CHAPTER 15

Cisco Unified MeetingPlace Express での SSL の設定と証明書の管理

この章の内容は、（音声、ビデオ、Web によるアドホック会議に使用する）Cisco Unified MeetingPlace Express と（アドホック会議に使用する）Cisco Unified MeetingPlace Express VT に適用されます。

証明書について

SSL を使用して Cisco Unified MeetingPlace Express とのセキュアな Web 通信を行うには、信頼された Certificate Authority（CA; 証明局）から次の 2 つの証明書を取得する必要があります。

- エンドユーザ インタフェースおよび管理センター用
- Web 会議用

Cisco Unified MeetingPlace Express では、自己署名証明書がサポートされていません。自己署名証明書または未署名の証明書を使用すると、Web 会議室の一部が正しく動作しません。

SSL が有効であるかどうかにかかわらず、電子メール通知では「https」ではなく「http」で始まる参加（Click-to-attend）URL が使用されます。SSL が有効な場合、ユーザは自動的に「https」URL にリダイレクトされます。

（注） Segmented Meeting Access（SMA）を使用する場合は、SSL も使用してプライマリ サーバとセカンダリ サーバ間でセキュアな Web 通信を行う必要があります。この場合、プライマリ サーバとセカンダリ サーバにそれぞれ 2 つ、計 4 つの証明書が必要です。セカンダリ サーバに SSL を設定する手順は、プライマリ サーバと同じです。ただし、管理センターの異なるページを使用します。

証明書署名要求（CSR）の生成と証明書の取得

ここでは、管理センターから証明書署名要求を生成し、その CSR を証明書を発行する CA に送信することによって証明書を取得する方法について説明します。CSR を生成する必要があるのは、SSL を最初にインストールするとき、または期限切れの SSL 証明書を置換するときのみです。

注意　有効な SSL 証明書がすでに Cisco Unified MeetingPlace Express サーバにインストールされている場合は、新しい CSR が生成されると既存の SSL 証明書は無効になります。SSL 証明書を初めてインストールする場合か、有効期限が切れた SSL 証明書を置き換える場合にのみ実行します。

制約事項

- 証明書はプライバシー エンハンスト メール（PEM）形式でなければなりません。証明書の形式を変換する方法については、「SSL 証明書の形式の変更」（P. 15-9）を参照してください。

始める前に

- CSR を生成するには、SSL が無効になっている必要があります。
- CSR と取得した証明書では、オペレーティング システムのインストール時にネットワークの設定で入力したホスト名が使用されます。
  - エンドユーザ インタフェースおよび管理センターの証明書では、イーサネット ポート 1（デバイス eth0）に割り当てられたホスト名が使われます。
  - Web 会議の証明書では、イーサネット ポート 2（デバイス eth1）に割り当てられたホスト名が使われます。

  システムのホスト名を変更した場合は、新しい証明書を取得する必要があります。

  オペレーティング システムのインストールについては、『*Installation and Upgrade Guide for Cisco Unified MeetingPlace Express Release 2.0*』を参照してください。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインして、[Administration] をクリックします。

ステップ 2　次のいずれかを実行します。

- プライマリ サーバの証明書を取得するには、[Certificate Management] > [Generate CSRs] の順にクリックします。
- セカンダリ サーバの証明書を取得するには、[System Configuration] > [SMA Configuration] > [SMA Certificate Management] > [SMA Generate CSRs] の順にクリックします。

ステップ 3　[Generate Certificate Signing Requests (CSRs)] ページ（プライマリ サーバ）、または [SMA Generate CSRs] ページ（セカンダリ サーバ）の各フィールドに値を入力します。

（注）　一部の CA は州を表す 2 文字の省略形を認識しないので、省略しない州名を使用してください。

ステップ 4　[Generate CSRs] をクリックします。

注意　[Generate CSRs] は一度だけクリックしてください。ページに入力した値を変更（たとえば、組織名を変更してから [Generate CSRs] を再度クリック）した場合、最終的に取得した証明書はシステムで使用できません。このページに入力した値を変更しないでください。また、[Generate CSRs] を複数回クリックしないでください。証明書がシステムで使用できなくなります。

SSL が有効になっている場合は、CSR を生成できないというメッセージが表示され、[Generate Certificate Signing Requests (CSRs)] ページに戻ります。

SSL が無効になっている場合は、CSR を生成すると使用中の既存の秘密鍵と公開証明書が破損するという警告メッセージが表示されます。現在保留中の署名証明書が削除され、それらの証明書を再請求する必要があります。続行するには、[OK] をクリックします。

ステップ 5　[Download Certificate Signing Requests] ページでいずれかの CSR を選択し、[Download CSR] をクリックします。

ステップ 6　［ファイルのダウンロード］ダイアログボックスで［保存］をクリックします。

ステップ 7　[名前を付けて保存] ダイアログボックスで次の手順に従います。

a.　［保存する場所］フィールドで、CSR を保存するディレクトリに移動します。

b.　[File name] の下に、ファイルの名前が表示されます。ブラウザによってファイル名に何かが追加された場合（中央に [1] が挿入されるなど）は削除します。

c.　[Save as type] の下で、ドロップダウン リストから [All Files] を選択します（選択しない場合、ファイルは .htm 拡張子を付けて保存されます）。

d.　［保存］をクリックします。

ステップ 8　他の CSR についてステップ 5 からステップ 7 までを繰り返します。

ステップ 9　これら 2 つの CSR を CA に送信します。CA によって証明書が生成されて送り返されます。（Cisco Unified MeetingPlace Express システムからコンピュータに CSR をダウンロードして、標準の電子メール プログラムで CSR を CA に送信できます）。

（注）　証明書はプライバシー エンハンスト メール（PEM）形式でなければなりません。

関連項目

- フィールド リファレンス：[Generate Certificate Signing Requests (CSRs)] ページ（P. C-56）
- ページの概要：[SMA Generate CSRs] ページ（P. C-112）

証明書のアップロードと SSL の有効化

始める前に

- 信頼された CA から必要な 2 つの証明書を取得します。「証明書署名要求（CSR）の生成と証明書の取得」（P. 15-2）を参照してください。

制約事項

- 証明書はプライバシー エンハンスト メール（PEM）形式でなければなりません。証明書の形式を変換する方法については、「SSL 証明書の形式の変更」（P. 15-9）を参照してください。
- プライマリ サーバの両方の証明書、セカンダリ サーバの両方の証明書をそれぞれ同時にアップロードする必要があります。

（注）　CLI からも SSL を有効にすることができます。「SSLUtil」（P. 19-8）を参照してください。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインして、[Administration] をクリックします。

ステップ 2　次のいずれかを実行します。

- プライマリ サーバの SSL を有効にするには、[Certificate Management] > [Enable SSL] の順にクリックします。
- セカンダリ サーバの SSL を有効にするには、[System Configuration] > [SMA Configuration] > [SMA Certificate Management] > [SMA Enable SSL] の順にクリックします。

SSL がすでに有効になっている場合は、Cisco Unified MeetingPlace Express システムによって、エンドユーザ インタフェース、管理センター、および Web 会議の SSL がすでに有効になっているというメッセージが表示されます。

ステップ 3　[Enable SSL for the End-User Interface, Administration Center, and Web Conferencing] ページ（プライマリ サーバ）、または [SMA Enable SSL] ページ（セカンダリ サーバ）の各フィールドに値を入力します。

CSR を生成したら、CA に送信します。証明書を受信したら、証明書ファイルのフィールドにのみ値を入力します。秘密鍵ファイルとパスワードのフィールドは特殊な場合にのみ使用します。

注意　フィールドには、必ず正しい値を入力してください。誤った値を入力すると、システムの再起動が必要になることがあります。

ステップ 4　[Upload and Enable SSL] をクリックします。SSL を有効にするにはサーバを再起動する必要があるというメッセージが表示されます。

ステップ 5　[Restart] をクリックして、サーバを再起動します。

トラブルシューティング

- 間違った証明書や秘密鍵の名前を入力して [Enable SSL] をクリックすると、Cisco Unified MeetingPlace Express システムからロックアウトされ、アプリケーションのどの部分にもアクセスできなくなります。システムへのアクセス方法については、「SSLUtil」（P. 19-8）を参照してください。
- 証明書が正しくロードされたことを確認するには、管理センターから実行できる情報取り込みログをチェックするか、/opt/macromedia/breeze/logs/support/diagnostic/edge.00.log でログインを調べます。

関連項目

- フィールド リファレンス：エンドユーザ インタフェース、管理センター、および Web 会議の SSL の有効化（P. C-53）
- フィールド リファレンス：[SMA Enable SSL] ページ（P. C-111）

SSL の無効化

制約事項

- エンドユーザ インタフェース、管理センター、または Web 会議など、1 つの Web インタフェースについてのみ SSL を無効にすることはできません。このタスクを実行すると、システム全体に対して SSL が完全に無効になります。

（注）　CLI からも SSL を無効にすることができます。「SSLUtil」（P. 19-8）を参照してください。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインして、[Administration] をクリックします。

ステップ 2　次のいずれかを実行します。

- プライマリ サーバの SSL を無効にするには、[Certificate Management] > [Disable SSL] の順にクリックします。
- セカンダリ サーバの SSL を無効にするには、[System Configuration] > [SMA Configuration] > [SMA Certificate Management] > [SMA Disable SSL] の順にクリックします。

SSL がすでに無効になっている場合は、Cisco Unified MeetingPlace Express システムによって、エンドユーザ インタフェース、管理センター、および Web 会議の SSL がすでに無効になっているというメッセージが表示されます。

ステップ 3　[Disable SSL] をクリックします。SSL を無効にするとシステムの処理が中断され、進行中の会議がすべて停止されるというメッセージが表示されます。SSL を無効にするには、サーバを再起動する必要があります。

ステップ 4　[Restart] をクリックして、サーバを再起動します。

関連項目

- ページの概要：SSL の無効化（P. C-41）
- ページの概要：[SMA Disable SSL] ページ（P. C-110）

証明書の内容の表示

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインして、[Administration] をクリックします。

ステップ 2　次のいずれかを実行します。

- プライマリ サーバの証明書を表示するには、[Certificate Management] > [Display Certificate] の順にクリックします。
- セカンダリ サーバの証明書を表示するには、[System Configuration] > [SMA Configuration] > [SMA Certificate Management] > [SMA Display Certificate] の順にクリックします。

Cisco Unified MeetingPlace Express システムによって、証明書の名前が表示されます。証明書を所有していない場合には、表示する証明書がないというメッセージが Cisco Unified MeetingPlace Express システムによって表示されます。

ステップ 3　証明書を選択し、[Display Certificate] をクリックして証明書を開きます。証明書ファイルのコンテンツが表示されます。

関連項目

- ページの概要：証明書の表示（P. C-43）
- ページの概要：[SMA Display Certificate] ページ（P. C-110）

SSL 設定のバックアップと復元

Cisco Unified MeetingPlace Express のアプリケーションの再インストールまたはアップグレードでは、SSL ファイルが保持されます。ただし、オペレーティング システムを再インストールする場合には、SSL ファイルは保持されず、バックアップから SSL ファイルを再インストールする必要があります。

ここでは、証明書を含む SSL 設定のバックアップ方法と復元方法について説明します。

（注）　CLI からも SSL 設定のバックアップと復元ができます。「SSLUtil」（P. 19-8）を参照してください。

手順

ステップ 1　Cisco Unified MeetingPlace Express にログインして、[Administration] をクリックします。

ステップ 2　次のいずれかを実行します。

- プライマリ サーバの証明書をバックアップするには、[Certificate Management] > [Back Up SSL Configuration] の順にクリックします。
- セカンダリ サーバの証明書をバックアップするには、[System Configuration] > [SMA Configuration] > [SMA Certificate Management] > [SMA Back Up SSL Configuration] の順にクリックします。

ステップ 3　バックアップする証明書を選択して、[Back up Certificate] をクリックします。

証明書がない場合には、Cisco Unified MeetingPlace Express システムにバックアップする証明書がないというメッセージが表示されます

ステップ 4　[Save] をクリックして、SSL 設定を zip ファイルとして保存します。

ステップ 5　以前保存した SSL 設定を復元するには、次のいずれかの操作を実行します。

- プライマリ サーバの証明書を復元するには、[Certificate Management] > [Restore SSL Configuration] の順にクリックします。
- セカンダリ サーバの証明書を復元するには、[System Configuration] > [SMA Configuration] > [SMA Certificate Management] > [SMA Restore SSL Configuration] の順にクリックします。

ステップ 6　アーカイブされているバックアップ ファイルの名前を入力します。ステップ 4 でファイルに付けた名前です。

ステップ 7　[Restore SSL Configuration] をクリックします。

関連項目

- ページの概要：[Back Up SSL Configuration] ページ（P. C-34）
- フィールド リファレンス：[Restore the SSL Configuration for the End-User Interface, Administration Center, and Web Conferencing] ページ（P. C-104）
- ページの概要：[SMA Back Up SSL Configuration] ページ（P. C-109）
- フィールド リファレンス：[SMA Restore SSL Configuration] ページ（P. C-112）

SSL 証明書の形式の変更

アップロードする SSL 証明書は PEM 形式である必要があります。SSL 証明書が DER 形式の場合は、PEM 形式に変換してからアップロードします。証明書を DER から PEM の形式に変換するには、CLI を使用します。

手順

ステップ 1　Cisco Unified MeetingPlace Express オペレーティング システムに **mpxadmin** ユーザとしてログインします。

ステップ 2　パスワードのプロンプトに、mpxadmin のパスワードを入力します。

Cisco Unified MeetingPlace Express オペレーティング システムのデスクトップが表示されます。

ステップ 3　デスクトップで右クリックします。

ステップ 4　メニューから [New Terminal] を選択します。端末セッションが開始されます。

ステップ 5　次のコマンドを入力します。

x509 -in <file1.crt> **-inform DER -out** <file2.crt> **[-outform PEM]**

file1.crt は DER ファイルの名前、*file2.crt* は PEM ファイルの名前です。**[-outform PEM]** はオプションで、デフォルトは PEM です。

ステップ 6　デスクトップで、[RedHat] > [Network Services] の順にクリックします。

ステップ 7　[Log out] をクリックします。

関連項目

- 第 19 章「Cisco Unified MeetingPlace Express のコマンドライン インタフェース（CLI）の使用方法」

SSL の問題のトラブルシューティング

この項を読んでも Cisco Unified MeetingPlace Express の問題が解決できない場合は、Cisco TAC に連絡してください。Cisco TAC への連絡方法については、「技術情報の入手方法、サポートの問い合せ、およびセキュリティ ガイドライン」（P. xxiii）を参照してください。

問題　SSL 証明書が PEM 形式でない。

解決策　SSL 証明書を PEM 形式に変換します。詳細については、「SSL 証明書の形式の変更」（P. 15-9）を参照してください。

問題　間違った証明書または秘密鍵の名前を入力して、[Enable SSL] をクリックした。Cisco Unified MeetingPlace Express システムによりロックアウトされ、アプリケーションのどの部分にもアクセスできません。

解決策　システムにアクセスするには、CLI で SSLUtil コマンドを使用します。詳細については、「SSLUtil」（P. 19-8）を参照してください。

問題　CSR の生成時に、[Generate CSR] を複数回クリックした。この操作により秘密鍵が新規作成され、以前にインストールしていた証明書はすべて無効になります。

解決策　SSL 設定をバックアップしている場合は、復元します。

解決策　SSL 設定をバックアップしていない場合は、CSR を新規生成して、証明局に新規証明書を請求します。

問題　SSL 証明書の取得後に Cisco Unified MeetingPlace Express の新規インストールを実行した。Cisco Unified MeetingPlace Express システムをインストールするときは常に、インストール プログラムによりハードディスク上の秘密鍵と公開証明書がすべて削除されます。

解決策　SSL 設定をバックアップしている場合は、復元します。

解決策　SSL 設定をバックアップしていない場合は、CSR を新規生成して、証明局に新規証明書を請求します。

問題　Cisco Unified MeetingPlace Express を SSL 用に設定した後に、システムのホスト名を変更した。ホスト名はインストール時に定義されます。

解決策　新しい証明書を取得します。

問題　対になっている公開証明書と秘密鍵の共通部分が一致しない。共通部分が一致しない場合、公開証明書と秘密鍵は組み合せても機能せず、システムは SSL を使用して通信できません。

解決策　公開証明書と秘密鍵が共に機能するためには、それぞれのモジュラスと指数のフィールドに同じ値が必要です。公開証明書と秘密鍵でそれ以外の値はすべて、異なっていてかまいません。値が一致しているかどうかを確認する方法については、「証明書の内容の表示」（P. 15-7）を参照してください。

問題　証明書の名前や内部内容が同一である。証明書は、プライマリ サーバに 2 つ、セカンダリ（SMA）サーバに 2 つ必要です。

- エンドユーザ インタフェースおよび管理センター用
- Web 会議用

解決策　証明書の内容を表示する方法については、「証明書の内容の表示」（P. 15-7）を参照してください。証明書を表示したら、名前と内容が異なることを確認してください。