CHAPTER 7

Cisco CNS Configuration Engine の SSL セキュリティ

この章では、CNS エージェントに対応した Cisco IOS デバイスと Cisco CNS Configuration Engine 間の 128 ビット Secure Sockets Layer（SSL）暗号化通信のセットアップとコンフィギュレーションについて説明します。

この章の内容は、次のとおりです。

CNS エージェントと Configuration Engine のセキュリティ

Cisco Configuration Engine サーバと CNS エージェント対応デバイス（ルータ）間の通信には、セキュリティとして次の 3 つの基本的な機能が組み込まれています。

- 識別：一意の CNS エージェント ID。デバイスが Cisco Configuration Engine サーバと通信するためには、少なくとも CNS エージェント ID が必要です。
- 認証：一意の CNS パスワード。認証機能は、通信ハンドシェイクの一環として CNS エージェントが Cisco Configuration Engine サーバに提示する CNS パスワードから成ります。
- 暗号化：128 ビット SSL / Shared PKI SSL トラスト ポイント証明書。SSL プロトコル。暗号化機能は、業界標準の SSL プロトコルから成ります。これにより、CNS エージェント デバイスと Cisco Configuration Engine サーバ間の通信が保護されます。

デバイス識別は必須機能であるのに対し、認証と暗号化はオプション機能です。2 つのオプション機能のうち、一方または両方をいつでも有効にできます。暗号化には認証は必要なく、認証には暗号化は必要ありません。

各セキュリティ機能は、Cisco Configuration Engine サーバと CNS エージェント デバイスのどちらにおいても、別々に設定および処理されます。

CNS ID、パスワード認証、SSL 暗号化

CNS Configuration Engine には、CPE デバイス識別、認証、および暗号化の設定があります。これらの機能はそれぞれ、CNS Configuration Engine、および CNS Configuration Engine と通信する CNS CPE デバイスのどちらにおいても、別々に設定および処理されます。

CNS エージェントに対応した CPE デバイスが CNS Configuration Engine サーバと通信するためには、CPE デバイス CNS エージェント ID が必要です。認証機能は、CNS エージェント対応デバイスが CNS サーバに提示する CNS パスワードから成ります。暗号化を選択した場合は、通信シーケンスの最初に CNS エージェントと CNS Configuration Engine 間で通信ネゴシエーションが行われます。SSL 暗号化が成功した場合に限り、CNS 識別および CNS 認証プロトコルが通過します。CNS Configuration Engine サーバですべてのオプションを有効にした場合は、CNS エージェント CPE デバイスが各オプションを無事通過する必要があります。そうでなければ、デバイスはどのような目的でもサーバに接続できず、拒否されます。

次のセクションでさらに詳しく説明します。

- 「識別」（P.7-2）
- 「認証」（P.7-3）
- 「暗号化」（P.7-4）

識別

これは必須の設定です。CNS 対応 CPE デバイス（ルータ）が CNS Configuration Engine との通信を開始するためには、事前に各 CPE デバイスに一意の ID を割り当てておく必要があります。1 台のルータに複数の CNS エージェントを設定できます。各エージェントには一意の ID を割り当てる必要があります。

CNS エージェント デバイスで CNS エージェント ID を設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

cns id string < *一意の文字列*>

cns id string < *イベント エージェントの一意の文字列*> **event**

cns id string < *イメージ エージェントの一意の文字列*> **image**

例

```
Router#enable
Router#configure terminal
Router(config)#cns id string my-asset-tag1
Router(config)#cns id string my-asset-tag1 event
Router(config)#cns id string my-asset-tag1 image
Router(config)#end
```

Cisco Configuration Engine サーバでユーザ インターフェイスから新しいデバイス オブジェクトをセットアップするとき、管理者はこれらの CNS エージェント ID を指定する必要があります。CNS エージェント デバイスとその ID が Cisco Configuration Engine サーバで設定されていない限り、エージェントからサーバへの接続は受け入れられません。

認証

認証機能は、通信ハンドシェイクの一環として CNS エージェント デバイスが Cisco Configuration Engine サーバに提示する CNS パスワードから成ります。CNS パスワードは次のように使用されます。

- CNS Configuration Engine サーバで、CNS Configuration Engine 管理者が知っているグローバルなワンタイム パスワードとして割り当てられます。
- デバイスが CNS Configuration Engine サーバへの接続を試行する前に、デバイス管理者がこのワンタイム パスワードを CNS エージェント対応デバイスのコンフィギュレーションに設定します。

CNS Configuration Engine の Web ユーザ インターフェイスには、[Devices] メニューの下に [Resync Device] というオプション ボタンがあります。管理者はこのオプション ボタンを使用して、任意の CPE デバイスの一意のパスワードをグローバルなワンタイム パスワードとしてリセットできます。その後、CNS エージェント デバイスが Cisco Configuration Engine サーバへの接続を試行する前に、管理者はこのワンタイム パスワードを CNS エージェント デバイスのコンフィギュレーションに入力する必要があります。デバイスがサーバと同期していない場合は、デバイスをリセットできます。そうすると、接続の成功時にサーバが新しいランダム値を再割り当てします。

CNS Configuration Engine のセットアップ プログラムの次のプロンプトは、サーバが CPE デバイスからの CNS パスワードを待つよう設定します。

```
Authentication settings:
------------------------
Cisco IOS Devices are normally authenticated before being allowed to connect to the Event
Gateway/Config Server. Disabling authentication will increase security risk.
Enable authentication (y/n)? [n] y
```

Cisco Configuration Engine サーバのセットアップ時に、管理者はこの CNS パスワードをグローバルなワンタイム パスワードとして割り当てる必要があります。その後、CNS エージェント デバイスが Cisco Configuration Engine サーバへの接続を試行する前に、管理者はこのワンタイム パスワードを CNS エージェント デバイスのコンフィギュレーションに入力する必要があります。

Cisco Configuration Engine サーバのセットアップ プログラムで「Enable authentication」のプロンプトに対して y と答えると、認証が有効になります（「認証の設定」（P.2-8）を参照）。こうすると、Cisco Configuration Engine サーバが CNS エージェント デバイスからのパスワードを待つよう設定されます。認証を有効にした後で、管理者は Cisco Configuration Engine のユーザ インターフェイスを使用して実際のパスワードを再設定する必要があります。パスワードを設定するには、CNS Configuration Engine Web UI のメニュー [Tools] > [Security Mgr] > [BootStrap] を使用します。

このパスワードは、CPE デバイスから CNS Configuration Engine サーバへの初期接続に使用できます。各 CPE デバイスの識別と認証が成功したら、CNS Configuration Engine サーバはパスワードを生成し、CPE デバイスにランダムなパスワードを自動的に割り当てます。

（注）　random cns password コマンドは、セキュリティを高めるために意図的に隠されています。この cns password コマンドは初期パスワードの設定またはリセットに使用できますが、設定後にパスワード値を表示することはできません。

CPE デバイスで CNS パスワードを設定するには、グローバル コンフィギュレーション モードで次のコマンドを入力します。

cns password <パスワード>

例

```
Router(config)# cns password fgfg123
Router(config)# end
```

暗号化

CNS エージェント対応デバイスと CNS Configuration Engine 間の CNS 通信は、128 ビット SSL プロトコルの強力暗号化を使用して暗号化できます。これにより、CNS エージェント対応デバイスと

CNS Configuration Engine 間の通信に、業界標準の SSL 暗号化

プロトコルが持つすべての利点がもたらされます。

SSL 暗号化機能に関連する CNS Configuration Engine セットアップ プログラムのプロンプトを次に示します。

```
...other prompts....
Encryption settings:
--------------------
Enable cryptographic (crypto) operation between Event Gateway(s)/Config
server and device(s) (y/n)? [n] y
Certificates already exist. Overwrite (y/n)? y
Enter certificate FTP server (hostname.domainname or IP address): cert-host.mydomain.com
Enter username used for FTP server: cnsie
Enter FTP password: ******
Re-enter FTP password: ******
Enter absolute pathname of remote key file: /tftpboot/server.key
Enter absolute pathname of remote certificate file: /tftpboot/server.cer
Enabling plaintext operation will increase security risk.
Enable plaintext operation between Config Server and devices/GUI
administration (y/n)? [y] n
Enable plaintext operation between Event Gateway and devices (y/n)? [y] n
Enter port number for https web access: [443]
...other prompts....
```

SSL ホスト通信の基礎

SSL ベースの通信に参加するためには、ホスト システムに次のものが必要です。

- 一般的な PKI 証明書サーバ（CS）、または SSL で使用するデジタル証明書の署名と発行を行う信頼された認証機関（CA）（トラストポイント）
- ホスト名
- DNS サーバ IP アドレス（名前解決）
- DNS ドメイン名（名前解決）
- 日付/時刻ゾーンの設定
- NTP 日付/時刻の更新
- SSL トラスト ポイントで署名された SSL 証明書

SSL 通信に参加するすべてのホストには、いくつかの基本的なホスト名解決機能とともに、正確な日付と時刻が設定されている必要があります。また、128 ビット SSL 輸出グレード暗号化通信を可能にする強力暗号化ベースのオペレーティング システムも必要となります。

CNS SSL 通信の 4 つのステップ

CNS エージェント、CNS Configuration Engine、および CNS エージェント SSL 暗号化機能を使用することにより、Cisco IOS デバイスと CNS Configuration Engine の間に信頼される暗号化通信チャネルを確立できます。単一の 128 ビット SSL 接続を介してすべての IOS syslog メッセージ（ファイアウォールや IDS センサのトラフィック、コンフィギュレーションの更新、統計情報の収集、デバイス検出など）の転送を暗号化できます。

CNS エージェントと CNS Configuration Engine 間の SSL 通信をセットアップするには、次の 4 つの基本ステップに従います。

ステップ 1　サーバの自己署名（ルート）証明書を取得する。配置の初期段階で CA を準備し、自己署名証明書を取得しておきます。

ステップ 2　CNS Configuration Engine の SSL 登録。

CNS Configuration Engine は自身の固有の SSL 証明書を登録し、その証明書を Cisco IOS CA サーバから取得する必要があります。CPE デバイスは SSL 接続を確立するために、CNS Configuration Engine の SSL 証明書とルート CA 署名を自身の SSL 証明書と照合します。この登録はファイルのコピーまたは端末/コンソールからのカット アンド ペーストの方法で行います。

（注）　CNS Configuration Engine のバージョン 1.3.2 および 1.4 には、SCEP プロトコル登録クライアントはありません。

ステップ 3　Cisco IOS トラストポイントを設定する。

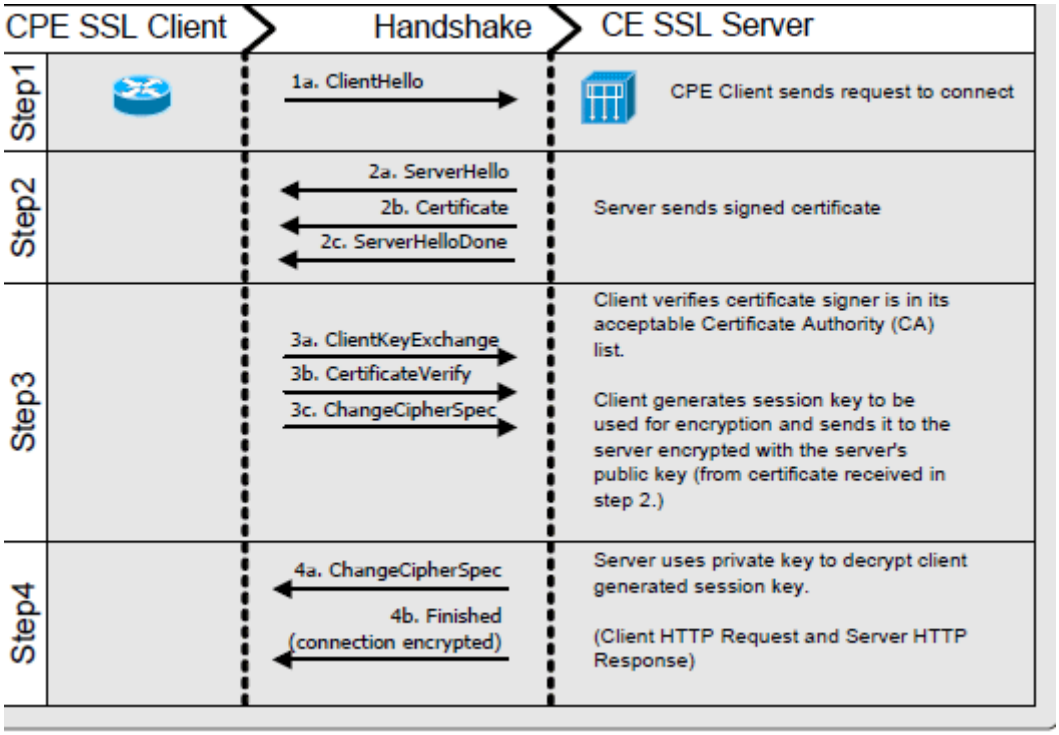
Cisco CNS エージェント CPE デバイスは、ルート CA の証明書の自己署名証明書のコピーだけを必要とします。CPE デバイスは自身の固有の証明書を登録する必要がないため、これは単に *Cisco IOS トラストポイントの設定*と呼ばれます。CNS Configuration Engine サーバ証明書の検証にも同じルート CA の自己署名証明書を使用できます。これは今日の PC Web ブラウザの機能とよく似ています。

Cisco CPE デバイスは、SSL トラストポイントの設定または CPE デバイス固有の証明書の登録に主に Cisco SCEP 登録プロトコルを利用するよう設計されています。シスコ デバイスでの SSL プロトコルの使用は 1999 ～ 2000 年に導入され、証明書登録用の SCEP プロトコルとその関連する機能は Cisco Systems Inc. と Verisign Inc. の合弁事業として開発されました。

ステップ 4　SSL を有効にする。

CNS Configuration Engine でセットアップ プログラムを再度実行し、サーバ側で暗号化を有効にします。CPE デバイスの CNS エージェントでは、encrypt キーワードを使用するコマンドを再設定する必要があります。

図 7-1　CNS 128 ビット SSL におけるクライアントとサーバのハンドシェイク



SSL 暗号化通信の実行

サーバ側で暗号化をセットアップすると、Cisco IOS デバイスと CNS Configuration Engine 間でいつでも SSL 暗号化通信を開始できます。キーワード *encrypt* を指定した IOS コマンドによって接続が試行された CNS エージェント インバウンド サービス接続はすべて、SSL で暗号化されます。

Cisco IOS v12.3(4)T 証明書サーバ

CNS Configuration Engine または SSL Cisco IOS デバイスを設定して証明書の取得やデバイス SSL トラストポイントの設定を行う前に、SSL 証明書サーバ（トラストポイント）をセットアップする必要があります。

Cisco IOS 証明書サーバは、プライマリ証明書登録プロトコルとして HTTP 上の Simple Certificate Enrollment Protocol（SCEP）をサポートします。

最近の Cisco IOS SSL クライアント デバイスは、SCEP をプライマリ証明書サーバ登録プロトコルとして使用して、自身の SSL Cisco IOS トラストポイントを設定します。CNS Configuration Engine は SCEP プロトコルまたはその他の自動登録プロトコルをサポートしていないため、手動での登録（端末からの書き込み）によって自身の SSL 証明書を登録し、その証明書を証明書サーバから取得します。

Engine の証明書登録 IOS コマンド

CNS Configuration Engine の証明書要求では、Cisco IOS CS で端末またはスクリーン ダンプからの証明書要求が受け入れられるように、次の構文が必要となります。

crypto pki server {cs-label} request pkcs10 terminal pem

Cisco IOS の証明書登録 IOS コマンド

SCEP による Cisco IOS CPE デバイスの証明書要求では、次のコマンドを使用します。

crypto pki server {cs-label} request pkcs10 url {url}

指定する URL は、Cisco IOS CPE デバイスで SCEP によるトラストポイントの設定に使用されるパスです。

Cisco IOS 証明書サーバのセットアップ

次に、IOS CS のセットアップおよびコンフィギュレーションの簡略版を示します。このうち、サーバ名と発行者名の値をご使用の値に置き換えてください。IOS 証明書サーバの詳細なセットアップについて説明するドキュメントは Cisco.com から入手できます。

```
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip http server
Router(config)#crypto pki server IOS-CA-10090
Router(cs-server)#issuer-name CN=My Company,L=San Francisco CA,C=us
Router(cs-server)#grant auto
% This will cause all certificate requests to be automatically granted.

Are you sure you want to do this? [yes/no]: yes
Router(cs-server)#no shutdown
% Once you start the server, you can no longer change some of % the configuration.
Are you sure you want to do this? [yes/no]: yes
% Generating 1024 bit RSA keys ...[OK]

Mar 13 02:15:37.029: %SSH-5-ENABLED: SSH 1.99 has been enabled
% Certificate Server enabled.
Router(cs-server)#end
```

IOS 証明書サーバの自己署名（ルート）証明書の表示

IOS 証明書サーバで CA の固有の（自己署名された）SSL 証明書を表示するには、次のコマンドを使用します。これは、この CA によって発行されたすべての SSL 証明書を認証する、デジタル署名された証明書です。

show crypto ca certificate

次の例は、ルータ プロンプトでの **crypto ca certificate** コマンドの使用方法を示します。

```
Router#show crypto ca certificates
CA Certificate
    Status: Available
    Certificate Serial Number: 01
    Certificate Usage: Signature
    Issuer:
        cn=My Company
        l=San Francisco CA
        c=us
    Subject:
        cn=My Company
        l=San Francisco CA
        c=us
    Validity Date:
        start date: 02:15:39 UTC Mar 13 2004
        end date: 02:15:39 UTC Mar 13 2007
    Associated Trustpoints: IOS-CA-10090
```

show crypto pki server

次の例は、ルータ プロンプトでの **crypto pki server** コマンドの使用方法を示します。

```
Router#show crypto pki server
Certificate Server IOS-CA-10090:
    Status: enabled, configured
    CA cert fingerprint: 7F1AEE23 9067BD38 97137AE7 24C80C37
    Granting mode is: auto
    Last certificate issued serial number: 0x1
    CA certificate expiration timer: 02:15:39 UTC Mar 13 2007
    CRL NextUpdate timer: 02:15:49 UTC Mar 20 2004
    Current storage dir: nvram:
    Database Level: Minimum - no cert data written to storage
```

IOS 証明書サーバへの登録

ここでは、IOS 証明書サーバへの登録手順について説明します。

SCEP プロトコルを使用した証明書の登録

SCEP は、すべての Cisco IOS デバイスで推奨される証明書登録方法です。SCEP 登録に関する IOS クライアントのコンフィギュレーションの例を次に示します。

```
crypto ca identity SSLrootCA
enrollment url http://myIOSCAserver.com
exit
```

端末からのコピー アンド ペーストを使用した証明書の登録

コマンド ライン登録には IOS コマンドへのアクセス権が必要です。証明書要求と応答の両方がコンソール セッション画面に出力されますが、これらはどのファイルにも保存されません。これを CNS Configuration Engine で使用するには、出力された結果を単にテキストとしてファイルにコピーして保存します。証明書を取得するには、次のコマンドを使用します。

```
Router#crypto pki server iosca request pkcs10 terminal
<<paste request>>
<<copy certificate>>
```

端末からの登録の例

次の例は、CNS Configuration Engine の証明書要求を使用する方法を示します。

（注）　証明書要求には PEM ヘッダーとフッターを付けることができます。

```
Cisco-1711#crypto pki server IOS-CA-10090 request pkcs10 terminal
% Enter Base64 encoded or PEM formatted PKCS10 enrollment request.
% End with a blank line or "quit" on a line by itself.
-----BEGIN CERTIFICATE
REQUEST----MIIDQDCCAigCAQAwgawxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MREwDwYDVQQHEwhTYW4gSm9zZTEbMBkGA1UEChMSQ2lzY28gU3lzdGVtcyBJbmMu
MSYwJAYDVQQLEx1OTVRHIENOUyBDb25maWd1cmF0aW9uIEVuZ2luZTENMAsGA1UE
AxMEb3B1czEhMB8GCSqGSIb3DQEJARYSZW1pa3VsaWNAY2lzY28uY29tMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA84y2NE0C1GY5nnubkG6u2ZYAxK7h
Qy+9UPSfeVYHE3EWuQNuZljoXOd40+/FTfeOEdhh9fsertl+wNavHXwpngDfhx59
dbRduYekAmL7kPVute1BtVB6yJJ7yWRoGW3pG5PinMPXwNQhSRZHgBVBusWtdsD/
/clo7Mly4F2vqYmSVaE0SHLR1QiJKO+0iOx9iBzGxH8S2BpfdjwBKwO2MzRFgPhV
PgjtMvNDA47DgwfcuSiO6liW1Cv/g3GgzBT/G6sWzf6ah2+kTLQq9XXim5b9J2Hf
IIniAwohSq+kHo8f/cbq+WT/BwLaU163oZXiNKUxeYBYCuzZ7GGMkRHVwQIDAQAB
oE4wGAYJKoZIhvcNAQkHMQsTCWNyaW1zb241NTAyBgkqhkiG9w0BCQIxJRMjTmV0
d29yayBNYW5hZ2VtZW50IFRlY2hub2xvZ3kgR3JvdXAwDQYJKoZIhvcNAQEEBQAD
ggEBABtrhmhJYP3iD5iencZzQr4P8bwDjtYAS4B0EpFAfeymGV5ZSKMM3pLEbac8
iVL2EbLwB1G25O24PiFOmysw60+ehmR4TR1yI3pMZ7oTn71md4a3z04GAw6o9q4u
xPEWx07LckkGdmaZAd5t9+hLrBWTq+gZmZszVkenhBPIEdDh8gN0XKM5xd9IVtio
jZNJVeXPlVxWFT/nIz+BaVolJenuqrB6wgWjMoAfvknr2v9axIf8P6j80vPSX3wU
H+JUNCYTa4hXoX8sK9xeoHpqNyvVMz6ntAgHe+JjJyfRlLxq/hnbcem83lyr2Mix
% Granted certificate:
MIIDBzCCAnCgAwIBAgIBAjANBgkqhkiG9w0BAQQFADA9MQswCQYDVQQGEwJ1czEZ
MBcGA1UEBxMQU2FuIEZyYW5jaXNjbyBDQTETMBEGA1UEAxMKTXkgQ29tcGFueTAe
Fw0wNDAzMTMwMjIzNDRaFw0wNTAzMTMwMjIzNDRaMIGsMQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxGzAZBgNVBAoT
EkNpc2NvIFN5c3RlbXMgSW5jLjEmMCQGA1UECxMdTk1URyBDTlMgQ29uZmlndXJh
dGlvbiBFbmdpbmUxDTALBgNVBAMTBG9wdXMxITAfBgkqhkiG9w0BCQEWEmVtaWt1
bGljQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPOM
tjRNAtRmOZ57m5BurtmWAMSu4UMvvVD0n3lWBxNxFrkDbmZY6FzneNPvxU33jhHY
YfX7Hq7ZfsDWrx18KZ4A34cefXW0XbmHpAJi+5D1brXtQbVQesiSe8lkaBlt6RuT
4pzD18DUIUkWR4AVQbrFrXbA//3JaOzJcuBdr6mJklWhNEhy0dUIiSjvtIjsfYgc
xsR/EtgaX3Y8ASsDtjM0RYD4VT4I7TLzQwOOw4MH3LkojupYltQr/4NxoMwU/xur
Fs3+modvpEy0KvV14puW/Sdh3yCJ4gMKIUqvpB6PH/3G6vlk/wcC2lNet6GV4jSl
MXmAWArs2exhjJER1cECAwEAAaMjMCEwHwYDVR0jBBgwFoAUUmc3z2kTZuJ3JJAW
BQGz2gYFGuQwDQYJKoZIhvcNAQEEBQADgYEAHOsmp3H2wii8NaoYV8uXsbIYyk5V
KDIpB3EX6G74b6MG0egzH+39HYJT7S7uevyPEbMg1xusJoeRmUGl0GricJcmlPUL
cqqSt+nueOpiZs0W1pwqunqYTkTy3DP1oyxSWA1Xe9sIJQXcPvppj+7KvpIvckCk
RqgVxWG1aPcBTYI=
```

（注）　PEM 形式の証明書が必要な場合は、次の PEM ヘッダーを手動で追加します。

```
-----BEGIN CERTIFICATE-----
<<hex data>>
-----END CERTIFICATE-----

Hence the issued request would end up with headers above and below it's first and last
data lines:
-----BEGIN CERTIFICATE----MIIDBzCCAnCgAwIBAgIBAjANBgkqhkiG9w0BAQQFADA9MQswCQYDVQQGEwJ1czEZ
MBcGA1UEBxMQU2FuIEZyYW5jaXNjbyBDQTETMBEGA1UEAxMKTXkgQ29tcGFueTAe
Fw0wNDAzMTMwMjIzNDRaFw0wNTAzMTMwMjIzNDRaMIGsMQswCQYDVQQGEwJVUzET
MBEGA1UECBMKQ2FsaWZvcm5pYTERMA8GA1UEBxMIU2FuIEpvc2UxGzAZBgNVBAoT
EkNpc2NvIFN5c3RlbXMgSW5jLjEmMCQGA1UECxMdTk1URyBDTlMgQ29uZmlndXJh
dGlvbiBFbmdpbmUxDTALBgNVBAMTBG9wdXMxITAfBgkqhkiG9w0BCQEWEmVtaWt1
bGljQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAPOM
tjRNAtRmOZ57m5BurtmWAMSu4UMvvVD0n3lWBxNxFrkDbmZY6FzneNPvxU33jhHY
YfX7Hq7ZfsDWrx18KZ4A34cefXW0XbmHpAJi+5D1brXtQbVQesiSe8lkaBlt6RuT
4pzD18DUIUkWR4AVQbrFrXbA//3JaOzJcuBdr6mJklWhNEhy0dUIiSjvtIjsfYgc
xsR/EtgaX3Y8ASsDtjM0RYD4VT4I7TLzQwOOw4MH3LkojupYltQr/4NxoMwU/xur
Fs3+modvpEy0KvV14puW/Sdh3yCJ4gMKIUqvpB6PH/3G6vlk/wcC2lNet6GV4jSl
MXmAWArs2exhjJER1cECAwEAAaMjMCEwHwYDVR0jBBgwFoAUUmc3z2kTZuJ3JJAW
BQGz2gYFGuQwDQYJKoZIhvcNAQEEBQADgYEAHOsmp3H2wii8NaoYV8uXsbIYyk5V
KDIpB3EX6G74b6MG0egzH+39HYJT7S7uevyPEbMg1xusJoeRmUGl0GricJcmlPUL
cqqSt+nueOpiZs0W1pwqunqYTkTy3DP1oyxSWA1Xe9sIJQXcPvppj+7KvpIvckCk
RqgVxWG1aPcBTYI=
-----END CERTIFICATE----
```

サンプル コマンドと出力

ここでは、サンプル コマンドとその出力を示します。

暗号キーと SSL 証明書要求の作成

次の手順は、CNS CE での RSA キーの生成と SSL 証明書要求の生成の基本を示します。生成された証明書は*証明書署名要求*と呼ばれます。証明書署名要求は有効な署名済み SSL 証明書の申請に使用するもので、これを元に CA から署名済み証明書が返送されます。

CNS Configuration Engine のコンソールまたは端末にログインし、ここに示す順にコマンドを入力します。

（注） サンプルのファイル名は、必要に応じて実際に使用する独自のファイル名に置き換える必要があります。ここに示す出力はテスト環境で実際に生成された OpenSSL の出力であり、ご使用の環境での出力とは少し異なる場合があります。以降のテキストでは、コマンド入力と生成された出力の両方が画面でキャプチャされたとおりに示されています。CNS Configuration Engine がインストールされていて、TCP/IP ネットワーク接続がセットアップされていることを確認してください。

RSA キーの生成

CNS Configuration Engine のコンソールまたは端末にログインし、RSA キーペアと証明書署名要求を生成するために次のコマンドを入力します。

- **% openssl genrsa -out /root/server.key 1024**

```
Generating RSA private key, 1024 bit long modulus
.................++++++
.....................................................++++++
e is 65537 (0x10001)
```

RSA キーのファイル所有権の変更

RSA キーのファイル所有権を変更するには、次のコマンドを使用します。

- **% chown -v root:root /root/server.key**

```
changed ownership of `/root/server.key' to root:root
```

- % chmod -v 400 /root/server.key

```
mode of `/root/server.key' changed to 0400 (r--------)
```

SSL 証明書署名要求の生成

SSL 証明書署名要求を生成するには、次のコマンドを使用します。

- **% openssl req -new -key /root/server.key -out /root/server.csr**

```
Using configuration from /usr/share/ssl/openssl.cnfer.key -out /root/server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Cisco Systems Inc.
Organizational Unit Name (eg, section) []:Network Management Technology Group
Common Name (eg, your name or your server's hostname) []:opus
Email Address []:administrator@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:.
```

上記の手順が完了したら、v2.0 Privacy Enhanced Mail（PEM）形式の SSL 証明書署名要求をローカルの CNS Configuration Engine ファイル システムに作成します。SSL 証明書は、ご使用の証明書サーバまたは CA の署名を取得する必要があります。この時点で、署名を取得するために *server.csr* ファイルを CA に送信できます。

次の例は、PEM 形式にする前のファイルを示します。

ヘッダー テキスト「-----BEGIN CERTIFICATE REQUEST-----」とフッター テキスト「-----END CERTIFICATE REQUEST-----」は各行に自動的に付加されます。

```
[root@opus root]# more /root/server.csr
-----BEGIN CERTIFICATE
REQUEST----MIICETCCAXoCAQAwgbcxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYWxpZm9ybmlh
MREwDwYDVQQHEwhTYW4gSm9zZTEbMBkGA1UEChMSQ2lzY28gU3lzdGVtcyBJbmMu
MSwwKgYDVQQLEyNOZXR3b3JrIE1hbmFnZW1lbnQgVGVjaG5vbG9neSBHcm91cDEN
MAsGA1UEAxMEb3B1czEmMCQGCSqGSIb3DQEJARYXYWRtaW5pc3RyYXRvckBjaXNj
by5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALSbTB5cijXDFzGmGxDK
z5FpR1I8PfzJI/2lEfOUzKwffzbUmKESLOTTQ3g1Y7Qbh7lZBU1rVsc4I1pwHyKu
JOGNhG8wJCUau3ErmhExEM/OunD6zXU1VT/CSvMzG2e6l5JHEBIuZyL/LWEiaA+0
+7NiqI/xgsYPAUVdheEOqgkdAgMBAAGgGTAXBgkqhkiG9w0BCQcxChMIY2lzY28x
MjMwDQYJKoZIhvcNAQEEBQADgYEAQfwCg/fceFdy/xgpps6GSkRt8EB6gsMwNv2E
Cp+FQR0CK9NcpNwNezevbhqpNoaVhsmXgfbAw8mVxJWLJeLe1Bhf9GBXPwIttqLJ
IyfNZfagXMkW+S9z53MnPXg49RaT07itYkqe/1h6RV4TeHYjhPkHGuFeb9GsKM4X
B35lEeo=
-----END CERTIFICATE REQUEST----
```

デジタル署名された発行済み証明書

SSL 証明書要求 *server.csr* ファイルを証明書サーバにコピーし、CS/CA の署名を取得するために提出します。CS/CA 管理者がそれぞれのポリシーに従って CNS Configuration Engine の証明書要求を CS/CA のルート証明書で検証し、署名された有効な SSL 証明書を *server.cer* という名前の PEM 形式のファイルで返送します。証明書を受け取ったら、この署名付き証明書を CNS Configuration Engine の任意のディレクトリまたは IP FTP クライアントからアクセスできる外部 FTP サーバにコピーまたは配置します。

CNS Configuration Engine 証明書の内容の表示

CNS Configuration Engine 証明書の内容を表示するには、CNS Configuration Engine コンソールで（ルートとして）次のコマンドを実行します。出力の中にシリアル番号（serial:）があります。

```
[root@nugi root]# openssl x509 -noout -text -in /etc/tibgate/server.crt
......other data.......
X509v3 Authority Key Identifier:
keyid:28:B6:86:CF:E5:52:C9:8C:23:BA:C2:A2:A0:22:F1:DA:5E:77:53:30
DirName:/Email=administrator@mycompany.com/C=US/ST=CA/L=San Jose/O=Company Co
Inc./OU=Dept/CN=Personnel
serial:4D:00:F1:83:1F:8D:56:AC:4F:63:BF:0A:CA:AB:4F:00
.....other data.......
```

発行済み SSL 証明書のプレビュー

CNS Configuration Engine 証明書を CNS Configuration Engine にコピーしたら、CNS Configuration Engine 証明書の署名された内容をプレビューするために、証明書 server.cer ファイルに対して次の OpenSSL コマンドを使用します。

root@opus root]# openssl x509 -noout -text -in /root/server.cer

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=us, L=San Francisco CA, CN=My Company
        Validity
            Not Before: Mar 13 02:23:44 2004 GMT
            Not After : Mar 13 02:23:44 2005 GMT
        Subject: C=US, ST=California, L=San Jose, O=My Company., OU=Personnel Dept,
    CN=myhostname/Email=administrator@company.com
    co.com
        Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (2048 bit)
            Modulus (2048 bit):
                00:f3:8c:b6:34:4d:02:d4:66:39:9e:7b:9b:90:6e:
                ae:d9:96:00:c4:ae:e1:43:2f:bd:50:f4:9f:79:56:
                07:13:71:16:b9:03:6e:66:58:e8:5c:e7:78:d3:ef:
                c5:4d:f7:8e:11:d8:61:f5:fb:1e:ae:d9:7e:c0:d6:
                af:1d:7c:29:9e:00:df:87:1e:7d:75:b4:5d:b9:87:
                a4:02:62:fb:90:f5:6e:b5:ed:41:b5:50:7a:c8:92:
                7b:c9:64:68:19:6d:e9:1b:93:e2:9c:c3:d7:c0:d4:
                21:49:16:47:80:15:41:ba:c5:ad:76:c0:ff:fd:c9:
                68:ec:c9:72:e0:5d:af:a9:89:92:55:a1:34:48:72:
                1:d5:08:89:28:ef:b4:88:ec:7d:88:1c:c6:c4:7f:
                12:d8:1a:5f:76:3c:01:2b:03:b6:33:34:45:80:f8:
                55:3e:08:ed:32:f3:43:03:8e:c3:83:07:dc:b9:28:
                8e:ea:58:96:d4:2b:ff:83:71:a0:cc:14:ff:1b:ab:
            16:cd:fe:9a:87:6f:a4:4c:b4:2a:f5:75:e2:9b:96:
```

```
            fd:27:61:df:20:89:e2:03:0a:21:4a:af:a4:1e:8f:
            1f:fd:c6:ea:f9:64:ff:07:02:da:53:5e:b7:a1:95:
            e2:34:a5:31:79:80:58:0a:ec:d9:ec:61:8c:91:11:
            d5:c1
        Exponent: 65537 (0x10001)
    X509v3 extensions:
        X509v3 Authority Key Identifier:
        keyid:52:67:37:CF:69:13:66:E2:77:24:90:16:05:01:B3:DA:06:05:1A:E4
Signature Algorithm: md5WithRSAEncryption
    1c:eb:26:a7:71:f6:c2:28:bc:35:aa:18:57:cb:97:b1:b2:18:
    ca:4e:55:28:32:29:07:71:17:e8:6e:f8:6f:a3:06:d1:e8:33:
    1f:ed:fd:1d:82:53:ed:2e:ee:7a:fc:8f:11:b3:20:d7:1b:ac:
    26:87:91:99:41:a5:d0:6a:e2:70:97:26:94:f5:0b:72:aa:92:
    b7:e9:ee:78:ea:62:66:cd:16:d6:9c:2a:ba:7a:98:4e:44:f2:
    dc:33:f5:a3:2c:52:58:0d:57:7b:db:08:25:05:dc:3e:fa:69:
    8f:ee:ca:be:92:2f:72:40:a4:46:a8:15:c5:61:b5:68:f7:01:
    4d:82
[root@opus root]#
```

CNS Configuration Engine の証明書要求

次に、テスト用 CNS Configuration Engine でのキーと証明書要求の例を示します。証明書要求（*.csr）はユーザが CNS Configuration Engine で作成し、CA はその証明書に署名して有効な証明書（*.cer）を返送します。

```
[root@opus root]# openssl req -new -key /root/server.key -out /root/my-cnsce.csr
Using configuration from /usr/share/ssl/openssl.cnf
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [GB]:us
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Francisco
Organization Name (eg, company) [My Company Ltd]:Company Co Inc.
Organizational Unit Name (eg, section) []:Department
Common Name (eg, your name or your server's hostname) []:my-cnsce
Email Address []:administrator@company.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:2FCE2F9EF109E
An optional company name []:Company Co Inc.
[root@nugi root]#
```

Configuration Engine での SSL の有効化

CNS Configuration Engine のコンソールまたは端末にルートとしてログインし、CNS Configuration Engine のセットアップ プログラムを実行してコマンド Setup に入ります。これにより、CNS Configuration Engine セットアップの暗号化設定に変更を加え、その変更だけを適用できます。この場合は、対象のホストで SSL を有効にし、キーと証明書の場所を指定します。

CNS Configuration Engine での SSL のセットアップ例

次の例は、テスト用の SSL 対応 CNS Configuration Engine のセットアップ画面を示します。

```
======CNS Configuration Engine SETUP=====================

Please review the following parameters:
username for user-level shell account: admin
password for user-level shell account:
eth0 IP address: 10.1.2.8
eth0 network mask: 255.255.255.0
eth0 default gateway IP address: 10.1.2.7 eth1 IP address:
primary DNS server IP address: 10.1.2.3
secondary DNS server IP address (optional):
Configuration Engine login name: gui-admin
Configuration Engine login password: ******
internal LDAP server password: *********
Enable cryptographic (crypto) operation between Event Gateway(s)/Config server and
device(s) (y/n)? yes
Certificates already exist. Overwrite (y/n)? no
Enable plaintext operation between Config Server and devices/GUI administration (y/n)? no
Enable plaintext operation between Event Gateway and devices (y/n)? no
Enable authentication (y/n)? no
NSM directive (none, default, http): default
Enable Event Gateway debug log (y/n)?no
log file rotation timer (minutes, 0 = no rotation): 15
max log file size (Kbytes): 3072
the max versions of log file (0-99): 1
number of Event Gateways that will be started with crypto operation: 1
number of Event Gateways that will be started with plaintext operation: 1
CNS Event Bus Network Parameter: 10.1.25.18
CNS Event Bus Service Parameter: 7500
Re-configure IMGW (y/n)? no

 Warning: setup cannot be aborted while committing changes.

Commit changes (y/n):yes
```

Cisco IOS SSL

ここでは、Cisco IOS SSL の設定方法について説明します。

Cisco IOS SSL トラストポイントの設定

Cisco IOS では、SCEP を使用してネットワーク上のトラストポイントを設定できます。また、terminal オプションを使用して、トラストポイントをスクリーン ダンプから設定することもできます。端末上でトラストポイントを貼り付けるには、特定の形式でエンコードする必要があります。端末から入力する方法では Base 64 エンコード形式を使用します。

SCEP を使用した CPE SSL トラストポイント

次の例は、SCEP プロトコルを使用してトラストポイントを取得する方法を示します。

```
!
Router(config)#crypto ca trustpoint company.com
Router(config)#enrollment mode ra
Router(config)#enrollment url http://my-iosca:80/
Router(config)#usage ssl-client
Router(config)#revocation-check none
Router(config)#crypto ca authenticate att.com
```

```
Certificate has the following attributes:
Fingerprint: 1D74D54A 464207FD 817901A4D 67B5112B
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
!
crypto ca certificate chain company.com
certificate ca 4D69F1831F8D56AF4F63BF0F1B6B4F9B
308202F2 3082029C A0030201 0202104D 69F1821F 8D56AC4F 63BF0ACA AB4F9F30
0D06092A 864886F7 0D010105 05003081 97312139 1F06092A 864886F7 0D010901
1612656D 696B756C 69634063 6973636E 2E636F6D 310B3009 06035504 06130255
53310B30 09060355 04081302 43413111 300F0603 55040713 084D696C 70697461
73311B30 19060355 040A1312 43697365 6F205379 7374656D 7320496E 632E3113
30110603 55040B13 0A434E53 2D494E77 4D425531 13301106 03550403 130A494E
534D4255 2D434131 301E170D 30333035 32383232 34333533 5F970D30 35303532
38323235 3231325A 30819731 21301F06 092A8648 86F70D01 09011612 656D696B
756C6963 40636973 636F2E63 6F6D310B 30090603 55040613 02123331 0B300906
03550408 13024411 3111300F 06035504 0713084D 696C7069 74617331 1B301906
0355040A 13124369 73636F20 53797374 656D7320 496E632E 31133011 06035504
0B130A43 4E532D49 4E534D42 55311330 11060355 0403130A 494E534D 42552D43
4131305C 300D0609 2A864886 F70D0101 01050003 4B003048 02410097 2E2CED5E
B0F1194F 572E3275 F54F8C92 1A489BD4 CAD7701B 2275EA6B 3520DC29 7D17A1C4
AC6EB48C B03B1AF1 8CDAB68A A31FB15A 55325A45 032106E6 8214B902 03010001
A381C130 81BE300B 0603551D 0F040403 0201C630 0F060355 1D130101 FF040530
030101FF 301D0603 551D0E04 16041428 B686CFE5 52C98C23 BAC2A2A0 22F1DA5E
77533030 6D060355 1D1F0466 3064302F A02DA02B 86296874 74703A2F 2F67696C
6C696761 6E2F4365 7274456E 726F6C6C 2F494E53 4D42552D 4341312E 63726C30
31A02FA0 2D862B66 696C653A 2F2F5C5C 67696C6C 6967616E 5C436572 74456E72
6F6C6C5C 494E534D 42552D43 41312E63 726C3010 06092B06 01040182 37150104
03020100 300D0609 2A864886 F70D0101 05050003 41012C82 FA96ED42 329B01B7
83A48A06 4CEDFE36 2CF9706D 1ED1B7C8 882B0B4C 039A4E15 14B410FC 4258FFED
C8069002 76446090 CA22B642 B4207869 F495F8F2 BA51
quit
```

端末からのコピー アンド ペーストを使用した CPE SSL トラストポイント

次の例は、端末セッションを使用してコンソール上でトラストポイントを設定する方法を示します。

```
!
Router(config)#crypto ca trustpoint company.com
Router(config)#enrollment mode ra
Router(config)#enrollment terminal
Router(config)#usage ssl-client
Router(config)#revocation-check none
Router(config)#
!
Router(config)#crypto ca authenticate company.com
Enter the base 64 encoded CA certificate.
End with a blank line or the word "quit" on a line by itself

-----BEGIN CERTIFICATE----MIIC8jCCApygAwIBAgIQTWnxgx+
NVqxPY78KyqtPnzANBgkqhkiG9w0BAQUFADCB
lzEhMB8GCSqGSIb3DQEJARYSZW1pa3VsaWNAY2lzY28uY29tMQswCQYDVQQGEwJV
UzELMAkGA1UECBMCQ0ExETAPBgNVBAcTCE1pbHBpdGFzMRswGQYDVQQKExJDaXNj
byBTeXN0ZW1zIEluYy4xEzARBgNVBAsTCkNOUy1JTlNNQlUxEzARBgNVBAMTCklO
U01CVS1DQTEwHhcNMDMwNTI4MjI0MzUzWhcNMDUwNTI4MjI1MjEyWjCBlzEhMB8G
CSqGSIb3DQEJARYSZW1pa3VsaWNAY2lzY28uY29tMQswCQYDVQQGEwJVUzELMAkG
A1UECBMCQ0ExETAPBgNVBAcTCE1pbHBpdGFzMRswGQYDVQQKExJDaXNjbyBTeXN0
ZW1zIEluYy4xEzARBgXMAAsTCkNOUy1JTlNNQlUxEzARBgNVBAMTCklOU01CVS1D
QTEwXDANBgkqhkiG9w0BAQEFAANLADBIAkEAly4s7V6w8RlPVy4ydfVPjJIaSJvU
ytdwGyJ16ms1INwpfRehxKxutIywOxrxjNq2iqMfsVpVMlpFAyEG5oIUuQIDAQAB
o4HBMIG+MAsGA1UdDwQEAwIBxjAPBgNVHRMBAf8EBTADAQH/MB0GA1UdDgQWBBQo
tobP5VLJjCO6wqKgIvHaXndTMDBtBgNVHR8EZjBkMC+gLaArhilodHRwOi8vZ2ls
```

```
bGlnYW4vQ2VydEVucm9sbC9JTlNNQlUtQ0ExLmNybDAxoC+gLYYrZmlsZTovL1xc
Z2lsbGlnYW5cQ2VydEVucm9sbFxJTlNNQlUtQ0ExLmNybDAQBgkrBgEEAYI3FQEE
AwIBADANBgkqhkiG9w0BAQUFAANBACyC+pbtQjKbAbeDpIoGTO3+Niz5cG0e0bfI
iCsLTAOaThUUtBD8Qlj/7cgGkAJ2RGCQyiK2QrQgeGn0lfjyukE=
-----END CERTIFICATE----quit
Certificate has the following attributes:
Fingerprint: 1D74D54A B64207FD 81831A4D 1EDF56194
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
% Certificate successfully imported
```

show crypto ca trustpoint IOS コマンド

次の例は、次の出力を得る方法を示します。この例の重要なフィールドは Serial Number です。

```
Router#show crypto ca trustpoints
Trustpoint company-IOS-CA:
Subject Name: mytrustpoint
CN = Department
OU = Personnel
O = Company Co Inc.
L = San Francisco
ST = CA
C = US
EA = administrator@company.com
Serial Number: 4D69F1831F8Ef1344F63BF0ACAAB4F9F
Certificate configured.
CEP URL: <http://my-iosca>
```

OpenSSL 証明書の形式

ここでは、OpenSSL 証明書の形式について説明します。

証明書およびキーの形式

証明書およびキーには次の形式があります。

- PEM
- DER
- PKCS#12

PEM

これは OpenSSL で使用されるデフォルトの形式で、CNS Configuration Engine v1.4 以前で使用できる唯一の形式です。この形式には、すべてのプライベート キー（RSA および DSA）、パブリック キー（RSA および DSA）、および（x509）証明書を含めることができます。PEM には Base64 でエンコードされた DER 形式のデータが格納され、それが ASCII ヘッダーで囲まれるので、システム間でのテキスト モードの転送に適しています。

DER

DER 形式には、すべてのプライベート キー、パブリック キー、および証明書を含めることができます。DER に格納されるデータは ASN1 DER 形式に従います。これはほとんどのブラウザのデフォルト形式です。

PKCS#12

PKCS#12 は PFX ファイルとも呼ばれます。これらのファイルには、すべてのプライベート キー、パブリック キー、および証明書を含めることができます。データはバイナリ形式で格納されます。

詳細については、http://www.drh-consultancy.demon.co.uk/pkcs12faq.html/ を参照してください。

X509 PEM 証明書の形式は次のとおりです。

（ヘッダー情報）

```
------BEGIN (TRUSTED|X509) CERTIFICATE----(
Certificate Data)
------END (TRUSTED|X509) CERTIFICATE---
```

OpenSSL による証明書形式の変換

ここでは、OpenSSL ツールを使用して証明書形式を変換する手順について説明します。詳細については、OpenSSL のドキュメントを参照してください。

OpenSSL から PKCS#12 への変換

次の例は、OpenSSL を PKCS#12 に変換する方法を示します。

```
openssl pkcs12 -export -in pem-certificate-and-key-file -out
pkcs-12-certificate-and-key-file
openssl pkcs12 -export -in pem-certificate-file -inkey pem-key-file -out
pkcs-12-certificate-and-key-file
```

PKCS#12 から PEM への OpenSSL の変換

次の例は、OpenSSL を PKCS#12 から PEM に変換する方法を示します。

```
openssl pkcs12 -in pkcs-12-certificate-file -out pem-certificate-file
openssl pkcs12 -in pkcs-12-certificate-and-key-file -out pem-certificate-and-key-file
```

PEM/DER から DER/PEM への OpenSSL の変換

次の例は、OpenSSL を PEM/DER から DER/PEMPKCS#12 に変換する方法を示します。

```
openssl dsa -inform PEM|DER -outform DER|PEM -in pem-file|der-file -out der-file|pem-file
```

OpenSSL 証明書の形式

次の例は、OpenSSL 証明書の形式を示します。

```
OpenSSL From PEM/DER to DER/PEM - RSA Keys
openssl rsa -inform PEM|DER -outform DER|PEM -in pem-file|der-file -out der-file|pem-file
```

CNS SSL 通信のトラブルシューティング

発行された CNS Configuration Engine 証明書の内容を CNS Configuration Engine で表示するには、次の OpenSSL コマンドを実行します。このサンプルは、シスコのラボで IOS CS/CA によって実際に発行された証明書から取得したものです。ここで注意すべき重要な値は、Serial Number: の後に続く 16 進数の文字列です。これは発行された証明書のシリアル番号を示します。

SSL 証明書の表示

次の例は、SSL 証明書を表示する方法を示します。

```
openssl x509 -noout -text -in /etc/tibgate/server.crt
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            15:79:ce:3e:00:00:ef:00:00:04
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: Email=administrator@mycompany.com, C=US, ST=CA, L=San Francisco, O=Company
Co Inc., OU=Department, CN=Personnel
        Validity
            Not Before: May 30 01:52:27 2003 GMT
            Not After : May 30 02:02:27 2004 GMT
        Subject: Email=administrator@mycompany.com, C=us, ST=California, L=San Jose,
O=Company Inc., OU=Department, CN=config-engine
    Subject Public Key Info:
        Public Key Algorithm: rsaEncryption
        RSA Public Key: (1024 bit)
            Modulus (1024 bit):
                00:c8:5a:71:55:f8:30:21:da:ef:f1:6f:5c:e5:df:
                92:66:be:d2:7f:86:65:e7:e1:de:f4:c2:ac:1e:e1:
                e9:7a:a2:64:20:81:ed:a6:ff:f8:85:ab:fc:63:0f:
                d3:71:93:b1:6b:31:f5:0b:11:64:c1:dc:29:88:7f:
                ab:81:69:bf:f0:81:5c:af:1b:86:9d:14:30:47:fd:
                44:04:ea:3e:e6:e0:2b:7d:33:d4:37:ba:a9:ba:ee:
                29:2f:52:a9:f3:e2:26:60:5d:c7:6d:25:92:80:fe:
                16:07:f8:c9:2d:75:6f:29:4c:17:3c:85:70:ad:c1:
                65:aa:ea:c5:e0:09:47:24:e1
            Exponent: 65537 (0x10001)
    X509v3 extensions:
    X509v3 Subject Key Identifier:
        35:7E:67:7C:B9:AC:79:ED:34:CB:08:DF:AB:1E:C6:0D:FC:41:3B:71
    X509v3 Authority Key Identifier:
        keyid:28:B6:86:CF:E5:52:C9:8C:23:BA:C2:A2:A0:22:F1:DA:5E:77:53:30
        DirName:/Email=administrator@mycompany.com/C=US/ST=CA/L=San Jose/O=Company
Co Inc./OU=Department/CN=Marketing
        serial:4D:69:F1:1F:EF:8E:56:AC:4F:63:BF:0A:CA:AB:4F:9F
    X509v3 CRL Distribution Points:
        URI:http://my-iosca/
        URI:file://\\my-iosca
    Authority Information Access:
        CA Issuers - URI:http://my-iosca
        CA Issuers - URI:file://\\my-iosca
Signature Algorithm: sha1WithRSAEncryption
    24:d7:86:57:95:78:08:60:8d:88:ab:6b:46:76:bc:45:ce:59:
    6c:af:29:43:17:22:a1:78:d0:65:8a:11:79:ef:6b:15:84:8b:
    bf:40:de:9a:08:81:8c:da:ea:e1:0c:fb:bb:0c:8d:96:74:31:
    30:a0:12:de:19:ca:1b:24:60:0d
```

SSL トランザクションのデバッグ ダンプ

SSL トランザクションの**デバッグ**出力を表示するには、次のコマンドを使用します。ssldump プログラムは OpenSSL ツールキットの一部であり、SSL トラストポイントを設定および共有する際に役立ちます。

```
/opt/CSCOcnsie/tools/ssldump -A -e -N -d -i eth0 port 443
..or more simply..
/opt/CSCOcnsie/tools/ssldump -i eth0 port 443
/opt/CSCOcnsie/tools/ssldump -i eth0 port 11012
```

```
..and the operator can easily pipe these to a file as such:
/opt/CSCOcnsie/tools/ssldump -i eth0 port 443 > ssl_http.log
/opt/CSCOcnsie/tools/ssldump -i eth0 port 11012 > ssl_event.log
```

IOS SSL デバイスのトラブルシューティング

次の debug および show コマンドは、SSL セキュリティ レイヤをサポートするほとんどの IOS CPE で使用できます。これらのコマンドは、CPE デバイスで SSL クライアント トラストポイントのセットアップをデバッグする際に役立つすべての情報をオペレータに提供します。

PKI デバッグ コマンド

次の例は、PKI デバッグ コマンドを示します。

```
debug crypto pki transactions
debug crypto pki messages
```

SSL デバッグ コマンド

次の例は、SSL デバッグ コマンドを示します。

```
debug ssl traffic
debug ssl error
debug ssh hdshake
```

show crypto コマンド

次の例は、crypto コマンドを示します。

```
show crypto key pubkey-chain rsa
show crypto ca trustpoints
show crypto ca certificate
```

show crypto key pubkey-chain rsa コマンド

次の例は、IOS デバイスにおけるトラストポイント証明書のパブリック キーの出力を示します。

```
Router#show crypto key pubkey-chain rsa
Codes: M - Manually configured, C - Extracted from certificate

Code     Usage      IP-Address/VRF         Keyring            Name
C       Signing                           default            X.500 DN name:
                              CN = IOS-CA1
                              OU = Marketing
                              O = Company Co Inc.
                              L = San Jose
                              ST = CA
                              C = US
                              EA = administrator@company.com
```

show crytpo ca trustpoint

次の例は、IOS デバイスにおける IOS SSL トラストポイント証明書の内容と署名の出力を示します。

```
Router#show crypto ca trustpoints
```

```
Trustpoint cisco-ssl-home:
    Subject Name:
    CN = IOS-CA1
    OU = Marketing
    O = Company Co Inc.
    L = San Jose
    ST = CA
    C = US
    EA = administrator@company.com
        Serial Number: 4D69F1E1D5F8D6AC4F63BF0ACAAB4F9F
Certificate configured.
CEP URL: http://my-iosca
```

show crypto ca certificate

次の例は、IOS デバイスにおける show crypto ca cert IOS コマンドの出力を示します。

```
Router#show crypto ca cert
CA Certificate
    Status: Available
    Certificate Serial Number: 2D19F1841F8D56AC4F63BF0AC1DB4F9F
Certificate Usage: Signature
Issuer:
    CN = IOS-CA1
    OU = Marketing
    O = Company Co Inc.
    L = San Jose
    ST = CA
    C = US
    EA = administrator@company.com
Subject:
    CN = IOS-CA1
    OU = Marketing
    O = Company Co Inc.
    L = San Jose
    ST = CA
    C = US
    EA = administrator@company.com
CRL Distribution Point:
    http://my-iosca
Validity Date:
    start date: 22:43:53 UTC May 28 2003
    end date: 22:52:12 UTC May 28 2005
Associated Trustpoints: ssl-home
```

CNS ID の構文

次の例は、CNS ID の構文を示します。

```
Router#enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#cns id ?
    Async          Async interface
    BVI            Bridge-Group Virtual Interface
    CDMA-Ix        CDMA Ix interface
    CTunnel        CTunnel interface
    Dialer         Dialer interface
    Ethernet       IEEE 802.3
    FastEthernet   FastEthernet IEEE 802.3
```

```
Group-Async    Async Group interface
Lex            Lex interface
Loopback       Loopback interface
MFR            Multilink Frame Relay bundle interface
Multilink      Multilink-group interface
Tunnel         Tunnel interface
Vif            PGM Multicast Host interface
Virtual-PPP Virtual PPP interface
Virtual-Template Virtual Template interface
Virtual-TokenRing Virtual TokenRing
Vlan Catalyst Vlans
hardware-serial Use hardware serial number as unique ID
hostname Use hostname as unique ID
string Use an arbitrary string as the unique ID
```

CNS ID ネットワーク インターフェイス値の参照

次の例は、CNS ID ネットワーク インターフェイス値の出力を示します。

```
Router#enable
Router#configure terminal
Router#(config)#cns id FastEthernet 0 ?
ipaddress Use IP address as unique ID
mac-address Use MAC address as unique ID

Router(config)#cns id Async 1 ?
ipaddress Use IP address as unique ID
mac-address Use MAC address as unique ID
```

CNS ID ハードウェア シリアル番号

次の例は、CNS ID ハードウェア シリアル番号の出力を示します。

```
Router(config)#cns id hardware-serial ?
event Set this ID as the event ID
image Set this ID as the image ID
<cr>
```

マザーボード ハードウェア シリアル番号の表示

次の例は、マザーボード ハードウェア シリアル番号の出力を示します。

```
Router#enable
Router#config terminal
Router(config)#do show version
Cisco IOS Software, C1700 Software (C1700-ADVENTERPRISEK9-M), Experimental Version 12.3
Copyright (c) 1986-2004 by Cisco Systems, Inc.
Compiled Fri 13-Feb-04 20:04 by ntimms
ROM: System Bootstrap, Version 12.2(7r)XM4, RELEASE SOFTWARE (fc1)
cisco-1711 uptime is 2 days, 19 hours, 27 minutes
System returned to ROM by reload
System restarted at 07:51:21 UTC Thu Mar 4 2004
System image file is "flash:c1700-adventerprisek9-mz.24.Feb.2004"
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
```

```
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html
If you require further assistance please contact us by sending email to export@cisco.com.

Cisco 1711 (MPC862P) processor (revision 0x100) with 116939K/14133K bytes of memory.
Processor board ID FOC07271A6Q (2119579075), with hardware revision 0000
MPC862P processor: part number 7, mask 0
1 Ethernet interface
5 FastEthernet interfaces
1 Serial interface
1 terminal line
1 Virtual Private Network (VPN) Module
32K bytes of NVRAM.
32768K bytes of processor board System flash (Read/Write)
Configuration register is 0x2102
```

ハードウェアシリアルの CNS イメージ ID の表示

次の例は、ハードウェアシリアルの CNS イメージの出力を示します。

```
Router#enable
Router#configure terminal
Router(config)#cns id hardware-serial image
Router(config)#do show cns image status
CNS Image Agent ID: FOC07271A6Q
Number of failed upgrades: 0
Number of successful upgrades: 0
Messages received: 8
Receive errors: 1
Bad XML format:1       Not Supported:0    Invalid Parameter:0
Memory exhausted:0     File too large:0   Operation failed:0
File Errors:0          Auth Errors: 0
Transmit Status
TX Attempts:7
Successes:6 Failures 3
Detailed Failures
Memory exhausted:0     queue error:0      external error:0
other error:3
```

ハードウェアシリアルの CNS コンフィギュレーション ID

次の例は、ハードウェアシリアルの CNS コンフィギュレーション ID の出力を示します。

```
Router#enable
Router#configure terminal
Router(config)#cns id hardware-serial
Router(config)#do show cns config connections
The partial configuration agent is enabled.
Configuration server: 10.1.25.94
Port number: 80
Encryption: disabled
Config id: FOC07271A6Q
Connection Status:
The initial configuration agent is not running.
```

（注）　ハードウェアシリアル ID は show version コマンドで表示される ID であり、CNS エージェントによって内部でデバイスのマザーボードから取得されます。この英数字文字列は、特定の Cisco IOS デバイスのシャーシに記載されているシリアル番号と同じである場合と異なる場合があります。

その他の情報源

追加の情報を得るために次のドキュメントを参照できます。

Cisco IOS 証明書サーバ

Cisco IOS 証明書サーバの詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1cb0.html

証明書サーバのデータ シート

証明書サーバのデータ シートの詳細については、次の URL にある技術ドキュメントを参照してください。

http://www.cisco.com/en/US/tech/tk583/tk372/tech_brief09186a00801e05dc.html

Cisco IOS PKI

Cisco IOS ソフトウェア Release 12.3 T / セキュリティ コマンド

For more information on Cisco IOS software releases and security commands, see the command reference document at:
http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_command_reference_chapter09186a00801a7f81.html

SSL パブリック キー インフラストラクチャ

SSL パブリック キー インフラストラクチャの詳細については、次の URL にあるホワイト ペーパーを参照してください。

http://www.cisco.com/en/US/tech/tk583/tk618/technologies_white_paper09186a0080179739.shtml

証明書セキュリティ属性ベースのアクセス コントロール

証明書セキュリティ属性ベースのアクセス コントロールの詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1839/products_feature_guide09186a00801541ce.html

Cisco IOS 証明書サーバのデータ シート

Cisco IOS 証明書サーバのデータ シートの詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/en/US/tech/tk583/tk372/tech_brief09186a00801e05dc.html

http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/certs_ds.pdf

Cisco IOS 証明書サーバおよびソフトウェア Release 12.3 T

Cisco IOS サーバおよびソフトウェア Release 12.4 の詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1cb0.html

信頼できるルート認証機関

信頼できるルート認証機関の詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps1834/products_feature_guide09186a008007fecf.html.

Online Certificate Status Protocol

Online Certificate Status Protocol の詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801a755b.html.

シスコの SCEP ホーム ページ

SCEP ホーム ページの詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.html.

Cisco IOS ソフトウェア Release 12.3 T

Cisco IOS ソフトウェア Release 12.3 T および RSA キー ペアの詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/en/US/products/sw/iosswrel/ps5207/products_feature_guide09186a00801d1cb4.html.

トラストポイント コマンド

トラストポイント コマンドの詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/fttrust.htm.

証明書登録の機能拡張

証明書登録の機能拡張の詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftenrol2.htm.

暗号マップの設定

DN ベースのアクセス コントロール用の暗号マップの設定に関する詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/warp/public/471/vpn_dn.html - tools

複数の RSA キー ペアのサポート

複数の RSA キー ペアのサポートの詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ftmltkey.htm-42193.

Simple Certificate Enrollment Protocol

Simple Certificate Enrollment Protocol の詳細については、次の URL にあるドキュメントを参照してください。

http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm.

パブリック ドメイン OpenSSL

OpenSSL の詳細については、*http://www.openssl.org* を参照してください。

OpenSSL 証明書

OpenSSL 証明書の詳細については、*http://www.openssl.org/docs/HOWTO/certificates.txt* を参照してください。