CHAPTER 27

IPSec VPN SPA を使用した PKI の設定

この章では、Cisco 7600 シリーズ ルータ上の IPSec VPN SPA を使用して Public Key Infrastructure（PKI; 公開鍵インフラストラクチャ）関連機能を設定する方法について説明します。具体的な内容は次のとおりです。

（注） この章の手順では、読者が PKI 設定の概念にある程度精通していると想定しています。PKI コンフィギュレーションの概念についての詳細は、『*Cisco IOS Security Configuration Guide*』および『*Cisco IOS Security Command Reference*』を参照してください。

システム イメージおよびコンフィギュレーション ファイルの管理については、『*Cisco IOS Configuration Fundamentals Configuration Guide*』および『*Cisco IOS Configuration Fundamentals Command Reference*』を参照してください。

この章で使用するコマンドの詳細については、『*Cisco IOS Software Releases 12.2SR Command Reference*s』および『*Cisco IOS Software Releases 12.2SX Command References*』を参照してください。また、関連する CiscoIOS Release12.2 ソフトウェア コマンド リファレンスおよびマスター インデックスも参照してください。詳細については、「関連資料」（p.lv）を参照してください。

ヒント　IPSec VPN SPA を使用して Virtual Private Network（VPN; バーチャル プライベート ネットワーク）を正しく設定するために、設定の概要および注意事項にすべて目を通してから設定作業を始めてください。

PKI の概要

Cisco IOS PKI には、IP Security（IPSec）、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機能があります。

PKI は次のエンティティで構成されます。

- セキュア ネットワークで通信するピア
- 証明書を設定して保持する 1 つまたは複数の CA（認証局）
- デジタル証明書。証明書の有効期間、ピア アイデンティティ情報、セキュアな通信を実現するために使用される暗号化キー、発行元 CA のシグニチャなどの情報が格納されます。
- 登録要求を処理して CA をオフロードするための、オプションの Registration Authority（RA; 登録局）
- Certificate Revocation List（CRL; 証明書失効リスト）用の配信メカニズム（Lightweight Directory Access Protocol（LDAP）または HTTP）

PKI はカスタマーに、セキュアなデータ ネットワークで暗号化情報およびアイデンティティ情報を配信、管理、および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提供します。セキュアな通信に関与するすべてのエンティティ（ユーザまたはデバイス）は、エンティティが Rivest, Shamir, and Adelman（RSA）キー ペア（1 つの秘密鍵および 1 つの公開鍵）を生成し、信頼できるエンティティ（別名 CA またはトラストポイント）でアイデンティティを検証するプロセスで、PKI に登録されます。

各エンティティが PKI に登録されると、PKI 内のすべてのピア（別名エンド ホスト）に、CA から発行されたデジタル証明書が設定されます。ピアがセキュアな通信セッションをネゴシエートする必要がある場合は、デジタル証明書が交換されます。ピアは証明書内の情報に基づいて、別のピアのアイデンティティを検証し、証明書内の公開鍵を使用して暗号化セッションを確立できます。

PKI を設定するには、次のタスクを実行します。

- PKI に RSA キーを配置します。ルータの証明書を取得するには、RSA キー ペア（公開鍵と秘密鍵が 1 つずつ）が必要です。つまり、エンド ホストが証明書を取得して、PKI に登録するには、RSA キー ペアを生成し、公開鍵を CA と交換する必要があります。
- PKI に証明書の許可および失効を設定します。適切に署名された証明書であると検証された証明書は、証明書マップ、PKI AAA、または証明書ベース Access Control List（ACL; アクセスコントロールリスト）などの方法で許可されます。また、発行元の CA で失効ステータスが調べられ、証明書が失効していないことが確認されます。
- 証明書登録を設定します。このプロセスでは、CA から証明書を取得します。証明書登録は、証明書の要求元エンド ホストと CA の間で実行されます。PKI に関与する各ピアで、CA 登録が必要になります。証明書登録には、さまざまな方法を使用できます。
- RSA キーや証明書など、PKI 証明書の保存。これらの証明書は、ルータのデフォルトの場所（NVRAM［不揮発性 RAM］）などに保存できます。

複数の RSA キー ペアの設定

複数の RSA キー ペア サポート機能を使用すると、Cisco 7600 シリーズ ルータが複数の RSA キー ペア を持つように設定できます。Cisco IOS ソフトウェアでは、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。

この機能が実装される前、Cisco IOS PKI 設定では 1 つの汎用キー ペアまたは一組の特定目的キー ペア（暗号化および署名キー ペア）のいずれかのみが使用可能でした。キー ペアが導入されるシナリオでは、多くの場合、ルータを複数の証明書サーバに登録する設定が必要です。各サーバには個別のポリシーが設定されており、また汎用証明書 / 特定目的証明書またはキーの長さなどの要件が異なる可能性があるためです。この機能を使用すると、ルータを登録する CA ごとに別個のキー ペアを設定し、他の CA が指定した要件（キーの長さ、キーのライフタイム、汎用キー / 特定目的キーなど）を損なうことなく各 CA のポリシー要件に対応することができます。

複数の RSA キー ペア設定時の注意事項および制約事項

複数の RSA キー ペアを設定する場合は、次の注意事項および制約事項に従ってください。

- SSL または他の PKI クライアントが、重複して同じ CA に登録を試みないようにすることを推奨します。
- Internet Key Exchange（IKE; インターネット キー エクスチェンジ）は、名前付きのキー ペアを使用するように設定されているアイデンティティに関しては無効です。IKE ピアが複数のキーをサポートする PKI トラストポイントからの証明書を要求する場合、交換の最初の部分は有効で、証明書応答では正しい証明書が送信されます。ただし、名前付きのキー ペアは使用されず、IKE ネゴシエーションが失敗します。
- キー ペアを再生成する場合は、必ずそのキー ペアを使用して証明書アイデンティティを再登録する必要があります。

RSA キー ペアを設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto key generate rsa [usage-keys | general-keys] [key-pair-label]`	RSA キー ペアを生成します。 • ***usage-keys*** — （任意）1 つの汎用キー ペアではなく、2 つの特定目的キー ペアを生成するように指定します。 • ***general-keys*** — （任意）汎用キー ペアを生成するように指定します。 • *key-pair-label* —（任意）ルータが使用するキー ペア名を指定します（この引数をイネーブルにする場合、***usage-keys*** または ***general-keys*** のどちらかを指定する必要があります）。

	コマンド	説明
ステップ 2	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA の名前
ステップ 3	`Router(ca-trustpoint)# rsakeypair key-label [key-size [encryption-key-size]]`	証明書と対応付けるキー ペアを指定します。 • *key-label* — キー ペアの名前がまだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合、登録時に生成されるキー ペアの名前 • *key-size* —（任意）希望する RSA キーのサイズ。指定しない場合、既存のキー サイズが使用されます（指定するサイズは、*encryption-key-size* と同じである必要があります）。 • *encryption-key-size* —（任意）個別の暗号化、シグニチャ キー、および証明書を要求する場合に使用する、2 番めのキーのサイズ（指定するサイズは、*key-size* と同じである必要があります）

RSA キー ペア設定の削除

特定の RSA キー ペアまたはルータが生成したすべての RSA キー ペアを削除するには、グローバル コンフィギュレーション モードで次のように **crypto key zeroize rsa** コマンドを入力します。

```
Router(config)# crypto key zeroize rsa [key-pair-label]
```

key-pair-label は、削除するキー ペアを指定します。*key-pair-label* 引数を使用すると、指定した RSA キー ペアだけが削除されます。引数を使用しない場合、すべての RSA キー ペアがルータから削除されます。

RSA キー情報の確認

RSA キー情報を確認するには、例で使用されている特権 EXEC コマンドのうち最低 1 つを使用します。

ルータの RSA 公開鍵を表示するには、**show crypto key mypubkey rsa** コマンドを使用します。

```
Router# show crypto key mypubkey rsa

% Key pair was generated at: 06:07:50 UTC Jan 13 1996

Key name: myルータ .example.com

 Usage: Encryption Key

 Key Data:

  00302017 4A7D385B 1234EF29 335FC973 2DD50A37 C4F4B0FD 9DADE748 429618D5

  18242BA3 2EDFBDD3 4296142A DDF7D3D8 08407685 2F2190A0 0B43F1BD 9A8A26DB

  07953829 791FCDE9 A98420F0 6A82045B 90288A26 DBC64468 7789F76E EE21
```

ルータに保存されているすべての RSA 公開鍵（IPSec のピア認証時にルータに証明書を送信したピアの公開鍵を含む）を一覧表示するか、またはルータに保存されている特定の RSA 公開鍵の詳細情報を表示するには、**show crypto key pubkey-chain rsa** コマンドを使用します。

```
Router# show crypto key pubkey-chain rsa

Codes: M - Manually Configured, C - Extracted from certificate

Code  Usage        IP-address     Name

M     Signature    10.0.0.1       myrouter.example.com

M     Encryption   10.0.0.1       myrouter.example.com

C     Signature    172.16.0.1     routerA.example.com

C     Encryption   172.16.0.1     routerA.example.com

C     General      192.168.10.3   routerB.domain1.com
```

複数の RSA キー ペアのサポートに関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmltkey.htm

RSA キー ペアの設定例は、「複数の RSA キー ペアの設定例」（p.27-55）を参照してください。

保護された秘密鍵ストレージの設定

保護された秘密鍵ストレージ機能により、Cisco 7600 シリーズ ルータで使用する RSA 秘密鍵を暗号化およびロックし、秘密鍵の不正使用を防ぐことができます。

保護された秘密鍵ストレージ設定時の注意事項および制約事項

保護された秘密鍵ストレージを設定する場合は、次の注意事項および制約事項に従ってください。

- ルータの起動後、キーを手動で（**crypto key unlock rsa** コマンドを使用して）アンロックするまで、暗号キーは有効ではありません。暗号化されているキー ペアによっては、この機能により IPSec、SSH、SSL などのアプリケーションに悪影響が及ぶ可能性があります。つまり、必要なキー ペアがアンロックされるまで、セキュア チャネル経由でのルータ管理ができない場合があります。
- パスフレーズを忘れた場合、キーを再生成し、CA サーバに再登録し、新しい証明書を取得する必要があります。消失したパスフレーズを回復することはできません。
- パスフレーズを変更するには、**crypto key decrypt rsa** コマンドを使用して現在のパスフレーズでキーを復号化し、そのキーを再び暗号化して、新しいパスフレーズを指定する必要があります。

秘密鍵の設定

秘密鍵を暗号化、復号化、ロック、およびアンロックするには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto key encrypt [write] rsa [name key-name] passphrase passphrase`	RSA キーを暗号化します。このコマンドの入力後も、引き続きそのキーはルータで使用できます。キーはアンロックされたままです。 • ***write*** — （任意）ルータ コンフィギュレーションをただちに NVRAM に書き込みます。**write** キーワードを指定しない場合、手動でコンフィギュレーションを NVRAM に書き込む必要があります。この作業を行わないと、次にルータをリロードした際に、暗号化されたキーが消去されます。 • ***name key-name*** —（任意）暗号化する RSA キー ペアの名前。キー名を指定しない場合、デフォルトのキー名である router name.domainname が使用されます。 • ***passphrase passphrase*** — RSA キーの暗号化に使用するパスフレーズ。RSA キー ペアにアクセスするには、このパスフレーズを指定する必要があります。
ステップ 2	`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 3	`Router# show crypto key mypubkey rsa`	（任意）秘密鍵が暗号化（保護）され、アンロックされていることを確認します。

	コマンド	説明
ステップ 4	Router# **crypto key lock rsa** [***name*** *key-name*] ***passphrase*** *passphrase*	(任意)暗号化された秘密鍵を稼働中のルータ上でロックします。 • ***name*** *key-name* —（任意）ロックする RSA キー ペアの名前。キー名を指定しない場合、デフォルトのキー名である router name.domainname が使用されます。 • ***passphrase*** *passphrase* — RSA キーのロックに使用するパスフレーズ。RSA キー ペアにアクセスするには、このパスフレーズを指定する必要があります。 **（注）** キーをロックしたあとは、そのキーを使用してピア デバイスにルータを認証することはできません。この動作により、ロックされたキーを使用する IPSec または SSL 接続はすべてディセーブルになります。ロックされたキーに基づいて作成された既存の IPSec トンネルは、閉じられます。すべての RSA キーをロックすると、SSH は自動的にディセーブルになります。
ステップ 5	Router# **show crypto key mypubkey rsa**	(任意)秘密鍵が保護されロックされていることを確認します。 このコマンドの出力では、IKE、SSH、SSL などのアプリケーションによって試行された接続の失敗も表示されます。
ステップ 6	Router# **crypto key unlock rsa** [***name*** *key-name*] **passphrase** *passphrase*	(任意）秘密鍵をアンロックします。 • ***name*** *key-name* —（任意）アンロックする RSA キー ペアの名前。キー名を指定しない場合、デフォルトのキー名である router name.domainname が使用されます。 • ***passphrase*** *passphrase* — RSA キーのアンロックに使用するパスフレーズ。RSA キー ペアにアクセスするには、このパスフレーズを指定する必要があります。 **（注）** このコマンドを入力すると、引き続き IKE トンネルの確立を実行できます。
ステップ 7	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 8	Router(config)# **crypto key decrypt** [***write***] ***rsa*** [***name*** *key-name*] ***passphrase*** *passphrase*	(任意）暗号化されたキーを削除し、暗号化されていないキーだけを残します。 • ***write*** —（任意）暗号化されていないキーをただちに NVRAM に書き込みます。**write** キーワードを指定しない場合、手動でコンフィギュレーションを NVRAM に書き込む必要があります。この作業を行わないと、次にルータをリロードした際に、キーが暗号化されたままになります。 • ***name*** *key-name* —（任意）削除する RSA キー ペアの名前。キー名を指定しない場合、デフォルトのキー名である router name.domainname が使用されます。 • ***passphrase*** *passphrase* — RSA キーの削除に使用するパスフレーズ。RSA キー ペアにアクセスするには、このパスフレーズを指定する必要があります。

秘密鍵の保護およびロックの確認

キーが保護（暗号化）およびロックされたことを確認するには、**show crypto key mypubkey rsa** コマンドを入力します。

```
Router# show crypto key mypubkey rsa

% Key pair was generated at:20:29:41 GMT Jun 20 2003
Key name:pki1-72a.cisco.com
Usage:General Purpose Key
*** The key is protected and LOCKED. ***
Key is exportable.
Key Data:
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00D7808D C5FF14AC
0D2B55AC 5D199F2F 7CB4B355 C555E07B 6D0DECBE 4519B1F0 75B12D6F 902D6E9F
B6FDAD8D 654EF851 5701D5D7 EDA047ED 9A2A619D 5639DF18 EB020301 0001
```

保護された秘密鍵ストレージに関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_ppkey.htm

秘密鍵の保護の設定例は、「保護された秘密鍵ストレージの設定例」（p.27-55）を参照してください。

トラストポイント CA の設定

crypto pki trustpoint コマンドを使用すると、ご使用のルータで使用する CA を宣言して、CA の特性を指定できます。

crypto pki trustpoint コマンドは、既存の **crypto ca identity** コマンドと **crypto ca trusted-root** コマンドの機能を統合および置換します。これら 2 つの既存のコマンドでもご使用のルータで使用する CA を宣言できますが、登録（CA からのルータ証明書の要求）をサポートしているのは **crypto ca identity** コマンドだけです。

トラストポイント CA 設定時の注意事項および制約事項

トラストポイント CA を設定する場合は、次の注意事項および制約事項に従ってください。

- トラストポイント CA を設定すると、**crypto pki authenticate** コマンドを使用して CA の証明書を取得できるほか、**crypto pki certificate query** コマンドを使用して、証明書をローカルに保存せず、CA トラストポイントから取得するように指定できます。
- 通常、証明書はルータの NVRAM にローカルに保存され、証明書ごとに相応のメモリを使用します。NVRAM のスペースを節約するには、**crypto pki certificate query** コマンドを使用してルータをクエリー モードにし、証明書をローカルに保存するのではなく、必要なときに特定の CA トラストポイントから取得するようにします。この方法では、NVRAM スペースを節約できますが、パフォーマンスに多少影響が出る可能性があります。

ルータが使用する CA を宣言し、トラストポイント CA の特性を指定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint` *name*	ルータが使用する CA を宣言します。このコマンドをイネーブルにすると、ca-trustpoint コンフィギュレーション モードが開始されます。 • *name* — CA トラストポイントの名前

	コマンド	説明
ステップ 2	`Router(ca-trustpoint)# enrollment [[mode ra] | [retry period minutes] | [retry count number] | [url url]]`	CA への登録パラメータを指定します。 • ***mode ra*** — （任意）CA システムが RA を提供している場合、RA モードを指定します。***mode ra*** キーワードをイネーブルにしないかぎり、*RA* モードはオフになります。 • *minutes* —（任意）証明書要求を再試行する間隔を指定します。デフォルトでは 1 分間隔で再試行されます。（1 ～ 60 分の範囲で指定）。 • *number* —（任意）要求への応答が得られない場合、ルータが証明書要求を再送信する回数を指定しますデフォルトは 10 回です（1 ～ 100 の範囲で指定）。 • *url* — ルータが証明書要求を送信する CA の URL（たとえば http://ca_server）を指定します。*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 または IP アドレスです。
	`Router(ca-trustpoint)# root tftp server-hostname filename`	TFTP（簡易ファイル転送プロトコル）を使用して CA を取得します。 • *server-hostname* — トラストポイント CA を保存するサーバの名前 • *filename* — トラストポイント CA を保存するファイルの名前
ステップ 3	`Router(ca-trustpoint)# enrollment http-proxy host-name port-num`	HTTP を使用し、プロキシ サーバ経由で CA を取得します。 • *host-name* — CA を取得するために使用するプロキシ サーバの名前 • *port-num* — CA にアクセスするために使用するポート番号 **（注）** このコマンドは、**enrollment** コマンドと組み合わせた場合のみ使用可能です。
ステップ 4	`Router(ca-trustpoint)# primary name`	（任意）特定のトラストポイントをルータのプライマリ トラストポイントに指定します。 • *name* — ルータのプライマリ トラストポイントの名前
ステップ 5	`Router(ca-trustpoint)# crl {query url | optional}`	（任意）CRL を照会し、ピアの証明書が失効していないことを確認します。 • *url* — CRL を照会するため、CA サーバが公開している LDAP URL（たとえば、ldap://another_server）を指定します。 • ***optional*** — CRL の確認は省略可能です。 **（注）** ***query url*** オプションをイネーブルにしない場合、ルータは証明書に埋め込まれている Certificate Distribution Point（CDP）をチェックします。

	コマンド	説明
ステップ 6	`Router(ca-trustpoint)# default command-name`	(任意) ca-trustpoint コンフィギュレーション モードの値をデフォルトに設定します。 • *command-name* — pki-trustpoint コンフィギュレーション サブコマンド。デフォルトはオフです。
ステップ 7	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 モードを開始します。
ステップ 8	`Router(config)# crypto pki authenticate name`	(CA の証明書を取得することにより) CA を認証します。 • *name* — CA の名前。ステップ 1 で入力した *name* 値を入力します。
ステップ 9	`Router(config)# crypto pki trustpoint name`	ca-trustpoint コンフィギュレーション モードを再び開始します。 • *name* — CA トラストポイントの名前
ステップ 10	`Router(ca-trustpoint)# crypto pki certificate query`	(任意) 特定のトラストポイントに関してクエリー モードをオンにし、証明書がローカルで保存されないようにします。

トラストポイント CA の確認

証明書、CA の証明書、および RA 証明書に関する情報を確認するには、**show crypto pki certificates** コマンドを入力します。

```
Router# show crypto pki certificates

CA Certificate

  Status: Available

  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F

  Key Usage: Not Set

RA Signature Certificate

  Status: Available

  Certificate Serial Number: 34BCF8A0

  Key Usage: Signature


RA KeyEncipher Certificate

  Status: Available

  Certificate Serial Number: 34BCF89F

  Key Usage: Encryption
```

ルータに設定されているトラストポイントを表示するには、**show crypto pki trustpoints** コマンドを入力します。

```
Router# show crypto pki trustpoints

Trustpoint bo:
Subject Name:
CN = bomborra Certificate Manager
O = cisco.com
C = US
Serial Number:01
Certificate configured.
CEP URL:http://bomborra
CRL query url:ldap://bomborra
```

トラストポイント CA に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fttrust.htm

トラストポイント CA の設定例は、「トラストポイント CA の設定例」(p.27-56) を参照してください。

トラストポイント単位でのクエリー モード定義の設定

証明書には公開鍵情報が含まれ、アイデンティティの証明として CA による署名がされています。通常、すべての証明書はルータの NVRAM にローカルに保存され、証明書ごとに相応のメモリを使用します。トラストポイント単位でのクエリー モード定義機能により、トラストポイントに関するクエリーを定義し、特定のトラストポイントに対応する証明書をリモート サーバに保存できるようになります。

この機能では、トラストポイントの使用をより詳しく制御できるため、ルータに複数のトラストポイントを設定している環境で特に役立ちます。ルータ上のすべてのトラストポイントではなく、特定のトラストポイントを対象に、クエリー モードをアクティブにできます。

トラストポイント単位でのクエリー モード定義設定時の注意事項および制約事項

トラストポイント単位でのクエリー モード定義を設定する場合は、次の注意事項および制約事項に従ってください。

- 通常、証明書はルータの NVRAM にローカルに保存され、証明書ごとに相応のメモリを使用します。NVRAM のスペースを節約するには、**query certificate** コマンドを使用して、証明書をローカルに保存するのではなく、起動時にリモート サーバ（CA、LDAP サーバなど）から取得するようにします。この方法では、NVRAM スペースを節約できますが、パフォーマンスに多少影響が出る可能性があります。
- 特定のトラストポイントに対応する証明書が NVRAM に書き込まれることはなく、次回ルータをリロードする際に証明書クエリーが試行されます。
- グローバルな **crypto pki certificate query** コマンドを使用する場合、ルータ上のすべてのトラストポイントに証明書のクエリーが追加されます。**no crypto pki certificate query** コマンドを使用すると、以前の証明書クエリーの設定がすべてのトラストポイントから削除され、実行中のクエリーが停止されて、この機能がディセーブルになります。

トラストポイント CA を設定し、そのトラストポイントに関してクエリー モードを開始するには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言します。このコマンドをイネーブルにすると、ca-trustpoint コンフィギュレーション モードが開始されます。 • *name* — CA トラストポイントの名前

	コマンド	説明
ステップ 2	`Router(ca-trustpoint)# enrollment [[mode ra] | [retry period minutes] | [retry count number] | [url url]]`	CA への登録パラメータを指定します。 • ***mode ra*** — （任意）CA システムが RA を提供している場合、RA モードを指定します。***mode ra*** キーワードをイネーブルにしないかぎり、*RA* モードはオフになります。 • *minutes* —（任意）証明書要求を再試行する間隔を指定します。デフォルトでは 1 分間隔で再試行されます。（1 ～ 60 分の範囲で指定）。 • *number* —（任意）要求への応答が得られない場合、ルータが証明書要求を再送信する回数を指定しますデフォルトは 10 回です（1 ～ 100 の範囲で指定）。 • *url* — ルータが証明書要求を送信する CA の URL（たとえば http://ca_server）を指定します。*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 または IP アドレスです。
ステップ 3	`Router(ca-trustpoint)# enrollment http-proxy host-name port-num`	（任意）HTTP を使用し、プロキシ サーバ経由で CA を取得します。 • *host-name* — CA を取得するために使用するプロキシ サーバの名前 • *port-num* — CA にアクセスするために使用するポート番号 **（注）** このコマンドは、**enrollment** コマンドと組み合わせた場合のみ使用可能です。
ステップ 4	`Router(ca-trustpoint)# crl query url`	（任意）CA サーバが LDAP によるクエリー モードをサポートしている場合、CA サーバの URL を指定します。 • *url* — CA サーバが公開している LDAP URL
ステップ 5	`Router(ca-trustpoint)# default command-name`	（任意）ca-trustpoint コンフィギュレーション モードの値をデフォルトに設定します。 • *command-name* — pki-trustpoint コンフィギュレーション サブコマンド。デフォルトはオフです。
ステップ 6	`Router(ca-trustpoint)# query certificate`	指定したトラストポイントに関するクエリー モードをオンにし、証明書をローカルに保存せず、リモート サーバから取得するようにします。
ステップ 7	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 モードを開始します。
ステップ 8	`Router(config)# crypto pki authenticate name`	（CA の証明書を取得することにより）CA を認証します。 • *name* — CA の名前。ステップ 1 で入力した *name* 値を入力します。
ステップ 9	`Router(config)# crypto key generate rsa`	（任意）RSA キー ペアを生成します。
ステップ 10	`Router(config)# crypto pki enroll trustpoint-name`	（任意）ルータ証明書を取得します。 • *trustpoint-name* — CA の名前ステップ 1 で入力した *name* 値を入力します。

トラストポイント CA 単位でのクエリー モード定義の確認

次のリロード時にクエリー モードを正常に動作させるには、トラストポイントに証明書が対応付けられている必要があります。**show crypto pki certificates** コマンドを使用して、各トラストポイントに必要な証明書があることを確認してから、コンフィギュレーションを保存しルータをリロードします。

```
Router# show crypto pki certificates status

Trustpoint yni:

  Issuing CA certificate pending:

    Subject Name:

     cn=nsca-r1 Cert Manager,ou=pki,o=cisco.com,c=US

    Fingerprint: C21514AC 12815946 09F635ED FBB6CF31

  Router certificate pending:

    Subject Name:

     hostname=trance.cisco.com,o=cisco.com

  Next query attempt:

    52 seconds
```

トラストポイント単位でのクエリー モード定義に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gt_qerym.htm

トラストポイント単位でのクエリー モード定義の設定例は、「トラストポイント単位でのクエリー モード定義の設定例」（p.27-56）を参照してください。

ローカル証明書ストレージ場所の設定

ローカル証明書ストレージ場所機能を使用すると、RSA キーや証明書などの PKI 証明書を特定の場所に保存できます。証明書ストレージ場所の例には、デフォルト場所の NVRAM、ご使用のプラットフォームでサポートされているその他のローカル ストレージ場所（フラッシュなど）が含まれます。

（注）　ローカル証明書保存場所機能は、Cisco IOS Release 12.2(33)SRA 以降でのみサポートされています。

ローカル証明書ストレージ場所設定時の注意事項および制約事項

ローカル証明書ストレージ場所を設定する場合は、次の注意事項および制約事項に従ってください。

- ローカル証明書ストレージ場所を指定する前に、システムが次の要件を満たしている必要があります。
  - Cisco IOS Release 12.4(2)T PKI 対応イメージまたはそれ以降のイメージ
  - PKI 証明書を独立したファイルとして保存可能なプラットフォーム
  - 少なくとも 1 つの証明書を含む設定
  - アクセス可能なローカル ファイル システム
- ローカル ストレージ場所に証明書を格納する場合は、次の制約事項が適用されます。
  - 使用できるのはローカル ファイル システムのみです。リモート ファイル システムが選択された場合は、エラー メッセージが表示され、コマンドは無効になります。
  - ローカル　ファイル　システムでサポートされているサブディレクトリを指定できます。NVRAM はサブディレクトリをサポートしません。
  - デフォルトでは、証明書は NVRAM に格納されます。ただし、ルータによっては、証明書を正常に保存するために必要なサイズの NVRAM が搭載されていないことがあります。Cisco IOS Release 12.4(2)T には、証明書を保存するローカル ファイル システム上の場所を指定する機能が導入されています。
  - 実行時に、証明書を保存するために使用するアクティブなローカル ストレージ デバイスを指定できます。

証明書のローカル ストレージ場所の指定

証明書のローカル ストレージ場所を指定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki certificate storage` *location-name*	証明書のローカル ストレージ場所を指定します。 • *location-name* — ストレージ場所の名前
ステップ 2	`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。

	コマンド	説明
ステップ 3	`Router# copy source-url destination-url`	（任意）実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存します。 • *source-url* — コピー元のファイルまたはディレクトリの場所を示す URL（またはエイリアス）。ファイルをダウンロードするのか、アップロードするのかに応じて、コピー元はローカルまたはリモートにできます。 • *destination-url* — コピー先のファイルまたはディレクトリを示す宛先 URL（またはエイリアス）。ファイルをダウンロードするのか、アップロードするのかに応じて、コピー先はローカルまたはリモートにできます。 （注）　設定を有効にするには、実行コンフィギュレーションをスタートアップ コンフィギュレーションに保存する必要があります。

ローカル証明書ストレージ場所の設定の確認

ローカル証明書ストレージ場所の設定を確認するには、**show crypto pki certificates storage** コマンドを入力します。

show crypto pki certificates storage コマンドは、PKI 証明書ストレージ場所の現在の設定を表示します。

次に、disk0 の certs サブディレクトリに証明書を保存する例を示します。

```
Router# show crypto pki certificates storage

Certificates will be stored in disk0:/certs/
```

ローカル証明書ストレージ場所の詳細な設定情報については、次の URL にある『*Cisco IOS Security Configuration Guide*』を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a00804a5a7f.html

ローカル証明書ストレージ場所の設定例は、「ローカル証明書ストレージ場所の設定例」（p.27-56）を参照してください。

HTTP による CA サーバへの直接登録（既存の証明書を使用した再登録）の設定

HTTP による CA サーバへの直接登録機能により、登録プロファイルを設定することで、CA に登録するときに RA をバイパスできます。この場合、HTTP 登録要求を CA サーバに直接送信できます。

「既存の証明書による再登録」機能により、サードパーティ製 CA に登録したルータが、既存の証明書を使用して Cisco IOS 証明書サーバに登録し、登録要求が自動的に許可されるようにすることができます。

HTTP による CA サーバへの直接登録設定時の注意事項および制約事項

HTTP による CA サーバへの直接登録を設定する場合は、次の注意事項および制約事項に従ってください。

- CA 証明書およびルータ証明書は、Privacy Enhanced Mail（PEM）フォーマットで返される必要があります。
- 登録プロファイルを指定する場合、トラストポイント設定に登録 URL を指定することはできません。
- 各種の CA で使用されている HTTP コマンドに関しては標準がないので、使用する CA に適したコマンドを入力する必要があります。
- 新しく作成したトラストポイントは、1 回しか使用できません（ルータを Cisco IOS CA に登録するときに使用します）。最初の登録が成功したあと、登録プロファイルから証明書情報が削除されます。
- Cisco IOS 証明書サーバは、非 Cisco IOS の CA にすでに登録しているクライアントからの要求だけを自動的に許可します。サーバを自動許可モードに設定している場合（**grant automatic** コマンドを使用）を除いて、その他の要求はすべて手動で許可する必要があります。
- HTTP による CA サーバへの直接登録を設定するには、次の作業を行います。
  - 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（「クライアント ルータの登録プロファイルの設定」[p.27-18] を参照）か、すでにサードパーティ製 CA に登録しているクライアント ルータの登録プロファイルを設定します（「サードパーティ製 CA に登録済みのクライアント ルータの登録プロファイルの設定」[p.27-20] を参照）。
  - サードパーティ製 CA トラストポイントにすでに登録しているクライアントからの登録要求だけを受け付けるように、CA 証明書サーバを設定します（「サードパーティ製 CA のクライアントからの登録要求を受け付けるための CA 設定」[p.27-21] を参照）。

クライアント ルータの登録プロファイルの設定

証明書登録プロファイルを設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	トラストポイントに対して所定の名前を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA トラストポイントの名前
ステップ 2	`Router(ca-trustpoint)# enrollment profile label`	証明書の認証および登録に、登録プロファイルを使用するよう指定します。 • *label* — 登録プロファイルの名前

	コマンド	説明
ステップ 3	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 モードを開始します。
ステップ 4	`Router(config)# crypto pki profile enrollment label`	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。**enrollment profile** コマンドで指定した名前と同じである必要があります。
ステップ 5	`Router(ca-profile-enroll)# authentication url url`	（任意）証明書認証要求を送信する 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べき CA サーバの URL。HTTP を使用する場合、この 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、この 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 Fully Qualified Domain Name（FQDN; 完全修飾ドメイン名）が使用されます。
	`Router(ca-profile-enroll)# authentication terminal`	（任意）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 6	`Router(ca-profile-enroll)# authentication command`	（任意）認証のため CA に HTTP 要求を送信します。 このコマンドは、**authentication url** コマンドを実行したあとで使用する必要があります。
ステップ 7	`Router(ca-profile-enroll)# enrollment url url` または	HTTP または TFTP で証明書登録要求を送信すべき CA サーバの URL を指定します。 • *url* — CA サーバの URL
	`Router(ca-profile-enroll)# enrollment terminal`	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 8	`Router(ca-profile-enroll)# enrollment command`	（任意）登録のため CA に HTTP コマンドを送信することを指定します。
ステップ 9	`Router(ca-profile-enroll)# parameter number {value value | prompt string}`	（任意）登録プロファイルのパラメータを指定します。 • *number* — ユーザ パラメータ。有効な値の範囲は 1 ～ 18 です。 • *value* — パラメータに定数値がある場合に使用します。 • *string* — **crypto pki authenticate** コマンドまたは **crypto pki enroll** コマンドを実行したあとでパラメータを指定する場合に使用します。 **（注）** *string* 引数の値は、ルータが使用する値には影響しません。 このコマンドを繰り返して使用し、複数の値を指定できます。

	コマンド	説明
ステップ 10	`Router(ca-profile-enroll config)# exit`	ca-profile-enroll 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 モードを開始します。
ステップ 11	`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、特権 EXEC モードを開始します。
ステップ 12	`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確認します。
ステップ 13	`Router# show crypto pki trustpoints`	（任意）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。

サードパーティ製 CA に登録済みのクライアント ルータの登録プロファイルの設定

すでにサードパーティ製 CA に登録しているクライアント ルータを Cisco IOS 証明書サーバに再登録するには、次の作業を行います。設定を始める前に、事前に必要な作業があります。

事前に必要な作業

サードパーティに登録済みのクライアント ルータの証明書登録プロファイルを設定する前に、関連するクライアント ルータで次の作業が完了している必要があります。

- サードパーティ製 CA を指定するトラストポイントの定義
- サードパーティ製 CA でのクライアント ルータの認証および登録

サードパーティ製 CA に登録済みのクライアント ルータの証明書登録プロファイルを設定し、ルータを Cisco IOS 証明書サーバに再登録するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint` *name*	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — 使用する Cisco IOS CA の名前
ステップ 2	`Router(ca-trustpoint)# enrollment profile` *label*	証明書登録のために、登録プロファイルの使用を指定します。 • *label* — 登録プロファイルの名前
ステップ 3	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 モードを開始します。
ステップ 4	`Router(config)# crypto pki profile enrollment` *label*	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。ステップ 2 の **enrollment profile** コマンドで指定した名前と同じである必要があります。
ステップ 5	`Router(ca-profile-enroll)# enrollment url` *url*	HTTP で証明書登録要求を送信する CA サーバの URL を指定します。 • *url* — Cisco IOS CA を指定する登録 URL

	コマンド	説明
ステップ 6	`Router(ca-profile-enroll)# enrollment credential label`	Cisco IOS CA に登録する非 Cisco IOS CA トラストポイントを指定します。 • *label* — 他社製 CA トラストポイントの名前
ステップ 7	`Router(ca-profile-enroll)# exit`	ca-profile-enroll 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 モードを開始します。
ステップ 8	`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、特権 EXEC モードを開始します。
ステップ 9	`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確認します。
ステップ 10	`Router# show crypto pki trustpoints`	（任意）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。

サードパーティ製 CA のクライアントからの登録要求を受け付けるための CA 設定

サードパーティ製 CA トラストポイントに登録済みのクライアントからのみ、登録要求を受け付けるように CA 証明書サーバを設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# ip http server`	システムで HTTP サーバをイネーブルにします。
ステップ 2	`Router(config)# crypto pki server cs-label`	証明書サーバをイネーブルにし、証明書サーバ コンフィギュレーション モードを開始します。 • *cs-label* — *cs-label* 引数は、クライアント ルータの **crypto pki trustpoint** コマンドで指定した名前と同じである必要があります。
ステップ 3	`Router(cs-server)# database url root-url`	証明書サーバのすべてのデータベース エントリを書き込む場所を指定します。 • *root-url* — ルート URL **（注）** このコマンドを指定しない場合、すべてのデータベース エントリが NVRAM に書き込まれます。

	コマンド	説明
ステップ 4	`Router(cs-server)# database level {minimal | names | complete}`	証明書登録データベースに保存するデータのタイプを制御します。 • ***minimal*** — 新しい証明書を競合を発生させずに発行し続けるために、十分な情報だけを保存します。これがデフォルト値です。 • ***names*** — minimal レベルで提供される情報に加えて、各証明書のシリアル番号および件名を保存します。 • ***complete*** — minimal および names レベルで提供される情報に加えて、発行した各証明書をデータベースに書き込みます。 （注）　**complete** キーワードを指定すると、大量の情報が生成されます。このキーワードを使用する場合は、**database url** コマンドを使用して、データを保存する外部 TFTP サーバを指定する必要があります。
ステップ 5	`Router(cs-server)# issuer-name DN-string`	CA 発行者名を指定した DN ストリングに設定します。 • *DN-string* — デフォルト値は次のとおりです。**issuer-name CN=***cs-label*
ステップ 6	`Router(cs-server)# grant auto trustpoint label`	証明書サーバで、特定の非 Cisco IOS CA トラストポイントにすでに登録しているクライアントからの要求のみ、自動的に許可するようにします。 • *label* — 他社製 CA トラストポイントの名前 （注）　*label* 引数は、クライアント ルータの登録プロファイルに（**enrollment credential** コマンドを使用して）指定されているトラストポイントと同じである必要があります。
ステップ 7	`Router(cs-server)# lifetime {ca-certificate | certificate} time`	（任意）CA 証明書または証明書のライフタイム（日数）を指定します。 • *time* — 有効な値の範囲は 1 ～ 1,825 日です。CA 証明書のデフォルトのライフタイムは 3 年、証明書のデフォルトのライフタイムは 1 年です。証明書の最大のライフタイムは、CA 証明書のライフタイムより 1 カ月短い日数です。
ステップ 8	`Router(cs-server)# lifetime crl time`	（任意）証明書サーバが使用する CRL のライフタイム（時間数）を指定します。 • *time* — 最大のライフタイム値は 336 時間（2 週間）です。デフォルト値は 168 時間（1 週間）です。
ステップ 9	`Router(cs-server)# cdp-url url`	（任意）証明書サーバが発行した証明書で使用される CDP を指定します。 • *url* — HTTP URL を使用する必要があります。
ステップ 10	`Router(cs-server)# shutdown`	コンフィギュレーションを削除せずに証明書サーバをディセーブルにします。 このコマンドは、証明書サーバの設定が完了したあとで入力します。

	コマンド	説明
ステップ 11	`Router(cs-server)# exit`	証明書サーバ コンフィギュレーション モードを終了します。
ステップ 12	`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 13	`Router# show crypto pki server`	（任意）証明書サーバの現在の状態および設定を表示します。

「既存の証明書による再登録」機能を含めて、HTTP による CA サーバへの直接登録に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122limit/122z/122zh13/gthttpca.htm

HTTP による CA サーバへの直接登録に関する詳しい設定情報は、「HTTP による CA サーバへの直接登録の設定例」（p.27-56）を参照してください。

手動での証明書登録（TFTP およびカットアンドペースト）の設定

手動での証明書登録（TFTP およびカットアンドペースト）機能により、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。これらの作業は、TFTP サーバを利用するか、または手動でのカットアンドペースト操作によって行います。次のような場合に、TFTP の利用またはカットアンドペーストによる登録を行うことができます。

- CA が Simple Certificate Enrollment Protocol（SCEP）をサポートしていない場合（SCEP は、要求の送信および証明書の受信方式として最もよく使用されています）。
- ルータと CA の間のネットワーク接続が不可能な場合（Cisco IOS ソフトウェアで稼働しているルータが証明書を取得するには、ネットワーク接続が必要です）。

手動での証明書登録（TFTP およびカットアンドペースト）の設定時の注意事項および制約事項

手動での証明書登録（TFTP およびカットアンドペースト）を設定する場合は、次の注意事項および制約事項に従ってください。

- TFTP とカットアンドペーストは切り替えることができます。たとえば、**enrollment terminal** コマンドを使用して CA 証明書をペーストし、次に **no enrollment terminal** および **enrollment url tftp://certserver/file_specification** を入力して TFTP に切り替え、要求の送信およびルータ証明書の受信ができます。ただし、SCEP を使用する場合は、URL の切り替えは推奨できません。つまり、登録 URL が「http://」である場合、CA 証明書を受け取るときと、その証明書を登録するときで、登録 URL を変更しないでください。

TFTP による手動登録の設定

TFTP による手動登録を設定するには、次の前提条件を満たしている必要があります。

- TFTP による証明書登録を設定する場合、使用すべき正しい URL を知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み可能でなければなりません。
- 一部の TFTP サーバでは、書き込み先のファイルがサーバに存在している必要があります。
- 大部分の TFTP サーバでは、誰でもファイルに書き込み可能であることが要求されます。このため、すべてのルータまたは別のデバイスによって、証明書要求の書き込みまたは上書きが実行される危険性があります。要求が変更されているため、ルータは、一度 CA から発行された証明書を再使用できません。

ルータが使用するトラストポイント CA を宣言し、そのトラストポイント CA に TFTP での手動登録を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA の名前
ステップ 2	`Router(ca-trustpoint)# enrollment [mode] [retry period minutes] [retry count number] url url`	CA の登録パラメータを指定します。 • ***mode*** — CA システムが RA を提供する場合、RA モードを指定します。 • *minutes* — 証明書要求を再試行する間隔を指定します。デフォルトでは 1 分間隔で再試行されます。 • *number* — 要求への応答が得られない場合、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 の範囲で指定）。 • *url* — ルータが証明書要求を送信する CA の URL を指定します。 登録に SCEP 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。 登録に 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。
ステップ 3	`Router(ca-trustpoint)# crypto pki authenticate name`	（CA の証明書を取得することにより）CA を認証します。 • *name* — CA の名前。ステップ 1 で入力した *name* 値を入力します。
ステップ 4	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 5	`Router(config)# crypto pki enroll name`	CA からルータの証明書を取得します。 • *name* — CA の名前。ステップ 1 で入力した *name* 値を入力します。
ステップ 6	`Router(config)# crypto pki import name certificate`	TFTP を使用して証明書をインポートします。 • *name* — CA の名前。ステップ 1 で入力した *name* 値を入力します。

カットアンドペーストによる証明書登録の設定

ルータが使用するトラストポイント CA を宣言し、そのトラストポイント CA にカットアンドペーストでの手動登録を設定するには、次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA の名前
ステップ 2	`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を指定します。
ステップ 3	`Router(ca-trustpoint)# crypto pki authenticate name`	（CA の証明書を取得することにより）CA を認証します。 • *name* — CA の名前を指定します。ステップ 1 で入力した *name* 値を入力します。
ステップ 4	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 5	`Router(config)# crypto pki enroll name`	CA からルータの証明書を取得します。 • *name* — CA の名前を指定します。ステップ 1 で入力した *name* 値を入力します。
ステップ 6	`Router(config)# crypto pki import name certificate`	端末で証明書を手動でインポートします。 • *name* — CA の名前を指定します。ステップ 1 で入力した *name* 値を入力します。 **（注）** 用途別キー（シグニチャおよび暗号化キー）を使用する場合は、**crypto pki import** コマンドを 2 回入力する必要があります。このコマンドの 1 回めの実行時に一方の証明書がルータにペーストされ、2 回めの実行時にはもう一方の証明書がルータにペーストされます（どちらの証明書を先にペーストしてもかまいません）。

手動での証明書登録の設定の確認

証明書、CA の証明書、および RA 証明書に関する情報を確認するには、**show crypto pki certificates** コマンドを入力します。

```
Router# show crypto pki certificates

Certificate
  Status:Available
  Certificate Serial Number:14DECE05000000000C48
  Certificate Usage:Encryption

  Issuer:
    CN = msca-root
    O = Cisco Systems
    C = U

  Subject:
    Name:Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com

     CRL Distribution Point:
    http://msca-root/CertEnroll/msca-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:MS

   Certificate
    Status:Available
    Certificate Serial Number:14DEC2E9000000000C47
    Certificate Usage:Signature

     Issuer:
    CN = msca-root
    O = Cisco Systems
    C = US

     Subject:
    Name:Router.cisco.com
    OID.1.2.840.113549.1.9.2 = Router.cisco.com

     CRL Distribution Point:
       http://msca-root/CertEnroll/msca-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:MS

   CA Certificate
    Status:Available
    Certificate Serial Number:3AC0A65E9547C2874AAF2468A942D5EE
    Certificate Usage:Signature

     Issuer:
    CN = msca-root
    O = Cisco Systems
    C = US

     Subject:
    CN = msca-root
    O = Cisco Systems
    C = US
```

```
    CRL Distribution Point:
      http://msca-root/CertEnroll/msca-root.crl

  Validity Date:
    start date:16:46:01 PST Feb 13 2002
    end   date:16:54:48 PST Feb 13 2007

  Associated Trustpoints:MS
```

ルータに設定されているトラストポイントを表示するには、**show crypto pki trustpoints** コマンドを入力します。

```
Router# show crypto pki trustpoints

Trustpoint bo:

    Subject Name:

    CN = bomborra Certificate Manager

     O = cisco.com

     C = US

          Serial Number:01

    Certificate configured.

    CEP URL:http://bomborra

    CRL query url:ldap://bomborra
```

手動での証明書登録（TFTP およびカットアンドペースト）に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t13/ftmancrt.htm

手動での証明書登録の設定例は、「手動での証明書登録の設定例」（p.27-58）を参照してください。

証明書の自動登録の設定

証明書の自動登録機能により、パラメータを使用して設定されている CA には、ルータが証明書を自動的に要求するように設定できます。したがって、CA サーバに登録要求を送信する時点で、演算子による条件設定は必要ありません。

設定済みで、有効な証明書のないトラストポイント CA への自動登録は、起動時に実行されます。証明書（自動登録が設定されたトラストポイント CA が発行した証明書）が期限切れになると、新しい証明書が要求されます。この機能では証明書がシームレスに更新されるわけではありませんが、期限切れの場合にユーザの介入なしで証明書を回復できます。

証明書の自動登録機能が導入される前は、証明書の登録を行うには複雑な対話型コマンドをルータごとに実行する必要がありました。この機能を使用すると、必要なすべての情報をコンフィギュレーションにロードしておき、各ルータの起動時に自動的に証明書を取得させることができます。自動登録では、ルータ証明書の期限切れもチェックされます。

（注） 自動登録要求を送信する前に、必要な登録情報をすべて設定しておく必要があります。

起動時の CA への自動登録を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA の名前を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA の名前
ステップ 2	`Router(ca-trustpoint)# enrollment url url`	ルータが証明書要求を送信する CA の URL（たとえば、http://ca_server）を指定します。 • *url* — 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 または IP アドレスです。
ステップ 3	`Router(ca-trustpoint)# subject-name [x.500-name]`	（任意）証明書要求に使用する件名を指定します。 • *x.500-name* — *x.500-name* 引数を指定しない場合、デフォルトの件名である FQDN が使用されます。
ステップ 4	`Router(ca-trustpoint)# ip-address {interface | none}`	指定し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。 • *interface* — インターフェイスの IP アドレス • ***none*** — IP アドレスを追加しない場合は、このキーワードを指定します。 このコマンドをイネーブルにすると、このトラストポイントへの登録時に IP アドレスを要求するプロンプトは表示されません。
ステップ 5	`Router(ca-trustpoint)# serial-number [none]`	***none*** キーワードを指定した場合を除き、証明書要求でルータ シリアル番号を指定します。 • ***none*** — シリアル番号を含めない場合は、このキーワードを指定します。

	コマンド	説明
ステップ 6	`Router(ca-trustpoint)# auto-enroll [regenerate]`	自動登録をイネーブルにします。このコマンドにより、CA に自動的にルータ証明書を要求できます。デフォルトでは、証明書にはルータの DNS 名だけが含まれます。 • ***regenerate*** — 名前付きのキーがすでに存在する場合に証明書の新しいキーを生成するには、このキーワードを指定します。
ステップ 7	`Router(ca-trustpoint)# password string`	（任意）証明書の失効パスワードを指定します。 • *string* — パスワードのテキスト **（注）** このコマンドをイネーブルにすると、このトラストポイントへの登録時にパスワードを要求するプロンプトは表示されません。
ステップ 8	`Router(ca-trustpoint)# rsakeypair key-label [key-size [encryption-key-size]]`	証明書と対応付けるキー ペアを指定します。 • *key-label* — キー ペアの名前がまだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合、登録時に生成されるキー ペアの名前 • *key-size* — （任意）希望する RSA キーのサイズ。指定しない場合、既存のキー サイズが使用されます（指定するサイズは、*encryption-key-size* と同じである必要があります）。 • *encryption-key-size* — （任意）個別の暗号化、シグニチャ キー、および証明書を要求する場合に使用する、2 番めのキーのサイズ（指定するサイズは、*key-size* と同じである必要があります） このコマンドをイネーブルにしない場合、FQDN キー ペアが使用されます。

ルート CA のプリロード

自動登録をイネーブルにしたあと、CA を認証して信頼のチェーンを確立する必要があります。これは次のいずれかの方法で実行できます。

- CA の証明書の取得（p.27-30）
- CA の証明書の追加（p.27-31）

CA の証明書の取得

CA の証明書を取得するには、グローバル コンフィギュレーション モードで **crypto pki authenticate** コマンドを入力します。

```
Router(config)# crypto pki authenticate name
```

name — CA の名前を指定します。

CA の証明書の追加

CA の証明書を追加するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	Router (config)# **crypto pki certificate chain** *name*	証明書チェーン コンフィギュレーション モードを開始します。このモードでは、特定の証明書を追加または削除できます。 • *name* — CA の名前
ステップ 2	Router (config-cert-chain)# **certificate** *certificate-serial-number*	証明書を手動で追加または削除します。 • *certificate-serial-number* — 追加する CA のシリアル番号

CA 情報の確認

証明書、CA の証明書、および RA 証明書に関する情報を表示するには、**show crypto pki certificates** コマンドを入力します。

```
Router# show crypto pki certificates

Certificate

  Subject Name

    Name: myrouter.example.com
    IP Address: 10.0.0.1

  Status: Available

  Certificate Serial Number: 428125BDA34196003F6C78316CD8FA95

  Key Usage: Signature


Certificate

  Subject Name

    Name: myルータ.example.com
    IP Address: 10.0.0.1

  Status: Available

  Certificate Serial Number: AB352356AFCD0395E333CCFD7CD33897

  Key Usage: Encryption


CA Certificate

  Status: Available

  Certificate Serial Number: 3051DF7123BEE31B8341DFE4B3A338E5F

  Key Usage: Not Set
```

ルータに設定されているトラストポイントを表示するには、**show crypto pki trustpoints** コマンドを入力します。

```
Router# show crypto pki trustpoints

Trustpoint bo:

    Subject Name:

    CN = bomborra Certificate Manager

     O = cisco.com

     C = US

    Serial Number:01

    Certificate configured.

    CEP URL:http://bomborra

    CRL query url:ldap://bomborra
```

証明書の自動登録に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftautoen.htm

証明書の自動登録の設定例は、「証明書の自動登録の設定例」（p.27-61）を参照してください。

キーのロールオーバーによる証明書の更新の設定

証明書の自動登録は、ルータから CA サーバに、自動的に証明書の要求が行われるようにする機能です。デフォルトの自動登録機能では、古い証明書が期限切れになった時点で新しい証明書を要求します。新しいキーが生成された直後に既存の証明書およびキー ペアが削除されるので、この要求を処理している間、接続が切断されることがあります。処理が完了するまでは新しいキーには対応する証明書がないため、新しい証明書が発行されるまで、着信 IKE 接続を確立できません。キーのロールオーバーによる証明書の更新機能により、証明書が期限切れにならないうち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の間、古いキーおよび証明書を継続使用できます。

キーのロールオーバーは、手動での証明書登録要求とともに使用することもできます。キーのロールオーバーによる証明書の自動登録と同じ方法を使用して、一時的な名前で新しいキー ペアが作成され、CA から新しい証明書を受け取るまでの間、古い証明書およびキー ペアが保持されます。新しい証明書を受信した時点で、古い証明書およびキー ペアがドロップされ、新しいキー ペアの名前が、元のキー ペアの名前に変更されます。キーを手動で再生成しないでください。**crypto pki enroll** コマンドを入力した時点で、キーのロールオーバーが行われます。

キーのロールオーバーによる証明書の更新設定時の注意事項および制約事項

キーのロールオーバーによる証明書の更新を設定する場合は、次の注意事項および制約事項に従ってください。

- **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したトラストポイントは、他のトラストポイントとキー ペアを共有することはできません。各トラストポイントに独自のキー ペアを与えるには、ca-trustpoint 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。再生成を行うトラストポイント間でのキー ペアの共有はサポートされておらず、キーと証明書の不一致により、一部のトラストポイントでサービスの停止を引き起こす原因になります。

キーのロールオーバーによる証明書の自動登録の設定

キーのロールオーバーによる証明書の自動登録を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA の名前を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA の名前
ステップ 2	`Router(ca-trustpoint)# enrollment url url`	ルータが証明書要求を送信する CA の URL（たとえば、http://ca_server）を指定します。 • *url* — 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 または IP アドレスです。
ステップ 3	`Router(ca-trustpoint)# subject-name [x.500-name]`	（任意）証明書要求に使用する件名を指定します。 • *x.500-name* — *x.500-name* 引数を指定しない場合、デフォルトの件名である FQDN が使用されます。

	コマンド	説明
ステップ 4	`Router(ca-trustpoint)# ip-address {interface | none}`	指定し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。 • *interface* — インターフェイスの IP アドレス • ***none*** — IP アドレスを追加しない場合は、このキーワードを指定します。 このコマンドをイネーブルにすると、このトラストポイントへの登録時に IP アドレスを要求するプロンプトは表示されません。
ステップ 5	`Router(ca-trustpoint)# serial-number [none]`	***none*** キーワードを指定した場合を除き、証明書要求でルータ シリアル番号を指定します。 • ***none*** — シリアル番号を含めない場合は、このキーワードを指定します。
ステップ 6	`Router(ca-trustpoint)# auto-enroll [percent] [regenerate]`	自動登録をイネーブルにします。このコマンドにより、CA に自動的にルータ証明書を要求できます。デフォルトでは、証明書にはルータの DNS 名だけが含まれます。 • *percent* — 現在の証明書のライフタイムが一定のパーセンテージに達したときに新しい証明書を要求するには、*percent* 引数を指定します。 • ***regenerate*** — 名前付きのキーがすでに存在する場合に証明書の新しいキーを生成するには、このキーワードを指定します。 **（注）** ロールオーバーされるキー ペアがエクスポート可能であれば、新しいキー ペアもエクスポート可能になります。キー ペアがエクスポート可能である場合、トラストポイントのコンフィギュレーションに次のコメントが書き込まれています。 `!RSA key pair associated with trustpoint is exportable.`
ステップ 7	`Router(ca-trustpoint)# password string`	（任意）証明書の失効パスワードを指定します。 • *string* — パスワードのテキスト **（注）** このコマンドをイネーブルにすると、このトラストポイントへの登録時にパスワードを要求するプロンプトは表示されません。

	コマンド	説明
ステップ 8	`Router(ca-trustpoint)# rsakeypair key-label [key-size [encryption-key-size]]`	証明書と対応付けるキー ペアを指定します。 • *key-label* — キー ペアの名前がまだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合、登録時に生成されるキー ペアの名前 • *key-size* —（任意）希望する RSA キーのサイズ。指定しない場合、既存のキー サイズが使用されます（指定するサイズは、*encryption-key-size* と同じである必要があります）。 • *encryption-key-size* —（任意）個別の暗号化、シグニチャ キー、および証明書を要求する場合に使用する、2 番めのキーのサイズ（指定するサイズは、*key-size* と同じである必要があります） （注）　このコマンドをイネーブルにしない場合、FQDN キー ペアが使用されます。
ステップ 9	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 10	`Router(config)# crypto pki authenticate name`	（CA の証明書を取得することにより）CA を認証します。 • *name* — CA の名前。ステップ 1 で入力した *name* 値を入力します。 プロンプトが表示された場合、証明書のフィンガープリントをチェックします。 （注）　CA　　証明書がすでにコンフィギュレーションにロードされている場合、このコマンドは省略可能です。
ステップ 11	`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、特権 EXEC モードに戻ります。
ステップ 12	`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 のスタートアップ コンフィギュレーションにコピーします。

キーのロールオーバーによる証明書の手動登録の設定

（注）　**crypto key generate** コマンドを使用して手動でキーを再生成しないでください。キーのロールオーバーは、**crypto pki enroll** コマンドを入力した時点で行われます。

キーのロールオーバーによる証明書の手動登録を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA の名前を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • name — CA の名前
ステップ 2	`Router(ca-trustpoint)# enrollment url url`	ルータが証明書要求を送信する CA の URL（たとえば、http://ca_server）を指定します。 • *url* — 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 または IP アドレスです。
ステップ 3	`Router(ca-trustpoint)# subject-name [x.500-name]`	（任意）証明書要求に使用する件名を指定します。 • *x.500-name* — *x.500-name* 引数を指定しない場合、デフォルトの件名である FQDN が使用されます。
ステップ 4	`Router(ca-trustpoint)# ip-address {interface | none}`	指定し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。 • *interface* — インターフェイスの IP アドレス • ***none*** — IP アドレスを追加しない場合は、このキーワードを指定します。 このコマンドをイネーブルにすると、このトラストポイントへの登録時に IP アドレスを要求するプロンプトは表示されません。
ステップ 5	`Router(ca-trustpoint)# serial-number [none]`	***none*** キーワードを指定した場合を除き、証明書要求でルータ シリアル番号を指定します。 • ***none*** — シリアル番号を含めない場合は、このキーワードを指定します。
ステップ 6	`Router(ca-trustpoint)# regenerate`	**crypto pki enroll** コマンドを入力した時点で、キーのロールオーバーによる証明書の登録をイネーブルにします。 **（注）** このコマンドは、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再生成します。 **crypto key generate** コマンドを、キーのロールオーバー機能と一緒に使用しないでください。 ロールオーバーされるキー ペアがエクスポート可能であれば、新しいキー ペアもエクスポート可能になります。キー ペアがエクスポート可能である場合、トラストポイントのコンフィギュレーションに次のコメントが書き込まれています。 `!RSA key pair associated with trustpoint is exportable.`
ステップ 7	`Router(ca-trustpoint)# password string`	（任意）証明書の失効パスワードを指定します。 • *string* — パスワードのテキスト **（注）** このコマンドをイネーブルにすると、このトラストポイントへの登録時にパスワードを要求するプロンプトは表示されません。

	コマンド	説明
ステップ 8	`Router(ca-trustpoint)# rsakeypair key-label [key-size [encryption-key-size]]`	証明書と対応付けるキー ペアを指定します。 • *key-label* — キー ペアの名前がまだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合、登録時に生成されるキー ペアの名前 • *key-size* —（任意）希望する RSA キーのサイズ。指定しない場合、既存のキー サイズが使用されます（指定するサイズは、*encryption-key-size* と同じである必要があります）。 • *encryption-key-size* —（任意）個別の暗号化、シグニチャ キー、および証明書を要求する場合に使用する、2 番めのキーのサイズ（指定するサイズは、*key-size* と同じである必要があります） **（注）** このコマンドをイネーブルにしない場合、FQDN キー ペアが使用されます。
ステップ 9	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 モードを開始します。
ステップ 10	`Router(config)# crypto pki authenticate name`	（CA の証明書を取得することにより）CA を認証します。 • *name* — CA の名前。ステップ 1 で入力した *name* 値を入力します。 プロンプトが表示された場合、証明書のフィンガープリントをチェックします。 **（注）** CA　証明書がすでにコンフィギュレーションにロードされている場合、このコマンドは省略可能です。
ステップ 11	`Router(config)# crypto pki enroll name`	すべての RSA キー ペアに証明書を要求します。 • *name* — CA の名前。このコマンドでは、ルータは存在する RSA キー ペアと同数の証明書を要求するので、特定目的の RSA キー ペアがある場合にも、このコマンドは 1 回しか実行する必要はありません。**regenerate** コンフィギュレーション コマンドが設定されている場合、このコマンドによってキーのロールオーバーが実行されます。 **（注）** このコマンドでは、コンフィギュレーションに保存されないチャレンジ パスワードを作成する必要があります。証明書を失効させる必要が生じた場合、このパスワードが要求されるので、このパスワードを覚えておく必要があります。
ステップ 12	`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。

キーのロールオーバーによる証明書の更新に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtkyroll.htm

キーのロールオーバーの設定例は、「キーのロールオーバーによる証明書更新の設定例」（p.27-61）を参照してください。

PKI：証明書失効チェック時の複数サーバのクエリーの設定

ピアが提示した X.509 証明書を有効化する前に、CRL をチェックして、その証明書が発行元の CA で失効していないかどうかを確認します。証明書には通常、CDP が URL の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。

旧バージョンの Cisco IOS ソフトウェアでは、証明書に複数の CDP が含まれている場合にも、CRL 取得の試行は 1 回しか行われません。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：証明書失効チェック時の複数サーバのクエリー機能により、Cisco IOS ソフトウェアから証明書にあるすべての CDP を使用して、CRL の取得を複数回にわたって試行できます。その結果、特定のサーバが使用できない場合にも、処理が続行されます。さらに、証明書の CDP を、手動で設定した CDP で上書きする機能も提供されます。証明書の CDP の手動での上書きは、特定のサーバが長時間にわたって使用不可能な場合に役立ちます。証明書の CDP は URL またはディレクトリ指定で置き換えることができ、元の CDP を含むすべての証明書を再発行する必要がありません。

証明書の既存の CDP を、手動で URL またはディレクトリを指定して上書きするには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router (config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA トラストポイントの名前
ステップ 2	`Router(ca-trustpoint)# match certificate certificate-map-label override cdp {url | directory} string`	証明書の既存の CDP エントリを、URL またはディレクトリを指定して手動で上書きします。 • *certificate-map-label* — ユーザが指定するラベル。前に定義した **crypto pki certificate map** コマンドで指定したラベル引数と同じである必要があります。 • ***url*** — 証明書の CDP を HTTP または LDAP URL で上書きすることを指定します。 • ***directory*** — 証明書の CDP を LDAP ディレクトリを指定して上書きすることを指定します。 • *string* — URL またはディレクトリ指定 アプリケーションによっては、すべての CDP が試行される前にタイムアウトが発生し、エラー メッセージが生成されることがありますが、これによるルータへの影響はありません。Cisco IOS ソフトウェアはすべての CDP を試行するまで、CRL の取得を続行します。

PKI：証明書失効チェック時の複数サーバのクエリー機能に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_7/gtcertrc.htm

複数サーバのクエリーの設定例は、「ローカル証明書ストレージ場所の設定例」（p.27-56）を参照してください。

OCSP の設定

Online Certificate Status Protocol（OCSP）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。

OSCP 設定時の注意事項および制約事項

OSCP を設定する場合は、次の注意事項および制約事項に従ってください。

- OCSP は HTTP を使用してメッセージを転送するので、OCSP サーバにアクセスする際には遅延が発生する場合があります。OCSP サーバが使用できない場合は、証明書の確認は失敗します。
- NVRAM に証明書を保存する場合、証明書の容量が大きいと、ローエンドのルータで問題が発生することがあります。証明書に Authority Info Access（AIA）拡張部を追加するときは、容量の増加によって運用に問題が発生しないことを事前に確認してください。
- OCSP サーバは通常、プッシュまたはポール モードで動作します。CA サーバが OCSP サーバに失効情報をプッシュするように設定することも、OCSP サーバが CA サーバから定期的に CRL をダウンロード（ポール）するように設定することもできます。証明書の失効ステータスをタイムリーに取得できるようにするには、「プッシュ アンド ポール」間隔を慎重に考慮する必要があります。
- OCSP サーバから CA サーバに失効ステータスを返すように設定するときは、CA サーバが発行した OCSP 応答署名証明書を OCSP サーバに設定する必要があります。この署名証明書が正しいフォーマットではない場合、ルータは OCSP 応答を受理しません。詳細については、OCSP のマニュアルを参照してください。

ルータで OCSP を有効にして証明書ステータスをチェックするように設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA トラストポイントの名前
ステップ 2	`Router(ca-trustpoint)# ocsp url url`	（任意）OCSP サーバの URL を指定し、トラストポイントが証明書ステータスをチェックできるようにします。この URL は、証明書の AIA 拡張部に指定されている OCSP サーバの URL（存在する場合）を上書きします。 • *url* — 使用する HTTP URL を指定します。
ステップ 3	`Router(ca-trustpoint)# revocation-check method1 [method2[method3]]`	証明書の失効ステータスをチェックします。 • *method1* [*method2*[*method3*]] — ルータが証明書の失効ステータスをチェックするために使用する方法を指定します。使用できる方法は次のとおりです。 – ***crl*** — CRL によって証明書をチェックします。これがデフォルトのオプションです。 – ***none*** — 証明書のチェックを無視します。 – ***ocsp*** — OCSP サーバによって証明書をチェックします。 2 番めと 3 番めの方法を指定する場合、各方法はその直前の方法でエラーが返された場合（サーバがダウンしている場合など）にのみ使用されます。

OCSP の設定の確認

証明書および CA 証明書に関する情報を表示するには、**show crypto pki certificates** コマンドを入力します。

```
Router# show crypto pki certificates

Certificate

  Status: Available
  Version: 3
  Certificate Serial Number: 18C1EE03000000004CBD
  Certificate Usage: General Purpose

  Issuer:
    cn=msca-root
    ou=pki msca-root
    o=cisco
    l=santa cruz2
    st=CA
    c=US
    ea=user@example.com

  Subject:
    Name: myrouter.example.com
    hostname=myrouter.example.com

  CRL Distribution Points:
    http://msca-root/CertEnroll/msca-root.crl

  Validity Date:
    start date: 19:50:40 GMT Oct 5 2004
    end   date: 20:00:40 GMT Oct 12 2004

    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (360 bit)

    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: 2B5F53E6 E3E892E6 3A9D3706 01261F10
    Fingerprint SHA1: 315D127C 3AD34010 40CE7F3A 988BBDA5 CD528824

    X509v3 extensions:
    X509v3 Key Usage: A0000000
    Digital Signature
    Key Encipherment
    X509v3 Subject Key ID: D156E92F 46739CBA DFE66D2D 3559483E B41ECCF4
    X509v3 Authority Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
    Authority Info Access:

    Associated Trustpoints: msca-root
    Key Label: myrouter.example.com

   CA Certificate

    Status: Available
    Version: 3
    Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
    Certificate Usage: Signature

    Issuer:
    cn=msca-root
    ou=pki msca-root
    o=cisco
    l=santa cruz2
    st=CA
    c=US
    ea=user@example.com
```

```
    Subject:
    cn=msca-root
    ou=pki msca-root
    o=cisco
    l=santa cruz2
    st=CA
    c=US
    ea=user@example.com

    CRL Distribution Points:
    http://msca-root.example.com/CertEnroll/msca-root.crl

    Validity Date:
    start date: 22:19:29 GMT Oct 31 2002
    end   date: 22:27:27 GMT Oct 31 2017

    Subject Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (512 bit)

    Signature Algorithm: SHA1 with RSA Encryption
    Fingerprint MD5: 84E470A2 38176CB1 AA0476B9 C0B4F478
    Fingerprint SHA1: 0F57170C 654A5D7D 10973553 EFB0F94F 2FAF9837

    X509v3 extensions:
    X509v3 Key Usage: C6000000
    Digital Signature
    Non Repudiation
    Key Cert Sign
    CRL Signature

  X509v3 Subject Key ID: 37F3CC61 AF5E7C0B 434AB364 CF9FA0C1 B17C50D9
  X509v3 Basic Constraints:
    CA: TRUE

  Authority Info Access:
  Associated Trustpoints: msca-root
```

ルータに設定されているトラストポイントおよび設定済みのトラストポイント サブコマンドを表示するには、**show crypto pki trustpoints** コマンドを入力します。

```
Router# show crypto pki trustpoints

Trustpoint bo:
    Subject Name:
    CN = bomborra Certificate Manager
    O = cisco.com
    C = US
    Serial Number:01
    Certificate configured.
    CEP URL:http://bomborra
    CRL query url:ldap://bomborra
```

OCSP の詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_2/gt_ocsp.htm

OCSP の設定例は、「OCSP の設定例」（p.27-62）を参照してください。

オプションの OCSP ナンスの設定

オプションの OCSP ナンス機能を使用すると、OCSP 通信時に、OCSP 要求に関する Unique Identifier（UID; 固有識別情報）であるナンスの送信をディセーブルにできます。

（注）　オプションの OCSP Nonce 機能は、Cisco IOS Release 12.2(33)SRA でのみサポートされています。

失効方式として OCSP を使用している場合、OCSP サーバとのピア通信中に、デフォルトで UID（ナンス）が送信されます。OCSP サーバ通信中に UID を使用すると、通信がさらにセキュアになり、信頼度が高まります。ただし、UID を使用できない OCSP サーバもあります（詳細については、OCSP のマニュアルを参照してください）。OCSP 通信時の UID の使用をディセーブルにするには、**crypto pki trustpoint** コマンドで ***ocsp disable-nonce*** サブコマンドを使用します。

OCSP ナンスのディセーブル化

デフォルトでは、OCSP ナンスが使用されます。これらのナンスの使用をディセーブルにして、OCSP 通信時にルータが UID（ナンス）を送信しないように指定するには、グローバル コンフィギュレーション モードで次のように **crypto pki trustpoint** コマンド内から **ocsp disable-nonce** サブコマンドを使用します。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA の名前
ステップ 2	`Router (ca-trustpoint)# ocsp disable-nonce`	OCSP 通信中に、ルータが UID（ナンス）を送信しないように指定します。
ステップ 3	`Router(ca-trustpoint)# end`	（任意）ca-trustpoint コンフィギュレーション モードを終了します。

オプションの OCSP ナンスの詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a008051eaf8.html

オプションの OCSP ナンスの設定例は、「オプションの OCSP ナンスの設定例」（p.27-63）を参照してください。

証明書セキュリティ アトリビュートに基づくアクセス制御の設定

IPSec プロトコルでは CA とのインターオペラビリティが実現され、Cisco IOS デバイスと CA が通信を行うことで、Cisco IOS デバイスが CA からデジタル証明書を取得して使用できます。証明書には、デバイスまたはユーザが特定のアクションを実行する権限があるかどうかを決定する、いくつかのフィールドが含まれます。証明書セキュリティ アトリビュートに基づくアクセス制御機能は、証明書にフィールドを追加して、証明書ベースの ACL を作成します。

証明書セキュリティ アトリビュートに基づくアクセス制御設定時の注意事項および制約事項

証明書セキュリティ アトリビュートに基づくアクセス制御を設定する場合は、次の注意事項および制約事項に従ってください。

- 証明書ベースの ACL では、証明書の 1 つまたは複数のフィールドと、各フィールドで許可される値を指定します。証明書でチェックすべきフィールドと、それらのフィールドで認められる値または認められない値を指定できます。フィールドと値の比較には、6 つの論理テスト（等しい、等しくない、含む、含まない、未満、以上）を使用できます。
- 1 つの証明書ベース ACL で複数のフィールドを指定した場合、その ACL と一致するには、ACL 内のすべてのフィールド条件に合致しなければなりません。
- 同じ ACL 内で、同じフィールドを複数回にわたって指定できます。
- 複数の ACL を指定できます。一致するものが見つかるか、またはすべての ACL の処理が終わるまで、各 ACL の処理が続行されます。
- ACL の作成およびコンフィギュレーション ファイルからのロードには、相応のメモリが必要です。メモリ量は、証明書のどのフィールドをチェックするかと、定義済みの ACL の数に応じて変わります。証明書ベースの ACL をサポートするには、証明書のフィールドをチェックするために、1 回または複数回の比較処理を行う必要があります。ACL で指定されたフィールドだけがチェックされます。この比較処理は証明書の確認処理のごく一部分です。証明書の確認時のルータ パフォーマンスに目立った影響はありません。

証明書セキュリティに基づくアクセス制御を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki certificate map label sequence-number`	ca-certificate-map モードを開始し、ACL（アクセス コントロール リスト）にラベルを割り当てて証明書ベース ACL を定義します。このラベルは **crypto pki trustpoint** コマンドでも参照されます。 • *label* — ACL を特定する任意のストリング • *sequence-number* — 同じラベルの ACL を順序付けるシーケンス番号

	コマンド	説明
ステップ 2	`Router(ca-certificate-map)# field-name match-criteria match-value`	ca-certificate-map モードでは、1 つまたは複数の証明書フィールドと、その一致基準および照合する値を指定します。 • *field-name* — 次のいずれかの名前ストリング（大文字と小文字を区別しない）または日付を指定します。 — ***subject-name*** — ***issuer-name*** — ***unstructured-subject-name*** — ***alt-subject-name*** — ***name*** — ***valid-start*** — ***expires-on*** （注） 日付フィールドのフォーマットは、*dd mm yyyy hh:mm:ss* または *mmm dd yyyy hh:mm:ss* です。 • *match-criteria* — 次のいずれかの論理演算子を指定します。 — ***eq*** — 等しい（名前および日付フィールドで有効） — ***ne*** — 等しくない（名前および日付フィールドで有効） — ***co*** — 含む（名前フィールドでのみ有効） — ***nc*** — 含まない（名前フィールドでのみ有効） — ***lt*** — 未満（日付フィールドでのみ有効） — ***ge*** — 以上（日付フィールドでのみ有効） • *match-value* — *match-criteria* で指定した論理演算子を使用して比較する名前または日付を指定します。 次に例を示します。 Router(ca-certificate-map)# **subject-name co Cisco**
ステップ 3	`Router(ca-certificate-map)# exit`	ca-certificate-map モードを終了します。
ステップ 4	`Router(config)# crypto pki trustpoint name`	ca-trustpoint コンフィギュレーション モードを開始し、CA の名前を作成します。 • *name* — CA の名前を指定します。
ステップ 5	`Router(ca-trustpoint)# match certificate certificate-map-label`	**crypto pki certificate map** コマンドで定義した証明書ベース ACL を、トラストポイントと対応付けます。 • *certificate-map-label* — ステップ 1 で定義した **crypto pki certificate map** コマンドで指定したラベル引数を指定します。
ステップ 6	`Router(ca-trustpoint)# exit`	ca-trustpoint コンフィギュレーション モードを終了します。

証明書ベース ACL の確認

証明書ベース ACL の設定を確認するには、**show crypto pki certificates** コマンドを入力します。次に、ルータがトラストポイントを使用して認証および登録された場合に、ルータにインストールされる証明書のコンポーネント（CA およびルータ証明書）の例を示します。

```
Router# show crypto pki certificates

CA Certificate
   Status: Available
   Certificate Serial Number: 1244325DE0369880465F977A18F61CA8
   Certificate Usage: Signature

   Issuer:
    CN = new-user
    OU = pki new-user
    O = cisco
    L = santa cruz2
    ST = CA
    C = US
    EA = user@cysco.net

    Subject:
    CN = new-user
    OU = pki new-user
    O = cisco
    L = santa cruz2
    ST = CA
    C = US
    EA = user@cysco.net

    CRL Distribution Point:
    http://new-user.cysco.net/CertEnroll/new-user.crl

    Validity Date:
    start date: 14:19:29 PST Oct 31 2002
    end date: 14:27:27 PST Oct 31 2017

    Associated Trustpoints: MS


Certificate
  Status: Available
  Certificate Serial Number: 193E28D20000000009F7
  Certificate Usage: Signature

  Issuer:
     CN = new-user
     OU = pki new-user
     O = cisco
     L = santa cruz2
     ST = CA
    C = US
     EA = user@cysco.net

  Subject:
    Name: User1.Cysco.Net
    OID.1.2.840.113549.1.9.2 = User1.Cysco.Net

  CRL Distribution Point:
    http://new-user.cysco.net/CertEnroll/new-user.crl

  Validity Date:
    start date: 12:40:14 PST Feb 26 2003
    end   date: 12:50:14 PST Mar 5 2003
    renew date: 16:00:00 PST Dec 31 1969

  Associated Trustpoints: MS
```

証明書セキュリティ アトリビュートに基づくアクセス制御の設定についての詳細は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ftcrtacl.htm

証明書ベース ACL の例は、「証明書セキュリティ アトリビュートに基づくアクセス制御の設定例」（p.27-63）を参照してください。

件名全体を使用する PKI AAA 許可の設定

PKI および AAA 機能を使用する場合、AV ペアがユーザごとに異なる場合があります。そのため、各ユーザには一意のユーザ名が必要になります。件名全体を使用する PKI AAA 許可機能により、ユーザは証明書の件名全体を一意の AAA ユーザ名として使用し、AAA サーバを照会できます。

件名全体を使用する PKI AAA 許可設定時の注意事項および制約事項

件名全体を使用する PKI AAA 許可を設定する場合は、次の注意事項および制約事項に従ってください。

- AAA サーバによっては、ユーザ名の長さに制限があります（たとえば 64 文字）。その場合、証明書の件名の全体の長さは、サーバの制限値を超えることはできません。
- AAA　サーバによっては、ユーザ名に使用できる文字の種類に制限があります（たとえば、スペース [ ] や等号 [=] は使用できません）。このような文字セットに関する制限のある AAA サーバには、この機能は使用できません。
- トラストポイント設定の **subject-name** コマンドは、常に最終的な AAA 件名になるとは限りません。証明書要求にルータの FQDN、シリアル番号、または IP アドレスが含まれる場合、発行された証明書の件名フィールドにも、これらのコンポーネントが含まれます。これらのコンポーネントを無効にするには、***none*** キーワードを指定した **fqdn**、**serial-number**、および **ip-address** コマンドを使用します。
- CA サーバが証明書を発行する際に、要求された件名が変更されることがあります。たとえば、あるベンダー製の CA サーバでは、要求された件名の中の Relative Distinguished Name（RDN）を CN、OU、O、L、ST、C という順序に並べます。一方、要求された件名の末尾に、設定されている LDAP ディレクトリ ルート（たとえば、O=cisco.com）を追加する CA サーバもあります。
- 証明書を表示するために選択したツールによって、件名の中の RDN の表示順序が異なる場合があります。Cisco IOS ソフトウェアは常に最下位 RDN を最初に表示しますが、Open Source Secure Socket Layer（OpenSSL）など、他のソフトウェアではその反対です。したがって、完全な DN（件名）に対応するユーザ名を使用して AAA サーバを設定する場合は、Cisco IOS ソフトウェアのスタイル（すなわち、最下位 RDN が最初）に従うようにしてください。

証明書の件名全体による PKI 認証を設定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# aaa new-model`	AAA アクセス制御モデルをイネーブルにします。
ステップ 2	`Router config)# aaa authorization network listname [method]`	ネットワークへのユーザ アクセスを制限するためのパラメータを設定します。 • *listname* — 認証方式のリスト名として使用するストリング • *method* —（任意）許可に使用する許可方式を指定します。*method* 引数としては、***group radius***、***group tacacs+***、または ***group*** *group-name* を指定できます。
ステップ 3	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA の名前
ステップ 4	`Router(ca-trustpoint)# enrollment url url`	CA の登録パラメータを指定します。 • *url* — *url* 引数は、ルータが証明書要求を送信する CA の URL です。
ステップ 5	`Router(ca-trustpoint)# revocation-check method`	（任意）証明書の失効ステータスをチェックします。 • *method* — ルータが失効ステータスをチェックする方式。使用できる方式は、**ocsp**、**none**、および **crl** です。
ステップ 6	`Router(ca-trustpoint)# exit`	ca-trustpoint 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 モードを開始します。
ステップ 7	`Router config)# authorization list {listname}`	AAA 許可リストを指定します。 • *listname* — リストの名前
ステップ 8	`Router(config)# authorization username subjectname all`	AAA ユーザ名の作成に使用する証明書の各フィールドのパラメータを設定します。 **all** パラメータは、証明書の件名全体を許可ユーザ名として使用することを指定します。
ステップ 9	`Router(config)# tacacs-server host hostname [key string]` または	TACACS+ ホストを指定します。 • *name* — ホストの名前 • *string* —（任意）認証および暗号キーを指定するストリング
	`Router (config)# radius-server host hostname [key string]`	RADIUS ホストを指定します。

件名全体を使用する PKI AAA 許可機能に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123newft/123t/123t_11/gt_dnall.htm

件名全体を使用する PKI AAA 許可の設定例は、「ローカル証明書ストレージ場所の設定例」（p.27-56）を参照してください。

CA での発信トラフィックの送信元インターフェイス選択の設定

CA での発信トラフィックの送信元インターフェイス選択機能により、指定トラストポイントが設定されている場合に、トラストポイントに対応付けられたすべての発信 TCP 接続の送信元アドレスとして、特定のインターフェイスのアドレスを使用するように指定できます。

トラストポイントに対応付けられたすべての発信 TCP 接続の送信元アドレスとして使用するインターフェイスを設定するには、グローバル コンフィギュレーション モードで次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA トラストポイントの名前
ステップ 2	`Router(ca-trustpoint)# enrollment url url`	CA の登録パラメータを指定します。 • *url* — ルータが証明書要求を送信する CA の URL（たとえば http://ca_server）を指定します。*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 または IP アドレスです。
ステップ 3	`Router(ca-trustpoint)# source interface interface-address`	このトラストポイントに対応付けられた、すべての発信 TCP 接続の送信元アドレスとして使用するインターフェイスを指定します。 • *interface-address* — インターフェイス アドレス
ステップ 4	`Router(config)# interface type slot/[subslot]/port`	インターフェイス タイプを設定し、インターフェイス コンフィギュレーション モードを開始します。 • *type* — 設定するインターフェイスのタイプ • *slot*/[subslot]/ *port* — 設定するスロット、サブスロット（省略可能）、およびポートの番号
ステップ 5	`Router(config-if)# description string`	インターフェイス設定に説明を追加します。 • *string* — 説明文字列
ステップ 6	`Router(config-if)# ip address ip-address mask`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレス • *mask* — サブネット マスク
ステップ 7	`Router(config-if)# interface type slot/[subslot]/port`	インターフェイス タイプを設定します。 • *type* — 設定するインターフェイスのタイプ • *slot*/[subslot]/ *port* — 設定するスロット、サブスロット（省略可能）、およびポートの番号
ステップ 8	`Router(config-if)# description string`	インターフェイス設定に説明を追加します。 • *string* — 説明文字列

	コマンド	説明
ステップ 9	`Router(config-if)# ip address ip-address mask [secondary]`	インターフェイスのプライマリまたはセカンダリ IP アドレスを設定します。 • *address* — IP アドレス • *mask* — サブネット マスク • [*secondary*] — セカンダリ アドレス
ステップ 10	`Router(config-if)# crypto map map-name`	事前に定義した暗号マップ セットをインターフェイスに適用します。 • *map-name* — 暗号マップ セットの識別名

CA での発信トラフィックの送信元インターフェイス選択に関する詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t15/ft_asish.htm

送信元インターフェイス選択の設定例は、「CA での発信トラフィックの送信元インターフェイス選択の設定」（p.27-63）を参照してください。

永続的自己署名証明書の設定

永続的自己署名証明書機能は、セキュアな HTTP（HTTPS）サーバによって生成された証明書を保存して、ルータのスタートアップ コンフィギュレーションで SSL ハンドシェイクを実行できるようにします。

（注）　永続的自己署名証明書機能は、Cisco IOS Release 12.2(33)SXH 以降でのみサポートされています。

Cisco IOS ソフトウェアには、セキュアな SSL 接続を使用して Web ベース管理ページへのアクセスを可能にする HTTPS サーバが組み込まれています。SSL を使用してサーバとクライアント間にセキュアな接続を確立には、SSL ハンドシェイク時にクライアント（Web ブラウザ）に送信される X.509 証明書をサーバ上に保持しておく必要があります。

クライアントは自身がすでに所有している証明書を使用して、SSL サーバの証明書を検証できると想定します。

Cisco IOS ソフトウェアが HTTPS 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 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、検証できない場合は、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、あるいはあとで使用するために保存するかをユーザに確認します。証明書を受け入れた場合は、SSL ハンドシェイクが継続されます。

これ以降に、同じクライアントとサーバ間で行われる 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。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、以前の証明書と異なるため、この証明書を受け入れるかどうかを再度確認されます。

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のは面倒であり、またこの確認中に、攻撃者に不正な証明書を使用する機会を与えることもあります。

永続的自己署名証明書機能は、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してこれらの制限をすべて解消し、次の利点をもたらします。

- ルータのスタートアップ コンフィギュレーション（NVRAM）に永続的自己署名証明書を保存すると、ルータから提供された証明書と保存済み証明書をブラウザで比較し、証明書が変更されている場合はユーザに警告できます。したがって、攻撃者が不正な証明書を使用する機会は削減されます。
- ルータのスタートアップ コンフィギュレーションに永続的自己署名証明書を保存すると、ルータをリロードするたびにユーザが介入して、証明書を受け入れる必要がなくなります。
- 証明書を受け入れるためのユーザ介入が不要になるため、セキュアな接続プロセスが高速化されます。

永続的自己署名証明書設定時の注意事項および制約事項

永続的自己署名証明書を設定する場合は、次の注意事項および制約事項に注意してください。

- SSL をサポートするイメージをロードする必要があります。
- 永続的自己署名証明書を設定できるのは、1 つのトラストポイントのみです。

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

（注） セキュア HTTP（HTTPS）サーバをイネーブルにした場合、デフォルト値を使用して自己署名証明書が自動生成されるため、このセクションの内容はオプションです。パラメータを指定するには、トラストポイントを作成して、設定する必要があります。デフォルト値を使用するには、既存の自己署名トラストポイントをすべて削除します。自己署名トラストポイントをすべて削除すると、HTTPS サーバをイネーブル化した直後に、デフォルト値を使用して永続的自己署名証明書が生成されます。

トラストポイントを設定して、自己署名証明書パラメータを指定するには、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# crypto pki trustpoint name`	ルータが使用する CA を宣言し、ca-trustpoint コンフィギュレーション モードを開始します。 • *name* — CA の名前
ステップ 2	`Router(ca-trustpoint)# enrollment selfsigned`	自己署名登録を指定します。
ステップ 3	`Router(ca-trustpoint)# subject-name [x.500-name]`	（任意）証明書要求に使用する件名を指定します。 • *x.500-name* — x.500-name 引数を指定しない場合、デフォルトの件名である FQDN が使用されます。
ステップ 4	`Router(ca-trustpoint)# rsakeypair key-label [key-size [encryption-key-size]]`	（任意）証明書と対応付けるキー ペアを指定します。 • *key-label* — キー ペアの名前がまだ存在しない場合、または **auto-enroll regenerate** コマンドが設定されている場合、登録時に生成されるキー ペアの名前 • *key-size* —（任意）希望する RSA キーのサイズ。指定しない場合、既存のキー サイズが使用されます（指定するサイズは、*encryption-key-size* と同じである必要があります）。 • *encryption-key-size* —（任意）個別の暗号化、シグニチャ キー、および証明書を要求する場合に使用する、2 番めのキーのサイズ（指定するサイズは、*key-size* と同じである必要があります） **（注）** このコマンドをイネーブルにしない場合、FQDN キー ペアが使用されます。
ステップ 5	`Router(ca-trustpoint)# crypto pki enroll trustpoint-name`	永続的自己署名証明書を生成するようにルータに指示します。 • *trustpoint-name* — CA の名前
ステップ 6	`Router(ca-trustpoint)# end`	（任意）ca-trustpoint コンフィギュレーション モードを終了します。

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、グローバル コンフィギュレーション モードから次の作業を行います。

	コマンド	説明
ステップ 1	`Router(config)# ip http secure-server`	セキュア HTTP Web サーバをイネーブルにします。 （注）　キー ペア（モジュール 1024）および証明書が生成されます。
ステップ 2	`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。

（注）　コンフィギュレーションを保存するには **write memory** コマンドを入力する必要があります。このコマンドでも自己署名証明書が保存され、HTTPS サーバがイネーブル モードになります。

永続的自己署名証明書の設定の確認

自己署名証明書およびトラストポイントが作成されたことを確認するには、**show crypto pki certificates**、**show crypto mypubkey rsa**、および **show crypto pki trustpoints** コマンドを使用します。

show crypto pki certificates コマンドは証明書、CA の証明書、および RA 証明書に関する情報を表示します。

```
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す。ルータの実際のシリアル番号に応じて変化します。

show crypto mypubkey rsa コマンドは、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 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 という名前の 2 番めのキー 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。

show crypto pki trustpoints コマンドは、ルータに設定されたトラストポイントを表示します。

```
Router# show crypto pki trustpoints

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

永続的自己署名証明書の詳しい設定情報は、次の URL を参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a008040adf0.html

永続的自己署名証明書の設定例は、「永続的自己署名証明書の設定例」（p.27-64）を参照してください。

証明書チェーン検証の設定

トラストポイントが正常に認証されたかどうか、証明書が要求されて許可されたかどうか、および証明書が現在有効かどうかを判別するには、**crypto pki cert validate** コマンドを使用します。

（注）　**crypto pki cert validate** コマンドは、Cisco IOS Release 12.2(33)SRA でのみサポートされます。

証明書チェーン検証設定時の注意事項および制約事項

証明書チェーン検証を設定する場合は、次の注意事項および制約事項に従ってください。

- **crypto pki cert validate** コマンドは、指定されたトラストポイントに対応するルータ独自の証明書を検証します。登録後にこのコマンドを使用して、トラストポイントが適切に認証されているか、トラストポイントに対応する証明書が要求されて許可されているか、および証明書が現在有効であるかを確認します。証明書がトラストポイント CA によって署名されていて、期限切れでない場合などは、この証明書は有効です。

ルータが Dead Peer Detection（DPD）メッセージをピアに送信できるようにするには、グローバル コンフィギュレーション モードで次のように **crypto pki cert validate** コマンドを使用します。

Router(config)# **crypto pki cert validate** *trustpoint*

このコマンドでは、*trustpoint* は検証するトラストポイントを指定します。

証明書チェーン検証に関する詳しい設定情報は、『*Cisco IOS Security Command Reference*』を参照してください。

証明書チェーン検証の設定例は、「証明書チェーン検証の設定例」（p.27-65）を参照してください。

設定例

ここでは、次の設定例を示します。

複数の RSA キー ペアの設定例

以下に、RSA キー ペア「exampleCAkeys」を指定するトラストポイントの設定例を示します。

```
Router(config)# crypto key generate rsa general-purpose exampleCAkeys
Router(config)# crypto pki trustpoint exampleCAkeys
Router(config)# enroll url http://exampleCAkeys/certsrv/mscep/mscep.dll
Router(config)# rsakeypair exampleCAkeys 1024 1024
```

保護された秘密鍵ストレージの設定例

ここでは、次の設定例を示します。

暗号化キーの設定例

以下に、RSA キー「pki1-72a.cisco.com」を暗号化する例を示します。

```
Router(config)# crypto key encrypt rsa name pki1-72a.cisco.com passphrase cisco1234
Router(config)# exit
```

ロックされたキーの設定例

以下に、RSA キー「pki1-72a.cisco.com」をロックする例を示します。

```
Router# crypto key lock rsa name pki1-72a.cisco.com passphrase cisco1234
```

トラストポイント CA の設定例

以下に、CA「kahului」を宣言し、このトラストポイント CA の特性を指定する例を示します。

```
Router(config)# crypto pki trustpoint kahului
Router(ca-trustpoint)# enrollment url http://kahului
Router(ca-trustpoint)# crl query ldap://kahului
```

トラストポイント単位でのクエリー モード定義の設定例

以下に、クエリー モードを使用するトラストポイント CA の設定例を示します。

```
Router(config)# crypto pki trustpoint trustpoint1
Router(ca-trustpoint)# enrollment url http://ca-server1
Router(ca-trustpoint)# crl query http://ca-server1
Router(ca-trustpoint)# default query certificate
Router(ca-trustpoint)# query certificate
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate trustpoint1
Router(config)# crypto key generate rsa
Router(config)# crypto pki enroll trustpoint1
```

ローカル証明書ストレージ場所の設定例

以下に、certs サブディレクトリに証明書を保存する例を示します。certs サブディレクトリは存在せず、自動的に作成されます。

```
Router(config)# crypto pki certificate storage disk0:/certs
Requested directory does not exist -- created
Certificates will be stored in disk0:/certs/
Router(config)# end
Router# write
*May 27 02:09:00:%SYS-5-CONFIG_I:Configured from console by consolemem
Building configuration...
[OK]
Router# directory disk0:/certs
Directory of disk0:/certs/
14  -rw-         707  May 27 2005 02:09:02 +00:00  ioscaroot#7401CA.cer
15  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#826E.cer
16  -rw-         759  May 27 2005 02:09:02 +00:00  msca-root#1BA8CA.cer
17  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#75B8.cer
18  -rw-        1149  May 27 2005 02:09:02 +00:00  storagename#6500CA.cer
19  -rw-         863  May 27 2005 02:09:02 +00:00  msca-root#83EE.cer
47894528 bytes total (20934656 bytes free)

! The certificate files are now on disk0/certs:
```

HTTP による CA サーバへの直接登録の設定例

ここでは、次の設定例を示します。

- クライアント ルータの登録プロファイルの設定例（p.27-57）
- サードパーティ製 CA に登録済みのクライアント ルータの登録プロファイルの例（p.27-57）
- クライアント ルータの登録要求のみを自動的に受け付ける証明書サーバの設定例（p.27-57）

クライアント ルータの登録プロファイルの設定例

以下に、HTTP による CA サーバへの直接的登録のための登録プロファイルを設定する例を示します。

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

サードパーティ製 CA に登録済みのクライアント ルータの登録プロファイルの例

この例では、クライアント ルータに次のタスクを設定します。

- サードパーティ製 CA を指定するトラストポイント「msca-root」を定義し、そのサードパーティ製 CA に対してクライアントを登録および認証します。
- Cisco IOS CA に対応するトラストポイント「cs」を定義します。
- 登録プロファイル「cs1」を定義します。このプロファイルは Cisco IOS CA を指定し、(enrollment credential コマンドによって)「msca-root」が Cisco IOS CA に最初に登録されるように設定します。

```
! Define trustpoint "msca-root" for non-Cisco IOS CA.
Router(config)# crypto pki trustpoint msca-root
Router(ca-trustpoint)# enrollment mode ra
Router(ca-trustpoint)# enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
Router(ca-trustpoint)# ip-address FastEthernet2/0
Router(ca-trustpoint)# revocation-check crl

! Configure trustpoint "cs" for Cisco IOS CA.
Router(config)# crypto pki trustpoint cs
Router(ca-trustpoint)# enrollment profile cs1
Router(ca-trustpoint)# revocation-check crl

! Define enrollment profile "cs1."
Router(config)# crypto pki profile enrollment cs1
Router(ca-profile-enroll)# enrollment url  http://cs:80
Router(ca-profile-enroll)# enrollment credential  msca-root
```

クライアント ルータの登録要求のみを自動的に受け付ける証明書サーバの設定例

この例では、証明書サーバがトラストポイント「msca-root」に登録済みのクライアントの登録要求のみを受け付けるように設定し、**grant auto trustpoint** コマンドを入力します。

```
Router(config)# crypto pki server cs
Router(cs-server)# database level minimum
Router(cs-server)# database url nvram:
Router(cs-server)# issuer-name CN=cs
Router(cs-server)# grant auto trustpoint msca-root

Router(config)# crypto pki trustpoint cs
Router(ca-trustpoint)# revocation-check crl
Router(ca-trustpoint)# rsakeypair cs

Router(ca-trustpoint)# crypto pki trustpoint msca-root
Router(ca-trustpoint)# enrollment mode ra
Router(ca-trustpoint)# enrollment url http://msca-root:80/certsrv/mscep/mscep.dll
Router(ca-trustpoint)# revocation-check crl
```

手動での証明書登録の設定例

ここでは、手動での証明書登録の設定例を示します。

- TFTP を使用する手動での証明書登録の設定例（p.27-58）
- カットアンドペーストを使用する手動での証明書登録の設定例（p.27-58）

TFTP を使用する手動での証明書登録の設定例

以下に、TFTP を使用する手動での証明書登録の設定例を示します。

```
Router(config)# crypto pki trustpoint MS
Router(ca-trustpoint)# enrollment url tftp://CA-Server/TFTPfiles/ルータ 1
Router(ca-trustpoint)# crypto pki authenticate MS
Router(ca-trustpoint)# exit
Router(config)# crypto pki enroll MS
Router(config)# crypto pki import MS certificate
```

カットアンドペーストを使用する手動での証明書登録の設定例

以下に、カットアンドペーストによる手動での証明書登録の設定例を示します。この例で、トラストポイント CA の名前は「MS」です。また、用途キー（シグニチャおよび暗号化キー）を使用しているため、**crypto pki import** コマンドを 2 回使用しています。

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


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)#
```

```
Router(config)# crypto pki enroll MS

% Start certificate enrollment..


% The subject name in the certificate will be:Router.cisco.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+

---End - This line not part of the certificate request---

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

---End - This line not part of the certificate request---


Redisplay enrollment request? [yes/no]:

n

Router(config)#crypto pki import MS 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)#

Router(config)# crypto pki import MS certificate


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
```

証明書の自動登録の設定例

以下に、ルータが起動時に CA に自動登録されるように設定する例を示します。

```
Router(config)# crypto pki trustpoint frog
Router(ca-trustpoint)# enrollment url http://frog.phoobin.com/
Router(ca-trustpoint)# subject-name OU=Spiral Dept., O=tiedye.com
Router(ca-trustpoint)# ip-address ethernet-0
Router(ca-trustpoint)# auto-enroll regenerate
Router(ca-trustpoint)# password revokeme
Router(ca-trustpoint)# rsa-key frog 2048
!
Router(config)# crypto pki certificate chain frog
Router(config-cert-chain)# certificate ca 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
```

キーのロールオーバーによる証明書更新の設定例

ここでは、次の例を示します。

- キーのロールオーバーによる証明書自動登録の設定例（p.27-61）
- キーのロールオーバーによる証明書手動登録の設定例（p.27-62）

キーのロールオーバーによる証明書自動登録の設定例

以下に、ルータが起動時に CA「trustme1」に自動登録されるように設定する例を示します。この例では、**regenerate** キーワードを指定しているため、証明書には新しいキーが生成されます。更新パーセンテージを 90 に設定しているので、証明書のライフタイムが 1 年とすると、古い証明書が期限切れになる 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 が更新されることがないため、実行コンフィギュレーションの変更を、NVRAM のスタートアップ コンフィギュレーションに保存します。

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

キーのロールオーバーによる証明書手動登録の設定例

以下に、CA 「trustme2」から手動で証明書登録を行い、キーのロールオーバーによってキーの再生成を行う設定例を示します。

```
Router(config)# crypto pki trustpoint trustme2
Router(ca-trustpoint)# enrollment url http://trustme2.company.com/
Router(ca-trustpoint)# subject-name OU=Spiral Dept., O=tiedye.com
Router(ca-trustpoint)# ip-address ethernet0
Router(ca-trustpoint)# serial-number none
Router(ca-trustpoint)# regenerate
Router(ca-trustpoint)# password revokeme
Router(ca-trustpoint)# rsakeypair trustme2 2048
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate trustme2
Router(config)# crypto pki enroll trustme2
Router(config)# exit
```

PKI：証明書失効チェック時の複数サーバのクエリー（CDP の上書き）の設定例

この例では、**crypto pki certificate map** コマンドで定義した証明書マップ Group1 について、**match certificate override cdp** コマンドを使用して CDP を上書きします。

```
Router(config)# crypto pki certificate map Group1 10
Router(ca-certificate-map)# subject-name co ou=WAN
Router(ca-certificate-map)# subject-name co o=Cisco
Router(config)# crypto pki trustpoint pki
Router(ca-trustpoint)# match certificate Group1 override cdp url
http://server.cisco.com
```

OCSP の設定例

ここでは、次の設定例を示します。

- OCSP サーバの設定例（p.27-62）
- CRL の次に OCSP サーバを使用する設定例（p.27-62）
- 特定の OCSP サーバの設定例（p.27-63）

OCSP サーバの設定例

以下に、証明書の AIA 拡張部で指定された OCSP サーバを使用するように、ルータを設定する例を示します。

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check ocsp
```

CRL の次に OCSP サーバを使用する設定例

以下に、ルータが CDP から CRL をダウンロードするように設定する例を示します。CRL が使用不可能な場合には、証明書の AIA 拡張部で指定された OCSP サーバを使用するように設定します。これらのオプションが両方とも失敗した場合には、証明書の検証も失敗します。

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# revocation-check crl ocsp
```

特定の OCSP サーバの設定例

以下に、HTTP URL「http://myocspserver:81」にある OCSP サーバを使用するようにルータを設定する例を示します。このサーバがダウンしている場合は、失効チェックは行われません。

```
Router(config)# crypto pki trustpoint mytp
Router(ca-trustpoint)# ocsp url http://myocspserver:81
Router(ca-trustpoint)# revocation-check ocsp none
```

オプションの OCSP ナンスの設定例

以下に、以前に作成されたトラストポイント ts との OCSP 通信に対して、UID をディセーブルにする例を示します。

```
Router(config)# crypto pki trustpoint ts
Router (ca-truspoint)# ocsp disable-nonce
Router(ca-trustpoint)# end
```

証明書セキュリティ アトリビュートに基づくアクセス制御の設定例

以下に、証明書ベース ACL の設定例を示します。

```
Router(config)# crypto pki certificate map Group 10
Router(ca-certificate-map)# subject-name co Cisco
Router(config-cert-map)# exit
Router(config)# crypto pki trustpoint Access
Router(ca-trustpoint)# match certificate Group
Router(ca-trustpoint)# exit
```

件名全体を使用する PKI AAA 許可の設定例

以下に、証明書の件名全体を PKI AAA 許可に使用する例を示します。

```
Router(config)# aaa new-model
Router(config)# aaa authorization network tac-o group tacacs+

Router(config)# crypto pki trustpoint test
Router(ca-trustpoint)# enrollment url http://caserver:80
Router(ca-trustpoint)# revocation-check crl
Router(ca-trustpoint)# exit
Router(config)# authorization list tac-o
Router(config)# authorization username subjectname all

Router(config)# tacacs-server host 20.2.2.2 key a_secret_ke
```

CA での発信トラフィックの送信元インターフェイス選択の設定

この例では、ルータがブランチ オフィスに配置されています。ルータは IPSec を使用して本社と通信します。Ethernet 1 は、ISP（インターネット サービス プロバイダー）に接続する「外部」インターフェイスです。Ethernet 0 は、ブランチ オフィスの LAN に接続するインターフェイスです。本社に配置された CA サーバにアクセスするには、ルータはインターフェイス Ethernet 1（アドレス 10.2.2.205）から IPSec トンネルを使用して IP データグラムを送信する必要があります。ISP によりアドレス 10.2.2.205 が割り当てられています。アドレス 10.2.2.205 は、ブランチ オフィスまたは本社の一部分ではありません。

ファイアウォールがあるため、CA は社外のアドレスにアクセスできません。CA は 10.2.2.205 から着信するメッセージを認識していますが、応答できません（つまり、CA は到達可能なアドレス 10.1.1.1 にあるブランチ オフィスに、ルータが配置されていることを認識していません）。

source interface コマンドを追加すると、CA に送信する IP データグラムの送信元アドレスとして、アドレス 10.1.1.1 を使用するようにルータに命令が出されます。CA は 10.1.1.1 に応答できます。

この例では、**source interface** コマンドおよび上記のインターフェイス アドレスを使用しています。

```
Router(config)# crypto pki trustpoint ms-ca
Router(ca-trustpoint)# enrollment url http://ms-ca:80/certsrv/mscep/mscep.dll
Router(ca-trustpoint)# source interface ethernet0

Router(config)# interface ethernet 0
Router(config-if)# description inside interface
Router(config-if)# ip address 10.1.1.1 255.255.255.0

Router(config)# interface ethernet 1
Router(config-if)# description outside interface
Router(config-if)# ip address 10.2.2.205 255.255.255.0
Router(config-if)# crypto map main-office
```

永続的自己署名証明書の設定例

以下に、永続的自己署名証明書を設定する例を示します。

- トラストポイントおよび自己署名証明書の設定例（p.27-64）
- HTTPS サーバのイネーブル化の設定例（p.27-65）

トラストポイントおよび自己署名証明書の設定例

以下に、トラストポイントおよび自己署名証明書を設定する例を示します。この例では、トラストポイント local が宣言され、登録が要求され、IP アドレスを含む自己署名証明書が生成されます。

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# crypto pki trustpoint local
Router(ca-trustpoint)# enrollment selfsigned
Router(ca-trustpoint)# end
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)# 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 つのみです。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確認されます。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設定例

この例では、HTTPS サーバがイネーブルにされ、まだ設定されていないデフォルト トラストポイントが生成されます。

```
Router(config)# 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

Router(config)#
```

（注）　自己署名証明書で使用されるキー ペアを作成すると、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 ACL 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。

証明書チェーン検証の設定例

以下に、**crypto pki cert validate** コマンドの有効な出力を示します。

```
Router(config)# crypto pki cert validate ka

Validation Failed: trustpoint not found for ka

Router(config)# crypto pki cert validate ka

Validation Failed: can't get local certificate chain

Router(config)# crypto pki cert validate ka

Certificate chain has 2 certificates.
Certificate chain for ka is valid

Router(config)# crypto pki cert validate ka

Certificate chain has 2 certificates.
Validation Error: no certs on chain

Router(config)# crypto pki cert validate ka

Certificate chain has 2 certificates.
Validation Error: unspecified error
```