PKI の証明書登録の設定

この章では、証明書登録に利用可能なさまざまな方式および参加する PKI ピアの各セットアップ方法について説明します。証明書登録は、認証局（CA）から証明書を取得するプロセスであり、証明書を要求するエンド ホストと CA の間で発生します。Public Key Infrastructure（PKI; 公開キー インフラストラクチャ）に参加する各ピアは、CA に登録する必要があります。

この章で紹介する機能情報の入手方法

ご使用のソフトウェア リリースでは、この章で説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「PKI 証明書登録の機能情報」（P.38）を参照してください。

プラットフォームのサポートと Cisco IOS および Catalyst OS 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。

この章の構成

PKI 証明書登録の前提条件

証明書登録用にピアを設定する前に、次のものを準備、あるいは次の作業を実行することが必要です。

- 登録用に生成された Rivest、Shamir、Adelman（RSA）キー ペアおよび登録する PKI。
- 認証された CA。
- 「Cisco IOS PKI Overview: Understanding and Planning a PKI」の内容を理解していること。

（注） コマンドの先頭に付けられていた「**crypto ca**」は、Cisco IOS Release 12.3(7)T の時点で、すべて「**crypto pki**」に変更されました。ルータは引き続き **crypto ca** コマンドを受け入れますが、すべての出力は **crypto pki** として読み替えられます。

PKI の証明書登録に関する情報

証明書を要求して PKI に登録するようにピアを設定する前に、次の概念を理解しておく必要があります。

CA とは

CA は他の通信相手が使用できるデジタル証明書を発行するエンティティです。これが、信頼できる第三者の例です。CA は多くの PKI スキームの特性です。

CA は証明書要求を管理し、参加ネットワーク装置に証明書を発行します。これらのサービスでは、身元情報を検証してデジタル証明書を作成するために、参加装置のキーを一元的に管理します。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。

Cisco IOS 証明書サーバまたはサードパーティの CA ベンダーが指定する CA を使用できます。

複数の CA のためのフレームワーク

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 キー 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。CA の複数の階層が、ルート CA または別の下位 CA で設定されます。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。

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 Certificate Revocation List（CRL; 証明書失効リスト）のサイズを制御しやすくなります。
- 下位の CA 証明書を発行する場合を除いて、オンラインの登録プロトコルが使用されているときは、ルート CA をオフラインにしておくことができます。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。

CA の認証

装置に自身の証明書が発行されて証明書登録が発生する前に、CA の証明書が認証される必要があります。CA の認証は通常、ルータで PKI サポートを初期設定するときにだけ実行されます。CA を認証するには、**crypto pki authenticate** コマンドを発行します。これにより、CA の公開キーが組み込まれた CA の自己署名証明書が取得されて CA がルータに対して認証されます。

fingerprint コマンドによる認証

Cisco IOS Release 12.3(12) 以降では、**fingerprint** コマンドを発行して、認証時に CA 証明書のフィンガープリントと照合するフィンガープリントを事前入力できます。

フィンガープリントがトラスト ポイントにあらかじめ入力されていない場合や、認証要求がインタラクティブでない場合は、CA 証明書の認証時に表示されるフィンガープリントを検証する必要があります。認証要求がインタラクティブでない場合、事前入力フィンガープリントがないと、証明書は拒否されます。

（注） 認証要求が Command-Line Interface（CLI; コマンドライン インターフェイス）を使用して行われる場合、その要求はインタラクティブな要求です。認証要求が HTTP または別の管理ツールを使用して行われる場合、その要求はインタラクティブでない要求です。

サポートされる証明書の登録方式

Cisco IOS ソフトウェアは、CA から証明書を取得するために次の方式をサポートしています。

- Simple Certificate Enrollment Protocol（SCEP）: HTTP を使用して CA または Registration Authority（RA; 登録局）と通信する、シスコシステムズが開発した登録プロトコル。SCEP は、要求および証明書の送受信用に最も一般的に使用される方式です。

（注） 自動証明書およびキー ロールオーバー機能を活用するには、ロールオーバーをサポートする CA を実行する必要があります。また、クライアント登録方式として SCEP を使用する必要があります。

Cisco IOS CA を実行する場合は、ロールオーバーをサポートするために Cisco IOS Release 12.4(2)T 以降のリリースを実行する必要があります。

- PKCS12：ルータは、外部のサーバから証明書を PKCS12 形式でインポートします。
- IOS File System（IFS; IOS ファイル システム）：ルータは、Cisco IOS ソフトウェアでサポートされるファイル システム（TFTP、FTP、フラッシュ、および NVRAM など）を使用して証明書要求を送信し、発行された証明書を受信します。ユーザの CA が SCEP をサポートしない場合、IFS 証明書登録をイネーブルにできます。

（注） Cisco IOS Release 12.3(4)T 以前のリリースでは、IFS 内で TFTP ファイル システムだけがサポートされます。

- 手動でのカットアンドペースト：ルータはコンソール端末に証明書要求を表示し、ユーザはコンソール端末で発行された証明書を入力できます。ルータと CA の間にネットワーク接続がない場合、ユーザは証明書要求および証明書を手動でカットアンドペーストできます。
- 登録プロファイル：ルータは、HTTP ベースの登録要求を RA モードの Certificate Server（CS; 証明書サーバ）ではなく、CA サーバに直接送信します。CA サーバが SCEP をサポートしない場合に、登録プロファイルを使用できます。
- トラストポイントの自己署名証明書登録：セキュア HTTP（HTTPS）サーバは、Secure Socket Layer（SSL; セキュア ソケット レイヤ）ハンドシェイク時に使用される自己署名証明書を生成し、HTTPS サーバとクライアントの間にセキュアな接続を確立します。自己署名証明書は、ルータのスタートアップ コンフィギュレーション（NVRAM）に保存されます。保存された自己署名証明書は、将来の SSL ハンドシェイクに使用できます。これにより、ルータがリロードされる度に、証明書を受け入れるために必要だったユーザによる介入が不要になります。

（注） 自動登録および自動再登録を活用するには、登録方式として、TFTP または手動でのカットアンドペースト登録を使用しないでください。TFTP およびカットアンドペーストによる手動での登録方式は手動の登録プロセスでは、ユーザによる入力が必要です。

PKI の証明書登録のための Cisco IOS Suite-B サポート

Suite B の要件は、IKE および IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートで構成され、RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。

Suite-B によって、PKI の証明書登録に次のサポートが追加されます。

- X.509 証明書内の署名操作で、Elliptic Curve Digital Signature Algorithm（ECDSA; 楕円曲線デジタル署名アルゴリズム）（256 ビットおよび 384 ビットの曲線）が使用されます。
- ECDSA の署名を使用した X.509 証明書の確認で PKI がサポートされます。
- ECDSA の署名を使用した証明書要求の生成、および発行された証明書の IOS へのインポートで、PKI がサポートされます。

Cisco IOS での Suite-B サポートに関する詳細については、『Configuring Security for VPNs with IPsec』フィーチャ モジュールを参照してください。

登録局

Cisco IOS 証明書サーバは、RA モードで実行できるように設定できます。RA は、CA から認証および認可責任をオフロードします。RA が SCEP または手動での登録要求を受信すると、管理者はローカル ポリシーごとに要求を拒否または許可できます。要求が許可された場合、その要求は発行元 CA に転送されます。また、自動的に証明書を生成して、証明書を RA に返すように CA を設定できます。クライアントは、許可された証明書を RA から後で取得できます。

自動証明書登録

証明書自動登録を使用すると、CA クライアントは、CA サーバから証明書を自動的に要求できます。この自動ルータ要求では、登録要求が CA サーバに送信された時点で、オペレータによる介入が不要になります。自動登録は、設定済みの、有効なクライアント証明書を持っていないトラストポイント CA の起動時に実行されます。証明書が失効すると、新しい証明書が自動的に要求されます。

（注） 自動登録が設定されると、クライアントは自動的にクライアント証明書を要求します。CA サーバは、独自の許可チェックを実行します。このチェックに証明書を自動的に発行するポリシーが含まれている場合は、すべてのクライアントが自動的に証明書を受信しますが、これはそれほど安全ではありません。そのため、自動証明書登録を追加の認証および許可メカニズム（既存の証明書およびワンタイム パスワードを活用した Secure Device Provisioning（SDP）など）と組み合せる必要があります。

自動クライアント証明書およびキー ロールオーバー

デフォルトでは、自動証明書登録機能により、クライアントの現在の証明書が失効する前に、CS から新しいクライアント証明書とキーが要求されます。証明書およびキー ロールオーバーにより、新しいキーおよび証明書、ロールオーバー、証明書が利用可能になるまで、現在のキーおよび証明書を保持して証明書が失効する前に証明書更新ロールオーバー要求を行うことができます。指定された時間が経過すると、ロールオーバー証明書およびキーがアクティブになります。失効した証明書およびキーは、ロールオーバー時にただちに削除され、証明書チェーンおよび CRL から削除されます。

自動ロールオーバーのセットアップは 2 段階で行われます。まず CA クライアントが自動的に登録され、クライアントの CA が自動的に登録される必要があります。さらに **auto-rollover** コマンドがイネーブルになる必要があります。CA サーバを自動証明書ロールオーバー用に設定する場合の詳細については、『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章にある「Automatic CA Certificate and Key Rollover」の項を参照してください。

任意の renewal percentage パラメータを **auto-enroll** コマンドと一緒に使用すると、証明書の指定されたパーセンテージの有効期間が経過したときに、新しい証明書を要求できます。たとえば、更新パーセンテージが 90 に設定され、証明書の有効期間が 1 年の場合は、古い証明書が失効する 36.5 日前に新しい証明書が要求されます。自動ロールオーバーが発生するには、更新パーセンテージが 100 未満である必要があります。指定するパーセント値は、10 以上でなくてはなりません。CA 証明書の失効が差し迫っているため、有効設定期間よりも短い期間のクライアント証明書を発行する場合、その期間の残り日数に対してロールオーバー証明書が発行されます。最低でも、設定されている有効期間の 10 % と、ロールオーバーが機能するのに十分な時間（絶対最小値：3 分）を見込んでおく必要があります。

ヒント CA 自動登録がイネーブルになっておらず、現在のクライアント証明書の有効期間が、対応する CA 証明書の有効期間と同じか、それよりも長い場合は、**crypto pki enroll** コマンドを使用して既存のクライアント上で手動でロールオーバーを開始できます。

クライアントはロールオーバー プロセスを開始しますが、このプロセスは、サーバが自動ロールオーバーに設定され、利用可能なロールオーバー サーバ証明書を保持している場合にだけ発生します。

（注） キー ペアが **auto-enroll re-generate** コマンドおよびキーワードによって設定されている場合は、キー ペアも送信されます。新しいキー ペアは、セキュリティ上の問題に対処するために発行することを推奨します。

証明書登録プロファイル

登録プロファイルを使用すると、証明書認証、登録および再登録の各パラメータを指定するよう求められたときにユーザは、これらのパラメータを指定できます。これらのパラメータ値は、プロファイルを構成する 2 つのテンプレートによって参照されます。このうち、1 つのテンプレートには、CA の証明書を取得するために CA サーバに送られる HTTP 要求のパラメータ（証明書認証としても知られる）が含まれ、もう 1 つのテンプレートには、証明書を登録するために CA に送られる HTTP 要求のパラメータが含まれます。

2 つのテンプレートを設定すると、ユーザは、証明書の認証と登録用に異なる URL または方法を指定できます。たとえば、認証（CA の証明書の取得）を TFTP によって（**authentication url** コマンドを使用して）実行できる一方で、（**enrollment terminal** コマンドを使用して）登録を手動で実行できます。

Cisco IOS Release 12.3(11)T 以前のリリースでは、証明書要求は PKCS10 形式でしか送信できませんでしたが、現在では、プロファイルにパラメータが追加されたことにより、証明書更新要求用に PKCS7 形式を指定できるようになりました。

（注） 1 つの登録プロファイルには、タスクごとに最大 3 つのセクション（証明書の認証、登録および再登録）を指定できます。

PKI の証明書登録を設定する方法

ここでは、次の登録の任意手順について説明します。登録または自動登録を設定する（最初の作業）場合は、手動での証明書登録を設定できません。また、TFTP またはカットアンドペーストによる手動での証明書登録を設定した場合、自動登録、自動再登録、登録プロファイルは設定できず、自動 CA 証明書ロールオーバー機能も利用できません。

- 「証明書登録または自動登録の設定」（P.6）
- 「手動での証明書登録の設定」（P.11）
- 「登録用の永続的自己署名証明書の SSL による設定」（P.21）
- 「登録または再登録用の証明書登録プロファイルの設定」（P.24）

証明書登録または自動登録の設定

PKI に参加しているクライアントの証明書登録を設定するには、次の作業を実行します。

自動登録の前提条件

自動証明書登録要求を設定する前に、必要な登録情報がすべて設定されていることを確認する必要があります。

自動クライアント証明書およびキー ロールオーバーをイネーブルにするための前提条件

自動登録を使用するときには、証明書ロールオーバーの CA クライアント サポートが自動的にイネーブルになります。自動 CA 証明書ロールオーバーを正常に実行するには、次の前提条件が適用されます。

- ネットワーク装置はシャドウ PKI をサポートしている必要があります。
- クライアントは Cisco IOS Release 12.4(2)T 以降のリリースを実行している必要があります。
- クライアントの CS は自動ロールオーバーをサポートする必要があります。CA サーバの自動ロールオーバー設定コンフィギュレーションに関する詳細については、『*Cisco IOS Security Configuration Guide: Secure Connectivity*』「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章にある「Automatic CA Certificate and Key Rollover」を参照してください。

自動登録の初期キー生成場所を指定するための前提条件

自動登録の初期キー生成場所を指定するには、Cisco IOS Release 12.4(11)T 以降のリリースを実行する必要があります。

自動登録の制約事項

自動登録の RSA キー ペアに関する制約事項

regenerate コマンドまたは **auto-enroll** コマンドの **regenerate** キーワードを使用して新しいキー ペアを生成するように設定されたトラストポイントは、他のトラストポイントとキー ペアを共有してはなりません。各トラストポイントに独自のキー ペアを付与するには、CA トラストポイント コンフィギュレーション モードで **rsakeypair** コマンドを使用します。再生トラストポイント間でのキー ペアの共有がサポートされていない場合にキー ペアを共有すると、キーと証明書が一致しなくなるため、トラストポイントの一部のサービスが失われます。

自動クライアント証明書およびキー ロールオーバーに関する制約事項

クライアントが自動 CA 証明書ロールオーバーを正常に実行するには、次の制約事項が適用されます。

- SCEP を使用してロールオーバーをサポートする必要があります。SCEP の代わりに証明書管理プロトコルまたはメカニズム（登録プロファイル、手動での登録、または TFTP による登録など）を使用して、PKI に登録する装置では、SCEP で提供されているロールオーバー機能を利用できません。
- シャドウ証明書の生成後に、設定をスタートアップ コンフィギュレーションに保存できない場合、ロールオーバーは発生しません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name* [**sign** | **verify**]
4. **enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
5. **eckeypair** *label*
6. **subject-name** [*x.500-name*]

7. **ip address** {*ip-address* | *interface* | **none**}
8. **serial-number** [**none**]
9. **auto-enroll** [*percent*] [**regenerate**]
10. **usage** *method1* [*method2* [*method3*]]
11. **password** *string*
12. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
13. **fingerprint** *ca-fingerprint*
14. **on** *devicename*:
15. **exit**
16. **crypto pki authenticate** *name*
17. **exit**
18. **copy system:running-config nvram:startup-config**
19. **show crypto pki certificates**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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 pki trustpoint name`
	
	例：
	`Router(config)# crypto pki trustpoint mytp`
		トラストポイントおよび設定された名前を宣言して、CA トラストポイント 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	`enrollment [mode] [retry period minutes] [retry count number] url url [pem]`
	
	例：
	`Router(ca-trustpoint)# enrollment url http://cat.example.com`
		ルータが証明書要求を送信する CA の URL を指定します。
		• **mode**：CA システムが RA を提供する場合は、RA モードを指定します。
		• **retry period** *minutes*：証明書要求を再試行するまでの待機時間を指定します。デフォルトでは、1 分間隔で再試行します。
		• **retry count** *number*：直前の要求に対する応答をルータが受信しないとき、ルータが証明書要求を再送信する回数を指定します（1 ～ 100 回の範囲で指定できます）。
		• **url** *url*：ルータが証明書要求を送信するファイル システムの URL。登録方式のオプションについては、『*Cisco IOS Security Command Reference*』の **enrollment** コマンドを参照してください。
		• **pem**：証明書要求に Privacy Enhanced Mail（PEM）の境界を追加します。
		（注） 自動登録をサポートするには、TFTP または手動でのカットアンドペースト以外の登録方式を設定する必要があります。

ステップ 5	**eckeypair** *label* **例：** `Router(ca-trustpoint)# eckeypair Router_1_Key`	（任意）ECDSA の署名を使用して証明書要求を生成する Elliptic Curve（EC）キーを使用するように、トラストポイントを設定します。*label* 引数には、EC キーのラベルを指定します。このラベルは、グローバル コンフィギュレーション モードで **crypto key generate rsa** または **crypto key generate ec keysize** コマンドを使用して設定します。詳細については、『Configuring Internet Key Exchange for IPsec VPNs』フィーチャ モジュールを参照してください。 **（注）** トラストポイントの設定を使用せずに ECDSA の署名を持つ証明書をインポートする場合、ラベルにはデフォルトで FQDN の値が使用されます。

ステップ 6	`subject-name [x.500-name]`
	
	例：
	`Router(ca-trustpoint)# subject-name cat`
		（任意）証明書要求で使用される件名を指定します。
		• *x.500-name*：この名前が指定されていない場合、Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）が使用されます。FQDN はデフォルトの件名です。

ステップ 7	`ip address {ip-address | interface | none}`
	
	例：
	`Router(ca-trustpoint)# ip address 192.168.1.66`
		（任意）指定されたインターフェイスの IP アドレスを証明書要求に含めます。
		• IP アドレスを含めない場合は、**none** キーワードを発行します。
		（注） このコマンドがイネーブルになっている場合、このトラストポイントの登録時に IP アドレスのプロンプトは表示されません。

ステップ 8	`serial-number [none]`
	
	例：
	`Router(ca-trustpoint)# serial-number`
		（任意）**none** キーワードが発行されない限り、証明書要求でルータのシリアル番号を指定します。
		• **none** キーワードを発行し、シリアル番号が証明書要求に含まれないことを指定します。

	コマンドまたはアクション	目的

ステップ 9	`auto-enroll [percent] [regenerate]`
	
	例：
	`Router(ca-trustpoint)# auto-enroll regenerate`
		（任意）自動登録をイネーブルにします。これにより、クライアントは CA から自動的にロールオーバー証明書を要求できます。
		• 自動登録イネーブルでない場合、証明書の失効時にクライアントを手動で PKI に再登録する必要があります。
		• デフォルトでは、ルータの Domain Name System（DNS; ドメイン ネーム システム）名だけが証明書に含められます。
		• 現行の証明書の有効期間が指定のパーセンテージに達したときに、新しい証明書が要求されるように指定するには、*percent* 引数を使用します。
		• 名前付きのキーがすでに存在する場合でも、証明書の新しいキーを生成するには、**regenerate** キーワードを使用します。
		（注） ロールオーバー中のキー ペアがエクスポート可能な場合、新しいキー ペアもエクスポート可能です。次のコメントがトラストポイント コンフィギュレーションに表示され、キー ペアがエクスポート可能かどうかが示されます。「!RSA key pair associated with trustpoint is exportable.」
		（注） 新しいキー ペアは、セキュリティ上の問題に対処するために生成することを推奨します。

ステップ 10	**usage** *method1* [*method2* [*method3*]] **例：** `Router(ca-trustpoint)# usage ssl-client`	（任意）証明書の目的の用途を指定します。 • 指定可能なオプションは **ike**、**ssl-client**、および **ssl-server** です。デフォルトは **ike** です。
ステップ 11	**password** *string* **例：** `Router(ca-trustpoint)# password string1`	（任意）証明書の失効パスワードを指定します。 • このコマンドがイネーブルになっている場合、このトラストポイントの登録時にパスワードは求められません。 **（注）** SCEP が使用されている場合、このパスワードを使用して証明書要求を認可できます（多くの場合、ワンタイム パスワードまたは類似のメカニズムによって行われます）。
ステップ 12	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **例：** `Router(ca-trustpoint)# rsakeypair cat`	（任意）証明書に関連付けるキー ペアを指定します。 • *key-label* 付きのキー ペアがまだ存在しない、あるいは **auto-enroll regenerate** コマンドが発行された場合は、登録時にキー ラベル付きのキー ペアが生成されます。 • キーを生成するための *key-size* 引数を指定し、*encryption-key-size* 引数を指定して、個別の暗号化、署名キー、および証明書を要求します。 **（注）** このコマンドがイネーブルでない場合に、FQDN キー ペアが使用されます。

	コマンドまたはアクション	目的
ステップ 13	**fingerprint** *ca-fingerprint* **例：** `Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E`	（任意）認証時に CA 証明書のフィンガープリントと照合するフィンガープリントを指定します。 **（注）** フィンガープリントが指定されておらず、CA 証明書の認証がインタラクティブな場合、フィンガープリントは検証用に表示されます。
ステップ 14	**on** *devicename*: **例：** `Router(ca-trustpoint)# on usbtoken0:`	（任意）自動登録の初期キー生成時に、RSA キーが指定された装置に対して作成されるよう指定します。 • 指定可能な装置には、NVRAM、ローカル ディスク、および Universal Serial Bus（USB; ユニバーサル シリアル バス）トークンがあります。USB トークンは、ストレージ デバイス以外に、暗号化装置として使用できます。USB トークンを暗号化装置として使用すると、トークンでキー生成、署名、認証などの RSA 操作を実行できます。
ステップ 15	**exit** **例：** `Router(ca-trustpoint)# exit`	CA トラストポイント 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 16	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate mytp`	CA 証明書を取得して、認証します。 • 証明書フィンガープリントをチェックするよう求められた場合、証明書フィンガープリントをチェックします。 **（注）** CA 証明書がコンフィギュレーションにすでにロードされている場合、このコマンドはオプションです。
ステップ 17	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 18	**copy system:running-config nvram:startup-config** **例：** `Router# copy system:running-config nvram:startup-config`	（任意）実行コンフィギュレーションを NVRAM スタートアップ コンフィギュレーションにコピーします。 **（注）** 実行コンフィギュレーションが変更されていても NVRAM に書き込まれていない場合は、自動登録によって NVRAM が更新されません。
ステップ 19	**show crypto pki certificates** **例：** `Router# show crypto pki certificates`	（任意）ロールオーバー証明書などの、証明書に関する情報を表示します。

手動での証明書登録の設定

手動での証明書登録は、TFTP または手動でのカットアンドペースト方式によって設定できます。これらの方式は両方とも、CA が SCEP をサポートしない場合またはルータと CA 間のネットワーク接続が不可能な場合に使用できます。手動での証明書登録を設定するには、次のいずれかの作業を実行します。

- 「カットアンドペーストによる証明書登録の設定」（P.12）
- 「TFTP による証明書登録の設定」（P.14）

- 「Trend Micro サーバとセキュアな通信を行うための URL リンクの認証」（P.17）

証明書登録要求用の PEM 形式ファイル

証明書要求用の PEM 形式ファイルは、端末またはプロファイルベースの登録を使用して CA サーバから証明書を要求する場合に役立ちます。PEM 形式ファイルを使用すると、Cisco IOS ルータで既存の証明書を直接使用できます。

手動での証明書登録に関する制約事項

SCEP の制約事項

SCEP が使用されている場合、URL を切り替えることは推奨しません。つまり、登録 URL が「http://myca」である場合、CA 証明書を取得した後と証明書を登録する前で、登録 URL を変更しないでください。ユーザは、TFTP と手動でのカットアンドペーストを切り替えることができます。

キー再生に関する制約事項

crypto key generate コマンドを使用して、キーを手動で再生しないでください。キーの再生は、**regenerate** キーワードを指定して **crypto pki enroll** コマンドを発行します。

カットアンドペーストによる証明書登録の設定

この作業は、カットアンドペーストによる証明書登録を設定するために実行します。PKI に参加しているピアに対してカットアンドペースト方式による手動での証明書登録を設定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment terminal** [**pem**]
5. **fingerprint** *ca-fingerprint*
6. **exit**
7. **crypto pki authenticate** *name*
8. **crypto pki enroll** *name*
9. **crypto pki import** *name* **certificate**
10. **exit**
11. **show crypto pki certificates**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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 pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint mytp`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント 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	**enrollment terminal** [**pem**] **例：** `Router(ca-trustpoint)# enrollment terminal`	カットアンドペーストによる手動での証明書登録方式を指定します。 • 証明書要求は、手動でコピー（または切り取り）できるように、コンソール端末上に表示されます。 • **pem**：PEM 形式の証明書要求をコンソール端末に対して生成するようトラストポイントを設定します。
ステップ 5	**fingerprint** *ca-fingerprint* **例：** `Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E`	（任意）認証時に CA 証明書のフィンガープリントと照合するフィンガープリントを指定します。 **（注）** フィンガープリントが指定されていない場合は、フィンガープリントは検証用に表示されます。
ステップ 6	**exit** **例：** `Router(ca-trustpoint)# exit`	CA トラストポイント 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 7	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate mytp`	CA 証明書を取得して、認証します。
ステップ 8	`crypto pki enroll` *name* **例：** `Router(config)# crypto pki enroll mytp`	証明書要求を生成し、証明書サーバにコピーおよびペーストするために要求を表示します。 • 証明書要求にルータの FQDN および IP アドレスを含めるかどうかなどの登録情報を求められます。コンソール端末に対して証明書要求を表示するかについても選択できます。 • 必要に応じて、Base 64 符号化証明書を PEM ヘッダーを付けて、または付けずに表示します。

	コマンドまたはアクション	目的

ステップ 9	`crypto pki import name certificate`
	
	例：
	`Router(config)# crypto pki import mytp certificate`
		コンソール端末で証明書を手動でインポートします（貼り付けます）。
		• Base 64 符号化証明書はコンソール端末から受け取られ、内部証明書データベースに挿入されます。
		（注） 用途キー、署名キー、および暗号キーを使用する場合は、このコマンドを 2 度入力する必要があります。このコマンドが初めて入力されたとき、証明書の 1 つがルータにペーストされます。このコマンドが 2 回目に入力されたとき、もう 1 つの証明書がルータにペーストされます。どちらの証明書が先にペーストされても問題ありません。
		（注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の認証局がこれに該当する場合は、汎用目的の証明書をインポートしてください。ルータは、生成される 2 つのキー ペアのいずれも使用しません。

ステップ 10	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show crypto pki certificates** **例：** `Router# show crypto pki certificates`	（任意）証明書、CA の証明書、および RA 証明書に関する情報を表示します。

TFTP による証明書登録の設定

この作業は、TFTP による証明書登録を設定するために実行します。この作業を実行すると、TFTP サーバを使用して手動で証明書登録を設定できます。

TFTP による証明書登録の前提条件

- TFTP によって証明書登録を設定する場合は、使用する適切な URL がわかっている必要があります。
- ルータは、**crypto pki enroll** コマンドで TFTP サーバにファイルを書き込むことができる必要があります。
- ファイル指定と共に **enrollment** コマンドを使用する場合、ファイルには、バイナリ フォーマットまたは Base 64 符号化の CA 証明書が含まれている必要があります。
- ご使用の CA が証明書要求内のキーの用途情報を無視し、汎用目的の証明書だけを発行するかどうかを知っておく必要があります。

注意 一部の TFTP サーバでは、サーバが書き込み可能になる前に、ファイルがサーバ上に存在している必要があります。

ほとんどの TFTP サーバでは、ファイルを上書きできる必要があります。任意のルータまたは他の

装置によって証明書要求が書き込まれたり、上書きされることがあるため、この要件によって危険が生じる可能性があります。そのため、証明書要求を許可する前に、まず登録要求フィンガープリントをチェックする必要がある CA 管理者は交換証明書要求を使用しません。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**]
5. **fingerprint** *ca-fingerprint*
6. **exit**
7. **crypto pki authenticate** *name*
8. **crypto pki enroll** *name*
9. **crypto pki import** *name* **certificate**
10. **exit**
11. **show crypto pki certificates**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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 pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint mytp`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント 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	**enrollment** [**mode**] [**retry period** *minutes*] [**retry count** *number*] **url** *url* [**pem**] **例：** `Router(ca-trustpoint)# enrollment url tftp://certserver/file_specification`	登録要求を送信して、CA 証明書とルータ証明書および任意のオプションのパラメータを取得するための登録方式として TFTP を指定します。 **（注）** TFTP 登録の場合、URL は TFTP URL（tftp://example_tftp_url）として設定する必要があります。 • TFTP URL には、任意のファイル指定ファイル名を使用できます。ファイル指定が含まれていない場合は、FQDN が使用されます。ファイル指定が含まれている場合は、ルータは指定されたファイル名に「.ca」という拡張子を付加します。

	コマンドまたはアクション	目的
ステップ 5	**fingerprint** *ca-fingerprint* **例：** `Router(ca-trustpoint)# fingerprint 12EF53FA 355CD23E 12EF53FA 355CD23E`	（任意）CA 管理者からアウトオブバンド方式によって受け取る CA 証明書のフィンガープリントを指定します。 **（注）** フィンガープリントが指定されていない場合は、フィンガープリントは検証用に表示されます。
ステップ 6	**exit** **例：** `Router(ca-trustpoint)# exit`	CA トラストポイント 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 7	**crypto pki authenticate** *name* **例：** `Router(config)# crypto pki authenticate mytp`	指定された TFTP サーバから CA 証明書を取得して認証します。
ステップ 8	`crypto pki enroll` *name* **例：** `Router(config)# crypto pki enroll mytp`	証明書要求を生成し、この要求を TFTP サーバに書き込みます。 • 証明書要求にルータの FQDN および IP アドレスを含めるかどうかなどの登録情報を求められます。コンソール端末に証明書要求を表示するかどうかについて尋ねられます。 • 書き込まれるファイル名には「.req」という拡張子が付加されます。用途キー、署名キー、および暗号キーの場合、2 つの要求が生成されて送信されます。用途キーの要求ファイル名には、拡張子「-sign.req」および「-encr.req」がそれぞれ付加されます。

ステップ 9	`crypto pki import` *name* `certificate`
	
	例：
	`Router(config)# crypto pki import mytp certificate`
		許可された証明書を取得するコンソール端末で、TFTP によって証明書をインポートします。
		
		• ルータは、拡張子が「.req」から「.crt」に変更されたことを除いて、要求の送信に使用した同じファイル名を使用して、許可された証明書を TFTP によって取得しようと試みます。用途キー証明書の場合、拡張子「-sign.crt」および「-encr.crt」が使用されます。
		
		• ルータは、受信したファイルを解析して証明書を検証し、証明書をルータの内部証明書データベースに挿入します。
		
		（注） 一部の CA は、証明書要求の用途キー情報を無視し、汎用目的の証明書を発行します。ご使用の CA が証明書要求の用途キー情報を無視する場合は、汎用目的の証明書だけをインポートしてください。ルータは、生成される 2 つのキー ペアのいずれも使用しません。

	コマンドまたはアクション	目的
ステップ 10	**exit** **例：** `Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 11	**show crypto pki certificates** **例：** `Router# show crypto pki certificates`	（任意）証明書、CA の証明書、および RA 証明書に関する情報を表示します。

Trend Micro サーバとセキュアな通信を行うための URL リンクの認証

この作業は、Trend Micro サーバとセキュアに通信できるようにする URL フィルタリングで使用されるリンクを認証するために実行します。

手順の概要

1. **enable**
2. **clock set** *hh*:*mm*:*ss date month year*
3. **configure terminal**
4. **clock timezone** *zone hours-offset* [*minutes-offset*]
5. **ip http server**
6. **hostname** ***name***
7. **ip domain-name** *name*
8. **crypto key generate rsa general-keys modulus** *modulus-size*
9. **crypto pki trustpoint** *name*
10. **enrollment terminal**
11. **crypto ca authenticate** *name*
12. Base 64 符号化の CA 証明書が含まれている次のテキスト部分をコピーし、プロンプトにペーストします。
13. **yes** と入力し、この証明書を受け入れます。
14. **serial-number**
15. **revocation-check none**
16. **end**
17. **trm register**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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	**clock set** *hh*:*mm*:*ss date month year* **例：** `Router# clock set 23:22:00 22 Dec 2009`	ルータのクロックを設定します。
ステップ 3	**configure terminal** **例：** `Router# 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 4	**clock timezone** *zone hours-offset* [*minutes-offset*] **例：** `Router(config)# clock timezone PST -08`	時間帯を設定します。 • *zone* 引数は、時間帯を表す名前（通常は標準的な略語）です。*hours-offset* 引数は、使用する時間帯が Universal Time Coordinated（UTC; 協定世界時）から異なる時間数です。*minutes-offset* 引数は、使用する時間帯が UTC から異なる分数です。 （注） **clock timezone** コマンドの *minutes-offset* 引数は、ローカル時間帯の UTC または Greenwich Mean Time（GMT; グリニッジ標準時）からの差が 1 時間未満の割合で異なる場合に使用できます。たとえば、Atlantic Canada（AST; カナダ大西洋時間）の一部の地区の時間帯が UTC–3.5 の場合です。この場合、使用するコマンドは **clock timezone AST –3 30** になります。
ステップ 5	**ip http server** **例：** `Router(config)# ip http server`	HTTP サーバをイネーブルにします。
ステップ 6	**hostname** *name* **例：** `Router(config)# hostname hostname1`	ルータのホスト名を設定します。
ステップ 7	**ip domain-name** *name* **例：** `Router(config)# ip domain-name example.com`	ルータのドメイン名を定義します。

	コマンドまたはアクション	目的
ステップ 8	**crypto key generate rsa general-keys modulus** *modulus-size* **例：** `Router(config)# crypto key generate rsa general-keys modulus general`	暗号キーを生成します。 • **general-keys** キーワードは、汎用のキー ペアが生成されることを指定します。これがデフォルトです。 • **modulus** キーワードと *modulus-size* 引数は、キーのモジュラスの IP サイズを指定します。デフォルトでは、CA キーのモジュラス サイズは 1024 ビットです。汎用キーのモジュラスのサイズを 360 ～ 2048 の範囲で選択します。キーのモジュラスのサイズに 512 を超える値を選択した場合、ルータでのコマンド処理に数分かかることがあります。 **（注）** 生成される汎用キーの名前は、手順 7 で設定したドメイン名に基づきます。たとえば、キーの名前は「example.com」になります。
ステップ 9	**crypto pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint mytp`	ルータが使用する CA を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 **（注）** Cisco IOS Release 12.3(8)T で有効です。**crypto ca trustpoint** コマンドは **crypto pki trustpoint** コマンドに置き換えられました。
ステップ 10	**enrollment terminal** **例：** `Router(ca-trustpoint)# enrollment terminal`	カットアンドペーストによる手動での証明書登録方式を指定します。 • 証明書要求は、手動でコピー（または切り取り）できるように、コンソール端末上に表示されます。

ステップ 11	**crypto ca authenticate** *name*
	
	例：
	`Router(ca-trustpoint)# crypto ca authenticate mytp`
		CA の名前を引数として取得し、これを認証します。
		• 次のコマンドの出力が表示されます。
		`Enter the base 64 encoded CA certificate.`
		`End with a blank line or the word "quit" on a line by itself.`

	コマンドまたはアクション	目的

ステップ 12	Base 64 符号化の CA 証明書が含まれている右のテキスト部分をコピーし、プロンプトにペーストします。	MIIDIDCCAomgAwIBAgIENd70zzANBgkqhkiG9w0BAQUFADBOMQswCQYDVQQGEwJV
		UzEQMA4GA1UEChMHRXF1aWZheDEtMCsGA1UECxMkRXF1aWZheCBTZWN1cmUgQ2Vy
		dGlmaWNhdGUgQXV0aG9yaXR5MB4XDTk4MDgyMjE2NDE1MVoXDTE4MDgyMjE2NDE1
		MVowTjELMAkGA1UEBhMCVVMxEDAOBgNVBAoTB0VxdWlmYXgxLTArBgNVBAsTJEVx
		dWlmYXggU2VjdXJlIENlcnRpZmljYXRlIEF1dGhvcml0eTCBnzANBgkqhkiG9w0B
		AQEFAAOBjQAwgYkCgYEAwV2xWGcIYu6gmi0fCG2RFGiYCh7+2gRvE4RiIcPRfM6f
		BeC4AfBONOziipUEZKzxa1NfBbPLZ4C/QgKO/t0BCezhABRP/PvwDN1Dulsr4R+A
		cJkVV5MW8Q+XarfCaCMczE1ZMKxRHjuvK9buY0V7xdlfUNLjUA86iOe/FP3gx7kC
		AwEAAaOCAQkwggEFMHAGA1UdHwRpMGcwZaBjoGGkXzBdMQswCQYDVQQGEwJVUzEQ
		MA4GA1UEChMHRXF1aWZheDEtMCsGA1UECxMkRXF1aWZheCBTZWN1cmUgQ2VydGlm
		aWNhdGUgQXV0aG9yaXR5MQ0wCwYDVQQDEwRDUkwxMBoGA1UdEAQTMBGBDzIwMTgw
		ODIyMTY0MTUxWjALBgNVHQ8EBAMCAQYwHwYDVR0jBBgwFoAUSOZo+SvSspXXR9gj
		IBBPM5iQn9QwHQYDVR0OBBYEFEjmaPkr0rKV10fYIyAQTzOYkJ/UMAwGA1UdEwQF
		MAMBAf8wGgYJKoZIhvZ9B0EABA0wCxsFVjMuMGMDAgbAMA0GCSqGSIb3DQEBBQUA
		A4GBAFjOKer89961zgK5F7WF0bnj4JXMJTENAKaSbn+2kmOeUJXRmm/kEd5jhW6Y
		7qj/WsjTVbJmcVfewCHrPSqnI0kBBIZCe/zuf6IWUrVnZ9NA2zsmWLIodz2uFHdh
		1voqZiegDfqnc1zqcPGUIWVEX/r87yloqaKHee9570+sB3c4
		
		次のコマンドの出力が表示されます。
		`Certificate has the following attributes:`
		`Fingerprint MD5: 67CB9DC0 13248A82 9BB2171E D11BECD4`
		`Fingerprint SHA1: D23209AD 23D31423 2174E40D 7F9D6213 9786633A`

ステップ 13	**yes** と入力し、この証明書を受け入れます。	`% Do you accept this certificate? [yes/no]: yes`
		
		次のコマンドの出力が表示されます。
		`Trustpoint CA certificate accepted.`
		`% Certificate successfully imported`

ステップ 14	**serial-number** **例：** `hostname1(ca-trustpoint)# serial-number`	ルータのシリアル番号を証明書要求で指定します。
ステップ 15	**revocation-check none** **例：** `hostname1(ca-trustpoint)# revocation-check none`	証明書の確認が無視されることを指定します。

	コマンドまたはアクション	目的
ステップ 16	**end** **例：** `hostname1(ca-trustpoint)# end`	CA トラストポイント 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。
ステップ 17	**trm register** **例：** `hostname1# trm register`	Trend Micro サーバ登録プロセスを手動で開始します。

登録用の永続的自己署名証明書の SSL による設定

ここでは、次の作業について説明します。

- 「トラストポイントの設定および自己署名証明書パラメータの指定」（P.22）
- 「HTTPS サーバのイネーブル化」（P.23）

（注） これらの作業は任意です。これは、HTTPS サーバをイネーブルにした場合、このサーバがデフォルト値を使用して自動的に自己署名証明書を生成するからです。

永続的自己署名証明書の概要

SSL プロトコルは、HTTPS サーバとクライアント（Web ブラウザ）の間でセキュアな接続を確立するために使用されます。SSL ハンドシェイクの間、クライアントは、すでに所有している証明書を使用して SSL サーバの証明書が検証可能であると想定します。

Cisco IOS ソフトウェアが HTTP サーバで使用できる証明書を保持していない場合、サーバは、PKI Application Programming Interface（API; アプリケーション プログラミング インターフェイス）を呼び出して自己署名証明書を生成します。クライアントがこの自己署名証明書を受け取ったにもかかわらず、検証できない場合、ユーザによる介入が必要です。クライアントは、証明書を受け入れるか、あとで使用するために保存するかどうかを尋ねます。証明書を受け入れると、SSL ハンドシェイクは続行されます。

それ以降、同じクライアントとサーバ間の SSL ハンドシェイクでは、同じ証明書が使用されます。ただし、ルータをリロードすると、自己署名証明書は失われます。その場合、HTTPS サーバは新しい自己署名証明書を作成する必要があります。この新しい自己署名証明書は前の証明書と一致しないため、この自己署名証明書を受け入れるかどうか再度確認されます。

ルータがリロードするたびにルータの証明書を受け入れるかどうか確認されると、この確認中に、攻撃者に不正な証明書を使用する機会を与えてしまうことがあります。永続的自己署名証明書では、ルータのスタートアップ コンフィギュレーションに証明書を保存することにより、これらの制約をすべて解消しています。

制約事項

1 つの永続的自己署名証明書には、トラストポイントを 1 つだけ設定できます。

（注） 自己署名証明書の作成後は、ルータの IP ドメイン名またはホスト名を変更しないでください。いずれかの名前を変更すると、自己署名証明書の再生がトリガーされて、設定済みのトラストポイントが上書きされます。WebVPN は、SSL トラストポイント名を WebVPN ゲートウェイ設定に結合します。新しい自己署名証明書がトリガーされると、新しいトラストポイント名が WebVPN 設定と一致しなくなり、WebVPN 接続は失敗します。

トラストポイントの設定および自己署名証明書パラメータの指定

トラストポイントを設定し、自己署名証明書パラメータを指定するには、次の作業を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment selfsigned**
5. **subject-name** [*x.500-name*]
6. **rsakeypair** *key-label* [*key-size* [*encryption-key-size*]]
7. **crypto pki enroll** *name*
8. **end**
9. **show crypto pki certificates** [*trustpoint-name* [**verbose**]]
10. **show crypto pki trustpoints** [**status** | *label* [**status**]]

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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 pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint local`	ルータが使用する CA を宣言し、CA トラストポイント コンフィギュレーション モードを開始します。 （注） Cisco IOS Release 12.3(8)T で有効です。**crypto ca trustpoint** コマンドは **crypto pki trustpoint** コマンドに置き換えられました。
ステップ 4	**enrollment selfsigned** **例：** `Router(ca-trustpoint)# enrollment selfsigned`	自己署名登録を指定します。

	コマンドまたはアクション	目的
ステップ 5	**subject-name** [*x.500-name*] **例：** `Router(ca-trustpoint)# subject-name`	（任意）証明書要求に使用する要求件名を指定します。 • *x-500-name* 引数を指定しない場合、デフォルト件名である FQDN が使用されます。
ステップ 6	**rsakeypair** *key-label* [*key-size* [*encryption-key-size*]] **例：** `Router(ca-trustpoint)# rsakeypair examplekeys 1024 1024`	（任意）証明書に関連付けるキー ペアを指定します。 • *key-label* 引数がまだ存在しない、あるいは **auto-enroll regenerate** コマンドが発行された場合は、*key-label* 引数の値は登録時に生成されます。 • キーを生成するための *key-size* 引数を指定し、*encryption-key-size* 引数を指定して、個別の暗号化、署名キー、および証明書を要求します。 **（注）** このコマンドがイネーブルでない場合に、FQDN キー ペアが使用されます。
ステップ 7	**crypto pki enroll** *name* **例：** `Router(ca-trustpoint)# crypto pki enroll local`	永続的自己署名証明書を生成するようルータに指示します。
ステップ 8	**end** **例：** `Router(ca-trustpoint)# end`	（任意）CA トラストポイント コンフィギュレーション モードを終了します。 • グローバル コンフィギュレーション モードを終了するため、このコマンドをもう一度入力します。
ステップ 9	**show crypto pki certificates** [*trustpoint-name* [**verbose**]] **例：** `Router# show crypto pki certificates local verbose`	証明書、認証局証明書、および任意の登録認局証明書に関する情報を表示します。
ステップ 10	**show crypto pki trustpoints** [**status** | *label* [**status**]] **例：** `Router# show crypto pki trustpoints status`	ルータに設定されているトラストポイントを表示します。

HTTPS サーバのイネーブル化

HTTPS サーバをイネーブルにするには、次の作業を実行します。

前提条件

パラメータを指定するには、トラストポイントを作成し、設定する必要があります。デフォルト値を使用するには、すべての既存の自己署名トラストポイントを削除します。自己署名トラストポイントをすべて削除すると、HTTPS サーバがイネーブルになるとただちに、サーバはデフォルト値を使用して永続的自己署名証明書を生成します。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip http secure-server**
4. **end**
5. **copy system:running-config nvram: startup-config**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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	**ip http secure-server** **例：** `Router(config)# ip http secure-server`	HTTPS Web サーバをイネーブルにします。 **（注）** キー ペア（Modulus 1024）および証明書が生成されます。
ステップ 4	**end** **例：** `Router(config)# end`	グローバル コンフィギュレーション モードを終了します。
ステップ 5	**copy system:running-config nvram: startup-config** **例：** `Router# copy system:running-config nvram: startup-config`	イネーブルになっているモードで自己署名証明書および HTTPS サーバを保存します。

登録または再登録用の証明書登録プロファイルの設定

この作業は、登録または再登録用の証明書登録プロファイルを設定するために実行します。この作業は、サードパーティ ベンダー製 CA にすでに登録されている証明書またはルータを Cisco IOS CA に登録または再登録するための登録プロファイルを設定するのに役立ちます。

登録要求が自動的に許可されるように、サードパーティ ベンダー製 CA に登録されているルータを Cisco IOS 証明書サーバに登録するには、このルータをイネーブルにして、その既存の証明書を使用します。この機能をイネーブルにするには、**enrollment credential** コマンドを発行する必要があります。また、手動による証明書登録は設定できません。

前提条件

次の作業は、サードパーティ ベンダー製 CA にすでに登録されているクライアント ルータの証明書登録プロファイルを設定する前に、クライアント ルータで実行します。これにより、そのルータを Cisco IOS 証明書サーバに再登録できます。

- サードパーティ ベンダー製 CA をポイントするトラストポイントの定義
- サードパーティ ベンダー製 CA でのクライアント ルータの認証および登録

制約事項

- 証明書プロファイルを使用するには、ネットワークに、CA への HTTP インターフェイスが設定されている必要があります。
- 登録プロファイルが指定されている場合、トラストポイント設定に登録 URL が指定されていないことがあります。両方のコマンドがサポートされていても、トラストポイントに使用できるコマンドは一度に 1 つだけです。
- 各 CA で使用される HTTP コマンドには規格がないため、ユーザは使用している CA に適したコマンドを入力する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **crypto pki trustpoint** *name*
4. **enrollment profile** *label*
5. **exit**
6. **crypto pki profile enrollment** *label*
7. **authentication url** *url*

   または

   authentication terminal
8. **authentication command**
9. **enrollment url** *url*

   または

   enrollment terminal
10. **enrollment credential** *label*
11. **enrollment command**
12. **parameter** *number* {**value** *value* | **prompt** *string*}
13. **exit**
14. **show crypto pki certificates**

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：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • 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：** `Router# 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 pki trustpoint** *name* **例：** `Router(config)# crypto pki trustpoint Entrust`	トラストポイントおよび設定された名前を宣言して、CA トラストポイント 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	`enrollment profile` *label* **例：** `Router(ca-trustpoint)# enrollment profile E`	登録プロファイルが証明書認証および登録用に使用されるように指定します。
ステップ 5	**exit** **例：** `Router(ca-trustpoint)# exit`	CA トラストポイント コンフィギュレーション モードを終了します。
ステップ 6	**crypto pki profile enrollment** *label* **例：** `Router(config)# crypto pki profile enrollment E`	登録プロファイルを定義し、ca-profile-enroll コンフィギュレーション モードを開始します。 • *label*：登録プロファイルの名前。登録プロファイル名は、**enrollment profile** コマンドで指定された名前と同じである必要があります。

ステップ 7	**authentication url** *url*
	または
	authentication terminal
	
	例：
	`Router(ca-profile-enroll)# authentication url http://entrust:81`
	または
	`Router(ca-profile-enroll)# authentication terminal`
		証明書認証要求の送信先となる CA サーバの URL を指定します。
		• *url*：ルータが認証要求を送信する CA サーバの URL。
		HTTP を使用する場合、URL は「http://CA_name」という形式にする必要があります。ここで、CA_name は CA のホスト DNS 名または IP アドレスです。
		TFTP を使用する場合、URL は「tftp://certserver/file_specification」という形式にする必要があります（URL にファイル指定が含まれない場合、ルータの FQDN が使用されます）。
		カットアンドペーストによる手動での証明書認証を指定します。

ステップ 8	**authentication command** **例：** `Router(ca-profile-enroll)# authentication command`	（任意）認証のために CA に送信される HTTP コマンドを指定します。

	コマンドまたはアクション	目的

ステップ 9	**enrollment url** *url*
	または
	enrollment terminal
	
	例：
	`Router(ca-profile-enroll)# enrollment url http://entrust:81/cda-cgi/clientcgi.exe`
	または
	`Router(ca-profile-enroll)# enrollment terminal`
		証明書登録要求を HTTP または TFTP によって送信する CA サーバの URL を指定します。
		
		カットアンドペーストによる手動での証明書登録を指定します。

ステップ 10	**enrollment credential** *label* **例：** `Router(ca-profile-enroll)# enrollment credential Entrust`	（任意）Cisco IOS CA に登録される サードパーティ ベンダー製 CA トラストポイントを指定します。 **（注）** 手動での証明書登録が使用されている場合、このコマンドは発行できません。
ステップ 11	**enrollment command** **例：** `Router(ca-profile-enroll)# enrollment command`	（任意）登録のために CA に送信される HTTP コマンドを指定します。
ステップ 12	**parameter** *number* {**value** *value* | **prompt** *string*} **例：** `Router(ca-profile-enroll)# parameter 1 value aaaa-bbbb-cccc`	（任意）登録プロファイルのパラメータを指定します。 • このコマンドを繰り返して使用すると、複数の値を指定できます。
ステップ 13	**exit** **例：** `Router(ca-profile-enroll)# exit`	（任意）ca-profile-enroll コンフィギュレーション モードを終了します。 • グローバル コンフィギュレーション モードを終了するため、このコマンドをもう一度入力します。
ステップ 14	**show crypto pki certificates** **例：** `Router# show crypto pki certificates`	（任意）証明書、CA の証明書、および RA 証明書に関する情報を表示します。

次の作業

Cisco IOS CA に再登録するようにルータを設定した場合にこの機能を活用するには、指定されたサードパーティ ベンダー製 CA トラストポイントに登録されたクライアントからだけ登録要求を受け入れるように Cisco IOS 証明書サーバを設定する必要があります。詳細については、「PKI 展開での Cisco IOS 証明書サーバの設定および管理」を参照してください。

PKI 証明書登録要求の設定例

ここでは、次の設定例を示します。

- 「証明書登録または自動登録の設定例」（P.28）
- 「自動登録の設定例」（P.28）

証明書登録または自動登録の設定例

次の例では、「mytp-A」証明書サーバおよび関連付けられたトラストポイントの設定を示します。この例では、トラストポイントの初期の自動登録によって生成された RSA キーが USB トークン「usbtoken0」に保管されます。

```
crypto pki server mytp-A
   database level complete
   issuer-name CN=company, L=city, C=country
   grant auto
! Specifies that certificate requests will be granted automatically.
!

crypto pki trustpoint mytp-A
   revocation-check none
   rsakeypair myTP-A
   storage usbtoken0:
! Specifies that keys will be stored on usbtoken0:.
   on usbtoken0:
! Specifies that keys generated on initial auto enroll will be generated on and stored on
! usbtoken0:
```

自動登録の設定例

次の例では、自動ロールオーバーをイネーブルにして、ルータが起動時に自動的に CA に登録されるように設定する方法、および必要なすべての登録情報を設定に指定する方法を示します。

```
crypto pki trustpoint trustpt1
 enrollment url http://trustpt1.example.com//
 subject-name OU=Spiral Dept., O=example.com
 ip-address ethernet-0
 serial-number none
 usage ike
 auto-enroll regenerate
 password password1
 rsa-key trustpt1 2048
!
crypto pki certificate chain trustpt1
certificate pki 0B
30820293 3082023D A0030201 0202010B 300D0609 2A864886 F70D0101 04050030
79310B30 09060355 04061302 5553310B 30090603 55040813 02434131 15301306
0355040A 130C4369 73636F20 53797374 656D3120 301E0603 55040B13 17737562
6F726420 746F206B 6168756C 75692049 50495355 31243022 06035504 03131B79
6E692D75 31302043 65727469 66696361 7465204D 616E6167 6572301E 170D3030
30373134 32303536 32355A17 0D303130 37313430 31323834 335A3032 310E300C
06035504 0A130543 6973636F 3120301E 06092A86 4886F70D 01090216 11706B69
2D343562 2E636973 636F2E63 6F6D305C 300D0609 2A864886 F70D0101 01050003
4B003048 024100B3 0512A201 3B4243E1 378A9703 8AC5E3CE F77AF987 B5A422C4
15E947F6 70997393 70CF34D6 63A86B9C 4347A81A 0551FC02 ABA62360 01EF7DD2
6C136AEB 3C6C3902 03010001 A381F630 81F3300B 0603551D 0F040403 02052030
```

```
1C060355 1D110415 30138211 706B692D 3435622E 63697363 6F2E636F 6D301D06
03551D0E 04160414 247D9558 169B9A21 23D289CC 2DDA2A9A 4F77C616 301F0603
551D2304 18301680 14BD742C E892E819 1D551D91 683F6DB2 D8847A6C 73308185
0603551D 1F047E30 7C307AA0 3CA03AA4 38303631 0E300C06 0355040A 13054369
73636F31 24302206 03550403 131B796E 692D7531 30204365 72746966 69636174
65204D61 6E616765 72A23AA4 38303631 0E300C06 0355040A 13054369 73636F31
24302206 03550403 131B796E 692D7531 30204365 72746966 69636174 65204D61
6E616765 72300D06 092A8648 86F70D01 01040500 03410015 BC7CECF9 696697DF
E887007F 7A8DA24F 1ED5A785 C5C60452 47860061 0C18093D 08958A77 5737246B
0A25550A 25910E27 8B8B428E 32F8D948 3DD1784F 954C70
quit
```

（注） この例では、キーは再生もロールオーバーもされません。

証明書自動登録とキー再生の設定例

次の例では、ルータが起動時に「trustme1」という CA に自動的に登録され、自動ロールオーバーがイネーブルになるように設定する方法を示します。**regenerate** キーワードが発行されるため、自動ロールオーバー プロセスが開始されると、新しいキーが証明書に対して生成され、再発行されます。更新パーセンテージが 90 に設定されているため、証明書の有効期間が 1 年の場合は、古い証明書が失効する 36.5 日前に新しい証明書が要求されます。実行コンフィギュレーションを変更しても、NVRAM に書き込まないかぎり自動登録によって NVRAM が更新されないため、実行コンフィギュレーションの変更は NVRAM スタートアップ コンフィギュレーションに保存されます。

```
crypto pki trustpoint trustme1
 enrollment url http://trustme1.example.com/
 subject-name OU=Spiral Dept., O=example.com
 ip-address ethernet0
 serial-number none
 auto-enroll 90 regenerate
 password password1
 rsakeypair trustme1 2048
 exit
crypto pki authenticate trustme1
copy system:running-config nvram:startup-config
```

カットアンドペーストによる証明書登録の設定例

次の例では、カットアンドペーストによる手動での登録方式を使用して、証明書登録を設定する方法を示します。

```
Router(config)# crypto pki trustpoint TP
Router(ca-trustpoint)# enrollment terminal
Router(ca-trustpoint)# crypto pki authenticate TP

Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIICNDCCAd6gAwIBAgIQOsCmXpVHwodKryRoqULV7jANBgkqhkiG9w0BAQUFADA5
MQswCQYDVQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJ
bXNjYS1yb290MB4XDTAyMDIxNDAwNDYwMVoXDTA3MDIxNDAwNTQ0OFowOTELMAkG
A1UEBhMCVVMxFjAUBgNVBAoTDUNpc2NvIFN5c3RlbXMxEjAQBgNVBAMTCW1zY2Et
cm9vdDBcMA0GCSqGSIb3DQEBAQUAA0sAMEgCQQCix8nIGFg+wvy3BjFbVi25wYoG
K2N0HWWHpqxFuFhqyBnIC0OshIn9CtrdN3JvUNHr0NIKocEwNKUGYmPwWGTfAgMB
AAGjgcEwgb4wCwYDVR0PBAQDAgHGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYE
```

```
FKIacsl6dKAfuNDVQymlSp7esf8jMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9t
c2NhLXJvb3QvQ2VydEVucm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8v
XFxtc2NhLXJvb3RcQ2VydEVucm9sbFxtc2NhLXJvb3QuY3JsMBAGCSsGAQQBgjcV
AQQDAgEAMA0GCSqGSIb3DQEBBQUAA0EAeuZkZMX9qkoLHfETYTpVWjZPQbBmwNRA
oJDSdYdtL3BcI/uLL5q7EmODyGfLyMGxuhQYx5r/40aSQgLCqBq+yg==
-----END CERTIFICATE-----

Certificate has the following attributes:
Fingerprint: D6C12961 CD78808A 4E02193C 0790082A
% Do you accept this certificate? [yes/no]: y
Trustpoint CA certificate accepted.
% Certificate successfully imported

Router(config)# crypto pki enroll TP
% Start certificate enrollment..

% The subject name in the certificate will be: Router.example.com
% Include the router serial number in the subject name? [yes/no]: n
% Include an IP address in the subject name? [no]: n
Display Certificate Request to terminal? [yes/no]: y
Signature key certificate request -
Certificate Request follows:

MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAxdhXFDiWAn/hIZs9zfOtssKA
daoWYu0ms9Fe/Pew01dh14vXdxgacstOs2Pr5wk6jLOPxpvxOJPWyQM6ipLmyVxv
ojhyLTrVohrh6Dnqcvk+G/5ohss9o9RxvONwx042pQchFnx9EkMuZC7evwRxJEqR
mBHXBZ8GmP3jYQsjS8MCAwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgeAMA0GCSqGSIb3DQEBBAUAA4GBAMT6WtyFw95POY7UtF+YIYHiVRUf4SCq
hRIAGrljUePLo9iTqyPU1Pnt8JnIZ5P5BHU3MfgP8sqodaWub6mubkzaohJ1qD06
O87fnLCNid5Tov5jKogFHIki2EGGZxBosUw9lJlenQdNdDPbJc5LIWdfDvciA6jO
Nl8rOtKnt8Q+
!
!
!
Redisplay enrollment request? [yes/no]:
Encryption key certificate request -
Certificate Request follows:

MIIBhTCB7wIBADAlMSMwIQYJKoZIhvcNAQkCFhRTYW5kQmFnZ2VyLmNpc2NvLmNv
bTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAwG60QojpDbzbKnyj8FyTiOcv
THkDP7XD4vLT1XaJ409z0gSIoGnIcdFtXhVlBWtpq3/O9zYFXr1tH+BMCRQi3Lts
0IpxYa3D9iFPqev7SPXpsAIsY8a6FMq7TiwLObqiQjLKL4cbuV0Frjl0Yuv5A/Z+
kqMOm7c+pWNWFdLe9lsCAwEAAaAhMB8GCSqGSIb3DQEJDjESMBAwDgYDVR0PAQH/
BAQDAgUgMA0GCSqGSIb3DQEBBAUAA4GBACF7feURj/fJMojPBlR6fa9BrlMJx+2F
H91YM/CIiz2n4mHTeWTWKhLoT8wUfa9NGOk7yi+nF/F7035twLfq6n2bSCTW4aem
8jLMMaeFxwkrV/ceQKrucmNC1uVx+fBy9rhnKx8j60XE25tnp1U08r6om/pBQABU
eNPFhozcaQ/2
!
!
!
Redisplay enrollment request? [yes/no]: n
Router(config)# crypto pki import TP certificate

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIDajCCAxSgAwIBAgIKFN7C6QAAAAAMRzANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0MloXDTAzMDYwODAxMjY0MlowJTEjMCEGCSqGSIb3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMXYVxQ4lgJ/4SGbPc3zrbLCgHWqFmLtJrPRXvz3sNNXYdeL13cYGnLL
TrNj6+cJOoyzj8ab8TiT1skDOoqS5slcb6I4ci061aIa4eg56nL5Phv+aIbLPaPU
cbzjcMdONqUHIRZ8fRJDLmQu3r8EcSRKkZgR1wWfBpj942ELI0vDAgMBAAGjggHM
```

```
MIIByDALBgNVHQ8EBAMCB4AwHQYDVR0OBBYEFL8Quz8dyz4EGIeKx9A8UMNHLE4s
MHAGA1UdIwRpMGeAFKIacsl6dKAfuNDVQymlSp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmRCYWdnZXIuY2lz
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QuY3JsMIGUBggrBgEFBQcBAQSBhzCBhDA/BggrBgEF
BQcwAoYzaHR0cDovL21zY2Etcm9vdC9DZXJ0RW5yb2xsL21zY2Etcm9vdF9tc2Nh
LXJvb3QuY3J0MEEGCCsGAQUFBzAChjVmaWxlOi8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAJo2
r6sHPGBdTQX2EDoJpR/A2UHXxRYqVSHkFKZw0z31r5JzUM0oPNUETV7mnZlYNVRZ
CSEX/G8boi3WOjz9wZo=

% Router Certificate successfully imported

Router(config)# crypto pki import TP cert

Enter the base 64 encoded certificate.
End with a blank line or the word "quit" on a line by itself

MIIDajCCAxSgAwIBAgIKFN7OBQAAAAAMSDANBgkqhkiG9w0BAQUFADA5MQswCQYD
VQQGEwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1y
b290MB4XDTAyMDYwODAxMTY0NVoXDTAzMDYwODAxMjY0NVowJTEjMCEGCSqGSIb3
DQEJAhMUU2FuZEJhZ2dlci5jaXNjby5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0A
MIGJAoGBAMButEKI6Q282yp8o/Bck4jnL0x5Az+1w+Ly09V2ieNPc9IEiKBpyHHR
bV4VZQVraat/zvc2BV69bR/gTAkUIty7bNCKcWGtw/YhT6nr+0j16bACLGPGuhTK
u04sCzm6okIyyi+HG7ldBa45dGLr+QP2fpKjDpu3PqVjVhXS3vZbAgMBAAGjggHM
MIIByDALBgNVHQ8EBAMCBSAwHQYDVR0OBBYEFPDO29oRdlEUSgBMg6jZR+YFRWlj
MHAGA1UdIwRpMGeAFKIacsl6dKAfuNDVQymlSp7esf8joT2kOzA5MQswCQYDVQQG
EwJVUzEWMBQGA1UEChMNQ2lzY28gU3lzdGVtczESMBAGA1UEAxMJbXNjYS1yb290
ghA6wKZelUfCh0qvJGipQtXuMCIGA1UdEQEB/wQYMBaCFFNhbmRCYWdnZXIuY2lz
Y28uY29tMG0GA1UdHwRmMGQwL6AtoCuGKWh0dHA6Ly9tc2NhLXJvb3QvQ2VydEVu
cm9sbC9tc2NhLXJvb3QuY3JsMDGgL6AthitmaWxlOi8vXFxtc2NhLXJvb3RcQ2Vy
dEVucm9sbFxtc2NhLXJvb3QuY3JsMIGUBggrBgEFBQcBAQSBhzCBhDA/BggrBgEF
BQcwAoYzaHR0cDovL21zY2Etcm9vdC9DZXJ0RW5yb2xsL21zY2Etcm9vdF9tc2Nh
LXJvb3QuY3J0MEEGCCsGAQUFBzAChjVmaWxlOi8vXFxtc2NhLXJvb3RcQ2VydEVu
cm9sbFxtc2NhLXJvb3RfbXNjYS1yb290LmNydDANBgkqhkiG9w0BAQUFAANBAHaU
hyCwLirUghNxCmLzXRG7C3W1j0kSX7a4fX9OxKR/Z2SoMjdMNPPyApuh8SoT2zBP
ZKjZU2WjcZG/nZF4W5k=

% Router Certificate successfully imported
```

証明書が正常にインポートされたかどうかを確認するには、**show crypto pki certificates** コマンドを発行します。

```
Router# show crypto pki certificates

Certificate
  Status: Available
  Certificate Serial Number: 14DECE05000000000C48
  Certificate Usage: Encryption
  Issuer:
    CN = TPCA-root
     O = Company
     C = US
  Subject:
    Name: Router.example.com
    OID.1.2.840.113549.1.9.2 = Router.example.com
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 18:16:45 PDT Jun 7 2002
    end   date: 18:26:45 PDT Jun 7 2003
```

```
    renew date: 16:00:00 PST Dec 31 1969
  Associated Trustpoints: TP

Certificate
  Status: Available
  Certificate Serial Number: 14DEC2E9000000000C47
  Certificate Usage: Signature
  Issuer:
    CN = tpca-root
     O = company
     C = US
  Subject:
    Name: Router.example.com
    OID.1.2.840.113549.1.9.2 = Router.example.com
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 18:16:42 PDT Jun 7 2002
    end   date: 18:26:42 PDT Jun 7 2003
    renew date: 16:00:00 PST Dec 31 1969
  Associated Trustpoints: TP

CA Certificate
  Status: Available
  Certificate Serial Number: 3AC0A65E9547C2874AAF2468A942D5EE
  Certificate Usage: Signature
  Issuer:
    CN = tpca-root
     O = Company
     C = US
  Subject:
    CN = tpca-root
     O = company
     C = US
  CRL Distribution Point:
    http://tpca-root/CertEnroll/tpca-root.crl
  Validity Date:
    start date: 16:46:01 PST Feb 13 2002
    end   date: 16:54:48 PST Feb 13 2007
  Associated Trustpoints: TP
```

キー再生を使用した手動での証明書登録の設定例

次の例では、「trustme2」という名前の CA から手動で証明書を登録して、新しいキーを再生する方法を示します。

```
crypto pki trustpoint trustme2
 enrollment url http://trustme2.example.com/
 subject-name OU=Spiral Dept., O=example.com
 ip-address ethernet0
 serial-number none
 regenerate
 password password1
 rsakeypair trustme2 2048s
 exit
crypto pki authenticate trustme2
crypto pki enroll trustme2
```

永続的自己署名の証明書の作成および検証例

次の例では、「local」という名前のトラストポイントを宣言して登録し、IP アドレスを含む自己署名証明書を生成する方法を示します。

```
crypto pki trustpoint local
 enrollment selfsigned
 end
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

crypto pki enroll local
Nov 29 20:51:13.067: %SSH-5-ENABLED: SSH 1.99 has been enabled
Nov 29 20:51:13.267: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
% Include the router serial number in the subject name? [yes/no]: yes
% Include an IP address in the subject name? [no]: yes
Enter Interface name or IP Address[]: ethernet 0
Generate Self Signed Router Certificate? [yes/no]: yes
Router Self Signed Certificate successfully created
```

（注） ルータに設定できる自己署名証明書は 1 つだけです。自己署名証明書がすでに存在する場合に、別の自己署名証明書用に設定されたトラストポイントを登録しようとすると、通知が表示され、自己署名証明書を置き換えるかどうか尋ねられます。置き換える場合は、新しい自己署名証明書が生成され、既存の自己署名証明書と置き換えられます。

HTTPS サーバのイネーブル化の例

次の例では、以前に HTTPS サーバが設定されていなかったため、HTTPS サーバをイネーブルにし、デフォルト トラストポイントを生成する方法を示します。

```
configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

ip http secure-server
% Generating 1024 bit RSA keys ...[OK]
*Dec 21 19:14:15.421:%PKI-4-NOAUTOSAVE:Configuration was modified.  Issue "write memory"
to save new certificate
Router(config)#
```

（注） 自己署名証明書を保持し、次にルータをリロードしたときに HTTPS サーバをイネーブルにする場合は、コンフィギュレーションを NVRAM に保存する必要があります。

次のメッセージも表示されます。

```
*Dec 21 19:14:10.441:%SSH-5-ENABLED:SSH 1.99 has been enabled
```

（注） 自己署名証明書で使用されたキー ペアを作成すると、Secure Shell（SSH）サーバが起動します。この動作は抑制できません。ご使用の Access Control List（ACL; アクセス制御リスト）を変更して、ルータへの SSH アクセスを許可または拒否できます。**ip ssh rsa keypair-name** *unexisting-key-pair-name* コマンドを使用し、SSH サーバをディセーブルにできます。

自己署名証明書設定の検証例

次の例では、作成した自己署名証明書に関する情報を表示します。

```
Router# show crypto pki certificates

Router Self-Signed Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: General Purpose
  Issuer:
    cn=IOS-Self-Signed-Certificate-3326000105
  Subject:
    Name: IOS-Self-Signed-Certificate-3326000105
    cn=IOS-Self-Signed-Certificate-3326000105
  Validity Date:
    start date: 19:14:14 GMT Dec 21 2004
    end   date: 00:00:00 GMT Jan 1 2020
  Associated Trustpoints: TP-self-signed-3326000105
```

（注） 上記の 3326000105 という数値はルータのシリアル番号で、これはルータの実際のシリアル番号によって異なります。

次の例では、自己署名証明書に対応するキー ペアに関する情報を表示します。

```
Router# show crypto key mypubkey rsa

% Key pair was generated at: 19:14:10 GMT Dec 21 2004
Key name: TP-self-signed-3326000105
 Usage: General Purpose Key
 Key is not exportable.
 Key Data:
  30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00B88F70
  6BC78B6D 67D6CFF3 135C1D91 8F360292 CA44A032 5AC1A8FD 095E4865 F8C95A2B
  BFD1C2B7 E64A3804 9BBD7326 207BD456 19BAB78B D075E78E 00D2560C B09289AE
  6DECB8B0 6672FB3A 5CDAEE92 9D4C4F71 F3BCB269 214F6293 4BA8FABF 9486BCFC
  2B941BCA 550999A7 2EFE12A5 6B7B669A 2D88AB77 39B38E0E AA23CB8C B7020301 0001
% Key pair was generated at: 19:14:13 GMT Dec 21 2004
Key name: TP-self-signed-3326000105.server
 Usage: Encryption Key
 Key is not exportable.
 Key Data:
  307C300D 06092A86 4886F70D 01010105 00036B00 30680261 00C5680E 89777B42
  463E5783 FE96EA9E F446DC7B 70499AF3 EA266651 56EE29F4 5B003D93 2FC9F81D
  8A46E12F 3FBAC2F3 046ED9DD C5F27C20 1BBA6B9B 08F16E45 C34D6337 F863D605
  34E30F0E B4921BC5 DAC9EBBA 50C54AA0 BF551BDD 88453F50 61020301 0001
```

（注） TP-self-signed-3326000105.server という 2 番目のキー ペアは、SSH キー ペアです。ルータに任意のキー ペアが作成されて SSH が起動すると、生成されます。

次の例では、「local」というトラストポイントに関する情報を表示します。

```
Router# show crypto pki trustpoints

Trustpoint local:
    Subject Name:
    serialNumber=C63EBBE9+ipaddress=10.3.0.18+hostname=test.example.com
          Serial Number: 01
    Persistent self-signed certificate trust point
```

HTTP による直接登録の設定例

次の例では、HTTP による CA サーバへの直接登録ための登録プロファイルを設定する方法を示します。

```
crypto pki trustpoint Entrust
 enrollment profile E
 serial

crypto pki profile enrollment E
 authentication url http://entrust:81
 authentication command GET /certs/cacert.der
 enrollment url http://entrust:81/cda-cgi/clientcgi.exe
 enrollment command POST reference_number=$P2&authcode=$P1
 &retrievedAs=rawDER&action=getServerCert&pkcs10Request=$REQ
 parameter 1 value aaaa-bbbb-cccc
 parameter 2 value 5001
```

その他の参考資料

ここでは、PKI での証明書登録に関する参考資料を示します。

関連資料

内容	参照先
USB トークンによる RSA 処理 : USB トークンを使用するメリット	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Storing PKI Credentials」の章
USB トークンによる RSA 処理 : 証明書サーバの設定	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Configuring and Managing a Cisco IOS Certificate Server for PKI Deployment」の章 「Generating a Certificate Server RSA Key Pair」、「Configuring a Certificate Server Trustpoint」、および関連する例を参照してください。
PKI の概要（RSA キー、証明書登録、および CA を含む）	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Cisco IOS PKI Overview: Understanding and Planning a PKI」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
RSA キーの生成および展開	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Deploying RSA Keys Within 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
USB トークンの設定および使用	『*Cisco IOS Security Configuration Guide: Secure Connectivity*』の「Storing PKI Credentials」の章
Cisco IOS セキュリティ コマンド	『*Cisco IOS Security Command Reference*』
Suite-B の ESP トランスフォーム	『Configuring Security for VPNs with IPsec』フィーチャ モジュール
Suite-B SHA-2 ファミリ（HMAC バリアント）および Elliptic Curve（EC）キー ペアの設定	『Configuring Internet Key Exchange for IPsec VPNs』フィーチャ モジュール

内容	参照先
Suite-B 整合性アルゴリズム タイプのトランスフォームの設定	『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール
IKEv2 用の Suite-B の Elliptic Curve Digital Signature Algorithm（ECDSA）signature（ECDSA-sig）認証方式の設定	『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール
IPsec SA ネゴシエーションでの Suite-B の Elliptic Curve Diffie-Hellman（ECDH）のサポート	『Configuring Internet Key Exchange for IPsec VPNs』および『Configuring Internet Key Exchange Version 2 (IKEv2)』フィーチャ モジュール

規格

規格	タイトル
新しい規格または変更された規格はサポートされていません。また、既存の規格に対するサポートに変更はありません。	—

MIB

MIB	MIB リンク
新しい MIB または変更された MIB はサポートされていません。また、既存の MIB に対するサポートに変更はありません。	選択したプラットフォーム、Cisco IOS 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。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
新しい RFC または変更された RFC はサポートされていません。また、既存の RFC に対するサポートに変更はありません。	—

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。 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。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・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 ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・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 ・トレーニング リソースへアクセスする ・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 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

PKI 証明書登録の機能情報

表 1 に、この章に記載されている機能および具体的な設定情報へのリンクを示します。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。

ここに記載されていないこのテクノロジーの機能情報については、「Implementing and Managing PKI Features Roadmap」を参照してください。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、Cisco IOS および Catalyst OS ソフトウェア イメージがサポートする特定のソフトウェア リリース、機能セット、またはプラットフォームを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスしてください。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　PKI 証明書登録の機能情報

機能名	リリース	機能情報
Cisco IOS USB トークン PKI 拡張：フェーズ 2	12.4(11)T	この機能では、USB トークンを暗号装置として使用することにより、USB トークンの機能を拡張します。USB トークンをキー生成、署名、認証などの RSA 処理に使用できます。 この機能に関する詳細については、次の項を参照してください。 • 「証明書登録または自動登録の設定」 **（注）** このマニュアルでは、トラストポイントの初期の自動登録時の RSA 処理における USB トークンの使用方法について説明します。この機能に関連するその他のマニュアルについては、「関連資料」を参照してください。
認証局キー ロールオーバー	12.4(2)T	この機能により、ルート CA は、手動による介入を行わずに、失効する CA 証明書およびキーをロールオーバーし、これらの変更を PKI ネットワークを介して伝搬できるようになりました。 この機能に関する詳細については、次の各項を参照してください。 • 「自動証明書登録」 • 「証明書登録または自動登録の設定」 この機能により、次のコマンドが導入または変更されました。**auto-rollover**、**crypto pki certificate chain**、**crypto pki export pem**、**crypto pki server**、**crypto pki server info request**、**show crypto pki certificates**、**show crypto pki server**、**show crypto pki trustpoint**
証明書の自動登録	12.2(8)T	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。 この機能に関する詳細については、次の各項を参照してください。 • 「自動証明書登録」 • 「証明書登録または自動登録の設定」 この機能により、**auto-enroll**、**rsakeypair**、**show crypto ca timers** の各コマンドが導入されました。

表 1　PKI 証明書登録の機能情報 （続き）

機能名	リリース	機能情報
証明書登録の拡張機能	12.2(8)T	この機能では、5 つの新しい **crypto ca 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ので、ユーザはプロンプトを最後まで進む必要はなく、設定でフィールドを指定できます。 この機能に関する詳細については、次の項を参照してください。 • 「証明書登録または自動登録の設定」 この機能により、**ip-address（CA トラストポイント）**、**password（CA トラストポイント）**、**serial-number**、**subject-name**、**usage** の各コマンドが導入されました。
HTTP による CA サーバへの直接登録	12.3(4)T	ユーザの CA サーバが SCEP をサポートしておらず、また RA モード CS を使用しない場合、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 モード CS ではなく CA サーバに直接送信できます。 この機能に関する詳細については、次の各項を参照してください。 • 「証明書登録プロファイル」 • 「登録または再登録用の証明書登録プロファイルの設定」 この機能により、次のコマンドが導入されました。**authentication command**、**authentication terminal**、**authentication url**、**crypto ca profile enrollment**、**enrollment command**、**enrollment profile**、**enrollment terminal**、**enrollment url**、**parameter**
RSA キー ペアおよび PEM 形式証明書のインポート	12.3(4)T	この機能を使用すると、証明書要求を発行したり、PEM 形式ファイルで発行された証明書を受け取ることができます。 この機能に関する詳細については、次の項を参照してください。 • 「手動での証明書登録の設定」 この機能により、**enrollment** および **enrollment terminal** コマンドが変更されました。

表 1　PKI 証明書登録の機能情報 （続き）

機能名	リリース	機能情報
証明書更新用のキー ロールオーバー	12.3(7)T	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い、新しい証明書が使用可能になるまで古いキーと証明書を保持できます。 この機能に関する詳細については、次の各項を参照してください。 • 「自動証明書登録」 • 「証明書登録または自動登録の設定」 • 「手動での証明書登録の設定」 この機能により、次のコマンドが導入または変更されました。**auto-enroll** および **regenerate**
手動での証明書登録（TFTP によるカットアンドペースト）	12.2(13)T	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。 この機能に関する詳細については、次の各項を参照してください。 • 「サポートされる証明書の登録方式」 • 「手動での証明書登録の設定」 この機能により、次のコマンドが導入または変更されました。**crypto ca import**、**enrollment**、および **enrollment terminal**
複数階層の CA 階層構造	12.2(15)T	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。 この拡張機能の詳細については、次の項を参照してください。 • 「複数の CA のためのフレームワーク」 **（注）** これはマイナーな拡張です。マイナーな拡張は、通常 Feature Navigator に記載されません。
永続的自己署名証明書	12.2(33)SXH 12.2(33)SRA 12.3(14)T	この機能により、HTTPS サーバ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。 この機能に関する詳細については、次の各項を参照してください。 • 「サポートされる証明書の登録方式」 • 「登録用の永続的自己署名証明書の SSL による設定」 この機能により、次のコマンドが導入または変更されました。**enrollment selfsigned**、**show crypto pki certificates**、**show crypto pki trustpoints**

表 1　PKI 証明書登録の機能情報 （続き）

機能名	リリース	機能情報
PKI ステータス	12.3(11)T	この拡張では、**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。これ以前の拡張では、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。 この拡張機能の詳細については、次の項を参照してください。 • 「PKI の証明書登録を設定する方法」 **（注）** これはマイナーな拡張です。マイナーな拡張は、通常 Feature Navigator に記載されません。
既存の証明書を使用した再登録	12.3(11)T	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。 この拡張機能の詳細については、次の項を参照してください。 • 「登録または再登録用の証明書登録プロファイルの設定」 この機能により、**enrollment credential** および **grant auto trustpoint** コマンドが導入されました。

表 1　PKI 証明書登録の機能情報 （続き）

機能名	リリース	機能情報
トラストポイント CLI	12.2(8)T	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。
IOS SW の暗号化での Suite-B のサポート	15.1(2)T	Suite-B によって、PKI の証明書登録に次のサポートが追加されます。 • X.509 証明書内の署名操作で、Elliptic Curve Digital Signature Algorithm（ECDSA）（256 ビットおよび 384 ビットの曲線）が使用されます。 • ECDSA の署名を使用した X.509 証明書の確認で PKI がサポートされます。 • ECDSA の署名を使用した証明書要求の生成、および発行された証明書の IOS へのインポートで、PKI がサポートされます。 Suite B の要件は、IKE および IPSec で使用するための暗号化アルゴリズムの 4 つのユーザ インターフェイス スイートで構成され、RFC 4869 に記述されています。各スイートは、暗号化アルゴリズム、デジタル署名アルゴリズム、キー合意アルゴリズム、ハッシュまたはメッセージ ダイジェスト アルゴリズムで構成されています。Cisco IOS での Suite-B サポートに関する詳細については、『Configuring Security for VPNs with IPsec』フィーチャ モジュールを参照してください。 この機能に関する詳細については、次の各項を参照してください。 • 「PKI の証明書登録のための Cisco IOS Suite-B サポート」（P.4） • 「証明書登録または自動登録の設定」（P.6） 次のコマンドが導入または変更されました。