CHAPTER 5

isakmp am-disable コマンド～ issuer-name コマンド

isakmp am-disable（廃止）

アグレッシブ モードの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 **isakmp 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。

isakmp am-disable

no isakmp 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	• Yes	—	• Yes	—	—

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)	このコマンドは廃止されました。**crypto isakmp am-disable** コマンドは、それに置き換わるものです。

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)# isakmp am-disable
```

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp disconnect-notify（廃止）

ピアへの切断通知をイネーブルにするには、グローバル コンフィギュレーション モードで **isakmp disconnect-notify** コマンドを使用します。切断通知をディセーブルにするには、このコマンドの **no** 形式を使用します。

isakmp disconnect-notify

no isakmp disconnect-notify

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルト値は [disabled] です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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)	このコマンドは廃止されました。**crypto isakmp disconnect-notify** コマンドは、それに置き換わるものです。

例

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

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

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp enable（廃止）

IPsec ピアが ASA と通信しているインターフェイスで ISAKMP 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 **isakmp enable** コマンドを使用します。インターフェイスで ISAKMP 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。

isakmp enable *interface-name*

no isakmp enable *interface-name*

構文の説明

interface-name	ISAKMP 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	• Yes	—	• Yes	—	—

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)	このコマンドは廃止されました。**crypto isakmp enable** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、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 isakmp enable inside
```

関連コマンド

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

コマンド	説明
clear 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 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。

isakmp identity（廃止）

ピアに送信されるフェーズ 2 ID 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 **isakmp identity** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

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

構文の説明

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

デフォルト

デフォルトの ISAKMP の識別情報は、**isakmp identity hostname** コマンドです。

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	• Yes	—	• Yes	—	—

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)	このコマンドは廃止されました。**crypto isakmp identity** コマンドは、それに置き換わるものです。

例

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

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

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp ipsec-over-tcp（廃止）

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 **isakmp 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。

isakmp ipsec-over-tcp [**port** *port1...port10*]

no isakmp 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	• Yes	—	• Yes	—	—

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)	このコマンドは廃止されました。**crypto isakmp ipsec-over-tcp** コマンドは、それに置き換わるものです。

例

次の例では、グローバル コンフィギュレーション モードで、IPsec over TCP をポート 45 でイネーブルにします。

```
ciscoasa(config)# isakmp ipsec-over-tcp port 45
```

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp keepalive

IKE キープアライブを設定するには、トンネル グループ ipsec 属性コンフィギュレーション モードで **isakmp keepalive** コマンドを使用します。キープアライブ パラメータをデフォルトのしきい値と再試行値でイネーブルの状態に戻すには、このコマンドの **no** 形式を使用します。

isakmp keepalive [**threshold** *seconds* | **infinite**] [**retry** *seconds*] [**disable**]

no isakmp keepalive disable [**threshold** *seconds* | **infinite**] [**retry** *seconds*] [**disable**]

構文の説明

disable	IKE キープアライブ処理をディセーブルにします。デフォルトではイネーブルになっています。
infinite	ASA でキープアライブ モニタリングを開始しません。
retry *seconds*	キープアライブ応答を受信しなかったことを受けて再試行する間隔を秒単位で指定します。指定できる範囲は 2 ～ 10 秒です。デフォルト値は 2 秒です。
threshold *seconds*	キープアライブ モニタリングを開始せずにピアがアイドル状態でいられる秒数を指定します。範囲は 10 ～ 3600 秒です。デフォルトは、LAN-to-LAN グループでは 10 秒、リモート アクセス グループでは 300 秒です。

デフォルト

リモート アクセス グループのデフォルトは、しきい値が 300 秒、再試行値が 2 秒です。

LAN-to-LAN グループのデフォルトは、しきい値が 10 秒、再試行値が 2 秒です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

あらゆるトンネル グループで、IKE キープアライブがデフォルトでイネーブルであり、しきい値と再試行値がデフォルト値になっています。この属性は、IPsec リモート アクセス タイプおよび IPsec LAN-to-LAN トンネル グループ タイプにのみ適用できます。

例

次に、トンネル グループ ipsec 属性コンフィギュレーション モードを開始し、IP アドレスが 209.165.200.225 の IPsec LAN-to-LAN トンネル グループに対して、IKE DPD を設定し、しきい値を 15 にし、再試行間隔を 10 に指定する例を示します。

```
ciscoasa(config)# tunnel-group 209.165.200.225 type IPSec_L2L
ciscoasa(config)# tunnel-group 209.165.200.225 ipsec-attributes
ciscoasa(config-tunnel-ipsec)# isakmp keepalive threshold 15 retry 10
ciscoasa(config-tunnel-ipsec)#
```

関連コマンド

コマンド	説明
clear-configure tunnel-group	設定されているすべてのトンネル グループをクリアします。
show running-config tunnel-group	すべてのトンネル グループまたは特定のトンネル グループのトンネル グループ コンフィギュレーションを表示します。
tunnel-group ipsec-attributes	このグループのトンネル グループ IPsec 属性を設定します。

isakmp nat-traversal（廃止）

NAT トラバーサルをグローバルにイネーブルにするには、ISAKMP がグローバル コンフィギュレーション モードでイネーブルになっていることを確認し（**isakmp enable** コマンドでイネーブルにできます）、次に **isakmp nat-traversal** コマンドを使用します。NAT トラバーサルをイネーブルにした場合、このコマンドの **no** 形式でディセーブルにできます。

isakmp nat-traversal *natkeepalive*

no isakmp nat-traversal *natkeepalive*

構文の説明

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

デフォルト

デフォルトでは、NAT トラバーサル（**isakmp nat-traversal** コマンド）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	• Yes	—	• Yes	—	—

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)	このコマンドは廃止されました。**crypto isakmp nat-traversal** コマンドは、それに置き換わるものです。

使用上のガイドライン

ポート アドレス変換（PAT）を含めネットワーク アドレス変換（NAT）は、IPsec が使用されているものの、IPsec パケットの NAT デバイス通過を阻害する非互換性がいくつもあるネットワークの多くで使用されています。NAT トラバーサルを使用すると、ESP パケットが 1 つ以上の NAT デバイスを通過できるようになります。

ASA は IETF のドラフト「UDP Encapsulation of IPsec Packets」のバージョン 2 およびバージョン 3（http://www.ietf.org/html.charters/ipsec-charter.html から入手可能）に従って NAT トラバーサルをサポートし、NAT トラバーサルはダイナミック クリプト マップとスタティック クリプト マップの両方に対応しています。

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

例

次に、グローバル コンフィギュレーション モードを開始し、ISAKMP をイネーブルにし、間隔を 30 秒にして NAT トラバーサルをイネーブルにする例を示します。

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

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp policy authentication

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

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

構文の説明

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

デフォルト

デフォルトの ISAKMP ポリシー認証は **pre-share** オプションです。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

IKE ポリシーは、IKE ネゴシエーション用のパラメータのセットを定義したものです。RSA シグニチャを指定した場合、認証局（CA）から証明書を取得するように、ASA とそのピアを設定する必要があります。事前共有キーを指定する場合は、ASA とそのピアに、事前共有キーを別々に設定する必要があります。

例

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 40 の IKE ポリシー内で認証方式として RSA シグニチャを使用するように設定する例を示します。

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

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp policy encryption（廃止）

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

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

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

構文の説明

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

デフォルト

デフォルトの ISAKMP ポリシー暗号化は、**3des** です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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)	このコマンドは廃止されました。**crypto isakmp policy encryption** コマンドは、それに置き換わるものです。

例

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 25 の IKE ポリシー内でアルゴリズムとして 128 ビット キー AES 暗号化を使用するように設定する例を示します。

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

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

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

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp policy group（廃止）

IKE ポリシーで使用する Diffie-Hellman グループを指定するには、グローバル コンフィギュレーション モードで **isakmp policy group** コマンドを使用します。Diffie-Hellman グループ識別子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。

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

no isakmp policy *priority* **group**

構文の説明

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

デフォルト

デフォルトはグループ 2 です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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。グループ 7 が追加されました。
7.2(1)	このコマンドは廃止されました。**crypto isakmp policy group** コマンドは、それに置き換わるものです。

使用上のガイドライン

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

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

(注) Cisco VPN Client バージョン 3.x 以降では、ISAKMP ポリシーで DH グループ 2 を設定する必要があります(DH グループ 1 を設定した場合、Cisco VPN Client は接続できません)。

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

例

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 40 の IKE ポリシーでグループ 2(1024 ビットの Diffie-Hellman)を使用するように設定する例を示します。

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

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp policy hash（廃止）

IKE ポリシーで使用するハッシュ アルゴリズムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy hash** コマンドを使用します。ハッシュ アルゴリズムをデフォルト値の SHA-1 にリセットするには、このコマンドの **no** 形式を使用します。

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

no isakmp policy *priority* **hash**

構文の説明

md5	IKE ポリシーでハッシュ アルゴリズムとして MD5（HMAC バリアント）を使用することを指定します。
priority	IKE ポリシーを一意に識別し、そのポリシーにプライオリティを割り当てます。1 ～ 65,534 の整数を使用します。1 はプライオリティが最も高く、65,534 が最も低くなります。
sha	IKE ポリシーでハッシュ アルゴリズムとして SHA-1（HMAC バリアント）を使用することを指定します。

デフォルト

デフォルトのハッシュ アルゴリズムは SHA-1 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	• Yes	—	• Yes	—	—

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)	このコマンドは廃止されました。**crypto isakmp policy hash** コマンドは、それに置き換わるものです。

使用上のガイドライン

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

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

例

次に、グローバル コンフィギュレーション モードを開始し、プライオリティ番号 40 の IKE ポリシー内で MD5 ハッシュ アルゴリズムを使用するように指定する例を示します。

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

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isakmp policy lifetime（廃止）

期限切れになるまでの IKE セキュリティ アソシエーションのライフタイムを指定するには、グローバル コンフィギュレーション モードで **isakmp policy lifetime** コマンドを使用します。セキュリティ アソシエーションのライフタイムをデフォルト値の 86,400 秒（1 日）にリセットするには、このコマンドの **no** 形式を使用します。

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

no isakmp policy *priority* **lifetime**

構文の説明

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

デフォルト

デフォルト値は 86,400 秒（1 日）です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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)	このコマンドは廃止されました。**crypto isakmp policy lifetime** コマンドは、それに置き換わるものです。

使用上のガイドライン

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

ライフタイムを長くするほど、ASA は以後の IPSec セキュリティ アソシエーションをより迅速にセットアップします。暗号化強度は十分なレベルにあるため、キーの再生成間隔を極端に短く（約 2 ～ 3 分ごとに）しなくてもセキュリティは保証されます。デフォルト値の採用を推奨しますが、ピアがライフタイムを提示しない場合には、無限のライフタイムを指定できます。

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

例

次に、グローバル コンフィギュレーション モードを開始し、IKE ポリシー内にプライオリティ番号 40 で IKE セキュリティ アソシエーションのライフタイムを 50,4000 秒（14 時間）を設定する例を示します。

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

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

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

関連コマンド

clear configure 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 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 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 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。

isakmp reload-wait（廃止）

すべてのアクティブなセッションが自主的に終了するまで待機してから ASA をリブート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 **isakmp reload-wait** コマンドを使用します。アクティブなセッションが終了するのを待たずに ASA をリブートするには、このコマンドの **no** 形式を使用します。

isakmp reload-wait

no isakmp reload-wait

構文の説明

このコマンドには引数またはキーワードはありません。

デフォルト

デフォルトの動作や値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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)	このコマンドは廃止されました。**crypto isakmp reload-wait** コマンドは、それに置き換わるものです。

例

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

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

関連コマンド

コマンド	説明
clear configure 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 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 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 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。

isis priority

インターフェイスで指定 ASA のプライオリティを設定するには、インターフェイス ISIS コンフィギュレーション モードで **isis priority** コマンドを使用します。デフォルトのプライオリティ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。

isis priority *number-value* **[level-1 | level-2]**

no isis priority [level-1 | level-2]

構文の説明

number-value	ルータのプライオリティを設定します。指定できる範囲は 0 ～ 127 です。
level-1	（任意）レベル 1 専用のプライオリティを設定します。
level-2	（任意）レベル 2 専用のプライオリティを設定します。

コマンド デフォルト

デフォルトは 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
インターフェイス ISIS コンフィギュレーション	• Yes	• Yes	• Yes	—	—

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

このコマンドは、LAN 上のどの ASA が指定ルータまたは DIS であるかを決定するために使用されるプライオリティを設定します。プライオリティは hello パケットでアドバタイズされます。最高のプライオリティを持つ ASA が DIS になります。

（注） IS-IS では、バックアップ指定ルータはありません。プライオリティを 0 に設定すると、そのシステムが DIS になる可能性は低くなりますが、完全には回避できません。プライオリティの高い ASA がオンラインになると、現在の DIS からその役割を引き継ぎます。プライオリティ値が同一の場合は、MAC アドレス値が高いルータが優先されます。

例

次に、プライオリティ レベルを 80 に設定して、レベル 1 ルーティングにプライオリティを与える例を示します。この ASA が DIS になる可能性が高くなります。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis priority 80 level-1
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接の確立をフィルタリングします。
isis advertise prefix	IS-IS インターフェイスでの LSP アドバタイズメントで接続されているネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。

コマンド	説明
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

isis protocol shutdown

IS-IS プロトコルが、指定されたインターフェイス上で隣接関係を形成できないようにするため、また、ASA が生成した LSP にインターフェイスの IP アドレスを設定するため、IS-IS プロトコルをディセーブルするには、インターフェイス ISIS コンフィギュレーション モードで **isis protocol shutdown** コマンドを使用します。IS-IS プロトコルを再び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。

isis protocol shutdown

no isis protocol shutdown

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

このコマンドにデフォルトの動作または値はありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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すると、コンフィギュレーション パラメータを削除せずに、指定されたインターフェイスの IS-IS プロトコルをディセーブルにできます。IS-IS プロトコルはこのコマンドを設定したインターフェイスの隣接関係を形成することはなく、ASA が生成した LSP にインターフェイスの IP アドレスが設定されます。IS-IS がインターフェイスの隣接関係を形成しないようにし、IS-IS LSP データベースをクリアするには、**protocol shutdown** コマンドを使用します。

例

次に、GigabitEthernet 0/0 上で IS-IS プロトコルをディセーブルにする例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis protocol shutdown
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接の確立をフィルタリングします。
isis advertise prefix	IS-IS インターフェイスでの LSP アドバタイズメントで接続されているネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

isis retransmit-interval

各 IS-IS LSP の再送信間隔を設定するには、インターフェイス ISIS コンフィギュレーション モードで **isis retransmit-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

isis retransmit-interval *seconds*

no isis retransmit-interval *seconds*

構文の説明

seconds	（オプション）各 LSP の再送信の間隔。接続ネットワーク上の任意の 2 台のルータ間で想定される往復遅延より大きな数値にする必要があります。指定できる範囲は 0 ～ 65535 です。

コマンド デフォルト

デフォルトは 5 分です。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

seconds 引数は控えめな値にする必要があります。そうしないと、不要な再送信が発生します。このコマンドは、LAN（マルチポイント）インターフェイスに影響を与えません。

例

次に、大容量のシリアル回線に対して各 IS-IS LSP を 60 秒ごとに再送信するように GigabitEthernet 0/0 を設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis retransmit-interval 60
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接の確立をフィルタリングします。
isis advertise prefix	IS-IS インターフェイスでの LSP アドバタイズメントで接続されているネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。

コマンド	説明
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

isis retransmit-throttle-interval

インターフェイスでの 各 IS-IS LSP の再送信間隔を設定するには、インターフェイス ISIS コンフィギュレーション モードで **isis retransmit-throttle-interval** コマンドを使用します。デフォルト値に戻すには、このコマンドの **no** 形式を使用します。

isis retransmit-throttle-interval *milliseconds*

no isis retransmit-throttle-interval

構文の説明

milliseconds	(オプション)インターフェイスでの LSP 再送信間の最小遅延。指定できる範囲は 0 ～ 65535 です。

コマンド デフォルト

この遅延は、**isis lsp-interval** コマンドで判断されます。

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
インターフェイス ISIS コンフィギュレーション	• Yes	• Yes	• Yes	—	—

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

このコマンドは、LSP 再送信トラフィックの制御方法と同様に、多くの LSP およびインターフェイスを持つ大規模なネットワークで役立つ場合があります。このコマンドは、インターフェイスで LSP を再送信できるレートを制御します。

このコマンドは、(**isis lsp-interval** コマンドで制御される)インターフェイスで LSP が送信されるレート、および(**isis retransmit-interval** コマンドで制御される)単一の LSP の再送信の周期とは区別されます。これらのコマンドを組み合わせて使用することにより、1 つの ASA からのそのネイバーへのルーティング トラフィックで発生する負荷を制御できます。

例

次に、LSP 再送信のレートが 300 ミリ秒あたり 1 回に制限されるように GigabitEthernet 0/0 を設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis retransmit-throttle-interval 300
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接の確立をフィルタリングします。
isis advertise prefix	IS-IS インターフェイスでの LSP アドバタイズメントで接続されているネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

isis tag

IP プレフィックスが IS-IS LSP に設定されている場合に、インターフェイスに設定されている IP アドレスにタグを設定するには、インターフェイス ISIS コンフィギュレーション モードで **isis tag** コマンドを使用します。IP アドレスのタグ設定を停止するには、このコマンドの **no** 形式を使用します。

isis tag *tag-number*

no isis tag *tag-number*

構文の説明

tag-number	IS-IS ルートでタグとして機能する番号。指定できる範囲は 1 ～ 4294967295 です。

コマンド デフォルト

インターフェイスに設定された IP アドレスに関連付けられているルート タグはありません。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

タグが使用されないかぎり、タグ付けされたルートではいかなるアクション（ルートの再配布やルートの集約のためのアクションなど）も発生しません。このコマンドを設定すると、タグがパケット内の新規の情報であるため、ASA は新しい LSP をトリガーします。

例

次に、「100」というタグを持つように GigabitEthernet 0/0 を設定する例を示します。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# isis tag 100
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接の確立をフィルタリングします。
isis advertise prefix	IS-IS インターフェイスでの LSP アドバタイズメントで接続されているネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。

コマンド	説明
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
is-type	IS-IS ルーティング プロセスのルーティング レベルを割り当てます。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更(アップまたはダウン)する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト(TLV)を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

is-type

IS-IS ルーティング プロセスのインスタンスのルーティング レベルを設定するには、ルータ ISIS コンフィギュレーション モードで **is-type** コマンドを使用します。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。

isis type [level-1 | level-1-2 | level-2-only]

no isis type [level-1 | level-1-2 | level-2-only]

構文の説明

level-1	(オプション)エリア内ルーティングを示します。この ASA は、エリア内の宛先についてのみ学習します。レベル 2(エリア間)ルーティングは、最も近いレベル 1 ～ 2 ASA によって実行されます。
level-1-2	(オプション)ASA は、レベル 1 およびレベル 2 のルーティングを実行します。この ASA は、ルーティング プロセスのインスタンスを 2 つ実行します。このルータは、エリア内(レベル 1 ルーティング)の宛先について 1 つのリンクステート パケット データベース(LSDB)を持っており、Shortest Path First(SPF)の計算を実行してエリア トポロジを検出します。また、他のすべてのバックボーン(レベル 2)ルータのリンクステート パケット(LSP)による別のリンクステート データベース(LSDB)を持ち、別の SPF 計算を実行して、バックボーンのトポロジと他のすべてのエリアの存在を検出します。
level-2-only	(オプション)エリア間ルーティングを示します。この ASA は、バックボーンの一部であり、それ自身のエリア内のレベル 1 だけの ASA とは通信しません。

コマンド デフォルト

従来の IS-IS コンフィギュレーションでは、ASA はレベル 1(エリア内)およびレベル 2(エリア間)ルータとしてだけ機能します。

マルチエリア IS-IS コンフィギュレーションでは、設定された IS-IS ルーティング プロセスの最初のインスタンスは、デフォルトでレベル 1-2(エリア内およびエリア間)ルータです。設定されている IS-IS プロセスの残りのインスタンスはデフォルトでレベル 1 ルータになります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

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

IS-IS ルーティング プロセスのタイプを設定することを水晶します。マルチエリア IS-IS を設定している場合は、ルータのタイプを設定するか、またはデフォルト設定のままにしておく必要があります。デフォルトでは、**router isis** コマンドを使用して設定した IS-IS ルーティング プロセスの最初のインスタンスは、レベル 1-2 ルータになります。

ネットワークにエリアが 1 つだけしかない場合は、必ずしもレベル 1 とレベル 2 の両方のルーティング アルゴリズムを実行する必要はありません。IS-IS がコネクションレス型ネットワーク サービス（CLNS）ルーティングに使用され、エリアが 1 つしかない場合は、レベル 1 だけを使用する必要があります。IS-IS が IP ルーティングだけに使用され、エリアが 1 つしかない場合は、常にレベル 2 だけを実行できます。すでにレベル 1-2 エリアがある場合は、その後に追加されたエリアは、デフォルトでレベル 1 エリアになります。

ルータ インスタンスがレベル 1-2（IS-IS ルーティング プロセスの最初のインスタンスのデフォルト）に設定されている場合は、**is-type** コマンドを使用して、そのエリアのレベル 2（エリア間）ルーティングを削除できます。**is-type** コマンドを使用してエリアのレベル 2 ルーティングを設定することもできます。

例

エリア ルータの指定例を示します。

```
ciscoasa# router isis
ciscoasa(config-router)# is-type level-2-only
```

関連コマンド

コマンド	説明
advertise passive-only	パッシブ インターフェイスをアドバタイズするように ASA を設定します。
area-password	IS-IS エリア認証パスワードを設定します。
認証キー	IS-IS の認証をグローバルで有効にします。
authentication mode	グローバルな IS-IS インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
authentication send-only	グローバルな IS-IS インスタンスでは、送信される（受信ではなく）IS-IS パケットでのみ認証が実行されるように設定します。
clear isis	IS-IS データ構造をクリアします。
default-information originate	IS-IS ルーティング ドメインへのデフォルト ルートを生成します。
distance	IS-IS プロトコルにより発見されたルートに割り当てられるアドミニストレーティブ ディスタンスを定義します。
domain-password	IS-IS ドメイン認証パスワードを設定します。
fast-flood	IS-IS LSP がフルになるように設定します。
hello padding	IS-IS hello をフル MTU サイズに設定します。
hostname dynamic	IS-IS ダイナミック ホスト名機能を有効にします。
ignore-lsp-errors	内部チェックサム エラーのある IS-IS LSP を受信した場合に LSP をパージするのではなく無視するように ASA を設定します。
isis adjacency-filter	IS-IS 隣接の確立をフィルタリングします。
isis advertise prefix	IS-IS インターフェイスでの LSP アドバタイズメントで接続されているネットワークの IS-IS プレフィックスをアドバタイズします。
isis authentication key	インターフェイスに対する認証を有効にします。

コマンド	説明
isis authentication mode	インターフェイスごとに、インスタンスに対して IS-IS パケットで使用される認証モードのタイプを指定します。
isis authentication send-only	送信される（受信ではなく）IS-IS パケットに対してのみ認証を実行するように、インターフェイスごとの IS-IS インスタンスを設定します。
isis circuit-type	IS-IS で使用される隣接関係のタイプを設定します。
isis csnp-interval	ブロードキャスト インターフェイス上で定期的に CSNP パケットが送信される間隔を設定します。
isis hello-interval	IS-IS が連続して hello パケットを送信する時間の長さを指定します。
isis hello-multiplier	ネイバーが見落とすことができる IS-IS hello パケット数の最大値を指定します。見落とされたパケット数がこの値を超えると、ASA は隣接がダウンしていると宣言します。
isis hello padding	IS-IS hello をインターフェイスごとのフル MTU サイズに設定します。
isis lsp-interval	インターフェイスごとの連続する IS-IS LSP 送信間の遅延時間を設定します。
isis metric	IS-IS メトリックの値を設定します。
isis password	インターフェイスの認証パスワードを設定します。
isis priority	インターフェイスでの指定された ASA のプライオリティを設定します。
isis protocol shutdown	インターフェイスごとに IS-IS プロトコルを無効にします。
isis retransmit-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis retransmit-throttle-interval	インターフェイス上の各 IS-IS LSP の再送信間の時間を設定します。
isis tag	IP プレフィックスが LSP に挿入されたときに、インターフェイスに設定された IP アドレスにタグを設定します。
log-adjacency-changes	NLSP IS-IS 隣接関係がステートを変更（アップまたはダウン）する際に、ASA がログ メッセージを生成できるようにします。
lsp-full suppress	PDU がフルになったときに、抑制されるルートを設定します。
lsp-gen-interval	LSP 生成の IS-IS スロットリングをカスタマイズします。
lsp-refresh-interval	LSP の更新間隔を設定します。
max-area-addresses	IS-IS エリアの追加の手動アドレスを設定します。
max-lsp-lifetime	LSP が更新されずに ASA のデータベース内で保持される最大時間を設定します。
maximum-paths	IS-IS のマルチパス ロード シェアリングを設定します。
metric	すべての IS-IS インターフェイスのメトリック値をグローバルに変更します。
metric-style	新規スタイル、長さ、および値オブジェクト（TLV）を生成し、TLV のみを受け入れるように、IS-IS を稼働している ASA を設定します。
net	ルーティング プロセスの NET を指定します。
passive-interface	パッシブ インターフェイスを設定します。
prc-interval	PRC の IS-IS スロットリングをカスタマイズします。

コマンド	説明
protocol shutdown	インターフェイス上で隣接関係を形成して LSP データベースをクリアすることができないように、IS-IS プロトコルをグローバルで無効にします。
redistribute isis	特にレベル 1 からレベル 2 へ、またはレベル 2 からレベル 1 へ、IS-IS ルートを再配布します。
route priority high	IS-IS IP プレフィックスにハイ プライオリティを割り当てます。
router isis	IS-IS ルーティングをイネーブルにします。
set-attached-bit	レベル 1 と レベル 2 間のルータが Attach ビットを設定する必要がある場合の制約を指定します。
set-overload-bit	SPF 計算の中間ホップとして使用できないことを他のルータに通知するように ASA を設定します。
show clns	CLNS 固有の情報を表示します。
show isis	IS-IS の情報を表示します。
show route isis	IS-IS ルートを表示します。
spf-interval	SPF 計算の IS-IS スロットリングをカスタマイズします。
summary-address	IS-IS の集約アドレスを作成します。

issuer（廃止）

(注) このコマンドをサポートする最後のリリースは、Version 9.5(1) でした。

アサーションを SAML-type SSO サーバに送信するセキュリティ デバイスを指定するには、その特定の SAML タイプの webvpn-sso-saml コンフィギュレーション モードで **issuer** コマンドを使用します。発行者名を削除するには、このコマンドの **no** 形式を使用します。

issuer *identifier*

no issuer [*identifier*]

構文の説明

identifier	セキュリティ デバイス名を指定します。通常は、デバイスのホスト名です。識別情報は、英数字で 65 文字未満に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
webvpn-sso-saml コンフィギュレーション	• Yes	—	• Yes	—	—

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。
9.5(2)	このコマンドは廃止されました。

使用上のガイドライン

WebVPN でだけ使用できる SSO のサポートにより、ユーザは、ユーザ名とパスワードを複数回入力しなくても、さまざまなサーバのセキュアな各種のサービスにアクセスできます。ASA は現在、SAML POST-type の SSO サーバと SiteMinder-type の SSO サーバをサポートしています。

このコマンドは、SAML-type の SSO サーバのみに適用されます。

例

次に、asa1.example.com というセキュリティ デバイスの発行者名を指定する例を示します。

```
ciscoasa(config-webvpn)# sso server myhostname type saml-v1.1-post
ciscoasa(config-webvpn-sso-saml# issuer asa1.example.com
ciscoasa(config-webvpn-sso-saml#
```

関連コマンド

コマンド	説明
assertion-consumer-url	セキュリティ デバイスが SAML-type SSO サーバ アサーション コンシューマ サービスに問い合わせる際に使用する URL を指定します。
request-timeout	SSO 認証の試行に失敗したときにタイムアウトになるまでの秒数を指定します。
show webvpn sso-server	セキュリティ デバイスに設定されているすべての SSO サーバの運用統計情報を表示します。
sso-server	シングル サインオン サーバを作成します。
トラストポイント	SAML-type のブラウザ アサーションへの署名に使用する証明書を含むトラストポイント名を指定します。

issuer-name

すべての発行済み証明書の発行者名 DN を指定するには、ローカル認証局（CA）サーバ コンフィギュレーション モードで **issuer-name** コマンドを使用します。認証局の証明書からサブジェクト DN を削除するには、このコマンドの **no** 形式を使用します。

issuer-name *DN-string*

no issuer-name *DN-string*

構文の説明

DN-string	自己署名 CA 証明書のサブジェクト名 DN でもある証明書の認定者名を指定します。属性と値のペアを区切るには、カンマを使用します。カンマを含む値は、引用符で囲んでください。発行者名は、英数字で 500 文字未満にする必要があります。

デフォルト

デフォルトの発行者名は cn=*hostame.domain-name* で、たとえば cn=asa.example.com となります。

コマンド モード

次の表に、コマンドを入力できるモードを示します。

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

コマンド履歴

リリース	変更内容
7.3(1)	このコマンドが追加されました。
8.0(2)	*DN-string* 値でカンマを保持するため、引用符のサポートが追加されました。

使用上のガイドライン

このコマンドでは、ローカル CA サーバが作成する証明書に表示される発行者名を指定します。この任意のコマンドは、発行者名をデフォルトの CA 名とは異なるものにする場合に使用します。

（注） この発行者名コンフィギュレーションは、CA サーバをイネーブルにし、**no shutdown** コマンドを発行して証明書を生成すると変更できなくなります。

例

次に、証明書認証を設定する例を示します。

```
ciscoasa(config)# crypto ca server
ciscoasa(config-ca-server)# issuer-name cn=asa-ca.example.com,ou=Eng,o=Example,c="cisco
systems, inc."
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 モードのコマンドにアクセスできるようにします。これらのコマンドを使用することで、ローカル CA を設定および管理できます。
keysize	証明書登録で生成される公開キーと秘密キーのサイズを指定します。
ライフタイム	CA 証明書と発行済みの証明書のライフタイムを指定します。
show crypto ca server	ローカル CA の特性を表示します。
show crypto ca server cert-db	ローカル CA サーバ証明書を表示します。