ia – inr

- icmp （3 ページ）
- icmp-object （6 ページ）
- icmp unreachable （8 ページ）
- id-cert-issuer （10 ページ）
- id-mismatch （12 ページ）
- id-randomization （14 ページ）
- id-usage （16 ページ）
- igmp （18 ページ）
- igmp access-group （19 ページ）
- igmp forward interface （21 ページ）
- igmp join-group （23 ページ）
- igmp limit （25 ページ）
- igmp query-interval （27 ページ）
- igmp query-max-response-time （29 ページ）
- igmp query-timeout （31 ページ）
- igmp static-group （33 ページ）
- igmp version （35 ページ）
- ignore-ipsec-keyusage（廃止） （37 ページ）
- ignore lsa mospf （39 ページ）
- ignore-lsp-errors （40 ページ）
- ignore-ssl-keyusage（廃止） （45 ページ）
- ike-retry-count （47 ページ）
- ikev1 pre-shared-key （49 ページ）
- ikev1 trust-point （51 ページ）
- ikev1 user-authentication （53 ページ）
- ikev2 local-authentication （55 ページ）
- ikev2 mobike-rrc （57 ページ）
- ikev2 remote-authentication （59 ページ）
- ikev2 rsa-sig-hash （62 ページ）
- im （64 ページ）

- imap4s（廃止） （66 ページ）
- imi-traffic-descriptor （68 ページ）
- import （70 ページ）
- import webvpn AnyConnect-customization （74 ページ）
- import webvpn customization （76 ページ）
- import webvpn mst-translation （78 ページ）
- import webvpn plug-in protocol （79 ページ）
- import webvpn translation-table （82 ページ）
- import webvpn url-list （85 ページ）
- import webvpn webcontent （87 ページ）

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	説明
[0]	echo-reply	エコー応答は、通信が成功したことを示すエコー要求への応答です。
3	unreachable	デバイスで、最終目的地にパッケージを配信できませんでした。
8	echo	送信元のアドレスを伝送するエコーメッセージ。このアドレスは、エコー応答メッセージの送信先です。
11	time-exceeded	パッケージの処理中にデバイスで存在可能時間（TTL）値がゼロであることを識別したため、パッケージは廃棄されます。

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。

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 500 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 500 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。

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。

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。