CHAPTER 5

cache コマンド～ clear compression コマンド

cache

キャッシュ モードを開始し、キャッシング属性の値を設定するには、webvpn コンフィギュレーション モードで **cache** コマンドを入力します。コンフィギュレーションからキャッシュ関連のコマンドをすべて削除し、これらをデフォルト値にリセットするには、このコマンドの **no** 形式を入力します。

cache

no cache

デフォルト

各キャッシュ属性のデフォルト設定でイネーブルになっています。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

キャッシングによって頻繁に再利用されるオブジェクトはシステム キャッシュに保存され、コンテンツを繰り返しリライトしたり圧縮したりする必要性を減らすことができます。キャッシングにより、WebVPN とリモート サーバおよびエンド ユーザのブラウザの両方の間のトラフィックが削減されて、多くのアプリケーションの実行効率が大幅に向上されます。

例

次に、キャッシュ モードを開始する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# cache
hostname(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache-static-content	書き換えの対象でないコンテンツをキャッシュします。
disable	キャッシュをディセーブルにします。
expiry-time	オブジェクトを再検証せずにキャッシュする有効期限を設定します。
lmfactor	最終変更時刻のタイムスタンプだけを持つオブジェクトのキャッシュに関する再確認ポリシーを設定します。
max-object-size	キャッシュするオブジェクトの最大サイズを定義します。
min-object-size	キャッシュするオブジェクトの最小サイズを定義します。

cache-fs limit

セキュリティ アプライアンスがリモート PC にダウンロードするイメージを保存するために使用するキャッシュ ファイル システムのサイズを制限するには、webvpn コンフィギュレーション モードで **cache-fs limit** 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。

cache-fs limit {*size*}

no cache-fs limit {*size*}

構文の説明

size	キャッシュ ファイル システムのサイズ制限（1 ～ 32 MB）。

デフォルト

デフォルト値は 20 MB です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

セキュリティ アプライアンスは、Cisco AnyConnect VPN Client および Cisco Secure Desktop（CSD）のイメージおよびファイルを含むパッケージ ファイルを、リモート PC へのダウンロード用にキャッシュ メモリ内で展開します。セキュリティ アプライアンスで正常にパッケージ ファイルを展開するには、このイメージとファイルを保存するのに十分なキャッシュ メモリが必要です。

パッケージの展開に十分なキャッシュ メモリがないことをセキュリティ アプライアンスが検出した場合、コンソールにエラー メッセージが表示されます。次に、**svc image** コマンドで AnyConnect VPN Client のイメージ パッケージをインストールしようとした後にレポートされるエラー メッセージの例を示します。

```
hostname(config-webvpn)# svc image disk0:/vpn-win32-Release-2.0-k9.pkg
ERROR: File write error (check disk space)
ERROR: Unable to load SVC image - extraction failed
```

イメージ パッケージをインストールしようとしてこのエラー メッセージがレポートされた場合は、グローバル コンフィギュレーション モードで **dir cache:/** コマンドを使用して、キャッシュ メモリの残量およびこれまでにインストールしたパッケージのサイズを検査できます。検査結果に応じて、キャッシュ サイズの制限を調整できます。

例

次に、CSD イメージ（sdesktop 内）および CVC イメージ（stc 内）が約 5.44 MB のキャッシュ メモリを使用している例を示します。

```
hostname(config-webvpn)# dir cache:/

Directory of cache:/

0      drw-  0           17:06:55 Nov 13 2006  sdesktop
0      drw-  0           16:46:54 Nov 13 2006  stc

5435392 bytes total (4849664 bytes free)
```

次に、キャッシュ サイズを 6 MB に制限する例を示します。

```
hostname(config-webvpn)# cache-fs limit 6
```

関連コマンド

コマンド	説明
dir cache:/	キャッシュ メモリの内容（予約されているキャッシュ メモリの総量やキャッシュ メモリの残量など）を表示します。
show run webvpn	現在の WebVPN コンフィギュレーション（キャッシュ メモリを消費する可能性があるインストール済みの SSL VPN クライアントや CSD イメージなど）を表示します。
show webvpn csd	CSD バージョンおよびインストール ステータスを表示します。
show webvpn svc	インストール済みの SSL VPN パッケージ ファイルの名前およびバージョンを表示します。

cache-static-content

クライアントレス SSL VPN 接続に使用するすべての静的コンテンツがキャッシュ メモリにロードされるようセキュリティ アプライアンスを設定するには、キャッシュ コンフィギュレーション モードで **cache-static-content** コマンドを使用します。

cache-static-content enable

no cache-static-content enable

構文の説明

enable	すべての静的コンテンツのキャッシュ メモリへのロードをイネーブルにします。

デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

キャッシュ可能なすべての静的コンテンツがセキュリティ アプライアンスのキャッシュに保存されるようセキュリティ アプライアンスを設定すると、バックエンド SSL VPN 接続のパフォーマンスが向上します。静的コンテンツには、PDF ファイルやイメージなど、セキュリティ アプライアンスによってデータの書き換え（上書き）が行われないオブジェクトが含まれています。

例

次の例は、静的コンテンツのキャッシュをイネーブルにする方法を示したものです。

```
hostname(config-webvpn-cache)# cache-static-content enable
```

関連コマンド

コマンド	説明
cache-compressed	WebVPN キャッシュの圧縮を設定します。
disable	キャッシュをディセーブルにします。

cache-time

CRL を失効と見なす前にキャッシュ内に残す時間を分単位で指定するには、crl 設定コンフィギュレーション モードで **cache-time** コマンドを使用します。このモードには、クリプト CA トラストポイント コンフィギュレーション モードからアクセスできます。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。

cache-time *refresh-time*

no cache-time

構文の説明

refresh-time	CRL をキャッシュ内に残す時間を分単位で指定します。指定できる範囲は 1 ～ 1440 分です。CRL に NextUpdate フィールドがない場合、CRL はキャッシュされません。

デフォルト

デフォルトの設定は 60 分です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	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
crl 設定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、ca-crl コンフィギュレーション モードを開始し、トラストポイント central でキャッシュ時間のリフレッシュ値を 10 分に指定する例を示します。

```
hostname(configure)# crypto ca trustpoint central
hostname(ca-trustpoint)# crl configure
hostname(ca-crl)# cache-time 10
hostname(ca-crl)#
```

関連コマンド

コマンド	説明
crl configure	CRL コンフィギュレーション モードを開始します。
crypto ca trustpoint	トラストポイント コンフィギュレーション モードを開始します。
enforcenextupdate	証明書で NextUpdate CRL フィールドを処理する方法を指定します。

call-agent

コール エージェントのグループを指定するには、MGCP マップ コンフィギュレーション モードで **call-agent** コマンドを使用します。このモードには、**mgcp-map** コマンドを使用してアクセスできます。設定を削除するには、このコマンドの **no** 形式を使用します。

call-agent *ip_address group_id*

no call-agent *ip_address group_id*

構文の説明

ip_address	ゲートウェイの IP アドレス。
group_id	コール エージェント グループの ID（0 ～ 2147483647）。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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

1 つ以上のゲートウェイを管理できるコール エージェントのグループを指定するには、**call-agent** コマンドを使用します。コール エージェントのグループ情報は、どのコール エージェントも応答を送信できるように、グループ内の（ゲートウェイがコマンドを送信する先以外の）コール エージェントに接続を開くために使用されます。同じ *group_id* を持つコール エージェントは、同じグループに属します。1 つのコール エージェントは複数のグループに所属できます。*group_id* オプションには、0 ～ 4294967295 の数字を指定します。*ip_address* オプションには、コール エージェントの IP アドレスを指定します。

例

次に、コール エージェント 10.10.11.5 および 10.10.11.6 にゲートウェイ 10.10.10.115 の制御を許可し、コール エージェント 10.10.11.7 および 10.10.11.8 にゲートウェイ 10.10.10.116 および 10.10.10.117 の制御を許可する例を示します。

```
hostname(config)# mgcp-map mgcp_inbound
hostname(config-mgcp-map)# call-agent 10.10.11.5 101
hostname(config-mgcp-map)# call-agent 10.10.11.6 101
hostname(config-mgcp-map)# call-agent 10.10.11.7 102
hostname(config-mgcp-map)# call-agent 10.10.11.8 102
hostname(config-mgcp-map)# gateway 10.10.10.115 101
hostname(config-mgcp-map)# gateway 10.10.10.116 102
```

```
hostname(config-mgcp-map)# gateway 10.10.10.117 102
```

関連コマンド

コマンド	説明
debug mgcp	MGCP のデバッグ情報の表示をイネーブルにします。
mgcp-map	MGCP マップを定義し、MGCP マップ コンフィギュレーション モードをイネーブルにします。
show mgcp	MGCP のコンフィギュレーションおよびセッションの情報を表示します。

call-duration-limit

H.323 コールのコール継続時間を設定するには、パラメータ コンフィギュレーション モードで **call-duration-limit** 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。

call-duration-limit *hh:mm:ss*

no call-duration-limit *hh:mm:ss*

構文の説明

hh:mm:ss	継続時間を時、分、および秒で指定します。

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
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、H.323 コールのコール継続時間を設定する例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-duration-limit 0:1:0
```

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。

call-party-numbers

H.323 コールの設定時に発信側の番号の送信を適用にするには、パラメータ コンフィギュレーション モードで **call-party-numbers** 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。

call-party-numbers

no call-party-numbers

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
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、H.323 コールのコール設定時に発信側の番号を適用する例を示します。

```
hostname(config)# policy-map type inspect h323 h323_map
hostname(config-pmap)# parameters
hostname(config-pmap-p)# call-party-numbers
```

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。

capture

パケット キャプチャ機能をイネーブルにして、パケットのスニッフィングやネットワーク障害を検出できるようにするには、特権 EXEC モードで **capture** コマンドを使用します。パケット キャプチャ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。

capture *capture_name* [**type** {**asp-drop all** [*drop-code*] | **tls-proxy**| **raw-data** | **isakmp** | **decrypted** | **webvpn user** *webvpn-user* [**url** *url*]}] [**access-list** *access_list_name*] [**buffer** *buf_size*] [**ethernet-type** *type*] [**interface** *interface_name*] [**packet-length** *bytes*] [**circular-buffer**] [**trace** *trace_count*] [**real-time**] [**dump**] [**detail**] [**trace**] [**match** *prot* {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

no capture *capture-name* [**type** {**asp-drop** [*drop-code*] | **tls-proxy** | **raw-data** | **isakmp** | **decrypted** | **webvpn user** *webvpn-user*] [**access-list** *access_list_name*] [**circular-buffer**] [**interface** *interface_name*] [**real-time**] [**dump**] [**detail**] [**trace**] [**match** *prot*] {**host** *source-ip* | *source-ip mask* | **any**}{**host** *destination-ip* | *destination-ip mask* | **any**} [*operator* **port**]

構文の説明

access-list *access_list_name*	（任意）アクセス リストと一致するトラフィックをキャプチャします。マルチ コンテキスト モードでは、1 つのコンテキスト内でのみこのコマンドを使用できます。
any	単一の IP アドレスおよびマスクではなく、任意の IP アドレスを指定します。
all	セキュリティ アプライアンスがドロップするパケットをすべてキャプチャします。
asp-drop [*drop-code*]	（任意）高速セキュリティ パスでドロップされるパケットをキャプチャします。*drop-code* は、高速セキュリティ パスでドロップされるトラフィックのタイプを指定します。ドロップ コードのリストについては、**show asp drop frame** コマンドを参照してください。*drop-code* 引数を入力しないと、ドロップされるパケットすべてがキャプチャされます。 このキーワードは、**packet-length**、**circular-buffer**、および **buffer** とともに入力できますが、**interface** または **ethernet-type** とともには入力できません。
buffer *buf_size*	（任意）パケットの保存に使用するバッファのサイズをバイト単位で定義します。このバイト数のバッファがいっぱいになると、パケット キャプチャは停止します。
capture_name	パケット キャプチャの名前を指定します。複数のタイプのトラフィックをキャプチャするには、複数の **capture** ステートメントで同じ名前を使用します。**show capture** コマンドを使用してキャプチャのコンフィギュレーションを表示すると、すべてのオプションが 1 行にまとめられます。
circular-buffer	（任意）バッファがいっぱいになったとき、バッファを先頭から上書きします。
detail	（任意）各パケットについて、プロトコル情報を追加表示します。
dump	（任意）データ リンク トランスポート経由で転送されたパケットの 16 進ダンプを表示します。
decrypted	（任意）復号化 TCP データは、L2-L4 ヘッダーでカプセル化され、キャプチャ エンジンによってキャプチャされます。
ethernet-type *type*	（任意）キャプチャするイーサネット タイプを選択します。デフォルトは IP パケットです。802.1Q タイプと VLAN タイプでは例外が発生します。802.1Q タグは自動的にスキップされ、照合には内部イーサネット タイプが使用されます。
host *ip*	パケット送信先ホストの単一の IP アドレスを指定します。

interface *interface_name*	パケット キャプチャを使用するインターフェイスの名前を設定します。キャプチャするすべてのパケットのインターフェイスを設定する必要があります。複数の **capture** コマンドで同じ名前を使用して、複数のインターフェイスを設定できます。ASA 5500 シリーズ適応型セキュリティ アプライアンスのデータプレーン上のパケットをキャプチャするには、**interface** キーワードとともにインターフェイスの名前として **asa_dataplane** を使用できます。
isakmp	（任意）ISAKMP トラフィックをキャプチャします。これは、マルチ コンテキスト モードでは使用できません。ISAKMP サブシステムは、上位層プロトコルにアクセスできません。このキャプチャは、PCAP パーサーを満たすために物理層、IP レイヤ、および UDP レイヤを組み合わせた疑似キャプチャです。このピア アドレスは、SA 交換から取得され、IP レイヤに保存されます。
mask	IP アドレスのサブネット マスク。ネットワーク マスクを指定する場合に使用する方式は、Cisco IOS ソフトウェア **access-list** コマンドの方式と異なります。このセキュリティ アプライアンスは、ネットワーク マスク（たとえば、クラス C マスクの場合は 255.255.255.0）を使用します。Cisco IOS マスクでは、ワイルドカード ビット（たとえば、0.0.0.255）が使用されます。
match *prot*	5 タプルが一致するパケットを指定し、キャプチャされるこれらのパケットのフィルタリングを許可します。1 行に最大 3 回このキーワードを使用できます。
operator	（任意）送信元または宛先で使用されるポート番号を照合します。使用できる演算子は、次のとおりです。 • **lt**：より小さい • **gt**：より大きい • **eq**：等しい
packet-length *bytes*	（任意）キャプチャ バッファに保存する各パケットの最大バイト数を設定します。
port	（任意）プロトコルを **tcp** または **udp** に設定する場合、TCP ポートまたは UDP ポートの番号（整数）か名前を指定します。
raw-data	（任意）着信パケットおよび発信パケットを 1 つ以上のインターフェイスでキャプチャします。この設定は、デフォルトです。
real-time	キャプチャしたパケットをリアルタイムで継続的に表示します。リアルタイムのパケット キャプチャを終了するには、**Ctrl+C** を押します。このオプションは、**raw-data** キャプチャおよび **asp-drop** キャプチャにだけ適用されます。
tls-proxy	（任意）1 つ以上のインターフェイスで TLS プロキシからの復号化されたインバウンド データおよびアウトバウンド データをキャプチャします。
trace *trace_count*	（任意）パケット トレース情報、およびキャプチャするパケット数をキャプチャします。これは、アクセス リストとともに使用され、トレース パケットをデータ パスに挿入して、パケットが想定どおりに処理されているかどうかを判別します。
type	（任意）キャプチャされるデータのタイプを指定します。
url *url*	（任意）データのキャプチャのために照合する URL プレフィックスを指定します。サーバへの HTTP トラフィックをキャプチャするには、URL の形式として http://*server*/*path* を使用します。サーバへの HTTPS トラフィックをキャプチャするには、https://*server*/*path* を使用します。
user *webvpn-user*	（任意）WebVPN キャプチャのユーザ名を指定します。
webvpn	（任意）特定の WebVPN 接続の WebVPN データをキャプチャします。

デフォルト

デフォルトの設定は次のとおりです。

- デフォルトの **type** は **raw-data** です。
- デフォルトの **buffer** *size* は 512 KB です。
- デフォルトのイーサネット タイプは IP です。
- デフォルトの **packet-length** は 1518 バイトです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
6.2(1)	このコマンドが導入されました。
7.0(1)	キーワード **type asp-drop**、**type isakmp**、**type raw-data**、および **type webvpn** を含むように変更されました。
7.0(8)	セキュリティ アプライアンスがドロップするパケットをすべてキャプチャするように、**all** オプションが追加されました。
7.2(1)	オプション **trace** *trace_count*、**match** *prot*、**real-time**、**host** *ip*、**any**、*mask*、および *operator* を含むように変更されました。
8.0(2)	キャプチャした内容にパスを更新するように変更されました。
8.0(4)	キーワード **type decrypted** を含むように変更されました。

使用上のガイドライン

パケット キャプチャは、接続の問題のトラブルシューティングまたは不審なアクティビティのモニタリングを行うときに役立ちます。複数のキャプチャを作成できます。パケット キャプチャを表示するには、**show capture** *name* コマンドを使用します。キャプチャをファイルに保存するには、**copy capture** コマンドを使用します。パケット キャプチャ情報を Web ブラウザで表示するには、**https://** *セキュリティ アプライアンス-ip-address*/*admin*/**capture**/*capture_name*[/**pcap**] コマンドを使用します。オプションの **pcap** キーワードを指定すると、libpcap 形式のファイルが Web ブラウザにダウンロードされ、Web ブラウザを使用してこのファイルを保存できます（libcap ファイルは、TCPDUMP または Ethereal で表示できます）。

バッファの内容を TFTP サーバに ASCII 形式でコピーする場合、パケットの詳細および 16 進ダンプは表示されず、ヘッダーだけが表示されます。詳細および 16 進ダンプを表示するには、バッファを PCAP 形式で転送し、TCPDUMP または Ethereal で読み取る必要があります。

（注） WebVPN キャプチャをイネーブルにすると、セキュリティ アプライアンスのパフォーマンスに影響します。トラブルシューティングに必要なキャプチャ ファイルを生成した後、必ずキャプチャをディセーブルにしてください。

オプションのキーワードを指定せずに **no capture** を入力すると、キャプチャが削除されます。オプションの **access-list** キーワードを指定すると、このアクセス リストがキャプチャから削除され、キャプチャは保持されます。**interface** キーワードを指定すると、指定したインターフェイスからキャプチャが分離され、キャプチャは保持されます。キャプチャ自体をクリアしない場合は、**no capture** コマンドをオプションの **access-list** キーワードまたは **interface** キーワードのいずれかを指定して入力します。

リアルタイム表示の進行中には、キャプチャに関するあらゆる操作を実行できません。低速のコンソール接続で **real-time** キーワードを使用すると、パフォーマンスが考慮されて、多数のパケットが非表示になる場合があります。バッファの固定の制限は、1000 パケットです。バッファがいっぱいになると、カウンタはキャプチャしたパケットで維持されます。別のセッションを開く場合、**no capture real-time** コマンドを入力して、リアルタイム表示をディセーブルにできます。

（注） **capture** コマンドは、コンフィギュレーションには保存されません。また、フェールオーバー時にスタンバイ ユニットにコピーされません。

例

パケットをキャプチャするには、次のコマンドを入力します。

```
hostname# capture captest interface inside
hostname# capture captest interface outside
```

Web ブラウザ上で、発行された capture コマンドの内容（「captest」という名前）は、次の場所に表示できます。

```
https://171.69.38.95/admin/capture/captest
```

libpcap ファイル（Web ブラウザが使用）をローカル マシンにダウンロードするには、次のコマンドを入力します。

```
https://171.69.38.95/capture/http/pcap
```

次に、外部ホスト 171.71.69.234 から内部 HTTP サーバにトラフィックがキャプチャされる例を示します。

```
hostname# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
hostname# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
hostname# capture http access-list http packet-length 74 interface inside
```

次に、ARP パケットをキャプチャする例を示します。

```
hostname# capture arp ethernet-type arp interface outside
```

次に、5 つのトレース パケットをデータ ストリームに挿入する例を示します。ここで、*access-list 101* は、TCP プロトコル FTP と一致するトラフィックを定義します。

```
hostname# capture ftptrace interface outside access-list 101 trace 5
```

トレースされたパケットおよびパケット処理に関する情報をわかりやすく表示するには、**show capture ftptrace** コマンドを使用します。

次に、キャプチャしたパケットをリアルタイムで表示する例を示します。

```
hostname# capture test interface outside real-time
Warning: Using this option with a slow console connection may result in an excess amount
of non-displayed packets due to performance limitations.
Use ctrl-c to terminate real-time capture.

10 packets displayed
12 packets not displayed due to performance limitations
```

関連コマンド

コマンド	説明
clear capture	キャプチャ バッファをクリアします。
copy capture	キャプチャ ファイルをサーバにコピーします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

cd

現在の作業ディレクトリから指定したディレクトリに変更するには、特権 EXEC モードで **cd** コマンドを使用します。

cd [**disk0: | disk1: | flash:**] [*path*]

構文の説明

disk0*:*	内部フラッシュ メモリを指定し、続けてコロンを入力します。
disk1:	取り外し可能な外部フラッシュ メモリ カードを指定し、続けてコロンを入力します。
flash:	内部フラッシュ メモリを指定し、続けてコロンを入力します。ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。
path	（任意）移動先ディレクトリの絶対パス。

デフォルト

ディレクトリを指定しないと、ルート ディレクトリに移動します。

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
特権 EXEC	•	•	•	—	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、「config」ディレクトリに移動する例を示します。

```
hostname# cd flash:/config/
```

関連コマンド

コマンド	説明
pwd	現在の作業ディレクトリを表示します。

cdp-url

ローカル CA によって発行された証明書に含める CDP を指定するには、CA サーバ コンフィギュレーション モードで **cdp-url** コマンドを使用します。デフォルトの CDP に戻すには、このコマンドの **no** 形式を使用します。

[no] cdp-url *url*

構文の説明

url	ローカル CA によって発行された証明書の失効ステータスを検証側が取得する URL を指定します。URL は、英数字 500 文字未満である必要があります。

デフォルト

デフォルトの CDP URL は、ローカル CA が含まれるセキュリティ アプライアンスの CDP URL です。デフォルトの URL の形式は、http://hostname.domain/+CSCOCA+/asa_ca.crl です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

CDP は、発行された証明書に含めることができる拡張であり、証明書の失効ステータスを検証側が取得できる場所を指定できます。一度に設定できる CDP は 1 つだけです。

（注） CDP URL が指定された場合、管理者はその場所から現在の CRL にアクセスできるように管理する必要があります。

例

次に、ローカル CA サーバが発行した証明書に対して、10.10.10.12 の CDP を設定する例を示します。

```
hostname(config)# crypto ca server
hostname(config-ca-server)# cdp-url http://10.10.10.12/ca/crl
hostname(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードの CLI コマンド セットにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	証明書データベースおよび CRL で、ローカル CA サーバによって発行された証明書を失効とマークします。
crypto ca server unrevoke	ローカル CA サーバによって発行され、以前に失効した証明書の失効を取り消します。
lifetime crl	証明書失効リストのライフタイムを指定します。

certificate

指定した証明書を追加するには、クリプト CA 証明書チェーン コンフィギュレーション モードで **certificate** コマンドを使用します。このコマンドを発行する場合、セキュリティ アプライアンスは、コマンドに含まれているデータを 16 進形式の証明書として解釈します。**quit** ストリングは、証明書の末尾を示します。証明書を削除するには、このコマンドの **no** 形式を使用します。

certificate [**ca** | **ra-encrypt** | **ra-sign** | **ra-general**] *certificate-serial-number*

no certificate *certificate-serial-number*

構文の説明

certificate-serial-number	証明書のシリアル番号を quit で終わる 16 進形式で指定します。
ca	証明書が CA 発行の証明書であることを示します。
ra-encrypt	証明書が SCEP で使用される RA キー暗号化証明書であることを示します。
ra-general	証明書が SCEP メッセージングのデジタル署名およびキー暗号化に使用される RA 証明書であることを示します。
ra-sign	証明書が SCEP メッセージングで使用される RA デジタル署名証明書であることを示します。

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
クリプト CA 証明書チェーン コンフィギュレーション	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(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

CA は、メッセージ暗号化のためのセキュリティ クレデンシャルおよび公開キーの発行および管理を行うネットワーク内の組織です。公開キー インフラストラクチャの一部である CA では、RA と連携して、デジタル証明書の要求者から取得した情報を確認します。RA が要求者の情報を確認すると、CA から証明書が発行されます。

例

次に、シリアル番号 29573D5FF010FE25B45 の CA 証明書を追加する例を示します。

```
hostname(config)# crypto ca trustpoint central
hostname(ca-trustpoint)# crypto ca certificate chain central
hostname(ca-cert-chain)# certificate ca 29573D5FF010FE25B45
  30820345 308202EF A0030201 02021029 572A3FF2 96EF854F D0D6732F E25B4530
```

```
0D06092A 864886F7 0D010105 05003081 8F311630 1406092A 864886F7 0D010901
16076140 622E636F 6D310B30 09060355 04061302 55533116 30140603 55040813
0D6D6173 73616368 75736574 74733111 300F0603 55040713 08667261 6E6B6C69
6E310E30 0C060355 040A1305 63697363 6F310F30 0D060355 040B1306 726F6F74
6F75311C 301A0603 55040313 136D732D 726F6F74 2D736861 2D30362D 32303031
301E170D 30313036 32363134 31313430 5A170D32 32303630 34313430 3133305A
30818F31 16301406 092A8648 86F70D01 09011607 6140622E 636F6D31 0B300906
03550406 13025553 31163014 06035504 08130D6D 61737361 63687573 65747473
3111300F 06035504 07130866 72616E6B 6C696E31 0E300C06 0355040A 13056369
73636F31 0F300D06 0355040B 1306726F 6F746F75 311C301A 06035504 0313136D
732D726F 6F742D73 68612D30 362D3230 3031305C 300D0609 2A864886 F70D0101
01050003 4B003048 024100AA 3EB9859B 8670A6FB 5E7D2223 5C11BCFE 48E6D3A8
181643ED CF7E75EE E77D83DF 26E51876 97D8281E 9F58E4B0 353FDA41 29FC791B
1E14219C 847D19F4 A51B7B02 03010001 A3820123 3082011F 300B0603 551D0F04
04030201 C6300F06 03551D13 0101FF04 05300301 01FF301D 0603551D 0E041604
14E0D412 3ACC96C2 FBF651F3 3F66C0CE A62AB63B 323081CD 0603551D 1F0481C5
3081C230 3EA03CA0 3A86386C 6461703A 2F2F7732 6B616476 616E6365 64737276
2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
63726C30 3EA03CA0 3A863868 7474703A 2F2F7732 6B616476 616E6365 64737276
2F436572 74456E72 6F6C6C2F 6D732D72 6F6F742D 7368612D 30362D32 3030312E
63726C30 40A03EA0 3C863A66 696C653A 2F2F5C5C 77326B61 6476616E 63656473
72765C43 65727445 6E726F6C 6C5C6D73 2D726F6F 742D7368 612D3036 2D323030
312E6372 6C301006 092B0601 04018237 15010403 02010130 0D06092A 864886F7
0D010105 05000341 0056221E 03F377B9 E6900BF7 BCB3568E ADBA146F 3B8A71F3
DF9EB96C BB1873B2 B6268B7C 0229D8D0 FFB40433 C8B3CB41 0E4D212B 2AEECD77
BEA3C1FE 5EE2AB6D 91
quit
```

関連コマンド

コマンド	説明
clear configure crypto map	すべてのクリプト マップのすべてのコンフィギュレーションをクリアします。
show running-config crypto map	クリプト マップの設定内容を表示します。
crypto ca certificate chain	証明書クリプト CA 証明書チェーン モードを開始します。
crypto ca trustpoint	CA トラストポイント モードを開始します。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。

certificate-group-map

証明書マップのルール エントリをトンネル グループに関連付けるには、webvpn コンフィギュレーション モードで **certificate-group-map** コマンドを使用します。現在のトンネル グループ マップの関連付けをクリアするには、このコマンドの **no** 形式を使用します。

certificate-group-map *certificate_map_name index tunnel_group_name*

no certificate-group-map

構文の説明

certificate_map_name	証明書マップの名前。
index	証明書マップのマップ エントリの数値識別子。index の値の範囲は、1 ～ 65535 です。
tunnel_group_name	マップ エントリが証明書と一致する場合に選択されるトンネル グループの名前。*tunnel-group name* はすでに存在している必要があります。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが導入されました。

使用上のガイドライン

certificate-group-map コマンドが有効な状態で、WebVPN クライアントから受信した証明書がマップ エントリに対応する場合、結果として得られるトンネル グループは、接続に関連付けられ、ユーザが選択したトンネル グループを上書きします。

certificate-group-map コマンドの複数のインスタンスを使用すると、複数のマッピングが可能です。

例

次に、tgl という名前のトンネル グループにルール 6 を関連付ける例を示します。

```
hostname(config)# webvpn

hostname(config-webvpn)# certificate-group-map map1 6 tg1
hostname(config-webvpn)#
```

関連コマンド

コマンド	説明
crypto ca certificate map	証明書の発行者名とサブジェクト Distinguished Name（DN; 認定者名）に基づいて、ルールを設定するために CA 証明書マップ コンフィギュレーション モードを開始します。
tunnel-group-map	証明書ベースの IKE セッションをトンネル グループにマップするときのポリシーおよびルールを設定します。

chain

証明書チェーンの送信をイネーブルにするには、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 **chain** コマンドを使用します。このアクションには、ルート証明書および送信内のすべての下位 CA 証明書が含まれます。このコマンド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。

chain

no chain

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

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
トンネル グループ ipsec 属性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 グループ ipsec 属性コンフィギュレーション モードを開始し、IPSec LAN-to-LAN トンネル グループのチェーンを IP アドレス 209.165.200.225 で送信することをイネーブルにする例を示します。このアクションには、ルート証明書およびすべての下位 CA 証明書が含まれます。

```
hostname(config)# tunnel-group 209.165.200.225 type IPSec_L2L
hostname(config)# tunnel-group 209.165.200.225 ipsec-attributes
hostname(config-tunnel-ipsec)# chain
hostname(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	現在のトンネル 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。

changeto

セキュリティ コンテキストとシステムの間で切り替えを行うには、特権 EXEC モードで **changeto** コマンドを使用します。

changeto {**system** | **context** *name*}

構文の説明

context *name*	指定した名前のコンテキストに切り替えます。
system	システム実行スペースに切り替えます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

システム実行スペースまたは管理コンテキストにログインしている場合、コンテキスト間で切り替えを行うことができ、各コンテキスト内でコンフィギュレーションおよびタスクのモニタリングを実行できます。コンフィギュレーション モードでの編集または **copy** コマンドあるいは **write** コマンドで使用される「実行」コンフィギュレーションは、ログインしている実行スペースによって異なります。システム実行スペースにログインしている場合、実行コンフィギュレーションは、システム コンフィギュレーションのみで構成されます。コンテキスト実行スペースにログインしている場合、実行コンフィギュレーションは、このコンテキストのみで構成されます。たとえば、**show running-config** コマンドを入力しても、すべての実行コンフィギュレーション（システムおよびすべてのコンテキスト）を表示することはできません。現在のコンフィギュレーションだけが表示されます。

例

次に、特権 EXEC モードでコンテキストとシステムの間で切り替えを行う例を示します。

```
hostname/admin# changeto system
hostname# changeto context customerA
hostname/customerA#
```

次に、インターフェイス コンフィギュレーション モードでシステムと管理コンテキストの間で切り替えを行う例を示します。実行スペース間で切り替えを行うときにコンフィギュレーション サブモードにログインしている場合、新しい実行スペースのグローバル コンフィギュレーション モードに変更されます。

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

関連コマンド

コマンド	説明
admin-context	コンテキストを管理コンテキストに設定します。
context	システム コンフィギュレーションにセキュリティ コンテキストを作成し、コンテキスト コンフィギュレーション モードを開始します。
show context	コンテキストのリスト（システム実行スペース）または現在のコンテキストに関する情報を表示します。

character-encoding

WebVPN ポータル ページでグローバルな文字エンコーディングを指定するには、webvpn コンフィギュレーション モードで **character-encoding** コマンドを使用します。character-encoding 属性の値を削除するには、このコマンドの **no** 形式を使用します。

character-encoding *charset*

no character-encoding [*charset*]

構文の説明

charset	最大 40 文字から成るストリングで、http://www.iana.org/assignments/character-sets で特定されている有効な文字セットのいずれかに相当するもの。このページに示されている文字セットの名前またはエイリアスのいずれかを使用できます。たとえば、iso-8859-1、shift_jis、ibm850 などです。 このストリングは、大文字と小文字が区別されません。セキュリティ アプライアンス コンフィギュレーション内では、コマンド インタプリタによって大文字が小文字に変換されます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

文字エンコーディング（「文字コーディング」または「文字セット」とも呼ばれます）は、raw データ（0 と 1 からなるデータなど）と文字をペアにすることで、データを表します。使用する文字エンコード方式は、言語によって決まります。ある言語では同じ方式を使用していても、別の言語でも同じとはかぎりません。通常、ブラウザで使用されるデフォルトのエンコーディング方式は地域によって決まりますが、ユーザはこの方式を変更できます。ブラウザはページに指定されたエンコードを検出することもでき、そのエンコードに従ってドキュメントを表示します。character-encoding 属性を使用すると、ユーザは、文字エンコーディング方式の値を WebVPN ポータル ページに指定し、ブラウザを使用している地域やブラウザに対して行われたあらゆる変更に関係なく、ブラウザでこのページを適切に処理できます。

character-encoding 属性は、デフォルトでは、すべての WebVPN ポータル ページに継承されるグローバルな設定です。ただし、ユーザは、character-encoding 属性の値と異なる文字エンコーディングを使用する Common Internet File System サーバの file-encoding 属性を上書きできます。異なる文字エンコーディングが必要な CIFS サーバには異なるファイル エンコーディング値を使用します。

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

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

（注） character-encoding の値および file-encoding の値は、ブラウザによって使用されるフォント ファミリを排除するものではありません。Shift_JIS 文字エンコーディングを使用している場合、次の例に示すように webvpn カスタマイゼーション コマンド モードで **page style** コマンドを使用して、これらの値の 1 つの設定を補完して、フォント ファミリを置き換える必要があります。あるいは、webvpn カスタマイゼーション コマンド モードで **no page style** コマンドを入力して、このフォント ファミリを削除する必要があります。

この属性に値が含まれていない場合、WebVPN ポータル ページの文字セットは、リモート ブラウザに設定されているエンコーディング タイプによって決まります。

例

次に、日本語 Shift_JIS 文字をサポートする character-encoding 属性を設定し、フォント ファミリを削除し、デフォルトの背景色を保持する例を示します。

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

関連コマンド

コマンド	説明
file-encoding	CIFS サーバおよび関連する文字エンコーディングを指定し、この属性の値を上書きします。
show running-config [all] webvpn	WebVPN の実行コンフィギュレーションを表示します。デフォルト コンフィギュレーションを組み込むには **all** キーワードを使用します。
debug webvpn cifs	CIFS に関するデバッグ メッセージを表示します。

checkheaps

checkheaps 検証の間隔を設定するには、グローバル コンフィギュレーション モードで **checkheaps** コマンドを使用します。この値をデフォルトに設定するには、このコマンドの **no** 形式を使用します。チェックヒープは、ヒープ メモリ バッファの正常性およびコード領域の完全性を検証する定期的なプロセスです（ダイナミック メモリはシステム ヒープ メモリ領域から割り当てられます）。

checkheaps {check-interval | validate-checksum} *seconds*

no checkheaps {check-interval | validate-checksum} [*seconds*]

構文の説明

check-interval	バッファ検証の間隔を設定します。バッファ検証プロセスでは、ヒープ（割り当てられ、解放されたメモリ バッファ）の健全性がチェックされます。このプロセスの各呼び出しの間、セキュリティ アプライアンスはヒープ全体をチェックし、各メモリ バッファを検証します。不一致がある場合、セキュリティ アプライアンスは、「バッファ割り当てエラー」または「バッファ解放エラー」を発行します。エラーがある場合、セキュリティ アプライアンスは可能であればトレースバック情報をダンプし、リロードします。
validate-checksum	コード スペースのチェックサム検証間隔を設定します。最初にセキュリティ アプライアンスを起動するときに、セキュリティ アプライアンスはコード全体のハッシュを計算します。その後、セキュリティ アプライアンスは、定期チェックの間に新しいハッシュを生成し、元のハッシュと比較します。不一致がある場合、セキュリティ アプライアンスは「テキスト チェックサム checkheaps エラー」を発行します。エラーがある場合、セキュリティ アプライアンスは可能であればトレースバック情報をダンプし、リロードします。
seconds	1 ～ 2147483 の間隔を秒単位で設定します。

デフォルト

デフォルトの間隔はそれぞれ 60 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

例

次に、バッファ割り当て間隔を 200 秒、コード スペースのチェックサムの間隔を 500 秒に設定する例を示します。

```
hostname(config)# checkheaps check-interval 200
```

```
hostname(config)# checkheaps validate-checksum 500
```

関連コマンド

コマンド	説明
show checkheaps	checkheaps 統計情報を表示します。

check-retransmission

TCP 再送信スタイルの攻撃を防止するには、tcp マップ コンフィギュレーション モードで **check-retransmission** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

check-retransmission

no check-retransmission

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
TCP マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。矛盾する再送信をエンド システムが解釈する際に生じる TCP 再送信スタイルの攻撃を防止するには、tcp マップ コンフィギュレーション モードで **check-retransmission** コマンドを使用します。

セキュリティ アプライアンスは、再送信のデータが元のデータと同じかどうかを確認しようとします。データが一致しない場合、接続がセキュリティ アプライアンスによってドロップされます。この機能がイネーブルの場合、TCP 接続上のパケットは順序どおりにのみ許可されます。詳細については、**queue-limit** コマンドを参照してください。

例

次に、すべての TCP フローで TCP チェック再送信機能をイネーブルにする例を示します。

```
hostname(config)# access-list TCP extended permit tcp any any
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# check-retransmission
hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP
```

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

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンドの構文ヘルプを表示します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

checksum-verification

TCP チェックサムの検証をイネーブルまたはディセーブルにするには、tcp マップ コンフィギュレーション モードで **checksum-verification** コマンドを使用します。この指定を削除するには、このコマンドの **no** 形式を使用します。

checksum-verification

no checksum-verification

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

チェックサムの検証は、デフォルトでディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。tcp マップ コンフィギュレーション モードで **checksum-verification** コマンドを使用して、TCP チェックサムの検証をイネーブルにします。このチェックに失敗すると、パケットはドロップされます。

例

次に、10.0.0.0 ～ 20.0.0.0 の TCP 接続で TCP チェックサムの検証をイネーブルにする例を示します。

```
hostname(config)# access-list TCP1 extended permit tcp 10.0.0.0 255.0.0.0 20.0.0.0
255.0.0.0
hostname(config)# tcp-map tmap
hostname(config-tcp-map)# checksum-verification

hostname(config)# class-map cmap
hostname(config-cmap)# match access-list TCP1

hostname(config)# policy-map pmap
hostname(config-pmap)# class cmap
```

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

hostname(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
help	**policy-map** コマンド、**class** コマンド、および **description** コマンドの構文ヘルプを表示します。
policy-map	ポリシーを設定します。これは、1 つのトラフィック クラスと 1 つ以上のアクションのアソシエーションです。
set connection	接続値を設定します。
tcp-map	TCP マップを作成して、TCP マップ コンフィギュレーション モードにアクセスできるようにします。

cipc security-mode authenticated

Cisco IP Communicator（CIPC）Softphone を音声 VLAN シナリオまたはデータ VLAN シナリオに導入する場合に、強制的に CIPC Softphone を認証済みモードで動作させるには、電話プロキシ コンフィギュレーション モードで **cipc security-mode authenticated** コマンドを使用します。

CIPC Softphone が暗号化をサポートしている場合に、このコマンドをオフにするには、このコマンドの **no** 形式を使用します。

cipc security-mode authenticated

no cipc security-mode authenticated

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、このコマンドは、no 形式によって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
Phone-Proxy 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(4)	このコマンドが追加されました。

使用上のガイドライン

データ VLAN に影響を及ぼそうとするセキュリティ上の脅威から音声ストリームを守るために、複数の VLAN を使用して音声とデータのトラフィックを分離することがセキュリティ上のベスト プラクティスです。ただし、Cisco IP Communicator（CIPC）Softphone アプリケーションは、それぞれの IP Phone に接続する必要があります。IP Phone は、音声 VLAN に常駐しています。この要件により、音声 VLAN とデータ VLAN を分離することが問題になります。これは、SIP プロトコルおよび SCCP プロトコルが広範囲のポートで RTP ポートおよび RTCP ポートをダイナミックにネゴシエートするためです。このダイナミック ネゴシエーションでは、特定の範囲のポートを 2 つの VLAN の間で開く必要があります。

（注） 認証済みモードをサポートしていない旧バージョンの CIPC は、電話プロキシではサポートされていません。

データ VLAN と音声 VLAN の間でのアクセスを広範囲のポートで行わずに、データ VLAN 上の CIPC Softphone を音声 VLAN 上の該当する IP Phone と接続するには、**cipc security-mode authenticated** コマンドを使用して電話プロキシを設定します。

このコマンドを使用すると、電話プロキシが CIPC コンフィギュレーション ファイルを参照し、CIPC Softphone が強制的に（暗号化済みモードではなく）認証済みモードになります。これは、現在のバージョンの CIPC が暗号化済みモードをサポートしていないためです。

このコマンドがイネーブルの場合、電話プロキシは、電話コンフィギュレーション ファイルを解析し、電話が CIPC Softphone かどうかを判別し、セキュリティ モードを認証済みに変更します。またデフォルトでは、電話プロキシがすべての電話を強制的に暗号化済みモードにしている間だけ、CIPC Softphone は認証済みモードをサポートします。

例

次に、**cipc security-mode authenticated** コマンドを使用して、音声 VLAN シナリオまたはデータ VLAN シナリオに Cisco IP Communicator（CIPC）Softphone を導入するときに CIPC Softphone を強制的に認証済みモードで動作させる例を示します。

```
hostname(config)# phone-proxy asa_phone_proxy
hostname(config-phone-proxy)#cipc security-mode authenticated
```

関連コマンド

コマンド	説明
phone-proxy	Phone Proxy インスタンスを設定します。

class（グローバル）

セキュリティ コンテキストの割り当て先のリソース クラスを作成するには、グローバル コンフィギュレーション モードで **class** コマンドを使用します。クラスを削除するには、このコマンドの **no** 形式を使用します。

class *name*

no class *name*

構文の説明

name	20 文字までの文字列で名前を指定します。デフォルト クラスに関する制限を設定するには、**default** という名前を入力します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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

デフォルトでは、コンテキストごとの上限値が適用されていない限り、すべてのセキュリティ コンテキストがセキュリティ アプライアンスのリソースに無制限にアクセスできます。ただし、1 つ以上のコンテキストがリソースを大量に使用しており、他のコンテキストが接続を拒否されている場合は、リソース管理を設定してコンテキストごとのリソースの使用を制限できます。

セキュリティ アプライアンスでは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

クラスを作成すると、セキュリティ アプライアンスは、クラスに割り当てられる各コンテキストに対してリソースの一部を確保しなくなります。その代わりに、セキュリティ アプライアンスは、コンテキストの上限を設定します。リソースをオーバーサブスクライブする場合、または一部のリソースを無制限にする場合は、少数のコンテキストがこれらのリソースを「使い果たし」、他のコンテキストへのサービスに影響する可能性があります。クラス用のリソースを設定するには、**limit-resource** コマンドを参照してください。

すべてのコンテキストは、別のクラスに割り当てられていない場合はデフォルト クラスに属します。コンテキストをデフォルト クラスに積極的に割り当てる必要はありません。

コンテキストがデフォルト クラス以外のクラスに属する場合、それらのクラス設定は常にデフォルト クラス設定を上書きします。ただし、他のクラスに定義されていない設定がある場合、メンバ コンテキストはそれらの制限にデフォルト クラスを使用します。たとえば、すべての同時接続に 2% の制限

を設定したがその他の制限を設定せずにクラスを作成した場合、他のすべての制限はデフォルト クラスから継承されます。逆に、すべてのリソースに対する制限を設定してクラスを作成した場合、そのクラスはデフォルト クラスの設定を使用しません。

デフォルトでは、デフォルト クラスは、すべてのコンテキストにリソースへのアクセスを無制限に提供します。ただし、次の制限が適用されます（この制限は、デフォルトではコンテキストあたりの最大許容値が設定されます）。

- Telnet セッション：5 セッション。
- SSH セッション：5 セッション。
- MAC アドレス：65,535 エントリ。

例

次に、接続のデフォルト クラスの制限に、無制限ではなく 10 % を設定する例を示します。

```
hostname(config)# class default
hostname(config-class)# limit-resource conns 10%
```

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

```
hostname(config)# class gold
hostname(config-class)# limit-resource mac-addresses 10000
hostname(config-class)# limit-resource conns 15%
hostname(config-class)# limit-resource rate conns 1000
hostname(config-class)# limit-resource rate inspects 500
hostname(config-class)# limit-resource hosts 9000
hostname(config-class)# limit-resource asdm 5
hostname(config-class)# limit-resource ssh 5
hostname(config-class)# limit-resource rate syslogs 5000
hostname(config-class)# limit-resource telnet 5
hostname(config-class)# limit-resource xlates 36000
```

関連コマンド

コマンド	説明
clear configure class	クラス コンフィギュレーションをクリアします。
context	セキュリティ コンテキストを設定します。
limit-resource	クラスのリソース制限を設定します。
member	コンテキストをリソース クラスに割り当てます。
show class	クラスに割り当てられているコンテキストを表示します。

class（ポリシー マップ）

クラス マップ トラフィックにアクションを割り当てることができるポリシー マップにクラス マップを割り当てるには、ポリシー マップ コンフィギュレーション モードで **class** コマンドを使用します。ポリシー マップからクラス マップを削除するには、このコマンドの **no** 形式を使用します。

class *classmap_name*

no class *classmap_name*

構文の説明

classmap_name	クラス マップの名前を指定します。レイヤ 3/4 ポリシー マップ（**policy-map** コマンド）の場合、レイヤ 3/4 クラス マップ名（**class-map** コマンドまたは **class-map type management** コマンド）を指定する必要があります。インスペクション ポリシー マップ（**policy-map type inspect** コマンド）の場合、インスペクション クラス マップ名（**class-map type inspect** コマンド）を指定する必要があります。

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
ポリシー マップ コンフィギュレーション	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

class コマンドを使用するには、Modular Policy Framework を使用します。レイヤ 3/4 ポリシー マップでクラスを使用するには、次のコマンドを入力します。

1. **class-map**：アクションを実行するトラフィックを識別します。
2. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するクラス マップを指定します。
   b. *commands for supported features*：特定のクラス マップについて、QoS、アプリケーション インスペクション、CSC または AIP SSM、TCP 接続と UDP 接続の制限とタイムアウト、TCP 正規化など、さまざまな機能の多数のアクションを設定できます。各機能で使用可能なコマンドの詳細については、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。
3. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

インスペクション ポリシー マップでクラスを使用するには、次のコマンドを入力します。

1. **class-map type inspect**：アクションを実行するトラフィックを指定します。

2. **policy-map type inspect**：各クラス マップに関連付けられているアクションを指定します。
   a. **class**：アクションを実行するインスペクション クラス マップを指定します。
   b. *アプリケーション タイプのコマンド*: 各アプリケーション タイプで使用可能なコマンドについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。インスペクション ポリシー マップのクラス コンフィギュレーション モードでサポートされているアクションには、次のものが含まれます。
   - パケットのドロップ
   - 接続のドロップ
   - 接続のリセット
   - ロギング
   - メッセージのレートの制限
   - コンテンツのマスキング

   c. **parameters**：インスペクション エンジンに影響を及ぼすパラメータを設定します。CLI はパラメータ コンフィギュレーション モードに移行します。使用可能なコマンドについては、『*Cisco ASA 5500 Series Configuration Guide using the CLI*』を参照してください。
3. **class-map**：アクションを実行するトラフィックを識別します。
4. **policy-map**：各クラス マップに関連付けるアクションを指定します。
   a. **class**：アクションを実行するレイヤ 3/4 クラス マップを指定します。
   b. **inspect** *application inspect_policy_map*：アプリケーション インスペクションをイネーブルにし、特別なアクションを実行するインスペクション ポリシー マップを呼び出します。
5. **service-policy**：ポリシー マップをインターフェイスごとに、またはグローバルに割り当てます。

このコンフィギュレーションには、すべてのトラフィックと一致する、**class-default** と呼ばれるクラス マップが必ず含まれています。各レイヤ 3/4 ポリシー マップの末尾には、アクションが定義されていない **class-default** クラス マップがコンフィギュレーションに含まれています。すべてのトラフィックと照合するが、別のクラス マップを作成しない場合、このクラス マップをオプションで使用できます。実際、一部の機能は、**class-default** クラス マップ用にのみ設定できます（**shape** コマンドなど）。

class-default クラス マップを含めて、最大 63 個の **class** コマンドおよび **match** コマンドをポリシー マップに設定できます。

例

次に、**class** コマンドを含む、接続ポリシーの **policy-map** コマンドの例を示します。このコマンドは、Web サーバ 10.1.1.1 への接続許可数を制限します。

```
hostname(config)# access-list http-server permit tcp any host 10.1.1.1
hostname(config)# class-map http-server
hostname(config-cmap)# match access-list http-server

hostname(config)# policy-map global-policy
hostname(config-pmap)# description This policy map defines a policy concerning connection
to http server.
hostname(config-pmap)# class http-server
hostname(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
hostname(config)# class-map inspection_default
hostname(config-cmap)# match default-inspection-traffic
hostname(config)# class-map http_traffic
hostname(config-cmap)# match port tcp eq 80
```

```
hostname(config)# policy-map outside_policy
hostname(config-pmap)# class inspection_default
hostname(config-pmap-c)# inspect http http_map
hostname(config-pmap-c)# inspect sip
hostname(config-pmap)# class http_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:10:0
```

次の例は、トラフィックが最初の利用可能なクラス マップと一致した場合に、同じ機能ドメインのアクションが指定されている後続のクラス マップと照合されないことを示しています。

```
hostname(config)# class-map telnet_traffic
hostname(config-cmap)# match port tcp eq 23
hostname(config)# class-map ftp_traffic
hostname(config-cmap)# match port tcp eq 21
hostname(config)# class-map tcp_traffic
hostname(config-cmap)# match port tcp range 1 65535
hostname(config)# class-map udp_traffic
hostname(config-cmap)# match port udp range 0 65535
hostname(config)# policy-map global_policy
hostname(config-pmap)# class telnet_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:0:0
hostname(config-pmap-c)# set connection conn-max 100
hostname(config-pmap)# class ftp_traffic
hostname(config-pmap-c)# set connection timeout tcp 0:5:0
hostname(config-pmap-c)# set connection conn-max 50
hostname(config-pmap)# class tcp_traffic
hostname(config-pmap-c)# set connection timeout tcp 2:0:0
hostname(config-pmap-c)# set connection conn-max 2000
```

Telnet 接続は、開始時に **class telnet_traffic** と一致します。同様に FTP 接続は、開始時に **class ftp_traffic** と一致します。Telnet および FTP 以外の TCP 接続の場合は、**class tcp_traffic** と一致します。Telnet 接続または FTP 接続は **class tcp_traffic** と一致しますが、すでに他のクラスと一致しているため、セキュリティ アプライアンスはこの照合を行いません。

関連コマンド

コマンド	説明
class-map	レイヤ 3/4 のクラス マップを作成します。
class-map type management	管理トラフィック用のレイヤ 3/4 クラス マップを作成します。
clear configure policy-map	service-policy コマンドで使用中のポリシー マップを除く、すべてのポリシー マップ コンフィギュレーションを削除します。
match	トラフィック照合パラメータを定義します。
policy-map	ポリシー（それぞれが 1 つ以上のアクションを持つ 1 つ以上のトラフィック クラスの関連付け）を設定します。

class-map

モジュラ ポリシー フレームワークを使用するとき、グローバル コンフィギュレーション モードで **class-map** コマンド（**type** キーワードは指定しない）を使用して、アクションを適用するレイヤ 3 またはレイヤ 4 のトラフィックを指定します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map *class_map_name*

no class-map *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。「class-default」という名前および「_internal」または「_default」で始まる任意の名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

このタイプのクラス マップは、レイヤ 3/4 通過トラフィック専用です。セキュリティ アプライアンス宛ての管理トラフィックについては、**class-map type management** コマンドを参照してください。

レイヤ 3/4 クラス マップにより、アクションを適用するレイヤ 3 および 4 のトラフィックを特定します。1 つのレイヤ 3/4 ポリシー マップに複数のレイヤ 3/4 クラス マップを作成できます。

デフォルトのクラス マップ

コンフィギュレーションには、デフォルト グローバル ポリシーでセキュリティ アプライアンスが使用するデフォルトのレイヤ 3/4 クラス マップが含まれます。これは、**inspection_default** と呼ばれ、デフォルト インスペクション トラフィックと一致します。

```
class-map inspection_default
 match default-inspection-traffic
```

デフォルトのコンフィギュレーションに存在する別のクラス マップは、class-default と呼ばれ、これはすべてのトラフィックと一致します。

```
class-map class-default
 match any
```

このクラス マップは、すべてのレイヤ 3/4 ポリシー マップの最後に表示され、原則的に、他のすべてのトラフィックでどんなアクションも実行しないようにセキュリティ アプライアンスに通知します。独自の **match any** クラス マップを作成するのではなく、必要に応じて class-default クラス マップを使用できます。実際のところ、class-default で使用可能な機能は、QoS トラフィック シェーピングなどの一部の機能だけです。

最大クラス マップ

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。

設定の概要

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドまたは **class-map type management** コマンドを使用して、アクションの適用対象となるレイヤ 3 と 4 のトラフィックを指定します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

class-map コマンドを使用して、クラス マップ コンフィギュレーション モードを開始します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。レイヤ 3/4 クラス マップには、クラス マップに含まれているトラフィックを指定する、**match** コマンド（**match tunnel-group** コマンドおよび **match default-inspection-traffic** コマンドを除く）が 1 つだけ含まれています。

例

次に、4 つのレイヤ 3/4 クラス マップを作成する例を示します。

```
hostname(config)# access-list udp permit udp any any
hostname(config)# access-list tcp permit tcp any any
hostname(config)# access-list host_foo permit ip any 10.1.1.1 255.255.255.255

hostname(config)# class-map all_udp
hostname(config-cmap)# description "This class-map matches all UDP traffic"
hostname(config-cmap)# match access-list udp

hostname(config-cmap)# class-map all_tcp
hostname(config-cmap)# description "This class-map matches all TCP traffic"
hostname(config-cmap)# match access-list tcp
```

```
hostname(config-cmap)# class-map all_http
hostname(config-cmap)# description "This class-map matches all HTTP traffic"
hostname(config-cmap)# match port tcp eq http

hostname(config-cmap)# class-map to_server
hostname(config-cmap)# description "This class-map matches all traffic to server 10.1.1.1"
hostname(config-cmap)# match access-list host_foo
```

関連コマンド

コマンド	説明
class-map type management	セキュリティ アプライアンスへのトラフィック用のクラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type inspect

モジュラ ポリシー フレームワーク を使用するときに、グローバル コンフィギュレーション モードで **class-map type inspect** コマンドを使用して検査アプリケーションに固有の基準と一致を確認します。インスペクション クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type inspect *application* [**match-all** | **match-any]** *class_map_name*

no class-map [**type inspect** *application* [**match-all** | **match-any**]] *class_map_name*

構文の説明

application	照合するアプリケーション トラフィックのタイプを指定します。利用可能なタイプは次のとおりです。 • **dns** • **ftp** • **h323** • **http** • **im** • **sip**
class_map_name	40 文字までの長さのクラス マップ名を指定します。「class-default」という名前および「_internal」または「_default」で始まる任意の名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。
match-all	（任意）トラフィックがクラス マップと一致するには、すべての基準と一致する必要があることを指定します。オプションを指定しない場合、**match-all** がデフォルトです。
match-any	（任意）トラフィックがクラス マップと一致するには、1 つ以上の基準と一致する必要があることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが導入されました。
8.0(2)	**match-any** キーワードが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 ポリシー マップでインスペクション エンジンをイネーブルにするときは、*インスペクション ポリシー マップ*で定義されているアクションを必要に応じてイネーブルにすることもできます（**policy-map type inspect** コマンドを参照）。

インスペクション ポリシー マップでは、インスペクション クラス マップを作成して、対象とするトラフィックを指定できます。このクラス マップには、1 つ以上の **match** コマンドが含まれます （あるいは、単一の基準とアクションをペアにする場合は、インスペクション ポリシー マップで **match** コマンドを直接使用できます）。アプリケーション固有の基準を照合できます。たとえば DNS トラフィックの場合は、DNS クエリー内のドメイン名と照合可能です。

クラス マップは、複数のトラフィック照合をグループ化します（match-all クラス マップ）。あるいはクラス マップで、照合リストのいずれかを照合できます（match-any クラス マップ）。クラス マップを作成することと、インスペクション ポリシー マップ内で直接トラフィック照合を定義することの違いは、クラス マップを使用して複数の match コマンドをグループ化できる点と、クラス マップを再使用できる点です。このクラス マップで指定するトラフィックに対しては、インスペクション ポリシー マップで、接続のドロップ、リセット、またはロギングなどのアクションを指定できます。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次の例では、すべての基準に一致する必要がある HTTP クラス マップを作成します。

```
hostname(config-cmap)# class-map type inspect http match-all http-traffic
hostname(config-cmap)# match req-resp content-type mismatch
hostname(config-cmap)# match request body length gt 1000
hostname(config-cmap)# match not request uri regex class URLs
```

次の例では、基準のいずれかに一致する必要がある HTTP クラス マップを作成します。

```
hostname(config-cmap)# class-map type inspect http match-any monitor-http
hostname(config-cmap)# match request method get
hostname(config-cmap)# match request method put
hostname(config-cmap)# match request method post
```

関連コマンド

コマンド	説明
class-map	通過トラフィック用のレイヤ 3/4 クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。

コマンド	説明
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type management

モジュラ ポリシー フレームワーク を使用するとき、グローバル コンフィギュレーション モードで **class-map type management** コマンドを使用して、アクションを適用するセキュリティ アプライアンス宛ての、レイヤ 3 またはレイヤ 4 の管理トラフィックを指定します。クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type management *class_map_name*

no class-map type management *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。「class-default」という名前および「_internal」または「_default」で始まる任意の名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。

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
7.2(1)	このコマンドが導入されました。
8.0(2)	セキュリティ アプライアンスに向かう管理トラフィックの場合、レイヤ 3/4 管理クラス マップに **set connection** コマンドが使用できるようになりました。**conn-max** キーワードおよび **embryonic-conn-max** キーワードだけが使用可能です。

使用上のガイドライン

このタイプのクラス マップは、管理トラフィック専用です。通過トラフィックについては、**class-map** コマンド（**type** キーワードは指定しない）を参照してください。

セキュリティ アプライアンスへの管理トラフィックに対して、この種類のトラフィックに特有のアクションの実行が必要になる場合があります。ポリシー マップの管理クラス マップで設定可能なアクションのタイプは、管理トラフィック専用です。たとえば、このタイプのクラス マップでは、RADIUS アカウンティング トラフィックをインスペクトして、接続制限を設定できます。

レイヤ 3/4 クラス マップにより、アクションを適用するレイヤ 3 および 4 のトラフィックを特定します。すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。

レイヤ 3/4 ポリシー マップそれぞれに、複数のレイヤ 3/4 クラス マップ（管理トラフィックまたは通過トラフィック）を作成できます。

モジュラ ポリシー フレームワークの設定手順は、次の 4 つの作業で構成されます。

1. **class-map** コマンドおよび **class-map type management** コマンドを使用して、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを識別します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

class-map type management コマンドを使用して、クラス マップ コンフィギュレーション モードを開始します。クラス マップ コンフィギュレーション モードから、**match** コマンドを使用して、クラスに含めるトラフィックを定義できます。管理クラス マップを指定して、アクセス リストまたは TCP や UDP のポートと照合できます。レイヤ 3/4 クラス マップには、クラス マップに含まれるトラフィックを指定する **match** コマンドが 1 つだけが含まれています。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次に、レイヤ 3/4 管理クラス マップを作成する例を示します。

```
hostname(config)# class-map type management radius_acct
hostname(config-cmap)# match port tcp eq 10000
```

関連コマンド

コマンド	説明
class-map	通過トラフィック用のレイヤ 3/4 クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
show running-config class-map	クラス マップ コンフィギュレーションに関する情報を表示します。

class-map type regex

モジュラ ポリシー フレームワーク を使用するときに、グローバル コンフィギュレーション モードで **class-map type regex** コマンドを使用して、一致テキストで利用する正規表現をグループ化します。正規表現クラス マップを削除するには、このコマンドの **no** 形式を使用します。

class-map type regex match-any *class_map_name*

no class-map [**type regex match-any**] *class_map_name*

構文の説明

class_map_name	40 文字までの長さのクラス マップ名を指定します。「class-default」という名前および「_internal」または「_default」で始まる任意の名前は予約されています。クラス マップのすべてのタイプで同じネーム スペースを使用するため、すでに別のクラス マップ タイプで使用されている名前は再利用できません。
match-any	トラフィックが正規表現のいずれかとだけ一致する場合でも、このトラフィックがクラス マップと一致しているとすることを指定します。**match-any** が唯一のオプションです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(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

モジュラ ポリシー フレームワークを使用すると、多くのアプリケーション インスペクションに対して特別なアクションを設定できます。レイヤ 3/4 ポリシー マップでインスペクション エンジンをイネーブルにするときは、*インスペクション ポリシー マップ*で定義されているアクションを必要に応じてイネーブルにすることもできます（**policy-map type inspect** コマンドを参照）。

インスペクション ポリシー マップでは、1 つ以上の **match** コマンドを含んだインスペクション クラス マップを作成することで、アクションの実行対象となるトラフィックを識別できます。または、**match** コマンドをインスペクション ポリシー マップ内で直接使用することもできます。一部の **match** コマンドでは、パケット内のテキストを正規表現を使用して識別できます。たとえば、HTTP パケット内の URL 文字列を照合できます。正規表現クラス マップで正規表現をグループ化できます。

正規表現クラス マップを作成する前に、**regex** コマンドを使用して、正規表現を作成します。次に、**match regex** コマンドを使用して、クラス マップ コンフィギュレーション モードで名前を付けられた正規表現を指定します。

すべてのタイプのクラス マップの最大数は、シングル モードでは 255 個、マルチ モードではコンテキストごとに 255 個です。クラス マップには、次のタイプがあります。

- **class-map**
- **class-map type management**
- **class-map type inspection**
- **class-map type regex**
- ポリシー マップ タイプの **match** コマンドでは、コンフィギュレーション モードを検査します。

この制限にはすべてのタイプのデフォルト クラス マップも含まれます。詳細については、**class-map** コマンドを参照してください。

例

次に、2 つの正規表現を作成し、これを正規表現クラス マップに追加する例を示します。トラフィックに「example.com」または「example2.com」というストリングが含まれている場合、このトラフィックはクラス マップと一致しています。

```
hostname(config)# regex url_example example\.com
hostname(config)# regex url_example2 example2\.com
hostname(config)# class-map type regex match-any URLs
hostname(config-cmap)# match regex example
hostname(config-cmap)# match regex example2
```

関連コマンド

コマンド	説明
class-map type inspect	アプリケーション固有のトラフィックと照合するインスペクション クラス マップを作成します。
policy-map	トラフィック クラスを 1 つ以上のアクションと関連付けることによって、ポリシー マップを作成します。
policy-map type inspect	アプリケーション インスペクションの特別なアクションを定義します。
service-policy	ポリシー マップを 1 つ以上のインターフェイスと関連付けることによって、セキュリティ ポリシーを作成します。
regex	正規表現を作成します。

clear aaa local user fail-attempts

ユーザのロック アウト ステータスを変更しないで、ユーザ認証失敗試行回数を 0 にリセットするには、特権 EXEC モードで **clear aaa local user fail-attempts** コマンドを使用します。

clear aaa local user authentication fail-attempts {**username** *name* | **all**}

構文の説明

all	すべてのユーザについて、失敗試行カウンタを 0 にリセットします。
name	失敗試行カウンタを 0 にリセットする特定のユーザ名を指定します。
username	続くパラメータが、失敗試行カウンタを 0 にリセットするユーザのユーザ名であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

ユーザが認証試行を何回か失敗した後に、ユーザ認証を失敗にするには、このコマンドを使用します。

設定された認証試行の失敗数に達すると、ユーザは、システムからロック アウトされ、システム管理者がこのユーザ名のロックを解除するか、またはシステムをリブートするまで、正常にログインできません。ユーザが正常に認証されるか、またはセキュリティ アプライアンスをリブートすると、失敗試行数が 0 にリセットされ、ロックアウト ステータスが No にリセットされます。また、コンフィギュレーションが変更されると、システムがカウンタを 0 にリセットします。

ユーザ名のロックまたはアンロックにより、システム ログ メッセージが生成されます。特権レベル 15 のシステム管理者は、ロック アウトされません。

例

次に、**clear aaa local user authentication fail-attempts** コマンドを使用して、ユーザ名 anyuser の失敗試行カウンタを 0 にリセットする例を示します。

```
hostname(config)# clear aaa local user authentication fail-attempts username anyuser
hostname(config)#
```

次に、**clear aaa local user authentication fail-attempts** コマンドを使用して、すべてのユーザの失敗試行カウンタを 0 にリセットする例を示します。

```
hostname(config)# clear aaa local user authentication fail-attempts all
```

```
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	許可される失敗ユーザ認証試行の回数制限を設定します。
clear aaa local user lockout	ユーザのロックアウト ステータスを変更することなく、失敗ユーザ認証試行の回数をゼロにリセットします。
show aaa local user [locked]	現在ロックされているユーザ名のリストを表示します。

clear aaa local user lockout

指定したユーザのロックアウト ステータスをクリアし、失敗試行カウンタを 0 に設定するには、特権 EXEC モードで **clear aaa local user lockout** コマンドを使用します。

clear aaa local user lockout {**username** *name* | **all**}

構文の説明

all	すべてのユーザについて、失敗試行カウンタを 0 にリセットします。
name	失敗試行カウンタを 0 にリセットする特定のユーザ名を指定します。
username	続くパラメータが、失敗試行カウンタを 0 にリセットするユーザのユーザ名であることを示します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

username オプションを使用して単一のユーザを指定するか、**all** オプションを使用してすべてのユーザを指定できます。

このコマンドは、ロックアウトされているユーザのステータスだけに影響します。

管理者をデバイスからロックアウトすることはできません。

ユーザ名のロックまたはアンロックにより、syslog メッセージが生成されます。

例

次に、**clear aaa local user lockout** コマンドを使用して、ユーザ名 anyuser のロックアウト状態をクリアし、失敗試行カウンタを 0 にリセットする例を示します。

```
hostname(config)# clear aaa local user lockout username anyuser
hostname(config)#
```

関連コマンド

コマンド	説明
aaa local authentication attempts max-fail	許可される失敗ユーザ認証試行の回数制限を設定します。
clear aaa local user fail-attempts	ユーザのロックアウト ステータスを変更することなく、失敗ユーザ認証試行の回数をゼロにリセットします。
show aaa local user [locked]	現在ロックされているユーザ名のリストを表示します。

clear aaa-server statistics

AAA サーバの統計情報をリセットするには、特権 EXEC モードで **clear aaa-server statistics** コマンドを使用します。

clear aaa-server statistics [**LOCAL** | *groupname* [**host** *hostname*] | **protocol** *protocol*]

構文の説明

LOCAL	（任意）LOCAL ユーザ データベースの統計情報をクリアします。
groupname	（任意）グループ内のサーバの統計情報をクリアします。
host *hostname*	（任意）グループ内の特定のサーバの統計情報をクリアします。
protocol *protocol*	（任意）次に指定するプロトコルのサーバの統計情報をクリアします。 • **kerberos** • **ldap** • **nt** • **radius** • **sdi** • **tacacs+**

デフォルト

すべてのグループのすべての AAA サーバの統計情報を削除します。

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
特権 EXEC	•	•	•	•	—

コマンド履歴

リリース	変更内容
7.0(1)	CLI ガイドラインに沿うように、このコマンドが変更されました。プロトコルの値において、以前の **nt-domain** から **nt** に、以前の **rsa-ace** から **sdi** に置き換えられました。

例

次に、グループ内の特定のサーバの AAA 統計情報をリセットするコマンドを示します。

```
hostname(config)# clear aaa-server statistics svrgrp1 host 1.2.3.4
```

次に、サーバ グループ全体の AAA 統計情報をリセットするコマンドを示します。

```
hostname(config)# clear aaa-server statistics svrgrp1
```

次に、すべてのサーバ グループの AAA 統計情報をリセットするコマンドを示します。

```
hostname(config)# clear aaa-server statistics
```

次に、特定のプロトコル（この場合は TACACS+）の AAA 統計情報をリセットするコマンドを示します。

```
hostname(config)# clear aaa-server statistics protocol tacacs+
```

関連コマンド

コマンド	説明
aaa-server protocol	AAA サーバ接続データのグループ化の指定および管理を行います。
clear configure aaa-server	デフォルト以外のすべての AAA サーバ グループを削除するか、または指定したグループをクリアします。
show aaa-server	AAA サーバの統計情報を表示します。
show running-config aaa-server	現在の AAA サーバ コンフィギュレーションの値を表示します。

clear access-list

アクセス リスト カウンタをクリアするには、グローバル コンフィギュレーション モードで **clear access-list** コマンドを使用します。

clear access-list *id* **counters**

構文の説明

counters	アクセス リストのカウンタをクリアします。
id	アクセス リストの名前または番号。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

clear access-list コマンドを入力したら、カウンタをクリアするアクセスリストの *ID* を指定します。そうしないと、カウンタはクリアされません。

例

次に、特定のアクセス リスト カウンタをクリアする例を示します。

```
hostname# clear access-list inbound counters
```

関連コマンド

コマンド	説明
access-list extended	アクセス リストをコンフィギュレーションに追加し、ファイアウォールを通過する IP トラフィック用のポリシーを設定します。
access-list standard	OSPF ルートの宛先 IP アドレスを識別するアクセス リストを追加します。このアクセス リストは、OSPF 再配布のルート マップで使用できます。
clear configure access-list	実行コンフィギュレーションからアクセス リストをクリアします。
show access-list	アクセス リスト エントリを番号で表示します。
show running-config access-list	セキュリティ アプライアンスで実行中のアクセス リスト コンフィギュレーションを表示します。

clear arp

ダイナミック ARP エントリまたは ARP 統計情報をクリアするには、特権 EXEC モードで **clear arp** コマンドを使用します。

clear arp [**statistics**]

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

例

次に、すべての ARP 統計情報をクリアする例を示します。

```
hostname# clear arp statistics
```

関連コマンド

コマンド	説明
arp	スタティック ARP エントリを追加します。
arp-inspection	トランスペアレント ファイアウォール モードで、ARP パケットを調査し、ARP スプーフィングを防止します。
show arp statistics	ARP 統計情報を表示します。
show running-config arp	ARP タイムアウトの現在のコンフィギュレーションを表示します。

clear asp drop

高速セキュリティ パスのドロップ統計情報をクリアするには、特権 EXEC モードで **clear asp drop** コマンドを使用します。

clear asp drop [**flow** *type* | **frame** *type*]

構文の説明

flow	（任意）ドロップされたフロー統計情報をクリアします。
frame	（任意）ドロップされたパケット統計情報をクリアします。
type	（任意）特定のプロセスのためにドロップされたフロー統計情報またはパケット統計情報をクリアします。タイプのリストについては、「使用上のガイドライン」を参照してください。

デフォルト

デフォルトでは、このコマンドを使用すると、すべてのドロップ統計情報がクリアされます。

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
特権 EXEC	•	•	•	•	•

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが導入されました。

使用上のガイドライン

プロセス タイプには、次のものが含まれます。

```
acl-drop
audit-failure
closed-by-inspection
conn-limit-exceeded
fin-timeout
flow-reclaimed
fo-primary-closed
fo-standby
fo_rep_err
host-removed
inspect-fail
ips-fail-close
ips-request
ipsec-spoof-detect
loopback
mcast-entry-removed
mcast-intrf-removed
mgmt-lockdown
nat-failed
nat-rpf-failed
need-ike
```

```
no-ipv6-ipsec
non_tcp_syn
out-of-memory
parent-closed
pinhole-timeout
recurse
reinject-punt
reset-by-ips
reset-in
reset-oout
shunned
syn-timeout
tcp-fins
tcp-intecept-no-response
tcp-intercept-kill
tcp-intercept-unexpected
tcpnorm-invalid-syn
tcpnorm-rexmit-bad
tcpnorm-win-variation
timeout
tunnel-pending
tunnel-torn-down
xlate-removed
```

例

次に、すべてのドロップ統計情報をクリアする例を示します。

```
hostname# clear asp drop
```

関連コマンド

コマンド	説明
show asp drop	ドロップされたパケットの高速セキュリティ パス カウンタを示します。

clear asp table

asp arp テーブルまたは asp classify テーブルのいずれか、あるいはこの両方でヒット カウンタをクリアするには、特権 EXEC モードで **clear asp table** コマンドを使用します。

clear asp table [**arp** | **classify**]

構文の説明

arp	asp arp テーブルのみでヒット カウンタをクリアします。
classify	asp classify テーブルのみでヒット カウンタをクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(4)	このコマンドが導入されました。

使用上のガイドライン

clear asp table コマンドでヒットを指定するオプションは arp と classify の 2 つだけです。

例

次に、すべてのドロップ統計情報をクリアする例を示します。

```
hostname# clear asp table

Warning: hits counters in asp arp and classify tables are cleared, which might impact the
hits statistic of other modules and output of other "show" commands! hostname#clear asp
table arp
Warning: hits counters in asp arp table are cleared, which might impact the hits statistic
of other modules and output of other "show" commands! hostname#clear asp table classify
Warning: hits counters in classify tables are cleared, which might impact the hits
statistic of other modules and output of other "show" commands! hostname(config)# clear
asp table
Warning: hits counters in asp tables are cleared, which might impact the hits statistics
of other modules and output of other "show" commands! hostname# sh asp table arp

Context: single_vf, Interface: inside 10.1.1.11 Active 00e0.8146.5212 hits 0

Context: single_vf, Interface: identity :: Active 0000.0000.0000 hits 0 0.0.0.0 Active
0000.0000.0000 hits 0
```

関連コマンド

コマンド	説明
show asp table arp	高速セキュリティ パスの内容を表示します。この情報は、問題のトラブルシューティングに役立つ場合があります。

clear blocks

最低水準点や履歴情報などのパケット バッファ カウンタをリセットするには、特権 EXEC モードで **clear blocks** コマンドを使用します。

clear blocks

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
既存	このコマンドは既存です。

使用上のガイドライン

最低水準点カウンタを各プール内で現在使用可能なブロックにリセットします。また、このコマンドは、前回のバッファ割り当ての失敗時に保存された履歴情報をクリアします。

例

次に、ブロックをクリアする例を示します。

```
hostname# clear blocks
```

関連コマンド

コマンド	説明
blocks	ブロック診断に割り当てるメモリを増やします。
show blocks	システム バッファの使用状況を表示します。

clear-button

WebVPN ユーザがセキュリティ アプライアンスに接続したときに表示される WebVPN ページ ログイン フィールドの [Clear] ボタンをカスタマイズするには、カスタマイゼーション コンフィギュレーション モードで **clear-button** コマンドを使用します。コンフィギュレーションからコマンドを削除して、値が継承されるようにするには、このコマンドの **no** 形式を使用します。

clear-button {**text** | **style**} *value*

no clear-button [{**text** | **style**}] *value*

構文の説明

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

デフォルト

デフォルトのテキストは「Clear」です。

デフォルトのスタイルは、border:1px solid black;background-color:white;font-weight:bold;font-size:80% です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
カスタマイゼーション コンフィギュレーション	•	—	•	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

使用上のガイドライン

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

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

- カンマ区切りの RGB 値、HTML の色値、または色の名前（HTML で認識される場合）を使用できます。
- RGB 形式は 0,0,0 で、各色（赤、緑、青）を 0 ～ 255 の範囲の 10 進値で入力します。このカンマ区切りのエントリは、他の 2 色と組み合わせる各色の明度レベルを示します。

- HTML 形式は #000000 で、16 進形式の 6 桁の数値です。先頭と 2 番めは赤を、3 番めと 4 番めは緑を、5 番めと 6 番めは青を表しています。

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

例

次に、[Clear] ボタンのデフォルトの背景色を黒から青に変更する例を示します。

```
hostname(config)# webvpn
hostname(config-webvpn)# customization cisco
hostname(config-webvpn-custom)# clear-button style background-color:blue
```

関連コマンド

コマンド	説明
login-button	WebVPN ページの Login フィールドのログイン ボタンをカスタマイズします。
login-title	WebVPN ページの Login フィールドのタイトルをカスタマイズします。
group-prompt	WebVPN ページの Login フィールドのグループ プロンプトをカスタマイズします。
password-prompt	WebVPN ページの Login フィールドのパスワード プロンプトをカスタマイズします。
username-prompt	WebVPN ページの Login フィールドのユーザ名プロンプトをカスタマイズします。

clear capture

キャプチャ バッファをクリアするには、特権 EXEC コンフィギュレーション モードで **clear capture** *capture_name* コマンドを使用します。

clear capture *capture_name*

構文の説明

capture_name	パケット キャプチャの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドがサポートされるようになりました。

使用上のガイドライン

誤ってすべてのパケット キャプチャを破棄することを防止するために、**clear capture** の短縮形（たとえば、**cl cap** や **clear cap**）は、サポートされていません。

例

次に、キャプチャ バッファ「example」のキャプチャ バッファをクリアする例を示します。

```
hostname(config)# clear capture example
```

関連コマンド

コマンド	説明
capture	パケット スニッフィングおよびネットワーク障害の切り分けのためにパケット キャプチャ機能をイネーブルにします。
show capture	オプションが指定されていない場合は、キャプチャ コンフィギュレーションを表示します。

clear compression

すべての SVC および WebVPN の接続の圧縮統計情報をクリアするには、特権 EXEC モードで **clear compression** コマンドを使用します。

clear compression {**all** | **svc** | **http-comp**}

構文の説明

all	すべての圧縮統計情報をクリアします。
http-comp	HTTP-COMP 統計情報をクリアします。
svc	SVC 圧縮統計情報をクリアします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが導入されました。

例

次に、ユーザの圧縮コンフィギュレーションをクリアする例を示します。

```
hostname# clear configure compression
```

関連コマンド

コマンド	説明
compression	すべての SVC 接続および WebVPN 接続の圧縮をイネーブルにします。
svc compression	特定のグループまたはユーザに対して、SVC 接続経由でのデータの圧縮をイネーブルにします。