GET VPN の GDOI MIB サポート

暗号化された既存の MIB はインターネット キー エクスチェンジ（IKE）および IP Security（IPsec）MIB であり、Group Domain of Interpretation（GDOI）には不十分です。GET VPN の GDOI MIB サポート機能では、RFC 6407、『The Group Domain of Interpretation』に MIB のサポートが追加されます。GDOI MIB IETF 標準規格に関連するオブジェクトのみがサポートされます。GDOI MIB .my ファイルは SNMP 管理ステーションにインポートして解析することにより、テーブル オブジェクトと階層情報を取得することができます。

GDOI MIB は、（トラップと呼ばれていた）オブジェクトおよび通知で構成されます。これには、GDOI グループ、グループ メンバー（GM）とキー サーバ（KS）のピア、および作成またはダウンロードされるポリシーに関する情報が含まれます。「get」操作のみが GDOI でサポートされます。

GET VPN の GDOI MIB のサポートを設定するには、「GET VPN の GDOI MIB サポートの設定」セクションを参照してください。

GET VPN の GDOI MIB サポートに関する情報

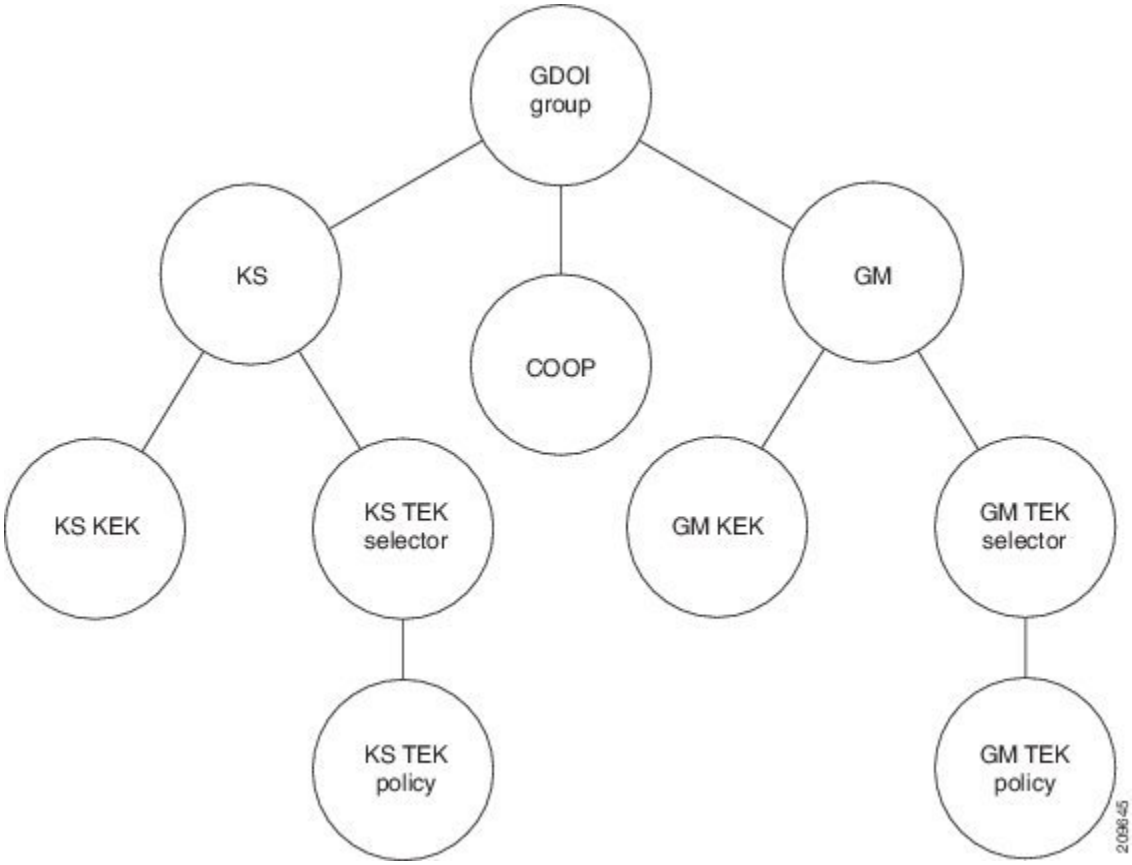
他の GET VPN ソフトウェア バージョンとの GDOI MIB の互換性

GET VPN の GDOI MIB サポート機能には、ネットワークのすべてのデバイスが GDOI MIB 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（プライマリ KS）で使用するコマンドが用意されています。詳細については、「GDOI MIB をサポートするソフトウェア バージョンを GM が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。

GDOI MIB テーブル階層

GDOI MIB オブジェクトは次の GDOI MIB テーブルで構成されます。次に、テーブル間の関係（階層）を示します。

図 *1 : GDOI MIB* テーブル階層



GDOI MIB テーブル オブジェクト

次は、MIB テーブル オブジェクトのリストです（グループごとにリスト）。

グループ テーブル オブジェクト：

- Group ID type：グループ ID が IP アドレス、グループ番号、ホスト名などのいずれであるかを指定します。
- Group ID length：グループ ID 値のオクテット数。
- Group ID value：グループ番号、IP アドレス、またはホスト名。
- Group name：文字列の値。
- Group member count：このグループに登録済みの KS 数を指定します。

- Group active peer KS count：このグループに対するアクティブな KS 数を指定します。
- Group last rekey retransmits：最後のキー再生成操作の一部として送信されたキー再生成メッセージと再送信メッセージの累積数を指定します。
- Group last rekey time taken：最後のキー再生成操作の完了に KS が費やした時間を指定します。

KS テーブル オブジェクト：

- KS ID type
- KS ID length
- KS ID value
- Active KEK：キー再生成メッセージを暗号化するために KS によって現在使用されている Key Encryption Key（KEK）の SPI。
- Last rekey sequence number：グループに KS から送信された最後のキー再生成番号。
- KS Role：プライマリまたはセカンダリ。
- Number of registered GMs：この KS に登録された GM の数。

COOP テーブル オブジェクト：

- COOP peer ID type
- COOP peer ID length
- COOP peer ID value
- COOP peer ID role：プライマリまたはセカンダリ
- COOP peer status：アライブ、デッド、または不明
- Number of registered GMs：この COOP ピアに登録された GM の数

GM テーブル：

- GM ID type
- GM ID length
- GM ID value
- Registered KS ID type：GM が登録されている KS の ID タイプ。
- Registered KS ID length
- Registered KS ID value
- Active KEK：キー再生成メッセージの復号化に GM が現在使用している KEK の SPI。
- Last rekey seq number：GM が受信した最後のキー再生成番号。

- Count of active TEKs：データプレーン トラフィックの暗号化/復号化/認証のために GM によって使用されるアクティブな TEK の数。

KS KEK テーブル：

- KEK index
- KEK SPI
- KEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- KEK source ID port：送信元 ID に関連付けられたポート。
- KEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- KEK destination ID port：宛先 ID に関連付けられたポート。
- IP protocol ID：UDP または TCP。
- キー管理アルゴリズム（未使用）。
- 暗号化アルゴリズムとキーの長さ（ビット）
- SIG ペイロード ハッシュ アルゴリズム、SIG ペイロード署名アルゴリズム、および SIG ペイロード キーの長さ（ビット）。
- ハッシュ アルゴリズム（IPsec MIB から再利用されます）
- Diffie-Hellman グループ
- KEK original lifetime (seconds)：KEK が有効である最長時間。
- KEK remaining lifetime (seconds)

KS TEK セレクタ テーブル（KS で GDOI グループ設定の IPsec SA の一部として設定された ACL に対応）：

- TEK selector index：トラフィック暗号キー（TEK）の整数のインデックス。
- TEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- TEK source ID port：送信元 ID に関連付けられたポート。
- TEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- TEK destination ID port：宛先 ID に関連付けられたポート。
- TEK Security protocol：SA TEK ペイロードの GDOI_PROTO_IPSEC_ESP プロトコル ID 値（RFC 6407 を参照）。

KS TEK ポリシー テーブル：

- TEK policy index：整数のインデックス。
- TEK SPI：4 つのオクテット

- Encapsulation mode：トンネルまたは転送。
- 暗号化アルゴリズムとキーの長さ（ビット）
- 整合性および認証アルゴリズムとキーの長さ（ビット）
- TBAR window size (seconds)
- TEK original lifetime (seconds)：TEK が有効である最長時間。
- TEK remaining lifetime (seconds)
- TEK Status：着信、発信、または不使用。

GM KEK テーブル：

- KEK index：整数のインデックス。
- KEK SPI
- KEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- KEK source ID port：送信元 ID に関連付けられたポート。
- KEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- KEK destination ID port：宛先 ID に関連付けられたポート。
- IP protocol ID：UDP または TCP。
- Key Management アルゴリズム（未使用）
- 暗号化アルゴリズムとキーの長さ（ビット）
- SIG ペイロード ハッシュ アルゴリズム、SIG ペイロード署名アルゴリズム、および SIG ペイロード キーの長さ（ビット）
- Hash algorithm
- Diffie-Hellman グループ
- KEK original lifetime (seconds)：KEK が有効である最長時間。
- KEK remaining lifetime (seconds)

GM TEK セレクタ テーブル（KS から TEK ポリシーの一部として GM にダウンロードされる ACL に対応）：

- TEK selector index：整数のインデックス。
- TEK source ID information：送信元 ID のタイプ、ID の長さ、および ID の値。
- TEK source ID port：送信元 ID に関連付けられたポート。
- TEK destination ID information：宛先 ID のタイプ、ID の長さ、および ID の値。
- TEK destination ID port：宛先 ID に関連付けられたポート。

- TEK Security protocol：SA TEK ペイロードの GDOI_PROTO_IPSEC_ESP プロトコル ID 値（RFC 6407 を参照）。

GM TEK ポリシー テーブル：

- TEK policy index：整数のインデックス。
- TEK SPI：4 つのオクテット。
- Encapsulation mode：トンネルまたは転送。
- 暗号化アルゴリズムとキーの長さ（ビット）
- 整合性および認証アルゴリズムとキーの長さ（ビット）
- TBAR window size (seconds)
- TEK original lifetime (seconds)：TEK が有効である最長時間。
- TEK remaining lifetime (seconds)
- TEK Status：着信、発信、または不使用。

GDOI MIB 通知

GDOI MIB は次の表の Simple Network Management Protocol（SNMP）通知をサポートしています。GDOI MIB には、KS によって生成された通知と各 GM によって生成された通知の 2 種類の通知があります。任意の組み合わせの通知（またはすべての通知）を有効にできます。

表 *1 : GDOI MIB* にサポートされる *SNMP* 通知

通知	説明
KS New Registration	KS が GM から最初に登録要求を受信した。
KS Registration Complete	GM が KS への登録を完了した。
KS Rekey Pushed	キー再生成メッセージが KS によって送信された。
KS No RSA Keys	RSA キーが見つからないために KS からエラー通知が受信された。
GM Register	GM が KS に最初の登録要求を送信した。
GM Registration Complete	GM が KS への登録を完了した。
GM Re-Register	GM が KS への登録プロセスを開始した。
GM Rekey Received	キー再生成メッセージが GM で受信された。
GM Incomplete Config	GM が設定の不足によるエラー通知を送信した。

通知	説明
GM Rekey Failure	GM がキー再生成の処理とインストールができないため、エラー通知を送信した。
KS Role Change	KS がプライマリとセカンダリ ロールを切り替えた。
KS GM Deleted	GM が KS から削除されると生成されます。
KS Peer Reachable	到達不能な COOP ピアが到達可能になると KS によって生成されます。
KS Peer Unreachable	到達可能な COOP ピアが到達不能になると KS によって生成されます。

詳細については、「GDOI MIB 通知の有効化」セクションを参照してください。

GDOI MIB の制限

GDOI MIB には RFC 6407 にリストされているオブジェクトのみが含まれ、GDOI のシスコ実装に固有の機能のためのオブェクトは含まれません。リストでは次の演算を使用します。

- 連携キー サーバ
- GM ACL
- 受信専用 SA
- Fail-Close またはフェール オープン
- 暗号マップ オブジェクト
- 他の Cisco GET VPN 固有の機能

GET VPN の GDOI MIB サポートの設定方法

GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する

GET VPN ネットワーク内のすべてのデバイスが GDOI MIB をサポートすることを確認するには、KS（またはプライマリ KS）でこの作業を実行します。

手順の概要

1. **enable**
2. **show crypto gdoi feature gdoi-mib**

3. **show crypto gdoi feature gdoi-mib | 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 gdoi-mib** 例： `Device# show crypto gdoi feature gdoi-mib`	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 GDOI MIB 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 gdoi-mib	include No** 例： `Device# show crypto gdoi feature gdoi-mib	include No`	（オプション）GDOI MIB をサポートしないデバイスのみ検索します。

SNMP コミュニティのアクセス コントロールの作成

SNMP へのアクセスを許可するために、KS または GM 上の SNMP マネージャと SNMP エージェント間の関係を定義する SNMP コミュニティ アクセス文字列を指定します。このコミュニティ アクセス文字列は、デバイス上のエージェントへのアクセスを制御するパスワードのように機能します。

コミュニティ アクセス文字列を指定するにはこの作業を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server community** *community-string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-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	**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	**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	**snmp-server community** *community-string* [**view** *view-name*] [**ro** | **rw**] [**ipv6** *nacl*] [*access-list-number* | *extended-access-list-number* | *access-list-name*] 例： `Device(config)# snmp-server community mycommunity`	コミュニティ アクセス文字列を指定します。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

コミュニティ アクセス文字列の指定に関する詳細については、『*SNMP Configuration Guide*』の「Configuring SNMP Support」モジュールを参照してください。**snmp-server community** コマンドに関する詳細（シンタックスと使用法に関するガイドラインを含む）については、『Cisco IOS SNMP Support Command Reference』を参照してください。

SNMP マネージャとの通信の有効化

KS の SNMP エージェントまたは GM と SNMP マネージャ間の通信を有効にするには、このタスクを実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server host** {*hostname* | *ip-address*} **version** {**1** | **2c** | **3**} *community-string*
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	**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：	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
	`Device# configure terminal`	
ステップ 3	**snmp-server host** {*hostname* | *ip-address*} **version** {**1** | **2c** | **3**} *community-string* 例： `Device(config)# snmp-server host 209.165.200.225 version 2c mycommunity`	ホストがSNMP通知を受信するように指定します。 • 2c は通常 SNMP バージョンとして使用されます。
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

SNMP マネージャとの通信を有効にする方法についての詳細は、『*SNMP Configuration Guide*』の「Configuring SNMP Support」モジュールを参照してください。**snmp-server host** コマンドに関する詳細（シンタックスと使用法に関するガイドラインを含む）については、『Cisco IOS SNMP Support Command Reference』を参照してください。

GDOI MIB 通知の有効化

KS または GM の GDOI MIB 通知を有効にするには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **snmp-server enable traps gdoi** [*notification-type*]
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	**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。

	コマンドまたはアクション	目的
ステップ 3	**snmp-server enable traps gdoi** [*notification-type*] 例： `Device(config)# snmp-server enable traps gdoi gm-registration-complete gm-rekey-rcvd ks-new-registration ks-reg-complete`	有効にする特定のSNMP通知を指定します。任意の順序で次の種類を組み合わせて指定できます。次のキーワードなしでコマンドを入力すると、すべてのGDOI MIB 通知が有効になります。 • **gm-incomplete-cfg**：設定が見つからないためGM がエラー通知を送信しました。 • **gm-re-register**：GM が KS で登録プロセスを開始しました。 • **gm-registration-complete**：GM が KS への登録を完了しました。 • **gm-rekey-fail**：キー再生成を正常に処理およびインストールできないため、GM がエラー通知を送信しました。 • **gm-rekey-rcvd**：GM がキー再生成メッセージを受信しました。 • **gm-start-registration**：GM が最初の登録要求をKS に送信しました。 • **ks-new-registration**：KS が最初の登録要求をGMから受信しました。 • **ks-no-rsa-keys**：RSA キーが見つからないためKS からのエラー通知を受信しました。 • **ks-reg-complete**：GM が KS への登録を完了しました。 • **ks-rekey-pushed**：KS からキー再生成メッセージが送信されました。 • **ks-gm-deleted**：GM が KS によって削除されます。 • **ks-peer-reachable**：到達不能な COOP ピアが到達可能になります。 • **ks-peer-unreachable**：到達可能な COOP ピアが到達不能になります。 • **ks-role-change**：KS の役割がプライマリからセカンダリ（またはその逆）に変更されます。

	コマンドまたはアクション	目的
ステップ 4	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、設定を保存して、特権 EXEC モードに戻ります。

GET VPN 用の GDOI MIB サポートの設定例

例：GDOI MIB をサポートするソフトウェア バージョンを GM が実行していることを確認する

次の例は、ネットワーク内のすべてのデバイスが GDOI MIB 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 gdoi-mib

Group Name: GET
 Key Server ID       Version   Feature Supported
    10.0.8.1         1.0.2          Yes
    10.0.9.1         1.0.2          Yes
    10.0.10.1        1.0.2          Yes
    10.0.11.1        1.0.2          Yes
 Group Member ID     Version   Feature Supported
    10.0.11.2          1.0.2          Yes
    10.0.11.3          1.0.1          No
```

次の例は、GDOI MIB をサポートしていないデバイスのみを検索する方法を示します。

```
Device# show crypto gdoi feature gdoi-mib | include No

       10.0.11.3          1.0.1          No
```

例：SNMP コミュニティのアクセス コントロールの作成

次の例では、SNMP へのアクセスを許可するために、KS または GM 上の SNMP マネージャと SNMP エージェント間の関係を定義するために mycommunity という名前の SNMP コミュニティ文字列を指定する方法を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server community mycommunity
Device(config)# end
```

例：SNMP マネージャとの通信の有効化

次に、SNMP マネージャとの通信を有効化する例を示します。この例では、すでに作成されている mycommunity という名前のコミュニティ文字列を使用します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server host 209.165.200.225 version 2c mycommunity
Device(config)# end
```

例：GDOI MIB 通知の有効化

次に、GDOI MIB 通知を有効化する例を示します。

```
Device> enable
Device# configure terminal
Device(config)# snmp-server enable traps gdoi gm-registration-complete gm-rekey-rcvd
ks-new-registration ks-reg-complete
Device(config)# end
```

GET VPN 用の GDOI MIB サポート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
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command References*』
SNMP の設定	• 『SNMP Configuration Guide, Cisco IOS Release 15.2M&T』の「Configuring SNMP Support」モジュール • 『Cisco IOS SNMP Support Command Reference』

MIB

MIB	MIB のリンク
CISCO-GDOI-MIB	選択したプラットフォーム、Cisco ソフトウェア リリース、およびフィーチャ 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

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 用の GDOI MIB 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 *2 : GET VPN* 用の *GDOI MIB* サポートの機能情報

機能名	リリース	機能情報
GET VPN の GDOI MIB サポート		この機能は、IETF RFC 6407『The Group Domain of Interpretation』用の MIB サポートを追加します。この機能は、GDOI MIB の IETF 標準に関連したオブジェクトのみをサポートします。またこの機能は、ネットワーク上のデバイスが GDOI MIB をサポートする GET VPN ソフトウェアのバージョンを実行しているかどうかを表示するコマンドも提供します。 GDOI MIB は、GDOI グループ、GM と KS ピア、および作成またはダウンロードされたポリシーに関する情報が含まれるオブジェクトと通知から構成されます。 次のコマンドが導入されました。 **snmp-server enable traps gdoi.**
XE 3.16 GETVPN GDOI/COOP MIBS		次のコマンドが変更されました。 **snmp-server enable traps 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。