公開キー インフラストラクチャ コマンド

ここでは、公開キーインフラストラクチャ（PKI）を設定するために使用されるコマンドについて説明します。

PKI の概念、設定作業、および例の詳細については、『*Cisco ASR 9000 Series Aggregation Services Router System Security Configuration Guide*』の「*Implementing Certification Authority Interoperability on Cisco ASR 9000 Series Router*」モジュールを参照してください。

clear crypto ca certificates

コンフィギュレーション ファイルに存在しないトラストポイントに関連付けられている証明書をクリアするには、EXEC モードで **clear crypto ca certificates** コマンドを使用します。

clear crypto ca certificates *trustpoint*

構文の説明

trustpoint	トラストポイント名。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータが、新しいコンフィギュレーション ファイルを使用してロードされており、新しいコンフィギュレーションファイルに対応するトラストポイントが設定されていない場合は、**clear crypto ca certificates** コマンドを使用して、コンフィギュレーション ファイルに存在しないトラストポイントに関連付けられている証明書をクリアします。

clear crypto ca certificates コマンドにより、Certification Authority（CA; 認証局）およびルータの両方の証明書がシステムから削除されます。

タスク ID

タスク ID	操作
crypto	実行

例

次に、コンフィギュレーション ファイルに存在しないトラストポイントに関連付けられている証明書をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# clear crypto ca certificates tp_1
```

clear crypto ca crl

ルータに保存されているすべての Certificate Revocation Lists（CRL; 証明書失効リスト）をクリアするには、EXEC モードで **clear crypto ca crl** コマンドを使用します。

clear crypto ca crl

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

デフォルトの動作または値はありません。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータに保存されているすべての CRL をクリアするには、**clear crypto ca crl** コマンドを使用します。 その結果、ルータは認証局（CA）に承認され、証明書を確認する着信要求に対する新しい CRL をダウンロードします。

タスク ID

タスク ID	操作
crypto	実行

例

次に、ルータに保存されているすべての CRL をクリアする例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ca crls

CRL Entry
================================================
  Issuer : cn=Certificate Manager,ou=HFR,o=Cisco Systems,l=San Jose,st=CA,c=US
```

```
  Last Update : [UTC] Wed Jun  5 02:40:04 2002
  Next Update : [UTC] Wed Jun  5 03:00:04 2002
  CRL Distribution Point :
ldap://manager.cisco.com/CN=Certificate Manager,O=Cisco Systems

RP/0/RSP0/CPU0:router# clear crypto ca crl
RP/0/RSP0/CPU0:router# show crypto ca crls
```

関連コマンド

コマンド	説明
show crypto ca crls, （56 ページ）	ルータの CRL に関する情報を表示します。

crl optional（トラストポイント）

他のピアの証明書が、対応するCRLを取得しなくても受け付けられるようにするには、トラストポイント コンフィギュレーション モードで **crl optional** コマンドを使用します。 ルータが証明書を受け付ける前にCRL チェックを必須とするデフォルト動作に戻すには、このコマンドの **no** 形式を使用します。

crl optional

no crl optional

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

ルータは、他のIPセキュリティ ピアの証明書を受け付ける前に、対応するCRLを取得しており、それをチェックしている必要があります。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスクIDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータがピアから証明書を受け取ると、対応するCRLがないかメモリを検索します。ルータが対応する CRL を見つけた場合は、その CRL が使用されます。 見つからなかった場合は、ルータはピアの証明書での指定に従って、認証局（CA）またはCRL Distribution Point（CDP; CRL 分散ポイント）のどちらかから CRL をダウンロードします。 次に、ルータはCRL をチェックして、ピアから送信された証明書が無効になっていないことを確認します。 証明書がCRLに表示されている場合、ルータは証明書を受け付けることができず、ピアを認証できません。CRLをダウンロードしないで、証明書を無効として処理するようルータに指示するには、**crl optional** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、CA を宣言して、CRL を取得しないでルータが証明書を受け付けることを許可します。 またこの例では、非標準のリトライ期間とリトライ回数も指定します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 20
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 100
RP/0/RSP0/CPU0:router(config-trustp)# crl optional
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment retry count, （32 ページ）	ルータが証明書要求を再送信する回数を指定します。
enrollment retry period, （34 ページ）	証明書要求の次のリトライまでの待機時間を指定します。
enrollment url, （38 ページ）	CA の URL を指定します。

crypto ca authenticate

認証局（CA）の証明書を取得することでCAを認証するには、EXECモードで**crypto ca authenticate**コマンドを使用します。

crypto ca authenticate *ca-name*

構文の説明

ca-name	CA サーバ名

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク IDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータで最初に CA サポートを設定する際は、**crypto ca authenticate** コマンドが必要です。

このコマンドは、CA の公開キーを含む CA 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。 自己署名のルート CA の場合は、CA がそれ自体の証明書に署名するため、このコマンドを使用する際に CA 管理者に連絡して、CA 公開キーを手動で認証する必要があります。 証明書のフィンガープリントの照合は、アウトオブバンド（電話機での通話など）で行われます。

ルート CA の認証前に、第 2 レベルの CA の認証を行う必要があります。

crypto ca authenticateコマンドを発行した後、指定されたタイムアウト期間までにCAが応答しない場合、もう一度端末コントロールを取得して、コマンドを再入力する必要があります。

タスク ID

タスク ID	操作
crypto	実行

例

CAによって証明書が送信され、ルータから、証明書のフィンガープリント（一意のID）をチェックすることで証明書を確認するよう管理者にプロンプトが表示されます。 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。 画面のフィンガープリントが、CA管理者によって表示されているフィンガープリントと一致した場合は、その証明書を有効な証明書として受け付ける必要があります。

次の例では、ルータによるCA証明書の要求を示します。

```
RP/0/RSP0/CPU0:router# crypto ca authenticate msiox
Retrieve Certificate from SFTP server? [yes/no]: yes
Read 860 bytes as CA certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Certificate has the following attributes:
   Fingerprint: D0 44 36 48 CE 08 9D 29 04 C4 2D 69 80 55 53 A3

Do you accept this certificate? [yes/no]: yes


RP/0/RSP0/CPU0:router#:Apr 10 00:28:52.324 : cepki[335]: %SECURITY-CEPKI-6-INFO : certificate
 database updated
Do you accept this certificate? [yes/no] yes
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
show crypto ca certificates, （54 ページ）	ご使用の証明書およびCAの証明書に関する情報を表示します。

crypto ca cancel-enroll

現在の登録要求をキャンセルするには、EXEC モードで **crypto ca cancel-enroll** コマンドを使用します。

crypto ca cancel-enroll *ca-name*

構文の説明

ca-name	認証局（CA）の名前

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

トラストポイント コンフィギュレーション モードで rsakeypair, （44 ページ） コマンドによって定義されているルータの Rivest, Shamir, and Adelman（RSA）キー ペアの証明書を CA から要求するには、**crypto ca enroll** コマンドを使用します。 現在のトラストポイントに対して rsakeypair, （44 ページ） コマンドが設定されていない場合は、登録にはデフォルトの RSA キー ペアが使用されます。 このタスクは、CA を使用した登録とも呼ばれます。 現在の登録要求をキャンセルするには、**crypto ca cancel-enroll** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	実行

例

次に、myca という名前の CA から現在の登録要求をキャンセルする例を示します。

```
RP/0/RSP0/CPU0:router# crypto ca cancel-enroll myca
```

関連コマンド

コマンド	説明
crypto ca enroll, （13 ページ）	CA からルータの証明書を取得します。
rsakeypair, （44 ページ）	トラストポイントに対する名前付きの RSA キーペアを指定します。

crypto ca enroll

認証局（CA）からルータの証明書を取得するには、EXEC モードで **crypto ca enroll** コマンドを使用します。

crypto ca enroll *ca-name*

構文の説明

ca-name	CA サーバ名

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

トラストポイント コンフィギュレーション モードで rsakeypair, （44 ページ） コマンドによって定義されているルータの Rivest, Shamir, and Adelman（RSA）キー ペアの証明書を CA から要求するには、**crypto ca enroll** コマンドを使用します。 現在のトラストポイントに対して rsakeypair, （44 ページ） コマンドが設定されていない場合は、登録にはデフォルトの RSA キー ペアが使用されます。 このタスクは、CA を使用した登録とも呼ばれます。 （証明書の登録と取得は、2 つの個別のイベントですが、**crypto ca enroll** コマンドが発行された場合はこれら両方のイベントが発生します）。手動登録を行った場合、この 2 つのイベントは個別に発生します。

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、このコマンドを設定できません。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 （既存の証明書を削除するには、**no**

crypto ca trustpoint コマンドを使用してトラストポイント コンフィギュレーションを削除します）。

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。

タスク ID

タスク ID	操作
crypto	実行

例

次に、**crypto ca enroll** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# crypto ca enroll msiox
% 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 you password will not be saved in the configuration.
% Please make a note of it.
%Password
re-enter Password:
    Fingerprint: 4F35ADC9 2791997A CE211437 AFC66CF7
RP/0/RSP0/CPU0:May 29 18:49:15.572 : pki_cmd: %PKI-6-LOG_INFO : certificate request pending
RP/0/RSP0/CPU0:May 29 18:52:17.705 : pki_get_cert: %PKI-6-LOG_INFO : certificate is granted
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
rsakeypair, （44 ページ）	トラストポイントに対する名前付きのRSA キーペアを指定します。

crypto ca import

認証局（CA）証明書を、TFTP、SFTP、または端末でのカットアンドペーストを使用して手動でインポートするには、EXEC モードで **crypto ca import** コマンドを使用します。

crypto ca import *name* **certificate**

構文の説明

name **certificate**	認証局（CA）の名前 この名前には、crypto ca trustpoint, （17 ページ）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

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	実行

例

次に、CA 証明書をカット アンド ペーストを使用してインポートする例を示します。 この例では、証明書は myca という名前です。

```
RP/0/RSP0/CPU0:router# crypto ca import myca certificate
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
show crypto ca certificates, （54 ページ）	証明書と認証局（CA）証明書に関する情報を表示します。

crypto ca trustpoint

信頼できるポイントを選択した名前で設定するには、グローバル コンフィギュレーション モードで **crypto ca trustpoint** コマンドを使用します。 信頼できるポイントの設定を解除するには、このコマンドの **no** 形式を使用します。

crypto ca trustpoint *ca-name*

no crypto ca trustpoint *ca-name*

構文の説明

ca-name	CA の名前。

コマンド デフォルト

なし

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	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

CA を宣言するには、**crypto ca trustpoint** コマンドを使用します。

このコマンドを使用して、選択した名前で信頼できるポイントを設定できるので、ルータはピアに対して発行された証明書を確認できます。 ルータは、ピアに対して証明書を発行した CA に登録する必要はありません。

crypto ca trustpoint コマンドを実行するとトラストポイント コンフィギュレーション モードが開始され、このモードで次のコマンドを使用して CA の特性を指定できます。

- crl optional（トラストポイント）, （7 ページ） コマンド：対応する CRL を取得しなくても他のピアの証明書が受け付けられます。
- enrollment retry count, （32 ページ） コマンド：ルータによって送信される、証明書要求のリトライ回数 オプション

- enrollment retry period, （34 ページ） コマンド：（任意）ルータが証明書要求のリトライを送信するまでの待機時間。
- enrollment terminal, （36 ページ） コマンド：ルータと認証局（CA）間がネットワーク接続されていない場合に、証明書要求と証明書を手動でカット アンド ペーストします。
- enrollment url, （38 ページ） コマンド：（任意）CA の URL。
- ip-address（トラストポイント）, （40 ページ） コマンド：証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレス
- query url, （42 ページ） コマンド：証明書失効リスト（CRL）が発行されるディレクトリ サーバの URL。「ldap://」で始まる文字列だけが受け付けられます。
  CA が Lightweight Directory Access Protocol（LDAP）をサポートしている場合に限り必要です。
- rsakeypair, （44 ページ） コマンド：このトラストポイントに対する名前付きの Rivest, Shamir, and Adelman（RSA）キー ペア。
- serial-number（トラストポイント）, （46 ページ） コマンド：証明書要求内のルータのシリアル番号。
- sftp-password（トラストポイント）, （48 ページ） コマンド：FTP セキュア パスワード。
- sftp-username（トラストポイント）, （50 ページ） コマンド：FTP セキュア ユーザ名。
- subject-name（トラストポイント）, （52 ページ） コマンド：証明書要求内の件名。

タスク ID

タスク ID	操作
crypto	実行

例

次に、**crypto ca trustpoint** コマンドを使用してトラストポイントを作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-password xxxxxx
RP/0/RSP0/CPU0:router(config-trustp)# sftp-username tmordeko
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url
sftp://192.168..254.254/tftpboot/tmordeko/CAcert
RP/0/RSP0/CPU0:router(config-trustp)# rsakeypair label-2
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （7 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。

コマンド	説明
enrollment retry count, （32 ページ）	ルータが証明書要求を再送信する回数を指定します。
enrollment retry period, （34 ページ）	証明書要求の次のリトライまでの待機時間を指定します。
enrollment terminal, （36 ページ）	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。
enrollment url, （38 ページ）	CA の URL を指定します。
query url, （42 ページ）	CRL 分散ポイントの LDAP の URL を指定します。
rsakeypair, （44 ページ）	このトラストポイントに対する名前付きのRSA キー ペアを指定します。
sftp-password（トラストポイント）, （48 ページ）	FTP パスワードを保護します。
sftp-username（トラストポイント）, （50 ページ）	FTP ユーザ名を保護します。

crypto key generate dsa

Digital Signature Algorithm（DSA; デジタル署名アルゴリズム）キー ペアを生成するには、EXEC モードで **crypto key generate dsa** コマンドを使用します。

crypto key generate dsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータに対して DSA キー ペアを作成するには、**crypto key generate dsa** コマンドを使用します。

DSA キーはペアで作成されます。1 つは DSA 公開キー、もう 1 つは DSA 秘密キーです。

このコマンドの発行時に、ルータにすでにDSAキーが設定されている場合は、警告が表示され、既存のキーを新しいキーと置き換えるようプロンプトが表示されます。

生成された DSA キーを削除するには、**crypto key zeroize dsa** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	実行

例

次に、512 ビットの DSA キーを生成する例を示します。

```
RP/0/RSP0/CPU0:router# crypto key generate dsa
The name for the keys will be: the_default
    Choose the size of your DSA key modulus. Modulus size can be 512, 768, or 1024 bits.
Choosing a key modulus
How many bits in the modulus [1024]: 512
Generating DSA keys...
Done w/ crypto generate keypair
[OK]
```

関連コマンド

コマンド	説明
crypto key zeroize dsa, （26 ページ）	ルータから DSA キー ペアを削除します。
show crypto key mypubkey dsa, （58 ページ）	ルータの DSA 公開キーを表示します。

crypto key generate rsa

Rivest, Shamir, and Adelman（RSA）キー ペアを作成するには、EXEC モードで **crypto key generate rsa** コマンドを使用します。

crypto key generate rsa [**usage-keys| general-keys**] [*keypair-label*]

構文の説明

usage-keys	（任意）署名および暗号化用に個別のRSAキーペアを作成します。
general-keys	（任意）署名および暗号化用に汎用のRSAキーペアを作成します。
keypair-label	（任意）RSA キー ペアに名前を付ける RSA キー ペアのラベル。

コマンド デフォルト

RSA キー ペアは存在しません。 **usage-keys** キーワードが使用されていない場合、汎用キーが作成されます。 RSA ラベルが指定されていない場合、キーはデフォルトの RSA キーとして生成されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータに RSA キー ペアを生成するには、**crypto key generate rsa** コマンドを使用します。

RSA キーはペアで作成されます。1 つは RSA 公開キー、もう 1 つは RSA 秘密キーです。

このコマンドの発行時に、ルータにRSAキーがすでに設定されている場合は、警告が表示され、既存のキーを新しいキーと置き換えるよう求めるプロンプトが表示されます。 このコマンドによって生成されるキーは、セキュア NVRAM（ユーザには表示されず、別のデバイスにもバックアップされません）に保存されます。

RSA キーを削除するには、**crypto key zeroize rsa** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	実行

例

次に、RSA キー ペアを作成する例を示します。

```
RP/0/RSP0/CPU0:router# crypto key generate rsa

The name for the keys will be: the_default

Choose the size of the key modulus in the range of 360 to 2048 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus[1024]: <return>
RP/0/RSP0/CPU0:router#
```

関連コマンド

コマンド	説明
crypto key zeroize rsa, （28 ページ）	ルータ用の RSA キー ペアを削除します。
show crypto key mypubkey rsa, （60 ページ）	ルータの RSA 公開キーを表示します。

crypto key import authentication rsa

Rivest, Shamir, and Adelman（RSA）方式を使用して公開キーをインポートするには、EXEC モードで **crypto key import authentication rsa** コマンドを使用します。

crypto key import authentication rsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.9.0	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

まず、ssh-keygen などのキー生成メカニズムを使用して UNIX クライアント上に RSA 公開キーと秘密キーのキーペアを生成する必要があります。 キーサイズの範囲は、512 ～ 2048 ビットです。

次に、公開キーをボックスに正しくインポートするために、公開キーを Base64 エンコード（バイナリ）形式に変換する必要があります。 nvram ボックスに保存できるキーの数は、個々のキー サイズによって異なります。 このサイズは、ユーザ定義の変数です。

公開キーが生成されると、RSA ベースの認証をイネーブルにするルータ上にキーを配置する必要があります。

タスク ID

タスク ID	操作
crypto	実行

例

次に、公開キーをインポートする例を示します。

```
RP/RSP0/0/CPU0:k2#crypto key import authentication rsa
```

crypto key zeroize dsa

デジタル署名アルゴリズム（DSA）キー ペアをルータから削除するには、EXEC モードで **crypto key zeroize dsa** コマンドを使用します。

crypto key zeroize dsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータによって以前生成された DSA キー ペアを削除するには、**crypto key zeroize dsa** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	実行

例

次に、ルータから DSA キーを削除する例を示します。

```
RP/0/RSP0/CPU0:router# crypto key zeroize dsa
% Keys to be removed are named the_default
Do you really want to remove these keys? [yes/no]: yes
```

関連コマンド

コマンド	説明
crypto key generate dsa, （20 ページ）	DSA キー ペアを作成します。
show crypto key mypubkey dsa, （58 ページ）	ルータの DSA 公開キーを表示します。

crypto key zeroize rsa

ルータからすべての Rivest, Shamir, and Adelman（RSA）キーを削除するには、EXEC モードで **crypto key zeroize rsa** コマンドを使用します。

crypto key zeroize rsa [*keypair-label*]

構文の説明

keypair-label	（任意）削除する RSA キー ペアを指定します。

コマンド デフォルト

キー ペアのラベルが指定されていない場合は、デフォルトの RSA キー ペアが削除されます。

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータによって以前生成されたすべての RSA キーを削除するには、**crypto key zeroize rsa** コマンドを使用します。 このコマンドの実行後、次の 2 つのタスクを追加で実行する必要があります。

- 認証局（CA）の管理者に、CA でルータの証明書を無効にするよう依頼する。このとき、当初 crypto ca enroll, （13 ページ） コマンドを使用してルータの証明書を取得する際に作成したチャレンジ パスワードを CA に提供する必要があります。
- **clear crypto ca certificates** コマンドを使用して、設定から証明書を手動で削除する。

タスク ID

タスク ID	操作
crypto	実行

例

次に、以前生成された汎用 RSA キー ペアを削除する例を示します。

```
RP/0/RSP0/CPU0:router# crypto key zeroize rsa key1
% Keys to be removed are named key1
Do you really want to remove these keys? [yes/no]: yes
```

関連コマンド

コマンド	説明
clear crypto ca certificates, （3 ページ）	コンフィギュレーション ファイルに存在しないトラストポイントに関連付けられた証明書をクリアします。
crypto ca enroll, （13 ページ）	CA からルータの証明書を取得します。
crypto key generate rsa, （22 ページ）	RSA キー ペアを生成します。
show crypto key mypubkey rsa, （60 ページ）	ルータの RSA 公開キーを表示します。

description（トラストポイント）

トラストポイントの説明を作成するには、トラストポイント コンフィギュレーション モードで **description** コマンドを使用します。トラストポイントの説明を削除するには、このコマンドの **no** 形式を使用します。

description *string*

no description

構文の説明

string	トラストポイントを説明する文字ストリング

コマンド デフォルト

デフォルトの説明は空白です。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

トラストポイントの説明を作成するには、トラストポイント コンフィギュレーション モードで **description** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、トラストポイントの説明を作成する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# description this is the primary trustpoint
```

enrollment retry count

ルータが認証局（CA）へ証明書要求を再送信する回数を指定するには、トラストポイント コンフィギュレーション モードで **enrollment retry count** コマンドを使用します。 リトライ回数をデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

enrollment retry count *number*

no enrollment retry count *number*

構文の説明

number	ルータが前回の要求で証明書を受け取っていない場合に、証明書要求を再送信する回数。 範囲は 1 ～ 100 です。

コマンド デフォルト

リトライ回数が指定されていない場合、デフォルト値は 10 です。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

証明書の要求後、ルータは CA からの証明書の受け取りを待機します。 指定された時間（リトライ期間）内にルータが証明書を受け取らなかった場合、ルータは再度証明書要求を送信します。 ルータは、有効な証明書を受け取るか、CA から登録エラーが返されるか、または設定されているリトライ回数を超えるまで、要求を送信し続けます。

リトライ回数をデフォルトの 10 にリセットするには、このコマンドの **no** 形式を使用します。 リトライ回数を 0 に設定すると、リトライが無制限に行われます。 ルータは、有効な証明書を受け取るまで CA の証明書要求を送信します（リトライ回数は無制限）。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、CA を宣言してリトライ期間を 10 分に変更し、リトライ回数を 60 回に変更する例を示します。 ルータは、証明書を受け取るか、最初の要求の送信後約 10 時間が経過するかのどちらか早い方まで、10 分おきに証明書要求を再送信します（10 分 x 60 回 = 600 分 = 10 時間）。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://ca_server
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 10
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry count 60
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （7 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment retry period, （34 ページ）	証明書要求の次のリトライまでの待機時間を指定します。
enrollment url, （38 ページ）	認証局（CA）の場所を、CA の URL で指定します。

enrollment retry period

証明書要求をリトライするまでの待機期間を指定するには、トラストポイント コンフィギュレーション モードで **enrollment retry period** コマンドを使用します。 リトライ期間をデフォルトの 1 分にリセットするには、このコマンドの **no** 形式を使用します。

enrollment retry period *minutes*

no enrollment retry period *minutes*

構文の説明

minutes	ルータから認証局（CA）へ行われる証明書要求をリトライするまでの期間（分単位）。 範囲は 1 ～ 60 分です。

コマンド デフォルト

minutes：*1*

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

証明書の要求後、ルータは CA からの証明書の受け取りを待機します。 指定された時間（リトライ期間）内にルータが証明書を受け取らなかった場合、ルータは再度証明書要求を送信します。ルータは、有効な証明書を受け取るか、CA から登録エラーが返されるか、または設定されているリトライ回数を超えるまで、要求を送信し続けます。

ルータは、有効な証明書を受け取るまで、CA に証明書要求を送信します（デフォルトでは、ルータは要求を 10 回送信しますが、**enrollment retry count** コマンドを使用して、リトライ回数を変更できます）。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、CA を宣言してリトライ期間を 5 分に変更する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment retry period 5
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （7 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment retry count, （32 ページ）	ルータが証明書要求を再送信する回数を指定します。

enrollment terminal

カットアンドペーストによる手動登録を指定するには、トラストポイント コンフィギュレーション モードで **enrollment terminal** 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。

enrollment terminal

no enrollment terminal

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ルータと認証局（CA）間がネットワーク接続されていない場合、証明書要求と証明書を手動でカット アンド ペーストできます。 **enrollment terminal** コマンドがイネーブルの場合、ルータのコンソール端末に証明書要求が表示され、これにより発行された証明書を端末上で入力できます。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、カット アンド ペーストにより証明書の登録を手動で指定する例を示します。 この例で、CA のトラストポイントは myca です。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment terminal
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。

enrollment url

認証局（CA）の場所を CA の URL で指定するには、トラストポイント コンフィギュレーション モードで **enrollment url** コマンドを使用します。 設定から CA の URL を削除するには、このコマンドの **no** 形式を使用します。

enrollment url *CA-URL*

no enrollment url *CA-URL*

構文の説明

CA-URL	CA サーバの URL。 URL ストリングの先頭は、http://CA_name であることが必要です。CA_name はホストのドメイン ネーム システム（DNS）の名前、または CA の IP アドレス（例：http://ca-server）です。 CA で CA cgi-bin スクリプトの場所が /cgi-bin/pkiclient.exe（デフォルトの CA cgi-bin スクリプトの場所）でない場合は、非標準スクリプトの場所も、http://CA-name/script-location（script-location は CA スクリプトのフル パス）の形式で URL に含める必要があります。

コマンド デフォルト

なし

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

CA の URL を指定するには、**enrollment url** コマンドを使用します。 このコマンドは、**crypto ca trustpoint** コマンドを使用して CA を宣言する際に必要です。 CA スクリプトがデフォルトの cgi-bin スクリプトの場所にロードされない場合は、URL に CA スクリプトの場所を含める必要があります。 CA スクリプトの場所については、CA 管理者に問い合わせます。

次の表に、使用可能な登録方式を示します。

表 *1*：証明書の登録方式

登録方式	説明
SFTP	SFTP: ファイル システムを使用した登録
TFTP[1]	TFTP: ファイル システムを使用した登録

1 登録に TFTP を使用している場合は、URL を tftp://certserver/file_specification の形式で指定する必要があります。（ファイルの指定は任意です）。

TFTP による登録では、登録要求が送信され、CA の証明書とルータの証明書が取得されます。URL でファイルが指定されている場合、ルータはそのファイルに拡張子を追加します。

CA の URL を変更するには、**enrollment url** コマンドを繰り返し実行して、以前の URL を上書きします。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、CA の宣言に必要な最小限の絶対設定を示します。

```
RP/0/RSP0/CPU0:router# configure RP/0/RSP0/CPU0:router(config)#
            crypto ca trustpoint myca RP/0/RSP0/CPU0:router(config-trustp)#
            enrollment url http://ca.domain.com/certsrv/mscep/mscep.dll
```

関連コマンド

コマンド	説明
crl optional（トラストポイント），（7 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint,（17 ページ）	信頼できるポイントを選択した名前で設定します。
ip-address（トラストポイント），（40 ページ）	証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレスを指定します。

ip-address（トラストポイント）

証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレスを指定するには、トラストポイント コンフィギュレーション モードで **ip-address** コマンドを使用します。デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

ip-address {*ip-address*| **none**}

no ip-address {*ip-address*| **none**}

構文の説明

ip-address	証明書要求内に含まれるドット付き IP アドレス
none	IP アドレスを証明書要求内に含まないことを指定します。

コマンド デフォルト

証明書の登録時に、IP アドレスを要求するプロンプトが表示されます。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

ip-address コマンドを使用して、指定されたインターフェイスの IP アドレスを証明書要求に含めたり、IP アドレスを証明書要求に含めないよう指定します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、Ethernet 0 インターフェイスの IP アドレスをトラストポイント フロッグの証明書要求に含める例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RSP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RSP0/CPU0:router(config-trustp)# ip-address 172.19.72.120
```

次に、IP アドレスを証明書要求に含めない例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RSP0/CPU0:router(config-trustp)# subject-name CN=subject1, OU=PKI, O=Cisco Systems,
C=US
RP/0/RSP0/CPU0:router(config-trustp)# ip-address none
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （7 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment url, （38 ページ）	認証局（CA）の場所を、CA の URL で指定します。
serial-number（トラストポイント）, （46 ページ）	証明書要求にルータのシリアル番号を含める必要があるかどうかを指定します。
subject-name（トラストポイント）, （52 ページ）	証明書要求の所有者名を指定します。

query url

Lightweight Directory Access Protocol（LDAP）プロトコルのサポートを指定するには、トラストポイント コンフィギュレーション モードで **query url** コマンドを使用します。 設定からクエリーの URL を削除するには、このコマンドの **no** 形式を使用します。

query url *LDAP-URL*

no query url *LDAP-URL*

構文の説明

LDAP-URL	LDAP サーバの URL（ldap://another-server など）。 この URL は、ldap://server-name の形式であることが必要です（server-name はホストの ドメイン ネーム システム（DNS）名または LDAP サーバの IP アドレス）。

コマンド デフォルト

ルータ証明書の CRLDistributionPoint 拡張子に提示されている URL が使用されます。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

LDAP は、ルータが証明書失効リスト（CRL）を取得する際に使用されるクエリー プロトコルです。 認証局（CA）の管理者は、CA が LDAP をサポートしているかどうかを把握している必要があります。CA が LDAP をサポートしている場合は、CA 管理者が証明書と証明書失効リストを取得する LDAP の場所を指示できます。

クエリーの URL を変更するには、**query url** コマンドを繰り返し実行して、以前の URL を上書きします。

タスク ID

タスク ID	操作
crypto	read, write

例

次の例では、CA が LDAP をサポートしている場合に CA の宣言に必要な設定を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# query url ldap://my-ldap.domain.com
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。

rsakeypair

このトラストポイントに対して名前付きの Rivest, Shamir, and Adelman（RSA）キー ペアを指定するには、トラストポイント コンフィギュレーション モードで **rsakeypair** コマンドを使用します。RSA キー ペアをデフォルトにリセットするには、このコマンドの **no** 形式を使用します。

rsakeypair *keypair-label*

no rsakeypair *keypair-label*

構文の説明

keypair-label	RSA キー ペアに名前を付ける RSA キー ペアのラベル

コマンド デフォルト

RSA キー ペアが指定されていない場合、このトラストポイントにはデフォルトの RSA キーが使用されます。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

このトラストポイントに **crypto key generate rsa** コマンドを使用して生成された、名前付きの RSA キー ペアを指定するには、**rsakeypair** コマンドを使用します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、トラストポイント myca に対して名前付きの RSA キー ペア key1 を指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RSP0/CPU0:router(config-trustp)# rsakeypair key1
```

関連コマンド

コマンド	説明
crypto key generate rsa, （22 ページ）	RSA キー ペアを生成します。

serial-number（トラストポイント）

ルータのシリアル番号を証明書要求に含めるかどうかを指定するには、トラストポイント コンフィギュレーション モードで **serial-number** コマンドを使用します。 デフォルトの動作に戻すには、このコマンドの **no** 形式を使用します。

serial-number [none]

no serial-number

構文の説明

none	（任意）証明書要求にシリアル番号を含めないよう指定します。

コマンド デフォルト

証明書の登録時に、シリアル番号を要求するプロンプトが表示されます。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

serial-number コマンドを使用する前に、**crypto ca trustpoint** コマンドをイネーブルにする必要があります。このコマンドにより、ルータが使用し、トラストポイント コンフィギュレーション モードを開始する認証局（CA）が宣言されます。

このコマンドを使用して、証明書要求でルータのシリアル番号を指定するか、**none** キーワードを使用して、証明書要求にシリアル番号を含めないよう指定します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、ルート証明書の要求でシリアル番号を省略する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint root
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://10.3.0.7:80
RP/0/RSP0/CPU0:router(config-trustp)# ip-address none
RP/0/RSP0/CPU0:router(config-trustp)# serial-number none
RP/0/RSP0/CPU0:router(config-trustp)# subject-name ON=Jack, OU=PKI, O=Cisco Systems, C=US
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （7 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment url, （38 ページ）	認証局（CA）の場所を、CA の URL で指定します。
ip-address（トラストポイント）, （40 ページ）	証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレスを指定します。
subject-name（トラストポイント）, （52 ページ）	証明書要求の所有者名を指定します。

sftp-password（トラストポイント）

FTP パスワードを保護するには、トラストポイント コンフィギュレーション モードで **sftp-password** コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sftp-password {*clear text*| **clear** *text*| **password** *encrypted string*}

no sftp-password {*clear text*| **clear** *text*| **password** *encrypted string*}

構文の説明

clear text	クリアテキストのパスワードで、表示目的のためだけに暗号化されます。
password *encrypted string*	パスワードを暗号化形式で入力します。

コマンド デフォルト

デフォルトでは *clear text* 引数が使用されます。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

パスワードは暗号化形式で保存され、プレーンテキストとしては保存されません。 コマンドライン インターフェイス（CLI）には、パスワード入力を指定するためのプロビジョニング（クリアおよび暗号化など）が含まれます。

SFTP プロトコルの一部として、ユーザ名とパスワードが必要です。 sftp:// というプレフィックスで始まる URL を指定する場合、トラストポイントで **sftp-password** コマンドに対するパラメータを設定する必要があります。 設定しなかった場合、証明書の手動登録に使用する証明書を SFTP サーバから取得できません。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、FTP パスワードを暗号化形式で保護する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-password password xxxxxx
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
sftp-username（トラストポイント）, （50 ページ）	FTP ユーザ名を保護します。

sftp-username（トラストポイント）

FTPユーザ名を保護するには、トラストポイント コンフィギュレーション モードで**sftp-username**コマンドを使用します。 この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

sftp-username *username*

no sftp-username *username*

構文の説明

username	ユーザ名。

コマンド デフォルト

なし

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク IDを含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

sftp-username コマンドが使用されるのは、URL のプレフィックスに sftp:// が含まれる場合だけです。 プレフィックスで sftp:// が指定されていない場合、SFTP を使用した証明書の手動登録は失敗します。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、FTP ユーザ名を保護する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint msiox
RP/0/RSP0/CPU0:router(config-trustp)# sftp-username tmordeko
```

関連コマンド

コマンド	説明
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
sftp-password（トラストポイント）, （48 ページ）	FTP パスワードを保護します。

subject-name（トラストポイント）

証明書要求で件名を指定するには、トラストポイント コンフィギュレーション モードで **subject-name** コマンドを使用します。 設定から件名をクリアするには、このコマンドの **no** 形式を使用します。

subject-name *x.500-name*

no subject-name *x.500-name*

構文の説明

x.500-name	（任意）証明書要求で使用される件名を指定します。

コマンド デフォルト

x.500-name 引数が指定されていない場合は、デフォルトの件名である fully qualified domain name（FQDN; 完全修飾ドメイン名）が使用されます。

コマンド モード

トラストポイント コンフィギュレーション

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

subject-name コマンドを使用する前に、**crypto ca trustpoint** コマンドをイネーブルにする必要があります。このコマンドにより、お使いのルータが使用し、トラストポイント コンフィギュレーション モードを開始する認証局（CA）が宣言されます。

subject-name コマンドは、自動登録に設定できる属性であるため、このコマンドを発行すると、登録時に件名を要求するプロンプトが表示されなくなります。

タスク ID

タスク ID	操作
crypto	read, write

例

次に、フロッグ証明書に件名を指定する例を示します。

```
RP/0/RSP0/CPU0:router# configure
RP/0/RSP0/CPU0:router(config)# crypto ca trustpoint frog
RP/0/RSP0/CPU0:router(config-trustp)# enrollment url http://frog.phoobin.com
RP/0/RSP0/CPU0:router(config-trustp)# subject-name OU=Spiral Dept., O=tiedye.com
RP/0/RSP0/CPU0:router(config-trustp)# ip-address 172.19.72.120
```

関連コマンド

コマンド	説明
crl optional（トラストポイント）, （7 ページ）	対応する CRL を取得しなくてもピアの証明書が受け付けられるようにします。
crypto ca trustpoint, （17 ページ）	信頼できるポイントを選択した名前で設定します。
enrollment url, （38 ページ）	認証局（CA）の場所を、CA の URL で指定します。
ip-address（トラストポイント）, （40 ページ）	証明書要求内に非構造化アドレスとして含まれているドット付き IP アドレスを指定します。
serial-number（トラストポイント）, （46 ページ）	証明書要求にルータのシリアル番号を含める必要があるかどうかを指定します。

show crypto ca certificates

ご使用の証明書および認証局（CA）証明書に関する情報を表示するには、EXEC モードで **show crypto ca certificates** コマンドを使用します。

show crypto ca certificates

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

次の証明書に関する情報を表示するには、**show crypto ca certificates** コマンドを使用します。

- ご使用の証明書（CA に要求した場合。**crypto ca enroll** コマンドを参照）
- CA 証明書（証明書を受け取っている場合。**crypto ca authenticate** コマンドを参照）

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto ca certificates** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ca certificates
Trustpoint       : msiox
================================================
```

```
CAa certificate
  Serial Number  : 06:A5:1B:E6:4F:5D:F7:83:41:11:D5:F9:22:7F:95:23
  Subject:
    Name: CA2
    CN= CA2
  Issued By      :
        cn=CA2
  Validity Start : 07:51:51 UTC Wed Jul 06 2005
  Validity End   : 08:00:43 UTC Tue Jul 06 2010
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Router certificate
  Status         : Available
  Key usage      : Signature
  Serial Number  : 38:6B:C6:B8:00:04:00:00:01:45
  Subject:
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:30:03 UTC Mon Apr 10 2006
  Validity End   : 08:40:03 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: MS-IOX
Router certificate
  Status         : Available
  Key usage      : Encryption
  Serial Number  : 38:6D:2B:A7:00:04:00:00:01:46
  Subject:
    Name: tdlr533.cisco.com
    IP Address: 3.1.53.3
    Serial Number: 8cd96b64
  Issued By      :
        cn=CA2
  Validity Start : 08:31:34 UTC Mon Apr 10 2006
  Validity End   : 08:41:34 UTC Tue Apr 10 2007
  CRL Distribution Point
        http://10.56.8.236/CertEnroll/CA2.crl
Associated Trustpoint: msiox
```

関連コマンド

コマンド	説明
crypto ca authenticate, （9 ページ）	CA の証明書を取得することにより、CA を認証します。
crypto ca enroll, （13 ページ）	CA からルータの証明書を取得します。
crypto ca import, （15 ページ）	認証局（CA）証明書を、TFTP、SFTP、または端末でのカット アンド ペーストを通じて、手動でインポートします。
crypto ca trustpoint, （17 ページ）	トラストポイントを選択した名前で設定します。

show crypto ca crls

ローカル キャッシュの証明書失効リスト（CRL）に関する情報を表示するには、EXEC モードで **show crypto ca crls** コマンドを使用します。

show crypto ca crls

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto ca crls** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto ca crls
CRL Entry
==============================================
Issuer : cn=xyz-w2k-root,ou=HFR,o=Cisco System,l=San Jose,st=CA,c=US
Last Update : [UTC] Thu Jan 10 01:01:14 2002
Next Update : [UTC] Thu Jan 17 13:21:14 2002
CRL Distribution Point :
http://xyz-w2k.cisco.com/CertEnroll/xyz-w2k-root.crl
```

関連コマンド

コマンド	説明
clear crypto ca crl, （5 ページ）	ルータに保存されているすべての CRL をクリアします。

show crypto key mypubkey dsa

ルータの Directory System Agent（DSA）公開キーを表示するには、EXEC モードで **show crypto key mypubkey dsa** コマンドを使用します。

show crypto key mypubkey dsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto key mypubkey dsa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto key mypubkey dsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created : 17:33:23 UTC Thu Sep 18 2003
Data :
3081F230 81AA0605 2B0E0302 0C3081A0 02020200 024100C8 A36B6179 56B8D620
1F77595C 32EF3004 577A9F79 0A8ABDA4 89FB969D 35C04E7E 5491ED4E 120C657C
610576E5 841696B6 0948846C C92F56E5 B4921458 70FC4902 1500AB61 5C0D63D3
EB082BB9 F16030C5 AA0B5D1A DFE50240 73F661EA 9F579E77 B413DBC4 9047B4F2
```

```
10A1CFCB 14D98B57 3E0BBA97 9B5120AD F52BBDC7 15B63454 8CB54885 92B6C9DF
7DC27768 FD296844 42024945 5E86C81A 03430002 4071B49E F80F9E4B AF2B62E7
AA817460 87EFD503 C668AD8C D606050B 225CC277 7C0A0974 8072D7D7 2ADDDE42
329FE896 AB015ED1 3A414254 6935FDCA 0043BA4F 66
```

関連コマンド

コマンド	説明
crypto key generate dsa, （20 ページ）	DSA キー ペアを作成します。
crypto key zeroize dsa, （26 ページ）	ルータからすべての DSA キーを削除します。

show crypto key mypubkey rsa

ルータの Rivest、Rivest, Shamir, and Adelman（RSA）公開キーを表示するには、EXEC モードで **show crypto key mypubkey rsa** コマンドを使用します。

show crypto key mypubkey rsa

構文の説明

このコマンドには、キーワードと引数はありません。

コマンド デフォルト

なし

コマンド モード

EXEC

コマンド履歴

リリース	変更箇所
リリース 3.7.2	このコマンドが追加されました。

使用上のガイドライン

このコマンドを使用するには、適切なタスク ID を含むタスク グループに関連付けられているユーザ グループに属している必要があります。 ユーザ グループの割り当てのためにコマンドを使用できない場合は、AAA 管理者に連絡してください。

タスク ID

タスク ID	操作
crypto	read

例

次に、**show crypto key mypubkey rsa** コマンドの出力例を示します。

```
RP/0/RSP0/CPU0:router# show crypto key mypubkey rsa

Key label: mykey
Type : RSA General purpose
Size : 1024
Created  : 07:46:15 UTC Fri Mar 17 2006
Data :
30819F30 0D06092A 864886F7 0D010101 05000381 8D003081 89028181 00CF8CDF
5BFCA055 DA4D164D F6EDB78B 926B1DDE 0383027F BA71BCC6 9D5592C4 5BA8670E
35CD19B7 1C973A46 62CC5F8C 82BD596C F292410F 8E83B753 4BA71BAC 41AB6B60
F34A2499 EDE11639 F88B4210 B2A0CF5F DD678C36 0D8B7DE1 A2AB5122 9ED947D5
```

```
76CF5BCD D9A2039F D02841B0 7F8BFF97 C080B791 10A9ED41 00FB6F40 95020301
0001

Key label: the_default
Type : RSA General purpose
Size : 512
Created  : 07:46:15 UTC Fri Mar 17 2006
Data :
305C300D 06092A86 4886F70D 01010105 00034B00 30480241 00C7DE73 7B3EA447
CCE8F3DF DD1327D8 C1C30C45 2EEB4981 B1B48D2B 1AF14665 178058FB 8F6BB6BB
E08C6163 FA0EE356 395C8E5F 2AC59383 0706BDDF EC8E5822 9B020301 0001
```

関連コマンド

コマンド	説明
crypto key generate rsa, （22 ページ）	RSA キー ペアを生成します。
crypto key zeroize rsa, （28 ページ）	ルータからすべての RSA キーを削除します。