CHAPTER 14

icmp コマンド ～ import webvpn webcontent コマンド

icmp

セキュリティ アプライアンス 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 3 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	*ip_address* に適用されるマスク。
permit	条件に合致している場合、アクセスを許可します。

デフォルト

セキュリティ アプライアンスのデフォルトの動作は、セキュリティ アプライアンス インターフェイス*に向かう*すべての ICMP トラフィックを許可することです。ただし、セキュリティ アプライアンスはデフォルトで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。また、セキュリティ アプライアンスは宛先が保護されたインターフェイスにある場合、は外部インターフェイスで受信された ICMP メッセージを拒否します。

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。

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

コマンド履歴

リリース	変更内容
6.0	このコマンドが導入されました。

使用上のガイドライン

icmp コマンドは、セキュリティ アプライアンス 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、セキュリティ アプライアンス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、セキュリティ アプライアンスはデフォルトで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。

セキュリティ アプライアンスは、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、インターフェイス経由で離れたインターフェイスに送信できません。

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 の実行がディセーブルの場合、セキュリティ アプライアンス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** コマンドはセキュリティ アプライアンス*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、セキュリティ アプライアンスは指定された 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、エントリに一致しない場合、セキュリティ アプライアンスによって 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。

表 3 に、サポートされている ICMP タイプの値を示します。

表 14-1　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、外部インターフェイスですべての ping 要求を拒否し、すべての到達不能メッセージを許可する例を示します。

```
hostname(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行します。

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。

```
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(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 unreachable

セキュリティ アプライアンス 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。このキーワードは、現在システムで使用されていないため、任意の値を選択できます。

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。

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

コマンド履歴

リリース	変更内容
7.2(2)	このコマンドが導入されました。

使用上のガイドライン

到達不能メッセージなどの ICMP メッセージにセキュリティ アプライアンス インターフェイスでの終了を許可する（**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。

セキュリティ アプライアンスをホップの 1 つとして表示する traceroute がセキュリティ アプライアンスを経由できるようにするには、**set connection decrement-ttl** コマンドとともにこのコマンドが必要です。

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。

```
hostname(config)# policy-map localpolicy1
hostname(config-pmap)# class local_server
hostname(config-pmap-c)# set connection decrement-ttl
hostname(config-pmap-c)# exit
hostname(config)# icmp permit host 172.16.2.15 echo-reply outside
hostname(config)# icmp permit 172.22.1.0 255.255.0.0 echo-reply outside
hostname(config)# icmp permit any unreachable outside
hostname(config)# icmp unreachable rate-limit 50 burst-size 1
```

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。

icmp-object

ICMP タイプのオブジェクト グループを追加するには、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。ネットワーク 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。

icmp-object *icmp_type*

no group-object *icmp_type*

構文の説明

icmp_type	ICMP タイプの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

icmp-object コマンドは、ICMP タイプの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。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**
4	**source-quench**
5	**redirect**
6	**alternate-address**
8	**echo**
9	**router-advertisement**
10	**router-solicitation**
11	**time-exceeded**
12	**parameter-problem**

番号	ICMP タイプ名
13	**timestamp-request**
14	**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。

```
hostname(config)# object-group icmp-type icmp_allowed
hostname(config-icmp-type)# icmp-object echo
hostname(config-icmp-type)# icmp-object time-exceeded
hostname(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。
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。
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。
show running-config object-group	現在のオブジェクト グループを表示します。

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 が発行した証明書を禁止するには、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。

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

次の表は、このコマンドを入力できるモードを示しています。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

使用上のガイドライン

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、セキュリティ アプライアンス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。

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

関連コマンド

コマンド	説明
crypto ca trustpoint	トラストポイント サブモードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。

コマンド	説明
enrollment retry period	登録要求の送信を試行するまでの待機時間を分単位で指定します。
enrollment terminal	このトラストポイントを使用したカット アンド ペースト登録を指定します。

id-mismatch

過度の DNS ID 不一致のロギングをイネーブルにするには、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**

no 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）。

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

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** コマンドを使用すると、システム管理者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、さらに情報を得ることができます。

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。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(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 クエリーの 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。

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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

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。

```
hostname(config)# policy-map type inspect dns preset_dns_map
hostname(config-pmap)# parameters
hostname(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。
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（クリプト CA トラスト ポイント）

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（**ssl-ipsec**）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 接続のサーバ側 ID として使用できます。

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。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

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 モードのすべてのコマンドは、セキュリティ アプライアンスが CA 証明書を取得する方法、セキュリティ アプライアンスが 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 か ssl-ipsec、またはその両方のトラストポイントをイネーブルにするには、コマンドを 1 回のみ使用して、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に指定する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(config-ca-trustpoint)# id-usage code-signer
hostname(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 接続のサーバ側 ID として指定する例を示します。

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

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

関連コマンド

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

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。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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。

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

関連コマンド

コマンド	説明
show igmp groups	セキュリティ アプライアンス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。

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**任意の**アドレスを指定できます。

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。

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

コマンド履歴

リリース	変更内容
7.0(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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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 レポートの転送をイネーブルにし、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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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セキュリティ アプライアンス 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、セキュリティ アプライアンス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するようになります。

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セキュリティ アプライアンスを設定するには、**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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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 ～ 500 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、（**igmp join-group** コマンドおよび **igmp static-group** コマンドを使用して）手動で定義したメンバーシップは引き続き許可されます。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。**igmp max-groups** コマンドに置き換わるものです。

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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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。

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。

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

コマンド履歴

リリース	変更内容
7.0(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。

ルータは、タイムアウト期間（**igmp query-timeout** コマンドで制御）にクエリーを受信しないと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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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 クエリー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。

igmp query-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。

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。

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

コマンド履歴

リリース	変更内容
7.0(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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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ー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。

igmp query-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。

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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

igmp static-group コマンドで設定された場合、セキュリティ アプライアンス 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、転送のみを行います。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セキュリティ アプライアンスを設定するには、**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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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。

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。

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

コマンド履歴

リリース	変更内容
7.0(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、セキュリティ アプライアンスはホストの存在を正しく検出して適切にホストを照会できます。

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。

```
hostname(config)# interface gigabitethernet 0/0
hostname(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

IPsec クライアント証明書でキー使用状況チェックを行わないようにするには、設定 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。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドは安全対策として導入されましたが、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。

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

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

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。

```
hostname(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。

ike-retry-count

SSL による接続試行に戻るまでに、Cisco AnyConnect VPN クライアントが 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。コンフィギュレーション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。

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。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco AnyConnect VPN クライアントが 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** と **ipsec** の両方の引数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。

```
hostname(config)# group-policy FirstGroup attributes
```

```
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# ike-retry-count 7
hostname(config-group-webvpn)#
```

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

```
hostname(config)# username Finance attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# ike-retry-count 9
hostname(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	セキュリティ アプライアンス データベースにユーザを追加します。
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 モードまたはユーザ名モード）	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名 webvpn コンフィギュレーション モードを開始します。

ike-retry-timeout

Cisco AnyConnect VPN Client の IKE 再試行の間隔を秒数で設定するには、グループ ポリシー webvpn またはユーザ名 webvpn コンフィギュレーション モードで **ike-retry-timeout** コマンドを使用します。このコマンドをコンフィギュレーションから削除する場合や、タイムアウト値をデフォルト値にリセットする場合は、このコマンドの **no** 形式を使用します。

ike-retry-count *seconds*

no ike-retry-count

構文の説明

seconds	Cisco AnyConnect VPN Client が、最初の接続の失敗後に実行する IKE 再試行の間隔（1 ～ 3600) を秒数で指定します。

デフォルト

デフォルトのタイムアウトは 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。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

Cisco AnyConnect VPN Client の IKE 再試行の間隔（時間の長さ）を制御するには、**ike-retry-timeout** コマンドを使用します。クライアントが、**ike-retry-count** コマンドで指定された数の再試行を行った後で、IKE を使用した接続に失敗した場合は、SSL に戻って接続が試行されます。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** と **ipsec** の両方の引数を設定する必要があります。

例

次の例では、FirstGroup というグループ ポリシーに対して、IKE 再試行間隔を 77 秒に設定しています。

```
hostname(config)# group-policy FirstGroup attributes
hostname(config-group-policy)# webvpn
hostname(config-group-webvpn)# ike-retry-timeout 77
hostname(config-group-webvpn)#
```

次の例では、Finance というユーザ名に対して、IKE 再試行回数を 99 回に設定しています。

```
hostname(config)# username Finance attributes
hostname(config-username)# webvpn
hostname(config-username-webvpn)# ike-retry-timeout 9
hostname(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-count	IKE を使用する Cisco AnyConnect VPN Client が、SSL に戻って接続を試行する前に実行する接続再試行の最大数を指定します。
username	セキュリティ アプライアンス データベースにユーザを追加します。
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 モードまたはユーザ名モード）	グループ ポリシー webvpn モードまたはユーザ名 webvpn モードに入ります。

im

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。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。

im

no im

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。

例

次に、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。

```
hostname(config)# policy-map type inspect sip sip_map
hostname(config-pmap)# parameters
hostname(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。
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

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。

IMAP4 は、インターネット サーバ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 プロトコルです。ユーザ（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。

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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが導入されました。

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。

```
hostname(config)# imap4s
hostname(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。

import webvpn customization

カスタマイゼーション オブジェクトをセキュリティ アプライアンスのフラッシュ デバイスにロードするには、特権 EXEC モードで **import webvpn customization** コマンドを入力します。

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 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 255 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

import customization コマンドを入力する前に、セキュリティ アプライアンス インターフェイスで WebVPN がイネーブルになっていることを確認します。そのためには、**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、セキュリティ アプライアンスは次のことを行います。

- カスタマイゼーション オブジェクトを URL からセキュリティ アプライアンス 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、セキュリティ アプライアンス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、セキュリティ アプライアンスは 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 からセキュリティ アプライアンスにインポートし、それに *custom1* という名前を付ける例を示します。

```
hostname# 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	セキュリティ アプライアンスのフラッシュ 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	セキュリティ アプライアンスのフラッシュ 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

セキュリティ アプライアンスのフラッシュ 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 *protocol 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*。これらの要件から逸脱する **import webvpn plug-in protocol** コマンドを削除するには、**revert webvpn plug-in protocol** コマンドを使用します。 • **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。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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

プラグインをインストールする前に、次のことを行います。

- セキュリティ アプライアンスのインターフェイス上でクライアントレス SSL VPN（「webvpn」）がイネーブルになっていることを確認します。これを行うには、**show running-config** コマンドを入力します。
- ローカル TFTP サーバ（たとえば、ホスト名が「local_tftp_server」のサーバ）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、セキュリティ アプライアンスは次のことを行います。

- *URL* に指定されている jar ファイルを解凍します。
- そのファイルをセキュリティ アプライアンス ファイル システムの `csco-config/97/plugin` ディレクトリに書き込みます。
- 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。表 14-2 に、ポータル ページのメイン メニューと Address フィールドに加えられた変更を示します。

表 14-2　クライアントレス SSL VPN ポータル ページへのプラグインの影響

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
rdp	ターミナル サーバ	rdp://
ssh、telnet	SSH	ssh://
	Telnet	telnet://
vnc	VNC Client	vnc://

セキュリティ アプライアンスは、**import webvpn plug-in protocol** コマンドをコンフィギュレーションに保持しません。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 セキュリティ アプライアンスは、プライマリ セキュリティ アプライアンス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） SSH クライアントは、SSH バージョン 1.0 のみをサポートします。

Java プラグインによっては、宛先サービスへのセッションが設定されていない場合でも、接続済みまたはオンラインというステータスがレポートされることがあります。open-source プラグインは、セキュリティ アプライアンスではなくステータスをレポートします。

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ディセーブルにするには、**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。

```
hostname# 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。

```
hostname# 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。

```
hostname# 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)
hostname#
```

関連コマンド

コマンド	説明
revert webvpn plug-in protocol	セキュリティ アプライアンスのフラッシュ 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	セキュリティ アプライアンスのフラッシュ 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

リモート ユーザが SSL VPN 接続を確立するときに表示される言語を変換するため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 モードから **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 ユーザに表示される機能エリアと関連するメッセージ。使用上のガイドラインのセクションに、使用可能な変換ドメインがリストされています。
url	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。

デフォルト

このコマンドには、デフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

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

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

表 14-3　変換ドメインと影響を受ける機能エリア

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

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

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

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 は中国語に短縮形 *zh* を使用します。セキュリティ アプライアンス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 AnyConnect クライアント ユーザに表示されます。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、AnyConnect クライアント ユーザ 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のもの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、新規オブジェクトを表示します。

```
hostname# import webvpn translation-table anyconnect language zh
tftp://209.165.200.225/anyconnect
hostname# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
hostname# 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。
revert	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

セキュリティ アプライアンスのフラッシュ 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 64 文字です。
URL	URL リストのソースへのリモート パス。最大 255 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
(8.0(2)	このコマンドが導入されました。

使用上のガイドライン

import url-list コマンドを入力する前に、セキュリティ アプライアンス インターフェイスで WebVPN がイネーブルになっていることを確認します。そのためには、**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、セキュリティ アプライアンスは次のことを行います。

- URL リストを URL からセキュリティ アプライアンス 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。無効な場合、セキュリティ アプライアンス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、セキュリティ アプライアンスは 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 からセキュリティ アプライアンスにインポートし、それに *ABCList* という名前を付ける例を示します。

```
hostname# 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	セキュリティ アプライアンスのフラッシュ デバイスから指定された URL リストを削除します。
show import webvpn url-list	セキュリティ アプライアンスのフラッシュ 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 モードから **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

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

デフォルト

このコマンドにデフォルトの動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

webcontent オプション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、不正なユーザと認可されたユーザ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。表 14-4 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。

表 14-4　標準のクライアントレス アプリケーション

URL	クライアントレス画面エリア
/+CSCOE+/help/<*language*>/app-access-hlp.inc	アプリケーション アクセス
/+CSCOE+/help/<*language*>/file-access-hlp.inc	ブラウズ ネットワーク
/+CSCOE+/help/<*language*>/net_access_hlp.html	AnyConnect クライアント
/+CSCOE+/help/<*language*>/web-access-help.inc	Web アクセス

表 14-5 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。

表 14-5　プラグイン クライアントレス アプリケーション

URL	クライアントレス画面エリア
/+CSCOE+/help/<*language*>/ica-hlp.inc	MetaFrame アクセス
/+CSCOE+/help/<*language*>/rdp-hlp.inc	ターミナル サーバ
/+CSCOE+/help/<*language*>/ssh,telnet-hlp.inc	Telnet/SSH サーバ
/+CSCOE+/help/<*language*>/vnc-hlp.inc	VNC コネクション

URL パスの <*language*> は、ヘルプ コンテンツ用に指定した言語の短縮形です。セキュリティ アプライアンスは、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、ファイルに言語の短縮形のラベルを付けます。

次に、HTML ファイル *application_access_help.html* を 209.165.200.225 の tftp サーバからフラッシュ 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。

```
hostname# 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
hostname#
```

例

次に、HTML ファイル *application_access_help.html* を 209.165.200.225 の tftp サーバからフラッシュ 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。

```
hostname# 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
hostname#
```

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。