CHAPTER 7

SSL の設定

ここでは、Secure Sockets Layer（SSL）開始または SSL 終了のために ACE Appliance を仮想 SSL サーバとして設定する手順について説明します。この章の内容は次のとおりです。

SSL の概要

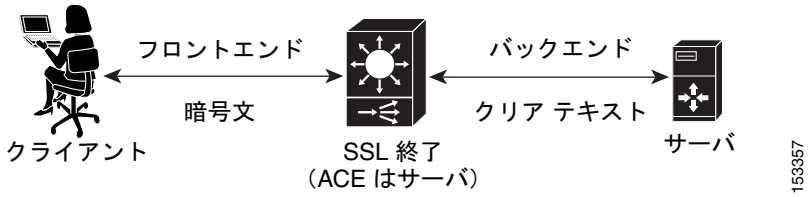
SSL は e- コマース Web サイトでのクレジット カード番号の送信など、インターネットで安全なトランザクションを確保するための暗号化テクノロジーを提供するアプリケーション レベルのプロトコルです。SSL 開始は、ACE Appliance がクライアントとして動作し、SSL サーバとの間で SSL セッションを開始する際に実行されます。SSL 終了は、SSL サーバとして動作する ACE がクライアントからの SSL 接続を終端し、続いて HTTP サーバと TCP 接続を確立するときに実行されます。

SSL は、プライバシー、認証、およびデータ整合性を組み合わせることで、クライアントとサーバの間のデータ トランザクションのセキュリティを確保します。SSL は、このアプリケーション レベルのセキュリティの実現に、証明書および秘密鍵と公開鍵の鍵交換ペアを使用します。

図 7-1 に、ACE がクライアントとの SSL 接続を終端しているネットワーク接続を示します。

- クライアントと ACE の間：クライアントと、SSL プロキシ サーバとして動作する ACE との間の SSL 接続
- ACE とサーバの間：ACE と HTTP サーバとの間の TCP 接続

図 7-1　クライアントとの SSL 終了



ACE は、パラメータ マップ、SSL プロキシ サービス、およびクラス マップを使用してポリシー マップを作成し、ポリシー マップによりクライアント、ACE、およびサーバの間の情報のフローが決まります。SSL 終了は、クライアントからのインバウンド トラフィック フローに含まれる宛先 IP アドレスに基づいているため、レイヤ 3 およびレイヤ 4 アプリケーションの 1 つです。この種類のアプリケーションの場合には、ACE がインバウンド トラフィックに適用するレイヤ 3 およびレイヤ 4 ポリシー マップをユーザが作成します。

SSL オブジェクト（認証グループ、チェーン グループ、パラメータ マップ、鍵、CRL、または証明書）のいずれかを削除する必要がある場合は、最初にプロキシ サービス内の依存関係を削除したあと SSL オブジェクトを削除しなければなりません。

ACE に SSL を設定する前に、「SSL 設定の前提条件」（P.7-3）を参照してください。

SSL 設定の前提条件

ACE に SSL 動作を設定する前に、最初に次のことを確認してください。

- ACE ハードウェアに Server Load Balancing（SLB; サーバ ロード バランシング）が設定されている。

（注）　実サーバとサーバ ファームの設定時、実サーバをサーバ ファームに関連付けるときは、実サーバの適切なポート番号を割り当てるようにしてください。ポートを指定しなかった場合、ACE のデフォルトの動作によりインバウンド接続で使用された宛先ポートがアウトバウンド サーバ接続に割り当てられます。

- ポリシー マップが、SSL セッション パラメータに加えて証明書や RSA 鍵ペアなどのクライアント/サーバ認証ツールを定義するように設定されている。
- クラス マップがポリシー マップに関連付けられており、インバウンド トラフィックの宛先 IP アドレスと完全に一致する仮想 SSL サーバ IP アドレスが定義されている。
- デジタル証明書およびそれに対応する公開鍵と秘密鍵ペアを所定の ACE コンテキストにインポートする必要があります。
- 少なくとも 1 つの SSL 証明書が使用可能である。
- 証明書とそれに対応する鍵ペアがない場合には、RSA 鍵ペアを生成し *Certificate Signing Request*（CSR）を作成できます。CSR は、*Certificate Authority*（CA; 認証局）に証明書を申請する必要がある場合に作成します。CA は CSR に署名し、認証したデジタル証明書を返します。

SSL 設定の RBAC ユーザ ロール要件

ACE での SSL に関するすべての設定では、ACE でのカスタム ロールを持つユーザは、割り当てられたロールの一部として、次の 2 つの規則を含む必要があります。

- SSL 機能を含む規則
- PKI 機能を含む規則

ユーザ ロールおよび規則の詳細については、第 13 章「ACE Appliance の管理」の「ユーザ ロールの作成」の項を参照してください。

SSL 設定手順の概要

表 7-1 に SSL 鍵と証明書を使用するための手順を示します。

表 7-1　SSL 鍵および証明書の手順概要

	作業	説明
ステップ 1	SSL パラメータ マップを作成する	SSL パラメータ マップを作成して、SSL 接続の終了方法、暗号スイート、SSL または TSL のバージョンなど、SSL セッションに適用するオプションを指定します。 「SSL パラメータ マップの設定」（P.7-17）を参照してください。
ステップ 2	SSL 鍵ペア ファイルを作成する	CSR の生成、デジタル署名の作成、および SSL ピアとの SSL ハンドシェイク時におけるパケット データの暗号化に必要な SSL RSA 鍵ペア ファイルを作成します。 「SSL 鍵ペアの生成」（P.7-12）を参照してください。
ステップ 3	CSR パラメータを作成する	CSR パラメータを設定して、CSR の Distinguished Name（DN; 認定者名）アトリビュートを定義します。 「SSL CSR パラメータの設定」（P.7-20）を参照してください。
ステップ 4	CSR を作成する	SSL 証明書の申請の際に鍵ペア ファイルと一緒に送信する CSR を作成します。 「CSR の生成」（P.7-21）を参照してください。
ステップ 5	CA の Web ベースアプリケーションに CSR をコピー アンド ペーストするか CA に CSR を E メールする	SSL 鍵ペアと CSR を使用し、CA に承認の証明書を申請します。 CA から指定される方法で申請します。
ステップ 6	CA からの承認済み証明書を、その受信形式で FTP、SFTP、または TFTP サーバに保存する	承認済み証明書を受信したら、FTP、SFTP、または TFTP 経由でアクセスできるネットワーク サーバ上に受信した形式で保存します。
ステップ 7	承認済み証明書と鍵ペアを所定の仮想コンテキストにインポートする	承認済み証明書および対応する SSL 鍵ペアを、ACE Appliance Device Manager を使用して適切なコンテキストにインポートします。 次を参照してください。 • 「SSL 証明書のインポート」（P.7-7） • 「SSL 鍵ペアのインポート」（P.7-10）
ステップ 8	鍵ペア ファイル内の公開鍵と証明書ファイル内の公開鍵が一致することを確認する	ファイルの内容を調べて、鍵ペア ファイルと証明書ファイルの中の鍵ペア情報が同一であることを確認します。
ステップ 9	仮想コンテキストに SSL を設定する	「トラフィック ポリシーの設定」（P.10-1）を参照してください。

表 7-1　SSL 鍵および証明書の手順概要 （続き）

	作業	説明
ステップ 10	認証グループを設定する	認証グループを作成することで、証明書の署名者として信頼できる証明書をグループ化します。「SSL 証明書グループの設定」（P.7-24）を参照してください。
ステップ 11	CRL を設定する	「クライアント認証での CRL の設定」（P.7-25）を参照してください。

ACE Appliance での SSL の使用方法の詳細については、『*Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*』を参照してください。

ACE Appliance に SSL を設定するには、次の内容を参照してください。

- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL パラメータ マップの設定」（P.7-17）
- 「SSL CSR パラメータの設定」（P.7-20）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL セットアップ シーケンス

SSL セットアップ シーケンスは、ACE Appliance Device Manager を使用した SSL 設定に関する詳しい説明を説明図付きで提供します（図 7-2）。このオプションの目的は、SSL CSR 生成、SSL プロキシ作成など、通常の SSL 操作を実行するための視覚的なガイドの提供です。このオプションは、ACE Appliance Device Manager にすでにある任意の既存の SSL 機能または設定画面に置き換わるものではありません。ACE で実行する必要がある SSL 操作に不慣れな方、または良く理解していない方を対象とした追加のガイドとしてだけ使用するようにしてください。SSL セットアップ シーケンスから、他の SSL 設定画面で提供される編集 / 削除 / テーブル / 表示操作と重複することなく、すべての SSL 操作を設定できます。

このオプションの目的は、次のような通常の SSL フローおよび通常の SSL 操作の実行に関連する操作の詳細を提供することです。

- SSL 鍵インポート / 作成
- SSL 証明書インポート
- SSL CSR 生成
- SSL プロキシ作成

SSL 設定機能の詳細については、「SSL 設定手順の概要」を参照してください。

図 7-2　SSL セットアップ シーケンス

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL パラメータ マップの設定」（P.7-17）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL 証明書の使用

デジタル証明書と鍵ペアは、ユーザを認証するためのデジタル識別情報の一種です。CA は証明書を発行し、その中に含まれている公開鍵が有効であることを証明します。クライアント証明書またはサーバ証明書には、次の識別情報アトリビュートがあります。

- CA の名前と CA デジタル署名
- 証明書で認証されるクライアントまたはサーバの名前（証明書サブジェクト）
- 発行元
- シリアル番号
- サブジェクトの公開鍵
- 証明書の開始日と満了日を示すタイム スタンプ

CA は、SSL 証明書と Certificate Revocation List（CRL; 証明書失効リスト）の作成に使用する 1 つ以上の署名証明書を所有しています。各署名証明書には、CA 署名の作成に使用される照合秘密鍵があります。CA は（公開鍵が組み込まれている）署名証明書を公開するため、SSL 証明書または CRL が実際に特定の CA により署名されたものであることを確認する場合には、この署名証明書にアクセスし使用することができます。

（注） ACE は、どのようなコンテキストでも最大 4 つの CRL の作成をサポートします。

ACE Appliance は、次の場合に証明書および対応する鍵ペアが必要になります。

- SSL 終了 : ACE Appliance が SSL プロキシ サーバとして動作し、クライアントとの間の SSL セッションを終端します。SSL 終了の場合、サーバ証明書および対応する鍵ペアを取得する必要があります。
- SSL 開始 : ACE Appliance がクライアントとして動作し、SSL サーバとの間の SSL セッションを開始します。SSL 開始の場合、クライアント証明書および対応する鍵ペアを取得する必要があります。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のエクスポート」（P.7-14）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵の使用」（P.7-9）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL CSR パラメータの設定」（P.7-20）
- 「CSR の生成」（P.7-21）

SSL 証明書のインポート

SSL 証明書をインポートするには、次の手順を使用します。

前提

- ACE Appliance にサーバ ロード バランシングが設定されている （「ロード バランシングの概要」（P.3-1）を参照）。
- CA から SSL 証明書を取得し、ACE Appliance がアクセスできるネットワーク サーバ上に置いてある。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Certificates]** の順に選択します。[Certificates] テーブルが表示され、有効な SSL 証明書がすべて表示されます。

ステップ 2　**[Import]** をクリックします。[Import] ダイアログボックスが表示されます。

ステップ 3　表 7-2 の情報を入力します。

表 7-2　SSL 証明書管理インポート アトリビュート

フィールド	説明
[Protocol]	ネットワーク サーバにアクセスする方法を指定します。 • [FTP] : SSL 証明書をインポートするときに、FTP サーバを使用してネットワーク サーバにアクセスします。 • [SFTP] : SSL 証明書をインポートするときに、SFTP サーバを使用してネットワーク サーバにアクセスします。 • [TFTP] : SSL 証明書をインポートするときに、TFTP サーバを使用してネットワーク サーバにアクセスします。 • [TERMINAL] : 証明書情報を端末の画面にカット アンド ペーストして、ファイルをインポートします。ASCII 形式の PEM ファイルを表示する場合は、[TERMINAL] だけを使用できます。
[IP Address]	このフィールドは、[FTP]、[TFTP]、および [SFTP] を選択した場合に表示されます。 SSL 証明書ファイルが存在するリモート サーバの IP アドレスを入力します。
[Remote File Name]	このフィールドは、[FTP]、[TFTP]、および [SFTP] を選択した場合に表示されます。 ネットワーク サーバ上の証明書ファイルのディレクトリとファイル名を入力します。
[Local File Name]	ACE Appliance に SSL 証明書ファイルがインポートされるときに使用するファイル名を入力します。
[User Name]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 ネットワーク サーバ上のユーザ アカウント名を入力します。
[Password]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 ネットワーク サーバ上のユーザ アカウントのパスワードを入力します。
[Confirm]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 パスワードを再度入力します。
[Passphrase]	このフィールドは、[FTP]、[SFTP]、および [TERMINAL] を選択した場合に表示されます。 ファイルと一緒に作成されたパスフレーズを入力します。パスフレーズがないとファイルを使用できません。パスフレーズは、暗号化された PEM と PKCS ファイルの場合にだけ使用されます。
[Confirm]	このフィールドは、[FTP]、[SFTP]、および [TERMINAL] を選択した場合に表示されます。 パスフレーズを再度入力します。

表 7-2　SSL 証明書管理インポート アトリビュート （続き）

フィールド	説明
[Non-Exportable]	SSL 証明書がエクスポート可能になっていると、署名付き証明書をネットワーク上の別のサーバにコピーして、そこから別の ACE Appliance または Web サーバにインポートできます。エクスポートは、オリジナル ファイルが削除されない点でコピーと同様の操作です。 チェックボックスを選択すると、この証明書ファイルは ACE Appliance からエクスポートできません。
[Import Text]	このフィールドは [Terminal] を選択した場合に表示されます。 証明書情報をリモート サーバから切り取り、このフィールドに貼り付けます。

ステップ 4　次のいずれかをクリックします。

- **[OK]**：入力した内容を受け入れて [Certificates] テーブルに戻ります。ACE Appliance Device Manager は、新しくインストールされた証明書で [Certificates] テーブルをアップデートします。
- **[Cancel]**：入力した内容を保存しないでこの手順は終了し、[Certificates] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 鍵の使用」（P.7-9）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL パラメータ マップの設定」（P.7-17）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL CSR パラメータの設定」（P.7-20）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL 鍵の使用

ACE Appliance とそのピアは、SSL セッションを確立する SSL ハンドシェイク時に、Rivest, Shamir, and Adelman Signatures（RSA）と呼ばれる公開鍵暗号方式を使用して認証を行います。RSA 方式では、公開鍵および対応する秘密鍵で構成される*鍵*ペアを使用します。ハンドシェイク時に RSA 鍵ペアによってセッション鍵が暗号化され、セッション鍵はハンドシェイクのあと両方のデバイスがデータを暗号化するために使用しす。

SSL および SSL 鍵の処理に必要なオプションを表示するには、次の手順を使用します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Keys]** を選択します。[Keys] テーブルが表示されます。

ステップ 2　次のいずれかのオプションに進みます。

- 鍵ペアの生成：「SSL 鍵ペアの生成」（P.7-12）を参照
- 鍵ペアのインポート：「SSL 鍵ペアのインポート」（P.7-10）を参照
- 鍵ペアのエクスポート：「SSL 鍵ペアのエクスポート」（P.7-15）を参照
- CSR の生成：「CSR の生成」（P.7-21）を参照

関連トピック

- 「SSL 鍵ペアの生成」（P.7-12）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL 鍵ペアの生成」（P.7-12）
- 「SSL 鍵ペアのエクスポート」（P.7-15）
- 「SSL の設定」（P.7-1）

SSL 鍵ペアのインポート

SSL 鍵ペア ファイルをインポートするには、次の手順を使用します。

前提

- ACE Appliance にサーバ ロード バランシングが設定されている （「ロード バランシングの概要」（P.3-1）を参照）。
- CA から SSL 鍵ペアを取得して、ACE Appliance がアクセスできるネットワーク サーバ上に置いてある。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Keys]** を選択します。[Keys] テーブルが表示され、既存の SSL 鍵が表示されます。

ステップ 2　**[Import]** をクリックします。[Import] ダイアログボックスが表示されます。

ステップ 3　表 7-3 の情報を入力します。

表 7-3　SSL 鍵ペア インポート アトリビュート

フィールド	説明
[Protocol]	ネットワーク サーバにアクセスする方法を指定します。 • [FTP] : SSL 鍵ペア ファイルをインポートするときに、FTP サーバを使用してネットワーク サーバにアクセスします。 • [SFTP] : SSL 鍵ペア ファイルをインポートするときに、SFTP サーバを使用してネットワーク サーバにアクセスします。 • [TFTP] : SSL 鍵ペア ファイルをインポートするときに、TFTP サーバを使用してネットワーク サーバにアクセスします。 • [TERMINAL] : 証明書と鍵ペア情報を端末の画面にカット アンド ペーストして、ファイルをインポートします。ASCII 形式の PEM ファイルを表示する場合は、[TERMINAL] だけを使用できます。
[IP Address]	このフィールドは、[FTP]、[TFTP]、および [SFTP] を選択した場合に表示されます。 SSL 鍵ペア ファイルが存在するリモート サーバの IP アドレスを入力します。
[Remote File Name]	このフィールドは、[FTP]、[TFTP]、および [SFTP] を選択した場合に表示されます。 ネットワーク サーバ上の鍵ペア ファイルのディレクトリとファイル名を入力します。
[Local File Name]	ACE Appliance に SSL 鍵ペア ファイルがインポートされるときに使用するファイル名を入力します。
[User Name]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 ネットワーク サーバ上のユーザ アカウント名を入力します。
[Password]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 ネットワーク サーバ上のユーザ アカウントのパスワードを入力します。
[Confirm]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 パスワードを再度入力します。
[Passphrase]	このフィールドは、[FTP]、[SFTP]、および [TERMINAL] を選択した場合に表示されます。 ファイルと一緒に作成されたパスフレーズを入力します。パスフレーズがないとファイルを使用できません。パスフレーズは、暗号化された PEM と PKCS ファイルの場合にだけ使用されます。
[Confirm]	このフィールドは、[FTP]、[SFTP]、および [TERMINAL] を選択した場合に表示されます。 パスフレーズを再度入力します。

表 7-3　SSL 鍵ペア インポート アトリビュート （続き）

フィールド	説明
[Non-Exportable]	SSL 鍵ペア ファイルがエクスポート可能になっていると、鍵ペア ファイルをネットワーク上の別のサーバにコピーして、そこから別の ACE Appliance または Web サーバにインポートできます。エクスポートは、オリジナル ファイルが削除されない点でコピーと同様の操作です。 チェックボックスを選択すると、この鍵ペア ファイルは ACE Appliance からエクスポートできません。チェックボックスをクリアすると、この鍵ペア ファイルは ACE Appliance からエクスポートできます。
[Import Text]	このフィールドは [Terminal] を選択した場合に表示されます。 鍵ペア情報をリモート サーバから切り取り、このフィールドに貼り付けます。

ステップ 4　次のいずれかをクリックします。

- **[OK]**：入力した内容を受け入れて [Keys] テーブルに戻ります。ACE Appliance Device Manager は、インポートした鍵ペア ファイル情報で [Keys] テーブルをアップデートします。
- **[Cancel]**：入力した内容を保存しないでこの手順は終了し、[Keys] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL パラメータ マップの設定」（P.7-17）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL CSR パラメータの設定」（P.7-20）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL 鍵ペアの生成

照合鍵ペアがない場合、ACE Appliance を使用して鍵ペアを生成できます。

SSL RSA 鍵ペアを生成するには、次の手順を使用します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Keys]** を選択します。[Keys] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして、新しい鍵ペアを追加します。[Keys] 設定画面が表示されます。

（注）　[Keys] テーブル内の既存のエントリを変更することはできません。変更する代わりに、その既存のエントリを削除してから新しいエントリを追加します。

ステップ 3　[Name] フィールドに、SSL 鍵ペアの名前を入力します。有効な入力は英数値ストリングで、最大 40 文字です。

ステップ 4　[Size] フィールドで、鍵ペアのセキュリティ強度を選択します。Web トランザクションの安全を確保するために使用される RSA 鍵ペアのサイズは、鍵ペア ファイルのビット数で決まります。鍵を長くするほど RSA セキュリティ ポリシーの強度が増し、より安全な実装になります。オプションと関連するセキュリティ レベルは次のとおりです。

- [512]：最低限のセキュリティ
- [768]：通常のセキュリティ
- [1024]：高度なセキュリティ、レベル 1
- [1536]：高度なセキュリティ、レベル 2
- [2048]：高度なセキュリティ、レベル 3

ステップ 5　[Type] フィールドに、認証に使用される公開鍵暗号方式として **[RSA]** を指定します。

ステップ 6　[Exportable Key] フィールドで、チェックボックスを選択して鍵ペア ファイルをエクスポート可能にします。チェックボックスをクリアすると、鍵ペア ファイルはエクスポートできません。

ステップ 7　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を適用します。
- **[Cancel]**：入力した内容を保存しないでこの手順は終了し、[Keys] テーブルに戻ります。
- **[Next]**：入力した内容が保存され、別の RSA 鍵ペアを定義します。

RSA 鍵ペアを生成した後は、次の作業を行うことができます。

- CSR パラメータ セットを作成します。CSR パラメータ セットでは、ACE Appliance が CSR 生成プロセス時に使用する DN 名アトリビュートを定義します。CSR パラメータ セットの定義方法の詳細については、「SSL CSR パラメータの設定」（P.7-20）を参照してください。
- RSA 鍵ペア ファイル用の CSR を生成し、CSR 要求を CA に送信して署名を求めます。この方法を採ると、RSA 秘密鍵は ACE Appliance 内で直接作成され、外で転送される必要がないことから、セキュリティが強化されます。生成した各鍵ペアは対応する証明書が伴わないと機能しません。CSR を生成する詳細については、「CSR の生成」（P.7-21）を参照してください。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL CSR パラメータの設定」（P.7-20）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL 証明書のエクスポート

SSL 証明書がエクスポート可能になっていると、署名付き証明書をネットワーク上の別のサーバにコピーして、そこから別の ACE Appliance または Web サーバにインポートできます。証明書のエクスポートは、オリジナルの証明書が削除されない点でコピーと同様の操作です。

SSL 証明書を ACE Appliance からリモート サーバにエクスポートするには、次の手順を使用します。

前提

SSL 証明書がエクスポート可能になっている （「SSL 証明書のインポート」（P.7-7）を参照）。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Certificates]** の順に選択します。[Certificates] テーブルが表示され、有効な SSL 証明書がすべて表示されます。

ステップ 2　エクスポートする証明書を選択し、**[Export]** をクリックします。[Export] ダイアログボックスが表示されます。

ステップ 3　表 7-4 の情報を入力します。

表 7-4　SSL 証明書エクスポート アトリビュート

フィールド	説明
[Protocol]	SSL 証明書をエクスポートする方法を指定します。 • [FTP] : SSL 証明書をエクスポートするときに、FTP サーバを使用してネットワーク サーバにアクセスします。 • [SFTP] : SSL 証明書をエクスポートするときに、SFTP サーバを使用してネットワーク サーバにアクセスします。 • [TFTP] : SSL 証明書をエクスポートするときに、TFTP サーバを使用してネットワーク サーバにアクセスします。 • [TERMINAL] : 証明書と鍵ペア情報を端末の画面にカット アンド ペーストして、証明書をエクスポートします。ASCII 形式の PEM ファイルを表示する場合は、[TERMINAL] だけを使用できます。
[IP Address]	このフィールドは、[FTP]、[TFTP]、および [SFTP] を選択した場合に表示されます。 SSL 証明書ファイルをエクスポートする先のリモート サーバの IP アドレスを入力します。
[Remote File Name]	このフィールドは、[FTP]、[TFTP]、および [SFTP] を選択した場合に表示されます。 リモート ネットワーク サーバの、SSL 証明書ファイル用に使用されるディレクトリとファイル名を入力します。
[User Name]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 リモート ネットワーク サーバのユーザ アカウント名を入力します。

表 7-4　SSL 証明書エクスポート アトリビュート （続き）

フィールド	説明
[Password]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 リモート ネットワーク サーバのユーザ アカウントのパスワードを入力します。
[Confirm]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 パスワードを再度入力します。

ステップ 4　次のいずれかをクリックします。

- **[OK]**：証明書をエクスポートして [Certificates] テーブルに戻ります。
- **[Cancel]**：証明書をエクスポートしないでこの手順は終了し、[Certificates] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL 鍵ペアの生成」（P.7-12）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL CSR パラメータの設定」（P.7-20）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL 鍵ペアのエクスポート

SSL 鍵ペアがエクスポート可能になっていると、SSL 鍵ペア ファイルをネットワーク上の別のサーバにコピーして、そこから別の ACE Appliance または Web サーバにインポートできます。鍵ペア ファイルのエクスポートは、オリジナルの鍵ペアが削除されない点でコピーと同様の操作です。

SSL 鍵ペアを ACE Appliance からリモート サーバにエクスポートするには、次の手順を使用します。

前提

SSL 鍵ペアがエクスポート可能になっている（「SSL 鍵ペアの生成」（P.7-12）を参照）

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Keys]** を選択します。[Keys] テーブルが表示されます。

ステップ 2　エクスポートする鍵のエントリを選択し、**[Export]** をクリックします。[Export] ダイアログボックスが表示されます。

ステップ 3　表 7-5 の情報を入力します。

表 7-5　SSL 鍵 エクスポート アトリビュート

フィールド	説明
[Protocol]	SSL 鍵ペアをエクスポートする方法を指定します。 • [FTP] : SSL 鍵ペアをエクスポートするときに、FTP サーバを使用してネットワーク サーバにアクセスします。 • [SFTP] : SSL 鍵ペアをエクスポートするときに、SFTP サーバを使用してネットワーク サーバにアクセスします。 • [TFTP] : SSL 鍵ペアをエクスポートするときに、TFTP サーバを使用してネットワーク サーバにアクセスします。 • [TERMINAL] : 鍵ペア情報を端末の画面にカット アンド ペーストして、鍵ペアをエクスポートします。ASCII 形式の PEM ファイルを表示する場合は、[TERMINAL] だけを使用できます。
[IP Address]	このフィールドは、[FTP]、[TFTP]、および [SFTP] を選択した場合に表示されます。 SSL 鍵ペアをエクスポートする先のリモート サーバの IP アドレスを入力します。
[Remote File Name]	このフィールドは、[FTP]、[TFTP]、および [SFTP] を選択した場合に表示されます。 リモート ネットワーク サーバの、SSL 鍵ペア ファイル用に使用されるディレクトリとファイル名を入力します。
[User Name]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 リモート ネットワーク サーバのユーザ アカウント名を入力します。
[Password]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 リモート ネットワーク サーバのユーザ アカウントのパスワードを入力します。
[Confirm]	このフィールドは、[FTP] と [SFTP] を選択した場合に表示されます。 パスワードを再度入力します。

ステップ 4　次のいずれかをクリックします。

- **[OK]**：鍵ペアをエクスポートして [Keys] テーブルに戻ります。
- **[Cancel]**：鍵ペアをエクスポートしないでこの手順は終了し、[Keys] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL 鍵ペアの生成」（P.7-12）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL CSR パラメータの設定」（P.7-20）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL パラメータ マップの設定

SSL パラメータ マップでは、ACE Appliance が SSL プロキシ サービスに適用する SSL セッション パラメータを定義します。SSL パラメータ マップを使用すると、同じ SSL セッション パラメータを異なるプロキシ サービスに適用できます。

SSL パラメータ マップを作成するには、次の手順を使用します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Parameter Maps]** を選択します。[Parameter Maps] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして新しい SSL パラメータ マップを追加するか、または変更する既存のエントリを選択し、**[Edit]** をクリックします。[Parameter Map] 設定画面が表示されます。

ステップ 3　[Parameter Map Name] フィールドにパラメータ マップの一意の名前を入力します。有効な入力は英数値ストリングで、最大 64 文字です。

ステップ 4　[In the Queue Delay Timeout (Milliseconds)] フィールドに、キューのデータを取り出して暗号化する前の待機時間をミリ秒で設定します。デフォルトの遅延時間は 200 ミリ秒です。0（ディセーブル）～ 10000 の間で調整できます。ディセーブル（0 に設定）にした場合、ACE はサーバからデータが着信するとすぐに暗号化し、暗号化したデータをクライアントに送信します。

（注）　[Queue Delay Timeout] は、SSL モジュールがクライアントに送信するデータにだけ適用されます。こうすることで、実サーバに小さな HTTP GET を渡す際に遅延が長くなる可能性を避けられます。

ステップ 5　[Session Cache Timeout (Milliseconds)] フィールドに、SSL セッション ID を有効なままにするタイムアウト値を指定します。この時間が経過すると、ACE は完全な SSL ハンドシェイクを行わないと新しい SSL セッションを確立できません。ACE はこの期間、クライアントとの後続の接続にマスター鍵を再利用することができ、SSL ネゴシエーション プロセスを短縮化できます。デフォルト値は 300 秒（5 分）で、0（無期限のタイムアウト、つまりセッション ID はキャッシュがフルになったときにだけキャッシュから削除されます）～ 72000（20 時間）です。0 を指定すると、ACE は Least Recently Used（LRU）タイムアウト ポリシーを適用します。このオプションをディセーブルにすると、ACE との新しい接続のたびに完全な SSL ハンドシェイクが行われます。

ステップ 6　[Reject Expired CRLs] フィールドで、チェックボックスをクリックして選択し、失効した CRL が使用できるかどうかを指定します。選択すると、失効した CRL は許可されません。

ステップ 7　[Close Protocol Behavior] フィールドで、SSL 接続の終了に使用する方法を選択します。

- [Disabled] : ACE Appliance は終了通知アラート メッセージを SSL ピアに送信しますが、SSL ピア側は終了通知アラート メッセージを待ってからセッションを削除することはしません。SSL ピアが終了通知アラート メッセージを送信するかどうかに関わらずセッション情報は保存されるため、以降の SSL セッションでセッションの回復が可能です。
- [None] : ACE Appliance は終了通知アラート メッセージを SSL ピアに送信せず、ACE Appliance は SSL ピアからの終了通知アラート メッセージを待つこともしません。ACE Appliance は以後の SSL 接続に SSL の回復ができるようにセッション情報を保存します。

ステップ 8　[SSL Version] フィールドに、SSL 通信時に使用する SSL のバージョンを入力します。

- [All] : ACE Appliance は、ピア ACE Appliance との通信に SSL v3 と TLS v1 の両方を使用します。
- [SSL3] : ACE Appliance は、ピア ACE Appliance との通信に SSL v3 だけを使用します。

- [TLS1]：ACE Appliance は、ピア ACE Appliance との通信に TLS v1 だけを使用します。

ステップ 9　[Ignore Authentication Failure] フィールドで、チェックボックスを選択すると、SSL 開始設定の際に失効または無効のサーバ証明書を無視し、バックエンド接続の設定を続行します。チェックボックスを選択解除すると、デフォルトの設定であるディセーブルに戻ります。このフィールドを選択すると、ACE Appliance はサーバ証明書に関する次の非重大エラーを無視します。

- Certificate not yet valid
- Certificate has expired
- Unable to get issuer certificate
- Certificate revoked

ステップ 10　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を適用します。[Parameter Map] 画面がアップデートされ、[Parameter Map Cipher] テーブルが表示されます。ステップ 11 に進みます。
- **[Cancel]**：入力した内容を保存しないでこの手順は終了し、[Parameter Map] テーブルに戻ります。
- **[Next]**：入力した内容を保存し、別のパラメータ マップを定義します。

ステップ 11　[Parameter Map Cipher] テーブルで、**[Add]** をクリックして暗号を追加するか、または既存の暗号を選択し、**[Edit]** をクリックします。[Parameter Map Cipher] 設定画面が表示されます。

ステップ 12　[Cipher Name] フィールドで、使用する暗号を選択します。ACE Appliance でサポートされる SSL 暗号スイートの詳細については、『*Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*』を参照してください。

ステップ 13　[Cipher Priority] フィールドに、この暗号スイートに割り当てるプライオリティを入力します。このプライオリティは、使用する暗号の優先順位を意味します。有効な値は 1 ～ 10 の整数です。1 は優先順位が最も低く、10 は優先順位が最も高くなります。ACE Appliance は使用する暗号スイートの決定時に、最高のプライオリティの暗号スイートを選択します。

ステップ 14　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を適用します。
- **[Cancel]**：入力した内容を保存しないで手順は終了し、[Parameter Map Cipher] テーブルに戻ります。
- **[Next]**：入力した内容が保存され、[Parameter Map Cipher] テーブルに別のエントリを追加します。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL 鍵ペアの生成」（P.7-12）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL CSR パラメータの設定」（P.7-20）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL チェーン グループ パラメータの設定

チェーン グループでは、ACE Appliance がハンドシェイク時にピアに送信する*証明書チェーン*を指定します。証明書チェーンは、ACE Appliance 証明書、ルート CA 証明書、および中間 CA 証明書などを含む証明書の階層リストです。証明書の検証者は、証明書チェーンで提供される情報を使用して、証明書階層リストをルート CA まで溯って信頼できる CA を検索できます。ルート CA 証明書に達する前に信頼できる CA を見つけた場合には、そこで検索を終えます。

仮想コンテキストの証明書チェーンを設定するには、次の手順を使用します。

前提

少なくとも 1 つの SSL 証明書が使用可能である。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Chain Group Parameters]** の順に選択します。[Chain Group Parameters] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして新しいチェーン グループを追加するか、または既存のチェーン グループを選択し、**[Edit]** をクリックして変更します。[Chain Group Parameters] 設定画面が表示されます。

ステップ 3　[Name] フィールドにチェーン グループの一意の名前を入力します。有効な入力は英数値ストリングで、最大 64 文字です。

ステップ 4　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を適用します。[Chain Group Parameters] 画面が更新され、[Chain Group Certificates] テーブルが表示されます。ステップ 5 に進みます。
- **[Cancel]**：入力した内容を保存しないで手順は終了し、[Chain Group Parameters] テーブルに戻ります。
- **[Next] :** 入力した内容が保存され、[Chain Group Parameters] テーブルに別のエントリを追加します。

ステップ 5　[Chain Group Certificates] テーブルで、**[Add]** をクリックしてエントリを追加します。[Chain Group Certificates] 設定画面が表示されます。

（注）　[Chain Group Certificates] テーブル内の既存のエントリを変更することはできません。変更する代わりに、そのエントリを削除してから新しいエントリを追加します。

ステップ 6　[Certificate Name] フィールドで、このチェーン グループに追加する証明書を選択します。

ステップ 7　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を適用します。
- **[Cancel]**：入力した内容を保存しないで手順は終了し、[Chain Group Certificates] テーブルに戻ります。
- **[Next]**：入力した内容が保存され、このチェーン グループ テーブル別の証明書を追加します。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）

SSL CSR パラメータの設定

Certificate Signing Request（CSR; 証明書署名要求）は、VeriSign や Thawte などの CA にデジタル ID 証明書を申請するために送信するメッセージです。CSR は、所在地、シリアル番号、選択した公開鍵など SSL サイトを特定する情報で構成されます。対応する秘密鍵は CSR に含まれていませんが、CSR にデジタル署名するために使用されます。CSR には、CA が必要とする身元についての他の認定証や証明情報が添付されることがあります。CA は申請者と連絡を取ってさらに情報を求めることがあります。

申請に問題がなければ、CA は（CA の秘密鍵で）デジタル署名された ID 証明書を返します。

CSR パラメータでは、ACE Appliance が CSR 生成プロセス時に CSR に適用する *Distinguished Name*（DN; 認定者名）アトリビュートを定義します。CA はサイトを認証するために必要な情報をこれらのアトリビュートから取得します。CSR パラメータ セットを定義すると、同じ DN アトリビュートを持つ複数の CSR を生成できます。

ACE Appliance の各コンテキストには、最大 8 つの CSR パラメータ セットを格納できます。

SSL CSR の DN アトリビュートを定義するには、次の手順を使用します。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [CSR Parameters]** の順に選択します。[CSR Parameters] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして新しい CSR アトリビュート セットを追加するか、または変更する既存のエントリを選択し、**[Edit]** をクリックします。[CSR Parameters] 設定画面が表示されます。

ステップ 3　[Name] フィールドにこのパラメータ セットの一意の名前を入力します。有効な入力は英数値ストリングで、最大 64 文字です。

ステップ 4　[Country] フィールドに、SSL サイトの所在する国名を入力します。有効な値は、国を表す英字 2 文字です（例：米国は *US*）。この有効な国コードの全リストは、International Organization for Standardization（ISO; 国際標準化機構）が Web 上で管理しています（www.iso.org）。

ステップ 5　[State] フィールドに、SSL サイトの所在する都道府県名を入力します。

ステップ 6　[Locality] フィールドに、SSL サイトの所在する市町村名を入力します。

ステップ 7　[Common Name] フィールドには、SSL サイトのドメイン名またはホスト名を入力します。有効な入力は英数値ストリングで、最大 64 文字です。ACE は、次の特殊文字をサポートしています。, . / = + - ^ @ ! % ~ # $ * ( ).

ステップ 8　[Serial Number] フィールドには、証明書に割り当てるシリアル番号を入力します。有効な入力は英数値ストリングで、最大 16 文字です。

ステップ 9　[Organization Name] フィールドに、証明書に記載する組織名を入力します。有効な入力は英数値ストリングで、最大 64 文字です。

ステップ 10　[Email] フィールドに、サイトの E メール アドレスを入力します。有効な入力は英数値ストリングで、最大 40 文字です。

ステップ 11　[Organization Unit] フィールドに、証明書に記載する組織名を入力します。有効な入力は英数値ストリングで、最大 64 文字です。

ステップ 12　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を適用します。
- **[Cancel]**：入力した内容を保存しないでこの手順は終了し、[CSR Parameters] テーブルに戻ります。
- **[Next]**：入力した内容を保存し、別の CSR アトリビュート セットを定義します。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL パラメータ マップの設定」（P.7-17）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL プロキシ サービスの設定」（P.7-22）

CSR の生成

Certificate Signing Request（CSR）は、VeriSign や Thawte などの CA にデジタル ID 証明書を申請するために送信するメッセージです。CA に証明書を申請する必要がある場合は、CSR を作成します。CA は申請を承認すると、CSR に署名し、認証したデジタル証明書を返します。この証明書には、CA の秘密鍵が含まれています。認証された証明書と鍵ペアを受信したら、インポートして使用することができます（「SSL 証明書のインポート」（P.7-7）および「SSL 鍵ペアのインポート」（P.7-10）を参照）。

SSL CSR を生成するには、次の手順を使用します。

前提

SSL CSR パラメータが設定されている（「SSL CSR パラメータの設定」（P.7-20）を参照）

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Keys]** を選択します。[Keys] テーブルが表示されます。

ステップ 2　テーブル内の鍵を選択し、**[Generate CSR]** をクリックします。[Generate a Certificate Signing Request] ダイアログボックスが表示されます。

ステップ 3　[CSR Parameter] フィールドで、使用する CSR パラメータを選択します。

ステップ 4　次のいずれかをクリックします。

- **[OK]**：CSR が生成されます。CSR がポップアップ ウィンドウに表示されます。これを CA に送信して承認を受けることができます。CA と連絡を取り、E メールや Web ベース アプリケーションなどの送信方法を決定します。**[Close]**：ポップアップ ウィンドウが閉じ、[Keys] テーブルに戻ります。
- **[Cancel]**：CSR を生成しないでこの手順は終了し、[Keys] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL パラメータ マップの設定」（P.7-17）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL プロキシ サービスの設定」（P.7-22）

SSL プロキシ サービスの設定

SSL プロキシ サービスでは、ACE Appliance が SSL ハンドシェイク時に使用する SSL パラメータ マップ、鍵ペア、証明書、およびチェーン グループを定義します。ACE Appliance に SSL プロキシ *サーバ* サービスを設定することで、ACE Appliance は SSL サーバとして動作できます。

ACE Appliance が SSL サーバとして動作できるよう SSL ハンドシェイク時に使用するアトリビュートを定義するには、次の手順を使用します。

前提

このプロキシ サービスに適用される少なくとも 1 つの SSL 鍵ペア、証明書、チェーン グループ、またはパラメータ マップが設定してある

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Proxy Service]** の順に選択します。[Proxy Service] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして新しいプロキシ サービスを追加するか、または既存のサービスを選択し、**[Edit]** をクリックして変更します。[Proxy Service] 設定画面が表示されます。

ステップ 3　[Name] フィールドにこのプロキシ サービスの一意の名前を入力します。有効な入力は英数値ストリングで、最大 26 文字です。

ステップ 4　[Key] フィールドで、ACE Appliance が SSL ハンドシェイク時にデータの暗号化に使用する鍵ペアを選択します。

ステップ 5　[Certificate] フィールドで、ACE Appliance が SSL ハンドシェイク時に自身の身元の証明に使用する鍵ペアを選択します。

ステップ 6　[Chain Groups] フィールドで、ACE Appliance が SSL ハンドシェイク時に使用するチェーン グループを選択します。

ステップ 7　[Auth Groups] フィールドで、ACE が SSL ハンドシェイク時に使用する認証グループ名を選択します。認証グループを作成するには、「SSL 証明書グループの設定」（P.7-24）を参照してください。

[CRL Best-Effort] フィールドは、Auth Group Name が選択された場合にだけ表示されます。これにより、ACE Appliance はサービスのクライアント証明書を検索して、拡張領域内に CRL が含まれているかどうかを確認できます。CRL がある場合、ACE Appliance は値を取得します。

ステップ 8　[CRL Name] フィールドに、CRL 名を入力します。

ステップ 9　[Parameter Maps] フィールドで、この SSL プロキシ サーバ サービスに関連付ける SSL パラメータ マップを選択します。

ステップ 10　次のいずれかをクリックします。

- **[Deploy Now]**：ACE Appliance にこの設定を適用します。
- **[Cancel]**：入力した内容を保存しないでこの手順は終了し、[Proxy Service] テーブルに戻ります。
- **[Next]**：入力した内容を保存し、別のプロキシ サービスを追加します。

関連トピック

- 「SSL の設定」（P.7-1）
- 「SSL 証明書のインポート」（P.7-7）
- 「SSL 鍵ペアのインポート」（P.7-10）
- 「SSL パラメータ マップの設定」（P.7-17）
- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「SSL CSR パラメータの設定」（P.7-20）

クライアント認証のイネーブル化

通常の SSL ハンドシェイクでは、SSL サーバが自身の証明書をクライアントに送信します。続いて、クライアントはその証明書からサーバの身元を確認します。ただし、クライアントは、クライアント自身の識別情報をサーバに送信しません。クライアント認証機能をイネーブルにすると、ACE はクライアントに対し証明書をサーバに送信するように要求します。次に、サーバは下記の情報について検証します。

- 認定されている CA が証明書を発行した。
- 証明書の有効期間が満了していない。
- 証明書の署名が有効で偽造されていない。
- CA が証明書を取り消していない。
- 少なくとも 1 つの SSL 証明書が使用可能である。

クライアント認証をイネーブルまたはディセーブルにするには、次の手順を使用します。

- 「SSL プロキシ サービスの設定」（P.7-22）
- 「SSL 証明書グループの設定」（P.7-24）
- 「クライアント認証での CRL の設定」（P.7-25）

SSL 証明書グループの設定

ACE では、認証グループを作成することで、証明書の署名者として信頼できる証明書のグループを実装できます。認証グループを作成し証明書を割り当てたら、SSL 終了設定内のプロキシ サービスに認証グループを割り当てて、クライアント認証をイネーブルにできます。クライアント認証の詳細については、「クライアント認証のイネーブル化」（P.7-23）を参照してください。

サーバ認証の情報と認証グループの割り当て方法については、「SSL プロキシ サービスの設定」（P.7-22）を参照してください。

SSL ハンドシェイク時に ACE が使用する証明書認証グループを指定し、この SSL プロキシ サービスのクライアント認証をイネーブルにするには、次の手順を使用します。ACE には、認証グループ内に設定されている証明書と SSL プロキシ サービスに指定されている証明書が含まれています。

前提

- 少なくとも 1 つの SSL 証明書が使用可能である。
- 使用する ACE Appliance が認証グループをサポートしている。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Auth Group Parameters]** の順に選択します。

[Auth Group Parameters] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして認証グループを追加するか、または既存の認証グループを選択し、**[Edit]** をクリックして変更します。[Auth Group Parameters] 設定画面が表示されます。

ステップ 3　[Name] フィールドに認証グループの一意の名前を入力します。有効な入力は英数値ストリングで、最大 64 文字です。

ステップ 4　次のいずれかをクリックします。

- **[Deploy Now]**：ACE にこの設定を適用します。[Auth Group Parameters] 画面が更新され、[Auth Group Certificates] テーブルが表示されます。ステップ 5 に進みます。
- **[Cancel]**：入力した内容を保存しないで手順は終了し、[Auth Group Parameters] テーブルに戻ります。
- **[Next]**：入力した内容が導入され、[Auth Group Parameters] テーブルに別のエントリを追加します。

ステップ 5　[Auth Group Certificate] フィールドで、**[Add]** をクリックしてエントリを追加します。[Auth Group Certificates] 設定画面が表示されます。

（注）　[Auth Group Certificates] テーブル内の既存のエントリを変更することはできません。変更する代わりに、そのエントリを削除してから新しいエントリを追加します。

ステップ 6　[Certificate Name] フィールドで、この認証グループに追加する証明書を選択します。

ステップ 7　次のいずれかをクリックします。

- **[Deploy Now]**：ACE にこの設定を適用します。
- **[Cancel]**：入力した内容を保存しないで手順は終了し、[Auth Group Parameters] テーブルに戻ります。
- **[Next]**：入力した内容が導入され、[Auth Group Parameters] テーブルに別のエントリを追加します。

ステップ 8　前のステップを繰り返すと認証グループにさらに証明書を追加できます。追加しない場合は、**[Deploy Now]** をクリックします。

ステップ 9　認証グループ パラメータを設定したら、CRL を使用するように SSL プロキシ サービスを設定できます。「クライアント認証での CRL の設定」（P.7-25）を参照してください。

（注）　クライアント認証をイネーブルにした場合、パフォーマンスが大きく低下することがあります。CRL 取得を設定すると遅延が増えることがあります。

関連トピック

- 「SSL チェーン グループ パラメータの設定」（P.7-19）
- 「クライアント認証での CRL の設定」（P.7-25）

クライアント認証での CRL の設定

デフォルトでは、ACE はクライアント認証時に CRL を使用しません。SSL プロキシ サービスで CRL を使用できるように設定するには、ACE にサービスの各クライアント証明書をスキャンさせて拡張領域内に CRL が含まれているかどうかを確認し、CRL がある場合は値を取得させます。ACE での SSL 終了の詳細については、『*Cisco 4700 Series Application Control Engine Appliance SSL Configuration Guide*』を参照してください。

（注）　ACE は、どのようなコンテキストでも最大 4 つの CRL の作成をサポートします。

（注）　クライアント認証をイネーブルにした場合、パフォーマンスが大きく低下することがあります。CRL 取得を設定すると遅延が増えることがあります。

スキャンによる CRL の確認と取得を行うように ACE を設定するには、次の手順を使用します。

前提

認証グループを最初に設定しないと SSL プロキシに CRL を設定できません。

手順

ステップ 1　**[Config] > [Virtual Contexts] > [*context*] > [SSL] > [Certificate Revocation Lists (CRL)]** の順に選択します。[Certificate Revocation List] テーブルが表示されます。

ステップ 2　**[Add]** をクリックして CRL を追加するか、または既存の CRL 選択し、**[Edit]** をクリックして変更します。[Certificate Revocation List] 画面が表示されます。

ステップ 3　表 7-6 の情報を入力します。

表 7-6　SSL 証明書失効リスト

フィールド	説明
[Name]	CRL 名を入力します。有効な値は、引用符なしの英数字です（最大 64 文字）。
[URL]	ACE が CRL を取得する URL を入力します。有効な値は、引用符なしの英数字です（最大 255 文字）。HTTP URL だけがサポートされています。ACE は URL をチェックし、一致しなければエラーを表示します。

ステップ 4　次のいずれかをクリックします。

- **[Deploy Now]**：ACE にこの設定を適用します。[Certificate Revocation List] テーブルが更新されて表示されます。
- **[Cancel]**：、入力した内容を保存しないで手順は終了し、[CRL] テーブルに戻ります。
- **[Next]**：入力した内容が導入され、[CRL] テーブルに別のエントリを追加します。

関連トピック

- 「SSL プロキシ サービスの設定」（P.7-22）
- 「SSL 証明書グループの設定」（P.7-24）