echo コマンド ～ extended-security コマンド

echo

BFD シングルホップ テンプレートでエコーを設定するには、BFD テンプレート コンフィギュレーション モードで **echo** コマンドを使用します。シングルホップ セッション用の BFD テンプレートでエコー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。

echo

no echo

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　このコマンドにデフォルトの動作または値はありません。

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
BFD 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
9.6(2)	このコマンドが追加されました。

使用上のガイドライン　シングルホップ テンプレートのみでエコー モード機能をイネーブルにするには、このコマンドを使用します。BFD エコーは、IPv6 BFD セッションではサポートされません。

例

次に、シングルホップ BFD テンプレートでエコーを設定する例を示します。

```
ciscoasa(config)# bfd-template single-hop template1
ciscoasa(config-bfd)# echo
```

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。
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。
clear bfd counters	BFD カウンタをクリアします。
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。

early-message

H.323 インスペクション中に H.255 SETUP メッセージの前にメッセージを許可するには、パラメータ コンフィギュレーション モードで **early-message** 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。

early-message *message_type*

no early-message *message_type*

構文の説明

message_type	H.225 SETUP メッセージの前に許可するメッセージのタイプです。次のタイプを入力できます。 • **facility**

デフォルト

このコマンドはディセーブルです。H.225 SETUP メッセージの前にメッセージは許可されず、接続がドロップされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
9.6(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

H.460.18 では、ネットワーク アドレス変換機能とファイアウォールを越えて H.323 シグナリングを伝送するための方法が定義されています。この方法を使用すると、H.225 FACILITY メッセージを H.225 SETUP メッセージの前に送信できます。H.323/H.225 を使用するときに、接続が完了前に終了するコール セットアップの問題が発生した場合、このコマンドを使用して早期メッセージを許可します。

また、必ず H.323 RAS と H.225 の両方にインスペクションをイネーブルにしてください(デフォルトではどちらもイネーブルになっています)。

例

次に、早期メッセージを許可する例を示します。

```
ciscoasa(config)# policy-map type inspect h323 h323_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# early-message FACILITY
```

関連コマンド

コマンド	説明
policy-map type inspect	インスペクション 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。

eigrp log-neighbor-changes

EIGRP ネイバーとの隣接関係の変更のロギングを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 **eigrp log-neighbor-changes** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-changes

no eigrp log-neighbor-changes

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

このコマンドは、デフォルトでイネ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
ルータ 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
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

eigrp log-neighbor-changes コマンドはデフォルトでイネーブルです。実行コンフィギュレーションには、コマンドの **no** 形式のみが表示されます。

例

次に、EIGRP ネイバーの変更のロギングをディセーブルにする例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-changes
```

関連コマンド

コマンド	説明
eigrp log-neighbor-warnings	ネイバー警告メッセージのロギングをイネーブルにします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp log-neighbor-warnings

EIGRP ネイバー警告メッセージのロギングを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 **eigrp log-neighbor-warnings** コマンドを使用します。この機能をオフにするには、このコマンドの **no** 形式を使用します。

eigrp log-neighbor-warnings [*seconds*]

no eigrp log-neighbor-warnings

構文の説明

seconds	（任意）ネイバー警告メッセージの反復間隔（秒数）。有効値は 1 ～ 65535 です。この間隔内に警告が繰り返し発生した場合、それらの警告はログに記録されません。

デフォルト

このコマンドは、デフォルトでイネーブルになっています。すべてのネイバー警告メッセージがログに記録されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

eigrp log-neighbor-warnings コマンドはデフォルトでイネーブルです。実行コンフィギュレーションには、コマンドの **no** 形式のみが表示されます。

例

次に、EIGRP ネイバーの警告メッセージのロギングをディセーブルにする例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# no eigrp log-neighbor-warnings
```

次に、EIGRP ネイバー警告メッセージをログに記録し、5 分（300 秒）間隔で警告メッセージを繰り返す例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp log-neighbor-warnings 300
```

関連コマンド

コマンド	説明
eigrp log-neighbor-messages	EIGRP ネイバーとの隣接関係に関する変更のロギングをイネーブルにします。
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp router-id

EIGRP ルーティング プロセスによって使用されるルータ ID を指定するには、ルータ コンフィギュレーション モードで **eigrp router-id** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

eigrp router-id *ip-addr*

no eigrp router-id [*ip-addr*]

構文の説明

ip-addr	IP アドレス形式（ドット付き 10 進形式）でのルータ ID。ルータ ID として 0.0.0.0 または 255.255.255.255 を使用することはできません。

デフォルト

指定しない場合、ASA 上で最上位の IP アドレスがルータ ID として使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

eigrp router-id コマンドが設定されていない場合、EIGRP プロセスが開始されたとき、EIGRP は、ルータ ID として使用するために、ASA 上で最上位の IP アドレスを自動的に選択します。EIGRP プロセスが **no router eigrp** コマンドによって削除されない限り、またはルータ ID が **eigrp router-id** コマンドによって手動で設定されていない限り、ルータ ID は変更されません。

ルータ ID は、外部ルートの発信元ルータを識別するために使用されます。外部ルートがローカルのルータ ID で受信された場合、このルートは廃棄されます。このような事態を回避するには、**eigrp router-id** コマンドを使用して、ルータ ID のグローバル アドレスを指定します。

各 EIGRP ルータには、一意の値を設定する必要があります。

例

次に、EIGRP ルーティング プロセスの固定ルータ ID として 172.16.1.3 を設定する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# eigrp router-id 172.16.1.3
```

関連コマンド

コマンド	説明
router eigrp	EIGRP ルーティング プロセスのルータ コンフィギュレーション モードを開始します。
show running-config router	グローバル ルータ コンフィギュレーションのコマンドを表示します。

eigrp stub

EIGRP ルーティング プロセスをスタブ ルーティング プロセスとして設定するには、ルータ コンフィギュレーション モードで **eigrp stub** コマンドを使用します。EIGRP スタブ ルーティングを削除するには、このコマンドの **no** 形式を使用します。

eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

no eigrp stub [**receive-only**] | {[**connected**] [**redistributed**] [**static**] [**summary**]}

構文の説明

接続	(任意)接続ルートをアドバタイズします。
receive-only	(任意)ASA を受信専用ネイバーとして設定します。
redistributed	(任意)他のルーティング プロトコルから再配布されたルートをアドバタイズします。
静的	(任意)スタティック ルートをアドバタイズします。
summary	(任意)集約ルートをアドバタイズします。

デフォルト

スタブ ルーティングはイネーブルになっていません。

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
ルータ 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
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

eigrp stub コマンドを使用して、ASA をスタブとして設定します。この場合、ASA では、すべての IP トラフィックがディストリビューション ルータに転送されます。

receive-only キーワードを使用すると、ASA が自律システム内の他のどのルータともルートを共有しないように設定できます。ASA は、EIGRP ネイバーからの更新のみを受信します。**receive-only** キーワードは他のキーワードと組み合わせて使用することはできません。

connected、**static**、**summary**、および **redistributed** の各キーワードは、1 つ以上を組み合わせて指定できます。これらのいずれかのキーワードを指定して **eigrp stub** コマンドを使用した場合、これらの特定のキーワードによって指定されたルート タイプのみが送信されます。

connected キーワードを指定すると、EIGRP スタブ ルーティング プロセスで接続ルートを送信できます。接続ルートが **network** ステートメントで指定されていない場合は、EIGRP プロセスで **redistribute** コマンドを使用して接続ルートの再配布が必要となることがあります。

static キーワードを指定すると、EIGRP スタブ ルーティング プロセスでスタティック ルートを送信できます。このオプションを設定していない場合は、EIGRP は、通常は自動的に再配布される内部スタティック ルートを含め、どのスタティック ルートも送信しません。**redistribute static** コマンドを使用して引き続きスタティック ルートを再配布する必要があります。

summary キーワードを指定すると、EIGRP スタブ ルーティング プロセスで集約ルートを送信できます。集約ルートは、**summary-address eigrp** コマンドを使用して手動で作成することも、**auto-summary** コマンドをイネーブルにして自動的に作成することもできます(このコマンドはデフォルトでイネーブルになっています)。

redistributed キーワードを指定すると、EIGRP スタブ ルーティング プロセスで、他のルーティング プロトコルから EIGRP ルーティング プロセスに再配布されたルートを送信できます。このオプションを設定しない場合、再配布されたルートは EIGRP によってアドバタイズされません。

例

次に、**eigrp stub** コマンドを使用して、接続ルートおよび集約ルートをアドバタイズする EIGRP スタブとして ASA を設定する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected summary
```

次に、**eigrp stub** コマンドを使用して、接続ルートおよびスタティック ルートをアドバタイズする EIGRP スタブとして ASA を設定する例を示します。集約ルートの送信は許可されません。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub connected static
```

次に、**eigrp stub** コマンドを使用して、EIGRP 更新の受信のみを行う EIGRP スタブとして ASA を設定する例を示します。接続ルート、集約ルート、およびスタティック ルートの情報は送信されません。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0 eigrp
ciscoasa(config-router)# eigrp stub receive-only
```

次に、**eigrp stub** コマンドを使用して、他のルーティング プロトコルから EIGRP に再配布されたルートをアドバタイズする EIGRP スタブとして ASA を設定する例を示します。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub redistributed
```

次に、オプションの引数を指定しないで **eigrp stub** コマンドを使用する例を示します。引数なしで **eigrp stub** コマンドを使用すると、デフォルトで接続ルートおよびスタティック ルートがアドバタイズされます。

```
ciscoasa(config)# router eigrp 100
ciscoasa(config-router)# network 10.0.0.0
ciscoasa(config-router)# eigrp stub
```

関連コマンド

コマンド	説明
router eigrp	実行コンフィギュレーションから EIGRP ルータ コンフィギュレーション モード コマンドをクリアします。
show running-config router eigrp	実行コンフィギュレーションの EIGRP ルータ コンフィギュレーション モード コマンドを表示します。

eject

ASA の外部コンパクト フラッシュ デバイスの取り外しをサポートするには、ユーザ EXEC モードで **eject** コマンドを使用します。

eject [**/noconfirm**] *disk1:*

構文の説明

disk1:	取り外すデバイスを指定します。
/noconfirm	ASA から外部フラッシュ デバイスを物理的に取り外す前に、デバイスを取り外すかどうかの確認が必要ないことを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
ユーザ 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
8.0(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

eject コマンドを使用すると、ASA 5500 シリーズからコンパクト フラッシュ デバイスを安全に取り外すことができます。

次に、**eject** コマンドを使用して、デバイスを ASA から物理的に取り外す前に *disk1* を正常にシャットダウンする例を示します。

```
ciscoasa# eject /noconfig disk1:
It is now safe to remove disk1:
ciscoasa# show version
Cisco Adaptive Security Appliance Software Version 8.0(2)34

Compiled on Fri 18-May-07 10:28 by juser System image file is "disk0:/cdisk.asa"
Config file at boot was "startup-config"

wef5520 up 5 hours 36 mins

Hardware:   ASA5520, 512 MB RAM, CPU Pentium 4 Celeron 2000 MHz
Internal ATA Compact Flash, 256MB
Slot 1: Compact Flash has been ejected!
It may be removed and a new device installed.
BIOS Flash M50FW016 @ 0xffe00000, 2048KB
<---More--->
```

関連コマンド

コマンド	説明
show version	オペレーティング システム ソフトウェアに関する情報を表示します。

email

登録時に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるには、クリプト CA トラストポイント コンフィギュレーション モードで **email** 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。

email *address*

no email

構文の説明

address	電子メール アドレスを指定します。最大長は、64 文字です。

デフォルト

デフォルト設定は設定されていません。

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
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	—	—

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、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の登録要求に電子メール アドレス user1@user.net を含める例を示します。

```
ciscoasa(config)# crypto ca-trustpoint central
ciscoasa(ca-trustpoint)# email user1@user.net
ciscoasa(ca-trustpoint)#
```

関連コマンド

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

enable（クラスタ グループ）

クラスタリングをイネーブルにするには、クラスタ グループ コンフィギュレーション モードで **enable** コマンドを使用します。クラスタリングをディセーブルにするには、このコマンドの **no** 形式を使用します。

enable [**as-slave** | **noconfirm**]

no enable

構文の説明

as-slave	（オプション）互換性のないコマンドの実行コンフィギュレーションを確認せずにクラスタリングをイネーブルにし、クラスタに参加させるスレーブが現在の選択においてマスターとなる可能性をなくします。スレーブのコンフィギュレーションは、マスター ユニットから同期されたコンフィギュレーションによって上書きされます。
noconfirm	（オプション）**enable** コマンドが入力されると、ASA は実行コンフィギュレーションをスキャンして、クラスタリングに対応していない機能の非互換コマンドの有無を調べます。デフォルト コンフィギュレーションにあるコマンドも、これに該当することがあります。互換性のないコマンドを削除するように求められます。応答として **No** を入力した場合は、クラスタリングはイネーブルになりません。確認を省略し、互換性のないコマンドを自動的に削除するには、**noconfirm** キーワードを使用します。

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
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

最初にイネーブルにしたユニットについては、マスター ユニット選定が発生します。最初のユニットは、その時点でクラスタの唯一のメンバーであるため、そのユニットがマスター ユニットになります。この期間中にコンフィギュレーション変更を実行しないでください。

すでにマスター ユニットがある場合に、クラスタにスレーブ ユニットを追加するときは、**enable as-slave** コマンドを使用すると、コンフィギュレーションの互換性の問題（主にまだクラスタリング用に設定されていないインターフェイスの存在）を回避できます。

クラスタリングをディセーブルにするには、**no enable** コマンドを入力します。

（注） クラスタリングをディセーブルにした場合は、すべてのデータ インターフェイスがシャットダウンされ、管理インターフェイスだけがアクティブになります。ユニットをクラスタから完全に削除する（その結果としてデータ インターフェイスをアクティブにする）場合は、クラスタ グループ コンフィギュレーション全体を削除する必要があります。

例

次に、クラスタリングをイネーブルにし、互換性のないコンフィギュレーションを削除する例を示します。

```
ciscoasa(config)# cluster group cluster1
ciscoasa(cfg-cluster)# enable
INFO: Clustering is not compatible with following commands:
policy-map global_policy
 class inspection_default
 inspect skinny
policy-map global_policy
 class inspection_default
  inspect sip
Would you like to remove these commands? [Y]es/[N]o:Y

INFO: Removing incompatible commands from running configuration...
Cryptochecksum (changed): f16b7fc2 a742727e e40bc0b0 cd169999
INFO: Done
```

関連コマンド

コマンド	説明
clacp system-mac	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。
cluster group	クラスタに名前を付け、クラスタ コンフィギュレーション モードを開始します。
cluster-interface	クラスタ制御リンク インターフェイスを指定します。
cluster interface-mode	クラスタ インターフェイス モードを設定します。
conn-rebalance	接続の再分散をイネーブルにします。
console-replicate	スレーブ ユニットからマスター ユニットへのコンソール複製をイネーブルにします。
health-check	クラスタのヘルス チェック機能（ユニットのヘルス モニタリングおよびインターフェイスのヘルス モニタリングを含む）をイネーブルにします。
key	クラスタ制御リンクの制御トラフィックの認証キーを設定します。
local-unit	クラスタ メンバーに名前を付けます。

コマンド	説明
mtu cluster-interface	クラスタ制御リンク インターフェイスの最大伝送ユニットを指定します。
priority（クラスタ グループ）	マスター ユニット選定のこのユニットのプライオリティを設定します。

enable(ユーザ EXEC)

特権 EXEC モードを開始するには、ユーザ EXEC モードで **enable** コマンドを使用します。

enable [*level*]

構文の説明

level	(任意)0 ～ 15 の特権レベル。enable 認証(**aaa authentication enable console** コマンド)では使用されません。

デフォルト

enable 認証(**aaa authentication enable console** コマンドを使用)を使用していない場合は、特権レベル 15 を開始します。enable 認証の場合、デフォルトのレベルは、ユーザ名に設定されているレベルに応じて異なります。

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
ユーザ 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
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

デフォルトのイネーブル パスワードはブランクです。パスワードの設定については、**enable password** コマンドを参照してください。

enable 認証を使用しない場合は、**enable** コマンドを入力すると、ユーザ名が enable_*level* に変更されます。デフォルトのレベルは 15 です。enable 認証を使用する場合(**aaa authentication enable console** コマンドを使用)、ユーザ名および関連するレベルは維持されます。ユーザ名の維持は、コマンド認可(ローカルまたは TACACS+ を使用した **aaa authorization command** コマンド)で重要です。

レベル 2 以上は特権 EXEC モードを開始します。レベル 0 およびレベル 1 は、ユーザ EXEC モードを開始します。中間のレベルを使用するには、ローカル コマンド認可(**aaa authorization command LOCAL** コマンド)をイネーブルにし、**privilege** コマンドを使用して異なる特権レベルにコマンドを設定します。TACACS+ コマンド認可では、ASA に設定された特権レベルは使用されません。

現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

特権 EXEC モードを終了するには、**disable** コマンドを入力します。

例

次に、特権 EXEC モードを開始する例を示します。

```
ciscoasa> enable
Password: Pa$$w0rd
ciscoasa#
```

次に、レベル 10 の特権 EXEC モードを開始する例を示します。

```
ciscoasa> enable 10
Password: Pa$$w0rd10
ciscoasa#
```

関連コマンド

コマンド	説明
イネーブル パスワード	イネーブル パスワードを設定します。
disable	特権 EXEC モードを終了します。
aaa authorization command	コマンド認可を設定します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。

enable e-mail proxy（廃止）

(注) このコマンドをサポートする最後のリリースは、9.5(1) でした。

以前に設定したインターフェイスで電子メール プロキシ アクセスをイネーブルにするには、**enable** コマンドを使用します。電子メール プロキシ（IMAP4S、POP3S、および SMTPS）の場合は、該当する電子メール プロキシ コンフィギュレーション モードでこのコマンドを使用します。インターフェイス上で電子メール プロキシ アクセス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。

enable *ifname*

no enable

構文の説明

ifname	以前に設定したインターフェイスを指定します。**nameif** コマンドを使用して、インターフェイスを設定します。

デフォルト

デフォルト値はありません。

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
Imap4s コンフィギュレーション	• 対応	—	• 対応	—	—
Pop3s コンフィギュレーション	• 対応	—	• 対応	—	—
smtps 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。
9.5(2)	このコマンドは廃止されました。

例

次に、Outside という名前のインターフェイスで POP3S 電子メール プロキシを設定する方法の例を示します。

```
ciscoasa(config)# pop3s
ciscoasa(config-pop3s)# enable Outside
```

enable gprs

RADIUS アカウンティングで GPRS をイネーブルにするには、RADIUS アカウンティング パラメータ コンフィギュレーション モードで **enable gprs** コマンドを使用します。このコマンド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。

enable gprs

no enable gprs

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
RADIUS アカウンティング パラメータ コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドには、**inspect radius-accounting** コマンドを使用してアクセスします。ASA は、セカンダリ PDP コンテキストを適切に処理するために、アカウンティング要求停止メッセージ内に 3GPP VSA 26-10415 があるかどうかをチェックします。このオプションは、デフォルトで無効です。この機能をイネーブルにするには、GTP ライセンスが必要です。

例

次に、RADIUS アカウンティングで GPRS をイネーブルにする例を示します。

```
ciscoasa(config)# policy-map type inspect radius-accounting ra
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# enable gprs
```

関連コマンド

コマンド	説明
inspect radius-accounting	RADIUS アカウンティングのインスペクションを設定します。
パラメータ	インスペクション ポリシー マップのパラメータを設定します。

enable password

特権 EXEC モードのイネーブル パスワードを設定するには、グローバル コンフィギュレーション モードで **enable password** コマンドを使用します。

enable password *password* [**level** *level*] [**pbkdf2** | **encrypted**]

構文の説明

encrypted	(任意)9.6 以前の場合は、32 文字以下のパスワードを暗号化することを指定します。**enable password** コマンドでパスワードを定義すると、ASA はセキュリティのためにそのパスワードをコンフィギュレーションに保存するときに MD5 ハッシュを作成します。**show running-config** コマンドを入力しても、**enable password** コマンドによって実際のパスワードは表示されず、暗号化されたパスワードと、その後に **encrypted** キーワードが表示されます。たとえば、"test" というパスワードを入力した場合、**show running-config** コマンドの出力は次のように表示されます。 `enable password rvEdRh0xPC8bel7s encrypted` CLI で実際に **encrypted** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストして、同じパスワードを使用する場合だけです。 9.7 以降では、すべての長さのパスワードで PBKDF2 を使用します。
level *level*	(任意)0 ～ 15 の特権レベルのパスワードを設定します。
password	3 ～ 127 文字の英数字および特殊文字から構成されるストリングとしてパスワードを設定します(大文字と小文字は区別されます)。パスワードには、疑問符とスペースを除いて、任意の文字を使用できます。
pbkdf2	(任意)パスワードの暗号化を指定します。9.6 以前の場合、PBKDF2 (パスワードベースのキー派生関数 2)ハッシュは、パスワードの長さが 32 文字を超える場合にのみ使用されます。9.7 以降では、すべてのパスワードで PBKDF2 を使用します。**enable password** コマンドでパスワードを定義すると、ASA はセキュリティのためにそのパスワードをコンフィギュレーションに保存するときに PBKDF2 (Password-Based Key Derivation Function 2)ハッシュを作成します。**show running-config** コマンドを入力しても、**enable password** コマンドによって実際のパスワードは表示されず、暗号化されたパスワードと、その後に **pbkdf2** キーワードが表示されます。たとえば、長いパスワードを入力した場合、**show running-config** コマンドの出力は次のように表示されます。 `username pat password rvEdRh0xPC8bel7s pbkdf2` CLI で実際に **pbkdf2** キーワードを入力するのは、コンフィギュレーションを別の ASA にカット アンド ペーストして、同じパスワードを使用する場合だけです。 新しいパスワードを入力しない限り、既存のパスワードは MD5 ベースのハッシュを使用し続けることに注意してください。

デフォルト

デフォルトのパスワードはブランクです。デフォルトのレベルは 15 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	• 対応

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.6(1)	パスワードの長さが 127 文字に増加し、**pbkdf2** キーワードが追加されました。
9.7(1)	すべての長さのパスワードが PBKDF2 ハッシュを使用してコンフィギュレーションに保存されるようになりました。
9.12(1)	**no enable password** コマンドは現在サポートされていません。

使用上のガイドライン

enable レベル 15（デフォルト レベル）のデフォルト パスワードは空白ですが、enable コマンドを最初に入力したときに変更するように求められます。パスワードを空白に設定できません。

CLI で **aaa authorization exec auto-enable** を有効にすると、**enable** コマンド、**login** コマンド（特権レベル 2 以上のユーザ）、または SSH/Telnet セッションを使用して特権 EXEC モードにアクセスできます。これらの方法ではすべて、イネーブル パスワードを設定する必要があります。

このパスワード変更の要件は、ASDM のログインには適用されません。ASDM のデフォルトでは、ユーザ名を使用せず enable パスワードを使用してログインすることができます。

マルチ コンテキスト モードでは、システム コンフィギュレーションおよび各コンテキストに対してイネーブル パスワードを作成できます。

デフォルトの 15 以外の特権レベルを使用するには、ローカル コマンド認可（**aaa authorization command** コマンドを使用して **LOCAL** キーワードを指定）を設定し、**privilege** コマンドを使用して異なる特権レベルにコマンドを設定します。ローカル コマンド認可を設定しない場合、イネーブル レベルは無視されて、設定したレベルにかかわらずレベル 15 へのアクセスが可能になります。現在の特権レベルを表示するには、**show curpriv** コマンドを使用します。

レベル 2 以上は特権 EXEC モードを開始します。レベル 0 およびレベル 1 は、ユーザ EXEC モードを開始します。

例

次に、イネーブル パスワードを Pa$$w0rd に設定する例を示します。

```
ciscoasa(config)# enable password Pa$$w0rd
```

次に、レベル 10 のイネーブル パスワードを Pa$$w0rd10 に設定する例を示します。

```
ciscoasa(config)# enable password Pa$$w0rd10 level 10
```

次に、イネーブル パスワードを、別の ASA からコピーした暗号化されたパスワードに設定する例を示します。

```
ciscoasa(config)# enable password jMorNbK0514fadBh pbkdf2
```

関連コマンド

コマンド	説明
aaa authorization command	コマンド認可を設定します。
enable	特権 EXEC モードを開始します。
privilege	ローカル コマンド認可のためのコマンド特権レベルを設定します。
show curpriv	現在ログインしているユーザ名とユーザの特権レベルを表示します。
show running-config enable	イネーブル パスワードを暗号化された形式で表示します。

webvpn の有効化

以前に設定したインターフェイスで WebVPN アクセスをイネーブルにするには、**enable** コマンドを使用します。このコマンドは、WebVPN コンフィギュレーション モードで使用します。インターフェイスで WebVPN 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。

enable *ifname*

no enable

構文の説明

ifname	以前に設定したインターフェイスを指定します。**nameif** コマンドを使用して、インターフェイスを設定します。

デフォルト

WebVPN は、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
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
7.0(1)	このコマンドが追加されました。

例

次に、Outside という名前のインターフェイスで WebVPN をイネーブルにする方法の例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# enable Outside
```

encapsulation-vxlan

VXLAN カプセル化を使用するようにネットワーク仮想化エンドポイント(NVE)インスタンスを設定するには、NVE コンフィギュレーション モードで **encapsulation-vxlan** コマンドを使用します。カプセル化を削除するには、このコマンドの **no** 形式を使用します。

encapsulation-vxlan

no encapsulation-vxlan

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、**nve** コマンドを入力した場合のデフォルトです。VXLAN のみがカプセル化の対象としてサポートされます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

encapsulation vxlan コマンドが NVE インスタンスのデフォルトにより追加されます。明示的に追加する必要はありません。

例

次に、NVE instance 1 を作成し、**encapsulation vxlan** コマンドを自動的に追加する例を示します。

```
ciscoasa(config)# nve 1
ciscoasa(cfg-nve)# show running-config nve
nve 1
 encapsulation vxlan
```

関連コマンド

コマンド	説明
debug vxlan	VXLAN トラフィックをデバッグします。
default-mcast-group	VTEP 送信元インターフェイスに関連付けられているすべての VNI インターフェイスのデフォルトのマルチキャスト グループを指定します。
inspect vxlan	標準 VXLAN ヘッダー形式に強制的に準拠させます。
interface vni	VXLAN タギング用の VNI インターフェイスを作成します。
mcast-group	VNI インターフェイスのマルチキャスト グループ アドレスを設定します。
nve	ネットワーク仮想化エンドポイント インスタンスを指定します。
nve-only	VXLAN 送信元インターフェイスが NVE 専用であることを指定します。
peer ip	ピア VTEP の IP アドレスを手動で指定します。
segment-id	VNI インターフェイスの VXLAN セグメント ID を指定します。
show arp vtep-mapping	リモート セグメント ドメインにある IP アドレスとリモート VTEP IP アドレス用の VNI インターフェイスにキャッシュされた MAC アドレスを表示します。
show interface vni	VNI インターフェイスのパラメータ、ステータス、および統計情報と、ブリッジされているインターフェイス(設定されている場合)のステータス、ならびに関連付けられている NVE インターフェイスを表示します。
show mac-address-table vtep-mapping	リモート VTEP IP アドレスが設定された VNI インターフェイス上のレイヤ 2 転送テーブル(MAC アドレス テーブル)を表示します。
show nve	NVE インターフェイスのパラメータ、ステータス、および統計情報とキャリア インターフェイス(送信元インターフェイス)のステータス、この NVE を VXLAN VTEP として使用する VNI、ならびにこの NVE インターフェイスに関連付けられているピア VTEP IP アドレスを表示します。
show vni vlan-mapping	VNI セグメント ID と、VLAN インターフェイスまたはトランスペアレント モードの物理インターフェイス間のマッピングを表示します。
source-interface	VTEP 送信元インターフェイスを指定します。
vtep-nve	VNI インターフェイスを VTEP 送信元インターフェイスに関連付けます。
vxlan port	VXLAN UDP ポートを設定します。デフォルトでは、VTEP 送信元インターフェイスは UDP ポート 4789 への VXLAN トラフィックを受け入れます。

暗号化

AnyConnect IPsec 接続に対して IKEv2 セキュリティ アソシエーション（SA）の暗号化アルゴリズムを指定するには、Ikev2 ポリシー コンフィギュレーション モードで **encryption** コマンドを使用します。コマンドを削除してデフォルト設定を使用するには、このコマンドの **no** 形式を使用します。

encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]

no encryption [**des** | **3des** | **aes** | **aes-192** | **aes-256** | **aes-gcm** | **aes-gcm-192** | **aes-gcm-256** | **null**]

構文の説明

des	56 ビット DES-CBC 暗号化を ESP に対して指定します。
3des	（デフォルト）トリプル DES 暗号化アルゴリズムを ESP に対して指定します。
aes	AES と 128 ビット キー暗号化を ESP に対して指定します。
aes-192	AES と 192 ビット キー暗号化を ESP に対して指定します。
aes-256	AES と 256 ビット キー暗号化を ESP に対して指定します。
aes-gcm	IKEv2 暗号化の AES-GCM アルゴリズムを指定します。
aes-gcm-192	IKEv2 暗号化の AES-GCM アルゴリズムを指定します。
aes-gcm-256	IKEv2 暗号化の AES-GCM アルゴリズムを指定します。
null	AES-GCM/GMAC が暗号化アルゴリズムとして設定されている場合は、ヌル整合性アルゴリズムを選択します。

デフォルト

デフォルトは 3DES です。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev2 policy** コマンドを入力した後、**encryption** コマンドを使用して、SA の暗号化アルゴリズムを設定できます。

OSPFv3 暗号化がインターフェイスでイネーブルの場合、IPsec トンネルを設定している間に隣接関係を確立すると、遅延が発生する可能性があります。基礎となる IPsec トンネルのステータスを判別し、処理が発生していることを確認するには、**show crypto sockets**、**show ipsec policy**、および **show ipsec sa** コマンドを使用します。

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
Ikev2 ポリシー 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
8.4(1)	このコマンドが追加されました。
9.0(1)	IKEv2 暗号化に使用される AES-GCM アルゴリズムが追加されました。

例

次に、Ikev2 ポリシー コンフィギュレーション モードを開始して、暗号化を AES-256 に設定する例を示します。

```
ciscoasa(config)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# encryption aes-256
```

関連コマンド

コマンド	説明
group	AnyConnect IPsec 接続に対して IKEv2 SA の Diffie-Hellman グループを指定します。
整合性	AnyConnect IPsec 接続に対して IKEv2 SA の ESP 整合性アルゴリズムを指定します。
prf	AnyConnect IPsec 接続に対して IKEv2 SA の疑似乱数関数を指定します。
ライフタイム	AnyConnect IPsec 接続に対して IKEv2 SA の SA ライフタイムを指定します。

エンドポイント

H.323 プロトコル インスペクションの HSI グループにエンドポイントを追加するには、HSI グループ コンフィギュレーション モードで **endpoint** 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。

endpoint *ip_address if_name*

no endpoint *ip_address if_name*

構文の説明

if_name	エンドポイントが ASA に接続するときに通過するインターフェイス。
ip_address	追加するエンドポイントの IP アドレス。HSI グループあたり最大で 10 のエンドポイントを設定できます。

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
hsi 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
7.2(1)	このコマンドが追加されました。

例

次に、H.323 インスペクション ポリシー マップの HSI グループにエンドポイントを追加する例を示します。

```
ciscoasa(config-pmap-p)# hsi-group 10
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.3.6.1 inside
ciscoasa(config-h225-map-hsi-grp)# endpoint 10.10.25.5 outside
```

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。
hsi-group	HSI グループを作成します。
hsi	HSI を HSI グループに追加します。

コマンド	説明
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

endpoint-mapper

DCERPC インスペクションのエンドポイント マッパー オプションを設定するには、パラメータ コンフィギュレーション モードで **endpoint-mapper** 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。

endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

no endpoint-mapper [**epm-service-only**] [**lookup-operation** [**timeout** *value*]]

構文の説明

epm-service-only	バインディング時にエンドポイント マッパー サービスを適用することを指定します。
lookup-operation	エンドポイント マッパー サービスのルックアップ動作をイネーブルにすることを指定します。
timeout *value*	ルックアップ動作におけるピンホールのタイムアウトを指定します。指定できる範囲は 0:0:1 ～ 1193:0:0 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
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、DCERPC ポリシー マップにエンドポイント マッパーを設定する例を示します。

```
ciscoasa(config)# policy-map type inspect dcerpc dcerpc_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# endpoint-mapper epm-service-only
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

enforcenextupdate

CRL の NextUpdate フィールドの処理方法を指定するには、ca-crl コンフィギュレーション モードで **enforcenextupdate** コマンドを使用します。期限が切れた NextUpdate フィールドがある場合や、NextUpdate フィールドがない場合を許容するには、このコマンドの **no** 形式を使用します。

enforcenextupdate

no enforcenextupdate

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

デフォルトの設定は強制（オン）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-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。

使用上のガイドライン

このコマンドが設定されている場合は、期限が切れていない NextUpdate フィールドが CRL に存在する必要があります。このコマンドが使用されていない場合、ASA では、CRL に NextUpdate フィールドがない場合や、期限が切れた NextUpdate フィールドがある場合が許容されます。

例

次に、クリプト ca-crl コンフィギュレーション モードを開始して、トラストポイント central に対して、期限が切れていない NextUpdate フィールドが CRL に存在することを必須とする例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# crl configure
ciscoasa(ca-crl)# enforcenextupdate
ciscoasa(ca-crl)#
```

関連コマンド]

コマンド	説明
cache-time	キャッシュのリフレッシュ時間を分単位で指定します。
crl configure	ca-crl コンフィギュレーション モードを開始します。
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。

enrollment protocol scep | cmp url

このトラストポイントの登録に自動登録(SCEP または CMP の場合)を指定して、登録 URL を設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment protocol scep| cmp url** コマンドを使用します。このコマンドの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。

enrollment protocol scep | smp *url*

no enrollment protocol scep | smp *url*

構文の説明

protocol	SCEP CA URL と CMP CA URL を区別します。

デフォルト

デフォルトの設定はオフです。

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
クリプト CA サーバ 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
9.7(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

LTE ワイヤレス ネットワークでセキュリティ ゲートウェイ デバイスとして機能するために、ASA は、SCEP に加えて Certificate Management Protocol(CMPv2)を使用していくつかの証明書管理機能をサポートします。ASA デバイス証明書の登録に CMPv2 を使用することで、CMPv2 が有効な CA からの最初の証明書とセカンダリ証明書を手動登録したり、同じキーペアを使用する以前に発行済みの証明書を差し替えるための証明書を手動更新したりできます。受信した証明書は従来の設定の外部に保存され、証明書が有効になっている IPsec の設定で使用されます。

例

次の例は、登録オプションを示しています。

```
(config)# crypto ca trustpoint new
(config-ca-trustpoint)# enrollment ?
crypto-ca-trustpoint mode commands/options:
    interface  Configure source interface
    protocol   Enrollment protocol
```

```
    retry       Polling parameters
    self        Enrollment will generate a self-signed certificate
    terminal    Enroll via the terminal (cut-and-paste)
asa2(config-ca-trustpoint)# enrollment protocol ?

crypto-ca-trustpoint mode commands/options:
    cmp         Certificate Management Protocol Version 2
    scep        Simple Certificate Enrollment Protocol
asa2(config-ca-trustpoint)# enrollment protocol cmp ?

crypto-ca-trustpoint mode commands/options:
    url         CA server enrollment URL
```

enrollment-retrieval

登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定するには、ローカル クリプト CA サーバ コンフィギュレーション モードで **enrollment-retrieval** コマンドを使用します。期間をデフォルトの時間数(24)にリセットするには、このコマンドの **no** 形式を使用します。

enrollment-retrieval *timeout*

no enrollment-retrieval

構文の説明

timeout	何時間以内にユーザがローカル CA 登録 Web ページから発行された証明書を取得しなければならないかを指定します。有効なタイムアウト値の範囲は 1 ～ 720 時間です。

デフォルト

デフォルトでは、PKCS12 登録ファイルは 24 時間保存されて取得できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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 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

PKCS12 登録ファイルには、発行された証明書とキー ペアが含まれています。ファイルはローカル CA サーバに保存され、**enrollment-retrieval** コマンドで指定された時間内は登録 Web ページから取得できます。

ユーザが登録可能とマークされている場合、そのユーザは **otp expiration** コマンドで指定した時間内であればそのパスワードを使用して登録できます。ユーザが正常に登録すると、PKCS12 ファイルが生成および保存され、コピーが登録 Web ページを経由して返されます。何らかの理由でファイルのコピーが再度必要になった場合(登録しようとしてダウンロードに失敗した場合など)、ユーザは **enrollment-retrieval** コマンドで指定した時間内であれば新しくコピーを取得できます。

(注) この時間は、OTP の有効期限とは関係ありません。

例

次に、証明書の発行後 48 時間以内は PKCS12 登録ファイルをローカル CA サーバから取得できるように指定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# enrollment-retrieval 48
ciscoasa(config-ca-server)#
```

次に、取得可能時間をデフォルトの 24 時間にリセットする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# no enrollment-retrieval
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 コマンド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。
OTP expiration	CA 登録ページ用に発行されたワンタイム パスワードの有効期間を時間単位で指定します。
smtp from-address	CA サーバが生成するすべての電子メールの送信者フィールドに使用する電子メール アドレスを指定します。
smtp subject	ローカル CA サーバが生成するすべての電子メールの件名フィールドに表示されるテキストを指定します。
subject-name-default	CA サーバが発行するすべてのユーザ証明書でユーザ名とともに使用される汎用的なサブジェクト名 DN を指定します。

enrollment retry count

再試行回数を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment retry count** コマンドを使用します。デフォルトの再試行回数設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry count *number*

no enrollment retry count

構文の説明

number	登録要求の送信を試行する最大回数。有効な値は、0、および 1 ～ 100 の再試行です。

デフォルト

number 引数のデフォルト設定は 0（無制限）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
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

証明書を要求した後、ASA は CA からの証明書の受信を待ちます。ASA は、設定された再試行間隔内に証明書を受信できない場合、証明書要求を再度送信します。ASA は、応答を受信するか、または設定されている再試行間隔が終了するまで、要求を繰り返し送信します。このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central 内の登録再試行回数を 20 回に設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry count 20
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。

enrollment retry period

再試行間隔を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment retry period** コマンドを使用します。デフォルトの再試行間隔設定に戻すには、このコマンドの **no** 形式を使用します。

enrollment retry period *minutes*

no enrollment retry period

構文の説明

minutes	登録要求の送信を試行する間隔（分単位）。有効な範囲は、1 ～ 60 分です。

デフォルト

デフォルトの設定は 1 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。

	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	• 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

証明書を要求した後、ASA は CA からの証明書の受信を待ちます。ASA は、指定された再試行間隔内に証明書を受信できない場合、証明書要求を再度送信します。このコマンドはオプションであり、自動登録を設定している場合のみ適用されます。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central 内の登録再試行間隔を 10 分に設定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment retry period 10
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	すべての登録パラメータを、システムのデフォルト値に戻します。
enrollment retry count	登録要求の再試行回数を定義します。

enrollment terminal

このトラストポイントでカット アンド ペースト登録(手動登録とも呼ばれます)を指定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment terminal** コマンドを使用します。このコマンドの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。

enrollment terminal

no enrollment terminal

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

デフォルトの設定はオフです。

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
クリプト CA トラストポイント コンフィギュレーション	• 対応	• 対応	• 対応	• 対応	—

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

例

次に、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central の CA 登録にカット アンド ペースト方式を指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment terminal
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。

コマンド	説明
enrollment retry period	登録要求を再送信するまでの待機時間を分単位で指定します。
enrollment url	このトラストポイントに対して自動登録（SCEP）を指定して、URL を設定します。

enrollment url（廃止）

このトラストポイントの登録に自動登録（SCEP）を指定して、登録 URL を設定するには、クリプト CA トラストポイント コンフィギュレーション モードで **enrollment url** コマンドを使用します。このコマンドの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。

enrollment url *url*

no enrollment url ***url***

構文の説明

url	自動登録の URL の名前を指定します。最大の長さは 1000 文字です（実質的に無制限です）。

デフォルト

デフォルトの設定はオフです。

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	• 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、トラストポイント central のクリプト CA トラストポイント コンフィギュレーション モードを開始して、トラストポイント central に URL https://enrollsite における SCEP 登録を指定する例を示します。

```
ciscoasa(config)# crypto ca trustpoint central
ciscoasa(ca-trustpoint)# enrollment url https://enrollsite
ciscoasa(ca-trustpoint)#
```

関連コマンド

コマンド	説明
crypto ca trustpoint	クリプト CA トラストポイント コンフィギュレーション モードを開始します。
default enrollment	登録パラメータをデフォルト値に戻します。
enrollment retry count	登録要求の送信を再試行する回数を指定します。

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

eool

IP オプション インスペクションにおいて、パケット ヘッダー内に End of Options List（EOOL）オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **eool** 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。

eool action {allow | clear}

no eool action {allow | clear}

構文の説明

allow	End of Options List IP オプションを含むパケットを許可します。
clear	End of Options List オプションをパケットから削除してから、そのパケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、End of Options List IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
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

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

オプション リストの終端オプションは、1 バイトのゼロのみを含み、すべてのオプションの終端に配置されて、オプションのリストの終端を示します。これは、ヘッダー長に基づくヘッダーの末尾とは一致しない場合があります。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# eool action allow
ciscoasa(config-pmap-p)# nop action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

eou allow（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC フレームワーク コンフィギュレーションでクライアントレス認証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 **eou allow** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

eou allow {**audit** | **clientless** | **none**}

no eou allow {**audit** | **clientless** | **none**}

構文の説明

監査	クライアントレス認証を実行します。
clientless	クライアントレス認証を実行します。
none	クライアントレス認証をディセーブルにします。

デフォルト

デフォルトのコンフィギュレーションには、**eou allow clientless** コンフィギュレーションが含まれています。

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
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	**audit** オプションが追加されました。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

ASA では、次の両方の条件が満たされている場合にのみこのコマンドが使用されます。

- NAC ポリシー タイプとして NAC フレームワークを使用するようにグループ ポリシーが設定されていること。
- セッションのホストが EAPoUDP 要求に応答しないこと。

例

次に、ACS を使用したクライアントレス認証の実行をイネーブルにする例を示します。

```
ciscoasa(config)# eou allow clientless
ciscoasa(config)#
```

次に、監査サーバを使用してクライアントレス認証を実行するように ASA を設定する例を示します。

```
ciscoasa(config)# eou allow audit
ciscoasa(config)#
```

次に、監査サーバの使用をディセーブルにする例を示します。

```
ciscoasa(config)# no eou allow clientless
ciscoasa(config)#
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou clientless	NAC フレームワーク コンフィギュレーションのクライアントレス認証で ACS に対して送信されるユーザ名およびパスワードを変更します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

eou clientless（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC フレームワーク コンフィギュレーションにおけるクライアントレス認証でアクセス コントロール サーバに送信するユーザ名とパスワードを変更するには、グローバル コンフィギュレーション モードで **eou clientless** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou clientless username *username* **password** *password*

no eou clientless username *username* **password** *password*

構文の説明

password	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を取得するためにアクセス コントロール サーバに送信するパスワードを変更する場合に入力します。
password	クライアントレス ホストをサポートするためにアクセス コントロール サーバに設定されているパスワードを入力します。4 ～ 32 文字の ASCII 文字を入力します。
username	EAPoUDP 要求に応答しないリモート ホストのクライアントレス認証を取得するためにアクセス コントロール サーバに送信するユーザ名を変更する場合に入力します。
username	クライアントレス ホストをサポートするためにアクセス コントロール サーバに設定されているユーザ名を入力します。先頭および末尾のスペース、シャープ記号（#）、疑問符（?）、引用符（"）、アスタリスク（*）、山カッコ（< および >）を除く、1 ～ 64 文字の ASCII 文字を入力します。

デフォルト

username 属性と password 属性のデフォルト値は、両方とも clientless 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	—	—

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。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは、次の条件をすべて満たしている場合にのみ有効です。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- ASA 上でクライアントレス認証がイネーブルになっている。
- NAC が ASA で設定されている。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、クライアントレス認証のユーザ名を sherlock に変更する例を示します。

```
ciscoasa(config)# eou clientless username sherlock
ciscoasa(config)#
```

次に、クライアントレス認証のユーザ名をデフォルト値である clientless に変更する例を示します。

```
ciscoasa(config)# no eou clientless username
ciscoasa(config)#
```

次に、クライアントレス認証のパスワードを secret に変更する例を示します。

```
ciscoasa(config)# eou clientless password secret
ciscoasa(config)#
```

次に、クライアントレス認証のパスワードをデフォルト値である clientless に変更する例を示します。

```
ciscoasa(config)# no eou clientless password
ciscoasa(config)#
```

関連コマンド

コマンド	説明
eou allow	NAC フレームワーク コンフィギュレーションでクライアントレス認証をイネーブルにします。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

eou initialize（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

1 つ以上の NAC フレームワーク セッションに割り当てられているリソースをクリアして、各セッションに対して新しい無条件のポスチャ検証を開始するには、特権 EXEC モードで **eou initialize** コマンドを使用します。

eou initialize {**all** | **group** *tunnel-group* | **ip** *ip-address*}

構文の説明

all	この ASA 上のすべての NAC フレームワーク セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC フレームワーク セッションを再確認します。
ip	単一の NAC フレームワーク セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

	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	—	—

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。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

リモート ピアのポスチャが変更されたり、割り当てられているアクセス ポリシー（つまりダウンロードされた ACL）が変更されたりしたときに、セッションに割り当てられているリソースをクリアする場合は、このコマンドを使用します。このコマンドを入力すると、ポスチャ検証に使用される EAPoUDP アソシエーションおよびアクセス ポリシーが消去されます。再検証中には NAC のデフォルトの ACL が有効となるため、セッションを初期化するとユーザ トラフィックに影響する場合があります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、すべての NAC フレームワーク セッションを初期化する例を示します。

```
ciscoasa# eou initialize all
ciscoasa
```

次に、tg1 というトンネル グループに割り当てられているすべての NAC フレームワーク セッションを初期化する例を示します。

```
ciscoasa# eou initialize group tg1
ciscoasa
```

次に、IP アドレス 209.165. 200.225 を持つエンドポイントの NAC フレームワーク セッションを再検証する例を示します。

```
ciscoasa# eou initialize 209.165.200.225
ciscoasa
```

関連コマンド

コマンド	説明
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。

eou max-retry（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

ASA が EAP over UDP メッセージをリモート コンピュータに再送信する回数を変更するには、グローバル コンフィギュレーション モードで **eou max-retry** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou max-retry *retries*

no eou max-retry

構文の説明

retries	再送信タイマーが期限切れになった場合に再送信する回数を制限します。1 ～ 3 の範囲の値を入力します。

デフォルト

デフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	—	—

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。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは、次の条件をすべて満たしている場合にのみ有効です。

- クライアントレス認証をサポートするために、ネットワーク上にアクセス コントロール サーバが設定されている。
- ASA 上でクライアントレス認証がイネーブルになっている。
- NAC が ASA で設定されている。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、EAP over UDP の再送信回数を 1 に制限する例を示します。

```
ciscoasa(config)# eou max-retry 1
ciscoasa(config)#
```

次に、EAP over UDP の再送信回数をデフォルト値である 3 に変更する例を示します。

```
ciscoasa(config)# no eou max-retry
ciscoasa(config)#
```

関連コマンド

eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。

eou port（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC フレームワーク コンフィギュレーションにおいて、Cisco Trust Agent との EAP over UDP 通信に使用するポート番号を変更するには、グローバル コンフィギュレーション モードで **eou port** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou port *port_number*

no eou port

構文の説明

port_number	EAP over UDP 通信用に指定するクライアント エンドポイントのポート番号。この番号は、Cisco Trust Agent に設定するポート番号です。1024 ～ 65535 の範囲の値を入力します。

デフォルト

デフォルト値は 21862 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	—	—

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。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、EAP over UDP 通信のポート番号を 62445 に変更する例を示します。

```
ciscoasa(config)# eou port 62445
ciscoasa(config)#
```

次に、EAP over UDP 通信のポート番号をデフォルト値に変更する例を示します。

```
ciscoasa(config)# no eou port
ciscoasa(config)#
```

関連コマンド

debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou initialize	1 つ以上の NAC フレームワーク セッションに割り当てられているリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始します。
eou revalidate	1 つ以上の NAC フレームワーク セッションのポスチャ再確認をただちに強制します。
show vpn-session.db	VLAN マッピングと NAC の結果を含む、VPN セッションの情報を表示します。
show vpn-session_summary.db	VLAN マッピング セッション データを含む、IPsec、Cisco AnyConnect、NAC の各セッションの数を表示します。

eou revalidate（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

1 つ以上の NAC フレームワーク セッションのポスチャ再検証をただちに実行するには、特権 EXEC モードで **eou revalidate** コマンドを使用します。

eou revalidate {**all** | **group** *tunnel-group* | **ip** *ip-address*}

構文の説明

all	この ASA 上のすべての NAC フレームワーク セッションを再確認します。
group	トンネル グループに割り当てられているすべての NAC フレームワーク セッションを再確認します。
ip	単一の NAC フレームワーク セッションを再確認します。
ip-address	トンネルのリモート ピア側の IP アドレス。
tunnel-group	トンネルをセットアップするパラメータのネゴシエーションに使用されるトンネル グループの名前。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

	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	—	—

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。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

ピアのポスチャ、または割り当てられているアクセス ポリシー(つまりダウンロードされた ACL が存在する場合その ACL)が変更された場合にこのコマンドを使用します。このコマンドは、新しい無条件のポスチャ検証を開始します。コマンド入力前に有効であったポスチャ検証および割り当てられているアクセス ポリシーは、新しいポスチャ検証に成功または失敗するまでは引き続き有効となります。このコマンドは、ポスチャ確認から免除されているピアには作用しません。

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、すべての NAC フレームワーク セッションを再検証する例を示します。

```
ciscoasa# eou revalidate all
ciscoasa
```

次に、tg-1 というトンネル グループに割り当てられているすべての NAC フレームワーク セッションを再検証する例を示します。

```
ciscoasa# eou revalidate group tg-1
ciscoasa
```

次に、IP アドレス 209.165. 200.225 を持つエンドポイントの NAC フレームワーク セッションを再検証する例を示します。

```
ciscoasa# eou revalidate ip 209.165.200.225
ciscoasa
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou initialize	1 つ以上の NAC フレームワーク セッションに割り当てられているリソースを消去し、セッションごとに新しい無条件のポスチャ確認を開始します。
eou timeout	NAC フレームワーク コンフィギュレーションで EAP over UDP メッセージをリモート ホストに送信した後に待機する秒数を変更します。
reval-period	NAC フレームワーク セッションでの成功したポスチャ確認の間隔を指定します。
sq-period	NAC フレームワーク セッションで正常に完了したポスチャ確認と、ホスト ポスチャの変化を調べる次回のクエリーとの間隔を指定します。

eou timeout（廃止）

（注） このコマンドをサポートする最後のリリースは、Version 9.1(1) でした。

NAC フレームワーク コンフィギュレーションにおいて、リモート ホストに対して EAP over UDP メッセージを送信した後に待機する秒数を変更するには、グローバル コンフィギュレーション モードで **eou timeout** コマンドを使用します。デフォルト値を使用するには、このコマンドの **no** 形式を使用します。

eou timeout {**hold-period** | **retransmit**} *seconds*

no eou timeout {**hold-period** | **retransmit**}

構文の説明

hold-period	EAPoUDP 再試行回数分の EAPoUDP メッセージを送信した後に待機する最大時間。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行した場合も、このタイマーがクリアされます。このタイマーが期限切れになった場合、ASA はリモート ホストとの新しい EAP over UDP アソシエーションを開始します。
retransmit	1 回の EAPoUDP メッセージ送信後に待機する最大時間。リモート ホストから応答があると、このタイマーはクリアされます。**eou initialize** コマンドまたは **eou revalidate** コマンドを実行した場合も、このタイマーがクリアされます。タイマーが期限切れになると、ASA はリモート ホストに対して EAPoUDP メッセージを再送信します。
seconds	ASA が待機する秒数。hold-period 属性には 60 ～ 86400 の範囲の値を、retransmit 属性には 1 ～ 60 の範囲の値を入力します。

デフォルト

hold-period オプションのデフォルト値は 180 です。

retransmit オプションのデフォルト値は 3 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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	—	—

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。
9.1(2)	このコマンドは廃止されました。

使用上のガイドライン

このコマンドは Cisco NAC のフレームワーク実装にだけ適用されます。

例

次に、新しい EAP over UDP アソシエーションを開始するまでの待機時間を 120 秒に変更する例を示します。

```
ciscoasa(config)# eou timeout hold-period 120
ciscoasa(config)#
```

次に、新しい EAP over UDP アソシエーションを開始するまでの待機時間をデフォルト値に変更する例を示します。

```
ciscoasa(config)# no eou timeout hold-period
ciscoasa(config)#
```

次に、再送信タイマーを 6 秒に変更する例を示します。

```
ciscoasa(config)# eou timeout retransmit 6
ciscoasa(config)#
```

次に、再送信タイマーをデフォルト値に変更する例を示します。

```
ciscoasa(config)# no eou timeout retransmit
ciscoasa(config)#
```

関連コマンド

コマンド	説明
debug eou	EAP over UDP イベントのロギングをイネーブルにして、NAC フレームワーク メッセージをデバッグします。
eou max-retry	ASA がリモート コンピュータに対して EAP over UDP メッセージを再送信する回数を変更します。

erase

ファイル システムを消去して再フォーマットするには、特権 EXEC モードで **erase** コマンドを使用します。このコマンドは、非表示のシステム ファイルを含むすべてのファイルを上書きしてファイル システムを消去し、ファイル システムを再インストールします。

erase [**disk0:** | **disk1:** | **flash:**]

構文の説明

disk0:	(任意)内蔵コンパクト 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。
disk1:	(任意)外部 コンパクト 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:	(任意)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。 **注意** フラッシュ メモリを消去すると、フラッシュ メモリに保存されているライセンス情報も削除されます。フラッシュ メモリを消去する前に、ライセンス情報を保存してください。 ASA 5500 シリーズでは、**flash** キーワードは **disk0** のエイリアスです。

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
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

erase コマンドは、0xFF パターンを使用してフラッシュメモリ上のすべてのデータを消去し、空のファイルシステム割り当てテーブルをデバイスに書き換えます。

(非表示のシステム ファイルを除く)表示されているすべてのファイルを削除する場合は、**erase** コマンドではなく **delete /recursive** コマンドを入力します。

（注） Cisco ASA 5500 シリーズでは、**erase** コマンドを実行すると、ディスク上のすべてのユーザ データが 0xFF パターンを使用して破棄されます。一方、**format** コマンドはファイル システムの制御構造をリセットするだけです。ロウ ディスク読み取りツールを使用すると、この情報はまだ参照できる可能性があります。

例

次に、ファイル システムを消去して再フォーマットする例を示します。

```
ciscoasa# erase flash:
```

関連コマンド

コマンド	説明
delete	非表示のシステム ファイルを除く表示されているすべてのファイルを削除します。
形式	(非表示のシステム ファイルを含む)すべてのファイルを消去して、ファイル システムをフォーマットします。

esp

IPsec パススルー インスペクションで ESP トンネルおよび AH トンネルのパラメータを指定するには、パラメータ コンフィギュレーション モードで **esp** 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。

{**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

no {**esp** | **ah**} [**per-client-max** *num*] [**timeout** *time*]

構文の説明

esp	ESP トンネルのパラメータを指定します。
ah	AH トンネルのパラメータを指定します。
per-client-max *num*	1 つのクライアントからの最大トンネル数を指定します。
timeout *time*	ESP トンネルのアイドル タイムアウトを指定します。

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
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、UDP 500 のトラフィックを許可する例を示します。

```
ciscoasa(config)# access-list test-udp-acl extended permit udp any any eq 500
ciscoasa(config)# class-map test-udp-class
ciscoasa(config-pmap-c)# match access-list test-udp-acl

ciscoasa(config)# policy-map type inspect ipsec-pass-thru ipsec-map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# esp per-client-max 32 timeout 0:06:00
ciscoasa(config-pmap-p)# ah per-client-max 16 timeout 0:05:00

ciscoasa(config)# policy-map test-udp-policy
ciscoasa(config-pmap)# class test-udp-class
ciscoasa(config-pmap-c)# inspect ipsec-pass-thru ipsec-map
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

established

確立された接続に基づく、ポートへの戻り接続を許可するには、グローバル コンフィギュレーション モードで **established** コマンドを使用します。**established** 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。

established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

no established *est_protocol dest_port* [*source_port*] [**permitto** *protocol port* [*-port*]] [**permitfrom** *protocol port*[*-port*]]

構文の説明

est_protocol	確立された接続のルックアップに使用する IP プロトコル（UDP または TCP）を指定します。
dest_port	確立された接続のルックアップに使用する宛先ポートを指定します。
permitfrom	（任意）指定したポートから発信される戻りプロトコル接続を許可します。
permitto	（任意）指定したポートに着信する戻りプロトコル接続を許可します。
port [*-port*]	（任意）戻り接続の（UDP または TCP）宛先ポートを指定します。
protocol	（任意）戻り接続で使用される IP プロトコル（UDP または TCP）。
source_port	（任意）確立された接続のルックアップに使用する送信元ポートを指定します

デフォルト

デフォルトの設定は次のとおりです。

- *dest_port*：0（ワイルドカード）
- *source_port*：0（ワイルドカード）

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)	キーワード **to** および **from** が CLI から削除されました。代わりにキーワード **permitto** および **permitfrom** を使用します。

使用上のガイドライン

established コマンドを使用すると、ASA 経由の発信接続の戻りアクセスを許可できます。このコマンドは、ネットワークから発信され、ASA によって保護されている元の接続、および外部ホストからの同じ 2 つのデバイス間の着信戻り接続に対して動作します。**established** コマンドでは、接続のルックアップに使用する宛先ポートを指定できます。宛先ポートを指定することによって、コマンドをより細かく制御でき、宛先ポートは既知であるが送信元ポートは不明であるプロトコルをサポートできます。**permitto** および **permitfrom** キーワードでは、リターン インバウンド接続を定義します。

注意 **established** コマンドでは、常に **permitto** キーワードおよび **permitfrom** キーワードを指定することを推奨します。これらのキーワードを指定しないで **established** コマンドを使用すると、外部システムに接続した場合にそれらのシステムから接続に関連する内部ホストに対して無制限に接続が可能となるため、セキュリティのリスクが発生します。このような状況は、内部システムの攻撃に悪用される可能性があります。

例

次に、**established** コマンドを正しく使用しない場合にセキュリティ違反が発生する可能性があることを示すいくつかの例を示します。

次に、内部システムから外部ホストのポート 4000 に TCP 接続を確立した場合に、外部ホストから任意のプロトコルを使用して任意のポートに戻り接続を確立できることを示す例を示します。

```
ciscoasa(config)# established tcp 4000 0
```

プロトコルで使用されるポートが規定されていない場合は、送信元ポートおよび宛先ポートに **0** を指定できます。ワイルドカード ポート(0)は、必要な場合にのみ使用します。

```
ciscoasa(config)# established tcp 0 0
```

(注) **established** コマンドが正しく動作するためには、クライアントは **permitto** キーワードで指定されたポートでリッスンする必要があります。

established コマンドは、**nat 0** コマンドとともに使用できます(**global** コマンドがない場合)。

(注) **established** コマンドは、PAT とともに使用することはできません。

ASA では、**established** コマンドを利用することによって XDMCP がサポートされます。

注意 ASA を通して XWindows システム アプリケーションを使用すると、セキュリティのリスクが発生する可能性があります。

デフォルトで、XDMCP はオンになっていますが、次のように **established** コマンドを入力しないとセッションが完了しません。

```
ciscoasa(config)# established tcp 6000 0 permitto tcp 6000 permitfrom tcp 1024-65535
```

established コマンドを入力すると、内部の XDMCP 実装ホスト（UNIX または Reflection X）から外部の XDMCP 実装 XWindows サーバにアクセスできます。UDP/177 ベースの XDMCP によって TCP ベースの XWindows セッションがネゴシエートされ、後続の TCP 戻り接続が許可されます。リターン トラフィックの送信元ポートは不明であるため、*source_port* フィールドには 0（ワイルドカード）を指定します。*dest_port* は 6000 + *n* となります。*n* は、ローカルのディスプレイ番号を表します。この値を変更するには、次の UNIX コマンドを使用します。

```
ciscoasa(config)# setenv DISPLAY hostname:displaynumber.screennumber
```

（ユーザ対話に基づいて）数多くの TCP 接続が生成され、これらの接続の送信元ポートが不明であるため、**established** コマンドが必要となります。宛先ポートのみがスタティックです。ASA では、XDMCP フィックスアップが透過的に実行されます。コンフィギュレーションは必要ありませんが、TCP セッションを確立できるように **established** コマンドを入力する必要があります。

次に、送信元ポート C からポート B 宛のプロトコル A を使用した 2 つのホスト間の接続の例を示します。ASA 経由でプロトコル D（プロトコル D はプロトコル A とは異なっていてもかまいません）による戻り接続を許可するには、送信元ポートがポート F に、宛先ポートがポート E に対応している必要があります。

```
ciscoasa(config)# established A B C permitto D E permitfrom D F
```

次に、TCP 宛先ポート 6060、および任意の送信元ポートを使用して、内部ホストから外部ホストに接続を開始する例を示します。ASA では、TCP 宛先ポート 6061 および任意の TCP 送信元ポートを使用したホスト間のリターン トラフィックが許可されます。

```
ciscoasa(config)# established tcp 6060 0 permitto tcp 6061 permitfrom tcp 0
```

次に、UDP 宛先ポート 6060、および任意の送信元ポートを使用して、内部ホストから外部ホストに接続を開始する例を示します。ASA では、TCP 宛先ポート 6061 および TCP 送信元ポート 1024 ～ 65535 を使用したホスト間のリターン トラフィックが許可されます。

```
ciscoasa(config)# established udp 6060 0 permitto tcp 6061 permitfrom tcp 1024-65535
```

次に、ローカル ホストから外部ホストにポート 9999 への TCP 接続を開始する例を示します。この例では、外部ホストのポート 4242 からローカル ホストのポート 5454 へのパケットが許可されます。

```
ciscoasa(config)# established tcp 9999 permitto tcp 5454 permitfrom tcp 4242
```

関連コマンド

コマンド	説明
clear configure established	確立されたコマンドをすべて削除します。
show running-config established	確立されている接続に基づく、許可済みの着信接続を表示します。

event crashinfo

ASA でクラッシュが発生した場合にイベント マネージャ アプレットをトリガーするには、イベント マネージャ アプレット コンフィギュレーション モードで **event crashinfo** コマンドを使用します。クラッシュ イベントを削除するには、このコマンドの **no** 形式を使用します。

event crashinfo

no event crashinfo

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
イベント マネージャ アプレット コンフィギュレーション	• 対応	• Yes	• 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

output コマンドの値に関係なく、**action** コマンドはクラッシュ情報ファイルに送られます。出力は、**show tech** コマンドの前に生成されます。

(注) ASA がクラッシュした場合、その状態は通常は不明です。一部の CLI コマンドは、この状態のときに実行するのは安全でない場合があります。

例

次に、ASA がクラッシュした場合にアプレットをトリガーする例を示します。

```
ciscoasa(config-applet)# event crashinfo
```

関連コマンド

コマンド	説明
event none	イベント マネージャ アプレットを手動で呼び出します。
event syslog id	イベント マネージャ アプレットに syslog イベントを追加します。
event timer absolute time	絶対イベント タイマーを設定します。
event timer countdown time	カウントダウン タイマー イベントを設定します。
event timer watchdog time	ウォッチドッグ タイマー イベントを設定します。

event manager applet

イベントをアクションや出力とリンクするイベント マネージャ アプレットを作成または編集するには、グローバル コンフィギュレーション モードで event manager applet コマンドを使用します。イベント マネージャ アプレットを削除するには、このコマンドの **no** 形式を使用します。

event manager applet *name*

no event manager applet *name*

構文の説明

name	イベント マネージャ アプレットの名前を指定します。名前には最大 32 文字の長さを使用できます。

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
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
9.2(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

イベント マネージャ アプレット コンフィギュレーション モードを開始するには、**event manager applet** コマンドを使用します。

例

次に、イベント マネージャ アプレットを作成し、イベント マネージャ アプレット コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config)# event manager applet appletexample1
ciscoasa(config-applet)#
```

関連コマンド

コマンド	説明
description	アプレットについて説明します。
event manager run	イベント マネージャ アプレットを実行します。

コマンド	説明
show event manager	設定された各イベント マネージャ アプレットの統計情報を表示します。
debug event manager	イベント マネージャのデバッグ トレースを管理します。

event memory-logging-wrap

メモリ ロギングのラップ イベント トリガーを設定するには、イベント マネージャ アプレット コンフィギュレーション モードで **event memory-logging-wrap** コマンドを使用します。

event memory-logging-wrap

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。

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
イベント マネージャ アプレット 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
9.4(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

メモリ ロギングのラップがイネーブルの場合、メモリ ロガーがイベントをイベント マネージャに送信し、設定されたアプレットをトリガーします。

例

次に、すべてのメモリ割り当てを記録するアプレットを示します。

```
ciscoasa(config-applet)# event manager applet memlog
ciscoasa(config-applet)# event memory-logging-wrap
ciscoasa(config-applet)# action 0 cli command "show memory logging wrap"
ciscoasa(config-applet)# output file append disk0:/memlog.log
```

関連コマンド

コマンド	説明
memory logging	メモリ ロギングをイネーブルにします。
show memory logging	メモリ ロギングの結果を表示します。

event none

イベント マネージャ アプレットを手動で呼び出すには、イベント マネージャ アプレット コンフィギュレーション モードで **event none** コマンドを使用します。手動呼び出しを削除するには、このコマンドの **no** 形式を使用します。

event none

no event none

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。

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
イベント マネージャ アプレット 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
9.2(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

event none コマンドを使用して他のイベントを設定できます。

例

次に、イベント マネージャ アプレットを手動で呼び出す例を示します。

```
ciscoasa(config-applet)# event none
```

関連コマンド

コマンド	説明
event crashinfo	ASA でクラッシュが発生した場合にイベント マネージャ アプレットをトリガーします。
event syslog id	イベント マネージャ アプレットに syslog イベントを追加します。
event timer absolute time	絶対イベント タイマーを設定します。

コマンド	説明
event timer countdown time	カウントダウン タイマー イベントを設定します。
event timer watchdog time	ウォッチドッグ タイマー イベントを設定します。

event syslog id

イベント マネージャ アプレットに syslog イベントを追加するには、イベント マネージャ アプレット コンフィギュレーション モードで **event syslog id** コマンドを使用します。イベント マネージャ アプレットから syslog イベントを削除するには、このコマンドの **no** 形式を使用します。

event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

no event syslog id *nnnnnn*[*-nnnnnn*] [**occurs** *n*] [**period** *seconds*]

構文の説明

nnnnnn	syslog メッセージ ID を指定します。
occurs *n*	アプレットを呼び出すために syslog メッセージが発生する必要がある回数を示します。デフォルトは 1 です。有効な値は、1 ～ 4294967295 です。
period *seconds*	イベントが発生する必要がある秒数を示し、アプレットが呼び出される頻度を設定された期間中最大で 1 回に制限します。有効な値は、0 ～ 604800 です。値 0 は、期間が定義されていないことを示しています。

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
イベント マネージャ アプレット 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
9.2(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

アプレットをトリガーする単一の syslog メッセージまたは syslog メッセージの範囲を指定するには、**event syslog id** コマンドを使用します。

例

次に、syslog メッセージ 106201 がアプレットをトリガーする例を示します。

```
ciscoasa(config-applet)# event syslog id 106201
```

関連コマンド

コマンド	説明
event crashinfo	ASA でクラッシュが発生した場合にイベント マネージャ アプレットをトリガーします。
event none	イベント マネージャ アプレットを手動で呼び出します。
event timer absolute time	絶対イベント タイマーを設定します。
event timer countdown time	カウントダウン タイマー イベントを設定します。
event timer watchdog time	ウォッチドッグ タイマー イベントを設定します。

event timer

タイマー イベントを設定するには、イベント マネージャ アプレット コンフィギュレーション モードで **event timer** コマンドを使用します。タイマー イベントを削除するには、このコマンドの **no** 形式を使用します。

event timer {watchdog time *seconds* **| countdown time** *seconds* **| absolute time** *hh:mm:ss***}**

no event timer {watchdog time *seconds* **| countdown time** *seconds* **| absolute time** *hh:mm:ss***}**

構文の説明

absolute time	イベントが 1 日 1 回指定した時間に発生し、自動的に再開されることを指定します。
countdown time	イベントが 1 回発生し、そのイベントが削除された後に再度追加されない限り再開されないことを指定します。
hh:mm:ss	時刻形式を指定します。時間範囲は 00:00:00（深夜）～ 23:59:59 です。
seconds	秒数を指定します。有効な値の範囲は 0 ～604800 です。0 の値の場合、このタイマーはディセーブルになります。
watchdog time	イベントが設定された期間ごとに 1 回発生し、自動的に再開されることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
イベント マネージャ アプレット 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
9.2(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

1 日の指定した時間にイベントが 1 回発生し、自動的に再開されるようにするには、**event timer absolute time** コマンドを使用します。

イベントが 1 回発生し、そのイベントを削除した後に再度追加しない限り再開されないようにするには、**event timer countdown time** コマンドを使用します。

指定した期間ごとにイベントが 1 回発生し、自動的に再開されるようにするには、**event timer watchdog time** コマンドを使用します。

例

次に、1 日の指定した時間が表示された場合にイベントを発生させる例を示します。

```
ciscoasa(config-applet)# event timer absolute time 10:30:20
```

次に、1 日の指定した時間が表示された場合にイベントを発生させる例を示します。

```
ciscoasa(config-applet)# event timer countdown time 10:30:20
```

次に、イベントが 1 日 1 回発生し、自動的に再開されるようにする例を示します。

```
ciscoasa(config-applet)# event timer watchdog time 30
```

関連コマンド

コマンド	説明
event crashinfo	ASA でクラッシュが発生した場合にイベント マネージャ アプレットをトリガーします。
event none	イベント マネージャ アプレットを手動で呼び出します。
event syslog id	イベント マネージャ アプレットに syslog イベントを追加します。
event timer countdown time	カウントダウン タイマー イベントを設定します。
event timer watchdog time	ウォッチドッグ タイマー イベントを設定します。

exceed-mss

3 ウェイ ハンドシェイクでピアによって設定された TCP 最大セグメント サイズ（MSS）を超えるデータ長のパケットを許可またはドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** 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。

exceed-mss {**allow** | **drop**}

no exceed-mss {**allow** | **drop**}

構文の説明

allow	MSS を超えるパケットを許可します。この設定は、デフォルトです。
drop	MSS を超えるパケットをドロップします。

デフォルト

パケットは、デフォルトで許可されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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。
7.2(4)/8.0(4)	デフォルトが **drop** から **allow** に変更されました。

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。スリーウェイ ハンドシェイクでピアによって設定された TCP 最大セグメント サイズを超えるデータ長の TCP パケットをドロップするには、tcp マップ コンフィギュレーション モードで **exceed-mss** コマンドを使用します。

例

次に、MSS を超えた場合にポート 21 のフローをドロップする例を示します。

```
ciscoasa(config)# tcp-map tmap
ciscoasa(config-tcp-map)# exceed-mss drop
ciscoasa(config)# class-map cmap
ciscoasa(config-cmap)# match port tcp eq ftp
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。
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 advanced-options	TCP 正規化を含む、高度な接続機能を設定します。
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。

exempt-list

ポスチャ検証を免除されるリモート コンピュータ タイプのリストにエントリを追加するには、nac ポリシー nac フレームワーク コンフィギュレーション モードで **exempt-list** コマンドを使用します。免除リストからエントリを削除するには、このコマンドの **no** 形式を使用して、削除するエントリのオペレーティング システムおよび ACL を指定します。

exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

no exempt-list os "*os-name*" [**disable** | **filter** *acl-name* [**disable**]]

構文の説明

acl-name	ASA コンフィギュレーションに存在する ACL の名前。指定する場合は、**filter** キーワードの後に指定する必要があります。
disable	次の 2 つの機能のいずれかを実行します。 • "os-name" の後に入力した場合、ASA は、指定したオペレーティング システムを実行するリモート ホストで免除を行わず、NAC ポスチャ検証を適用します。 • *acl-name* の後に入力した場合、ASA は指定したオペレーティング システムを免除しますが、関連するトラフィックに ACL を割り当てません。
filter	コンピュータのオペレーティング システムが *os name* に一致する場合にトラフィックをフィルタリングするための ACL を適用します。**filter** と *acl-name* のペアは省略可能です。
os	オペレーティング システムをポスチャ検証から免除します。
os name	オペレーティング システム名。名前にスペースが含まれている場合にのみ引用符が必要です（たとえば "Windows XP"）。

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
nac ポリシー nac フレームワーク コンフィギュレーション	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
7.2(1)	このコマンドが追加されました。
8.0(2)	コマンド名が **vpn-nac-exempt** から **exempt-list** に変更されました。コマンドが、グループ ポリシー コンフィギュレーション モードから nac ポリシー nac フレームワーク コンフィギュレーション モードに移動されました。

使用上のガイドライン

コマンドでオペレーティング システムを指定しても、例外リストに追加済みのエントリは上書きされません。免除する各オペレーティング システムおよび ACL に対して 1 つずつコマンドを入力します。

no exempt-list コマンドを入力すると、NAC フレームワーク ポリシーからすべての免除が削除されます。エントリを指定してこのコマンドの **no** 形式を発行すると、そのエントリが免除リストから削除されます。

NAC ポリシーに関連付けられている免除リストからすべてのエントリを削除するには、キーワードを指定しないでこのコマンドの **no** 形式を使用します。

例

次に、ポスチャ検証を免除するコンピュータのリストに Windows XP を実行するすべてのホストを追加する例を示します。

```
ciscoasa(config-group-policy)# exempt-list os "Windows XP"
ciscoasa(config-group-policy)
```

次に、Windows XP を実行するすべてのホストを免除して、これらのホストのトラフィックに ACL acl-1 を適用する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

次に、免除リストから上記の例と同じエントリを削除する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list os "Windows XP" filter acl-1
ciscoasa(config-nac-policy-nac-framework)
```

次に、免除リストからすべてのエントリを削除する例を示します。

```
ciscoasa(config-nac-policy-nac-framework)# no exempt-list
ciscoasa(config-nac-policy-nac-framework)
```

関連コマンド

コマンド	説明
debug nac	NAC フレームワーク イベントのロギングをイネーブルにします。
nac-policy	Cisco NAC ポリシーを作成してアクセスし、そのタイプを指定します。
nac-settings	NAC ポリシーをグループ ポリシーに割り当てます。
show vpn-session.db	NAC の結果を含む、VPN セッションの情報を表示します。
show vpn-session_summary.db	IPsec、Cisco AnyConnect、および NAC の各セッションの数を表示します。

exit

現在のコンフィギュレーション モードを終了するか、特権 EXEC モードまたはユーザ EXEC モードからログアウトするには、**exit** コマンドを使用します。

exit

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
ユーザ 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
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

キー シーケンス Ctrl+Z を使用して、グローバル コンフィギュレーション（および上位の）モードを終了することもできます。このキー シーケンスは、特権 EXEC モードまたはユーザ EXEC モードでは動作しません。

特権 EXEC モードまたはユーザ EXEC モードで **exit** コマンドを入力すると、ASA からログアウトします。特権 EXEC モードからユーザ EXEC モードに戻るには、**disable** コマンドを使用します。

例

次に、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、セッションからログアウトする方法の例を示します。

```
ciscoasa(config)# exit
ciscoasa# exit

Logoff
```

次に、**exit** コマンドを使用してグローバル コンフィギュレーション モードを終了し、その後 **disable** コマンドを使用して特権 EXEC モードを終了する例を示します。

```
ciscoasa(config)# exit
ciscoasa# disable
ciscoasa#
```

関連コマンド

コマンド	説明
quit	コンフィギュレーション モードを終了するか、特権 EXEC モードまたはユーザ EXEC モードからログアウトします。

exp-flow-control

IP オプション インスペクションにおいて、パケット ヘッダー内に実験的フロー制御（FINN）オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **exp-flow-control** 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。

exp-flow-control action {allow | clear}

no exp-flow-control action {allow | clear}

構文の説明

allow	実験的フロー制御 IP オプションを含むパケットを許可します。
clear	実験的フロー制御オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、実験的フロー制御 IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# exp-flow-control action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

exp-measure

IP オプション インスペクションにおいて、パケット ヘッダー内に実験的測定（ZSU）オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **exp-measure** 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。

exp-measure action {allow | clear}

no exp-measure action {allow | clear}

構文の説明

allow	実験的測定 IP オプションを含むパケットを許可します。
clear	実験測定オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、実験的測定 IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# exp-measure action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。

expiry-time

再検証しないでオブジェクトをキャッシュする有効期限を設定するには、キャッシュ コンフィギュレーション モードで **expiry-time** コマンドを使用します。コンフィギュレーションから有効期限を削除して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。

expiry-time *time*

no expiry-time

構文の説明

時刻	ASA が再検証しないでオブジェクトをキャッシュする時間（分）。

デフォルト

デフォルトは 1 分です。

コマンド モード

次の表は、このコマンドを入力するモードを示しています。

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

有効期限とは、ASA が再検証しないでオブジェクトをキャッシュする時間（分）を指します。再検証では、内容が再度チェックされます。

例

次に、有効期限を 13 分に設定する例を示します。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# cache
ciscoasa(config-webvpn-cache)#expiry-time 13
ciscoasa(config-webvpn-cache)#
```

関連コマンド

コマンド	説明
cache	webvpn キャッシュ コンフィギュレーション モードを開始します。
cache-compressed	WebVPN キャッシュの圧縮を設定します。

コマンド	説明
disable	キャッシュをディセーブルにします。
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。

export

証明書をクライアントにエクスポートすることを指定するには、CTL プロバイダー コンフィギュレーション モードで **export** 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。

export certificate *trustpoint_name*

no export certificate [*trustpoint_name*]

構文の説明

certificate *trustpoint_name*　クライアントにエクスポートする証明書を指定します。

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
Ctl プロバイダー 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
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

CTL プロバイダー コンフィギュレーション モードで **export** コマンドを使用して、証明書をクライアントにエクスポートすることを指定します。トラストポイント名は、**crypto ca trustpoint** コマンドで定義します。証明書は、CTL クライアントで構成された CTL ファイルに追加されます。

例

次の例は、CTL プロバイダー インスタンスを作成する方法を示しています。

```
ciscoasa(config)# ctl-provider my_ctl
ciscoasa(config-ctl-provider)# client interface inside 172.23.45.1
ciscoasa(config-ctl-provider)# client username CCMAdministrator password XXXXXX encrypted
ciscoasa(config-ctl-provider)# export certificate ccm_proxy
ciscoasa(config-ctl-provider)# ctl install
```

関連コマンド

コマンド	説明
ctl	CTL クライアントの CTL ファイルを解析し、トラストポイントをインストールします。
ctl-provider	CTL プロバイダー コンフィギュレーション モードで CTL プロバイダー インスタンスを設定します。
クライアント	CTL プロバイダーへの接続が許可されるクライアントを指定し、クライアント認証用のユーザ名とパスワードを指定します。
service	CTL プロバイダーがリッスンするポートを指定します。
tls-proxy	TLS プロキシ インスタンスを定義し、最大セッション数を設定します。

export webvpn AnyConnect-customization

AnyConnect クライアント GUI をカスタマイズするカスタマイゼーション オブジェクトをエクスポートするには、特権 EXEC モードで **export webvpn AnyConnect-customization** コマンドを使用します。

export webvpn AnyConnect-customization type *type* **platform** *platform* **name** *name*

構文の説明

name	カスタマイゼーション オブジェクトを識別する名前。最大数は 64 文字です。
type	カスタマイゼーションのタイプ: • バイナリ:AnyConnect GUI を置き換える実行可能ファイル。 • トランスフォーム:MSI をカスタマイズするトランスフォーム。
url	XML カスタマイゼーション オブジェクトをエクスポートする *URL/filename* 形式のリモート パスとファイル名(最大 255 文字)。

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	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

AnyConnect カスタマイゼーション オブジェクトとは、キャッシュ メモリ内にあり、AnyConnect クライアント ユーザに表示される GUI 画面をカスタマイズする XML ファイルです。カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。

カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度 ASA にインポートできます。

Template の内容は、DfltCustomization オブジェクトの初期状態と同じです。

AnyConnect GUI で使用されるリソース ファイルの完全なリストおよびそれらのファイル名については『*AnyConnect VPN Client Administrator Guide*』を参照してください。

例

次に、AnyConnect GUI で使用されるシスコのロゴをエクスポートする例を示します。

```
ciscoasa# export webvpn AnyConnect-customization type resource company_logo.bmp
tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

関連コマンド

コマンド	説明
import webvpn customization	XML ファイルをカスタマイゼーション オブジェクトとしてキャッシュ メモリにインポートします。
revert webvpn customization	キャッシュ メモリからカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	キャッシュ メモリにあるカスタマイゼーション オブジェクトに関する情報を表示します。

export webvpn customization

クライアントレス SSL VPN ユーザに表示される画面をカスタマイズするカスタマイゼーション オブジェクトをエクスポートするには、特権 EXEC モードで **export webvpn customization** コマンドを使用します。

export webvpn customization *name url*

構文の説明

name	カスタマイゼーション オブジェクトを識別する名前。最大数は 64 文字です。
url	XML カスタマイゼーション オブジェクトをエクスポートする *URL/filename* 形式のリモート パスとファイル名（最大 255 文字）。

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	—	—

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

カスタマイゼーション オブジェクトとは、キャッシュ メモリ内にあり、クライアントレス SSL VPN ユーザに表示される画面（ログイン画面、ログアウト画面、ポータル ページ、使用可能な言語など）をカスタマイズする XML ファイルです。カスタマイゼーション オブジェクトをエクスポートすると、XML タグを含む XML ファイルが、指定した URL に作成されます。

カスタマイゼーション オブジェクトによって作成される *Template* という名前の XML ファイルには、空の XML タグが含まれており、新しいカスタマイゼーション オブジェクトを作成するための基礎として利用できます。このオブジェクトは変更したり、キャッシュ メモリから削除したりすることはできませんが、エクスポートし、編集して、新しいカスタマイゼーション オブジェクトとして再度 ASA にインポートできます。

Template の内容は、DfltCustomization オブジェクトの初期状態と同じです。

export webvpn customization コマンドを使用してカスタマイゼーション オブジェクトをエクスポートし、XML タグを変更し、**import webvpn customization** コマンドを使用して新しいオブジェクトとしてファイルをインポートできます。

例

次に、デフォルトのカスタマイゼーション オブジェクト（DfltCustomization）をエクスポートして、dflt_custom という名前の XML ファイルを作成する例を示します。

```
ciscoasa# export webvpn customization DfltCustomization tftp://209.165.200.225/dflt_custom
!!!!!!!!!!!!!!!!INFO: Customization object 'DfltCustomization' was exported to
tftp://10.86.240.197/dflt_custom
ciscoasa#
```

関連コマンド

コマンド	説明
import webvpn customization	XML ファイルをカスタマイゼーション オブジェクトとしてキャッシュ メモリにインポートします。
revert webvpn customization	キャッシュ メモリからカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	キャッシュ メモリにあるカスタマイゼーション オブジェクトに関する情報を表示します。

export webvpn plug-in

ASA のフラッシュ デバイスからプラグインをエクスポートするには、特権 EXEC モードで **export webvpn plug-in** コマンドを入力します。

import webvpn plug-in protocol *protocol URL*

構文の説明

protocol	• **rdp** Remote Desktop Protocol プラグインにより、リモート ユーザは Microsoft Terminal Services が実行するコンピュータに接続できます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://properjavardp.sourceforge.net/ です。 • **ssh,telnet** セキュア シェル プラグインにより、リモート ユーザがリモート コンピュータへのセキュア チャネルを確立したり、リモート ユーザが Telnet を使用してリモート コンピュータに接続したりできます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://javassh.org/ です。 **注意** **export webvpn plug-in protocol ssh,telnet** *URL* コマンドは、SSH と Telnet の*両方のプラグイン*をエクスポートします。SSH 用と Telnet 用にこのコマンドをそれぞれ入力*しないでください*。**ssh,telnet** ストリングを入力する場合は、両者の間にスペースは挿入*しません*。 • **vnc** Virtual Network Computing プラグインを使用すると、リモート ユーザはリモート デスクトップ共有をオンにしたコンピュータを、モニタ、キーボード、およびマウスを使用して表示および制御できます。シスコでは、変更を加えずにこのプラグインを再配布しています。オリジナルを掲載している Web サイトは、http://www.tightvnc.com/ です。
URL	リモート デバイスへのパス。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
	ルーテッド	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 モード	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

プラグインをエクスポートしても、フラッシュから削除されることはありません。エクスポートすると、指定した URL にプラグインのコピーが作成されます。

例

次のコマンドでは、RDP プラグインをエクスポートしています。

```
ciscoasa# export webvpn plug-in protocol rdp tftp://209.165.201.22/plugins/rdp-plugin.jar
```

関連コマンド

コマンド	説明
import webvpn plugin	指定されたプラグインをローカル デバイスから ASA フラッシュにインポートします。
revert webvpn plug-in protocol	ASA のフラッシュ デバイスから指定されたプラグインを削除します。
show import webvpn plug-in	ASA のフラッシュ デバイスに存在するプラグインのリストを示します。

export webvpn mst-translation

AnyConnect インストーラ プログラムを変換する Microsoft トランスフォーム（MST）をエクスポートするには、特権 EXEC モードで **export webvpn mst-translation** コマンドを使用します。

export webvpn mst-translation *component* **language** *language URL*

構文の説明

component	この MST が適用されるコンポーネント。有効な選択肢は AnyConnect のみです。
language	エクスポートされる MST の言語コード。ブラウザで必要とされるのと同じ形式のコードを使用します。
URL	トランスフォームをエクスポートする *URL/filename* 形式のリモート パスとファイル名（最大 255 文字）。

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	—	—

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

AnyConnect クライアント GUI と同様に、クライアント インストーラ プログラムに表示されるメッセージを翻訳できます。ASA はトランスフォームを使用して、インストーラに表示されるメッセージを翻訳します。トランスフォームによってインストレーションが変更されますが、元のセキュリティ署名 MSI は変化しません。これらのトランスフォームではインストーラ画面だけが翻訳され、クライアント GUI 画面は翻訳されません。

言語にはそれぞれ独自のトランスフォームがあります。トランスフォームは Orca などのトランスフォーム エディタで編集して、メッセージの文字列を変更できます。その後、トランスフォームを ASA にインポートします。ユーザがクライアントをダウンロードすると、クライアントはコンピュータの目的の言語（オペレーティング システムのインストール時に指定されたロケール）を検出し、該当するトランスフォームを適用します。

現時点では、30 の言語に対応するトランスフォームが用意されています。これらのトランスフォームは、cisco.com の AnyConnect クライアント ソフトウェア ダウンロード ページから、次の .zip ファイルで入手できます。

anyconnect-win-<VERSION>-web-deploy-k9-lang.zip

このファイルの <VERSION> は、AnyConnect のリリース バージョン（2.2.103 など）を表します。

例

次に、英語のトランスフォームを AnyConnect_Installer_English としてエクスポートする例を示します。

```
ciscoasa# export webvpn mst-translation AnyConnect language es
tftp://209.165.200.225/AnyConnect_Installer_English
```

関連コマンド

コマンド	説明
import webvpn customization	XML ファイルをカスタマイゼーション オブジェクトとしてキャッシュ メモリにインポートします。
revert webvpn customization	キャッシュ メモリからカスタマイゼーション オブジェクトを削除します。
show import webvpn customization	キャッシュ メモリにあるカスタマイゼーション オブジェクトに関する情報を表示します。

export webvpn translation-table

SSL VPN 接続を確立するリモート ユーザに表示される用語を変換するために使用される変換テーブルをエクスポートするには、特権 EXEC モードで **export webvpn translation-table** コマンドを使用します。

export webvpn translation-table *translation_domain* {**language** *language* | **template**} *url*

構文の説明

language	事前にインポート済みの変換テーブルの名前を指定します。値は、ブラウザの言語オプションの表現に従って入力します。
translation_domain	機能エリアおよび関連するメッセージです。表14-1 に、使用可能な変換ドメインを示します。
url	オブジェクトの URL 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	—	—

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

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

リモート ユーザに表示される各機能エリアとそのメッセージには独自の変換ドメインがあります。この変換ドメインは *translation_domain* 引数で指定します。表14-1 に、変換ドメインと変換される機能エリアを示します。

表14-1　変換ドメインと影響を受ける機能エリア

変換ドメイン	変換される機能エリア
AnyConnect	Cisco AnyConnect VPN Client のユーザ インターフェイスに表示されるメッセージ。
バナー	リモート ユーザに表示されるバナーと、VPN アクセスが拒否されたときのメッセージ。
CSD	Cisco Secure Desktop（CSD）のメッセージ。
customization	ログイン ページ、ログアウト ページ、ポータル ページのメッセージ、およびユーザによるカスタマイズが可能なすべてのメッセージ。
plugin-ica	Citrix プラグインのメッセージ。
plugin-rdp	Remote Desktop Protocol プラグインのメッセージ。
plugin-telnet,ssh	Telnet および SSH プラグインのメッセージ。
plugin-vnc	VNC プラグインのメッセージ。
PortForwarder	ポート フォワーディング ユーザに表示されるメッセージ。
url-list	ユーザがポータル ページの URL ブックマークに指定するテキスト。
webvpn	カスタマイズできないすべてのレイヤ 7 メッセージ、AAA メッセージ、およびポータル メッセージ。

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

以前にインポートされた変換テーブルをエクスポートすると、URL の場所にそのテーブルの XML ファイルが作成されます。**show import webvpn translation-table** コマンドを使用して、使用可能なテンプレート、およびインポート済みのテーブルのリストを表示できます。

export webvpn translation-table コマンドを使用してテンプレートまたは変換テーブルをダウンロードし、メッセージを変更し、**import webvpn translation-table** コマンドを使用して変換テーブルをインポートします。

例

次に、変換ドメイン *customization* 用のテンプレートをエクスポートする例を示します。このドメインは、クライアントレス SSL VPN 接続を確立するリモート ユーザがカスタマイズおよび表示可能なログイン ページ、ログアウト ページ、ポータル ページ、およびすべてのメッセージを変換するために使用します。ASA は、*Sales* という名前の XML ファイルを作成します。

```
ciscoasa# export webvpn translation-table customization template
tftp://209.165.200.225/Sales
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

次に、*zh* という名前の、以前にインポートされた中国語用変換テーブルをエクスポートする例を示します。この短縮形 zh は、Microsoft Internet Explorer ブラウザの [インターネット オプション] で中国語に指定されている短縮形に準拠しています。ASAは、*Chinese* という名前の XML ファイルを作成します。

```
ciscoasa# export webvpn translation-table customization language zh
tftp://209.165.200.225/Chinese
ciscoasa# !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

関連コマンド

コマンド	説明
import webvpn translation-table	変換テーブルをインポートします。
revert	キャッシュ メモリから変換テーブルを削除します。
show import webvpn translation-table	インポートした変換テーブルに関する情報を表示します。

export webvpn url-list

URL リストをリモートの場所にエクスポートするには、特権 EXEC モードで **export webvpn url-list** コマンドを使用します。

export webvpn url-list *name url*

構文の説明

name	URL リストを識別する名前。最大数は 64 文字です。
url	URL リストのソースへのリモート パス。最大数は 255 文字です。

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		—

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

WebVPN には、デフォルトで URL リストはありません。

export webvpn url-list コマンドを使用して、Template というオブジェクトをダウンロードできます。Template オブジェクトは変更または削除できません。Template オブジェクトの内容を編集してカスタム URL リストとして保存し、**import webvpn url-list** コマンドを使用してインポートし、カスタム URL リストを追加できます。

インポート済みの URL リストをエクスポートすると、URL の場所にそのリストの XML ファイルが作成されます。**show import webvpn url-list** コマンドを使用して、使用可能なテンプレート、およびインポート済みのテーブルのリストを表示できます。

例

次に、URL リスト *servers* をエクスポートする例を示します。

```
ciscoasa# export webvpn url-list servers2 tftp://209.165.200.225
ciscoasa#
```

関連コマンド

コマンド	説明
import webvpn url-list	URL リストをインポートします。
revert webvpn url-list	キャッシュ メモリから URL リストを削除します。
show import webvpn url-list	インポート済みの URL リストに関する情報を表示します。

export webvpn webcontent

リモートのクライアントレス SSL VPN ユーザに表示される、フラッシュ メモリ内のインポート済みコンテンツをエクスポートするには、特権 EXEC モードで **export webvpn webcontent** コマンドを使用します。

export webvpn webcontent *source url destination url*

構文の説明

destination url	エクスポート先の URL。最大数は 255 文字です。
source url	コンテンツがある ASA のフラッシュ メモリの URL。最大数は 64 文字です。

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		—

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

webcontent オプションを使用してエクスポートされるコンテンツは、リモートのクライアントレス ユーザに表示されるコンテンツです。これには、クライアントレス ポータルに表示されるインポート済みのヘルプ コンテンツや、カスタマイゼーション オブジェクトによって使用されるロゴなどがあります。

export webvpn webcontent コマンドの後に疑問符（**?**）を入力すると、エクスポート可能なコンテンツのリストを表示できます。次に例を示します。

```
ciscoasa# export webvpn webcontent ?

Select webcontent to export:
  /+CSCOE+/help/en/app-access-hlp.inc
  /+CSCOU+/cisco_logo.gif
```

例

次に、TFTP を使用してファイル *logo.gif* を、*logo_copy.gif* というファイル名で 209.165.200.225 にエクスポートする例を示します。

```
ciscoasa# export webvpn webcontent /+CSCOU+/logo.gif tftp://209.165.200.225/logo_copy.gif
!!!!* Web resource `/+CSCOU+/logo.gif' was successfully initialized
```

関連コマンド

コマンド	説明
import webvpn webcontent	クライアントレス SSL VPN ユーザに表示されるコンテンツをインポートします。
revert webvpn webcontent	コンテンツをフラッシュ メモリから削除します。
show import webvpn webcontent	インポートされたコンテンツに関する情報を表示します。

extended-security

IP オプション インスペクションにおいて、パケット ヘッダー内に拡張セキュリティ(E-SEC)オプションが存在する場合のアクションを定義するには、パラメータ コンフィギュレーション モードで **extended-security** 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。

extended-security action {allow | clear}

no extended-security action {allow | clear}

構文の説明

allow	拡張セキュリティ IP オプションを含むパケットを許可します。
clear	拡張セキュリティ オプションをパケット ヘッダーから削除してから、パケットを許可します。

デフォルト

デフォルトでは、IP オプション インスペクションは、拡張セキュリティ IP オプションを含むパケットをドロップします。

IP オプション インスペクション ポリシー マップで **default** コマンドを使用するとデフォルト値を変更できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	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
9.5(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、IP オプション インスペクション ポリシー マップで設定できます。

IP オプション インスペクションを設定して、どの IP パケットが所定の IP オプションを持ち、ASA を通過できるかを制御できます。変更せずにパケットを通過させたり、指定されている IP オプションをクリアしてからパケットを通過させたりできます。

例

次に、IP オプション インスペクションのアクションをポリシー マップで設定する例を示します。

```
ciscoasa(config)# policy-map type inspect ip-options ip-options_map
ciscoasa(config-pmap)# parameters
ciscoasa(config-pmap-p)# extended-security action allow
ciscoasa(config-pmap-p)# router-alert action allow
```

関連コマンド

コマンド	説明
class	ポリシー マップのクラス マップ名を指定します。
class-map type inspect	アプリケーション固有のトラフィックを照合するためのインスペクション クラス マップを作成します。
policy-map	レイヤ 3/4 のポリシー マップを作成します。
show running-config policy-map	現在のポリシー マップ コンフィギュレーションをすべて表示します。