GETVPN G-IKEv2

Cisco Group Encrypted Transport VPN（GET VPN）には、シスコ デバイス上で発生する、またはシスコ デバイスを経由するエンタープライズ プライベート WAN 上の IP マルチキャスト トラフィック グループまたはユニキャスト トラフィックの安全を守るために必要な一連の機能が含まれます。GETVPN G-IKEv2 機能は GETVPN にインターネット キー エクスチェンジ バージョン 2（IKEv2）プロトコルを実装するため、GETVPN は IKEv2 のメリットを享受できます。

GETVPN G-IKEv2 の制約事項

- キー サーバ（KS）には Group Key Management（GKM）と Group Domain of Interpretation（GDOI）の両方を設定できますが、グループ メンバー（GM）には GKM と GDOI のいずれかを設定できます。
- COOP 用の IKEv2 はサポートされていません。G-IKEv2 セットアップではキーサーバー間の COOP に IKEv1 を使用してください。
- EAP は現在、G-IKEv2 ではサポートされていません。
- GETVPN G-IKEv2 は IP-D3P をサポートしていません。G-IKEv2 を使用した IP-D3P は、引き続き GETVPN グループメンバー（GM）でサポートされています。

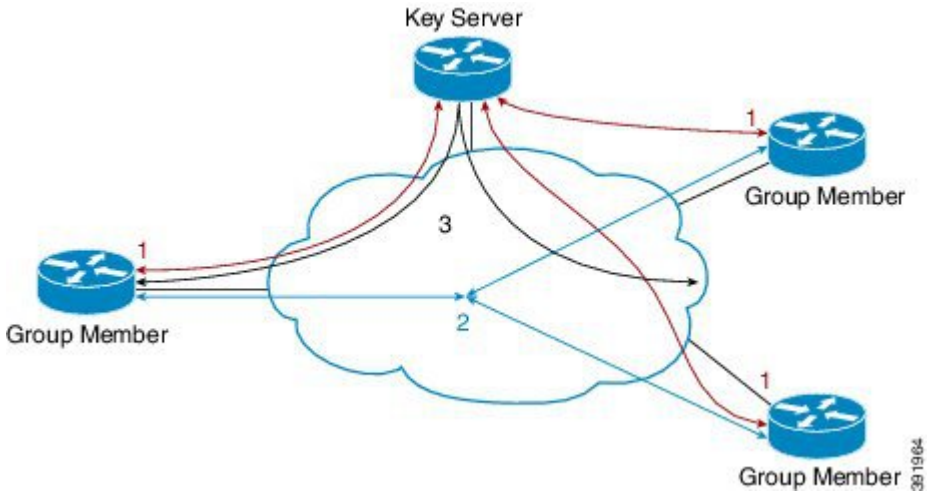
GETVPN G-IKEv2 に関する情報

GETVPN G-IKEv2 の概要

Cisco Group Encrypted Transport バーチャル プライベート ネットワーク（GETVPN）アーキテクチャは、Group Domain of Interpretation（GDOI）プロトコルに基づいています。GETVPN では、Internet Security Exchange and Key Management Protocol（ISAKMP）を使用して、新しいグループ メンバーの認証、暗号化ポリシーのダウンロード、およびグループ メンバーへのトラフィック暗号キー（TEK）と Key Encryption Key（KEK）の配信を行います。ただし、インターネット キー エクスチェンジ バージョン 2（IKEv2）は置き換えられます。IKEv2 は、ネットワーク遅延を軽減し、メッセージ交換の複雑さを軽減し、相互運用性と信頼性を向上させ、ハッシュ認証の暗号化の問題を修正します。GET VPN は IKEv2 プロトコルと IPsec を組み合わせ、GETVPN G-IKEv2 機能によって IP マルチキャスト トラフィックまたはユニキャスト トラフィックを保護する効果的な方法を提供します。この機能では、シスコのすべての VPN Technologies を利用して完全な IKEv2 ソリューションを提供します。

G-IKEv2 プロトコルは、グループ メンバー（GM）に対し、キー サーバ（KS）からポリシーおよびキーをダウンロードするメカニズムを提供します。これらのポリシーおよびキーは、グループ内の GM 間の通信を保護するために使用されます。G-IKEv2 は、企業のプライベート WAN におけるリモート ロケーション間のグループ通信を保護する新しいモデルです。次の図は、G-IKEv2 を使用して GM を KS に登録し、KS から GM にキーおよびポリシーをダウンロードする GETVPN の基本システム アーキテクチャを示しています。

図 *1: G-IKEv2* プロトコルを使用する *GETVPN* アーキテクチャ



インターネット キー エクスチェンジ バージョン 2（IKEv2）

RFC 4306 に基づく次世代のキー管理プロトコルであるインターネット キー エクスチェンジ バージョン 2（IKEv2）は、IKE プロトコルの機能拡張です。IKEv2 は、相互認証を実行して

SA を確立および管理するために使用します。IKEv2 の詳細については、『*FlexVPN and Internet Key Exchange Version 2 Configuration Guide*』を参照してください。

次の表では、IKE と IKEv2 間のトンネル パフォーマンスを比較します。

プロトコル	1 秒あたりのトンネル数	最大同時トンネル数
IKE	45	60
IKEv2	89	200

IKEv2 の利点は次のとおりです。

デッド ピア検出とネットワーク アドレス変換トラバーサル

インターネット キー エクスチェンジ バージョン 2（IKEv2）にはデッド ピア検出（DPD）とネットワーク アドレス変換トラバーサル（NAT-T）のサポートが組み込まれています。

証明書の URL

証明書はIKEv2パケット内で送信されるのではなくURLとハッシュを通じて参照できるため、フラグメンテーションを回避できます。

DoS 攻撃の復元力

IKEv2は、要求者を確認するまで要求を処理しません。これにより、偽の場所から大量の暗号化（高コスト）処理を実行するようにスプーフィングされる可能性があるIKEv1でのサービス妨害（DoS）の問題にある程度対処しています。

EAP のサポート

IKEv2 では認証に Extensible Authentication Protocol（EAP）を使用できます。

複数の暗号エンジン

ネットワークに IPv4 と IPv6 の両方のトラフィックがあり、複数の暗号エンジンがある場合、次のいずれかの設定オプションを選択します。

- 1 つのエンジンで IPv4 トラフィックを処理し、他方のエンジンで IPv6 トラフィックを処理する。
- 1 つのエンジンで IPv4 と IPv6 の両方のトラフィックを処理する。

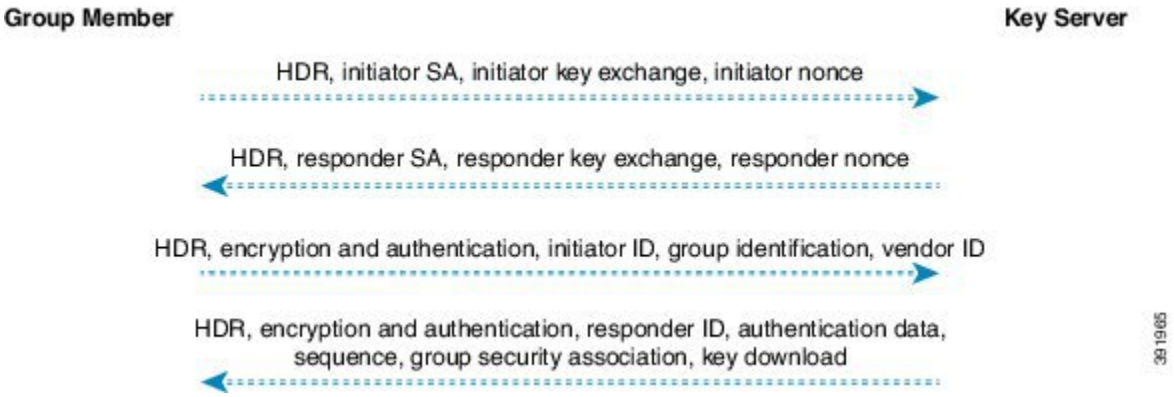
信頼性と状態管理（ウィンドウイング）

IKEv2 では、信頼性を提供するためにシーケンス番号と確認が使用され、エラー処理ロジスティックと共有状態管理が要求されます。

GETVPN G-IKEv2 の交換

GM と KS 間のメッセージ交換は、IKEv2 の標準ドラフトを使用する Internet Engineering Task Force（IETF）のグループ キー管理に準拠しています。

図 *2 : G-IKEv2* メッセージ交換



1. グループ メンバーは、優先される暗号化アルゴリズム（SAi ペイロード）、発信側のキー交換（KE）フェーズ 1 ペイロードの Diffie-Hellman 公開番号、および発信側のナンス ペイロードの存在を保証するための乱数であるナンスを送信することによってキー サーバへの登録要求を開始します。
2. キー サーバはネゴシエート済みの暗号化アルゴリズム（応答側の SA フェーズ 1 ペイロード）、Diffie-Hellman 公開番号（応答側の KE ペイロード）、ナンス（応答側のナンス ペイロード）を使用して応答します。オプションで、認証方式として Rivest、Shamir、Adleman（RSA）デジタル署名を使用するようにキー サーバが設定されている場合、キー サーバも証明書要求を送信します。
3. 登録要求に対するキー サーバの応答を受信すると、グループ メンバーは SAr1 ペイロードの暗号化アルゴリズムと Diffie-Hellman 値を使用してキーを作成し、キー サーバに送信されるメッセージを暗号化します。RSA デジタル署名が認証方式として使用される場合、暗号化されたメッセージには、発信側の ID と、オプションで証明書および証明書要求が含まれます。スイート B の実装の場合、Galois/Counter Mode（GCM）–Advanced Encryption Standard（AES）または Galois Message Authentication Code（GMAC）–Advanced Encryption Standard（AES）トランスフォームとともに使用される送信者 ID を要求するために通知ペイロードが送信されます。

（注） グループ メンバーは、1 日のライフタイムの間、インターフェイスに適用可能な一連の送信元 ID を要求します。登録（長い SA ライフタイムの場合）またはキー再生成（短い SA ライフタイムの場合）のメッセージでライフタイムを受け取ると、グループ メンバーは将来の登録のため送信者 ID の数を計算するためにライフタイムを保存します。

4. グループ マネージャの認証後、キー サーバはグループ マネージャを登録する前にグループ メンバーを承認します。登録後、キー サーバはグループ マネージャにグループ ポリ

シー（GSA ペイロード）およびグループのキーイング マテリアル（KD ペイロード）を送信します。SEQ ペイロードはオプションであり、キー サーバでキー再生成メッセージの現在のシーケンス番号をグループ マネージャに通知する場合に送信されます。これらのペイロードは、GSA_AUTH 応答メッセージに含められます。

グループ メンバーの通信

グループ メンバーは相互に IPsec トンネルを確立するのではなく、IPsec ポリシーおよびキーを使用してグループ内のグループ メンバー間の通信を保護します。

将来の登録

セキュアな登録チャネルがグループ マネージャとキー サーバとの間に確立されると、そのほかのグループの追加のグループ メンバー登録は、確立されたセキュアな登録チャネルを通じて行われます。そのようなシナリオでは、グループ メンバーはグループ ID（IDg）を含む GSA_CLIENT_SERVER 交換を使用して、キー サーバから Key Encryption Key（KEK）またはトラフィック暗号キー（TEK）のいずれかを要求します。

キー サーバのキー再生成

キー サーバはユニキャストまたはマルチキャスト通信を介して G-IKEv2 グループ メンテナンス チャネルを使用するグループ メンバーに新しいグループ キーを配布します。キー再生成は G-IKEv2 のオプションです。キー再生成を使用すると、KS はグループ メンバーにキー再生成メッセージを送信します。このメッセージはキー サーバの設定に応じてユニキャストまたはマルチキャストにできます。キー サーバでは、登録時にグループ メンバーに送信される KEK を使用してキー再生成メッセージを暗号化します。キー再生成メッセージを受信したら、グループ メンバーは、キー再生成メッセージの SEQ 番号が最後に受信した SEQ 番号より大きいことを確認する必要があります。グループ メンバーは、どちらが後でも、登録メッセージまたはキー再生成メッセージのいずれかから SEQ 番号を受け取っているはずです。GDOI（IKEv1）と G-IKEv2 の両方のグループとしてキー サーバ グループが設定されている場合、マルチキャスト キー再生成のため、2 つのキー再生成メッセージ（GDOI 用に 1 つと G-IKEv2 用に 1 つ）が送信されます。ユニキャスト キー再生成の場合、キー サーバはグループ メンバーのモードまたはタイプに応じて GDOI または G-IKEv2 のキー再生成のみを送信します。

（注） キー再生成がユニキャストの場合、グループ メンバーはキー サーバに確認応答を送信する必要があります。

サポートされる機能と GKM のバージョン

GETVPN G-IKEv2 機能では、次のような既存の GETVPN 機能がサポートされています。

- キー再生成と再送信
- GM アクセス コントロール リスト（ACL）

- Fail-Close モード
- 受信専用モード
- アンチリプレイ
- グループ メンバー登録の認証ポリシー
- GDOI MIB
- VRF 認識型グループ メンバー
- グループ メンバーの削除とポリシー交換
- 連携キー サーバ
- GETVPN IPv6 データプレーン
- IPsec インライン タギングのサポート
- GETVPN の復元力のフェーズ 1 とフェーズ 2
- 連携通知メッセージの最適化

GETVPN G-IKEv2 機能は、GKM バージョン 1.0.12 以降のリリースでサポートされています。キーサーバーでサポートされる GKM のバージョンは 1.0.13 で、グループメンバーでサポートされる GKM のバージョンは 1.0.12 です。キーサーバーとグループメンバーのバージョンの違いは、GETVPN キーサーバーでの IP D3P サポートと Cisco GETVPN キーサーバーのインターネットドラフト ACK の機能が、 1.0.13 以降のキーサーバーでのみ使用できるためです。

GDOI から G-IKEv2 への移行

長期にわたって、キー サーバとグループ メンバーを G-IKEv2 にアップグレードして移行することを希望している場合があります。GETVPN グループ全体の GDOI から G-IKEv2 への移行には、慎重な計画が必要です。すべてのグループ メンバーを同時に移行することはできません。移行では、GDOI グループ メンバーと G-IKEv2 グループ メンバーが、GDOI と G-IKEv2 の異なるコントロール プレーン プロトコルを使用する一方で、同じトラフィック暗号キー（TEK）を使用した通信を可能にする必要があります。GDOI から G-IKEv2 への移行の順番は次のとおりです。

- 後方互換性：GETVPN G-IKEv2 機能を含む新しい Cisco IOS ソフトウェア イメージでは既存の GDOI 機能をサポートしている必要があり、Cisco IOS ソフトウェアの以前のリリースの GDOI 機能との互換性が必要です。
- サービス アップグレード：Cisco IOS ソフトウェア イメージを変更する推奨順序は、セカンダリ キー サーバ、プライマリ キー サーバ、およびグループ メンバーです。
- サービス ダウングレード：Cisco IOS ソフトウェア イメージを変更する推奨順序は、グループ メンバー、セカンダリ キー サーバ、プライマリ キー サーバです。

サービス アップグレード手順

1. 既存のキー サーバとグループ メンバーの GDOI 設定を保存します。詳細については、『*Managing Configuration Files Configuration Guide*』の「Configuration Replace and Configuration Rollback」機能モジュールを参照してください。
2. キー サーバの移行中のネットワーク分割およびマージを防ぐため、すべてのキー サーバで Key Encryption Key（KEK）とトラフィック暗号キー（TEK）のライフタイムを設定します。新しいライフタイムを設定するには、crypto gdoi ks rekey コマンドを使用します。
3. 新しい Cisco IOS ソフトウェア イメージにキー サーバをアップグレードします。上記の順序に従います。セカンダリ キー サーバから開始し、プライマリ キー サーバに続きます。キーワード **gdoi** を使用するすべての既存の設定がキーワード **gkm** に変換されます。たとえば、グローバル コンフィギュレーション コマンド **crypto gdoi group** は **crypto gkm group** コマンドに変換されます。ただし、再登録とキー再生成にはグループは引き続き GDOI を使用します。
4. キーサーバーで、GDOI および G-IKEv2 グループメンバーをサポートするグループに対してサーバーローカルコマンドの **gikev2** コマンドを実行します。
5. 新しい Cisco IOS ソフトウェア イメージにグループ メンバーをアップグレードします。キーワード「**gdoi**」を使用するすべての既存の設定がキーワード **gkm** に変換されます。たとえば、グローバル コンフィギュレーション コマンド **crypto gdoi group** と **crypto map gdoi** は、「**crypto gkm group**」と **crypto map gkm** にそれぞれ変換されます。これらのグループは再登録とキー再生成には GDOI を引き続き使用し、**client protocol gdoi** コマンドを含めます。
6. グループメンバーで G-IKEv2 を使用するには、**client protocol gikev2** コマンドを設定します。
7. GDOI グループメンバーへのサービスを停止するには、サーバーのローカルコマンドの **no gdoi** コマンドを設定します。

G-IKEv2 へのアップグレード後に GDOI を使用するグループメンバーに対して、グループメンバーグループ設定の **client protocol gdoi** コマンドを設定します。グループ メンバーは G-IKEv2 の代わりに GDOI を使用してキー サーバに再度登録します。

（注） グループ メンバーを変換する前に、グループ メンバーの登録先のキー サーバが GDOI ローカル サーバ コンフィギュレーション モードの gdoi コマンドで設定されていることを確認します。

サービス ダウングレード手順

以前に保存（アップグレード手順の前に保存）した GDOI 設定を使用し、各グループ メンバーの Cisco IOS ソフトウェアをダウングレードします。次に、キー サーバをダウングレードします。セカンダリ キー サーバから開始し、プライマリ キー サーバに続きます。詳細について

は、『*Managing Configuration Files Configuration Guide*』の「Configuration Replace and Configuration Rollback」機能モジュールを参照してください。

移行例

このセクションでは、GDOI から G-IKEv2 への移行の例を示します。次に、G-IKEv2 Cisco IOS ソフトウェア イメージにアップグレードした後に GDOI グループ g1 を GKM グループに変換する例を示します。Cisco IOS ソフトウェアのアップグレードの前のキー サーバ設定の例を次に示します。

```
crypto gdoi group g1
 identity 1111
 server local
  .
  .
  .
  sa ipsec 1
   profile getvpn_profile
   match address getvpn_acl
   .
   .
   .
   redundancy
   .
   .
   .
```

Cisco IOS ソフトウェアのアップグレードの後のキー サーバ設定の例を次に示します。この例では、コマンド **gdoi**、**no gikev2**、および **gikev2** が自動的に追加されます。**gikev2** コマンドは G-IKEv2 登録の受け入れを開始します。

```
crypto gkm group g1
 identity 1111
 server local
  gdoi
  no gikev2
  gikev2 ikev2_profile1
  .
  .
  .
  sa ipsec 1
   profile getvpn_profile
   match address getvpn_acl
   .
   .
   .
   redundancy
   .
   .
   .
```

Cisco IOS ソフトウェアのアップグレードの前のグループ メンバー設定の例を次に示します。

```
crypto gdoi group g1
 identity 1111
 server address ipv4 ks1
 server address ipv4 ks2

crypto map GETVPN_CM 10 gdoi
```

```
 set group g1

interface g0/0/0
 crypto map GETVPN_CM
```

Cisco IOS ソフトウェアのアップグレードの後のグループ メンバー設定の例を次に示します。この例では、コマンド **client protocol gdoi** および **client protocol gikev2** が自動的に追加されます。**client protocol gikev2** コマンドは G-IKEv2 の使用を開始します。

```
crypto gkm group g1
 identity 1111
 server address ipv4 ks1
 server address ipv4 ks2
 client protocol gdoi
 client protocol gikev2 ikev2_profile1 ] - Configure this to start using G-IKEv2

crypto map GETVPN_CM 10 gdoi
 set group g1

interface g0/0/0
 crypto map GETVPN_CM
```

GETVPN G-IKEv2 の設定

すべての GETVPN コマンド（EXEC およびグローバル コンフィギュレーション コマンド）にはキーワード **gdoi** が含まれます。G-IKEv2 にはドメイン オブ インタープリテーションが含まれていないため、登録およびキー再生成に GDOI と G-IKEv2 のいずれかのプロトコルを使用できるグループではグループ キー管理を指す全般的な短縮形 **gkm** が使用されます。現時点では、**crypto gdoi** コマンドと **crypto gkm** コマンドの両方を使用できます。ただし、**GDOI** キーワードは廃止されるため、今後は **gkm** キーワードに置き換わります。たとえば、キーサーバーグループを設定する場合、GDOI コマンドは **crypto gdoi group** *group-name* ですが、GKM コマンドは **crypto gkm group** *group-name* になります。

GETVPN G-IKEv2 の設定方法

IKEv2 プロファイルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 profile** *profile-name*
4. **authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}}
5. **identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*}

6. **keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] }
7. **match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*}
8. **pki trustpoint** *trustpoint-label* [**sign** | **verify**]
9. **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 ikev2 profile** *profile-name* 例： `Device(config)# crypto ikev2 profile gkm-gikev2`	IKEv2 プロファイルを定義し、IKEv2 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	**authentication** {**local** {**rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig** | **eap** [**gtc** | **md5** | **ms-chapv2**] [**username** *username*] [**password** {**0** | **6**} *password*}]} | **remote** {**eap** [**query-identity** | **timeout** *seconds*] | **rsa-sig** | **pre-share** [**key** {**0** | **6**} *password*}] | **ecdsa-sig**}} 例： `Device(config-ikev2-profile)# authentication local ecdsa-sig`	ローカルまたはリモートの認証方式を指定します。 • **rsa-sig**：認証方式として RSA-sig を指定します。 • **pre-share**：認証方式として事前共有キーを指定します。 • **ecdsa-sig**：認証方式として ECDSA-sig を指定します。 • **eap**：リモート認証方式として EAP を指定します。 • **query-identity**：ピアに EAP ID を問い合わせます。 • **timeout** *seconds*：最初の IKE_AUTH 応答を返してから次の IKE_AUTH 要求を受け取るまでの期間を秒単位で指定します。 （注） ローカル認証方式は 1 つしか指定できませんが、リモート認証方式は複数指定できます。

	コマンドまたはアクション	目的
ステップ 5	**identity local** {**address** {*ipv4-address* | *ipv6-address*} | **dn** | **email** *email-string* | **fqdn** *fqdn-string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# identity local email abc@example.com`	この手順は任意です。（任意）ローカル IKEv2 アイデンティティタイプを指定します。 （注） ローカル認証方式が事前共有キーの場合は、デフォルトのローカル ID が IP アドレスになります。ローカル認証方式が Rivest、Shamir、および Adleman（RSA）署名の場合は、デフォルトのローカル ID が識別名になります。
ステップ 6	**keyring** {**local** *keyring-name* | **aaa** *list-name* [**name-mangler** *mangler-name* | **password** *password*] } 例： `Device(config-ikev2-profile)# keyring aaa keyring1 name-mangler mangler1`	ローカルまたはリモートの事前共有キー認証方式で使用する必要があるローカルまたは AAA ベースのキーリングを指定します。 （注） 1 つのキーリングしか指定することができません。ローカル AAA は AAA ベースの事前共有キーに対してサポートされません。 （注） リリースによっては、**local** キーワードと **name-mangler** *mangler-name* キーワード引数ペアを使用する必要があります。 （注） AAA を使用する場合、Radius アクセス要求のデフォルトパスワードは「cisco」です。パスワードを変更するには、**keyring** コマンド内で **password** キーワードを使用します。
ステップ 7	**match** {**address local** {*ipv4-address* | *ipv6-address* | **interface** *name*} | **certificate** *certificate-map* | **fvrf** {*fvrf-name* | **any**} | **identity remote address** {*ipv4-address* [*mask*] | *ipv6-address prefix*} | {**email** [*domain string*] | **fqdn** [*domain string*]} *string* | **key-id** *opaque-string*} 例： `Device(config-ikev2-profile)# match address local interface Ethernet 2/0`	match ステートメントを使用して、ピア用の IKEv2 プロファイルを選択します。
ステップ 8	**pki trustpoint** *trustpoint-label* [**sign** | **verify**] 例： `Device(config-ikev2-profile)# pki trustpoint tsp1 sign`	RSA 署名認証方式で使用する Public Key Infrastructure（PKI）トラストポイントを指定します。 （注） **sign** または **verify** キーワードが指定されていない場合、トラストポイントは署名と検証に使用されます。

	コマンドまたはアクション	目的
		（注） IKEv1 とは対照的に、証明書ベースの認証を成功させるためにトラストポイントを IKEv2 プロファイル内で設定する必要があります。このコマンドが設定内に存在しない場合は、グローバルに設定されたトラストポイントのフォールバックが存在しません。トラストポイント設定は IKEv2 イニシエータおよびレスポンダに適用されます。
ステップ 9	**end** 例： `Device(config-ikev2-profile)# end`	IKEv2 プロファイル 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。

キーサーバーでの GKM ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group** [**ipv6**] *group-name*
4. **server local**
5. **gikev2** *IKEv2-profile-name*
6. **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 gkm group** [**ipv6**] *group-name* 例： `Device(config)# crypto gkm group gkm-grp1`	GKM ポリシーを設定し、GKM グループ 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 4	**server local** 例： `Device(config-gkm-group)# server local`	デバイスを GKM キーサーバーとして指定し、GKM ローカル サーバー コンフィギュレーション モードを開始します。
ステップ 5	**gikev2** *IKEv2-profile-name* 例： `Device(gkm-local-server)# gikev2 gkm-gikev2`	キーサーバーでの登録およびキー再生成のために G-IKEv2 プロファイルを有効にします。
ステップ 6	**end** 例： `Device(gkm-local-server)# end`	GKM ローカル サーバー 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。

グループメンバーでの GKM ポリシーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto gkm group** [**ipv6**] *group-name*
4. **client protocol gikev2** *gkm-gikev2*
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 gkm group** [**ipv6**] *group-name* 例： `Device(config)# crypto gkm group gkm-grp2`	GKM ポリシーを設定し、GKM 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	**client protocol gikev2** *gkm-gikev2* 例： `Device(config-gkm-group)# client protocol gikev2 gkm-gikev2`	グループメンバーでの登録およびキー再生成のために G-IKEv2 プロファイルを有効にします。

	コマンドまたはアクション	目的
ステップ 5	**end** 例： `Device(config-gkm-group)# end`	GKM グループ 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。

GETVPN G-IKEv2 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
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*』

標準および RFC

標準/RFC	タイトル
RFC 4306	*Internet Key Exchange (IKEv2) Protocol*
IKEv2 を使用したグループ キー管理	『*draft-yeung-g-ikev2-07*』

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

GETVPN G-IKEv2 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 : GETVPN G-IKEv2* の機能情報

機能名	リリース	機能情報
GETVPN G-IKEv2		次のコマンドが導入または変更されました。**client protocol**、**crypto gkm group**、**gikev2**、**show crypto gkm**

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。