# Cisco IOS XE PKI の概要

Cisco IOS XE 公開キー インフラストラクチャ（PKI）には、IP Security（IPSec）、セキュアシェル（SSH）、Secure Socket Layer（SSL）などのセキュリティ プロトコルをサポートする証明書管理機能があります。

このマニュアルでは、PKI を理解、計画、実装するために必要な概念を確認、説明します。


- Cisco IOS XE PKI の情報 （1 ページ）
- PKI の計画 （5 ページ）
- 次の作業 （6 ページ）
- その他の参考資料 （6 ページ）
- 用語集 （8 ページ）


# Cisco IOS XE PKI の情報

## Cisco IOS XE PKI とは

PKI は以下のエンティティで構成されています。

- セキュアなネットワークで通信する複数のピア
- 証明書を発行および維持する認証局（CA）を最低 1 つ
- デジタル証明書（証明書の有効期間、ピアの ID 情報、セキュアな通信に使用する暗号キー、CA 発行のシグニチャなどで構成）
- 登録要求を処理し CA の負荷を軽減する登録局（RA）（任意）
- 証明書失効リスト（CRL）を配信するメカニズム（Lightweight Directory Access Protocol（LDAP）、HTTP など）

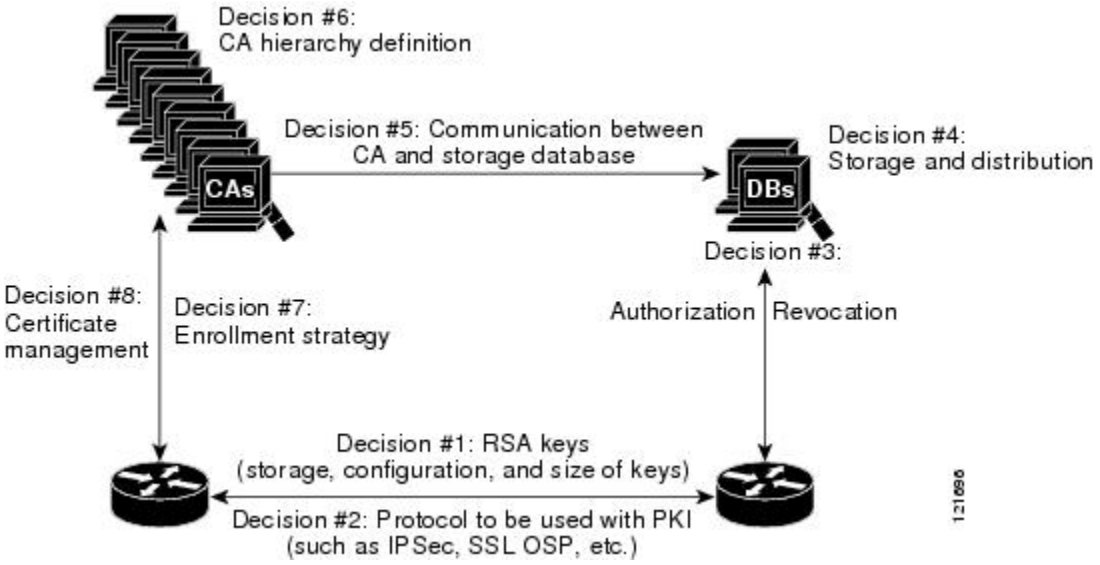
（注） Public Key Infrastructure（PKI）は、重要な拡張である **Inhibit Any Policy** をサポートしていません（内部 PKI ライブラリがこの拡張を認識しないため）。

PKI を使用すると、セキュアなデータ ネットワークで暗号化情報と ID 情報を配信、管理、失効するためのスケーラブルでセキュアなメカニズムを実現できます。セキュアな通信に関係するエンティティ（人物またはデバイス）はすべて、あるプロセスを経て PKI に登録されます。そのプロセスでは、エンティティが RSA（Rivest、Shamir、Adelman）キーのペア（秘密キーが 1 つ、公開キーが 1 つ）を生成し、信頼されているエンティティ（CA またはトラストポイントともいいます）でキーの ID を確認します。

各エンティティが PKI に登録されると、PKI のすべてのピア（エンド ホストともいいます）は、CA が発行したデジタル証明書を付与されます。セキュアな通信セッションをネゴシエーションする必要があるときは、ピアはデジタル証明書を交換します。ピアは証明書内の情報を基に他のピアの ID を確認し、証明書内の公開キーを使って、暗号化されたセッションを確立します。

PKI はさまざまな方法で計画、設定できますが、次の図に、PKI を構成する主なコンポーネントと、PKI で実行される各選択の順番を示します。図をアプローチとして推奨していますが、別の方法で PKI を設定してもかまいません。

**図 *1 : PKI* の設定方法の決定**




# RSA キーの概要

RSA キー ペアは、公開キーと秘密キーで構成されます。PKI を設定する場合、証明書登録要求に公開キーを含める必要があります。証明書が付与された後、ピアが公開キーを使用して、ルータに送信されるデータを暗号化できるように、公開キーが証明書に組み込まれます。秘密キーはルータに保持され、ピアによって送信されたデータの復号化と、ピアとネゴシエーションするときの、トランザクションのデジタル署名に使用されます。

RSA キーペアには、キーのモジュラス値が含まれています。モジュラス値に応じて、RSA キーのサイズが決まります。モジュラス値が大きいほど、RSA キーの安全性が高まります。ただし、モジュラス値が大きくなると、キーの生成にかかる時間が長くなり、キーのサイズが大きくなると暗号化処理および復号化処理にかかる時間が長くなります。

（注） デフォルトのキーサイズは 1024 ビットです。

# CA とは

CA（トラストポイントともいいます）は、証明書要求を管理し、参加ネットワーク デバイスに証明書を発行します。証明書要求の管理や証明書発行などのサービスにより、参加デバイスを一元的に管理します。またこれらのサービスによって受信者は、明示的に信頼してアイデンティティを確認し、デジタル証明書を作成できます。PKI の動作を開始する前に、CA は独自の公開キー ペアを生成し、自己署名 CA 証明書を作成します。その後、CA は、証明書要求に署名し、PKI に対してピア登録を開始できます。

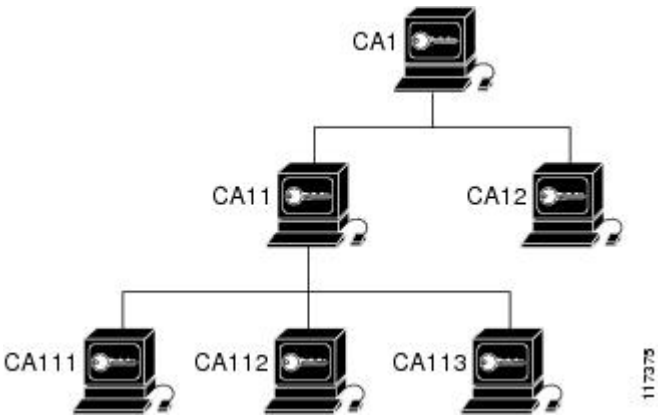
CA は、サードパーティの CA ベンダーが提供する CA を使用するか、内部の CA、つまり Cisco IOS 証明書サーバを使用します。

## 階層型 PKI：複数の CA

PKI は、複数の CA をサポートするために階層型フレームワーク内に設定できます。階層の最上位にはルート CA があり、自己署名証明書を保持しています。階層全体の信頼性は、ルート CA の RSA キー ペアから導出されます。階層構造内の下位 CA は、ルート CA または別の下位 CA に登録できます。どちらの方法で登録するかによって、CA の複数階層の設定方法が決まります。階層型 PKI 内では、登録されているすべてのピアが信頼できるルート CA 証明書または共通の下位 CA を共有している場合、証明書を相互に検証できます。

次の表 は、3 段の階層の CA 間の登録関係を示したものです。

**図 *2 : 3* 段の *CA* 階層のサンプル トポロジ**




各 CA が 1 つのトラストポイントに対応します。たとえば、CA11 および CA12 は従属 CA で、CA1 が発行した CA 証明書を保持しています。CA111、CA112、CA113 も従属 CA ですが、その CA 証明書を発行したのは CA11 です。

### 複数 CA を使用する場合

複数 CA を使用することにより、柔軟性および信頼性が向上します。たとえば、ルート CA を本社オフィスに配置し、下位 CA をブランチ オフィスに配置できます。また、CA ごとに異なる許可ポリシーを実行できるため、階層構造内の、ある CA では各証明書要求を手動で許可する必要があるように、別の CA では証明書要求を自動的に許可するように設定できます。

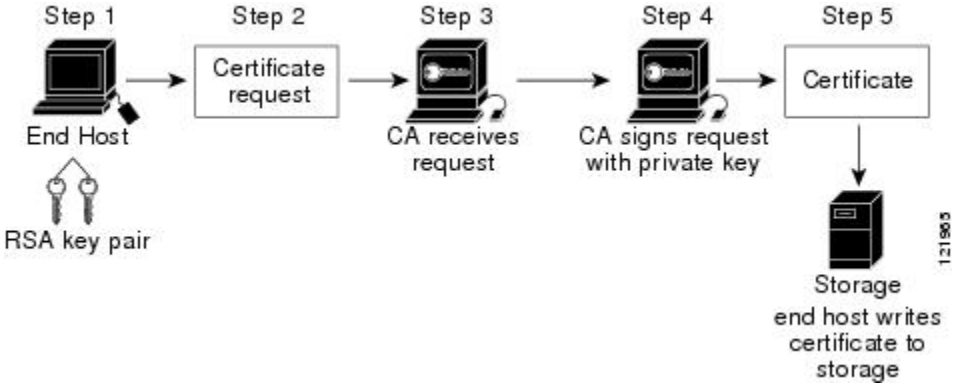
少なくとも 2 階層の CA が推奨されるシナリオは、次のとおりです。

- 多数の証明書が失効し、再発行される大規模かつ非常にアクティブなネットワーク。複数の階層を使用することにより、CA は CRL のサイズを制御しやすくなります。
- オンライン登録方式を使用するときに、ルート CA をオフラインのままにできる場合（従属 CA の証明書の発行を除く）。このシナリオでは、ルート CA のセキュリティが向上します。

## 証明書の登録：登録の動作

証明書の登録は、CA から証明書を取得するプロセスです。PKI に加わるエンド ホストは、それぞれ証明書を取得する必要があります。証明書の登録は、証明書を要求しているエンドホストと CA との間で行われます。次の表および手順によって、証明書の登録プロセスを説明します。

**図 *3:* 証明書の登録プロセス**




1. エンド ホストが RSA キーのペアを生成します。
2. エンド ホストが証明書要求を生成し、CA（または使用可能な場合は RA）に送ります。
3. CA が証明書登録要求を受け取ります。ネットワークの設定によって、次のいずれかになります。
    1. 要求の承認に手動による操作が必要。
    2. CA に証明書を自動で要求するようにエンド ホストが設定されている。これにより、登録要求が CA サーバに送信されたときのオペレータによる手動操作は不要になります。

（注） CA に証明書を自動で要求するようにエンド ホストを設定するには、別の認証メカニズムが必要になります。

1. 要求が承認されると、CA は自分の秘密キーを使って要求に署名し、処理の終わった証明書をエンド ホストに戻します。
2. エンド ホストは、証明書を NVRAM などの保管領域に書き込みます。

### Secure Device Provisioning による証明書登録

Secure Device Provisioning（SDP）は、Cisco IOS XE クライアントと Cisco IOS 証明書サーバなど、2 つのエンド デバイス間で PKI を簡単に配置できる、Web ベースの証明書登録インターフェイスです。

SDP（Trusted Transitive Introduction（TTI）とも呼ばれている）は、新しいネットワーク デバイスと VPN 間といった 2 つのエンド エンティティ間の双方向導入を実現する通信プロトコルです。SDP では次の 3 つのエンティティが関係します。

- イントロデューサ：ペティショナをレジストラに紹介する、相互に信頼できるデバイス。イントロデューサは、システム管理者などのデバイス ユーザの場合があります。
- ペティショナ：セキュアなドメインに参加した新しいデバイス。
- レジストラ：申請者を承認する証明書サーバなどのサーバ。

SDP は Web ブラウザを使い、ようこそ、紹介、完了の 3 つの段階で実装します。各段階は、Web ページを通してユーザに表示されます。

## 証明書の失効：失効する理由

各ピアが正常に PKI に登録されると、ピアは互いにセキュアな接続を行うためのネゴシエーションを開始できます。そのためにピアは確認に自分の証明書を提示し、失効のチェックを受けます。ピアは、通信相手のピアの証明書が、認証済みの CA によって発行された証明書であることを確認すると、CRL サーバまたは OCSP（Online Certificate Status Protocol）サーバをチェックし、証明書を発行した CA によって証明書が失効になっていないことを確認します。証明書には通常、証明書分散ポイント（CDP）が URL 形式で含まれています。Cisco IOS ソフトウェアはこの CDP を使用して、CRL の場所の特定と取得を行います。CDP サーバが応答しないと Cisco IOS ソフトウェアはエラーを生成し、ピアの証明書が拒否される場合があります。

# PKI の計画

PKI の計画では、それぞれの PKI コンポーネントの要件と予定の用途を評価する必要があります。ユーザ（またはネットワーク管理者）の方で十分に PKI を計画してから、PKI の設定を始めること推奨します。

PKI の計画では検討すべきアプローチがいくつかありますが、このマニュアルでは、ピアツーピアの通信から始めます。ただし、ユーザまたはネットワーク管理者が PKI の計画を選択するときは、特定の決定が PKI の他の決定に影響することを理解しておいてください。たとえば、登録および展開をどのようにするかによって、CA の階層の計画が変わってくる場合があります。このため、PKI 内の各コンポーネントがどのように機能するか、また、特定のコンポーネントのオプションが、計画プロセスで行った決定によってどのように変わるかを理解することが重要です。

# 次の作業

RSA キー ペアを生成したら、トラストポイントを設定する必要があります。すでにトラストポイントを設定している場合は、ルータを認証し、PKI に登録する必要があります。登録に関する情報については、「PKI の証明書登録の設定」を参照してください。

# 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 コマンド | 『Cisco IOS Master Command List, All Releases』 |
| PKI コマンド | • 『Cisco IOS Security Command Reference Commands A to C』<br>• 『Cisco IOS Security Command Reference Commands D to L』<br>• 『Cisco IOS Security Command Reference Commands M to R』<br>• 『Cisco IOS Security Command Reference Commands S to Z』 |
| 証明書登録：サポートされる方法、登録プロファイル、設定作業 | 『*Configuring Certificate Enrollment for a PKI*』 |
| 証明書の許可および失効：設定作業 | 『*Configuring Revocation and Authorization of Certificates in a PKI*』 |
| Cisco IOS 証明書サーバの概要および設定作業 | 「*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*」 |
| 安全なデバイス プロビジョニング：機能概要および設定作業 | 「*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*」 |

| 関連項目 | マニュアル タイトル |
|---|---|
| USB eToken への RSA キーおよび証明書の保存 | 「*PKI* クレデンシャルの保存」 |

### 標準および RFC

| 標準/RFC | タイトル |
|---|---|
| RFC 2459 | 『*Internet X.509 Public Key Infrastructure Certificate and CRL Profile*』 |
| RFC 2511 | 『*Internet X.509 Certificate Request Message Format*』 |
| RFC 2527 | 『*Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework*』 |
| RFC 2528 | 『*Internet X.509 Public Key Infrastructure*』 |
| RFC 2559 | 『*Internet X.509 Public Key Infrastructure Operational Protocols - LDAPv2*』 |
| RFC 2560 | 『*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*』 |
| RFC 2585 | 『*Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*』 |
| RFC 2587 | 『*Internet X.509 Public Key Infrastructure LDAPv2 Schema*』 |
| RFC 2875 | 『*Diffie-Hellman Proof-of-Possession Algorithms*』 |
| RFC 3029 | 『*Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols*』 |

### MIB

| MIB | MIB のリンク |
|---|---|
| • PKI MIB | 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。<br>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 |

# 用語集

**CDP**：Certificate Distribution Point（証明書分散ポイント）。デジタル証明書内のフィールドで、証明書の CRL の取り出し方法を記述した情報が含まれています。最も一般的な CDP としては HTTP や LDAP の URL があります。CDP には、他の種類の URL または LDAP のディレクトリ指定が含まれている場合もあります。それぞれの CDP には、URL またはディレクトリの指定が 1 つ含まれています。

**certificates**：ユーザー名またはデバイス名を公開キーにバインドする電子ドキュメント。証明書は、一般的にデジタル署名を確認するために使用されます。

**CRL**：Certificate Revocation List（証明書失効リスト）。失効した証明書のリストが含まれる電子ドキュメントです。CRL は、証明書を発行した CA によって作成され、デジタル署名されます。CRL には、証明書の発行日と失効日が含まれています。現行の CRL が失効すると、新しい CRL が発行されます。

**CA**：Certification Authority（認証局）。証明書要求の管理と、関係する IPSec ネットワーク デバイスへの証明書の発行を担当しているサービス。このサービスは、参加デバイスを一元的に管理します。またこれらのサービスによって受信者は、明示的に信頼してアイデンティティを確認し、デジタル証明書を作成できます。

**peer certificate**：ピアが提示する証明書のことで、ピアの公開キーが含まれており、トラストポイント CA が署名します。

**PKI**：Public Key Infrastructure（公開キーインフラストラクチャ）。セキュアに設定された通信に使用されているネットワーク コンポーネントの暗号キーと ID 情報を管理するシステムです。

**RA**：Registration Authority（登録局）。CA のプロキシとして機能するサーバーで、CA がオフラインのときでも CA の機能を継続できます。RA は CA サーバー上に設定するのが通常ですが、別アプリケーションとして、稼働のための別デバイスを必要とする場合もあります。

**RSA keys**：公開キー暗号化システムで、Ron Rivest（ロナルド・リベスト）、Adi Shamir（アディ・シャミア）、Leonard Adleman（レオナルド・エーデルマン）の 3 人によって開発されました。ルータの証明書を取得するには、RSA キーのペア（公開キーと秘密キー）が必要です。

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。