CHAPTER 19

SSL/TLS によるトラフィックの保護

この章では、サービス トラフィックを保護するために SSL/TLS を使用する方法について説明します。内容は次のとおりです。

SSL/TLS トラフィックの暗号化について

Secure Sockets Layer（SSL）、および、SSL の後継の標準である Transport Layer Security（TLS）は、ネットワーク トラフィックの保護に広く使用されている方式です。ACE XML Gateway では、ACE XML Gateway とサービス ユーザとの間の通信や、ACE XML Gateway とバックエンド サービス プロバイダーとの間の通信を保護するために、SSL を使用できます。

ユーザとの接続で SSL を使用するには、使用される SSL セッションを確立するために、公開鍵と秘密鍵のペアをアップロードし、指定する必要があります。キーペアのロードに関する詳細は、「キーペア リソースのアップロード」（P.28-292）を参照してください。

SSL は、サービス トラフィックの保護以外の目的にもシステムで使用されることに、注意してください。たとえば、ACE XML Manager は、SSL を介した Web コンソールの役割を果たします。また、ログ情報と管理情報が、SSL によって、ACE XML Gateway と Manager との間で渡されます。したがって、Web コンソールには、SSL 認証を設定するためのいくつかのエリアがあります。この章では、特にサービス トラフィックに対して SSL を使用するために ACE XML Gateway を方法について説明します。

サービス ユーザ接続の保護

ユーザ接続に SSL を使用するには、ACE XML Gateway では、公開鍵と秘密鍵のキーペアが必要です。キーペアは、自己署名証明書または認証局によって署名された証明書のいずれかの場合があります。ユーザが組織の内部に存在する場合は、通常、自己署名証明書で十分です。その他の目的の場合は、CA によって署名された証明書を使用する必要があります。

特定のタイプのクライアントとの互換性のために、（ここで説明されているように）ACE XML Gateway のポートで使用される証明書を、サーバ証明書として設定できます。つまり、証明書は、`TLS Web Server 認証の X509v3 Extended Key Usage` アトリビュートを持つ必要があります。ただし、これは、特定のクライアントで潜在的な要件です。ACE XML Gateway システムでは、サーバ証明書の使用は必須ではなく、非サーバ証明書が多くのインスタンスで動作可能な場合があります。

ACE XML Gateway とユーザとの間で暗号化チャネルを設定するには、次の操作を実行します。

ステップ 1　操作メニューで [HTTP Ports & Hostnames] リンクをクリックします。

ステップ 2　SSL 接続を設定するポートがすでに存在する場合、そのポートの [edit] リンクをクリックします。ポートが存在しない場合は、第 15 章「ポートおよびホスト名に関する作業」に説明されているようにポートをオープンします。

SSL には、通常、ポート番号 443 が使用されます。ただし、セキュリティ保護されていない HTTP 接続のデフォルト ポート番号であるポート 80 を含む、任意のポート番号を指定できます。

ステップ 3　[Edit Port] ページで [SSL] チェックボックスをクリックします。このオプションが選択されている場合、そのポートの通信に SSL の暗号化が使用されます。

ステップ 4　[Public/Private Keypairs] メニューで、接続に使用するキーペアを選択します。

使用するキーペアが ACE XML Manager にまだアップロードされていない場合、「キーペア リソースのアップロード」（P.28-292）の説明に従ってキーペアをアップロードします。

ステップ 5　SSL 接続の設定中、ACE XML Gateway とクライアントでは、メッセージの暗号化または認証に使用される SSL Cipher Suite を含む、接続のさまざまパラメータがネゴシエートされます。デフォルトでは、ポートで受け付ける暗号スイートは ACE XML Gateway では選択できません。64 ビット キーまたは 56 ビット キーの使用を含む、ほとんどの暗号化アルゴリズムが受け付けられます。

特に、使用されるデフォルトの Cipher Suite リストは、
ALL:!ADH:!EXPORT:!SSLv2:!LOW:+HIGH:+MEDIUM です。

[SSL Cipher Suite] メニューから [custom] を選択することによって、ポート上で ACE XML Gateway によって受け付けられる暗号スイートを制限できます。http://www.openssl.org/docs/apps/ciphers.html で説明されているように、表示されるテキスト フィールドに、標準の OpenSSL Cipher 文字列形式で許可される暗号スイートのセットを入力します。

たとえば、長さが 128 ビット以上かまたは匿名 DH を持つキーが使用されるアルゴリズムだけを許可するには、次のように使用します。

HIGH:MEDIUM:!ADH

これは、次の指定と同等です。

DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-SHA
:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA:
DES-CBC3-SHA:DES-CBC3-MD5:DHE-RSA-AES128-SHA:
DHE-DSS-AES128-SHA:AES128-SHA:DHE-DSS-RC4-SHA:
KRB5-RC4-MD5:KRB5-RC4-SHA:RC4-SHA:RC4-MD5:
RC2-CBC-MD5:RC4-MD5:KRB5-DES-CBC3-MD5: KRB5-DES-CBC3-SHA

クライアントで、指定されたどの SSL Cipher Suites も使用できない場合、接続は許可されません。イベント ログには、"Terminating HTTP session: 400 Bad request" のような警告レベル イベントが表示されます。

（注）　暗号スイート文字列を入力する際には、注意してください。ACE XML Manager インターフェイスでは、入力した値は確認されません。入力を間違えた場合や無意味な値を入力した場合、ポートは使用できなくなります。

ステップ 6　[Save Changes] をクリックし、ポートの設定を終了します。

これで、ポートを使用する仮想 Web アプリケーションまたは仮想サービス オブジェクトを設定できます。たとえば、仮想 Web アプリケーションで、次の手順を実行します。

ステップ 1　操作メニューで [Virtual Web Applications] をクリックします。

ステップ 2　トラフィックを保護する基本仮想サービス オブジェクトまたはサービスのハンドラを選択します。

ステップ 3　仮想サービスのプロパティ ページの **Consumer Interface** という見出しの横の [Edit] リンクをクリックします。

ステップ 4　[Port] の値について、SSL を設定したばかりのポートをリストから選択します。

ステップ 5　[Save Changes] をクリックし、変更内容をアクティブなサブポリシーにコミットします。

これで、クライアント側の SSL 設定は完了です。ポリシーを導入して、Gateway への変更内容を反映させます。

サービス プロバイダー接続の保護

ACE XML Gateway とバックエンド サービス プロバイダーとの間の接続の SSL 暗号を設定できます。

バックエンド サーバ接続のセキュリティを保護するには、リモート サーバ証明書、または、リモート ユーザによって使用される信頼済み CA の証明書の、いずれかのサーバ証明書を検証するために適切なセキュリティ リソースを持つ必要があります。CA への信頼を指定するには、ポリシーでその証明書をインポートする必要があります。ポリシーには、デフォルトで、事前にロードされた CA 証明書は含まれていません。

ACE XML Gateway では、双方向 SSL もサポートされ、ここで、ACE XML Gateway によって、それ自体が、バックエンド システムに対して認証されることに、注意してください。双方向 SSL を使用するには、ACE XML Gateway の公開鍵と秘密鍵のキーペアを ACE XML Manager にロードする必要があります。

双方向 SSL を設定するには、次の操作を実行します。

ステップ 1　操作メニューで [Destination HTTP Servers] リンクをクリックします。

ステップ 2　SSL を設定するポートがすでに存在する場合、そのサーバの [view] リンクをクリックします。

サーバがサーバ リストに表示されない場合、[Add a New Server] ボタンをクリックし、「宛先 HTTP サーバの追加」（P.14-152）で説明されているように、バックエンド サーバを作成します。

ステップ 3　[Edit Server] ページで、一般設定の見出しの横にある [Edit] リンクをクリックします。

ステップ 4　SSL チャネルを介してサーバと通信するには、[SSL] オプションをイネーブルにします。

SSL チャネル設定の制御がイネーブルにされます。

ステップ 5　双方向 SSL では、サーバにより、クライアント（この場合は ACE XML Gateway）に対して、SSL ネゴシエーションの一部として、サーバ自体が認証されます。この場合、[If requested, use client public/private keypair] メニューから、使用するクライアントの公開鍵と秘密鍵のキーペアを指定できます。

ステップ 6　ACE XML Gateway によって、サーバで提示される証明書の確認方法を指定します。

- Web サービスから提示された証明書を受け付けるには、[Require remote server certificate signed by this CA certificate] オプションを、そのデフォルト値の [none] のままにします。この設定は、デフォルトです。ACE XML Gateway により、サーバで提示される証明書が受け付けられます。

- 指定された認証局（CA）が署名された証明書を受け付けるには、[Require remote server certificate signed by this CA certificate] オプションが選択された状態で、メニューに表示されているリストで 1 つまたは複数の CA を選択します。証明書がメニューに表示されない場合、[Upload] を選択し、Trusted Certificate Authority（Trusted CA）の ACE XML Manager のリストに証明書を追加します。
- 特定の証明書と同等の証明書を受け付けるには、[Require a certificate from the remote server that is identical to this certificate] をクリックし、メニューから証明書を選択します。証明書がメニューに表示されない場合、[Upload] を選択し、リモート サーバ証明書の ACE XML Manager のリストに証明書を追加します。

ステップ 7　SSL 接続の設定中、ACE XML Gateway とバックエンド サーバでは、メッセージの暗号化または認証に使用される SSL Cipher Suite を含む、接続のさまざまパラメータがネゴシエートされます。デフォルトでは、受け付ける暗号スイートは ACE XML Gateway では選択できません。64 ビット キーまたは 56 ビット キーの使用を含む、ほとんどの暗号化アルゴリズムが受け付けられます。

[SSL Cipher Suite] メニューから [custom] を選択することによって、バックエンドサーバとの通信を確立するときに ACE XML Gateway によって受け付けられる暗号スイートを制限できます。http://www.openssl.org/docs/apps/ciphers.html で説明されているように、表示されるテキスト フィールドに、標準の OpenSSL Cipher 文字列形式でサーバ接続に使用される暗号スイートを入力します。

たとえば、長さが 128 ビット以上か匿名 DH を持つキーだけが使用されるアルゴリズムだけを許可するには、次のようにテキスト フィールドに入力します。

HIGH:MEDIUM:!ADH

これは、次の指定と同等です。

DHE-RSA-AES256-SHA:DHE-DSS-AES256-SHA:AES256-SHA:EDH-RSA-DES-CBC3-SHA:EDH-DSS-DES-CBC3-SHA: DES-CBC3-SHA:DES-CBC3-MD5:DHE-RSA-AES128-SHA:
DHE-DSS-AES128-SHA:AES128-SHA:DHE-DSS-RC4-SHA:
KRB5-RC4-MD5:KRB5-RC4-SHA:RC4-SHA:RC4-MD5:
RC2-CBC-MD5:RC4-MD5:KRB5-DES-CBC3-MD5: KRB5-DES-CBC3-SHA

サーバで、設定した SSL Cipher Suites の 1 つを使用できない場合、接続のネゴシエーションに失敗し、イベント ログに障害が記録されます。

（注）　フィールドに暗号スイートを入力する際には、注意してください。ACE XML Manager Web コンソールでは、入力値は検証されません。入力を間違えた場合や無意味な値を入力した場合、Gateway はサーバには接続できません。

ステップ 8　[Save Changes] をクリックし、サーバの設定を終了します。

これで、SSL 設定は完了です。ポリシーの導入後、設定されたサーバに依存している仮想サービスでは、SSL を使用してバックエンド サーバと通信します。