CHAPTER 7

バックエンド システムへの認証要求

この章では、発信要求のクレデンシャルの設定方法について説明します。内容は次のとおりです。

概要

ACE XML Gateway は、ネットワークベースのコントロール エンフォースメント ポイントとして動作することによって、一貫性ポリシーがダイバース システムおよびアプリケーションに確実に適用されるよう支援します。バックエンド システムも Gateway によって大量の処理を伴うクレデンシャル確認の作業の実施から開放されます。

それにもかかわらず、バックエンド システムが、受信要求のユーザ クレデンシャルに頼ることがあります。それらのシナリオの場合、ACE XML Gateway は、発信メッセージに含めるためのクレデンシャルを生成できます。

ACE XML Gateway は、新しいクレデンシャルの生成、または、クレデンシャル メディエーションを実行できます。クレデンシャル メディエーションでは、外部へ配信するために受信クレデンシャルが別の種類（例：HyperText Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル）Basic 認証から Web Services Security（WSS UsernameToken または Security Assertion Markup Language（SAML）情報）に変換されます。

ACE XML Gateway は、受信クレデンシャルの値に加えて、ポリシーに設定された値、または、認証のために LDAP ディレクトリを検索して得られたデータを使用してクレデンシャルを生成できます。

Gateway は次の種類のクレデンシャルを生成できます。

- Basic 認証 HTTP ヘッダー
- NT LAN Manager（NTLM）ヘッダー
- WSS UsernameToken
- SAML トークン

Service Authentication 設定の横の [Edit] をクリックして、バックエンド認証を設定します。この設定は、仮想サービスの設定ページにある [Backend Service] という見出しの下に表示されます。

HTTP ヘッダーベースのクレデンシャルの生成

一般的なクラスのクレデンシャルの場合、メッセージの HTTP ヘッダー部分でクレデンシャルが送信されます。発信要求に付加できる HTTP ヘッダー認証クレデンシャルには次の 2 種類があります。

- Basic 認証 HTTP ヘッダー
- NTLM 認証ヘッダー

HTTP Basic 認証は、メッセージ ヘッダー内でパスワードをハッシュ化して送信する、一般的に使用されるクレデンシャルの形式です。[HTTP Authentication] メニューの Send Basic Auth ヘッダー オプションのうちの 1 つを選択すると、ACE XML Gateway は発信要求にそのヘッダーを追加します。

ACE XML Gateway は、NTLM ヘッダーの生成もサポートします。NTLM は Microsoft 社が開発した、認証およびセッション セキュリティ プロトコルであり、特に Integrated Windows Authentication（IWA; Windows 統合認証）テクノロジー セットで使用されます。

NTLM クレデンシャルは、ユーザ名とパスワード、および任意でサブジェクトのターゲット ドメインを示す HTTP ヘッダーです。ACE XML Gateway によって NTLM クレデンシャルを発信要求に追加するには、[HTTP Authentication] メニューで「Send NTLM auth header」オプションを選択します。任意で、NTLM オプションが選択されているときに表示される Domain フィールドに値を入力すると、ドメインを追加できます。

WSS UsernameToken クレデンシャルの生成

WSS ユーザ名（Web Services Security UsernameToken Profile）は、Organization for the Advancement of Structured Information Standards（OASIS）Web Services Security 技術委員会が定義したクレデンシャルの種類です。ACE XML Gateway は、WSS UsernameToken を発信 Simple Object Access Protocol（SOAP）要求に追加できます。

ACE XML Gateway が要求に追加するユーザ名とパスワードには、受信クレデンシャル内の値またはポリシーで指定された値を指定できます。例 7-1 に、着信 SOAP 要求のために ACE XML Gateway が生成した UsernameToken の例を示します。

例 7-1　WSS UsernameToken

```
<soap:Envelope>
  <soap:Header>
    <wsse:Security>
      <wsse:UsernameToken>
        <wsse:Username>alice</wsse:Username>
        <wsse:Password
          Type="http://docs.oasis-open.org/wss/2004/01/oasis
          -200401-wss-username-token-profile-1.0#PasswordText">
          mypassword</wsse:Password>
        <wsse:Nonce>4MK0BeHCtAXiwrQF48K0BQ==</wsse:Nonce>
        <wsu:Created>2006-04-25T18:17:30Z</wsu:Created>
      </wsse:UsernameToken>
    </wsse:Security>
  </soap:Header>
  <soap:Body>
    <retrieveQuote>
      ...
    </retrieveQuote>
  </soap:Body>
</soap:Envelope>
```

デフォルトで、パスワードはクリアテキストです。設定で指定した鍵を使用してパスワード値を暗号化するように ACE XML Gateway を設定できます。

WSS UsernameToken を発信要求に追加するには、次の作業を行います。

ステップ 1　[Virtual Services] ブラウザで、クレデンシャル生成を設定する基本仮想サービス オブジェクトまたはサービス識別子をクリックします。

ステップ 2　[Service Authentication] という見出しの横の [Edit] リンクをクリックします。基仮想サービス オブジェクトで、まず、エキスパンダ コントロールをクリックして、[Backend Service] 設定を表示します。

ステップ 3　[WSS Username Token] メニューから [Send this WSS Username Token in the WSS header] を選択します。

ステップ 4　任意で、[SOAP Role] メニューから項目を選択し、目的の SOAP ヘッダーのプロセッサであるメッセージ受信者を特定します。Gateway は、このロールを持つ発信メッセージの SOAP ヘッダーに WSS UsernameToken を追加します。発信メッセージに該当するヘッダーが存在しない場合は、ヘッダーが作成されます。

ロールは、特に宛先までの経路においてメッセージが複数の SOAP ノードによって送信される場合に、目的の SOAP ヘッダーのプロセッサを特定します。システムのヘッダー プロセッサを特定するためにロールを使用しない場合は、デフォルト値である no role を使用します。

ヘッダーに SOAP ロールを選択するには、次のオプションから選択します。

- [custom] : ユーザ定義の管理者が指定した名前付きロールを指定する場合。
- [next] : WSS ヘッダーが、メッセージを処理する次の SOAP ロールを対象とする場合。
- [ultimateReceiver] : WSS ヘッダーが、メッセージの最終受信者を対象とする場合。

ステップ 5　[Generate] メニューから項目を選択し、サービス記述子がトークンのユーザ名とパスワードを生成する方法を指定します。次のオプションを使用できます。

- [Using the username and password from the credential] は、ACE XML Gateway に、ACE XML Gateway への要求認証に使用されるクレデンシャルから得たユーザ名とパスワード値を生成されたトークンの組み込むように指示します。
- [Using the following username and password menu item] は、WSS UsernameToken で使用される固定のユーザ名およびパスワードを指定します。

ステップ 6　オプションで、[Encrypt Username Token] チェックボックスをクリックし、次の暗号化設定を設定することによって、ACE XML Gateway がトークンを暗号化するように設定します。

- [Transport key] は、ユーザ名トークンを暗号化するために使用される公開鍵です。

  鍵リソースが ACE XML Manager にロードされていない場合は、[Upload] ボタンをクリックして、使用する鍵を含む証明書ファイルから鍵リソースを作成ます。
- [Encryption Algorithm] は、トークンの暗号化に使用される暗号化方式です。標準アルゴリズム：3DES、AES256、AES-192、AES-128 から選択します。
- [Transport Cipher] は、転送されたパケットの暗号化に使用される暗号です。Ricest, Shamir, and Adleman-Public Key Cryptography Standards#1（RSA-PKCS#1）または RSA-OAEP から選択します。

ステップ 7　[Save Changes] をクリックして、変更内容を作業ポリシーにコミットします。

ポリシーが導入されると、設定された仮想サービスから送信されるメッセージに WSS UsernameToken が追加されます。

新しい WSS UsernameToken の生成に加えて、ACE XML Gateway は、受信メッセージで受信したトークンをパススルーすることができます。このオプションを設定するには、[Pass through WSS Username Token(s) from the inbound message] を選択します。この場合、Gateway はインバウンド メッセージで受信した WSS UsernameToken をアウトバウンド メッセージに追加します。

別の ACE XML Gateway に限って処理されることを目的とするトークン（AXG -only）を作成することもできます。AXG-only トークンは、ある ACE XML Gateway から別の ACE XML Gateway にメッセージが渡され、非信頼ネットワーク（たとえば、異なるブランチ オフィスの ACE XML Gateway 間など）を経由する可能性があるシナリオを対象としています。AXG-only ロールは、別の ACE XML Gateway による処理だけを対象とするヘッダーを特定します。発信元の ACE XML Gateway は、トークン パススルー 設定で、[Pass through as AXG-only UsernameToken] オプションがイネーブルである場合、この種類の発信トークンを組み立てます。[Decrypt AXG-only WSS Username Token(s) and pass through] オプションを使用してトークンを処理するように宛先 ACE XML Gateway を設定できます。受信 AXG-only トークンを復号した後、受信 Gateway は、このトークンに対して設定された別の設定が指定するとおりに、トークンを発信要求に反映します。

（注）　ACE XML Gateway は、カスタム ロール アトリビュート値を使用して、WSS UsernameToken が別の ACE XML Gateway による処理にだけを対象としていることを示します。[Decrypt AXG-only WSS Username Token(s) and pass through] オプションの使用による場合を除き、SOAP ヘッダー設定などのポリシーの他の設定を使用して、このロールを持つヘッダーの取得と処理を試みてはなりません。

SAML 情報の生成

発信要求に SAML 情報を追加することによって、ACE XML Gateway は、SAML クレデンシャルに依存するシステムのアサート パーティとして機能できます。ACE XML Gateway によって生成された SAML 情報は、SAML 1.0、SAML 1.1、または、SAML 2.0 クレデンシャルの形式になります。

SAML クレデンシャルは、情報内の Subject NameIdentifier エレメントによって示される特定の個人またはアプリケーションの ID をアサートします。生成されたクレデンシャルには、着信要求のクレデンシャルから Subject NameIdentifier の値が取り込まれます。使用できる値の種類には、ユーザ名 / パスワード クレデンシャルのユーザ名、クライアント SSL 証明書のサブジェクト名、または、固定の値があります。さらに、発信元クレデンシャルが WSS ユーザ名である場合、WSS ユーザ名エレメントのアトリビュートから生成した、SAML 情報へのアトリビュートを追加します。

ACE XML Gateway は、発信要求へ単一の SAML 情報、または、複数の受信クレデンシャルから生成した複数の情報を追加できます（複数の情報の場合、ACE XML Gateway は、WSS UsernameToken および受信要求で確認されたクライアント SSL クレデンシャルごとに情報を生成できます）。

ACE XML Gateway によって、複数の SAML 情報を生成するには、ここで記載した設定手順に加えて、要求を受信したオーセンティケータによる複数の情報検証をイネーブルにする必要があります。複数情報の検証をイネーブル化は、あるオーセンティケータ内の単なる複数のクレデンシャル要求の指定とは異なることに注意してください。複数のクレデンシャル要求のイネーブル化によって、ACE XML Gateway は、同一の種類の複数のクレデンシャルを検査し、検証されたクレデンシャルは発信情報の生成に使用され続けます。

SAML 情報を発信要求に追加するには、次の作業を実行します。

ステップ 1　[Virtual Services] ブラウザで、クレデンシャルの生成を設定する仮想サービスまたはサービス記述子をクリックします。

ステップ 2　サービス設定ページで、[Service Authentication] というタイトルの横にある [Edit] リンクをクリックします。基本仮想サービスで、まず、エキスパンダ コントロールをクリックして、[Backend Service] 設定を表示します。

ステップ 3　次のように、単一のトークンまたは複数の発信 SAML トークンを生成できます。

- ACE XML Gateway に単一の SAML トークンを生成させるには、Service Authentication ページの [SAML Token] メニューから、[Send one SAML token with an Authentication Statement as specified] を選択します。
- WSS UsernameToken、クライアント SSL 証明書、またはエクステンションによって設定されたデータに基づいて複数の SAML トークンを生成するには、[Send multiple SAML tokens with an Authentication Statement as specified] を選択します。

SAML トークン設定が表示されます。

ステップ 4　複数の SAML トークンの生成の場合、[Credential Sources] セクションでトークンのデータ ソースを選択します。たとえば、ソースとして WSS UsernameToken を選択した場合、SAML トークンは、受信要求の WSS UsernameToken 見出しそれぞれに対して生成され、受信トークンのユーザ名が発信 SAML トークンの Subject NameIdentifier として使用されます。

このモードでは、[Inbound SAML Assertions] メニューから、ヘッダーを廃棄するか、パススルーするかのオプションを選択することで、インバウンド SAML トークンの処理も指定できます。

ステップ 5　クレデンシャルが、ロールによって指定される特定の受信者による処理を対象とする場合、[SOAP Role] メニューからトークンのロールを選択します。ACE XML Gateway は、このロールが含まれた受信メッセージの WSS ヘッダーにトークンを追加するか、または、ヘッダーがまだ存在しない場合は、このロールを持つヘッダーを追加します。

ロールは、`Security` タグのオプションのアトリビュートであり、トークンを消費する、メッセージの複数の受信者候補者の中の 1 人を特定するために使用する必要があります。次のオプションから選択します。

- [no role]（デフォルト値）：トークンが特定のロールを意図していないことを示す場合。
- [custom]：ユーザ定義の管理者が指定した名前付きロールを指定する場合。
- [next]：WSS ヘッダーが、メッセージを受信しトークンを消費できる次の処理を対象とすることを示す場合。
- [ultimateReceiver]：WSS ヘッダーが、メッセージの最終受信者を対象とすることを示す場合。

ステップ 6　生成される SAML 情報のバージョン（1.0、1.1、または 2.0）を選択します。選択したバージョンは、ページで使用可能なオプションの内容に影響を与えることに注意してください。

ステップ 7　**Subject NameIdentifier** は、トークンが識別情報を提供する主体を特定します。生成するトークンが複数か単一かによって、生成されるトークンの **Subject NameIdentifier** を複数の方法で設定できます。

- 複数のトークンを生成する場合、使用される DN に認証の目的でクライアントの LDAP 検索を実行させ、生成されたトークンの subject nameIdentifier 値として使用させるときは、任意で [Set Subject Name Identifier to User DN, if available] オプションを選択します。
- 単一のトークンを生成する場合、[Subject NameIdentifer] メニューの次のオプションから選択します。
  - [SAML Token Subject NameIdentifier] は、受信要求の SAML 情報のサブジェクトを、発信要求情報のサブアジェクトに使用します。
  - [HTTPS Certificate Subject DN] は、要求の認証に使用される証明書のサブジェクトの DN を使用します。
  - [HTTP Basic Auth Username] は、要求の認証に使用される HTTP Basic 認証クレデンシャルからユーザ名を取得します。
  - [XPath Username] は、受信要求の認証に使用される XPath パスワード クレデンシャルからユーザ名を取得します
  - [WSS UsernameToken] は、要求の認証に使用される WSS ユーザ名 / パスワードのユーザ名を使用します。

- [fixed value] を使用すると、NameIdentifier エレメントに特定の固定値を使用できます。この項目を選択した場合、使用する識別情報を入力するテキスト フィールドが表示されます。

ステップ 8　任意で、タイムスタンプに基づいて情報の有効性を制限するために、SAML トークンにタイムベースの条件を追加します。

次の制限を設定します。

- [NotBefore] によって、`NotBefore` アトリビュートが設定された時間とともに情報に追加されます。これは、情報が有効と見なされる最も早い時間を示します。
- [NotOnOrAfter] によって、メッセージに `NotOnOrAfter` アトリビュートが追加され、情報の有効期限を示します。

  いずれの場合でも ACE XML Gateway は、情報が生成された時間を基準にアトリビュートの値を計算します。例：

  ```
  <Conditions NotBefore="2006-03-24T21:54:08Z" NotOnOrAfter="2006-03-25T05:54:13Z">
  ```

ステップ 9　任意で、[Audience] チェックボックスをチェックし、情報の意図する対象読者（またはリレー パーティ）の Uniform Resource Identifier（URI; ユニフォーム リソース識別子）を入力することで、1 つ以上の Audience 条件を SAML トークンに追加します。

ステップ 10　[Confirmation Method] メニューで次のオプションを選択し、情報の確認方法の値を指定します。

- [Sender Vouches] は、ACE XML Gateway によって SAML 情報が保証されること、および、情報のサブジェクトまたは情報自身の認証方法をメッセージが提供するとは限らないことをリレー パーティに通知します。これは、サービスが信頼する情報に関して、ACE XML Gateway とバックエンド サービスとの間に信頼関係が存在することを意味します。
- [Holder-of-key] は、元の受信要求を受け入れたオーセンティケータの SSL/TLS 証明書を使用して ACE XML Gateway が確認できる Extensible Markup Language（XML）署名によって、サブジェクトがカバーされることを指定します。

  [Holder-of-Key] 確認方法を選択する場合は、confirmation key も選択する必要があります。

  [Sender Vouches] 確認方法の場合は、confirmation key の選択はオプションです。

ステップ 11　[Confirmation Key] メニューで鍵リソースを選択し、サブジェクト確認の `KeyInfo` エレメントに表示される鍵を指定します。

ステップ 12　任意で、[Sign the SAML token with the Confirmation Key] オプションをイネーブルにして、confirmation key を使用してトークンが署名されるようにします。署名は受信者が発信元およびトークンの完全性の確認に使用します。署名については、さらに次のオプションから選択できます。

a. [Include X.509 certificate with signature] を選択すると、トークンの署名に使用される証明書が含められます。

b. Microsoft .NET WSE 2.0 を使用して開発されたエンドポイントによってメッセージが消費される場合は、[Add unqualified "Id" attributes to Assertion elements for .NET WSE 2.0 compatibility] チェックボックスをクリックします。

これは ACE XML Gateway に、Microsoft .NET WSE 2.0 が要求する `Id` アトリビュートを署名されたエレメントに追加するよう指示します。

ステップ 13　SAML トークンの生成に [Send multiple SAML tokens with an Authentication Statement as specified] オプションを選択した場合、追加の設定オプション、[Include LDAP records, if available, as SAML Attribute] が表示されます。このオプションをイネーブルにすると、元の要求の認証を目的とした LDAP ディレクトリ検索の結果として得られた LDAP レコードの値が、生成されたトークンの SAML アトリビュート文として含められます。この値には、dn、cn、フィルタ処理されたアトリビュートが含まれます。したがって、オーセンティケータの確認設定のすべてのアトリビュートに * を使用すると、認証サーバによって検索された LDAP レコードのすべてのアトリビュートが SAML アトリビュートに組み込まれます。たとえば、アトリビュート「member」だけにフィルタを制限すると、「member=groupName」および dn と cn が含められます。

ステップ 14 上の手順に記載したとおりに SAML アトリビュート文を LDAP レコードから生成することを選択した場合、または、WSS UsernameToken を SAML アトリビュート文にマッピングすることを選択した場合、URI テキスト フィールドに名前空間を入力して、Gateway がこれらのアトリビュートを許可するために使用するデフォルトの名前空間を指定します。このフィールドは、SAML 1.0 および 1.1 の場合は [Attribute Namespace URI] と表示され、SAML 2.0 の場合は [Attribute Format URI] と表示されます。生成されたトークンのアトリビュートが許可された名前空間にない場合、この URI で許可されます。

[System Management] > [Gateway Settings] ページには、Gateway に、認証された WSS UsernameToken のカスタム アトリビュートを、生成する SAML トークンの SAML アトリビュート文のアトリビュートとして含めるよう指示するオプションがあります。

ここで入力した名前空間 URI は、LDPAP レコード検索および WSS UsernameToken アトリビュートの両方に由来する非許可アトリビュートに追加されます。

ステップ 15 [Save Changes] をクリックした後、ポリシーを導入して ACE XML Gateway への変更を有効にします。