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

ディセーブル

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
9.5(2)	デフォルトがイネーブルからディセーブルに変更されました。

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。これにより、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します。

(注) コンテンツ キャッシングをイネーブルにすると、一部のシステムの信頼性が低下します。コンテンツ キャッシングをイネーブルにした後、ランダムにクラッシュが発生する場合は、この機能をディセーブルにしてください。

次に、キャッシュ モードを開始する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(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。

ca-check

基本制約の拡張を設定し、トラストポイント証明書に CA フラグを設定するには、crypto ca トラストポイント コンフィギュレーション モードで **ca-check** コマンドを使用します。基本制約の拡張と CA フラグを設定しない場合は、このコマンドの **no** 形式を使用します。

ca-check

no ca-check

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、基本制約の拡張と CA フラグが設定されます。これらを無効にするには、**no** 形式を使用する必要があります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

基本制約の拡張によって、証明書のサブジェクトが認証局（CA）かどうかが識別されます。この場合、証明書を使用して他の証明書に署名することができます。CA フラグは、この拡張の一部です。これらの項目が証明書に存在することは、証明書の公開キーを使用して証明書の署名を検証できることを示します。

例

次に、CA フラグと基本制約の拡張を無効にする例を示します。

```
ciscoasa(config)# crypto ca trustpoint newtrust
ciscoasa(config-ca-trustpoint)# no ca-check
ciscoasa(config-ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。このコマンドは、グローバル コンフィギュレーション モードで使用します。

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をキャッシュするには、webvpn キャッシュ コンフィギュレーション モードで **cache-static-content** コマンドを入力します。静的コンテンツのキャッシングをディセーブルにするには、このコマンドの **no** 形式を入力します。

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

ディセーブル

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

キャッシュ可能なすべての静的コンテンツがアプライアンス 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が行われないオブジェクトが含まれています。

例

次に、静的コンテンツのキャッシングをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
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。

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、ca-crl 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	トランスペアレント	シングル	コンテキスト	システム
ca-crl コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、ca-crl コンフィギュレーション モードを開始し、トラストポイント central 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。

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

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

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	トランスペアレント	シングル	コンテキスト	システム
MGCP マップ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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。

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。

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

```
ciscoasa(config-mgcp-map)# gateway 10.10.10.116 102
ciscoasa(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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 コールのコール継続時間を設定する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# 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 またはレイヤ 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強制するには、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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、H.323 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。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(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 またはレイヤ 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-home

Call Home 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 **call-home** コマンドを使用します。

call-home

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

call-home コマンドを入力すると、プロンプトが hostname (cfg-call-home)# に変更され、次の Call Home コンフィギュレーション コマンドを利用できます。

- [**no**] **alert-group** {**group name** | **all**}：Smart Call Home グループをイネーブルまたはディセーブルにします。デフォルトでは、すべてのアラート グループに対してイネーブルになっています。
  group name：syslog、診断、環境、インベントリ、コンフィギュレーション、スナップショット、脅威、テレメトリ、テスト。
- [**no**] **contact-e-mail-addr e-mail-address**：カスタマーの連絡先電子メール アドレスを指定します。このフィールドは必須です。
  e-mail-address：最大 127 文字のカスタマーの電子メール アドレス。
- [**no**] **contact-name contact name**：カスタマーの名前を指定します。
  e-mail-address：最大 127 文字のカスタマーの名前。
- [**no**] **contract-id contract-id-string**：カスタマーの契約 ID を指定します。
  contract-id-string：最大 128 文字の ID 番号。スペースを使用できますが、スペースが含まれる場合はストリングの前後に引用符を付ける必要があります。

- **copy profile src-profile-name dest-profile-name**：既存のプロファイル（**src-profile-name**）の内容を新しいプロファイル（**dest-profile-name**）にコピーします。
  src-profile-name：23 文字までの既存プロファイルの名前。
  dest-profile-name：23 文字までの新規プロファイルの名前。
- **rename profile src-profile-name dest-profile-name**：既存のプロファイルの名前を変更します。
  src-profile-name：23 文字までの既存プロファイルの名前。
  dest-profile-name：23 文字までの新規プロファイルの名前。
- **no configuration all**：Smart Call-home コンフィギュレーションをクリアします。
  [**no**] **customer-id customer-id-string**：カスタマー ID を指定します。
  customer-id-string：最大 64 文字のカスタマー ID。このフィールドは、XML 形式のメッセージでは必須です。
- [**no**] **event-queue-size queue_size**：イベント キュー サイズを指定します。
  queue-size：5 ～ 60 でイベント数を示します。デフォルトは 10 です。
- [**no**] **mail-server ip-address | name priority 1-100 all**：SMTP メール サーバを指定します。顧客は、最大 5 つのメール サーバを指定できます。Smart Call Home メッセージに電子メール転送を使用するには、少なくとも 1 つのメール サーバが必要です。
  ip-address：メール サーバの IPv4 アドレスまたは IPv6 アドレス。
  name：メール サーバのホスト名。
  1-100：メール サーバのプライオリティ。値が小さいほど、プライオリティが高くなります。
- [**no**] **phone-number phone-number-string**：カスタマーの電話番号を指定します。このフィールドは任意です。
  phone-number-string：電話番号。
- [**no**] **rate-limit msg-count**：Smart Call Home が 1 分間に送信できるメッセージの数を指定します。
  msg-count：1 分間に送信できるメッセージ数。デフォルトは 10 です。
- [**no**] **sender** {**from e-mail-address | reply-to e-mail-address**}：電子メール メッセージの from および reply-to の電子メール アドレスを指定します。このフィールドは任意です。
  e-mail-address：発信元または応答先の電子メール アドレス。
- [**no**] **site-id site-id-string**：カスタマー サイト ID を指定します。このフィールドは任意です。
  site-id-string：カスタマーの場所を識別するサイト ID。
- [**no**] **street-address street-address**：カスタマーの住所を指定します。このフィールドは任意です。
  street-address：最大 255 文字の自由形式の文字列。
- [**no**] **alert-group-config environment**：環境グループ コンフィギュレーション モードを開始します。
  [**no**] **threshold** {**cpu | memory**} **low-high**：環境リソースしきい値を指定します。
  low、**high**：有効な値は 0 ～ 100 です。デフォルトは 85 ～ 90 です。
- [**no**] **alert-group-config snapshot**：スナップショット グループ コンフィギュレーション モードを開始します。
  system、**user**：システム コンテキストまたはユーザ コンテキスト（マルチ モードでのみ使用可）で CLI を実行します。
- [**no**] **add-command “cli command”** [{**system | user**}]：スナップショット グループにキャプチャする CLI コマンドを指定します。
  cli command：入力する CLI コマンド。
  system、**user**：CLI をシステム コンテキストまたはユーザ コンテキストで実行します（マルチ モードだけで使用可能）。システムもユーザも指定しないと、CLI はシステム コンテキストとユーザ コンテキストの両方で実行されます。デフォルトは、ユーザ コンテキストです。

（注） Call-Home HTTPS メッセージは、ここで説明する **vrf** コマンドとは別に、**ip http client source-interface** コマンドを使用して、指定した VRF 上の送信元インターフェイスを介してだけ送信できます。

例

次に、連絡先情報を設定する例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# contact-e-mail-addr username@example.com
hostname(cfg-call-home)# customer-id Customer1234
hostname(cfg-call-home)# phone-number +1-800-555-0199
hostname(cfg-call-home)# site-id Site1
hostname(cfg-call-home)# street-address "1234 Any Street, Any city, Any state, 12345"
```

次に、Call Home メッセージのレート制限しきい値を設定する例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# rate-limit 50
```

次に、Call Home メッセージのレート制限しきい値をデフォルト設定にする例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# default rate-limit
```

次に、既存のプロファイルと同じコンフィギュレーション設定の新しい宛先プロファイルを作成する例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# copy profile profile1 profile1a
```

次に、一般的な電子メール パラメータ(プライマリ電子メール サーバ、セカンダリ電子メール サーバなど)を設定する例を示します。

```
hostname(config)# call-home
hostname(cfg-call-home)# mail-server smtp.example.com priority 1
hostname(cfg-call-home)# mail-server 192.168.0.1 priority 2
hostname(cfg-call-home)# sender from username@example.com
hostname(cfg-call-home)# sender reply-to username@example.com
```

関連コマンド

コマンド	説明
alert-group	アラート グループをイネーブルにします。
profile	Call Home プロファイル コンフィギュレーション モードを開始します。
show call-home	Call Home コンフィギュレーション情報を表示します。

call-home send

CLI コマンドを実行し、指定されたアドレスにコマンド出力を電子メールで送信するには、特権 EXEC モードで **call-home send** コマンドを使用します。

call-home send cli command [**email** *email*] [**service-number** *service number*]

構文の説明

cli-command	実行する CLI コマンドを指定します。コマンド出力は電子メールで送信されます。
email *email*	CLI コマンド出力の送信先の電子メール アドレスを指定します。電子メール アドレスを指定していない場合、コマンド出力は Cisco TAC（attach@cisco.com）に送信されます。
service-number *service number*	コマンド出力が関係するアクティブな TAC ケース番号を指定します。この番号は、電子メール アドレス（または TAC 電子メール アドレス）が指定されていない場合にのみ必要で、電子メールの件名行に表示されます。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、指定した CLI コマンドがシステム上で実行されます。指定する CLI コマンドは、引用符（""）で囲む必要があります。また、任意の **run** コマンドまたは **show** コマンド（すべてのモジュール用のコマンドを含む）を指定できます。

その後、コマンド出力は、電子メールで指定の電子メール アドレスに送信されます。電子メール アドレスを指定していない場合、コマンド出力は Cisco TAC（attach@cisco.com）に送信されます。電子メールは、件名行にサービス番号を付けて（指定した場合）ロング テキスト形式で送信されます。

例

次に、CLI コマンドを送信し、コマンド出力を電子メールで送信する例を示します。

```
hostname# call-home send "show diagnostic result module all" email support@example.com
```

関連コマンド

call-home	Call Home コンフィギュレーション モードを開始します。
call-home test	定義した Call Home テスト メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。
show call-home	Call Home コンフィギュレーション情報を表示します。

call-home send alert-group

特定のアラート グループ メッセージを送信するには、特権 EXEC モードで **call-home send alert-group** コマンドを使用します。

call-home send alert-group {**configuration** | **telemetry** | **inventory** | **group snapshot**} [**profile** *profile-name*]

構文の説明

設定	コンフィギュレーション アラート グループ メッセージを宛先プロファイルに送信します。
group snapshot	スナップショット グループを送信します。
インベントリ	インベントリ call-home メッセージを送信します。
profile *profile-name*	(任意)宛先プロファイルの名前を指定します。
Telemetry	特定のモジュール、スロット/サブスロット、またはスロット/ベイ番号に関する診断アラート グループ メッセージを宛先プロファイルに送信します。

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

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

profile *profile-name* を指定しない場合は、サブスクライブ対象のすべての宛先プロファイルにメッセージが送信されます。

手動で送信できるのは、コンフィギュレーション、診断、およびインベントリ アラート グループだけです。宛先プロファイルは、アラート グループにサブスクライブされる必要はありません。

例

次に、コンフィギュレーション アラート グループ メッセージを宛先プロファイルに送信する例を示します。

```
hostname# call-home send alert-group configuration
```

次に、特定のモジュール、スロット/サブスロット、またはスロット/ベイ番号に関する診断アラート グループ メッセージを宛先プロファイルに送信する例を示します。

```
hostname# call-home send alert-group diagnostic module 3 5/2
```

次に、特定のモジュール、スロット/サブスロット、またはスロット/ベイ番号に関する診断アラート グループ メッセージをすべての宛先プロファイルに送信する例を示します。

```
hostname# call-home send alert-group diagnostic module 3 5/2 profile Ciscotac1
```

次に、インベントリ call-home メッセージを送信する例を示します。

```
hostname# call-home send alert-group inventory
```

関連コマンド

call-home	Call Home コンフィギュレーション モードを開始します。
call-home test	定義した Call Home テスト メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。
show call-home	Call Home コンフィギュレーション情報を表示します。

call-home test

プロファイルのコンフィギュレーションを使用して Call Home テスト メッセージを手動で送信するには、特権 EXEC モードで **call-home test** コマンドを使用します。

call-home test [“*test-message*”] **profile** *profile-name*

構文の説明

profile *profile-name*	宛先プロファイルの名前を指定します。
“*test-message*”	（任意）テスト メッセージ テキスト。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

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

コマンド履歴

リリース	変更内容
8.2(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用すると、テスト メッセージが指定の宛先プロファイルに送信されます。テスト メッセージ テキストを入力する場合、テキストにスペースが含まれている場合は、このテキストを引用符（""）で囲む必要があります。メッセージを入力しない場合、デフォルト メッセージが送信されます。

例

次に、Call Home テスト メッセージを手動で送信する例を示します。

```
hostname# call-home test “test of the day” profile Ciscotac1
```

関連コマンド

call-home	Call Home コンフィギュレーション モードを開始します。
call-home send alert-group	特定のアラート グループ メッセージを送信します。
service call-home	Call Home をイネーブルまたはディセーブルにします。
show call-home	Call Home コンフィギュレーション情報を表示します。

capability lls

LLS 機能はデフォルトでイネーブルです。送信される OSPF パケットのリンクローカル シグナリング（LLS）データ ブロックの使用を明示的にイネーブルにし、OSPF NSF 認識を再度イネーブルにするには、ルータ コンフィギュレーション モードで **capability lls** コマンドを使用します。LLS と OSPF NSF 認識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。

capability lls

no capability lls

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

LLS 機能はデフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが導入されました。

使用上のガイドライン

送信される OSPF パケットの LLS データ ブロックの使用をディセーブルにすることで、NSF 認識をディセーブルにすることが必要な場合があります。また、LLS を使用するアプリケーションがルータで動作していない場合に、NSF 認識をディセーブルにすることが必要な場合があります。

NSF が設定されている状態で LLS をディセーブルにしようとすると、「OSPF Non-Stop Forwarding (NSF) must be disabled first」というエラー メッセージが表示されます。

LLS がディセーブルになっている状態で、NSF を設定しようとすると、「OSPF Link-Local Signaling (LLS) capability must be enabled first」というエラー メッセージが表示されます。

例

次に、LLS のサポートと OSPF 認識をイネーブルにする例を示します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability lls
```

関連コマンド		
	capability opaque	Opaque LSA を使用して MPLS TE 情報をネットワークにフラッディングできるようにします。

capability opaque

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング（MPLS TE）トポロジ情報を Opaque LSA を介してネットワークにフラッディングできるようにするには、ルータ コンフィギュレーション モードで **capability opaque** コマンドを使用します。MPLS TE トポロジ情報が Opaque LSA を介してネットワークにフラッディングされないようにするには、このコマンドの no 形式を使用します。

capability opaque

no capability opaque

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

Opaque LSA はデフォルトでイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが導入されました。

使用上のガイドライン

capability opaque コマンドは、すべての範囲（タイプ 9、10、11）の Opaque LSA を介して MPLS TE 情報（タイプ 1 および 4）をフラッディングします。

Opaque LSA サポート機能の制御は、MPLS TE をサポートするために OSPF でイネーブルにする必要があります。

MPLS TE トポロジ情報は、デフォルトで、Opaque LSA を介してエリアにフラッディングされます。

例

次に、Opaque 機能をイネーブルにする例を示します。

```
ciscoasa(config)# router ospf 2
ciscoasa(config-router)# capability opaque
```

関連コマンド		
	capability lls	送信される OSPF パケットの LLS データ ブロックの使用をイネーブルにし、OSPF NSF 認識をイネーブルにします。

captive-portal

ASA FirePOWER モジュールのキャプティブ ポータルをイネーブルにするには、グローバル コンフィギュレーション モードで **captive-portal** コマンドを使用します。キャプティブ ポータル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。

captive-portal {**global** | **interface** *name*} [**port** *number*]

no captive-portal {**global** | **interface** *name*} [**port** *number*]

構文の説明

global	すべてのインターフェイスでキャプティブ ポータルをグローバルにイネーブルにします。
interface *name*	指定したインターフェイスのみでキャプティブ ポータルをイネーブルにします。コマンドを複数入力して複数のインターフェイスでイネーブルにできます。この方法は、一部のインターフェイスのみのトラフィックを ASA FirePOWER モジュールにリダイレクトする場合に使用します。
port *number*	（任意）認証プロキシ ポートを 1025 以上に設定します。デフォルト ポートである 885 を設定する場合は、このキーワードを指定しないでください。

コマンド デフォルト

デフォルト ポートは 885（TCP）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	トランスペアレント	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	• 対応	• —	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
9.5(2)	このコマンドが追加されました。

使用上のガイドライン

キャプティブ ポータルは、ASA FirePOWER モジュールで定義されたアイデンティティ ポリシーと連携して動作します。

HTTP/HTTPS 接続については、アクティブな認証を通じてユーザ ID を収集するアイデンティティ ルールを定義できます。アクティブな認証アイデンティティ ルールを実装する場合は、認証プロキシ ポートとして機能するように ASA でキャプティブ ポータルを設定する必要があります。接続がアクティブ認証を要求するアイデンティティ ルールに一致すると、ASA FirePOWER モジュールは、認証要求を ASA インターフェイスの IP アドレス/キャプティブ ポータルにリダイレクトします。デフォルト ポートは 885 ですが、これは変更可能です。

認証プロキシのキャプティブ ポータルをイネーブルにしない場合は、パッシブ認証のみを使用できます。

例

次に、デフォルト ポート 885 でキャプティブ ポータルをグローバルにイネーブルにする例を示します。

```
ciscoasa(config)# captive-portal global
ciscoasa(config)#
```

関連コマンド

コマンド	説明
sfr	ASA FirePOWER モジュールにトラフィックをリダイレクトします。
show running-config captive-portal	キャプティブ ポータル コンフィギュレーションを表示します。
show service-policy	サービス ポリシーの統計情報を表示します。

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。

ネットワークトラフィックをキャプチャします。

capture *capture_name* [**type** {**asp-drop** [**all** | *drop-code*] | **tls-proxy** | **raw-data** | **isakmp** [**ikev1** | **ikev2**] | **inline-tag** [*tag*] | **webvpn user** *webvpn-user*}] [**access-list** *access_list_name*] {**interface** {*interface_name* | **asa_dataplane** | **asa_mgmt_plane** | **cplane**} } [**buffer** *buf_size*] [**ethernet-type** *type*] [**reeinject-hide**] [**packet-length** *bytes*] [**circular-buffer**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4** | **any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4** | **any6**} [*operator dest_port*]] [**switch**] [**offload**] [**ivlan** *number*] [**ovlan** *number*]

クラスタ制御リンクトラフィックをキャプチャします。

capture *capture_name* {**type lacp interface** *interface_id* [**buffer** *buf_size*] [**packet-length** *bytes*] [**circular-buffer**] [**real-time** [**dump**] [**detail**]]

capture *capture_name* **interface cluster** [**buffer** *buf_size*] [**ethernet-type** *type*] [**packet-length** *bytes*] [**circular-buffer**] [**cp-cluster**] [**trace** [**trace-count** *number*]] [**real-time** [**dump**] [**detail**]] [**trace**] [**match** *protocol* {**host** *source-ip* | *source-ip mask* | **any** | **any4** | **any6**} [*operator src_port*] {**host** *dest_ip* |*dest_ip mask* | **any** | **any4** | **any6**} [*operator dest_port*]]

クラスタ全体のパケットをキャプチャします。

cluster exec capture *capture_name* [**persist**] [**include-decrypted**]

永続的なパケットトレースクラスタ全体をクリアします。

cluster exec clear packet-trace

パケットキャプチャを削除します。

no capture *capture_name* [*arguments*]

パケットキャプチャを手動で開始または停止します。

capture *capture_name* **stop**

no capture *capture_name* **stop**

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	すべての IPv4 トラフィックを指定します。
any4	すべての IPv4 トラフィックを指定します。
any6	すべての IPv6 トラフィックを指定します。
all	高速セキュリティ パスでドロップされるすべてのパケットをキャプチャします。

asa_dataplane	ASA とバックプレーンを使用するモジュール（ASA FirePOWER モジュールなど）の間を通過する ASA バックプレーンのパケットをキャプチャします。
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。このキーワードは、**packet-length**、**circular-buffer**、および **buffer** の各キーワードとともに入力できますが、**interface** キーワードや **ethernet-type** キーワードとともに入力することはできません。クラスタでは、ドロップされた、ユニット間の転送データ パケットもキャプチャされます。マルチ コンテキスト モードでは、このオプションがシステム実行スペースで発行されると、すべてのドロップされたデータ パケットがキャプチャされます。このオプションがコンテキストで発行されたときは、ドロップされたデータ パケットのうち、そのコンテキストに属するインターフェイスから入ったものだけがキャプチャされます。
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。クラスタ内で使用されるときは、これはユニットあたりのサイズです（全ユニットの合計ではありません）。
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。
cp-cluster	（任意）クラスタ インターフェイスで制御パケットをキャプチャします。
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。サポートされるイーサネット タイプには、8021Q、ARP、IP、IP6、LACP、PPPOED、PPPOES、RARP、および VLAN などがあります。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。
include-decrypted	（オプション）ファイアウォールデバイスに入った時点で、通常のトラフィックと復号化されたトラフィックの両方を含む復号化された IPsec パケットをキャプチャします。
inline-tag *tag*	特定の SGT 値のタグを指定するか、または未指定のままにしてすべての SGT 値のタグ付きパケットをキャプチャします。
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。**type asp-drop** を除いて、パケットをキャプチャするには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 のデータプレーン、管理プレーン、またはコントロール プレーンでパケットをキャプチャするには、**interface** キーワードを **asa_dataplane**、**asa_mgmt_plane**、または **cplane** とともにインターフェイス名として指定できます。インターフェイス名として **cluster** を指定すると、クラスタ制御リンク インターフェイスでトラフィックをキャプチャできます。キャプチャのタイプとして **lacp** が設定されている場合は、インターフェイス名は物理名です。
ikev1 または **ikev2**	IKEv1 または IKEv2 プロトコル情報だけをキャプチャします。

isakmp	(オプション)VPN 接続の ISAKMP トラフィックをキャプチャします。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 パーサーを満足させるために物理、IP、および UDP の各レイヤを 1 つにまとめ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。
lacp	(オプション)LACP トラフィックをキャプチャします。設定されている場合は、インターフェイス名は物理インターフェイス名です。
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。ASA では、ネットワーク マスク(たとえば、Class C マスクの 255.255.255.0)が使用されます。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 *protocol*	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 • **neq**:等しくない • **range**:範囲
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。
persit	(オプション)クラスタユニットで永続的なパケットをキャプチャします。
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。
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 パケット キャプチャを終了するには、**Ctrl + c** を入力します。キャプチャを完全に削除するには、このコマンドの **no** 形式を使用します。このオプションは、**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。このオプションは、**cluster exec capture** コマンドを使用するときはサポートされません。
reinject-hide	(オプション)再注入されたパケットがキャプチャされないことを指定します。クラスタリング環境でだけ適用されます。
stop	(任意)手動でキャプチャを削除せずに停止します。キャプチャを開始するには、このコマンドの **no** 形式を使用します。
tls-proxy	(オプション)復号化された着信データおよび発信データを 1 つ以上のインターフェイス上の TLS プロキシからキャプチャします。
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。このオプションをアクセス リストとともに使用すると、トレース パケットがデータ パスに挿入されるので、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できます。
type	(任意)キャプチャされるデータのタイプを指定します。

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 パケットです。
- 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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
6.2(1)	このコマンドが追加されました。
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)	ASA 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。
8.4(1)	新しい **type** キーワードの **ikev1** と **ikev2** が追加されました。
8.4(2)	IDS の出力に追加の詳細が追加されました。
8.4(4.1)	バックプレーン経由の ASA CX モジュールへのトラフィックをサポートするために **asa_dataplane** オプションが追加されました。
9.0(1)	**cluster**、**cluster exec**、および **reinject-hide** キーワードが追加されました。新しい **type** オプションの **lacp** が追加されました。ISAKMP についてマルチ コンテキスト モードのサポートが追加されました。
9.1(3)	ASA CX バックプレーンでキャプチャされたパケットのフィルタリングが **asa_dataplane** オプションによってサポートされるようになりました。
9.2(1)	ASA FirePOWER モジュールをサポートするように **asa_dataplane** オプションが拡張されました。
9.3(1)	SGT およびイーサネット タギング機能をサポートするために **inline-tag** *tag* のキーワードと引数のペアが追加されました。

リリース	変更内容
9.6(2)	**type asp-drop** のパケット キャプチャは、ACL と一致フィルタリングをサポートします。
9.7(1)	パケット キャプチャを手動で停止したり開始したりするために、**stop** キーワードを追加しました。
9.8(1)	このコマンドは、ボックス クラッシュ時にすべてのアクティブなキャプチャの内容をフラッシュまたはディスク上のファイルに保存するように更新されました。
9.9(1)	クラスタリングの永続的トレースおよび復号化されたパケットのキャプチャがサポートされるようになりました。新しいオプションとして **persist** および **include-decrypted** が追加されました。 また、IPX は 3 つの異なるイーサネット タイプに対応するため、**ethernet-type ipx** が削除されました。代わりに、キャプチャする IPX タイプの 16 進数値を使用します。
9.10(1)	**match** オプションで IPv4 と IPv6 のネットワーク トラフィックをそれぞれキャプチャするために、**any4** および **any6** キーワードを追加しました。
9.12(1)	クラスタ インターフェイスで制御パケットをキャプチャするために、**cp-cluster** を追加しました。

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。**capture** コマンドは、実行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。

ASA では、通過するすべての IP トラフィックを追跡でき、すべての管理トラフィック（SSH トラフィック、Telnet トラフィックなど）を含む、着信するすべての IP トラフィックをキャプチャできます。

ASA のアーキテクチャは、パケット処理のための異なる 3 セットのプロセッサで構成されています。このアーキテクチャに起因して、キャプチャ機能の性能に一定の制限が加わります。通常は、ASA のパケット転送機能の大部分が 2 個のフロントエンド ネットワーク プロセッサで処理され、アプリケーション インスペクションが必要なパケットに限り、コントロール プレーン汎用プロセッサに送信されます。パケットがセッション管理パス ネットワーク プロセッサに送信されるのは、高速パス プロセッサで処理されないセッションがある場合だけです。

ASA によって転送またはドロップされるすべてのパケットがこの 2 つのフロントエンド ネットワーク プロセッサを通るため、パケット キャプチャ機能はこれらのネットワーク プロセッサに実装されています。したがって、該当するトラフィック インターフェイス用の適切なキャプチャが設定されていれば、ASA を通過するすべてのパケットをこれらのフロントエンド プロセッサでキャプチャできます。入力側では、ASA インターフェイスに到着した時点でパケットがキャプチャされ、出力側では、ネットワークに送信される直前でパケットがキャプチャされます。

（注） WebVPN キャプチャをイネーブルにすると、ASA 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。

キャプチャの保存

ASA 上のすべてのアクティブなキャプチャの内容は、ボックスがクラッシュしたときに保存されます。

トラブルシューティング プロセスの一部としてキャプチャをアクティブ化する場合は、次の点に注意する必要があります。

- 使用するキャプチャ バッファのサイズ、およびフラッシュまたはディスクに十分なスペースがあるかどうか。
- キャプチャされたパケットがクラッシュ前の最新のものになるように、キャプチャ バッファはすべての使用例で円形としてマークする必要があります。

アクティブなキャプチャの内容を保存するファイルの名前は、次の形式となります。

[<context_name>.]<capture_name>.pcap

context_name は、マルチコンテキスト モードでキャプチャがアクティブになっているユーザ コンテキストの名前を示します。シングル コンテキスト モードでは、*context_name* は適用されません。

capture_name は、アクティブ化されたキャプチャの名前を示します。

キャプチャの保存は、コンソールまたはクラッシュ ダンプの前に行われます。これにより、33 MB のキャプチャ バッファでクラッシュのダウンタイムが約 5 秒増加します。キャプチャしたコンテンツをファイルにコピーするのは簡単なプロセスなので、ネストされたクラッシュのリスクは最小限です。

キャプチャの表示

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://***ASA-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。

キャプチャの停止と開始

パケットをバッファから削除することなく、パケット キャプチャを停止することができます。キャプチャ停止のステータスが表示されます。キャプチャされたパケットは、バッファ内に保持されます。

パケット キャプチャを手動で停止するには、次のコマンドを使用します。

capture *name* **stop**

パケット キャプチャを開始するには、次のコマンドを使用します。

no capture *name* **stop**

キャプチャの削除

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。キャプチャを保持するには、**access-list** または **interface** キーワードを指定します。キャプチャは指定した ACL またはインターフェイスから分離されて保持されます。

リアルタイム操作

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。

クラスタ

capture コマンドの前に **cluster exec** を指定すると、あるユニットで **capture** コマンドを発行し、そのコマンドを他のすべてのユニットで同時に実行できます。クラスタ全体のキャプチャを実行した後、同じキャプチャ ファイルをクラスタ内のすべてのユニットから同時に TFTP サーバにコピーするには、マスター ユニットで **cluster exec copy** コマンドを入力します。

```
ciscoasa# cluster exec capture capture_name arguments
ciscoasa# cluster exec copy /pcap capture: cap_name tftp://location/path/filename.pcap
```

複数の PCAP ファイル（各ユニットから 1 つずつ）が TFTP サーバにコピーされます。宛先のキャプチャ ファイル名には自動的にユニット名が付加され、filename_A.pcap、filename_B.pcap などとなります。この例では、A と B がクラスタ ユニット名です。

トレースをクラスタ ユニットでキャプチャする場合、トレースは、バッファから手動でクリアされるまで、各クラスタ ノードに永続します。復号化された IPsec パケットは、ASA に入るとキャプチャされます。キャプチャされたパケットには、通常のトラフィックとカプセル化解除されたトラフィックの両方が含まれます。

（注） ファイル名の末尾にユニット名を追加すると、別の宛先名が生成されます。

制限事項

次に、キャプチャ機能の制限の一部を示します。制限の大部分は、ASA のアーキテクチャが本質的に分散型であることと、ASA で使用するハードウェア アクセラレータを原因としています。

- コンテキスト内のクラスタ制御リンクでキャプチャを設定できます。この場合、そのクラスタ制御リンクで送信されるコンテキストに関連付けられているパケットだけがキャプチャされます。
- 共有 VLAN には、次のガイドラインが適用されます。
  - VLAN ごとに設定できるキャプチャは 1 つだけです。共有 VLAN の複数のコンテキストでキャプチャを設定した場合は、最後に設定したキャプチャだけが使用されます。
  - 最後に設定した（アクティブ）キャプチャを削除した場合は、別のコンテキストで事前に設定したキャプチャがあっても、アクティブになるキャプチャはありません。キャプチャをアクティブにするには、キャプチャを削除して追加し直す必要があります。
  - キャプチャを指定したインターフェイス（キャプチャ アクセス リストと一致するインターフェイス）に着信するすべてのトラフィックがキャプチャされます。これには、共有 VLAN の他のコンテキストへのトラフィックが含まれます。
  - したがって、ある VLAN のコンテキスト A でのキャプチャをイネーブルにしたときに、その VLAN がコンテキスト B でも使用される場合は、コンテキスト A とコンテキスト B の両方の入力トラフィックがキャプチャされます。
- 出力トラフィックの場合は、アクティブ キャプチャのあるコンテキストのトラフィックだけがキャプチャされます。唯一の例外は、ICMP 検査をイネーブルにしない（したがって、ICMP トラフィックのセッションが高速パスにない）場合です。この場合は、共有 VLAN のすべてのコンテキストで入力と出力の ICMP トラフィックがキャプチャされます。

- キャプチャを設定する場合、通常は、キャプチャする必要のあるトラフィックを照合するアクセス リストを設定します。トラフィック パターンを照合するアクセス リストの設定が終われば、キャプチャを定義し、キャプチャを設定するインターフェイスとともに、このアクセス リストをキャプチャに関連付ける必要があります。キャプチャは、アクセス リストおよびインターフェイスと、IPv4 トラフィックをキャプチャするためのキャプチャを関連付けた場合に限り機能することに注意してください。IPv6 トラフィックの場合、アクセス リストは不要です。
- ASA CX モジュール トラフィックの場合、キャプチャされたパケットに含まれている追加 AFBP ヘッダーを、PCAP ビューアが認識しないことがあります。このようなパケットを表示するには、適切なプラグインを使用してください。
- インライン SGT タグ付きパケットの場合、キャプチャされたパケットに含まれている追加 CMD ヘッダーを、PCAP ビューアが認識しないことがあります。
- 受信側インターフェイスがないためグローバル インターフェイスがない場合、バックプレーン上で送信されるパケットは、システム コンテキストの制御パケットとして扱われます。これらのパケットはアクセス リスト チェックをバイパスし、常にキャプチャされます。この動作は、シングル モードとマルチ コンテキスト モードの両方に適用されます。
- 特定の asp-drop をキャプチャする場合に適切な理由を表示するには、**show capture** コマンドを使用します。ただし、**show capture** コマンドは、すべての asp-drop をキャプチャする場合は適切な理由を表示しません。

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。

```
ciscoasa# capture captest interface inside
ciscoasa# capture captest interface outside
```

Web ブラウザで、発行した「captest」という名前の **capture** コマンドの内容を表示できます。次の場所にあります。

```
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、ASA ボックスがクラッシュしたときにシングルモードでパケットをキャプチャする例を示します。

```
ciscoasa# capture 123 interface inside
```

キャプチャ「123」のコンテンツは、*123.pcap* ファイルとして保存されます。

次に、ASA ボックスがクラッシュしたときにマルチモードでパケットをキャプチャする例を示します。

```
ciscoasa# capture 456 interface inside
```

「管理」コンテキスト内のキャプチャ「456」のコンテンツは、*admin.456.pcap* ファイルとして保存されます。

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。

```
ciscoasa# access-list http permit tcp host 10.120.56.15 eq http host 171.71.69.234
ciscoasa# access-list http permit tcp host 171.71.69.234 host 10.120.56.15 eq http
ciscoasa# 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。

```
ciscoasa# 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。

次の例では、キャプチャされたパケットをリアルタイムで表示する方法を示します。

```
ciscoasa# 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
```

次の例では、キャプチャする必要のある IPv4 トラフィックを照合する拡張アクセス リストを設定する方法を示します。

```
ciscoasa (config)# access-list capture extended permit ip any any
```

次の例では、キャプチャを設定する方法を示します。

```
ciscoasa (config)# capture name access-list acl_name interface interface_name
```

デフォルトでは、キャプチャを設定すると、512 KB のサイズのリニア キャプチャ バッファが作成されます。オプションで循環バッファを設定できます。デフォルトでは、パケットの 68 バイトだけがバッファにキャプチャされます。オプションでこの値を変更できます。

次に、事前に設定されたキャプチャ アクセス リストを使用し、outside インターフェイスに適用される「ip-capture」というキャプチャを作成する例を示します。

```
ciscoasa (config)# capture ip-capture access-list capture interface outside
```

次の例では、キャプチャを表示する方法を示します。

```
ciscoasa (config)# show capture name
```

次の例では、キャプチャを終了する一方でバッファを保持する方法を示します。

```
ciscoasa (config)# no capture name access-list acl_name interface interface_name
```

次の例では、キャプチャを終了し、バッファを削除する方法を示します。

```
ciscoasa (config)# no capture name
```

次の例では、シングル モードでバックプレーンでキャプチャされたトラフィックをフィルタリングする方法を示します。

```
ciscoasa# capture x interface asa_dataplane access-list any4
ciscoasa# capture y interface asa_dataplane match ip any any
```

（注） 制御パケットは、アクセス リストを指定した場合にも、シングル モードでキャプチャされます。

次の例では、マルチ コンテキスト モードでバックプレーンでキャプチャされたトラフィックをフィルタリングする方法を示します。

ユーザ コンテキストでの使用方法:

```
ciscoasa (contextA)# capture x interface asa_dataplane access-list any4
ciscoasa (contextA)# capture y interface asa_dataplane match ip any any
```

システム コンテキストでの使用方法:

```
ciscoasa# capture z interface asa_dataplane
```

(注) マルチ コンテキスト モードでは、**access-list** オプションと **match** オプションはシステム コンテキストで使用できません。

クラスタリングでのキャプチャ

クラスタ内のすべてのユニットでのキャプチャをイネーブルにするには、これらの各コマンドの前に **cluster exec** キーワードを追加します。

次の例では、クラスタリング環境の LACP キャプチャを作成する方法を示します。

```
ciscoasa (config)# capture lacp type lacp interface gigabitEthernet0/0
```

次の例では、クラスタリング リンクでの制御パス パケットのキャプチャを作成する方法を示します。

```
ciscoasa (config)# cap cp interface cluster match udp any eq 49495 any
ciscoasa (config)# cap cp interface cluster match udp any any eq 49495
```

次の例では、クラスタリング リンクでのデータ パス パケットのキャプチャを作成する方法を示します。

```
ciscoasa (config)# access-list cc1 extended permit udp any any eq 4193
ciscoasa (config)# access-list cc1 extended permit udp any eq 4193 any
ciscoasa (config)# capture dp interface cluster access-list cc1
```

次の例では、クラスタを通過するデータ パス トラフィックをキャプチャする方法を示します。

```
ciscoasa (config)# capture abc interface inside match tcp host 1.1.1.1 host 2.2.2.2 eq www
ciscoasa (config)# capture abc interface inside match dup host 1.1.1.1 any
ciscoasa (config)# capture abc interface inside access-list xxx
```

次の例では、指定した実際の発信元から実際の宛先へのフローに対する論理アップデート メッセージをキャプチャし、指定した実際の発信元から実際の宛先へ CCL を介して転送されるパケットをキャプチャする方法を示します。

```
ciscoasa (config)# access-list dp permit real src real dst
```

次の例では、特定タイプのデータ プレーン メッセージ(たとえば ICMP エコー要求/応答)のうち、ある ASA から別の ASA に転送されたものを、メッセージ タイプに応じた **match** キーワードまたはアクセス リストを使用してキャプチャする方法を示します。

```
ciscoasa (config)# capture capture_name interface cluster access-list match icmp any any
```

次の例では、クラスタリング環境内のクラスタ制御リンク上でアクセス リスト 103 を使用してキャプチャを作成する方法を示します。

```
ciscoasa (config)# access-list 103 permit ip A B
ciscoasa (config)# capture example1 interface cluster
```

前の例で、A と B が CCL インターフェイスの IP アドレスである場合は、この 2 つのユニット間で送信されるパケットだけがキャプチャされます。

A および B が、デバイスを通過するトラフィックの IP アドレスである場合は、次のことが当てはまります。

- 転送されたパケットは、通常どおりにキャプチャされます。ただし、送信元および宛先の IP アドレスがアクセス リストに一致することが条件です。
- データ パス ロジック アップデート メッセージがキャプチャされるのは、そのメッセージが A と B の間のフローに対するものであるか、特定のアクセス リスト（たとえば、access-list 103）に対するものである場合です。埋め込まれたフローの 5 タプルが一致するものがキャプチャされます。
- UDP パケットの送信元と宛先のアドレスは CCL のアドレスですが、このパケットがフローを更新するためのものであり、そのフローにアドレス A および B が関連付けられている場合は、このパケットもキャプチャされます。つまり、パケットに埋め込まれているアドレス A および B が一致している限り、そのパケットもキャプチャされます。

次の例では、persistent オプションを使用してキャプチャを設定する方法を示します。

```
cluster2-asa5585a(config)# cluster exec capture test interface outside trace persist
  a(LOCAL):*******************************************************
  cluster2-asa5585a(config)#
```

これで、トラフィックを送信できるようになりました。

```
cluster2-asa5585a(config)# cluster exec show packet-tracer
  a(LOCAL):*******************************************************
  tracer 29/25 (allocate/freed), handle 29/25 (allocated/freed), error 0
  =======  Tracer origin-id a:23, hop 0 =======
  packet-id: Protocol: 0 src-port: 0 dst-port: 0

  Phase: 1
  Type: CAPTURE
  Subtype:
  Result: ALLOW
  Config:
  Additional Information:
  MAC Access list

  Phase: 2
  Type: ACCESS-LIST
  Subtype:
  Result: DROP
  Config:
  Implicit Rule
  Additional Information:
  MAC Access list

  Result:
  input-interface: outside
  input-status: up
  input-line-status: up
  Action: drop
  Drop-reason: (l2_acl) FP L2 rule drop
```

次の例では、メモリの一部を開放するためには、キャプチャされた永続的なトレースをボックスからクリアする必要があることが示されています。

```
ciscoasa# cluster exec clear packet-trace
```

次に、include-decrypted オプションを使用してキャプチャを設定する例を示します。

```
cluster2-asa5585a(config)# cluster exec show capture
  a(LOCAL):**************************************************************
  capture in type raw-data trace interface outside include-decrypted [Capturing – 588
bytes]
  capture out type raw-data trace interface outside include-decrypted [Capturing - 420
bytes]
  cluster2-asa5585a(config)#
```

これで、IPSec トンネルを介して ICMP トラフィックを送信できるようになりました。説明したとおり、キャプチャ コマンドは復号化された ICMP パケットを取得します。

```
cluster2-asa5585a(config)# cluster exec show capture in | i icmp
  a(LOCAL):**************************************************************
  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture out | i icmp
  a(LOCAL):**************************************************************
  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture in | i icmp
  a(LOCAL):**************************************************************
     8: 07:22:57.065014       802.1Q vlan#212 P0 211.1.1.1 > 213.1.1.2: icmp: echo request
  b:**********************************************************************
  cluster2-asa5585a(config)# cluster exec show capture out | i icmp
  a(LOCAL):**************************************************************
    10: 07:22:57.068004       802.1Q vlan#214 P0 213.1.1.2 > 211.1.1.1: icmp: echo reply
  b:**********************************************************************
  cluster2-asa5585a(config)#
```

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、「config」ディレクトリに変更する例を示します。

```
ciscoasa# 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 ASA 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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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。

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

証明書

指定した証明書を追加するには、crypto 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。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

ca	証明書が CA 発行の証明書であることを示します。
certificate-serial-number	証明書のシリアル番号を 16 進形式で指定し、末尾に「quit」という語を指定します。
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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドを発行する場合、ASA 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。

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 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。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crypto ca certificate chain central
ciscoasa(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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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。

```
ciscoasa(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名の識別名(DN)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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

このコマンドの入力には、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。

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。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# chain
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

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

change-password

ユーザが自分のアカウント パスワードを変更できるようにするには、特権 EXEC モードで **change-password** コマンドを使用します。

change-password [**/silent**] [**old-password** *old-password* [**new-password** *new-password*]]

構文の説明

new-password *new-password*	新しいパスワードを指定します。
old-password *old-password*	ユーザを再認証します。

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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	—	—	• 対応
グローバル コンフィギュレーション	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(4.1)	このコマンドが追加されました。

使用上のガイドライン

ユーザがパスワードを省略すると、ASA から入力を求めるプロンプトが表示されます。ユーザが **change-password** コマンドを入力すると、実行コンフィギュレーションを保存するように求められます。ユーザが正常にパスワードを変更した後、ユーザに設定変更を保存するように再通知するメッセージが表示されます。

例

次に、ユーザ アカウントのパスワードを変更する例を示します。

```
ciscoasa# change-password old-password myoldpassword000 new password mynewpassword123
```

関連コマンド

コマンド	説明
show run password-policy	現在のコンテキストのパスワード ポリシーを表示します。
clear configure password-policy	現在のコンテキストのパスワード ポリシーをデフォルト値にリセットします。
clear configure username	ユーザ アカウントからユーザ名を削除します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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 モードで編集したか、あるいは **copy** または **write** コマンドで使用した「実行」コンフィギュレーションは、その時点での実行スペースによって異なります。現在の実行スペースがシステム実行スペースの場合、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の場合、実行コンフィギュレーションは、そ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。

```
ciscoasa/admin# changeto system
ciscoasa# changeto context customerA
ciscoasa/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。実行スペースを変更するときにコンフィギュレーション モードを開始している場合、モードは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 モードに変わります。

```
ciscoasa(config-if)# changeto context admin
ciscoasa/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。

channel-group

EtherChannel に物理インターフェイスを割り当てるには、インターフェイス コンフィギュレーション モードで **channel-group** コマンドを使用します。インターフェイスの割り当てを解除するには、このコマンドの **no** 形式を使用します。

channel-group *channel_id* **mode** {**active** | **passive** | **on**} [**vss-id** {**1** | **2**}]

no channel-group *channel_id*

構文の説明

channel_id	このインターフェイスに割り当てる EtherChannel を 1 ～ 48 の範囲で指定します。
vss-id {**1** | **2**}	（オプション）クラスタリングでは、VSS または vPC の 2 台のスイッチに ASA を接続する場合は、このインターフェイスをどのスイッチに接続するかを指定するために **vss-id** キーワードを設定します（1 または 2）。また、**port-channel span-cluster vss-load-balance** コマンドをポートチャネル インターフェイスに対して使用する必要があります。
mode {**active** | **passive** | **on**}	EtherChannel 内の各物理インターフェイスを次のように設定できます。 • アクティブ：Link Aggregation Control Protocol（LACP）アップデートを送受信します。アクティブ EtherChannel は、アクティブまたはパッシブ EtherChannel と接続を確立できます。LACP トラフィックを最小にする必要がある場合以外は、アクティブ モードを使用する必要があります。 • パッシブ：LACP アップデートを受信します。パッシブ EtherChannel は、アクティブ EtherChannel のみと接続を確立できます。 • オン：EtherChannel は常にオンであり、LACP は使用されません。「オン」の EtherChannel は、別の「オン」の EtherChannel のみと接続を確立できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(1)	ASA クラスタリングおよびスパンド EtherChannel をサポートするために **vss-id** キーワードが追加されました。

使用上のガイドライン

チャネル グループ 1 つにつき 8 個のインターフェイスをアクティブにすることができます。1 つのチャネル グループに最大 16 個のインターフェイスを割り当てることができます。アクティブにできるインターフェイスは 8 個のみですが、残りのインターフェイスはインターフェイスに障害が発生した場合のスタンバイ リンクとして動作できます。

チャネル グループのすべてのインターフェイスは、同じタイプと速度である必要があります。チャネル グループに追加された最初のインターフェイスによって、正しいタイプと速度が決まります。

このチャネル ID のポートチャネル インターフェイスがコンフィギュレーションにまだ存在しない場合、ポートチャネル インターフェイスが作成されます。

interface port-channel *channel_id*

リンク集約制御プロトコル（LACP）では、2 つのネットワーク デバイス間でリンク集約制御プロトコル データ ユニット（LACPDU）を交換することによって、インターフェイスが集約されます。LACP では、ユーザが介入しなくても、EtherChannel へのリンクの自動追加および削除が調整されます。また、コンフィギュレーションの誤りが処理され、メンバ インターフェイスの両端が正しいチャネル グループに接続されていることがチェックされます。「オン」モードではインターフェイスがダウンしたときにチャネル グループ内のスタンバイ インターフェイスを使用できず、接続とコンフィギュレーションはチェックされません。

ASA クラスタリング

1 つの ASA につき複数のインターフェイスを、スパンド EtherChannel に入れることができます。1 つの ASA につき複数のインターフェイスが特に役立つのは、VSS または vPC の両方のスイッチに接続するときです。ASA を VSS または vPC の 2 台のスイッチに接続する場合は、**vss-load-balance** キーワードを使用して VSS ロード バランシングをイネーブルにする必要があります。この機能を使用すると、ASA と VSS（または vPC）ペアとの間の物理リンク接続の負荷が確実に分散されます。ロード バランシングをイネーブルにする前に、各メンバー インターフェイスに対して **channel-group** コマンドの **vss-id** キーワードを設定する必要があります。

例

次に、チャネル グループ 1 にインターフェイスを割り当てる例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/1
ciscoasa(config-if)# channel-group 1 mode active
ciscoasa(config-if)# interface GigabitEthernet0/2
ciscoasa(config-if)# channel-group 1 mode passive
```

関連コマンド

コマンド	説明
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。

コマンド	説明
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブ インターフェイスの最小数を指定します。
show lacp	LACP 情報（トラフィック統計情報、システム ID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

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。 この文字列は、大文字と小文字が区別されません。ASA 設定内では、コマンド インター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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

*文字エンコーディング*は「文字コード」や「文字セット」とも呼ばれ、raw データ（0 や 1 など）を文字と組み合わせ、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正しく処理できます。

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（CIFS）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 パスを正しく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。

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

関連コマンド

コマンド	説明
debug webvpn cifs	CIFS サーバに関するデバッギング メッセージを表示します。
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。

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。

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、ASA 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、ASA 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、ASA 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。
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 ASA を起動するときに、ASA はコード全体のハッシュを計算します。その後、ASA 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、ASA は「テキスト チェックサム チェックヒープ エラー」を発行します。エラーがある場合、ASA 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。

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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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)。

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。

```
ciscoasa(config)# checkheaps check-interval 200
ciscoasa(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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。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。

ASA 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 ASA 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。

```
ciscoasa(config)# access-list TCP extended permit tcp any any
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# check-retransmission
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match access-list TCP
ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap
ciscoasa(config)# service-policy pmap global
```

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。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。

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

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

ciscoasa(config)# policy-map pmap
ciscoasa(config-pmap)# class cmap
ciscoasa(config-pmap)# set connection advanced-options tmap

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

関連コマンド

コマンド	説明
class	トラフィック分類に使用するクラス マップを指定します。
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（廃止）

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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(4)	コマンドが追加されました。
9.4(1)	このコマンドは、すべての **phone-proxy** モード コマンドとともに廃止されました。

使用上のガイドライン

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 ソフトフォンが強制的に（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。

```
ciscoasa(config)# phone-proxy asa_phone_proxy
ciscoasa(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。

clacp static-port-priority

クラスタリング スパンド EtherChannel の LACP でダイナミック ポート プライオリティをディセーブルにするには、グローバル コンフィギュレーション モードで **clacp static-port-priority** コマンドを使用します。これは、アクティブ EtherChannel メンバーが 8 を超過する場合に必要となります。ダイナミック ポート プライオリティをイネーブルにするには、このコマンドの **no** 形式を使用します。

clacp static-port-priority

no clacp static-port-priority

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドはデフォルトでディセーブルです。ダイナミック ポート プライオリティはイネーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

一部のスイッチはダイナミック ポート プライオリティをサポートしていないため、このコマンドはスイッチの互換性を高めます。さらに、このコマンドは、9 ～ 32 のアクティブ スパンド EtherChannel メンバーのサポートをイネーブルにします。このコマンドを使用しないと、サポートされるのは 8 個のアクティブ メンバと 8 個のスタンバイ メンバのみです。

ASA EtherChannel は、最大 16 のアクティブ リンクをサポートします。スパンド EtherChannel では、vPC の 2 台のスイッチとともに使用し、**clacp static-port-priority** コマンドによってダイナミック ポート プライオリティをディセーブルにした場合、この機能はクラスタ全体で最大 32 のアクティブ リンクをサポートするように拡張されます。スイッチは、16 のアクティブ リンクを持つ EtherChannel をサポートする必要があります（Nexus 7000 の F2 シリーズ 10 ギガビット イーサネット モジュールなど）。

8 つのアクティブ リンクをサポートする VSS または vPC のスイッチの場合、スパンド EtherChannel に 16 のアクティブ リンクを設定できます（各スイッチに 8 つ接続）。

(注) スパンド EtherChannel で 8 つを超えるアクティブ リンクを使用する場合は、スタンバイ リンクも使用することはできません。9 ～ 32 のアクティブ リンクのサポートでは、スタンバイ リンクを使用できる cLACP ダイナミック ポート プライオリティをディセーブルにする必要があります。

例

次に、ダイナミック ポート プライオリティをディセーブルにする例を示します。

```
ciscoasa(config)# clacp static-port-priority
```

関連コマンド

コマンド	説明
clacp system-mac	cLACP システム ID を設定します。

clacp system-mac

ASA クラスタのマスター ユニットで cLACP システム ID を手動で設定する場合、クラスタ グループ コンフィギュレーション モードで **clacp system-mac** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

no clacp system-mac {*mac_address* | **auto**} [**system-priority** *number*]

構文の説明

mac_address	システム ID を *H.H.H* の形式で手動で設定します。H は 16 ビットの 16 進数の 1 桁です。たとえば、MAC アドレス 00-0A-00-00-AA-AA は、000A.0000.AAAA と入力します。
[auto]	システム ID を自動生成します。
system-priority *number*	システム プライオリティを 1 ～ 65535 の範囲で設定します。優先度はどのユニットがバンドルの決定を行うかを決定するため使用されます。デフォルトでは、ASA はプライオリティ 1（最高のプライオリティ）を使用します。このプライオリティは、スイッチのプライオリティよりも高いことが必要です。

コマンド デフォルト

デフォルトでは、システム MAC は自動生成されます（**auto**）。

デフォルトでは、system-priority は 1 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

スパンド EtherChannel を使用するときは、ASA は cLACP を使用してネイバー スイッチとの間で EtherChannel のネゴシエーションを行います。cLACP ネゴシエーションのときに、同じクラスタ内の ASA は互いに連携し、スイッチに対して全体で 1 つの（仮想）デバイスであるかのように見せます。cLACP ネゴシエーションのパラメータの 1 つであるシステム ID は、MAC アドレスの形式をとります。すべての ASA で同じシステム ID が使用されます。システム ID は、マスター ユニットによって自動生成され（デフォルト）、すべてのスレーブに複製されるか、このコマンドに手動で指定します。トラブルシューティングの目的で、たとえば、識別が容易な MAC アドレスを使用できるように、手動で MAC アドレスを設定することがあります。一般的には、自動生成された MAC アドレスを使用します。

このコマンドは、ブートストラップ コンフィギュレーションの一部ではなく、マスター ユニットからスレーブ ユニットに複製されます。ただし、クラスタリングをイネーブルにした後は、この値は変更できません。

例

次に、システム ID を手動で設定する例を示します。

```
cluster group pod1
    local-unit unit1
    cluster-interface port-channel1 ip 192.168.1.1 255.255.255.0
    priority 1
    key chuntheunavoidable
    health-check
    clacp system-mac 000a.0000.aaaa
    enable noconfirm
```

関連コマンド

コマンド	説明
cluster group	クラスタ パラメータを設定します。

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	トランスペアレント	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	• 対応	• 対応	—	—	• 対応

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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

ASA 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、ASA 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、ASA 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。

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

他のリソースはすべて無制限のままです。

gold というクラスを追加するには、次のコマンドを入力します。

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

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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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、CLI 設定ガイド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、CLI 設定ガイド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、CLI 設定ガイド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。

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

ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
to http server.
```

```
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

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

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

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

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

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

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。名前「class-default」と、「_internal」または「_default」で始まるすべて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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このタイプのクラス マップは、レイヤ 3/4 通過トラフィック専用です。ASA 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 ASA 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 ASA 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。

コンフィギュレーションの概要

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。

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

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

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

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

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

関連コマンド

コマンド	説明
class-map type management	ASA 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。 • **dcerpc** • **diameter** • **dns** • **FTP** • **h323** • **http** • **im** • **rtsp** • **scansafe** • **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。名前「class-default」と、「_internal」または「_default」で始まるすべて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。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	**match-any** キーワードが追加されました。
9.0(1)	**scansafe** キーワードが追加されました。
9.5(2)	**dcerpc** および **diameter** 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。

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

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。

```
ciscoasa(config-cmap)# class-map type inspect http match-any monitor-http
ciscoasa(config-cmap)# match request method get
ciscoasa(config-cmap)# match request method put
ciscoasa(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。
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 ASA 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。名前「class-default」と、「_internal」または「_default」で始まるすべて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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	ASA 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。

ASA 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。

```
ciscoasa(config)# class-map type management radius_acct
ciscoasa(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。名前「class-default」と、「_internal」または「_default」で始まるすべて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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークを使用すると、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。トラフィックに文字列「example.com」または「example2.com」が含まれる場合、トラフィックはクラス マップと一致します。

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

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	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 kerberos

Kerberos 情報をクリアするには、特権 EXEC モードで **clear aaa kerberos** コマンドを使用します。

clear aaa kerberos {**tickets** [**username** *user*] | **keytab**}

構文の説明

keytab	Kerberos キータブファイルをクリアします。
tickets [**username** *user*]	Kerberos チケット情報をクリアします。チケットをクリアするユーザを指定する username キーワードを含めない限り、すべてのチケットがクリアされます。

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.8(4)	**keytab** キーワードが追加されました。

例

次に、すべての Kerberos チケットをクリアする例を示します。

```
ciscoasa# clear aaa kerberos tickets
Proceed with deleting kerberos tickets? [confirm] y
```

次に、Kerberos キータブファイルを表示した後にクリアする例を示します。

```
ciscoasa# show aaa kerberos keytab
Principal:   host/asa2@BXB-WIN2016.EXAMPLE.COM
Key version: 10
Key type:    arcfour (23)
ciscoasa# clear aaa kerberos keytab
ciscoasa# show aaa kerberos keytab
No keys found
ciscoasa#
```

関連コマンド

コマンド	説明
show aaa kerberos	システム上のキャッシュされたすべての Kerberos チケット、またはキータブファイルを表示します。

clear aaa local user

ユーザをロック解除したり、ユーザの失敗した認証試行回数をゼロにリセットしたりするには、特権 EXEC モードで **clear aaa local user** コマンドを使用します。

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

構文の説明

all	ロックアウトされたすべてのユーザをロック解除するか、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。
failed-attempts	指定したユーザまたは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。
lockout	現在ロックアウトされているユーザをロック解除し、ユーザの失敗試行カウンタを 0 にリセットします。このオプションは、ロックアウトされていないユーザには影響を与えません。 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。
username *name*	ロック解除するか、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。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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、またはシステムをリブートすると、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、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。

```
ciscoasa# clear aaa local user fail-attempts username anyuser
ciscoasa#
```

次に、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。

```
ciscoasa# clear aaa local user fail-attempts all
ciscoasa#
```

次に、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。

```
ciscoasa# clear aaa local user lockout username anyuser
ciscoasa#
```

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。
show aaa local user	試行失敗カウンタおよびロックアウト ステータスを持つユーザ名のリストを表示します。

clear aaa sdi node-secret

RSA SecurID サーバのノードシークレットファイルを削除するには、特権 EXEC モードで **clear aaa sdi node-secret** コマンドを使用します。

clear aaa sdi node-secret *rsa_server_address*

構文の説明

rsa_server_address	ノードシークレットファイルを削除する RSA SecurID/Authentication Manager サーバの IP アドレスまたは完全修飾ホスト名。

デフォルト

デフォルト設定はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.15(1)	このコマンドが追加されました。

例

次に、ノードシークレットファイルのリストを表示し、その 1 つを削除する例を示します。必要に応じて、aaa sdi import-node-secret コマンドを使用して、サーバの新しいノードシークレットファイルをインポートしてください。

```
ciscoasa# show aaa sdi node-secrets
Last update                    SecurID server
--------------------           --------------------
15:16:13 Jun 24 2020           rsaam.example.com
15:20:07 Jun 24 2020           10.11.12.13
ciscoasa# clear aaa sdi node-secret rsaam.example.com
```

関連コマンド

コマンド	説明
aaa sdi import-node-secret	RSA SecurID Authentication Manager ノードシークレットファイルをインポートします。
show aaa sdi node-secrets	すべての SecurID ノードシークレットファイルを表示します。

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

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。
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。
protocol *protocol*	(任意) 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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	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例を示します。

```
ciscoasa(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例を示します。

```
ciscoasa(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例を示します。

```
ciscoasa(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例を示します。

```
ciscoasa(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。

コマンド モード	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	トランスペアレント	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	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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。

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。

```
ciscoasa# 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。

コマンド	説明
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	適応型セキュリティ 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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、すべての ARP 統計情報をクリアする例を示します。

```
ciscoasa# 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

高速セキュリティ パス(ASP)の統計情報をクリアするには、**clear asp** コマンドを使用します。

clear asp {**cluster counter** | **drop** [**flow** | **frame**] | **event dp-cp** | **queue-exhaustion** [**snapshot** *number*] | **load-balance history** | **overhead** | **table** [**arp** | **classify** | **filter** [**access-list** *acl_name*]]}

構文の説明

access-list *acl_name*	(任意)指定したアクセス リストのヒット カウンタだけをクリアします。
arp	(任意)ASP ARP テーブルのみでヒット カウンタをクリアします。
classify	(任意)ASP 分類テーブルのみでヒット カウンタをクリアします。
cluster counter	クラスタ カウンタをクリアします。
event	データ パスからコントロール プレーンへのイベントの統計情報をクリアします。
filter	(任意)ASP フィルタ テーブルのみでヒット カウンタをクリアします。
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)ドロップされたフレーム/パケット統計情報をクリアします。
load-balance history	パケット単位の ASP ロード バランシングの履歴をクリアし、自動切り替えが発生した回数をリセットします。
overhead	すべての ASP マルチプロセッサ オーバーヘッドの統計情報をクリアします。
queue-exhaustion	データ パス インスペクションの Snort キュー スナップショットをクリアします。
snapshot *number*	(任意)スナップショット ID 別にキューの枯渇をクリアします。
table	ASP ARP テーブルおよび ASP 分類テーブルのヒット 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。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
7.2(4)	**table** キーワードが追加されました。
8.2(2)	**filter** キーワードが追加されました。
9.3(1)	**load-balance history** キーワードが追加されました。

例

次に、すべての ASP テーブルの統計情報をクリアする例を示します。

```
ciscoasa# 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!ciscoasa#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!ciscoasa#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!ciscoasa(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!ciscoasa# 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
asp load-balance per-packet	ロード バランシング動作を変更します。
show asp load-balance	ロード バランサのキュー サイズのヒストグラムを表示します。
show asp load-balance per-packet	現在のステータス、最高水準点と最低水準点、およびグローバルなしきい値を表示します。
show asp load-balance per-packet history	現在のステータス、最高水準点と最低水準点、グローバルなしきい値、最後のリセット以降のパケットごとの ASP ロード バランシングのオンとオフの切り替え回数、タイム スタンプ付きのパケットごとの ASP ロード バランシングの履歴、およびオンとオフを切り替えた理由を表示します。
show asp	ASP 統計情報を表示します。

clear bfd counters

BFD カウンタをクリアするには、特権 EXEC モードで **clear bfd counters** コマンドを使用します。

clear bfd counters [ld *local_discr* **|** *interface_name* **| ipv4** *ip-address* **| ipv6** *ipv6-address***]**

構文の説明

ld *local_discr*	（任意）指定したローカル識別子の BFD カウンタをクリアします（1 - 4294967295）。
interface_name	（任意）指定したインターフェイスの BFD カウンタをクリアします。
ipv4 *ip_address*	（任意）指定したネイバー IP アドレスの BFD カウンタをクリアします。
ipv6 *ip_address*	（任意）指定したネイバー IPv6 アドレスの BFD カウンタをクリアします。

デフォルト

このコマンドは、すべての BFD カウンタをクリアします。

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

コマンド履歴

リリース	変更内容
9.6(2)	このコマンドが追加されました。

例

次に、すべての BFD カウンタをクリアする例を示します。

```
ciscoasa# clear bfd counters
```

関連コマンド

コマンド	説明
authentication	シングルホップ セッションとマルチホップ セッションの BFD テンプレートに認証を設定します。
bfd echo	インターフェイスで BFD エコー モードを有効にします。
bfd interval	インターフェイスにベースライン BFD パラメータを設定します。
bfd map	アドレスとマルチホップ テンプレートを関連付ける BFD マップを設定します。
bfd slow-timers	BFD スロー タイマー値を設定します。

コマンド	説明
bfd template	シングルホップ BFD テンプレートをインターフェイスにバインドします。
bfd-template single-hop | multi-hop	BFD テンプレートを設定し、BFD コンフィギュレーション モードを開始します。
echo	BFD シングルホップ テンプレートにエコーを設定します。
neighbor	BGP が登録され、BFD から転送パス検出失敗メッセージを受信できるように、BGP の BFD サポートを設定します。
show bfd drops	BFD でドロップされたパケットの数を表示します。
show bfd map	設定済みの BFD マップを表示します。
show bfd neighbors	既存の BFD 隣接関係の詳細なリストを表示します。
show bfd summary	BFD のサマリー情報を表示します。

clear bgp

ハードまたはソフト再構成を使用して Border Gateway Protocol（BGP）接続をリセットするには、特権 EXEC モードで **clear bgp** コマンドを使用します。

clear bgp {[***** | **external**] [**ipv4 unicast** [*as_number* | *neighbor_address* | **table-map**] | **ipv6 unicast** [*as_number* | *neighbor_address*]] [**soft**] [**in** | **out**] | *as_number* [**soft**] [**in** | **out**] | *neighbor_address* [**soft**] [**in** | **out**] | **table-map**}

構文の説明

*****	現在のすべての BGP セッションをリセットすることを指定します。
as_number	（任意）すべての BGP ピア セッションがリセットされる自律システムの番号。
external	外部のすべての BGP セッションをリセットすることを指定します。
in	（オプション）インバウンド再構成を開始します。**in** と **out** のどちらのキーワードも指定しない場合は、インバウンドとアウトバウンドの両方のセッションがリセットされます。
ipv4 unicast	IPv4 アドレス ファミリ セッションのハードまたはソフト再構成を使用して BGP 接続をリセットします。
ipv6 unicast	IPv6 アドレス ファミリ セッションのハードまたはソフト再構成を使用して BGP 接続をリセットします。
neighbor_address	（任意）指定された BGP ネイバーのみをリセットすることを指定します。この引数の値には、IPv4 アドレスまたは IPv6 アドレスを指定できます。
out	（オプション）インバウンド再構成またはアウトバウンド再構成を開始します。**in** と **out** のどちらのキーワードも指定しない場合は、インバウンドとアウトバウンドの両方のセッションがリセットされます。
soft	（任意）低速ピアのステータスを強制的にクリアして、元のアップデート グループに移します。
table-map	BGP ルーティング テーブルの table-map 設定情報をクリアします。このコマンドを使用して、BGP ポリシー アカウンティング機能で設定されたトラフィック インデックス情報をクリアできます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	• 対応

コマンド履歴

リリース	変更内容
9.2(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

clear bgp コマンドを使用して、ハード リセットまたはソフト再構成を開始できます。ハード リセットは、指定されたピアリング セッションを切断して再構築し、BGP ルーティング テーブルを再構築します。ソフト再構成は、保存されたプレフィックス情報を使用し、既存のピアリング セッションを切断せずに BGP ルーティング テーブルの再構成とアクティブ化を行います。ソフト再構成では、保存されているアップデート情報が使用されます。アップデートを保存するために追加のメモリが必要になりますが、ネットワークを中断せずに、新しい BGP ポリシーを適用することができます。ソフト再構成は、インバウンド セッション、またはアウトバウンド セッションに対して設定できます。

マルチ コンテキスト モードでは、**clear bgp *** コマンドだけがシステム実行スペースで使用可能です。

例

次の例では、システム実行スペースで **clear bgp** コマンドが指定されたときに、すべてのコンテキストですべての BGP セッションがリセットされます。このコマンドはすべての BGP セッションをリセットするため、アクションを確認する警告が表示されます。

```
ciscoasa# clear bgp *

This command will reset BGP in ALL contexts.
Are you sure you want to continue? [no]:
```

次の例では、すべての BGP セッションが、シングル モードまたはマルチ コンテキスト モードのコンテキストでリセットされます。

```
ciscoasa# clear bgp *
```

次の例では、ネイバー 10.100.0.1 とのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp 10.100.0.1 soft in
```

次の例では、ルート リフレッシュ機能が BGP ネイバー ルータでイネーブルになっており、ネイバー 172.16.10.2 とのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp 172.16.10.2 in
```

次の例では、自律システム番号 35700 のすべてのルータとのセッションに対してハード リセットが開始されます。

```
ciscoasa# clear bgp 35700
```

次の例では、すべてのインバウンド eBGP ピアリング セッションに対してソフト再構成が設定されます。

```
ciscoasa# clear bgp external soft in
```

次の例では、すべてのアウトバウンド アドレス ファミリ IPv4 マルチキャスト eBGP ピアリング セッションがクリアされます。

```
ciscoasa# clear bgp external ipv4 multicast out
```

次の例では、自律システム 65400 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーのインバウンド セッションに対してソフト再構成が開始され、アウトバウンド セッションは影響を受けません。

```
ciscoasa# clear bgp ipv4 unicast 65400 soft in
```

次の例では、asplain 表記の 4 バイトの自律システム番号 65538 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーに対してハード リセットが開始されます。

```
ciscoasa# clear bgp ipv4 unicast 65538
```

次の例では、asdot 表記の 4 バイトの自律システム番号 1.2 の IPv4 ユニキャスト アドレス ファミリ セッションで BGP ネイバーに対してハード リセットが開始されます。

```
ciscoasa# clear bgp ipv4 unicast 1.2
```

次の例は、IPv4 ユニキャスト ピアリング セッションのテーブル マップをクリアします。

```
ciscoasa# clear bgp ipv4 unicast table-map
```

clear blocks

枯渇状態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 [**exhaustion** {**history** | **snapshot**} | **export-failed** | **queue** [**history** [**core-local** [*number*]]]]

構文の説明

core-local [*number*]	（任意）すべてのコア、またはコア番号を指定する場合は特定のコアに対し、アプリケーションによってキューに入れられたシステム バッファをクリアします。
exhaustion	（任意）枯渇状態をクリアします。
export-failed	（任意）エクスポート失敗カウンタをクリアします。
history	（任意）履歴をクリアします。
queue	（任意）キューに入れられたブロックをクリアします。
snapshot	（任意）スナップショット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。

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.1(5)	**history** および **snapshot** オプションが追加されました。

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。

```
ciscoasa# 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 ASA 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または Cascading Style Sheet（CSS）パラメータ（それぞれ許容最大文字数は 256 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	トランスペアレント	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	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

style オプションは有効な 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。

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

関連コマンド

コマンド	説明
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。
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。
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** コマンドを使用します。

clear capture {**/all** | *capture_name*}

構文の説明

/all	すべてのインターフェイス上のパケットをクリアします。
capture_name	パケット キャプチャ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	トランスペアレント	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)	このコマンドが追加されました。

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。

```
ciscoasa(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 clns cache

Connectionless Network Service（CLNS）ルーティング キャッシュをクリアして再初期化するには、clear clns cache EXEC コマンドを使用します。

clear clns cache

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

使用上のガイドライン

ルーティング キャッシュ情報をクリアするには、**clear clns cache** コマンドを使用します。

例

次に、CLNS ルーティング キャッシュをクリアする例を示します。

```
ciscoasa# clear clns cache
```

関連コマンド

コマンド	説明
show clns cache	clns ルーティング キャッシュを表示します。

clear clns is-neighbors

隣接データベースから IS ネイバー情報を削除するには、clear clns is-neighbors EXEC コマンドを使用します。

clear clns is-neighbors

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

使用上のガイドライン

隣接データベースから IS ネイバー情報をクリアするには、**clear clns is-neighbors** コマンドを使用します。

例

次に、CLNS es-neighbor をクリアする例を示します。

```
ciscoasa# clear clns is-neighbors
```

関連コマンド

コマンド	説明
clear clns neighbors	clns ネイバー情報を削除します。
show clns is-neighbors	clns がネイバー情報であることを示します。

clear clns neighbors

隣接データベースから CLNS ネイバー情報を削除するには、clear clns neighbors EXEC コマンドを使用します。

clear clns neighbors

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

デフォルトの動作や値はありません。

コマンドモード

EXEC

使用上のガイドライン

隣接データベースからネイバー情報をクリアするには、**clear clns neighbors** コマンドを使用します。

例

次に、隣接データベースから CLNS ネイバー情報を削除する例を示します。

```
ciscoasa# clear clns neighbors
```

関連コマンド

コマンド	説明
clear clns is-neighbors	clns is-neighbor 情報を削除します。
show clns neighbors	clns ネイバー情報を表示します。

clear clns route

動的に導出されたすべての CLNS ルーティング情報を削除するには、clear clns route EXEC コマンドを使用します。

clear clns route

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

EXEC

使用上のガイドライン

ルーティング情報をクリアするには、**clear clns is-neighbors** コマンドを使用します。

例

次に、動的に導出されたすべての CLNS ルーティング情報を削除する例を示します。

```
ciscoasa# clear clns route
```

関連コマンド

コマンド	説明
show clns route	clns ルート情報を表示します。

clear cluster info

クラスタ統計情報をクリアするには、特権 EXEC モードで **clear cluster info** コマンドを使用します。

clear cluster info {flow-mobility counters | health details | trace | transport}

構文の説明

flow-mobility counters	クラスタ フローモビリティ カウンタをクリアします。
health details	クラスタ ヘルス情報をクリアします。
trace	クラスタ イベント トレース情報をクリアします。
transport	クラスタ転送統計情報をクリアします。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	トランスペアレント	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	• 対応	• 対応	• 対応	—	• 対応

コマンド履歴

リリース	変更内容
9.5(2)	**flow-mobility counters** キーワードが追加されました。
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

クラスタ統計情報を表示するには、**show cluster info** コマンドを使用します。

例

次に、クラスタ イベント トレース情報をクリアする例を示します。

```
ciscoasa# clear cluster info trace
```

関連コマンド

コマンド	説明
show cluster info	クラスタ統計情報を表示します。

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** | **anyconnect-ssl** | **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。
anyconnect-ssl	AnyConnect SSL 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	トランスペアレント	シングル	コンテキスト	システム
特権 EXEC	• 対応	—	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。
8.4(1)	SVC は AnyConnect SSL に置き換えられました。
9.5(2)	マルチ コンテキスト モードのサポートが追加されました。

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。