Cisco VCS 証明書の作成および使用

導入ガイド

最終更新日：2015 年 11 月

ソフトウェア バージョン：X8.7

はじめに

この導入ガイドでは、Cisco TelePresence Video Communication Server（VCS）で使用する X.509 暗号化証明書を作成し、それを VCS にロードする方法について説明します。

PKI の概要

公開キー インフラストラクチャ（PKI）では、セキュアな通信を確立し（暗号化され完全性が保護される）、ID を確認できるメカニズムが提供されます。基本的な PKI は次のとおりです。

- **公開キーと秘密キーのペア**：公開キーを使用してサーバに送信するデータを暗号化します。これを復号化するために使用できるのは、秘密キー（サーバによって秘密に保たれる）のみです。
- **データの署名**：データは、データの暗号化ハッシュとサーバの秘密キーの組み合わせを使用してサーバが「署名」できます。クライアントは、サーバの公開キーを使用して、同じハッシュを確認することにより、シグニチャを確認できます。これにより、データが予期されたサーバから送信され、改ざんされていないことが保証されます。
- **証明書**：証明書は公開キーのラッパーで、キーの所有者に関する情報を提供します。このメタデータは X.509 形式で提供され、通常、所有者のサーバ名と連絡先の詳細が含まれます。
- **証明書チェーン**：証明書には、認証局（CA）が独自の秘密キーを使用して署名できます。したがって、証明書は CA の証明書（公開キー）に対するシグニチャを確認して、証明書が CA によって署名されていることを検証できます。Web ブラウザと他のクライアントには、信用する CA 証明書のリストがあり、個々のサーバの証明書を確認することができます。

Transport Layer Security（TLS）は、TCP/IP ネットワーク上のホスト間のセキュアな TCP 接続を確立する標準メカニズムです。たとえば、セキュアな HTTP（HTTPS）は TLS を使用してトラフィックを暗号化し確認します。TLS 接続を確立するには、次の手順に従います。

1. 最初の TCP 接続が行われると、クライアントがその機能（暗号スイートを含む）と乱数を送信します。
2. サーバはこれらの機能の選択、別の乱数およびその証明書に対応します。
3. クライアントは、サーバ証明書が信頼する CA によって発行（署名）され、廃止されていないことを確認します。
4. クライアントは、サーバの公開キーで暗号化された「プリマスタ シークレット」を送信します。
5. このプリマスタ シークレット（リプレイ アタックを防ぐため交換された乱数と組み合わせたもの）は、「マスター シークレット」を生成するために使用され、このマスター シークレットを使用してこの TLS セッションの残りの通信がクライアントとサーバ間で暗号化されます。

以降の項では、VCS でこれらの PKI コンポーネントを使用する方法について説明します。

VCS での証明書の使用法の概要

VCS には、以下についての証明書が必要です。

- TLS（HTTPS）接続によるセキュアな HTTP
- SIP シグナリング、エンドポイントおよびネイバー ゾーンの TLS 接続
- Unified CM、Cisco TMS、LDAP サーバおよび syslog サーバなどの他のシステムへの接続

信頼できる認証局（CA）の証明書のリストと関連する証明書失効リスト（CRL）を使用して接続している他のデバイスを検証します。

サーバ証明書と秘密キーを使用して署名付きの証明書を提供し、VCS がそのデバイスであるという証拠を示します。これは、Microsoft Lync または Unified CM などの隣接デバイスおよび Web インターフェイスを使用する管理者が使用できます。

証明書で VCS を識別します。これには、それによって認識されトラフィックがルーティングされる名前が含まれます。クラスタの一部である場合など、これらの目的で複数の名前によって VCS が認識されている場合、RFC5922 のガイダンスに従い、X.509 のサブジェクト データ内でこれを表す必要があります。証明書には VCS 自体とクラスタの両方の FQDN が必要です。次のリストには、選択された導入モデルに応じて X.509 サブジェクトに含める必要があるものを示します。

VCS がクラスタ化されていない場合は、次のようになります。

- サブジェクトの共有名 = VCS の FQDN
- サブジェクトの代替名 = 空欄のまま

VCS ごとの個別の証明書により VCS がクラスタ化されている場合は、次のようになります。

- サブジェクトの共有名 = VCS の FQDN
- サブジェクトの代替名 = VCS の FQDN、クラスタの FQDN

ワイルドカード証明書は、サポートする複数のサブドメインとサービス名を管理し、SAN（サブジェクトの代替名）証明書よりも安全度が低い場合があります。VCS はワイルドカード証明書をサポートしていません。

証明書生成の概要

X.509 証明書がサードパーティから提供されることがあります。または、OpenSSL などの証明書発行システムや Microsoft 認証局などのアプリケーションで使用できるツールで生成されることがあります。認識された認証局によって提供されたサードパーティの証明書を推奨します。ただし、管理された環境またはテスト環境での VCS の導入では、内部的に生成された証明書を使用できます。

証明書の生成には通常 3 段階のプロセスがあります。

- ステージ 1：秘密キーの生成

- ステージ 2：証明書要求の作成
- ステージ 3：証明書の承認と作成

このマニュアルでは、ルート証明書、VCS 用のクライアント/サーバ証明書、および秘密キーを生成する代替方法を示します。

- 「証明書署名要求（CSR）の生成」（4 ページ）では、VCS 自体を使用した秘密キーと証明書要求の生成方法について説明します。
- 「付録 2：OpneSSL のみを使用した証明書の生成」（18 ページ）では、サードパーティの CA または内部的に管理された CA で使用できる OpenSSL 専用のプロセスについて説明します。

相互 TLS 認証の場合、VCS の**サーバ**証明書は**クライアント**証明書としても使用可能で、VCS がクライアント デバイスとして隣接サーバに認証できるようにする必要があります（「付録 5：「クライアント証明書およびサーバ証明書を発行するための AD CS の有効化」（26 ページ）」を参照してください。

注：2050 年以降の日付の処理方法に変更が加えられます。そのため、有効期限日がそれ以降の証明書によって運用上の問題が引き起こされる可能性があることに注意してください。

証明書署名要求（CSR）の生成

CSR には、秘密キーの所有者の ID 情報が含まれます。また、署名付き証明書の生成のためにサードパーティまたは内部の認証機関に渡すことができます。また、Microsoft 認証局または OpenSSL などのアプリケーションで使用できます。

VCS を使用した CSR の作成

VCS はサーバの証明書署名要求を生成できます。そのため、証明書要求を生成し、取得するために外部機能を使用する必要はありません。

CSR を生成するには、次の手順を実行します。

1. [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）] に移動します。
2. [CSR の作成（Generate CSR）] をクリックして [CSR の作成（Generate CSR）] ページに移動します。
3. 証明書に必要なプロパティを入力します。
   - VCS がクラスタの一部である場合、「サーバ証明書とクラスタ化システム（5 ページ）」を参照してください。
   - VCS が Unified Communications のソリューションの一部である場合は、「Unified Communications のサーバ証明書の要件（6 ページ）」を参照してください。
   - 証明書要求には、証明書で使用される公開キーと、クライアントおよびサーバ認証の Enhanced Key Usage（EKU）の拡張が自動的に含まれます。

4. [CSR の作成（Generate CSR）] をクリックします。システムが署名要求と関連する秘密キーを生成します。

   VCS に秘密キーが安全に保存され、表示することもダウンロードすることもできません。認証局に対しても秘密キーを開示してはなりません。

5. [サーバ証明書（Server certificate）] ページに戻ります。グローバル設定に関して実行できることは次のとおりです。

   - 認証局に送信できるように、要求をローカル ファイル システムに**ダウンロード**します。ファイルを保存するよう求められます（実際の表現はブラウザによって異なります）。
   - 現在の要求を表示（[表示（復号化）（Show (decoded)）] をクリックして人が判読できる形式で表示するか、または [表示（PEM ファイル）（Show （PEM file））] をクリックして RAW 形式でファイルを表示します。

（注）

- 1 回に 1 つの署名要求だけを進行させることができます。これは、現在の要求に関連付けられている秘密キー ファイルを VCS で追跡する必要があるためです。現在の要求を破棄して新しい要求を開始するには、[CSR の破棄（Discard CSR）] をクリックします。
- バージョン X8.5.1 から、ユーザ インタフェースにダイジェスト アルゴリズムを設定するオプションがあります。デフォルトでは SHA-256 に設定されており、SHA-1、SHA-384、または SHA-512 に変更するオプションがあります。
- 証明書署名要求の保存場所が X8 で変更されました。

  CSR を X7 で生成すると、アプリケーションは **csr.pem** と **privkey_csr.pem** を **/tandberg/persistent/certs** に配置します。

  CSR を X8 で生成すると、アプリケーションは **csr.pem** と **privkey.pem** を **/tandberg/persistent/certs/generated_csr** に配置します。

  X7からアップグレードする場合で 未送信の CSR がある場合は、アップグレードの前にその CSR を破棄し、アップグレード後にもう一度 CSR を生成することを推奨します。

ここで要求を承認し、署名済み PEM 証明書ファイルを生成する必要があります。そのファイルをサードパーティや内部認証機関に渡したり、Microsoft 認証局（「Microsoft 認証局を使用した要求の承認と証明書の生成」（8 ページ）を参照）または OpenSSL（「OpenSSL を使用した認証局としての動作」（20 ページ）を参照）と組み合わせて使用することができます。

署名付きサーバ証明書が認証局から戻ってきたら、「VCS への証明書およびキーのロード」（10 ページ）で説明するように、それを VCS へアップロードする必要があります。

サーバ証明書とクラスタ化システム

CSR の生成時には、1 つの要求および秘密キーの組み合わせがそのピア専用に生成されます。

VCS クラスタがある場合は、ピアごとに個別の署名要求を生成する必要があります。これらの要求はその後、認証局に送信し、返されたサーバ証明書を関連する各ピアにアップロードする必要があります。

正しいサーバ証明書が適切なピアにアップロードされていることを確認する必要があります。そうでないと、各ピアに保存された秘密キーがアップロードされた証明書に対応しません。

ユニファイド コミュニケーションのサーバ証明書要件

Cisco Unified CM の証明書

Mobile & Remote Access で重要な 2 つの Cisco Unified Communications Manager 証明書は、*CallManager* 証明書と *tomcat* 証明書です。これらは Cisco Unified Communications Manager に自動的にインストールされ、デフォルトで自己署名されて同じ一般名（CN）を持ちます。

外部エンドポイントと内部エンドポイント間で最適なエンドツーエンドのセキュリティを達成するため、CA 署名付き証明書の使用を推奨します。ただし、自己署名証明書を使用する場合、この 2 つの証明書には、異なる一般名が必要です。これは、VCS が同じ CN を持つ二つの自己署名証明書を許可しないためです。*CallManager* と *tomcat* の自己署名証明書に VCN の信頼できる CA リストと同じ CN がある場合、そのうちの 1 つのみを信頼できます。その場合、VCS Control と Cisco Unified Communications Manager 間のセキュア HTTP またはセキュア SIP は失敗します。

また、Cisco Collaboration システム リリース 10.5.2 の製品に対する *tomcat* 証明書署名要求を作成する場合、CSCus47235 に注意する必要があります。ノードの FQDN がサブジェクト代替名として証明書にあることを保証するため、この問題を回避する必要があります。*VCS X8.5.2 リリース ノート*に回避策の詳細があります。

VCS 証明書

VCS の証明書署名要求（CSR）ツールでは、VCS でサポートされるユニファイド コミュニケーション機能に適した関連するサブジェクト代替名（SAN）について確認が求められ、組み込まれます。

次の表は、どのユニファイド コミュニケーションの機能にどの CSR 代替名の要素が適用されるかを示します。

CSR SAN 要素	Mobile & Remote Access	Jabber Guest	XMPP フェデレーション
Unified CM 登録ドメイン	✓（VCS Expressway のみ）	X	X
XMPP フェデレーション ドメイン	X	X	✓（VCS Expressway のみ）
IM and Presence のチャット ノード エイリアス（フェデレーテッド グループ チャット）	X	X	✓
Unified CM 電話セキュリティ プロファイル名	✓（VCS Control のみ）	X	X

（注）

- IM や Presence ノードが追加または名前が変更されるなど、チャット ノード エイリアスが追加されたか、または名前が変更されている場合や、新しい TLS フォンのセキュリティ プロファイルが追加されている場合は、新しい VCS Control 証明書を VCS Control 用に作成する必要がある場合があります。

- 新しいチャット ノードがシステムに追加されている場合や Unified CM または XMPP フェデレーション ドメインが変更されている場合は、新しい VCS Express 証明書を作成する必要があります。
- 新しくアップロードされたサーバ証明書を有効にするには、VCS を再起動する必要があります。

VCS Control / VCS Expressway の各機能要件についての詳細は、次のとおりです。

VCS Control サーバ証明書の要件

VCS Control サーバ証明書ではサブジェクト代替名のリストに、次の要素を含める必要があります。

- **Unified CM 電話セキュリティ プロファイル名**：暗号化された TLS 用に設定され、リモート アクセスを必要とするデバイスに使用される Unified CM のすべての**電話セキュリティ プロファイル**の FQDN 形式での名前。FQDN 形式を使用し、複数のエントリをカンマで区切ります。

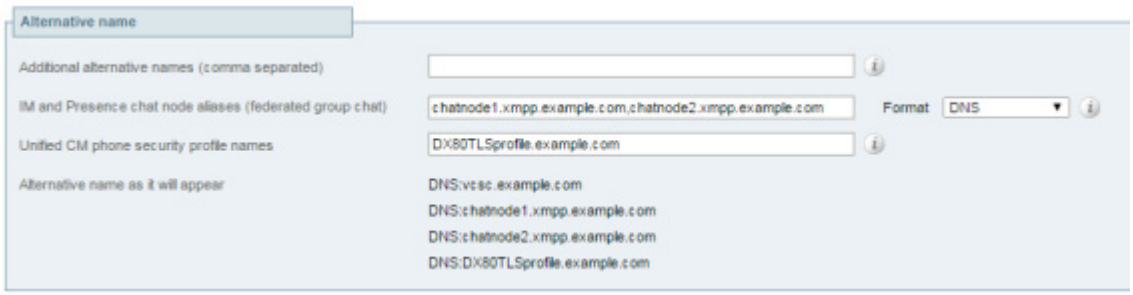
  代替名としてセキュア電話プロファイルを持つことで、これらのプロファイルを使用するデバイスからのメッセージ転送の場合、Unified CM は VCS Control と TLS 経由で通信できます。

- **IM and Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）**：IM and Presence サーバで設定される**チャット ノード エイリアス**（たとえば chatroom1.example.com）。これらは、フェデレーテッド連絡先との TLS を介したグループ チャットをサポートするユニファイド コミュニケーション XMPP フェデレーション導入にのみ必要です。

  VCS Control は一連の IM&P サーバを検出すると、CSR にチャット ノード エイリアスを自動的に含めます。

  CSR を生成するときは、チャット ノード エイリアスに DNS 形式を使用することを推奨します。VCS Expressway サーバ証明書の代替名には、同一のチャット ノード エイリアスを含める必要があります。

図 1：VCS Control の CSR ジェネレータでのセキュリティ プロファイルおよびチャット ノード エイリアスのサブジェクト代替名の入力



VCS Expressway サーバ証明書の要件

VCS Expressway サーバ証明書ではサブジェクト代替名のリストに、次の要素を含める必要があります。

- **[Unified CM 登録ドメイン（Unified CM registrations domains）]**：Unified CM の登録用に VCS Control で設定されているすべてのドメイン。これらはエンドポイント デバイスと VCS Expressway 間のセキュアな通信に必要です。

DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。代わりに *CollabEdgeDNS* 形式を選択すると、入力したドメインにプリフィックス `collab-edge.` が追加されます。この形式は、トップ レベル ドメインを SAN として含めたくない場合に推奨されます（次のスクリーンショットの例を参照してください）。

- **XMPP フェデレーション ドメイン**：ポイントツーポイント XMPP フェデレーションに使用するドメイン。これらは、IM&P サーバで設定され、XMPP フェデレーション用のドメインとして VCS Control でも設定する必要があります。

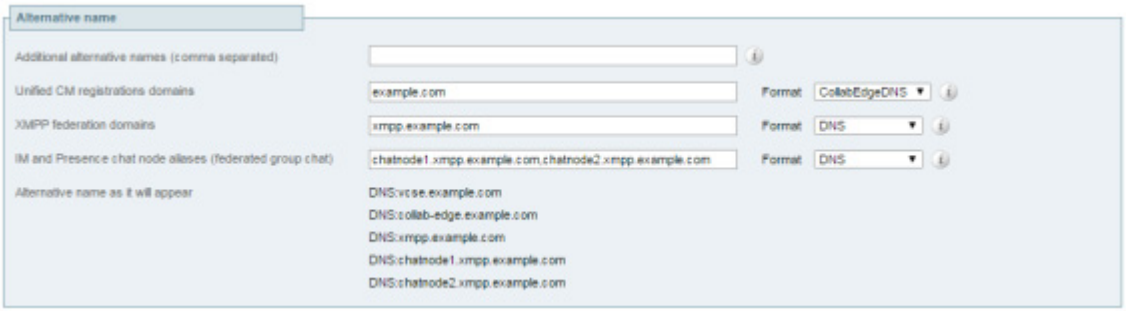
  DNS 形式を選択し、必要な FQDN を手動で指定します。複数のドメインが必要な場合は FQDN をカンマで区切ります。*XMPPAddress* 形式を使用しないでください。この形式は CA によってサポートされない可能性があり、VCS ソフトウェアの将来のバージョンでは廃止される可能性があります。

- **IM および Presence チャット ノード エイリアス（フェデレーテッド グループ チャット）（IM and Presence chat node aliases (federated group chat)）**：VCS Control の証明書で入力されたものと同じ**チャット ノード エイリアス**のセット。フェデレーテッド連絡先との TLS を介したグループ チャットをサポートする音声とプレゼンスの導入にのみ必要です。

  DNS 形式を選択し、必要な FQDN を手動で指定する必要があります。複数のドメインが必要な場合は FQDN をカンマで区切ります。*XMPPAddress* 形式を使用しないでください。この形式は CA によってサポートされない可能性があり、VCS ソフトウェアの将来のバージョンでは廃止される可能性があります。

  VCS コントロールの同等の**[CSR の作成（Generate CSR）]** ページから、チャット ノード エイリアスのリストをコピーできます。

図 2：VCS Expressway の CSR ジェネレータでの Unified CM 登録ドメイン、XMPP フェデレーション ドメイン、およびチャット ノード エイリアスのサブジェクト代替名の入力



Microsoft 認証局を使用した要求の証人と証明書の生成

ここでは、Microsoft 認証局を使用して、証明書要求を承認し PEM 証明書ファイルを生成する方法について説明します。

注：Microsoft Active Directory Certificate Services（AD CS）の CA コンポーネントは、クライアントまたはサーバとして VCS の認証に使用可能な証明書を発行できなければなりません。

Windows Server 2008 Standard R2（および以降）の AD CS では、適切な証明書テンプレートを作成すると、そのようなタイプの証明書を発行できます。**以前のバージョンの Windows Server Standard Edition は適していません。**

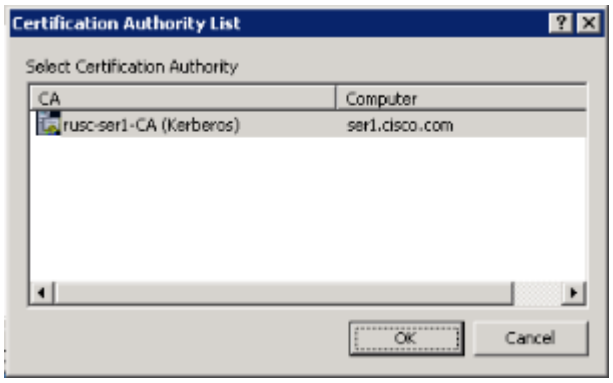
1. 証明書要求ファイル（たとえば、OpenSSL を使用して生成した場合は **certcsr.der**）をデスクトップなどのサーバ上で、Microsoft 認証局アプリケーションがインストールされている場所にコピーします。
2. コマンド プロンプトから証明書要求を送信します。
   - 相互認証でネイバーまたはトラバーサル ゾーンを設定する場合（**TLS 検証モード**）に必要なサーバ認証とクライアント認証で証明書を生成するには、次のように入力します。

     ```
     certreq -submit -attrib "CertificateTemplate:Webclientandserver"
     C:\Users\<user>\Desktop\certcsr.der
     ```

     Webclientandserver 証明書テンプレートの設定方法の詳細については、「付録 5：「クライアントおよびサーバ」証明書を発行するための AD CS の有効化」（26 ページ）を参照してください。
   - サーバ認証のみを使用して証明書を生成するには、次を入力します。

     ```
     certreq -submit -attrib "CertificateTemplate:WebServer" C:\Users\<user>\Desktop\certcsr.der
     ```

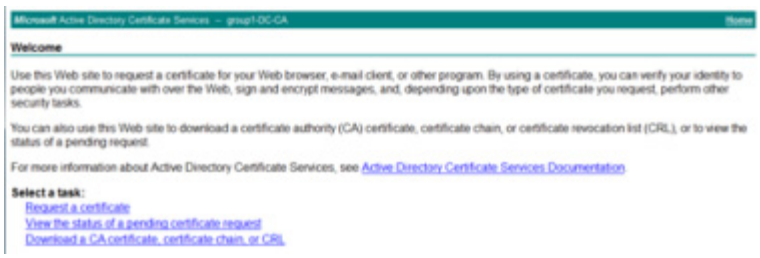
   これにより [認証局（Certification Authority）] ウィンドウが開きます。

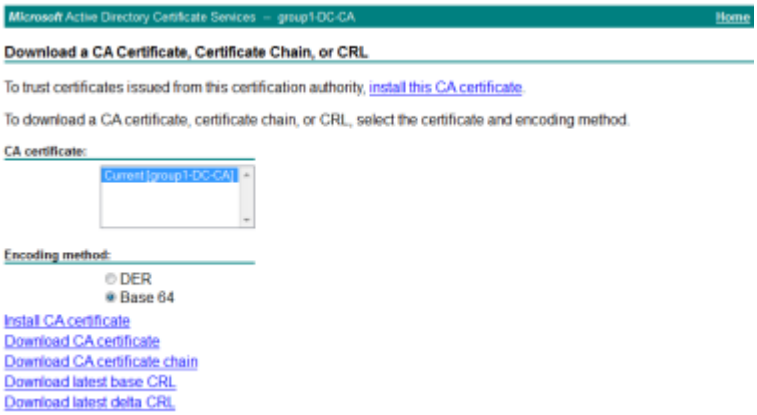
   コマンドは、管理者ユーザとして実行する必要があります。
3. 使用する**認証局**を選択し（通常は 1 つのみ表示）、[OK] をクリックします。
4. 要求された場合は、たとえば、**server.cer** という名前で証明書を保存します（デフォルトの [ライブラリ（Libraries）] > [ドキュメント（Documents）] フォルダを使用しない場合は必要なフォルダを参照）。
5. VCS で使用するには、**server.cer** という名前を **server.pem** に変更します。

Microsoft の CA 証明書の取得

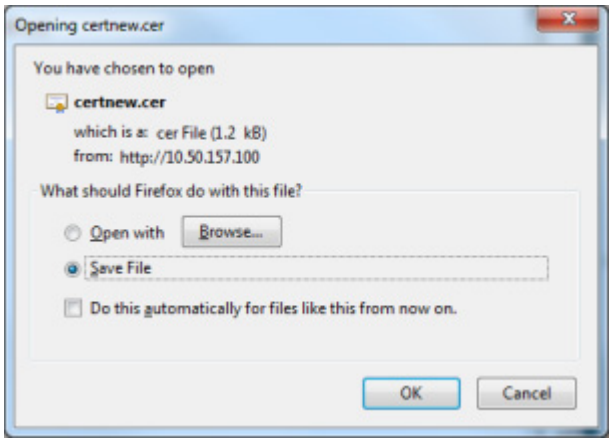
1. Web ブラウザで、[<Microsoft Certificate Server の IP または URL>/certsrv（<IP or URL of the Microsoft Certificate Server>/certsrv）] に移動し、ログインします。

2. [CA 証明書のダウンロード、証明書チェーン、または CRL（Download a CA certificate, certificate chain or CRL）] を選択します。



3. [Base 64] を選択します。.
4. [CA 証明書のダウンロード（Download CA certificate）] を選択します。



5. [ファイルの保存（Save File）] を選択し、[OK] をクリックします。
6. **certnew.cer** という名前を **certnew.pem** に変更します。

これで、ファイル **server.pem** と **certnew.pem** が使用できるようになりました。

このマニュアルの 「VCS への証明書およびキーのロード」（10 ページ）」の項に移動し、**server.pem** と **certnew.pem** を VCS にアップロードします。

VCS への証明書およびキーのロード

VCS は標準の X.590 証明書を使用します。証明書情報は、PEM 形式で VCS に提供する必要があります。通常、次の 3 つの要素がロードされます。

- サーバ証明書（証明書の所有者の ID を識別することで認証局によって生成され、クライアントおよびサーバ両方の証明書として機能できる必要があります）。

- 秘密キー（クライアントに送信されるデータに署名し、サーバ証明書の公開キーで暗号化されたクライアントから送信されたデータを複合化するために使用されます）。これは、VCS 上にのみ保管し、安全な場所にバックアップする必要があります。TLS 通信のセキュリティは、この保持された秘密に依存します。
- 信頼できる認証局の証明書のリスト。

注：新しい VCS ソフトウェアのインストール（X8.1 以降）には、一時的に信頼された CA と、その一時的な CA が発行するサーバ証明書が付属しています。サーバ証明書を信頼できる認証局により生成された証明書に置き換え、信頼する認証局の CA 証明書をインストールすることを強く推奨します。

VCS へのサーバ証明書および秘密キーのロード

TLS 暗号化を使用してクライアント システムと通信するときや、HTTPS を使用して Web ブラウザと通信するときに VCS を識別するには、VCS のサーバ証明書を使用します。

サーバ証明書をアップロードするには、次の手順を実行します。

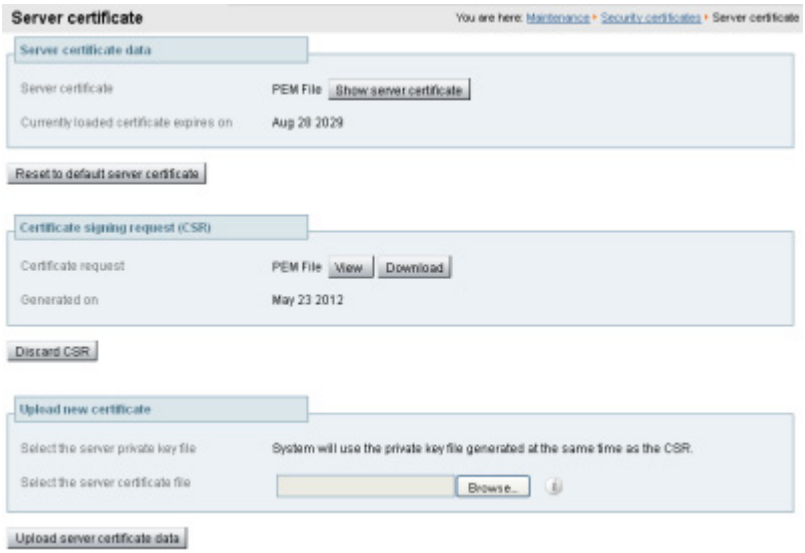
1. [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）] に移動します。
2. [新規証明書のアップロード（Upload new certificate）] セクションの [参照（Browse）] ボタンを使用して、**server certificate** PEM ファイルを選択し、アップロードします。
3. 外部システムを使用して証明書署名要求（CSR）を生成する場合は、サーバ証明書を暗号化するために使用した **server private key** PEM ファイルもアップロードする必要があります（以前に VCS を使用してこのサーバ証明書の CSR を作成していた場合は、秘密キー ファイルが自動的に生成され、保存されます）。
   - **server private key** PEM ファイルのパスワードは保護しないでください。
   - 証明書署名要求の進行中は、サーバ秘密キーをアップロードできません。
4. [サーバ証明書データのアップロード（Upload server certificate data）] をクリックします。

証明書署名要求の保存場所が X8 で変更されました。

CSR を X7 で生成すると、アプリケーションは **csr.pem** と **privkey_csr.pem** を **/tandberg/persistent/certs** に配置します。

CSR を X8 で生成すると、アプリケーションは **csr.pem** と **privkey.pem** を **/tandberg/persistent/certs/generated_csr** に配置します。

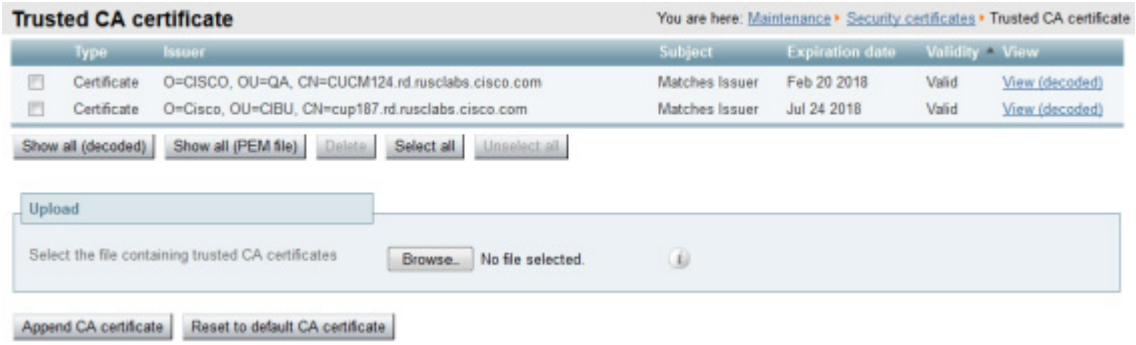
X7からアップグレードする場合で 未送信の CSR がある場合は、アップグレードの前にその CSR を破棄し、アップグレード後にもう一度 CSR を生成することを推奨します。



信頼された CA 証明書リストの管理

[信頼された CA 証明書（Trusted CA certificate）] ページ（[メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [信頼されたCA証明書（Trusted CA certificate）]）では、この VCS によって信頼された認証局（CA）用の証明書のリストを管理できます。VCS への TLS 接続に証明書の検証が必要な場合は、VCS へ提示される証明書にはこの CA リスト内の承認された CA による署名が必要であり、また、ルート CA への完全な信頼チェーン（中間 CA）が存在している必要があります。

- 1 つ以上の CA 証明書を含む新しいファイルをアップロードするには、必要な PEM ファイルを**参照し**、[CA 証明書の追加（Append CA certificate）] をクリックします。この手順によって、CA 証明書の既存のリストに新しい証明書を追加します。特定の発行者およびサブジェクトの既存の証明書を交換する場合は、手動で以前の証明書を削除する必要があります。
- 現在アップロードされているすべての CA 証明書を信頼された CA 証明書のシステムの元のリストで置き換えるには、[デフォルト CA 証明書にリセット（Reset to default CA certificate）] をクリックします。
- 現在アップロードされている信頼された CA 証明書のリスト全体を表示するには、[すべて表示（復号化）（Show all (decoded)）] をクリックして人が判読できる形式で表示するか、または [すべて表示（PEM ファイル）（Show all (PEM file)）]をクリックして RAW 形式でファイルを表示します。
- 信頼された個別の CA 証明書を表示するには、特定の CA 証明書を RAW 形式で表示する [表示（復号化）（View (decoded)）] をクリックします。
- 1 つ以上の CA 証明書を削除するには、該当する CA 証明書の横にあるボックスをオンにし、[削除（Delete）] をクリックします。



証明書失効リスト（CRL）の管理

VCS は証明書失効リスト（CRL）ファイルを使用して、TLS/HTTPS を介して通信するクライアント ブラウザおよび外部システムが提示した証明書を検証します。CRL は、失効して VCS との通信に使用できなくなっている証明書を特定します。

TLS/HTTPS クライアントおよびサーバ証明書に署名する CA の CRL データをアップロードすることを推奨します。イネーブルの場合、CRL のチェックはトラスト チェーンのすべての CA に適用されます。

証明書失効ソース

VCS は複数のソースから証明書失効情報を取得できます。

- CRL 分散ポイントからの CRL データの自動ダウンロード
- チェックされる証明書の OCSP（Online Certificate Status Protocol）レスポンダ URI を経由（SIP TLS のみ）
- CRL データの手動アップロード
- VCS の **Trusted CA certificate** ファイル内に埋め込まれた CRL データ

次の制約事項および使用上のガイドラインが適用されます。

- SIP TLS 接続を確立したときに、CRL のデータ ソースが [SIP] 設定ページの [証明書失効確認（Certificate revocation checking）] の設定によって影響を受ける場合
- 自動的にダウンロードされた CRL ファイルが、手動でロードされた CRL ファイルを上書きする場合（SIP TLS 接続を確認する場合、手動でアップロードされた CRL データと自動でダウンロードされた CRL データの両方を使用する可能性がある場合は除く）
- 外部ポリシー サーバが提示した証明書を検証するときに VCS が手動でロードされた CRL のみを使用する場合
- リモート ログイン アカウントを認証するために TLS と LDAP サーバとの接続を検証するときに、UCS が **信頼された CA 証明書**内のみの CRL データを使用する場合

自動 CRL 更新

自動 CRL 更新を実行するように VCS を設定することを推奨します。これにより、最新の CRL が証明書の検証に使用できるようになります。

自動 CRL 更新を使用するように VCS を設定するには、次の手順を実行します。

1. [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [CRL 管理（CRL management）] に移動します。
2. [自動 CRL 更新（Automatic CRL updates）] を [有効（Enabled）] に設定します。
3. VCS が CRL ファイルを取得できる一連の **HTTP（S）分散ポイント**を入力します。

   （注）

   - 新しい行にそれぞれ分散ポイントを指定する必要があります。
   - HTTP/HTTPS 分散ポイントのみがサポートされます。HTTPS を使用する場合、分散ポイントのサーバ自体に有効な証明書が必要です。
   - PEM および DER エンコード CRL ファイルがサポートされています。
   - 分散ポイントは、CRL ファイルまたは複数の CRL ファイルを含む ZIP および GZIP アーカイブを直接示す場合があります。
   - URL 内、またはダウンロードしたアーカイブからの圧縮を解除したファイルのファイル拡張子は、VCS が基盤となるファイル タイプの特定に関係ありません。ただし、通常の URL の形式は次のとおりです。
     - http://example.com/crl.pem
     - http://example.com/crl.der
     - http://example.com/ca.crl
     - https://example.com/allcrls.zip
     - https://example.com/allcrls.gz
4. [毎日の更新時刻（Daily update time）] を入力します（UTC 単位）。これは、VCS が分散ポイントからの CRL の更新を試行するおおよその時刻です。
5. [保存（Save）] をクリックします。

手動 CRL 更新

CRL ファイルは VCS に手動でアップロードできます。外部ポリシー サーバによって提示された証明書は、手動でロードされた CRL に対してのみ検証できます。

CRL ファイルをアップロードするには、次の手順を実行します。

1. [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [CRL 管理（CRL management）] に移動します。

2. [参照（Browse）] をクリックして、ファイル システムから必要なファイルを選択します。また、PEM エンコード形式である必要があります。
3. [CRL ファイルのアップロード（Upload CRL file）] をクリックします。
   これによって、選択したファイルがアップロードされ、以前にアップロードした CRL ファイルが置換されます。

手動でアップロードしたファイルを VCS から削除する場合は、[失効リストの削除（Remove revocation list）] をクリックします。

注：認証局の CRL が期限切れの場合、その CA から発行されたすべての証明書が無効として扱われます。

オンライン証明書ステータス プロトコル（OCSP）

VCS は OCSP レスポンダとの接続を確立して特定の証明書のステータスを照会することができます。VCS は使用する OCSP レスポンダを、確認する証明書に示されているレスポンダ URI から決定します。OCSP レスポンダは「良好（good）」、「失効（revoked）」、または「不明（unknown）」で証明書のステータスを送信します。

OCSP の利点は、失効リスト全体をダウンロードする必要がないことです。OCSP は SIP TLS接続のみでサポートされます。OCSP を有効にする方法については、以下を参照してください。

OCSP レスポンダへ接続するには、VCS Expressway からのアウトバウンド コミュニケーションが必要です。使用している OCSP レスポンダのポート番号（通常はポート 80 または 443）をチェックし、VCS Expressway からそのポートへのアウトバウンド通信ができることを確認します。

SIP TLS 接続を確認する失効の設定

また、証明書失効確認が SIP TLS 接続でどのように管理されるかを設定する必要があります。

1. [設定（Configuration）] > [SIP] に移動します。
2. [証明書失効確認（Certificate revocation checking）] セクションまで下にスクロールし、以下に従って設定します。

フィールド	説明	使用方法のヒント
証明書失効確認モード（Certificate revocation checking mode）	失効確認が SIP TLS 接続の確立時に交換された証明書に対し実行されるかどうかを制御します。	失効確認をイネーブルにすることを推奨します。
OCSP を使用（Use OCSP）	Online Certificate Status Protocol（OCSP）を証明書失効確認を実行するために使用するかどうかを制御します。	OCSP を使用するには、チェック対象の X.509 証明書に OCSP レスポンダの URI が含まれている必要があります。
CRL を使用（Use CRLs）	証明書失効リスト（CRL）を証明書失効確認を実行するために使用するかどうかを制御します。	CRL は、証明書が OCSP をサポートしていない場合に使用できます。

フィールド	説明	使用方法のヒント
CDP からの CRL のダウンロードを許可する（Allow CRL downloads from CDPs）	X.509 証明書に含まれる CDP URI からの CRL のダウンロードを許可するかどうかを制御します。	
フォールバック動作（Fallback behavior）	たとえば、失効の送信元に連絡を取れないなど、失効ステータスを確立できない場合に、失効確認の動作を制御します。 [失効済みとして処理（Treat as revoked）]：失効しているものとして証明書を処理します（したがって、TLS 接続は許可しません）。 [失効していないものとして処理（Treat as not revoked）]：失効していないものとして証明書を処理します。 [デフォルト（Default）]：*失効していないものとして処理します。*	[失効していないものとして処理（Treat as not revoked）]：失効ソースに確認できないものの、失効済み証明書が許可されることを示唆している可能性がある場合は、システムが通常どおりに動作し続けるようにします。

付録 1： トラブルシューティング

ネイバーおよびトラバーサル ゾーンでの SIP TLS ネゴシエーションの失敗

[TLS 検証モード（TLS verify mode）] が有効になっている場合は、ゾーンの設定の [ピア アドレス（Peer address）] フィールドで指定されているネイバー システムの FQDN または IP アドレスを使用して、そのシステムが提示した X.509 証明書内に含まれている証明書ホルダーの名前と照合して確認します（名前は証明書のサブジェクト共通名の属性またはサブジェクト代替名の属性のいずれかに含まれている必要があります）。証明書自体も有効であり、信頼された認証局によって署名されている必要があります。

したがって、ピアまたはクラスタ FQDN で証明書が作成されている場合は、ゾーンの [ピア アドレス（Peer address）] フィールドが IP アドレスではなく、FQDN で設定されていることを確認します。

999 文字を超える [サブジェクト代替名（Subject Alternative Name）] フィールド

安全なトラバーサル ゾーンまたはユニファイド コミュニケーション ゾーンが TLS ネゴシエーション エラーのために起動しない場合は、証明書で長い SAN フィールドを確認します。

VCS は 999 文字を超えた SAN を解析しません。そのため、証明書に多くの代替名がある場合、VCS Expressway の FQDN が VCS Control が読み取る部分の外にある可能性があります。

この問題を回避または対処するには、VCS が信頼する必要がある SAN が **subjectAltName** の最初の 999 文字内に完全に入っていることを確認する必要があります。

8192 ビットのキー長を有する証明書

8192 ビットのキー長を有する証明書を使用する場合、SIP TLS ゾーンがアクティブになれない場合があります。4096 ビットのキー長を有する証明書を使用することを推奨します。

モバイル アクセスおよびリモート アクセス使用時のサービス障害

末尾の改行文字を含まない秘密キー ファイルをアップロードした場合、証明書のエラーによりユニファイド コミュニケーションの Mobile & Remote Access サービスが失敗する場合があります。

秘密キー ファイルに末尾の改行文字が含まれていることを確認してください。

SSH 障害およびサポート対象外の OID による問題

ssh トンネルの確立ができないなどの不明な ssh 障害が発生した場合は、証明書に不明な OID がないかを確認してください。復号化されていない数字のエントリが [発行者（Issuer）] フィールドおよび [件名（Subject）] フィールドにないことを確認します（GUI から [メンテナンス（Maintenance）] > [セキュリティ証明書（Security Certificates）] > [サーバ 証明書（Server Certificate）] > [表示（復号化）（Show (decoded)）] を選択するか、またはコンソールから次を入力します。**openssl x509 -text -noout -in /tandberg/persistent/certs/server.pem**′)

Invalid

subject=CN=blahdeblah,OU=IT

Security,O=BigBang,L=Washington,ST=District of

Columbia,C=US,1.3.6.1.4.1.6449.1.2.1.5.1 = #060C2B06010401B2310102010501

有効(Valid)

subject=CN=blahdeblah,OU=IT

Security,O=BigBang,L=Washington,ST=District of

Columbia,C=US,jurisdictionOfIncorporationLocalityName=Dover

たとえば、現在、唯一サポートされている Extended Validation OID（EV OID）は次のとおりです。

- 1.3.6.1.4.1.311.60.2.1.1 jurisdictionOfIncorporationLocalityName
- 1.3.6.1.4.1.311.60.2.1.2 jurisdictionOfIncorporationStateOrProvinceName
- 1.3.6.1.4.1.311.60.2.1.3 jurisdictionOfIncorporationCountryName.

付録 2：OpenSSL のみを使用した証明書の生成

ここでは、OpenSSL を使用して、VCS に秘密キーと証明書要求を生成するプロセスについて説明します。これは、フリーの OpenSSL パッケージのみに依存する一般的なプロセスで、他のソフトウェアには依存しません。これは、証明書がテスト目的でネイバー デバイスとの連動を必要とする場合や、認証局と相互作用するために出力の提供を必要とする場合に適しています。

証明書要求生成プロセスの出力は認証局に渡すことができます。この認証局は組織内でも組織外でもかまわず、また、隣接デバイスとともに VCS 自体を認証するために VCS が必要とする X.509 証明書の作成に使用できます。

ここでは、プライベート認証局の管理に OpenSSL をどのように使用できるかについても簡単に説明しますが、包括的なものではありません。これらのプロセスのさまざまなコンポーネントは、サードパーティ CA とやりとりするときに使用できます。

OpenSSL および Mac OS X または Linux

OpenSSL は、Mac OS X にすでにインストールされており、通常は Linux にインストールされています。

OpenSSL と Windows

OpenSSL をまだインストールしていない場合は、http://www.openssl.org/related/binaries.html から無料で入手できます。

適切な 32 ビットまたは 64 ビットの OpenSSL を選択します。「Light」バージョンで十分です。

OpenSSL のインストール中に C++ ファイルを検出できないという警告を受信した場合は、このサイトでも使用可能な「Visual C++ 再頒布可能パッケージ」をロードし、OpenSSL ソフトウェアをリロードします。

OpenSSLを使用した証明書要求の作成

このプロセスでは、後で CA によって検証される場合があるサーバの秘密キーと証明書要求が作成されます。これは、ローカルで作成および管理されている CA やサードパーティ CA にすることができます。

（注）

- CSR を作成するこの方法は、コマンドが誤って入力される可能性があるため（特に SAN エントリが多数ある場合）、OpenSSL での作業に関する詳しい知識を持っている場合にのみ使用してください。関連する SAN エントリが不足していると、証明書を後日再作成する必要があります。
- バージョン X8.5.1 から、ユーザ インタフェースにダイジェスト アルゴリズムを設定するオプションがあります。デフォルトでは SHA-256 に設定されており、SHA-1、SHA-384、または SHA-512 に変更するオプションがあります。

OpenSSL のコマンド ラインから CSR を生成するには、次の手順を使用します。

1. SSH で VCS にアクセスし、root としてログインします。
2. **`mkdir /tmp/certtemp`** で作業するための新しいディレクトリを作成します。

3. **cd /tmp/certtemp** ディレクトリへ移動します。
4. 編集する必要があるため、CSR に使用する OpenSSL 設定ファイルを **cp /etc/openssl/csrreq.cnf.** ディレクトリへコピーします（**注：末尾のドットを保持**）。
5. **vi csrreq.cnf** ファイルを編集のために開きます
6. 「**default_md = sha1**」という行を見つけ、「**default_md = sha256**」となるように編集します。
7. 「**# req_extensions = v3_req**」の行から先頭にある **#** を削除してコメント解除します
8. 「**extendedKeyUsage=serverAuth, clientAuth**」という行が 「**v3_req**」セクション内にあることを確認します。
9. 「**subjectAltName = ${ENV::CSR_ALT_NAME}**」の行を見つけて、たとえば、「**subjectAltName = DNS:peer1vcs.example.com,DNS:peer2vcs.example.com,DNS:ClusterFQDN.example.com**」のように、証明書のサブジェクト代替名に含める語句が示されるように置き換えます。関連するエントリをすべて追加していることを確認します。MRA の場合は、次のように構成されます。
   1. **Expressway E：** **DNS:<CM domain name>, DNS:<XMPP federation domain>, DNS:<federation chat alias 1>, DNS:<federation chat alias 2>** など
   2. **Expressway C：** **DNS:<secure profile name 1>, DNS:<secure profile name 2>** など.
10. ここでファイルを保存して終了します。
11. VCS に新しい CSR および秘密キーを生成するには、OpenSSL コマンド「**openssl req -nodes -newkey rsa:4096 -keyout privatekey.pem -out myrequest.csr -config csrreq.cnf**」を実行します。必要に応じて **rsa:nnnn** を変更してください（nnnn はキー長で、推奨値は **4096** です）。
12. 次の例のような出力がコンソールに表示されます。ここで、必要な情報を入力します。すべてに入力する必要はありませんが、必須フィールドもあります。
    - 国（Country）
    - 州と地域（State and province）
    - 地域名（Locality name）
    - 組織名（Organization name）
    - 共通名（Common name）
    - 電子メール アドレス（Email address）：任意、空欄のままでも可
    - チャレンジ パスワード（A challenge password）：任意、空欄のままでも可
    - 任意の会社名（An optional company name）：任意、空欄のままでも可

```
Generating a 4096 bit RSA private key
............++
.....................................................++
writing new private key to 'privatekey.pem'
-----
```

```
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) [AU]:GB
State or Province Name (full name) [Some-State]:Berkshire
Locality Name (eg, city) []:Reading
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:CIBU
Common Name (eg, YOUR name) []:vcs01.example.com
Email Address []:
```

フィールドに入力すると、**myrequest.csr** および **privatekey.pem** という 2 つのファイルが作成されます。

13. （任意）DNS エントリが要求に正しく入力されていることを検証する場合は、**myrequest.csr** ファイルを `openssl req -text -noout -in myrequest.csr` コマンドを使用して復号化します。
14. CSR を選択した認証局に送信します。その認証局からは公開証明書が提供されます。
15. [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）] Web ページの [サーバ証明書ファイルの選択（Select the server certificate file）] エントリ ボックスを使用して、公開証明書を VCS にアップロードします。
16. [メンテナンス（Maintenance）] > [セキュリティ証明書（Security certificates）] > [サーバ証明書（Server certificate）] Web ページの [サーバ秘密キーファイルの選択（Select the server private key file）] エントリ ボックスを使用して、**privatekey.pem** を VCS にアップロードします。

privatekey.pem は安全を保持してください。

OpenSSL を使用した認証局の操作

主要な導入では、サードパーティの認証局を使用するか、または組織の IT 部門にすでに内部認証局が 1 つ存在する可能性があります。ただし、次に説明するように、OpenSSL を使用してプライベート認証局で証明書を管理することができます。

OpenSSL を CA として機能するようにすでに設定している場合は、「OpenSSL を使用した署名付き証明書の作成」（22 ページ）という項を参照してください。

CA として機能する OpenSSL の設定

OpenSSL は強力なソフトウェアで、CA として動作するには、発行された証明書を追跡するためのいくつかのディレクトリとデータベースの設定が必要です。

ディレクトリとファイルのリストは、`[ CA_default ]` セクションの openssl コンフィギュレーション ファイルにあります。デフォルトでは、作成が必要なファイル/ディレクトリは次のとおりです。

- 現在のディレクトリ内に**demoCA**ディレクトリと **certs**、**newcerts**、および **private** の 3 つのサブディレクトリ。
- **demoCA** ディレクトリ内に **index.txt**という空のファイル。
- **demoCA** ディレクトリ内に「10」などの 2 桁の数字を保存する **serial** というファイル。

たとえば、次のコマンドを使用します。

```
mkdir demoCA
cd demoCA
mkdir certs
mkdir newcerts
mkdir private
touch index.txt
echo 10 > serial
```

OpenSSL を使用した認証局の作成

このプロセスで、認証局（CA）の秘密キーと証明書が作成され、他の証明書を検証するために使用可能になります。これは明示的にインストールされるもの以外のデバイスから信頼されることはないことに注意してください。

コマンド プロンプトから次を実行します。

1. **demoCA** ディレクトリに移動していることを確認します。
2. Windows の場合：**openssl.cfg** を**demoCA** がインストールされているディレクトリからコピーし、名前を **openssl_local.cfg**に変更します。

   Mac OS X の場合：**/System/Library/OpenSSL/openssl.cnf** を **demoCA** ディレクトリにコピーし、名前を **openssl_local.cfg** に変更します。
3. テキスト エディタを使用して、上記のコピー コマンドで作成した **openssl_local.cfg** ファイルを編集します。次の変更を `[CA_default]` セクションに加えます。
   1. `copy_extensions = copy` という行の先頭に # がないことを確認します。# がある場合は削除します。その行がコメント アウトされたままの場合は、CSR の属性が除去され、SSL サーバと SSL クライアントの属性は証明書に表示されません。
   2. `policy = policy_match` を `policy = policy_anything` に変更します。
   3. `dir = ./demoCA` を `dir =` に変更します。
   4. 任意で、`default_days = 365`（生成した証明書の 1 年の有効期間）を`default_days = 3650`（10 年または適切な値）に変更します。
   5. ファイルを保存します。
4. 次のコマンドを実行して、CA の秘密キーを生成します。

   ```
   openssl genrsa -aes256 -out private/cakey.pem 4096
   ```

ここで、秘密キーを暗号化するパスワードが求められるので、強力なパスワードを選択し、安全な場所に記録します。cakey.pem ファイルが CA 証明書を作成し、他の証明書に署名するために使用されるので、安全に保持する必要があります。

5. 次のコマンドを実行して、CA 証明書を生成します。

   Windows の場合：**`openssl req -new -x509 -days 3650 -key private/cakey.pem -config openssl_local.cfg -sha1 -extensions v3_ca -out cacert.pem`**

   OS X の場合：**`openssl req -new -x509 -days 3650 -key private/cakey.pem -config openssl_local.cfg -sha1 -extensions v3_ca -out cacert.pem`**

6. キーのパスフレーズを入力し、次の項目を含む要求されたデータを入力します。
   - 国（Country）
   - 州または地域（State or province）
   - 地域名（Locality name）
   - 組織名（Organization name）
   - 組織単位（Organizational Unit）
   - 共通名（Common name）：通常は、この CA の担当者の名前になります
   - 電子メール アドレス（Email address）：任意、空欄のままでも可

要求された日付を入力すると操作が完了し、認証局が **cacert.pem** を認証して使用できるようになります。

OpenSSL を使用した署名付き証明書の作成

このプロセスでは、以前に生成された証明書要求を使用して生成された CA キーでサーバ証明書に署名します。

コマンド プロンプトから次を実行します。

1. **demoCA** ディレクトリに移動していることを確認します。
2. 証明書要求ファイル（**certcsr.pem**）が使用可能であることを確認します。
   - 証明書要求を VCS を使用して作成した場合（推奨プロセス）、次を実行します。

     ダウンロードしたファイルを VCS から **demoCA** ディレクトリにコピーし、名前を **certcsr.pem** に変更します。
   - 証明書要求が OpenSSL を使用して作成された場合は、次の手順を実行します。

     以前に生成した証明書要求を **demoCA** ディレクトリにコピーし、次のコマンドを実行して PEM 形式に変換します。

     `openssl req -in certcsr.der -inform DER -out certcsr.pem -outform PEM`
3. 次のコマンドを実行して、署名済みサーバ証明書を生成します。

   `openssl ca -config openssl_local.cfg -cert cacert.pem -keyfile private/cakey.pem -in certcsr.pem -out certs/server.pem -md sha1`

   「データベース TXT_DB の更新に失敗しました エラー番号 2（failed to update database TXT_DB error number 2）」というエラー メッセージが表示された場合は、**index.txt** ファイルの内容を削除してから、コマンドに戻ります。

4. CA の秘密キーのパスワードを入力するように求められます。

サーバ用の署名付き証明書が **demoCA/certs/server.pem** として使用できるようになります。

OpenSSL を使用した自己署名証明書の作成

自己署名証明書を作成することは推奨しません。それらは、ユニファイド コミュニケーションの導入環境では動作しません。

その代わりに、前述のように OpenSSL を使用して認証局を作成する必要があります。

付録 3：PEM 形式への DER 証明書ファイルの変換

秘密キー、ルート（CA）証明書およびサーバ/クライアント証明書は、サードパーティ製ツール（または認証局から購入したツール）を使用して生成でき、PEM（必須形式、拡張子 .pem）または DER（拡張子 .cer）形式のファイルとして生成できます。

証明書を VCS で使用するには、PEM 形式である必要があります。DER から PEM 形式への変換は、次の項に記載されているように、OpenSSL または Windows を使用する 2 通りの方法のいずれかで行うことができます。

OpenSSL を使用した DER 証明書ファイルの PEM ファイルへの変換

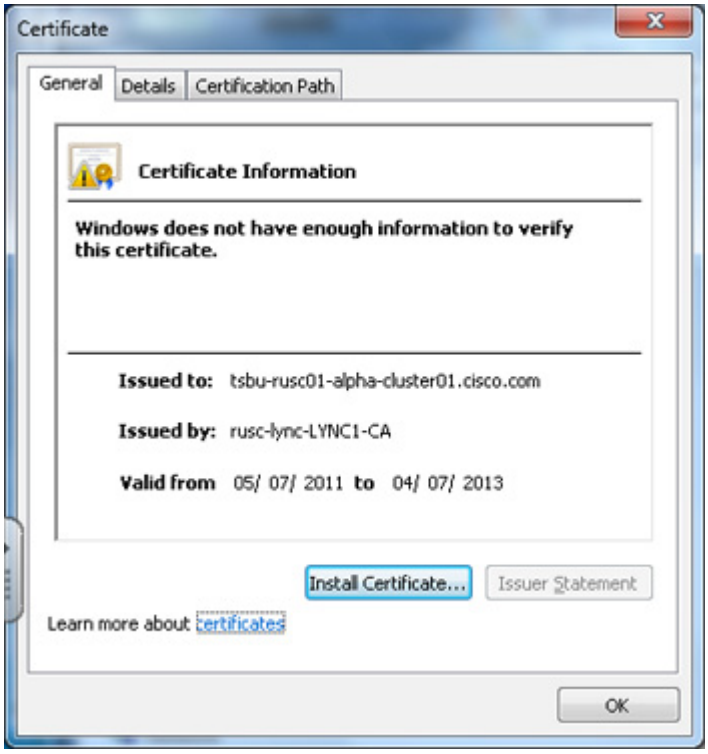
DER から PEM 形式へ変換するには、openssl を実行しているシステム上で次のコマンドを実行します。

```
openssl x509 -in <filename>.cer -inform DER -out <filename>.pem -outform PEM
```

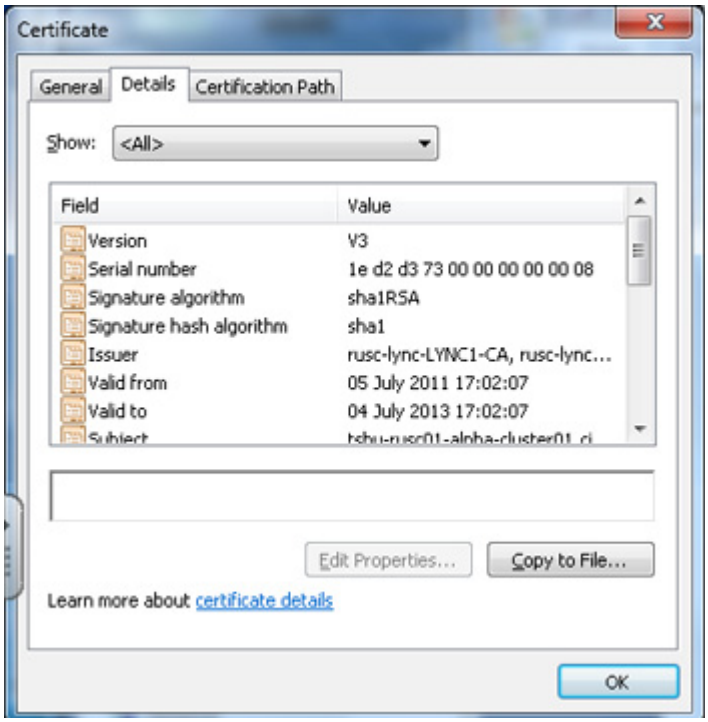
Microsoft Windows を使用した DER 証明書ファイルの PEM ファイルへの変換

Microsoft Windows を使用して DER から PEM 形式へ変換するには、次の手順を実行します。

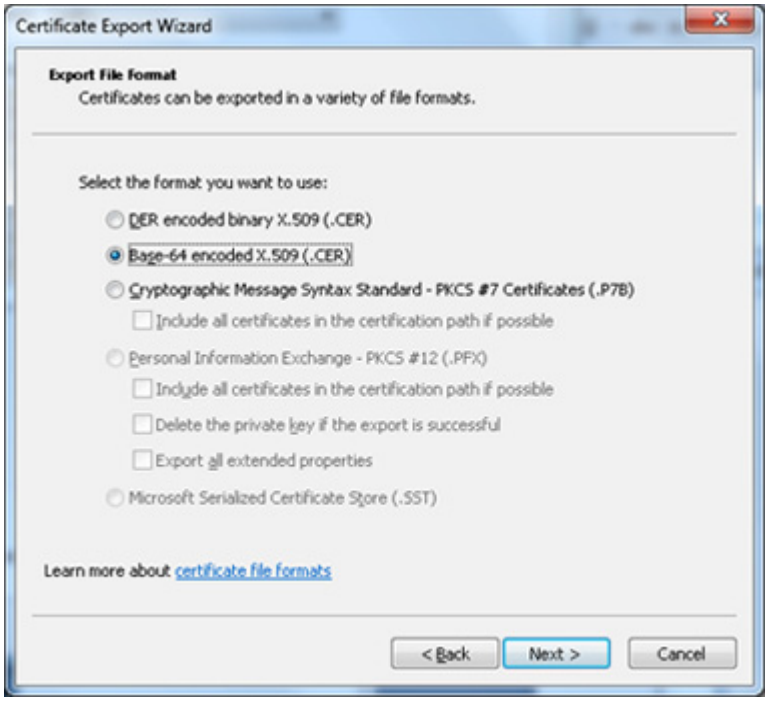
1. 変換する DER ファイルをダブルクリックします（拡張子は「.cer」である可能性があります）。



2. [詳細（Details）] タブを選択します。



3. [コピー先ファイル（Copy to File…）] をクリックします。
4. [ようこそ（Welcome）] ページで [次へ（Next）] をクリックします。
5. [Base-64 暗号化 X.509（.CER）（Base-64 encoded X.509 (.CER)）] を選択し、[次へ（Next）] をクリックします。



6. [参照（Browse）] をクリックし、ファイル（たとえば、**server.pem**）に必要な宛先を選択して [次へ（Next）] をクリックします。
7. [終了（Finish）] をクリックします。
8. ファイル名を **server.pem.cer** から **server.pem** に変更します。
9. このファイルは、このガイドの「VCS への証明書およびキーのロード」（10 ページ）セクションで使用します。

付録 4：証明書の復号化

ここでは、証明書の内容を復号して表示する方法についていくつか説明します。

OpenSSL

PEM ファイル（たとえば、**cert.pem**）は次のコマンドで復号化できます。

```
openssl x509 -text -in cert.pem
```

DER ファイル（たとえば、**cert.cer**）は次のコマンドで復号化できます。

```
openssl x509 -text -inform DER -in cert.cer
```

Firefox

閲覧している Web サイトで使用中の証明書は、アドレスバーのセキュリティ情報ボタンをクリックし、[詳細] をクリックしてから [証明書] をクリックすると Firefox に表示できます。

Internet Explorer

閲覧している Web サイトで使用中の証明書は、アドレス バーの右側にあるロック アイコンをクリックすることで Internet Explorer に表示できます。[Web サイトの識別] ダイアログが表示されます。下部にある [証明書の表示] リンクをクリックします。

付録 5：「クライアントおよびサーバ」の証明書を発行するための AD CS の有効化

注：Microsoft Active Directory Certificate Services（AD CS）の CA コンポーネントは、クライアントまたはサーバとして VCS の認証に使用可能な証明書を発行できなければなりません。

Windows Server 2008 Standard R2（および以降）の AD CS では、適切な証明書テンプレートを作成すると、そのようなタイプの証明書を発行できます。**以前のバージョンの Windows Server Standard Edition は適していません。**

AD CS のデフォルトの「Web サーバ」証明書テンプレートは、サーバ認証用の証明書を作成します。また、ネイバーまたはトラバーサル ゾーンを相互認証で設定する（[TLS 検証モード（TLS verify mode）がオンになっている）場合は、VCS 用のサーバ証明書にクライアント認証も必要です。

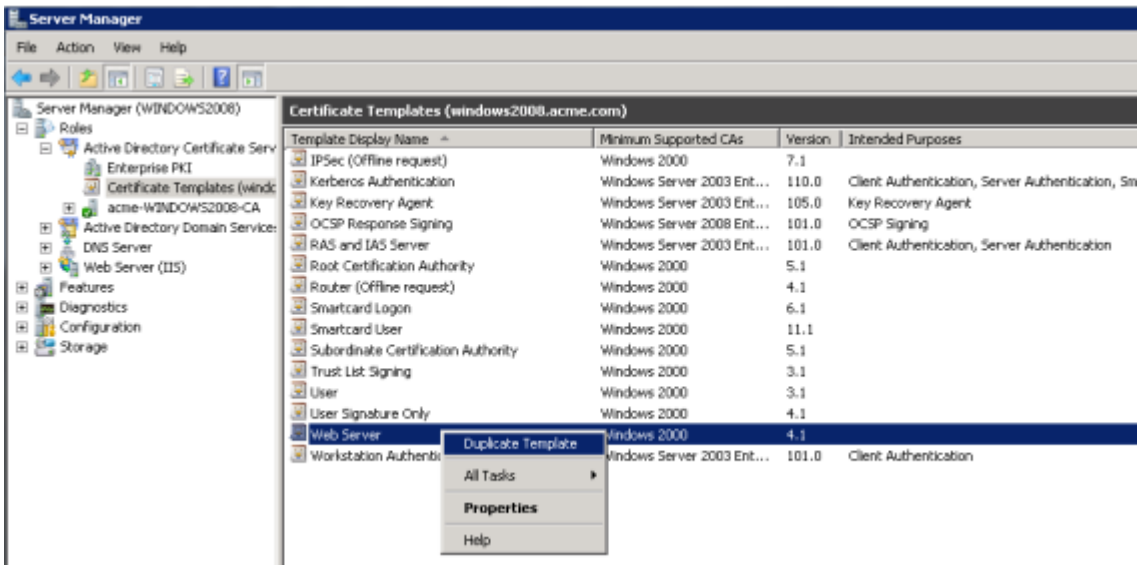
サーバ認証とクライアント認証の両方で証明書テンプレートを設定するには、次の手順を実行します。

1. Windows でサーバ マネージャを起動します（[スタート] > [管理ツール] > [サーバー マネージャー]）。

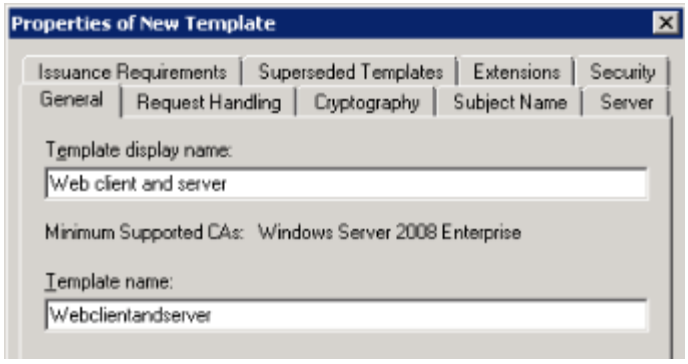
   （Server Manager は、Windows のサーバー エディションに含まれる機能です。）

2. [サーバー マネージャー] ナビゲーション ツリーを展開し、[ロール] > [Active Directory 証明書サービス（<ドメイン>）] を選択します。

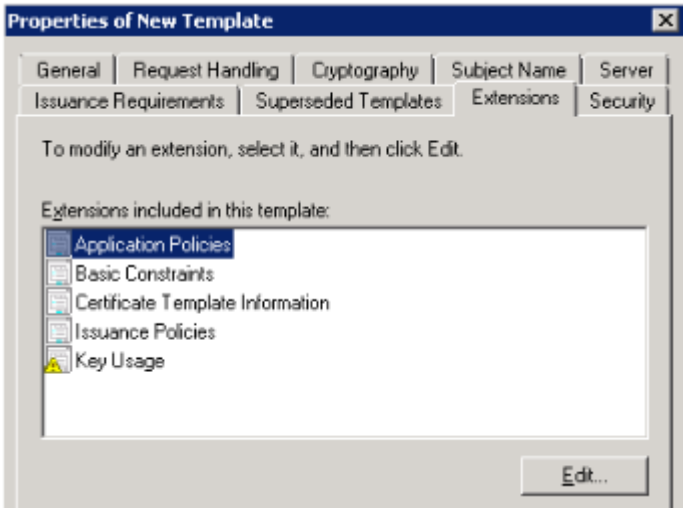
3. [Web サーバー] を右クリックして [テンプレートの複製] を選択します。



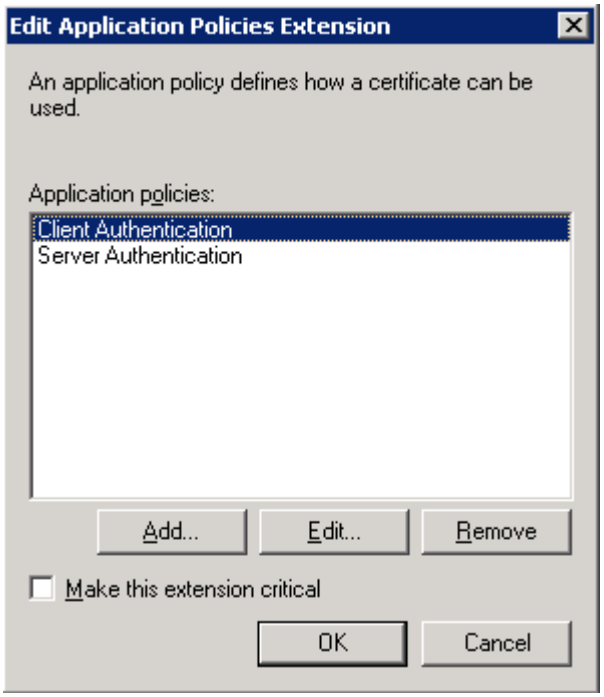
4. [Windows Server 2003 Enterprise] を選択して [OK] をクリックします。
5. [全般] タブで [テンプレートの表示名] と [テンプレート名] に入力します。（たとえば、**`Web client and server`** と **`Webclientandserver`**）。



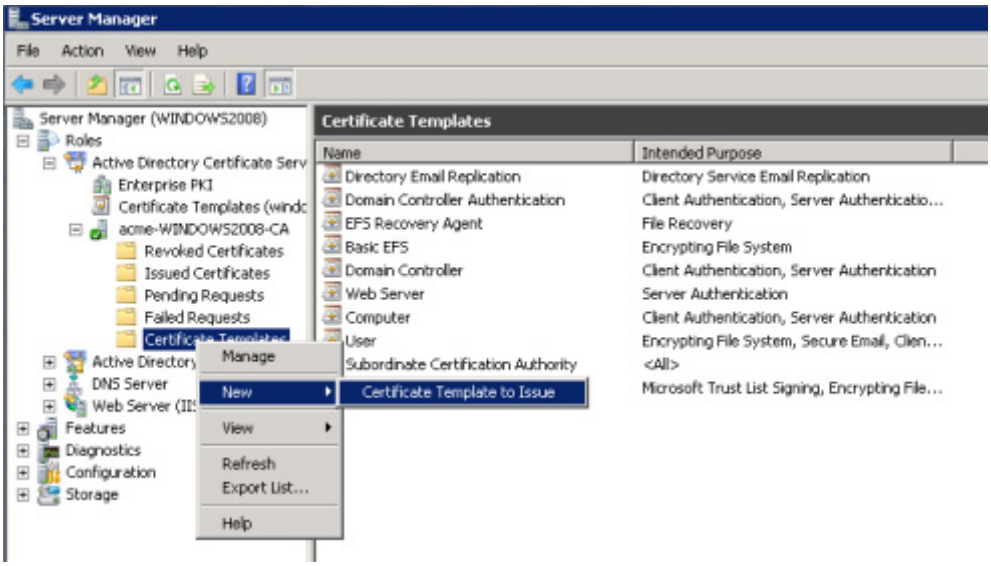
6. [拡張機能] タブで、[アプリケーション ポリシー] を選択し、[編集] をクリックします。



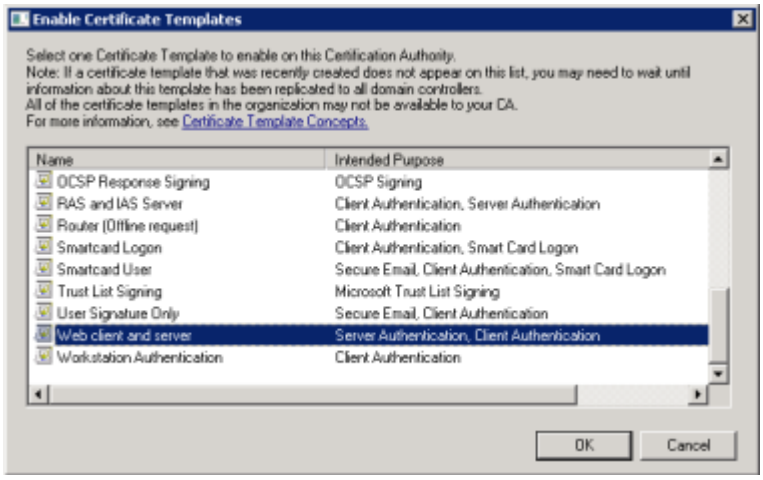
7. [クライアント認証] を一連のアプリケーション ポリシーに追加します。
    1. [追加] をクリックします。
    2. [クライアント認証] を選択し、[OK] をクリックします。
    3. [OK] をクリックします。



8. [OK] をクリックして新しいテンプレートの追加を完了します。
9. 認証局に新しいテンプレートを追加するには、次の手順を実行します。
   1. [ロール] > [Active Directory 証明書サービス] > [<ご自身の認証局>] に移動します。
   2. [証明書テンプレート] を右クリックして [新規] > [発行する証明書テンプレート] を選択します。



   3. [Web クライアントおよびサーバー] テンプレートを選択し、[OK] をクリックします。



これで、その Microsoft の認証局に証明書要求を送信する際に新しい **Web クライアントおよびサーバ**のテンプレートを使用できるようになりました。

マニュアルの変更履歴

次の表に、このマニュアルの変更履歴の要約を示します。

リビジョン	日付（Date）	説明
	2015 年 11 月	新しいテンプレートを適用。X8.7 用に再発行。
	2015 年 7 月	X8.6 に関する内容を更新。
13	2015 年 4 月	X8.5.2 に関する更新。CRL 情報、CSR 生成ページのデフォルト、SAN の 999 の文字制限を変更。
12	2015 年 1 月	X8.5.1 の更新。ダイジェスト アルゴリズムを選択するユーザ インターフェイスのオプションが導入されました。デフォルトは、SHA-256（ハッシュ アルゴリズム）に設定されます。
11	2014 年 12 月	X8.5 用に再発行されました。2050 年の日付管理とサポートされていない OID の注釈が挿入されました。付録 2「OpenSSL のみを使用した証明書の生成」の手順が変更されました。
10	2014 年 7 月	X8.2 用に再発行されました。ユニファイド コミュニケーション導入時のサーバ証明書用に変更された推奨されるオプション。
9	2014 年 6 月	X8.2 用に再発行。ユニファイド コミュニケーションの導入に関するサーバ証明書の要件が強化されました。
	2015 年 11 月	新しいテンプレートを適用。X8.7 用に再発行。
8	2013 年 12 月	X8.1 に関する内容を更新。「Microsoft OCS を使用した証明書の生成」の付録を削除。「OpenSSL のみを使用した証明書の生成」の付録をさまざまな面で改善および明確化。
7	2013 年 2 月	CRL 管理、トラブルシューティング、ならびに「クライアントおよびサーバ」の証明書のテンプレートによる Windwos サーバ マネージャの設定方法に関する項を追加。
6	2012 年 8 月	証明書署名要求を生成する VCS X7.2 の機能に関する更新。
5	2012 年 2 月	OpenSSL 固有の項を含めた大幅な明確化および更新。
4	2011 年 12 月	明確化のためのマイナー更新。
3	2011 年 9 月	Microsoft Lync 2010（Lync）に関する更新。
2	2010 年 10 月	新しいドキュメント スタイルを適用。証明書の復号化および Microsoft Office Communications Server（OCS）で使用するための証明書生成に関するガイダンスについての新しい付録を追加。
1	2009 年 11 月	初版。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system.All rights reserved.Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries.A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks.その他の商標はそれぞれの権利者の財産です。The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

シスコの商標または登録商標

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries.シスコの商標の一覧は www.cisco.com/web/JP/trademark_statement.html に掲載されています。Third-party trademarks mentioned are the property of their respective owners.The use of the word partner does not imply a partnership relationship between Cisco and any other company.(1110R)