



デジタル証明書の管理

この章では、CLI (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、ローカル ファイル システム内の、デジタル証明書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。

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、証明書に入力する通常名 (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。

証明書を管理するには、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、残りの情報の入力を求めるプロンプトが表示されます。

コマンドライン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 オペレーションおよび delete オペレーションと共にのみ使用できます。また、このフラグは、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。

指定した証明書に対するオペレーションを、-op 引数の後に入力します。証明書の管理コマンドでの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 (通常名): 所有者の名前 (通常、姓と名の両方)。このフィールドで、公開キーインフラストラクチャ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 (組織ユニット) 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している都道府県 (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 (E メール): 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 に問い合わせれば、このハッシュ ID と比較してこの証明書が正当かどうかを確認できます。
- 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)。このフィールドで、証明書の所有者が LDAP と X.500 ディレクトリのクエリー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; 通常名)
 - organizational unit または department (ou; 組織ユニットまたは部門)
 - 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、上記以外の項目が Subject に含まれている場合があります。

- Serial number (シリアル番号): Certificate Revocation List (CRL) 上で証明書の有効性をトラッキングする際に使用される固有の ID。
- Issuer (発行元): 証明書を発行した機関の完全修飾識別名 (FQDN)。
- Not before (有効期間の開始): 証明書の発効日。
- Not after (有効期間の終了): 証明書の終了日。この日の翌日から無効になります。

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、パスワードを一度入力してから、確認のためにもう一度入力します。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 に示されています。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、コマンドライン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、コマンドライン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ライン引数（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ラインに入力します。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で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表示します。各証明書は、固有の証明書タグ（ <i>Cert #</i> ）で識別されます。
view -ct <i>Cert #</i>	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 <i>Cert #</i>	指定された証明書が有効かどうかを確認します。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 <i>Cert #</i> 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 <i>Cert #</i> 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 <i>Cert #</i>	指定し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 <i>Cert #</i> -f <i>filename</i>	特定の証明書を証明書ストアから指定され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、コマンドライン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 <i>filename</i>	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
enroll -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。コマンドライン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、「証明書の登録」(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>
enroll_file -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 [base64 binary]	<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できます。CA が証明書を生成する場合は、ユーザが import 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、「証明書の登録」(P. 5-7) を参照してください。</p>
enroll_resume -E -ct <i>Cert #</i>	<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>
changepassword -ct <i>Cert #</i>	<p>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。</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 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、証明書をネットワーク上で CA に登録して取得できます。CA の URL、CA のドメイン名、および通常名 (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できます。ファイル名、通常名、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追加情報を指定できます。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 オペレーションと関連するキーワードをコマンドラインに入力します。

- 次の例は、通常名 (-cn)、CA の URL (-caurl) および CA のドメイン名 (-cadn) の必須のキーワードが指定された enroll コマンドを示しています。

```
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、ファイル名 (-f)、通常名 (-cn) およびエンコーディングタイプ (-enc) の必須のキーワードが指定された enroll_file コマンドを示しています。

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

- 次の例は、必須の最小識別単位の引数と追加のキーワードが指定された enroll_file コマンドを示しています。

```
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通常名です。
-ou <i>organizational_unit</i>	証明書に記載される組織ユニットです。
-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。
-e <i>email</i>	証明書に記載されるユーザの E メール アドレスです。
-ip <i>IP_Address</i>	ユーザのシステムの IP アドレスです。
-dn <i>domain_name</i>	ユーザのシステムの FQDN です。
-caurl <i>url_of_CA</i>	CA の URL またはネットワーク アドレスです。
-cadn <i>domain_name</i>	CA のドメイン名です。
[-chall <i>challenge_phrase</i>]	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。
-enc [base64 binary]	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"> base64 は、ASCII 文字に符号化された PKCS10 ファイルです。このファイルはテキスト形式なので、表示可能です。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。 binary は、base-2 PKCS10 (Public-Key Cryptography Standards) ファイルです。バイナリ符号化されたファイルは表示できません。

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、CA が識別名情報の一部を変更した可能性があります。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。

登録要求の通常名およびサブジェクト情報は、要求されたユーザ証明書に間違いがないことが確認できるように CA が VPN Client に対して生成する証明書のものと同じでなければなりません。情報が一致しない場合、VPN Client では、新規のユーザ証明書が要求したユーザ証明書としてインストールされません。

この問題について確認するには、VPN Client で登録要求を表示して、共通名とサブジェクトを CA からの証明書のものと比較します。情報が一致しない場合は、CA が Client から要求された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、部門フィールド間にプラス記号 (+) を使用します。