CHAPTER 9

コマンド ラインでのデジタル証明書の管理

この章では、コマンドライン インターフェイスを使用して証明書ストアのデジタル証明書を管理する方法について説明します。証明書ストアは、ローカル ファイル システムにあるデジタル証明書を保存している場所です。VPN クライアントのストアは Cisco ストアです。

証明書のキーワードの設定

証明書を使用して認証するには、ユーザ プロファイルの証明書に適用するすべてのキーワードを正しく設定する必要があります。次のキーワードの設定を確認します。

- **AuthType = 3**（証明書の認証）
- **CertStore = 1**（Cisco 証明書ストア）
- **CertName = Common Name**（証明書に入力された名前と同じ）

ユーザ プロファイルでのパラメータ設定の詳細については、「ユーザ プロファイル」（P.5-1）を参照してください。

証明書のコマンド構文

証明書管理のコマンドライン インターフェイスは次の 2 とおりの方法で動作します。

- 標準 UNIX シェルまたは DOS コマンドライン プロンプトで、指定のコマンドのすべての引数を同じ行に入力します。

  ```
  cisco_cert_mgr -U -op enroll -f filename -chall challenge_phrase
  ```

- プロンプト モードで、指定のコマンドに最小限の引数を入力すると、残りの情報の入力を求められます。

  最低限のコマンド ライン引数は、次の基本形式に従います。

  ```
  cisco_cert_mgr -U -op operation
  cisco_cert_mgr -R -op operation
  cisco_cert_mgr -E -op operation
  ```

  値は次のとおりです。

  - **-U** はユーザ証明書またはプライベート証明書に適用します。

    enroll_resume を除くすべての証明書管理コマンド オペレーションに -U フラグを使用できます。

  - **-R** はルート証明書または認証局（CA）証明書に適用します。

- **-R** はルート証明書または認証局（CA）証明書に適用します。

  list、view、verify、delete、export、import、change の各パスワード オペレーションに -R フラグを使用できます。

- **-E** は証明書登録に適用します。

  -E フラグは list および delete でのみ使用でき、enroll_resume オペレーションを使用して指定する必要があります。

指定された証明書のオペレーションは、**-op** 引数に従います。certificate manager コマンドに有効なオペレーションは、list、view、verify、delete、export、import、enroll、enroll_file、および enroll_resume です。これらのオペレーションの詳細については、「証明書管理オペレーション」を参照してください。

たとえば、次のコマンドを入力するとします。

```
cisco-cert-mgr -R -op import
```

Certificate Manager により、インポートするファイルの名前の入力を求められます。

証明書の内容

この項では、デジタル証明書に記載の情報の種類について説明します。

一般的なデジタル証明書には次の情報が記載されています。

- [Common name]：所有者の名前で、通常は姓名です。このフィールドは、公開キー インフラストラクチャ（PKI）組織内の所有者を示します。
- [Department]：所有者の部門の名前です。これは組織ユニットと同じです。

  VPN 3000 Concentrator に接続している場合、このフィールドはデバイスの所有者に設定された**グループ名**と一致する必要があります。
- [Company]：所有者が証明書を使用している会社です。これは組織と同じです。
- [State]：所有者が証明書を使用している都道府県です。
- [Country]：所有者のシステムがある 2 文字の国番号です。
- [Email]：証明書の所有者の電子メール アドレスです。
- [Thumbprint]：証明書の内容一式の MD5 ハッシュです。証明書の真偽を確認する方法を提供します。たとえば、発行側 CA と連絡する場合、この ID を使用して、これが使用すべき正しい証明書かどうか確認できます。
- [Key size]：署名キー ペアのサイズ（ビット単位）です。
- [Subject]：証明書の所有者の完全修飾ドメイン名（FQDN）です。このフィールドは、LDAP および X.500 ディレクトリ クエリーに使用できる形式で、証明書の所有者を一意に識別します。通常、件名には次のフィールドが含まれています。
  - 通常名（**cn**）
  - 組織ユニット、または部門（**ou**）
  - 組織または会社（**o**）
  - 地名、市、町（**l**）
  - 州または都道府県（**st**）
  - 国（**c**）
  - 電子メール アドレス（**e**）

- [Serial number]：証明書失効リスト（CRL）の証明書の有効性を追跡する場合に使用する一意の ID です。
- [Issuer]：証明書の提供元の FQDN です。
- [Not before]：証明書が有効になる開始日です。
- [Not after]：証明書が失効する前の最終日です。

次の出力は、デジタル証明書に記載されている情報の種類の例です。

```
Common Name: Fred Flintstone
Department: Rock yard
Company: Stone Co.
State: (null)
Country: (null)
Email: fredf@stonemail.fake
Thumb Print: 2936A0C874141273761B7F06F8152CF6
Key Size: 1024
Subject:e=fredf@stonemail.fake,cn=Fred Flinstone,ou=Rockyard,o=Stone Co. l=Bedrock
Serial #: 7E813E99B9E0F48077BF995AA8D4ED98
Issuer: Stone Co.
Not before: Thu May 24 18:00:00 2001
Not after: Mon May 24 17:59:59 2004
```

証明書パスワード

デジタル証明書はそれぞれパスワードで保護されています。証明書管理コマンドで行われるオペレーションの多くでは、オペレーションを行う前にパスワードを入力する必要があります。

パスワードの入力が必要なオペレーションは次のとおりです。

- Delete
- Import
- Export
- Enroll

（注） enroll オペレーションの場合、デジタル証明書を保護するパスワードは、サーバ証明書用に入力するオプションのチャレンジ パスワードとは別のパスワードです。

コマンドの完了に必要なパスワードの入力を求められます。パスワードを入力し、パスワードを再度確認してからでないと、コマンドを実行できません。パスワードが承認されない場合は、コマンドを再入力する必要があります。

証明書で VPN 接続を確立する場合は、証明書パスワードも必要です。

すべてのパスワードの最大長は英数字 32 文字で、大文字と小文字を区別します。

証明書タグ

証明書タグは、一意の証明書それぞれの ID です。証明書ストアに追加された証明書にはそれぞれ、証明書タグが割り当てられています。enroll オペレーションが完了していなくても、このオペレーションで証明書タグが生成されます。

一部の証明書管理オペレーションでは、オペレーションを行う前に証明書タグ引数を入力しなければなりません。証明書タグが必要なオペレーションを表 9-1 に示します。**list** オペレーションを使用して証明書タグを見つけます。

証明書タグ引数を入力するには、**-ct** コマンドの後に、オペレーションの隣に **-ct *Cert #*** と示しているように証明書 ID を指定します。

次の例は、必須証明書タグのある **view** コマンドを示しています。

```
cisco_cert_mgr -U -op view -ct 0
```

オペレーションが **view** の場合、証明書タグは **0** です。

-ct 引数と証明書タグを入力しない場合は、コマンド ラインでそれらを入力するよう求められます。無効な証明書タグを入力すると、コマンド ラインでは証明書ストアのすべての証明書タグが示され、再度、証明書タグを入力するよう求められます。

証明書管理オペレーション

最低限のコマンド ライン引数に続く、コマンド ラインの証明書管理オペレーションをすべて示します。有効なオペレーション文字列により、ストアのデジタル証明書をリスト、表示、確認、削除、エクスポート、インポート、および登録できます。

list オペレーションを使用した証明書管理コマンドの例とサンプル出力を次に示します。

```
cisco_cert_mgr -U -op list

cisco_cert_mgr Version 3.0.7

        Cert #          Common Name
          0             Fred Flinstone
          1             Dino
```

表 9-1 では、証明書管理コマンドで使用できるオペレーションを説明しています。

表 9-1　cert_mgr コマンドのパラメータ

パラメータ	説明
list	証明書ストアにある証明書をすべてリストします。リストの証明書はそれぞれ、一意の証明書タグ（*Cert #*）で識別されます。
view -ct *Cert #*	指定された証明書を表示します。証明書タグを入力する必要があります。
verify -ct *Cert #*	指定された証明書が有効なことを確認します。証明書タグを入力する必要があります。 証明書が確認されると、「Certificate *Cert #* verified」というメッセージが表示されます。 何らかの理由で証明書の確認に失敗すると、「Certificate *Cert #* failed verification」というメッセージが表示されます。このメッセージの後に、失敗の理由を示すテキスト文字列が続きます。

表 9-1　cert_mgr コマンドのパラメータ （続き）

パラメータ	説明
delete -ct *Cert #*	指定された証明書を削除します。証明書タグを入力する必要があります。
export -ct *Cert #* **-f** *filename*	特定された証明書を証明書ストアから指定のファイルへエクスポートします。証明書タグとファイル名を入力する必要があります。いずれか一方でも省略すると、コマンド ラインでそれらを入力するよう求められます。 宛先のフル パスを入力する必要があります。ファイル名のみ入力した場合、ファイルは作業ディレクトリに格納されます。 **証明書のエクスポート** 主に、証明書と秘密キーをバックアップしたり、それらを別のシステムに移行したりするために証明書をエクスポートします。証明書をエクスポートすると、そのコピーが作成されています。 証明書は、別の Cisco VPN クライアントでのみインポートできる、シスコ独自の形式でエクスポートされます。
import -f *filename*	指定のファイルから証明書ストアに証明書をインポートします。 このオペレーションには 2 種類のパスワードが必要です。（管理者により割り当てられた）ファイルを保護するパスワードと、証明書を保護するために選択するパスワードです。 証明書の形式は次のいずれかで、Windows VPN クライアントが証明書をインポートできるよう秘密キーが含まれている必要があります。 • PKCS#12 (.PFX) • PKCS#7 (P&B) • X.509 (.CER)
enroll **-cn** *common_name* **-ou** *organizational_unit* **-o** *organization* **-st** *state* **-c** *country* **-e** *email* **-ip** *IP_Address* **-dn** *domain_name* **-caurl** *url_of _CA* **-cadn** *domain_name* **[-chall** *challenge_phrase***]**	ユーザ証明書のみ対象です。 ネットワーク経由で認証局（CA）に登録することで証明書を取得します。 コマンド ラインにキーワードを 1 つずつ入力します。 詳細については、「証明書の登録」を参照してください。 管理者または CA からチャレンジ フレーズを取得できます。

表 9-1　cert_mgr コマンドのパラメータ （続き）

パラメータ	説明
enroll_file **-cn** *common_name* **-ou** *organizational_unit* **-o** *organization* **-st** *state* **-c** *country* **-e** *email* **-ip** *IP_Address* **-dn** *domain_name* **-f** *filename* **-enc [base64 | binary]**	ユーザ証明書のみ対象です。 CA に電子メールで送信するか、Web ページ フォームにペーストできる登録要求ファイルを生成します。CA が証明書を生成したら、**import** オペレーションを使用して証明書をインポートする必要があります。 詳細については、「証明書の登録」を参照してください。
enroll_resume -E -ct *Cert #*	ユーザ証明書またはルート証明書ではこのオペレーションは使用できません。 中断されたネットワーク登録を再開します。**-E** 引数および証明書タグを入力する必要があります。
changepassword -ct *Cert #*	指定されたデジタル証明書のパスワードを変更します。証明書タグを入力する必要があります。 現在のパスワードを入力してから、新しいパスワードを選択し、確認する必要があります。

証明書の登録

認証局（CA）は、ユーザが要求している本人であることを確認するため、ユーザにデジタル証明書を発行する信頼された組織です。証明書登録オペレーションにより、ネットワーク上の CA または登録要求ファイルから証明書を取得できます。

3 種類の証明書登録オペレーションがあります。

- **enroll** オペレーションにより、ネットワークで CA に登録することで証明書を取得できます。CA の URL、CA のドメイン名、および通常名を入力する必要があります。
- **enroll_file** オペレーションは、CA に電子メールで送信するか、Web ページ フォームに掲載できる登録要求ファイルを生成します。ファイル名、通常名、および符号化タイプを入力する必要があります。

  enroll オペレーションと enroll_file オペレーションでは、追加情報を提供するためにキーワードを指定できます（表 9-2 を参照）。
- **enroll_resume** オペレーションは、中断されたネットワーク登録を再開します。**-E** 引数および証明書タグを入力する必要があります。証明書タグを見つけるには、**list** オペレーションを使用します。

登録オペレーション

登録オペレーションを使用するには、certificate manager コマンド、enroll オペレーション、および関連するキーワードをコマンド ラインに入力します。

- 次に、通常名（-cn）、CA の URL（-caurl）、および CA のドメイン名（-cadn）に必要最小限のキーワードを指定した enroll コマンドの例を示します。

```
cisco_cert_mgr -U -op enroll -cn Ren Hoek -caurl
http://172.168.0.32/certsrv/mscep/mscep.dll -cadn nobody.fake
```

- 次に、ファイル名（-f）、通常名（-cn）、および符号化タイプ（-enc）に必要最小限のキーワードを指定した enroll_file コマンドの例を示します。

```
cisco_cert_mgr -U -op enroll_file -f filename -cn Ren Hoek -enc base64
```

- 次に、必要最小限の引数と追加のキーワードを指定した enroll_file コマンドの例を示します。

```
cisco_cert_mgr -U -op enroll_file -f filename -cn Ren Hoek -ou Customer Service -o
Stimpy, Inc, -st CO -c US -e ren@fake.fake -ip 10.10.10.10 -dn fake.fake -enc binary
```

- 次に、enroll_resume コマンドの例を示します。

```
cisco_cert_mgr -E -op enroll_resume -ct 4
```

表 9-2 は、enroll、enroll_file、enroll_resume の各オペレーションのオプションを示します。

表 9-2　登録オペレーションのキーワード

パラメータ	説明
-cn *common_name*	証明書の通常名です。
-ou *organizational_unit*	証明書の組織ユニットです。
-o *organization*	証明書の組織です。
-st *state*	証明書の状態です。
-c *country*	証明書の国です。
-e *email*	証明書のユーザの電子メール アドレスです。
-ip *IP_Address*	ユーザのシステムの IP アドレスです。
-dn *domain_name*	ユーザのシステムの FQDN です。
-caurl *url_of_CA*	CA の URL またはネットワーク アドレスです。
-cadn *domain_name*	CA のドメイン名です。
[-chall *challenge_phrase* **]**	管理者または CA からチャレンジ フレーズを取得できます。
-enc [base64 | binary]	出力ファイルの符号化を選択します。デフォルトは base64 です。 • **base64** は、テキスト形式であるため表示できる ASCII 符号化 PKCS10 ファイルです。テキストを CA の Web サイトへカット アンド ペーストする場合はこのタイプを選択します。 • **binary** は base-2 PKCS10（秘密キー暗号化規格）ファイルです。binary 符号化ファイルは表示できません。

登録のトラブルシューティング時のヒント

enroll オペレーションまたは enroll_file オペレーションを使用したユーザ証明書の登録要求で、ユーザ証明書ではなく CA 証明書が生成される場合は、CA は一部の目立った命名情報を上書きしている可能性があります。これは、CA の設定に問題があるか、CA が登録要求に応答する方法に制限があるために発生している可能性があります。

VPN クライアントについて CA により生成された証明書を要求したユーザ証明書と認識するため、登録要求の通常名と件名は CA により生成された証明書と一致する必要があります。一致しない場合は、VPN クライアントは要求どおり新しいユーザ証明書をインストールしません。

この問題がないかどうか確認するには、VPN クライアント上の登録要求を表示し、CA からの証明書のビューで、通常名と件名の行を比較します。それらが一致していない場合は、CA はクライアント要求からの情報を上書きしています。

この問題を回避するには、無効な証明書を例として使用し、CA 証明書の出力と一致する登録要求を作成します。

（注） CA の証明書に複数の部門（複数の ou フィールド）が入っている場合は、部門フィールド間にプラス記号（+）を使用して、VPN クライアント登録要求に複数の部門を追加できます。