ポスト量子事前共有キーを使用した量子安全暗号化の設定

このモジュールでは、ポスト量子事前共有キー（PPK）を使用した量子安全暗号化について説明します。この機能により、PPK を使用した IKEv2 および IPsec パケットの量子安全暗号化のために、RFC 8784 および Cisco Secure Key Integration Protocol（SKIP）が実装されます。

ポスト量子事前共有キーを使用した量子安全暗号化に関する制約事項

- ポスト量子事前共有キーを使用した量子安全暗号化の機能は、GETVPN を除くすべての IKEv2 および IPsec VPN（FlexVPN（SVTI-DVTI）、DMVPN など）に適用できます。

サポートされるプラットフォーム

ポスト量子事前共有キーを使用した量子安全暗号化の機能は、次のプラットフォームで使用できます。

Cisco IOS XE リリース 17.11 以降	**Cisco IOS XE リリース 17.12 以降**
Cisco Catalyst 8000V Edge ソフトウェア	Cisco 1000 シリーズ サービス統合型ルータ

Cisco IOS XE リリース 17.11 以降	Cisco IOS XE リリース 17.12 以降
Cisco Catalyst 8300 シリーズ エッジ プラットフォーム	Cisco Catalyst 8500 シリーズ エッジプラットフォーム
Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ	

ポスト量子事前共有キーを使用した量子安全暗号化に関する情報

以下のセクションでは、ポスト量子事前共有キーを使用した量子安全暗号化の機能に関する詳細情報を提供します。

量子コンピュータが暗号に与える影響

量子コンピュータは、現在普及している暗号アルゴリズムおよびプロトコルに深刻な課題をもたらします。量子コンピュータは、Diffie-Hellman（DH）および楕円曲線Diffie-Hellman（ECDH）の問題を多項式時間で解決できるため、既存のIKEv2システムのセキュリティが侵害される可能性があります。今日のVPN通信を保存している中間者は、後で量子コンピュータが使用可能になると、それらを復号できます。

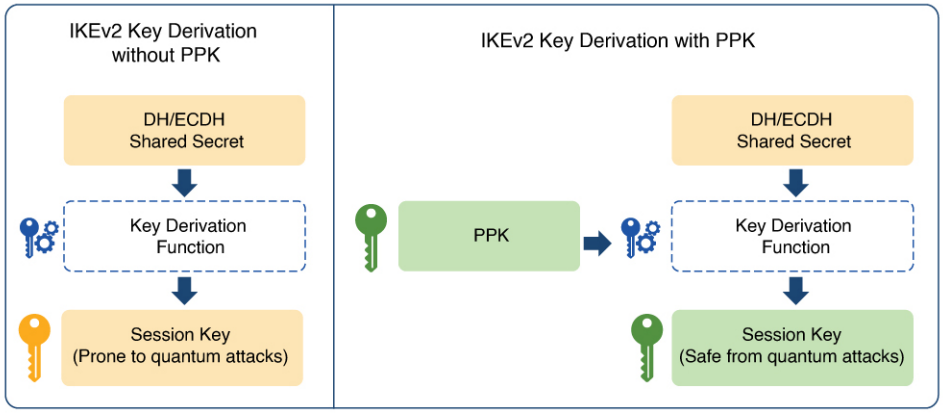
ポスト量子事前共有キー

事前共有キーに十分なエントロピーがあり、疑似乱数関数（PRF）、暗号化、および認証変換が量子セキュアである場合、事前共有キーに基づくセッションキーは、量子攻撃に対して脆弱ではありません。このようにして得られるシステムは、今日の古典的な攻撃者や量子コンピュータを使用する将来の攻撃者に対してセキュアであると考えられます。

RFC 8784（ポスト量子セキュリティのためのIKEv2での事前共有キーの混合）には、「PPK」と呼ばれる事前共有キーを使用して量子コンピュータに対する耐性を実現するIKEv2プロトコルの機能拡張が記述されています。このRFCでは、PPK機能のネゴシエーション、PPK IDの通信、セッションキー導出の追加入力としてのPPKの混合、および非PPKベースのセッションへのオプションのフォールバックが定義されています。

図1に、PPKを使用する場合と使用しない場合のIKEv2キーの導出を示します。

図 *1 : IKEv2* キーの導出：*PPK* を使用する場合と使用しない場合



DH: Diffie-Hellman
ECDH: Elliptic-curve Diffie-Hellman
PPK: Postquantum Preshared Key

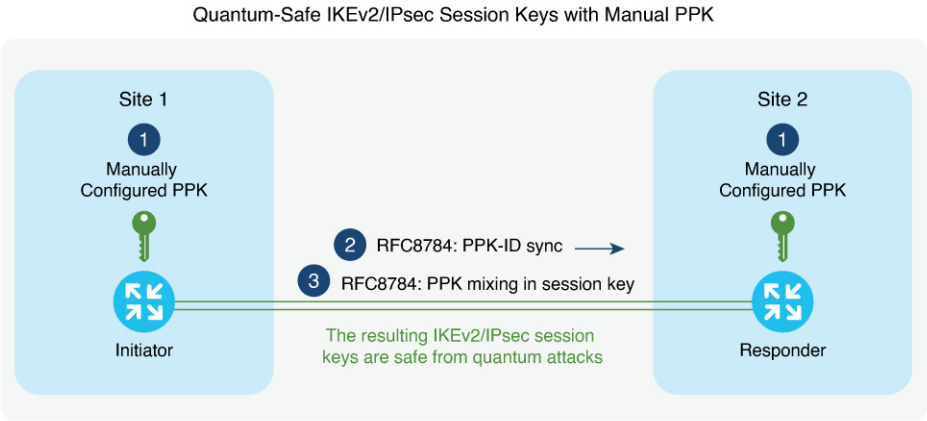
手動ポスト量子事前共有キー

IKEv2 および IPsec の発信側と応答側のペアで同じ PPK を提供する最も簡単なプロビジョニングメカニズムは、両側で PPK を手動で設定することです。手動で設定された PPK は、「手動 PPK」と呼ばれます。

手動 PPK の場合、管理者は、PPK のサイズとエントロピーが十分であり、頻繁にローテーションされることを確認する必要があります。

図 2 は、手動 PPK を使用した量子安全な IKEv2 および IPsec セッションキーを示しています。

図 *2 :* 手動 *PPK* を使用した量子安全な *IKEv2* および *IPsec* セッションキー



Cisco Secure Key Integration Protocol およびダイナミックポスト量子事前共有キー

Cisco SKIP は、ルータなどの暗号化デバイスが外部キーソースから PPK をインポートすることを可能にする HTTPS ベースのプロトコルです。ダイナミック PPK と呼ばれる外部からインポートされた PPK は、自動プロビジョニングおよび更新と、PPK のエントロピーの向上という利点を提供します。

Cisco SKIP は、TLS1.2 と PSK-DHE 暗号スイートを使用して、SKIP プロトコルを量子安全にします。暗号化デバイスは SKIP クライアントを実装する必要があり、外部キーソースは SKIP サーバーを実装する必要があります。

外部キーソースを SKIP 準拠にするには、Cisco SKIP プロトコルを実装し、アウトオブバンド同期メカニズムを使用して、2 つの暗号化デバイス（イニシエータとレスポンダ）に同じ PPK を提供する必要があります。外部キーソースには、量子キー配布（QKD）デバイス、ソフトウェア、もしくはクラウドベースキーソースまたはサービスを使用できます。

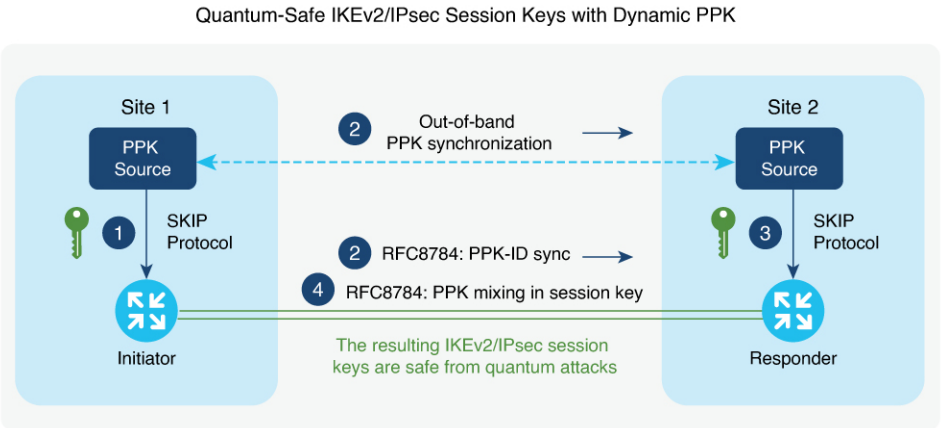
外部キーソースは、SKIP に準拠するために次の要件を満たす必要があります。

- Cisco SKIP 仕様で定義されているように、SKIP プロトコルまたは API を実装する必要があります。
- アウトオブバンド同期メカニズムを使用して、暗号化デバイスのペア（イニシエータとレスポンダ）に同じ PPK を提供する必要があります。

（注） 主要なソースベンダー（QKD ベンダーなど）は、シスコの担当者に連絡して、Cisco SKIP プロトコルを実装する必要があります。

図 3 は、ダイナミック PPK を使用した量子安全な IKEv2 および IPsec セッションキーを示しています。

図 *3:* ダイナミック *PPK* を使用した量子安全な *IKEv2* および *IPsec* セッションキー



IKEv2 イニシエータとレスポンダは、ローカルキーソースに接続され、キーソースの IP アドレスおよびポートと TLS1.2 セッションの事前共有キーを指定する SKIP クライアントで設定されます。PPK ソースは、ローカル キー ソース アイデンティティとピアキーソースのアイデンティティリストを含む SKIP パラメータを使用して設定されます。

次に、Cisco SKIP プロトコルの動作の概要を示します。

1. IKEv2 イニシエータは、そのキーソースに PPK を要求します。キーソースは、PPK と対応する PPK ID で応答します。
2. イニシエータ側のキーソースは、キーソースのタイプに固有のアウトオブバンドメカニズムを使用して、PPK をレスポンダ側のキーソースに同期します。IKEv2 イニシエータは、RFC 8784 の機能拡張を使用して、IKEv2 経由で IKEv2 レスポンダに PPK ID を伝達します。
3. IKEv2 レスポンダは、そのキーソースに、IKEv2 イニシエータから受信した PPK ID に対応する PPK を要求します。キーソースは、PPK ID に対応する PPK で応答します。
4. IKEv2 イニシエータおよびレスポンダは、RFC 8784 で規定されているように、キー導出で PPK を混合します。結果として得られる IKEv2 および IPsec セッションキーは、量子安全です。

ポスト量子事前共有キーを使用した量子安全暗号化の設定方法

以下のセクションでは、ポスト量子事前共有キーを使用した量子安全暗号化の設定に関連するプロセスについて説明します。

手動ポスト量子事前共有キーの設定

手動 PPK を設定するには、次の作業を実行します。

IKEv2 キーリングでの手動ポスト量子事前共有キーの設定

IKEv2 キーリングで 1 つ以上のピアまたはピアグループの手動 PPK を設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto ikev2 keyring** *keyring-name*
4. **peer** *name*
5. 次のコマンドの 1 つを実行します。
   - **address** {*ipv4-address mask* | *ipv6-address prefix*}

- **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}

6. **ppk manual id** *ppk-id* **key** [**0** | **6** | **hex**] *password* [**required**]

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。 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： `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 keyring** *keyring-name* 例： `Device(config)# crypto ikev2 keyring keyring1`	IKEv2 キーリングを定義し、IKEv2 キーリング 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	**peer** *name* 例： `Device(config-ikev2-keyring)# peer peer1`	ピアまたはピア グループを定義し、IKEv2 キーリング 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	次のコマンドの 1 つを実行します。
	• **address** {*ipv4-address mask* | *ipv6-address prefix*}
	• **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
	例：
	`Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.0.0.0`
	例：
	`Device(config-ikev2-keyring-peer)# identity address 10.0.0.1`
		WAN IP アドレスまたは IKEv2 アイデンティティに基づいてリモート IKEv2 ピアを指定します。
		• **address** コマンドは、ピアまたはピアグループの IPv4 または IPv6 アドレスあるいは範囲を指定します。
		（注） この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。
		• **identity** コマンドは、次のアイデンティティを使用して IKEv2 ピアを特定します。
		• 電子メール
		• 完全修飾ドメイン名（FQDN）
		• IPv4 アドレスまたは IPv6 アドレス
		• キー ID
		（注） **identity** コマンドは、IKEv2 レスポンダ上のキールックアップにしか使用できません。

	コマンドまたはアクション	目的
ステップ 6	**ppk manual id** *ppk-id* **key** [**0** | **6** | **hex**] *password* [**required**] 例： `Device(config-ikev2-keyring-peer)# ppk manual id ppk_id key cisco123`	特定されたピアの PPK ID および PPK を設定します。 • **ppk manual**：PPK ID と PPK が手動で設定されていることを示します。 • **id** *ppk-id*：PPK ID を指定します。 • **key** *password*：PPK を指定します。 • **required**：PPK を使用した量子安全暗号化が必須であり、通常の IKEv2 または IPsec セッションへのフォールバックが存在してはならないことを示します。 （注） *ppk-id* と PPK は、両方のピアで一致する必要があります。

IKEv2 プロファイルでの IKEv2 キーリングの設定

手順の概要

1. **crypto ikev2 profile** *profile-name*
2. **keyring ppk** *keyring-name*
3. **exit**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ikev2 profile** *profile-name* 例： `Device(config-ikev2-keyring-peer)# crypto ikev2 profile profile1`	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 2	**keyring ppk** *keyring-name* 例： `Device(config-ikev2-profile)# keyring ppk keyring1`	手動または動的 PPK が設定されているキーリングを指定します。 （注） IKEv2 プロファイルからキーリングを削除するには、**no keyring** {**aaa** | **local** | **ppk**} *keyring-name* コマンドを使用します。
ステップ 3	**exit** 例： `Device(config-ikev2-profile)# exit`	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、グローバル コンフィギュレーション モードに戻ります。

	コマンドまたはアクション	目的
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ダイナミックポスト量子事前共有キーの設定

ダイナミック PPK を設定するには、次の作業を実行します。

Secure Key Integration Protocol クライアントの設定

SKIP クライアントの設定では、外部の SKIP 準拠キーソースとセキュアに通信し、そこから PPK を要求するために必要なパラメータを指定します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto skip-client** *skip-client-name*
4. **server** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **fqdn** *domain-name*} **port** *port-number*
5. **psk id** *id-name* **key** [**0** | **6** | **hex**] *password*
6. **exit**

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。 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： `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 skip-client** *skip-client-name* 例： `Device(config-crypto-skip-client)# crypto skip-client skip-client-cfg`	SKIP クライアント設定ブロックの名前を指定し、SKIP クライアント 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	**server** {**ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **fqdn** *domain-name*} **port** *port-number* 例： `Device(config-crypto-skip-client)# server ipv4 10.10.0.3 port 9993`	外部キーソースに接続するIPアドレスまたはFQDNとポートを指定します。

	コマンドまたはアクション	目的
ステップ 5	**psk id** *id-name* **key** [**0** | **6** | **hex**] *password* 例： `Device(config-crypto-skip-client)# psk id psk-id key 0 cisco123`	SKIP TLS セッションの事前共有キーアイデンティティと事前共有キーを指定します。
ステップ 6	**exit** 例： `Device(config-crypto-skip-client)# exit`	SKIP クライアント コンフィギュレーション モードを終了して、グローバル コンフィギュレーション モードに戻ります。

IKEv2 キーリングの Secure Key Integration Protocol クライアントの設定

IKEv2 キーリングで 1 つ以上のピアまたはピアグループの手動 PPK を設定するには、次の手順を実行します。

手順の概要

1. **crypto ikev2 keyring** *keyring-name*
2. **peer** *name*
3. 次のいずれかのコマンドを実行します。
   - **address** {*ipv4-address mask* | *ipv6-address prefix*}
   - **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*}
4. **ppk dynamic** *skip-client-name* [**required**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ikev2 keyring** *keyring-name* 例： `Device(config)# crypto ikev2 keyring keyring1`	IKEv2 キーリングを定義し、IKEv2 キーリング コンフィギュレーション モードを開始します。
ステップ 2	**peer** *name* 例： `Device(config-ikev2-keyring)# peer peer1`	ピアまたはピア グループを定義し、IKEv2 キーリング 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	次のいずれかのコマンドを実行します。 • **address** {*ipv4-address mask* | *ipv6-address prefix*} • **identity** {**address** {*ipv4-address* | *ipv6-address*} | **fqdn domain** *domain-name* | **email domain** *domain-name* | **key-id** *key-id*} 例： `Device(config-ikev2-keyring-peer)# address 10.0.0.1 255.0.0.0`	WAN IP アドレスまたは IKEv2 アイデンティティに基づいてリモート IKEv2 ピアを指定します。 **address** コマンドは、ピアまたはピアグループの IPv4 または IPv6 アドレスあるいは範囲を指定します。 （注） この IP アドレスが IKE エンドポイント アドレスであり、ID アドレスとは別個のものです。

	コマンドまたはアクション	目的
	例： `Device(config-ikev2-keyring-peer)# identity address 10.0.0.1`	**identity** コマンドは、次のアイデンティティを使用して IKEv2 ピアを特定します。 • 電子メール • 完全修飾ドメイン名（FQDN） • IPv4 アドレスまたは IPv6 アドレス • キー ID （注） **identity** コマンドは、IKEv2 レスポンダ上のキールックアップにしか使用できません。
ステップ 4	**ppk dynamic** *skip-client-name* [**required**] 例： `Device(config-ikev2-keyring-peer)# ppk dynamic skip-client1`	ダイナミック PPK に使用する外部キーソースを指定します。 • **ppk dynamic**：PPK が外部キーソースから動的にインポートされることを示します。 • **required**：PPK を使用した量子安全暗号化が必須であり、通常の IKEv2 または IPsec セッションへのフォールバックが存在してはならないことを示します。

IKEv2 プロファイルでの IKEv2 キーリングの設定

手順の概要

1. **crypto ikev2 profile** *profile-name*
2. **keyring ppk** *keyring-name*
3. **exit**
4. **exit**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**crypto ikev2 profile** *profile-name* 例： `Device(config-ikev2-keyring-peer)# crypto ikev2 profile profile1`	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 2	**keyring ppk** *keyring-name* 例：	手動または動的 PPK が設定されているキーリングを指定します。

	コマンドまたはアクション	目的
	`Device(config-ikev2-profile)# keyring ppk keyring1`	（注） IKEv2プロファイルからキーリングを削除するには、**no keyring** {**aaa** | **local** | **ppk**} *keyring-name* コマンドを使用します。
ステップ 3	**exit** 例： `Device(config-ikev2-profile)# exit`	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、グローバル コンフィギュレーション モードに戻ります。
ステップ 4	**exit** 例： `Device(config)# exit`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ポスト量子事前共有キーを使用した量子安全暗号化の設定例

以下のセクションでは、PPK を使用した量子安全暗号化の設定に関連する詳細な設定例を示します。

例：手動ポスト量子事前共有キーの設定

例：イニシエータの設定

次に、イニシエータの PPK を手動で設定する例を示します。

```
conf t
hostname Router1
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk manual id ppk_id key cisco123
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
ip address 10.10.0.1 255.255.255.0
tunnel source GigabitEthernet1
tunnel destination 10.10.10.1
tunnel protection ipsec profile prof
!
```

```
interface GigabitEthernet1
ip address 10.10.10.2 255.255.255.0
no shut
!
```

例：応答側の設定

次に、レスポンダの PPK を手動で設定する例を示します。

```
conf t
hostname Router2
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk manual id ppk_id key cisco
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
ip address 10.10.0.2 255.255.255.0
tunnel source GigabitEthernet1
tunnel destination 10.10.10.2
tunnel protection ipsec profile prof
!
interface GigabitEthernet1
ip address 10.10.0.1 255.255.255.0
no shut
!
```

例：ダイナミックポスト量子事前共有キーの設定

例：イニシエータの設定

次に、イニシエータのダイナミック PPK の設定方法の例を示します。

```
conf t
hostname Router1
!
crypto skip-client skip-client-cfg
server ipv4 10.10.0.4  port 9991
psk id psk-id1 key 0 cisco123
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk dynamic skip-client-cfg
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
```

```
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
ip address 10.10.0.2 255.255.255.0
tunnel source GigabitEthernet1
tunnel destination 10.10.10.1
tunnel protection ipsec profile prof
!
interface GigabitEthernet1
ip address 10.10.10.2 255.255.255.0
no shut
!
interface GigabitEthernet1
ip address 10.10.10.3 255.255.255.0
no shut
!
```

例：応答側の設定

次に、応答側のダイナミック PPK の設定方法の例を示します。

```
conf t
hostname Router2
!
crypto skip-client skip-client-cfg
server ipv4 10.10.0.4 port 9992
psk id vedge-sim-1 key 0 cisco123
!
crypto ikev2 keyring ppk-keyring
peer 1
address 10.10.0.1 255.255.255.0
ppk dynamic skip-client-cfg
!
crypto ikev2 profile prof
match identity remote address 10.10.0.1
authentication local pre-share key cisco
authentication remote pre-share key cisco
keyring ppk ppk-keyring
!
crypto ipsec profile prof
set ikev2-profile prof
!
interface Tunnel0
ip address 10.10.0.2 255.255.255.0
tunnel source GigabitEthernet1
tunnel destination 10.10.10.2
tunnel protection ipsec profile prof
!
interface GigabitEthernet1
ip address 10.10.10.1 255.255.255.0
no shut
!
interface GigabitEthernet1
ip address 10.10.10.4 255.255.255.0
!
```

ポスト量子事前共有キーの設定の確認

現在の IKEv2 セキュリティ アソシエーションに関する情報を表示するには、**show crypto ikev2 sa detailed** コマンドを使用します。出力に表示される「Quantum Resistance Enabled」メッセージは、PPK ベースの量子安全暗号化が有効になっていることを示します。

次に、**show crypto ikev2 sa detailed** コマンドの出力例を示します。

```
IPv4 Crypto IKEv2  SA
Tunnel-id       Local                Remote                  fvrf/ivrf           Status

   3        <src IP>/SrcPort     <Dst IP>/DstPort              none/none        READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:19,
Auth sign:
.
.
.
Initiator of SA : No
Quantum Resistance Enabled
```

ポスト量子事前共有キーを使用した量子安全暗号化に関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List』、すべてのリリース
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』
IPsec の設定	『Configuring Security for VPNs with IPsec』

RFC

RFC	タイトル
RFC 8784	『*Mixing Preshared Keys in the Internet Key Exchange Protocol Version 2 (IKEv2) for Postquantum Security*』

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

ポスト量子事前共有キーを使用した量子安全暗号化に関する機能情報

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:* ポスト量子事前共有キーを使用した量子安全暗号化に関する機能情報

機能名	リリース	機能情報
ポスト量子事前共有キーを使用した量子安全暗号化	Cisco IOS XE リリース 17.11.1a	この機能により、ポスト量子事前共有キー（PPK）を使用した IKEv2 および IPsec パケットの量子安全暗号化のために、RFC 8784 および Cisco Secure Key Integration Protocol（SKIP）が実装されます。手動で設定された PPK は「手動 PPK」と呼ばれ、SKIP プロトコルを使用して外部キーソースからインポートされる PPK は「ダイナミック PPK」と呼ばれます。
ポスト量子事前共有キーを使用した量子安全暗号化	Cisco IOS XE リリース 17.12.1a	この機能拡張により、次のプラットフォームに、ポスト量子事前共有キーを使用した量子安全暗号化のサポートが導入されます。 • Cisco 1000 シリーズ サービス統合型ルータ • Cisco Catalyst 8500 シリーズ エッジプラットフォーム

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。