crypto ca authenticate ～ crypto ca trustpoint

crypto ca aunticate

（注） Cisco IOS Release 12.3(7)T および 12.2(18)SXE から、このコマンドが **crypto pki authenticate** コマンドに置き換えられました。

（CA の証明書を取得することによって）認証局を認証するには、グローバル コンフィギュレーション モードで **crypto ca authenticate** コマンドを使用します。

crypto ca authenticate *name*

構文の説明

name	CA 名を指定します。 これは、**crypto ca identity** コマンドを使用して CA を宣言した際と同じ名前を指定します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3 T	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、ルータで最初に CA サポートを設定する場合に必要です。

このコマンドは、CA の公開キーを含む CA の自己署名証明書を取得することで、ルータに対して CA を認証します。 CA では、証明書が自己署名されるため、このコマンドを実行するときは、CA 管理者に問い合わせて、CA の公開キーを手作業で認証する必要があります。

RA モードを使用する場合（**enrollment mode ra** コマンドを使用する場合）は、**crypto ca authenticate** コマンドを発行すると、登録局の署名と暗号化証明書が CA と CA 証明書から返されます。

このコマンドはルータ コンフィギュレーションに保存されません。 ただし、受信した CA（および RA）証明書に埋め込まれている公開キーについては、RSA 公開キー レコード（「RSA 公開キー チェーン」と呼ばれます）の一部としてコンフィギュレーションに保存されます。

このコマンドを発行した後で CA がタイムアウト期間内に応答しない場合は、このコマンドが停滞しないように端末制御が返されます。 これが発生した場合、コマンドを再入力する必要があります。 Cisco IOS ソフトウェアは、西暦 2049 年より後に設定された CA 証明書の有効期限を認識しません。 CA 証明書の有効期限が西暦 2049 年より後に期限切れになるように設定すると、CA サーバの認証の試行時に次のエラー メッセージが表示されます。

error retrieving certificate :incomplete chain

これと同様のエラー メッセージを受け取った場合は CA 証明書の有効期限を確認してください。 CA 証明書の有効期限が西暦 2049 年より後に設定されている場合は、有効期限を西暦 2049 年より前に設定し直す必要があります。

例

次に、ルータが CA の証明書を要求する例を示します。 CA は証明書を送信し、ルータは、管理者に CA 証明書のフィンガープリントをチェックして CA 証明書を確認するように要求します。 CA 管理者は、CA 証明書のフィンガープリントを表示することもできるので、CA 管理者が実際に見ているものと、ルータの画面に表示されるものとを比較する必要があります。 ルータの画面のフィンガープリントと、CA 管理者が表示するフィンガープリントが一致した場合、証明書は有効です。

```
Router(config)#
crypto ca authenticate myca
Certificate has the following attributes:
Fingerprint: 0123 4567 89AB CDEF 0123
Do you accept this certificate? [yes/no] y
#
```

関連コマンド

コマンド	説明
debug crypto pki transactions	CA とルータ間の相互作用（メッセージ タイプ）のトレースのデバッグ メッセージを表示します。
show crypto pki certificates	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。

crypto ca enroll

（注） Cisco IOS Release 12.3(7)T および 12.2(18)SXE から、このコマンドが **crypto pki enroll** コマンドに置き換えられました。

認証局からルータ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 ca enroll** コマンドを使用します。 現在の登録要求を削除するには、このコマンドの **no** 形式を使用します。

crypto ca enroll *name*

no crypto ca enroll *name*

構文の説明

name	CA 名を指定します。 **crypto pki trustpoint** コマンドを使用して CA を宣言したときと同じ名前を使用します。

コマンド デフォルト

デフォルトの動作や値はありません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
11.3 T	このコマンドが導入されました。

使用上のガイドライン

このコマンドは、すべてのルータの RSA キー ペアに対して CA からの証明書を要求します。 このタスクは、CA を使用した登録とも呼ばれます。 （理論的には、証明書の登録と取得は 2 つの別々のイベントですが、このコマンドが発行される際はこれらの両方が発生します）。

ルータは、ルータ上の各 RSA キー ペアに対して CA からの署名付き証明書が必要です。以前に汎用キーを作成している場合、このコマンドにより、1 組の汎用 RSA キー ペアに対応する 1 つの証明書が取得されます。 特殊用途キーを以前に作成している場合、このコマンドにより、この特殊用途の RSA キー ペアそれぞれに対応する 2 つの証明書が取得されます。

キーに対する証明書をすでに持っている場合は、このコマンドを完了できません。代わりに、まず既存の証明書の削除を求めるプロンプトが表示されます（**no certificate** コマンドで既存の証明書を削除できます）。

crypto ca enroll コマンドは、ルータ コンフィギュレーションには保存されません。

（注） **crypto ca enroll** コマンドを発行した後、証明書を受信する前にルータがリブートした場合は、コマンドを再発行する必要があります。

プロンプトへの応答

crypto ca enroll コマンドを発行すると、次の作業を求められます。

まず、チャレンジ パスワードを作成するように求められます。 このパスワードの長さは最大 80 文字です。 このパスワードは、ルータの証明書を取り消す場合に必要です。 CA 管理者に証明書を無効にするよう依頼する場合は、不正なまたは誤った失効要求からの保護としてこのチャレンジ パスワードを入力する必要があります。

（注） このパスワードはどこにも保存されないため、覚えておく必要があります。

パスワードを忘れた場合は、CA 管理者によってルータの証明書を取り消すことができる場合がありますが、ルータの管理者 ID の手動による認証が必要になる場合もあります。

また、取得した証明書にルータのシリアル番号を含めるかどうかを指示するように求められます。シリアル番号は IP セキュリティまたはインターネット キー交換には使用されませんが、CA によって証明書の認証または後で特定のルータに証明書を関連付けるために使用される場合があります（保存されるシリアル番号は、本体ケースではなく内部ボードのシリアル番号であることに注意してください）。シリアル番号を含める必要があるかどうかを CA 管理者に問い合わせてください。 不明な場合は、シリアル番号を含めてください。

通常、IP アドレスは含めません。これは、IP アドレスが特定のエンティティに証明書をより厳密にバインドするためです。 また、ルータが移動すると、新しい証明書を発行する必要があります。 最後に、ルータには複数の IP アドレスがありますが、いずれも IPSec で使用されることはありません。

IP アドレスを含めることが必要であることを示す場合、IP アドレスのインターフェイスを指定するように求められます。 このインターフェイスは、クリプト マップ セットを適用するインターフェイスに対応している必要があります。 複数のインターフェイスにクリプト マップ セットを適用する場合は、**crypto map local-address** コマンドで指定するインターフェイスを指定します。

例

次に、汎用 RSA キー ペアを持つルータが CA からの証明書を要求する例を示します。 ルータが証明書フィンガープリントを表示する場合、管理者は、番号を検査する CA 管理者に問い合わせてこの番号を確認します。 フィンガープリントが正しければ、ルータ管理者は証明書を受け入れます。

ルータ管理者が要求を送信してから、証明書がルータによって実際に届くまで遅延が発生する場合があります。 遅延の量はCAの動作方法によって異なります。

```
Router(config)# crypto ca enroll myca
%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
   password to the CA Administrator in order to revoke your certificate.
   For security reasons your password will not be saved in the configuration.
   Please make a note of it.
Password: <mypassword>
Re-enter password: <mypassword>
% The subject name in the certificate will be: myrouter.example.com
% Include the router serial number in the subject name? [yes/no]: yes
% The serial number in the certificate will be: 03433678
% Include an IP address in the subject name [yes/no]? yes
Interface: ethernet0/0
Request certificate from CA [yes/no]? yes
% Certificate request sent to Certificate Authority
% The certificate request fingerprint will be displayed.
% The 'show crypto pki certificates' command will also show the fingerprint.
```

その後、ルータがCAから証明書を受け取ると、次の確認メッセージが表示されます。

```
Router(config)#   Fingerprint: 01234567 89ABCDEF FEDCBA98 75543210
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
Router(config)#
```

必要に応じて、ルータ管理者はCA管理者とともに表示されたフィンガープリントを確認できます。

証明書要求に問題があり、証明書が許可されない場合、代わりに次のメッセージがコンソールに表示されます:

```
%CRYPTO-6-CERTREJ: Certificate enrollment request was rejected by Certificate Authority
```

証明書のサブジェクト名は、RSAキー ペアの名前と同じになるように自動的に割り当てられます。 上記の例では、RSAキー ペアの名前が「myrouter.example.com.」（ルータが割り当てた名前）になっています。

特殊用途キーを持つルータの証明書を要求する場合は、上記の例と同じですが、CAによって2つの証明書が返されることもあります。 ルータが2つの証明書を受け取る場合は、同じ確認メッセージを表示します。

```
%CRYPTO-6-CERTRET: Certificate received from Certificate Authority
```

関連コマンド

コマンド	説明
debug crypto pki messages	CAとルータ間の相互作用（メッセージ ダンプ）の詳細のデバッグ メッセージを表示します。
debug crypto pki transactions	CAとルータ間の相互作用（メッセージ タイプ）のトレースのデバッグ メッセージを表示します。

コマンド	説明
show crypto pki certificates	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。

crypto ca trustpoint

（注） Cisco IOS Release 12.3(8)T、12.2(18)SXD、および 12.2(18)SXE から、**crypto ca trustpoint** コマンドが **crypto pki trustpoint** コマンドに置き換えられました。 詳細については、**crypto pki trustpoint** コマンドを参照してください。

ルータが使用する認証局（CA）を宣言するには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。 CA に関連するすべての ID 情報および証明書を削除するには、このコマンドの **no** 形式を使用します。

crypto ca trustpoint *name*

no crypto ca trustpoint *name*

構文の説明

name	CA の名前を作成します （以前に CA を宣言していて、その特性を更新する場合は、以前に作成した名前を指定します）。

コマンド デフォルト

このコマンドを使用して CA を宣言するまで、ルータは CA を認識しません。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.2(8)T	このコマンドが導入されました。
12.2(15)T	**match certificate** サブコマンドが導入されました。
12.3(7)T	このコマンドが **crypto pki trustpoint** コマンドに置き換えられました。 **crypto ca trusted-root** または **crypto ca trustpoint** コマンドも入力はできますが、コマンドはコンフィギュレーション内に「crypto pki trustpoint」として書き込まれます。

使用上のガイドライン

自己署名ルート CA または下位 CA となる CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。 **crypto ca trustpoint** コマンドを発行すると、ca-trustpoint コンフィギュレーション モードが開始されます。

次のサブコマンドを使用して、トラストポイント CA の特性を指定できます。

- **crl**：証明書失効リスト（CRL）をクエリーし、ピアの証明書が失効していないことを確認します。
- **default**（**ca-trustpoint**）：ca-trustpool コンフィギュレーション モードのサブコマンドの値をデフォルトにリセットします。
- **enrollment**：登録パラメータを指定します（任意）。
- **enrollment http-proxy**：HTTP を使用し、プロキシ サーバ経由で CA にアクセスします。
- **match certificate**：**crypto ca certificate map** コマンドで定義された証明書ベースのアクセス コントロール リスト（ACL）を関連付けます。
- **primary**：特定のトラストポイントをルータのプライマリ トラストポイントとして割り当てます。
- **root**：CA を取得するための簡易ファイル転送プロトコル（TFTP）を定義し、CA 証明書に保存されるサーバ名とファイル名の両方を指定します。

（注） Cisco IOS Release 12.2(8)T 以降では、**crypto ca identity** および **crypto ca trusted-root** コマンドは、その機能が **crypto ca trustpoint** コマンドに統合され、置き換えられました。 **crypto ca identity** または **crypto ca trusted-root** コマンドも入力はできますが、コンフィギュレーション モードおよびコマンドは、コンフィギュレーション内に「**crypto ca trustpoint**」として書き込まれます。

例

次に、「ka」という名前の CA を宣言し、登録および CRL パラメータを指定する例を示します。

```
crypto ca trustpoint ka
 enrollment url http://kahului:80
```

次に、**crypto ca certificate map** コマンドで定義され、**crypto ca | pki trustpoint** コマンドの **match certificate** サブコマンドに含まれる「Group」というラベルを持つ、証明書ベースのアクセス コントロール リスト（ACL）の例を示します。

```
crypto ca certificate map Group 10
 subject-name co ou=WAN
 subject-name co o=Cisco
!
crypto ca trustpoint pki
 match certificate Group
```

関連コマンド

コマンド	説明
crl	CRL をクエリーし、ピアの証明書が失効していないことを確認します。
default（ca-trustpoint）	ca-trustpoint コンフィギュレーション サブコマンドの値をデフォルトにリセットします。
enrollment	CA の登録パラメータを指定します。
enrollment http-proxy	HTTP を使用し、プロキシ サーバ経由で CA にアクセスします。
primary	特定のトラストポイントをルータのプライマリ トラストポイントとして割り当てます。
root	TFTP を使用して CA 証明書を取得します。