# Cisco IOS PKI の概要：PKI の理解および計画

Cisco IOS public key infrastructure（PKI; 公開鍵インフラストラクチャ）を使用すると、IP Security（IPSec; IP セキュリティ）、Secure Shell（SSH; セキュア シェル）、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を実現できます。

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。

**変更履歴**

このマニュアルの初版の発行は 2005 年 5 月 2 日 で、最終更新日は 2008 年 7 月 17 日 です。

## この章の構成


- 「Cisco IOS PKI に関する情報」（P.1）
- 「PKI の計画」（P.5）
- 「関連情報」（P.6）
- 「その他の参考資料」（P.6）
- 「用語集」（P.8）


## Cisco IOS PKI に関する情報

基本的な PKI の実装には、次の概念を理解する必要があります。


- 「Cisco IOS PKI とは」（P.2）
- 「RSA 鍵の概要」（P.3）
- 「CA とは」（P.3）
- 「証明書の登録：登録の動作」（P.4）
- 「証明書の失効：失効する理由」（P.5）

# Cisco IOS PKI とは

PKI は以下のエンティティで構成されています。

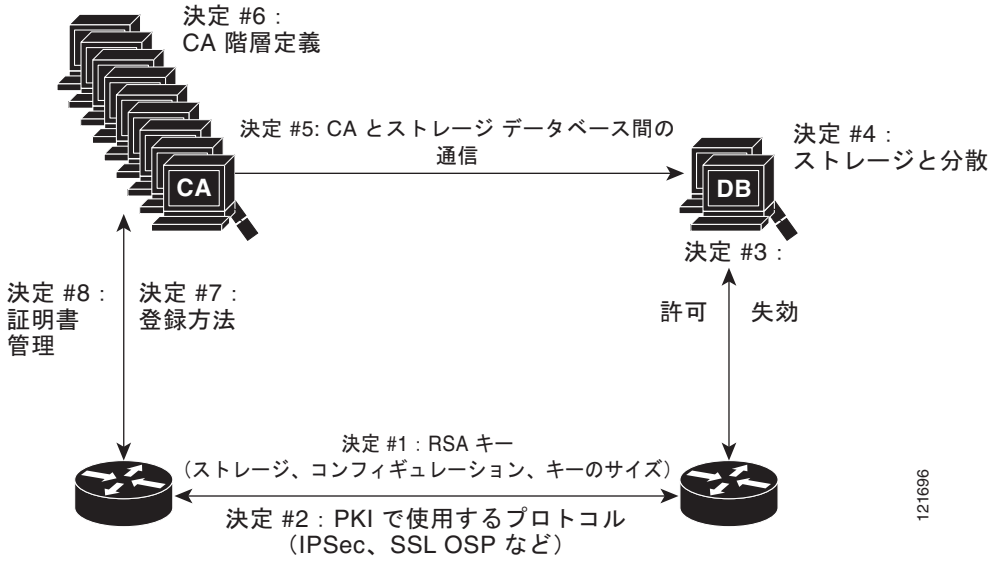
- セキュアなネットワークで通信する複数のピア
- 証明書を発行および維持する Certification Authority（CA; 認証局）を最低 1 つ
- デジタル証明書（証明書の有効期間、ピアの ID 情報、セキュアな通信に使用する暗号鍵、CA 発行のシグニチャなどで構成）
- 登録要求を処理し CA の負荷を軽減する Registration Authority（RA; 登録局）（任意）
- Certificate Revocation List（CRL; 証明書失効リスト）を配信するメカニズム（Lightweight Directory Access Protocol（LDAP）、HTTP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

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）鍵のペア（秘密鍵が 1 つ、公開鍵が 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）で鍵の 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、証明書内の公開鍵を使って、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、図 1 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 1 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 鍵の概要

RSA キー ペアは、公開鍵と秘密鍵で構成されます。PKI を設定する場合、証明書登録要求に公開鍵を含める必要があります。証明書が付与された後、ピアが公開鍵を使用して、ルータに送信されるデータを暗号化できるように、公開鍵が証明書に組み込まれます。秘密鍵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、鍵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 鍵のサイズが決まります。モジュラス値が大きいほど、RSA 鍵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、鍵の生成にかかる時間が長くなり、鍵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。

# 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 は独自の公開鍵ペアを生成し、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。

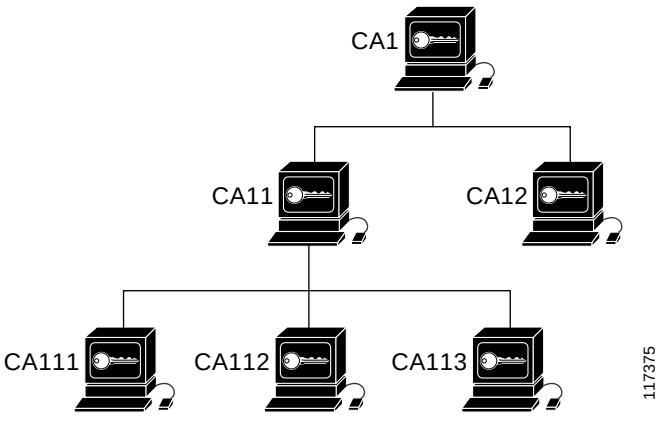
CA は、サードパーティの CA ベンダーが提供する CA を使用するか、「内部の」CA、つまり Cisco IOS 証明書サーバを使用します。

## 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。階層構造の最上位はルート CA で、ここに自己署名証明書が保持されます。階層構造全体における信頼性は、ルート CA の RSA 鍵ペアから得られます。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。

図 2 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。

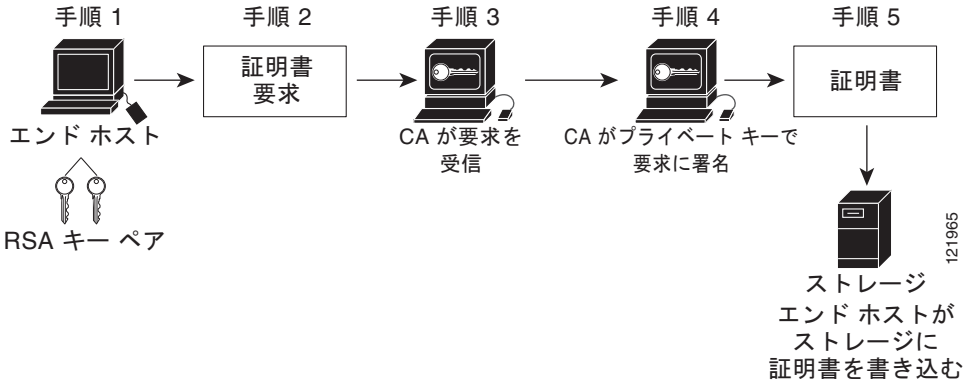
少なくとも 2 階層の CA が推奨されるシナリオは、次のとおりです。

- 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。図 3 および次の手順によって、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 鍵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。
   a. 要求の承認に手動による操作が必要。
   b. 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。

4. 要求が承認されると、CA は自分の秘密鍵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。
5. 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 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 Virtual Private Network（VPN; バーチャル プライベート ネットワーク）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、ウェルカム、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。各段階と SDP の動作に関する詳細については、「PKI への登録のための Secure Device Provisioning（SDP）の設定」の章を参照してください。

## 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 CDP を使って CRL を検索し、取得します。CDP サーバが要求に返答しない場合は、Cisco IOS ソフトウェアはエラーを報告し、その結果、ピアの証明書が拒否されることがあります。

# PKI の計画

PKI の計画では、図 1 のそれぞれの 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て、図 1 のような設定に進みます。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。

# 関連情報

図 1 で説明したように、PKI の設定では最初に RSA 鍵を設定し、展開します。詳細については、「PKI 内での RSA 鍵の展開」の章を参照してください。

# その他の参考資料

ここでは、Cisco IOS PKI に関する関連資料について説明します。

## 関連資料

| 内容 | 参照先 |
|---|---|
| PKI コマンド：完全なコマンドの構文、コマンド モード、デフォルト、使用上の注意事項、例 | 『*Cisco IOS Security Command Reference*』 |
| 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 | 『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring Certificate Enrollment for a PKI」の章。 |
| 証明書の許可および失効：設定作業 | 『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring Revocation and Authorization of Certificates in a PKI」の章 |
| Cisco IOS 証明書サーバの概要および設定作業 | 『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章 |
| 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 | 『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI」の章 |
| USB eToken への RSA 鍵および証明書の保存 | 『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Storing PKI Credentials」の章 |

## 規格

| 規格 | タイトル |
|---|---|
| なし | — |

## MIB

| MIB | MIB リンク |
|---|---|
| なし | 選択したプラットフォーム、Cisco IOS ソフトウェア リリース、および機能セットの 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 |

# RFC

| 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』 |

# 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。<br><br>以下を含むさまざまな作業にこの Web サイトが役立ちます。<br>・テクニカル サポートを受ける<br>・ソフトウェアをダウンロードする<br>・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける<br>・ツールおよびリソースへアクセスする<br>- Product Alert の受信登録<br>- Field Notice の受信登録<br>- Bug Toolkit を使用した既知の問題の検索<br>・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する<br>・トレーニング リソースへアクセスする<br>・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する<br><br>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/techsupport |

# 用語集

**CDP**：Certificate Distribution Point（CDP; 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。

**CRL**：Certificate Revocation List（CRL; 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（CA; 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。

**PKI**：Public Key Infrastructure（PKI; 公開鍵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（RA; 登録局）。CA のプロキシとして機能するサーバで、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、稼動のための別デバイスを必要とする場合もあります。

**RSA 鍵**：公開鍵暗号化システムで、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 鍵のペア（公開鍵と秘密鍵）が必要です。

**証明書**：ユーザ名またはデバイス名を公開鍵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。

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

**（注）** この用語集に記載されていない用語については、『*Internetworking Terms and Acronyms*』を参照してください。