PKI 機能のインプリメントと管理のロードマップ

このロードマップには、『*Cisco IOS セキュリティ コンフィギュレーション ガイド：セキュア接続*』に記載されている Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）機能のリストと、各機能を説明する章が示されています。いずれの機能に関しても、「説明している章」列のリンクをクリックすると、その機能に関する情報を含むモジュールが表示されます。

機能とリリース サポート

表 1 に、Cisco IOS Release 12.2T、12.3、および 12.3T の Cisco IOS ソフトウェア リリースでサポートされている PKI 機能をリストします。

この表には、Cisco IOS Release 12.2(1) 以降のリリースで導入または変更された機能だけを示します。*ご使用の Cisco IOS ソフトウェア リリースによっては、機能の中に一部サポートされていないものがあります。*

Cisco Feature Navigator を使用すると、プラットフォーム、および Cisco ソフトウェア イメージの各サポート情報を検索できます。Cisco Feature Navigator には、http://www.cisco.com/go/cfn からアクセスします。Cisco.com のアカウントは必要ありません。

（注） 表 1 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。その機能は、特に断りがない限り、それ以降の一連の Cisco IOS ソフトウェア リリースでもサポートされます。

表 1　サポート対象の PKI 機能

リリース	機能名	機能の説明	説明している章
12.3(14)T	Administrative Secure Device Provisioning Introducer	この機能により、デバイスを PKI ネットワークに紹介し、AAA データベースのレコード ロケータのデバイス名としてユーザ名を提供する管理イントロデューサとしての役割を果たすことができます。	「*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*」の章
12.3(14)T	永続的自己署名証明書	この機能により、HTTPS サーバのユーザは自己署名証明書を生成し、ルータのスタートアップ コンフィギュレーションに保存できます。そのため、それ以降のクライアントと HTTPS サーバ間の SSL ハンドシェイクで、ユーザが介入しなくても同じ自己署名証明書が使用されます。	「*Configuring Certificate Enrollment for a PKI*」の章
12.3(14)T	Secure Device Provisioning 証明書を使用した認可	この機能により、その他の認証局（CA）サーバで発行された証明書が SDP 導入に使用できるようになります。	「*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*」の章
12.3(14)T	下位証明書サーバ	この拡張機能では、すべての SCEP 証明書要求または特定の SCEP 証明書要求あるいは手動による証明書要求を許可するように下位証明書サーバを設定できます。	「*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*」の章
12.3(14)T	USB ストレージ	この機能を使用すると、USB eToken を使用してルータ外のデバイスに RSA キーを保存します。USB キー フォーム ファクタ（USB eToken ともいいます）で SmartCard テクノロジー（Aladdin Knowledge Systems 社製）を使用すると、設定をセキュアに配信できます。また、RSA キーなどの PKI クレデンシャルを保存しておき、導入できます。	「*Storing PKI Credentials*」
12.3(11)T	証明書サーバの自動アーカイブ	この拡張機能では、CA 証明書および CA キーが証明書サーバによって一度生成されると、これらを自動的にバックアップします。つまり、CA バックアップが妥当であれば、エクスポート可能な CA キーを生成する必要がありません。	「*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*」の章
12.3(11)T	所有者名全体を使用した PKI AAA 認可	この機能により、ユーザは、所有者名全体を一意の AAA ユーザ名として使用し、証明書から AAA サーバを照会できます。	「*Configuring Authorization and Revocation of Certificates in a PKI*」の章
12.3(11)T	PKI ステータス	この機能では、**show crypto pki trustpoints** コマンドに **status** キーワードが追加されました。これにより、トラストポイントの現在のステータスを表示できます。これ以前の機能では、現在のステータスを表示するために、**show crypto pki certificates** および **show crypto pki timers** コマンドを発行する必要がありました。	「*Configuring Certificate Enrollment for a PKI*」の章
12.3(11)T	既存の証明書を使用した再登録	この機能では、既存の証明書を使用して、ルータをサードパーティ ベンダー製の CA から Cisco IOS CA に再登録できます。	「*Configuring Certificate Enrollment for a PKI*」の章
12.3(8)T	Easy Secure Device Deployment	この機能は、SDP（正式には EzSDD）をサポートできるようにします。SDP は、ネットワーク管理者が大規模ネットワークで新しいデバイスを展開できるようにする Web ベースの登録インターフェイスを実現します。	「*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*」の章

表 1　サポート対象の PKI 機能 （続き）

リリース	機能名	機能の説明	説明している章
12.3(8)T	Easy Secure Device Deployment AAA Integration	この機能により外部 AAA データベースが統合され、ローカルなシスコ証明書サーバのイネーブル パスワードを使用しなくても、イントロデューサが AAA データベースに対して認証できるようにします。	「*Setting Up Secure Device Provisioning (SDP) for Enrollment in a PKI*」の章
12.3(7)T	証明書サーバ登録局（RA）モード	RA モードで実行するよう証明書サーバを設定できます。	「*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*」の章
12.3(7)T	**crypto pki** コマンドは **crypto ca** コマンドと同義であることが要求される	この拡張機能は、コマンドの先頭の **crypto ca** をすべて **crypto pki** に変更します。ルータは引き続き **crypto ca** コマンドを受信しますが、出力はすべて **crypto pki** コマンドに読み替えられます。	**crypto ca** コマンドが記載されているすべてのモジュール
12.3(7)T	証明書更新用のキー ロールオーバー	この機能では、証明書が失効する前に証明書の更新要求を行うことができます。新しい証明書が使用可能になるまで、古いキーと証明書は保持されます。	「*Configuring Certificate Enrollment for a PKI*」の章
12.3(7)T	PKI：証明書失効チェック時の複数のサーバ照会	この機能により、Cisco IOS ソフトウェアは、特定のサーバが利用できない場合に操作を続行できるように CRL の取得を複数回試行できます。また、この機能により手動で設定した CDP で証明書内の CDP を上書きできます。 証明書の CDP の手動による上書きは、特定のサーバが長時間利用できない場合に便利です。元の CDP を含む証明書のすべてを再発行しなくても、証明書の CDP を URL またはディレクトリ指定に置き換えることができます。	「*Configuring Authorization and Revocation of Certificates in a PKI*」の章
12.3(7)T	秘密キー保管の保護	この機能により、ユーザは、Cisco IOS ルータで使用される RSA 秘密キーを暗号化およびロックできます。これにより、秘密キーの不正使用を防止できます。	「*Deploying RSA Keys Within a PKI*」の章
12.3(4)T	RSA キー ペアおよび PEM 形式証明書のインポート	この機能を使用すると、PEM 形式ファイルを使用して、RSA キー ペアをインポートまたはエクスポートできます。PEM 形式のファイルを使用すると、新しいキーを生成しなくても、既存の RSA キー ペアを Cisco IOS ルータで直接使用できます。また、証明書の要求と発行された証明書の受け取りを PEM 形式のファイルで行えます。	「*Deploying RSA Keys Within a PKI*」モジュールおよび「*Configuring Certificate Enrollment for a PKI*」モジュール
12.3(4)T	証明書 ACL を使用して失効チェックおよび失効した証明書の無視	この機能により、指定基準を満たす証明書は、証明書の有効期間にかかわらず受け入れることができます。また、証明書が指定基準を満たしている場合は失効チェックを実行する必要がなくなります。 証明書 ACL は、証明書を受け入れるために満たす必要がある基準を指定する場合や、失効チェックを回避する場合に使用されます。さらに、AAA 通信が証明書によって保護されている場合、この機能を使用して無視される証明書に対して AAA チェックを実行できます。	「*Configuring Authorization and Revocation of Certificates in a PKI*」の章

表 1　　サポート対象の PKI 機能 （続き）

リリース	機能名	機能の説明	説明している章
12.3(4)T	Cisco IOS 証明書サーバ	この機能は、Cisco IOS 証明書サーバをサポートしています。これにより、CA が Cisco IOS ソフトウェアと直接統合され、基本 PKI ネットワークの展開がより簡単になりました。	「*Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment*」の章
12.3(4)T	HTTP による CA サーバへの直接登録	ユーザの CA サーバが SCEP をサポートしておらず、また RA をプロキシとして使用しない場合、この機能を使用すると、登録プロファイルを設定できます。登録プロファイルにより、HTTP 要求を RA プロキシではなく CA サーバに直接送信できます。	「*Configuring Certificate Enrollment for a PKI*」の章
12.3(2)T	Online Certificate Status Protocol（OCSP）	この機能により、CRL の代わりに OCSP をイネーブルにして、証明書のステータスをチェックできます。証明書のステータスを定期的に提供するだけの CRL とは異なり、OCSP では証明書ステータスに関する情報をタイムリーに利用できます。	「*Configuring Authorization and Revocation of Certificates in a PKI*」の章
12.3(1)	AAA サーバとの PKI 統合	この機能では、ピアによって提出された証明書から AAA ユーザ名を生成することにより、許可に関するスケーラビリティが向上します。AAA サーバは、内部コンポーネントでの証明書の使用を許可するか決定するよう尋ねられます。許可は、コンポーネントで指定されたラベルによって示され、このラベルはユーザの AV ペアに存在している必要があります。	「*Configuring Authorization and Revocation of Certificates in a PKI*」の章
12.2(15)T	証明書のセキュリティ アトリビュート ベースのアクセス コントロール	IPsec プロトコルでは、CA の相互運用性により、Cisco IOS デバイスと CA が通信を行い、Cisco IOS デバイスは、CA からデジタル証明書を取得し、使用できるようになります。 証明書には、指定された処理の実行をデバイスまたはユーザが許可されているかどうかの判別に使用されるフィールドがいくつか含まれています。この機能により、ACL の指定が可能な証明書にフィールドを追加し、証明書ベース ACL を作成できます。	「*Configuring Authorization and Revocation of Certificates in a PKI*」の章
12.2(15)T	RSA キーのエクスポートおよびインポート	この機能では、RSA キーをエクスポートし、インポートすることにより、デバイス間でセキュリティ クレデンシャルを転送できます。キー ペアを 2 台のデバイス間で共有すると、一方のデバイスが、もう一方のデバイスの機能を迅速かつトランスペアレントに引き継ぐことができます。	「*Deploying RSA Keys Within a PKI*」の章
12.2(15)T	複数階層の CA 階層構造	この拡張により、PKI を階層フレームワークに設定して複数の CA をサポートできるようになりました。階層型 PKI 内では、登録されているすべてのピアは、信頼できるルート CA 証明書または共通の下位 CA を共有しているかぎり、証明書を相互に検証できます。	「*Configuring Certificate Enrollment for a PKI*」の章
12.2(13)T	手動での証明書登録（TFTP によるカットアンドペースト）	この機能では、TFTP サーバまたは手動でのカットアンドペースト操作により、証明書要求を生成し、CA 証明書およびルータの証明書を受け取ることができます。	「*Configuring Certificate Enrollment for a PKI*」の章
12.2(8)T	証明書の自動登録	この機能では、証明書の自動登録が導入されています。これにより、ルータは、設定内のパラメータを使用する CA から自動的に証明書を要求できます。	「*Configuring Certificate Enrollment for a PKI*」の章

表 1　　サポート対象の PKI 機能 （続き）

リリース	機能名	機能の説明	説明している章
12.2(8)T	証明書登録の拡張機能	この機能では、5 つの新しい **crypto pki trustpoint** サブコマンドが導入されています。これらのサブコマンドでは、証明書要求用に新しいオプションが提供されているため、ユーザはプロンプトを最後まで進まずに、設定でフィールドを指定できます。	「*Configuring Certificate Enrollment for a PKI*」の章
12.2(8)T	複数の RSA キー ペアのサポート	この機能では、複数の RSA キー ペアを保持するようにルータを設定できます。したがって、Cisco IOS ソフトウェアはアイデンティティ証明書ごとに異なるキー ペアを維持できます。	「*Deploying RSA Keys Within a PKI*」の章
12.2(8)T	トラストポイント CLI	この機能では、**crypto pki trustpoint** コマンドが導入されています。これにより、トラストポイント CA をサポートできるようになりました。	「*Configuring Certificate Enrollment for a PKI*」の章