SCCP IP Phone の SSL VPN クライアントの設定

この章では、Cisco Unified CME における SCCP IP Phone に対する SSL VPN クライアント サポートについて説明します。各機能がサポートされているバージョンのリストについては、「SSL VPN クライアントの機能情報」（P.1477）を参照してください。

このモジュールで紹介する機能情報の入手方法

お使いの Cisco Unified CME のバージョンが、このモジュールで説明されている機能の一部をサポートしていないことがあります。

内容

- 「SSL VPN クライアントについて」（P.1443）
- 「SSL VPN クライアントの設定方法」（P.1447）
- 「その他の参考資料」（P.1476）
- 「SSL VPN クライアントの設定例」（P.1474）
- 「SSL VPN クライアントの機能情報」（P.1477）

SSL VPN クライアントについて

- 「DTLS による Cisco Unified CME での SSL VPN サポート」（P.1443）
- 「SCCP IP Phone での SSL VPN クライアントのサポート」（P.1446）

DTLS による Cisco Unified CME での SSL VPN サポート

Communications Manager Express 8.6 以降のバージョンでは、企業のネットワーク外にある 7945、7965、および 7975 などの Cisco Unified SCCP IP Phone を、SSL VPN 接続により Cisco Unified CME に登録できます。SSL VPN 接続は電話機と VPN ヘッドエンドの間でセットアップされます。VPN ヘッドエンドにすることができるのは、Adaptive Secure Appliance（ASA 5500）または Datagram Transport Layer Security（DTLS）対応の IOS SSL VPN ルータです。図 68 を参照してください。ASA ヘッドエンドでの VPN 機能のサポートは、Cisco Unified CME 8.5 で追加されました。詳細については、「SCCP IP Phone での SSL VPN クライアントのサポート」（P.1446）を参照してください。

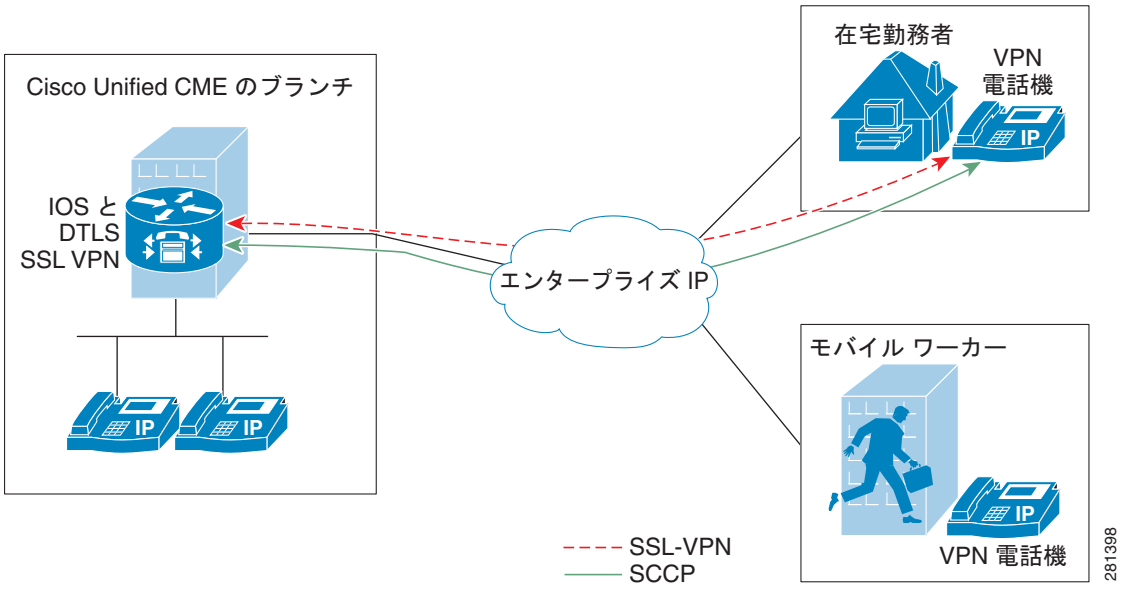

図 68　　Cisco Unified IP Phone と VPN ヘッドエンド（ASA と DTLS）の間の VPN 接続

Cisco Unified CME 8.6 は IOS SSL DTLS をヘッドエンドまたはゲートウェイとして使用します。電話機と VPN ヘッドエンドの間で VPN 接続を確立するには、電話機に VPN 設定パラメータを設定する必要があります。VPN 設定パラメータには、VPN ヘッドエンド アドレス、VPN ヘッドエンド クレデンシャル、ユーザまたは電話機の ID、およびクレデンシャル ポリシーなどがあります。これらのパラメータは機密情報と見なされ、署名付きコンフィギュレーション ファイルまたは署名付きで暗号化されたコンフィギュレーション ファイルを使用してセキュアな環境で配布する必要があります。電話機を企業のネットワーク外に配置できるようにする前に、企業のネットワーク内でプロビジョニングする必要があります。

信頼できる環境で電話機が「ステージング」されると、VPN ヘッドエンドを接続できる場所に、その電話機を展開できます。電話機の VPN 設定パラメータは、電話機のユーザ インターフェイスおよび動作を指示します。

電話機またはクライアントの認証

電話機の認証は、VPN DTLS を介して Cisco Unified CME に登録しようとしているリモート電話機が正当な電話機であることを確認するために必要です。電話機またはクライアントの認証は次のタイプの認証で行うことができます。

h. ユーザ名とパスワードによる認証。

i. 証明書ベースの認証（電話機の認証は電話機の LSC 証明書または MIC 証明書を使用して行われます）。証明書ベースの認証は次の 2 レベルで構成されます。

- 証明書のみの認証：電話機の LSC のみが使用されます（ユーザはユーザ名またはパスワードの入力を電話機で要求されません）。
- AAA または 2 要素による認証：電話機の LSC とユーザ名およびパスワードが電話機の認証に使用されます。2 要素認証は、ユーザ名の事前入力の有無にかかわらず実行できます。（ユーザ名の事前入力ありの場合、電話機からユーザ名の入力は求められず、ユーザ名は該当するトラストポイントの設定に応じてピックアップされます）。

（注） 証明書認証には LSC の使用を推奨します。証明書認証に MIC を使用することは推奨されません。また、証明書認証を行う場合には、「認証済み」（暗号化なし）セキュリティ モードで ephone を設定することも推奨します。証明書のみの認証および 2 要素認証の詳細については、次のリンクを参照してください。
https://www.cisco.com/en/US/docs/ios/sec_secure_connectivity/configuration/guide/sec_ssl_vpn_ps6350_TSD_Products_Configuration_Guide_Chapter.html#wp1465191

Cisco Unified CME は暗号化モードでセットアップできますが、暗号化された SCCP 電話機のメディア コール フロー サポートが制限されます。認証済みモードで電話機を使用する場合、メディア関連のコール フローに制限はありません。

SCCP IP Phone での SSL VPN クライアントのサポート

Cisco Unified CME 8.5 以降のバージョンでは、7945、7965、および 7975 などの SCCP IP Phone で Secure Sockets Layer（SSL）バーチャル プライベート ネットワーク（VPN）がサポートされます。

Cisco Unified CME 8.5 では、企業のネットワーク外の SCCP IP Phone は、図 69 に示すように、VPN 接続経由で Cisco Unified CME 8.5 に登録できます。

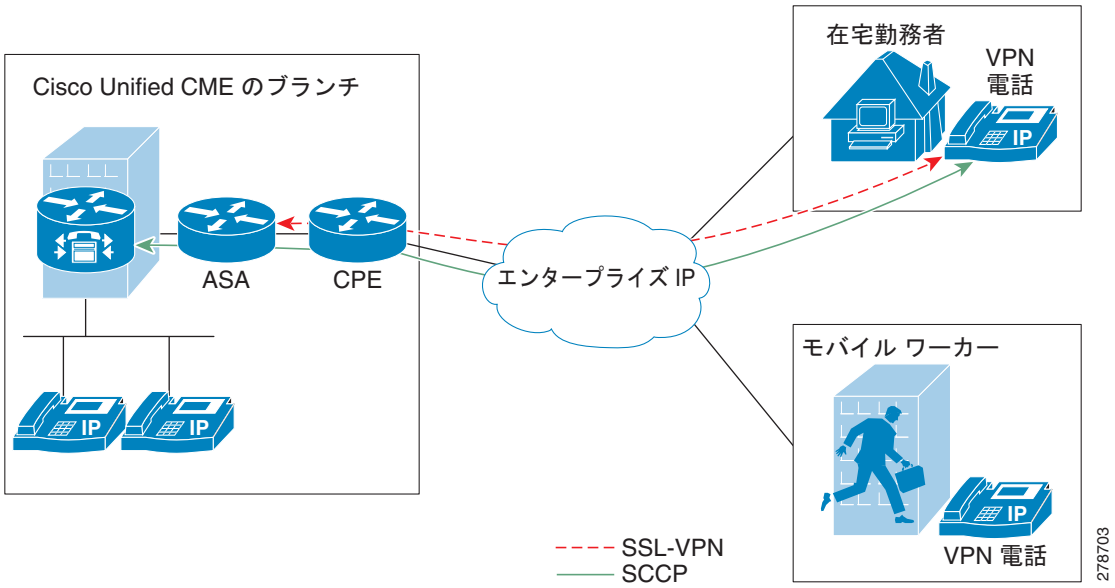

図 69　　電話機と VPN ヘッドエンドの間の接続

SSL VPN は、2 つのエンドポイント間で送信されるデータやその他の情報のためのセキュアな通信メカニズムを提供します。VPN 接続は SCCP IP Phone と VPN ヘッドエンドまたは VPN ゲートウェイの間でセットアップされます。Cisco Unified CME 8.5 では、適応型セキュリティ アプライアンス（ASA モデル 55x0）を VPN ヘッドエンドまたはゲートウェイとして使用します。

電話機と VPN ゲートウェイの間の VPN 接続を確立するために、電話機を VPN ゲートウェイ アドレス、VPN ヘッドエンド クレデンシャル、ユーザまたは電話機の ID、クレデンシャル ポリシーなどの VPN 設定パラメータで設定する必要があります。これらのパラメータには機密情報が含まれており、署名付きコンフィギュレーション ファイルまたは署名付きで暗号化されたコンフィギュレーション ファイルを使用してセキュアな環境で配布する必要があります。電話機を企業のネットワーク外に配置する前に、企業のネットワーク内でプロビジョニングする必要があります。

信頼できるセキュアな環境で電話機がプロビジョニングされると、VPN ヘッドエンドに到達できる場所ならどこからでも、その電話機を Cisco Unified CME に接続できます。電話機の VPN 設定パラメータは電話機のユーザ インターフェイスおよび動作を制御します。SCCP IP Phone での SSL VPN 機能の設定の詳細については、「SCCP IP Phone での SSL VPN クライアントの設定方法」（P.1447）を参照してください。

エクスポート可能なキーでトラストポイントを生成し、それを sast1 として使用する必要があります。

SSL VPN クライアントの設定方法

ここでは、次の作業について説明します。

- 「SCCP IP Phone での SSL VPN クライアントの設定方法」（P.1447）
- 「Cisco Unified CME での DTLS による SSL VPN クライアントの設定」（P.1467）

SCCP IP Phone での SSL VPN クライアントの設定方法

SCCP IP Phone で SSL VPN 機能を設定するには、次の手順を表示されている順に実行します。

1. 「Cisco Unified CME での基本設定」（P.1447）
2. 「CA サーバとしての Cisco Unified CME の設定」（P.1453）
3. 「電話機の登録と電話機ファームウェアの確認」（P.1457）
4. 「SSL VPN 用の ASA（ゲートウェイ）の設定」（P.1457）
5. 「Cisco Unified CME での VPN グループおよびプロファイルの設定」（P.1461）
6. 「VPN グループおよびプロファイルの SCCP IP Phone への関連付け」（P.1463）
7. 「電話機での代替 TFTP アドレスの設定」（P.1466）
8. 「リモート サイトからの電話機の登録」（P.1467）

前提条件

- Cisco Unified CME 8.5 以降のバージョン。
- Cisco Unified SCCP IP Phone 7942、7945、7962、7965、および 7975 と phone image 9.0 以降。
- イメージ asa828-7-k8.bin 以降の ASA 5500 シリーズ。
- SSLVPN 機能の設定には、パッケージ anyconnect-win-2.4.1012-k9.pkg が必要。ただし、電話機にはダウンロードされません。
- VPN クライアントで接続できるようにするには、適切な ASA ライセンス（AnyConnect for Cisco VPN Phone）を要求して、ASA にインストールすること。www.cisco.com/go/license にアクセスして PAK を入力すると、新しいアクティベーション キーが電子メールで送信されます。

（注） ASDM を介して設定する場合は、互換性のある Adaptive Security Device Manager（ASDM）イメージが必要です。

Cisco Unified CME での基本設定

次の手順は、SSL VPN 機能を組み込むための基本的な Cisco Unified 設定です。

手順の概要

1. **enable**
2. **configure terminal**
3. **ip dhcp pool** *pool-name*
4. **network** *ip-address* [*mask* | *prefix-length*]

5. **option 150 ip** *ip-address*
6. **default-router** *ip-address*
7. **exit**
8. **telephony-service**
9. **max-ephones** *max-phones*
10. **max-dn** *max-directory-numbers* [**preference** *preference-order*] [**no-reg primary** | **both**]
11. **ip source-address** *ip-address* **port** *port* [**any-match** | **strict-match**]
12. **cnf-file** {**perphone**}
13. **load** [*phone-**type firmware-file***]
14. **no shutdown**
15. **exit**
16. **ephone-dn** *dn-tag* [dual-line]
17. **number** *number* [**secondary** *number*] [**no-reg** [**both** | **primary**]]
18. **ephone** *phone-tag*
19. **description** *string*
20. **device-security-mode** {**authenticated** | **none** | **encrypted**}
21. **mac-address** [*mac-address*]
22. **type** *phone-type* [addon 1 module-type [2 module-type]]
23. **button** *button-number*{separator}*dn-tag* [,*dn-tag*...] [*button-number*{x}overlay-*button-number*] [button-number...]
24. **exit**
25. **telephony-service**
26. **create cnf-files**
27. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**ip dhcp pool** *pool-name* **例：** `Router(config)# ip dhcp pool mypool`	DHCP サーバ アドレス プールの名前を作成し、DHCP プール コンフィギュレーション モードを開始します。 **（注）** DHCP IP アドレス プールをすでに設定している場合は、ステップ 2 ～ステップ 7 をスキップし、ステップ 8 から続行してください。

	コマンドまたはアクション	目的
ステップ 4	**network** *ip-address* [*mask* | *prefix-length*] **例：** `Router(config-dhcp)#network 192.168.11.0 255.255.255.0`	設定する DHCP アドレス プールの IP アドレスを指定します。
ステップ 5	**option 150 ip** *ip-address* **例：** `Router(config-dhcp)# option 150 ip 192.168.11.1`	Cisco Unified IP Phone でイメージ コンフィギュレーション ファイルをダウンロードする TFTP サーバ アドレスを指定します。 • これはご使用の Cisco Unified CME ルータのアドレスです。
ステップ 6	**default-router** *ip-address* **例：** `Router(config-dhcp)# default router 192.168.11.1`	（任意）IP Phone でローカル サブネットの外部にある IP トラフィックを送受信するために使用するルータを指定します。 • Cisco Unified CME ルータがネットワーク上の唯一のルータである場合、このアドレスは Cisco Unified CME の IP ソース アドレスにする必要があります。IP Phone でローカル サブネット上のデバイスのみと IP トラフィックの送受信を行う必要がある場合は、このコマンドは省略できます。 • デフォルト ルータに指定する IP アドレスは、フォールバックの目的で IP Phone で使用されます。Cisco Unified CME の IP ソース アドレスが到達不能になった場合、IP Phone はこのコマンドで指定されたアドレスへの登録を試行します。
ステップ 7	**exit** **例：** `Router(config-dhcp)# end`	DHCP プール コンフィギュレーション モードを終了します。
ステップ 8	**telephony-service** **例：** `Router(config)# telephony-service`	telephony-service コンフィギュレーション モードを開始します。
ステップ 9	**max-ephones** *max-phones* **例：** `Router(config-telephony)# max-ephones 24`	Cisco Unified CME に登録できる電話機の最大数を設定します。 • 最大数はプラットフォームとバージョンで異なります。範囲を表示するには ? と入力します。 • Cisco Unified CME 7.0/4.3 以降のバージョンでは、登録できる電話機の最大数が、設定できる電話機の最大数とは異なります。設定できる電話機の最大数は 1000 です。 • Cisco Unified CME 7.0/4.3 よりも前のバージョンでは、このコマンドがルータで設定できる電話機の数に制限されていました。

	コマンドまたはアクション	目的
ステップ 10	**max-dn** *max-directory-numbers* [**preference** *preference-order*] [**no-reg primary | both**] **例：** `Router(config-telephony)# max-dn 24 no-reg primary`	このルータでサポートされるディレクトリ番号の数を制限します。 • 最大数はプラットフォームとバージョンで異なります。値を表示するには ? と入力します。
ステップ 11	**ip source-address** *ip-address* [**port** *port*] [**any-match** | **strict-match**] **例：** `Router(config-telephony)# ip source-address 192.168.11.1 port 2000`	Cisco Unified CME ルータで IP Phone の登録に使用する IP アドレスとポート番号を指定します。 • **port** *port*：（任意）SCCP に使用する TCP/IP ポート番号。範囲は 2000 ～ 9999 です。デフォルトでは 2000 です。 • **any-match**：（任意）登録のための厳密な IP アドレスのチェックをディセーブルにします。これがデフォルトです。 • **strict-match**：（任意）電話機で使用される IP サーバアドレスがソース アドレスと厳密に一致していない場合、ルータに IP Phone の登録試行を拒否するように指示します。
ステップ 12	**cnf-file** {**perphone**} **例：** `Router(config-telephony)#xnf-file perphone`	システムで各 IP Phone に個別の設定 XML ファイルを生成することを指定します。 • セキュリティのために、各エンドポイントに個別のコンフィギュレーション ファイルが必要です。 **（注）** 各電話に個別の XML ファイルを生成するには、cnf-file（perphone）コマンドを設定する必要があります。
ステップ 13	**load** [*phone-type firmware-file*] **例：** `Router(config-telephony)# load 7965 SCCP45.9-0-1TD1-36S.loads`	電話機のタイプを電話機のファームウェア ファイルに関連付けます。ファイルのサフィクスを含めて完全なファイル名を使用する必要があります。電話機のファームウェア バージョンがバージョン 9.0 よりも新しい場合、すべての電話機のタイプに 7965 SCCP45.9-0-1TD1-36S をロードします
ステップ 14	**no shutdown** **例：** `Router(config-telephony)# no shutdown`	SCCP サービス リスニング ソケットをイネーブルにできます。
ステップ 15	**exit** **例：** `Router(config-telephony)# end`	telephony-service コンフィギュレーション モードを終了します。

	コマンドまたはアクション	目的
ステップ 16	**ephone-dn** *dn-tag* [dual-line] **例：** Router(config)# ephone-dn 1	ephone dn コンフィギュレーション モードを開始して、IP Phone、インターコム回線、音声ポート、または Message Waiting Indicator（MWI）のディレクトリ番号を定義します。 • *dn-tag*：設定タスク中の特定のディレクトリ番号を指定します。範囲は 1 からルータのプラットフォームで許可されるディレクトリ番号の最大数までです。範囲を表示するには、? と入力します。
ステップ 17	**number** number [**secondary** number] [**no-reg** [**both** |**primary**]] **例：** Router(config-ephone-dn)# number 1001	内線番号をこのディレクトリ番号に関連付けます。 • *number*：内線または E.164 電話番号を示す最大 16 桁の文字列。
ステップ 18	**ephone** *phone-tag* **例：** Router(config)# ephone 1	ephone コンフィギュレーション モードを開始して、ephone 固有のパラメータを設定します。 • *phone-tag*：電話機を識別する一意のシーケンス番号。範囲はバージョンとプラットフォームに依存します。範囲を表示するには、? と入力します。
ステップ 19	**description** *string* **例：** Router(config-ephone)description SSL VPN Remote Phone	eXtensible Markup Language（XML）クエリーを使用して、ネットワーク管理システムに対して ephone を説明します。 • *string*：スペースを含めて最大 128 文字を使用できます。文字に制限はありません。
ステップ 20	**device-security-mode** {**authenticated** | **none** | **encrypted**} **例：** Router(config-ephone)# device-security-mode none	デバイスと Cisco Unified CME ルータとのグローバルな、または ephone 単位での通信のための SCCP シグナリングにセキュリティ モードを設定できます。 • authenticated：TCP ポート 2443 上でのセキュアな TLS 接続を介したデバイスと Cisco Unified CME との間の SCCP シグナリング。 • none：SCCP シグナリングはセキュアではありません。 • encrypted：TCP ポート 2443 上でのセキュアな TLS 接続を介したデバイスと Cisco Unified CME との間の SCCP シグナリング。メディアは Secure Real-Time Transport Protocol（SRTP）を使用します。
ステップ 21	**mac-address** [*mac-address*] **例：** Router(config-ephone)# mac-address 0022.555e.00f1	Cisco IP Phone の MAC アドレスを Cisco Unified CME システムの ephone 設定に関連付けます • *mac-address*：IP Phone の MAC アドレスを指定します。これは、電話機の底面にあるシールに記載されています。

	コマンドまたはアクション	目的
ステップ 22	**type** phone-type [addon 1 module-type [2 module-type]] **例：** Router(config-ephone)# type 7965	電話機のタイプを指定します。 • Cisco Unified CME 4.0 以降のバージョン：アドオン モジュールを適用できるタイプは、7960、7961、7961GE、および 7970 のみです。
ステップ 23	**button** button-number{separator}dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...] **例：** Router(config-ephone)# button 1:1	ボタン番号と回線の特性を ephone-dn に関連付けます。ボタンの最大数は電話機のタイプによって決まります。
ステップ 24	**exit** **例：** Router(config-ephone)#exit	ephone コンフィギュレーション モードを終了します。
ステップ 25	**telephony-service** **例：** Router(config)telephony-service	telephony-service コンフィギュレーション モードを開始します。
ステップ 26	**create cnf-files** **例：** Router(config-telephony)# create cnf-files	SCCP 電話機で必要とされる XML コンフィギュレーション ファイルを構築します。
ステップ 27	**end** **例：** Router(config-telephony)# end	特権 EXEC モードに戻ります。

CA サーバとしての Cisco Unified CME の設定

CA サーバでの基本設定では、SSL VPN 機能をイネーブルにするために必要な IP 接続、ネットワーク タイム プロトコル（NTP）、時刻の同期を設定します。CA サーバを設定するには、次の手順を実行します。

ステップ 1 Cisco Unified CME ルータで IP アドレス、NTP および HTTP サーバを設定します。

```
Router(config)#Interface GigabitEthernet0/0
Router(config-if)#no ip address
Router(config-if)#interface GigabitEthernet0/0.10
Router(config-subif)#description DATA VLAN
Router(config-subif)#encapsulation dot1Q 10 native
Router(config-subif)#ip address 192.168.10.1 255.255.255.0

Router(config)#interface GigabitEthernet0/0.11
Router(config-subif)#description VOICE VLAN
Router(config-subif)#encapsulation dot1Q 11
Router(config-subif)#ip address 192.168.11.1 255.255.255.0

Router(config)#interface GigabitEthernet0/1
Router(config-if)#description INTERFACE CONNECTED TO ASA
Router(config-if)#ip address 192.168.20.1 255.255.255.0

Router(config)#! Default router is ASA Inside Interface
Router(config)#ip route 0.0.0.0 0.0.0.0 192.168.20.254
Router(config)#clock timezone PST -8
Router(config)#clock summer-time PST recurring

Router#! Set clock to current time
Router#clock set 10:10:00 15 oct 2010

Router(config)#ntp source GigabitEthernet0/1
Router(config)#ntp master 2

Router(config)#ip http server
Router(config)#ip domain-name cisco.com
```

（注） クロックを手動で設定して Cisco Unified CME ルータの時刻に合わせていない場合は、NTP の同期化は失敗します。

ステップ 2 CA サーバとして Cisco Unified CME を設定します。次の設定例では、CA サーバとして設定される Cisco Unified CME を示します。

例：

```
Router(config)#crypto pki server cme_root
Router(config)#database level complete
Router(cs-server)#database url nvram:
Router(cs-server)#grant auto
Router(cs-server)#lifetime certificate 7305
Router(cs-server)#lifetime ca-certificate 7305
Router(cs-server)#exit

Router(config)#crypto pki trustpoint cme_root
Router(ca-trustpoint)# enrollment url http://192.168.20.1:80
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# rsakeypair cme_root
Router(cs-server)#exit

Router(config)# crypto pki server cme_root
Router(cs-server)#no shutdown
%Some server settings cannot be changed after CA certificate generation.
% Please enter a passphrase to protect the private key
% or type Return to exit
Password: *****
Re-enter password: ****
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)
Mar 10 16:44:00.576: %SSH-5-ENABLED: SSH 1.99 has been enabled% Exporting Certificate
Server signing certificate and keys...
% Certificate Server enabled.
Router(cs-server)#
Mar 10 16:44:41.812: %PKI-6-CS_ENABLED: Certificate server now enabled.
```

ステップ 3 別のトラストポイントを作成し、トラストポイントを認証し、CA で登録します。

例：

```
Router(config)#crypto pki trustpoint cme_cert
Router(ca-trustpoint)# enrollment url http://192.168.20.1:80
Router(ca-trustpoint)# revocation-check none
Router(ca-trustpoint)# exit
Router(config)# crypto pki authenticate cme_cert
Certificate has the following attributes:
Fingerprint MD5: 995C157D AABB8EE2 494E7B35 00A75A88
Fingerprint SHA1: F934871E 7E2934B1 1C0B4C9A A32B7316 18A5858F
% Do you accept this certificate? [yes/no]: yes
Trustpoint CA certificate accepted.
Router(config)# crypto pki enroll cme_cert
%
% 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 your password will not be saved in the
configuration. Please make a note of it.
Password:
Jan 20 16:03:24.833: %CRYPTO-6-AUTOGEN: Generated new 512 bit key pair
Re-enter password:
% The subject name in the certificate will include: CME1.cisco.com
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose cme_cert' command will show the fingerprint.
! Verify Certificates
```

証明書の確認（任意）

証明書を確認するには、Cisco Unified CME ルータで **show crypto pki certificates** コマンドを使用します。

例：

```
Router#sh crypto pki certificates
Certificate
  Status: Available
  Certificate Serial Number (hex): 07
  Certificate Usage: General Purpose
  Issuer:
    cn=cme_root
  Subject:
    Name: CME1.cisco.com
    hostname=CME1.cisco.com
  Validity Date:
    start date: 15:32:23 PST Apr 1 2010
    end   date: 09:44:00 PST Mar 10 2030
  Associated Trustpoints: cisco2
  Storage: nvram:cme_root#7.cer

Certificate
  Status: Available
  Certificate Serial Number (hex): 06
  Certificate Usage: General Purpose
  Issuer:
    cn=cme_root
  Subject:
    Name: CME1.cisco.com
    hostname=CME1.cisco.com
  Validity Date:
    start date: 15:30:11 PST Apr 1 2010
    end   date: 09:44:00 PST Mar 10 2030
  Associated Trustpoints: cisco1
  Storage: nvram:cme_root#6.cer

Certificate
  Status: Available
  Certificate Serial Number (hex): 02
  Certificate Usage: General Purpose
  Issuer:
    cn=cme_root
  Subject:
    Name: CME1.cisco.com
    hostname=CME1.cisco.com
  Validity Date:
    start date: 08:47:42 PST Mar 10 2010
    end   date: 09:44:00 PST Mar 10 2030
  Associated Trustpoints: cme_cert
  Storage: nvram:cme_root#2.cer

CA Certificate
  Status: Available
  Certificate Serial Number (hex): 01
  Certificate Usage: Signature
  Issuer:
    cn=cme_root
  Subject:
    cn=cme_root
  Validity Date:
    start date: 08:44:00 PST Mar 10 2010
    end   date: 09:44:00 PST Mar 10 2030
  Associated Trustpoints: cisco2 cisco1 cme_cert cme_root
  Storage: nvram:cme_root#1CA.cer
```

電話機の登録と電話機ファームウェアの確認

ステップ 1 電話機の登録の詳細を確認するには、**show ephone** コマンドを使用します。

例：

```
Router# Show ephone
ephone-1[0] Mac:0022.555E.00F1 TCP socket:[2] activeLine:0 whisperLine:0 REGISTERED in
SCCP ver 19/17 max_streams=5 mediaActive:0 whisper_mediaActive:0 startMedia:0 offhook:0
ringing:0 reset:0 reset_sent:0 paging 0 debug:0 caps:9
IP:192.168.11.4 * 49269 7965  keepalive 0 max_line 6 available_line 6
button 1: cw:1 ccw:(0 0) dn 1  number 1001 CH1    IDLE         CH2    IDLE
Preferred Codec: g711ulaw
Lpcor Type: none
```

（注） 電話機に正しいファームウェアがインストールされ、電話機が Cisco Unified CME でローカルに登録されているかどうかを確認します。

ステップ 2 電話機ファームウェアを確認するには、**show ephone phone load** コマンドを使用します。

例：

```
Show ephone phoneload
DeviceName        CurrentPhoneload       PreviousPhoneload      LastReset

SEP0016C7EF9B13    9.0(1TD1.36S)          9.0(1TD1.36S)         UCM-closed-TCP
```

SSL VPN 用の ASA（ゲートウェイ）の設定

ステップ 1 インターフェイス、IP ルーティング、および NTP を設定します。

```
ciscoasa(config)# Interface Ethernet0/1
ciscoasa(config-if)# nameif Inside
ciscoasa(config-if)# description INTERFACE CONNECTED TO CUCME
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 192.168.20.254 255.255.255.0


ciscoasa(config)# interface Ethernet 0/0
ciscoasa(config-if)# description INTERFACE CONNECTED TO WAN
ciscoasa(config-if)# nameif Outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 9.10.60.254 255.255.255.0
ciscoasa(config)# router ospf 100
ciscoasa(config-router)network 9.10.60.0 255.255.255.0 area 1


ciscoasa(config-if)# ntp server 192.168.20.1
```

ステップ 2　ASA 上にトラストポイントを作成し、CME（CA）の証明書を取得します。

```
ciscoasa(config)#crypto key generate rsa label cmeasa
ciscoasa(config)#crypto ca trustpoint asatrust
ciscoasa(config)#! Enrollment URL = CA Server = CUCME
ciscoasa(config-ca-trustpoint)#enrollment url http://192.168.20.1:80
ciscoasa(config-ca-trustpoint)#subject-name cn=cmeasa.cisco.com
ciscoasa(config-ca-trustpoint)#crl nocheck
ciscoasa(config-ca-trustpoint)#keypair cmeasa

ciscoasa (config)# crypto ca authenticate asatrust
INFO: Certificate has the following attributes:
Fingerprint: 27d00cdf 1144c8b9 90621472 786da0cf
Do you accept this certificate? [yes/no]: yes
! Enroll the Trustpoint
ciscoasa(config)# crypto ca enroll asatrust
% 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 your password will not be saved in the configuration.
Please make a note of it.
Password: ********
Re-enter password: ********
% The subject name in the certificate will be: cn=cmeasa.cisco.com
% The fully-qualified domain name in the certificate will be: ciscoasa.cisco.com
% Include the device serial number in the subject name? [yes/no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
ciscoasa(config)# The certificate has been granted by CA!
ciscoasa# show crypto ca certificates
```

ステップ 3　証明書の確認（任意）

証明書を確認するには、ASA ルータで **show crypto ca certificate** コマンドを使用します。

例：

```
ciscoasa# show crypto ca certificate
Certificate
  Status: Available
  Certificate Serial Number: 03
  Certificate Usage: General Purpose
  Public Key Type: RSA (1024 bits)
  Issuer Name:
    cn=cme_root
  Subject Name:
    hostname=ciscoasa.cisco.com
    cn=cmeasa.cisco.com
  Validity Date:
    start date: 09:04:40 PST Mar 10 2010
    end   date: 08:44:00 PST Mar 10 2030
  Associated Trustpoints: asatrust

CA Certificate
  Status: Available
  Certificate Serial Number: 01
  Certificate Usage: Signature
  Public Key Type: RSA (1024 bits)
  Issuer Name:
    cn=cme_root
  Subject Name:
    cn=cme_root
  Validity Date:
    start date: 08:44:00 PST Mar 10 2010
    end   date: 08:44:00 PST Mar 10 2030
  Associated Trustpoints: asatrust
```

ステップ 4　SSL パラメータを設定します。

```
ciscoasa(config)# ssl encryption 3des-sha1 aes128-sha1 aes256-sha1 des-sha1 null-sha1
ciscoasa(config)#
ciscoasa(config)# ssl trust-point asatrust
ciscoasa(config)# ssl trust-point asatrust inside
ciscoasa(config)# ssl trust-point asatrust outside
ciscoasa(config)# no ssl certificate-authentication interface outside port 443
ciscoasa(config)# ssl certificate-authentication interface inside port 443
```

ステップ 5　ローカル IP アドレス プールを設定します。

```
ciscoasa(config)#ip local pool SSLVPNphone_pool 192.168.20.50-192.168.20.70 mask
255.255.255.0
```

ステップ 6　VPN を介した NAT トラフィックを回避するために、アクセス リストを設定します。

```
ciscoasa(config)# access-list no_nat_to_vpn extended permit ip any 9.10.60.0 2$
ciscoasa(config)# nat (inside) 0 access-list no_nat_to_vpn
```

ステップ 7 VPN を設定します。VPN の設定の詳細については、http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/svc.html を参照してください。

```
ciscoasa(config-webvpn)# enable inside
INFO: WebVPN and DTLS are enabled on 'Inside'.
ciscoasa(config-webvpn)# enable outside
INFO: WebVPN and DTLS are enabled on 'Outside'.
ciscoasa(config-webvpn)# svc image disk0:/anyconnect-win-2.4.1012-k9.pkg 1
ciscoasa(config-webvpn)# svc enable
ciscoasa(config-webvpn)# group-policy SSLVPNphone internal
ciscoasa(config)# group-policy SSLVPNphone attribute
ciscoasa(config-group-policy)# banner none
ciscoasa(config-group-policy)# vpn-simultaneous-logins 10
ciscoasa(config-group-policy)# vpn-idle-timeout none
ciscoasa(config-group-policy)# vpn-session-timeout none
ciscoasa(config-group-policy)# vpn-tunnel-protocol svc webvpn
ciscoasa(config-group-policy)# address-pools value SSLVPNphone_pool
ciscoasa(config-group-policy)# webvpn
ciscoasa(config-group-webvpn)# svc dtls enable
ciscoasa(config-group-webvpn)# svc keepalive 120
ciscoasa(config-group-webvpn)# svc ask none
ciscoasa(config-group-webvpn)#
```

ステップ 8 SSL VPN トンネルを設定します。詳細については、http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/vpngrp.html を参照してください。

```
ciscoasa(config)# tunnel-group SSLVPN_tunnel type remote-access
ciscoasa(config)# tunnel-group SSLVPN_tunnel general-attributes
ciscoasa(config-tunnel-general)#
ciscoasa(config-tunnel-general)#
ciscoasa(config-tunnel-general)# address-pool SSLVPNphone_pool
ciscoasa(config-tunnel-general)# default-group-policy SSLVPNphone
ciscoasa(config-tunnel-general)# tunnel-group SSLVPN_tunnel webvpn-attributes
ciscoasa(config-tunnel-webvpn)# group-url https://9.10.60.254/SSLVPNphone enable
```

ステップ 9 Cisco Unified CME の音声 VLAN へのスタティック ルートをイネーブルにします。詳細については、http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/route_static.html を参照してください。

```
ciscoasa(config)# route Inside 192.168.11.0 255.255.255.0 192.168.20.254 1
```

ステップ 10 ユーザに対して ASA ローカル データベースを設定します。詳細については、次のサイトを参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa82/configuration/guide/access_aaa.html#wpmkr1083932

```
ciscoasa(config)# username anyone password cisco
ciscoasa(config)# username anyone attributes
ciscoasa(config-username)# vpn-group-policy SSLVPNphone
ciscoasa(config-username)# vpn-tunnel-protocol IPSec l2tp-ipsec svc webvpn
ciscoasa(config-username)# webvpn
ciscoasa(config-username-webvpn)# svc dtls enable
ciscoasa(config-username-webvpn)# svc ask none
```

ステップ 11 ASA メディア間トラフィックをイネーブルにします。

```
ciscoasa(config)# same-security-traffic permit inter-interface
ciscoasa(config)# same-security-traffic permit intra-interface
```

Cisco Unified CME での VPN グループおよびプロファイルの設定

Cisco Unified CME で VPN グループおよびプロファイルを設定するには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **voice service voip**
4. **vpn-group** *tag*
5. **vpn-gateway** [*number* | url]
6. **vpn-trustpoint {[*number* [raw | trustpoint]}**
7. **vpn-hash-algorithm** *sha-1*
8. **exit**
9. **vpn-profile** *tag*
10. **host-id-chec**k **[enable | disable]**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**voice service voip** **例：** `Router(config)#voice service voip`	Voice over IP コンフィギュレーション モードを開始します。
ステップ 4	**vpn-group** *tag* **例：** `Router (conf-voi-serv)#vpn-group 1`	Voice over IP コンフィギュレーション モードで vpn-group モードを開始します。 • *tag* : vpn-group タグ。範囲：1 または 2。
ステップ 5	**vpn-gateway [** *number* **| url]** **例：** `Router(conf-vpn-group)#vpn-gateway 1 https://9.10.60.254/SSLVPNphone`	VPN のゲートウェイ URL を定義できます。 • *number* : VPN ゲートウェイとして定義できるゲートウェイの数。範囲は 1 ～ 3 です。 • url : VPN ゲートウェイの URL。

ステップ 6	**vpn-trustpoint** {[*number* [**raw** | **trustpoint**]}
	
	例：
	`Router(conf-vpn-group)#vpn-trustpoint ?`
	`vpn-trustpoint 1 trustpoint cme_cert root`
		VPN ゲートウェイ トラストポイントを入力できます。
		• *number* : 使用できるトラストポイントの数。範囲：1 ～ 10。
		• **raw** : VPN ゲートウェイ トラストポイントを raw 形式で入力できます。
		• **trustpoint** : IOS 形式で作成された VPN ゲートウェイ トラストポイントを入力できます。

ステップ 7	**vpn-hash-algorithm** *sha-1* **例：** `Router(conf-vpn-group)#vpn-hash-algorithm sha-1`	VPN ゲートウェイ トラストポイントの vpn hash 暗号化を入力できます。 • *sha-1* : 暗号化アルゴリズム。
ステップ 8	**exit** **例：** `Router(conf-vpn-group)#exit`	VPN-group コンフィギュレーション モードを終了します。
ステップ 9	**vpn-profile** *tag* **例：** `Router (conf-voi-serv)#vpn-profile 1`	VPN-profile コンフィギュレーション モードを開始します。 *tag* : VPN プロファイル タグ番号。範囲：1 ～ 6。

	コマンドまたはアクション	目的
ステップ 10	**host-id-check [enable | disable]** **例：** `Router(conf-vpn-profile)#host-id-check disable`	VPN プロファイルでホスト ID チェック オプションを設定できます。 • disable：ホスト ID チェック オプションをディセーブルにします。 • enable：ホスト ID チェック オプションをイネーブルにします。デフォルトは enable です。
ステップ 11	**end** **例：** `Router(conf-vpn-profile)#end`	特権 EXEC モードに戻ります。

VPN グループおよびプロファイルの SCCP IP Phone への関連付け

VPN グループおよびプロファイルを SCCP IP Phone に関連付けるには、次の手順を実行します。

手順の概要

1. **enable**
2. **configure terminal**
3. **telephony-service**
4. **cnf-file perphone**
5. **ephone** ***phone-tag***
6. **device-security-mode** {authenticated | none | encrypted}
7. **mac-address** [mac-address]
8. **type** *phone-type* **[addon 1** *module-type* **[2** *module-type***]]**
9. **vpn-group** *tag*
10. **vpn-profile** *tag*
11. **button button-number**{separator}***dn-tag [,dn-tag...][button-number{x}overlay-button-number] [button-number...]***
12. **exit**
13. **telephony-service**
14. **create cnf-file**
15. **exit**
16. **ephone** *phone-tag*
17. **reset**
18. **end**

	コマンドまたはアクション	目的
ステップ 1	**enable** **例：** `Router> enable`	特権 EXEC モードをイネーブルにします。プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** **例：** `Router# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**telephony-service** **例：** `Router#(config)telephony-service`	telephony-service コンフィギュレーション モードを開始します。
ステップ 4	**cnf-file perphone** **例：** `Router(config-telephony)# create cnf-files`	IP Phone で必要とされる XML コンフィギュレーション ファイルを構築します。
ステップ 5	**ephone** *phone-tag* **例：** `Router(config)# ephone 1`	ephone コンフィギュレーション モードを開始して、SCCP 電話機の電話機固有のパラメータを設定します。 • *phone-tag*：電話機を識別する一意のシーケンス番号。範囲はバージョンとプラットフォームに依存します。範囲を表示するには、? と入力します
ステップ 6	**device-security-mode {**authenticated | none | encrypted} **例：** `Router(config-telephony)# device-security-mode none`	エンドポイントのセキュリティ モードをイネーブルにします。 • authenticated：暗号化なしで TLS 接続を確立するようにデバイスに指示します。メディア パスにセキュアな Real-Time Transport Protocol（SRTP）がありません。 • none：SCCP シグナリングはセキュアではありません。これがデフォルトです。 • encrypted：デバイスに、SRTP を使用してセキュアなメディア パスへの暗号化された TLS 接続を確立するように指示します。 • ephone コンフィギュレーション モードでこのコマンドに設定された値は、telephony-service コンフィギュレーション モードで設定された値よりも優先されます。
ステップ 7	**mac-address** [mac-address] **例：** `Router(config-ephone)#mac-address 0022.555e.00f1`	設定される IP Phone の MAC アドレスを指定します

	コマンドまたはアクション	目的
ステップ 8	**type** phone-type [addon 1 module-type [2 module-type]] **例：** Router(config-ephone)# type 7965	電話機のタイプを指定します。 • Cisco Unified CME 4.0 以降のバージョン：アドオン モジュールを適用できるタイプは、7960、7961、7961GE、および 7970 のみです。 • Cisco CME 3.4 以前のバージョン：アドオン モジュールを適用できるタイプは 7960 だけです。
ステップ 9	**vpn-group** *tag* **例：** Router (conf-voi-serv)#vpn-group 1	Voice over IP コンフィギュレーション モードで vpn-group モードを開始します。 • *tag*：vpn-group タグ。範囲：1 または 2。
ステップ 10	**vpn-profile** *tag* **例：** Router (conf-voi-serv)#vpn-profile 1	VPN-profile コンフィギュレーション モードを開始します。 • *tag*：VPN プロファイル タグ番号。範囲：1 ～ 6。デフォルト：
ステップ 11	**button** button-number{separator}*dn-tag* [,dn-tag...][button-number{x}overlay-button-number] [button-number...] **例：** Router(config-ephone)# button 1:5	ボタン番号と回線の特性を ephone-dn に関連付けます。ボタンの最大数は電話機のタイプによって決まります。
ステップ 12	**exit** **例：** Router(config-ephone)exit	ephone コンフィギュレーション モードを終了します。
ステップ 13	**telephony-service** **例：** Router(config)# telephony-service	telephony-service コンフィギュレーション モードを開始します。
ステップ 14	**create cnf-file** **例：** Router(config-telephony)# create cnf-files	IP Phone で必要とされる XML コンフィギュレーション ファイルを構築します。
ステップ 15	**exit** **例：** Router(Config-telepony)exit	telephony service コンフィギュレーション モードを終了します。
ステップ 16	**ephone** *phone-tag* **例：** Router(config)# ephone 1	ephone コンフィギュレーション モードを開始します。 • *phone-tag*：設定タスク中にこの ephone を識別する一意のシーケンス番号。

	コマンドまたはアクション	目的
ステップ 17	**reset** **例：** `Router(config-ephone)# reset`	設定される個々の SCCP 電話機の完全なリブートを実行します。
ステップ 18	**end** **例：** `Router(config-ephone)# end`	特権 EXEC モードに戻ります。

電話機での代替 TFTP アドレスの設定

ステップ 1 電話機から、次のように操作します。

```
Settings->Network Configuration->IPv4 Configuration->Alternate TFTP
Press **# to unlock
Select YES

If the phone is already registered, "TFTP Server 1" will already be populated.  Otherwise,
enter the CUCME address as the alternate TFTP Server 1.
```

ステップ 2 電話機の設定を保存します。

ステップ 3 電話機から VPN がイネーブルになっていることを確認します。

```
Press Settings -> Security Configuration -> VPN
When you press "Enable" from this menu, it should prompt for username and password.
```

ステップ 4 電話機から、次のように操作します。

```
Settings->Network Configuration->IPv4 Configuration->Alternate TFTP.
Press **# to unlock and select YES.

If the phone is already registered, "TFTP Server 1" will already be populated. Otherwise,
enter the CUCME address as the alternate TFTP Server 1.
```

ステップ 5 設定を保存します。

ステップ 6 自宅またはリモート サイトから電話機をネットワークに接続します。

```
Select Settings ->Security Settings ->VPN Configurations?
Enable VPN
Enter Username and Password. Phone will register with CUCME
```

リモート サイトからの電話機の登録

リモート サイトから Cisco Unified IP Phone を登録するには、次の手順を実行します。

ステップ 1 自宅またはリモート サイトから電話機をネットワークに接続します。電話機が DHCP を受信します。

ステップ 2 電話機のメニューから [設定（Settings）] を選択し、[セキュリティ設定（Security Settings）] に移動します。

ステップ 3 [VPN の設定（VPN Configurations）] を選択します。次に [VPN の有効化（Enable VPN）] を選択します。

ステップ 4 ユーザ名とパスワードを入力します。これで電話機が Cisco Unified CME に登録されます。

Cisco Unified CME での DTLS による SSL VPN クライアントの設定

始める前に、基本 SSL VPN 設定を Cisco Unified CME で行ったことを確認します（「Cisco Unified CME での基本設定」（P.1447）を参照）。

SCCP IP Phone で DTLS による SSL VPN クライアントを設定するには、次の手順を表示されている順に実行します。

1. 「クロック、ホスト名、およびドメイン名のセットアップ」（P.1468）
2. 「トラストポイントの設定と証明書での登録」（P.1469）
3. 「VPN ゲートウェイでのトラストポイント（デフォルト以外）の設定」（P.1469）
4. 「ユーザ データベースの設定」（P.1469）
5. 「仮想ゲートウェイの設定」（P.1469）
6. 「仮想コンテキストの設定」（P.1470）
7. 「グループ ポリシーの設定」（P.1470）
8. 「IOS SSL VPN 接続の確認」（P.1471）
9. 「SSL VPN 用の Cisco Unified SCCP IP Phone の設定」（P.1471）
10. 「Cisco Unified SCCP IP Phone の設定」（P.1472）
11. 「Cisco Unified CME での SSL VPN の設定」（P.1473）

（注） 設定することを選択した認証のタイプによって、設定のステップ 3 ～ステップ 11 はここに記載されている方法とはやや異なる場合があります。

クロック、ホスト名、およびドメイン名のセットアップ

クロック、ホスト名、およびドメイン名をセットアップする必要があります。

ステップ 1 次に、設定されたホスト名とドメイン名の例を示します。

```
hostname Router2811
ip domain name cisco.com

Interfaces on the Router_2811:

interface FastEthernet0/0
 ip address 1.5.37.13 255.255.0.0
 duplex auto
 speed auto

interface FastEthernet0/1
 ip address 30.0.0.1 255.255.255.0
 duplex auto
 speed auto
```

ステップ 2 IOS のクロックを表示します。

```
Router#show clock
*10:07:57.109 pacific Thu Oct 7 2010
```

a. クロックを直接設定：

```
Router#clock set 9:53:0 Oct 7 2010

Set time zone (Pacific Standard Time)
Router#configure terminal
Router(config)#clock timezone pst -8

(optional)
Set summer-time
Router#configure terminal

Router(config)#clock summer-time pst recurring

Or

Router(config)#
clock summer-time pst date apr 11 2010 12:00 nov 11 2010 12:00
```

b. NTP を使用してクロックを設定：

```
Router(config)#ntp server 192.18.2.1
Router(config)#ntp master 2
```

トラストポイントの設定と証明書での登録

トラストポイントを設定して証明書サーバに登録するには、「CA サーバとしての Cisco Unified CME の設定」（P.1453）を参照してください。webvpn で生成されるデフォルトの自己署名証明書を使用することもできます。このデフォルトの**トラストポイント**は、**webvpn gateway *gateway name*** コマンドが初めて入力されたときに生成されます。

（注） IOS SSL VPN の DTLS は、SSL 認証中に子証明書を使用するため、「vpn-trustpoint」の設定時に「リーフ」オプションを選択する必要があります。

VPN ゲートウェイでのトラストポイント（デフォルト以外）の設定

WebVPN ゲートウェイはデフォルトのトラストポイント名 SSL VPN を使用します。Web VPN ゲートウェイに別の名前のトラストポイントを使用するように指示するには、次の設定を使用します。

```
Router(config)#webvpn gateway GW1
Router(config-webvpn-gateway)#ssl trustpoint <trustpoint-name>
```

（注） webvpn 自体が生成するトラストポイントではなく、Cisco Unified CME が生成するトラストポイントを使用することを推奨します。

ユーザ データベースの設定

1. ローカル データベースを次のように設定します。

```
Router(config)#aaa new-model
username anyone password 0 cisco
aaa authentication login default local
```

2. 認証用にリモート AAA RADIUS サーバを次のように設定します。

```
Router(config)#aaa new-model
aaa authentication login default group radius
radius-server host 172.19.159.150 auth-port 1923 acct-port 1924
radius-server key cisco
```

詳細については、次のサイトを参照してください。

http://www.cisco.com/en/US/docs/security/asa/asa71/configuration/guide/aaa.html#wp1062044

仮想ゲートウェイの設定

「webvpn gateway <name>」と入力すると、自己署名証明書が生成されます。IP アドレスは、WebVPN ゲートウェイ上のインターフェイスまたはループバック インターフェイスで設定されたパブリック IP アドレスにする必要があります。次に、WebVPN ゲートウェイ上で設定されたパブリック IP アドレスの例を示します。

```
Router(config)#webvpn gateway sslvpn_gw
Router(config-webvpn)# ip address 1.5.37.13 port 443
 ssl encryption 3des-sha1 aes-sha1
 ssl trustpoint R2811_cert
 inservice
```

仮想コンテキストの設定

ユーザは WebVPN ゲートウェイへのアクセス時に、https://1.5.37.13/SSLVPNphone のように URL に「ドメイン名」を指定することにより、仮想コンテキストにアクセスできます。次に、設定された仮想 VPN コンテキストの例を示します。

```
Router(config)# webvpn context sslvpn_context
 ssl encryption 3des-sha1 aes-sha1
 ssl authenticate verify all
 gateway sslvpn_gw domain SSLVPNphone
 inservice
```

```
When inservice was entered, the system prompted: 000304: Jan  7 00:30:01.206:
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
```

グループ ポリシーの設定

電話機の SSL VPN クライアントはフルトンネル モードで動作するため、WebVPN ゲートウェイはゲートウェイにログインする各クライアントに IP アドレスを提供します。次を設定します。

```
ip local pool SSLVPNphone_pool 30.0.0.50 30.0.0.70
webvpn context sslvpn_context
 ssl encryption 3des-sha1 aes-sha1
 ssl authenticate verify all
 !
 !
 policy group SSLVPNphone
   functions svc-enabled
   hide-url-bar
   svc address-pool "SSLVPNphone_pool"
   svc default-domain "cisco.com"
 default-group-policy SSLVPNphone
 no aaa authentication domain local
 gateway sslvpn_gw domain SSLVPNphone
 authentication certificate
 ca trustpoint <trust point name>
 inservice
```

IOS SSL VPN 接続の確認

ステップ 1 PC のブラウザ（MS Internet Explorer）で、https://1.5.37.13/SSLVPNphone に接続して証明書を受け入れます。ログインするには、ユーザ名とパスワード（anyone と cisco）を入力します。IOS SSL VPN のホーム ページが表示されるはずです。

ステップ 2 IOS WebVPN のデバッグ：

PC のブラウザから https://1.5.37.13/SSLVPNphone で IOS（1.5.37.x ネットワーク上）に接続します。デフォルトのバナーがポップアップします。ユーザ名とパスワードを入力します。

```
debug ssl openssl errors
debug ssl openssl msg
debug ssl openssl states

debug webvpn sdps
debug webvpn aaa (login authentication)

debug webvpn http verbose (for authentication)
debug webvpn webservice verbose
debug webvpn tunnel

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

ステップ 3 デフォルトの IP ルートを、たとえば、次のように指定します。

```
Router (c3745): ip route 30.0.0.0 255.255.255.0 FastEthernet0/0
Router (c3745): ip route 10.0.0.0 255.255.255.0 1.5.37.11
```

（この制限されたルートを強制的に使用する必要があり、そうしないと失敗します）

SSL VPN 用の Cisco Unified SCCP IP Phone の設定

ステップ 1 電話機ファームウェアは、『*Cisco Unified Communications Manager Express Introduction*』でダウンロードできます。

ステップ 2 [互換性情報（Compatibility Information）] を選択します。

ステップ 3 電話機に該当する電話機ファームウェア バージョンを選択します。

汎用ソフトウェアのダウンロードは『*Product/Technology Support*』でも入手できます。[音声およびユニファイド コミュニケーション（Voice and Unified Communications）] > [IP テレフォニー（IP Telephony）] > [IP Phones] を選択します。

（注） 電話機ファームウェア バージョン 8.3 を電話機ファームウェア バージョン 9.0 にアップグレードする前に、電話機ファームウェア バージョン 8.4 をダウンロードすることを推奨します。電話機ファームウェア バージョンを 8.4 にアップグレードしないで電話機ファームウェアを 9.0 にアップグレードしても機能しません。詳細については、『*Firmware Upgrade Issues for SCCP*』を参照してください。

ステップ 4 ハード リセット（電源投入時に # を押します）後に、term65.default.loads を使用して、残りのイメージをロードできます。

Cisco Unified SCCP IP Phone の設定

ステップ 1 [設定（Settings）] > [セキュリティ設定（Security configuration）]（4）> [VPN の設定（VPN Configuration）]（8）に移動します。

ステップ 2 VPN コンセントレータの IP アドレスを調べます。VPN ヘッドエンドをポイントしている必要があります。

ステップ 3 代替 TFTP を確認します（[設定（Settings）] > [ネットワークの設定（Network Configuration）] > [IPv4 設定（IPv4 Configuration）]）。手動で TFTP サーバ アドレスを入力するには、[代替 TFTP（Alternate TFTP）] オプションを [はい（Yes）] に設定します。関連付ける IP アドレスは、Cisco Unified CME の IP アドレスです。

ステップ 4 VPN 設定を「enable」に設定します。ユーザ インターフェイスに「VPN 接続試行中 ...（Attempting VPN Connection...）」と表示されます。

ステップ 5 VPN 接続が確立していることを確認します。[設定（Settings）] > [ネットワークの設定（Network Configuration）] に移動します。「VPN」ラベルに「接続しました（connected）」と表示されます。

（注） セキュア モードで電話機を使用する場合は、**capf-ip-in-cnf** コマンドを ephone コンフィギュレーション モードで必ず追加してください。

Cisco Unified CME での SSL VPN の設定

Cisco Unified CME で SSL VPN を設定するには、「Cisco Unified CME での VPN グループおよびプロファイルの設定」（P.1461）を参照してください。

Example:

```
voice service voip
 vpn-group 1
  vpn-gateway 1 https://1.5.37.13/SSLVPNphone
  vpn-trustpoint 1 trustpoint R2811_cert leaf
 vpn-profile 1
  host-id-check disable

crypto pki server R2811_root
 database level complete
 grant auto
 lifetime certificate 7305
 lifetime ca-certificate 7305
crypto pki token default removal timeout 0
!
crypto pki trustpoint R2811_root
 enrollment url http://30.0.0.1:80
 revocation-check none
 rsakeypair R2811_root
!
crypto pki trustpoint R2811_cert
 enrollment url http://30.0.0.1:80
 serial-number
 revocation-check none

telephony-service
 cnf-file perphone

ephone  2
 device-security-mode none
 mac-address 001E.7AC4.DD25
 type 7965
 vpn-group 1
 vpn-profile 1
 button  1:5

telephony-service
 create cnf-files

ephone 2
 reset
```

DTLS による Cisco Unified CME の VPN 電話機の冗長性サポート

VPN 電話機は、IOS および Cisco Unified CME による冗長性を次の 2 とおりの方法によりサポートします。

a. 2 つ以上の vpn-gateway 設定を同じ vpn-group で使用する。

b. Cisco Unified CME の冗長性設定と 1 つ以上の vpn-gateway 設定を使用する。そのためには、vpn-gateway を 1 つだけ使用する場合、DTLS および SSL VPN ヘッドエンド IP が稼働し続ける必要があります。

Cisco Unified CME の冗長性は、トランスポイントをプライマリ CME からセカンダリ CME にインポートすると機能します。
http://www.cisco.com/en/US/docs/ios/security/command/reference/sec_c5.html#wp1044112 を参照してください。冗長 Cisco Unified CME の詳細については、『*Redundant Cisco Unified CME Router*』を参照してください。

エクスポート可能なキーでトラストポイントを生成し、それを sast1 として使用する必要があります。

SSL VPN クライアントの設定例

ここでは、次の例について説明します。

- 「Cisco Unified CME での VPN グループおよびプロファイルの設定：例」（P.1474）
- 「VPN グループおよび VPN プロファイルの SCCP IP Phone への関連付け：例」（P.1475）

Cisco Unified CME での VPN グループおよびプロファイルの設定：例

次の例では、Cisco Unified CME で設定された vpn-group 1 と vpn-profile1 を示します。

```
Router# show running config
!
no ip domain lookup
no ipv6 cef
!
multilink bundle-name authenticated
!
!
voice-card 0
 dsp services dspfarm
!
voice-card 3
 dspfarm
 dsp services dspfarm
!
!
voice service voip
 ip address trusted list
  ipv4 20.20.20.1
 vpn-group 1
  vpn-gateway 1 https://9.10.60.254/SSLVPNphone
  vpn-trustpoint 1 trustpoint cme_cert root
  vpn-hash-algorithm sha-1
 vpn-profile 1
  host-id-check disable
 sip
!
```

VPN グループおよび VPN プロファイルの SCCP IP Phone への関連付け：例

```
ip dhcp pool CME1
   network 192.168.11.0 255.255.255.0
   default-router 192.168.11.1
   option 150 ip 192.168.11.1

telephony-service
 max-ephones 24
 max-dn 24
 ip source-address 192.168.11.1 port 2000
! Each remote phone should have a separate cnf file.
 cnf-file perphone
!Upgrade phone firmware to latest supported load
 load 7965 SCCP45.9-0-1TD1-36S
no shutdown
ephone-dn  1  dual-line
 number 1001

ephone  1
description SSL VPN REMOTE PHONE
 device-security-mode none
 mac-address 0022.555e.00f1
 type 7965
 button  1:1
 vpn-group 1
 vpn-profile 1

ephone  2
 device-security-mode none
 mac-address 001E.be91.37fb
 type 7965
 button  1:5

telephony-service
create cnf-files
!
```

次の例では、VPN 設定を示します。

```
Router #show voice vpn
The Voice Service VPN Group 1 setting:
    VPN Gateway 1 URL https://9.10.60.254/SSLVPNphone
    VPN Trustpoint hash in sha-1
    VPN Trustpoint 1 trustpoint cme_cert root fbUqFIbtWtaYSGSlTP/Umshcgyk= The Voice
Service VPN Profile 1 setting:
    The host_id_check setting: 0
```

その他の参考資料

次の各項では、Cisco Unified CME 機能に関連するその他の資料について説明します。

関連資料

関連項目	参照先
Cisco Unified CME の設定	• *『Cisco Unified Communications Manager Express System アドミニストレータ ガイド』* • *『Cisco Unified Communications Manager Express Command Reference』*
Cisco Unified CME ネットワーク設計	• *『Cisco Unified CallManager Express Solution Reference Network Design Guide』*
Cisco IOS の音声設定	• *『Cisco IOS Voice Configuration Library』* • *『Cisco IOS Voice Command Reference』*
Cisco Unified CME 用の電話機のマニュアル	• *『User Documentation for Cisco Unified IP Phones』*
Cisco Unified IP Phone ファームウェアのリリースノート	• *『Cisco Unified IP Phone Release Notes for Firmware Release 9.0(2)SR1 (SCCP and SIP)』*

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/en/US/support/index.html

SSL VPN クライアントの機能情報

表 134 に、このモジュールで説明した機能、およびバージョンごとの拡張機能を示します。

特定の Cisco Unified CME バージョンをサポートするための適切な Cisco IOS リリースを判断するには、http://www.cisco.com/en/US/docs/voice_ip_comm/cucme/requirements/guide/33matrix.htm にある『*Cisco Unified CME and Cisco IOS Software Version Compatibility Matrix*』を参照してください。

プラットフォームのサポートおよびソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator では、特定のソフトウェア リリース、フィーチャ セット、またはプラットフォームをサポートしている Cisco IOS ソフトウェア イメージを確認できます。Cisco Feature Navigator にアクセスするには、http://www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

（注） 表 134 には、特定の機能に対するサポートを導入した Cisco Unified CME のバージョンが示されています。特に明記されていない限り、Cisco Unified CME ソフトウェアの後続のバージョンでもこの機能をサポートします。

表 134　SSL VPN クライアントの機能情報

機能名	Cisco Unified CME のバージョン	機能情報
DTLS による Cisco Unified CME でのサポート	8.6	DTLS による Cisco Unified CME でのサポートが導入されました。
SCCP IP Phone での SSL VPN クライアントのサポート	8.5	SSL VPN クライアント サポート機能が導入されました。