



## デジタル証明書の管理

この章では、CLI (コマンド行インターフェイス) を使用して、証明書ストア内の Cisco VPN Client 用デジタル証明書を管理する方法について説明します。証明書ストアとは、デジタル証明書が保存されているローカルファイルシステム内の保存場所のことです。VPN Client では、Cisco ストア方式を採用しています。

この章の構成は、次のとおりです。

- [証明書キーワードの設定 \(P. 5-1\)](#)
- [証明書のコマンド構文 \(P. 5-2\)](#)
- [証明書の内容 \(P. 5-3\)](#)
- [証明書パスワード \(P. 5-4\)](#)
- [証明書タグ \(P. 5-4\)](#)
- [証明書の管理オペレーション \(P. 5-5\)](#)
- [証明書の登録 \(P. 5-7\)](#)

### 証明書キーワードの設定

認証に証明書を使用するには、証明書に適用するすべてのキーワードをユーザプロファイルに正しく設定する必要があります。次のキーワードの設定値を確認してください。

- `AuthType = 3` (証明書による認証)
- `CertStore = 1` (Cisco 証明書ストア)
- `CertName = Common Name` (これは、証明書に入力する一般名 (CN) と同じでなければなりません。)

ユーザプロファイルでのパラメータの設定については、[第 3 章「ユーザプロファイル」](#)を参照してください。

## 証明書のコマンド構文

デジタル証明書の管理は、CLI を使用して行われます。

証明書の管理には、次の 2 通りの方法で CLI を実行します。

- 標準 UNIX シェル。ある所定コマンドに対して、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。ある所定コマンドに対して、最小識別単位の引数（たとえば、-U）を入力すると、残りの情報に対するプロンプトが表示されます。

コマンド行に入力する最小識別単位の引数の基本形式は、次のとおりです。

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

各引数の意味は、次のとおりです。

- U は、ユーザ証明書または個人証明書に適用されます。  
-U フラグは、証明書管理コマンドのすべてのオペレーションで使用できます。ただし、enroll\_resume を除きます。
- R は、ルート証明書または認証機関（CA）証明書に適用されます。  
-R フラグは、list、view、verify、delete、export、import、および change password の各オペレーションで使用できます。
- E は、証明書の登録に適用されます。  
-E フラグは、list および delete のオペレーションのみで使用できます。また、enroll\_resume オペレーションを使用してこの -E フラグを指定する必要があります。

証明書に対するオペレーションは、-op 引数の後に入力します。証明書の管理コマンドに対する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は、「[証明書の管理オペレーション](#)」(P. 5-5) を参照してください。

## 証明書の内容

ここでは、デジタル証明書を構成する各種の情報について説明します。

デジタル証明書には、一般的に、次の情報が含まれています。

- Common name (一般名): 所有者の名前 (通常、姓と名の両方)。このフィールドにより、PKI (Public Key Infrastructure) 内の所有者が識別されます。
- Department (部門): 所有者の部門。このフィールドは、Organizational unit (組織単位) と同じです。
  - VPN 3000 Concentrator に接続する場合、このフィールドは接続先の Concentrator で所有者に設定されている **Group Name** と一致する必要があります。
  - VPN 5000 Concentrator に接続する場合、このフィールドは接続先の Concentrator で設定されている **VPNGroup-groupname** と一致する必要があります。
- Company (会社): 証明書を使用している所有者が所属する会社。このフィールドは、Organization (組織) と同じです。
- State (都道府県): 証明書を使用している所有者が居住する都道府県 (米国では州)。
- Country (国): 所有者のシステムが設置されている国の 2 文字の国別コード。
- Email: 証明書の所有者の E メールアドレス。
- Thumbprint (捺印): 証明書のすべての内容の MD5 ハッシュ。この Thumbprint は、証明書の信頼性を確認する手段の一つです。たとえば、発行元 CA に連絡する場合、この ID を使用して証明書が正しいものであることを証明できます。
- Key size (鍵サイズ): 署名鍵ペアのサイズ (ビット数)。
- Subject (サブジェクト): 証明書の所有者の完全修飾ドメイン名 (FQDN)。このフィールドにより、証明書の所有者が LDAP と X.500 ディレクトリの照会に使用できる形式で固有に識別されます。一般的な Subject には、次のフィールドが含まれます。
  - common name (cn; 一般名)
  - organizational unit または department (ou; 組織単位または部門)
  - organization または company (o; 組織または会社)
  - locality、city、または town (l; 市区町村)
  - state または province (st; 都道府県)
  - country (c; 国)
  - e-mail address (e; E メールアドレス)

証明書によっては、前述以外の項目が Subject に含まれている場合があります。

- Serial number (シリアル番号): 証明書失効リスト (CRL) で証明書の有効性の追跡に使用される固有の ID。
- Issuer (発行元): 証明書の提供元の FQDN。
- Not before (有効期間の開始): 証明書が有効になる開始日。
- Not after (有効期間の終了): 証明書が有効である最終日。

次の出力例は、デジタル証明書に含まれている各種の情報を示しています。

```
Common Name: Fred Flinstone
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

各デジタル証明書は、パスワードで保護されています。証明書の管理コマンドで実行するほとんどのオペレーションでは、オペレーションの実行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 (削除)
- import (インポート)
- export (エクスポート)
- enroll (登録)



(注) enroll オペレーションの場合、デジタル証明書を保護するためのパスワードは、サーバ証明書に入力するオプションのチャレンジパスワードとは異なります。

コマンドの実行に必要なパスワードを入力するようにプロンプトが表示されます。コマンドを実行する前に、パスワードを入力し、もう一度入力してそのパスワードを確認します。パスワードが受け入れられない場合は、コマンドを入力し直す必要があります。

VPN 接続を証明書付きで確立する際は、証明書パスワードも入力してください。

すべてのパスワードは、最長 32 文字の英数字で、大文字と小文字の区別があります。

## 証明書タグ

証明書タグとは、証明書ごとに固有の ID です。証明書ストアに追加された各証明書には、証明書タグが割り当てられます。enroll オペレーションでは、オペレーションが完了しない場合でも証明書タグが生成されます。

一部の証明書の管理オペレーションでは、オペレーションの実行前に証明書タグ引数を入力する必要があります。証明書タグが必要なオペレーションは、表 5-1 に記述されています。使用する証明書タグを検索するには、list オペレーションを使用します。

証明書タグ引数を入力するには、-ct コマンドの後に証明書 ID を指定します。オペレーションの後に -ct Cert # (証明書 ID) のように入力します。

次の例は、view コマンドと必要な証明書タグを示しています。

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

ここでのオペレーションは view で、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、コマンド行に入力するようにプロンプトが表示されます。無効な証明書タグを入力した場合、コマンド行に証明書ストアのすべての証明書が表示され、証明書タグを再度入力するようにプロンプトが表示されます。

## 証明書の管理オペレーション

最小識別単位のコマンド行引数（たとえば、-U）に続いて、証明書の管理オペレーションをコマンド行に入力します。有効なオペレーション文字列を使用して、ストア内のデジタル証明書の list（一覧表示）、view（表示）、verify（確認）、delete（削除）、export（エクスポート）、import（インポート）、および enroll（登録）の各オペレーションを実行することができます。

次の例は、証明書の管理コマンドと list オペレーション、またその出力を示しています。

```
cisco_cert_mgr -U -op list

cisco_cert_mgr Version 3.0.7

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

表 5-1 では、証明書の管理コマンドに使用可能なオペレーションについて説明します。

表 5-1 cert\_mgr コマンドのパラメータ

パラメータ	説明
list	証明書ストア内のすべての証明書を一覧で表示します。各証明書は、固有の証明書タグ (Cert #) で識別されます。
view -ct Cert #	指定した証明書を表示します。証明書タグを入力してください。
verify -ct Cert #	指定した証明書が有効であるかどうかを確認します。証明書タグを入力してください。  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が失敗した場合は、「Certificate Cert # failed verification」というメッセージが表示されます。このメッセージに続いて、失敗の理由を示す文字列が表示されます。
delete -ct Cert #	指定した証明書を削除します。証明書タグを入力してください。
export -ct Cert # -f filename	特定の証明書を証明書ストアから指定したファイルに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。どちらかを入力しないと、コマンド行に入力するようにプロンプトが表示されます。  宛先の完全パスを入力する必要があります。ファイル名だけを入力すると、そのファイルは作業ディレクトリに置かれます。
import -f filename	証明書を指定したファイルから証明書ストアにインポートします。  import オペレーションには、ファイルを保護するパスワード（管理者が指定）と、証明書を保護するパスワード（ユーザが指定）の2つの異なるパスワードが必要です。

表 5-1 cert\_mgr コマンドのパラメータ ( 続き )

パラメータ	説明
<b>enroll</b> -cn <i>common_name</i> -ou <i>organizational_unit</i> -o <i>organization</i> -st <i>state</i> -c <i>country</i> -e <i>email</i> -ip <i>IP_Address</i> -dn <i>domain_name</i> -caurl <i>url_of_CA</i> -cadn <i>domain_name</i> [-chall <i>challenge_phrase</i> ]	<p>ユーザ証明書のみ適用されます。</p> <p>ネットワーク上の認証機関 ( CA ) に登録して、証明書を取得します。</p> <p>コマンド行にそれぞれのキーワードを個別に入力します。</p> <p>詳細は、「<a href="#">証明書の登録</a>」( P. 5-7 ) を参照してください。</p> <p>チャレンジフレーズ ( challenge phrase ) は、管理者または CA から入手できます。</p>
<b>enroll_file</b> -cn <i>common_name</i> -ou <i>organizational_unit</i> -o <i>organization</i> -st <i>state</i> -c <i>country</i> -e <i>email</i> -ip <i>IP_Address</i> -dn <i>domain_name</i> -f <i>filename</i> -enc [ <i>base64</i>   <i>binary</i> ]	<p>ユーザ証明書のみ適用されます。</p> <p>登録要求ファイルを生成します。このファイルは E メールで CA に送信したり、Web ページのフォームで送信したりすることができます。CA が証明書を生成する場合は、ユーザが <b>import</b> オペレーションを使用してその証明書をインポートする必要があります。</p> <p>詳細は、「<a href="#">証明書の登録</a>」( P. 5-7 ) を参照してください。</p>
<b>enroll_resume -E -ct Cert #</b>	<p>このオペレーションは、ユーザ証明書またはルート証明書には使用できません。</p> <p>中断されていたネットワーク登録を再開します。-E 引数と証明書タグを入力する必要があります。</p>
<b>changepassword -ct Cert #</b>	<p>指定し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。</p> <p>現在のパスワードを入力してから、新しいパスワードを入力し、確認する必要があります。</p>

## 証明書の登録

認証機関 (CA) は、ユーザにデジタル証明書を発行し、ユーザが申告通りの個人であることを確認する手段を提供する信頼できる機関です。証明書の登録オペレーションを使用すると、証明書をネットワーク上の認証機関 (CA) から、または登録要求ファイルから取得できます。

証明書の登録オペレーションには、次の3つのタイプがあります。

- **enroll** オペレーションを使用すると、ネットワーク上で CA に登録して、証明書を取得できます。CA の URL、CA のドメイン名、および一般名 (CN) を入力する必要があります。
- **enroll\_file** オペレーションを使用すると、登録要求ファイルを生成できます。このファイルは、Eメールで CA に送信したり、Web ページのフォームで送信したりすることができます。ファイル名、一般名、および使用するエンコーディングタイプを入力する必要があります。  
enroll オペレーションおよび enroll\_file オペレーションでは、キーワードを使用してさらに追加情報を指定することができます。これらのキーワードは、表 5-2 に記述されています。
- **enroll\_resume** オペレーションを使用すると、中断されていたネットワーク登録を再開できます。-E 引数と証明書タグを入力する必要があります。使用する証明書タグを検索するには、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、証明書の管理コマンド、および enroll オペレーションと対応するキーワードをコマンド行に入力します。

- 次の例は、enroll コマンドと必須の一般名 (-cn)、CA の URL (-caurl)、および CA のドメイン名 (-cadn) の各キーワードを示しています。

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

- 次の例は、enroll\_file コマンドと必須のファイル名 (-f)、一般名 (-cn)、およびエンコーディングタイプ (-enc) の各キーワードを示しています。

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

- 次の例は、enroll\_file コマンドと最小識別単位の引数を指定した追加のキーワードを示しています。

```
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
```

- 次の例は、enroll\_resume コマンドを示しています。

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

表 5-2 では、enroll、enroll\_file、および enroll\_resume の各オペレーションに使用するオプションについて説明します。

表 5-2 登録オペレーションのキーワード

パラメータ	説明
-cn <i>common_name</i>	証明書に記載される一般名です。
-ou <i>organizational_unit</i>	証明書に記載される組織単位です。
-o <i>organization</i>	証明書に記載される組織です。
-st <i>state</i>	証明書に記載される都道府県です。
-c <i>country</i>	証明書に記載される国です。

表 5-2 登録オペレーションのキーワード (続き)

パラメータ	説明
<code>-e email</code>	証明書に記載されるユーザの E メール アドレスです。
<code>-ip IP_Address</code>	ユーザのシステムの IP アドレスです。
<code>-dn domain_name</code>	ユーザのシステムの FQDN です。
<code>-caurl url_of_CA</code>	CA の URL またはネットワーク アドレスです。
<code>-cadn domain_name</code>	CA のドメイン名です。
<code>[-chall challenge_phrase]</code>	チャレンジフレーズは、管理者または CA から入手できます。
<code>-enc [ base64   binary ]</code>	出力ファイルのエンコーディングを選択します。デフォルトは base64 です。 <ul style="list-style-type: none"> <li>base64 は、ASCII エンコード PKCS10 ファイルです。このファイルはテキスト形式のため、表示することができます。テキストを CA の Web サイトにカットアンドペーストしたい場合に、このタイプを選択してください。</li> <li>binary は、base-2 PKCS10( Public-Key Cryptography Standards ) ファイルです。バイナリ エンコード ファイルは表示することができません。</li> </ul>

### 登録に関するトラブルシューティングのヒント

enroll オペレーションまたは enroll\_file オペレーションのいずれかを使用したユーザ証明書の登録要求で、ユーザ証明書の代わりに CA 証明書が生成される場合、この CA が一部の識別名情報を変更していることがあります。これは、CA の構成上の問題、または登録要求への CA の応答方法における制限により発生します。

登録要求の一般名およびサブジェクト情報は、CA が生成した証明書と一致し、VPN Client が要求したユーザ証明書と同じであることが確認されなければなりません。情報が一致しない場合、VPN Client が要求したユーザ証明書として新規のユーザ証明書はインストールされません。

この問題を検討するには、VPN Client で登録要求を表示して、その一般名とサブジェクトを CA からの証明書と比較します。情報が一致しない場合は、CA が Client 要求の情報を変更しています。

この問題を解決するには、無効な証明書をサンプルとして使用し、CA 証明書の出力と一致する登録要求を作成します。



(注)

CA 証明書に複数の部門 (複数の ou フィールド) が含まれている場合、VPN Client の登録要求に複数の部門を追加できます。この場合、部門とフィールドの間にプラス記号 (+) を使用します。