IPsec SNMP サポート

IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。

この機能のコマンドを使用すれば、IPsec MIB 機能のバージョンを確認したり、SNMP トラップをディセーブルにしたり、この機能によって使用されるバッファのサイズをモニタリングおよび制御したりできます。

（注） このマニュアルでは、Cisco IPsec MIB の Cisco IOS XE CLI サポートを中心に説明します。また、このマニュアルでは現在サポートされている MIB の要素も示します。このマニュアルでは、Cisco IPsec MIB の（ネットワーク管理ステーションからの）SNMP 設定については説明しません。

IPsec SNMP サポートの制限事項

- IPsec--SNMP サポート機能でサポートされるトンネル設定エラー ログは次のものだけです。
  - NOTIFY_MIB_IPSEC_PROPOSAL_INVALID
  - 「A tunnel could not be established because the peer did not supply an acceptable proposal.」
  - NOTIFY_MIB_IPSEC_ENCRYPT_FAILURE
  - 「A tunnel could not be established because it failed to encrypt a packet to be sent to a peer.」
  - NOTIFY_MIB_IPSEC_SYSCAP_FAILURE
  - 「A tunnel could not be established because the system ran out of resources.」

- NOTIFY_MIB_IPSEC_LOCAL_FAILURE
- 「A tunnel could not be established because of an internal error.」

これらのエラー通知はエラーテーブルに記録されますが、SNMP 通知（トラップ）としては使用できないことに注意してください。

- 次の機能は、IPsec MIB 機能ではサポートされていません。
  - チェックポインティング
  - CISCO-IPSEC-MIB の Dynamic Cryptomap テーブル
- CISCO-IPSEC-POLICY-MAP-MIB（ciscoIpSecPolMap）で定義されている通知はありません（「IPSec Policy Map Notifications Group」は空です）。

IPsec SNMP サポートの情報

IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。

IPsec MIB を使用すれば、SNMP を使用した IPsec 設定のモニタリングおよび IPsec ステータスのモニタリングが可能です。また、IPsec MIB を各種バーチャル プライベート ネットワーク（VPN）ソリューションに統合できます。

たとえば、この機能を使用すれば、Cisco IOS XE CLI を使用して、トンネル履歴テーブルやトンネル エラー テーブルのサイズを細かく指定できます。履歴テーブルには、トンネルに関する属性および統計情報がアーカイブされます。エラーテーブルには、トンネルのエラーの原因とエラーが発生した時刻がアーカイブされます。エラー履歴テーブルは、トンネルの終了が通常のものか異常なものかを区別するための簡単な手段として使用できます。つまり、トンネル履歴テーブル内のトンネル エントリに関連するエラー レコードがない場合、トンネルは正常に終了したことになります。ただし、すべてのエラーがトンネルのものとは限らないので、トンネル履歴テーブルがすべてのエラーテーブルを伴うわけではありません。そのため、サポート対象の設定エラーはエラーテーブルに記録されますが、関連する履歴テーブルは、トンネルが設定されていないので、記録されません。

この機能では、ネットワーク管理システムで使用される IPsec 簡易ネットワーク管理プロトコル（SNMP）通知も提供されます。

関連機能およびテクノロジー

IPsec--SNMP サポート機能は、VPN Device Manager（VDM）をサポートするように設計されました。VDM によって、ネットワーク管理者は、Web ブラウザから単一デバイス上のサイト間 VPN を管理および設定でき、また、リアルタイムで変更の効果を確認できます。VDM では、IPsec プロトコルを使用したサイト間 VPN の設定プロセスを簡単にするために、ウィザードベースのグラフィカル ユーザ インターフェイス（GUI）が実装されます。VDM ソフトウェアは Cisco VPN ルータに直接インストールされます。また、VDM ソフトウェアは、次世代の Device Manager 製品で使用でき、互換性を保つように設計されています。

IPsec SNMP サポートの設定方法

IPsec SNMP 通知のイネーブル化

IPsec SNMP 通知をイネーブルにするには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps ipsec cryptomap** [**add** | **delete** | **attach** | **detach**]
4. **snmp-server enable traps isakmp** [**policy** {**add** | **delete**} | **tunnel** {**start** | **stop**}]
5. **snmp-server host** *host-address* **traps** *community-string* **ipsec**

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	**snmp-server enable traps ipsec cryptomap** [**add**	**delete**	**attach**	**detach**] 例： `Router (config)# snmp-server enable traps ipsec cryptomap add`	ルータを、IPsec SNMP 通知を送信するようにルータをイネーブルにします。
ステップ 4	**snmp-server enable traps isakmp** [**policy** {**add**	**delete**}	**tunnel** {**start**	**stop**}] 例： `Router (config)# snmp-server enable traps isakmp policy add`	ルータを、IPsec ISAKMP SNMP 通知を送信するようにルータをイネーブルにします。
ステップ 5	**snmp-server host** *host-address* **traps** *community-string* **ipsec** 例：	IPsec SNMP 通知動作の受信者を指定します。

	コマンドまたはアクション	目的
	`Router (config)# snmp-server host my.example.com traps version2c`	

次のタスク

SNMP の設定の詳細については、『*Cisco IOS XE Configuration Fundamentals Configuration Guide*』の「Configuring SNMP Support」章を参照してください。

IPsec エラー履歴テーブルのサイズの設定

デフォルトのエラー履歴テーブルのサイズは200です。エラー履歴テーブルのサイズを変更するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto mib ipsec flowmib history failure size** *number*

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 mib ipsec flowmib history failure size** *number* 例： `Router (config)# crypto mib ipsec flowmib history failure size 220`	IPsec エラー履歴テーブルのサイズを変更します。

IPsec トンネル履歴テーブルのサイズの設定

デフォルトのトンネル履歴テーブルのサイズは200です。トンネル履歴テーブルのサイズを変更するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto mib ipsec flowmib history tunnel size** *number*

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 mib ipsec flowmib history tunnel size** *number* 例： `Router (config)# crypto mib ipsec flowmib history tunnel size`	IPsec トンネル履歴テーブルのサイズを変更します。

IPsec MIB 設定の確認

IPsec MIB 機能が正しく設定されているかどうかを確認するには、次のタスクを実行します。

- **show crypto mib ipsec flowmib history failure size** 特権 EXEC コマンドを入力して、エラー履歴テーブルのサイズを表示します。

```
Router# show crypto mib ipsec flowmib history failure size
IPSec Failure Window Size: 140
```

- **show crypto mib ipsec flowmib history tunnel size** 特権 EXEC コマンドを入力して、トンネル履歴テーブルのサイズを表示します**:**

```
Router# show crypto mib ipsec flowmib history tunnel size
IPSec History Window Size: 130
```

- **show crypto mib ipsec flowmib version** 特権 EXEC コマンドを入力して、管理アプリケーションによって使用される MIB バージョンを表示して、フィーチャセットを識別します。

```
Router# show crypto mib ipsec flowmib version
IPSec Flow MIB version: 1
```

- **debug crypto mib** コマンドを入力して、IPsec MIB デバッグメッセージ通知を表示します。

```
Router# debug crypto mib
Crypto IPSec Mgmt Entity debugging is on
```

IPsec MIB のモニタおよびメンテナンス

IPsec MIB 情報のステータスをモニタリングするには、次のコマンドのいずれかを使用します。

手順の概要

1. **enable**
2. **show crypto mib ipsec flowmib history failure size**
3. **show crypto mib ipsec flowmib history tunnel size**
4. **show crypto mib ipsec flowmib version**

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	**show crypto mib ipsec flowmib history failure size** 例： `Router# show crypto mib ipsec flowmib history failure size`	IPsec エラー履歴テーブルのサイズを表示します。
ステップ 3	**show crypto mib ipsec flowmib history tunnel size** 例： `Router# show crypto mib ipsec flowmib history tunnel size`	IPsec トンネル履歴テーブルのサイズを表示します。
ステップ 4	**show crypto mib ipsec flowmib version** 例： `Router# show crypto mib ipsec flowmib version`	ルータによって使用される IPsec Flow MIB のバージョンを表示します。

IPsec SNMP サポートの設定例

IPsec 通知のイネーブル化の例

次に、IPsec 通知がイネーブルにされている例を示します。

```
snmp-server enable traps ipsec isakmp
```

次に、ルータが、ホスト nms1.example.com に IPsec 通知を送信するように設定されている例を示します。

```
snmp-server host nms1.example.com public ipsec isakmp
Translating "nms1.example.com"...domain server (172.00.0.01) [OK]
```

履歴テーブルのサイズの指定例

次に、指定したエラー履歴テーブルのサイズが 140 になっている例を示します。

```
crypto mib ipsec flowmib history failure size 140
```

次に、指定したトンネル履歴テーブルのサイズが 130 になっている例を示します。

```
crypto mib ipsec flowmib history tunnel size 130
```

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
AAA アカウンティングの設定	• 「Configuring Accounting」
IPsec VPN アカウンティングの設定	• 「Configuring Security for VPNs with IPsec」
基本 AAA RADIUS の設定	• Cisco.com にある『*Cisco IOS Security Configuration Guide: User Services*』の「Configuring RADIUS」の章
ISAKMP プロファイルの設定	「VRF Aware IPsec」
TACACS+ および RADIUS での権限レベル	• 「Configuring TACACS+」 • Cisco.com にある『*Cisco IOS Security Configuration Guide: User Services*』の「Configuring RADIUS」の章
IP セキュリティ、RADIUS、および AAA コマンド	『*Cisco IOS Security Command Reference*』
推奨される暗号化アルゴリズム	『Next Generation Encryption』

MIB

MIB	MIB のリンク
なし	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB を探して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

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

IPsec SNMP サポートの機能情報

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 : IPsec SNMP* サポートの機能情報

機能名	リリース	機能情報
IPsec SNMP サポート	Cisco IOS XE Release 2.1	IP セキュリティ（IPsec）SNMP サポート機能には、業界標準の IPsec MIB および Cisco IOS XE ソフトウェア固有の IPsec MIB が導入されています。 次のコマンドが導入または変更されました。**crypto mib ipsec flowmib history failure size, crypto mib ipsec flowmib history tunnel size, debug crypto mib, show crypto mib ipsec flowmib history failure size, show crypto mib ipsec flowmib history tunnel size, show crypto mib ipsec flowmib version, snmp-server enable traps ipsec, snmp-server enable traps isakmp, snmp-server host**。

用語集

CA ：認証局。認証局（CA）は、メッセージ暗号化用のセキュリティ証明書および公開キー（X509v3 証明書の形式）を発行および管理する、ネットワーク内のエンティティです。CA は、公開キー インフラストラクチャ（PKI）の一部として、デジタル証明書の要求側が提供した情報を確認するために登録局（RA）に問い合わせます。RA によって要求側の情報が確認されると、CA は証明書を発行できます。一般に、証明書には、オーナーの公開キー、証明書の失効日、およびそ公開キーのオーナーに関するその他の情報が含まれています。

IP Security ：「IPsec」を参照してください。

IPsec ：インターネット プロトコル セキュリティ。参加ピア間でのデータの機密性、整合性、および認証を提供するオープン スタンダードの枠組みです。IPsec では、これらのセキュリティ サービスが IP レイヤで実現されます。IPsec では、インターネット キー交換（IKE）によって、ローカル ポリシーに基づいたプロトコルおよびアルゴリズムのネゴシエーションが処理され、IPsec によって使用される暗号キーおよび認証キーが生成されます。IPsec は、1 組のホスト間、1 組のセキュリティ ゲートウェイ間、またはセキュリティ ゲートウェイとホスト間で 1 つ以上のデータ フローを保護するために使用できます。

Management Information Base ：「MIB」を参照してください。

MIB ：管理情報ベース。ネットワーク管理情報のデータベースです。これらの情報は、簡易ネットワーク管理プロトコル（SNMP）や共通管理情報プロトコル（CMIP）などのネットワーク管理プロトコルにより使用および保持されます。MIB オブジェクトの値は、SNMP コマンドまたは CMIP コマンドを使用して変更および取得できます。これらのコマンドは通常、グラフィカル ユーザ インターフェイス（GUI）のネットワーク管理システム（NMS）から実行します。MIB オブジェクトはツリー構造であり、ツリーにはパブリック（標準）ブランチとプライベート（独自）ブランチを含みます。

Simple Network Management Protocol ：「SNMP」を参照してください。

SNMP ：簡易ネットワーク管理プロトコル。アプリケーション層プロトコルであり、SNMP マネージャと SNMP エージェントとの通信に使用されるメッセージ形式を規定します。

trap ：重要なイベントを知らせるためのメッセージです。指定された重大な状況が発生したり、しきい値を超過した場合、SNMP エージェントから、ネットワーク管理システム、コンソール、または端末へ送信されます。

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。