IPsec SA アイドル タイマー

Cisco IOS ソフトウェアを実行しているルータによってピアの IPsec Security Association（SA; セキュリティ アソシエーション）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。この機能の利点は次のとおりです。

- 向上したリソースの可用性
- 改善された Cisco IOS IPsec 配置のスケーラビリティ

IPsec SA アイドル タイマーの機能仕様

機能の履歴	
リリース	**変更点**
12.2(15)T	この機能が追加されました。
12.3(14)T	**set security-association idle-time** コマンドが追加され、指定されたクリプト 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。
サポートされているプラットフォーム	
Cisco 1700 シリーズ アクセス ルータ、Cisco 2400 シリーズ統合アクセス 装置、Cisco 2600 シリーズ マルチサービス プラットフォーム、Cisco 3600 シリーズ マルチサービス プラットフォーム、Cisco 3700 シリーズ マルチサービス アクセス ルータ、Cisco 7100 シリーズ VPN ルータ、Cisco 7200 シリーズ ルータ、Cisco 7400 シリーズ ルータ、Cisco 7500 シリーズ ルータ、Cisco 801–804 ISDN ルータ、Cisco 805 シリアル ルータ、Cisco 806 ブロードバンド ルータ、Cisco 811、Cisco 813、Cisco 820、Cisco 827 ADSL ルータ、Cisco 828 G.SHDSL ルータ、Cisco 8850-RPM、Cisco 950、Cisco AS5350 ユニバーサル ゲートウェイ、Cisco AS5400 シリーズ ユニバーサル ゲートウェイ、Cisco 統合通信システム 7750、Cisco MC3810 シリーズ マルチサービス アクセス コンセントレータ、Cisco ubr7200、Cisco ubr900 シリーズ ケーブル アクセス ルータ	

プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索するには

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco IOS ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。アクセスには、Cisco.com のアカウントが必要です。アカウントを持っていないか、ユーザ名またはパスワードが不明の場合は、ログイン ダイアログボックスの [Cancel] をクリックし、表示される指示に従ってください。

この章の構成

IPsec SA アイドル タイマーの前提条件

「*Internet Key Exchange for IPsec VPNs*」で記述したとおりに Internet Key Exchange（IKE; インターネット キー エクスチェンジ）を設定する必要があります。

IPsec SA アイドル タイマーに関する情報

IPsec SA アイドル タイマー機能を設定するには、次の概念を理解しておく必要があります。

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 種類があります。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 SA アイドル タイマーの利点

向上したリソースの可用性

IPsec SA アイドル タイマー機能を設定すると、アイドル状態のピアに関連付けられた SA が削除されることによって、リソースの可用性が増加します。

改善された Cisco IOS IPsec 配置のスケーラビリティ

IPsec SA アイドル タイマー機能によって、アイドル状態のピアによるリソースの無駄遣いを防止できるので、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 SA アイドル タイマーの設定方法

IPsec SA Idle Timer 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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
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。

クリプト マップごとの IPsec SA アイドル タイマーの設定

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。

（注） この設定タスクは、Cisco IOS Release 12.3(14)T から有効になりました。

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 モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
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 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 SA アイドル タイマーの設定例

IPsec SA アイドル タイマー のグローバルな設定例

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
```

クリプト 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
```

（注） 上記の設定は、Cisco IOS Release 12.3(14)T までは使用できませんでした。

その他の参考資料

IPsec SA アイドル タイマー の関連資料については、次の項を参照してください。

関連資料

内容	参照先
IKE の設定に関する追加情報	「*Internet Key Exchange for IPsec VPNs*」
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	• 「*Configuring Security for VPNs with IPsec*」 • 「*IPsec Preferred Peer*」
追加セキュリティ コマンド	『*Cisco IOS Security Command Reference*』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの MIB を検索してダウンロードする場合は、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
なし	—

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。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する 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/techsupport

コマンド リファレンス

次のコマンドは、このモジュールに記載されている機能または機能群において、新たに導入または変更されたものです。

- **crypto ipsec security-association idle-time**
- **set security-association idle-time**

これらのコマンドの詳細については、『Cisco IOS Security Command Reference』（http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_book.html）を参照してください。

Cisco IOS の全コマンドを参照する場合は、Command Lookup Tool（http://tools.cisco.com/Support/CLILookup）にアクセスするか、または『*Master Command List*』を参照してください。