CHAPTER 9

SSL の設定

（注） この章の情報は、ペイロード暗号化プロトコルを排除した ACE NPE のソフトウェア バージョンに適用されません（「ACE No Payload Encryption ソフトウェア バージョン関する情報」（P.1-2）を参照）。

この章では、Secure Sockets Layer（SSL）開始または SSL 終了のために、ACE アプライアンスを仮想 SSL サーバとして設定する手順について説明します。

（注） ACE CLI を使用して名前付きオブジェクト（実サーバ、仮想サーバ、パラメータ マップ、クラス マップ、ヘルス プローブなど）を設定するとき、Device Manager（DM）でサポートされるのは、1 ～ 64 文字の英数字文字列を使用したオブジェクト名であることに注意してください。オブジェクト名には、下線（_）、ハイフン（-）、ドット（.）、およびアスタリスク（*）の特殊文字を含めることができます。スペースは使用できません。

ACE CLI を使用して、DM でサポートされていない特殊文字を含んだ名前付きオブジェクトを設定した場合、DM を使用して ACE を設定できない場合があります。

この章は、次のセクションで構成されています。

SSL の概要

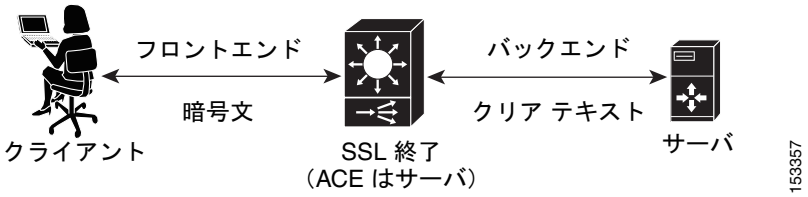
SSL は e- コマース Web サイトでのクレジット カード番号の送信など、インターネットで安全なトランザクションを確保するための暗号化テクノロジーを提供するアプリケーション レベルのプロトコルです。SSL 開始は、ACE アプライアンスがクライアントとして動作し、SSL サーバとの間で SSL セッションを開始する際に実行されます。SSL 終了は、SSL サーバとして動作する ACE がクライアントからの SSL 接続を終端し、続いて HTTP サーバと TCP 接続を確立するときに実行されます。

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、証明書および秘密キーと公開キーのキー交換ペアを使用します。

図 9-1 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 9-1　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、キー、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.9-3）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 ハードウェアにサーバ ロード バランシング（SLB）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 キー 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キーと秘密キー 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キー ペアがない場合には、RSA キー ペアを生成し *Certificate Signing Request*（CSR）を作成できます。CSR は、*認証局*（CA）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 15 章「ACE アプライアンスの管理」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 9-1 に SSL キーと証明書を使用するための手順を示します。

表 9-1　SSL キー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 TLS 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.9-20）を参照してください。
ステップ 2	SSL キー 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 キー ペア ファイルを作成します。 「SSL キーペアの生成」（P.9-15）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 の認定者名（DN）属性を定義します。 「SSL CSR パラメータの設定」（P.9-26）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キー 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.9-27）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 キー 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	承認済み証明書とキー 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 キー ペアを、ACE アプライアンス 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。 次の項を参照してください。 • 「SSL 証明書のインポート」（P.9-8） • 「SSL キー ペアのインポート」（P.9-12）
ステップ 8	キー ペア ファイル内の公開キーと証明書ファイル内の公開キーが一致することを確認する	ファイルの内容を調べて、キー ペア ファイルと証明書ファイルの中のキー 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.12-1）を参照してください。
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.9-32）を参照してください。

表 9-1　SSL キーおよび証明書の手順概要 （続き）

	作業	説明
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.9-33）を参照してください。
ステップ 12	SSL OCSP サービスを設定する	「SSL OCSP サービスの設定」（P.9-30）を参照してください。

ACE アプライアンスでの SSL の使用方法の詳細については、『*SSL Guide, Cisco ACE Application Control Engine*』を参照してください。

ACE アプライアンス で SSL を使用するための設定方法については、次のトピックを参照してください。

- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL パラメータ マップの設定」（P.9-20）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL プロキシ サービスの設定」（P.9-28）
- 「SSL OCSP サービスの設定」（P.9-30）

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 アプライアンス 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 9-2）。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 アプライアンス 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 キー 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

（注）　ACE Device Manager の SSL セットアップ シーケンスでは、*SSL ポリシー*および *SSL プロキシ サービス*という用語を共通の意味で使用しています。

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 9-2　SSL セットアップ シーケンス

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL パラメータ マップの設定」（P.9-20）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL プロキシ サービスの設定」（P.9-28）

SSL 証明書の使用

[Config] > [Virtual Contexts] > [*context*] > [Certificates] を選択することによって、ACE にインストールされたコンテキストの証明書および照合キー ペアのリストを表示できます。[Certificates] ウィンドウが開き、インストールされている証明書のリストを表示します。

デジタル証明書とキー 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キー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、次の識別情報属性があります。

- 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）
- 発行者
- シリアル番号
- サブジェクトが一致する証明書の公開キー
- 証明書の開始日と満了日を示すタイム スタンプ
- CA 証明書

CA は、SSL 証明書と証明書失効リスト（CRL）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キーがあります。CA は（公開キー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 8 つの CRL の作成をサポートします。

ACE アプライアンスは、次の場合に証明書および対応するキー ペアが必要になります。

- SSL 終了 : ACE アプライアンスが 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キー ペアを取得する必要があります。
- SSL 開始 : ACE アプライアンス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キー ペアを取得する必要があります。

[Certificates] ウィンドウ（[Config] > [Virtual Contexts] > [context] > [Certificates]）の [Matching Key] カラムは、ACE アプライアンス Device Manager で証明書と一致したキー ペアの名前を表示します。ACE アプライアンス Device Manager で証明書の照合キー ペアを検出できない場合は、[Matching Key] テーブルのセルを空白のままにします。一致しない証明書とキー ペアの数が 50 を超えると、一致する証明書とキー ペアがコンテキストにある場合でも、ACE アプライアンス Device Manager では [Matching Key] カラム全体が空白のままになります。この場合、SSL セットアップ シーケンス機能を使用して、証明書とキー ペアの一致を確認できます。

手順

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

[Setup Sequence] ウィンドウが表示されます。

ステップ 2　[Setup Sequence] ウィンドウで、[Configure SSL Polices] をクリックします。

[Configure SSL Policies] ウィンドウが表示されます。

ステップ 3　[Configure SSL Policies] の [Basic Settings] セクションの [Certificate] ドロップダウン リストから、証明書を選択します。

ステップ 4　[Configure SSL Policies] の [Basic Settings] セクションの [Keys] ドロップダウン リストから、キー ペアを選択します。

ステップ 5　[Verify Key] をクリックします。

ACE アプライアンス Device Manager では、選択された証明書とキー ペアが一致するかどうかを確認します。ポップアップ ウィンドウには、2 つの項目が一致するかどうかが示されます。

（注）　ACE には、プレインストールされたサンプル証明書および対応するキー ペアが含まれます。証明書は、デモンストレーションのみを目的としていて、有効なドメインはありません。*cisco-sample-cert* という名前の基本的な拡張子を使用した自己署名証明書です。このキー ペアは、*cisco-sample-key* という名前の RSA 1024 ビット キー ペアです。

次のように、サンプル証明書ファイルおよび対応するキー ペア ファイルを表示します。

- シスコ サンプル証明書ファイルを表示するには、[Config] > [Virtual Contexts] > [context] > [SSL] > [Certificates] の順に選択します。
- シスコ サンプル キー ファイルを表示するには、[Config] > [Virtual Contexts] > [context] > [SSL] > [Keys] の順に選択します。

SSL プロキシ サービス（「SSL プロキシ サービスの設定」（P.9-28）を参照）にこれらのファイルを追加でき、各コンテキストで同じファイル名の任意のコンテキストで使用できます。

ACE では、これらのファイルをエクスポートすることはできますが、これらの名前のファイルをインポートできません。ACE ソフトウェアをアップグレードする場合、これらのファイルはアップグレード イメージで提供されるファイルで上書きされます。ソフトウェアのダウングレードがこれらのファ

イルをユーザ インストールされた SSL ファイルであるかのように保護するため、ACE ソフトウェアをダウングレードしなければ、これらのファイルを削除する **crypto delete** CLI コマンドは使用できません。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のエクスポート」（P.9-16）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キーの使用」（P.9-11）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「CSR の生成」（P.9-27）

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。

（注） 1 つの ACE で最大 4,096 の証明書がサポートされます。

前提

- ACE アプライアンスにサーバ 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.5-1）を参照）。
- CA から SSL 証明書を取得し、ACE アプライアンスがアクセスできるネットワーク サーバ上に置いてある。
- DM のこの機能を使用するには、SSH がアプライアンスでイネーブルになっている必要があります。また、**ssh key rsa 1024 force** コマンドがアプライアンスに適用されている必要があります。

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。

シスコ サンプル証明書の証明書がリストに含まれています。このサンプル証明書の詳細については、「SSL 証明書の使用」（P.9-6）を参照してください。

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。

複数の SSL 証明書をインポートするには、[Bulk Import] をクリックします。[Bulk Import] ダイアログボックスが表示されます。

（注） SSL の一括インポートは、インポートされる SSL 証明書の数により、時間が長くかかることがあります。また、ACE で完了まで進行します。ACE Device Manager にインポートした証明書を表示するには、SSL の一括インポート完了後に、このコンテキストの CLI 同期を実行します。コンテキストの同期の詳細については、「仮想コンテキスト設定の同期」（P.4-82）を参照してください。

ステップ 3　該当する情報を入力します。

- [Import] ダイアログボックスについては、表 9-2 を参照してください。
- [Bulk Import] ダイアログボックスについては、表 9-3 を参照してください。

表 9-2　SSL 証明書管理インポート属性

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 IPv4 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 アプライアンスに 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]、[TFTP]、[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 9-2　SSL 証明書管理インポート属性 （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 アプライアンスまたは 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 アプライアンス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。

表 9-3　SSL 証明書管理一括インポート属性

フィールド	説明
Protocol	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。一括インポートに対してサポートされているプロトコルは SFTP だけです。
IP Address	SSL 証明書ファイルが存在するリモート サーバの IPv4 アドレスを入力します。
Remote Path	リモート サーバに存在する SSL 証明書ファイルのパス。ACE は、パスで指定されたファイルのみフェッチします。再帰的にリモート ディレクトリをフェッチすることはありません。ワイルドカードを含むファイル名のパスを入力します（たとえば、/remote/path/*.pem）。ACE は、IEEE Std 1003.1-2004 の「Shell and Utilities」のセクション 2.13 の指定された POSIX パターン マッチング表記をサポートします。この表記には、「*」、「?」および「[」のメタ文字が含まれます。 リモート ディレクトリからすべてのファイルをフェッチするには、ワイルドカード文字で終わるリモート パス（/remote/path/* など）を指定します。スペースや以下の特殊文字は使用しないでください。 ;<>|`@$&() ACE は、ワイルドカードの基準に一致するリモート サーバのファイルをすべてフェッチします。ただし、名前が最大で 40 文字のファイルだけをインポートします。ファイルの名前が 40 文字を超えていると、ACE はそのファイルをインポートせず、廃棄します。
User Name	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	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	パスワードを再度入力します。
Passphrase	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 ファイルと PKCS ファイルの場合にだけ使用されます。
Confirm	パスフレーズを再度入力します。
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 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オンにすると、この証明書ファイルは ACE からエクスポートできません。

ステップ 4　次の手順を実行します。

- [OK] をクリックして、エントリを確定し、[Certificates] テーブルに戻ります。ACE アプライアンス 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] をクリックすると、エントリを保存しないでこの手順を終了し、[Certificates] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL キーの使用」（P.9-11）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL パラメータ マップの設定」（P.9-20）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL プロキシ サービスの設定」（P.9-28）

SSL キーの使用

ACE アプライアンスとそのピアは、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）と呼ばれる公開キー暗号方式を使用して認証を行います。RSA 方式では、公開キーおよび対応する秘密キーで構成される キー ペアを使用します。ハンドシェイク時に RSA キー ペアによってセッション キーが暗号化され、セッション キー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ます。

SSL および SSL キー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] の順に選択します。[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。

- キー ペアの生成：「SSL キーペアの生成」（P.9-15）を参照
- キー ペアのインポート：「SSL キー ペアのインポート」（P.9-12）を参照
- キー ペアのエクスポート：「SSL キーペアのエクスポート」（P.9-18）を参照
- CSR の生成：「CSR の生成」（P.9-27）を参照

関連トピック

- 「SSL キーペアの生成」（P.9-15）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL キーペアの生成」（P.9-15）
- 「SSL キーペアのエクスポート」（P.9-18）

- 「SSL の設定」（P.9-1）

SSL キー ペアのインポート

SSL キー 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。

（注）　1 つの ACE で最大 4,096 のキー ペアがサポートされます。

前提

- ACE アプライアンスにサーバ 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.5-1）を参照）。
- CA から SSL キー ペアを取得して、ACE アプライアンス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] の順に選択します。[Keys] テーブルが表示され、既存の SSL キーが表示されます。

シスコ サンプル キーのキー ペアがリストに含まれています。このサンプル キー ペアの詳細については、「SSL 証明書の使用」（P.9-6）を参照してください。

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。

複数の SSL キー ペアをインポートするには、[Bulk Import] をクリックします。[Bulk Import] ダイアログボックスが表示されます。

（注）　SSL の一括インポートは、インポートされる SSL キーの数により、時間が長くかかることがあります。また、ACE で完了まで進行します。ACE Device Manager にインポートしたキーを表示するには、SSL の一括インポート完了後に、この *コンテキスト*の CLI 同期を実行します。コンテキストの同期の詳細については、「仮想コンテキスト設定の同期」（P.4-82）を参照してください。

ステップ 3　次のように該当する情報を入力します。

- [Import] ダイアログボックスについては、表 9-4 を参照してください。
- [Bulk Import] ダイアログボックスについては、表 9-5 を参照してください。

表 9-4　SSL キー ペア インポート属性

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 キー 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 キー 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 キー 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] : 証明書とキー 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 キー ペア ファイルが存在するリモート サーバの IPv4 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 サーバ上のキー 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 アプライアンスに SSL キー 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]、[TFTP]、[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 9-4　SSL キー ペア インポート属性 （続き）

フィールド	説明
Non-Exportable	SSL キー ペア ファイルがエクスポート可能になっていると、キー 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 アプライアンスまたは 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、このキー ペア ファイルは ACE アプライアンス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、このキー ペア ファイルは ACE アプライアンス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。 キー 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。

表 9-5　SSL キー ペア 一括インポート属性

フィールド	説明
Protocol	SSL キー ペア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。一括インポートに対してサポートされているプロトコルは SFTP だけです。
IP Address	SSL キー ペア ファイルが存在するリモート サーバの IPv4 アドレスを入力します。
Remote Path	リモート サーバに存在するキー ペア ファイルのパスを入力します。ACE は、パスで指定されたファイルのみフェッチします。再帰的にリモート ディレクトリをフェッチすることはありません。ワイルドカードを含むファイル名のパスを入力します（たとえば、/remote/path/*.pem）。ACE は、IEEE Std 1003.1-2004 の「Shell and Utilities」のセクション 2.13 の指定された POSIX パターン マッチング表記をサポートします。この表記には、「,」、「?」および「[」のメタ文字が含まれます。 リモート ディレクトリからすべてのファイルをフェッチするには、ワイルドカード文字で終わるリモート パス（/remote/path/* など）を指定します。スペースや以下の特殊文字は使用しないでください。 ;<>|`@$&() ACE は、ワイルドカードの基準に一致するリモート サーバのファイルをすべてフェッチします。ただし、名前が最大で 40 文字のファイルだけをインポートします。ファイルの名前が 40 文字を超えていると、ACE はそのファイルをインポートせず、廃棄します。
User Name	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	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	パスワードを再度入力します。
Passphrase	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 ファイルと PKCS ファイルの場合にだけ使用されます。

表 9-5　SSL キー ペア 一括インポート属性 （続き）

フィールド	説明
Confirm	パスフレーズを再度入力します。
Non-Exportable	このチェックボックスをオンにすると、この証明書ファイルは ACE からエクスポートできません。SSL キー ペア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 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。

ステップ 4　次の手順を実行します。

- [OK] をクリックして、エントリを確定し、[Keys] テーブルに戻ります。ACE アプライアンス Device Manager は、インポートしたキー 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] をクリックすると、エントリを保存しないでこの手順を終了し、[Keys] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL パラメータ マップの設定」（P.9-20）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL プロキシ サービスの設定」（P.9-28）

SSL キーペアの生成

照合キー ペアがない場合、ACE アプライアンスを使用してキー ペアを生成できます。

SSL RSA キー 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] の順に選択します。[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、新しいキー 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、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 キー 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、キー 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 キー ペアのサイズは、キー ペア ファイルのビット数で決まります。キーを長くするほど 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
- [4096] : 高度なセキュリティ、レベル 4

ステップ 5　[Type] フィールドに、認証に使用される公開キー暗号方式として [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キー 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、キー ペア ファイルはエクスポートできません。

ステップ 7　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- [Cancel] をクリックすると、エントリを保存しないでこの手順を終了し、[Keys] テーブルに戻ります。
- [Next] をクリックすると、エントリが保存され、別の RSA キー ペアを定義します。

RSA キー 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 アプライアンスが CSR 生成プロセス時に使用する DN 名属性を定義します。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.9-26）を参照してください。
- RSA キー 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 秘密キーは ACE アプライアンス内で直接作成され、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。生成した各キー 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.9-27）を参照してください。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL プロキシ サービスの設定」（P.9-28）

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 アプライアンスまたは 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 アプライアンスからリモート 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.9-8）を参照）。
- DM のこの機能を使用するには、SSH がアプライアンスでイネーブルになっている必要があります。また、**ssh key rsa 1024 force** コマンドがアプライアンスに適用されている必要があります。

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 9-6 の情報を入力します。

表 9-6　SSL 証明書エクスポート属性

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] : 証明書とキー 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 IPv4 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。
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　次の手順を実行します。

- [OK] をクリックすると、証明書をエクスポートして [Certificates] テーブルに戻ります。
- [Cancel] をクリックすると、証明書をエクスポートしないでこの手順を終了し、[Certificates] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL キーペアの生成」（P.9-15）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL プロキシ サービスの設定」（P.9-28）

SSL キーペアのエクスポート

SSL キー ペアがエクスポート可能になっていると、SSL キー 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 アプライアンスまたは Web サーバにインポートできます。キー ペア ファイルのエクスポートは、オリジナルのキー ペアが削除されない点でコピーと同様の操作です。

SSL キー ペアを ACE アプライアンスからリモート 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 キー ペアがエクスポート可能になっている（「SSL キーペアの生成」（P.9-15）を参照）

手順

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

ステップ 2　エクスポートするキー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 9-7 の情報を入力します。

表 9-7　SSL キー エクスポート属性

フィールド	説明
Protocol	SSL キー ペアをエクスポートする方法を指定します。 • [FTP] : SSL キー 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 キー 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 キー 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] : キー ペア情報を端末の画面にカット アンド ペーストして、キー 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 キー ペアをエクスポートする先のリモート サーバの IPv4 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 キー 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　次の手順を実行します。

- [OK] をクリックすると、キー ペアをエクスポートして [Keys] テーブルに戻ります。
- [Cancel] をクリックすると、キー ペアをエクスポートしないでこの手順を終了し、[Keys] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL キーペアの生成」（P.9-15）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL プロキシ サービスの設定」（P.9-28）

SSL パラメータ マップの設定

SSL パラメータ マップでは、ACE アプライアンスが 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] の順に選択します。[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　[Description] フィールドに、パラメータ マップの簡単な説明を入力します。最大 240 文字の英数字（A ～ Z、a ～ z、0 ～ 9）からなるテキスト文字列を入力します。スペースと特殊文字は使用できます。二重引用符は 1 組で入力します。

ステップ 5　[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 6　[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 キー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 7　[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 8　[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 アプライアンス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かか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 アプライアンスは終了通知アラート メッセージを SSL ピアに送信せず、ACE アプライアンスは 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 アプライアンスは以後の 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 9　[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 アプライアンスは、ピア ACE アプライアンスとの通信に SSL v3 と TLS v1 の両方を使用します。
- [SSL3] : ACE アプライアンスは、ピア ACE アプライアンスとの通信に SSL v3 だけを使用します。
- [TLS1] : ACE アプライアンスは、ピア ACE アプライアンスとの通信に TLS v1 だけを使用します。

ステップ 10　[Ignore Authentication Failure] フィールドで、チェックボックスをオンにすると、失効または無効のクライアントまたはサーバ証明書を無視し、SSL 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。このフィールドでは、ACE アプライアンス は、SSL 終了設定のクライアント証明書、または SSL 開始設定のサーバ証明書に関する次の致命的でないエラーを無視することができます。

- Certificate not yet valid（両方）
- Certificate has expired（両方）
- Certificate revoked（両方）
- Unknown issuer（両方）
- No client certificate（クライアント証明書のみ）
- CRL not available（クライアント証明書のみ）
- CRL has expired（クライアント証明書のみ）
- Certificate has signature failure（クライアント証明書のみ）
- Certificate other error（クライアント証明書のみ）

ステップ 11　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。[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 12 に進みます。

- [Cancel] をクリックすると、エントリを保存しないでこの手順を終了し、[Parameter Map] テーブルに戻ります。
- [Next] をクリックすると、エントリが保存され、別のパラメータ マップを定義します。

ステップ 12　[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。

表 9-8 の情報を入力します。

表 9-8　SSL パラメータ マップ暗号設定属性

フィールド	説明
Cipher Name	使用する暗号。 ACE でサポートされる SSL 暗号スイートの詳細については、『*SSL Guide, Cisco ACE Application Control Engine*』を参照してください。
Cipher Priority	ユーザがこの暗号スイートに割り当てるプライオリティ。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 で、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 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 13　[Parameter Map Cipher] テーブルで、次のいずれかを実行します。

- [Deploy Now]：ACE アプライアンス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。

ステップ 14　[Redirect Authentication Failure] タブをクリックし、[Add] をクリックしてリダイレクトを追加するか、既存のリダイレクトを選択して、[Edit] をクリックします。

表 9-9 の情報を入力します。

（注）　Redirect Authentication Failure 機能は、ACE がクライアント認証を実行する SSL 終了の設定用のみです。SSL 開始の設定用に設定した場合、ACE ではこれらの属性は無視されます。

表 9-9　SSL パラメータ マップ リダイレクト設定属性

フィールド	説明
Client Certificate Validation	リダイレクトする証明書検証の失敗の種類を選択します。ドロップダウン リストからリダイレクトのタイプを選択します。 • any：リダイレクトと任意の証明書の失敗を関連付けます。リダイレクトの個別の理由で authentication-failure redirect any コマンドを設定できます。設定すると、ACE は any の理由を使用する前に個別の理由の 1 つへの一致を試みます。authentication-failure redirect any コマンドは authentication-failure ignore コマンドと設定できません。 • Cert-expired：リダイレクトと期限切れの証明書の失敗を関連付けます。 • Cert-has-signature-failure：リダイレクトと証明書の署名の失敗を関連付けます。 • Cert-not-yet-valid：リダイレクトとまだ有効な失敗ではない証明書を関連付けます。 • Cert-other-error：リダイレクトと他のすべての証明書の失敗を関連付けます。 • Cert-revoked：リダイレクトと失効した証明書の失敗を関連付けます。 • CRL-has-expired：リダイレクトと期限切れの CRL の失敗を関連付けます。 • CRL-not-available：リダイレクトと使用できない CRL の失敗を関連付けます。 • No-client-cert：リダイレクトとクライアント認証がない失敗を関連付けます。 • Unknown-issuer：リダイレクトと発行元が不明な証明書の失敗を関連付けます。
Redirect Type	使用するリダイレクトのタイプを次から選択します。 • Server Farm：リダイレクト用にサーバ ファームを指定します。 • URL：リダイレクトのスタティック URL パスを指定します。
Server Farm Name	このフィールドは、Redirect Type が Server Farm に設定されている場合に表示されます。ACE Device Manager が設定済みのすべてのホストおよびリダイレクト サーバ ファームを表示します。使用可能なサーバ ファーム オプションの 1 つを選択するか、[Plus]（+）をクリックしてサーバ ファーム設定のポップアップを開き、リダイレクト サーバ ファームを設定します（「サーバ ファームの設定」（P.6-18）を参照）。
Redirect URL	このフィールドは、Redirect Type が Server URL に設定されている場合に表示されます。リダイレクトのスタティック URL パスを入力します。最大 255 文字の文字列をスペースを入れずに入力します。
Redirect Code	このフィールドは、Redirect Type が Server URL に設定されている場合に表示されます。 クライアントに返信されるリダイレクト コードを入力します。 • 301：完全に新しい場所に移動するリソースのステータス コード。 • 302：一時的に新しい場所に移動するリソースのステータス コード。

ステップ 15　[Redirect Authentication Failure] テーブルで、次のいずれかを実行します。

- ACE に [Redirect Authentication Failure] テーブルを配置し、実行コンフィギュレーションおよびスタートアップ コンフィギュレーション ファイルにエントリを保存するには、[Deploy Now] をクリックします。
- エントリを保存せずに手順を終了し、[Redirect Authentication Failure] テーブルに戻るには [Cancel] をクリックします。
- [Next] をクリックして、エントリを導入し、別のエントリを [Redirect Authentication Failure] テーブルに追加します。

ステップ 16　[Parameter Map] テーブルで、次のいずれかを実行します。

- [Deploy Now] をクリックして、ACE にこの設定を導入し、実行コンフィギュレーション ファイルおよびスタートアップ コンフィギュレーション ファイルにエントリを保存します。
- [Cancel] をクリックすると、エントリを保存しないで手順は終了し、[Parameter Map] テーブルに戻ります。
- [Next] をクリックして、エントリを導入し、[Parameter Map] 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.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL キーペアの生成」（P.9-15）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL プロキシ サービスの設定」（P.9-28）

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 アプライアンス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 アプライアンス証明書、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　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。[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] をクリックすると、エントリ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] をクリックすると、エントリが保存され、[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　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- [Cancel] をクリックすると、エントリ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] をクリックすると、エントリが保存され、このチェーン グループ テーブルに別の証明書を追加します。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL キーペアの生成」（P.9-15）
- 「SSL パラメータ マップの設定」（P.9-20）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL プロキシ サービスの設定」（P.9-28）

SSL CSR パラメータの設定

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。CSR は、所在地、シリアル番号、選択した公開キーなど SSL サイトを特定する情報で構成されます。対応する秘密キーは 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 の秘密キーで）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 アプライアンス が CSR 生成プロセス時に CSR に適用する*認定者名*（DN）属性を定義します。CA はサイトを認証するために必要な情報をこれらの属性から取得します。CSR パラメータ セットを定義すると、同じ DN 属性を持つ複数の CSR を生成できます。

ACE アプライアンス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 属性を定義するには、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 属性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、国際標準化機構（ISO）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　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- [Cancel] をクリックすると、エントリを保存しないでこの手順を終了し、[CSR Parameters] テーブルに戻ります。
- [Next] をクリックすると、エントリが保存されし、別の CSR 属性セットを定義します。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL パラメータ マップの設定」（P.9-20）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL プロキシ サービスの設定」（P.9-28）

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 の秘密キーが含まれています。認証された証明書とキー 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.9-8）および 「SSL キー ペアのインポート」（P.9-12）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.9-26）を参照）
- DM のこの機能を使用するには、SSH がアプライアンスでイネーブルになっている必要があります。また、**ssh key rsa 1024 force** コマンドがアプライアンスに適用されている必要があります。

手順

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

ステップ 2　テーブル内のキーを選択し、[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　次の手順を実行します。

- [OK] をクリックすると、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] をクリックすると、CSR を生成しないでこの手順を終了し、[Keys] テーブルに戻ります。

関連トピック

- 「SSL の設定」（P.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL パラメータ マップの設定」（P.9-20）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL プロキシ サービスの設定」（P.9-28）

SSL プロキシ サービスの設定

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

ACE アプライアンスが 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属性を定義するには、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 キー 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 64 文字です。

ステップ 4　[Key] フィールドで、ACE アプライアンスが SSL ハンドシェイク時にデータの暗号化に使用するキー ペアを選択します。

注意　キー ペアをドロップダウン リストから選択した場合は、選択した証明書に対応するキーを選択してください。

（注）　プロキシ サービスの作成に SSL セットアップ シーケンスを使用する場合、ACE Appliance Device Manager は、選択した証明書に対応するキーを選択します。ACE Appliance Device Manager が対応するキー ペアを検出できない場合は、ドロップダウン リストからキー ペアを選択し、ACE Appliance Device Manager にキーが選択した証明書に対応していることを確認するには、[Verify Key] をクリックします。ACE Appliance Device Manager は、キー ペアの選択が選択した証明書に一致するかどうかを通知するメッセージを表示します。SSL セットアップ シーケンスの詳細については、「SSL セットアップ シーケンス」（P.9-5）を参照してください。

シスコ サンプル キー オプションは、サンプル キー ペアで利用可能です。このサンプル キー ペアの詳細については、「SSL 証明書の使用」（P.9-6）を参照してください。

ステップ 5　[Certificate] フィールドで、ACE アプライアンスが SSL ハンドシェイク時に自身の身元の証明に使用するキー ペアを選択します。

注意　証明書をドロップダウン リストから選択した場合は、選択したキーに対応する証明書を選択してください。

（注）　プロキシ サービスの作成に SSL セットアップ シーケンスを使用する場合、ACE Appliance Device Manager は、選択した証明書に対応するキーを選択します。ACE Appliance Device Manager が対応するキー ペアを検出できない場合は、ドロップダウン リストからキー ペアを選択し、ACE Appliance Device Manager にキーが選択した証明書に対応していることを確認するには、[Verify Key] をクリックします。ACE Appliance Device Manager は、キー ペアの選択が選択した証明書に一致するかどうかを通知するメッセージを表示します。SSL セットアップ シーケンスの詳細については、「SSL セットアップ シーケンス」（P.9-5）を参照してください。

シスコ サンプル証明書オプションは、サンプル証明書で利用可能です。このサンプル証明書の詳細については、「SSL 証明書の使用」（P.9-6）を参照してください。

ステップ 6　[Chain Groups] フィールドで、ACE アプライアンスが 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、次のいずれかを実行します。

- 証明書がこのプロキシ サービスには適用されない場合に [N/A] を選択します。次に、ステップ 11に進みます。
- 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.9-32）を参照してください。

ステップ 8　CRL がエクステンションに含まれているかどうかを判別するサービスを求めて、ACE アプライアンスがクライアント証明書を調べることができるようにする場合に、[CRL Best-Effort] チェックボックスをオンにします。CRL がある場合、ACE アプライアンス は値を取得します。

CRL 名を選択するために CRL の名前フィールドを表示するには、チェックボックスをオフにします。

ステップ 9　[CRL Name] フィールドで、次のいずれかを実行します。

- CRL の名前が適用されない場合に [N/A] を選択します。
- ACE で認証に使用する CRL 名を選択します。

ステップ 10　ACE アプライアンス で、失効ステータスから、証明書に関する情報が得られる場所で証明書自体の OCSP サーバ情報を見つけるために拡張を取得できるように OCSP [Best-Effort] チェックボックスをオンにします。この拡張が証明書から欠落し、ベスト エフォート OCSP サーバ情報が SSL プロキシで設定されている場合、証明書が失効したと見なされます。

使用可能な OCSP サーバを選択するために OCSP サーバ フィールドを表示するには、チェックボックスをオフにします。

ステップ 11　[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 12　Revcheck の優先順位について、失効チェックのプライオリティを設定するには、次のいずれかを選択します。

- [N/A] : このフィールドは使用できません。
- [CRL-OCSP] : ACE は失効ステータスの判別に最初に CRL を使用し、次に OCSP サーバを使用します。
- [OCSP-CRL] : ACE は失効ステータスの判別に最初に OCSP サーバを使用し、次に CRL を使用します。

ステップ 13　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- [Cancel] をクリックすると、エントリを保存しないでこの手順を終了し、[Proxy Service] テーブルに戻ります。
- [Next] をクリックすると、エントリが保存され、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.9-1）
- 「SSL 証明書のインポート」（P.9-8）
- 「SSL キー ペアのインポート」（P.9-12）
- 「SSL パラメータ マップの設定」（P.9-20）
- 「SSL チェーン グループ パラメータの設定」（P.9-25）
- 「SSL CSR パラメータの設定」（P.9-26）
- 「SSL OCSP サービスの設定」（P.9-30）

SSL OCSP サービスの設定

SSL Online Certificate Status Protocol (OCSP) サービスは OCSP を使用して証明書の失効チェック用のホスト サーバを定義します。OCSP サーバ（別名 OCSP レスポンダ）では、取り消されたおよび取り消されない可能性がある異なる CA によって作成された証明書についての情報を維持または取得し、OCSP クライアントから要求された場合に、この情報を提供します。OCSP は、証明書の失効ステータスに関する最新情報を提供できます。OCSP の使用により、サイズが非常に大きく、システムに大きなメモリが必要となる CRL のダウンロードとキャッシュが不要になります。

ACE のシステム全体で、最大 64 の OCSP サーバ設定を設定できます。シングルまたはマルチ コンテキストで、これらのサーバすべてを設定できます。

ACE アプライアンスが 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属性を定義するには、次の手順を使用します。

前提

関連するプロキシ サービスの OCSP を設定します。

認証には OCSP と CRL の両方の設定が可能です。

手順

ステップ 1　[Config] > [Virtual Contexts] > [*context*] > [SSL] > [OCSP Service] の順に選択します。[OCSP 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 OCSP 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。[OCSP 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 OCSP 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 64 文字です。この名前は、SSL プロキシ サービスにこの設定を適用する場合に使用します。

ステップ 4　[URL] フィールドで、HTTP ベースの URL を http://*ocsp_hostname*.com:*port_id* の形式で OCSP ホスト名と任意のポート ID に入力します。ポート ID を指定しない場合、ACE はデフォルト値の 2560 を使用します。

ステップ 5　オプションで、[Request Signer's Certificate] フィールドで、サーバへの要求に署名する署名者証明書のファイル名を選択できます。デフォルトでは、要求は署名されていません。

ステップ 6　オプションで、[Response Signer's Certificate] フィールドで、サーバ応答で署名を確認する署名者証明書のファイル名を選択できます。デフォルトでは、応答は確認されません。

ステップ 7　サーバへの要求でナンスの包含を有効にするには、[Enable Nonce] チェックボックスをオンにします。デフォルトでは、ナンスはディセーブル（オフ）に設定されています。

サーバへの要求でナンスの含有をディセーブルにするには、チェックボックスをオフにします。

ステップ 8　[TCP Connection Inactivity Timeout] フィールドに、TCP 接続非アクティブ タイムアウトを指定する 2 ～ 3600（秒）の整数を入力します。デフォルトは 300 秒です。

ステップ 9　次の手順を実行します。

- [Deploy Now] をクリックして、ACE アプライアンスにこの設定を導入します。
- [Cancel] をクリックすると、エントリを保存しないでこの手順を終了し、[OCSP Service] テーブルに戻ります。
- [Next] をクリックすると、エントリが保存され、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.9-1）
- 「SSL プロキシ サービスの設定」（P.9-28）

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.9-28）
- 「SSL 証明書グループの設定」（P.9-32）
- 「クライアント認証での CRL の設定」（P.9-33）

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.9-31）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.9-28）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 アプライアンス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　次の手順を実行します。

- [Deploy Now] をクリックして、ACE にこの設定を導入します。[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] をクリックすると、エントリ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] をクリックして、エントリを導入し、[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　次の手順を実行します。

- [Deploy Now] をクリックして、ACE にこの設定を導入します。
- [Cancel] をクリックすると、エントリ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] をクリックして、エントリを導入し、[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.9-33）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.9-25）
- 「クライアント認証での CRL の設定」（P.9-33）

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、『*SSL Guide, Cisco ACE Application Control Engine*』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 8 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 9-10 の情報を入力します。

表 9-10　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　次の手順を実行します。

- [Deploy Now] をクリックして、ACE にこの設定を導入します。[Certificate Revocation List] テーブルが更新されて表示されます。
- [Cancel] をクリックすると、エントリを保存しないで手順は終了し、[CRL] テーブルに戻ります。
- [Next] をクリックして、エントリを導入し、[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.9-28）
- 「SSL 証明書グループの設定」（P.9-32）