CHAPTER 9

crypto am-disable コマンド ～ crypto ipsec security-association replay コマンド

crypto am-disable

アグレッシブ モードの IPsec IKEv1 着信接続をディセーブルにするには、グローバル コンフィギュレーション モードで **crypto ikev1 am-disable** コマンドを使用します。アグレッシブ モードの着信接続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 ikev1 am-disable

no crypto ikev1 am-disable

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	—	—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp am-disable** コマンドが追加されました。
7.2.(1)	**isakmp am-disable** コマンドが、**crypto isakmp am-disable** コマンドに置き換えられました。
8.4(1)	コマンド名が **crypto isakmp am-disable** から **crypto ikev1 am-disable** に変更されました。

例

次に、グローバル コンフィギュレーション モードでの入力で、アグレッシブ モードの着信接続をディセーブルにする例を示します。

```
ciscoasa(config)# crypto ikev1 am-disable
```

関連コマンド

コマンド	説明
clear configure crypto isakmp	ISAKMP コンフィギュレーションをクリアします。
clear configure crypto isakmp policy	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	アクティブな設定を表示します。

crypto ca alerts expiration

インストールされているすべての証明書の有効期限チェックは **crypto ca alerts expiration** コマンドによりデフォルトでイネーブルになっています。有効期限チェック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 ca alerts expiration [begin <days before expiration>] [repeat <days>]

[no] crypto ca alerts expiration [begin <days before expiration>] [repeat <days>]

構文の説明

begin <*days before expiration*>	最初のアラートが発行される有効期限までの日数を設定し、リマインダが送信される間隔を設定します。指定できる範囲は 1 ～ 90 日です。
repeat <*days*>	証明書が更新されない場合のアラート頻度を設定します。範囲は 1 ～ 14 日です。

デフォルト

インストールされたすべての証明書の有効期限チェック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
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
9.4(1)	このコマンドが追加されました。

使用上のガイドライン

リマインダは syslog メッセージであるため、無効にする必要はないと考えています。このコマンドが確認されるのは、1 日 1 回だけであるため、パフォーマンスにほとんど影響を与えません。デフォルトでは、最初のアラートは有効期限の 60 日前に送信され、その後は証明書が更新または削除されるまで毎週 1 回送信されます。さらに、有効期限が切れる日にアラートが送信され、その後は毎日 1 回送信されます。アラートの設定に関係なく、有効期限の直前の週はリマインダが毎日送信されます。

例

```
100(config)# crypto ca ?

configure mode commands/options:
  alerts        Configure alerts

100(config)# crypto ca alerts ?
```

```
configure mode commands/options:
  expiration  Configure an alert for certificates nearing expiration
100(config)# crypto ca alerts expiration ?

configure mode commands/options:
  begin   Begin alert
  repeat  Repeat alert
  <cr>100(config)# crypto ca alerts expiration begin ?

configure mode commands/options:
  <1-90>  Days prior to expiration at which the first alert should be sent

100(config)# crypto ca alerts expiration begin 10 ?

configure mode commands/options:
  repeat  Repeat alert
  <cr>
100(config)# crypto ca alerts expiration begin 10 repeat ?

configure mode commands/options:
  <1-14>  Number of days at which the alert should be repeated after the prior
           alert

100(config)# crypto ca alerts expiration begin 10 repeat 1

100(config)# show run crypto ca ?

exec mode commands/options:
  alerts       Show alerts
       certificate  Show certificate map entries

    server         Show local certificate server configuration
    trustpoint   Show trustpoints
     trustpool    Show trustpool
  |             Output modifiers
  <cr>
100(config)# show run crypto ca alerts
crypto ca alerts expiration begin 10 repeat 1

100(config)# clear conf crypto ca ?

configure mode commands/options:
  alerts       Clear alerts
  certificate  Clear certificate map entries
  server       Clear Local CA server
  trustpoint   Clear trustpoints
  trustpool    Clear trustpool

100(config)# clear conf crypto ca alerts
```

関連コマンド

コマンド	説明
clear conf crypto ca alerts	設定済みの暗号 CA アラートをクリアします。
show run crypto ca alerts	設定済みの暗号 CA アラートを表示します。

crypto ca authenticate

トラストポイントに関連付けられている CA 証明書をインストールおよび認証するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。

crypto ca authenticate *trustpoint* [**fingerprint** *hexvalue*] [**nointeractive]**

構文の説明

fingerprint	ASA が CA 証明書の認証に使用する、英数字で構成されたハッシュ値を指定します。フィンガープリントが指定されている場合、ASA は、そのフィンガープリントを、CA 証明書の計算されたフィンガープリントと比較して、2 つの値が一致した場合にだけその証明書を受け入れます。フィンガープリントがない場合、ASA は計算されたフィンガープリントを表示し、証明書を受け入れるかどうかを尋ねます。
hexvalue	フィンガープリントの 16 進数値を指定します。
nointeractive	Device Manager 専用の非対話形式モードを使用して、このトラストポイントの CA 証明書を取得します。そのとき、フィンガープリントがない場合、ASA は確認せずに証明書を受け入れます。
trustpoint	CA 証明書を取得するトラストポイントを指定します。名前の最大長は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、CA 証明書は SCEP 経由でダウンロードされます。そうでない場合、ASA は、ユーザに Base 64 形式の CA 証明書を端末に貼り付けるように要求します。

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次に、CA 証明書を要求する ASA の例を示します。CA は証明書を送信し、ASA は、管理者に CA 証明書のフィンガープリントをチェックして CA 証明書を確認するように要求します。ASA の管理者は、表示されたフィンガープリントの値を既知の正しい値と照合する必要があります。ASA によって表示されたフィンガープリントが正しい値と一致した場合は、その証明書を有効であるとして受け入れる必要があります。

```
ciscoasa(config)# crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y#
ciscoasa(config)#
```

次に、トラストポイント tp9 が、端末ベース（手動）の登録用に設定される例を示します。ASA は、管理者に CA 証明書を端末に貼り付けるように要求します。証明書のフィンガープリントを表示した後、ASA は、管理者に証明書を保持することを確認するように要求します。

```
ciscoasa(config)# crypto ca authenticate tp9
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

MIIDjjCCAvegAwIBAgIQejIaQ3SJRIBMHcvDdgOsKTANBgkqhkiG9w0BAQUFADBA
MQswCQYDVQQGEwJVUzELMAkGA1UECBMCTUExETAPBgNVBAcTCEZyYW5rbGluMREw
DwYDVQQDEwhCcmlhbnNDQTAeFw0wMjEwMTcxODE5MTJaFw0wNjEwMjQxOTU3MDha
MEAxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4x
ETAPBgNVBAMTCEJyaWFuc0NBMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCd
jXEPvNnkZD1bKzahbTHuRot1T8KRUbCP5aWKfqViKJENzI2GnAheArazsAcc4Eaz
LDnpuyyqa0j5LA3MI577MoN1/nll018fbpqOf9eVDPJDkYTvtZ/X3vJgnEjTOWyz
T0pXxhdU1b/jgqVE74OvKBzU7A2yoQ2hMYzwVbGkewIDAQABo4IBhzCCAYMwEwYJ
KwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgFGMA8GA1UdEwEB/wQFMAMBAf8w
HQYDVR0OBBYEFBHr3holowFDmniI3FBwKpSEucdtMIIBGwYDVR0fBIIBEjCCAQ4w
gcaggcOggcCGgb1sZGFwOi8vL0NOPUJyaWFuc0NBLENOPWJyaWFuLXcyay1zdnIs
Q049Q0RQLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENO
PUNvbmZpZ3VyYXRpb24sREM9YnJpYW5wZGMsREM9YmRzLERDPWNvbT9jZXJ0aWZp
Y2F0ZVJldm9jYXRpb25MaXN0P2Jhc2U/b2JqZWN0Y2xhc3M9Y1JMRGlzdHJpYnV0
aW9uUG9pbnQwQ6BBoD+GPWh0dHA6Ly9icmlhbi13Mmstc3ZyLmJyaWFucGRjLmJk
cy5jb20vQ2VydEVucm9sbC9CcmlhbnNDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEw
DQYJKoZIhvcNAQEFBQADgYEAdLhc4Za3AbMjRq66xH1qJWxKUzd4nE9wOrhGgA1r
j4B/Hv2K1gUie34xGqu9OpwqvJgp/vCU12Ciykb1YdSDy/PxN4KtR9Xd1JDQMbu5
f20AYqCG5vpPWavCgmgTLcdwKa3ps1YSWGkhWmScHHSiGg1a3tevYVwhHNPA4mWo
7sQ=

Certificate has the following attributes:
Fingerprint: 21B598D5 4A81F3E5 0B24D12E 3F89C2E4
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca enroll	CA への登録を開始します。
crypto ca import certificate	手動登録要求への応答として CA から受信した証明書をインストールします。
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

crypto ca certificate chain

指定したトラストポイントの証明書チェーン コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca certificate chain** コマンドを使用します。

crypto ca certificate chain *trustpoint*

構文の説明

trustpoint	証明書チェーンを設定するトラストポイントを指定します。

デフォルト

デフォルトの値または動作はありません。

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。

例

次に、トラストポイント central の証明書チェーン 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)# crypto ca certificate chain central
ciscoasa(config-cert-chain)#
```

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。

crypto ca certificate map

証明書マッピング ルールの優先順位付けされたリストを管理するには、グローバル コンフィギュレーション モードで **crypto ca certificate map** コマンドを使用します。クリプト CA コンフィギュレーション マップ ルールを削除するには、このコマンドの **no** 形式を使用します。

crypto ca certificate map {*sequence-number* | *map-name sequence-number*}

no crypto ca certificate map {*sequence-number* | *map-name* [*sequence-number*]}

構文の説明

map-name	certificate-to-group マップの名前を指定します。
sequence-number	作成する証明書マップルールの番号を指定します。指定できる範囲は 1 ～ 65535 です。トンネル グループを証明書マップ ルールにマッピングするトンネル グループ マップを作成するときに、この番号を使用できます。

デフォルト

map-name のデフォルトの値は、DefaultCertificateMap 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	• 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)	*map-name* オプションが追加されました。

使用上のガイドライン

このコマンドを発行すると、ASA は CA 証明書マップ コンフィギュレーション モードになり、証明書の発行者およびサブジェクトの識別名（DN）に基づいてルールを設定できます。マッピング ルールの順序はシーケンス番号によって決まります。これらのルールの一般的な形式は次のとおりです。

- *DN match-criteria match-value*
- *DN* は、*subject-name* または *issuer-name* のいずれかです。DN は、ITU-T X.509 標準で定義されています。
- *match-criteria* は、次の表現または演算子で構成されます。

attr *tag*	比較を一般名（CN）などの特定の DN 属性に制限します。
co	含む
eq	等しい
nc	含まない
ne	等しくない

DN の一致表現は大文字と小文字が区別されません。

例

次に、example-map というマップ名とシーケンス番号 1（ルール番号 1）で CA 証明書マップ モードを開始し、subject-name という一般名（CN）属性が Example1 と一致する必要があることを指定する例を示します。

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name attr cn eq Example1
ciscoasa(ca-certificate-map)#
```

次に、example-map というマップ名とシーケンス番号 1 で CA 証明書マップ モードを開始して、subject-name 内に値 cisco が含まれることを指定する例を示します。

```
ciscoasa(config)# crypto ca certificate map example-map 1
ciscoasa(ca-certificate-map)# subject-name co cisco
ciscoasa(ca-certificate-map)#
```

関連コマンド

コマンド	説明
issuer-name	ルール エントリが IPsec ピア証明書の発行者 DN に適用されることを指定します。
subject-name（クリプト CA 証明書マップ）	ルール エントリが IPsec ピア証明書のサブジェクト DN に適用されることを指定します。
tunnel-group-map enable	**crypto ca certificate map** コマンドを使用して作成された証明書マップ エントリをトンネル グループに関連付けます。

crypto ca crl request

指定したトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求するには、クリプト CA トラストポイント コンフィギュレーション モードで **crypto ca crl request** コマンドを使用します。

crypto ca crl request *trustpoint*

構文の説明

trustpoint	トラストポイントを指定します。許容最大文字数は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.0(1)	このコマンドが追加されました。

使用上のガイドライン

このコマンドの呼び出しは、実行コンフィギュレーションの一部になりません。

例

次に、central という名前のトラストポイントに基づいて CRL を要求する例を示します。

```
ciscoasa(config)# crypto ca crl request central
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crl configure	CRL コンフィギュレーション モードを開始します。

crypto ca enroll

CA との登録プロセスを開始するには、グローバル コンフィギュレーション モードで **crypto ca enroll** コマンドを使用します。

crypto ca enroll *trustpoint* **[regenerate] [shared-secret <value> | signing-certificate <value>** [**noconfirm**]

構文の説明

noconfirm	(任意)すべてのプロンプトを表示しないようにします。要求される場合がある登録オプションは、トラストポイントに事前設定されている必要があります。このオプションは、スクリプト、ASDM、または他の非インタラクティブ形式で使用するためのものです。
regenerate	登録要求を作成する前に、新しいキー ペアを生成すべきかどうかを示します。
shared-secret	ASA と交換されるメッセージの信頼性と整合性を確認するために使用される、CA によるアウトオブバンド指定値。
signing-certificate	cmp 登録要求に署名するために使用された、以前の発行済みデバイス証明書を持つトラストポイントの名前。
トラストポイント	登録するトラストポイントの名前を指定します。許容最大文字数は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表は、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。
9.7(1)	再生成するオプションが追加され、共有秘密キーワードと署名証明書キーワードが追加されました。

使用上のガイドライン

トラストポイントが SCEP 登録用に設定されている場合、ASA はただちに CLI プロンプトを表示し、ステータス メッセージがコンソールに非同期的に表示されます。トラストポイントが手動登録用に設定されている場合、ASA が Base 64 エンコードの PKCS10 証明書要求をコンソールに書き込んでから、CLI プロンプトが表示されます。

このコマンドは、参照されるトラストポイントの設定された状態に応じて、異なるインタラクティブ プロンプトを生成します。このコマンドが正常に実行されるには、トラストポイントが正しく設定されている必要があります。

トラストポイントが CMP 用に設定されている場合、共有秘密値(ir)またはリクエストに署名する証明書を含むトラストポイントの名前(cr)のどちらかを指定できますが、両方を指定することはできません。共有秘密または署名証明書のキーワードは、トラストポイント登録プロトコルが CMP に設定されている場合にのみ使用できます。

例

次に、SCEP 登録を使用して、トラストポイント tp1 でアイデンティティ証明書の登録を要求する例を示します。ASA は、トラストポイント コンフィギュレーションで保存されていない情報を要求します。

```
ciscoasa(config)# crypto ca enroll tp1
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
% password to the CA Administrator in order to revoke your certificate.
% For security reasons your password will not be saved in the configuration.
% Please make a note of it.
Password:
Re-enter password:
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: xyz.example.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA [yes/no]: yes
% Certificate request sent to Certificate authority.
% The certificate request fingerprint will be displayed.
% The 'show crypto ca certificate' command will also show the fingerprint.

ciscoasa(config)#
```

次に、CA 証明書の手動登録の例を示します。

```
ciscoasa(config)# crypto ca enroll tp1

% Start certificate enrollment ..
% The fully-qualified domain name in the certificate will be: xyz.example.com
% The subject name in the certificate will be: wb-2600-3.example.com
if serial number not set in trustpoint, prompt:
% Include the router serial number in the subject name? [yes/no]: no
If ip-address not configured in trustpoint:
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: 1.2.3.4
Display Certificate Request to terminal? [yes/no]: y
Certificate Request follows:
MIIBFTCBwAIBADA6MTgwFAYJKoZIhvcNAQkIEwcxLjIuMy40MCAGCSqGSIb3DQEJ
AhYTd2ItMjYwMC0zLmNpc2NvLmNvbTBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQDT
IdvHa4D5wXZ+40sKQV7Uek1E+CC6hm/LRN3p5ULW1KF6bxhA3Q5CQfh4jDxobn+A
Y8GoeceulS2Zb+mvgNvjAgMBAAGgITAfBgkqhkiG9w0BCQ4xEjAQMA4GA1UdDwEB
/wQEAwIFoDANBgkqhkiG9w0BAQQFAANBACDhnrEGBVtltG7hp8x6Wz/dgY+ouWcA
lzy7QpdGhb1du2P81RYn+8pWRA43cikXMTeM4ykEkZhLjDUgv9t+R9c=

---End - This line not part of the certificate request---

Redisplay enrollment request? [yes/no]: no
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca aunticate	このトラストポイントの CA 証明書を取得します。
crypto ca import pkcs12	手動登録要求への応答として CA から受信した証明書をインストールします。
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

crypto ca export

ASA のトラストポイント コンフィギュレーションを、関連付けられているすべてのキーおよび証明書とともに PKCS12 形式でエクスポートするには、またはデバイスのアイデンティティ証明書を PEM 形式でエクスポートするには、グローバル コンフィギュレーション モードで **crypto ca export** コマンドを使用します。

crypto ca export *trustpoint* **identity-certificate**

構文の説明

identity-certificate	指定したトラストポイントに関連付けられている登録済み証明書をコンソールに表示することを指定します。
trustpoint	証明書が表示されるトラストポイントの名前を指定します。トラストポイント名の許容最大文字数は 128 文字です。

デフォルト

デフォルトの値または動作はありません。

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。
8.0(2)	このコマンドは、PEM 形式での証明書のエクスポートに対応するために変更されました。

使用上のガイドライン

このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。PEM データまたは PKCS12 データはコンソールに書き込まれます。

Web ブラウザでは、パスワードベースの対称キーで保護された付属の公開キー証明書とともに秘密キーを格納するために PKCS12 形式を使用しています。ASA は、トラストポイントに関連付けられている証明書とキーを Base 64 エンコードの PKCS12 形式でエクスポートします。この機能を使用して、証明書とキーを ASA 間で移動できます。

証明書の PEM エンコーディングは、PEM ヘッダーで囲まれた X.509 証明書の Base-64 エンコーディングです。このエンコーディングは、証明書を ASA 間でテキストベースで転送するための標準的なメソッドです。ASA がクライアントとして動作している場合は、SSL/TLS プロトコルを使用した *proxy-ldc-issuer* 証明書のエクスポートに PEM エンコーディングを使用できます。

例

次に、トラストポイント 222 の PEM 形式の証明書をコンソール表示としてエクスポートする例を示します。

```
ciscoasa (config)# crypto ca export 222 identity-certificate

Exported 222 follows:
-----BEGIN CERTIFICATE-----
MIIGDzCCBXigAwIBAgIKFiUgwwAAAAAFPDANBgkqhkiG9w0BAQUFADCBnTEfMB0G
CSqGSIb3DQEJARYQd2Jyb3duQGNpc2NvLmNvbTELMAkGA1UEBhMCVVMxCzAJBgNV
BAgTAk1BMREwDwYDVQQHEwhGcmFua2xpbjEWMBQGA1UEChMNQ2lzY28gU3lzdGVt
czEZMBcGA1UECxMQRnJhbmtsaW4gRGV2VGVzdDEaMBgGA1UEAxMRbXMtcm9vdC1j
YS01LTIwMDQwHhcNMDYxMTAyMjIyNjU3WhcNMjQwNTIwMTMzNDUyWjA2MRQwEgYD
VQQFEwtKTVgwOTQwSzA0TDEeMBwGCSqGSIb3DQEJAhMPQnJpYW4uY2lzY28uY29t
MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCvxxIYKcrb7cJpsiFKwwsQUph5
4M5Y3CDVKEVF+98HrD6rhd0n/d6R8VYSfu76aeJC5j9Bbn3xOCx2aY5K2enf3SBW
Y66S3JeZBV88etFmyYJ7rebjUVVQZaFcq79EjoP99IeJ3a89Y7dKvYqq8I3hmYRe
uipm1G6wfKHOrpLZnwIDAQABo4IDujCCA7YwCwYDVR0PBAQDAgWgMBoGA1UdEQQT
MBGCD0JyaWFuLmNpc2NvLmNvbTAdBgNVHQ4EFgQUocM/JeVV3fjZh4wDe0JS74Jm
pvEwgdkGA1UdIwSB0TCBzoAUYZ8t0+V9pox+Y47NtCLk7WxvIQShgaOkgaAwgZ0x
HzAdBgkqhkiG9w0BCQEWEHdicm93bkBjaXNjby5jb20xCzAJBgNVBAYTAlVTMQsw
CQYDVQQIEwJNQTERMA8GA1UEBxMIRnJhbmtsaW4xFjAUBgNVBAoTDUNpc2NvIFN5
c3RlbXMxGTAXBgNVBAsTEEZyYW5rbGluIERldlRlc3QxGjAYBgNVBAMTEW1zLXJv
b3QtY2EtNS0yMDA0ghBaZ5s0Ng4SskMxF2NlIoxgMIIBSAYDVR0fBIIBPzCCATsw
geuggeiggeWGgeJsZGFwOi8vd2luMmstYWQuRlJLLU1TLVBLSS5jaXNjby5jb20v
Q049bXMtcm9vdC1jYS01LTIwMDQsQ049d2luMmstYWQsQ049Q0RQLENOPVB1Ymxp
YyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNvbmZpZ3VyYXRpb24s
REM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y2VydGlmaWNhdGVSZXZvY2F0
aW9uTGlzdD9iYXNlP29iamVjdGNsYXNzPWNSTERpc3RyaWJ1dGlvblBvaW50MEug
SaBHhkVodHRwOi8vd2luMmstYWQuZnJrLW1zLXBraS5jaXNjby5jb20vQ2VydEVu
cm9sbC9tcy1yb290LWNhLTUtMjAwNC5jcmwwggFCBggrBgEFBQcBAQSCATQwggEw
MIG8BggrBgEFBQcwAoaBr2xkYXA6Ly8vQ049bXMtcm9vdC1jYS01LTIwMDQsQ049
QUlBLENOPVB1YmxpYyUyMEtleSUyMFNlcnZpY2VzLENOPVNlcnZpY2VzLENOPUNv
bmZpZ3VyYXRpb24sREM9RlJLLU1TLVBLSSxEQz1jaXNjbyxEQz1jb20/Y0FDZXJ0
aWZpY2F0ZT9iYXNlP29iamVjdGNsYXNzPWNlcnRpZmljYXRpb25BdXRob3JpdHkw
bwYIKwYBBQUHMAKGY2h0dHA6Ly93aW4yay1hZC5mcmstbXMtcGtpLmNpc2NvLmNv
bS9DZXJ0RW5yb2xsL3dpbjJrLWFkLkZSSy1NUy1QS0kuY2lzY28uY29tX21zLXJv
b3QtY2EtNS0yMDA0LmNydDANBgkqhkiG9w0BAQUFAAOBgQBlh7maRutcKNpjPbLk
bdcafJfHQ3k4UoWo0s1A0LXzdF4SsBIKQmpbfqEHtlx4EsfvfHXxUQJ6TOab7axt
hxMbNX3m7giebvtPkreqR9OYWGUjZwFUZ16TWnPA/NP3fbqRSsPgOXkC7+/5oUJd
eAeJOF4RQ6fPpXw9LjO5GXSFQA==
-----END CERTIFICATE-----
ciscoasa (config)#
```

関連コマンド

コマンド	説明
crypto ca aunticate	このトラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。

コマンド	説明
crypto ca import	手動登録要求への応答として CA から受信した証明書をインストールします。
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

crypto ca import

手動登録要求への応答で CA から受信した証明書をインストールしたり、PKCS12 データを使用してトラストポイントの証明書とキー ペアをインポートしたりするには、グローバル コンフィギュレーション モードで **crypto ca import** コマンドを使用します。

crypto ca import *trustpoint* **certificate** [**nointeractive**]

crypto ca import *trustpoint* **pkcs12** *passphrase* [**nointeractive**]

構文の説明

certificate	トラストポイントによって示される CA から証明書をインポートするよう ASA に指示します。
nointeractive	(オプション)非インタラクティブ モードを使用して証明書をインポートします。すべてのプロンプトが抑制されます。このオプションは、スクリプト、ASDM、または他の非インタラクティブ形式で使用するためのものです。
passphrase	PKCS12 データの復号化に使用するパスフレーズを指定します。
pkcs12	PKCS12 形式を使用してトラストポイントの証明書とキー ペアをインポートするよう ASA に指示します。
trustpoint	インポート アクションを関連付けるトラストポイントを指定します。許容最大文字数は 128 文字です。PKCS12 データをインポートし、トラストポイントが RSA キーを使用する場合、インポートされるキー ペアにはトラストポイントと同じ名前が割り当てられます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

例

次に、トラストポイント Main の証明書を手動でインポートする例を示します。

```
ciscoasa (config)# crypto ca import Main certificate
% The fully-qualified domain name in the certificate will be:
securityappliance.example.com
```

```
Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself
[ certificate data omitted ]
quit
INFO: Certificate successfully imported
ciscoasa (config)#
```

次に、PKCS12 データをトラストポイント central に手動でインポートする例を示します。

```
ciscoasa (config)# crypto ca import central pkcs12

Enter the base 64 encoded pkcs12.
End with a blank line or the word "quit" on a line by itself:
[ PKCS12 data omitted ]
quit
INFO: Import PKCS12 operation completed successfully
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、RSA キーペアを保存する十分なスペースが NVRAM にないため、警告メッセージが生成されています。

```
ciscoasa(config)# crypto ca import central pkcs12 mod 2048
INFO: The name for the keys will be: central
Keypair generation process begin. Please wait...
NV RAM will not have enough space to save keypair central. Remove any unnecessary keypairs
and save the running config before using this keypair.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ca export	トラストポイントの証明書とキー ペアを PKCS12 形式でエクスポートします。
crypto ca aunticate	トラストポイントの CA 証明書を取得します。
crypto ca enroll	CA への登録を開始します。
crypto ca trustpoint	指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始します。

crypto ca reference-identity

参照 ID オブジェクトを設定するには、コンフィギュレーション モードで **crypto ca reference-identity** コマンドを使用します。参照 ID オブジェクトを削除するには、このコマンドの **no** 形式を使用します。

crypto ca reference-identity *reference_identity_name*

no crypto ca reference-identity *reference_identity_name*

ASA を *ca-reference-identity* モードにするには、グローバル コンフィギュレーション モードで **crypto ca reference-identity** コマンドを入力します。*ca-reference-identity* モードで、次の参照 ID を入力します。任意のタイプの参照 ID を複数追加することができます。参照 ID を削除するには、各コマンドの **no** 形式を使用します。

[**no**] **cn-id** *value*

[**no**] **dns-id** *value*

[**no**] **srv-id** *value*

[**no**] **uri-id** *value*

構文の説明

reference-identity-name	参照 ID オブジェクトの名前。
value	各参照 ID の値。
cn-id	一般名（CN）。この値は、ドメイン名の全体的な形式に一致します。CN 値は自由形式のテキストにすることはできません。CN-ID 参照 ID では、アプリケーション サービスは特定されません。
dns-id	タイプ dNSName の subjectAltName エントリ。これは DNS ドメイン名です。DNS-ID 参照 ID では、アプリケーション サービスは特定されません。
srv-id	RFC 4985 に定義されている SRVName 形式の名前をもつ、otherName タイプの subjectAltName エントリ。SRV-ID 識別子には、ドメイン名とアプリケーション サービス タイプの両方を含めることができます。たとえば、「_imaps.example.net」の SRV-ID は、DNS ドメイン名部分の「example.net」と、アプリケーション サービス タイプ部分の「imaps」に分けられます。
uri-id	タイプ uniformResourceIdentifier の subjectAltName エントリです。この値には、「scheme」コンポーネントと、RFC 3986 に定義されている「reg-name」ルールに一致する「host」コンポーネント（またはこれに相当するコンポーネント）の両方が含まれます。URI-ID 識別子には、IP アドレスではなく、およびホスト名だけではなく、DNS ドメイン名を含める必要があります。たとえば、「sip:voice.example.edu」という URI-ID は、DNS ドメイン名の「voice.example.edu」とアプリケーション サービス タイプの「sip」に分割できます。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード　次の表に、コマンドを入力できるモードを示します。

コマンド モード	ファイアウォール モード		セキュリティ コンテキスト		
				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
9.6(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

ASA を *ca-reference-identity* モードにするには、グローバル コンフィギュレーション モードで **crypto ca reference-identity** コマンドを入力します。*ca-reference-identity* モードで、参照 ID（cn-id、dns-id、srv-id、または uri-id）を入力します。任意のタイプの参照 ID を複数追加することができます。参照 ID を削除するには、各コマンドの **no** 形式を使用します。

参照 ID は、未使用の名前を設定すると作成されます。参照 ID が作成されると、4 つの ID タイプと関連付けられた値を参照 ID に追加、または参照 ID から削除することができます。

複数のエントリが使用されている場合、証明書に srv-id、uri-id、または dns-id の少なくとも 1 つのインスタンスが含まれていると、次の動作が予想されます。

- 証明書内の uri-id のいずれかのインスタンスが、名前付き参照 id の uri-id の任意のインスタンスと一致する場合、証明書は参照 ID と一致します。
- 証明書内の srv-id のいずれかのインスタンスが、名前付き参照 id の srv-id の任意のインスタンスと一致する場合、証明書は参照 ID と一致します。
- 証明書内の dns-id のいずれかのインスタンスが、名前付き参照 id の dns-id の任意のインスタンスと一致する場合、証明書は参照 ID と一致します。
- これらのシナリオが存在しない場合、証明書は参照 ID と一致しません。

複数のエントリが使用されている場合、証明書に srv-id、uri-id、または dns-id の少なくとも 1 つのインスタンスが含まれていないが、少なくとも 1 つの cn-id が含まれていると、次の動作が予想されます。

- 証明書内の cn-id のいずれかのインスタンスが、名前付き参照 id の cn-id の任意のインスタンスと一致する場合、証明書は参照 ID と一致します。それ以外の場合、証明書は参照 ID と一致しません。
- 証明書に srv-id、uri-id、dns-id、または cn-id の少なくとも 1 つのインスタンスが含まれていない場合、証明書は参照 ID と一致しません。

ASA が TLS クライアントとして動作する場合、ASA は RFC 6125 で定義されているアプリケーション サーバの ID の検証ルールをサポートします。ASA で設定される参照 ID は、接続の確立中にサーバ証明書で提示される ID と比較されます。これらの ID は、RFC 6125 で定義されている 4 つの ID タイプの特定のインスタンスです。

参照 ID の **cn ID** と **dns ID** には、アプリケーション サービスを特定する情報を含めることができず、DNS ドメイン名を特定する情報が含まれている必要があります。

例

次に、syslog サーバの参照 ID を作成する例を示します。

```
ciscoasa(config)# crypto ca reference-identity syslogServer
ciscoasa(config-ca-ref-identity)# dns-id syslog1-bxb.cisco.com
ciscoasa(config-ca-ref-identity)# cn-id syslog1-bxb.cisco.com
```

関連コマンド

コマンド	説明
cn-id	参照 ID オブジェクトのコモン ネーム ID を設定します。
dns-id	参照 ID オブジェクトの DNS ドメイン名 ID を設定します。
srv-id	参照 ID オブジェクトで SRV-ID 識別子を設定します。
uri-id	参照 ID オブジェクトの URI ID を設定します。
logging host	セキュアな接続のために参照 ID オブジェクトを使用できるロギング サーバを設定します。
call-home profile destination address http	安全な接続のために参照 ID オブジェクトを使用できる Smart Call Home サーバを設定します。

crypto ca server（廃止）

ASA 上のローカル CA サーバを設定および管理するには、グローバル コンフィギュレーション モードで **crypto ca server** コマンドを使用します。設定されているローカル CA サーバを ASA 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 ca server

no crypto ca server

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

認証局サーバは、ASA 上でイネーブルになっていません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
8.0(2)	このコマンドが追加されました。
9.12(1)	**smtp** コマンドで、登録 URL のユーザの FQDN を設定するためのプロビジョニング。設定されていない場合、デフォルトで ASA の FQDN が使用されます。 このコマンドは廃止予定で、将来のリリースでは削除されます。
9.13(1)	このコマンドは削除されました。

使用上のガイドライン

ASA 上にローカル CA は 1 つしか存在できません。

crypto ca server コマンドは CA サーバを設定しますが、イネーブルにはしません。ローカル CA をイネーブルにするには、CA サーバ コンフィギュレーション モードで **shutdown** コマンドの **no** 形式を使用します。

no shutdown コマンドで CA サーバをアクティブにすると、CA および LOCAL-CA-SERVER というトラストポイントの RSA キー ペアが確立されて自己署名証明書が保持されます。この新しく生成された自己署名証明書には、デジタル署名、CRL 署名、および証明書署名キーの使用法の設定が常に含まれます。

バージョン 9.12(1) 以降では、ASA を使用して登録 URL の FQDN を設定できます。通常、ユーザは、内部 DNS を ASA FQDN として設定し、外部 DNS を登録電子メールに含まれる FQDN で設定します。ユーザは **fqdn** コマンドを使用して、ASA の FQDN ではなく、登録 URL の FQDN を設定できます。設定されていない場合、ASA はデフォルトでその FQDN を使用します。

注意 **no crypto ca server** コマンドは、ローカル CA サーバの現在の状態に関係なく、設定されているローカル CA サーバ、その RSA キー ペア、および関連付けられているトラストポイントを削除します。

例

次に、CA サーバ コンフィギュレーション モードを開始して、このモードで使用可能なローカル CA サーバ コマンドをリストする例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# ?

CA Server configuration commands:
  cdp-url               CRL Distribution Point to be included in the issued
                        certificates
  database              Embedded Certificate Server database location
                        configuration
  enrollment-retrieval  Enrollment-retrieval timeout configuration
  exit                  Exit from Certificate Server entry mode
  help                  Help for crypto ca server configuration commands
  issuer-name           Issuer name
  keysize               Size of keypair in bits to generate for certificate
                        enrollments
  lifetime              Lifetime parameters
  no                    Negate a command or set its defaults
  otp                   One-Time Password configuration options
  renewal-reminder      Enrollment renewal-reminder time configuration
  shutdown              Shutdown the Embedded Certificate Server
  smtp                  SMTP settings for enrollment E-mail notifications
  subject-name-default  Subject name default configuration for issued
                        certificates
```

次に、**smtp** コマンドでユーザの *fqdn* を設定し、出力を検証する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# smtp fqdn asa1-localCA.server.amazon.com
ciscoasa(config-ca-server)# show run crypto ca server

crypto ca server
    smtp fqdn asa1-localCA.server.amazon.com
```

次に、設定済みでイネーブルになっている CA サーバを ASA から削除するために、CA サーバ コンフィギュレーション モードで **crypto ca server** コマンドの **no** 形式を使用する例を示します。

```
ciscoasa(config-ca-server)# no crypto ca server

Certificate server 'remove server' event has been queued for processing.
ciscoasa(config)#
```

関連コマンド

コマンド	説明
debug crypto ca server	ローカル CA サーバを設定するときに、デバッグ メッセージを表示します。
show crypto ca server	設定されている CA サーバのステータスおよびパラメータを表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。

crypto ca server crl issue

証明書失効リスト(CRL)の発行を強制的に行うには、特権 EXEC モードで **crypto ca server crl issue** コマンドを使用します。

crypto ca server crl issue

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
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

失われた CRL を回復するには、このコマンドを使用します。通常、CRL は失効時に既存の CRL に再署名することで自動的に再発行されます。**crypto ca server crl issue** コマンドは、証明書データベースに基づいて CRL を再生成します。また、このコマンドを使用するのは、証明書データベースの内容に基づいて CRL を再生成する必要がある場合だけです。

例

次に、ローカル CA サーバによる CRL の発行を強制的に行う例を示します。

```
ciscoasa(config-ca-server)# crypto ca server crl issue
A new CRL has been issued.
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
cdp-url	CA によって発行される証明書に含める証明書失効リスト配布ポイントを指定します。
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。

crypto ca server revoke

ローカル認証局（CA）サーバによって発行された証明書を証明書データベースと CRL で失効としてマークするには、特権 EXEC モードで **crypto ca server revoke** コマンドを使用します。

crypto ca server revoke *cert-serial-no*

構文の説明

cert-serial-no	失効させる証明書のシリアル番号を指定します。16 進形式で指定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA 上のローカル CA によって発行された特定の証明書を失効させるには、その ASA で **crypto ca server revoke** コマンドを入力します。証明書は、このコマンドによって CA サーバの証明書データベースと CRL に失効としてマークされると失効します。失効させる証明書を指定するには、証明書のシリアル番号を 16 進形式で入力します。

指定した証明書が失効した後に、CRL が自動的に再生成されます。

例

次に、ローカル CA サーバによって発行されたシリアル番号 782ea09f の証明書を失効させる例を示します。

```
ciscoasa(config-ca-server)## crypto ca server revoke 782ea09f
Certificate with the serial number 0x782ea09f has been revoked. A new CRL has been issued.
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server unrevoke	ローカル CA サーバによって発行され、失効した証明書の失効を取り消します。
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
show crypto ca server crl	ローカル CA の現在の CRL を表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server unrevoke

ローカル CA サーバによって発行され、失効した証明書の失効を取り消すには、特権 EXEC モードで **crypto ca server unrevoke** コマンドを使用します。

crypto ca server unrevoke *cert-serial-no*

構文の説明

cert-serial-no	失効を取り消す証明書のシリアル番号を指定します。16 進形式で指定する必要があります。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

ASA 上のローカル CA によって発行され、失効した証明書の失効を取り消すには、**crypto ca server unrevoke** コマンドを入力します。証明書は、このコマンドによって証明書が証明書データベースで有効とマークされ、CRL から削除されると、再び有効になります。失効を取り消す証明書を指定するには、証明書のシリアル番号を 16 進形式で入力します。

指定した証明書の失効が取り消された後に、CRL が再生成されます。

例

次に、ローカル CA サーバによって発行されたシリアル番号 782ea09f の証明書の失効を取り消す例を示します。

```
ciscoasa(config-ca-server)# crypto ca server unrevoke 782ea09f
Certificate with the serial number 0x782ea09f has been unrevoked. A new CRL has been
issued.
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server user-db add

CA サーバのユーザ データベースに新しいユーザを挿入するには、特権 EXEC モードで **crypto ca server user-db add** コマンドを使用します。

crypto ca server user-db add *user* [**dn** *dn*] [**email** *e-mail-address*]

構文の説明

dn *dn*	追加するユーザに対して発行される証明書のサブジェクト名認定者名を指定します。DN ストリングにスペースが含まれている場合は、値を二重引用符で囲みます。カンマは、DN 属性を区切るためにのみ使用できます（「OU=Service, O=Company, Inc.」など）。
email *e-mail-address*	新しいユーザの電子メール アドレスを指定します。
user	登録特権の付与対象となる 1 人のユーザを指定します。ユーザ名は、単純なユーザ名または電子メール アドレスです。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

user 引数には単純なユーザ名（user1 など）または電子メール アドレス（user1@example.com など）を指定できます。*username* は、エンド ユーザが登録ページで指定したユーザ名と一致する必要があります。

username は、特権のないユーザとしてデータベースに追加されます。登録特権を付与するには、**crypto ca server allow** コマンドを使用する必要があります。

username 引数をワンタイム パスワードとともに使用して、登録インターフェイス ページでユーザを登録します。

(注) ワンタイム パスワード(OTP)を電子メールで通知するには、*username* 引数または *email-address* 引数に電子メール アドレスを指定する必要があります。メール送信時に電子メール アドレスが指定されていない場合、エラーが生成されます。

email *e-mail-address* のキーワードと引数のペアは、ユーザに登録と更新を忘れないように通知するための電子メール アドレスとしてのみ使用され、発行される証明書には表示されません。

電子メール アドレスを指定すると、質問がある場合にユーザに連絡することができ、また、その電子メール アドレス宛てに、登録に必要なワンタイム パスワードが通知されます。

ユーザにオプションの DN が指定されていない場合、サブジェクト名 DN は、*username* と subject-name-default DN 設定を使用して cn=*username*, subject-name-default として形成されます。

例

次に、ユーザ名 user1@example.com のユーザを完全なサブジェクト名 DN とともにユーザ データベースに追加する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db add dn "cn=Jane Doe, ou=engineering,
o=Example, l=RTP, st=NC, c=US"
ciscoasa(config-ca-server)#
```

次に、user2 というユーザに登録特権を付与する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user2
ciscoasa(config-ca-server)
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、CA への登録を許可します。
crypto ca server user-db remove	CA サーバ データベースからユーザを削除します。
crypto ca server user-db write	**database path** コマンドで指定したファイルに、CA サーバ データベース内のユーザ情報をコピーします。
database path	ローカル CA データベースのパスまたは場所を指定します。デフォルトの場所はフラッシュ メモリです。

crypto ca server user-db allow

ユーザまたはユーザのグループにローカル CA サーバ データベースへの登録を許可するには、特権 EXEC モードで **crypto ca server user-db allow** コマンドを使用します。このコマンドには、ワンタイム パスワードを生成および表示したり、ワンタイム パスワードをユーザに電子メールで送信したりするオプションも含まれています。

crypto ca server user-db allow {*username* | **all-unenrolled** | **all-certholders**} [**display-otp**] [**email-otp**] [**replace-otp**]

構文の説明

all-certholders	証明書が有効かどうかに関係なく、証明書が発行されているデータベース内のすべてのユーザに登録特権を付与することを指定します。これは、更新特権の付与と同じです。
all-unenrolled	証明書が発行されていないデータベース内のすべてのユーザに登録特権を付与することを指定します。
email-otp	(任意)指定したユーザのワンタイム パスワードを、それらのユーザの設定済み電子メール アドレスに電子メールで送信します。
replace-otp	(任意)指定したユーザのうち、有効なワンタイム パスワードを当初は持っていたすべてのユーザに対してワンタイム パスワードを再生成することを指定します。
display-otp	(オプション)指定したすべてのユーザのワンタイム パスワードをコンソールに表示します。
username	登録特権の付与対象となる 1 人のユーザを指定します。ユーザ名として簡易ユーザ名または電子メール アドレスを指定できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

replace-otp キーワードを指定すると、指定したすべてのユーザに対して OTP が生成されます。指定したユーザに対して生成された有効な OTP は、これらの新しい OTP で置き換えられます。

OTP は、ASA に保存されませんが、ユーザに通知したり、登録時にユーザを認証したりする必要がある場合に生成および再生成されます。

例

次に、データベース内のすべての未登録ユーザに登録特権を付与する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db allow all-unenrolled
ciscoasa(config-ca-server)#
```

次に、user1 というユーザに登録特権を付与する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db allow user1
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server	CA サーバ コンフィギュレーション モードのコマンド セットにアクセスできるようにします。これらのコマンド セットを使用することで、ローカル CA を設定および管理できます。
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db write	**database path** コマンドで指定したファイルに、CA サーバ データベース内のユーザ情報をコピーします。
enrollment-retrieval	登録されたユーザが PKCS12 登録ファイルを取得できる期間を時間単位で指定します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

crypto ca server user-db email-otp

ローカル CA サーバ データベース内の特定のユーザまたはユーザのサブセットに OTP を電子メールで送信するには、特権 EXEC モードで **crypto ca server user-db email-otp** コマンドを使用します。

crypto ca server user-db email-otp {*username* | **all-unenrolled** | **all-certholders**}

構文の説明

all-certholders	証明書が有効かどうかに関係なく、その証明書が発行されているデータベース内のすべてのユーザに OTP を電子メールで送信することを指定します。
all-unenrolled	証明書が一度も発行されていないか、期限が切れた証明書または失効した証明書しか保持していない、データベース内のすべてのユーザに OTP を電子メールで送信することを指定します。
username	1 人のユーザ用の OTP をそのユーザに電子メールで送信することを指定します。ユーザ名として、ユーザ名または電子メール アドレスを使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、データベース内のすべての未登録ユーザに OTP を電子メールで送信する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp all-unenrolled
ciscoasa(config-ca-server)#
```

次に、user1 というユーザに OTP を電子メールで送信する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db email-otp user1
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db show-otp	CA サーバ データベース内の特定のユーザまたはユーザのサブセットのワンタイム パスワードを表示します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca server user-db remove

ローカル CA サーバのユーザ データベースからユーザを削除するには、特権 EXEC モードで **crypto ca server user-db remove** コマンドを使用します。

crypto ca server user-db remove *username*

構文の説明

username	削除するユーザの名前を、ユーザ名または電子メール アドレスの形式で指定します。

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
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、CA ユーザ データベースからユーザ名を削除して、ユーザが登録できないようにします。また、このコマンドには、前に発行された有効な証明書を失効させるオプションもあります。

例

次に、ユーザ名 user1 のユーザを CA サーバのユーザ データベースから削除する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db remove user1

WARNING: No certificates have been automatically revoked. Certificates issued to user
user1 should be revoked if necessary.

ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server crl issue	CRL を強制的に発行します。
crypto ca server revoke	ローカル CA サーバが発行した証明書を、証明書データベースと CRL で失効としてマークします。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。
crypto ca server user-db write	ローカル CA データベースに設定されているユーザ情報を、**database path** コマンドで指定したファイルに書き込みます。

crypto ca server user-db show-otp

ローカル CA サーバ データベース内の特定のユーザまたはユーザのサブセットの OTP を表示するには、特権 EXEC モードで **crypto ca server user-db show-otp** コマンドを使用します。

crypto ca server user-db show-otp {*username* | **all-certholders** | **all-unenrolled**}

構文の説明

all-certholders	証明書が現在有効かどうかに関係なく、その証明書が発行されているデータベース内のすべてのユーザの OTP を表示します。
all-unenrolled	証明書が一度も発行されていないか、期限が切れた証明書または失効した証明書しか保持していない、データベース内のすべてのユーザの OTP を表示します。
username	1 人のユーザの OTP を表示することを指定します。*ユーザ名*として、ユーザ名または電子メール アドレスを使用できます。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

例

次に、有効または無効な証明書を持つデータベース内のすべてのユーザの OTP を表示する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp all-certholders
ciscoasa(config-ca-server)#
```

次に、user1 というユーザの OTP を表示する例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db show-otp user1
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
crypto ca server user-db allow	CA サーバ データベース内の特定のユーザまたはユーザのサブセットに、ローカル CA への登録を許可します。
crypto ca server user-db email-otp	CA サーバ データベース内の特定のユーザまたはユーザのサブセットにワンタイム パスワードを電子メールで送信します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。

crypto ca server user-db write

すべてのローカル CA データベース ファイルを保存するディレクトリの場所を設定するには、特権 EXEC モードで **crypto ca server user-db write** コマンドを使用します。

crypto ca server user-db write

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
CA サーバ コンフィギュレーション	• 対応	—	• 対応	—	—
グローバル コンフィギュレーション	• 対応	—	• 対応	—	—
特権 EXEC	• 対応	—	• 対応	—	—

コマンド履歴

リリース	変更内容
8.0(2)	このコマンドが追加されました。

使用上のガイドライン

crypto ca server user-db write コマンドを使用して、新しいユーザベースのコンフィギュレーション データを、データベース パス コンフィギュレーションで指定したストレージに保存します。この情報は、**crypto ca server user-db add** コマンドおよび **crypto ca server user-db allow** コマンドで新しいユーザが追加または許可されると生成されます。

例

次に、ローカル CA データベースに設定されているユーザ情報を保存場所に書き込む例を示します。

```
ciscoasa(config-ca-server)# crypto ca server user-db write
ciscoasa(config-ca-server)#
```

関連コマンド

コマンド	説明
crypto ca server user-db add	CA サーバのユーザ データベースにユーザを追加します。
database path	ローカル CA データベースのパスまたは場所を指定します。デフォルトの場所はフラッシュ メモリです。
crypto ca server user-db remove	CA サーバのユーザ データベースからユーザを削除します。
show crypto ca server cert-db	ローカル CA によって発行された証明書をすべて表示します。
show crypto ca server user-db	CA サーバのユーザ データベースに含まれているユーザを表示します。

crypto ca trustpoint

指定したトラストポイントのクリプト CA トラストポイント コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。指定した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 ca trustpoint *trustpoint-name*

no crypto ca trustpoint *trustpoint-name* [**noconfirm**]

構文の説明

noconfirm	すべての対話形式プロンプトを非表示にします。
trustpoint-name	管理するトラストポイントの名前を指定します。許容される名前の最大長は 128 文字です。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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)	OCSP をサポートするためにオプションが追加されました。これらのサブコマンドには、**match certificate map**、**ocsp disable-nonce**、**ocsp url**、**revocation-check** が含まれます。
8.0(2)	証明書の検証をサポートするためにオプションが追加されました。これらのサブコマンドには、**id-usage** と **validation-policy** が含まれます。**accept-subordinates**、**id-cert-issuer**、および **support-user-cert-validation** は廃止されました。
8.0(4)	信頼できるエンタープライズ間（電話プロキシと TLS プロキシ間など）での自己署名証明書の登録をサポートするために、**enrollment self** オプションが追加されました。
9.13(1)	The **crl required | optional | nocheck** オプションは削除されました。 **match certificate** オプションが変更され、**ovreride CDP** 設定が含まれるようになりました。

使用上のガイドライン

CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。このコマンドを発行すると、クリプト CA トラストポイント コンフィギュレーション モードが開始されます。

このコマンドは、トラストポイント情報を管理します。トラストポイントは、CA が発行する証明書に基づいた CA のアイデンティティとデバイスのアイデンティティを表します。トラストポイント モード内のコマンドは、CA 固有のコンフィギュレーション パラメータを制御します。これらのパラメータでは、ASA が CA 証明書を取得する方法、ASA が CA から証明書を取得する方法、および CA が発行するユーザ証明書の認証ポリシーを指定します。

トラストポイントの特性を指定するには、次のコマンドを入力します。

- **accept-subordinates**：廃止されました。トラストポイントに関連付けられた CA に従属する CA 証明書が ASA にインストールされていない場合、フェーズ 1 の IKE 交換中にその CA 証明書が提供されたときに、それを受け入れるかどうかを指定します。
- **auto-enroll**：CMPv2 自動更新の使用/不使用、トリガーのタイミング、および新しいキーペアの生成/不生成をパラメータで設定します。ライフタイムの後に自動登録を要求する、証明書の絶対ライフタイムの割合を入力します。次に、証明書を更新する際に新しいキーを生成するかどうかを指定します：**[no] auto-enroll [<percent>] [regenerate]**
- **crl required | optional | nocheck**：CRL コンフィギュレーション オプションを指定します。ASA 9.13(1) で削除されました。
- **crl configure**：crl コンフィギュレーション モードを開始します（**crl** コマンドを参照）。
- **default enrollment**：すべての登録パラメータをシステム デフォルト値に戻します。このコマンドの呼び出しは、アクティブなコンフィギュレーションには含まれません。
- **email** *address*：登録中に、指定した電子メール アドレスを証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **enrollment protocol cmp|scep** *url*：このトラストポイントに登録する CMP または SCEP 登録を指定し、登録 URL（*url*）を設定します。
- **enrollment retry period**：SCEP 登録の再試行期間を分単位で指定します。
- **enrollment retry count**：SCEP 登録に許可する最大試行回数を指定します。
- **enrollment terminal**：このトラストポイントへのカット アンド ペースト登録を指定します。
- **enrollment self**：自己署名証明書を生成する登録を指定します。
- **enrollment url**：このトラストポイントに登録する SCEP 登録を指定し、登録 URL（*url*）を設定します。
- **exit**：コンフィギュレーション モードを終了します。
- **fqdn** *fqdn*：登録中に、指定した FQDN を証明書のサブジェクト代替名の拡張に含めるかどうかを CA に確認します。
- **id-cert-issuer**：廃止されました。このトラストポイントに関連付けられた CA によって発行されるピア証明書をシステムが受け入れるかどうかを指定します。
- **id-usage**：トラストポイントの登録済み ID の使用方法を指定します。
- **ip-addr** *ip-address*：登録中に、ASA の IP アドレスを証明書に含めるかどうかを CA に確認します。
- **keypair** *name*：公開キーが証明対象となるキー ペアを指定します。
- keypair [<name>]：RSA または ECDSA のいずれかとして、公開キーを認証するキーペアと、そのモジュラス ビットまたは楕円曲線ビットを指定します。
- **match certificate** *map-name* **override ocsp | override cdp**：証明書マップを OCSP 上書きルールまたは CDP 上書きルールと照合します。

- **ocsp disable-nonce**：ナンス拡張子をディセーブルにします。ナンス拡張子は、失効要求と応答を結び付けて暗号化して、リプレイ アタックを回避するためのものです。
- **ocsp url**：この URL の OCSP サーバで、トラストポイントに関連するすべての証明書の失効ステータスをチェックすることを指定します。
- **exit**：コンフィギュレーション モードを終了します。
- **password** *string*：登録中に CA に登録されるチャレンジ フレーズを指定します。通常、CA はこのフレーズを使用して、その後の失効要求を認証します。
- **revocation check**：失効をチェックする方法（CRL、OCSP、なし）を指定します。
- **serial-number**：登録時に、ASA のシリアル番号を証明書に含めるように CA に要求します。
- **subject-name** *X.500 name*：登録中に、指定したサブジェクト DN を証明書に含めるかどうかを CA に確認します。DN ストリングにカンマが含まれる場合、値のストリングを二重引用符で囲みます（たとえば、O="Company, Inc."）。
- **support-user-cert-validation**：廃止されました。イネーブルの場合、リモート証明書を発行した CA に対してトラストポイントが認証されていれば、リモート ユーザ証明書を検証するコンフィギュレーション設定をこのトラストポイントから取得できます。このオプションは、サブコマンド **crl required | optional | nocheck** および CRL モードのすべての設定に関連付けられたコンフィギュレーション データに適用されます。
- **validation-policy**：ユーザ接続に関連付けられている証明書を検証するためのトラストポイントの条件を指定します。

（注） 接続しようとすると、トラストポイントからの ID 証明書の取得の試行時にそのトラストポイントに ID 証明書が含まれていないことを示す警告が表示されます。

例

次に、central という名前のトラストポイントを管理するために CA トラストポイント コンフィギュレーション モードを開始する例を示します。

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

関連コマンド

コマンド	説明
clear configure crypto ca trustpoint	すべてのトラストポイントを削除します。
crypto ca aunticate	このトラストポイントの CA 証明書を取得します。
crypto ca certificate map	クリプト CA 証明書マップ コンフィギュレーション モードを開始します。証明書ベースの ACL を定義します。
crypto ca crl request	指定されたトラストポイントのコンフィギュレーション パラメータに基づいて CRL を要求します。
crypto ca import	手動登録要求への応答として CA から受信した証明書をインストールします。

crypto ca trustpool export

PKI trustpool を構成する証明書をエクスポートするには、特権 EXEC コンフィギュレーション モードで **crypto ca trustpool export** コマンドを使用します。

crypto ca trustpool export *filename*

構文の説明

filename	エクスポートされた trustpool 証明書を保存するファイル。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

このコマンドは、アクティブな trustpool の内容全体を、指定されたファイルパスに pem コード形式でコピーします。

例

```
ciscoasa# crypto ca trustpool export disk0:/exportfile.pem
Trustpool certificates exported to disk0:/exportfile.pem
ciscoasa#
ciscoasa# more exportfile.pem
-----BEGIN CERTIFICATE-----
MIIEMjCCAxqgAwIBAgIBATANBgkqhkiG9w0BAQUFADB7MQswCQYDVQQGEwJHQjEb
MBkGA1UECAwSR3JlYXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHDAdTYWxmb3JkMRow
GAYDVQQKDBFDb21vZG8gQ0EgTGltaXRlZDEhMB8GA1UEAwwYQUFBIENlcnRpZmlj
YXRlIFNlcnZpY2VzMB4XDTA0MDEwMTAwMDAwMFoXDTI4MTIzMTIzNTk1OVowezEL
MAkGA1UEBhMCR0IxGzAZBgNVBAgMEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4GA1UE

<More>
```

関連コマンド

コマンド	説明
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。

crypto ca trustpool import

PKI trustpool を構成する証明書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 **crypto ca trustpool import** コマンドを使用します。

crypto ca trustpool import [clean] url *url* [**noconfirm** [**signature-required**]]

構文の説明

clean	インポート前にダウンロードされたすべての trustpool 証明書を削除します。
noconfirm	すべてのインタラクティブ プロンプトを抑制します。
signature-required	署名されたファイルのみを受け入れることを指定します。
url	インポートする trustpool ファイルの場所。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
9.0(1)	このコマンドが追加されました。
9.12(1)	ASA のデフォルトの信頼できる CA リストを使用するオプションが削除されました。

使用上のガイドライン

このコマンドを使用すると、trustpool バンドルを cisco.com からダウンロードするときに、ファイルのシグネチャを検証できます。バンドルを他のソースからダウンロードする場合や、シグネチャをサポートしていない形式でダウンロードする場合は、有効なシグネチャは必須ではありません。ユーザにはシグネチャのステータスが通知され、バンドルを受け入れるかどうかを選択できます。

表示される可能性のあるインタラクティブな警告は、次のとおりです。

- 無効なシグネチャを持つシスコ バンドル形式
- シスコ以外のバンドル形式
- 有効なシグネチャを持つシスコ バンドル形式

signature-required キーワードは、**noconfirm** オプションを選択した場合にだけ使用できます。**signature-required** キーワードが含まれている場合に、シグネチャが存在しないか確認できないと、インポートが失敗します。

(注) ファイルのシグネチャを確認できない場合は、その他の方法によって正規のファイルであることを確認していない限り、証明書をインストールしないでください。

次に、インタラクティブ プロンプトを抑制し、シグネチャを要求する場合の **crypto ca trustpool import** コマンドの動作の例を示します。

```
ciscoasa(config)# crypto ca trustpool import url ?

configure mode commands/options:
disk0: Import from disk0: file system
disk1: Import from disk1: file system
flash: Import from flash: file system
ftp: Import from ftp: file system
http: Import from http: file system
https: Import from https: file system
smb: Import from smb: file system
system: Import from system: file system
tftp: Import from tftp: file system

ciscoasa(config)# crypto ca trustpool import url http://mycompany.com ?
exec mode commands/options:
noconfirm Specify this keyword to suppress all interactive prompting.

ciscoasa(config)# crypto ca trustpool import url http://mycompany.com noconfirm ?
exec mode commands/options:
signature-required Indicate that only signed files will be accepted
```

関連コマンド

コマンド	説明
crypto ca trustpool export	PKI trustpool を構成する証明書をエクスポートします。

crypto ca trustpool policy

trustpool ポリシーを定義するコマンドを提供するサブモードを開始するには、グローバル コンフィギュレーション モードで **crypto ca trustpool policy** コマンドを使用します。trustpool 証明書バンドルの自動インポートを設定するには、バンドルをダウンロードしてインポートするために ASA が使用する URL を指定します。

crypto ca trustpool policy

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。

auto-import	trustpool 証明書の自動インポートを設定します。
auto-import [time <H:M:S>] [url <URL address>]	オフピーク時などの便利な時間帯にダウンロードをスケジュールする必要がある場合は、trustpool に証明書をダウンロードする時間と URL を設定します。
auto-import time	ダウンロード時刻を、時、分、秒で指定します。24 時間ごとに指定した時刻にダウンロードが試行されます。指定しない場合は、デフォルト時刻の 22:00 が使用されます。
auto-import url	trustpool 証明書の自動インポートを指定します。指定しない場合は、デフォルトのシスコ URL が使用されます。

デフォルト

デフォルトの動作や値はありません。

自動インポート オブジェクトは、デフォルトでオフになっています。

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	—	—
オブジェクト コンフィギュレーション	• 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。
9.5(2)	auto-import コマンド オプションが追加されました。

例

```
ciscoasa(config)# crypto ca trustpool ?

configure mode commands/options:
policy Define trustpool policy

ciscoasa(config)# crypto ca trustpool policy
ciscoasa(config-ca-trustpool)# ?

CA Trustpool configuration commands:
crl               CRL options
exit              Exit from certificate authority trustpool entry mode
match             Match a certificate map
no                Negate a command or set its defaults
revocation-check  Revocation checking options

auto-import Configure automatic import of trustpool certificates
ciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import?

crypto-ca-trustpool mode commands/options:

time Specify the auto import time in hours, minutes, and seconds
Default is 22:00:00. An attempt is made every 24 hours at the specified time.
url Specify the HTTP based URL address for automatic import of trustpool certificates

<cr>

ciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import url ?

crypto-ca-trustpool mode commands/options:
LINE  URL for automatic import
ciscoasa(config-ca-trustpool)#

ciscoasa(config-ca-trustpool)# auto-import time ?
H:M:S    Specify the auto import time in hours, minutes & seconds. E.g. 18:00:00 (attempt
to import is made at every 24 hours at 6PM)
ciscoasa(config-ca-trustpool)#
```

関連コマンド

コマンド	説明
show crypto ca trustpool policy	設定された trustpool ポリシーを表示します。

crypto ca trustpool remove

PKI trustpool から 1 つの指定された証明書を削除するには、特権 EXEC コンフィギュレーション モードで **crypto ca trustpool remove** コマンドを使用します。

crypto ca trustpool remove *cert fingerprint* **[noconfirm]**

構文の説明

cert fingerprint	16 進データ。
noconfirm	すべてのインタラクティブ プロンプトを抑制するには、このキーワードを指定します。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

このコマンドは信頼できるルート証明書の内容に対する変更をコミットするため、インタラクティブなユーザはアクションを確認することを求められます。

例

```
ciscoasa# crypto ca trustpool remove ?

  Hex-data Certificate fingerprint
ciscoasa# crypto ca trustpool remove 497904b0eb8719ac47b0bc11519b74d0 ?
noconfirm Specify this keyword to suppress all interactive prompting.
```

関連コマンド

コマンド	説明
clear crypto ca trustpool	trustpool からすべての証明書を削除します。
crypto ca trustpool export	PKI trustpool を構成する証明書をエクスポートします。
crypto ca trustpool import	PKI trustpool を構成する証明書をインポートします。

crypto dynamic-map match address

アクセス リストのアドレスをダイナミック クリプト マップ エントリに一致させるには、グローバル コンフィギュレーション モードで **crypto dynamic-map match address** コマンドを使用します。アドレス一致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 dynamic-map *dynamic-map-name dynamic-seq-num* **match address** *acl_name*

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

構文の説明

acl-name	ダイナミック クリプト マップ エントリを照合するアクセス リストを指定します。
dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック 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。

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)	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

このコマンドの詳細については、**crypto map match address** コマンドを参照してください。

例

次に、**crypto dynamic-map** コマンドを使用して、aclist1 という名前のアクセス リストのアドレスに一致させる例を示します。

```
ciscoasa(config)# crypto dynamic-map mymap 10 match address aclist1
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 dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

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

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

構文の説明

name	ダイナミック クリプト マップ セットの名前を指定します。
priority	ダイナミック 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 dynamic-map set ikev1 transform-set

ダイナミック 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 dynamic-map set ikev1 transform-set** コマンドを使用します。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*… transform-set-name11*]

ダイナミック クリプト マップ エントリからトランスフォーム セットを削除するには、このコマンドの **no** 形式でトランスフォーム セット名を指定します。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set** *transform-set-name1* [*… transform-set-name*11]

ダイナミック 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、トランスフォーム セットすべて指定するか何も指定ません。

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set ikev1 transform-set**

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック 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 セットはすべて、**crypto ipsec ikev1 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。
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。
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。

使用上のガイドライン

ダイナミック クリプト マップは、いずれのパラメータも設定されていないクリプト マップです。ダイナミック クリプト マップは、不足しているパラメータが、ピアの要件に合うように後でダイナミックに取得される（IPsec ネゴシエーションの結果として）ポリシー テンプレートの役割を果たします。ASA は、スタティック クリプト マップでピアの IP アドレスがまだ指定されていない場合、ピアでトンネルをネゴシエートさせるためにダイナミック クリプト マップを適用します。これは、次のタイプのピアで発生します。

- パブリック IP アドレスがダイナミックに割り当てられるピア。

  LAN-to-LAN のピア、およびリモート アクセスするピアは、両方とも DHCP を使用してパブリック IP アドレスを取得できます。ASA は、トンネルを開始するときだけこのアドレスを使用します。

- プライベート IP アドレスがダイナミックに割り当てられるピア。

  通常、リモート アクセスのトンネルを要求するピアは、ヘッドエンドによって割り当てられたプライベート IP アドレスを持っています一般に、LAN-to-LAN トンネルには事前に決定されたプライベート ネットワークのセットがあります。これがスタティック マップの設定に使用されるので、結果として IPsec SA の確立にも使用されます。

管理者がスタティック クリプト マップを設定するため、（DHCP または別の方法で）ダイナミックに割り当てられた IP アドレスがわからない場合や、割り当て方法には関係なく他のクライアントのプライベート IP アドレスがわからない場合があります。通常、VPN クライアントには、スタティック IP アドレスがなく、IPsec ネゴシエーションを発生させるためのダイナミック クリプト マップが必要です。たとえば、ヘッドエンドは IKE ネゴシエーション中に IP アドレスを Cisco VPN Client に割り当て、クライアントはこのアドレスを使用して IPsec SA をネゴシエートします。

ダイナミック クリプト マップは、IPsec コンフィギュレーションを容易にするので、ピアが必ずしも事前設定されていないネットワークで使用するのに適しています。ダイナミック クリプト マップは、Cisco VPN Client（モバイル ユーザなど）、およびダイナミックに割り当てられた IP アドレスを取得するルータに対して使用してください。

ヒント ダイナミック クリプト マップの **permit** エントリに **any** キーワードを使用する場合は、注意が必要です。このような **permit** エントリの対象となるトラフィックにマルチキャストやブロードキャストのトラフィックが含まれる場合、該当するアドレス範囲について **deny** エントリをアクセス リストに挿入します。ネットワークとサブネット ブロードキャスト トラフィックに対して、また IPsec で保護しないその他のトラフィックに対しては、必ず **deny** エントリを挿入してください。

ダイナミック クリプト マップは、接続を開始したリモートのピアと SA をネゴシエートするときだけ機能します。ASA は、ダイナミック クリプト マップを使用してリモート ピアとの接続を開始することはできません。ダイナミック クリプト マップを設定した場合は、発信トラフィックがアクセス リストの permit エントリに一致する場合でも、対応する SA が存在しないと、ASA はそのトラフィックをドロップします。

クリプト マップ セットには、ダイナミック クリプト マップを含めることができます。ダイナミック暗号マップのセットには、暗号マップ セットで一番低いプライオリティ（つまり、一番大きいシーケンス番号）を設定し、ASA が他の暗号マップを先に評価するようにする必要があります。セキュリティ アプライアンスは、他の（スタティック）マップのエントリが一致しない場合にだけ、ダイナミック クリプト マップのセットを調べます。

スタティック クリプト マップ セットと同様に、ダイナミック クリプト マップ セットにも、同じダイナミック マップ名を持つすべてのダイナミック クリプト マップを含めます。ダイナミック シーケンス番号によって、セット内のダイナミック クリプト マップが区別されます。ダイナミック クリプト マップを設定する場合は、IPsec ピアのデータ フローを暗号アクセス リストで識別するために、ACL の許可を挿入します。このように設定しないと、ASA は、ピアが提示するあらゆるデータ フロー ID を受け入れることになります。

注意 ダイナミック クリプト マップ セットを使用して設定された ASA インターフェイスにトンネリングされるトラフィックに対してスタティック（デフォルト）ルートを割り当てないでください。トンネリングされるトラフィックを指定するには、ダイナミック クリプト マップに ACL を追加します。リモート アクセス トンネルに関連付けられた ACL を設定する場合は、適切なアドレス プールを指定してください。逆ルート注入を使用してルートをインストールするのは、必ずトンネルがアップ状態になった後にしてください。

1 つのクリプト マップ セット内で、スタティック マップ エントリとダイナミック マップ エントリを組み合わせることができます。

例

次に、10 個の同じトランスフォーム セットで構成された「dynamic0」というダイナミック 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 dynamic-map dynamic0 1 set ikev1 transform-set 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
crypto ipsec ikev1 transform-set	IKEv1 トランスフォーム セットを設定します。
crypto map set transform-set	クリプト マップ エントリで使用するトランスフォーム セットを指定します。
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。
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 dynamic-map set ikev2 ipsec-proposal

ダイナミック クリプト マップ エントリで使用する IKEv2 の IPsec 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 dynamic-map set ikev2 ipsec-proposal** コマンドを使用します。ダイナミック クリプト マップ エントリからトランスフォーム セットの名前を削除するには、このコマンドの **no** 形式を使用します。

crypto dynamic-map *dynamic-map-name* **set ikev2 ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

no crypto dynamic-map *dynamic-map-name* **set ikev2 ipsec-proposal** *transform-set-name1* [*… transform-set-name11*]

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
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 ikev2 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。

crypto dynamic-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 dynamic-map set nat-t-disable** コマンドを使用します。この暗号マップ 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 dynamic-map *dynamic-map-name dynamic-seq-num* **set nat-t-disable**

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

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック 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
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。次に、**crypto dynamic-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 をディセーブルにします。

例

次のコマンドでは、mymap という名前のダイナミック クリプト マップの NAT-T をディセーブルにします。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set nat-t-disable
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 dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set peer

このコマンドの詳細については、**crypto map set peer** コマンドを参照してください。

crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set peer** *ip_address* | *hostname*

構文の説明

dynamic-map-name	ダイナミック クリプト マップ セットの名前を指定します。
dynamic-seq-num	ダイナミック 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。
hostname	**name** コマンドで定義されているように、ダイナミック クリプト マップ エントリのピアをホスト名で指定します。
ip_address	**name** コマンドで定義されているように、ダイナミック クリプト マップ エントリのピアを IP アドレスで指定します。

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
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。

例

次に、IP アドレス 10.0.0.1 を、mymap という名前のダイナミック マップのピアとして設定する例を示します。

```
ciscoasa(config)# crypto dynamic-map mymap 10 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 dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set pfs

ダイナミック 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 dynamic-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 dynamic-map *map-name map-index* **set pfs** [**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

no crypto dynamic-map *map-name map-index* **set pfs**[**group1 | group2 | group5 | group14 | group19 | group20 | group21 | group24**]

構文の説明

group14	使用する Diffie-Hellman キー交換グループを指定します。
group15	使用する Diffie-Hellman キー交換グループを指定します。
group16	使用する Diffie-Hellman キー交換グループを指定します。
group19	使用する Diffie-Hellman キー交換グループを指定します。
group20	使用する Diffie-Hellman キー交換グループを指定します。
group21	使用する Diffie-Hellman キー交換グループを指定します。
group24	使用する Diffie-Hellman キー交換グループを指定します。
map-name	クリプト マップ セットの名前を指定します。
map-index	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。

リリース	変更内容
9.13(1)	**group14**、**15**、および **16** コマンドオプションが追加されました。**group 1**、**2**、および **group 5** コマンドは廃止され、以降のリリースで削除されます。
9.15(1)	**グループ 1**、**2**、**5**、および **24** のコマンドオプションは、このリリースでサポートが廃止されました。

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。

crypto dynamic-map コマンド（**match address**、**set peer**、**set pfs** など）については、**crypto map** コマンドの項で説明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 PFS が指定されていない場合は、ピアからの PFS のオファーがすべて受け入れられます。

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、ダイナミック 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 を使用するよう指定する例を示します。指定されているグループはグループ 2 です。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2
```

次に、group14 のサポートを指定する例を示します。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs groyp14
ciscoasa(config)# crypto dynamic-map mymap 10 set pfs group2 (DEPRECATED)
```

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 dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set reverse route

このコマンドの詳細については、**crypto map set reverse-route** コマンドを参照してください。

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

no crypto dynamic-map *dynamic-map-name dynamic-seq-num* **set reverse route**

構文の説明

dynamic-map-name	クリプト マップ セットの名前を指定します。
dynamic-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値はオフです。

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
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。

例

次のコマンドでは、mymap という名前のダイナミック クリプト マップの逆ルート注入をイネーブルにします。

```
ciscoasa(config)# crypto dynamic-map mymap 10 set reverse route
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 dynamic-map	すべてのダイナミック クリプト マップのすべてのコンフィギュレーションを表示します。

crypto dynamic-map set security-association lifetime

特定のダイナミック暗号マップ 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 dynamic-map set security-association lifetime** コマンドを使用します。ダイナミック暗号マップ 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 dynamic-map *map-name seq-num* **set security-association lifetime** {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

no crypto dynamic-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

ダイナミック暗号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 dynamic-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

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コマンドでは、ダイナミック暗号のダイナミック 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 dynamic-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 dynamic-map	すべての暗号ダイナミック 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 dynamic-map	暗号ダイナミック マップの設定を表示します。

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

no crypto dynamic-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 dynamic-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を宛先とする着信 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 dynamic-map set validate-icmp-errors** コマンドを使用します。ダイナミック クリプト マップ エントリから着信 ICMP エラー メッセージの検証を削除するには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

name	ダイナミック クリプト マップ セットの名前を指定します。
priority	ダイナミック 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。

crypto engine accelerator-bias

Symmetric Multi-Processing（SMP）プラットフォームで暗号化コアの割り当てを変更するには、グローバル コンフィギュレーション モードで **crypto engine accelerator-bias** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]

no crypto engine accelerator-bias [**balanced** | **ipsec** | **ssl**]

構文の説明

balanced	暗号化ハードウェア リソースを均等に分散します（Admin/SSL および IPsec コア）。
ipsec -client	暗号化ハードウェア リソースを好きな IPsec コアに割り当てます（SRTP 暗号化音声トラフィックを含む）。
ssl-client	暗号化ハードウェア リソースを好きな Admin/SSL コアに割り当てます。

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	• 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

暗号化コアの再分散は、プラットフォーム ASA 5585、5580、5545/5555、ASASM、FP4110、FP4120、FP4140、FP4150、FP9300、SM-24、SM-36、および SM-44 で可能です。

このコマンドを実行すると、暗号化操作を必要とするサービスへのトラフィックが中断されます。このコマンドは、IPsec の障害が設定されていない状態で、メンテナンス期間中に適用する必要があります。

例

次に、crypto engine acccelerator-bias コマンドの設定に使用可能なオプションの例を示します。

```
ciscoasa (config)# crypto engine ?

configure mode commands/options:
accelerator-bias
Specify how to allocate crypto accelerator processors
```

```
ciscoasa (config)# crypto engine accelerator-bias ?
configure mode commands/options
balanced - Equally distribute crypto hardware resources
ipsec-client - Allocate crypto hardware resources to favor IPsec/Encrypted Voice (SRTP)
ssl-client - Allocate crypto hardware resources to favor SSL

ciscoasa (config)# crypto engine accelerator-bias ssl
```

crypto engine large-mod-accel

ラージ モジュラス演算を ASA 5510、5520、5540、または 5550 でソフトウェアからハードウェアに切り替えるには、グローバル コンフィギュレーション モードで **crypto engine large-mod-accel** コマンドを使用します。このコマンドをコンフィギュレーションから削除するには、このコマンドの **no** 形式を使用します。

crypto engine large-mod-accel

no crypto engine large-mod-accel

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 は、ソフトウェアでラージ モジュラス演算を実行します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
8.3(2)	このコマンドが追加されました。
9.0(1)	マルチ コンテキスト モードのサポートが追加されました。

使用上のガイドライン

このコマンドは、ASA モデル 5510、5520、5540、および 5550 だけで使用可能です。大きなモジュラスの演算をソフトウェアからハードウェアに切り替えます。ハードウェアへの切り替えによって、次のことが高速化されます。

- 2048 ビット RSA 公開キー証明書の処理。
- Diffie Hellman グループ 5（DH5）キーの生成。

このコマンドは、1 秒あたりの接続を向上する必要がある場合に使用することを推奨します。負荷によっては、SSL スループットに限定的なパフォーマンス上の影響がある場合があります。

また、ソフトウェアからハードウェア、またはハードウェアからソフトウェアへの処理の移行時に発生する可能性がある一時的なパケット損失を最小限に抑えるために、使用率が低いとき、またはメンテナンス期間に（いずれかの形式の）このコマンドを使用することを推奨します。

（注） ASA 5580/5500-X プラットフォームには、ラージ モジュラス演算を切り替える機能がすでに統合されています。したがって、**crypto engine** コマンドは、これらのプラットフォームには適用されません。

例

次に、大きなモジュラスの演算をソフトウェアからハードウェアに切り替える例を示します。

```
ciscoasa(config)# crypto engine large-mod-accel
```

次に、前のコマンドをコンフィギュレーションから削除し、大きなモジュラスの演算をソフトウェアに切り替えて戻す例を示します。

```
ciscoasa(config)# no crypto engine large-mod-accel
```

関連コマンド

コマンド	説明
show running-config crypto engine	ラージ モジュラス演算がハードウェアに切り替えられているかどうかを示します。
clear configure crypto engine	ラージ モジュラス演算をソフトウェアに戻します。このコマンドは、**no crypto engine large-mod-accel** コマンドと同等です。

crypto ikev1 enable

IPsec ピアが ASA と通信するインターフェイス上で ISAKMP IKEv1 ネゴシエーション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 ikev1 enable** コマンドを使用します。ISAKMP IKEv1 をインターフェイスで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 ikev1 enable *interface-name*

no crypto ikev1 enable *interface-name*

構文の説明

interface-name	ISAKMP IKEv1 ネゴシエーションをイネーブルまたはディセーブルにするインターフェイ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	—

コマンド履歴

リリース	変更内容
7.0(1)	この **isakmp enable** コマンドが追加されました。
7.2(1)	**isakmp enable** コマンドが、**crypto isakmp enable** コマンドに置き換えられました。
8.4(1)	IKEv2 機能が追加されたことにより、**crypto isakmp enable** コマンドが **crypto ikev1 enable** コマンドに変更されました。
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。

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、内部インターフェイス上で ISAKMP をディセーブルにする方法を示しています。

```
ciscoasa(config)# no crypto isakmp enable inside
```

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 ikev1 ipsec-over-tcp

IPsec over TCP 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 ikev1 ipsec-over-tcp** コマンドを使用します。IPsec over TCP 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 ikev1 ipsec-over-tcp [**port** *port1...port10*]

no crypto ikev1 ipsec-over-tcp [**port** *port1...port10*]

構文の説明

port *port1...port10*	(オプション)デバイスが IPsec over TCP 接続を受け入れるポートを指定します。最大 10 のポートを指定できます。ポート番号には 1 ～ 65535 の範囲の数値を指定できます。デフォルトのポート番号は 10000 です。

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		—

コマンド履歴

リリース	変更内容
7.0(1)	**isakmp ipsec-over-tcp** コマンドが追加されました。
7.2.(1)	**isakmp ipsec-over-tcp** コマンドが、**crypto isakmp ipsec-over-tcp** コマンドに置き換えられました。
8.4(1)	コマンド名が **crypto isakmp ipsec-over-tcp** から **crypto ikev1 ipsec-over-tcp** に変更されました。

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、IPsec over TCP をポート 45 でイネーブルにします。

```
ciscoasa(config)# crypto ikev1 ipsec-over-tcp port 45
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 ikev1 limit max-in-negotiation-sa

ASA の IKEv1 ネゴシエーション中（オープン）SA の数を制限するには、グローバル コンフィギュレーション モードで **crypto ikev1 limit max-in-negotiation-sa** コマンドを使用します。オープン SA の数の制限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 ikev1 limit max-in-negotiation-sa *threshold percentage*

no crypto ikev1 limit max-in-negotiation-sa *threshold percentage*

構文の説明

threshold percentage	ASA に対して許容される合計 SA のうち、ネゴシエーション中（オープン）であることが許容されるもののパーセンテージ。しきい値に達すると、追加の接続が拒否されます。範囲は 1 ～ 100 % です。ASA5506/ASA5508（100 %）を除くすべての ASA プラットフォームのデフォルトは 20 % です。

デフォルト

デフォルトは 20 % です。ASA は、ASA5506/ASA5508 を除くオープン SA の数を 20 % に制限します。

使用上のガイドライン

crypto ikev1 limit-max-in-negotiation-sa コマンドは、任意の時点においてネゴシエーション中であることが可能な SA の最大数を制限します。1

crypto ikev1 limit max in-negotiation-sa コマンドは、現在の接続を保護し、クッキー チャレンジ機能が阻止できない可能性があるメモリや CPU の攻撃を防ぐために、以降の接続のネゴシエーションを停止します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
9.1(2)	このコマンドが追加されました。

例

次に、ネゴシエーション中の IKEv1 接続の数を、許容される最大 IKEv1 接続の 70 % に制限する例を示します。

```
ciscoasa(config)# crypto ikev1 limit max in-negotiation-sa 70
```

関連コマンド

コマンド	説明
crypto ikev1 limit max-sa	ASA での IKEv1 接続数を制限します。
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 ikev1 policy

IPsec 接続の IKEv1 セキュリティ アソシエーション（SA）を作成するには、グローバル コンフィギュレーション モードで **crypto ikev2 policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

crypto ikev1 policy *priority*

no crypto ikev1 policy *priority*

構文の説明

priority	ポリシー スイートのプライオリティ。指定できる範囲は 1 ～ 65535 です。1 は最高のプライオリティを、65535 は最低のプライオリティを示します。

デフォルト

デフォルトの動作や値はありません。

使用上のガイドライン

このコマンドは IKEv1 ポリシー コンフィギュレーション モードを開始します。このモードで追加の IKEv1 SA 設定を指定します。IKEv1 SA は、IKEv1 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev1 policy** コマンドを入力した後、追加のコマンドを使用して、SA 暗号化アルゴリズム、DH グループ、整合性アルゴリズム、ライフタイム、ハッシュ アルゴリズムを設定できます。

3DES 暗号化方式は廃止されているため、新しく作成された IKE ポリシーと IPsec プロポーザルのデフォルトの暗号化方式は AES-128 になります。これは、新しいポリシーとプロポーザルのみに適用され、既存の設定項目には影響しません。

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。

リリース	変更内容
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。**groups 1、2**、および **group 5** オプションは、安全でないと見なされます。これら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。 • いくつかの整合性および PRF 暗号方式使用する ASA/Lina IKE、IPsec、および SSH モジュールは、安全ではないと見なされます。次の暗号方式は廃止され、以降のリリースで削除されます。 – HMAC-MD5 整合性と PRF 暗号方式 – IPsec での HMAC-MD5 整合性暗号 – HMAC-MD5、HMAC-MD5-96、および HMAC-SHA1-96 整合性暗号 – AES-GMAC、3DES、DES
9.15(1)	• **DH グループ 1、2**、および **5** のオプションは安全でないと見なされ、サポートが廃止されました。 • ASA/Lina IKE、IPsec、および SSH で使用される次の整合性および PRF 暗号は安全でないと見なされ、IKEv1 ポリシー設定から削除されました。 – HMAC-MD5 整合性と PRF 暗号方式 – IPsec での HMAC-MD5 整合性暗号 – HMAC-MD5、HMAC-MD5-96、および HMAC-SHA1-96 整合性暗号 – AES-GMAC、3DES、DES

例

次に、プライオリティ 1 の IKEv1 SA を作成し、IKEv1 ポリシー 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)# crypto ikev1 policy 1
ciscoasa(config-ikev1-policy)# authentication rsa-sig
ciscoasa(config-ikev1-policy)# hash md5
ciscoasa(config-ikev1-policy)# group 14
ciscoasa(config-ikev1-policy)# lifetime 300
```

関連コマンド

コマンド	説明
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
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 ikev2 cookie-challenge

SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信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 ikev2 cookie-challenge** コマンドを使用します。クッキー チャレンジ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 ikev2 cookie-challenge *threshold percentage* | **always** | **never**

no crypto ikev2 cookie-challenge *threshold percentage* | **always** | **never**

構文の説明

threshold percentage	ASA に対して許容される合計 SA のうち、以降の SA ネゴシエーションに対してクッキー チャレンジをトリガーする、ネゴシエーション中のもののパーセンテージ。範囲は 0 ～ 99 % です。デフォルト値は 50 % です。
always	着信 SA に対して常にクッキー チャレンジを行います。
never	着信 SA に対してクッキー チャレンジを行いません。

デフォルト

デフォルトの動作や値はありません。

使用上のガイドライン

ピアに対してクッキー チャレンジを行うことによって、サービス妨害（DoS）攻撃を防止できます。攻撃者は、ピア デバイスが SA によって開始されたパケットを送信し、ASA がその応答を送信しても、ピア デバイスがそれに応答しない場合、DoS 攻撃を開始します。ピア デバイスがこれを継続的に行うと、許可されている数の SA 要求が使い果たされてしまい、最終的に ASA が応答を停止してしまうことがあります。

crypto ikev2 cookie-challenge コマンドを使用してしきい値パーセンテージをイネーブルにすると、オープン SA ネゴシエーションの数を制限できます。たとえば、デフォルト設定の 50% では、許可される SA の 50 % がネゴシエーション中（オープン）のときに、ASA は、それ以降到着した SA 初期パケットに対してクッキー チャレンジを行います。10,000 個の IKEv2 SA が許可される Cisco ASA 5580 では、5000 個の SA がオープンになると、それ以降の着信 SA に対してクッキー チャレンジが行われます。

crypto kev2 limit max in-negotiation-sa コマンドとともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値を最大ネゴシエーション中のしきい値よりも低く設定してください。

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
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

次の例では、クッキー チャレンジのしきい値が 30 % に設定されます。

```
ciscoasa(config)# crypto ikev2 cookie-challenge 30
```

関連コマンド

コマンド	説明
crypto ikev2 limit max-sa	ASA での IKEv2 接続数を制限します。
crypto ikev2 limit max-in-negotiation-sa	ASA での IKEv2 ネゴシエーション中（オープン）SA の数を制限します。
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 ikev2 enable

IPsec ピアが ASA と通信するインターフェイス上で ISAKMP IKEv2 ネゴシエーション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 ikev2 enable** コマンドを使用します。ISAKMP IKEv2 をインターフェイスで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 ikev2 enable *interface-name* [**client-services** [**port** *port*]]

no crypto ikev2 enable *interface-name* [**client-services** [**port** *port*]]

構文の説明

interface-name	ISAKMP IKEv2 ネゴシエーションをイネーブルまたはディセーブルにするインターフェイスの名前を指定します。
client-services	インターフェイスで IKEv2 接続に対してクライアント サービスをイネーブルにします。クライアント サービスには、ソフトウェア アップデート、クライアント プロファイル、GUI のローカリゼーション（翻訳）とカスタマイゼーション、Cisco Secure Desktop、SCEP プロキシなどの拡張 Anyconnect セキュア モビリティ クライアント機能が含まれています。クライアント サービスをディセーブルにしても、AnyConnect クライアントでは IKEv2 との基本的な IPsec 接続が確立されます。
port *port*	IKEv2 接続に対してクライアント サービスをイネーブルにするポートを指定します。範囲は 1 ～ 65535 です。デフォルトはポート 443 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	—

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。

使用上のガイドライン

このコマンドを単独で使用した場合、クライアント サービスはイネーブルになりません。

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、outside インターフェイス上で IKEv2 をイネーブルにする方法を示しています。

```
ciscoasa(config)# crypto ikev2 enable outside client-services port 443
```

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 ikev2 fragmentation

IKEv2 のフラグメンテーション設定を構成するには、グローバル コンフィギュレーション モードで **crypto ikev2 fragmentation** コマンドを使用します。

[no] **crypto ikev2 fragmentation** [**mtu** *mtu-size*] | [**preferred-method** [**ietf** | **cisco**]]

no crypto ikev2 fragmentation [**mtu** *mtu-size*] | [**preferred-method** [**ietf** | **cisco**]]

構文の説明

mtu-size	MTU サイズ（68 ～ 1500）。使用する MTU 値には、IPv4/IPv6 ヘッダー + UDP ヘッダーのサイズを含める必要があります。 値を指定すると、IPv4 と IPv6 の両方で同じ値が使用されます。
preferred-method	推奨フラグメンテーション方法：RFC-7383 標準ベースの方法（**ietf**）またはシスコ独自の方法（**cisco**）です。

デフォルト

デフォルトでは、両方の IKEv2 フラグメンテーション方法がイネーブルにされており、MTU は 576（IPv4）または 1280（IPv6）であり、推奨方法は IETF 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
9.6(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

このコマンドを使用して、次を実行します。

- IKE パケットがフラグメンテーションを必要とするかどうかを決定するために使用する MTU を設定します。この値を超えたパケットはフラグメント化されます。
- 推奨フラグメンテーション方法を変更します。
- IKE フラグメンテーションをすべてディセーブルにします。

IETF RFC-7383 標準ベースの IKEv2 フラグメンテーション方法は、両方のピアがネゴシエーション中にサポートとプリファレンスを指定したときに使用されます。この方法を使用すると、暗号化はフラグメンテーション後に行われ、各 IKEv2 フラグメント メッセージが個別に保護されます。

シスコ独自のフラグメンテーションは、AnyConnect クライアントなどのピアがこの方法だけを提供する場合、または両方のピアがネゴシエーション中にサポートとプリファレンスを指定した場合に使用されます。この方式を使用すると、暗号化の後にフラグメンテーションが実行されます。受信側のピアは、すべてのフラグメントを受信するまで、メッセージを復号することも認証することもできません。

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、outside インターフェイス上で IKEv2 をイネーブルにする方法を示しています。

MTU 値を 600 に変更します。

```
ciscoasa(config)# crypto ikev2 fragmentation mtu 600
```

優先するフラグメンテーション方式をシスコ方式に変更する場合:

```
ciscoasa(config)# crypto ikev2 fragmentation preferred-method cisco
```

関連コマンド

コマンド	説明
show crypto ikev2 sa detail	MTU を表示します。
show running-config all crypto ikev2	設定を表示します。

crypto ikev2 limit max-in-negotiation-sa

ASA の IKEv2 ネゴシエーション中（オープン）SA の数を制限するには、グローバル コンフィギュレーション モードで **crypto ikev2 limit max in-negotiation-sa** コマンドを使用します。オープン SA の数の制限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 ikev2 limit max in-negotiation-sa *value*

no crypto ikev2 limit max in-negotiation-sa *value*

構文の説明

value	ASA に対して許容される合計 SA のうち、ネゴシエーション中（オープン）であることが許容されるものの数またはしきい値パーセンテージ。しきい値に達すると、追加の接続が拒否されます。範囲は 1 ～ 100 % です。デフォルトは 100 % です。

デフォルト

デフォルトではディセーブルになっています。ASA はオープン SA の数を制限しません。

使用上のガイドライン

crypto ikev2 limit-max-in-negotiation-sa コマンドは、任意の時点においてネゴシエーション中であることが可能な SA の最大数を制限します。**crypto ikev2 cookie-challenge** コマンドとともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこの制限よりも低く設定してください。

クッキーを使用して着信接続に対してチャレンジを行う **crypto ikev2 cookie-challenge** コマンドとは異なり、**crypto kev2 limit max in-negotiation-sa** コマンドは、現在の接続を保護し、クッキー チャレンジ機能が阻止できない可能性があるメモリや CPU の攻撃を防ぐために、以降の接続のネゴシエーションを停止します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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。
9.15(1)	ネゴシエーション中の SA の最大数を絶対値として 15000 まで、または最大デバイスキャパシティから得られる最大値を設定できるようになりました（以前はパーセンテージのみが許可されていました）。

例

次に、ネゴシエーション中の IKEv2 接続の数を、許容される最大 IKEv2 接続の 70% に制限する例を示します。

```
ciscoasa(config)# crypto ikev2 limit max in-negotiation-sa 70
```

関連コマンド

コマンド	説明
crypto ikev2 limit max-sa	ASA での IKEv2 接続数を制限します。
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
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 ikev2 limit max-sa

ASA での IKEv2 接続数を制限するには、グローバル コンフィギュレーション モードで **crypto ikev2 limit max-sa** コマンドを使用します。接続数の制限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 ikev2 limit max-sa *number*

no crypto ikev2 limit max-sa *number*

構文の説明

number	ASA で許可される IKEv2 接続数。制限に達すると、追加の接続が拒否されます。範囲は 1 ～ 10000 です。

デフォルト

デフォルトではディセーブルになっています。ASA は IKEv2 接続数を制限しません。許可される IKEv2 接続の最大数は、ライセンスで指定された接続の最大数になります。

使用上のガイドライン

crypto ikev2 limit max-sa コマンドは、ASA での SA の最大数を制限します。

crypto ikev2 cookie-challenge コマンドとともに使用する場合は、有効なクロス チェックが行われるように、クッキー チャレンジのしきい値をこの制限よりも低く設定してください。

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、IKEv2 接続数を 5000 に制限する例を示します。

```
ciscoasa(config)# crypto ikev2 limit max-sa 5000
```

関連コマンド

コマンド	説明
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
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 ikev2 notify

着信パケットが、SA のトラフィック セレクタと一致しない SA で受信された場合に IKE 通知のピアへの送信を管理者がイネーブルにできるようにするには、**crypto ikev2 notify** コマンドを使用します。この通知の送信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 ikev2 notify invalid-selectors

[no] crypto ikev2 notify invalid-selectors

構文の説明

invalid-selectors	パケットが SA に着信してもトラフィック セレクタと一致しない場合にピアに通知します。
notify	ピアに送信される IKEv2 通知をイネーブルまたはディセーブルにします。

デフォルト

デフォルトでは、この通知はディセーブルになっています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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
9.4(1)	このコマンドが追加されました。

例

```
100/act(config) # crypto ikev2 ?

configure mode commands/options:
    cookie-challenge   Enable and configure IKEv2 cookie challenges based on half-open SAs
    enable             Enable IKEv2 on the specified interface
    limit              Enable limits on IKEv2 SAs
    policy             Set IKEv2 policy suite
    redirect           Set IKEv2 redirect
    remote-access      Configure IKEv2 for Remote Access
    notify             Enable/Disable IKEv2 notifications to be sent to the peer

100/act(config)# crypto ikev2 notify ?

configure mode commands/options:
    invalid-selectors  Notify the peer if a packet is received on an SA but does not match
the traffic selectors
```

crypto ikev2 policy

AnyConnect IPsec 接続の IKEv2 セキュリティ アソシエーション(SA)を作成するには、グローバル コンフィギュレーション モードで **crypto ikev2 policy** コマンドを使用します。ポリシーを削除するには、このコマンドの **no** 形式を使用します。

crypto ikev2 policy *policy_index group <number>*

no crypto ikev2 policy *policy_index group <number>*

構文の説明

group <number>	このポリシーインデックスの Diffie-Hellman グループを 14、15、16、19、20、または 21 として指定します。
policy index	IKEv2 ポリシー コンフィギュレーション モードにアクセスし、ポリシー エントリの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。

使用上のガイドライン

IKEv2 SA は、IKEv2 ピアがフェーズ 2 で安全に通信できるようにするためにフェーズ 1 で使用されるキーです。**crypto ikev2 policy** コマンドを入力すると、IKEv2 ポリシー コンフィギュレーション モードが開始され、このモードで追加の IKEv2 SA の設定を指定します。追加のコマンドを使用して、SA 暗号化アルゴリズム、DH グループ、整合性アルゴリズム、ライフタイム、ハッシュ アルゴリズムを設定できます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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。policy index オプションが追加されました。

リリース	変更内容
9.13(1)	次の整合性、暗号化、および暗号化方式は廃止され、以降のリリースで削除されます。 • md5 • 3des 暗号化 • des 暗号化 • ヌル暗号化 Diffie-Hellman グループ 15 および 16 が追加され、DH グループ 1、2、5、および 24 が廃止されました。
9.15(1)	次の整合性、暗号化、および暗号化方式は、このリリースの強力な暗号化ライセンスモードから削除されました。 • md5 • 3des 暗号化 • des 暗号化 • ヌル暗号化（強力な暗号化と脆弱な暗号化の両方のライセンスモードから削除） DH グループ 1、2、5、および 24 のサポートが廃止されました。

例

次に、プライオリティ 1 の IKEv2 SA を作成し、IKEv2 ポリシー 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)# crypto ikev2 policy 1
ciscoasa(config-ikev2-policy)# integrity md5(DEPRECATED)
ciscoasa(config-ikev2-policy)# integrity sha

ciscoasa(config-ikev2-policy)# prf mad5(DEPRECATED)
ciscoasa(config-ikev2-policy)# prf sha

ciscoasa(config-ikev2-policy)# encryption 3des(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption des(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption null(DEPRECATED)
ciscoasa(config-ikev2-policy)# encryption aes
ciscoasa(config-ikev2-policy)# encryption aes-192
```

関連コマンド

コマンド	説明
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
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 ikev2 redirect

マスターからクラスタ メンバーへのロード バランシング リダイレクションが行われる IKEv2 フェーズを指定するには、グローバル コンフィギュレーション モードで **crypto ikev2 redirect** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

crypto ikev2 redirect {**during-init** | **during-auth**}

no crypto ikev2 redirect {**during-init** | **during-auth**}

構文の説明

during-auth	IKEv2 認証交換中のクラスタ メンバーへのロード バランシング リダイレクションをイネーブルにします。
during-init	IKEv2 SA によって開始された交換中のクラスタ メンバーへのロード バランシング リダイレクションをイネーブルにします。

デフォルト

デフォルトでは、クラスタ メンバーへのロード バランシング リダイレクションは IKEv2 認証交換中に行われます。

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
8.4(1)	このコマンドが追加されました。

例

次に、クラスタ メンバーへのロード バランシング リダイレクションが IKEv2 によって開始された交換中に実行されるように設定する例を示します。

```
ciscoasa(config)# crypto ikev2 redirect during-init
```

関連コマンド

コマンド	説明
crypto ikev2 cookie-challenge	SA によって開始されたパケットへの応答として、ASA がピア デバイスにクッキー チャレンジを送信できるようにします。
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。

コマンド	説明
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 ikev2 remote-access trust-point

AnyConnect IKEv2 接続で ASA のアイデンティティ証明書トラストポイントとして参照および使用されるグローバル トラストポイントを指定するには、トンネル グループ コンフィギュレーション モードで **crypto ikev2 remote-access trust-point** コマンドを使用します。設定からコマンドを削除するには、このコマンドの **no** 形式を使用します。

crypto ikev2 remote-access trust-point *name* [*line number*]

no crypto ikev2 remote-access trust-point *name* [*line number*]

構文の説明

name	トラストポイントの名前（最大 65 文字）。
line number	トラストポイントを挿入する行番号の場所を指定します。通常、このオプションは、別の行を削除および再追加しないで一番上にトラストポイントを挿入するために使用されます。行が指定されていない場合、ASA はリストの末尾にトラストポイントを追加します。

デフォルト

デフォルトの動作や値はありません。

使用上のガイドライン

すべての IKEv2 接続で ASA のトラストポイントが AnyConnect クライアントに対して自身を認証するように設定するには、**crypto ikev2 remote-access trust-point** コマンドを使用します。このコマンドを使用すると、AnyConnect クライアントは、ユーザのグループ選択をサポートできます。

2 つのトラストポイントを同時に設定できます。RSA を 2 つ、ECDSA を 2 つ、またはそれぞれ 1 つずつ設定できます。ASA は、設定したトラストポイント リストをスキャンし、クライアントがサポートする最初の 1 つを選択します。ECDSA を使用する場合は、RSA トラストポイントの前に、このトラストポイントを設定する必要があります。

すでに存在するトラストポイントを追加しようとすると、エラーが表示されます。削除するトラストポイント名を指定しないで **no crypto ikev2 remote-access trustpoint** コマンドを使用すると、すべてのトラストポイント コンフィギュレーションが削除されます。

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
トンネル グループ 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、および 2 つのトラストポイントの設定が追加されました。

例

次に、トラストポイント *cisco_asa_trustpoint* を指定する例を示します。

```
ciscoasa(config)# crypto ikev2 remote-access trust-point cisco_asa_trustpoint
```

crypto ipsec df-bit

IPsec パケットの DF-bit 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 ipsec df-bit** コマンドを使用します。

crypto ipsec df-bit [**clear-df** | **copy-df** | **set-df**] *interface*

構文の説明

clear-df	(オプション)外部 IP ヘッダーで DF ビットがクリアされること、および ASA はパケットをフラグメント化して IPsec カプセル化を追加する場合があることを指定します。
copy-df	(任意)ASA が外部 DF ビット設定を元のパケット内で探すことを指定します。
set-df	(任意)外部 IP ヘッダーに DF ビットを設定することを指定します。ただし、元のパケットで DF ビットがクリアされている場合、ASA はパケットをフラグメント化することがあります。
interface	インターフェイス名を指定します。

デフォルト

このコマンドは、デフォルトでディセーブルになっています。設定を指定せずにこのコマンドをイネーブルにすると、ASA はデフォルトとして **copy-df** 設定を使用します。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

DF ビットを IPsec トンネル機能とともに使用すると、ASA が、カプセル化されたヘッダーの Don't Fragment(DF)ビットをクリア、設定、またはコピーできるかどうかを指定できます。IP ヘッダー内の DF ビットにより、デバイスがパケットをフラグメント化できるかどうかが決定されます。

カプセル化されたヘッダーに DF ビットを指定するように ASA 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 ipsec df-bit** コマンドを使用します。このコマンドは、クリア テキスト パケットの DF ビット設定を処理し、暗号化が適用されるときに、外部 IPsec ヘッダーに対して DF ビットをクリア、設定、またはコピーします。

トンネル モードの IPsec トラフィックをカプセル化する場合は、DF ビットに **clear-df** 設定を使用します。この設定を使用すると、デバイスは、使用可能な MTU サイズよりも大きなパケットを送信できます。また、この設定は、使用可能な MTU サイズが不明な場合にも適しています。

注意 パケットは、次の矛盾した設定を行うとドロップされます。
crypto ipsec fragmentation after-encryption（フラグメント パケット）
crypto ipsec df-bit set-df outside（DF ビットを設定）

例

次に、グローバル コンフィギュレーション モードで、IPsec DF ポリシーを **clear-df** に設定する例を示します。

```
ciscoasa(config)# crypto ipsec df-bit clear-df outside
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを設定します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。
show crypto ipsec fragmentation	指定したインターフェイスのフラグメンテーション ポリシーを表示します。

crypto ipsec fragmentation

IPsec パケットのフラグメンテーション 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 ipsec fragmentation** コマンドを使用します。

crypto ipsec fragmentation {**after-encryption** | **before-encryption**} *interface*

構文の説明

after-encryption	暗号化の後で MTU の最大サイズに近い IPsec パケットを ASA がフラグメント化するように指定します(事前フラグメント化をディセーブルにします)。
before-encryption	暗号化の前に MTU の最大サイズに近い IPsec パケットを ASA がフラグメント化するように指定します(事前フラグメント化をイネーブルにします)。
interface	インターフェイス名を指定します。

デフォルト

before-encryption 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

パケットは、暗号化する ASA の発信リンクの MTU サイズに近い場合、IPsec ヘッダーを付けてカプセル化されると、発信リンクの MTU を超える可能性があります。超えた場合は、暗号化の後にパケットがフラグメント化され、復号化デバイスがプロセス パスで再構築することになります。IPsec VPN の事前フラグメント化では、デバイスはプロセス パスではなく高性能な CEF パスで動作するため、復号化時のデバイスのパフォーマンスが向上します。

IPsec VPN の事前フラグメント化により、暗号化デバイスは、IPsec SA の一部として設定されたトランスフォーム セットで使用可能な情報から、カプセル化されたパケット サイズを事前に設定します。デバイスでパケットが出力インターフェイスの MTU を超えることが事前に設定されている場合、デバイスは暗号化する前にそのパケットをフラグメント化します。これにより、復号化前にプロセス レベルでパケットを再構築する必要がなくなるため、復号化のパフォーマンスと IPsec トラフィックの全体的なスループットが向上します。

IPv6 対応インターフェイスで許可される最小 MTU は 1280 バイトです。ただし、IPsec がインターフェイスでイネーブルになっている場合、MTU 値は、IPsec 暗号化のオーバーヘッドのために 1380 未満に設定できません。インターフェイスを 1380 バイト未満に設定すると、パケットのドロップが発生する可能性があります。

注意 パケットは、次の矛盾した設定を行うとドロップされます。
crypto ipsec fragmentation after-encryption（フラグメント パケット）
crypto ipsec df-bit set-df outside（DF ビットを設定）

例

次に、グローバル コンフィギュレーション モードで、IPsec パケットの事前フラグメント化を内部インターフェイス上だけでイネーブルにする例を示します。

```
ciscoasa(config)# crypto ipsec fragmentation before-encryption inside
ciscoasa(config)#
```

次に、グローバル コンフィギュレーション モードで、IPsec パケットの事前フラグメント化をインターフェイス上でディセーブルにする例を示します。

```
ciscoasa(config)# crypto ipsec fragmentation after-encryption inside
ciscoasa(config)#
```

関連コマンド

コマンド	説明
crypto ipsec df-bit	IPsec パケットの DF ビット ポリシーを設定します。
show crypto ipsec fragmentation	IPsec パケットのフラグメンテーション ポリシーを表示します。
show crypto ipsec df-bit	指定したインターフェイスの DF ビット ポリシーを表示します。

crypto ipsec ikev1 transform-set

IKEv1 トランスフォーム セットを作成または削除するには、グローバル コンフィギュレーション モードで **crypto ipsec ikev1 transform-set** コマンドを使用します。トランスフォームを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

no crypto ipsec ikev1 transform-set *transform-set-name encryption* [*authentication*]

構文の説明

authentication	(オプション)IPsec のデータ フローの整合性を保証する認証方法を次の中から 1 つ指定します。 **esp-md5-hmac**:ハッシュ アルゴリズムとして MD5/HMAC-128 を使用する場合。 **esp-sha-hmac**:ハッシュ アルゴリズムとして SHA/HMAC-160 を使用する場合。 **esp-none**:HMAC 認証を使用しない場合。
暗号化	IPsec のデータ フローを保護する暗号化方法を次の中から 1 つ指定します。 **esp-aes**:128 ビット キーで AES を使用する場合。 **esp-aes-192**:192 ビット キーで AES を使用する場合。 **esp-aes-256**:256 ビット キーで AES を使用する場合。 **esp-des**:56 ビットの DES-CBC を使用する場合。 **esp-3des**:トリプル DES アルゴリズムを使用する場合。 **esp-null**:暗号化を使用しない場合。
transform-set-name	作成または変更するトランスフォーム セットの名前。すでにコンフィギュレーションに存在するトランスフォーム セットを表示するには、**show running-config ipsec** コマンドを入力します。

デフォルト

デフォルトの認証設定は、esp-none(認証しない)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	このコマンドが追加されました。
7.2(1)	この項は書き換えられました。
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)	次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。 • esp-md5-hmac • esp-3des • esp-des
9.15(1)	次のオプションは、このリリースから削除されました。 • esp-md5-hmac • esp-3des • esp-des

使用上のガイドライン

このコマンドでは、トランスフォーム セットが使用する IPsec 暗号化およびハッシュ アルゴリズムを指定します。

トランスフォーム セットを設定したら、そのセットをクリプト マップに割り当てます。1 つのクリプト マップに対して最大 6 つのトランスフォーム セットを割り当てることができます。ピアが IPsec セッションを確立しようとすると、ASA は、一致が検出されるまで、各クリプト マップのアクセス リストを使用してピアを評価します。次に、ASA は、一致が検出されるまで、ピアがネゴシエートするすべてのプロトコル、アルゴリズム、およびその他の設定を、クリプト マップに割り当てられているトランスフォーム セット内の設定を使用して評価します。ASA では、ピアの IPsec ネゴシエーションとトランスフォーム セット内の設定とが一致すると、IPsec セキュリティ アソシエーションの一部としてその設定を保護されたトラフィックに適用します。ASA は、ピアがアクセス リストに一致しない場合や、クリプト マップに割り当てられているトランスフォーム セット内にピアのセキュリティ設定と完全に一致するセキュリティ設定が見つからない場合、IPsec セッションを終了します。

暗号化と認証のどちらを先に指定してもかまいません。認証を指定せずに暗号化を指定することもできます。作成するトランスフォーム セットに認証を指定する場合は、暗号化も指定する必要があります。変更するトランスフォーム セットに認証だけを指定した場合、トランスフォーム セットでは、現在の暗号化設定が維持されます。

AES 暗号化を指定する場合は、グローバル コンフィギュレーション モードでも **isakmp policy priority group 5** コマンドを使用して、AES で提供される大きなキー サイズに対応できるように Diffie-Hellman グループ 5 を割り当てることを推奨します。

ヒント クリプト マップまたはダイナミック クリプト マップにトランスフォーム セットを適用し、そのマップに割り当てられているトランスフォーム セットを表示する場合は、トランスフォーム セットにコンフィギュレーションの内容を表す名前を付けておくと便利です。たとえば、次に示す最初の例の「3des-md5」は、トランスフォーム セットで使用する暗号化と認証を示しています。この名前の後に続く値は、トランスフォーム セットに割り当てる実際の暗号化と認証の設定です。

例

次のコマンドは、使用可能な暗号化と認証のすべてのオプション（暗号化と認証をまったく指定しないオプションは除く）を示しています。

```
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-md5 esp-3des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 3des-sha esp-3des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-md5 esp-des esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 56des-sha esp-des esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-md5 esp-aes esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 128aes-sha esp-aes esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-md5 esp-aes-192 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 192aes-sha esp-aes-192 esp-sha-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-md5 esp-aes-256 esp-md5-hmac
ciscoasa(config)# crypto ipsec ikev1 transform-set 256aes-sha esp-aes-256 esp-sha-hmac

ciscoasa(config)# crypto ipsec ikev1 transform-set esp-des (DEPRECATED)
ciscoasa(config)# crypto ipsec ikev1 transform-set esp-3des(DEPRECATED)
iscoasa(config)# crypto ipsec ikev1 transform-set esp-md5-hmac (DEPRECATED)
```

関連コマンド

コマンド	説明
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。
crypto map set transform-set	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 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。
show running-config crypto map	クリプト マップの設定内容を表示します。
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。

crypto ipsec ikev1 transform-set mode transport

IPsec IKEv1 接続に対して転送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 ipsec ikev1 transform-set mode transport** コマンドを使用します。このコマンドを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec ikev1 transform-set *transform-set-name* **mode** {**transport**}

no crypto ipsec ikev1 transform-set *transform-set-name* **mode** {**transport**}

構文の説明

transform-set-name	変更するトランスフォーム セットの名前。すでにコンフィギュレーションに存在するトランスフォーム セットを表示するには、**show running-config ipsec** コマンドを入力します。

デフォルト

転送モードのデフォルト設定はディセーブルです。IPsec ではネットワーク トンネル モードが使用されます。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

	ファイアウォール モード		セキュリティ コンテキスト		
				マルチ	
コマンド モード	ルーテッド	トランスペアレント	シングル	コンテキスト	システム
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)	このコマンドが書き換えられました。
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。

使用上のガイドライン

デフォルトのネットワーク トンネル モードの代わりに、IPsec にホスト間転送モードを指定するには、**crypto ipsec ikev1 transform-set mode transport** コマンドを使用します。

例

次のコマンドは、使用可能な暗号化と認証のすべてのオプション（暗号化と認証をまったく指定しないオプションは除く）を示しています。

```
ciscoasa(config)# crypto ipsec ikev1 transform-set
ciscoasa(config)#
```

関連コマンド

コマンド	説明
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。
crypto map set transform-set	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 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。
show running-config crypto map	クリプト マップの設定内容を表示します。
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。

crypto ipsec ikev2 ipsec-proposal

IKEv2 プロポーザルを作成するには、グローバル コンフィギュレーション モードで **crypto ipsec ikev2 ipsec-proposal** コマンドを使用します。プロポーザルを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

no crypto ipsec ikev2 ipsec-proposal *proposal tag proposal_name*

構文の説明

proposal name	IPsec ESP プロポーザル サブモードにアクセスします。
proposal tag	IKEv2 IPsec プロポーザルの名前で、1 ～ 64 文字の文字列です。

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
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。
9.13(1)	次の IKEv2/IPsec プロポーザル整合性と暗号化方式は廃止され、以降のリリースで削除されます。 • md5 • 3des • des • aes-gmac • aes-gmac-192 • aes-gmac-256

リリース	変更内容
9.15(1)	次の IKEv2/IPsec プロポーザル整合性と暗号化方式は、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

このコマンドは、プロポーザルを作成し、ipsec プロポーザル コンフィギュレーション モードを開始します。このモードで、プロポーザルの複数の暗号化および整合性タイプを指定できます。

例

次に、secure という名前の IPsec プロポーザルを作成し、IPsec プロポーザル 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)# crypto ipsec ikev2 ipsec-proposal secure
ciscoasa(config-ipsec-proposal)# protocol esp encryption ?
ciscoasa (config-ipsec-提案) # protocol esp aes
ciscoasa(config-ipsec-proposal)# protocol esp 3des(DEPRECATED)

ciscoasa(config-ipsec-proposal)# protocol esp integrity ?
ciscoasa (config-ipsec-提案) # protocol esp sha
ciscoasa(config-ipsec-proposal)# protocol esp md5(DEPRECATED)
```

関連コマンド

コマンド	説明
show running-config ipsec	すべてのトランスフォーム セットのコンフィギュレーションを表示します。
crypto map set transform-set	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 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。
show running-config crypto map	クリプト マップの設定内容を表示します。
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。

crypto ipsec ikev2 sa-strength-enforcement

IKEv2 暗号化暗号の強度が、子 IPsec SA の暗号化暗号の強度よりも確実に高くなるようにします。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

crypto ipsec ikev2 sa-strength-enforcement

no crypto ipsec ikev2 sa-strength-enforcement

デフォルト

適用は、デフォルトで無効になっています。

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	• 対応	—

コマンド履歴

リリース	変更内容
9.1(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

子 SA の暗号化暗号の強度が親 IKEv2 接続の暗号化暗号よりも高い場合、セキュリティは向上しません。セキュリティ対策として、このような状況が発生しないように IPsec を設定することをお勧めします。強度適用の設定は、暗号化暗号にのみ影響します。整合性アルゴリズムやキー交換アルゴリズムは変更されません。IKEv2 システムでは、各子 SA の選択された暗号化暗号の相対的な強度を次のように比較します。

イネーブルの場合、子 SA に設定されている暗号化暗号の強度が親 IKEv2 の暗号化暗号よりも高くないことを確認します。親よりも強力な暗号方式が見つかった場合、子 SA は親の暗号方式を使用するように更新されます。互換性のある暗号方式が見つからない場合、子 SA のネゴシエーションは中断されます。これらのアクションは、syslog およびデバッグ メッセージに記録されます。

次に、サポートされている暗号化暗号を、強度の高い順に示します。同じ行の暗号方式は、このチェックの目的では、同等の強度となります。

- AES-GCM-256、AES-CBC-256
- AES-GCM-192、AES-CBC、192
- AES-GCM-128、AES-CBC-128
- 3DES
- DES
- AES-GMAC（すべてのサイズ）、NULL

関連コマンド

コマンド	説明
show running-config ipsec	イネーブルの場合、crypto ipsec ikev2 sa-strength-enforcement を表示します。

crypto ipsec inner-routing-lookup

IPsec 内部ルーティング ルックアップをイネーブルにするには、コンフィギュレーション モードで **crypto ipsec inner-routing-lookup** コマンドを使用します。IPsec 内部ルーティング ルックアップ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 ipsec inner-routing-lookup

no crypto ipsec inner-routing-lookup

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

IPsec 内部ルーティング ルックアップはデフォルトでディセーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

デフォルトでは、外部 ESP パケットに対してはパケット単位の隣接関係ルックアップが行われますが、IPSec トンネル経由で送信されるパケットに対してはルックアップが行われません。

一部のネットワーク トポロジでは、ルーティング アップデートによって内部パケットのパスが変更され、ローカル IPsec トンネルが引き続きアップ状態である場合、トンネル経由のパケットは正しくルーティングされず、宛先に到達しません。

これを防止するには、IPSec 内部パケットに対してパケット単位のルーティング ルックアップをイネーブルにします。この機能がデフォルトでディセーブルになっているのは、こうしたルックアップによるパフォーマンスの低下を回避するためです。この機能は、必要な場合にのみイネーブルにしてください。

このコマンドが設定されている場合、非 VTI ベースのトンネルにのみ適用されます。

例

次に、内部ルーティング ルックアップをイネーブルにする例を示します。

```
ciscoasa(config)# crypto ipsec inner-routing-lookup
ciscoasa(config)# show run crypto ipsec
crypto ipsec inner-routing-lookup
```

関連コマンド

コマンド	説明
show run crypto ipsec	実行中の crypto ipsec 設定を表示します。

crypto ipsec profile

新しい IPsec プロファイルを作成するには、グローバル コンフィギュレーション モードで **crypto ipsec profile** コマンドを使用します。IPsec プロファイルを削除するには、このコマンドの **no** 形式を使用します。

crypto ipsec profile *name set pfs <group #>*

no crypto ipsec profile *name set pfs <group #>*

構文の説明

name	新しい IPsec プロファイルの名前を指定します。名前には最大 64 文字を使用できます。
group #	使用する Diffie-Hellman キー交換グループを指定します。

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
グローバル設定	• 対応	• x	• 対応	• 非対応	• -

コマンド履歴

リリース	変更内容
9.7(1)	このコマンドとそのサブモードを導入しました。

例

次の例では、VTIipsec が新しい IPsec プロファイルです。

```
ciscoasa(config)# crypto ipsec profile VTIipsec
```

関連コマンド

コマンド	説明
responder-only	VTI トンネル インターフェイスをレスポンダ専用モードに設定します。
set ikev1 transform-set	IKEv1 変換セットを IPsec プロファイル設定に使用するように指定します。
set pfs	PFS グループを IPsec プロファイル設定に使用するように指定します。
set security-association lifetime	IPsec プロファイル設定でのセキュリティ アソシエーションの期間を指定します。これは、キロバイト単位か秒単位、またはその両方で指定します。
set trustpoint	VTI トンネル接続の開始時に使用する証明書を定義するトラストポイントを指定します。

crypto ipsec security-association lifetime

グローバル ライフタイム値を設定するには、グローバル コンフィギュレーション モードで **crypto ipsec security-association lifetime** コマンドを使用します。グローバル ライフタイム値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 ipsec security-association lifetime {**seconds** *number* | **kilobytes** {*number* | **unlimited**}}

no crypto ipsec 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。デフォルトは 4,608,000 KB 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。
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。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。
unlimited	ASA がトンネルの発信側である場合に、クイック モードの 1 パケットでキロバイトを送信しません。

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

crypto ipsec security-association lifetime コマンドは、IPsec セキュリティ アソシエーションのネゴシエート時に使用されるグローバル ライフタイム値を変更します。

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。

個々のクリプト マップ エントリでライフタイム値が設定されていない場合、ASA は、ネゴシエート中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、ピアへの要求の中でグローバル ライフタイム値を指定します。セキュリティ アプライアンスは、こ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。

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。変更された場合、ASA では、変更によって影響を受ける接続のみが切断されます。クリプト マップに関連付けられている既存のアクセス リストをユーザが変更した場合（たとえばアクセス リスト内のエントリを削除した場合）、関連する接続のみが切断されます。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。

グローバルな指定時刻ライフタイムを変更するには、**crypto ipsec 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セキュリティ アソシエーションがタイムアウトします。

グローバル トラフィック量ライフタイムを変更するには、**crypto ipsec security-association lifetime kilobytes** コマンドを使用します。トラフィック量ライフタイムを使用すると、指定した量のトラフィック（KB 単位）がセキュリティ アソシエーション キーによって保護された後に、セキュリティ アソシエーションがタイムアウトします。

ライフタイムを短くするほど、同一キーで暗号化されている解析対象データが少なくなるため、攻撃者はキー回復攻撃を開始することが難しくなります。ただし、ライフタイムを短くするほど、新しいセキュリティ アソシエーションの確立にかかる CPU 処理時間が長くなります。

セキュリティ アソシエーション（および対応するキー）は、指定した秒数または指定したトラフィック量（KB 単位）のうち、いずれかを最初に超えた時点で有効期限が切れます。

例

次に、セキュリティ アソシエーションのグローバル指定時刻ライフタイムを指定する例を示します。

```
ciscoasa(config)# crypto ipsec-security association lifetime seconds 240
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	グローバル ライフタイム、トランスフォーム セットなど、すべての IPsec コンフィギュレーションをクリアします。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。

crypto ipsec security-association pmtu-aging

パス最大伝送単位（PMTU）のエージング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 ipsec security-association pmtu-aging** コマンドを使用します。PMTU エージ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。

crypto ipsec security-association pmtu-aging *reset-interval*

no crypto ipsec security-association pmtu-aging *reset-interval*

構文の説明

reset-interval	PMTU 値がリセットされる間隔を設定します。

デフォルト

この機能は、デフォルトでイネーブルにされています。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

リセット間隔は秒単位で指定します。

crypto ipsec security-association replay

IPsec アンチリプレイ ウィンドウ サイズを設定するには、グローバル コンフィギュレーション モードで **crypto ipsec security-association replay** コマンドを使用します。ウィンドウ サイズ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 ipsec security-association replay {**window-size** *n* | **disable**}

no crypto ipsec security-association replay {**window-size** *n* | **disable**}

構文の説明

n	ウィンドウ サイズを設定します。指定できる値は、64、128、256、512、または 1024 です。デフォルトは 64 です。
disable	アンチリプレイ チェックをディセーブルにします。

デフォルト

デフォルトのウィンドウ サイズは 64 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
7.2(4)/8.0(4)	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

Cisco IPsec 認証では、暗号化されたパケットそれぞれに対して固有のシーケンス番号を割り当てることによって、暗号化されたパケットを複製する攻撃者に対するアンチリプレイ保護が提供されます(セキュリティ アソシエーション アンチリプレイは、受信側がリプレイ攻撃から自身を保護するために、古いパケットまたは重複パケットを拒否できるセキュリティ サービスです)。復号機能によって、以前に認識したシーケンス番号が除外されます。エンクリプタによって、シーケンス番号が昇順で割り当てられます。すでに検出されている最も高いシーケンス番号である値 X はデクリプタによって記録されます。また、デクリプタによって、X-N+1 ～ X(N はウィンドウ サイズ)までのシーケンス番号を持つパケットが検出されているかどうかも記録されます。シーケンス番号 X-N を持つすべてのパケットが廃棄されます。現在、N は 64 に設定されているため、デクリプタによって追跡できるパケットは 64 までです。

ただし、64 パケット ウィンドウ サイズでは不十分な場合があります。たとえば、QoS はプライオリティが高いパケットを優先しますが、これにより、プライオリティが低いパケットが、デクリプタによって受信された最後の 64 パケットの 1 つであっても、廃棄される場合があります。このイベントにより、誤ったアラームである警告 syslog メッセージが生成される可能性があります。**crypto ipsec security-association replay** コマンドを使用すると、ウィンドウ サイズを拡張して、デクリプタが 64 を超えるパケットを追跡できます。

アンチリプレイ ウィンドウ サイズを増やしても、スループットおよびセキュリティに影響はありません。メモリへの影響は限定的です。デクリプタ上にシーケンス番号を保管するために必要となるのは、着信 IPsec SA ごとに追加の 128 バイトだけであるためです。今後アンチリプレイに関する問題が発生しないように、最大のウィンドウ サイズである 1024 を使用することを推奨します。

例

次に、セキュリティ アソシエーションのアンチリプレイ ウィンドウ サイズを指定する例を示します。

```
ciscoasa(config)# crypto ipsec security-association replay window-size 1024
ciscoasa(config)#
```

関連コマンド

コマンド	説明
clear configure crypto map	グローバル ライフタイム、トランスフォーム セットなど、すべての IPsec コンフィギュレーションをクリアします。
shape	トラフィック シェーピングをイネーブルにします。
priority	プライオリティ キューイングをイネーブルにします。
show running-config crypto map	すべてのクリプト マップのすべてのコンフィギュレーションを表示します。