GETVPN CRL チェック

Group Encrypted Transport VPN（GET VPN）プロセスの間、証明書は認証局（CA）から受信され、アイデンティティの証明として使用されます。証明書は、キーのセキュリティ侵害や証明書の喪失など、さまざまな理由により失効する可能性があります。失効した証明書はリポジトリに定期的に発行される証明書失効リスト（CRL）に配置されます。このリストは設定済みのCRL ライフタイムで指定された期間、リポジトリに格納されます。数時間から数日の任意の期間にすることができます。

GETVPN CRL チェックに関する情報

インターネット キー エクスチェンジ（IKE）では、証明書は2台のピア間でセッションが確立されるときに検証されます。現在のセッションは証明書失効の影響を受けません。ただし、新しいセッションを確立することはできず、グループ メンバーがキー サーバ（KS）に再登録しない限り証明書は再検証されません。

GETVPN CRL チェック機能では、設定されたトラストポイントで新しい CRL が利用可能なときに公開キー インフラストラクチャ（PKI）がグループ ドメイン オブ インタープリテーション（GDOI）KS に通知することができます。その後 KS は新しい Key Encryption Key（KEK）を作成し、グループ メンバーデバイスに再認証メッセージを送信します。これにより、syslog メッセージが出力され、現在の KEK が削除され、KS に再登録されます。

連携キー サーバのプロトコル統合

連携キー サーバのプロトコル（COOP）は、VPN ネットワークに複数のキー サーバ（KS）を設定できるようにする GET VPN の機能です。KS 冗長性のために使用されます。

すべての KS でグループ メンバー（GM）の再認証を有効にすることで、GETVPN CRL チェックは COOP と統合されます。ただし、連携 KS 間で一時的に接続が失われる場合、COOP 分割が発生する可能性は常にあります。

再認証がトリガーされたときの COOP 分割なし

COOP 分割が発生しない場合、プライマリ GM デバイスはセカンダリ KS の Key Encryption Key（KEK）を削除し、GM に再認証メッセージを送信します。セカンダリ KS は GM が再登録を開始する前に現在のポリシーをプライマリ ポリシーと同期させます。すべての GM が使用可能な KS に再登録して再認証され、新しい KEK を受信します。

再認証がトリガーされたときの COOP 分割

再認証がトリガーされる前に COOP 分割が発生し、2 つのプライマリ KS しかない場合、両者が再認証メッセージを送信します。それぞれのプライマリ KS は異なる新しい KEK を作成します。GM は、メッセージを受信するとすぐに既存の KEK をすべて削除するため、受信する最初の再認証メッセージだけを理解します。GM は使用可能な KS に再登録し、CRL チェックが行われます。再登録のとき、GM が登録した KS に応じて GM は最初のプライマリの KEK または 2 番目のプライマリの KEK のいずれかを受け取ります。GM はその KEK をインストールし、そのプライマリ KS からのみ今後のキー再生成を受信します。COOP マージが発生すると、KS はポリシーを同期し、キー再生成を送信して、すべての GM が最新の KEK とトラフィック暗号キー（TEK）を持つようにします。

異なる KEK の作成の回避

COOP 分割中に再認証がトリガーされる場合も、再認証と CRL チェックは依然として発生します。ただし、KS での異なる KEK の作成をトリガーすることは、再認証を遅らすことによって回避できます。プライマリ KS はすべての COOP KS に到達可能な（分割されない）場合にのみ、再認証を開始します。1 つの COOP KS に到達できない場合、プライマリ KS はすべての COOP KS が到達可能になるまで再認証メッセージの送信を遅らせます。

GETVPN CRL チェックの設定方法

GETVPN CRL チェック機能を有効にする前に、複数のコンポーネントを設定する必要があります。次の作業を行います。

- グループ メンバーとキー サーバが PKI クライアントとなるために定義された公開キー インフラストラクチャ（PKI）認証局（CA）（証明書を取得するように登録する必要があります）。
- PKI での証明書失効リスト（CRL）チェックを有効にするように設定されたキー サーバ（KS）。
- CA で利用可能であり、最初に必要なときに CRL をダウンロードするように設定された KS。これは、新しい CRL が利用可能になった後に最初のグループ メンバー（GM）登録に続いて KS が CRL をダウンロードすることを意味します。「GETVPN CRL チェックのためのキー サーバの設定」セクションを参照してください。

- PKI のグループ メンバー デバイスで無効化された CRL チェック。「グループ メンバーでの CRL チェックの無効化」セクションを参照してください。
- 証明書に対して設定されたインターネット キー エクスチェンジ（IKE）認証。「証明書の IKE 認証の設定」セクションを参照してください。

GETVPN CRL チェックのためのキー サーバの設定

新しい CRL が認証局（CA）で利用可能になった後に最初のグループ メンバー（GM）登録が発生した場合にキー サーバ（KS）が証明書失効リスト（CRL）をダウンロードするように設定するには、次のステップを実行します。

手順の概要

1. **ip domain name** *name*
2. **ip http server**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **revocation-check** *method*
6. **exit**
7. **crypto identity** *method*
8. **fqdn** *domain*
9. **fqdn** *domain*
10. **exit**
11. **crypto gdoi group** *group-name*
12. **server local**
13. **authorization identity** *name*
14. **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	**ip domain name** *name* 例： `Device(config)# ip domain name cisco.com`	Cisco IOS ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに使用するデフォルトのドメイン名を定義します。
ステップ 2	**ip http server** 例： `Device(config)# ip http server`	IP または IPv6 システム上の HTTP サーバを有効化します。

	コマンドまたはアクション	目的
ステップ 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint mycert`	デバイスで使用するトラストポイントを定義し、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。
ステップ 4	**enrollment url** *url* 例： `Device(config-ca-trustpoint)# enrollment url http://10.1.3.1:80`	CA の登録 URL を指定します。
ステップ 5	**revocation-check** *method* 例： `Device(config-ca-trustpoint)# revocation-check crl`	CRL による証明書チェックが行われることを確認します。
ステップ 6	**exit** 例： `Device(config-ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 7	**crypto identity** *method* 例： `Device(config)# crypto identity abcd`	デバイスの証明書内にある指定の識別名（DN）リストを使用してデバイスのアイデンティティを設定し、暗号アイデンティティ コンフィギュレーション モードを開始します。 （注） 特定の証明書、特に特定の DN の証明書を使用して、ピアが指定された暗号化インターフェイスにアクセスしないようにするデバイス構成の制限を設定できます。
ステップ 8	**fqdn** *domain* 例： `Device(config-crypto-identity)# fqdn ut01-unix5.cisco.com`	GM の完全修飾ドメイン名（FQDN）のリモート アイデンティティからネーム マングラーを取得します。
ステップ 9	**fqdn** *domain* 例： `Device(config-crypto-identity)# fqdn ut01-unix6.cisco.com`	次の GM の FQDN のリモート アイデンティティからネーム マングラーを取得します。

	コマンドまたはアクション	目的
ステップ 10	**exit** 例： `Device(config-crypto-identity)# exit`	暗号アイデンティティ コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに戻ります。
ステップ 11	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group gdoi-group1`	グループ ドメイン オブ インタープリテーション（GDOI）グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 12	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。
ステップ 13	**authorization identity** *name* 例： `Device(config-gdoi-local-server)# authorization identity abcd`	識別名（DN）または FQDN に基づいて GDOI グループの認証アイデンティティを指定します。
ステップ 14	**end** 例： `Device(config-gdoi-local-server)# end`	GDOI ローカル サーバ 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。

グループ メンバーでの CRL チェックの無効化

Public Key Infrastructure（PKI）のグループ メンバー（GM）をチェックする証明書失効リスト（CRL）を無効にするには、次のステップを実行してください。

手順の概要

1. **ip domain name** *name*
2. **ip http server**
3. **crypto pki trustpoint** *name*
4. **enrollment url** *url*
5. **revocation-check** *method*
6. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ip domain name** *name* 例： `Device(config)# ip domain name cisco.com`	Cisco IOS ソフトウェアが未修飾ホスト名（ドット付き 10 進ドメイン名を含まない名前）を作成するときに使用するデフォルトのドメイン名を定義します。
ステップ 2	**ip http server** 例： `Device(config)# ip http server`	IP または IPv6 システム上の HTTP サーバを有効化します。
ステップ 3	**crypto pki trustpoint** *name* 例： `Device(config)# crypto pki trustpoint mycert`	デバイスで使用するトラストポイントを定義し、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。
ステップ 4	**enrollment url** *url* 例： `Device(config-ca-trustpoint)# enrollment url http://10.1.3.1:80`	認証局（CA）の登録 URL を指定します。
ステップ 5	**revocation-check** *method* 例： `Device(config-ca-trustpoint)# revocation-check none`	GM の証明書チェックを無効にします。
ステップ 6	**exit** 例： `Device(config-ca-trustpoint)# exit`	CA トラストポイント モードを終了し、グローバル コンフィギュレーション モードに戻ります。

証明書の IKE 認証の設定

手順の概要

1. **crypto isakmp policy** *priority*
2. **no authentication pre-share**
3. **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	**crypto isakmp policy** *priority* 例： `Router(config)# crypto isakmp policy 1`	インターネット キー エクスチェンジ（IKE）ポリシーを定義して、ISAKMP ポリシー コンフィギュレーション モードを開始します。
ステップ 2	**no authentication pre-share** 例： `Router(config-isakmp)# no authentication pre-share`	IKE ポリシー内の認証方式をデフォルト値にリセットします。
ステップ 3	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

キー サーバでの GETVPN CRL チェックの有効化

新しい証明書失効リスト（CRL）が設定されているトラストポイント認証局（CA）で利用可能になったときに Public Key Infrastructure（PKI）がドメイン オブ インタープリテーション（GDOI）キー サーバ（KS）に通知するように設定するには、次のステップを実行します。

手順の概要

1. **crypto gdoi group** *group-name*
2. **server local**
3. **registration periodic crl trustpoint** *trustpoint-name*
4. **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	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group gdoi_group1`	GDOI グループを作成し、GDOI グループ コンフィギュレーション モードを開始します。
ステップ 2	**server local** 例： `Device(config-gdoi-group)# server local`	デバイスを GDOI キー サーバとして指定し、GDOI ローカル サーバ コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**registration periodic crl trustpoint** *trustpoint-name* 例： `Device(config-gdoi-local-server)# registration periodic crl trustpoint mycert`	設定されている PKI トラストポイント認証局で新しい CRL が使用可能になったときに GDOI KS の定期的な登録を有効にします。
ステップ 4	**end** 例： `Device(config-gdoi-local-server)# end`	GDOI ローカル サーバ モードを終了し、特権 EXEC モードに戻ります。

GETVPN CRL チェックの設定例

例：GETVPN CRL チェックの有効化

次の例は、すべての必須の事前設定を含めた、GETVPN CRL チェック機能を有効にする方法を示します。

例：GETVPN CRL チェックのためのキー サーバの設定

次の例では、新しい CRL が mycert という名前のトラストポイントの認証局（CA）で利用可能になった後に最初のグループ メンバー登録が発生すると、キー サーバ（KS）が証明書失効リスト（CRL）をダウンロードするように設定されます。

```
ip domain name cisco.com
ip http server
crypto pki trustpoint mycert
 enrollment url http://10.1.3.1:80
 revocation-check crl

crypto identity abcd
 fqdn ut01-unix5.cisco.com
 fqdn ut01-unix6.cisco.com

crypto gdoi group gdoi-group1
 server local
 authorization identity abcd
```

例：グループ メンバーでの CRL チェックの無効化

次の例では、Public Key Infrastructure（PKI）のグループ メンバー（GM）の CRL チェックが無効化されます。

```
ip domain name cisco.com
ip http server
crypto pki trustpoint mycert
```

```
 enrollment url http://10.1.3.1:80
 revocation-check none
```

例：証明書の IKE 認証の設定

```
crypto isakmp policy 1
 no authentication pre-share
```

例：キー サーバの GETVPN CRL チェックの有効化

次の例では、新しい CRL が mycert という名前のトラストポイント CA で利用可能になると、PKI が group1 という名前の GDOI KS に通知するように設定されます。

```
Crypto gdoi group gdoi_group1
 Server local
  registration periodic crl trustpoint mycert
```

GETVPN CRL チェックに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
エンタープライズ ネットワークの GET VPN の有効化のための基本的な導入ガイドライン	『*Cisco IOS GETVPN Solution Deployment Guide*』
GET VPN ネットワークの設計と実装	『*Group Encrypted Transport VPN (GETVPN) Design and Implementation Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2401	『*Security Architecture for the Internet Protocol*』
RFC 6407	『*The Group Domain of Interpretation*』

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

GETVPN CRL チェックに関する機能情報

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 : GETVPN CRL* チェックに関する機能情報

機能名	リリース	機能情報
GETVPN CRL チェック		新しい証明書失効リスト（CRL）が設定されているトラストポイントで利用可能になったときに Public Key Infrastructure（PKI）がドメイン オブ インタープリテーション（GDOI）キー サーバ（KS）に通知できるようにします。 次のコマンドが導入されました。 **registration periodic crl trustpoint.**

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。