失効したピア証明書の暗号セッションの削除

CRL ダウンロード時の失効したピア証明書の暗号セッションの削除機能は、新しい CRL のダウンロード中に証明書が失効していることが判明した場合にピアとのアクティブな暗号セッションを削除します。

失効したピア証明書の暗号セッションの削除に関する制約事項

- 失効チェックがオフで、この機能が有効になっている場合は、IKE データベースにセッション番号が入力されません。show 出力に、削除されたセッションに関する情報が表示されません。
- この機能を（デバイス上のアクティブ セッションで）頻繁に有効化/無効化するのはお勧めできません。
- 同じ発行者名（CA サーバ）の CRL を頻繁にダウンロードする（30 分間隔）のはお勧めできません。
- CRL キャッシュを有効にする必要があります。CRL キャッシングをトラストポイントベースのプリフェッチに対して無効にすることはできません。ただし、CRL キャッシングを URL ベースのプリフェッチに対して無効にすることはできます。

- IKE 上の自動登録の場合は、セッションが次の IKE キー再生成まで削除されませんが、IKEv2 の場合は、トンネルを手動でクリアするか、証明書が失効するまで待つ必要があります。
- IKE が "issuer-name" と "SN" のデータベースを生成し、PKI から証明書の失効に関する通知を受け取ると、IKE がその PKI 通知を処理します。

失効したピア証明書の暗号セッションの削除に関する情報

暗号セッションの削除方法

1. 証明書認証経由でネゴシエートする場合は、ピアが CERT ペイロードをデバイスに送信し、デバイスが各証明書を解析してシリアル番号と発行者名に関する情報を保存します。この情報は、対応する CA サーバによって発行されたシリアル番号のリストを形成し、PKI に渡され、失効がチェックされます。
2. revocation-check crl コマンドがトラストポイント用に設定されている場合は、PKI が IKE に失効チェックの結果を伝達するため、IKE は不要なピア認定情報を保存せずに済みます。
3. CRL のダウンロードが成功すると、PKI が IKE に "issuer-name" を含む通知を送信します。CRL の署名と内容が検証されます。CRL の内容に変更がなければ、PKI は IKE に通知しません。
4. PKI が IKE に発行者名を通知すると、IKE は発行者名に関するシリアル番号のリストを作成して、そのリストを PKI に渡し、リスト内のシリアル番号が失効しているかどうかが検証されます。
5. PKI は IKE から渡されたシリアル番号のリストに対して失効チェックを実行し、ダウンロードした CRL に照らしてそのリストをチェックします。失効したシリアル番号のリストが IKE に返されます。
6. 失効したシリアル番号のリストを含む通知を PKI から受信すると、IKE はそのようなシリアル番号に関連付けられたセッションを特定して削除します。

失効したピア証明書の暗号セッションの削除のイネーブル化方法

暗号セッションの削除の有効化

このタスクは、失効した証明書の暗号セッションの削除を有効にするために実行します。

手順の概要

1. **enable**
2. **clear crypto session**
3. **configure terminal**
4. 次のいずれかを実行します。
   - **crypto isakmp disconnect-revoked-peers**
   - **crypto ikev2 disconnect-revoked-peers**
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**clear crypto session** 例： `Device# clear crypto session`	（任意）IPSec暗号セッション、IKE、およびセキュリティ アソシエーションを削除します。 （注） このコマンドは、以前確立したセッションの機能を有効にするために使用します。そうでない場合は、機能が新しいセッションでのみ有効になります。
ステップ 3	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

ステップ 4	次のいずれかを実行します。
	• **crypto isakmp disconnect-revoked-peers**
	• **crypto ikev2 disconnect-revoked-peers**
	例：
	`Device(config)# crypto isakmp disconnect-revoked-peers`
	例：
	`Device(config)# crypto ikev2 disconnect-revoked-peers`
		証明書が失効したピアとの IKE または IKEv2 暗号セッションを切断します。
		このコマンドを有効にするには、既存のセッションを再接続します。

ステップ 5	**end** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

失効したピア証明書の暗号セッションの削除機能の確認

このタスクは、暗号セッションの削除機能が show 出力に表示されるかどうかを確認するために実行します。

手順の概要

1. **enable**
2. **show crypto isakmp peers**
3. **show crypto ikev2 session detail**

手順の詳細

ステップ 1 **enable**

例：

```
Device> enable
```

特権 EXEC モードを有効にします。

- パスワードを入力します（要求された場合）。

ステップ 2 **show crypto isakmp peers**

例：

```
Device# show crypto isakmp peers
```

Internet Security Association and Key Management Protocol（ISAKMP）ピアの説明を表示します。

ステップ 3 **show crypto ikev2 session detail**

例：

```
Device# show crypto ikev2 session detail
```

アクティブなインターネット キー エクスチェンジ バージョン 2（IKEv2）セッションのステータスを表示します。

失効したピア証明書の暗号セッションを削除する設定例

例：IKE セッションの暗号セッションの削除のイネーブル化

```
Device> enable
Device# clear crypto session
Device# configure terminal
Device(config)# crypto isakmp disconnect-revoked-peers
Device# show crypto isakmp peers
```

```
Peer: 150.1.1.2 Port: 500 Local: 150.1.1.1
 Phase1 id: 150.1.1.2
 Disconnect Revoked Peer: Enabled
```

例：IKEv2 セッションの暗号セッションの削除のイネーブル化

```
Device> enable
Device# clear crypto session
Device# configure terminal
Device(config)# crypto ikev2 disconnect-revoked-peers
Device# show crypto ikev2 session detail

Session-id:1, Status:UP-ACTIVE, IKE count:1, CHILD count:1
Tunnel-id   Local          Remote           fvrf/ivrf          Status
1           10.0.0.1/500    10.0.0.2/500      (none)/(none)      READY
      Encr: 3DES, Hash: SHA96, DH Grp:2, Auth: PSK
      Life/Remaining/Active Time: 86400/86157/248 sec
      CE id: 0, Session-id: 1, MIB-id: 1
      Status Description: Negotiation done
      Local spi: 750CBE827434A245       Remote spi: 4353FEDBABEBF24C
      Local id:          10.0.0.1        Remote id:          10.0.0.2
      Local req mess id:    0           Remote req mess id: 0
      Local next mess id:    0          Remote next mess id: 2
      Local req queued:    0            Remote req queued: 0
      Local window:    5                 Remote window: 5
      DPD configured for 0 seconds
      NAT-T is not detected
      Disconnect Revoked Peer: Enabled
Child sa: local selector  10.0.0.1/0 - 10.0.0.1/65535
          remote selector 10.0.0.2/0 - 10.0.0.2/65535
          ESP spi in/out: 0x9360A95/0x6C340600
          CPI in/out: 0x9FE5/0xC776
          AH spi in/out: 0x0/0x0
          Encr: AES CBC, keysize: 128, esp_hmac: SHA96
          ah_hmac: Unknown - 0, comp: IPCOMP_LZS, mode tunnel
```

失効したピアの暗号セッションの削除に関する追加のリファレンス

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Commands List, All Releases*』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『*Cisco IOS Security Command Reference: Commands A to C*』 • 『*Cisco IOS Security Command Reference: Commands D to L*』 • 『*Cisco IOS Security Command Reference: Commands M to R*』 • 『*Cisco IOS Security Command Reference: Commands S to Z*』
IKE の設定	「*Configuring Internet Key Exchange for IPsec VPNs*」
IKEv2 の設定	『*Configuring Internet Key Exchange Version 2 and FlexVPN Site-to-Site*』
推奨される暗号化アルゴリズム	『*Next Generation Encryption*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

失効したピア証明書の暗号セッションの削除に関する機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1*: 失効したピア証明書の暗号セッションの削除に関する機能情報

機能名	リリース	機能情報
CRL ダウンロード時の失効したピア証明書の暗号セッションの削除		CRL ダウンロード時の失効したピア証明書の暗号セッションの削除機能は、新しい CRL のダウンロード中に証明書が失効していることが判明した場合にピアとのアクティブな暗号セッションを削除します。 次のコマンドが導入または変更されました。**crypto ikev2 disconnect-revoked-peers**、**crypto isakmp disconnect-revoked-peers**、**show crypto isakmp peers**、**show crypto ikev2 session detail**

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