ca - cld

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

コマンド デフォルト

ディセーブル

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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 サーバーおよびエンド ユーザー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。

コマンド 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。

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

コマンド履歴

リリース	変更内容
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

イネーブル化	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。

コマンド デフォルト

ディセーブル

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

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

コマンド 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

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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。

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

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、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。

コマンド	説明
show running-config policy-map	現在のポリシーマップ コンフィギュレーションをすべて表示します。

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

例

次に、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。

コマンド	説明
show running-config policy-map	現在のポリシーマップ コンフィギュレーションをすべて表示します。

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

コマンド履歴

リリース	変更内容
8.2(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。デフォルトはすべてのアラートグループがイネーブルです。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。必須フィールドです。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：カスタマー名を指定します。e-mail-address：最大 127 文字のカスタマー名。
- [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：最大 23 文字の既存のプロファイル名。dest-profile-name：最大 23 文字の新しいプロファイル名。
- 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：最大 23 文字の既存のプロファイル名。dest-profile-name：最大 23 文字の新しいプロファイル名。
- no configuration all：Smart Call-home 設定をクリアします。[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 までのイベントの数。デフォルトは 10 です。
- [no] mail-server ip-address | name priority 1-100 all：SMTP メール サーバーを指定します。顧客は、最大 5 つのメール サーバーを指定できます。Smart Call Home メッセージの電子メール トランスポートを使用するには、少なくとも 1 つのメールサーバーが必要です。
  ip-address：メールサーバーの IPv4 または IPv6 アドレス。name：メールサーバーのホスト名。1 ー 100：メールサーバーの優先順位。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 分間当たりのメッセージの数。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：環境リソースのしきい値を指定します。low, high：有効な値は 0 ー 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：CLI を sysem またはユーザーコンテキストで実行します（マルチモードでのみ使用可能）。
- [no] add-command “cli command” [{system | user}]：スナップショットでキャプチャする CLI コマンドを指定します。cli command：入力する CLI コマンド。system, user：システムまたはユーザーコンテキストで CLI を実行します（マルチモードでのみ使用可能）。システム

もユーザーも指定しないと、CLI はシステム コンテキストとユーザー コンテキストの両方で実行されます。デフォルトは、ユーザー コンテキストです。

- 以下のすべての箇条書き項目は profile コマンドに移動します。
- [no] profile profile-name | no profile all：プロファイルの作成、削除、および編集を行います。プロファイル コンフィギュレーション モードを開始し、プロンプトを hostname (cfg-call-home-profile)# に変更します。profile-name：最大 20 文字のプロファイル名。
- [no] active：プロファイルをイネーブルまたはディセーブルにします。デフォルトはイネーブルです。no destination address {e-mail | http} all | [no] destination {address {e-mail | http} e-mail-address | http-url [msg-format short-text | long-text | xml] | message-size-limit max-size | preferred-msg-format short-text | long-text | xml | transport-method e-mail | http}：Smart Call Home メッセージ受信者の宛先、メッセージサイズ、メッセージ形式、および転送方法を設定します。デフォルトのメッセージ形式は XML で、デフォルトで有効になっている転送方式は e-mail です。e-mail-address：Smart Call Home レシーバの電子メールアドレス（最大 100 文字）。http-url：HTTP または HTTPS URL。max-size：最大メッセージサイズ（バイト単位）。0 は、制限がないことを意味します。デフォルトは 5 MB です。
- [no] subscribe-to-alert-group alert-group-name [severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging}]：指定した重大度レベルのグループのイベントにサブスクライブします。alert-group-name：有効な値は、syslog、diagnostic、environment、または threat です。
- [no] subscribe-to-alert-group syslog [{severity {catastrophic | disaster | emergencies | alert | critical | errors | warning | notifications | informational | debugging} | message start [-end]}]：重大度レベルまたはメッセージ ID のある syslog にサブスクライブします。start-[end]：1 つの syslog メッセージ ID またはある範囲の syslog メッセージ ID。
- [no] subscribe-to-alert-group inventory [periodic {daily | monthly day_of_month | weekly day_of_week [hh:mm]]：インベントリイベントにサブスクライブします。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。
- [no] subscribe-to-alert-group configuration [export full | minimum] [periodic {daily | month day_of_month | weekly day_of_week [hh：mm]]：設定イベントにサブスクライブします。full：実行コンフィギュレーション、スタートアップ コンフィギュレーション、機能リスト、アクセスリストの要素数、およびマルチモードのコンテキスト名をエクスポートするコンフィギュレーション。minimum：機能リスト、アクセスリスト内の要素数、およびマルチモードのコンテキスト名だけをエクスポートするコンフィギュレーション。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。
- [no] subscribe-to-alert-group telemetry periodic {hourly | daily | monthly day_of_month | weekly day_of_week [hh:mm]：テレメトリ定期イベントをサブスクライブします。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。
- [no] subscribe-to-alert-group snapshot periodic {interval minutes | hourly [mm] | daily | monthly day_of_month |weekly day_of_week [hh:mm]}：スナップショット定期イベントにサブスクラ

イブします。minutes：分単位の間隔。day_of_month：1 ～ 31 までの日付。day_of_week：曜日（日曜日、月曜日、火曜日、水曜日、木曜日、金曜日、土曜日）。hh, mm ：1 日の時間と分（24 時間形式）。

（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ー、セカンダリ電子メール サーバーなど）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。

コマンド	説明
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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

configuration	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。
inventory	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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.2(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。

コマンド 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。

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

コマンド 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。

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

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

コマンド履歴

リリース	変更内容
9.5(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ー 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**]] [**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** キーワードと一緒に入力できますが、**interface** または **ethernet-type** キーワードと一緒には入力できません。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。複数のトラフィックのタイプ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。また、SSL 復号トラフィックのパケットもキャプチャします。ただし、VTI からの復号化されたパケットはキャプチャに含まれません。これらは VTI インターフェイスでのみ使用でき、外部インターフェイスでは使用できないためです。
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 マスクを指定するときは、指定方法が Cisco IOS ソフトウェアの access-list コマンドとは異なることに注意してください。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**、**switch**、および **asp-drop** キャプチャにのみ適用されます。**cluster exec capture** コマンドを使用する場合、このオプション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ー名を指定します。
webvpn	（任意）特定の WebVPN 接続の WebVPN データをキャプチャします。

コマンド デフォルト

デフォルトの設定は次のとおりです。

- 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。

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

コマンド履歴

リリース	変更内容
6.2(1)	このコマンドが追加されました。
7.0(1)	このコマンドは、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)	このコマンドは、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 **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。

リリース	変更内容
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。
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：**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。
9.18(1)	リアルタイムのスイッチパケットキャプチャを有効にする **real-time** キーワードが含まれています。

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ー 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。**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 サーバーに 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 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無効にできます。

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 サーバーにコピーするには、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 サーバーにコピーされます。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** コマンドの内容を次の場所に表示できます。

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

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

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

次に、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 サーバー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。

ユーザー 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 ccl
```

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 ファイルをサーバーにコピーします。
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: （任意）リムーバブル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。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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サーバー 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。

コマンド 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。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

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サーバー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 サーバー 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 サーバー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 サーバーによって発行され、以前に失効した証明書の失効を取り消します。
lifetime crl	証明書失効リストのライフタイムを指定します。

certificate

指定した証明書を追加するには、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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
クリプト CA 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。

コマンド	説明
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。

コマンド デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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、ユーザー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。

コマンド デフォルト

このコマンドのデフォルト設定は、ディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
トンネル グループ ipsec 属性コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

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

ユーザー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*	ユーザーを再認証します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

ユーザー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。ユーザーが **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。ユーザーが正常にパスワードを変更した後、ユーザー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、ユーザー 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	ユーザー アカウントからユーザー名を削除します。

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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。

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

コマンド履歴

リリース	変更内容
8.4(1)	このコマンドが追加されました。
9.0(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
channel-group	EtherChannel にインターフェイスを追加します。
interface port-channel	EtherChannel を設定します。
lacp max-bundle	チャネル グループで許可されるアクティブ インターフェイスの最大数を指定します。
lacp port-priority	チャネル グループの物理インターフェイスのプライオリティを設定します。
lacp system-priority	LACP システム プライオリティを設定します。
port-channel load-balance	ロード バランシング アルゴリズムを設定します。
port-channel min-bundle	ポートチャネル インターフェイスがアクティブになるために必要な、アクティブインターフェイスの最小数を指定します。
show lacp	LACP情報（トラフィック統計情報、システムID、ネイバーの詳細など）が表示されます。
show port-channel	EtherChannel 情報が、詳細に 1 行のサマリー形式で表示されます。このコマンドは、ポートとポートチャネルの情報も表示します。
show port-channel load-balance	ポートチャネル負荷分散情報が、指定のパラメータ セットに対するハッシュ結果および選択されたメンバー インターフェイスとともに表示されます。

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.1(1)	このコマンドが追加されました。

使用上のガイドライン

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、ユーザー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、ユーザーは、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、ユーザーは、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）サーバーの 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 サーバー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 サーバーから WebVPN ユーザーにダウンロードされた WebVPN ポータル ページは、サーバーを識別する 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 ユーザーのブラウザでは、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 サーバー用の 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 サーバー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 サーバーに関するデバッギング メッセージを表示します。
file-encoding	CIFS サーバー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。

コマンド	説明
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。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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。

コマンド デフォルト

デフォルトではディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	シングル	マルチ	
				コンテキスト	システム
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**、**class**、および **description** コマンドの構文の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。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。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**、**class**、および **description** コマンドの構文の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。

コマンド 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。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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

tcp-map コマンドを使用して、TCP マップ コンフィギュレーション モードを開始します。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**、**class**、および **description** コマンドの構文の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。

コマンド 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。

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

コマンド履歴

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

使用上のガイドライン

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

コマンド履歴

リリース	変更内容
9.2(1)	このコマンドが追加されました。

使用上のガイドライン

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個より多くの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できません。9 ～ 32 個のアクティブリンクをサポートするには、スタンバイリンクの使用を可能にする 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* 形式で手動で設定します。*H*。*H*、H は 16 ビットの 16 進数です。たとえば、MAC アドレス00-0A-00-00-AA-AA は 000A.0000.AAAA と入力されます。
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。プライオリティは意思決定を担当するユニットの決定に使用されます。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。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。

使用上のガイドライン

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際に、同じクラスタ内の ASA は互いに連携するため、スイッチには 1 つの（仮想）デバイスであるかのように

見えます。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。デフォルトクラスの制限値を設定するには、名前として **default** と入力します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

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

ASAは、リソース クラスにコンテキストを割り当てることによって、リソースを管理します。各コンテキストでは、クラスによって設定されたリソース制限が使用されます。

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 のポリシーマップ（**policy-map** コマンド）の場合、レイヤ 3/4 クラスマップ名（**class-map** 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(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。
    1. **class**：アクションを実行するクラスマップを指定します。

2. *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。各機能で使用できるコマンドの詳細については、CLI コンフィギュレーション ガイドを参照してください。

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識別します。
2. **policy-map type inspect**：各クラスマップに関連付けるアクションを指定します。
    1. **class**：アクションを実行するインスペクション クラス マップを指定します。
    2. 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 コンフィギュレーション 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。
    3. パケットのドロップ
    4. 接続のドロップ
    5. 接続のリセット
    6. ロギング
    7. メッセージのレートの制限
    8. コンテンツのマスキング
    9. **parameters**：インスペクションエンジンに影響する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 コンフィギュレーション 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。
    1. **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。
    2. **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 サーバー 10.1.1.1 への接続許可数を制限します。

```
ciscoasa(config)# access-list http-server permit tcp any host 10.1.1.1
ciscoasa(config)# class-map http-server
ciscoasa(config-cmap)# match access-list http-server
ciscoasa(config)# policy-map global-policy
ciscoasa(config-pmap)# description This policy map defines a policy concerning connection
 to http server.
ciscoasa(config-pmap)# class http-server
ciscoasa(config-pmap-c)# set connection conn-max 256
```

次の例は、ポリシー マップでの複数の照合の動作を示しています。

```
ciscoasa(config)# class-map inspection_default
ciscoasa(config-cmap)# match default-inspection-traffic
ciscoasa(config)# class-map http_traffic
ciscoasa(config-cmap)# match port tcp eq 80
ciscoasa(config)# policy-map outside_policy
ciscoasa(config-pmap)# class inspection_default
ciscoasa(config-pmap-c)# inspect http http_map
ciscoasa(config-pmap-c)# inspect sip
ciscoasa(config-pmap)# class http_traffic
ciscoasa(config-pmap-c)# set connection timeout tcp 0:10:0
```

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

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

```
ciscoasa(config-pmap-c)# set connection timeout tcp 2:0:0
ciscoasa(config-pmap-c)# set connection conn-max 2000
```

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

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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

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 マップの最後に示され、原則的に、他のすべてのトラフィックでどのよう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、アクションを適用するレイヤ 3 およびレイヤ 4 のトラフィックを指定します。
2. （アプリケーション インスペクションのみ）**policy-map type inspect** コマンドを使用して、アプリケーション インスペクション トラフィックの特別なアクションを定義します。
3. **policy-map** コマンドを使用して、レイヤ 3 と 4 のトラフィックにアクションを適用します。
4. **service-policy** コマンドを使用して、インターフェイスでのアクションをアクティブにします。

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るトラフィックを指定する **match** コマンド（**matchtunnel-group** コマンドおよび **matchdefault-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*
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のデフォルトは **match-all** 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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	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 フレームワークでは、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。レイヤ 3/4 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場合は、インスペクション ポリシー マップで定義され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。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンドモード	ファイアウォールモード		セキュリティコンテキスト		
	ルーテッド	トランスペアレント	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)	**et connection** コマンドが、ASA への管理トラフィックにおいて、レイヤ 3/4 管理クラス マップでも使用できるようになりました。 **conn-max** キーワードと **embryonic-conn-max** キーワードのみ使用できます。

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 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 managementclass_map_name *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** は唯一のオプションです。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

モジュラ ポリシー フレームワークでは、多くのアプリケーション インスペクションで実行される特別なアクションを設定できます。レイヤ 3/4 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場合は、インスペクション ポリシー マップで定義され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。

コマンド	説明
regex	正規表現を作成します。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。