IPsec SA アイドル タイマー

Cisco IOS XE ソフトウェアを実行しているルータによってピアの IPsec セキュリティ アソシエーション（SA）が作成される場合、そのSAを維持するためにリソースを割り当てる必要があります。SA には、メモリと、複数の管理されたタイマーが必要です。ピアがアイドル状態だと、それらのリソースが無駄になってしまいます。あまりに多くのリソースがアイドル状態のピアによって浪費されてしまうと、ルータによる他のピアとの新しい SA の作成ができなくなる可能性があります。IPsec SA アイドル タイマー機能では、SA のアクティビティをモニタリングするための、設定可能なアイドルタイマーが導入されており、これにより、アイドル状態のピアの SA を削除できます。この機能には、次のような利点があります。

- 向上したリソースの可用性
- Cisco IOS XE IPSec 配置のスケーラビリティの向上この機能によって、アイドル状態のピアによるリソースの浪費を防止できるので、より多くのリソースを、必要に応じた新しい SA の作成に使用できます。

IPsec セキュリティ アソシエーション アイドル タイマーの前提条件

インターネット キー エクスチェンジ（IKE）は、『*Cisco IOS XE Security Configuration Guide*』の「Configuring Internet Key Exchange Security Protocol」の章に従って設定する必要があります。

IPsec セキュリティ アソシエーション アイドル タイマーに関する情報

IPsec セキュリティ アソシエーションのライフタイム

現在、Cisco IOS ソフトウェアでは、IPsec SA のライフタイムの設定が可能です。ライフタイムは、グローバルに、またはクリプトマップごとに設定できます。ライフタイムには、「指定時刻」ライフタイムと「トラフィック量」ライフタイムの2つがあります。これらのライフタイムに到達すると、セキュリティ アソシエーションが期限切れになります。

IPsec SA アイドル タイマー

IPsec SA アイドル タイマーは、IPsec SA のグローバル ライフタイムとは異なります。グローバルライフタイムの有効期間は、ピアのアクティビティとは独立しています。IPsec SA アイドル タイマーを使用すれば、非アクティブなピアに関連付けられた SA を、グローバル ライフタイムが期限切れになる前に削除できます。

IPsec SA アイドル タイマーが設定されていない場合、IPsec SA のグローバル ライフタイムだけが適用されます。SA は、ピアのアクティビティと関わりなく、グローバル タイマーが有効期限切れになるまで維持されます。

（注） アイドル タイマーの期限切れのために、特定のピアに対する最新の IPsec SA が削除された場合、そのピアに対する IKE も削除されます。

IPsec セキュリティ アソシエーション アイドル タイマーの設定方法

IPSec SA アイドル タイマーのグローバルな設定

このタスクでは、IPsec SA アイドル タイマーをグローバルに設定します。このアイドル タイマーの設定は、すべての SA に適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ipsec security-association idle-time** *seconds*

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： `Router> 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： `Router# 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 security-association idle-time** *seconds* 例： `Router(config)# crypto ipsec security-association idle-time 600`	IPsec SA アイドル タイマーを設定します。 • *seconds* 引数では、アイドル タイマーが非アクティブ ピアによる SA の維持を許可する時間を秒単位で指定します。*seconds* 引数の有効な値の範囲は 60 ～ 86400 です。

IPSec SA アイドル タイマーのクリプト マップ単位での設定

このタスクでは、指定されたクリプト マップの IPsec SA アイドル タイマーを設定します。アイドル タイマーの設定は、指定されたクリプト マップ下のすべての SA に適用されます。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto map** *map-name seq-number* **ipsec-isakmp**
4. **set security-association idle-time** *seconds*

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： `Router> 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： `Router# 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。

	コマンドまたはアクション	目的
ステップ 3	**crypto map** *map-name seq-number* **ipsec-isakmp** 例： `Router(config)# crypto map test 1 ipsec-isakmp`	クリプト マップ エントリを作成または変更し、クリプト マップ 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	**set security-association idle-time** *seconds* 例： `Router(config-crypto-map)# set security-association idle-time 600`	デフォルト ピアが使用される前に、現在のピアをアイドル状態にしておける最大期間を指定します。 • *seconds* 引数は、デフォルト ピアが使用される前に現在のピアをアイドル状態にできる秒数です。有効値は 60 ～ 86400 です。

IPsec セキュリティ アソシエーション アイドル タイマーの設定例

IPsec SA アイドル タイマー のグローバル設定例

次に、IPsec SA アイドル タイマー をグローバルに設定して、600 秒後に非アクティブなピアの SA を廃棄している例を示します。

```
crypto ipsec security-association idle-time 600
```

暗号マップごとの IPsec SA アイドル タイマーの設定例

次に、test という名前のクリプト マップの IPsec SA アイドル タイマーを設定して、600 秒後に非アクティブなピアの SA を廃棄している例を示します。

```
crypto map test 1 ipsec-isakmp
 set security-association idle-time 600
```

その他の参考資料

ここでは、IPsec セキュリティ アソシエーション アイドル タイマー機能の関連資料について説明します。

関連資料

関連項目	マニュアル タイトル
IKE の設定に関する追加情報	「Internet Key Exchange for IPsec VPNs」

関連項目	マニュアル タイトル
IPsec SA のグローバル ライフタイムの設定に関する追加情報	• IPsec を使用した VPN のセキュリティの設定 • IPSEC 優先ピア
追加セキュリティ コマンド	『Cisco IOS Security Command Reference』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	---

シスコのテクニカル サポート

説明	リンク
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

IPsec セキュリティ アソシエーション アイドル タイマーの機能仕様

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 : IPsec* セキュリティ アソシエーション アイドル タイマーの機能仕様

機能名	リリース	機能情報
IPsec SA アイドル タイマー	Cisco IOS XE Release 2.1	Cisco IOS XE ソフトウェアを実行しているルータによってピアの IPsec セキュリティ アソシエーション（SA）が作成される場合、その SA を維持するためにリソースを割り当てる必要があります。SA には、メモリと、複数の管理されたタイマーが必要です。ピアがアイドル状態だと、それらのリソースが無駄になってしまいます。あまりに多くのリソースがアイドル状態のピアによって浪費されてしまうと、ルータによる他のピアとの新しい SA の作成ができなくなる可能性があります。IPsec SA アイドル タイマー機能では、SA のアクティビティをモニタリングするための、設定可能なアイドル タイマーが導入されており、これにより、アイドル状態のピアの SA を削除できます。 次のコマンドが導入または変更されました。**crypto ipsec security-association idle-time**
	Cisco IOS XE Release 2.1	**set security-association idle-time** コマンドが追加され、指定された暗号マップに対する IPsec アイドル タイマーの設定が可能になりました。 次のコマンドが導入または変更されました。**set security-association idle-time**。

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。