsec セッションを確立できません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

リリース	変更内容
8.4(1)	コマンド名が isakmp **ikev1-user-authentication** から **ikev1 user-authentication.** 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、ASA認証にデジタル証明書を使用し、リモートVPNユーザー認証にRADIUS、TACACS+、SecurIDなどの異なる従来の方式を使用する必要がある場合に使用します。このコマンドは、IKE のフェーズ 1 をハイブリッド認証と呼ばれる次の 2 つの手順に分けます。

1. ASA は、標準の公開キー技術を使用して、リモート VPN ユーザーに対して認証します。これにより、単方向に認証する IKE セキュリティ アソシエーションが確立されます。
2. 次に、XAUTH交換がリモートVPNユーザーを認証します。この拡張認証では、サポートされている従来のいずれかの認証方式を使用できます。

（注） 認証タイプをハイブリッドに設定するには、事前に認証サーバーを設定し、事前共有キーを作成し、トラストポイントを設定する必要があります。

交換タイプがメイン モードの場合、IPsec ハイブリッド RSA 認証タイプは拒否されます。

任意の *interface* 引数を省略すると、コマンドはすべてのインターフェイスに適用され、インターフェイスごとのコマンドが指定されていないときにはバックアップとなります。トンネルグループに指定されている **ikev1 user-authentication** コマンドが 2 つある場合、1 つのコマンドでは *interface* 引数を使用し、もう 1 つのコマンドでは使用しません。インターフェイスを指定しているコマンドが、その特定のインターフェイスでは優先されます。

例

次に、example-group というトンネル グループの内部インターフェイスでハイブリッド XAUTH をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev1 user-authentication (inside) hybrid
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバーを定義します。
pre-shared-key	IKE 接続をサポートするための事前共有キーを作成します。
tunnel-group	IPsec、L2TP/IPsec、および WebVPN 接続の接続固有レコードのデータベースを作成および管理します。

ikev2 local-authentication

IKEv2 LAN-to-LAN 接続のリモート認証を指定するには、トンネルグループ ipsec 属性コンフィギュレーション モードで **ikev2 local-authentication** 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。

ikev2 local-authentication { **pre-shared-key** *key_value* | **hex** < *string* > | **certificate trustpoint**
no ikev2 local-authentication { **pre-shared-key** *key_value* | **hex** < *string* > | **certificate trustpoint**

構文の説明

証明書	証明書認証を指定します。
hex	16 進数の事前共有キーを設定します。
key_value	1 ～ 128 文字のキーの値。
pre-shared-key	リモート ピアの認証に使用するローカルの事前共有キーを指定します。
string	2 ～ 256 の偶数の数値で 16 進数の事前共有キーを入力します。
トラストポイント	リモート ピアに送信する証明書を識別するトラストポイントを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.3(2)	EAP を使用したリモート認証が追加されました。
9.4(1)	hex キーワードと hex string キーワードが追加されました。

使用上のガイドライン

このコマンドは、IPsec IKEv2 LAN-to-LAN トンネル グループだけに適用されます。

ローカル認証に対しては、認証オプションは 1 つしか設定できません。

ikev2 remote-authentication コマンドを使用して EAP 認証を有効にする場合は、**certificate** オプションを使用してこのコマンドを設定しておく必要があります。

IKEv2 接続の場合、トンネル グループのマッピングで、リモート認証に使用できる認証方式（PSK、証明書、およびEAP）とローカル認証に使用できる認証方式（PSKおよび証明書）、およびローカル認証で使用するトラストポイントを特定する必要があります。

例

次に、209.165.200.225 という名前の IPsec LAN-to-LAN トンネル グループの IKE 接続をサポートするように事前共有キー XYZX を指定する例を示します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key XYZX
```

次に、トラストポイント myIDcert に関連付けられた ID 証明書を使用して ASA をピアに対して認証するようにリモート アクセス トンネル グループを設定する例を示します。ピアの認証には、事前共有キー、証明書、または EAP も使用できます。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_l2l
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key XYZX
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネルグループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ IPsec 属性を設定します。

ikev2 mobike-rrc

IPsec IKEv2 RA VPN 接続のモバイル IKE（mobike）通信時にリターン ルータビリティ チェックを有効にするには、トンネルグループ IPsec 属性コンフィギュレーション モードで **ikev2 mobike-rrc** コマンドを使用します。リターン ルータビリティ チェックを無効にするには、このコマンドの **no** 形式を使用します。

ikev2 mobike-rrc
no ikev2 mobike-rrc

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。

コマンド 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。

Mobike は「常にオン」になっています。このコマンドは、mobike 接続の RRC をイネーブルするために使用されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IPsec IKEv2 RA VPN トンネル グループだけに適用されます。

例

次に、example-group というトンネル グループの mobike のリターン ルータビリティ チェックをイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group example-group type ipsec-ra
ciscoasa(config)# tunnel-group example-group ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 mobike-rrc
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ IPsec 属性を設定します。

ikev2 remote-authentication

IPsec IKEv2 LAN-to-LAN 接続のリモート認証を指定するには、トンネルグループ ipsec 属性コンフィギュレーション モードで **ikev2 remote-authentication** 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。

ikev2 remote-authentication { **pre-shared-key** *key_value* | **certificate** | **hex <string>** | **eap** [**query-identity**] }
no ikev2 remote-authentication { **pre-shared-key** *key_value* | **certificate** | **hex <string>** | **eap** [**query-identity**] }

構文の説明

証明書	証明書認証を指定します。
eap	拡張可能認証プロトコル（EAP）を指定します。この方式では、（AnyConnect に加えて）サードパーティの汎用の IKEv2 リモート アクセス クライアントによるユーザー認証がサポートされます。
hex	16 進数の事前共有キーを設定します。
key_value	1 ～ 128 文字のキーの値。
pre-shared-key	リモート ピアの認証に使用するローカルの事前共有キーを指定します。
query-identity	ピアに EAP ID を要求します。
string	2 ～ 256 の偶数の数値で 16 進数の事前共有キーを入力します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

リリース	変更内容
9.3(2)	**eap** および **query-identity** キーワードが追加されました。
9.4(1)	hex キーワードと hex-string キーワードが追加されました。

使用上のガイドライン

このコマンドは、IPsec IKEv2 LAN-to-LAN トンネル グループだけに適用されます。

リモート認証で EAP を有効にする前に、**ikev2 local-authentication pre-shared-key** *key-value* | **certificate** *trustpoint* コマンドを使用し、証明書と有効なトラストポイントを使用してローカル認証を設定する必要があります。そうしないと、エラーが発生して、EAP認証要求が拒否されます。

リモート認証では、複数の認証オプションを設定できます。

（注） IKEv2 接続の場合、トンネル グループのマッピングで、リモート認証に使用できる認証方式（PSK、証明書、およびEAP）とローカル認証に使用できる認証方式（PSKおよび証明書）、およびローカル認証で使用するトラストポイントを特定する必要があります。現在、マッピングの実行には、ピアまたはピア証明書のフィールドの値から取得（証明書マップを使用）された IKE ID が使用されます。両方のオプションが失敗した場合、デフォルトのリモート アクセス トンネル グループに着信接続がマッピングされます。証明書マップは、リモート ピアが証明書で認証された場合にのみ適用されるオプションです。このマップにより、異なるトンネル グループへのマッピングが可能です。証明書認証の場合のみ、ルールまたはデフォルトの設定を使用してトンネル グループの参照が行われます。EAP 認証および PSK 認証の場合は、クライアント（トンネル グループ名が一致するクライアント）の IKE ID またはデフォルトの設定を使用してトンネル グループの参照が行われます。

例

次に、209.165.200.225 という名前の IPsec LAN-to-LAN トンネル グループの IKEv2 接続をサポートするように事前共有キー XYZX を指定する例を示します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication pre-shared-key xyzx
```

次に、EAP 認証要求が拒否される例を示します。

```
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication eap query-identity
ciscoasa(config-tunnel-ipsec)# ikev2 remote-authentication certificate
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication pre-shared-key 12345678
ERROR: The local-authentication method is required to be certificate based
if remote-authentication allows EAP
ciscoasa(config-tunnel-ipsec)# ikev2 local-authentication certificate myIDcert
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ IPsec 属性を設定します。

ikev2 rsa-sig-hash

IKEv2 RSA 署名ハッシュを設定するには、トンネルグループ ipsec 属性コンフィギュレーションで **ikev2 rsa-sig-hash** 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。

ikev2rsa-sig-hashsha1
no ikev2 rsa-sig-hash sha1

構文の説明

sha1	SHA-1 ハッシュ関数を使用して IKEv2 認証ペイロードに署名します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.12(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IPsec IKEv2 LAN-to-LAN トンネル グループだけに適用されます。

例

次のコマンドで、SHA-1 関数を使用して IKEv2 認証ペイロードに署名します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# ikev2 rsa-sig-hash sha
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。

コマンド	説明
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ IPsec 属性を設定します。

im

SIP を使用したインスタントメッセージを有効にするには、パラメータ コンフィギュレーション モードで **im** コマンドを使用します。このモードには、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。

im
noim

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップで SIP を経由するインスタント メッセージングをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# im
```

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。

コマンド	説明
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。

imap4s（廃止）

（注） このコマンドをサポートする最後のリリースは、 9.5(1) でした。

IMAP4S コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **imap4s** コマンドを使用します。IMAP4S コマンドモードで入力されたコマンドを削除するには、このコマンドの **no** 形式を使用します。

imap4s
no imap4s

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

IMAP4 は、インターネット サーバーが電子メールを受信し、保持する際に使用するクライアント/サーバー プロトコルです。ユーザー（または電子メール クライアント）は、電子メールのヘッダーおよび送信者だけを表示して、電子メールをダウンロードするかどうかを判別できます。また、サーバーに複数のフォルダまたはメールボックスを作成および操作したり、メッセージを削除したり、メッセージの一部または全体を検索したりできます。IMAP では、電子メールでの作業中、サーバーに連続してアクセスする必要があります。IMAP4S を使用すると、SSL 接続で電子メールを受信できます。

例

次に、IMAP4S コンフィギュレーション モードを開始する例を示します。

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)#
```

関連コマンド

コマンド	説明
clear configure imap4s	IMAP4S コンフィギュレーションを削除します。
show running-config imap4s	IMAP4S の実行コンフィギュレーションを表示します。

imi-traffic-descriptor

IP オプションインスペクションが設定されたパケットヘッダーで IMI トラフィック記述子（IMITD）オプションが発生したときに実行するアクションを定義するには、パラメータ コンフィギュレーション モードで **imi-traffic-descriptor** 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。

imi-traffic-descriptor action { **allow** | **clear** }
no imi-traffic-descriptor action { **allow** | **clear** }

構文の説明

allow	IMI トラフィック記述子 IP オプションを含むパケットを許可します。
clear	IMI トラフィック記述子オプションをパケット ヘッダーから削除してから、パケットを許可します。

コマンド デフォルト

デフォルトでは、IP オプション インスペクションは、IMI トラフィック記述子 IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用すると、デフォルト値を変更できます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプションインスペクションを設定して、特定の IP オプションを持つどの IP パケットが ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# imi-traffic-descriptor action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

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。

import

プレフィックス委任クライアント インターフェイスで ASA が DHCPv6 サーバーから取得した 1 つ以上のパラメータをステートレスアドレス自動設定（SLAAC）クライアントに提供するには、IPv6 DHCP プール コンフィギュレーション モードで **import** コマンドを使用します。パラメータを削除するには、このコマンドの **no** 形式を使用します。

import { [**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**] }
no import { [**dns-server**] [**domain-name**] [**nis address**] [**nis domain-name**] [**nisp address**] [**nisp domain-name**] [**sip address**] [**sip domain-name**] [**sntp address**] }

構文の説明

dns-server	ドメイン ネーム サーバー（DNS）サーバーの IP アドレスをインポートします。
domain-name	ドメイン名をインポートします。
nis address	ネットワーク インフォメーション サービス（NIS）サーバーの IP アドレスをインポートします。
nis domain-name	NIS ドメイン名をインポートします。
nisp address	ネットワーク インフォメーション サービス プラス（NIS+）サーバーの IP アドレスをインポートします。
nisp domain-name	NIS+ ドメイン名をインポートします。
sip address	Session Initiation Protocol（SIP）サーバーの IP アドレスをインポートします。
sip domain-name	SIP ドメイン名をインポートします。
sntp address	Simple Network Time Protocol（SNTP）サーバの IP アドレスをインポートします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合、クライアントが情報要求（IR）パケットを ASA に送信するときに、DNS サーバーやドメイン名を含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。手動で設定されたパラメータとインポートされたパラメータを組み合わせて使用できますが、同じパラメータを手動で設定し、かつ **import** コマンドで設定することはできません。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。

コマンド	説明
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

import webvpn AnyConnect-customization

ASA のフラッシュデバイス上に AnyConnect カスタマイゼーション オブジェクトをロードするには、特権 EXEC モードで **import webvpn AnyConnect-customization** コマンドを使用します。

import webvpn AnyConnect-customization type { **binary** | **resource** | **transform** } **platform** { **linux** | **linux-64** | **mac-intel** | **mac-powerpc** | **win** | **win-mobile** } **name** *name* { *URL* | **stdin** { *num_chars* | *data* **quit** } }

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。最大数は 64 文字です。
platform {**linux** | **linux-64** | **mac-intel** | **mac-powerpc** | **win** | **win-mobile**}	オブジェクトを適用するクライアントのプラットフォーム。
stdin {*num_chars data* | *data* **quit**}	データが stdin から提供されることを指定します。文字数が指定されていない場合、標準入力から読み取られるデータは base64 でエンコードされ、その後に "\nquit\n" が付けられます。
type {**binary** | **resource** | **transform**}	インポート対象のカスタマイゼーション オブジェクトのタイプ。
URL	XML カスタマイゼーション オブジェクトのソースへのリモート パス。最大数は 255 文字です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

import customization コマンドを入力する前に、ASA インターフェイスで WebVPN が有効になっていることを確認します。確認するためには、**show running-config** コマンドを入力します。

ASA はカスタマイゼーション オブジェクトを URL または stdin から ASA ファイルシステムの disk0:/csco_config/customization にコピーします。AnyConnect のカスタマイズには、カスタム AnyConnect GUI リソース、バイナリ カスタム ヘルプ ファイルとバイナリ VPN スクリプト、およびインストーラ変換を含めることができます。

関連コマンド

コマンド	説明
revert webvpn AnyConnect-customization	ASA のフラッシュデバイスから指定された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 AnyConnect-customization	ASA のフラッシュデバイスに存在するカスタマイゼーション オブジェクトを一覧表示します。

import webvpn customization

ASA のフラッシュデバイス上にカスタマイゼーション オブジェクトをロードするには、特権 EXEC モードで **import webvpn customization** コマンドを使用します。

import 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。最大数は 64 文字です。
URL	XML カスタマイゼーション オブジェクトのソースへのリモート パス。最大数は 255 文字です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

import customization コマンドを入力する前に、ASA インターフェイスで WebVPN が有効になっていることを確認します。確認するためには、**show running-config** コマンドを入力します。

カスタマイゼーション オブジェクトをインポートすると、ASA で次のことが実行されます。

- カスタマイゼーション オブジェクトを URL から ASA ファイルシステム disk0:/csco_config/customization に MD5*name* としてコピーします。
- ファイルに対して基本的な XML 構文チェックを実行します。無効な場合、ASA はファイルを削除します。
- index.ini ファイルにレコード MD5*name* が含まれていることをチェックします。含まれていない場合、ASA は MD5*name* をファイルに追加します。

- MD5*name* ファイルを RAMFS /csco_config/customization/ に ramfs *name* としてコピーします。

例

次に、カスタマイゼーション オブジェクト *General.xml* を URL 209.165.201.22/customization から ASA にインポートし、*custom1* という名前を付ける例を示します。

```
ciscoasa# import webvpn customization custom1 tftp://209.165.201.22/customization
/General.xml
Accessing
tftp://209.165.201.22/customization/General.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/custom1...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

関連コマンド

コマンド	説明
revert webvpn customization	ASA のフラッシュデバイスから指定された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	ASA のフラッシュデバイスに存在するカスタマイゼーション オブジェクトを一覧表示します。

import webvpn mst-translation

MST（Microsoft Transform）オブジェクトを ASA のフラッシュデバイスにロードするには、特権 EXEC モードで **import webvpn mst-translation** コマンドを入力します。

import webvpn mst-transation AnyConnect language *language URL* | **stdin** { *num_chars data* | *data* **quit** } }

構文の説明

language *language*	変換言語。
stdin {*num_chars data* | *data* **quit**}	データが stdin から提供されることを指定します。文字数が指定されていない場合、標準入力から読み取られるデータは base64 でエンコードされ、その後に "\nquit\n" が付けられます。
URL	XML カスタマイゼーション オブジェクトのソースへのリモートパス。最大数は 255 文字です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このファイルは、AnyConnect インストーラを変換します。

関連コマンド

コマンド	説明
show import webvpn mst-translation	ASA のフラッシュデバイスに存在するカスタマイゼーション オブジェクトを一覧表示します。

import webvpn plug-in protocol

ASA のフラッシュデバイスにプラグインをインストールするには、特権 EXEC モードで **import webvpn plug-in protocol** コマンドを入力します。

import webvpn plug-in protocol プロトコル *URL*

構文の説明

protocol

- **rdp—**Remote Desktop Protocol プラグインにより、リモート ユーザーは Microsoft Terminal Services が実行するコンピュータに接続できます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://properjavardp.sourceforge.net/ です。
- **ssh,telnet—**セキュア シェル プラグインにより、リモート ユーザーがリモート コンピュータへのセキュア チャネルを確立したり、リモート ユーザーが Telnet を使用してリモート コンピュータに接続したりできます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://javassh.org/ です。

  注意 **import webvpn plug-in protocol ssh,telnet** *URL* コマンドは、SSH と Telnet の両方のプラグインをインストールします。SSH 用と Telnet 用にこのコマンドをそれぞれ入力しないでください。**ssh,telnet** ストリングを入力する場合は、両者の間にスペースは挿入しません。**revert webvpn plug-in protocol** コマンドを使用して、これらの要件から逸脱する **import webvpn plug-in protocol** コマンドを削除します。

- **vnc—**Virtual Network Computing プラグインを使用すると、リモート ユーザーはリモート デスクトップ共有をオンにしたコンピュータを、モニター、キーボード、およびマウスを使用して表示および制御できます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://www.tightvnc.com/ です。

URL　プラグインのソースへのリモート パス。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチコンテキストモードのサポートが追加されました。

使用上のガイドライン

プラグインをインストールする前に、以下の手順に従ってください。

- ASA のインターフェイス上でクライアントレス SSL VPN（「webvpn」）が有効になっていることを確認します。確認するためには、**show running-config** コマンドを入力します。
- ローカル TFTP サーバー（たとえば、ホスト名が「local_tftp_server」のサーバー）で一時ディレクトリを「plugins」という名前で作成し、プラグインをシスコの Web サイトから「plugins」ディレクトリにダウンロードします。TFTP サーバーのホスト名またはアドレスを入力し、必要なプラグインへのパスを **import webvpn plug-in protocol** コマンドの URL フィールドに入力します。

プラグインをインポートすると、ASA で次のことが実行されます。

- *URL* に指定されている .jar ファイルを解凍します。
- ASA ファイル システムの csco-config/97/plugin ディレクトリにファイルを書き込みます。
- ASDM の URL 属性の横にあるドロップダウン メニューに情報を入力します。
- 以後のすべてのクライアントレス SSL VPN セッションでプラグインをイネーブルにし、ポータル ページの Address フィールドの横にあるドロップダウン メニューにメイン メニュー オプションとオプションを追加します。次の表に、ポータル ページのメイン メニューと [Address] フィールドへの変更を示します。

プラグイン	ポータル ページに追加されるメイン メニュー オプション	ポータル ページに追加される [Address] フィールド オプション
citrix	Citrix クライアント	citrix://
rdp	Terminal Servers	rdp://
ssh,telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

ASA は、**import webvpn plug-in protocol** コマンドを構成に保持しません。その代わりに、csco-config/97/plugin ディレクトリの内容を自動的にロードします。セカンダリ ASA は、プライマリ ASA からプラグインを取得します。

クライアントレス SSL VPN セッションでユーザーがポータル ページの関連付けられたメニュー オプションをクリックすると、ポータル ページにはインターフェイスへのウィンドウとヘルプ

ペインが表示されます。ドロップダウン メニューに表示されたプロトコルをユーザーが選択して [Address] フィールドに URL を入力すると、接続を確立できます。

（注） 以前からサポートされている SSH V1 および Telnet に加え、SSH V2 のサポートが追加されています。プラグインのプロトコルは同じ（SSH と Telnet）で、URL の形式は次のとおりです。ssh://<target> — uses SSH V2ssh://<target>/?version=1 — uses SSH V1telnet://<target> — uses telnet

import webvpn plug-in protocol コマンドを個別に削除し、プロトコルのサポートを無効にするには、**revert webvpn plug-in protocol** コマンドを使用します。

例

次のコマンドでは、RDP のクライアントレス SSL VPN サポートを追加しています。

```
ciscoasa# import webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
Accessing
tftp://209.165.201.22/plugins/rdp-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/rdp...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

次のコマンドでは、SSH および Telnet のクライアントレス SSL VPN サポートを追加しています。

```
ciscoasa# import webvpn plug-in protocol ssh,telnet
tftp://209.165.201.22/plugins/ssh-plugin.jar
Accessing
tftp://209.165.201.22/plugins/ssh-plugin.jar...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/ssh...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
238510 bytes copied in 3.650 secs (79503 bytes/sec)
```

次のコマンドでは、VNC のクライアントレス SSL VPN サポートを追加しています。

```
ciscoasa# import webvpn plug-in protocol vnc tftp://209.165.201.22/plugins/vnc-plugin.jar
Accessing tftp://209.165.201.22/plugins/vnc-plugin.jar...!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/plugin/vnc...
!!!!!!!!!!!!!!!
58147 bytes copied in 2.40 secs (29073 bytes/sec)
ciscoasa#
```

関連コマンド

コマンド	説明
revert webvpn plug-in protocol	ASA のフラッシュデバイスから指定されたプラグインを削除します。
show import webvpn plug-in	ASA のフラッシュデバイスに存在するプラグインのリストを示します。

import webvpn translation-table

SSL VPN接続を確立するリモートユーザーに表示される用語の変換に使用される変換テーブルをインポートするには、特権 EXEC モードで **import webvpn translation-table** コマンドを使用します。

import webvpn translation-table *translation_domain* **language** *language url*

構文の説明

language	変換テーブルの言語を指定します。*language* の値は、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	リモート ユーザーに表示される機能エリアと関連するメッセージを指定します。
url	カスタマイゼーション オブジェクトの作成に使用される XML ファイルの URL を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ASA 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ー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ーに表示されるユーザーインターフェイスで使用される言語を変換できます。

リモートユーザー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 argument* 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。

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN Client のユーザーインターフェイスに表示されるメッセージ。
バナー	リモートユーザー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。
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、およびユーザーによるカスタマイズが可能なすべてのメッセージ。
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。
PortForwarder	ポート フォワーディング ユーザーに表示されるメッセージ。
url-list	ユーザーがポータル 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。

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。ASA 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ー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、ASA は **generates the customization** および **url-list** 変換ドメインテンプレートを動的に生成します。テンプレートにより、変更内容が機能エリアに自動的に反映されます。

export webvpn translation-table コマンドを使用して変換ドメインのテンプレートをダウンロードし、メッセージに変更を加え、**import webvpn translation-table** コマンドを使用してオブジェクトを作成します。**show import webvpn translation-table** コマンドを使用して、使用可能なオブジェクトを表示できます。

ブラウザの言語オプションの表現に従って language を指定してください。たとえば、Microsoft Internet Explorer では中国語に短縮形の *>zh* が使用されます。ASA にインポートする変換テーブルも、*>zh* という名前にする必要があります。

カスタマイゼーション オブジェクトを作成し、そのオブジェクトで使用する変換テーブルを識別し、グループ ポリシーまたはユーザーのカスタマイズを指定するまで、AnyConnect 変換ドメインを除いて、変換テーブルは機能せず、メッセージは変換されません。AnyConnect ドメインの変換テーブルに対する変更は、ただちに セキュアクライアント ユーザーに表示されます。詳細については、**import webvpn customization** コマンドを参照してください。

例

次に、セキュアクライアントユーザーインターフェイスに影響を与える変換ドメインの変換テーブルをインポートし、変換テーブルが中国語用であることを指定する例を示します。**show import webvpn translation-table** コマンドは、新しいオブジェクトを表示します。

```
ciscoasa# import webvpn translation-table anyconnect language zh
tftp://209.165.200.225/anyconnect
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
ciscoasa# show import webvpn translation-table
Translation Tables' Templates:
customization
AnyConnect
CSD
PortForwarder
url-list
webvpn
Citrix-plugin
RPC-plugin
Telnet-SSH-plugin
VNC-plugin
Translation Tables:
zh AnyConnect
```

関連コマンド

コマンド	説明
export webvpn translation-table	変換テーブルをエクスポートします。
import webvpn customization	変換テーブルを参照するカスタマイゼーションオブジェクトをインポートします。
復元	フラッシュから変換テーブルを削除します。
show import webvpn translation-table	使用可能な変換テーブルテンプレートおよび変換テーブルを表示します。

import webvpn url-list

ASA のフラッシュデバイス上に URL リストをロードするには、特権 EXEC モードで **import webvpn url-list** コマンドを使用します。

import webvpn url-list *name URL*

構文の説明

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

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

import url-list コマンドを入力する前に、ASA インターフェイスで WebVPN が有効になっていることを確認します。確認するためには、**show running-config** コマンドを入力します。

URL リストをインポートすると、ASA で次のことが実行されます。

- URL リストを URL から ASA ファイルシステム（disk0:/csco_config/url-lists）に *name on flash* = base 64*name* としてコピーします。
- ファイルに対して基本的な XML 構文チェックを実行します。構文が無効な場合、ASA はファイルを削除します。
- index.ini ファイルにレコード base 64*name* が含まれていることをチェックします。含まれていない場合、ASA は base 64*name* をファイルに追加します。
- *name* ファイルを RAMFS /csco_config/url-lists/ に ramfs name = *name* としてコピーします。

例

次に、*NewList.xml* という URL リストを URL 209.165.201.22/url-lists から ASA にインポートし、*ABCList* という名前を付ける例を示します。

```
ciscoasa# import webvpn url-list ABCList tftp://209.165.201.22/url-lists/NewList.xml
Accessing
tftp://209.165.201.22/url-lists/NewList.xml...!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Writing file disk0:/csco_config/97/ABClist...
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
329994 bytes copied in 5.350 secs (65998 bytes/sec)
```

関連コマンド

コマンド	説明
revert webvpn url-list	指定された URL リストを ASA のフラッシュデバイスから削除します。
show import webvpn url-list	ASA のフラッシュデバイスに存在する URL リストを一覧表示します。

import webvpn webcontent

リモートのクライアントレス SSL VPN ユーザーに表示されるコンテンツをフラッシュメモリにインポートするには、特権 EXEC モードで **import webvpn webcontent** コマンドを使用します。

import webvpn webcontent *destination url source url*

構文の説明

destination url	**The URL to export to**. 最大数は 255 文字です。
source url	コンテンツがある ASA のフラッシュメモリの URL。最大数は 64 文字です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

webcontent オプションでイン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ーに表示されます。この中には、クライアントレス ポータルに表示されるヘルプ コンテンツや、ユーザー画面をカスタマイズするカスタマイゼーション オブジェクトで使用されるロゴなどがあります。

パス /+CSCOE+/ で URL にインポートされるコンテンツは、認可されたユーザーにのみ表示されます。

パス /+CSCOU+/ で URL にインポートされるコンテンツは、不正なユーザーと認可されたユーザーの両方に表示されます。

たとえば、/+CSCOU+/logo.gif としてインポートした企業ロゴを、ポータル カスタマイゼーション オブジェクトに使用し、ログイン ページおよびポータル ページに表示できま

す。/+CSCOE+/logo.gif としてインポートした同じ logo.gif ファイルは、正常にログインしたリモート ユーザーにのみ表示されます。

さまざまなアプリケーション画面に表示されるヘルプ コンテンツは、特定の URL にインポートする必要があります。次の表に、標準のクライアントレス アプリケーション用に表示されるヘルプ コンテンツの URL および画面エリアを示します。

URL	クライアントレス画面エリア
/+CSCOE+/help/*language* /app-access-hlp.inc	Application Access
/+CSCOE+/help/*language* /file-access-hlp.inc	Browse Networks
/+CSCOE+/help/*language* /net_access_hlp.html	セキュアクライアント
/+CSCOE+/help/*language* /web-access-help.inc	Web Access

次の表に、任意のプラグイン クライアントレス アプリケーション用に表示されるヘルプ コンテンツの URL および画面エリアを示します。

URL	クライアントレス画面エリア
/+CSCOE+/help/*language* /ica-hlp.inc	MetaFrame Access
/+CSCOE+/help/*language* /rdp-hlp.inc	Terminal Servers
/+CSCOE+/help/*language* /ssh,telnet-hlp.inc	Telnet/SSH Servers
/+CSCOE+/help/*language* /vnc-hlp.inc	VNC Connections

URL パスの *language* エントリは、ヘルプ コンテンツ用に指定した言語の短縮形です。ASA は、ファイルを指定された言語に実際に変換するわけではなく、ファイルに言語の省略形のラベルを付けます。

例

次に、HTML ファイル *application_access_help.html* を 209.165.200.225 の TFTP サーバーからフラッシュ メモリ内の Application Access ヘルプ コンテンツを保管する URL にインポートする例を示します。URL には英語の省略形 *en* が含まれています。

```
ciscoasa# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

次に、HTML ファイル *application_access_help.html* を 209.165.200.225 の tftp サーバーからフラッシュ メモリ内の Application Access ヘルプ コンテンツを保管する URL にインポートする例を示します。URL には英語の省略形 *en* が含まれています。

```
ciscoasa# import webvpn webcontent /+CSCOE+/help/en/app-access-hlp.inc
tftp://209.165.200.225/application_access_help.html
!!!!* Web resource `+CSCOE+/help/en/ap-access-hlp.inc' was successfully initialized
ciscoasa#
```

関連コマンド

コマンド	説明
export webvpn webcontent	クライアントレスSSL VPNユーザー向けに以前にインポートしたコンテンツをエクスポートします。
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。

inspect a – inspect z

inspect ctiqbe

CTIQBEプロトコルインスペクションを有効にするには、クラス コンフィギュレーション モードで **inspect ctiqbe** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。インスペクションを無効にするには、このコマンドの **no** 形式を使用します。

inspect ctiqbe
no inspect ctiqbe

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加され、以前の **fixup** コマンドは置き換えられて廃止されました。

使用上のガイドライン

inspect ctiqbe コマンドは、NAT、PAT、および双方向 NAT をサポートしている CTIQBE プロトコルインスペクションを有効にします。有効にすると、Cisco IP SoftPhone と他の Cisco TAPI/JTAPI アプリケーションが Cisco CallManager と連動し、ASA を経由してコールセットアップを実行できるようになります。

Telephony Application Programming Interface（TAPI）および Java Telephony Application Programming Interface（JTAPI）は、多数の Cisco VoIP アプリケーションで使用されます。Computer Telephony Interface Quick Buffer Encoding（CTIQBE）は、 Cisco CallManager と通信するために Cisco TAPI Service Provider（TSP）によって使用されます。

CTIQBE アプリケーション インスペクションの使用時に適用される制限を次にまとめます。

- CTIQBE コールのステートフル フェールオーバーはサポートされていません。
- **debug ctiqbe** コマンドを使用すると、メッセージ送信が遅延することがあり、リアルタイム環境のパフォーマンスに影響が出る可能性があります。このデバッグまたはロギングを有効にし、ASA を介して Cisco IP SoftPhone でコールセットアップを完了できない場合は、

Cisco IP SoftPhone の動作するシステムで Cisco TSP 設定のタイムアウト値を増やしてください。

- CTIQBE アプリケーション インスペクションでは、複数の TCP パケットにフラグメント化された CTIQBE メッセージはサポートしていません。

次に、CTIQBEアプリケーションインスペクションを特定の事例で使用する際に、特別に注意が必要な事項をまとめます。

- 2 つの Cisco IP SoftPhone が異なる Cisco CallManager に登録されていて、各 CallManager が ASA の異なるインターフェイスに接続されている場合、これら2つの電話機間のコールは失敗します。
- Cisco IP SoftPhone よりも Cisco CallManager の方が高セキュリティ インターフェイス上に配置されている状態で、NAT または外部 NAT が Cisco CallManager IP アドレスに必要な場合、マッピングはスタティックである必要があります。Cisco IP SoftPhone では Cisco CallManager IP アドレスを PC 上の Cisco TSP コンフィギュレーションで明示的に指定する必要があるためです。
- PAT または外部 PAT を使用しているときに Cisco CallManager の IP アドレスを変換する場合、Cisco IP SoftPhone を正常に登録するためには、TCP ポート 2748 を PAT（インターフェイス）アドレスの同一ポートに対してスタティックにマッピングする必要があります。CTIQBE 受信ポート（TCP 2748）は固定されているため、Cisco CallManager、Cisco IP SoftPhone、または Cisco TSP では、ユーザーは設定できません。

シグナリングメッセージのインスペクション

シグナリングメッセージのインスペクションでは、多くの場合、 **inspect** ctiqbe コマンドでメディアエンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、手動のコンフィギュレーションを行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス コントロールと NAT ステートを準備するために使用されます。

これらの場所を特定するときに、 **inspect** ctiqbe コマンドはトンネル デフォルト ゲートウェイ ルートを使用しません。トンネルデフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPsec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect** ctiqbe コマンドが必要な場合は、トンネル デフォルト ゲートウェイ ルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次に、CTIQBE インスペクション エンジンをイネーブルにし、CTIQBE トラフィックをデフォルト ポート（2748）上で照合するクラスマップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
ciscoasa(config)# class-map ctiqbe-port
ciscoasa(config-cmap)# match port tcp eq 2748
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ctiqbe_policy
```

```
ciscoasa(config-pmap)# class ctiqbe-port
ciscoasa(config-pmap-c)# inspect ctiqbe
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ctiqbe_policy interface outside
```

すべてのインターフェイスに対して CTIQBE インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
show conn	さまざまな接続タイプの接続状態を表示します。
show ctiqbe	ASA を介して確立されている CTIQBE セッション、および CTIQBE 検査エンジンで割り当てられたメディア接続に関する情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect dcerpc

エンドポイントマッパー宛ての DCERPC トラフィックのインスペクションをイネーブルにするには、クラス コンフィギュレーション モードで inspect dcerpc コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect dcerpc [*map_name*]
no inspect dceprc [*map_name*]

構文の説明

map_name	（オプション）DCERPC インスペクション マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

inspect dcerpc コマンドは、DCERPC プロトコルに対するアプリケーション インスペクションを有効または無効にします。

例

次の例は、DCERPC インスペクション ポリシー マップを定義し、DCERPC のピンホールのタイムアウトを設定する方法を示しています。

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# timeout pinhole 0:10:00
ciscoasa(config)# class-map dcerpc
ciscoasa(config-cmap)# match port tcp eq 135
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# class dcerpc
ciscoasa(config-pmap-c)# inspect dcerpc dcerpc_map
ciscoasa(config)# service-policy global-policy global
```

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。
policy-map type inspect	インスペクション 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。
timeout pinhole	DCERPC ピンホールのタイムアウトを設定して、グローバル システムのピンホール タイムアウトを上書きします。

inspect diameter

Diameterアプリケーションインスペクションを有効にするには、クラス コンフィギュレーション モードで **diameter** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect diameter [*diameter_map*] [**tls-proxy** *proxy_name*]
no inspect diameter [*diameter_map*] [**tls-proxy** *proxy_name*]

（注） Diameter インスペクションには Carrier ライセンスが必要です。

構文の説明

diameter_map	Diameter ポリシー マップ名を指定します。
tls-proxy *proxy_name*	暗号化された接続を検査できるように、指定されたTLSプロキシを使用します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。
9.6(1)	**tls-proxy** キーワードが追加されました。

使用上のガイドライン

Diameter は、LTE（Long Term Evolution）および IMS（IP Multimedia Subsystem）用の EPS（Evolved Packet System）などの次世代モバイルと固定電気通信ネットワークで使用される認証、認可、およびアカウンティング（AAA）プロトコルです。RADIUS や TACACS がこれらのネットワークで Diameter に置き換えられます。

Diameter はトランスポート層として TCP および SCTP を使用し、TCP/TLS および SCTP/DTLS によって通信を保護します。また、オプションで、データ オブジェクトの暗号化も提供できます。Diameter の詳細については、RFC 6733 を参照してください。

Diameterアプリケーションは、課金のユーザーアクセス、サービス認証、QoS、およびレートの決定といったサービス管理タスクを実行します。Diameter アプリケーションは LTE アーキテクチャのさまざまなコントロール プレーン インターフェイスで使用されますが、ASA は、次のインターフェイスについてのみ、Diameter コマンド コードおよび属性値ペア（AVP）を検査します。

- S6a：モビリティ マネージメント エンティティ（MME）-ホーム サブスクリプション サービス（HSS）
- S9：PDN ゲートウェイ（PDG）- 3GPP AAA プロキシ/サーバー
- Rx：ポリシー/課金ルール機能（PCRF） - コール セッション制御機能（CSCF）

Diameterインスペクションでは、Diameterエンドポイント用にピンホールを開いて通信を可能にします。このインスペクションは、3GPP バージョン 12 をサポートし、RFC 6733 に準拠しています。TCP/TLS（インスペクションをイネーブルにするときに TLS を指定する場合）および SCTP には使用できますが、SCTP/DTLS には使用できません。SCTP Diameter セッションにセキュリティを提供するには IPsec を使用します。

パケットや接続のドロップまたはロギングなどの特別なアクションを適用するために、オプションで、Diameter インスペクション ポリシー マップを使用し、アプリケーション ID、コマンド コード、および AVP に基づいてトラフィックをフィルタリングできます。新規に登録された Diameter アプリケーション用のカスタム AVP を作成できます。フィルタリングにより、ネットワークで許可するトラフィックをきめ細かく設定できます。

（注） 他のインターフェイス上で動作するアプリケーションに対する Diameter メッセージはデフォルトで許可され、渡されます。ただし、アプリケーション ID によってこれらのアプリケーションを破棄するための Diameter インスペクション ポリシー マップを設定できますが、これらのサポートされていないアプリケーションに対してコマンド コードまたは AVP に基づいてアクションを指定することはできません。

例

次に、Diameterインスペクションをデフォルト ポート（TCP/3868、TCP/5868、および SCTP/3868）にグローバルに適用する例を示します。

```
ciscoasa(config)# policy-map global_policy

ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect diameter
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy global_policy global
```

関連コマンド

コマンド	説明
class	セキュリティ アクションを適用するトラフィック クラスを定義します。
inspect sctp	SCTP インスペクションをイネーブルにします。
policy-map type inspect	インスペクション ポリシー マップを作成します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show service-policy inspect diameter	inspect diameter ポリシーのステータスおよび統計情報を表示します。
tls-proxy	TLS プロキシを定義します。

inspect dns

無効になっている DNS インスペクションを有効にする、または DNS インスペクションパラメータを設定するには、クラス コンフィギュレーション モードで **inspect dns** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。DNS インスペクションを無効にするには、このコマンドの **no** 形式を使用します。

inspect dns [*map_name*] [**dynamic-filter-snoop**]
no inspect dns [*map_name*] [**dynamic-filter-snoop**]

構文の説明

dynamic-filter-snoop	（オプション）ダイナミック フィルタ スヌーピングをイネーブルにします。これはボットネット トラフィック フィルタでのみ使用されます。ボットネット トラフィック フィルタリングを使用する場合に限り、このキーワードを指定します。DNS スヌーピングは、外部 DNS 要求が送信されるインターフェイスでだけイネーブルにすることを推奨します。すべての UDP DNS トラフィック（内部 DNS サーバーへの送信トラフィックを含む）に対して DNS スヌーピングをイネーブルにすると、ASA で不要な負荷が発生します。
map_name	（任意）DNS マップの名前を指定します。

コマンド 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。ボットネット トラフィック フィルタのスヌーピングは、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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。
7.2(1)	このコマンドは、DNSインスペクションの追加パラメータを設定できるように変更されました。

リリース	変更内容
8.2(1)	**dynamic-filter-snoop** キーワードが追加されました。

使用上のガイドライン

DNS インスペクションは、次のような preset_dns_map インスペクション クラス マップを使用して、デフォルトでイネーブルになっています。

- 最大 DNS メッセージ長は、512 バイトです。
- 最大クライアント DNS メッセージ長は、リソース レコードに一致するように自動的に設定されます。
- DNS ガードはイネーブルになり、ASA によって DNS 応答が転送されるとすぐに、ASA は DNS クエリに関連付けられている DNS セッションを切断します。ASA はまた、メッセージ交換をモニターして DNS 応答の ID が DNS クエリの ID と一致することを確認します。
- NAT の設定に基づく DNS レコードの変換はイネーブルです。
- プロトコルの強制はイネーブルであり、DNS メッセージ形式チェックが行われます。ドメイン名の長さが 255 文字以下、ラベルの長さが 63 文字、圧縮、ループ ポインタのチェックなどです。

DNS リライトに必要な DNS インスペクション

DNS インスペクションがイネーブルであるとき、DNS リライトは、任意のインターフェイスから送信された DNS メッセージの NAT を完全にサポートします。

内部のネットワーク上のクライアントが、外部インターフェイス上の DNS サーバーから送信される内部アドレスの DNS 解決を要求した場合、DNS A レコードは正しく変換されます。DNS インスペクション エンジンがディセーブルである場合、A レコードは変換されません。

DNS リライトは、次の 2 つの機能を実行します。

- DNS クライアントがプライベート インターフェイスにある場合、DNS 応答のパブリック アドレス（ルーティング可能なアドレスまたは「マッピング」アドレス）をプライベート アドレス（「実際の」アドレス）に変換します。
- DNS クライアントがパブリック インターフェイスにある場合、プライベート アドレスをパブリック アドレスに変換します。

DNS インスペクションがイネーブルであれば、NAT の DNS リライトを設定できます。

例

次に、DNS メッセージの最大長を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns dns-inspect
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 1024
```

次に、すべての UDP DNS トラフィック用のクラス マップを作成し、デフォルトの DNS インスペクション ポリシー マップで DNS インスペクションおよびボットネット

トラフィック フィルタのスヌーピングをイネーブルにして、外部インターフェイスに適用する例を示します。

```
ciscoasa(config)# class-map dynamic-filter_snoop_class
ciscoasa(config-cmap)# match port udp eq domain
ciscoasa(config-cmap)# policy-map dynamic-filter_snoop_policy
ciscoasa(config-pmap)# class dynamic-filter_snoop_class
ciscoasa(config-pmap-c)# inspect dns preset_dns_map dynamic-filter-snoop
ciscoasa(config-pmap-c)# service-policy dynamic-filter_snoop_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
policy-map type inspect	インスペクション ポリシー マップを作成します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect esmtp

SMTP/ESMTP アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect esmtp** コマンドを使用します。クラス コンフィギュレーション モードは、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可能です。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。

inspect esmtp [*map_name*]
no inspect esmtp [*map_name*]

構文の説明

map_name	（任意）ESMTPマップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

ESMTP インスペクションは、_default_esmtp_map インスペクション ポリシー マップを使用して、デフォルトで有効になります。

- サーバー バナーはマスクされます。
- 暗号化されたトラフィックが検査されます。
- 送信側と受信側のアドレスの特殊文字は認識されず、アクションは実行されません。
- コマンド行の長さが 512 より大きい接続は、ドロップされてログに記録されます。
- 受信者が 100 より多い接続は、ドロップされてログに記録されます。
- 本文の長さが 998 バイトより大きいメッセージはログに記録されます。

- ヘッダー行の長さが 998 より大きい接続は、ドロップされてログに記録されます。
- MIME ファイル名が 255 文字より長いメッセージは、ドロップされてログに記録されます。
- 「others」に一致する EHLO 応答パラメータはマスクされます。

ESMTP アプリケーション インスペクションを使用すると、ASA を通過できる SMTP コマンドの種類を制限し、モニタリング機能を追加することによって、SMTP ベースの攻撃に対する保護を強化できます。

ESMTP は SMTP プロトコルの拡張で、ほとんどの観点で SMTP に似ています。便宜上、このマニュアルでは、SMTP という用語を SMTP と ESMTP の両方に使用します。拡張 SMTP に対するアプリケーション インスペクション処理は、SMTP アプリケーション インスペクションに似ており、SMTP セッションのサポートが含まれています。拡張 SMTP セッションで使用するほとんどのコマンドは、SMTP セッションで使用するコマンドと同じですが、ESMTP セッションの方が大幅に高速で、配信ステータス通知など信頼性およびセキュリティに関するオプションが増えています。

拡張 SMTP アプリケーション インスペクションでは、AUTH、EHLO、ETRN、HELP、SAML、SEND、SOML、STARTTLS、および VRFY を含む拡張 SMTP コマンドに対するサポートが追加されています。ASA は、7 つの RFC 821 コマンド（DATA、HELO、MAIL、NOOP、QUIT、RCPT、RSET）をサポートするとともに、合計 15 個の SMTP コマンドをサポートします。

ATRN、ONEX、VERB、CHUNKING などのその他の拡張 SMTP コマンドおよびプライベート拡張はサポートされていません。サポートされないコマンドは、内部サーバーにより拒否される X に変換されます。この結果は、「500 Command unknown: 'XXX'」のようなメッセージで表示されます。不完全なコマンドは、破棄されます。

ESMTP インスペクション エンジンは、文字「2」、「0」、「0」を除くサーバーの SMTP バナーの文字をアスタリスクに変更します。復帰（CR）、および改行（LF）は無視されます。

SMTP インスペクションをイネーブルにする場合、次のルールに従わないと、対話型の SMTP に使用する Telnet セッションが停止することがあります。SMTP コマンドの長さは 4 文字以上にする必要があります。復帰と改行で終了する必要があります。次の応答を発行する前に現在の応答を待機する必要があります。

SMTP サーバーは、数値の応答コード、およびオプションの可読文字列でクライアント要求に応答します。SMTP アプリケーション インスペクションは、ユーザーが使用できるコマンドとサーバーが返送するメッセージを制御し、その数を減らします。SMTP インスペクションは、次の 3 つの主要なタスクを実行します。

- SMTP 要求を 7 つの基本 SMTP コマンドと 8 つの拡張コマンドに制限します。
- SMTP コマンド応答シーケンスをモニターします。
- 監査証跡の生成：メールアドレス内に埋め込まれている無効な文字が置き換えられたときに、監査レコード 108002 を生成します。詳細については、RFC 821 を参照してください。

SMTP インスペクションでは、次の異常な署名がないかどうか、コマンドと応答のシーケンスをモニターします。

- 切り捨てられたコマンド
- 不正なコマンド終端（<CR><LR> で終了していない）
- MAIL コマンドと RCPT コマンドでは、メールの送信者と受信者が指定されます。異常な文字がないか、メール アドレスがスキャンされます。縦棒（|）は削除され（ブランクに変更されます）、「<」および「>」はメール アドレスを定義する場合にのみ許可されます（「>」より前に「<」がある必要があります）。
- SMTP サーバーによる不意の移行
- 未知のコマンドの場合、ASA はパケット内のすべての文字を X に変更します。この場合、サーバーがクライアントに対してエラーコードを生成します。パケット内が変更されるため、TCP チェックサムの再計算または調整が必要になります。
- TCP ストリーム編集
- コマンド パイプライン

例

次に、SMTP インスペクション エンジンをイネーブルにし、SMTP トラフィックをデフォルト ポート（25）上で照合するクラスマップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
ciscoasa(config)# class-map smtp-port
ciscoasa(config-cmap)# match port tcp eq 25
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map smtp_policy

ciscoasa(config-pmap)# class smtp-port
ciscoasa(config-pmap-c)# inspect esmtp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy smtp_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
policy-map type inspect	インスペクション ポリシー マップを作成します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	SMTP を含む各種接続タイプの接続状態を表示します。

inspect ftp

ポートをFTPインスペクション用に設定したり、拡張インスペクションを有効にしたりするには、クラス コンフィギュレーション モードで **inspect ftp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect ftp [**strict** [*map_name*]]
no inspect ftp [**strict** [*map_name*]]

構文の説明

map_name	FTP インスペクション マップの名前。
strict	（任意）FTP トラフィックの拡張インスペクションをイネーブルにして、RFC 標準への準拠を強制します。

コマンド デフォルト

FTP インスペクションはデフォルトで有効になり、ASA は FTP ポート 21 をリッスンします。

FTP を上位のポートに移動する場合には注意が必要です。たとえば、FTP ポートを 2021 に設定した場合、ポート 2021 に対して開始されるすべての接続で、データ ペイロードが FTP コマンドとして解釈されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。*map_name* オプションが追加されました。

使用上のガイドライン

FTP アプリケーション インスペクションは、FTP セッションを検査し、次の 4 つのタスクを実行します。

- ダイナミックな二次的データ接続の準備
- FTP コマンド応答シーケンスの追跡
- 監査証跡の生成

- 埋め込み IP アドレスの変換

FTP アプリケーション インスペクションによって、FTP データ転送用にセカンダリ チャネルが用意されます。これらのチャネルのポートは、PORT コマンドまたは PASV コマンドを使用してネゴシエートされます。セカンダリ チャネルは、ファイル アップロード、ファイル ダウンロード、またはディレクトリ リスト イベントへの応答で割り当てられます。

（注） インスペクションはFTPコントロール接続のポートだけに適用し、データ接続のポートには適用しないでください。ASAのステートフル検査エンジンは、必要に応じて動的にデータ接続を準備します。

no inspect ftp コマンドを使用して、FTP 検査エンジンを有効にすると、発信ユーザーはパッシブモードだけで接続を開始でき、着信 FTP はすべて無効になります。

厳密な FTP

厳密な FTP を使用すると、Web ブラウザが FTP 要求内の埋め込みコマンドを送信できなくなるため、保護されたネットワークのセキュリティが強化されます。厳密なFTPを有効にするには、**inspect ftp** コマンドに strict オプションを含めます。

厳密な FTP を使用するときは、オプションで FTP インスペクション ポリシー マップを指定して、ASA を通過することが許可されない FTP コマンドを指定できます。

インターフェイスに対して **strict** オプションを有効にすると、FTP インスペクションによって次の動作が適用されます。

- FTP コマンドが確認応答されてからでないと、ASA は新しいコマンドを許可しません。
- ASA は、埋め込みコマンドを送信する接続をドロップします。
- 227 コマンドと PORT コマンドが、エラー文字列に表示されないように確認されます。

注意 **strict** オプションを使用すると、FTP RFC に厳密に準拠していない FTP クライアントは失敗することがあります。

strictオプションが有効になっている場合、次の異常なアクティビティを確認するために各FTPコマンドと応答シーケンスが追跡されます。

- 切り捨てされたコマンド：PORT コマンドおよび PASV 応答コマンドのカンマの数が 5 であるかどうかが確認されます。カンマの数が 5 でない場合は、PORT コマンドが切り捨てられていると見なされ、TCP 接続は閉じられます。
- 不正なコマンド：FTP コマンドが、RFC の要求どおりに <CR><LF> 文字で終了しているかどうか確認されます。終了していない場合は、接続が閉じられます。

- RETR コマンドと STOR コマンドのサイズ：これらが、固定の定数と比較チェックされます。サイズが定数より大きい場合は、エラーメッセージがロギングされ、接続が閉じられます。
- コマンドスプーフィング：PORT コマンドは、常にクライアントから送信されます。PORT コマンドがサーバーから送信される場合、TCP 接続は拒否されます。
- 応答スプーフィング：PASV 応答コマンド（227）は、常にサーバーから送信されます。PASV 応答コマンドがクライアントから送信される場合、TCP 接続は拒否されます。これにより、ユーザーが「227 xxxxx a1, a2, a3, a4, p1, p2」を実行する場合のセキュリティ ホールが予防できます。
- TCP ストリーム編集：ASA は、TCP ストリーム編集を検出した場合に接続が閉じられます。
- 無効ポート ネゴシエーション：ネゴシエートされたダイナミック ポート値が、1024 未満であるかどうかが調べられます。1 ～ 1024 の範囲のポート番号は、予約済み接続用に指定されているため、ネゴシエートされたポートがこの範囲内であった場合、TCP 接続は解放されます。
- コマンド パイプライン：PORT コマンドと PASV 応答コマンド内のポート番号の後に続く文字数が、定数の 8 と比べられます。8 より大きい場合は、TCP 接続が閉じられます。
- ASA は SYST コマンドに対する FTP サーバーの応答を連続した X で置き換えて、サーバーのシステムタイプが FTP クライアントに知られないようにします。このデフォルトの動作を無効にするには、FTP マップで、**no mask-syst-reply** コマンドを使用します。

FTP ログメッセージ

FTP アプリケーション インスペクションでは、次のログ メッセージが生成されます。

- 取得またはアップロードされたファイルごとに監査レコード 302002 が生成されます。
- メモリ不足によって動的なセカンダリ チャネルの準備に失敗した場合は、監査レコード 201005 が生成されます。

例

ユーザー名とパスワードを送信する前に、すべての FTP ユーザーに接続時バナーが表示されます。デフォルトでは、このバナーには、ハッカーがシステムの弱点を特定するのに役立つバージョン情報が含まれます。このバナーをマスクする方法を次に示します。

```
ciscoasa(config)# policy-map type inspect ftp mymap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
ciscoasa(config-pmap-p)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# class-map match-all ftp-traffic
ciscoasa(config-cmap)# match port tcp eq ftp
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ftp-policy
ciscoasa(config-pmap)# class ftp-traffic
```

```
ciscoasa(config-pmap-c)# inspect ftp strict mymap
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy ftp-policy interface inside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
mask-syst-reply	FTP サーバー応答をクライアントに対して非表示にします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
policy-map type inspect	インスペクション ポリシー マップを作成します。
request-command deny	不許可にする FTP コマンドを指定します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect gtp

GTP インスペクションを有効にするには、クラス コンフィギュレーション モードで **inspect gtp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。GTP インスペクションを無効にするには、このコマンドの **no** 形式を使用します。

inspect gtp [*map_name*]
no inspect gtp [*map_name*]

（注） GTP インスペクションには GTP/GPRS または Carrier ライセンスが必要です。

構文の説明

map_name （オプション）GTP インスペクション ポリシー マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(1)	GTPv2 および IPv6 アドレスのサポートが追加されました。

使用上のガイドライン

GPRS トンネリング プロトコルは、General Packet Radio Service（GPRS）トラフィック用に GSM、UMTS および LTE ネットワークで使用されます。GTP は、トンネル制御および管理プロトコルを提供します。このプロトコルによるトンネルの作成、変更、および削除により、モバイル ステーションに GPRS ネットワーク アクセスが提供されます。GTP は、ユーザー データ パケットの伝送にもトンネリング メカニズムを使用します。サービス プロバイダー ネットワークは、GTP を使用して、エンドポイント間の GPRS バックボーンを介してマルチプロトコル パケットをトンネリングします。

GTPインスペクションはデフォルトではイネーブルになっていません。ただし、ユーザー自身のインスペクションマップを指定せずにイネーブルにすると、次の処理を行うデフォルトマップが使用されます。マップを設定する必要があるのは、異なる値が必要な場合のみです。

- エラーは許可されません。
- 要求の最大数は 200 です。
- トンネルの最大数は 500 です。
- GSN/エンドポイント タイムアウトは 30 分です。
- PDP コンテキストのタイムアウトは 30 分です。GTPv2 では、これはベアラ- コンテキスト タイムアウトです。
- 要求のタイムアウトは 1 分です。
- シグナリング タイムアウトは 30 分です。
- トンネリングのタイムアウトは 1 時間です。
- T3 応答タイムアウトは 20 秒です。
- 未知のメッセージ ID はドロップされ、ログに記録されます。この動作は、3GPP が S5S8 インターフェースについて定義するメッセージに制限されます。他の GPRS インターフェイスについて定義されたメッセージは、最小限の検査によって許可される場合があります。

policy-map type inspect gtp コマンドを使用して GTP のパラメータを定義します。GTP マップを定義した後、**inspect gtp** コマンドを使用してマップを有効にします。次に、**class-map**、**policy-map**、**service-policy** の各コマンドを使用して、トラフィックのクラス定義、inspect コマンドのクラスへの適用、1 つ以上のインターフェイスへのポリシー適用を定義します。

GTP の既知のポートは UDP 3386、2123、および 2152 です。

シグナリングメッセージのインスペクション

シグナリングメッセージのインスペクションでは、多くの場合、**inspect gtp** コマンドでメディアエンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、手動のコンフィギュレーションを行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス コントロールと NAT ステートを準備するために使用されます。

これらの場所を特定するときに、**inspect gtp** コマンドではトンネル デフォルト ゲートウェイのルートを使用しません。**not** トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPsec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect gtp** コマンドが必要な場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次の例は、ネットワークのトンネル数を制限する方法を示しています。

```
ciscoasa(config)# policy-map type inspect gtp
 gmap

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# tunnel-limit 3000

ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default

ciscoasa(config-pmap-c)# inspect gtp gmap

ciscoasa(config)# service-policy global_policy global
```

関連コマンド

コマンド	説明
class	セキュリティ アクションを適用するトラフィック クラスを定義します。
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
policy-map type inspect	インスペクション ポリシー マップを作成します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show service-policy inspect gtp	inspect gtp ポリシーのステータスおよび統計情報を表示します。

inspect h323

H.323 アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect h323** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect h323 { **h225** | **ras** } [*map_name*]
no inspect h323 { **h225** | **ras** } [*map_name*]

構文の説明

h225	H.225 シグナリング インスペクションをイネーブルにします。
map_name	（任意）H.323 マップの名前。
ras	RAS インスペクションをイネーブルにします。

コマンド デフォルト

デフォルトのポート割り当ては次のとおりです。

- h323 h225 1720
- h323 ras 1718 ～ 1719

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

inspect h323 コマンドは、Cisco CallManager や VocalTec Gatekeeper などの H.323 に準拠したアプリケーションに対するサポートを提供します。H.323 は国際電気通信連合（ITU）で定義されている、LAN を介したマルチメディア会議用のプロトコル スイートです。ASA では、H.323 v3 機能の同一コールシグナリングチャネルでの複数コールを含め、バージョン 6 までの H.323 をサポートしています。

H.323 インスペクションを有効にした場合、ASA は、H.323 バージョン 3 で追加された同一コールシグナリングチャネル機能での複数コールをサポートします。この機能によってセットアップ時間が短縮され、ASA でのポート使用が減少します。

H.323 インスペクションの 2 つの主要機能は次のとおりです。

- H.225 と H.245 の両メッセージ内に埋め込まれている必要な IPv4 アドレスを NAT 処理します。H.323 メッセージは PER 符号化形式で符号化されているため、ASA では ASN.1 デコーダを使用して H.323 メッセージを復号化します。
- ネゴシエートされた H.245 と RTP/RTCP 接続をダイナミックに割り当てます。

シグナリングメッセージのインスペクション

シグナリングメッセージのインスペクションでは、多くの場合、 **inspect h323** コマンドでメディアエンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、手動のコンフィギュレーションを行わずに、メディア トラフィックがファイアウォールをトランスペアレントに通過できるよう、アクセス コントロールと NAT ステートを準備するために使用されます。

これらの場所を特定するときに、 **inspect h323** コマンドではトンネル デフォルト ゲートウェイのルートを使用しません。**not** トンネルデフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPsec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect h323** コマンドが必要な場合は、トンネルデフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次に、H.323 インスペクション エンジンをイネーブルにし、H.323 トラフィックをデフォルト ポート（1720）上で照合するクラス マップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
ciscoasa(config)# class-map h323-port
ciscoasa(config-cmap)# match port tcp eq 1720
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map h323_policy

ciscoasa(config-pmap)# class h323-port
ciscoasa(config-pmap-c)# inspect h323
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy h323_policy interface outside
```

関連コマンド

コマンド	説明
policy-map type inspect	インスペクション ポリシー マップを作成します。
show h225	ASA 間で確立された H.225 セッションの情報を表示します。

コマンド	説明
show h245	スロースタートを使用しているエンドポイントによってASA間で確立された H.245 セッションの情報を表示します。
show h323 ras	ASA 間で確立された H.323 RAS セッションの情報を表示します。
timeout {**h225** | **h323**}	H.225 シグナリング接続または H.323 制御接続が終了するまでのアイドル時間を設定します。

inspect http

HTTP アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect http command** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect http [*map_name*]
no inspect http [*map_name*]

構文の説明

map_name （オプション）HTTP インスペクション マップの名前。

コマンド デフォルト

HTTP のデフォルト ポートは 80 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

ヒント アプリケーションおよび URL のフィルタリングを実行するサービス モジュールをインストールできます。これには、ASA CX や ASA FirePOWER などの HTTP インスペクションが含まれます。ASA 上で実行される HTTP インスペクションは、これらのモジュールと互換性がありません。HTTP インスペクション ポリシー マップを使用して ASA 上で手作業による設定を試みるより、専用のモジュールを使用してアプリケーション フィルタリングを設定する方がはるかに簡単であることに注意してください。

HTTP インスペクション エンジンを使用して、HTTP トラフィックに関係する特定の攻撃やその他の脅威から保護します。

HTTP アプリケーション インスペクションで HTTP のヘッダーと本文をスキャンし、さまざまなデータ チェックができます。これらのチェックで、HTTP 構築、コンテンツ タイプ、トンネル プロトコル、メッセージ プロトコルなどがセキュリティ アプライアンスを通過することを防止します。

拡張 HTTP インスペクション機能はアプリケーション ファイアウォールとも呼ばれ、HTTP インスペクション ポリシーマップを設定するときに使用できます。これによって、攻撃者がネットワーク セキュリティ ポリシーに従わない HTTP メッセージを使用できないようにします。

HTTP アプリケーション インスペクションでトンネル アプリケーションと ASCII 以外の文字を含む HTTP 要求や応答をブロックして、悪意のあるコンテンツが Web サーバに到達することを防ぎます。HTTP 要求や応答ヘッダーのさまざまな要素のサイズ制限、URL のブロッキング、HTTP サーバ ヘッダー タイプのスプーフィングもサポートされています。

拡張 HTTP インスペクションは、すべての HTTP メッセージについて次の点を確認します。

- RFC 2616 への準拠
- RFC で定義された方式だけを使用していること
- 追加の基準への準拠

例

この例では、任意のインターフェイスを通過して ASA に入るすべての HTTP 接続（ポート 80 の TCP トラフィック）が HTTP インスペクション対象として分類されます。このポリシーはグローバル ポリシーなので、インスペクションが発生するのは各インターフェイスにトラフィックが入ったときだけです。

```
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map http_traffic_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# inspect http
ciscoasa(config)# service-policy http_traffic_policy global
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
policy-map type inspect	インスペクション ポリシー マップを作成します。

inspect icmp

ICMP 検査エンジンを設定するには、クラス コンフィギュレーション モードで **inspect icmp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect icmp
no inspect icmp

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

ICMP インスペクション エンジンを使用すると、TCP や UDP トラフィックのように ICMP トラフィックを検査できます。ICMP インスペクション エンジンを使用しない場合は、ACL で ICMP が ASA を通過するのを禁止することを推奨します。ステートフル インスペクションを実行しないと、ICMP がネットワーク攻撃に利用される可能性があります。ICMP インスペクション エンジンにより、それぞれの要求に対して 1 つの応答しか返されなくなり、正確なシーケンス番号が設定されるようになります。

ICMP インスペクションがディセーブルの場合（デフォルト設定）、セキュリティの低いインターフェイスからセキュリティの高いインターフェイスへの ICMP エコー応答メッセージは、ICMP エコー要求への応答であっても拒否されます。

例

次の例に示すように、ICMP アプリケーション インスペクション エンジンをイネーブルにします。この例では、ICMP プロトコル ID（IPv4 の場合は 1、IPv6 の場合は 58）を使用して ICMP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに

対して ICMP インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy

ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
icmp	ASA インターフェイスが終端となる ICMP トラフィックのアクセスルールを設定します。
policy-map	セキュリティ アクションを 1 つ以上のトラフィック クラスに関連付けるポリシーを定義します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect icmp error

ICMP エラーメッセージに対してアプリケーション インスペクションを有効にするには、クラス コンフィギュレーション モードで **inspect icmp** error コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect icmp error
no inspect icmp error

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

ICMP エラー インスペクションをイネーブルにすると、ASA は NAT の設定に基づいて、ICMP エラー メッセージを送信する中間ホップ用の変換セッションを作成します。ASA は、変換後の IP アドレスでパケットを上書きします。

ディセーブルの場合、ASA は、ICMP エラー メッセージを生成する中間ノード用の変換セッションを作成しません。内部ホストと ASA の間にある中間ノードによって生成された ICMP エラーメッセージは、NAT リソースをそれ以上消費することなく、外部ホストに到達します。外部ホストが traceroute コマンドを使用して ASA の内部にある宛先までのホップをトレースする場合、これは適切ではありません。ASA が中間ホップを変換しない場合、すべての中間ホップは、マッピングされた宛先 IP アドレスとともに表示されます。

ICMP ペイロードがスキャンされて、元のパケットから 5 つのタプルが取得されます。取得した 5 つのタプルを使用してルックアップを実行し、クライアントの元のアドレスを判別します。ICMP エラー インスペクション エンジンは、ICMP パケットに対して次の変更を加えます。

- IP ヘッダー内のマッピング IP を実際の IP（宛先アドレス）に変更し、IP チェックサムを修正する。
- ICMP パケットに変更を加えたため、ICMP ヘッダー内の ICMP チェックサムを修正する。
- ペイロードに次の変更を加える。
  - 元のパケットのマッピング IP を実際の IP に変更する。
  - 元のパケットのマッピング ポートを実際のポートに変更する。
  - 元のパケットの IP チェックサムを再計算する。

例

次に、ICMP エラー アプリケーション インスペクション エンジンをイネーブルにし、クラス マップを作成して、IPv4 の場合は 1、IPv6 の場合は 58 の ICMP プロトコル ID を使用して ICMP トラフィックを照合する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して ICMP エラーインスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map icmp-class
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map icmp_policy

ciscoasa(config-pmap)# class icmp-class
ciscoasa(config-pmap-c)# inspect icmp error
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy icmp_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
icmp	ASA インターフェイスが終端となる ICMP トラフィックのアクセスルールを設定します。
inspect icmp	ICMP インスペクション エンジンをイネーブルまたはディセーブルにします。
policy-map	セキュリティ アクションを 1 つ以上のトラフィック クラスに関連付けるポリシーを定義します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect ils

ILS アプリケーション インスペクションを有効にするには、クラス コンフィギュレーション モードで inspect **ils command** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect ils
no inspect ils

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

inspect ils コマンドは、LDAP を使用してディレクトリ情報を ILS サーバーと交換する Microsoft NetMeeting、SiteServer、および Active Directory 製品に対する NAT のサポートを提供します。

ASA は ILS に対して NAT をサポートします。NAT は、ILS または SiteServer Directory のエンドポイントの登録および検索で使用されます。LDAP データベースには IP アドレスだけが保存されるため、PAT はサポートされません。

LDAP サーバーが外部にある場合、内部ピアが外部 LDAP サーバーに登録された状態でローカルに通信できるように、検索応答に対して NAT を行うことを検討してください。このような検索応答では、最初に xlate が検索され、次に DNAT エントリが検索されて正しいアドレスが取得されます。これらの検索が両方とも失敗した場合、アドレスは変更されません。NAT 0（NAT なし）を使用していて、DNAT の相互作用を想定していないサイトの場合は、パフォーマンスを向上させるためにインスペクション エンジンをオフにすることをお勧めします。

ILS サーバーが ASA 境界の内部にある場合は、さらに設定が必要なことがあります。この場合、外部クライアントが指定されたポート（通常は TCP 389）の LDAP サーバーにアクセスするためのホールが必要となります。

ILS トラフィックはセカンダリ UDP チャネルだけで発生するため、TCP 接続は一定の間隔 TCP アクティビティがなければ切断されます。デフォルトでは、この間隔は 60 分です。この値は、**timeout** コマンドを使用して調整できます。

ILS/LDAP はクライアント/サーバー モデルに従っており、セッションは 1 つの TCP 接続で処理されます。クライアントのアクションに応じて、このようなセッションがいくつか作成されることがあります。

接続ネゴシエーション時間中、クライアントからサーバーに BIND PDU が送信されます。サーバーから成功を示す BIND RESPONSE を受信すると、ILS Directory に対する操作を実行するためのその他の操作メッセージ（ADD、DEL、SEARCH、MODIFY など）が交換される場合があります。ADD REQUEST PDU および SEARCH RESPONSE PDU には、NetMeeting セッションを確立するために H.323（SETUP および CONNECT メッセージ）によって使用される、NetMeeting ピアの IP アドレスが含まれている場合があります。Microsoft NetMeeting v2.X および v3.X は、ILS をサポートしています。

ILS インスペクションでは、次の操作が実行されます。

- BER 復号化機能を使用して LDAP REQUEST PDU/RESPONSE PDU を復号化する。
- LDAP パケットを解析する。
- IP アドレスを抽出する。
- 必要に応じて IP アドレスを変換する。
- BER 符号化機能を使用して、変換後のアドレスが含まれる PDU を符号化する。
- 新しく符号化された PDU を元の TCP パケットにコピーする。
- TCP チェックサムとシーケンス番号の増分を調整する。

ILS インスペクションには、次の制限事項があります。

- 照会要求や応答はサポートされません。
- 複数のディレクトリのユーザーは統合されません。
- 複数のディレクトリに複数の ID を持っている単一のユーザーは NAT には認識されません。

（注） H.225 コール シグナリング トラフィックが発生するのはセカンダリ UDP チャネル上のみのため、TCP の **timeout** コマンドにより指定された間隔が経過すると、TCP 接続は切断されます。デフォルトで、この間隔は 60 分に設定されています。

例

次の例に示すように、ILS インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（389）上の ILS トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべ

てのインターフェイスに対して ILS インスペクションを有効にするには、**interface outside** の代わりに、**global** パラメータを使用します。

```
ciscoasa(config)# class-map ils-port
ciscoasa(config-cmap)# match port tcp eq 389
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map ils_policy

ciscoasa(config-pmap)# class ils-port
ciscoasa(config-pmap-c)# inspect ils
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy ils_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
policy-map type inspect	インスペクション ポリシー マップを作成します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect im

インスタント メッセンジャー トラフィックのインスペクションをイネーブルにするには、クラス コンフィギュレーション モードで inspect im コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect im *map_name*
no inspect im *map_name*

構文の説明

map_name IM マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

inspect im コマンドは、IM プロトコルに対するアプリケーション インスペクションを有効または無効にします。インスタント メッセージ（IM）インスペクション エンジンを使用すると、IM のネットワーク使用を制御し、機密情報の漏洩、ワームの送信、および企業ネットワークへのその他の脅威を停止できます。

例

次の例は、IM インスペクション ポリシー マップを定義する方法を示しています。

```
ciscoasa(config)# regex loginname1 "user1\@example.com"
ciscoasa(config)# regex loginname2 "user2\@example.com"
ciscoasa(config)# regex loginname3 "user3\@example.com"
ciscoasa(config)# regex loginname4 "user4\@example.com"
ciscoasa(config)# regex yahoo_version_regex "1\.0"
ciscoasa(config)# regex gif_files ".*\.gif"
ciscoasa(config)# regex exe_files ".*\.exe"
ciscoasa(config)# class-map type regex match-any yahoo_src_login_name_regex
```

```
ciscoasa(config-cmap)# match regex loginname1
ciscoasa(config-cmap)# match regex loginname2
ciscoasa(config)# class-map type regex match-any yahoo_dst_login_name_regex
ciscoasa(config-cmap)# match regex loginname3
ciscoasa(config-cmap)# match regex loginname4
ciscoasa(config)# class-map type inspect im match-any yahoo_file_block_list
ciscoasa(config-cmap)# match filename regex gif_files
ciscoasa(config-cmap)# match filename regex exe_files

ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy
ciscoasa(config-cmap)# match login-name regex class yahoo_src_login_name_regex
ciscoasa(config-cmap)# match peer-login-name regex class yahoo_dst_login_name_regex
ciscoasa(config)# class-map type inspect im match-all yahoo_im_policy2
ciscoasa(config-cmap)# match version regex yahoo_version_regex
ciscoasa(config)# class-map im_inspect_class_map
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# policy-map type inspect im im_policy_all
ciscoasa(config-pmap)# class yahoo_file_block_list
ciscoasa(config-pmap-c)# match service file-transfer
ciscoasa(config-pmap)# class yahoo_im_policy
ciscoasa(config-pmap-c)# drop-connection
ciscoasa(config-pmap)# class yahoo_im_policy2
ciscoasa(config-pmap-c)# reset
ciscoasa(config)# policy-map global_policy_name
ciscoasa(config-pmap)# class im_inspect_class_map
ciscoasa(config-pmap-c)# inspect im im_policy_all
```

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。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
policy-map type inspect	インスペクション 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。
match protocol	インスペクションクラスマップまたはインスペクションポリシー マップで、特定の IM プロトコルを一致させます。

inspect ip-options

パケット内の IP オプションのインスペクションをイネーブルにするには、クラスまたはポリシー マップ タイプ インスペクション コンフィギュレーション モードで inspect ip-options コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect ip-options [*map_name*]
no inspect ip-options *map_name*

構文の説明

map_name	（任意）IP オプション マップの名前。

コマンド デフォルト

このコマンドは、グローバル ポリシーでデフォルトでイネーブルになっています。デフォルトのインスペクション マップでは、ルータ アラート オプションを持つパケットは許可されますが、その他のオプションを持つパケットはドロップされます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシーまたはクラス マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。サポートされているオプションは、**eool**、**nop**、および **router-alert** です。IP ヘッダーに EOOL、NOP、または RTRALT 以外のオプションが含まれている場合、ASA はそれらのオプションを許可するように設定されているかどうかに関係なく、そのパケットをドロップします。
9.5(1)	すべての IP オプションのサポートが追加されました。

使用上のガイドライン

パケットの IP ヘッダーには Options フィールドが含まれています。Options フィールドは、通常は IP オプションと呼ばれ、制御機能を提供します。特定の状況で必要になりますが、一般的な通信では必要ありません。具体的には、IP オプションにはタイムスタンプ、セキュリティ、

および特殊なルーティングの規定が含まれています。IPオプションの使用は任意であり、フィールドにはゼロまたは 1 つ以上の数のオプションを含めることができます。

IP オプション インスペクションを設定して、パケット ヘッダーの [IP Options] フィールドのコンテンツに基づいてどの IP パケットを許可するかについて制御できます。望ましくないオプションがあるパケットをドロップしたり、オプションをクリア（してパケットを許可）したり、変更なしでパケットを許可したりできます。

デフォルト以外の処理を行うには、IP オプション インスペクション ポリシー マップを作成し、**parameter** コマンドを入力して、さまざまなオプションに対して実行するアクションを指定します。次のオプションを検査できます。いずれの場合も、allowアクションはそのオプションを含むパケットを変更なしで許可し、clearアクションはパケットを許可しますがヘッダーからそのオプションを除去します。

マップからオプションを削除するには、このコマンドの **no** 形式を使用します。パケットに他の許可されているオプションまたはクリアされたオプションが含まれている場合でも、マップで指定されていないオプションを含むパケットはすべてドロップされます。

IP オプションおよび関連する RFC の参照のリストについては、IANA のページ（http://www.iana.org/assignments/ip-parameters/ip-parameters.xhtml）を参照してください。

- **default action** {**allow** | **clear**}：マップに明示的に含まれていないオプションに対するデフォルトアクションを設定します。許可またはクリアのデフォルト アクションを設定しないと、許可されていないオプションを持つパケットはドロップされます。
- **basic-security action** {**allow** | **clear**}：Security（SEC）オプションを許可またはクリアします。
- **commercial-security action** {**allow** | **clear**}：Commercial Security（CIPSO）オプションを許可またはクリアします。
- **eool action** {**allow** | **clear**}：End of Options List（EOOL）オプションを許可またはクリアします。ゼロ バイトが 1 つだけ含まれたこのオプションは、オプションのリストの終わりを示すために、すべてのオプションの末尾に表示されます。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。
- **exp-flow-control action** {**allow** | **clear**}：Experimental Flow Control（FINN）オプションを許可またはクリアします。
- **exp-measurement action** {**allow** | **clear**}：Experimental Measurement（ZSU）オプションを許可またはクリアします。
- **extended-security action** {**allow** | **clear**}：Extended Security（E-SEC）オプションを許可またはクリアします。
- **imi-traffic-descriptor action** {**allow** | **clear**}：IMI Traffic Descriptor（IMITD）オプションを許可またはクリアします。
- **nop action** {**allow** | **clear**}：No Operation オプションを許可またはクリアします。IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍数で

ある必要があります。すべてのオプションのビット数が32ビットの倍数でない場合、NOPオプションは、オプションを32ビット境界上に揃えるために、「内部パディング」として使用されます。

- **quick-start action** {**allow** | **clear**}：Quick-Start（QS）オプションを許可またはクリアします。
- **record-route action** {**allow** | **clear**}：Record Route（RR）オプションを許可またはクリアします。
- **router-alert action** {**allow** | **clear**}：Router Alert（RTRALT）オプションを許可またはクリアします。このオプションは、デフォルトのIPオプションインスペクションポリシーマップで許可されます。このオプションは、中継ルータに対し、パケットの宛先がそのルータでない場合でも、パケットのコンテンツを検査するよう通知します。このインスペクションは、RSVPを実装している場合に役に立ちます。同様のプロトコルは、パケットの配信パス上にあるルータでの比較的複雑な処理を必要とします。Router Alertオプションが含まれたRSVPパケットをドロップすると、VoIPの実装で問題が生じることがあります。
- **timestamp action** {**allow** | **clear**}：Time Stamp（TS）オプションを許可またはクリアします。
- {**0-255**} **action** {**allow** | **clear**}：オプションタイプ番号によって識別されるオプションを許可またはクリアします。番号は全オプションタイプのオクテット（コピー、クラス、およびオプション番号）で、オクテットのオプションの番号部分だけではありません。これらのオプションタイプは、実際のオプションに表示されない可能性があります。非標準オプションは、インターネットプロトコルRFC 791、http://tools.ietf.org/html/rfc791 で定義された予測されるタイプ/長さ/値の形式である必要があります。

例

次に、パケットヘッダーにEOOL、NOP、およびRTRALTオプションを含むパケットをASAが通過させるようにIPオプションインスペクションポリシーマップを定義する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow

ciscoasa(config-pmap-p)# nop action allow

ciscoasa(config-pmap-p)# router-alert action allow
```

次に、任意のIPオプションを持つパケットを許可する新しいデフォルトアクションを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# default action allow
```

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。

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。
policy-map type inspect	インスペクション ポリシーマップを作成します。

inspect ipsec-pass-thru

IPsec パススルー インスペクションをイネーブルにするには、クラス マップ コンフィギュレーション モードで inspect ipsec-pass-thru コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect ipsec-pass-thru [*map_name*]
no inspect ipsec-pass-thru [*map_name*]

構文の説明

map_name	（オプション）IPsec パススルー マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

inspect ipsec-pass-thru コマンドは、アプリケーション インスペクションを有効または無効にします。IPsec パススルー アプリケーション インスペクションによって、IKE UDP ポート 500 接続に関連付けられた ESP（IP プロトコル 50）トラフィックか AH（IP プロトコル 51）トラフィックまたはその両方の便利なトラバーサルが提供されます。このインスペクションは、冗長なアクセス リスト コンフィギュレーションを回避して ESP および AH トラフィックを許可し、タイムアウトと最大接続数を使用してセキュリティも確保します。

インスペクションのパラメータの定義に使用する特定のマップを識別するには、IPsec パススルー パラメータ マップを使用します。パラメータ コンフィギュレーションにアクセスするには、policy-map type inspect コマンドを使用します。このコンフィギュレーションで、ESP または AH トラフィックの制限を指定できます。パラメータ コンフィギュレーション モードでは、クライアントあたりの最大接続数と、アイドル タイムアウトを設定できます。

class-map、policy-map、および service-policy の各コマンドを使用してトラフィックのクラスを定義し、inspect コマンドをクラスに適用して、ポリシーを 1 つまたは複数のインターフェイスに適用します。定義したパラメータ マップは、inspect ipsec-pass-thru コマンドで使用されたときにイネーブルになります。

NAT および非 NAT トラフィックは許可されます。ただし、PAT はサポートされません。

（注） ASA 7.0(1) では、**inspect ipsec-pass-thru** コマンドでは ESP トラフィックの通過のみ許可されていました。最新バージョンで同じ動作を保持するために、**inspect ipsec-pass-thru** コマンドが引数なしで指定されている場合は、ESP を許可するデフォルトマップが作成され、付加されます。このマップは show running-config all コマンドの出力で確認できます。

例

次に、アクセス リストを使用して IKE トラフィックを識別し、IPsec パススルー パラメータ マップを定義して、ポリシーを定義し、外部インターフェイスにポリシーを適用する例を示します。

```
ciscoasa(config)# access-list ipsecpassthruacl permit udp any any eq 500
ciscoasa(config)# class-map ipsecpassthru-traffic
ciscoasa(config-cmap)# match access-list ipsecpassthruacl
ciscoasa(config)# policy-map type inspect ipsec-pass-thru iptmap
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 10 timeout 0:11:00
ciscoasa(config-pmap-p)# ah per-client-max 5 timeout 0:06:00
ciscoasa(config)# policy-map inspection_policy
ciscoasa(config-pmap)# class ipsecpassthru-traffic
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru iptmap
ciscoasa(config)# service-policy inspection_policy interface outside
```

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。
match protocol	インスペクション クラス マップまたはインスペクション ポリシー マップで、特定の IM プロトコルを一致させます。

inspect ipv6

IPv6 インスペクションをイネーブルにするには、クラス コンフィギュレーション モードで inspect ipv6 コマンドを使用します。クラス 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。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。

inspect ipv6 [*map_name*]
no inspect ipv6 [*map_name*]

構文の説明

map_name	（任意）IPv6 インスペクション ポリシーマップの名前。

コマンド デフォルト

IPv6 インスペクションは、デフォルトでディセーブルになっています。

IPv6 インスペクションをイネーブルにし、インスペクション ポリシーマップを指定しないと、デフォルトの IPv6 インスペクション ポリシー マップが使用され、次のアクションが実行されます。

- 既知の IPv6 拡張ヘッダーのみを許可します。準拠しないパケットはドロップされ、ログに記録されます。
- RFC 2460 仕様で定義されている IPv6 拡張ヘッダーの順序を適用します。準拠しないパケットはドロップされ、ログに記録されます。
- ルーティング タイプ ヘッダーを含むパケットをドロップします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 インスペクションを使用すると、拡張ヘッダーに基づいて IPv6 トラフィックを選択的にログに記録したりドロップしたりできます。さらに、IPv6 インスペクションでは、IPv6 パケット内の拡張ヘッダーのタイプと順序が RFC 2460 に準拠しているかどうかも確認できます。

例

次に、ヘッダーが hop-by-hop、destination-option、routing-address、および routing type 0 である IPv6 トラフィックをすべて削除する例を示します。

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop
 match header destination-option
  drop
 match header routing-address count gt 0
  drop
 match header routing-type eq 0
  drop
policy-map global_policy
 class class-default
  inspect ipv6 ipv6-pm
!
service-policy global_policy global
```

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。
match header	IPv6 インスペクション ポリシー マップで IPv6 ヘッダーを照合します。
policy-map type inspect ipv6	IPv6 のインスペクション ポリシー 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。
verify-header	IPv6 インスペクション パラメータを設定します。

inspect lisp

LISP インスペクションを有効にするには、クラス コンフィギュレーション モードで **inspect lisp** コマンドを使用します。クラス コンフィギュレーション モードにアクセスするには、**policy-map** コマンドを入力します。LISP インスペクションを無効にするには、このコマンドの **no** 形式を使用します。

inspect lisp [*inspect_map_name*]
no inspect lisp [*inspect_map_name*]

構文の説明

inspect_map_name	EID を制限する場合または LISP メッセージの事前共有キーを指定する必要がある場合は、LISP インスペクションマップ名を指定します（**policy-map type inspect lisp**）。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

ASAは、ファースト ホップ ルータと ITR または ETR の間で送信される EID 通知メッセージの LISP トラフィックを検査します。ASA は、EID とサイト ID を関連付ける EID テーブルを保持します。

クラスタ フロー モビリティの LISP インスペクションについて

ASA は、場所の変更について LISP トラフィックを検査し、シームレスなクラスタリング操作のためにこの情報を使用します。LISP の統合により、ASA クラスタ メンバーは、最初のホップ ルータと ETR または ITR との間で渡される LISP トラフィックを検査し、その後、フローの所有者を新しいサイトへ変更できます。

クラスタ フロー モビリティには複数の相互に関連する設定が含まれています。

1. （オプション）ホストまたはサーバーの IP アドレスに基づく検査される EID の限定：最初のホップ ルータは、ASA クラスタが関与していないホストまたはネットワークに関する EID 通知メッセージを送信することがあるため、EID をクラスタに関連するサーバーまたはネットワークのみに限定することができます。たとえば、クラスタが 2 つのサイトのみに関連しているが、LISP は 3 つのサイトで稼働している場合は、クラスタに関連する 2 つのサイトの EID のみを含めます。**policy-map type inspect lisp**、**allowed-eid,** および **validate-key** コマンドを参照してください。
2. LISP トラフィックのインスペクション：ASA は、最初のホップ ルータと ITR または ETR 間で送信された EID 通知メッセージに関して LISP トラフィックを検査します。ASA は EID とサイト ID を相関付ける EID テーブルを維持します。たとえば、最初のホップ ルータの送信元 IP アドレスと ITR または ETR の宛先アドレスをもつ LISP トラフィックを検査する必要があります。**inspect lisp** コマンドを参照してください。
3. 指定されたトラフィックでのフロー モビリティを有効にするサービス ポリシー：ビジネスクリティカルなトラフィックでフローモビリティを有効にする必要があります。たとえば、フロー モビリティを、HTTPS トラフィックのみに制限したり、特定のサーバとの間でやり取りされるトラフィックのみに制限したりできます。**cluster flow-mobility lisp** コマンドを参照してください。
4. サイト ID：ASA は各クラスタ ユニットのサイト ID を使用して、新しい所有者を判別します。**site-id** コマンドを参照してください。
5. フロー モビリティを有効にするクラスタレベルの設定：クラスタ レベルでもフロー モビリティを有効にする必要があります。このオン/オフの切り替えを使用することで、特定のクラスのトラフィックまたはアプリケーションに対してフローモビリティを簡単に有効または無効にできます。**flow-mobility lisp** コマンドを参照してください。

例

次に、192.168.50.89（内部）にある LISP ルータと 192.168.10.8（別の ASA インターフェイス上）にある ITR または ETR ルータの間の LISP トラフィック（UDP 4342）を検査する例を示します。

```
ciscoasa(config)# access-list LISP_ACL extended permit udp host 192.168.50.89 host
192.168.10.8 eq 4342
ciscoasa(config)# class-map LISP_CLASS
ciscoasa(config-cmap)# match access-list LISP_ACL
ciscoasa(config-cmap)# policy-map INSIDE_POLICY
ciscoasa(config-pmap)# class LISP_CLASS
ciscoasa(config-pmap-c)# inspect lisp LISP_EID_INSPECT
ciscoasa(config)# service-policy INSIDE_POLICY interface inside
```

関連コマンド

コマンド	説明
allowed-eids	IP アドレスに基づいて検査される EID を限定します。
clear cluster info flow-mobility counters	フロー モビリティ カウンタをクリアします。
clear lisp eid	ASA EID テーブルから EID を削除します。

コマンド	説明
cluster flow-mobility lisp	サービス ポリシーのフロー モビリティを有効にします。
flow-mobility lisp	クラスタのフロー モビリティを有効にします。
inspect lisp	LISP トラフィックを検査します。
policy-map type inspect lisp	LISP 検査をカスタマイズします。
site-id	クラスタ シャーシのサイト ID を設定します。
show asp table classify domain inspect-lisp	LISP 検査用の ASP テーブルを表示します。
show cluster info flow-mobility counters	フロー モビリティ カウンタを表示します。
show conn	LISP フロー モビリティの対象となるトラフィックを表示します。
show lisp eid	ASA EID テーブルを表示します。
show service-policy	サービス ポリシーを表示します。
validate-key	LISP メッセージを検証するための事前共有キーを入力します。

inspect m3ua

M3UA インスペクションを有効にするには、クラス コンフィギュレーション モードで **inspect m3ua** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。M3UA インスペクションを無効にするには、このコマンドの **no** 形式を使用します。

inspect m3ua [*map_name*]
no inspect m3ua [*map_name*]

（注） M3UA インスペクションには Carrier ライセンスが必要です。

構文の説明

map_name （オプション）M3UA インスペクション ポリシーマップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

MTP3 User Adaptation（M3UA）は、SS7 Message Transfer Part 3（MTP3）レイヤと連動する IP ベースアプリケーション用の SS7 ネットワークへのゲートウェイを提供するクライアント/サーバー プロトコルです。M3UA により、IP ネットワーク上で SS7 ユーザー パート（ISUP など）を実行することが可能になります。M3UA は RFC 4666 で定義されています。

M3UA は SCTP をトランスポート層として使用します。SCTP ポート 2905 が想定されるポートですが、異なるポートを使用するようにシグナリング ゲートウェイを設定することもできます。

MTP3 レイヤは、ルーティングおよびノードアドレッシングなどのネットワーク機能を提供しますが、ノードの識別にポイント コードを使用します。M3UA 層は、発信ポイント コード

（OPC）および宛先ポイント コード（DPC）を交換します。これは、IP が IP アドレスを使用してノードを識別する仕組みと似ています。

M3UA インスペクションは、限定されたプロトコル準拠を提供します。

オプションで、M3UA インスペクション ポリシー マップを作成し、ポイント コードまたはサービスインジケータ（SI）に基づいてアクセスポリシーを適用することができます。また、メッセージ クラスおよびタイプに基づいてレート制限を適用することもできます。

例

次に、M3UA インスペクション ポリシー マップおよびインスペクション ポリシーの例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasahostname(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
ciscoasa(config-pmap-p)# timeout endpoint 00:45:00
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect m3ua m3ua-map
ciscoasa(config)# service-policy global_policy global
```

関連コマンド

コマンド	説明
class	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map type inspect	インスペクション ポリシー マップを作成します。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show service-policy inspect m3ua	inspect m3ua ポリシーのステータスおよび統計情報を表示します。

inspect mgcp

MGCP アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **mgcp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect mgcp [*map_name*]
no inspect mgcp [*map_name*]

構文の説明

map_name	（任意）MGCP マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

MGCP を使用するには、通常、2 つ以上の **inspect** コマンドを設定する必要があります。1 つはゲートウェイがコマンドを受信するポート用で、もう 1 つはコールエージェントがコマンドを受信するポート用です。一般的に、コール エージェントはゲートウェイのデフォルト MGCP ポート 2427 にコマンドを送信し、ゲートウェイはコール エージェントのデフォルト MGCP ポート 2727 にコマンドを送信します。

MGCP は、メディア ゲートウェイ コントローラまたはコール エージェントと呼ばれる外部コール制御要素からメディア ゲートウェイを制御するために使用されます。メディア ゲートウェイは一般に、電話回線を通じた音声信号と、インターネットまたは他のパケット ネットワークを通じたデータ パケットとの間の変換を行うネットワーク要素です。NAT および PAT を MGCP とともに使用すると、限られた外部（グローバル）アドレスのセットで、内部ネットワークの多数のデバイスをサポートできます。

メディア ゲートウェイの例は次のとおりです。

- トランキング ゲートウェイ。電話ネットワークと Voice over IP ネットワークとの間のインターフェイスです。このようなゲートウェイは通常、大量のデジタル回線を管理します。
- 住宅用ゲートウェイ。従来のアナログ（RJ11）インターフェイスを Voice over IP ネットワークに提供します。住宅用ゲートウェイの例としては、ケーブルモデムやケーブルセットトップ ボックス、xDSL デバイス、ブロードバンド ワイヤレス デバイスなどがあります。
- ビジネスゲートウェイ。従来のデジタルPBX（構内交換機）インターフェイスまたは統合>soft PBX インターフェイスを Voice over IP ネットワークに提供します。

MGCP メッセージは UDP を介して送信されます。応答はコマンドの送信元アドレス（IP アドレスと UDP ポート番号）に返送されますが、コマンド送信先と同じアドレスからの応答は到達しない場合があります。これは、複数のコール エージェントがフェールオーバー コンフィギュレーションで使用されているときに、コマンドを受信したコール エージェントが制御をバックアップ コール エージェントに引き渡し、バックアップ コール エージェントが応答を送信する場合に起こる可能性があります。

（注） MGCP コール エージェントは、AUEP メッセージを送信して、MGCP エンドポイントが存在するかどうかを判定します。これによって、ASA を通過するフローが確立され、MGCP エンドポイントをコール エージェントに登録できます。

1 つ以上のコールエージェントおよびゲートウェイの IP アドレスを設定するには、MGCP マップ コンフィギュレーション モードで **call-agent** および **gateway** コマンドを使用します。コマンドキューで一度に許可される MGCP コマンドの最大数を指定するには、MGCP マップ コンフィギュレーション モードで **command-queue** コマンドを使用します。

シグナリングメッセージのインスペクション

シグナリングメッセージのインスペクションでは、多くの場合、 **inspect mgcp** コマンドでメディアエンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、 **inspect mgcp** コマンドではトンネル デフォルト ゲートウェイのルートを使用しません。**not** トンネルデフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPsec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect mgcp** コマンドが必要な場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

キューに入れることができる MGCP コマンドの最大数は 150 です。

例

次に、MGCP トラフィックを指定し、MGCP インスペクション マップを定義し、ポリシーを定義して、そのポリシーを外部インターフェイスに適用する例を示します。この例では、デフォルト ポート（2427 および 2727）上の MGCP トラフィックと一致するクラスマップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。このコンフィギュレーションでは、コール エージェント 10.10.11.5 および 10.10.11.6 でゲートウェイ 10.10.10.115 を制御し、コール エージェント 10.10.11.7 および 10.10.11.8 で、10.10.10.116 と 10.10.10.117 の両方のゲートウェイを制御できるようにします。すべてのインターフェイスに対して MGCP インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2427

ciscoasa(config)# access-list mgcp_acl permit tcp any any eq 2727
ciscoasa(config)# class-map mgcp_port
ciscoasa(config-cmap)# match access-list mgcp_acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect mgcp inbound_mgcp
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# call-agent 10.10.11.5 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.6 101
ciscoasa(config-pmap-p)# call-agent 10.10.11.7 102
ciscoasa(config-pmap-p)# call-agent 10.10.11.8 102
ciscoasa(config-pmap-p)# gateway 10.10.10.115 101
ciscoasa(config-pmap-p)# gateway 10.10.10.116 102
ciscoasa(config-pmap-p)# gateway 10.10.10.117 102
ciscoasa(config-pmap-p)# command-queue 150
ciscoasa(config-mgcp-map)# exit
ciscoasa(config)# policy-map inbound_policy
ciscoasa(config-pmap)# class mgcp_port
ciscoasa(config-pmap-c)# inspect mgcp
mgcp-map inbound_mgcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy inbound_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map type inspect mgcp	MGCP のインスペクション ポリシー マップを作成します。
show mgcp	ASA を介して確立された MGCP セッションの情報を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。

inspect mmp

MMP 検査エンジンを設定するには、クラス コンフィギュレーション モードで **inspect mmp** コマンドを使用します。MMP インスペクションを削除するには、このコマンドの **no** 形式を使用します。

inspect mmp tls-proxy [*name*]
no inspect mmp tls-proxy [*name*]

構文の説明

name	TLS プロキシ インスタンス名を指定します。
tls-proxy	MMP インスペクションに対して TLS プロキシをイネーブルにします。MMP プロトコルではさらに TCP トランスポートも使用できますが、CUMA クライアントでは TLS トランスポートしかサポートしていません。そのため、MMP インスペクションを有効にするには **tls-proxy** キーワードが必要です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。

使用上のガイドライン

ASA には、CUMA Mobile Multiplexing Protocol（MMP）を検証するインスペクション エンジンが含まれています。MMP は、CUMA クライアントとサーバー間でデータ エンティティを送信するためのデータ トランスポート プロトコルです。ASA が CUMA クライアントとサーバーの間に配置されており、MMP パケットのインスペクションが必要な場合は、**inspect mmp** コマンドを使用します。

MMP トラフィックは TLS 接続でしか転送できないため、MMP インスペクションは TLS プロキシとともにイネーブルにする必要があります。

（注） MMP インスペクションエンジンを設定するときは、デフォルト以外のインスペクション クラスでしか追加できないことに注意してください。

例

次に、**inspect mmp** コマンドを使用して MMP トラフィックを検査する例を示します。

```
ciscoasa
(config)#
class-map mmp
ciscoasa
(config-cmap)#
match port tcp eq 5443
ciscoasa
(config-cmap)#
exit
ciscoasa
(config)#
policy-map mmp-policy
ciscoasa
(config-pmap)#
class mmp
ciscoasa(config-pmap-c)# inspect mmp tls-proxy myproxy
ciscoasa(config-pmap-c)# exit
ciscoasa(config-pmap)# exit
ciscoasa
(config)#
service-policy mmp-policy interface outside
```

関連コマンド

コマンド	説明
tls-proxy	TLS プロキシインスタンスを設定します。

inspect netbios

NetBIOS アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで inspect netbios **command** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect netbios [*map_name*]
no inspect netbios [*map_name*]

構文の説明

map_name （任意）NetBIOS マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

inspect netbios コマンドは、NetBIOS プロトコルに対するアプリケーション インスペクションを有効または無効にします。NETBIOS インスペクションはデフォルトでイネーブルになっています。NetBIOS 検査エンジンは、ASA の NAT 構成に従い、NetBIOS ネームサービス（NBNS）パケット内の IP アドレスを変換します。必要に応じて、NetBIOS プロトコル違反をドロップまたはログに記録するポリシー マップを作成できます。

例

次に、NetBIOS インスペクション ポリシー マップを定義する例を示します。

```
ciscoasa(config)# policy-map type inspect netbios netbios_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation drop
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
policy-map type inspect netbios	NetBIOS のインスペクション ポリシー マップを作成します。
service-policy	1つ以上のインターフェイスにポリシーマップを適用します。

inspect pptp

RTSP アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **pptp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect pptp
no inspect pptp

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

Point-to-Point Tunneling Protocol（PPTP）は、PPP トラフィックをトンネリングするためのプロトコルです。PPTP セッションは、1 つの TCP チャネルと通常 2 つの PPTP GRE トンネルで構成されます。TCP チャネルは、PPTP GRE トンネルのネゴシエートと管理に使用される制御チャネルです。GRE トンネルは、2 つのホスト間の PPP セッションを伝送します。

PPTP アプリケーション インスペクションは、イネーブルになると、PPTP プロトコル パケットを検査し、PPTP トラフィックを許可するために必要な GRE 接続と xlate をダイナミックに作成します。RFC 2637 で定義されているバージョン 1 だけがサポートされます。

PAT は、PPTP TCP 制御チャネル上で修正バージョンの GRE（RFC 2637）がネゴシエートされたときに、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

具体的には、ASA は、PPTP のバージョン通知と発信コールの要求/応答シーケンスを検査します。RFC 2637 で定義されている PPTP バージョン 1 だけが検査されます。どちらかの側から通

知されたバージョンがバージョン 1 でない場合、TCP 制御チャネルでのそれ以降のインスペクションはディセーブルになります。また、発信コールの要求と応答のシーケンスは追跡されます。接続と xlate は、後続のセカンダリ GRE データ トラフィックを許可するために、必要に応じてダイナミックに割り当てられます。

PPTP インスペクション エンジンは、PPTP トラフィックを PAT で変換できるように、イネーブルにする必要があります。また、PAT は、PPTP TCP 制御チャネルで修正バージョンの GRE（RFC 2637）がネゴシエートされた場合に限り、その GRE に対してだけ実行されます。PAT は、未修正バージョンの GRE（RFC 1701、RFC 1702）には実行されません。

RFC 2637 で定義されているように、PPTP プロトコルは、主に、モデム バンク PAC（PPTP アクセス コンセントレータ）から開始されたヘッドエンド PNS（PPTP ネットワーク サーバー）への PPP セッションのトンネリングに使用されます。このように使用された場合、PAC がリモート クライアントで PNS がサーバーです。

ただし、Windows によって VPN で使用された場合、この関係は逆になります。PNS は、中央のネットワークにアクセスするためにヘッドエンド PAC への接続を開始するリモートのシングル ユーザー PC です。

すべてのインターフェイスに対して PPTP インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

例

次の例に示すように、PPTP インスペクション エンジンをイネーブルにします。この例では、デフォルト ポート（1723）上の PPTP トラフィックと一致するクラス マップを作成します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
ciscoasa(config)# class-map pptp-port
ciscoasa(config-cmap)# match port tcp eq 1723
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pptp_policy
ciscoasa(config-pmap)# class pptp-port
ciscoasa(config-pmap-c)# inspect pptp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy pptp_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect radius-accounting

RADIUS アカウンティング インスペクションを有効または無効にする、またはトラフィックまたはトンネルを制御するためのマップを定義するには、クラス コンフィギュレーション モードで **inspect radius-accounting** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect radius-accounting *map_name*
no inspect radius-accounting [*map_name*]

構文の説明

map_name	RADIUS アカウンティング マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

RADIUS アカウンティング インスペクションの目的は、RADIUS サーバーを使用した GPRS ネットワークの過剰請求攻撃を防ぐことです。RADIUS アカウンティング インスペクションを実行するには、GTP/GPRS または Carrier ライセンスは必要ありませんが、GTP インスペクションを実行し、GPRS セットアップをセットアップしない限り、意味がありません。

policy-map type inspect radius-accounting コマンドを使用して、RADIUS アカウンティングのパラメータの定義に使用するインスペクションマップを作成します。parameters コマンドを入力後、**send response**、**host**、**validate-attribute**、**enable gprs**、および **timeout users** コマンドを使用してインスペクションの特性や動作を定義できます。

次に **class-map type management**、**policy-map**、および **service-policy** コマンドを使用して、トラフィックのクラスを定義し、inspect radius-accounting コマンドをクラスに適用し、1 つ以上のインターフェイスにポリシーを適用します。

（注） **inspect radius-accounting** コマンドは **class-map type management** コマンドとともにのみ使用できます。

例

次に、RADIUS アカウンティング インスペクション マップを設定し、インスペクションをグローバルにイネーブルにする例を示します。

```
policy-map type inspect radius-accounting radius-acct-pmap
  parameters
    send response
    enable gprs
    validate-attribute 31
    host 10.2.2.2 key 123456789
    host 10.1.1.1 key 12345
class-map type management radius-class
  match port udp eq radius-acct
policy-map global_policy
  class radius-class
    inspect radius-accounting radius-acct-pmap
```

関連コマンド

コマンド	説明
parameters	セキュリティ アクションを適用するトラフィック クラスを定義します。
class-map type management	アクションを適用する ASA 宛てのレイヤ 3 またはレイヤ 4 管理トラフィックを識別します。
policy-map type inspect radius-accounting	RADIUS アカウンティングのインスペクション ポリシーマップを作成します。
show および **clear service-policy**	サービス ポリシー設定の表示とクリアを行います。
service-policy	1 つ以上のインターフェイスにポリシーマップを適用します。

inspect rsh

RSH アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **rsh** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect rsh
no inspect rsh

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

RSH プロトコルは、TCP ポート 514 で RSH クライアントから RSH サーバーへの TCP 接続を使用します。クライアントとサーバーは、クライアントが STDERR 出力ストリームを受信する TCP ポート番号をネゴシエートします。RSH インスペクションは、必要に応じて、ネゴシエートされたポート番号の NAT をサポートします。

例

次に、RSHインスペクションエンジンをイネーブルにし、RSHトラフィックをデフォルトポート（514）上で照合するクラスマップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスのRSHインスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map rsh-port
ciscoasa(config-cmap)# match port tcp eq 514
```

```
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rsh_policy

ciscoasa(config-pmap)# class rsh-port
ciscoasa(config-pmap-c)# inspect rsh
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rsh_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect rtsp

RTSP アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで inspect **rtsp** コマンドを使用します。クラス 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。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。

inspect rtsp [*map_name*]
no inspect rtsp [*map_name*]

構文の説明

map_name	（任意）RTSP マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

inspect rtsp コマンドを使用すると、ASA で RTSP パケットを通過させることができます。RTSP は、RealAudio、RealNetworks、Apple QuickTime 4、RealPlayer、および Cisco IP/TV の各接続で使用されます。

（注） Cisco IP/TV では、RTSP TCP ポート 554 と TCP 8554 を使用します。

RTSP アプリケーションは、制御チャネルとしての TCP（例外的に UDP）とともに予約済みポート 554 を使用します。ASA は、RFC 2326 に準拠して、TCP だけをサポートします。この TCP コントロール チャネルは、クライアントに設定されているトランスポート モードに応じて、オーディオ/ビデオ トラフィックの送信に使用されるデータ チャネルをネゴシエートするために使用されます。

サポートされている RDT トランスポートは、rtp/avp、rtp/avp/udp、x-real-rdt、x-real-rdt/udp、x-pn-tng/udp です。

ASA はステータスコード 200 の SETUP 応答メッセージを解析します。SETUP 応答メッセージが、着信方向に移動している場合、サーバーは ASA との相対位置関係で外部に存在することになるため、サーバーから着信する接続に対してダイナミック チャネルを開くことが必要になります。この応答メッセージがアウトバウンド方向である場合、ASA は、ダイナミック チャネルを開く必要はありません。

RFC 2326 では、クライアントとサーバーのポートを SETUP 応答メッセージ内に含める必要があるとは規定されていないため、ASA で状態を保持し、SETUP メッセージに含まれているクライアントポートを記憶しておく必要があります。QuickTime が、SETUP メッセージ内にクライアント ポートを設定すると、サーバーは、サーバー ポートだけで応答します。

RealPlayer の使用方法

RealPlayer を使用するときは、転送モードを正しく設定することが重要です。ASA では、サーバーからクライアントまたはその逆の **access-list** コマンドステートメントを追加します。RealPlayer の場合、[**Options**] > [**Preferences**] > [**Transport**] > [**RTSP Settings**] を選択して、転送モードを変更します。

RealPlayer で TCP モードを使用している場合は、[**Use TCP to Connect to Server**] チェックボックスと [**Attempt to use TCP for all content**] チェックボックスをオンにします。ASA で、インスペクション エンジンを設定する必要はありません。

RealPlayer で UDP モードを使用する場合は、[**Use TCP to Connect to Server**] および [**Attempt to use UDP for static content**] チェックボックスをオンにします。また、マルチキャスト経由でライブコンテンツは利用できません。ASA で、**inspect rtsp** *port* コマンドステートメントを追加します。

制約事項と制限

RSTP インスペクションには次の制限が適用されます。

- ASA は、マルチキャスト RTSP または UDP による RTSP メッセージをサポートしません。
- ASA には、RTSP メッセージが HTTP メッセージ内に隠されている HTTP クローキングを認識する機能はありません。
- 埋め込み IP アドレスが HTTP メッセージまたは RTSP メッセージの一部として SDP ファイル内に含まれているため、ASA は、RTSP メッセージに NAT を実行できません。パケットはフラグメント化できますが、ASA ではフラグメント化されたパケットに対して NAT を実行することはできません。
- Cisco IP/TV では、メッセージの SDP 部分に対して ASA が実行する変換の数は、Content Manager にあるプログラム リストの数に比例します（各プログラム リストには、少なくとも 6 個の埋め込み IP アドレスを含めることができます）。
- Apple QuickTime 4 または RealPlayer 用の NAT を設定できます。Cisco IP/TV は、ビューアと Content Manager が外部ネットワークにあり、サーバーが内部ネットワークにあるときにだけ NAT を使用できます。

例

次に、RTSP インスペクション エンジンをイネーブルにし、RTSP トラフィックをデフォルト ポート（554 および 8554）上で照合するクラス マップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。

```
ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 554

ciscoasa(config)# access-list rtsp-acl permit tcp any any eq 8554
ciscoasa(config)# class-map rtsp-traffic

ciscoasa(config-cmap)# match access-list rtsp-acl

ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map rtsp_policy

ciscoasa(config-pmap)# class rtsp-traffic
ciscoasa(config-pmap-c)# inspect rtsp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy rtsp_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect scansafe

クラスのトラフィックに対するクラウド Web セキュリティ インスペクションを有効にするには、クラス コンフィギュレーション モードで **inspect scansafe** コマンドを使用します。クラス コンフィギュレーション モードにアクセスするには、**policy-map** コマンドを入力します。インスペクションアクションを削除するには、このコマンドの **no** 形式を使用します。

inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]
no inspect scansafe *scansafe_policy_name* [**fail-open** | **fail-close**]

構文の説明

scansafe_policy_name	**policy-map type inspect scansafe** コマンドで定義するインスペクション クラス マップの名前を指定します。
fail-open	（任意）クラウド Web セキュリティサーバーを使用できない場合に ASA を通過するトラフィックを許可します。
fail-close	（任意）クラウド Web セキュリティサーバーを使用できない場合にすべてのトラフィックがドロップされます。 **fail-close** がデフォルトです。

コマンド デフォルト

fail-close がデフォルトです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco クラウド Web セキュリティでは、Software as a Service（SaaS）による Web セキュリティおよび Web フィルタリング サービスが提供されます。ネットワークで ASA を使用している企業は、追加ハードウェアをインストールせずにクラウド Web セキュリティ サービスを使用できます。

（注） この機能は「ScanSafe」とも呼ばれていますので、ScanSafe という名前が表示されるコマンドがあります。

モジュラ ポリシー フレームワークを使用してこのコマンドを設定する手順は次のとおりです。

1. **policy-map type inspect scansafe** コマンドを使用してインスペクション ポリシー マップを作成します。HTTP と HTTPS の両方のトラフィックタイプを検査する場合、タイプごとに少なくとも 1 つ作成する必要があります。
2. （任意）**class-map type inspect scansafe** コマンドを使用してホワイトリストを設定します。
3. **class-map** コマンドを使用して、検査するトラフィックを定義します。HTTP と HTTPS のトラフィックについて、それぞれクラス マップを設定する必要があります。
4. **policy-map** コマンドを入力してポリシーを定義します。
5. HTTP の場合、**class** コマンドを入力して HTTP クラスマップを参照します。
6. **inspect scansafe** コマンドを入力して HTTP インスペクション ポリシー マップを参照します。
7. HTTPS の場合、**class** コマンドを入力して HTTPS クラスマップを参照します。
8. **inspect scansafe** コマンドを入力して HTTPS インスペクション ポリシー マップを参照します。
9. 最後に、**service-policy** コマンドを使用して、インターフェイスにポリシーマップを適用します。

例

次に、2 つのクラス（HTTP に 1 つ、HTTPS に 1 つ）を設定する例を示します。各 ACL は www.cisco.com と tools.cisco.com、DMZ ネットワーク、および HTTP と HTTPS の両方に対するトラフィックを免除します。他のすべてのトラフィックは、複数のホワイトリストに記載されたユーザーおよびグループを除き、クラウド Web セキュリティに送信されます。ポリシーは、内部インターフェイスに適用されます。

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# https
```

```
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# object network cisco1
ciscoasa(config-object-network)# fqdn www.cisco.com
ciscoasa(config)# object network cisco2
ciscoasa(config-object-network)# fqdn tools.cisco.com
ciscoasa(config)# object network dmz_network
ciscoasa(config-object-network)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco1 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object cisco2 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network
eq 80
ciscoasa(config)# access-list SCANSAFE_HTTP extended permit tcp any4 any4 eq 80
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco1 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended deny tcp any4 object cisco2 eq 443
ciscoasa(config)# access-list SCANSAFE_HTTP extended deny tcp any4 object dmz_network
eq 443
ciscoasa(config)# access-list SCANSAFE_HTTPS extended permit tcp any4 any4 eq 443
ciscoasa(config)# class-map cws_class1
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTP
ciscoasa(config)# class-map cws_class2
ciscoasa(config-cmap)# match access-list SCANSAFE_HTTPS
ciscoasa(config)# policy-map cws_policy
ciscoasa(config-pmap)# class cws_class1
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap1 fail-open
ciscoasa(config-pmap)# class cws_class2
ciscoasa(config-pmap-c)# inspect scansafe cws_inspect_pmap2 fail-open
ciscoasa(config)# service-policy cws_policy inside
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合のデフォルトのユーザー名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定します。
match user group	ユーザーまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。

コマンド	説明
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティプロキシサーバーをポーリングする前に ASA が待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバー オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバーの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバーが現在のアクティブ サーバー、バックアップ サーバー、または到達不能のいずれであるか、サーバーのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザーまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

inspect sctp

Stream Control Transmission Protocol（SCTP）インスペクションを有効または無効にするには、クラス コンフィギュレーション モードで **inspect sctp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。SCTP インスペクションを無効にするには、このコマンドの **no** 形式を使用します。

inspect sctp [*map_name*]
no inspect sctp [*map_name*]

（注） SCTP インスペクションには Carrier ライセンスが必要です。

構文の説明

map_name （オプション）SCTP インスペクション ポリシー マップの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

SCTP（Stream Control Transmission Protocol）は、テレフォニー シグナリング プロトコル SS7 をサポートしており、4G LTE モバイル ネットワーク アーキテクチャのいくつかのインターフェイス用のトランスポート プロトコルでもあります。デバイスを通過するモバイル ネットワーク トラフィックがある場合は、SCTP インスペクションを GTP および Diameter インスペクションとともに使用します。

オプションで、SCTP ポリシー マップを指定できます。これにより、SCTP アプリケーションでフィルタ処理を実行して、さまざまなサービスを提供できます。また、ペイロードプロトコル ID（PPID）に基づいて SCTP トラフィック クラスを選択的にドロップしたり、ログに記録

したり、それらにレート制限を適用したりすることができます。**policy-map type inspect sctp** コマンドを使用してポリシーマップを作成します。

例

次の例では、未割り当ての PPID（この例の作成時点で未割り当て）をドロップし、PPID 32 ～ 40 をレート制限し、Diameter PPID をログに記録するインスペクション ポリシー マップを作成します。このサービス ポリシーは、すべての SCTP トラフィックを照合する inspection_default クラスにインスペクションを適用します。

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
  drop
 match ppid 26
  drop
 match ppid 49
  drop
 match ppid 32 40
  rate-limit 1000
 match ppid diameter
  log
policy-map global_policy
 class inspection_default
  inspect sctp sctp-pmap
!
service-policy global_policy global
```

関連コマンド

コマンド	説明
class	セキュリティ アクションを適用するトラフィック クラスを定義します。
clear service-policy inspect sctp	グローバルな SCTP 統計情報をクリアします。
policy-map type inspect	インスペクション ポリシー マップを作成します。
service-policy	1 つ以上のインターフェイスにポリシーマップを適用します。
show service-policy inspect sctp	inspect sctp ポリシーのステータスおよび統計情報を表示します。

inspect sip

SIPアプリケーションインスペクションを有効にしたり、ASAがリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **sip** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]
no inspect sip [*sip_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*] [**uc-ime** *proxy_name*]

構文の説明

phone-proxy *proxy_name*	指定したインスペクション セッションの Phone Proxy をイネーブルにします。
sip_map	SIP ポリシー マップ名を指定します。
tls-proxy *proxy_name*	指定されたインスペクション セッションで TLS プロキシをイネーブルにします。キーワード **tls-proxy** は、レイヤ 7 ポリシーマップ名として使用できません。
uc-ime *proxy_name*	SIP インスペクションの Cisco Intercompany Media Engine プロキシをイネーブルにします。

コマンド デフォルト

SIP インスペクションはデフォルトでイネーブルになっており、次を含むデフォルトのインスペクション ポリシー マップを使用します。

- SIP インスタント メッセージ（IM）の拡張機能：イネーブル
- SIP トラフィック以外の SIP ポート使用：許可
- サーバーとエンドポイントの IP アドレスの非表示：ディセーブル
- ソフトウェアのバージョンと SIP 以外の URI をマスク：ディセーブル
- 1 以上の宛先ホップ カウントを保証：イネーブル
- RTP 準拠：適用強制しない
- SIP 準拠：ステート チェックとヘッダー検証を実行しない

暗号化されたトラフィックのインスペクションがイネーブルになっていないことにも注意してください。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

SIP のデフォルトのポート割り当ては 5060 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。
8.0(2)	tls-proxy キーワードが追加されました。
9.4(1)	**phone-proxy** キーワードと **uc-ime** キーワードが削除されました。

使用上のガイドライン

SIP は、インターネット会議、テレフォニー、プレゼンス、イベント通知、およびインスタントメッセージングに広く使用されているプロトコルです。テキストベースの性質とその柔軟性により、SIP ネットワークは数多くのセキュリティ脅威にさらされます。

SIP アプリケーション インスペクションでは、メッセージ ヘッダーおよび本文のアドレス変換、ポートの動的なオープン、および基本的な健全性チェックが行われます。SIP メッセージの健全性を実現するアプリケーション セキュリティおよびプロトコルへの準拠と、SIP ベースの攻撃の検出もサポートされます。

SIP インスペクションはデフォルトでイネーブルになっています。これは、デフォルト以外の処理が必要な場合、または暗号化されたトラフィックのインスペクションをイネーブルにするために TLS プロキシを設定する場合にのみ設定する必要があります。

ASA 経由の SIP コールをサポートする場合は、シグナリング メッセージは予約済みの宛先ポート（UDP/TCP 5060）経由で送信され、メディア ストリームはダイナミックに割り当てられるため、メディア接続アドレスのシグナリング メッセージ、メディア ポート、およびメディアの初期接続を検査する必要があります。また、SIP は、IP パケットのユーザーデータ部分に IP アドレスを埋め込みます。SIP インスペクションは、それらの埋め込まれた IP アドレスに NAT を適用します。

SIP インスペクションの制限事項

SIP インスペクションは、埋め込まれた IP アドレスに NAT を適用します。ただし、送信元と宛先両方のアドレスを変換するように NAT を設定している場合、外部アドレス（「trying」応答メッセージの SIP ヘッダー内の「from」）は書き換えられません。そのため、宛先アドレスの変換を回避するように SIP トラフィックを使用している場合は、オブジェクト NAT を使用する必要があります。

PAT を SIP で使用する場合、次の制限事項が適用されます。

- ASA で保護されているネットワークの SIP プロキシにリモート エンドポイントを登録しようとすると、次のような一定の条件下で登録が失敗します。
  - PAT がリモート エンドポイント用に設定されている。
  - SIP レジストラ サーバーが外部ネットワークにある。
  - エンドポイントからプロキシ サーバーに送信された REGISTER メッセージの接続先フィールドにポートが設定されていない。
- SDP 部分の所有者/作成者フィールド（o=）の IP アドレスが接続フィールド（c=）の IP アドレスと異なるパケットを SIP デバイスが送信すると、o= フィールドの IP アドレスが正しく変換されない場合があります。これは、o= フィールドでポート値を提供しない SIP プロトコルの制限によるものです。
- PAT を使用する場合は、ポートを持たない内部 IP アドレスを含む SIP ヘッダー フィールドは変換されない可能性があるため、内部 IP アドレスが外部に漏れます。この漏出を避けるには、PAT の代わりに NAT を設定します。

シグナリングメッセージのインスペクション

シグナリングメッセージのインスペクションでは、多くの場合、**inspect sip** コマンドでメディア エンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、**inspect sip** コマンドではトンネル デフォルト ゲートウェイのルートを使用しません。**not** トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPsec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect sip** コマンドが必要な場合は、トンネルデフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次に、SIP インスペクション エンジンをイネーブルにし、SIP トラフィックをデフォルト ポート（5060）上で照合するクラス マップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して SIP インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map sip-port
ciscoasa(config-cmap)# match port tcp eq 5060
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sip_policy

ciscoasa(config-pmap)# class sip-port
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sip_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map type inspect sip	SIP のインスペクション ポリシー マップを作成します。
show sip	ASA を介して確立された SIP セッションの情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。
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。

inspect skinny

SCCP（Skinny）アプリケーション インスペクションを有効にするには、クラス コンフィギュレーション モードで **skinny** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]
no inspect skinny [*skinny_map*] [**tls-proxy** *proxy_name*] [**phone-proxy** *proxy_name*]

構文の説明

phone-proxy *proxy_name*	インスペクションセッションの phone proxy をイネーブルにします。
skinny_map	skinny ポリシー マップ名を指定します。
tls-proxy *proxy_name*	インスペクションセッションで TLS プロキシをイネーブルにします。

コマンド デフォルト

SCCP インスペクションは、次のデフォルト値を使用してデフォルトでイネーブルになっています。

- 登録：適用強制しない
- メッセージの最大 ID：0x181
- プレフィックスの長さの最小値：4
- メディア タイムアウト：00:05:00
- シグナリング タイムアウト：01:00:00
- RTP 準拠：適用強制しない

暗号化されたトラフィックのインスペクションがイネーブルになっていないことにも注意してください。暗号化されたトラフィックを検査するには、TLS プロキシを設定する必要があります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。
8.0(2)	キーワード **tls-proxy** が追加されました。
9.4(1)	**phone-proxy** キーワードは推奨しません。
9.13(1)	**tls-proxy** キーワードは推奨しません。このキーワードは今後のリリースで削除される予定です。
9.14(1)	**tls-proxy** キーワード、および SCCP/Skinny 暗号化インスペクションのサポートは削除されました。

使用上のガイドライン

Skinny（SCCP）は、VoIP ネットワークで使用される簡易プロトコルです。SCCP を使用する Cisco IP Phone は、H.323 環境でも使用できます。Cisco CallManager とともに使用する場合、SCCP クライアントは H.323 準拠端末と相互運用できます。

ASA は、SCCP に対して PAT と NAT をサポートします。IP 電話で使用できるグローバル IP アドレスよりも IP 電話が多い場合は、PAT が必要です。Skinny アプリケーション インスペクションは、SCCP シグナリング パケットの NAT と PAT をサポートすることで、すべての SCCP シグナリング パケットとメディア パケットが ASA を通過できるようにします。

Cisco CallManager と Cisco IP Phones 間の通常のトラフィックは SCCP を使用しており、特別な設定をしなくても SCCP インスペクションによって処理されます。ASA は、TFTP サーバーの場所を Cisco IP Phone とその他の DHCP クライアントに送信することで、DHCP オプション 150 および 66 もサポートします。Cisco IP Phone では、デフォルト ルートを設定する DHCP オプション 3 を要求に含めることもできます。

（注） ASA は、SCCP プロトコル バージョン 22 以前が稼働している Cisco IP Phone からのトラフィックのインスペクションをサポートします。

Cisco IP Phone のサポート

Cisco CallManager が Cisco IP Phone と比べて高セキュリティ インターフェイスにあるトポロジでは、NAT が Cisco CallManager の IP アドレスに必要な場合、マッピングはスタティックである必要があります。これは、Cisco IP Phone では Cisco CallManager の IP アドレスをコンフィギュレーションで明示的に指定する必要があるためです。スタティック アイデンティティ エントリを使用すると、セキュリティが高いインターフェイス上にある Cisco CallManager が Cisco IP Phone からの登録を受け付けるようにできます。

Cisco IP Phone では、TFTP サーバーにアクセスして、Cisco CallManager サーバーに接続するために必要な設定情報をダウンロードする必要があります。

TFTP サーバーと比較して Cisco IP Phone の方がセキュリティの低いインターフェイス上にある場合は、ACL を使用して UDP ポート 69 の保護された TFTP サーバーに接続する必要があります。TFTP サーバーに対してはスタティック エントリが必要ですが、識別スタティック エントリにする必要はありません。NAT を使用する場合、識別スタティック エントリは同じ IP アドレスにマッピングされます。PAT を使用する場合は、同じ IP アドレスとポートにマッピングされます。

Cisco IP Phone が TFTP サーバーおよび Cisco CallManager と比べてセキュリティの高いインターフェイス上にある場合、Cisco IP Phone が接続を開始するための、ACL やスタティックエントリは必要ありません。

制約事項と制限

内部の Cisco CallManager のアドレスが NAT または PAT 用に別の IP アドレスかポートに設定されている場合、ASA は現在、TFTP 経由で転送するファイルコンテンツに対して NAT や PAT をサポートしていないため、外部の Cisco IP Phone 用の登録は失敗します。ASA は TFTP メッセージの NAT をサポートし、TFTP ファイル用にピンホールを開きますが、ASA は電話の登録中に TFTP によって転送された Cisco IP Phone のコンフィギュレーション ファイルに埋め込まれた Cisco CallManager の IP アドレスとポートを変換することはできません。

（注） ASA は、コール セットアップ中のコールを除き、SCCP コールのステートフル フェールオーバーをサポートします。

シグナリングメッセージのインスペクション

シグナリングメッセージのインスペクションでは、多くの場合、 **inspect skinny** コマンドでメディアエンドポイント（IP 電話など）の場所を特定する必要があります。

この情報は、メディア トラフィックのアクセス コントロールと NAT 状態を準備して、手動で設定を行わずにメディア トラフィックが透過的にファイアウォールを通過するために使用されます。

これらの場所を特定するときに、 **inspect skinny** コマンドではトンネル デフォルト ゲートウェイのルートを使用しません。**not** トンネル デフォルト ゲートウェイのルートは、**route** *interface* **0 0** *metric* **tunneled** という形式のルートです。このルートは、IPsec トンネルから出力されるパケットのデフォルト ルートを上書きします。そのため、VPN トラフィックに対して **inspect skinny** コマンドが必要な場合は、トンネル デフォルト ゲートウェイのルートを設定しないでください。代わりに、他のスタティック ルーティングまたはダイナミック ルーティングを使用します。

例

次に、SCCP インスペクション エンジンをイネーブルにし、SCCP トラフィックをデフォルト ポート（2000）上で照合するクラス マップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して SCCP インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map skinny-port
```

```
ciscoasa(config-cmap)# match port tcp eq 2000
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map skinny_policy

ciscoasa(config-pmap)# class skinny-port
ciscoasa(config-pmap-c)# inspect skinny
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy skinny_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map type inspect skinny	SCCP のインスペクション ポリシー マップを作成します。
show skinny	ASA を介して確立された SCCP セッションの情報を表示します。
show conn	さまざまな接続タイプの接続状態を表示します。
timeout	さまざまなプロトコルおよびセッション タイプのアイドル状態の最大継続時間を設定します。
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。

inspect snmp

SNMP アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **snmp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect snmp [*map_name*]
no inspect snmp [*map_name*]

構文の説明

map_name SNMP マップ名です。

コマンド デフォルト

このコマンドは、9.14(1) 以降、デフォルトで有効になっています。以前のリリースでは、デフォルトで無効になっていました。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.14(1)	このコマンドはデフォルトで有効になっており、SNMP マップはオプションになりました。

使用上のガイドライン

9.14(1) 以降、SNMP アプリケーション インスペクションは、デバイスへのトラフィックとデバイス経由のトラフィックの両方に適用されます。このインスペクションは、ユーザーが特定の SNMP ホストに制限される SNMP v3 を設定する場合に必要です。インスペクションなしの場合、定義された v3 ユーザーは任意の許可されたホストからデバイスをポーリングできます。SNMP インスペクションはデフォルトポートではデフォルトで有効になっているため、デフォルト以外のポートを使用する場合にのみ設定する必要があります。デフォルトポートは UDP/161、162 であり（すべてのデバイスタイプ）、FXOS は UDP/161 でリッスンするため、Cisco Secure Firewall Extensible Operating System（FXOS）も実行するデバイスでは UDP/4161 です。

9.14(1) より前のリリースでは、SNMP インスペクションはデフォルトで有効になっておらず、through-the-box トラフィックにのみ適用されます。

また、SNMP アプリケーション インスペクションでは、SNMP トラフィックを特定のバージョンの SNMP に制限できます。以前のバージョンの SNMP は安全性が低いため、セキュリティ ポリシーを使用して特定の SNMP バージョンを拒否する必要が生じる場合もあります。システムは、SNMP バージョン 1、2、2c、または 3 を拒否できます。SNMP の特定のバージョンを拒否するには、**snmp-map** コマンドを使用して作成する SNMP マップで、**deny version** コマンドを使用します。SNMP マップの設定後に、**inspect snmp** コマンドを使用してマップを有効にし、**service-policy** コマンドを使用して 1 つ以上のインターフェイスに適用します。

9.14(1) 以降、バージョンを制御する必要がない場合は、マップなしで SNMP インスペクションを有効にします。以前のバージョンではマップが必要です。

例

次に、SNMP トラフィックを識別し、SNMP マップを定義して、ポリシーを定義し、SNMP インスペクションをイネーブルにして、外部インターフェイスにポリシーを適用する例を示します。

```
ciscoasa(config)# access-list snmp-acl permit tcp any any eq 161

ciscoasa(config)# access-list snmp-acl permit tcp any any eq 162
ciscoasa(config)# class-map snmp-port

ciscoasa(config-cmap)# match access-list snmp-acl
ciscoasa(config-cmap)# exit
ciscoasa(config)# snmp-map inbound_snmp
ciscoasa(config-snmp-map)# deny version 1
ciscoasa(config-snmp-map)# exit
ciscoasa(config)# policy-map inbound_policy

ciscoasa(config-pmap)# class snmp-port
ciscoasa(config-pmap-c)# inspect snmp inbound_snmp

ciscoasa(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
deny version	特定のバージョンの SNMP を使用したトラフィックを不許可にします。
snmp-map	SNMP マップを定義し、SNMP マップ コンフィギュレーション モードをイネーブルにします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect sqlnet

Oracle SQL*Net アプリケーション インスペクションを有効にするには、クラス コンフィギュレーション モードで inspect **sqlnet** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect sqlnet
no inspect sqlnet

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。

コマンド 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。

デフォルトのポート割り当ては 1521 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

SQL*Net プロトコルは、さまざまなパケットタイプで構成されています。ASA はそれらのパケットを処理して、ASA の両側の Oracle アプリケーションに一貫性のあるデータストリームが表示されるようにします。

SQL*Net のデフォルトのポート割り当ては 1521 です。これは、Oracle が SQL*Net 用に使用している値ですが、構造化照会言語（SQL）の IANA ポート割り当てとは一致しません。SQL*Net インスペクションを一連のポート番号に適用するには、**class-map** コマンドを使用します。

（注） SQL 制御 TCP ポート 1521 と同じポートで SQL データ転送が行われる場合は、SQL*Net のインスペクションをディセーブルにします。SQL*Net インスペクションが有効になっていると、ASA はプロキシとして機能し、クライアントのウィンドウサイズを 65000 から約 16000 に減らすため、データ転送の問題が発生します。

ASA は、すべてのアドレスの NAT を実行し、パケット内のすべての埋め込みポートを検索して、SQL*Net バージョン 1 用に開きます。

SQL*Net バージョン 2 の場合、データ長ゼロの REDIRECT パケットの直後に続くすべての DATA パケットまたは REDIRECT パケットはフィックスアップされます。

フィックスアップが必要なパケットには、埋め込みホスト アドレスおよびポート アドレスが次の形式で含まれています。

```
(ADDRESS=(PROTOCOL=tcp)(DEV=6)(HOST=a.b.c.d)(PORT=a))
```

SQL*Net バージョン 2 の各 TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker）は、NAT 対象のアドレスがあるかどうかがスキャンされません。また、インスペクションがパケット内に埋め込まれたポートにダイナミック接続を開くこともありません。

SQL*Net バージョン 2 の TNSFrame、Redirect パケット、および Data パケットは、ペイロードのデータ長がゼロの REDIRECT TNSFrame タイプの後に続く場合、開くポートおよび NAT 対象のアドレスがあるかどうかスキャンされます。データ長がゼロの Redirect メッセージが ASA を通過すると、後続の Data または Redirect メッセージの NAT が実行され、ポートが動的に開かれることを想定するフラグが接続データ構造に設定されます。先行するパラグラフの TNS フレームのいずれかが Redirect メッセージの後に到着した場合、フラグはリセットされます。

SQL*Net インスペクション エンジンは、チェックサムを再計算し、IP および TCP の長さを変更し、新旧のメッセージの長さの差を使用してシーケンス番号と確認応答番号を再調整します。

SQL*Net バージョン 1 では、その他のすべての場合を想定しています。TNSFrame タイプ（Connect、Accept、Refuse、Resend、Marker、Redirect、Data）とすべてのパケットは、ポートおよびアドレスがあるかどうかスキャンされます。アドレスの NAT が実行され、ポート接続が開かれます。

例

次に、SQL*Net インスペクション エンジンをイネーブルにし、SQL*Net トラフィックをデフォルト ポート（1521）上で照合するクラスマップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して SQL*Net インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map sqlnet-port
ciscoasa(config-cmap)# match port tcp eq 1521
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sqlnet_policy

ciscoasa(config-pmap)# class sqlnet-port
```

```
ciscoasa(config-pmap-c)# inspect sqlnet
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sqlnet_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。
show conn	SQL*net など、さまざまな接続タイプの接続状態を表示します。

inspect stun

Session Traversal Utilities for NAT（STUN）アプリケーション インスペクションを有効にするには、クラス コンフィギュレーション モードで inspect **stun** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect stun
no inspect stun

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。

コマンド 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。

デフォルトのポート割り当ては TCP/3478 および UDP/3478 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

RFC 5389 で定義されている Session Traversal Utilities for NAT（STUN）は、プラグインが不要になるように、ブラウザベースのリアルタイム コミュニケーション用に WebRTC クライアントによって使用されます。WebRTC クライアントは、多くの場合、クラウド STUN サーバーを使用してパブリック IP アドレスおよびポートを学習します。WebRTC は、Interactive Connectivity Establishment（ICE、RFC 5245）を使用してクライアント間の接続を確認します。これらのクライアントは、TCP やその他のプロトコルを使用することもできますが、通常、UDP を使用します。

ファイアウォールは、多くの場合、発信 UDP トラフィックをブロックするため、Cisco Spark などの WebRTC 製品が接続を完了できないことがあります。STUN インスペクションでは、STUN エンドポイント用のピンホールが開かれ、STUN と ICES の基本コンプライアンスが適用されます。これにより、両側で接続チェックが確認応答された場合にクライアントの通信が

許可されます。このため、これらのアプリケーションをイネーブルにするためにアクセスルールで新しいポートを開く必要がなくなります。

デフォルトのインスペクションクラスでSTUNインスペクションをイネーブルにすると、STUNトラフィックに関して TCP/UDP ポート 3478 が監視されます。このインスペクションは、IPv4 アドレスと TCP/UDP のみをサポートします。

STUN インスペクションには NAT に関するいくつかの制限があります。WebRTC トラフィックについては、スタティック NAT/PAT44 がサポートされます。Cisco Spark はピンホールを必要としないので、Spark は追加のタイプの NAT をサポートできます。Cisco Spark では NAT/PAT64（ダイナミック NAT/PAT を含む）も使用できます。

ピンホールが複製されるとき、STUN インスペクションはフェールオーバーモードとクラスタモードでサポートされます。ただし、トランザクション ID はユニット間で複製されません。ユニットが STUN 要求を受信した後に故障し、別のユニットが STUN 応答を受信した場合、その STUN 応答はドロップされます。

例

次に、STUN インスペクションをデフォルト グローバル インスペクション ルールの一部としてイネーブルにする例を示します。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect stun
ciscoasa(config)# service-policy global_policy global
```

関連コマンド

コマンド	説明
class	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシーマップを適用します。
show conn	STUN を含む各種接続タイプの接続状態を表示します。
show service-policy inspect diameter	inspect diameter ポリシーのステータスおよび統計情報を表示します。

inspect sunrpc

Sun RPC アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで inspect sunrpc コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect sunrpc
no inspect sunrpc

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

Sun RPC アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、ポリシー マップ クラス コンフィギュレーション モードで inspect sunrpc コマンドを使用します。このモードにアクセスするには、ポリシー マップ コンフィギュレーション モードで **class** 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。

inspect sunrpc コマンドは、Sun RPC プロトコルに対するアプリケーション インスペクションを有効または無効にします。Sun RPC は、NFS および NIS で使用されます。Sun RPC サービスはシステムの任意のポートで実行できます。クライアントがサーバー上の Sun RPC サービスにアクセスしようとする場合には、サービスが実行されているポートを検出する必要があります。これを行うには、既知のポート 111 でポートマッパー プロセスを照会します。

クライアントはサービスの Sun RPC プログラム番号を送信して、ポート番号を取得します。この時点より、クライアント プログラムは Sun RPC クエリーをその新しいポートに送信します。

サーバーから応答が送信されると、ASA はこのパケットを代行受信し、そのポートで TCP と UDP の両方の初期接続を開きます。

（注） Sun RPC ペイロード情報の NAT または PAT はサポートされていません。

例

次に、RPC インスペクション エンジンをイネーブルにし、RPC トラフィックをデフォルト ポート（111）上で照合するクラスマップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して RPC インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map sunrpc-port
ciscoasa(config-cmap)# match port tcp eq 111
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map sample_policy
ciscoasa(config-pmap)# class sunrpc-port
ciscoasa(config-pmap-c)# inspect sunrpc
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy sample_policy interface outside
```

関連コマンド

コマンド	説明
clear configure sunrpc_server	**sunrpc-server** コマンドを使用して実行されている構成を削除します。
clear sunrpc-server active	Sun RPC アプリケーション インスペクションによって、NFS または NIS などの特定のサービス用に開けられているピンホールをクリアします。
show running-config sunrpc-server	Sun RPC サービス テーブル コンフィギュレーションの情報を表示します。
sunrpc-server	NFS または NIS などの Sun RPC サービス用に、タイムアウトを指定してピンホールを作成できるようにします。
show sunrpc-server active	Sun RPC サービス用に開けられているピンホールを表示します。

inspect tftp

TFTP アプリケーション インスペクションを無効にしたり、無効になっている場合に有効にしたりするには、クラス コンフィギュレーション モードで inspect **tftp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect tftp
no inspect tftp

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。

コマンド 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。

デフォルトのポート割り当ては 69 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

RFC 1350 に規定されている Trivial File Transfer Protocol（TFTP）は、TFTP サーバーとクライアント間でファイルを読み書きするための簡易プロトコルです。

ASA は TFTP トラフィックを検査し、必要に応じて動的に接続と変換を作成し、TFTP クライアントとサーバー間のファイル転送を許可します。具体的には、インスペクション エンジンは TFTP 読み取り要求（RRQ）、書き込み要求（WRQ）、およびエラー通知（ERROR）を検査します。

有効な読み取り要求（RRQ）または書き込み要求（WRQ）を受信すると、必要に応じて、ダイナミックなセカンダリ チャネルと PAT 変換が割り当てられます。このセカンダリ チャネルは、これ以降 TFTP によってファイル転送またはエラー通知用に使用されます。

TFTP サーバーだけがセカンダリ チャネル経由のトラフィックを開始できます。また、TFTP クライアントとサーバーの間に存在できる不完全なセカンダリ チャネルは1つまでです。サーバーからのエラー通知があると、セカンダリ チャネルは閉じます。

TFTP トラフィックのリダイレクトにスタティック PAT が使用されている場合は、TFTP インスペクションをイネーブルにする必要があります。

例

次に、TFTP インスペクション エンジンをイネーブルにし、TFTP トラフィックをデフォルト ポート（69）上で照合するクラス マップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して TFTP インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map tftp-port
ciscoasa(config-cmap)# match port udp eq 69
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map tftp_policy

ciscoasa(config-pmap)# class tftp-port
ciscoasa(config-pmap-c)# inspect tftp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy tftp_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect vxlan

Virtual Extensible Local Area Network（VXLAN）アプリケーション インスペクションを有効にするには、クラス コンフィギュレーション モードで **inspect vxlan** コマンドを使用します。クラス コンフィギュレーション モードは、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可能です。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。

inspect vxlan
no inspect vxlan

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。

コマンド 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。

デフォルトのポート割り当ては UDP/4789 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

Virtual Extensible Local Area Network （VXLAN）インスペクションは、ASA を通過する VXLAN のカプセル化されたトラフィックで機能します。VXLAN ヘッダー フォーマットが標準に準拠し、不正な形式のパケットをドロップすることを確認します。VXLAN インスペクションは、ASA が VXLAN トンネル エンドポイント（VTEP）または VXLAN ゲートウェイとして機能するトラフィックでは行われません。これは、それらのチェックが VXLAN パケットの通常の非カプセル化の一部として行われるためです。

VXLAN パケットは通常、ポート 4789 の UDP です。このポートは、default-inspection-traffic クラスの一部であるため、inspection_default グローバル サービス ポリシー ルールに VXLAN インスペクションを追加するだけです。または、それに対してポートまたは ACL マッチングを使用してクラスを作成することもできます。

例

次に、VXLAN インスペクションをグローバル インスペクションのデフォルト ルールの一部としてイネーブルにする例を示します。

```
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect vxlan
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect waas

WAAS アプリケーション インスペクションを有効にするには、クラス コンフィギュレーション モードで **inspect waas** コマンドを使用します。クラス コンフィギュレーション モードは、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可能です。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。

inspect waas
no inspect waas

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、デフォルトのインスペクション クラスで WAAS アプリケーション インスペクションをイネーブルにする例を示します。

```
policy-map global_policy
 class inspection_default
  inspect waas
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

inspect xdmcp

XDMCP アプリケーション インスペクションを有効にしたり、ASA がリッスンするポートを変更したりするには、クラス コンフィギュレーション モードで **inspect xdmcp** コマンドを使用します。クラス コンフィギュレーション モードはポリシー 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。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。

inspect xdmcp
no inspect xdmcp

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。

コマンド デフォルト

9.16 以降、このコマンドはデフォルトで無効になっています。以前のリリースでは、デフォルトで有効になっていました。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。このコマンドによって置き換えられた **fixup** コマンドは廃止されました。

使用上のガイドライン

inspect **xdmcp** コマンドは、XDMCP プロトコルに対するアプリケーション インスペクションを有効または無効にします。

XDMCP は、UDP ポート 177 を使用して X セッションをネゴシエートするプロトコルです。X セッションは確立時に TCP を使用します。

XWindows セッションを正常にネゴシエートして開始するために、ASA は、Xhosted コンピュータからの TCP 戻り接続を許可する必要があります。戻り接続を許可するには、ASA で **established** コマンドを使用します。XDMCP がディスプレイを送信するポートをネゴシエートすると、**established** コマンドが参照され、この戻り接続を許可すべきか確認されます。

XWindows セッション中、マネージャは予約済みポート 6000 | n 上でディスプレイ Xserver と通信します。次の端末設定を行うと、各ディスプレイは別々に Xserver と接続します。

```
setenv DISPLAY Xserver:n
```

n はディスプレイ番号です。

XDMCP が使用されている場合、ディスプレイは IP アドレスを使用してネゴシエートされます。IP アドレスは、ASA が必要に応じて NAT を行うことができます。XDCMP インスペクションでは、PAT はサポートされません。

例

次に、XDMCP インスペクション エンジンをイネーブルにし、XDMCP トラフィックをデフォルト ポート（177）上で照合するクラス マップを作成する例を示します。その後、サービス ポリシーは外部インターフェイスに適用されます。すべてのインターフェイスに対して XDMCP インスペクションを有効にするには、**interface outside** の代わりに **global** パラメータを使用します。

```
ciscoasa(config)# class-map xdmcp-port
ciscoasa(config-cmap)# match port tcp eq 177
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map xdmcp_policy

ciscoasa(config-pmap)# class xdmcp-port
ciscoasa(config-pmap-c)# inspect xdmcp
ciscoasa(config-pmap-c)# exit
ciscoasa(config)# service-policy xdmcp_policy interface outside
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
service-policy	1 つ以上のインターフェイスにポリシー マップを適用します。

int – ipu

integrity

AnyConnect IPsec 接続に使用する IKEv2 セキュリティ アソシエーション（SA）の ESP 整合性アルゴリズムを指定するには、IKEv2 ポリシー コンフィギュレーション モードで integrity コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

integrity { **md5** | **sha** | **sha256** | **sha384** | **sha512** | **null** }
no integrity { **md5** | **sha** | **sha256** | **sha384** | **sha512** | **null** }

構文の説明

md5	ESP の整合性保護のために MD5 アルゴリズムを指定します。
null	AES-GCM を暗号化アルゴリズムとして指定されている場合に管理者が IKEv2 整合性アルゴリズムとして null を選択できるようにします。
sha	（デフォルト）は、ESP の整合性保護のために米国連邦情報処理標準（FIPS）で定義されたセキュア ハッシュ アルゴリズム（SHA）SHA 1 を指定します。
sha256	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha384	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha512	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。

コマンド デフォルト

デフォルトは **sha (**SHA 1 アルゴリズム）です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。crypto ikev2 policy コマンドを入力後、**integrity** コマンドを使用して ESP プロトコルの整合性アルゴリズムを設定します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

リリース	変更内容
8.4(2)	SHA 2 をサポートするために、sha256、sha384、および sha512 の各キーワードが追加されました。
9.0(1)	IKEv2 整合性アルゴリズムとして null オプションが追加されました。

例

次に、IKEv2 ポリシー コンフィギュレーション モードを開始し、整合性アルゴリズムを MD5 に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5
```

関連コマンド

コマンド	説明
encryption	AnyConnect IPsec 接続に対して IKEv2 SA の暗号化アルゴリズムを指定します。
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
ライフタイム	AnyConnect IPsec 接続に対して IKEv2 SA の SA ライフタイムを指定します。
prf	AnyConnect IPsec 接続に対して IKEv2 SA の疑似乱数関数を指定します。

intercept-dhcp

DHCP 代行受信を有効にするには、グループ ポリシー コンフィギュレーション モードで **intercept-dhcp enable** コマンドを使用します。実行コンフィギュレーションから **intercept-dhcp** 属性を削除し、ユーザーがデフォルトまたはその他のグループポリシーから DHCP 代行受信コンフィギュレーションを継承できるようにするには、このコマンドの **no** 形式を使用します。

intercept-dhcp *netmask* { **enable** | **disable** }
no intercept-dhcp

構文の説明

disable	DHCP 代行受信をディセーブルにします。
enable	DHCP 代行受信をイネーブルにします。
netmask	トンネル IP アドレスのサブネット マスクを提供します。

コマンド デフォルト

DHCP 代行受信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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

DHCP 代行受信を無効にするには、**intercept-dhcp disable** コマンドを使用します。

スプリット トンネル オプションが 255 バイトを超えていると、Microsoft XP で異常が発生し、ドメイン名が破損します。この問題を回避するには、ASA で送信ルートの数を 27 ～ 40 に制限します。ルートの数はルートのクラスによって異なります。

DHCP 代行受信によって、Microsoft XP クライアントは ASA でスプリット トンネリングを使用できるようになります。ASA は、Microsoft Windows XP クライアント DHCP Inform メッセージに直接応答して、クライアントにトンネル IP アドレス用のサブネット マスク、ドメイン名、およびクラスレス スタティック ルートを提供します。Windows クライアントが XP 以前であ

る場合は、DHCP代行受信により、ドメイン名およびサブネットマスクが提供されます。これは、DHCP サーバーを使用するのが効果的でない環境で役立ちます。

例

次に、FirstGroupというグループ ポリシーにDHCP代行受信を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# intercept-dhcp enable
```

interface (global)

インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface** コマンドを使用します。サブ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。物理インターフェイスやマッピングインターフェイスは削除できません。

物理インターフェイスの場合（ASASM を除くすべてのモデルが対象）：

interface *physical_interface*
サブインターフェイスの場合（ASA 5505 や ASASM 、または ASA 5506-X ～ ASA 5555-X の管理インターフェイスには使用不可）：

interface { *physical_interface* | **redundant** *number* | **port-channel** *number* } **.** *subinterface*
no interface { *physical_interface* | **redundant** *number* | **port-channel** *number* } **.** *subinterface*

マルチ コンテキスト モードの場合（マッピング名が割り当てられているとき）：

interface *mapped_name*

構文の説明

mapped_name	マルチコンテキストモードで、マッピング名を **allocate-interface** コマンドを使用して割り当てた場合、その名前を指定します。
physical_interface	*type*[*slot*/]*port* という形式で物理インターフェイスのタイプ、スロット、およびポート番号を指定します。タイプとスロット/ポート間のスペースは任意です。 物理インターフェイスのタイプには、次のものがあります。 • **ethernet** • gigabitethernet • **tengigabitethernet** • **management** タイプに続けてスロット/ポートを入力します。例、**gigabitethernet 0/1**。 管理インターフェイスは、管理トラフィック専用のインターフェイスです。ただし、モデルによっては、必要に応じて通過トラフィックに使用できます（**management-only** コマンドを参照）。 インターフェイスのタイプ、スロット、およびポート番号を確認するには、モデルに付属のハードウェア マニュアルを参照してください。

subinterface	論理サブインターフェイスに指定されている 1 ～ 4294967293 の整数を指定します。サブインターフェイスの最大数は、ASA モデルによって異なります。サブインターフェイスは、ASA 5505 および や、ASA 5512-X ～ ASA 5555-X の管理インターフェイスには使用できません。プラットフォームあたりのサブインターフェイス（またはVLAN）の最大数については構成ガイドを参照してください。VLAN サブインターフェイスが 1 つ以上あるインターフェイスは、自動的に 802.1Q トランクとして設定されます。

コマンド デフォルト

ASA のデフォルトでは、すべての物理インターフェイスを対象に **interface** コマンドが自動的に生成されます。

マルチコンテキストモードでは、ASA は **allocate-interface** コマンドを使用して、コンテキストに割り当てられているすべてのインターフェイスを対象に **interface** コマンドを自動的に生成します。

インターフェイスのデフォルトの状態は、そのタイプおよびコンテキストモードによって異なります。

- マルチ コンテキスト モード、コンテキスト：システム実行スペース内でのインターフェイスの状態にかかわらず、すべての割り当て済みのインターフェイスがデフォルトでイネーブルになっています。ただし、トラフィックがインターフェイスを通過するためには、そのインターフェイスもシステム実行スペース内でイネーブルになっている必要があります。インターフェイスをシステム実行スペースでシャットダウンすると、そのインターフェイスは、それを共有しているすべてのコンテキストでダウンします。
- シングルモードまたはマルチコンテキストモード、システム：インターフェイスのデフォルトの状態は次のとおりです。
  - 物理インターフェイス：ディセーブル。
  - サブインターフェイス：イネーブル。ただし、トラフィックがサブインターフェイスを通過するためには、物理インターフェイスもイネーブルになっている必要があります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、サブインターフェイスの新しい命名規則に対応し、インターフェイス コンフィギュレーション モードでは引数が独立したコマンドとなるように変更されました。

使用上のガイドライン

インターフェイス コンフィギュレーション モードでは、インターフェイスのタイプおよびセキュリティ コンテキスト モードに応じて、ハードウェアの設定（物理インターフェイスの場合）、名前の割り当て、VLANの割り当て、IPアドレスの割り当てなど、その他多くの設定を実行できます。

有効になっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッドモードの場合には **ip address** を設定します。サブインターフェイスの場合は、**vlan** コマンドも設定します。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

ASA 5512-X ～ ASA 5555-X の Management 0/0 インターフェイスには、次の特性があります。

- 通過トラフィックはサポートされません。
- サブインターフェイスはサポートされません
- プライオリティ キューはサポートされません
- マルチキャスト MAC はサポートされません
- IPS SSP ソフトウェア モジュールによって Management 0/0 インターフェイスは共有されます。ASA と IPS モジュールに対して別の MAC アドレスと IP アドレスがサポートされます。IPS オペレーティング システムで IPS の IP アドレスのコンフィギュレーションを実行する必要があります。ただし、物理特性（インターフェイスの有効化など）は、ASA上で設定されます。

例

次に、シングル モードで物理インターフェイスのパラメータを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

次に、シングル モードでサブインターフェイスのパラメータを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
```

```
ciscoasa(config-subif)# nameif dmz1
ciscoasa(config-subif)# security-level 50
ciscoasa(config-subif)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-subif)# no shutdown
```

次に、システム コンフィギュレーション用にマルチ コンテキスト モードでインターフェイス パラメータを設定し、GigabitEthernet 0/1.1 サブインターフェイスをコンテキスト A に割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# speed 1000
ciscoasa(config-if)# duplex full
ciscoasa(config-if)# no
shutdown
ciscoasa(config-if)# interface gigabitethernet0/1.1
ciscoasa(config-subif)# vlan 101
ciscoasa(config-subif)# no shutdown
ciscoasa(config-subif)# context contextA
ciscoasa(config-ctx)# ...
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/1.1
```

次に、コンテキスト コンフィギュレーション用にマルチ コンテキスト モードでパラメータを設定する例を示します。

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# no shutdown
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
member-interface	インターフェイスを冗長インターフェイスに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
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。
vlan	サブインターフェイスに VLAN を割り当てます。

interface（vpn ロード バランシング）

VPN ロードバランシングの仮想クラスタで VPN ロードバランシング用にデフォルト以外のパブリックインターフェイスまたはプライベート インターフェイスを指定するには、VPN ロードバランシングモードで **interface** コマンドを使用します。このインターフェイス指定を削除し、デフォルトのインターフェイスに戻すには、このコマンドの **no** 形式を使用します。

interface { **lbprivate** | **lbpublic** } *interface-name*
interface { **lbprivate** | **lbpublic** }

構文の説明

interface-name	VPN ロード バランシング クラスタのパブリック インターフェイスまたはプライベート インターフェイスとして設定されるインターフェイスの名前。
lbprivate	このコマンドが VPN ロード バランシングのプライベート インターフェイスを設定することを指定します。
lbpublic	このコマンドが VPN ロード バランシングのパブリック インターフェイスを設定することを指定します。

コマンド デフォルト

interface コマンドを省略した場合、 **lbprivate** インターフェイスはデフォルトで **inside** に設定され、**lbpublic** インターフェイスはデフォルトで **outside** に設定されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
vpn ロード バランシング	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロード バランシング コンフィギュレーション モードを開始する必要があります。

また、あらかじめ **interface**、**ip address**、**nameif** の各コマンドを使用して、このコマンドで指定するインターフェイスを設定し、名前を割り当てておく必要があります。

例

次に、**vpn load-balancing** コマンドシーケンスの例を示します。シーケンス内の **interface** コマンドでは、クラスタのプライベート インターフェイスをデフォルト（inside）に戻す「test」インターフェイスとして、クラスタのパブリック インターフェイスを指定しています。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# no
 interface lbprivate
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

ciscoasa(config-load-balancing)# **participate**

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング コンフィギュレーション モードを開始します。

interface bvi

ブリッジグループのブリッジ仮想インターフェイス（BVI）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 **interface bvi** コマンドを使用します。BVI 構成を削除するには、このコマンドの **no** 形式を使用します。

interface bvi *bridge_group_number*
no interface bvi *bridge_group_number*

構文の説明

bridge_group_number	ブリッジ グループの番号を 1 ～ 100 の範囲で指定します。9.3(1) 以降では、範囲が 1 ～ 250 に拡大されています。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.3(1)	250 BVI をサポートするために数値の範囲が 1 ～ 250 に増加しました。
9.6(2)	ブリッジ グループあたりのインターフェイスの最大数が 4 から 64 に拡張されました。

使用上のガイドライン

このコマンドを使用してインターフェイス コンフィギュレーション モードを開始すると、ブリッジ グループの管理用 IP アドレスを設定できます。セキュリティ コンテキストのオーバーヘッドを避けたい場合、またはセキュリティ コンテキストを最大限に使用したい場合、インターフェイスをブリッジ グループにグループ化し、各ネットワークに1つずつ複数のブリッジ グループを設定できます。ブリッジ グループのトラフィックは他のブリッジ グループから隔離され、トラフィックはASA内の他のブリッジグループにはルーティングされません。また、トラフィックは外部ルータから ASA 内の他のブリッジ グループにルーティングされる前に、ASA から出る必要があります。ブリッジング機能はブリッジ グループごとに分かれていますが、その他の多くの機能はすべてのブリッジ グループ間で共有されます。たとえば、syslog サーバーまたは AAA サーバーの設定は、すべてのブリッジ グループで共有されます。セキュ

リティ ポリシーを完全に分離するには、各コンテキスト内に 1 つのブリッジ グループにして、セキュリティ コンテキストを使用します。コンテキストまたはシングル モードごとに、少なくとも 1 つのブリッジ グループが必要です。

ブリッジ グループにはそれぞれ管理 IP アドレスが必要です。ASA は、ブリッジ グループから発信されるパケットの送信元アドレスとしてこの IP アドレスを使用します。管理 IP アドレスは、接続されているネットワークと同じサブネット内にある必要があります。IPv4 トラフィックの場合、すべてのトラフィックを通過させるには、管理 IP アドレスが必要です。IPv6 トラフィックの場合は、少なくとも、トラフィックを通過させるリンクローカルアドレスを設定する必要があります。リモート管理などの管理操作を含めたフル機能を実現するために、グローバル管理アドレスを設定することを推奨します。他の管理方法としては、ブリッジグループとは別に管理インターフェイスを設定する方法があります。

9.2 以前では、シングル モードまたはマルチ モードのコンテキストごとに最大 8 個のブリッジ グループを設定できます。9.3(1) 以降では、最大 250 個のブリッジ グループを設定できます。各ブリッジ グループには、最大 4 つのインターフェイスを含めることができます。9.6(2) 以降では、最大 64 のインターフェイスをブリッジ グループに追加できます。同一インターフェイスを複数のブリッジ グループに割り当てることはできません。少なくとも 1 つのブリッジ グループを使用し、データ インターフェイスがブリッジ グループに属している必要があることに注意してください。

（注） ASA 5505 に複数のブリッジ グループを設定できますが、ASA 5505 のトランスペアレント モードのデータ インターフェイスは 2 つという制限は、実質的にブリッジ グループを 1 つだけ使用できることを意味します。

（注） 個別の管理インターフェイスでは、設定できないブリッジグループ（ID 301）は、設定に自動的に追加されます。このブリッジ グループはブリッジ グループの制限に含まれません。

（注） ASA では、セカンダリネットワーク上のトラフィックはサポートされていません。管理 IP アドレスと同じネットワーク上のトラフィックのみサポートされています。

例

次の例では、3 つのインターフェイスそれぞれの 2 つのブリッジ グループと管理専用インターフェイスを示します。

```
interface gigabitethernet 0/0
nameif inside
security-level 100
bridge-group 1
no shutdown
interface gigabitethernet 0/1
nameif outside
security-level 0
```

```
bridge-group 1
no shutdown
interface gigabitethernet 0/2
nameif dmz
security-level 50
bridge-group 1
no shutdown
interface bvi 1
ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
interface gigabitethernet 1/0
nameif inside
security-level 100
bridge-group 2
no shutdown
interface gigabitethernet 1/1
nameif outside
security-level 0
bridge-group 2
no shutdown
interface gigabitethernet 1/2
nameif dmz
security-level 50
bridge-group 2
no shutdown
interface bvi 2
ip address 10.3.5.8 255.255.255.0 standby 10.3.5.9
interface management 0/0
nameif mgmt
security-level 100
ip address 10.2.1.1 255.255.255.0 standby 10.2.1.2
no shutdown
```

関連コマンド

コマンド	説明
ace/bvi	ブリッジ仮想インターフェイスの設定を消去します。
bridge-group	トランスペアレント ファイアウォール インターフェイスをブリッジ グループにグループ化します。
interface	インターフェイスを設定します。
ip address	ブリッジ グループの管理 IP アドレスを設定します。
show bridge-group	メンバインターフェイスや IP アドレスなど、ブリッジ グループの情報を表示します。
show running-config interface bvi	ブリッジ グループ インターフェイス コンフィギュレーションを表示します。

interface loopback

ループバック インターフェイスを作成するには、グローバル コンフィギュレーション モードで **interface loopback** コマンドを使用します。ループバック 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。

interface loopback *number*
no interface loopback *number*

コマンド 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

次の表は、このコマンドを入力できるモードを示しています。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

使用上のガイドライン

ループバック インターフェイスは、物理インターフェイスをエミュレートするソフトウェア専用インターフェイスであり、複数の物理インターフェイスを介して到達可能です。ループバック インターフェイスは、デバイス間のトラフィックにのみ使用できます。

次の機能は、ループバック インターフェイスをサポートしています。

- AAA
- BGP
- SNMP
- SSH
- Syslog
- Telnet
- VTI 送信元インターフェイス

コマンド履歴

リリース	変更内容
9.18(2)	このコマンドが追加されました。
9.19(1)	VTIのサポートが追加されました。

例

次の例では、新しいループバック インターフェイスを作成します。

```
ciscoasa(config)# interface loopback 10
```

関連コマンド

コマンド	説明
tunnel source interface	VTI トンネルを作成するための送信元インターフェイスを指定します。
ssh	インターフェイスの SSH を設定します。
logging host	Syslog ホストを指定します。
neighbor update-source	インターフェイスを BGP スピーキングネイバーの送信元として設定します。
snmp-server host	SNMP サーバーを指定します。
telnet	インターフェイスの Telnet を設定します。

interface-policy

モニタリングでインターフェイスの障害を検出する際にフェールオーバーのポリシーを指定するには、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。

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

構文の説明

num	パーセンテージとして使用するときには 1 ～ 100 の数値を指定し、そうでなければインターフェイスの最大数として 1 を指定します。
%	（任意）*num* の数字が、モニター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。

コマンド デフォルト

ユニットに **failover interface-policy** コマンドが設定されている場合は、その値が **interface-policy failover group** コマンドのデフォルトと見なされます。そうでない場合、*num* は 1 となります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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したポリシーを満たし、他の ASA が正しく機能している場合、ASA が自らを障害発生としてマークし、フェールオーバーが発生することがあります（アクティブな ASA 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** コマンドでモニター対象として指定したインターフェイスのみです。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# interface-policy 25%
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover interface-policy	インターフェイス モニタリング ポリシーを設定します。
monitor-interface	フェールオーバーのためにモニター対象にするインターフェイスを指定します。

interface port-channel

EtherChannelインターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface port-channel** コマンドを使用します。EtherChannel 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。

interfaceport-channel*number*
no interface port-channel *number*

構文の説明

number EtherChannel チャネル グループ ID を指定します。範囲は 1 ～48 です。このインターフェイスは、チャネル グループにインターフェイスを追加したときに自動的に作成されたものです。まだインターフェイスを追加していない場合は、このコマンドを実行するとポートチャネル インターフェイスが作成されます。

（注） 少なくとも 1 つのメンバ インターフェイスをポートチャネル インターフェイスに追加してからでなければ、インターフェイスの論理パラメータ（名前など）は設定できません。

コマンド デフォルト

デフォルトでは、ポートチャネルインターフェイスはイネーブルになっています。ただし、トラフィックが EtherChannel を通過するためには、チャネル グループ物理インターフェイスもイネーブルになっている必要があります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイス コンフィギュレーション モードでは、名前や IP アドレスの割り当て、およびさまざまな設定ができます。

有効になっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッドモードの場合には **ip address** を設定します。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

（注） このコマンドは、ASA 5505 や ASASM ではサポートされません。4GE SSM（これには ASA 5550 のスロット 1 の統合 4GE SSM も含まれます）上のインターフェイスを EtherChannel の一部として使用することはできません。

インターフェイスの詳細については、CLI 設定ガイドを参照してください。

例

次の例では、3 つのインターフェイスを EtherChannel の一部として設定します。また、システム プライオリティをより高く設定するとともに、GigabitEthernet 0/2 のプライオリティを他のインターフェイスよりも高く設定します。これは、8 個を超えるインターフェイスが EtherChannel に割り当てられた場合に備えるためです。

```
ciscoasa(config)# lacp system-priority 1234
ciscoasa(config-if)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode passive
ciscoasa(config-if)# interface Port-channel1
ciscoasa(config-if)# lacp max-bundle 4
ciscoasa(config-if)# port-channel min-bundle 2
ciscoasa(config-if)# port-channel load-balance dst-ip
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。

コマンド	説明
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

interface redundant

冗長インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface redundant** コマンドを使用します。冗長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。

interface redundant *number*
no interface redundant *number*

構文の説明

number 論理冗長インターフェイス ID を指定します。範囲は 1 ～8 です。**redundant** と ID 間のスペースは任意です。

コマンド デフォルト

デフォルトでは、冗長インターフェイスはイネーブルになっています。ただし、トラフィックが冗長インターフェイスを通過するためには、メンバ物理インターフェイスもイネーブルになっている必要があります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

冗長インターフェイスは、アクティブとスタンバイの物理インターフェイスからなるペアです（**member-interface** コマンドを参照）。アクティブ インターフェイスで障害が発生すると、スタンバイ インターフェイスがアクティブになって、トラフィックを通過させ始めます。

すべての ASA コンフィギュレーションは、メンバ物理インターフェイスではなく論理冗長インターフェイスを参照します。

インターフェイス コンフィギュレーション モードでは、名前や IP アドレスの割り当て、およびさまざまな設定ができます。

有効になっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッドモードの場合には **ip address** を設定します。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

（注） このコマンドは、ASA 5505 や ASASM ではサポートされません。

インターフェイスの詳細については、CLI 設定ガイドを参照してください。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
debug redundant-interface	冗長インターフェイスのイベントまたはエラーに関するデバッグメッセージを表示します。
interface redundant	冗長インターフェイスを作成します。
member-interface	物理インターフェイスを冗長インターフェイスに割り当てます。
redundant-interface	アクティブなメンバインターフェイスを変更します。
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。

interface tunnel

新しい VTI トンネルインターフェイスを作成するには、グローバル コンフィギュレーション モードで **interface tunnel** コマンドを使用します。VTI トンネル 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。

interface tunnel *number*
no interface tunnel *number*

構文の説明

number トンネルインターフェイスに番号を割り当てます。0 から 1024 までの任意の番号を指定できます。

コマンド 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

次の表は、このコマンドを入力できるモードを示しています。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• ×	• 対応	• ×	• -

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドとそのサブモードを導入しました。
9.16(1)	デバイスごとにサポートされるトンネルインターフェイスの数が 100 から 1024 に増えました。

例

次に、新しいトンネル インターフェイスを作成する例を示します。

```
ciscoasa(config)# interface tunnel 10
```

関連コマンド

コマンド	説明
tunnel source interface	VTI トンネルを作成するための送信元インターフェイスを指定します。
tunnel destination	VTI トンネルの宛先の IP アドレスを指定します。
tunnel mode	IPsec がトンネル保護に使用されることを指定します。

コマンド	説明
tunnel protection ipsec	トンネル保護に使用される IPsec プロファイルを指定します。

interface vlan

ASA 5505 および ASASM で、VLAN インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface vlan** コマンドを使用します。VLAN 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。

interface vlan *number*
no interface vlan *number*

構文の説明

number VLAN ID を指定します。

ASA 5505 の場合、1 ～ 4090 の ID を使用します。VLAN インターフェイス ID は、デフォルトでは VLAN 1 でイネーブルになっています。

ASASM の場合は、2 ～ 1000 および 1025 ～ 4094 の ID を使用します。

コマンド デフォルト

デフォルトで、VLAN インターフェイスは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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.4(1)	ASASM のサポートが追加されました。

使用上のガイドライン

ASASM の場合、構成に任意の VLAN ID を追加できますが、トラフィックを転送できるのはスイッチによって ASA に割り当てられた VLAN だけです。ASA に割り当てられたすべての VLAN を表示するには、**show vlan** コマンドを使用します。スイッチによって ASA にまだ割り当てられていない VLAN にインターフェイスを追加した場合、そのインターフェイスはダウン ステートになります。ASA に VLAN を割り当てた時点で、インターフェイスはアップ ステートに変化します。インターフェイスステートの詳細については、**show interface** コマンドを参照してください。

インターフェイス コンフィギュレーション モードでは、名前や IP アドレスの割り当て、およびさまざまな設定ができます。

有効になっているインターフェイスでトラフィックを通過させるには、インターフェイス コンフィギュレーション モード コマンドである **nameif** を設定し、ルーテッドモードの場合には **ip address** を設定します。ASA 5505 スイッチの物理インターフェイスは、 **switchport access vlan** コマンドを使用して VLAN インターフェイスに割り当てます。

インターフェイス設定を変更し、既存接続のタイムアウトを待たずに新しいセキュリティ情報を使用する場合は、**clear local-host** コマンドを使用して接続をクリアできます。

インターフェイスの詳細については、CLI 設定ガイドを参照してください。

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。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address dhcp
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
ciscoasa(config-if)# nameif work
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# no forward interface vlan 200
ciscoasa(config-if)# nameif home
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
```

次に、 **failover lan** コマンドを使用して個別に設定されるフェールオーバー インターフェイスを含め、5 つの VLAN インターフェイスを設定する例を示します。

```
ciscoasa(config)# interface vlan 100
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 200
```

```
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.2.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 300
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.3.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface vlan 400
ciscoasa(config-if)# nameif backup-isp
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# failover lan faillink vlan500
ciscoasa(config)# failover interface ip faillink 10.4.1.1 255.255.255.0 standby 10.4.1.2
 255.255.255.0
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config-if)# switchport access vlan 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/1
ciscoasa(config-if)# switchport access vlan 200
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/2
ciscoasa(config-if)# switchport access vlan 300
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/3
ciscoasa(config-if)# switchport access vlan 400
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface ethernet 0/4
ciscoasa(config-if)# switchport access vlan 500
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
allocate-interface	インターフェイスおよびサブインターフェイスをセキュリティ コンテキストに割り当てます。
clear interface	**show interface** コマンドのカウンタをクリアします。
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。

interface vni

VXLAN ネットワーク ID（VNI）インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **interface vni** コマンドを使用します。VNI 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。

interface vni *number*
no interface vni *number*

構文の説明

number	1 ～ 10000 の範囲で ID を設定します。この ID は内部インターフェイス識別子です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

vtep-nve コマンドを使用して VNI インターフェイスと VTEP 送信元インターフェイスを関連付ける必要があります。また、VXLAN **segment-id** を設定する必要があります。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、VNI 1 インターフェイスをそれに関連付ける例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
```

```
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル（MAC アドレス テーブル）を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。

コマンド	説明
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

interim-accounting-update

AAA サーバーグループ用の RADIUS 中間アカウンティング更新メッセージの生成を有効にするには、AAA サーバー グループ コンフィギュレーション モードで **interim-accounting-update** コマンドを使用します。中間アカウンティング更新メッセージを無効にするには、このコマンドの **no** 形式を使用します。

interim-accounting-update [**periodic** [*hours*]]
no interim-accounting-update [**periodic** [*hours*]]

構文の説明

periodic [*hours*]	（オプション）対象のサーバー グループにアカウンティング レコードを送信するように設定されたすべての VPN セッションのアカウンティング レコードの定期的な生成と伝送をイネーブルにします。オプションで、これらの更新の送信間隔（時間単位）を含めることができます。デフォルトは 24 時間で、指定できる範囲は 1 ～ 120 時間です。 このオプションは、ISE 認証変更用に設定されたサーバー グループに対して使用します。

コマンド デフォルト

デフォルトでは、中間アカウンティング更新はイネーブルになりません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
aaa サーバー グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	**periodic** キーワードが追加されました。

使用上のガイドライン

periodic キーワードなしでこのコマンドを使用すると、ASA は、VPN トンネル接続がクライアントレス VPN セッションに追加されたときにのみ中間アカウンティング更新メッセージを送信します。これが発生した場合、新たに割り当てられた IP アドレスを RADIUS に通知するためのアカウンティング アップデートが生成されます。

サーバーグループを使用してリモートアクセスVPNのISE認可変更を設定する場合は、**periodic** キーワードを追加します。定期期間には、AnyConnect 接続とクライアントレス セッションが含まれます。

ISEは、ASAなどのNASデバイスから受信するアカウンティング レコードに基づいてアクティブセッションのディレクトリを保持します。ただし、セッションが依然としてアクティブなアカウンティング メッセージ（またはポスチャ トランザクション）であるという通知を 5 日間にわたって受信しない場合、ISEはセッション レコードをデータベースから削除します。長期間アクティブな VPN 接続が削除されないようにするには、すべてのアクティブ セッションに関して定期的な中間アカウンティング更新メッセージをISE送信するようにグループを設定します。

例

次の例は、ISE サーバー グループに、動的認可（CoA）のアップデートと時間ごとの定期的なアカウンティングを設定する方法を示しています。ISE によるパスワード認証を設定するトンネル グループ設定が含まれています。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

次に、ISE でローカル証明書の検証と認可用のトンネル グループを設定する例を示します。この場合、サーバーグループは認証用に使用されないため、**authorize-only** コマンドをサーバー グループ コンフィギュレーションに組み込みます。

```
ciscoasa(config)# aaa-server ise protocol radius
ciscoasa(config-aaa-server-group)# authorize-only
ciscoasa(config-aaa-server-group)# interim-accounting-update periodic 1
ciscoasa(config-aaa-server-group)# dynamic-authorization
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ise (inside) host 10.1.1.3
ciscoasa(config-aaa-server-host)# key sharedsecret
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# tunnel-group aaa-coa general-attributes
ciscoasa(config-tunnel-general)# address-pool vpn
ciscoasa(config-tunnel-general)# authentication certificate
ciscoasa(config-tunnel-general)# authorization-server-group ise
ciscoasa(config-tunnel-general)# accounting-server-group ise
ciscoasa(config-tunnel-general)# exit
```

関連コマンド

コマンド	説明
authorize-only	RADIUS サーバー グループ用の認可専用モードをイネーブルにします。

コマンド	説明
dynamic-authorization	RADIUS サーバー グループ用のダイナミック認可をイネーブルにします。

internal-password

クライアントレス SSL VPN ポータル ページで追加パスワードフィールドを表示するには、webvpn コンフィギュレーション モードで **internal-password** コマンドを使用します。この追加パスワードは、SSO を許可しているファイルサーバーに対して ASA が ユーザーを認証するために使用されます。

内部パスワードの使用を無効にするには、このコマンドの **no** 形式を使用します。

internal-passwordenable
no internal password

構文の説明

enable	内部パスワードの使用をイネーブルにします。

コマンド デフォルト

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

イネーブルにした場合、エンド ユーザーはクライアントレス SSL VPN セッションにログインするときに 2 つめのパスワードを入力します。クライアントレス SSL VPN サーバーは、HTTPS を使用して、ユーザー名やパスワードなどの SSO 認証要求を認証サーバーに送信します。認証サーバーが認証要求を承認すると、SSO 認証クッキーがクライアントレス SSL VPN サーバーに返されます。このクッキーはユーザーに代わって ASA に保持され、SSO サーバーにより保護されているドメイン内の Web サイトの安全を確保するために、ユーザー認証で使用されます。

内部パスワード機能は、内部パスワードを SSL VPN パスワードとは異なるものにする場合に便利です。特に、ASA への認証にはワンタイムパスワードを使用し、内部サイトの認証には別のパスワードを使用できます。

例

次に、内部パスワードをイネーブルにする例を示します。

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
 internal password enable
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始します。このモードではクライアントレス SSL VPN 接続の属性を設定できます。

internal-port

Azure Gateway Load Balancer（GWLB）の Azure 上の ASA Virtual の VNI インターフェイスに VXLAN 内部ポートを指定するには、インターフェイス コンフィギュレーション モードで **internal-port** コマンドを使用します。ポートを削除するには、このコマンドの **no** 形式を使用します。

internal-port *port*
no internal-port *port*

構文の説明

port ポートを 1024 ～ 65535 に設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.19(1)	このコマンドが追加されました。

使用上のガイドライン

Azure サービスチェーンでは、ASA Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

例

次の例では、Azure GWLB の VNI 1 インターフェイスを設定します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
```

```
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
external-port	外部 VXLAN ポートを設定します。
external-segment-id	VNI インターフェイスの VXLAN 外部セグメント ID を指定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
internal-segment-id	VNI インターフェイスの VXLAN 内部セグメント ID を指定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
proxy paired	インターフェイスをペアプロキシモードに設定します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNIインターフェイスをVTEP送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスはUDP ポート 4789 への VXLAN トラフィックを受け入れます。

internal-segment-id

Azure Gateway Load Balancer（GWLB）の Azure 上の ASA Virtual の VNI インターフェイスに VXLAN 内部セグメント ID を指定するには、インターフェイス コンフィギュレーション モードで **internal-segment-id** コマンドを使用します。ID を削除するには、このコマンドの **no** 形式を使用します。

internal-segment-id *id*
no internal-segment-id *id*

構文の説明

id	1 ～ 16777215 の範囲で ID を設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.19(1)	このコマンドが追加されました。

使用上のガイドライン

Azure サービスチェーンでは、ASA Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

例

次の例では、Azure GWLB の VNI 1 インターフェイスを設定します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
```

```
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
external-port	外部 VXLAN ポートを設定します。
external-segment-id	VNI インターフェイスの VXLAN 外部セグメント ID を指定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
internal-port	内部 VXLAN ポートを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
proxy paired	インターフェイスをペアプロキシモードに設定します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNIインターフェイスをVTEP送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスはUDP ポート 4789 への VXLAN トラフィックを受け入れます。

interval maximum

DDNS 更新方式による更新試行の最大間隔を設定するには、DDNS 更新方式モードで **interval** コマンドを使用します。実行コンフィギュレーションから DDNS 更新方式の間隔を削除するには、このコマンドの **no** 形式を使用します。

interval maximum *days hours minutes seconds*
no interval maximum *days hours minutes seconds*

構文の説明

days	更新試行間の日数を 0 ～ 364 の範囲で指定します。
hours	更新試行間の時間数を 0 ～ 23 の範囲で指定します。
minutes	更新試行間の分数を 0 ～ 59 の範囲で指定します。
seconds	更新試行間の秒数を 0 ～ 59 の範囲で指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
DDNS 更新方式コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

日、時間、分、および秒を足すと、間隔の合計時間になります。

例

次に、3 分 15 秒ごとに更新を試行する方式を ddns-2 という名前で設定する例を示します。

```
ciscoasa(config)# ddns update method ddns-2
ciscoasa(DDNS-update-method)# interval maximum 0 0 3 15
```

関連コマンド

コマンド	説明
ddns	作成済みの DDNS 方式に対して、DDNS アップデート方式のタイプを指定します。
ddns update	DDNS アップデート方式を ASA のインターフェイスまたは DDNS アップデートホスト名に関連付けます。
ddns update method	DNS のリソース レコードをダイナミックにアップデートするための方式を作成します。
dhcp-client update dns	DHCP クライアントが DHCP サーバーに渡すアップデート パラメータを設定します。
dhcpd update dns	DHCP サーバーによる DDNS アップデートの実行をイネーブルにします。

invalid-ack

ACK が無効になっているパケットに対するアクションを設定するには、tcp-map コンフィギュレーション モードで **invalid-ack** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、 **set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

invalid-ack { **allow** | **drop** }
no invalid-ack

構文の説明

allow	ACK が無効になっているパケットを許可します。
drop	ACK が無効になっているパケットをドロップします。

コマンド デフォルト

デフォルト アクションは、ACK が無効になっているパケットをドロップすることです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(4)/8.0(4)	このコマンドが追加されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1. **tcp-map**：TCP 正規化アクションを指定します。
    1. **invalid-ack**：tcp マップ コンフィギュレーション モードでは、 **invalid-ack** コマンドおよびその他数多くのコマンドを入力できます。
2. **class-map**：TCP 正規化を実行するトラフィックを指定します。
3. **policy-map**：各クラスマップに関連付けるアクションを指定します。
    1. **class**：アクションを実行するクラスマップを指定します。
    2. **set connection advanced-options**：作成した TCP マップを識別します。

4. **service-policy**：ポリシーマップをインターフェイスごとに、またはグローバルに割り当てます。

次のような場合に無効な ACK が検出される可能性があります。

- TCP 接続が SYN-ACK-received ステータスでは、受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号と同じでない場合、その ACK は無効です。
- 受信した TCP パケットの ACK 番号が次の TCP パケット送信のシーケンス番号より大きい場合は常に、その ACK は無効です。

（注） 無効な ACK を含む TCP パケットは、WAAS 接続で自動的に許可されます。

例

次に、ACK が無効になっているパケットを許可するように ASA を設定する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# invalid-ack allow
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match any
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシーのトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
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。

ip address

インターフェイスの IP アドレス（ルーテッドモード）や、ブリッジ仮想インターフェイス（BVI）（ルーテッドモードまたはトランスペアレントモード）を設定するには、インターフェイス コンフィギュレーション モードで **ip address** 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。

ip address *ip_address* [*mask*] **standby** *ip_address* | **cluster-pool** *poolname*]
no ip address [*ip_address*]

構文の説明

cluster-pool *poolname*	（任意）ASA クラスタリングの場合に、**ip local pool** コマンドで定義されたアドレスのクラスタプールを設定します。*ip_address* 引数で定義されたメインクラスタの IP アドレスは、現在のマスターユニットにのみ属します。各クラスタ メンバには、このプールからローカル IP アドレスが割り当てられます。 各ユニットに割り当てられるアドレスは、事前に正確に特定できません。各ユニットで使用されているアドレスを表示するには、**show ip local pool** *poolname* コマンドを入力します。各クラスタ メンバには、クラスタに参加したときにメンバ ID が割り当てられます。この ID によって、プールから使用されるローカル IP が決定します。
ip_address	インターフェイスの IP アドレス。
mask	（任意）IP アドレスのサブネットマスク。マスクを設定しない場合、ASA では IP アドレスクラスのデフォルトマスクが使用されます。
standby *ip_address*	（オプション）フェールオーバーの場合に、スタンバイ ユニットの IP アドレスを設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	ルーテッド モードの場合、このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モードのコマンドに変更されました。
8.4(1)	トランスペアレント モード用にブリッジ グループが追加されました。BVI の IP アドレスを設定し、グローバルには設定しません。
9.0(1)	ASA クラスタリングをサポートするために、**cluster-pool** キーワードが追加されました。
9.7(1)	ルーテッドインターフェイスに関しては、ポイントツーポイント接続向けの31 ビットのサブネット に IP アドレスを設定できます。

使用上のガイドライン

このコマンドはこの他、フェールオーバーのスタンバイ アドレスを設定します。

マルチ コンテキスト モードのガイドライン

シングル コンテキスト ルーテッド ファイアウォール モードでは、各インターフェイス アドレスはそれぞれ固有のサブネットに存在する必要があります。マルチ コンテキスト モードでは、このインターフェイスが共有インターフェイスにある場合、各 IP アドレスはそれぞれ固有であるものの、同じサブネットに存在する必要があります。インターフェイスが固有のものである場合、この IP アドレスを必要に応じて他のコンテキストで使用できます。

トランスペアレント ファイアウォールのガイドライン

トランスペアレント ファイアウォールは、IP ルーティングに参加しません。ASA に必要な唯一の IP 構成は、BVI アドレスの設定です。このアドレスが必要になるのは、システムメッセージや AAA サーバーとの通信などで発信されるトラフィックの送信元アドレスとして、ASA がこのアドレスを使用するためです。このアドレスは、リモート管理アクセスにも使用できます。このアドレスは、上流のルータおよび下流のルータと同じサブネットに存在する必要があります。マルチ コンテキスト モードの場合、各コンテキスト内の管理 IP アドレスを設定します。管理インターフェイスを含むモデルの場合は、このインターフェイスの IP アドレスを管理用に設定することもできます。

フェールオーバーのガイドライン

スタンバイ IP アドレスは、メイン IP アドレスと同じサブネットに存在する必要があります。

ASA クラスタリングのガイドライン

個々のインターフェイスのクラスタプールは、クラスタ インターフェイス モードを個別に設定（**cluster-interface mode individual** コマンド）しないと設定できません。唯一の例外は管理専用インターフェイスです。

- 管理専用インターフェイスはいつでも、個別インターフェイスとして設定できます（スパンド EtherChannel モードのときでも）。管理インターフェイスは、個別インターフェイスとすることができます（トランスペアレント ファイアウォール モードのときでも）。

- スパンド EtherChannel モードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミック ルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。

/31 サブネットのガイドライン

ルーテッド インターフェイスに関しては、ポイントツーポイント接続向けの 31 ビットのサブネットに IP アドレスを設定できます。31 ビット サブネットには 2 つのアドレスのみが含まれます。通常、サブネットの最初と最後のアドレスはネットワーク用とブロードキャスト用に予約されており、2 アドレス サブネットは使用できません。ただし、ポイントツーポイント接続があり、ネットワーク アドレスやブロードキャスト アドレスが不要な場合は、IPv4 形式でアドレスを保持するのに 31 サブネット ビットが役立ちます。たとえば、2 つの ASA 間のフェールオーバー リンクに必要なアドレスは 2 つだけです。リンクの一方の側から送信されるパケットはすべてもう一方の側で受信され、ブロードキャスティングは必要ありません。また、SNMP や Syslog を実行する管理ステーションを直接接続することもできます。

- 31 ビット サブネットとクラスタリング：スパンド EtherChannel に 31 ビット サブネット マスクを使用できます。個々のインターフェイス（スパンド EtherChannel モードの管理 IP アドレスを含む）は 31 ビット サブネットをサポートしていません。また、クラスタ制御リンクにも 31 ビット サブネットを使用できません。
- 31 ビット サブネットとフェールオーバー：フェールオーバーに関しては、ASA インターフェイスの IP アドレスに 31 ビットのサブネットを使用した場合、アドレスが不足しているため、インターフェイス用のスタンバイ IP アドレスは設定できません。通常、アクティブなユニットがインターフェイスのテストを実行し、スタンバイのインターフェイスの健全性を保証できるよう、フェールオーバー インターフェイスはスタンバイ IP アドレスを必要とします。スタンバイ IP アドレスがないと、ASA はネットワークのテストを実行できず、リンク ステートのみしか追跡できません。ポイントツーポイント接続であるフェールオーバーと任意のステートリンクでは、31 ビットのサブネットも使用できます。
- 31 ビット サブネットと管理：直接接続されている管理ステーションがあれば、ASA 上で SSH または HTTP にポイントツーポイント接続を、または管理ステーション上で SNMP または Syslog にポイントツーポイント接続をそれぞれ使用できます。
- 31 ビット サブネットをサポートしていない機能：次の機能は、31 ビット サブネットをサポートしていません。
  - ブリッジ グループ用 BVI インターフェイス：ブリッジ グループには BVI、2 つのブリッジ グループ メンバーに接続された 2 つのホスト用に、少なくとも 3 つのホスト アドレスが必要です。/29 サブネット以下を使用する必要があります。
  - マルチキャスト ルーティング

例

次に、2 つのインターフェイスの IP アドレスおよびスタンバイ アドレスを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2
ciscoasa(config-if)# nameif inside
```

```
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/3
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0 standby 10.1.2.2
ciscoasa(config-if)# no shutdown
```

次に、ブリッジ グループ 1 の管理アドレスおよびスタンバイ アドレスを設定する例を示します。

```
ciscoasa(config)# interface bvi 1
ciscoasa(config-if)# ip address 10.1.3.1 255.255.255.0 standby 10.1.3.2
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、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。
ip address dhcp	インターフェイスで DHCP サーバーから IP アドレスを取得できるように設定します。
show ip address	インターフェイスに割り当てられた IP アドレスを表示します。

ip address dhcp

DHCP を使用してインターフェイスの IP アドレスを取得するには、インターフェイス コンフィギュレーション モードで **ip address dhcp** コマンドを使用します。このインターフェイスの DHCP クライアントを無効にするには、このコマンドの **no** 形式を使用します。

ip address dhcp [**setroute**]
no ip address dhcp

構文の説明

setroute （任意）ASA が DHCP サーバーから提供されるデフォルトルートを使用できるようにします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モード コマンドに変更されました。このコマンドは、外部インターフェイスだけでなく、任意のインターフェイスもイネーブルにできます。

使用上のガイドライン

DHCP リースをリセットし、新規リースを要求するには、このコマンドを再入力します。

ip address dhcp コマンドを入力する前に、**no shutdown** コマンドを使用してインターフェイスを有効にしていない場合、一部の DHCP 要求が送信されないことがあります。

（注） ASA はタイムアウトが 32 秒未満のリースを拒否します。

例

次に、Gigabitethernet0/1 インターフェイスで DHCP をイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# ip address dhcp
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、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。
ip address	インターフェイスの IP アドレス、またはトランスペアレント ファイアウォールの管理 IP アドレスを設定します。
show ip address dhcp	DHCP サーバーから取得された IP アドレスを示します。

ip address pppoe

PPPoE を有効にするには、インターフェイス コンフィギュレーション モードで **ip address pppoe** コマンドを使用します。PPPoE を無効にするには、このコマンドの **no** 形式を使用します。

ip address [*ip_address* [*mask*]] **pppoe** [**setroute**]
no ip address [*ip_address* [*mask*]] **pppoe**

構文の説明

ip_address	IP アドレスを PPPoE サーバーから受信するのではなく手動で設定します。
mask	IP アドレスのサブネット マスクを指定します。マスクを設定しない場合、ASA では IP アドレスクラスのデフォルトマスクが使用されます。
setroute	ASA が、PPPoE サーバーから提供されるデフォルトルートを使用できるようにします。PPPoE サーバーがデフォルトルートを送信しない場合、ASA はアクセスコンセントレータのアドレスをゲートウェイとするデフォルトルートを作成します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

PPPoE は、イーサネットと PPP という広く受け入れられている 2 つの標準を結合して、IP アドレスをクライアント システムに割り当てる認証方式を提供します。ISP は、既存のリモート アクセス インフラストラクチャを使用して高速ブロードバンド アクセスをサポートするためと、顧客の使い勝手向上のために、PPPoE を配置します。

PPPoE を使用して IP アドレスを設定する前に、**vpdn** コマンドでユーザー名、パスワード、および認証プロトコルを設定します。複数のインターフェイスでこのコマンドをイネーブルにした場合（たとえば、ISP へのバックアップ リンク用）は、pppoe client vpdn group コマンドを使

用して、必要に応じて各インターフェイスをそれぞれ異なるVPDNグループに割り当てることができます。

最大伝送単位（MTU）サイズは、自動的に 1492 バイトに設定されます。これは、イーサネット フレーム内で PPPoE 伝送を許可する正しい値です。

PPPoE セッションをリセットして再起動するには、このコマンドを再入力します。

このコマンドは、**ip address** コマンドまたは **ip address dhcp** コマンドと同時には設定できません。

例

次に、GigabitEthernet 0/1 インターフェイスで PPPoE をイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address pppoe
ciscoasa(config-if)# no shutdown
```

次に、PPPoE インターフェイスの IP アドレスを手動で設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 pppoe
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、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。
ip address	インターフェイスの IP アドレスを設定します。
pppoe client vpdn group	このインターフェイスを特定の VPDN グループに割り当てます。
show ip address pppoe	PPPoE サーバーから取得された IP アドレスを表示します。
vpdn group	VPDN グループを作成し、PPPoE クライアントを設定します。

ip-address-privacy

IP アドレスのプライバシーを有効にするには、パラメータ コンフィギュレーション モードで **ip-address-privacy** 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。

ip-address-privacy
no ip-address-privacy

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、SIP インスペクション ポリシー マップで SIP を経由する IP アドレスのプライバシーをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ip-address-privacy
```

関連コマンド

コマンド	説明
policy-map type inspect	インスペクション 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。

ip audit attack

攻撃シグネチャーに一致するパケットに対してデフォルトアクションを設定するには、グローバル コンフィギュレーション モードで **ip audit attack** コマンドを使用します。（接続をリセットするために）デフォルトアクションを復元するには、このコマンドの **no** 形式を使用します。

ip audit attack [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit attack

構文の説明

action （任意）一連のデフォルト アクションを定義することを指定します。このキーワードの後にアクションを指定しない場合、ASA はアクションを実行しません。**action** キーワードを入力しない場合、ASA ではキーワードが入力されたものと見なされ、**action** キーワードが構成に記述されます。

alarm （デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。

drop （任意）パケットをドロップします。

reset （任意）パケットをドロップし、接続を閉じます。

コマンド デフォルト

デフォルト アクションは、送信し、アラームを生成することです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

アクションは複数指定することも、まったく指定しないこともできます。このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドでアクションを指定しない場合、このコマンドで設定したアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次に、攻撃シグニチャに一致するパケットに対してアラームを生成し、リセットするデフォルト アクションを設定する例を示します。内部インターフェイスの監査ポリシーは、アラームのみにするようにこのデフォルトを上書きしますが、外部インターフェイスのポリシーは **ip audit attack** コマンドで設定されたデフォルト設定を使用します。

```
ciscoasa(config)# ip audit attack action alarm reset
ciscoasa(config)# ip audit name insidepolicy attack action alarm
ciscoasa(config)# ip audit name outsidepolicy attack
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit info	情報シグニチャに一致するパケットのデフォルトアクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit attack	**ip audit attack** コマンドの設定を表示します。

ip audit info

情報シグニチャに一致するパケットに対してデフォルトアクションを設定するには、グローバル コンフィギュレーション モードで **ip audit info** コマンドを使用します。（アラームを生成するために）デフォルトアクションを復元するには、このコマンドの **no** 形式を使用します。アクションは複数指定することも、まったく指定しないこともできます。

ip audit info [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit info

構文の説明

action （任意）一連のデフォルト アクションを定義することを指定します。このキーワードの後にアクションを指定しない場合、ASA はアクションを実行しません。**action** キーワードを入力しない場合、ASA ではキーワードが入力されたものと見なされ、**action** キーワードが構成に記述されます。

alarm （デフォルト）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。

drop （任意）パケットをドロップします。

reset （任意）パケットをドロップし、接続を閉じます。

コマンド デフォルト

デフォルト アクションは、アラームを生成することです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドで設定するアクションは、**ip audit name** コマンドを使用して監査ポリシーを設定すると上書きできます。**ip audit name** コマンドでアクションを指定しない場合、このコマンドで設定したアクションが使用されます。

シグニチャのリストについては、**ip audit signature** コマンドを参照してください。

例

次に、情報シグニチャに一致するパケットに対してアラームを生成し、リセットするデフォルト アクションを設定する例を示します。内部インターフェイスの監査ポリシーは、アラームを生成し、ドロップするようにこのデフォルトを上書きしますが、外部インターフェイスのポリシーは **ip audit info** コマンドで設定されたデフォルト設定を使用します。

```
ciscoasa(config)# ip audit info action alarm reset
ciscoasa(config)# ip audit name insidepolicy info action alarm drop
ciscoasa(config)# ip audit name outsidepolicy info
ciscoasa(config)# ip audit interface inside insidepolicy
ciscoasa(config)# ip audit interface outside outsidepolicy
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルトアクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit info	**ip audit info** コマンドの設定を表示します。

ip audit interface

監査ポリシーをインターフェイスに割り当てるには、グローバル コンフィギュレーション モードで **ip audit interface** コマンドを使用します。インターフェイスからポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit interface *interface_name policy_name*
no ip audit interface *interface_name policy_name*

構文の説明

interface_name	インターフェイス名を指定します。
policy_name	**ip audit name** コマンドで追加したポリシーの名前。各インターフェイスに info ポリシーおよび attack ポリシーを割り当てることができます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、監査ポリシーを内部インターフェイスおよび外部インターフェイスに適用する例を示します。

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルトアクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルトアクションを設定します。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
ip audit signature	シグニチャをディセーブルにします。
show running-config ip audit interface	**ip audit interface** コマンドの設定を表示します。

ip audit name

パケットが定義済みの攻撃シグネチャーまたは情報シグニチャに一致したときに実行するアクションを識別する名前付き監査ポリシーを作成するには、グローバル コンフィギュレーション モードで **ip audit name** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

ip audit name *name* { **info** | **attack** } [**action** [**alarm**] [**drop**] [**reset**]]
no ip audit name *name* { **info** | **attack** } [**action** [**alarm**] [**drop**] [**reset**]]

構文の説明

action （任意）一連のアクションを定義することを指定します。このキーワードの後にアクションを指定しない場合、ASA はアクションを実行しません。**action** キーワードを入力しないと、ASA は **ip audit attack** コマンドおよび **ip audit info** コマンドによって設定されたデフォルトアクションを使用します。

alarm （任意）パケットがシグニチャに一致したことを示すシステム メッセージを生成します。

attack 攻撃シグニチャの監査ポリシーを作成します。パケットは、DoS 攻撃や不正な FTP コマンドなど、ネットワークでの攻撃の一部となる可能性があります。

drop （任意）パケットをドロップします。

info 情報シグニチャの監査ポリシーを作成します。パケットは、現時点ではネットワークを攻撃していませんが、ポート スイープなど情報収集アクティビティの一部である可能性があります。

name ポリシーの名前を設定します。

reset （任意）パケットをドロップし、接続を閉じます。

コマンド デフォルト

ip audit attack および **ip audit info** コマンドを使用してデフォルトアクションを変更しなかった場合、攻撃シグネチャーおよび情報シグニチャのデフォルトアクションでアラームが生成されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

シグニチャは、既知の攻撃パターンに一致するアクティビティです。たとえば、DoS 攻撃に一致するシグニチャがあります。ポリシーを適用するには、**ip audit interface** コマンドを使用して、そのポリシーをインターフェイスに割り当てます。各インターフェイスに info ポリシーおよび attack ポリシーを割り当てることができます。

シグニチャのリストについては、 **ip audit signature** コマンドを参照してください。

トラフィックがシグニチャに一致した場合、そのトラフィックに対してアクションを実行するには、**shun** コマンドを使用して、問題のホストからの新たな接続を阻止し、既存の接続からのパケットの受信を禁止します。

例

次に、内部インターフェイスには攻撃シグニチャおよび情報シグニチャに関するアラームを生成する監査ポリシーを設定し、外部インターフェイスには攻撃に備えて接続をリセットする監査ポリシーを設定する例を示します。

```
ciscoasa(config)# ip audit name insidepolicy1 attack action alarm
ciscoasa(config)# ip audit name insidepolicy2 info action alarm
ciscoasa(config)# ip audit name outsidepolicy1 attack action reset
ciscoasa(config)# ip audit name outsidepolicy2 info action alarm
ciscoasa(config)# ip audit interface inside insidepolicy1
ciscoasa(config)# ip audit interface inside insidepolicy2
ciscoasa(config)# ip audit interface outside outsidepolicy1
ciscoasa(config)# ip audit interface outside outsidepolicy2
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルトアクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルトアクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit signature	シグニチャをディセーブルにします。
shun	特定の送信元アドレスおよび宛先アドレスでパケットをブロックします。

ip audit signature

監査ポリシーに対してシグニチャを無効にするには、グローバル コンフィギュレーション モードで **ip audit signature** コマンドを使用します。シグニチャを再び有効にするには、このコマンドの **no** 形式を使用します。

ip audit signature *signature_number* **disable**
no ip audit signature *signature_number*

構文の説明

disable	シグニチャをディセーブルにします。
signature_number	ディセーブルにするシグニチャ番号を指定します。サポートされているシグニチャのリストについては、表 2 : シグニチャ ID とシステム メッセージ番号 を参照してください。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

正規のトラフィックが頻繁にシグニチャに一致する場合には、シグニチャをディセーブルにしてみてください。リスクが伴うことを承知でシグニチャをディセーブルにすると、多数のアラームを回避できます。表 2 : シグニチャ ID とシステム メッセージ番号 に、サポートされているシグニチャおよびメッセージ番号の一覧を示します。

表 *2:* シグニチャ *ID* とシステム メッセージ番号

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1000	400000	IP options-Bad Option List	情報	IP データグラム ヘッダーの IP オプションのリストが不完全であるか、または不正な形式になっている IP データグラムを受信するとトリガーされます。IP オプションのリストには、さまざまなネットワーク管理タスクまたはデバッグ タスクを実行するオプションが 1 つ以上含まれています。
1001	400001	IP options-Record Packet Route	情報	データグラムの IP オプション リスト中にオプション 7（記録パケット ルート）を含む IP データグラムを受信するとトリガーされます。
1002	400002	IP options-Timestamp	情報	データグラムの IP オプション リスト中にオプション 4（タイムスタンプ）を含む IP データグラムを受信するとトリガーされます。
1003	400003	IP options-Security	情報	データグラムの IP オプション リスト中にオプション 2（セキュリティ オプション）を含む IP データグラムを受信するとトリガーされます。
1004	400004	IP options-Loose Source Route	情報	データグラムの IP オプション リスト中にオプション 3（緩慢な送信元ルート）を含む IP データグラムを受信するとトリガーされます。
1005	400005	IP options-SATNET ID	情報	データグラムの IP オプション リスト中にオプション 8（SATNET ストリーム ID）を含む IP データグラムを受信するとトリガーされます。
1006	400006	IP options-Strict Source Route	情報	データグラムの IP オプション リスト中にオプション 2（厳密な送信元ルーティング）を含む IP データグラムを受信するとトリガーされます。
1100	400007	IP Fragment 攻撃	攻撃	オフセット フィールドのオフセット値が 0 より大きく 5 未満になっている IP データグラムを受信するとトリガーされます。
1102	400008	IP Impossible Packet	攻撃	送信元と宛先が同じアドレスになっている IP パケットが到着するとトリガーされます。このシグニチャは、いわゆる Land Attack を捕捉します。

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
1103	400009	IP Overlapping Fragments（Teardrop）	攻撃	同じ IP データグラム内に含まれている 2 つのフラグメントのオフセット値が、そのデータグラム内の位置決めを共有していることを示す場合にトリガーされます。これは、フラグメント A がフラグメント B によって完全に上書きされること、またはフラグメント A がフラグメント B によって部分的に上書きされることを意味する場合があります。オペレーティング システムによっては、このように重複するフラグメントが正しく処理されず、重複フラグメントを受信すると例外をスローしたり、他の不適切な動作を行ったりします。Teardrop 攻撃では、これにより DoS 状態を引き起こします。
2000	400010	ICMP Echo Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 0（エコー応答）に設定された IP データグラムを受信するとトリガーされます。
2001	400011	ICMP Host Unreachable	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 3（ホスト到達不能）に設定された IP データグラムを受信するとトリガーされます。
2002	400012	ICMP Source Quench	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 4（ソース クエンチ）に設定された IP データグラムを受信するとトリガーされます。
2003	400013	ICMP Redirect	情報	P ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 5（リダイレクト）に設定された IP データグラムを受信するとトリガーされます。
2004	400014	ICMP Echo Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 8（エコー要求）に設定された IP データグラムを受信するとトリガーされます。
2005	400015	ICMP Time Exceeded for a Datagram	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 11（データグラムの超過時間）に設定された IP データグラムを受信するとトリガーされます。

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2006	400016	ICMP Parameter Problem on Datagram	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 12（データグラムのパラメータ問題）に設定された IP データグラムを受信するとトリガーされます。
2007	400017	ICMP Timestamp Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 13（タイムスタンプ要求）に設定された IP データグラムを受信するとトリガーされます。
2008	400018	ICMP Timestamp Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 14（タイムスタンプ応答）に設定された IP データグラムを受信するとトリガーされます。
2009	400019	ICMP Information Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 15（情報要求）に設定された IP データグラムを受信するとトリガーされます。
2010	400020	ICMP Information Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 16（ICMP 情報応答）に設定された IP データグラムを受信するとトリガーされます。
2011	400021	ICMP Address Mask Request	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 17（アドレス マスク要求）に設定された IP データグラムを受信するとトリガーされます。
2012	400022	ICMP Address Mask Reply	情報	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、ICMP ヘッダーのタイプ フィールドが 18（アドレス マスク応答）に設定された IP データグラムを受信するとトリガーされます。
2150	400023	Fragmented ICMP Traffic	攻撃	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、他にも 1（ICMP）に設定されたフラグメント フラグが存在するか、またはオフセットフィールドにオフセット値が指定されている IP データグラムを受信するとトリガーされます。
2151	400024	Large ICMP Traffic	攻撃	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、IP 長が 1024 より大きくなっている IP データグラムを受信するとトリガーされます。

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
2154	400025	Ping of Death Attack	攻撃	IP ヘッダーのプロトコル フィールドが 1（ICMP）に設定され、最終フラグメント ビットが設定され、さらに（IP オフセット * 8）+（IP データ長）が 65535 を超えている場合、つまり IP オフセット（このフラグメントの元のパケットでの開始位置を表し、かつ 8 バイト単位であるもの）にパケットの残りを加えた値が、IP パケットの最大サイズを超えている IP データグラムを受信するとトリガーします。
3040	400026	TCP NULL flags	攻撃	SYN、FIN、ACK、または RST のいずれのフラグも設定されていない 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3041	400027	TCP SYN+FIN flags	攻撃	SYN および FIN のフラグが設定されている 1 つの TCP パケットが特定のホストに送信されるとトリガーされます。
3042	400028	TCP FIN only flags	攻撃	1 つの孤立 TCP FIN パケットが特定のホストの特権ポート（ポート番号が 1024 未満）に送信されるとトリガーされます。
3153	400029	FTP Improper Address Specified	情報	要求側ホストと異なるアドレスを指定して port コマンドが発行された場合にトリガーされます。
3154	400030	FTP Improper Port Specified	情報	1024 未満または 65535 より大きい値のデータ ポートを指定して port コマンドが発行された場合にトリガーされます。
4050	400031	UDP Bomb attack	攻撃	指定されている UDP 長が、指定されている IP 長より短い場合にトリガーされます。この不正な形式のパケット タイプは、サービス拒絶攻撃と関連付けられています。
4051	400032	UDP Snork attack	攻撃	送信元ポートが 135、7、または 19 のいずれかで、宛先ポートが 135 になっている UDP パケットが検出されるとトリガーされます。
4052	400033	UDP Chargen DoS attack	攻撃	このシグニチャは、送信元ポート 7 および宛先ポート 19 において UDP パケットが検出されるとトリガーされます。
6050	400034	DNS HINFO Request	情報	DNS サーバーから HINFO レコードへのアクセスが試みられるとトリガーされます。
6051	400035	DNS Zone Transfer	情報	送信元ポートが 53 の通常の DNS ゾーン転送が実行されるとトリガーされます。

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6052	400036	DNS Zone Transfer from High Port	情報	送信元ポートが 53 以外のときに不正な DNS ゾーン転送が発生するとトリガーされます。
6053	400037	DNS Request for All Records	情報	すべてのレコードに対する DNS 要求があるとトリガーされます。
6100	400038	RPC Port Registration	情報	ターゲット ホストで新しい RPC サービスを登録する試みがあるとトリガーされます。
6101	400039	RPC Port Unregistration	情報	ターゲット ホストで既存の RPC サービスを登録解除する試みがあるとトリガーされます。
6102	400040	RPC Dump	情報	ターゲット ホストに対して RPC ダンプ要求が発行されるとトリガーされます。
6103	400041	Proxied RPC Request	攻撃	ターゲット ホストのポートマッパーにプロキシ RPC 要求が送信されるとトリガーされます。
6150	400042	ypserv (YP server daemon) Portmap Request	情報	YP サーバー デーモン（ypserv）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6151	400043	ypbind (YP bind daemon) Portmap Request	情報	YP バインド デーモン（ypbind）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6152	400044	yppasswdd (YP password daemon) Portmap Request	情報	YP パスワード デーモン（yppasswdd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6153	400045	ypupdated (YP update daemon) Portmap Request	情報	YP 更新デーモン（ypupdated）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6154	400046	ypxfrd (YP transfer daemon) Portmap Request	情報	YP 転送デーモン（ypxfrd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6155	400047	mountd (mount daemon) Portmap Request	情報	マウント デーモン（mountd）ポートのポートマッパーに対して要求が行われるとトリガーされます。
6175	400048	rexd (remote execution daemon) Portmap Request	情報	リモート実行デーモン（rexd）ポートのポートマッパーに対して要求が行われるとトリガーされます。

シグニチャ ID	メッセージ番号	シグニチャ タイトル	シグニチャ タイプ	説明
6180	400049	rexd (remote execution daemon) Attempt	情報	rexd プログラムの呼び出しが行われるとトリガーされます。リモート実行デーモンは、プログラムをリモート実行する役割を担うサーバーです。rexd プログラムの呼び出しは、システム リソースへの不正アクセスの試みを示唆している場合があります。
6190	400050	statd Buffer Overflow	攻撃	サイズの大きな statd 要求が送信されるとトリガーされます。これは、バッファをオーバーフローさせてシステムへアクセスしようとする試みの可能性があります。

例

次に、シグニチャ 6100 をディセーブルにする例を示します。

```
ciscoasa(config)# ip audit signature 6100 disable
```

関連コマンド

コマンド	説明
ip audit attack	攻撃シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit info	情報シグニチャに一致するパケットのデフォルト アクションを設定します。
ip audit interface	監査ポリシーをインターフェイスに割り当てます。
ip audit name	パケットが攻撃シグニチャまたは情報シグニチャに一致した場合に実行するアクションを指定する、名前付き監査ポリシーを作成します。
show running-config ip audit signature	**ip audit signature** コマンドの設定を表示します。

ip-client

FXOS での管理トラフィックの開始と、Firepower 2100 ASA データインターフェイスから外部への送信を許可するには、グローバル コンフィギュレーション モードで **ip-client** コマンドを使用します。トラフィックの開始を無効にするには、このコマンドの **no** 形式を使用します。

ip-client*interface_name*
no ip-client *interface_name*

構文の説明

interface_name FXOS が管理トラフィックを送信できるインターフェイス名を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.8(2)	このコマンドが追加されました。

使用上のガイドライン

ASA データ インターフェイスで FXOS 管理トラフィック開始を有効にすることができます。これは、たとえば、SNMP トラップ、NTP と DNS のサーバ アクセスなどに必要です。着信管理トラフィックについては、**fxos permit** コマンドを参照してください。

FXOS の設定で、デフォルト ゲートウェイが 0.0.0.0 に設定されていることを確認します。これは ASA をゲートウェイとして設定します。FXOS **set out-of-band** コマンドを参照してください。

例

次のコマンドにより、外部インターフェイスを介して FXOS トラフィックを開始できます。

```
ciscoasa(config)# ip-client outside
```

関連コマンド

コマンド	説明
connect fxos	ASA CLI から FXOS CLI に接続します。
fxos permit	ASA データ インターフェイスでの FXOS 管理アクセスを許可します。
fxos port	FXOS 管理アクセス ポートを設定します。

ip-comp

LZS IP 圧縮を有効にするには、グループ ポリシー コンフィギュレーション モードで **ip-comp enable** コマンドを使用します。IP 圧縮を無効にするには、**ip-comp disable** コマンドを使用します。実行コンフィギュレーションから **ip-comp** 属性を削除するには、このコマンドの **no** 形式を使用します。

ip-comp { **enable** | **disable** }
no ip-comp

構文の説明

disable	IP 圧縮をディセーブルにします。
enable	IP 圧縮をイネーブルにします。

コマンド デフォルト

IP 圧縮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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの **no** 形式を使用すると、別のグループポリシーから値を継承できます。データ圧縮をイネーブルにすると、モデムで接続するリモート ダイヤルイン ユーザーのデータ伝送レートが向上する場合があります。

⚠

注意 データ圧縮を使用すると、各ユーザーセッションのメモリ要件と CPU 使用率が高くなり、結果として ASA 全体のスループットが低下します。そのため、データ圧縮はモデムで接続しているリモート ユーザーに対してだけイネーブルにすることを推奨します。モデム ユーザーに固有のグループ ポリシーを設計し、それらのユーザーに対してだけ圧縮をイネーブルにします。

エンドポイントで IP 圧縮トラフィックが生成される場合、パケットの不正な圧縮解除を防ぐために、IP 圧縮をディセーブルにする必要があります。特定の LAN-to-LAN トンネルで IP 圧縮がイネーブルになっている場合、トンネルの一方からもう一方に IP 圧縮データを渡そうとするときに、ホスト A はホスト B と通信できません。

（注） **ip-comp** コマンドが無効で、「暗号化前」の処理として IPsec フラグメンテーションが設定されている場合、IPsec 圧縮（ip-comp_option と pre-encryption）は使用できません。暗号化チップに送信される IP ヘッダーが圧縮によってあいまいになり、暗号化チップによる着信パケットの処理時にエラーが生成されるためです。この場合は、MTU レベルをチェックして少量（600 バイトなど）であることを確認してください。

例

次に、「FirstGroup」というグループ ポリシーの IP 圧縮をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-comp enable
```

ip local pool

IP アドレスプールを設定するには、グローバル コンフィギュレーション モードで **ip local pool** コマンドを使用します。アドレスプールを削除するには、このコマンドの **no** 形式を使用します。

ip local pool *poolname first-address-last-address* [**mask** *mask*]
no ip local pool *poolname*

構文の説明

first-address	IP アドレスの範囲における開始アドレスを指定します。
last-address	IP アドレスの範囲における最終アドレスを指定します。
mask *mask*	（任意）アドレスプールのサブネットマスクを指定します。255.255.255.254（/31）または 255.255.255.255（/32）サブネットマスクは使用できません。
poolname	IP アドレス プールの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ASA クラスタリングをサポートするために、クラスタプールの IP ローカルプールが追加されました（**ip address** コマンド）。

使用上のガイドライン

VPN クライアントに割り当てられた IP アドレスが標準以外のネットワークに属しているときには、マスク値を指定する必要があります。デフォルトマスクを使用した場合には、データが誤ってルーティングされることがあります。典型的な例が、IP ローカル プールに 10.10.10.0/255.255.255.0 アドレスが含まれている場合で、これはデフォルトではクラス A ネットワークです。この結果、VPN クライアントが異なるインターフェイス経由で 10 ネットワーク内の別のサブネットにアクセスする必要がある場合には、ある種のルーティング問題が発生することがあります。たとえば、アドレス 10.10.100.1/255.255.255.0 のプリンタがインターフェ

イス 2 を介して使用できるようになっているものの、10.10.10.0 ネットワークが VPN トンネルを経由するためインターフェイス 1 で使用できるようになっている場合、VPN クライアントはプリンタ宛てのデータのルーティング先を正確に把握できなくなります。10.10.10.0 と 10.10.100.0 のサブネットは両方とも、10.0.0.0 クラス A ネットワークに分類されるため、プリンタ データが VPN トンネル経由で送信される可能性があります。

例

次に、firstpool という名前で IP アドレス プールを設定する例を示します。開始アドレスは 10.20.30.40 で、最終アドレスは 10.20.30.50 です。ネットワーク マスクは 255.255.255.0 です。

```
ciscoasa(config)# ip local pool firstpool 10.20.30.40-10.20.30.50 mask 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure ip local pool	すべての IP ローカル プールを削除します。
show running-config ip local pool	IP プール コンフィギュレーションを表示します。特定の IP アドレス プールを指定するには、その名前をコマンドに含めます。

ip unnumbered

インターフェイス（ループバック インターフェイスなど）から IP アドレスを借用または継承するには、インターフェイス コンフィギュレーション モードで **ip unnumbered** コマンドを使用します。インターフェイスからの IP アドレスの継承を停止するには、このコマンドの **no** 形式を使用します。

ip unnumbered *interface-name*
no ip unnumbered

構文の説明

interface-name	IP アドレスを引き継ぐインターフェイスの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.19(1)	このコマンドが追加されました。

使用上のガイドライン

ip unnumbered コマンドは、選択したインターフェイスの IP アドレスを現在のインターフェイスのアドレスとして継承するために使用されます。

例

次に、ループバック インターフェイスから IP アドレスを借りる例を示します。

```
ciscoasa(config)# interface tunnel 1

ciscoasa(conf-if)# ip unnumbered loopback1
```

関連コマンド

コマンド	説明
ipv6 unnumbered *interface-name*	指定されたインターフェイスの IPv6 アドレスを継承します。

コマンド	説明
interface loopback *loopback-number*	ループバック インターフェイスを作成します。

ip-phone-bypass

IP Phone Bypass を有効にするには、グループ ポリシー コンフィギュレーション モードで **ip-phone-bypass enable** コマンドを使用します。実行コンフィギュレーションから IP Phone Bypass 属性を削除するには、このコマンドの **no** 形式を使用します。

ip-phone-bypass { **enable** | **disable** }
no ip-phone-bypass

構文の説明

disable	IP Phone Bypass をディセーブルにします。
enable	IP Phone Bypass をイネーブルにします。

コマンド デフォルト

IP Phone Bypass 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

IP Phone Bypass を無効にするには、**ip-phone-bypass disable** コマンドを使用します。このコマンドオプションの **no** 形式を使用すると、別のグループポリシーから IP Phone Bypass の値を継承できます。

IP Phone Bypass を使用すると、ハードウェア クライアントの背後にある IP フォンが、ユーザー認証プロセスなしで接続できます。イネーブルの場合、セキュア ユニット認証は有効のままになります。

IP Phone Bypass は、ユーザー認証をイネーブルにした場合にだけ設定する必要があります。

また、**mac-exempt** オプションを設定してクライアントの認証を免除する必要があります。詳細については、**vpnclient mac-exempt** コマンドを参照してください。

例

次の例は、FirstGroup というグループ ポリシーに対して IP Phone Bypass をイネーブルにする方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ip-phone-bypass enable
```

関連コマンド

コマンド	説明
user-authentication	ハードウェアクライアントの背後にいるユーザーに対して、接続前にASAに識別情報を示すように要求します。

ips

検査のために ASA から AIP SSM にトラフィックを迂回させるには、クラス コンフィギュレーション モードで **ips** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

ips { **inline** | **promiscuous** } { **fail-close** | **fail-open** } [**sensor** { *sensor_name* | *mapped_name* }]
no ips { **inline** | **promiscuous** } { **fail-close** | **fail-open** } [**sensor** { *sensor_name* | *mapped_name* }]

構文の説明

fail-close	AIP SSM の障害発生時にトラフィックをブロックします。
fail-open	AIP SSM の障害発生時にトラフィックを許可します。
inline	パケットを AIP SSM に向けて送ります。パケットは、IPS が動作した結果、ドロップされる場合があります。
promiscuous	AIP SSM のパケットを複製します。元のパケットは AIP SSM でドロップできません。
sensor {*sensor_name* | *mapped_name* }	このトラフィックの仮想センサー名を設定します。AIP SSM（バージョン 6.0 以降）で仮想センサーを使用する場合は、この引数を使用してセンサー名を指定できます。使用可能なセンサー名を参照するには、**ips ... sensor ?** コマンドを入力します。使用可能なセンサーの一覧が表示されます。**show ips** コマンドも使用できます。 ASA でマルチコンテキストモードを使用する場合は、コンテキストに割り当てたセンサーのみを指定できます（**allocate-ips** コマンドを参照）。コンテキストで設定する場合は、*mapped_name* 引数を使用します。 センサー名を指定しないと、トラフィックはデフォルトのセンサーを使用します。マルチ コンテキスト モードでは、コンテキストのデフォルトのセンサーを指定できます。シングルモードの場合、またはマルチモードでデフォルト センサーを指定しない場合、トラフィックでは AIP SSM で設定されているデフォルト センサーが使用されます。 AIP SSM にまだ存在しない名前を入力すると、エラーになり、コマンドは拒否されます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	仮想センサーのサポートが追加されました。

使用上のガイドライン

ASA 5500 シリーズは AIP SSM をサポートします。AIP SSM は、プロアクティブでフル機能の侵入防御サービスを提供する高度な IPS ソフトウェアを実行して、ワームやネットワークウイルスなど悪意のあるトラフィックを停止し、ネットワークに影響が及ばないようにします。ASA で **ips** コマンドを設定する前または後に、AIP SSM でセキュリティポリシーを設定します。ASA（**session** コマンド）から AIP SSM にセッションするか、管理インターフェイスで SSH または Telnet を使用して AIP SSM に直接接続できます。または、ASDM を使用できます。AIP SSM の設定の詳細については、コマンド ライン インターフェイスを使用した Cisco Intrusion Prevention System Sensor の設定 [英語] を参照してください。

ips コマンドを設定するには、まず **class-map**　コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

AIP SSM は ASA から個別のアプリケーションを実行します。ただし、AIP SSM/SSC は ASA のトラフィック フローに統合されます。AIP SSM には、管理インターフェイス以外の外部インターフェイス自体は含まれません。ASA でトラフィッククラスの **ips** コマンドを適用すると、トラフィックは次のように ASA と AIP SSM を通過します。

1. トラフィックが ASA に入ります。
2. ファイアウォール ポリシーが適用されます。
3. トラフィックがバックプレーン経由で AIP SSM に送信されます（**inline** キーワードを使用。トラフィックのコピーを AIP SSM に送信するだけの場合は、**promiscuous** キーワードを参照してください）。
4. AIP SSM が、セキュリティポリシーをトラフィックに適用し、適切なアクションを実行します。
5. 有効なトラフィックがバックプレーン経由で ASA に返送されます。AIP SSM が、セキュリティポリシーに従ってトラフィックをブロックすることがあり、ブロックされたトラフィックは渡されません。

6. VPN ポリシーが適用されます（設定されている場合）。
7. トラフィックが ASA を出ます。

例

次に、無差別モードですべての IP トラフィックを AIP SSM に迂回させ、何らかの理由で AIP SSM カードで障害が発生した場合はすべての IP トラフィックをブロックする例を示します。

```
ciscoasa(config)# access-list IPS permit ip any any
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list IPS
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips promiscuous fail-close
ciscoasa(config-pmap-c)# service-policy my-ips-policy global
```

次に、インラインモードで 10.1.1.0 ネットワークおよび 10.2.1.0 ネットワーク宛てのすべての IP トラフィックを AIP SSM に迂回させ、何らかの理由で AIP SSM カードで障害が発生た場合はすべてのトラフィックを許可する例を示します。my-ips-class トラフィックにはセンサー 1 が使用され、my-ips-class2 トラフィックにはセンサー 2 が使用されます。

```
ciscoasa(config)# access-list my-ips-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-ips-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-ips-class
ciscoasa(config-cmap)# match access-list my-ips-acl
ciscoasa(config)# class-map my-ips-class2
ciscoasa(config-cmap)# match access-list my-ips-acl2
ciscoasa(config-cmap)# policy-map my-ips-policy
ciscoasa(config-pmap)# class my-ips-class
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor1
ciscoasa(config-pmap)# class my-ips-class2
ciscoasa(config-pmap-c)# ips inline fail-open sensor sensor2
ciscoasa(config-pmap-c)# service-policy my-ips-policy interface outside
```

関連コマンド

コマンド	説明
allocate-ips	セキュリティ コンテキストに仮想センサーを割り当てます。
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。
class-map	ポリシー マップ用にトラフィックを識別します。
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。
show running-config policy-map	現在のすべてのポリシーマップ コンフィギュレーションを表示します。

ipsec-udp

IPsec over UDP を有効にするには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp enable** コマンドを使用します。現在のグループポリシーから IPsec over UDP 属性を削除するには、このコマンドの **no** 形式を使用します。

ipsec-udp { **enable** | **disable** }
no ipsec-udp

構文の説明

disable	IPsec over UDP をディセーブルにします。
enable	IPsec over UDP をイネーブルにします。

コマンド デフォルト

IPsec over UDP 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの **no** 形式を使用すると、別のグループポリシーから IPsec over UDP の値を継承できます。

IPsec over UDP（IPsec through NAT と呼ばれることもある）を使用すると、Cisco VPN Client またはハードウェアクライアントは、NAT を実行している ASA に UDP 経由で接続できます。

IPsec over UDP を無効にするには、**ipsec-udp disable** コマンドを使用します。

IPsec over UDP を使用するには、**ipsec-udp-port** コマンドも設定する必要があります。

また、IPsec over UDP を使用するように Cisco VPN Client を設定しておく必要があります（Cisco VPN Client は、デフォルトで IPsec over UDP を使用するように設定されています）。VPN 3002 では、IPsec over UDP を使用するためのコンフィギュレーションが必要ありません。

IPsec over UDP は独自仕様で、リモートアクセス接続にだけ適用され、モードコンフィギュレーションが必要です。つまり、ASA は SA のネゴシエーション中にクライアントとコンフィギュレーション パラメータを交換します。

IPSec over UDP を使用すると、システム パフォーマンスが若干低下します。

ipsec-udp-port コマンドは、VPN クライアントとして動作する ASA 5505 ではサポートされません。クライアント モードの ASA 5505 では、UDP ポート 500 または 4500 で IPsec セッションを開始できます。

例

次に、FirstGroup というグループ ポリシーの IPsec over UDP を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp enable
```

関連コマンド

コマンド	説明
ipsec-udp-port	ASA が UDP トラフィックをリッスンするポートを指定します。

ipsec-udp-port

IPsec over UDP の UDP ポート番号を設定するには、グループ ポリシー コンフィギュレーション モードで **ipsec-udp-port** コマンドを使用します。UDP ポートを無効にするには、このコマンドの **no** 形式を使用します。

ipsec-udp-port*port*
noipsec-udp-port

構文の説明

port	4001 ～ 49151 の範囲内の整数を使用して、UDP ポート番号を識別します。

コマンド デフォルト

デフォルトのポートは 10000 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの **no** 形式を使用すると、別のグループポリシーから IPsec over UDP ポートの値を継承できます。

IPSec ネゴシエーションでは、ASA は設定されたポートでリッスンし、他のフィルタルールで UDP トラフィックがドロップされていても、そのポート宛ての UDP トラフィックを転送します。

この機能をイネーブルにすると、複数のグループ ポリシーを設定し、各グループ ポリシーでそれぞれ別のポート番号を使用できます。

例

次に、FirstGroup というグループ ポリシーの IPsec UDP ポートをポート 4025 に設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# ipsec-udp-port 4025
```

関連コマンド

コマンド	説明
ipsec-udp	Cisco VPN Client またはハードウェアクライアントが、NAT を実行している ASA に UDP 経由で接続できるようにします。

ipv – ir

ipv4-prefix

マッピングアドレスおよびポート（MAP）ドメイン内の基本マッピングルールの IPv4 プレフィックスを設定するには、MAP ドメインの基本マッピング ルール コンフィギュレーション モードで **ipv4-prefix** コマンドを使用します。プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

ipv4-prefix*ipv4_network_addressnetmask*
no ipv4-prefix *ipv4_network_address netmask*

構文の説明

ipv4_network_address netmask	カスタマー エッジ（CE）デバイスの IPv4 アドレス プールを定義する IPv4 プレフィックス。ネットワーク アドレスとサブネット マスク（たとえば、192.168.3.0 255.255.255.0）を指定します。異なる MAP ドメインで同じ IPv4 プレフィックスを使用することはできません。

コマンド デフォルト

デフォルト設定はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
MAP ドメインの基本マッピング ルール コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(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

IPv4 プレフィックスは、カスタマー エッジ（CE）デバイスの IPv4 アドレス プールを定義します。CE デバイスは、最初に IPv4 アドレスを、IPv4 プレフィックスによって定義されたプール内のアドレス（およびポート番号）に変換します。次に、MAP は、デフォルトのマッピング ルールのプレフィックスを使用して、この新しいアドレスを IPv6 アドレスに変換します。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート（MAP）ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート（MAP）ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

ipv6 address

IPv6 を有効にし、インターフェイスで IPv6 アドレスを設定（ルーテッドモード）したり、ブリッジグループまたは管理インターフェイスアドレスの IPv6 アドレスを設定（トランスペアレントモード）したりするには、**ipv6 address** コマンドを使用します。IPv6 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。

ipv6 prefix { **autoconfig** [**autoconfig** [**default trust** { **dhcp** | **ignore** }] | **dhcp** [**defualt**] | *ipv6_address* | *prefix_name ipv6_address* | *prefix_length* | *ipv6_address* **link-local** [**standby** *ipv6_adress*] }
no ipv6 prefix { **autoconfig** [**autoconfig** [**default trust** { **dhcp** | **ignore** }] | **dhcp** [**defualt**] | *ipv6_address* | *prefix_name ipv6_address* | *prefix_length* | *ipv6_address* **link-local** [**standby** *ipv6_adress*] }

構文の説明

autoconfig	インターフェイスでステートレスな自動設定をイネーブルにします。インターフェイスでステートレスな自動設定をイネーブルにすると、ルータ アドバタイズメント メッセージで受信したプレフィックスに基づいて IPv6 アドレスが設定されます。ステートレスな自動設定がイネーブルになっている場合、インターフェイスのリンクローカル アドレスは、Modified EUI-64 インターフェイス ID に基づいて自動的に生成されます。トランスペアレント ファイアウォール モードではサポートされません。 （注） RFC 4862 では、ステートレスな自動設定に設定されたホストはルータ アドバタイズメント メッセージを送信しないと規定していますが、ASA はこの場合、ルータ アドバタイズメント メッセージを送信します。メッセージを抑制するには、**ipv6 nd suppress-ra** コマンドを参照してください。
cluster-pool *poolname*	（任意）ASA クラスタリングの場合に、**ipv6 local pool** コマンドで定義されたアドレスのクラスタプールを設定します。引数で定義されたメイン クラスタの IP アドレスは、現在のマスター ユニットだけに属します。各クラスタ メンバには、このプールからローカル IP アドレスが割り当てられます。 各ユニットに割り当てられるアドレスは、事前に正確に特定できません。各ユニットで使用されているアドレスを表示するには、**show ipv6 local pool** *poolname* コマンドを入力します。各クラスタ メンバには、クラスタに参加したときにメンバ ID が割り当てられます。この ID によって、プールから使用されるローカル IP が決定します。
default	（オプション）ルータ アドバタイズメントからデフォルト ルートを取得します。

default trust	（オプション）ルータ アドバタイズメントからデフォルトルートをインストールします。
dhcp (autoconfig)	（オプション）信頼できる送信元から（言い換えると、IPv6 アドレスを提供した同じサーバーから）取得されたルータ アドバタイズメントからのデフォルト ルートのみを ASA が使用することを指定します。
dhcp	DHCPv6 サーバーから IPv6 アドレスを取得します。
ignore	（オプション）別のネットワークからルータ アドバタイズメントを取得できる（よりリスクの高い方法となる可能性がある）ことを指定します。
ipv6_address/prefix_length	インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。
ipv6_prefix/prefix_length **eui-64**	Modified EUI-64 形式を使用してインターフェイスの MAC アドレスから生成されたインターフェイス ID と、指定されたプレフィックスを結合することによって、インターフェイスにグローバル アドレスを割り当てます。グローバル アドレスを割り当てると、インターフェイスのリンクローカル アドレスが自動的に作成されます。>*prefix-length* 引数に指定されている値が 64 ビットを超えている場合は、プレフィックス ビットがインターフェイス ID よりも優先されます。指定したアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。 スタンバイ アドレスを指定する必要はありません。インターフェイス ID が自動的に生成されます。 Modified EUI-64 形式のインターフェイス ID は、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）の間に 16 進数の FFFE を挿入することで、48 ビット リンク層（MAC）アドレスから導出されます。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

ipv6_address **link-local**	手動でリンクローカル アドレスだけを設定します。このコマンドに指定された *ipv6_address* は、インターフェイス用に自動的に生成されるリンクローカルアドレスを上書きします。リンクローカルアドレスは、リンクローカル プレフィックス FE80::/64 と Modified EUI-64 形式のインターフェイス ID で形成されます。MAC アドレスが 00E0.B601.3B7A のインターフェイスの場合、リンクローカルアドレスは FE80::2E0:B6FF:FE01:3B7A になります。指定したアドレスを別のホストが使用している場合は、エラー メッセージが表示されます。
prefix_name *ipv6_address/prefix_length*	委任されたプレフィックスを使用します。この機能は、ASA インターフェイスに DHCPv6 プレフィクス委任クライアントを有効にさせる（**ipv6 dhcp client pd**）ために必要です。通常、委任されたプレフィクスは /60 以下であるため、複数 /64 ネットワークにサブネット化できます。接続されるクライアント用に SLAAC をサポートする必要がある場合は、/64 がサポートされるサブネット長です。/60 サブネットを補完するアドレス（1:0:0:0:1 など）を指定する必要があります。プレフィックスが /60 未満の場合は、アドレスの前に :: を入力します。たとえば、委任されたプレフィクスが 2001:DB8:1234:5670::/60 である場合、このインターフェイスに割り当てられるグローバル IP アドレスは 2001:DB8:1234:5671::1/64 です。ルータ アドバタイズメントでアドバタイズされるプレフィクスは 2001:DB8:1234:5671::/64 です。この例では、プレフィクスが /60 未満である場合、プレフィックスの残りのビットは、前に配置される :: によって示されるように、0 になります。たとえば、プレフィクスが 2001:DB8:1234::/48 である場合、IPv6 アドレスは 2001:DB8:1234::1:0:0:0:1/64 になります。
standby *ipv6_address*	（任意）フェールオーバーペアのセカンダリ ユニットまたはフェールオーバー グループで使用されるインターフェイス アドレスを指定します。

コマンド デフォルト

IPv6 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。
8.2(2)	スタンバイ アドレスのサポートが追加されました。
8.4(1)	トランスペアレント モード用にブリッジ グループが追加されました。BVI の IP アドレスを設定し、グローバルには設定しません。
9.0(1)	ASA クラスタリングをサポートするために、**cluster-pool** キーワードが追加されました。
9.6(2)	次のオプションが追加されました。 • **autoconfig default trust** {**dhcp** | **ignore**} • **dhcp** [**default**] • *prefix_name ipv6_address/prefix_length*

使用上のガイドライン

インターフェイスに IPv6 アドレスを設定すると、そのインターフェイスで IPv6 が有効になります。IPv6 アドレスを指定した後で **ipv6 enable** コマンドを使用する必要はありません。

マルチ コンテキスト モードのガイドライン

シングル コンテキスト ルーテッド ファイアウォール モードでは、各インターフェイス アドレスはそれぞれ固有のサブネットに存在する必要があります。マルチ コンテキスト モードでは、このインターフェイスが共有インターフェイスにある場合、各 IP アドレスはそれぞれ固有であるものの、同じサブネットに存在する必要があります。インターフェイスが固有のものである場合、この IP アドレスを必要に応じて他のコンテキストで使用できます。

DHCPv6 およびプレフィクス委任オプションは、マルチ コンテキスト モードではサポートされていません。

トランスペアレント ファイアウォールのガイドライン

トランスペアレント モードでは、IPv6 アドレスの手動設定のみがサポートされています。トランスペアレント ファイアウォールは、IP ルーティングに参加しません。ASA に必要な唯一の IP 構成は、BVI アドレスの設定です。このアドレスが必要になるのは、システムメッセージや AAA サーバーとの通信などで発信されるトラフィックの送信元アドレスとして、ASA がこのアドレスを使用するためです。このアドレスは、リモート管理アクセスにも使用できます。このアドレスは、上流のルータおよび下流のルータと同じサブネットに存在する必要があります。マルチ コンテキスト モードの場合、各コンテキスト内の管理 IP アドレスを設定します。管理インターフェイスを含むモデルの場合は、このインターフェイスの IP アドレスを管理用に設定することもできます。

フェールオーバーのガイドライン

スタンバイ IP アドレスは、メイン IP アドレスと同じサブネットに存在する必要があります。

ASA クラスタリングのガイドライン

個々のインターフェイスのクラスタプールは、クラスタ インターフェイス モードを個別に設定（**cluster-interface mode individual**）しないと設定できません。唯一の例外は管理専用インターフェイスです。

- 管理専用インターフェイスはいつでも、個別インターフェイスとして設定できます（スパンドEtherChannelモードのときでも）。管理インターフェイスは、個別インターフェイスとすることができます（トランスペアレント ファイアウォール モードのときでも）。
- スパンドEtherChannelモードでは、管理インターフェイスを個別インターフェイスとして設定すると、管理インターフェイスに対してダイナミック ルーティングをイネーブルにできません。スタティック ルートを使用する必要があります。

DHCPv6 およびプレフィクス委任オプションは、クラスタリングではサポートされていません。

例

次に、選択したインターフェイスのグローバルアドレスとして2001:0DB8:BA98::3210/64を割り当て、スタンバイ ユニットの対応するインターフェイスのアドレスとして2001:0DB8:BA98::3211 を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 address 2001:0DB8:BA98::3210/64 standby 2001:0DB8:BA98::3211
```

次に、選択したインターフェイスに自動的にIPv6 アドレスを割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 address autoconfig
```

次に、IPv6 プレフィックス 2001:0DB8:BA98::/64 を選択したインターフェイスに割り当て、アドレスの下位64 ビットにEUI-64 インターフェイスID を指定する例を示します。このデバイスがフェールオーバーペアの一部である場合、**standby** キーワードは指定する必要がありません。スタンバイアドレスは、Modified EUI-64 インターフェイスID を使用して自動的に作成されます。

```
ciscoasa(config)# interface gigabitethernet 0/2
ciscoasa(onfig-if)# ipv6 address 2001:0DB8:BA98::/64 eui-64
```

次に、選択したインターフェイスのリンクレベル アドレスとしてFE80::260:3EFF:FE11:6670 を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local
```

次に、フェールオーバーペアのプライマリ ユニットで選択したインターフェイスのリンクレベル アドレスとしてFE80::260:3EFF:FE11:6670 を割り当て、セカンダリ ユニットの対応するインターフェイスのリンクレベルアドレスとしてFE80::260:3EFF:FE11:6671を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/3
ciscoasa(config-if)# ipv6 address FE80::260:3EFF:FE11:6670 link-local standby
FE80::260:3EFF:FE11:6671
```

次に、委任されたプレフィクスを補完するためのアドレスとして ::1:0:0:0:1/64 を割り当てる例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/5
ciscoasa(config-if)# ipv6 address Outside-Prefix ::1:0:0:0:1/64
```

関連コマンド

コマンド	説明
debug ipv6 interface	IPv6 インターフェイスのデバッグ情報を表示します。
show ipv6 interface	IPv6 用に設定されたインターフェイスのステータスを表示します。

ipv6-address-pool

アドレスをリモートクライアントに割り当てるための IPv6 アドレスプールのリストを指定するには、トンネルグループ一般属性コンフィギュレーション モードで **ipv6-address-pool** コマンドを使用します。IPv6 アドレスプールを削除するには、このコマンドの **no** 形式を使用します。

ipv6-address-pool [（ *interface_name* ）] *ipv6_address_pool* [*...ipv6_address_pool6*]
no ipv6-address-pool [（ *interface_name* ）] *ipv6_address_pool* [*...ipv6_address_pool6*]

構文の説明

interface_name	（任意）アドレス プールに使用するインターフェイスを指定します。
ipv6_address_pool	**ipv6 local pool** コマンドで設定したアドレスプールの名前を指定します。最大 6 個のローカル アドレス プールを指定できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

これらのコマンドは、インターフェイスごとに 1 つずつ、複数入力できます。インターフェイスが指定されていない場合、コマンドは明示的に参照されていないインターフェイスすべてに対してデフォルトを指定します。

グループポリシーの **ipv6-address-pools** コマンドによる IPv6 アドレスプールの設定により、トンネルグループの **ipv6-address-pool** コマンドによる IPv6 アドレスプールの設定が上書きされます。

プールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

例

次に、トンネル グループ一般属性コンフィギュレーション モードを開始し、IPsec リモート アクセス トンネル グループ テスト用に、アドレスをリモート クライアントに割り当てるための IPv6 アドレス プール リストを指定する例を示します。

```
ciscoasa(config)# tunnel-group test type remote-access
ciscoasa(config)# tunnel-group test general-attributes
ciscoasa(config-tunnel-general)# ipv6-address-pool (inside) ipv6addrpool1 ipv6addrpool2
 ipv6addrpool3
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
ipv6-address-pools	グループ ポリシーの IPv6 アドレス プール設定を設定します。これらの設定は、トンネル グループの IPv6 アドレス プール設定を上書きします。
ipv6 local pool	VPN リモート アクセス トンネルに使用する IP アドレス プールを設定します。
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group	トンネル グループを設定します。

ipv6-address-pools

アドレスをリモートクライアントに割り当てるための IPv6 アドレスプールリストを最大 6 つ指定するには、グループポリシー属性コンフィギュレーション モードで **ipv6-address-pools** コマンドを使用します。グループポリシーから属性を削除し、別のグループポリシーソースからの継承をイネーブルにするには、このコマンドの **no** 形式を使用します。

ipv6-address-pools value *ipv6_address_poll1*［ *...ipv6_address_pool6* ］
no ipv6-address-pools value *ipv6_address_poll1*［ *...ipv6_address_pool6* ］
ipv6-address-poolsnone
noipv6-address-poolsnone

構文の説明

ipv6_address_pool	**ipv6 local pool** コマンドで設定した最大 6 つの IPv6 アドレスプールの名前を指定します。各 IPv6 アドレス プール名を区切るには、スペースを使用します。
none	IPv6 アドレス プールが設定されず、他のグループ ポリシーからの継承をディセーブルにすることを指定します。
value	アドレスを割り当てるための IPv6 アドレス プールを最大 6 つ指定します。

コマンド デフォルト

デフォルトでは、IPv6 アドレス プールの属性は設定されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

IPv6 アドレスプールを設定するには、**ipv6 local pool** コマンドを使用します。

ipv6-address-pools コマンドにおけるプールの指定順序は重要です。ASA では、このコマンドでプールを指定した順序に従って、それらのプールからアドレスが割り当てられます。

ipv6-address-pools none コマンドは、ポリシーの別のソース（DefaultGrpPolicy など）からこの属性を継承することを無効にします。**no ipv6-address-pools none** コマンドは、**ipv6-address-pools none** コマンドを構成から削除して、継承を許可するためにデフォルト値に戻します。

例

次に、グループポリシー属性コンフィギュレーションモードを開始し、アドレスをリモートクライアントに割り当てるために使用される IPv6 アドレス プールを firstipv6pool という名前で設定し、そのプールを GroupPolicy1 に関連付ける例を示します。

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1000/32 100
ciscoasa(config)# group-policy GroupPolicy1 attributes
ciscoasa(config-group-policy)# ipv6-
address-pools value firstipv6pool
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
ipv6 local pool	VPN グループ ポリシーに使用される IPv6 アドレス プールを設定します。
clear configure group-policy	設定されているすべてのグループポリシーをクリアします。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。

ipv6 dhcp client pd

DHCPv6プレフィクス委任クライアントを有効にし、インターフェイスで取得されるプレフィックスに名前を付けるには、インターフェイス コンフィギュレーション モードで**ipv6 dhcp client pd** コマンドを使用します。クライアントを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp client pd *name*
no ipv6 dhcp client pd *name*

構文の説明

name このプレフィックスの名前を設定します。名前には最大 200 文字を使用できます。プレフィックス（**ipv6 address** *prefix_name*）を使用してインターフェイスに IP アドレスを割り当てるときに、この名前を使用します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

1 つ以上のインターフェイスで DHCPv6 プレフィクス委任クライアントをイネーブルにします。ASA は、サブネット化して内部ネットワークに割り当てることができる 1 つ以上の IPv6 プレフィックスを取得します。通常、プレフィックス委任クライアントをイネーブルにしたインターフェイスは DHCPv6 アドレス クライアントを使用して IP アドレスを取得し、その他の ASA インターフェイスだけが、委任されたプレフィックスから取得されるアドレスを使用します。

この機能は、クラスタリングではサポートされていません。

この機能は管理専用インターフェイスでは設定できません。

例

次に、GigabitEthernet 0/0 で DHCPv6 アドレスクライアントおよびプレフィックス委任クライアントを設定した後に、アドレスをプレフィックスとともに GigabitEthernet 0/1 および 0/2 に割り当てる例を示します。

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。

コマンド	説明
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

ipv6 dhcp client pd hint

受信する委任されたプレフィクスに関する 1 つ以上のヒントを提供するには、インターフェイス コンフィギュレーション モードで **ipv6 dhcp client pd hint** コマンドを使用します。クライアントを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcp client pd hint *ipv6_prefix / prefix_length*
no ipv6 dhcp client pd hint *ipv6_prefix / prefix_length*

構文の説明

ipv6_prefix/prefix_length	受信する IPv6 プレフィックスとプレフィックス長を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

通常、特定のプレフィクス長（::/60 など）を要求しますが、以前に特定のプレフィックスを受信しており、リースの期限が切れるときにそれを確実に再取得したい場合は、そのプレフィックスの全体をヒントとして入力できます。複数のヒント（異なるプレフィックスまたはプレフィックス長）を入力すると、どのヒントに従うのか、またはそもそもヒントに従うのかどうかが DHCP サーバーによって決定されます。

例

次に、GigabitEthernet 0/0 で DHCPv6 アドレスクライアントおよびプレフィックス委任クライアントを設定した後に、アドレスをプレフィックスとともに GigabitEthernet 0/1 および 0/2 に割り当てる例を示します。

```
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
ipv6 dhcp client pd hint ::/60
```

```
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。

コマンド	説明
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

ipv6 dhcp pool

DHCPv6 サーバーからステートレスアドレス自動設定（SLAAC）クライアントに提供させる情報を含む IPv6 DHCP プールを設定するには、グローバル コンフィギュレーション モードで **ipv6 dhcp pool** コマンドを使用します。プールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 dhcp pool *pool_name*
no ipv6 dhcp pool *pool_name*

構文の説明

pool_name	プールの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

SLAAC をプレフィックス委任機能とともに使用するクライアントについては、情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、 **ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、このプール名を指定します。必要に応じてインターフェイスごとに個別のプールを設定できます。また、複数のインターフェイスで同じプールを使用することもできます。 **ipv6 dhcp pool** コマンドを入力した後に、クライアントに提供する 1 つ以上のパラメータを設定できます。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

ipv6 dhcprelay enable

インターフェイスでDHCPv6リレーサービスを無効にするには、グローバルコンフィギュレーション モードで **ipv6 dhcprelay enable** コマンドを使用します。DHCPv6 リレーサービスを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 dhcprelay enable *interface*
no ipv6 dhcprelay enable *interface*

構文の説明

interface	宛先の出力インターフェイスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、インターフェイスで DHCPv6 リレー サービスをイネーブルにすることができます。このサービスをイネーブルにすると、インターフェイスに対するクライアントからの着信 DHCPv6 メッセージ（他のリレー エージェントでリレーされたメッセージも含む）が、設定されているすべての発信リンクを介してすべての設定済みリレー宛先に転送されます。マルチコンテキストモードの場合は、複数のコンテキストで使用されているインターフェイス（つまり、共有インターフェイス）で DHCP リレー サービスをイネーブルにすることはできません。

例

次に、ASA の外部インターフェイスの DHCPv6 サーバー（IP アドレス 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701）に対する DHCPv6 リレーエージェントを設定する例を示します。クライアント要求の送信元は ASA の内部インターフェイスであり、バインディングのタイムアウト値は 90 秒です。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
```

```
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

関連コマンド

コマンド	説明
ipv6 dhcprelay server	クライアント メッセージの転送先となる IPv6 DHCP サーバーの宛先アドレスを指定します。
ipv6 dhcprelay timeout	DHCPv6 サーバーからの応答をリレー バインディング構造を通して DHCPv6 クライアントに渡すときに許容する時間の長さを秒単位で設定します。

ipv6 dhcprelay server

クライアントメッセージの転送先となるIPv6 DHCPサーバーの宛先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 **ipv6 dhcprelay server** コマンドを使用します。IPv6 DHCP サーバーの宛先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。

ipv6 dhcprelay server *ipv6-address* [*interface*]
no ipv6 dhcprelay server *ipv6-address* [*interface*]

構文の説明

interface	（オプション）宛先の出力インターフェイスを指定します。
ipv6-address	リンク スコープのユニキャスト、マルチキャスト、サイト スコープのユニキャスト、またはグローバル IPv6 アドレスを指定できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、クライアント メッセージの転送先となる IPv6 DHCP サーバーの宛先アドレスを指定できます。クライアントのメッセージは、この出力インターフェイスが接続されたリンクを経由して宛先アドレスに転送されます。指定したアドレスがリンク スコープのアドレスである場合は、インターフェイスを指定する必要があります。リレー宛先の指定は必須です。ループバックやノードローカルのマルチキャストアドレスは指定できません。サーバーは 1 つのコンテキストに対して 10 台まで指定できます。

例

次に、ASA の外部インターフェイスの DHCPv6 サーバー（IP アドレス 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701）に対する DHCPv6 リレーエージェントを設定する例を示します。クライアント要求の送信元は ASA の内部インターフェイスであり、バインディングのタイムアウト値は 90 秒です。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

関連コマンド

コマンド	説明
ipv6 dhcprelay enable	インターフェイスで IPv6 DHCP リレー サービスをイネーブルにします。
ipv6 dhcprelay timeout	DHCPv6 サーバーからの応答をリレー バインディング構造を通して DHCPv6 クライアントに渡すときに許容する時間の長さを秒単位で設定します。

ipv6 dhcprelay timeout

DHCPv6 サーバーからの応答をリレーバインディング構造を通して DHCPv6 クライアントに渡すときに許容する時間の長さ（秒数）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 **ipv6 dhcprelay timeout** 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。

ipv6dhcprelaytimeout*seconds*
noipv6dhcprelaytimeout *seconds*

構文の説明

seconds DHCPv6 リレーアドレス ネゴシエーションの許容時間（秒数）を設定します。有効な値の範囲は、1 ～ 3600 です。

コマンド デフォルト

デフォルトは 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、DHCPv6 サーバからの応答をリレーバインディング構造を通して DHCPv6 クライアントに渡すときに許容する時間の長さを秒単位で設定できます。

例

次に、ASA の外部インターフェイスの DHCPv6 サーバー（IP アドレス 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701）に対する DHCPv6 リレーエージェントを設定する例を示します。クライアント要求の送信元は ASA の内部インターフェイスであり、バインディングのタイムアウト値は 90 秒です。

```
ciscoasa(config)# ipv6 dhcprelay server 3FFB:C00:C18:6:A8BB:CCFF:FE03:2701 outside
ciscoasa(config)# ipv6 dhcprelay timeout 90
ciscoasa(config)# ipv6 dhcprelay enable inside
```

関連コマンド

コマンド	説明
ipv6 dhcprelay server	クライアント メッセージの転送先となる IPv6 DHCP サーバーの宛先アドレスを指定します。
ipv6 dhcprelay enable	クライアント メッセージの転送先となる IPv6 DHCP サーバーの宛先アドレスを指定します。

ipv6 dhcp server

ステートレスアドレス自動設定 (SLAAC) をプレフィックス委任機能とともに使用しているクライアントの場合は、インターフェイス設定モードで **ipv6 dhcp server** コマンドを使用して DHCPv6 ステートレスサーバーを設定します。DHCP サ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。

ipv6 dhcp server *pool_name*
no ipv6 dhcp server *pool_name*

構文の説明

pool_name	**ipv6 dhcp pool** コマンドで設定した IPv6 プールの名前を設定します。このプールには、特定のインターフェイスでクライアントに提供する情報が含まれます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

SLAAC をプレフィックス委任機能とともに使用するクライアントについては、情報要求（IR）パケットを ASA に送信する際に情報（DNS サーバー、ドメイン名など）を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
```

```
domain-name eng.example.com
import dns-server
ipv6 dhcp pool IT-Pool
domain-name it.example.com
import dns-server
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。

コマンド	説明
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

ipv6 enable

まだ明示的な IPv6 アドレスを設定していない場合に IPv6 処理を有効にするには、グローバル コンフィギュレーション モードで **ipv6 enable** コマンドを使用します。明示的な IPv6 アドレスでまだ設定されていないインターフェイスで IPv6 処理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。

ipv6 enable
no ipv6 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。

コマンド デフォルト

IPv6 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—
グローバル コンフィギュレーション	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

ipv6 enable コマンドを実行すると、インターフェイスで IPv6 リンクローカル ユニキャスト アドレスが自動的に設定され、IPv6 処理のインターフェイスも有効になります。

no ipv6 enable コマンドを使用しても、明示的な IPv6 アドレスが設定されているインターフェイスでの IPv6 処理は無効になりません。

例

次に、選択したインターフェイスで IPv6 処理をイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 enable
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスの IPv6 アドレスを設定し、インターフェイス上で IPv6 の処理をイネーブルにします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 enforce-eui64

ローカルリンク上の IPv6 アドレスに Modified EUI-64 形式のインターフェイス ID の使用を適用するには、グローバル コンフィギュレーション モードで **ipv6 enforce-eui64** コマンドを使用します。Modified EUI-64 アドレス形式の適用を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 enforce-eui64 *if_name*
no ipv6 enforce-eui64 *if_name*

構文の説明

if_name Modified EUI-64 アドレス形式の適用を有効にするインターフェイスの名前を **nameif** コマンドで指定されているとおりに指定します。

コマンド デフォルト

Modified EUI-64 形式の適用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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

このコマンドがインターフェイスでイネーブルになっていると、そのインターフェイス ID が Modified EUI-64 形式を採用していることを確認するために、インターフェイスで受信した IPv6 パケットの送信元アドレスが送信元 MAC アドレスに照らして確認されます。IPv6 パケットがインターフェイス ID に Modified EUI-64 形式を採用していない場合、パケットはドロップされ、次の syslog メッセージが生成されます。

```
%ASA-3-325003: EUI-64 source address check failed.
```

アドレス形式の確認は、フローが作成される場合にのみ実行されます。既存のフローからのパケットは確認されません。また、アドレスの確認はローカルリンク上のホストに対してのみ実行できます。ルータの背後にあるホストから受信したパケットは、アドレス形式の検証に失敗

してドロップされます。これは、その送信元MACアドレスがルータのMACアドレスであり、ホストの MAC アドレスではないためです。

48 ビット リンク層（MAC）アドレスから Modified EUI-64 形式のインターフェイス ID を取得するには、リンク層アドレスの上位 3 バイト（OUI フィールド）と下位 3 バイト（シリアル番号）との間に 16 進数 FFFE を挿入します。選択されたアドレスが一意のイーサネット MAC アドレスから生成されることを保証するため、上位バイトの下位から 2 番めのビット（ユニバーサル/ローカル ビット）が反転され、48 ビット アドレスの一意性が示されます。たとえば、MAC アドレス 00E0.B601.3B7A のインターフェイスには、02E0:B6FF:FE01:3B7A の 64 ビット インターフェイス ID が指定されます。

例

次に、内部インターフェイスで受信した IPv6 アドレスに対して Modified EUI-64 形式の適用をイネーブルにする例を示します。

```
ciscoasa(config)# ipv6 enforce-eui64 inside
```

関連コマンド

コマンド	説明
ipv6 address	インターフェイスで IPv6 アドレスを設定します。
ipv6 enable	インターフェイス上で IPv6 をイネーブルにします。

ipv6 icmp

インターフェイスのICMPアクセスルールを設定するには、グローバル コンフィギュレーション モードで **ipv6 icmp** コマンドを使用します。ICMP アクセスルールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 icmp { **permit** | **deny** } { *ipv6-prefix* / *prefix-length* | **any** | **host** *ipv6-address* } [*icmp-type*] *if-name*
no ipv6 icmp { **permit** | **deny** } { *ipv6-prefix* / *prefix-length* | **any** | **host** *ipv6-address* } [*icmp-type*] *if-name*

構文の説明

any	IPv6 アドレスを指定するキーワード。IPv6 プレフィックス ::/0 の省略形。
deny	選択したインターフェイスで指定の ICMP トラフィックを阻止します。
host	アドレスが特定のホストを指すよう指定します。
icmp-type	アクセスルールによってフィルタリングされるICMPメッセージタイプを指定します。値は、有効な ICMP タイプ番号（0 ～ 255）、または次の ICMP タイプ リテラルのいずれかを指定できます。 • destination-unreachable • packet-too-big • time-exceeded • parameter-problem • echo-request • echo-reply • membership-query • membership-report • membership-reduction • router-renumbering • router-solicitation • router-advertisement • neighbor-solicitation • neighbor-advertisement • neighbor-redirect
if-name	アクセスルールが適用されるインターフェイスの名前（**nameif** コマンドで指定した名前）。

ipv6-address	ICMPv6 メッセージをインターフェイスに送信しているホストの IPv6 アドレス。
ipv6-prefix	ICMPv6 メッセージをインターフェイスに送信している IPv6 ネットワーク。
permit	選択したインターフェイスで指定の ICMP トラフィックを許可します。
prefix-length	IPv6プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。

コマンド デフォルト

ICMP アクセス ルールが定義されていない場合、すべての ICMP トラフィックが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

IPv6 の ICMP は、IPv4 の ICMP と同じ働きをします。ICMPv6 によって、ICMP 宛先到達不能メッセージなどのエラー メッセージや、ICMP エコー要求および応答メッセージのような情報メッセージが生成されます。さらに、IPv6 の ICMP パケットは IPv6 ネイバー探索プロセスおよびパス MTU ディスカバリに使用されます。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

インターフェイスに対して定義されている ICMP ルールがない場合、すべての IPv6 ICMP トラフィックが許可されます。

インターフェイスに対して定義されている ICMP ルールが複数ある場合は、最初に一致したルールから順に処理され、その後暗黙のすべて拒否ルールが続きます。たとえば、最初に一致したルールが許可ルールである場合、ICMP パケットは処理されます。最初に一致したルール

が拒否ルールである場合、またはICMPパケットがそのインターフェイスのいずれのルールにも一致しなかった場合、ASA は ICMP パケットを廃棄し、syslog メッセージを生成します。

そのため、ICMP ルールを入力する順序が重要になります。特定のネットワークからの ICMP トラフィックをすべて拒否するルールを入力し、その後にそのネットワーク上の特定のホストからのICMP トラフィックを許可するルールが続く場合、ホストのルールはいっさい処理されません。ICMP トラフィックは、ネットワークのルールによってブロックされます。ただし、ホストのルールを先に入力し、その後にネットワークのルールを続けた場合、そのホストからの ICMP トラフィックは許可され、そのネットワークからのそれ以外の ICMP トラフィックはブロックされます。

ipv6 icmp コマンドは、ASA インターフェイスで終了する ICMP トラフィックのアクセスルールを設定します。パススルー ICMP トラフィックのアクセスルールを設定するには、 **ipv6 access-list** コマンドを参照してください。

例

次に、外部インターフェイスですべての ping 要求を拒否し、すべての packet-too-big メッセージを許可する（パス MTU ディスカバリをサポートするため）方法を示します。

```
ciscoasa(config)# ipv6 icmp deny any echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

次に、ホスト 2000:0:0:4::2 またはプレフィックス 2001::/64 上のホストに対して外部インターフェイスへの ping を許可する例を示します。

```
ciscoasa(config)# ipv6 icmp permit host 2000:0:0:4::2 echo-reply outside
ciscoasa(config)# ipv6 icmp permit 2001::/64 echo-reply outside
ciscoasa(config)# ipv6 icmp permit any packet-too-big outside
```

関連コマンド

コマンド	説明
ipv6 access-list	アクセス リストを設定します。

ipv6 local pool

IPv6 アドレスプールを設定するには、グローバル コンフィギュレーション モードで **ipv6 local pool** コマンドを使用します。プールを削除するには、このコマンドの **no** 形式を使用します。

ipv6 local pool *pool_name ipv6_address / prefix_length number_of_addresses*
no ipv6 local pool *pool_name ipv6_address / prefix_length number_of_addresses*

構文の説明

ipv6_address	プールの開始 IPv6 アドレスを指定します。
number_of_addresses	範囲：1 ～ 16384。
pool_name	この IPv6 アドレス プールに割り当てる名前を指定します。
prefix_length	範囲：0 ～ 128。

コマンド デフォルト

デフォルトでは、IPv6 ローカル アドレス プールは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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	ASA クラスタリングをサポートするために、**ipv6 address** コマンドでクラスタプールとして IPv6 ローカルプールが追加されました。

使用上のガイドライン

VPN の場合、IPv6 ローカルプールを割り当てるには、トンネルグループで **ipv6-local-pool** コマンドを使用するか、またはグループポリシーで **ipv6-address-pools**（末尾の「s」に注意）コマンドを使用します。グループ ポリシーの ipv6-address-pools 設定は、トンネル グループの ipv6-address-pools 設定を上書きします。

例

次に、アドレスをリモート クライアントに割り当てるために使用する firstipv6pool という名前の IPv6 アドレス プールを設定する例を示します。

```
ciscoasa(config)# ipv6 local pool firstipv6pool 2001:DB8::1001/32 100
ciscoasa(config)#
```

関連コマンド

コマンド	説明
ipv6-address-pool	IPv6 アドレス プールを VPN トンネル グループ ポリシーに関連付けます。
ipv6-address-pools	IPv6 アドレス プールを VPN グループ ポリシーに関連付けます。
clear configure ipv6 local pool	設定済みのすべての IPv6 ローカル プールをクリアします。
show running-config ipv6	IPv6 のコンフィギュレーションを表示します。

ipv6 nd dad attempts

重複アドレス検出時にインターフェイスに連続して送信されるネイバー送信要求メッセージの数を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd dad attempts** コマンドを使用します。送信する重複アドレス検出メッセージの数を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。

ipv6 nd dad attempts *value*
no ipv6 nd dad attempts *value*

構文の説明

value	0 ～ 600 の数値。0 を入力すると、指定したインターフェイスでの重複アドレス検出がディセーブルになります。1 を入力すると、後続の送信なしの単一の送信が設定されます。デフォルト値は 1 メッセージです。

コマンド デフォルト

デフォルトの試行回数は 1 回です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

アドレスがインターフェイスに割り当てられる前に、重複アドレス検出によって、新しいユニキャスト IPv6 アドレスの一意性が確認されます（重複アドレス検出の実行中、新しいアドレスは一時的な状態になります）。重複アドレス検出では、ネイバー送信要求メッセージを使用して、ユニキャスト IPv6 アドレスの一意性を確認します。ネイバー送信要求メッセージの送信頻度を設定するには、**ipv6 nd ns-interval** コマンドを使用します。

重複アドレス検出は、管理上ダウンしているインターフェイスでは停止します。インターフェイスが管理上ダウンしている間、そのインターフェイスに割り当てられたユニキャスト IPv6 アドレスは保留状態に設定されます。

インターフェイスが管理上アップ状態に戻ると、そのインターフェイスで重複アドレス検出が自動的に再起動されます。管理上アップ状態に戻っているインターフェイスでは、インターフェイス上のすべてのユニキャスト IPv6 アドレスを対象に重複アドレス検出が再起動されます。

（注） インターフェイスのリンクローカル アドレスで重複アドレス検出が実行されている間、他の IPv6 アドレスの状態は仮承諾に設定されたままとなります。リンクローカル アドレスで重複アドレス検出が完了すると、残りの IPv6 アドレスで重複アドレス検出が実行されます。

重複アドレス検出によって重複アドレスが特定された場合、そのアドレスの状態はDUPLICATEに設定され、アドレスは使用されなくなります。重複アドレスがインターフェイスのリンクローカル アドレスの場合は、そのインターフェイス上で IPv6 パケットの処理がディセーブルになり、次のようなエラー メッセージが発行されます。

```
%ASA-4-DUPLICATE: Duplicate address FE80::1 on outside
```

重複アドレスがインターフェイスのグローバルアドレスである場合、そのアドレスは使用されず、次のようなエラー メッセージが発行されます。

```
%ASA-4-DUPLICATE: Duplicate address 3000::4 on outside
```

アドレスの状態がDUPLICATEに設定されている間、重複アドレスに関連付けられたコンフィギュレーション コマンドはすべて設定済みのままとなります。

インターフェイスのリンクローカル アドレスが変更された場合、新しいリンクローカル アドレスで重複アドレス検出が実行され、インターフェイスに関連付けられた他のすべての IPv6 アドレスが再生成されます（重複アドレス検出は新規のリンクローカルアドレスでのみ実行されます）。

例

次に、重複アドレス検出がインターフェイスの仮承諾のユニキャストIPv6アドレスで実行された場合に、5 つ連続して送信されるネイバー送信要求メッセージを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd dad attempts 5
```

次に、選択したインターフェイスで重複アドレス検出をディセーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/1
ciscoasa(config-if)# ipv6 nd dad attempts 0
```

関連コマンド

コマンド	説明
ipv6 nd ns-interval	インターフェイスで IPv6 ネイバー送信要求メッセージが送信される時間間隔を設定します。

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd managed-config-flag

IPv6 ルータ アドバタイズメント パケットに管理対象アドレス設定フラグを設定するように ASA を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd managed config-flag** 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。

ipv6 nd managed-config-flag
no ipv6 managed-config-flag

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 自動設定クライアント ホストでは、このフラグを使用して、取得されるステートレス自動設定アドレスに加えて、ステートフルアドレス設定プロトコル（DHCPv6）に基づいてアドレスを取得する必要があることを示すことができます。

例

次に、インターフェイス GigabitEthernet 0/0 で IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd managed config-flag
```

関連コマンド

コマンド	説明
ipv6 nd other-config-flag	IPv6 ルータ アドバタイズメント パケットに他の設定フラグを設定するように ASA を設定します。

ipv6 nd ns-interval

インターフェイスで IPv6 ネイバー送信要求（NS）メッセージが再送信される時間間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ns-interval** 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。

ipv6 nd ns-interval *value*
no ipv6 nd ns-interval [*value*]

構文の説明

value IPv6 ネイバー送信要求メッセージが送信される時間間隔（ミリ秒単位）。有効な値の範囲は、1000 ～ 3600000 ミリ秒です。デフォルト値は 1000 ミリ秒です。

コマンド デフォルト

ネイバー送信要求のデフォルトの送信間隔は 1,000 ミリ秒です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

この値は、このインターフェイスから送信されるすべての IPv6 ルータ アドバタイズメントに含まれます。

例

次の例では、GigabitEthernet 0/0 での IPv6 ネイバー送信要求の送信間隔を 9000 ミリ秒に設定します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ns-interval 9000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd other-config-flag

IPv6 ルータ アドバタイズメント パケットの他の設定フラグを設定するように ASA を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd other-config-flag** 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。

ipv6 nd other-config-flag
no ipv6 other-config-flag

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 自動設定クライアント ホストでは、このフラグを使用して、ステートフル アドレス設定プロトコル（DHCPv6）に基づいて DNS サーバーなどの非アドレス設定情報を取得する必要があることを示すことができます。

例

次に、インターフェイス GigabitEthernet 0/0 で IPv6 ルータ アドバタイズメント パケットの他の設定フラグを設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
ipv6 nd managed-config-flag	IPv6 ルータ アドバタイズメント パケットの管理対象アドレス設定フラグを設定するように ASA を設定します。

ipv6 nd prefix

IPv6 ルータアドバタイズメントに含める IPv6 プレフィックスを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd prefix** コマンドを使用します。プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

ipv6 nd prefix *ipv6-prefix* | *prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]
no ipv6 nd prefix *ipv6-prefix* | *prefix-length* | **default** [[*valid-lifetime preferred-lifetime*] | [**at** *valid-date preferred-date*] | **infinite** | **no-advertise** | **off-link** | **no-autoconfig**]

構文の説明

at *valid-date preferred-date*	ライフタイムおよびプリファレンスが期限切れになる日付と時刻。プレフィックスは、この指定された日付と時刻に達するまで有効です。日付は *date-valid-expire month-valid-expire hh:mm-valid-expire date-prefer-expire month-prefer-expire hh:mm-prefer-expire* の形式で表されます。
default	デフォルト値が使用されます。
infinite	（任意）有効なライフタイムが期限切れになりません。
ipv6-prefix	ルータ アドバタイズメントに含まれる IPv6 ネットワーク番号。 この引数は、RFC 2373 に記述されている形式である必要があります。RFC 2373 では、コロンで区切った 16 ビット値を使用して 16 進数形式でアドレスを指定します。
no-advertise	（任意）ローカル リンク上のホストでは、指定されたプレフィックスが IPv6 自動設定に使用されないことを示します。
no-autoconfig	（任意）ローカル リンク上のホストでは、指定されたプレフィックスが IPv6 自動設定に使用できないことを示します。
off-link	（任意）指定されたプレフィックスがオンリンクの判別に使用されないことを示します。
preferred-lifetime	指定された IPv6 プレフィックスが優先プレフィックスとしてアドバタイズされる時間（秒単位）。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは **infinite** キーワードを使用して指定することもできます。デフォルトは 604800（7 日間）です。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。

valid-lifetime	指定された IPv6 プレフィックスが有効プレフィックスとしてアドバタイズされる時間。有効値の範囲は 0 ～ 4294967295 秒です。最大値は無限ですが、これは **infinite** キーワードを使用して指定することもできます。デフォルトは 2592000（30 日間）です。

コマンド デフォルト

IPv6 ルータ アドバタイズメントを発信するインターフェイスに設定されているすべてのプレフィックスが、有効ライフタイム 2592000 秒（30 日）および優先ライフタイム 604800 秒（7 日）でアドバタイズされます。どちらのライフタイムにも「onlink」フラグと「autoconfig」フラグが設定されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、プレフィックスをアドバタイズするかどうかなど、プレフィックスごとに個々のパラメータを制御できます。

デフォルトでは、 **ipv6 address** コマンドを使用してインターフェイスにアドレスとして設定されるプレフィックスは、ルータアドバタイズメントでアドバタイズされます。**ipv6 nd prefix** コマンドを使用してプレフィックスをアドバタイズメント用に設定すると、設定したプレフィックスだけがアドバタイズされます。

default キーワードを使用すると、すべてのプレフィックスのデフォルトパラメータを設定できます。

プレフィックスの有効期限を指定するための日付を設定できます。有効な推奨ライフタイムは、リアルタイムでカウントダウンされます。有効期限に達すると、プレフィックスはアドバタイズされなくなります。

onlink が「on」（デフォルト）である場合、指定されたプレフィックスがそのリンクに割り当てられます。指定されたプレフィックスを含むそのようなアドレスにトラフィックを送信するノードは、宛先がリンク上でローカルに到達可能であると見なします。

autoconfig が「on」（デフォルト）である場合、ローカル リンク上のホストに対して、指定されたプレフィックスが IPv6 自動設定に使用できることを示します。

例

次に、有効ライフタイムを 1000 秒、優先ライフタイムを 900 秒にして、指定したインターフェイスから送信されるルータ アドバタイズメントに IPv6 プレフィックス 2001:200::/35 を含める例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd prefix 2001:200::/35 1000 900
```

関連コマンド

コマンド	説明
ipv6 address	IPv6 アドレスを設定し、インターフェイスで IPv6 処理を有効にします。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ra-interval

インターフェイス上で IPv6 ルータアドバタイズメントの送信間隔を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-interval** コマンドを使用します。デフォルトの間隔に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd ra-interval ［ **msec** ］ *value*
no ipv6 nd ra-interval ［ ［ **msec** ］ *value* ］

構文の説明

msec （任意）指定される値がミリ秒単位であることを示します。このキーワードが指定されていない場合、指定される値は秒単位となります。

value IPv6 ルータ アドバタイズメントの送信間隔。有効な値の範囲は、3 ～ 1800 秒です、ただし、**msec** キーワードが指定されている場合は 500 ～ 1800000 ミリ秒です。デフォルトは 200 秒です。

コマンド デフォルト

200 秒。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ipv6 nd ra-lifetime コマンドを使用して、ASA をデフォルトルータとして設定する場合、伝送間隔は IPv6 ルータアドバタイズメントの有効期間以下にする必要があります。他の IPv6 ノードとの同期を防止するには、実際に使用される値を指定値の 20 % 以内でランダムに調整します。

例

次に、選択したインターフェイスで IPv6 ルータ アドバタイズメントの間隔を 201 秒に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-interval 201
```

関連コマンド

コマンド	説明
ipv6 nd ra-lifetime	IPv6 ルータ アドバタイズメントのライフタイムを設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd ra-lifetime

インターフェイスの IPv6 ルータアドバタイズメントの「ルータライフタイム」の値を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd ra-lifetime** 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。

ipv6 nd ra-lifetime *seconds*
no ipv6 nd ra-lifetime [*seconds*]

構文の説明

seconds ASA がこのインターフェイスでデフォルトルータであることの有効性。有効な値の範囲は、0 ～ 9000 秒です。デフォルトは 1,800 秒です。0 の場合、ASA は選択したインターフェイスのデフォルトルータと見なされません。

コマンド デフォルト

1800 秒。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

「ルータ ライフタイム」の値は、このインターフェイスから送信されるすべての IPv6 ルータアドバタイズメントに含まれます。この値は、このインターフェイス上のデフォルトルータとしての ASA の有用性を示します。

値をゼロ以外の値に設定すると、ASA はこのインターフェイス上のデフォルトルータであると見なされます。「ルータ ライフタイム」の値としてゼロ以外の値を設定する場合は、その値がルータ アドバタイズメント間隔以上でなければなりません。

値を 0 に設定すると、ASA はこのインターフェイス上のデフォルトルータとは見なされません。

例

次に、選択したインターフェイス上でIPv6ルータアドバタイズメントのライフタイムを 1801 秒に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd ra-lifetime 1801
```

関連コマンド

コマンド	説明
ipv6 nd ra-interval	インターフェイスで IPv6 ルータ アドバタイズメント メッセージが送信される時間間隔を設定します。
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd reachable-time

何らかの到達可能性確認イベントが発生してからリモート IPv6 ノードが到達可能と見なされるまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 nd reachable-time** コマンドを使用します。デフォルトの時間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 nd reachable-time *value*
no ipv6 nd reachable-time [*value*]

構文の説明

value リモート IPv6 ノードが到達可能であると見なされる時間（ミリ秒単位）。有効な値の範囲は、0 ～ 3600000 ミリ秒です。デフォルト値は 0 です

value 引数に 0 を使用すると、到達可能時間が未定のまま送信されます。到達可能時間の値を設定し、追跡するのは、受信デバイスの役割です。

コマンド デフォルト

0 ミリ秒。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

時間を設定すると、使用不可能なネイバーの検出がイネーブルになります。設定時間を短くすると、使用不可能なネイバーをさらに迅速に検出できます。ただし、時間を短くすると、すべての IPv6 ネットワーク デバイスで IPv6 ネットワーク帯域幅および処理リソースの消費量が増えます。通常の IPv6 の運用では、あまり短い時間設定は推奨できません。

このコマンドが 0 に設定されている際の実際の値を含め、ASA で使用されている到達可能時間を確認するには、**show ipv6 interface** コマンドを使用して、使用されている ND 到達可能時間など IPv6 インターフェイスに関する情報を表示します。

例

次に、選択したインターフェイスで IPv6 到達可能時間を 1700000 ミリ秒に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd reachable-time 1700000
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 nd suppress-ra

ローカルエリアネットワーク（LAN）インターフェイスで IPv6 ルータアドバタイズメントの送信を抑制するには、インターフェイス コンフィギュレーション モードで **ipv6 nd suppress-ra** コマンドを使用します。LAN インターフェイスで IPv6 ルータアドバタイズメントの送信を再び有効にするには、このコマンドの **no** 形式を使用します。

ipv6 nd suppress-ra
no ipv6 nd suppress-ra

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。

コマンド デフォルト

IPv6 ユニキャスト ルーティングがイネーブルになっている場合、ルータ アドバタイズメントは LAN インターフェイスで自動的に送信されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

LAN以外のインターフェイスタイプ（たとえばシリアルインターフェイスやトンネルインターフェイス）でIPv6ルータアドバタイズメントの送信を有効にするには、**no ipv6 nd suppress-ra** コマンドを使用します。

例

次に、選択したインターフェイスでIPv6ルータアドバタイズメントを抑制する例を示します。

```
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-if)# ipv6 nd suppress-ra
```

関連コマンド

コマンド	説明
show ipv6 interface	IPv6 向けに設定されたインターフェイスの使用状況を表示します。

ipv6 neighbor

IPv6 ネイバー探索キャッシュにスタティックエントリを設定するには、グローバル コンフィギュレーション モードで **ipv6 neighbor** コマンドを使用します。ネイバー探索キャッシュからスタティックエントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 neighbor *ipv6_address if_name mac_address*
no ipv6 neighbor *ipv6_address if_name* [*mac_address*]

構文の説明

if_name	**nameif** コマンドで指定された内部インターフェイス名または外部インターフェイス名。
ipv6_address	ローカル データ リンク アドレスに対応する IPv6 アドレス。
mac_address	ローカル データ回線（ハードウェア MAC）アドレス。

コマンド デフォルト

スタティック エントリは、IPv6 ネイバー探索キャッシュに設定されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

ipv6 neighbor コマンドは、**arp** コマンドと類似しています。IPv6 ネイバー探索プロセスによる学習を通して、指定された IPv6 アドレスのエントリがネイバー探索キャッシュにすでに存在する場合、エントリは自動的にスタティック エントリに変換されます。変換されたエントリは、 **copy** コマンドを使用して設定を保存するときに設定に保存されます。

show ipv6 neighbor コマンドは、IPv6 ネイバー探索キャッシュ内のスタティック エントリを表示するために使用します。

clear ipv6 neighbors コマンドは、スタティックエントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。**no ipv6 neighbor** コマンドは、指定されたスタティックエントリをネイバー探索キャッシュから削除します。IPv6 ネイバー探索プロセスで学習されたダイナミックエントリはキャッシュから削除されません。**no ipv6 enable** コマンドを使用してインターフェイスで IPv6 を無効にすると、スタティックエントリを除く、そのインターフェイス用に設定されたすべての IPv6 ネイバー探索キャッシュエントリが削除されます（エントリの状態が INCMP [Incomplete] に変更されます）。

IPv6 ネイバー探索キャッシュ内のスタティック エントリがネイバー探索プロセスによって変更されることはありません。

例

次に、IPv6 アドレスを 3001:1::45A、MAC アドレスを 0002.7D1A.9472 にして、内部ホスト用のスタティック エントリをネイバー探索キャッシュに追加する例を示します。

```
ciscoasa(config)# ipv6 neighbor 3001:1::45A inside 0002.7D1A.9472
```

関連コマンド

コマンド	説明
clear ipv6 neighbors	スタティック エントリを除く、IPv6 ネイバー探索キャッシュ内のすべてのエントリを削除します。
show ipv6 neighbor	IPv6 ネイバー キャッシュ情報を表示します。

ipv6 ospf

IPv6 の OSPFv3 インターフェイスのコンフィギュレーションを有効にするには、グローバル コンフィギュレーション モードで **ipv6 ospf** コマンドを使用します。IPv6 の OSPFv3 インターフェイスのコ構成を無効にするには、このコマンドの **no** 形式を使用します。

ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]
no ipv6 ospf [*process-id*] [**cost** | **database-filter** | **dead-interval** *seconds* | **flood-reduction** | **hello-interval** *seconds* | **mtu-ignore** | **neighbor** | **network** | **priority** | **retransmit-interval** *seconds* | **transmit-delay** *seconds*]

構文の説明

cost	インターフェイス上でパケットを送信するコストを明示的に指定します。
database-filter	OSPFv3 インターフェイスへの発信 LSA をフィルタリングします。
dead-interval *seconds*	秒単位で設定する期間内に hello パケットが確認されないと、当該ルータがダウンしていることがネイバーによって示されます。この値はネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルト値は、**ipv6 ospf hello-interval** コマンドで設定された間隔の 4 倍です。
flood-reduction	インターフェイスに LSA のフラッディング削減を指定します。
hello-interval *seconds*	インターフェイス上で送信される hello パケット間の間隔（秒数）を指定します。この値は特定のネットワーク上のすべてのノードで同じにする必要があります。値の範囲は、1 ～ 65535 です。デフォルトの間隔は、イーサネット インターフェイスで 10 秒、非ブロードキャスト インターフェイスで 30 秒です。
mtu-ignore	DBD パケットを受信した場合の OSPF MTU 不一致検出をディセーブルにします。OSPF MTU 不一致検出は、デフォルトでイネーブルになっています。
neighbor	非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定します。
network	ネットワーク タイプに依存するデフォルト以外のタイプに OSPF ネットワーク タイプを設定します。
priority	ルータ プライオリティを設定します。これは、ネットワークにおける指定ルータの特定に役立ちます。有効値の範囲は 0 ～ 255 です。
process-id	イネーブルにする OSPFv3 プロセスを指定します。有効値の範囲は 1 ～ 65535 です。

retransmit-interval *seconds*	インターフェイスに属する隣接関係の LSA 再送信間の時間を秒単位で指定します。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。デフォルトは 5 秒です。
transmit-delay *seconds*	インターフェイス上でリンクステート更新パケットを送信する時間を秒単位で設定します。有効な値の範囲は、1 ～ 65535 秒です。デフォルト値は 1 秒です。

コマンド デフォルト

デフォルトではすべての IPv6 アドレスが含まれます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 エリアを作成する前に OSPFv3 ルーティング プロセスをイネーブルにする必要があります。

例

次に、OSPFv3 インターフェイスのコンフィギュレーションをイネーブルにする例を示します。

```
ciscoasa(config)# ipv6 ospf 3
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf area

IPv6 の OSPFv3 エリアを作成するには、グローバル コンフィギュレーション モードで **ipv6 ospf area** コマンドを使用します。IPv6 の OSPFv3 エリアのコンフィギュレーションを無効にするには、このコマンドの **no** 形式を使用します。

ipv6 ospf area [*area-num*] [**instance**]
no ipv6 ospf area [*area-num*] [**instance**]

構文の説明

area-num	イネーブルにする OSPFv3 エリアを指定します。
instance	インターフェイスに割り当てるエリア インスタンス ID を指定します。

コマンド デフォルト

デフォルトではすべての IPv6 アドレスが含まれます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPFv3 ルーティングは、それぞれのインターフェイスについて個別に設定する必要があります。OSPFv3 エリアは各インターフェイスに 1 つだけ設定でき、ASA の OSPFv3 でサポートされるインスタンスはインターフェイスごとに 1 つだけです。使用されるエリア インスタンス ID はインターフェイスごとに異なります。エリア インスタンス ID は、OSPF パケットの受信にのみ影響し、OSPF の通常のインターフェイスと仮想リンクに適用されます。

例

次に、OSPFv3 インターフェイスのコンフィギュレーションをイネーブルにする例を示します。

```
ciscoasa(config)# ipv6 ospf 3 area 2
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf cost

インターフェイスでパケットを送信するコストを明示的に指定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf cost** コマンドを使用します。インターフェイスでパケットを送信するコストをデフォルト値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。

ipv6 ospf cost *interface-cost*
no ipv6 ospf cost *interface-cost*

構文の説明

interface-cost	リンクステート メトリックとして表される符号なし整数値を指定します。値の範囲は、1 ～ 65535 です。

コマンド デフォルト

デフォルトのコストは帯域幅に基づきます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスのパケット コストを明示的に指定する場合に使用します。

例

次に、パケット コストを 65 に設定する例を示します。

```
ciscoasa(config-if)# ipv6 ospf cost 65
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。

コマンド	説明
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf database-filter all out

OSPFv3 インターフェイスへの発信 LSA をフィルタリングするには、インターフェイス コンフィギュレーション モードで **ipv6 ospf databse-filter all out** コマンドを使用します。インターフェイスに対する LSA の転送を元に戻すには、このコマンドの **no** 形式を使用します。

ipv6 ospf database-filter all out
no ipv6 ospf database-filter all out

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。

コマンド デフォルト

すべての発信 LSA がインターフェイスにフラッディングされます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、OSPFv3インターフェイスへの発信LSAをフィルタリングする場合に使用します。

例

次に、指定したインターフェイスへの発信LSAをフィルタリングする例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf database-filter all out
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。

コマンド	説明
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf dead-interval

helloパケットを確認できないときにネイバーがルータのダウンを宣言するまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf dead-interval** コマンドを使用します。デフォルト時間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 ospf dead-interval *seconds*
no ipv6 ospf dead-interval *seconds*

構文の説明

seconds	間隔を秒単位で指定します。この値はネットワーク上のすべてのノードで同じにする必要があります。有効値の範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルト値は、**ipv6 ospf hello-interval** コマンドで設定された間隔の 4 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、helloパケットを確認できないときにネイバーがルータのダウンを通知するまでの時間を設定する場合に使用します。

例

次に、デッド間隔を 60 に設定する例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。

コマンド	説明
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf encryption

インターフェイスの暗号化タイプを指定するには、インターフェイスコンフィギュレーションモードで **ipv6 ospf encryption** コマンドを使用します。インターフェイスの暗号化タイプを削除するには、このコマンドの **no** 形式を使用します。

ipv6 ospf encryption { **ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null** }
no ipv6 ospf encryption { **ipsec spi** *spi* **esp** *encryption-algorithm* [[*key-encryption-type*] *key*] *authentication-algorithm* [*key-encryption-type*] *key* | **null** }

構文の説明

authentication-algorithm	使用する暗号化アルゴリズムを指定します。有効な値は次のいずれかです。 • **md5**：Message Digest 5（MD5）を有効にします。 • **sha1**：SHA-1 を有効にします。
encryption-algorithm	ESP で使用する暗号化アルゴリズムを指定します。.有効な値は次のとおりです。 • **aes-cdc**：AES-CDC 暗号化を有効にします。 • **3des**：トリプル DES 暗号化を有効にします。 • **des**：DES 暗号化を有効にします。 • **null**：暗号化なしの ESP を指定します。
esp	カプセル化セキュリティ ペイロード（ESP）を指定します。
ipsec	IP セキュリティ プロトコルを指定します。
key	メッセージダイジェストの計算で使用される番号を指定します。MD5 認証を使用する場合、キーの長さは 32 桁の 16 進数（16 バイト）である必要があります。SHA-1 認証を使用する場合、キーの長さは 40 桁の 16 進数（20 バイト）である必要があります。
key-encryption-type	（オプション）キー暗号化タイプを指定します。次のいずれかの値を指定できます。 • **0**：キーは暗号化されません。 • **7**：キーは暗号化されます。
null	この設定をエリア認証よりも優先します。

spi *spi*	セキュリティ ポリシー インデックス（SPI）の値を指定します。*spi* の有効な値の範囲は 256 ～ 42949667295 で、10 進数で入力する必要があります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスの暗号化タイプを指定する場合に使用します。

例

次に、インターフェイスで SHA-1 暗号化をイネーブルにする例を示します。

```
ciscoasa(config)# interface ethernet 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf encryption ipsec spi 1001 esp null sha1
123456789A123456789B123456789C123456789D
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf flood-reduction

インターフェイスへのLSAのフラッディング削減を指定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf flood-reduction** コマンドを使用します。インターフェイスへの LSA のフラッディング削減を削除するには、このコマンドの **no** 形式を使用します。

ipv6 ospf flood-reduction
no ipv6 ospf flood-reduction

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスへの LSA のフラッディング削減を指定する場合に使用します。

例

次に、インターフェイスへのLSAのフラッディング削減をイネーブルにする例を示します。

```
ciscoasa(config-if)# interface GigabitEthernet3/2.200
 vlan 200
 nameif outside
 security-level 100
 ip address 20.20.200.30 255.255.255.0 standby 20.20.200.31
 ipv6 address 3001::1/64 standby 3001::8
 ipv6 address 6001::1/64 standby 6001::8
 ipv6 enable
 ospf priority 255
 ipv6 ospf cost 100
```

```
 ipv6 ospf 100 area 10 instance 200
ipv6 ospf flood reduction
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf hello-interval

helloパケットを確認できないときにネイバーがルータのダウンを宣言するまでの時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf dead-interval** コマンドを使用します。デフォルト時間に戻すには、このコマンドの **no** 形式を使用します。

ipv6 ospf dead-interval *seconds*
no ipv6 ospf dead-interval *seconds*

構文の説明

seconds	間隔を秒単位で指定します。この値はネットワーク上のすべてのノードで同じにする必要があります。有効値の範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルトの間隔は、イーサネットを使用する場合は 10 秒、非ブロードキャストを使用する場合は 30 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、helloパケットを確認できないときにネイバーがルータのダウンを通知するまでの時間を設定する場合に使用します。

例

次に、デッド間隔を 60 に設定する例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf dead-interval 60
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf mtu-ignore

ASA でデータベース記述子（DBD）パケットを受信した際の OSPFv3 最大伝送ユニット（MTU）不一致検出を無効にするには、インターフェイス コンフィギュレーション モードで **ipv6 ospf mtu-ignore** コマンドを使用します。ASA で DBD パケットを受信した際の MTU 不一致検出をデフォルト設定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。

ipv6 ospf mtu-ignore
no ipv6 ospf mtu-ignore

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。

コマンド デフォルト

OSPFv3 MTU 不一致検出は、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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ASA で DBD パケットを受信した際の OSPFv3 MTU 不一致検出を無効にする場合に使用します。

例

次に、ASA で DBD パケットを受信した際の OSPFv3 MTU 不一致検出を無効にする例を示します。

```
ciscoasa(config)# interface serial 0/0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf mtu-ignore
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6 ospf neighbor

非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf neighbor** コマンドを使用します。構成を削除するには、このコマンドの **no** 形式を使用します。

ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]
no ipv6 ospf neighbor *ipv6-address* [**priority** *number*] [**poll-interval** *seconds*] [**cost** *number*] [**database-filter**]

構文の説明

cost *number*	（オプション）ネイバーに 1 ～ 65535 の整数を使用したコストを割り当てます。コストが具体的に設定されていないネイバーについては、インターフェイスのコストは **ipv6 ospf cost** コマンドに基づいて想定されます。
database-filter	（任意）OSPF ネイバーに送出されるリンクステート アドバタイズメント（LSA）をフィルタリングします。
ipv6-address	ネイバーのリンクローカル IPv6 アドレス。この引数は、RFC 2373 に記述されている形式である必要があります。RFC 2373 では、コロンで区切った 16 ビット値を使用して 16 進数形式でアドレスを指定します。
poll-interval *seconds*	（オプション）ポーリングの時間間隔（秒）を表す数値。RFC 2328 では、この値を hello interval よりずっと大きくすることが推奨されています。デフォルトは 120 秒（2 分）です。このキーワードはポイントツーマルチポイント インターフェイスには適用されません。
priority *number*	（オプション）指定の IPv6 プレフィックスが関連付けられている非ブロードキャスト ネイバーのルータ プライオリティ値を示す数。デフォルトは 0 です。

コマンド デフォルト

デフォルトはネットワーク タイプによって異なります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、非ブロードキャスト ネットワークへの OSPFv3 ルータの相互接続を設定する場合に使用します。

例

次に、OSPFv3 ネイバー ルータを設定する例を示します。

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf neighbor FE80::A8BB:CCFF:FE00:C01
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
ipv6 ospf priority	指定したネットワークにおける指定ルータのプライオリティを指定します。

ipv6 ospf network

OSPFv3 ネットワークタイプをデフォルト以外のタイプに設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf network** コマンドを使用します。デフォルトのタイプに戻すには、このコマンドの **no** 形式を使用します。

ipv6 ospf network { **broadcast** | **point-to-point non-broadcast** }
no ipv6 ospf network { **broadcast** | **point-to-point non-broadcast** }

構文の説明

broadcast	ネットワーク タイプをブロードキャストに設定します。
point-to-point non-broadcast	ネットワーク タイプをポイントツーポイントの非ブロードキャストに設定します。

コマンド デフォルト

デフォルトはネットワーク タイプによって異なります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、OSPFv3 ネットワーク タイプをデフォルト以外のタイプに設定する場合に使用します。

例

次に、OSPFv3 ネットワークをブロードキャスト ネットワークに設定する例を示します。

```
ciscoasa(config)# interface serial 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf 1 area 0
ciscoasa(config-if)# ipv6 ospf network broadcast
ciscoasa(config-if)# encapsulation frame-relay
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
ipv6 ospf priority	指定したネットワークにおける指定ルータのプライオリティを指定します。

ipv6 ospf priority

指定したネットワークにおいて指定ルータを特定するためのルータのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf priority** 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。

ipv6 ospf priority *number-value*
no ipv6 ospf priority *number-value*

構文の説明

number-value	ルータのプライオリティを指定する数値を設定します。有効値の範囲は0～255です。

コマンド デフォルト

デフォルトのプライオリティは 1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ルータのプライオリティを設定する場合に使用します。

例

次に、ルータのプライオリティを 4 に設定する例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config-if)# ipv6 ospf priority 4
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。

コマンド	説明
ipv6 ospf retransmit-interval	インターフェイスに属する隣接関係の LSA 再送信の間隔を指定します。

ipv6 ospf retransmit-interval

インターフェイスに属する隣接のLSA再送信間隔を指定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf retransmit-interval** 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。

ipv6 ospf retransmit-interval *seconds*
no ipv6 ospf retransmit-interval *seconds*

構文の説明

seconds	再送信の間隔（秒数）を指定します。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな値にする必要があります。有効な値の範囲は、1 ～ 65535 秒です。

コマンド デフォルト

デフォルトは 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスに属する隣接関係の LSA 再送信の間隔を指定する場合に使用します。

例

次に、再送信間隔を 8 秒に設定する例を示します。

```
ciscoasa(config)# interface ethernet 2
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf retransmit-interval 8
```

関連コマンド

コマンド	説明
ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
ipv6 ospf priority	指定したネットワークにおける指定ルータのプライオリティを指定します。

ipv6 ospf transmit-delay

インターフェイス上でリンクステート更新パケットを送信するために必要な推定時間を設定するには、インターフェイス コンフィギュレーション モードで **ipv6 ospf transmit-delay** 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。

ipv6 ospf transmit-delay *seconds*
no ipv6 ospf transmit-delay *seconds*

構文の説明

seconds	リンクステートの更新を送信するために必要な時間（秒数）を指定します。有効な値の範囲は、1 ～ 65535 秒です。

コマンド デフォルト

デフォルト値は 1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスでリンクステート更新パケットを送信するために必要とされる時間を設定する場合に使用します。

例

次に、転送遅延を 3 秒に設定する例を示します。

```
ciscoasa(config)# interface ethernet 0
ciscoasa(config)# ipv6 enable
ciscoasa(config-if)# ipv6 ospf transmit-delay 3
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。

コマンド	説明
ipv6 ospf priority	指定したネットワークにおける指定ルータのプライオリティを指定します。

ipv6-prefix

マッピングアドレスおよびポート（MAP）ドメイン内の基本マッピングルールの IPv6 プレフィックスを設定するには、MAP ドメインの基本マッピング ルール コンフィギュレーションモードで **ipv6-prefix** コマンドを使用します。プレフィックスを削除するには、このコマンドの **no** 形式を使用します。

ipv6-prefix *ipv6_prefix / prefix_length*
no ipv6-prefix *ipv6_prefix / prefix_length*

構文の説明

ipv6_prefix/prefix_length	IPv6 プレフィックスは、カスタマーエッジ（CE）デバイスの IPv6 アドレスのアドレスプールを定義します。IPv6プレフィックスおよびプレフィックス長（通常は 64）を指定しますが、8 未満を指定することはできません。異なる MAP ドメインで同じ IPv6 プレフィックスを使用することはできません。

コマンド デフォルト

デフォルト設定はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
MAP ドメインの基本マッピング ルール コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(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

IPv6 プレフィックスは、CE デバイスの IPv6 アドレスのアドレスプールを定義します。MAP は、このプレフィックスを持つ宛先アドレスと、デフォルトのマッピングルールで定義されている IPv6 プレフィックスを持つ送信元アドレスを持つパケットが、適切なポート範囲内にある場合にのみ、IPv6 パケットを IPv4 に戻します。他のアドレスから CE デバイスに送信されるすべての IPv6 パケットは、MAP を変換せずに IPv6 トラフィックとして処理されるだけです。MAPの送信元/宛先プールからのパケットは、範囲外のポートでは単にドロップされます。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート（MAP）ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート（MAP）ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

ipv6 prefix-list

IPv6 プレフィックスリストのエントリを作成するには、グローバル コンフィギュレーション モードで **ipv6 prefix-list** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

ipv6 prefix-list *list-name* [**seq** *seq-number*] { **deny** *ipv6-prefix* | *prefix-length* | **description** *text* } [**ge** *ge-value*] [**le** *le-value*]
no ipv6 prefix-list *list-name*

構文の説明

list-name	プレフィックス リストの名前。 既存のアクセス リストと同じ名前にすることはできません。 （注） 「detail」または「summary」はキーワードであるため、名前に使用できません。
seq *seq-number*	（オプション）設定するプレフィックス リスト エントリのシーケンス番号。
deny	条件に一致するネットワークを拒否します。
permit	条件に一致するネットワークを許可します。
ipv6-prefix	指定したプレフィックス リストに割り当てられている IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式にする必要があります。コロン区切りの 16 ビット値を使用して、アドレスを 16 進数で指定します。
prefix-length	IPv6プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。
description *text*	プレフィックス リストの説明。最大 80 文字です。
ge *ge-value*	（任意）*ipv6-prefix*/*prefix-length* 引数の値以上のプレフィックス長を指定します。これは長さの範囲の最小値です（長さ範囲の「下限」に該当する値）。
le *le-value*	（任意）*ipv6-prefix*/*prefix-length* 引数の値以下のプレフィックス長を指定します。これは長さの範囲の最大値です（長さ範囲の「上限」に該当する値）。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

関連コマンド

コマンド	説明
show ipv6 prefix-list	IPv6 プレフィックス リストを表示します。
show ipv6 route	IPv6 ルーティングテーブルの現在の内容を表示します。

ipv6 route

IPv6 ルートを IPv6 ルーティングテーブルに追加するには、グローバル コンフィギュレーション モードで **ipv6 route** コマンドを使用します。IPv6 デフォルトルートを削除するには、このコマンドの **no** 形式を使用します。

ipv6 route *if_name ipv6-prefix* | *prefix-length ipv6-address* [*administrative-distance* | **tunneled**]
no ipv6 route *if_name ipv6-prefix* | *prefix-length ipv6-address* [*administrative-distance* | **tunneled**]

構文の説明

administrative-distance	（任意）ルートのアドミニストレーティブ ディスタンス。デフォルト値は 1 です。この場合、スタティック ルートは接続ルートを除く他のどのタイプのルートよりも優先されます。
if_name	ルートを設定するインターフェイスの名前。
ipv6-address	指定したネットワークに到達するために使用可能なネクスト ホップの IPv6 アドレス。
ipv6-prefix	スタティック ルートの宛先となる IPv6 ネットワーク。 この引数は、RFC 2373 に記述されている形式である必要があります。RFC 2373 では、コロンで区切った 16 ビット値を使用して 16 進数形式でアドレスを指定します。
prefix-length	IPv6 プレフィックスの長さ。この値は、アドレスの高次の連続ビットのうち、プレフィックスのネットワーク部分を構成しているビットの数を示します。プレフィックス長の前にスラッシュ（/）を使用する必要があります。
tunneled	（オプション）ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。

コマンド デフォルト

デフォルトでは、アドミニストレーティブ ディスタンスは 1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(1)	トランスペアレント ファイアウォール モードのサポートが追加されました。

使用上のガイドライン

IPv6 ルーティングテーブルの内容を表示するには、**show ipv6 route** コマンドを使用します。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。**tunneled** オプションを使用してデフォルトルートを作成すると、ASA に着信するトンネルからのトラフィックはすべて、学習したルートまたはスタティックルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルトルートをすべて上書きします。

tunneled オプションが指定されたデフォルトルートには、次の制限事項が適用されます。

- トンネルルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path** コマンド）を有効にしないでください。トンネル ルートの出力インターフェイスで uRPF をイネーブルにすると、セッションに障害が発生します。
- トンネル ルートの出力インターフェイスで、TCP 代行受信をイネーブルにしないでください。イネーブルにすると、セッションでエラーが発生します。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、トンネル ルートでは使用しないでください。これらのインスペクション エンジンは、トンネル ルートを無視します。

tunneled オプションを使用して複数のデフォルトルートは定義できません。トンネルトラフィックの ECMP はサポートされていません。

例

次に、アドミニストレーティブ ディスタンスを 110 にして、ネットワーク 7fff::0/32 のパケットを 3FFE:1100:0:CC00::1 にある内部インターフェイス上のネットワーキング デバイスにルーティングする例を示します。

```
ciscoasa(config)# ipv6 route inside 7fff::0/32 3FFE:1100:0:CC00::1 110
```

関連コマンド

コマンド	説明
debug ipv6 route	IPv6 ルーティング テーブルの更新およびルート キャッシュの更新に関するデバッグ メッセージを表示します。
show ipv6 route	IPv6 ルーティングテーブルの現在の内容を表示します。

ipv6 router ospf

OSPFv3 ルーティングプロセスを作成し、IPv6 ルータ コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **ipv6 router ospf** コマンドを使用します。

ipv6 router ospf *process-id*

構文の説明

process-id	ローカルに割り当てられる内部 ID を指定します。有効な値は 1 ～ 65535 の正の整数です。この番号は、IPv6 の OSPFv3 ルーティング プロセスをイネーブルにしたときに管理目的で割り当てられます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ipv6 router ospf コマンドは、ASA 上で実行される OSPFv3 ルーティングプロセスのグローバル コンフィギュレーション コマンドです。**ipv6 router ospf** コマンドを入力すると、IPv6 ルータ コンフィギュレーション モードであることを示す (config-rtr)# がコマンドプロンプトに表示されます。

no ipv6 router ospf コマンドを使用する場合、必要な情報を指定する場合を除き、オプションの引数を指定する必要はありません。**no ipv6 router ospf** コマンドは、 *process-id* argument 引数によって指定された *OSPFv3* ルーティングプロセスを終了します。*process-id* の値は、ASA においてローカルに割り当てます。OSPFv3 ルーティング プロセスごとに固有の値を割り当てる必要があります。最大 2 つのプロセスが使用できます。

IPv6 ルータ コンフィギュレーション モードで **ipv6 router ospf** コマンドを使用し、OSPFv3 固有の次のオプションを指定して OSPFv3 ルーティングプロセスを設定できます。

- **area**：OSPFv3 エリアパラメータを設定します。サポートされているパラメータには、0 ～ 4294967295 の 10 進数値のエリア ID、**A.B.C.D** の IP アドレス形式のエリア ID などがあります。
- **default**：コマンドをデフォルト値に設定します。**originate** パラメータはデフォルトルートを配布します。
- **default-information**：デフォルト情報の配布を制御します。
- **distance**：ルートタイプに基づいて、OSPFv3 ルート アドミニストレーティブ ディスタンスを定義します。サポートされるパラメータには、1 ～ 254 の値のアドミニストレーティブ ディスタンス、OSPF ディスタンスの **ospf** などがあります。
- **exit—**：IPv6 ルータ コンフィギュレーション モードを終了します。
- **ignore**：ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合に、**lsa** パラメータが指定されている syslog メッセージの送信を抑止します。
- **log-adjacency-changes**：OSPFv3 ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。**detail** パラメータによって、すべての状態変更がログに記録されます。
- **passive-interface**：次のパラメータを使用してインターフェイスでのルーティング更新を抑制します。
  - **GigabitEthernet**：GigabitEthernet IEEE 802.3z インターフェイスを指定します。
  - **Management**：管理インターフェイスを指定します。
  - **Port-channel**：インターフェイスのイーサネットチャネルを指定します。
  - **Redundant**：冗長インターフェイスを指定します。
  - **default**：すべてのインターフェイス上でルーティングが更新されないようにします。
- **redistribute**：次のパラメータに基づいて 1 つのルーティング ドメインから別のルーティング ドメインへのルートの再配布を設定します。
  - **connected**：接続ルートを指定します。
  - **ospf**：OSPF ルートを指定します。
  - **static**：スタティックルートを指定します。
- **router-id**：次のパラメータを使用して、指定されたプロセスの固定ルータ ID を作成します。
  - **A.B.C.D**：IP アドレス形式の OSPF ルータ ID を指定します。
  - **cluster-pool**：レイヤ 3 クラスタリングが設定されている場合に、IP アドレスプールを設定します。

- **summary-prefix**：0 ～ 128 の有効な値で IPv6 アドレスサマリーを設定します。**X:X:X:X::X/** パラメータは、IPv6 プレフィックスを指定します。
- **timers—**：次のパラメータを使用して、ルーティングタイマーを調整します。
  - **lsa**：OSPF LSA タイマーを指定します。
  - **pacing**：OSPF ペーシングタイマーを指定します。
  - **throttle**：OSPF スロットルタイマーを指定します。

例

次に、OSPFv3 ルーティング プロセスをイネーブルにし、IPv6 ルータ コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# ipv6 router ospf 10
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
clear ipv6 ospf	OSPFv3 ルーティング プロセスの IPv6 設定をすべて削除します。
debug ospfv3	OSPFv3 ルーティング プロセスのトラブルシューティング用のデバッグ情報を表示します。

ipv6-split-tunnel-policy

IPv6 スプリット トンネリング ポリシーを設定するには、グループ ポリシー コンフィギュレーション モードで **ipv6-split-tunnel-policy** コマンドを使用します。実行コンフィギュレーションから ipv6-split-tunnel-policy 属性を削除するには、このコマンドの **no** 形式を使用します。

ipv6-split-tunnel-policy { **tunnelall** | **tunnelspecified** | **excludespecified** }
no ipv6-split-tunnel-policy

構文の説明

excludespecified	トラフィックを暗号化しないで送信する先となるネットワークのリストを定義します。この機能は、社内ネットワークにトンネルを介して接続しながら、ローカル ネットワーク上のデバイス（プリンタなど）にアクセスするリモート ユーザーにとって役立ちます。
ipv6-split-tunnel-policy	トラフィックのトンネリングのルールを設定することを指定します。
tunnelall	トラフィックを暗号化しないで送信しないこと、またはASA以外の宛先に送信しないことを指定します。リモート ユーザーは企業ネットワークを経由してインターネットにアクセスしますが、ローカル ネットワークにはアクセスできません。
tunnelspecified	指定したネットワークから、または指定したネットワークへのすべてのトラフィックをトンネリングします。このオプションによって、スプリット トンネリングが有効になります。トンネリングするアドレスのネットワーク リストを作成できるようになります。その他のすべてのアドレスへのデータは暗号化しないで送信され、リモート ユーザーのインターネット サービス プロバイダーによってルーティングされます。

コマンド デフォルト

IPv6 スプリットトンネリングは、デフォルト（**tunnelall**）では無効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

IPv6 スプリット トンネリングは、本来は、セキュリティ機能ではなくトラフィック管理機能です。最適なセキュリティを確保するには、IPv6 スプリット トンネリングをイネーブルにしないことを推奨します。

これにより、別のグループ ポリシーから IPv6 スプリット トンネリングの値を継承できます。

IPv6 スプリット トンネリングを使用すると、リモートアクセス VPN クライアントは、条件に応じて、パケットを IPsec または SSL IPv6 トンネルを介して暗号化された形式で送信したり、クリア テキスト形式でネットワーク インターフェイスに送信したりできます。IPv6 スプリット トンネリングをイネーブルにすると、宛先が IPsec または SSL VPN トンネル エンドポイントの反対側ではないパケットでは、暗号化、トンネルを介した送信、復号化、および最終的な宛先へのルーティングは必要なくなります。

このコマンドでは、IPv6 スプリット トンネリング ポリシーが特定のネットワークに適用されます。

例

次に、FirstGroup という名前のグループ ポリシーに対して、指定したネットワークのみをトンネリングするスプリット トンネリング ポリシーを設定する例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-split-
tunnel-policy tunnelspecified
```

関連コマンド

コマンド	説明
split-tunnel-network-list none	スプリット トンネリングのアクセス リストがないことを指定します。トラフィックはすべてトンネルを通過します。
split-tunnel-network-list value	トンネリングが必要なネットワークと不要なネットワークを区別するために、ASA が使用するアクセスリストを指定します。

ipv6-vpn-address-assign

IPv6 アドレスをリモート アクセス クライアントに割り当てる方法を指定するには、グローバル コンフィギュレーション モードで **ipv6-vpn-addr-assign** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** バージョンを使用します。設定されている VPN アドレスの割り当て方法を ASA からすべて削除するには、引数なしで、このコマンドの **no** 形式を使用します。

ipv6-vpn-addr-assign { **aaa** | **local** }
no ipv6-vpn-addr-assign { **aaa** | **local** }

構文の説明

aaa 外部または内部（LOCAL）の AAA（認証、認可、アカウンティング）サーバーからユーザー単位でアドレスを取得します。IP アドレスが設定された認証サーバーを使用している場合は、この方式を使用することをお勧めします。

local ASA の内部で設定されているアドレス プールから IPv6 アドレスを配布します。

コマンド デフォルト

デフォルトでは、AAA とローカルの両方の VPN アドレス割り当てオプションがイネーブルになります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ASA では、AAA またはローカルのいずれかの方法でリモート アクセス クライアントに IPv6 アドレスを割り当てることができます。複数のアドレス割り当て方式を設定すると、ASA は IPv6 アドレスが見つかるまで各オプションを検索します。

例

次に、アドレス割り当て方法として AAA を設定する例を示します。

```
ciscoasa(config)# ipv6-vpn-addr-assign aaa
```

次に、アドレス割り当て方法としてローカルアドレス プールを使用するように設定する例を示します。

```
ciscoasa(config)# no ipv6-vpn-addr-assign local
```

関連コマンド

コマンド	説明
ipv6 local pool	VPN グループ ポリシーに使用される IPv6 アドレス プールを設定します。
show running-config group-policy	すべてのグループ ポリシーまたは特定のグループ ポリシーのコンフィギュレーションを表示します。
vpn-addr-assign	リモート アクセス クライアントに IPv4 アドレスを割り当てる方法を指定します。

ipv6-vpn-filter

VPN 接続に使用する IPv6 ACL の名前を指定するには、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ー名コンフィギュレーション モードで **ipv6-vpn-filter** コマンドを使用します。**ipv6-vpn-filter none** コマンドを発行して作成したヌル値を含めて、ACL を削除するには、このコマンドの **no** 形式を使用します。

ipv6-vpn-filter { **value** *IPV6-ACL-NAME* | **none** }
no ipv6-vpn-filter

構文の説明

none	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 *IPV6-ACL-NAME*	事前に設定済みのアクセス リストの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	**ipv6-vpn-filter** コマンドは廃止されました。IPv4 または IPv6 エントリを指定して統合フィルタを設定するには、**vpn-filter** コマンドを使用します。この IPv6 フィルタは、**vpn-filter** コマンドで指定されたアクセスリストに IPv6 エントリがない場合にのみ使用されます。

リリース	変更内容
9.1(4)	**ipv6-vpn-filter** コマンドは無効になっており、コマンドの「no」形式のみ使用できます。IPv4 と IPv6 のエントリに対応した統合フィルタを設定するには、**vpn-filter** コマンドを使用します。このコマンドを誤って使用して IPv6 ACL を指定した場合、接続は終了します。

使用上のガイドライン

クライアントレス SSL VPN では、**ipv6-vpn-filter** コマンドで定義された ACL は使用されません。

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。値が継承されないようにするには、**ipv6-vpn-filter none** コマンドを使用します。

このユーザー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。次に、**ipv6-vpn-filter** コマンドを使用して、それらの ACL を適用します。

例

次に、FirstGroup というグループ ポリシーの ipv6_acl_vpn というアクセス リストを呼び出すフィルタを設定する例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
 ipv6-vpn-filter value ipv6_acl_vpn
```

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。
vpn-filter	VPN 接続に使用する IPv4 または IPv6 の ACL の名前を指定します。

ip verify reverse-path

ユニキャスト RPF を有効にするには、グローバル コンフィギュレーション モードで **ip verify reverse-path** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

ip verify reverse-path interface *interface_name*
no ip verify reverse-path interface *interface_name*

構文の説明

interface_name	ユニキャスト RPF をイネーブルにするインターフェイス。

コマンド デフォルト

この機能はデフォルトで無効に設定されています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Unicast RPF は、ルーティング テーブルに従い、すべてのパケットが正しい発信元インターフェイスと一致する送信元 IP アドレスを持っていることを確認して、IP スプーフィング（パケットが不正な送信元 IP アドレスを使用し、実際の送信元を隠蔽すること）から保護します。

通常、ASA は、パケットの転送先を判定するときに宛先アドレスだけを調べます。ユニキャスト RPF は、送信元アドレスも調べるように ASA に指示するため、リバース パス フォワーディング（RPF）と呼ばれます。ASA の通過を許可するすべてのトラフィックについて、送信元アドレスに戻るルートを ASA のルーティングテーブルに含める必要があります。詳細については、RFC 2267 を参照してください。

たとえば、外部トラフィックの場合、ASA はデフォルトルートを使用してユニキャスト RPF 保護の条件を満たすことができます。トラフィックが外部インターフェイスから入り、送信元アドレスがルーティングテーブルにない場合、ASA はデフォルトルートを使用して、外部インターフェイスを送信元インターフェイスとして正しく識別します。

ルーティングテーブルにあるアドレスから外部インターフェイスにトラフィックが入り、そのアドレスが内部インターフェイスに関連付けられている場合、ASA はパケットをドロップします。同様に、未知の送信元アドレスから内部インターフェイスにトラフィックが入った場合、一致するルート（デフォルトルート）が外部インターフェイスを示しているため、ASA はパケットをドロップします。

ユニキャスト RPF は、次のように実装されます。

- ICMP パケットにはセッションがないため、個々のパケットはチェックされません。
- UDP と TCP にはセッションがあるため、最初のパケットは逆ルート ルックアップが必要です。セッション中に到着する後続のパケットは、セッションの一部として保持されている既存の状態を使用してチェックされます。最初のパケット以外のパケットは、最初のパケットと同じインターフェイスに到着したことを保証するためにチェックされます。

例

次に、外部インターフェイスでユニキャスト RPF をイネーブルにする例を示します。

```
ciscoasa(config)# ip verify reverse-path interface outside
```

関連コマンド

コマンド	説明
clear configure ip verify reverse-path	**ip verify reverse-path** コマンドを使用して設定された構成をクリアします。
clear ip verify statistics	ユニキャスト RPF の統計情報をクリアします。
show ip verify statistics	ユニキャスト RPF 統計情報を表示します。
show running-config ip verify reverse-path	**ip verify reverse-path** コマンドを使用して設定された構成を表示します。

ipv6 unnumbered

インターフェイス（ループバック インターフェイスなど）から IPv6 アドレスを借用または継承するには、インターフェイス コンフィギュレーション モードで **ipv6 unnumbered** コマンドを使用します。インターフェイスからの IP アドレスの継承を停止するには、このコマンドの **no** 形式を使用します。

ipv6 unnumbered *interface-name*
no ipv6 unnumbered

構文の説明

interface-name	IPv6アドレスを引き継ぐインターフェイスの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.19(1)	このコマンドが追加されました。

使用上のガイドライン

`ipv6 unnumbered` コマンドは、選択した *interface* の IPv6 アドレスを現在のインターフェイスのアドレスとして継承するために使用されます。

例

次に、ループバック インターフェイスから IPv6 アドレスを借りて、VTI トンネルインターフェイスに使用する例を示します。

```
ciscoasa(config)# interface tunnel 1

ciscoasa(conf-if)# ipv6 unnumbered loopback1
```

関連コマンド

コマンド	説明
ip unnumbered *interface-name*	指定されたインターフェイスのIPアドレスを継承します。

コマンド	説明
interface loopback *loopback-number*	ループバック インターフェイスを作成します。

is – iz

isakmp am-disable（廃止）

アグレッシブモードの着信接続を無効にするには、グローバル コンフィギュレーション モードで **isakmp am-disable** コマンドを使用します。アグレッシブモードの着信接続をイネーブルにするには、このコマンドの **no** 形式を使用します。

isakmp am-disable
no isakmp am-disable

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。

コマンド デフォルト

デフォルト値はイネーブルです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp am-disable** コマンドは、それに置き換わるものです。

例

次に、グローバル コンフィギュレーション モードでの入力で、アグレッシブ モードの着信接続をディセーブルにする例を示します。

```
ciscoasa(config)# isakmp am-disable
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp disconnect-notify（廃止）

ピアへの切断通知を有効にするには、グローバル コンフィギュレーション モードで **isakmp disconnect-notify** コマンドを使用します。切断通知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。

isakmp disconnect-notify
no isakmp disconnect-notify

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。

コマンド デフォルト

デフォルト値は [disabled] 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp disconnect-notify** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
ciscoasa(config)# isakmp disconnect-notify
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。

コマンド	説明
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp enable（廃止）

IPsec ピアが ASAと通信するインターフェイス上で ISAKMP IKEv2 ネゴシエーションを有効にするには、グローバル コンフィギュレーション モードで **isakmp enable** コマンドを使用します。ISAKMP をインターフェイスで無効にするには、このコマンドの **no** 形式を使用します。

isakmp enable *interface-name*
no isakmp enable *interface-name*

構文の説明

interface-name	ISAKMP ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp enable** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
ciscoasa(config)# no isakmp enable
 inside
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。

コマンド	説明
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp identity（廃止）

フェーズ 2 ID をピアに送信するように設定するには、グローバル コンフィギュレーション モードで **isakmp identity** 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。

isakmp identity { **address** | **hostname** | **key-id** *key-id-string* | **auto** }
no isakmp identity { **address** | **hostname** | **key-id** *key-id-string* | **auto** }

構文の説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	接続タイプによってISKMPネゴシエーションを決定します。事前共有キーの場合は IP アドレス、証明書認証の場合は証明書 DN になります。
hostname	ISAKMP 識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

コマンド デフォルト

デフォルトの ISAKMP ID は **isakmp identity hostname** コマンドです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp identity** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、接続タイプに応じて、IPsec ピアと通信するためのインターフェイス上でISAKMPネゴシエーションをイネーブルにします。

```
ciscoasa(config)# isakmp identity auto
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp ipsec-over-tcp（廃止）

IPsec over TCP を有効にするには、グローバル コンフィギュレーション モードで **isakmp ipsec-over-tcp** コマンドを使用します。IPsec over TCP 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。

isakmp ipsec-over-tcp [**port** *port1...port10*]
no isakmp ipsec-over-tcp [**port** *port1...port10*]

構文の説明

port *port1...port10*	（オプション）デバイスが IPsec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。デフォルトのポート番号は 10000 です。

コマンド デフォルト

デフォルト値は [disabled] 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp ipsec-over-tcp** コマンドに置き換わっています。

例

次の例では、グローバル コンフィギュレーション モードで、IPsec over TCP をポート 45 でイネーブルにします。

```
ciscoasa(config)# isakmp ipsec-over-tcp port 45
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。

コマンド	説明
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp keepalive

IKE キープアライブを設定するには、トンネルグループ ipsec 属性コンフィギュレーション モードで **isakmp keepalive** コマンドを使用します。キープアライブパラメータをデフォルトのしきい値と再試行値で有効な状態に戻すには、このコマンドの **no** 形式を使用します。

isakmp keepalive [**threshold** *seconds* | *infinite*] [**retry** *seconds*] [**disable**]
no isakmp keepalive [**threshold** *seconds* | *infinite*] [**retry** *seconds*] [**disable**]

構文の説明

disable	IKE キープアライブ処理をディセーブルにします。デフォルトではイネーブルになっています。
infinite	ASA でキープアライブモニタリングを開始しません。
retry *seconds*	キープアライブ応答を受信しなかったことを受けて再試行する間隔を秒単位で指定します。指定できる範囲は 2 ～ 10 秒です。デフォルト値は 2 秒です。
threshold *seconds*	キープアライブ モニタリングを開始せずにピアがアイドル状態でいられる秒数を指定します。範囲は 10 ～ 3600 秒です。デフォルトは、LAN-to-LAN グループでは 10 秒、リモート アクセス グループでは 300 秒です。

コマンド デフォルト

リモート アクセス グループのデフォルトは、しきい値が 300 秒、再試行値が 2 秒です。

LAN-to-LAN グループのデフォルトは、しきい値が 10 秒、再試行値が 2 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

あらゆるトンネル グループで、IKE キープアライブがデフォルトでイネーブルであり、しきい値と再試行値がデフォルト値になっています。この属性は、IPsec リモート アクセス タイプおよび IPsec LAN-to-LAN トンネル グループ タイプにのみ適用できます。

例

次に、トンネル グループ ipsec 属性コンフィギュレーション モードを開始し、IP アドレスが 209.165.200.225 の IPsec LAN-to-LAN トンネル グループに対して、IKE DPD を設定し、しきい値を 15 にし、再試行間隔を 10 に指定する例を示します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ IPsec 属性を設定します。

isakmp nat-traversal（廃止）

NAT トラバーサルをグローバルに有効にするには、ISAKMP がグローバル コンフィギュレーション モードで有効になっていることを確認し（**isakmp enable** コマンドで有効にできます）、次に **isakmp nat-traversal** コマンドを使用します。NAT トラバーサルを有効にした場合、このコマンドの **no** 形式で無効にできます。

isakmp nat-traversal *natkeepalive*
no isakmp nat-traversal *natkeepalive*

構文の説明

natkeepalive	NAT キープアライブ インターバルを 10 ～ 3600 秒に設定します。デフォルトは 20 秒です。

コマンド デフォルト

デフォルトでは、NAT トラバーサル（**isakmp nat-traversal** コマンド）は無効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp nat-traversal** コマンドは、それに置き換わるものです。

使用上のガイドライン

ポート アドレス変換（PAT）を含めネットワーク アドレス変換（NAT）は、IPsec が使用されているものの、IPsec パケットの NAT デバイス通過を阻害する非互換性がいくつもあるネットワークの多くで使用されています。NAT トラバーサルを使用すると、ESP パケットが 1 つ以上の NAT デバイスを通過できるようになります。

ASA は IETF のドラフト「UDP Encapsulation of IPsec Packets」のバージョン 2 およびバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に従って NAT トラバーサルをサポートし、NAT トラバーサルはダイナミック クリプト マップとスタティック クリプト マップの両方に対応しています。

このコマンドは、ASA 上で NAT-T をグローバルにイネーブルにします。クリプトマップエントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードを開始し、ISAKMP をイネーブルにし、間隔を 30 秒にして NAT トラバーサルをイネーブルにする例を示します。

```
ciscoasa(config)# isakmp enable
ciscoasa(config)# isakmp nat-traversal 30
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy authentication

IKE ポリシー内の認証方式を指定するには、グローバル コンフィギュレーション モードで **isakmp policy authentication** コマンドを使用します。ISAKMP 認証方式を削除するには、**clear configure** コマンドを使用します。

isakmp policy *priority* **authentication** { **crack** | **pre-share** | **rsa-sig** }

構文の説明

crack	認証方式として IKE Challenge/Response for Authenticated Cryptographic Keys（CRACK）を指定します。
pre-share	認証方式として事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
rsa-sig	認証方式として RSA シグニチャを指定します。 RSA シグニチャにより、IKE ネゴシエーションに対して否認防止を実行できます。これは、ユーザーがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。

コマンド デフォルト

デフォルトの ISAKMP ポリシー認証は **pre-share** オプションです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。RSA シグニチャを指定する場合、認証局（CA）から証明書を取得するように、ASA とそのピアを設定する必要があります。事前共有キーを指定する場合は、ASA とそのピアに事前共有キーを別々に設定する必要があります。

例

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 40 のIKEポリシー内で認証方式としてRSAシグニチャを使用するように設定する例を示します。

```
ciscoasa(config)# isakmp policy 40 authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy encryption（廃止）

IKE ポリシー内で使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値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。

isakmp policy *priority* **encryption** { **aes** | **aes-192** | **aes-256** | **des** | **3des** }
no isakmp policy *priority* **encryption** { **aes** | **aes-192** | **aes-256** | **des** | **3des** }

構文の説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

コマンド デフォルト

デフォルトの ISAKMP ポリシー暗号化は、**3des** 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy encryption** コマンドは、それに置き換わるものです。

例

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 25 の IKE ポリシー内でアルゴリズムとして 128 ビット キー AES 暗号化を使用するように設定する例を示します。

```
ciscoasa(config)# isakmp policy 25 encryption aes
```

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 40 の IKE ポリシー内で 3DES アルゴリズムを使用するように設定する例を示します。

```
ciscoasa(config)# isakmp policy 40 encryption 3des
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy group（廃止）

IKE ポリシーで使用する Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **isakmp policy group** コマンドを使用します。Diffie-Hellman グループ識別子をデフォルト値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。

isakmp policy *priority* **group** { **1** | **2** | **5** }
no isakmp policy *priority* **group**

構文の説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。これはデフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。
priority	インターネット キー交換（IKE）ポリシーを一意に指定し、ポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

コマンド デフォルト

デフォルトはグループ 2 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。グループ 7 が追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy group** コマンドは、それに置き換わるものです。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

グループ オプションには、768 ビット（DH グループ 1）、1024 ビット（DH グループ 2）、および 1536 ビット（DH グループ 5）の 3 つがあります。1024 ビットと 1536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注） Cisco VPN Client バージョン 3.x 以降では、ISAKMP ポリシーで DH グループ 2 を設定する必要があります（DH グループ 1 を設定した場合、Cisco VPN Client は接続できません）。AES は、VPN-3DES のライセンスがある ASA に限りサポートされます。AES では大きなキー サイズが提供されるため、ISAKMP ネゴシエーションでは Diffie-Hellman（DH）グループ 1 やグループ 2 ではなく、グループ 5 を使用する必要があります。これは、**isakmp policy priority group 5** コマンドを使用して実行します。

例

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 40 の IKE ポリシーでグループ 2（1024 ビットの Diffie-Hellman）を使用するように設定する例を示します。

```
ciscoasa(config)# isakmp policy 40 group   2
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy hash（廃止）

IKE ポリシーで使用するハッシュアルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy hash** コマンドを使用します。ハッシュアルゴリズムをデフォルト値の SHA-1 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。

isakmp policy *priority* **hash** { **md5** | **sha** }
no isakmp policy *priority* **hash**

構文の説明

md5	IKE ポリシーでハッシュ アルゴリズムとして MD5（HMAC バリアント）を使用することを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
sha	IKE ポリシーでハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を使用することを指定します。

コマンド デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy hash** コマンドに置き換わっています。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。

例

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 40 の IKE ポリシー内で MD5 ハッシュ アルゴリズムを使用するように指定する例を示します。

```
ciscoasa(config)# isakmp policy 40 hash    md5
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp policy lifetime（廃止）

期限切れになるまでの IKE セキュリティ アソシエーションのライフ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 **isakmp policy lifetime** コマンドを使用します。セキュリティアソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）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。

isakmp policy *priority* **lifetime** *seconds*
no isakmp policy *priority* **lifetime**

構文の説明

priority IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

seconds 各セキュリティアソシエーションが期限切れになるまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2147483647 秒の整数を使用します。無制限のライフタイムの場合は、0 秒を使用します。

コマンド デフォルト

デフォルト値は 86,400 秒（1 日）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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy lifetime** コマンドは、それに置き換わるものです。

使用上のガイドライン

IKEは、ネゴシエーションを開始するとき、自身のセッション用のセキュリティパラメータについて合意しようとします。次に、各ピアのセキュリティアソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限切れになるまで、セキュリティ アソシエーションを保持します。セキュリティアソシエーションは、期限切れになるまで、その後の IKE ネゴシエーションで利用できるため、新しい IPsec セキュリティ アソシエーションを設定

するときに時間を節約できます。ピアは、現在のセキュリティアソシエーションが期限切れになる前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、ASA は以後の IPsec セキュリティアソシエーションをより迅速にセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルト値の採用を推奨しますが、ピアがライフタイムを提示しない場合には、無限のライフタイムを指定できます。

（注） IKE セキュリティアソシエーションのライフタイムが無限に設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからネゴシエートされた有限のライフタイムが使用されます。

例

次に、グローバル コンフィギュレーション モードを開始し、IKE ポリシー内にプライオリティ番号 40 で IKE セキュリティ アソシエーションのライフタイムを 50,4000 秒（14 時間）を設定する例を示します。

```
ciscoasa(config)# isakmp policy 40 lifetime 50400
```

次に、グローバル コンフィギュレーション モードでの入力で、IKE セキュリティ アソシエーションのライフタイムを無限に設定する例を示します。

```
ciscoasa(config)# isakmp policy 40 lifetime 0
```

関連コマンド

clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isakmp reload-wait（廃止）

すべてのアクティブなセッションが自主的に終了するまで待機してから ASA をリブートできるようにするには、グローバル コンフィギュレーション モードで **isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するのを待たずにASAをリブートするには、このコマンドの **no** 形式を使用します。

isakmp reload-wait
no isakmp reload-wait

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp reload-wait** コマンドは、それに置き換わるものです。

例

次に、グローバル コンフィギュレーション モードを開始し、すべてのアクティブセッションが終了するまで待機してからリブートすることを ASA に指示する例を示します。

```
ciscoasa(config)# isakmp reload-wait
```

関連コマンド

コマンド	説明
clear configure isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。

コマンド	説明
clear isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config isakmp	アクティブなコンフィギュレーションをすべて表示します。

isis priority

インターフェイスで指定されたASAのプライオリティを設定するには、インターフェイスISIS コンフィギュレーション モードで **isis priority** コマンドを使用します。デフォルトのプライオリティ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。

isis priority *number-value* [**level-1** | **level-2**]
no isis priority [**level-1** | **level-2**]

構文の説明

number-value	ルータのプライオリティを設定します。指定できる範囲は 0 ～ 127 です。
level-1	（任意）レベル 1 専用のプライオリティを設定します。
level-2	（任意）レベル 2 専用のプライオリティを設定します。

コマンド デフォルト

デフォルトは 64 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス ISIS コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、LAN 上のどの ASA が指定ルータまたは DIS であるかを決定するために使用されるプライオリティを設定します。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つ ASA が DIS になります。

（注） IS-IS では、バックアップ指定ルータはありません。プライオリティを 0 に設定すると、そのシステムが DIS になる可能性は低くなりますが、完全には回避できません。プライオリティの高い ASA がオンラインになると、現在の DIS からその役割を引き継ぎます。プライオリティ値が同一の場合は、MAC アドレス値が高いルータが優先されます。

例

次に、プライオリティ レベルを 80 に設定して、レベル 1 ルーティングにプライオリティを与える例を示します。この ASA が DIS になる可能性が高くなります。

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis priority 80 level-1
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。

コマンド	説明
isis authentication mode	インターフェイスごとに、インスタンスに対してIS-ISパケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-ISパケットに対してのみ認証を実行するように、インターフェイスごとのIS-ISインスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャストインターフェイス上で定期的にCSNPパケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS helloをインターフェイスごとのフルMTUサイズに設定します。
isis lsp-interval	インターフェイスごとの連続するIS-ISLSP送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定されたASAのプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各IS-ISLSPの再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各IS-ISLSPの再送信間の時間を設定します。
isis tag	IPプレフィックスがLSPに挿入されたときに、インターフェイスに設定されたIPアドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASAがログメッセージを生成できるようにします。

コマンド	説明
lsp-full suppress	PDUがフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSPが更新されずにASAのデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべてのIS-ISインターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成してLSPデータベースをクリアすることができないように、IS-ISプロトコルをグローバルで無効にします。
redistribute isis	特にレベル1からレベル2へ、またはレベル2からレベル1へ、IS-IS ルートを再配布します。
route priority high	IS-IS IPプレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。

コマンド	説明
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

isis protocol shutdown

IS-IS プロトコルを無効にして、指定されたインターフェイス上で隣接関係を形成できないようにする、およびASAが生成したLSPにインターフェイスのIPアドレスを設定できるようにするには、インターフェイス ISIS コンフィギュレーション モードで **isis protocol shutdown** コマンドを使用します。IS-IS プロトコルを再び有効にするには、このコマンドの **no** 形式を使用します。

isis protocol shutdown
no isis protocol shutdown

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。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス ISIS コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、コンフィギュレーションパラメータを削除せずに、指定されたインターフェイスのIS-IS プロトコルをディセーブルにできます。IS-IS プロトコルはこのコマンドを設定したインターフェイスの隣接関係を形成することはなく、ASA が生成した LSP にインターフェイスの IP アドレスが設定されます。IS-IS がインターフェイスの隣接関係（アジャセンシー）を形成しないようにし、IS-IS LSP データベースをクリアする場合は、**protocol shutdown** コマンドを使用します。

例

次に、GigabitEthernet 0/0 上で IS-IS プロトコルを無効にする例を示します。

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis protocol shutdown
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。

コマンド	説明
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。

コマンド	説明
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

isis retransmit-interval

各 IS-IS LSP の再送信間隔を設定するには、インターフェイス ISIS コンフィギュレーションモードで **isis retransmit-interval** 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。

isis retransmit-interval *seconds*
no isis retransmit-interval *seconds*

構文の説明

seconds （オプション）各 LSP の再送信の間隔。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな数値にする必要があります。指定できる範囲は 0 ～ 65535 です。

コマンド デフォルト

デフォルトは 5 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス ISIS コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

seconds 引数は控えめな値にする必要があります。そうしないと、不要な再送信が発生します。このコマンドは、LAN（マルチポイント）インターフェイスに影響を与えません。

例

次に、大容量のシリアル回線に対して各 IS-IS LSP を 60 秒ごとに再送信するように GigabitEthernet 0/0 を設定する例を示します。

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-interval 60
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。

コマンド	説明
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。

コマンド	説明
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

isis retransmit-throttle-interval

インターフェイスでの 各 IS-IS LSP の再送信間隔を設定するには、インターフェイス ISIS コンフィギュレーション モードで **isis retransmit-throttle-interval** 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。

isis retransmit-throttle-interval *milliseconds*
no isis retransmit-throttle-interval

構文の説明

milliseconds	（オプション）インターフェイスでの LSP 再送信間の最小遅延。指定できる範囲は 0 ～ 65535 です。

コマンド デフォルト

この遅延は、**isis lsp-interval** コマンドで判断されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス ISIS コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、LSP 再送信トラフィックの制御方法と同様に、多くの LSP およびインターフェイスを持つ大規模なネットワークで役立つ場合があります。このコマンドは、インターフェイスで LSP を再送信できるレートを制御します。

このコマンドは、LSP がインターフェイス上で送信されるレート（**isis lsp-interval** コマンドで制御）および単一 LSP の再送信間隔（**isis retransmit-interval** コマンドで制御）とは異なります。これらのコマンドを組み合わせて使用することにより、1 つの ASA からのそのネイバーへのルーティング トラフィックで発生する負荷を制御できます。

例

次に、LSP 再送信のレートが 300 ミリ秒あたり 1 回に制限されるように GigabitEthernet 0/0 を設定する例を示します。

```
ciscoasa(config)#
```

```
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis retransmit-throttle-interval 300
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。

コマンド	説明
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

isis tag

IP プレフィックスが IS-IS LSP に設定されている場合に、インターフェイスに設定されている IP アドレスにタグを設定するには、インターフェイス ISIS コンフィギュレーション モードで **isis tag** コマンドを使用します。IP アドレスのタグ設定を停止するには、このコマンドの **no** 形式を使用します。

isis tag *tag-number*
no isis tag *tag-number*

構文の説明

tag-number	IS-IS ルートでタグとして機能する番号。指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

インターフェイスに設定された IP アドレスに関連付けられているルート タグはありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インターフェイス ISIS コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

タグが使用されないかぎり、タグ付けされたルートではいかなるアクション（ルートの再配布やルートの集約のためのアクションなど）も発生しません。このコマンドを設定すると、タグがパケット内の新規の情報であるため、ASA は新しい LSP をトリガーします。

例

次に、100 というタグを持つように GigabitEthernet 0/0 を設定する例を示します。

```
ciscoasa(config)#
interface GigabitEthernet0/0
ciscoasa(config-if)#
isis tag 100
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。

コマンド	説明
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。

コマンド	説明
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

is-type

IS-IS ルーティングプロセスのインスタンスのルーティングレベルを設定するには、ルータ ISIS コンフィギュレーション モードで **is-type** コマンドを使用します。デフォルト値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。

isis type [**level-1** | **level 1-2** | **level-2-only**
no isis type [**level-1** | **level 1-2** | **level-2-only**

構文の説明

level-1	（オプション）エリア内ルーティングを示します。この ASA は、エリア内の宛先についてのみ学習します。レベル 2（エリア間）ルーティングは、最も近いレベル 1 ～ 2 ASA によって実行されます。
level-1-2	（オプション）ASA は、レベル 1 およびレベル 2 のルーティングを実行します。この ASA は、ルーティング プロセスのインスタンスを 2 つ実行します。このルータは、エリア内（レベル 1 ルーティング）の宛先について 1 つのリンクステート パケット データベース（LSDB）を持っており、Shortest Path First（SPF）の計算を実行してエリア トポロジを検出します。また、他のすべてのバックボーン（レベル 2）ルータのリンクステート パケット（LSP）による別のリンクステート データベース（LSDB）を持ち、別の SPF 計算を実行して、バックボーンのトポロジと他のすべてのエリアの存在を検出します。
level-2-only	（オプション）エリア間ルーティングを示します。この ASA は、バックボーンの一部であり、それ自身のエリア内のレベル 1 だけの ASA とは通信しません。

コマンド デフォルト

従来の IS-IS コンフィギュレーションでは、ASA はレベル 1（エリア内）およびレベル 2（エリア間）ルータとしてだけ機能します。

マルチエリア IS-IS コンフィギュレーションでは、設定された IS-IS ルーティング プロセスの最初のインスタンスは、デフォルトでレベル 1-2（エリア内およびエリア間）ルータです。設定されている IS-IS プロセスの残りのインスタンスはデフォルトでレベル 1 ルータになります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

IS-IS ルーティング プロセスのタイプを設定することを水晶します。マルチエリア IS-IS を設定している場合は、ルータのタイプを設定するか、またはデフォルト設定のままにしておく必要があります。デフォルトでは、**router isis** コマンドを使用して設定した IS-IS ルーティングプロセスの最初のインスタンスは、レベル 1-2 ルータになります。

ネットワークにエリアが 1 つだけしかない場合は、必ずしもレベル 1 とレベル 2 の両方のルーティング アルゴリズムを実行する必要はありません。IS-IS がコネクションレス型ネットワーク サービス（CLNS）ルーティングに使用され、エリアが 1 つしかない場合は、レベル 1 だけを使用する必要があります。IS-IS が IP ルーティングだけに使用され、エリアが 1 つしかない場合は、常にレベル 2 だけを実行できます。すでにレベル 1-2 エリアがある場合は、その後に追加されたエリアは、デフォルトでレベル 1 エリアになります。

ルータインスタンスがレベル 1-2（IS-IS ルーティングプロセスの最初のインスタンスのデフォルト）に設定されている場合は、**is-type** コマンドを使用して、そのエリアのレベル 2（エリア間）ルーティングを削除できます。**is-type** コマンドを使用してエリアのレベル 2 ルーティングも設定できます。

例

エリア ルータの指定例を示します。

```
ciscoasa#
router isis
ciscoasa(config-router)#
is-type level-2-only
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。

コマンド	説明
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。

コマンド	説明
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定されたASAのプライオリティを設定します。
isis protocol shutdown	インターフェイスごとにIS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各IS-IS LSPの再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各IS-IS LSPの再送信間の時間を設定します。
isis tag	IPプレフィックスがLSPに挿入されたときに、インターフェイスに設定されたIP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASAがログ メッセージを生成できるようにします。
lsp-full suppress	PDUがフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSPが更新されずにASAのデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべてのIS-ISインターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。

コマンド	説明
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

issuer（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

アサーションを SAML-type SSO サーバーに送信するセキュリティデバイスを指定するには、その特定の SAML タイプの webvpn-sso-saml コンフィギュレーション モードで **issuer** コマンドを使用します。発行者名を削除するには、このコマンドの **no** 形式を使用します。

issuer識別情報
no issuer [*identifier*]

構文の説明

identifier セキュリティ デバイス名を指定します。通常は、デバイスのホスト名です。識別情報は、英数字で 65 文字未満にする必要があります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn-sso-saml コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

WebVPN でだけ使用できる SSO のサポートにより、ユーザは、ユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。ASA は現在、SAML POST-type の SSO サーバーと SiteMinder-type の SSO サーバーをサポートしています。

このコマンドは、SAML-type の SSO サーバーのみに適用されます。

例

次に、asa1.example.com というセキュリティ デバイスの発行者名を指定する例を示します。

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# issuer asa1.example.com
ciscoasa(config-webvpn-sso-saml#
```

関連コマンド

コマンド	説明
assertion-consumer-url	セキュリティ デバイスが SAML-type SSO サーバー アサーション コンシューマ サービスに問い合わせる際に使用する URL を指定します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。
sso-server	シングル サインオン サーバーを作成します。
トラストポイント	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。

issuer-name

すべての発行済み証明書の発行者名 DN を指定するには、ローカル認証局（CA）サーバー コンフィギュレーション モードで **issuer-name** コマンドを使用します。認証局の証明書からサブジェクト DN を削除するには、このコマンドの **no** 形式を使用します。

issuer-name*DN-string*
no issuer-name *DN-string*

構文の説明

DN-string	自己署名 CA 証明書のサブジェクト名 DN でもある証明書の認定者名を指定します。属性と値のペアを区切るには、カンマを使用します。カンマを含む値は、引用符で囲んでください。発行者名は、英数字で 500 文字未満にする必要があります。

コマンド デフォルト

デフォルトの発行者名は cn=*hostame.domain-name* で、たとえば cn=asa.example.com となります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.3(1)	このコマンドが追加されました。
8.0(2)	*DN-string* 値でカンマを保持するため、引用符のサポートが追加されました。

使用上のガイドライン

このコマンドでは、ローカル CA サーバーが作成する証明書に表示される発行者名を指定します。この任意のコマンドは、発行者名をデフォルトの CA 名とは異なるものにする場合に使用します。

（注） この発行者名構成は、CA サーバーを有効にし、**no shutdown** コマンドを発行して証明書を生成すると変更できなくなります。

例

次に、証明書認証を設定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco systems, inc.”
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードのコマンド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。
keysize	証明書登録で生成される公開キーと秘密キーのサイズを指定します。
lifetime	CA 証明書と発行済みの証明書のライフタイムを指定します。
show crypto ca server	ローカル CA の特性を表示します。
show crypto ca server cert-db	ローカル CA サーバー証明書を表示します。

第 II 部

J - M コマンド

j – k

java-trustpoint（廃止）

指定したトラストポイントの場所から PKCS12 証明書およびキー関連情報を使用するように WebVPN Java オブジェクト署名機能を設定するには、webvpn コンフィギュレーション モードで **java-trustpoint** コマンドを使用します。Java オブジェクト署名のトラストポイントを削除するには、このコマンドの **no** 形式を使用します。

java-trustpoint*trustpoint*
no java-trustpoint

構文の説明

トラストポイント	**crypto ca import** コマンドで設定したトラストポイントの場所を指定します。

コマンド デフォルト

デフォルトでは、Java オブジェクト署名のトラストポイントは none に設定されています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(2)	このコマンドが追加されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

トラストポイントは、認証局（CA）または ID キー ペアを表します。**java-trustpoint** コマンドの場合、指定したトラストポイントにはアプリケーション署名エンティティの X.509 証明書、その証明書に対応する RSA 秘密鍵、ルート CA までの認証局チェーンを含める必要があります。通常は、**crypto ca import** コマンドを使用して PKCS12 形式のバンドルをインポートします。PKCS12 バンドルは、信頼できる CA 認証局から入手するか、openssl といったオープン ソース ツールを使用して既存の X.509 証明書と RSA 秘密キーから手動で作成できます。

（注） アップロードされた証明書は、パッケージ（CSD パッケージなど）に組み込まれた Java オブジェクトの署名には使用できません。

例

次に、最初に新しいトラストポイントを設定してから、そのトラストポイントを WebVPN Java オブジェクト署名用に設定する例を示します。

```
ciscoasa(config)# crypto ca import mytrustpoint pkcs12 mypassphrase
Enter the base 64 encoded PKCS12.
End with the word "quit" on a line by itself.
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully.
ciscoasa(config)#
```

次に、WebVPN Java オブジェクトに署名する新しいトラストポイントを設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config)# java-trustpoint mytrustpoint
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca import	PKCS12 データを使用してトラストポイントの証明書とキー ペアをインポートします。

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るには、コンテキストコンフィギュレーション モードで **join-failover-group** 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。

join-failover-group*group_num*
no join-failover-group *group_num*

構文の説明

group_num フェールオーバー グループの番号を指定します。

コマンド デフォルト

フェールオーバー グループ 1。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
コンテキストコンフィギュレーション	• 対応	• 対応	—	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

管理コンテキストは、常にフェールオーバー グループ 1 に割り当てられます。フェールオーバーグループとコンテキスト アソシエーションを表示するには、**show context detail** コマンドを使用できます。

コンテキストをフェールオーバーグループに割り当てる前に、**failover group** コマンドを使用して、フェールオーバーグループをシステムコンテキスト内に作成する必要があります。このコマンドは、コンテキストがアクティブ状態になっているユニット上で入力します。デフォルトでは、未割り当てのコンテキストは、フェールオーバー グループ 1 のメンバーになっています。そのため、コンテキストがまだフェールオーバー グループに割り当てられていない場合は、フェールオーバー グループ 1 がアクティブ状態になっているユニット上で、このコマンドを入力する必要があります。

システムからフェールオーバーグループを削除するには、事前に **no join-failover-group** コマンドを使用して、フェールオーバーグループからコンテキストをすべて削除しておく必要があります。

例

次に、ctx1 というコンテキストをフェールオーバー グループ 2 に割り当てる例を示します。

```
ciscoasa(config)# context ctx1
ciscoasa(config-context)# join-failover-group 2
ciscoasa(config-context)# exit
```

関連コマンド

コマンド	説明
context	指定したコンテキストのコンテキスト コンフィギュレーション モードを開始します。
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
show context detail	コンテキストの詳細情報（名前、クラス、インターフェイス、フェールオーバー グループ アソシエーション、およびコンフィギュレーション ファイルの URL など）を表示します。

jumbo-frame reservation

ジャンボフレームをサポート対象のモデルで有効にするには、グローバル コンフィギュレーション モードで **jumbo-frame reservation** コマンドを使用します。ジャンボフレームを無効にするには、このコマンドの **no** 形式を使用します。

（注） この設定を変更した場合は、ASA のリブートが必要です。

jumbo-frame reservation
no jumbo-frame reservation

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。

コマンド デフォルト

ジャンボフレームの予約は、ASA ハードウェア、ASA 仮想、および ISA 3000 では、デフォルトで無効になっています。

ジャンボフレームは、他のモデルではデフォルトでサポートされています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが ASA 5580 に追加されました。
8.2(5)/8.4(1)	ASA 5585-X のサポートが追加されました。
8.6(1)	ASA 5512-X ～ ASA 5555-X のサポートが追加されました。
9.3(2)	ASA 5506-X のサポートが追加されました。
9.3(3)	ASA 5508-X および 5516-X のサポートが追加されました。

使用上のガイドライン

この手順は、ASA ハードウェアモデル、ISA 3000、および ASA 仮想 にのみ適用できます。その他のモデルは、デフォルトでジャンボフレームをサポートしています。

ジャンボフレームは、8GB RAM 未満の ASAv5 および ASAv10 ではサポートされません。

ジャンボ フレームとは、標準的な最大値 1518 バイト（レイヤ 2 ヘッダーおよび VLAN タギングの 18 バイトを含む）より大きく、9216 バイトまでのイーサネット パケットのことです。**mtu** コマンドは *payload* 値のみを指定するため、9216 バイトのジャンボフレームについては MTU が 9198（ヘッダーの場合は 9216 ～ 18 バイト）になるように設定する必要があります。

ジャンボ フレームをサポートするには追加のメモリが必要となるため、アクセス リストなどの他の機能の最大使用量が制限される可能性があります。

ジャンボ フレームは管理 *n* /*n* インターフェイスではサポートされません。

ジャンボフレームを送信する必要のある各インターフェイスの MTU を、デフォルト値の 1500 より大きい値に設定してください。たとえば、**mtu** コマンドを使用して値を 9198 に設定します。ASASM では、デフォルトでジャンボフレームがサポートされるため、 **jumbo-frame reservation** コマンドを設定する必要はありません。MTU の値の設定だけ行ってください。

また、ジャンボ フレームを使用する場合は、TCP の最大セグメント サイズ（MSS）の値を設定してください。MSS は、MTU より 120 バイト小さい値に設定する必要があります。たとえば、MTU を 9000 に設定した場合、MSS は 8880 に設定する必要があります。MSS は、**sysopt connection tcpmss** コマンドで設定できます。

フェールオーバー ペアでジャンボ フレームがサポートされるようにするには、プライマリ ユニットとセカンダリ ユニットの両方をリブートする必要があります。ダウン時間を回避するには、次の手順を実行します。

- アクティブ ユニットでコマンドを発行します。
- アクティブ ユニットで実行コンフィギュレーションを保存します。
- プライマリ ユニットとセカンダリ ユニットを 1 つずつリブートします。

例

次に、ジャンボ フレームの予約をイネーブルにし、コンフィギュレーションを保存して ASA をリロードする例を示します。

```
ciscoasa(config)# jumbo-frame reservation
WARNING: this command will take effect after the running-config is saved
and the system has been rebooted. Command accepted.
ciscoasa(config)# write memory
Building configuration...
Cryptochecksum: 718e3706 4edb11ea 69af58d0 0a6b7cb5
70291 bytes copied in 3.710 secs (23430 bytes/sec)
[OK]
ciscoasa(config)# reload
Proceed with reload? [confirm] Y
```

関連コマンド

コマンド	説明
mtu	インターフェイスの最大伝送単位を指定します。
show jumbo-frame reservation	**jumbo-frame reservation** コマンドの現在の設定を表示します。

kcd-server

クライアントレス SSL リモートアクセス VPN の Kerberos Constrained Delegation（KCD）を設定するには、webvpn コンフィギュレーション モードで **kcd-server** コマンドを使用します。KCD を無効にするには、このコマンドの **no** 形式を使用します。

kcd-server *aaa-server-group_name* **username** *user_id* **password** *password* [**validate-server-certificate**]
no kcd-server

構文の説明

username	管理者またはサービスレベル特権を持つ Active Directory ユーザーを指定して、デバイスをドメインに追加します。
パスワード	ユーザーのパスワードを指定します。
validate-server-certificate	（任意）ドメインを結合するときにサーバー証明書およびサーバーの ID を検証するように ASA に指示します。このオプションを省略すると、システムはドメインコントローラが有効であると見なします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.15(1)	**validate-server-certificate** キーワードが追加されました。

使用上のガイドライン

Active Directory ドメインに参加できるように ASA を設定するには、webvpn コンフィギュレーション モードで **kcd-server** コマンドを使用します。ドメインコントローラの名前とレルムは **aaa-server-groupname** コマンドで指定します。AAA サーバーグループのタイプは Kerberos サーバーにする必要があります。**username** オプションと **password** オプションは、管理者特権

を持つユーザーには対応しませんが、ドメインコントローラのサービスレベル特権を持つユーザーに対応する必要があります。既存の設定を表示するには、**show webvpn kcd** コマンドを使用します。

ASA 環境の Kerberos Constrained Delegation（KCD）は、ケルベロスで保護されているすべての Web サービスへのシングルサインオン（SSO）アクセスをクライアントレス SSL リモートアクセス VPN ユーザーに提供します。ユーザーの代わりに ASA でログイン情報（サービスチケット）を管理し、そのチケットを使用してサービスに対してユーザーを認証します。

kcd-server コマンドを機能させるために、ASA はソースドメイン（ASA が常駐するドメイン）とターゲットまたはリソースドメイン（Web サービスが常駐するドメイン）間の信頼関係を確立する必要があります。ASA は、サービスにアクセスするリモートアクセスユーザーの代わりに、ソースから宛先ドメインへの認証パスを横断し、必要なチケットを取得します。

このパスのことをクロスレルム認証と呼びます。クロスレルム認証の各フェーズにおいて、ASA は特定のドメインのクレデンシャルおよび後続ドメインとの信頼関係に依存しています。

また、KCD の設定では、ドメインコントローラを DNS サーバー（たとえば、DefaultDNS グループ）として設定し、ドメインコントローラが到達できるインターフェイスで DNS ルックアップをイネーブルにする必要があります。

例

次に、KCD の設定例を示します。ドメインコントローラは 10.1.1.10（内部インターフェイスで到達可能）、ドメイン名は PRIVATE.NET です。また、ドメインコントローラのサービスアカウントのユーザー名は dcuser、パスワードは dcuser123! です。

```
----Enable a DNS lookup by configuring the DNS server and Domain name --------------
ciscoasa
(config)#
dns domain-lookup inside
ciscoasa
(config)#
dns server-group DefaultDNS
ciscoasa
(config-dns-server-group)#
name-server 10.1.1.10
ciscoasa
(config-dns-server-group)#
domain-name
private.net
----Configure the AAA server group with Server and Realm-----------------------------
ciscoasa
(config)#
aaa-server KerberosGroup protocol Kerberos
ciscoasa
(config-asa-server-group)#
aaa-server KerberosGroup (inside) host 10.1.1.10
ciscoasa
(config-asa-server-group)#
kerberos-realm PRIVATE.NET
----Enable KCD------------------------------
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
```

```
kcd-server KerberosGroup username dcuser password dcuser123!
validate-server-certificate
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバー コンフィギュレーション モードを開始します。このモードでは、AAA サーバーのパラメータを設定できます。
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバーパラメータを設定できます。
show aaa kerberos	Kerberos チケットを表示します。
show webvpn kcd	KCD 設定を表示します。

keepout

（ASA のメンテナンスまたはトラブルシューティングの実行中に）新しいユーザーセッションのログインページではなく、管理者定義のメッセージを表示するには、webvpn コンフィギュレーション モードで **keepout** コマンドを使用します。以前に設定された立ち入り禁止ページを削除するには、このコマンドの **no** 形式を使用します。

keepout
no keepout *string*

構文の説明

string 二重引用符で囲んだ英数字ストリング。

コマンド デフォルト

立ち入り禁止ページはありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドがイネーブルにされると、クライアントレスの WebVPN ポータル ページが使用不可になります。ポータルのログインページではなく、ポータルが使用不可であることを通知する管理者定義メッセージが表示されます。クライアントレスアクセスは無効にし、AnyConnect アクセスは許可するには、**keepout** コマンドを使用します。また、このコマンドを使用して、メンテナンス中のためポータルが使用不可であることを示すこともできます。

（注） HostScan がインストールされている場合、立ち入り禁止機能は、ASA が Cisco Secure Desktop ポータルなどのページを開くことを停止しません。Cisco Secure Desktop ポートを回避するには、HostScan をアンインストールする必要があります。

例

次に、立ち入り禁止ページを設定する例を示します。

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
 keepout "The system is unavailable until 7:00 a.m. EST."
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn コンフィギュレーション モードを開始します。このモードではクライアントレス SSL VPN 接続の属性を設定できます。

kerberos-realm

このケルベロスサーバーのレルム名を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **kerberos-realm** コマンドを使用します。レルム名を削除するには、このコマンドの **no** 形式を使用します。

kerberos-realm*string*
no kerberos-realm

構文の説明

string 大文字と小文字が区別される最大 64 文字の英数字ストリング。ストリングにスペースは使用できません。

（注） Kerberos レルム名では数字と大文字だけを使用します。ASA では、*string* 引数に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。大文字だけを使用してください。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Kerberos サーバに対してのみ有効です。

Microsoft Windows の **set USERDNSDOMAIN** コマンドをケルベロスレルムの Windows 2000 Active Directory サーバー上で実行する場合は、 *string* 引数の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レルム名です。

```
C:\>set USERDNSDOMAIN
USERDNSDOMAIN=EXAMPLE.COM
```

string 引数には、数字と大文字のアルファベットのみを使用する必要があります。**kerberos-realm** コマンドでは、大文字と小文字が区別されます。また、ASA では小文字は大文字に変換されません。

例

次のシーケンスは、AAA サーバーホストの設定に関するコンテキストでケルベロスレルムを「EXAMPLE.COM」に設定するための **kerberos-realm** コマンドを示しています。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa
(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション サブモードを開始し、ホスト固有の AAA サーバー パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

key（AAA サーバー ホスト）

AAA サーバーに対して NAS を認証するために使用されるサーバーシークレットの値を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **key** コマンドを使用します。AAA サーバー ホスト コンフィギュレーション モードには、AAA サーバー プロトコル コンフィギュレーション モードからアクセスできます。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。

key [**0** | **8**] *key*
no key

構文の説明

key 最大 127 文字の英数字キーワード。オプションで、キーの前に暗号化を示す番号を追加できます。

- 0 は、キーは暗号化されないことを意味します。これがデフォルトです。
- 8 は、キーが AES で暗号化された Base64 ハッシュであることを意味します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

key の値は、127 文字までの英数字で構成されているキーワードで、TACACS+ サーバー上のキーと同じ値にします。大文字と小文字は区別されます。127 を超える文字は無視されます。このキーは、クライアントとサーバーの間でやり取りするデータを暗号化するために使用されます。キーは、クライアント システムとサーバー システムの両方で同一である必要があります。キーにスペースは使用できませんが、その他の特殊文字は使用できます。キー（サーバーシークレット）の値で、ASA が AAA サーバーに対して認証されます。

このコマンドは、RADIUS サーバーと TACACS+ サーバーに対してのみ有効です。

例

次に、ホスト「1.2.3.4」に「srvgrp1」という TACACS+ AAA サーバーを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、キーを「myexclusivemumblekey」に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry-interval 7
ciscoasa
(config-aaa-server-host)# key myexclusivemumblekey
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始します。このモードでは、ホストに固有の AAA サーバー パラメータを設定できます。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	AAA サーバーの設定を表示します。

key（クラスタ グループ）

クラスタ制御リンクの制御トラフィックの認証キーを設定するには、クラスタ グループ コンフィギュレーションモードで**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。

key *shared_secret*
no key [*shared_secret*]

構文の説明

shared_secret	共有秘密を 1 ～ 63 文字の ASCII 文字列に設定します。共有秘密は、キーを生成するために使用されます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、データパス トラフィック（接続状態アップデートや転送されるパケットなど）には影響しません。データパス トラフィックは、常にクリア テキストとして送信されます。

例

次に、共有秘密を設定する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# key chuntheunavoidable
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。
enable (cluster group)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルスチェック機能（ユニットのヘルスモニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority (cluster group)	マスター ユニット選定のこのユニットのプライオリティを設定します。

key chain

IGP ピアを認証するためのローテーションキーを設定するには、グローバル コンフィギュレーション モードで **key chain** コマンドを使用します。構成を削除するには、このコマンドの **no** 形式を使用します。

key chain *key-chain-name* **key** *key-id* **key-string** { **0** | **8** } *key-string-text* **cryptographic-algorithm md5** [**accept-lifetime** [*local* | *start-time*] [**duration** { *duration value* | *infinite* | *end-time* }]

no key chain *key-chain-name* **key** *key-id* **key-string** { **0** | **8** } *key-string-text* **cryptographic-algorithm md5** [**accept-lifetime** [*local* | *start-time*] [**duration** { *duration value* | *infinite* | *end-time* }]

構文の説明

key-chain-name	OSPFv2 認証用に設定するキー チェーンの名前。
key-id	キー チェーン内の固有識別子。有効な範囲は 1 ～ 255 です。
0	暗号化されていないパスワードが続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。
key-string-text	キー id のパスワード。文字列には、プレーン テキストまたは暗号化された値を使用できます。
md5	サポートされている暗号化アルゴリズム。md5 のみがサポートされています。
accept-lifetime	（任意）別のデバイスとのキー交換時にデバイスがそのキーを受け入れる期間。
send-lifetime	（任意）別のデバイスとのキー交換時にデバイスがそのキーを送信する期間。

コマンド デフォルト

受け入れまたは送信のライフタイムが指定されていない場合は、デフォルトで常にアクティブになります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• ×

コマンド履歴

リリース	変更内容
9.12(1)	このコマンドが追加されました。

使用上のガイドライン

key chain コマンドを使用して、インターフェイスの OSPFv2 認証で使用されるキーチェーンを設定します。**key id**、**key string,** 、および **cryptographic-algorithm** コマンドを入力する必要があります。**accept and send lifetimes** を入力して、キーのローテーションをスケジュールします。 ライフタイム変数は、セキュアなキー ロールオーバーを処理するのに便利です。デバイスはキーのライフタイムを使用して、特定の期間にキーチェーン内のどのキーがアクティブになるかを判断します。ライフタイムが指定されていない場合、キー チェーン認証は、タイムラインを使用しない MD5 認証と同様に機能します。キーチェーンの設定を削除するには、**no key chain** を使用します。

例

次の例は、キー チェーンの設定コマンドを示しています。

```
ciscoasa(config)# key chain CHAIN1
ciscoasa(config-keychain)# key 1
ciscoasa(config-keychain-key)# key-string 0 CHAIN1KEY1STRING
ciscoasa(config-keychain-key)# cryptographic-algorithm md5
ciscoasa(config-keychain-key)# accept-lifetime 11:22:33 1 SEP 2018 infinite

ciscoasa(config-keychain-key)#
```

例

次の例は、実行中のキーチェーン設定の出力を示しています。

```
ciscoasa# show running key chain
key chain CHAIN2
 key 1
  key-string KEY1CHAIN2
  cryptographic-algorithm md5
 key 2
  accept-lifetime 11:00:12 Sep 1 2018 11:12:12 Sep 1 2018
  cryptographic-algorithm md5
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa# show runing key chain CHAIN1
key chain CHAIN1
 key 1
  key-string CHAIN1KEY1STRING
  accept-lifetime 11:22:33 Sep 1 2018 duration -1
  cryptographic-algorithm md5
ciscoasa#
```

関連コマンド

コマンド	説明
show key chain	設定されたキー チェーンを表示します。

コマンド	説明
show running key chain	現在アクティブなキー チェーンの詳細を表示します。
clear configure key chain	設定されているキー チェーンを削除します。

key config-key password-encryption

暗号キーの生成に使用するマスターパスフレーズを設定し、プレーンテキストのパスワードを暗号化形式で安全に保存するには、グローバル コンフィギュレーション モードで **key config-key password-encryption** コマンドを使用します。パスフレーズで暗号化されたパスワードを復号化するには、このコマンドの no 形式を使用します。

key config-key password-encryption *passphrase* [*old_passphrase*]
no key config-key password-encryption *passphrase*

構文の説明

passphrase	パスフレーズの長さは、8 ～ 128 文字にする必要があります。パスフレーズには、バックスペースと二重引用符を除くすべての文字を使用できます。コマンドにパスフレーズを入力しないと、入力を求めるプロンプトが表示されます。インタラクティブ プロンプトを使用してパスワードを入力し、パスワードがコマンド履歴バッファに記録されないようにします。
old_passphrase	パスフレーズを変更する場合は、以前のパスフレーズを入力します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

マスター パスフレーズを使用する機能としては、次のものがあります。

- OSPF
- EIGRP
- VPN ロード バランシング
- VPN (リモート アクセスおよびサイトツーサイト)

- フェールオーバー
- AAA サーバー
- Logging
- 共有ライセンス

パスワードの暗号化をトリガーするには、**key config-key password-encrypt** コマンドと **password encryption aes** コマンドの両方を任意の順序で入力する必要があります。**write memory** と入力して、暗号化されたパスワードをスタートアップ コンフィギュレーションに保存します。そうしないと、スタートアップ コンフィギュレーション内のパスワードが表示されることがあります。マルチコンテキストモードでは、システム実行スペースに **write memory all** を使用してすべてのコンテキストの設定を保存します。

このコマンドを実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュア セッションにおいてのみです。

暗号化されたパスワードがプレーンテキストパスワードに変換されるため、**no key config-key password-encrypt** コマンドは注意して使用してください。パスワードの暗号化がサポートされていないソフトウェアバージョンにダウングレードするときは、このコマンドの **no** 形式を使用できる場合があります。

フェールオーバーがイネーブルであっても、フェールオーバー共有キーが設定されていない場合に、マスターパスフレーズを変更すると、エラーメッセージが表示されます。このメッセージには、マスター パスフレーズの変更がプレーン テキストとして送信されないよう、フェールオーバー共有キーを入力する必要があることが示されます。

Active/Standby フェールオーバーでパスワードの暗号化を有効化または変更すると、**write standby** が実行され、アクティブな構成がスタンバイユニットに複製されます。この複製が行われない場合、スタンバイユニットの暗号化されたパスワードは、同じパスフレーズを使用している場合でも異なるものになります。構成を複製することで、構成が同じであることが保証されます。Active/Standby フェールオーバーの場合は、手動で **write standby** を入力する必要があります。**write standby** は、Active/Active モードでトラフィックの中断を引き起こす場合があります。これは、新しい構成が同期される前に、セカンダリユニットで構成が消去されるためです。**failover active group 1** および **failover active group 2** コマンドを使用してプライマリ ASA ですべてのコンテキストをアクティブにし、**write standby** を入力してから、**no failover active group 2** コマンドを使用してセカンダリユニットにグループ 2 コンテキストを復元する必要があります。

write erase コマンドに続いて reload コマンドを使用すると、マスター パスフレーズを紛失した場合はそのマスター パスフレーズとすべての設定が削除されます。

例

次に、暗号キーの生成に使用するパスフレーズを設定し、パスワード暗号化をイネーブルにする例を示します。

```
ciscoasa
(config)#
 key config-key password-encryption
Old key: bumblebee
```

```
New key: haverford
Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasa(config)# write memory
```

関連コマンド

コマンド	説明
password encryption aes	パスワードの暗号化をイネーブルにします。
write erase	reload コマンドを続いて使用すると、マスターパスフレーズが紛失された場合にパスフレーズを削除します。

key-hash

オンボードのセキュアコピー（SCP）クライアントのサーバーに対するハッシュ SSH ホストキーを手動で追加するには、サーバー コンフィギュレーション モードで **key-hash** コマンドを使用します。サーバー コンフィギュレーション モードにアクセスするには、まず **ssh pubkey-chain** コマンドを入力します。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。

key-hash { **md5** | **sha256** } *fingerprint*
no key-hash { **md5** | **sha256** } *fingerprint*

構文の説明

fingerprint	ハッシュ キーを入力します。
{md5 | sha256}	使用するハッシュのタイプ（MD5 または SHA-256）を設定します。ASA の構成では、常に SHA-256 が使用されます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
サーバー コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

オンボードの SCP クライアントを使用して、ASA との間でファイルをコピーすることができます。ASA は接続先の各 SCP サーバーの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバーとそのキーを追加または削除できます。

各サーバーについて、SSH ホストの **key-string**（公開キー）または **key-hash**（ハッシュ値）を指定できます。**key-hash** では、すでにハッシュされているキーを入力します（MD5 または SHA-256 キーを使用）。たとえば、**show** コマンドの出力からコピーしたキーを入力します。

例

次に、10.86.94.170 にあるサーバのすでにハッシュされているホスト キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.86.94.170
ciscoasa(config-ssh-pubkey-server)# key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

関連コマンド

コマンド	説明
copy	ASA との間でファイルをコピーします。
key-hash	ハッシュ SSH ホスト キーを入力します。
key-string	公開 SSH ホスト キーを入力します。
ssh pubkey-chain	ASA のデータベースに格納されるサーバーとそのキーを手動で追加または削除します。
ssh stricthostkeycheck	オンボードのセキュア コピー（SCP）クライアントの SSH ホスト キーのチェックをイネーブルにします。

keypair

証明する公開キーのキーペアを指定するには、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 **keypair** 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。

[no] keypair *name* | [**rsa modulus** | **2048** | **4096**] | [**ecdsa elliptic-curve 256** | **384** | **521**] | [**eddsa edwards-curve Ed25519**]

構文の説明

name	CMP 以外の登録用のキー ペアの名前を指定します。
rsa	CMP の手動登録と自動登録用の RSA キーを生成します。
ecdsa	CMP の手動登録と自動登録用の ECDSA キーを生成します。
eddsa	CMP の手動登録と自動登録用の EdDSA キーを生成します。

コマンド デフォルト

デフォルト設定では、キー ペアは含まれません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	新しい EDCSA と RSA のキーペアが追加されました。
9.16(1)	• 2048 ビットより小さい RSA キーサイズの証明書のサポートが削除されました。したがって、RSA モジュラスオプションは、2048 ビット以上の値を表示するように変更されました。 • 新しい EdDSA キーペアが追加されました。

例

次に、central トラストポイントのクリプト 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、central トラストポイント用に証明するキー ペアを指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# keypair exchange
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
crypto key generate dsa	DSA キーを生成します。
crypto key generate rsa	RSA キーを生成します。
default enrollment	登録パラメータをデフォルト値に戻します。

keysize

ユーザー証明書の登録で、ローカルの認証局（CA）サーバーによって生成される公開キーと秘密鍵のサイズを指定するには、CA サーバー コンフィギュレーション モードで **keysize** コマンドを使用します。キーサイズをデフォルトの 1024 ビットの長さ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。

keysize*size*
no keysize

構文の説明

size キーのサイズ（ビット単位）。サイズは次のいずれかになります。

- 512
- 768
- 1024
- 2048
- 4096

コマンド デフォルト

デフォルトでは、このキー ペアの各キーの長さは 1024 ビットです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.13(1)	このコマンドは削除されました。

例

次に、ローカル CA サーバーによってユーザー用に生成される、公開キーと秘密キーのすべてのキー ペアのキーのサイズを 2048 ビットに指定する例を示します。

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

```
ciscoasa
(config-ca-server)
)# keysize 2048
ciscoasa
(config-ca-server)
#
```

次に、ローカル CA サーバーによってユーザー用に生成される、公開キーと秘密キーのすべてのキー ペアのキーのサイズを、デフォルトの 1024 ビットの長さにリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no keysize
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードのコマンドセットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
subject-name-default	CA サーバーが発行するすべてのユーザー証明書でユーザー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。

keysize server

ローカルの認証局（CA）サーバーによって生成される公開キーと秘密鍵のサイズを指定し、CA のキーペアのサイズを設定するには、CA サーバー コンフィギュレーション モードで **keysize server** コマンドを使用します。キーサイズをデフォルトの 1024 ビットの長さ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。

keysize server *size*
no keysize server

構文の説明

size キーのサイズ（ビット単位）。サイズは次のいずれかになります。

- 512
- 768
- 1024
- 2048
- 4096

コマンド デフォルト

デフォルトでは、このキー ペアの各キーの長さは 1024 ビットです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.13(1)	このコマンドは削除されました。

例

次に、CA 証明書のキー サイズを 2048 ビットに指定する例を示します。

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

```
(config-ca-server)
)# keysize server 2048
ciscoasa
(config-ca-server)
#
```

次に、CA 証明書のキー サイズをデフォルトの 1024 ビットにリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no keysize server
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードのコマンド セットへのアクセスを提供し、ローカル CA の設定と管理ができるようにします。
issuer-name	認証局証明書のサブジェクト名 DN を指定します。
keysize	ユーザー証明書のキー ペアのサイズを指定します。
subject-name-default	CA サーバーが発行するすべてのユーザー証明書でユーザー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。

key-string

オンボードのセキュア コピー（SCP）クライアントのサーバーに対するパブリック SSH ホストキーを手動で追加するには、サーバー コンフィギュレーション モードで **key-string** コマンドを使用します。サーバー コンフィギュレーション モードにアクセスするには、まず **ssh pubkey-chain** コマンドを入力します。このコマンドを入力すると、キー ストリングを入力するプロンプトが表示されます。ストリングが構成に保存されると、SHA-256 を使用してハッシュされ、**key-hash** コマンドとして保存されます。したがって、ストリングを削除するときは、**no key-hash** コマンドを使用します。

key-string *key_string*

構文の説明

key_string	公開キーを入力します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
サーバー コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.1(5)	このコマンドが追加されました。

使用上のガイドライン

オンボードの SCP クライアントを使用して、ASA との間でファイルをコピーすることができます。ASA は接続先の各 SCP サーバーの SSH ホストキーを保存します。必要に応じて、ASA データベースから手動でサーバーとそのキーを追加または削除できます。

各サーバーについて、SSH ホストの **key-string**（公開キー）または **key-hash**（ハッシュ値）を指定できます。*key_string* はリモート ピアの Base64 で符号化された RSA 公開キーです。オープン SSH クライアントから（言い換えると .ssh/id_rsa.pub ファイルから）公開キー値を取得できます。Base64 で符号化された公開キーを送信した後、SHA-256 によってそのキーがハッシュされます。

例

次に、10.7.8.9 にあるサーバーのホスト ストリング キーを追加する例を示します。

```
ciscoasa(config)# ssh pubkey-chain
ciscoasa(config-ssh-pubkey-chain)# server 10.7.8.9
ciscoasa(config-ssh-pubkey-server)# key-string
Enter the base 64 encoded RSA public key.
End with the word "exit" on a line by itself
ciscoasa(config-ssh-pubkey-server-string)# c1:b1:30:29:d7:b8:de:6c:97:77:10:d7:46:41:63:87
ciscoasa(config-ssh-pubkey-server-string)# exit
```

次に、保存されたハッシュ キーを表示する例を示します。

```
ciscoasa(config-ssh-pubkey-server)# show running-config ssh
ssh scopy enable
ssh stricthostkeycheck
ssh pubkey-chain
  server 10.7.8.9
    key-hash sha256
65:d9:9d:fe:1a:bc:61:aa:64:9d:fc:ee:99:87:38:df:a8:8e:d9:e9:ff:42:de:e8:8d:2d:bf:a9:2b:85:2e:19
```

関連コマンド

コマンド	説明
copy	ASA との間でファイルをコピーします。
key-hash	ハッシュ SSH ホスト キーを入力します。
key-string	公開 SSH ホスト キーを入力します。
ssh pubkey-chain	ASA のデータベースに格納されるサーバーとそのキーを手動で追加または削除します。
ssh stricthostkeycheck	オンボードのセキュア コピー（SCP）クライアントの SSH ホスト キーのチェックをイネーブルにします。

kill

Telnet セッションを終了するには、特権 EXEC モードで **kill** コマンドを使用します。

kill*telnet_id*

構文の説明

telnet_id	Telnet セッションの ID を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

kill コマンドを使用すると、Telnet セッションを終了できます。Telnet セッションの ID を表示するには、who コマンドを使用します。Telnet セッションを終了すると、ASA は警告を表示することなく、すべてのアクティブなコマンドを終了して接続をドロップします。

例

次に、ID「2」の Telnet セッションを終了する例を示します。最初に、who コマンドを入力して、アクティブな Telnet セッションのリストを表示します。次に、**kill 2** コマンドを入力して、ID「2」の Telnet セッションを終了します。

```
ciscoasa# who
2: From 10.10.54.0

ciscoasa# kill 2
```

関連コマンド

コマンド	説明
telnet	ASA への Telnet アクセスを設定します。
who	アクティブな Telnet セッションのリストを表示します。

l2 – lof

l2tp tunnel hello

L2TP over IPsec 接続における hello メッセージの間隔を指定するには、グローバル コンフィギュレーション モードで **l2tp tunnel hello** コマンドを使用します。この間隔をデフォルト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。

l2tp tunnel hello *interval*
no l2tp tunnel hello *interval*

構文の説明

interval	hello メッセージ間の間隔（秒）。デフォルトは 60 秒です。指定できる範囲は 10 ～ 300 秒です。

コマンド デフォルト

デフォルトは 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

l2tp tunnel hello コマンドは、ASA による L2TP 接続の物理層に関する問題の検出を有効にします。デフォルトは 60 秒です。デフォルト設定を使用すると、L2TP トンネルが 180 秒後に切断されることが予想されます。60 秒未満の値に設定すると、問題が発生している接続はより早く切断されます。L2TP の最大再試行回数は 3 回です。

例

次に、hello メッセージ間の間隔を 30 秒に設定する例を示します。

```
ciscoasa(config)# l2tp tunnel hello 30
```

関連コマンド

コマンド	説明
show vpn-sessiondb detail remote filter protocol L2TPOverIPsec	L2TP 接続の詳細を表示します。

コマンド	説明
vpn-tunnel-protocol l2tp-ipsec	L2TP を特定のトンネル グループのトンネリング プロトコルとしてイネーブルにします。

lacp max-bundle

EtherChannel チャネルグループで許可されるアクティブインターフェイスの最大数を指定するには、インターフェイス コンフィギュレーション モードで **lacp max-bundle** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

lacp max-bundle *number*
no lacp max-bundle

構文の説明

number このチャネル グループで許可されるアクティブ インターフェイスの最大数を 1 ～ 8 の範囲内で指定します。9.2(1) 以降では、最大数が 16 に引き上げられています。スイッチが 16 個のアクティブ インターフェイスをサポートしていない場合、このコマンドは必ず 8 以下に設定する必要があります。

コマンド デフォルト

（9.1 以前）デフォルトは 8 です。

（9.2(1) 以降）デフォルトは 16 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.2(1)	アクティブ インターフェイスの数が 8 から 16 に増加しました。

使用上のガイドライン

このコマンドは、ポートチャネル インターフェイスに対して入力します。チャネル グループあたりのアクティブ インターフェイスの最大数は 8 です。このコマンドは、最大数を減らす場合に使用します。

例

次に、EtherChannel のインターフェイスの最大数を 4 に設定する例を示します。

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# lacp max-bundle 4
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

lacp port-priority

EtherChannel における物理インターフェイスのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **lacp port-priority** コマンドを使用します。プライオリティをデフォルトに設定するには、このコマンドの **no** 形式を使用します。

lacp port-priority *number*
no lacp port-priority

構文の説明

number プライオリティ（1 ～ 65535）を設定します。数字が大きいほど、プライオリティは低くなります。

コマンド デフォルト

デフォルトは 32768 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

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。使用可能な数よりも多くのインターフェイスを割り当てた場合、ASA ではこの設定を使用して、アクティブ インターフェイスとスタンバイ インターフェイスを決定します。ポート プライオリティ設定がすべてのインターフェイスで同じ場合、プライオリティはインターフェイス ID（スロット/ポート）で決まります。最も小さいインターフェイス ID が、最も高いプライオリティになります。たとえば、GigabitEthernet 0/0 のプライオリティは GigabitEthernet 0/1 よりも高くなります。

あるインターフェイスについて、インターフェイス ID は大きいが、そのインターフェイスがアクティブになるように優先順位を付ける場合は、より小さい値を持つようにこのコマンドを設定します。たとえば、GigabitEthernet 1/3 を GigabitEthernet 0/7 よりも前にアクティブにするには、0/7 インターフェイスでのデフォルトの 32768 に対し、1/3 インターフェイスで **lacp port-priority** 値を 12345 にします。

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。**lacp system-priority** コマンドを参照してください。

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバインターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。

例

次に、GigabitEthernet 0/2 のポート プライオリティの値を小さくして、EtherChannel で GigabitEthernet 0/0 および 0/1 よりも先に使用されるように設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# lacp port-priority 1234
ciscoasa(config-if)# channel-group 1 mode active
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。

コマンド	説明
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

lacp system-priority

EtherChannel の場合、ASA の LACP システムのプライオリティをグローバルに設定するには、グローバル コンフィギュレーション モードで **lacp system-priority** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

lacp system-priority *number*
no lacp system-priority

構文の説明

number LACP システム プライオリティを 1 ～ 65535 の範囲で設定します。デフォルトは 32768 です。数字が大きいほど、プライオリティは低くなります。このコマンドは、ASA に対してグローバルです。

コマンド デフォルト

デフォルトは 32768 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

EtherChannel の反対の端にあるデバイスのポート プライオリティが衝突している場合、システム プライオリティを使用して使用するポート プライオリティが決定されます。EtherChannel 内でのインターフェイス プライオリティについては、**lacp port-priority** コマンドを参照してください。

例

次に、システムのプライオリティをデフォルトよりも高くする（小さい数値を設定する）例を示します。

```
ciscoasa(config)# lacp system-priority 12345
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

ldap-attribute-map

既存のマッピング構成を LDAP ホストにバインドするには、AAA サーバー ホスト コンフィギュレーション モードで **ldap-attribute-map** コマンドを使用します。バインデ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。

ldap-attribute-map *map-name*
no ldap-attribute-map *map-name*

構文の説明

map-name	LDAP 属性マッピング コンフィギュレーションを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

シスコ定義の LDAP 属性名が使いやすさやその他の要件を満たしていない場合は、独自の属性名を作成し、それをシスコの属性にマッピングして、作成された属性コンフィギュレーションを LDAP サーバーにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、未入力の属性マップを作成します。このコマンドにより、LDAP 属性マップ コンフィギュレーション モードが開始されます。このコマンドでは、「ldap」の後にハイフンを入力しないでください。
2. LDAP 属性マップ コンフィギュレーション モードで **map-name** コマンドと **map-value** コマンドを使用して、属性マッピング構成に情報を入力します。
3. AAA サーバーホストモードで **ldap-attribute-map** コマンドを使用し、属性マップ構成を LDAP サーバーにバインドします。

例

次に、AAA サーバ ホスト コンフィギュレーション モードで、myldapmap という名前の既存の属性マップを ldapsvr1 という名前の LDAP サーバにバインドするコマンドの例を示します。

```
ciscoasa(config)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-attribute-map myldapmap
ciscoasa(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
ldap attribute-map (global configuration mode)	ユーザー定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
map-name	ユーザー定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。
map-value	ユーザー定義の属性値をシスコ属性にマッピングします。
show running-config ldap attribute-map	特定の実行 LDAP 属性マッピング コンフィギュレーションまたはすべての実行属性マッピング コンフィギュレーションを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

ldap-base-dn

サーバーが認可要求を受信したときに検索を開始する、LDAP階層内の位置を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **ldap-base-dn** コマンドを使用します。AAA サーバー ホスト コンフィギュレーション モードは、AAA サーバー プロトコル コンフィギュレーション モードからアクセスできます。この指定を削除して、検索の開始位置をリストの先頭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。

ldap-base-dn*string*
no ldap-base-dn

構文の説明

string サーバーが認可要求を受信したときに検索を開始するLDAP階層内の位置を指定する、最大128文字のストリング（たとえば、OU=Cisco）。大文字と小文字は区別されます。

コマンド デフォルト

リストの先頭から検索を開始します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは LDAP サーバーでのみ有効です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバーを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ベース DN を starthere に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
```

```
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host
)# ldap-base-dn starthere
ciscoasa
(config-aaa-server-host)#
exit
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバー パラメータを設定できるようにします。
ldap-scope	サーバーが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。
ldap-naming-attribute	LDAP サーバー上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。

ldap-defaults

LDAP デフォルト値を定義するには、crl 設定コンフィギュレーション モードで **ldap-defaults** コマンドを使用します。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのデフォルト値は、LDAP サーバーが必要とする場合にのみ使用されます。LDAPデフォルト値を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-defaults *server* [*port*]
no ldap-defaults

構文の説明

port （任意）LDAP サーバー ポートを指定します。このパラメータが指定されていない場合、ASA は標準の LDAP ポート（389）を使用します。

server LDAP サーバーの IP アドレスまたはドメイン名を指定します。CRL 配布ポイント内にサーバーが存在する場合、この値はそのサーバーによって上書きされます。

コマンド 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

次の表に、コマンドを入力できるモードを示します。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
crl 設定コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、デフォルト ポート（389）に LDAP デフォルト値を定義する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-defaults ldapdomain4 8389
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。

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。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-dn

CRL 取得のために認証を要求する LDAP サーバーに X.500 認定者名とパスワードを渡すには、crl 設定コンフィギュレーション モードで **ldap-dn** コマンドを使用します。crl 設定コンフィギュレーション モードは、暗号 CA トラストポイント コンフィギュレーション モードからアクセスできます。これらのパラメータは、LDAP サーバーで必要な場合のみ使用されます。LDAP DN を指定しない場合は、このコマンドの **no** 形式を使用します。

ldap-dn *x.500-name password*
no ldap-dn

構文の説明

password	この認定者名のパスワードを定義します。最大のフィールドの長さは 128 文字です。
x.500-name	この CRL データベースにアクセスするためのディレクトリ パスを定義します（たとえば、cn=crl,ou=certs,o=CAName,c=US）。最大のフィールドの長さは 128 文字です。

コマンド デフォルト

デフォルト値は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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
crl 設定コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central の X.500 名として CN=admin,OU=devtest,O=engineering、パスワードとして xxzzyy を指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# ldap-dn cn=admin,ou=devtest,o=engineering xxzzyy
```

関連コマンド

コマンド	説明
crl configure	crl 設定コンフィギュレーション モードを開始します。
crypto ca trustpoint	CA トラストポイント コンフィギュレーション モードを開始します。
protocol ldap	CRL の取得方法として LDAP を指定します。

ldap-group-base-dn

ダイナミック アクセス ポリシーによってグループ検索に使用される Active Directory 階層の基本グループを指定するには、AAA サーバー ホスト コンフィギュレーション モードで **ldap-group-base-dn** コマンドを使用します。このコマンドを実行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。

ldap-group-base-dn [*string*]
no ldap-group-base-dn [*string*]

構文の説明

string サーバーが検索を開始する Active Directory 階層内の位置を指定する、最大 128 文字のストリング。大文字と小文字は区別されます。たとえば、ou=Employees を指定します。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

コマンド デフォルト

デフォルトの動作や値はありません。グループ検索 DN を指定しない場合、ベース DN から検索が開始されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。

使用上のガイドライン

ldap-group-base-dn コマンドは、LDAP を使用する Active Directory サーバーにのみ適用され、**show ad-groups** コマンドがグループ検索を開始するために使用する Active Directory 階層レベルを指定します。検索で取得されたグループは、ダイナミック グループ ポリシーによって特定のポリシーの選択基準として使用されます。

例

次に、組織の部門（ou）レベルの Employees から検索を開始するようにグループ ベース DN を設定する例を示します。

```
ciscoasa(config-aaa-server-host)# ldap-group-base-dn ou=Employees
```

関連コマンド

コマンド	説明
group-search-timeout	グループのリストについて Active Directory サーバーからの応答を ASA が待機する時間を調整します。
show ad-groups	Active Directory サーバー上でリストされるグループを表示します。

ldap-login-dn

システムがバインドするディレクトリオブジェクトの名前を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **ldap-login-dn** コマンドを使用します。AAA サーバー ホスト コンフィギュレーション モードは、AAA サーバー プロトコル 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。

ldap-login-dn*string*
no ldap-login-dn

構文の説明

string LDAP 階層内のディレクトリ オブジェクトの名前を指定する、最大 128 文字のストリング。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは LDAP サーバーでのみ有効です。サポートされるストリングの最大長は 128 文字です。

Microsoft Active Directory サーバーなどの一部の LDAP サーバーでは、他の LDAP 動作の要求を受け入れる前に、ASA が認証済みバインディングを介してハンドシェイクを確立している必要があります。ASA は、ログイン DN フィールドをユーザー認証要求にアタッチして、認証済みバインディングに対して識別情報を示します。ログイン DN フィールドには、ASA の認証特性が記述されます。これらの特性は、管理者特権を持つユーザーの特性に対応している必要があります。

string 変数には、VPN コンセントレータの認証済みバインディングのディレクトリ オブジェクト名を入力します（たとえば、cn=Administrator, cn=users, ou=people, dc=XYZ Corporation, dc=com）。匿名アクセスの場合は、このフィールドをブランクのままにします。

例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバーを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ログイン DN を myobjectname に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host)
# ldap-login-dn myobjectname
ciscoasa(config-aaa-server
-host)
#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバー パラメータを設定できるようにします。
ldap-base-dn	サーバーが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバーでのみ有効です。
ldap-naming-attribute	LDAP サーバー上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-scope	サーバーが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-login-password

LDAP サーバーのログインパスワードを指定するには、AAA サーバー ホスト コンフィギュレーション モードで **ldap-login-password** コマンドを使用します。AAA サーバー ホスト コンフィギュレーション モードは、AAA サーバー プロトコル コンフィギュレーション モードからアクセスできます。このパスワード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。

ldap-login-password*string*
no ldap-login-password

構文の説明

string 最大 64 文字の英数字のパスワード。大文字と小文字は区別されます。パスワードにスペース文字を含めることはできません。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは LDAP サーバーでのみ有効です。パスワードの最大長は 64 文字です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバーを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP ログイン パスワードを obscurepassword に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server)# timeout 9
```

```
ciscoasa
(config-aaa-server)# retry 7
ciscoasa(config-aaa-server)# ldap-login-password obscurepassword
ciscoasa
(config-aaa-server)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバー パラメータを設定できるようにします。
ldap-base-dn	サーバーが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-naming-attribute	LDAP サーバー上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。
ldap-scope	サーバーが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-naming-attribute

相対識別名属性を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **ldap-naming-attribute** コマンドを使用します。AAA サーバー ホスト コンフィギュレーション モードは、AAA サーバー プロトコル コンフィギュレーション モードからアクセスできます。この仕様を削除するには、このコマンドの **no** 形式を使用します。

ldap-naming-attribute*string*
no ldap-naming-attribute

構文の説明

string LDAP サーバー上のエントリを一意に識別する、最大 128 文字の英数字の相対認定者名属性を指定します。大文字と小文字は区別されます。文字列でスペースは使用できませんが、他の特殊文字は使用できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

LDAP サーバー上のエントリを一意に識別するための、相対認定者名属性を指定します。共通の命名属性は、一般名（cn）とユーザー ID（uid）です。

このコマンドは LDAP サーバーでのみ有効です。サポートされるストリングの最大長は 128 文字です。

例

次に、ホスト 1.2.3.4 に srvgrp1 という名前の LDAP AAA サーバーを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP 命名属性を cn に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
```

```
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server
-host
)# ldap-naming-attribute cn
ciscoasa
(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバー パラメータを設定できるようにします。
ldap-base-dn	サーバーが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバーでのみ有効です。
ldap-scope	サーバーが認可要求を受信した場合に検索する LDAP 階層の範囲を指定します。

ldap-over-ssl

セキュアな SSL 接続を ASA と LDAP サーバーの間で確立するには、AAA サーバー ホスト コンフィギュレーション モードで **ldap-over-ssl** コマンドを使用します。接続の SSL を無効にするには、このコマンドの **no** 形式を使用します。

ldap-over-ssl [**enable** | **reference-identity** *ref_id_name*]

no ldap-over-ssl *ref_id_name* [enable|reference-identity]

構文の説明

enable	SSL で LDAP サーバーへの接続を保護することを指定します。
reference-identity *ref_id_name*	LDAP サーバー ID を検証するための参照 ID 名を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.18(1)	このコマンドは、LDAP サーバー ID を検証するように拡張されました。

使用上のガイドライン

このコマンドを使用して、SSL で ASA と LDAP サーバー間の接続を保護することを指定します。

（注） プレーン テキスト認証を使用している場合は、この機能をイネーブルにすることを推奨します。**sasl-mechanism command.** を参照してください。

例

次に、AAA サーバー ホスト コンフィギュレーション モードで、ASA と LDAP サーバー ldapsvr1（IP アドレスは 10.10.0.1）間の接続に対して SSL を有効にするコマンドの例を示します。PLAIN SASL 認証メカニズムも設定します。

```
ciscoasa(config)# aaa-server ldapsvr1 protocol ldap
ciscoasa(config-aaa-server-host)# aaa-server ldapsvr1 host 10.10.0.1
ciscoasa(config-aaa-server-host)# ldap-over-ssl enable
ciscoasa(config-aaa-server-host)#
```

参照 ID 名を指定して LDAP サーバー ID を検証するには、**reference-identity** *ref_id_name* を使用します。参照 ID オブジェクトは、一致基準を指定し、**crypto ca reference-identity refidname** を使用して作成されます。LDAP AAA サーバー構成で参照 ID を設定すると、ASA は LDAP サーバー証明書と一致するホスト名を見つけようとします。ホストの解決に失敗するか、一致するものが見つからない場合、エラーメッセージが表示されて接続が終了します。

```
asa(config-aaa-server-host)# ldap-over-ssl ?

aaa-server-host mode commands/options:
  enable              Require an SSL connection to the LDAP server
  reference-identity  Enter reference-identity name to validate LDAP server identity

asa(config-aaa-server-host)# ldap-over-ssl reference-identity ?

aaa-server-host mode commands/options:
  WORD < 65 char  Enter reference-identity name to validate LDAP server identity
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname ?

aaa-server-host mode commands/options:
  <cr>
asa(config-aaa-server-host)# ldap-over-ssl reference-identity refidname
```

show running-config aaa server は、設定された参照 ID 名をオプションの 1 つとして表示します。

```
asa(config-aaa-server-host)# show running-config aaa-server
aaa-server ldaps protocol ldap
aaa-server ldaps (manif) host 10.86.93.107
server-port 636
ldap-base-dn CN=Users,DC=BXBCASERVERS,DC=COM
ldap-scope subtree
ldap-naming-attribute cn
ldap-login-password *****
ldap-login-dn CN=administrator,CN=Users,DC=BXBCASERVERS,DC=com
ldap-over-ssl enable
ldap-over-ssl reference-identity refidname
server-type microsoft
```

関連コマンド

コマンド	説明
sasl-mechanism	LDAP クライアントとサーバーの間に SASL 認証を指定します。

コマンド	説明
server-type	LDAP サーバー ベンダーに Microsoft または Sun のいずれかを指定します。
ssl-client-certificate	LDAPS を使用する場合に、ASA がクライアント証明書として LDAP サーバーに提示する証明書を指定します。
crypto ca reference-identity refidname	参照 ID オブジェクトを設定するには、次の手順を実行します。

ldap-scope

サーバーが認可要求を受信したときに検索するLDAP階層内の範囲を指定するには、AAAサーバー ホスト コンフィギュレーション モードで **ldap-scope** コマンドを使用します。AAA サーバー ホスト コンフィギュレーション モードは、AAA サーバー プロトコル 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。

ldap-scope*scope*
no ldap-scope

構文の説明

scope サーバーが認可要求を受信したときに検索する LDAP 階層内のレベルの数を指定します。有効な値は次のとおりです。

- **onelevel**：ベース DN の 1 つ下のレベルのみを検索します。
- **subtree**：ベース DN の下のレベルをすべて検索します。

コマンド デフォルト

デフォルト値は **onelevel** 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

scope に **onelevel** を指定すると、ベース DN の 1 つ下のレベルのみが検索されるため、検索速度が向上します。**subtree** を指定すると、ベース DN の下のレベルがすべて検索されるため、検索速度が低下します。

このコマンドは LDAP サーバーでのみ有効です。

例

次に、ホスト 1.2.3.4 に svrgrp1 という名前の LDAP AAA サーバーを設定し、タイムアウトを 9 秒、再試行間隔を 7 秒、LDAP 範囲を subtree に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol ldap
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# ldap-scope subtree
ciscoasa
(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始し、ホスト固有の AAA サーバー パラメータを設定できるようにします。
ldap-base-dn	サーバーが認可要求を受信した場合に検索を開始する LDAP 階層の位置を指定します。
ldap-login-dn	システムがバインドするディレクトリ オブジェクト名を指定します。
ldap-login-password	ログイン DN のパスワードを指定します。このコマンドは LDAP サーバーでのみ有効です。
ldap-naming-attribute	LDAP サーバー上のエントリを一意に識別する、1 つ以上の相対識別名属性を指定します。

leap-bypass

LEAP バイパスを有効にするには、グループ ポリシー コンフィギュレーション モードで **leap-bypass enable** コマンドを使用します。LEAP バイパスを無効にするには、**leap-bypass disable** コマンドを使用します。実行コンフィギュレーションから LEAP バイパス属性を削除するには、このコマンドの **no** 形式を使用します。このオプションにより、別のグループ ポリシーから LEAP バイパスの値を継承できます。

leap-bypass { **enable** | **disable** }
no leap-bypass

構文の説明

disable	LEAP バイパスをディセーブルにします。
enable	LEAP バイパスをイネーブルにします。

コマンド デフォルト

LEAP バイパス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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

LEAP バイパスをイネーブルにすると、VPN ハードウェア クライアントの背後にある無線デバイスからの LEAP パケットは、ユーザー認証の前に VPN トンネルを通過できます。これにより、シスコ ワイヤレス アクセス ポイント デバイスを使用するワークステーションで LEAP 認証を確立できるようになります。デバイスは、ユーザー認証ごとに認証を再実行できます。

インタラクティブ ハードウェア クライアント認証をイネーブルにした場合、この機能は正常に動作しません。

詳細については、CLI 設定ガイドを参照してください。

（注） 認証されていないトラフィックがトンネルを通過できるようにすると、セキュリティリスクが発生する可能性があります。

例

次の例は、「FirstGroup」という名前のグループポリシーにLEAPバイパスを設定する方法を示しています。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# leap-bypass enable
```

関連コマンド

コマンド	説明
secure-unit-authentication	VPNハードウェアクライアントに、トンネルを開始するたびにユーザー名とパスワードによる認証を要求します。
user-authentication	VPN ハードウェアクライアントの背後にいるユーザーに対して、接続前に ASA に識別情報を示すように要求します。

license

要求の送信元の組織を示すために ASA からクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定するには、scansafe 汎用オプション コンフィギュレーション モードで **license** コマンドを使用します。ライセンスを削除するには、このコマンドの **no** 形式を使用します。

license*hex_key*
no license [*hex_key*]

構文の説明

hex_key	16 バイトの 16 進数の形式で認証キーを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

各 ASA は、クラウド Web セキュリティから取得した認証キーを使用する必要があります。クラウド Web セキュリティでは認証キーを使用して、Web 要求に関連付けられた会社を識別し、ASA が有効なお客様に関連付けられていることを確認できます。

ASA では、2 つの認証キー（企業キーおよびグループ キー）のいずれか 1 つを使用できます。

企業認証キー

企業認証キーは、同一企業内の複数の ASA で使用できます。このキーは、単に ASA のクラウド Web セキュリティ サービスを有効にします。管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。生成したキーは後で使用するために電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、https://www.cisco.com/c/ja_jp/products/index.html から入手できます。

グループ認証キー

グループ認証キーは 2 つの機能を実行する各 ASA に固有の特別なキーです。

- 1 つの ASA のクラウド Web セキュリティ サービスを有効にします。
- ASA からのすべてのトラフィックが識別されるため、ASA ごとに ScanCenter ポリシーを作成できます。

管理者は ScanCenter（https://scancenter.scansafe.com/portal/admin/login.jsp）でこのキーを生成します。生成したキーは後で使用するために電子メールで送信できます。ScanCenter では、後でこのキーを検索できません。ScanCenter には、最後の 4 桁だけが表示されます。詳細については、クラウド Web セキュリティのマニュアルを参照してください。マニュアルは、https://www.cisco.com/c/ja_jp/products/index.html から入手できます。

例

次に、プライマリ サーバーのみを設定する例を示します。

```
scansafe general-options
 server primary ip 180.24.0.62 port 8080
 retry-count 5
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合のデフォルトのユーザー名やグループを指定します。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定します。
match user group	ユーザーまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、クラウド Web セキュリティプロキシサーバーをポーリングする前に ASA が待機する時間です。

コマンド	説明
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバー オプションを設定します。
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバーの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバーが現在のアクティブ サーバー、バックアップ サーバー、または到達不能のいずれであるか、サーバーのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザーまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

license-server address

参加者が使用する共有ライセンスサーバーの IP アドレスと共有秘密を指定するには、グローバル コンフィギュレーション モードで **license-server address** コマンドを使用します。共有ライセンスへの参加を無効にするには、このコマンドの **no** 形式を使用します。共有ライセンスを使用すると、ASA の 1 台を共有ライセンスサーバーに、残りの ASA を共有ライセンス参加者として設定することで、多数の SSL VPN セッションを購入し、ASA のグループ間で必要に応じてセッションを共有できます。

license-server address *address* **secret** *secret* [**port port**]
no license-server address [*address* **secret** *secret* [**port port**]]

構文の説明

address	共有ライセンス サーバーの IP アドレスを指定します。
port *port*	（任意）**license-server port** コマンドを使用してサーバー構成のデフォルトポートを変更した場合は、その変更に合わせてバックアップサーバーのポート（1 ～ 65535）を設定します。デフォルトのポートは 50554 です。
secret *secret*	共有秘密を指定します。共有秘密は、**license-server secret** コマンドを使用してサーバーに設定された秘密と一致する必要があります。

コマンド デフォルト

デフォルトのポートは 50554 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

共有ライセンス参加ユニットには、共有ライセンス参加キーが必要です。インストールされているライセンスを確認するには、**show activation-key** コマンドを使用します。

参加ユニットごとに共有ライセンス サーバーを 1 つのみ指定できます。

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバーとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバーのライセンスを購入します。
2. いずれの ASA を共有ライセンス バックアップ サーバーを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （オプション）別の ASA を共有ライセンス バックアップ サーバーとして指定します。バックアップ サーバーには 1 台のみ指定できます。

（注） 共有ライセンス バックアップ サーバーに必要なのは参加ライセンスのみです。

1. 共有ライセンス サーバー上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
2. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバーに登録します。

（注） 参加者は IP ネットワークを経由してサーバーと通信できる必要がありますが、同じサブネット上にある必要はありません。

1. 共有ライセンス サーバーは、参加者がサーバーにポーリングするべき頻度の情報で応答します。
2. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバーに 50 セッション単位で追加セッションの要求を送信します。
3. 共有ライセンス サーバーは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

（注） 共有ライセンスサーバーは、ローカル セッションを使い果たした場合に共有ライセンス プールに参加もできます。参加には参加ライセンスもサーバー ライセンスも必要ありません。

1. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバーは使用可能な限りのセッション数で応答します。
2. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバーが要求に適切に対応できるまで続けます。
3. 参加者の負荷が減少した場合、参加者はサーバーに共有セッションを解放するようにメッセージを送信します。

（注） ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

参加者とサーバー間の通信問題

参加者とサーバー間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔3倍の時間が経過した後で、サーバーはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバーに到達できない場合、参加者はサーバーから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24時間を経過しても参加者がまだライセンス サーバーと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバーに再接続したが、サーバーが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバーは、参加者に再割り当てできる限りのセッション数で応答します。

例

次に、ライセンス サーバーの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバーの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバー コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server backup address	参加者の共有ライセンス バックアップ サーバーを指定します。
license-server backup backup-id	メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバーになるユニットをイネーブルにします。

コマンド	説明
license-server port	サーバーが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバーに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバー コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server backup address

参加者が使用する共有ライセンス バックアップ サーバーの IP アドレスを特定するには、グローバル コンフィギュレーション モードで **license-server backup address** コマンドを使用します。バックアップサーバーの使用を無効にするには、このコマンドの **no** 形式を使用します。

license-server backup address *address*
no license-server address [**address**]

構文の説明

address	共有ライセンス バックアップ サーバーの IP アドレスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

共有ライセンス バックアップ サーバーには、 **license-server backup enable** コマンドが設定されている必要があります。

例

次に、ライセンス サーバーの IP アドレスおよび共有秘密、ならびにバックアップ ライセンス サーバーの IP アドレスの設定例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup address 10.1.1.2
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。

コマンド	説明
clear configure license-server	共有ライセンス サーバー コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。
license-server backup backup-id	メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバーになるユニットをイネーブルにします。
license-server port	サーバーが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバーに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバー コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server backup backup-id

メイン共有ライセンスサーバー構成で共有ライセンスバックアップサーバーを指定するには、グローバル コンフィギュレーション モードで **license-server backup backup-id** コマンドを使用します。バックアップサーバー構成を削除するには、このコマンドの **no** 形式を使用します。

license-server backup *address* **backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]
no license-server backup *address* [**backup-id** *serial_number* [**ha-backup-id** *ha_serial_number*]]

構文の説明

address	共有ライセンス バックアップ サーバーの IP アドレスを指定します。
backup-id*serial_number*	共有ライセンスバックアップサーバーのシリアル番号を指定します。
ha-backup-id *ha_serial_number*	バックアップサーバでフェールオーバーを使用する場合は、セカンダリ共有ライセンスバックアップサーバのシリアル番号を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

1 つのバックアップ サーバとそのオプションのスタンバイ ユニットのみを指定できます。

バックアップサーバーのシリアル番号を表示するには、**show activation-key** コマンドを入力します。

参加ユニットをバックアップサーバーとして有効にするには、**license-server backup enable** コマンドを使用します。

共有ライセンス バックアップ サーバーは、バックアップの役割を実行する前にメインの共有ライセンス サーバーへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバーは共有ライセンス情報に加えてサーバー設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サーバーとバックアップ サーバーは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバーはリロード後でもバックアップの役割を実行できます。

メイン サーバーがダウンすると、バックアップ サーバーがサーバー動作を引き継ぎます。バックアップ サーバーは継続して最大 30 日間動作できます。30 日を超えると、バックアップ サーバーは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン サーバーをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバーが復旧した場合、メイン サーバーはバックアップ サーバーと同期してから、サーバー動作を引き継ぎます。

バックアップ サーバーがアクティブでないときは、メインの共有ライセンス サーバーの通常の参加者として動作します。

（注） メインの共有ライセンス サーバーの初回起動時には、バックアップ サーバーは独立して 5 日間のみ動作できます。動作制限は 30 日に到達するまで日ごとに増加します。また、メイン サーバーがその後短時間でもダウンした場合、バックアップ サーバーの動作制限は日ごとに減少します。メイン サーバーが復旧した場合、バックアップ サーバーは再び日ごとに増加を開始します。たとえば、メイン サーバーが 20 日間ダウンしていて、その期間中バックアップ サーバーがアクティブであった場合、バックアップ サーバーには、10 日間の制限のみが残っています。バックアップ サーバーは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバー コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバーを指定します。
license-server backup enable	共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバーになるユニットをイネーブルにします。
license-server port	サーバーが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバーに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバー コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server backup enable

このユニットを共有ライセンス バックアップ サーバーとして有効にするには、グローバル コンフィギュレーション モードで **license-server backup enable** コマンドを使用します。バックアップサーバーを無効にするには、このコマンドの **no** 形式を使用します。

license-server backup enable *interface_name*
no license-server enable *interface_name*

構文の説明

interface_name	参加ユニットがバックアップ サーバーとの通信に使用するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

バックアップ サーバーには、共有ライセンス参加キーが必要です。

共有ライセンス バックアップ サーバーは、バックアップの役割を実行する前にメインの共有ライセンス サーバーへの登録に成功している必要があります。登録時には、メインの共有ライセンス サーバーは共有ライセンス情報に加えてサーバー設定もバックアップと同期します。情報には、登録済み参加者の一覧および現在のライセンス使用状況が含まれます。メイン サーバーとバックアップ サーバーは、10 秒間隔でデータを同期します。初回同期の後で、バックアップ サーバーはリロード後でもバックアップの役割を実行できます。

メイン サーバーがダウンすると、バックアップ サーバーがサーバー動作を引き継ぎます。バックアップ サーバーは継続して最大 30 日間動作できます。30 日を超えると、バックアップ サーバーは参加者へのセッション発行を中止し、既存のセッションはタイムアウトします。メイン

サーバーをこの 30 日間中に確実に復旧するようにします。クリティカル レベルの syslog メッセージが 15 日めに送信され、30 日めに再送信されます。

メイン サーバーが復旧した場合、メイン サーバーはバックアップ サーバーと同期してから、サーバー動作を引き継ぎます。

バックアップ サーバーがアクティブでないときは、メインの共有ライセンス サーバーの通常の参加者として動作します。

（注） メインの共有ライセンス サーバーの初回起動時には、バックアップ サーバーは独立して 5 日間のみ動作できます。動作制限は30日に到達するまで日ごとに増加します。また、メインサーバーがその後短時間でもダウンした場合、バックアップサーバーの動作制限は日ごとに減少します。メイン サーバーが復旧した場合、バックアップ サーバーは再び日ごとに増加を開始します。たとえば、メイン サーバーが 20 日間ダウンしていて、その期間中バックアップ サーバーがアクティブであった場合、バックアップ サーバーには、10 日間の制限のみが残っています。バックアップ サーバーは、非アクティブなバックアップとしてさらに 20 日間が経過した後で、最大の 30 日間まで「充電」されます。この充電機能は共有ライセンスの誤使用を防ぐために実装されています。

例

次に、ライセンス サーバーと共有秘密を指定し、このユニットを内部インターフェイスと dmz インターフェイス上のバックアップ共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server address 10.1.1.1 secret farscape
ciscoasa(config)# license-server backup enable inside
ciscoasa(config)# license-server backup enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバー コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバーを指定します。
license-server backup backup-id	メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。

コマンド	説明
license-server enable	共有ライセンス サーバーになるユニットをイネーブルにします。
license-server port	サーバーが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバーに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバー コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server enable

このユニットを共有ライセンスサーバーとして指定するには、グローバル コンフィギュレーション モードで **license-server enable** コマンドを使用します。共有ライセンスサーバーを無効にするには、このコマンドの **no** 形式を使用します。共有ライセンスを使用すると、ASA の 1 台を共有ライセンスサーバーに、残りの ASA を共有ライセンス参加者として設定することで、多数の SSL VPN セッションを購入し、ASA のグループ間で必要に応じてセッションを共有できます。

license-server enable *interface_name*
no license-server enable *interface_name*

構文の説明

interface_name	参加ユニットがサーバーとの通信に使用するインターフェイスを指定します。このコマンドは必要なインターフェイスの数だけ繰り返せます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

共有ライセンス サーバには、共有ライセンス サーバ キーが必要です。インストールされているライセンスを確認するには、**show activation-key** コマンドを使用します。

次に、共有ライセンスの動作手順を示します。

1. いずれの ASA を共有ライセンス サーバーとするかを決定し、デバイス シリアル番号を使用する共有ライセンス サーバーのライセンスを購入します。

2. いずれの ASA を共有ライセンス バックアップ サーバーを含む共有ライセンス参加者とするかを決定し、各デバイス シリアル番号を使用して各デバイスに対して共有ライセンス参加ライセンスを取得します。
3. （オプション）別の ASA を共有ライセンス バックアップ サーバーとして指定します。バックアップ サーバーには 1 台のみ指定できます。

（注） 共有ライセンス バックアップ サーバーに必要なのは参加ライセンスのみです。

1. 共有ライセンス サーバー上に共有秘密を設定します。共有秘密を保持する参加者であればいずれも共有ライセンスを使用できます。
2. ASA を参加者として設定する場合、ローカル ライセンスおよびモデル情報を含む自身の情報を送信することで共有ライセンス サーバーに登録します。

（注） 参加者は IP ネットワークを経由してサーバーと通信できる必要がありますが、同じサブネット上にある必要はありません。

1. 共有ライセンス サーバーは、参加者がサーバーにポーリングするべき頻度の情報で応答します。
2. 参加者がローカル ライセンスのセッションを使い果たした場合、参加者は共有ライセンス サーバーに 50 セッション単位で追加セッションの要求を送信します。
3. 共有ライセンス サーバーは、共有ライセンスで応答します。1 台の参加者が使用する合計セッション数は、プラットフォーム モデルの最大セッション数を超えられません。

（注） 共有ライセンスサーバーは、ローカル セッションを使い果たした場合に共有ライセンス プールに参加もできます。参加には参加ライセンスもサーバー ライセンスも必要ありません。

1. 参加者に対して共有ライセンス プールに十分なセッションがない場合、サーバーは使用可能な限りのセッション数で応答します。
2. 参加者はさらなるセッションを要求するリフレッシュ メッセージの送信をサーバーが要求に適切に対応できるまで続けます。
3. 参加者の負荷が減少した場合、参加者はサーバーに共有セッションを解放するようにメッセージを送信します。

（注） ASA は、サーバと参加者間のすべての通信の暗号化に SSL を使用します。

参加者とサーバー間の通信問題

参加者とサーバー間の通信問題については、次のガイドラインを参照してください。

- 参加者が更新の送信に失敗して更新間隔3倍の時間が経過した後で、サーバーはセッションを解放して共有ライセンス プールに戻します。
- 参加者が更新を送信するためにライセンス サーバーに到達できない場合、参加者はサーバーから受信した共有ライセンスを最大 24 時間使用し続けられます。
- 24時間を経過しても参加者がまだライセンス サーバーと通信できない場合、参加者はセッションがまだ必要であっても共有ライセンスを解放します。参加者は既存の確立している接続を維持しますが、ライセンス制限を超えて新しい接続を受け入れられません。
- 参加者が 24 時間経過前にサーバーに再接続したが、サーバーが参加セッションを期限切れにした後である場合、参加者はセッションに対する新しい要求を送信する必要があります。サーバーは、参加者に再割り当てできる限りのセッション数で応答します。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットをinsideインターフェイスおよびDMZインターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバー コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバーのIPアドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバーを指定します。
license-server backup backup-id	メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。

コマンド	説明
license-server port	サーバーが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバーに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバー コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server port

共有ライセンスサーバーが参加者からの SSL 接続をリッスンするポートを設定するには、グローバル コンフィギュレーション モードで **license-server port** コマンドを使用します。デフォルトポートに戻すには、このコマンドの **no** 形式を使用します。

license-server port *port*
no license-server port [*port*]

構文の説明

seconds 参加ユニットからの SSL 接続をサーバーがリッスンするポート（1 ～ 65535）を設定します。デフォルトは、TCP ポート 50554 です。

コマンド デフォルト

デフォルトのポートは 50554 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

デフォルトポートを変更する場合は、**license-server address** コマンドを使用して、各参加者に同じポートを設定してください。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび DMZ インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

```
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバー コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバーを指定します。
license-server backup backup-id	メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバーになるユニットをイネーブルにします。
license-server refresh-interval	サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
license-server secret	共有秘密を共有ライセンス サーバーに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバー コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server refresh-interval

参加者が共有ライセンスサーバーと通信する頻度を設定するために参加者に提供されるリフレッシュ間隔を設定するには、グローバル コンフィギュレーション モードで **license-server refresh-interval** コマンドを使用します。デフォルトのリフレッシュ間隔に戻すには、このコマンドの **no** 形式を使用します。

license-server refresh-interval *seconds*
no license-server refresh-interval [*seconds*]

構文の説明

seconds リフレッシュ間隔（10 ～ 300 秒）を設定します。デフォルトは 30 秒です。

コマンド デフォルト

デフォルトは 30 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

各参加ユニットは、SSL を使用して定期的に共有ライセンス サーバーと通信します。そのため、共有ライセンス サーバーは現在のライセンス使用状況を把握し、ライセンス要求を受信したりライセンス要求に応答できます。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
```

```
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバー コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバーを指定します。
license-server backup backup-id	メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバーになるユニットをイネーブルにします。
license-server port	サーバーが参加者からの SSL 接続をリッスンするポートを設定します。
license-server secret	共有秘密を共有ライセンス サーバーに設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバー コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license-server secret

共有ライセンスサーバーに共有秘密を設定するには、グローバル コンフィギュレーション モードで **license-server secret** コマンドを使用します。共有秘密を削除するには、このコマンドの **no** 形式を使用します。

license-server secret *secret*
no license-server secret *secret*

構文の説明

secret 共有秘密を 4 ～ 128 文字の ASCII 文字のストリングで設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

この共有秘密を持つ、**license-server address** コマンドで指定された参加者は、ライセンスサーバーを使用できます。

例

次に、共有秘密を設定し、更新間隔とポートを変更し、バックアップ サーバーを設定し、このユニットを inside インターフェイスおよび dmz インターフェイスで共有ライセンス サーバーとしてイネーブルにする例を示します。

```
ciscoasa(config)# license-server secret farscape
ciscoasa(config)# license-server refresh-interval 100
ciscoasa(config)# license-server port 40000
ciscoasa(config)# license-server backup 10.1.1.2 backup-id JMX0916L0Z4 ha-backup-id
JMX1378N0W3
ciscoasa(config)# license-server enable inside
ciscoasa(config)# license-server enable dmz
```

関連コマンド

コマンド	説明
activation-key	ライセンス アクティベーション キーを入力します。
clear configure license-server	共有ライセンス サーバー コンフィギュレーションをクリアします。
clear shared license	共有ライセンス統計情報をクリアします。
license-server address	共有ライセンス サーバーの IP アドレスと参加者の共有秘密を指定します。
license-server backup address	参加者の共有ライセンス バックアップ サーバーを指定します。
license-server backup backup-id	メインの共有ライセンス サーバーのバックアップ サーバーの IP アドレスおよびシリアル番号を指定します。
license-server backup enable	共有ライセンス バックアップ サーバーになるユニットをイネーブルにします。
license-server enable	共有ライセンス サーバーになるユニットをイネーブルにします。
license-server port	サーバーが参加者からの SSL 接続をリッスンするポートを設定します。
license-server refresh-interval	サーバーと通信する頻度を設定するために参加者に提供される更新間隔を設定します。
show activation-key	インストールされている現在のライセンスを表示します。
show running-config license-server	共有ライセンス サーバー コンフィギュレーションを表示します。
show shared license	共有ライセンス統計情報を表示します。
show vpn-sessiondb	VPN セッションのライセンス情報を表示します。

license smart

スマートライセンス資格要求を設定するには、グローバル コンフィギュレーション モードで **license smart** コマンドを使用します。資格を削除してデバイスのライセンスを解除するには、このコマンドの **no** 形式を使用します。

（注） この機能は、ASA 仮想 およびシャーシのみでサポートされています。

license smart
no license smart

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドは、ASA 仮想のサポートのために追加されました。
9.4(1.152)	Firepower 9300 のサポートが追加されました。
9.6(1)	Firepower 4100 シリーズのサポートが追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

このコマンドを使用すると、ライセンス スマート コンフィギュレーション モードになり、機能層やその他のライセンス資格を設定できます。ASA 仮想 の場合、初めて権限付与を要求したときは、変更を有効にするためにライセンス スマート コンフィギュレーション モードを終了する必要があります。

例

次に、機能階層を標準に設定し、スループット レベルを 2G に設定する例を示します。

```
ciscoasa# license smart
ciscoasa(config-smart-lic)# feature tier standard
ciscoasa(config-smart-lic)# throughput level 2G
ciscoasa(config-smart-lic)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

license smart deregister

Cisco License Authority に対するデバイスのスマートライセンス登録を解除するには、特権 EXEC モードで **license smart deregister** コマンドを使用します。

（注） この機能は、ASA 仮想 および Firepower 2100 だけでサポートされています。

license smart deregister

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドは、ASA 仮想 のサポートのために追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

ASA の登録を解除すると、アカウントから ASA が削除されます。ASA のすべてのライセンス権限付与と証明書が削除されます。登録を解除することで、ライセンスを新しい ASA に利用することもできます。このコマンドを実行すると、ASA がリロードします。

例

次に、デバイスの登録を解除する例を示します。

```
ciscoasa# license smart deregister
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。

コマンド	説明
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

license smart register

Cisco License Authority に対するデバイスのスマートライセンスを登録するには、特権 EXEC モードで **license smart register** コマンドを使用します。

（注） この機能は、ASA 仮想 および Firepower 2100 だけでサポートされています。

license smart register idtoken *id_token*［ **force** ］

構文の説明

idtoken *id_token*	Smart Software Manager で、この ASA を追加するバーチャル アカウントの登録トークンを要求してコピーします。
force	License Authority と同期されていない可能性がある登録済みの ASA を登録します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドは、ASA 仮想のサポートのために追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

License Authority に ASA を登録すると、ASA と License Authority の間の通信に使用する ID 証明書が発行されます。また、該当するバーチャル アカウントに ASA が割り当てられます。通常、この手順は1回で済みます。ただし、通信の問題などが原因でアイデンティティ証明書の期限が切れた場合は、ASA の再登録が必要になります。

例

次に、登録トークンを使用して登録を行う例を示します。

```
ciscoasa# license smart register idtoken
```

YjE3NjcyMzYtMGQzMi00OTA4LWJhODItNzBhMGQ2NGRlYjUxLTE0MTQ5NDAy%0ACDQzNzl8NXk2bzV3SDE0ZkgwQkdMRmZlNINCNG1vRnBHUEpjcm02WlB4TU4w%0Ac2NrMD0%3D%0A

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

license smart renew

スマートライセンスの登録またはソフトウェア利用資格の認証を更新するには、特権 EXEC モードで **license smart renew** コマンドを使用します。

（注） この機能は、ASA 仮想 および Firepower 2100 だけでサポートされています。

license smart renew { **id** | **auth** }

構文の説明

id	デバイスの登録を更新します。
auth	ライセンス資格を更新します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドは、ASA 仮想のサポートのために追加されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

デフォルトでは、アイデンティティ証明書は 6 ヵ月ごと、ライセンス資格は 30 日ごとに自動的に更新されます。インターネット アクセスの期間が限られている場合や、Smart Software Manager でライセンスを変更した場合などは、これらの登録を手動で更新することもできます。

例

次に、登録とライセンスの両方の認証を更新する例を示します。

```
ciscoasa# license smart renew id
ciscoasa# license smart renew auth
```

関連コマンド

コマンド	説明
call-home	Smart Call Home を設定します。スマート ライセンスでは、Smart Call Home インフラストラクチャが使用されます。
clear configure license	スマート ライセンス設定をクリアします。
feature tier	スマート ライセンスの機能層を設定します。
http-proxy	スマート ライセンスおよび Smart Call Home の HTTP(S) プロキシを設定します。
license smart	スマート ライセンスのライセンス権限付与を要求できます。
license smart deregister	ライセンス認証局からデバイスを登録解除します。
license smart register	デバイスをライセンス認証局に登録します。
license smart renew	登録またはライセンス権限を更新します。
service call-home	Smart Call Home をイネーブルにします。
show license	スマート ライセンスのステータスを表示します。
show running-config license	スマート ライセンスの設定を表示します。
throughput level	スマート ライセンスのスループット レベルを設定します。

license smart reservation

永続ライセンス予約を有効にするには、グローバル コンフィギュレーション モードで **license smart reservation** コマンドを使用します。永続ライセンス予約を無効にするには、このコマンドの **no** 形式を使用します。

license smart reservation
no license smart reservation

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

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。

コマンド デフォルト

この機能はデフォルトで無効に設定されています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASA 仮想 のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

インターネットアクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます（https://software.cisco.com/#SmartLicensing-Inventory）。パーマネント ライセンスでは、すべての機能を最大限に使用できます。

ASA 仮想 の場合、**license smart reservation** コマンドを入力すると、次のコマンドが削除されます。

```
license smart
feature tier standard
throughput level {100M | 1G | 2G}
```

通常のスマート ライセンスを使用するには、このコマンドの **no** 形式を使用し、上記のコマンドを再入力します。その他の Smart Call Home 設定はそのまま維持されますが、使用されないため、それらのコマンドを再入力する必要はありません。

シャーシの場合、コンテキストライセンスなどのデフォルト以外のライセンスに対しては、**license smart**/**feature** コマンドを入力する必要があります。これらのコマンドは、ASA に機能の設定を許可するよう指定するために必要です。

（注） 永続ライセンスの予約については、ASA を廃棄する前にライセンスを戻す必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、新しい ASA に再使用できません。**license smart reservation return** コマンドを参照してください。

例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。
license smart reservation install	承認コードを入力します。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

license smart reservation cancel

まだ Smart Software Manager でコードを入力していない場合に永続ライセンス予約の要求をキャンセルするには、特権 EXEC モードで **license smart reservation cancel** コマンドを使用します。

license smart reservation cancel

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASA 仮想 のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

license smart reservation request universal コマンドを使用して Smart Software Manager に入力するライセンスコードを要求した場合、そのコードをまだ Smart Software Manager に入力していなければ、**license smart reservation cancel** コマンドを使用して要求をキャンセルできます。

永続ライセンスの予約を無効にする（**no license smart reservation**）と、保留中のすべての要求がキャンセルされます。

すでに Smart Software Manager にコードを入力している場合は、ASA へのライセンスの適用を完了する必要があります。その時点から、**license smart reservation return** コマンドを使用してライセンスを返却できます。

例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求した後に、要求をキャンセルする例を示します。

```
ciscoasa(config)# license smart reservation
```

```
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
ciscoasa(config)# license smart reservation cancel
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネントライセンスの要求をキャンセルします。
license smart reservation install	承認コードを入力します。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

license smart reservation install

Smart Software Manager から受け取った永続ライセンスの予約の承認コードを入力するには、特権 EXEC モードで **license smart reservation install** コマンドを使用します。

license smart reservation install *code*

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

構文の説明

code	Smart Software Manager から受け取ったパーマネント ライセンスの予約の承認コード。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASA 仮想 のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

インターネットアクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます（https://software.cisco.com/#SmartLicensing-Inventory）。**license smart reservation request universal** コマンドを使用して Smart Software Manager に入力するコードを要求します。Smart Software Manager にコードを入力するときは、受け取った承認コードをコピーして、**license smart reservation install** コマンドを使用して ASA に入力します。

例

次に、パーマネント ライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
```

```
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネントライセンスの要求をキャンセルします。
license smart reservation install	承認コードを入力します。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

license smart reservation universal

Smart Software Manager に入力するライセンスコードを要求するには、特権 EXEC モードで **license smart reservation universal** コマンドを使用します。

license smart reservation universal

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASA 仮想 のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。**license smart reservation request universal** コマンドを使用して Smart Software Manager に入力するコードを要求します。

ASA 仮想 の導入により、要求するライセンス（ASAv5/ASAv10/ASAv30）が決まります。

このコマンドを再入力すると、リロード後にも同じコードが表示されます。このコードをまだ Smart Software Manager に入力していない場合、要求をキャンセルするには、**license smart reservation cancel** コマンドを入力します。

パーマネントライセンスの予約をディセーブルにすると、保留中のすべての要求がキャンセルされます。すでに Smart Software Manager にコードを入力している場合は、その手順を完了して ASA にライセンスを適用する必要があります。その時点から、必要に応じてライセンスを戻すことが可能になります。**license smart reservation return** コマンドを参照してください。

承認コードを要求するには、Smart Software Manager のインベントリ画面（https://software.cisco.com/#SmartLicensing-Inventory）に移動して、[**Licenses**] タブをクリックします。**Licenses** タブにアカウントに関連するすべての既存のライセンスが、標準およびパーマネントの両方とも表示されます。[**License Reservation**] をクリックして、ASA のコードをボックスに入力します。**Reserve License** をクリックします。Smart Software Manager が承認コードを生成します。コードをダウンロードまたはクリップボードにコピーできます。この時点で、ライセンスは、Smart Software Manager に従って使用中です。

[**License Reservation**] ボタンが表示されない場合、お使いのアカウントには永続ライセンスの予約が許可されていません。この場合、パーマネントライセンスの予約を無効にして標準のスマート ライセンス コマンドを再入力する必要があります。

license smart reservation install コマンドを使用して ASA に承認コードを入力します。

例

次に、パーマネントライセンスの予約をイネーブルにして、Smart Software Manager に入力するライセンス コードを要求し、Smart Software Manager から受け取った承認コードをインストールする例を示します。

```
ciscoasa(config)# license smart reservation
ciscoasa(config)# license smart reservation request universal
Enter this request code in the Cisco Smart Software Manager portal:
ABP:ASAv,S:9AU5ET6UQHD{A8ug5/1jRDaSp3w8uGlfeQ{53C13E
...
ciscoasa(config)# license smart reservation install AAu3431rGRS00Ig5HQl2vpzg{MEYCIQCBw$
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネントライセンスの要求をキャンセルします。
license smart reservation install	承認コードを入力します。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

license smart reservation return

Smart Software Manager にライセンスを戻すためのリターンコードを生成するには、特権 EXEC モードで **license smart reservation return** コマンドを使用します。

license smart reservation return

（注） この機能は、ASA 仮想 と Firepower 2100 にのみ適用されます。

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2.200)	このコマンドは、ASA 仮想 のサポート用に導入されました。
9.8(2)	Firepower 2100 シリーズのサポートが追加されました。

使用上のガイドライン

インターネット アクセスを持たない ASA の場合は、Smart Software Manager から永続ライセンスを要求できます。永続ライセンスが不要になった場合（ASA を廃棄する場合や ASA 仮想 のモデルレベルの変更によって新しいライセンスが必要になった場合など）、ライセンスを正式に Smart Software Manager に返却する必要があります。ライセンスを正式に戻さないと、ライセンスが使用中の状態のままになり、他の場所で使用するために容易に解除できません。

license smart reservation return コマンドを入力すると、ASA がただちにライセンス未適用状態になり、評価状態に移行します。このコードを再度表示する必要がある場合は、このコマンドを再入力します。新しい永続ライセンスを要求する（**license smart reservation request universal**）か、ASA 仮想 のモデルレベルを変更する（電源を切って vCPU/RAM を変更する）と、このコードは再表示できないことに注意してください。必ず、コードをキャプチャして、戻す作業を完了してください。

Smart Software Manager にコードを入力する前に、**show license udi** コマンドを使用して ASA のユニバーサル デバイス識別子（UDI）を表示すると、この ASA インスタンスを Smart Software

Manager で確認できます。Smart Software Manager インベントリ画面（https://software.cisco.com/#SmartLicensing-Inventory）に移動して、[**Product Instances**] タブをクリックします。[**Product Instances**] タブに、ライセンスが付与されているすべての製品が UDI で表示されます。ライセンスを解除する ASA 仮想 を確認し、[**Actions > Remove**] を選択して、ASA のリターンコードをボックスに入力します。**Remove Product Instance** をクリックします。パーマネント ライセンスが使用可能なライセンスのプールに戻されます。

例

次に、ASA 仮想 でリターンコードを生成し、ASA 仮想 UDI を表示する例を示します。

```
ciscoasa# license smart reservation return
Enter this return code in the Cisco Smart Software Manager portal:
Au3431rGRS00Ig5HQl2vpcg{uXiTRfVrp7M/zDpirLwYCaq8oSv60yZJuFDVBS2QliQ=
ciscoasa# show license udi
UDI: PID:ASAv,SN:9AHV3KJBEKE
```

関連コマンド

コマンド	説明
license smart reservation	パーマネント ライセンスの予約をイネーブルにします。
license smart reservation cancel	Smart Software Manager でコードを入力していない場合に、パーマネント ライセンスの要求をキャンセルします。
license smart reservation install	承認コードを入力します。
license smart reservation request universal	Smart Software Manager に入力するライセンス コードを要求します。
license smart reservation return	Smart Software Manager にライセンスを戻します。

lifetime（CA サーバー モード）

ローカル認証局（CA）証明書、各発行済み証明書、または証明書失効リスト（CRL）の有効期間を指定するには、CA サーバー コンフィギュレーション モードで **lifetime** コマンドを使用します。パラメータをデフォルト設定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。

lifetime { **ca-certificate** | **certificate** | **crl** } *time*
lifetime { **ca-certificate** | **certificate** | **crl** }

構文の説明

ca-certificate	ローカル CA サーバー証明書のライフタイムを指定します。
certificate	CA サーバーが発行するすべてのユーザー証明書のライフタイムを指定します。
crl	CRL のライフタイムを指定します。
time	CA 証明書およびすべての発行済み証明書の場合、*time* はその証明書の有効日数を指定します。有効範囲は 5 ～ 30 年です。デフォルトのライフタイム値は 15 年です。 発行されたすべてのユーザー証明書の有効範囲は 1 日 ～ 4 年です。デフォルトのライフタイム値は 2 年です。 CRL の場合、*time* は CRL の有効時間数を指定します。CRL の有効な範囲は、1 ～ 720 時間です。

コマンド デフォルト

デフォルトのライフタイムは次のとおりです。

- CA 証明書：15 年
- 発行済み証明書：2 年
- CRL：6 時間

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.12(1)	lifetime ca-certificate で使用可能な値は、5 ～ 30 年に変更されており、デフォルトは 15 年です。 lifetime certificate で使用可能な値は、1 日 ～ 4 年に変更されており、デフォルトは 2 年です。

使用上のガイドライン

証明書または CRL が有効である日数または時間数を指定すると、このコマンドは、証明書または CRL に含める有効期限を決定します。

lifetime ca-certificate コマンドは、ローカル CA サーバー証明書の初回生成時（初めてローカル CA サーバーを設定し、**no shutdown** コマンドを発行するとき）に有効になります。CA 証明書の期限が切れると、設定されたライフタイム値を使用して新しい CA 証明書が生成されます。既存の CA 証明書のライフタイム値は変更できません。

例

次に、3 か月間有効な証明書を発行するように CA を設定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime certificate 90
ciscoasa
(config-ca-server)
)#
```

次に、2 日間有効な CRL を発行するように CA を設定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# lifetime crl 48
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
cdp-url	CA が発行する証明書に含める証明書失効リストの配布ポイント（CDP）を指定します。
crypto ca server	CA サーバー コンフィギュレーション モードのコマンド 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 セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。

コマンド	説明
show crypto ca server	ローカル CA コンフィギュレーションの詳細を ASCII テキストで表示します。
show crypto ca server cert-db	ローカル CA サーバー証明書を表示します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

lifetime（IKEv2 ポリシー モード）

AnyConnect IPsec 接続に使用する IKEv2 セキュリティ アソシエーション（SA）の暗号化アルゴリズムを指定するには、IKEv2 ポリシー コンフィギュレーション モードで encryption コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

lifetime { { **seconds** *seconds* } | **none** }

構文の説明

seconds	ライフタイムの秒数（120 ～ 2,147,483,647 秒）。デフォルトは 86,400 秒（24 時間）です。

コマンド デフォルト

デフォルトは 86,400 秒（24 時間）です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。crypto ikev2 policy コマンドを入力した後、**lifetime** コマンドを使用して SA ライフタイムを設定します。

このコマンドでは、IKEv2 SA のキーを再生成する間隔を設定します。none キーワードを使用すると、SA のキー再生成がディセーブルになります。ただし、引き続き セキュアクライアント で SA のキー再生成を実行できます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

例

次に、IKEv2 ポリシー コンフィギュレーション モードを開始し、ライフタイムを 43,200 秒（12 時間）に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# lifetime 43200
```

関連コマンド

コマンド	説明
encryption	AnyConnect IPsec 接続に対して IKEv2 SA の暗号化アルゴリズムを指定します。
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
integrity	AnyConnect IPsec 接続に対して IKEv2 SA の ESP 整合性アルゴリズムを指定します。
prf	AnyConnect IPsec 接続に対して IKEv2 SA の疑似乱数関数を指定します。

limit-resource

マルチコンテキストモードでクラスのリソース制限を指定するには、クラス コンフィギュレーション モードで **limit-resource** コマンドを使用します。制限をデフォルトに戻すには、このコマンドの **no** 形式を使用します。ASA は、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

limit-resource [**rate**] { **all** | *resource_name* } *number* [**%**] }
no limit-resource [**rate**] { **all** | *resource_name* }

構文の説明

all	すべてのリソースの制限を設定します。
number [**%**]	リソース制限を 1 以上の固定数、またはパーセント記号（%）付きのシステム制限のパーセンテージ（1 ～ 100）として指定します。リソースに制限がないことを示すには、制限を **0** に設定します。VPN リソース タイプの場合は、制限をなしに設定します。システム制限がないリソースの場合は、パーセンテージ（%）を設定できません。絶対値のみを設定できます。
rate	リソースの 1 秒あたりのレートを設定することを指定します。1 秒あたりのレートを設定できるリソースについては、表 3 : リソース名および制限 を参照してください。
resource_name	制限を設定するリソース名を指定します。この制限で、**all** に設定されている制限が上書きされます。

コマンド デフォルト

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルトクラスに属します。コンテキストをデフォルトクラスに積極的に割り当てる必要はありません。

ほとんどのリソースについては、デフォルトクラスではすべてのコンテキストがリソースに無制限でアクセスできます。ただし、次の制限を除きます。

- Telnet セッション：5 セッション。（コンテキストあたりの最大値）。
- SSH セッション：5 セッション。（コンテキストあたりの最大値）。
- ASDM セッション：5 セッション。（コンテキストあたりの最大値）。
- IPsec セッション：5 セッション。（コンテキストあたりの最大値）。
- MAC アドレス：65,535 エントリ。（コンテキストあたりの最大値）。
- AnyConnect ピア：0 セッション（AnyConnect ピアを許可するようにクラスを手動で設定する必要があります）。
- VPN サイトツーサイトトンネル：0 セッション（VPN セッションを許可するようにクラスを手動で設定する必要があります）。
- HTTPS セッション：6 セッション。（コンテキストあたりの最大値）。

（注） また、コンテキスト内で **quota management-session** コマンドを設定して最大管理セッション（SSH など）を設定した場合は、小さい方の値が使用されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.0(1)	各コンテキストでのルーティング テーブル エントリの最大数を設定するために、新規リソース タイプ **routes** が作成されました。 各コンテキストでのサイトツーサイト VPN トンネルの最大数を設定するために、新しいリソースタイプ **vpn other** と **vpn burst other** が作成されました。
9.5(2)	各コンテキストでの AnyConnect VPN ピアの最大数を設定するために、新しいリソースタイプ **vpn anyconnect** と **vpn burst anyconnect** が作成されました。
9.6(2)	最大ストレージを設定するために、新しいリソースタイプ **storage** が作成されました。
9.12(1)	HTTPS 接続を制御するために、新しいリソースタイプ **http** が追加されました。

使用上のガイドライン

デフォルトでは、すべてのセキュリティ コンテキストは ASA のリソースに無制限でアクセスできますが、コンテキストあたりの上限が定められている場合を除きます。唯一の例外は、VPN のリソース（デフォルトでディセーブルになっています）です。特定のコンテキストが使用しているリソースが多すぎることが原因で、他のコンテキストが接続を拒否されるといった現象が発生した場合は、コンテキストあたりのリソースの使用量を制限するようにリソース管理を設定できます。VPN のリソースについては、VPN トンネルを許可するようにリソース管理を設定する必要があります。

表 3 : リソース名および制限 に、リソースタイプと制限を示します。 **show resource types** コマンドも参照してください。

表 *3:* リソース名および制限

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限[1]	説明
asdm	同時接続数	最小 1 最大 5	200	ASDM 管理セッション。 （注） ASDM セッションでは、2 つの HTTPS 接続が使用されます。一方は常に存在するモニター用で、もう一方は変更を行ったときにだけ存在する設定変更用です。たとえば、ASDM セッションのシステム制限が 200 の場合、HTTPS セッション数は 400 に制限されます。
conns	同時またはレート	該当なし	同時接続数：プラットフォームの接続制限については、CLI 設定ガイドを参照してください。 レート：該当なし	任意の 2 つのホスト間の TCP または UDP 接続（1 つのホストと他の複数のホストとの間の接続を含む）。
hosts	同時接続数	該当なし	該当なし	ASA 経由で接続可能なホスト。
http	同時接続数	最小 1 最大 6	100	非 ASDM HTTPS セッション
inspects	利率	該当なし	該当なし	アプリケーション インスペクション。
mac-addresses	同時接続数	該当なし	65,535	トランスペアレント ファイアウォール モードでは、MAC アドレス テーブルで許可される MAC アドレス数。
routes	同時接続数	該当なし	該当なし	ダイナミック ルート。
ssh	同時接続数	最小 1 最大 5	100	SSH セッション。
storage	MB	最大値は、指定するフラッシュ メモリのドライブによって異なります。	最大値は、指定するフラッシュ メモリのドライブによって異なります。	コンテキストでのディレクトリのストレージ制限（MB 単位）。ドライブを指定するには、**storage-url** コマンドを使用します。
syslogs	利率	該当なし	該当なし	システム ログ メッセージ。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限[1]	説明
telnet	同時接続数	最小 1 最大 5	100	Telnet セッション。
vpn burst anyconnect	同時接続数	該当なし	モデルに応じた AnyConnect Premium ピア数から、vpn anyconnect 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn anyconnect** でコンテキストに割り当てられた数を超えて許可される AnyConnect セッションの数。たとえば、使用するモデルで 5000 のピアがサポートされており、**vpn anyconnect** で割り当てたピア数の合計が全コンテキストで 4000 の場合は、残りの 1000 セッションが **vpn burst anyconnect** に使用可能です。**vpn anyconnect** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst anyconnect** ではオーバーサブスクライブが可能で、すべてのコンテキストがバーストプールを先着順に使用できます。
vpn anyconnect	同時接続数	該当なし	モデルごとの使用可能な AnyConnect VPN ピア数については、CLI 設定ガイドの「モデルごとにサポートされている機能のライセンス」を参照してください。	AnyConnect ピア。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたピアは、そのコンテキストに対して保証されます。
vpn burst other	同時接続数	該当なし	モデルに応じた Other VPN セッション数から、**vpn other** 用にすべてのコンテキストに割り当てられたセッション数の合計を差し引いた値。	**vpn other** でコンテキストに割り当てられた数を超えて許可されるサイトツーサイト VPN セッションの数。たとえば、使用するモデルで 5000 のセッションがサポートされており、**vpn other** で割り当てたセッションの合計が全コンテキストで 4000 の場合、残りの 1000 セッションを **vpn burst other** に使用できます。**vpn other** ではセッション数がコンテキストに対して保証されますが、対照的に **vpn burst other** ではオーバーサブスクライブが可能で、すべてのコンテキストがバーストプールを先着順に使用できます。
vpn other	同時接続数	該当なし	モデルごとの使用可能な Other VPN セッション数については、CLI 設定ガイドの「モデルごとにサポートされている機能のライセンス」を参照してください。	サイトツーサイト VPN セッション。このリソースはオーバーサブスクライブできません。すべてのコンテキストへの割り当て合計がモデルの制限を超えてはなりません。このリソースに割り当てたセッションは、そのコンテキストに対して保証されます。

リソース名	レートまたは同時	コンテキストあたりの最小数と最大数	システム制限[1]	説明
xlates	同時接続数	該当なし	該当なし	アドレス変換。

[1] この列に「該当なし」と記述されている場合、そのリソースにはハードシステム制限がないため、リソースのパーセンテージを設定できません。

例

次に、接続のデフォルト クラスの制限に、無制限ではなく 10 % を設定する例を示します。

```
ciscoasa(config)# class default
ciscoasa(config-class)# limit-resource conns 10%
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
ciscoasa(config)# class gold
ciscoasa(config-class)#
limit-resource mac-addresses 10000
ciscoasa(config-class)#
limit-resource conns 15%
ciscoasa(config-class)#
limit-resource rate conns 1000
ciscoasa(config-class)#
limit-resource rate inspects 500
ciscoasa(config-class)#
limit-resource hosts 9000
ciscoasa(config-class)#
limit-resource asdm 5
ciscoasa(config-class)#
limit-resource ssh 5
ciscoasa(config-class)#
limit-resource rate syslogs 5000
ciscoasa(config-class)#
limit-resource telnet 5
ciscoasa(config-class)#
limit-resource xlates 36000
ciscoasa(config-class)#
limit-resource routes 700
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
member	コンテキストをリソース クラスに割り当てます。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。

コマンド	説明
show resource types	制限を設定できるリソース タイプを表示します。

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ングに関する再検証ポリシーを設定するには、キャッシュ コンフィギュレーション モードで **lmfactor** コマンドを使用します。このようなオブジェクトを再検証するための新しいポリシーを設定するには、このコマンドを再度使用します。属性をデフォルト値の 20 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。

lmfactor*value*
nolmfactor

構文の説明

value	0 ～ 100 の範囲の整数。

コマンド デフォルト

デフォルト値は 20 です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は lmfactor の値を使用して、キャッシュされたオブジェクトを変更なしと見なす時間の長さを推定します。これは有効期限と呼ばれます。ASA は最終変更後の経過時間に lmfactor をかけることによって有効期限を推定します。

lmfactor を 0 に設定すると、ただちに再検証が強制されます。100 に設定すると、再検証までの時間は可能な限り長くなります。

例

次に、lmfactor を 30 に設定する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
```

```
 cache
ciscoasa(config-webvpn-cache)# lmfactor 30
ciscoasa(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。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
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。

load-monitor

クラスタ トラフィック ロード モニタリングを設定するには、クラスタ コンフィギュレーション モードで **load-monitor** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

load-monitor [**frequency** *seconds*] [**intervals** *intervals*]
no load-monitor [**frequency** *seconds*] [**intervals** *intervals*]

構文の説明

frequency *seconds*	（オプション）モニタリング メッセージの間隔を 10 ～ 360 秒の範囲で設定します。デフォルトは 20 秒です。
intervals *intervals*	（オプション）ASA がデータを保持する間隔の数を 1 ～ 60 の範囲で設定します。デフォルトは 30 です。

コマンド 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。デフォルトの頻度は、20秒です。デフォルトの間隔は、30 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスタ構成	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

クラスタメンバのトラフィック負荷をモニターできます。対象には、合計接続数、CPU とメモリの使用率、バッファドロップなどが含まれます。負荷が高すぎる場合、残りのユニットが負荷を処理できる場合は、ユニットのクラスタリングを手動で無効にするか、外部スイッチのロードバランシングを調整するかを選択できます。この機能は、デフォルトでイネーブルにされています。たとえば、各シャーシに 3 つのセキュリティモジュールが搭載された Firepower 9300 のシャーシ間クラスタリングの場合、シャーシ内の 2 つのセキュリティモジュールがクラスタを離れると、そのシャーシに対する同じ量のトラフィックが残りのモジュールに送信され、過負荷になる可能性があります。トラフィックの負荷を定期的にモニターできます。負荷が高すぎる場合は、ユニットでクラスタリングを手動で無効にすることを選択できます。

トラフィック負荷を表示するには、**show cluster info load-monitor** コマンドを使用します。

例

次に、周波数を 50 秒に、間隔を 25 に設定する例を示します。

```
ciscoasa(cfg-cluster)# load-monitor frequency 50 intervals 25
```

関連コマンド

コマンド	説明
cluster	クラスタ コンフィギュレーション モードを開始します

local-domain-bypass

DNS 要求が Cisco Umbrella をバイパスする必要があるローカルドメインを設定するには、Cisco Umbrella コンフィギュレーションモードで **local-domain-bypass** 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。

local-domain-bypass { *regular_expression* | **regex class** *regex_classmap* }
no local-domain-bypass { *regular_expression* | **regex class** *regex_classmap* }

構文の説明

regular_expression	バイパスするローカル ドメインを識別する正規表現。この正規表現は、ローカル ドメインのように単純にすることができます（たとえば、example.com）。最大 100 文字の正規表現を入力できます。 このオプションを使用する場合、**local-domain-bypass** コマンドを複数回入力して、複数のローカルドメインを定義できます。
regex class *regex_classmap*	バイパスするローカル ドメイン名を定義する正規表現クラスの名前。クラス内の正規表現に一致する完全修飾ドメイン名に対するすべての DNS 要求は、Umbrella サーバーではなく、設定された DNS サーバーに直接送信されます。

コマンド デフォルト

デフォルトでは、すべてのドメインに対する DNS 要求が Cisco Umbrella に送信されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Umbrella の設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.12(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する場合のガイドラインを次に示します。

- このコマンドを複数回入力して、ドメイン名の正規表現を直接定義することができます。
- 正規表現クラスを使用するときは、このコマンドを 1 回だけ入力できます。ただし、正規表現を直接使用する場合は、コマンドの単一の正規表現クラスバージョンと複数のインスタンスを組み合わせることができます。

例

次の例では、バイパスするローカルドメインとして example.com を定義しています。

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass example.com
```

次の例では、example.com と一致する正規表現を作成しています。これは、*example.com 上の完全修飾ドメイン名と一致します。次に、この例では、必要な正規表現クラスマップを作成して、Umbrella のローカル ドメイン バイパスとして使用しています。

```
ciscoasa(config)# regex example-com example.com

ciscoasa(config)# class-map type regex match-any umbrella-bypass

ciscoasa(config-cmap)# match regex example-com

ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# local-domain-bypass regex class umbrella-bypass
```

関連コマンド

コマンド	説明
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

local-unit

このクラスタメンバーの名前を指定するには、クラスタ グループ コンフィギュレーション モードで **local-unit** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。

local-unit *unit_name*
no local-unit [*unit_name*]

構文の説明

unit_name このクラスタ メンバの固有の名前を、1 ～ 38 文字の ASCII 文字列で指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

各ユニットに固有の名前が必要です。クラスタ内の他のユニットと同じ名前を付けることはできません。

例

次に、このユニットに unit1 という名前を付ける例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# local-unit unit1
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。

コマンド	説明
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
enable (cluster group)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルス チェック機能（ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority (cluster group)	マスター ユニット選定のこのユニットのプライオリティを設定します。

location-logging

GTPインスペクションで、モバイルステーションの場所と場所の変更をログに記録するには、GTP インスペクションのポリシー マップ パラメータ コンフィギュレーション モードで **location-logging** コマンドを使用します。場所のロギングを無効にするには、このコマンドの **no** 形式を使用します。

location-logging [**cell-id**]
no location-logging [**cell-id**]

構文の説明

cell-id ユーザーが現在登録されているセル ID を含めるかどうかを指定します。セル ID は、セル グローバル識別（CGI）または E-UTRAN セル グローバル識別子（ECGI）から抽出されます。

コマンド デフォルト

デフォルトでは、場所のロギングは無効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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 モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(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

GTPインスペクションを使用すると、モバイル端末の場所の変更を追跡できます。場所の変更を追跡すると、不正なローミング請求を特定するのに役立つ場合があります。たとえば、モバイル端末が、米国のセルから欧州のセルに 30 分以内に移動するなど、ある場所から別の場所にありえない時間で移動した場合などです。

場所のロギングを有効にすると、システムは International Mobile Subscriber Identity（IMSI）ごとに新しい場所または変更された場所の syslog メッセージを生成します。

- 324010 は新しい PDP コンテキストの作成を示し、携帯電話の国コード（MCC）、モバイル ネットワーク コード（MNC）、情報要素、および必要に応じてユーザーが現在登録さ

れているセルIDが含まれます。セルIDは、セル グローバル識別（CGI）またはE-UTRAN セル グローバル識別子（ECGI）から抽出されます。

- 324011 は、IMSI が PDP コンテキストの作成中に保存されたものから移動したことを示します。メッセージには、以前および現在の MCC/MNC および必要に応じてセル ID が表示されます。

デフォルトでは、syslog メッセージにタイムスタンプ情報は含まれません。これらのメッセージを分析してありえないローミングを識別する場合は、タイムスタンプも有効にする必要があります。タイムスタンプ ロギングは GTP インスペクション マップに含まれません。**logging timestamp** コマンドを使用します。

例

次の例では、タイムスタンプを syslog メッセージに追加してから、セルIDを使用して場所のロギングを有効にしています。

```
ciscoasa(config)# logging timestamp
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# location-logging cell-id
```

関連コマンド

コマンド	説明
inspect gtp	GTP アプリケーション インスペクションをイネーブルにします。
policy-map type inspect gtp	GTP インスペクション ポリシー マップを作成または編集します。
show service-policy inspect gtp	GTP 設定および統計情報を表示します。

log – lz

log

モジュラ ポリシー フレームワークを使用する場合は、一致またはクラスコンフィギュレーション モードで **log** コマンドを使用して、**match** コマンドまたはクラスマップと一致するパケットをログに記録します。このログアクションは、アプリケーション トラフィックのインスペクション ポリシー マップ（**policy-map type inspect** コマンド）で利用できます。このアクション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。

log
nolog

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照します）、**log** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するすべてのパケットをログに記録できます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、パケットが http-traffic クラス マップに一致する場合にログを送信する例を示します。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# log
```

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。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

log-adjacency-changes

NLSP IS-IS 隣接がステートを変更（アップまたはダウン）する際に IS-IS が syslog メッセージを送信することを可能にするには、ルータ ISIS コンフィギュレーション モードで **log-adjacency-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。

log-adjacency-changes ［ **all** ］
no log-adjacency-changes ［ **all** ］

構文の説明

all	（オプション）non_IIH イベントによって生成される変更を含みます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、IS-IS 隣接のステート変更のモニタリングが可能になります。これは、大規模なネットワークをモニタリングする場合に非常に役立つことがあります。メッセージは、システム エラー メッセージ機能を使用してロギングされます。メッセージは次の形式になります。

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

例

次に、隣接の変更をログに記録するように ルータ に指示する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# log-adjacency-changes
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。

コマンド	説明
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。

コマンド	説明
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

log-adj-changes

OSPF ネイバーが起動または停止したときに syslog メッセージを送信するようにルータを設定するには、ルータ コンフィギュレーション モードで **log-adj-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。

log-adj-changes [**detail**]
no log-adj-changes [**detail**]

構文の説明

detail （任意）ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

log-adj-changes コマンドはデフォルトで有効になっているため、コマンドの **no** 形式を指定して削除しない限り、実行コンフィギュレーションに表示されます。

例

次に、OSPF ネイバーが起動または停止したときに syslog メッセージを送信しないようにする例を示します。

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)# no log-adj-changes
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPF ルーティング プロセスに関する一般情報を表示します。

log-adjacency-changes

OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信するようにルータを設定するには、IPv6 ルータ コンフィギュレーション モードで **log-adjacency-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。

log-adjacency-changes [**detail**]
no log-adjacency-changes [**detail**]

構文の説明

detail （任意）ネイバーが起動または停止した場合だけでなく、状態が変わるたびに syslog メッセージを送信します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

log-adjacency-changes コマンドはデフォルトで有効になっているため、コマンドの **no** 形式を指定して削除しない限り、実行コンフィギュレーションに表示されます。

例

次に、OSPFv3 ネイバーが起動または停止したときに syslog メッセージを送信しないようにする例を示します。

```
ciscoasa(config)# ipv6
 router ospf 5
ciscoasa(config-router)# no log-adjacency-changes
```

関連コマンド

コマンド	説明
ipv6 router ospf	ルータ コンフィギュレーション モードを開始します。

コマンド	説明
show ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。

logging asdm

syslog メッセージを ASDM ログバッファに送信するには、グローバル コンフィギュレーション モードで **logging asdm** コマンドを使用します。ASDM ログバッファへのロギングを無効にするには、このコマンドの **no** 形式を使用します。

logging asdm [*logging_list* | *level*]
no logging asdm [*logging_list* | *level*]

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list ASDM ログバッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

コマンド デフォルト

ASDM ロギングはデフォルトで無効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASDM ログバッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングを有効にしておく必要があります。

ASDM ログバッファがいっぱいになると、ASA は最も古いメッセージを削除して、新しいメッセージ用の領域をバッファに確保します。ASDM ログバッファに保持される syslog メッセージの数を制御するには、**logging asdm-buffer-size** コマンドを使用します。

ASDM ログバッファは、**logging buffered** コマンドで有効にするログバッファとは異なります。

例

次に、ロギングを有効にして、ASDM に重大度 0、1、および 2 のログバッファメッセージを送信し、ASDM ログバッファのサイズを 200 メッセージに設定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログバッファから、保持されているすべてのメッセージをクリアします。

コマンド	説明
logging asdm-buffer-size	ASDM ログバッファに保持される ASDM メッセージの数を指定します。
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	ロギング設定を表示します。

logging asdm-buffer-size

ASDM ログバッファに保持される syslog メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging asdm-buffer-size** コマンドを使用します。ASDM ログバッファをデフォルトのサイズの 100 メッセージ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。

loggingasdm-buffer-size*num_of_msgs*
no logging asdm-buffer-size *num_of_msgs*

構文の説明

num_of_msgs	ASA によって ASDM ログバッファに保持される syslog メッセージの数を指定します。

コマンド デフォルト

デフォルトの ASDM syslog のバッファサイズは 100 メッセージです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASDM ログバッファがいっぱいになると、ASA は最も古いメッセージを削除して、新しいメッセージ用の領域をバッファに確保します。ASDM ログバッファへのロギングを有効にするかどうかを制御する、または ASDM ログバッファに保持される syslog メッセージの種類を制御するには、**logging asdm** コマンドを使用します。

ASDM ログバッファは、**logging buffered** コマンドで有効にするログバッファとは異なります。

例

次に、ロギングを有効にして、ASDM ログバッファに重大度 0、1、および 2 のメッセージを送信し、ASDM ログバッファのサイズを 200 メッセージに設定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging asdm 2
```

```
ciscoasa(config)# logging asdm-buffer-size 200
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: level critical, 48 messages logged
```

関連コマンド

コマンド	説明
clear logging asdm	ASDM ログバッファから、保持されているすべてのメッセージをクリアします。
logging asdm	ASDM ログバッファへのロギングを有効にします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	現在実行中のロギング コンフィギュレーションを表示します。

logging buffered

ASA から syslog メッセージをログバッファに送信できるようにするには、グローバル コンフィギュレーション モードで **logging buffered** コマンドを使用します。ログバッファへのロギングを無効にするには、このコマンドの **no** 形式を使用します。

logging buffered [*logging_list* | *level*]
no logging buffered [*logging_list* | *level*]

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list ログ バッファに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- バッファ サイズは 4 KB です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ログバッファにメッセージが送信される前に、**logging enable** コマンドを使用してロギングを有効にしておく必要があります。

新しいメッセージは、バッファの最後に追加されます。バッファがいっぱいになると、ASA によってバッファがクリアされてから、メッセージの追加が続行されます。ログバッファがいっぱいになると、ASA によって最も古いメッセージが削除されて、バッファに新しいメッセージ用の領域が確保されます。バッファの内容が「ラップ」されるたびにバッファの内容を自動的に保存することができます。これは、最後に保存されてから追加されたすべてのメッセージが新しいメッセージに置き換えられることを意味します。詳細については、**logging flash-bufferwrap** および **logging ftp-bufferwrap** コマンドを参照してください。

バッファの内容は、いつでもフラッシュ メモリに保存できます。詳細については、**logging savelog** コマンドを参照してください。

バッファに送信された syslog メッセージは、**show logging** コマンドで表示できます。

例

次に、重大度レベルが 0 および 1 のイベントに対して、バッファへのロギングを設定する例を示します。

```
ciscoasa(config)# logging buffered alerts
ciscoasa(config)#
```

次の例では、最大重大度 7 の「notif-list」というリストを作成し、「notif-list」リストで識別される syslog メッセージに対して、バッファへのロギングを設定します。

```
ciscoasa(config)# logging list notif-list level 7
ciscoasa(config)# logging buffered notif-list
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持している syslog メッセージをすべて消去します。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。

logging buffer-size

ログバッファのサイズを指定するには、グローバル コンフィギュレーション モードで **logging buffer-size** コマンドを使用します。ログバッファをメモリのデフォルトサイズの 4 KB 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。

loggingbuffer-size*bytes*
no logging buffer-size *bytes*

構文の説明

bytes ログバッファに使用するメモリ量をバイト単位で設定します。たとえば、8192 を指定した場合、ASA によってログバッファに 8 KB のメモリが使用されます。

コマンド デフォルト

デフォルトのログ バッファ サイズは 4 KB のメモリです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトのバッファサイズと異なるサイズのログバッファが ASA によって使用されているか確認するには、**show running-config logging** コマンドを使用します。**logging buffer-size** コマンドが表示されない場合、ASA によって 4 KB のログバッファが使用されています。

ASA によるバッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次に、ロギングを有効にし、ロギングバッファを有効にし、ログバッファ用に 16 KB のメモリが ASA で使用されることを指定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging buffer-size 16384
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持している syslog メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログ バッファがいっぱいになっている場合に、ログ バッファをフラッシュ メモリに書き込みます。
logging savelog	ログ バッファの内容をフラッシュ メモリに保存します。

logging class

メッセージクラスに対して、ロギング先ごとの最大重大度を設定するには、グローバル コンフィギュレーション モードで **logging class** コマンドを使用します。メッセージクラスの重大度レベル構成を削除するには、このコマンドの **no** 形式を使用します。

logging class *class destination level* [*destination level* . . .]
nologgingclass*class*

構文の説明

class	ロギング先ごとに最大重大度レベルを設定するメッセージ クラスを指定します。*class* の有効な値については、「使用上のガイドライン」を参照してください。
destination	*class* に対してロギング先を指定します。ロギング先について、*destination* に送信される最大重大度レベルは *level* によって決まります。*destination* の有効な値については、後述する「使用上のガイドライン」を参照してください。
level	syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システムが使用不能。 • **1** または **alerts**：すぐに対処が必要。 • **2** または **critical**：重大な状態。 • **3** または **errors**：エラー状態。 • **4** または **warnings**：警告状態。 • **5** または **notifications**：通常の状態だが、重要な状態。 • **6** または **informational**：Informational（情報提供）メッセージ。 • **7** または **debugging**：Debug（デバッグ）メッセージ。 （注） デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

コマンド デフォルト

ASA のデフォルトでは、重大度レベルはロギング先およびメッセージクラスに基づいて適用されません。代わりに、イネーブルにされた各ロギング先では、logging list で決定された重大度

レベル、または各ロギング先をイネーブルにしたときに指定された重大度レベルで、すべてのクラスに対するメッセージが受信されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	有効な class の値に **eigrp** オプションが追加されました。
8.2(1)	有効な class の値に **dap** オプションが追加されました。

使用上のガイドライン

class の有効な値は次のとおりです。

- **auth**：ユーザー認証。
- **bridge**：トランスペアレント ファイアウォール。
- **ca**：PKI 認証局。
- **config**：コマンドインターフェイス。
- **dap—**：ダイナミック アクセス ポリシー。
- **eap**：Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）。ネットワーク アドミッション コントロールをサポートする、EAP セッション状態の変更、EAP ステータスのクエリー イベントといったタイプのイベント、および EAP ヘッダーおよびパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：拡張可能認証プロトコル（EAP）over UDP。ネットワーク アドミッション コントロールをサポートする EAPoUDP のイベントをログに記録し、EAPoUDP ヘッダーおよびパケット内容の完全な記録を生成します。
- **eigrp**：EIGRP ルーティング。
- **email**：電子メールプロキシ。
- **ha**：フェールオーバー。

- **ids**：侵入検知システム。
- **ip**：IP スタック。
- **ipaa—**IP アドレスの割り当て
- **nac**：ネットワークアドミッションコントロール。初期化、例外リスト照合、ACS トランザクション、クライアントレス認証、デフォルト ACL 適用、および再評価といったタイプのイベントのログを記録します。
- **np**：ネットワークプロセッサ。
- **ospf**：OSPF ルーティング。
- **rip**：RIP ルーティング。
- **rm**：Resource Manager。
- **session**：ユーザーセッション。
- **snmp**：SNMP。
- **sys—**システム。
- **vpn**：IKE および IPsec。
- **vpnc**：VPN クライアント。
- **vpnfo**：VPN フェールオーバー。
- **vpnlb**：VPN ロードバランシング。

有効なロギング先は、次のとおりです。

- **asdm**：この宛先については、**logging asdm** コマンドを参照してください。
- **buffered**：この宛先については、**logging buffered** コマンドを参照してください。
- **console**：この宛先については、**logging console** コマンドを参照してください。
- **history**：この宛先については、**logging history** コマンドを参照してください。
- **mail**：この宛先については、**logging mail** コマンドを参照してください。
- **monitor**：この宛先については、**logging monitor** コマンドを参照してください。
- **trap**：この宛先については、**logging trap** コマンドを参照してください。

例

次に、フェールオーバー関連のメッセージについて、ASDM ログバッファの最大重大度が 2 で、syslog バッファの最大重大度が 7 であることを指定する例を示します。

```
ciscoasa(config)# logging class ha asdm 2 buffered 7
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging console

ASA で syslog メッセージをコンソールセッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging console** コマンドを使用します。コンソールセッションへの syslog メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。

logging console [*logging_list* | *level*]
nologgingconsole

（注） バッファ オーバーフローによって数多くの syslog メッセージがドロップされる可能性があるため、このコマンドは使用しないことを推奨します。詳細については、「使用上のガイドライン」セクションを参照してください。

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list コンソール セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

コマンド デフォルト

デフォルトでは、ASA によって syslog メッセージはコンソールセッションに表示されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コンソールにメッセージが送信される前に、 **logging enable** コマンドを使用してロギングを有効にする必要があります。

⚠

注意 **logging console** コマンドを使用すると、システムパフォーマンスが大幅に低下する可能性があります。代わりに、logging buffered コマンドを使用してロギングを開始し、show logging コマンドを使用してメッセージを表示します。最新のメッセージをより簡単に表示するには、clear logging **buffer** コマンドを使用してバッファをクリアします。

例

次に、重大度レベル 0、1、2、および 3 の syslog メッセージをコンソール セッションに表示できるようにする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging console errors
ciscoasa(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging debug-trace

デバッグメッセージを重大度レベル 7 で発行される syslog メッセージ 711001 としてログにリダイレクトするには、グローバル コンフィギュレーション モードで **logging debug-trace** コマンドを使用します。デバッグメッセージのログへの送信を停止するには、このコマンドの **no** 形式を使用します。

loggingdebug-trace
nologgingdebug-trace

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。

コマンド デフォルト

ASA のデフォルトでは、デバッグ出力は syslog メッセージに含まれません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

デバッグ メッセージは重大度レベル 7 のメッセージとして生成されます。syslog メッセージ番号 711001 でログに表示されますが、モニタリング セッションには表示されません。

例

次に、ロギングをイネーブルにし、ログ メッセージをシステム ログ バッファに送信し、デバッグ出力をログにリダイレクトし、ディスク アクティビティのデバッグをオンにする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace
ciscoasa(config)# debug disk filesystem
```

次に、ログに表示されるデバッグ メッセージの出力例を示します。

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging debug-trace persistent

特定のセッションでアクティブなデバッグ syslog をセッションの終了後もログに記録されるようにするには、グローバル コンフィギュレーション モードで **logging debug-trace persistent** コマンドを使用します。特定の永続的なデバッグ設定を無効にするには、このコマンドの **no** 形式を使用します。これにより、ローカルセッションと永続的なデバッグからエントリがクリアされます。

loggingdebug-tracepersistent
nologgingdebug-tracepersistent

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。

コマンド デフォルト

デフォルトでは、セッションが終了すると、その特定のセッションでイネーブルになっているすべてのデバッグ コマンドが設定から削除され、syslog サーバーにログが記録されなくなります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

logging debug-trace persistent コマンドがイネーブルになっている場合、セッションで入力されたデバッグ コマンドはグローバルに保存され、すべてのセションで表示できます。このコマンドは、実行コンフィギュレーションに保存され、再起動後も保持されます。

例

次に、ロギングをイネーブルにし、ログ メッセージをシステム ログ バッファに送信し、デバッグ出力をログにリダイレクトし、ディスク アクティビティの永続的なデバッグをオンにする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging debug-trace persistent
ciscoasa(config)# debug disk filesystem
```

次に、ログに表示されるデバッグ メッセージの出力例を示します。

```
%ASA-7-711001: IFS: Read: fd 3, bytes 4096
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging device-id

EMBLEM 形式でない syslog メッセージにデバイス ID を含めるように ASA 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 **logging device-id** コマンドを使用します。デバイス ID の使用を無効にするには、このコマンドの **no** 形式を使用します。

logging device-id { **cluster-id** | **context-name** | **hostname ipaddress** *interface_name* [**system**] | **string** *text* }
no logging device-id { **cluster-id** | **context-name** | **hostname ipaddress** *interface_name* [**system**] | **string** *text* }

構文の説明

cluster-id	クラスタにある個別の ASA ユニットに関する一意の名前をデバイス ID として指定します。
hostname	ASA のホスト名をデバイス ID として指定します。
ipaddress *interface_name*	デバイス ID または *interface_name* のインターフェイスの IP アドレスを指定します。ipaddress キーワードを使用すると、ログデータを外部サーバーに送信するために ASA で使用されるインターフェイスに関係なく、指定したインターフェイスの IP アドレスが外部サーバーに送信される syslog メッセージに含まれます。
string *text*	デバイス ID として *text* に含める文字を指定します。最大 16 文字です。スペースおよび次の文字は使用できません。 • &：アンパサンド • '：一重引用符 • "：二重引用符 • <：未満 • >：より大きい • ?：疑問符
system	（オプション）クラスタ環境において、インターフェイスのシステムの IP アドレスをデバイス ID として指定します。

コマンド 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

次の表は、このコマンドを入力できるモードを示しています。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	**cluster-id** および **system** キーワードが追加されました。

使用上のガイドライン

ipaddress キーワードを使用すると、メッセージが送信されるインターフェイスに関係なく、デバイス ID が指定した ASA インターフェイスの IP アドレスになります。このキーワードにより、そのデバイスから送信されるすべてのメッセージに対して、単一の一貫したデバイス ID が指定されます。**system** キーワードを使用すると、クラスタのユニットのローカル IP アドレスではなく、システムの IP アドレスが指定した ASA で使用されます。**cluster-id** および **system** キーワードは、ASA 5580 と 5585-X のみに適用されます。

例

次に、「secappl-1」というホストを設定する例を示します。

```
ciscoasa(config)# logging device-id hostname
ciscoasa(config)# show logging
Syslog logging: disabled
Facility: 20
Timestamp logging: disabled
Standby logging: disabled
Console logging: disabled
Monitor logging: disabled
Buffer logging: level informational, 991 messages logged
Trap logging: disabled
History logging: disabled
Device ID: hostname "secappl-1"
```

ホスト名は、次のメッセージに示すように、syslog メッセージの先頭に表示されます。

```
secappl-1 %ASA-5-111008: User 'enable_15' executed the 'logging buffer-size 4096' command.
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。

コマンド	説明
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging emblem

syslog サーバー以外の宛先に送信される syslog メッセージに EMBLEM 形式を使用するには、グローバル コンフィギュレーション モードで **logging emblem** コマンドを使用します。EMBLEM 形式の使用を無効にするには、このコマンドの **no** 形式を使用します。

loggingemblem
nologgingemblem

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。

コマンド デフォルト

ASA のデフォルトでは、syslog メッセージに EMBLEM 形式は使用されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは **logging host** コマンドと無関係になるように変更されました。

使用上のガイドライン

logging emblem コマンドを使用すると、syslog サーバー以外のすべてのロギング先に対して、EMBLEM形式のロギングを有効にできます。**logging timestamp** キーワードも有効にする場合、タイムスタンプが付いたメッセージが送信されます。

syslog サーバーに対して EMBLEM 形式のロギングを有効にするには、**logging host** コマンドで **format emblem** オプションを使用します。

（注） EMBLEM 形式のタイムスタンプ文字列には年は含まれません。イベント syslog に年を表示するには、**logging timestamp rfc5424** コマンドを使用して RFC 5424 に従ってタイムスタンプを有効にします。次に、RFC 5424 形式の出力例を示します。

```
<166>2018-06-27T12:17:46Z asa : %ASA-6-110002: Failed to locate egress interface for
protocol from src interface :src IP/src port to dest IP/dest port
```

または、**logging device-id** コマンドを使用できます。

例

次に、ロギングをイネーブルにし、syslog サーバを除くすべてのロギング先へのロギングに対して EMBLEM 形式の使用をイネーブルにする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging emblem
ciscoasa(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging enable

設定済みのすべての出力場所に対してロギングを有効にするには、グローバル コンフィギュレーション モードで **logging enable** コマンドを使用します。ロギングを無効にするには、このコマンドの **no** 形式を使用します。

loggingenable
nologgingenable

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。

コマンド デフォルト

ロギング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

次の表は、このコマンドを入力できるモードを示しています。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、**logging on** コマンドから変更されました。

使用上のガイドライン

logging enable コマンドを使用すると、サポートされている任意のロギング先への syslog メッセージの送信を有効または無効にできます。no logging enable コマンドを使用して、すべてのロギングを停止できます。

次のコマンドを使用して、個別のロギング先へのロギングをイネーブルにすることができます。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

例

次に、ロギングをイネーブルにする例を示します。**show logging** コマンドの出力は、使用可能な各ロギング先を個別に有効にする必要がある状況を示しています。

```
ciscoasa
(config)#
logging enable
ciscoasa
(config)#
show logging
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: disabled
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging facility

syslog サーバーに送信されるメッセージに使用するロギングファシリティを指定するには、グローバル コンフィギュレーション モードで **logging facility** コマンドを使用します。ロギングファシリティをデフォルトの 20 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。

loggingfacility*facility*
nologgingfacility

構文の説明

facility	ロギング ファシリティを指定します。有効な値は、16 ～ 23 です。

コマンド デフォルト

デフォルトのファシリティは 20（LOCAL4）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。例外については、「構文の説明」を参照してください。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

Syslog サーバは、メッセージ内のファシリティ番号に応じてメッセージをファイルに送信します。使用可能なファシリティには、16（LOCAL0）～ 23（LOCAL7）の 8 つがあります。

例

次に、ASA によってロギングファシリティが syslog メッセージに 16 として示されるように指定する例を示します。**show logging** コマンドの出力には、ASA によって使用されているファシリティが含まれます。

```
ciscoasa(config)# logging facility 16
ciscoasa(config)# show logging
Syslog logging: enabled
    Facility: 16
    Timestamp logging: disabled
    Standby logging: disabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
```

```
Monitor logging: disabled
Buffer logging: disabled
Trap logging: level errors, facility 16, 3607 messages logged
    Logging to infrastructure 10.1.2.3
History logging: disabled
Device ID: 'inside' interface IP address "10.1.1.1"
Mail logging: disabled
ASDM logging: disabled
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバーを定義します。
logging trap	syslog サーバーへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging flash-bufferwrap

未保存のメッセージでログバッファがいっぱいになるたびに、 ASA がログバッファをフラッシュメモリに書き込めるようにするには、グローバル コンフィギュレーション モードで**logging flash-bufferwrap** コマンドを使用します。フラッシュメモリへのログバッファの書き込みを無効にするには、このコマンドの **no** 形式を使用します。

loggingflash-bufferwrap
nologgingflash-bufferwrap

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。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- フラッシュ メモリへのログ バッファの書き込みはディセーブルです。
- バッファ サイズは 4 KB です。
- フラッシュ メモリの最小の空き容量は 3 MB です。
- バッファ ロギングに対するフラッシュ メモリの最大割り当て容量は 1 MB です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASAによってログバッファがフラッシュメモリに書き込まれるようにするには、バッファへのロギングを有効にする必要があります。有効にしないと、ログバッファのデータはフラッシュメモリに書き込まれません。バッファへのロギングを有効にするには、**logging buffered** コマンドを使用します。ただし、設定されたロギングバッファサイズが 2MB を超える場合、内部ログバッファはフラッシュメモリに書き込まれません。

ASA では、ログバッファの内容をフラッシュメモリに書き込む間も、新しいイベントメッセージがログバッファに保存されます。

ASA では、次のようなデフォルトのタイムスタンプ形式を使用した名前のログファイルが作成されます。

```
LOG-YYYY
-MM
-DD
-HHMMSS
.TXT
```

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

logging flash-bufferwrap コマンドを使用する場合、フラッシュメモリの可用性が、ASA による syslog メッセージの保存方法に影響します。詳細については、**logging flash-maximum-allocation** および **logging flash-minimum-free** コマンドを参照してください。

例

次に、ロギングとログバッファを有効にし、ASA によるフラッシュメモリへのログバッファの書き込みを有効にする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持している syslog メッセージをすべて消去します。
copy	TFTP サーバーまたは FTP サーバーを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ ファイルなどのファイルをディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。

logging flash-maximum-allocation

ログデータを保管するために ASA で使用するフラッシュメモリの最大量を指定するには、グローバル コンフィギュレーション モードで **logging flash-maximum-allocation** コマンドを使用します。この目的に使用するフラッシュメモリの最大量をデフォルトサイズの 1 MB 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。

loggingflash-maximum-allocation*kbytes*
nologgingflash-maximum-allocation*kbytes*

構文の説明

kbytes ログバッファデータを保存するために ASA で使用できるフラッシュメモリの最大量（KB 単位）。

コマンド デフォルト

ログ データ用のデフォルトの最大フラッシュ メモリ割り当ては 1 MB です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドで使用できるフラッシュメモリの量が決まります。

logging savelog または **logging flash-bufferwrap** で保存されるログファイルにより、ログファイル用のフラッシュメモリの使用量が **logging flash-maximum-allocation** コマンドで指定された最大量を超える場合、ASAによって最も古いログファイルが削除され、新しいログファイル用に十分な量のメモリが解放されます。削除するファイルがない場合や、古いファイルをすべて削除しても空きメモリが新しいログ ァイルには小さすぎる場合は、ASA で新しいログファイルを保存できません。

デフォルトサイズとは異なるサイズの最大フラッシュメモリ割り当て量が ASA にあるか確認するには、**show running-config logging** コマンドを使用します。**logging flash-maximum-allocation** コマンドが表示されない場合、ASA では保存されるログバッファデータに対して最大 1 MB が

使用されます。割り当てられたメモリは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンドの両方に使用されます。

ASA によるログバッファの使用方法の詳細については、**logging buffered** コマンドを参照してください。

例

次に、ロギングとログバッファを有効にし、ASA によるフラッシュメモリへのログバッファの書き込みを有効にし、ログファイルの書き込みに使用されるフラッシュメモリの最大量を約 1.2 MB に設定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-maximum-allocation 1200
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファに含まれているすべての syslog メッセージをクリアします。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログバッファがいっぱいになっている場合に、ログバッファをフラッシュ メモリに書き込みます。
logging flash-minimum-free	フラッシュメモリへのログバッファの書き込みを許可するために、ASA で使用可能にする必要があるフラッシュメモリの最小量を指定します。

logging flash-minimum-free

ASA で新しいログファイルを保存するために必要なフラッシュメモリの最小空き領域を指定するには、グローバル コンフィギュレーション モードで **logging flash-minimum-free** コマンドを使用します。フラッシュメモリの必要最小空き領域をデフォルトサイズの 3 MB 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。

loggingflash-minimum-free*kbytes*
nologgingflash-minimum-free*kbytes*

構文の説明

kbytes ASA で新しいログファイルを保存する前に使用可能にしておく必要のあるフラッシュメモリの最小量（KB 単位）。

コマンド デフォルト

フラッシュ メモリのデフォルトの最小空き領域は 3 MB です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logging flash-minimum-free コマンドでは、**logging savelog** コマンドと **logging flash-bufferwrap** コマンド用に常に保持しておく必要があるフラッシュメモリの量を指定します。

logging savelog または **logging flash-bufferwrap** で保存されるログファイルにより、フラッシュメモリの空き領域が **logging flash-minimum-free** コマンドで指定された制限を下回る場合、ASA によって最も古いログファイルが削除され、新しいログファイルの保存後も最低限の空き容量がメモリに残るようにします。削除するファイルがない場合や、古いファイルをすべて削除しても空きメモリの量がまだ制限を下回っている場合、ASA で新しいログファイルを保存できません。

例

次に、ロギングを有効にし、ログバッファを有効にし、ASA によるフラッシュメモリへのログバッファの書き込みを有効にし、フラッシュメモリの最小空き領域を 4000 KB に指定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging flash-bufferwrap
ciscoasa(config)# logging flash-minimum-free 4000
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持している syslog メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging flash-bufferwrap	ログバッファがいっぱいになっている場合に、ログバッファをフラッシュ メモリに書き込みます。
logging flash-maximum-allocation	ログ バッファの内容の書き込みに使用できるフラッシュ メモリの最大量を指定します。

logging flow-export-syslogs

NetFlow によってキャプチャされるすべての syslog メッセージを有効または無効にするには、グローバル コンフィギュレーション モードで **logging flow-export-syslogs** コマンドを使用します。

logging flow-export-syslogs { **enable** | **disable** }

構文の説明

enable	NetFlow によってキャプチャされるすべての syslog メッセージをイネーブルにします。
disable	NetFlow によってキャプチャされるすべての syslog メッセージをディセーブルにします。

コマンド デフォルト

デフォルトでは、NetFlow によってキャプチャされるすべての syslog は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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.1(1)	このコマンドが追加されました。

使用上のガイドライン

セキュリティアプライアンスが NetFlow データをエクスポートするように設定されている場合、パフォーマンス向上のため、**logging flow-export-syslogs disable** コマンドを入力して（NetFlow でキャプチャされた）冗長な syslog メッセージをディセーブルにすることを推奨します。ディセーブルにされる syslog メッセージは、次のとおりです。

syslog メッセージ	説明
106015	最初のパケットが SYN パケットではなかったため、TCP フローが拒否されました。
106023	**access-group** コマンドを使用してインターフェイスに付加される入力 ACL または出力 ACL によって拒否されたフロー。

syslog メッセージ	説明
106100	ACL によって許可または拒否されたフロー。
302013 および 302014	TCP 接続および削除。
302015 および 302016	UDP 接続および削除。
302017 および 302018	GRE 接続および削除。
302020 および 302021	ICMP 接続および削除。
313001	セキュリティ アプライアンスへの ICMP パケットが拒否されました。
313008	セキュリティアプライアンスへの ICMPv6 パケットが拒否されました。
710003	セキュリティ アプライアンスへの接続試行が拒否されました。

（注） これはコンフィギュレーションモードのコマンドですが、コンフィギュレーションに格納されません。**no logging message xxxxxx** コマンドのみが、構成に保存されます。

例

次に、NetFlow によってキャプチャされる冗長な syslog メッセージをディセーブルにする例と表示される出力例を示します。

```
ciscoasa(config)# logging flow-export-syslogs disable
ciscoasa(config)# show running-config logging
no logging message xxxxx1
no logging message xxxxx2
```

xxxxx1 および *xxxxx2* は、NetFlow によって同じ情報がキャプチャされているために冗長である syslog メッセージです。このコマンドはコマンド エイリアスに似ており、no logging message xxxxxx コマンドのバッチに変換されます。syslog メッセージは、無効にした後、**logging message xxxxxx** コマンドを使用して個別に有効にできます。*xxxxxx* は特定の syslog メッセージ番号です。

関連コマンド

コマンド	説明
flow-export destination	NetFlow コレクタの IP アドレスまたはホスト名と、NetFlow コレクタがリッスンする UDP ポートを指定します。
flow-export template timeout-rate	テンプレート情報が NetFlow コレクタに送信される間隔を制御します。
show flow-export counters	NetFlow のランタイム カウンタのセットを表示します。

logging from-address

ASA によって送信される syslog メッセージの送信者電子メール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 **logging from-address** コマンドを使用します。送信されるすべての syslog メッセージは、指定したアドレスから送信されたように表示されます。送信者電子メール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。

loggingfrom-address*from-email-address*
no logging from-address *from-email-address*

構文の説明

from-email-address	送信元電子メール アドレス。つまり、syslog メッセージの送信元として表示される電子メール アドレス（cdb@example.com など）。

コマンド 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

次の表は、このコマンドを入力できるモードを示しています。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

電子メールによる syslog メッセージの送信は、**logging mail** コマンドで有効にします。

このコマンドで指定するアドレスは、既存の電子メールアカウントに対応している必要はありません。

例

ロギングを有効にし、syslog メッセージを電子メールで送信するように ASA を設定するには、次の基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する

- プライマリ サーバー pri-smtp-host およびセカンダリ サーバー sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
ciscoasa
(config)#
logging enable
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging mail	ASA の電子メールによる syslog メッセージの送信を有効にし、電子メールで送信するメッセージを決定します。
logging recipient-address	syslog メッセージの送信先の電子メール アドレスを指定します。
smtp-server	SMTP サーバーを設定します。
show logging	イネーブルなロギング オプションを表示します。

logging ftp-bufferwrap

未保存のメッセージでログバッファがいっぱいになるたびに、ASA が FTP サーバーにログバッファを送信できるようにするには、グローバル コンフィギュレーション モードで **logging ftp-bufferwrap** コマンドを使用します。FTP サーバーへのログバッファの送信を無効にするには、このコマンドの **no** 形式を使用します。

loggingftp-bufferwrap
no logging ftp-bufferwrap

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。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- バッファへのロギングはディセーブルです。
- FTP サーバーへのログ バッファの送信はディセーブルです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logging ftp-bufferwrap を有効にすると、ASA により、ログバッファデータは **logging ftp-server** コマンドで指定した FTP サーバーに送信されます。ASA は、ログデータを FTP サーバーに送信する間も、新しいイベントメッセージをログバッファに保管し続けます。

ASA によってログバッファの内容が FTP サーバーに送信されるようにするには、バッファへのロギングを有効にする必要があります。有効にしないと、ログバッファのデータはフラッシュメモリに書き込まれません。バッファへのロギングを有効にするには、**logging buffered** コマンドを使用します。

ASA では、次のようなデフォルトのタイムスタンプ形式を使用した名前のログファイルが作成されます。

```
LOG-YYYY
-MM
-DD
-HHMMSS
.TXT
```

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

例

次に、ロギングとログバッファを有効にし、FTP サーバーを指定して、ASA が FTP サーバーにログバッファを書き込めるようにする例を示します。この例では、ホスト名が logserver-352 である FTP サーバーを指定しています。サーバーには、ユーザー名 logsupervisor およびパスワード 1luvMy10gs でアクセスできます。ログ ファイルは /syslogs ディレクトリに保存されます。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver-352 /syslogs logsupervisor 1luvMy10gs
ciscoasa(config)# logging ftp-bufferwrap
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持している syslog メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-server	**logging ftp-bufferwrap** コマンドで使用する FTP サーバーパラメータを指定します。

logging ftp-server

logging ftp-bufferwrap が有効になっている場合に ASA からログバッファデータが送信される FTP サーバーの詳細を指定するには、グローバル コンフィギュレーション モードで **logging ftp-server** コマンドを使用します。FTP サーバーの詳細をすべて削除するには、このコマンドの **no** 形式を使用します。

logging ftp-server *ftp_server path username* [*0* | *8*] *password*
no logging ftp-server *ftp_server path username* [*0* | *8*] *password*

構文の説明

0	（任意）暗号化されていない（クリアテキストの）ユーザーパスワードが続くことを指定します。
8	（任意）暗号化されたユーザー パスワードが続くことを指定します。
ftp-server	外部 FTP サーバーの IP アドレスまたはホスト名。 （注） ホスト名を指定した場合、DNS がご使用のネットワークで適切に運用されていることを確認してください。
password	指定したユーザー名のパスワード。最大 64 文字です。
path	ログ バッファ データが保存される FTP サーバー上のディレクトリ パス。このパスは、FTP ルート ディレクトリに対する相対パスです。次に例を示します。 `/security_appliances/syslogs/appliance107`
username	FTP サーバーへのログインに有効なユーザー名。

コマンド デフォルト

デフォルトでは、FTP サーバーは指定されていません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
8.3(1)	パスワード暗号化のサポートが追加されました。

使用上のガイドライン

FTP サーバは 1 つのみ指定できます。ロギング FTP サーバーがすでに指定されている場合、**logging ftp-server** コマンドを使用すると、この FTP サーバー構成は入力した新しい構成に置き換えられます。

指定した FTP サーバー情報は ASA によって検証されません。詳細を誤って設定した場合、ASA から FTP サーバーにログバッファデータを送信できません。

ASA の起動やアップグレードでは、1 桁のパスワードや、数字で始まりその後にスペースが続くパスワードはサポートされません。たとえば、0 pass や 1 は不正なパスワードです。

例

次に、ロギングとログバッファを有効にし、FTP サーバーを指定して、ASA が FTP サーバーにログバッファを書き込めるようにする例を示します。この例では、logserver というホスト名の FTP サーバーを指定します。サーバーは、ユーザー名 user1 とパスワード pass1 でアクセスできるものとします。ログ ファイルは /path1 ディレクトリに保存されます。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# logging ftp-server logserver /path1 user1 pass1
ciscoasa(config)# logging ftp-bufferwrap
```

次に、暗号化されたパスワードを入力する例を示します。

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 8
JPAGWzIIFVlheXv2I9nglfytOzHU
```

次に、暗号化されていない（クリア テキストの）パスワードを入力する例を示します。

```
ciscoasa(config)# logging ftp-server logserver /path1 user1 0 pass1
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持している syslog メッセージをすべて消去します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging buffer-size	ログ バッファ サイズを指定します。
logging enable	ロギングをイネーブルにします。
logging ftp-bufferwrap	ログ バッファがいっぱいになったときに、ログ バッファを FTP サーバーに送信します。

logging hide username

ユーザー名の有効性が不明である場合に syslog のユーザー名を非表示（「*****」など）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 **logging hide username** コマンドを使用します。非表示にしたユーザー名を表示するには、このコマンドの **no** 形式を使用します。

logginghideusername
no logging hide username

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。

コマンド デフォルト

デフォルトでは、ユーザー名は非表示です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(3)	このコマンドが追加されました。

使用上のガイドライン

logging hide username コマンドにより、有効性が確認されていないユーザーのユーザー名を syslog で非表示にできます。

（注） このコマンドは、バージョン 9.4(1) では使用できません。

例

次に、有効性が確認されていないユーザー名を syslog で非表示にする例を示します。

```
ciscoasa(config)# logging hide username
ciscoasa# show logging
Syslog logging: enabled
...
Hide Username logging: enabled | disabled
...
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging history

SNMP ロギングを有効にし、SNMP サーバーに送信するメッセージを指定するには、グローバル コンフィギュレーション モードで **logging history** コマンドを使用します。SNMP ロギングを無効にするには、このコマンドの **no** 形式を使用します。

logging history [**rate-limit** *rate-limit number* | *logging_list* | *level*]
no logging history

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list SNMP サーバーに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

rate-limit SNMP に転送されるログを制限するには、このキーワードを使用します。syslog にログに記録するためのレート制限を秒単位で指定します。

コマンド デフォルト

デフォルトでは、ASA によって SNMP サーバーにロギングされません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logging history コマンドを使用すると、SNMP サーバーへのロギングを有効にし、SNMP メッセージレベルまたはイベントリストを設定できます。SNMP に記録される syslog の **rate-limit** キーワードのイネーブルは、「logging history」CLI の「rate-limit」および「level」で指定された値に基づいて実行されます。

例

次に、SNMP ロギングをイネーブルにし、重大度レベル 0、1、2、および 3 のメッセージが設定済みの SNMP サーバに送信されることを指定する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# snmp-server host infrastructure 10.2.3.7 trap community gam327
ciscoasa(config)# snmp-server enable traps syslog
ciscoasa(config)# logging history errors
ciscoasa(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。
snmp-server	SNMP サーバーの詳細を指定します。

logging host

syslog サーバーを定義するには、グローバル コンフィギュレーション モードで **logging host** コマンドを使用します。syslog サーバー定義を削除するには、このコマンドの **no** 形式を使用します。

logging host *interface_name syslog_ip* [**tcp** [*/ port*] | **udp** [*/ port*]] [**format emblem**]] [**secure** [**reference-identity** *reference_identity_name*]]
no logging host *interface_name syslog_ip* [**tcp** [*/ port*] | **udp** [*/ port*] [**format emblem**]] [**secure** [**reference-identity** *reference_identity_name*]]

構文の説明

format emblem	（任意）syslog サーバーに対して EMBLEM 形式のロギングをイネーブルにします。EMBLEM 形式のロギングは、UDP syslog メッセージのみに使用できます。
interface_name	syslog サーバーが配置されているインターフェイスを指定します。
port	syslog サーバーがメッセージをリッスンするポートを指定します。有効なポート値は、いずれのプロトコルも 1025 ～ 65535 です。ポート番号として 0 を入力したり、無効な文字や記号を使用したりすると、エラーが発生します。
secure	（オプション）リモート ロギング ホストへの接続に SSL/TLS を使用するように指定します。このオプションは、選択されたプロトコルが TCP の場合にだけ有効です。 （注） セキュアなロギング接続は、SSL/TLS 対応の syslog サーバーとのみ確立できます。SSL/TLS 接続を確立できない場合、新しい接続はすべて拒否されます。このデフォルトの動作は、**logging permit-hostdown** コマンドを入力して変更できます。
syslog_ip	syslog サーバーの IP アドレス（IPv4 または IPv6）を指定します。
tcp	ASA が TCP を使用して syslog サーバーにメッセージを送信するよう指定します。
udp	ASA が UDP を使用して syslog サーバーにメッセージを送信するよう指定します。
reference_identity_name	セキュリティを強化するための RFC 6125 参照アイデンティティ チェックを可能にする参照アイデンティティ オブジェクトの名前を指定します。受信したサーバー証明書に関するアイデンティティ チェックは、この事前に設定された参照アイデンティティ オブジェクトに基づいて実行されます。

timestamp [**legacy** | **rfc5424**]	（任意）従来の形式またはRFC5424形式（yyyy-MM-THH:mm:ssZ、文字ZはUTCタイムゾーンを示す）で指定できるタイムスタンプ形式を有効にします。

コマンド デフォルト

デフォルト プロトコルは UDP です。

format emblem オプションのデフォルト設定は false です。

secure オプションのデフォルト設定は false です。

デフォルトのポート番号は次のとおりです。

- UDP：514
- TCP：1470

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。
8.0(2)	**secure** キーワードが追加されました。
8.4(1)	接続のブロッキングをイネーブルまたはディセーブルにできるようになりました。
9.6.2	**reference-identity** オプションが追加されました。
9.7(1)	syslog サーバーに IPv6 アドレスを使用できるようになりました。直接接続された syslog サーバーがある場合、ASA および syslog サーバーの /31 サブネットを使用してポイントツーポイント接続を作成できます。

使用上のガイドライン

logging host *syslog_ip* format emblem コマンドを使用すると、各 syslog サーバーに対して EMBLEM 形式のロギングを有効にできます。EMBLEM 形式のロギングは、UDP syslog メッセージのみに使用できます。EMBLEM 形式のロギングを特定の syslog サーバーに対してイネーブルにすると、メッセージはそのサーバーに送信されます。**logging timestamp** コマンドを使用すると、タイムスタンプが付与されたメッセージも送信されます。

複数の logging host コマンドを使用して、追加サーバーを指定できます。それらすべてで syslog メッセージが受信されます。ただし、UDP と TCP 両方ではなく、いずれかの syslog メッセージのみが受信されるようにサーバーを指定できます。

サーバー証明書で提示されるアイデンティティが、設定済みの **reference-identity** と一致しない場合、接続は確立されず、エラーがログに記録されます。

接続のブロッキングに対するデフォルト設定は、 syslog サーバーへのメッセージ送信に TCP を使用するように、**logging host** コマンドが設定されている場合にのみ有効になります。TCP ベースの syslog サーバーが設定されている場合、 **logging permit-hostdown** コマンドを使用して、接続のブロッキングを無効にできます。

（注） **logging host** コマンドで **tcp** オプションを使用すると、syslog サーバーに到達できない場合、ファイアウォールを通過する接続は ASA によってドロップされます。

以前に入力した *port* 値と *protocol* 値のみを表示するには、 **show running-config logging** コマンドを使用して、リストからコマンドを見つけます。TCP は 6、UDP は 17 として表示されます。TCP ポートは syslog サーバーのみで機能します。*port* は、syslog サーバーがリッスンするポートと同じである必要があります。

（注） **logging host** コマンドと **secure** キーワードを UDP で使用しようとすると、エラーメッセージが表示されます。

TCP での syslog の送信は、スタンバイ ASA ではサポートされていません。

例

次に、重大度レベル 0、1、2、および 3 の syslog メッセージを、デフォルトのプロトコルとポート番号を使用する内部インターフェイス上の syslog サーバーに送信する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 2001:192:168:88::111
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging trap	syslog サーバーへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。

コマンド	説明
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging list

さまざまな基準（ログレベル、イベントクラス、およびメッセージ ID）でメッセージを指定するために、他のコマンドで使用するロギングリストを作成するには、グローバル コンフィギュレーション モードで **logging list** コマンドを使用します。リストを削除するには、このコマンドの **no** 形式を使用します。

logging list *name* { **level** *level* [**class** *event_class*] | **message** *start_id* [*-end_id*] }
no logging list *name*

構文の説明

class *event_class*	（任意）syslog メッセージのイベントのクラスを設定します。指定したレベルについて、指定したクラスの syslog メッセージのみがコマンドによって識別されます。クラスのリストについては、「使用上のガイドライン」を参照してください。
level *level*	syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。 • **0** または **emergencies**：システムが使用不能。 • **1** または **alerts**：すぐに対処が必要。 • **2** または **critical**：重大な状態。 • **3** または **errors**：エラー状態。 • **4** または **warnings**：警告状態。 • **5** または **notifications**：通常の状態だが、重要な状態。 • **6** または **informational**：Informational（情報提供）メッセージ。 • **7** または **debugging**：Debug（デバッグ）メッセージ。 （注） デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

message *start_id* [*-end_id*]	メッセージ ID または ID の範囲を指定します。メッセージのデフォルレベルを調べるには、**show logging** コマンドを使用するか、syslog メッセージガイドを参照してください。
name	ロギング リスト名を設定します。

コマンド 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

次の表は、このコマンドを入力できるモードを示しています。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

リストを使用できるロギング コマンドは、次のとおりです。

- **logging asdm**
- **logging buffered**
- **logging console**
- **logging history**
- **logging mail**
- **logging monitor**
- **logging trap**

event_class で使用できる値は、次のとおりです。

- **auth**：ユーザー認証。
- **bridge**：トランスペアレント ファイアウォール。
- **ca**：PKI 認証局。
- **config**：コマンドインターフェイス。

- **eap**：Extensible Authentication Protocol（EAP; 拡張可能認証プロトコル）。ネットワーク アドミッション コントロールをサポートする、EAP セッション状態の変更、EAP ステータスのクエリー イベントといったタイプのイベント、および EAP ヘッダーおよびパケット内容の 16 進ダンプをログに記録します。
- **eapoudp**：拡張可能認証プロトコル（EAP）over UDP。ネットワーク アドミッション コントロールをサポートする EAPoUDP のイベントをログに記録し、EAPoUDP ヘッダーおよびパケット内容の完全な記録を生成します。
- **email**：電子メールプロキシ。
- **ha**：フェールオーバー。
- **ids**：侵入検知システム。
- **ip**：IP スタック。
- **nac**：ネットワーク アドミッション コントロール。初期化、例外リスト照合、ACS トランザクション、クライアントレス認証、デフォルト ACL 適用、および再評価といったタイプのイベントのログを記録します。
- **np**：ネットワークプロセッサ。
- **ospf**：OSPF ルーティング。
- **rip**：RIP ルーティング。
- **session**：ユーザーセッション。
- **snmp**：SNMP。
- **sys**—システム。
- **vpn**：IKE および IPsec。
- **vpnc**：VPN クライアント。
- **vpnfo**：VPN フェールオーバー。
- **vpnlb**：VPN ロードバランシング。

例

次に、logging list コマンドの使用例を示します。

```
ciscoasa(config)# logging list my-list 100100-100110
ciscoasa(config)# logging list my-list level critical
ciscoasa(config)# logging list my-list level warning class vpn
ciscoasa(config)# logging buffered my-list
```

上記の例は、指定された基準と一致する syslog メッセージがロギング バッファに送信されることを示しています。この例で指定されている基準は、次のとおりです。

- 100100 ～ 100110 の範囲の syslog メッセージ ID
- critical レベル以上のすべての syslog メッセージ（emergency、alert、または critical）

- warning レベル以上のすべての VPN クラスの syslog メッセージ（emergency、alert、critical、error、または warning）

syslog メッセージがこれらの条件のいずれかを満たしている場合、そのメッセージはバッファにロギングされます。

（注） リストの基準を設計する場合、メッセージを重複して指定する基準でも構いません。複数の基準と一致する syslog メッセージも正常にロギングされます。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging mail

ASA で syslog メッセージを電子メールで送信できるようにし、電子メールで送信するメッセージを決定できるようにするには、グローバル コンフィギュレーション モードで **logging mail** コマンドを使用します。syslog メッセージの電子メール送信を無効にするには、このコマンドの **no** 形式を使用します。

logging mail [*logging_list* | *level*]
no logging mail [*logging_list* | *level*]

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list 電子メールの受信者に送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

コマンド デフォルト

電子メールへのロギングは、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

次の表は、このコマンドを入力できるモードを示しています。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

電子メールで送信される syslog メッセージは、送信された電子メールの件名欄に表示されます。

例

電子メールで syslog メッセージを送信するように ASA を設定するには、次のような基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバー pri-smtp-host およびセカンダリ サーバー sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。

コマンド	説明
logging from-address	電子メールで送信される syslog メッセージの送信元として表示される電子メール アドレスを指定します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
logging recipient-address	電子メールで送信される syslog メッセージの送信先の電子メール アドレスを指定します。
smtp-server	SMTP サーバーを設定します。

logging message

syslog メッセージのロギングを有効にする、またはメッセージのレベルを変更するには、グローバル コンフィギュレーション モードで **logging message** コマンドを使用します。メッセージのロギングを無効にする、またはメッセージをデフォルトのレベルに設定するには、このコマンドの **no** 形式を使用します。

logging message *syslog_id* [**level** *level* | **standby**]
no logging message *syslog_id* [**level** *level* | **standby**]

構文の説明

level *level*
（オプション）指定された syslog メッセージの重大度レベルを設定します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

メッセージのデフォルレベルを調べるには、**show logging** コマンドを使用するか、syslog メッセージガイドを参照してください。

syslog_id
イネーブルまたはディセーブルにする syslog メッセージまたは重大度レベルを変更する syslog メッセージの ID。

standby
（任意）スタンバイユニットで特定の syslog メッセージが生成されないようにするには、このコマンドの **no** 形式を **standby** キーワードとともに指定します。

コマンド デフォルト

デフォルトでは、すべてのsyslogメッセージはイネーブルであり、すべてのメッセージの重大度レベルはデフォルトのレベルに設定されています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.4(1)	**standby** キーワードが追加されました。

使用上のガイドライン

logging message コマンドは次の目的に使用できます。

- メッセージをイネーブルにするかディセーブルにするかを指定します。
- スタンバイ ユニットでの syslog メッセージの生成をディセーブルにします。
- メッセージの重大度レベルを指定します。

show logging コマンドを使用して、メッセージに現在割り当てられているレベルや、メッセージが有効かどうかを判別できます。

ASA で特定の syslog メッセージを生成しないようにするには、グローバル コンフィギュレーション モードで **logging message** コマンドの **no** 形式を使用します（**level** キーワードは不要）。ASA で特定の syslog メッセージを生成できるようにするには、**logging message** コマンドを使用します（**level** キーワードは不要）。これら 2 つの種類の **logging message** コマンドは、並行して実行できます。

例

次の例にある一連のコマンドは、**logging message** コマンドを使用して、メッセージを有効にするかどうか、およびメッセージの重大度を指定する方法を示しています。

```
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
ciscoasa(config)# logging message 403503 level 1
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no
logging message 403503
ciscoasa(config)# show logging message 403503
```

```
syslog 403503: default-level errors, current-level alerts (disabled)
ciscoasa(config)# logging message 403503
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled)
ciscoasa(config)# no
logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled),standby logging (disabled)
ciscoasa(config)# no logging message 403503 level 3
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors (enabled)
```

関連コマンド

コマンド	説明
clear configure logging	すべてのロギング コンフィギュレーションまたはメッセージ コンフィギュレーションのみをクリアします。
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging message standby

スタンバイユニットでの生成を以前にブロックした特定のsyslogメッセージのブロックを解除するには、**logging message standby** コマンドを使用します。スタンバイ装置で特定の syslog メッセージが生成されないようにブロックするには、このコマンドの **no** 形式を使用します。

logging message *syslog_id* **standby**
no logging message *syslog_id* **standby**

構文の説明

syslog_id	スタンバイ ユニットでイネーブルまたはディセーブルにする syslog メッセージの ID。

コマンド デフォルト

デフォルトでは、すべての syslog メッセージがスタンバイ ユニットで生成されます（logging standby コマンドがイネーブルの場合のみ）。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

[no] logging message *syslog_id* **standby** コマンドを使用して、スタンバイユニットで syslog メッセージを有効にするか無効にするかを指定できます。

show logging コマンドを使用して、syslog メッセージが有効になっているかどうかを確認できます。

例

次に、**logging message** *syslog_id* **standby** コマンドの使用例を示します。この一連の例では、スタンバイユニットで syslog メッセージが有効になっているかどうかを確認しています。

```
ciscoasa(config)# no logging message 403503 standby
ciscoasa(config)# show logging message 403503
syslog 403503: default-level errors, current-level alerts (enabled), standby logging
disabled
```

関連コマンド

コマンド	説明
clear configure logging	すべてのロギング コンフィギュレーションまたはsyslogメッセージ コンフィギュレーションのみをクリアします。
logging enable	ロギングをイネーブルにします。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging monitor

ASA で syslog メッセージを SSH セッションおよび Telnet セッションに表示できるようにするには、グローバル コンフィギュレーション モードで **logging monitor** コマンドを使用します。SSH セッションおよび Telnet セッションへの syslog メッセージの表示を無効にするには、このコマンドの **no** 形式を使用します。

logging monitor [*logging_list* | *level*]
nologgingmonitor

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list SSH セッションまたは Telnet セッションに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

コマンド デフォルト

ASA のデフォルトでは、syslog メッセージは SSH セッションや Telnet セッションに表示されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logging monitor コマンドにより、現在のコンテキストのセッションすべてに対して syslog メッセージが有効になります。ただし、各セッションに syslog メッセージが表示されるかどうかは、**terminal** コマンドによって制御されます。

例

次に、コンソール セッションで syslog メッセージの表示をイネーブルにする例を示します。**errors** キーワードの使用は、重大度レベル 0、1、2、および 3 のメッセージが SSH セッションおよび Telnet セッションに表示されることを示しています。**terminal** コマンドを使用すると、メッセージを現在のセッションに表示できます。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging monitor errors
ciscoasa(config)# terminal monitor
ciscoasa(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。
terminal	端末回線のパラメータを設定します。

logging permit-hostdown

TCPベースのsyslogサーバーのステータスを新しいユーザーセッションと無関係にするには、グローバル コンフィギュレーション モードで **logging permit-hostdown** コマンドを使用します。TCP ベースの syslog サーバーが使用できないときに ASA で新しいユーザーセッションを拒否するには、このコマンドの **no** 形式を使用します。

loggingpermit-hostdown
nologgingpermit-hostdown

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。

コマンド デフォルト

デフォルトでは、TCP接続を使用するsyslogサーバーへのロギングを有効にした場合、何らかの理由で syslog サーバーが使用できないと、ASA では新しいネットワーク アクセス セッションが許可されません。**logging permit-hostdown** コマンドのデフォルト設定は false です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

syslogサーバーにメッセージを送信するためのロギング トランスポート プロトコルとしてTCPを使用している場合、ASAは、syslogサーバーに到達できない際、セキュリティ対策として新しいネットワーク アクセス セッションを拒否します。**logging permit-hostdown** コマンドを使用して、この制限を削除できます。

例

次に、TCP ベースの syslog サーバーのステータスを、ASA で新しいセッションが許可されるかどうかと無関係にする例を示します。**show running-config logging** コマンドの出力に **logging permit-hostdown** コマンドが含まれている場合、TCP ベースの syslog サーバーのステータスは、新しいネットワーク アクセス セッションと無関係です。

```
ciscoasa(config)# logging permit-hostdown
ciscoasa(config)# show running-config logging
```

```
logging enable
logging trap errors
logging host infrastructure 10.1.2.3 6/1470
logging permit-hostdown
ciscoasa(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバーを定義します。
logging trap	syslog サーバーへのロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging queue

ロギング構成に従って処理する前に ASA のキューに保持できる syslog メッセージの数を指定するには、グローバル コンフィギュレーション モードで **logging queue** コマンドを使用します。ロギングキューのサイズをデフォルトの 512 メッセージ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。

logging queue *queue_size*
no logging queue *queue_size*

構文の説明

queue_size 処理前の syslog メッセージを保管するために使用されるキューで許可される syslog メッセージの数。有効な値は、プラットフォームの種類に応じて 0 ～ 8192 メッセージです。ロギング キューが 0 に設定されている場合、プラットフォームに応じて、キューは設定可能な最大サイズ（8192 メッセージ）になります。ASA-5505 では、キューの最大サイズは 1024 です。ASA-5510 では 2048 です。その他のすべてのプラットフォームでは 8192 です。

コマンド デフォルト

デフォルトのキュー サイズは 512 メッセージです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

トラフィックが多いためにキューがいっぱいになった場合、ASA によってメッセージが破棄される場合があります。ASA-5505 では、キューの最大サイズは 1024 です。ASA-5510 では 2048 です。その他のすべてのプラットフォームでは 8192 です。

注意 ローエンドプラットフォーム上のロギングキューサイズを大きくすると、ASDM、WebVPN、DHCPサーバーなど、他の機能に使用可能なDMAメモリ容量が減少します。これらの機能は、システムがDMAメモリを使い果たした場合に機能を停止することができます。MEMPOOL_DMAプール内の DMA メモリの空き容量を確認するには、**show memory detail** コマンドを使用します。

例

次に、logging queue コマンドおよび show logging queue コマンドの出力を表示する例を示します。

```
ciscoasa(config)# logging queue 0
ciscoasa(config)# show logging queue
Logging Queue length limit : Unlimited
Current 5 msg on queue, 3513 msgs most on queue, 1 msg discard.
```

この例では、logging queue コマンドは 0 に設定されています。つまり、キューは最大の 8192 に設定されます。キュー内の syslog メッセージは、ロギング構成で指定された方法で ASA によって処理されます。たとえば、syslog メッセージがメールの受信者に送信されたり、フラッシュメモリに保存されたりします。

この例の show logging queue コマンドの出力には、5 つのメッセージがキューにあり、ASA が最後に起動されて以降、同時にキューにあった最大メッセージ数は 3513 であり、1 つのメッセージが廃棄されたことが示されています。キューのメッセージは無制限に設定されていましたが、メッセージをキューに追加するためのブロック メモリを使用できなかったために、メッセージは廃棄されました。

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging rate-limit

syslog メッセージの生成レートを制限するには、特権 EXEC モードで **logging rate-limit** コマンドを使用します。レート制限を無効にするには、特権 EXEC モードでこのコマンドの **no** 形式を使用します。

logging rate-limit { **unlimited** | **dynamic** { **block** *value* [**message limit** *value*] } | { *num* [*interval*] } | **message** { *syslog_id* | **level** *severity_level* } }
[**no**] **logging rate-limit** { **unlimited** | **dynamic** { **block** *value* [**message limit** *value*] } | { *num* [*interval*] } | **message** { *syslog_id* | **level** *severity_level* } }

構文の説明

interval	（任意）メッセージの生成レートを測定するために使用する時間間隔（秒単位）。*interval* 値の有効な範囲は、0 ～ 2147483647 です。
level *severity_level*	設定されたレート制限を、特定の重大度レベルに属するすべての syslog メッセージに適用します。指定した重大度レベルのすべての syslog メッセージは、個別にレート制限されます。*severity_level* の有効な範囲は、1 ～ 7 です。
message	この syslog メッセージのレポートを抑制します。
num	指定した時間間隔で生成できる syslog メッセージの数。*num* 値の有効な範囲は、0 ～ 2147483647 です。
syslog_id	抑制する syslog メッセージの ID。有効な値の範囲は 100000 ～ 999999 です。
unlimited	レート制限をディセーブルにします。これは、ロギング レートが制限されないことを意味します。
dynamic	ブロック使用量が指定されたしきい値（256）を超えたときにロギングレートを制限します。ブロックの使用量が通常の値に戻ったときにレート制限を無効にします。
block*value*	レート制限のしきい値として機能するブロックのパーセンテージ。
message limit*value*	動的レート制限で許可されるメッセージの数。

コマンド デフォルト

interval のデフォルト設定は 1 です。

message limit*value* のデフォルト設定は 10 です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。
9.18(1)	レート制限の動的オプションが追加されました。

使用上のガイドライン

syslog メッセージの重大度レベルは、次のとおりです。

- 0：システムが使用不能
- 1：すぐに対処が必要
- 2：重大な状態
- 3：エラー状態
- 4：警告状態
- 5：通常の状態だが、重要な状態
- 6：情報メッセージ
- 7：デバッグ メッセージ

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

例

syslog メッセージの生成レートを制限するために、特定のメッセージ ID を入力できます。次に、特定のメッセージ ID と時間間隔を使用して syslog メッセージの生成レートを制限する例を示します。

```
ciscoasa(config)# logging rate-limit 100 600 message 302020
```

この例では、指定した 600 秒の間隔でレート制限 100 に達すると、syslog メッセージ 302020 はホストに送信されなくなります。

syslog メッセージの生成レートを制限するために、特定の重大度レベルを入力できます。次に、特定の重大度レベルと時間間隔を使用して syslog メッセージの生成レートを制限する例を示します。

```
ciscoasa(config)# logging rate-limit 1000 600 level 6
```

この例では、重大度レベル 6 のすべての syslog メッセージは、指定した 600 秒の時間間隔で指定したレート制限 1000 に抑制されます。重大度レベル 6 の各 syslog メッセージには、レート制限 1000 があります。

サイズ 256 のブロック使用率が高い場合にメッセージの動的レート制限を有効にするには、**dynamic** キーワードを使用します。動的レート制限をトリガーするためのしきい値として、サイズ 256 の空きブロックの割合を指定できます。また、**message limit** キーワードを使用して、動的レート制限のメッセージ数を許可できます。デフォルト値は 10 です。

```
asa(config)# logging rate-limit ?

configure mode commands/options:
  <1-2147483647>  Specify logging rate-limit number
  dynamic         Specify dynamic option for rate-limit
  unlimited       Specify unlimited option for rate-limit

asa(config)# logging rate-limit dynamic ?

configure mode commands/options:
  block  Dynamic rate-limit for block usage

asa(config)# logging rate-limit dynamic block ?

configure mode commands/options:
  <1-100>  Specify 256 blocks free percentage to trigger dynamic rate-limit
asa(config)# logging rate-limit dynamic block 50 ?

configure mode commands/options:
  messagelimit  Specify the number of messages allowed for dynamic rate-limit

asa(config)# logging rate-limit dynamic block 50 messagelimit ?

configure mode commands/options:
  <1-100>  Specify logging rate-limit interval
```

関連コマンド

コマンド	説明
clear running-config logging rate-limit	ロギング レート制限の設定をデフォルトにリセットします。
show logging	内部バッファ内の現在のメッセージ、またはロギング コンフィギュレーションの設定を表示します。

コマンド	説明
show running-config logging rate-limit	現在のロギング レート制限の設定を表示します。

logging recipient-address

ASA によって送信される syslog メッセージの受信者の電子メール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 **logging recipient-address** コマンドを使用します。受信者の電子メール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。

logging recipient-address *address* [**level** *level*]
no logging recipient-address *address* [**level** *level*]

構文の説明

address	syslog メッセージを電子メールで送信するときの受信者の電子メール アドレスを指定します。
level	重大度レベルが後に続くことを示します。

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力は CPU プロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

（注） **logging recipient-address** コマンドで 3 よりも大きい重大度レベルを使用することは推奨しません。重大度レベルを大きくすると、バッファ オーバーフローによって syslog メッセージがドロップされる可能性があります。

logging recipient-address コマンドで指定するメッセージ重大度レベルによって、**logging mail** コマンドで指定するメッセージ重大度レベルは上書きされます。たとえば、**logging recipient-address** コマンドで重大度レベル 7 を指定するが、**logging mail** コマンドで重大度レベル 3 を指定している場合、ASA によって、重大度レベル 4、5、6、および 7 のメッセージを含むすべてのメッセージが受信者に送信されます。

コマンド デフォルト

デフォルトでは、errors ログ レベルに設定されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

最大 5 つの受信者アドレスを設定できます。必要に応じて、受信者アドレスごとに、 **logging mail** コマンドで指定されたメッセージレベルとは異なるメッセージレベルを指定できます。電子メールによる syslog メッセージの送信は、**logging mail** コマンドで有効にします。

このコマンドは、緊急性の高いメッセージを多数の受信者に送信する場合に使用します。

例

電子メールで syslog メッセージを送信するように ASA を設定するには、次のような基準を使用します。

- critical、alert、または emergency レベルのメッセージを送信する
- ciscosecurityappliance@example.com を送信元アドレスに使用して、メッセージを送信する
- admin@example.com にメッセージを送信する
- プライマリ サーバー pri-smtp-host およびセカンダリ サーバー sec-smtp-host を使用して、SMTP でメッセージを送信する

次のコマンドを入力します。

```
ciscoasa
(config)#
logging mail critical
ciscoasa
(config)#
logging from-address ciscosecurityappliance@example.com
ciscoasa
(config)#
logging recipient-address admin@example.com
ciscoasa
(config)#
smtp-server pri-smtp-host sec-smtp-host
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging from-address	syslog メッセージの送信元として表示される電子メール アドレスを指定します。
logging mail	ASA の電子メールによる syslog メッセージの送信を有効にし、電子メールで送信するメッセージを決定します。
smtp-server	SMTP サーバーを設定します。
show logging	イネーブルなロギング オプションを表示します。

logging savelog

ログバッファをフラッシュメモリに保存するには、特権 EXEC モードで **logging savelog** コマンドを使用します。

logging savelog [*savefile*]

構文の説明

savefile （任意）保存するフラッシュ メモリ ファイルの名前。ファイル名を指定しない場合は、次に示すように、ログファイルはASAによってデフォルトのタイムスタンプ形式を使用して保存されます。

```
LOG-YYYY
-MM
-DD
-HHMMSS
.TXT
```

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- バッファ サイズは 4 KB です。
- フラッシュ メモリの最小の空き容量は 3 MB です。
- バッファ ロギングに対するフラッシュ メモリの最大割り当て容量は 1 MB です。
- デフォルトのログ ファイル名については、「構文の説明」を参照してください。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ログ バッファをフラッシュ メモリに保存する前に、バッファへのロギングをイネーブルにする必要があります。イネーブルにしないと、ログ バッファのデータはフラッシュ メモリに保

存されません。バッファへのロギングを有効にするには、**logging buffered** コマンドを使用します。

（注） **logging savelog** コマンドによってバッファはクリアされません。バッファをクリアするには、**clear logging buffer** コマンドを使用します。

例

次に、ロギングとログ バッファをイネーブルにし、グローバル コンフィギュレーション モードを終了し、ファイル名 latest-logfile.txt を使用してログ バッファをフラッシュ メモリに保存する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging buffered
ciscoasa(config)# exit
ciscoasa# logging savelog latest-logfile.txt
ciscoasa#
```

関連コマンド

コマンド	説明
clear logging buffer	ログ バッファが保持している syslog メッセージをすべて消去します。
copy	TFTP サーバーまたは FTP サーバーを使用して、ファイルをある場所から別の場所にコピーします。
delete	保存されたログ ファイルなどのファイルをディスク パーティションから削除します。
logging buffered	ログ バッファへのロギングをイネーブルにします。
logging enable	ロギングをイネーブルにします。

logging standby

フェールオーバースタンバイ ASA で syslog メッセージをロギング先に送信できるようにするには、グローバル コンフィギュレーション モードで **logging standby** コマンドを使用します。syslog メッセージングと SNMP ロギングを無効にするには、このコマンドの **no** 形式を使用します。

loggingstandby
nologgingstandby

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。

コマンド デフォルト

logging standby コマンドは、デフォルトでディセーブルです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

フェールオーバー発生時に、フェールオーバースタンバイ ASA の syslog メッセージの同期を継続させるために、**logging standby** コマンドを有効にできます。

（注） **logging standby** コマンドを使用すると、syslog サーバー、SNMP サーバー、FTP サーバーなどの共有ロギング先でのトラフィックは 2 倍になります。

例

次に、ASA で syslog メッセージをフェールオーバースタンバイ ASA に送信できるようにする例を示します。**show logging** コマンドの出力は、この機能が有効になっていることを示しています。

```
ciscoasa(config)# logging standby
ciscoasa(config)# show logging
```

```
Syslog logging: enabled
    Facility: 20
    Timestamp logging: disabled
    Standby logging: enabled
    Deny Conn when Queue Full: disabled
    Console logging: disabled
    Monitor logging: disabled
    Buffer logging: disabled
    Trap logging: disabled
    History logging: disabled
    Device ID: 'inside' interface IP address "10.1.1.1"
    Mail logging: disabled
    ASDM logging: disabled
```

関連コマンド

コマンド	説明
failover	フェールオーバー機能をイネーブルにします。
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバーを定義します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging timestamp

メッセージが生成された日付と時刻をsyslogメッセージに含めることを指定するには、グローバル コンフィギュレーション モードで **logging timestamp** コマンドを使用します。日付と時刻を syslog メッセージから削除するには、このコマンドの **no** 形式を使用します。

logging timestamp [**rfc5424**]
nologgingtimestamp

構文の説明

rfc5424 （任意）syslog メッセージのすべてのタイムスタンプには、RFC 5424 形式に従って時刻が表示されます。

```
YYYY
-MM
-DD
THH:MM:SS
Z
```

YYYY は年、*MM* は月、*DD* は日付、*HHMMSS* は時間、分、および秒で示された時刻です。

コマンド デフォルト

ASA のデフォルトでは、日付と時刻は syslog メッセージに含まれません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.10(1)	**The option to enable timestamp as per RFC 5424 format was added**

使用上のガイドライン

logging timestamp コマンドを使用すると、ASA によってすべての syslog メッセージにタイムスタンプが含まれます。バージョン 9.10(1) までは、syslog のタイムスタンプは RFC 3164 に準拠しており、タイムスタンプは「MM DD YYYY HH:MM:SS」形式で表示されていました。

この形式は SIEM では優先されないため、9.10(1) では、RFC 5424 オプションが導入されました。

logging timestamp コマンドで RFC 5424 オプションを使用して、RFC 5424 に従って syslog サポート タイムゾーンを有効にします。

例

次に、すべての syslog メッセージにタイムスタンプ情報が含まれるようにする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp
ciscoasa(config)#
```

次に、すべての syslog メッセージに RFC 5424 形式のタイムスタンプ情報が含まれるようにする例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging timestamp rfc5424
ciscoasa(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

logging trap

ASA によって syslog サーバーに送信される syslog メッセージを指定するには、グローバル コンフィギュレーション モードで **logging trap** コマンドを使用します。構成からこのコマンドを削除するには、このコマンドの **no** 形式を使用します。

logging trap [*logging_list* | *level*]
nologgingtrap

構文の説明

level syslog メッセージの最大重大度を設定します。たとえば、重大度を 3 に設定すると、ASA は重大度 3、2、1、0 の syslog メッセージを生成します。次のように、数値または名前のいずれかを指定できます。

- **0** または **emergencies**：システムが使用不能。
- **1** または **alerts**：すぐに対処が必要。
- **2** または **critical**：重大な状態。
- **3** または **errors**：エラー状態。
- **4** または **warnings**：警告状態。
- **5** または **notifications**：通常の状態だが、重要な状態。
- **6** または **informational**：Informational（情報提供）メッセージ。
- **7** または **debugging**：Debug（デバッグ）メッセージ。

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカル サポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

logging_list syslog サーバーに送信するメッセージを識別するリストを指定します。リストの作成については、**logging list** コマンドを参照してください。

コマンド デフォルト

デフォルトの syslog メッセージ トラップは定義されていません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ロギング トランスポート プロトコルとして TCP を使用している場合、ASA が syslog サーバーに到達できないか、syslog サーバーが誤って設定されているか、ディスクがいっぱいになると、ASA はセキュリティ対策として新しいネットワーク アクセス セッションを拒否します。

UDP ベースのロギングでは、syslog サーバーに障害が発生しても、ASA によるトラフィックの送信は停止されません。

例

次に、重大度レベル 0、1、2、および 3 の syslog メッセージを、内部インターフェイス上に配置されていてデフォルトのプロトコルとポート番号を使用している syslog サーバに送信する例を示します。

```
ciscoasa(config)# logging enable
ciscoasa(config)# logging host inside 10.2.2.3
ciscoasa(config)# logging trap errors
ciscoasa(config)#
```

関連コマンド

コマンド	説明
logging enable	ロギングをイネーブルにします。
logging host	syslog サーバーを定義します。
logging list	メッセージ選択基準の再使用可能なリストを作成します。
show logging	イネーブルなロギング オプションを表示します。
show running-config logging	実行コンフィギュレーションのログ関連部分を表示します。

login

ローカル ユーザー データベースを使用して特権 EXEC モードにログインするか（username コマンドを参照）、ユーザー名を変更するには、ユーザー EXEC モードで **login** コマンドを使用します。

login

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ユーザーEXECモードから、**login**コマンドを使用して、ローカルデータベース内の任意のユーザー名で特権 EXEC モードにログインできます。認証をオンにした場合、**login** コマンドは **enable** コマンドと類似しています（ **aaa authentication console** コマンドを参照）。enable 認証と異なり、**login** コマンドではローカルユーザー名データベースのみを使用でき、常に認証が必要です。CLI モードから **login** コマンドを使用して、ユーザーを変更することもできます。

ユーザーがログイン時に特権EXECモード（およびすべてのコマンド）にアクセスできるようにするには、ユーザーの特権レベルを 2（デフォルト）～ 15 に設定します。ローカル コマンド認可を設定した場合、ユーザーは、その特権レベル以下のレベルに割り当てられているコマンドのみを入力できます。詳細については、**aaa authorization command** を参照してください。

注意 CLI にアクセスできるユーザーや特権 EXEC モードを開始できないようにするユーザーをローカルデータベースに追加する場合は、コマンド認可を設定する必要があります。コマンド許可がない場合、特権レベルが 2 以上（2 がデフォルト）のユーザーは、CLI で自分のパスワードを使用して特権 EXEC モード（およびすべてのコマンド）にアクセスできます。または、RADIUS または TACACS+ 認証を使用できます。あるいは、すべてのローカル ユーザーをレベル 1 に設定して、システム イネーブル パスワードを使用して特権 EXEC モードにアクセスできるユーザーを制御できます。

例

次に、**login** コマンドを入力した後のプロンプトの例を示します。

```
ciscoasa> login
Username:
```

関連コマンド

コマンド	説明
aaa authorization command	CLI アクセスのためのコマンド認可をイネーブルにします。
aaa authentication console	コンソール、Telnet、HTTP、SSH、または **enable** コマンドアクセスに対して認証を要求します。
logout	CLI からログアウトします。
username	ユーザーをローカル データベースに追加します。

login-button

WebVPN ユーザーがセキュリティアプライアンスに接続するときに表示される WebVPN ページのログインボックスの[ログイン（Login）]ボタン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 **login-button** 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、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。

login-button { **text** | **style** } *value*

[**no**] **login-button** { **text** | **style** } *value*

構文の説明

style	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 Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

コマンド デフォルト

デフォルトのログイン ボタン テキストは「Login」です。

デフォルトのログイン ボタン スタイルは、次のとおりです。

border: 1px solid black;background-color:white;font-weight:bold; font-size:80%

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（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、World Wide Web コンソーシアム（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、ログイン ボタンをテキスト「OK」でカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-button text OK
```

関連コマンド

コマンド	説明
login-title	WebVPN ページ ログイン ボックスのタイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワードをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザー名プロンプトをカスタマイズします。

login-message

WebVPN ユーザーがセキュリティアプライアンスに接続するときに表示される WebVPN ページのログインメッセージ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 **login-message** 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、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。

login-message { **text** | **style** } *value*

[**no**] **login-message** { **text** | **style** } *value*

構文の説明

text	テキストを変更することを指定します。
style	スタイル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 Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

コマンド デフォルト

デフォルトのログイン メッセージは、「Please enter your username and password」です。

デフォルトのログイン メッセージのスタイルは、background-color:#CCCCCC;color:black 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（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、World Wide Web コンソーシアム（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

次の例では、ログイン メッセージのテキストは「username and password」に設定されます。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-message text username and password
```

関連コマンド

コマンド	説明
login-title	WebVPN ページのログイン ボックスのタイトルをカスタマイズします。
username-prompt	WebVPN ページ ログインのユーザー名プロンプトをカスタマイズします。
password-prompt	WebVPN ページ ログインのパスワード プロンプトをカスタマイズします。
group-prompt	WebVPN ページ ログインのグループ プロンプトをカスタマイズします。

login-title

WebVPN ユーザーに表示される WebVPN ページのログインボックスのタイトル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 **login-title** 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、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。

login-title { **text** | **style** } *value*

[**no**] **login-title** { **text** | **style** } *value*

構文の説明

text	テキスト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。
value	実際に表示するテキスト（最大 256 文字）、または Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

コマンド デフォルト

デフォルトのログイン テキストは「Login」です。

ログイン タイトルのデフォルトの HTML スタイルは、background-color: #666666; color: white 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（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、World Wide Web コンソーシアム（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、ログイン タイトルのスタイルを設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# login-title style background-color: rgb(51,51,255);color:
 rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style: italic; font-weight:
 bold
```

関連コマンド

コマンド	説明
login-message	WebVPN ログイン ページのログイン メッセージをカスタマイズします。
username-prompt	WebVPN ログイン ページのユーザー名プロンプトをカスタマイズします。
password-prompt	WebVPN ログイン ページのパスワードプロンプトをカスタマイズします。
group-prompt	WebVPN ログイン ページのグループ プロンプトをカスタマイズします。

logo

WebVPN ユーザーがセキュリティアプライアンスに接続するときに表示される WebVPN ページのロゴをカスタマイズするには、webvpn カスタマイゼーションモードで **logo** コマンドを使用します。構成からロゴを削除してデフォルト（Cisco ロゴ）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。

logo { **none** | **file** { *path value* } }

[**no**] **logo** { **{none** | **file** { *path value* } }

構文の説明

file	ロゴを含むファイルを指定することを示します。
none	ロゴがないことを指定します。ヌル値を設定して、ロゴを拒否します。ロゴを継承しないようにします。
path	ファイル名のパス。可能なパスは、disk0:、disk1:、または flash: です。
value	ロゴのファイル名を指定します。最大長は 255 文字です（スペースを含めることはできません）。ファイル タイプは JPG、PNG、または GIF であり、100 KB 未満である必要があります。

コマンド デフォルト

デフォルトのロゴは Cisco ロゴです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

指定したファイル名が存在しない場合は、エラー メッセージが表示されます。ロゴ ファイルを削除したが、コンフィギュレーションがまだそのファイルを指している場合、ロゴは表示されません。

ファイル名にスペースを含めることはできません。

例

次の例では、ファイル cisco_logo.gif にカスタム ロゴが含まれています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)#logo file disk0:cisco_logo.gif
```

関連コマンド

コマンド	説明
title	WebVPN ページのタイトルをカスタマイズします。
page style	カスケーディング スタイル シート（CSS）パラメータを使用して WebVPN ページをカスタマイズします。

logout

CLI を終了するには、ユーザー EXEC モードで **logout** コマンドを使用します。

logout

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

logout コマンドを使用すると、ASA からログアウトできます。**exit** コマンドまたは **quit** コマンドを使用して、非特権モードに戻ることができます。

例

次に、ASA からログアウトする例を示します。

```
ciscoasa> logout
```

関連コマンド

コマンド	説明
login	ログイン プロンプトを開始します。
exit	アクセス モードを終了します。
quit	コンフィギュレーション モードまたは特権モードを終了します。

logout-message

WebVPN ユーザーが WebVPN サービスからログアウトするときに表示される WebVPN ログアウト画面のログアウトメッセージ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 **logout-message** 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、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。

logout-message { **text** | **style** } *value*

[**no**] **logout-message** { **text** | **style** } *value*

構文の説明

style	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 Cascading Style Sheet（CSS）パラメータ（最大 256 文字）です。

コマンド デフォルト

デフォルトのログアウト メッセージ テキストは「Goodbye」です。

デフォルトのログアウト メッセージのスタイルは、background-color:#999999;color:black 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（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、World Wide Web コンソーシアム（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、ログアウト メッセージのスタイルを設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# logout-message style background-color:
rgb(51,51,255);color: rgb(51,51,255); font-family: Algerian; font-size: 12pt; font-style:
 italic; font-weight: bold
```

関連コマンド

コマンド	説明
logout-title	WebVPN ページのログアウト タイトルをカスタマイズします。
group-prompt	WebVPN ページのログイン ボックスのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページのログイン ボックスのパスワードをカスタマイズします。
username-prompt	WebVPN ページのログイン ボックスのユーザー名プロンプトをカスタマイズします。

lsp-full suppress

リンクステート プロトコル データ ユニット（PDU）がフルになった場合に、抑制するルートを制御するには、ルータ ISIS コンフィギュレーション モードで **lsp-full suppress** コマンドを使用します。再配布されたルートの抑制を停止するには、このコマンドの **no** 形式を指定します。

lsp-full suppress { **external** [**interlevel**] | **interlevel** [**external**] | **none** }
nolsp-fullsuppress

構文の説明

external	この ASA 上にある再配布済みルートを抑制します。
interlevel	他のレベルからのルートを抑制します。たとえば、レベル 2 の LSP がフルになると、レベル 1 からのルートが抑制されます。
none	ルートを抑制しません。

コマンド デフォルト

再配布済みルートは抑制されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、IS-IS 隣接のステート変更のモニタリングが可能になります。これは、大規模なネットワークをモニタリングする場合に非常に役立つことがあります。メッセージは、システム エラー メッセージ機能を使用してロギングされます。メッセージは次の形式になります。

```
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Up, new adjacency
%CLNS-5-ADJCHANGE: ISIS: Adjacency to 0000.0000.0034 (Serial0) Down, hold time expired
```

例

次に、LSP がフルになった場合に、再配布ルートと別のレベルからのルートの両方が LSP によって抑制される例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-full suppress interlevel external
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。

コマンド	説明
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
pnrotocol shutdow	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

lsp-gen-interval

LSP 生成の IS-IS スロットリングをカスタマイズするには、ルータ ISIS コンフィギュレーション モードで **lsp-gen-interval** 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。

lsp-gen-interval [**level-1** | **level-2**] *lsp-max-wait* [*lsp-initial-wait lsp-second-wait*
nolsp-gen-interval

構文の説明

level-1	（オプション）レベル 1 エリアだけに間隔を適用します。
level-2	（オプション）レベル 2 エリアだけに間隔を適用します。
lsp-max-wait	2 つの LSP が連続して生成される最大間隔を示します。範囲は、1 ～ 120 秒です。
lsp-initial-wait	（オプション）初期 LSP 生成の遅延を示します。値の範囲は 1 ～ 120,000 ミリ秒です。
lsp-second-wait	（オプション）最初と 2 番めの LSP 生成間のホールド タイムを示します。値の範囲は 1 ～ 120,000 ミリ秒です。

コマンド デフォルト

lsp-max-wait：5 秒

lsp-initial-wait：50 ミリ秒

lsp-second-wait：5000 ミリ秒

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

次の説明を参照して、このコマンドのデフォルト値を変更するかどうか決定する際の参考にしてください。

- l*sp-initial-wait* 引数は、最初の LSP を生成する前の初期待機時間を表します。
- 3 番めの引数は、最初と 2 番めの LSP 生成間の待機時間を示します。
- 後続の各待機時間は、*lsp-max-wait* 時間の指定値に到達するまで、直前の間隔の 2 倍になります。したがって、初回および2回目の間隔後にLSPの生成は減速されます。最大時間に到達すると、ネットワークが安定するまで、待機時間は最大値のままとなります。
- ネットワークが安定し、*lsp-max-wait* 時間 2 回の間トリガーがなければ、高速動作（最初の待機時間）に戻ります。

例

次に、LSP 生成スロットリングの時間の間隔を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-gen-interval 2 50 100
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルなIS-ISインスタンスでは、送信される（受信ではなく）IS-ISパケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-ISプロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。

コマンド	説明
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。

コマンド	説明
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

lsp-refresh-interval

LSP の更新間隔を設定するには、ルータ ISIS コンフィギュレーション モードで **lsp-refresh-interval** コマンドを使用します。デフォルトのリフレッシュ間隔に戻すには、このコマンドの **no** 形式を使用します。

lsp-refresh-interval *seconds*
no lsp-refresh-interval

構文の説明

seconds	LSP がリフレッシュされる間隔。範囲は 1 ～ 65535 秒です。

コマンド デフォルト

デフォルト値は 900 秒（15 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

リフレッシュ間隔によって、ソフトウェアが定期的に LSP で発信元のルート トポロジ情報を送信するレートが決定されます。これは、データベース情報が古くなるのを避けるために実行されます。

（注） LSP は、ライフタイムが経過するまで定期的にリフレッシュされる必要があります。**lsp-refresh-interval** コマンドに対して設定される値は、**max-lsp-lifetime** コマンドに対して設定される値よりも小さな値である必要があり、そうでない場合、リフレッシュされる前に LSP がタイムアウトします。LSP 間隔と比べて LSP ライフタイムを大幅に少なく設定する場合、ソフトウェアが LSP リフレッシュ間隔を減らして、LSP がタイムアウトしないようにします。

例

次に、IS-IS LSP リフレッシュ間隔を 1080 秒に設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# lsp-refresh-interval 1080
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。

コマンド	説明
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

maa – match d

mac アドレス

アクティブユニットおよびスタンバイユニットの仮想 MAC アドレスを指定するには、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** コマンドを使用します。デフォルトの仮想 MAC アドレスに戻すには、このコマンドの **no** 形式を使用します。

mac address *phy_if* [*active_mac*] [*standby_mac*]
no 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 ユニットの仮想 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 ユニットの仮想 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。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- アクティブユニットのデフォルトの MAC アドレス：00a0.c9*physical_port_number*.*failover_group_id* 01
- スタンバイユニットのデフォルトの MAC アドレス：00a0.c9*physical_port_number*.*failover_group_id* 02

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

仮想 MAC アドレスがフェールオーバー グループに対して定義されていない場合は、デフォルト値が使用されます。

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。ネットワーク上で MAC アドレスが重複することを回避するには、必ず各物理インターフェイスに仮想のアクティブおよびスタンバイ MAC アドレスを割り当てます。

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

例

次の部分的な例では、フェールオーバー グループで可能な設定を示します。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover mac address	物理インターフェイスの仮想 MAC アドレスを指定します。

mac-address

プライベート MAC アドレスをインターフェイスまたはサブインターフェイスに手動で割り当てるには、インターフェイス コンフィギュレーション モードで **mac-address** コマンドを使用します。マルチ コンテキスト モードでは、このコマンドは各コンテキストでそれぞれ別の MAC アドレスをインターフェイスに割り当てることができます。クラスタの個々のインターフェイスに、MAC アドレスのクラスタ プールを割り当てることができます。MAC アドレスをデフォルトに戻すには、このコマンドの **no** 形式を使用します。

mac-address { *mac_address* [**standby** *mac_address* | **site-id** *number* [**site-ip ip_address**]] | **cluster-pool** *pool_name* }
no mac-address { *mac_address* [**standby** *mac_address* | **site-id** *number* [**site-ip ip_address**]] | **cluster-pool** *pool_name* }

構文の説明

cluster-pool *pool_name*	個別インターフェイスモードのクラスタ（**cluster interface-mode** コマンドを参照）、または任意のクラスタインターフェイスモードの管理インターフェイスについて、各クラスタメンバーの特定のインターフェイスに使用する MAC アドレスのプールを設定します。プールは **mac-address pool** コマンドを使用して定義します。
mac_address	このインターフェイスの MAC アドレスを H.H.H 形式で設定します。H は 16 ビットの 16 進数です。たとえば、MAC アドレスが 00-0C-F1-42-4C-DE の場合、000C.F142.4CDE と入力します。フェールオーバーを使用する場合は、この MAC アドレスがアクティブな MAC アドレスとなります。 （注） 自動生成されたアドレス（**mac-address auto** コマンドを使用）は A2 で始まるため、自動生成も使用する場合、手動 MAC アドレスを A2 で始めることはできません。
site-id *number*	（任意、ルーテッドモードのみ）サイト間クラスタリングの場合、各サイトのサイト固有 MAC アドレスを設定します。
site-ip *ip_address*	（任意、ルーテッドモードのみ）サイト間クラスタリングの場合、各サイトのサイト固有 IP アドレスを設定します。この IP アドレスはグローバル IP アドレスと同じサブネット内になければなりません。
standby *mac_address*	（任意）フェールオーバーのスタンバイ MAC アドレスを設定します。アクティブ装置がフェールオーバーし、スタンバイ装置がアクティブになると、新しいアクティブ装置はアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。一方、古いアクティブ装置はスタンバイ アドレスを使用します。

コマンド デフォルト

デフォルトの MAC アドレスは、物理インターフェイスのバーンドイン MAC アドレスです。サブインターフェイスは、物理インターフェイスの MAC アドレスを継承します。一部のコマンド（シングル モードでのこのコマンドを含む）は物理インターフェイスの MAC アドレスを設定するため、継承されるアドレスはその設定によって異なります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(5)/8.2(2)	**mac-address auto** コマンドとともに使用する場合、MAC アドレスを開始する A2 の使用が制限されました。
9.0(1)	クラスタリングをサポートするために、**cluster-pool** キーワードが追加されました。
9.5(1)	**site-id** キーワードが追加されました。
9.6(1)	**site-ip** キーワードが追加されました。

使用上のガイドライン

マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有している場合、固有の MAC アドレスをそれぞれのコンテキストのインターフェイスに割り当てることができます。この機能を使用すると、ASA はパケットを適切なコンテキストに簡単に分類できます。固有の MAC アドレスを持たない共有インターフェイスも使用できますが、その場合制限があります。詳細については、CLI コンフィギュレーション ガイドを参照してください。

このコマンドで各 MAC アドレスを手動で割り当てることができます。または、**mac-address auto** コマンドを使用して、コンテキストで共有インターフェイスの MAC アドレスを自動的に生成できます。MAC アドレスを自動的に生成する場合、 **mac-address** コマンドを使用して、生成されたアドレスを上書きできます。

シングル コンテキスト モード、またはマルチ コンテキスト モードで共有されないインターフェイスの場合は、固有の MAC アドレスをサブインターフェイスに割り当てることを推奨します。たとえば、サービス プロバイダーによっては、MAC アドレスに基づいてアクセス コントロールを実行する場合があります。

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

クラスタリングの場合は、スパンド EtherChannel のグローバル MAC アドレスを設定する必要があります。MACアドレスが手動設定されている場合、そのMACアドレスは現在のマスターユニットに留まります。マルチ コンテキスト モードでは、コンテキスト間でインターフェイスを共有した場合、MAC アドレスの自動生成をイネーブルにする必要があります。非共有インターフェイスについては MAC アドレスを手動で設定する必要があることに注意してください。

ルーテッドモードのサイト間クラスタリングの場合は、各サイトのマスターユニットでサイト固有の MAC アドレスと IP アドレスを設定してから、各ユニットで **site-id** コマンドを使用してアドレスをサイトに割り当てます。

例

次に、GigabitEthernet 0/1.1 の MAC アドレスを設定する例を示します。

```
ciscoasa/contextA(config)# interface gigabitethernet0/1.1
ciscoasa/contextA(config-if)# nameif inside
ciscoasa/contextA(config-if)# security-level 100
ciscoasa/contextA(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa/contextA(config-if)# mac-address 030C.F142.4CDE standby 040C.F142.4CDE
ciscoasa/contextA(config-if)# no shutdown
```

次に、スパンド EtherChannel ポートチャネル 1 のサイト固有 MAC アドレスを設定する例を示します。

```
ciscoasa(config-if)# interface port-channel 1
ciscoasa(config-if)# port-channel span-cluster
ciscoasa(config-if)# mac-address aaaa.1111.1234
ciscoasa(config-if)# mac-address aaaa.1111.aaaa site-id 1 site-ip 10.7.7.1
ciscoasa(config-if)# mac-address aaaa.1111.bbbb site-id 2 site-ip 10.7.7.2
ciscoasa(config-if)# mac-address aaaa.1111.cccc site-id 3 site-ip 10.7.7.3
ciscoasa(config-if)# mac-address aaaa.1111.dddd site-id 4 site-ip 10.7.7.4
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address auto	マルチ コンテキスト モードでの共有インターフェイスの MAC アドレス（アクティブおよびスタンバイ）を自動生成します。
mode	セキュリティ コンテキスト モードをマルチまたはシングルに設定します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

mac-address auto

プライベート MAC アドレスを各共有コンテキスト インターフェイスに自動的に割り当てるには、グローバル コンフィギュレーション モードで **mac-address auto** コマンドを使用します。自動 MAC アドレスを無効にするには、このコマンドの **no** 形式を使用します。

mac-address auto [**prefix** *prefix*]
no mac-address auto

構文の説明

prefix *prefix*	（オプション）MAC アドレスの一部として使用するユーザー定義のプレフィックスを設定します。*prefix* は、0 ～ 65535 の 10 進数です。プレフィックスを入力しない場合、ASA によりデフォルトのプレフィックスが生成されます。 このプレフィックスは、4 桁の 16 進数値に変換されます。プレフィックスにより、各 ASA は固有の MAC アドレスを使用（異なるプレフィックスの値を使用）するため、1 つのネットワークセグメントに複数の ASA を配置したりできます。

コマンド デフォルト

自動 MACアドレス 生成はデフォルトでディスエーブルになっています（デフォルトでイネーブルになっている ASASM の場合を除く）。イネーブルにすると、ASA は、インターフェイス（ASA 5500-X）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。必要に応じて、プレフィックスをカスタマイズできます。

MAC アドレスの生成をディセーブルにした場合は、デフォルトの MAC アドレスは次のようになります。

- ASA 5500-X シリーズアプライアンスの場合：物理インターフェイスはバーンドイン MAC アドレスを使用し、1 つの物理インターフェイスのすべてのサブインターフェイスは同じバーンドイン MAC アドレスを使用します。
- ASASM の場合：すべての VLAN インターフェイスが同じ MAC アドレスを使用します。これは、バックプレーンの MAC アドレスから導出されたものです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(5)/8.2(2)	**prefix** キーワードが追加されました。プレフィックスを使用し、固定の開始値（A2）を使用し、フェールオーバー ペアのプライマリ ユニットおよびセカンダリ ユニットの MAC アドレスで別の方式を使用するように、MAC アドレス形式が変更されました。MACアドレスはリロード後も維持されるようになりました。コマンドパーサーは現在、自動生成がイネーブルになっているかどうかをチェックします。MACアドレスを手動でも割り当てることができるようにする場合は、A2 を含む手動 MAC アドレスは開始できません。
8.5(1)	ASASM の場合にのみ自動生成がデフォルトで有効になる（**mac-address auto**）ようになりました。
8.6(1)	現在、ASA はデフォルトのプレフィックスを使用するように MAC アドレスの自動生成設定を変換します。ASA は、インターフェイス（ASA 5500）またはバックプレーン（ASASM）の MAC アドレスの最後の 2 バイトに基づいてプレフィックスを自動生成します。この変換は、リロード時または MAC アドレス生成を再度イネーブルにすると、自動的に行われます。MAC アドレス生成の従来の方法は使用できなくなります。 （注） フェールオーバーペアのヒットレスアップグレードを維持するため、ASA は、フェールオーバーが有効である場合、既存のコンフィギュレーションの MAC アドレス メソッドをリロード時に変換しません。

使用上のガイドライン

インターフェイスを共有するコンテキストを許可するには、固有の MAC アドレスを各共有コンテキスト インターフェイスに割り当てることを推奨します。MAC アドレスは、コンテキスト内でパケットを分類するために使用されます。インターフェイスを共有するものの、各コンテキストにインターフェイスの固有の MAC アドレスがない場合は、宛先 IP アドレスがパケットの分類に使用されます。宛先アドレスは、コンテキスト NAT コンフィギュレーションと照合されます。この方法には、MACアドレスの方法に比べるといくつか制限があります。パケットの分類の詳細については、CLI 設定ガイドを参照してください。

生成した MAC アドレスがネットワーク内の別のプライベート MAC アドレスと競合することがまれにあります。この場合は、コンテキスト内のインターフェイスの MAC アドレスを手動で設定できます。MACアドレスの手動設定の詳細については、**mac-address** コマンドを参照してください。

手動 MAC アドレスとの通信

MAC アドレスを手動で割り当てた場合、自動生成がイネーブルになっていても、手動で割り当てた MAC アドレスが使用されます。後で手動 MAC アドレスを削除すると、自動生成されたアドレスが使用されます。

自動生成されたアドレスは A2 で始まるため、手動 MAC アドレスを A2 で始めることはできません。たとえ自動生成も使用する予定であってもそれは同じです。

フェールオーバー用の MAC アドレス

フェールオーバーで使用できるように、ASA はインターフェイスごとにアクティブとスタンバイの両方の MAC アドレスを生成します。アクティブ ユニットがフェールオーバーしてスタンバイ ユニットがアクティブになると、その新規アクティブ ユニットがアクティブな MAC アドレスの使用を開始して、ネットワークの切断を最小限に抑えます。詳細については、<xref> を参照してください。

prefix キーワードが追加される前に従来のバージョンの **mac-address auto** コマンドを使用してフェールオーバーユニットをアップグレードする場合は、<xref> を参照してください。

プレフィックスを使用する場合の MAC アドレス形式

ASA は、次の形式を使用して MAC アドレスを生成します。

A2*xx.yyzz.zzzz*

xx.yy はユーザー定義プレフィックスまたはインターフェイス（ASA 5500）またはバックプレーン（ASASM）MAC アドレスの最後の 2 バイトに基づいて自動生成されたプレフィックスで、*zz.zzzz* は ASA によって生成される内部カウンタです。スタンバイ MAC アドレスの場合、内部カウンタが 1 増えることを除けばアドレスは同じです。

プレフィックスの使用方法を示す例の場合、プレフィックス 77 を設定すると、ASA は 77 を 16 進数値 004D（*yyxx*）に変換します。MAC アドレスで使用すると、プレフィックスは ASA ネイティブ形式に一致するように反転されます（*xxyy*）。

A2**4D.00***zz.zzzz*

プレフィックス 1009（03F1）の場合、MAC アドレスは次のようになります。

A2**F1.03***zz.zzzz*

プレフィックスを使用しない場合の MAC アドレス形式（従来の方法）

この方法は、フェールオーバーを使用しており、バージョン 8.6 以降にアップグレードした場合に使用できます。この場合、プレフィックス方式を手動でイネーブルにする必要があります。

プレフィックスを指定しないと、MAC アドレスは次の形式で生成されます。

- アクティブユニットの MAC アドレス：12*_slot.port_subid.contextid*。
- スタンバイユニットの MAC アドレス：02*_slot.port_subid.contextid*。

インターフェイス スロットがないプラットフォームの場合、スロットは常に 0 です。*port* はインターフェイス ポートです。*subid* は、表示不可能なサブインターフェイスの内部 ID です。*contextid* は、**show context detail** コマンドで表示可能なコンテキストの内部 ID です。たとえば、ID 1 のコンテキスト内のインターフェイス GigabitEthernet 0/1.200 には、次の生成済み MAC アドレスがあります。サブインターフェイス 200 の内部 ID は 31 です。

- アクティブ：1200.0131.0001
- スタンバイ：0200.0131.0001

この MAC アドレス生成方法では、リロード間で MAC アドレスが持続されず、同じネットワークセグメントに複数の ASA を配置できず（固有の MAC アドレスが保証されないため）、手

動で割り当てた MAC アドレスとの MAC アドレスの重複が回避されません。これらの問題を回避するため、プレフィックスを使用して MAC アドレスを生成することをお勧めします。

MAC アドレスが生成される場合

コンテキストでインターフェイスの **nameif** コマンドを設定すると、新しい MAC アドレスがただちに生成されます。コンテキストインターフェイスを設定した後でこのコマンドをイネーブルにした場合、コマンドを入力するとただちにすべてのインターフェイスの MAC アドレスが生成されます。**no mac-address auto** コマンドを使用すると、各インターフェイスの MAC アドレスはデフォルトの MAC アドレスに戻ります。たとえば、GigabitEthernet 0/1 のサブインターフェイスは GigabitEthernet 0/1 の MAC アドレスを使用するようになります。

他の方法を使用した MAC アドレスの設定

他のコマンドまたは方法を使用して MAC アドレスを設定することもできますが、1 つの方法だけを使用することを推奨します。複数の方法を使用して MAC アドレスを設定した場合は、どの MAC アドレスが使用されるかは多くの可変要素によって決まるため、予測できないことがあります。

システム構成での MAC アドレスの表示

割り当てられた MAC アドレスをシステム実行スペースから表示するには、**show running-config all context** コマンドを入力します。

割り当てられた MAC アドレスを表示するには、**all** オプションを指定する必要があります。このコマンドはグローバル コンフィギュレーション モードでのみユーザーによる設定が可能ですが、**mac-address auto** コマンドは割り当てられた MAC アドレスとともに各コンテキストの構成に読み取り専用エントリとして表示されます。コンテキスト内で **nameif** コマンドで設定される割り当て済みのインターフェイスだけに MAC アドレスが割り当てられます。

（注） MAC アドレスをインターフェイスに手動で割り当てるものの、その際に自動生成がイネーブルになっていると、手動 MAC アドレスが使用中のアドレスとなりますが、コンフィギュレーションには自動生成されたアドレスが引き続き表示されます。後で手動 MAC アドレスを削除すると、表示されている自動生成アドレスが使用されます。

コンテキスト内の MAC アドレスの表示

コンテキスト内で各インターフェイスによって使用されている MAC アドレスを表示するには、**show interface | include (Interface)|(MAC)** コマンドを入力します。

（注） **show interface** コマンドは、使用中の MAC アドレスを表示します。MAC アドレスを手動で割り当て、自動生成も有効にしている場合、システム構成内にある未使用の自動生成アドレスのみを表示できます。

例

次に、プレフィックス 78 で自動 MAC アドレス生成をイネーブルにする例を示します。

```
ciscoasa(config)# mac-address auto prefix 78
```

show running-config all context admin コマンドからの次の出力には、Management0/0 インターフェイスに割り当てられたプライマリおよびスタンバイ MAC アドレスが表示されます。

```
ciscoasa# show running-config all context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a24d.0000.1440 a24d.0000.1441
  config-url disk0:/admin.cfg
```

show running-config all context コマンドからの次の出力には、すべてのコンテキストインターフェイスに関するすべての MAC アドレス（プライマリおよびスタンバイ）が表示されます。GigabitEthernet0/0 と GigabitEthernet0/1 の各メインインターフェイスは、**nameif** コマンドを使用してコンテキスト内部で設定されないため、各インターフェイスの MAC アドレスは生成されていないことに注意してください。

```
ciscoasa# show running-config all context
admin-context admin
context admin
  allocate-interface Management0/0
  mac-address auto Management0/0 a2d2.0400.125a a2d2.0400.125b
  config-url disk0:/admin.cfg
!
context CTX1
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11bc a2d2.0400.11bd
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11c0 a2d2.0400.11c1
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c4 a2d2.0400.11c5
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c8 a2d2.0400.11c9
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11cc a2d2.0400.11cd
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120c a2d2.0400.120d
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.1210 a2d2.0400.1211
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1214 a2d2.0400.1215
  config-url disk0:/CTX1.cfg
!
context CTX2
  allocate-interface GigabitEthernet0/0
  allocate-interface GigabitEthernet0/0.1-GigabitEthernet0/0.5
  mac-address auto GigabitEthernet0/0.1 a2d2.0400.11ba a2d2.0400.11bb
  mac-address auto GigabitEthernet0/0.2 a2d2.0400.11be a2d2.0400.11bf
  mac-address auto GigabitEthernet0/0.3 a2d2.0400.11c2 a2d2.0400.11c3
  mac-address auto GigabitEthernet0/0.4 a2d2.0400.11c6 a2d2.0400.11c7
  mac-address auto GigabitEthernet0/0.5 a2d2.0400.11ca a2d2.0400.11cb
  allocate-interface GigabitEthernet0/1
  allocate-interface GigabitEthernet0/1.1-GigabitEthernet0/1.3
  mac-address auto GigabitEthernet0/1.1 a2d2.0400.120a a2d2.0400.120b
  mac-address auto GigabitEthernet0/1.2 a2d2.0400.120e a2d2.0400.120f
  mac-address auto GigabitEthernet0/1.3 a2d2.0400.1212 a2d2.0400.1213
  config-url disk0:/CTX2.cfg
!
```

関連コマンド

コマンド	説明
failover mac address	Active/Standby フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac address	Active/Active フェールオーバーの物理インターフェイスに対して、アクティブ MAC アドレスとスタンバイ MAC アドレスを設定します。
mac-address	物理インターフェイスまたはサブインターフェイスの MAC アドレス（アクティブとスタンバイ）を手動で設定します。マルチ コンテキスト モードでは、同じインターフェイスに対して、コンテキストごとにそれぞれ別の MAC アドレスを設定することができます。
mode	セキュリティ コンテキスト モードをマルチまたはシングルに設定します。
show interface	MAC アドレスを含む、インターフェイスの特性を表示します。

mac-address pool

ASA クラスタの個々のインターフェイスで使用する MAC アドレスプールを追加するには、グローバル コンフィギュレーション モードで **mac-address pool** コマンドを使用します。未使用のプールを削除するには、このコマンドの **no** 形式を使用します。

mac-address pool *name start_mac_address - end_mac_address*
no mac-address pool *name* [*start_mac_address - end_mac_address*]

構文の説明

name	プールの名前を 63 文字以内で指定します。
start_mac_address - end_mac_address	最初の MAC アドレスと最後の MAC アドレスを指定します。ダッシュ（-）の前後にスペースが必要です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このプールは、インターフェイス コンフィギュレーション モードの **mac-address cluster-pool** コマンドで使用できます。インターフェイスに MAC アドレスを手動で設定することはあまりありませんが、そのような場合には、このプールを使用して各インターフェイスに一義的な MAC アドレスを割り当てます。

例

次に、8 個の MAC アドレスを含む MAC アドレス プールを追加し、GigabitEthernet 0/0 インターフェイスに割り当てる例を示します。

```
ciscoasa(config)# mac-address pool pool1 000C.F142.4CD1 - 000C.F142.4CD7
ciscoasa(config)# interface gigabitethernet 0/0
ciscoasa(config-ifc)# mac-address cluster-pool pool1
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定します。
mac-address	インターフェイスのMACアドレスを設定します。

mac-address-table aging-time

MAC アドレステーブルエントリのタイムアウトを設定するには、グローバル コンフィギュレーション モードで **mac-address-table aging-time** コマンドを使用します。デフォルト値の 5 分に戻すには、このコマンドの **no** 形式を使用します。

mac-address-tableaging-time*timeout_value*
no mac-address-table aging-time

構文の説明

timeout_value	タイムアウトするまで MAC アドレス エントリが MAC アドレス テーブルにとどまることができる時間。有効な値は、5 ～ 720 分（12 時間）です。5 分がデフォルトです。

コマンド デフォルト

デフォルトのタイムアウトは 5 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードでこのコマンドを設定できるようになりました。

使用上のガイドライン

使用方法のガイドラインはありません。

例

次に、MAC アドレスのタイムアウトを 10 分に設定する例を示します。

```
ciscoasa(config)# mac-address-timeout aging time 10
```

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。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
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 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。

mac-address-table static

スタティック ARP エントリを ARP テーブルに追加するには、グローバル コンフィギュレーション モードで **mac-address-table static** コマンドを使用します。スタティックエントリを削除するには、このコマンドの **no** 形式を使用します。通常、MAC アドレスは、特定の MAC アドレスからのトラフィックがインターフェイスに入ったときに、MAC アドレス テーブルに動的に追加されます。スタティック MAC アドレスは、必要に応じて MAC アドレス テーブルに追加できます。スタティック エントリを追加する利点の 1 つに、MAC スプーフィングに対処できることがあります。スタティックエントリと同じ MAC アドレスを持つクライアントが、そのスタティックエントリに一致しないインターフェイスにトラフィックを送信しようとすると、ASA はトラフィックをドロップし、システムメッセージを生成します。

mac-address-table static *interface_name mac_address*
no mac-address-table static *interface_name mac_address*

構文の説明

interface_name	送信元のブリッジ グループ メンバー インターフェイス。
mac_address	テーブルに追加する MAC アドレス。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードでこのコマンドを設定できるようになりました。

例

次に、スタティック MAC アドレスのエントリを MAC アドレス テーブルに追加する例を示します。

```
ciscoasa(config)# mac-address-table static inside 0010.7cbe.6101
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
firewall transparent	ファイアウォール モードをトランスペアレントに設定します。
mac-address-table aging-time	ダイナミック MAC アドレス エントリのタイムアウトを設定します。
mac-learn	MAC アドレス ラーニングをディセーブルにします。
show mac-address-table	MAC アドレス テーブルのエントリを表示します。

mac-learn disable

インターフェイスの MAC アドレスラーニングを無効にするには、グローバル コンフィギュレーション モードで **mac-learn** コマンドを使用します。MAC アドレスラーニングを再び有効にするには、このコマンドの **no** 形式を使用します。デフォルトで、各インターフェイスは着信トラフィックの MAC アドレスを自動的に学習し、ASA は対応するエントリを MAC アドレス テーブルに追加します。必要に応じて MAC アドレス ラーニングをディセーブルにできます。

mac-learn*interface_name***disable**
no mac-learn *interface_name* **disable**

構文の説明

interface_name	MAC 学習をディセーブルにするブリッジ グループ メンバー インターフェイス。
disable	MAC 学習をディセーブルにします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	Integrated Routing and Bridging（IRB; 統合ルーティングおよびブリッジング）を使用するときに、ルーテッド モードでこのコマンドを設定できるようになりました。

例

次に、外部インターフェイスでの MAC アドレス学習をディセーブルにする例を示します。

```
ciscoasa(config)# mac-learn outside disable
```

関連コマンド

コマンド	説明
clear configure mac-learn	**mac-learn** 構成をデフォルトに設定します。
firewall transparent	ファイアウォールモードをトランスペアレントに設定します。
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。
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。
show running-config mac-learn	**mac-learn** の設定を表示します。

mac-learn flood

非 IPv4/IPv6 パケットの不明な MAC アドレスのフラッディングを有効にするには、グローバル コンフィギュレーション モードで **mac-learn flood** コマンドを使用します。 MAC アドレスのフラッディングを無効にするには、このコマンドの **no** 形式を使用します。

mac-learn flood
no mac-learn flood

コマンド デフォルト

フラッディング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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

例

次に、MAC フラッディングを有効にする例を示します。

```
ciscoasa(config)# mac-learn flood
```

関連コマンド

コマンド	説明
clear configure mac-learn	**mac-learn** 構成をデフォルトに設定します。
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。
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。
show running-config mac-learn	**mac-learn** の設定を表示します。

mac-list

認証や許可から MAC アドレスを免除するために使用される MAC アドレスのリストを指定するには、グローバル コンフィギュレーション モードで **mac-list** コマンドを使用します。MAC アドレスリストのエントリを削除するには、このコマンドの **no** 形式を使用します。

mac-list *id* { **deny** | **permit** } *mac macmask*
no mac-list *id* { **deny** | **permit** } *mac macmask*

構文の説明

deny	この MAC アドレスに一致するトラフィックは MAC アドレスリストと照合せず、**aaa mac-exempt** コマンドに指定されているときには認証と許可の両方の対象となることを示します。ffff.ffff.0000 などの MAC アドレス マスクを使用して、ある範囲の MAC アドレスを許可し、その範囲の MAC アドレスを強制的に認証および許可する場合には、MACアドレス リストに拒否エントリを追加することが必要になる場合があります。
id	MAC アクセス リストの 16 進数値を指定します。一連の MAC アドレスをグループ化するには、同じ ID 値で必要な回数 **mac-list** コマンドを入力します。パケットが最適に一致するエントリではなく最初に一致するエントリを使用するため、エントリの順序が重要になります。 許可エントリがあり、その許可エントリで許可されているアドレスを拒否する場合は、許可エントリよりも前に拒否エントリを入力してください。
mac	送信元 MAC アドレスを 12 桁の 16 進数形式、つまり、nnnn.nnnn.nnnn で指定します。
macmask	MAC アドレスのどの部分を照合に使用するかを指定します。たとえば、ffff.ffff.ffff は MAC アドレスと完全に一致し、ffff.ffff.0000 は 最初の 8 桁のみと一致します。
permit	このMACアドレスに一致するトラフィックはMACアドレスリストと照合せず、**aaa mac-exempt** コマンドに指定されているときには認証と許可の両方から免除されることを示します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

認証および許可からの MAC アドレスの免除を有効にするには、**aaa mac-exempt** コマンドを使用します。 **aaa mac-exempt** コマンドの 1 インスタンスのみを追加できるため、免除するすべての MAC アドレスが MAC アドレスリストに含まれるようにしてください。複数の MAC リストを作成できますが、一度に使用できるのは 1 つだけです。

例

次の例では、1 個の MAC アドレスに対する認証をバイパスします。

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

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

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

次の例では、00a0.c95d.02b2 以外の MAC アドレス グループの認証をバイパスします。00a0.c95d.02b2 は許可ステートメントにも一致するため、許可ステートメントよりも前に拒否ステートメントを入力します。許可ステートメントが前にある場合、拒否ステートメントには一致しません。

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

関連コマンド

コマンド	説明
aaa authentication	ユーザー認証をイネーブルにします。
aaa authorization	ユーザー認可サービスをイネーブルにします。
aaa mac-exempt	MAC アドレスのリストを認証と認可の対象から免除します。
clear configure mac-list	**mac-list** コマンドで指定されている MAC アドレスのリストを削除します。
show running-config mac-list	**mac-list** コマンドで以前指定された MAC アドレスのリストを表示します。

mail-relay

ローカルドメイン名を設定するには、パラメータ コンフィギュレーション モードで **mail-relay** 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。

mail-relay domain_name action { **drop-connection** | **log** }
no mail-relay domain_name action { **drop-connection** | **log** }

構文の説明

domain_name	ドメイン名を指定します。
drop-connection	接続を閉じます。
ログ	システム ログ メッセージを生成します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、特定のドメインへのメール中継を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mail-relay mail action drop-connection
```

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。

コマンド	説明
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。

management-access

VPN の使用時に ASA への通過ルートとなるインターフェイス以外のインターフェイスへの管理アクセスを許可するには、グローバル コンフィギュレーション モードで **management-access** コマンドを使用します。管理アクセスを無効にするには、このコマンドの **no** 形式を使用します。

management-access*mgmt_if*
no management-access *mgmt_if*

構文の説明

mgmt_if 別のインターフェイスから ASA に入るときにアクセスする管理インターフェイスの名前を指定します。物理または仮想インターフェイスを指定できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.9.(2)	仮想インターフェイスが指定可能になりました。
9.14(1)	SNMP のサポートは終了しました。
9.17(1)	CiscoSSH スタックを使用する場合（**ssh stack ciscossh** コマンド）、この機能は SSH ではサポートされません。

使用上のガイドライン

このコマンドを使用すると、フルトンネル IPsec VPN または SSL VPN クライアント（AnyConnect 2.x クライアント、SVC 1.x）を使用するときや、サイトツーサイト IPsec トンネルを横断するときには、ASA への通過ルートとなるインターフェイス以外のインターフェイスに接続できます。ASA インターフェイスへの接続には Telnet、SSH、Ping、または ASDM を使用できます。また、VPN トンネル経由で送信される syslog メッセージの送信元インターフェイスとして、管理アクセスインターフェイスを使用できます。

管理アクセス インターフェイスは 1 つだけ定義できます。

9.5(1) 以降、別個の管理/データ ルーティング テーブルでのルーティングを考慮すると、VPN の端末インターフェイスと管理アクセスインターフェイスは同じ種類である（つまり両方とも管理専用インターフェイスであるか、通常のデータ インターフェイスである）必要があります。したがって、稀に VPN 端末インターフェイスが管理専用である場合を除き、管理専用インターフェイス上には管理アクセスを設定しないでください。

CiscoSSH スタックを使用する場合（**ssh stack ciscossh** コマンド）、この機能は SSH ではサポートされません。

この機能は、9.14(1) 以降の SNMP ではサポートされていません。 VPN 経由の SNMP の場合、9.18(2) 以降のループバック インターフェイスで SNMP を有効にすることを推奨します。ループバック インターフェイスで SNMP を使用するために、管理アクセス機能を有効にする必要はありません。ループバックは SSH でも機能します。

管理アクセスインターフェイスと VPN ネットワークの間でアイデンティティ NAT を使用する場合（VPN トラフィックに共通の NAT 構成を使用する場合）、**nat** コマンドの **route-lookup** キーワードを指定する必要があります。ルートルックアップがない場合、ASA は、ルーティングテーブルの内容に関係なく、**nat** コマンドで指定されたインターフェイスからトラフィックを送信します。たとえば、**management-access inside** を設定すると、VPN ユーザーが外部から内部インターフェイスを管理できます。アイデンティティ **nat** コマンドで **(inside,outside)** を指定した場合、ASA では管理トラフィックが内部ネットワークに送信されず、内部インターフェイスの IP アドレスには戻りません。ルートルックアップ オプションを使用すると、ASA は、内部ネットワークの代わりに内部インターフェイスの IP アドレスに直接トラフィックを送信できます。VPN クライアントから内部ネットワーク上のホストへのトラフィックの場合、ルートルックアップ オプションがあっても正しい出力インターフェイス（内部）になるため、通常のトラフィック フローは影響を受けません。

例

次に、ファイアウォール インターフェイスを管理アクセス インターフェイスとして inside という名前で設定する例を示します。

```
ciscoasa(config)# management-access inside
```

関連コマンド

コマンド	説明
clear configure management-access	ASA の管理アクセスのための、内部インターフェイスのコンフィギュレーションを削除します。
show management-access	管理アクセスのために設定された内部インターフェイスの名前を表示します。

management-only

管理トラフィックのみを受け付けるようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **management-only** コマンドを使用します。通過トラフィックを許可するには、このコマンドの **no** 形式を使用します。

management-only [**individual**]
no management-only [**individual**]

構文の説明

individual Firepower 9300 ASA セキュリティ モジュール クラスタの場合は、スパンド インターフェイス モードのときに管理インターフェイスに **individual** キーワードを指定する必要があります。

コマンド デフォルト

Management *n*/*n* インターフェイス（使用しているモデルで使用可能な場合）は、デフォルトで管理専用モードに設定されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ASA クラスタリングをサポートするために、管理インターフェイスの例外として、このコマンドが実行コンフィギュレーションからインターフェイス セクションの先頭に移動されました。
9.4(1.152)	**individual** キーワードが追加されました。

使用上のガイドライン

ほとんどのモデルには、Management *n* /*n* という専用の管理インターフェイスが含まれ、ASA へのトラフィックをサポートするようになっています。ただし、**management-only** コマンドを使用することで、任意のインターフェイスを管理専用インターフェイスとして設定できます。

（注） ASA 5585-X を除くすべてのモデルでは、管理インターフェイスの管理専用モードをディセーブルにすることはできません。このコマンドはデフォルトで常にイネーブルになります。

トランスペアレントファイアウォールモードでは、許可される最大通過トラフィックインターフェイスに加えて、管理インターフェイス（物理インターフェイス、サブインターフェイス（使用しているモデルでサポートされている場合）、管理インターフェイスからなるEtherChannelインターフェイス（複数の管理インターフェイスがある場合）のいずれか）を個別の管理インターフェイスとして使用できます。他のインターフェイスタイプは管理インターフェイスとして使用できません。

使用しているモデルに管理インターフェイスが含まれていない場合は、データインターフェイスからトランスペアレント ファイアウォールを管理する必要があります。

マルチ コンテキスト モードでは、どのインターフェイスも（これには管理インターフェイスも含まれます）、コンテキスト間で共有させることはできません。コンテキスト単位で管理を行うには、管理インターフェイスのサブインターフェイスを作成し、管理サブインターフェイスを各コンテキストに割り当てます。ASA 5585-X 以外では、管理インターフェイスがサブインターフェイスを許可しないため、コンテキスト単位で管理を行うにはデータインターフェイスに接続する必要があることに注意してください。

管理インターフェイスは、通常のブリッジ グループの一部ではありません。動作上の目的から、設定できないブリッジ グループの一部です。

例

次に、管理インターフェイスで管理専用モードをディセーブルにする例を示します。

```
ciscoasa(config)# interface management0/0
ciscoasa(config-if)# no management-only
```

次に、サブインターフェイスで管理専用モードをイネーブルにする例を示します。

```
ciscoasa(config)# interface gigabitethernet0/2.1
ciscoasa(config-subif)# management-only
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、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。

map-domain

マッピングアドレスとポート（MAP）ドメインを設定するには、グローバル コンフィギュレーション モードで **map-domain** コマンドを使用します。MAP ドメインを削除するには、このコマンドの **no** 形式を使用します。

map-domain*name*
no map-domain *name*

構文の説明

name MAP ドメインの名前は、英数字で最大 48 文字です。また、名前には、ピリオド（.）、スラッシュ（/）、およびコロン（:）の特殊文字を含めることもできます。

コマンド デフォルト

デフォルト設定はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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 モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.13(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

アドレスとポートのマッピング (MAP) は、主にサービスプロバイダー (SP) ネットワークで使用する機能です。サービス プロバイダーは、IPv6 専用ネットワーク、MAP ドメインを稼働でき、同時に、IPv4 専用のサブスクライバをサポートし、パブリック インターネット上の IPv4 専用サイトとの通信ニーズに対応します。MAP は、RFC7597、RFC7598、および RFC7599 で定義されています。

MAP ドメイン内のサービスプロバイダーの場合、NAT46 を介した MAP の利点は、サブスクライバの IPv4 アドレスに対する IPv6 アドレスの代替（および SP ネットワークエッジでの IPv4 への変換）がステートレスであることです。これにより、NAT46 と比較して SP ネットワーク内の効率が向上します。

MAP 変換（MAP-T）と MAP カプセル化（MAP-E）という 2 つのマップ技術があります。ASA は MAP-T をサポートしています。MAP-E はサポートされていません。

MAP-T を設定するには、1 つまたは複数のドメインを作成します。カスタマーエッジ（CE）およびボーダーリレー（BR）デバイスで MAP-T を設定する場合は、各ドメインに参加するデバイスごとに同じパラメータを使用するようにしてください。

最大 25 個の MAP-T ドメインを設定できます。マルチコンテキストモードでは、コンテキストごとに最大 25 のドメインを設定できます。

例

次の例では、1 という名前の MAP-T ドメインを作成して、ドメインの変換ルールを設定しています。

```
ciscoasa(config)# map-domain 1
ciscoasa(config-map-domain)# default-mapping-rule 2001:DB8:CAFE:CAFE::/64
ciscoasa(config-map-domain)# basic-mapping-rule
ciscoasa(config-map-domain-bmr)# ipv4-prefix 192.168.3.0 255.255.255.0
ciscoasa(config-map-domain-bmr)# ipv6-prefix 2001:cafe:cafe:1::/64
ciscoasa(config-map-domain-bmr)# start-port 1024
ciscoasa(config-map-domain-bmr)# share-ratio 16
```

関連コマンド

コマンド	説明
basic-mapping-rule	MAP ドメインの基本マッピング ルールを設定します。
default-mapping-rule	MAP ドメインのデフォルト マッピング ルールを設定します。
ipv4-prefix	MAP ドメインの基本マッピング ルールの IPv4 プレフィックスを設定します。
ipv6-prefix	MAP ドメインの基本マッピング ルールの IPv6 プレフィックスを設定します。
map-domain	マッピング アドレスおよびポート（MAP）ドメインを設定します。
share-ratio	MAP ドメインの基本マッピング ルールのポート数を設定します。
show map-domain	マッピング アドレスおよびポート（MAP）ドメインに関する情報を表示します。
start-port	MAP ドメインの基本マッピング ルールの開始ポートを設定します。

map-name

ユーザー定義の属性名をシスコ属性名にマッピングするには、LDAP 属性マップ コンフィギュレーション モードで **map-name** コマンドを使用します。

このマッピ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。

map-name *user-attribute-name Cisco-attribute-name*
no map-name *user-attribute-name Cisco-attribute-name*

構文の説明

user-attribute-name	シスコ属性にマッピングするユーザー定義の属性名を指定します。
Cisco-attribute-name	ユーザー定義の属性名にマッピングするシスコ属性名を指定します。

コマンド デフォルト

デフォルトでは、名前のマッピングはありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
LDAP 属性マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

map-name コマンドを使用すると、独自の属性名をシスコ属性名にマッピングできます。その後、作成された属性マップを LDAP サーバーにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、未入力の属性マップを作成します。このコマンドにより、LDAP 属性マップ コンフィギュレーション モードが開始されます。
2. LDAP 属性マップ コンフィギュレーション モードで **map-name** コマンドと **map-value** コマンドを使用し、属性マップに情報を入力します。

3. AAA サーバーホストモードで **ldap-attribute-map** コマンドを使用し、属性マップを LDAP サーバーにバインドします。このコマンドでは、「ldap」の後にハイフンを入力しないでください。

（注） 属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザー定義属性名と値を理解しておく必要があります。

例

次に、LDAP 属性マップ myldapmap でユーザー定義の属性名 Hours をシスコ属性名 cVPN3000-Access-Hours にマッピングする例を示します。

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-name Hours cVPN3000-Access-Hours
ciscoasa(config-ldap-attribute-map)#
```

LDAP 属性マップ コンフィギュレーション モードで「?」を入力すると、シスコのすべての LDAP 属性名を表示できます。

```
ciscoasa(config-ldap-attribute-map)# map-name <name>
ldap mode commands/options:
cisco-attribute-names:
  cVPN3000-Access-Hours
  cVPN3000-Allow-Network-Extension-Mode
  cVPN3000-Auth-Service-Type
  cVPN3000-Authenticated-User-Idle-Timeout
  cVPN3000-Authorization-Required
  cVPN3000-Authorization-Type
 :
 :
  cVPN3000-X509-Cert-Data
ciscoasa(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap attribute-map (global configuration mode)	ユーザー定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
ldap-attribute-map (aaa-server host mode)	LDAP 属性マップを LDAP サーバーにバインドします。
map-value	ユーザー定義の属性値をシスコ属性にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP 属性マップを削除します。

mapping-service（廃止予定）

Cisco Intercompany Media Engine プロキシに対してマッピングサービスを設定するには、UC-IME コンフィギュレーション モードで **mapping-service** コマンドを使用します。プロキシからマッピングサービスを削除するには、このコマンドの **no** 形式を使用します。

mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*
no mapping-service listening-interface *interface* [**listening-port** *port*] **uc-ime-interface** *interface*

構文の説明

interface	リッスンするインターフェイスまたは uc-ime インターフェイスに使用されるインターフェイスの名前を指定します。
listening-interface	マッピング要求を ASA がリッスンするインターフェイスを設定します。
listening-port	（任意）マッピング サービスのリスニング ポートを設定します。
port	（任意）マッピング要求を ASA がリッスンする TCP ポート番号を指定します。このポート番号は、デバイス上の他のサービス（Telnet や SSH など）との競合を避けるために、1024 以上にする必要があります。デフォルトでは、このポート番号は TCP 8060 です。
uc-ime-interface	リモート Cisco UCM に接続するインターフェイスを設定します。

コマンド デフォルト

デフォルトでは、Cisco Intercompany Media Engine プロキシのオフパス配置のためのマッピングサービスは、TCP ポート 8060 でリッスンします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
UC-IME コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.4(1)	このコマンドは、すべての **uc-ime** モードコマンドとともに廃止されました。

使用上のガイドライン

ASA の Cisco Intercompany Media Engine プロキシのオフパス配置の場合、マッピングサービスをプロキシ構成に追加します。マッピングサービスを設定するには、マッピング要求をリッスンする外部インターフェイス（リモート エンタープライズ側）およびリモートの Cisco UCM に接続するインターフェイスを指定する必要があります。

（注） Cisco Intercompany Media Engine プロキシに対して設定できるマッピング サーバーは 1 つだけです。

Cisco Intercompany Media Engine プロキシがオフパス配置に対して設定されたときにマッピングサービスを設定します。

オフ パス配置では、Cisco Intercompany Media Engine のインバウンド コールおよびアウトバウンドコールは、Cisco Intercompany Media Engine プロキシを使用して有効にされた適応型セキュリティアプライアンスを通過します。適応型セキュリティアプライアンスは DMZ にあり、主に Cisco Intercompany Media Engine をサポートするように設定されています。通常のインターネットに接続するトラフィックは、この ASA を通過しません。

すべてのインバウンドコールのシグナリングは、宛先の Cisco UCM のグローバル IP アドレスが ASA 上に設定されているため、ASA に誘導されます。アウトバウンドコールの場合、着信側はインターネット上の任意の IP アドレスになる可能性があります。そのため、ASA には、インターネット上の着信側のグローバル IP アドレスごとに ASA 上で内部 IP アドレスを動的に提供するマッピングサービスが設定されます。

Cisco UCM は、すべてのアウトバウンドコールを、インターネット上の着信側のグローバル IP アドレスではなく、適応型セキュリティアプライアンス上のマッピング内部 IP アドレスに直接送信します。その後、それらのコールは、ASA によって着信側のグローバル IP アドレスに転送されます。

例

次に ... をする例を示します。

```
ciscoasa
(config)# uc-ime offpath_uc-ime_proxy
ciscoasa(config-uc-ime)# media-termination ime-media-term
ciscoasa(config-uc-ime)# ucm address 192.168.10.30 trunk-security-mode non-secure
ciscoasa(config-uc-ime)# ticket epoch 1 password password1234
ciscoasa(config-uc-ime)# fallback monitoring timer 120
ciscoasa(config-uc-ime)# fallback hold-down timer 30
ciscoasa(config-uc-ime)# mapping-service listening-interface inside listening-port 8060
 uc-ime-interface outside
```

関連コマンド

コマンド	説明
show running-config uc-ime	Cisco Intercompany Media Engine プロキシの実行コンフィギュレーションを表示します。

コマンド	説明
show uc-ime	フォールバック通知、マッピングサービスセッション、およびシグナリング セッションに関する統計情報または詳細情報を表示します。
uc-ime	Cisco Intercompany Media Engine プロキシインスタンスを ASA に作成します。

map-value

ユーザー定義の値をシスコの LDAP の値にマッピングするには、LDAP 属性マップ コンフィギュレーション モードで **map-value** コマンドを使用します。マップ内のエントリを削除するには、このコマンドの **no** 形式を使用します。

map-value *user-attribute-name user-value-string Cisco-value-string*
no map-value *user-attribute-name user-value-string Cisco-value-string*

構文の説明

Cisco-value-string	シスコ属性のシスコ値ストリングを指定します。
user-attribute-name	シスコ属性名にマッピングするユーザー定義の属性名を指定します。
user-value-string	シスコ属性値にマッピングするユーザー定義の値のストリングを指定します。

コマンド デフォルト

デフォルトでは、シスコ属性にマッピングされるユーザー定義の値がありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
LDAP 属性マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

map-value コマンドでは、ユーザー定義の属性値をシスコの属性名および属性値にマッピングできます。その後、作成された属性マップを LDAP サーバーにバインドできます。一般的な手順には次のものが含まれます。

1. グローバル コンフィギュレーション モードで **ldap attribute-map** コマンドを使用し、未入力の属性マップを作成します。このコマンドにより、LDAP 属性マップ コンフィギュレーション モードが開始されます。
2. LDAP 属性マップ コンフィギュレーション モードで **map-name** コマンドと **map-value** コマンドを使用し、属性マップに情報を入力します。

3. AAA サーバーホストモードで **ldap-attribute-map** コマンドを使用し、属性マップを LDAP サーバーにバインドします。このコマンドでは、「ldap」の後にハイフンを入力しないでください。

（注） 属性マッピング機能を正しく使用するには、Cisco LDAP 属性名と値の両方を理解し、さらにユーザー定義属性名と値を理解しておく必要があります。

例

次に、LDAP 属性マップ コンフィギュレーション モードを開始し、ユーザー定義の属性 Hours のユーザー定義の値をユーザー定義の時間ポリシー workDay とシスコ定義の時間ポリシー Daytime に設定する例を示します。

```
ciscoasa(config)# ldap attribute-map myldapmap
ciscoasa(config-ldap-attribute-map)# map-value Hours workDay Daytime
ciscoasa(config-ldap-attribute-map)#
```

関連コマンド

コマンド	説明
ldap attribute-map (global configuration mode)	ユーザー定義の属性名を Cisco LDAP 属性名にマッピングするために、LDAP 属性マップを作成して名前を付けます。
ldap-attribute-map (aaa-server host mode)	LDAP 属性マップを LDAP サーバーにバインドします。
map-name	ユーザー定義の LDAP 属性名を、Cisco LDAP 属性名にマッピングします。
show running-config ldap attribute-map	実行中の特定の LDAP 属性マップまたは実行中のすべての属性マップを表示します。
clear configure ldap attribute-map	すべての LDAP マップを削除します。

mask

モジュラポリシーフレームワークを使用する場合は、一致またはクラスコンフィギュレーション モードで **mask** コマンドを使用してパケットをドロップし、**match** コマンドまたはクラスマップと一致するトラフィックの接続を閉じます。このマスクアクションは、アプリケーショントラフィックのインスペクションポリシーマップに使用できますが（**policy-map type inspect** コマンド）、すべてのアプリケーションでこのアクションが許可されているわけではありません。たとえば、トラフィックに ASA の通過を許可する前に、DNS アプリケーション インスペクションに **mask** コマンドを使用してヘッダーフラグをマスクします。このアクション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。

mask［ **log** ］
no mask［ **log** ］

構文の説明

log 一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect**

コマンドを参照）、**mask** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するすべてのパケットの一部をマスクできます。

レイヤ 3/4 ポリシーマップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーションインスペクションを有効にする場合、このアクションを含むインスペクションポリシーマップを有効にできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、トラフィックに ASA の通過を許可する前に、DNS ヘッダーで RD フラグおよび RA フラグをマスクする例を示します。

```
ciscoasa(config-cmap)# policy-map type inspect dns dns-map1
ciscoasa(config-pmap-c)# match header-flag RD
ciscoasa(config-pmap-c)# mask log
ciscoasa(config-pmap-c)# match header-flag RA
ciscoasa(config-pmap-c)# mask log
```

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。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

mask-banner

サーバーバナーを難読化するには、パラメータ コンフィギュレーション モードで **mask-banner** 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。

mask-banner
no mask-banner

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、サーバ バナーをマスクする例を示します。

```
ciscoasa(config)# policy-map type inspect esmtp esmtp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mask-banner
```

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。

コマンド	説明
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。

mask-syst-reply

FTP サーバー応答をクライアントから見えないようにするには、**ftp-map** コマンドを使用してアクセスできる FTP マップ コンフィギュレーション モードで **mask-syst-reply** 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。

mask-syst-reply
no mask-syst-reply

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
FTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

クライアントから FTP サーバ システムを保護するには、厳格な FTP インスペクションで mask-syst-reply コマンドを使用します。このコマンドを有効にすると、**syst** コマンドに対するサーバーからの応答は一連の X に置き換えられます。

例

次に、ASA で syst コマンドに対する FTP サーバーの応答を一連の X に置き換える例を示します。

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# mask-syst-reply
ciscoasa(config-ftp-map)#
```

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。

コマンド	説明
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーションインスペクションに使用する特定の FTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。
request-command deny	不許可にする FTP コマンドを指定します。

match access-list

モジュラ ポリシー フレームワークを使用するときは、クラス マップ コンフィギュレーション モードで **match access-list** コマンドを使用し、アクセスリストを使用してアクションを適用するトラフィックを特定します。**match access-list** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match access-list *access_list_name*
no match access-list *access_list_name*

構文の説明

access_list_name 一致条件として使用するアクセス リストの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップコンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドを使用して、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを指定します。

class-map コマンドの入力後に、**match access-list** コマンドを入力してトラフィックを指定します。または、別のタイプの **match** コマンド（**match port** コマンドなど）を入力できます。クラスマップには **match access-list** コマンドを 1 つだけ含めることができ、他のタイプの **match** コマンドと組み合わせることはできません。ASA で検査できるすべてのアプリケーションが使用するデフォルトの TCP ポートおよび UDP ポートを照合する **matchdefault-inspection-traffic** コマンドを定義する場合は、例外として **match access-list** コマンドを使用して照合するトラフィックの範囲を絞り込めます。**match default-inspection-traffic** コマンドによって照合するポートが指定されるため、アクセスリストのポートはすべて無視されます。

1. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
2. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
3. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

例

次に、3 つのアクセス リストに一致する 3 つのレイヤ 3/4 クラス マップを作成する例を示します。

```
ciscoasa(config)# access-list udp permit udp any any
ciscoasa(config)# access-list tcp permit tcp any any
ciscoasa(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255
ciscoasa(config)# class-map all_udp
ciscoasa(config-cmap)# description "This class-map matches all UDP traffic"
ciscoasa(config-cmap)# match access-list udp
ciscoasa(config-cmap)# class-map all_tcp
ciscoasa(config-cmap)# description "This class-map matches all TCP traffic"
ciscoasa(config-cmap)# match access-list tcp
ciscoasa(config-cmap)# class-map to_server
ciscoasa(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
ciscoasa(config-cmap)# match access-list host_foo
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match any

モジュラ ポリシー フレームワークを使用する場合、クラスマップ コンフィギュレーション モードで **match any** コマンドを使用して、アクションを適用するすべてのトラフィックを照合します。 **match any** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match any
no match any

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドを使用して、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを指定します。

class-map コマンドの入力後に、 **match any** コマンドを入力してすべてのトラフィックを指定します。または、別のタイプの **match** コマンド（**match port** コマンドなど）を入力できます。**match any** コマンドは、他のタイプの **match** コマンドとは組み合わせることができません。

1. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
2. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
3. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

例

次に、クラスマップおよび **match any** コマンドを使用して、トラフィッククラスを定義する例を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 any
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match access-list	アクセス リストに従ってトラフィックを照合します。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match apn

GTP メッセージのアクセスポイント名に関して一致条件を設定するには、ポリシー マップ コンフィギュレーションモードで**match apn**コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **apn regex** { *regex_name* | **class** *regex_class_name* }
no match [**not**] **apn regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、GTP ポリシー マップで設定できます。

例

次に、GTP インスペクション ポリシー マップのアクセス ポイント名に関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match apn class gtp_regex_apn
```

関連コマンド

コマンド	説明
inspect gtp	GTP トラフィックのインスペクションを設定します。

match application-id

Diameter メッセージの Diameter アプリケーション ID に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match application-id** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **application-id** *app_id* [*app_id_2*]
no match [**not**] **application-id** *app_id* [*app_id_2*]

構文の説明

app_id Diameter アプリケーションの名前または番号（0 ～ 4294967295）。照合する連続番号が付されたアプリケーションの範囲がある場合は、2 番目の ID を含めることができます。アプリケーションの名前または番号別に範囲を定義でき、第 1 ID および第 2 ID の間のすべての番号に適用されます。

コマンド デフォルト

Diameter インスペクションでは、すべてのアプリケーションが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Diameter インスペクション クラス マップまたは Diameter インスペクション ポリシー マップで設定できます。このコマンドを使用すると、Diameter アプリケーション ID に基づいてトラフィックをフィルタ処理できます。その後、パケットをドロップしたり、接続をドロップしたり、一致するトラフィックをログに記録したりすることができます。

これらのアプリケーションは IANA に登録されます。次のコア アプリケーションがサポートされますが、他のアプリケーションもフィルタ処理できます。アプリケーション名のリストについては、CLI ヘルプを参照してください。

- **3gpp-rx-ts29214** （16777236）

- **3gpp-s6a** （16777251）
- **3gpp-s9** （16777267）
- **common-message** （0）。（基本 Diameter プロトコル）

http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml に IETF の登録済みアプリケーション、コマンドコード、および属性値ペアのリストがありますが、リストにあるすべての項目が Diameter インスペクションでサポートされているわけではありません。技術仕様については、3GPP Web サイトを参照してください。

例

次に、アプリケーション ID 3gpp-s6a と 3gpp-s13 に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect diameter match-any log_app
ciscoasa(config-cmap)# match application-id 3gpp-s6a
ciscoasa(config-cmap)# match application-id 3gpp-s13
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
inspect diameter	Diameter インスペクションを有効にします。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match as-path

BGP 自律システム パス アクセス リストを照合するには、ルートマップ コンフィギュレーション モードでmatch as-path コマンドを使用します。パス リスト エントリを削除するには、このコマンドの no 形式を使用します。

match as-path *path-list-number*
no match as-path *path-list-number*

構文の説明

path-list-number	自律システム パス アクセス リストの番号。

コマンド デフォルト

パス リストは定義されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

match as-path コマンドおよび set weight コマンドで設定した値はグローバル値よりも優先されます。たとえば、match as-path コマンドおよび set weight route-map コマンドで割り当てた重みは、neighbor weight コマンドで割り当てた重みよりも優先されます。

ルート マップは、いくつかの部分にわかれている可能性があります。route-map コマンドに関連付けられているどの match ステートメントとも一致しないルートは無視されます。したがって、そのルートは発信ルート マップ用にアドバタイズされることも、着信ルート マップ用に受け入れられることもありません。一部のデータのみを変更したい場合は、別のルートマップ セクションに明示的にmatch を指定する必要があります。この方法でパス リスト名を複数指定することができます。

例

次に、自律システム（AS）パスと BGP AS パス アクセス リスト as-path-acl を照合する設定の例を示します。

```
ciscoasa(config)# route-map IGP2BGP
ciscoasa(config-route-map)# match as-path 23
```

関連コマンド

コマンド	説明
set-weight	ルーティングプロトコルのBGP重みを指定します。
neighbor-weight	ネイバー接続に重みを割り当てます。

match avp

Diameter メッセージの Diameter 属性値ペア（AVP）に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match avp** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

属性によってのみ AVP を照合するには、次の手順を実行します。

match [**not**] **avp** *code* [*code-2*] [**vendor-id** *id_number*]
no match [**not**] **avp** *code* [*code-2*] [**vendor-id** *id_number*]

属性の値に基づいて AVP を照合する場合：

match [**not**] **avp** *code* [**vendor-id** *id_number*] *value*
no match [**not**] **avp** *code* [**vendor-id** *id_number*] *value*

構文の説明

code	属性値ペアの名前または番号（1 ～ 4294967295）。最初のコードについては、カスタム AVP、RFC または 3GPP 技術仕様に登録されている AVP、およびソフトウェアで直接サポートされている AVP の名前を指定できます。特定の範囲の AVP を照合する場合は、2 つ目のコードを番号のみで指定します。値によって AVP を照合する場合は、2 つ目のコードを指定できません。AVP 名のリストについては、CLI ヘルプを参照してください。
value	AVP の値の部分。これは、AVP の データ タイプがサポートされている場合にのみ設定できます。たとえば、アドレス データ タイプがある AVP の IP アドレスを指定できます。このパラメータを設定する方法の詳細については、この後の「使用上のガイドライン」を参照してください。
vendor-id *id_number*	（任意）ベンダーの ID 番号（0 ～ 4294967295）も照合します。たとえば、3GPP ベンダー ID は 10415、IETF は 0。

コマンド デフォルト

Diameter インスペクションでは、すべての AVP が許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Diameter インスペクション クラス マップまたは Diameter インスペクション ポリシー マップで設定できます。このコマンドを使用すると、Diameter AVP に基づいてトラフィックをフィルタ処理できます。その後、パケットをドロップしたり、接続をドロップしたり、一致するトラフィックをログに記録したりすることができます。

AVP 名のリストについては、CLI ヘルプを参照してください。https://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml に IETF の登録済みアプリケーション、コマンドコード、および属性値ペアのリストがありますが、リストにあるすべての項目が Diameter インスペクションでサポートされているわけではありません。技術仕様については、3GPP Web サイトを参照してください。

値の照合を設定する場合は、サポートされているデータ タイプに固有の値オプションの構文は次のとおりです。

- [Diameter Identity]、[Diameter URI]、[Octet String]：これらのデータ タイプの照合には正規表現または正規表現クラス オブジェクトを使用します。

{**regex** *regex_name* | **class** *regex_class*}

- [Address]：照合する IPv4 または IPv6 アドレスを指定します。たとえば、10.100.10.10 または 2001:DB8::0DB8:800:200C:417A。
- [Time]：開始日時と終了日時を指定します。両方を指定する必要があります。時間は 24 時間形式で指定します。

date *year month day* **time** *hh*:*mm*:*ss* **date** *year month day* **time** *hh*:*mm*:*ss*

次に例を示します。

date 2015 feb 5 time 12:00:00 date 2015 mar 9 time 12:00:00

- [Numeric]：番号の範囲を指定します。

range *number_1 number_2*

有効な番号の範囲は、データ タイプによって異なります。

- Integer32：-2147483647 ～ 2147483647
- Integer64：-9223372036854775807 ～ 9223372036854775807
- Unsigned32：0 ～ 4294967295
- Unsigned64：0 ～ 18446744073709551615
- Float32：8 桁の小数点表現
- Float64：16 桁精度の小数点表記

例

次に、機能交換要求/応答コマンド メッセージで host-ip-address AVP に含まれる特定の IP アドレスに関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip
ciscoasa(config-cmap)# match command-code cer-cea
ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
diameter	カスタム属性値ペアを作成します。
inspect diameter	Diameter インスペクションを有効にします。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match body

ESMTP本文メッセージの長さまたは1行の長さに対して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match body** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **body** [**length** | **line length**] **gt** *bytes*
no match [**not**] **body** [**length** | **line length**] **gt** *bytes*

構文の説明

length	ESMTP 本文メッセージの長さを指定します。
line length	ESMTP本文メッセージの1行の長さを指定します。
bytes	一致する数値をバイト単位で指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ESMTP インスペクション ポリシー マップで本文 1 行の長さに関して一致条件を設定する例を示します。

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match body line length gt 1000**

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match called-party

H.323 着信側に関して一致条件を設定するには、ポリシーマップ コンフィギュレーション モードで **match called-party** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **called-party** [**regex** *regex*]
no match [**not**] **match** [**not**] **called-party** [**regex** *regex*]

構文の説明

regex regex	正規表現を照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション クラス マップで着信側に関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match called-party regex caller1
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match calling-party

H.323 発信側に関して一致条件を設定するには、ポリシーマップ コンフィギュレーション モードで **match calling-party** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **calling-party** [**regex** *regex*]
no match [**not**] **match** [**not**] **calling-party** [**regex** *regex*]

構文の説明

regex regex	正規表現を照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション クラス マップで発信側に関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match calling-party regex caller1
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。

コマンド	説明
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match certificate

証明書一致ルールを設定するには、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 **match certificate** コマンドを使用します。構成からルールを削除するには、このコマンドの **no** 形式を使用します。

match certificate *map-name* [**override ocsp** [**trustpoint** *trustpoint-name*] *seq-num* **url** *URL* | **override cdp** *seq-num* **url** *URL*]
no match certificate *map-name* [**override ocsp** [*seq-num* **url** *URL*] | **override cdp** [*seq-num* **url** *URL*]]

構文の説明

map-name	このルールに一致する証明書マップの名前を指定します。一致ルールを設定する前に、証明書マップを設定する必要があります。65 文字以内で指定します。
override ocsp	ルールの目的が証明書の OCSP URL を上書きすることであることを指定します。
seq-num	この一致ルールのプライオリティを設定します。有効な範囲は 1 ～ 10000 です。ASA では、まずシーケンス番号が最も小さい一致ルールが評価され、一致が見つかるまで順番に高い番号の一致ルールが評価されます。
トラストポイント	（任意）トラストポイントを使用して OCSP 応答側証明書を確認することを指定します。
trustpoint-name	（オプション）レスポンダ証明書を検証するために上書きに使用するトラストポイントを指定します。
url	OCSP 失効ステータスの URL にアクセスすることを指定します。
URL	OCSP 失効ステータスのためにアクセスする URL を識別します。
override cdp	ルールの目的が証明書の CRL URL を上書きすることであることを指定します。
seq-num	リスト内の各 URL のランクを設定します。1 ～ 5 の値を指定します。ASA では、最初に最低ランク (1) の URL が試されます。
url	CRL 失効ステータスの URL にアクセスすることを指定します。
URL	CRL 失効ステータスにアクセスする URL。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.13(1)	cdp オーバーライドを設定するためのプロビジョニングが追加されました。
9.15(1)	このリリースより前のリリースでは、スタティック CDP は、検証中のチェーン内の各証明書に一意にマッピングできました。ただし、このようなマッピングは各証明書で 1 つだけサポートされていました。 このリリース以降、match certificate cdp override コマンドは、同じマップ名の複数のインスタンスを受け入れます。

使用上のガイドライン

PKI証明書検証プロセスでは、セキュリティを維持するために、ASAによって証明書の失効ステータスがチェックされます。チェックには、CRL チェックまたは Online Certificate Status Protocol（OCSP）が使用されます。CRLチェックを使用すると、失効した証明書がすべてリストされている CRL が、ASA によって取得、解析、およびキャッシュされます。OCSP は失効ステータスを確認する拡張性の高い方法であり、検証局で証明書ステータスをローカライズします。この検証局が特定の証明書のステータスを問い合わせます。

証明書一致ルールには、OCSP URL オーバーライドを設定できます。このオーバーライドには、リモートユーザー証明書の AIA フィールドの URL ではなく、失効ステータスを確認するための URL を指定します。一致ルールには、OCSP応答側証明書の検証に使用するトラストポイントも設定できます。設定することで、ASAは自己署名証明書やクライアント証明書の検証パスの外部にある証明書など、任意の CA からの応答側証明書を検証できます。

OCSP と同様に、**match certificate** コマンドを使用して CDP URL のオーバーライドを設定できます。このコマンドは、証明書マップを介したスタティック CDP URL の識別をサポートします。CRL 検証が必要な証明書ごとに、証明書の CDP 拡張とこの設定にマッピングされている URL に基づいて CRL が取得されます。**config-ca-crl** サブモードで **policy** コマンドを使用すると、証明書またはスタティック CDP から CDP を除外できます。

1つのマップに複数のスタティックCDPを設定できるようになりました。個々のインスタンスを削除するには、コマンドの **no** 形式でURLとシーケンス番号を指定します。指定されたURLおよびシーケンス番号が、構成した値と同じ値であることを確認してください。特定の情報に

言及しない場合、マップのすべてのエントリが削除されます。複数のインスタンスをマップに設定する、またはマップから削除するためのプロビジョニングは、OCSPには適用されません。

OCSP を設定するときは、次の要件に注意してください。

- 1 つのトラストポイント コンフィギュレーション内に複数の一致ルールを設定できますが、各クリプト CA 証明書マップに指定できる一致ルールは 1 つだけです。ただし、複数のクリプト CA 証明書マップを設定し、それらを同じトラストポイントに関連付けることができます。
- 一致ルールを設定する前に、証明書マップを設定する必要があります。
- 自己署名 OCSP 応答側証明書を検証するようにトラストポイントを設定するには、自己署名応答側証明書を信頼できる CA 証明書として独自のトラストポイントにインポートします。次に、クライアント証明書を検証するトラストポイントで **match certificate** コマンドを設定して、応答側の証明書を検証するために、OCSP の自己署名応答側証明書を含むトラストポイントを使用するようにします。同じことが、クライアント証明書の検証パスの外部にある応答側証明書の検証にも当てはまります。
- クライアント証明書と応答側証明書の両方を同じ CA が発行している場合には、1 つのトラストポイントでどちらも検証できます。しかし、クライアント証明書と応答側証明書を発行している CA が異なる場合は、トラストポイントを証明書ごとに 1 つずつ計 2 つ設定する必要があります。
- OCSP サーバー（応答側）証明書は一般に、OCSP 応答に署名します。ASA が応答を受け取ると、応答側の証明書を検証しようとします。CA は通常、自身の OCSP 応答側証明書のライフタイムを比較的短い期間に設定して、証明書が侵害される可能性を最小限に抑えます。CA は一般に、応答側証明書に ocsp-no-check 拡張を含めて、この証明書では失効ステータスチェックが必要ないことを示します。しかし、この拡張が含まれていない場合、ASA はトラストポイントに指定されているのと同じ方法を使用して、自身の失効ステータスのチェックを試みます。応答側証明書が検証可能でない場合、失効チェックは失敗します。この可能性を防ぐには、**revocation-check none** コマンドを使用して応答側の証明書を検証するトラストポイントを設定し、**revocation-check ocsp** コマンドを使用してクライアント証明書を設定します。
- ASA は、一致が見つからない場合、 **ocsp url** コマンドで指定された URL を使用します。**ocsp url** コマンドが設定されていない場合、ASA はリモートユーザー証明書の AIA フィールドを使用します。証明書に AIA 拡張がない場合、失効ステータスのチェックは失敗します。

例

次に、newtrust という名前のトラストポイントの証明書一致ルールを作成する例を示します。ルールには、マップ名 mymap、シーケンス番号 4、トラストポイント mytrust があり、URL として 10.22.184.22 が指定されています。

```
ciscoasa(config)# crypto ca trustpoint
 newtrust
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint mytrust
 4 url 10.22.184.22
ciscoasa(config-ca-trustpoint)#
```

次に、クリプトCA証明書マップを設定し、CA証明書が含まれているトラストポイントを識別して応答側証明書を検証するための一致証明書ルールを設定する例を示します。この証明書が必要になるのは、newtrust トラストポイントで識別した CA が OCSP 応答側証明書を発行していない場合です。

1. マップ ルールの適用先のクライアント証明書を識別する証明書マップを設定します。この例では、証明書マップの名前は mymap で、シーケンス番号は 1 です。サブジェクト名に mycert という CN 属性が含まれているクライアント証明書はどれも、mymap エントリに一致します。

```
ciscoasa(config)# crypto ca certificate map mymap 1 subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)# subject-name attr cn eq mycert
ciscoasa(config-ca-cert-map)#
```

2. OCSP応答側証明書の検証に使用するCA証明書が含まれているトラストポイントを設定します。自己署名証明書の場合、これは自己署名証明書自体であり、インポートされてローカルに信頼できるようになっています。この目的で外部の CA 登録を介して証明書を取得することもできます。CA証明書に貼り付けるように求められたら貼り付けます。

```
ciscoasa(config-ca-cert-map)# exit
ciscoasa(config)# crypto ca trustpoint mytrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate mytrust
Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself

MIIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
v8RqzqpmZYguveV9cLQK5tsxqW3DysMU/4/qUGPfkVZ0iKPCgpIAWmq2ojhCFPyx
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit

INFO: Certificate has the following attributes:
Fingerprint: 7100d897 05914652 25b2f0fc e773df42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
```

3. OCSP を失効チェック方法にして、元のトラストポイント newtrust を設定します。次に、ステップ 2 で設定した証明書マップ mymap および自己署名トラストポイント mytrust を含めた一致ルールを設定します。

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# enroll terminal
ciscoasa(config-ca-trustpoint)# crypto ca authenticate newtrust

Enter the base 64 encoded CA certificate.
End with the word "quit" on a line by itself
ywsDsjl6YamF8mpMoruvwOuaUOsAK6KO54vy0QIBAzANBgkqhkiG9w0BAQQFAAOB
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
AxQMNjMuNjcuNzIuMTg4MIGdMA0GCSqGSIb3DQEBAQUAA4GLADCBhwKBgQDnXUHv
7//x1xEAOYfUzJmH5sr/NuxAbA5gTUbYA3pcE0KZHt761N+/8xGxC3DIVB8u7T/b
gQCSOihb2NH6mga2eLqEsFP1oVbBteSkEAm+NRCDK7ud1l3D6UC01EgtkJ81QtCk
```

```
tvX2T2Y/5sdNW4gfueavbyqYDbk4yxCKaofPp1ffAD9rrUFQJM1uQX14wclPCcAN
NzIuMTg4MB4XDTA2MDExODIwMjYyMloXDTA5MDExNzIwMjYyMlowFzEVMBMGA1UE
OPIBnjCCAQcCBEPOpG4wDQYJKoZIhvcNAQEEBQAwFzEVMBMGA1UEAxQMNjMuNjcu
e7kR+rscOKYBSgVHrseqdB8+6QW5NF7f2dd+tSMvHtUMNw==
quit
INFO: Certificate has the following attributes:
Fingerprint: 9508g897 82914638 435f9f0fc x9y2p42
Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.

% Certificate successfully imported
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# revocation-check ocsp
ciscoasa(config-ca-trustpoint)# match certificate mymap override ocsp trustpoint
mytrust 4 url 10.22.184.22
```

クライアント証明書認証にnewtrustトラストポイントを使用する接続はどれも、mymap証明書マップに指定されている属性ルールにクライアント証明書が一致するかどうかを確認します。一致する場合、ASA は、10.22.184.22 にある OCSP 応答側にアクセスして証明書失効ステータスをチェックし、mytrustトラストポイントを使用して応答側証明書を検証します。

（注） newtrustトラストポイントは、OCSP経由でクライアント証明書の失効チェックを実行するように設定されます。ただし、mytrust トラストポイントにはデフォルトの失効チェック方法が設定されています。デフォルトは none であるため、OCSP 応答側証明書に対して失効チェックは実行されません。

次に、CDP を使用して一致証明書ルールを構成する例を示します。このルールには、test というマップ名があり、シーケンス番号として 1、2、および 3 があり、静的 URL が含まれています。証明書の CDP を選択するときに、ASA は、*test* という名前の証明書マップに一致するすべての証明書に対して 3 つの CDP を選択します。証明書の検証中に CRL が必要であると ASA が判断した場合、CRL が正常に取得されるまで、指定された順序で URL が試行されます。

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 1 url http://1.1.1.1
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 2 url http://1.1.1.2
ciscoasa(config-ca-trustpoint)# match certificate test override cdp 3 url http://1.1.1.3
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	クリプト CA 証明書マップを作成します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
crypto ca trustpoint	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ます。このコマンドは、グローバル コンフィギュレーション モードで使用します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。

コマンド	説明
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバーを指定します。
revocation-check	失効チェックに使用する方法とその順序を指定します。

match certificate allow expired-certificate（廃止）

特定の証明書に対する有効期限チェックを管理者が免除できるようにするには、CA トラストプール コンフィギュレーション モードで **match certificate allow expired-certificate** コマンドを使用します。特定の証明書の免除を無効にするには、このコマンドの **no** 形式を使用します。

match certificate < **map** > **allow expired-certificate**
no match certificate < **map** > **allow expired-certificate**

構文の説明

allow	失効した証明書を受け入れます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Ca trustpool コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.13(1)	このコマンドは削除されました。

使用上のガイドライン

トラストプールの match コマンドでは、証明書マップ オブジェクトを利用して、証明書固有の例外やグローバル トラストプール ポリシーに対するオーバーライドを設定します。一致ルールは検証する証明書ごとに記述されます。

関連コマンド

コマンド	説明
match certificate skip revocation check	特定の証明書に対する失効チェックを免除します。

match certificate skip revocation-check

特定の証明書に対する失効チェックを管理者が免除できるようにするには、CA トラストプール コンフィギュレーション モードで **match certificate skip revocation-check** コマンドを使用します。失効チェックの免除を無効にするには、このコマンドの **no** 形式を使用します。

matchcertificatemapskiprevocation-check
nomatchcertificatemapskiprevocation-check

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Ca trustpool コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

トラストプールのmatchコマンドでは、証明書マップオブジェクトを利用して、証明書固有の例外やグローバル トラストプール ポリシーに対するオーバーライドを設定します。一致ルールは検証する証明書ごとに記述されます。

例

次に、サブジェクト DN の共通名が「mycompany123」である証明書に対する有効性チェックをスキップする例を示します。

```
crypto ca certificate map mycompany 1subject-name attr cn eq mycompany123
crypto ca trustpool policymatch certificate mycompany skip revocation-check
```

関連コマンド

コマンド	説明
match certificate allow expired-certificate	特定の証明書に対する有効期限チェックを免除します。

match cmd

ESMTP コマンド verb に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match cmd** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]
no match [**not**] **cmd** [**verb** *verb* | **line length gt** *bytes* | **RCPT count gt** *recipients_number*]

構文の説明

verb verb	ESMTP コマンド verb を指定します。
line length gt bytes	1 行の長さを指定します。
RCPT count gt recipients_number	受信者の電子メールアドレスの数を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ESMTP トランザクションで交換される verb（メソッド）NOOP に関して一致条件を ESMTP インスペクション ポリシー マップに設定する例を示します。

```
ciscoasa(config-pmap)# match cmd verb NOOP
```

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。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match command-code

Diameter メッセージの Diameter コマンドコードに関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match command-code** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **command-code** *code* [*code_2*]
no match [**not**] **command-code** *code* [*code_2*]

構文の説明

code Diameter コマンドコードの名前または番号（0 ～ 4294967295）。照合する連続番号が付されたコマンドコードの範囲がある場合は、2 番目のコードを含めることができます。コマンドコードの名前または番号別に範囲を定義でき、第 1 コードおよび第 2 コードの間のすべての番号に適用されます。コマンドコード名のリストについては、CLI ヘルプを参照してください。

コマンド デフォルト

Diameter インスペクションでは、すべてのコマンド コードが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、Diameter インスペクション クラス マップまたは Diameter インスペクション ポリシー マップで設定できます。このコマンドを使用すると、Diameter コマンド コードに基づいてトラフィックをフィルタ処理できます。その後、パケットをドロップしたり、接続をドロップしたり、一致するトラフィックをログに記録したりすることができます。

http://www.iana.org/assignments/aaa-parameters/aaa-parameters.xhtml に IETF の登録済みアプリケーション、コマンドコード、および属性値ペアのリストがありますが、リストにあるすべての項目が Diameter インスペクションでサポートされているわけではありません。技術仕様については、3GPP Web サイトを参照してください。

例

次に、機能交換要求/応答コマンド メッセージで host-ip-address AVP に含まれる特定の IP アドレスに関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect diameter match-all block-ip
ciscoasa(config-cmap)# match command-code cer-cea
ciscoasa(config-cmap)# match avp host-ip-address 1.1.1.1
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
inspect diameter	Diameter インスペクションを有効にします。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match community

ボーダー ゲートウェイ プロトコル（BGP）コミュニティを照合するには、ルートマップ コンフィギュレーション モードで match community コマンドを使用します。コンフィギュレーション ファイルから match community コマンドを削除し、システムをデフォルトの条件（BGP コミュニティ リスト エントリを削除）に戻すには、このコマンドの no 形式を使用します。

match community { *standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**] }
no match community { *standard-list-number* | *expanded-list-number* | *community-list-name* [**exact**] }

構文の説明

standard-list-number	コミュニティの 1 つ以上の許可グループまたは拒否グループを識別する標準コミュニティ リスト番号（1 ～ 99）を指定します。
expanded-list-number	コミュニティの 1 つ以上の許可グループまたは拒否グループを識別する拡張コミュニティ リスト番号（100 ～ 500）を指定します。
community-list-name	コミュニティ リストの名前。
exact	（任意）完全一致が必要であることを示します。指定されたすべてのコミュニティのみが存在する必要があります。

コマンド デフォルト

ルート マップではコミュニティ リストの照合は行われません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ルート マップは、いくつかの部分にわかれている可能性があります。route-map コマンドに関連した match コマンドと 1 つも一致しないルートは無視されます。そのため、このようなルートは、アウトバウンド ルート マップではアドバタイズされず、インバウンド ルート マップで

は受け入れられません。一部のデータのみを変更したい場合は、別のルートマップセクションに明示的に match を指定する必要があります。

コミュニティリスト番号に基づく照合は、BGP に適用できる match コマンドのタイプの 1 つです。

例

次に、コミュニティ リスト 1 と一致するルートの重みが 100 に設定される例を示します。コミュニティ 109 を含むすべてのルートの重みが 100 に設定されます。

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)#  match community 1
ciscoasa(config-route-map)# set weight 100
```

次に、コミュニティ リスト 1 と一致するルートの重みを 200 に設定する例を示します。コミュニティ 109 を含むすべてのルートの重みが 200 に設定されます。

```
ciscoasa(config)#  community-list 1 permit 109
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community 1 exact
ciscoasa(config-route-map)# set weight 200
```

次の例では、コミュニティ リスト LIST_NAME と一致するルートの重みが 100 に設定されます。コミュニティ 101 を含むすべてのルートの重みが 100 に設定されます。

```
ciscoasa(config)#  community-list LIST_NAME permit 101
ciscoasa(config)# route-map set_weight
ciscoasa(config-route-map)# match community LIST_NAME
ciscoasa(config-route-map)# set weight 100
```

次の例は、拡張コミュニティ リスト 500 と一致するルートを示しています。拡張コミュニティ 1 のあるルートに、150 に設定されたウェイトがあります。

```
ciscoasa(config)#  community-list 500 permit [0-9]*
ciscoasa(config)# route-map MAP_NAME permit 10
ciscoasa(config-route-map)# match extcommunity 500
ciscoasa(config-route-map)# set weight 150
```

関連コマンド

コマンド	説明
set-weight	ルーティング プロトコルの BGP 重みを指定します。
community-list	BGP コミュニティ リストを作成または設定します。

match default-inspection-traffic

クラスマップに inspect コマンドのデフォルトのトラフィックを指定するには、クラス マップ コンフィギュレーション モードで **match default-inspection-traffic** 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。

matchdefault-inspection-traffic
nomatchdefault-inspection-traffic

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。

コマンド デフォルト

各インスペクションのデフォルトのトラフィックについては、「使用上のガイドライン」を参照してください。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.6(2)	DNS over TCP インスペクション用に TCP/53 が追加されました（デフォルトではディスエーブル）。M3UA および STUN のデフォルト ポートも追加されました。

使用上のガイドライン

match コマンドは、クラスマップのトラフィッククラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラスマップに含まれるトラフィックを定義するさまざまな基準が含まれています。モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定する一環として、**class-map** グローバル コンフィギュレーション コマンドを使用してトラフィッククラスを定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィッククラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラスマップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

match default-inspection-traffic コマンドを使用すると、個々の **inspect** コマンドのデフォルトのトラフィックを照合できます。**match default-inspection-traffic** コマンドは、一般に **permit ip** *src-ip dst-ip* という形式のアクセスリストであるもう 1 つの match コマンドと併用できます。

match default-inspection-traffic コマンドともう 1 つの **match** コマンドを組み合わせるためのルールは、**match default-inspection-traffic** コマンドを使用してプロトコルおよびポート情報を指定し、別の **match** コマンドを使用して他のすべての情報（IP アドレスなど）を指定するというルールです。もう 1 つの **match** コマンドに指定されているプロトコルやポート情報は、**inspect** コマンドでは無視されます。

たとえば、次の例に指定されているポート 65535 は無視されます。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 default-inspection-traffic
ciscoasa(config-cmap)# match port 65535
```

インスペクション用のデフォルトのトラフィックは、次のようになります。

Inspection Type	Protocol Type	Source Port	Destination Port
ctiqbe	tcp	該当なし	2748
dcerpc	tcp	該当なし	135
diameter	tcp、sctp	該当なし	3868
dns	udp、tcp	53	53
ftp	tcp	該当なし	21
gtp	udp	2123、3386	2123、3386
h323 h225	tcp	該当なし	1720
h323 ras	udp	該当なし	1718 ～ 1719
http	tcp	該当なし	80
icmp	icmp	該当なし	該当なし
ils	tcp	該当なし	389
im	tcp	該当なし	1 ～ 65539
ip-options	rsvp	該当なし	該当なし
ipsec-pass-thru	udp	該当なし	500
m3ua	sctp	該当なし	2905

mgcp	udp	2427、2727	2427、2727
netbios	udp	137 ～ 138	該当なし
radius-accounting	udp	該当なし	1646
rpc	udp	111	111
rsh	tcp	該当なし	514
rtsp	tcp	該当なし	554
sctp	sctp	any	any
sip	tcp、udp	該当なし	5060
skinny	tcp	該当なし	2000
smtp	tcp	該当なし	25
sqlnet	tcp	該当なし	1521
stun	tcp、udp	該当なし	3478
tftp	udp	該当なし	69
waas	tcp	該当なし	1 ～ 65535
xdmcp	udp	177	177

例

次に、クラスマップおよび **match default-inspection-traffic** コマンドを使用して、トラフィッククラスを定義する例を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 default-inspection-traffic
ciscoasa(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラスマップ内のアクセスリストトラフィックを指定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dns-class

DNS Resource Record or Question セクションの Domain System Class に関して一致条件を設定するには、クラスマップまたはポリシーマップ コンフィギュレーション モードで **match dns-class** コマンドを使用します。設定済みのクラスを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **dns-class** { **eq** *c_well_known* | *c_val* } { **range** *c_val1 c_val2* }
no match [**not**] **dns-class** { **eq** *c_well_known* | *c_val* } { **range** *c_val1 c_val2* }

構文の説明

eq	完全一致を指定します。
c_well_known	既知の名前 IN で DNS クラスを指定します。
c_val	DNS クラス フィールド（0 ～ 65535）に任意の値を指定します。
range	範囲を指定します。
c_val1 c_val2	一致範囲を示す値を指定します。それぞれの値の範囲は、0 ～ 65535 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、このコマンドはDNSメッセージのすべてのフィールド（質問およびRR）を調べ、指定されたクラスを照合します。DNS クエリーと応答の両方が検査されます。

一致対象は、match not header-flag QR と match question の 2 つのコマンドによって DNS クエリーのクエスチョン部分にまで絞ることができます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップ内で入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS クラスに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-class eq IN
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dns-type

クエリタイプや RR タイプなど DNS タイプの一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match dns-type** コマンドを使用します。設定された DNS タイプを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **dns-type** { **eq** *t_well_known* | *t_val* } { **range** *t_val1 t_val2* }
no match [**not**] **dns-type** { **eq** *t_well_known* | *t_val* } { **range** *t_val1 t_val2* }

構文の説明

eq	完全一致を指定します。
t_well_known	A、NS、CNAME、SOA、TSIG、IXFR、AXFR のいずれかの既知の名前で DNS タイプを指定します。
t_val	DNS タイプ フィールド（0 ～ 65535）に任意の値を指定します。
range	範囲を指定します。
t_val1 t_val2	一致範囲を示す値を指定します。それぞれの値の範囲は、0 ～ 65535 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、このコマンドはDNSメッセージのすべてのセクション（質問およびRR）を調べ、指定されたタイプを照合します。DNS クエリーと応答の両方が検査されます。

一致対象は、match not header-flag QR と match question の 2 つのコマンドによって DNS クエリーのクエスチョン部分にまで絞ることができます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップ内で入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS タイプに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match dns-type eq a
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match domain-name

DNS メッセージドメイン名リストに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match domain-name** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **domain-name regex** *regex_id*
match [**not**] **domain-name regex class** *class_id*
no match [**not**] **domain-name regex** *regex_id*
no match [**not**] **domain-name regex class** *class_id*

構文の説明

regex	正規表現を指定します。
regex_id	正規表現 ID を指定します。
class	複数の正規表現エントリが含まれているクラスマップを指定します。
class_id	正規表現クラス マップ ID を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、定義済みのリストと DNS メッセージのドメイン名を照合します。圧縮されたドメイン名は、照合の前に展開されます。一致条件は、他の DNS match コマンドと併用して、特定のフィールドにまで絞り込むことができます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップ内で入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップで DNS ドメイン名を照合する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match domain-name regex
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match dpc

M3UA データメッセージの宛先ポイントコード（DPC）に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match dpc** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match ［ **not** ］ **dpc** *code*
no match ［ **not** ］ **dpc** *code*

構文の説明

code	*zone -region -sp* 形式の宛先ポイントコード。

コマンド デフォルト

M3UA インスペクションでは、すべての宛先ポイント コードが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは M3UA インスペクション ポリシー マップで設定できます。宛先ポイント コードに基づいてパケットをドロップできます。ポイントコードは *zone -region -sp* 形式で、各要素に使用可能な値は SS7 バリアントによって異なります。バリアントはポリシーマップの **ss7 variant** コマンドで定義できます。

- ITU：ポイント コードは 14 ビットで 3-8-3 形式です。値の範囲は、[0-7]-[0-255]-[0-7] です。これは、デフォルトの SS7 バリエーションです。
- ANSI：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。
- Japan：ポイント コードは 16 ビットで 5-4-7 形式です。値の範囲は、[0-31]-[0-15]-[0-127] です。
- China：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。

例

次に、ITU の特定の宛先ポイント コードに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match dpc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
match opc	M3UA 発信ポイント コードと一致させます。
policy-map type inspect	インスペクション ポリシー マップを作成します。
ss7 variant	ポリシー マップで使用する SS7 バリアントを指定します。

match dscp

クラスマップの（IP ヘッダーの）IETF-defined DSCP 値を識別するには、クラス マップ コンフィギュレーション モードで **match dscp** 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。

match dscp { *values* }
no match dscp { *values* }

構文の説明

値IP ヘッダーに最大 8 種類の IETF-defined DSCP 値を指定します。指定できる範囲は、0 ～ 63 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップコンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、クラスマップのトラフィッククラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラスマップに含まれるトラフィックを定義するさまざまな基準が含まれています。モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定する一環として、**class-map** グローバル コンフィギュレーション コマンドを使用してトラフィッククラスを定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィッククラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラスマップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

match dscp コマンドを使用すると、IP ヘッダーの IETF-defined DSCP 値を照合できます。

例

次に、クラスマップおよび**match dscp** コマンドを使用して、トラフィッククラスを定義する例を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 dscp af43 cs1 ef
ciscoasa(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラスマップ内のアクセスリストトラフィックを指定します。
match port	TCP/UDP ポートをそのインターフェイスで受信したパケットに対する比較基準として指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match e – match q

- match question （856 ページ）

match ehlo-reply-parameter

ESMTP ehlo reply パラメータに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match ehlo-reply-parameter** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **ehlo-reply-parameter** *parameter*
no match [**not**] **ehlo-reply-parameter** *parameter*

構文の説明

パラメータ	ehlo reply パラメータを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ESMTP インスペクション ポリシー マップに ehlo reply パラメータに関して一致条件を設定する例を示します。

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match ehlo-reply-parameter auth**

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。

コマンド	説明
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match filename

FTP転送のファイル名に関して一致条件を設定するには、クラスマップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match filename** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **filename regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class regex_class_name	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション クラス マップに FTP 転送ファイル名に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# description Restrict FTP users ftp1, ftp2, and ftp3 from accessing
 /root
ciscoasa(config-cmap)# match username regex class ftp_regex_user
ciscoasa(config-cmap)# match filename regex ftp-file
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match filetype

FTP転送のファイルタイプに関して一致条件を設定するには、クラスマップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match filetype** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **filetype regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class regex_class_name	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション ポリシー マップに FTP 転送ファイルタイプに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match filetype class regex ftp-regex-filetype
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match flow ip destination-address

クラスマップにフロー IP 宛先アドレスを指定するには、クラス マップ コンフィギュレーション モードで **match flow ip destination-address** 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。

matchflowipdestination-address
nomatchflowipdestination-address

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、クラスマップのトラフィッククラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラスマップに含まれるトラフィックを定義するさまざまな基準が含まれています。モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定する一環として、**class-map** グローバル コンフィギュレーション コマンドを使用してトラフィッククラスを定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィッククラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラスマップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

トンネルグループでフローベースのポリシーアクションを有効にするには、**match flow ip destination-address** と **match tunnel-group** コマンドを、**class-map**、**policy-map**、および **service-policy** コマンドとともに使用します。フローを定義する基準は、宛先 IP アドレスです。

固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。ポリシーのアクションは、トラフィックのクラス全体ではなく各フローに適用されます。QoS アクションポリシーを適用するには、**match flow ip destination-address** コマンドを使用します。トンネルグループ内の各トンネルを指定されたレートに規制するには、**match tunnel-group** を使用します。

例

次の例では、トンネル グループ内でフローベースのポリシングをイネーブルにして、指定のレートに各トンネルを制限する方法を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラスマップ内のアクセス リスト トラフィックを指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。
tunnel-group	VPN の接続固有レコードを格納するデータベースを作成し、管理します。

match header（ポリシー マップ タイプ インスペクション ESMTP）

ESMTPヘッダーの一致条件を設定するには、ポリシーマップタイプインスペクションESMTPコンフィギュレーション モードで **match header** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match ［ **not** ］ **header** ［ ［ **length** | **line length** ］ **gt** *bytes* | **to-fields count gt** *to_fields_number* ］
no match ［ **not** ］ **header** ［ ［ **length** | **line length** ］ **gt** *bytes* | **to-fields count gt** *to_fields_number* ］

構文の説明

length gt bytes	ESMTP ヘッダー メッセージの長さを照合することを指定します。
line length gt bytes	ESMTP ヘッダー メッセージの 1 行の長さを照合することを指定します。
to-fields count gt to_fields_number	To: フィールドの数を照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ タイプ インスペクション ESMTP コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ESMTP インスペクション ポリシー マップにヘッダーに関して一致条件を設定する例を示します。

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match header length gt 512**

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match header（ポリシー マップ タイプ インスペクション IPv6）

IPv6 ヘッダーの一致条件を設定するには、ポリシー マップ タイプ インスペクション IPv6 コンフィギュレーション モードで **match header** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **header** { **ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** { **eq** | **range** } *number* }
no match [**not**] **header** { **ah** | **count gt** *number* | **destination-option** | **esp** | **fragment** | **hop-by-hop** | **routing-address count gt** *number* | **routing-type** { **eq** | **range** } *number* }

構文の説明

ah	IPv6 認証拡張ヘッダーを照合します。
count gt *number*	IPv6 拡張ヘッダーの最大数（0 ～ 255）を指定します。
destination-option	IPv6 宛先オプション拡張ヘッダーを照合します。
esp	IPv6 カプセル化セキュリティ ペイロード（ESP）拡張ヘッダーを照合します。
fragment	IPv6 フラグメント拡張ヘッダーを照合します。
hop-by-hop	IPv6 ホップバイホップ拡張ヘッダーを照合します。
not	（オプション）指定したパラメータを照合しません。
routing-address count gt *number*	IPv6 ルーティング ヘッダー タイプ 0 のアドレスの最大数として、0 ～ 255 の数値よりも大きい値を設定します。
routing-type {**eq** | **range**} *number*	IPv6 ルーティング ヘッダー タイプ（0 ～ 255）を照合します。範囲を指定するには、値をスペースで区切ります（例：**30 40**）

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ タイプ インスペクション IPv6 コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

照合するヘッダーを指定します。デフォルトでは、パケットはログに記録されます（**log**）。パケットを破棄する場合は、一致コンフィギュレーション モードで **drop** コマンドを入力します（必要に応じて、**log** コマンドを入力してログに記録することもできます）。

照合する拡張ごとに、**match** コマンドと **drop** アクション（オプション）を再入力します。

例

次に、ヘッダーが hop-by-hop、destination-option、routing-address、および routing type 0 であるすべての IPv6 パケットを破棄してログに記録するインスペクション ポリシー マップを作成する例を示します。

```
policy-map type inspect ipv6 ipv6-pm
 parameters
 match header hop-by-hop
  drop log
 match header destination-option
  drop log
 match header routing-address count gt 0
  drop log
 match header routing-type eq 0
  drop log
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。

コマンド	説明
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match header-flag

DNS ヘッダーフラグに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match header-flag** コマンドを使用します。設定されたヘッダーフラグを削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **header-flag** [**eq**] { *f_well_known* | *f_value* }
no match [**not**] **header-flag** [**eq**] { *f_well_known* | *f_value* }

構文の説明

eq	完全一致を指定します。設定されていない場合は、match-all ビット マスク照合を指定します。
f_well_known	既知の名前で DNS ヘッダー フラグ ビットを指定します。複数のフラグ ビットを入力し、論理 OR を適用することもできます。 QR（Query、（注）QR=1、DNS 応答を示します） AA（Authoritative Answer） TC（TrunCation） RD（Recursion Desired） RA（Recursion Available）
f_value	任意の 16 ビット値を 16 進数形式で指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、DNS クラス マップまたは DNS ポリシー マップで設定できます。DNS クラス マップでは、入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS ヘッダー フラグに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match header-flag AA
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match im-subscriber

SIP IM 加入者に関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match im-subscriber** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **im-subscriber regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class regex_class_name	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次に、SIP インスペクション クラス マップに SIP IM 加入者に関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match im-subscriber regex class im_sender
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match interface

指定されたインターフェイスのいずれかを起点とするネクストホップが存在するルートを配布するには、ルート マップ コンフィギュレーション モードで **match interface** コマンドを使用します。match interface エントリを削除するには、このコマンドの **no** 形式を使用します。

match interface *interface-name*
no match interface *interface-name*

構文の説明

interface-name	インターフェイスの名前（物理インターフェイスではありません）。複数のインターフェイス名を指定できます。

コマンド デフォルト

一致インターフェイスは定義されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

コマンド構文内の省略記号（...）は、コマンドを入力するときに、interface-type interface-number 引数に対応する値を複数指定できることを意味します。

route-map global コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用すると、あるルーティングプロトコルから別のルーティングプロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、そのコマンドに関連付けられた **match** および **set** コマンドがあります。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドは、ルートマップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で指定できます。**set** コマンドで指定した設定アクションに従ってルー

トを再配布するには、すべての **match** コマンドで「一致」する必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。**match** コマンドで複数のインターフェイスが指定されている場合は、**no match interface** interface-name を使用して 1 つのインターフェイスを削除できます。

ルートマップは、いくつかの部分にわかれている可能性があります。**route-map** コマンドに関係のあるいずれの match 句とも一致しないルートは無視されます。一部のデータだけを変更する場合は、別のルート マップ セクションを設定し、明示的な一致を指定します。

例

次に、ネクスト ホップが外部のルートを配布する例を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match interface outside
```

関連コマンド

コマンド	説明
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
match ip route-source	アクセス リストで指定されたアドレスにあるルータおよびアクセス サーバーによってアドバタイズされたルートを再配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match invalid-recipients

ESMTP 無効受信者アドレスに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match invalid-recipients** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **invalid-recipients count gt** *number*
no match [**not**] **invalid-recipients count gt** *number*

構文の説明

count gt number	無効な受信者数を照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ESMTP インスペクション ポリシー マップに無効な受信者数に関して一致条件を設定する例を示します。

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match invalid-recipients count gt 1000**

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。

コマンド	説明
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match ip address

指定したいずれかのアクセスリストによって渡されるルートアドレスまたはマッチパケットがあるルートを再配布するには、ルートマップコンフィギュレーションモードで **match ip address** 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。

match ip address { *acl* . . . } **prefix-list**
no match ip address { *acl* . . . } **prefix-list**

構文の説明

acl	アクセスリストの名前を指定します。複数のアクセスリストを指定できます。
prefix-list	照合するプレフィックスリストの名前を指定します。

コマンドデフォルト

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルートマップコンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチコンテキストモードのサポートが追加されました。

使用上のガイドライン

route-map global コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用すると、あるルーティングプロトコルから別のルーティングプロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、そのコマンドに関連付けられた **match** および **set** コマンドがあります。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドは、ルートマップを削除します。

例

次の例では、内部ルートを再配布する方法を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip address acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
match ipv6 address	指定したいずれかのアクセス リストによって渡される IPv6 ルート アドレスまたはマッチ パケットがあるルートを再配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match ip next-hop

指定されたいずれかのアクセスリストによって渡されるネクストホップ ルータ アドレスがあるルートを再配布するには、ルートマップ コンフィギュレーション モードで **match ip next-hop** コマンドを使用します。ネクストホップエントリを削除するには、このコマンドの **no** 形式を使用します。

match ip next-hop { *acl . . .* } | **prefix-list** *prefix_list*
no match ip next-hop { *acl . . .* } | **prefix-list** *prefix_list*

構文の説明

acl	ACL の名前です。複数の ACL を指定できます。
prefix-list *prefix_list*	プレフィックス リストの名前です。

コマンド デフォルト

ルートは自由に配布されます。ネクストホップ アドレスを照合する必要はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

コマンド構文に含まれる省略符号（...）は、コマンド入力に *acl* 引数の値を複数含めることができることを示します。

route-map global コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用すると、あるルーティングプロトコルから別のルーティングプロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、そのコマンドに関連付けられた **match** および **set** コマンドがあります。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドは、ルートマップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートを再配布するには、すべての **match** コマンドで「一致」する必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルートがルート マップを通過するようにするときには、ルート マップに複数の要素を持たせることができます。 **route-map** コマンドに関係のあるいずれの match 句とも一致しないルートは無視されます。一部のデータのみを修正するには、別のルート マップ セクションを設定して、正確に一致する基準を指定する必要があります。

例

次に、アクセス リスト acl_dmz1 または acl_dmz2 によって渡されるネクストホップ ルータ アドレスがあるルートを配布する例を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip next-hop acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match ip route-source

ACLに指定されているアドレスにあるルータおよびアクセスサーバーによってアドバタイズされたルートを再配布するには、ルート マップ コンフィギュレーション モードで **match ip route-source** コマンドを使用します。ネクストホップエントリを削除するには、このコマンドの **no** 形式を使用します。

match ip route-source { *acl* . . . } **prefix-list** *prefix_list*
match ip route-source { *acl* . . . }

構文の説明

acl	ACLの名前です。複数のACLを指定できます。
prefix_list	プレフィックス リストの名前です。

コマンド デフォルト

ルート送信元でのフィルタリングはありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチコンテキストモードのサポートが追加されました。

使用上のガイドライン

コマンド構文に含まれる省略符号（...）は、コマンド入力にaccess-list-name引数の値を複数含めることができることを示します。

route-map global コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用すると、あるルーティングプロトコルから別のルーティングプロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、そのコマンドに関連付けられた **match** および **set** コマンドがあります。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドは、ルートマップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートを再配布するには、すべての **match** コマンドで「一致」する必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルートマップは、いくつかの部分にわかれている可能性があります。**route-map** コマンドに関係のあるいずれの match 句とも一致しないルートは無視されます。一部のデータのみを修正するには、別のルート マップ セクションを設定して、正確に一致する基準を指定する必要があります。ルートのネクストホップ アドレスと送信元ルータ アドレスが同じではない場合があります。

例

次に、acl_dmz1 および acl_dmz2 という ACL で指定されたアドレスにあるルータおよびアクセス サーバーによってアドバタイズされたルートを配布する例を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ip route-source acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したいずれかの ACL によって渡されたネクストホップ ルータ アドレスを持つ、すべてのルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match ipv6 address

指定したいずれかのアクセスリストによって渡されるIPv6ルートアドレスまたはマッチパケットがあるルートを再配布するには、ルート マップ コンフィギュレーション モードで **match ipv6 address** 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。

match ipv6 address { *acl . . .* } **prefix-list**
no match ipv6 address { *acl . . .* } **prefix-list**

構文の説明

acl	アクセス リストの名前を指定します。複数のアクセス リストを指定できます。
prefix-list	照合するプレフィックス リストの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

route-map global コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用すると、あるルーティングプロトコルから別のルーティングプロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、そのコマンドに関連付けられた **match** および **set** コマンドがあります。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドは、ルートマップを削除します。

例

次に、内部ルートを再配布する例を示します。access-list acl_dmz1 extended permit ipv6 any <net> <mask>

```
ciscoasa(config)# access-list acl_dmz1 extended permit ipv6 any <net> <mask>
```

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match ipv6 address acl_dmz1 acl_dmz2
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを配布します。
match ip address	指定したいずれかのアクセス リストによって渡されるルート アドレスまたはマッチ パケットがあるルートを再配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクスト ホップ ルータ アドレスを持つルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match login-name

インスタントメッセージ用のクライアントログイン名に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match login-name** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **login-name regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class regex_class_name	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにクライアント ログイン名に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match login-name regex login
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match media-type

H.323 メディアタイプに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match media-type** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **media-type** [**audio** | **data** | **video**]
no match [**not**] **media-type** [**audio** | **data** | **video**]

構文の説明

audio	オーディオ メディア タイプを照合することを指定します。
data	データ メディア タイプを照合することを指定します。
video	ビデオ メディア タイプを照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション クラス マップにオーディオ メディア タイプに関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match media-type audio
```

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。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match message class

M3UA メッセージのメッセージクラスおよびタイプに対して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match message class** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message class** *class_id* [**id** *message_id*]
no match [**not**] **message class** *class_id* [**id** *message_id*]

構文の説明

class_id	メッセージ クラス。サポートされているクラスとタイプのリストについては、「使用上のガイドライン」を参照してください。
id *message_id*	指定されているクラス内のメッセージ タイプ。

コマンド デフォルト

M3UA インスペクションでは、レート制限なしにすべてのメッセージ クラスおよびタイプが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドはM3UA インスペクション ポリシー マップで設定できます。メッセージ クラスおよびタイプに基づいてパケットをドロップまたはレート制限できます。次の表に、使用可能な値を示します。これらのメッセージの詳細については、M3UA のRFC およびドキュメンテーションを参照してください。

M3UA メッセージ クラス	メッセージ ID タイプ
0（管理メッセージ）	0 ～ 1
1（転送メッセージ）	1

M3UA メッセージ クラス	メッセージ ID タイプ
2（SS7 シグナリング ネットワーク管理メッセージ）	1 ～ 6
3（ASP 状態メンテナンス メッセージ）	1 ～ 6
4（ASP トラフィック メンテナンス メッセージ）	1 ～ 4
9（ルーティング キー管理メッセージ）	1 ～ 4

例

次に、M3UA メッセージに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match message class 2 id 6
ciscoasa(config-pmap-c)# drop
ciscoasa(config-pmap-c)# match message class 9
ciscoasa(config-pmap-c)# drop
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match message id

GTP メッセージ ID の一致条件を設定するには、ポリシーマップ コンフィギュレーション モードで **match message id** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message** { **v1** | **v2** } **id** [*message_id* | **range** *lower_range upper_range* }
no match [**not**] **message** { **v1** | **v2** } **id** [*message_id* | **range** *lower_range upper_range* }

構文の説明

{**v1** | **v2**}	（9.5(1) 以降）GTP のバージョンを示します。GTPv0 ～ 1 の場合は **v1**、GTPv2 の場合は **v2** を使用します。
message_id	メッセージ ID。1 ～ 255 を指定できます。
range *lower_range upper_range*	メッセージ ID の範囲。範囲の下限と上限を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.5(1)	{**v1** | **v2**} キーワードが追加されました。

使用上のガイドライン

このコマンドは、GTP ポリシー マップで設定できます。

例

次に、GTP インスペクション ポリシー マップにメッセージ ID に関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match message id 33
```

リリース 9.5(1) 以降では、{**v1** | **v2**} キーワードを追加する必要があります。

```
ciscoasa(config-pmap)# match message v2 id 33
```

関連コマンド

コマンド	説明
inspect gtp	GTP トラフィックのインスペクションを設定します。

match message length

GTP メッセージ ID の一致条件を設定するには、ポリシーマップ コンフィギュレーション モードで **match message length** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message length min** *min_length* **max** *max_length*
no match [**not**] **message length min** *min_length* **max** *max_length*

構文の説明

min *min_length*	メッセージ ID の最小の長さを指定します。値の範囲は 1 ～ 65536 です。
max *max_length*	メッセージ ID の最大の長さを指定します。値の範囲は 1 ～ 65536 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、GTP ポリシー マップで設定できます。

例

次に、GTP インスペクション ポリシーマップにメッセージの長さに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match message length min 8 max 200
```

関連コマンド

コマンド	説明
inspect gtp	GTP トラフィックのインスペクションを設定します。

コマンド	説明
match message id	メッセージIDに基づいてトラフィックを照合します。

match message-path

Via ヘッダーフィールドの指定に従って SIP メッセージが通過するパスに関する一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match message-path** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **message-path regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class regex_class_name	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次の例では、SIP インスペクション クラス マップで SIP メッセージによって取得されるパスの一致条件を設定する方法を示します。

```
ciscoasa(config-cmap)# match message-path regex class sip_message
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match metric

指定されたメトリックを持つルートを再配布するには、ルート マップ コンフィギュレーション モードで **match metric** コマンドを使用します。エントリを削除するには、このコマンドの **no** 形式を使用します。

match metric *number*
no match metric *number*

構文の説明

number	ルート メトリック（5 つの部分からなる IGRP のメトリック）。有効な値は 0 ～ 4294967295 です。

コマンド デフォルト

メトリック値に関するフィルタリングを行いません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

route-map global コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用すると、あるルーティングプロトコルから別のルーティングプロトコルにルートを再配布するための条件を定義できます。各 **route-map** コマンドには、そのコマンドに関連付けられた **match** および **set** コマンドがあります。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドは、ルートマップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドの順序は任意に指定できます。すべての **match** コマンドが満たされないと、**set** コマンドで指定した設定アクションに従ってルートの再配布が行われません。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルートマップは、いくつかの部分にわかれている可能性があります。**route-map** コマンドに関係のあるいずれの match 句とも一致しないルートは無視されます。一部のデータのみを修正するには、別のルート マップ セクションを設定して、正確に一致する基準を指定する必要があります。

例

次に、メトリックが 5 のルートを再配布する例を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match metric 5
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクストホップ ルータ アドレスを持つルートを配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match mime

ESMTP MIME エンコーディングタイプ、MIME ファイル名の長さ、または MIME ファイルタイプに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match mime** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **mime** [**encoding** *type* | **filename length gt** *bytes* | **filetype** *regex*]
no match [**not**] **mime** [**encoding** *type* | **filename length gt** *bytes* | **filetype** *regex*]

構文の説明

encoding type	エンコーディング タイプを照合することを指定します。
filename length gt bytes	ファイル名の長さを照合することを指定します。
filetype regex	ファイル タイプを照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ESMTP インスペクション ポリシー マップに MIME ファイル名の長さに関して一致条件を設定する例を示します。

```
ciscoasa
(config)#
 policy-map type inspect esmtp esmtp_map
```

ciscoasa (config-pmap)# **match mime filename length gt 255**

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match msisdn

Create PDP Context 要求、Create Session 要求、および Modify Bearer Response メッセージの GTP モバイルステーション国際サブスクライバディレクトリ番号（MSISDN）情報要素の一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match msisdn** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **msisdn regex** { *regex_name* | **class** *class_name* }
no match [**not**] **msisdn regex** { *regex_name* | **class** *class_name* }

構文の説明

regex_name	正規表現オブジェクトの名前。
class *class_name*	正規表現クラスの名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(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、GTP ポリシー マップで設定できます。

Create PDP Context 要求のモバイル ステーション国際サブスクライバ ディレクトリ番号（MSISDN）情報要素をフィルタリングできます。特定の MSISDN に基づいて、または最初の x 桁数に応じた MSISDN の範囲に基づいて、メッセージをドロップしたり、必要に応じてログに記録したりできます。MSISDN を指定するには、正規表現を使用します。MSISDN フィルタリングは GTPv1 および GTPv2 のみでサポートされています。

例

次に、正規表現オブジェクトを使用して MSISDN 一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match msisdn regex msisdn1
ciscoasa(config-pmap-c)# drop log
```

次に、正規表現クラスを使用して MSISDN 一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match msisdn regex class msisdn2
ciscoasa(config-pmap-c)# drop log
```

関連コマンド

コマンド	説明
drop	基準に一致するパケットをドロップします。
log	基準に一致するパケットをログに記録します。
inspect gtp	GTP アプリケーション インスペクションをイネーブルにします。
policy-map type inspect gtp	GTP インスペクション ポリシー マップを作成または編集します。

match opc

M3UAデータメッセージの発信ポイントコード（OPC）に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match opc** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match ［ **not** ］ **opc** *code*
no match ［ **not** ］ **opc** *code*

構文の説明

code	*zone -region -sp* 形式の発信ポイントコード。

コマンド デフォルト

M3UA インスペクションでは、すべての発信ポイント コードが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドはM3UA インスペクション ポリシーマップで設定できます。発信ポイント コードに基づいてパケットをドロップできます。ポイントコードは *zone -region -sp* 形式で、各要素に使用可能な値は SS7 バリアントによって異なります。バリアントはポリシーマップの **ss7 variant** コマンドで定義できます。

- ITU：ポイント コードは 14 ビットで 3-8-3 形式です。値の範囲は、[0-7]-[0-255]-[0-7] です。これは、デフォルトの SS7 バリエーションです。
- ANSI：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。
- Japan：ポイント コードは 16 ビットで 5-4-7 形式です。値の範囲は、[0-31]-[0-15]-[0-127] です。

- China：ポイント コードは 24 ビットで 8-8-8 形式です。値の範囲は、[0-255]-[0-255]-[0-255] です。

例

次に、ITU の特定の発信ポイント コードに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match opc 1-5-1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# ss7 variant ITU
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
match dpc	M3UA 宛先ポイント コードと一致させます。
policy-map type inspect	インスペクション ポリシー マップを作成します。
ss7 variant	ポリシー マップで使用する SS7 バリアントを指定します。

match peer-ip-address

インスタントメッセージのピア IP アドレスに関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match peer-ip-address** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **peer-ip-address** *ip_address ip_address_mask*
no match [**not**] **peer-ip-address** *ip_address ip_address_mask*

構文の説明

ip_address	クライアントまたはサーバーのホスト名またはIPアドレスを指定します。
ip_address_mask	クライアントまたはサーバー IP アドレスのネットマスクを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにピア IP アドレスに関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-ip-address 10.1.1.0 255.255.255.0
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match peer-login-name

インスタントメッセージのピアログイン名に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match peer-login-name** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **peer-login-name regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class regex_class_name	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにピア ログイン名に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match peer-login-name regex peerlogin
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match port

モジュラ ポリシー フレームワークを使用する場合、クラスマップ コンフィギュレーション モードで**match port** コマンドを使用して、アクションを適用するポートを照合します。 **match port** コマンドを削除するには、このコマンドの **no** 形式を使用します。

match port { **tcp** | **udp** | **sctp** } { **eq** *port* | **range** *beg_port end_port* }
no match port { **tcp** | **udp** | **sctp** } { **eq** *port* | **range** *beg_port end_port* }

構文の説明

eq *port*	単一のポート名またはポート番号を指定します。
range *beg_port end_port*	ポート範囲の開始値および終了値を 1 ～ 65535 の範囲で指定します。
tcp	TCP ポートを指定します。
sctp	SCTP ポートを指定します。
udp	UDP ポートを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.7(1)	**sctp** キーワードが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを指定します。

class-map コマンドの入力後に、**match port** コマンドを入力してトラフィックを指定します。あるいは、 **match access-list** コマンドなど、別のタイプの **match** コマンドを入力できます（**class-map type management** コマンドでのみ match port コマンドが許可されます）。クラスマップには **match port** コマンドを 1 つだけ含めることができ、他のタイプの **match** コマンドと組み合わせることはできません。

1. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
2. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
3. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

例

次に、クラスマップおよび **match port** コマンドを使用して、トラフィック クラスを定義する例を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq 8080
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match access-list	アクセス リストに従ってトラフィックを照合します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match ppid

SCTP インスペクションのためにペイロードプロトコル ID（PPID）に関して一致条件を設定するには、インスペクション ポリシー マップ コンフィギュレーション モードで **match ppid** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **ppid** *ppid_1* [*ppid_2*]
no match [**not**] **ppid** *ppid_1* [*ppid_2*]

構文の説明

ppid_1 [*ppid_2*]	PPID 番号（0 ～ 4294967295）または名前で SCTP PPID を指定します（使用可能な名前については、CLI ヘルプを参照）。範囲を指定するための 2 つ目の（より大きな） PPID を含めることができます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
インスペクション ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SCTP インスペクション ポリシーマップで設定できます。このコマンドを使用すると、PPID に対してフィルタ処理を行い、それらの ID に特別なアクション（ドロップ、ログ、レート制限など）を適用できます。

PPID に対してフィルタ処理を行う場合は、次の点に注意してください。

- PPID はデータ チャンクに含まれており、1 つのパケットが複数のデータ チャンクを持つ場合があります。パケットに異なる PPID を持つデータ チャンクが含まれている場合、パケットはフィルタ処理されず、割り当てられたアクションがパケットに適用されません。
- PPID フィルタリングを使用してパケットをドロップまたはレート制限する場合は、トランスミッタによりドロップされたパケットが再送されることに注意してください。レート

制限が適用された PPID のパケットは再試行で通過する可能性がありますが、ドロップされたPPIDのパケットは再びドロップされます。ネットワーク上のこのような反復的ドロップの最終成果を評価することができます。

例

次に、未割り当ての PPID （この例の作成時点で未割り当て）をドロップし、PPID 32 ～ 40 にレート制限を適用し、Diameter PPID をログに記録する SCTP インスペクション ポリシー マップを作成する例を示します。

```
policy-map type inspect sctp sctp-pmap
 match ppid 58 4294967295
  drop
 match ppid 26
  drop
 match ppid 49
  drop
 match ppid 32 40
  rate-limit 1000
 match ppid diameter
  log
```

関連コマンド

コマンド	説明
drop	一致するトラフィックをドロップします。
inspect sctp	SCTP インスペクションをイネーブルにします。
log	一致するトラフィックをログに記録します。
policy-map type inspect sctp	SCTPインスペクション ポリシーマップを作成します。
rate-limit	一致するトラフィックにレート制限を適用します。

match precedence

クラスマップに precedence 値を指定するには、クラス マップ コンフィギュレーション モードで **match precedence** 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。

matchprecedence*value*
nomatchprecedence値

構文の説明

value	最大 4 つの precedence 値をスペースで区切って指定します。指定できる範囲は、0 ～ 7 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、クラスマップのトラフィッククラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラスマップに含まれるトラフィックを定義するさまざまな基準が含まれています。モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定する一環として、**class-map** グローバル コンフィギュレーション コマンドを使用してトラフィッククラスを定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィッククラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラスマップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

IP ヘッダーに TOS バイトで表される値を指定するには、**match precedence** コマンドを使用します。

例

次に、クラスマップおよび **match precedence** コマンドを使用して、トラフィッククラスを定義する例を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 precedence 1
ciscoasa(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラスマップ内のアクセスリストトラフィックを指定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match protocol

MSN や Yahoo などの特定のインスタント メッセージ プロトコルに関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match protocol** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **protocol** { **msn-im** | **yahoo-im** }
no match [**not**] **protocol** { **msn-im** | **yahoo-im** }

構文の説明

msn-im	MSN インスタント メッセージング プロトコルを照合することを指定します。
yahoo-im	Yahoo インスタント メッセージング プロトコルを照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップに Yahoo インスタント メッセージング プロトコルに関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match protocol yahoo-im
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match question

DNS の質問またはリソースレコードに関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match question** コマンドを使用します。設定されたセクションを削除するには、このコマンドの **no** 形式を使用します。

match { **question** | { **resource-record answer** | **authority** | **additional** } }
no match { **question** | { **resource-record answer** | **authority** | **additional** } }

構文の説明

question	DNS メッセージの質問部分を指定します。
resource-record	DNS メッセージのリソース レコード部分を指定します。
answer	Answer RR セクションを指定します。
authority	Authority RR セクションを指定します。
additional	Additional RR セクションを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、このコマンドは DNS ヘッダーを調べ、指定されたフィールドとマッチングします。また、他の DNS match コマンドと併用して、特定の質問または RR タイプのインスペクションを定義できます。

このコマンドは、DNS クラス マップまたは DNS ポリシー マップ内で設定できます。DNS クラス マップ内で入力できるエントリは 1 つのみです。

例

次に、DNS インスペクション ポリシー マップに DNS 質問に関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# match question
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match r – me

match regex

正規表現クラスマップで正規表現を識別するには、クラスマップタイプ正規表現コンフィギュレーション モードで **match regex** コマンドを使用します。クラスマップから正規表現を削除するには、このコマンドの **no** 形式を使用します。

match regex *name*
no match regex *name*

構文の説明

name	**regex** コマンドを使用して追加した正規表現の名前。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップ タイプ正規表現コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(2)	このコマンドが追加されました。

使用上のガイドライン

regex コマンドは、テキスト照合が必要なさまざまな機能で使用できます。正規表現は、**class-map type regex** コマンドの後に複数の **match regex** コマンドを使用して、正規表現クラスマップにグループ化できます。

たとえば、インスペクション ポリシー マップを使用して、アプリケーション インスペクションの特別なアクションを設定できます（**policy map type inspect** コマンドを参照）。インスペクション ポリシー マップでは、1 つ以上の **match** コマンドを含んだインスペクション クラスマップを作成することで、アクションの実行対象となるトラフィックを識別できます。または、**match** コマンドをインスペクション ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケット内のテキストを正規表現を使用して識別できます。たとえば、HTTP パケット内の URL 文字列を照合できます。

例

次の例では、HTTP インスペクション ポリシー マップとその関連クラス マップを示します。このポリシー マップは、サービス ポリシーがイネーブルにするレイヤ 3/4 ポリシー マップによってアクティブになります。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match regex url_example
ciscoasa(config-cmap)# match regex url_example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
 [a Layer 3/4 class map not shown]
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy test interface outside
```

関連コマンド

コマンド	説明
class-map type regex	正規表現クラスマップを作成します。
regex	正規表現を追加します。
test regex	正規表現をテストします。

match req-resp

HTTP 要求と応答の両方に関して一致条件を設定するには、ポリシーマップ コンフィギュレーション モードで **match req-resp** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match ［ **not** ］ **req-resp content-type mismatch**
no match ［ **not** ］ **req-resp content-type mismatch**

構文の説明

content-type mismatch	HTTP 応答の content-type フィールドが対応する HTTP 要求メッセージの accept フィールドと一致しないトラフィックを照合します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、次のチェックを行うことができます。

- content-type ヘッダーの値がサポート対象コンテンツ タイプの内部リストにあることを確認します。
- ヘッダー content-type が、メッセージのデータまたはエンティティ本文の実際のコンテンツに一致することを確認します。
- HTTP 応答の content type フィールドが、対応する HTTP 要求メッセージの **accept** フィールドと一致することを確認します。

メッセージが前述のいずれかのチェックに失敗した場合、ASA は設定されたアクションを実行します。

次に、サポート対象コンテンツ タイプのリストを示します。

audio/* |	audio/basic |	video/x-msvideo
audio/mpeg |	audio/x-adpcm |	audio/midi
audio/x-ogg |	audio/x-wav |	audio/x-aiff |
application/octet-stream	application/pdf	application/msword
application/vnd.ms-excel	application/vnd.ms-powerpoint	application/postscript
application/x-java-arching	application/x-msn-messenger	application/x-gzip
image |	application/x-java-xm	application/zip
image/jpeg |	image/cgf |	image/gif |
image/x-3ds |	image/png |	image/tiff |
image/x-portable-bitmap |	image/x-bitmap |	image/x-niff |
text/* |	image/x-portable-greymap |	image/x-xpm |
text/plain |	text/css	text/html |
text/xmcd	text/richtext |	text/sgml
video/-flc	text/xml	video/*
video/sgi	video/mpeg	video/quicktime
video/x-mng	video/x-avi	video/x-fli

このリストのコンテンツ タイプの中には、メッセージの本文部分で確認できないように、対応する正規表現（magic number）がないものがあります。この場合、HTTP メッセージは許可されます。

例

次に、HTTP ポリシーマップで HTTP メッセージのコンテンツ タイプに基づいて HTTP トラフィックを制限する例を示します。

```
ciscoasa
(config)#
 policy-map type inspect http http_map
ciscoasa
(config-pmap)#
 match req-resp content-type mismatch
```

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。

コマンド	説明
clear configure class-map	すべてのクラス マップを削除します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request-command

特定の FTP コマンドを制限するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match request-command** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **request-command** *ftp_command* [*ftp_command* . . .]
no match [**not**] **request-command** *ftp_command* [*ftp_command* . . .]

構文の説明

ftp_command	制限する FTP コマンドを 1 つ以上指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション ポリシー マップに特定の FTP コマンドに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ftp ftp_map1
ciscoasa(config-pmap)# match request-command stou
```

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。

コマンド	説明
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request-method

SIP メソッドタイプに関して一致条件を設定するには、クラスマップまたはポリシーマップ コンフィギュレーション モードで **match request-method** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **request-method** *method_type*
no match [**not**] **request-method** *method_type*

構文の説明

method_type RFC 3261 およびサポートされている拡張に従って、メソッド タイプを指定します。サポートされているメソッド タイプには、ack、bye、cancel、info、invite、message、notify、options、prack、refer、register、subscribe、unknown、update があります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次の例では、SIP インスペクション クラス マップで SIP メッセージによって取得されるパスの一致条件を設定する方法を示します。

```
ciscoasa(config-cmap)# match request-method ack
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match request method

HTTP 要求に関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match request method** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **request** { *built-in-regex* | **regex** { **regex_name** | **class** *class_map_name* } }
no match [**not**] **request** { *built-in-regex* | **regex** { **regex_name** | **class** *class_map_name* } }

構文の説明

built-in-regex	コンテンツ タイプ、方法、または転送エンコーディングの組み込みの正規表現を指定します。
class *class_map name*	正規表現タイプのクラス マップの名前を指定します。
regex *regex_name*	**regex** コマンドを使用して設定されている正規表現の名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

表 *4:* 組み込みの正規表現値

bcopy	bdelete	bmove	bpropfind
bproppatch	connect	copy	delete
edit	get	getattribute	getattributenames
getproperties	head	index	lock
mkcol	mkdir	move	notify

options	poll	post	propfind
proppatch	put	revadd	revlabel
revlog	revnum	save	search
setattribute	startrev	stoprev	subscribe
trace	unedit	unlock	unsubscribe

例

次に、「GET」メソッドまたは「PUT」メソッドで「www\.example.com/.*\.asp」または「www\example[0-9][0-9]\.com」にアクセスしようとしている HTTP 接続を許可し、ロギングする HTTP インスペクション ポリシー マップを定義する例を示します。それ以外の URL/メソッドの組み合わせは、サイレントに許可されます。

```
ciscoasa(config)# regex url1 "www\.example.com/.*\.asp
ciscoasa(config)# regex url2 "www\.example[0-9][0-9]\.com"
ciscoasa(config)# regex get "GET"
ciscoasa(config)# regex put "PUT"
ciscoasa(config)# class-map type regex match-any url_to_log
ciscoasa(config-cmap)# match regex url1
ciscoasa(config-cmap)# match regex url2
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type regex match-any methods_to_log
ciscoasa(config-cmap)# match regex get
ciscoasa(config-cmap)# match regex put
ciscoasa(config-cmap)# exit
ciscoasa(config)# class-map type inspect http http_url_policy
ciscoasa(config-cmap)# match request uri regex class url_to_log
ciscoasa(config-cmap)# match request method regex class methods_to_log
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map type inspect http http_policy
ciscoasa(config-pmap)# class http_url_policy
ciscoasa(config-pmap-c)# log
```

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。
clear configure class-map	すべてのクラス マップを削除します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match route-type

指定されたタイプのルートを再配布するには、ルートマップ コンフィギュレーション モードで **match route-type** コマンドを使用します。ルートタイプエントリを削除するには、このコマンドの **no** 形式を使用します。

match route-type { **local** | **internal** | { **external** [**type-1** | **type-2**] } | { **nssa-external** [**type-1** | **type-2**] } }
no match route-type { **local** | **internal** | { **external** [**type-1** | **type-2**] } | { **nssa-external** [**type-1** | **type-2**] } }

構文の説明

external	OSPF 外部ルートまたは EIGRP 外部ルート。
internal	OSPF エリア内およびエリア間ルート、または EIGRP 内部ルート
local	ローカルに生成された BGP ルート。
nssa-external	外部 NSSA を指定します。
type-1	（任意）ルート タイプ 1 を指定します。
type-2	（任意）ルート タイプ 2 を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルート マップ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

route-map グローバル コンフィギュレーション コマンド、**match** および **set** コンフィギュレーション コマンドを使用すると、あるルーティング プロトコルから別のルーティング プロトコル

にルートを再配布するための条件を定義できます。各 **route-map** コマンドには、そのコマンドに関連付けられた **match** および **set** コマンドがあります。**match** コマンドは、一致基準（現在の **route-map** コマンドで再配布が許可される条件）を指定します。**set** コマンドは、設定アクション（**match** コマンドが指定している基準を満たした場合に実行する特定の再配布アクション）を指定します。**no route-map** コマンドは、ルートマップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。**match** コマンドは任意の順序で入力できます。**set** コマンドで指定した設定アクションに従ってルートを再配布するには、すべての **match** コマンドで「一致」する必要があります。**match** コマンドの **no** 形式を使用すると、指定した一致基準が削除されます。

ルートマップは、いくつかの部分にわかれている可能性があります。**route-map** コマンドに関係のあるいずれの match 句とも一致しないルートは無視されます。一部のデータのみを修正するには、別のルート マップ セクションを設定して、正確に一致する基準を指定する必要があります。

OSPF の場合、**external type-1** キーワードはタイプ 1 外部ルートにのみ一致し、**external type-2** キーワードはタイプ 2 外部ルートにのみ一致します。

例

次の例では、内部ルートを再配布する方法を示します。

```
ciscoasa(config)# route-map name
ciscoasa(config-route-map)# match route-type internal
```

関連コマンド

コマンド	説明
match interface	指定したいずれかのインターフェイスの外部にネクスト ホップを持つ、すべてのルートを再配布します。
match ip next-hop	指定したアクセス リストのいずれかによって渡されるネクストホップ ルータ アドレスを持つルートを配布します。
match metric	指定したメトリックを持つルートを再配布します。
route-map	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
set metric	ルート マップの宛先ルーティング プロトコルのメトリック値を指定します。

match rtp

クラスマップに偶数ポートの UDP ポート範囲を指定するには、クラス マップ コンフィギュレーション モードで **match rtp** 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。

match rtp *starting_port range*
no match rtp *starting_port range*

構文の説明

starting_port	偶数 UDP 宛先ポートの下限を指定します。指定できる範囲は、2000 ～ 65535 です。
range	RTP ポートの範囲を指定します。指定できる範囲は、0 ～ 16383 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、クラスマップのトラフィッククラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラスマップに含まれるトラフィックを定義するさまざまな基準が含まれています。モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定する一環として、**class-map** グローバル コンフィギュレーション コマンドを使用してトラフィッククラスを定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィッククラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラスマップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

RTP ポート（*starting_port* から *starting_port* に *range* を加えた値の範囲の偶数 UDP ポート番号）と照合するには、**match rtp** コマンドを使用します。

例

次に、クラスマップおよび **match rtp** コマンドを使用して、トラフィッククラスを定義する例を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 rtp 20000 100
ciscoasa(config-cmap)#
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラスマップ内のアクセスリストトラフィックを指定します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match selection-mode

Create PDP Context 要求の選択モード情報要素の一致を設定するには、ポリシー マップ コンフィギュレーション モードで **match selection-mode** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **selection-mode** *mode_value*
no match [**not**] **selection-mode** *mode_value*

構文の説明

mode_value Create PDP Context 要求の選択モード情報要素。選択モードでは、メッセージにアクセス ポイント名（APN）の発信元を指定しますが、次のいずれかになります。

- 0：確認済み。APN はモバイル ステーションまたはネットワークによって指定されており、サブスクリプションが確認されています。
- 1：モバイル ステーション。APN はモバイル ステーションによって指定されており、サブスクリプションは確認されていません。
- 2：ネットワーク。APN はネットワークによって指定されており、サブスクリプションは確認されていません。
- 3：予約済み（未使用）

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(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、GTP ポリシー マップで設定できます。

Create PDP Context 要求の選択モード情報要素をフィルタリングすることができます。選択モードでは、メッセージにアクセス ポイント名（APN）の発信元を指定します。これらのモードに基づいて、メッセージをドロップしたり、必要に応じてログに記録したりできます。選択モード フィルタリングは、GTPv1 および GTPv2 のみでサポートされています。

例

次の例では、選択モード 1 および 2 を照合し、それらのモードを持つ Create PDP Context メッセージをドロップしたり、ログに記録したりする方法を示しています。

```
ciscoasa(config)# policy-map type inspect gtp gtp-map
ciscoasa(config-pmap)# match selection-mode 1
ciscoasa(config-pmap-c)# drop log
ciscoasa(config-pmap)# match selection-mode 2
ciscoasa(config-pmap-c)# drop log
```

関連コマンド

コマンド	説明
drop	基準に一致するパケットをドロップします。
log	基準に一致するパケットをログに記録します。
inspect gtp	GTP アプリケーション インスペクションをイネーブルにします。
policy-map type inspect gtp	GTP インスペクション ポリシーマップを作成または編集します。

match sender-address

ESMTP 送信者電子メールアドレスに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match sender-address** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

match [**not**] **sender-address** [**length gt** *bytes* | **regex** *regex*]
no match [**not**] **sender-address** [**length gt** *bytes* | **regex** *regex*]

構文の説明

length gt *bytes*	送信者電子メールアドレスの長さを照合することを指定します。
regex *regex*	正規表現を照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ESMTP インスペクション ポリシー マップに長さが 320 文字を超える送信者電子メール アドレスに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match sender-address length gt 320
```

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。
clear configure class-map	すべてのクラス マップを削除します。

コマンド	説明
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match server

FTP サーバーに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match server** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **server regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

ASA は、FTP サーバーに接続するときにログインプロンプトの上方に表示される初期 220 サーバーメッセージに基づいて、サーバー名と照合します。220 サーバー メッセージには、行が複数含まれることがあります。サーバーとのマッチングは、DNS を介して解決されるサーバー名の FQDN に基づきません。

例

次に、FTP インスペクション ポリシー マップに FTP サーバーに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match server class regex ftp-server
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match service

特定のインスタント メッセージ サービスに関して一致条件を設定するには、クラス マップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match service** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] { **service** { **chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference** }
no match [**not**] { **service** { **chat** | **file-transfer** | **games** | **voice-chat** | **webcam** | **conference** }

構文の説明

chat	インスタント メッセージング チャット サービスを照合することを指定します。
file-transfer	インスタント メッセージング ファイル転送サービスを照合することを指定します。
games	インスタント メッセージング ゲーム サービスを照合することを指定します。
voice-chat	インスタント メッセージング音声チャット サービスを照合することを指定します。
webcam	インスタントメッセージング Web カメラ サービスを照合することを指定します。
conference	インスタント メッセージング会議サービスを照合することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IM クラス マップまたは IM ポリシー マップ内で設定できます。IM クラス マップに入力できるエントリは 1 つのみです。

例

次に、インスタント メッセージング クラス マップにチャット サービスに関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect im im_class
ciscoasa(config-cmap)# match service chat
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match service-indicator

M3UA メッセージのサービスインジケータに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match service-indicator** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **service-indicator** *number*
no match [**not**] **service-indicator** *number*

構文の説明

number サービス インジケータ番号（0 ～ 15）。サポートされているインジケータのリストについては、「使用上のガイドライン」を参照してください。

コマンド デフォルト

M3UA インスペクションでは、すべてのサービス インジケータが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは M3UA インスペクション ポリシー マップで設定できます。サービス インジケータに基づいてパケットをドロップできます。使用可能なサービスインジケータは次のとおりです。これらのサービス インジケータの詳細については、M3UA RFC およびドキュメントを参照してください。

- 0：シグナリング ネットワーク管理メッセージ
- 1：シグナリング ネットワーク テストおよびメンテナンス メッセージ
- 2：シグナリング ネットワーク テストおよびメンテナンス特別メッセージ
- 3：SCCP
- 4：電話ユーザー部
- 5：ISDN ユーザー部
- 6：データ ユーザー部（コールおよび回線関連のメッセージ）

- 7：データ ユーザー部（設備の登録およびキャンセル メッセージ）
- 8：MTP テスト ユーザー部に予約済み
- 9：ブロードバンド ISDN ユーザー部
- 10：サテライト ISDN ユーザー部
- 11：予約済み
- 12：AAL タイプ 2 シグナリング
- 13：ベアラー非依存コール制御
- 14：ゲートウェイ制御プロトコル
- 15：予約済み

例

次に、M3UA サービス インジケータに関して一致条件を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# match service-indicator 15
ciscoasa(config-pmap-c)# drop
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match third-party-registration

第三者登録の要求者に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match third-party-registration** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **third-party-registration regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

third-party registration match コマンドは、SIP 登録または SIP プロキシで他のユーザーを登録できるユーザーを特定するために使用されます。From と To の値が一致しない場合には、REGISTER メッセージの From ヘッダー フィールドで識別されます。

例

次に、SIP インスペクション クラス マップに第三者登録に関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match third-party-registration regex class sip_regist
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match tunnel-group

以前に定義したトンネルグループに属するクラスマップのトラフィックと照合するには、クラス マップ コンフィギュレーション モードで **match tunnel-group** 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。

matchtunnel-group*name*
nomatchtunnel-group*name*

構文の説明

name トンネル グループ名のテキスト。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

match コマンドは、クラスマップのトラフィッククラスに含まれているトラフィックを指定するために使用されます。これらのコマンドには、クラスマップに含まれるトラフィックを定義するさまざまな基準が含まれています。モジュラ ポリシー フレームワークを使用したセキュリティ機能を設定する一環として、**class-map** グローバル コンフィギュレーション コマンドを使用してトラフィッククラスを定義します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。

トラフィッククラスをインターフェイスに適用すると、そのインターフェイス上で受信したパケットは、クラスマップの **match** ステートメントで定義した基準と比較されます。指定した基準にパケットが一致すると、パケットはトラフィック クラスに含まれ、そのトラフィック クラスに関連付けられているアクションの対象になります。あらゆるトラフィック クラスのいずれの基準にも一致しないパケットは、デフォルトのトラフィック クラスに割り当てられます。

フローベースのポリシーアクションを有効にするには、**match flow ip destination-address** と **match tunnel-group** コマンドを、**class-map**、**policy-map**、および **service-policy** コマンドとも

に使用します。フローを定義する基準は、宛先 IP アドレスです。固有の IP 宛先アドレスに向かうトラフィックは、すべてフローと見なされます。ポリシーのアクションは、トラフィックのクラス全体ではなく各フローに適用されます。QoS アクションポリシーを適用するには、**police** コマンドを使用します。トンネルグループ内の各トンネルを指定されたレートに規制するには、 **match tunnel-group** とともに **match flow ip destination-address** を使用します。

例

次の例では、トンネル グループ内でフローベースのポリシングをイネーブルにして、指定のレートに各トンネルを制限する方法を示します。

```
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match
 tunnel-group
ciscoasa(config-cmap)# match flow ip destination-address
ciscoasa(config-cmap)# exit
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# police 56000
ciscoasa(config-pmap)# exit
ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class-map	トラフィック クラスをインターフェイスに適用します。
clear configure class-map	すべてのトラフィック マップ定義を削除します。
match access-list	クラスマップ内のアクセス リスト トラフィックを指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。
tunnel-group	IPsec および L2TP の接続固有レコードのデータベースを作成および管理します。

match uri

SIP ヘッダーの URI に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match uri** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **uri** { **sip** | **tel** } **length gt** *gt_bytes*
no match [**not**] **uri** { **sip** | **tel** } **length gt** *gt_bytes*

構文の説明

sip	SIP URI を指定します。
tel	TEL URI を指定します。
length gt *gt_bytes*	URI の最大長を指定します。値の範囲は、0 ～ 65536 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	— • 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、SIP クラス マップまたは SIP ポリシー マップ内で設定できます。SIP クラス マップに入力できるエントリは 1 つのみです。

例

次に、SIP メッセージの URI に関して一致条件を設定する例を示します。

```
ciscoasa(config-cmap)# match uri sip length gt
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match url-filter

RTSP メッセージの URL フィルタリングに関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match url-filter** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **url-filter regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、RTSP クラス マップまたはポリシー マップで設定できます。

例

次に、RTSP インスペクション ポリシー マップに URL フィルタリングに関して一致条件を設定する例を示します。

```
ciscoasa(config)# regex badurl www.example.com/rtsp.avi
ciscoasa(config)# policy-map type inspect rtsp rtsp-map
ciscoasa(config-pmap)# match url-filter regex badurl
ciscoasa(config-pmap-p)# drop-connection
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match user group

クラウドWebセキュリティのホワイトリストに追加するユーザーやグループを指定するには、クラス マップ コンフィギュレーション モードで **match user group** コマンドを使用します。一致を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] { [**user** *username*] [**group** *groupname*] }
no match [**not**] { [**user** *username*] [**group** *groupname*] }

構文の説明

not	（オプション）ユーザーやグループをクラウド Web セキュリティを使用してフィルタリングするように指定します。たとえば、グループ「cisco」をホワイトリストに登録し、ユーザー「johncrichton」および「aerynsun」からのトラフィックをスキャンする場合、これらのユーザーに **match not** を指定できます。
user *username*	ホワイトリストに追加するユーザーを指定します。
group *groupname*	ホワイトリストに追加するグループを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

AAA ルールまたは IDFW を使用する場合、その他の場合にはサービスポリシールールに一致する特定のユーザーやグループからの Web トラフィックが、スキャンのためにクラウド Web セキュリティ プロキシ サーバーにリダイレクトされないように ASA を設定できます。クラウド Web セキュリティスキャンをバイパスすると、ASA はプロキシサーバーに接続せず、最初に要求された Web サーバーからコンテンツを直接取得します。Web サーバーから応答を受け

取ると、データをクライアントに送信します。このプロセスはトラフィックの「ホワイトリスト」といいます。

ACL を使用してクラウド Web セキュリティに送信するトラフィックのクラスを設定すると、ユーザーまたはグループに基づいてトラフィックを免除する同じ結果を得ることができますが、ホワイトリストを使用した方がより簡単です。ホワイトリスト機能は、ユーザーおよびグループだけに基づき、IP アドレスには基づかないことに注意してください。

ホワイトリストをインスペクション ポリシー マップ（**policy-map type inspect scansafe**）の一部として作成しておくことで、**inspect scansafe** コマンドを使用してクラウド Web セキュリティのアクションを指定する際にそのマップを使用できます。

例

次に、HTTP および HTTPS インスペクション ポリシー マップの同じユーザーおよびグループをホワイトリストに記載する例を示します。

```
ciscoasa(config)# class-map type inspect scansafe match-any whitelist1
ciscoasa(config-cmap)# match user user1 group cisco
ciscoasa(config-cmap)# match user user2
ciscoasa(config-cmap)# match group group1
ciscoasa(config-cmap)# match user user3 group group3
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap1
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# http
ciscoasa(config-pmap-p)# default group default_group
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
ciscoasa(config)# policy-map type inspect scansafe cws_inspect_pmap2
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# https
ciscoasa(config-pmap-p)# default group2 default_group2
ciscoasa(config-pmap-p)# class whitelist1
ciscoasa(config-pmap-c)# whitelist
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
match user group	ユーザーまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

match username

FTPユーザー名に関して一致条件を設定するには、クラスマップ コンフィギュレーション モードまたはポリシー マップ コンフィギュレーション モードで **match username** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]
no match [**not**] **username regex** [*regex_name* | **class** *regex_class_name*]

構文の説明

regex_name	正規表現を指定します。
class *regex_class_name*	正規表現のクラスマップを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、FTP クラス マップまたは FTP ポリシー マップ内で設定できます。FTP クラス マップに入力できるエントリは 1 つのみです。

例

次に、FTP インスペクション クラス マップに FTP ユーザー名に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect ftp match-all ftp_class1
ciscoasa(config-cmap)# match username regex class ftp_regex_user
```

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。
clear configure class-map	すべてのクラス マップを削除します。
match any	クラス マップにすべてのトラフィックを含めます。
match port	クラス マップ内の特定のポート番号を指定します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

match uuid

DCERPC メッセージの汎用一意識別子（UUID）に関して一致条件を設定するには、クラスマップまたはポリシー マップ コンフィギュレーション モードで **match uuid** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match ［ **not** ］ **uuid** *type*
no match ［ **not** ］ **uuid** *type*

構文の説明

type 照合する UUID タイプ。次のいずれかが必要です。

- **ms-rpc-epm**：Microsoft RPC EPM メッセージを照合します。
- **ms-rpc-isystemactivator**：ISystemMapper メッセージを照合します。
- **ms-rpc-oxidresolver**：OxidResolver メッセージを照合します。

コマンド デフォルト

DCERPC インスペクションでは、すべてのメッセージ タイプが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップまたはポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、DCERPC インスペクション クラス マップまたは DCERPC インスペクション ポリシーマップで設定できます。このコマンドを使用すると、DCERPC UUID に基づいてトラフィックをフィルタ処理できます。その後、リセットしたり、一致するトラフィックをログに記録したりすることができます。

例

次に、DCERPC メッセージに含まれる ms-rpc-isyustemactivator UUID に関して一致条件を設定する例を示します。

```
ciscoasa(config)# class-map type inspect dcerpc dcerpc-cmap
ciscoasa(config-cmap)# match uuid ms-rpc-isystemactivator
```

関連コマンド

コマンド	説明
class-map type inspect	インスペクション クラス マップを作成します。
policy-map type inspect	インスペクション ポリシー マップを作成します。

match version

GTP インスペクションで GTP バージョンに関して一致条件を設定するには、ポリシー マップ コンフィギュレーション モードで **match version** コマンドを使用します。一致条件を削除するには、このコマンドの **no** 形式を使用します。

match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]
no match [**not**] **version** [*version_id* | **range** *lower_range upper_range*]

構文の説明

version_id	バージョンを 0 ～ 255 の範囲で指定します。
range *lower_range upper_range*	バージョンの下限および上限を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、GTP ポリシー マップで設定できます。

例

次に、GTP インスペクション ポリシー マップにメッセージ バージョンに関して一致条件を設定する例を示します。

```
ciscoasa(config-pmap)# match version 1
```

関連コマンド

コマンド	説明
inspect gtp	GTP トラフィックのインスペクションを設定します。

max-area-addresses

IS-IS エリアの追加の手動アドレスを設定するには、ルータ ISIS コンフィギュレーション モードで **max-area-addresses** コマンドを使用します。手動のアドレスを無効にするには、このコマンドの **no** 形式を使用します。

max-area-addresses *number*
no max-area-addresses *number*

構文の説明

number	追加するマニュアル アドレスの数。範囲は3 ～ 234 です。

コマンド デフォルト

IS-IS エリア用のマニュアル アドレスは設定されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、追加マニュアル アドレスを設定することでIS-IS エリアのサイズを最大化できるようになります。各マニュアルアドレスを作成するには、追加するアドレスの数を指定し、NET アドレスを割り当てます。

例

次に、3 つのアドレスを設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-are-addreses 3
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。

コマンド	説明
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。

コマンド	説明
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。

コマンド	説明
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

max-failed-attempts

サーバーグループ内の所定のサーバーが停止するまでに、サーバーで許可される AAA トランザクションの失敗数を指定するには、AAA サーバー グループ コンフィギュレーション モードで **max-failed-attempts** コマンドを使用します。この指定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。

max-failed-attempts*number*
nomax-failed-attempts

構文の説明

number 前述の **aaa-server** コマンドに指定されているサーバーグループの特定のサーバーに対して許可されている AAA トランザクションの失敗数を指定する 1 ～ 5 の範囲の整数。

コマンド デフォルト

number 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
aaa サーバーグループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを発行する前に、AAA サーバまたは AAA サーバ グループを設定しておく必要があります。

例

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-server-group)# max-failed-attempts 4
ciscoasa
(config-aaa-server-group)#
```

関連コマンド

コマンド	説明
aaa-server *server-tag***protocol** *protocol*	AAA サーバー グループ コンフィギュレーション モードを開始して、グループ固有の AAA サーバー パラメータおよびグループ内のすべてのホストに共通の AAA サーバー パラメータを設定します。
clear configure aaa-server	AAA サーバーのコンフィギュレーションをすべて削除します。
show running-config aaa	すべての AAA サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

max-forwards-validation

Max-forwardsヘッダーフィールドが0かチェックするには、パラメータ コンフィギュレーション モードで **max-forwards-validation** 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。

max-forwards-validation action { **drop** | **drop-connection** | **reset** | **log** } [**log**]
no max-forwards-validation action { **drop** | **drop-connection** | **reset** | **log** } [**log**]

構文の説明

drop	検証発生時にパケットをドロップします。
drop-connection	違反が発生した場合、接続をドロップします。
reset	違反が発生した場合、接続をリセットします。
log	違反が発生した場合、スタンドアロンまたは追加のログを記録することを指定します。任意のアクションと関連付けることができます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、宛先へのホップの数をカウントします。宛先に達する前に0になることができません。

例

次に、SIP インスペクション ポリシー マップに最大転送数の検証をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect sip sip_map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# max-forwards-validation action log
```

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。

max-header-length

HTTP ヘッダーの長さに基づいて HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセスできる HTTP マップ コンフィギュレーション モードで **max-header-length** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

max-header-length { **request** *bytes* [**response** *bytes*] | **response** *bytes* } **action** { **allow** | **reset** | **drop** } [**log**]
no max-header-length { **request** *bytes* [**response** *bytes*] | **response** *bytes* } **action** { **allow** | **reset** | **drop** } [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
bytes	バイト数です。範囲は 1 ～ 65535 です。
log	（任意）syslog を生成します。
request	要求メッセージ。
reset	クライアントおよびサーバーに TCP リセット メッセージを送信します。
response	（任意）応答メッセージ。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
HTTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

max-header-length コマンドを有効にすると、ASA は設定された制限内の HTTP ヘッダーがあるメッセージのみを許可し、その他のメッセージの場合には指定されたアクションを実行します。ASA に TCP 接続をリセットさせて、必要に応じて、syslog エントリを作成させるには、**action** キーワードを使用します。

例

次に、HTTP 要求を HTTP ヘッダーが 100 バイトを超えない要求に制限する例を示します。ヘッダーが大きすぎる場合、ASA は TCP 接続をリセットして、syslog エントリを作成します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-header-length request bytes 100 action log reset
ciscoasa(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張HTTPインスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

max-lsp-lifetime

ASA のデータベースで更新されることなく、LSP を保持できる最大時間を設定するには、ルータ コンフィギュレーション モードで **max-lsp-lifetime** コマンドを使用します。デフォルトの有効期間に戻すには、このコマンドの **no** 形式を使用します。

max-lsp-lifetime *seconds*
nomax-lsp-lifetime

構文の説明

seconds	LSP のライフタイム（秒数）。指定できる範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルト値は 1200 秒（20 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

更新 LSP の着信前にライフタイムを超えると、LSP がデータベースからドロップされます。

lsp-refresh-interval コマンドを使用して LSP の更新間隔を変更する場合、LSP の最大有効期間を調整する必要がある場合があります。LSP は、ライフタイムが経過するまで定期的にリフレッシュされる必要があります。**lsp-refresh-interval** コマンドに対して設定される値は、**max-lsp-lifetime** コマンドに対して設定される値よりも小さな値である必要があり、そうでない場合、リフレッシュされる前に LSP がタイムアウトします。LSP 間隔と比べて LSP ライフタイムを大幅に少なくするという設定ミスをした場合、ソフトウェアが LSP リフレッシュ間隔を減らして、LSP がタイムアウトしないようにします。

各コマンドでより大きな値を使用して、制御トラフィックを削減することができます。この場合、クラッシュしたルータや到達不能のルータからの古い LSP がより長くデータベースで保持されるようになり（そのために無駄なコストが発生する）、未検出の不適切な LSP がアクティブなままとなる（非常にまれ）リスクも増大します。

例

次に、40 分間の LSP ライフタイムを設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# max-lsp-lifetime 2400
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。

コマンド	説明
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

maximum-paths（BGP）

ルーティング テーブルにインストールできる並列 BGP ルートの最大数を制御するには、アドレス ファミリ コンフィギュレーション モードで maximum-paths 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。

maximum-paths [**ibgp**] *number-of-paths*
no maximum-paths [**ibgp**] *number-of-paths*

構文の説明

ibgp	（オプション）ルーティング テーブルにインストールできる内部 BGP ルートの最大数を制御できます。
number-of-paths	ルーティング テーブルにインストールするルートの数。

コマンド デフォルト

デフォルトでは、BGP はルーティング テーブルにベストパスを 1 つだけインストールします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

maximum-paths コマンドは、BGP ピアリング セッションに等コストまたは非等コスト マルチパス ロード シェアリングを設定するために使用されます。ルートを BGP ルーティング テーブル内のマルチパスとして導入する場合、ルートはすでにある他のルートと同じネクスト ホップを持つことはできません。BGP ルーティング プロセスは、BGP マルチパス ロード シェアリングが設定されている場合、BGP ピアに最適パスをアドバタイズします。等コスト ルートの場合、最下位のルータ ID を持つネイバーからのパスは、ベストパスとしてアドバタイズされます。

BGP 等コスト マルチパス ロード シェアリングを設定するには、すべてのパス属性を同じにする必要があります。パスの属性には、重み値、ローカル プリファレンス、自律システム パス

（長さだけでなく、属性全体）、オリジン コード、MED、および Interior Gateway Protocol（IGP）のディスタンスが含まれます。

例

次に、2 つの並列 iBGP パスをインストールする例を示します。

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# maximum-paths ibgp 2
```

関連コマンド

コマンド	説明
show bgp	BGP ルーティング テーブル内のエントリを表示します。

maximum-paths（IS-IS）

IS-IS プロトコルのマルチパス ロード シェアリングを設定するには、ルータ ISIS コンフィギュレーション モードで **maximum-paths** コマンドを使用します。ISIS ルートのマルチパス ロード シェアリングを無効にするには、このコマンドの **no** 形式を使用します。

maximum-paths *number-of-paths*
no maximum-paths *number-of-paths*

構文の説明

number-of-paths	ルーティング テーブルにインストールするルートの数。指定できる範囲は 1 ～ 8 です。

コマンド デフォルト

デフォルトでは、IS-IS はルーティング テーブルにベストパスを 1 つだけインストールします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

maximum-paths コマンドは、ASA で ECMP が設定されている場合に IS-IS マルチパス ロード シェアリングを設定するために使用されます。

例

次に、ルーティング テーブルの最大パス数を 8 に設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# maximum-paths 8
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。

コマンド	説明
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。

コマンド	説明
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。

コマンド	説明
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

max-object-size

WebVPN セッションに対してが ASA キャッシュできるオブジェクトの最大サイズを設定するには、キャッシュモードで max-object-size コマンドを使用します。サイズを変更するには、このコマンドを再度使用します。

max-object-size*integerrange*

構文の説明

integer range	0 ～ 10000 KB

コマンド デフォルト

1000 KB

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
キャッシュモード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

最大オブジェクトサイズは、最小オブジェクトサイズよりも大きい値である必要があります。キャッシュ圧縮が有効になっている場合、ASA では、オブジェクトを圧縮してからサイズが計算されます。

例

次に、最大オブジェクト サイズを 4000 KB に設定する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# max-object-size
 4000
ciscoasa(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。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
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。
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。

max-retry-attempts（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

要求がタイムアウトされるまでに ASA が失敗した SSO 認証を再試行できる回数を設定するには、特定の SSO サーバータイプの webvpn コンフィギュレーション モードで **max-retry-attempts** 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。

max-retry-attempts *retries*
nomax-retry-attempts

構文の説明

retries	ASA が失敗した SSO 認証を再試行する回数。指定できる範囲は 1 ～ 5 回です。

コマンド デフォルト

このコマンドのデフォルト値は 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス マップ タイプ正規表現コンフィギュレーション	• 対応	—	• 対応	—	—
config-webvpn-sso-saml-idp	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングルサインオンは、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスに

アクセスできます。ASA は、現在、SiteMinder-type の SSO サーバーと SAML POST-type の SSO サーバーをサポートしています。

このコマンドは SSO サーバーの両タイプに適用されます。

一度 SSO 認証をサポートするように ASA を設定すると、必要に応じて、2 つのタイムアウトパラメータを調整できます。

- **max-retry-attempts command.** を使用して、ASA が失敗した SSO 認証を再試行する回数。
- 失敗した SSO 認証の試行がタイムアウトになるまでの秒数（**request-timeout** コマンドを参照）。

例

次に、webvpn-sso-siteminder コンフィギュレーション モードを開始し、my-sso-server という名前の SiteMinder SSO サーバ名に対する認証再試行を 4 つ設定する例を示します。

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)#
max-retry-attempts 4
ciscoasa(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
policy-server-secret	SiteMinder SSO サーバーへの認証要求の暗号化に使用する秘密キーを作成します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。
sso-server	シングル サインオン サーバーを作成します。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバーの URL を指定します。

max-uri-length

HTTP 要求メッセージの URI の長さに基づいて HTTP トラフィックを制限するには、**http-map** コマンドを使用してアクセスできる HTTP マップ コンフィギュレーション モードで **max-uri-length** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

max-uri-length *bytes* **action** { **allow** | **reset** | **drop** } [**log**]
no max-uri-length *bytes* **action** { **allow** | **reset** | **drop** } [**log**]

構文の説明

action	メッセージがこのコマンド インスペクションに合格しなかったときに実行されるアクションです。
allow	メッセージを許可します。
drop	接続を閉じます。
bytes	バイト数です。範囲は 1 ～ 65535 です。
log	（任意）syslog を生成します。
reset	クライアントおよびサーバに TCP リセット メッセージを送信します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
HTTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

max-uri-length コマンドを有効にすると、ASA は設定された制限内の URI があるメッセージのみを許可し、そ例外のメッセージには指定されたアクションを実行します。ASA に TCP 接続をリセットさせて、Syslog エントリを作成させるには、**action** キーワードを使用します。

長さが設定された値以下のURIが許可されます。それ以外の場合には、指定されたアクションが実行されます。

例

次に、HTTP 要求を URI が 100 バイトを超えない要求に制限する例を示します。URI が大きすぎる場合、ASA は TCP 接続をリセットし、syslog エントリを作成します。

```
ciscoasa(config)# http-map inbound_http
ciscoasa(config-http-map)# max-uri-length 100 action reset log
ciscoasa(config-http-map)#
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
debug appfw	拡張HTTPインスペクションに関連するトラフィックの詳細情報を表示します。
http-map	拡張 HTTP インスペクションを設定するための HTTP マップを定義します。
inspect http	アプリケーション インスペクション用に特定の HTTP マップを適用します。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

mcast-group

VXLAN VNI インターフェイスのマルチキャストグループを指定するには、インターフェイスコンフィギュレーションモードで**mcast-group** コマンドを使用します。この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。

mcast-group *mcast_ip*
nomcast-group

構文の説明

mcast_ip	マルチキャスト グループの IP アドレスを設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA がピア VTEP の背後にあるデバイスにパケットを送信する場合、ASA には次の 2 つの重要な情報が必要です。

- リモート デバイスの宛先 MAC アドレス
- ピア VTEP の宛先 IP アドレス

ASA がこの情報を検出するには 2 つの方法あります。

- 単一のピア VTEP IP アドレスを ASA に静的に設定できます。

手動で複数のピアを定義することはできません。

ASA が VXLAN カプセル化 ARP ブロードキャストを VTEP に送信し、エンド ノードの MAC アドレスを取得します。

- マルチキャストグループは、**mcast-group** コマンドを使用して VNI インターフェイスごとに（または VTEP 全体に）設定できます。

ASA は、IP マルチキャスト パケット内の VXLAN カプセル化 ARP ブロードキャスト パケットを VTEP 送信元インターフェイスを経由して送信します。この ARP 要求への応答により、ASA はリモート VTEP の IP アドレスと、リモート エンド ノードの宛先 MAC アドレスの両方を取得することができます。

ASA は VNI インターフェイスのリモート VTEP IP アドレスに対する宛先 MAC アドレスのマッピングを維持します。

VNI インターフェイスに対してマルチキャストグループを設定しない場合、使用可能な場合は、VTEP 送信元インターフェイス設定のデフォルトグループが使用されます（**default-mcast-group** コマンド）。**peer ip** コマンドを使用して VTEP 送信元インターフェイスに対して手動で VTEP ピア IP を設定した場合、VNI インターフェイスに対してマルチキャストグループは指定できません。マルチキャストは、マルチ コンテキスト モードではサポートされていません。

例

次に、VNI 1 インターフェイスを設定し、マルチキャスト グループ 236.0.0.100 を指定する例を示します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。

コマンド	説明
nve-only	VXLAN送信元インターフェイスがNVE専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ2転送テーブル（MACアドレステーブル）を表示します。
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

mcc

GTP インスペクションで IMSI プレフィックス フィルタリングのモバイル国コードおよびモバイルネットワークコードを識別するには、ポリシー マップ パラメータ コンフィギュレーション モードで **mcc** 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。

［ **drop** ］ **mcc** *country_code* **mnc** *network_code*
no ［ **drop** ］ **mcc** *country_code* **mnc** *network_code*

構文の説明

drop	プレフィックスの組み合わせに一致する接続をドロップすることを指定します。結果として、指定された組み合わせが不要なプレフィックスを示していることになります。 このキーワードを指定しない場合、接続は許可されるプレフィックスの組み合わせと一致する必要があります。 特定のマップ内のすべてのプレフィックス フィルタリングは、「すべてドロップ」または「すべて許可」で統一されている必要があります。
country_code	モバイル国コードを識別するゼロ以外の 3 桁の値。エントリが 1 桁または 2 桁の場合には、その先頭に 0 が付加されて 3 桁の値が作成されます。
network_code	ネットワーク コードを識別する 2 桁または 3 桁の値。

コマンド デフォルト

デフォルトでは、GTP インスペクションは有効な MCC/MNC の組み合わせをチェックしません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.16(1)	**drop** キーワードが追加されました。

使用上のガイドライン

コマンドは必要な回数入力して、ターゲットとなるすべての MCC/MNC ペアを指定できますが、ポリシーマップ内のすべてのコマンドは **mcc** または **drop mcc** である必要があります。これらのコマンドを組み合わせることはできません。

デフォルトでは、GTP インスペクションは、有効なモバイル カントリ コード（MCC）とモバイル ネットワーク コード（MNC）の組み合わせをチェックしません。IMSI プレフィックス フィルタリングを設定すると、受信パケットの IMSI の MCC と MNC が、設定された MCC と MNC の組み合わせと比較されます。次に、コマンドに基づいて次のいずれかのアクションが実行されます。

- **mcc** コマンド：一致しない場合、パケットはドロップされます。
- **drop mcc** コマンド：一致する場合、パケットはドロップされます。

モバイル カントリ コードは 0 以外の 3 桁の数字で、1 桁または 2 桁の値のプレフィックスとして 0 が追加されます。モバイル ネットワーク コードは 2 桁または 3 桁の数字です。

許可またはドロップするすべての MCC と MNC の組み合わせを追加します。デフォルトでは、ASA は MNC と MCC の組み合わせが有効であるかどうかをチェックしないため、設定した組み合わせが有効であるかどうかを確認する必要があります。MCC および MNC コードの詳細については、ITU E.212 勧告『*Identification Plan for Land Mobile Stations*』を参照してください。

例

次に、MCC を 111、MNC を 222 として、IMSI プレフィックス フィルタリングのトラフィックを識別する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# mcc 111 mnc 222
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

media-termination（廃止予定）

電話プロキシ機能へのメディア接続に使用するメディア ターミネーション インスタンスを指定するには、電話プロキシ コンフィギュレーション モードで **media-termination** コマンドを使用します。

電話プロキシ コンフィギュレーションからメディア ターミネーション 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。

media-terminationinstance_name
nomedia-termination*instance_name*

構文の説明

instance_name	メディア ターミネーション アドレスを使用するインターフェイスの名前を指定します。1 つのインターフェイスに設定できるメディア ターミネーション アドレスは 1 つだけです。

コマンド デフォルト

このコマンドには、デフォルト設定はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
8.2(1)	このコマンドは、メディア ターミネーション アドレスで NAT を使用できるように更新されました。 **rtp-min-port** キーワードおよび **rtp-max-ports** キーワードがコマンドシンタックスから削除され、独立したコマンドとなりました。
9.4(1)	このコマンドは、すべての **phone-proxy** モードコマンドとともに廃止されました。

使用上のガイドライン

ASA では、次の基準を満たすメディアターミネーションの IP アドレスが設定されている必要があります。

メディア ターミネーション インスタンスでは、すべてのインターフェイスに対してグローバルなメディア ターミネーション アドレスを設定することも、インターフェイスごとにメディ

アターミネーションアドレスを設定することもできます。しかし、グローバルなメディア ターミネーション アドレスと、インターフェイスごとに設定するメディア ターミネーション アドレスは同時に使用できません。

複数のインターフェイスに対してメディア ターミネーション アドレスを設定する場合、IP 電話との通信時に ASA で使用するアドレスを、インターフェイスごとに設定する必要があります。

IP アドレスは、そのインターフェイスのアドレス範囲内で使用されていない、パブリックにルーティング可能な IP アドレスです。

メディア ターミネーション インスタンスの作成時およびメディア ターミネーション アドレスの設定時に満たす必要がある前提条件の完全なリストについては、CLI 設定ガイドを参照してください。

例

次に、media-termination address コマンドを使用して、メディア接続に使用する IP アドレスを指定する例を示します。

```
ciscoasa(config-phone-proxy)# media-termination mta_instance1
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

media-type

メディアタイプを銅線またはファイバギガビットイーサネットに設定するには、インターフェイス コンフィギュレーション モードで **media-type** コマンドを使用します。ASA 5500 シリーズ適応型セキュリティアプライアンスの 4GE SSM でファイバ SFP コネクタが使用可能になります。メディアタイプ設定をデフォルトに戻すには、このコマンドの **no** 形式を使用します。

media-type { **rj45** | **sfp** }
no media-type [**rj45** | **sfp**]

構文の説明

rj45	（デフォルト）メディア タイプを銅線 RJ-45 コネクタに設定します。
sfp	メディア タイプをファイバ SFP コネクタに設定します。

コマンド デフォルト

デフォルトは **rj45** 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。

使用上のガイドライン

sfp 設定では、固定速度（1000 Mbps）が使用されるため、**speed** コマンドを使用すると、インターフェイスにリンクパラメータをネゴシエートさせるかどうかを設定できます。**duplex** コマンドは、**sfp** ではサポートされません。

例

次に、メディア タイプを SFP に設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet1/1
ciscoasa(config-if)# media-type sfp
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
interface	インターフェイスを設定し、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。
show running-config interface	インターフェイス コンフィギュレーションを表示します。
speed	インターフェイスの速度を設定します。

member

コンテキストをリソースクラスに割り当てるには、コンテキストコンフィギュレーションモードで**member**コマンドを使用します。コンテキストをリソースクラスから削除するには、このコマンドの **no** 形式を使用します。

member*class_name*
nomember*class_name*

構文の説明

class_name	**class** コマンドで作成したクラス名を指定します。

コマンド デフォルト

デフォルトでは、コンテキストはデフォルトのクラスに割り当てられます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
コンテキストコンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、コンテキストごとの上限値が適用されていない限り、すべてのセキュリティコンテキストがASAのリソースに無制限にアクセスできます。ただし、1つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。ASAは、リソースクラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

例

次に、コンテキスト テストをゴールド クラスに割り当てる例を示します。

```
ciscoasa(config-ctx)# context
 test
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.100 int1
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.102 int2
ciscoasa(config-ctx)# allocate-interface gigabitethernet0/0.110-gigabitethernet0/0.115
int3-int8
ciscoasa(config-ctx)# config-url
```

```
 ftp://user1:passw0rd@10.1.1.1/configlets/test.cfg
ciscoasa(config-ctx)# member gold
```

関連コマンド

コマンド	説明
class	リソース クラスを作成します。
context	セキュリティ コンテキストを設定します。
limit-resource	リソースの制限を設定します。
show resource allocation	リソースを各クラスにどのように割り当てたかを表示します。
show resource types	制限を設定できるリソース タイプを表示します。

member-interface

物理インターフェイスを冗長インターフェイスに割り当てるには、インターフェイス コンフィギュレーション モードで **member-interface** コマンドを使用します。このコマンドは、冗長インターフェイス タイプでのみ使用できます。2 つのメンバ インターフェイスを冗長インターフェイスに割り当てることができます。メン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。冗長インターフェイスから両方のメンバ インターフェイスは削除できません。冗長インターフェイスには、少なくとも 1 つのメンバインターフェイスが必要です。

member-interface*physical_interface*
nomember-interface*physical_interface*

構文の説明

physical_interface	インターフェイス ID（**gigabitethernet 0/1** など）を指定します。有効値については、**interface** コマンドを参照してください。両方のメンバー インターフェイスが同じ物理タイプである必要があります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

両方のメンバインターフェイスが同じ物理タイプである必要があります。たとえば、両方ともイーサネットにする必要があります。

名前が設定されている場合は、物理インターフェイスを冗長インターフェイスに追加できません。まず **no nameif** コマンドを使用して名前を削除する必要があります。

⚠

注意 コンフィギュレーション内で物理インターフェイスをすでに使用している場合、名前を削除すると、このインターフェイスを参照しているすべてのコンフィギュレーションが消去されます。

冗長インターフェイスペアの一部である物理インターフェイスに使用できる唯一の構成は物理パラメータ（**speed** コマンド、**duplex** コマンド、**description** コマンド、**shutdown** コマンドなど）です。また、**default** や **help** などの実行時コマンドも入力できます。

アクティブ インターフェイスをシャットダウンすると、スタンバイ インターフェイスがアクティブになります。

アクティブインターフェイスを変更するには、 **redundant-interface** コマンドを入力します。

冗長インターフェイスでは、追加した最初の物理インターフェイスの MAC アドレスを使用します。コンフィギュレーションでメンバー インターフェイスの順序を変更すると、MAC アドレスは、リストの最初になったインターフェイスの MAC アドレスと一致するように変更されます。または、冗長インターフェイスに MAC アドレスを割り当てることができます。これはメンバーインターフェイスの MAC アドレスに関係なく使用されます（**mac-address** コマンドまたは **mac-address auto** コマンドを参照）。アクティブインターフェイスがスタンバイインターフェイスにフェールオーバーした場合、同じMACアドレスが維持されるため、トラフィックが妨げられることはありません。

例

次の例では、2 つの冗長インターフェイスを作成します。

```
ciscoasa(config)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# interface redundant 2
ciscoasa(config-if)# member-interface gigabitethernet 0/2
ciscoasa(config-if)# member-interface gigabitethernet 0/3
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
debug redundant-interface	冗長インターフェイスのイベントまたはエラーに関するデバッグメッセージを表示します。
interface redundant	冗長インターフェイスを作成します。
redundant-interface	アクティブなメンバ インターフェイスを変更します。
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。

memberof

このユーザーがメンバーであるグループ名のリストを指定するには、ユーザー名属性コンフィギュレーション モードで **memberof** コマンドを使用します。この属性を構成から削除するには、このコマンドの **no** 形式を使用します。

memberof *group_1*［，*group_2*，．．．*group_n*］
no memberof *group_1*［，*group_2*，．．．*group_n*］

構文の説明

group_1 through group_n	このユーザーが所属するグループを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー名属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このユーザーが所属するグループ名のカンマ区切りリストを入力します。

例

次に、グローバル コンフィギュレーション モードを開始し、ユーザー名を newuser という名前で作成し、newuser が DevTest グループおよび管理グループのメンバであることを指定する例を示します。

```
ciscoasa(config)# username newuser nopassword
ciscoasa(config)# username newuser attributes
ciscoasa(config-username)# memberof DevTest,management
ciscoasa(config-username)#
```

関連コマンド

コマンド	説明
clear configure username	ユーザー名データベース全体または指定されたユーザー名のみをクリアします。
show running-config username	特定のユーザーまたはすべてのユーザーに対して現在実行されているユーザー コンフィギュレーションを表示します。
username	ユーザー名のデータベースを作成および管理します。

memory appcache-threshold enable

メモリ アプリケーション キャッシュのしきい値を有効にするには、コンフィギュレーション モードで **memory appcache-threshold enable** コマンドを使用します。**memory appcache-threshold,** を無効にするには、このコマンドの **no** 形式を使用します。

memoryappcache-thresholdenable
nomemoryappcache-thresholdenable

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。

コマンド デフォルト

この **memory appcache-threshold enable** コマンドは、Cisco ASA 5585-X FirePOWER SSP-60（5585-60）ではデフォルトで有効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.10(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

memory appcache-threshold を有効にすると、特定のメモリしきい値に達した後、アプリケーション キャッシュの割り当てが制限されるため、デバイスの管理性と安定性を維持するためのメモリが予約ができます。

ASA 9.10.1 リリースでは、memory appcache-threshold 機能が 5585-60 に実装され、through-the-box 接続のみに対して、アプリケーション キャッシュの割り当てが制限されていました。

このコマンドは、システム メモリの 85 % にアプリケーション キャッシュの割り当てしきい値を設定します。メモリ使用率がしきい値レベルに達すると、デバイスへの新しい through-the-box 接続がドロップされます。

コマンドの **no** 形式を使用すると、すべてのメモリ割り当て制限が検証なしに使用されます。現在の統計カウンタは、**clear memory appcache-threshold** コマンドが実行されるまで、トラブルシューティング履歴を維持するために保持されます。

9.10.1 リリースでは、SNP Conn Core 00 アプリケーション キャッシュ タイプのみが管理されます。この名前は、「show mem app-cache」の出力と一致しています。

例

次に、appcache-memory しきい値を有効にする例を示します。

```
ciscoasa(config)# memory appcache-threshold enable
```

関連コマンド

コマンド	説明
show memory appcache-threshold	メモリ appcache しきい値のステータスとヒット数を表示します。
clear memory appcache-threshold	memory appcache-threshold のヒット カウントをクリアします。

memory delayed-free-poisoner enable

delayed free-memory poisoner ツールを有効にするには、特権 EXEC モードで **memory delayed-free-poisoner enable** コマンドを使用します。delayed free-memory poisoner ツールを無効にするには、このコマンドの **no** 形式を使用します。delayed free-memory poisoner ツールを使用すると、アプリケーションによってメモリが解放された後、解放メモリの変化をモニターできます。

memorydelayed-free-poisonerenable
nomemorydelayed-free-poisonerenable

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。

コマンド デフォルト

memory delayed-free-poisoner enable コマンドは、デフォルトで無効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

delayed free-memory poisoner ツールをイネーブルにすると、メモリ使用状況およびシステム パフォーマンスに大きな影響を及ぼします。このコマンドは、Cisco TAC の指導の下でのみ使用する必要があります。システムの使用率が高い間は、実働環境では実行しないでください。

このツールを有効にすると、ASA で実行されているアプリケーションによって、メモリ解放要求が FIFO キューに書き込まれます。要求がキューに書き込まれるたびに、それに伴うメモリ バイトのうち、下位メモリ管理には必要ないバイトが、値 0xcc で書き込まれて「改ざん」されます。

メモリ解放要求は、空きメモリ プールにある量よりも多くのメモリがアプリケーションで必要になるまで、キューに残ります。メモリが必要になると、最初のメモリ解放要求がキューから取り出され、改ざんされたメモリが検証されます。

メモリに変更がない場合、メモリは下位メモリ プールに返され、ツールは最初に要求を行ったアプリケーションからのメモリ要求を再発行します。この処理は、要求元のアプリケーションに十分なメモリが解放されるまで続きます。

改ざんされたメモリに変更があった場合、システムは強制的にクラッシュし、クラッシュの原因を突き止めるための診断出力を作成します。

delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。また、**memory delayed-free-poisoner validate** コマンドを使用して手動で検証を開始できます。

このコマンドの **no** 形式を実行すると、キュー内の要求で参照されるすべてのメモリが検証されずに空きメモリプールに返され、すべての統計カウンタがクリアされます。

例

次に、delayed free-memory poisoner ツールをイネーブルにする例を示します。

```
ciscoasa# memory delayed-free-poisoner enable
```

次に、delayed free-memory poisoner ツールが不正なメモリ再利用を検出した場合の出力例を示します。

```
delayed-free-poisoner validate failed because a
        data signature is invalid at delayfree.c:328.
    heap region:    0x025b1cac-0x025b1d63 (184 bytes)
    memory address: 0x025b1cb4
    byte offset:    8
    allocated by:   0x0060b812
    freed by:       0x0060ae15
Dumping 80 bytes of memory from 0x025b1c88 to 0x025b1cd7
025b1c80:                         ef cd 1c a1 e1 00 00 00  |          ........
025b1c90: 23 01 1c a1 b8 00 00 00 15 ae 60 00 68 ba 5e 02  |  #.........`.h.^.
025b1ca0: 88 1f 5b 02 12 b8 60 00 00 00 00 00 6c 26 5b 02  |  ..[...`.....l&[.
025b1cb0: 8e a5 ea 10 ff ff ff ff cc cc cc cc cc cc cc cc  |  ................
025b1cc0: cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc cc  |  ................
025b1cd0: cc cc cc cc cc cc cc cc                         |  ........
An internal error occurred.  Specifically, a programming assertion was
violated.  Copy the error message exactly as it appears, and get the
output of the show version command and the contents of the configuration
file.  Then call your technical support representative.
assertion "0" failed: file "delayfree.c", line 191
```

<xref> に、出力の重要な部分を示します。

表 *5:* 不正なメモリ使用に関する出力の説明

フィールド	説明
heap region	要求元のアプリケーションが使用できるメモリ領域のアドレス領域およびサイズ。これは、要求されたサイズと同じ値ではなく、メモリ要求が行われたときにシステムがメモリを配分できるように小さくなることがあります。
memory address	障害が検出されたメモリの位置。

フィールド	説明
byte offset	バイト オフセットはヒープ領域の先頭を基準にしており、このアドレスから始まるデータ構造を保持するためにフィールドが変更された場合には、バイト オフセットを使用してそのフィールドを見つけることができます。値が 0 か、またはヒープ領域バイト カウントよりも大きい値である場合は、問題が下位ヒープ パッケージの予期しない値であることを示している可能性があります。
allocated by/freed by	この特定のメモリ領域に関して実施された最後の malloc/calloc/realloc および解放要求の命令アドレス。
Dumping...	検出された障害がヒープ メモリ領域の先頭にどれだけ近いかに応じて、1 つまたは 2 つのメモリ領域のダンプ。システム ヒープ ヘッダーに続く 8 バイトは、このツールがさまざまなシステム ヘッダー値のハッシュとキュー リンクを保持するために使用するメモリです。システム ヒープ トレーラが検出されるまでの領域内のそれ以外のバイトは、0xcc に設定する必要があります。

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner validate	delayed free-memory poisoner ツールのキュー内要素の検証を強制実行します。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

memory delayed-free-poisoner validate

memory delayed-free-poisoner キューのすべての要素を強制的に検証するには、特権 EXEC モードで **memory delayed-free-poisoner validate** コマンドを使用します。

memorydelayed-free-poisonervalidate

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

memory delayed-free-poisoner validate コマンドを発行する場合は、事前に **memory delayed-free-poisoner enable** コマンドを使用して delayed free-memory poisoner ツールを有効にする必要があります。

memory delayed-free-poisoner validate コマンドにより、**memory delayed-free-poisoner** キューの各要素が検証されます。要素に予期しない値が含まれている場合、システムは強制的にクラッシュし、クラッシュの原因を突き止めるための診断出力を作成します。予期しない値が存在しない場合、要素はキューに残り、ツールによって正常に処理されます。**memory delayed-free-poisoner validate** コマンドを実行しても、キュー内のメモリはシステムメモリプールに返されません。

（注） delayed free-memory poisoner ツールは、定期的にキューのすべての要素を自動的に検証します。

例

次に、**memory delayed-free-poisoner** キューのすべての要素を検証する例を示します。

```
ciscoasa# memory delayed-free-poisoner validate
```

関連コマンド

コマンド	説明
clear memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューおよび統計情報をクリアします。
memory delayed-free-poisoner enable	delayed free-memory poisoner ツールをイネーブルにします。
show memory delayed-free-poisoner	delayed free-memory poisoner ツールのキューの使用状況に関する要約を表示します。

memory caller-address

コールトレースまたは発信元 PC 用にプログラムメモリの特定の範囲を設定して、メモリの問題を特定できるようにするには、特権 EXEC モードで **memory caller-address** コマンドを使用します。発信元PCは、メモリ割り当てプリミティブを呼び出したプログラムのアドレスです。アドレス範囲を削除するには、このコマンドの **no** 形式を使用します。

memorycaller-address*startPCendPC*
nomemorycaller-address

構文の説明

endPC	メモリブロックの終了アドレス範囲を指定します。
startPC	メモリブロックの開始アドレス範囲を指定します。

コマンド デフォルト

メモリを追跡できるように、実際の発信元 PC が記録されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。

使用上のガイドライン

メモリの問題を特定のメモリブロックに限定するには、**memory caller-address** コマンドを使用します。

場合によっては、メモリ割り当てプリミティブの実際の発信元 PC が、プログラムの多くの場所で使用されている既知のライブラリ関数であることがあります。プログラムの個々の場所を特定するには、そのライブラリ関数の開始プログラム アドレスおよび終了プログラム アドレスを設定し、それによってライブラリ関数の呼び出し元のプログラムアドレスを記録します。

（注） 発信元アドレスの追跡を有効にすると、ASA のパフォーマンスが一時的に低下することがあります。

例

次に、**memory caller-address** コマンドで設定したアドレスの範囲、および **show memory-caller address** コマンドの表示結果の例を示します。

```
ciscoasa# memory caller-address 0x00109d5c 0x00109e08

ciscoasa# memory caller-address 0x009b0ef0 0x009b0f14

ciscoasa# memory caller-address 0x00cf211c 0x00cf4464

ciscoasa# show memory-caller address
Move down stack frame for the addresses:
pc = 0x00109d5c-0x00109e08
pc = 0x009b0ef0-0x009b0f14
pc = 0x00cf211c-0x00cf4464
```

関連コマンド

コマンド	説明
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory	物理メモリの最大量とオペレーティング システムで現在使用可能な空きメモリ量について要約を表示します。
show memory binsize	特定のバイナリ サイズに割り当てられているチャンクの要約情報を表示します。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory-caller address	ASA 上に設定されているアドレス範囲を表示します。

memory logging

メモリロギングを有効にするには、グローバル コンフィギュレーション モードで **memory logging** コマンドを使用します。メモリロギングを無効にするには、このコマンドの **no** 形式を使用します。

memory logging [**1024-4194304**] [**wrap**] [**size** [**1-2147483647**]] [**process** *process-name*] [**context** *context-name*]
nomemorylogging

構文の説明

1024-4194304	メモリ ロギング バッファのロギング エントリの数を指定します。指定する必要がある引数はこれだけです。
context *context-name*	モニターする仮想コンテキストおよびコンテキスト名を指定します。
process *process-name*	モニターするプロセスおよびプロセス名を指定します。 （注） Checkheaps プロセスは、非標準の方法でメモリ アロケータを使用するため、プロセスとして完全に無視されます。
size 1-2147483647	モニターするサイズおよびエントリ数を指定します。
wrap	バッファのラップ時にバッファを保存します。保存できるのは一度だけです。複数回ラップされると上書きされる可能性があります。バッファがラップすると、そのデータの保存をイネーブルにするトリガーがイベント マネージャに送信されます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

メモリ ロギング パラメータを変更するには、それをディセーブルにしてから、再度イネーブルにします。

例

次に、メモリ ロギングをイネーブルにする例を示します。

```
ciscoasa
(config)#
memory logging 202980
```

関連コマンド

コマンド	説明
event memory-logging-wrap	メモリ ロギング ラップ イベントへの応答をイネーブルにします。
show memory logging	メモリ ロギングの結果を表示します。

memory profile enable

メモリ使用状況のモニタリング（メモリプロファイリング）を有効にするには、特権 EXEC モードで **memory profile enable** コマンドを使用します。メモリプロファイルリングを無効にするには、このコマンドの **no** 形式を使用します。

memoryprofileenablepeak*peak_value*
nomemoryprofileenablepeak*peak_value*

構文の説明

peak_value メモリ使用状況のスナップショットを使用率ピーク バッファに保存するメモリ使用状況しきい値を指定します。このバッファの内容を後で分析して、システムのピーク時のメモリ ニーズを判断できます。

コマンド デフォルト

デフォルトでは、メモリ プロファイリング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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。

使用上のガイドライン

メモリプロファイリングを有効にする前に、**memory profile text** コマンドを使用して、プロファイリングするメモリのテキスト範囲を設定する必要があります。

一部のメモリは、**clear memory profile** コマンドを入力するまでプロファイリングシステムによって保持されます。**show memory status** コマンドの出力を参照してください。

（注） メモリプロファイリングをイネーブルにすると、ASA のパフォーマンスが一時的に低下する場合があります。

次に、メモリ プロファイリングをイネーブルにする例を示します。

```
ciscoasa# memory profile enable
```

関連コマンド

コマンド	説明
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。

memory profile text

プロファイリングするメモリのプログラムテキスト範囲を設定するには、特権EXECモードで **memory profile text** コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します。

memory profile text { *startPC endPC* | **all** *resolution* }
no memory profile text { *startPC endPC* | **all** *resolution* }

構文の説明

all	メモリブロックのテキスト範囲全体を指定します。
endPC	メモリブロックの終了テキスト範囲を指定します。
resolution	ソース テキスト領域の追跡精度を指定します。
startPC	メモリブロックの開始テキスト範囲を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。

使用上のガイドライン

テキスト範囲が小さい場合、精度を「4」にすると、命令への呼び出しが正常に追跡されます。テキスト範囲が大きい場合、精度を粗くしても初回通過には十分であり、範囲は次回の通過でさらに小さな領域にまで絞り込むことができます。

メモリプロファイリングを開始するには、**memory profile text** コマンドでテキスト範囲を入力した後、**memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリプロファイリングはディセーブルになっています。

（注） メモリプロファイリングをイネーブルにすると、ASAのパフォーマンスが一時的に低下する場合があります。

例

次に、精度を 4 にして、プロファイリングするメモリのテキスト範囲を設定する例を示します。

```
ciscoasa# memory profile text 0x004018b4 0x004169d0 4
```

次に、メモリ プロファイリングのテキスト範囲のコンフィギュレーションおよびステータス（OFF）を表示する例を示します。

```
ciscoasa# show memory profile
InUse profiling: OFF Peak profiling: OFF Profile: 0x004018b4-0x004169d0(00000004)
```

（注） メモリプロファイリングを開始するには、**memory profile enable** コマンドを入力する必要があります。デフォルトでは、メモリ プロファイリングはディセーブルになっています。

関連コマンド

コマンド	説明
clear memory profile	メモリ プロファイリング機能によって保持されているバッファをクリアします。
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。
show memory-caller address	ASA 上に設定されているアドレス範囲を表示します。

memory-size

WebVPN のさまざまなコンポーネントがアクセスできる ASA 上のメモリ容量を設定するには、webvpn モードで **memory-size** コマンドを使用します。設定されたメモリ容量（KB 単位）または合計メモリの割合として、メモリ容量を設定できます。設定されたメモリサイズを削除するには、このコマンドの **no** 形式を使用します。

（注） 新しいメモリ サイズ設定を有効にするには、リブートが必要です。

memory-size { **percent** | **kb** } *size*
no memory-size [{ **percent** | **kb** } *size*]

構文の説明

kb	メモリ容量をキロバイト単位で指定します。
percent	ASA 上のメモリ容量を合計メモリの割合として指定します。
size	メモリ容量を KB 単位または合計メモリの割合として指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

設定したメモリ容量は、ただちに割り当てられます。このコマンドを設定する前に、show memory を使用して、使用可能なメモリ容量を確認してください。設定に合計メモリの割合を使用する場合は、設定した値が使用可能な割合を下回っていることを確認してください。設定にキロバイトの値を使用する場合は、設定した値がキロバイト単位の使用可能なメモリ容量を下回っていることを確認してください。

例

次に、WebVPN メモリ サイズを 30 % に設定する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 memory-size percent 30
ciscoasa(config-webvpn)#
ciscoasa(config-webvpn)# reload
```

関連コマンド

コマンド	説明
show memory webvpn	WebVPN メモリ使用状況の統計情報を表示します。

memory tracking enable

ヒープメモリ要求の追跡を有効にするには、特権 EXEC モードで **memory tracking enable** コマンドを使用します。メモリ追跡を無効にするには、このコマンドの **no** 形式を使用します。

memorytrackingenable
nomemorytrackingenable

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(8)	このコマンドが追加されました。

使用上のガイドライン

ヒープメモリ要求を追跡するには、**memory tracking enable** コマンドを使用します。メモリ追跡を無効にするには、このコマンドの **no** 形式を使用します。

メモリ追跡をイネーブルにする前に、app-agent heartbeat コマンドのデフォルトの間隔とカウント値を次のように変更してください。

app-agent heartbeat interval 6000 retry-count 6

例

次に、ヒープ メモリ要求の追跡をイネーブルにする例を示します。

```
ciscoasa# memory tracking enable
```

関連コマンド

コマンド	説明
clear memory tracking	現在収集されているすべての情報をクリアします。
show memory tracking	現在割り当てられているメモリを表示します。

コマンド	説明
show memory tracking address	ツールの追跡対象である現在割り当てられている各メモリのサイズ、位置、および最上位呼び出し元関数を一覧表示します。
show memory tracking dump	このコマンドは、指定されたメモリアドレスのサイズ、位置、呼び出しスタックの一部、およびメモリダンプを表示します。
show memory tracking detail	ツール内部の動作の洞察に使用されるさまざまな内部詳細情報を表示します。

memory-utilization

システム メモリが事前に定義されたレベルまで使用されたときに、自動的にリブートするか、またはクラッシュするように ASA を設定するには、memory utilization コマンドを使用します。メモリ使用状況が設定されたしきい値の上限に到達すると、システムは自動的にリロードします。しきい値は 90 ～ 99 % の範囲です。

memory-utilization reload-threshold < **%** >
memory-utilization reload-threshold < **%** > [**crashinfo**]

構文の説明

reload-threshold	システム メモリのしきい値の上限を指定します。
crashinfo	（オプション）使用する場合、システム リロードの前にクラッシュ情報を保存することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

一般にメモリ使用状況が極めて高くなる環境に遭遇することがわかっているシステム上にこの機能を設定しないことを推奨します。システム リロードの前にクラッシュ情報ファイルを生成するには、オプションの crashinfo 引数を使用します。

例

次に、ASA 上にメモリ使用状況機能を設定する例を示します。

```
ciscoasa# memory-utilization reload-threshold 95
```

関連コマンド

コマンド	説明
memory profile text	プロファイルするメモリのテキスト範囲を設定します。
memory profile enable	メモリ使用状況（メモリ プロファイリング）のモニタリングをイネーブルにします。
clear memory profile	メモリ プロファイリング機能によって保持されているバッファをクリアします。
show memory profile	ASA のメモリ使用状況（プロファイリング）に関する情報を表示します。

merge-dacl

ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL をマージするには、AAA サーバー グループ コンフィギュレーション モードで **merge-dacl** コマンドを使用します。ダウンロード可能 ACL と、RADIUS パケットから Cisco AV ペアで受信した ACL のマージを無効にするには、このコマンドの **no** 形式を使用します。

merge dacl { **before_avpair** | **after_avpair** }
nomergedacl

構文の説明

after_avpair	ダウンロード可能 ACL のエントリを Cisco AV ペアのエントリの後に配置する必要があることを指定します。このオプションは、VPN 接続にのみ適用されます。VPN ユーザーの場合は、ACL は Cisco AV ペア ACL、ダウンロード可能 ACL、および ASA で設定される ACL の形式になります。このオプションでは、ダウンロード可能 ACL と AV ペア ACL を結合するかどうかを決定します。ASA で設定されている ACL には適用されません。
before_avpair	ダウンロード可能 ACL のエントリを Cisco AV ペア のエントリの前に配置する必要があることを指定します。

コマンド デフォルト

デフォルト設定は **no merge dacl** で、ダウンロード可能な ACL は Cisco AV ペア ACL とマージされません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA-server グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

AV ペアおよびダウンロード可能 ACL の両方を受信した場合は、AV ペアが優先し、使用されます。

例

次の例では、ダウンロード可能 ACL のエントリが Cisco AV ペアのエントリの前に配置されるように指定しています。

```
ciscoasa(config)# aaa-server servergroup1 protocol radius
ciscoasa(config-aaa-server-group)# merge-dacl before-avpair
```

関連コマンド

コマンド	説明
aaa-server host	サーバーと、そのサーバーが属する AAA サーバー グループを識別します。
aaa-server protocol	サーバー グループ名とプロトコルを識別します。
max-failed-attempts	次のサーバーを試す前にグループ内の AAA サーバーに送信する要求の最大数を指定します。

message-length

設定された最大の長さを満たさない DNS パケットをフィルタリングするには、パラメータ コンフィギュレーション モードで message-length コマンドを使用します。このコマンドを削除するには、**no** 形式を使用します。

message-length maximum { *length* | **client** { *length* | **auto** } | **server** { *length* | **auto** } }
no message-length maximum { *length* | **client** { *length* | **auto** } | **server** { *length* | **auto** } }

構文の説明

length	DNS メッセージの最大許容バイト数（512 ～ 65535）を指定します。
client {*length* | **auto**}	クライアント DNS メッセージの最大許容バイト数（512 ～ 65535）を指定します。最大長をリソースレコードと同じ値に設定する場合は、**auto** を指定します。
server {*length* | **auto**}	サーバー DNS メッセージの最大許容バイト数（512 ～ 65535）を指定します。最大長をリソースレコードと同じ値に設定する場合は、**auto** を指定します。

コマンド デフォルト

デフォルトの検査では、DNS メッセージの最大長は 512、クライアントの長さは **auto** に設定されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

DNS インスペクション マップのパラメータとして DNS メッセージの最大長を設定できます。

例

次に、DNS インスペクション ポリシー マップで DNS メッセージの最大長を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length 512
ciscoasa(config-pmap-p)# message-length client auto
```

関連コマンド

コマンド	説明
parameter	ポリシー マップ コンフィギュレーション モードからパラメータ コンフィギュレーション モードを開始します。
policy-map type inspect dns	DNS インスペクション ポリシー マップを作成します。

message-tag-validation

M3UA メッセージに含まれる特定のフィールドの内容を検証するには、パラメータ コンフィギュレーション モードで **message-tag-validation** 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 モードにアクセスするには、まず **policy-map type inspect m3ua** コマンドを入力します。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。

message-tag-validation { **dupu** | **error** | **notify** }
no message-tag-validation { **dupu** | **error** | **notify** }

構文の説明

dupu 宛先ユーザー部使用不可（DUPU）メッセージの検証をイネーブルにします。ユーザー/理由フィールドが存在し、有効な理由およびユーザー コードのみが含まれている必要があります。

error エラー メッセージの検証をイネーブルにします。すべての必須フィールドが存在し、許可された値のみが含まれている必要があります。各エラー メッセージには、そのエラー コードの必須フィールドが含まれている必要があります。

notify 通知メッセージの検証をイネーブルにします。ステータス タイプおよびステータス情報フィールドには、許可された値のみが含まれている必要があります。

コマンド デフォルト

このコマンドのデフォルト設定は、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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

特定のフィールドの内容がチェックされ、指定された M3UA メッセージ タイプに関して検証されるようにするには、このコマンドを使用します。検証で合格しなかったメッセージはドロップされます。

例

次に、M3UA インスペクションでの DUPU、エラー、および通知メッセージの検証をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect m3ua m3ua-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-tag-validation dupu
ciscoasa(config-pmap-p)# message-tag-validation error
ciscoasa(config-pmap-p)# message-tag-validation notify
```

関連コマンド

コマンド	説明
inspect m3ua	M3UA インスペクションをイネーブルにします。
policy-map type inspect	インスペクション ポリシー マップを作成します。
show service-policy inspect m3ua	M3UA 統計情報を表示します。

metric

すべての IS-IS インターフェイスのメトリック値をグローバルに変更するには、ルータ ISIS コンフィギュレーション モードで **metric** コマンドを使用します。メトリック値を無効にして、デフォルトメトリック値の 10 に戻すには、このコマンドの **no** 形式を使用します。

metric *default-value* [**level-1** | **level-2**]
no metric *default-value* [**level-1** | **level-2**]

構文の説明

default-value	リンクに割り当てられ、宛先へのリンクを介したパス コストを計算するために使用されるメトリック値。指定できる範囲は 1 ～ 63 です。
level-1	（任意）IS-IS レベル 1 IPv4 または IPv6 メトリックを設定します。
level-2	（任意）IS-IS レベル 2 IPv4 または IPv6 メトリックを設定します。

コマンド デフォルト

デフォルトは 10 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

すべての IS-IS インターフェイスのデフォルトメトリック値を変更する必要がある場合、**metric** コマンドを使用して、すべてのインターフェイスをグローバルに設定することを推奨します。メトリック値がグローバルに設定されている場合、新規値を設定せずに誤って設定済みのメトリックをインターフェイスから削除したり、デフォルト メトリック 10 に戻るよう誤ってインターフェイスに許可したりするなどの、ユーザーのエラーを防ぐことができるため、ネットワーク内で優先度の高いインターフェイスとなります。

metric コマンドを入力して、デフォルトの IS-IS インターフェイスメトリック値を変更すると、有効になっているインターフェイスでは、デフォルト値 の10 ではなく新しい値が使用されます。パッシブ インターフェイスでは、メトリック値 0 が引き続き使用されます。

例

次に、グローバル メトリック 111 で IS-IS インターフェイスを設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric 111
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。

コマンド	説明
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。

コマンド	説明
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。

コマンド	説明
summary-address	IS-IS の集約アドレスを作成します。

metric-style

新スタイルのタイプ、長さ、および値（TLV）オブジェクトだけを生成して受け入れるように IS-IS が動作するルータを設定するには、ルータ ISIS コンフィギュレーション モードで **metric-style** コマンドを使用します。この機能を無効にするには、このコマンドの **no** 形式を使用します。

metric-style [**narrow** | **transition** | **wide**] [**level-1** | **level-2** | **level-1-2**]
no metric [**level-1** | **level-2** | **level-1-2**]

構文の説明

narrow	旧スタイルの TLV とナロー メトリックを使用するように ASA に指示します。
transition	（任意）移行時に旧スタイルおよび新スタイルの TLV の両方を受け入れるように ASA に指示します。
wide	新スタイルの TLV を使用してワイド メトリックを伝送するように ASA に指示します。
level-1	（任意）ルーティング レベル 1 でこのコマンドをイネーブルにします。
level-2	（任意）ルーティング レベル 2 でこのコマンドをイネーブルにします。
level-1-2	（任意）旧スタイルおよび新スタイルの TLV の両方を受け入れようにルータに指示します。

コマンド デフォルト

デフォルトは 10 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

metric-style wide コマンドを入力する場合、ASA は新スタイル TLV だけを生成し、受け入れます。したがって、ASA で使用されるメモリやリソースは、旧スタイルと新スタイルの両方の TLV を生成した場合よりも少なくなります。

このスタイルは、ネットワーク全体で MPLS トラフィック エンジニアリングをイネーブルにする場合に最適です。

例

次に、レベル 1 で新スタイルの TLV を生成し、受け入れるように ASA を設定する例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# metric-style wide level-1
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。

コマンド	説明
isis advertise-prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。

コマンド	説明
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が ASA のデータベースに更新されずに存在する最長時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。

コマンド	説明
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

mf – mz

mfib forwarding

インターフェイスで MFIB 転送を再び無効にするには、インターフェイス コンフィギュレーション モードで **mfib forwarding** を使用します。インターフェイスで MFIB 転送を無効にするには、このコマンドの **no** 形式を使用します。

mfibforwarding
nomfibforwarding

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。

コマンド デフォルト

multicast-routing コマンドは、デフォルトではすべてのインターフェイスの MFIB 転送を有効にします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

マルチキャストルーティングをイネーブルにすると、デフォルトではすべてのインターフェイスで MFIB 転送がイネーブルになります。特定のインターフェイスで MFIB 転送を無効にするには、このコマンドの **no** 形式を使用します。実行コンフィギュレーションには、このコマンドの **no** 形式だけが表示されます。

インターフェイスでMFIB転送がディセーブルになっている場合、特に他の方法を設定しない限り、そのインターフェイスはマルチキャストパケットを受け付けません。MFIB転送がディセーブルになっていると、IGMP パケットも阻止されます。

例

次に、指定されたインターフェイスでMFIB転送をディセーブルにする例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/0
ciscoasa(config-if)# no mfib forwarding
```

関連コマンド

コマンド	説明
multicast-routing	マルチキャスト ルーティングをイネーブルにします。
pim	インターフェイスに対して PIM をイネーブルにします。

migrate

LAN-to-LAN の設定（IKEv1）やリモート アクセスの設定（SSL または IKEv1）を IKEv2 に移行するには、グローバル コンフィギュレーション モードで migrate コマンドを使用します。

migrate { **l2l** | **remote-access** { **ikev2** | **ssl** } | **overwrite** }

構文の説明

l2l	IKEv1 の LAN-to-LAN の設定を IKEv2 に移行します。
remote-access	リモート アクセスの設定を指定します。
ikev2	リモート アクセスの IKEv1 設定を IKEv2 に移行します。
ssl	リモート アクセスの SSL 設定を IKEv2 に移行します。
overwrite	既存の IKEv2 設定を上書きします。

コマンド 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

次の表は、このコマンドを入力するモードを示しています。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

migrate l2l コマンドを使用すると、LAN-to-LAN のすべての IKEv1 設定が IKEv2 に移行されます。

overwrite キーワードを使用すると、ASA は既存の IKEv2 設定を移行されたコマンドとマージせずに、移行されたコマンドで上書きします。

migrate remote-access コマンドを使用すると、IKEv1 または SSL の設定が IKEv2 に移行されます。ただし、次の設定タスクは別途実行する必要があります。

- webvpn コンフィギュレーション モードで セキュアクライアント パッケージファイルをロードします。
- セキュアクライアント プロファイルを設定し、グルー ポリシーに対して指定します。
- IKEv1 接続にカスタマイゼーション オブジェクトを使用している場合は、IKEv2 接続に使用するトンネル グループにそれらを関連付けます。
- **crypto ikev2 remote-access trust-point** コマンドを使用して、サーバー認証のアイデンティティ証明書（トラストポイント）を指定します。ASA は、IKEv2 で接続しているリモートの セキュアクライアント に対して ASA 自体を認証するときにこのトラストポイントを使用します。
- デフォルトのもの以外にもトンネル グループおよび/またはグループ ポリシーを設定している場合は、それらに対して IKEv2 または SSL を指定します（デフォルトの DefaultWEBVPNGroup トンネル グループとデフォルトのグループ ポリシーは IKEv2 または SSL を許可するように設定されています）。
- クライアントからデフォルト以外のグループに接続できるようにするには、トンネル グループでグループのエイリアスまたは URL を設定します。
- 外部のグループ ポリシーやユーザー レコードを更新します。
- グローバル、トンネル グループ、またはグループ ポリシーのその他の設定でクライアントの動作を変更します。
- **crypto ikev2 enable** <interface> [client-services [port]] コマンドを使用して、IKEv2 のファイルのダウンロードやソフトウェアのアップグレードにクライアントが使用するポートを設定します。

関連コマンド

コマンド	説明
crypto ikev2 enable	IPsec ピアの通信に使用するインターフェイスで IKEv2 ネゴシエーションをイネーブルにします。
show run crypto ikev2	IKEv2 設定情報を表示します。

min-object-size

WebVPN セッションに対して ASA がキャッシュできるオブジェクトの最小サイズを設定するには、キャッシュモードで min-object-size コマンドを使用します。サイズを変更するには、このコマンドを再度使用します。最小オブジェクトサイズを設定しないようにするには、値にゼロ（0）を入力します。

min-object-size*integerrange*

構文の説明

integer range	0 ～ 10000 KB。

コマンド デフォルト

デフォルトのサイズは 0 KB です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
キャッシュの設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

最小オブジェクトサイズは、最大オブジェクトサイズよりも小さい値である必要があります。キャッシュ圧縮が有効になっている場合、ASA では、オブジェクトを圧縮してからサイズが計算されます。

例

次に、最大オブジェクト サイズを 40 KB に設定する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 cache
ciscoasa(config-webvpn-cache)# min-object-size
 40
ciscoasa(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。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
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。
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。

mkdir

新規ディレクトリを作成するには、特権 EXEC モードで **mkdir** コマンドを使用します。

mkdir [/ **noconfirm**] [**disk0:** | **disk1:** | | **flash:**] *path*

構文の説明

noconfirm	（任意）確認プロンプトを表示しないようにします。
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。ASA 5500 シリーズの適応型セキュリティアプライアンスでは、**flash** キーワードは **disk0** のエイリアスです。
path	作成するディレクトリの名前およびパス。

コマンド デフォルト

パスを指定しないと、現在の作業ディレクトリにディレクトリが作成されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

同じ名前のディレクトリがすでに存在する場合、新規のディレクトリは作成されません。

例

次に、新規ディレクトリを「backup」という名前で作成する例を示します。

```
ciscoasa# mkdir backup
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。

コマンド	説明
dir	ディレクトリの内容を表示します。
rmdir	指定されたディレクトリを削除します。
pwd	現在の作業ディレクトリを表示します。

mobile-device portal

すべてのモバイルデバイスのクライアントレス VPN アクセス Web ポータルをミニポータルからフルブラウザポータルに変更するには、webvpn コンフィギュレーションモードで**mobile-device portal** コマンドを使用します。この設定が必要なのは、Windows CE などの古いオペレーティングシステムを実行するスマートフォンだけです。新しいスマートフォンではデフォルトでフルブラウザ ポータルが使用されているため、このオプションを設定する必要はありません。

mobile-device portal { **full** }
no mobile-device portal { **full** }

構文の説明

mobile-device portal {full}	すべてのモバイル デバイスのクライアントレス VPN アクセス ポータルをミニポータルからフルブラウザ ポータルに変更します。

コマンド デフォルト

このコマンドを実行する前のデフォルトの動作では、モバイルデバイスによって、クライアントレス VPN アクセスにミニ ポータルを使用するかフル ポータルを使用するかが異なります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(5)	このコマンドが 8.2(5) と 8.4(2) で同時に追加されました。
8.4(2)	このコマンドが 8.2(5) と 8.4(2) で同時に追加されました。

使用上のガイドライン

このコマンドは、Cisco Technical Assistance Center（TAC）から推奨された場合にのみ使用してください。

例

すべてのモバイル デバイスのクライアントレス VPN アクセス ポータルをフルブラウザ ポータルに変更します。

```
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mobile-device portal full
```

関連コマンド

コマンド	説明
show running-config webvpn	WebVPN の実行コンフィギュレーションを表示します。

mode

セキュリティ コンテキスト モードをシングルまたはマルチに設定するには、グローバル コンフィギュレーション モードで **mode** コマンドを使用します。単一の ASA は、セキュリティ コンテキストと呼ばれる複数の仮想デバイスにパーティション化できます。各コンテキストは独立したデバイスとして動作し、独自のセキュリティポリシー、インターフェイス、および管理者で構成されています。複数のコンテキストが存在することは、複数のスタンドアロンアプライアンスが設置されていることと同じです。シングルモードでは、ASA はシングル構成で、単一デバイスとして動作します。マルチモードでは、複数のコンテキストを作成し、それぞれに独自のコンフィギュレーションを設定できます。許可されるコンテキストの数は、保有するライセンスによって異なります。

mode { **single** | **multiple** } [**noconfirm**]

構文の説明

multiple	マルチ コンテキスト モードを設定します。
noconfirm	（任意）ユーザーに確認を求めることなく、モードを設定します。このオプションは自動スクリプトで役立ちます。
single	コンテキスト モードを single に設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

マルチコンテキストモードでは、ASA に各コンテキストの構成が含まれ、各構成では、スタンドアロンデバイスに設定できるセキュリティポリシー、インターフェイス、およびほぼすべてのオプションが識別されます（コンテキスト構成の場所の識別については、**config-url** コマンドを参照してください）。システム管理者がコンテキストを追加および管理するには、コンテキストをシステム コンフィギュレーションに設定します。これが、シングル モード設定と同じく、スタートアップ コンフィギュレーションとなります。システム コンフィギュレーショ

ンは、ASA の基本設定を識別します。システム コンフィギュレーションには、ネットワーク インターフェイスやネットワーク設定は含まれません。その代わりに、ネットワーク リソースにアクセスする必要が生じたときに（サーバーからコンテキストをダウンロードするなど）、システムは管理コンテキストとして指定されているコンテキストのいずれかを使用します。

mode コマンドを使用してコンテキストモードを変更すると、再起動を求められます。

コンテキスト モード（シングルまたはマルチ）は、リブートされても持続されますが、コンフィギュレーション ファイルには保存されません。構成を別のデバイスにコピーする必要がある場合は、**mode** コマンドを使用して、新しいデバイスのモードを match に設定します。

シングルモードからマルチモードに変換すると、ASA は実行コンフィギュレーションを 2 つのファイル（システム コンフィギュレーションで構成される新規スタートアップ コンフィギュレーション、および内部フラッシュメモリのルートディレクトリ内の管理コンテキストで構成される admin.cfg）に変換します。元の実行コンフィギュレーションは、old_running.cfg として（内部フラッシュメモリのルートディレクトリ）に保存されます。元のスタートアップ コンフィギュレーションは保存されません。ASA は、管理コンテキストのエントリをシステム コンフィギュレーションに「admin」という名前で自動的に追加します。

マルチモードからシングルモードに変換する場合は、先にスタートアップ コンフィギュレーション全体（使用可能な場合）を ASA にコピーすることを推奨します。マルチモードから継承されるシステム コンフィギュレーションは、シングルモードデバイスで完全に機能するコンフィギュレーションではありません。

マルチ コンテキスト モードのすべての機能がサポートされるわけではありません。詳細については、CLI コンフィギュレーション ガイドを参照してください。

例

次に、モードを multiple に設定する例を示します。

```
ciscoasa(config)# mode multiple
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Convert the system configuration? [confirm] y
Flash Firewall mode: multiple
***
*** --- SHUTDOWN NOW ---
***
*** Message to all terminals:
***
***   change mode
Rebooting....
Booting system, please wait...
```

次に、モードを single に設定する例を示します。

```
ciscoasa(config)# mode single
WARNING: This command will change the behavior of the device
WARNING: This command will initiate a Reboot
Proceed with change mode? [confirm] y
Flash Firewall mode: single
***
*** --- SHUTDOWN NOW ---
***
```

```
*** Message to all terminals:
***
***   change mode
Rebooting....
Booting system, please wait...
```

関連コマンド

コマンド	説明
context	システム コンフィギュレーションにコンテキストを設定し、コンテキスト コンフィギュレーション モードを開始します。
show mode	現在のコンテキスト モード（シングルまたはマルチ）を表示します。

monitor-interface

特定のインターフェイスでヘルスモニタリングを有効にするには、グローバル コンフィギュレーション モードで **monitor-interface** コマンドを使用します。インターフェイスのモニタリングを無効にするには、このコマンドの **no** 形式を使用します。

monitor-interface { *if_name* | **service-module** }
no monitor-interface { *if_name* **service-module** }

構文の説明

if_name	モニターするインターフェイスの名前を指定します。
service-module	サービス モジュールをモニターします。ASA FirePOWER モジュールなど、ハードウェアモジュールの障害でフェールオーバーをトリガーさせない場合は、このコマンドの **no** 形式を使用してモジュールのモニタリングを無効にできます。

コマンド デフォルト

物理インターフェイスとサービス モジュールのモニタリングは、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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.3(1)	service-module キーワードが追加されました。

使用上のガイドライン

ASA について監視できるインターフェイスの数はプラットフォームごとに異なり、**show failover** コマンドの出力で確認できます。

インターフェイス ポーリング頻度ごとに、ASA フェールオーバーペア間で hello メッセージが交換されます。フェールオーバー インターフェイスのポーリング時間は 3 ～ 15 秒です。たとえば、ポーリング時間を 5 秒に設定すると、あるインターフェイスで 5 回連続して hello が検出されないと（25 秒間）、そのインターフェイスでテストが開始します。

モニター対象のフェールオーバー インターフェイスには、次のステータスが設定されます。

- Unknown：初期ステータスです。このステータスは、ステータスを特定できないことを意味する場合もあります。
- Normal：インターフェイスはトラフィックを受信しています。
- Testing：ポーリング 5 回の間、インターフェイスで hello メッセージが検出されていません。
- Link Down：インターフェイスまたは VLAN は管理上ダウンしています。
- No Link：インターフェイスの物理リンクがダウンしています。
- Failed：インターフェイスではトラフィックを受信していませんが、ピア インターフェイスではトラフィックを検出しています。

アクティブ/アクティブ フェールオーバーでは、このコマンドはコンテキスト内でだけ有効です。

例

次の例では、「inside」という名前のインターフェイスでモニタリングをイネーブルにしています。

```
ciscoasa(config)# monitor-interface inside
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure monitor-interface	すべてのインターフェイスでデフォルトのインターフェイス ヘルス モニタリングに戻します。
failover interface-policy	モニターするインターフェイスの数または割合を指定します。モニターの対象となるのは、障害が発生すると、フェールオーバーが発生するインターフェイスです。
failover polltime	インターフェイスでの hello メッセージ間の間隔を指定します（Active/Standby フェールオーバー）。
polltime interface	インターフェイスでの hello メッセージ間の間隔を指定します（Active/Active フェールオーバー）。
show running-config monitor-interface	実行コンフィギュレーションの **monitor-interface** コマンドを表示します。

more

ファイルの内容を表示するには、特権 EXEC モードで **more** コマンドを使用します。

more { **/ascii** | **/binary** | **/ebcdic** / **disk0:** | **disk1:** | **flash:** | **ftp:** | **http:** | **https:** | **system:** | **tftp:** } *filename*

構文の説明

/ascii	（任意）バイナリ ファイルをバイナリ モード、ASCII ファイルをバイナリ モードで表示します。
/binary	（任意）任意のファイルをバイナリ モードで表示します。
/ebcdic	（任意）バイナリ ファイルを EBCDIC で表示します。
disk0：	（任意）内部フラッシュメモリ上のファイルを表示します。
disk1：	（任意）外部フラッシュメモリカード上のファイルを表示します。
filename	表示するファイルの名前を指定します。
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。ASA 5500 シリーズの適応型セキュリティアプライアンスでは、**flash** キーワードは **disk0** のエイリアスです。
ftp：	（任意）FTP サーバー上のファイルを表示します。
http：	（任意）Web サイト上のファイルを表示します。
https：	（任意）セキュアな Web サイト上のファイルを表示します。
system：	（任意）ファイル システムを表示します。
tftp：	（任意）TFTP サーバ上のファイルを表示します。

コマンド デフォルト

ASCII モード

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

more filesystem: コマンドを入力すると、ローカルディレクトリまたはファイルシステムのエイリアスを入力するように求められます。

（注） **more** コマンドを使用して保存した構成ファイルを表示すると、この構成ファイルのトンネルグループパスワードがクリアテキストに表示されます。

例

次に、「test.cfg」というローカル ファイルの内容を表示する例を示します。

```
ciscoasa# more test.cfg
: Saved
: Written by enable_15 at 10:04:01 Apr 14 2005
XXX Version X.X(X)
nameif vlan300 outside security10
enable password 8Ry2YjIyt7RRXU24 encrypted
passwd 2KFQnbNIdI.2KYOU encrypted
ciscoasa test
fixup protocol ftp 21
fixup protocol h323 H225 1720
fixup protocol h323 ras 1718-1719
fixup protocol ils 389
fixup protocol rsh 514
fixup protocol smtp 25
fixup protocol sqlnet 1521
fixup protocol sip 5060
fixup protocol skinny 2000
names
access-list deny-flow-max 4096
access-list alert-interval 300
access-list 100 extended permit icmp any any
access-list 100 extended permit ip any any
pager lines 24
icmp permit any outside
mtu outside 1500
ip address outside 172.29.145.35 255.255.0.0
no asdm history enable
arp timeout 14400
access-group 100 in interface outside
!
interface outside
!
route outside 0.0.0.0 0.0.0.0 172.29.145.1 1
timeout xlate 3:00:00
timeout conn 1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 rpc 0:10:00 h3
23 0:05:00 h225 1:00:00 mgcp 0:05:00 sip 0:30:00 sip_media 0:02:00
timeout uauth 0:05:00 absolute
aaa-server TACACS+ protocol tacacs+
aaa-server RADIUS protocol radius
aaa-server LOCAL protocol local
snmp-server host outside 128.107.128.179
snmp-server location my_context, USA
```

```
snmp-server contact admin@example.com
snmp-server community public
no snmp-server enable traps
floodguard enable
fragment size 200 outside
no sysopt route dnat
telnet timeout 5
ssh timeout 5
terminal width 511
gdb enable
mgcp command-queue 0
Cryptochecksum:00000000000000000000000000000000
: end
```

関連コマンド

コマンド	説明
cd	指定されたディレクトリに変更します。
pwd	現在の作業ディレクトリを表示します。

mount type cifs

セキュリティアプライアンスから Common Internet File System（CIFS; 共通インターネット ファイル システム）にアクセスできるようにするには、グローバル コンフィギュレーション モードで **mount type cifs** コマンドを使用します。このコマンドを使用すると、mount cifs コンフィギュレーション モードに入ることができます。CIFS ネットワーク ファイル システムをマウント解除するには、このコマンドの **no** 形式を使用します。

mount *name* **type cifs server** *server-name* **share** *share* { **status enable** | **status disable** } [**domain** *domain-name*] **username** *username* **password** *password*
[**mount**] **mount** *name* **type cifs server** *server-name* **share** *share* { **status enable** | **status disable** } [**domain** *domain-name*] **username** *username* **password** *password*

構文の説明

domain *domain-name*	（任意）CIFS ファイル システムでのみ、この引数には Windows NT ドメイン名を指定します。最大 63 文字が許可されます。
name	ローカル CA に割り当てられる既存のファイル システムの名前を指定します。
password password	ファイル システムのマウントのための認可されたパスワードを指定します。
server *server-name*	CIFS ファイル システム サーバの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
share *sharename*	サーバ内のファイルデータにアクセスするために、特定のサーバ共有（フォルダ）を名前で明示的に識別します。
status enable または **disable**	ファイル システムの状態をマウント済みまたはマウント解除済み（使用可能または使用不能）として識別します。
user *username*	ファイル システムのマウントが認可されているユーザ名。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

mount コマンドは、Installable File System（IFS）を使用して、CIFS ファイルシステムをマウントします。IFS（ファイル システム API）を使用すると、セキュリティ アプライアンスはファイル システム用のドライバを認識し、ロードすることができます。

mount コマンドは、セキュリティアプライアンス上の CIFS ファイルシステムを UNIX ファイルツリーにアタッチします。逆に、**no mount** コマンドはアタッチを解除します。

mount コマンドに指定されている *mount-name* は、セキュリティアプライアンスにすでにマウントされているファイルシステムを参照するために、他の CLI コマンドで使用されます。たとえば、ローカル認証局にファイルストレージを設定する **database** コマンドでは、データベースファイルをフラッシュストレージ以外のストレージに保存するために、すでにマウントされているファイルシステムのマウント名が必要です。

CIFS リモート ファイル アクセス プロトコルは、アプリケーションがローカル ディスクおよびネットワーク ファイル サーバー上のデータを共有する方法と互換性があります。TCP/IP を運用し、インターネットのグローバル DNS を使用する CIFS は、Windows オペレーティング システムにネイティブのファイル共有プロトコルである Microsoft のオープンでクロス プラットフォームのサーバー メッセージ ブロック（SMB）プロトコルを拡張したものです。

mount コマンドを使用した後は、必ずルートシェルを終了してください。mount-cifs-config モードの **exit** キーワードは、ユーザーをグローバル コンフィギュレーション モードに戻します。

再接続するには、接続をストレージに再マッピングします。

（注） CIFS ファイル システムと FTP ファイル システムのマウントがサポートされています（**mount** *name* **type ftp** コマンドを参照してください）。このリリースではネットワーク ファイル システム（NFS）ボリュームのマウントはサポートされていません。

例

次に、*cifs://amer;chief:big-boy@myfiler02/my_share* を *cifs_share* というラベルとしてマウントする例を示します。

```
ciscoasa
(config)#
mount cifs_share type CIFS

ciscoasa (config-mount-cifs)#
server myfiler02a
```

関連コマンド

コマンド	説明
debug cifs	CIFS デバッグ メッセージをロギングします。

コマンド	説明
debug ntdomain	Web VPN NT ドメイン デバッグ メッセージをロギングします。
debug webvpn cifs	WebVPN CIFS デバッグ メッセージをロギングします。
dir all-filesystems	ASA にマウントされているすべてのファイルシステムのファイルを表示します。

mount type ftp

セキュリティアプライアンスからファイル転送プロトコル（FTP）ファイルシステムにアクセスできるようにするには、グローバル コンフィギュレーション モードで **mount type ftp** コマンドを使用して、マウント FTP コンフィギュレーション モードを開始します。**no mount type ftp** コマンドは、FTP ネットワーク ファイル システムをマウント解除するために使用されます。

[**no**] **mount** *name* **type ftp server** *server-name* **path** *pathname* { **status enable** | **status disable** } { **mode active** | **mode passive** } **username** *username* **password** *password*

構文の説明

mode active または **passive**	FTP 転送モードをアクティブまたはパッシブとして識別します。
no	すでにマウントされている FTP ファイル システムを削除し、アクセスできないようにします。
password password	ファイル システムのマウントのための認可されたパスワードを指定します。
path *pathname*	指定された FTP ファイル システム サーバーへのディレクトリ パス名を指定します。パス名にスペースを含めることはできません。
server *server-name*	FTPFS ファイル システム サーバの定義済みの名前（またはドット付き 10 進表記の IP アドレス）を指定します。
status enable または **disable**	ファイル システムの状態をマウント済みまたはマウント解除済み（使用可能または使用不能）として識別します。
username *username*	ファイル システムのマウントが認可されているユーザ名を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

mount *name* **type ftp** コマンドは、Installable File System（IFS）を使用して、指定されたネットワーク ファイル システムをマウントします。IFS（ファイル システム API）を使用すると、セキュリティ アプライアンスはファイル システム用のドライバを認識し、ロードすることができます。

FTP ファイルシステムが実際にマウントされていることを確認するには、**dir all-filesystems** 命令を使用します。

mount コマンドに指定されているマウント名は、セキュリティアプライアンスにすでにマウントされているファイルシステムを他の CLI コマンドが参照するときに使用されます。たとえば、ローカル認証局用にファイルストレージを設定する **database** コマンドでは、データベースファイルを非フラッシュストレージに保存するために、すでにマウントされているファイルシステムのマウント名が必要です。

（注） FTP タイプのマウントの作成時に **mount** コマンドを使用するには、FTP サーバーに UNIX ディレクトリリストスタイルが必要です。Microsoft FTP サーバーには、デフォルトで MS-DOS ディレクトリ リスト スタイルがあります。

（注） CIFS ファイル システムと FTP ファイル システムのマウントがサポートされています（**mount** *name* **type ftp** コマンドを参照してください）。このリリースではネットワーク ファイル システム（NFS）ボリュームのマウントはサポートされていません。

例

次に、*ftp://amor;chief:big-kid@myfiler02* を *my ftp:* というラベルとしてマウントする例を示します。

```
ciscoasa
(config)#
mount myftp type ftp server myfiler02a path status enable username chief password big-kid
```

関連コマンド

コマンド	説明
debug webvpn	WebVPN デバッグ メッセージをロギングします。
ftp mode passive	ASA 上の FTP クライアントと FTP サーバーとの通信を制御します。

mroute

スタティック マルチキャスト ルートを設定するには、グローバル コンフィギュレーション モードで **mroute** コマンドを使用します。スタティック マルチキャスト ルートを削除するには、このコマンドの **no** 形式を使用します。

mroute *src smask* { *in_if_name* [**dense** *output_if_name*] | *rpf_addr* } [*distance*]
no *mroute src smask* { *in_if_name* [**dense** *output_if_name*] | *rpf_addr* } [*distance*]

構文の説明

dense *output_if_name*	（任意）デンス モード出力のインターフェイス名。 **dense** *output_if_name* キーワードと引数のペアは、SMR スタブ マルチキャスト ルーティング（igmp 転送）でのみサポートされています。
distance	（任意）ルートのアドミニストレーティブ ディスタンス。ディスタンスが小さいルートが優先されます。デフォルトは 0 です。
in_if_name	mroute の着信インターフェイス名を指定します。
rpf_addr	mroute の着信インターフェイスを指定します。RPF アドレスが PIM ネイバーである場合、PIM Join メッセージ、接合メッセージ、および Prune メッセージがそのアドレスに送信されます。*rpf-addr* 引数には、直接接続されたシステムのホスト IP アドレスまたはネットワーク/サブネット番号を指定します。ルートである場合、直接接続されたシステムを検索するために、ユニキャスト ルーティング テーブルから再帰検索が実施されます。
smask	マルチキャスト送信元ネットワーク アドレス マスクを指定します。
src	マルチキャスト送信元の IP アドレスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、マルチキャスト送信元の検索場所をスタティックに設定できます。ASAは、特定の送信元にユニキャストパケットを送信する際に使用するのと同じインターフェイスでマルチキャストパケットを受信するものと想定します。場合によっては、マルチキャスト ルーティングをサポートしないルートをバイパスするなど、マルチキャスト パケットがユニキャスト パケットとは別のパスをたどることがあります。

スタティック マルチキャスト ルートはアドバタイズも再配布もされません。

マルチキャスト ルート テーブルの内容を表示するには、**show mroute** コマンドを使用します。実行コンフィギュレーションで mroute コマンドを表示するには、**show running-config mroute** コマンドを使用します。

例

次に、**mroute** コマンドを使用して、スタティック マルチキャスト ルートを設定する例を示します。

```
ciscoasa(config)# mroute 172.16.0.0 255.255.0.0 inside
```

関連コマンド

コマンド	説明
clear configure mroute	構成から **mroute** コマンドを削除します。
show mroute	IPv4 マルチキャスト ルーティング テーブルを表示します。
show running-config mroute	構成内の **mroute** コマンドを表示します。

mschapv2-capable

RADIUS サーバーに対する MS-CHAPv2 認証要求を有効にするには、aaa-server ホスト コンフィギュレーション モードで **mschapv2-capable** コマンドを使用します。MS-CHAPv2 を無効にするには、このコマンドの **no** 形式を使用します。

mschapv2-capable
nomschapv2-capable

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。

コマンド デフォルト

デフォルトでは、MS-CHAPv2 は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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA と RADIUS サーバー間の VPN 接続で使用されるプロトコルとして MS-CHAPv2 を有効にするには、トンネルグループ一般属性でパスワード管理を有効にする必要があります。パスワード管理を有効にすると、ASA から RADIUS サーバーへの MS-CHAPv2 認証要求が生成されます。詳細については、**password-management** コマンドの説明を参照してください。

二重認証を使用し、トンネルグループでパスワード管理をイネーブルにした場合は、プライマリ認証要求とセカンダリ認証要求に MS-CHAPv2 要求属性が含まれます。RADIUS サーバーが MS-CHAPv2 をサポートしない場合は、**no mschapv2-capable** コマンドを使用して、そのサーバーが MS-CHAPv2 以外の認証要求を送信するように設定できます。

例

次に、RADIUS サーバ authsrv1.cisco.com の MS-CHAPv2 をディセーブルにする例を示します。

```
ciscoasa(config)# aaa-server rsaradius protocol radius
ciscoasa(config-aaa-server-group)# aaa-server rsaradius (management) host
```

```
authsrv1.cisco.com
ciscoasa(config-aaa-server-host)# key secretpassword
ciscoasa(config-aaa-server-host)# authentication-port 21812
ciscoasa(config-aaa-server-host)# accounting-port 21813
ciscoasa(config-aaa-server-host)# no mschapv2-capable
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバ グループの AAA サーバを識別します。
password-management	password-management コマンドを設定すると、ASA は、リモート ユーザがログインするときに、そのユーザの現在のパスワードの期限切れが迫っている、または期限が切れたことを通知します。それから ASA は、ユーザーがパスワードを変更できるようにします。
secondary-authentication-server-group	SDI サーバー グループになることができないセカンダリ AAA サーバー グループを指定します。

msie-proxy except-list

グループ ポリシー コンフィギュレーション モードで **msie-proxy except-list** コマンドを入力して、クライアントデバイスのブラウザがローカルでプロキシをバイパスするためのプロキシの例外リストの設定を設定します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy except-list { **value** *server* [*:port*] | **none** }
nomsie-proxyexcept-list

構文の説明

none	IP アドレス/ホスト名またはポートがなく、例外リストを継承しないことを示します。
value *server:port*	IP アドレスまたは MSIE サーバーの名前、およびこのクライアント デバイスに適用されるポートを指定します。ポート番号は任意です。

コマンド デフォルト

デフォルトでは、msie-proxy except-list 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

プロキシ設定の詳細については、Cisco Secure Client管理者ガイド、リリース *3.1* [英語]、またはお使いのモバイルデバイスのリリースノートを参照してください。

例

次に、Microsoft Internet Explorer のプロキシ例外リストを設定する例を示します。IP アドレス 192.168.20.1 のサーバで構成され、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象とします。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy except-list value 192.168.20.1:880
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy local-bypass

クライアンデバイスのブラウザプロキシローカルバイパス設定を設定するには、グループポリシーコンフィギュレーションモードで**msie-proxy local-bypass**コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの**no**形式を使用します。

msie-proxy local-bypass { **enable** | **disable** }
no msie-proxy local-bypass { **enable** | **disable** }

構文の説明

disable	クライアントデバイスのブラウザプロキシローカルバイパス設定をディセーブルにします。
enable	クライアントデバイスのブラウザプロキシローカルバイパス設定をイネーブルにします。

コマンドデフォルト

デフォルトでは、msie-proxy local-bypass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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループポリシーコンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

プロキシ設定の詳細については、Cisco Secure Client管理者ガイド、リリース *3.1* [英語]、またはお使いのモバイルデバイスのリリースノートを参照してください。

例

次に、FirstGroupというグループポリシーのMicrosoft Internet Explorerのプロキシローカルバイパスをイネーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy local-bypass enable
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy lockdown

AnyConnect VPN セッションの間、Microsoft Internet Explorer の [接続（Connections）] タブと、設定アプリの [システムプロキシ（System Proxy）] タブを非表示にするか、あるいはそのままにするには、グループ ポリシー コンフィギュレーション モードで、**msie-proxy lockdown** コマンドを使用します。

msie-proxy lockdown [**enable** | **disable**]

構文の説明

disable Microsoft Internet Explorer の [接続（Connections）] タブと、設定アプリのシステム プロキシ タブをそのままにします。

enable AnyConnect VPN セッションの間、Microsoft Internet Explorer の [接続（Connections）] タブと、設定アプリのシステム プロキシ タブを非表示にします。

コマンド デフォルト

デフォルトのグループポリシーでのこのコマンドのデフォルト値はイネーブルです。グループポリシーそれぞれがデフォルトのグループ ポリシーからデフォルト値を継承します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(3)	このコマンドが追加されました。

使用上のガイドライン

この機能をイネーブルにすると AnyConnect VPN セッションの間 Microsoft Internet Explorer の接続タブが非表示になります。また、Windows 10 バージョン 1703（以降）では、この機能を有効にすると、AnyConnect VPN セッションの間、設定アプリのシステム プロキシ タブも非表示になります。この機能を無効にすると、Microsoft Internet Explorer の [接続（Connections）] タブと、設定アプリのシステム プロキシ タブがそのままになります。

この機能を使用するには、プライベート側のプロキシも指定する必要があります。

（注） AnyConnect VPN セッションの間、設定アプリのシステム プロキシ タブを非表示にするには、AnyConnect バージョン 4.7.03052 以降が必要です。

このコマンドは、ユーザー レジストリを AnyConnect VPN セッションの間、一時的に変更します。AnyConnect が VPN セッションを閉じると、レジストリはセッション前の状態に戻ります。

この機能をイネーブルにして、ユーザーがプロキシ サービスを指定して LAN 設定を変更することを防止できます。これらの設定へのユーザーアクセスを防止すると、AnyConnectセッション中のエンドポイント セキュリティが向上します。

プロキシ設定の詳細については、Cisco Secure Client管理者ガイド [英語]、またはお使いのモバイルデバイスのリリースノートを参照してください。

例

次の例では、AnyConnect セッションの間、接続タブを非表示にします。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy lockdown enable
```

次の例では、接続タブをそのままにします。

```
ciscoasa(config-group-policy)# msie-proxy lockdown disable
```

関連コマンド

コマンド	説明
msie-proxy except-list	クライアント デバイスのブラウザのプロキシ サーバの例外リストを指定します。
msie-proxy local-bypass	クライアント デバイスで設定されているローカル ブラウザ プロキシ設定をバイパスします。
msie-proxy method	クライアント デバイスのブラウザ プロキシ アクションを指定します。
msie-proxy pac-url	プロキシサーバーを定義するプロキシ自動コンフィギュレーション ファイルの取得元の URL を指定します。
msie-proxy server	クライアント デバイスのブラウザのプロキシ サーバーを設定します。
show running-config group-policy	実行コンフィギュレーションのグループ ポリシー設定を表示します。

msie-proxy method

クライアントデバイスのブラウザプロキシアクション（「メソッド」）を設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy method** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url**]
no msie-proxy method [**auto-detect** | **no-modify** | **no-proxy** | **use-server** | **use-pac-url** }

（注） この構文に適用される条件については、「使用上のガイドライン」を参照してください。

構文の説明

auto-detect	クライアントデバイスのブラウザでプロキシ サーバの自動検出の使用をイネーブルにします。
no-modify	このクライアント デバイスでは、ブラウザの HTTP ブラウザ プロキシ サーバー設定をそのままにしておきます。
no-proxy	このクライアント デバイスでは、ブラウザの HTTP プロキシ設定をディセーブルにします。
use-pac-url	**msie-proxy pac-url** コマンドに指定されているプロキシ自動コンフィギュレーション ファイル URL から HTTP プロキシサーバー設定を取得するようにブラウザに指示します。
use-server	**msie-proxy server** コマンドに設定された値を使用するように、ブラウザの HTTP プロキシサーバー設定を設定します。

コマンド デフォルト

デフォルトのメソッドは use-server 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	use-pac-url オプションが追加されました。

使用上のガイドライン

プロキシ サーバーの IP アドレスまたはホスト名およびポート番号が含まれている行には、最大 100 文字含めることができます。

このコマンドでサポートされるオプションの組み合わせは次のとおりです。

- **[no] msie-proxy method no-proxy**
- **[no] msie-proxy method no-modify**
- **[no] msie-proxy method [auto-detect] [use-server] [use-pac-url]**

テキストエディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバーを指定するロジックを含む JavaScript ファイルです。.pac ファイルは、Web サーバーにあります。**use-pac-url** を指定すると、ブラウザは .pac ファイルを使用してプロキシ設定を判別します。.pac ファイルの取得元の URL を指定するには、**msie-proxy pac-url** コマンドを使用します。

プロキシ設定の詳細については、Cisco Secure Client管理者ガイド、リリース *3.1* [英語]、またはお使いのモバイルデバイスのリリースノートを参照してください。

例

次に、FirstGroup というグループ ポリシーの Microsoft Internet Explorer プロキシ設定として自動検出を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy method auto-detect
ciscoasa(config-group-policy)#
```

次に、クライアント PC のサーバーとしてサーバー QASERVER、ポート 1001 を使用するように、FirstGroup というグループ ポリシーの Microsoft Internet Explorer プロキシ設定を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server QAserver:port 1001
ciscoasa(config-group-policy)# msie-proxy method use-server
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy pac-url	プロキシ自動コンフィギュレーション ファイルの取得先となる URL を指定します。

コマンド	説明
msie-proxy server	クライアント デバイスのブラウザ プロキシ サーバーおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy pac-url

プロキシ情報の検索場所をブラウザに指示するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy pac-url** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy pac-url { **none** | **value** *url* }
nomsie-proxypac-url

構文の説明

none	URL 値がないことを指定します。
value *url*	使用するプロキシ サーバが 1 つ以上定義されているプロキシ自動コンフィギュレーション ファイルをブラウザが取得できる Web サイトの URL を指定します。

コマンド デフォルト

デフォルト値は none 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

要件

プロキシ自動コンフィギュレーション機能を使用するには、リモート ユーザーは Cisco AnyConnect VPN クライアントを使用する必要があります。プロキシ自動コンフィギュレーション URL の使用を有効にするには、**msie-proxy method** コマンドを **use-pac-url** オプションとともに設定する必要があります。

このコマンドを使用する理由

多くのネットワーク環境が、Web ブラウザを特定のネットワーク リソースに接続する HTTP プロキシを定義しています。HTTP トラフィックがネットワーク リソースに到達できるのは、プロキシがブラウザに指定され、クライアントが HTTP トラフィックをプロキシにルーティン

グする場合だけです。SSLVPN トンネルにより、HTTP プロキシの定義が複雑になります。企業ネットワークにトンネリングするときに必要なプロキシが、ブロードバンド接続経由でインターネットに接続されるときや、サード パーティ ネットワーク上にあるときに必要なものとは異なることがあるためです。

また、大規模ネットワークを構築している企業では、複数のプロキシサーバーを設定し、一時的な状態に基づいてユーザーがその中からプロキシサーバーを選択できるようにすることが必要になる場合があります。.pac ファイルを使用すると、管理者は数多くのプロキシからどのプロキシを社内のすべてのクライアントコンピュータに使用するかを決定する単一のスクリプトファイルを作成できます。

次に、PAC ファイルを使用する例をいくつか示します。

- ロード バランシングのためリストからプロキシをランダムに選択します。
- サーバーのメンテナンス スケジュールに対応するために、時刻または曜日別にプロキシを交代で使用します。
- プライマリ プロキシで障害が発生した場合に備えて、使用するバックアップ プロキシサーバーを指定します。
- ローカル サブネットを元に、ローミング ユーザー用に最も近いプロキシを指定します。

プロキシ自動コンフィギュレーション機能の使用方法

テキストエディタを使用して、自分のブラウザにプロキシ自動コンフィギュレーション（.pac）ファイルを作成できます。.pac ファイルとは、URL のコンテンツに応じて、使用する 1 つ以上のプロキシ サーバーを指定するロジックを含む JavaScript ファイルです。.pac ファイルの取得元の URL を指定するには、**msie-proxy pac-url** コマンドを使用します。次に、**msie-proxy method** コマンドに **use-pac-url** を指定すると、ブラウザは .pac ファイルを使用してプロキシ設定を判別します。

プロキシ設定の詳細については、Cisco Secure Client管理者ガイド、リリース *3.1* [英語]、またはお使いのモバイルデバイスのリリースノートを参照してください。

例

次に、FirstGroup というグループ ポリシーのプロキシ設定を www.example.com という URL から取得するように、ブラウザを設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url value http://www.example.com
ciscoasa(config-group-policy)#
```

次に、FirstGroup というグループ ポリシーのプロキシ自動コンフィギュレーション機能をディセーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy pac-url none
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
msie-proxy method	クライアント デバイスのブラウザ プロキシ アクション（「メソッド」）を設定します。
msie-proxy server	クライアント デバイスのブラウザ プロキシ サーバーおよびポートを設定します。
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

msie-proxy server

クライアントデバイスのブラウザプロキシサーバーおよびポートを設定するには、グループ ポリシー コンフィギュレーション モードで **msie-proxy server** コマンドを入力します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

msie-proxy server { **value** *server* [*:port*] | **none** }
nomsie-proxyserver

構文の説明

none	プロキシ サーバーに指定されている IP アドレス/ホスト名またはポートがなく、サーバーが継承されないことを示します。
value *server:port*	IP アドレスまたは MSIE サーバーの名前、およびこのクライアント デバイスに適用されるポートを指定します。ポート番号は任意です。

コマンド デフォルト

デフォルトでは、no msie-proxy server が指定されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

プロキシ サーバの IP アドレスまたはホスト名およびポート番号が含まれている行の長さは、100 文字未満である必要があります。

プロキシ設定の詳細については、Cisco Secure Client管理者ガイド、リリース *3.1* [英語]、またはお使いのモバイルデバイスのリリースノートを参照してください。

例

次に、Microsoft Internet Explorer プロキシ サーバとして IP アドレス 192.168.10.1 を設定し、ポート 880 を使用し、FirstGroup というグループ ポリシーを対象にする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# msie-proxy server value 192.168.21.1:880
ciscoasa(config-group-policy)#
```

関連コマンド

コマンド	説明
show running-configuration group-policy	設定されているグループ ポリシー属性の値を表示します。
clear configure group-policy	設定されているすべてのグループ ポリシー属性を削除します。

mtu

インターフェイスの最大伝送ユニットを指定するには、グローバル コンフィギュレーション モードで **mtu** コマンドを使用します。イーサネット インターフェイスの MTU ブロック サイズを 1500 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。このコマンドは、IPv4 トラフィックと IPv6 トラフィックをサポートしています。

mtu*interface_namebytes*
nomtu*interface_namebytes*

構文の説明

bytes	MTU のバイト数。有効な値は 64 ～ 9198 バイト（セキュアクライアント および Firepower 9300 ASA セキュリティ モジュールの場合は 9000）です。
interface_name	内部または外部ネットワーク インターフェイス名。

コマンド デフォルト

イーサネット インターフェイスのデフォルトの *bytes* は 1500 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	—	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(6)	最大 MTU が 65535 から 9198（モデルによっては 9000）に変更されました。

使用上のガイドライン

mtu コマンドを使用すると、接続で送信されるペイロードサイズ（レイヤ 2 ヘッダーや VLAN タギングを除く）を設定できます。MTU 値よりも大きいデータは、送信前にフラグメント化されます。イーサネット インターフェイスのデフォルト MTU は 1500 バイトです（これは、ジャンボ フレーム予約なしの最大サイズでもある）。この場合、レイヤ 2 ヘッダー（14バイト）と VLAN タギング（4バイト）を持つパケットのサイズは 1518 バイトです。ほとんどのアプリケーションではこの値で十分ですが、ネットワーク状況によってはこれよりも小さい値にすることもできます。

ASA は、IP パス MTU ディスカバリを（RFC 1191 での規定に従って）サポートします。これにより、ホストはパスに沿ったさまざまなリンクで許容される最大 MTU サイズを動的に検出

し、サイズの差に対処できます。パケットがインターフェイスに対して設定されている MTU よりも大きいが、「Don't Fragment」（DF）ビットが設定されているために、ASA がデータグラムを転送できないことがあります。ネットワーク ソフトウェアは、メッセージを送信ホストに送信して、問題を警告します。送信ホストは、パスに沿ったすべてのリンクのうち最小のパケット サイズに適合するように、宛先へのパケットをフラグメント化する必要があります。

レイヤ 2 トンネリング プロトコル（L2TP）を使用するときは、L2TP ヘッダーと IPsec ヘッダーの長さを踏まえて MTU サイズを 1380 に設定することを推奨します。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

バージョン 9.1(6) 以降では、ASA が使用できる最大 MTU は 9198 バイトです。この値にはレイヤ 2 ヘッダーは含まれません。以前は、ASA で 65535 バイトの最大 MTU を指定できましたが、これは不正確であり、問題が発生する可能性がありました。9198 よりも大きいサイズに MTU を設定している場合は、アップグレード時に MTU のサイズが自動的に削減されます。場合によっては、この MTU の変更により MTU の不一致が発生する可能性があります。接続している機器が新しい MTU 値を使用するように設定されていることを確認してください。

例

次に、インターフェイスの MTU を指定する例を示します。

```
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 1500
ciscoasa(config)# mtu inside 8192
ciscoasa(config)# show running-config mtu
mtu outside 1500
mtu inside 8192
```

関連コマンド

コマンド	説明
clear configure mtu	すべてのインターフェイスの設定済み最大伝送単位値をクリアします。
show running-config mtu	現在の最大伝送単位のブロック サイズを表示します。

mtu cluster

クラスタ制御リンクの最大伝送ユニットを設定するには、グローバル コンフィギュレーション モードで **mtu cluster** 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。

mtu cluster *bytes*
no mtu cluster [*bytes*]

構文の説明

bytes クラスタ制御リンク インターフェイスの最大伝送単位を 64 ～ 65,535 バイトの範囲内で指定します。デフォルトの MTU は 1500 バイトです。

コマンド デフォルト

デフォルトの MTU は 1500 バイトです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

MTU を 1600 バイト以上に設定することを推奨します。設定するには、**jumbo-frame reservation** コマンドを使用して、ジャンボフレームの予約を有効にする必要があります。

このコマンドはグローバル コンフィギュレーション コマンドですが、ブートストラップ コンフィギュレーションの一部でもあります。ブートストラップ コンフィギュレーションは、ユニット間で複製されません。

例

次に、クラスタ制御リンクの MTU を 9000 バイトに設定する例を示します。

```
ciscoasa(config)# mtu cluster 9000
```

関連コマンド

コマンド	説明
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
jumbo frame-reservation	ジャンボイーサネットフレームの使用をイネーブルにします。

multicast boundary

管理用スコープのマルチキャストアドレスのマルチキャスト境界を設定するには、インターフェイス コンフィギュレーション モードで **multicast boundary** コマンドを使用します。境界を削除するには、このコマンドの **no** 形式を使用します。マルチキャスト境界により、マルチキャスト データ パケット フローが制限され、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できるようになります。

multicast boundary *acl* [**filter-autorp**]
no multicast boundary *acl* [**filter-autorp**]

構文の説明

acl	アクセス リストの名前または番号を指定します。アクセス リストには、境界の影響を受けるアドレスの範囲を定義します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。
filter-autorp	境界 ACL によって拒否された Auto-RP メッセージをフィルタリングします。指定されていない場合、すべての Auto-RP メッセージが通過します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、*acl* 引数によって定義されている範囲でマルチキャスト グループ アドレスをフィルタリングするようにインターフェイスに管理用スコープの境界を設定するために使用されます。影響を受けるアドレス範囲は、標準アクセス リストによって定義されます。このコマンドが設定されている場合、マルチキャスト データ パケットはいずれの方向であっても境界を通過できません。マルチキャスト データ パケット フローを制限すると、同じマルチキャスト グループ アドレスを複数の管理ドメインで再利用できます。

filter-autorp キーワードを設定した場合、管理用スコープの境界で Auto-RP 検出メッセージおよびアナウンスメッセージが検査され、境界 ACL によって拒否される Auto-RP パケットから Auto-RP グループ範囲アナウンスメントが削除されます。Auto-RP グループ範囲通知は、Auto-RP グループ範囲のすべてのアドレスが境界 ACL によって許可される場合に限り境界を通過できます。許可されないアドレスがある場合は、グループ範囲全体がフィルタリングされ、Auto-RP メッセージが転送される前に Auto-RP メッセージから削除されます。

例

次に、すべての管理用スコープのアドレスの境界を設定し、Auto-RP メッセージをフィルタリングする例を示します。

```
ciscoasa(config)# access-list boundary_test deny 239.0.0.0 0.255.255.255
ciscoasa(config)# access-list boundary_test permit 224.0.0.0 15.255.255.255
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# multicast boundary boundary_test filter-autorp
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

multicast-routing

ASA で IP マルチキャストルーティングを有効にするには、グローバル コンフィギュレーション モードで **multicast routing** コマンドを使用します。IP マルチキャストルーティング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。

multicast-routing
nomulticast-routing

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。

コマンド デフォルト

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM と IGMP を有効にします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

multicast-routing コマンドは、すべてのインターフェイスの PIM と IGMP を有効にします。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してだけ動作します。セキュリティ アプライアンスが PIM RP の場合は、セキュリティ アプライアンスの未変換の外部アドレスを、RP アドレスとして使用します。

マルチキャスト ルーティング テーブルのエントリの数は、システムに搭載されているメモリの量によって制限されます。<xref> に、セキュリティアプライアンスの RAM の量に基づいた特定のマルチキャストテーブルに関するエントリの最大数を示します。この上限に達すると、新しいエントリは廃棄されます。

表 *6:* マルチキャストテーブルのエントリ制限（スタティックエントリとダイナミックエントリの組み合わせ）

テーブル	16 MB	128 MB	128+ MB
MFIB	[1000]	3000	5000
IGMP グループ	[1000]	3000	5000
PIM ルート	3000	7000	12000

例

次に、ASA で IP マルチキャストルーティングを有効にする例を示します。

```
ciscoasa(config)# multicast-routing
```

関連コマンド

コマンド	説明
igmp	インターフェイスに対して IGMP をイネーブルにします。
pim	インターフェイスに対して PIM をイネーブルにします。

mus

ASA が WSA を指定する IP 範囲と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 **mus** コマンドを使用します。このサービスを無効にするには、このコマンドの **no** 形式を使用します。このコマンドは、IPv4 トラフィックと IPv6 トラフィックをサポートしています。指定したサブネットおよびインターフェイスで検索される WSA のみが登録されます。

mus *IPv4 address IPv4 mask interface_name*
no mus *IPv4 address IPv4 mask interface_name*

（注） このコマンドを想定どおりに機能させるためには、Cisco Secure Clientの AnyConnect セキュア モビリティ ライセンス サポートを提供する AsyncOS for Web バージョン 7.0 のリリースが必要です。また、AnyConnect Secure Mobility、ASA 8.3、ASDM 6.3 をサポートする AnyConnect リリースも必要です。

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

次のコマンドを使用できます。

- A.B.C.D：ASA へのアクセスを認可された WSA の IP アドレスです。
- host：クライアントは、架空のホストに要求を送信して Web セキュリティ アプライアンスへの接続を定期的にチェックします。デフォルトでは、架空のホストの URL は mus.cisco.com です。AnyConnect Security Mobility をイネーブルにすると、Web セキュリ

ティアプライアンスは、この架空のホストへの要求を傍受し、このクライアントに応答します。

- password：WSA パスワードを設定します。
- server：WSA サーバーを設定します。

例

次の例では、1.2.3.x サブネットの WSA サーバーが、*inside* インターフェイスのセキュア モビリティ ソリューションにアクセスすることを許可します。

```
ciscoasa(config)# mus 1.2.3.0 255.255.255.0 inside
```

関連コマンド

コマンド	説明
mus password	AnyConnect Secure Mobility 通信の共有秘密を設定します。
mus server	ASA が WSA 通信を聴取するポートを指定します。
show webvpn mus	アクティブな WSA 接続セキュリティ アプライアンスに関する情報を表示します。

mus host

ASA でMUS ホスト名を指定するには、グローバル コンフィギュレーション モードで **mus host** コマンドを入力します。これは、ASA から セキュアクライアント に送信されるテレメトリの URL です。セキュアクライアント では、この URL を使用して、MUS 関連サービス用のプライベートネットワークにある WSA と通信します。このコマンドで入力したコマンドを削除するには、**no mus host** コマンドを使用します。

mus host *host name*
nomushost

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

所定のポートに対して AnyConnect Secure Mobility をイネーブルにできます。WSA ポートの値は 1 ～ 21000 です。このコマンドでポートが指定されていない場合、ポート 11999 が使用されます。

このコマンドを実行する前に AnyConnect Secure Mobility の共有秘密を設定する必要があります。

（注） このコマンドを想定どおりに機能させるためには、Cisco Secure Clientの AnyConnect セキュアモビリティ ライセンス サポートを提供する AsyncOS for Web バージョン 7.0 のリリースが必要です。また、AnyConnect Secure Mobility、ASA 8.3、ASDM 6.3 をサポートする AnyConnect リリースも必要です。

例

次の例では、AnyConnect Secure Mobility ホストと WebVPN コマンド サブモードを入力する方法を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# mus 0.0.0.0 0.0.0.0 inside
ciscoasa(config-webvpn)# mus password abcdefgh123
ciscoasa(config-webvpn)# mus server enable 960 # non-default port
ciscoasa(config-webvpn)# mus host mus.cisco.com
```

関連コマンド

コマンド	説明
mus	ASA が WSA を指定する IP 範囲およびインターフェイスを指定します。
mus password	AnyConnect Secure Mobility 通信の共有秘密を設定します。
show webvpn mus	アクティブな WSA 接続セキュリティ アプライアンスに関する情報を表示します。

mus password

AnyConnectセキュアモビリティ通信の共有秘密を設定するには、グローバル コンフィギュレーション モードで **mus password** コマンドを入力します。共有秘密を削除するには、**no mus password** コマンドを使用します。

muspassword
nomuspassword

（注） このコマンドを想定どおりに機能させるためには、Cisco Secure Clientの AnyConnect セキュアモビリティ ライセンス サポートを提供する AsyncOS for Web バージョン 7.0 のリリースが必要です。また、AnyConnect Secure Mobility、ASA 8.3、ASDM 6.3 をサポートする AnyConnect リリースも必要です。

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。

コマンド デフォルト

有効なパスワードは、正規表現 [0-9, a-z, A-Z,:;_/-]{8,20} で定義されます。共有秘密パスワードの全長は、最小 8 文字、最大 20 文字です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

この WebVPN サブモードを使用すると、WebVPN 用のグローバル設定を設定できます。AnyConnect Secure Mobility 通信に共有秘密を設定できます。

例

次の例では、AnyConnect Secure Mobility パスワードと WebVPN コマンド サブモードを入力する方法を示します。

```
ciscoasa
```

```
(config)#
 mus password <password_string>
ciscoasa
(config-webvpn)#
```

関連コマンド

コマンド	説明
mus	ASA が WSA を指定する IP 範囲およびインターフェイスを指定します。
mus server	ASA が WSA 通信を聴取するポートを指定します。
show webvpn mus	アクティブな WSA 接続セキュリティ アプライアンスに関する情報を表示します。

mus server

ASA が WSA 通信をリッスンするポートを指定するには、グローバル コンフィギュレーション モードで **mus server** コマンドを入力します。このコマンドで入力したコマンドを削除するには、**no mus server** コマンドを使用します。

musserverenable
nomusserverenable

（注） このコマンドを想定どおりに機能させるためには、Cisco Secure Clientの AnyConnect セキュア モビリティ ライセンス サポートを提供する AsyncOS for Web バージョン 7.0 のリリースが必要です。また、AnyConnect Secure Mobility、ASA 8.3、ASDM 6.3 をサポートする AnyConnect リリースも必要です。

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

AnyConnect Secure Mobility サービスで使用するポートを指定する必要があります。ASA と WSA の間の通信には、管理者が指定したポート（1 ～ 21000）で確立されたセキュアな SSL 接続が使用されます。

このコマンドを実行する前に AnyConnect Secure Mobility の共有秘密を設定する必要があります。

例

次の例では、AnyConnect Secure Mobility パスワードと WebVPN コマンド サブモードを入力する方法を示します。

```
ciscoasa
(config-webvpn)#
mus server enable
?
webvpn mode commands/options
 port Configure WSA port
ciscoasa(config-webvpn)# mus server enable port 12000
```

関連コマンド

コマンド	説明
mus	ASA が WSA を指定する IP 範囲およびインターフェイスを指定します。
mus password	AnyConnect Secure Mobility 通信の共有秘密を設定します。
show webvpn mus	アクティブな WSA 接続セキュリティ アプライアンスに関する情報を表示します。

第 III 部

N-R コマンド

n

nac-authentication-server-group（廃止）

ネットワーク アドミッション コントロールのポスチャ検証に使用される認証サーバーグループを識別するには、トンネルグループ一般属性コンフィギュレーション モードで **nac-authentication-server-group** コマンドを使用します。デフォルトのリモートアクセスグループから認証サーバーグループを継承するには、継承元となる代替のグループポリシーにアクセスし、このコマンドの **no** 形式を使用します。

nac-authentication-server-group *server-group*
no nac-authentication-server-group

構文の説明

server-group	**aaa-server host** コマンドを使用して ASA に設定されたポスチャ検証サーバーグループの名前。この名前は、そのコマンドに指定された server-tag 変数に一致する必要があります。

コマンド デフォルト

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 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(1)	このコマンドは廃止されました。nac ポリシー nac フレームワーク コンフィギュレーション モードの **authentication-server-group** コマンドに置き換えられました。

使用上のガイドライン

NAC をサポートするように、少なくとも 1 つのアクセス コントロール サーバーを設定します。ACS グループの名前を指定するには、**aaa-server** コマンドを使用します。次に、その同じ名前をサーバーグループに使用して、**nac-authentication-server-group** コマンドを使用します。

例

次に、NAC ポスチャ検証に使用される認証サーバー グループとして acs-group1 を識別する例を示します。

```
ciscoasa(config-group-policy)# nac-authentication-server-group acs-group1
ciscoasa(config-group-policy)
```

次に、デフォルトのリモート アクセス グループから認証サーバー グループを継承する例を示します。

```
ciscoasa(config-group-policy)# no nac-authentication-server-group
ciscoasa(config-group-policy)
```

関連コマンド

コマンド	説明
aaa-server	AAA サーバーまたはグループのレコードを作成し、ホスト固有の AAA サーバー属性を設定します。
debug eap	EAP イベントのロギングをイネーブルにして、NAC メッセージをデバッグします。
debug eou	NAC メッセージングをデバッグするための EAP over UDP（EAPoUDP）イベントのロギングをイネーブルにします。
debug nac	NAC イベントのロギングをイネーブルにします。
nac	グループ ポリシーに対するネットワーク アドミッション コントロールをイネーブルにします。

nac-policy（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

シスコ ネットワーク アドミッション コントロール（NAC）ポリシーを作成し、または NAC ポリシーにアクセスし、ポリシーのタイプを指定するには、グローバル コンフィギュレーション モードで **nac-policy** コマンドを使用します。NAC ポリシーを構成から削除するには、このコマンドの **no** 形式を使用します。

nac-policy *nac-policy-name* **nac-framework**
no nac-policy *nac-policy-name* **nac-framework**

構文の説明

nac-policy-name	NAC ポリシーの名前。最大 64 文字で NAC ポリシーの名前を指定します。**show running-config nac-policy** コマンドは、セキュリティアプライアンスにすでに存在する各 NAC ポリシーの名前および構成を表示します。
nac-framework	NAC フレームワークを使用して、リモート ホストのネットワーク アクセス ポリシーを提供することを指定します。ASA の NAC フレームワークサービスを提供するには、シスコ アクセス コントロール サーバーがネットワークに存在している必要があります。 このタイプを指定した場合、プロンプトは現在のモードが設定 nac ポリシー nac フレームワーク コンフィギュレーション モードであることを示します。このモードでは、NAC フレームワーク ポリシーを設定できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

グループ ポリシーに割り当てられる NAC アプライアンスごとにこのコマンドを一度使用します。次に、**nac-settings** コマンドを使用して、該当する各グループポリシーに NAC ポリシーを割り当てます。IPSec または Cisco AnyConnect VPN トンネルのセットアップ時に、ASA は使用中のグループポリシーに関連付けられた NAC ポリシーを適用します。

NAC ポリシーが 1 つ以上のグループポリシーにすでに割り当てられている場合、**no nac-policy** *name* コマンドを使用してその NAC ポリシーを削除できません。

例

次のコマンドでは、NAC フレームワーク ポリシーを nac-framework1 という名前で作成し、そのポリシーにアクセスしています。

```
ciscoasa
(config)
# nac-policy nac-framework1 nac-framework
ciscoasa
(config-nac-policy-nac-framework)
```

次のコマンドでは、nac-framework1 という名前の NAC フレームワーク ポリシーを削除しています。

```
ciscoasa
(config)
# no nac-policy nac-framework1
ciscoasa
(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
show running-config nac-policy	ASA 上の各 NAC ポリシーの構成を表示します。
show nac-policy	ASA での NAC ポリシー使用状況の統計情報を表示します。
clear nac-policy	NAC ポリシー使用状況の統計情報をリセットします。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
clear configure nac-policy	グループ ポリシーに割り当てられているものを除き、すべての NAC ポリシーを実行コンフィギュレーションから削除します。

nac-settings（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC ポリシーをグループ ポリシーに割り当てるには、グループ ポリシー コンフィギュレーション モードで **nac-settings** コマンドを実行します。

nac-settings { **value** *nac-policy-name* | **none** }
no nac-settings { **value** *nac-policy-name* | **none** }

構文の説明

nac-policy-name	グループ ポリシーに割り当てられる NAC ポリシー。名前を付ける NAC ポリシーは、ASA の構成に存在している必要があります。**show running-config nac-policy** コマンドは、各 NAC ポリシーの名前および構成を表示します。
none	グループ ポリシーから *nac-policy-name* を削除し、このグループ ポリシーに関してNACポリシーの使用をディセーブルにします。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承しません。
value	名前を付ける NAC ポリシーをグループ ポリシーに割り当てます。

コマンド デフォルト

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 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

nac-policy コマンドを使用してNACポリシーの名前とタイプを指定してから、このコマンドを使用して名前とタイプをグループポリシーに割り当てます。

show running-config nac-policy コマンドは、各NACポリシーの名前および構成を表示します。

NACポリシーをグループポリシーに割り当てると、ASAはそのグループポリシーのNACを自動的に有効にします。

例

次のコマンドでは、グループ ポリシーから *nac-policy-name* を削除しています。グループ ポリシーは、デフォルトのグループ ポリシーから *nac-settings* 値を継承します。

```
ciscoasa(config-group-policy)
# no nac-settings
ciscoasa(config-group-policy)
```

次のコマンドでは、グループ ポリシーから *nac-policy-name* を削除し、このグループ ポリシーに関して NAC ポリシーの使用をディセーブルにしています。グループ ポリシーは、デフォルト グループ ポリシーから nac-settings 値を継承しません。

```
ciscoasa(config-group-policy)
# nac-settings none
ciscoasa(config-group-policy)
```

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。
show running-config nac-policy	ASA 上の各 NAC ポリシーの構成を表示します。
show nac-policy	ASA での NAC ポリシー使用状況の統計情報を表示します。
show vpn-session_summary.db	IPsecセッション、WebVPNセッション、およびNAC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。

name（ダイナミック フィルタ ブラックリストまたはホワイトリスト）

ドメイン名をボットネット トラフィック フィルタ ブラックリストまたはホワイトリストに追加するには、ダイナミック フィルタ ブラックリストまたはホワイトリスト コンフィギュレーション モードで **name** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。スタティック データベースを使用すると、ホワイトリストまたはブラックリストに追加するドメイン名または IP アドレスでダイナミック データベースを増強できます。

name *domain_name*
no name *domain_name*

構文の説明

domain_name	ブラックリストに名前を追加します。このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のブラックリスト エントリを追加できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ダイナミック フィルタ ブラックリストまたはホワイトリスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

ダイナミック フィルタ ホワイトリストまたはブラックリスト コンフィギュレーション モードを開始した後、**address** コマンドおよび **name** コマンドを使用して、適切な名前としてホワイトリストに、または不適切な名前としてブラックリストにタグ付けするドメイン名または IP アドレス（ホストまたはサブネット）を手動で入力できます。

このコマンドを複数回入力して、複数のエントリを追加できます。最大 1000 個のブラックリスト エントリと、最大 1000 個のホワイトリスト エントリを追加できます。

スタティックデータベースにドメイン名を追加した場合、ASA は、1 分間待機してからそのドメイン名の DNS 要求を送信し、ドメイン名と IP アドレスの組を *DNS* ホストキャッシュに追加します（このアクションはバックグラウンドプロセスで、ASA の設定の続行に影響しません）。

ASA にドメイン名サーバーが設定されていない、あるいはドメイン名サーバーが利用できない場合は、代わりにボットネット トラフィック フィルタ スヌーピング（ **inspect dns dynamic-filter-snooping** コマンド参照）を使用した DNS パケットインスペクションを有効にできます。DNS スヌーピングを使用している場合、感染したホストがスタティックデータベース内の名前に対して DNS 要求を送信すると、ASA は DNS パケットの中からそのドメイン名と関連 IP アドレスを見つけ出し、その名前と IP アドレスを DNS 逆ルックアップキャッシュに追加します。DNS 逆ルックアップキャッシュについては、 **inspect dns dynamic-filter-snooping** コマンドを参照してください。

DNS ホスト キャッシュのエントリには、DNS サーバーから提供される存続可能時間（TTL）値があります。許容される最大 TTL 値は 1 日（24 時間）です。DNS サーバーによって提供された TTL がこれより大きい場合は、TTL が 1 日以下に切り詰められます。

DNS ホストキャッシュの場合、エントリがタイムアウトすると、ASA がエントリの更新を定期的に要求します。

例

次に、ブラックリストおよびホワイトリストのエントリを作成する例を示します。

```
ciscoasa(config)# dynamic-filter blacklist
ciscoasa(config-llist)# name bad1.example.com
ciscoasa(config-llist)# name bad2.example.com
ciscoasa(config-llist)# address 10.1.1.1 255.255.255.0
ciscoasa(config-llist)# dynamic-filter whitelist
ciscoasa(config-llist)# name good.example.com
ciscoasa(config-llist)# name great.example.com
ciscoasa(config-llist)# name awesome.example.com
ciscoasa(config-llist)# address 10.1.1.2
 255.255.255.255
```

関連コマンド

コマンド	説明
address	IP アドレスをブラックリストまたはホワイトリストに追加します。
clear configure dynamic-filter	実行ボットネット トラフィック フィルタ コンフィギュレーションをクリアします。
clear dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピング データをクリアします。
clear dynamic-filter reports	ボットネット トラフィック フィルタのレポート データをクリアします。

コマンド	説明
clear dynamic-filter statistics	ボットネット トラフィック フィルタの統計情報をクリアします。
dns domain-lookup	サポートされているコマンドに対してネームルックアップを実行するために、ASA が DNS サーバーに DNS 要求を送信できるようにします。
dns server-group	ASA の DNS サーバーを指定します。
dynamic-filter blacklist	ボットネット トラフィック フィルタのブラックリストを編集します。
dynamic-filter database fetch	ボットネット トラフィック フィルタのダイナミック データベースを手動で取得します。
dynamic-filter database find	ドメイン名または IP アドレスをダイナミック データベースから検索します。
dynamic-filter database purge	ボットネット トラフィック フィルタのダイナミック データベースを手動で削除します。
dynamic-filter enable	アクセス リストを指定しない場合に、トラフィックのクラスまたはすべてのトラフィックのボットネット トラフィック フィルタをイネーブルにします。
dynamic-filter updater-client enable	ダイナミック データベースのダウンロードをイネーブルにします。
dynamic-filter use-database	ダイナミック データベースの使用をイネーブルにします。
dynamic-filter whitelist	ボットネット トラフィック フィルタのホワイトリストを編集します。
inspect dns dynamic-filter-snoop	DNS インスペクションとボットネット トラフィック フィルタ スヌーピングをイネーブルにします。
name	ブラックリストまたはホワイトリストに名前を追加します。
show asp table dynamic-filter	高速セキュリティ パスにインストールされているボットネット トラフィック フィルタ ルールを表示します。
show dynamic-filter data	ダイナミック データベースが最後にダウンロードされた日時、データベースのバージョン、データベースに含まれているエントリの数、10 個のサンプル エントリなど、ダイナミック データベースに関する情報を表示します。

コマンド	説明
show dynamic-filter dns-snoop	ボットネット トラフィック フィルタの DNS スヌーピングの概要を表示します。**detail** キーワードを指定した場合は、実際の IP アドレスおよび名前を表示します。
show dynamic-filter reports	上位 10 個のボットネット サイト、ポート、および感染したホストに関するレポートを生成します。
show dynamic-filter statistics	ボットネット トラフィック フィルタでモニターされた接続の数、およびこれらの接続のうち、ホワイトリスト、ブラックリスト、グレイリストに一致する接続の数を表示します。
show dynamic-filter updater-client	サーバーの IP アドレス、ASA が次にサーバーに接続する日時、最後にインストールされたデータベースのバージョンなど、アップデートサーバーに関する情報を表示します。
show running-config dynamic-filter	ボットネット トラフィック フィルタの実行コンフィギュレーションを表示します。

name（グローバル）

IP アドレスに名前を関連付けるには、グローバル コンフィギュレーション モードで **name** コマンドを使用します。テキスト名の使用は無効にするが、構成からは削除しない場合は、このコマンドの **no** 形式を使用します。

name *ip_address* [*name* [**description** *text*]]
no name *ip_address* [*name* [**description** *text*]]

構文の説明

description	（任意）IP アドレス名の説明を指定します。
ip_address	名前を付けるホストの IP アドレスを指定します。
name	IP アドレスに割り当てられる名前を指定します。使用できる文字は、a ～ z、A ～ Z、0 ～ 9、ダッシュ、およびアンダースコアです。*name* は、63 文字以下である必要があります。また、*name* は数値で開始できません。
text	説明のテキストを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.0(4)	このコマンドは、任意の説明を含めることができるように拡張されました。
8.3(1)	**nat** コマンドまたは **access-list** コマンドでは名前付き IP アドレスを使用できなくなりました。代わりに **object network** 名を使用する必要があります。オブジェクトグループの **network-object** コマンドでは、**object network** 名を指定できますが、**name** コマンドで指定した名前付き IP アドレスも引き続き使用できます。

使用上のガイドライン

名前と IP アドレスとの関連付けを有効にするには、**names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。

name コマンドを使用する前に、まず **names** コマンドを使用する必要があります。name コマンドは、names コマンドの使用直後、かつ **write memory** コマンドの前に使用します。

name コマンドを使用すると、テキスト名でホストを識別し、テキスト文字列を IP アドレスにマッピングします。**no name** コマンドを使用すると、テキスト名の使用を無効化できますが、構成からテキスト名は削除されません。構成から名前のリストをクリアするには、**clear configure name** コマンドを使用します。

name 値の表示を無効にするには、**no names** コマンドを使用します。

name コマンドと names コマンドは両方ともコンフィギュレーションに保存されます。

name コマンドは、ネットワーク マスクへの名前の割り当てをサポートしません。たとえば、次のコマンドは拒否されます。

```
ciscoasa(config)# name 255.255.255.0 class-C-mask
```

（注） マスクを必要とするいずれのコマンドも、受け入れ可能なネットワーク マスクとして名前を処理できません。

例

次に、**names** コマンドを使用して、 **name** コマンドの使用を有効にする例を示します。**name** コマンドは、192.168.42.3 の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用します。IP アドレスをネットワーク インターフェイスに割り当てるときに、**ip address** コマンドでこれらの名前を使用できます。**no names** コマンドは、**name** コマンド値の表示を無効にします。後で **names** コマンドを使用すると、 **name** コマンド値が再度表示されるようになります。

```
ciscoasa(config)# names
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前のリストをクリアします。

コマンド	説明
names	名前と IP アドレスの関連付けをイネーブルにします。
show running-config name	IP アドレスに関連付けられた名前を表示します。

nameif

インターフェイスの名前を指定するには、インターフェイス コンフィギュレーション モードで **nameif** コマンドを使用します。名前を削除するには、このコマンドの **no** 形式を使用します。インターフェイス名はインターフェイスタイプおよびID（gigabitethernet0/1 など）ではなく ASA のすべてのコンフィギュレーション コマンドで使用されるため、トラフィックがインターフェイスを通過するためにはインターフェイス名が必要です。

nameif *name*
no nameif

構文の説明

name 最大 48 文字で名前を設定します。名前は大文字と小文字が区別されません。「Metrics_History」または「MH」という名前を使用しないでください。これらの名前を使用すると、ASDM はインターフェイスをダウン状態として表示します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、グローバル コンフィギュレーション コマンドからインターフェイス コンフィギュレーション モード コマンドに変更されました。

使用上のガイドライン

サブインターフェイスの場合、 **nameif** コマンドを入力する前に、**vlan** コマンドで VLAN を割り当てる必要があります。

名前を変更するには、このコマンドで新しい値を再入力します。その名前を参照するすべてのコマンドが削除されるため、 **no** 形式は入力しないでください。

例

次に、2 つのインターフェイスにそれぞれ「inside」と「outside」という名前を設定する例を示します。

```
ciscoasa(config)# interface gigabitethernet0/1
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# interface gigabitethernet0/0
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 10.1.2.1 255.255.255.0
ciscoasa(config-if)# no shutdown
```

関連コマンド

コマンド	説明
clear xlate	既存の接続に対するすべての変換をリセットして、その結果として接続をリセットします。
interface	インターフェイスを設定し、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。
security-level	インターフェイスのセキュリティ レベルを設定します。
vlan	サブインターフェイスに VLAN ID を割り当てます。

names

名前と IP アドレスの関連付けを有効にするには、グローバル コンフィギュレーション モードで **names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。**name** 値の表示を無効にするには、**no names** コマンドを使用します。

names
no names

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

名前と IP アドレスとの関連付けを有効にするには、**names** コマンドを使用します。IP アドレスに関連付けできる名前は 1 つだけです。

name コマンドを使用する前に、まず **names** コマンドを使用する必要があります。name コマンドは、names コマンドの使用直後、かつ **write memory** コマンドの前に使用します。

name 値の表示を無効にするには、**no names** コマンドを使用します。

name コマンドと names コマンドは両方ともコンフィギュレーションに保存されます。

例

次に、**names** コマンドを使用して、 **name** コマンドの使用を有効にする例を示します。**name** コマンドは、192.168.42.3 の代わりに **sa_inside** を使用し、209.165.201.3 の代わりに **sa_outside** を使用します。IP アドレスをネットワーク インターフェイスに割り当てるときに、**ip address** コマンドでこれらの名前を使用できます。**no names** コマンドは、**name** コマンド値の表示を無効にします。後で **names** コマンドを使用すると、 **name** コマンド値が再度表示されるようになります。

```
ciscoasa(config)# names
```

```
ciscoasa(config)# name 192.168.42.3 sa_inside
ciscoasa(config)# name 209.165.201.3 sa_outside
ciscoasa(config-if)# ip address inside sa_inside 255.255.255.0
ciscoasa(config-if)# ip address outside sa_outside 255.255.255.224
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
ciscoasa(config)# no names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address 192.168.42.3 mask 255.255.255.0
outside ip address 209.165.201.3 mask 255.255.255.224
ciscoasa(config)# names
ciscoasa(config)# show ip address
System IP Addresses:
inside ip address sa_inside mask 255.255.255.0
outside ip address sa_outside mask 255.255.255.224
```

関連コマンド

コマンド	説明
clear configure name	コンフィギュレーションから名前のリストをクリアします。
name	名前を IP アドレスに関連付けます。
show running-config name	IP アドレスに関連付けられた名前のリストを表示します。
show running-config names	IP アドレスと名前の変換を表示します。

name-separator（pop3s、imap4s、smtps）（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

電子メール、VPNユーザー名、パスワード間のデリミタとなる文字を指定するには、適用可能な電子メールプロキシモードで **name-separator** コマンドを使用します。デフォルトの「:」に戻すには、このコマンドの **no** 形式を使用します。

name-separator [*symbol*]
no name-separator

構文の説明

シンボル	（任意）電子メール、VPN ユーザー名、パスワードを区切る文字。使用できるのは、「@」（アットマーク）、「|」（パイプ）、「:」（コロン）、「#」（番号記号）、「,」（カンマ）、および「;」（セミコロン）です。

コマンド デフォルト

デフォルトは「:」（コロン）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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
pop3s	• 対応	• —	• 対応	• —	—
Imap4s	対応	—	対応	—	—
Smtps	対応	—	対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

名前の区切り文字には、サーバーの区切り文字とは異なる文字を使用する必要があります。

例

次に、番号記号（#）を POP3S の名前区切り文字として設定する例を示します。

```
ciscoasa
```

```
(config)#
 pop3s
ciscoasa(config-pop3s)# name-separator #
```

関連コマンド

コマンド	説明
server-separator	電子メールとサーバー名を区切ります。

name-server

ASA がホスト名を IP アドレスに解決できるように 1 つ以上の DNS サーバーを識別するには、DNS サーバー グループ コンフィギュレーション モードで **name-server** コマンドを使用します。1 つ以上のサーバーを削除するには、このコマンドの **no** 形式を使用します。

（注） ASA では、機能に応じて DNS サーバーの使用が限定的にサポートされます。たとえば、ほとんどのコマンドでは、IP アドレスを入力する必要があります。名前を使用できるのは、名前と IP アドレスを関連付けるように **name** コマンドを手動で設定し、**names** コマンドを使用して名前の使用を有効にした場合だけです。

name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] [*interface_name*]
no name-server *ip_address* [*ip_address2*] [...] [*ip_address6*] [*interface_name*]

構文の説明

interface_name	（オプション）ASA がサーバーとの通信に使用するインターフェイス名を指定します。インターフェイスを指定しなかった場合、ASA はデータ ルーティング テーブルを確認し、一致するものが見つからなければ、管理専用ルーティング テーブルを確認します。
ip_address	DNS サーバーの IP アドレスを指定します。最大 6 つのアドレスを個別のコマンドとして指定するか、便宜上最大 6 つのアドレスをスペースで区切って 1 つのコマンドで指定できます。1 つのコマンドに複数のサーバーを入力した場合、ASA は各サーバーを個別のコマンドとして構成に保存します。ASA では、応答を受信するまで各 DNS サーバを順に試します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
DNS サーバー グループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(1)	*interface_name* 引数が追加されました。

使用上のガイドライン

DNS ルックアップを有効にするには、**dns domain-lookup** コマンドを使用します。DNS ルックアップをイネーブルにしないと、DNS サーバーは使用されません。

ASA のデフォルトでは、発信要求に **dns server-group DefaultDNS** サーバーグループが使用されます。**dns-group** コマンドを使用してデフォルトのサーバーグループを変更できます。他のサーバーグループを特定のドメインに関連付けることができます。DNS サーバーグループに関連付けられたドメインに一致する DNS 要求は、そのグループを使用します。たとえば、内部の eng.cisco.com サーバー宛てのトラフィックで内部の DNS サーバーを使用する場合は、eng.cisco.com を内部の DNS グループにマッピングできます。ドメインマッピングと一致しないすべての DNS 要求は、関連付けられたドメインを持たないデフォルトの DNS サーバーグループを使用します。たとえば、DefaultDNS グループには、外部インターフェイスで使用可能なパブリック DNS サーバーを含めることができます。PN トンネル グループ用に他の DNS サーバー グループを設定できます。詳細については、**tunnel-group** コマンドを参照してください。

一部の ASA 機能では、ドメイン名で外部サーバーにアクセスするために DNS サーバーを使用する必要があります。たとえば、ボットネット トラフィック フィルタ機能では、ダイナミック データベース サーバーにアクセスして、スタティック データベースのエントリを解決するために DNS サーバーが必要です。さらに、Cisco Smart Software Licensing では、ライセンス機関のアドレスの解決に DNS が必要です。他の機能（**ping** コマンドや **traceroute** コマンドなど）では、ping や traceroute を実行する名前を入力できるため、ASA は DNS サーバーと通信することで名前を解決できます。名前は、多くの SSL VPN コマンドおよび certificate コマンドでもサポートされます。また、アクセス ルールに完全修飾ドメイン名（FQDN）ネットワーク オブジェクトを使用するために、DNS サーバーを設定する必要もあります。

name-server のインターフェイスを指定しない場合、ASA はデータのルーティング テーブルをチェックします。ここで一致が見つからない場合は、管理専用のルーティング テーブルをチェックします。データ インターフェイスを経由するデフォルト ルートがある場合は、すべての DNS トラフィックがそのルートに一致するため、管理専用ルーティング テーブルが確認されることはありません。このシナリオでは、管理インターフェイスを経由してサーバーにアクセスする必要がある場合は常にインターフェイスを指定します。

例

次に、3 つの DNS サーバーをグループ「DefaultDNS」に追加する例を示します。

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.1.1.1 10.2.3.4 192.168.5.5
```

ASA では、次に示すように、別々のコマンドとして構成が保存されます。

```
name-server 10.1.1.1
```

```
name-server 10.2.3.4
name-server 192.168.5.5
```

さらに 2 つのサーバーを追加するには、それらを 1 つのコマンドとして入力します。

```
ciscoasa(config)# dns server-group
DefaultDNS
ciscoasa(config-dns-server-group)# name-server 10.5.1.1 10.8.3.8
```

複数のサーバーを削除するには、次のようにそれらのサーバーを複数のコマンドまたは 1 つのコマンドとして入力します。

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# no
 name-server 10.5.1.1 10.8.3.8
```

関連コマンド

コマンド	説明
domain-name	デフォルトのドメイン名を設定します。
retries	ASA が応答を受信しないときに、DNS サーバーのリストを再試行する回数を指定します。
timeout	次の DNS サーバーを試行するまでに待機する時間を指定します。
show running-config dns server-group	既存の DNS サーバー グループ コンフィギュレーションのうちの 1 つまたはすべてを表示します。

nat（グローバル）

IPv4、IPv6、または IPv4 と IPv6 の間（NAT64）で Twice NAT 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 **nat** コマンドを使用します。Twice NAT コンフィギュレーションを削除するには、このコマンドの **no** 形式を使用します。

スタティック NAT の場合：

nat [(*real_ifc* , *mapped_ifc*)] [*line* | { **after-auto** [*line*] }] **source static** { *real_obj* | **any** } { *mapped_obj* | **interface** [**ipv6**] | **any** }] [**destination static** { *mapped_obj* | **interface** [**ipv6**] } { *real_obj* | **any** }] [**service** { *real_src_mapped_dest_svc_obj* | **any** } *mapped_src_real_dest_svc_obj*] [**net-to-net**] [**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**inactive**] [**description** *desc*

no nat [(*real_ifc* , *mapped_ifc*)] [*line* | { **after-auto** [*line*] }] **source static** { *real_obj* | **any** } { *mapped_obj* | **interface** [**ipv6**] | **any** }] [**destination static** { *mapped_obj* | **interface** [**ipv6**] } { *real_obj* | **any** }] [**service** { *real_src_mapped_dest_svc_obj* | **any** } *mapped_src_real_dest_svc_obj*] [**net-to-net**] [**dns**] [**unidirectional** | [**no-proxy-arp**] [**route-lookup**]] [**inactive**] [**description** *desc*

ダイナミック NAT の場合：

nat [(*real_ifc* , *mapped_ifc*)] [*line* | { **after-auto** [*line*] }] **source dynamic** { *real_obj* | **any** } { *mapped_obj* | **interface** [**ipv6**] | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**block-allocation**] [**interface** [**ipv6**]] | **interface** [**ipv6**] } [**destination static** { *mapped_obj* | **interface** [**ipv6**] } { *real_obj* | **any** }] [**service** { *mapped_dest_svc_obj* *real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*

no nat [(*real_ifc* , *mapped_ifc*)] [*line* | { **after-auto** [*line*] }] **source dynamic** { *real_obj* | **any** } { *mapped_obj* | **interface** [**ipv6**] | **pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**block-allocation**] [**interface** [**ipv6**]] | **interface** [**ipv6**] } [**destination static** { *mapped_obj* | **interface** [**ipv6**] } { *real_obj* | **any** }] [**service** { *mapped_dest_svc_obj* *real_dest_svc_obj*] [**dns**] [**unidirectional**] [**inactive**] [**description** *desc*

または

no nat { *line* **after-auto** *line* }

構文の説明

(*real_ifc***,***mapped_ifc***)**	（任意）実際のインターフェイスおよびマッピングインターフェイスを指定します。実際のインターフェイスおよびマッピングインターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、インターフェイスのいずれかまたは両方に **any** キーワードを指定できます。ブリッジグループのメンバーインターフェイス（トランスペアレントモードまたはルーテッドモード）の場合、実際のインターフェイスおよびマッピングインターフェイスを指定する必要があります。**any** は使用できません。 Twice NAT は送信元アドレスと宛先アドレスの両方を変換するため、これらのインターフェイスを送信元インターフェイスと宛先インターフェイスとして考えると理解しやすくなります。
after-auto	NAT テーブルのセクション 3 の最後の、ネットワーク オブジェクト NAT ルールの後にルールを挿入します。デフォルトでは、Twice NAT ルールはセクション 1 に追加されます。*line* 引数を使用して、セクション 3 の任意の場所にルールを挿入できます。

any	（任意）ワイルドカードの値を指定します。**any** の主な用途は次のとおりです。 • インターフェイス：インターフェイスのいずれかまたは両方に **any** を使用できます（**(any,outside)** など）。インターフェイスを指定しない場合は、**any** がデフォルトです。ただし、**any** はブリッジグループのメンバーインターフェイスに適用されません。また、**any** はトランスペアレントモードで使用できません。 • スタティック NAT 送信元の実際の IP アドレスおよびマッピング IP アドレス：**source static any any** を指定して、すべてのアドレスに対してアイデンティティ NAT を有効にできます。 • ダイナミック NAT またはダイナミック PAT 送信元の実際のアドレス：**source dynamic any** *mapped_obj* を指定して、送信元インターフェイス上のすべてのアドレスを変換できます。 スタティック NAT の場合、実際の送信元ポートやマッピング宛先ポートに対しても、送信元または宛先の実際のアドレスに対しても、**any** を使用できますが（マッピングアドレスとしての **any** は除く）、使用すると、予期せぬ動作が発生する可能性があります。 （注） 「any」トラフィックの定義（IPv4 と IPv6）は、ルールによって異なります。ASA がパケットに対して NAT を実行するためには、そのパケットが IPv6-to-IPv6 または IPv4-to-IPv4 である必要があります。この前提条件により、ASA は、NAT ルールの **any** の値を決定できます。たとえば、「any」から IPv6 サーバーへのルールを設定しており、このサーバーが IPv4 アドレスからマッピングされている場合、**any** は「任意の IPv6 トラフィック」を意味します。「any」から「any」へのルールを設定しており、送信元をインターフェイス IPv4 アドレスにマッピングする場合、マッピングインターフェイスのアドレスによって宛先も IPv4 であることが示されるため、**any** は「任意の IPv4 トラフィック」を意味します。

block-allocation	ポートブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT の場合は、NAT に一度に 1 つずつポート変換を割り当てさせる代わりに、各ホストのポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ～ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当ては**round-robin** と互換性がありますが、**extended** または **flat** [**include-reserve**] オプションは使用できません。また、インターフェイス PAT のフォールバックを使用することもできません。
description *desc*	（任意）最大 200 文字で説明を入力します。
destination	（任意）宛先アドレスの変換を設定します。Twice NAT の主な機能は、宛先 IP アドレスを含めることですが、宛先アドレスはオプションです。宛先アドレスを指定した場合、このアドレスにスタティック変換を設定できるか、単にアイデンティティ NAT を使用できます。宛先アドレスを使用せずに Twice NAT を設定して、実際のアドレスに対するネットワーク オブジェクト グループの使用または手動でのルールの順序付けを含む、Twice NAT の他の特質の一部を活用することができます。詳細については、CLI 設定ガイドを参照してください。
dns	（任意）DNS 応答を変換します。DNS インスペクションが有効になっていることを確認してください（**inspect dns**）（デフォルトでは有効）。**destination** アドレスを設定する場合、**dns** キーワードは設定できません。このオプションを PAT ルールとともに使用することはできません。詳細については、CLI コンフィギュレーション ガイドを参照してください。
dynamic	送信元アドレスのダイナミック NAT またはダイナミック PAT を設定します。宛先変換は、常にスタティックです。
extended	（オプション）PAT プールの拡張 PAT をイネーブルにします。拡張 PAT では、変換情報に宛先アドレスとポートを含めることで、IP アドレスごとではなく、*service* ごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。

flat [**include-reserve**] **include-reserve**	（任意、9.15 より前）ポートを割り当てるときに 1024 ～ 65535 のポート範囲全体を使用できるようにします。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲（1～511、512 ～ 1023、および 1024 ～ 65535）からマッピング ポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、**include-reserve** キーワードも指定します。 (9.15 以降) 9.15 以降、falt は PAT プールのデフォルト設定不可能な動作です。**include-reserve** キーワードは flat キーワードから独立しているため、予約済みポートの 1 ～ 1023 を PAT プールに含めることを引き続き選択できます。
inactive	（任意）コマンドを削除する必要がなく、このルールを非アクティブにするには、**inactive** キーワードを使用します。再度アクティブ化するには、**inactive** キーワードを除いてコマンド全体を再入力します。
interface [**ipv6**]	（任意）インターフェイス IP アドレスをマッピング アドレスとして使用します。**ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。 ダイナミック NAT の送信元マッピングアドレスに対して、マッピングされたオブジェクトまたはグループに続けて **interface** キーワードを指定した場合、マッピングインターフェイスの IP アドレスは、他のすべてのマッピングアドレスがすでに割り当てられている場合にのみ使用されます。 ダイナミック PAT の場合は、送信元マッピングアドレスに対して **interface** のみ指定できます。 ポート変換を使用するスタティック NAT（送信元または宛先）の場合は、**service** キーワードも設定します。 このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。 このオプションは、トランスペアレント モードでは使用できません。ルーテッド モードでは、宛先インターフェイスがブリッジ グループのメンバーの場合、このオプションを使用することはできません。

line	（任意）NAT テーブルのセクション 1 の任意の場所にルールを挿入します。デフォルトでは、セクション 1 の最後に NAT ルールが追加されます（詳細については、設定ガイドを参照してください）。その代わりに、セクション 3 に（ネットワークオブジェクト NAT ルールの後）ルールを追加する場合は、**after-auto** *line* オプションを使用します。
mapped_dest_svc_obj	（任意）ダイナミック NAT およびダイナミック PAT の場合は、マッピング宛先ポートを指定します（宛先の変換は常に固定です）。詳細については、**service** キーワードを参照してください。
mapped_object	マッピングされたネットワークオブジェクトまたはオブジェクトグループ（**object network** または **object-group network**）を指定します。 ダイナミック NAT では、通常、大きいアドレスのグループが小さいグループにマッピングされます。 （注） マッピングされたオブジェクトやグループにサブネットを含めることはできませんが、必要に応じて、このマッピングされた IP アドレスを異なるダイナミック NAT ルール間で共有できます。IPv4 アドレスと IPv6 アドレスの両方で 1 つのオブジェクトグループを使用することはできません。そのオブジェクトグループには、1 種類のアドレスのみを含める必要があります。 ダイナミック PAT の場合は、単一のアドレスにマッピングするアドレスのグループを設定します。実際のアドレスを選択した単一のマッピング アドレスに変換するか、またはマッピング インターフェイス アドレスに変換できます。インターフェイスアドレスを使用する場合は、マッピングアドレスにネットワークオブジェクトを設定せずに、**interface** キーワードを使用します。 スタティック NAT のマッピングは、通常 1 対 1 です。したがって、実際のアドレスとマッピング アドレスの数は同じです。ただし、必要に応じて異なる数にすることができます。詳細については、CLI 設定ガイドを参照してください。
mapped_src_real_dest_svc_obj	（オプション）スタティック NAT の場合は、マッピング送信元ポート、実際の宛先ポート、またはその両方を指定します。詳細については、**service** キーワードを参照してください。
net-to-net	（任意）スタティック NAT 46 の場合は、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に変換されます（以降も同様）。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。

no-proxy-arp	（オプション）スタティック NAT の場合に、マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。
pat-pool *mapped_obj*	（オプション）アドレスの PAT プールをイネーブルにします。オブジェクトのすべてのアドレスが PAT アドレスとして使用されるようになります。ダイナミック NAT の場合、PAT プールをフォールバック方式として設定できます。1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
real_dest_svc_obj	（任意）ダイナミック NAT およびダイナミック PAT の場合は、実際の宛先ポートを指定します（宛先の変換は常に固定です）。詳細については、**service** キーワードを参照してください。
real_ifc	（任意）パケットが発信される可能性のあるインターフェイスの名前を指定します。送信元オプション。送信元オプションの場合、origin_ifc は実際のインターフェイスです。宛先オプションの場合、real_ifc はマッピング インターフェイスです。
real_object	マッピングされた実際のネットワークオブジェクトまたはオブジェクトグループ（**object network** または **object-group network**）を指定します。1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
real_src_mapped_dest_svc_obj	（任意）スタティック NAT の場合は、実際の送信元ポート、マッピング宛先ポート、またはその両方を指定します。詳細については、**service** キーワードを参照してください。
round-robin	（オプション）PAT プールのラウンドロビン アドレス割り当てをイネーブルにします。デフォルトでは、次の PAT アドレスが使用される前に PAT アドレスのすべてのポートが割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2 番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。
route-lookup	（オプション）ルーテッド モードのアイデンティティ NAT で、NAT コマンドで指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定します。NAT コマンドでインターフェイスを指定しない場合、デフォルトでルート ルックアップが使用されます。

service	（任意）ポート変換を指定します。 • ダイナミック NAT およびダイナミック PAT：ダイナミック NAT およびダイナミック PAT では、（追加的な）ポート変換はサポートされません。しかし、宛先変換は常にスタティックなので、宛先ポートに対してポート変換を実行できます。サービスオブジェクト（**object service**）には送信元ポートと宛先ポートの両方を含めることができますが、両方含めた場合、宛先ポートだけが使用されます。送信元ポートを指定した場合、無視されます。 • ポート変換を使用するスタティック NAT：両方のサービスオブジェクトに送信元ポートまたは宛先ポートのいずれかを指定する必要があります。ご使用のアプリケーションが固定の送信元ポートを使用する場合（一部の DNS サーバーなど）に送信元ポートおよび宛先ポートの両方を指定する必要がありますが、固定の送信元ポートはめったに使用されません。 送信元ポート変換の場合、オブジェクトは送信元サービスを指定する必要があります。この場合、コマンドのサービスオブジェクトの順番は、**service** *real_port mapped_port* です。宛先ポート変換の場合、オブジェクトは宛先サービスを指定する必要があります。この場合、サービスオブジェクトの順番は、**service** *mapped_port real_port* です。オブジェクトで送信元ポートと宛先ポートの両方を指定することはほとんどありませんが、この場合には、最初のサービス オブジェクトに実際の送信元ポート/マッピングされた宛先ポートが含まれます。2 つめのサービス オブジェクトには、マッピングされた送信元ポート/実際の宛先ポートが含まれます。「送信元」および「宛先」の用語については、「使用上のガイドライン」を参照してください。 アイデンティティ ポート変換の場合は、実際のポートとマッピング ポートの両方（コンフィギュレーションに応じて、送信元ポート、宛先ポート、またはその両方）に同じサービス オブジェクトを使用するだけです。「not equal（等しくない）」（**neq**）演算子はサポートされていません。 NAT では、TCP または UDP のみがサポートされます。ポートを変換する場合、実際のサービス オブジェクトのプロトコルとマッピング サービス オブジェクトのプロトコルの両方が同じになるようにします（両方とも TCP または両方とも UDP）。
source	送信元アドレスの変換を設定します。
static	スタティック NAT またはポート変換を使用するスタティック NAT を設定します。

unidirectional	（任意）スタティック NAT の場合は、変換を送信元から宛先への単方向にします。宛先アドレスは、送信元アドレスへのトラフィックを開始できません。テストを目的とする場合は、このオプションが便利です。

コマンド デフォルト

- デフォルトでは、NAT テーブルのセクション 1 の最後にルールが追加されます。
- *real_ifc* および *mapped_ifc* のデフォルト値は **any** で、すべてのインターフェイスにルールが適用されます。
- （8.3(1)、8.3(2)、8.4(1)）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。（8.4(2) 以降）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。
- オプションのインターフェイスを指定する場合、ASA によって NAT 構成が使用されて、出力インターフェイスが決定されます。（8.3(1) ～ 8.4(1)）唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルート ルックアップが使用されます。（8.4(2) 以降）アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションの使用ですが、代わりにルート ルックアップを常に使用するオプションがあります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
8.3(2)	8.3 よりも前の NAT 免除コンフィギュレーションの移行時にスタティック アイデンティティ NAT ルールを生成する **unidirectional** キーワードが追加されました。

リリース	変更内容
8.4(2)/8.5(1)	**no-proxy-arp**、**route-lookup**、 **pat-pool**、および **round-robin** キーワードが追加されました。 アイデンティティ NAT のデフォルトの動作が、プロキシ ARP をイネーブルにし、他のスタティック NAT ルールと照合するように変更されました。 8.3 よりも前の設定の場合、8.4(2) 以降への NAT 免除ルール（**nat 0 access-list** コマンド）の移行には、プロキシ ARP を無効にするキーワード **no-proxy-arp** およびルートルックアップを使用するキーワード **route-lookup** があります。8.3(2) および 8.4(1) への移行に使用された **unidirectional** キーワードは、移行に使用されなくなりました。8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードする場合、既存の機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに **no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになりました。**unidirectional** キーワードが削除されました。
8.4(3)	**extended**、**flat**、および **include-reserve** キーワードが追加されました。 ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 この機能は、*8.5(1)* では使用できません。
9.0(1)	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。**interface ipv6** オプションと **net-to-net** オプションが追加されました。
9.5(1)	**block-allocation** キーワードが追加されました。
9.15(1)	**flat** キーワードが削除され、**include-reserve** キーワードは flat のサブパラメータではなくなりました。すべての PAT プールで 1024 ー 65535 のフラットなポート範囲が使用されるようになり、オプションで予約済みポート（1 ー 1023）を含めることができるようになりました。
9.17(1)	変換された（マッピングされた）宛先として FQDN ネットワークオブジェクトを指定できます。

使用上のガイドライン

使用上のガイドライン

Twice NAT では、1 つのルールで送信元アドレスおよび宛先アドレスの両方を識別できます。送信元アドレスと宛先アドレスの両方を指定すると、たとえば送信元アドレスが宛先 X に向かう場合は A に変換され、宛先 Y に向かう場合は B に変換されるように指定できます。

（注） スタティック NAT の場合、ルールは双方向であるため、たとえば、特定の接続が「宛先」アドレスから発生する場合でも、このガイドを通じてのコマンドおよび説明では「送信元」および「宛先」が使用されていることに注意してください。たとえば、ポート変換を使用するスタティック NAT を設定し、送信元アドレスを Telnet サーバーとして指定する場合に、Telnet サーバーに向かうすべてのトラフィックのポートを 2323 から 23 に変換するには、このコマンドで、変換する送信元ポート（実際：23、マッピング：2323）を指定する必要があります。Telnet サーバーアドレスを**source**アドレスとして指定しているため、その送信元ポートを指定します。

宛先アドレスはオプションです。宛先アドレスを指定する場合、宛先アドレスを自身にマッピングするか（アイデンティティ NAT）、別のアドレスにマッピングできます。宛先マッピングは、常にスタティック マッピングです。

Twice NAT では、ポート変換が設定されたスタティック NAT のサービス オブジェクトを使用できます。ネットワーク オブジェクト NAT は、インライン定義だけを受け入れます。

Twice NAT とネットワーク オブジェクト NAT の違いの詳細については、CLI 設定ガイドを参照してください。

Twice NAT ルールは、NAT ルール テーブルのセクション 1 に追加されます。指定した場合には、セクション 3 に追加されます。NAT 順序の詳細については、CLI 設定ガイドを参照してください。

マッピングアドレスのガイドライン

マッピング IP アドレス プールに、次のアドレスを含めることはできません。

- マッピング インターフェイスの IP アドレス。ルールに **any** インターフェイスを指定した場合は、すべてのインターフェイス IP アドレスが無効になります。インターフェイス PAT（ルーテッドモードのみ）の場合は、IP アドレスの代わりに **interface** キーワードを使用します。
- （トランスペアレント モード）管理 IP アドレス。
- （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
- 既存の VPN プールのアドレス。

前提条件

- 実際のアドレスとマッピングアドレスの両方に、ネットワークオブジェクトまたはネットワーク オブジェクト グループを設定します（**object network** または **object-group network** コマンド）。ネットワーク オブジェクト グループは、非連続的な IP アドレスの範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。

- ポート変換を使用するスタティック NAT の場合は、TCP または UDP のサービスオブジェクト（**object service** コマンド）を設定します。

NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。

変換セッションのクリア

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするまで待たずに新しい NAT 情報を使用するために、clear xlate コマンドを使用して変換テーブルをクリアできます。ただし、変換テーブルをクリアすると、現在の接続がすべて切断されます。

PAT プールのガイドライン

- 個々の A レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- （9.15 より前）使用可能な場合、実際の送信元ポート番号がマッピングポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピングポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。（8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）下位ポート範囲を使用するトラフィックが多数ある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます（1024 ～ 65535、または 1 ～ 65535）。
- （9.15 以降）ポートは、1024 ー 65535 の範囲の使用可能なポートにマッピングされます。必要に応じ、1024 番未満の予約ポートを含めて、ポート範囲全体を変換に使用することもできます。

クラスタで動作する場合、アドレスごとに 512 個のポートのブロックがクラスタのメンバーに割り当てられ、これらのポートブロック内でマッピングが行われます。ブロック割り当ても有効にした場合は、ブロック割り当てサイズに従ってポートが分配されます。このデフォルトも 512 です。

- PAT プールに対してブロック割り当てを有効にする場合、ポートブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号（1 ～ 1023）を必要とするときは、機能しない可能性があります。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。
- ダイナミック NAT によってマッピングされた IP アドレスにオブジェクト グループを使用し、そのグループにホスト アドレスを含める場合、PAT プールをイネーブルにすると、ホスト アドレスの使用が PAT フォールバックからダイナミック NAT へと変更されます。
- （8.4(3) 以降、8.5(1) または 8.6(1) を除く）2 つの個別のルールで同じ PAT プール オブジェクトを使用する場合は、各ルールに対して同じオプションを指定します。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールの拡張 PAT のガイドライン

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションのリストについては、設定ガイドを参照してください。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合は、PAT プール内のアドレスを、ポート変換ルールを設定した別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーション ルールを持つスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンドロビンのガイドライン

- （8.4(3) 以降、8.5(1) または 8.6(1) を除く）ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。**Note**：この「粘着性」は、フェールオーバーが発生すると失われます。ASA がフェールオーバーすると、ホストからの後続の接続で最初の IP アドレスが使用されない場合があります。
- （8.4(2)、8.5(1)、および 8.6(1)）ホストに既存の接続がある場合、そのホストからの後続の接続では、ラウンドロビン割り当てのため、接続ごとに別の PAT アドレスが使用される可能性があります。この場合、ホストについて情報を交換する 2 つの Web サイト（e-コマース サイトと支払サイトなど）にアクセスするときに問題が発生する可能性があります。これらのサイトが、1 つのホストとして扱うべきものを 2 つの異なる IP アドレスと見なした場合、トランザクションは失敗することがあります。

NAT と IPv6

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。インターフェイスが同じブリッジ グループのメンバーの場合は NAT64/46 を実行できないことに注意してください。

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（Twice NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（Twice NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスは IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アド

レスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。

- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

例

次の例では、2 つの異なるサーバーにアクセスする、10.1.2.0/24 ネットワーク上のホストがあります。ホストがサーバー 209.165.201.11 にアクセスすると、実際のアドレスは 209.165.202.129:*port* に変換されます。ホストがサーバー 209.165.200.225 にアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
ciscoasa(config)# object network DMZnetwork1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress1 destination
 static DMZnetwork1 DMZnetwork1
ciscoasa(config)# object network DMZnetwork2
ciscoasa(config-network-object)# subnet 209.165.200.224 255.255.255.224
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# nat (inside,dmz) source dynamic myInsideNetwork PATaddress2 destination
 static DMZnetwork2 DMZnetwork2
```

次に、送信元ポートおよび宛先ポートの使用例を示します。10.1.2.0/24 ネットワークのホストは Web サービスと Telnet サービスの両方を提供する 1 つのホストにアクセスします。ホストが Telnet サービスを求めてサーバーにアクセスすると、実際のアドレスは 209.165.202.129:*port* に変換されます。ホストが Web サービスを求めて同じサーバーにアクセスすると、実際のアドレスは 209.165.202.130:*port* に変換されます。

```
ciscoasa(config)# object network myInsideNetwork
ciscoasa(config-network-object)# subnet 10.1.2.0 255.255.255.0
ciscoasa(config)# object network TelnetWebServer
ciscoasa(config-network-object)# host 209.165.201.11
ciscoasa(config)# object network PATaddress1
ciscoasa(config-network-object)# host 209.165.202.129
ciscoasa(config)# object service TelnetObj
ciscoasa(config-network-object)# service
 tcp
 destination eq telnet
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress1
destination static TelnetWebServer TelnetWebServer service TelnetObj TelnetObj
ciscoasa(config)# object network PATaddress2
ciscoasa(config-network-object)# host 209.165.202.130
ciscoasa(config)# object service HTTPObj
ciscoasa(config-network-object)# service
```

```
 tcp
 destination eq http
ciscoasa(config)# nat (inside,outside) source dynamic myInsideNetwork PATaddress2
destination static TelnetWebServer TelnetWebServer service HTTPObj HTTPObj
```

次に、ポート変換を使用するスタティック インターフェイス NAT の使用例を示します。外部にあるホストが、宛先ポート 65000 ～ 65004 を指定して外部インターフェイス IP アドレスに接続することにより、内部にある FTP サーバーにアクセスします。トラフィックは、192.168.10.100:6500 ～ :65004 の内部 FTP サーバーに変換されません。コマンドで指定した送信元アドレスとポートを変換するため、サービス オブジェクトには送信元ポート範囲（宛先ポートではなく）を指定することに注意してください。宛先ポートは「any」です。スタティック NAT は双方向であるため、「送信元」および「宛先」を使用して一次的にコマンド キーワードを扱うものであり、パケット内の実際の送信元および実際の宛先のアドレスとポートは、パケットを送信するホストによって異なります。この例では、外部から内部への接続が発生しているため、FTP サーバーの「送信元」アドレスとポートは、実際には発信元パケット内では宛先アドレスとポートになります。

```
ciscoasa(config)# object service FTP_PASV_PORT_RANGE
ciscoasa(config-service-obvject)# service tcp source range 65000 65004
ciscoasa(config)# object network HOST_FTP_SERVER
ciscoasa(config-network-obvject)# host 192.168.10.100
ciscoasa(config)# nat (inside,outside) source static HOST_FTP_SERVER interface service
FTP_PASV_PORT_RANGE FTP_PASV_PORT_RANGE
```

次に、IPv4 209.165.201.1/27 ネットワークのサーバーおよび 203.0.113.0/24 ネットワークのサーバーにアクセスする場合の IPv6 内部ネットワーク 2001:DB8:AAAA::/96 のダイナミック NAT を設定する例を示します。

```
ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# object network MAPPED_1
ciscoasa(config-network-object)# range 209.165.200.225 209.165.200.254
ciscoasa(config)# object network MAPPED_2
ciscoasa(config-network-object)# range 209.165.202.129 209.165.200.158
ciscoasa(config)# object network SERVERS_1
ciscoasa(config-network-object)# subnet 209.165.201.0 255.255.255.224
ciscoasa(config)# object network SERVERS_2
ciscoasa(config-network-object)# subnet 203.0.113.0 255.255.255.0
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_1 destination
static SERVERS_1 SERVERS_1
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW MAPPED_2 destination
static SERVERS_2 SERVERS_2
```

次に、外部 IPv6 Telnet サーバー 2001:DB8::23 へのアクセス時に内部ネットワーク 192.168.1.0/24 のインターフェイス PAT を設定し、2001:DB8:AAAA::/96 ネットワーク上のサーバーへのアクセス時に PAT プールを使用してダイナミック PAT を設定する例を示します。

```
ciscoasa(config)# object network INSIDE_NW
ciscoasa(config-network-object)# subnet 192.168.1.0 255.255.255.0
ciscoasa(config)# object network PAT_POOL
ciscoasa(config-network-object)# range 2001:DB8:AAAA::1 2001:DB8:AAAA::200
ciscoasa(config)# object network TELNET_SVR
```

```
ciscoasa(config-network-object)# host 2001:DB8::23
ciscoasa(config)# object service TELNET
ciscoasa(config-service-object)# service tcp destination eq 23
ciscoasa(config)# object network SERVERS
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW interface ipv6 destination
 static TELNET_SVR TELNET_SVR service TELNET TELNET
ciscoasa(config)# nat (inside,outside) source dynamic INSIDE_NW pat-pool PAT_POOL
destination static SERVERS SERVERS
```

関連コマンド

コマンド	説明
clear configure nat	NAT コンフィギュレーション（Twice NAT とネットワーク オブジェクト NAT の両方）を削除します。
show nat	NAT ポリシーの統計情報を表示します。
show nat pool	NAT プールに関する情報を表示します。
show running-config nat	NAT コンフィギュレーションを表示します。
show xlate	NAT セッション（xlate）情報を表示します。
xlate block-allocation	PAT ポート ブロック割り当ての特性を設定します。

nat（オブジェクト）

ネットワークオブジェクト用の NAT を設定するには、ネットワーク オブジェクト コンフィギュレーション モードで **nat** コマンドを使用します。NAT 構成を削除するには、このコマンドの **no** 形式を使用します。

ダイナミック NAT およびダイナミック PAT の場合：

nat [(*real_ifc* , *mapped_ifc*)] **dynamic** { *mapped_inline_host_ip* [**interface** [**ipv6**]] | [*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**block-allocation**]] [**interface** [**ipv6**]] } [**dns**]

no nat [(*real_ifc* , *mapped_ifc*)] **dynamic** { *mapped_inline_host_ip* [**interface** [**ipv6**]] | [*mapped_obj*] [**pat-pool** *mapped_obj* [**round-robin**] [**extended**] [**flat** [**include-reserve**]] [**block-allocation**]] [**interface** [**ipv6**]] } [**dns**]

スタティック NAT およびポート変換を使用するスタティック NAT の場合：

nat [(*real_ifc* , *mapped_ifc*)] **static** { *mapped_inline_host_ip* | *mapped_obj* | **interface** [**ipv6**] } [**net-to-net**] [**dns** | **service** { **tcp** | **udp** | **sctp** } *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]

no nat [(*real_ifc* , *mapped_ifc*)] **static** { *mapped_inline_host_ip* | *mapped_obj* | **interface** [**ipv6**] } [**net-to-net**] [**dns** | **service** { **tcp** | **udp** | **sctp** } *real_port mapped_port*] [**no-proxy-arp**] [**route-lookup**]

構文の説明

(*real_ifc***,***mapped_ifc***)**	（任意）スタティック NAT の場合は、実際のインターフェイスおよびマッピングインターフェイスを指定します。実際のインターフェイスおよびマッピング インターフェイスを指定しない場合は、すべてのインターフェイスが使用されます。また、インターフェイスのいずれかまたは両方に **any** キーワードを指定できます。コマンドには、丸カッコを含める必要があります。ブリッジグループのメンバーインターフェイス（トランスペアレントモードまたはルーテッドモード）の場合、実際のインターフェイスおよびマッピングインターフェイスを指定する必要があります。**any** は使用できません。
block-allocation	ポートブロック割り当てをイネーブルにします。キャリアグレードまたは大規模 PAT の場合は、NAT に一度に 1 つずつポート変換を割り当てさせる代わりに、各ホストのポートのブロックを割り当てることができます。ポートのブロックを割り当てると、ホストからのその後の接続では、ブロック内のランダムに選択される新しいポートが使用されます。必要に応じて、ホストが元のブロック内のすべてのポートに関してアクティブな接続を持つ場合は追加のブロックが割り当てられます。ポートブロックは、1024 ～ 65535 の範囲でのみ割り当てられます。ポートのブロック割り当ては **round-robin** と互換性がありますが、**extended** または **flat** [**include-reserve**] オプションは使用できません。また、インターフェイス PAT のフォールバックを使用することもできません。

dns	（任意）DNS 応答を変換します。DNS インスペクションが有効になっていることを確認してください（**inspect dns**）（デフォルトでは有効）。（スタティック NAT の場合）**service** キーワードを指定する場合、このオプションは使用できません。このオプションを PAT ルールとともに使用することはできません。詳細については、CLI 設定ガイドを参照してください。
dynamic	ダイナミック NAT またはダイナミック PAT を設定します。
extended	（オプション）PAT プールの拡張 PAT をイネーブルにします。拡張 PAT では、変換情報に宛先アドレスとポートを含めることで、IP アドレスごとではなく、*service* ごとに 65535 個のポートが使用されます。通常、PAT 変換の作成時に宛先ポートとアドレスは考慮されないため、PAT アドレスあたり 65535 個のポートに制限されます。たとえば、拡張 PAT を使用して、192.168.1.7:23 に向かう場合の 10.1.1.1:1027 の変換、および 192.168.1.7:80 に向かう場合の 10.1.1.1:1027 の変換を作成できます。
flat [**include-reserve**] **include-reserve**	（任意、9.15 より前）ポートを割り当てるときに 1024 ～ 65535 のポート範囲全体を使用できるようにします。変換のマッピング ポート番号を選択するときに、ASA によって、使用可能な場合は実際の送信元ポート番号が使用されます。ただし、このオプションを設定しないと、実際のポートが使用できない場合、デフォルトでは、実際のポート番号と同じポート範囲（1 ～ 511、512 ～ 1023、および 1024 ～ 65535）からマッピング ポートが選択されます。下位の範囲でポートが不足するのを回避するには、この設定を行います。1 ～ 65535 の範囲全体を使用するには、**include-reserve** キーワードも指定します。 (9.15 以降) 9.15 以降、falt は PAT プールのデフォルト設定不可能な動作です。**include-reserve** キーワードは flat キーワードから独立しているため、予約済みポートの 1 ～ 1023 を PAT プールに含めることを引き続き選択できます。

interface [**ipv6**]	（任意）ダイナミック NAT では、マッピング IP アドレス、オブジェクト、またはグループの後に続けて **interface** キーワードを指定した場合、マッピングインターフェイスの IP アドレスは、他のすべてのマッピングアドレスがすでに割り当てられている場合にのみ使用されます。 ダイナミック PAT では、マッピング IP アドレス、オブジェクト、またはグループの代わりに **interface** キーワードを指定した場合、マッピング IP アドレスのインターフェイス IP アドレスを使用します。このキーワードは、インターフェイスの IP アドレスを使用するときに使用する必要があります。インラインで、またはオブジェクトとして入力することはできません。 **ipv6** を指定した場合、インターフェイスの IPv6 アドレスが使用されます。 ポート変換を使用するスタティック NAT では、**service** キーワードを設定する場合にも **interface** キーワードを指定できます。 このオプションでは、*mapped_ifc* に特定のインターフェイスを設定する必要があります。 透過モードでは **interface** を指定できません。ルーテッド モードでは、宛先インターフェイスがブリッジグループのメンバーの場合、このオプションを使用することはできません。
mapped_inline_host_ip	**dynamic** を指定する場合は、ホスト IP アドレスを使用してダイナミック PAT を設定します。**static** を指定する場合、マッピングネットワークのネットマスクや範囲は実際のネットワークと同じです。たとえば、実際のネットワークがホストの場合、このアドレスは、ホストアドレスとして処理されます。範囲またはサブネットの場合、マッピングアドレスには、実際の範囲またはサブネットと同じ数のアドレスが含まれます。たとえば、実際のアドレスが 10.1.1.1 ～ 10.1.1.6 の範囲として定義され、172.20.1.1 をマッピング アドレスとして指定する場合、マッピング範囲には、172.20.1.1 ～ 172.20.1.6 が含まれます。推奨されない多対 1 のマッピングが必要な場合は、インライン アドレスの代わりにホスト ネットワーク オブジェクトを使用します。

mapped_obj	1 つ以上のマッピング IP アドレスをネットワークオブジェクト（**object network**）またはオブジェクトグループ（**object-group network**）として指定します。1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。 ダイナミック NAT の場合は、オブジェクトまたはグループにサブネットを含めることはできません。必要に応じて、このマッピングされたオブジェクトを異なるダイナミック NAT ルール間で共有できます。拒否されるマッピング IP アドレスについては、「マッピングアドレスのガイドライン」を参照してください。 スタティック NAT の場合、通常は、1 対 1 のマッピングに対応するように、実際のアドレスと同じ数のマッピングアドレスを設定します。しかし、アドレスの数が一致しない場合もあります。詳細については、CLI 設定ガイドを参照してください。
mapped_port	（オプション）マッピング TCP/UDP/SCTP ポートを指定します。リテラル名または 0 ～ 65535 の範囲の数字でポートを指定できます。
net-to-net	（任意）NAT 46 の場合は、**net-to-net** を指定すると、最初の IPv4 アドレスが最初の IPv6 アドレスに、2 番目が 2 番目に変換されます（以降も同様）。このオプションを指定しない場合は、IPv4 埋め込み方式が使用されます。1 対 1 変換の場合は、このキーワードを使用する必要があります。
no-proxy-arp	（オプション）スタティック NAT の場合に、マッピング IP アドレスへの着信パケットのプロキシ ARP をディセーブルにします。
pat-pool *mapped_obj*	（オプション）アドレスの PAT プールをイネーブルにします。オブジェクトのすべてのアドレスが PAT アドレスとして使用されるようになります。ダイナミック NAT の場合、PAT プールをフォールバック方式として設定できます。1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。
real_port	（オプション）スタティック NAT の場合は、実際の TCP/UDP/SCTP ポートを指定します。リテラル名または 0 ～ 65535 の範囲の数字でポートを指定できます。
round-robin	（オプション）PAT プールのラウンドロビンアドレス割り当てをイネーブルにします。デフォルトでは、次の PAT アドレスが使用される前に PAT アドレスのすべてのポートが割り当てられます。ラウンドロビン方式では、最初のアドレスに戻って再び使用される前に、2 番目のアドレス、またその次と、プール内の各 PAT アドレスからアドレス/ポートが割り当てられます。

route-lookup	（オプション）ルーテッド モードのアイデンティティ NAT で、NAT コマンドで指定したインターフェイスを使用する代わりに、ルート ルックアップを使用して出力インターフェイスを決定します。NAT コマンドでインターフェイスを指定しない場合、デフォルトでルート ルックアップが使用されます。
service {**tcp** | **udp** | **sctp**}	（オプション）ポート変換を使用するスタティック NAT の場合は、ポート変換用のプロトコル（TCP、UDP、SCTP）を指定します。
static	スタティック NAT またはポート変換を使用するスタティック NAT を設定します。

コマンド デフォルト

- *real_ifc* および *mapped_ifc* のデフォルト値は **any** で、すべてのインターフェイスにルールが適用されます。
- （8.3(1)、8.3(2)、8.4(1)）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はディセーブルにされます。これは設定できません。（8.4(2) 以降）アイデンティティ NAT のデフォルト動作で、プロキシ ARP はイネーブルにされ、他のスタティック NAT ルールと一致します。必要に応じてプロキシ ARP を無効にできます。
- オプションのインターフェイスを指定する場合、ASA によって NAT 構成が使用されて、出力インターフェイスが決定されます。（8.3(1) ～ 8.4(1)）唯一の例外はアイデンティティ NAT です。アイデンティティ NAT では、NAT コンフィギュレーションに関係なく、常にルート ルックアップが使用されます。（8.4(2) 以降）アイデンティティ NAT の場合、デフォルト動作は NAT コンフィギュレーションの使用ですが、代わりにルート ルックアップを常に使用するオプションがあります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
オブジェクト ネットワーク コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

リリース	変更内容
8.4(2)/8.5(1)	**no-proxy-arp**、**route-lookup**、 **pat-pool**、および **round-robin** キーワードが追加されました。 アイデンティティ NAT のデフォルトの動作が、プロキシ ARP をイネーブルにし、他のスタティック NAT ルールと照合するように変更されました。 8.3(1)、8.3(2)、8.4(1) から 8.4(2) にアップグレードする場合、既存の機能を保持するため、すべてのアイデンティティ NAT コンフィギュレーションに**no-proxy-arp** キーワードと **route-lookup** キーワードが含まれるようになりました。
8.4(3)	**extended**、**flat**、および **include-reserve** キーワードが追加されました。 ラウンドロビン割り当てで PAT プールを使用するときに、ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。 この機能は、*8.5(1)* では使用できません。
9.0(1)	NAT が IPv6 トラフィックをサポートするようになり、IPv4 と IPv6 の間の変換もサポートされます。IPv4 と IPv6 の間の変換は、トランスペアレント モードではサポートされません。**interface ipv6** オプションと **net-to-net** オプションが追加されました。
9.5(1)	**block-allocation** キーワードが追加されました。
9.5(2)	**service sctp** キーワードが追加されました。
9.15(1)	**flat** キーワードが削除され、**include-reserve** キーワードは flat のサブパラメータではなくなりました。すべての PAT プールで 1024 ー 65535 のフラットなポート範囲が使用されるようになり、オプションで予約済みポート（1 ー 1023）を含めることができるようになりました。

使用上のガイドライン

パケットが ASA に入ると、送信元 IP アドレスと宛先 IP アドレスの両方がネットワークオブジェクト NAT ルールと照合されます。個別の照合が行われる場合、パケット内の送信元アドレスと宛先アドレスは、個別のルールによって変換できます。これらのルールは、相互に結び付けられていません。トラフィックに応じて、異なる組み合わせのルールを使用できます。

ルールがペアになることはありません。したがって、宛先Xに向かう場合は送信元アドレスが A と変換され、宛先 Y に向かう場合は B と変換されるように指定することはできません。この種の機能には、Twice NAT を使用します（Twice NAT を使用すると、1 つのルールで送信元アドレスおよび宛先アドレスを識別できます）。

Twice NAT とネットワーク オブジェクト NAT の違いの詳細については、CLI 設定ガイドを参照してください。

ネットワーク オブジェクト NAT ルールは、NAT ルール テーブルのセクション 2 に追加されます。NAT 順序の詳細については、CLI 設定ガイドを参照してください。

構成に応じて、マッピングアドレスをインラインで設定したり、マッピングアドレスに対応する別のネットワークオブジェクトやネットワーク オブジェクト グループを作成したりできます（**object network** または **object-group network** コマンドを使用）。ネットワーク オブジェクト グループは、非連続的な IP アドレスの範囲または複数のホストやサブネットで構成されるマッピング アドレスを作成する場合に特に便利です。1 つのオブジェクト グループに IPv4 と IPv6 の両方のアドレスを入れることはできません。オブジェクト グループには、1 つのタイプのアドレスだけが含まれている必要があります。

NAT で使用されるオブジェクトおよびオブジェクト グループを未定義にすることはできません。IP アドレスを含める必要があります。

特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。複数の NAT ルールを設定する場合は、**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** などのように、同じ IP アドレスを指定する複数のオブジェクトを作成する必要があります。

マッピングアドレスのガイドライン

マッピング IP アドレス プールに、次のアドレスを含めることはできません。

- マッピング インターフェイスの IP アドレス。ルールに **any** インターフェイスを指定した場合は、すべてのインターフェイス IP アドレスが無効になります。インターフェイス PAT（ルーテッドモードのみ）の場合は、IP アドレスの代わりに **interface** キーワードを使用します。
- （トランスペアレント モード）管理 IP アドレス。
- （ダイナミック NAT）VPN がイネーブルの場合は、スタンバイ インターフェイスの IP アドレス。
- 既存の VPN プールのアドレス。

変換セッションのクリア

NAT コンフィギュレーションを変更する場合、既存の変換がタイムアウトするまで待たずに新しい NAT 情報を使用するために、clear xlate コマンドを使用して変換テーブルをクリアできます。ただし、変換テーブルをクリアすると、現在の接続がすべて切断されます。

PAT プールのガイドライン

- 個々の A レコードに複数の PAT ルールを適用できることで、使用する PAT ルールが不明確になるため、DNS リライトは PAT には適用されません。
- （9.15 より前）使用可能な場合、実際の送信元ポート番号がマッピングポートに対して使用されます。ただし、実際のポートが使用できない場合は、デフォルトで、マッピングポートは実際のポート番号と同じポート範囲（0 ～ 511、512 ～ 1023、および 1024 ～ 65535）から選択されます。そのため、1024 よりも下のポートでは、小さい PAT プールのみを使用できます。（8.4(3) 以降、ただし 8.5(1) と 8.6(1) を除く）下位ポート範囲を使用するトラフィックが多数ある場合は、サイズが異なる 3 つの層の代わりにフラットなポート範囲を使用するように指定できます（1024 ～ 65535、または 1 ～ 65535）。

- （9.15 以降）ポートは、1024 ー 65535 の範囲の使用可能なポートにマッピングされます。必要に応じ、1024 番未満の予約ポートを含めて、ポート範囲全体を変換に使用することもできます。

クラスタで動作する場合、アドレスごとに 512 個のポートのブロックがクラスタのメンバーに割り当てられ、これらのポートブロック内でマッピングが行われます。ブロック割り当ても有効にした場合は、ブロック割り当てサイズに従ってポートが分配されます。このデフォルトも 512 です。

- PAT プールに対してブロック割り当てを有効にする場合、ポートブロックは 1024 ～ 65535 の範囲でのみ割り当てられます。そのため、アプリケーションが小さいポート番号（1 ～ 1023）を必要とするときは、機能しない可能性があります。たとえば、ポート 22（SSH）を要求するアプリケーションは、1024 ～ 65535 の範囲内で、ホストに割り当てられたブロック内の、マッピングされたポートを取得します。

ダイナミック NAT によってマッピングされた IP アドレスにオブジェクト グループを使用し、そのグループにホスト アドレスを含める場合、PAT プールをイネーブルにすると、ホスト アドレスの使用が PAT フォールバックからダイナミック NAT へと変更されます。

- （8.4(3) 以降、8.5(1) または 8.6(1) を除く）2 つの個別のルールで同じ PAT プール オブジェクトを使用する場合は、各ルールに対して同じオプションを指定します。たとえば、1 つのルールで拡張 PAT およびフラットな範囲が指定される場合は、もう一方のルールでも拡張 PAT およびフラットな範囲が指定される必要があります。

PAT プールの拡張 PAT のガイドライン

- 多くのアプリケーション インスペクションでは、拡張 PAT はサポートされていません。サポート対象外のインスペクションのリストについては、設定ガイドを参照してください。
- ダイナミック PAT ルールに対して拡張 PAT をイネーブルにする場合は、PAT プール内のアドレスを、ポート変換ルールを設定した別のスタティック NAT の PAT アドレスとしても使用することはできません。たとえば、PAT プールに 10.1.1.1 が含まれている場合、PAT アドレスとして 10.1.1.1 を使用する、ポート トランスレーション ルールを持つスタティック NAT は作成できません。
- PAT プールを使用し、フォールバックのインターフェイスを指定する場合、拡張 PAT を使用できません。
- ICE または TURN を使用する VoIP 配置では、拡張 PAT を使用しないでください。ICE および TURN は、すべての宛先に対して同じであるために PAT バインディングに依存しています。

PAT プールのラウンドロビンのガイドライン

- （8.4(3) 以降、8.5(1) または 8.6(1) を除く）ホストに既存の接続がある場合、そのホストからの後続の接続では、ポートが使用可能であれば同じ PAT IP アドレスが使用されます。**Note**：この「粘着性」は、フェールオーバーが発生すると失われます。ASA がフェール

オーバーすると、ホストからの後続の接続で最初の IP アドレスが使用されない場合があります。

- （8.4(2)、8.5(1)、および 8.6(1)）ホストに既存の接続がある場合、そのホストからの後続の接続では、ラウンドロビン割り当てのため、接続ごとに別の PAT アドレスが使用される可能性があります。この場合、ホストについて情報を交換する 2 つの Web サイト（e-コマースサイトと支払サイトなど）にアクセスするときに問題が発生する可能性があります。これらのサイトが、1 つのホストとして扱うべきものを 2 つの異なる IP アドレスと見なした場合、トランザクションは失敗することがあります。
- ラウンドロビンでは、特に拡張 PAT と組み合わせた場合に、大量のメモリが消費されます。

NAT と IPv6

NAT を使用すると、IPv6 ネットワーク間、さらに IPv4 および IPv6 ネットワークの間で変換できます（ルーテッド モードのみ）。次のベスト プラクティスを推奨します。インターフェイスが同じブリッジ グループのメンバーの場合は NAT64/46 を実行できないことに注意してください。

- NAT66（IPv6-to-IPv6）：スタティック NAT を使用することを推奨します。ダイナミック NAT または PAT を使用できますが、IPv6 アドレスは大量にあるため、ダイナミック NAT を使用する必要がありません。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（Twice NAT のみ）。
- NAT46（IPv4-to-IPv6）：スタティック NAT を使用することを推奨します。IPv6 アドレス空間は IPv4 アドレス空間よりもかなり大きいので、容易にスタティック変換に対応できます。リターン トラフィックを許可しない場合は、スタティック NAT ルールを単一方向にできます（Twice NAT のみ）。IPv6 サブネットに変換する場合（/96 以下）、結果のマッピング アドレスは IPv4 埋め込み IPv6 アドレスとなります。このアドレスでは、IPv4 アドレスの 32 ビットが IPv6 プレフィックスの後に埋め込まれています。たとえば、IPv6 プレフィックスが /96 プレフィックスの場合、IPv4 アドレスは、アドレスの最後の 32 ビットに追加されます。たとえば、201b::0/96 に 192.168.1.0/24 をマッピングする場合、192.168.1.4 は 201b::0.192.168.1.4 にマッピングされます（混合表記で表示）。/64 など、より小さいプレフィックスの場合、IPv4 アドレスがプレフィックスの後に追加され、サフィックスの 0s が IPv4 アドレスの後に追加されます。
- NAT64（IPv6-to-IPv4）：IPv6 アドレスの数に対応できる十分な数の IPv4 アドレスがない場合があります。大量の IPv4 変換を提供するためにダイナミック PAT プールを使用することを推奨します。

例

ダイナミック NAT の例

次の例では、外部アドレス 2.2.2.1 ～ 2.2.2.10 の範囲の背後に 192.168.2.0 ネットワークを隠すダイナミック NAT を設定します。

```
ciscoasa(config)# object network my-range-obj
```

```
ciscoasa(config-network-object)# range 2.2.2.1 2.2.2.10
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic my-range-obj
```

次の例では、ダイナミック PAT バックアップを設定したダイナミック NAT を設定します。ネットワーク 10.76.11.0 内のホストは、まず nat-range1 プール（10.10.10.10 ～ 10.10.10.20）にマッピングされます。nat-range1 プール内のすべてのアドレスが割り当てられたら、pat-ip1 アドレス（10.10.10.21）を使用してダイナミック PAT が実行されます。PAT 変換もすべて使用されることはほとんどありませんが、このような場合には、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
ciscoasa(config)# object network nat-range1
ciscoasa(config-network-object)# range 10.10.10.10 10.10.10.20
ciscoasa(config-network-object)# object network pat-ip1
ciscoasa(config-network-object)# host 10.10.10.21
ciscoasa(config-network-object)# object-group network nat-pat-grp
ciscoasa(config-network-object)# network-object object nat-range1
ciscoasa(config-network-object)# network-object object pat-ip1
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 10.76.11.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic nat-pat-grp interface
```

次の例では、ダイナミック NAT とダイナミック PAT バックアップを使用して IPv6 ホストを IPv4 に変換するように設定します。内部ネットワーク 2001:DB8::/96 上のホストは最初に、IPv4_NAT_RANGE プール（209.165.201.30 ～ 209.165.201.1）にマッピングされます。IPv4_NAT_RANGE プール内のすべてのアドレスが割り当てられた後は、IPv4_PAT アドレス（209.165.201.31）を使用してダイナミック PAT が実行されます。PAT 変換もすべて使用されてしまった場合は、外部インターフェイス アドレスを使用してダイナミック PAT が実行されます。

```
ciscoasa(config)# object network IPv4_NAT_RANGE
ciscoasa(config-network-object)# range 209.165.201.1 209.165.201.30
ciscoasa(config-network-object)# object network IPv4_PAT
ciscoasa(config-network-object)# host 209.165.201.31
ciscoasa(config-network-object)# object-group network IPv4_GROUP
ciscoasa(config-network-object)# network-object object IPv4_NAT_RANGE
ciscoasa(config-network-object)# network-object object IPv4_PAT
ciscoasa(config-network-object)# object network my_net_obj5
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic IPv4_GROUP interface
```

ダイナミック PAT の例

次の例では、アドレス 2.2.2.2 の背後に 192.168.2.0 ネットワークを隠すダイナミック PAT を設定します。

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic 2.2.2.2
```

次の例では、外部インターフェイスアドレスの背後に 192.168.2.0 ネットワークを隠蔽するダイナミック PAT を設定します。

```
ciscoasa(config)# object network my-inside-net
ciscoasa(config-network-object)# subnet 192.168.2.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) dynamic interface
```

次の例では、ダイナミック PAT と PAT プールを使用して内部 IPv6 ネットワークを外部 IPv4 ネットワークに変換するように設定します。

```
ciscoasa(config)# object network IPv4_POOL
ciscoasa(config-network-object)# range 203.0.113.1 203.0.113.254
ciscoasa(config)# object network IPv6_INSIDE
ciscoasa(config-network-object)# subnet 2001:DB8::/96
ciscoasa(config-network-object)# nat (inside,outside) dynamic pat-pool IPv4_POOL
```

スタティック NAT の例

次の例では、内部にある実際のホスト 1.1.1.1 の、DNS リライトがイネーブルに設定された外部にある 2.2.2.2 へのスタティック NAT を設定します。

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 2.2.2.2 dns
```

次の例では、内部にある実際のホスト 1.1.1.1 の、マッピングされたオブジェクトを使用する外部にある 2.2.2.2 へのスタティック NAT を設定します。

```
ciscoasa(config)# object network my-mapped-obj
ciscoasa(config-network-object)# host 2.2.2.2
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-mapped-obj
```

次の例では、1.1.1.1 の TCP ポート 21 の、外部インターフェイスのポート 2121 への、ポート変換を使用するスタティック NAT を設定します。

```
ciscoasa(config)# object network my-ftp-server
ciscoasa(config-network-object)# host 1.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static interface service tcp 21
2121
```

次の例では、内部 IPv4 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
ciscoasa(config)# object network inside_v4_v6
ciscoasa(config-network-object)# subnet 10.1.1.0 255.255.255.0
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8::/96
```

次の例では、内部 IPv6 ネットワークを外部 IPv6 ネットワークにマッピングします。

```
ciscoasa(config)# object network inside_v6
ciscoasa(config-network-object)# subnet 2001:DB8:AAAA::/96
ciscoasa(config-network-object)# nat (inside,outside) static 2001:DB8:BBBB::/96
```

アイデンティティ NAT の例

次の例では、インラインのマッピングアドレスを使用して、ホストアドレスを自身にマッピングします。

```
ciscoasa(config)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static 10.1.1.1
```

次の例では、ネットワークオブジェクトを使用して、ホストアドレスを自身にマッピングします。

```
ciscoasa(config)# object network my-host-obj1-identity
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# object network my-host-obj1
ciscoasa(config-network-object)# host 10.1.1.1
ciscoasa(config-network-object)# nat (inside,outside) static my-host-obj1-identity
```

関連コマンド

コマンド	説明
clear configure nat	NAT コンフィギュレーション（Twice NAT とネットワーク オブジェクト NAT の両方）を削除します。
show nat	NAT ポリシーの統計情報を表示します。
show nat pool	NAT プールに関する情報を表示します。
show running-config nat	NAT コンフィギュレーションを表示します。
show xlate	xlate 情報を表示します。
xlate block-allocation	PAT ポート ブロック割り当ての特性を設定します。

nat（VPN ロード バランシング）

NAT で変換されるこのデバイスの IP アドレスの変換先 IP アドレスを設定するには、VPN ロード バランシング コンフィギュレーション モードで **nat** コマンドを使用します。この NAT 変換を無効にするには、このコマンドの **no** 形式を使用します。

nat *ip-address*
no nat [*ip-adddress*]

構文の説明

ip-address この NAT でこのデバイスの IP アドレスの変換先となる IP アドレス。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
VPN ロードバランシング コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシングモードを開始する必要があります。

このコマンドの **no nat** 形式で任意の *ip-address* 値を指定する場合、IP アドレスは実行コンフィギュレーションの既存の NAT IP アドレスに一致する必要があります。

例

次に、**nat** コマンドを含む VPN ロード バランシング コマンド シーケンスの例を示します。この例では、NAT で変換するアドレスを 192.168.10.10 に設定しています。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
```

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster port 9023
ciscoasa(config-load-balancing)# participate
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードを開始します。

nat-assigned-to-public-ip

VPN ピアのローカル IP アドレスを変換してピアの実際の IP アドレスに自動的に戻すには、トンネルグループ一般属性コンフィギュレーション モードで **nat-assigned-to-public-ip** コマンドを使用します。NAT ルールを無効にするには、このコマンドの **no** 形式を使用します。

nat-assigned-to-public-ip *interface*
no nat-assigned-to-public-ip *interface*

構文の説明

interface NAT を適用するインターフェイスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(3)	このコマンドが追加されました。

使用上のガイドライン

まれに、内部ネットワークで、割り当てられたローカル IP アドレスではなく、VPN ピアの実際の IP アドレスを使用する場合があります。VPN では通常、内部ネットワークにアクセスするために、割り当てられたローカル IP アドレスがピアに指定されます。ただし、内部サーバーおよびネットワーク セキュリティがピアの実際の IP アドレスに基づく場合などに、ローカル IP アドレスを変換してピアの実際のパブリック IP アドレスに戻す場合があります。

この機能は、トンネル グループごとに 1 つのインターフェイスでイネーブルにすることができます。VPN セッションが確立または切断されると、オブジェクト NAT ルールが動的に追加および削除されます。ルールは **show nat** コマンドを使用して表示できます。

データフロー

次に、この機能を有効にした場合に ASA を通過するパケットフローの手順を示します。

1. VPN ピアから ASA にパケットが送信されます。

外部用の送信元/宛先は、ピアのパブリック IP アドレスまたは ASA の IP アドレスで構成されます。暗号化された内部用の送信元/宛先は、VPN で割り当てられた IP アドレス/内部サーバーのアドレスで構成されます。

2. ASA でパケットが復号されます（外部用の送信元/宛先が削除されます）。

3. ASA で内部サーバーのルートルックアップが実行され、内部インターフェイスにパケットが送信されます。

4. 自動的に作成される VPN NAT ポリシーに基づいて、VPN で割り当てられた送信元 IP アドレスがピアのパブリック IP アドレスに変換されます。

5. 変換されたパケットが ASA からサーバーに送信されます。

6. パケットに対するサーバーからの応答がピアのパブリック IP アドレスに送信されます。

7. 応答を受け取ると、ASA により、宛先 IP アドレスが VPN で割り当てられた IP アドレスに戻されます。

8. 変換が解除されたパケットが ASA から暗号化が行われた外部インターフェイスに転送され、ASA の IP アドレスまたはピアのパブリック IP アドレスで構成される外部用の送信元/宛先が追加されます。

9. ASA からピアにパケットが返送されます。

10. ピアでデータが復号化されて処理されます。

制限事項

ルーティングの問題のため、この機能が必要でない場合は、この機能の使用は推奨しません。ご使用のネットワークとの機能の互換性を確認するには、Cisco TAC にお問い合わせください。次の制限事項を確認してください。

- Cisco IPsec および セキュアクライアント のみがサポートされます。
- NAT ポリシーおよび VPN ポリシーが適用されるように、パブリック IP アドレスへのリターン トラフィックは ASA にルーティングされる必要があります。
- リバース ルート インジェクション（**set reverse-route** コマンドを参照）を有効にすると、VPN で割り当てられた IP アドレスだけがアドバタイズされます。
- ロードバランシングはサポートされません（ルーティングの問題のため）。
- ローミング（パブリック IP 変更）はサポートされません。

例

次に、「vpnclient」トンネル グループに対してパブリック IP への NAT をイネーブルにする例を示します。

```
ciscoasa# ip local pool client 10.1.226.4-10.1.226.254
ciscoasa# tunnel-group vpnclient type remote-access
ciscoasa# tunnel-group vpnclient general-attributes
ciscoasa(config-tunnel-general)# address-pool client
ciscoasa(config-tunnel-general)# nat-assigned-to-public-ip inside
```

次に、IP 10.1.226.174 が割り当てられたピア 209.165.201.10 の自動 NAT ルールを表示する **show nat detail** コマンドの出力例を示します。

```
ciscoasa# show nat detail
 Auto NAT Policies (Section 2)
 1 (outside) to (inside) source static _vpn_nat_10.1.226.174 209.165.201.10
     translate_hits = 0, untranslate_hits = 0
     Source - Origin: 10.1.226.174/32, Translated: 209.165.201.10/32
```

関連コマンド

コマンド	説明
show nat	現在の xlate を表示します。
tunnel-group general-attributes	トンネル グループの一般属性を設定します。
debug menu webvpn 99	AnyConnect SSL セッションで、VPN NAT インターフェイスがセッションに保存されます。
debug menu ike 2 *peer_ip*	Cisco IPsec クライアント セッションで、VPN NAT インターフェイスが SA に保存されます。
debug nat 3	NAT のデバッグ メッセージを表示します。

nat-rewrite

DNS 応答の A レコードに組み込まれている IP アドレスの NAT リライトを有効にするには、パラメータ コンフィギュレーション モードで **nat-rewrite** 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。

nat-rewrite
no nat-rewrite

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。

コマンド デフォルト

NAT リライトは、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** コマンドを定義していない場合でも、**inspect dns** コマンドを設定していれば有効にできます。無効にするには、ポリシー マップ コンフィギュレーションで **no nat-rewrite** コマンドを明示的に指定する必要があります。**inspect dns** が設定されていない場合、NAT リライトは実行されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

この機能は、DNS 応答の A タイプのリソース レコード（RR）の NAT 変換を実行します。

例

次に、DNS インスペクション ポリシー マップで NAT リライトをイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# nat-rewrite
```

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。

nbns-server

NBNS サーバーを設定するには、トンネルグループ webvpn 属性コンフィギュレーション モードで **nbns-server** コマンドを使用します。構成から NBNS サーバーを削除するには、このコマンドの **no** 形式を使用します。

ASA は、NetBIOS 名を IP アドレスにマップするために NBNS サーバーをクエリします。WebVPN では、リモート システム上のファイルへのアクセスまたはファイルの共有に NetBIOS が必要です。

nbns-server { *ipaddr* | *hostname* } [**master**] [**timeout** *timeout*] [**retry** *retries*]
no nbns-server

構文の説明

hostname	NBNS サーバーのホスト名を指定します。
ipaddr	NBNS サーバーの IP アドレスを指定します。
master	これは WINS サーバーではなく、マスター ブラウザであることを示します。
retry	再試行値が後に続くことを示します。
retries	NBNS サーバーへのクエリーを再試行する回数を指定します。ASA は、エラーメッセージを送信するまでに、ここに指定する回数、サーバーのリストを繰り返し使用します。デフォルト値は 2 で、指定できる範囲は 1 ～ 10 です。
timeout	タイムアウト値が後に続くことを示します。
timeout	NBNS サーバーが 1 つだけ存在する場合は同じサーバーに、複数存在する場合は別のサーバーに、ASA がクエリを再送信するまでに待機する時間を指定します。デフォルトのタイムアウトは 2 秒で、指定できる範囲は 1 ～ 30 秒です。

コマンド デフォルト

NBNS サーバーは、デフォルトでは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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ webvpn 属性コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	webvpn モードからトンネル グループ webvpn コンフィギュレーション モードに移行しました。

使用上のガイドライン

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

サーバー エントリは最大 3 つです。冗長性のために、設定する最初のサーバーはプライマリ サーバーで、その他のサーバーはバックアップです。

no オプションを使用して、構成から一致するエントリを削除します。

例

次に、NBNS サーバーでトンネル グループ「test」を設定する例を示します。NBNS サーバーはマスターブラウザであり、IP アドレスを 10.10.10.19、タイムアウト値を 10 秒、および再試行回数を 8 としています。また、IP アドレス 10.10.10.24、タイムアウト値 15 秒、再試行回数 8 回の NBNS WINS サーバーを設定する例も示します。

```
ciscoasa
(config)#
 tunnel-group test type webvpn
ciscoasa
(config)#
 tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.19 master timeout 10 retry 8
ciscoasa(config-tunnel-webvpn)# nbns-server 10.10.10.24 timeout 15 retry 8
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
clear configure group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーのコンフィギュレーションを削除します。
show running-config group-policy	特定のグループ ポリシーまたはすべてのグループ ポリシーの実行コンフィギュレーションを表示します。
tunnel-group webvpn-attributes	指定したトンネル グループの WebVPN 属性を指定します。

neighbor（ルータ EIGRP）

ルーティング情報を交換する EIGRP ネイバールータを定義するには、ルータ EIGRP コンフィギュレーションモードで**neighbor** コマンドを使用します。ネイバーエントリを削除するには、このコマンドの **no** 形式を使用します。

neighbor *ip_address* **interface** *name*
no neighbor *ip_address* **interface** *name*

構文の説明

interface *name*	**nameif** コマンドで指定されたインターフェイス名。ネイバーにはこのインターフェイス経由で到達できます。
ip_address	ルーティング情報を交換するネイバールータの IPv4 アドレス。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ EIGRP コンフィギュレーション	—	•	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

複数のネイバー ステートメントを使用して、特定の EIGRP ネイバーでピアリング セッションを確立できます。EIGRP がルーティング更新を交換するインターフェイスは、ネイバー ステートメントで指定する必要があります。2 つの EIGRP ネイバーがルーティング更新を交換するインターフェイスは、同じネットワークにある IP アドレスで設定する必要があります。

（注） インターフェイスに対して **passive-interface** コマンドを設定すると、そのインターフェイスではすべての発着信ルーティング アップ デートメッセージと hello メッセージが抑制されます EIGRP ネイバーとの隣接関係は、パッシブとして設定されるインターフェイス経由で確立および維持できません。

EIGRP hello メッセージは、 **neighbor** コマンドを使用して定義されたネイバーにユニキャスト メッセージとして送信されます。

例

次に、ネイバーを 192.168.1.1 および 192.168.2.2 として EIGRP ピアリング セッション を設定する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 192.168.0.0
ciscoasa(config-router)# neighbor 192.168.1.1 interface outside
ciscoasa(config-router)# neighbor 192.168.2.2 interface branch_office
```

関連コマンド

コマンド	説明
debug eigrp neighbors	EIGRP ネイバー メッセージに関するデバッグ情報を表示します。
show eigrp neighbors	EIGRP ネイバー テーブルを表示します。

neighbor（ルータ OSPF）

ポイントツーポイントの非ブロードキャストネットワークにスタティックネイバーを定義するには、ルータ OSPF コンフィギュレーション モードで **neighbor** コマンドを使用します。コンフィギュレーションからスタティックに定義されたネイバーを削除するには、このコマンドの **no** 形式を使用します。

neighbor *ip_address* [**interface** *name*]
no neighbor *ip_address* [**interface** *name*]

構文の説明

interface *name*	（任意）**nameif** コマンドで指定されたインターフェイス名を指定します。ネイバーにはこのインターフェイス経由で到達できます。
ip_address	ネイバー ルータの IP アドレスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ OSPF コンフィギュレーション	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

neighbor コマンドは、VPN トンネル経由で OSPF ルートをアドバタイズするために使用されます。既知の非ブロードキャスト ネットワーク ネイバーごとにネイバー エントリを 1 つ含める必要があります。ネイバー アドレスは、インターフェイスのプライマリ アドレスに存在する必要があります。

ネイバーがシステムに直接接続されたいずれかのインターフェイスと同じネットワークにない場合は、**interface** オプションを指定する必要があります。また、ネイバーに到達するには、スタティック ルートを作成する必要があります。

例

次に、アドレス 192.168.1.1 でネイバー ルータを定義する例を示します。

```
ciscoasa(config-router)# neighbor 192.168.1.1
```

関連コマンド

コマンド	説明
router ospf	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。

neighbor activate

ボーダー ゲートウェイ プロトコル（BGP）ネイバーとの情報交換をイネーブルにするには、アドレス ファミリ コンフィギュレーション モードで neighbor activate コマンドを使用します。BGP ネイバーとのアドレス交換を無効にするには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **activate**
no neighbor { *ip_address* | *ipv6-address* } **activate**

構文の説明

ip_address	BGP ルータの IP アドレス。
ipv6-address	BGP ルータの IPv6 アドレス。

コマンド デフォルト

BGP ネイバーとのアドレス交換は、IPv4 アドレス ファミリについてデフォルトでイネーブルになります。それ以外のアドレス ファミリについてアドレス交換をイネーブルにすることはできません。

（注） IPv4 アドレス ファミリのアドレス交換は、neighbor remote-as コマンドで定義された各 BGP ルーティング セッションに対してデフォルトで有効になります。ただし、neighbor remote-as コマンドの設定前に no bgp default ipv4-activate コマンドを設定した場合や、no neighbor activate コマンドを使用して特定のネイバーとのアドレス交換を無効にした場合は除きます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用すると、アドレス情報を IP プレフィックスの形式でアドバタイズできます。BGP では、このアドレス プレフィックス情報をネットワーク層到達可能性情報（NLRI）と呼びます。

例

次に、BGP ネイバー 172.16.1.1 について、IPv4 アドレス ファミリ ユニキャストのアドレス交換をイネーブルにする例を示します。

```
ciscoasa(config)# router bgp 50000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 4
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

次に、group2 という名前の BGP ピア グループのすべてのネイバーと BGP ネイバー 7000::2 について、IPv6 アドレス ファミリのアドレス交換をイネーブルにする例を示します。

```
Router(config)# address-family ipv6
Router(config-router-af)# neighbor group2 activate
Router(config-router-af)# neighbor 7000::2 activate
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。

neighbor advertise-map

設定されたルート マップに一致する BGP テーブル内のルートをアドバタイズするには、ルータ コンフィギュレーション モードで neighbor advertise-map コマンドを使用します。ルート アドバタイズメント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。

neighbor { *ip_address* | *ipv6-address* } **advertise-map** *map-name* { **exist-map** *map-name* | **non-exist-map** *map-name* } [**check-all-paths**]
no neighbor { *ip_address* | *ipv6-address* } **advertise-map** *map-name* { **exist-map** *map-name* | **non-exist-map** *map-name* } [**check-all-paths**]

構文の説明

ipv4_address	条件付きアドバタイズメントを受け取るルータの IPv4 アドレスを指定します。
ipv6_address	条件付きアドバタイズメントを受け取るルータの IPv6 アドレスを指定します。
advertise-map map-name	存在マップまたは非存在マップの条件を満たす場合にアドバタイズするルート マップの名前を指定します。
exist-map map-name	アドバタイズ マップのルートをアドバタイズするかどうかを決定するために BGP テーブル内のルートと比較する存在マップの名前を指定します。
non-exist-map map-name	アドバタイズ マップのルートをアドバタイズするかどうかを決定するために BGP テーブル内のルートと比較する非存在マップの名前を指定します。
check-all-paths	（オプション）BGPテーブル内のプレフィックスを使用した存在マップによるすべてのパスのチェックをイネーブルにします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

neighbor advertise-map コマンドは、選択されたルートを条件付きでアドバタイズするために使用します。条件付きでアドバタイズされるルート（プレフィックス）は、アドバタイズマップと存在マップまたは非存在マップの 2 つのルート マップで定義されます。

存在マップまたは不在マップと関連付けられているルート マップは、BGP スピーカーが追跡するプレフィックスを指定します。

アドバタイズ マップと関連付けられているルート マップは、条件が満たされたときに、指定されたネイバーにアドバタイズされるプレフィックスを指定します。

存在マップが設定されている場合、プレフィックスがアドバタイズマップと存在マップの両方に存在するときに条件が満たされます。

非存在マップが設定されている場合、プレフィックスがアドバタイズマップには存在するが、不在マップには存在しないときに条件が満たされます。

条件が満たされない場合、ルートは取り消され、条件付きアドバタイズメントは行われません。条件付きアドバタイズメントを行うには、ダイナミックにアドバタイズされるルート、またはアドバタイズされないルートがすべて BGP ルーティング テーブルに存在する必要があります。

例

次のルート コンフィギュレーションの例では、すべてのパスをチェックするように BGP を設定しています。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.2.1.1 advertise-map MAP1 exist-map MAP2
ciscoasa(config-router-af)# neighbor 172.16.1.1 activate
```

次のアドレス ファミリ コンフィギュレーションの例では、非存在マップを使用して、10.1.1.1 ネイバーに条件付きでプレフィックスをアドバタイズするように BGP を設定しています。プレフィックスが MAP3 にあり、MAP4 にない場合に条件を満たし、プレフィックスがアドバタイズされます。

```
ciscoasa(config)# router bgp 5000
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.1.1.1 advertise-map MAP3 non-exist-map MAP4
```

次のピア グループ コンフィギュレーションの例では、BGP ネイバーのすべてのパスをプレフィックスと照合してチェックするように BGP を設定しています。

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# redistribute static
ciscoasa(config-router-af)# neighbor route1 send-community both
ciscoasa(config-router-af)# neighbor route1 advertise-map MAP1 exist-map MAP2
check-all-paths
```

関連コマンド

コマンド	説明
address-family ipv4	アドレス ファミリ コンフィギュレーション モードを開始します。

neighbor advertisement-interval

BGP ルーティング アップデートを送信する最小ルート アドバタイズメント インターバル（MRAI）を設定するには、アドレス ファミリ コンフィギュレーション モードで neighbor advertisement-interval 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。

neighbor { *ip_address* | *ipv6-address* } **advertisement-interval** *seconds*
no neighbor { *ip_address* | *ipv6-address* } **advertisement-interval** *seconds*

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
seconds	BGP ルーティング アップデートの最小送信間隔。 有効な値は、0 ～ 600 です。

コマンド デフォルト

VRF 以外の eBGP セッション：30 秒

VRF の eBGP セッション：0 秒

iBGP セッション：0 秒

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

MRAI が 0 秒の場合は、BGP ルーティング テーブルが変更された時点ですぐに BGP ルーティング アップデートが送信されます。

例

次に、BGP ルーティング アップデートの最小送信間隔を 10 秒に設定する例を示します。

```
ciscoasa(config-router-af)# neighbor 172.16.1.1 advertisement-interval 10
```

次に、BGPv6 ルーティング アップデートの最小送信間隔を 100 秒に設定する例を示します。

```
asa(config-router-af)# neighbor 2001::1 advertisement-interval 100
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor default-originate

BGP スピーカー（ローカルルータ）にネイバーへのデフォルトルート 0.0.0.0 の送信を許可して、そのルートがデフォルトルートとして使用されるようにするには、アドレス ファミリ コンフィギュレーション モードで neighbor default-originate コマンドを使用します。デフォルトルートを送信しないようにするには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **default-originate** [**route-map** *route-map name*]
no neighbor { *ip_address* | *ipv6-address* } **default-originate** [**route-map** *route-map name*]

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
route-map route-map name	（オプション）ルートマップの名前。ルートマップでは、条件に応じてルート 0.0.0.0 を挿入できます。

コマンド デフォルト

ネイバーにデフォルト ルートは送信されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用すると、ローカル ルータの 0.0.0.0 が不要になります。match ip address 句を含むルート マップとともに使用することで、IP アクセス リストと完全に一致するルートがある場合にデフォルト ルート 0.0.0.0 が挿入されるようにすることができます。ルート マップには他の match 句も含めることができます。

neighbor default-originate コマンドでは、標準アクセス リストまたは拡張アクセス リストを使用できます。

例

次に、ネイバー 72.16.2.3 にルート 0.0.0.0 を無条件で挿入するようにローカル ルータを設定する例を示します。

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 default-originate
In the following example, the local router injects route 0.0.0.0 to the neighbor 2001::1:
asa(config-router-af)#neighbor 2001::1 default-originate route-map default-map
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor description

説明をネイバーに関連付けるには、アドレス ファミリ コンフィギュレーション モードで neighbor description コマンドを使用します。説明を削除するには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **description** *text*
no neighbor { *ip_address* | *ipv6-address* } **description** *text*

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
text	ネイバーを説明するテキスト（最大 80 文字）。

コマンド デフォルト

ネイバーの説明はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

例

次に、ネイバーに「peer with example.com」という説明を設定する例を示します。

```
ciscoasa(config-router-af)# neighbor 172.16.2.3 description peer with example.com
```

次に、IPv6 ネイバーに「peer with example.com」という説明を設定する例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 description peer with example.com
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor disable-connected-check

ループバック インターフェイスを使用するシングル ホップ ピアとの eBGP ピアリング セッションを確立するために接続の検証をディセーブルにするには、アドレス ファミリ コンフィギュレーション モードで neighbor disable-connected-check コマンドを使用します。eBGP ピアリング セッションについての接続の検証をイネーブルにするには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **disable-connected-check**
no neighbor { *ip_address* | *ipv6-address* } **disable-connected-check**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。

コマンド デフォルト

デフォルトでは、シングル ホップ eBGP ピアリング セッション（TTL=254）について、BGP ルーティング プロセスで接続が検証され、eBGP ピアが同じネットワーク セグメントに直接接続されているかどうか確認されます。ピアが同じネットワーク セグメントに直接接続されていない場合、ピアリング セッションは確立されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

neighbor disable-connected-check コマンドは、シングルホップで到達可能だが、ループバック インターフェイス上に設定されている、あるいじは直接接続されない IP アドレスで設定されている eBGP ピアリングセッションの接続検証プロセスを無効にする場合に使用します。

このコマンドが必要になるのは、neighbor ebgp-multihop コマンドで TTL 値を 1 に設定している場合だけです。シングル ホップ eBGP ピアのアドレスに到達できる必要があります。neighbor update-source コマンドを使用して、BGP ルーティング プロセスでピアリング セッションにループバック インターフェイスを使用できるように設定する必要があります。

例

次に、2 つの BGP ピア間でシングル ホップ eBGP ピアリング セッションを設定する例を示します。この 2 つのピアは各ルータ上のローカル ループバック インターフェイスを経由して同じネットワーク セグメント上で到達可能になっています。

BGP ピア 1

```
ciscoasa(config)# interface loopback1
ciscoasa(config-if)# ip address 10.0.0.100 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 64512
ciscoasa(config-router)# neighbor 192.168.0.200 remote-as 65534
ciscoasa(config-router)# neighbor 192.168.0.200 ebgp-multihop 1
ciscoasa(config-router)# neighbor 192.168.0.200 update-source loopback2
ciscoasa(config-router)# neighbor 192.168.0.200 disable-connected-check
BGP Peer 2
ciscoasa(config)# interface loopback2
ciscoasa(config-if)# ip address 192.168.0.200 255.255.255
ciscoasa(config-if)# exit
ciscoasa(config)# router bgp 65534
ciscoasa(config-router)# neighbor 10.0.0.100 remote-as 64512
ciscoasa(config-router)# neighbor 10.0.0.100 ebgp-multihop 1
ciscoasa(config-router)# neighbor 10.0.0.100 update-source loopback1
ciscoasa(config-router)# neighbor 10.0.0.100 disable-connected-check
BGPv6 Peer
ciscoasa(config-router)# neighbor 2001::1 disable-connected-check
```

関連コマンド

コマンド	説明
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
neighbor ebgp-multihop	直接接続されていないネットワークに存在する外部ピアへの BGP 接続を受け入れるか、または開始します。

neighbor distribute-list

アクセス リストで指定された BGP ネイバー情報を配布するには、アドレス ファミリ コンフィギュレーション モードで neighbor distribute-list コマンドを使用します。エントリを削除するには、このコマンドの no 形式を使用します。

neighbor *ip_address* **distribute-list** { **access-list-name** } { **in** | **out** }
no neighbor *ip_address* **distribute-list** { **access-list-name** } { **in** | **out** }

構文の説明

ip_address	ネイバー ルータの IP アドレス。
access-list-name	標準アクセス リスト名。
in	指定したネイバーからの着信アドバタイズメントにアクセス リストを適用します。
out	指定したネイバーへの発信アドバタイズメントにアクセス リストを適用します。

コマンド デフォルト

BGP ネイバーは指定されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

配布リストは、アドバタイズメントをフィルタリングする方法の1つです。アドバタイズメントをフィルタリングする方法には、ほかにも次のような方法があります。

- ip as-path access-list コマンドおよび neighbor filter-list コマンドで自律システムパスフィルタを設定できます。

- access-list（IP 標準）コマンドでアドバタイズメントのフィルタリングに使用する標準アクセスリストを設定できます。
- route-map（IP）コマンドでアドバタイズメントをフィルタリングできます。ルートマップは、自律システム フィルタ、プレフィックス フィルタ、アクセス リスト、配布リストで設定できます。

標準アクセスリストはルーティングアップデートのフィルタリングに使用できます。ただし、クラスレス ドメイン間ルーティング（CIDR）を使用している場合、標準アクセス リストによるルート フィルタリングでは、ネットワーク アドレスやマスクの高度なフィルタリングに必要な細かい設定は行えません。

例

次に、標準アクセス リスト distribute-list-acl の BGP ネイバー情報をネイバー 172.16.4.1 の着信アドバタイズメントに適用する例を示します。

```
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af) neighbor 172.16.4.1 distribute-list distribute-list-acl in
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
network	BGP でアドバタイズするネットワークを指定します。
access-list permit	転送するパケットを指定します。
access-list deny	拒否するパケットを指定します。

neighbor ebgp-multihop

直接接続されていないネットワークに存在する外部ピアへの BGP 接続を受け入れて試行するには、アドレス ファミリ コンフィギュレーション モードで neighbor ebgp-multihop コマンドを使用します。デフォルトに戻るには、no 形式のコマンドを使用します。

neighbor { *ip_address* | *ipv6-address* } **ebgp-multihop** [**ttl**]
no neighbor { *ip_address* | *ipv6-address* } **ebgp-multihop**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
ttl	（オプション）存続可能時間。 有効な値の範囲は 1 ～ 255 ホップです。

コマンド デフォルト

直接接続されたネイバーだけが許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

この機能は、シスコ テクニカル サポート担当者の指示のもとでのみ使用してください。ルートが一定でないことによるループの発生を回避するために、マルチホップピアのルートがデフォルトルート（0.0.0.0）だけの場合はマルチホップは確立されません。

例

次に、直接接続されていないネットワークに存在するネイバー 10.108.1.1 との間の接続を許可する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af) neighbor 10.108.1.1 ebgp-multihop
```

次に、直接接続されていないネットワークに存在するネイバー2001::1との間の接続を許可する例を示します。

```
ciscoasa(config)# router bgp 3
ciscoasa(config-router)# address-family ipv6
ciscoasa(config-router-af) neighbor 12001::1 ebgp-multihop
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor fall-over bfd（ルータ BGP）

BGP の BFD サポートを設定して、BFD からの転送パス検出障害メッセージを受信するように BGP を登録するには、ネイバーの設定時に **fall-over** オプションを使用します。

neighbor *ip_address* | *ipv6_address* **fall-over bfd**

構文の説明

ip_address/ipv6_address	ネイバー ルータの IP/IPv6 アドレス（A.B.C.D/ X:X:X:X::X 形式）。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ BFD コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

マルチホップ用に BGP の BFD サポートを設定する場合は、送信元/宛先ペアに関して BFD マップがすでに作成されていることを確認します。

例

次に、172.16.10.2 ネイバーと 1001::2 ネイバーの BFD サポートを設定する例を示します。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.10.2 fall-over bfd
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 1001::2 fall-over bfd
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。

コマンド	説明
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップテンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
clear bfd counters	BFD カウンタをクリアします。
echo	BFD シングルホップ テンプレートにエコーを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

neighbor filter-list

BGP フィルタを設定するには、アドレス ファミリ コンフィギュレーション モードで neighbor filter-list 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。

neighbor { *ip_address* | *ipv6-address* } **filter-list** *access-list-name* { **in** | **out** }
no neighbor { *ip_address* | *ipv6-address* } **filter-list** *access-list-name* { **in** | **out** }

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
access-list-name	自律システム パス アクセス リストの名前。このアクセスリストは as-path access-list コマンドで定義します。
in	着信ルートにアクセス リストを適用します。
out	発信ルートにアクセス リストを適用します。

コマンド デフォルト

BGP フィルタは使用されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドでは、着信と発信の両方 BGP ルートに対するフィルタを作成します。

（注） 特定の方向（着信または発信）のネイバーに対して neighbor distribute-list コマンドと neighbor prefix-list コマンドの両方を適用しないでください。これら 2 つのコマンド（neighbor distribute-list コマンドと neighbor prefix-list コマンド）は相互に排他的であり、着信または発信の各方向に対して 1 つしか適用できません。

例

次のアドレス ファミリ コンフィギュレーション モードの例では、隣接する自律システム 123 を経由するすべてのパスについて、IP アドレス 172.16.1.1 のネイバーでアドバタイズメントを送信しないように設定しています。

```
ciscoasa(config)# as-path access-list as-path-acl deny _123_
ciscoasa(config)# as-path access-list as-path-acl deny ^123$
ciscoasa(config)#router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 remote-as 123
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 47
ciscoasa(config-router-af)# neighbor 172.16.1.1 filter-list as-path-acl out
```

次のアドレス ファミリ コンフィギュレーション モードの例では、隣接する自律システムを経由するすべてのパスについて、IP アドレス 2001::1 の BGPv6 ネイバーでアドバタイズメントを送信しないように設定しています。

```
ciscoasa(config-router-af)# neighbor 2001::1 filter-list as-path-acl out
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
network	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。

neighbor ha-mode graceful-restart

ボーダー ゲートウェイ プロトコル（BGP）ネイバーの BGP グレースフル リスタート機能をイネーブルまたはディセーブルにするには、アドレス ファミリ コンフィギュレーション モードで neighbor ha-mode graceful-restart コマンドを使用します。コンフィギュレーションからネイバーの BGP グレースフル リスタート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。

neighbor *ip_address* **ha-mode graceful-restart** [**disable**]
no neighbor *ip_address* **ha-mode graceful-restart**

構文の説明

ip_address	ネイバーの IP アドレス。
disable	（オプション）ネイバーの BGP グレースフル リスタート機能をディセーブルにします。

コマンド デフォルト

BGP グレースフル リスタート機能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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

neighbor ha-mode graceful-restart コマンドは、個々の BGP ネイバーについて、グレースフル リスタート機能をイネーブルまたはディセーブルにする場合に使用します。グレースフル リスタート機能が BGP ピアでイネーブルになっている場合は、disable キーワードを使用してディセーブルにできます。

グレースフル リスタート機能は、セッションの確立時に OPEN メッセージのノンストップ フォワーディング（NSF）対応ピアと NSF 認識ピアの間でネゴシエートされます。BGP セッションの確立後にグレースフル リスタート機能をイネーブルにした場合は、セッションをソフト リセットまたはハード リセットして再起動する必要があります。

グレースフル リスタート機能は、NSF 対応 ASA および NSF 認識 ASA でサポートされます。NSF 対応 ASA では、ステートフル スイッチオーバー（SSO）処理（グレースフル リスタート）を実行し、その処理が完了するまでルーティング テーブル情報を保持することによってピアの再起動を支援できます。NSF 認識ルータは NSF 対応 ルータと同様に機能しますが、SSO 処理を実行することはできません。

（注） BGP グレースフル リスタート機能をすべての BGP ネイバーに対してグローバルにイネーブルにするには、bgp graceful-restart コマンドを使用します。個別のネイバーで BGP グレースフル リスタート機能が設定されている場合は、グレースフル リスタートを設定するためのそれぞれの方法のプライオリティは同じであり、最後の設定インスタンスがネイバーに適用されます。

BGP ネイバーの BGP グレースフル リスタートの設定を確認するには、show bgp neighbors コマンドを使用します。

例

次に、BGP ネイバー 172.21.1.2 に対して BGP グレースフル リスタート機能をイネーブルにする例を示します。

```
Ciscoasa(config)# router bgp 45000
Ciscoasa(config-router)# bgp log-neighbor-changes
Ciscoasa(config-router)# address-family ipv4 unicast
Ciscoasa(config-router-af)# neighbor 172.21.1.2 remote-as 45000
Ciscoasa(config-router-af)# neighbor 172.21.1.2 activate
Ciscoasa(config-router-af)# neighbor 172.21.1.2 ha-mode graceful-restart
```

関連コマンド

コマンド	説明
bgp graceful-restart	BGP グレースフル リスタート機能をすべての BGP ネイバーに対してグローバルにイネーブルまたはディセーブルにします。
show bgp neighbors	ネイバーへの TCP 接続および BGP 接続についての情報を表示します。

neighbor local-as

外部ボーダー ゲートウェイ プロトコル（eBGP）ネイバーから受信したルートの AS_PATH 属性をカスタマイズするには、アドレス ファミリ コンフィギュレーション モードで neighbor local-as コマンドを使用します。AS_PATH 属性のカスタマイズを無効にするには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **local-as** [*autonomous-system-number* [**no-prepend** [**replace-as** [**dual-as**]]]
no neighbor { *ip_address* | *ipv6-address* } **local-as**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
autonomous-system-number	（オプション）AS_PATH 属性の先頭に追加する自律システムの番号。この引数の値の範囲は、1 ～ 65535 の有効な自律システム番号です。 （注） この引数では、ローカル BGP ルーティング プロセスまたはリモート ピアのネットワークからの自律システム番号は指定できません。 自律システム番号の形式の詳細については、router bgp コマンドの説明を参照してください。
no-prepend	（オプション）eBGP ネイバーから受信したルートにローカル自律システム番号を追加しません。
replace-as	（オプション）実際の自律システム番号を eBGP アップデートのローカル自律システム番号で置き換えます。ローカル BGP ルーティング プロセスからの自律システム番号は、追加されません。
dual-as	（任意）ローカル BGP ルーティングプロセスからの実際の自律システム番号または autonomous-system-number 引数（local-as）で設定した自律システム番号を使用してピアリングセッションを確立するように eBGP ネイバーを設定します。

コマンド デフォルト

ローカル BGP ルーティング プロセスからの自律システム番号は、デフォルトで、すべての外部ルートに追加されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

neighbor local-as コマンドを使用して、eBGP ネイバーから受信するルートの自律システム番号を追加および削除して、AS_PATH 属性がカスタマイズされます。このコマンドの設定により、自律システム番号を移行するために、外部ピアに対して別の自律システムのメンバとしてルータを表示できます。この機能を使用すると、既存のピアリング関係を維持したまま、ネットワーク オペレータが通常のサービス時間内に顧客を新しいコンフィギュレーションに移行できるため、BGP ネットワークの自律システム番号を変更するプロセスが簡単になります。

⚠

注意 BGP は、ネットワーク到着可能性情報を維持し、ルーティング ループを防ぐために、ルートが通過する各 BGP ネットワークから自律システム番号をプリペンドします。このコマンドは自律システムの移行のためだけに設定し、移行が完了した後は設定を解除する必要があります。この手順は、経験豊富なネットワーク オペレータだけが行うべきものです。不適切な設定によってルーティング ループが作成される可能性があります。

このコマンドは、正しい eBGP ピアリング セッションにのみ使用できます。2 つのピアがコンフェデレーションの別々のサブ自律システムにある場合は機能しません。

円滑に移行するには、4 バイト自律システム番号を使用して指定されている自律システム内にあるすべてのBGPスピーカーで、4バイト自律システム番号をサポートするようアップグレードすることを推奨します。

例

Local-AS の例

次に、local-as 機能を使用して、ルータ 1 とルータ 2 のピアリングを自律システム 300 を介して確立する例を示します。

Router 1 (Local router)

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 172.16.1.1 remote-as 200
ciscoasa(config-router-af)# neighbor 172.16.1.1 local-as 300
Router 2 (Remote router)
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.0.0.1 remote-as 300
```

no-prepend キーワードの設定例

次に、ネイバー 192.168.1.1 から受信したルートに自律システム 500 を追加しないように BGP を設定する例を示します。

```
ciscoasa(config)# router bgp 400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.0.0
ciscoasa(config-router-af)# neighbor 192.168.1.1 local-as 500 no-prepend
```

replace-as キーワードの設定例

次の例では、プライベート自律システム 64512 を 172.20.1.1 ネイバーに対するアウトバウンドルーティング アップデートから取り除き、これを自律システム 600 に置き換えます。

```
ciscoasa(config)# router bgp 64512

ciscoasa(config-router)# address-family ipv4

ciscoasa(config-router-af)# neighbor 172.20.1.1 local-as 600 no-prepend replace-as

ciscoasa(config-router-af)# neighbor 172.20.1.1 remove-private-as
```

dual-as キーワードの設定例

次に、2 つのプロバイダー ネットワークと 1 つの顧客ネットワークの設定例を示します。ルータ 1 は自律システム 100 に属し、ルータ 2 は自律システム 200 に属しています。自律システム 200 は自律システム 100 にマージされます。この移行は自律システム 300 （顧客ネットワーク）のルータ 3 へのサービスを中断せずに行う必要があります。ルータ 1 で neighbor local-as コマンドを設定して、この移行の実行中にルータ 3 で自律システム 200 とのピアリングを維持するようにします。移行の完了後、通常のメンテナンス時間中またはその他のスケジュール済みのダウンタイム中にルータ 3 の設定を自律システム 100 を持つピアに対してアップデートできます。

Router 1 Configuration (Local Provider Network)

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# no synchronization
```

```
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
ciscoasa(config-router-af)# neighbor 10.3.3.33 local-as 200 no-prepend replace-as dual-as
```

Router 2 Configuration (Remote Provider Network)

```
ciscoasa(config)# router bgp 200

ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.11
 ciscoasa(config-router-af)# neighbor 10.3.3.33 remote-as 300
```

Router 3 Configuration (Remote Customer Network)

```
ciscoasa(config)# router bgp 300
ciscoasa(config-router)# address-family pv4
ciscoasa(config-router-af)# bgp router-id 100.0.0.3
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 200
```

2 つの自律システムをマージした後、移行を完了するために、ルータ 3 でピアリング セッションを更新します。

```
ciscoasa(config-router-af)# neighbor 10.3.3.11 remote-as 100
```

BGPv6 の設定

```
ciscoasa(config-router-af)# neighbor 2001::1 local-as 500 no-prepend
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
bgp router-id	ローカル ボーダー ゲートウェイ プロトコル（eBGP）ルーティング プロセスの固定ルータ ID を設定します。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。
network	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。
同期	BGP と内部ゲートウェイ プロトコル（IGP）システムの間の同期をイネーブルにします。

neighbor maximum-prefix

ネイバーから受信できるプレフィックスの数を制御するには、アドレス ファミリ コンフィギュレーション モードで neighbor maximum-prefix 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。

neighbor { *ip_address* | *ipv6-address* } **maximum-prefix** *maximum* [*threshold*] [**restart** *restart-interval*] [**warning-only**]
no neighbor { *ip_address* | *ipv6-address* } **maximum-prefix** *maximum*

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
maximum	このネイバーから許可されるプレフィックスの最大数。
threshold	（任意）maximum の値の何パーセントになったらルータが警告メッセージを生成するかを示す整数。指定できる範囲は 1 ～ 100 です。デフォルト値は 75（%）です。
restart	（オプション）最大プレフィックス数の制限を超えたためにディセーブルになったピアリング セッションを BGP を実行するルータで自動的に再確立するように設定します。再起動タイマーは restart-interval 引数で設定します。
restart-interval	（オプション）ピアリング セッションを再確立する時間間隔（分）。範囲は 1 ～ 65535 分です。
warning-only	（任意）maximum の値を超えた場合、ピアリングを終了せずに、ルータがログメッセージを生成できるようにします。

コマンド 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。プレフィックス数に制限はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドを使用すると、BGP ルータがピアから受信できるプレフィックスの最大数を設定できます。これは、ピアから受信されるプレフィックスの制御メカニズムを提供します（配布リスト、フィルタ リスト、ルート マップに加えて）。

受信プレフィックスの数が設定されている最大数を超えると、ルータはピアリングを終了します（デフォルト）。しかし、 warning-only キーワードが設定されている場合、代わりにログ メッセージが送信されるだけで、送信元とのピアリングは続行されます。終了されたピアは、clear bgp コマンドが発行されるまでダウンしたままになります。

例

次に、ネイバー 192.168.6.6 から受信できるプレフィックスの最大数を 1000 に設定する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 192.168.6.6 maximum-prefix 1000
```

次に、ネイバー 2001::1 から受信できるプレフィックスの最大数を 1000 に設定する例を示します。

```
ciscoasa(config-router-af)# neighbor 2001::1 maximum-prefix 1000
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
network	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。

neighbor next-hop-self

ルータを BGP スピーキングネイバーのネクストホップとして設定するには、アドレス ファミリ コンフィギュレーション モードで neighbor next-hop-self 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。

neighbor { *ip_address* | *ipv6-address* } **next-hop-self**
no neighbor { *ip_address* | *ipv6-address* } **next-hop-self**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
warning-only	（任意）maximum の値を超えた場合、ピアリングを終了せずに、ルータがログ メッセージを生成できるようにします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドは、BGP ネイバーから同じ IP サブネット上の他の一部のネイバーに直接アクセスできない非メッシュ型のネットワーク（フレーム リレーや X.25 など）で便利です。

例

次に、10.108.1.1 向けのすべてのアップデートに対し、このルータをネクスト ホップとしてアドバタイズするように設定する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 next-hop-self
```

次に、2001::1 向けのすべてのアップデートに対し、このルータをネクストホップとしてアドバタイズするように設定する例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 next-hop-selfs
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor password

2 つの BGP ピアの間の TCP 接続で Message Digest 5（MD5）認証を有効にするには、アドレス ファミリ コンフィギュレーション モードで neighbor password 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。

neighbor { *ip_address* | *ipv6-address* } **password** [**0-7**] *string*
no neighbor { *ip_address* | *ipv6-address* } **password**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
string	最大 25 文字のパスワード。大文字と小文字が区別されます。 最初の文字を数値にはできません。この文字列には、スペースも含め、あらゆる英数字を使用できます。数字-スペース-任意の文字の形式でパスワードを指定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。
0 ～ 7	（オプション）暗号化タイプ。0 ～ 6 を指定した場合は暗号化されません。暗号化する場合は 7 を使用します。

コマンド デフォルト

2 つの BGP ピアの間の TCP 接続で MD5 認証は使用されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

2 つの BGP ピアの間で MD5 認証を設定できます。ピア間の TCP 接続で送信された各セグメントが検証されます。MD5 認証は、両方の BGP ピアで同じパスワードを使用して設定する必要があります。そうしないと、接続を行うことはできません。MD5 認証を設定すると、ASA ソフトウェアにより、TCP 接続で送信される各セグメントの MD5 ダイジェストが生成され、チェックされるようになります。

MD5 認証を設定する場合、service password-encryption コマンドが有効になっているかどうかに関係なく、最大 25 文字のパスワード（大文字と小文字を区別する）を指定できます。パスワードの長さが 25 文字を超える場合は、エラー メッセージが表示され、パスワードが受け入れられません。この文字列には、スペースも含め、あらゆる英数字を使用できます。ただし、数字-スペース-任意の文字の形式でパスワードを設定することはできません。数字の後にスペースを使用すると、認証に失敗する原因となることがあります。さらに、英数字とともに次の記号を任意に組み合わせて使用できます。

` ~ ! @ # $ % ^ & * ( ) - _ = + | \ } ] { [ " ` : ; / > < . , ?

注意 認証文字列が正しく設定されていないと、BGP ピアリング セッションは確立されません。認証文字列を注意して入力するとともに、認証の設定後にピアリングセッションが確立されたかどうかを確認することを推奨します。

ネイバーに対してパスワードを設定しているルータと設定していないルータとの間でBGPセッションを確立しようとすると、次のようなメッセージがコンソールに表示されます。

%TCP-6-BADAUTH: No MD5 digest from [peer's IP address]:11003 to [local router's IP address]:179

同様に、2 台のルータに異なるパスワードが設定されている場合、次のようなメッセージが画面に表示されます。

%TCP-6-BADAUTH: Invalid MD5 digest from [peer's IP address]:11004 to [local router's IP address]:179

BGP セッション確立後の MD5 パスワードの設定

2 つの BGP ピアの間で MD5 認証に使用されるパスワードやキーを設定または変更した場合、パスワードの設定後にローカル ルータの既存のセッションは切断されません。ローカル ルータでは、BGP ホールド ダウン タイマーの期限が切れるまで、新しいパスワードを使用してピアリング セッションを維持しようとします。デフォルトの期間は 180 秒です。ホールド ダウン タイマーの期限が切れるまでの間にローカル ルータでパスワードを入力または変更しないと、セッションはタイムアウトします。

（注） ホールド ダウン タイマーに対して新しいタイマー値を設定した場合、その値はセッションがリセットされてからでないと有効になりません。したがって、ホールド ダウン タイマーの設定を変更しても、BGP セッションのリセットの回避には役立ちません。

例

次に、10.108.1.1 ネイバーとのピアリング セッションに対して MD5 認証を設定する例を示します。ホールド ダウン タイマーの期限が切れるまでの間に、リモート ピアで同じパスワードを設定する必要があります。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 10.108.1.1 password bla4u00=2nkq
```

次に、service password-encryption コマンドが無効になっている状態で 25 文字を超えるパスワードを設定する例を示します。

```
ciscoasa(config)# router bgp 200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# bgp router-id 2.2.2.2
ciscoasa(config-router-af)# neighbor remote-as 3
 ciscoasa(config-router-af)# neighbor 209.165.200.225 password 12345678912345678912345678901

    % BGP: Password length must be less than or equal to 25.
ciscoasa(config-router-af)# do show run | i password
 no service password-encryption
  neighbor 209.165.200.225 password 123456789123456789123456
```

次に、service password-encryption コマンドが有効になっている状態で 25 文字を超えるパスワードを設定した場合のエラーメッセージの例を示します。

```
 Router(config)# service password-encryption
 Router(config)# router bgp 200
 Router(config-router)# bgp router-id 2.2.2.2
 Router(config-router)# neighbor 209.165.200.225 remote-as 3
 Router(config-router)# neighbor 209.165.200.225 password 12345678912345678912345678901

 % BGP: Password length must be less than or equal to 25.
  Router(config-router)# do show run | i password  service password-encryption
  neighbor 209.165.200.225 password 123456789123456789123456
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
bgp router-id	ローカル ボーダー ゲートウェイ プロトコル（eBGP）ルーティング プロセスの固定ルータ ID を設定します。
neighbor remote-as	BGP ネイバー テーブルまたはマルチプロトコル BGP ネイバー テーブルにエントリを追加します。

neighbor prefix-list

プレフィックスリストで指定されたボーダー ゲートウェイ プロトコル（BGP）ネイバー情報を配布しないようにするには、アドレス ファミリ コンフィギュレーション モードで neighbor prefix-list コマンドを使用します。フィルタリストを削除するには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **prefix-list** *prefix-list-name* { **in** | **out** }
no neighbor { *ip_address* | *ipv6-address* } **prefix-list** *prefix-list-name* { **in** | **out** }

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-adress	ネイバー ルータの IPv6 アドレス。
prefix-list-name	プレフィックス リストの名前。
in	指定したネイバーからの着信アドバタイズメントにフィルタ リストを適用します。
out	指定したネイバーへの発信アドバタイズメントにフィルタ リストを適用します。

コマンド デフォルト

外部アドレスおよびアドバタイズされたアドレスのすべてのプレフィックスが BGP ネイバーに配布されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレス ファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

プレフィックス リストは、BGP アドバタイズメントをフィルタリングする 3 つの方法のうちの 1 つです。また、ip as-path access-list グローバル コンフィギュレーション コマンドで定義した AS パスフィルタを、neighbor filter-list コマンドで使用して BGP アドバタイズメントをフィルタリングできます。さらに、BGP アドバタイズメントをフィルタリングする 3 つ目の方法として、neighbor distribute-list コマンドでアクセスリストまたはプレフィックスリストを使用する方法があります。

（注） 特定の方向（着信または発信）のネイバーに対して neighbor distribute-list コマンドと neighbor prefix-list コマンドの両方を適用しないでください。これら 2 つのコマンド（neighbor distribute-list コマンドと neighbor prefix-list コマンド）は相互に排他的であり、着信または発信の各方向に対して 1 つしか適用できません。

例

次のアドレス ファミリ コンフィギュレーション モードの例では、abc という名前のプレフィックスリストをネイバー 10.23.4.1 からの着信アドバタイズメントに適用しています。

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.1.2
ciscoasa(config-router-af)# neighbor 10.23.4.1 prefix-list abc in
```

次のアドレス ファミリ ルータ コンフィギュレーション モードの例では、CustomerA いという名前のプレフィックス リストをネイバー 10.23.4.3 への発信アドバタイズメントに適用しています。

```
ciscoasa(config)# router bgp 64800
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 192.168.3.6
ciscoasa(config-router-af)# neighbor 10.23.4.3 prefix-list CustomerA out
The following address family router configuration mode example applies the prefix list
named CustomerA to outgoing advertisements to neighbor 2001::1:
ciscoasa(config-router-af)#neighbor 2001::1 prefix-list CustomerA out
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
network	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。

neighbor remote-as

BGP またはマルチプロトコル BGP ネイバーテーブルにエントリを追加するには、アドレス ファミリ コンフィギュレーション モードで neighbor remote-as コマンドを使用します。テーブルからエントリを削除するには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **remote-as** *autonomous-system-number*
no neighbor { *ip_address* | *ipv6-address* } **remote-as** *autonomous-system-number*

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
autonomous-system-number	ネイバーが属する自律システムの 1 ～ 65535 の範囲内の番号。 自律システム番号の形式の詳細については、router bgp コマンドの説明を参照してください。 alternate-as キーワードと一緒に使用した場合は、5 つまでの自律システム番号を入力できます。

コマンド デフォルト

BGP ネイバー ピアもマルチプロトコル BGP ネイバー ピアもありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

router bgp グローバル コンフィギュレーション コマンドで指定されている自律システム番号に一致する自律システム番号を持つネイバーを指定することにより、ローカル自律システムの内部にネイバーが指定されます。それ以外の場合は、ネイバーは外部にあると認識されます。

デフォルトでは、ルータ コンフィギュレーション モードで neighbor remote-as コマンドを使用して定義したネイバーが、ユニキャスト アドレス プレフィックスのみを交換します。

alternate-as キーワードを使用すると、ダイナミックな BGP ネイバーを識別できる代替自律システムを最大 5 つまで指定できます。BGP ダイナミック ネイバーのサポートは、IP アドレスの範囲で定義されたリモート ネイバーのグループへの BGP ピアリングを可能にします。BGP ダイナミック ネイバーは、IP アドレスおよび BGP ピア グループの範囲を使用して設定されます。bgp listen コマンドでサブネットの範囲が設定されて BGP ピアグループに関連付けられた後、そのサブネットの範囲の IP アドレスに対する TCP セッションを開始すると、新しい BGP ネイバーがそのグループのメンバーとして動的に作成されます。この新しい BGP ネイバーは、グループの設定やテンプレートをすべて継承します。

シスコが採用している 4 バイト自律システム番号では、自律システム番号の正規表現のマッチングおよび出力表示のデフォルトの形式として asplain（たとえば、65538）を使用していますが、RFC 5396 で定義されているとおり、4 バイト自律システム番号を asplain 形式および asdot 形式の両方で設定できます。4 バイト自律システム番号の正規表現マッチングと出力表示のデフォルトを asdot 形式に変更するには、bgp asnotation dot コマンドに続けて、clear bgp * コマンドを実行し、現在の BGP セッションをすべてハードリセットします。

例

次に、アドレス 10.108.1.2 にあるルータが、自律システム番号 65200 にある内部 BGP（iBGP）ネイバーになるよう指定する例を示します。

```
ciscoasa(config)# router bgp 65200
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# neighbor 10.108.1.2 remote-as 65200
```

次に、BGP ルータを自律システム 65400 に割り当て、自律システムの送信元として 2 つのネットワークのリストが表示される例を示します。3 つのリモート ルータ（とその自律システム）のアドレスのリストが表示されます。設定中のルータでは、ネットワーク 10.108.0.0 とネットワーク 192.168.7.0 の情報が、隣接ルータと共有されます。1 つ目の router は、この設定が入力されたルータ（eBGP ネイバー）とは異なる自律システムにあるリモート ルータです。2 つ目の neighbor remote-as コマンドにより、アドレス 10.108.234.2 の（自律システムの番号が同じの）内部 BGP ネイバーが表示されます。最後の neighbor remote-as コマンドにより、この設定が入力されたルータとは異なるネットワークにあるネイバー（これも eBGP ネイバー）が指定されます。

```
ciscoasa(config)# router bgp 65400
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
ciscoasa(config-router-af)# network 192.168.7.0
ciscoasa(config-router-af)# neighbor 10.108.200.1 remote-as 65200
ciscoasa(config-router-af)# neighbor 10.108.234.2 remote-as 65400
ciscoasa(config-router-af)# neighbor 172.29.64.19 remote-as 65300
```

次に、ユニキャスト ルータだけでやり取りするため、自律システム番号 65001 にあるネイバー 10.108.1.1 を設定する例を示します。

```
ciscoasa(config)# router bgp 65001
ciscoasa(config-router)# address-family ipv4
```

```
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.31 1.2 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.2 remote-as 65002
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
network	BGP ルーティング プロセスでアドバタイズするネットワークを指定します。
neighbor remove private-as	プライベート自律システム番号を eBGP アウトバウンド ルーティング アップデートから削除します。

neighbor remove-private-as

eBGP アウトバウンドルーティングアップデートからプライベート自律システム番号を削除するには、アドレス ファミリ コンフィギュレーション モードで neighbor remove-private-as 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。

neighbor { *ip_address* | *ipv6-address* } **remove-private-as** [**all** [**replace-as**]]
no neighbor { *ip_address* | *ipv6-address* } **remove-private-as** [**all** [**replace-as**]]

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
all	（オプション）発信更新の AS パスからプライベート AS 番号をすべて削除します。
replace-as	（任意）all キーワードを指定している限り、replace-as キーワードを指定すると、AS パスのすべてのプライベート AS 番号がルータのローカルの AS 番号に置き換わります。

コマンド デフォルト

AS パスからプライベート AS 番号は削除されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドは、外部 BGP（eBGP）ネイバーでのみ使用できます。プライベート AS の値の範囲は 64512 ～ 65535 です。外部ネイバーにアップデートを渡すときに AS パスにプライベート AS 番号が含まれていると、それらのプライベート AS 番号が削除されます。

- neighbor remove-private-as コマンドでは、AS パスにパブリックとプライベートの両方の ASN が含まれている場合でも、AS パスからプライベート AS 番号が削除されます。
- neighbor remove-private-as コマンドでは、AS パスにプライベート AS 番号のみが含まれている場合でも、AS パスからプライベート AS 番号が削除されます。このコマンドは eBGP ピアのみに適用され、その場合、eBGP ピアではローカル ルータの AS 番号が AS パスに付加されるため、長さ 0 の AS パスにはなることはありません。neighbor remove-private-as コマンドでは、AS パスでコンフェデレーション セグメントの前にプライベート ASN が出現する場合でも、プライベート AS 番号が削除されます。
- AS パスからプライベート AS 番号を削除すると、送信されるプレフィックスのパス長が減少します。AS パス長は BGP 最良パス選択の重要な要素であるため、パス長を保持するために必要な場合があります。replace-as キーワードは、削除されたすべての AS 番号をローカルルータの AS 番号で置き換えることでパス長が維持されるようにします。
- この機能は、アドレス ファミリ単位でネイバーに適用できます。そのため、この機能をあるアドレス ファミリのネイバーには適用して、別のアドレス ファミリでは適用しないようにすることで、機能が設定されているアドレス ファミリのみのアウトバウンド側のアップデート メッセージに影響を与えることができます。

例

次に、172.16.2.33 に送信されるアップデートからプライベート AS 番号を削除するように設定する例を示します。これにより、10.108.1.1 でアドバタイズされた AS 100 を経由するパスの AS パス（自律システム 2051 で認識されるパス）が「100」だけになります。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 description peer with private-as
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 65001
ciscoasa(config-router-af)# neighbor 172.16.2.33 description eBGP peer

ciscoasa(config-router-af)# neighbor 172.16.2.33 remote-as 2051
ciscoasa(config-router-af)# neighbor 172.16.2.33 remove-private-as


Router-in-AS100# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 15
Paths: (1 available, best #1)
 Advertised to non peer-group peers:
   172.16.2.33
 65001
    10.108.1.1 from 10.108.1.1
     Origin IGP, metric 0, localpref 100, valid, external, best
Router-in-AS2501# show bgp 10.0.0.0
BGP routing table entry for 10.0.0.0/8, version 3
Paths: (1 available, best #1)
  Not advertised to any peer
  2
```

```
172.16.2.32 from 172.16.2.32
 Origin IGP, metric 0, localpref 100, valid, external, best
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor description	ネイバーに説明を関連付けます。
neighbor remote-as	ルーティング テーブルに BGP またはマルチプロトコル BGP のルーティング エントリを追加します。

neighbor route-map

着信ルートまたは発信ルートにルートマップを適用するには、アドレスファミリ コンフィギュレーション モードで neighbor route-map コマンドを使用します。ルート マップを削除するには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **route-map** *map-name* { **in** | **out** }
no neighbor { *ip_address* | *ipv6-address* } **route-map** *map-name* { **in** | **out** }

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
map-name	ルート マップの名前。
in	着信ルートにルートマップを適用します。
out	発信ルートにルートマップを適用します。

コマンド デフォルト

ピアにルート マップは適用されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドをアドレス ファミリ コンフィギュレーション モードで指定した場合、そのアドレス ファミリだけにルート マップが適用されます。ルータ コンフィギュレーション モードで指定した場合は、IPv4 ユニキャスト ルートだけにルート マップが適用されます。

発信ルートマップを指定した場合、ルートマップの少なくとも1のセクションに一致するルートだけがアドバタイズされます。これは適切な動作です。

例

次に、172.16.70.24 からの BGP 着信ルートに internal-map という名前のルート マップを適用する例を示します。

```
ciscoasa(config)# router bgp 5
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.24 route-map internal-map in
ciscoasa(config-router-af)# route-map internal-map
ciscoasa(config-route-map)# match as-path 1
ciscoasa(config-route-map)# set local-preference 100
```

次に、2001::1 からの BGP 着信ルートに internal-map という名前のルート マップを適用する例を示します。

```
ciscoasa(config-router-af)# neighbor 2001::1 route-map internal-map in
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
match as-path	アクセス リストで指定されている BGP 自律システム パスを照合します。
ルート マップ	あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義します。
match as-path	アクセス リストで指定されている BGP 自律システム パスを照合します。
set local-preference	自律システム パスのプリファレンス値を指定します。

neighbor send-community

コミュニティ属性を BGP ネイバーに送信するように指定するには、アドレス ファミリ コンフィギュレーション モードで neighbor send-community コマンドを使用します。エントリを削除するには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **send-community**
no neighbor { *ip_address* | *ipv6-address* } **send-community**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。

コマンド デフォルト

いずれのネイバーにもコミュニティ属性は送信されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

例

次に示すアドレス ファミリ コンフィギュレーション モードの例では、ルータが自律システム 109 に属しており、IP アドレス 172.16.70.23 のネイバーにコミュニティ属性を送信するように設定します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.70.23 send-community
```

次の例では、IP アドレス 2001::1 のネイバーにコミュニティ属性を送信するようにルータを設定しています。

```
ciscoasa(config-router-af)# neighbor 2001::1 send-community
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。

neighbor shutdown

ネイバーを無効にするには、アドレス ファミリ コンフィギュレーション モードで neighbor shutdown コマンドを使用します。ネイバーを再び有効にするには、このコマンドの no 形式を使用します。

neighbor *ip_address* **shutdown**
no neighbor *ip_address* **shutdown**

構文の説明

ip_address ネイバールータの IP アドレス。

コマンド デフォルト

いずれの BGP ネイバーの状態も変更されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

neighbor shutdown コマンドを使用すると、指定したネイバーに対するアクティブなセッションが終了し、関連するルーティング情報がすべて削除されます。

BGP ネイバーの要約を表示するには、show bgp summary コマンドを使用します。アイドル状態のネイバーと Admin エントリは neighbor shutdown コマンドによって無効化されています。

「State/PfxRcd」には、BGP セッションの現在の状態、またはルータがネイバーから受信したプレフィックスの数が表示されます。最大数（neighbor maximum-prefix コマンドで設定）に達すると、文字列「PfxRcd」がエントリに表示され、ネイバーがシャットダウンされて、接続がアイドルになります。

例

次に、ネイバー 172.16.70.23 に対するアクティブなセッションをディセーブルにする例を示します。

```
ciscoasa(config-router-af)# neighbor 172.16.70.23 shutdown
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
show bgp summary	BGP ネイバー ステータスの要約を表示します。

neighbor timers

特定の BGP ピアのタイマーを設定するには、アドレス ファミリ コンフィギュレーション モードで neighbor timers コマンドを使用します。特定の BGP ピアのタイマーをクリアするには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **timers** *keepalive holdtime* [*min-holdtime*]

no neighbor { *ip_address* | *ipv6-address* } **timers**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
Keepalive（キープアライブ）	ASA ソフトウェアからピアにキープアライブメッセージを送信する間隔（秒数）。デフォルトは 60 秒で、範囲は 0 ～ 65535 秒です。
holdtime	キープアライブメッセージを受信できない状態が継続して、ピアがデッドであるとソフトウェアが宣言するまでの時間（秒単位）。デフォルト値は 180 秒です。範囲は 0 ～ 65535 です。
min-holdtime	（オプション）BGP ネイバーからの最小許容ホールド タイムを指定する間隔（秒単位）。最小許容ホールドタイムは、holdtime 引数で指定された間隔以下にする必要があります。指定できる範囲は 0 ～ 65535 です。

コマンド デフォルト

キープアライブ時間：60 秒

ホールド時間：180 秒。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

リリース	変更内容
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

- 特定のネイバーに対して設定したタイマーは、timers bgp コマンドを使用してすべての BGP ネイバーに対して設定したタイマーよりも優先されます。
- holdtime 引数の値を 20 秒未満に設定すると、「A hold time of less than 20 seconds increases the chances of peer flapping」という警告が表示されます。
- 指定したホールド時間よりも最小許容ホールド時間の方が長い場合、「Minimum acceptable hold time should be less than or equal to the configured hold time」という通知が表示されます。

（注） BGP ルータに最小許容ホールド タイムが設定されている場合、リモート BGP ピア セッションは、リモート ピアが最小許容ホールド タイム間隔以上のホールド タイムをアドバタイズする場合にのみ確立されます。最小許容ホールド タイム間隔が、設定されたホールド タイムを超過する場合、次回のリモート セッション確立の試行は失敗し、ローカル ルータは「unacceptable hold time」という示す通知を送信します。

例

次に、BGP ピア 192.168.47.0 について、キープアライブタイマーを 70 秒、ホールド時間タイマーを 210 秒に変更する例を示します。

```
ciscoasa(config-router-af)# neighbor 192.168.47.0 timers 70 210
```

次に、BGP ピア 192.168.1.2 について、キープアライブタイマーを 70 秒、ホールド時間タイマーを 130 秒、最小ホールド時間を 100 秒に変更する例を示します。

```
ciscoasa(config-router-af)# neighbor 192.168.1.2 timers 70 130 100
```

次に、BGP ピア 2001::1 について、キープアライブタイマーを 70 秒、ホールド時間タイマーを 210 秒に変更する例を示します。

```
ciscoasa(config-router-af)# neighbor 2001::1 timers 70 210
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor transport

ボーダー ゲートウェイ プロトコル（BGP）セッションの TCP 転送セッションオプションを有効にするには、ルータ コンフィギュレーション モードまたはアドレス ファミリ コンフィギュレーション モードで neighbor transport コマンドを使用します。BGP セッションの TCP 転送セッションオプションを無効にするには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **transport** { **connection-mode** { **active** | **passive** } | **path-mtu-discovery** [**disable**] }
no neighbor { *ip_address* | *ipv6-address* } **transport** { **connection-mode** { **active** | **passive** } | **path-mtu-discovery** [**disable**] }

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
connection-mode	接続のタイプ（アクティブまたはパッシブ）を指定します。
active	アクティブ接続を指定します。
passive	パッシブ接続を指定します。
path-mtu-discovery	TCP 転送パスの最大伝送ユニット（MTU）ディスカバリをイネーブルにします。TCP パス MTU ディスカバリは、デフォルトではイネーブルです。
disable	TCP パス MTU ディスカバリをディセーブルにします。

コマンド デフォルト

このコマンドを設定しない場合、TCP パス MTU ディスカバリはデフォルトでイネーブルになりますが、それ以外の TCP 転送セッション オプションはイネーブルになりません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

リリース	変更内容
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドは、各種の転送オプションを指定するために使用されます。BGPセッションに対して、アクティブまたはパッシブのいずれかの転送接続を指定できます。より大規模な MTU のリンクをBGPセッションで利用するには、TCP転送パスのMTUディスカバリをイネーブルにします。TCP パスの MTU ディスカバリが有効になっているか確認するには、show bgp neighbors コマンドを使用します。disable キーワードを使用してディスカバリを無効にした場合、無効にしたディスカバリのテンプレートを継承するすべてのピアでディスカバリが無効になります。

例

次に、1 つの内部 BGP（iBGP）ネイバーについて、TCP 転送接続をアクティブに設定する例を示します。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# neighbor 172.16.1.2 transport connection-mode active
```

次に、1 つの外部 BGP（eBGP）ネイバーについて、TCP 転送接続をパッシブに設定する例を示します。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 192.168.1.2 remote-as 40000
ciscoasa(config-router-af)# neighbor 192.168.1.2 activate
ciscoasa(config-router-af)# neighbor 192.168.1.2 transport connection-mode passive
```

次に、1 つの BGP ネイバーについて、TCP パスの MTU ディスカバリをディセーブルにする方法の例を示します。

```
ciscoasa(config)# router bgp 45000
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.1.2 remote-as 45000
ciscoasa(config-router-af)# neighbor 172.16.1.2 activate
ciscoasa(config-router-af)# no neighbor 172.16.1.2 transport path-mtu-discovery
```

次に、1 つの BGPv6 ネイバーについて、TCP 転送接続をアクティブに設定する例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 transport connection-mode active
```

次に、1 つの BGPv6 ネイバーについて、TCP パスの MTU ディスカバリをイネーブルにする方法の例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 transport path-mtu-discovery
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor remote-as	BGP またはマルチプロトコル BGP のルーティング テーブルにエントリを追加します。
show bgp neighbor	BGP ネイバーに関する情報を表示します。

neighbor ttl-security

ボーダー ゲートウェイ プロトコル（BGP）ピアリングセッションを保護し、2 つの外部 BGP（eBGP）ピアを区切るホップの最大数を設定するには、アドレス ファミリ コンフィギュレーション モードで neighbor ttl-security 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。

neighbor { *ip_address* | *ipv6-address* } **ttl-security hops** *hop-count*
no neighbor { *ip_address* | *ipv6-address* } **ttl-security hops** *hop-count*

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
hop-count	eBGP ピアを区切るホップの数。TTL 値は、設定された hop-count 引数に基づいてルータにより計算されます。 有効な値は 1 ～ 254 の数値です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

neighbor ttl-security コマンドは、CPU 利用率に基づく攻撃から BGP ピアリングセッションを保護するための簡単なセキュリティメカニズムを提供します。この種の攻撃は、通常、パケットヘッダーの送信元と宛先の IP アドレスを偽造した大量の IP パケットでネットワークをあふれ

させてネットワークをディセーブルにしようとする典型的な力任せのサービス拒否（DoS）攻撃です。

この機能は、TTL カウントがローカルの設定値以上である IP パケットだけを受け入れるという IP パケットの設計上の動作を利用したものです。IP パケットの TTL カウントを完全に偽造することは一般には不可能であると考えられます。内部の送信元ネットワークまたは宛先ネットワークにアクセスしない限り、信頼できるピアからの TTL カウントに完全に一致するパケットを偽造することはできません。

この機能は、参加している各ルータで設定する必要があります。この機能では、eBGP セッションが受信方向だけ保護され、送信 IP パケットまたはリモート ルータは影響を受けません。この機能がイネーブルの場合、BGP は、IP パケット ヘッダーの TTL 値がピアリング セッション用に設定された TTL 値以上の場合だけセッションを確立または維持します。この機能は BGP ピアリング セッションには影響しません。この機能がイネーブルの場合でも、キープアライブ パケットを受信しなければピアリング セッションは期限切れになります。受信パケットの TTL 値が、ローカルで設定された値未満の場合、パケットはサイレントに廃棄され、インターネット制御メッセージ プロトコル（ICMP）メッセージは生成されません。これは設計された動作です。偽造パケットへの応答は必要ありません。

この機能の効果を最大化するには、ローカルネットワークと外部ネットワーク間のホップ数が一致するように hop-count の値を正確に設定する必要があります。また、この機能をマルチホップ ピアリング セッションに対して設定する場合は、パスがそれぞれで異なる点についても考慮する必要があります。

このコマンドの設定には、次の制限が適用されます。

- この機能は、内部 BGP（iBGP）ピアではサポートされません。
- neighbor ttl-security コマンドは、すでに neighbor ebgp-multihop コマンドが設定されているピアには設定できません。これらのコマンドのコンフィギュレーションは相互に排他的であり、マルチホップ eBGP ピアリング セッションをイネーブルにする場合はどちらか一方のみを設定する必要があります。同じピアリング セッションに対して両方のコマンドを設定しようとすると、コンソールにエラー メッセージが表示されます。
- 大きい直径のマルチホップ ピアリングでは、この機能の効果は下がります。大きい直径のピアリング用に設定された BGP ルータに対する CPU 利用率に基づく攻撃の場合は、影響を受けたピアリング セッションをシャットダウンして、この攻撃に対処する必要がある場合があります。
- この機能は、ネットワーク内部が損なわれているピアからの攻撃には効果的ではありません。この制約事項には、送信元ネットワークと宛先ネットワークの間のネットワーク セグメント上のピアも含まれます。

例

次に、直接接続されたネイバーのホップ カウントを 2 に設定する例を示します。hop-count 引数が 2 に設定されるため、BGP は、ヘッダーの TTL カウントが 253 以上の IP パケットだけを受け入れます。IP パケット ヘッダーの TTL 値がそれ以外の値であるパケットは、サイレントに廃棄されます。

```
ciscoasa(config-router-af)# neighbor 10.0.0.1 ttl-security hops 2
```

次に、直接接続された BGPv6 ネイバーのホップ カウントを 2 に設定する例を示します。

```
ciscoasa(config-router-af)#neighbor 2001::1 ttl-security hops 2
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor ebgp-multihop	直接接続されていないネットワーク上の外部ピアからの BGP 接続を受け入れ、またそのピアへの BGP 接続を試みます。

neighbor update-source

インターフェイスを BGP スピーキングネイバーの送信元として設定するには、アドレス ファミリ コンフィギュレーション モードで **neighbor update-source** 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。

neighbor { *ipv_address* | *ipv6-address* } **update-source** { *interface name* }

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
interface name	ASA が BGP ルーティングの送信元として使用する、`nameif` コマンドで指定されたインターフェイスの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.18(2)	このコマンドが追加されます。

使用上のガイドライン

このコマンドは、ループバック インターフェイス上で BGP プロトコルを実行し、ループバック インターフェイスが再配布とプレフィックス アドバタイズメントに参加できるようにする場合に役立ちます。

例

次に、BGP ネイバー 10.108.1.1 の送信元としてループバック インターフェイス loop1 を更新する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4 unicast
ciscoasa(config-router-af)# neighbor 10.108.1.1 remote-as 109
ciscoasa(config-router-af)# neighbor 10.108.1.1 update-source loop1
```

次に、BGP ネイバー 2001::1 の送信元としてループバック インターフェイス loop1 を更新する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv6 unicast
ciscoasa(config-router-af)# neighbor 2001::1 remote-as 109
ciscoasa(config-router-af)# neighbor 2001::1 update-source loop1
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。
neighbor remote-as	ルーティング テーブルに BGP またはマルチプロトコル BGP のルーティング エントリを追加します。

neighbor version

特定のバージョンの BGP だけを受け入れるように ASA ソフトウェアを設定するには、アドレス ファミリ コンフィギュレーション モードで neighbor version コマンドを使用します。デフォルトのバージョンレベルのネイバーを使用するには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **version** *number*
no neighbor { *ip_address* | *ipv6-address* } **version** *number*

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
number	BGP バージョン番号。バージョンを 2 に設定すると、指定されたネイバーとの間でバージョン 2 だけが使用されます。デフォルトでは、バージョン 4 が使用され、要求された場合は動的にネゴシエートしてバージョン 2 に下がります。

コマンド デフォルト

BGP バージョン 4。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このコマンドを入力すると、バージョンの動的なネゴシエーションがディセーブルになります。

例

次に、BGP プロトコルをバージョン 4 だけに制限する例を示します。

```
ciscoasa(config)# router bgp 109
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# neighbor 172.16.27.2 version 4
ciscoasa(config-router-af)# neighbor 2001::1 version 4
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

neighbor weight

ネイバー接続に重みを割り当てるには、アドレス ファミリ コンフィギュレーション モードで neighbor weight コマンドを使用します。重みの割り当てを削除するには、このコマンドの no 形式を使用します。

neighbor { *ip_address* | *ipv6-address* } **weight number**
no neighbor { *ip_address* | *ipv6-address* } **weight number**

構文の説明

ip_address	ネイバー ルータの IP アドレス。
ipv6-address	ネイバー ルータの IPv6 アドレス。
number	割り当てる重み。 有効な値は、0 ～ 65535 です。

コマンド デフォルト

別の BGP ピアから学習されたルートのデフォルトの重みは 0 です。ローカル ルータから送信されたルートのデフォルトの重みは 32768 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

このネイバーから学習したすべてのルートに、まず重みが割り当てられます。特定のネットワークへのルートが複数ある場合、重みが最大のルートが優先ルートとして選ばれます。

set weight route-map コマンドで割り当てた重みは、neighbor weight コマンドで割り当てた重みより優先されます。

例

次のアドレス ファミリ コンフィギュレーション モードの例では、172.16.12.1 から学習したすべてのルートの重みを 50 に設定しています。

```
ciscoasa(config-router-af)# neighbor 172.16.12.1 weight 50
```

次のアドレス ファミリ コンフィギュレーション モードの例では、2001::1 から学習したすべてのルートの重みを設定しています。

```
ciscoasa(config-router-af)# neighbor 2001::1 weight 50
```

関連コマンド

コマンド	説明
address-family ipv4	アドレスファミリ コンフィギュレーション モードに入ります。
neighbor activate	BGP ネイバーとの情報交換をイネーブルにします。

nem

ハードウェアクライアントのネットワーク拡張モードを有効にするには、グループ ポリシー コンフィギュレーション モードで **nem enable** コマンドを使用します。NEM を無効にするには、**nem disable** コマンドを使用します。実行コンフィギュレーションから NEM 属性を削除するには、このコマンドの **no** 形式を使用します。このオプションを使用すると、別のグループ ポリシーの値を継承できます。

nem { **enable|disable** }
no nem

構文の説明

disable	ネットワーク拡張モードをディセーブルにします。
enable	ネットワーク拡張モードをイネーブルにします。

コマンド デフォルト

ネットワーク拡張モード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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

使用上のガイドライン

ネットワーク拡張モードを使用すると、ハードウェア クライアントは、VPN トンネルを介したリモート プライベート ネットワークへの単一のルーティング可能なネットワークを提供できます。IPsec は、ハードウェアクライアントの背後にあるプライベートネットワークから ASA の背後にあるネットワークへのトラフィックをすべてカプセル化します。PAT は適用されません。したがって、ASA の背後にあるデバイスは、ハードウェアクライアントの背後にある、トンネルを介したプライベートネットワーク上のデバイスに直接アクセスできます。これはトンネルを介した場合に限ります。逆の場合も同様です。トンネルはハードウェア クライアントによって開始される必要がありますが、トンネルがアップ状態になったあとは、いずれの側もデータ交換を開始できます。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、FirstGroup というグループ ポリシーの NEM を設定する例を示します。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)
# nem enable
```

netmod

ネットワークモジュールを無効にするには、グローバル コンフィギュレーション モードで **netmod** コマンドを使用します。ネットワークモジュールを有効にするには、このコマンドの **no** 形式を使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

netmod 2 disable
no netmod 2 disable

構文の説明

2	スロット 2 のモジュールを指定します。
disable	ネットワークモジュールを無効にしました。

コマンド デフォルト

最初の起動時にインストールされていたモジュールは、有効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドは、Cisco Secure Firewall 3100 に導入されました。

使用上のガイドライン

最初にファイアウォールの電源をオンにする前にネットワークモジュールをインストールした場合、アクションは不要です。ネットワークモジュールは有効になり、使用できる状態になっています。初回ブートアップ後にネットワークモジュールのインストールを変更する必要がある場合は、このコマンドを使用します。

新しいモジュールを追加したり、モジュールを完全に削除したりする場合は、リロードが必要です。リロードすることなく、同じタイプの新しいモジュールのネットワークモジュールをホットスワップできます。ただし、現在のモジュールを安全に取り外すには、シャットダウンする必要があります。ネットワークモジュールを別のタイプに交換する場合は、リロードが必

要です。新しいモジュールのインターフェイス数が古いモジュールよりも少ない場合は、存在しなくなるインターフェイスに関連する構成を手動で削除する必要があります。

例

次に、ネットワークモジュールを無効にする例を示します。

```
ciscoasa(config)# netmod 2 disable
```

次に、ネットワークモジュールを有効にする例を示します。

```
ciscoasa(config)# no netmod 2 disable
```

network（アドレス ファミリ）

ボーダー ゲートウェイ プロトコル（BGP）ルーティングプロセスでアドバタイズするネットワークを指定するには、アドレス ファミリ コンフィギュレーション モードで network コマンドを使用します。ルーティング テーブルからエントリを削除するには、このコマンドの no 形式を使用します。

network { *ipv4_address* [**mask** *network_mask*] | *IPv6_prefix* | *prefix_length* | *prefix_delegation_name* [*subnet_prefix* | *prefix_length*] } [**route-map** *route_map_name*]
no network { *ipv4_address* [**mask** *network_mask*] | *IPv6_prefix* | *prefix_length* | *prefix_delegation_name* [*subnet_prefix* | *prefix_length*] } [**route-map** *route_map_name*]

構文の説明

ipv4_address	BGP またはマルチプロトコル BGP でアドバタイズする IPv4 ネットワーク。
ipv6_prefix/prefix_length	BGP またはマルチプロトコル BGP でアドバタイズする IPv6 ネットワーク。
mask network_mask	（オプション）ネットワークまたはサブネットワークのマスクとそのアドレス。
prefix_delegation_name	DHCPv6 プレフィクス委任クライアント（**ipv6 dhcp client pd**）を有効にすると、プレフィックスをアドバタイズできます。
subnet_prefix/prefix_length	（オプション）プレフィックスをサブネットするには、subnet_prefix/プレフィックス長を指定します。
route-map route_map_name	（オプション）設定されているルート マップの ID。ルート マップは、アドバタイズされるネットワークをフィルタリングするために調べる必要があります。この値を指定しない場合、すべてのネットワークがアドバタイズされます。このキーワードを指定し、ルート マップ タグを 1 つも指定しないと、いずれのネットワークもアドバタイズされません。

コマンド デフォルト

ネットワークは指定されていません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
アドレスファミリ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。
9.6(2)	*prefix_delegation_name* [*subnet_prefix*/*prefix_length*] 引数が追加されました。

使用上のガイドライン

BGP およびマルチプロトコル BGP のネットワークは、接続されたルート、ダイナミック ルーティング、およびスタティック ルートの情報源から学習できます。

使用できる network コマンドの最大数は、設定されている NVRAM や RAM など、ルータのリソースで決まります。

例

次に、ネットワーク 10.108.0.0 を BGP アップデートに含めるように設定する例を示します。

```
ciscoasa(config)# router bgp 65100
ciscoasa(config-router)# address-family ipv4
ciscoasa(config-router-af)# network 10.108.0.0
```

関連コマンド

コマンド	説明
show bgp interfaces	BGPルーティングテーブル内のエントリを表示します。

network（ルータ EIGRP）

EIGRP ルーティングプロセスのネットワークのリストを指定するには、ルータ コンフィギュレーション モードで **network** コマンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

network *ip_addr* [*mask*]
no network *ip_addr* [*mask*]

構文の説明

ip_addr	直接接続されたネットワークの IP アドレス。指定されたネットワークに接続されているインターフェイスが、EIGRP ルーティング プロセスに参加します。
mask	（任意）IP アドレスのネットワーク マスク。

コマンド デフォルト

ネットワークは指定されていません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

network コマンドは、指定されたネットワークに IP アドレスが少なくとも 1 つ存在するすべてのインターフェイスで EIGRP を開始します。また、指定されたネットワークから接続済みのサブネットを EIGRP トポロジ テーブルに挿入します。

次に、ASA は一致したインターフェイス経由でネイバーを確立します。ASA に設定できる **network** コマンドの数に制限はありません。

例

次に、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されているすべてのインターフェイスで使用されるルーティング プロトコルとして EIGRP を定義する例を示します。

```
ciscoasa(config)# router eigrp 100
```

```
ciscoasa(config-router)# network 10.0.0.0 255.0.0.0
ciscoasa(config-router)# network 192.168.7.0 255.255.255.0
```

関連コマンド

コマンド	説明
show eigrp interfaces	EIGRP に設定されているインターフェイスに関する情報を表示します。
show eigrp topology	EIGRP トポロジ テーブルを表示します。

network（ルータ RIP）

RIP ルーティングプロセスのネットワークのリストを指定するには、ルータ コンフィギュレーション モードで **network** コマンドを使用します。ネットワーク定義を削除するには、このコマンドの **no** 形式を使用します。

network { *ip_addr* | *ipv6-address* } | < *prefix-length* >
no network { *ip_addr* | *ipv6-address* } |< *prefix-length* >[**route-map** *route-map-name*]

構文の説明

ip_addr	直接接続されたネットワークの IP アドレス。指定されたネットワークに接続されているインターフェイスが、RIP ルーティング プロセスに参加します。
ipv6-address	使用する IPv6 アドレス。IPv6 アドレスは、X:X:X:X::X の形式で入力する必要があります。
prefix-length	IPv6 プレフィックスの長さ。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。 有効な値は、0 ～ 128 です。
route-map-name	属性を変更するルート マップ。

コマンド デフォルト

ネットワークは指定されていません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション、アドレス ファミリ コンフィギュレーション モード	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

リリース	変更内容
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.3(2)	ipv6-address 引数が追加され、IPv6 アドレス ファミリがサポートされるようになりました。

使用上のガイドライン

指定されたネットワーク番号は、サブネット情報に含めないでください。ルータで使用できる network コマンドの数に制限はありません。指定されたネットワーク上のインターフェイスのみを経由して、RIP ルーティング更新が送受信されます。また、インターフェイスのネットワークが指定されていない場合は、どのRIPルーティング更新でもインターフェイスがアドバタイズされません。

例

次に、ネットワーク 10.0.0.0 および 192.168.7.0 に接続されているすべてのインターフェイスで使用されるルーティング プロトコルとして RIP を定義する例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# network 192.168.7.0
In the following example the attributes of the test-route-map route map connected to the
 2001::1 network will be modified.
ciscoasa(config-router)# network 2001:0:0:0::1 route-map test-route-map
```

関連コマンド

コマンド	説明
router rip	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。

network-acl

access-list コマンドを使用して以前に設定したファイアウォールの ACL 名を指定するには、ダイナミック アクセス ポリシー レコード コンフィギュレーション モードで **network-acl** コマンドを使用します。既存のネットワーク ACL を削除するには、このコマンドの **no** 形式を使用します。すべてのネットワーク ACL を削除するには、このコマンドを引数なしで使用します。

network-acl *name*
no network-acl [*name*]

構文の説明

name ネットワーク ACL の名前を指定します。名前の最大文字数は 240 文字です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ダイナミック アクセス ポリシー レコード コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

複数のファイアウォール ACL を DAP レコードに割り当てるには、このコマンドを複数回使用します。

ASA は、指定された各 ACL を検証して、アクセスリストエントリの許可ルールのみまたは拒否ルールのみが含まれていることを確認します。指定されたいずれかの ACL に許可ルールと拒否ルールが混在している場合、ASA はコマンドを拒否します。

次に、Finance Restrictions というネットワーク ACL を Finance という DAP レコードに適用する例を示します。

```
ciscoasa
(config)#

dynamic-access-policy-record Finance
```

```
ciscoasa
(config-dynamic-access-policy-record)#
 network-acl Finance Restrictions
ciscoasa
(config-dynamic-access-policy-record)#
```

関連コマンド

コマンド	説明
access-policy	ファイアウォール アクセス ポリシーを設定します。
dynamic-access-policy-record	DAP レコードを作成します。
show running-config dynamic-access-policy-record [*name*]	すべての DAP レコードまたは指定した DAP レコードの実行コンフィギュレーションを表示します。

network area

OSPF が動作するインターフェイスを定義し、そのインターフェイスのエリア ID を定義するには、ルータ コンフィギュレーション モードで **network area** コマンドを使用します。アドレス/ネットマスクのペアで定義されたインターフェイスの OSPF ルーティングを無効にするには、このコマンドの **no** 形式を使用します。

network *addr mask* **area** *area_id*
no network *addr mask* **area** *area_id*

構文の説明

addr	[IP Address]。
area *area_id*	OSPF アドレス範囲に関連付けられるエリアを指定します。*area_id* は、IP アドレス形式または 10 進表記で指定できます。10 進表記で指定する場合、有効な値の範囲は、0 ～ 4294967295 です。
mask	ネットワーク マスク。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスで OSPF を動作させるには、インターフェイスのアドレスを **network area** コマンドの対象にする必要があります。**network area** コマンドがインターフェイスの IP アドレスを対象にしていない場合、そのインターフェイスを経由する OSPF は有効になりません。

ASA で使用できる **network area** コマンドの数に制限はありません。

例

次に、192.168.1.1 インターフェイスで OSPF をイネーブルにし、エリア 2 に割り当てる例を示します。

```
ciscoasa(config-router)# network 192.168.1.1 255.255.255.0 area 2
```

関連コマンド

コマンド	説明
router ospf	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。

network-object

ホスト オブジェクト、ネットワーク オブジェクト、またはサブネット オブジェクトをネットワーク オブジェクト グループに追加するには、オブジェクト グループ ネットワーク コンフィギュレーション モードで network-object コマンドを使用します。ネットワークオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

network-object { **host** *address* | *IPv4_address mask* | *IPv6_address* | *IPv6_prefix* | **object** *name* }
no network-object { **host** *ip_address* | *ip_address mask* | **object** *name* }

構文の説明

host *ip_address*	ホストの IPv4 アドレスまたは IPv6 アドレスを指定します。
IPv4_address mask	IPv4 ネットワーク アドレスおよびサブネット マスクを指定します。
IPv6_address/IPv6_prefix	IPv6 ネットワーク アドレスおよびプレフィックス長を指定します。
object *name*	ネットワークオブジェクト（**object network** コマンドで作成）を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
オブジェクト グループ ネットワーク コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	ネットワークオブジェクト（**object network** コマンド）をサポートするために、**object** 引数が追加されました。
9.0(1)	以前は、ネットワーク オブジェクト グループに含まれているのは、すべて IPv4 アドレスであるか、すべて IPv6 アドレスでなければなりませんでした。現在は、ネットワーク オブジェクト グループで IPv4 と IPv6 の両方のアドレスの混合がサポートされるようになりました。ただし、NAT で混合グループを使用することはできません。

使用上のガイドライン

network-object コマンドは、ホストオブジェクト、ネットワークオブジェクト、またはサブネットオブジェクトを定義するために、**object-group** コマンドとともに使用されます。

例

次に、 **network-object** コマンドを使用して、新しいホストオブジェクトをネットワーク オブジェクト グループに作成する例を示します。

```
ciscoasa(config)# object-group network sjj_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjj.eng.ftp
ciscoasa(config-network-object-group)# network-object host 172.16.56.195
ciscoasa(config-network-object-group)# network-object 192.168.1.0 255.255.255.224
ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
object network	ネットワーク オブジェクトを追加します。
object-group network	ネットワーク オブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

network-service-member

ネットワーク サービス グループにネットワーク サービス オブジェクトを追加するには、オブジェクト グループ コンフィギュレーション モードで **network-service-member** コマンドを使用します。オブジェクトをグループから削除するには、コマンドの **no** 形式を使用します。

network-service-member *object_name*
no network-service-member *object_name*

構文の説明

object_name ネットワーク サービス オブジェクトの名前。名前にスペースが含まれている場合は、その名前を二重引用符で囲みます。

コマンド デフォルト

デフォルト値はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ネットワーク サービス オブジェクトグループ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドが追加されました。

例

次に、3 つの既存のネットワーク サービス オブジェクトをネットワーク サービス オブジェクト グループに追加する例を示します。

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

関連コマンド

コマンド	説明
clear object-group	オブジェクトグループのヒットカウントをクリアします。
object-group network-service	ネットワーク サービス オブジェクト グループを定義します。
show object-group network-service	ネットワークサービス オブジェクトとそれぞれのヒットカウントを表示します。

nis address

DHCPv6 サーバーの設定時にネットワーク インフォメーション サービス（NIS）アドレスをステートレスアドレス自動設定（SLAAC）クライアントに提供するには、IPv6 DHCP プール コンフィギュレーション モードで **nis address** コマンドを使用します。NIS サーバーを削除するには、このコマンドの **no** 形式を使用します。

nis address *nis_ipv6_address*
no nis address *nis_ipv6_address*

構文の説明

nis_ipv6_address	NIS の IPv6 アドレスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、NIS アドレスを含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
nis address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答でSLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答でSLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答でSLAAC クライアントに提供される SNTP アドレスを設定します。

nis domain-name

DHCPv6 サーバーの設定時にネットワーク インフォメーション サービス（NIS）ドメイン名をステートレスアドレス自動設定（SLAAC）クライアントに提供するには、IPv6 DHCP プール コンフィギュレーション モードで **nis domain-name** コマンドを使用します。NIS ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

nis domain-name *nis_domain_name*
no nis domain-name *nis_domain_name*

構文の説明

nis_domain_name	NIS ドメイン名を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、NIS ドメイン名を含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nis domain-name eng.example.com
nis address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nis domain-name it.example.com
nis address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

nisp address

DHCPv6 サーバーの設定時にネットワーク インフォメーション サービス プラス（NIS+）サーバーの IP アドレスをステートレスアドレス自動設定（SLAAC）クライアントに提供するには、IPv6 DHCP プール コンフィギュレーション モードで **nisp address** コマンドを使用します。NIS+ サーバーを削除するには、このコマンドの **no** 形式を使用します。

nisp address *nisp_ipv6_address*
no nisp address *nisp_ipv6_address*

構文の説明

nisp_ipv6_address	NIS+ サーバーの IPv6 アドレスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、NIS+ サーバーを含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答でSLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答でSLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答でSLAAC クライアントに提供される SNTP アドレスを設定します。

nisp domain-name

DHCPv6 サーバーの設定時にネットワーク インフォメーション サービス プラス（NIS+）ドメイン名をステートレスアドレス自動設定（SLAAC）クライアントに提供するには、IPv6 DHCP プール コンフィギュレーション モードで **nisp domain-name** コマンドを使用します。NIS+ ドメイン名を削除するには、このコマンドの **no** 形式を使用します。

nisp domain-name *nisp_domain_name*
no nisp domain-name *nisp_domain_name*

構文の説明

nisp_domain_name	NIS+ ドメイン名を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 DHCP プール コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

使用上のガイドライン

プレフィックス委任機能とともに SLAAC を使用しているクライアントの場合は、クライアントが情報要求（IR）パケットを ASA に送信したときに、NIS+ ドメイン名を含め、**ipv6 dhcp pool** 内の情報を提供するように ASA を設定できます。ASA は、IR パケットを受け取るだけで、クライアントにアドレスを割り当てません。DHCPv6 ステートレスサーバーを設定するには、**ipv6 dhcp server** コマンドを使用します。サーバーを有効にする場合は、**ipv6 dhcp pool** 名を指定します。

プレフィックス委任を設定するには、**ipv6 dhcp client pd** コマンドを使用します。

この機能は、クラスタリングではサポートされていません。

例

次に、2 つの IPv6 DHCP プールを作成して、2 つのインターフェイスで DHCPv6 サーバーを有効にする例を示します。

```
ipv6 dhcp pool Eng-Pool
domain-name eng.example.com
dns-server 2001:DB8:1::1
nisp domain-name eng.example.com
nisp address 2001:DB8:1::2
ipv6 dhcp pool IT-Pool
domain-name it.example.com
dns-server 2001:DB8:1::1
nisp domain-name it.example.com
nisp address 2001:DB8:1::2
interface gigabitethernet 0/0
ipv6 address dhcp setroute default
ipv6 dhcp client pd Outside-Prefix
interface gigabitethernet 0/1
ipv6 address Outside-Prefix ::1:0:0:0:1/64
ipv6 dhcp server Eng-Pool
ipv6 nd other-config-flag
interface gigabitethernet 0/2
ipv6 address Outside-Prefix ::2:0:0:0:1/64
ipv6 dhcp server IT-Pool
ipv6 nd other-config-flag
```

関連コマンド

コマンド	説明
clear ipv6 dhcp statistics	DHCPv6 統計情報をクリアします。
domain-name	IR メッセージへの応答で SLAAC クライアントに提供されるドメイン名を設定します。
dns-server	IR メッセージへの応答で SLAAC クライアントに提供される DNS サーバーを設定します。
import	ASA がプレフィックス委任クライアントインターフェイスで DHCPv6 サーバーから取得した 1 つ以上のパラメータを使用し、その後、IR メッセージへの応答でそれらを SLAAC クライアントに提供します。
ipv6 address	IPv6 を有効にし、インターフェイスに IPv6 アドレスを設定します。
ipv6 address dhcp	インターフェイスの DHCPv6 を使用してアドレスを取得します。
ipv6 dhcp client pd	委任されたプレフィックスを使用して、インターフェイスのアドレスを設定します。
ipv6 dhcp client pd hint	受信を希望する委任されたプレフィックスについて 1 つ以上のヒントを提供します。
ipv6 dhcp pool	DHCPv6 ステートレス サーバーを使用して、特定のインターフェイスで SLAAC クライアントに提供する情報を含むプールを作成します。
ipv6 dhcp server	DHCPv6 ステートレス サーバーを有効にします。

コマンド	説明
network	サーバーから受信した委任されたプレフィックスをアドバタイズするように BGP を設定します。
nis address	IR メッセージへの応答で SLAAC クライアントに提供される NIS アドレスを設定します。
nis domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NIS ドメイン名を設定します。
nisp address	IR メッセージへの応答で SLAAC クライアントに提供される NISP アドレスを設定します。
nisp domain-name	IR メッセージへの応答で SLAAC クライアントに提供される NISP ドメイン名を設定します。
show bgp ipv6 unicast	IPv6 BGP ルーティング テーブルのエントリを表示します。
show ipv6 dhcp	DHCPv6 情報を表示します。
show ipv6 general-prefix	DHCPv6 プレフィックス委任クライアントによって獲得されたすべてのプレフィックスと、そのプレフィックスの他のプロセスへの ASA 配布を表示します。
sip address	IR メッセージへの応答で SLAAC クライアントに提供される SIP アドレスを設定します。
sip domain-name	IR メッセージへの応答で SLAAC クライアントに提供される SIP ドメイン名を設定します。
sntp address	IR メッセージへの応答で SLAAC クライアントに提供される SNTP アドレスを設定します。

nop

IP オプションインスペクションが設定されたパケットヘッダーで No Operation IP オプションが発生したときに実行するアクションを定義するには、パラメータ コンフィギュレーション モードで **nop** 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。

nop action { **allow | clear** }
no nop action { **allow | clear** }

構文の説明

allow	No Operation IP オプションを含むパケットを許可します。
clear	No Operation オプションをパケット ヘッダーから削除してから、パケットを許可します。

コマンド デフォルト

デフォルトでは、IP オプション インスペクションは、No Operation IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用すると、デフォルト値を変更できます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプションインスペクションを設定して、特定の IP オプションを持つどの IP パケットが ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

IP ヘッダーの Options フィールドには、オプションを 0 個、1 個、またはそれ以上含めることができ、これがフィールド変数全体の長さになります。ただし、IP ヘッダーは 32 ビットの倍

数である必要があります。すべてのオプションのビット数が 32 ビットの倍数でない場合は、オプションが 32 ビット境界に合うように、No Operation（NOP）または IP オプション 1 が「内部パディング」として使用されます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

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。

nsf cisco

Open Shortest Path First（OSPF）を実行している ASA で Cisco ノンストップ フォワーディング（NSF）動作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 nsf cisco コマンドを使用します。デフォルトに戻るには、no 形式のコマンドを使用します。

nsf cisco［ **enforce global** ］
no nsf cisco［ **enforce global** ］

構文の説明

enforce global	（オプション）NSF の再起動時にいずれかのインターフェイスで NSF 認識でないネイバー ネットワーキング デバイスが検出された場合に、すべてのインターフェイスで再起動をキャンセルします。

コマンド デフォルト

Cisco NSF グレースフル リスタートはデフォルトではディセーブルになります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、OSPF ルータで Cisco NSF がイネーブルになります。ルータで NSF がイネーブルになっている場合、ルータは NSF 対応であり、リスタート モードで動作します。

ルータが NSF グレースフル リスタートを実行するネイバーとしか連携しないと想定される場合、隣接するルータで NSF をサポートするシスコ ソフトウェア リリースが実行されている必要がありますが、ルータで NSF が設定されている必要はありません。NSF をサポートするシスコ ソフトウェア リリースを実行している場合、ルータは NSF 認識です。

デフォルトでは、隣接する NSF 認識ルータは、グレースフル リスタート時に NSF ヘルパー モードで動作します。

NSF グレースフル リスタートの実行時にネットワーク インターフェイスで NSF 認識でないネイバーが検出された場合、そのインターフェイスでのみ再起動が中止され、他のインターフェイスではグレースフル リスタートが続行されます。再起動時に NSF 認識でないネイバーが検

出された場合に OSPF プロセス全体で再起動をキャンセルするには、enforce global キーワードを指定してこのコマンドを設定します。

（注） ネイバーとの隣接関係のリセットが任意のインターフェイスで検出された場合、または、OSPF インターフェイスがダウンした場合も、プロセス全体でNSFの再起動がキャンセルされます。

例

次に、enforce global オプションを指定して Cisco NSF グレースフル リスタートをイネーブルにする例を示します。

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# cisco nsf enforce global
```

関連コマンド

コマンド	説明
nsf cisco helper	ASA で Cisco NSF ヘルパー モードをイネーブルにします。
nsf ietf	IETF NSF をイネーブルにします。

nsf cisco helper

Open Shortest Path First（OSPF）を実行している ASA で Cisco ノンストップ フォワーディング（NSF）ヘルパー モード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 nsf cisco helper コマンドを使用します。Cisco NSF ヘルパー モードはデフォルトでイネーブルになり、ルータ コンフィギュレーション モードで no nsf cisco helper を発行することでディセーブルにできます。

nsf cisco helper
no nsf cisco helper

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。

コマンド デフォルト

Cisco NSF ヘルパー モードはデフォルトでイネーブルになります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

ASA で NSF をイネーブルにしている場合、この ASA は NSF 対応であると考えられ、グレースフル リスタート モードで動作します。OSPF ルータ プロセスは、ルート プロセッサ（RP）スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパー モードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。再起動するネイバーのノンストップ フォワーディングの復帰を ASA で支援しないようにするには、no nsf cisco helper コマンドを入力します。

例

次に、NSF ヘルパー モードをディセーブルにする例を示します。

```
ciscoasa
(config)# router ospf 24
```

```
ciscoasa
(config-router)# no nsf cisco helper
```

関連コマンド

コマンド	説明
nsf cisco	ASA で Cisco NSF をイネーブルにします。
nsf ietf	IETF NSF をイネーブルにします。

nsf ietf

OSPF を実行している ASA で Internet Engineering Task Force（IETF）NSF 動作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 nsf ietf コマンドを使用します。デフォルトに戻るには、no 形式のコマンドを使用します。

nsf ietf [**restart-interval** *seconds*]
no nsf ietf

構文の説明

restart-interval seconds	（オプション）グレースフル リスタートの間隔を秒数で指定します。有効な範囲は 1 ～ 1800 です。デフォルトは 120 です。 （注） 30 秒未満の再起動間隔では、グレースフル リスタートが中断します。

コマンド デフォルト

IETF NSF グレースフル リスタート モード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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、ASA で IETF NSF がイネーブルになります。ASA で NSF がイネーブルになっている場合、ASA は NSF 対応であり、リスタート モードで動作します。

ASA が NSF グレースフル リスタートを実行するネイバーとしか連携しないと想定される場合、隣接する ASA で NSF がサポートされている必要がありますが、ルータで NSF が設定されている必要はありません。NSF をサポートするアプリケーションを実行している場合、ASA は NSF 認識です。

例

次に、NSF ヘルパー モードをディセーブルにする例を示します。

```
ciscoasa
(config)# router ospf 24
```

```
ciscoasa
(config-router)# nsf ietf restart-interval 240
```

関連コマンド

コマンド	説明
nsf cisco	ASA で Cisco NSF をイネーブルにします。
nsf cisco helper	ASA で Cisco NSF ヘルパー モードをイネーブルにします。
nsf ietf helper	ASA で IETF NSF ヘルパー モードをイネーブルにします。

nsf ietf helper

IETF NSF ヘルパー モードはデフォルトでイネーブルになります。IETF NSF ヘルパー モードを明示的に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 nsf ietf helper コマンドを使用します。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。

必要に応じて、nsf ietf helper strict-lsa-checking コマンドを使用してリンクステート アドバタイズメント（LSA）の厳密なチェックを有効にできます。

nsf ietf helper [**strict-lsa-checking**]
no nsf ietf helper

構文の説明

strict-lsa-checking	（オプション）ヘルパー モードの厳密なリンクステート アドバタイズメント（LSA）をイネーブルにします。

コマンド デフォルト

IETF NSF ヘルパー モードはデフォルトでイネーブルになります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

ASA が NSF をイネーブルにしている場合、ASA は NSF 対応であると考えられ、グレースフル リスタート モードで動作します。OSPF プロセスは、ルート プロセッサ（RP）スイッチオーバーのため、ノンストップ フォワーディングの復帰を実行します。デフォルトでは、NSF 対応 ASA に隣接する ASA は NSF 認識となり、NSF ヘルパー モードで動作します。NSF 対応 ASA がグレースフル リスタートを実行しているときは、ヘルパーの ASA はそのノンストップ フォワーディングの復帰プロセスを支援します。再起動するネイバーのノンストップ フォワーディングの復帰を ASA が支援しないようにする場合は、no nsf ietf helper コマンドを入力します。

NSF 認識 ASA および NSF 対応 ASA の両方で厳密な LSA チェックをイネーブルにするには、nsf ietf helper strict-lsa-checking コマンドを入力します。ただし、IETF グレースフル リスタート プロセス時に ASA がヘルパー ASA になるまでは厳密な LSA チェックは有効になりません。

厳密な LSA チェックをイネーブルにすると、ヘルパー ASA は、LSA の変更があるために再起動 ASA にフラッディングされる場合、または、グレースフル リスタート プロセスが開始されたときに再起動 ASA の再送リスト内の LSA に変更があると検出された場合、再起動 ASA のプロセスの支援を終了します。

例

次に、厳密な LSA チェックを指定して IETF NSF ヘルパーをイネーブルにする例を示します。

```
ciscoasa
(config)# router ospf 24
ciscoasa
(config-router)# nsf ietf helper strict-lsa-checking
```

関連コマンド

コマンド	説明
nsf cisco	ASA で Cisco NSF をイネーブルにします。
nsf cisco helper	ASA で Cisco NSF ヘルパー モードをイネーブルにします。
nsf ietf	ASA で IETF NSF をイネーブルにします。

nt-auth-domain-controller

このサーバーの NT プライマリ ドメイン コントローラの名前を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **nt-auth-domain-controller** 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。

nt-auth-domain-controller *string*
no nt-auth-domain-controller

構文の説明

string このサーバーのプライマリ ドメイン コントローラの名前を最大 16 文字で指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、NT 認証 AAA サーバに対してのみ有効です。ホスト コンフィギュレーション モードを開始するには、まず **aaa-server host** コマンドを使用する必要があります。*string* 変数の名前は、そのサーバー自体の NT エントリに一致する必要があります。

例

次に、このサーバーの NT プライマリ ドメイン コントローラの名前を「primary1」に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol nt
ciscoasa
(configaaa-sesrver-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# nt-auth-domain-controller primary1
ciscoasa
(config-aaa-server-host)#
```

関連コマンド

コマンド	説明
aaa server host	ホスト固有の AAA サーバー パラメータを設定できるように、aaa サーバー ホスト コンフィギュレーション モードを開始します。
clear configure aaa-server	すべてのAAAコマンドステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

ntp authenticate

NTP サーバーによる認証を有効にするには、グローバル コンフィギュレーション モードで **ntp authenticate** コマンドを使用します。NTP 認証を無効にするには、このコマンドの **no** 形式を使用します。

ntp authenticate
no ntp authenticate

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• —	対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

認証を有効にしていて、NTP サーバーがパケットで正しい信頼できるキーを使用している場合（**ntp trusted-key** コマンドを参照）、ASA はその NTP サーバーとのみ通信します。サーバーキーも指定する必要があります（**ntp server key** コマンドを参照）。サーバーキーを指定しないと、ASA は、**ntp authenticate** コマンドが設定されている場合でも、認証なしでサーバーと通信します。また、ASA は認証キーを使用して NTP サーバーと同期します（**ntp authentication-key** コマンドを参照）。

例

次に、2 つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
```

```
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
```

関連コマンド

コマンド	説明
ntp authentication-key	NTP サーバーと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバーを指定します。
ntp trusted-key	NTP サーバーによる認証用パケットで使用するための、ASA のキー ID を指定します。
show ntp associations	ASA が関連付けられている NTP サーバーを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp authentication-key

NTP サーバーで認証するキーを設定するには、グローバル コンフィギュレーション モードで **ntp authentication-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。

ntp authentication-key *key_id* { **md5 | sha1 | sha256 | sha512 | cmac** } *key*
no ntp authentication-key *key_id* [{ **md5 | sha1 | sha256 | sha512 | cmac** } [**0|8**] *key*]

構文の説明

0	（任意）<key_value> がプレーン テキストであることを示します。0 または 8 が示されない場合、形式はプレーン テキストです。
8	（任意）<key_value> が暗号化されたテキストであることを示します。0 または 8 が示されない場合、形式はプレーン テキストです。
key	キー値を最大 32 文字のストリングとして設定します。
key_id	キー ID 1 ～ 4294967295 を識別します。この ID は、**ntp trusted-key** コマンドを使用して信頼できるキーとして指定する必要があります。
md5	認証アルゴリズムとして MD5 を指定します。
sha1	認証アルゴリズムとして SHA-1 を指定します。
sha256	認証アルゴリズムとして SHA-256 を指定します。
sha512	認証アルゴリズムとして SHA-512 を指定します。
cmac	認証アルゴリズムとして AES-CMAC を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• —	対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
9.13(1)	**sha1**、**sha256**、**sha512**、および **cmac** キーワードが追加されました。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドと **ntp server key** コマンドも設定する必要があります。

例

次に、2 つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp server	NTP サーバーを指定します。
ntp trusted-key	NTP サーバーによる認証用パケットで使用するための、ASA のキー ID を指定します。
show ntp associations	ASA が関連付けられている NTP サーバーを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp server

NTP サーバーを指定して、ASA 上の時間を設定するには、グローバル コンフィギュレーション モードで **ntp server** コマンドを使用します。サーバーを削除するには、このコマンドの **no** 形式を使用します。

ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]
no ntp server *ip_address* [**key** *key_id*] [**source** *interface_name*] [**prefer**]

構文の説明

ip_address	NTP サーバーの IPv4 または IPv6 IP アドレスを設定します。
key *key_id*	**ntp authenticate** コマンドを使用して認証を有効にした場合は、このサーバーの信頼できるキー ID を設定します。**ntp trusted-key** コマンドも参照してください。
source *interface_name*	ルーティング テーブルにデフォルトのインターフェイスを使用しない場合に、NTP パケットの発信インターフェイスを識別します。マルチ コンテキスト モードではシステムにインターフェイスが含まれないため、管理コンテキストに定義されているインターフェイス名を指定します。
prefer	精度に差がないサーバーが複数ある場合は、この NTP サーバーを優先サーバーとして設定します。NTP では、どのサーバーの精度が最も高いかを判断するためのアルゴリズムを使用し、そのサーバーに同期します。サーバーの精度に差がない場合は、**prefer** キーワードで使用するサーバーを指定します。ただし、優先サーバーよりも精度が大幅に高いサーバーがある場合、ASA は精度の高いそのサーバーを使用します。たとえば、ASA は優先サーバーであるストラタム 3 のサーバーよりもストラタム 2 のサーバーを使用します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、送信元インターフェイスを任意とするように変更されました。

リリース	変更内容
9.12(1)	IPv6 のサポートが追加されました。
9.14(1)	NTPv4 のサポートが追加されました。

使用上のガイドライン

NTP を使用して階層的なサーバ システムを実現し、ネットワーク システム間の時刻を正確に同期します。このような精度は、CRL の検証など正確なタイム スタンプを含む場合など、時刻が重要な操作で必要になります。複数の NTP サーバーを設定できます。ASA は、データ信頼度の尺度となる一番下のストラタムのサーバーを選択します。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にのみ NTP サーバーを設定します。

手動で設定した時刻はすべて、NTP サーバーから取得された時刻によって上書きされます。

ASA は NTPv4 をサポートします。

例

次に、2 つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp trusted-key 3
ciscoasa(config)# ntp trusted-key 4
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
ciscoasa(config)# ntp authentication-key 3 md5 aNiceKey3
ciscoasa(config)# ntp authentication-key 4 md5 aNiceKey4
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp server 2001:DB8::178 key 3
ciscoasa(config)# ntp server 2001:DB8::8945:ABCD key 4
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバーと同期するために、暗号化された認証キーを設定します。
ntp trusted-key	NTP サーバーによる認証用パケットで使用するための、ASA のキー ID を指定します。
show ntp associations	ASA が関連付けられている NTP サーバーを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

ntp trusted-key

NTP サーバーによる認証を必要とする信頼できるキーに認証キー ID 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 **ntp trusted-key** コマンドを使用します。信頼できる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。複数のサーバーで使用できるように複数の信頼できるキーを入力できます。

ntp trusted-key *key_id*
no ntp trusted-key *key_id*

構文の説明

key_id	キー ID 1 ～ 4294967295 を設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• —	対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

NTP 認証を使用するには、**ntp authenticate** コマンドと **ntp server key** コマンドも設定する必要があります。サーバーと同期するには、**ntp authentication-key** コマンドを使用して、キー ID の認証キーを設定します。

例

次に、2 つの NTP サーバを識別し、キー ID 1 および 2 に対する認証をイネーブルにする例を示します。

```
ciscoasa(config)# ntp server 10.1.1.1 key 1 prefer
ciscoasa(config)# ntp server 10.2.1.1 key 2
ciscoasa(config)# ntp authenticate
ciscoasa(config)# ntp trusted-key 1
ciscoasa(config)# ntp trusted-key 2
ciscoasa(config)# ntp authentication-key 1 md5
aNiceKey
ciscoasa(config)# ntp authentication-key 2 md5
aNiceKey2
```

関連コマンド

コマンド	説明
ntp authenticate	NTP 認証をイネーブルにします。
ntp authentication-key	NTP サーバーと同期するために、暗号化された認証キーを設定します。
ntp server	NTP サーバーを指定します。
show ntp associations	ASA が関連付けられている NTP サーバーを表示します。
show ntp status	NTP アソシエーションのステータスを表示します。

num-packets

SLA 動作中に送信される要求パケットの数を指定するには、SLA モニター プロトコル コンフィギュレーション モードで **num-packets** 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。

num-packets *number*
no num-packets *number*

構文の説明

number SLA 動作中に送信されるパケットの数。有効な値は、1 ～ 100 です。

（注） このコマンドで number 引数として指定したすべてのパケットが失われた場合は、追跡したルートで障害が発生しています。

コマンド デフォルト

エコー タイプの場合に送信されるデフォルトのパケット数は 1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
SLA モニター プロトコル コンフィギュレーション	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

パケット損失のために到達可能性情報が不正確になるのを防ぐには、送信されるデフォルトのパケット数を増やします。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。この例では、エコー要求パケットのペイロード サイズを 48 バイト、SLA 動作中に送信されるエコー要求の数を 5 に設定しています。5 つのパケットがすべて失われるまでは、追跡したルートは削除されません。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
```

```
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
request-data-size	要求パケットのペイロードのサイズを指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA動作をエコー応答時間プローブ動作として設定します。

nve

VXLAN カプセル化のためのネットワーク仮想化エンドポイント（NVE）インスタンスを作成するには、グローバル コンフィギュレーション モードで **nve** コマンドを使用します。NVE インスタンスを削除するには、このコマンドの **no** 形式を使用します。

nve 1
no nve 1

構文の説明

1	NVE インスタンスを指定します（常に 1）。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。この VTEP 送信元インターフェイスを指定する NVE インスタンスを 1 つ設定できます。すべての VNI インターフェイスはこの NVE インスタンスに関連付けられている必要があります。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、VNI 1 インターフェイスをそれに関連付ける例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# segment-id 1000
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
```

```
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# mcast-group 236.0.0.100
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN送信元インターフェイスがNVE専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ2転送テーブル（MACアドレステーブル）を表示します。
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、このNVEをVXLAN VTEPとして使用するVNI、ならびにこのNVEインターフェイスに関連付けられているピア VTEP IP アドレスを表示します。

コマンド	説明
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

nve-only

VXLAN 送信元インターフェイスが NVE のみであることを指定するには、インターフェイス コンフィギュレーション モードで **nve-only** コマンドを使用します。NVE のみという制限を削除するには、このコマンドの **no** 形式を使用します。

nve-only
[**cluster**]
no nve-only

構文の説明

構文の説明

cluster ASA 仮想 クラスタリングを構成する場合、クラスタ制御リンクの **nev-only cluster** を指定する必要があります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。
9.17(1)	ASA 仮想 クラスタリングをサポートするために、**cluster** キーワードが追加されました。

使用上のガイドライン

ASA ごと、またはセキュリティ コンテキストごとに 1 つの VTEP 送信元インターフェイスを設定できます。VTEP は、ネットワーク仮想化エンドポイント（NVE）として定義されます。VXLAN VTEP が現時点でサポートされている NVE です。

トランスペアレントモードでは、VTEP インターフェイスに関して **nve-only** を設定する必要があり、VTEP インターフェイスの IP アドレスを設定できます。このコマンドは、この設定によってトラフィックがこのインターフェイスの VXLAN および共通の管理トラフィックのみに制限されるルーテッド モードではオプションです。

ASA 仮想 クラスタリングの場合、クラスタ制御リンクに VXLAN インターフェイスを使用する必要があります。この場合、**nev-only cluster** を指定します。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、そのインターフェイスが NVE のみであることを指定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nve-only
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN送信元インターフェイスがNVE専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ2転送テーブル（MACアドレステーブル）を表示します。

コマンド	説明
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、このNVEをVXLAN VTEPとして使用するVNI、ならびにこのNVEインターフェイスに関連付けられているピアVTEP IPアドレスを表示します。
show vni vlan-mapping	VNIセグメントIDと、VLANインターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP送信元インターフェイスを指定します。
vtep-nve	VNIインターフェイスをVTEP送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDPポートを設定します。デフォルトでは、VTEP送信元インターフェイスはUDPポート4789へのVXLANトラフィックを受け入れます。

O

object-group

構成の最適化に使用できるオブジェクトグループを定義するには、グローバル コンフィギュレーション モードで **object-group** コマンドを使用します。構成からオブジェクト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。

object-group { **protocol | network | icmp-type | security | user | network-service** } *grp_name*
object-group service *grp_name* [**tcp | udp | tcp-udp**]

構文の説明

grp_name	オブジェクト グループ（1 ～ 64 文字）を指定します。文字、数字、および「_」、「-」、「.」の組み合わせが使用可能です。
icmp-type	（推奨されません。代わりに **service** を使用してください）。echo や echo-reply など ICMP タイプのグループを定義します。**object-group icmp-type** コマンドを入力後、**icmp-object** コマンドと **group-object** コマンドを使用して ICMP オブジェクトを追加します。
network	ホストまたはサブネットの IP アドレスのグループを定義します。**object-group network** コマンドを入力後、**network-object** コマンドと **group-object** コマンドを使用してネットワークオブジェクトを追加します。IPv4 アドレスと IPv6 アドレスが混在したグループを作成できます。 （注） 混合オブジェクト グループを NAT に使用することはできません。
network-service	オプションのサービス仕様でサブネットまたはドメイン名のグループを定義します。このコマンドを入力したら、**network-service-member** コマンドを使用してネットワーク サービス オブジェクトを追加するか、**domain** コマンドと **subnet** コマンドを使用してメンバーを直接追加します。
protocol	（推奨されません。代わりに **service** を使用してください）。TCP や UDP などプロトコルのグループを定義します。**object-group protocol** コマンドを入力後、**protocol-object** コマンドと **group-object** コマンドを使用してプロトコルオブジェクトを追加します。
security	Cisco TrustSec で使用するセキュリティ グループ オブジェクトを定義します。**object-group protocol** コマンドを入力後、**security-group** コマンドと **group-object** コマンドを使用してセキュリティ グループ オブジェクトを追加します。

service **[tcp | udp | tcp-udp**	プロトコル、ICMP タイプ、および TCP/UDP/SCTP ポートに基づいてサービスを定義します。 サービスの混合グループまたは SCTP ポートを定義する場合は、オブジェクトグループのプロトコルタイプを指定しないでください。**object-group service** コマンドを入力後、**service-object** コマンドと **group-object** コマンドを使用してサービスグループにサービスオブジェクトを追加します。オブジェクトに TCP ポートまたは UDP ポート（あるいはその両方）のリストしか含めない場合も、この方法を使用することを推奨します。 object-group service コマンドで **tcp**、**udp**、および **tcp-udp** キーワードを直接使用することは推奨されません。これらのキーワードを使用する代わりに、**service-object** コマンドで TCP ポートと UDP ポートを設定します。これらのキーワードを含めない場合は、**port-object** コマンドと **group-object** コマンドを使用してポートグループを追加します。
user	アイデンティティ ファイアウォールでアクセスを制御するために使用できるユーザーおよびユーザー グループを定義します。**object-group protocol** コマンドを入力後、**user**、**user-group**、および **group-object** コマンドを使用してユーザーおよびユーザー グループ オブジェクトを追加します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.4(2)	アイデンティティ ファイアウォールをサポートするために **user** キーワードのサポートが追加されました。
9.0(1)	IPv4 アドレスと IPv6 アドレスが混在したネットワーク オブジェクト グループを作成できるようになりました。 Cisco TrustSec をサポートするために **security** キーワードのサポートが追加されました。

リリース	変更内容
9.14	**icmp-type** キーワードは推奨しません。代わりに、**service** キーワードを使用してオブジェクトに **service icmp** を指定します。
9.17(1)	**network-service** キーワードが追加されました。

使用上のガイドライン

ホストやサービスなどのオブジェクトをグループ化し、そのオブジェクトグループを ACL（**access-list**）やNAT（**nat**）などの機能で使用できます。次に、ACL でネットワーク オブジェクト グループを使用する例を示します。

```
ciscoasa(config)# access-list access_list_name extended permit tcp any object-group
NWgroup1
```

コマンドを階層的にグループ化できます。つまり、オブジェクトグループを別のオブジェクトグループのメンバーにすることができます。

例

次に、**object-group network** コマンドを使用して、ネットワーク オブジェクト グループを作成する例を示します。

```
ciscoasa(config)# object-group network sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.eng.ftp.servcers
ciscoasa(config-network-object-group)# network-object host 172.23.56.194
ciscoasa(config-network-object-group)# network-object 192.1.1.0 255.255.255.224
ciscoasa(config-network-object-group)# exit
```

次に、**object-group network** コマンドを使用して、既存のオブジェクトグループを含むネットワーク オブジェクト グループを作成する例を示します。

```
ciscoasa(config)# object-group network sjc_ftp_servers
ciscoasa(config-network-object-group)# network-object host sjc.ftp.servers

ciscoasa(config-network-object-group)# network-object host 172.23.56.195
ciscoasa(config-network-object-group)# network-object 193.1.1.0 255.255.255.224

ciscoasa(config-network-object-group)# group-object sjc_eng_ftp_servers
ciscoasa(config-network-object-group)# exit
```

次に、**group-object** モードを使用して、事前に定義したオブジェクトで構成される新しいオブジェクトグループを作成し、それらのオブジェクトを ACL で使用する例を示します。

```
ciscoasa(config)# object-group network host_grp_1
ciscoasa(config-network-object-group)# network-object host 192.168.1.1
ciscoasa(config-network-object-group)# network-object host 192.168.1.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network host_grp_2
ciscoasa(config-network-object-group)# network-object host 172.23.56.1
ciscoasa(config-network-object-group)# network-object host 172.23.56.2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# object-group network all_hosts
ciscoasa(config-network-object-group)# group-object host_grp_1
```

```
ciscoasa(config-network-object-group)# group-object host_grp_2
ciscoasa(config-network-object-group)# exit
ciscoasa(config)# access-list grp_1 permit tcp object-group host_grp_1 any eq ftp
ciscoasa(config)#access-list grp_2 permit tcp object-group host_grp_2 any eq smtp
ciscoasa(config)#access-list all permit tcp object-group all_hosts any eq www
```

group-object コマンドを使用しない場合は、*host_grp_1* および *host_grp_2* にすでに定義されているすべての IP アドレスが含まれるように、*all_hosts* グループを定義する必要があります。**group-object** コマンドを使用すると、重複するホストの定義が削除されます。

次の例では、TCP と UDP の両方のサービスを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service CommonApps
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object tcp destination eq h323
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
```

次の例では、複数のサービス オブジェクトを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service SSH
ciscoasa(config-service-object)# service tcp destination eq ssh
ciscoasa(config)# object-group service EIGRP
ciscoasa(config-service-object)# service eigrp
ciscoasa(config)# object-group service HTTPS
ciscoasa(config-service-object)# service tcp source range 0 1024 destination eq https
ciscoasa(config)# object-group service Group1
ciscoasa(config-service-object-group)# group-object SSH
ciscoasa(config-service-object-group)# group-object EIGRP
ciscoasa(config-service-object-group)# group-object HTTPS
```

次の例では、指定したプロトコル、ポート、および ICMP の組み合わせを同じサービス オブジェクト グループに追加する方法を示します。

```
ciscoasa(config)# object-group service mixed
ciscoasa(config-service-object-group)# service-object tcp destination eq ftp
ciscoasa(config-service-object-group)# service-object tcp-udp destination eq www
ciscoasa(config-service-object-group)# service-object ipsec
ciscoasa(config-service-object-group)# service-object tcp destination eq domain
ciscoasa(config-service-object-group)# service-object icmp echo
```

次に、**service-object** サブコマンドを使用する例を示します。このサブコマンドは、TCP サービスおよび UDP サービスをグループ化する場合に便利です。

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host kqk.suu.dri.ixx
ciscoasa(config-network-object-group)# network-object host kqk.suu.pyl.gnl
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host 209.165.200.225
ciscoasa(config-network-object-group)# network-object host 209.165.200.230
ciscoasa(config-network-object-group)# network-object host 209.165.200.235
ciscoasa(config-network-object-group)# network-object host 209.165.200.240
ciscoasa(config)# object-group service usr_svc
ciscoasa(config-service-object-group)# service-object tcp destination eq www
```

```
ciscoasa(config-service-object-group)# service-object tcp destination eq https
ciscoasa(config-service-object-group)# service-object tcp destination eq pop3
ciscoasa(config-service-object-group)# service-object udp destination eq ntp
ciscoasa(config-service-object-group)# service-object udp destination eq domain
ciscoasa(config)# access-list acl extended permit object-group usr_svc object-group
locals object-group remote
```

次に、**object-group user** コマンドを使用して、ユーザー グループ オブジェクトを作成する例を示します。

```
ciscoasa(config)# object-group user sampleuser1-group
ciscoasa(config-object-group user)# description group members of sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-all
ciscoasa(config-object-group user)# user EXAMPLE\user2
ciscoasa(config-object-group user)# exit
ciscoasa(config)# object-group user sampleuser2-group
ciscoasa(config-object-group user)# description group members of sampleuser2-group
ciscoasa(config-object-group user)# group-object sampleuser1-group
ciscoasa(config-object-group user)# user-group EXAMPLE\\group.sampleusers-marketing
ciscoasa(config-object-group user)# user EXAMPLE\user3
```

（推奨されません。代わりにサービス オブジェクトを使用してください）次に、**object-group icmp-type** モードを使用して ICMP オブジェクトグループを作成する例を示します。

```
ciscoasa(config)# object-group icmp-type icmp-allowed
ciscoasa(config-icmp-object-group)# icmp-object echo
ciscoasa(config-icmp-object-group)# icmp-object time-exceeded
ciscoasa(config-icmp-object-group)# exit
```

（推奨されません。代わりにサービス オブジェクトを使用してください）次に、**object-group protocol** モードを使用してプロトコル オブジェクト グループを作成する例を示します。

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol-object-group)# protocol-object udp
ciscoasa(config-protocol-object-group)# protocol-object ipsec
ciscoasa(config-protocol-object-group)# exit
ciscoasa(config)# object-group protocol proto_grp_2
ciscoasa(config-protocol-object-group)# protocol-object tcp
ciscoasa(config-protocol-object-group)# group-object proto_grp_1
ciscoasa(config-protocol-object-group)# exit
```

（推奨されません。**tcp** キーワードを使用する代わりに **service-object** コマンドでポートを定義します）。次に、**object-group service** モードを使用して TCP ポートオブジェクトグループを作成する例を示します。

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service-object-group)# group-object eng_www_service
ciscoasa(config-service-object-group)# port-object eq ftp
ciscoasa(config-service-object-group)# port-object range 2000 2005
ciscoasa(config-service-object-group)# exit
```

次に、オブジェクト グループを使用して、アクセス リスト コンフィギュレーションを簡素化する例を示します。グループ化を使用しないとアクセス リストの設定には24行必要ですが、このグループ化により、1 行で設定できます。

```
ciscoasa(config)# object-group network remote
ciscoasa(config-network-object-group)# network-object host 10.1.1.15
ciscoasa(config-network-object-group)# network-object host 10.1.1.16
ciscoasa(config)# object-group network locals
ciscoasa(config-network-object-group)# network-object host
209.165.200.225
ciscoasa(config-network-object-group)# network-object host
209.165.200.230
ciscoasa(config-network-object-group)# network-object host
209.165.200.235
ciscoasa(config-network-object-group)# network-object host
209.165.200.240
ciscoasa(config)# object-group service eng_svc tcp
ciscoasa(config-service-object-group)# port-object eq www
ciscoasa(config-service-object-group)# port-object eq smtp
ciscoasa(config-service-object-group)# port-object range 25000 25100
ciscoasa(config)# access-list acl extended permit tcp object-group remote object-group
locals object-group eng_svc
```

（注） **show running-config access-list** コマンドは、オブジェクトグループ名を指定して設定されたアクセスリストを表示します。**show access-list** コマンドは、その情報に加え、グループを使用するアクセスリストエントリを、オブジェクトはグループ化せずに個々のエントリに展開して表示します。

次に、事前に定義されたネットワーク サービス オブジェクトを使用して、一連の SaaS アプリケーションを設定する例を示します。

```
object-group network-service SaaS_Applications
    description This group includes relevant 'Software as a Service' applications
    network-service-member "outlook 365"
    network-service-member webex
    network-service-member box
```

関連コマンド

コマンド	説明
clear configure object-group	すべての object group コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
port-object	サービス オブジェクト グループにポート オブジェクトを追加します。
security-group	セキュリティ グループ オブジェクト グループにセキュリティ グループを追加します。
show running-config object-group	現在のオブジェクト グループを表示します。

コマンド	説明
user	ユーザー グループ オブジェクトにユーザー名を追加します。
user-group	ユーザー グループ オブジェクトにユーザー グループ名を追加します。

object-group-search

ACL の最適化を有効にするには、グローバル コンフィギュレーション モードで **object-group-search** コマンドを使用します。ACL の最適化を無効にするには、このコマンドの **no** 形式を使用します。

object-group-search { **access-control | threshold** }
no object-group-search { **access-control | threshold** }

構文の説明

access-control	アクセス コントロール ルールのオブジェクト グループ検索を有効にします。
threshold	オブジェクト グループ検索処理の最大しきい値を有効にします。詳細については、「Usage Notes」を参照してください。

コマンド デフォルト

（9.18 より前）オブジェクトグループ検索はデフォルトで無効になっています。そのしきい値もデフォルトで無効になっています。

9.18以降、オブジェクトグループ検索は、新規展開のアクセス制御に対してデフォルトで有効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.12(1)	**threshold** キーワードが追加されました。このキーワードは、9.8、9.9、および 9.10 の暫定リリースでも追加されました。
9.18(1)	新規展開のアクセス制御のデフォルトが有効に変更されました。以前に有効にしていなかった場合は、アップグレード時に有効にする必要があります。

使用上のガイドライン

object-group-search コマンドは、着信方向のすべての ACL を最適化します。

オブジェクト グループ検索をイネーブルにすると、ルックアップのパフォーマンスは低下し、CPU使用率は増加しますが、アクセス ルールの検索に必要なメモリを抑えることができます。オブジェクト グループ検索をイネーブルにした場合、ASP テーブルのネットワークまたはサー

ビス オブジェクトを使用する ACL は拡張されませんが、それらのグループの定義に基づいて一致するアクセス ルールが検索されます。これは **show access-list** 出力に表示されます。

オブジェクト グループ検索は、しきい値の影響を受けます。接続ごとに、送信元と宛先の両方の IP アドレスがネットワーク オブジェクトと照合されます。発信元アドレスに一致するオブジェクトの数が、宛先アドレスと一致する数の 1 万倍を超えると接続が切断されます。このチェックは、パフォーマンスの低下を防止します。一致件数が膨大になることを防ぐためにルールを設定します。

リリース 9.12(1) 以降と暫定リリース 9.8(x) では、このしきい値はデフォルトで無効になっています。しきい値オプションが設定されているかどうか、および設定されている場合の現在の設定を確認するには、**show running-config all object-group-search** コマンドを使用します。

オブジェクト グループ検索を有効にした場合に、多数の機能が有効になっていると、アクティブな接続の数が増えて、アクセス グループのために大量の ACL が必要になり、処理中に接続が切断されたり、新しい接続を確立する際のパフォーマンスが低下したりすることがあります。パフォーマンスの低下は、トランザクションコミットを有効にしている場合でも発生する可能性があります（**asp rule-engine transactional-commit access-group**）。

（注） オブジェクト グループの検索は、ネットワーク オブジェクトとサービス オブジェクトのみで動作します。セキュリティ グループまたはユーザー オブジェクトでは動作しません。ACL にセキュリティ グループが含まれている場合は、この機能を有効にしないでください。ACL が非アクティブになったり、その他の予期しない動作となる可能性があります。

例

次に、**object-group-search** コマンドを使用して、ACL の最適化を有効にする例を示します。

```
ciscoasa(config)# object-group-search access-control
```

次に、**object-group-search** が有効になっていない場合の **show access-list** コマンドの出力例を示します。

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 9 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN object-group
BLK-LAN 0x724c956b
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
192.168.4.0 255.255.255.0 (hitcnt=10) 0x30fe29a6
  access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 192.168.4.0
 255.255.255.0 (hitcnt=4) 0xc6ef2338
   access-list KH-BLK-Tunnel line 1 extended permit ip 192.168.97.0 255.255.255.0
14.14.14.0 255.255.255.0 (hitcnt=2) 0xce8596ec
  access-list KH-BLK-Tunnel line 1 extended permit ip 13.13.13.0 255.255.255.0 14.14.14.0
 255.255.255.0 (hitcnt=0) 0x9a2f1c4d
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
 (hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
```

```
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
 0xa52a0761
```

次に、**object-group-search** が有効になっている場合の **show access-list** コマンドの出力例を示します。

```
ciscoasa# show access-list KH-BLK-Tunnel
access-list KH-BLK-Tunnel; 6 elements
access-list KH-BLK-Tunnel line 1 extended permit ip object-group KH-LAN(1) object-group
 BLK-LAN(2)(hitcount=16) 0x724c956b
access-list KH-BLK-Tunnel line 2 extended permit ospf interface pppoe1 host 87.139.87.200
 (hitcnt=0) 0xb62d5832
access-list KH-BLK-Tunnel line 3 extended permit ip interface pppoe1 any (hitcnt=0)
0xa2c9ed34
access-list KH-BLK-Tunnel line 4 extended permit ip host 1.1.1.1 any (hitcnt=0) 0xd06f7e6b
access-list KH-BLK-Tunnel line 5 extended deny ip 1.1.0.0 255.255.0.0 any (hitcnt=0)
0x9d979934
access-list KH-BLK-Tunnel line 6 extended permit ip 1.1.1.0 255.255.255.0 any (hitcnt=0)
 0xa52a0761
```

関連コマンド

コマンド	説明
clear config object-group search	オブジェクト グループ検索コンフィギュレーションをクリアします。
show object-group	オブジェクト グループがネットワーク オブジェクト グループ タイプの場合にヒット カウントを表示します。
show running-config object-group	現在のオブジェクト グループを表示します。
show running-config object-group-search	実行コンフィギュレーション内のオブジェクト グループ検索コンフィギュレーションを表示します。

object network

名前付きネットワークオブジェクトを設定するには、グローバル コンフィギュレーション モードで **object network** コマンドを使用します。コンフィギュレーションからオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

object network *name* [**rename** *new_obj_name*]
no object network *name*

構文の説明

name	ネットワーク オブジェクトの名前を指定します。名前は 1 ～ 64 文字で、文字、数字、およびアンダースコア、ハイフン、カンマ、スラッシュ、ピリオドの特殊文字を使用できます。オブジェクトおよびオブジェクト グループは、同じ名前スペースを共有します。
rename *new_obj_name*	（オプション）オブジェクトの名前を新しいオブジェクト名に変更します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
8.4(2)	完全修飾ドメイン名（FQDN）がサポートされるようになりました。**fqdn** コマンドを参照してください。

使用上のガイドライン

ネットワーク オブジェクトには、ホスト、ネットワーク、IP アドレス（IPv4 または IPv6）の範囲、または FQDN を含めることができます。このコマンドを入力した後、**host**、**fqdn**、**subnet**、または **range** コマンドを使用してオブジェクトにアドレスを 1 つ追加します。

また、**nat** コマンドを使用して、このネットワークオブジェクトに対して NAT ルールを有効にできます。特定のオブジェクトに対して 1 つの NAT ルールだけを定義できます。複数の NAT ルールを設定する場合は、**object network obj-10.10.10.1-01**、**object network obj-10.10.10.1-02** などのように、同じ IP アドレスを指定する複数のオブジェクトを作成する必要があります。

既存のネットワーク オブジェクトを異なるIPアドレスを使用して設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションに置き換わります。

例

次に、ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network OBJECT1
ciscoasa (config-network-object)# host 10.1.1.1
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
description	ネットワーク オブジェクトに説明を追加します。
fqdn	完全修飾ドメイン名のネットワーク オブジェクトを指定します。
host	ホスト ネットワーク オブジェクトを指定します。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。
object-group network	ネットワーク オブジェクト グループを作成します。
range	ネットワーク オブジェクトのアドレス範囲を指定します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。
subnet	サブネット ネットワーク オブジェクトを指定します。

object network-service

名前付きネットワーク サービス オブジェクトを設定するには、グローバル コンフィギュレーション モードで **object network-service** コマンドを使用します。コンフィギュレーションからオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

object network-service *name* [**dynamic**]
no object network-service *name*

構文の説明

dynamic	（任意）**dynamic** キーワードは、オブジェクトが実行コンフィギュレーションに保存されず、**show object** 出力にのみ表示されることを意味します。**dynamic** キーワードは、主に外部デバイスマネージャーが使用するためのものです。
name	名前は最大128文字で、スペースを含めることができます。スペースを含める場合、名前を二重引用符で囲む必要があります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.17(2)	このコマンドが追加されました。

使用上のガイドライン

ネットワーク サービス オブジェクトでは、単一のアプリケーションを定義します。また、サブネット仕様やより一般的には DNS ドメイン名のいずれかによってアプリケーションの場所を定義します。必要に応じて、プロトコルとポートを含めて、アプリケーションの範囲を絞り込めます。

ネットワーク サービス オブジェクトは、ネットワーク サービス グループ オブジェクトでのみ使用できます。アクセス制御リストエントリ（ACE）でネットワーク サービス オブジェクトを直接使用することはできません。

次のいずれかのコマンドを使用して、1 つ以上のアプリケーションの場所とオプションサービスをオブジェクトに追加します。場所を削除するには、このコマンドの**no**形式を使用します。これらのコマンドは、複数回入力できます。

- **domain** *domain_name* [*service*]：最大 253 文字の DNS 名。この名前は、完全修飾名（www.example.com など）または部分的な名前（example.com など）にすることができます。部分的な名前の場合、すべてのサブドメイン、つまりその名前を含むすべてのサーバー（www.example.com、www1.example.com、long.server.name.example.com など）に一致します。完全一致がある場合は、最も長い名前で接続が照合されます。ドメイン名は複数の IP アドレスに解決できます。
- **subnet** {*IPv4_address IPv4_mask* | *IPv6_address/IPv6_prefix*} [*service*]：ネットワークのアドレス。IPv4 サブネットの場合、10.0.0.0 255.0.0.0 のように、スペースの後ろにマスクを含めます。IPv6 の場合、2001:DB8:0:CD30::/60 のように、アドレスとプレフィックスを単一のユニット（スペースなし）として含めます。

これらのコマンドのサービス仕様は同じです。一致する接続の範囲を制限する場合にのみ、サービスを指定します。デフォルトでは、解決済みの IP アドレスへのすべての接続がオブジェクトと一致します。

protocol [*operator port*]

引数の説明

- *protocol* は、tcp、udp、ip など、接続で使用されるプロトコルです。プロトコルのリストを確認するには ? を使用します。
- （TCP/UDP のみ）*operator* は次のいずれかです。
  - **eq** は、指定したポート番号と等しいポートを意味します。
  - **lt** は、指定したポート番号より小さい任意のポートを意味します。
  - **gt** は、指定したポート番号より大きい任意のポートを意味します。
  - **range** は、指定した 2 つのポートの間の任意のポートを意味します。
- （TCP/UDP のみ）*port* は 1 ～ 65535 のポート番号か www などのニーモニックです。ニーモニックを確認するには ? を使用します。範囲の場合は 2 つのポートを指定する必要があります。最初のポートを 2 番目のポートよりも小さい番号にします。

例

次、ネットワーク サービス オブジェクトの例を示します。

```
object network-service outlook365
    description This defines Microsoft office365 'outlook' application.
  domain outlook.office.com tcp eq 443
object network-service webex
  domain webex.com tcp eq 443
object network-service partner
  subnet 10.34.56.0 255.255.255.0 ip
```

関連コマンド

コマンド	説明
app-id	オブジェクトのアプリケーション ID を指定します。
clear object	ネットワーク サービス オブジェクトとヒットカウントをクリアします。
description	オブジェクトに説明を追加します。
domain	オブジェクトのドメイン名を指定します。
object-group network-service	ネットワークサービス オブジェクト グループを作成します。
show object	ネットワーク サービス オブジェクトを表示します。
subnet	オブジェクトのサブネットを指定します。

object service

サービスオブジェクトを、そのオブジェクトを使用しているすべての構成に自動的に反映させるように設定するには、グローバル コンフィギュレーション モードで **object service** コマンドを使用します。オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

object service *name*［ **rename** *new_obj_name* ］
no object service *object name*［ **rename** *new_obj_name* ］

構文の説明

name	サービス オブジェクトの名前を指定します。名前には、1～64 文字で、文字、数字、およびアンダースコア、ハイフン、カンマ、ピリオドの特殊文字を使用できます。オブジェクト名は文字で始める必要があります。
rename *new_obj_name*	（オプション）オブジェクトの名前を新しいオブジェクト名に変更します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

サービス オブジェクトには、プロトコル、ICMP、ICMPv6、または TCP /UDP/SCTP のポートまたはポート範囲を含めることができます。このコマンドを入力した後、**service** コマンドを使用してオブジェクトにサービス仕様を 1 つ追加します。

既存のサービス オブジェクトを別のプロトコルおよび1つ以上の別のポートを使用して設定する場合、新しいコンフィギュレーションにより、既存のプロトコルおよび1つ以上のポートが新しい設定に置き換わります。

例

次に、サービス オブジェクトを作成する例を示します。

```
ciscoasa(config)# object service SERVOBJECT1
ciscoasa(config-service-object)# service tcp source eq www destination eq ssh
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
service	サービスオブジェクトのプロトコルとポートを設定します。

ocsp disable-nonce

ナンス拡張をディセーブルにするには、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 ocsp disable-nonce コマンドを使用します。ナンス拡張を再び有効にするには、このコマンドの **no** 形式を使用します。

ocsp disable-nonce
no ocsp disable-nonce

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。

コマンド デフォルト

デフォルトでは、OCSP 要求にナンス拡張が含まれています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するとき、OCSP 要求には OCSP ナンス拡張が含まれないため、ASA でチェックされません。デフォルトでは、OCSP 要求にナンス拡張が含まれています。ナンス拡張は、暗号化によって要求を応答にバインドし、リプレイ アタックを回避します。ただし、OCSP サーバーによっては、この一致するナンス拡張が含まれていない事前生成の応答が使用される場合があります。このようなサーバーでOCSPを使用するには、ナンス拡張をディセーブルにする必要があります。

例

次に、newtrust というトラストポイントのナンス拡張をディセーブルにする例を示します。

```
ciscoasa(config)# crypto ca trustpoint
 newtrust
ciscoasa(config-ca-trustpoint)# ocsp disable-nonce
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書きルールを設定します。
ocsp interface*nameif*	OCSP 失効チェックで使用できるインターフェイスを指定します。
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバーを指定します。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

ocsp interface

ASA が OCSP に到達するように送信元インターフェイスを設定するには、crypto ca trustpool コンフィギュレーションモードで **interface** *nameif* コマンドを使用します。 構成から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。

ocsp interface *nameif*
no ocsp interface *nameif*

構文の説明

interface *nameif*	ASA が OCSP サーバーに到達するために使用するインターフェイスを指定します。

コマンド デフォルト

このコマンドのデフォルトはありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、OCSP は管理インターフェイスエントリを含まないグローバル ルーティング テーブルを使用します。OCSP が管理インターフェイスの背後にある場合、OCSP 失効チェックは失敗します。このコマンドを使用すると、必要に応じて管理インターフェイスを含むインターフェイスを使用するように OCSP 失効チェックを設定できます。

例

次に、OCSP の送信元インターフェイスを設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint TP
ciscoasa(config-ca-trustpoint)# ocsp ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  interface      Configure Source interface
```

```
  url             OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp  interface
ciscoasa(config-ca-trustpoint)# ocsp interface ?

crypto-ca-trustpoint mode commands/options:
Current available interface(s):
  inside   Name of interface GigabitEthernet0/0.100
  inside1  Name of interface GigabitEthernet0/0.41
  mgmt     Name of interface Management0/0
  outside  Name of interface GigabitEthernet0/0.51
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt ?

crypto-ca-trustpoint mode commands/options:
  disable-nonce  Disable OCSP Nonce Extension
  url            OCSP server URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt  url
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url  ?

crypto-ca-trustpoint mode commands/options:
  LINE < 500 char  URL
ciscoasa(config-ca-trustpoint)# ocsp interface mgmt url http://lal-bagh:8888
```

関連コマンド

コマンド	説明
ocsp url	トラストポイントに関連付けられているすべての証明書をチェックするために使用する OCSP サーバーを指定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
revocation-check	失効チェックに使用する方法と各方法を試す順序を指定します。

ocsp url

クライアント証明書の AIA 拡張で指定されたサーバーではなく、ASA の OCSP サーバーを、トラストポイントに関連付けられたすべての証明書のチェックに使用するように設定するには、暗号 CA トラストポイント コンフィギュレーション モードで **ocsp url** コマンドを使用します。このサーバーを構成から削除するには、このコマンドの **no** 形式を使用します。

ocsp url *URL*
no ocsp url

構文の説明

URL OCSP サーバーの HTTP URL を指定します。

（注） ASA は、IPv4 OCSP URL のみをサポートします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は HTTP URL のみをサポートします。トラストポイントごとに URL を 1 つだけ指定できます。

ASA では 3 つの方法で OCSP サーバーの URL を定義できます。また、定義方法に従って次の順序で OCSP サーバーの使用が試行されます。

- **match certificate** コマンドを使用して設定した OCSP サーバー。
- **ocsp url** コマンドを使用して設定した OCSP サーバー。
- クライアント証明書の AIA フィールドに指定された OCSP サーバー。

match certificate コマンドまたは **ocsp url** コマンドで OCSP URL を設定しない場合、ASA はクライアント証明書の AIA 拡張に指定された OCSP サーバーを使用します。証明書に AIA 拡張がない場合、失効ステータスのチェックは失敗します。

例

次に、URL http://10.1.124.22 で OCSP サーバーを設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint
 newtrust
ciscoasa(config-ca-trustpoint)# ocsp url http://10.1.124.22
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。
match certificate	OCSP 上書きルールを設定します。
ocsp disable-nonce	OCSP 要求のナンス拡張をディセーブルにします。
ocsp interface*nameif*	OCSP 失効チェックで使用できるインターフェイスを指定します。
revocation-check	失効確認に使用する方法、および確認を行う順序を指定します。

onscreen-keyboard（廃止）

ログイン/パスワード要件とともにオンスクリーンキーボードをログインペインまたはすべてのペインに挿入するには、webvpn モードで **onscreen-keyboard** コマンドを使用します。以前に設定したオンスクリーンキーボ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。

onscreen-keyboard { **logon** | **all** }
no onscreen-keyboard [**logon** | **all**]

構文の説明

logon	ログイン ペインのオンスクリーン キーボードを挿入します。
all	ログイン/パスワードの要件とともに、ログイン ペインおよび他のすべてのペインのオンスクリーン キーボードを挿入します。

コマンド デフォルト

オンスクリーン キーボードはありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

オンスクリーン キーボードを使用すると、キーストロークなしでユーザー クレデンシャルを入力できます。

例

次に、ログイン ページのオンスクリーン キーボードをイネーブルにする例を示します。

```
ciscoasa
(config)#
webvpn
ciscoasa
(config-webvpn)#
```

```
 onscreen-keyboard logon
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
webvpn	webvpn モードを開始し、クライアントレス SSLVPN 接続の属性を設定できるようにします。

ospf authentication

OSPF 認証の使用を有効にするには、インターフェイス コンフィギュレーション モードで **ospf authentication** コマンドを使用します。デフォルトの認証状態に戻すには、このコマンドの **no** 形式を使用します。

ospf authentication { **key-chain key-chain-name** | **message-digest** | **null** }
no ospf authentication

構文の説明

key-chain *key-chain-name*	（任意）認証に使用するキー チェーンを指定します。key-name 引数には最大 63 文字の英数字を指定できます。
message-digest	（任意）OSPF メッセージ ダイジェスト認証を使用することを指定します。
null	（任意）OSPF 認証を使用しないことを指定します。

コマンド デフォルト

デフォルトでは、OSPF 認証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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.12(1)	OSPF 認証のローテーション キーをサポートするためにキー チェーン機能が追加されました。

使用上のガイドライン

ospf authentication コマンドを使用する前に、**ospf authentication-key** コマンドを使用してインターフェイスのパスワードを設定します。**message-digest** キーワードを使用する場合は、**ospf message-digest-key** コマンドを使用して、インターフェイスのメッセージダイジェストキーを設定します。

下位互換性を確保するため、エリアの認証タイプは引き続きサポートされます。インターフェイスの認証タイプを指定しないと、エリアの認証タイプが使用されます（エリアのデフォルトはヌル認証です）。

このコマンドをオプションなしで使用すると、簡易パスワード認証がイネーブルになります。

例

次に、選択したインターフェイスで OSPF の簡易パスワード認証をイネーブルにする例を示します。

```
ciscoasa(config-if)# ospf authentication
ciscoasa(config-if)#
```

次に、選択したインターフェイスで OSPF のキー チェーン パスワード認証を有効にする例を示します。

```
ciscoasa(config)# interface gigabitEthernet 0/0
ciscoasa(config-if)# ospf authentication key-chain CHAIN-INT-OSPFKEYS
```

関連コマンド

コマンド	説明
ospf **authentication-key**	ネイバー ルーティング デバイスで使用されるパスワードを指定します。
ospf message-digest-key	MD5 認証をイネーブルにし、MD5 キーを指定します。

ospf authentication-key

ネイバー ルーティング デバイスで使用されるパスワードを指定するには、インターフェイス コンフィギュレーション モードで **ospf authentication-key** コマンドを使用します。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。

ospf authentication-key [**0** | **8** } *password*
no ospf authentication-key

構文の説明

0	暗号化されていないパスワードが後に続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。
password	ネイバー ルーティング デバイスで使用される OSPF 認証パスワードを割り当てます。パスワードは、9 文字未満にする必要があります。2 文字間にブランクを含めることができます。パスワードの先頭または末尾のブランクは無視されます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドが作成するパスワードは、ルーティング プロトコル パケットの送信時に、OSPF ヘッダーに直接挿入されるキーとして使用されます。各ネットワークにはインターフェイスごとに個別のパスワードを割り当てることができます。OSPF 情報を交換するには、同じネットワーク上のすべての隣接ルータが同じパスワードを持っている必要があります。

例

次に、OSPF 認証のパスワードを指定する例を示します。

```
ciscoasa(config-if)# ospf authentication-key 8
yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

関連コマンド

コマンド	説明
area authentication	指定したエリアの OSPF 認証をイネーブルにします。
ospf authentication	OSPF 認証の使用をイネーブルにします。

ospf cost

インターフェイス経由でパケットを送信するコストを指定するには、インターフェイス コンフィギュレーション モードで **ospf cost** コマンドを使用します。インターフェイスコストをデフォルト値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。

ospf cost *interface_cost*
no ospf cost

構文の説明

interface_cost インターフェイス経由でパケットを送信するコスト（リンクステート メトリック）。これは、符号なし整数値 0 ～ 65535 です。0 はインターフェイスに直接接続されているネットワークを表し、インターフェイス帯域幅が大きくなるほど、そのインターフェイス経由のパケット送信に伴うコストは低くなります。つまり、コストの値が大きければインターフェイス帯域幅が小さく、コストの値が小さければインターフェイス帯域幅が大きいということになります。

ASA での OSPF インターフェイスのデフォルトのコストは 10 です。このデフォルトは、Cisco IOS ソフトウェアとは異なります。Cisco IOS ソフトウェアの場合、デフォルトのコストはファスト イーサネットおよびギガビット イーサネットでは 1、10BaseT では 10 です。ネットワークで ECMP を使用している場合には、このことを考慮に入れることが重要です。

コマンド デフォルト

デフォルトの *interface_cost* は、10 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ospf cost コマンドを使用すると、インターフェイスでパケットを送信するコストを明示的に指定できます。*interface_cost* パラメータは、符号なし整数値 0 ～ 65535 です。

no ospf cost コマンドを使用すると、パスコストをデフォルト値にリセットできます。

例

次に、選択したインターフェイスでパケットを送信するコストを指定する例を示します。

```
ciscoasa(config-if)# ospf cost 4
```

関連コマンド

コマンド	説明
show running-config interface	指定したインターフェイスの設定を表示します。

ospf database-filter

同期およびフラッディング時に OSPF インターフェイスへの発信 LSA をすべてフィルタリングするには、インターフェイス コンフィギュレーション モードで **ospf database-filter** コマンドを使用します。LSA を復元するには、このコマンドの **no** 形式を使用します。

ospf database-filter all out
no ospf database-filter all out

構文の説明

all	OSPF インターフェイスへの発信 LSA をすべてフィルタリングします。
out	

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ospf database-filter コマンドは、OSPF インターフェイスへの発信 LSA をフィルタリングします。**no ospf database-filter all out** コマンドは、インターフェイスへの LSA の転送を復元します。

例

次に、**ospf database-filter** コマンドを使用して、発信 LSA をフィルタリングする例を示します。

```
ciscoasa(config-if)# ospf database-filter all out
```

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情報を表示します。

ospf dead-interval

ネイバーがルータのダウンを宣言するまでの間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf dead-interval** 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。

ospf dead-interval { *seconds* **minimal** | **hello-multiplier** *multiplier* }
no ospf dead-interval

構文の説明

seconds	hello パケットが確認されない時間の長さ。*seconds* のデフォルトは、**ospf hello-interval** コマンドで設定された間隔（1 ～ 65535）の 4 倍です。
minimal	デッドインターバルを 1 秒に設定します。このキーワードを使用するには、キーワード hello-multiplier と引数 multiplier も設定する必要があります。
hello-multiplier *multiplier*	1 秒間に送信する hello パケットの個数を表す 3 ～ 20 の範囲の整数値。

コマンド デフォルト

seconds のデフォルト値は、**ospf hello-interval** コマンドで設定された間隔の 4 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。
9.2(1)	fast hello パケットのサポートが追加されました。

使用上のガイドライン

ospf dead-interval コマンドを使用すると、ネイバーがルータのダウンを宣言するまでのデッド間隔（no hello パケットが確認されない時間の長さ）を設定できます。*seconds* 引数にはデッド

間隔を指定し、その値はネットワーク上のすべてのノードで同じである必要があります。*seconds* のデフォルトは、**ospf hello-interval** コマンドで設定された間隔（1 ～ 65535）の 4 倍です。

no ospf dead-interval コマンドを使用すると、デフォルトの間隔値に戻ります。

デッドインターバルは、OSPF helloパケットでアドバタイズされます。この値は、特定のネットワーク上の全ネットワーキング デバイスに対して同じにする必要があります。

小さいデッドインターバル（秒）を指定すると、ネイバーのダウンがより早く検出され、収束効率が高まりますが、ルーティングが不安定になる可能性があります。

fast hello パケットに対する OSPF のサポート

キーワード minimal とキーワード hello-multiplier を引数 multiplier とともに指定することで、OSPF fast hello パケットがイネーブルになります。キーワード minimal は、デッド インターバルを 1 秒に設定し、hello-multiplier の値は、その 1 秒間に送信される hello パケットの数を設定します。これにより、1 秒未満の「fast（高速な）」hello パケットの送信が可能になります。

インターフェイスで fast hello パケットが設定されている場合、このインターフェイスから送出される hello パケットでアドバタイズされる Hello インターバルは 0 に設定されます。このインターフェイス経由で受信した hello パケットの Hello インターバルは無視されます。

dead 間隔は、1 つのセグメント上で一貫している必要があり、1 秒に設定するか（fast hello パケットの場合）、他の任意の値を設定します。dead 間隔内に少なくとも 1 つの hello パケットが送信される限り、hello multiplier がセグメント全体で同じである必要はありません。

デッド インターバルと fast hello 間隔を確認するには、show ospf interface コマンドを使用します。

例

次の例では、minimal キーワードおよび hello-multiplier キーワードと値を指定することにより、fast hello パケットに対する OSPF のサポートがイネーブルになっています。multiplier キーワードが 5 に設定されているため、hello パケットが毎秒 5 回送信されます。

```
ciscoasa(config-if)# ospf dead-interval minimal hello-multiplier 5
```

関連コマンド

コマンド	説明
ospf hello-interval	インターフェイス上での hello パケットの送信間隔を指定します。
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf hello-interval

インターフェイス上で送信される hello パケットの間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf hello-interval** コマンドを使用します。hello 間隔を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。

ospf hello-interval *seconds*
no ospf hello-interval

構文の説明

seconds	インターフェイス上で送信される hello パケット間の間隔を指定します。有効な値は 1 ～ 65535 秒です。

コマンド デフォルト

hello-interval *seconds* のデフォルト値は 10 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

この値は、hello パケットでアドバタイズされます。hello 間隔を小さくするほど、トポロジの変更が速く検出されますが、ルーティング トラフィックの増加につながります。この値は、特定のネットワーク上のすべてのルータおよびアクセス サーバーで同じにする必要があります。

例

次に、OSPF hello 間隔を 5 秒に設定する例を示します。

```
ciscoasa(config-if)# ospf hello-interval 5
```

関連コマンド

コマンド	説明
ospf dead-interval	ネイバーがルータのダウンを宣言するまでの間隔を指定します。
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf message-digest-key

OSPF MD5 認証を有効にするには、インターフェイス コンフィギュレーション モードで **ospf message-digest-key** コマンドを使用します。MD5 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。

ospf message-digest-key *key-id* **md5** [**0** | **8**] *key*
no ospf message-digest-key

構文の説明

key-id	MD5 認証をイネーブルにし、認証キー ID 番号を数値で指定します。有効な値は、1 ～ 255 です。
md5 *key*	最大 16 バイトの英数字のパスワード。キーの文字間にスペースを含めることができます。キーの先頭または末尾のスペースは無視されます。MD5 認証は、通信の整合性を検証し、発信元を認証し、適時性をチェックします。
0	暗号化されていないパスワードが後に続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ospf message-digest-key コマンドを使用すると、MD5 認証をイネーブルにできます。コマンドの **no** 形式を使用すると、古い MD5 キーを削除できます。*key_id* は、認証キーの 1 ～ 255 の数値識別子です。*key* は、最大 16 バイトの英数字のパスワードです。MD5 は通信の整合性を確認し、発信元を認証して、適時性をチェックします。

例

次に、OSPF 認証の MD5 キーを指定する例を示します。

```
ciscoasa(config-if)# ospf message-digest-key 3 md5 8
yWIvi0qJAnGK5MRWQzrhIohkGP1wKb
```

関連コマンド

コマンド	説明
area authentication	OSPFエリア認証をイネーブルにします。
ospf authentication	OSPF認証の使用をイネーブルにします。

ospf mtu-ignore

受信データベースパケットでOSPF最大伝送ユニット（MTU）ミスマッチ検出を無効にするには、インターフェイス コンフィギュレーション モードで **ospf mtu-ignore** コマンドを使用します。MTU ミスマッチ検出を復元するには、このコマンドの **no** 形式を使用します。

ospf mtu-ignore
no ospf mtu-ignore

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。

コマンド デフォルト

デフォルトでは **ospf mtu-ignore** は有効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

OSPF は、ネイバーが共通インターフェイスで同じ MTU を使用しているかどうかをチェックします。このチェックは、ネイバーがデータベース記述子（DBD）パケットを交換するときに実行されます。DBDパケットの受信MTUが、着信インターフェイスに設定されているIPMTUよりも高い場合、OSPF 隣接関係は確立されません。**ospf mtu-ignore** コマンドは、受信 DBD パケットでOSPFMTUミスマッチ検出を無効にします。デフォルトでは有効になっています。

例

次に、**ospf mtu-ignore** コマンドを無効にする例を示します。

```
ciscoasa(config-if)# ospf mtu-ignore
```

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情報を表示します。

ospf network point-to-point non-broadcast

OSPF インターフェイスをポイントツーポイントのノンブロードキャスト ネットワークとして設定するには、インターフェイス コンフィギュレーション モードで **ospf network point-to-point non-broadcast** コマンドを使用します。構成からこのコマンドを削除するには、このコマンドの **no** 形式を使用します。

ospf network point-to-point non-broadcast
no ospf network point-to-point non-broadcast

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

ospf network point-to-point non-broadcast コマンドを使用して、VPNトンネルを介して OSPF ルートを送信できます。

インターフェイスをポイントツーポイントとして指定したときは、OSPF ネイバーを手動で設定する必要があります。ダイナミック探索は機能しません。OSPF ネイバーを手動で設定するには、ルータ コンフィギュレーション モードで **neighbor** コマンドを使用します。

インターフェイスをポイントツーポイントとして設定したときには、次の制約事項が適用されます。

- インターフェイスにはネイバーを 1 つだけ定義できます。
- クリプト ポイントを指すスタティック ルートを定義する必要があります。

- ネイバーを明示的に設定しない限り、インターフェイスは隣接を形成できません。
- トンネル経由の OSPF がインターフェイスで実行中である場合は、その同じインターフェイスでは上流のルータがある通常の OSPF を実行できません。
- OSPF 更新が VPN トンネルを通過できるように、OSPF ネイバーを指定する前に、クリプトマップをインターフェイスにバインドする必要があります。OSPF ネイバーを指定した後で暗号マップをインターフェイスにバインドする場合は、 **clear local-host all** コマンドを使用して OSPF 接続をクリアし、OSPF 隣接関係を VPN トンネル経由で確立できるようにします。

例

次に、選択したインターフェイスをポイントツーポイントの非ブロードキャストインターフェイスとして設定する例を示します。

```
ciscoasa(config-if)# ospf network point-to-point non-broadcast
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
neighbor	手動で設定した OSPF ネイバーを指定します。
show interface	インターフェイスのステータス情報を表示します。

ospf priority

OSPF ルータのプライオリティを変更するには、インターフェイス コンフィギュレーション モードで **ospf priority** コマンドを使用します。デフォルトのプライオリティに戻すには、このコマンドの **no** 形式を使用します。

ospf priority *number*
no ospf priority [*number*]

構文の説明

number	ルータのプライオリティを指定します。有効な値は、0 ～ 255 です。

コマンド デフォルト

number のデフォルト値は、1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

使用上のガイドライン

ネットワークにアタッチされている 2 つのルータがともに指定ルータになろうとした場合、ルータのプライオリティの高い方が優先されます。プライオリティが同じ場合、より高位のルータ ID を持つルータが優先されます。ルータのプライオリティがゼロに設定されているルータには、指定ルータまたはバックアップ指定ルータになる資格がありません。ルータのプライオリティは、マルチアクセス ネットワークへのインターフェイス専用に設定されます（つまり、ポイントツーポイント ネットワークへのインターフェイスには設定されません）。

マルチコンテキストモードでは、共有インターフェイスに 0 を指定して、デバイスが指定ルータにならないようにします。OSPFv2 インスタンスは、共有インターフェイス間で相互に隣接関係を形成できません。

例

次に、選択したインターフェイスで OSPF プライオリティを変更する例を示します。

```
ciscoasa(config-if)# ospf priority 4
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf retransmit-interval

インターフェイスに属する隣接のLSA再送信間隔を指定するには、インターフェイス コンフィギュレーション モードで **ospf retransmit-interval** 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。

ospf retransmit-interval [*seconds*]
no ospf retransmit-interval [*seconds*]

構文の説明

seconds インターフェイスに属する隣接ルータのLSA再送信間の時間を指定します。有効な値は、1 ～ 65535 秒です。

コマンド デフォルト

retransmit-interval *seconds* のデフォルト値は 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチコンテキストモードのサポートが追加されました。

使用上のガイドライン

ルータが自身のネイバーに LSA を送信する場合、ルータは確認応答メッセージを受信するまでその LSA を保持します。確認応答メッセージを受信しないと、ルータは LSA を再送信します。

このパラメータの設定値は控えめにする必要があります。そうしないと、不要な再送信が発生します。シリアル回線および仮想リンクの場合は、値を大きくする必要があります。

例

次に、LSA の再送信間隔を変更する例を示します。

```
ciscoasa(config-if)# ospf retransmit-interval 15
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

ospf transmit-delay

インターフェイス上でリンクステート更新パケットを送信するために必要な推定時間を設定するには、インターフェイス コンフィギュレーション モードで **ospf transmit-delay** 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。

ospf transmit-delay [*seconds*]
no ospf transmit-delay [*seconds*]

構文の説明

seconds インターフェイス上でリンクステート更新パケットを送信するために必要とされる時間を設定します。デフォルト値は 1 秒で、有効な値の範囲は 1 ～ 65535 秒です。

コマンド デフォルト

seconds のデフォルト値は、1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

更新パケット内の LSA には、送信前に、*seconds* 引数で指定した値によって増加された経過時間が格納されます。値は、インターフェイスの送信および伝播遅延を考慮して割り当てる必要があります。

リンクでの送信前に遅延が加算されていない場合、LSA がリンクを介して伝播する時間は考慮されません。この設定は、非常に低速のリンクでより重要な意味を持ちます。

例

次に、選択したインターフェイスの送信遅延を 3 秒に設定する例を示します。

```
ciscoasa(config-if)# ospf restransmit-delay 3
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
show ospf interface	OSPF に関連するインターフェイス情報を表示します。

otp expiration

ローカル認証局（CA）登録ページ用に発行されたワンタイムパスワード（OTP）の有効期間を時間単位で指定するには、CA サーバー コンフィギュレーション モードで **otp expiration** コマンドを使用します。期間をデフォルトの時間数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。

otp expiration *timeout*
no otp expiration

構文の説明

timeout 登録ページ用の OTP が期限切れになる前に、ユーザーがローカル CA から証明書を登録する必要がある期間を時間単位で指定します。有効な値の範囲は、1 ～ 720 時間（30 日）です。

コマンド デフォルト

デフォルトでは、証明書登録用の OTP の有効期限は 72 時間（3 日）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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

OTP の有効期限には、ユーザが CA サーバの登録ページにログインする必要がある時間数を指定します。ユーザーがログインし、証明書を登録すると、**enrollment retrieval** コマンドで指定された期間が開始されます。

（注） 登録インターフェイス ページで証明書を登録するためのユーザー OTP は、そのユーザーの発行済みの証明書とキーペアが含まれている PKCS12 ファイルをアンロックするためのパスワードとしても使用されます。

例

次に、登録ページ用の OTP が 24 時間適用されることを指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# otp expiration 24
ciscoasa
(config-ca-server)
#
```

次に、OTP 期間をデフォルトの 72 時間にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
)# no otp expiration
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンドセットを使用することで、ローカル CA を設定および管理できます。
enrollment-retrieval	登録されたユーザーが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。
show crypto ca server	認証局コンフィギュレーションを表示します。

output console

action コマンドの出力をコンソールに送るには、イベントマネージャアプレットコンフィギュレーション モードで **output console** コマンドを使用します。コンソールを出力先から削除するには、このコマンドの **no** 形式を使用します。

output console
no output console

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**action** コマンドの出力をコンソールに送信する場合に使用します。

例

次に、**action** コマンドの出力をコンソールに送信する例を示します。

```
ciscoasa(config-applet)# output console
```

関連コマンド

コマンド	説明
output file append	**action** コマンドの出力は単一のファイルに書き込まれますが、ファイルには毎回出力が追加されます。
output file new	**action** コマンドの出力は、呼び出された各アプレットの新しいファイルに送信されます。

コマンド	説明
output file overwrite	**action** コマンドの出力を単一のファイルに書き込みます。このファイルは毎回上書きされます。
output file rotate	ローテーションで使用する一連のファイルを作成します。
output none	**action** コマンドの出力を破棄します。

output file

指定したファイルに **action** コマンドの出力をリダイレクトするには、イベント マネージャ アプレット コンフィギュレーション モードで **output file** コマンドを使用します。指定したアクションを削除するには、このコマンドの **no** 形式を使用します。

output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]
no output file [**append** *filename* | **new** | **overwrite** *filename* | **rotate** *n*]

構文の説明

append *filename*	指定したファイル名に出力を追加していきます。これは、ASAに対してローカルのファイル名です。
new	eem-*applet*-*timestamp* .log という名前の新しい出力先ファイルを作成します。*applet* はイベント マネージャ アプレットの名前、*timestamp* は YYYYMMDD-hhmmss の形式のタイムスタンプです。
overwrite *filename*	指定したファイルに出力を書き込み、イベント マネージャ アプレットを起動するたびに出力を上書きします。
rotate *n*	eem-*applet*-*x* .log という名前の出力ファイルを作成します。*applet* はイベント マネージャ アプレットの名前、*x* はファイルの番号です。新しいファイルが書き込まれる場合、最も古いファイルが削除され、最初のファイルが書き込まれる前に後続のすべてのファイルに番号が再度割り振られます。最も新しいファイルが 0 で示され、最も古いファイルが最大数（*n*-1）で示されます。*n* 引数には、ローテーションの値を指定します。有効な値の範囲は 2 ～ 100 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

output file コマンドは、指定したファイルに **action** コマンドの出力をリダイレクトする場合に使用します。

例

次に、単一のファイルに出力を追加する例を示します。

```
ciscoasa(config-applet)# output file append examplefile1
```

次に、**action** コマンドの出力を新しいファイルに送信する例を示します。

```
ciscoasa(config-applet)# output file new
```

次に、単一のファイルに出力を上書きする例を示します。

```
ciscoasa(config-applet)# output file overwrite examplefile1
```

次に、ローテーションで使用する一連のファイルを作成する例を示します。

```
ciscoasa(config-applet)# output file rotate 50
```

関連コマンド

コマンド	説明
output console	**action** コマンドの出力をコンソールに送信します。
output none	**action** コマンドの出力を破棄します。

output none

action コマンドの出力を破棄するには、イベントマネージャアプレットコンフィギュレーション モードで **output none** コマンドを使用します。**action** コマンドの出力を保持するには、このコマンドの **no** 形式を使用します。

output none
no output none

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。

コマンド デフォルト

デフォルトでは、**action** コマンドの出力はすべて破棄されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
イベント マネージャ アプレット コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**action** コマンドの出力を破棄する場合に使用します。

例

次に、**action** コマンドの出力を破棄する例を示します。

```
ciscoasa(config-applet)# output none
```

関連コマンド

コマンド	説明
output console	**action** コマンドの出力をコンソールに送信します。
output file append	**action** コマンドの出力は単一のファイルに書き込まれますが、ファイルには毎回出力が追加されます。

コマンド	説明
output file new	**action** コマンドの出力は、呼び出された各アプレットの新しいファイルに送信されます。
output file overwrite	**action** コマンドの出力を単一のファイルに書き込みます。このファイルは毎回上書きされます。
output file rotate	ローテーションで使用する一連のファイルを作成します。

outstanding（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

認証されていない電子メールプロキシセッションの数を制限するには、適用可能な電子メールプロキシ コンフィギュレーション モードで **outstanding** コマンドを使用します。構成から属性を削除するには、このコマンドの **no** 形式を使用します。

outstanding { *number* }
no outstanding

構文の説明

number 認証されていないセッションを許可する数。範囲は 1 ～ 1000 です。

コマンド デフォルト

デフォルトは 20 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
pop3s	• 対応	—	• 対応	•	—
Imap4s	• 対応	—	• 対応	—	—
Smtps	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

認証されていないセッションを許可する数に制限がないコンフィギュレーションから属性を削除するには、このコマンドの no 形式を使用します。これは、電子メール ポートに対する DoS 攻撃も制限します。

電子メール プロキシ接続には、3 つの状態があります。

- **1.** 新規に電子メール接続が確立されると、「認証されていない」状態になります。

- **2.** この接続でユーザー名が提示されると、「認証中」状態になります。
- **3.** ASA が接続を認証すると、「認証済み」状態になります。

認証されていない状態の接続の数が設定済みの制限値を超えた場合、ASAは最も古い認証されていない接続を終了して、過負荷を回避します。認証済みの接続は終了しません。

例

次に、POP3S 電子メール プロキシの認証されていないセッションの制限を 12 に設定する例を示します。

```
ciscoasa
(config)#
 pop3s
ciscoasa(config-pop3s)
#
 outstanding 12
```

override-account-disable（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

AAA サーバーからの account-disabled インジケータを上書きするには、トンネルグループ一般属性コンフィギュレーション モードで **override-account-disable** コマンドを使用します。上書きを無効にするには、このコマンドの **no** 形式を使用します。

override-account-disable
no override-account-disable

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは、NT LDAP がある RADIUS や Kerberos など、「account-disabled」インジケータを返すサーバーに有効です。

IPsec RA および WebVPN トンネル グループにこの属性を設定できます。

例

次に、「testgroup」という WebVPN トンネル グループについて AAA サーバーからの「account-disabled」インジケータの上書きを許可する例を示します。

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

次に、「QAgroup」という IPsec リモート アクセス トンネル グループについて AAA サーバーからの「account-disabled」インジケータの上書きを許可する例を示します。

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# override-account-disable
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure tunnel-group	特定のトンネル グループのトンネル グループ データベースまたはコンフィギュレーションをクリアします。
tunnel-group general-attributes	トンネル グループ一般属性値を設定します。

override-svc-download

AnyConnect クライアントまたは SSL VPN クライアントをダウンロードするためのグループポリシーまたはユーザー名属性構成を上書きするように接続プロファイルを設定するには、トンネルグループ webvpn 属性コンフィギュレーション モードで **override-svc-download** 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するには、**no** 形式を使用します。

override-svc-download enable
no override-svc-download enable

コマンド デフォルト

デフォルトではディセーブルになっています。ASA は、クライアントをダウンロードするためのグループポリシーまたはユーザー名属性構成を上書きしません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

セキュリティアプライアンスは、**vpn-tunnel-protocol** コマンドによってグループポリシーまたはユーザー名属性でクライアントレスや SSL VPN が有効になっているかどうかに基づいて、リモートユーザーに対してクライアントレス接続、AnyConnect クライアント接続、または SSL VPN クライアント接続を許可します。**svc ask** コマンドは、クライアントをダウンロードするか、または WebVPN ホームページに戻るようにユーザーに要求して、クライアントのユーザーエクスペリエンスをさらに変更します。

ただし、特定のトンネル グループのもとでログインしているクライアントレス ユーザーが、ダウンロードの要求が期限切れになってクライアントレス SSL VPN ホームページが表示されるまで待たなくてもよいようにすることを推奨します。**override-svc-download** コマンドを使用すると、接続プロファイル レベルでこのようなユーザーに対する遅延を防止できます。このコマンドにより、接続プロファイル経由でログインするユーザーには、**vpn-tunnel-protocol** コマンドまたは **svc ask** コマンドの設定に関係なく、クライアントレス SSL VPN ホームページがただちに表示されるようになります。

例

次に、ユーザーが接続プロファイル *>engineering* のトンネルグループ webvpn 属性コンフィギュレーション モードを開始し、この接続プロファイルでクライアントのダウンロード要求に関するグループポリシーおよびユーザー名属性の設定を上書きする例を示します。

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# override-svc-download
```

関連コマンド

コマンド	説明
show webvpn svc	インストールされている SSL VPN クライアントに関する情報を表示します。
svc	特定のグループまたはユーザーに対して SSL VPN クライアントをイネーブルまたは必須にします。
svc image	リモート PC へのダウンロードのために ASA がキャッシュメモリで展開するクライアント パッケージ ファイルを指定します。

pa - pn

packet-tracer

packet-tracer コマンドを特権 EXEC モードで使用すると、ファイアウォールの現在の設定に対して 5 ～ 6 タプルのパケットを生成することができます。ここでは、わかりやすいように、ICMP、CP/UDP/SCTP、および IP の各パケットのモデリング別に packet-tracer の構文を示します。複数のパケットを再生し、 **pcap** キーワードを使用して完全なワークフローをトレースできます。

packet-tracer input *ifc_name* ［ **vlan-id** *vlan_id* ］**icmp** ［ **inline-tag** *tag* ］｛ *src_ip* ｜ **user** *username* ｜ **security-group** ｛ **name** *name* ｜ **tag** *tag* ｝ ｜ **fqdn** *fqdn_string* ｝ *icmp_value* ［ *icmp_code* ］ ［ *dmac* ］ ｛ *dst_ip* ｜ **security-group** ｛ **name** *name* ｜ **tag** *tag* ｝ ｜ **fqdn** *fqdn_string* ｝ ［ **detailed** ］ ［ **xml** ］

packet-tracer input *ifc_name* ［ **vlan-id** *vlan_id* ］**rawip** ［ **inline-tag** *tag* ］｛ *src_ip* ｜ **user** *username* ｜ **security-group** ｛ **name** *name* ｜ **tag** *tag* ｝ ｜ **fqdn** *fqdn_string* ｝ *protocol* ［ *dmac* ］ ｛ *dst_ip* ｜ **security-group** ｛ **name** *name* ｜ **tag** *tag* ｝ ｜ **fqdn** *fqdn_string* ｝ ［ **detailed** ］ ［ **xml** ］

packet-tracer input *ifc_name* ［ **vlan-id** *vlan_id* ］ ｛ **tcp** ｜ **udp** ｜ **sctp** ｝ ［ **inline-tag** *tag* ］｛ *src_ip* ｜ **user** *username* ｜ **security-group** ｛ **name** *name* ｜ **tag** *tag* ｝ ｜ **fqdn** *fqdn_string* ｝ *src_port* ［ *dmac* ］ ｛ *dst_ip* ｜ **security-group** ｛ **name** *name* ｜ **tag** *tag* ｝｜ **fqdn** *fqdn_string* ｝ *dst_port* ［ *options* ］ ［ **detailed** ］ ［ **xml** ］

packet-tracer input *ifc_name* **pcap** *pcap_filename* ［ **bypass-checks** ｜ **decrypted** ｜ **detailed** ｜ **persist** ｜ **transmit** ｜ **xml** ｜ **json** ｜ **force** ］

構文の説明

bypass-checks	（任意）シミュレートされたパケットのセキュリティチェックをバイパスします。
decrypted	（任意）シミュレートされたパケットを、復号された IPSec/SSL VPN と見なします。
detailed	（オプション）トレース結果の詳細な情報を表示します。
dmac	宛先 MAC アドレスを指定します。出力インターフェイスの選択肢を表示することで交換されたパケットの寿命に関する全体像を提供するとともに、宛先 MAC アドレスが不明であったことによるパケット ドロップも提供します。
dst_ip	パケット トレースの宛先アドレス（IPv4 または IPv6）を指定します。
dst_port	TCP/UDP/SCTP パケット トレースの宛先ポートを指定します。ポートによっては、**vxlan** および**geneve** 内部パケットなどの追加オプションがある場合があります。
fqdn *fqdn_string*	ホストの完全修飾ドメイン名を指定します。送信元と宛先のどちらの IP アドレスにも使用できます。IPv4 の FQDN のみがサポートされます。

force	既存の pcap トレースを削除し、新しい pcap ファイルを実行します。
icmp	使用するプロトコルとして ICMP を指定します。
icmp_type	ICMP パケット トレースの ICMP タイプを指定します。ICMPv6 パケット トレーサには必ず V6 タイプを使用してください。
icmp_code	ICMP パケット トレーサのタイプに対応する ICMP コードを指定します。ICMPv6 パケット トレーサには必ず V6 コードを使用してください。
input *ifc_name*	パケットの入力インターフェイスを指定します。
inline-tag *tag*	レイヤ 2 CMD ヘッダーに埋め込まれているセキュリティ グループ タグの値を指定します。有効な値の範囲は 0 ～ 65533 です。
json	（任意）トレース結果を JSON 形式で表示します。
pcap	pcap を入力として指定します。
pcap_filename	トレース用のパケットを含む pcap ファイル名。
protocol	raw IP パケット トレーシングのプロトコル番号（0 ～ 255）を指定します。
persist	（任意）長期間のトレースを有効にし、クラスタでのトレースも有効にします。
rawip	使用するプロトコルとして raw IP を指定します。
sctp	使用するプロトコルとして SCTP を指定します。
security-group {**name** *name* | **tag** *tag* }	TrustSec の IP-SGT ルックアップに基づいて送信元と宛先のセキュリティ グループを指定します。セキュリティ グループの名前またはタグ番号を指定できます。
src_port	TCP/UDP/SCTP パケット トレースの送信元ポートを指定します。
src_ip	パケット トレースの送信元アドレス（IPv4 または IPv6）を指定します。
tcp	使用するプロトコルとして TCP を指定します。
transmit	（任意）シミュレートされたパケットがデバイスから送信できるようにします。
type	ICMP パケット トレースの ICMP タイプを指定します。
udp	使用するプロトコルとして UDP を指定します。

user *username*	送信元 IP アドレスとしてユーザーを指定する場合に *domain\user* の形式でユーザーアイデンティティを指定します。ユーザーに対して最後にマッピングされたアドレス（複数ある場合）がトレースに使用されます。
vlan-id *vlan_id*	（オプション）フローの VLAN アイデンティティを指定します。有効範囲は 1 ～ 4096 です。
xml	（オプション）トレース結果を XML 形式で表示します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.4(2)	キーワードと引数のペアが 2 組追加されました（user *username* と fqdn *fqdn_string*）。いくつかのキーワードの名前と定義が変更されました。IPv6 送信元アドレスのサポートが追加されました。
9.0(1)	ユーザーアイデンティティのサポートが追加されました。IPv4 の完全修飾ドメイン名（FQDN）のみがサポートされます。
9.3(1)	キーワードと引数のペア **inline-tag** *tag* が追加され、レイヤ 2 CMD ヘッダーに埋め込まれているセキュリティ グループ タグの値がサポートされるようになりました。
9.4(1)	キーワードと引数のペアが 2 つ追加されました（**vlan-id** *vlan_id* と **vxlan-inner** *vxlan_inner_tag*）。
9.5(2)	sctp キーワードが追加されました。
9.7(1)	トランスペアレント ファイアウォール モードのサポート。宛先 MAC アドレスに新しいトレース モジュールが追加されました。

リリース	変更内容
9.9.(1)	永続的なトレースをクラスタリングするためのサポートが導入されました。この機能によって、クラスタ ユニットでパケットを追跡できます。新しいオプションの persist、bypass-checks、decrypted、transmit、id、および origin が追加されました。
9.14(1)	パケットトレーサの出力が強化され、パケットのルーティング中にパケットを許可/拒否する特定の理由を提供するようになりました。
9.17(1)	トレースの入力として pcap ファイルを使用できるように、packet-tracer コマンドが拡張されました。**geneve** のサポートも追加されました。

使用上のガイドライン

Capture コマンドによるパケットのキャプチャに加えて、ASA を介してパケットの寿命をトレースして、想定どおりに動作しているかどうかを確認できます。packet-tracer コマンドを使用すると、次の操作を実行できます。

- ネットワーク内にドロップするすべてのパケットをデバッグする。
- コンフィギュレーションが意図したとおりに機能しているかを確認する。
- パケットに適用可能なすべてのルール、およびルールが追加される原因となった CLI 行を表示する。
- データ パスのパケット変更をタイムラインで表示する。
- データ パスにトレーサ パケットを挿入する。
- ユーザー アイデンティティおよび FQDN に基づいて IPv4 アドレスまたは IPv6 アドレスを検索する。
- クラスタ ノード間でパケットをデバッグする。

packet-tracer コマンドは、パケットに関する詳細情報と、ASA によるパケットの処理方法を提供します。ファイアウォール管理者は、**packet-tracer** を使用して、セキュリティアプライアンスに仮想パケットを送信し、入口から出口へのフローを追跡できます。その途中で、フローおよびルート ルックアップ、ACL、プロトコル インスペクション、および NAT に対してパケットが評価されます。ユーティリティの能力は、送信元および宛先のアドレスと、プロトコルおよびポート情報を指定して実際のトラフィックをシミュレートする機能によってもたらされます。

オプションの **vlan-id** キーワードを使用すると、パケットトレーサが親インターフェイスに入り、その後、VLAN アイデンティティと一致するサブインターフェイスにリダイレクトされます。VLAN アイデンティティは、サブインターフェイス以外だけに使用可能なオプション エントリです。管理インターフェイスは例外です。ペアレント管理専用インターフェイスが持つことができるのは管理専用サブインターフェイスだけです。

宛先 MAC アドレスのルックアップを使用できます。

トランスペアレントファイアウォールモードでは、入力インターフェイスがVTEPの場合に、VLANに値を入力すると宛先MACアドレスはオプションで有効になります。一方、ブリッジグループメンバーインターフェイスでは、宛先MACアドレスは必須フィールドですが、vlan-idキーワードを入力した場合はオプションになります。

ルーテッドファイアウォールモードでは、入力インターフェイスがブリッジグループメンバーインターフェイスの場合、vlan-idキーワードとdmac引数はオプションです。

次の表に、トランスペアレントファイアウォールモードとルーテッドファイアウォールモードでのそれぞれのVLANアイデンティティと宛先MACアドレスのインターフェイス依存型の動作に関する詳しい情報を示します。

Transparent firewall mode：

インターフェイス	VLAN	宛先 MAC アドレス
管理	イネーブル（オプション）	無効
VTEP	イネーブル（オプション）	ディセーブルユーザーがVLANに値を入力すると、宛先 MAC アドレスはイネーブルになりますが、これはオプションです。
ブリッジ仮想インターフェイス（BVI）	イネーブル（オプション）	イネーブル（必須）ユーザーがVLANに値を入力した場合、宛先 MAC アドレスはオプションです。

Routed firewall mode：

インターフェイス	VLAN	宛先 MAC アドレス
管理	イネーブル（オプション）	無効
ルーテッドインターフェイス	イネーブル（オプション）	無効
ブリッジ グループ メンバー	イネーブル（オプション）	イネーブル（オプション）

入力インターフェイスを使用して **packet-tracer** コマンドを実行しているときにパケットがドロップされない場合、そのパケットはUN-NAT、ACL、NAT、IP-OPTIONS、FLOW-CREATIONのようなさまざまなフェーズを通過します。その結果、「ALLOW」というメッセージが表示されます。

ファイアウォール設定によってライブトラフィックがドロップされる可能性があるシナリオでは、シミュレーションされたトレーサパケットもドロップされます。場合によっては、ドロップの特定の理由が表示されることがあります。たとえば、ヘッダーの検証が無効なためパケットがドロップされた場合、「packet dropped due to bad ip header (reason)」というメッセージが表示されます。宛先 MAC アドレスが不明な場合は、スイッチング シーケンスでパケットがドロップされます。これにより宛先MACアドレスを検索するようにASAが起動されます。MACアドレスが見つかった場合は、packet-tracerを再度実行することができ、宛先L2ルックアップに成功します。

パケットトレーサでの VXLAN および Geneve サポートにより、内部パケットのレイヤ 2 送信元と宛先 MAC アドレス、レイヤ 3 送信元と宛先 IP アドレス、レイヤ 4 プロトコル、レイヤ 4 送信元と宛先ポート番号、仮想ネットワーク インターフェイス（VNI）番号を指定できます。TCP、SCTP、UDP、raw IP、および ICMP のみが内部パケットでサポートされます。

ドメイン/ユーザーの形式を使用して送信元のユーザー アイデンティティを指定できます。ASA では、そのユーザーの IP アドレスを検索し、該当する IP アドレスをパケット トレースのテストで使用します。ユーザーが複数の IP アドレスにマッピングされている場合、最後にログインした IP アドレスが使用され、IP アドレスとユーザーのマッピングがほかにもあることを示す出力が表示されます。このコマンドの送信元の部分でユーザー アイデンティティを指定した場合、ASA では、ユーザーが入力した宛先アドレスのタイプに基づいて IPv4 または IPv6 のいずれかのアドレスを検索します。

セキュリティ グループ名またはセキュリティ グループ タグを送信元として指定できます。ASA では、そのセキュリティ グループ名またはセキュリティ グループ タグに基づいて IP アドレスを検索し、該当する IP アドレスをパケット トレースのテストで使用します。セキュリティ グループ タグまたはセキュリティ グループ名が複数の IP アドレスにマッピングされている場合、それらのいずれかの IP アドレスが使用され、IP アドレスとセキュリティ グループ タグのマッピングがほかにもあることを示す出力が表示されます。

また、送信元と宛先アドレスの両方に FQDN を指定できます。ASA では、DNS ルックアップを実行し、パケットの構造で最初に返された IP アドレスを取得します。

L3 からブリッジ仮想インターフェイス、ブリッジ仮想インターフェイスからブリッジ仮想インターフェイスなど、宛先 IP が ASA 上の BVI インターフェイスを通じたネクスト ホップの場合のトラフィック シナリオでは、パケット トレーサはダブル ルートルックアップを実行します。また、フローは作成されません。

ARP と MAC アドレス テーブル エントリをクリアすることで、パケット トレーサは常にダブル ルートルックアップを実行し、宛先 MAC アドレスが解決されてデータベースに保存されます。しかし、これはその他のトラフィック シナリオには当てはまりません。L3 インターフェイスである場合は、宛先 MAC アドレスは解決されずにデータベースに保存されます。BVI インターフェイスは *nameif* で設定され、L3 プロパティがあるため、DMAC ルックアップを実行してはなりません。

MAC アドレスと ARP エントリがない場合の初回の試行にだけ、この動作が見られます。DMAC にエントリがあれば、パケット トレーサの出力は予期どおりになります。フローが作成されます。

永続的トレースによって、パケットがクラスタ ユニット間を通過するときにトレースできます。クラスタ ユニット間で追跡するパケットは永続化オプションを使用して送信する必要があります。各パケットの永続的なトレースのために、packet-id とホップ カウントが用意されており、送信されたパケットの起点とクラスタ ノードを通過するパケットのホップのフェーズを判断できます。packet-id は、<パケットが発信されたデバイスのノード名> と増分値の組み合わせです。packet-id は、ノードで初めて受信する新しいパケットごとに一意です。ホップ カウントは、パケットがあるクラスタ メンバーから別のクラスタ メンバーに移動するたびに読み込まれます。たとえば、クラスタリングにおいてパケットは、外部の負荷分散番号付きリストに基づいてメンバーに到着します。Host-1 は、Host-2 にパケットを送信します。送信されたパケットは、Host-2 に送信される前に、クラスタ ノード間でリダイレクトされます。メタデータ

の出力で、Tracer origin-id B:7 hop 0、Tracer origin-id B:7 hop 1、および Tracer origin-id B:7 hop 2 がそれぞれ表示されます。B は、パケットの発信元であるクラスタ ノードの名前です。7 は増分値で、クラスタ ノードから発信された 7 番目のパケットを表します。この値は、ノードから新しいパケットが発信されるたびに増やされます。"B" と "7"の組み合わせによって、パケットを特定する一意の ID が形成されます。クラスタ ユニットのローカル名は、このユニットを通過するすべてのパケットで同じです。各パケットは、グローバル バッファが unique-id とホップ カウントを使用するときに区別されます。パケットがトレースされると、永続的トレースが各ノードで使用可能になります。これは、メモリを解放するために手動で破棄するまで継続します。あるコンテキストで有効な永続的トレースは、コンテキストごとのバッファに格納されます。一連のトレースの中で特定のトレースを検索するには、origin-owner-ID（<origin-owner> <id> の 2 つの値）を使用します。

この場合、ASA から出力されるパケットをシミュレートすることができます。packet-tracer を介して transmit オプションを使用することにより、ネットワークでパケットを送信できます。デフォルトでは、packet-tracer はパケットを転送する前に廃棄します。パケットが出力されると、フロー テーブルでフローが生成されます。

packet-tracer で bypass-checks オプションを使用することにより、ACL、VPN フィルタ、uRPF、および IPsec スプーフィング チェックをバイパスできます。これは入力と出力条件の両方に適用され、シミュレートされた IPSec パケットはドロップされません

VPN トンネル内で復号化されたパケットを送信できます。VPN トンネルは汎用的で IPSec と TLS の両方に適用できます。VPN トンネル経由で送信されるパケットをシミュレートすることもできます。シミュレートされた「復号化」パケットは、既存の VPN トンネルに対応し、関連するトンネルポリシーが適用されます。ただし、この機能はルートベースの VPN トンネルには適用できません。

packet-tracer が単一のパケットを注入してトレースしている間、**pcap** キーワードにより、パケットトレーサは複数のパケット（最大 100 パケット）を再生し、フロー全体をトレースできます。pcap ファイルを入力として提供し、さらに分析するために XML または JSON 形式で結果を取得できます。トレース出力をクリアするには、**clear packet-tracer** の **pcap trace** サブコマンドを使用します。トレースの進行中は、トレース出力を使用できません。

次に、入力として pcap ファイルを使用してパケットトレーサを実行する例を示します。

```
ciscoasa# packet-tracer input inside pcap http_get.pcap detailed xml
```

次に、既存の pcap トレースバッファをクリアし、入力として pcap ファイルを提供することにより、パケットトレーサを実行する例を示します。

```
ciscoasa# packet-tracer input inside pcap http_get.pcap force
```

例

次に、HTTP ポート 201.1.1.1 から 202.1.1.1 への TCP パケットをトレースする例を示します。

```
ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a
detailed
```

```
Result:
Action: drop
Drop-reason: (dst-l2_lookup-fail) Dst MAC L2 Lookup Failed
ciscoasa# packet-tracer input inside tcp 201.1.1.1 13 202.1.1.1 324 000c.29a3.b07a
detailed
Phase: 1
Type: L2-EGRESS-IFC-LOOKUP
Subtype: Destination MAC Address Lookup
Result: ALLOW
Config:
Additional Information:
Destination MAC address lookup resulted in egress ifc outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbe83542f0, priority=1, domain=permit, deny=false
hits=7313, user_data=0x0, cs_id=0x0, l3_type=0x8
src mac=0000.0000.0000, mask=0000.0000.0000
dst mac=0000.0000.0000, mask=0100.0000.0000
input_ifc=inside, output_ifc=any
Phase: 3
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbd94026a0, priority=12, domain=permit, deny=false
hits=8, user_data=0x7fdbf07cbd00, cs_id=0x0, use_real_addr,
flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=10, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x7fdbe8363790, priority=0, domain=inspect-ip-options, deny=true
hits=212, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
```

```
input_ifc=inside, output_ifc=any
Phase: 6
Type: NAT
          Subtype: per-session
Result: ALLOW
Config:
Additional Information:

Reverse Flow based lookup yields rule:
in  id=0x7fdbd90a2990, priority=0, domain=nat-per-session, deny=false
hits=12, user_data=0x0, cs_id=0x0, reverse, use_real_addr,
flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x7fdbd93dfc10, priority=0, domain=inspect-ip-options, deny=true
hits=110, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside, output_ifc=any
Phase: 8
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 221, packet dispatched to next module
Module information for forward flow …
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat
Module information for reverse flow …
snp_fp_tracer_drop
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_tfw
snp_fp_fragment
snp_ifc_stat
Result:
input-interface: inside
input-status: up
input-line-status: up
Action: allow
44# command example
ciscoasa(config)# command example
resulting screen display here
<Text omitted.>
```

次に、HTTP ポート 10.100.10.10 から 10.100.11.11 への TCP パケットをトレースする例を示します。暗黙の拒否アクセス ルールによってパケットがドロップされることを示す結果が表示されます。

```
ciscoasa(config)# packet-tracer input outside tcp 10.100.10.10  80 10.100.11.11 80
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 10.86.116.1 using egress ifc  outside
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: DROP
Config:
Implicit Rule
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
```

次に、ユーザー CISCO\abc による内部ホスト 10.0.0.2 から外部ホスト 20.0.0.2 へのパケットをトレースする例を示します。

```
ciscoasa# packet-tracer input inside icmp user CISCO\abc 0 0 1 20.0.0.2
Source: CISCO\abc 10.0.0.2
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 20.0.0. 255.255.255.0 outside
...
Result:
input-interface: inside
input-status: up
input-line-status: up
output-interfce: outside
output-status: up
output-line-status: up
Action: allow
```

次に、ユーザー CISCO\abc による内部ホスト 20.0.0.2 からのパケットをトレースし、トレース結果を XML 形式で表示する例を示します。

```
<Source>
<user>CISCO\abc</user>
<user-ip>10.0.0.2</user-ip>
<more-ip>1</more-ip>
</Source>
<Phase>
<id>1</id>
<type>ROUTE-LOOKUP</type>
<subtype>input</subtype>
<result>ALLOW</result>
<config>
```

```
</config>
<extra>
in 20.0.0.0 255.255.255.0 outside
</extra>
</Phase>
```

次に、内部ホスト xyz.example.com から外部ホスト abc.example.com へのパケットをトレースする例を示します。

```
ciscoasa# packet-tracer input inside tcp fqdn xyz.example.com 1000 fqdn abc.example.com
 23
Mapping FQDN xyz.example.com to IP address 10.0.0.2
(More IP addresses resolved. Please run “show dns-host” to check.)
Mapping FQDN abc.example.com to IP address 20.0.0.2
(More IP addresses resolved. Please run “show dns-host” to check.)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
```

次に、**packet-tracer** コマンドの出力例を示します。この出力から、セキュリティグループタグと IP アドレスの対応付けがわかります。

```
ciscoasa# packet-tracer input inside tcp security-group name alpha 30 security-group tag
 31 300
Mapping security-group 30:alpha to IP address 10.1.1.2.
Mapping security-group 31:bravo to IP address 192.168.1.2.
Phase: 1
Type: ROUTE-LOOKUP
Subtype: input
Result: ALLOW
Config:
Additional Information:
in 192.168.1.0 255.255.255.0 outside....
----------------More---------------------
```

次に、レイヤ 2 SGT インポジションを表示する **packet-tracer** コマンドの出力の例を示します。

```
ciscoasa# packet-tracer input inside tcp inline-tag 100 10.1.1.2 30 192.168.1.2 300
```

次の例では、UDP/TCP および ICMP の内部パケットに対する VXLAN のサポートについて概要を示します。

```
packet-tracer in inside udp 30.0.0.2 12345 30.0.0.100 vxlan vxlan-inner 1234 1.1.1.1
11111 2.2.2.2 22222 aaaa.bbbb.cccc aaaa.bbbb.dddd detailedOuter packet: UDP from 30.0.0.2
 to 30.0.0.100 (vtep/nve source-interface IP) with default vxlan destination port.
Inner packet: VXLAN in-tag 1234, UDP from 1.1.1.1/11111 to 2.2.2.2/22222 with smac
aaaa.bbbb.cccc and dmac aaaa.bbbb.dddd
```

次に、クラスタ ユニット間で渡される永続的トレースの出力の例を示します。

```
ciscoasa# cluster exec show packet-tracer
B(LOCAL):**********************************************************
tracer 10/8 (allocate/freed), handle 10/8 (allocated/freed), error 0
=======  Tracer origin-id B:7, hop 0 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
```

```
<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) am asking director (0).
Phase: 5
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To A(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
=======  Tracer origin-id B:7, hop 2 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
<Snipping phase 1-3: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From A(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
<Snipping phase 2-4: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP>
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (1) have been elected owner by (0).
<Snipping phase 6-16: ACCESS-LIST, NAT, IP-OPTIONS, INSPECT, INSPECT, FLOW-CREATION,
ACCESS-LIST, NAT, IP-OPTIONS, ROUTE-LOOKUP, ADJACENCY-LOOKUP>
A:**********************************************************************
tracer 6/5 (allocate/freed), handle 6/5 (allocated/freed), error 0
=======  Tracer origin-id B:7, hop 1 =======
packet-id: icmp src inside:15.11.1.122 dst 15.11.2.124 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From B(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
<Snipping phase 2-7: CAPTURE, ACCESS-LIST, ROUTE-LOOKUP, ACCESS-LIST, NAT, IP-OPTIONS>
Phase: 8
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'inside'
Flow type: NO FLOW
I (0) am director, not creating dir flow for ICMP pkt recvd by (1).
Phase: 9
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
```

```
Config:
Additional Information:
To B(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
ciscoasa#
```

次に、origin と id のオプションを使用してクラスタ ノードからパケットがトレースされるときの出力の例を示します。

```
cluster2-asa5585a# cluster exec show packet-tracer | i origin-id
b(LOCAL):**************************************************************
=======  Tracer origin-id b:2, hop 0 =======
=======  Tracer origin-id b:2, hop 2 =======
a:**************************************************************
=======  Tracer origin-id a:17, hop 0 =======
=======  Tracer origin-id b:2, hop 1 =======
=======  Tracer origin-id b:2, hop 3 =======
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer ori
cluster2-asa5585a# cluster exec show packet-tracer origin b id 2
b(LOCAL):**************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
=======  Tracer origin-id b:2, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) am asking director (0).
Phase: 4
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
=======  Tracer origin-id b:2, hop 2 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
```

```
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From a(0), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (1) have been elected owner by (0).
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: INSPECT
```

```
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: FULL
I (1) am redirecting to (0) due to matching action (1).
Phase: 15
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To a(0), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
a:**********************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id b:2, hop 1 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW_OWNER_REQUEST(17), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 3
Type: ACCESS-LIST
```

```
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am director, found static rule to classify owner as (253).
Phase: 7
Type: CLUSTER-EVENT
Subtype: forward
Result: ALLOW
Config:
Additional Information:
To b(1), cq_type CQ_FLOW_OWNER_REPLY(18), flags 0, frag-cnt 0, trace-options 0x10
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
=======  Tracer origin-id b:2, hop 3 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 0, code 0)
Phase: 1
Type: CLUSTER-EVENT
Subtype: receive
Result: ALLOW
Config:
Additional Information:
From b(1), cq_type CQ_FLOW(1), flags 0, frag-cnt 0, trace-options 0x10
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 4
```

```
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) have been elected owner by (0).
Phase: 5
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:

Phase: 6
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
```

```
Phase: 14
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 70, packet dispatched to next module
Phase: 19
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc  identity
Phase: 20
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1730 reference 6
Phase: 21
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside2
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
cluster2-asa5585a#
cluster2-asa5585a#
```

```
cluster2-asa5585a# cluster exec show packet-tracer origin a
b(LOCAL):*******************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
a:*******************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id a:17, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
```

```
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 0.0.0.0 using egress ifc  identity
Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1577 reference 6
Result:
input-interface: outside2
```

```
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
cluster2-asa5585a# cluster exec show packet-tracer id 17
b(LOCAL):************************************************************
tracer 3/1 (allocate/freed), handle 3/1 (allocated/freed), error 0
a:************************************************************************
tracer 20/17 (allocate/freed), handle 20/17 (allocated/freed), error 0
=======  Tracer origin-id a:17, hop 0 =======
packet-id: icmp src outside2:212.1.1.9 dst 214.1.1.10 (type 8, code 0)
Phase: 1
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.10 using egress ifc  identity
Phase: 2
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside2'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 3
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
```

```
Additional Information:
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: CLUSTER-REDIRECT
Subtype: cluster-redirect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:

Phase: 13
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 69, packet dispatched to next module
Phase: 17
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 0.0.0.0 using egress ifc  identity
Phase: 18
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
```

```
found adjacency entry for Next-hop 0.0.0.0 on interface  outside
adjacency Active
mac address 0000.0000.0000 hits 1577 reference 6
Result:
input-interface: outside2
input-status: up
input-line-status: up
output-interface: NP Identity Ifc
Action: allow
cluster2-asa5585a#
```

次の例では、クラスタ ノードからの永続的トレースをクリアする概要を示します。

```
ciscoasa# cluster exec clear packet-tracer
```

IPSec トンネルで復号化されたパケットを送信する場合は、いくつかの条件があります。IPSec トンネルがネゴシエートされていない場合、エラー メッセージが表示されます。次に、IPSec トンネルがネゴシエートされると、パケットが通過します。

次の例では、復号されたパケットを送信するために IPSec トンネルがネゴシエートされた場合の概要を示します。**not**

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
decrypted
  ********************************************************************
  WARNING: An existing decryption SA was not found. Please confirm the
  IPsec Phase 2 SA or Anyconnect Tunnel is established.
  ********************************************************************
  Phase: 1
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list
  Phase: 2
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 3
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.
  Phase: 4
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
```

```
  I (0) am becoming owner
  Phase: 5
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
  access-list ALLOW extended permit ip any any
  Additional Information:
  Phase: 6
  Type: NAT
  Subtype: per-session
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 7
  Type: IP-OPTIONS
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 8
  Type: INSPECT
  Subtype: inspect-ftp
  Result: ALLOW
  Config:
  class-map inspection_default
  match default-inspection-traffic
  policy-map global_policy
  class inspection_default
  inspect ftp
  service-policy global_policy global
  Additional Information:
  Phase: 9
  Type: VPN
  Subtype: ipsec-tunnel-flow
  Result: DROP
  Config:
  Additional Information:
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: drop
  Drop-reason: (acl-drop) Flow is denied by configured rule
  cluster2-asa5585a(config)#
```

次の例では、復号化されたパケットを送信するために IPSec トンネルがネゴシエートされた場合の概要を示します。

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21 decrypted

  Phase: 1
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 2
```

```
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 3
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
```

```
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 19
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 20
```

```
  Type: VPN
  Subtype: encrypt
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 21
  Type: FLOW-CREATION
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  New flow created with id 1099, packet dispatched to next module
  Phase: 22
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 23
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  Phase: 24
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  Phase: 25
  Type: FLOW-CREATION
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  New flow created with id 1100, packet dispatched to next module
  Phase: 26
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 99 reference 2
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: allow
```

次の例では、送信オプションを使用して、シミュレートされたパケットの送信を許可し、発信インターフェイスで同じパケットをキャプチャします。

```
cluster2-asa5585a(config)# packet-tracer input outside icmp 211.1.1.10 8 0 213.1.1.10
transmit
  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list
  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: ALLOW
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list
  Phase: 3
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2

  Phase: 4
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) am becoming owner
  Phase: 5
  Type: ACCESS-LIST
  Subtype: log
  Result: ALLOW
  Config:
  access-group ALLOW global
  access-list ALLOW extended permit ip any any
  Additional Information:
  Phase: 6
  Type: NAT
  Subtype: per-session
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 7
  Type: IP-OPTIONS
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Phase: 8
  Type:
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
```

```
Phase: 9
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: np-inspect
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type:
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 6449, packet dispatched to next module
Phase: 15
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 16
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
```

```
  Phase: 19
  Type: ADJACENCY-LOOKUP
  Subtype: Resolve Nexthop IP address to MAC
  Result: ALLOW
  Config:
  Additional Information:
  found adjacency entry for next-hop 214.1.1.9 on interface  outside
  adjacency Active
  mac address 4403.a74a.9a32 hits 15 reference 1
  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  output-interface: outside2
  output-status: up
  output-line-status: up
  Action: allow
  cluster2-asa5585a(config)#
```

次の例では、発信インターフェイスでキャプチャされる ICMP パケットの概要を示します。

```
cluster2-asa5585a(config)# cluster exec show capture test | i icmp
  a(LOCAL):*******************************************************
    14: 02:18:16.717736       802.1Q vlan#212 P0 211.1.1.10 > 213.1.1.10: icmp: echo
request
  cluster2-asa5585a(config)#
```

packet-tracer の bypass-checks オプションの例については、以下のフェーズで概要を示します。各シナリオでは、特定の例が想定されています。

- スポークとハブ間に IPSec トンネルが作成されない場合。
- 2 つのボックス間で IPSec トンネルをネゴシエートする必要があり、最初のパケットがトンネルの確立をトリガーします。
- IPSec ネゴシエーションが完了し、トンネルが生成されます。
- トンネルが起動すると、発信されるパケットはトンネルを介して送信されます。パケットパスで使用できるセキュリティチェック（ACL、VPN フィルタリング..）がバイパスまたはスキップされます。

IPSec トンネルは作成されません。

```
cluster2-asa5585a(config)# sh crypto ipsec sa
  There are no ipsec sas
  cluster2-asa5585a(config)#
```

トンネル ネゴシエーション プロセスが開始されます。

```
cluster2-asa5585a(config)# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
bypass-checks
  Phase: 1
  Type: CAPTURE
  Subtype:
```

```
Result: ALLOW
Config:
Additional Information:
MAC Access list
Phase: 2
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
MAC Access list
Phase: 3
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2

Phase: 4
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) got initial, attempting ownership.
Phase: 5
Type: CLUSTER-EVENT
Subtype:
Result: ALLOW
Config:
Additional Information:
Input interface: 'outside'
Flow type: NO FLOW
I (0) am becoming owner
Phase: 6
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
```

```
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 12
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: encrypt
Result: DROP
Config:
Additional Information:
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: drop
Drop-reason: (acl-drop) Flow is denied by configured rule
cluster2-asa5585a(config)#
```

IPSec トンネルがネゴシエートされると、トンネルが生成されます。

```
cluster2-asa5585a#
  cluster2-asa5585a(config)# sh crypto ipsec sa
  interface: outside2
      Crypto map tag: crypto-map-peer4, seq num: 1, local addr: 214.1.1.10
        access-list toPeer4 extended permit ip host 211.1.1.1 host 213.1.1.2
        local ident (addr/mask/prot/port): (211.1.1.1/255.255.255.255/0/0)
        remote ident (addr/mask/prot/port): (213.1.1.2/255.255.255.255/0/0)
        current_peer: 214.1.1.9
        #pkts encaps: 0, #pkts encrypt: 0, #pkts digest: 0
        #pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
        #pkts compressed: 0, #pkts decompressed: 0
        #pkts not compressed: 0, #pkts comp failed: 0, #pkts decomp failed: 0
        #pre-frag successes: 0, #pre-frag failures: 0, #fragments created: 0
        #PMTUs sent: 0, #PMTUs rcvd: 0, #decapsulated frgs needing reassembly: 0
        #TFC rcvd: 0, #TFC sent: 0
```

```
        #Valid ICMP Errors rcvd: 0, #Invalid ICMP Errors rcvd: 0
        #send errors: 0, #recv errors: 0
        local crypto endpt.: 214.1.1.10/500, remote crypto endpt.: 214.1.1.9/500
        path mtu 1500, ipsec overhead 74(44), media mtu 1500
        PMTU time remaining (sec): 0, DF policy: copy-df
        ICMP error validation: disabled, TFC packets: disabled
        current outbound spi: A642726D
        current inbound spi : CF1E8F90

      inbound esp sas:
        spi: 0xCF1E8F90 (3474886544)
           SA State: active
           transform: esp-aes-256 esp-sha-hmac no compression
           in use settings ={L2L, Tunnel, IKEv2, }
           slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
           sa timing: remaining key lifetime (kB/sec): (4285440/28744)
           IV size: 16 bytes
           replay detection support: Y
           Anti replay bitmap:
            0x00000000 0x00000001
      outbound esp sas:
        spi: 0xA642726D (2789372525)
           SA State: active
           transform: esp-aes-256 esp-sha-hmac no compression
           in use settings ={L2L, Tunnel, IKEv2, }
           slot: 0, conn_id: 2, crypto-map: crypto-map-peer4
           sa timing: remaining key lifetime (kB/sec): (4239360/28744)
           IV size: 16 bytes
           replay detection support: Y
           Anti replay bitmap:
            0x00000000 0x00000001
  cluster2-asa5585a(config)#
```

トンネルが生成されるとパケットが通過できるようになり、bypass-checks オプションが適用されるため、セキュリティ チェックがスキップされます。

```
cluster2-asa5585a# packet-tracer input outside tcp 211.1.1.1 5050 213.1.1.2 21
bypass-checks
  Phase: 1
  Type: ROUTE-LOOKUP
  Subtype: Resolve Egress Interface
  Result: ALLOW
  Config:
  Additional Information:
  found next-hop 214.1.1.9 using egress ifc  outside2
  Phase: 2
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) got initial, attempting ownership.
  Phase: 3
  Type: CLUSTER-EVENT
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  Input interface: 'outside'
  Flow type: NO FLOW
  I (0) am becoming owner
```

```
Phase: 4
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group ALLOW global
access-list ALLOW extended permit ip any any
Additional Information:
Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 7
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 8
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 9
Type: INSPECT
Subtype: inspect-ftp
Result: ALLOW
Config:
class-map inspection_default
 match default-inspection-traffic
policy-map global_policy
 class inspection_default
  inspect ftp
service-policy global_policy global
Additional Information:
Phase: 10
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 11
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 12
Type: VPN
```

```
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 13
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 14
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 15
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 16
Type: VPN
Subtype: ipsec-tunnel-flow
Result: ALLOW
Config:
Additional Information:
Phase: 17
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Phase: 18
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Phase: 19
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 20
Type: VPN
Subtype: encrypt
Result: ALLOW
Config:
Additional Information:
Phase: 21
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1099, packet dispatched to next module
Phase: 22
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
```

```
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 23
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 24
Type: ACCESS-LIST
Subtype:
Result: ALLOW
Config:
Implicit Rule
Additional Information:
Phase: 25
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 1100, packet dispatched to next module
Phase: 26
Type: ROUTE-LOOKUP
Subtype: Resolve Egress Interface
Result: ALLOW
Config:
Additional Information:
found next-hop 214.1.1.9 using egress ifc  outside2
Phase: 27
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 214.1.1.9 on interface  outside
adjacency Active
mac address 4403.a74a.9a32 hits 99 reference 2
Result:
input-interface: outside
input-status: up
input-line-status: up
output-interface: outside2
output-status: up
output-line-status: up
Action: allow
```

次の例では、ネクストホップのARPエントリが含まれる直接接続されたホストでTCPパケットを追跡します。

```
ciscoasa# packet-tracer input inside tcp 192.168.100.100 12345 192.168.102.102 80 detailed


Phase: 1
Type: ROUTE-LOOKUP
Subtype: No ECMP load balancing
Result: ALLOW
Config:
Additional Information:
Destination is locally connected. No ECMP load balancing.
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)
```

```
Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=17, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 3
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=34, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 4
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8488800, priority=0, domain=inspect-ip-options, deny=true
hits=22, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=inside(vrfid:0), output_ifc=any

Phase: 5
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=36, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 6
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=10, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
```

```
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 7
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 21, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 8
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 9
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for next-hop 192.168.102.102 on interface  outside
Adjacency :Active
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: inside(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
```

次の例では、ネクストホップに対する有効なARPエントリがないためにドロップされたTCPパケットを追跡します。ドロップされた理由では、ARPテーブルをチェックするためのヒントも提供されています。

```
<Displays same phases as in the previous example till Phase 8>
Result:
input-interface: inside(vrfid:0)
input-status: up
```

```
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-v4-adjacency) No valid V4 adjacency. Check ARP table (show arp) has
entry for nexthop., Drop-location: frame snp_fp_adj_process_cb:200 flow (NA)/NA
```

次の例では、NAT と到達可能なネクストホップを使用した準最適ルーティングのパケットトレーサを示しています。

```
ciscoasa# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1
route outside 0.0.0.0 0.0.0.0 192.168.102.102 10

ciscoasa# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24
ciscoasa# packet-tracer input dmz tcp 192.168.104.104 12345 10.10.10.10 80 detailed

Phase: 1
Type: UN-NAT
Subtype: static
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
NAT divert to egress interface outside(vrfid:0)
Untranslate 10.10.10.10/80 to 9.9.9.10/80

Phase: 2
Type: ACCESS-LIST
Subtype: log
Result: ALLOW
Config:
access-group TEST global
access-list TEST advanced trust ip any any
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa5e90, priority=12, domain=permit, trust
hits=20, user_data=0x2ae29aabc100, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, ifc=any, vlan=0, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
Static translate 192.168.104.104/12345 to 192.168.104.104/12345
Forward Flow based lookup yields rule:
in  id=0x2ae2a8aa4ff0, priority=6, domain=nat, deny=false
hits=4, user_data=0x2ae2a8a9d690, cs_id=0x0, flags=0x0, protocol=0
```

```
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=10.10.10.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 4
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=40, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any

Phase: 5
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Forward Flow based lookup yields rule:
in  id=0x2ae2a89de1b0, priority=0, domain=inspect-ip-options, deny=true
hits=4, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=any

Phase: 6
Type: NAT
Subtype: rpf-check
Result: ALLOW
Config:
nat (outside,dmz) source static src_real src_mapped destination static dest_real
dest_mapped
Additional Information:
Forward Flow based lookup yields rule:
out id=0x2ae2a8aa53d0, priority=6, domain=nat-reverse, deny=false
hits=5, user_data=0x2ae2a8a9d580, cs_id=0x0, use_real_addr, flags=0x0, protocol=0
src ip/id=192.168.104.0, mask=255.255.255.0, port=0, tag=any
dst ip/id=9.9.9.0, mask=255.255.255.0, port=0, tag=any, dscp=0x0
input_ifc=dmz(vrfid:0), output_ifc=outside(vrfid:0)

Phase: 7
Type: NAT
Subtype: per-session
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
in  id=0x2ae2a69a7240, priority=0, domain=nat-per-session, deny=false
hits=42, user_data=0x0, cs_id=0x0, reverse, use_real_addr, flags=0x0, protocol=6
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=any, output_ifc=any
Phase: 8
Type: IP-OPTIONS
Subtype:
Result: ALLOW
Config:
Additional Information:
Reverse Flow based lookup yields rule:
```

```
in  id=0x2ae2a893e230, priority=0, domain=inspect-ip-options, deny=true
hits=13, user_data=0x0, cs_id=0x0, reverse, flags=0x0, protocol=0
src ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any
dst ip/id=0.0.0.0, mask=0.0.0.0, port=0, tag=any, dscp=0x0
input_ifc=outside(vrfid:0), output_ifc=any

Phase: 9
Type: FLOW-CREATION
Subtype:
Result: ALLOW
Config:
Additional Information:
New flow created with id 24, packet dispatched to next module
Module information for forward flow ...
snp_fp_inspect_ip_options
snp_fp_tcp_normalizer
snp_fp_translate
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Module information for reverse flow ...
snp_fp_inspect_ip_options
snp_fp_translate
snp_fp_tcp_normalizer
snp_fp_adjacency
snp_fp_fragment
snp_fp_tracer_drop
snp_ifc_stat

Phase: 10
Type: INPUT-ROUTE-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Resolve Preferred Egress interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.100.100 using egress ifc  inside(vrfid:0)

Phase: 11
Type: SUBOPTIMAL-LOOKUP
Subtype: suboptimal next-hop
Result: ALLOW
Config:
Additional Information:
Input route lookup returned ifc  inside is not same as existing ifc  outside
Doing adjacency lookup lookup on existing ifc outside

Phase: 12
Type: NEXTHOP-LOOKUP-FROM-OUTPUT-ROUTE-LOOKUP
Subtype: Lookup Nexthop on interface
Result: ALLOW
Config:
Additional Information:
Found next-hop 192.168.102.102 using egress ifc  outside(vrfid:0)

Phase: 13
Type: ADJACENCY-LOOKUP
Subtype: Resolve Nexthop IP address to MAC
Result: ALLOW
Config:
Additional Information:
found adjacency entry for Next-hop 192.168.102.102 on interface  outside
Adjacency :Active
```

```
mac address 0aaa.0bbb.00cc hits 5 reference 1

Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: allow
The following example depicts packet tracer for sub-optimal routing with NAT, where, the
 packet is dropped due to non-reachable nexthop.
ciscoasa# sh run route
route inside 0.0.0.0 0.0.0.0 192.168.100.100 1

ciscoasa# sh nat detail
Manual NAT Policies (Section 1)
1 (outside) to (dmz) source static src_real src_mapped  destination static dest_real
dest_mapped
translate_hits = 3, untranslate_hits = 3
Source - Origin: 9.9.9.0/24, Translated: 10.10.10.0/24
Destination - Origin: 192.168.104.0/24, Translated: 192.168.104.0/24


<Displays same phases as in the previous example till Phase 11>
Result:
input-interface: dmz(vrfid:0)
input-status: up
input-line-status: up
output-interface: outside(vrfid:0)
output-status: up
output-line-status: up
Action: drop
Drop-reason: (no-adjacency) No valid adjacency, Drop-location: frame
snp_fp_adjacency_internal:5890 flow (NA)/NA
```

関連コマンド

コマンド	説明
capture	トレース パケットを含めて、パケット情報をキャプチャします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。
show packet-tracer	PCAP ファイルに対して最後に実行されたパケットトレーサのトレースバッファ出力を表示します。

pager

Telnet セッションで「---More---」プロンプトが表示されるまでの 1 ページあたりのデフォルト行数を設定するには、グローバル コンフィギュレーション モードで **pager** コマンドを使用します。

pager [**lines**] 回線

構文の説明

[**lines**] *lines*	「---More---」プロンプトが表示されるまでの 1 ページあたりの行数を設定します。デフォルトは 24 行です。0 は、ページの制限がないことを示します。指定できる範囲は 0 ～ 2147483647 行です。**lines** キーワードは任意であり、このキーワードの有無にかかわらずコマンドは同一です。

コマンド デフォルト

デフォルトは 24 行です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドは、特権 EXEC モードのコマンドからグローバル コンフィギュレーション モードのコマンドに変更されました。**terminal pager** コマンドが特権 EXEC モードのコマンドとして追加されました。

使用上のガイドライン

このコマンドは、Telnet セッションでのデフォルトの pager line 設定を変更します。現在のセッションについてのみ、設定を一時的に変更する場合は、 **terminal pager** コマンドを使用します。

管理コンテキストに Telnet 接続する場合、特定のコンテキスト内の **pager** コマンドに異なる設定がある場合でも、他のコンテキストに変更すると、pager line 設定はユーザーのセッションに従います。現在の pager 設定を変更するには、新しい設定で **terminal pager** コマンドを入力するか、**pager** コマンドを現在のコンテキストで入力します。**pager** コマンドは、コンテキスト コンフィギュレーションに新しい pager 設定を保存する以外に、新しい設定を現在の Telnet セッションに適用します。

例

次に、表示される行数を 20 に変更する例を示します。

```
ciscoasa(config)# pager 20
```

関連コマンド

コマンド	説明
clear configure terminal	端末の表示幅設定をクリアします。
show running-config terminal	現在の端末設定を表示します。
terminal	システム ログ メッセージを Telnet セッションで表示できるようにします。
terminal pager	Telnet セッションで「---more---」プロンプトが表示されるまでの行数を設定します。このコマンドはコンフィギュレーションに保存されません。
terminal width	グローバル コンフィギュレーション モードでの端末の表示幅を設定します。

page style

WebVPN ユーザーがセキュリティアプライアンスに接続するときに表示される WebVPN ページ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 **page style** 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。

page style *value*
［ **no** ］ **page style** *value*

構文の説明

value カスケーディング スタイル シート（CSS）パラメータ（最大 256 文字）。

コマンド デフォルト

デフォルトのページ スタイルは、background-color:white;font-family:Arial,Helv,sans-serif 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効なカスケーディング スタイル シート（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、World Wide Web コンソーシアム（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、ページ スタイルを large にカスタマイズする例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization cisco
ciscoasa(config-webvpn-custom)# page style font-size:large
```

関連コマンド

コマンド	説明
logo	WebVPN ページのロゴをカスタマイズします。
title	WebVPN ページのタイトルをカスタマイズします。

パラメータ

パラメータ コンフィギュレーション モードを開始してインスペクション ポリシー マップのパラメータを設定するには、ポリシー マップ コンフィギュレーション モードで **parameters** コマンドを使用します。

parameters

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ポリシー マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークでは、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。レイヤ 3/4 のポリシーマップ（**policy-map** コマンド）で、**inspect** コマンドを使用して検査エンジンを有効にする場合は、**policy-map type inspect** コマンドで作成されたインスペクション ポリシーマップで定義されているアクションもオプションで有効にできます。たとえば、**inspect dns dns_policy_map** コマンドを入力します。dns_policy_map は、インスペクション ポリシー マップの名前です。

インスペクション ポリシー マップは、1 つ以上の **parameters** コマンドをサポートできます。パラメータは、インスペクションエンジンの動作に影響します。パラメータ コンフィギュレーション モードで使用できるコマンドは、アプリケーションによって異なります。

例

次に、デフォルトのインスペクション ポリシー マップにおける DNS パケットの最大メッセージ長を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
```

```
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# message-length maximum 512
```

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。

participate

デバイスを仮想ロードバランシングクラスタに強制参加させるには、VPN ロード バランシング コンフィギュレーション モードで **participate** コマンドを使用します。クラスタに参加しているデバ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。

participate
no participate

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。

コマンド デフォルト

デフォルトの動作では、デバイスは VPN ロード バランシング クラスタに参加しません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
VPN ロード バランシング コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

まず、**interface** および **nameif** コマンドを使用してインターフェイスを設定し、**vpn load-balancing** コマンドを使用して VPN ロードバランシングモードを開始する必要があります。さらに、**cluster ip** コマンドを使用してクラスタ IP アドレスを設定し、仮想クラスタ IP アドレスが参照するインターフェイスを設定しておく必要があります。

このコマンドは、このデバイスを仮想ロードバランシング クラスタに強制的に参加させます。デバイスへの参加をイネーブルにするには、このコマンドを明示的に発行する必要があります。

クラスタに参加するすべてのデバイスは、IP アドレス、暗号設定、暗号キー、およびポートというクラスタ固有の同一値を共有する必要があります。

（注） 暗号化を使用するときは、**isakmp enable** *inside* コマンドを事前に設定しておく必要があります。*inside* では、ロードバランシングの内部インターフェイスを指定します。ロードバランシングの内部インターフェイス上で isakmp が有効になっていない場合、クラスタ暗号化の設定を試みたときにエラーメッセージが表示されます。**cluster encryption** コマンドの設定時に isakmp が有効であっても、**participate** コマンドを設定する前に無効になった場合、**participate** コマンドの入力時にエラーメッセージが表示され、ローカルデバイスはクラスタに参加しません。

例

次に、現在のデバイスを VPN ロードバランシングクラスタに参加できるようにする **participate** コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードを開始します。

passive-interface（IPv6 ルータ OSPF）

特定のインターフェイスまたはOSPFv3プロセスを使用しているすべてのインターフェイスでルーティング更新の送受信を行わないようにするには、IPv6 ルータ OSPF コンフィギュレーション モードで **passive-interface** コマンドを使用します。特定のインターフェイスまたはOSPFv3 プロセスを使用しているすべてのインターフェイスでルーティング更新を再び有効にするには、このコマンドの **no** 形式を使用します。

passive-interface [*interface_name*]
no passive-interface [*interface_name*]

構文の説明

interface_name	（オプション）OSPFv3 プロセスが実行されているインターフェイスの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスでパッシブ ルーティングをイネーブルにします。

例

次に、内部インターフェイスでルーティング更新の送受信を行わないようにする例を示します。

```
ciscoasa(config)# ipv6
router ospf 10
ciscoasa(config-rtr)# passive-interface interface
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
show running-config router	実行コンフィギュレーションに含まれるルータ コンフィギュレーション コマンドを表示します。

passive-interface（ISIS）

トポロジデータベースにインターフェイスアドレスが含まれている場合に、インターフェイスで ISIS hello パケットおよびルーティングアップデートを選択するには、ルータ ISIS コンフィギュレーション モードで **passive-interface** コマンドを使用します。発信 hello パケットおよびルーティングアップデートを再び有効にするには、このコマンドの **no** 形式を使用します。

passive-interface [**default** | **inside** | **management** | **management2**]
no passive-interface [**default** | **inside** | **management** | **management2**]

構文の説明

default	すべてのインターフェイス上でルーティングが更新されないようにします。
inside	インターフェイス GigabithEthernet0/0 の名前。
management	インターフェイス Management0/0 の名前。
management2	インターフェイス Management0/1 の名前。

コマンド デフォルト

デフォルトでは、すべてのインターフェイス上でルーティングが更新されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、インターフェイスでパッシブ ルーティングをイネーブルにします。

例

次に、内部インターフェイスでルーティング更新の送受信を行わないようにする例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# passive-interface inside
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。

コマンド	説明
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。

コマンド	説明
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

passive-interface（ルータ EIGRP）

インターフェイスで EIGRP ルーティング更新の送受信を無効にするには、ルータ EIGRP コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスでルーティング更新を再び有効にするには、このコマンドの **no** 形式を使用します。

passive-interface {**default***if_name*}
no passive-interface {**default***if_name*}

構文の説明

default	（任意）すべてのインターフェイスを受動モードに設定します。
if_name	（任意）**nameif** コマンドでパッシブモードに指定したインターフェイスの名前。

コマンド デフォルト

そのインターフェイスでルーティングがイネーブルになると、アクティブ ルーティング（ルーティング更新の送受信）に対してすべてのインターフェイスがイネーブルになります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ EIGRP コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	EIGRP ルーティングのサポートが追加されました。

使用上のガイドライン

インターフェイス上でパッシブ ルーティングをイネーブルにします。EIGRP の場合は、これによりそのインターフェイスでのルーティング更新の送受信がディセーブルになります。

EIGRP 構成では、複数の **passive-interface** コマンドを使用できます。**passive-interface default** コマンドを使用してすべてのインターフェイスで EIGRP ルーティングを無効にし、**no passive-interface** コマンドを使用して特定のインターフェイスで EIGRP ルーティングを有効にできます。

例

次に、外部インターフェイスをパッシブ EIGRP に設定する例を示します。セキュリティ アプライアンスの他のインターフェイスは、EIGRP 更新を送受信します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

次に、内部インターフェイスを除くすべてのインターフェイスをパッシブ EIGRP に設定する例を示します。内部インターフェイスのみが EIGRP 更新を送受信します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface default
ciscoasa(config-router)# no passive-interface inside
```

関連コマンド

コマンド	説明
show running-config router	実行コンフィギュレーションに含まれるルータ コンフィギュレーション コマンドを表示します。

passive-interface（ルータ RIP）

インターフェイスで RIP ルーティング更新の送信を無効にするには、ルータ RIP コンフィギュレーション モードで **passive-interface** コマンドを使用します。インターフェイスで RIP ルーティング更新を再び有効にするには、このコマンドの **no** 形式を使用します。

passive-interface { **default** | *if_name* }
no passive-interface { **default** | *if_name* }

構文の説明

default	（任意）すべてのインターフェイスを受動モードに設定します。
if_name	（任意）指定したインターフェイスをパッシブ モードに設定します。

コマンド デフォルト

RIP がイネーブルになると、アクティブ RIP に対してすべてのインターフェイスがイネーブルになります。

インターフェイスまたは **default** キーワードを指定しない場合、コマンドのデフォルトは **default** であり、構成には passive-interface default と表示されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ RIP コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

インターフェイス上でパッシブ RIP をイネーブルにします。インターフェイスは RIP ルーティング ブロードキャストを受信し、その情報を使用してルーティング テーブルを設定しますが、ルーティング更新はブロードキャストしません。

例

次に、外部インターフェイスをパッシブ RIP に設定する例を示します。セキュリティ アプライアンスの他のインターフェイスは、RIP 更新を送受信します。

```
ciscoasa(config)# router rip
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# passive-interface outside
```

関連コマンド

コマンド	説明
clear configure rip	実行コンフィギュレーションからすべてのRIPコマンドをクリアします。
router rip	RIP ルーティング プロセスをイネーブルにし、RIP 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 rip	実行コンフィギュレーションの RIP コマンドを表示します。

passwd

Telnet のログイン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 **passwd** コマンドを使用します。パスワードをリセットにするには、このコマンドの **no** 形式を使用します。

passwd *password* ［ **encrypted** ］
no passwd *password*

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。何らかの理由でパスワードを別の ASA にコピーする必要があるが、元のパスワードがわからない場合、暗号化されたパスワードとこのキーワードを指定して **passwd** コマンドを入力できます。通常、このキーワードは、**show running-config passwd** コマンドを入力したときにのみ表示されます。

password パスワードを最大 80 文字のストリングで設定します。大文字と小文字は区別されます。パスワードにスペースを含めることはできません。

コマンド デフォルト

9.1(1)：デフォルトのパスワードは「cisco」です。

9.1(2)：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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.3(1)	エイリアス **password** コマンドが削除され、**passwd** のみサポートされています。
8.4(2)	SSH デフォルトユーザー名がサポートされなくなり、**pix** または **asa** ユーザー名とログインパスワードで SSH を使用して ASA に接続できなくなりました。

リリース	変更内容
9.0(2)、9.1(2)	デフォルトのパスワード「cisco」が削除され、ログイン パスワードを能動的に設定しなければならなくなりました。 **no passwd** コマンドまたは **clear configure passwd** コマンドを使用した場合、パスワードが削除されるようになりました。以前のバージョンではパスワードがデフォルトの「cisco」にリセットされました。

使用上のガイドライン

telnet コマンドを使用して Telnet を有効にする場合、**passwd** コマンドで設定したパスワードでログインできます。ログイン パスワードを入力すると、ユーザー EXEC モードが開始されます。**aaa authentication telnet console** コマンドを使用して Telnet のユーザーごとに CLI 認証を設定する場合、このパスワードは使用されません。

このパスワードは、スイッチから ASASM への Telnet セッションでも使用されます（**session** コマンドを参照）。

例

次に、パスワードを Pa$$w0rd に設定する例を示します。

```
ciscoasa(config)# passwd
Pa$$w0rd
```

次に、パスワードを、別の ASA 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。

```
ciscoasa(config)# passwd jMorNbK0514fadBh encrypted
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードをクリアします。
enable	特権 EXEC モードを開始します。
enable password	イネーブル パスワードを設定します。
show curpriv	現在ログインしているユーザー名とユーザーの特権レベルを表示します。
show running-config passwd	暗号化された形式でログイン パスワードを表示します。

password（クリプト CA トラストポイント）

登録時に CA に登録されたチャレンジフレーズを指定するには、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 **password** 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。

password *string*
no password *string*

構文の説明

string パスワードの名前をストリングとして指定します。最初の文字を数値にはできません。ストリングには、80 文字以下の任意の英数字（スペースを含む）を指定できます。数字-スペース-任意の文字の形式ではパスワードを指定できません。数字の後にスペースを使用すると、問題が発生します。たとえば、「hello 21」は有効なパスワードですが、「21 hello」は無効です。パスワード チェックでは、大文字と小文字が区別されます。たとえば、パスワード「Secret」とパスワード「secret」は異なります。

コマンド デフォルト

デフォルト設定では、パスワードを含めません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、実際の証明書登録を開始する前に、証明書失効パスワードを指定できます。指定されたパスワードは、更新された構成が ASA によって NVRAM に書き込まれるときに暗号化されます。

CA は、通常、チャレンジ フレーズを使用して、その後の失効要求を認証します。

このコマンドがイネーブルの場合、証明書登録時にパスワードを求められません。

例

次に、トラストポイント central に対してクリプト 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 に対する登録要求で CA に登録されたチャレンジ フレーズを指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# password zzxxyy
```

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。

password encryption aes

マスターパスフレーズを使用してパスワードの暗号化を有効にするには、グローバルコンフィギュレーションモードで **password encryption aes** コマンドを使用します。パスワードの暗号化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。

password encryption aes
no password encryption aes

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。

使用上のガイドライン

パスワードの暗号化をトリガーするには、**key config-key password-encrypt** コマンドと **password encryption aes** コマンドの両方を任意の順序で入力する必要があります。**write memory** と入力して、暗号化されたパスワードをスタートアップコンフィギュレーションに保存します。そうしないと、スタートアップコンフィギュレーション内のパスワードが表示されることがあります。マルチコンテキストモードでは、システム実行スペースに **write memory all** を使用してすべてのコンテキストの設定を保存します。後から **no password encryption aes** コマンドを使用してパスワードの暗号化を無効にすると、暗号化された既存のパスワードはすべて変更されず、マスターパスフレーズが存在する限り、暗号化されたパスワードはアプリケーションによって必要に応じて復号されます。

このコマンドを実行できるのは、コンソール、SSH、HTTPS 経由の ASDM などによるセキュア セッションにおいてのみです。

Active/Standby フェールオーバーでパスワードの暗号化を有効化または変更すると、**write standby** が実行され、アクティブな構成がスタンバイユニットに複製されます。この複製が行われない場合、スタンバイユニットの暗号化されたパスワードは、同じパスフレーズを使用している場合でも異なるものになります。構成を複製することで、構成が同じであることが保証されま

す。Active/Standby フェールオーバーの場合は、手動で **write standby** を入力する必要があります。**write standby** は、Active/Active モードでトラフィックの中断を引き起こす場合があります。これは、新しい構成が同期される前に、セカンダリユニットで構成が消去されるためです。**failover active group 1** および **failover active group 2** コマンドを使用してプライマリ ASA ですべてのコンテキストをアクティブにし、**write standby** を入力してから、**no failover active group 2** コマンドを使用してセカンダリユニットにグループ 2 コンテキストを復元する必要があります。

write erase コマンドに続いて reload コマンドを使用すると、マスター パスフレーズを紛失した場合はそのマスター パスフレーズとすべての設定が削除されます。

例

次に、暗号キーの生成に使用するパスフレーズを設定し、パスワード暗号化をイネーブルにする例を示します。

```
ciscoasa
(config)#
 key config-key password-encryption
Old key: bumblebee
New key: haverford
Confirm key: haverford
ciscoasa(config)# password encryption aes
ciscoasa(config)# write memory
```

関連コマンド

コマンド	説明
key config-key password-encryption	暗号キーの生成に使用されるパスフレーズを設定します。
write erase	reload コマンドを続いて使用すると、マスター パスフレーズが紛失された場合にパスフレーズを削除します。

password-history

このコマンドは、**password-policy reuse-interval** コマンドを有効にしたときに **username attributes** コマンドの設定に表示されます。ユーザーはこのコマンドを設定できません。以前のパスワードを暗号化された形式で保存します。

password-history *hash1,hash2,hash3...*

構文の説明

hash1,hash2,hash3, ...	PBKDF2（パスワードベースのキー派生関数2）を使用してハッシュされた以前のパスワードを表示します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザー名属性コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドはユーザーが設定できないため、**password-policy reuse-interval** コマンドを有効にした場合に show コマンドの出力にだけ表示されます。

例

次に、パスワードを 2 回変更してから以前のハッシュされたパスワードを表示する例を示します。

```
ciscoasa(config)# username test password pw1
ciscoasa(config)# show running-config username test
username test password $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
pbkdf2
ciscoasa(config)# username test password pw2
ciscoasa(config)# show running-config username test
username test password $sha512$5000$d8ebNCK2oTyzSiHjSh2T6w==$urDQ/+9sOPwi4IUftWFMcw==
pbkdf2
username test attributes
  password-history $sha512$5000$4tAPQTnL3WG1aa4xrfGMjA==$wbi1ks6eo381Km1qOiwqnQ==
```

```
ciscoasa(config)# username test password pw3
ciscoasa(config)# show running-config username test
username test password $sha512$5000$o8WLa1qnLdp2Js4OlW+NdQ==$4Be4eHtPmOxdpfH6j+F4qQ==
pbkdf2
username test attributes
  password-history
$sha512$5000$d8ebNCK2cIyzSiHjSh2T6w==$urDQ/+9sOPwi4IUftWFMcw==,$sha512$5000$4tAPQInL3WG1aa4xrfGMjA==$wbi1ks6eo381KmlqOiwqrQ==
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa authentication login-history	ローカル **username** のログイン履歴を保存します。
password-history	直前の **username** パスワードを保存します。ユーザーはこのコマンドを設定できません。
password-policy reuse-interval	**username** パスワードの再利用を禁止します。
password-policy username-check	**username** の名前と一致するパスワードを禁止します。
show aaa login-history	ローカル **username** のログイン履歴を表示します。
username	ローカル ユーザーを設定します。

password-management

パスワード管理を有効にするには、トンネルグループ一般属性コンフィギュレーションモードで **password-management** コマンドを使用します。パスワード管理を無効にするには、このコマンドの **no** 形式を使用します。日数をデフォルト値にリセットするには、**password-expire-in-days** キーワードを指定して、このコマンドの **no** 形式を使用します。

password-management [**password-expire-in-days** *days*]
nopassword-management
no password-management password-expire-in-days [*days*]

構文の説明

days	現行のパスワードが失効するまでの日数（0 ～ 180）を指定します。**password-expire-in-days** キーワードを指定する場合、このパラメータは必須です。
password-expire-in-days	（任意）ASA がユーザーに対して失効が迫っている警告を開始してから、現行のパスワードが失効するまでの日数を直後のパラメータが指定していることを示します。このオプションは、LDAP サーバーに対してのみ有効です。詳細については、「Usage Notes」を参照してください。

コマンド デフォルト

デフォルトでは、パスワード管理は行われません。LDAP サーバーに対して **password-expire-in-days** キーワードを指定しない場合、現行のパスワードが失効する前に警告を開始するデフォルトの期間は 14 日です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ一般属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA は、RADIUS および LDAP プロトコルのパスワード管理をサポートしています。「password-expire-in-days」オプションは、LDAP に対してのみサポートされます。

IPsec リモート アクセスと SSL VPN トンネルグループのパスワード管理を設定できます。

password-management コマンドを設定すると、ASA は、リモート ユーザがログインするときに、そのユーザの現在のパスワードの期限切れが迫っている、または期限が切れたことを通知します。それから ASA は、ユーザーがパスワードを変更できるようにします。現行のパスワードが失効していない場合、ユーザーはそのパスワードを使用してログインし続けることができます。

このコマンドは、それらの通知をサポートする AAA サーバー、つまりネイティブの LDAP サーバーおよび RADIUS プロキシとして構成された NT 4.0 または Active Directory サーバーに対して有効です。RADIUS または LDAP 認証が設定されていない場合、ASA ではこのコマンドが無視されます。

（注） MSCHAP をサポートする一部の RADIUS サーバーは、現在 MSCHAPv2 をサポートしていません。このコマンドには MSCHAPv2 が必要なため、ベンダーに問い合わせてください。

ASA のリリース 7.1 以降では、通常、LDAP による認証時または MS-CHAPv2 をサポートする RADIUS コンフィギュレーションによる認証時に、次の接続タイプに対するパスワード管理がサポートされます。

- AnyConnect VPN クライアント（ASA ソフトウェア バージョン 8.0 以降）
- IPsec VPN クライアント
- クライアントレス SSL VPN（ASA ソフトウェア バージョン 8.0 以降）、WebVPN（ASA ソフトウェア バージョン 7.1 ～ 7.2.x）
- SSL VPN フル トンネル クライアント

これらの RADIUS 設定には、ローカル認証の RADIUS、Active Directory/Kerberos Windows DC の RADIUS、NT/4.0 ドメインの RADIUS、LDAP の RADIUS が含まれます。

Kerberos/Active Directory（Windows パスワード）または NT 4.0 ドメインでは、これらの接続タイプのいずれについても、パスワード管理はサポートされません。RADIUS サーバー（Cisco ACS など）は、認証要求を別の認証サーバーにプロキシする場合があります。ただし、ASA からは RADIUS サーバーとのみ通信しているように見えます。

（注） LDAP でパスワードを変更するには、市販の LDAP サーバーごとに独自の方法が使用されています。現在、ASA では Microsoft Active Directory および Sun LDAP サーバーに対してのみ、独自のパスワード管理ロジックを実装しています。

ネイティブ LDAP には、SSL 接続が必要です。LDAP のパスワード管理を実行する前に、SSL 上での LDAP をイネーブルにする必要があります。デフォルトでは、LDAP はポート 636 を使用します。

このコマンドは、パスワードが失効するまでの日数は変更せず、ASA がユーザーに対してパスワード失効の警告を開始してから失効するまでの日数を変更する点に注意してください。

password-expire-in-days キーワードを指定する場合は、日数も指定する必要があります。

このコマンドで日数に 0 を指定すると、このコマンドはディセーブルになります。ASA は、ユーザーに対して失効が迫っていることを通知しませんが、失効後にユーザーはパスワードを変更できます。

（注） RADIUS では、パスワードが変更されることも、パスワードの変更を求められることもありません。

例

次に、WebVPN トンネル グループ「testgroup」について、ユーザーに対して失効が迫っている警告を開始してからパスワードが失効するまでの日数を 90 に設定する例を示します。

```
ciscoasa(config)# tunnel-group testgroup type webvpn
ciscoasa(config)# tunnel-group testgroup general-attributes
ciscoasa(config-tunnel-general)# password-management password-expire-in-days 90
ciscoasa(config-tunnel-general)#
```

次に、IPsec リモート アクセス トンネル グループ「QAgroup」について、ユーザーに対して失効が迫っている警告を開始してからパスワードが失効するまでの日数としてデフォルトの 14 日を使用する例を示します。

```
ciscoasa(config)# tunnel-group QAgroup type ipsec-ra
ciscoasa(config)# tunnel-group QAgroup general-attributes
ciscoasa(config-tunnel-general)# password-management
ciscoasa(config-tunnel-general)#
```

関連コマンド

コマンド	説明
clear configure passwd	ログイン パスワードをクリアします。
passwd	ログイン パスワードを設定します。
radius-with-expiry	RADIUS 認証時のパスワード更新のネゴシエーションをイネーブルにします（廃止）。
show running-config passwd	暗号化された形式でログイン パスワードを表示します。
tunnel-group general-attributes	トンネル グループ一般属性値を設定します。

password-parameter

SSO 認証用にユーザーパスワードを送信する必要がある HTTP POST 要求パラメータの名前を指定するには、AAA サーバー ホスト コンフィギュレーション モードで **password-parameter** コマンドを使用します。これは HTTP フォームのコマンドを使用した SSO です。

password-parameter *string*

（注） HTTP を使用して SSO を正しく設定するには、認証と HTTP 交換についての詳しい実務知識が必要です。

構文の説明

string HTTP POST 要求に含まれるパスワード パラメータの名前。パスワードの最大長は 128 文字です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバー ホスト コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

ASA の WebVPN サーバーは、HTTP POST 要求を使用して、認証 Web サーバーにシングルサインオン認証要求を送信します。必須のコマンド **password-parameter** では、POST 要求に SSO 認証用のユーザー パスワード パラメータを含める必要があることを指定します。

（注） ユーザーは、ログイン時に実際のパスワード値を入力します。このパスワード値は POST 要求に入力され、認証 Web サーバーに渡されます。

例

次に、AAA サーバー ホスト コンフィギュレーション モードで、user_password という名前のパスワード パラメータを指定する例を示します。

```
ciscoasa(config)# aaa-server testgrp1 host example.com
ciscoasa(config-aaa-server-host)# password-parameter user_password
```

関連コマンド

コマンド	説明
action-uri	シングル サインオン認証用のユーザー名およびパスワードを受信するための Web サーバー URI を指定します。
auth-cookie-name	認証クッキーの名前を指定します。
hidden-parameter	認証 Web サーバーと交換するための非表示パラメータを作成します。
start-url	プリログイン クッキーを取得する URL を指定します。
user-parameter	SSO 認証用にユーザー名を送信する必要がある HTTP POST 要求のパラメータの名前を指定します。

password-policy authenticate enable

各自のユーザーアカウントの変更をユーザーに許可するかどうかを指定するには、グローバルコンフィギュレーションモードで **password-policy authenticate enable** コマンドを使用します。対応するパスワードポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

password-policy authenticate enable
no password-policy authenticate 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。

コマンド デフォルト

認証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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

認証が有効な場合、ユーザーは **username** コマンドを使用して各自のパスワードを変更したり、アカウントを削除したりできません。**clear configure username** コマンドを使用して各自のアカウントを削除することもできません。

例

次に、各自のユーザー アカウントの変更をユーザーに許可する例を示します。

```
ciscoasa(config)# password-policy authenticate enable
```

関連コマンド

コマンド	説明
password-policy minimum-changes	新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。
password-policy minimum length	パスワードの最小長を設定します。

コマンド	説明
password-policy minimum-lowercase	パスワードに含める小文字の最小個数を設定します。

password-policy lifetime

現在のコンテキストのパスワードポリシーおよびパスワードの有効期間（日数）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 **password-policy lifetime** コマンドを使用します。対応するパスワードポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

password-policy lifetime *value*
no password-policy lifetime *value*

構文の説明

value パスワードの有効期間を指定します。有効な値の範囲は、0～65535 日です。

コマンド デフォルト

有効期間のデフォルト値は 0 日です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

パスワードには有効期間が指定されています。有効期間の値が 0 日の場合、ローカルユーザーのパスワードは期限切れになりません。ライフタイム有効期間の翌日のAM 12:00 にパスワードの期限が切れることに注意してください。

例

次に、パスワードの有効期間の値を 10 日に設定する例を示します。

```
ciscoasa(config)# password-policy lifetime 10
```

関連コマンド

コマンド	説明
password-policy minimum-changes	新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。
password-policy minimum length	パスワードの最小長を設定します。

コマンド	説明
password-policy minimum-lowercase	パスワードに含める小文字の最小個数を設定します。

password-policy minimum-changes

新しいパスワードと古いパスワードの間で変更する必要がある最小文字数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-changes** コマンドを使用します。対応するパスワードポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

password-policy minimum-changes *value*
no password-policy minimum-changes *value*

構文の説明

value 新規のパスワードと古いパスワードとの間で変更しなければならない文字数を指定します。有効値の範囲は 0 ～ 64 文字です。

コマンド デフォルト

デフォルトの変更文字数は 0 文字です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

新しいパスワードには、現在のパスワードから少なくとも 4 文字は変更される必要があり、現在のパスワードの一部に新しいパスワードが含まれない場合のみ変更されたと見なされます。

例

次に、古いパスワードと新規のパスワードとの間の最小変更文字数を 6 文字に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-changes 6
```

関連コマンド

コマンド	説明
password-policy lifetime	パスワードの有効期間（日数）を設定します。
password-policy minimum-length	パスワードの最小長を設定します。

コマンド	説明
password-policy minimum-lowercase	パスワードに含める小文字の最小個数を設定します。

password-policy minimum-length

パスワードの最小長を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-length** コマンドを使用します。対応するパスワードポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

password-policy minimum-length*value*
no password-policy minimum-length *value*

構文の説明

value	パスワードの最小長を指定します。有効値の範囲は 3 ～ 32 文字です。

コマンド デフォルト

デフォルトの最小長は 3 文字です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

最小長がその他の最小文字数の属性（変更文字、小文字、大文字、数字、特殊文字）の値よりも小さい場合、エラーメッセージが表示され、最小長の値は変更されません。推奨されるパスワードの長さは 8 文字です。

例

次に、パスワードの最小文字数を 8 文字に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-length 8
```

関連コマンド

コマンド	説明
password-policy lifetime	パスワードの有効期間の値（日数）を設定します。
password-policy minimum-changes	古いパスワードと新規のパスワードとの間の最小変更文字数を設定します。
password-policy minimum-lowercase	パスワードに含める小文字の最小個数を設定します。

password-policy minimum-lowercase

パスワードに含める小文字の最小数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-lowercase** コマンドを使用します。対応するパスワードポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

password-policy minimum-lowercase*value*
no password-policy minimum-lowercase*value*

構文の説明

value	パスワードで使用される小文字の最小個数を指定します。有効値の範囲は 0 ～ 64 文字です。

コマンド デフォルト

小文字の最小個数のデフォルト値は 0 で、小文字を含める必要はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、パスワードに含める小文字の最小個数を設定します。有効値の範囲は 0 ～ 64 文字です。

例

次に、パスワードに含める小文字の最小個数を 6 個に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-lowercase 6
```

関連コマンド

コマンド	説明
password-policy lifetime	パスワードの有効期間の値（日数）を設定します。
password-policy minimum-changes	新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。
password-policy minimum-length	パスワードの最小長を設定します。

password-policy minimum-numeric

パスワードに含める数字の最小数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-numeric** コマンドを使用します。対応するパスワードポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

password-policy minimum-numeric *value*
no password-policy minimum-numeric *value*

構文の説明

value パスワードで使用される数字の最小個数を指定します。有効値の範囲は 0 ～ 64 文字です。

コマンド デフォルト

数字の最小個数のデフォルト値は 0 で、数字を含める必要はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、パスワードに含める数字の最小個数を設定します。有効値の範囲は 0 ～ 64 文字です。

例

次に、パスワードに含める数字の最小個数を 8 個に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-numeric 8
```

関連コマンド

コマンド	説明
password-policy lifetime	パスワードの有効期間の値（日数）を設定します。
password-policy minimum-changes	新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。
password-policy minimum-length	パスワードの最小長を設定します。

password-policy minimum-special

パスワードに含める特殊文字の最小数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-special** コマンドを使用します。対応するパスワードポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

password-policy minimum-special *value*
no password-policy minimum-special *value*

構文の説明

value パスワードで使用される特殊文字の最小個数を指定します。有効値の範囲は 0 ～ 64 文字です。

コマンド デフォルト

特殊文字の最小個数のデフォルト値は 0 で、特殊文字を含める必要はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、パスワードに含める特殊文字の最小個数を設定します。特殊文字には、!、@、#、$、%、^、&、*、(、および)。

例

次に、パスワードに含める特殊文字の最小個数を 2 個に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-special 2
```

関連コマンド

コマンド	説明
password-policy lifetime	パスワードの有効期間の値（日数）を設定します。
password-policy minimum-changes	新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。
password-policy minimum-length	パスワードの最小長を設定します。

password-policy minimum-uppercase

パスワードに含める大文字の最小数を設定するには、グローバル コンフィギュレーション モードで **password-policy minimum-uppercase** コマンドを使用します。対応するパスワードポリシー属性をデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

password-policy minimum-uppercase *value*
no password-policy minimum-uppercase *value*

構文の説明

value パスワードで使用される大文字の最小個数を指定します。有効値の範囲は 0 ～ 64 文字です。

コマンド デフォルト

大文字の最小個数のデフォルト値は 0 で、大文字を含める必要はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、パスワードに含める大文字の最小個数を設定します。有効値の範囲は 0 ～ 64 文字です。

例

次に、パスワードに含める大文字の最小個数を 4 個に設定する例を示します。

```
ciscoasa(config)# password-policy minimum-uppercase 4
```

関連コマンド

コマンド	説明
password-policy lifetime	パスワードの有効期間の値（日数）を設定します。
password-policy minimum-changes	新規のパスワードと古いパスワードとの間で変更しなければならない最小文字数を設定します。
password-policy minimum-length	パスワードの最小長を設定します。

password-policy reuse-interval

ローカルユーザー名へのパスワードの再利用を禁止するには、グローバル コンフィギュレーション モードで **password-policy reuse-interval** コマンドを使用します。この制限を削除するには、このコマンドの **no** 形式を使用します。

password-policy reuse-interval *value*
no password-policy reuse-interval [*value*]

構文の説明

value 新しいパスワードを作成するときに使用できない以前のパスワードの数を 2 ～ 7 で設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。

使用上のガイドライン

以前に使用したパスワードと一致しているパスワードの再利用を禁止できます。以前のパスワードは、**password-history** コマンドを使用して、暗号化された形で各 **username** の設定に保存されます。ユーザーはこのコマンドを設定できません。

例

次に、パスワード再利用間隔を 5 に設定する例を示します。

```
ciscoasa(config)# password-policy reuse-interval 5
```

関連コマンド

コマンド	説明
aaa authentication login-history	ローカル **username** のログイン履歴を保存します。
password-history	直前の **username** パスワードを保存します。ユーザーはこのコマンドを設定できません。

コマンド	説明
password-policy reuse-interval	**username** パスワードの再利用を禁止します。
password-policy username-check	**username** の名前と一致するパスワードを禁止します。
show aaa login-history	ローカル **username** のログイン履歴を表示します。
username	ローカル ユーザーを設定します。

password-policy username-check

ユーザー名と一致するパスワードを禁止するには、グローバル コンフィギュレーション モードで **password-policy username-check** コマンドを使用します。この制限を削除するには、このコマンドの **no** 形式を使用します。

password-policy username-check
no password-policy username-check

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.8(1)	このコマンドが追加されました。

使用上のガイドライン

username コマンドの名前と一致するパスワードを禁止できます。

例

次に、ユーザー名の john_crichton に一致しないようにパスワードを制限する例を示します。

```
ciscoasa(config)# password-policy username-check
ciscoasa(config)# username john_crichton password moya privilege 15
ciscoasa(config)# username aeryn_sun password john_crichton privilege 15
ERROR: Password must contain:
ERROR:  a value that complies with the password policy
ERROR: Username addition failed.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
aaa authentication login-history	ローカル **username** のログイン履歴を保存します。

コマンド	説明
password-history	直前の **username** パスワードを保存します。ユーザーはこのコマンドを設定できません。
password-policy reuse-interval	**username** パスワードの再利用を禁止します。
password-policy username-check	**username** の名前と一致するパスワードを禁止します。
show aaa login-history	ローカル **username** のログイン履歴を表示します。
username	ローカル ユーザーを設定します。

password-storage

ユーザーがログインパスワードをクライアントシステムに保存できるようにするには、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ー名コンフィギュレーション モードで **password-storage enable** コマンドを使用します。パスワード保存を無効にするには、**password-storage disable** コマンドを使用します。

実行コンフィギュレーションから password-storage 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、別のグループ ポリシーから password-storage 値を継承できます。

password-storage { **enable** | **disable** }
no password-storage

構文の説明

disable パスワードの保管をディセーブルにします。

enable パスワードの保管をイネーブルにします。

コマンド デフォルト

パスワードの保管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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—
ユーザー名コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

セキュア サイトにあることがわかっているシステム上でのみ、パスワードの保管をイネーブルにしてください。

このコマンドは、ハードウェア クライアントのインタラクティブ ハードウェア クライアント認証または個別ユーザー認証には関係ありません。

例

次に、FirstGroup という名前のグループ ポリシーに対してパスワードの保管をイネーブルにする例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# password-storage enable
```

peer-group

VXLAN クラスタ制御リンクの ASA 仮想 クラスタノードを識別するには、NVE コンフィギュレーション モードで **peer-group** コマンドを使用します。ピア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。

peer-group *network_object_name*
no peer-group *network_object_name*

構文の説明

network_object_name	**object-group network** コマンドによって定義されたネットワークオブジェクトを識別します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Nve コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドが追加されました。

使用上のガイドライン

object-group network コマンドを使用して、ネットワーク オブジェクト グループを作成し、VTEP ピアの IP アドレスを識別します。

VTEP 間の基礎となる IP ネットワークは、VNI インターフェイスが使用するクラスタ制御リンクネットワークから独立しています。VTEP ネットワークには他のデバイスが含まれている場合があり、VTEP ピアが同じサブネット上にない場合もあります。

VTEP 送信元アドレスは、ネットワーク オブジェクト グループのピアの 1 つとして含める必要があります。

例

次に、インラインで定義されたホストを含むネットワーク オブジェクト グループを作成する例を示します。

```
ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object host 10.6.6.51
```

```
ciscoasa(network-object-group)# network-object host 10.6.6.52
ciscoasa(network-object-group)# network-object host 10.6.6.53
ciscoasa(network-object-group)# network-object host 10.6.6.54
```

次の例では、スタンドアロン ネットワーク オブジェクトを参照するネットワーク オブジェクト グループを作成します。

```
ciscoasa(config)# object network xyz
ciscoasa(config-network-object)# range 10.6.6.51 10.6.6.54

ciscoasa(config)# object-group network cluster-peers
ciscoasa(network-object-group)# network-object object xyz
```

次に、インターフェイス GigabitEthernet 0/7 をクラスタ制御リンク VTEP 送信元インターフェイスとして定義し、クラスタ ピア ネットワーク オブジェクト グループをピアグループとして識別する例を示します。

```
interface gigabitethernet 0/7
    nve-only cluster
    nameif ccl
    ip address 10.6.6.51 255.255.255.0
    no shutdown

nve 1
    source-interface ccl
    peer-group cluster-peers

interface vni 1
    segment-id 1000
    vtep-nve 1
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only cluster	クラスタ制御リンクの NVE を指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。

コマンド	説明
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、このNVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNIインターフェイスをVTEP送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスはUDP ポート 4789 への VXLAN トラフィックを受け入れます。

peer-id-validate

ピアの証明書を使用してピアの ID を検証するかどうかを指定するには、トンネルグループ IPSec 属性モードで **peer-id-validate** 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。

peer-id-validate *option*
no peer-id-validate

構文の説明

option 次のいずれかのオプションを指定します。

- **req**：必須
- **cert**：証明書でサポートされている場合
- **nocheck**：チェックしない

コマンド デフォルト

このコマンドのデフォルト設定は、**req** 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

この属性は、すべての IPsec トンネル グループ タイプに適用できます。

例

次に、設定 IPsec コンフィギュレーション モードで、209.165.200.225 という名前の IPsec LAN-to-LAN トンネル グループ用のピア証明書の ID を使用してピアの検証を要求する例を示します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPsec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
```

```
ciscoasa(config-tunnel-ipsec)# peer-id-validate req
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネルグループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

peer ip

ピア VXLAN トンネルエンドポイント（VTEP）の IP アドレスを手動で指定するには、NVE コンフィギュレーションモードで **peer ip** コマンドを使用します。ピア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。

peer ip *ip_address*
no peer ip

構文の説明

ip_address ピア VTEP の IP アドレスを設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Nve コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

ピア IP アドレスを指定した場合、マルチキャスト グループ ディスカバリは使用できません。マルチキャストは、マルチ コンテキスト モードではサポートされていないため、手動設定が唯一のオプションです。VTEP には 1 つのピアのみを指定できます。

例

次に、GigabitEthernet 1/1 インターフェイスを VTEP 送信元インターフェイスとして設定し、ピア IPアドレス 10.1.1.2 を指定する例を示します。

```
ciscoasa(config)# interface gigabitethernet 1/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0
ciscoasa(config-if)# nve 1
ciscoasa(cfg-nve)# source-interface outside
ciscoasa(cfg-nve)# peer ip 10.1.1.2
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN送信元インターフェイスがNVE専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNIインターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ2転送テーブル（MACアドレステーブル）を表示します。
show nve	NVEインターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、このNVEをVXLAN VTEPとして使用するVNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレントモードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。

コマンド	説明
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

perfmon

パフォーマンス情報を表示するには、特権 EXEC モードで **perfmon** コマンドを使用します。

perfmon { **verbose** | **interval** *seconds* | **quiet** | **settings** } [*detail*]

構文の説明

verbose	パフォーマンスモニター情報を ASA コンソールに表示します。
interval *seconds*	コンソールでパフォーマンス表示がリフレッシュされるまでの秒数を指定します。
quiet	パフォーマンス モニター表示をディセーブルにします。
settings	間隔、および quiet と verbose のどちらであるかを表示します。
detail	パフォーマンスに関する詳細情報を表示します。

コマンド デフォルト

seconds は 120 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0	このコマンドのサポートが ASA に追加されました。
7.2(1)	**detail** キーワードのサポートが追加されました。

使用上のガイドライン

perfmon コマンドを使用すると、ASA のパフォーマンスをモニターできます。show perfmon コマンドを使用すると、ただちに情報が表示されます。perfmon verbose コマンドを使用すると、2 分間隔で継続して情報が表示されます。perfmon interval seconds コマンドと perfmon verbose コマンドを組み合わせて使用すると、指定した秒数の間隔で情報が継続して表示されます。

次に、パフォーマンス情報の表示例を示します。

PERFMON STATS:	Current	Average
Xlates	33/s	20/s

Connections	110/s	10/s
TCP Conns	50/s	42/s
WebSns Req	4/s	2/s
TCP Fixup	20/s	15/s
HTTP Fixup	5/s	5/s
FTP Fixup	7/s	4/s
AAA Authen	10/s	5/s
AAA Author	9/s	5/s
AAA Account	3/s	3/s

この情報には、毎秒発生する変換数、接続数、Websense 要求数、アドレス変換数（フィックスアップ数）、AAA トランザクション数が示されます。

例

次に、パフォーマンスモニター統計情報を 30 秒間隔で ASA コンソールに表示する例を示します。

```
ciscoasa(config)# perfmon interval 120
ciscoasa(config)# perfmon quiet
ciscoasa(config)# perfmon settings
interval: 120 (seconds)
quiet
```

関連コマンド

コマンド	説明
show perfmon	パフォーマンス情報を表示します。

periodic

時間範囲機能をサポートする機能に対して、定期的な（週単位の）時間範囲を指定するには、時間範囲コンフィギュレーションモードで**periodic** コマンドを使用します。無効にするには、このコマンドの **no** 形式を使用します。

periodic *days-of-the-week time* **to** ［ *days-of-the-week* ］ *time*
no periodic *days-of-the-week time* **to** ［ *days-of-the-week* ］ *time*

構文の説明

days-of-the-week	（任意）1 番めの days-of-the-week 引数は、関連付けられている時間範囲の有効範囲が開始する日または曜日です。2 番めの days-of-the-week 引数は、関連付けられているステートメントの有効期間が終了する日または曜日です。 この引数は、単一の曜日または曜日の組み合わせです（Monday（月曜日）、Tuesday（火曜日）、Wednesday（水曜日）、Thursday（木曜日）、Friday（金曜日）、Saturday（土曜日）、および Sunday（日曜日））。他に指定できる値は、次のとおりです。 • daily：月曜日～日曜日 • weekdays：月曜日～金曜日 • weekend：土曜日と日曜日 終了の曜日が開始の曜日と同じ場合は、終了の曜日を省略できます。
time	時刻を HH:MM 形式で指定します。たとえば、午前 8 時は 8:00、午後 8 時は 20:00 とします。
to	「開始時刻から終了時刻まで」の範囲を入力するには、**to** キーワードを入力する必要があります。

コマンド デフォルト

periodic コマンドで値を入力しない場合は、ASA へのアクセスが **time-range** コマンドでの定義に従い、ただちに有効になり、常にオンになります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
時間範囲コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

時間ベース ACL を実装するには、**time-range** コマンドを使用して、特定の日時および曜日を定義します。次に、**access-list extended time-range** コマンドを使用して、時間範囲を ACL にバインドします。

periodic コマンドは、時間範囲が有効になるタイミングを指定する 1 つの方法です。**absolute** コマンドを使用して絶対期間を指定する方法もあります。**time-range** グローバル コンフィギュレーション コマンドで時間範囲の名前を指定後、いずれかのコマンドを使用します。**time-range** コマンドごとに、複数の **periodic** エントリを使用できます。

終了の days-of-the-week 値が開始の days-of-the-week 値と同じ場合、終了の days-of-the-week 値を省略できます。

time-range コマンドに **absolute** 値と **periodic** 値の両方が指定されている場合、**periodic** コマンドは **absolute start** 時刻に達した後にのみ評価の対象になり、 **absolute end** 時刻に達すると評価の対象にはなりません。

時間範囲機能は、ASA のシステムクロックに依存しています。ただし、この機能は NTP 同期を使用すると最適に動作します。

例

次に例をいくつか示します。

必要な設定	入力内容
月曜日から金曜日の午前 8:00 ～午後 6:00 のみ	**periodic weekdays 8:00 to 18:00**
毎日午前 8:00 ～午後 6:00 のみ	**periodic daily 8:00 to 18:00**
月曜日午前 8:00 ～金曜日午後 8:00 の 1 分おき	**periodic monday 8:00 to friday 20:00**
週末（土曜日の朝～日曜日の夜）	**periodic weekend 00:00 to 23:59**
土曜日と日曜日の正午～深夜	**periodic weekend 12:00 to 23:59**

次に、月曜日から金曜日の午前 8:00 ～午後 6:00 のみ、ASA へのアクセスを許可する例を示します。

```
ciscoasa(config-time-range)# periodic weekdays 8:00 to 18:00
ciscoasa(config-time-range)#
```

次に、特定の曜日（月曜日、火曜日、および金曜日）の午前 10:30 ～午後 12:30 に、ASA へのアクセスを許可する例を示します。

```
ciscoasa(config-time-range)# periodic Monday Tuesday Friday 10:30 to 12:30
ciscoasa(config-time-range)#
```

関連コマンド

コマンド	説明
absolute	時間範囲が有効になる絶対時間を定義します。
access-list extended	ASA 経由の IP トラフィックを許可または拒否するためのポリシーを設定します。
default	**time-range** コマンドの **absolute** キーワードと **periodic** キーワードをデフォルト設定に戻します。
time-range	時間に基づいて ASA のアクセスコントロールを定義します。

periodic-authentication certificate

定期的な証明書の検証を有効にするには、**periodic-authentication certificate** コマンドを使用します。デフォルトのグループポリシーから設定を継承するには、このコマンドの **no** 形式を使用します。

periodic-authentication certificate <*time in hours*> **none**
no periodic-authentication certificate <*time in hours*> **none**

構文の説明

time in hours	間隔（1 ～ 168 時間）を設定します。
none	定期的な認証がディセーブルになります。

コマンド デフォルト

デフォルトでは、定期的な証明書の検証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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
デフォルト グループ ポリシー コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトグループポリシーの場合、このコマンドはデフォルトで **periodic-authentication certificate none** になります。他のグループ ポリシーの場合は、変更されないかぎり、デフォルト ポリシーから設定が継承されます。

例

```
100(config-group-policy)# periodic-authentication ?
group-policy mode commands/options:
  certificate  Configure periodic certificate authentication
100(config-group-policy)# periodic-authentication certificate ?
group-policy mode commands/options:
  <1-168>  Enter periodic authentication interval in hours
  none     Disable periodic authentication
```

```
100(config-group-policy)# periodic-authentication certificate ?
group-policy mode commands/options:
  <1-168>  Enter periodic authentication interval in hours
  none     Disable periodic authentication
100(config-group-policy)# help periodic-authentication
```

permit-errors

無効なGTPパケットを許可するか、または許可しないと解析が失敗してドロップされるパケットを許可するには、ポリシーマップ パラメータ コンフィギュレーション モードで**permit-errors**コマンドを使用します。デフォルトの動作（無効なパケットまたは解析中に失敗したパケットをすべてドロップする）に戻すには、このコマンドの **no** 形式を使用します。

permit-errors
no permit-errors

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。

コマンド デフォルト

デフォルトでは、無効なパケットまたは解析時に失敗したパケットはすべてドロップされます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

GTP インスペクション ポリシー マップ パラメータで **permit-errors** コマンドを使用すると、無効なパケットやメッセージの検査中にエラーが発生したパケットをドロップせずに、ASA経由で送信できます。

例

次に、無効なパケットや解析中に失敗したパケットを含むトラフィックを許可する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# permit-errors
```

関連コマンド

コマンド	説明
policy-map type inspect gtp	GTP インスペクション ポリシー マップを定義します。
inspect gtp	アプリケーション インスペクションに使用する特定の GTP マップを適用します。

permit-response

GSN または PGW プーリングを設定するには、ポリシー マップ パラメータ コンフィギュレーション モードで permit-response コマンドを使用します。プーリング関係を削除するには、このコマンドの **no** 形式を使用します。

permit-response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*
no permit-response to-object-group *to_obj_group_id* **from-object-group** *from_obj_group_id*

構文の説明

from-object-group *from_obj_group_id*	GSN/PGW エンドポイントを識別するネットワーク オブジェクト グループ。これは、オブジェクトグループ（**object-group** コマンド）である必要があります。これらのエンドポイントは、**to-object-group** に対して要求を送信し、応答を受信できます。 リリース 9.5(1) 以降では、オブジェクト グループは、IPv4 アドレスだけでなく IPv6 アドレスを含むことができます。
to-object-group *to_obj_group_id*	SGSN/SGW を識別するネットワーク オブジェクト グループ。これは、オブジェクトグループ（**object-group** コマンド）である必要があります。これらのアドレスは、**from-object-group** で識別される一連のエンドポイントから応答を受信できます。 リリース 9.5(1) 以降では、オブジェクト グループは、IPv4 アドレスだけでなく IPv6 アドレスを含むことができます。

コマンド デフォルト

ASA は、GTP 要求で指定されていない GSN または PGW からの GTP 応答をドロップします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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 モード	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(4)	このコマンドが追加されました。GTP インスペクションは IPv4 アドレスのみをサポートします。
9.5(1)	IPv6 アドレスのサポートが追加されました。

使用上のガイドライン

ASA が GTP インスペクションを実行する場合、デフォルトで ASA は、GTP 要求で指定されていない GSN または PGW からの GTP 応答をドロップします。これは、GSN または PGW のプール間でロードバランシングを使用して、GPRS の効率とスケーラビリティを高めているときに発生します。

GSN/PGW プーリングを設定し、ロード バランシングをサポートするために、GSN/PGW エンドポイントを指定するネットワーク オブジェクト グループを作成し、これを from-object-group パラメータで指定します。同様に、SGSN/SGW のネットワーク オブジェクト グループを作成し、to-object-group パラメータで選択します。応答を行う GSN/PGW が GTP 要求の送信先 GSN/PGW と同じオブジェクト グループに属しており、応答している GSN/PGW による GTP 応答の送信が許可されている先のオブジェクト グループに SGSN/SGW がある場合に、ASA で応答が許可されます。

ネットワーク オブジェクト グループは、エンドポイントをホスト アドレスまたはエンドポイントを含むサブネットから識別できます。

例

次に、192.168.32.0 ネットワーク上の任意のホストから IP アドレス 192.168.112.57 のホストへの GTP 応答を許可する例を示します。

```
ciscoasa(config)# object-group network gsnpool32
ciscoasa(config-network)# network-object 192.168.32.0 255.255.255.0
ciscoasa(config)# object-group network sgsn1

ciscoasa(config-network)# network-object host 192.168.112.57
ciscoasa(config-network)# exit

ciscoasa(config)# policy-map type inspect gtp gtp-policy

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# permit-response to-object-group sgsn1 from-object-group gsnpool32
```

関連コマンド

コマンド	説明
policy-map type inspect gtp	GTP インスペクション ポリシー マップを定義します。
inspect gtp	アプリケーションインスペクションに使用する特定の GTP マップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

pfs

PFS を無効にするには、グループ ポリシー コンフィギュレーション モードで **pfs enable** コマンドを使用します。PFS を無効にするには、**pfs disable** コマンドを使用します。実行コンフィギュレーションから PFS 属性を削除するには、このコマンドの **no** 形式を使用します。

pfs { **enable** | **disable** }
no pfs

構文の説明

disable	PFS をディセーブルにします。
enable	PFS をイネーブルにします。

コマンド デフォルト

PFS 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

VPN クライアントと ASA の PFS 設定は一致している必要があります。

別のグループポリシーから PFS の値を継承できるようにするには、このコマンドの **no** 形式を使用します。

IPsec ネゴシエーションでは、PFS によって、新しい各暗号キーが以前のいずれのキーとも関連しないことが保証されます。

例

次に、FirstGroup という名前のグループ ポリシーに対して PFS を設定する例を示します。

```
ciscoasa(config)# group-policy FirstGroup attributes
ciscoasa(config-group-policy)# pfs enable
```

phone-proxy（廃止）

電話プロキシインスタンスを設定するには、グローバル コンフィギュレーション モードで **phone-proxy** コマンドを使用します。

電話プロキシインスタンスを削除するには、このコマンドの **no** 形式を使用します。

phone-proxy*phone_proxy_name*
no phone-proxy *phone_proxy_name*

構文の説明

phone_proxy_name	Phone Proxy インスタンスの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
9.4(1)	このコマンドは廃止されました。

使用上のガイドライン

ASA では、電話プロキシインスタンスを 1 つだけ設定できます。

HTTP プロキシ サーバー用に NAT が設定されている場合、IP 電話に関する HTTP プロキシ サーバーのグローバルまたはマッピング IP アドレスは、電話プロキシ コンフィギュレーション ファイルに書き込まれます。

例

次に、 **phone-proxy** コマンドを使用して、電話プロキシインスタンスを設定する例を示します。

```
ciscoasa
(config)# phone-proxy asa_phone_proxy
ciscoasa(config-phone-proxy)# tftp-server address 128.106.254.8 interface outside
ciscoasa
(config-phone-proxy)#
media-termination address
```

```
192.0.2.25
 interface inside
ciscoasa
(config-phone-proxy)#
media-termination address 128.106.254.3 interface outside
ciscoasa(config-phone-proxy)# tls-proxy asa_tlsp
ciscoasa
(config-phone-proxy)#
ctl-file asactl
ciscoasa
(config-phone-proxy)#
cluster-mode nonsecure
ciscoasa
(config-phone-proxy)#
timeout secure-phones 00:05:00
ciscoasa
(config-phone-proxy)#
disable service-settings
```

関連コマンド

コマンド	説明
ctl-file (global)	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file (phone-proxy)	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
tls-proxy	TLS プロキシ インスタンスを設定します。

pim

インターフェイス上で PIM を再び有効にするには、インターフェイス コンフィギュレーション モードで **pim** コマンドを使用します。PIM を無効にするには、このコマンドの **no** 形式を使用します。

pim
no pim

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。

コマンド デフォルト

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM を有効にします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

デフォルトでは、**multicast-routing** コマンドは、すべてのインターフェイスの PIM を有効にします。**pim** コマンドの **no** 形式のみが構成に保存されます。

（注） PIM は、PAT ではサポートされません。PIM プロトコルはポートを使用せず、PAT はポートを使用するプロトコルに対してのみ動作します。

例

次に、選択したインターフェイスで PIM をディセーブルにする例を示します。

```
ciscoasa(config-if)# no pim
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

pim accept-register

PIM 登録メッセージをフィルタリングするように ASA 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 **pim accept-register** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

pim accept-register { **list** *acl* | **route-map** *map-name* }
no pim accept-register

構文の説明

list *acl*	アクセス リストの名前または番号を指定します。このコマンドでは、拡張ホスト ACL のみを使用します。
route-map *map-name*	ルートマップ名を指定します。参照されるルートマップでは、拡張ホスト ACL を使用します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、不正な送信元を RP に登録できないようにするために使用します。不正な送信元が RP に登録メッセージを送信すると、ASA はただちに登録停止メッセージを送り返します。

例

次に、「no-ssm-range」という名前のアクセス リストで定義された送信元からの PIM 登録メッセージを制限する例を示します。

```
ciscoasa(config)# pim accept-register list no-ssm-range
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

pim bidir-neighbor-filter

DF 選出に参加できる双方向対応ネイバーを制御するには、インターフェイス コンフィギュレーション モードで **pim bidir-neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

pim bidir-neighbor-filter *acl*
no pim bidir-neighbor-filter *acl*

構文の説明

acl	アクセス リストの名前または番号を指定します。アクセス リストは、双方向 DF 選出に参加できるネイバーを定義します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。

コマンド デフォルト

すべてのルータは双方向対応であると見なされます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

双方向 PIM では、マルチキャスト ルータで保持するステート情報を減らすことができます。双方向で DF を選定するために、セグメント内のすべてのマルチキャスト ルータが双方向でイネーブルになっている必要があります。

pim bidir-neighbor-filter コマンドを使用すると、すべてのルータのスパースモードドメインへの参加を許可しながら、DF 選出へ参加する必要があるルータを指定することで、スパースモード専用ネットワークから双方向ネットワークへの移行が可能になります。双方向にイネーブルにされたルータは、セグメントに非双方向ルータがある場合でも、それらのルータの中から DF を選定できます。非双方向ルータ上のマルチキャスト境界により、双方向グループから PIM メッセージやデータが双方向サブセット クラウドに出入りできないようにします。

pim bidir-neighbor-filter コマンドが有効になっている場合、ACL で許可されているルータは双方向対応であると見なされます。したがって、次のようにします。

- 許可されたネイバーが双方向対応でない場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向対応である場合、DF 選択は実施されません。
- 拒否されたネイバーが双方向をサポートしない場合、DF 選定が実行される可能性があります。

例

次に、10.1.1.1 を PIM 双方向ネイバーにできる例を示します。

```
ciscoasa(config)# access-list bidir_test permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list bidir_test deny any
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pim bidir-neighbor-filter bidir_test
```

関連コマンド

コマンド	説明
multicast boundary	管理上有効範囲が設定されたマルチキャストアドレスに対してマルチキャスト境界を定義します。
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

pim bsr-border

ブートストラップルータ（BSR）メッセージがインターフェイス経由で送受信されることを防止するには、インターフェイス コンフィギュレーション モードで pim bsr-border コマンドを使用します。

（注） PIM スパース モード（PIM-SM）のドメインの境界インターフェイスには、特にそのインターフェイスによって到達可能な隣接ドメインも PIM-SM を実行している場合、そのドメインとの特定のトラフィックのやりとりを阻止する特別な防止策が必要です。

pim bsr-border
no pim bsr-border

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドがインターフェイスで設定されている場合、PIM バージョン 2 BSR メッセージはインターフェイス経由で送受信されません。2 つのドメイン間で BSR メッセージが交換されないようにするには、このコマンドで別の PIM ドメインに隣接するインターフェイスを設定します。一方のドメインにあるルータは他方のドメインにあるランデブー ポイント（RP）を選択し、その結果ドメイン間でプロトコルが誤動作したり分離が行われない可能性があるため、BSR メッセージを異なるドメイン間で交換しないでください。

（注） このコマンドはマルチキャスト境界をセットアップしません。PIM ドメイン BSR メッセージ境界のみをセットアップします。

例

次に、PIM ドメイン境界となるようにインターフェイスを設定する例を示します。

```
ciscoasa(config)# interface gigabit 0/0
ciscoasa(config-if)# pim bsr-border
ciscoasa(config)# show runn interface gigabitEthernet 0/0
!
interface GigabitEthernet0/0
 nameif outsideA
 security-level 0
 ip address 2.2.2.2 255.255.255.0
 pim bsr-border
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。
pim bsr-candidate	ASA をBSR 候補に設定します。

pim bsr-candidate

ルータがブートストラップ ルータ（BSR）の候補であることをアナウンスするよう設定するには、グローバル コンフィギュレーション モードで pim bsr-candidate コマンドを使用します。ブートストラップ ルータの候補としてのこのルータを削除するには、このコマンドの no 形式を使用します。

pim bsr-candidate *interface-name* [*hash-mask-length* [*priority*]]
no pim bsr-candidate

構文の説明

interface-name	BSR アドレスが取得されるこのルータでのインターフェイス名。このアドレスは、BSR メッセージで送信されます。
hash-mask-length	（任意）PIMv2 ハッシュ機能がコールされる前にグループ アドレスと論理積をとるマスク長（最大 32 ビット）。ハッシュ元が同じであるすべてのグループは、同じランデブー ポイント（RP）に対応します。 たとえば、マスク長が 24 の場合、グループ アドレスの最初の 24 ビットだけが使用されます。ハッシュ マスク長により、1 つの RP を複数のグループで使用できるようになります。 デフォルトのハッシュ マスク長は 0 です。
priority	（任意）BSR（C-BSR）候補のプライオリティ。有効な範囲は 0 ～ 255 です。最高のプライオリティ値を持つ C-BSR が優先されます。プライオリティ値が同じ場合は、IP アドレスがより高位であるルータが BSR となります。 デフォルトのプライオリティは 0 です。

コマンド 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。

デバイスがハッシュ長およびプライオリティなしで BSR 候補として設定されている場合は、デフォルトのハッシュ長（0）とデフォルトのプライオリティ（0）が前提となります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、ブートストラップ メッセージはBSRアドレスとして指定されたインターフェイスのアドレスをつけてすべての PIM ネイバーに送信されます。各ネイバーは、以前のブートストラップ メッセージから受信したアドレスと BSR アドレスを比較します（同じインターフェイスで受信される必要はない）。現在のアドレスが同じかまたはより高位のアドレスである場合、現在のアドレスはキャッシュに格納され、ブートストラップ メッセージは転送されます。それ以外の場合は、ブートストラップ メッセージがドロップされます。

この ASA よりもプライオリティが高い（プライオリティが同じ場合は、より高位の IP アドレスを持つ）とされる他の BSR 候補からブートストラップ メッセージを受信するまで、この ASA は BSR のままです。

例

次に、「内部」インターフェイスで、30 のハッシュ長と 10 のプライオリティにより、ASA をブートストラップ ルータ（C-BSR）候補として設定する例を示します。

```
ciscoasa(config)# pim bsr-candidate inside 30 10
ciscoasa(config)# sh runn pim
pim bsr-candidate inside 30 10
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。
pim bsr-border	ASA を境界 BSR として設定します。

pim dr-priority

指定ルータ選出に使用されるASAでネイバーのプライオリティを設定するには、インターフェイス コンフィギュレーション モードで **pim dr-priority** コマンドを使用します。デフォルトのプライオリティに戻すには、このコマンドの **no** 形式を使用します。

pim dr-priority *number*
no pim dr-priority

構文の説明

number 0 ～ 4294967294 の番号。この番号は、指定ルータを決定するときにデバイスのプライオリティを判断するために使用されます。0 を指定すると、ASA は指定ルータになりません。

コマンド デフォルト

デフォルト値は 1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

インターフェイスでプライオリティ値が最大のデバイスが PIM 指定ルータになります。複数のデバイスで指定ルータのプライオリティが同じである場合は、IP アドレスが最大のデバイスが DR になります。デバイスの hello メッセージに DR-Priority Option が含まれていない場合は、プライオリティが最大のデバイスとして扱われ、指定ルータになります。複数のデバイスで hello メッセージにこのオプションが含まれていない場合は、IP アドレスが最大のデバイスが指定ルータになります。

例

次に、インターフェイスの DR プライオリティを 5 に設定する例を示します。

```
ciscoasa(config-if)# pim dr-priority 5
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

pim hello-interval

PIM hello メッセージの頻度を設定するには、インターフェイス コンフィギュレーション モードで **pim hello-interval** コマンドを使用します。hello-interval を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。

pim hello-interval *seconds*
no pim hello-interval [*seconds*]

構文の説明

seconds	ASA が hello メッセージを送信するまでの待機秒数。有効な値の範囲は 1 ～ 3600 秒です。デフォルト値は 30 秒です。

コマンド デフォルト

間隔のデフォルト値は 30 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、PIM hello 間隔を 1 分に設定する例を示します。

```
ciscoasa(config-if)# pim hello-interval 60
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

pim join-prune-interval

PIM Join/Prune 間隔を設定するには、インターフェイス コンフィギュレーション モードで **pim join-prune-interval** コマンドを使用します。間隔を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。

pim join-prune-interval *seconds*
no pim join-prune-interval [*seconds*]

構文の説明

seconds	ASA が Join/Prune メッセージを送信するまでの待機秒数。有効な値の範囲は、10 ～ 600 秒です。デフォルトは 60 秒です。

コマンド デフォルト

デフォルトの間隔は 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、PIM Join/Prune 間隔を 2 分に設定する例を示します。

```
ciscoasa(config-if)# pim join-prune-interval 120
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

pim neighbor-filter

PIM に参加できるネイバールータを制御するには、インターフェイス コンフィギュレーション モードで **pim neighbor-filter** コマンドを使用します。フィルタリングを削除するには、このコマンドの **no** 形式のコマンドを使用します。

pim neighbor-filter *acl*
no pim neighbor-filter *acl*

構文の説明

acl アクセス リストの名前または番号を指定します。このコマンドでは、標準 ACL だけを使用します。拡張 ACL はサポートされていません。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、PIM に参加できるネイバー ルータを定義します。このコマンドがコンフィギュレーションに存在しない場合、制限はありません。

コンフィギュレーションでこのコマンドを使用するには、マルチキャスト ルーティングおよび PIM がイネーブルである必要があります。マルチキャスト ルーティングをディセーブルにすると、このコマンドはコンフィギュレーションから削除されます。

例

次に、IP アドレスが 10.1.1.1 であるルータをインターフェイス GigabitEthernet 0/2 で PIM ネイバーにする例を示します。

```
ciscoasa(config)# access-list pim_filter permit 10.1.1.1 255.255.255.55
ciscoasa(config)# access-list pim_filter deny any
ciscoasa(config)# interface gigabitEthernet0/2
ciscoasa(config-if)# pim neighbor-filter pim_filter
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

pim old-register-checksum

古いレジスタチェックサム方式を使用するランデブー ポイント（RP）での後方互換性を保つには、グローバル コンフィギュレーション モードで **pim old-register-checksum** コマンドを使用します。PIM RFC 準拠レジスタを生成するには、このコマンドの **no** 形式を使用します。

pim old-register-checksum
no pim old-register-checksum

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。

コマンド デフォルト

ASA は PIM RFC 準拠レジスタを生成します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA ソフトウェアは、Cisco IOS 方式を使用せずに、PIM ヘッダーにチェックサムのあるレジスタメッセージとそれに続く 4 バイトのみを受け入れます。つまり、すべての PIM メッセージタイプについて PIM メッセージ全体を含むレジスタメッセージを受け入れます。**pim old-register-checksum** コマンドを使用すると、Cisco IOS ソフトウェアと互換性のあるレジスタが生成されます。

例

次に、古いチェックサム計算を使用するように ASA を設定する例を示します。

```
ciscoasa(config)# pim old-register-checksum
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

pim rp-address

PIM ランデブーポイント（RP）のアドレスを使用するには、グローバル コンフィギュレーション モードで **pim rp-address** コマンドを使用します。RP 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。

pim rp-address *ip_address* ［ *acl* ］ ［ **bidir** ］
no pim rp-address *ip_address*

構文の説明

acl	（任意）RP とともに使用されるマルチキャスト グループを定義する標準アクセス リストの名前または番号。このコマンドではホスト ACL を使用しないでください。
bidir	（任意）指定したマルチキャスト グループが双方向モードで動作することを指定します。このオプションを指定せずにコマンドを設定した場合、指定したグループは PIM スパース モードで動作します。
ip_address	PIM RP になるルータの IP アドレス。これは、4 分割ドット付き 10 進表記のユニキャスト IP アドレスです。

コマンド デフォルト

PIM RP アドレスは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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

一般的な PIM スパース モード（PIM-SM）内または双方向ドメイン内にあるすべてのルータは、既知の PIM RP アドレスを認識する必要があります。アドレスは、このコマンドを使用してスタティックに設定されます。

（注） ASA では、Auto-RP はサポートされないため、**pim rp-address** コマンドを使用して、RP アドレスを指定する必要があります。

複数のグループにサービスを提供するように単一の RP を設定できます。アクセス リストに指定されているグループ範囲によって、PIM RP のグループ マッピングが決まります。アクセス リストを指定しない場合、グループの RP は IP マルチキャスト グループの範囲（224.0.0.0/4）全体に適用されます。

（注） ASA は、実際の双方向構成とは関係なく、常に双方向機能を PIM hello メッセージ内でアドバタイズします。

例

次に、すべてのマルチキャスト グループに対して PIM RP アドレスを 10.0.0.1 に設定する例を示します。

```
ciscoasa(config)# pim rp-address 10.0.0.1
```

関連コマンド

コマンド	説明
pim accept-register	PIM レジスタ メッセージをフィルタリングするように候補 RP を設定します。

pim spt-threshold infinity

常に共有ツリーを使用し、最短パスツリー（SPT）スイッチオーバーを実行しないようにラストホップルータの動作を変更するには、グローバル コンフィギュレーション モードで **pim spt-threshold infinity** 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。

pim spt-threshold infinity [**group-list** *acl*]
no pim spt-threshold

構文の説明

group-list *acl*	（任意）送信元グループはアクセス リストによって制限されていることを示します。*acl* 引数には、標準 ACL を指定する必要があります。拡張 ACL はサポートされません。

コマンド デフォルト

ラスト ホップ PIM ルータは、デフォルトで最短パスの送信元に切り替わります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

group-list キーワードを使用しない場合、このコマンドはすべてのマルチキャストグループに適用されます。

例

次に、最短パス送信元ツリーに切り替えるのではなく、常に共有ツリーを使用するようにラスト ホップ PIM ルータを設定する例を示します。

```
ciscoasa(config)# pim spt-threshold infinity
```

関連コマンド

コマンド	説明
multicast-routing	ASA でマルチキャストルーティングをイネーブルにします。

ping

指定したインターフェイスから IP アドレスへの接続をテストするには、特権 EXEC モードで **ping** コマンドを使用します。使用できるパラメータは、通常の ICMP ベースの ping と TCP の pingとで異なります。パラメータで指定できない特性などの値の入力を求める場合は、このコマンドをパラメータなしで入力します。

ping [*if_name*] *host* [**repeat** *count*] [**timeout** *seconds*] [**data** *pattern*] [**size** *bytes* [**validate**]
ping tcp [*if_name*] *host port* [**repeat** *count*] [**timeout** *seconds*] [**source** *host port*]
ping

（注） source と port のオプションは、tcp オプションでのみ使用できます。data、size、および validate のオプションは、tcp オプションでは使用できません。

構文の説明

data *pattern*	（オプション、ICMP のみ）16 ビット データ パターン（16 進数形式、0 ～ FFFF）を指定します。デフォルトは 0xabcd です。
host	ping の送信先ホストの IPv4 アドレスまたは名前を指定します。ICMP ping では、IPv6 アドレスも指定できます（TCP ping ではサポートされません）。 ホスト名を使用する場合、ホスト名にはDNS 名、または **name** コマンドで割り当てた名前を使用できます。DNS 名の最大文字数は 128、**name** コマンドで作成した名前の最大文字数は 63 です。DNS 名を使用するように DNS サーバーを設定する必要があります。
if_name	（任意）これは、**nameif** コマンドで設定されているインターフェイス名で、*host* でアクセスできます。指定しない場合、*host* は IP アドレスに解決され、宛先インターフェイスを決定するためにデータルーティングテーブルが参照されます。
port	（TCP のみ）ping を送信するホストの TCP ポート番号（1 ～ 65535）を指定します。
repeat *count*	（任意）ping 要求を繰り返す回数を指定します。デフォルトは 5 分です。
size *bytes*	（オプション、ICMP のみ）データグラム サイズ（バイト単位）を指定します。デフォルトは 100 です。
source *host port*	（オプション、TCP のみ）ping の送信元の特定の IP アドレスおよびポートを指定します（特定のポートを指定しない場合は port=0 を使用します）。ソースアドレスは、パケットのルーティング方法には影響しません。

tcp	（オプション）TCP での接続をテストします（デフォルトは ICMP です）。TCP ping では、SYN パケットを送信し、宛先から SYN-ACK パケットが返されると成功と見なします。TCP ping は同時に複数実行することもできます。
timeout *seconds*	（オプション）タイムアウト間隔（秒数）を指定します。デフォルト値は 2 秒です。
validate	（オプション、ICMP のみ）応答データを検証します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	DNS名のサポートが追加されました。
8.4(1)	**tcp** オプションが追加されました。

使用上のガイドライン

ping コマンドを使用すると、ASA が接続可能か、またはホストがネットワークで使用可能かを判断できます。

通常の ICMP ベースの ping を使用する場合、それらのパケットの送信を禁止する **icmp** ルールがないことを確認してください（ICMP ルールを使用しない場合、すべての ICMP トラフィックが許可されます）。内部ホストから外部ホストに対してICMP でpingを送信するには、次のいずれかを実行します。

- エコー応答の場合は、ICMP **access-list** コマンドを使用します。たとえば、すべてのホストに対して ping アクセスを与えるには、**access-list acl_grp permit icmp any any** コマンドを使用し、**access-group** コマンドを使用してテストするインターフェイスに対して **access-list** コマンドをバインドします。
- **inspect icmp** コマンドを使用して ICMP 検査エンジンを設定します。たとえば、**inspect icmp** コマンドをグローバル サービス ポリシーの **class default_inspection** クラスに追加すると、内部ホストによって開始されるエコー要求に対して、エコー応答は ASA を通過できます。

TCP ping を使用する場合は、指定したポートでの TCP トラフィックの送受信がアクセス ポリシーで許可されている必要があります。

この構成は、**ping** コマンドで生成されたメッセージに対して、ASA が応答したり受け入れたりするために必要です。**ping** コマンドの出力は、応答が受け入れられたかどうかを示します。ホストが応答しない場合は、**ping** コマンドを入力すると、次のようなメッセージが表示されます。

```
ciscoasa(config)# ping 10.1.1.1

Sending 5, 100-byte ICMP Echos to 10.1.1.1, timeout is 2 seconds:
?????
Success rate is 0 percent (0/5)
```

ping パケットをルーティングするために、ASA はデータルーティングテーブルを使用し、データテーブルに一致するルートがない場合にのみ、管理ルーティングテーブルにフォールバックします。コマンドでインターフェイス名を指定すると、ASA はそのインターフェイスを介して ping を送信し、ルート ルックアップを使用しません。TCP ping の送信元 IP アドレスを指定しても、パケットのルーティング方法には影響しません。たとえば、インターフェイスの IP アドレスと一致するように送信元アドレスを手動で指定した場合でも、そのインターフェイスから ping は送信されません。出力インターフェイスは、*if_name* またはルートルックアップによってのみ決定されます。

ASA がネットワークに接続していて、トラフィックを送受信していることを確認するには、**show interface** コマンドを使用します。指定した *if_name* のアドレスは、別の送信元アドレスを指定しない限り、ping の送信元アドレスとして使用されます（TCP ping のみ）。

また、パラメータを指定せずに **ping** を入力して、拡張された ping を実行できますこの場合、キーワードとして指定できない一部の特性などのパラメータの入力が求められます。

例

次に、他の IP アドレスが ASA から認識できるか判断する例を示します。

```
ciscoasa# ping 171.69.38.1
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、DNS 名を使用してホストを指定する例を示します。

```
ciscoasa# ping www.example.com
Sending 5, 100-byte ICMP Echos to www.example.com, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
```

次に、拡張された ping を使用する例を示します。

```
ciscoasa# ping
TCP [n]:
Interface: outside
Target IP address: 171.69.38.1
Repeat count: [5]
Datagram size: [100]
Timeout in seconds: [2]
Extended commands [n]:
```

```
Sweep range of sizes [n]:
Sending 5, 100-byte ICMP Echos to 171.69.38.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/10 ms
The following are examples of the ping tcp command:
ciscoasa# ping
TCP [n]: yes
Interface: dmz
Target IP address: 10.0.0.1
Target IP port: 21
Specify source? [n]: y
Source IP address: 192.168.2.7

Source IP port: [0] 465

Repeat count: [5]
Timeout in seconds: [2] 5

Type escape sequence to abort.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 192.168.2.7 starting port 465, timeout is 5 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa# ping tcp 10.0.0.1 21
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 10.0.0.1 port 21
from 10.0.0.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
ciscoasa# ping tcp 10.0.0.1 21 source 192.168.1.1 2002 repeat 10
Type escape sequence to abort.
Sending 10 TCP SYN requests to 10.0.0.1 port 21
from 192.168.1.1 starting port 2002, timeout is 2 seconds:
!!!!!!!!!!
Success rate is 100 percent (10/10), round-trip min/avg/max = 1/2/2 ms
ciscoasa(config)# ping tcp www.example.com 80
Type escape sequence to abort.
No source specified. Pinging from identity interface.
Sending 5 TCP SYN requests to 74.125.19.103 port 80
from 171.63.230.107, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/4 ms
ciscoasa# ping tcp 192.168.1.7 23 source 192.168.2.7 24966
Type escape sequence to abort.
Source port 24966 in use! Using port 24967 instead.
Sending 5 TCP SYN requests to 192.168.1.7 port 23
from 192.168.2.7 starting port 24967, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms
```

関連コマンド

コマンド	説明
icmp	インターフェイスが終端となる ICMP トラフィックのアクセス ルールを設定します。
show interface	VLAN コンフィギュレーションの情報を表示します。

po - pq

police

QoS ポリシングをクラスマップに適用するには、クラス コンフィギュレーション モードで **police** コマンドを使用します。レート制限を削除するには、このコマンドの **no** 形式を使用します。

police { **output** | **input** } *conform-rate* [*conform-burst*] [**conform-action** [**drop** | **transmit**] [**exceed-action** [**drop** | **transmit**]]]
no police

構文の説明

conform-rate	このトラフィッククラスのレート制限を 8000 ～ 2000000000 ビット/秒の範囲で設定します。ASA 仮想 および Firepower 4100/9300 の場合、範囲は 8000 ～ 100000000000 です。たとえば、トラフィックを 5 Mbps に制限するには、5000000 と入力します。
conform-burst	適合レート値にスロットリングするまでに、持続したバーストで許可された最大瞬間バイト数を 1000 ～ 512000000 バイトの範囲で指定します。ASA 仮想 および Firepower 4100/9300 の場合、範囲は 1000 ～ 25600000000 です。 このパラメータを省略した場合、デフォルト値は conform-rate のバイト数の 1/32 です（つまり、conform-rate が 100,000 の場合、conform-burst のデフォルト値は 100,000/32 = 3,125 です）。conform-rate の単位はビット/秒で、conform-burst の単位はバイト数です。
conform-action [**drop** | **transmit**]	トラフィックがポリシングレートとバーストサイズを下回った場合に実行するアクションを設定します。トラフィックを **drop** または **transmit** できます。デフォルトでは、トラフィックは送信されます。
exceed-action [**drop** | **transmit**]	トラフィックがポリシングレートとバーストサイズを上回った場合に実行するアクションを設定します。ポリシングレートとバーストサイズを上回ったパケットを **drop** または **transmit** できます。デフォルトでは、超過パケットはドロップされます。
input	入力方向のトラフィック フローのポリシングをイネーブルにします。
output	出力方向のトラフィック フローのポリシングをイネーブルにします。

コマンド デフォルト

デフォルトの動作や変数はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	**input** オプションが追加されました。着信方向のトラフィックのポリシングがサポートされます。

使用上のガイドライン

ポリシングは、設定した最大レート（ビット/秒単位）を超えるトラフィックが発生しないようにして、1つのトラフィック フローが全体のリソースを占有しないようにする方法です。トラフィックが最大レートを超えると、ASAは超過した分のトラフィックをドロップします。また、ポリシングでは、許可されるトラフィックの最大単一バーストも設定されます。

ポリシングをイネーブルにするには、Modular Policy Framework を使用して次のように設定します。

1.class-map：ポリシングを実行するトラフィックを指定します。

2.policy-map：各クラスマップに関連付けるアクションを指定します。

- **a.class**：アクションを実行するクラスマップを指定します。
- **b.police**：クラスマップのポリシングを有効にします。

3.service-policy：ポリシーマップをインターフェイスごとに、またはグローバルに割り当てます。

ASA で必要な場合は、個々の QoS 機能を単独で設定できます。ただし、普通は、たとえば一部のトラフィックを優先させて、他のトラフィックによって帯域幅の問題が発生しないようにするために、複数の QoS 機能を ASA に設定します。

次に、インターフェイスごとにサポートされる機能の組み合わせを示します。

- 標準プライオリティキューイング（特定のトラフィックの場合）+ ポリシング（その他のトラフィックの場合）

同じトラフィックのセットに対して、プライオリティキューイングとポリシングを両方設定することはできません。

- トラフィックシェーピング（1 つのインターフェイス上のすべてのトラフィックの場合）+ 階層型プライオリティキューイング（トラフィックのサブセットの場合）。

通常、トラフィックシェーピングをイネーブルにした場合、同じトラフィックに対してはポリシングをイネーブルにしません。ただし、このような設定は ASA では制限されていません。

次のガイドラインを参照してください。

- QoS は単方向に適用されます。ポリシーマップを適用するインターフェイスに出入りする（**input** または **output** を指定したかによって異なる）トラフィックだけが影響を受けます。
- 確立済みのトラフィックが存在するインターフェイスに対して、サービス ポリシーが適用または削除されると、トラフィック ストリームに対して QoS ポリシーは適用または削除されません。そのような接続の QoS ポリシーを適用または削除するには、接続をクリアして再確立する必要があります。**clear conn** コマンドを参照してください。
- to-the-box トラフィックはサポートされません。
- VPN トンネル バイパス インターフェイスとの間のトラフィックはサポートされません。
- トンネル グループ クラス マップを照合する場合、出力ポリシングのみがサポートされます。

例

次に、出力方向の **police** コマンドの例を示します。このコマンドは、適合レートを 100,000 ビット/秒、バースト値を 20,000 バイトに設定します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class-map firstclass
ciscoasa(config-cmap)# class localclass

ciscoasa(config-pmap-c)# police output 100000 20000
ciscoasa(config-cmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

次に、内部 Web サーバーを宛先とするトラフィックにレート制限を実行する例を示します。

```
ciscoasa# access-list http_traffic permit tcp any 10.1.1.0 255.255.255.0 eq 80
ciscoasa# class-map http_traffic
ciscoasa(config-cmap)# match access-list http_traffic
ciscoasa(config-cmap)# policy-map outside_policy
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# police input 56000
ciscoasa(config-pmap-c)# service-policy outside_policy interface outside
ciscoasa(config)#
```

関連コマンド

class	トラフィックの分類に使用するクラス マップを指定します。
clear configure policy-map	すべてのポリシーマップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
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。

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。

policy

CRL の取得元を指定するには、ca-crl コンフィギュレーション モードで **policy** コマンドを使用します。

policy { **static** | **cdp** | **both** }

構文の説明

both CRL 配布ポイントを使用した CRL の取得に失敗した場合は、スタティック CDP を最大 5 つ使用して再試行します。

cdp チェック対象の証明書内に埋め込まれている CDP 拡張を使用します。この場合、ASA は検証対象の証明書の CDP 拡張から最大 5 つの CRL 配布ポイントを取得します。さらに必要に応じて、設定されたデフォルト値を使用して情報を増強します。ASA がプライマリ CDP を使用して CRL を取得するのに失敗した場合は、リストで次に使用可能な CDP を使用して再試行します。再試行は、ASA が CRL を取得するかリストの最後に到達するまで、繰り返されます。

static 最大で 5 つのスタティック CRL 配布ポイントを使用します。このオプションを指定する場合は、**protocol** コマンドを使用して LDAP または HTTP URL も指定します。

コマンド デフォルト

デフォルト設定は**cdp**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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CRL コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、チェック対象の証明書内にある CRL 配布ポイント拡張を使用して CRL 取得を行うように設定し、失敗した場合はスタティック CDP を使用する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
```

```
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# policy both
```

関連コマンド

コマンド	説明
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。
url	CRL 取得用のスタティック URL のリストを作成および維持します。

policy-list

ボーダー ゲートウェイ プロトコル（BGP）のポリシーリストを作成するには、ポリシー マップ コンフィギュレーション モードで **policy-list** コマンドを使用します。ポリシーリストを削除するには、このコマンドの **no** 形式を使用します。

policy-list *policy-list-name* { **permit** | **deny** }
no policy-list *policy-list-name*

構文の説明

policy-list-name	設定するポリシー リストの名前。
permit	条件に一致した場合にアクセスを許可します。
deny	条件に一致した場合にアクセスを拒否します。

コマンド デフォルト

このコマンド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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

ルート マップ内でポリシー リストが参照されると、ポリシー リスト内の match 文すべてが評価され、処理される。1 つのルート マップに 2 つ以上のポリシー リストを設定できる。1 つのルート マップ内で設定された複数のポリシー リストは、AND セマンティクスまたは OR セマンティクスを使用して評価されます。ポリシー リストは、同じルート マップ内にあるがポリシー リストの外で設定されている他の既存の match および set 文とも共存できます。1 つのルート マップ エントリ内で複数のポリシー リストが照合を行う場合、ポリシー リストすべては受信属性だけで照合を行います。

policy-list のサブコマンドを次に示します。

サブコマンド	Details
match as-path [path-list-number]	AS パスを照合します。AS パスのパス リスト番号を複数指定できます。
Match community[community-name][exact-match]	コミュニティ名は必須で、完全一致は任意です。複数の名前を指定できます。
Match interface [interface-name]	複数のインターフェイス名を指定できます。
match metric <0-4294967295>	複数の番号を指定できます。
Match ip address [acl name prefix-list [prefix-listname]]	ACL またはプレフィックス リストの名前を複数指定できます。ただし、1 つのポリシー リストにプレフィックスリストと ACL の両方を含めることはできず、どちらか一方しか指定できません。
Match ip next-hop [acl name | prefix-list [prefix-listname]]	ACL またはプレフィックス リストの名前を複数指定できます。ただし、1 つのポリシー リストにプレフィックスリストと ACL の両方を含めることはできず、どちらか一方しか指定できません。
Match ip route-source [acl name | prefix-list [prefix-listname]]	ACL またはプレフィックス リストの名前を複数指定できます。ただし、1 つのポリシー リストにプレフィックスリストと ACL の両方を含めることはできず、どちらか一方しか指定できません。
Default match	上記のすべての「照合」オプションをデフォルトに設定します。
Help	後続のコマンドのヘルプを表示します。
なし	コマンドの否定です。
終了	ポリシー マップ モードを終了します。

例

次に、AS が 1 でメトリックが 10 のネットワーク プレフィックスをすべて許可するポリシーリストの設定例を示します。

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-1 permit
ciscoasa(config-policy-list)# match as-path 1
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

次に、コミュニティが 20 でメトリックが 10 のトラフィックを許可するポリシー リストの設定例を示します。

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-2 permit
ciscoasa(config-policy-list)# match community 20
```

```
ciscoasa(config-policy-list)# match metric 10
ciscoasa(config-policy-list)# end
```

次に、コミュニティが 20 でメトリックが 10 のトラフィックを拒否するポリシー リストの設定例を示します。

```
ciscoasa(config)#  policy-list POLICY-LIST-NAME-3 deny
ciscoasa(config-policy-list)# match community 20
ciscoasa(config-policy-list)# match metric 10
```

policy-map

モジュラ ポリシー フレームワークを使用する場合、グローバル コンフィギュレーション モードで **policy-map** コマンド（**type** キーワードなし）を使用し、レイヤ 3/4 クラスマップ（**class-map** または **class-map type management** コマンド）で特定したトラフィックにアクションを割り当てます。レイヤ 3/4 ポリシーマップを削除するには、このコマンドの **no** 形式を使用します。

policy-map*name*
no policy-map *name*

構文の説明

name	このポリシー マップの名前を最大 40 文字で指定します。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシーマップですでに使用されている名前は再度使用できません。

コマンド デフォルト

デフォルトでは、すべてのデフォルト アプリケーション インスペクション トラフィックに一致するポリシーがコンフィギュレーションに含まれ、特定のインスペクションがすべてのインターフェイスのトラフィックに適用されます（グローバル ポリシー）。すべてのインスペクションがデフォルトでイネーブルになっているわけではありません。適用できるグローバル ポリシーは 1 つだけなので、グローバル ポリシーを変更する場合は、デフォルトのポリシーを編集するか、デフォルトのポリシーをディセーブルにして新しいポリシーを適用します。（特定の機能では、グローバル ポリシーはインターフェイス ポリシーより優先されます）。

デフォルト ポリシーには、次のアプリケーション インスペクションが含まれます。

- DNS
- FTP
- H323（H225）
- H323（RAS）
- RSH
- RTSP
- ESMTP
- SQLnet
- Skinny（SCCP）
- SunRPC
- XDMCP
- SIP
- NetBios
- TFTP

• IP オプション

デフォルト ポリシー コンフィギュレーションには、次のコマンドが含まれます。

```
class-map inspection_default
 match default-inspection-traffic
policy-map type inspect dns preset_dns_map
 parameters
message-length maximum client auto
message-length maximum 512
dns-guard
protocol-enforcement
nat-rewrite
policy-map global_policy
 class inspection_default
  inspect dns preset_dns_map
  inspect ftp
  inspect h323 h225 _default_h323_map
  inspect h323 ras _default_h323_map
  inspect ip-options _default_ip_options_map
  inspect netbios
  inspect rsh
  inspect rtsp
  inspect skinny
  inspect esmtp _default_esmtp_map
  inspect sqlnet
  inspect sunrpc
  inspect tftp
  inspect sip
  inspect xdmcp
```

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. class-map コマンドまたは **class-map type management** コマンドを使用して、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを指定します。

2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。

3.policy-map コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。

4.service-policy コマンドを使用して、インターフェイスでのアクションをアクティブにします。

ポリシー マップの最大数は 64 ですが、各インターフェイスには、ポリシー マップを 1 つだけ適用できます。同一のポリシー マップを複数のインターフェイスに適用できます。レイヤ 3/4 ポリシーマップ内にある複数のレイヤ 3/4 クラスマップを特定でき（**class** コマンドを参照）、1 つ以上の機能タイプの複数のアクションを各クラスマップに割り当てることができます。

例

次に、接続ポリシーの **policy-map** コマンドの例を示します。このコマンドは、Web サーバー 10.1.1.1 への接続許可数を制限します。

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
 to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラスマップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラスマップと照合されないことを示しています。

```
ciscoasa(config)# class-map telnet_traffic
ciscoasa(config-cmap)# match port tcp eq 23
ciscoasa(config)# class-map ftp_traffic
ciscoasa(config-cmap)# match port tcp eq 21
ciscoasa(config)# class-map tcp_traffic
ciscoasa(config-cmap)# match port tcp range 1 65535
ciscoasa(config)# class-map udp_traffic
ciscoasa(config-cmap)# match port udp range 0 65535
ciscoasa(config)# policy-map global_policy
ciscoasa(config-pmap)# class telnet_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:0:0
ciscoasa(config-pmap-c)# set connection conn-max 100
ciscoasa(config-pmap)# class ftp_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:5:0
ciscoasa(config-pmap-c)# set connection conn-max 50
ciscoasa(config-pmap)# class tcp_traffic
```

```
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、ASA はこの照合を行いません。

NetFlow イベントは、Modular Policy Framework を使用して設定されます。Modular Policy Framework が NetFlow 用に設定されていない場合、イベントはログに記録されません。トラフィックはクラスが設定される順序に基づいて照合されます。一致が検出されると、その他のクラスはチェックされません。NetFlow イベントの場合、コンフィギュレーションの要件は次のとおりです。

- flow-export destination（NetFlow コレクタ）は、その IP アドレスによって一意に識別されます。
- サポートされるイベント タイプは、flow-create、flow-teardown、flow-denied、および all です（前述の 4 つのイベント タイプを含みます）。
- 各コレクタに送信する NetFlow レコードを決定するために NetFlow コレクタおよびフィルタのアドレスを設定するには、**flow-export event-type** {**all** | **flow-create** | **flow-denied** | **flow-update** | **flow-teardown**} **destination** コマンドを使用します。
- flow-export アクションは、インターフェイス ポリシーでサポートされません。
- flow-export アクションがサポートされるのは、**class-default** コマンド、および **match any** コマンドまたは **match access-list** コマンドで使用されるクラスに限られます。
- NetFlow コレクタが定義されていない場合は、コンフィギュレーション アクションは発生しません。
- NetFlow セキュア イベント ロギングのフィルタリングは、順序に関係なく実行されます。

次に、ホスト 10.1.1.1 と 20.1.1.1 の間のすべての NetFlow イベントを送信先 15.1.1.1 にエクスポートする例を示します。

```
ciscoasa(config)# access-list
 flow_export_acl
 permit ip host 10.1.1.1 host 20.1.1.1
ciscoasa(config)# class-map flow_export_classciscoasa(config-cmap)# match access-list
flow_export_aclciscoasa(config)# policy-map global_policyciscoasa(config-pmap)# class
flow_export_classciscoasa(config-pmap-c)# flow-export event-type all destination
15.1.1.1
```

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。

コマンド	説明
clear configure policy-map	すべてのポリシー マップ コンフィギュレーションを削除します。ポリシーマップが **service-policy** コマンドで使用されている場合、そのポリシーマップは削除されません。
class-map	トラフィック クラス マップを定義します。
service-policy	ポリシー マップをインターフェイスに割り当てるか、またはすべてのインターフェイスにグローバルに割り当てます。
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。

policy-map type inspect

モジュラ ポリシー フレームワークを使用する場合、グローバル コンフィギュレーション モードで **policy-map type inspect** コマンドを使用して、アプリケーション トラフィック検査のための特別なアクションを定義します。インスペクション ポリシー マップを削除するには、このコマンドの **no** 形式を使用します。

policy-map type inspect *application policy_map_name*
no policy-map［ **type inspect** *application* ］*policy_map_name*

構文の説明

application	対象とするアプリケーション トラフィックのタイプを指定します。利用可能なタイプは次のとおりです。 • **dcerpc** • **diameter** • **dns** • **esmtp** • **ftp** • **gtp** • **h323** • **http** • **im** • **ip-options** • **ipsec-pass-thru** • **ipv6** • **lisp** • **m3ua** • **mgcp** • **netbios** • **radius-accounting** • **rtsp** • **scansafe** • **sctp** • **sip** • **skinny** • **snmp**
policy_map_name	このポリシー マップの名前を最大 40 文字で指定します。「_internal」または「_default」で始まる名前は予約されており、使用できません。すべてのタイプのポリシー マップで同じ名前スペースが使用されるため、別のタイプのポリシー マップですでに使用されている名前は再度使用できません。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.2(1)	IPv6 インスペクションをサポートするために **ipv6** キーワードが追加されました。
9.0(1)	クラウド Web セキュリティをサポートするために **scansafe** キーワードが追加されました。
9.5(2)	LISP インスペクションをサポートするために **lisp** キーワードが追加されました。
9.5(2)	**diameter** および **sctp** キーワードが追加されました。
9.6(2)	**m3ua** キーワードが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークでは、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。レイヤ 3/4 のポリシーマップ（**policy-map** コマンド）で、**inspect** コマンドを使用して検査エンジンを有効にする場合は、**policy-map type inspect** コマンドで作成されたインスペクション ポリシーマップで定義されているアクションもオプションで有効にできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map はインスペクション ポリシー マップの名前です。

インスペクション ポリシーマップは、ポリシーマップ コンフィギュレーション モードで入力するコマンドのうち、次の 1 つ以上のコマンドで構成されます。インスペクション ポリシーマップで使用できる実際のコマンドは、アプリケーションによって異なります。

- **match** コマンド：**match** コマンドをインスペクション ポリシー マップで直接定義して、アプリケーション固有の基準（URL ストリングなど）とアプリケーション トラフィックを照合できます。次に、一致コンフィギュレーション モードで **drop**、**reset**、**log** などのアクションを有効にします。**match** コマンドを使用できるかどうかは、アプリケーションによって異なります。
- **class** コマンド：このコマンドは、ポリシーマップ内のインスペクション クラス マップを特定します（インスペクション クラス マップの作成については、**class-map type inspect** コマンドを参照してください）。インスペクション クラス マップには、**match** コマンドが含まれます。このコマンドは、ポリシーマップ内のアクションを有効にするアプリケーション固有の基準（URL ストリングなど）とアプリケーション トラフィックを照合します。クラスマップを作成することと、インスペクション ポリシー マップ内で **match** コマ

ンドを直接使用することの違いは、複数の照合結果をグループ化できることと、クラスマップを再使用できることです。

- **parameters** コマンド：パラメータは検査エンジンの動作に影響します。パラメータ コンフィギュレーションモードで使用できるコマンドは、アプリケーションによって異なります。

ポリシーマップでは、複数の **class** または **match** コマンドを指定できます。

一部の **match** コマンドでは、パケット内のテキストと照合する正規表現を指定できます。**regex** コマンドおよび **class-map type regex** コマンド（複数の正規表現をグループ化）を参照してください。

デフォルトのインスペクション ポリシー マップ コンフィギュレーションには、次のコマンドが含まれます。

```
policy-map type inspect dns preset_dns_map
 parameters
 message-length maximum client auto
 message-length maximum 512
 dns-guard
 protocol-enforcement
 nat-rewrite
```

1 つのパケットが複数の異なる **match** コマンドまたは **class** コマンドと一致する場合、ASA のアクション適用順序は、ポリシーマップにアクションが追加された順序ではなく、ASA の内部ルールによって決まります。内部ルールは、アプリケーションのタイプとパケット解析の論理的進捗によって決まり、ユーザーが設定することはできません。HTTP トラフィックの場合、Request Method フィールドの解析が Header Host Length フィールドの解析よりも先に行われ、Request Method フィールドに対するアクションは Header Host Length フィールドに対するアクションより先に行われます。たとえば、次の match コマンドは任意の順序で入力できますが、**match request method get** コマンドが最初に照合されます。

```
ciscoasa(config-pmap)# match request header host length gt 100
ciscoasa(config-pmap-c)# reset
ciscoasa(config-pmap-c)# match request method get
ciscoasa(config-pmap-c)# log
```

アクションがパケットをドロップすると、それ以降のアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** コマンドが一致することはありません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの 2 番目のアクションは実行されます（同じ **match** コマンドに対して **reset**（**drop-connection** など）と **log** アクションの両方を設定できます。その場合、パケットは特定の一致でリセットされる前にログに記録されます）。

パケットは、同じ複数の **match** または **class** コマンドと照合される場合、ポリシーマップ内の各コマンドの順序に従って照合されます。たとえば、ヘッダーの長さが 1001 のパケットの場合は、次に示す最初のコマンドと照合されてログに記録され、それから 2 番目のコマンドと照合されてリセットされます。2 つの **match** コマンドの順序を逆にすると、2 番目の **match** コマンドとの照合前にパケットのドロップと接続のリセットが実行され、ログには記録されません。

```
ciscoasa(config-pmap)# match request header length gt 100
ciscoasa(config-pmap-c)# log
ciscoasa(config-pmap-c)# match request header length gt 1000
ciscoasa(config-pmap-c)# reset
```

クラスマップは、そのクラスマップ内で優先順位が最低の**match**コマンドに基づいて、別のクラスマップまたは**match**コマンドと同じタイプであると判断されます（優先順位は内部ルールに基づいています）。クラスマップに、別のクラスマップと同じタイプの優先順位が最低の**match**コマンドがある場合、そのクラスマップはポリシーマップに追加された順序で照合されます。クラスマップごとに優先順位が最低のコマンドが異なる場合は、優先順位が最高の**match**コマンドを持つクラスマップが最初に照合されます。

使用中のインスペクション ポリシー マップを別のマップ名と交換する場合は、**inspect** *protocol map* コマンドを削除し、新しいマップを使用して再度入力する必要があります。次に例を示します。

```
ciscoasa(config)# policy-map test
ciscoasa(config-pmap)# class sip
ciscoasa(config-pmap-c)# no
 inspect sip sip-map1
ciscoasa(config-pmap-c)# inspect sip sip-map2
```

例

次の例では、HTTP インスペクション ポリシー マップとその関連クラス マップを示します。このポリシー マップは、サービス ポリシーがイネーブルにするレイヤ 3/4 ポリシー マップによってアクティブになります。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
ciscoasa(config)# class-map type regex match-any URLs
ciscoasa(config-cmap)# match
 regex
 example
ciscoasa(config-cmap)# match
 regex
 example2
ciscoasa(config-cmap)# class-map type inspect http match-all http-traffic
ciscoasa(config-cmap)# match req-resp content-type mismatch
ciscoasa(config-cmap)# match request body length gt 1000
ciscoasa(config-cmap)# match not request uri regex class URLs
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# drop-connection log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# parameters
ciscoasa(config-pmap-p)# protocol-violation action log
ciscoasa(config-pmap-p)# policy-map test
ciscoasa(config-pmap)# class test
(a Layer 3/4 class map not shown)
ciscoasa(config-pmap-c)# inspect http http-map1
ciscoasa(config-pmap-c)# service-policy inbound_policy interface outside
```

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。
parameters	インスペクション ポリシー マップのパラメータ コンフィギュレーション モードを開始します。
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。

policy-route

インターフェイスでポリシーベースルーティングを設定するには、インターフェイス コンフィギュレーション モードで **policy-route** コマンドを使用します。

policy-route { **route-map** *route_map_name* | **cost** *value* | **path-monitoring** { **IPv4** | **IPv6** | **auto** | **auto4** | **auto6**
no policy-route { **route-map** *route_map_name* | **cost** *value* | **path-monitoring** { **IPv4** | **IPv6** | **auto** | **auto4** | **auto6**

構文の説明

cost *value*	ポリシーベースルーティング評価のインターフェイスの相対コストを設定します。値は 1 ー 65535 です。デフォルトは 0 です。この値は、コマンドの **no** バージョンを使用してリセットできます。値が小さいほど、プライオリティが高くなります。たとえば、1 は 2 よりも優先されます。
route-map*route_map_name*	ポリシーベースルーティングに使用するルートマップの名前を指定します。
path-monitoring	インターフェイスのピアのモニタリングタイプを設定して、フレキシブルメトリックを収集します。

コマンド デフォルト

デフォルトのルートマップはありません。デフォルトのコストは 0 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。
9.17(1)	**cost** キーワードが追加されました。
9.18(1)	このコマンドは、トラフィックをルーティングするための最適なパスを決定する PBR のパスモニタリング機能を含めるように拡張されました。

使用上のガイドライン

一致基準とすべての match 句を満たす場合のアクションを指定するルートマップを設定したら、**policy-route route-map** コマンドを使用して、特定のインターフェイスに適用します。

ルートマップの基準として **set adaptive-interface cost** を使用する場合は、**policy-route cost** コマンドを使用して、インターフェイスのコストを設定します。

policy-route コストを設定し、ルートマップで **set adaptive-interface cost** コマンドを使用すると、出力トラフィックは、同じインターフェイスコストを持つ任意の選択されたインターフェイス間（アップしていると仮定）でラウンドロビン ロード バランシングされます。コストが異なる場合、コストの高いインターフェイスが、最もコストの低いインターフェイスへのバックアップとして使用されます。

たとえば、2 つの WAN リンクに同じコストを設定すると、これらのリンク間でトラフィックをロードバランシングして、パフォーマンスを向上させることができます。ただし、一方の WAN リンクの帯域幅が他方よりも高い場合は、高帯域幅リンクのコストを 1 に設定し、低帯域幅リンクを2に設定して、高帯域幅リンクがダウンしている場合にのみ低帯域幅リンクを使用します。

例

次に、ポリシーベースルーティングのインターフェイスにルートマップを適用する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmapv4
ciscoasa(config)# show run interface GigabitEthernet0/0
!
interface GigabitEthernet0/0
  nameif inside
  security-level 100
  ip address 192.168.1.1 255.255.255.0
  policy-route route-map testmapv4
!
ciscoasa(config)# show route-map testmapv4
route-map testmapv4, permit, sequence 10
   Match clauses:
       ip address (access-lists): testaclv4
   Set clauses:
               ip next-hop 1.1.1.1
```

次に、不等コストを設定する例、つまり、output1 が優先リンクで、output2 は output1 がダウンしている場合にのみ使用される例を示します。インターフェイス間でロードバランシングを設定するには、等コスト値を設定します。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

パスモニタリング機能は、トラフィックを転送しなくなったルートリンクまたはパスの障害を検出します。脅威防御が RTT、ジッター、パケット損失、平均オピニオン評点（MOS）などの評価指標を収集して、トラフィックを転送するためのベストパスを決定できるようにします。

パスモニタリングを設定するには、**policy-route** コマンドを使用します。ピアゲートウェイから評価指標を収集するためにデバイスが使用する必要があるモニタリングタイプを指定する必要があります。自動オプションの場合、モニタリングのために、デフォルトルートのネクストホップがピアとして使用されます。IPv4が最初に試行され、次に IPv6 が試行されます。VTI インターフェイスの場合、auto オプションはサポートされていません。ピアの IPv4 または IPv6 アドレスを指定する必要があります。

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost              set interface cost
  path-monitoring   Keyword for path monitoring
  route-map         Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D     peer-ipv4
  X:X:X:X::X  peer-ipv6
  auto        Use remote peer IPv4/6 based on config
  auto4       Use only IPv4 address based on config
  auto6       Use only IPv6 address based on config

ciscoasa(config-if)# policy-route path-monitoring auto
```

policy-server-secret（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

SiteMinder SSO サーバーへの認証要求を暗号化するために使用する秘密鍵を設定するには、webvpn sso siteminder コンフィギュレーション モードで **policy-server-secret** コマンドを使用します。秘密鍵を削除するには、このコマンドの **no** 形式を使用します。

policy-server-secret *secret-key*
no policy-server-secret

（注） このコマンドは、SiteMinder SSO 認証で必要です。

構文の説明

secret-key 認証通信を暗号化するために秘密キーとして使用されるストリング。文字の最小数や最大数の制限はありません。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
config-webvpn-sso-siteminder コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングル サインオンは、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスにアクセスできます。まず **sso-server** コマンドを使用して SSO サーバーを作成します。SiteMinder

SSO サーバーの場合、**policy-server-secret** コマンドを使用して ASA と SSO サーバー間の認証通信を保護します。

コマンド引数 *secret-key* は、パスワードと同様に作成、保存、および設定が可能です。このコマンド引数は、**policy-server-secret** コマンドを使用して ASA で設定され、Cisco Java プラグイン認証スキームを使用して SiteMinder Policy Server で設定されます。

このコマンドは、SiteMinder-type の SSO サーバーにのみ適用されます。

例

次に、config-webvpn-sso-siteminder モードで、引数としてランダムなストリングを使用して、SiteMinder SSO サーバー認証通信の秘密キーを作成する例を示します。

```
ciscoasa(config-webvpn)# sso-server my-sso-server type siteminder
ciscoasa(config-webvpn-sso-siteminder)# policy-server-secret @#ET&
ciscoasa(config-webvpn-sso-siteminder)#
```

関連コマンド

コマンド	説明
max-retry-attempts	SSO 認証に失敗した場合に ASA が再試行する回数を設定します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。
sso-server	シングル サインオン サーバーを作成します。
test sso-server	テスト認証要求で SSO サーバーをテストします。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバーの URL を指定します。

policy static sgt

手動で設定した Cisco TrustSec リンクにポリシーを適用するには、CTS 手動インターフェイス コンフィギュレーション モードで **policy static sgt** コマンドを使用します。手動で設定した CTS リンクに対するポリシーを削除するには、このコマンドの **no** 形式を使用します。

policy static sgt *sgt_number*［ **trusted** ］
no policy static sgt *sgt_number*［ **trusted** ］

構文の説明

sgt *sgt_number*	ピアからの着信トラフィックに適用する SGT 番号を指定します。有効な値の範囲は 2 ～ 65519 です。
static	リンクの着信トラフィックに SGT ポリシーを指定します。
trusted	コマンドで SGT が指定されたインターフェイスの入力トラフィックでは、SGT を上書きしてはいけないことを示します。デフォルトは untrusted です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CTS 手動インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドでは、手動で設定した CTS リンクにポリシーを適用します。

制約事項

- 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイスおよび冗長インターフェイスでのみサポートされます。
- BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。

例

次に、レイヤ2SGTインポジション用のインターフェイスをイネーブルにし、インターフェイスが信頼できるかどうかを定義する例を示します。

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# policy static sgt 50 trusted
```

関連コマンド

コマンド	説明
cts manual	レイヤ 2 SGT インポジションをイネーブルにし、CTS 手動インターフェイス コンフィギュレーション モードを開始します。
propagate sgt	インターフェイスでセキュリティグループタグ（**sgt** と呼ばれる）を伝播します。伝搬はデフォルトでイネーブルになっています。

polltime interface

Active/Active フェールオーバー コンフィギュレーションのデータインターフェイス polltime および holdtime を指定するには、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 **polltime interface** 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。

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

構文の説明

holdtime 時刻	（任意）ピア ユニットからの最後に受信した hello メッセージとインターフェイステストの開始との間の時間（計算として）を設定して、インターフェイスの健全性を判断します。また、各インターフェイステストの期間を *holdtime*/16 として設定します。有効な値は 5 ～ 75 秒です。デフォルトは、*polltime* の 5 倍です。*polltime* の 5 倍よりも短い holdtime 値は入力できません。 インターフェイス テストを開始するまでの時間（y）を計算するには、次のようにします。 **1.** x = (*holdtime* /*polltime)/2*、最も近い整数に丸められます。（.4 以下は切り下げ、.5 以上は切り上げ。） **2.** y = x**polltime* たとえば、デフォルトの holdtime は 25 で、polltime が 5 の場合は y は 15 秒です。
interface *time*	hello パケットをピアに送信するまで待機する時間を指定します。有効な値の範囲は、1 ～ 15 秒です。デフォルトは 5 分です。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。

コマンド デフォルト

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは、任意の **holdtime** *time* 値とポーリング時間をミリ秒で指定する機能を含めるように変更されました。

このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。Active/Standby フェールオーバー コンフィギュレーションで **failover polltime interface** コマンドを使用します。

ポーリング時間を短縮すると、ASA で障害を検出し、フェールオーバーをトリガーする速度が速くなります。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。

構成に **polltime unit** コマンドおよび **polltime interface** コマンドの両方を含めることができます。

（注） フェールオーバー設定で、CTIQBE トラフィックが ASA を通過する場合は、ASA のフェールオーバーホールド時間を 30 秒未満にする必要があります。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

次の部分的な例では、フェールオーバー グループで可能な設定を示します。フェールオーバー グループ 1 のデータ インターフェイスのインターフェイス ポーリング時間を 500 ミリ秒に設定し、保持時間を 5 秒に設定します。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# polltime interface msec 500 holdtime 5
ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
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。

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。

poll-timer

ネットワーク オブジェクト グループで定義された完全修飾ドメイン名（FQDN）を解決するために、ASA が DNS サーバーにクエリする期間のタイマーを指定するには、DNS サーバー グループ グローバル コンフィギュレーション モードで **poll-timer** コマンドを使用します（DefaultDNS サーバーグループの場合のみ）。タイマーを削除するには、このコマンドの **no** 形式を使用します。

poll-timer minutes *minutes*
no poll-timer minutes *minutes*

構文の説明

minutes *minutes*	タイマーを分単位で指定します。有効な値は、1 ～ 65535 分です。

コマンド デフォルト

デフォルトでは、DNS タイマーは 240 分または 4 時間です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
DNS サーバーグループ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.4(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、DefaultDNS サーバーグループでのみサポートされます。

このコマンドは、ネットワーク オブジェクト グループで定義された FQDN を解決するために、ASA が DNS サーバーに照会する期間のタイマーを指定します。FQDN は、DNS ポーリング タイマーの期限切れ、または、解決された IP エントリの TTL の期限切れのいずれかが発生した時点で解決されます。

このコマンドは、少なくとも 1 つのネットワーク オブジェクト グループがアクティブ化されている場合にのみ有効です。

例

次に、DNS ポーリング タイマーを 240 分に設定する例を示します。

```
ciscoasa(config)# dns server-group DefaultDNS
ciscoasa(config-dns-server-group)# poll-timer minutes 240
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバー グループを設定できる DNS サーバー グループ モードを開始します。
show running-config dns-server group	既存の DNS サーバー グループ コンフィギュレーションを 1 つまたはすべて表示します。

pop3s（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

POP3S コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **pop3s** コマンドを使用します。POP3S コマンドモードで入力したすべてのコマンドを削除するには、このコマンドの **no** 形式を使用します。

POP3 は、インターネット サーバーが電子メールを受信して保持するために使用するクライアント/サーバー プロトコルです。ユーザー（またはクライアント電子メール レシーバ）は、定期的にメールボックスをチェックして、メールがある場合はそれをダウンロードします。この標準プロトコルは、ほとんどの著名な電子メール製品に組み込まれています。POP3S を使用すると、SSL 接続で電子メールを受信できます。

pop3s
no pop3

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.5(2)	このコマンドは廃止されました。

例

次に、POP3S コンフィギュレーション モードを開始する例を示します。

```
ciscoasa
(config)#
```

```
 pop3s
ciscoasa(config-pop3s)#
```

関連コマンド

コマンド	説明
clear configure pop3s	POP3S コンフィギュレーションを削除します。
show running-config pop3s	POP3S の実行コンフィギュレーションを表示します。

port（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

電子メールプロキシでリッスンするポートを指定するには、適切な電子メール プロキシ コマンド モードで **port** 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。

port *portnum*
no port

構文の説明

portnum	電子メール プロキシで使用するポート。ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

コマンド デフォルト

電子メール プロキシのデフォルト ポートは次のとおりです。

電子メール プロキシ	デフォルト ポート
IMAP4S	993
POP3S	995
SMTPS	988

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
pop3s	• 対応	—	• 対応	—	—
Imap4s	• 対応	—	• 対応	—	—
Smtps	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

リリース	変更内容
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

ローカル TCP サービスとの競合を避けるには、1024 ～ 65535 の範囲にあるポート番号を使用します。

例

次に、IMAP4S 電子メール プロキシ用にポート 1066 を設定する例を示します。

```
ciscoasa
(config)#
 imap4s
ciscoasa(config-imap4s)# port 1066
```

portal-access-rule（廃止）

HTTP ヘッダー内に存在するデータに基づいて、クライアントレス SSL VPN セッションを許可または拒否するグローバルなクライアントレス SSL VPN アクセス ポリシーを設定できます。拒否された場合は、エラー コードがクライアントに返されます。この拒否は、ユーザー認証の前に行われるため、処理リソースの使用が最小限に抑えられます。

portal-access-rule none
no portal-access-rule *priority* [{ **permit** | **deny** [**code** *code*]} { **any** | **user-agent match** *string* }
no portal-access-rule *priority* [{ **permit** | **deny** [**code** *code*]} { **any** | **user-agent match** *string* }]
clear configure webvpn portal-access-rule

構文の説明

none	すべてのポータルアクセスルールを削除します。クライアントレス SSL VPN セッションが HTTP ヘッダーに基づいて制限されません。
priority	ルールのプライオリティ。範囲：1 ～ 65535。
permit	HTTP ヘッダーに基づいてアクセスを許可します。
deny	HTTP ヘッダーに基づいてアクセスを拒否します。
code	返された HTTP ステータス コードに基づいてアクセスを許可または拒否します。デフォルト：403。
code	アクセスを許可するか拒否するかの基準として使用する HTTP ステータス コードの番号。範囲：200 ～ 599。
any	HTTP ヘッダーのすべての文字列を照合します。
user-agent match	HTTP ヘッダーの文字列の比較をイネーブルにします。
string	照合する HTTP ヘッダーの文字列を指定します。検索する文字列をワイルドカード（*）で囲むと、その文字列を含む文字列が照合されます。ワイルドカードを使用しない場合は、完全に一致する文字列だけが照合されます。 （注） 検索文字列でワイルドカードを使用することを推奨します。ワイルドカードを使用しないと、ルールでいずれの文字列も照合されなかったり、想定よりもはるかに少ない文字列しか照合されないことがあります。 スペースを含む文字列を検索する場合は、“*a string*” のように引用符で囲む必要があります。引用符とワイルドカードの両方を使用する場合、検索文字列は、“**a string**” のようになります。
no portal-access-rule	単一のポータル アクセス ルールを削除する場合に使用します。

clear configure webvpn portal-access-rule	portal-access-rule none コマンドと同じです。

コマンド デフォルト

portal-access-rule none

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(5)	このコマンドが ASA 8.2.5 と 8.4(2) で同時に追加されました。
8.4(2)	このコマンドが ASA 8.2.5 と 8.4(2) で同時に追加されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

このチェックは、ユーザー認証の前に実行されます。

例

次に、3 つのポータル アクセス ルールを作成する例を示します。

- ポータル アクセス ルール 1 では、ASA からコード 403 が返され、HTTP ヘッダーに Thunderbird が含まれている場合に、試行されたクライアントレス SSL VPN 接続を拒否します。
- ポータル アクセス ルール 10 では、HTTP ヘッダーに MSIE 8.0（Microsoft Internet Explorer 8.0）が含まれている場合に、試行されたクライアントレス SSL VPN 接続を許可します。
- ポータル アクセス ルール 65535 では、それ以外に試行されたクライアントレス SSL VPN 接続をすべて許可します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# portal-access-rule 1 deny code 403 user-agent match *Thunderbird*
ciscoasa(config-webvpn)# portal-access-rule 10 permit user-agent match "*MSIE 8.0*"
ciscoasa(config-webvpn)# portal-access-rule 65535 permit any
```

（注） HostScan がインストールされている場合、port-access-rule 機能は、ASA が Cisco Secure Desktop ポータルなどのページを開くことを停止しません。Cisco Secure Desktop ポートを回避するには、HostScan をアンインストールする必要があります。

関連コマンド

コマンド	説明
show run webvpn	WebVPN コンフィギュレーションをポータル アクセス ルールもすべて含めて表示します。
show vpn-sessiondb detail webvpn	VPNセッションに関する情報を表示します。このコマンドには、情報を完全または詳細に表示するためのオプションが含まれています。表示するセッションのタイプを指定できる他、情報をフィルタリングおよびソートするためのオプションが用意されています。
debug webvpn request *n*	特定のレベルのデバッグ メッセージのロギングをイネーブルにします。デフォルト：1。範囲：1 ～ 255。

port-channel load-balance

EtherChannel について、ロードバランシング アルゴリズムを指定するには、インターフェイス コンフィギュレーション モードで **port-channel load-balance** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

port-channel load-balance { **dst-ip** | **dst-ip-port** | **dst-mac** | **dst-port** | **src-dst-ip** | **src-dst-ip-port** | **src-dst-mac** | **src-dst-port** | **src-ip** | **src-ip-port** | **src-mac** | **src-port** | **vlan-dst-ip** | **vlan-dst-ip-port** | **vlan-only** | **vlan-src-dst-ip** | **vlan-src-dst-ip-port** | **vlan-src-ip** | **vlan-src-ip-port** }
no port-channel load-balance

構文の説明

dst-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 宛先 IP アドレス
dst-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 宛先 IP アドレス • 接続先ポート
dst-mac	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 宛先 MAC アドレス
dst-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 宛先ポート
src-dst-ip	（デフォルト）パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 IP アドレス • 宛先 IP アドレス

src-dst-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 IP アドレス • 宛先 IP アドレス • 送信元ポート（Source Port） • 接続先ポート
src-dst-mac	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 MAC アドレス • 宛先 MAC アドレス
src-dst-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元ポート • 宛先ポート
src-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 IP アドレス
src-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 IP アドレス • ソース ポート
src-mac	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元 MAC アドレス
src-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • 送信元ポート

vlan-dst-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 宛先 IP アドレス
vlan-dst-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 宛先 IP アドレス（Destination IP address） • 宛先ポート
vlan-only	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN
vlan-src-dst-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 送信元 IP アドレス • 宛先 IP アドレス
vlan-src-dst-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 送信元 IP アドレス • 宛先 IP アドレス • 送信元ポート • 宛先ポート
vlan-src-ip	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 送信元 IP アドレス

vlan-src-ip-port	パケットの次の特性に基づいてインターフェイスにパケットの負荷を分散します。 • VLAN • 送信元 IP アドレス • ソース ポート

コマンド デフォルト

デフォルトは **src-dst-ip** 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。

使用上のガイドライン

ASA では、パケットの送信元および宛先の IP アドレス（**src-dst-ip**）をハッシュすることによって、パケットを EtherChannel 内のインターフェイスに分散します。生成されたハッシュ値をアクティブなリンクの数で割り、そのモジュロ演算で求められた余りの値によってフローの割り当て先のインターフェイスが決まります。*hash_value* **mod** *active_links* の結果が 0 となるパケットはすべて、EtherChannel 内の最初のインターフェイスに送信されます。以降、結果が 1 となるパケットは 2 番目のインターフェイスに、結果が 2 となるパケットは 3 番目のインターフェイスに、というように送信されます。たとえば、15 個のアクティブ リンクがある場合、モジュロ演算では 0 ～ 14 の値が得られます。6 個のアクティブ リンクの場合、値は 0 ～ 5 となり、以降も同様になります。

クラスタリングのスパンド EtherChannel の場合、ロード バランシングは ASA 単位で行われます。たとえば、8 台の ASA にわたるスパンド EtherChannel 内に 32 個のアクティブ インターフェイスがあり、EtherChannel 内の 1 台の ASA あたり 4 個のインターフェイスがある場合、ロード バランシングは 1 台の ASA の 4 個のインターフェイス間でのみ行われます。

アクティブ インターフェイスがダウンし、スタンバイ インターフェイスに置き換えられない場合、トラフィックは残りのリンク間で再バランスされます。失敗はレイヤ 2 のスパニングツリーとレイヤ 3 のルーティング テーブルの両方からマスクされるため、他のネットワーク デバイスへのスイッチオーバーはトランスペアレントです。

例

次に、送信元および宛先のIPアドレスとポートを使用するようにロードバランシング アルゴリズムを設定する例を示します。

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel load-balance src-dst-ip-port
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP情報（トラフィック統計情報、システムID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

port-channel min-bundle

EtherChannel について、ポートチャネル インターフェイスがアクティブになるために必要なアクティブインターフェイスの最小数を指定するには、インターフェイス コンフィギュレーション モードで **port-channel min-bundle** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。

port-channel min-bundle *number*
no port-channel min-bundle

構文の説明

number	ポートチャネル インターフェイスがアクティブになるために必要なアクティブ インターフェイスの最小数を 1 ～ 8 の範囲で指定します。9.2(1) 以降では、1 ～ 16 の範囲で指定できます。

コマンド デフォルト

デフォルトは 1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.2(1)	アクティブ インターフェイスの数が 8 から 16 に増加しました。

使用上のガイドライン

このコマンドは、ポートチャネル インターフェイスに対して入力します。チャネル グループ内のアクティブインターフェイス数がこの値よりも小さい場合、ポートチャネルインターフェイスがダウンし、デバイスレベル フェールオーバーが開始されます。

例

次に、ポートチャネルがアクティブになるために必要なアクティブ インターフェイスの最小数を 2 に設定する例を示します。

```
ciscoasa(config)# interface port-channel 1
ciscoasa(config-if)# port-channel min-bundle 2
```

関連コマンド

コマンド	説明
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

port-channel span-cluster

EtherChannel を ASA クラスタのスパンド EtherChannel として設定するには、インターフェイス コンフィギュレーション モードで **port-channel span-cluster** コマンドを使用します。スパニングを無効にするには、このコマンドの **no** 形式を使用します。

port-channel span-cluster [**vss-load-balance**]
no port-channel span-cluster [**vss-load-balance**]

構文の説明

vss-load-balance （オプション）VSS ロードバランシングをイネーブルにします。ASA を VSS または vPC の 2 台のスイッチに接続する場合は、VSS ロードバランシングを有効にする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。ロードバランシングをイネーブルにする前に、各メンバーインターフェイスに対して **channel-group** コマンドの **vss-id** キーワードを設定する必要があります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

この機能を使用するには、スパンド EtherChannel モード（**cluster interface-mode spanned**）に移行する必要があります。

この機能を使用すると、ユニットあたり 1 つ以上のインターフェイスをグループ化して、クラスタのすべてのユニットに広がる EtherChannel とすることができます。EtherChannel によって、チャネル内の使用可能なすべてのアクティブ インターフェイスのトラフィックが集約されます。スパンド EtherChannel は、ルーテッドとトランスペアレントのどちらのファイアウォール モードでも設定できます。ルーテッド モードでは、EtherChannel は単一の IP アドレスを持つルーテッド インターフェイスとして設定されます。トランスペアレントモードでは、IP アド

レスはインターフェイスではなくブリッジグループに割り当てられます。EtherChannelは初めから、ロードバランシング機能を基本的動作の一部として備えています。

例

次に、tengigabitethernet 0/8インターフェイスを唯一のメンバとするEtherChannel（ポートチャネル2）を作成し、クラスタ全体のスパンドEtherChannelにする例を示します。ポート チャネル 2 に 2 つのサブインターフェイスを追加しています。

```
interface tengigabitethernet 0/8
channel-group 2 mode active
no shutdown
interface port-channel 2
port-channel span-cluster
interface port-channel 2.10
vlan 10
nameif inside
ip address 10.10.10.5 255.255.255.0
ipv6 address 2001:DB8:1::5/64
mac-address 000C.F142.4CDE
interface port-channel 2.20
vlan 20
nameif outside
ip address 209.165.201.1 255.255.255.224
ipv6 address 2001:DB8:2::8/64
mac-address 000C.F142.5CDE
```

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。
cluster interface-mode	クラスタインターフェイスモードを設定します。スパンドEtherChannelまたは個別インターフェイスのどちらかを設定できます。

port-forward（廃止）

クライアントレス SSL VPN セッションのユーザーが転送先 TCP ポートからアクセスできるアプリケーションセットを設定するには、webvpn コンフィギュレーション モードで **port-forward** コマンドを使用します。

port-forward { *list_name local_port remote_server remote_port description* }

複数アプリケーションへのアクセスを設定するには、アプリケーションごとに同じ *list_name* を 1 回ずつ、複数回指定してこのコマンドを使用します。

リストから設定済みアプリケーションを削除するには、**no port-forward** *list_name local_port* コマンドを使用します（*remote_server* and *remote_port* パラメータを指定する必要はありません）。

no port-forward *listname localport*

設定済みのリスト全体を削除するには、**no port-forward** *list_name* コマンドを使用します。

no port-forward *list_name*

構文の説明

description	エンドユーザーのポート フォワーディング Java アプレット画面に表示されるアプリケーション名または短い説明を指定します。最大 64 文字です。
list_name	クライアントレス SSL VPN セッションのユーザーがアクセスできる一連のアプリケーション（転送先 TCP ポート）をグループ化します。最大 64 文字です。
local_port	アプリケーションの TCP トラフィックを受信するローカル ポートを指定します。ローカル ポート番号は *list_name* あたり 1 回のみ使用できます。1 ～ 65535 の範囲のポート番号を入力します。既存サービスとの競合を避けるために、1024 よりも大きいポート番号を使用します。
remote_port	リモート サーバーでこのアプリケーション用に接続するポートを指定します。これは、アプリケーションで使用する実際のポートです。1 ～ 65535 の範囲のポート番号、またはポート名を入力します。
remote_server	アプリケーションのリモート サーバーの DNS 名または IP アドレスを指定します。IP アドレスを入力する場合は、IPv4 形式か IPv6 形式で入力できます。特定の IP アドレス用にクライアント アプリケーションを設定する必要がないように、ホスト名を使用することを推奨します。dns server-group コマンドの **name-server** では、ホスト名を IP アドレスに解決する必要があります。

コマンド デフォルト

デフォルトのポート フォワーディング リストはありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	コマンド モードが webvpn に変更されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

ポート転送は Microsoft Outlook Exchange（MAPI）プロキシをサポートしていません。ただし、Microsoft Outlook Exchange 2010 に対してはスマート トンネルのサポートを設定できます。

例

次の表に、サンプル アプリケーションで使用する値を示します。

アプリケーション	ローカルポート	サーバー DNS 名	リモートポート	説明
IMAP4S 電子メール	20143	IMAP4Sserver	143	メール取得
SMTPS 電子メール	20025	SMTPSserver	25	メール送信
DDTS over SSH	20022	DDTSserver	22	DDTS over SSH
Telnet	20023	Telnetserver	23	Telnet

次に、これらのアプリケーションへのアクセスを提供する *SalesGroupPorts* という名前のポート フォワーディング リストを作成する例を示します。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20143 IMAP4Sserver 143 Get Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20025 SMTPSserver 25 Send Mail
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20022 DDTSserver 22 DDTS over SSH
```

```
ciscoasa
(config-webvpn)#
 port-forward SalesGroupPorts 20023 Telnetserver 23 Telnet
```

関連コマンド

コマンド	説明
port-forward auto-start	このコマンドはグループ ポリシー webvpn またはユーザー名 webvpn モードで入力します。ユーザーがクライアントレス SSL VPN セッションにログインするときに、ポート フォワーディングを自動的に開始して、指定したポート フォワーディング リストを割り当てます。
port-forward enable	このコマンドはグループポリシー webvpn またはユーザー名 Wwebvpn モードで入力します。ユーザーがログインするときに、指定したポートフォワーディング リストを割り当てますが、ポートフォワーディングはユーザーが手動で開始する必要があります。開始するには、クライアントレス SSL VPN ポータルページで [**Application Access**] > [**Start Applications**] ボタンを使用します。
port-forward disable	このコマンドはグループ ポリシー webvpn またはユーザー名 webvpn モードで入力します。ポート フォワーディングをオフにします。

port-forward-name（廃止）

特定のユーザーポリシーやグループポリシーのエンドユーザーに対して TCP ポートフォワーディングを特定する表示名を設定するには、グループポリシーモードまたはユーザー名モードから開始する webvpn モードで **port-forward-name** コマンドを使用します。**port-forward-name none** コマンドを使用して作成したヌル値を含めて、表示名を削除するにはこのコマンドの no 形式を入力します。**,no** オプションを指定すると、デフォルト名「Application Access」が復元されます。表示名を使用しないようにするには、**port-forward none** コマンドを入力します。

port-forward-name { **value** *name* | **none** }
no port-forward-name

構文の説明

none	表示名がないことを指定します。ヌル値を設定して、表示名を拒否します。値は継承しません。
value *name*	エンドユーザーにポート フォワーディングを説明します。最大 255 文字です。

コマンド デフォルト

デフォルトの名前は「Application Access」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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

例

次の例は、FirstGroup という名前のグループ ポリシーに「Remote Access TCP Applications」という名前を設定する方法を示しています。

```
ciscoasa
(config)#
 group-policy FirstGroup attributes
ciscoasa
(config-group-policy)#
```

```
 webvpn
ciscoasa(config-group-webvpn)# port-forward-name value Remote Access TCP Applications
```

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ー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ー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。

port-object

タイプが TCP、UDP、または TCP-UDP のサービスオブジェクトグループにポートオブジェクトを追加するには、オブジェクトグループサービス コンフィギュレーション モードで**port-object** コマンドを使用します。ポートオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

port-object { **eq** *port* | **range** *begin_port end_port* }
no port-object { **eq** *port* | **range** *begin_port end_port* }

構文の説明

range *begin_port end_port*	ポート範囲の開始値と終了値を 0 ～ 65535 の範囲で指定します。
eq *port*	サービス オブジェクトの TCP または UDP ポートの 10 進数（0 ～ 65535）または名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
オブジェクト ネットワーク サービス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

port-object コマンドは、特定のポートまたはポート範囲のオブジェクトを定義するために、**object-group service** *protocol* コマンドと組み合わせて使用します。

TCP または UDP サービスの名前を指定する場合は、サポートされる TCP や UDP のいずれかの名前で、オブジェクト グループのプロトコル タイプと整合性を持つものである必要があります。たとえば、プロトコル タイプが tcp、udp、および tcp-udp の場合、名前はそれぞれ有効な TCP サービス名、有効な UDP サービス名、または有効な TCP および UDP サービス名である必要があります。

番号を指定した場合、オブジェクトが表示されるときに、プロトコルタイプに基づいて、その番号が対応する名前（存在する場合）に変換されます。

次のサービス名がサポートされています。

[TCP]	UDP	TCP および UDP
bgp	biff	discard
chargen	bootpc	domain
cmd	bootps	echo
daytime	dnsix	pim-auto-rp
exec	nameserver	sunrpc
finger	mobile-ip	syslog
ftp	netbios-ns	tacacs
ftp-data	netbios-dgm	talk
gopher	ntp	
ident	rip	
irc	snmp	
h323	snmptrap	
hostname	tftp	
http	time	
klogin	who	
kshell	xdmcp	
login	isakmp	
lpd		
nntp		
pop2		
pop3		
smtp		
sqlnet		
Telnet		
uucp		

[TCP]	UDP	TCP および UDP
whois		
www		

例

次に、新規ポート（サービス）オブジェクトグループを作成するために、サービス コンフィギュレーション モードで **port-object** コマンドを使用する例を示します。

```
ciscoasa(config)# object-group service eng_service tcp
ciscoasa(config-service)# port-object eq smtp
ciscoasa(config-service)# port-object eq telnet
ciscoasa(config)# object-group service eng_service udp
ciscoasa(config-service)# port-object eq snmp
ciscoasa(config)# object-group service eng_service tcp-udp
ciscoasa(config-service)# port-object eq domain
ciscoasa(config-service)# port-object range 2000 2005
ciscoasa(config-service)# quit
```

関連コマンド

コマンド	説明
clear configure object-group	すべての **object-group** コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

post-max-size

アップロードするオブジェクトの最大許容サイズを指定するには、グループポリシー webvpn コンフィギュレーション モードで **post-max-size** コマンドを使用します。このオブジェクト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** バージョンを使用します。

post-max-size *size*
no post-max-size

構文の説明

size ポストするオブジェクトに許可される最大サイズを指定します。指定できる範囲は 0 ～ 2147483647 です。サイズを 0 に設定すると、オブジェクトのポストが実質的に禁止されます。

コマンド デフォルト

デフォルトのサイズは 2147483647 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー webvpn コンフィギュレーション モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、ポストするオブジェクトの最大サイズを 1500 バイトに設定する例を示します。

```
ciscoasa
(config)#

group-policy test attributes
ciscoasa
(config-group-policy)#
 webvpn
ciscoasa
(config-group-webvpn)#
post-max-size 1500
```

関連コマンド

コマンド	説明
download-max-size	ダウンロードするオブジェクトの最大サイズを指定します。
upload-max-size	アップロードするオブジェクトの最大サイズを指定します。
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ー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ー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。

power inline

Firepower 1010 イーサネット 1/7 または 1/8 インターフェイスで Power on Ethernet+（PoE+）を有効または無効にするには、インターフェイス コンフィギュレーション モードで **power inline** コマンドを使用します。デフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

power inline { **auto** | **never** | **consumption wattage** *milliwatts* }

（注） Firepower 1010 でのみサポートされています。Firepower 1010E ではサポートされていません。

構文の説明

consumption wattage *milliwatts*	ワット数をミリワット単位で手動で指定します（4000～30000）。ワット数を手動で設定し、LLDP ネゴシエーションを無効にする場合は、このコマンドを使用します。
auto	給電先デバイスのクラスに適したワット数を使用して、給電先デバイスに自動的に電力を供給します。Firepower 1010 は LLDP を使用して、適切なワット数をさらにネゴシエートします。
never	PoE を無効にします。

コマンド デフォルト

デフォルトは **auto** 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.13(1)	コマンドが追加されました。

使用上のガイドライン

Firepower 1010 は、IEEE 802.3af（PoE）と 802.3at（PoE+）の両方をサポートしています。PoE+ は、Link Layer Discovery Protocol（LLDP）を使用して電力レベルをネゴシエートします。PoE+

は、受電デバイスに最大 30 ワットの電力を提供できます。電力は必要なときのみ供給されます。

インターフェイスをシャットダウンすると、デバイスへの給電が無効になります。Firepower 1010 の場合、イーサネット 1/7 および 1/8 は PoE+ をサポートします。

例

次に、イーサネット 1/7 のワット数を手動で設定し、イーサネット 1/8 の電力を auto に設定する例を示します。

```
ciscoasa(config)# interface ethernet1/7
ciscoasa(config-if)# power inline consumption wattage 10000
ciscoasa(config-if)# interface ethernet1/8
ciscoasa(config-if)# power inline auto
ciscoasa(config-if)#
```

関連コマンド

コマンド	説明
show power inline	PoE ステータスを表示します。

power-supply

ISA 3000 のデュアル電源の場合、デュアル電源を ASA OS で想定される構成として確立するには、グローバル コンフィギュレーション モードで **power-supply** コマンドを使用します。デュアル電源を無効にするには、このコマンドの **no** 形式を使用します。

power-supply dual
no power-supply dual

構文の説明

dual	デュアル電源を指定します。

コマンド デフォルト

デフォルトでは、デュアル電源が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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

1 つの電源に障害が発生すると、ASA はアラームを発します。デフォルトでは、ASA で単一電源が想定されており、装備している電源のいずれかが機能しているかぎりアラームを発しません。

例

次に、デュアル電源を確立する例を示します。

```
ciscoasa(config)# power-supply dual
```

pppoe client route distance

PPPoE を通じて学習したルートにアドミニストレーティブ ディスタンスを設定するには、インターフェイス コンフィギュレーション モードで **pppoe client route distance** 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。

pppoe client route distance *distance*
no pppoe client route distance *distance*

構文の説明

distance PPPoE を介して学習したルートに適用するアドミニストレーティブ ディスタンス。有効な値は、1 ～ 255 です。

コマンド デフォルト

PPPoE を介して学習したルートには、デフォルトで 1 のアドミニストレーティブ ディスタンスが割り当てられます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

pppoe client route distance コマンドは、ルートが PPPoE を通じて学習された場合にのみチェックされます。ルートが PPPoE を通じて学習された後に **pppoe client route distance** コマンドを入力しても、指定したアドミニストレーティブディスタンスは、学習された既存のルートに影響を与えません。指定したアドミニストレーティブディスタンスが設定されるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE でルートを取得するには、**ip address pppoe** コマンドで **setroute** オプションを指定する必要があります。

PPPoE を複数のインターフェイスで設定している場合、インストールされたルートの優先順位を指定するには、各インターフェイスで **pppoe client route distance** コマンドを使用する必要があります。複数のインターフェイスでの PPPoE クライアントのイネーブル化は、オブジェクト トラッキングでのみサポートされています。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニターされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route track	PPPoE により学習したルートを、トラッキング エントリ オブジェクトに関連付けます。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

pppoe client route track

追加ルートをトラッキング済みの指定オブジェクト番号に関連付けるように PPPoE クライアントを設定するには、インターフェイス コンフィギュレーション モードで **pppoe client route track** コマンドを使用します。PPPoE ルートトラッキ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。

pppoe client route track *number*
no pppoe client route track

構文の説明

number トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

pppoe client route track コマンドは、ルートが PPPoE を通じて学習された場合にのみチェックされます。ルートが PPPoE から学習された後で **pppoe client route track** コマンドを入力すると、学習された既存のルートはトラッキングオブジェクトに関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE でルートを取得するには、**ip address pppoe** コマンドで **setroute** オプションを指定する必要があります。

PPPoE を複数のインターフェイスで設定している場合、インストールされたルートの優先順位を指定するには、各インターフェイスで **pppoe client route distance** コマンドを使用する必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングのみでサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニターされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route distance	PPPoE によって学習されたルート アドミニストレーティブ ディスタンスを割り当てます。
sla monitor	SLA モニタリング動作を定義します。
track rtr	SLA をポーリングするためのトラッキング エントリを作成します。

pppoe client secondary

PPPoE クライアントをトラッキング済みオブジェクトのクライアントとして登録し、トラッキング状態に基づいて起動または終了するように設定するには、インターフェイス コンフィギュレーション モードで **pppoe client secondary** コマンドを使用します。クライアントの登録を削除するには、このコマンドの **no** 形式を使用します。

pppoe client secondary track *number*
no pppoe client secondary track

構文の説明

number トラッキング エントリのオブジェクト ID。有効な値は、1 ～ 500 です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

pppoe client secondary コマンドは、PPPoE セッションが開始されたときにのみチェックされます。ルートが PPPoE から学習された後で **pppoe client route track** コマンドを入力すると、学習された既存のルートはトラッキングオブジェクトに関連付けられません。指定したトラッキング オブジェクトに関連付けられるのは、このコマンドの入力後に学習されたルートだけです。

PPPoE でルートを取得するには、**ip address pppoe** コマンドで **setroute** オプションを指定する必要があります。

PPPoE を複数のインターフェイスで設定している場合、インストールされたルートの優先順位を指定するには、各インターフェイスで **pppoe client route distance** コマンドを使用する必要があります。PPPoE クライアントを複数のインターフェイス上でイネーブルにすることは、オブジェクト トラッキングのみでサポートされます。

PPPoE を使用して IP アドレスを取得する場合は、フェールオーバーを設定できません。

例

次に、GigabitEthernet0/2 上で PPPoE によりデフォルト ルートを取得する例を示します。このルートは、トラッキング エントリ オブジェクト 1 によって追跡されます。SLA 動作によって、outside インターフェイスからの 10.1.1.1 ゲートウェイの可用性がモニターされます。この SLA 動作が失敗した場合は、GigabitEthernet0/3 上で PPPoE により取得したセカンダリ ルートが使用されます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# pppoe client route track 1
ciscoasa(config-if)# ip address pppoe setroute
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# pppoe client secondary track 1
ciscoasa(config-if)# pppoe client route distance 254
ciscoasa(config-if)# ip address pppoe setroute
```

関連コマンド

コマンド	説明
ip address pppoe	PPPoE により取得した IP アドレスを使用して、指定したインターフェイスを設定します。
ppoe client secondary	セカンダリ PPPoE クライアント インターフェイスのトラッキングを設定します。
pppoe client route distance	PPPoE によって学習されたルート アドミニストレーティブ ディスタンスを割り当てます。
pppoe client route track	PPPoE により学習したルートを、トラッキング エントリ オブジェクトに関連付けます。
sla monitor	SLA モニタリング動作を定義します。

prc-interval

部分的なルート計算（PRC）の IS-IS スロットリングをカスタマイズするには、ルータ ISIS コンフィギュレーション モードで **prc-interval** 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。

prc-interval *prc-max-wait* ［ *prc-initial-wait prc-second-wait* ］
no prc-interval

構文の説明

prc-max-wait	2 つの連続 PRC 計算の最大間隔を示します。範囲は、1 ～ 120 秒です。
prc-initial-wait	（任意）トポロジ変更後の初期 PRC 計算遅延を示します。値の範囲は 1 ～ 120,000 ミリ秒です。デフォルトは 2000 ミリ秒です。
prc-second-wait	（任意）最初と 2 番めの PRC 計算間のホールド タイム（ミリ秒単位）を示します。値の範囲は 1 ～ 120,000 ミリ秒です。

コマンド デフォルト

デフォルトは、次のとおりです。

prc-max-wait：5 秒

prc-initial-wait：2000 ミリ秒

prc-second-wait：5000 ミリ秒

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

PRC は Shortest Path First（SPF）計算を実行せずにルートを計算するソフトウェア プロセスです。これは、ルーティング システム自体のトポロジが変更されていないものの特定の IS でアナウンスされた情報で変更が検出されたり、そのようなルートをルーティング情報ベース（RIB）に再インストールしようとしたりすることが必要な場合に可能です。

次の説明を参照して、このコマンドのデフォルト値を変更するかどうか決定する際の参考にしてください。

- *prc-initial-wait* 引数は、最初の LSP を生成する前の初期待機時間（ミリ秒）を表します。
- *prc-second-wait* 引数は、最初と 2 番めの LSP 生成間の待機時間（ミリ秒単位）を示します。
- 各後続待機間隔は、*prc-max-wait* 間隔で指定された待機間隔に到達するまで、前の間隔の 2 倍であるため、この値により最初と 2 番めの間隔の後、PRC 計算のスロットリングまたは低下が発生します。最大時間に到達すると、ネットワークが安定するまで、待機時間は最大値のままとなります。
- ネットワークが安定し、*prc-max-wait* 間隔の 2 倍の時間内にトリガーがなければ、高速動作（最初の待機時間）に戻ります。

例

次に、PRC の間隔の例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# prc-interval 2 50 100
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
authentication key	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。

コマンド	説明
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接関係の確立をフィルタ処理します。
isis advertise prefix	IS-IS インターフェイスで、LSP アドバタイズメントを使用して接続中のネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。

コマンド	説明
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。

コマンド	説明
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

pr - pz

pre-fill-username

認証と認可で使用するクライアント証明書からユーザー名を抽出できるようにするには、トンネルグループ webvpn 属性モードで **pre-fill-username** コマンドを使用します。コンフィギュレーションから属性を削除するには、このコマンドの **no** 形式を使用します。

pre-fill-username { **client** | **clientless** }
no pre-fill-username

構文の説明

client **ssl-client**	この機能を AnyConnect VPN クライアント接続でイネーブルにします。9.8(1) 以降では **client** キーワードを使用してください。
clientless	この機能をクライアントレス接続でイネーブルにします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ webvpn 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	このコマンドが追加されました。
9.8(1)	**ssl-client** キーワードが **client** に変更されました。

使用上のガイドライン

pre-fill-username コマンドは、**username-from-certificate** コマンドで指定された証明書フィールドから抽出されたユーザー名を、ユーザー名またはパスワード認証のユーザー名として使用できるようにします。証明書機能からこの事前充填ユーザー名を使用するには、両方のコマンドを設定する必要があります。

この機能を有効にするには、トンネルグループ一般属性モードで **username-from-certificate** コマンドを入力する必要もあります。

例

次に、グローバル コンフィギュレーション モードで、remotegrp という名前の IPsec リモート アクセス トンネル グループを作成し、SSL VPN クライアントの認証または認可クエリーの名前をデジタル証明書から取得する必要があることを指定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp webvpn-attributes
ciscoasa(config-tunnel-webvpn)# pre-fill-username client
ciscoasa(config-tunnel-webvpn)#
```

関連コマンド

コマンド	説明
pre-fill-username	事前入力ユーザー名機能をイネーブルにします。
show running-config tunnel-group	指定されたトンネル グループ コンフィギュレーションを表示します。
tunnel-group general-attributes	名前付きのトンネル グループの一般属性を指定します。
username-from-certificate	認可時のユーザー名として使用する証明書内のフィールドを指定します。

preempt

フェールオーバーグループが優先ユニットでアクティブになるようにするには、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 **preempt** コマンドを使用します。プリエンプションを削除するには、このコマンドの **no** 形式を使用します。

preempt [*delay*]
no preempt [*delay*]

構文の説明

seconds ピアがプリエンプション処理されるまでの待機時間（秒数）。有効な値は、1 ～ 1200 秒です。

コマンド デフォルト

デフォルトでは遅延はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバー グループを優先ユニットでアクティブにする **preempt** コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバー グループが最初に起動するユニットでアクティブになるように変更されました。

使用上のガイドライン

primary または **secondary** 優先順位をフェールオーバーグループに割り当てると、**preempt** コマンドが設定されているときに、フェールオーバーグループがどのユニット上でアクティブになるかが指定されます。グループの **primary** または **secondary** の設定にかかわらず、両方のフェールオーバーグループがブートアップした最初のユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。もう一方のユニットがオンラインになったとき、2 番目のユニットをプライオリティの高いユニットとして所有するフェールオーバーグループは、そのフェールオーバーグループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニッ

トに強制されない限り、2 番めのユニットではアクティブになりません。フェールオーバーグループが **preempt** コマンドで設定される場合、指定されたユニットでフェールオーバーグループが自動的にアクティブになります。

（注） ステートフル フェールオーバーがイネーブルの場合、プリエンプションは、フェールオーバーグループが現在アクティブになっている装置から接続が複製されるまで遅延されます。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どちらのフェールオーバーグループも **preempt** コマンドで待機時間が 100 秒に設定されているため、グループは、ユニットが使用可能になってから 100 秒後に自動的にその優先ユニットでアクティブになります。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
primary	設定対象のフェールオーバー グループに対するフェールオーバー ペア プライオリティにおける、プライマリ ユニットを指定します。
secondary	設定対象のフェールオーバー グループに対するフェールオーバー ペア プライオリティにおける、セカンダリ ユニットを指定します。

prefix-list

OSPFv2、EIGRP、およびBGPプロトコルでは、グローバル コンフィギュレーション モードで **prefix-list** コマンドを使用します。プレフィックスリストのエントリを削除するには、このコマンドの **no** 形式を使用します。

prefix-list*prefix-list-name*［**seq***seq_num*］{ **permit** | **deny** } *network*/*len*［**ge***min_value*］［**le***max_value*］
no prefix-list *prefix-list-name* ［ **seq** *seq_num* ］{ **permit** | **deny** } *network* / *len* ［ **ge** *min_value* ］［ **le** *max_value* ］

構文の説明

/	*network* 値と *len* 値との間に必要な区切り文字。
deny	一致した条件へのアクセスを拒否します。
ge *min_value*	（任意）照会されるプレフィックスの最小の長さを指定します。*min_value* 引数の値は、*len* 引数の値よりも大きく、*max_value* 引数が存在する場合はそれ以下である必要があります。
le *max_value*	（任意）照会されるプレフィックスの最大の長さを指定します。*max_value* 引数の値は、*min_value* 引数が存在する場合はその値以上、*min_value* 引数が存在しない場合は *len* 引数よりも大きい値にする必要があります。
len	ネットワーク マスクの長さ。有効な値は、0 ～ 32 です。
network	ネットワーク アドレス。
permit	一致した条件へのアクセスを許可します。
prefix-list-name	プレフィックス リストの名前。プレフィックス リスト名にスペースを含めることはできません。
seq *seq_num*	（任意）作成するプレフィックス リストに指定されたシーケンス番号を適用します。

コマンド デフォルト

シーケンス番号を指定しない場合、プレフィックス リストの先頭エントリにはシーケンス番号 5 が割り当てられ、その後のエントリのシーケンス番号は 5 ずつ増えていきます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチコンテキストモードのサポートが追加されました。
9.2(1)	BGP のサポートが追加されました。

使用上のガイドライン

prefix-list コマンドは、ABR のタイプ 3 LSA フィルタリングコマンドです。ABR のタイプ 3 LSA フィルタリングは、OSPF を実行している ABR の機能を拡張して、異なる OSPF エリア間のタイプ 3 LSA をフィルタリングします。プレフィックス リストが設定されると、指定したプレフィックスのみがエリア間で送信されます。その他のすべてのプレフィックスは、それぞれの OSPF エリアに制限されます。このタイプのエリア フィルタリングは、OSPF エリアを出入りするトラフィックに対して、またはそのエリアの着信と発信の両方のトラフィックに対して適用できます。

プレフィックスリストの複数のエントリが指定されたプレフィックスと一致する場合、シーケンス番号が最も小さいエントリが使用されます。ASA では、プレフィックスリストの先頭、つまりシーケンス番号が最も小さいエントリから検索が開始されます。一致が見つかると、ASA はリストの残りを検索しません。効率性を高めるため、頻繁に一致するエントリまたは一致しないエントリに、小さいシーケンス番号を手動で割り当てることで、それらをリストの上部に配置することもできます。

デフォルトでは、シーケンス番号は自動的に生成されます。自動生成されるシーケンス番号は、**no prefix-list sequence-number** コマンドで抑制できます。シーケンス番号は、5 ずつ増分されます。プレフィックスリストで生成される最初のシーケンス番号は5です。そのリストの次のエントリにはシーケンス番号 10 が設定され、以降も同様に設定されます。あるエントリに値を指定し、その後のエントリに値を指定しない場合、生成されるシーケンス番号は指定された値から5ずつ増分されます。たとえば、プレフィックスリストの最初のエントリのシーケンス番号を 3 と指定し、その後シーケンス番号を指定しないで 2 つのエントリを追加した場合、これら2つエントリに対して自動的に生成されるシーケンス番号は、8および13となります。

ge キーワードおよび **le** キーワードを使用して、*network*/*len* 引数よりも具体的なプレフィックスに対して一致するプレフィックス長の範囲を指定できます。**ge** または **le** キーワードが指定されていない場合、完全一致であると見なされます。**ge** キーワードのみが指定されている場合の範囲は、*min_value* ～ 32 です。**le** キーワードのみが指定されている場合の範囲は、*len* ～ *max_value* です。

min_value 引数および *max_value* 引数の値は、次の条件を満たす必要があります。

len < *min_value* <= *max_value* <= 32

プレフィックスリストから特定のエントリを削除するには、このコマンドの **no** 形式を使用します。プレフィックスリストを削除するには、**clear configure prefix-list** コマンドを使用します。clear **configure prefix-list** コマンドを使用すると、関連する **prefix-list description** コマンド（ある場合）も構成から削除されます。

例

次に、デフォルト ルート 0.0.0.0/0 を拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0
```

次に、プレフィックス 10.0.0.0/8 を許可する例を示します。

```
ciscoasa(config)# prefix-list abc permit 10.0.0.0/8
```

次に、プレフィックス 192/8 のルートで最大 24 ビットのマスク長を許可する例を示します。

```
ciscoasa(config)# prefix-list abc permit 192.168.0.0/8 le 24
```

次に、プレフィックス 192/8 のルートで 25 ビットよりも大きいマスク長を拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 192.168.0.0/8 ge 25
```

次に、すべてのアドレス空間で 8 ～ 24 ビットのマスク長を許可する例を示します。

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 ge 8 le 24
```

次に、すべてのアドレス空間で25ビットよりも大きいマスク長を拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 0.0.0.0/0 ge 25
```

次に、プレフィックス 10/8 のすべてのルートを拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 10.0.0.0/8 le 32
```

次に、プレフィックス 192.168.1/24 のルートで 25 ビットよりも大きいすべてのマスクを拒否する例を示します。

```
ciscoasa(config)# prefix-list abc deny 192.168.1.0/24 ge 25
```

次に、プレフィックス 0/0 のすべてのルートを許可する例を示します。

```
ciscoasa(config)# prefix-list abc permit 0.0.0.0/0 le 32
```

関連コマンド

コマンド	説明
clear configure prefix-list	実行コンフィギュレーションから **prefix-list** コマンドを削除します。
prefix-list description	プレフィックス リストの説明を入力できます。
prefix-list sequence-number	プレフィックス リストのシーケンス番号付けをイネーブルにします。

コマンド	説明
show running-config prefix-list	実行コンフィギュレーションの **prefix-list** コマンドを表示します。

prefix-list description

プレフィックスリストに説明を追加するには、グローバル コンフィギュレーション モードで **prefix-list description** コマンドを使用します。プレフィックスリストの説明を削除するには、このコマンドの **no** 形式を使用します。

prefix-list*prefix-list-name***description***text*
no prefix-list *prefix-list-name* **description** [*text*]

構文の説明

prefix-list-name	プレフィックス リストの名前。
text	プレフィックスリストの説明テキスト。最大80文字を入力できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

prefix-list および **prefix-list description** コマンドは、特定のプレフィックスリスト名に対して、任意の順序で入力できます。プレフィックスリストの説明を入力する前に、プレフィックスリストを作成する必要はありません。**prefix-list description** コマンドは、コマンドの入力順に関係なく、構成内の関連するプレフィックスリストの前の行に必ず記述されます。

すでに説明が入力されているプレフィックス リスト エントリに対して **prefix-list description** コマンドを入力した場合、新しい説明によって元の説明が置き換えられます。

このコマンドの **no** 形式を使用する場合、テキストの説明を入力する必要はありません。

例

次に、MyPrefixList という名前のプレフィックス リストの説明を追加する例を示します。**show running-config prefix-list** コマンドを実行すると、プレフィックスリストの説明が実行コンフィギュレーションに追加されていても、プレフィックスリスト自体は設定されていないことが示されます。

```
ciscoasa(config)# prefix-list MyPrefixList description A sample prefix list description
ciscoasa(config)# show running-config prefix-list
!
prefix-list MyPrefixList description A sample prefix list description
!
```

関連コマンド

コマンド	説明
clear configure prefix-list	実行コンフィギュレーションから **prefix-list** コマンドを削除します。
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーションの **prefix-list** コマンドを表示します。

prefix-list sequence-number

プレフィックスリストのシーケンス番号付けを有効にするには、グローバル コンフィギュレーション モードで **prefix-list sequence-number** コマンドを使用します。プレフィックスリストのシーケンス番号付けを無効にするには、このコマンドの **no** 形式を使用します。

prefix-list sequence-number

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。

コマンド デフォルト

プレフィックス リストのシーケンス番号付けは、デフォルトでイネーブルです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

コンフィギュレーションには、このコマンドの **no** 形式だけが記述されます。このコマンドの **no** 形式が構成内にある場合、シーケンス番号（手動設定した番号を含む）は構成内の **prefix-list** コマンドから削除され、プレフィックスリストの新しいエントリにシーケンス番号は割り当てられません。

プレフィックスリストのシーケンス番号付けがイネーブルの場合、デフォルトの番号付け方式（5 で始まり、番号が 5 ずつ増分される）を使用して、プレフィックス リストのすべてのエントリにシーケンス番号が割り当てられます。番号付けがディセーブルになる前に、シーケンス番号がプレフィックスリストのエントリに手動で割り当てられた場合、手動で割り当てられた番号が復元されます。自動番号付けがディセーブルのときに手動で割り当てたシーケンス番号も復元されます。ただし、番号付けがディセーブルの間、これらのシーケンス番号は表示されません。

例

次に、プレフィックス リストのシーケンス番号付けをディセーブルにする例を示します。

```
ciscoasa(config)# no prefix-list sequence-number
```

関連コマンド

コマンド	説明
prefix-list	ABR タイプ 3 LSA フィルタリングのプレフィックス リストを定義します。
show running-config prefix-list	実行コンフィギュレーションの **prefix-list** コマンドを表示します。

prf

AnyConnect IPsec 接続に使用する IKEv2 セキュリティ アソシエーション（SA）の疑似乱数関数（PRF）を指定するには、IKEv2 ポリシー コンフィギュレーション モードで prf コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの no 形式を使用します。

prf { **md5** | **sha** | **sha256** | **sha384** | **sha512** }
no prf { **md5** | **sha** | **sha256** | **sha384** | **sha512** }

構文の説明

md5	MD5 アルゴリズムを指定します。
sha	（デフォルト）セキュア ハッシュ アルゴリズム SHA 1 を指定します。
sha256	256 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha384	384 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。
sha512	512 ビットのダイジェストでセキュア ハッシュ アルゴリズム SHA 2 を指定します。

コマンド デフォルト

デフォルトは **sha**（SHA 1）です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。crypto ikev2 policy コマンドを入力後、**prf** コマンドを使用して、SA で使用されるすべての暗号化アルゴリズムのキー関連情報の構築に使用する疑似乱数関数を選択します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
8.4(2)	SHA 2 をサポートするために、sha256、sha384、および sha512 の各キーワードが追加されました。

例

次に、IKEv2 ポリシー コンフィギュレーション モードを開始し、PRF を MD5 に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# prf md5
```

関連コマンド

コマンド	説明
encryption	AnyConnect IPsec 接続に対して IKEv2 SA の暗号化アルゴリズムを指定します。
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
integrity	AnyConnect IPsec 接続に対して IKEv2 SA の ESP 整合性アルゴリズムを指定します。
ライフタイム	AnyConnect IPsec 接続に対して IKEv2 SA の SA ライフタイムを指定します。

primary

preempt コマンドの使用時にフェールオーバーグループの優先ユニットを設定するには、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 **primary** 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。

primary
no primary

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。

コマンド デフォルト

フェールオーバーグループに **primary** または **secondary** が指定されていない場合は、フェールオーバーグループはデフォルトで **primary** に設定されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	以前のバージョンのソフトウェアでは「同時」ブートアップが許可されていたため、フェールオーバー グループを優先ユニットでアクティブにする **preempt** コマンドは必要ありませんでした。しかし、この機能は、両方のフェールオーバー グループが最初に起動するユニットでアクティブになるように変更されました。

使用上のガイドライン

primary または **secondary** 優先順位をフェールオーバーグループに割り当てると、**preempt** コマンドが設定されているときに、フェールオーバーグループがどのユニット上でアクティブになるかが指定されます。グループの **primary** または **secondary** の設定にかかわらず、両方のフェールオーバーグループがブートアップした最初のユニットでアクティブになります（それらが同時に起動したように見える場合でも、一方のユニットが最初にアクティブになります）。もう一方のユニットがオンラインになったとき、2 番目のユニットをプライオリティの高いユニットとして所有するフェールオーバーグループは、そのフェールオーバーグループが **preempt** コマンドで設定されているか、**no failover active** コマンドを使用して手動でもう一方のユニットに強制されない限り、2 番めのユニットではアクティブになりません。フェールオーバーグ

ループが **preempt** コマンドで設定される場合、指定されたユニットでフェールオーバーグループが自動的にアクティブになります。

例

次の例では、プライマリ装置のフェールオーバー グループ 1 をより高いプライオリティに設定し、セカンダリ装置のフェールオーバー グループ 2 をより高いプライオリティに設定します。どのフェールオーバーグループも **preempt** コマンドを使用して設定されているため、これらのグループは、優先するユニットが使用可能になったときにそのユニット上で自動的にアクティブになります。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# exit
ciscoasa(config)# failover group 2
ciscoasa(config-fover-group)# secondary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# mac-address e1 0000.a000.a011 0000.a000.a012

ciscoasa(config-fover-group)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
preempt	優先するユニットが使用可能になったときに、フェールオーバー グループをそのユニット上で強制的にアクティブにします。
secondary	セカンダリ ユニットにプライマリ ユニットよりも高いプライオリティを指定します。

priority（クラス）

QoS プライオリティキューイングを有効にするには、クラス コンフィギュレーション モードで **priority** コマンドを使用します。Voice over IP（VoIP）のように遅延を許容できない重要なトラフィックでは、常に最低レートで送信されるように低遅延キューイング（LLQ）のトラフィックを特定できます。プライオリティの要件を削除するには、このコマンドの **no** 形式を使用します。

（注） このコマンドは、ASA サービス モジュールではサポートされていません。

priority
no priority

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。

コマンド デフォルト

デフォルトの動作や変数はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラス コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

ASA は、次の 2 つのタイプのプライオリティキューイングをサポートしています。

- 標準プライオリティキューイング：標準プライオリティキューイングではインターフェイスでLLQプライオリティキューを使用しますが（**priority-queue** コマンドを参照）、他のすべてのトラフィックは「ベストエフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになる

と、以降のパケットはキューに入ることができず、すべてドロップされます。これはテールドロップと呼ばれます。キューがいっぱいになるのを避けるには、キューのバッファサイズを大きくします。送信キューに入れることのできるパケットの最大数も微調整できます。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。

- 階層型プライオリティキューイング：階層型プライオリティキューイングは、トラフィック シェーピング キュー（**shape** コマンド）を有効にしているインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。階層型プライオリティ キューイングについては、次のガイドラインを参照してください。
- プライオリティ パケットは常にシェープ キューの先頭に格納されるので、常に他の非プライオリティ キュー パケットよりも前に送信されます。
- プライオリティ トラフィックの平均レートがシェープ レートを超えない限り、プライオリティ パケットがシェープ キューからドロップされることはありません。
- IPsec-encrypted パケットの場合、DSCP または先行する設定に基づいてのみトラフィックを照合することができます。
- プライオリティ トラフィック分類では、IPsec-over-TCP はサポートされません。

モジュラ ポリシー フレームワークを使用した QoS の設定

プライオリティ キューイングをイネーブルにするには、モジュラー ポリシー フレームワークを使用します。標準プライオリティ キューイングまたは階層型プライオリティ キューイングを使用できます。

標準プライオリティ キューイングの場合は、次の作業を実行します。

1.class-map：プライオリティキューイングを実行するトラフィックを指定します。

2.policy-map：各クラスマップに関連付けるアクションを指定します。

- **a.class**：アクションを実行するクラスマップを指定します。
- **b.priority**：クラスマップのプライオリティキューイングを有効にします。

3.service-policy：ポリシーマップをインターフェイスごとに、またはグローバルに割り当てます。

階層型プライオリティ キューイングの場合は、次の作業を実行します。

1.class-map：プライオリティキューイングを実行するトラフィックを指定します。

2.policy-map（プライオリティキューイングの場合）：各クラスマップに関連付けるアクションを指定します。

- **a.class**：アクションを実行するクラスマップを指定します。

- **b.priority**：クラスマップのプライオリティキューイングを有効にします。ポリシー マップを階層的に使用する場合は、このポリシー マップに priority コマンドだけを含めることができます。

3.policy-map（トラフィックシェーピングの場合）：**class-default** クラスマップに関連付けるアクションを指定します。

- **a.class class-default**：アクションを実行する **class-default** クラスマップを指定します。
- **b.shape**：トラフィックシェーピングをクラスマップに適用します。
- **c.service-policy**：プライオリティキューイングをシェーピングされたトラフィックのサブセットに適用できるように、**priority** コマンドを設定したプライオリティ キューイング ポリシー マップを呼び出します。

4.service-policy：ポリシーマップをインターフェイスごとに、またはグローバルに割り当てます。

例

次に、ポリシー マップ コンフィギュレーション モードでの **priority** コマンドの例を示します。

```
ciscoasa(config)# policy-map localpolicy1
ciscoasa(config-pmap)# class firstclass
ciscoasa(config-pmap-c)# priority
ciscoasa(config-pmap-c)# class class-default
ciscoasa(config-pmap-c)#
```

関連コマンド

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。
clear configure policy-map	すべてのポリシーマップ コンフィギュレーションを削除します。ただし、ポリシー マップが service-policy コマンド内で使用されている場合、そのポリシー マップは削除されません。
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。
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。

priority（クラスタ グループ）

ASA クラスタにおけるこのユニットのマスターユニット選定に関するプライオリティを設定するには、クラスタ コンフィギュレーション モードで **priority** コマンドを使用します。プライオリティを削除するには、このコマンドの **no** 形式を使用します。

priority *priority_number*
no priority [*priority_number*]

構文の説明

priority_number	マスター ユニット選定用に、このユニットのプライオリティを 1 ～ 100 の範囲内で設定します。1 が最高のプライオリティです。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスタ グループ コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

クラスタのメンバは、クラスタ制御リンクを介して通信してマスターユニットを選定します。方法は次のとおりです。

1. ユニットに対してクラスタリングをイネーブルにしたとき（または、クラスタリングがイネーブル済みの状態でそのユニットを初めて起動したとき）に、そのユニットは選定要求を 3 秒間隔でブロードキャストします。

2. プライオリティの高い他のユニットがこの選定要求に応答します。プライオリティは 1 ～ 100 の範囲内で設定され、1 が最高のプライオリティです。

3. 45 秒経過しても、プライオリティの高い他のユニットからの応答を受信していない場合は、そのユニットがマスターになります。

（注） 最高のプライオリティを持つユニットが複数ある場合は、クラスタユニット名、次にシリアル番号を使用してマスターが決定されます。

4. 後からクラスタに参加したユニットのプライオリティの方が高い場合でも、そのユニットが自動的にマスターユニットになることはありません。既存のマスターユニットは常にマスターのままです。ただし、マスター ユニットが応答を停止すると、その時点で新しいマスター ユニットが選定されます。

（注） **cluster master unit** コマンドを使用して、手動で強制的に特定のユニットをマスターにできます。中央集中型機能については、マスターユニット変更を強制するとすべての接続がドロップされるので、新しいマスターユニット上で接続を再確立する必要があります。中央集中型機能のリストについては、設定ガイドを参照してください。

例

次に、プライオリティ を 1（最高）に設定する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# priority 1
```

関連コマンド

コマンド	説明
clacp system-mac	スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバースイッチとの間で EtherChannel のネゴシエーションを行います。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブユニットからマスターユニットへのコンソール複製をイネーブルにします。
enable (cluster group)	クラスタリングをイネーブルにします。
health-check	クラスタのヘルスチェック機能（ユニットのヘルスモニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。

コマンド	説明
local-unit	クラスタ メンバーに名前を付けます。
mtu cluster-interface	クラスタ制御リンクインターフェイスの最大伝送ユニットを指定します。
priority (cluster group)	マスター ユニット選定のこのユニットのプライオリティを設定します。

priority（vpn ロード バランシング）

仮想ロードバランシングクラスタに参加するローカルデバイスのプライオリティを設定するには、VPN ロードバランシングモードで **priority** コマンドを使用します。デフォルトのプライオリティ指定に戻すには、このコマンドの **no** 形式を使用します。

priority *priority*
no priority

構文の説明

priority このデバイスに割り当てるプライオリティ（1～10の範囲）。

コマンド デフォルト

デフォルトのプライオリティは、デバイスのモデル番号によって異なります。

モデル番号	デフォルトのプライオリティ
5520	5
5540	7

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
VPN ロード バランシング	—	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

まず、**vpn load-balancing** コマンドを使用して、VPN ロードバランシングモードを開始する必要があります。

このコマンドは、仮想ロード バランシング クラスタに参加するローカル デバイスのプライオリティを設定します。

プライオリティは、1（最低）～ 10（最高）の範囲の整数である必要があります。

プライオリティは、VPN ロード バランシング クラスタ内でクラスタのマスターまたはプライマリ デバイスになるデバイスを決定する方法の1つとして、マスター選出プロセスで使用されます。マスター選出プロセスの詳細については、CLI 設定ガイドを参照してください。

プライオリティ指定を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。

例

次に、現在のデバイスのプライオリティを9に設定する **priority** コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
vpn load-balancing	VPN ロードバランシング モードを開始します。

priority-queue

priority コマンドで使用するインターフェイスで標準プライオリティキューを作成するには、グローバル コンフィギュレーション モードで **priority-queue** コマンドを使用します。キューを削除するには、このコマンドの **no** 形式を使用します。

（注） このコマンドは、ASA 5580 の 10 ギガビット イーサネットインターフェイスではサポートされていません（10 ギガビット イーサネットインターフェイスは、ASA 5585-X でプライオリティキュー用にサポートされています）。また、このコマンドは、ASA 5512-X ～ ASA 5555-X の管理インターフェイスではサポートされていません。このコマンドは、ASA サービスモジュールではサポートされていません。

priority-queue *interface-name*
no priority-queue *interface-name*

構文の説明

interface-name	プライオリティキューを有効にする物理インターフェイスの名前を指定します。ASA 5505 や ASASM の場合は、VLAN インターフェイスの名前を指定します。

コマンド デフォルト

デフォルトでは、プライオリティ キューイング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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.2(3)/8.4(1)	ASA 5585-X 用に 10 ギガビット イーサネット インターフェイスのサポートが追加されました。

使用上のガイドライン

LLQ プライオリティ キューイングを使用すると、特定のトラフィック フロー（音声やビデオのような遅延の影響を受けやすいトラフィックなど）をその他のトラフィックよりも優先できます。

ASA は、次の 2 つのタイプのプライオリティキューイングをサポートしています。

- 標準プライオリティキューイング：標準プライオリティキューイングでは、インターフェイスで **priority-queue** コマンドを使用して作成する LLQ プライオリティキューを使用しますが、他のすべてのトラフィックは「ベストエフォート」キューに入ります。キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これはテールドロップと呼ばれます。キューがいっぱいになるのを防ぐために、キューのバッファサイズを増やせます（**queue-limit** コマンド）。送信キューに入れることができるパケットの最大数も微調整できます（**tx-ring-limit** コマンド）。これらのオプションを使用して、プライオリティ キューイングの遅延と強固さを制御できます。LLQ キュー内のパケットは、常に、ベストエフォート キュー内のパケットよりも前に送信されます。
- 階層型プライオリティキューイング：階層型プライオリティ キューイングは、トラフィック シェーピング キューがイネーブルなインターフェイスで使用されます。シェーピングされるトラフィックのサブセットに優先順位を付けることができます。標準プライオリティ キューは使用されません。

（注） ASA 5505 に限り、1 つのインターフェイスでプライオリティ キューを設定すると、他のすべてのインターフェイスの同じコンフィギュレーションが上書きされます。つまり、最後に適用されたコンフィギュレーションだけがすべてのインターフェイスに存在することになります。また、プライオリティ キュー コンフィギュレーションは、1 つのインターフェイスから削除すると、すべてのインターフェイスから削除されます。この問題を回避するには、priority-queue コマンドを 1 つのインターフェイスにのみ設定します。queue-limit コマンドと tx-ring-limit コマンドの両方またはそのいずれかの設定を、さまざまなインターフェイスで異なる設定にする必要がある場合、任意の 1 つのインターフェイスで、すべての queue-limit のうちで最大の値と、すべての tx-ring-limit のうちで最小の値を使用します（CSCsi13132）。

例

次に、test という名前のインターフェイスに対してプライオリティ キューを設定し、キュー制限に 30,000 パケット、送信キュー制限に 256 パケットを指定する例を示します。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 30000
ciscoasa(priority-queue)# tx-ring-limit 256
ciscoasa(priority-queue)#
```

関連コマンド

コマンド	説明
queue-limit	プライオリティ キューに入れることができるパケットの最大数を指定します。この数を超えると、以後のデータはドロップされます。

コマンド	説明
tx-ring-limit	イーサネット送信ドライバのキューに任意のタイミングで入れることができるパケットの最大数を設定します。
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。
clear configure priority-queue	現在のプライオリティ キュー コンフィギュレーションを削除します。
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、このコマンドは現在のすべてのプライオリティキュー、queue-limit、および tx-ring-limit コンフィギュレーションの値を表示します。

privilege

コマンド認可（ローカル、RADIUS、および LDAP（マッピング）のみ）で使用するコマンド特権レベルを設定するには、グローバル コンフィギュレーション モードで **privilege** コマンドを使用します。構成を拒否するには、このコマンドの **no** 形式を使用します。

privilege ［ **show** ｜ **clear** ｜ **configure** ］ **level** *level* ［ **mode** *cli_mode* ］ **command** *command*
no privilege ［ **show** ｜ **clear** ｜ **configure** ］ **level** *level* ［ **mode** *cli_mode* ］ **command** *command*

構文の説明

clear	（任意）コマンドの clear 形式に対してのみ特権を設定します。**clear**、**show**、または **configure** キーワードを使用しない場合は、コマンドのすべての形式が影響を受けます。
command *command*	設定するコマンドを指定します。設定できるのは、*main* コマンドの特権レベルだけです。たとえば、すべての **aaa** コマンドのレベルを設定できますが、**aaa authentication** コマンドと **aaa authorization** コマンドのレベルは個別に設定できません。
configure	（任意）コマンドの configure 形式に対してのみ特権を設定します。コマンドの configure 形式は、通常、未修正コマンド（**show** または **clear** プレフィックスなしで）または **no** 形式として、コンフィギュレーションの変更を引き起こす形式です。**clear**、**show**、または **configure** キーワードを使用しない場合は、コマンドのすべての形式が影響を受けます。
level *level*	特権レベルを指定します。有効な値は、0 ～ 15 です。特権レベルの番号が小さいと、特権レベルが低くなります。

mode *cli_mode*	（オプション）ユーザー EXEC/特権 EXEC モード、グローバル コンフィギュレーション モード、特定のコマンドのコンフィギュレーション モードなど、複数の CLI モードでコマンドを入力できる場合、それらのモードの特権レベルを個別に設定することができます。モードを指定しない場合は、コマンドのすべてのバージョンで同じレベルが使用されます。次のモードを参照してください。 • **exec**：ユーザー EXEC モードと特権 EXEC モードの両方を指定します。 • **configure**：**configure terminal** コマンドを使用してアクセスされるグローバル コンフィギュレーション モードを指定します。 • *command_config_mode*：コマンドのコンフィギュレーション モードを指定します。グローバル コンフィギュレーション モードまたは別のコマンドのコンフィギュレーション モードでコマンド名を指定してアクセスできます。 たとえば、**mac-address** コマンドは、グローバル コンフィギュレーション モードとインターフェイス コンフィギュレーション モードの両方で入力できます。mode キーワードを使用して、各モードのレベルを個別に設定できます。 このコマンドを使用してコマンドのレベルを設定することはできません。
show	（任意）コマンドの show 形式に対してのみ特権を設定します。**clear**、**show**、または **configure** キーワードを使用しない場合は、コマンドのすべての形式が影響を受けます。

コマンド デフォルト

デフォルトでは、次のコマンドが特権レベル 0 に割り当てられます。その他のコマンドはすべて、レベル 15 です。

- **show checksum**
- **show curpriv**
- **enable**
- **help**
- **show history**
- **login**
- **logout**
- **pager**
- **show pager**
- **clear pager**
- **quit**
- **show version**

コンフィギュレーション モード コマンドを 15 より低いレベルに移動する場合は、**configure** コマンドも同じレベルに移動してください。そうしないと、ユーザーはコンフィギュレーション モードを開始できません。

すべての特権レベルを表示する方法については、**show running-config all privilege all** コマンドを参照してください。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	Cisco VSA CVPN3000-Privilege-Level を使用する RADIUS ユーザーのサポートが追加されました。 **ldap map-attributes** コマンドを使用して LDAP 属性を CVPN3000-Privilege-Level にマッピングすると、LDAP ユーザーがサポートされます。

使用上のガイドライン

privilege コマンドを使用すると、**aaa authorization command LOCAL** コマンドを設定するときに、ASA コマンドの特権レベルを設定できます。このコマンドで **LOCAL** キーワードを使用する場合でも、このキーワードによってローカル、RADIUS、および LDAP（マッピング）認可が有効になります。

例

たとえば、**filter** コマンドの形式は次のとおりです。

- **filter**（**configure** オプションで表現）
- **show running-config filter**
- **clear configure filter**

特権レベルを形式ごとに個別に設定することができます。または、このオプションを省略してすべての形式に同じ特権レベルを設定することもできます。たとえば、それぞれの形式を別々に設定するには、次のように指定します。

```
ciscoasa(config)# privilege
 show
 level
 5
 command
 filter
ciscoasa(config)# privilege
```

```
 clear
 level
 10
 command
 filter
ciscoasa(config)# privilege
 cmd
 level
 10
 command
 filter
```

また、すべてのフィルタ コマンドを同じレベルに設定できます。

```
ciscoasa(config)# privilege
 level
 5
 command
 filter
```

show privilege コマンドは、形式を分けて表示します。

次の例では、**mode** キーワードの使用方法を示します。**enable** コマンドは、ユーザー EXEC モードから入力する必要があります。一方、**enable password** コマンドは、コンフィギュレーション モードでアクセスでき、最も高い特権レベルが必要です。

```
ciscoasa(config)# privilege cmd level 0 mode exec command enable
ciscoasa(config)# privilege cmd level 15 mode configure command enable
ciscoasa(config)# privilege show level 15 mode configure command enable
```

次に、2 つのモードの **mac-address** コマンドの例を示します。show、clear、および cmd のレベルを個別に設定しています。

```
ciscoasa(config)# privilege cmd level 10 mode configure command mac-address
ciscoasa(config)# privilege cmd level 15 mode interface command mac-address
ciscoasa(config)# privilege clear level 10 mode configure command mac-address
ciscoasa(config)# privilege clear level 15 mode interface command mac-address
ciscoasa(config)# privilege show level 2 mode configure command mac-address
ciscoasa(config)# privilege show level 2 mode interface command mac-address
```

関連コマンド

コマンド	説明
clear configure privilege	コンフィギュレーションから privilege コマンド ステートメントを削除します。
show curpriv	現在の特権レベルを表示します。
show running-config privilege	コマンドの特権レベルを表示します。

profile

Call Home プロファイルを作成または編集するには、Call Home コンフィギュレーション モードで **profile** コマンドを使用します。設定済みの 1 つまたはすべての Call Home プロファイルを削除するには、このコマンドの **no** 形式を使用して、1 つまたはすべてのプロファイルを指定します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力します。

profile *profile-name*
no profile { *profile-name* | **all** }

構文の説明

profile-name	プール名（最大 20 文字）。
all	すべての設定済みプロファイルが含まれます。

コマンド デフォルト

デフォルトプロファイル **Cisco TAC** が提供されました。デフォルト プロファイルには、事前定義されたモニター対象グループ（診断、環境、インベントリ、コンフィギュレーション、テレメトリ）のセットと、事前定義された宛先電子メールおよび HTTPS URL があります。デフォルト プロファイルは、Smart Call Home を初めて設定するときに自動的に作成されます。宛先電子メールは callhome@cisco.com で、宛先 URL は https://tools.cisco.com/its/service/oddce/services/DDCEService 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Call Home コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。
8.2(2)	キーワード all が追加されました。
9.3(2)	スマート ソフトウェア ライセンシング用に **License** プロファイルが追加されました。
9.6(2)	**destination address http** の reference-identity オプションが導入されました。

使用上のガイドライン

次のコマンドは、イン プロファイル コンフィギュレーション モードで使用されます。

プロファイルの有効化または無効化

Call Home プロファイルを有効にするには、Call Home プロファイル コンフィギュレーション モードで **active** コマンドを使用します。Call Home プロファイルを無効にするには、Call Home プロファイル コンフィギュレーション モードで **no active** コマンドを使用します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力して、**profile** コマンドを入力します。デフォルトではイネーブルになっています。

active

no active

Profile コマンドのデフォルトへの設定

Call Home プロファイル設定をデフォルト値に設定するには、Call Home プロファイル コンフィギュレーション モードで default コマンドを使用します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力して、**profile** コマンドを入力します。このモードから Call Home コンフィギュレーション モード設定をリセットすることもできます。すべての Call Home プロファイルおよび全般設定を確認およびリセットする方法については、コマンドヘルプ（**default ?**）を参照してください。

default {**activedestinationemail-subjectsubscribe-to-alert-group**}

宛先タイプ、アドレス、および設定

Smart Call Home メッセージ受信者の宛先アドレス、参照アイデンティティ、メッセージ形式、およびトランスポート方式を設定するには、Call Home プロファイル コンフィギュレーション モードで **destination** コマンドを使用します。宛先パラメータを削除、またはパラメータをデフォルトにリセットするには、**no destination** コマンドまたは **default** コマンドを使用します。

デフォルト メッセージ形式は XM、デフォルト メッセージ サイズは 5 MB（0 にすると無制限）、デフォルトのトランスポート方式は電子メールです。事前に設定された参照アイデンティティを指定する必要があります。これは、接続時に Call Home サーバーの証明書を検証するために使用されます。これは、HTTP 宛先にのみ適用されます。

destination address {**e-mail** *e-mail-address***http** *http-url*}
no destination address {**e-mailhttp** [**all**]}
destination address http *http-url* **reference-identity** *ref-id-name*
no destination address http *http-url* **reference-identity** *ref-id-name*
destination address {**e-mail** *e-mail-address***http** *http-url*} **msg-format** {**short-textlong-textxml**}
no destination address {**e-mail** *e-mail-address***http** *http-url*} **msg-format** {**short-textlong-textxml**}
destination message-size-limit *max-size*
no destination message-size-limit *max-size*
destination preferred-msg-format {**short-textlong-textxml**}
no destination preferred-msg-format {**short-textlong-textxml**}
destination transport-method {**e-mailhttp**}
no destination transport-method {**e-mailhttp**}

電子メールの件名の設定

Call Home 電子メールの件名のプレフィックスまたはサフィックスを設定するには、Call Home プロファイル コンフィギュレーション モードで **email-subject** コマンドを使用します。これらのフィールドをクリアするには、**no email-subject** コマンドを使用します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力して、**profile** コマンドを入力します。

email-subject {**appendprepend**} *chars*
no email-subject {**appendprepend**} *chars*

アラートグループへの登録

アラートグループに登録するには、Call Home プロファイル コンフィギュレーション モードで **ubscribe-to-alert-group** コマンドを使用します。これらのサブスクリプションをクリアするには、no s**ubscribe-to-alert-group** コマンドを使用します。Call Home コンフィギュレーション モードにアクセスするには、まず **call-home** コマンドを入力して、**profile** コマンドを入力します。

- [no] subscribe-to-alert-group alert-group-name [severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging}]：指定した重大度レベルのグループのイベントにサブスクライブします。alert-group-name：有効な値は、syslog、diagnostic、environment、または threat です。
- [no] subscribe-to-alert-group syslog [{severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging} | message start [-end]}]：重大度レベルまたはメッセージ ID のある syslog にサブスクライブします。start-[end]：1 つの syslog メッセージ ID またはある範囲の syslog メッセージ ID。

（注） デバッグ出力はCPUプロセスで高プライオリティが割り当てられているため、デバッグ出力を行うとシステムが使用できなくなることがあります。したがって、**debugging** を使用するのは、特定の問題のトラブルシューティング時、またはシスコのテクニカルサポート担当者とともにトラブルシューティングを行う場合に限定してください。また、このコマンドは、ネットワークトラフィックやユーザーが少ない時間帯に使用してください。デバッギングをこのような時間帯に行うと、システムの使用に影響が及ぶ処理のオーバーヘッドが増加する可能性が低くなります。

- [no] subscribe-to-alert-group inventory [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]：インベントリイベントにサブスクライブします。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。
- [no] subscribe-to-alert-group configuration [export full | minimum] [periodic {daily | month day_of_month | weekly day_of_week [hh：mm]]：設定イベントにサブスクライブします。full：実行コンフィギュレーション、スタートアップ コンフィギュレーション、機能リスト、アクセスリストの要素数、およびマルチモードのコンテキスト名をエクスポートするコンフィギュレーション。minimum：機能リスト、アクセスリスト内の要素数、およびマ

ルチモードのコンテキスト名だけをエクスポートするコンフィギュレーション。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。

- [no] subscribe-to-alert-group telemetry periodic {hourly | daily | monthly day_of_month | weekly day_of_week [hh:mm]：テレメトリ定期イベントをサブスクライブします。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。
- [no] subscribe-to-alert-group snapshot periodic {interval minutes | hourly [mm] | daily | monthly day_of_month |weekly day_of_week [hh:mm]}：スナップショット定期イベントにサブスクライブします。minutes：分単位の間隔。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。

関連コマンド

コマンド	説明
call-home	ユーザーを Call Home コンフィギュレーション モードにします。
show call-home	Call Home コンフィギュレーション情報を表示します。
reference-identity	参照アイデンティティ オブジェクトを設定します。

prompt

CLI プロンプトをカスタマイズするには、グローバル コンフィギュレーション モードで prompt コマンドを使用します。デフォルトのプロンプトに戻すには、このコマンドの no 形式を使用します。

prompt { [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]
no prompt [**hostname**] [**context**] [**domain**] [**slot**] [**state**] [**priority**] [**cluster-unit**]

構文の説明

cluster-unit	クラスタ ユニット名を表示します。クラスタの各ユニットは一意の名前を持つことができます。
context	（マルチ モードのみ）現在のコンテキストを表示します。
domain	ドメイン名を表示します。
hostname	ホスト名を表示します。
priority	フェールオーバー プライオリティを [pri]（プライマリ）または [sec]（セカンダリ）として表示します。プライオリティは **failover lan unit** コマンドを使用して設定します。
state	ユニットのトラフィック通過状態またはロールを表示します。 フェールオーバーの場合、**state** キーワードに対して次の値が表示されます。 • [act]：フェールオーバーがイネーブルであり、装置ではトラフィックをアクティブに通過させています。 • stby：フェールオーバーはイネーブルです。ユニットはトラフィックを通過させていません。スタンバイ、失敗、または他の非アクティブ状態です。 • [actNoFailove]：フェールオーバーはディセーブルであり、装置ではトラフィックをアクティブに通過させています。 • [stbyNoFailover]：フェールオーバーはディセーブルであり、装置ではトラフィックを通過させていません。これは、スタンバイ ユニットでしきい値を上回るインターフェイス障害が発生したときに生じることがあります。 クラスタリングの場合、**state** キーワードに対して次の値が表示されます。 • control node • data node たとえば、**prompt hostname cluster-unit state** と設定して「ciscoasa/cl2/data node>」と表示された場合、ホスト名は ciscoasa、ユニット名は cl2、状態名は data node です。

コマンド デフォルト

デフォルトのプロンプトはホスト名です。マルチコンテキストモードでは、ホスト名の後に現在のコンテキスト名（*hostname* /*context*）が続きます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グローバル設定	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.0(1)	**cluster-unit** オプションが追加されました。クラスタリング用に **state** キーワードが更新されました。
9.19(1)	クラスタリングの場合、**state** 表示が **master** と **slave** から **control node** と **data node** に変更されました。

使用上のガイドライン

キーワードを入力する順序によって、プロンプト内の要素の順序が決まります。要素はスラッシュ（/）で区切ります。

マルチ コンテキスト モードでは、システム実行スペースまたは管理コンテキストにログインするときに、拡張プロンプトを表示できます。非管理コンテキスト内では、デフォルトのプロンプト（ホスト名およびコンテキスト名）のみが表示されます。

プロンプトに情報を追加する機能により、複数のモジュールが存在する場合にログインしている ASA を一目で確認することができます。この機能は、フェールオーバー時に、両方の ASA に同じホスト名が設定されている場合に便利です。

例

次に、フェールオーバー用のプロンプトで使用可能なすべての要素を表示する例を示します。

```
ciscoasa(config)# prompt hostname context slot state priority
```

プロンプトが次のストリングに変化します。

```
ciscoasa/admin/pri/act(config)#
```

関連コマンド

コマンド	説明
clear configure prompt	設定したプロンプトをクリアします。

コマンド	説明
show running-config prompt	設定したプロンプトを表示します。

propagate sgt

インターフェイスでのセキュリティグループタグ（**sgt**）の伝達を有効にするには、CTS 手動インターフェイス コンフィギュレーション モードで **propagate sgt** コマンドを使用します。インターフェイスでのセキュリティグループタグ（**sgt**）の伝達を無効にするには、このコマンドの **no** 形式を使用します。

propagate sgt
no propagate sgt

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。

コマンド デフォルト

伝搬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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CTS 手動インターフェイス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、CTS レイヤ 2 SGT インポジションのセキュリティ グループ タグの伝播をイネーブルまたはディセーブルにできます。

制約事項

- 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイスおよび冗長インターフェイスでのみサポートされます。
- BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。

例

次に、レイヤ 2 SGT インポジションのインターフェイスをイネーブルにし、SGT の伝播は行わないように設定する例を示します。

```
ciscoasa(config)# interface gi0/0
ciscoasa(config-if)# cts manual

ciscoasa(config-if-cts-manual)# no propagate sgt
```

関連コマンド

コマンド	説明
cts manual	レイヤ 2 SGT インポジションをイネーブルにし、CTS 手動インターフェイス コンフィギュレーション モードを開始します。
policy static sgt	手動で設定された CTS リンクにポリシーを適用します。

protocol

IKEv2 接続の IPsec プロポーザルに使用するプロトコルタイプと暗号化タイプを指定するには、IPsec プロポーザル コンフィギュレーション モードで **protocol** コマンドを使用します。プロトコルおよび暗号化タイプを削除するには、このコマンドの no 形式を使用します。

protocol esp { **encryption** { **des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **aes-gmac** | **aes-gmac-192** | **aes-gmac-256** | **null** } | **integrity** { **md5** | **sha-1** | **sha-256** | **sha-384** | **sha-512** | **null** }
no protocol esp { **encryption** { **des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **aes-gmac** | **aes-gmac-192** | **aes-gmac-256** | **null** } | **integrity** { **md5** | **sha-1** | **sha-256** | **sha-384** | **sha-512** | **null** }

構文の説明

esp	カプセル化セキュリティ ペイロード（ESP）IPsec プロトコルを指定します（現在、唯一サポートされている IPsec のプロトコルです）。
des	56 ビット DES-CBC 暗号化を ESP に対して指定します。
3des	（デフォルト）トリプル DES 暗号化アルゴリズムを ESP に対して指定します。
aes	AES と 128 ビット キー暗号化を ESP に対して指定します。
aes-192	AES と 192 ビット キー暗号化を ESP に対して指定します。
aes-256	AES と 256 ビット キー暗号化を ESP に対して指定します。
aes-gcm	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gcm-192	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gcm-256	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gmac	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gmac-192	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
aes-gmac-256	使用する AES-GCM または AES-GMAC のアルゴリズムを指定します。
null	ESP に暗号化を使用しません。
integrity	IPsec プロトコルの整合性アルゴリズムを指定します。
md5	ESP の整合性保護のために MD5 アルゴリズムを指定します。
sha-1	（デフォルト）は、ESP の整合性保護のために米国連邦情報処理標準（FIPS）で定義されたセキュア ハッシュ アルゴリズム（SHA）SHA-1 を指定します。
sha-256	IPsec 整合性アルゴリズムとして使用するアルゴリズムを指定します。
sha-384	IPsec 整合性アルゴリズムとして使用するアルゴリズムを指定します。

sha-512	IPsec 整合性アルゴリズムとして使用するアルゴリズムを指定します。
null	AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合に選択します。

コマンド デフォルト

IPsec プロポーザルのデフォルトの設定は、暗号化タイプが 3DES で、整合性タイプが SHA-1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPsec プロポーザル コンフィギュレーション	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	AES-GCM または AES-GMAC アルゴリズムのサポートが追加されました。IPsec 整合性アルゴリズムとして使用するアルゴリズムを選択できるようになりました。

使用上のガイドライン

IKEv2 IPsec プロポーザルには、暗号化タイプと整合性タイプを複数設定できます。このコマンドで指定したタイプの中から、必要なタイプをピアで選択することができます。

AES-GMC/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択する必要があります。

例

次に、proposal_1 という IPsec プロポーザルを作成する例を示します。ESP 暗号化タイプとして DES と 3DES を設定し、整合性保護のために暗号化アルゴリズム MD5 と SHA-1 を指定しています。

```
ciscoasa(config)# crypto ipsec ikev2 ipsec-proposal proposal_1
ciscoasa(config-ipsec-proposal)# protocol ESP encryption des 3des
ciscoasa(config-ipsec-proposal)# protocol ESP integrity md5 sha-1
```

関連コマンド

コマンド	説明
crypto ikev2 enable	IPsec ピアの通信に使用するインターフェイスで ISAKMP IKEv2 ネゴシエーションをイネーブルにします。

コマンド	説明
crypto ipsec ikev2 ipsec-proposal	IPsec プロポーザルを作成し、IPsec プロポーザル コンフィギュレーション モードを開始します。このコンフィギュレーション モードで、プロポーザルに対して暗号化タイプと整合性タイプを複数指定できます。
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。
crypto map set transform-set	クリプトマップエントリで使用するトランスフォームセットを指定します。
crypto dynamic-map set transform-set	ダイナミック クリプトマップエントリで使用するトランスフォーム セットを指定します。
show running-config crypto map	クリプト マップの設定内容を表示します。
show running-config crypto dynamic-map	ダイナミック クリプトマップのコンフィギュレーションを表示します。

protocol-enforcement

ドメイン名、ラベル長、形式チェック（圧縮およびループポインタのチェックを含む）を有効にするには、パラメータ コンフィギュレーション モードで **protocol-enforcement** コマンドを使用します。プロトコルの強制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。

protocol-enforcement
no protocol-enforcement

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。

コマンド デフォルト

プロトコルの強制は、デフォルトでイネーブルになっています。この機能は、**policy-map type inspect dns** コマンドを定義していない場合でも、**inspect dns** コマンドを設定していれば有効にできます。無効にするには、ポリシーマップ コンフィギュレーションで **no protocol-enforcement** コマンドを明示的に指定する必要があります。**inspect dns** が設定されていない場合、NAT リライトは実行されません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

状況によっては、コマンドがディセーブルであっても、プロトコルの強制が実行されます。これは、DNS リソース レコードの分類、NAT、TSIG チェックなど、他の目的で DNS リソース レコードの解析が必要なときに発生します。

例

次に、DNS インスペクション ポリシー マップ内でプロトコルの強制をイネーブルにする方法を示します。

```
ciscoasa(config)# policy-map type inspect dns preset_dns_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-enforcement
```

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。

protocol http

CRL を取得するための許可された配布ポイントプロトコルとして HTTP を指定するには、ca-crl コンフィギュレーション モードで **protocol http** コマンドを使用します。CRL 取得方法として許可した HTTP を削除するには、このコマンドの **no** 形式を使用します。

protocol http
no protocol 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。

コマンド デフォルト

デフォルトの設定は、HTTP を許可します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ca-crl コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用する場合は、HTTP ルールをパブリック インターフェイス フィルタに適用してください。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

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 の CRL を取得するための配布ポイント プロトコルとして HTTP を許可する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol http
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。

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。
protocol ldap	CRL の取得方法として LDAP を指定します。
protocol scep	CRL の取得方法として SCEP を指定します。

protocol ldap

CRL を取得するための配布ポイントプロトコルとして LDAP を指定するには、ca-crl コンフィギュレーション モードで **protocol ldap** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した LDAP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol ldap
no protocol ldap

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。

コマンド デフォルト

デフォルトの設定は、LDAP を許可します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CRL コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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 の CRL を取得するための配布ポイント プロトコルとして LDAP を許可する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol ldap
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。

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。
protocol http	CRL の取得方法として HTTP を指定します。
protocol scep	CRL の取得方法として SCEP を指定します。

protocol-object

プロトコル オブジェクト グループにプロトコル オブジェクトを追加するには、プロトコル コンフィギュレーション モードで protocol-object コマンドを使用します。ポートオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

protocol-object *protocol*
no protocol-object *protocol*

構文の説明

protocol プロトコルの名前または番号。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
プロトコル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

protocol-object コマンドは、**object-group** コマンドとともに使用して、プロトコル コンフィギュレーション モードでプロトコルオブジェクトを定義します。

IP プロトコルの名前や番号は、*protocol* 引数を使用して指定できます。udp プロトコル番号は 17、tcp プロトコル番号は 6、egp プロトコル番号は 47 です。

例

次に、プロトコル オブジェクトを定義する例を示します。

```
ciscoasa(config)# object-group protocol proto_grp_1
ciscoasa(config-protocol)# protocol-object udp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# exit
ciscoasa(config)# object-group protocol proto_grp
ciscoasa(config-protocol)# protocol-object tcp
ciscoasa(config-protocol)# group-object proto_grp_1
ciscoasa(config-protocol)# exit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure object-group	すべての object group コマンドをコンフィギュレーションから削除します。
group-object	ネットワーク オブジェクト グループを追加します。
network-object	ネットワーク オブジェクト グループにネットワーク オブジェクトを追加します。
object-group	コンフィギュレーションを最適化するためのオブジェクト グループを定義します。
show running-config object-group	現在のオブジェクト グループを表示します。

protocol scep

CRL を取得するための配布ポイントプロトコルとして SCEP を指定するには、crl コンフィギュレーション モードで **protocol scep** コマンドを使用します。権限があれば、CRL 配布ポイントの内容によって取得方法（HTTP、LDAP、SCEP のいずれかまたは複数）が決まります。

CRL 取得方法として許可した SCEP プロトコルを削除するには、このコマンドの **no** 形式を使用します。

protocol scep
no protocol scep

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。

コマンド デフォルト

デフォルトの設定は、SCEP を許可します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CRL コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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 の CRL を取得するための配布ポイント プロトコルとして SCEP を許可する例を示します。

```
ciscoasa(configure)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# protocol scep
ciscoasa(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	ca-crl コンフィギュレーション モードを開始します。

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。
protocol http	CRL の取得方式として HTTP を指定します。
protocol ldap	CRL の取得方法として LDAP を指定します。

protocol shutdown

いずれのインターフェイスとの隣接関係も形成できず IS-IS LSP データベースをクリアさせるために IS-IS プロトコルを無効にするには、ルータ ISIS コンフィギュレーション モードで **protocol shutdown** コマンドを使用します。IS-IS プロトコルを再び有効にするには、このコマンドの **no** 形式を使用します。

protocol shutdown
no protocol shutdown

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。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドにより、既存の IS-IS コンフィギュレーション パラメータを削除することなく特定のルーティング インスタンスの IS-IS プロトコルをディセーブルにすることができます。**protocol shutdown** コマンドを入力した場合、IS-IS プロトコルは引き続き ASA 上で動作し、ユーザーは現在の IS-IS 設定を使用できますが、IS-IS はいずれのインターフェイスでも隣接関係を確立せず、IS-IS LSP データベースもクリアします。

特定のインターフェイスで IS-IS プロトコルを無効にするには、**isis protocol shutdown** コマンドを使用します。

例

次に、特定のルーティング インスタンスの IS-IS プロトコルをディセーブルにする例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# protocol shutdown
```

関連コマンド

protocol-violation

HTTP および NetBIOS インスペクションでプロトコル違反が発生したときのアクションを定義するには、パラメータ コンフィギュレーション モードで **protocol-violation** 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。

protocol-violation action [**drop** [**log**] | **log**]
no protocol-violation action [**drop** [**log**] | **log**]

構文の説明

drop	プロトコルに準拠しないパケットをドロップすることを指定します。
ログ	プロトコル違反をログに記録することを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、HTTP または NetBIOS ポリシーマップで設定できます。HTTP または NetBIOS パーサーが HTTP または NetBIOS メッセージの最初の数バイトで有効なメッセージを検出できない場合、syslog が発行されます。たとえば、チャンク エンコーディングの形式が不正であるためにメッセージを解析できない場合に、このような状況が発生します。

例

次に、ポリシーマップにおけるプロトコル違反に対するアクションを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect http http_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# protocol-violation action drop
```

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。

proxy-auth

トンネルグループにフラグを付けて特定のプロキシ認証のトンネルグループとして設定するには、webvpn コンフィギュレーション モードで **proxy-auth** コマンドを使用します。

proxy-auth [**sdi**]

構文の説明

sdi	RADIUS/TACACS SDI プロキシ メッセージをネイティブ SDI ディレクティブに解析します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

proxy-auth コマンドは、AAA サーバープロキシ認証のテキストメッセージのネイティブ プロトコル ディレクティブへの解析を有効にする場合に使用します。

proxy-auth_map sdi

RADIUS プロキシサーバーから返された RADIUS チャレンジメッセージをネイティブ SDI メッセージにマッピングするには、AAA サーバー コンフィギュレーション モードで **proxy-auth_map sdi** コマンドを使用します。

proxy-auth_map sdi [**sdi_message**] [**radius_challenge_message**]

構文の説明

radius_challenge_message	特定の SDI メッセージのマッピングに使用する RADIUS チャレンジ メッセージを指定します。次のいずれかを指定できます。 • new-pin-meth：新しい PIN 方式。デフォルトは「Do you want to enter your own pin」 • new-pin-reenter：新しい PIN の再入力。デフォルトは「Reenter PIN:」 • new-pin-req：新しい PIN の要求。デフォルトは「Enter your new Alpha-Numerical PIN」 • new-pin-sup：新しい PIN の提供。デフォルトは「Please remember your new PIN」 • new-pin-sys-ok：新しい PIN の受理。デフォルトは「New PIN Accepted」 • next-ccode-and-reauth：トークン変更時の再認証。デフォルトは「new PIN with the next card code」 • next-code：PIN なしのトークンコードの指定。デフォルトは「Enter Next PASSCODE」 • ready-for-sys-pin：システムで生成された PIN の受け入れ。デフォルトは「ACCEPT A SYSTEM GENERATED PIN」
sdi_message	ネイティブ SDI メッセージを指定します。

コマンド デフォルト

ASA のデフォルトのマッピングは、Cisco ACS のデフォルト設定（システム管理、構成、RSA SecureID のプロンプトなど）と対応しており、RSA 認証マネージャのデフォルト設定とも同期されています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバーコンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

RADIUS プロキシからの RADIUS チャレンジメッセージの解析とマッピングを有効にするには、トンネル グループ コンフィギュレーション モードで **proxy-auth** コマンドを有効にする必要があります。これにより、デフォルトのマッピングの値が使用されます。デフォルトのマッピングの値は、**proxy-auth_map** コマンドを使用して変更できます。

リモートユーザーは、セキュアクライアント で ASA に接続し、RSA SecurID トークンを使用して認証を試みます。RADIUS プロキシサーバーを使用して、認証に関する SDI サーバーと通信するように ASA を設定できます。

認証の間に、RADIUS サーバは ASA にアクセス チャレンジ メッセージを提示します。これらのチャレンジ メッセージ内に、SDI サーバからのテキストを含む応答メッセージがあります。このメッセージテキストは、ASA が SDI サーバーと直接通信している場合と RADIUS プロキシを経由して通信している場合では異なります。

そのため、セキュアクライアント にネイティブ SDI サーバーとして認識させるために、ASA は RADIUS サーバーからのメッセージを解釈する必要があります。また、SDI メッセージは SDI サーバで設定可能であるため、ASA のメッセージテキストの全体または一部が、SDI サーバのメッセージ テキストと一致する必要があります。一致しない場合、リモート クライアント ユーザに表示されるプロンプトが、認証中に必要とされるアクションに対して適切でない場合があります。この場合、セキュアクライアント が応答できずに認証が失敗する場合があります。

関連コマンド

コマンド	説明
proxy-auth	RADIUS プロキシからの RADIUS チャレンジ メッセージの解析とマッピングをイネーブルにします。

proxy-bypass

コンテンツの最低限の書き換えを実行し、書き換えるコンテンツのタイプ（外部リンクや XML）を指定するように ASA を設定するには、webvpn コンフィギュレーション モードで **proxy-bypass** コマンドを使用します。プロキシのバイパスを無効にするには、このコマンドの **no** 形式を使用します。

proxy-bypass interface *interface name* { **port** *port number* | **path-mask** *path mask* } **target** *url* [**rewrite** { **link** | **xml** | **none**] }
no proxy-bypass interface *interface name* { **port** *port number* | **path-mask** *path mask* } **target** *url* [**rewrite** { **link** | **xml** | **none**] }

構文の説明

ホスト	トラフィックの転送先ホストを示します。ホストの IP アドレスまたはホスト名を使用します。
interface	プロキシ バイパス用の ASA インターフェイスを示します。
interface name	ASA インターフェイスを名前で指定します。
link	絶対外部リンクの書き換えを指定します。
none	書き換えを指定しません。
path-mask	一致パターンを指定します。
path-mask	照合対象として正規表現を含むことができるパターンを指定します。次のワイルドカードを使用できます。 *：完全一致。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 ? ：少なくとも 1 文字を一致させます。 [!seq]：順序に関係なく、任意の文字を含みます。 [seq]：順序も含め、任意の文字を含みます。 最大 128 バイトです。
port	プロキシ バイパス用に予約されているポートを示します。
port number	プロキシ バイパス用に予約されているポート（大きい番号）を指定します。ポートの範囲は 20000 ～ 21000 です。1 つのプロキシ バイパス ルールのみにポートを使用できます。
rewrite	（任意）書き換え用の追加ルール（なし、または XML やリンクの組み合わせ）を指定します。
target	トラフィックの転送先リモート サーバーを示します。

url	URL を **http(s)://***fully_qualified_domain_name*[:*port*] という形式で入力します。最大 128 バイトです。別のポートを指定しない限り、HTTP のポートは 80、HTTPS のポートは 443 です。
xml	書き換える XML コンテンツを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
WebVPN コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

プロキシ バイパスは、コンテンツの書き換えを最小限に実行して、アプリケーションおよび Web リソースの動作を向上させるために使用します。proxy-bypass コマンドは、ASA を通過する特定の Web アプリケーションの処理方法を決定します。

このコマンドは複数回使用できます。エントリを設定する順序は重要ではありません。インターフェイスとパスマスク、またはインターフェイスとポートにより、プロキシバイパスルールが一意に指定されます。

パスマスクではなくポートを使用してプロキシバイパスを設定する場合、ネットワーク構成によっては、それらのポートが ASA にアクセスできるようにするために、ファイアウォール構成を変更する必要があります。この制限を回避するには、パスマスクを使用します。ただし、パス マスクは変化することがあるため、複数のパス マスク ステートメントを使用して変化する可能性をなくすことが必要になる場合があります。

パスは、URL で .com や .org、またはその他のタイプのドメイン名の後に続く全体です。たとえば、www.example.com/hrbenefits という URL では、*hrbenefits* がパスになります。同様に、www.example.com/hrinsurance という URL では、*hrinsurance* がパスです。すべての hr サイトでプロキシ バイパスを使用する場合は、*（ワイルドカード）を /hr* のように使用して、コマンドを複数回使用しないようにできます。

例

次に、WebVPN インターフェイス上のプロキシバイパス用にポート 20001 を使用するように ASA を設定する例を示します。HTTP とそのデフォルトポート 80 を使用してトラフィックを example.com に転送し、XML コンテンツを書き換えます。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface webvpn port 20001 target http://example.com rewrite xml
```

次に、外部インターフェイスでのプロキシバイパス用にパスマスク mypath/* を使用するように ASA を設定する例を示します。HTTP とそのデフォルトポート 443 を使用してトラフィックを example.com に転送し、XML およびリンクコンテンツを書き換えます。

```
ciscoasa
(config)#
 webvpn
ciscoasa
(config-webvpn)#
 proxy-bypass interface outside path-mask /mypath/* target https://example.com rewrite
xml,link
```

関連コマンド

コマンド	説明
apcf	特定のアプリケーションに使用する非標準のルールを指定します。
rewrite	トラフィックが ASA を通過するかどうかを決定します。

proxy-ldc-issuer

TLS プロキシ ローカル ダイナミック証明書を発行するには、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 proxy-ldc-issuer 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。

proxy-ldc-issuer
no proxy-ldc-issuer

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

TLS プロキシ ローカル ダイナミック証明書を発行するには、proxy-ldc-issuer コマンドを使用します。proxy-ldc-issuer コマンドは、クリプト トラストポイントにローカル CA としてのロールを付与して LDC を発行します。クリプト ca トラストポイント コンフィギュレーション モードからアクセスできます。

proxy-ldc-issuer コマンドは、TLS プロキシのダイナミック証明書を発行するトラストポイントに、ローカル CA の役割を定義します。このコマンドは、「自己登録」を使用するトラストポイントでのみ設定できます。

例

次に、内部ローカル CA を作成し、電話用の LDC を署名する例を示します。このローカル CA は、proxy-ldc-issuer がイネーブルな標準の自己署名トラストポイントとして作成されます。

```
ciscoasa(config)# crypto ca trustpoint ldc_server
```

```
ciscoasa(config-ca-trustpoint)# enrollment self
ciscoasa(config-ca-trustpoint)# proxy-ldc-issuer
ciscoasa(config-ca-trustpoint)# fqdn my _ldc_ca.example.com
ciscoasa(config-ca-trustpoint)# subject-name cn=FW_LDC_SIGNER_172_23_45_200
ciscoasa(config-ca-trustpoint)# keypair ldc_signer_key
ciscoasa(config)# crypto ca enroll ldc_server
```

関連コマンド

コマンド	説明
ctl-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
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。

proxy paired

Azure Gateway Load Balancer（GWLB）の Azure 上の ASA Virtual のペアプロキシモードに VNI インターフェイスを指定するには、インターフェイス コンフィギュレーション モードで **proxy paired** コマンドを使用します。プロキシを削除するには、このコマンドの **no** 形式を使用します。

proxy paired
no proxy paired

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.19(1)	このコマンドが追加されました。

使用上のガイドライン

Azure サービスチェーンでは、ASA Virtual がインターネットと顧客サービス間のパケットをインターセプトできる透過的なゲートウェイとして機能します。ASA Virtual は、ペアプロキシの VXLAN セグメントを利用して、単一の NIC に外部インターフェイスと内部インターフェイスを定義します。

例

次の例では、Azure GWLB の VNI 1 インターフェイスを設定します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# proxy paired
ciscoasa(config-if)# internal-segment-id 1000
ciscoasa(config-if)# external-segment-id 1001
ciscoasa(config-if)# internal-port 101
ciscoasa(config-if)# external-port 102
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif vxlan1000
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0 standby 10.1.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
encapsulation vxlan	NVE インスタンスを VXLAN カプセル化に設定します。
external-port	外部 VXLAN ポートを設定します。
external-segment-id	VNI インターフェイスの VXLAN 外部セグメント ID を指定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
internal-port	内部 VXLAN ポートを設定します。
internal-segment-id	VNI インターフェイスの VXLAN 内部セグメント ID を指定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

proxy-server（廃止予定）

IP 電話の構成ファイルの <proxyServerURL> タグの下に書き込まれる、電話プロキシ機能に対して HTTP プロキシを設定するには、電話プロキシ コンフィギュレーション モードで **proxy-server** コマンドを使用します。電話プロキシから HTTP プロキシ構成を削除するには、このコマンドの **no** 形式を使用します。

proxy-server address *ip_address* [*listen_port*] **interface** *ifc*
no proxy-server address *ip_address* [*listen_port*] **interface** *ifc*

構文の説明

interface *ifc*	ASA で HTTP プロキシが常駐するインターフェイスを指定します。
ip_address	HTTP プロキシの IP アドレスを指定します。
listen_port	HTTP プロキシのリスニング ポートを指定します。指定しない場合、デフォルトは 8080 になります。

コマンド デフォルト

リッスン ポートを指定しない場合、ポートはデフォルトで 8080 に設定されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モードコマンドとともに廃止されました。

使用上のガイドライン

電話プロキシのプロキシサーバー コンフィギュレーション オプションを設定すると、DMZ または外部ネットワークで HTTP プロキシを使用できます。これらのネットワークでは、電話機上のサービスについてすべての IP フォンの URL がこのプロキシ サーバーに誘導されます。この設定では、非セキュアな HTTP トラフィックに対応します。このようなトラフィックは社内ネットワークに入ることはできません。

入力する *ip_address* は、IP フォンおよび HTTP プロキシ サーバーの配置場所に基づくグローバル IP アドレスにする必要があります。

プロキシサーバーが DMZ 内にあり、IP 電話がネットワークの外部にある場合、ASA は NAT ルールの存在を確認するためにルックアップを実行し、グローバル IP アドレスを使用して構成ファイルに書き込みます。

ASA はホスト名を IP アドレスに解決できる場合（DNS ルックアップが設定されている場合など）、そのホスト名を IP アドレスに解決するため、*ip_address* 引数にホスト名を入力できます。

デフォルトでは、エンタープライズ パラメータの下に設定された電話の URL パラメータは、URL 内で FQDN を使用しています。HTTP プロキシ用の DNS lookup で FQDN が解決されない場合は、IP アドレスを使用するようにこれらのパラメータを変更する必要があります。

プロキシ サーバー URL が IP フォンのコンフィギュレーション ファイルに正しく書き込まれたかどうかを確認するには、[Settings] > [Device Configuration] > [HTTP configuration] > [Proxy Server URL] で IP フォンの URL をチェックします。

電話プロキシでは、プロキシ サーバーに対するこの HTTP トラフィックを検査しません。

ASA が IP 電話と HTTP プロキシサーバーのパス内にある場合は、既存のデバッグ手法（syslog やキャプチャなど）を使用して、プロキシサーバーをトラブルシューティングします。

電話プロキシが使用中の場合は、プロキシサーバーを 1 つだけ設定できます。ただし、プロキシ サーバーを設定した後に IP 電話にコンフィギュレーション ファイルをダウンロードした場合は、IP 電話を再起動して、プロキシサーバーのアドレスが記載されたコンフィギュレーション ファイルが取り込まれるようにする必要があります。

例

次に、**proxy-server** コマンドを使用して電話プロキシ用に HTTP プロキシサーバーを設定する例を示します。

```
ciscoasa(config-phone-proxy)# proxy-server 192.168.1.2 interface inside
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

proxy single-arm

VXLAN VNI インターフェイスの single-arm プロキシを指定するには、インターフェイス コンフィギュレーション モードで **proxy single-arm** コマンドを使用します。プロキシを無効にするには、このコマンドの **no** 形式を使用します。

proxy single-arm
no proxy single-arm

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

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• —	• 対応	• —	—

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドが追加されました。

使用上のガイドライン

AWS ゲートウェイロードバランサは、透過的なネットワークゲートウェイと、トラフィックを分散し、仮想アプライアンスをオンデマンドで拡張するロードバランサを組み合わせます。ASA 仮想は、分散データプレーン（ゲートウェイ ロードバランサ エンドポイント）を備えたゲートウェイロードバランサ集中型コントロールプレーンをサポートします。このユースケースでは、VNI インターフェイスを single-arm プロキシとして設定する必要があります。**same-security-traffic permit intra-interface** も有効にして、トラフィックが VTEP 送信元インターフェイスを U ターンできるようにしてください。

例

次に、VNI インターフェイスを single-arm プロキシとして設定する例を示します。

```
ciscoasa(config)# interface vni 1
ciscoasa(config-if)# vtep-nve 1
ciscoasa(config-if)# nameif geneve1000
ciscoasa(config-if)# ip address 192.168.1.1 255.255.255.0 standby 192.168.1.2
ciscoasa(config-if)# ipv6 address 2001:0DB8::BA98:0:3210/48
ciscoasa(config-if)# security-level 50
```

```
ciscoasa(config-if)# proxy single-arm
ciscoasa(config)# same-security-traffic permit intra-interface
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
encapsulation geneve	NVE インスタンスを Geneve カプセル化に設定します。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス（設定されている場合）のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリアインターフェイス（送信元インターフェイス）のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。

ptp domain

ISA 3000 上のすべての PTP ポートのドメイン番号を指定するには、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 **ptp domain** コマンドを使用します。ドメイン番号は 0 ～ 255 で、デフォルト値は 0 です。設定したドメインとは異なるドメイン上で受け取ったパケットは、通常のマルチキャストパケットのように処理され、PTP 処理は行われません。ドメイン番号をデフォルト値の 0 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。

ptp domain *domain_num*
no ptp domain

（注） このコマンドは、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

domain *domain_num* ISA 3000 上の PTP 対応のすべてのポートにドメイン番号を指定します。

コマンド デフォルト

デフォルトの **ptp domain** 番号は、0 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

ptp domain コマンドは、グローバル コンフィギュレーション モードでも使用できます。

例

次に、**ptp domain** コマンドを使用して、PTP ドメイン番号を 127 に設定する例を示します。

```
ciscoasa# ptp domain 127
```

関連コマンド

コマンド	説明
show ptp port	PTP インターフェイス/ポート情報を表示します。

ptp enable

ISA 3000 上のインターフェイスで PTP を有効にするには、インターフェイス コンフィギュレーション モードで **ptp enable** コマンドを使用します。PTP が有効になるモードは、**ptp mode** コマンドで指定します。インターフェイスで PTP を無効にするには、このコマンドの **no** 形式を使用します。インターフェイスとの間で着信および発信する PTP パケットは、通常のマルチキャスト パケットと同様に扱われます。

ptp enable
no ptp enable

（注） このコマンドは、Cisco ISA 3000 アプライアンスのみで使用できます。

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。

コマンド デフォルト

デフォルトでは、トランスペアレント モードのすべての ISA 3000 インターフェイスで PTP がイネーブルになっています。ルーテッドモードでは、PTP パケットがデバイスを通過できるようにするために必要な設定を追加する必要があります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを入力できるのは、インターフェイス コンフィギュレーション モードのみです。

このコマンドは物理インターフェイスのみで使用できます。サブインターフェイス、その他の仮想インターフェイス、または管理インターフェイスでは使用できません。

VLAN サブインターフェイスでの PTP フローは、適切な PTP 設定が親インターフェイス上に存在する場合にサポートされます。

PTP がどのモードでもイネーブルになっていない場合、このコマンドは受け入れられても何も効果がありません。警告が発行されます。

関連コマンド

コマンド	説明
show ptp clock	PTP クロックのプロパティを表示します。

ptp mode

ISA 3000 でPTP クロックモードを指定するには、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 **ptp mode** コマンドを使用します。すべてのインターフェイスで PTP を無効にするには、このコマンドの **no** 形式を使用します。

ptp mode e2etransparent
no ptp mode

（注） このコマンドは、Cisco ISA 3000 アプライアンスのみで使用できます。

構文の説明

e2etranparent エンドツーエンド トランスペアレント モードを ISA 3000 上のすべての PTP 対応インターフェイスでイネーブルにします。

コマンド デフォルト

エンドツーエンド トランスペアレント モー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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

エンドツーエンド トランスペアレント モードがディセーブルの場合、すべての PTP パケットは他のマルチキャスト パケットのように扱われます。これは転送モードと同等です。

ptp mode コマンドは、グローバル コンフィギュレーション モードでも使用できます。

例

次に、**ptp mode** コマンドを使用して、PTP クロックモードをエンドツーエンド トランスペアレントに設定する例を示します。

```
ciscoasa# ptp mode e2etranparent
```

関連コマンド

コマンド	説明
show ptp internal-info	PTP 統計情報とカウンタ情報を表示します。

public-key

Cisco Umbrella によって要求される証明書の検証に DNSCrypt プロバイダーの公開キーを指定するには、Cisco Umbrella コンフィギュレーション モードで **public-key** コマンドを使用します。キーを削除して、デフォルトのキーを使用するには、このコマンドの **no** 形式を使用します。

public-key *dnscrypt_key*
no public-key [*dnscrypt_key*]

構文の説明

dnscrypt_key DNScrypt 用に Cisco Umbella サーバーによって使用される公開キー。このキーは、Cisco Umbrella のために使用される DNS インスペクション ポリシー マップで dnscrypt を有効にした場合にのみ関連します。

キーは 32 バイトの 16 進数値です。2 バイトごとにコロンで区切った ASCII の 16 進数値を入力します。キー長は 79 バイトです。このキーは Cisco Umbrella から取得します。

コマンド デフォルト

デフォルトのキーが使用されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Umbrella の設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.10(1)	このコマンドが追加されました。

使用上のガイドライン

DNS インスペクション ポリシー マップで DNScrypt をイネーブルにする場合は、必要に応じて証明書の検証に DNScrypt プロバイダーの公開キーを設定できます。キーを設定しない場合は、現在配布されているデフォルトの公開キーが検証に使用されます。

キーの設定が必要になるのは、DNScrypt 暗号化に使用する公開キーが Cisco Umbrella によって変更された場合だけです。

例

次に、Cisco Umbrella で使用する公開キーを設定する例を示します。この例では、グローバル DNS インスペクションで使用されるデフォルトの DNS インスペクション ポリシー マップで DNScrypt を有効にする方法も示しています。

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# public-key
B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

ciscoasa(config-umbrella)# token AABBA59A0BDE1485C912AFE

Please make sure all the Umbrella Connector prerequisites are satisfied:
1. DNS server is configured to resolve api.opendns.com
2. Route to api.opendns.com is configured
3. Root certificate of Umbrella registration is installed
4. Unit has a 3DES license
ciscoasa(config)# policy-map type inspect dns preset_dns_map

ciscoasa(config-pmap)# parameters

ciscoasa(config-pmap-p)# umbrella

ciscoasa(config-pmap-p)# dnscrypt
```

関連コマンド

コマンド	説明
dnscrypt	デバイスと Cisco Umbrella 間の接続で DNScrypt 暗号化を有効にします。
inspect dns	DNS インスペクションをイネーブルにします。
policy-map type inspect dns	DNS インスペクション ポリシー マップを作成します。
timeout edns	アイドル タイムアウトを設定します。その時間が経過するまでサーバーからの応答がない場合、クライアントから Umbrella サーバーへの接続は削除されます。
token	Cisco Umbrella への登録に必要な API トークンを指定します。
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

publish-crl

ローカル CA が発行した証明書の失効状態を他の ASA が検証できるようにするには、CA サーバー コンフィギュレーション モードで **publish-crl** コマンドを使用します。その結果、ASA のインターフェイスから CRL を直接ダウンロードできます。CRL をダウンロードできないようにするには、このコマンドの **no** 形式を使用します。

[**no**] **publish-crl interface** *interface* [**port** *portnumber*]

構文の説明

interface *interface*	インターフェイスに使用される *nameif* を指定します（gigabitethernet0/1 など）。詳細については、interface コマンドを参照してください。
port *portnumber*	（オプション）インターフェイス デバイスで CRL をダウンロードするときに使用するポートを指定します。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。

コマンド デフォルト

デフォルト **publish-crl** ステータスは **no publish** です。TCP ポート 80 は、HTTP のデフォルトです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

CRL は、デフォルトでアクセス不可です。必要なインターフェイスおよびポートで CRL ファイルへのアクセスをイネーブルにする必要があります。

TCP ポート 80 は、HTTP のデフォルト ポート番号です。デフォルト以外のポート（ポート 80 以外）を設定する場合は、他のデバイスがそのポートへのアクセス方法を認識できるように、**cdp-url** 構成にその新しいポート番号が含まれるようにします。

CRL 配布ポイント（CDP）は、ローカル CA ASA における CRL の場所です。**cdp-url** コマンドで設定する URL は、発行されるすべての証明書に埋め込まれます。CDP 用に特定の場所を設定しない場合、デフォルトの CDP の URL は http://hostname.domain/+CSCOCA+/asa_ca.crl です。

クライアントレス SSL VPN が同じインターフェイスでイネーブルになっている場合、HTTP リダイレクトと CRL ダウンロード要求は、同じ HTTP リスナーによって処理されます。リスナーが着信 URL をチェックし、**cdp-url** コマンドで設定した URL と一致する場合、CRL ファイルがダウンロードされます。URL が **cdp-url** コマンドと一致しない場合、接続が HTTPS にリダイレクトされます（HTTP リダイレクトが有効な場合）。

例

次に、CA サーバー コンフィギュレーション モードで **publish-crl** コマンドを入力して、外部インターフェイスのポート 70 を CRL ダウンロード用に有効にする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa (config-ca-server)#publish-crl outside 70
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	自動生成される CRL 用に特定の場所を指定します。
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。

pwd

現在の作業ディレクトリを表示するには、特権 EXEC モードで **pwd** コマンドを使用します。

pwd

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。

コマンド デフォルト

ルート ディレクトリ（/）がデフォルトです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、**dir** コマンドと機能が類似しています。

例

次に、現在の作業ディレクトリを表示する例を示します。

```
ciscoasa# pwd
disk0:/
ciscoasa# pwd
flash:
```

関連コマンド

コマンド	説明
cd	現在の作業ディレクトリから、指定したディレクトリに変更します。
dir	ディレクトリの内容を表示します。
more	ファイルの内容を表示します。

q - res

queue-limit（プライオリティ キュー）

プライオリティキューの深さを指定するには、プライオリティ キュー コンフィギュレーション モードで **queue-limit** 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。

（注） このコマンドは、ASA 5580 の 10 ギガビット イーサネットインターフェイスではサポートされていません（10 ギガビット イーサネットインターフェイスは、ASA 5585-X でプライオリティ キュー用にサポートされています）。また、このコマンドは、ASA 5512-X ～ ASA 5555-X の管理インターフェイスではサポートされていません。このコマンドは、ASA サービスモジュールではサポートされていません。

queue-limit *number-of-packets*
no queue-limit *number-of-packets*

構文の説明

number-of-packets キューイング（バッファリング）可能な低遅延または通常のプライオリティのパケットの最大数を指定します。この最大数を超えると、インターフェイスでパケットのドロップが開始されます。値の範囲の上限は、実行時にダイナミックに決定されます。この制限を表示するには、コマンドラインで **help** または **?** を入力します。主な決定要素は、キューをサポートするために必要なメモリと、デバイス上で使用可能なメモリです。キューは、使用可能なメモリを超えることはできません。理論的な最大パケット数は、2147483647 です。

コマンド デフォルト

デフォルトのキューの制限は 1024 パケットです。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
プライオリティ キュー コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ASA では、遅延の影響を受けやすい、プライオリティの高いトラフィック（音声およびビデオなど）用の低遅延キューイング（LLQ）と、それ以外のトラフィック用のベストエフォート（デフォルト）という 2 つのトラフィッククラスを使用できます。ASA は、プライオリティトラフィックを認識して、適切な Quality of Service（QoS）ポリシーを適用します。プライオリティ キューのサイズと深さを設定して、トラフィック フローを微調整できます。

（注） インターフェイスのプライオリティキューイングを有効にするには、**priority-queue** コマンドを設定する必要があります。

1 つの **priority-queue** コマンドを、**nameif** コマンドで定義できるすべてのインターフェイスに対して適用できます。

priority-queue コマンドで、プライオリティ キュー コンフィギュレーション モードを開始します。これはプロンプトに表示されます。プライオリティキューモードでは、いつでも送信キューに入れることができるパケットの最大数（**tx-ring-limit** コマンド）、およびパケットをドロップする前にバッファに入れることができるタイプ（プライオリティまたはベストエフォート）のパケット数（**queue-limit** コマンド）を設定できます。

指定する tx-ring-limit および queue-limit は、プライオリティの高い低遅延キューとベストエフォート キューの両方に適用されます。tx-ring-limit は、ドライバが許容できる両方のタイプのパケットの数です。このパケット数を超えると、ドライバはインターフェイスの先頭にある複数のキューにパケットを戻し、輻輳が解消するまでそのキューでパケットをバッファしておきます。通常、これらの 2 つのパラメータを調整することで、低遅延トラフィックのフローを最適化できます。

キューは無限大ではないため、いっぱいになってオーバーフローすることがあります。キューがいっぱいになると、以降のパケットはキューに入ることができず、すべてドロップされます。これがテールドロップです。キューがいっぱいになることを避けるには、**queue-limit** コマンドを使用して、キューのバッファサイズを大きくします。

例

次に、test というインターフェイスのプライオリティ キューを設定して、キュー制限を 234 パケット、送信キュー制限を 3 パケットに指定する例を示します。

```
ciscoasa(config)# priority-queue test
ciscoasa(priority-queue)# queue-limit 234
ciscoasa(priority-queue)# tx-ring-limit 3
```

関連コマンド

コマンド	説明
clear configure priority-queue	指定したインターフェイスの現在のプライオリティ キュー コンフィギュレーションを削除します。
priority-queue	インターフェイスにプライオリティ キューイングを設定します。

コマンド	説明
show priority-queue statistics	指定されたインターフェイスのプライオリティ キュー統計情報を表示します。
show running-config [all] priority-queue	現在のプライオリティ キュー コンフィギュレーションを表示します。**all** キーワードを指定すると、このコマンドは現在のすべてのプライオリティキュー、queue-limit、および tx-ring-limit コンフィギュレーションの値を表示します。
tx-ring-limit	イーサネット送信ドライバのキューに任意のタイミングで入れることができるパケットの最大数を設定します。

queue-limit（tcp マップ）

TCP接続において、順序が不正なパケットのバッファリング可能最大数を設定し、正しい順序に整列するには、tcp マップ コンフィギュレーション モードで **queue-limit** コマンドを使用します。値をデフォルトに戻すには、このコマンドの **no** 形式を使用します。このコマンドは、**set connection advanced-options** コマンドを使用してイネーブルにされる TCP 正規化ポリシーの一部です。

queue-limit *pkt_num* **timeout** *seconds*
no queue-limit

構文の説明

pkt_num	TCP接続において、正しい順序に整列し直すことができる、順序が不正なパケットのバッファリング可能最大数を 1 ～ 250 の範囲で指定します。デフォルトは 0 です。この値は、この設定がディセーブルであり、トラフィックのタイプに応じてデフォルトのシステム キュー制限が使用されることを意味しています。詳細については、「使用上のガイドライン」を参照してください。
timeout *seconds*	（任意）順序が不正なパケットをバッファ内に保持可能な最大時間を 1 ～ 20 秒の範囲で設定します。デフォルトは 4 秒です。パケットの順序が不正であり、このタイムアウト期間内に渡されなかった場合、それらのパケットはドロップされます。 *pkt_num* 引数を 0 に設定した場合は、どのトラフィックのタイムアウトも変更できません。**timeout** キーワードを有効にするには、 limit を 1 以上に設定する必要があります。

コマンド デフォルト

デフォルト設定は0です。この値は、このコマンドがディセーブルであることを意味しています。

デフォルトのタイムアウトは 4 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(4)/8.0(4)	**timeout** キーワードが追加されました。

使用上のガイドライン

TCP 正規化をイネーブルにするには、モジュラ ポリシー フレームワークを次のように使用します。

1.tcp-map：TCP 正規化アクションを指定します。

- **a.queue-limit**：tcp マップ コンフィギュレーション モードでは、 **queue-limit** コマンドおよびその他数多くのコマンドを入力できます。

2.class-map：TCP 正規化を実行するトラフィックを指定します。

3.policy-map：各クラスマップに関連付けるアクションを指定します。

- **a.class**：アクションを実行するクラスマップを指定します。
- **b.set connection advanced-options**：作成した TCP マップを指定します。

4.service-policy：ポリシーマップをインターフェイスごとに、またはグローバルに割り当てます。

TCP 正規化を有効にしない場合、または **queue-limit** コマンドがデフォルトの 0 に設定されている場合（つまりコマンドが無効の場合）、トラフィックのタイプに応じてデフォルトのシステムキュー制限が使用されます。

- アプリケーション インスペクション（**inspect** コマンド）、IPS（**ips** コマンド）、および TCP チェック再送信（TCP map **check-retransmission** コマンド）のための接続のキュー制限は 3 パケットです。ASA が異なるウィンドウ サイズの TCP パケットを受信した場合は、アドバタイズされた設定と一致するようにキュー制限がダイナミックに変更されます。
- 他の TCP 接続の場合は、異常なパケットはそのまま通過します。

queue-limit コマンドを 1 以上に設定した場合、すべての TCP トラフィックに対して許可される異常なパケットの数は、この設定と一致します。たとえば、アプリケーション インスペクション、IPS、および TCP チェック再送信トラフィックの場合、**queue-limit** 設定が優先され、TCP パケットからアドバタイズされたすべての設定が無視されます。その他の TCP トラフィックについては、異常なパケットはバッファに格納されて、そのまま通過するのではなく、正しい順序に設定されます。

例

次に、すべての Telnet 接続のキュー制限を 8 パケットに、バッファ タイムアウトを 6 秒に設定する例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# queue-limit 8 timeout 6
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq telnet
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
class-map	サービス ポリシーに対してトラフィックを指定します。
policy-map	サービス ポリシーのトラフィックに適用するアクションを指定します。
set connection advanced-options	TCP 正規化をイネーブルにします。
service-policy	サービス ポリシーをインターフェイスに適用します。
show running-config tcp-map	TCP マップ コンフィギュレーションを表示します。
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。

quick-start

IP オプションインスペクションが設定されたパケットヘッダーでクイックスタート（QS）オプションが発生したときに実行するアクションを定義するには、パラメータ コンフィギュレーション モードで **quick-start** 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。

quick-start action { **allow** | **clear** }
no quick-start action { **allow** | **clear** }

構文の説明

allow	クイックスタート IP オプションを含むパケットを許可します。
clear	クイックスタート オプションをパケット ヘッダーから削除してから、パケットを許可します。

コマンド デフォルト

デフォルトでは、IP オプション インスペクションは、クイックスタート IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用すると、デフォルト値を変更できます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプションインスペクションを設定して、特定の IP オプションを持つどの IP パケットが ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシーマップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# quick-start action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

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。

quit

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ーEXECモードからログアウトするには、**quit** コマンドを使用します。

quit

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ユーザーEXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

また、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ーEXECモードでは動作しません。

特権 EXEC モードまたはユーザー EXEC モードで **quit** コマンドを入力すると、ASA からログアウトします。特権 EXEC モードからユーザー EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**quit** 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、セッションからログアウトする例を示します。

```
ciscoasa(config)# quit
ciscoasa# quit
Logoff
```

次に、**quit** 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。

```
ciscoasa(config)# quit
```

```
ciscoasa# disable
ciscoasa>
```

関連コマンド

コマンド	説明
exit	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モードやユーザーEXEC モードからログアウトします。

quota management-session

ASA で許可する集約管理セッション、ユーザーごとの管理セッション、およびプロトコルごとの管理セッションの最大数を設定するには、グローバル コンフィギュレーション モードで **quota management-session** コマンドを使用します。クォータをデフォルト値に設定するには、このコマンドの **no** 形式を使用します。

quota management-session [**ssh** | **telnet** | **http** | **user**] *number*
no quota management-session [**ssh** | **telnet** | **http** | **user**] *number*

構文の説明

number	実行を許可する ASDM、SSH、および Telnet の最大同時セッション数を指定します。（9.12 以降）その他のキーワードを指定せずに入力すると、この引数では 1 ～ 15 のセッションの集約数が設定されます。デフォルトは 15 です。（9.10 以前）有効な値は 0（無制限）～ 10,000 です。
ssh	1 ～ 5 の SSH セッションの最大数を設定します。デフォルトは 5 分です。
telnet	1 ～ 5 の Telnet セッションの最大数を設定します。デフォルトは 5 分です。
http	1 ～ 5 の HTTPS（ASDM）セッションの最大数を設定します。デフォルトは 5 分です。
user	1 ～ 5 のユーザーごとのセッションの最大数を設定します。デフォルトは 5 分です。

コマンド デフォルト

（9.12 以降）集約のデフォルト値は 15 です。

SSH、Telnet、HTTP、およびユーザーのデフォルト値は 5 です。

（9.10 以前）デフォルト値は 0 で、セッション数の制限はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.1(2)	このコマンドが追加されました。

リリース	変更内容
9.12(1)	システムではなく、コンテキスト内でこのコマンドを入力できるようになりました。また、集約制限に加えて、ユーザーとプロトコルごとの制限を設定できるようになりました。集約セッションの最大数が15になりました。0（無制限）または16以上に設定してアップグレードすると、値は15に変更されます。

使用上のガイドライン

割り当て量に達すると、それ以降の管理セッション要求は拒否され、syslogメッセージが生成されます。デバイスのロックアウトを回避するため、管理セッション割り当て量のメカニズムではコンソール セッションはブロックされません。

（注） マルチコンテキストモードではASDMセッションの数を設定することはできず、最大セッション数は5で固定されています。

（注） また、**limit-resource** コマンドを使用して最大管理セッション（SSHなど）のコンテキストあたりのリソース制限を設定した場合は、小さい方の値が使用されます。

例

次の例では、集約管理セッション クォータを8に設定し、個々のセッション制限をさまざまな数量に設定しています。

```
ciscoasa
(config)#
quota management-session 8
ciscoasa(config)# quota management-session ssh 3
ciscoasa(config)# quota management-session telnet 1
ciscoasa(config)# quota management-session http 4
ciscoasa(config)# quota management-session user 2
```

関連コマンド

コマンド	説明
show run quota management-session	管理セッション割り当て量の現在の値を表示します。
show quota management-session	管理セッションの統計情報を表示します。

radius-common-pw

ASA経由でRADIUS認可サーバーにアクセスするすべてのユーザーが使用する共通のパスワードを指定するには、AAAサーバーホストモードで**radius-common-pw** 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。

radius-common-pw *string*
no radius-common-pw

構文の説明

string RADIUSサーバーにおけるすべての認可トランザクションで共通パスワードとして使用される最大 127 文字の英数字キーワード。大文字と小文字は区別されます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
aaa-server host	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、RADIUS 認可サーバーに対してのみ有効です。

RADIUS 認可サーバーでは、各接続ユーザーに対してパスワードおよびユーザー名が必要です。ASA では、ユーザー名が自動的に指定されます。ここでは、パスワードを入力します。RADIUSサーバー管理者は、このASA経由でRADIUSサーバーに対して認可を行う各ユーザーにこのパスワードが関連付けられるようにRADIUSサーバーを設定する必要があります。この情報は、RADIUS サーバー管理者に伝えてください。

共通のユーザーパスワードを指定しなかった場合、各ユーザーのパスワードはユーザー名になります。共通ユーザーパスワードにユーザー名を使用する場合は、セキュリティ上の予防措置として、ネットワーク上の他のいずれの場所でもRADIUSサーバーを認可に使用しないでください。

13-125

（注） *string* 引数は、実質的には意味がありません。RADIUS サーバーはこのフィールドを要求しますが、実際には使用されません。ユーザはこのことを知っている必要はありません。

例

次に、ホスト「1.2.3.4」に「svrgrp1」という名前の RADIUS AAA サーバー グループを設定し、タイムアウト時間を 9 秒に、再試行間隔を 7 秒に、RADIUS 共通パスワードを「allauthpw」に設定する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 9
ciscoasa
(config-aaa-server-host)# retry 7
ciscoasa
(config-aaa-server-host)#
radius-common-pw allauthpw
ciscoasa
(config-aaa-server-host)#
exit
ciscoasa
(config)#
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始して、ホスト固有の AAA サーバー パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。

radius-reject-message

認証が拒否された場合のログイン画面でのRADIUS拒否メッセージの表示を有効にするには、トンネルグループ webvpn 属性コンフィギュレーション モードで **radius-eject-message** 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するには、**no** 形式を使用します。

radius-reject-message
no radius-reject-message

コマンド デフォルト

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

リモート ユーザーに対して、認証の失敗についての RADIUS メッセージを表示する場合は、このコマンドをイネーブルにします。

例

次に、engineering という名前の接続プロファイルに対して RADIUS 拒否メッセージの表示をイネーブルにする例を示します。

```
ciscoasa(config)# tunnel-group engineering webvpn-attributes
ciscoasa(config-tunnel-webvpn)# radius-reject-message
```

radius-with-expiry (Deprecated)

（注） このコマンドをサポートする最後のリリースは、Version 8.0(1) でした。

認証中に MS-CHAPv2 を使用してユーザーとパスワードアップデートをネゴシエートするように ASA を設定するには、トンネルグループ ipsec 属性コンフィギュレーション モードで **radius-with-expiry** 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。

radius-with-expiry
no radius-with-expiry

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。

コマンド デフォルト

このコマンドのデフォルト設定は、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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.1(1)	このコマンドは廃止されました。**password-management** コマンドに置き換わっています。**radius-with-expiry** コマンドの **no** 形式はサポートされなくなりました。
8.0(2)	このコマンドは廃止されました。

使用上のガイドライン

この属性は、IPSec リモート アクセス トンネル グループ タイプに対してのみ適用できます。RADIUS 認証が設定されていない場合、ASA ではこのコマンドは無視されます。

例

次に、設定 ipsec コンフィギュレーション モードで、remotegrp という名前のリモート アクセス トンネル グループに対して radius-with-expiry を設定する例を示します。

```
ciscoasa(config)# tunnel-group remotegrp type ipsec_ra
ciscoasa(config)# tunnel-group remotegrp ipsec-attributes
ciscoasa(config-tunnel-ipsec)# radius-with-expiry
```

関連コマンド

コマンド	説明
clear configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
password-management	パスワード管理をイネーブルにします。このコマンドは、トンネルグループ一般属性モードでは、**radius-with-expiry** コマンドに置き換えられます。
show running-config tunnel-group	指定した証明書マップ エントリを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ ipsec 属性を設定します。

RAID

RAID 内の SSD を管理するには、特権 EXEC モードで **raid** コマンドを使用します。

（注） このコマンドは、Cisco Secure Firewall 3100 でのみサポートされています。

raid { **add** | **remove** | **remove-secure** } **local-disk** { **1** | **2** } [*psid*]

構文の説明

add	SSD を RAID に追加します。新しい SSD と RAID の同期が完了するまでに数時間かかることがありますが、その間、ファイアウォールは完全に動作します。再起動もでき、電源投入後に同期は続行されます。
psid	以前に別のシステムで使用されていて、まだロックされている SSD を追加する場合は、*psid* と入力します。*psid* は SSD の背面に貼られたラベルに印刷されています。または、システムを再起動し、SSD を再フォーマットして RAID に追加できます。
remove	SSD を RAID から取り外し、データをそのまま保持します。
remove-secure	SSD を RAID から取り外し、自己暗号化ディスク機能を無効にして、SSD を安全に消去します。
local-disk {**1** | **2**}	SSD（disk1 または disk2）を指定します。

コマンド デフォルト

SSD が 2 つある場合、起動時に RAID が形成されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.17(1)	このコマンドは、Cisco Secure Firewall 3100 に導入されました。

使用上のガイドライン

ファイアウォールの電源が入っているときに、次のタスクを実行できます。

- SSD の 1 つをホットスワップする：SSD に障害がある場合は、交換できます。SSD が 1 つしかない場合、ファイアウォールの電源がオンになっている間 SSD は取り外せません。
- SSD の 1 つを取り外す：SSD が 2 つある場合は、1 つを取り外すことができます。
- 2 つ目の SSD を追加する：SSD が 1 つの場合は、2 つ目の SSD を追加して RAID を形成できます。

注意 この手順を使用して、SSD を RAID から削除する前に SSD を取り外さないでください。データが失われる可能性があります。

例

次に、RAID から disk2 が削除され、安全に消去される例を示します。

```
ciscoasa# raid remove-secure local-disk 2
```

関連コマンド

コマンド	説明
show raid	RAID ステータスを表示します。
show ssd	SSD ステータスを表示します。

range

ネットワークオブジェクトのアドレスの範囲を設定するには、オブジェクトコンフィギュレーション モードで **range** コマンドを使用します。コンフィギュレーションからオブジェクトを削除するには、このコマンドの **no** 形式を使用します。

range *ip_addr_1 ip_addr2*
no range *ip_addr_1 ip_addr2*

構文の説明

ip_addr_1	範囲の最初の IP アドレス（IPv4 または IPv6）を指定します。
ip_addr_2	範囲の最後の IP アドレスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
オブジェクトネットワークコンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.3(1)	このコマンドが追加されました。
9.0(1)	IPv6 アドレスのサポートが追加されました。

使用上のガイドライン

既存のネットワーク オブジェクトを異なる IP アドレスを使用して設定すると、新しいコンフィギュレーションが既存のコンフィギュレーションに置き換わります。

例

次に、範囲ネットワーク オブジェクトを作成する例を示します。

```
ciscoasa (config)# object network OBJECT_RANGE
ciscoasa (config-network-object)# range 10.1.1.1 10.1.1.8
```

関連コマンド

コマンド	説明
clear configure object	作成されたすべてのオブジェクトをクリアします。
description	ネットワーク オブジェクトに説明を追加します。
fqdn	完全修飾ドメイン名のネットワーク オブジェクトを指定します。
host	ホスト ネットワーク オブジェクトを指定します。
nat	ネットワーク オブジェクトの NAT をイネーブルにします。
object network	ネットワーク オブジェクトを作成します。
object-group network	ネットワーク オブジェクト グループを作成します。
show running-config object network	ネットワーク オブジェクト コンフィギュレーションを表示します。
subnet	サブネット ネットワーク オブジェクトを指定します。

ras-rcf-pinholes

ゲートキーパーがネットワーク内にある場合に、H.323 エンドポイント間でのコール設定を有効にするには、パラメータ コンフィギュレーション モードで **ras-rcf-pinholes** 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。

ras-rcf-pinholes enable
no ras-rcf-pinholes enable

構文の説明

enable	H.323 エンドポイント間でのコール設定をイネーブルにします。

コマンド デフォルト

デフォルトでは、このオプションは無効になっています。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(5)	このコマンドが追加されました。

使用上のガイドライン

ASA には、RegistrationRequest/RegistrationConfirm（RRQ/RCF）メッセージに基づいてコールのピンホールを開くオプションが含まれています。これらの RRQ/RCF メッセージはゲートキーパーとの間で送信されるため、コール側エンドポイントの IP アドレスは不明であり、ASA は送信元 IP アドレス/ポート 0/0 を通じてピンホールを開けます。

例

次に、これらのコールのピンホールを開くアクションをポリシーマップに設定する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# ras-rcf-pinholes enable
```

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。

コマンド	説明
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。

rate-limit

モジュラポリシーフレームワークを使用する場合は、一致またはクラスコンフィギュレーションモードで **rate-limit** コマンドを使用して、**match** コマンドまたはクラスマップと一致するパケットのメッセージレートを制限します。このレート制限アクションは、アプリケーショントラフィックのインスペクション ポリシー マップに使用できますが（**policy-map type inspect** コマンド）、すべてのアプリケーションでこのアクションが許可されているわけではありません。このアクション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。

rate-limit *rate*
no rate-limit *rate*

構文の説明

rate トラフィックにレート制限を適用します（1 ～ 4294967295）。ESMTP、GTP、RTSP、および SIP の場合、レートはパケット/秒単位です。SCTP の場合、レートはキロビット/秒（Kbps）単位です。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
9.5(2)	このコマンドはSCTPインスペクションに拡張されました（レートはパケット/秒単位ではなく Kbps 単位）。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect**

コマンドを参照します）、**rate-limit** コマンドを入力して、メッセージのレートを制限できます。

レイヤ 3/4 ポリシーマップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションを有効にする場合、このアクションを含むインスペクション ポリシー マップを有効にできます。たとえば、**inspect sip sip_policy_map** コマンドを入力します。sip_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、invite 要求を 1 秒あたり 100 メッセージに制限する例を示します。

```
ciscoasa(config-cmap)# policy-map type inspect sip sip-map1
ciscoasa(config-pmap-c)# match request-method invite
ciscoasa(config-pmap-c)# rate-limit 100
```

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。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

reactivation-mode

グループ内の障害が発生したサーバーを再アクティブ化する方法を指定するには、AAA サーバー プロトコル モードで **reactivation-mode** 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。

reactivation-mode { **depletion** [**deadtime** *minutes*] | **timed** }
no reactivation-mode { **depletion** [**deadtime** *minutes*] | **timed** }

構文の説明

deadtime *minutes*	（任意）グループ内の最後のサーバーがディセーブルになってから、その後すべてのサーバーを再度イネーブルにするまでの時間を 0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。
depletion	グループ内のすべてのサーバーが非アクティブになった後でのみ、障害が発生したサーバーを再アクティブ化します。
timed	30 秒のダウン時間の後、障害が発生したサーバを再アクティブ化します。

コマンド デフォルト

デフォルトの再アクティブ化モードは depletion で、デフォルトの deadtime の値は 10 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバープロトコル コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

各サーバ グループには、所属するサーバの再アクティブ化ポリシーを指定する属性があります。

depletion モードでは、非アクティブになったサーバーは、グループにある他のすべてのサーバーが非アクティブになるまで非アクティブのままとなります。すべてのサーバーが非アクティブになると、グループ内のすべてのサーバーが再アクティブ化されます。このアプローチでは、障害が発生したサーバーに起因する接続遅延の発生を最小限に抑えられます。**depletion** モードが使用されている場合は、**deadtime** パラメーターも指定できます。**deadtime** パラメー

タでは、グループ内の最後のサーバーが無効になってから、その後すべてのサーバーを再度有効にするまでの時間を分単位で指定します。このパラメータは、サーバー グループがローカル フォールバック機能とともに使用されている場合にのみ意味があります。さらに、ローカル フォールバックが使用されないアカウンティングにもグループを使用すると、デッドタイムがキャンセルされます。この問題は、アカウンティング用に（同じサーバーで）別のグループを作成することで回避できます。

timedモードでは、障害が発生したサーバーは30秒のダウンタイム後に再アクティブ化されます。このモードは、サーバー リスト内の最初のサーバーをプライマリ サーバーとして使用しており、このサーバーを可能な限りオンラインに維持する必要がある場合に役立ちます。このポリシーは、UDP サーバーの場合は機能しません。サーバーが存在しない場合でも UDP サーバーへの接続に障害が発生することはないため、UDPサーバーはすぐに再度オンラインになります。サーバー リストに到達不能な複数のサーバーが含まれている場合には、接続時間が遅延したり、接続に失敗する場合があります。

同時アカウンティングが無効になっているアカウンティング サーバー グループでは、**timed** モードが強制的に使用されます。このことは、特定のリスト内のすべてのサーバーが同等に扱われることを意味しています。

（注） SDI サーバー グループには、1 つのサーバーしか含まれていないため、このコマンドは SDI サーバー グループに対して無視されます。

例

次に、「svrgrp1」という TACACS+ AAA サーバーを設定し、deadtime を 15 分に設定して、depletion の再アクティベーション モードを使用する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol tacacs+
ciscoasa
(config-aaa-sersver-group)# reactivation-mode depletion deadtime 15
ciscoasa
(config-aaa-server)#
exit
ciscoasa
(config)#
```

次に、「svrgrp1」という TACACS+ AAA サーバーを設定し、timed の再アクティベーション モードを使用する例を示します。

```
ciscoasa
(config)# aaa-server svrgrp2 protocol tacacs+
ciscoasa
(config-aaa-server)# reactivation-mode timed
ciscoasa
(config-aaa-server)#
```

関連コマンド

accounting-mode	アカウンティング メッセージが単一のサーバーに送信されるか、またはグループ内のすべてのサーバーに送信されるかを示します。

aaa-server protocol	AAA サーバー グループ コンフィギュレーション モードを開始して、グループ内のすべてのホストに共通する、グループ固有のAAA サーバー パラメータを設定できるようにします。
max-failed-attempts	サーバー グループ内の所定のサーバーが非アクティブ化されるまでに、そのサーバーで許容される接続試行の失敗数を指定します。
clear configure aaa-server	AAA サーバー コンフィギュレーションをすべて削除します。
show running-config aaa-server	すべてのAAAサーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルのAAAサーバー統計情報を表示します。

record-entry

CTL ファイルの作成に使用されるトラストポイントを指定するには、CTL ファイル コンフィギュレーション モードで record-entry コマンドを使用します。CTL からレコードエントリを削除するには、このコマンドの **no** 形式を使用します。

record-entry [**capf cucm cucm-tftp tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]
no record-entry [**capf cucm cucm-tftp tftp**] **trustpoint** *trustpoint* **address** *ip_address* [**domain-name** *domain_name*]

構文の説明

capf	このトラストポイントのロールを CAPF に指定します。1 つの CAPF トラストポイントのみを設定できます。
cucm	このトラストポイントのロールを CCM に指定します。複数の CCM トラストポイントを設定できます。
cucm-tftp	このトラストポイントのロールを CCM+TFTP に指定します。複数の CCM+TFTP トラストポイントを設定できます。
domain-name *domain_name*	（任意）トラストポイントの DNS フィールドの作成に使用されるトラストポイントのドメイン名を指定します。この名前は、サブジェクト DN の一般名フィールドに追加されて、DNS 名が作成されます。トラストポイントに FQDN が設定されていない場合は、ドメイン名を設定する必要があります。
address *ip_address*	トラストポイントの IP アドレスを指定します。
tftp	このトラストポイントのロールを TFTP に指定します。複数の TFTP トラストポイントを設定できます。
trustpoint *trust_point*	インストールされているトラストポイントの名前を設定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CTL ファイル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。

使用上のガイドライン

domain-name は、1 つのみ指定できます。CTL ファイルが存在しない場合は、手動でこの証明書を CUCM から ASA にエクスポートします。

このコマンドは、電話プロキシの CTL ファイルを設定していない場合にのみ使用します。すでに CTL ファイルを設定している場合は、このコマンドを使用しないでください。

ip_address 引数に指定する IP アドレスは、トラストポイントの CTL レコードで使用される IP アドレスとなるため、グローバル アドレス、または IP Phone によって認識されるアドレスである必要があります。

CTL ファイルで必要な各エントリに対して、さらに record-entry コンフィギュレーションを追加します。

例

次に、**record-entry** コマンドを使用して、CTL ファイルの作成に使用されるトラストポイントを指定する例を示します。

```
ciscoasa(config-ctl-file)# record-entry
 cucm-tftp
 trustpoint cucm1 address 192.168.1.2
```

関連コマンド

コマンド	説明
ctl-file (global)	Phone Proxy コンフィギュレーション用に作成する CTL ファイル、またはフラッシュ メモリから解析するための CTL ファイルを指定します。
ctl-file (phone-proxy)	Phone Proxy コンフィギュレーションで使用する CTL ファイルを指定します。
phone-proxy	Phone Proxy インスタンスを設定します。

record-route

IP オプションインスペクションが設定されたパケットヘッダーで Record Route（RR）オプションが発生したときに実行するアクションを定義するには、パラメータ コンフィギュレーション モードで **record-route** 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。

record-route action { **allow** | **clear** }
no record-route action { **allow** | **clear** }

構文の説明

allow	レコード ルート IP オプションを含むパケットを許可します。
clear	レコードルート オプションをパケット ヘッダーから削除してから、パケットを許可します。

コマンド デフォルト

デフォルトでは、IP オプション インスペクションは、レコード ルート IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用すると、デフォルト値を変更できます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプションインスペクションを設定して、特定の IP オプションを持つどの IP パケットが ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# record-route action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

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。

redirect-fqdn

VPN ロードバランシングモードで完全修飾ドメイン名を使用したリダイレクトを有効または無効にするには、グローバル コンフィギュレーション モードで **redirect-fqdn enable** コマンドを使用します。

redirect-fqdn { **enable** | **disable** }
no redirect-fqdn { **enable** | **disable** }

（注） VPN ロード バランシングを使用するには、Plus ライセンスを備えた ASA モデル 5510、または ASA モデル 5520 以降が必要です。また、VPN ロード バランシングには、アクティブな 3DES/AES ライセンスも必要です。セキュリティ アプライアンスは、ロード バランシングをイネーブルにする前に、この暗号ライセンスが存在するかどうかをチェックします。アクティブな 3DES または AES のライセンスが検出されない場合、セキュリティ アプライアンスはロード バランシングをイネーブルにせず、ライセンスでこの使用方法が許可されていない場合には、ロードバランシング システムによる 3DES の内部コンフィギュレーションも抑止します。

構文の説明

disable	完全修飾ドメイン名を使用したリダイレクトをディセーブルにします。
enable	完全修飾ドメイン名を使用したリダイレクトをイネーブルにします。

コマンド デフォルト

この動作は、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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
VPN ロード バランシング モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

デフォルトで、ASA はロードバランシング リダイレクションの IP アドレスだけをクライアントに送信します。DNS 名に基づく証明書が使用されている場合、セカンダリ デバイスにリダイレクトされるとその証明書は無効になります。

VPN クライアント接続を別のクラスタ デバイス（クラスタ内の別の ASA）にリダイレクトするときに、この ASA は VPN クラスタ マスターとして、DNS 逆ルックアップを使用し、そのクラスタ デバイスの（外部 IP アドレスではなく）完全修飾ドメイン名（FQDN）を送信できます。

クラスタ内のロードバランシング デバイスのすべての外部および内部ネットワーク インターフェイスは、同じ IP ネットワーク上に存在する必要があります。

IP アドレスではなく FQDN を使用して WebVPN ロード バランシングを実行するには、次の設定手順を実行する必要があります。

1. **redirect-fqdn enable** コマンドを使用して、ロードバランシングのための FQDN の使用を有効にします。
2. DNS サーバーに、各 ASA 外部インターフェイスのエントリを追加します（エントリが存在しない場合）。それぞれの ASA 外部 IP アドレスに、ルックアップ用にそのアドレスに関連付けられた DNS エントリが設定されている必要があります。これらの DNS エントリに対しては、逆ルックアップもイネーブルにする必要があります。
3. dns domain-lookup inside コマンドを使用して、ASA で DNS ルックアップをイネーブルにします。inside の部分には、DNS サーバーへのルートを持つ任意のインターフェイスを指定します。
4. dns name-server 10.2.3.4 のように、ASA に DNS サーバーの IP アドレスを定義します（10.2.3.4 は、DNS サーバーの IP アドレス）。

例

次に、リダイレクトを無効にする **redirect-fqdn** コマンドの例を示します。

```
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# redirect-fqdn disable
ciscoasa(config-load-balancing)#
```

次に、完全修飾ドメイン名のリダイレクトをイネーブルにし、クラスタのパブリック インターフェイスを「test」と指定し、クラスタのプライベート インターフェイスを「foo」と指定するインターフェイス コマンドを含む、VPN ロード バランシング コマンド シーケンスの例を示します。

```
ciscoasa(config)# interface GigabitEthernet 0/1
ciscoasa(config-if)# ip address 209.165.202.159 255.255.255.0
ciscoasa(config)# nameif test
ciscoasa(config)# interface GigabitEthernet 0/2
ciscoasa(config-if)# ip address 209.165.201.30 255.255.255.0
ciscoasa(config)# nameif foo
ciscoasa(config)# vpn load-balancing
ciscoasa(config-load-balancing)# nat 192.168.10.10
ciscoasa(config-load-balancing)# priority 9
ciscoasa(config-load-balancing)# interface lbpublic test
ciscoasa(config-load-balancing)# interface lbprivate foo
ciscoasa(config-load-balancing)# cluster ip address 209.165.202.224
ciscoasa(config-load-balancing)# cluster key 123456789
ciscoasa(config-load-balancing)# cluster encryption
ciscoasa(config-load-balancing)# cluster port 9023
```

```
ciscoasa(config-load-balancing)# redirect-fqdn enable
ciscoasa(config-load-balancing)# participate
```

関連コマンド

コマンド	説明
clear configure vpn load-balancing	ロード バランシングの実行時コンフィギュレーションを削除し、ロード バランシングをディセーブルにします。
show running-config vpn load-balancing	現在の VPN ロードバランシング仮想クラスタのコンフィギュレーションを表示します。
show vpn load-balancing	VPN ロード バランシング実行時の統計情報を表示します。
vpn load-balancing	VPN ロード バランシング モードを開始します。

redistribute（IPv6 ルータ OSPF）

OSPFv3 ルーティングドメインから別の OSPFv3 ルーティングドメインに IPv6 ルートを再配布するには、IPv6 ルータ OSPF コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を無効にするには、このコマンドの **no** 形式を使用します。

redistribute *source-protocol* [*process-id*] [**include-connected** { **level-1** | **level-1-2** | **level-2** }] [*as-number*] [**metric** { *metric-value* **transparent** }] [**metric-type** *type-value* **] [match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**tag** *tag-value*] [**route-map** *map-tag*]

no redistribute *source-protocol* [*process-id*] [**include-connected** { **level-1** | **level-1-2** | **level-2** }] [*as-number*] [**metric** { *metric-value* **transparent** }] [**metric-type** *type-value* **] [match** { **external** [**1** | **2**] | **internal** | **nssa-external** [**1** | **2**] }] [**tag** *tag-value*] [**route-map** *map-tag*]

構文の説明

as-number	ルーティング プロセスの自律システム番号を指定します。有効値の範囲は 1 ～ 65535 です。
external	指定した自律システムの外部にあり、タイプ 1 またはタイプ 2 の外部ルートとして OSPFv3 にインポートされる OSPFv3 メトリック ルートを指定します。有効な値は、1 または 2 です。
include-connected	（オプション）ソース プロトコルから学習したルートと、ソース プロトコルが動作しているインターフェイス上の接続先プレフィックスを、ターゲット プロトコルで再配布できるようにします。
internal	指定した自律システムの内部にある OSPFv3 メトリック ルートを指定します。
level-1	Intermediate System-to-Intermediate System（IS-IS）用に、レベル 1 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
level-1-2	IS-IS 用に、レベル 1 とレベル 2 の両方のルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
level-2	IS-IS 用に、レベル 2 ルートが他の IP ルーティング プロトコルに個別に再配布されることを指定します。
map-tag	設定したルート マップの識別情報を指定します。
match	（オプション）他のルーティング ドメインにルートを再配布します。
metric *metric_value*	（オプション）OSPFv3 のデフォルト メトリック値を指定します。有効な値の範囲は、0 ～ 16777214 です。

metric-type *metric_type*	（オプション）OSPFv3 ルーティング ドメインにアドバタイズされるデフォルトのルートに関連付けられる外部リンク タイプを指定します。1（タイプ 1 外部ルート）または 2（タイプ 2 外部ルート）を指定できます。
nssa-external	自律システムの外部にあり、タイプ 1 またはタイプ 2 の外部ルートとして IPv6 用の Not-So-Stubby Area（NSSA）の OSPFv3 にインポートされるルートを指定します。
process-id	（オプション）OSPFv3 ルーティング プロセスをイネーブルにする場合に管理目的で割り当てる番号を指定します。
route-map *map_name*	（オプション）送信元ルーティング プロトコルから現在の OSPFv3 ルーティング プロトコルにインポートするルートをフィルタリングするために使用するルート マップの名前を指定します。このキーワードを指定し、ルート マップ タグを 1 つも指定しないと、いずれのルートもインポートされません。指定しない場合は、すべてのルートが再配布されます。
source-protocol	ルートの再配布元のプロトコルを指定します。有効な値は、connected、ospf、または static です。
tag *tag_value*	（オプション）各外部ルートに付加する 32 ビットの 10 進値を指定します。この値は OSPFv3 自身には使用されませんが、ASBR 間の情報伝達に使用できます。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効値の範囲は、0 ～ 4294967295 です。
transparent	（オプション）再配布ルートのルーティング テーブル メトリックを RIP メトリックとして使用します。

コマンド デフォルト

コマンドのデフォルトは次のとおりです。

- **metric** *metric-value*：**0**
- **metric-type** *type-value*：**2**
- **match**：**internal**、**external 1**、**external 2**
- **tag** *tag-value*：**0**

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPv6 ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

例

次に、スタティック ルートを現在の OSPFv3 プロセスに再配布する例を示します。

```
ciscoasa(config-if)# ipv6
 router ospf 1
ciscoasa(config-rtr)# redistribute static
```

関連コマンド

コマンド	説明
ipv6 router ospf	OSPFv3 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 ipv6 router	OSPFv3 のルータ コンフィギュレーションのコマンドを表示します。

redistribute（ルータ EIGRP）

1 つのルーティングドメインから EIGRP ルーティングプロセスにルートを再配布するには、ルータ EIGRP コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** } [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*
no redistribute { { **eigrp** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** } [**metric** *bandwidth delay reliability load mtu*] [**route-map** *map_name*

構文の説明

bandwidth	EIGRP 帯域幅メトリック（キロビット/秒）。有効な値は、1 ～ 4294967295 です。
connected	インターフェイスに接続されているネットワークを EIGRP ルーティング プロセスに再配布することを指定します。
delay	EIGRP 遅延メトリック（10 マイクロ秒単位）有効な値は、0 ～ 4294967295 です。
external *type*	指定した自律システムの外部にある EIGRP メトリック ルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある EIGRP メトリック ルートを指定します。
load	EIGRP 有効帯域幅（負荷）メトリック。有効な値は、1 ～ 255 です（255 は 100% の負荷を示します）。
match	（任意）OSPF から EIGRP にルートを再配布する条件を指定します。
metric	（任意）EIGRP ルーティング プロセスに再配布されるルートの EIGRP メトリックの値を指定します。
mtu	パスの MTU。有効値は 1 ～ 65535 です。
nssa-external *type*	NSSA の外部にあるルートの EIGRP メトリック タイプを指定します。有効な値は、**1** または **2** です。
eigrp *pid*	EIGRP ルーティング プロセスに EIGRP ルーティング プロセスを再配布するために使用します。*pid* では、EIGRP ルーティング プロセス内部で使用される識別パラメータを指定します。有効値は 1 ～ 65535 です。
信頼性	EIGRP 信頼性メトリック。有効な値は、0 ～ 255 です（255 は 100% の信頼性を示します）。
rip	RIP ルーティング プロセスから EIGRP ルーティング プロセスへのネットワークの再配布を指定します。

route-map *map_name*	（任意）送信元ルーティング プロトコルから EIGRP ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルートマップの名前。指定しない場合は、すべてのルートが再配布されます。
static	EIGRP ルーティング プロセスにスタティック ルートを再配布するために使用します。

コマンド デフォルト

コマンドのデフォルトは次のとおりです。

- **match**：**Internal**、**external 1**、**external 2**

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ EIGRP コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

EIGRP 構成に **default-metric** コマンドを設定していない場合は、redistribute コマンドで **metric** を指定する必要があります。

例

次に、スタティック ルートおよび接続ルートを EIGRP ルーティング プロセスに再配布する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# redistribute static
ciscoasa(config-router)# redistribute connected
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスを作成し、このプロセスのコンフィギュレーション モードを開始します。

コマンド	説明
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。

redistribute（ルータ OSPF）

1 つのルーティングドメインから OSPF ルーティングプロセスにルートを再配布するには、ルータ OSPF コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式をオプションを指定せずに使用します。このコマンドの **no** 形式でオプションを指定した場合、そのオプションの構成だけが削除されます。

redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]
no redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**metric-type** *metric_type*] [**route-map** *map_name*] [**tag** *tag_value*] [**subnets**]

構文の説明

connected	インターフェイスに接続されているネットワークを OSPF ルーティング プロセスに再配布することを指定します。
eigrp *as-number*	OSPF ルーティング プロセスに EIGRP ルートを再配布するために使用します。*as-number* は、EIGRP ルーティング プロセスの自律システム番号を指定します。有効値は 1 ～ 65535 です。
external *type*	指定した自律システムの外部にある OSPF メトリックルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある OSPF メトリック ルートを指定します。
match	（任意）あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布するための条件を指定します。
metric *metric_value*	（任意）OSPF のデフォルト メトリック値を、0 ～ 16777214 の範囲で指定します。
metric-type *metric_type*	（任意）OSPF ルーティング ドメインにアドバタイズされるデフォルト ルートに関連付けられている外部リンク タイプ。**1**（タイプ 1 外部ルート）または **2**（タイプ 2 外部ルート）のいずれかの値を指定できます。
nssa-external *type*	NSSA の外部にあるルートの OSPF メトリックタイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	現在の OSPF ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
rip	RIP ルーティング プロセスから現在の OSPF ルーティング プロセスへのネットワークの再配布を指定します。

route-map *map_name*	（任意）送信元ルーティング プロトコルから現在の OSPF ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルートマップの名前。指定しない場合は、すべてのルートが再配布されます。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。
subnets	（任意）OSPF へのルートの再配布において、指定したプロトコルの再配布の範囲を指定します。使用しない場合は、クラスフル ルートのみが再配布されます。
tag *tag_value*	（任意）各外部ルートに付けられた 32 ビットの 10 進値。この値は OSPF 自体には使用されません。ASBR 間での情報通信に使用されることはあります。何も指定しない場合、BGP および EGP からのルートにはリモート自律システムの番号が使用され、その他のプロトコルには 0 が使用されます。有効値の範囲は、0 ～ 4294967295 です。

コマンド デフォルト

コマンドのデフォルトは次のとおりです。

- **metric** *metric-value*：0
- **metric-type** *type-value*：**2**
- **match**：**Internal**、**external 1**、**external 2**
- **tag** *tag-value*：0

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ OSPF コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	このコマンドは、**rip** キーワードを含むように変更されました。
8.0(2)	このコマンドは、**eigrp** キーワードを含むように変更されました。

リリース	変更内容
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

例

次に、スタティック ルートを現在の OSPF プロセスに再配布する例を示します。

```
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# redistribute static
```

関連コマンド

コマンド	説明
redistribute (RIP)	RIP ルーティング プロセスにルートを再配布します。
router ospf	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。

redistribute（ルータ RIP）

別のルーティングドメインからRIPルーティングプロセスにルートを再配布するには、ルータ RIP コンフィギュレーション モードで **redistribute** コマンドを使用します。再配布を削除するには、このコマンドの **no** 形式を使用します。

redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**transparent**] [**route-map** *map_name*]
no redistribute { { **ospf** *pid* [**match** { **internal** | **external** [**1** | **2**] | **nssa-external** [**1** | **2**] }] } | **rip** | **static** | **connected** | **eigrp** *as-number* } [**metric** *metric_value*] [**transparent**] [**route-map** *map_name*]

構文の説明

connected	インターフェイスに接続されているネットワークを RIP ルーティング プロセスに再配布することを指定します。
eigrp *as-number*	RIP ルーティング プロセスに EIGRP ルートを再配布するために使用します。*as-number* は、EIGRP ルーティング プロセスの自律システム番号を指定します。有効値は 1 ～ 65535 です。
external *type*	指定した自律システムの外部にある OSPF メトリックルートを指定します。有効な値は、**1** または **2** です。
internal *type*	指定した自律システムの内部にある OSPF メトリック ルートを指定します。
match	（任意）OSPF から RIP にルートを再配布する条件を指定します。
metric {*metric_value* | **transparent**}	（任意）再配布するルートの RIP メトリック値を指定します。*metric_value* の有効な値は、0 ～ 16 です。メトリックを **transparent** に設定すると、現在のルートメトリックが使用されます。
nssa-external *type*	Not-So-Stubby Area（NSSA）の外部にあるルートの OSPF メトリック タイプを指定します。有効な値は、**1** または **2** です。
ospf *pid*	RIP ルーティング プロセスに OSPF ルーティング プロセスを再配布するために使用します。*pid* は OSPF ルーティング プロセス用に内部で使用される ID パラメータを指定します。有効な値は 1 ～ 65535 です。
route-map *map_name*	（任意）送信元ルーティング プロトコルから RIP ルーティング プロセスにインポートされるルートをフィルタリングするために使用されるルート マップの名前。指定しない場合は、すべてのルートが再配布されます。
static	スタティック ルートを OSPF プロセスに再配布するために使用されます。

コマンド デフォルト

コマンドのデフォルトは次のとおりです。

- **metric** *metric-value*：0
- **match**：**Internal**、**external 1**、**external 2**

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ RIP コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	このコマンドは、**eigrp** キーワードを含むように変更されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

例

次に、スタティック ルートを現在の RIP プロセスに再配布する例を示します。

```
ciscoasa(config)# router rip
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# redistribute static metric 2
```

関連コマンド

コマンド	説明
redistribute (router eigrp)	他のルーティング ドメインから EIGRP にルートを再配布します。
redistribute (router ospf)	他のルーティング ドメインから OSPF にルートを再配布します。
router rip	RIP ルーティング プロセスをイネーブルにして、そのプロセスのルータ 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。

redistribute isis

特にレベル 1 からレベル 2 またはレベル 2 からレベル 1 へ IS-IS ルートを再配布するには、ルータ ISIS コンフィギュレーション モードで **redistribute isis** コマンドを使用します。再配布を無効にするには、このコマンドの **no** 形式を使用します。

redistribute isis ip { **level-1** | **level-2** } **into** { **level-2** | **level-1** } [[**distribute-list** *list-number*] | [**route-map** *map-tag*]]
no redistribute isis ip { **level-1** | **level-2** } **into** { **level-2** | **level-1** } [[**distribute-list** *list-number*] | [**route-map** *map-tag*]]

構文の説明

level-1 | level-2	IS-IS ルートを再配布するレベル元とレベル先。
into	ルートが再配布されるレベル元と、ルートを再配布するレベル先を区別するキーワード。
distribute-list *list-number*	（任意）IS-IS 再配布を制御する配布リスト番号。配布リストまたはルートマップのいずれかを指定できますが、両方を指定できません。
route-map *map-tag*	（任意）IS-IS 再配布を制御するルートマップ名。配布リストまたはルートマップのいずれかを指定できますが、両方を指定できません。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ isis コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

IS-IS では、すべてのエリアがスタブ エリアで、バックボーン（レベル 2）からエリア（レベル 1）へルーティング情報がリークしません。レベル 1 だけのルートは、そのエリア内にある最も近いレベル 1 - レベル 2 ルータへのデフォルト ルートを使用します。このコマンドにより、レベル 2 IP ルートをレベル 1 エリアに再配布することができます。この再配布により、レベル 1 だけのルータが IP プレフィックスのエリア外への最良パスを選択することができるよ

うになります。これは IP のみの機能であり、CLNS ルーティングはまだスタブ ルーティングです。

制御と安定性を増すために、配布リストまたはルートマップを設定して、どのレベル 2 IP ルートをレベル 1 に再配布できるのかを制御できます。これを使用すると、大規模な IS-IS-IP ネットワークは、スケーラビリティを向上させるためにエリアを使用できます。

（注） **redistribute isis** コマンドを機能させるためには、**metric-style wide** コマンドを指定する必要があります。

例

次の例では、アクセス リスト 100 がレベル 1 からレベル 2 への IS-IS の再配布を制御しています。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 distribute-list 100
ciscoasa(config-router)# access-list 100 permit ip 10.10.10.0 0.0.0.255 any
```

次の例では、110 のタグの付いたルートだけが再配布されるように、match-tag という名前のルート マップがレベル 1 からレベル 2 への IS-IS の再配布を制御します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# net 49.0000.0000.0001.00
ciscoasa(config-router)# metric-style wide
ciscoasa(config-router)# redistribute isis ip level-1 into level-2 route-map match-tag
ciscoasa(config-router)# route-map match-tag permit 10
ciscoasa(config-router)# match tag 11
```

関連コマンド

redundant-interface

アクティブにする冗長インターフェイスのメンバーインターフェイスを設定するには、特権 EXEC モードで **redundant-interface** コマンドを使用します。

redundant-interface redundant *number* **active-member** *physical_interface*

構文の説明

active-member *physical_interface*	アクティブ メンバーを設定します。有効値については、**interface** コマンドを参照してください。両方のメンバー インターフェイスが同じ物理タイプである必要があります。
redundant *number*	冗長インターフェイス ID（**redundant1** など）を指定します。

コマンド デフォルト

デフォルトで、コンフィギュレーション内の最初のメンバーインターフェイスが使用可能な場合、そのインターフェイスがアクティブ インターフェイスとなります。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

どのインターフェイスがアクティブであるかを表示するには、次のコマンドを入力します。

```
ciscoasa# show interface redundant
number
 detail
 | grep Member
```

次に例を示します。

```
ciscoasa# show interface redundant1
 detail
 | grep Member
      Members GigabitEthernet0/3(Active), GigabitEthernet0/2
```

例

次に、冗長インターフェイスを作成する例を示します。デフォルトでは、gigabitethernet 0/0がコンフィギュレーション内の最初のインターフェイスであるため、このインターフェイスがアクティブです。redundant-interface コマンドでは、gigabitethernet 0/1 をアクティブ インターフェイスに設定しています。

```
ciscoasa(config-if)# interface redundant 1
ciscoasa(config-if)# member-interface gigabitethernet 0/0
ciscoasa(config-if)# member-interface gigabitethernet 0/1
ciscoasa(config-if)# redundant-interface redundant1 active-member gigabitethernet0/1
```

関連コマンド

コマンド	説明
clear interface	**show interface** コマンドのカウンタをクリアします。
debug redundant-interface	冗長インターフェイスのイベントまたはエラーに関するデバッグ メッセージを表示します。
interface redundant	冗長インターフェイスを作成します。
member-interface	冗長インターフェイス ペアにメンバー インターフェイスを割り当てます。
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。

regex

テキストを照合する正規表現を作成するには、グローバル コンフィギュレーション モードで **regex** コマンドを使用します。正規表現を削除するには、このコマンドの **no** 形式を使用します。

regex *name regular_expression*
regex *name* [*regular_expression*]

構文の説明

name	正規表現名を最大 40 文字で指定します。
regular_expression	最大 100 文字の正規表現を指定します。正規表現で使用できるメタ文字のリストについては、「使用上のガイドライン」を参照してください。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

regex コマンドは、テキスト照合が必要なさまざまな機能で使用できます。たとえば、インスペクション ポリシー マップを使用して、モジュラ ポリシー フレームワークを使用したアプリケーション インスペクションの特別なアクションを設定できます（**policy map type inspect** コマンドを参照）。インスペクション ポリシー マップでは、1 つ以上の **match** コマンドを含んだインスペクション クラスマップを作成することで、アクションの実行対象となるトラフィックを識別できます。または、**match** コマンドをインスペクション ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケット内のテキストを正規表現を使用して識別できます。たとえば、HTTP パケット内の URL 文字列を照合できます。正規表現クラスマップで正規表現をグループ化できます（**class-map type regex** コマンドを参照）。

正規表現は、ストリングそのものとしてテキスト ストリングと文字どおりに照合することも、*metacharacters* を使用してテキスト ストリングの複数のバリアントと照合することもできます。

正規表現を使用して、特定のアプリケーショントラフィックの内容（HTTP パケット内の本文テキストなど）を照合できます。

（注） 最適化のために、ASA では、難読化解除された URL が検索されます。難読化解除では、複数のスラッシュ（/）が単一のスラッシュに圧縮されます。通常、「http://」のようなダブル スラッシュが使用される文字列では、代わりに「http:/」を検索してください。

表 7 : regex メタ文字 に、特別な意味を持つメタ文字の一覧を示します。

表 *7: regex* メタ文字

文字	説明	注記
.	ドット	任意の単一文字と一致します。たとえば、**d.g** は、dog、dag、dtg、およびこれらの文字を含む任意の単語（doggonnit など）に一致します。
(*exp***)**	サブ表現	サブ表現は、文字を周囲の文字から分離して、サブ表現に他のメタ文字を使用できるようにします。たとえば、**d(o|a)g** は dog および dag に一致しますが、**do|ag** は do および ag に一致します。また、サブ表現を繰り返し限定作用素とともに使用して、繰り返す文字を区別できます。たとえば、**ab(xy){3}z** は、abxyxyxyz に一致します。
|	代替	このメタ文字によって区切られている複数の表現のいずれかと一致します。たとえば、**dog|cat** は、dog または cat に一致します。
?	疑問符	直前の表現が 0 または 1 個存在することを示す修飾子。たとえば、**lo?se** は、lse または lose に一致します。 （注） **Ctrl+V** を入力してから疑問符を入力しないと、ヘルプ機能が呼び出されます。
*	アスタリスク	直前の表現が 0、1、または任意の個数存在することを示す修飾子。たとえば、**lo*se** は、lse、lose、loose などに一致します。
+	プラス	直前の表現が少なくとも 1 個存在することを示す修飾子。たとえば、**lo+se** は、lose および loose に一致しますが、lse には一致しません。
{*x***}** または **{***x***,}**	最小繰り返し限定作用素	少なくとも *x* 回繰り返します。たとえば、 **ab(xy){2,}z** は、abxyxyz や abxyxyxyz などに一致します。
[*abc***]**	文字クラス	カッコ内の任意の文字と一致します。たとえば、**[abc]** は、a、b、または c に一致します。

文字	説明	注記
[^*abc*]	否定文字クラス	角カッコに含まれていない単一文字と一致します。たとえば、**[^abc]** は a、b、c 以外の任意の文字に一致し、**[^A-Z]** は大文字以外の任意の 1 文字に一致します。
[*a-c*]	文字範囲クラス	範囲内の任意の文字と一致します。**[a-z]** は、任意の小文字と一致します。文字と範囲の組み合わせも可能です。**[abcq-z]** は、a、b、c、q、r、s、t、u、v、w、x、y、z、および**[a-cq-z]** に一致します。 ダッシュ（-）文字は、角カッコ内の最初の文字または最後の文字である場合にのみリテラルとなります（**[abc-]** や **[-abc]**）。
""	引用符	文字列の末尾または先頭のスペースを保持します。たとえば、**"test"** は、一致を検索する場合に先頭のスペースを保持します。
^	キャレット	行の先頭を指定します。
\	エスケープ文字	メタ文字とともに使用すると、リテラル文字と一致します。たとえば、**\[** は左角カッコに一致します。
char	文字	文字がメタ文字でない場合は、リテラル文字と一致します。
\r	復帰	復帰 0x0d と一致します。
\n	改行	改行 0x0a と一致します。
\t	タブ	タブ 0x09 と一致します。
\f	改ページ	フォーム フィード 0x0c と一致します。
\x*NN*	エスケープされた 16 進数	16 進数（厳密に 2 桁）を使用した ASCII 文字と一致します。
\NNN	エスケープされた 8 進数	8 進数（厳密に 3 桁）としての ASCII 文字と一致します。たとえば、文字 040 はスペースを表します。

使用上のガイドライン

正規表現が想定どおりに一致するかどうかをテストするには、**test regex** コマンドを入力します。

正規表現のパフォーマンスへの影響は、主に次の 2 つの要因によって決定されます。

- 正規表現照合で検索される必要があるテキストの長さ。

検索長が短い場合は、正規表現エンジンの ASA に対するパフォーマンス上の影響は小さくなります。

- 正規表現照合で検索される必要がある正規表現チェーン テーブルの数。

検索長のパフォーマンスへの影響

正規表現検索を設定すると、通常は、検索対象テキストのすべてのバイトが正規表現データベースに対して検査されて、一致が検索されます。検索対象テキストが長くなるほど、検索時間も長くなります。次に、この現象を表すパフォーマンス テスト ケースを示します。

- ある HTTP トランザクションでは、1 回の 300 バイトの GET 要求と 1 回の 3250 バイトの応答が行われます。
- URI 検索には 445 の正規表現が、要求本文検索には 34 の正規表現が使用されます。
- 応答本文検索には 55 の正規表現が使用されます。

URI および HTTP GET 要求の本文のみを検索するようにポリシーを設定すると、スループットは次のようになります。

- 対応する正規表現データベースが検索されない場合は 420 Mbps。
- 対応する正規表現データベースが検索される場合は 413 Mbps（正規表現を使用するオーバーヘッドが比較的小さいことがわかります）。

ただし、HTTP 応答本文全体も検索するようにポリシーを設定すると、応答本文の検索対象が長いため（3250 バイト）、スループットは 145 Mbps まで低下します。

正規表現検索のテキスト長が長くなる要因は次のとおりです。

- 複数の異なるプロトコル フィールドに対して正規表現検索が設定されている場合。たとえば、HTTP インスペクションでは、URI にのみ正規表現照合が設定されていると、URI フィールドのみが正規表現照合のために検索され、検索長は URI 長に制限されます。ただし、ヘッダーや本文などの他のプロトコル フィールドにも正規表現照合が設定されていると、ヘッダー長や本文長の分だけ検索長が長くなります。
- 検索対象のフィールドが長い場合。たとえば、URI に正規表現検索が設定されている場合、GET 要求内の長い URI の検索長は長くなります。また、現在、HTTP 本文の検索長はデフォルトで 200 バイトまでに制限されています。ただし、本文を検索するようにポリシーを設定し、本文検索長が 5000 バイトに変更されると、本文検索が長くなるため、パフォーマンスに対して大きな影響があります。

正規表現チェーンテーブル数のパフォーマンスへの影響

現在、同じプロトコル フィールドに設定されたすべての正規表現（URI に対するすべての正規表現など）は、1 つ以上の正規表現チェーン テーブルで構成されるデータベースに構築されます。テーブルの数は、必要な合計メモリ量、およびテーブル構築時に使用可能なメモリ量によって決定されます。次のいずれかの条件が満たされる場合、正規表現データベースは複数のテーブルに分割されます。

- 必要な合計メモリが 32 MB を超える場合。これは、最大テーブル サイズが 32 MB に制限されているためです。

- 最大連続メモリ サイズが正規表現データベース全体を構築するのに十分ではない場合、複数の小さなテーブルが構築されて、それらのテーブルにすべての正規表現が格納されます。メモリ フラグメンテーションの程度は、相互に関連する数多くの要因によって左右されるため、フラグメンテーションのレベルを予測することは事実上不可能です。

複数のチェーン テーブルがある場合、正規表現照合において各テーブルが検索される必要があるため、検索時間は検索対象のテーブル数に比例して長くなります。

特定のタイプの正規表現では、テーブル サイズが大幅に増加する傾向があります。可能な限りワイルドカードおよび繰り返し要素を避けるように正規表現を設計することを推奨します。次のメタ文字については、表 7 : regex メタ文字 を参照してください。

- ワイルドカード タイプの指定を伴う正規表現
- ドット（.）
- クラス内の任意の文字に一致するさまざまな文字クラス
- [^a-z]
- [a-z]
- [abc]]
- 繰り返しタイプの指定を伴う正規表現
- *
- +
- {n,}
- 次のようにワイルドカードタイプの正規表現と繰り返しタイプの正規表現を組み合わせると、テーブル サイズが大幅に増加する可能性があります。
- 123.*xyz
- 123.+xyz
- [^a-z]+
- [^a-z]*
- .*123.*（これは、「123」と照合することと同じであるため、このような指定は行わないでください）。

次に、ワイルドカードや繰り返しの有無によって正規表現のメモリ使用量がどのように異なるかについての例を示します。

- 次の 4 つの正規表現のデータベース サイズは 958,464 バイトです。

```
regex r1 "q3rfict9(af.*12)*ercvdf"
regex r2 "qtaefce.*qeraf.*adasdfev"
regex r3 "asdfdfdfds.*wererewr0e.*aaaxxxx.*xxx"
regex r4 "asdfdfdfds.*wererewr0e.*afdsvcvr.*aefdd"
```

• 次の 4 つの正規表現のデータベース サイズはわずか 10240 バイトです。

```
regex s1 "abcde"
regex s2 "12345"
regex s3 "123xyz"
regex s4 "xyz123"
```

正規表現の数が増えると、正規表現データベースで必要になる合計メモリ量も増え、そのためメモリがフラグメント化されている場合にはより多くのテーブル数が必要になる可能性があります。次に、異なる正規表現数でのメモリ使用量の例を示します。

• 100 サンプル URI：3,079,168 バイト

• 200 サンプル URI：7,156,224 バイト

• 500 サンプル URI：11,198,971 バイト

（注） コンテキストごとの正規表現の最大数は 2048 です。**debug menu regex 40 10** コマンドを使用して、各 regex データベースにあるチェーンテーブルの数を表示できます。

例

次に、インスペクション ポリシー マップで使用する 2 つの正規表現を作成する例を示します。

```
ciscoasa(config)# regex url_example example\.com
ciscoasa(config)# regex url_example2 example2\.com
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックと照合するインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
class-map type regex	正規表現クラス マップを作成します。
test regex	正規表現をテストします。

reload

リブートして構成をリロードするには、特権 EXEC モードで **reload** コマンドを使用します。

reload [**at** *hh* : *mm* [*month day* | *day month*]] [**cancel**] [**in** [*hh* :] *mm*] [**max-hold-time** [*hh* :] *mm*] [**noconfirm**] [**quick**] [**reason** *text*] [**save-config**]

構文の説明

at *hh*:*mm*	（任意）ソフトウェアのリロードが（24 時間制で）指定された時刻に行われるようにスケジューリングします。月日を指定しない場合、リロードは、指定時刻が現在時刻よりも後の場合は当日の指定時刻に、指定時刻が現在時刻よりも前の場合は翌日の指定時刻に行われます。00:00 を指定すると、深夜 0 時のリロードが設定されます。リロードは、24 時間以内に実行される必要があります。
cancel	（任意）スケジューリングされているリロードをキャンセルします。
day	（任意）1 ～ 31 の範囲で日付を指定します。
in [*hh*:]*mm*]	（任意）指定した分数、または時間および分数が経過したときにソフトウェアがリロードされるようにスケジューリングします。リロードは、24 時間以内に実行される必要があります。
max-hold-time [*hh*:*mm*	（任意）シャットダウンまたはリブートの前に他のサブシステムに対して通知するために ASA が待機する最大ホールド時間を指定します。この時間が経過すると、（強制）クイック シャットダウンまたはリブートが実行されます。
month	（任意）月の名前を指定します。月の名前を表す一意のストリングを作成するために十分な文字を入力します。たとえば、「Ju」は、June または July を表すことができるため一意ではありませんが、「Jul」は一意です。これは、「Jul」で始まる月は「July」しかないためです。
noconfirm	（任意）ユーザーの確認なしでリロードすることを ASA に許可します。
quick	（任意）通知したり、すべてのサブシステムを正常にシャットダウンしたりすることなく、クイック リロードを強制します。
reason *text*	（任意）リロードの理由を 1 ～ 255 文字で指定します。理由のテキストは、すべての開いている IPsec VPN クライアント、端末、コンソール、Telnet、SSH、および ASDM 接続またはセッションに送信されます。 （注） ISAKMP などの一部のアプリケーションでは、IPsec VPN クライアントに理由のテキストを送信するために追加のコンフィギュレーションが必要となります。詳細については、VPN CLI 設定ガイドを参照してください。

save-config	（任意）シャットダウンの前に、実行コンフィギュレーションをメモリに保存します。**save-config** キーワードを入力しない場合、未保存の構成の変更はリロード後にすべて失われます。
save-show-tech	（任意）リロードの実行前に **show tech** コマンドの出力をファイルに保存します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが変更されて、*day*、*hh*、*mm*、*month*、**quick**、**save-config**、および *text* という新しい引数とキーワードが追加されました。
9.1(3)	**save-show-tech** キーワードが追加されました。

使用上のガイドライン

このコマンドを使用すると、ASA をリブートして、構成をフラッシュメモリからリロードできます。

reload コマンドは、デフォルトではインタラクティブです。ASA は、まず構成が変更されていて、未保存であるかどうかをチェックします。未保存の場合、構成を保存するように求められます。マルチコンテキストモードでは、ASA によって、未保存の構成がある各コンテキストに対してプロンプトが表示されます。**save-config** キーワードを指定すると、構成はプロンプトなしで保存されます。次に、システムのリロードを確認するプロンプトが表示されます。**y** と入力するか、または **Enter** キーを押した場合にのみリロードが行われます。確認後、ASA は遅延キーワード（**in** または **at**）の指定状況に応じて、リロードプロセスを開始またはスケジューリングします。

デフォルトでは、リロードプロセスは「グレースフル」モードで実行されます。すべての登録されているサブシステムは、リブート実行の前に通知されるため、リブート前に適切にシャットダウンできます。このようなシャットダウンが発生するまで待機しない場合は、**max-hold-time** キーワードを指定して、待機する最大時間を指定します。または、**quick** キーワードを使用して、影響のあるサブシステムに通知したり、グレースフルシャットダウンを待機したりせずに、すぐに強制的にリロードプロセスを開始できます。

noconfirm キーワードを指定すると、**reload** コマンドを非対話形式で強制的に実行できます。この場合、ASA では、**save-config** キーワードを指定していない限り、未保存の構成の有無はチェックされません。また、システムをリブートする前に、確認のプロンプトは表示されません。遅延キーワードを指定していない限り、リロードプロセスがすぐに開始またはスケジューリングされます。ただし、**max-hold-time** キーワードまたは **quick** キーワードを指定して、動作またはリロードプロセスを制御できます。

スケジューリングされたリロードをキャンセルするには、**reload cancel** コマンドを使用します。すでに進行中のリロードはキャンセルできません。

（注） フラッシュパーティションに書き込まれていないコンフィギュレーションの変更は、リロード後に失われます。リブートの前に、**write memory** コマンドを入力して、フラッシュパーティションに現在の構成を保存してください。

例

次に、リブートしてコンフィギュレーションをリロードする例を示します。

```
ciscoasa#
reload
Proceed with ?  [confirm]
 y
Rebooting...
XXX
Bios VX.X
...
```

関連コマンド

コマンド	説明
show reload	ASA のリロードステータスを表示します。

remote-access threshold session-threshold-exceeded

しきい値を設定するには、グローバル コンフィギュレーション モードで **remote-access threshold** コマンドを使用します。しきい値を削除するには、このコマンドの **no** 形式を使用します。このコマンドは、アクティブなリモートアクセスセッションの数を指定します。この数を超えると、ASA によってトラップが送信されます。

remote-access threshold session-threshold-exceeded *threshold-value*
no **remote-access threshold session-threshold-exceeded**

構文の説明

threshold-value	ASA でサポートされるセッションの制限数以下の整数を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、しきい値を 1500 に設定する例を示します。

```
ciscoasa# remote-access threshold session-threshold-exceeded 1500
```

関連コマンド

コマンド	説明
snmp-server enable trap remote-access	しきい値によるトラッピングをイネーブルにします。

rename（クラス マップ）

クラスマップの名前を変更するには、クラスマップ コンフィギュレーション モードで**rename** コマンドを入力します。

rename *new_name*

構文の説明

new_name	クラス マップの新しい名前を最大 40 文字で指定します。「class-default」という名前は予約されています。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クラスマップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、test というクラス マップの名前を test2 に変更する例を示します。

```
ciscoasa(config)# class-map test
ciscoasa(config-cmap)# rename test2
```

関連コマンド

コマンド	説明
class-map	クラスマップを作成します。

rename（特権 EXEC）

ファイルまたはディレクトリの名前を送信元のファイル名から宛先のファイル名に変更するには、特権 EXEC モードで **rename** コマンドを使用します。

rename [**/noconfirm**] [**disk0 :** | **disk1 :** | **flash:**] *source-path* [**disk0 :** | **disk1 :** | **flash:**] *destination-path*

構文の説明

/noconfirm	（任意）確認プロンプトを表示しないようにします。
destination-path	新しいファイル名のパスを指定します。
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。
source-path	元のファイル名のパスを指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

rename flash: flash: コマンドを入力すると、送信元と宛先のファイル名を入力するように求められます。

ファイル システムにまたがってファイルやディレクトリの名前を変更することはできません。

次に例を示します。

```
ciscoasa# rename flash: disk1:
Source filename []? new-config
```

```
Destination filename []? old-config
%Cannot rename between filesystems
```

例

次に、「test」というファイルの名前を「test1」に変更する例を示します。

```
ciscoasa# rename flash: flash:
Source filename [running-config]? test
Destination filename [n]? test1
```

関連コマンド

コマンド	説明
mkdir	新しいディレクトリを作成します。
rmdir	ディレクトリを削除します。
show file	ファイルシステムに関する情報を表示します。

renewal-reminder

ユーザー証明書が期限切れになる何日前に、証明書所有者に再登録の初回リマインダを送信するかを指定するには、CA サーバー コンフィギュレーション モードで **renewal-reminder** コマンドを使用します。期間をデフォルトの 14 日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。

renewal-reminder *days*
no renewal-reminder

構文の説明

days	発行されている証明書が期限切れになる何日前に証明書所有者に対して再登録の初回リマインダを送信するかを指定します。有効な値の範囲は、1 ～ 90 日です。

コマンド デフォルト

デフォルト値は 14 日間です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
CA サーバー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

通知は全部で 3 種類あります。ユーザー データベースに電子メール アドレスが指定されていれば、3 種類の通知がそれぞれ電子メールで自動的に証明書所有者に送信されます。電子メールアドレスが存在しない場合は、更新を管理者に通知する syslog メッセージが生成されます。

デフォルトでは、証明書が期限切れになる前に、CA サーバーから次の 3 種類の電子メール メッセージが指定した順序で送信されます。

1. 証明書の登録案内

2. 確認：証明書の登録案内

3. 最終確認：証明書の登録案内

最初の電子メールは案内で、2 番目の電子メールは確認、3 番目の電子メールは最終確認です。この通知のデフォルトの設定は 14 日です。証明書の有効期限の 14 日前に最初の案内が送信さ

れ、有効期限の 7 日前に確認の電子メールが送信され、有効期限の 3 日前に最終確認の電子メールが送信されます。

renewal-reminder の間隔は、**renewal-reminder** *days* コマンドを使用してカスタマイズできます。

例

次に、証明書有効期限の 7 日前に ASA からユーザーに対して有効期限通知を送信するように指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# renewal-reminder 7
ciscoasa
(config-ca-server)
#
```

次に、有効期限通知のタイミングをデフォルトである証明書有効期限の 14 日前にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa
(config-ca-server)
# no renewal-reminder
ciscoasa
(config-ca-server)
#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバー コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンドセットを使用することで、ローカル CA を設定および管理できます。
lifetime	CA 証明書、すべての発行されている証明書、および CRL のライフタイムを指定します。
show crypto ca server	ローカル CA サーバーのコンフィギュレーション詳細を表示します。

replication http

フェールオーバーグループに対してHTTP接続のレプリケーションを有効にするには、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。

replication http
no 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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
フェールオーバー グループ コンフィギュレーション	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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、ASA 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。**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出る可能性があります。

このコマンドを使用できるのは、Active/Active フェールオーバーに対してのみです。このコマンドは、Active/Active フェールオーバー構成のフェールオーバーグループ用であることを除いて、Active/Standby フェールオーバー用の **failover replication http** コマンドと機能的に同じです。

例

次の例では、フェールオーバー グループで可能な設定を示します。

```
ciscoasa(config)# failover group 1

ciscoasa(config-fover-group)# primary
ciscoasa(config-fover-group)# preempt 100
ciscoasa(config-fover-group)# replication http
ciscoasa(config-fover-group)# exit
```

関連コマンド

コマンド	説明
failover group	Active/Active フェールオーバーのためのフェールオーバー グループを定義します。
failover replication http	HTTP 接続を複製するためのステートフル フェールオーバーを設定します。

request-command deny

FTP 要求内の特定のコマンドを禁止するには、**ftp-map** コマンドを使用してアクセスできる FTP マップ コンフィギュレーション モードで **request-command deny** 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。

request-command deny { **appe** | **cdup** | **dele** | **get** | **help** | **mkd** | **put** | **rmd** | **rnfr** | **rnto** | **site** | **stou** }
no request-command deny { **appe** | **cdup** | **help** | **retr** | **rnfr** | **rnto** | **site** | **stor** | **stou** }

構文の説明

appe	ファイルへの追加を行うコマンドを拒否します。
cdup	現在の作業ディレクトリの親ディレクトリに移動するコマンドを拒否します。
dele	サーバーのファイルを削除するコマンドを拒否します。
get	サーバーからファイルを取得するクライアント コマンドを拒否します。
help	ヘルプ情報を提供するコマンドを拒否します。
mkd	サーバー上にディレクトリを作成するコマンドを拒否します。
put	サーバーにファイルを送信するクライアント コマンドを拒否します。
rmd	サーバー上のディレクトリを削除するコマンドを拒否します。
rnfr	変更元ファイル名を指定するコマンドを拒否します。
rnto	変更先ファイル名を指定するコマンドを拒否します。
site	サーバー システムに固有のコマンドを禁止します。通常、リモート管理に使用します。
stou	固有のファイル名を使用してファイルを保存するコマンドを拒否します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
FTP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、ストリクト FTP インスペクションを使用する場合に、ASA を通過する FTP 要求内で許可されるコマンドを制御するために使用します。

例

次に、**stor**、**stou**、または **appe** コマンドを含む FTP 要求を ASA でドロップする例を示します。

```
ciscoasa(config)# ftp-map inbound_ftp
ciscoasa(config-ftp-map)# request-command deny put stou appe
```

関連コマンド

コマンド	説明
class-map	セキュリティ アクションを適用するトラフィック クラスを定義します。
ftp-map	FTP マップを定義し、FTP マップ コンフィギュレーション モードをイネーブルにします。
inspect ftp	アプリケーション インスペクションに使用する特定の FTP マップを適用します。
mask-syst-reply	FTP サーバー応答をクライアントに対して非表示にします。
policy-map	特定のセキュリティ アクションにクラス マップを関連付けます。

request-data-size

SLA 動作要求パケットのペイロードのサイズを設定するには、SLA モニター プロトコル コンフィギュレーション モードで **request-data-size** 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。

request-data-size *bytes*
no request-data-size

構文の説明

bytes 要求パケットのペイロードのサイズ（バイト単位）。有効な値は、0 ～ 16384 です。最小値は、使用するプロトコルに応じて異なります。エコー タイプでは、最小値は 28 バイトです。プロトコルまたは PMTU で許可されている最大値よりも大きい値を設定しないでください。

（注） ASA によって 8 バイトのタイムスタンプがペイロードに追加されるため、実際のペイロードは *bytes* + 8 バイトになります。

コマンド デフォルト

デフォルトの *bytes* は 28 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
SLA モニター プロトコル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

到達可能性を確保するために、デフォルトのデータ サイズを大きくして、送信元と宛先との間の PMTU の変化を検出する必要がある場合があります。PMTU が低いと、セッションのパフォーマンスに影響を与える可能性が高くなります。また、低い PMTU が検出された場合は、セカンダリ パスが使用されることを示している可能性があります。

例

次の例では、ICMP エコー要求/応答時間プローブ動作を使用する、ID が 123 の SLA 動作を設定しています。この例では、エコー要求パケットのペイロード サイズを 48 バイト、SLA 動作中に送信されるエコー要求の数を 5 に設定しています。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# num-packets 5
ciscoasa(config-sla-monitor-echo)# request-data-size 48
ciscoasa(config-sla-monitor-echo)# timeout 4000
ciscoasa(config-sla-monitor-echo)# threshold 2500
ciscoasa(config-sla-monitor-echo)# frequency 10
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
```

関連コマンド

コマンド	説明
num-packets	SLA 動作中に送信する要求パケットの数を指定します。
sla monitor	SLA モニタリング動作を定義します。
type echo	SLA動作をエコー応答時間プローブ動作として設定します。

request-queue

キューで応答待ちができる GTP 要求数の最大値を指定するには、ポリシー マップ パラメータ コンフィギュレーション モードで request-queue コマンドを使用します。この数字をデフォルトの 200 に戻すには、このコマンドの **no** 形式を使用します。

request-queue *max_requests*
no request-queue *max_requests*

構文の説明

max_requests 応答を待機する GTP 要求のキューイング可能最大数（1 ～ 4294967295）。

コマンド デフォルト

デフォルトは 200 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

request-queue コマンドは、応答を待機する GTP 要求のキューイング可能最大数を指定します。この上限に達した後に新しい要求が到着すると、最も長い時間キューに入っていた要求が削除されます。「Error Indication」、「Version Not Supported」および「SGSN Context Acknowledge」というメッセージは、要求と見なされないため、応答待ち要求のキューに入れられません。

例

次に、最大要求キュー サイズを 300 に指定する例を示します。

```
ciscoasa(config)# policy-map type inspect gtp gtp-policy
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# request-queue 300
```

関連コマンド

コマンド	説明
clear service-policy inspect gtp	グローバルな GTP 統計情報をクリアします。
inspect gtp	アプリケーションインスペクションに使用する特定のGTPマップを適用します。
show service-policy inspect gtp	GTP コンフィギュレーションを表示します。

request-timeout（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

失敗した SSO 認証の試行がタイムアウトになるまでの秒数を設定するには、webvpn コンフィギュレーション モードで **request-timeout** 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。

request-timeout *seconds*
no request-timeout

構文の説明

seconds	失敗した SSO 認証の試行がタイムアウトするまでの秒数。指定できる範囲は 1 ～ 30 秒です。小数の値はサポートされていません。

コマンド デフォルト

このコマンドのデフォルト値は 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1.1	このコマンドが追加されました。
9.5(2)	SAML 2.0 がサポートされたため、このコマンドは廃止されました。

使用上のガイドライン

シングルサインオンは、WebVPN でのみサポートされています。これにより、ユーザーはユーザー名とパスワードを一度だけ入力すれば、別のサーバーでさまざまなセキュアなサービスにアクセスできます。現在、ASA では、SiteMinder-type および SAML POST-type の SSO サーバーがサポートされています。

このコマンドは SSO サーバーの両タイプに適用されます。

SSO 認証をサポートするように ASA を設定後、2 つのタイムアウトパラメータを調整できます。

- 失敗した SSO 認証の試行がタイムアウトになるまでの秒数（**request-timeout** コマンドを使用）。
- ASA が失敗した SSO 認証を再試行する回数。（**max-retry-attempts command.)** を参照）。

例

次に、webvpn 設定 sso siteminder モードで、SiteMinder-type SSO サーバー「example」の認証タイムアウトを 10 秒に設定する例を示します。

```
ciscoasa(config-webvpn)# sso-server example type siteminder
ciscoasa(config-webvpn-sso-siteminder)# request-timeout 10
```

関連コマンド

コマンド	説明
max-retry-attempts	SSO 認証に失敗した場合に ASA が再試行する回数を設定します。
policy-server-secret	SiteMinder SSO サーバーへの認証要求の暗号化に使用する秘密キーを作成します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバーの運用統計情報を表示します。
sso-server	シングル サインオン サーバーを作成します。
test sso-server	テスト認証要求で SSO サーバーをテストします。
web-agent-url	ASA が SiteMinder SSO 認証を要求する SSO サーバーの URL を指定します。

reserved-bits

TCPヘッダーの予約ビットをクリアしたり、予約ビットが設定されているパケットをドロップしたりするには、tcp マップ コンフィギュレーション モードで **reserved-bits** 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。

reserved-bits { **allow** | **clear** | **drop** }
no reserved-bits { **allow** | **clear** | **drop** }

構文の説明

allow	TCP ヘッダーの予約ビットが設定されているパケットを許可します。
clear	TCP ヘッダーの予約ビットをクリアして、パケットを許可します。
drop	TCPヘッダーの予約ビットが設定されているパケットをドロップします。

コマンド デフォルト

デフォルトで、予約ビットは許可されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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。予約ビットが設定されているパケットの末端のホストにおける処理方法を明確に指定するには、tcp マップ コンフィギュレーション モードで **reserved-bits** コマンドを使用します。処理方法が明確でないと、ASA が非同期の状態になる可能性があります。TCP ヘッダーの予約ビットをクリアしたり、予約ビットが設定されているパケットをドロップしたりできます。

例

次に、すべての TCP フローにおいて、予約ビットが設定されているパケットをクリアする例を示します。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# reserved-bits clear
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(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	接続値を設定します。
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。

reserve-port-protect

メディアネゴシエーション中の予約ポートの使用を制限するには、パラメータ コンフィギュレーション モードで **reserve-port-protect** 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。

reserve-port-protect
no reserve-port-protect

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、RTSPインスペクション ポリシーマップで予約ポートを保護する例を示します。

```
ciscoasa(config)# policy-map type inspect rtsp rtsp_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# reserve-port-protect
```

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。

コマンド	説明
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。

reset

モジュラ ポリシー フレームワークを使用する場合は、パケットをドロップし、接続を閉じ、一致またはクラス コンフィギュレーション モードで **reset** コマンドを使用して、**match** コマンドまたはクラスマップと一致するトラフィックに TCP リセットを送信します。このリセットアクションは、インスペクション ポリシー マップ（**policy-map type inspect** コマンド）でアプリケーション トラフィックに対して使用できますが、すべてのアプリケーションでリセットアクションを使用できるわけではありません。このアクション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。

reset [**log**]
no reset [**log**]

構文の説明

log 一致をログに記録します。システム ログ メッセージの番号は、アプリケーションによって異なります。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
一致コンフィギュレーションおよびクラス コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

インスペクション ポリシー マップは、1 つ以上の **match** コマンドと **class** コマンドで構成されます。インスペクション ポリシー マップで使用できる実際のコマンドは、アプリケーションによって異なります。**match** コマンドまたは **class** コマンドを入力してアプリケーション トラフィックを指定した後（**class** コマンドは、**match** コマンドを含む既存の **class-map type inspect** コマンドを参照します）、**reset** コマンドを入力して、**match** コマンドまたは **class** コマンドに一致するトラフィックに対してパケットをドロップし、接続を閉じることができます。

接続をリセットした後は、インスペクション ポリシーマップのアクションは実行されません。たとえば、最初のアクションが接続のリセットである場合、それ以降の **match** または **class** コマンドが一致することはありません。最初のアクションがパケットのログへの記録である場合、接続のリセットなどの2番目のアクションは実行されます同じ**match**コマンドまたは**class**コマンドに対して**reset** アクションと**log**アクションの両方を設定できます。その場合、パケットは特定の一致でリセットされる前にログに記録されます。

レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）で **inspect** コマンドを使用してアプリケーション インスペクションをイネーブルにする場合、このアクションを含むインスペクション ポリシー マップをイネーブルにできます。たとえば、**inspect http http_policy_map** コマンドを入力します。http_policy_map は、インスペクション ポリシー マップの名前です。

例

次に、http-traffic クラス マップに一致した場合に、接続をリセットして、ログを送信する例を示します。同じパケットが 2 番めの **match** コマンドにも一致する場合、そのパケットはすでにドロップされているため、処理されません。

```
ciscoasa(config-cmap)# policy-map type inspect http http-map1
ciscoasa(config-pmap)# class http-traffic
ciscoasa(config-pmap-c)# reset log
ciscoasa(config-pmap-c)# match req-resp content-type mismatch
ciscoasa(config-pmap-c)# reset log
```

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。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
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。

resolver

DNS 要求を解決する Cisco Umbrella DNS サーバーのアドレスを設定するには、Cisco Umbrella コンフィギュレーション モードで **resolver** 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。

resolver { **ipv4** | **ipv6** } *ip_address*
no resolver { **ipv4** | **ipv6** } *ip_address*

構文の説明

ipv4 *ip_address*	使用する Umbrella DNS サーバーの IPv4 アドレス。
ipv6 *ip_address*	使用する Umbrella DNS サーバーの IPv6 アドレス。

コマンド デフォルト

デフォルトの DNS リゾルバは 208.67.220.220 および 2620:119:53::53 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Umbrella の設定	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.12(1)	このコマンドが追加されました。

使用上のガイドライン

コマンドを2回入力して、IPv4アドレスとIPv6アドレスの両方を設定できます。有効なUmbrella DNS サーバーのみを指定できます。

例

次の例は、Cisco Umbrella のデフォルト以外の DNS リゾルバを定義しています。サーバーは 208.67.222.222 および 2620:119:35::35 です。

```
ciscoasa(config)# umbrella-global

ciscoasa(config-umbrella)# resolver ipv4 208.67.222.222

ciscoasa(config-umbrella)# resolver ipv6 2620:119:35::35
```

関連コマンド

コマンド	説明
umbrella-global	Cisco Umbrella グローバルパラメータを設定します。

responder-only

VTI トンネルの一端をレスポンダとしてのみ動作するように設定するには、IPsec プロファイル コンフィギュレーション モードで responder-only コマンドを使用します。レスポンダ専用モ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。

responder-only
no responder-only

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
IPsec プロファイル設定	• 対応	• ×	• 対応	—	—

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用して、VTI トンネルの一端がレスポンダとしてのみ動作するように設定できます。

レスポンダ専用の一端は、トンネルまたはキー再生成を開始しません。

このオプションは、コリジョン処理が使用できない場合、または IKEv1 を使用しているときにトンネルの両端が同時にトンネリングを開始する場合に便利です。レスポンダ専用の終端上の IKE トンネルまたは IPsec トンネルのキー再生成設定は、設定済みの場合もすべて無視されます。

例

次に、IPsec プロファイルにレスポンダ専用モードを追加する例を示します。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
ciscoasa(config-ipsec-profile)# responder-only
```

関連コマンド

コマンド	説明
crypto ipsec profile	新しい IPsec プロファイルを作成します。
set ikev1 transform-set	IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。
set pfs	PFS グループを IPsec プロファイル設定に使用するように指定します。
set security-association lifetime	IPsec プロファイル設定でのセキュリティ アソシエーションの期間を指定します。これは、キロバイト単位か秒単位、またはその両方で指定します。
set trustpoint	VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

rest-api

インストール済みの REST API エージェントをフラッシュから有効にするには、**agent** キーワードを使用します。エージェント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。

この ASA に REST API パッケージをダウンロード（**copy** コマンドを使用）した後、パッケージを確認してインストールするには、image キーワードを使用します。REST API エージェントのバージョンと ASA のバージョンが一致している必要があります。このパッケージをアンインストールするには、このコマンドの no 形式を使用します。

rest-api [**agent** | **image disk0 :** / *package*]
no rest-api [**agent** | **image disk0 :** / *package*]

構文の説明

agent	インストール済みの REST API エージェントをイネーブルにします。
image disk0:/*package*	*package* で指定したダウンロード済みの REST API イメージをインストールします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
REST API エージェントのイネーブル化/ディセーブル化	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。

使用上のガイドライン

指定した REST API パッケージについて互換性と有効性のチェックを実行するには、**image** キーワードを指定してこのコマンドを発行します。パッケージがすべてのチェックにパスすると、内部フラッシュにインストールされます。

REST API のコンフィギュレーションはスタートアップ コンフィギュレーション ファイルに保存されます。この構成をクリアするには、**clear configure** コマンドを使用します。

REST API パッケージをインストールまたは更新した後、ASA はリブートされません。

インストール済みの REST API エージェントを有効にするには、このコマンドを **agent** キーワードを指定して使用します。

例

次に、REST API パッケージを cisco.com からダウンロードしてインストールする例を示します。

```
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-9.3.2-32.pkg  disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
```

次に、実行中の REST API エージェントをディセーブルにして既存の REST API エージェントをアップグレードしてから、新しい REST API エージェントをダウンロードし、インストールして起動する例を示します。

```
ciscoasa(config)# no rest-api agent
ciscoasa(config)# copy tftp://10.7.0.80/asa-restapi-121-lfbff-k8.SPA disk0:
ciscoasa(config)# rest-api image disk0:/asa-restapi-121-lfbff-k8.SPA
ciscoasa(config)# rest-api agent
```

関連コマンド

コマンド	説明
copy	指定した REST API パッケージを TFTP サーバーから内部フラッシュ メモリにコピーします。
show rest-api agent	REST API エージェントが実行中かどうかを確認します。
clear configure	REST API のコンフィギュレーションを含む実行コンフィギュレーションをクリアします。

restore

ASA の構成、証明書、キー、およびイメージをバックアップファイルから復元するには、特権 EXEC モードで **restore** コマンドを使用します。

restore [**/noconfirm**] [**context** *ctx-name*] [**interface** *name*] [**cert-passphrase** *value*] [**location** *path*]

構文の説明

cert-passphrase *value*	VPN の証明書や事前共有キーを復元する際は、証明書を復号するために、**cert-passphrase** キーワードで秘密鍵を指定する必要があります。証明書の復号化に使用するパスフレーズを PKCS12 形式で入力します。
context *ctx-name*	システム実行スペースからマルチコンテキストモードに入り、指定したコンテキストを復元する場合は、**context** キーワードを入力します。バックアップされた各コンテキストファイルは、個別に復元する必要があります。つまり、**restore** コマンドをファイルごとに再入力する必要があります。
interface *name*	（任意）バックアップをコピーするインターフェイスの名前を指定します。インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティング テーブルを確認します。
location *path*	復元先 **location** として、ローカルディスクまたはリモートの URL を指定できます。location を指定しない場合は、次のデフォルト名が使用されます。 • シングルモード：disk0:*hostname*.backup.*timestamp*.tar.gz • マルチモード：disk0:*hostname*.context-*ctx-name*.backup.*timestamp*.tar.gz
/noconfirm	**location** パラメータと **cert-passphrase** パラメータの入力を要求しないように指定します。警告およびエラーメッセージをバイパスしてバックアップを続行できるようにします。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.3(2)	このコマンドが追加されました。
9.5(1)	**interface** *name* 引数が追加されました。

使用上のガイドライン

次のガイドラインを参照してください。

- 復元を開始するには、復元先に少なくとも 300 MB の使用可能なディスク領域が必要です。
- バックアップ中またはバックアップ後にコンフィギュレーションを変更した場合、その変更内容はバックアップに含められません。バックアップの実行後にコンフィギュレーションを変更してから復元を実行した場合、このコンフィギュレーションの変更は上書きされます。結果として、ASA は異なる挙動をすることもあります。
- 復元は一度に 1 つしか開始できません。
- コンフィギュレーションは、元のバックアップを実行したときと同じ ASA バージョンにのみ復元できます。復元ツールを使用して、ASA の異なるバージョン間でコンフィギュレーションを移行することはできません。コンフィギュレーションの移行が必要な場合、ASA は、新しい ASA OS をロードした時に常駐するスタートアップ コンフィギュレーションを自動的にアップグレードします。
- クラスタリングを使用している場合、スタートアップ コンフィギュレーション、実行コンフィギュレーション、およびアイデンティティ証明書のみを復元できます。ユニットごとに別々にバックアップを作成および復元する必要があります。
- フェールオーバーを使用する場合、バックアップの作成および復元は、アクティブ ユニットとスタンバイ ユニットに対して別々に行う必要があります。
- ASA にマスター パスフレーズを設定している場合は、この手順で作成したバックアップ コンフィギュレーションの復元時にそのマスター パスフレーズが必要となります。ASA のマスターパスフレーズが不明な場合は、CLI コンフィギュレーション ガイドを参照して、バックアップを続行する前に、マスターパスフレーズをリセットする方法を確認してください。
- PKCS12 データをインポート（**crypto ca trustpoint** コマンドを使用）する際にトラストポイントが RSA キーを使用している場合、インポートされたキーペアにはトラストポイントと同じ名前が割り当てられます。この制約のため、ASDM コンフィギュレーションを復元した後でトラストポイントおよびそのキー ペアに別の名前を指定した場合、スタートアップ コンフィギュレーションは元のコンフィギュレーションと同じになるのに、実行コンフィギュレーションには異なるキー ペア名が含まれることになります。つまり、キーペアとトラストポイントに別の名前を使用した場合は、元のコンフィギュレーションを復元できないということです。この問題を回避するため、トラストポイントとそのキーペアには必ず同じ名前を使用してください。

- インターフェイスを指定しなかった場合、ASA は管理専用ルーティング テーブルを確認し、一致するものが見つからなければ、データのルーティングテーブルを確認します。管理専用インターフェイスを経由するデフォルトルートがある場合は、すべての**restore**トラフィックがそのルートに一致するため、データルーティングテーブルが確認されることはありません。このシナリオでは、データインターフェイスから復元する必要がある場合にそのインターフェイスを指定します。
- CLIを使用してバックアップしてからASDMを使用して復元したり、その逆を行うことはできません。
- 各バックアップ ファイルに含まれる内容は次のとおりです。
- 実行コンフィギュレーション
- スタートアップ コンフィギュレーション
- すべてのセキュリティ イメージ

Cisco Secure Desktop およびホスト スキャンのイメージ

Cisco Secure Desktop およびホスト スキャンの設定

AnyConnect（SVC）クライアントのイメージおよびプロファイル

AnyConnect（SVC）のカスタマイズおよびトランスフォーム

- アイデンティティ証明書（アイデンティティ証明書に関連付けられた RSA キー ペアは含まれるが、スタンドアロン キーは除外される）
- VPN 事前共有キー
- SSL VPN コンフィギュレーション
- アプリケーション プロファイルのカスタム フレームワーク（APCF）
- ブックマーク
- カスタマイゼーション
- ダイナミック アクセス ポリシー（DAP）
- プラグイン
- 接続プロファイル用の事前入力スクリプト
- プロキシ自動設定
- 変換テーブル
- Web コンテンツ
- バージョン情報

例

次に、バックアップを復元する例を示します。

```
ciscoasa# restore location disk0:/5525-2051.backup.2014-07-09-223$
restore location [disk0:/5525-2051.backup.2014-07-09-223251.tar.gz]?
Copying Backup file to local disk... Done!
Extracting the backup file ... Done!
Warning: The ASA version of the device is not the same as the backup version, some
configurations might not work after restore!
 Do you want to continue? [confirm] y
Begin restore ...
IMPORTANT: This backup configuration uses master passphrase encryption. Master passphrase
 is required to restore running configuration, startup configuration and VPN pre-shared
 keys.
Backing up [VPN Pre-shared keys] … Done!
Backing up [SSL VPN Configurations: Application Profile Custom Framework] … Done!
Backing up [SSL VPN Configurations: Bookmarks]… Done!
Backing up [SSL VPN Configurations: Customization] … Done!
Backing up [SSL VPN Configurations: Dynamic Access Policy] … Done!
Backing up [SSL VPN Configurations: Plug-in] … Done!
Backing up [SSL VPN Configurations: Pre-fill scripts for Connection Profile] … Done!
Backing up [SSL VPN Configurations: Proxy auto-config] … Done!
Backing up [SSL VPN Configurations: Translation table] … Done!
Backing up [SSL VPN Configurations: Web Content] … Done!
Backing up [Anyconnect(SVC) client images and profiles] … Done!
Backing up [Anyconnect(SVC) customizations and transforms] … Done!
Backing up [Cisco Secure Desktop and Host Scan images] … Done!
Backing up [UC-IME tickets] … Done!
Restoring [Running Configuration]
Following messages are as a result of applying the backup running-configuration to this
 device, please note them for future reference.
ERROR: Interface description was set by failover and cannot be changed
ERROR: Unable to set this url, it has already been set
Remove the first instance before adding this one
INFO: No change to the stateful interface
Failed to update LU link information
.Range already exists.
WARNING: Advanced settings and commands should only be altered or used
under Cisco supervision.
ERROR: Failed to apply media termination address 198.0.1.228 to interface outside, the
IP is already used as media-termination address on interface outside.
ERROR: Failed to apply media termination address 198.0.0.223 to interface inside, the
IP is already used as media-termination address on interface inside.
WARNING: PAC settings will override http- and https-proxy configurations. Do not overwrite
 configuration file if you want to preserve the old http- and https-proxy configurations.
Cryptochecksum (changed): 98d23c2c ccb31dc3 e51acf88 19f04e28
 Done!
Restoring UC-IME ticket ... Done!
Enter the passphrase used while backup to encrypt identity certificates. The default is
 cisco. If the passphrase is not correct, certificates will not be restored.
No passphrase was provided for identity certificates. Using the default value: cisco.
If the passphrase is not correct, certificates will not be restored.
Restoring Certificates ...
Enter the PKCS12 data in base64 representation....
ERROR: A keypair named Main already exists.
INFO: Import PKCS12 operation completed successfully
. Done!
Cleaning up ... Done!
Restore finished!
```

関連コマンド

コマンド	説明
backup	ASA の構成、キー、証明書、およびイメージをバックアップファイルからバックアップします。

ret - rz

retries

ASA が応答を受信しないときに、DNS サーバーのリストに再試行する回数を指定するには、グローバル コンフィギュレーション モードで **dns retries** 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。

retries *number*
no retries [*number*]

構文の説明

number	再試行回数を 0 ～ 10 の範囲で指定します。デフォルトは 2 です。

コマンド デフォルト

デフォルトの再試行回数は 2 回です。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

name-server コマンドを使用して DNS サーバーを追加します。

このコマンドは **dns name-server** コマンドの代わりに使用します。

例

次に、再試行回数を 0 回に設定する例を示します。ASA は各サーバーを 1 回だけ試行します。

```
ciscoasa(config)# dns server-group dnsgroup1
ciscoasa(config-dns-server-group)# retries 0
```

関連コマンド

コマンド	説明
clear configure dns	DNS コマンドをすべて削除します。
dns server-group	DNS サーバー グループ モードを開始します。

コマンド	説明
show running-config dns server-group	既存の DNS サーバー グループ コンフィギュレーションのうちの 1 つまたはすべてを表示します。

retry-count

クラウド Web セキュリティ プロキシ サーバーが到達不能であると見なす、連続したポーリングの失敗回数を設定するには、scansafe 汎用オプション コンフィギュレーション モードで **retry-count** 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** 形式を使用します。

retry-count *value*
no retry-count [*value*]

構文の説明

value	再試行回数の値（2 ～ 100）を入力します。デフォルトは 5 分です。

コマンド デフォルト

デフォルト値は 5 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
scansafe 汎用オプション コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

Cisco Cloud Web Security サービスに登録すると、プライマリ Cloud Web Security プロキシ サーバーとバックアップ プロキシ サーバーが割り当てられます。

クライアントがプライマリ サーバーに到達できない場合、ASA は可用性を判定するためにタワーのポーリングを開始します。（クライアントのアクティビティが存在しない場合、ASA は 15 分ごとにポーリングします）。設定された回数だけ再試行してもプロキシ サーバーが使用できない場合（デフォルトは 5 回。この設定は設定可能）、サーバーは到達不能として宣言され、バックアップ プロキシ サーバーがアクティブになります。

クライアントまたは ASA が、再試行回数に到達する前に少なくとも 2 回連続してサーバーに到達できる場合、ポーリングは停止し、タワーはアクセス可能であると判定されます。

再試行回数は、アプリケーション健全性チェックにも適用されます（イネーブルの場合）。

バックアップ サーバーへのフェールオーバー後、ASA はプライマリ サーバーをポーリングし続けます。プライマリ サーバーが到達可能になると、ASA はプライマリ サーバーの使用に戻ります。

例

次に、再試行回数の値を 7 に設定する例を示します。

```
scansafe general-options
 server primary ip 10.24.0.62 port 8080
 server backup ip 10.10.0.7 port 8080
 health-check application
 retry-count 7
 license 366C1D3F5CE67D33D3E9ACEC265261E5
```

関連コマンド

コマンド	説明
class-map type inspect scansafe	ホワイトリストに記載されたユーザーとグループのインスペクション クラス マップを作成します。
default user group	ASA に入ってくるユーザーのアイデンティティを ASA が判別できない場合のデフォルトのユーザー名やグループを指定します。
health-check application	フェールオーバーのための、クラウド Web セキュリティのアプリケーション健全性チェックを有効にします。
http[**s**]（パラメータ）	インスペクション ポリシー マップのサービス タイプ（HTTP または HTTPS）を指定します。
inspect scansafe	このクラスのトラフィックに対するクラウド Web セキュリティ インスペクションをイネーブルにします。
license	要求の送信元の組織を示すため、ASA がクラウド Web セキュリティ プロキシ サーバーに送信する認証キーを設定します。
match user group	ユーザーまたはグループをホワイトリストと照合します。
policy-map type inspect scansafe	インスペクション ポリシー マップを作成すると、ルールのために必要なパラメータを設定し、任意でホワイトリストを識別できます。
retry-count	再試行回数値を入力します。この値は、可用性をチェックするために、 プロキシサーバーをポーリングする前に待機する時間です。
scansafe	マルチ コンテキスト モードでは、コンテキストごとにクラウド Web セキュリティを許可します。
scansafe general-options	汎用クラウド Web セキュリティ サーバー オプションを設定します。

コマンド	説明
server {**primary** | **backup**}	プライマリまたはバックアップのクラウド Web セキュリティ プロキシ サーバーの完全修飾ドメイン名または IP アドレスを設定します。
show conn scansafe	大文字の Z フラグに示されたようにすべてのクラウド Web セキュリティ接続を表示します。
show scansafe server	サーバーが現在のアクティブ サーバー、バックアップ サーバー、または到達不能のいずれであるか、サーバーのステータスを表示します。
show scansafe statistics	合計と現在の http 接続を表示します。
user-identity monitor	AD エージェントから指定したユーザーまたはグループ情報をダウンロードします。
whitelist	トラフィックのクラスでホワイトリスト アクションを実行します。

retry-interval

aaa-server host コマンドで事前に指定された特定の AAA サーバーに対する再試行の時間間隔を設定するには、AAA サーバー ホスト モードで **retry-interval** コマンドを使用します。再試行間隔をデフォルト値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。

retry-interval *seconds*
no retry-interval

構文の説明

seconds 要求の再試行間隔（1 ～ 10 秒）を指定します。これは、接続要求を再試行するまでに ASA が待機する時間です。

コマンド デフォルト

デフォルトの再試行間隔は 10 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
AAA サーバーホスト	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドはCLIガイドラインに沿うように変更されました。

使用上のガイドライン

接続試行間に ASA が待機する秒数を指定またはリセットするには、**retry-interval** コマンドを使用します。ASA が AAA サーバーへの接続を試行する時間の長さを指定するには、**timeout** コマンドを使用します。

このコマンドは、RSA SecurID REST API サーバーグループ内のサーバーには適用されません。

（注） RADIUS プロトコルの場合、サーバーが ICMP ポート到達不能メッセージで応答すると、再試行間隔の設定が無視され、AAA サーバーはただちに障害状態になります。このサーバーが AAA グループ内の唯一のサーバーである場合は、サーバーが再アクティブ化され、別の要求がサーバーに送信されます。これは意図された動作です。

例

次に、コンテキストでの **retry-interval** コマンドの例を示します。

```
ciscoasa
(config)# aaa-server svrgrp1 protocol radius
ciscoasa
(config-aaa-server-group)# aaa-server svrgrp1 host 1.2.3.4
ciscoasa
(config-aaa-server-host)# timeout 7
ciscoasa
(config-aaa-server-host)# retry-interval 9
```

関連コマンド

コマンド	説明
aaa-server host	AAA サーバー ホスト コンフィギュレーション モードを開始して、ホスト固有の AAA サーバー パラメータを設定できるようにします。
clear configure aaa-server	すべての AAA コマンド ステートメントをコンフィギュレーションから削除します。
show running-config aaa-server	すべての AAA サーバー、特定のサーバー グループ、特定のグループ内の特定のサーバー、または特定のプロトコルの AAA サーバー統計情報を表示します。
timeout	ASA が AAA サーバーへの接続を試行する時間の長さを指定します。

reval-period

NAC フレームワークセッションにおける成功した各ポスチャ検証間の間隔を指定するには、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 **reval-period** コマンドを使用します。このコマンドを NAC フレームワークポリシーから削除するには、このコマンドの **no** 形式を使用します。

reval-period *seconds*
no reval-period [*seconds*]

構文の説明

seconds 正常に完了した各ポスチャ確認の間隔の秒数。指定できる範囲は300～86400です。

コマンド デフォルト

デフォルト値は 36000 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
7.3(0)	コマンド名から「nac-」が削除されました。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。

使用上のガイドライン

ASA では、ポスチャ検証に成功するたびに、再検証タイマーが開始されます。このタイマーが期限切れになると、次の無条件のポスチャ検証がトリガーされます。ASA では、再検証中はポスチャ検証が維持されます。ポスチャ検証または再検証中にアクセス コントロール サーバーが使用できない場合、デフォルトのグループ ポリシーが有効になります。

例

次に、再検証タイマーを 86400 秒に変更する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# reval-period 86400
ciscoasa(config-nac-policy-nac-framework)
```

次に、NAC ポリシーから再検証タイマーを削除する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# no reval-period
ciscoasa(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
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。
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。
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 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。

revert webvpn all

ASA のフラッシュメモリから、すべての Web 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除するには、特権 EXEC モードで **revert webvpn all** コマンドを入力します。

revert webvpn all

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA のフラッシュメモリから Web 関連のすべての情報（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を無効にし、削除するには、**revert webvpn all** コマンドを使用します。すべての Web 関連データを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、ASA からすべての Web 関連コンフィギュレーション データを削除するコマンドを示します。

```
ciscoasa# revert webvpn all
ciscoasa
```

関連コマンド

コマンド	説明
show import webvpn (option)	現在、ASA のフラッシュメモリに存在する、インポートされたさまざまな WebVPN データおよびプラグインを表示します。

revert webvpn AnyConnect-customization

Cisco Secure Client GUI のカスタマイズに使用されているファイルを ASA から削除するには、特権 EXEC モードで **revert webvpn AnyConnect-customization** コマンドを使用します。

revert webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

構文の説明

type	カスタマイズ ファイルのタイプ。 • バイナリ：AnyConnect GUI を置き換える実行可能ファイル。 • resource：企業ロゴなどのリソース ファイル。 • トランスフォーム：MSI をカスタマイズするトランスフォーム。
platform	セキュアクライアント を実行しているエンドポイントデバイスの OS。linux、mac-intel、mac-powerpc、win、または win-mobile のいずれかを指定します。
name	削除するファイルを識別する名前（最大 64 文字）。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	このコマンドが追加されました。

使用上のガイドライン

セキュアクライアント GUI のカスタマイズ手順の詳細については、AnyConnect VPN クライアント管理者ガイド [英語] を参照してください。

例

次に、AnyConnect GUI をカスタマイズするために以前にリソース ファイルとしてインポートした Cisco ロゴを削除する例を示します。

```
ciscoasa# revert webvpn AnyConnect-customization type resource platform win name
cisco_logo.gif
```

関連コマンド

コマンド	説明
customization	トンネル グループ、グループ、またはユーザーに対して使用するカスタマイゼーション オブジェクトを指定します。
export customization	カスタマイゼーション オブジェクトをエクスポートします。
import customization	カスタマイゼーション オブジェクトをインストールします。
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn customization	ASA のフラッシュデバイスに存在する現在のカスタマイゼーション オブジェクトを表示します。

revert webvpn customization

ASA の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するには、特権 EXEC モードで **revert webvpn customization** コマンドを入力します。

revert webvpn customization *name*

構文の説明

name	削除するカスタマイゼーション オブジェクトの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

指定したカスタマイゼーションのクライアントレス SSL VPN サポートを削除し、ASA のキャッシュメモリからそのカスタマイゼーションを削除するには、**revert webvpn customization** コマンドを使用します。カスタマイゼーション オブジェクトを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。カスタマイゼーション オブジェクトには、特定の指定されたポータル ページのコンフィギュレーション パラメータが含まれています。

バージョン 8.0 ソフトウェアでは、カスタマイゼーションの設定機能が拡張されており、新しいプロセスは以前のバージョンと互換性がありません。セキュリティ アプライアンスでは、8.0 ソフトウェアへのアップグレード時に、古い設定を使用して新しいカスタマイゼーション オブジェクトを生成することによって、現在の設定が保持されます。このプロセスは 1 回のみ実行されます。また、古い値は新しい値の一部を構成するサブセットに過ぎないため、このプロセスは古い形式から新しい形式への単なる変換ではありません。

（注） バージョン 7.2 のポータル カスタマイゼーションおよび URL リストは、バージョン 8.0 へのアップグレード前にバージョン 7.2(x) のコンフィギュレーション ファイルで適切なインターフェイスにおいてクライアントレス SSL VPN（WebVPN）がイネーブルになっている場合にのみ、ベータ 8.0 コンフィギュレーションで動作します。

例

次に、GroupB という名前のカスタマイゼーション オブジェクトを削除するコマンドを示します。

```
ciscoasa# revert webvpn customization groupb
ciscoasa
```

関連コマンド

コマンド	説明
customization	トンネル グループ、グループ、またはユーザーに対して使用するカスタマイゼーション オブジェクトを指定します。
export customization	カスタマイゼーション オブジェクトをエクスポートします。
import customization	カスタマイゼーション オブジェクトをインストールします。
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn customization	ASA のフラッシュデバイスに存在する現在のカスタマイゼーション オブジェクトを表示します。

revert webvpn plug-in protocol

ASA のフラッシュデバイスからプラグインを削除するには、特権 EXEC モードで **revert webvpn plug-in protocol** コマンドを入力します。

revert plug-in protocol *protocol*

構文の説明

protocol 次のいずれかのストリングを入力します。

- rdp

Remote Desktop Protocol プラグインにより、リモート ユーザーは Microsoft Terminal Services が実行するコンピュータに接続できます。

- **ssh**

セキュア シェル プラグインにより、リモートユーザーがリモート コンピュータへのセキュア チャネルを確立したり、リモート ユーザーが Telnet を使用してリモート コンピュータに接続したりできます。

- **vnc**

Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

指定した Java ベースのクライアント アプリケーションのクライアントレス SSL VPN サポートを無効にして削除し、ASA のフラッシュドライブからも削除するには、**revert webvpn plug-in protocol** コマンドを使用します。

例

次に、RDP のサポートを削除するコマンドを示します。

```
ciscoasa# revert webvpn plug-in protocol rdp
ciscoasa
```

関連コマンド

コマンド	説明
import webvpn plug-in protocol	指定したプラグインを URL から ASA のフラッシュデバイスにコピーします。このコマンドを発行すると、クライアントレス SSL VPN での今後のセッションにおいて、Java ベースのクライアント アプリケーションの使用が自動的にサポートされます。
show import webvpn plug-in	ASA のフラッシュデバイスに存在するプラグインのリストを示します。

revert webvpn translation-table

ASA のフラッシュメモリから変換テーブルを削除するには、特権 EXEC モードで **revert webvpn translation-table** コマンドを入力します。

revert webvpn translation-table *translationdomain* **language** *language*

構文の説明

translationdomain 使用可能な変換ドメインは、次のとおりです。

- **AnyConnect**
- **PortForwarder**
- **banners**
- **csd**
- **customization**
- **url-list**
- **webvpn**
- 使用可能な場合、Citrix、RPC、Telnet-SSH、および VNC のプラグインからのメッセージの変換。

language *language* 削除する言語を指定します。2 文字のコードを使用して言語を指定します。? と入力して、インストールされている言語を確認します。各ドメインにインストールされている言語を表示するには、**show import webvpn translation-table** コマンドを使用します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

インポートされた変換テーブルを無効にして削除し、フラッシュメモリから削除するには、**revert webvpn translation-table** コマンドを使用します。変換テーブルを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、フランス語の AnyConnect 変換テーブルを削除するコマンドを示します。

```
ciscoasa# revert webvpn translation-table anyconnect language fr

ciscoasa#
```

関連コマンド

コマンド	説明
revert webvpn all	WebVPN 関連のすべてのデータ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show import webvpn translation-table	フラッシュ デバイスに存在する現在の変換テーブルを表示します。

revert webvpn url-list

ASA から URL リストを削除するには、特権 EXEC モードで **revert webvpn url-list** コマンドを入力します。

revert webvpn url-list template *name*

構文の説明

template *name*	URL リストの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA のフラッシュドライブにある現在の URL リストを無効にし、削除するには、**revert webvpn url-list** コマンドを使用します。URL リストを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

revert webvpn url-list コマンドで使用される template 引数では、設定済みの URL リストの名前を指定します。このようなリストを設定するには、グローバル コンフィギュレーション モードで **url-list** コマンドを使用します。

例

次に、servers2 という URL リストを削除するコマンドを示します。

```
ciscoasa# revert webvpn url-list servers2
ciscoasa
```

関連コマンド

コマンド	説明
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show running-configuration url-list	現在の設定済みURLリストコマンドのセットを表示します。
url-list (WebVPN mode)	特定のユーザーまたはグループ ポリシーに、WebVPN サーバーおよびURL のリストを適用します。

revert webvpn webcontent

ASA のフラッシュメモリ内の場所から指定した Web オブジェクトを削除するには、特権 EXEC モードで **revert webvpn webcontent** コマンドを入力します。

revert webvpn webcontent *filename*

構文の説明

filename 削除する Web コンテンツを含むフラッシュ メモリ ファイルの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Web コンテンツを含むファイルを無効にして削除し、ASA のフラッシュメモリから削除するには、**revert webvpn content** コマンドを使用します。Web コンテンツを削除すると、デフォルト設定が使用可能な場合にはデフォルト設定に戻ります。

例

次に、ASA のフラッシュメモリから ABCLogo という Web コンテンツファイルを削除するコマンドを示します。

```
ciscoasa# revert webvpn webcontent abclogo
ciscoasa
```

関連コマンド

コマンド	説明
revert webvpn all	すべての webvpn 関連データ（カスタマイゼーション、プラグイン、変換テーブル、URL リスト、および Web コンテンツ）を削除します。
show webvpn webcontent	ASA のフラッシュメモリに現存する Web コンテンツを表示します。

revocation-check

トラストプールポリシーについて失効チェックが必要であるかどうかを定義するには、クリプト CA トラストプール コンフィギュレーション モードで **revocation-check** コマンドを使用します。デフォルトの失効チェック方法（*none*）に戻すには、このコマンドの **no** 形式を使用します。

revocation-check { [**crl**] [**ocsp**] [**none**] }
no revocation-check { [**crl**] [**ocsp**] [**none**] }

構文の説明

crl	ASA では、失効チェック方法として CRL を使用する必要があることを指定します。
none	ASA では、すべての方法でエラーが返された場合でも証明書ステータスを有効であると解釈する必要があることを指定します。
ocsp	ASA では、失効チェック方法として OCSP を使用する必要があることを指定します。

コマンド デフォルト

デフォルト値は *none* 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クリプト CA トラストプール コンフィギュレーション モード	• 対応	• 対応	• 対応	—	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.5(1)	OCSP URL を使用した失効チェックのインターフェイスキーワードが追加されました。
9.13(1)	CRL または OCSP サーバーとの接続問題に起因する失効チェックをバイパスするオプションが削除されました。
9.15(1)	9.13(1) で削除された、失効チェックをバイパスするオプションが復元されました。

使用上のガイドライン

OCSP 応答の署名者は、通常、OCSP サーバー（レスポンダ）証明書です。デバイスは、応答を受信した後、レスポンダ証明書の検証を試みます。

通常、CA は、セキュリティが侵害される危険性を最小限に抑えるために、OCSP レスポンダ証明書のライフタイムを比較的短い期間に設定します。CA は、失効ステータス チェックが必要ないことを示す ocsp-no-check 拡張をレスポンダ証明書に組み込みます。ただし、この拡張が存在しない場合、デバイスは、この **revocation-check** コマンドでトラストポイントに設定した失効方法を使用して、証明書失効ステータスのチェックを試みます。*none* オプションを設定してステータス チェックを無視していない限り、OCSP 失効チェックの失敗後、OCSP レスポンダ証明書に ocsp-no-check 拡張がない場合、OCSP レスポンダ証明書は検証可能である必要があります。

（注） オプションの引数を指定する場合、順序は問いませんが、*none* キーワードは必ず最後にする必要があります。

ASA では、すべての方法が設定した順序で試行されます。2 番目と 3 番目の方法は、前の方法でエラー（サーバーのダウンなど）が返された場合にのみ、ステータスを失効と見なさずに試行されます。

クライアント証明書検証トラストポイントで、失効チェック方法を設定できます。また、レスポンダ証明書検証トラストポイントでは、失効チェックなし（**revocation-check none)**）を設定できます。構成例については、**match certificate** コマンドを参照してください。

ASA で **revocation-check crl none** コマンドを設定している場合、クライアントが ASA に接続すると、CRL がまだキャッシュされていないためダウンロードが自動的に開始され、証明書が検証されてから CRL のダウンロードが終了します。この場合、CRL がキャッシュされていないと、CRL のダウンロード前に ASA で証明書が検証されます。

ASA 9.13(1) で削除された、失効チェックをバイパスするための次のオプションは、後に復元されました。

オプション	Action
revocation-check crl none	CRL にアクセスできない場合は、失効チェックをバイパスします
revocation-check ocsp none	OCSP チェックを実行できない場合は、失効チェックをバイパスします
revocation-check crl ocsp none	CRL にアクセスできない場合は、OCSP を試してください。OCSP を実行できない場合は、失効チェックをバイパスします
revocation-check ocsp crl none	OCSP を実行できない場合は、CRL を試し、それ以外の場合は失効チェックをバイパスします

失効チェックに OCSP URL を割り当てる場合、OCSP が到達可能な管理インターフェイスを指定できます。このインターフェイス値によってルーティングの判断が決まります。

例

```
ciscoasa(config-ca-trustpoint)# revocation-chec
k ?
crypto-ca-trustpoint mode commands/options:
  crl   Revocation check by CRL
  none  Ignore revocation check
  ocsp  Revocation check by OCSP
(config-ca-trustpoint)# ocsp
ocsp interface mgmt url http://1.1.1.1:8888
```

ここで、mgmt は管理インターフェイスの名前です。

関連コマンド

コマンド	説明
crypto ca trustpool policy	トラストプールポリシーを定義するコマンドを提供するサブモードを開始します。
match certificate allow expired-certificate	特定の証明書に対する有効期限チェックを管理者が免除できるようにします。
match certificate skip revocation-check	特定の証明書に対する失効チェックを管理者が免除できるようにします。

rewrite（廃止）

WebVPN接続上で、特定のアプリケーションまたはトラフィックタイプのコンテンツのリライトを無効にするには、webvpn モードで **rewrite** コマンドを使用します。リライトルールを削除するには、ルールを一意に識別するルール番号を指定して、このコマンドの **no** 形式を使用します。すべてのリライトルールを削除するには、このコマンドの **no** 形式をルール番号を指定せずに使用します。

ASA のデフォルトでは、すべての WebVPN トラフィックがリライトまたは変換されます。

rewrite order *integer* { **enable | disable** } **resource-mask** *string* [**name** *resource name*]
no rewrite order *integer* { **enable | disable** } **resource-mask** *string* [**name** *resource name*]

構文の説明

disable	このリライト ルールを、指定したトラフィックに対するコンテンツのリライトをディセーブルにするルールとして定義します。コンテンツのリライトをディセーブルにすると、トラフィックはセキュリティ アプライアンスを通過しません。
イネーブル化	このリライト ルールを、指定したトラフィックに対するコンテンツのリライトをイネーブルにするルールとして定義します。
integer	設定されているすべてのルール内でのルールの順序を設定します。指定できる範囲は 1 ～ 65534 です。
name	（任意）ルールを適用するアプリケーションまたはリソースの名前を指定します。
order	ASA のルール適用順序を定義します。
resource-mask	ルールのアプリケーションまたはリソースを指定します。
resource name	（任意）ルールを適用するアプリケーションまたはリソースを指定します。最大 128 バイトです。
string	照合するアプリケーションまたはリソースの名前を指定します。正規表現を使用できます。次のワイルドカードを使用できます。 照合対象として正規表現を含むことができるパターンを指定します。次のワイルドカードを使用できます。 *：完全一致。このワイルドカードはこれだけでは使用できません。英数字の文字列とともに使用する必要があります。 ？：少なくとも 1 文字を一致させます。 [!seq]：順序に関係なく、任意の文字を含みます。 [seq]：順序も含め、任意の文字を含みます。 最大 300 バイトです。

コマンド デフォルト

デフォルトでは、すべてをリライトします。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
webvpn コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.17(1)	Web VPN のサポートが終了したため、このコマンドは廃止されました。

使用上のガイドライン

ASA では、WebVPN 接続経由で正しくレンダリングされるように、アプリケーションのコンテンツがリライトされます。外部パブリック Web サイトなどの一部のアプリケーションでは、この処理は必要ありません。これらのアプリケーションでは、コンテンツ リライトをオフにできます。

disable オプションを指定して rewrite コマンドを使用して、コンテンツリライトを選択的にオフにし、ユーザーが ASA を経由せずに直接特定のサイトを参照できるようにします。これは、IPsec VPN 接続におけるスプリット トンネリングに似ています。

このコマンドは複数回使用できます。ASA では、順序番号に従ってリライトルールが検索され、一致する最初のルールが適用されるため、エントリの設定順序は重要です。

例

次に、cisco.com ドメインの URL に対するコンテンツ リライトをオフにする順序番号 1 のリライト ルールを設定する例を示します。

```
ciscoasa
(config-webpn)#
 rewrite order 2 disable resource-mask *cisco.com/*
```

関連コマンド

コマンド	説明
apcf	特定のアプリケーションに使用する非標準のルールを指定します。
proxy-bypass	特定のアプリケーションに対してコンテンツの最低限の書き換えを設定します。

re-xauth

IPSec ユーザーに対して IKE キー再生成時に再認証を要求するには、グループ ポリシー コンフィギュレーション モードで **re-xauth enable** コマンドを発行します。IKE キー再生成時にユーザーの再認証を無効にするには、**re-xauth disable** コマンドを使用します。

実行コンフィギュレーションから re-xauth 属性を削除するには、このコマンドの **no** 形式を使用します。これにより、他のグループ ポリシーから IKE キー再生成時の再認証についての値が継承されます。

re-xauth { **enable** [**extended**] | **disable** }
no re-xauth

構文の説明

disable	IKE キー再生成時の再認証をディセーブルにします。
enable	IKE キー再生成時の再認証をイネーブルにします。
extended	認証クレデンシャルを再入力可能な時間を、設定されている SA の最大ライフタイムまで延長します。

コマンド デフォルト

IKE キー再生成時の再認証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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
グループ ポリシー コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0.4	**extended** キーワードが追加されました。

使用上のガイドライン

IKE キー再生成時の再認証は、IPsec 接続に対してのみ適用されます。

IKE キー再生成時の再認証を有効にすると、ASA では、最初のフェーズ 1 IKE ネゴシエーション時にユーザーはユーザー名とパスワードの入力を求められ、その後 IKE キー再生成が実行されるたびにユーザー認証を求められます。再認証によって、セキュリティが強化されます。

ユーザーは、30 秒以内にクレデンシャルを入力する必要があります。また、約 2 分間で SA が期限切れになり、トンネルが終了するまでの間に、3 回まで入力を再試行できます。ユーザーに対して、設定されている SA の最大ライフタイムまで認証ログイン情報の再入力を許可するには、**extended** キーワードを使用します。

設定されているキー再生成間隔を確認するには、モニタリングモードで **show crypto ipsec sa** コマンドを入力して、セキュリティアソシエーションの秒単位のライフタイム、およびデータのキロバイト単位のライフタイムを表示します。

（注） 接続の他方の終端にユーザーが存在しない場合、再認証は失敗します。

例

次に、FirstGroup という名前のグループ ポリシーに対して、キー再生成時の再認証をイネーブルにする例を示します。

```
ciscoasa(config) #group-policy FirstGroup attributes
ciscoasa(config-group-policy)# re-xauth enable
```

rip authentication mode

RIP バージョン 2 パケットで使用される認証のタイプを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication mode** コマンドを使用します。デフォルトの認証方法に戻すには、このコマンドの **no** 形式を使用します。

rip authentication mode { **text | md5** }
no rip authentication mode

構文の説明

md5	RIP メッセージ認証に MD5 を使用します。
text	RIP メッセージ認証にクリア テキストを使用します（非推奨）。

コマンド デフォルト

デフォルトで、クリア テキスト認証が使用されます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

インターフェイス上の **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet0/3 上で設定された RIP 認証の例を示します。

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key thisismykey key_id 5
```

関連コマンド

コマンド	説明
rip authentication key	RIP バージョン 2 認証をイネーブルにして、認証キーを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	ASA でグローバルに使用される RIP のバージョンを指定します。

rip authentication key

RIP バージョン 2 パケットの認証を有効にし、認証キーを指定するには、インターフェイス コンフィギュレーション モードで **rip authentication key** コマンドを使用します。RIP バージョン 2 認証を無効にするには、このコマンドの **no** 形式を使用します。

rip authentication key [**0|8**] *string* **key_id** *id*
no rip authentication key

構文の説明

0	暗号化されていないパスワードが続くことを指定します。
8	暗号化されたパスワードが後に続くことを指定します。
id	キー ID 値を指定します。有効な値の範囲は 1 ～ 255 です。
key	認証キー ストリングに使用される共有キーを指定します。このキーには、最大 16 文字を含めることができます。
string	暗号化されていない（クリアテキスト）ユーザー パスワードを指定します。

コマンド デフォルト

RIP 認証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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。ネイバー認証をイネーブルにする場合は、*key* 引数および *key_id* 引数が、RIP バージョン 2 更新を提供するネイバー デバイスによって使用されているものと同じである必要があります。key は、最大 16 文字のテキスト ストリングです。

インターフェイス上の **rip authentication** コマンドを表示するには、**show interface** コマンドを使用します。

例

次に、インターフェイス GigabitEthernet 0/3 上で設定された RIP 認証の例を示します。

```
ciscoasa(config)# interface Gigabit0/3
ciscoasa(config-if)# rip authentication mode md5
ciscoasa(config-if)# rip authentication key 8 yWIvi0qJAnGK5MRWQzrhIohkGP1wKb 5
```

関連コマンド

コマンド	説明
rip authentication mode	RIP バージョン 2 パケットで使用される認証のタイプを指定します。
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
show running-config interface	指定したインターフェイスのコンフィギュレーション コマンドを表示します。
version	ASA でグローバルに使用される RIP のバージョンを指定します。

rip receive version

インターフェイスで受け入れる RIP のバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip receive version** 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** 形式を使用します。

version { [**1**] [**2**] }
no version

構文の説明

1	RIP バージョン 1 を指定します。
2	RIP バージョン 2 を指定します。

コマンド デフォルト

ASA は RIP バージョン 1 とバージョン 2 のパケットを受け入れます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

グローバル設定をインターフェイスごとに上書きするには、インターフェイスで **rip receive version** コマンドを入力します。

RIP バージョン 2 を指定した場合は、ネイバー認証をイネーブルにし、MD5 ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを受信するように、ASA を設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip send version	特定のインターフェイスからアップデートを送信するときに使用する RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにして、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	ASA でグローバルに使用される RIP のバージョンを指定します。

rip send version

インターフェイスでRIPアップデートを送信するために使用されるRIPのバージョンを指定するには、インターフェイス コンフィギュレーション モードで **rip send version** 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** 形式を使用します。

rip send version { [**1**] [**2**] }
no rip send version

構文の説明

1	RIPバージョン1を指定します。
2	RIPバージョン2を指定します。

コマンド デフォルト

ASA は RIP バージョン 1 パケットを送信します。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

グローバルRIP送信バージョン設定をインターフェイスごとに上書きするには、インターフェイスで **rip send version** コマンドを入力します。

RIPバージョン2を指定した場合は、ネイバー認証をイネーブルにし、MD5ベースの暗号化を使用して、RIP アップデートを認証できます。

例

次に、指定したインターフェイス上で RIP バージョン 1 と 2 のパケットを送受信するように、ASA を設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/3
ciscoasa(config-if)# rip send version 1 2
ciscoasa(config-if)# rip receive version 1 2
```

関連コマンド

コマンド	説明
rip receive version	特定のインターフェイス上でアップデートを受信するときに受け入れる RIP バージョンを指定します。
router rip	RIP ルーティング プロセスをイネーブルにし、そのプロセスのルータ コンフィギュレーション モードを開始します。
version	ASA でグローバルに使用される RIP のバージョンを指定します。

rmdir

既存のディレクトリを削除するには、特権 EXEC モードで **rmdir** コマンドを使用します。

rmdir ［ / **no confirm** ］［ **disk0:| disk1:| flash:** ］ *path*

構文の説明

/noconfirm	（任意）確認プロンプトを表示しないようにします。
disk0：	（任意）非着脱式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）脱着式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：	（任意）非着脱式内部フラッシュを指定し、続けてコロンを入力します。ASA 5500 シリーズの適応型セキュリティアプライアンスでは、**flash** キーワードは **disk0** のエイリアスです。
path	（任意）削除するディレクトリの絶対または相対パス。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ディレクトリが空でない場合、**rmdir** コマンドは失敗します。

例

次に、「test」という名前の既存のディレクトリを削除する例を示します。

```
ciscoasa# rmdir test
```

関連コマンド

コマンド	説明
dir	ディレクトリの内容を表示します。
mkdir	新しいディレクトリを作成します。
pwd	現在の作業ディレクトリを表示します。
show file	ファイルシステムに関する情報を表示します。

route

指定したインターフェイスにスタティックルートまたはデフォルトルートを入力するには、グローバル コンフィギュレーション モードで **route** コマンドを使用します。指定されたインターフェイスからルートを削除するには、このコマンドの **no** 形式を使用します。

route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] | **tunneled**]
no route *interface_name ip_address netmask gateway_ip* [[*metric*] [**track** *number*] **tunneled**]

構文の説明

gateway_ip	ゲートウェイ ルータの IP アドレス（このルートのネクストホップ アドレス）を指定します。 （注） トランスペアレント モードでは、*gateway_ip* 引数は省略可能です。
interface_name	トラフィックがルーティングされるインターフェイスの名前を指定します。トランスペアレント モードの場合は、ブリッジ グループのメンバー インターフェイスの名前を指定します。ブリッジ グループでルーテッド モードを使用する場合は、BVI 名を指定します。ルーテッドモードで、不要なトラフィックを「ブラック ホール化」するには、**null0** インターフェイスを入力します。
ip_address	内部または外部ネットワーク IP アドレスを指定します。
metric	（オプション）このルートのアドミニストレーティブ ディスタンスを指定します。有効値の範囲は、1 ～ 255 です。デフォルト値は 1 です。
netmask	*ip_address* に適用するネットワーク マスクを指定します。
track*number*	（任意）このルートにトラッキング エントリを関連付けます。有効な値は、1 ～ 500 です。 （注） **track** オプションは、シングル、ルーテッドモードでのみ使用できます。
tunneled	ルートを VPN トラフィックのデフォルト トンネル ゲートウェイとして指定します。

コマンド デフォルト

metric のデフォルトは 1 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(1)	**track** *number* の値が追加されました。
9.2(1)	**null0** インターフェイスオプションが追加されました。
9.7(1)	統合ルーティングおよびブリッジングを使用している場合のルーテッド モードの BVI インターフェイスのサポートが追加されました。

使用上のガイドライン

インターフェイスに対してデフォルトルートまたはスタティックルートを入力するには、**route** コマンドを使用します。デフォルトルートを入力するには、*ip_address* および *netmask* を **0.0.0.0,** に設定するか、短縮形の **0** を使用します。**route** コマンドを使用して入力されたすべてのルートは、構成の保存時に保存されます。

トンネル トラフィックには、標準のデフォルト ルートの他に別のデフォルト ルートを 1 つ定義することができます。**tunneled** オプションを使用してデフォルトルートを作成すると、ASA に着信するトンネルからのトラフィックはすべて、学習したルートまたはスタティックルートを使用してルーティングできない場合、このルートに送信されます。トンネルから出るトラフィックの場合、このルートは、その他の設定または学習されたデフォルト ルートをすべて上書きします。

tunneled オプションが指定されたデフォルトルートには、次の制限事項が適用されます。

- トンネルルートの出力インターフェイスで、ユニキャスト RPF（**ip verify reverse-path**）を有効にしないでください。トンネル ルートの出力インターフェイスで uRPF をイネーブルにすると、セッションに障害が発生します。
- セッションでエラーが発生する原因となるため、トンネル ルートの出力インターフェイスで TCP 代行受信をイネーブルにしないでください。
- VoIP インスペクション エンジン（CTIQBE、H.323、GTP、MGCP、RTSP、SIP、SKINNY）、DNS インスペクション エンジン、または DCE RPC インスペクション エンジンは、vlan-mapping オプションまたはトンネル ルートでは使用しないでください。vlan-mapping 設定によってパケットが間違ってルーティングされる可能性があるため、これらのインスペクション エンジンは、vlan-mapping 設定を無視します。

tunneled オプションを使用して複数のデフォルトルートは定義できません。トンネルトラフィックの ECMP はサポートされていません。

スタティック ルートは、任意のインターフェイスで、ルータの外部に接続されているネットワークにアクセスする場合に作成します。たとえば、次のスタティック route コマンドでは、192.168.42.0 ネットワークに向かうすべてのパケットが、ASA によって 192.168.1.5 ルータ経由で送信されます。

```
ciscoasa(config)# route dmz 192.168.42.0 255.255.255.0 192.168.1.5 1
```

各インターフェイスの IP アドレスを入力すると、ASA によって、ルートテーブルに CONNECT ルートが作成されます。**clear route** や **clear configure route** コマンドを使用しても、このエントリは削除されません。

ACL の場合とは異なり、スタティック **null0** ルートではパフォーマンスが低下することはありません。**null0** 設定は、ルーティングループの防止に使用されます。BGP では、リモートトリガ型ブラックホールルーティングのために **null0** 設定を利用します。

例

次に、外部インターフェイスに対して、1 つのデフォルト route コマンドを指定する例を示します。

```
ciscoasa(config)# route outside 0 0 209.165.201.1 1
```

次に、ネットワークへのアクセスを提供するスタティック route コマンドを追加する例を示します。

```
ciscoasa(config)# route dmz1 10.1.2.0 255.0.0.0 10.1.1.4 1
ciscoasa(config)# route dmz1 10.1.3.0 255.0.0.0 10.1.1.4 1
```

次に、SLA 動作を使用して、外部インターフェイスに対して、10.1.1.1 ゲートウェイへのデフォルトルートをインストールする例を示します。SLA 動作によって、このゲートウェイの可用性がモニターされます。この SLA 動作が失敗した場合は、DMZ インターフェイスのバックアップ ルートが使用されます。

```
ciscoasa(config)# sla monitor 123
ciscoasa(config-sla-monitor)# type echo protocol ipIcmpEcho 10.1.1.1 interface outside

ciscoasa(config-sla-monitor-echo)# timeout 1000
ciscoasa(config-sla-monitor-echo)# frequency 3
ciscoasa(config)# sla monitor schedule 123 life forever start-time now
ciscoasa(config)# track 1 rtr 123 reachability
ciscoasa(config)# route outside 0.0.0.0 0.0.0.0 10.1.1.1 track 1
ciscoasa(config)# route dmz 0.0.0.0 0.0.0.0 10.2.1.1 254
```

次に、スタティック null0 ルートを設定する例を示します。

```
ciscoasa(config)# route null0 192.168.2.0 255.255.255.0
```

関連コマンド

コマンド	説明
clear configure route	スタティックに設定された **route** コマンドを削除します。

コマンド	説明
clear route	RIP などのダイナミック ルーティング プロトコルを通じて学習されたルートを削除します。
show route	ルート情報を表示します。
show running-config route	設定されているルートを表示します。

route-map

ルーティング プロトコル間でルートを再配布する条件を定義したり、ポリシー ルーティングをイネーブルにしたりするには、グローバル コンフィギュレーション モードで route-map コマンドを使用し、さらにルート マップ コンフィギュレーション モードで match コマンドと set コマンドを使用します。エントリを削除するには、このコマンドの no 形式を使用します。

route-map *name* [**permit | deny**] [*sequence number*]
no route-map *name* [**permit | deny**] [*sequence number*]

構文の説明

name	ルート マップに意味のある名前を指定します。redistribute ルータ コンフィギュレーション コマンドはこの名前を使用して、このルート マップを参照します。複数のルート マップで同じ名を共有できます。
permit	（オプション）このルート マップの一致基準が満たされた場合、permit キーワードが指定されていると、設定アクションに従ってルートが再配布されます。ポリシー ルーティングの場合、パケットはポリシーに従ってルーティングされます。 一致基準が満たされなかった場合、permit キーワードが指定されていると、同じマップ タグを持つ次のルート マップがテストされます。あるルートが、同じ名前を共有するルート マップ セットの一致基準のいずれをも満たさない場合、そのセットによる再配布は行われません。 permit キーワードがデフォルトです。
deny	（オプション）ルート マップの一致基準が満たされた場合でも、deny キーワードが指定されているとルートは再配布されません。ポリシー ルーティングの場合、パケットはポリシーに従ってルーティングされません。また、同じマップ タグ名を共有するルート マップは、これ以上検証されません。パケットがポリシー ルーティングの対象にならない場合、通常の転送アルゴリズムが使用されます。
sequence-number	（任意）すでに同じ名前で設定されているルート マップ リスト内の新しいルート マップの位置を指定する番号。このコマンドの no 形式を指定すると、このルート マップの位置が削除されます。

コマンド デフォルト

デフォルト設定はありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

ルートを再配布するには、ルート マップを使用します。

あるルーティング プロトコルから別のルーティング プロトコルにルートを再配布する条件を定義するには、route-map グローバル コンフィギュレーション コマンドと、match および set ルート マップ コンフィギュレーション コマンドを使用します。route-map コマンドごとに、それに関連した match および set コマンドのリストがあります。match コマンドは、一致基準（現在の route-map コマンドで再配布が許可される条件）を指定します。set コマンドは、set 処理（match コマンドによって強制される基準が満たされた場合に実行される特定の再配布アクション）を指定します。no route-map コマンドはルート マップを削除します。

match ルート マップ コンフィギュレーション コマンドには、複数の形式があります。match コマンドの順序は任意に指定できます。すべての match コマンドが満たされないと、set コマンドで指定した set 処理に従ってルートの再配布が行われません。match コマンドの no 形式を使用すると、指定した一致基準が削除されます。

ルーティング プロセス間でルートを再配布する方法を詳細に制御する必要がある場合にルート マップを使用します。宛先ルーティング プロトコルは router グローバル コンフィギュレーション コマンドを使用して指定します。ソース ルーティング プロトコルは redistribute ルータ コンフィギュレーション コマンドを使用して指定します。ルート マップの設定方法の例については、「例」のセクションを参照してください。

ルートがルート マップを通過するようにするときには、ルート マップに複数の要素を持たせることができます。route-map コマンドに関連付けられているどの match ステートメントとも一致しないルートは無視されます。したがって、そのルートは発信ルートマップ用にアドバタイズされることも、着信ルートマップ用に受け入れられることもありません。一部のデータのみ修正したい場合は、別にルート マップ セクションを設定して明示的に一致基準を指定する必要があります。

sequence-number 引数を使用した場合の動作は次のとおりです。

1. route-map name でエントリが定義されていない場合、sequence-number 引数を 10 にしたエントリが作成されます。

2. route-map name でエントリが 1 つしか定義されていない場合、そのエントリが後続の route-map コマンドのデフォルト エントリになります。このエントリの sequence-number 引数は変わりません。

3. route-map name で複数のエントリが定義されている場合、sequence-number 引数が必要であることを伝えるエラー メッセージが表示されます。

4. no route-map name コマンドが指定されると（sequence-number 引数なし）、ルート マップ全体が削除されます。

例

次の例は、ホップ カウント 1 でルートを OSPF に再配布する方法を示しています。ASA は、これらのルートをメトリック 5、メトリック タイプ 1 で外部 LSA として再配布します。

```
ciscoasa(config)# route-map 1-to-2 permit
ciscoasa(config-route-map)# match metric 11
ciscoasa(config-route-map)# set metric 5
ciscoasa(config-route-map)# set metric-type type-1
```

次に、メトリック値が設定された EIGRP プロセス 1 に 10.1.1.0 のスタティック ルートを再配布する例を示します。

```
ciscoasa (config)# route outside 10.1.1.0 255.255.255.0 192.168.1.1
ciscoasa(config-route-map)# access-list mymap2 line 1 permit 10.1.1.0 255.255.255.0
ciscoasa(config-route-map)# route-map mymap2 permit 10
ciscoasa(config-route-map)# match ip address mymap2
ciscoasa(config-route-map)# router eigrp 1
ciscoasa(config)# redistribute static metric 250 250 1 1 1 route-map
```

関連コマンド

コマンド	説明
redistribute	ルートを 1 つのルーティング ドメインから他のルーティング ドメインに再配布します。
route	インターフェイスのスタティック ルートまたはデフォルト ルートを作成します。
ルータ	指定したプロトコルのルータ コンフィギュレーション モードを開始します。

route priority high

IS-IS プレフィックスに高いプライオリティを割り当てるには、ルータ ISIS コンフィギュレーション モードで **route priority high** コマンドを使用します。IP プレフィックスプライオリティを削除するには、このコマンドの **no** 形式を使用します。

route priority high *tag-value*
no route priority high *tag-value*

構文の説明

tag-value 特定のルート タグを持つ IS-IS IP プレフィックスにハイ プライオリティを割り当てます。指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

IP プレフィックス プライオリティは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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

グローバル ルーティング テーブルでより高速な処理とインストールを実行するために、**route priority high** コマンドを使用して、より高いプライオリティの IS-IS IP プレフィックスにタグ付けすると、より高速なコンバージェンスを実現できます。たとえば、Voice over IP（VoIP）トラフィックが、その他のタイプのパケットよりも速く更新されるようにするために、VoIP ゲートウェイ アドレスが最初に処理されるようにすることができます。

例

次に、**route priority high** コマンドを使用して、IS-IS IP プレフィックスにタグ値 100 を割り当てる例を示します。

```
ciscoasa(config)# router isis
ciscoasa(config-router)# route priority high tag 100
```

関連コマンド

router-alert

IP オプションインスペクションにおいて、パケットヘッダー内でルータアラート IP オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **router-alert** 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。

router-alert action { **allow | clear** }
no router-alert action { **allow | clear** }

構文の説明

allow	ルータ アラート IP オプションを含むパケットを許可します。
clear	ルータ アラート オプションをパケット ヘッダーから削除してから、パケットを許可します。

コマンド デフォルト

デフォルトで、IP オプション インスペクションは、ルータ アラート IP オプションを含むパケットを許可します。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用すると、デフォルト値を変更できます。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプションインスペクションを設定して、特定の IP オプションを持つどの IP パケットが ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

ルータ アラート（RTRALT）または IP オプション 20 は、中継ルータに対して、そのルータ宛てのパケットではない場合でもパケットの内容を検査するように指示します。このインスペク

ションは、RSVP を実装している場合に役に立ちます。同様のプロトコルは、パケット配信パス上にあるルータでの比較的複雑な処理を必要とします。

例

次に、ポリシーマップにおけるプロトコル違反に対するアクションを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

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。

router bgp

ボーダー ゲートウェイ プロトコル（BGP）ルーティング プロセスを設定するには、グローバル コンフィギュレーション モードで router bgp コマンドを使用します。BGP ルーティング プロセスを削除するには、このコマンドの no 形式を使用します。

router bgp *autonomous-system-number*
no router bgp *autonomous-system-number*

構文の説明

autonomous-system-number	他の BGP ルータに対するルータを指定し、同時に渡されるルーティング情報のタギングをする、自律システムの番号。番号の範囲は 1 ～ 65535 です。

コマンド デフォルト

デフォルトでは BGP ルーティング プロセスはイネーブルではありません。

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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、自律システム間でのルーティング情報のループなしのやり取りが自動的に保証される、分散ルーティング コアを設定できます。

2009 年 1 月まで、企業に割り当てられていた BGP 自律システム番号は、RFC 4271『A Border Gateway Protocol 4 (BGP-4)』に記述された、1 ～ 65535 の範囲の 2 オクテットの数値でした。

現在は、自律システム番号の要求の増加に伴い、インターネット割り当て番号局（IANA）により割り当てられる自律システム番号は 65536 ～ 4294967295 の範囲の 4 オクテットの番号になります。

RFC 5396『Textual Representation of Autonomous System (AS) Numbers』には、自律システム番号を表す 3 つの方式が記述されています。シスコでは、次の 2 つの方式を実装しています。

- asplain：10 進表記方式。2 バイトおよび 4 バイト自律システム番号をその 10 進数値で表します。たとえば、65526 は 2 バイト自律システム番号、234567 は 4 バイト自律システム番号になります。
- asdot：自律システム ドット付き表記。2 バイト自律システム番号は 10 進数で、4 バイト自律システム番号はドット付き表記で表されます。たとえば、65526 は 2 バイト自律システム番号、1.169031（10 進表記の 234567 をドット付き表記にしたもの）は 4 バイト自律システム番号になります。

自律システム番号を表す 3 つ目の方法については、RFC 5396 を参照してください。

例

次の例は、自律システム番号 100 用に BGP プロセスを設定する方法を示しています。

```
ciscoasa(config)# router bgp 100
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
show route bgp	ルーティング テーブルを表示します。
show bgp summary	すべてのボーダー ゲートウェイ プロトコル（BGP）接続のステータスを表示します。

router eigrp

EIGRP ルーティングプロセスを開始し、プロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router eigrp** コマンドを使用します。EIGRP ルーティングを無効にするには、このコマンドの **no** 形式を使用します。

router eigrp *as-number*
no router eigrp *as-number*

構文の説明

as-number	他の EIGRP ルータへのルートを識別する自律システム番号。ルーティング情報のタギングにも使用されます。有効値は 1 ～ 65535 です。

コマンド デフォルト

EIGRP ルーティング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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

router eigrp コマンドは、EIGRP ルーティングプロセスを作成するか、または既存の 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。ASA では、単一の EIGRP ルーティングプロセスのみを作成できます。

次のルータ コンフィギュレーション モード コマンドを使用して、EIGRP ルーティング プロセスを設定します。

- **auto-summary**：自動ルート集約を有効または無効にします。
- **default-information**：デフォルトルート情報の送受信を有効または無効にします。
- **default-metric**：EIGRP ルーティングプロセスに再配布されるルートのデフォルトのメトリックを定義します。

- **distance eigrp**：内部および外部 EIGRP ルートのアドミニストレーティブ ディスタンスを設定します。
- **distribute-list**：ルーティング更新で送受信されるネットワークをフィルタリングします。
- **eigrp log-neighbor-changes**：ネイバーステートの変更のロギングを有効または無効にします。
- **eigrp log-neighbor-warnings**：ネイバーの警告メッセージのロギングを有効にします。
- **eigrp router-id**：固定ルータ ID を作成します。
- **eigrp stub**：ASA でスタブ EIGRP ルーティングを設定します。
- **neighbor**：EIGRP ネイバーをスタティックに定義します。
- **network**：EIGRP ルーティングプロセスに参加するネットワークを設定します。
- **passive-interface**：パッシブインターフェイスとして動作するインターフェイスを設定します。
- **redistribute**：他のルーティングプロセスから EIGRP にルートを再配布します。

次のインターフェイス コンフィギュレーション モード コマンドを使用して、インターフェイス固有の EIGRP パラメータを設定します。

- **authentication key eigrp**：EIGRP メッセージ認証で使用される認証キーを定義します。
- **authentication mode eigrp**：EIGRP メッセージ認証で使用される認証アルゴリズムを定義します。
- **delay**：インターフェイスの遅延メトリックを設定します。
- **hello-interval eigrp**：EIGRP の hello パケットがインターフェイスから送信される間隔を変更します。
- **hold-time eigrp**：ASA によってアドバタイズされるホールド時間を変更します。
- **split-horizon eigrp**：インターフェイスで EIGRP スプリットホライズンを有効または無効にします。
- **summary-address eigrp**：サマリーアドレスを手動で定義します。

例

次に、自律システム番号 100 が付けられた EIGRP ルーティング プロセスのコンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
clear configure 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。

router-id

固定ルータ ID を使用するには、ルータ コンフィギュレーション モード（OSPFv2 の場合）または IPv6 ルータ コンフィギュレーション モード（OSPFv3 の場合）で **router-id** コマンドを使用します。以前のルータ ID 動作を使用するように OSPF をリセットするには、このコマンドの **no** 形式を使用します。

router-id *id*
no router-id [*id*]

構文の説明

id	IP アドレス形式でルータ ID を指定します。

コマンド デフォルト

指定しない場合、ASA 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(2)	このコマンドの処理順序が変更されました。このコマンドは、OSPFv2 構成では、**network** コマンドよりも先に処理されるようになりました。
9.0(1)	マルチ コンテキスト モードおよび OSPFv3 がサポートされています。

使用上のガイドライン

ASA のデフォルトでは、OSPF コンフィギュレーションにおいて、**network** コマンドによって指定されているインターフェイス上の最上位の IP アドレスが使用されます。最上位の IP アドレスがプライベート アドレスである場合、そのアドレスは hello パケットおよびデータベース定義で送信されます。特定のルータ ID を使用するには、**router-id** コマンドを使用して、ルータ ID としてグローバルアドレスを指定します。

ルータ ID は、OSPF ルーティング ドメイン内で一意である必要があります。同じ OSPF ドメイン内の 2 つのルータが同じルータ ID を使用している場合、ルーティングが正しく動作しない可能性があります。

OSPF 構成では、**network** コマンドを入力する前に **router-id** コマンドを入力する必要があります。そうすることで、ASA によって生成されるデフォルトのルータ ID との競合を回避できます。競合がある場合は、次のメッセージが表示されます。

```
ERROR: router-id id in use by ospf process pid
```

競合する ID を入力するには、競合の原因となっている IP アドレスを含む **network** コマンドを削除し、**router-id** コマンドを入力して、**network** コマンドを再入力します。

クラスタ

レイヤ 2 クラスタリングでは、すべてのユニットで同じルータ ID を受け取る場合、**router-id** *id* コマンドを設定するか、ルータ ID を空白のままにする必要があります。

例

次に、ルータ ID を 192.168.1.1 に設定する例を示します。

```
ciscoasa(config-rtr)# router-id 192.168.1.1
ciscoasa(config-rtr)#
```

関連コマンド

コマンド	説明
router ospf	ルータ コンフィギュレーション モードを開始します。
show ospf	OSPFv2 ルーティング プロセスに関する一般情報を表示します。

router-id cluster-pool

レイヤ 3 クラスタリング用のルータ ID のクラスタプールを指定するには、ルータ コンフィギュレーション モード（OSPFv2 の場合）またはIPv6 ルータ コンフィギュレーション モード（OSPFv3 の場合）で **router-id cluster-pool** コマンドを使用します。

router-id cluster-pool hostname | A.B.C.D *ip_pool*

構文の説明

cluster-pool	レイヤ 3 クラスタリングが設定されている場合に IP アドレス プールを設定します。
hostname | A.B.C.D	この OSPF プロセスの OSPF ルータ ID を指定します。
ip_pool	IP アドレス プールの名前を指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
ルータ コンフィギュレーション	• 対応	—	• 対応	—	—
IPv6 ルータ コンフィギュレーション	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

ルータ ID は、クラスタリングの OSPFv2 または OSPFv3 ルーティング ドメイン内で一意である必要があります。同じ OSPFv2 または OSPFv3 ドメイン内の 2 つのルータが同じルータ ID を使用している場合、クラスタリングでのルーティングが正しく動作しない可能性があります。

レイヤ 2 クラスタリングでは、すべてのユニットで同じルータ ID を受け取る場合、**router-id** *id* コマンドを設定するか、ルータ ID を空白のままにする必要があります。

レイヤ 3 クラスタのインターフェイスを設定するときは、インターフェイスの IP アドレスをユニットごとに一意にする必要があります。各ユニットのインターフェイスの IP アドレスが一意になるようにするには、**router-id cluster-pool** コマンドを使用して、OSPFv2 または OSPFv3 用に IP アドレスのローカルプールを設定します。

例

次に、OSPFv2 用にレイヤ 3 クラスタリングが設定されている場合の IP アドレス プールを設定する例を示します。

```
ciscoasa(config)# ip local pool rpool 1.1.1.1-1.1.1.4
ciscoasa(config)# router ospf 1
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# network 17.5.0.0 255.255.0.0 area 1
ciscoasa(config-rtr)# log-adj-changes
```

次に、OSPFv3 用にレイヤ 3 クラスタリングが設定されている場合の IP アドレス プールを設定する例を示します。

```
ciscoasa(config)# ipv6 router ospf 2
ciscoasa(config-rtr)# router-id cluster-pool rpool
ciscoasa(config-rtr)# interface gigabitEthernet0/0
ciscoasa(config-rtr)# nameif inside
ciscoasa(config-rtr)# security-level 0
ciscoasa(config-rtr)# ip address 17.5.33.1 255.255.0.0 cluster-pool inside_pool
ciscoasa(config-rtr)# ipv6 address 8888::1/64 cluster-pool p6
ciscoasa(config-rtr)# ipv6 nd suppress-ra
ciscoasa(config-rtr)# ipv6 ospf 2 area 0.0.0.0
```

関連コマンド

コマンド	説明
ipv6 router ospf	IPv6 のルータ コンフィギュレーション モードを開始します。
router ospf	ルータ コンフィギュレーション モードを開始します。
show ipv6 ospf	OSPFv3 ルーティング プロセスに関する一般情報を表示します。
show ospf	OSPFv2 ルーティング プロセスに関する一般情報を表示します。

router isis

IS-IS ルーティングプロトコルを有効にし、IS-IS プロセスを指定するには、グローバル コンフィギュレーション モードで **router isis** コマンドを使用します。IS-IS ルーティングを無効にするには、このコマンドの **no** 形式を使用します。

router isis
no router isis

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。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
9.6(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、エリアの IS-IS ルーティングをイネーブルするために使用されます。エリアのエリアアドレスおよびASAのシステムIDを指定するために、適切なネットワークエンティティタイトル（NET）が設定されている必要があります。隣接関係が確立されてダイナミックルーティングが可能になる前に、1 つ以上のインターフェイスでルーティングをイネーブルにする必要があります。IS-ISの設定に使用するコマンドのリストについては、「関連コマンド」の表を参照してください。

例

次に、IS-IS ルーティングをイネーブルにする例を示します。

```
ciscoasa# configure terminal
ciscoasa(config)# router isis
ciscoasa(config-router)#
```

関連コマンド

router ospf

OSPF ルーティングプロセスを開始し、プロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router ospf** コマンドを使用します。OSPF ルーティングを無効にするには、このコマンドの **no** 形式を使用します。

router ospf *pid*
no router ospf *pid*

構文の説明

pid OSPF ルーティング プロセスの内部的に使用される ID パラメータ。有効な値は、1 ～ 65535 です。*pid* は、他のルータの OSPF プロセスの ID と一致する必要はありません。

コマンド デフォルト

OSPF ルーティング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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードはサポートされます。

使用上のガイドライン

router ospf コマンドは、ASA 上で実行される OSPF ルーティングプロセスのグローバル コンフィギュレーション コマンドです。**router ospf** コマンドを入力すると、コマンドプロンプトに (config-router)# と表示され、ルータ コンフィギュレーション モードが開始したことが示されます。

no router ospf コマンドを使用する場合、必要な情報を指定する場合を除き、オプションの引数を指定する必要はありません。**no router ospf** コマンドは、*pid* によって指定された OSPF ルーティングプロセスを終了します。*pid* は、ASA においてローカルに割り当てます。OSPF ルーティング プロセスごとに固有の値を割り当てる必要があります。

router ospf コマンドは、次の OSPF 固有のコマンドとともに、OSPF ルーティングプロセスを設定するために使用されます。

- **area**：通常の OSPF エリアを設定します。
- **compatible rfc1583**：サマリールートのコスト計算に使用される方法を RFC 1583 に従った方法に戻します。
- **default-information originate**：デフォルトの外部ルートを OSPF ルーティングドメインに生成します。
- **distance**：ルートタイプに基づいて、OSPF ルート アドミニストレーティブ ディスタンスを定義します。
- **ignore**：ルータがタイプ 6 Multicast OSPF（MOSPF）パケットのリンクステート アドバタイズメント（LSA）を受信した場合の syslog メッセージの送信を抑制します。
- **log-adj-changes**：OSPF ネイバーが起動または停止したときに、ルータが syslog メッセージを送信するように設定します。
- **neighbor**：ネイバールータを指定します。VPN トンネル経由での隣接関係の確立を許可するために使用します。
- **network**：OSPF が実行するインターフェイスと、各インターフェイスに対するエリア ID を定義します。
- **redistribute**：指定されたパラメータに従って、ルーティングドメイン間でのルートの再配布を設定します。
- **router-id**：固定ルータ ID を作成します。
- **summary-address**：OSPF の集約アドレスを作成します。
- **timer lsa arrival**：OSPF ネイバーから同一のリンクステート アドバタイズメント（LSA）を受け入れる最小間隔（ミリ秒）を定義します。
- **timer pacing flood**：フラッディングキュー内の LSA の最小更新間隔（ミリ秒）を定義します。
- **timer pacing lsa-group**：LSA のグループのリフレッシュまたは管理の間隔（秒）を定義します。
- **timer pacing retransmission**：ネイバー再送信の最小間隔（ミリ秒）を定義します。
- **timer throttle lsa**：LSA の最初のオカレンスを生成する遅延（ミリ秒）を定義します。
- **timer throttle spf**：SPF 計算の変更を受信する遅延（ミリ秒）を定義します。
- **timer nsf wait**：NSF 再起動中のインターフェイス待機間隔を定義します。デフォルト値は 20 秒です。許容範囲は 1 ～ 65535 秒です。

例

次に、OSPF ルーティング プロセス番号 5 のコンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# router ospf 5
ciscoasa(config-router)#
```

関連コマンド

コマンド	説明
clear configure router	実行コンフィギュレーションから OSPF ルータ コマンドをクリアします。
show running-config router ospf	実行コンフィギュレーション内の OSPF ルータ コマンドを表示します。

router rip

RIP ルーティングプロセスを開始し、プロセスのパラメータを設定するには、グローバル コンフィギュレーション モードで **router rip** コマンドを使用します。RIP ルーティングプロセスを無効にするには、このコマンドの **no** 形式を使用します。

router rip
no router rip

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。

コマンド デフォルト

RIP ルーティング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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

router rip コマンドは、ASA 上の RIP ルーティングプロセスを設定するためのグローバル コンフィギュレーション コマンドです。ASA では、1 つの RIP プロセスのみ設定できます。**no router rip** コマンドは、RIP ルーティングプロセスを終了し、そのプロセスのすべてのルータ構成を削除します。

router rip コマンドを入力すると、ルータ コンフィギュレーション モードであることを示す (config-router)# にコマンドプロンプトが変更されます。

router rip コマンドは、次のルータ コンフィギュレーション コマンドとともに、RIP ルーティングプロセスを設定するために使用されます。

- **auto-summary**：ルートの自動集約を有効または無効にします。
- **default-information originate**：デフォルトルートを配布します。
- **distribute-list in**：ネットワークの着信ルーティングアップデートをフィルタリングします。

- **distribute-list out**：ネットワークの発信ルーティングアップデートをフィルタリングします。
- **network**：ルーティングプロセスでインターフェイスを追加または削除します。
- **passive-interface**：特定のインターフェイスをパッシブモードに設定します。
- **redistribute**：他のルーティングプロセスからRIPルーティングプロセスにルートを再配布します。
- **version**：ASA で使用される RIP プロトコルバージョンを設定します。

また、次のコマンドをインターフェイス コンフィギュレーションモードで使用して、インターフェイスごとの RIP プロパティを設定できます。

- **rip authentication key**：認証キーを設定します。
- **rip authentication mode**：RIP バージョン 2 によって使用される認証のタイプを設定します。
- **rip send version**：インターフェイスから更新を送信するために使用する RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。
- **rip receive version**：インターフェイスで受け入れる RIP のバージョンを設定します。グローバル ルータ コンフィギュレーション モードでバージョンが設定されている場合は、このコマンドによって上書きされます。

トランスペアレント モードでは RIP はサポートされていません。ASA のデフォルトでは、すべてのRIPブロードキャストパケットおよびマルチキャストパケットが拒否されます。これらの RIP メッセージが、トランスペアレントモードで動作する ASA を通過できるようにするには、このトラフィックを許可するアクセスリストエントリを定義する必要があります。たとえば、RIP バージョン 2 トラフィックが ASA を通過できるようにするには、次のようなアクセスリストエントリを作成します。

ciscoasa(config)# **access-list myriplist extended permit ip any host 224.0.0.9**

RIP バージョン 1 のブロードキャストを許可するには、次のようなアクセス リスト エントリを作成します。

ciscoasa(config)# **access-list myriplist extended permit udp any any eq rip**

access-group コマンドを使用して、それらのアクセスリストエントリを適切なインターフェイスに適用します。

ASA では、RIP ルーティングと OSPF ルーティングの両方を同時に有効にできます。

例

次に、OSPF ルーティング プロセス番号 5 のコンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# router rip
```

```
ciscoasa(config-rtr)# network 10.0.0.0
ciscoasa(config-rtr)# version 2
```

関連コマンド

コマンド	説明
clear configure router rip	実行コンフィギュレーションからRIPルータ コマンドをクリアします。
show running-config router rip	実行コンフィギュレーション内のRIPルータ コマンドを表示します。

rtp-conformance

ピンホールを通過する RTP パケットが H.323 および SIP プロトコルに準拠しているかチェックするには、パラメータ コンフィギュレーション モードで **rtp-conformance** 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。

rtp-conformance [**enforce-payloadtype**]
no rtp-conformance [**enforce-payloadtype**]

構文の説明

enforce-payloadtype	シグナリング交換に基づいて、ペイロードタイプをオーディオまたはビデオであると指定します。

コマンド 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、ピンホールを通過する RTP パケットが H.323 コールのプロトコルに準拠しているかどうかをチェックする例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# rtp-conformance
```

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
debug rtp	H.323 および SIP インスペクションに関連する RTP パケットのデバッグ情報およびエラー メッセージを表示します。
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。

rtp-min-port rtp-max-port（廃止予定）

電話プロキシ機能の rtp-min-port および rtp-max-port の制限を設定するには、電話プロキシ コンフィギュレーション モードで **rtp-min-port rtp-max-port** コマンドを使用します。電話プロキシ コンフィギュレーションから制限を削除するには、このコマンドの **no** 形式を使用します。

rtp-min-port *port1* **rtp-maxport** *port2*
no rtp-min-port *port1* **rtp-maxport** *port2*

構文の説明

port1 メディア ターミネーション ポイントの RTP ポート範囲の最小値を指定します。*port1* には、1024 ～ 16384 の値を指定できます。

port2 メディア ターミネーション ポイントの RTP ポート範囲の最大値を指定します。*port2* には、32767 ～ 65535 の値を指定できます。

コマンド デフォルト

デフォルトでは、**rtp-min-port** キーワードの *port1* の値は 16384、**rtp-max-port** キーワードの *port2* の値は 32767 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。

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		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
Phone-Proxy コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.2(1)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モードコマンドとともに廃止されました。

使用上のガイドライン

電話プロキシでサポートするコール数の規模を調整する必要がある場合は、メディア ターミネーション ポイントの RTP ポート範囲を設定します。

例

次に、**rtp-min-port** コマンドを使用して、メディア接続に使用するポートを指定する例を示します。

```
ciscoasa
```

```
(config-phone-proxy)#
rtp-min-port 2001 rtp-maxport 32770
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。