CHAPTER 10

crypto isakmp disconnect-notify コマンド～ cxsc auth-proxy port コマンド

crypto isakmp disconnect-notify

ピアに対する切断通知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 **crypto isakmp disconnect-notify** コマンドを使用します。切断通知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。

crypto isakmp disconnect-notify

no crypto isakmp disconnect-notify

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　デフォルト値は [disabled] です。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp disconnect-notify** コマンドが追加されました。
7.2.(1)	**isakmp disconnect-notify** コマンドが、**crypto isakmp disconnect-notify** コマンドに置き換えられました。
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

次の削除理由を使用して、ピアに対する切断通知をイネーブルにできます。

- IKE_DELETE_RESERVED = 0
  無効なコード。送信しません。
- IKE_DELETE_BY_ERROR = 1
  タイムアウトの伝送エラー、またはキープアライブやその他の IKE パケット ACK に対する応答が予期されるときに発生した障害。デフォルトのテキストは「Connectivity to client lost.」です。
- IKE_DELETE_BY_USER_COMMAND = 2
  SA は、ユーザまたは管理者の手動による介入によって削除されました。デフォルトのテキストは「Manually Disconnected by Administrator.」です。
- IKE_DELETE_BY_EXPIRED_LIFETIME = 3
  SA の期限が切れています。デフォルトのテキストは「Maximum Configured Lifetime Exceeded.」です。
- IKE_DELETE_NO_ERROR = 4
  不明なエラーにより削除されました。
- IKE_DELETE_SERVER_SHUTDOWN = 5
  サーバをシャットダウンしています。
- IKE_DELETE_SERVER_IN_FLAMES = 6
  サーバに重大な問題があります。デフォルトのテキストは「Peer is having heat problems.」です。
- IKE_DELETE_MAX_CONNECT_TIME = 7
  アクティブなトンネルの最大許容時間が経過しました。EXPIRED_LIFETIME とは異なり、この理由は、この 1 つの SA だけでなく、IKE ネゴシエート/制御されたトンネル全体が切断されることを示します。デフォルトのテキストは「Maximum Configured Connection Time Exceeded.」です。
- IKE_DELETE_IDLE_TIMEOUT = 8
  トンネルがアイドル状態のまま最大許容時間が経過しました。そのため、この 1 つの SA だけでなく、IKE ネゴシエートされたトンネル全体が切断されます。デフォルトのテキストは「Maximum Idle Time for Session Exceeded.」です。
- IKE_DELETE_SERVER_REBOOT = 9
  サーバを再起動しています。
- IKE_DELETE_P2_PROPOSAL_MISMATCH = 10
  Phase2 プロポーザルの不一致。
- IKE_DELETE_FIREWALL_MISMATCH = 11
  ファイアウォール パラメータの不一致。
- IKE_DELETE_CERT_EXPIRED = 12
  ユーザ認定が必要です。デフォルトのメッセージは「User or Root Certificate has Expired.」です。
- IKE_DELETE_CLIENT_NOT_ALLOWED = 13
  許可されていないクライアント タイプまたはバージョン。
- IKE_DELETE_FW_SERVER_FAIL = 14
  Zone Integrity サーバに接続できませんでした。
- IKE_DELETE_ACL_ERROR = 15
  AAA からダウンロードされた ACL は挿入できません。デフォルトのメッセージは「ACL parsing error.」です。

例

次の例では、グローバル コンフィギュレーション モードで、ピアに対する切断通知をイネーブルにします。

```
ciscoasa(config)# crypto isakmp disconnect-notify
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp identity

フェーズ 1 ID をピアに送信するように設定するには、グローバル コンフィギュレーション モードで **crypto isakmp identity** 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。

crypto isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

no crypto isakmp identity {**address** | **hostname** | **key-id** *key-id-string* | **auto**}

構文の説明

address	ISAKMP の識別情報を交換するホストの IP アドレスを使用します。
auto	ISAKMP ネゴシエーションを、接続のタイプ（事前共有キーの IP アドレス、または証明書認証用の証明書 DN）によって判別します。
hostname	ISAKMP 識別情報を交換するホストの完全修飾ドメイン名を使用します（デフォルト）。この名前は、ホスト名とドメイン名で構成されます。
key-id *key_id_string*	リモート ピアが事前共有キーを検索するために使用するストリングを指定します。

デフォルト

デフォルトの ISAKMP ID は、**crypto isakmp identity auto** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp identity** コマンドが追加されました。
7.2(1)	**isakmp identity** コマンドが、**crypto isakmp identity** コマンドに置き換えられました。
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。

例

次の例では、グローバル コンフィギュレーション モードで、接続タイプに応じて、IPsec ピアと通信するためのインターフェイス上で ISAKMP ネゴシエーションをイネーブルにします。

```
ciscoasa(config)# crypto isakmp identity auto
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp nat-traversal

NAT トラバーサルをグローバルに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 ISAKMP がイネーブルになっていることを確認します(イネーブルにするには **crypto isakmp enable** コマンドを使用します)。NAT トラバーサ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。

crypto isakmp nat-traversal *natkeepalive*

no crypto isakmp nat-traversal *natkeepalive*

構文の説明

natkeepalive	NAT キープアライブ間隔を、10 ～ 3600 秒の範囲で設定します。デフォルトは 20 秒です。

デフォルト

デフォルトでは、NAT トラバーサルは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
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
7.0(1)	**isakmp nat-traversal** コマンドが追加されました。
7.2.(1)	**isakmp nat-traversal** コマンドが、**crypto isakmpnat-traversal** コマンドに置き換えられました。
8.0(2)	NAT トラバーサルが、デフォルトでイネーブルになりました。
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

NAT(PAT を含む)は、IPsec も使用されている多くのネットワークで使用されていますが、IPsec パケットが NAT デバイスを正常に通過することを妨げる非互換性が数多くあります。NAT トラバーサルを使用すると、ESP パケットが 1 つ以上の NAT デバイスを通過できるようになります。

ASA は、IETF の「UDP Encapsulation of IPsec Packets」ドラフトのバージョン 2 とバージョン 3 (http://www.ietf.org/html.charters/ipsec-charter.html から入手可能)に記述されているとおりに NAT トラバーサルをサポートしています。また、ダイナミック クリプト マップとスタティック クリプト マップの両方で NAT トラバーサルをサポートしています。

このコマンドは、ASA 上で NAT-T をグローバルにイネーブルにします。クリプト マップ エントリでディセーブルにするには、**crypto map set nat-t-disable** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードで、ISAKMP をイネーブルにし、NAT トラバーサルのキープアライブ間隔を 30 秒に設定する例を示します。

```
ciscoasa(config)# crypto isakmp enable
ciscoasa(config)# crypto isakmp nat-traversal 30
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy authentication

IKE ポリシー内の認証方式を指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy authentication** コマンドを使用します。ISAKMP 認証方式を削除するには、関連する **clear configure** コマンドを使用します。

crypto isakmp policy *priority* **authentication** {**crack** | **pre-share** | **rsa-sig**}

構文の説明

crack	認証方式として、IKE CRACK を指定します。
pre-share	認証方式として事前共有キーを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
rsa-sig	認証方式として RSA シグニチャを指定します。 RSA シグニチャにより、IKE ネゴシエーションに対して否認防止を実行できます。これは基本的に、ユーザがピアとの IKE ネゴシエーションを行ったかどうかを、第三者に証明できることを意味します。

デフォルト

デフォルトの ISAKMP ポリシー認証は **pre-share** 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
7.0(1)	**isakmp policy authentication** コマンドが追加されました。
7.2.(1)	**isakmppolicy authentication** コマンドが、**crypto isakmppolicy authentication** コマンドに置き換えられました。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。

RSA シグニチャを指定する場合は、CA サーバから証明書を取得するように ASA とそのピアを設定する必要があります。事前共有キーを指定する場合は、ASA とそのピアに、事前共有キーを別々に設定する必要があります。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy authentication** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーで RSA シグネチャの認証方式を使用するように設定します。

```
ciscoasa(config)# crypto isakmp policy 40 authentication rsa-sig
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy encryption

IKE ポリシーで使用する暗号化アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy encryption** コマンドを使用します。暗号化アルゴリズムをデフォルト値の **des** 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。

crypto isakmp policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

no crypto isakmp policy *priority* **encryption** {**aes** | **aes-192** | **aes-256** | **des** | **3des**}

構文の説明

3des	IKE ポリシーで、Triple DES 暗号化アルゴリズムを使用することを指定します。
aes	IKE ポリシーで使用する暗号化アルゴリズムが、128 ビット キーを使用する AES であることを指定します。
aes-192	IKE ポリシーで使用する暗号化アルゴリズムが、192 ビット キーを使用する AES であることを指定します。
aes-256	IKE ポリシーで使用する暗号化アルゴリズムが、256 ビット キーを使用する AES であることを指定します。
des	IKE ポリシーで使用する暗号化アルゴリズムが、56 ビット DES-CBC であることを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトの ISAKMP ポリシー暗号化は、**3des** 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
7.0(1)	**isakmp policy encryption** コマンドが追加されました。
7.2.(1)	**isakmp policy encryption** コマンドが、**crypto isakmp policy encryption** コマンドに置き換えられました。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy encryption** コマンドを使用する例を示します。この例では、プライオリティ番号 25 の IKE ポリシーに使用するアルゴリズムとして 128 ビット キーの AES 暗号化を設定します。

```
ciscoasa(config)# crypto isakmp policy 25 encryption aes
```

次に、グローバル コンフィギュレーション モードでの入力で、プライオリティ番号 40 の IKE ポリシー内で 3DES アルゴリズムを使用するように設定する例を示します。

```
ciscoasa(config)# crypto isakmp policy 40 encryption 3des
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy group

IKE ポリシーに対して Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy group** コマンドを使用します。Diffie-Hellman グループ ID をデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

crypto isakmp policy *priority* **group** {**1** | **2** | **5**}

no crypto isakmp policy *priority* **group**

構文の説明

group 1	IKE ポリシーで、768 ビットの Diffie-Hellman グループを使用することを指定します。これはデフォルト値です。
group 2	IKE ポリシーで、1024 ビットの Diffie-Hellman グループ 2 を使用することを指定します。
group 5	IKE ポリシーで、1536 ビットの Diffie-Hellman グループ 5 を使用することを指定します。
priority	IIKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。

デフォルト

デフォルトのグループ ポリシーはグループ 2 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
7.0(1)	**isakmp policy group** コマンドが追加されました。
7.2.(1)	**isakmp policy group** コマンドが、**crypto isakmppolicy group** コマンドに置き換えられました。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

グループ オプションには、768 ビット（DH グループ 1）、1024 ビット（DH グループ 2）、および 1536 ビット（DH グループ 5）の 3 つがあります。1024 ビットと 1536 ビットの Diffie-Hellman グループは、セキュリティが高くなりますが、CPU の処理時間は長くなります。

（注） Cisco VPN Client のバージョン 3.x 以上では、ISAKMP ポリシーで DH グループ 2 を使用する必要があります（DH グループ 1 に設定すると、Cisco VPN Client は接続できません）。

AES は、VPN-3DES のライセンスがある ASA に限りサポートされます。AES では大きなキー サイズが提供されるため、ISAKMP ネゴシエーションでは Diffie-Hellman（DH）グループ 1 やグループ 2 ではなく、グループ 5 を使用する必要があります。グループ 5 を設定するには、**crypto isakmp policy priority group 5** コマンドを使用します。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy group** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに対し、グループ 2、1024 ビットの Diffie Hellman を使用するように設定しています。

```
ciscoasa(config)# crypto isakmp policy 40 group 2
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy hash

IKE ポリシーのハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy hash** コマンドを使用します。ハッシュ アルゴリズムをデフォルト値の SHA-1 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。

crypto isakmp policy *priority* hash {**md5** | **sha**}

no crypto isakmp policy *priority* **hash**

構文の説明

md5	IKE ポリシーのハッシュ アルゴリズムとして MD5（HMAC バリアント）を指定します。
priority	プライオリティをポリシーに一意に指定および割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
sha	IKE ポリシーのハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1（HMAC バリアント）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
7.0(1)	**isakmp policy hash** コマンドが追加されました。
7.2.(1)	**isakmp policy hash** コマンドが、**crypto isakmp policy hash** コマンドに置き換えられました。

使用上のガイドライン

IKE ポリシーは、IKE ネゴシエーション時に使用するパラメータのセットを定義したものです。

ハッシュ アルゴリズムのオプションには、SHA-1 と MD5 の 2 つがあります。MD5 のダイジェストの方が小さく、SHA-1 よりもやや速いと見なされています。

例

次に、グローバル コンフィギュレーション モードで、**crypto isakmp policy hash** コマンドを使用する例を示します。この例では、プライオリティ番号 40 の IKE ポリシーに MD5 ハッシュ アルゴリズムを使用することを指定します。

```
ciscoasa(config)# crypto isakmp policy 40 hash md5
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp policy lifetime

IKE セキュリティ アソシエーションが期限切れになるまでのライフタイムを指定するには、グローバル コンフィギュレーション モードで **crypto isakmp policy lifetime** コマンドを使用します。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）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。

crypto isakmp policy *priority* **lifetime** *seconds*

no crypto isakmp policy *priority* **lifetime**

構文の説明

priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
seconds	各セキュリティ アソシエーションが期限切れになるまでの秒数を指定します。有限のライフタイムを提示するには、120 ～ 2147483647 秒の整数を使用します。無制限のライフタイムの場合は、0 秒を使用します。

デフォルト

デフォルト値は 86,400 秒（1 日）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
7.0(1)	**isakmp policy lifetime** コマンドが追加されました。
7.2.(1)	**isakmp policy lifetime** コマンドが、**crypto isakmp policy lifetime** コマンドに置き換えられました。

使用上のガイドライン

IKE は、ネゴシエーションを開始するとき、自身のセッション用のセキュリティ パラメータについて合意しようとします。次に、各ピアのセキュリティ アソシエーションが、合意されたパラメータを参照します。ピアは、ライフタイムが期限切れになるまで、セキュリティ アソシエーションを保持します。ピアがライフタイムを提示していない場合は、無限のライフタイムを指定できます。セキュリティ アソシエーションは、期限切れになるまで、その後の IKE ネゴシエーションで利用できるため、新しい IPsec セキュリティ アソシエーションを設定するときに時間を節約できます。ピアは、現在のセキュリティ アソシエーションが期限切れになる前に、新しいセキュリティ アソシエーションをネゴシエートします。

ライフタイムを長くするほど、ASA は以後の IPSec セキュリティ アソシエーションをより迅速にセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルトをそのまま使用することを推奨します。

（注） IKE セキュリティ アソシエーションのライフタイムが無限に設定されている場合、ピアが有限のライフタイムを提示したときは、ピアからネゴシエートされた有限のライフタイムが使用されます。

例

次に、グローバル コンフィギュレーション モードで、プライオリティ番号 40 の IKE ポリシーに IKE セキュリティ アソシエーションのライフタイムを 50,400 秒（14 時間）に設定する例を示します。

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 50400
```

次に、グローバル コンフィギュレーション モードでの入力で、IKE セキュリティ アソシエーションのライフタイムを無限に設定する例を示します。

```
ciscoasa(config)# crypto isakmp policy 40 lifetime 0
```

関連コマンド

clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto isakmp reload-wait

すべてのアクティブなセッションが自発的に終了しないと ASA をリブートできないようにするは、グローバル コンフィギュレーション モードで **crypto isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するのを待たずに ASA をリブートするには、このコマンドの **no** 形式を使用します。

crypto isakmp reload-wait

no crypto isakmp reload-wait

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
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
7.0(1)	**isakmp reload-wait** コマンドが追加されました。
7.2.(1)	**isakmp reload-wait** コマンドが、**crypto isakmpreload-wait** コマンドに置き換えられました。
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。

例

次に、グローバル コンフィギュレーション モードを開始し、すべてのアクティブ セッションが終了するまで待機してからリブートすることを ASA に指示する例を示します。

```
ciscoasa(config)# crypto isakmp reload-wait
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	すべての ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	すべての ISAKMP ポリシー コンフィギュレーションをクリアします。

コマンド	説明
clear crypto isakmp sa	IKE ランタイム SA データベースをクリアします。
show running-config crypto isakmp	アクティブなコンフィギュレーションをすべて表示します。

crypto key generate

アイデンティティ証明書用のキー ペアを生成するには、グローバル コンフィギュレーション モードで **crypto key generate** コマンドを使用します。このコマンドは、RSA と楕円曲線署名アルゴリズム（ECDSA）キーによって異なります。

crypto key generate rsa [**usage-keys** | **general-keys**] [**label** *key-pair-label*] [**modulus** *size*] [**noconfirm**]

crypto key generate ecdsa [**label** *key-pair-label*] **elliptic-curve** [**256** | **384** | **521**] [**noconfirm**]

構文の説明

dsa [**label name**]	キー ペアの生成時に Suite-B EDCSA アルゴリズムを使用します。
elliptic-curve [**256** | **384** | **521**]	スイート B EDCSA キー ペアのビット長を指定します。デフォルト値は 384 です。
general-keys	1 つの汎用キー ペアを生成します。これはデフォルトのキー ペア タイプです。
label *key-pair-label*	キー ペアに関連付ける名前を指定します。このキー ペアのラベルは一意である必要があります。ラベルを指定しない場合、キー ペアは静的に Default-RSA-Key または Default-ECDSA-Key という名前になります。
modulus *size*	キー ペアのモジュラス サイズ（512、768、1024、2048、3072 および 4096）を指定します。デフォルトのモジュラス サイズは 2048 です。
noconfirm	すべての対話型プロンプトを非表示にします。
usage-keys	シグニチャ用と暗号化用の 2 つのキー ペアを生成します。これは、対応する識別用に 2 つの証明書が必要なことを意味します。

デフォルト

デフォルトの RSA キー ペアのタイプは、**general key** です。デフォルトのモジュラス サイズは 2048 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
9.0(1)	ECDSA キーのサポートが追加されました。
9.9(2)	モジュラス サイズを 3072 に設定できるようになりました。

使用上のガイドライン

SSL、SSH、および IPsec 接続をサポートするためにキー ペアを生成するには、**crypto key generate** コマンドを使用します。生成されたキー ペアは、コマンド構文の一部として指定できるラベルで識別されます。キー ペアを参照しないトラストポイントは、デフォルトの Default-RSA-Key を使用できます。SSH 接続では常にこのキーが使用されます。SSL は独自の証明書やキーをダイナミックに生成するため、証明書やキーがトラストポイントに設定されていない限り、このことは SSL に影響を与えません。

例

次に、ラベル mypubkey を持つ RSA キー ペアを生成する例を示します。

```
ciscoasa(config)# crypto key generate rsa label mypubkey
INFO: The name for the keys will be: mypubkey
Keypair generation process
ciscoasa(config)#
```

次に、デフォルトのラベルを持つ RSA キー ペアを生成する例を示します。

```
ciscoasa(config)# crypto key generate rsa
INFO: The name for the keys will be: <Default-RSA-Key>
Keypair generation process begin. Please wait...
ciscoasa(config)#
```

次に、ECDSA キーを生成する例を示します。RSA キーペアを保存するための十分なスペースがないため警告メッセージが表示されます。

```
ciscoasa(config)# crypto key generate ecdsa label new-ecdsa-key elliptic-curve 521
INFO: The name for the keys will be: new-ecdsa-key
Keypair generation process begin. Please wait...
```

関連コマンド

コマンド	説明
crypto key zeroize	キー ペアを削除します。
show crypto key	キー ペアを表示します。

crypto key zeroize

指定したタイプのキー ペアを削除するには、グローバル コンフィギュレーション モードで **crypto key zeroize** コマンドを使用します。

crypto key zeroize {**rsa** | **ecdsa**} [**label** *key-pair-label*] [**default**] [**noconfirm**]

構文の説明

default	指定されたタイプのデフォルトのキー ペアを削除します。
ecdsa	キー タイプとして ECDSA を指定します。
label *key-pair-label*	削除するキー ペアを識別します。ラベルを指定しない場合、システムは、指定されたタイプのキー ペアをすべて削除します。
noconfirm	すべての対話型プロンプトを非表示にします。
rsa	キー タイプとして RSA 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
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。
9.0(1)	ECDSA のサポートが追加されました。

例

次に、グローバル コンフィギュレーション モードで、すべての RSA キー ペアを削除する例を示します。

```
ciscoasa(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All router certs issued using these keys will also be removed.

Do you really want to remove these keys? [yes/no] y
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto key generate	アイデンティティ証明書用のキー ペアを生成します。

crypto large-cert-acceleration enable（廃止）

ASA がハードウェアで 2048 ビットの RSA キー演算を実行できるようにするには、グローバル コンフィギュレーション モードで **crypto large-cert-acceleration enable** コマンドを使用します。ソフトウェアで 2048 ビットの RSA キー演算を実行するには、**no crypto large-cert-acceleration enable** コマンドを使用します。

crypto large-cert-acceleration enable

no crypto large-cert-acceleration enable

構文の説明

このコマンドにはキーワードまたは引数はありません。

デフォルト

デフォルトでは、2048 ビットの RSA キー演算がソフトウェアで実行されます。

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
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
8.2(3)	このコマンドが追加されました。
8.2(5)	このコマンドは廃止されました。**crypto engine large-mod-accel** コマンドに置き換えられました。

使用上のガイドライン

このコマンドは、ASA 5510、ASA 5520、ASA 5540、および ASA 5550 でのみ使用できます。このコマンドは、ASA 5580 では使用できません。

例

次に、2048 ビットの RSA キー演算がハードウェアでイネーブルになっている例を示します。

```
ciscoasa (config)# show running-config crypto large-cert-acceleration
crypto large-cert-acceleration enable
ciscoasa (config)#
```

関連コマンド

コマンド	説明
clear configure crypto	2048 ビットの RSA キー コンフィギュレーションを、残りのクリプト コンフィギュレーションとともにクリアします。
show running-config crypto	2048 ビットの RSA キー コンフィギュレーションを、残りのクリプト コンフィギュレーションとともに表示します。

crypto map interface

以前に定義したクリプト マップ セットをインターフェイスに適用するには、グローバル コンフィギュレーション モードで **crypto map interface** コマンドを使用します。このクリプト マップ セットをインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

no crypto map *map-name* **interface** *interface-name* [**ipv6-local-address** *ipv6-address*]

構文の説明

interface-name	ASA が VPN ピアとのトンネルの確立に使用するインターフェイスを指定します。ISAKMP がイネーブルになっており、CA を使用して証明書を取得する場合は、CA 証明書で指定されているアドレスを持つインターフェイスにする必要があります。
map-name	クリプト マップ セットの名前を指定します。
ipv6-local-address *ipv6-address*	IPv6 アドレスを指定します。

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
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。
8.3(1)	**ipv6-local-address** キーワー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

このコマンドを使用して、クリプト マップ セットを任意のアクティブな ASA のインターフェイスに割り当てます。ASA では、あらゆるアクティブ インターフェイスを IPsec の終端にすることができます。インターフェイスで IPSec サービスを提供するには、事前にそのインターフェイスにクリプト マップ セットを割り当てる必要があります。

インターフェイスに割り当てることができるクリプト マップ セットは 1 つだけです。同じマップ名でシーケンス番号が異なるクリプト マップ エントリが複数ある場合、それらのエントリは同じセットの一部であり、そのインターフェイスにすべて適用されます。ASA は、シーケンス番号が最も小さいクリプト マップ エントリを最初に評価します。

インターフェイスに複数の IPv6 アドレスが設定されており、IPv6 環境で LAN-to-LAN VPN トンネルをサポートするように ASA を設定する場合、**ipv6-local-address** キーワードを使用します。

(注) ASA では、クリプト マップ、ダイナミック マップ、および IPSec 設定を、オンザフライで変更できます。設定を変更する場合、変更によって影響を受ける接続のみが ASA によって停止させられます。たとえば、アクセス リスト内のエントリを削除して、クリプト マップに関連付けられた既存のアクセス リストを変更した場合、関連する接続だけがダウンします。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

すべてのスタティック クリプトマップでは、アクセス リスト、トランスフォーム セット、および IPsec ピアという 3 つの部分を定義する必要があります。これらの 1 つが欠けている場合、そのクリプト マップは不完全であるため、ASA は次のエントリに進みます。ただし、クリプト マップがアクセス リストと一致し、他の 2 つの要件のいずれか、または両方と一致しない場合には、ASA はトラフィックを廃棄します。

すべてのクリプト マップが完全であることを確認するには、**show running-config crypto map** コマンドを使用します。不完全なクリプト マップを修正するには、クリプト マップを削除し、欠けているエントリを追加してからクリプト マップを再適用します。

例

次に、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップ セットを外部インターフェイスに割り当てる例を示します。トラフィックは、この outside インターフェイスを通過するとき、ASA によって mymap セット内のすべてのクリプト マップ エントリを使用して評価されます。発信トラフィックが、いずれかの mymap クリプト マップ エントリのアクセス リストと一致する場合、ASA はそのクリプト マップ エントリのコンフィギュレーションを使用して、セキュリティ アソシエーションを形成します。

```
ciscoasa(config)# crypto map mymap interface outside
```

次に、必要最小限のクリプト マップ エントリ コンフィギュレーションの例を示します。

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap set transform-set my_t_set1
ciscoasa(config)# crypto map mymap set peer 10.0.0.1
```

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 map ipsec-isakmp dynamic

所定のクリプト マップ エントリで既存のダイナミック クリプト マップを参照させるようにするには、グローバル コンフィギュレーション モードで **crypto map ipsec-isakmp dynamic** コマンドを使用します。クロス リファレンスを削除するには、このコマンドの **no** 形式を使用します。

ダイナミック クリプト マップ エントリを作成するには、**crypto dynamic-map** コマンドを使用します。ダイナミック クリプト マップ セットを作成した後に、**crypto map ipsec-isakmp dynamic** コマンドを使用して、ダイナミック クリプト マップ セットをスタティック クリプト マップに追加します。

crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

no crypto map *map-name seq-num* **ipsec-isakmp dynamic** *dynamic-map-name*

構文の説明

dynamic-map-name	既存のダイナミック クリプト マップを参照するクリプト マップ エントリの名前を指定します。
ipsec-isakmp	IKE がクリプト マップ エントリの IPsec セキュリティ アソシエーションを確立することを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

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
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
7.0(1)	このコマンドは、**ipsec-manual** キーワードを削除するように変更されました。
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

クリプト マップ エントリを定義してから、**crypto map interface** コマンドを使用して、ダイナミック クリプト マップ セットをインターフェイスに割り当てることができます。

ダイナミック クリプト マップを使用することで、保護の対象となるトラフィックのフィルタリングと分類、そのトラフィックに適用するポリシーの定義という 2 つの機能を利用できます。最初の機能はインターフェイス上のトラフィック フローが対象となり、2 番めの機能はそのトラフィックのために（IKE を通じて）実行されるネゴシエーションが対象となります。

IPsec ダイナミック クリプト マップでは、次のことを指定します。

- 保護するトラフィック
- セキュリティ アソシエーションを確立する IPsec ピア
- 保護対象のトラフィックとともに使用するトランスフォーム セット
- キーおよびセキュリティ アソシエーションの使用方法または管理方法

クリプト マップ セットとは、それぞれ異なるシーケンス番号（*seq-num*）を持つが、マップ名が同じであるクリプト マップ エントリの集合です。したがって、所定のインターフェイスで、あるトラフィックには指定のセキュリティを適用してピアに転送し、その他のトラフィックには別の IPsec セキュリティを適用して同じまたは別のピアに転送できます。これを行うには、マップ名は同じであるが、シーケンス番号がそれぞれ異なる 2 つのクリプト マップ エントリを作成します。

seq-num 引数として割り当てる番号は、任意に決定しないでください。この番号によって、クリプト マップ セット内の複数のクリプト マップ エントリにランクが付けられます。小さいシーケンス番号のクリプト マップ エントリは、大きいシーケンス番号のマップ エントリよりも先に評価されます。つまり、番号の小さいマップ エントリの方がプライオリティが高くなります。

（注） クリプト マップをダイナミック クリプト マップにリンクする場合は、ダイナミック クリプト マップを指定する必要があります。指定すると、**crypto dynamic-map** コマンドを使用して以前に定義した既存のダイナミック クリプト マップにクリプト マップがリンクされます。クリプト マップ エントリが変換された後に加えた変更は、有効になりません。たとえば、set peer 設定への変更は有効になりません。ただし、ASA は起動中に変更を保存します。ダイナミック クリプト マップをクリプト マップに変換して戻す場合、この変更は有効となり、**show running-config crypto map** コマンドの出力に表示されます。ASA は、リブートされるまでこれらの設定を維持します。

例

次に、グローバル コンフィギュレーション モードで、mymap というクリプト マップが test というダイナミック クリプト マップを参照するように設定する例を示します。

```
ciscoasa(config)# crypto map mymap ipsec-isakmp dynamic test
ciscoasa(config)#
```

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 map match address

アクセス リストをクリプト マップ エントリに割り当てるには、グローバル コンフィギュレーション モードで **crypto map match address** コマンドを使用します。クリプト マップ エントリからアクセス リストを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **match address** *acl_name*

no crypto map *map-name seq-num* **match address** *acl_name*

構文の説明

acl_name	暗号化アクセス リストの名前を指定します。この名前は、一致対象となる名前付き暗号化アクセス リストの名前引数と一致している必要があります。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

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
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。
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

このコマンドは、すべてのスタティック クリプトマップに対して必要です。**crypto dynamic-map** コマンドを使用してダイナミック クリプト マップを定義する場合、このコマンドは必須ではありませんが、使用することを強く推奨します。

アクセス リストを定義するには、**access-list** コマンドを使用します。アクセス リストのヒット カウントは、トンネルが開始されたときにのみ増加します。トンネルが動作状態になると、パケット単位のフローではヒット カウントは増加しません。トンネルがドロップされてから再開されると、ヒット カウントは増加します。

ASA は、アクセス リストを使用して、IPsec クリプトで保護するトラフィックと保護を必要としないトラフィックとを区別します。また、許可 ACE に一致する発信パケットを保護し、許可 ACE に一致する着信パケットが確実に保護されるようにします。

ASA は、パケットが deny ステートメントと一致すると、クリプト マップ内の残りの ACE を使用したパケットの評価を省略して、順番に次のクリプト マップ内の ACE を使用したパケットの評価を再開します。*ACL のカスケード処理*には、ACL 内の残りの ACE の評価をバイパスする拒否 ACE の使用、およびクリプト マップ セット内の次のクリプト マップに割り当てられた ACL を使用したトラフィックの評価の再開が含まれています。クリプト マップごとに異なる IPsec 設定を関連付けることができるため、拒否 ACE を使用することで、特別なトラフィックを対応するクリプト マップでの以後の評価から除外し、異なるセキュリティを提供する別のクリプト マップ、または異なるセキュリティを必要とする別のクリプト マップの permit 文と特別なトラフィックを照合することができます。

（注） クリプト アクセス リストでは、インターフェイスを通過するトラフィックを許可するかどうかは判別されません。このような判別は、**access-group** コマンドを使用してインターフェイスに直接適用されるアクセス リストによって行われます。

トランスペアレント モードでは、宛先アドレスは ASA の IP アドレス、管理アドレスである必要があります。トランスペアレント モードでは、ASA へのトンネルだけが許可されます。

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 map set connection-type

クリプト マップ エントリのバックアップ サイト間機能の接続タイプを指定するには、グローバル コンフィギュレーション モードで **crypto map set connection-type** 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。

crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

no crypto map *map-name seq-num* **set connection-type** {**answer-only** | **originate-only** | **bidirectional**}

構文の説明

answer-only	ピアが、適切な接続先ピアを決定するための最初の独自の交換中に、まず着信 IKE 接続だけに応答することを指定します。
bidirectional	ピアが、クリプト マップ エントリに基づいて接続を受け入れ、発信できることを指定します。これは、すべての Site-to-Site 接続のデフォルトの接続タイプです。
map-name	クリプト マップ セットの名前を指定します。
originate-only	ピアが、適切な接続先ピアを決定するために最初の独自の交換を開始することを指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
set connection-type	クリプト マップ エントリのバックアップ サイト間機能の接続タイプを指定します。answer-only、originate-only、および bidirectional の 3 つのタイプの接続があります。

デフォルト

デフォルトの設定は bidirectional です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0	このコマンドが追加されました。
9.0	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

crypto map set connection-type コマンドは、バックアップ LAN-to-LAN 機能の接続タイプを指定します。接続の一方の側で複数のバックアップ ピアを指定できます。

この機能は、次のプラットフォーム間でのみ使用できます。

- 2 つの Cisco ASA 5500 シリーズ
- Cisco ASA 5500 シリーズと Cisco VPN 3000 コンセントレータ
- Cisco ASA 5500 シリーズと、Cisco PIX セキュリティ アプライアンス ソフトウェア バージョン 7.0 以上を実行しているセキュリティ アプライアンス

バックアップ LAN-to-LAN 接続を設定するには、接続の一方の側を **originate-only** キーワードを使用して originate-only として設定し、複数のバックアップ ピアがある側を **answer-only** キーワードを使用して answer-only として設定することを推奨します。originate-only 側では、**crypto map set peer** コマンドを使用してピアのプライオリティを指定します。originate-only ASA は、リストの最初のピアとネゴシエートしようとします。ピアが応答しない場合、ASA はピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。

（注） IKEv2 は、サイトからサイトへのバックアップをサポートしていません。これは、発信専用または応答専用のキーワードを使用する場合に設定されます。IKEv2 を使用する場合、暗号マップ セット接続タイプは双方向でなければなりません。

このように設定した場合、originate-only ピアは、最初に独自のトンネルを確立してピアとネゴシエートしようとします。その後は、いずれかのピアが通常の LAN-to-LAN 接続を確立することができ、いずれかの側からのデータがトンネル接続を開始できます。

トランスペアレント ファイアウォール モードでは、このコマンドは表示されますが、インターフェイスに対応付けられたクリプト マップに含まれるクリプト マップ エントリでは、connection-type 値は answer-only 以外の値に設定できません。

表10-1 に、サポートされているすべてのコンフィギュレーションを示します。他の組み合わせは、予測不可能なルーティング問題を引き起こす場合があります。

表10-1　サポートされているバックアップ LAN-to-LAN 接続タイプ

リモート側	中央側
Originate-Only	Answer-Only
Bi-Directional	Answer-Only
Bi-Directional	Bi-Directional

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、接続タイプを originate-only に設定する例を示します。

```
ciscoasa(config)# crypto map mymap 10 set connection-type originate-only
ciscoasa(config)#
```

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 map set df-bit

per-signature algorithm（SA）do-not-fragment（DF）ポリシーを設定するには、グローバル コンフィギュレーション モードで **crypto map set df-bit** コマンドを使用します。DF ポリシ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。

crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

no crypto map *name priority* **set df-bit** [**clear-df** | **copy-df** | **set-df**]

構文の説明

name	クリプト マップ セットの名前を指定します。
priority	クリプト マップ エントリに割り当てるプライオリティを指定します。

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
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
9.0(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

元の DF ポリシー コマンドが保持され、インターフェイスのグローバル ポリシー設定として機能しますが、SA については **crypto map** コマンドが優先されます。

crypto map set ikev1 phase1-mode

メインまたはアグレッシブへの接続を開始する場合にフェーズ 1 の IKEv1 モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev1 phase1-mode** コマンドを使用します。フェーズ 1 IKEv1 ネゴシエーションの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。

crypto map *map-name seq-num* **set ikev1 phase1-mode** {**main** | **aggressive [group1** | **group2** | **group5** | **group14** | **group15** | **group16**| **group19** | **group20** | **group21**]}

no crypto map *map-name seq-num* **set ikev1 phase1-mode** {**main** | **aggressive [group1** | **group2** | **group5** | **group14** | **group15** | **group16** | **group19** | **group20** | **group21**]}

構文の説明

aggressive	フェーズ 1 の IKEv1 ネゴシエーションにアグレッシブ モードを指定します。
group14	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group15	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group16	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group19	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group20	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group21	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
主要	フェーズ 1 の IKEv1 ネゴシエーションにメイン モードを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトのフェーズ 1 モードは **main** 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	—

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。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。
8.4(1)	**ikev1** キーワー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。
9.13(1)	**DH グループ 14、15、および 16** のサポートが追加され、デフォルトとして設定されています。**グループ 1、2** および**グループ 5** のオプションは廃止され、以降のリリースで削除されます。
9.15(1)	**DH グループ 1、2**、および **5** のサポートは廃止されました。

使用上のガイドライン

このコマンドは、発信側モードでのみ機能します。応答側モードでは機能しません。アグレッシブ モードの Diffie-Hellman グループを含めるかどうかは任意です。含めない場合、ASA はグループ 2 を使用します。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、グループ 2 を使用してフェーズ 1 のモードをアグレッシブに設定する例を示します。

```
ciscoasa(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group2
ciscoasa(config)# crypto map mymap 10 set ikev1 phase1mode aggressive group14
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
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 map set ikev2 ipsec-proposal

クリプト マップ エントリで使用する IKEv2 プロポーザルを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev2 ipsec-proposal** コマンドを使用します。クリプト マップ エントリから特定のプロポーザルを削除するには、プロポーザルの名前を指定してこのコマンドの **no** 形式を使用します。プロポーザルをすべて指定するか何も指定せずに、クリプト マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1*
[*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal** *propsal-name1*
[*… proposal-name11*]

no crypto map *map-name seq-num* **set ikev2 ipsec-proposal**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに対応するシーケンス番号を指定します。
propsal-name1 *proposal-name11*	IKEv2 の IPsec プロポーザルの名前を 1 つ以上指定します。このコマンドで指定するプロポーザルはすべて、**crypto ipsec ikev2 ipsec-proposal** コマンドで定義されている必要があります。各暗号マップ エントリは、最大 11 個のプロポーザルをサポートします。

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
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(1)	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。

リリース	変更内容
9.15(1)	次の整合性、暗号化、および暗号化方式は、このリリースから削除されました。 • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

使用上のガイドライン

すべてのクリプト マップ エントリに、IKEv1 トランスフォーム セットまたは IKEv2 プロポーザルが必要です。

IPsec IKEv2 の開始側とは反対側にあるピアは、最初に一致したプロポーザルをセキュリティ アソシエーションに使用します。ローカルの ASA がネゴシエーションを開始した場合、ASA は、**crypto map** コマンドで指定した順番どおりに、トランスフォーム セットの内容をピアに提示します。ピアがネゴシエーションを開始すると、ローカルの ASA は、クリプト マップ エントリ内の、ピアから送信された IPsec パラメータと一致する最初のプロポーザルを使用します。

IPsec の開始側とは反対側にあるピアが、一致するプロポーザルの値を見つけられない場合、IPsec はセキュリティ アソシエーションを確立しません。トラフィックを保護するセキュリティ アソシエーションがないため、開始側はトラフィックをドロップします。

プロポーザルのリストを変更するには、新しいリストを作成して指定し、古いリストと置き換えます。

次のコマンドを使用してクリプト マップを変更すると、ASA は、指定したシーケンス番号と同じ番号のクリプト マップ エントリだけを変更します。たとえば、次のコマンドを入力すると、ASA は、56des-sha というプロポーザルをリストの最後に挿入します。

```
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal 128aes-md5 128aes-sha
192aes-md5
ciscoasa(config)# crypto map map1 1 set ikev2 ipsec-proposal 56des-sha
ciscoasa(config)#
```

次のコマンドの応答は、前の 2 つのコマンドで行った変更を合わせたものになります。

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set ipsec-proposal 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

クリプト マップ エントリ内のプロポーザルの順番を再設定するには、エントリを削除し、マップ名とシーケンス番号の両方を指定してから、エントリを再作成します。たとえば、次のコマンドでは、シーケンス番号 3 の *map2* というクリプト マップ エントリを再設定します。

```
asa2(config)# no crypto map map2 3 set ikev2 ipsec-proposal
asa2(config)# crypto map map2 3 set ikev2 ipsec-proposal 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

例

次に、10 個のプロポーザルで構成された、map2 というクリプト マップ エントリを作成する例を示します。

```
ciscoasa(config)# crypto map map2 10 set ikev2 ipsec-proposal 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップをコンフィギュレーションからクリアします。
clear configure crypto map	コンフィギュレーションから、すべてのクリプト マップをクリアします。
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
crypto ipsec transform-set	トランスフォーム セットを設定します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set ikev2 mode

クリプト マップ エントリで使用する IKEv2 モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev2 mode** コマンドを使用します。このモードをリセットするには、コンフィギュレーション モードで このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set ikev2 mode** {**transport** | **transport-require** | **tunnel**}

no crypto map *map-name seq-num* **set ikev2 mode** {**transport** | **transport-require** | **tunnel**}

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに対応するシーケンス番号を指定します。
transport	transport モードに設定します。
transport-require	transport モードを必須にします。
tunnel	tunnel モード(デフォルト)を設定します。

コマンド デフォルト

モードが設定されていない場合、デフォルトのモードは tunnel です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

IKEv2 では、このモードはトンネルに ESP 暗号化と認証を適用するために指定します。これにより、ESP が適用されるオリジナルの IP パケットの部分が決定されます。

デフォルトは tunnel カプセル化モードです。transport カプセル化モードは、ピアがこのモードをサポートしていない場合に tunnel モードにフォールバックできる転送モードです。transport モードは、リモート アクセス VPN では推奨されません。

- tunnel モード(デフォルト):カプセル化モードは tunnel モードになります。tunnel モードでは、ESP 暗号化と認証が元の IP パケット全体(IP ヘッダーおよびデータ)に適用され、最終的な送信元アドレスと宛先アドレスが非表示になります。元の IP データグラム全体が暗号化され、新しい IP パケットのペイロードになります。

このモードでは、ルータなどのネットワーク デバイスが IPsec のプロキシとして動作できます。つまり、ルータがホストに代わって暗号化を行います。送信元ルータがパケットを暗号化し、IPsec トンネルを使用して転送します。宛先ルータは元の IP データグラムを復号化し、宛先システムに転送します。トンネル モードの大きな利点は、エンド システムを変更しなくても IPsec を利用できるということです。また、トラフィック分析から保護することもできます。トンネル モードを使用すると、攻撃者にはトンネルのエンドポイントしかわからず、トンネリングされたパケットの本来の送信元と宛先はわかりません（これらがトンネルのエンドポイントと同じ場合でも同様）。

- transport モード：カプセル化モードは transport モードになります。ピアがこのモードをサポートしていない場合は tunnel モードにフォールバックできます。transport モードでは IP ペイロードだけが暗号化され、元の IP ヘッダーはそのまま使用されます。

  このモードには、各パケットに数バイトしか追加されず、パブリック ネットワーク上のデバイスに、パケットの最終的な送信元と宛先を認識できるという利点があります。transport モードでは、中間ネットワークでの特別な処理（たとえば QoS）を、IP ヘッダーの情報に基づいて実行できるようになります。ただし、レイヤ 4 ヘッダーが暗号化されるため、パケットの検査が制限されます。

- transport-require：カプセル化モードは transport 専用モードになり、トンネル モードへのフォールバックは許可されません。

カプセル化モードのネゴシエーションは次のとおりです。

- イニシエータが転送モードを提案し、レスポンダがトンネル モードで応答した場合、イニシエータはトンネル モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport モードで応答した場合、応答側は tunnel モードにフォールバックします。
- 発信側が tunnel モードを提示し、応答側が transport-require モードの場合、応答側はプロポーザルを送信しません。
- 同様に、イニシエータが transport-require モードで、レスポンダがトンネル モードの場合は、レスポンダから NO PROPOSAL CHOSEN が送信されます。

関連コマンド

コマンド	説明
show running-config crypto map	クリプト マップの設定内容を表示します。
clear configure crypto map	コンフィギュレーションから、すべてのクリプト マップをクリアします。

crypto map set ikev2 phase1-mode

メインまたはアグレッシブへの接続を開始する場合にフェーズ 1 の IKEv2 モードを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev2 phase1-mode** コマンドを使用します。フェーズ 1 IKEv2 ネゴシエーションの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。

crypto map *map-name seq-num* **set ikev2 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

no crypto map *map-name seq-num* **set ikev2 phase1-mode** {**main** | **aggressive** [**group1** | **group2** | **group5**]}

構文の説明

aggressive	フェーズ 1 の IKEv2 ネゴシエーションにアグレッシブ モードを指定します。
group1	IPsec で新しい Diffie-Hellman 交換を実行するときに、768 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group2	IPsec で新しい Diffie-Hellman 交換を実行するときに、1024 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group5	IPsec で新しい Diffie-Hellman 交換を実行するときに、1536 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
主要	フェーズ 1 の IKEv2 ネゴシエーションにメイン モードを指定します。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトのフェーズ 1 モードは **main** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。
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

このコマンドは、発信側モードでのみ機能します。応答側モードでは機能しません。アグレッシブ モードの Diffie-Hellman グループを含めるかどうかは任意です。含めない場合、ASA はグループ 2 を使用します。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、グループ 2 を使用してフェーズ 1 のモードをアグレッシブに設定する例を示します。

```
ciscoasa(config)# crypto map mymap 10 set ikev2 phase1mode aggressive group2
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
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 map set ikev2 pre-shared-key

AnyConnect IKEv2 接続の事前共有キーを指定するには、グローバル コンフィギュレーション モードで **crypto map set ikev2 pre-shared-key** 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。

crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

no crypto map *map-name seq-num* **set ikev2 pre-shared-key** *key*

構文の説明

key	1 ～ 128 文字の英数字文字列。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの値や動作はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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
8.4(1)	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。

例

次に、事前共有キー SKTIWHT を設定する例を示します。

```
ciscoasa(config)# crypto map crypto_map_example set ikev2 pre-shared-key SKTIWHT
```

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 map set inheritance

クリプト マップ エントリ用に生成されるセキュリティ アソシエーションの精度（シングルまたはマルチ）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 **set inheritance** コマンドを使用します。クリプト マップ エントリの継承の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。

crypto map *map-name seq-num* **set inheritance** {**data** | **rule**}

no crypto map *map-name seq-num* **set inheritance** {**data** | **rule**}

構文の説明

data	ルールで指定されているアドレス範囲内のアドレス ペアごとに 1 つのトンネルを指定します。
map-name	クリプト マップ セットの名前を指定します。
rule	クリプト マップに関連付けられている各 ACL エントリに 1 つのトンネルを指定します。これはデフォルトです。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
set inheritance	継承のタイプを **data** または **rule** に指定します。継承では、各セキュリティ ポリシー データベース（SPD）ルールに対して 1 つのセキュリティ アソシエーション（SA）を生成したり、範囲内の各アドレス ペアに対して複数のセキュリティ SA を生成したりすることができます。

デフォルト

デフォルト値は **rule** です。

コマンド モード

次の表は、このコマンドを入力できるモードを示しています。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
7.0(1)	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

このコマンドは、ASA がトンネルに応答しているときではなく、トンネルを開始しているときにのみ機能します。データ設定を使用すると、多数の IPsec SA が作成される可能性があります。この場合、メモリが消費され、全体としてのトンネルが少なくなります。データ設定は、セキュリティへの依存が非常に高いアプリケーションに対してのみ使用してください。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap を設定し、継承タイプを data に設定する例を示します。

```
ciscoasa(config)# crypto map mymap 10 set inheritance data
ciscoasa(config)#
```

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 map set nat-t-disable

接続の NAT-T をクリプト マップ エントリに基づいて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 **crypto map set nat-t-disable** コマンドを使用します。このクリプト マップ エントリの NAT-T 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。

crypto map *map-name seq-num* **set nat-t-disable**

no crypto map *map-name seq-num* **set nat-t-disable**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

このコマンドのデフォルト設定はオンではありません（したがって、NAT-T はデフォルトでイネーブルです）。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

isakmp nat-traversal コマンドを使用して NAT-T をグローバルにイネーブルにします。その後に、**crypto map set nat-t-disable** コマンドを使用して、特定のクリプト マップ エントリの NAT-T をディセーブルにできます。

例

次のコマンドでは、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップ エントリの NAT-T をディセーブルにします。

```
ciscoasa(config)# crypto map mymap 10 set nat-t-disable
ciscoasa(config)#
```

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。
isakmp nat-traversal	すべての接続の NAT-T をイネーブルにします。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set peer

クリプト マップ エントリの IPsec ピアを指定するには、グローバル コンフィギュレーション モードで **crypto map set peer** コマンドを使用します。クリプト マップ エントリから IPsec ピアを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

no crypto map *map-name seq-num* **set peer** {*ip_address* | *hostname*}{*...ip_address10* | *hostname10*}

構文の説明

hostname	ピアを、ASA **name** コマンドで定義したホスト名で指定します。
ip_address	ピアを IP アドレス（IPv4 または IPv6）で指定します。
map-name	クリプト マップ セットの名前を指定します。
peer	クリプト マップ エントリ内で IPsec ピアをホスト名または IP アドレス（IPv4 または IPv6）で指定します。9.14(1) 以降、IKEv2 でも複数のピアがサポートされています。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

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
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)	このコマンドは、最大 10 個のピア アドレスを許容するように変更されました。
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。
9.14(1)	IKEv2 の複数ピアサポートが追加されました。

使用上のガイドライン

このコマンドは、すべてのスタティッククリプトマップに対して必要です。**crypto dynamic-map** コマンドを使用してダイナミック クリプト マップ エントリを定義する場合、このコマンドは必須ではなく、ほとんど使用しません。これは、ピアが通常は未知のものであるためです。

複数のピアを設定することは、フォールバックリストを指定することと同じです。各トンネルについて、ASA は、リストの最初のピアとネゴシエーションを試みます。ピアが応答しない場合、ASA はピアが応答するか、またはリストにピアがなくなるまで下に向かってリストを検索します。バックアップ LAN-to-LAN 機能を使用している場合（つまり、クリプトマップ接続タイプが originate-only の場合）にのみ複数のピアを設定できます。詳細については、**crypto map set connection-type** コマンドを参照してください。

(注) 9.14(1) 以降、IKEv2 では複数のピアがサポートされています。

例

次に、グローバル コンフィギュレーション モードで、IKE を使用してセキュリティ アソシエーションを確立するクリプト マップ コンフィギュレーションの例を示します。この例では、ピア 10.0.0.1 またはピア 10.0.0.2 のどちらかと、セキュリティ アソシエーションを確立できます。

```
ciscoasa(config)# crypto map mymap 10 ipsec-isakmp
ciscoasa(config)# crypto map mymap 10 match address 101
ciscoasa(config)# crypto map mymap 10 set transform-set my_t_set1
ciscoasa(config)# crypto map mymap 10 set peer 10.0.0.1 10.0.0.2
```

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 map set pfs

クリプト マップ エントリ用の新しいセキュリティ アソシエーションの要求時に PFS を要求するように IPsec を設定するか、または新しいセキュリティ アソシエーションの要求の受信時に PFS を要求するように IPsec 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 **crypto map set pfs** コマンドを使用します。IPsec が PFS を要求しないことを指定するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group14 | group 15 | group 16 | group19 | group20 | group21 | group24]**

no crypto map *map-name seq-num* **set pfs [group1 | group2 | group5 | group14 | group 15 | group 16 | group19 | group20 | group21 | group24]**

構文の説明

group14	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group15	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group16	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。
group19	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。IKEv1 ではサポートされていません。
group20	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。IKEv1 ではサポートされていません。
group21	IPsec で新しい Diffie-Hellman 交換を実行するときに、2048 ビットの Diffie-Hellman プライム モジュラス グループを使用することを指定します。IKEv1 ではサポートされていません。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトでは、PFS は設定されません。

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
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)	このコマンドは変更され Diffie-Hellman グループ 7 が追加されました。
8.0(4)	**group 7** コマンド オプションは廃止されました。グループ 7 を設定しようとするとエラー メッセージが生成され、代わりにグループ 5 が使用されます。
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。
9.13(1)	DH グループ 14、15、および 16 のサポートが追加されました。DH グループ 1、2、5、および 24 のオプションは廃止され、以降のリリースで削除されます。
9.15(1)	DH グループ 1、2、5、および 24 のオプションは、このリリースでサポートが廃止されました。

使用上のガイドライン

PFS を使用すると、新しいセキュリティ アソシエーションをネゴシエートするたびに新しい Diffie-Hellman 交換が発生します。この交換によって、処理時間が長くなります。PFS を使用すると、セキュリティがさらに向上します。1 つのキーが攻撃者によってクラックされた場合でも、侵害されるのはそのキーで送信されたデータだけになるためです。

このコマンドを使用すると、クリプト マップ エントリ用の新しいセキュリティ アソシエーションを要求するとき、ネゴシエーション中に IPsec が PFS を要求します。**set pfs** ステートメントでグループが指定されていない場合、ASA はデフォルト（グループ 2）を送信します。

ピアがネゴシエーションを開始するときに、ローカル コンフィギュレーションで PFS が指定されている場合、ピアは PFS 交換を実行する必要があります。実行しない場合、ネゴシエーションは失敗します。ローカル コンフィギュレーションでグループが指定されていない場合、ASA はデフォルトの group2 が指定されているものと見なします。ローカル コンフィギュレーションでグループ 2 またはグループ 5 が指定されている場合は、そのグループがピアのオファーに含まれている必要があります。含まれていない場合、ネゴシエーションは失敗します。

ネゴシエーションが成功するには、（Diffie-Hellman グループの有無に関係なく）LAN to LAN トンネルの両端で PFS が設定されている必要があります。設定されている場合、グループは完全一致でなければなりません。ASA はピアからのいずれの PFS のオファーも受け入れません。

1536 ビットの Diffie-Hellman プライム モジュラス グループであるグループ 5 は、グループ 1 やグループ 2 よりも高いセキュリティを提供します。ただし、他のグループより処理時間が長くなります。

ASA は、Cisco VPN Client と対話するときに PFS 値を使用しません。その代わり、フェーズ 1 でネゴシエートされた値を使用します。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap 10 用の新しいセキュリティ アソシエーションをネゴシエートするときに、必ず PFS を使用することを指定する例を示します。

```
ciscoasa(config)# crypto map mymap 12 set pfs ipsec-isakmp
ciscoasa(config)#crypto map mymap 12 set pfs group2
ciscoasa{config}# crypto map mymap 12 set pfs group14.
```

関連コマンド

コマンド	説明
clear isakmp sa	アクティブな IKE セキュリティ アソシエーションを削除します。
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。
tunnel-group	トンネル グループとそのパラメータを設定します。

crypto map set reverse-route

クリプト マップ エントリに基づいた任意の接続の逆ルート注入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 **crypto map set reverse-route** コマンドを使用します。クリプト マップ エントリに基づいた任意の接続の逆ルート注入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。

crypto map *map-name seq-num* **set reverse-route [dynamic]**

no crypto map *map-name seq-num s***et reverse-route [dynamic]**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
dynamic	RRI は、IPsec トンネルが作成または破棄されると動的になり、追加または削除されます。

デフォルト

このコマンドのデフォルト設定はオフです。

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
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。
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。
9.7(1)	ダイナミック RRI のサポートが追加されました。

使用上のガイドライン

ダイナミックが指定されていない場合:

RRI は設定で行われ、静的とみなされます。設定が変更または削除されるまでそのままになります。ASA は、ルーティング テーブルにスタティック ルートを自動的に追加し、OSPF を使用してそれらのルートをプライベート ネットワークまたはボーダー ルータに通知します。

ダイナミックが指定されている場合:

このアプローチでは、IPsec セキュリティ アソシエーション（SA）の確立が成功するとルートが作成されます。ルートは、ネゴシエートされたセレクタの情報に基づいて追加されます。IPsec SA's が削除されると、このルートは削除されます。また、ダイナミックからスタティックへの設定変更、およびその逆の設定変更により、その暗号マップの既存の IPsec トンネルが破棄されます。

通常、RRI ルートは、ルートが存在せず、トラフィックを暗号化する必要がある場合に、トンネルを開始するために使用されます。ダイナミック RRI がサポートされると、トンネルが確立されるまでルートが存在しません。したがって、ダイナミック RRI が設定された ASA は通常、レスポンダとしてのみ動作します。

ダイナミック RRI は IKEv2 ベースのスタティック暗号マップだけに適用されます。

例

次に、グローバル コンフィギュレーション モードで、mymap という名前のクリプト マップの逆ルート注入をイネーブルにする例を示します。

```
ciscoasa(config)# crypto map mymap 10 set reverse-route
ciscoasa(config)#
```

グローバル コンフィギュレーション モードで入力された次の例では、トンネル確立時にリバース ルート インジェクションが有効になります。

```
ciscoasa(config)#crypto map mymap 1 set reverse-route dynamic
```

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 map set security-association lifetime

特定のクリプト マップ エントリについて、IPsec セキュリティ アソシエーションをネゴシエートするときに使用されるグローバル ライフタイム値を上書きするには、グローバル コンフィギュレーション モードで **crypto map set security-association lifetime** コマンドを使用します。クリプト マップ エントリのライフタイム値をグローバル値にリセットするには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set security-association lifetime** {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

no crypto map *map-name seq-num* **set security-association lifetime** {**seconds** ***number*** | **kilobytes** {***number*** | **unlimited**}}

構文の説明

kilobytes {*number* | **unlimited**}	所定のセキュリティ アソシエーションの有効期限が切れるまでに、そのセキュリティ アソシエーションを使用してピア間を通過できるトラフィックの量を KB 単位で指定します。指定できる範囲は 10 ～ 2147483647 KB です。グローバル デフォルトは 4,608,000 キロバイトです。 この設定は、リモート アクセス VPN 接続には適用されません。サイト間 VPN のみに適用されます。
map-name	クリプト マップ セットの名前を指定します。
seconds *number*	セキュリティ アソシエーションの有効期限が切れるまでの存続時間（秒数）を指定します。指定できる範囲は 120 ～ 214783647 秒です。グローバルのデフォルトは 28,800 秒（8 時間）です。 この設定は、リモート アクセスとサイト間 VPN の両方に適用されます。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。

デフォルト

デフォルトの KB 数は 4,608,000 で、デフォルトの秒数は 28,800 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。
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。
9.1(2)	unlimited 引数が追加されました。

使用上のガイドライン

クリプト マップのセキュリティ アソシエーションは、グローバル ライフタイムに基づいてネゴシエートされます。

IPsec セキュリティ アソシエーションでは、共有秘密キーが使用されます。これらのキーとセキュリティ アソシエーションは、両方同時にタイムアウトになります。

特定のクリプト マップ エントリでライフタイム値が設定されている場合、ASA は、セキュリティ アソシエーションのネゴシエート時に新しいセキュリティ アソシエーションを要求するときに、ピアへの要求でクリプト マップ ライフタイム値を指定し、これらの値を新しいセキュリティ アソシエーションのライフタイムとして使用します。ASA は、ピアからネゴシエーション要求を受信すると、ピアが指定するライフタイム値またはローカルに設定されたライフタイム値のうち、小さい方を新しいセキュリティ アソシエーションのライフタイムとして使用します

サイト間 VPN 接続の場合、「時間指定」と「トラフィック量」の 2 つのライフタイムがあります。これらのライフタイムのいずれかに最初に到達すると、セキュリティ アソシエーションが期限切れになります。リモート アクセス VPN セッションでは、指定時刻ライフタイムのみが適用されます。

（注） ASA では、クリプト マップ、ダイナミック マップ、および IPsec 設定を動作中に変更できます。設定を変更する場合、変更によって影響を受ける接続のみが ASA によって停止させられます。たとえば、アクセス リスト内のエントリを削除して、クリプト マップに関連付けられた既存のアクセス リストを変更した場合、関連する接続だけがダウンします。アクセス リスト内の他のエントリに基づく接続は、影響を受けません。

指定時刻ライフタイムを変更するには、**crypto map set security-association lifetime seconds** コマンドを使用します。指定時刻ライフタイムを使用すると、指定した秒数が経過した後にキーおよびセキュリティ アソシエーションがタイムアウトします。

例

次のコマンドでは、グローバル コンフィギュレーション モードで、クリプト マップ mymap のセキュリティ アソシエーション ライフタイムを秒単位および KB 単位で指定します。

```
ciscoasa(config)# crypto map mymap 10 set security-association lifetime seconds 1400
kilobytes 3000000
ciscoasa(config)#
```

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 map set tfc-packets

IPsec SA でダミーのトラフィック フローの機密性(TFC)パケット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 **crypto map set tfc-packets** コマンドを使用します。IPsec SA で TFC パケット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。

crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

no crypto map *name priority* **set tfc-packets** [**burst** *length* | *auto*] [**payload-size** *bytes* | *auto*] [**timeout** *second* | *auto*]

構文の説明

name	クリプト マップ セットの名前を指定します。
priority	クリプト マップ エントリに割り当てるプライオリティを指定します。

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
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
9.0(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

このコマンドは、クリプト マップの既存の DF ポリシー(SA レベルで)を設定します。

crypto map set transform-set

クリプト マップ エントリで使用する IKEv1 トランスフォーム セットを指定するには、グローバル コンフィギュレーション モードで **crypto map set transform-set** コマンドを使用します。クリプト マップ エントリから特定のトランスフォーム セット名を削除するには、トランスフォーム セットの名前を指定してこのコマンドの **no** 形式を使用します。トランスフォーム セットをすべて指定するか何も指定せずに、クリプト マップ エントリを削除するには、このコマンドの **no** 形式を使用します。

crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set** *transform-set-name1*
[*… transform-set-name11*]

no crypto map *map-name seq-num* **set transform-set**

構文の説明

map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに対応するシーケンス番号を指定します。
transform-set-name1 *transform-set-name11*	トランスフォーム セットの名前を 1 つ以上指定します。このコマンドで指定するトランスフォーム セットは、**crypto ipsec transform-set** コマンドで定義されている必要があります。各クリプト マップ エントリは、11 個までのトランスフォーム セットをサポートしています。

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
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。
7.2(1)	クリプト マップ エントリにおけるトランスフォーム セットの最大数が変更されました。
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

このコマンドは、すべてのクリプト マップ エントリで必要です。

IPsec の開始側とは反対側にあるピアは、最初に一致したトランスフォーム セットをセキュリティ アソシエーションに使用します。ローカルの ASA がネゴシエーションを開始した場合、ASA は、**crypto map** コマンドで指定した順番どおりに、トランスフォーム セットの内容をピアに提示します。ピアがネゴシエーションを開始すると、ローカルの ASA は、クリプト マップ エントリ内の、ピアから送信された IPsec パラメータと一致する最初のトランスフォーム セットを使用します。

IPsec の開始側とは反対側にあるピアが、一致するトランスフォーム セットの値を見つけられない場合、IPsec はセキュリティ アソシエーションを確立しません。トラフィックを保護するセキュリティ アソシエーションがないため、開始側はトラフィックをドロップします。

トランスフォーム セットのリストを変更するには、新しいリストを再度指定して、古いリストと置き換えます。

次のコマンドを使用してクリプト マップを変更すると、ASA は、指定したシーケンス番号と同じ番号のクリプト マップ エントリだけを変更します。たとえば、次のコマンドを入力すると、ASA は、56des-sha というトランスフォーム セットをリストの最後に挿入します。

```
ciscoasa(config)# crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5
ciscoasa(config)# crypto map map1 1 transform-set 56des-sha
ciscoasa(config)#
```

次のコマンドの応答は、前の 2 つのコマンドで行った変更を合わせたものになります。

```
ciscoasa(config)# show running-config crypto map
crypto map map1 1 set transform-set 128aes-md5 128aes-sha 192aes-md5 56des-sha
ciscoasa(config)#
```

クリプト マップ エントリ内のトランスフォーム セットの順番を再設定するには、エントリを削除し、マップ名とシーケンス番号の両方を指定してから、エントリを再作成します。たとえば、次のコマンドでは、シーケンス番号 3 の map2 というクリプト マップ エントリを再設定します。

```
asa2(config)# no crypto map map2 3 set transform-set
asa2(config)# crypto map map2 3 set transform-set 192aes-sha 192aes-md5 128aes-sha
128aes-md5
asa2(config)#
```

例

「**crypto ipsec transform-set**（トランスフォーム セットの作成または削除）」の項には、10 個のトランスフォーム セット コマンドが示されています。次に、10 個の同じトランスフォーム セットで構成された、map2 というクリプト マップ エントリを作成する例を示します。

```
ciscoasa(config)# crypto map map2 10 set transform-set 3des-md5 3des-sha 56des-md5
56des-sha 128aes-md5 128aes-sha 192aes-md5 192aes-sha 256aes-md5 256aes-sha
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、ASA が IKE を使用してセキュリティ アソシエーションを確立する場合に最小限必要となるクリプト マップ コンフィギュレーションの例を示します。

```
ciscoasa(config)# crypto map map2 10 ipsec-isakmp
ciscoasa(config)# crypto map map2 10 match address 101
ciscoasa(config)# crypto map map2 set transform-set 3des-md5
ciscoasa(config)# crypto map map2 set peer 10.0.0.1
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto dynamic-map	すべてのダイナミック クリプト マップをコンフィギュレーションからクリアします。
clear configure crypto map	コンフィギュレーションから、すべてのクリプト マップをクリアします。
crypto dynamic-map set transform-set	ダイナミック クリプト マップ エントリで使用するトランスフォーム セットを指定します。
crypto ipsec transform-set	トランスフォーム セットを設定します。
show running-config crypto dynamic-map	ダイナミック クリプト マップのコンフィギュレーションを表示します。
show running-config crypto map	クリプト マップの設定内容を表示します。

crypto map set trustpoint

クリプト マップ エントリのフェーズ 1 ネゴシエーション中に、認証用に送信する証明書を指定するトラストポイントを指定するには、グローバル コンフィギュレーション モードで **crypto map set trustpoint** コマンドを使用します。クリプト マップ エントリからトラストポイ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。

crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

no crypto map *map-name seq-num* **set trustpoint** *trustpoint-name* [**chain**]

構文の説明

chain	(任意)証明書チェーンを送信します。CA 証明書チェーンには、ルート証明書からアイデンティティ証明書まで、証明書の階層内のすべての CA 証明書が含まれています。デフォルト値はディセーブル(チェーンなし)です。
map-name	クリプト マップ セットの名前を指定します。
seq-num	クリプト マップ エントリに割り当てる番号を指定します。
trustpoint-name	フェーズ 1 ネゴシエーション中に送信する証明書を指定します。デフォルトは none 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
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。
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

このクリプト マップ コマンドは、接続の開始に対してのみ有効です。応答側の情報については、**tunnel-group** コマンドを参照してください。

例

次に、グローバル コンフィギュレーション モードで、クリプト マップ mymap にトラストポイント tpoint 1 を指定し、証明書チェーンを含める例を示します。

```
ciscoasa(config)# crypto map mymap 10 set trustpoint tpoint1 chain
ciscoasa(config)#
```

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。
tunnel-group	トンネル グループを設定します。

crypto map set validate-icmp-errors

IPsec トンネルを介して受信した、プライベート ネットワークの内部ホスト宛ての着信 ICMP エラー メッセージを検証するかどうかを指定するには、グローバル コンフィギュレーション モードで **crypto map set validate-icmp-errors** コマンドを使用します。クリプト マップ エントリからトラストポイ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。

crypto map *name priority* **set validate-icmp-errors**

no crypto map *name priority* **set validate-icmp-errors**

構文の説明

name	クリプト マップ セットの名前を指定します。
priority	クリプト マップ エントリに割り当てるプライオリティを指定します。

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
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
9.0(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

このクリプト マップ コマンドは、着信 ICMP エラー メッセージの検証に対してのみ有効です。

csc

ASA がネットワーク トラフィックを CSC SSM に送信できるようにするには、クラス コンフィギュレーション モードで **csc** 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。

csc {**fail-open** | **fail-close**}

no csc

構文の説明

fail-close	CSC SSM が失敗した場合、ASA がトラフィックをブロックする必要があることを指定します。これは、クラス マップで選択されたトラフィックにのみ適用されます。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。
fail-open	CSC SSM が失敗した場合、ASA がトラフィックを許可する必要があることを指定します。これは、クラス マップで選択されたトラフィックにのみ適用されます。CSC SSM に送信されていない他のトラフィックは、CSC SSM 障害による影響を受けません。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	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 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
7.1(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

クラス コンフィギュレーション モードはポリシー マップ コンフィギュレーション モードからアクセスできます。

csc コマンドは、該当するクラス マップに一致したすべてのトラフィックを CSC SSM に送信するようにセキュリティ ポリシーを設定します。この設定の後、ASA は、トラフィックが宛先に引き続き送信されるのを許可します。

CSC SSM がトラフィックをスキャンできない場合は、一致しているトラフィックを ASA が処理する方法を指定できます。**fail-open** キーワードは、CSC SSM を使用できない場合でも、トラフィックが宛先に引き続き送信されるのを ASA が許可するように指定します。**fail-close** キーワードは、CSC SSM が使用できない場合、一致しているトラフィックが宛先に引き続き送信されるのを ASA が許可しないように指定します。

CSC SSM は、HTTP、SMTP、POP3、および FTP トラフィックをスキャンできます。接続を要求しているパケットの宛先ポートが、これらのプロトコルにとって既知のポートである場合にのみ、これらのプロトコルがサポートされます。つまり、CSC SSM は、次の接続のみをスキャンできます。

- TCP ポート 21 に対してオープンされている FTP 接続
- TCP ポート 80 に対してオープンされている HTTP 接続
- TCP ポート 110 に対してオープンされている POP3 接続
- TCP ポート 25 に対してオープンされている SMTP 接続

csc コマンドを使用しているポリシーで、これらのポートを他のプロトコルに誤用する接続が選択された場合、ASA はパケットを CSC SSM に渡しますが、CSC SSM はパケットをスキャンせずに渡します。

CSC SSM の効率を最大限にするには、次のように、**csc** コマンドを実装しているポリシーが使用するクラス マップを設定します。

- サポートされているプロトコルのうち、CSC SSM がスキャンするプロトコルだけを選択します。たとえば、HTTP トラフィックをスキャンしない場合は、サービス ポリシーが HTTP トラフィックを CSC SSM に転送しないようにしてください。
- ASA によって保護されている信頼できるホストを危険にさらす接続だけを選択します。これらは、外部ネットワークまたは信頼できないネットワークから内部ネットワークへの接続です。次の接続をスキャンすることを推奨します。
  - 発信 HTTP 接続
  - ASA の内部のクライアントから ASA の外部のサーバへの FTP 接続
  - ASA の内部のクライアントから ASA の外部サーバへの POP3 接続
  - 内部メール サーバ宛ての着信 SMTP 接続

FTP スキャン

CSC SSM は、FTP セッションのプライマリ チャネルが標準ポート（TCP ポート 21）を使用している場合にのみ、FTP ファイル転送のスキャンをサポートします。

FTP インスペクションは、CSC SSM がスキャンする FTP トラフィックに対してイネーブルである必要があります。これは、FTP が、データ転送用にダイナミックに割り当てられたセカンダリ チャネルを使用するためです。ASA は、セカンダリ チャネルに割り当てられるポートを決定し、データ転送の実行を許可するピンホールを開きます。FTP データをスキャンするように CSC SSM が設定されている場合、ASA はデータ トラフィックを CSC SSM に転送します。

FTP インスペクションは、グローバルに、または **csc** コマンドが適用される同じインターフェイスに適用できます。デフォルトでは、FTP インスペクションはグローバルにイネーブルになっています。デフォルトのインスペクション コンフィギュレーションを変更していない場合、CSC SSM による FTP スキャンをイネーブルにするために必要なその他の FTP インスペクション コンフィギュレーションはありません。

FTP インスペクションまたはデフォルトのインスペクション コンフィギュレーションの詳細については、CLI 設定ガイドを参照してください。

例

内部ネットワーク上のクライアントから HTTP、FTP、および POP3 接続で外部のネットワークに要求されたトラフィック、および外部のホストから DMZ ネットワーク上のメール サーバに着信する SMTP 接続を CSC SSM に転送するように、ASA を設定する必要があります。内部ネットワークから DMZ ネットワーク上の Web サーバへの HTTP 要求は、スキャンされません。

次のコンフィギュレーションでは、2 つのサービス ポリシーを作成します。最初のポリシー csc_out_policy は、内部インターフェイスに適用され、csc_out アクセス リストを使用して、FTP および POP3 に対するすべての発信要求が確実にスキャンされるようにします。csc_out アクセス リストにより、内部から外部インターフェイス上のネットワークへの HTTP 接続が確実にスキャンされるようにもなりますが、このアクセス リストには、内部から DMZ ネットワーク上のサーバへの HTTP 接続を除外する拒否 ACE が含まれています。

2 番めのポリシー csc_in_policy は、外部インターフェイスに適用されます。このポリシーは csc_in アクセス リストを使用して、外部インターフェイスで発信され、DMZ ネットワークを宛先とする SMTP 要求と HTTP 要求が CSC SSM で確実にスキャンされるようにします。HTTP 要求をスキャンすることで、Web サーバは HTTP ファイルのアップロードから保護されます。

```
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 21
ciscoasa(config)# access-list csc_out deny tcp 192.168.10.0 255.255.255.0 192.168.20.0 255.255.255.0 eq 80
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 80
ciscoasa(config)# access-list csc_out permit tcp 192.168.10.0 255.255.255.0 any eq 110

ciscoasa(config)# class-map csc_outbound_class
ciscoasa(config-cmap)# match access-list csc_out

ciscoasa(config)# policy-map csc_out_policy
ciscoasa(config-pmap)# class csc_outbound_class
ciscoasa(config-pmap-c)# csc fail-close

ciscoasa(config)# service-policy csc_out_policy interface inside

ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 25
ciscoasa(config)# access-list csc_in permit tcp any 192.168.20.0 255.255.255.0 eq 80

ciscoasa(config)# class-map csc_inbound_class
ciscoasa(config-cmap)# match access-list csc_in

ciscoasa(config)# policy-map csc_in_policy
ciscoasa(config-pmap)# class csc_inbound_class
ciscoasa(config-pmap-c)# csc fail-close

ciscoasa(config)# service-policy csc_in_policy interface outside
```

（注） FTP で転送されるファイルをスキャンするには、CSC SSM に対して FTP 検査がイネーブルになっている必要があります。FTP インスペクションは、デフォルトでイネーブルになっています。

関連コマンド

コマンド	説明
class（ポリシー マップ）	トラフィック分類のクラス マップを指定します。
class-map	ポリシー マップで使用するトラフィック分類マップを作成します。
match port	宛先ポートを使用してトラフィックを照合します。
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。
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。

csd enable（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 9.5(1) でした。

クライアントレス SSL VPN リモート アクセスまたは AnyConnect クライアントを使用したリモート アクセスに対して Cisco Secure Desktop（CSD）をイネーブルにするには、webvpn コンフィギュレーション モードで **csd enable** コマンドを使用します。CSD 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。

csd enable

no csd enable

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
webvpn コンフィギュレーション モード	• 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)	このコマンドは廃止され、**hostscan** コマンドに置き換えられました。

使用上のガイドライン

CSD は、1 つの例外を除いて、ASA へのすべてのリモート アクセス接続試行に対してグローバルにイネーブルまたはディセーブルに設定されます。

csd enable コマンドは、次の処理を実行します。

1. 以前の **csd image** *path* コマンドによって実行されたチェックを補足する有効性チェックを提供します。
2. sdesktop フォルダがまだ存在しない場合は、disk0: 上に作成します。
3. data.xml（Cisco Secure Desktop コンフィギュレーション）ファイルが sdesktop フォルダにまだ存在しない場合は、追加します。

4. フラッシュ デバイスの data.xml を実行コンフィギュレーションにロードします。
5. CSD をイネーブルにします。

（注）
- **show webvpn csd** コマンドを入力して、Cisco Secure Desktop がイネーブルであるかどうかを確認できます。
- **csd enable** コマンドを入力する前に、実行コンフィギュレーション内に **csd image** *path* コマンドが存在する必要があります。
- **no csd enable** コマンドは、実行コンフィギュレーションで CSD をディセーブルにします。CSD がディセーブルの場合、管理者は CSD Manager にアクセスできず、リモート ユーザは CSD を使用できません。
- data.xml ファイルを転送または交換する場合は、このファイルを実行コンフィギュレーションにロードするために、CSD をいったんディセーブルにしてからイネーブルにします。
- CSD は、ASA へのすべてのリモート アクセス接続試行に対してグローバルにイネーブルまたはディセーブルに設定されます。個別の接続プロファイルやグループ ポリシーに対して CSD をイネーブルまたはディセーブルに設定することはできません。

  例外：クライアントレス SSL VPN 接続の接続プロファイルは、コンピュータがグループ URL を使用して ASA への接続を試み、CSD がグローバルにイネーブルの場合、CSD がクライアント コンピュータで実行されないように設定できます。次に例を示します。

```
ciscoasa(config)# tunnel-group group-name webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://www.url-string.com
ciscoasa(config-tunnel-webvpn)# without-csd
```

例

次に、CSD イメージのステータスを表示し、CSD イメージをイネーブルにするためのコマンドを示します。

```
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop is not enabled.
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
csd image	コマンドに指定された CSD イメージを、パスに指定されたフラッシュ ドライブから実行コンフィギュレーションにコピーします。
show webvpn csd	イネーブルの場合、CSD のバージョンを識別します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
without-csd	クライアントレス SSL VPN セッションの接続プロファイルを、コンピュータがグループ URL を使用して ASA への接続を試み、CSD がグローバルにイネーブルの場合、CSD がクライアント コンピュータで実行されないように設定します。

csd hostscan image（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 9.5(1) でした。

シスコのホスト スキャン配布パッケージをインストールまたはアップグレードし、実行コンフィギュレーションに追加するには、webvpn コンフィギュレーション モードで **csd hostscan image** コマンドを使用します。ホスト スキャン配布パッケージを実行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。

csd hostscan image *path*

no csd hostscan image *path*

構文の説明

path	シスコのホスト スキャン パッケージのパスおよびファイル名を 255 文字以内で指定します。 ホスト スキャン パッケージには、ファイル名の命名規則 hostscan-*version*.pkg を持つスタンドアロンのホスト スキャン パッケージを指定するか、または、Cisco.com からダウンロードでき、ファイル名の命名規則 anyconnect-win-*version*-k9.pkg を持つ完全な AnyConnect セキュア モビリティ クライアント パッケージを指定できます。顧客が AnyConnect セキュア モビリティ クライアントを指定すると、ASA は AnyConnect パッケージからホスト スキャン パッケージを取得してインストールします。 ホスト スキャン パッケージには、ホスト スキャン ソフトウェアおよびホスト スキャン ライブラリとサポート チャートが含まれています。 このコマンドは、CSD イメージをアップロードできません。この操作を行うには、**csd image** コマンドを使用します。

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
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
8.4(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。このコマンドは **hostscan image** に置き換えられました。

使用上のガイドライン

現在インストールされ、イネーブルになっているホスト スキャン イメージのバージョンを確認するには、**show webvpn csd hostscan** コマンドを入力します。

csd hostscan image コマンドを使用してホスト スキャンをインストールしたら、**csd enable** コマンドを使用してイメージをイネーブルにします。

次回の ASA のリブート時にホスト スキャン イメージを確実に使用できるように、**write memory** コマンドを入力して実行コンフィギュレーションを保存します。

例

次に、シスコのホスト スキャン パッケージをインストールし、イネーブルにして、表示およびフラッシュ ドライブへの設定の保存を行うコマンドを示します。

```
ciscoasa> en
Password: ******
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan is not enabled.
ciscoasa(config-webvpn)# csd hostscan image disk0:/hostscan_3.0.0333-k9.pkg
ciscoasa(config-webvpn)# csd enable
ciscoasa(config-webvpn)# show webvpn csd hostscan
Hostscan version 3.0.0333 is currently installed and enabled
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 2e7126f7 71214c6b 6f3b28c5 72fa0a1e

22067 bytes copied in 3.460 secs (7355 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn csd hostscan	シスコのホスト スキャンがイネーブルである場合、そのバージョンを示します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。

csd image（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 9.5(1) でした。

Cisco Secure Desktop（CSD）配布パッケージを検証して、実行コンフィギュレーションに追加するには、CSD を効率的にインストールし、webvpn コンフィギュレーション モードで **csd image** コマンドを使用します。CSD 配布パッケージを実行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。

csd image *path*

no csd image *path*

構文の説明

path	CSD パッケージのパスおよびファイル名を 255 文字以内で指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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)	このコマンドは廃止され、**hostscan image** コマンドに置き換えられました。

使用上のガイドライン

このコマンドを入力する前に、**show webvpn csd** コマンドを入力して、CSD イメージがイネーブルであるかどうかを判断します。CLI は、現在インストールされている CSD イメージがイネーブルである場合、そのバージョンを示します。

新しい Cisco Secure Desktop イメージをコンピュータにダウンロードし、フラッシュ ドライブに転送してから、**csd image** コマンドを使用して、イメージをインストールするか、または既存のイメージをアップグレードします。ダウンロードする場合、使用している ASA に合ったファイルを必ず取得してください。ファイルの形式は、securedesktop_asa_<n>_<n>*.pkg です。

no csd image コマンドを入力すると、CSD Manager への管理アクセスと CSD へのリモート ユーザ アクセスの両方が削除されます。このコマンドを入力しても、ASA は CSD ソフトウェアおよびフラッシュ ドライブの CSD コンフィギュレーションに変更を加えません。

(注) 次回の ASA のリブート時に CSD を確実に使用できるようにするために、**write memory** コマンドを入力して実行コンフィギュレーションを保存します。

例 次に、現在の CSD 配布パッケージを表示し、フラッシュ ファイル システムの内容を表示して、新しいバージョンにアップグレードするためのコマンドを示します。

```
ciscoasa# show webvpn csd
Secure Desktop version 3.1.0.24 is currently installed and enabled.
ciscoasa# config t
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# show disk all
-#- --length-- -----date/time------ path
  6 8543616    Nov 02 2005 08:25:36 PDM
  9 6414336    Nov 02 2005 08:49:50 cdisk.bin
 10 4634       Sep 17 2004 15:32:48 first-backup
 11 4096       Sep 21 2004 10:55:02 fsck-2451
 12 4096       Sep 21 2004 10:55:02 fsck-2505
 13 21601      Nov 23 2004 15:51:46 shirley.cfg
 14 9367       Nov 01 2004 17:15:34 still.jpg
 15 6594064    Nov 04 2005 09:48:14 asdmfile.510106.rls
 16 21601      Dec 17 2004 14:20:40 tftp
 17 21601      Dec 17 2004 14:23:02 bingo.cfg
 18 9625       May 03 2005 11:06:14 wally.cfg
 19 16984      Oct 19 2005 03:48:46 tomm_backup.cfg
 20 319662     Jul 29 2005 09:51:28 sslclient-win-1.0.2.127.pkg
 21 0          Oct 07 2005 17:33:48 sdesktop
 22 5352       Oct 28 2005 15:09:20 sdesktop/data.xml
 23 369182     Oct 10 2005 05:27:58 sslclient-win-1.1.0.133.pkg
 24 1836210    Oct 12 2005 09:32:10 securedesktop_asa_3_1_0_24.pkg
 25 1836392    Oct 26 2005 09:15:26 securedesktop_asa_3_1_0_25.pkg

38600704 bytes available (24281088 bytes used)

******** Flash Card Geometry/Format Info ********

COMPACT FLASH CARD GEOMETRY
   Number of Heads:            4
   Number of Cylinders       978
   Sectors per Cylinder       32
   Sector Size               512
   Total Sectors          125184

COMPACT FLASH CARD FORMAT
   Number of FAT Sectors      61
   Sectors Per Cluster         8
   Number of Clusters      15352
   Number of Data Sectors 122976
   Base Root Sector          123
   Base FAT Sector             1
   Base Data Sector          155
ciscoasa(config-webvpn)# csd image disk0:securedesktop_asa_3_1_0_25.pkg
ciscoasa(config-webvpn)# show webvpn csd
Secure Desktop version 3.1.0.25 is currently installed and enabled.
ciscoasa(config-webvpn)# write memory
Building configuration...
Cryptochecksum: 5e57cfa8 0e9ca4d5 764c3825 2fc4deb6

19566 bytes copied in 3.640 secs (6522 bytes/sec)
[OK]
ciscoasa(config-webvpn)#
```

関連コマンド

コマンド	説明
show webvpn csd	イネーブルの場合、CSD のバージョンを識別します。ディセーブルの場合、CLI に「Secure Desktop is not enabled.」と表示されます。
csd enable	管理およびリモート ユーザ アクセスの CSD をイネーブルにします。

ctl

証明書信頼リスト(CTL)プロバイダーをイネーブルにして、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 **ctl** 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。

ctl install

no ctl install

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
Ctl プロバイダー 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
8.0(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 プロバイダーをイネーブルにして、CTL クライアントの CTL ファイルを解析し、CTL ファイルのエントリに対するトラストポイントをインストールするには、ctl プロバイダー コンフィギュレーション モードで **ctl** コマンドを使用します。このコマンドでインストールされたトラストポイントには、「_internal_CTL_<ctl_name>」というプレフィックスが付いた名前が設定されます。

このコマンドがディセーブルの場合は、**crypto ca trustpoint** コマンドと **crypto ca certificate chain** コマンドを使用して、各 CallManager サーバと CAPF 証明書を手動でインポートおよびインストールする必要があります。

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-provider	CTL プロバイダー インスタンスを定義し、プロバイダー コンフィギュレーション モードを開始します。
server trust-point	TLS ハンドシェイク中に提示するプロキシ トラストポイント証明書を指定します。
show tls-proxy	TLS プロキシを表示します。
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。

ctl-file（廃止）

電話プロキシ用に作成するための CTL インスタンス、またはフラッシュ メモリに格納されている CTL ファイルを解析するための CTL インスタンスを指定するには、グローバル コンフィギュレーション モードで **ctl-file** コマンドを使用します。電話プロキシの設定時に使用する CTL インスタンスを指定するには、電話プロキシ コンフィギュレーション モードで **ctl-file** コマンドを使用します。CTL インスタンスを削除するには、このコマンドの **no** 形式を使用します。

ctl-file *ctl_name*

no ctl-file *ctl_name* [**noconfirm**]

構文の説明

ctl_name	CTL インスタンスの名前を指定します。
noconfirm	（任意、グローバル モードのみ）**no** コマンドとともに使用して、CTL ファイルの削除時に、トラストポイントの削除に関する警告が ASA コンソールに表示されないようにします。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(4)	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

LSC プロビジョニングが必要な電話をユーザが所有している場合は、**ctl-file** コマンドを使用して CTL ファイル インスタンスを設定するときに、CAPF 証明書を CUMC から ASA にインポートする必要もあります。

(注) CTL ファイルを作成するには、ctl ファイル コンフィギュレーション モードで **no shutdown** コマンドを使用します。CTL ファイルのエントリを変更したり CTL ファイルにエントリを追加したりするには、または CTL ファイルを削除するには、**shutdown** コマンドを使用します。

このコマンドの **no** 形式を使用すると、CTL ファイル、および電話プロキシによって内部的に作成されたすべての登録済みトラストポイントが削除されます。また、CTL ファイルを削除すると、関連する認証局から受信したすべての証明書が削除されます。

例

次に、電話プロキシ機能用の CTL ファイルを設定する例を示します。

```
ciscoasa(config)# ctl-file myctl
```

次に、**ctl-file** コマンドを使用して、電話プロキシ モードで電話プロキシ機能用の CTL ファイルを設定する例を示します。

```
ciscoasa(config-phone-proxy)# ctl-file myctl
```

関連コマンド

コマンド	説明
ctl-file（Phone-Proxy）	電話プロキシ インスタンスの設定時に使用する CTL ファイルを指定します。
cluster-ctl-file	フラッシュ メモリに格納されている CTL ファイルからトラストポイントをインストールするために、CTL ファイルを解析します。
phone-proxy	電話プロキシ インスタンスを設定します。
record-entry	CTL ファイルの作成に使用するトラストポイントを指定します。
sast	CTL レコードに作成する SAST 証明書の数を指定します。

ctl-provider

CTL プロバイダー モードで CTL プロバイダー インスタンスを設定するには、グローバル コンフィギュレーション モードで **ctl-provider** 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。

ctl-provider *ctl_name*

no ctl-provider *ctl_name*

構文の説明

ctl_name	CTL プロバイダー インスタンスの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
8.0(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 モードを開始して CTL プロバイダー インスタンスを作成するには、**ctl-provider** コマンドを使用します。

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

cts import-pac

Cisco ISE から Protected Access Credential（PAC）ファイルをインポートするには、グローバル コンフィギュレーション モードで **cts import-pac** コマンドを使用します。

cts import-pac *filepath* **password** *value*

構文の説明

filepath	次のいずれかの **exec** モード コマンドおよびオプションを指定します。 シングル モード • **disk0**：disk0 のパスおよびファイル名 • **disk1**：disk1 のパスおよびファイル名 • **flash**：フラッシュのパスおよびファイル名 • **ftp**：FTP のパスおよびファイル名 • **http**：HTTP のパスおよびファイル名 • **https**：HTTPS のパスおよびファイル名 • **smb**：SMB のパスおよびファイル名 • **tftp**：TFTP のパスおよびファイル名 マルチ モード • **http**：HTTP のパスおよびファイル名 • **https**：HTTPS のパスおよびファイル名 • **smb**：SMB のパスおよびファイル名 • **tftp**：TFTP のパスおよびファイル名
password *value*	PAC ファイルの暗号化に使用されるパスワードを指定します。このパスワードは、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。 パスワードは、PAC ファイルが要求されたときに入力されたパスワードと一致する必要があり、PAC データを復号化するために必要です。このパスワードは、デバイス クレデンシャルの一部として ISE で設定したパスワードとは関係ありません。

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
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
9.0(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

PAC ファイルを ASA にインポートすると、ISE との接続が確立されます。チャネルが確立されると、ASA は、ISE を使用してセキュア RADIUS トランザクションを開始し、Cisco TrustSec 環境データをダウンロードします。具体的には、ASA は、セキュリティ グループ テーブルをダウンロードします。セキュリティ グループ テーブルによって、SGT がセキュリティ グループ名にマッピングされます。セキュリティ グループの名前は ISE 上で作成され、セキュリティ グループをわかりやすい名前で識別できるようになります。チャネルは RADIUS トランザクションの前には確立されません。ASA は、認証用の PAC を使用して ISE の RADIUS トランザクションを開始します。

ヒント PAC ファイルには、ASA および ISE がその間で発生する RADIUS トランザクションを保護できる共有キーが含まれています。このキーは、その機密性により、ASA に安全に保存する必要があります。

ファイルの正常なインポート後に、ASA は、ISE で設定されたデバイスのパスワードを要求せずに、ISE から Cisco TrustSec 環境データをダウンロードします。

ASA は、ユーザ インターフェイスからアクセスできない NVRAM の領域に PAC ファイルを保存します。

前提条件

- ASA が PAC ファイルを生成するには、ISE の認識された Cisco TrustSec ネットワーク デバイスとして ASA を設定する必要があります。ASA は、任意の PAC ファイルをインポートできますが、PAC ファイルは、正しく設定された ISE によって生成された場合にのみ ASA で動作します。
- ISE での PAC ファイルの生成時に PAC ファイルを暗号化するために使用されたパスワードを取得します。

  ASA は、PAC ファイルをインポートし、復号化する場合にこのパスワードが必要となります。
- ISE で生成された PAC ファイルにアクセスします。ASA は、フラッシュ、または TFTP、FTP、HTTP、HTTPS、SMB を介してリモート サーバから PAC ファイルをインポートできます（PAC ファイルは、インポート前に ASA フラッシュに配置されている必要はありません）。
- ASA のサーバ グループを設定します。

[Restrictions（機能制限）]

- ASA が HA 設定の一部である場合、プライマリ ASA デバイスに PAC ファイルをインポートする必要があります。
- ASA がクラスタリング設定の一部である場合、マスター デバイスに PAC ファイルをインポートする必要があります。

例

次に、ISE から PAC をインポートする例を示します。

```
ciscoasa(config)# cts import pac disk0:/pac123.pac password hideme
PAC file successfully imported
```

関連コマンド

コマンド	説明
cts refresh environment-data	ASA が Cisco TrustSec と統合されると、ISE からの Cisco TrustSec 環境データをリフレッシュします
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts manual

SGT およびイーサネット タギング（レイヤ 2 SGT インポジションとも呼ばれる）をイネーブルにし、cts manual インターフェイス コンフィギュレーション モードを開始するには、インターフェイス コンフィギュレーション モードで **cts manual** コマンドを使用します。SGT およびイーサネット タギ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。

cts manual

no cts manual

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
9.3(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、レイヤ 2 SGT インポジションをイネーブルにし、cts manual インターフェイス コンフィギュレーション モードを開始します。

[Restrictions（機能制限）]

- 物理インターフェイス、VLAN インターフェイス、ポート チャネル インターフェイスおよび冗長インターフェイスでのみサポートされます。
- BVI、TVI、VNI などの論理インターフェイスや仮想インターフェイスではサポートされません。
- フェールオーバー リンクはサポートしません。
- クラスタ制御リンクはサポートしません。

例

次に、レイヤ 2 SGT インポジションをイネーブルにし、cts manual インターフェイス コンフィギュレーション モードを開始する例を示します。

```
ciscoasa(config-if)# cts manual
ciscoasa(config-if-cts-manual)#
```

関連コマンド

コマンド	説明
policy static sgt	手動で設定された CTS リンクにポリシーを適用します。
propagate sgt	インターフェイスでのセキュリティ グループ タグ（**sgt** と呼ばれる）の伝播をイネーブルにします。

cts refresh environment-data

ISE からの Cisco TrustSec 環境データをリフレッシュし、調整タイマーを設定されたデフォルト値にリセットするには、グローバル コンフィギュレーション モードで **cts refresh environment-data** コマンドを使用します。

cts refresh environment-data

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
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
9.0(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

ASA が Cisco TrustSec と統合されると、ASA は ISE から環境データをダウンロードします。このデータには、セキュリティ グループ タグ(SGT)名テーブルが含まれます。ASA で次のタスクを完了すると、ASA は、ISE から取得した環境データを自動的にリフレッシュします。

- ISE と通信するように AAA サーバを設定します。
- ISE から PAC ファイルをインポートします。
- Cisco TrustSec 環境データを取得するために ASA で使用する AAA サーバ グループを識別します。

通常、ISE からの環境データを手動でリフレッシュする必要はありません。ただし、セキュリティ グループが ISE で変更されることがあります。これらの変更は、ASA セキュリティ グループ テーブルのデータをリフレッシュするまで ASA には反映されません。ASA でデータをリフレッシュして、ISE 上で作成されたセキュリティ グループが ASA に反映されるようにします。

ヒント　メンテナンス時間中に ISE のポリシー設定および ASA での手動データ リフレッシュをスケジュールすることを推奨します。このようにポリシー設定の変更を処理すると、セキュリティ グループ名が解決される可能性が最大化され、セキュリティ ポリシーが ASA で即時にアクティブ化されます。

前提条件

Cisco TrustSec の変更が ASA に適用されるように、ASA は、ISE の認識された Cisco TrustSec ネットワーク デバイスとして設定される必要があり、ASA は PAC ファイルを正常にインポートする必要があります。

[Restrictions（機能制限）]

- ASA が HA 設定の一部である場合、プライマリ ASA デバイスで環境データをリフレッシュする必要があります。
- ASA がクラスタリング設定の一部である場合、マスター デバイスで環境データをリフレッシュする必要があります。

例

次に、ISE から Cisco TrustSec 環境データをダウンロードする例を示します。

```
ciscoasa(config)# cts refresh environment-data
```

関連コマンド

コマンド	説明
cts import-pac	ASA が Cisco TrustSec と統合されると、Cisco ISE から Protected Access Credential（PAC）ファイルをインポートします。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts role-based sgt-map

IP-SGT バインディングを手動で設定するには、グローバル コンフィギュレーション モードで **cts role-based sgt-map** 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。

cts role-based sgt-map {*IPv4_addr*[*/mask*] | *IPv6_addr*[*/prefix*]} **sgt** *sgt_value*

no cts role-based sgt-map {*IPv4_addr*[*/mask*] | *IPv6_addr*[*/prefix*]} **sgt** *sgt_value*

構文の説明

IPv4_addr[*/mask*]	使用する IPv4 アドレスを指定します。サブネットのマッピングを作成するために CIDR 形式のサブネット マスクを追加します（10.100.10.0/24 など）。
IPv6_addr[*/prefix*]	使用する IPv6 アドレスを指定します。IPv6 ネットワークのマッピングを作成するためにプレフィックスを追加します。
sgt *sgt_value*	IP アドレスをマッピングする SGT 番号を指定します。有効な値の範囲は 2 ～ 65519 です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.3(1)	このコマンドが追加されました。
9.6(1)	サブネットのマッピングを追加する機能が追加されました。

使用上のガイドライン

このコマンドを使用すると、IP-SGT バインディングを手動で設定することができます。

例

次に、IP-SGT バインディング テーブル エントリを設定する例を示します。

```
ciscoasa(config)# cts role-based sgt-map 10.2.1.2 sgt 50
```

関連コマンド

コマンド	説明
clear configure cts role-based [**sgt-map**]	ユーザ定義の IP-SGT バインディング テーブル エントリを削除します。
show running-config [**all**] **cts role-based [sgt-map]**	ユーザ定義の IP-SGT バインディング テーブル エントリを表示します。

cts server-group

環境データを取得する Cisco TrustSec と統合するために ASA で使用する AAA サーバ グループを識別するには、グローバル コンフィギュレーション モードで **cts server-group** コマンドを使用します。コマンドのサポート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。

cts server-group *aaa-server-group-name*

no cts server-group [*aaa-server-group-name*]

構文の説明

aaa-server-group-name	既存のローカルで設定された AAA サーバ グループの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(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

Cisco TrustSec と統合するための ASA の設定の一環として、ISE と通信できるように ASA を設定する必要があります。ASA では、サーバ グループの 1 つのインスタンスだけを Cisco TrustSec 用に設定できます。

前提条件

- 参照先のサーバ グループは、RADIUS プロトコルを使用するように設定する必要があります。ASA に非 RADIUS サーバ グループを追加すると、機能の設定は失敗します。
- ISE もユーザ認証に使用する場合は、ISE に ASA を登録したときに ISE で入力した共有秘密を取得します。この情報が不明な場合は、ISE 管理者にお問い合わせください。

例

次に、ISE 用の AAA サーバ グループを ASA でローカルに設定し、ASA と Cisco TrustSec を統合するためにその AAA サーバ グループを使用するように ASA を設定する例を示します。

```
ciscoasa(config)# aaa-server ISEserver protocol radius
ciscoasa(config-aaa-server-group)# exit
ciscoasa(config)# aaa-server ISEserver (inside) host 192.0.2.1
ciscoasa(config-aaa-server-host)# key myexclusivemumblekey
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)# cts server-group ISEserver
```

関連コマンド

コマンド	説明
aaa-server *server-tag* **protocol radius**	AAA サーバ グループを作成し、ASA の AAA サーバ パラメータを ISE サーバと通信するように設定します。*server-tag* では、サーバ グループの名前を指定します。
aaa-server *server-tag* (*interface-name*) **host** *server-ip*	AAA サーバを AAA サーバ グループの一部として設定し、ホスト固有の接続データを設定します。(*interface-name*) では、ISE サーバが配置されているネットワーク インターフェイスを指定し、*server-tag* は Cisco TrustSec 統合の AAA サーバ グループの名前です。*server-ip* では、ISE サーバの IP アドレスを指定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp connection peer

SXP ピアへの SXP 接続を設定するには、グローバル コンフィギュレーション モードで **cts sxp connection peer** コマンドを使用します。コマンドのサポート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。

cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] **password** {**default** | **mode**} [**mode** {**local** | **peer**}] {**speaker** | **listener**}

no cts sxp connection peer *peer_ip_address* [**source** *source_ip_address*] [**password** {**default** | **none**}] [**mode** {**local** | **peer**}] [**speaker** | **listener**]

構文の説明

default	**password** キーワードとともに使用されます。SXP 接続に設定されたデフォルト パスワードを使用することを指定します。
listener	ASA が SXP 接続でリスナーとして機能することを指定します。これは、ASA がダウンストリーム デバイスから IP-SGT マッピングを受信できることを意味します。SPX 接続について、ASA にスピーカーまたはリスナーの役割が必要であることを指定します。
ローカル	**mode** キーワードとともに使用されます。ローカル SXP デバイスを使用することを指定します。
mode	（オプション）SXP 接続のモードを指定します。
none	**password** キーワードとともに使用されます。SXP 接続にパスワードを使用しないことを指定します。
password	（オプション）SXP 接続に認証キーを使用するかどうかを指定します。
peer	**mode** キーワードとともに使用されます。ピア SXP デバイスを使用することを指定します。
peer_ip_address	SXP ピアの IPv4 アドレスまたは IPv6 アドレスを指定します。ピア IP アドレスは、ASA 発信インターフェイスからアクセスできる必要があります。
source *source_ip_address*	（オプション）SXP 接続のローカル IPv4 または IPv6 アドレスを指定します。
speaker	ASA が SXP 接続でスピーカーとして機能することを指定します。これは、ASA がアップストリーム デバイスに IP-SGT マッピングを転送できることを意味します。SPX 接続について、ASA にスピーカーまたはリスナーの役割が必要であることを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(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

ピア間の SXP 接続はポイントツーポイントであり、基礎となるトランスポート プロトコルとして TCP を使用します。SXP 接続は IP アドレスごとに設定されます。単一デバイスのペアは複数の SXP 接続に対応できます。

[Restrictions（機能制限）]

- ASA は SXP 接続用の接続ごとのパスワードをサポートしません。
- **cts sxp default password** を使用してデフォルトの SXP パスワードを設定する場合、デフォルトのパスワードを使用するように SXP 接続を設定する必要があります。逆に、デフォルトのパスワードを設定しない場合は、SXP 接続用のデフォルトのパスワードを設定しないでください。この 2 つのガイドラインに従っていない場合、SXP 接続は失敗する可能性があります。
- デフォルトのパスワードを使用する SXP 接続を設定しましたが、ASA にデフォルトのパスワードが設定されていない場合、SXP 接続は失敗します。
- SXP 接続の送信元 IP アドレスを設定する場合は、ASA 発信インターフェイスと同じアドレスを指定する必要があります。送信元 IP アドレスが発信インターフェイスのアドレスと一致しない場合、SXP 接続は失敗します。

  SXP 接続の送信元 IP アドレスが設定されていない場合、ASA は、route/ARP 検索を実行して、SXP 接続用の発信インターフェイスを判別します。SXP 接続の送信元 IP アドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。
- SXP ピアまたは送信元に対する IPv6 ローカル リンク アドレスの設定はサポートされていません。
- SXP 接続の同一インターフェイスに複数の IPv6 アドレスを設定することはサポートされていません。

例

次に、ASA で SXP 接続を作成する例を示します。

```
ciscoasa(config)# cts sxp connection peer 192.168.1.100
source 192.168.1.1 password default mode peer speaker
```

関連コマンド

コマンド	説明
cts sxp default password	SXP 接続のデフォルト パスワードを指定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp default password

SXP ピアでの TCP MD5 認証のデフォルト 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 **cts sxp default password** コマンドを使用します。コマンドのサポート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。

cts sxp default password [**0** | **8**] *password*

no cts sxp default password [**0** | **8**] [*password*]

構文の説明

0	(オプション)デフォルトのパスワードで暗号化レベルに暗号化されていないクリアテキストを使用することを指定します。デフォルトのパスワードに設定できる暗号化レベルは 1 つだけです。
8	(オプション)デフォルトのパスワードで暗号化レベルに暗号化テキストを使用することを指定します。
password	162 文字までの暗号化された文字列または 80 文字までの ASCII キー文字列を指定します。

デフォルト

デフォルトでは、SXP 接続にパスワードは設定されていません。

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
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
9.0(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

デフォルトのパスワードを使用する SXP 接続を設定しましたが、ASA にデフォルトのパスワードが設定されていない場合、SXP 接続は失敗します。

[Restrictions(機能制限)]

- ASA は SXP 接続用の接続ごとのパスワードをサポートしません。
- **cts sxp default password** を使用してデフォルトの SXP パスワードを設定する場合、デフォルトのパスワードを使用するように SXP 接続を設定する必要があります。逆に、デフォルトのパスワードを設定しない場合は、SXP 接続用のデフォルトのパスワードを設定しないでください。この 2 つのガイドラインに従っていない場合、SXP 接続は失敗する可能性があります。

例

次に、SXP 接続のデフォルトのパスワードを含む、すべての SXP 接続のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。このコマンドで **password default** キーワードを指定すると、SXP 接続のデフォルトのパスワードを使用できるようになります。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp default source-ip

SXP 接続のデフォルトのローカル IP アドレスを設定するには、グローバル コンフィギュレーション モードで **cts sxp default source-ip** コマンドを使用します。コマンドのサポート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。

cts sxp default source-ip *ipaddress*

no cts sxp default source-ip [*ipaddress*]

構文の説明

ipaddress	送信元 IP アドレスの IPv4 または IPv6 アドレスを指定します。

デフォルト

デフォルトでは、デフォルトの送信元 IP アドレスは設定されていません。

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
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
9.0(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

SXP 接続のデフォルトの送信元 IP アドレスを設定する場合は、ASA 発信インターフェイスと同じアドレスを指定する必要があります。送信元 IP アドレスが発信インターフェイスのアドレスと一致しない場合、SXP 接続は失敗します。

SXP 接続の送信元 IP アドレスが設定されていない場合、ASA は、route/ARP 検索を実行して、SXP 接続用の発信インターフェイスを判別します。SXP 接続のデフォルトの送信元 IP アドレスを設定せずに、ASA が route/ARP 検索を実行して SXP 接続の送信元 IP アドレスを決定できるようにすることを推奨します。

例

次に、SXP 接続のデフォルトの送信元 IP アドレスを含む、すべての SXP 接続のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA の SXP 接続を設定します。このコマンドで **source** *source_ip_address* キーワードおよび引数を指定すると、SXP 接続のデフォルトの送信元 IP アドレスを使用できるようになります。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp delete-hold-down period

SXP ピアが SXP 接続を終了した後にピアから学習した IP-SGT マッピングに削除ホールド ダウン タイマーを設定するには、グローバル コンフィギュレーション モードで **cts sxp delete-hold-down period** コマンドを使用します。タイマーをデフォルト値にリセットするには、このコマンドの **no** 形式を使用します。

cts sxp delete-hold-down period *timervalue*

no cts sxp delete-hold-down period

構文の説明

timervalue	SXP 接続の切断から学習した IP-SGT マッピングが削除されるまで保持する秒数を 120 ～ 64000 の範囲で指定します。

デフォルト

デフォルトでは、*timervalue* は 120 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.8(3)	このコマンドが追加されました。

使用上のガイドライン

各 SXP 接続が削除ホールド ダウン タイマーに関連付けられます。このタイマーは、リスナー側の SXP 接続が切断されたときにトリガーされます。この SXP 接続から学習した IP-SGT マッピングはすぐには削除されません。その代わりに、削除ホールド ダウン タイマーの有効期限が切れるまで保持されます。このタイマーの有効期限が切れると、マッピングが削除されます。

例

次に、削除ホールド ダウン期間を設定する例を示します。

```
ciscoasa(config)# cts sxp delete-hold-down period 240
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp enable

ASA 上の SXP プロトコ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 **cts sxp enable** コマンドを使用します。コマンドのサポート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。

cts sxp enable

no cts sxp enable

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトでは、ASA 上の SXP プロトコルはディセーブルです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
9.0(1)	このコマンドが追加されました。

例

次に、ASA 上の SXP プロトコルをイネーブルにする例を示します。

```
ciscoasa(config)# cts sxp enable
```

関連コマンド

コマンド	説明
clear cts	Cisco TrustSec と統合されたときに ASA で使用されるデータをクリアします。
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。

cts sxp mapping network-map

SXPv2 以前を使用しているピアのスピーカーとして機能している場合、IPv4 サブネット拡張の深さを設定するには、グローバル コンフィギュレーション モードで **cts sxp mapping network-map** 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。

cts sxp mapping network-map *maximum_hosts*

no cts sxp mapping network-map *maximum_hosts*

構文の説明

maximum_hosts	ネットワーク バインドから拡張できるホスト バインドの最大数（0 ～ 65535）です。デフォルトは 0 です。

デフォルト

デフォルトでは拡張は行われません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.6(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

リスナー ピアが SXPv2 以下を使用している場合、ピアは SGT とサブネットのバインドを理解できません。ASA は、個々のホスト バインディングに IPv4 サブネット バインディングを拡張できます（IPv6 バインディングは拡張されません）。このコマンドでは、サブネット バインディングから生成できるホスト バインディングの最大数が指定されます。すべてのリスナー ピアが SXPv3 以降を使用しているか、ASA がリスナーである場合、このコマンドの効果はありません。

例

次に、サブネット マッピングを 1000 ホスト バインドまで拡張できるようにする例を示します。

```
ciscoasa(config)# cts sxp mapping network-map 1000
```

関連コマンド

コマンド	説明
cts sxp connection peer	Trustsec ピアを設定します。

cts sxp reconciliation period

SXP ピアが SXP 接続を終了した後にホールド ダウン タイマーを開始するには、グローバル コンフィギュレーション モードで **cts sxp reconciliation period** コマンドを使用します。コマンドのサポート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。

cts sxp reconciliation period *timervalue*

no cts sxp reconciliation period [*timervalue*]

構文の説明

timervalue	調整タイマーのデフォルト値を指定します。1 ～ 64000 秒の範囲で秒数を入力します。

デフォルト

デフォルトでは、*timervalue* は 120 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

SXP ピアが SXP 接続を終了すると、ASA はホールド ダウン タイマーを開始します。ホールド ダウン タイマーの実行中に SXP ピアが接続されると、ASA は調整タイマーを開始します。次に、ASA は、SXP マッピング データベースを更新して、最新のマッピングを学習します。

調整タイマーの期限が切れると、ASA は、SXP マッピング データベースをスキャンして、古いマッピング エントリ（前回の接続セッションで学習されたエントリ）を識別します。ASA は、これらの接続を廃止としてマークします。調整タイマーが期限切れになると、ASA は、SXP マッピング データベースから廃止エントリを削除します。

0 を指定すると調整タイマーが開始されないため、このタイマーには 0 を指定できません。調整タイマーを実行できないようにすると、失効する時間の定義がない状態で古いエントリが維持され、ポリシーの適用に対する予期しない結果が発生します。

例

次に、デフォルトの調整タイマーを含む、すべての SXP 接続のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

cts sxp retry period

ASA が SXP ピア間での新しい SXP 接続の設定を試行するデフォルトの時間間隔を指定するには、グローバル コンフィギュレーション モードで **cts sxp retry period** コマンドを使用します。コマンドのサポート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。

cts sxp retry period *timervalue*

no cts sxp retry period [*timervalue*]

構文の説明

timervalue	再試行タイマーのデフォルト値を指定します。0 ～ 64000 秒の範囲で秒数を入力します。

デフォルト

デフォルトでは、*timervalue* は 120 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
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

ASA が SXP ピア間での新しい SXP 接続の設定を試行するデフォルトの時間間隔を指定します。ASA は、成功した接続が確立されるまで接続を試み続けます。

ASA で確立されていない SXP 接続が存在する限り、再試行タイマーがトリガーされます。

0 秒を指定すると、タイマーの期限が切れず、ASA は SXP ピアへの接続を試行しません。

再試行タイマーが期限切れになると、ASA は接続データベースを順に検索し、データベースに切断されているか、または「保留中」状態の接続が含まれている場合、ASA は、再試行タイマーを再開します。

再試行タイマーは、SXP ピア デバイスとは異なる値に設定することを推奨します。

例

次に、デフォルトの再試行タイマーを含む、すべての SXP 接続のデフォルト値を設定する例を示します。

```
ciscoasa(config)# cts sxp enable
ciscoasa(config)# cts sxp default source-ip 192.168.1.100
ciscoasa(config)# cts sxp default password 8 ********
ciscoasa(config)# cts sxp retry period 60
ciscoasa(config)# cts sxp reconcile period 60
```

関連コマンド

コマンド	説明
cts sxp connection peer	ASA と SXP ピアとの SXP 接続を設定します。
cts sxp enable	ASA で SXP プロトコルをイネーブルにします。

customization

トンネル グループ、グループ、またはユーザに使用するカスタマイゼーションを指定するには、トンネル グループ webvpn 属性コンフィギュレーション モードまたは webvpn コンフィギュレーション モードで **customization** コマンドを使用します。カスタマイゼーションを指定しない場合は、このコマンドの **no** 形式を使用します。

customization *name*

no customization *name*

customization {**none** | **value** *name*}

no customization {**none** | **value** *name*}

構文の説明

name	グループまたはユーザに適用する WebVPN カスタマイゼーションの名前を指定します。
none	グループまたはユーザのカスタマイゼーションをディセーブルにし、カスタマイゼーションが継承されないようにします。
value *name*	グループ ポリシーまたはユーザに適用するカスタマイゼーションの名前を指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

トンネル グループ webvpn 属性コンフィギュレーション モードで **customization** コマンドを入力する前に、webvpn コンフィギュレーション モードで **customization** コマンドを使用してカスタマイゼーションの名前を付け、設定する必要があります。

Mode-Dependent コマンド オプション

customization コマンドで使用できるキーワードは使用しているモードによって異なります。グループ ポリシー属性コンフィギュレーション モードおよびユーザ名属性コンフィギュレーション モードでは、追加のキーワード **none** と **value** が表示されます。

たとえば、ユーザ名属性コンフィギュレーション モードで **customization none** コマンドを入力すると、ASA は、グループ ポリシーやトンネル グループ内の値を検索しません。

例

次に、パスワード プロンプトを定義する「123」という名前の WebVPN カスタマイゼーションを最初に確立するコマンド シーケンスの例を示します。この例では、次に「test」という名前の WebVPN トンネル グループを定義し、**customization** コマンドを使用して、「123」という名前の WebVPN カスタマイゼーションを使用することを指定しています。

```
ciscoasa(config)# webvpn
ciscoasa(config-webvpn)# customization 123
ciscoasa(config-webvpn-custom)# password-prompt Enter password
ciscoasa(config-webvpn)# exit
ciscoasa(config)# tunnel-group test type webvpn
ciscoasa(config)# tunnel-group test webvpn-attributes
ciscoasa(config-tunnel-webvpn)# customization 123
ciscoasa(config-tunnel-webvpn)#
```

次に、「cisco」というカスタマイゼーションを「cisco_sales」というグループ ポリシーに適用する例を示します。webvpn コンフィギュレーション モード経由でグループポリシー属性コンフィギュレーション モードになった場合は、**customization** コマンドに追加のコマンド オプション **value** が必要になります。

```
ciscoasa(config)# group-policy cisco_sales attributes
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# customization value cisco
```

関連コマンド

コマンド	説明
clear configure tunnel-group	すべてのトンネル グループ コンフィギュレーションを削除します。
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 webvpn-attributes	WebVPN トンネル グループ属性を設定する webvpn コンフィギュレーション モードを開始します。

cxsc

ASA CX モジュールにトラフィックをリダイレクトするには、クラス コンフィギュレーション モードで **cxsc** コマンドを使用します。ASA CX アクションを削除するには、このコマンドの **no** 形式を使用します。

cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

no cxsc {**fail-close** | **fail-open**} [**auth-proxy** | **monitor-only**]

構文の説明

auth-proxy	(オプション)アクティブ認証に必要な認証プロキシをイネーブルにします。
fail-close	ASA CX モジュールが使用できない場合、すべてのトラフィックをブロックするように ASA を設定します。
fail-open	ASA CX モジュールが使用できない場合、すべてのトラフィックの通過を検査なしで許可するように ASA を設定します。
monitor-only	デモンストレーションの目的のみで、**monitor-only** を指定して、トラフィックの読み取り専用コピーを ASA CX モジュールに送信します。このオプションを設定すると、次のような警告メッセージが表示されます。 `WARNING: Monitor-only mode should be used for demonstrations and evaluations only. This mode prevents CXSC from denying or altering traffic.`

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 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。
9.1(2)	デモンストレーション機能をサポートするために **monitor-only** キーワードが追加されました。
9.1(3)	コンテキストごとの ASA CX ポリシーを設定できるようになりました。

使用上のガイドライン

クラス コンフィギュレーション モードにアクセスするには、policy-map コマンドを入力します。

ASA で **cxsc** コマンドを設定する前または後に、Cisco Prime Security Manager（PRSM）を使用して ASA CX モジュールでセキュリティ ポリシーを設定します。

cxsc コマンドを設定するには、先に **class-map** コマンド、**policy-map** コマンド、および **class** コマンドを設定する必要があります。

トラフィック フロー

ASA CX モジュールは、ASA とは別のアプリケーションを実行します。ただし、そのアプリケーションは ASA のトラフィック フローに統合されます。ASA でトラフィックのクラスの **cxsc** コマンドを適用すると、トラフィックは次のように ASA と ASA CX モジュールを通過します。

1. トラフィックは ASA に入ります。
2. 着信 VPN トラフィックが復号化されます。
3. ファイアウォール ポリシーが適用されます。
4. バックプレーンを介して ASA CX モジュールにトラフィックが送信されます。
5. ASA CX モジュールはセキュリティ ポリシーをトラフィックに適用し、適切なアクションを実行します。
6. 有効なトラフィックがバックプレーンを介して ASA に返送されます。ASA CX モジュールがセキュリティ ポリシーに従ってトラフィックをブロックすることがあり、そのトラフィックは渡されません。
7. 発信 VPN トラフィックが暗号化されます。
8. トラフィックが ASA から出ます。

認証プロキシに関する情報

ASA CX が HTTP ユーザを認証する必要がある場合は（アイデンティティ ポリシーを利用するために）、認証プロキシとして動作するように ASA を設定する必要があります。つまり、ASA CX モジュールは認証要求を ASA インターフェイス IP アドレス/プロキシ ポートにリダイレクトします。デフォルトでは、ポートは 885 です（**cxsc auth-proxy port** コマンドでユーザが設定できます）。この機能は、トラフィックを ASA から ASA CX モジュールに誘導するサービス ポリシーの一部として設定します。認証プロキシ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。

ASA の機能との互換性

ASA には、HTTP インスペクションを含む、多数の高度なアプリケーション インスペクション機能があります。ただし、ASA CX モジュールには ASA よりも高度な HTTP インスペクション機能があり、その他のアプリケーションについても機能が追加されています。たとえば、アプリケーション使用状況のモニタリングと制御です。

ASA CX モジュールの機能を最大限に活用するには、ASA CX モジュールに送信するトラフィックに関する次のガイドラインを参照してください。

- HTTP トラフィックに対して ASA インスペクションを設定しないでください。
- クラウド Web セキュリティ（ScanSafe）インスペクションを設定しないでください。同じトラフィックに対して ASA CX のアクションとクラウド Web セキュリティ インスペクションの両方が設定されている場合に、ASA が実行するのは ASA CX のアクションのみです。
- ASA 上の他のアプリケーション インスペクションは ASA CX モジュールと互換性があり、これにはデフォルト インスペクションも含まれます。

- Mobile User Security（MUS）サーバをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- ASA クラスタリングをイネーブルにしないでください。これは、ASA CX モジュールとの間に互換性がありません。
- フェールオーバーをイネーブルにした場合は、ASA がフェールオーバーしたときに、既存の ASA CX フローは新しい ASA に転送されますが、トラフィックは ASA CX モジュールによる処理を受けることなく ASA の通過を許可されます。新しい ASA が受信した新しいフローだけが、ASA CX モジュールによる処理の対象となります。

モニタ専用モード

テストおよびデモンストレーション用に、**monitor-only** キーワードを使用して、ASA CX モジュールに読み取り専用トラフィックの重複ストリームを送信するように ASA を設定できるので、モジュールが ASA トラフィック フローに影響を与えることなく、どのようにトラフィックをインスペクションするかを確認できます。このモードでは、ASA CX モジュールが通常どおりトラフィックをインスペクションし、ポリシーを決定し、イベントを生成します。ただし、パケットが読み取り専用コピーであるため、モジュールのアクションは実際のトラフィックには影響しません。代わりに、モジュールはインスペクション後コピーをドロップします。

次のガイドラインを参照してください。

- ASA 上でモニタ専用モードと通常のインライン モードの両方を同時に設定できません。セキュリティ ポリシーの 1 つのタイプのみが許可されます。
- 次の機能は、モニタ専用モードでサポートされません。
  - 拒否ポリシー
  - アクティブ認証
  - 復号化ポリシー
- ASA CX は、モニタ専用モードでパケット バッファリングを実行せず、イベントはベスト エフォート方式で生成されます。たとえば、長い URL がパケット境界にまたがっている一部のイベントは、バッファリングの欠如の影響を受ける可能性があります。
- ASA ポリシーと ASA CX の両方でモードが一致するように設定する必要があります（両方ともモニタ専用モード、または両方とも通常のインライン モード）。

例

次の例では、すべての HTTP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合はすべての HTTP トラフィックがブロックされます。

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
```

次の例では、10.1.1.0 ネットワークと 10.2.1.0 ネットワーク宛てのすべての IP トラフィックが ASA CX モジュールに誘導され、何らかの理由で ASA CX モジュールに障害が発生した場合は、すべてのトラフィックの通過が許可されます。

```
ciscoasa(config)# access-list my-cx-acl permit ip any 10.1.1.0 255.255.255.0
ciscoasa(config)# access-list my-cx-acl2 permit ip any 10.2.1.0 255.255.255.0
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list my-cx-acl
ciscoasa(config)# class-map my-cx-class2
ciscoasa(config-cmap)# match access-list my-cx-acl2
```

```
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-open auth-proxy
ciscoasa(config-pmap)# class my-cx-class2
ciscoasa(config-pmap-c)# cxsc fail-open auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy interface outside
```

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。
class-map	ポリシー マップ用にトラフィックを識別します。
cxsc auth-proxy port	認証プロキシのポートを設定します。
debug cxsc	ASA CX デバッグ メッセージをイネーブルにします。
hw-module module password-reset	モジュールのパスワードをデフォルトにリセットします。
hw-module module reload	モジュールをリロードします。
hw-module module reset	リセットを実行してから、モジュールをリロードします。
hw-module module shutdown	モジュールをシャットダウンします。
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。
session do get-config	モジュール設定を取得します。
session do password-reset	モジュールのパスワードをデフォルトにリセットします。
session do setup host ip	モジュール管理アドレスを設定します。
show asp table classify domain cxsc	トラフィックを ASA CX モジュールに送信するために作成された NP ルールを表示します。
show asp table classify domain cxsc-auth-proxy	ASA CX モジュールの認証プロキシ用に作成された NP ルールを表示します。
show module	モジュールのステータスを表示します。
show running-config policy-map	現在のすべてのポリシー マップ 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。

cxsc auth-proxy port

ASA CX モジュール トラフィックの認証プロキシ ポートを設定するには、グローバル コンフィギュレーション モードで **cxsc auth-proxy port** コマンドを使用します。このポート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。

cxsc auth-proxy port *port*

no cxsc auth-proxy port [*port*]

構文の説明

port *port*	認証プロキシのポートを 1024 より大きい値に設定します。デフォルト値は 885 です。

コマンド デフォルト

デフォルト ポートは 885 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.4(4.1)	このコマンドが追加されました。
9.1(3)	コンテキストごとの ASA CX ポリシーを設定できるようになりました。

使用上のガイドライン

cxsc コマンドの設定時に認証プロキシをイネーブルにする場合は、このコマンドを使用してポートを変更できます。

ASA CX が HTTP ユーザを認証する必要がある場合は（アイデンティティ ポリシーを利用するために）、認証プロキシとして動作するように ASA を設定する必要があります。つまり、ASA CX モジュールは認証要求を ASA インターフェイス IP アドレス/プロキシ ポートにリダイレクトします。デフォルトでは、port は 885 です。この機能は、トラフィックを ASA から ASA CX モジュールに誘導するサービス ポリシーの一部として設定します。認証プロキシ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、ASA CX トラフィックの認証プロキシをイネーブルにし、ポートを 5000 に変更する例を示します。

```
ciscoasa(config)# access-list ASACX permit tcp any any eq port 80
ciscoasa(config)# class-map my-cx-class
ciscoasa(config-cmap)# match access-list ASACX
ciscoasa(config-cmap)# policy-map my-cx-policy
ciscoasa(config-pmap)# class my-cx-class
ciscoasa(config-pmap-c)# cxsc fail-close auth-proxy
ciscoasa(config-pmap-c)# service-policy my-cx-policy global
ciscoasa(config)# cxsc auth-port 5000
```

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。
class-map	ポリシー マップ用にトラフィックを識別します。
cxsc	ASA CX モジュールにトラフィックをリダイレクトします。
debug cxsc	ASA CX デバッグ メッセージをイネーブルにします。
hw-module module password-reset	モジュールのパスワードをデフォルトにリセットします。
hw-module module reload	モジュールをリロードします。
hw-module module reset	リセットを実行してから、モジュールをリロードします。
hw-module module shutdown	モジュールをシャットダウンします。
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。
session do get-config	モジュール設定を取得します。
session do password-reset	モジュールのパスワードをデフォルトにリセットします。
session do setup host ip	モジュール管理アドレスを設定します。
show asp table classify domain cxsc	トラフィックを ASA CX モジュールに送信するために作成された NP ルールを表示します。
show asp table classify domain cxsc-auth-proxy	ASA CX モジュールの認証プロキシ用に作成された NP ルールを表示します。
show module	モジュールのステータスを表示します。
show running-config policy-map	現在のすべてのポリシー マップ 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。