GET VPN の復元力

GET VPN の復元力機能では、Cisco Group Encrypted Transport（GET）VPN の復元力を改善し、エラーが発生したときのデータ トラフィックの中断を防止したり最小化したりします。

GET VPN の復元力の前提条件

この機能を有効にするすべてのキー サーバ（KS）およびグループ メンバー（GM）で、GET VPN ソフトウェア バージョン 1.0.4 以降を実行している必要があります。この機能は、GET VPN ネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。この機能は、ネットワークのすべてのデバイスがこの機能をサポートするバージョンを実行しているかどうかを確認するために KS（またはプライマリ KS）で使用するコマンドを提供します。詳細については「*GM* が長い *SA* ライフタイムをサポートするソフトウェア バージョンを実行していることを確認する」セクションを参照してください。

GET VPN の復元力の制約事項

- すべてキー サーバ（KS）およびグループ メンバー（GM）は、長い SA ライフタイム向けにアップグレードする必要があります。

GET VPN の復元力に関する情報

長い SA ライフタイム

長いセキュリティアソシエーション（SA）ライフタイム機能では、Key Encryption Key（KEK）およびトラフィック暗号キー（TEK）の最大ライフタイムを 24 時間から 30 日に延長します。この機能により、スケジュールされた最後のキー再生成時に確認応答に応答しないグループメンバー（GM）に対して定期的なリマインダキー再生成を送信し続けるようにキーサーバ（KS）を設定することもできます。

定期的なリマインダキー再生成と長い SA ライフタイムを組み合わせて使用することにより、キーがロールオーバーする前にスケジュールされたキー再生成に失敗した場合、KS が効果的に GM を同期することができます。

（注） 24 時間より長いライフタイムでは、暗号化アルゴリズムを、128 ビット以上の AES キーを使用する Advanced Encryption Standard-Cipher Block Chaining（AES-CBC）または Advanced Encryption Standard-Galois/Counter Mode（AES-GCM）にする必要があります。

長い SA ライフタイム機能は GETVPN スイート B 機能とともに使用すると、GCM-AES と GMAC-AES でカプセル化されたパケットのグループでトラフィック暗号キー（TEK）ポリシーがトランスフォームされるときに AES-GSM および Galois Message Authentication Code-Advanced Encryption Standard（GMAC-AES）を使用できます。

長い SA ライフタイムへの移行

長い SA ライフタイム機能（1 日以上）に移行するときには、次のルールが適用されます。

- 長い SA ライフタイムが暗号 IPsec プロファイルに設定されているとき、GETVPN は非 Group Domain of Interpretation（GDOI）グループに対して IPsec プロファイルを使用しないように警告メッセージを表示します。
- グループメンバーが短い SA ライフタイムでキーサーバーに登録され、キーサーバーがポリシーを長い SA ライフタイムに変更する場合、GETVPN は **crypto gdoi ks rekey** コマンドを設定してポリシー変更を開始するときにすべての GM のソフトウェアバージョンをチェックします。KS に登録されている GM が長い SA ライフタイムをサポートしていない場合、すべての GM がアップグレードされるまでポリシーの変更を推奨しないというメッセージが表示されます。
- 長い SA 機能が KS で有効になると、この機能をサポートしていない古い Cisco IOS リリースを実行している GM からの登録がブロックされます。

クロック スキューの軽減

セキュリティアソシエーション（SA）のライフタイムが長いとき、グループメンバー（GM）は長期間、キーサーバから更新を受信しないことがあります。これにより、グループメンバーは Key Encryption Key（KEK）ライフタイム、トラフィック暗号キー（TEK）ライフタイム、および時間ベースアンチリプレイ（TBAR）疑似時間の間クロック スキューを経験することがあります。更新のキー再生成と新しい発信 IPsec SA へのロールオーバーによって GM はクロック スキューの問題を軽減することができます。

更新のキー再生成

トラフィック暗号キー（TEK）のライフタイムが 2 日以上の期間に設定され、時間ベースのアンチリプレイ（TBAR）が無効である場合、キー サーバは 24 時間ごとに更新のキー再生成を送信し、すべてのグループ メンバー（GM）の Key Encryption Key（KEK）ライフタイム、TEK ライフタイム、および TBAR 疑似時間を更新します。簡単に言うと、更新のキー再生成は、最後のユニキャスト確認応答（ACK）の受信状態に関係ない、すべての GM への現在の KEK ポリシー、TEK ポリシー、および TBAR 疑似時間（有効な場合）の再送信です。TBAR が有効な場合、更新のキー再生成は疑似時間を同期するために 2 時間ごとに送信され、追加の更新のキー再生成は必要ありません。

新しい発信 IPsec SA へのロールオーバー

長い SA ライフタイム（1 日を超える）が設定されている場合、トラフィック暗号キー（TEK）の残りのライフタイムが、下限が 30 秒のライフタイムに設定された古い TEK の 1 % に達し、古い TEK の残りのライフタイムの 30 秒でないとき、ロールオーバーが発生します。これにより、（他の GM が古い TEK を削除してから）1 つの GM から新しい TEK 遅延にロールオーバーされるトラフィックが破棄されるまで、グループ メンバー（GM）間のより大きなクロック スキューが可能になります。これによって、長期間 GM が「オフライン」（KS からの切断）になり、クロック スキューを軽減するための更新のキー再生成を受信できない問題が緩和されます。

定期的なリマインダ同期キー再生成

キー サーバ（KS）の定期的なリマインダ同期キー再生成機能を使用すると、スケジュールされている直前のキー再生成時に確認応答（ACK）に応答しないグループ メンバー（GM）に対して定期的なリマインダ キー再生成を送信できます。長い SA ライフタイム機能とこの機能の組み合わせは、キーのロールオーバーの前にスケジュールされたキー再生成に失敗した GM と KS が同期するために有効です。KS グループ設定で、キー再生成の再送信を設定するときの **rekey retransmit** コマンドに新しいキーワード **periodic** が追加されています。

キー再生成の再送信と同様に、定期的な再送信はそれぞれシーケンス番号を増加させます。スケジュールされた 3 回のキー再生成（再送信ではない）で GM が ACK を送信しないと、GM は KS のデータベースから削除されます。

事前配置されたキー再生成

長い SA ライフタイム（1 日を超える）が設定されているとき、事前配置されたキー再生成機能を使用すると、キーサーバー（KS）はSAライフタイムの半分の期間より先にキー再生成を送信できます。キー再生成の送信の通常な動作は短い SA ライフタイムに使用されます。グループ メンバー（GM）はこの早いキー再生成を受信すると、新しい TEK が発信としてロールオーバーされるまで、引き続き古い TEK を発信として使用します。事前配置されたキー再生成機能と長い SA ライフタイム機能の組み合わせはキーのロールオーバーの安定性を向上させます。この機能により、定期的なリマインダ キー再生成や同期キー再生成などのキー再生成エラーを回復するための十分な時間（KS）が確保されます。

GET VPN の復元力の設定方法

GM が長い SA ライフタイムをサポートするソフトウェア バージョンを実行していることを確認する

長いSAライフタイムは、GET VPNネットワーク内のすべてのデバイスをこの機能をサポートする GET VPN ソフトウェア バージョンにアップグレードしてから使用する必要があります。

ネットワーク内のすべてのデバイスが長い SA ライフタイムをサポートしていることを確認するには、キー サーバ（またはプライマリ キー サーバ）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature long-sa-lifetime**
3. **show crypto gdoi feature long-sa-lifetime | include No**

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	**show crypto gdoi feature long-sa-lifetime** 例： `Device# show crypto gdoi feature long-sa-lifetime`	GET VPN ネットワーク内の各 KS および GM で実行されている GET VPN ソフトウェアのバージョンを表示し、そのデバイスが長い SA ライフタイムをサポートしているかどうかを表示します。
ステップ 3	**show crypto gdoi feature long-sa-lifetime | include No** 例： `Device# show crypto gdoi feature long-sa-lifetime | include No`	（オプション）長い SA ライフタイムをサポートしないデバイスのみ表示します。

長い SA ライフタイムの設定

TEK の長い SA ライフタイムの設定

トラフィック暗号キー（TEK）の長い SA ライフタイムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec profile** *name*
4. **set security-association lifetime days** *days*
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	**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 3	**crypto ipsec profile** *name* 例： `Device(config)# crypto ipsec profile gdoi-p`	2 つの IPsec デバイス間における IPsec 暗号化で使用される IPsec パラメータを定義し、暗号化 IPsec プロファイル 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	**set security-association lifetime days** *days* 例： `Device(ipsec-profile)# set security-association lifetime days 15`	セキュリティ アソシエーション（SA）のライフタイムを 1 日に設定します。 • 最大日数は 30 日です。
ステップ 5	**end** 例： `Device(ipsec-profile)# end`	暗号 IPsec プロファイル ピア 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。

KEK の長い SA ライフタイムの設定

キー暗号キー（TEK）の長い SA ライフタイムを設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
5. **server local**
6. **rekey lifetime days** *days*
7. **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	**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 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group GET`	GDOI グループを指定し、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 4	**identity number** *number* 例： `Device(config-gdoi-group)# identity number 3333`	GDOI グループ番号を指定します。
ステップ 5	**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 6	**rekey lifetime days** *days* 例： `Device(gdoi-local-server)# rekey lifetime days 20`	KEK の日数または秒数を制限します。
ステップ 7	**end** 例： `Device(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。

定期的なリマインダ同期キー再生成の設定

定期的なリマインダ同期キー再生成を設定するには、次のステップを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gdoi group** *group-name*
4. **identity number** *number*
5. **server local**
6. **rekey retransmit** *number-of-seconds* **periodic**
7. **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	**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 3	**crypto gdoi group** *group-name* 例： `Device(config)# crypto gdoi group group1`	GDOI グループを指定し、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 4	**identity number** *number* 例： `Device(config-gdoi-group)# identity number 3333`	GDOI グループ番号を指定します。
ステップ 5	**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 6	**rekey retransmit** *number-of-seconds* **periodic** 例： `Device(gdoi-local-server)# rekey retransmit 10 periodic`	キー再生成メッセージが定期的に再送信される回数を指定します。 • このコマンドが設定されていない場合、再送信は行われません。
ステップ 7	**end** 例： `Device(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。

GET VPN の復元力の確認とトラブルシューティング

キー サーバの GET VPN の復元力の確認とトラブルシューティング

キーサーバー（KS）で実行されている設定を表示するには、**show running-config** コマンドと次のコマンドを使用します。

手順の概要

1. **enable**
2. **show crypto gdoi**
3. **show crypto gdoi ks rekey**

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	**show crypto gdoi** 例： `Device# show crypto gdoi`	現在の GDOI 構成、および KS からダウンロードされたポリシーを表示します。
ステップ 3	**show crypto gdoi ks rekey** 例： `Device#  show crypto gdoi ks rekey`	KS から送信されるキー再生成に関する情報を表示します。

グループ メンバーの GET VPN の復元力の確認とトラブルシューティング

グループメンバー（GM）で実行されている設定を表示するには、**show running-config** コマンドと次のコマンドを使用します。

手順の概要

1. **enable**
2. **show crypto gdoi ks rekey**
3. **show crypto gdoi ks policy**

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）。

	コマンドまたはアクション	目的
ステップ 2	**show crypto gdoi ks rekey** 例： `Device# show crypto gdoi ks rekey`	KS から送信されるキー再生成に関する情報を表示します。
ステップ 3	**show crypto gdoi ks policy** 例： `Device# show crypto gdoi ks policy`	次のキー再生成までの時間を表示します。

GET VPN 復元力の設定例

例：GMが長いSAライフタイムをサポートするソフトウェアバージョンを実行していることを確認する

次の例は、各グループ内のすべてのデバイスが長い SA ライフタイムをサポートしているかどうかを確認するために KS（またはプライマリ KS）で GET VPN ソフトウェア バージョン管理コマンドを使用する方法を示します。

```
Device# show crypto gdoi feature long-sa-lifetime

Group Name: GETVPN
    Key Server ID       Version   Feature Supported
        10.0.5.2         1.0.4          Yes
        10.0.6.2         1.0.4          Yes
        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No

    Group Member ID     Version   Feature Supported
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
        10.0.3.1         1.0.4          Yes
        10.0.3.2         1.0.4          Yes
```

また、上記のコマンドは GM でも入力できます（その GM の情報を表示します。KS や他の GM には使用できません）。

次の例は、KS（プライマリ KS）で長い SA ライフタイムをサポートしていない GET VPN ネットワークのデバイスのみ検索するコマンドを入力する方法を示しています。

```
Device# show crypto gdoi feature long-sa-lifetime | include No

        10.0.7.2         1.0.3          No
        10.0.8.2         1.0.2          No
        10.0.1.2         1.0.2          No
        10.0.2.5         1.0.3          No
```

例：長い SA ライフタイムの設定

例：TEK の長い SA ライフタイムの設定

次に、トラフィック暗号キー（TEK）の長い SA ライフタイムの設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto ipsec profile gdoi-p
Device(ipsec-profile)# set security-association lifetime days 15
Device(ipsec-profile)# end
```

例：KEK の長い SA ライフタイムの設定

次に、キー暗号キー（KEK）の長い SA ライフタイムの設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group GET
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey lifetime days 20
Device(gdoi-local-server)# end
```

例：定期的なリマインダ同期キー再生成の設定

次に、定期的なリマインダ同期キー再生成の設定方法の例を示します。

```
Device> enable
Device# configure terminal
Device(config)# crypto gdoi group group1
Device(config-gdoi-group)# identity number 3333
Device(config-gdoi-group)# server local
Device(gdoi-local-server)# rekey retransmit 10 periodic
Device(gdoi-local-server)# end
```

GET VPN の復元力のその他の参考資料

関連資料

関連項目	マニュアル タイトル

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 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*』
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 GET VPN Solutions 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

GET VPN の復元力の機能情報

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 : GET VPN* の復元力の機能情報

機能名	リリース	機能情報
GET VPN の復元力		次のコマンドが導入または変更されました。 **rekey lifetime, rekey retransmit, set security-association lifetime, show crypto gdoi.**

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。