CHAPTER 11

Simple Object Access Protocol（SOAP）メッセージの処理

この章では、SOAP 機能と WS-Security 機能の概要を説明します。内容は次のとおりです。

SOAP 機能と WS-Security 機能の概要

ACE XML Gateway は、SOAP プロトコルおよび Web Service（WS）標準の幅広くサポートします。SOAP は、一般的に使用できるトランスポートで（最も一般的には HyperText Transfer Protocol（HTTP; ハイパーテキスト転送プロトコル））Extensible Markup Language（XML）メッセージを送信することによって、リモート プロシージャを起動するためのメッセージ トランスファ プロトコルです。

SOAP は、World Wide Web Consortium（W3C）勧告、W3C Note 08 May 2000（http://www.w3.org/TR/SOAP/）および W3C Recommendation 24 June 2003（http://www.w3.org/TR/soap12-part0/）で定義されます。

ACE XML Gateway および Manager には、安全で信頼できるサービス指向のシステムを実現する作業を非常に簡単にするツールと機能があります。この章では、SOAP テクノロジーおよび WS-Security テクノロジーのサポートの概要、および、これらを使用して安全なネットワーク サービスを導入する方法を説明します。

SOAP のバージョンおよび機能のサポート

ACE XML Gateway は SOAP バージョン 1.1 および 1.2 をサポートします。SOAP および Web Service（WS）仕様のサポートについて次の点に注意してください。

- WS-Security 1.0、および、Organization for the Advancement of Structured Information Standards（OASIS）document Web Services Security に記述される相互運用シナリオ、Security Assertion Markup Language（SAML）Interop 1 Scenarios の 4 つすべてがサポートされます。

- ACE XML Gateway は、SOAP バージョニングをサポートし、メッセージのバージョンが不正なときには、VersionMismatch エラーを報告します。しかし ACE XML Gateway は、Upgrade メッセージをサポートしません。
- どのヘッダーを誰が処理するかをメッセージが指定できるようにするロールの使用による SOAP ヘッダー エンドポイントのターゲティングの使用、および、特定のヘッダーが後続の受信者にパスされるべきかどうかをメッセージが指定できるようにするロールの使用による SOAP ヘッダー エンドポイントのリレーの使用をサポートします。
- ACE XML Gateway は、SOAP 1.2 スタイルの Content-Type 宣言（`application/soap+xml`）、および、任意の `action` パラメータをサポートします。SOAP 1.2 スタイルの Fault エレメントをサポートします。
- ACE XML Gateway は WS-Security UsernameToken エレメントの検証と生成をサポートしますが、ナンス キャッシング、Hash Message Authentication Codes（HMAC）鍵、XRML をサポートしません。また、SOAP メッセージの SAML プロファイル、および、X.509 証明書をサポートしますが、PKIPath はサポートしません。

SOAP メッセージ形式

SOAP メッセージにはエンベロープ（必須）、SOAP ヘッダー（任意）、および SOAP 本文（必須）が含まれます。SOAP エンベロープは、SOAP Envelope 名前空間での名前が「Envelope」である XML エレメントです。Envelope エレメントは、SOAP ヘッダー（SOAP Envelope 名前空間での名前が「Header」である）を任意で含み、SOAP 本文（SOAP Envelope 名前空間での名前が「Body」である）を含まれなければなりません。

SOAP メッセージは、2 つのスタイルに準拠します。

- SOAP RPC スタイルは、より厳しく、SOAP ルーチンへのパラメータが、メッセージの本文内で指定された形式で順次エンコードされることを要求します。
- SOAP Document スタイルは、より柔軟であり、有効な XML ドキュメントをメッセージの本文として許可します。個々の SOAP Document メッセージの構造と有効性は、XML スキーマによって検証されると推定します。

多くの場合、SOAP サービスのユーザは、SOAP メッセージ形式の詳細を知る必要はありません。クライアントまたはサービスが、どのスタイルとエンコードを予期しているか、および、どのヘッダーが予期されているかを知るだけで十分です。

SOAP および WS-Security

SOAP そのものは、SOAP メッセージの安全性や信頼性を保証しません。これらの問題を解決するに、Organization for the Advancement of Structured Information Standards（OASIS）は Web Services Security（WS-Security）標準および Web Services Utility（WS-Utility）標準を開発しました。これらの標準は、安全性と信頼性の向上のための SOAP の拡張機能を指定します。

ネットワークの防御のために最も頻繁に使用される SOAP 機能は、次のとおりです。

1. **デジタル署名**：SOAP メッセージは、XML エレメントをデジタル署名とともに転送でき、ACE XML Gateway は、署名されたエレメントの検証に署名を使用できます。
2. **コンテンツ レベル暗号化**：SOAP メッセージは、コンテンツの全部または一部を暗号化されたエレメントとして転送します。
3. **WS-Security ユーザ名トークンおよびパスワード トークン**：WS-Security 標準は、SOAP メッセージが自身の認証に使用するユーザ名情報およびパスワード情報を安全に転送する方法を提供します。

4. **SOAP タイムスタンプ**：SOAP メッセージに、メッセージの作成時間、有効時間、および、特定の中間ノードから受信した時間を示すタイムスタンプを付けることができます。

Web Service 機能は、通常、SOAP ヘッダーとしてメッセージで伝達されます。ACE XML Gateway はヘッダーを検証してメッセージから削除する、または、バックエンド システムの要望に応じて転送するなどの SOAP ヘッダーの処理を行います。しかし場合によっては、特定の SOAP ヘッダーを受け入れ、変更することなく宛先にパススルーする必要があることもあります。

この章では、SOAP 機能および Web Service 機能の設定方法と使用方法について説明します。

SOAP ヘッダー処理を有効にする

SOAP ヘッダーは、特別な処理の指示やメッセージに適用可能なその他の種類の情報を含む、SOAP メッセージのエレメントです。SOAP ヘッダー エレメントは、WS-Security および WS-Utility などの仕様によって定義され、タイムスタンプ、XML 署名、または、Web Services Security（WSS）UsernameToken クレデンシャルなどを含みます。

（注） 正式に定義されたヘッダータイプに加えて、SOAP メッセージは、カスタム SOAP ヘッダーを搬送できます。ACE XML Manager インターフェイスは、それぞれ「known headers」および「user-specified headers」の用語によって、正式に規定されたヘッダーおよびカスタム ヘッダーを識別します。

ACE XML Gateway が受信メッセージの SOAP ヘッダーを処理するようにするには、仮想サービス設定で、SOAP Header processing オプションを有効にする必要があります。Web Services Description Language（WSDL）を使用して SOAP ヘッダー要件に含まれるサービス定義を生成しない限り、このオプションはデフォルトで無効です。また、SOAP ヘッダーは処理されずにパススルーされます。

WSDL は、オペレーション バインディング定義の input エレメントまたは output エレメントの `soap:header` エレメントを使用して、ヘッダー要件を指定できます。この要件のある WSDL をインポートした場合、デフォルトでこのサービスに対する SOAP ヘッダーの処理は有効にされます。また、SOAP ヘッダー処理設定の [Advanced Options] ページに示されるように、WSDL で要求されたヘッダーそれぞれに、ユーザ指定ヘッダーが設定されます。WSDL がヘッダーを指定しない場合、直接、ヘッダー処理を有効にして、ACE XML Gateway が SOAP ヘッダーを検証し、処理するようにしなければなりません。

ヘッダー処理を有効にすると、ACE XML Gateway は、受信メッセージの SOAP ヘッダーを消費するように指示されます。処理を有効にすることで、特定のヘッダーの存在が要求されることはありませんが、存在する場合、ヘッダーは有効性が確認され、発信メッセージから削除されます（WS-Addressing ヘッダーでない限り。WS WS-Addressing であれば、デフォルトでパススルーされます）。

（注） 受け入れられるメッセージに SOAP ヘッダーが存在しなければならないことを指定するには、Advanced SOAP Processing 設定を使用します。

SOAP ヘッダー処理を有効にするには、次の手順を実行します。

ステップ 1　Web コンソールで `Administrator` ユーザ、または、`Routing` ロールを持つ `Privileged` ユーザでログインしているときに、操作メニューで [Virtual Services] リンクをクリックします。

ステップ 2　ヘッダーを処理する SOAP メッセージを扱う仮想サービス オブジェクトの名前をクリックします。

ステップ 3　[Incoming Request] セクションで、[SOAP Header Processing] ペインの [Edit] リンクをクリックします。

ステップ 4　[Process header elements for SOAP] チェックボックスをクリックします。

ステップ 5　[Role] メニューで、処理を行うヘッダーのロール アトリビュート値を選択します。

SOAP ロールを選択すると、ヘッダーがそのロールを示すときだけ、ACE XML Gateway は SOAP ヘッダーを検査します。SOAP ロール アトリビュートは、特定のヘッダーの意図するプロセッサを指定します。受信者、または、SOAP メッセージをリレーする中間ノードがそのメッセージに割り当てられた SOAP ロールを与えられている場合で、SOAP メッセージにそのロールに割り当てられたヘッダーを見つけた場合は、そのヘッダーを処理します。各ヘッダーに割り当てられた SOAP ロールを別々に設定できます。「no role」が選択されている場合、ハンドラはロール アトリビュートのないヘッダーだけを処理します。

ステップ 6　このページの別のコントロールを使用して、ヘッダーの処理方法を指定します。Web Services Utility（WSU）Timestamp 設定には、[Timestamp Expires] および [Timestamp Created and Timestamp Expires values differ by more than] があります。これらのオプションを有効にすると、指示された要件に合致しないタイムスタンプ プロパティのあるメッセージは拒否されます。また、必要に応じて、XML 復号化および署名検証を設定します。

ステップ 7　完了したら [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。

SOAP ヘッダー拡張設定

SOAP ヘッダー処理をオンにする場合、メッセージの SOAP ヘッダーが有効である必要があります。SOAP ヘッダー拡張設定の場合は、さらに、必ずヘッダーが存在することが求められます。特に、ACE XML Gateway が WS-Security ヘッダー、WS-Addressing ヘッダー、およびその他の指定したヘッダーや未知のヘッダーを処理する方法の設定が必要です。

WSDL のインポートによって作成されたサービス定義の場合、カスタム ヘッダーの設定は、WSDL の内容に基づいて自動で設定されます。WSDL にカスタム SOAP ヘッダー要件が含まれる場合は、ポリシーのヘッダー要件セクションにある対応する設定が代入され、ヘッダー 要件が反映されます（さらに、SOAP ヘッダー処理はデフォルトで有効に設定されます）。

仮想サービスの SOAP ヘッダー拡張オプションを開くには、[SOAP Header Processing] ペインの [advanced options] リンク（SOAP ヘッダー処理設定がすでに変更されている場合）、または、[SOAP Header Processing] ページの下部にある [Advanced SOAP Header Processing] リンクをクリックします。

ページは、Extra Headers（拡張ヘッダー）、Known Headers（既知のヘッダー）、および、User-Specified Headers（ユーザ指定ヘッダー）のエリアから構成されます。

Extra Headers

拡張ヘッダーは、ポリシー設定内の名前で指定されていない（known ヘッダーまたは user-defined ヘッダー）メッセージのヘッダーです。拡張ヘッダーでは、ヘッダーが受け入れられるかどうか、および、ACE XML Gateway が `mustUnderstand` アトリビュートをどのように評価するかを指定できます。SOAP ヘッダーで `MustUnderstand` アトリビュートが true に設定されている場合、SOAP 中間ノードおよび宛先ノードは、このヘッダーを処理する必要があります。ヘッダーの 1 つに `MustUnderstand` が設定されているメッセージを受信した SOAP ノードは、ヘッダーが既知でない場合は、メッセージを拒否し、SOAP Fault 応答を返す必要があります。ACE XML Gateway を `MustUnderstand` アトリビュートを強制するかまたは無視するかのいずれかに設定できます。

受信ハンドラが特定の SOAP ロールに割り当てられている場合、ロールの対象のヘッダーだけに `MustUnderstand` を強制します。`MustUnderstand` アトリビュートを含むかどうかにかかわらず、他のロールの対象となるヘッダーは無視されます。

Known Headers

既知の SOAP ヘッダーに対して、ヘッダーが任意であるか、必須であるか、禁止であるかを設定できます。デフォルトで、ヘッダーは任意であり、処理されます。処理されるとは、ACE XML Gateway がヘッダーを消費することを意味します。たとえば、署名のあるセキュリティ ヘッダーの適正さが検証されます。処理をオフにすることや、発信メッセージにヘッダーを渡すなどの、必要に応じた代わりのヘッダー出力処理を設定することができます。

User-Specified Headers

カスタム ヘッダーを記述することで、該当するヘッダーの要件を設定できます。カスタム ヘッダーの仕様には、ヘッダーの名前空間、ローカル名、およびロールの設定があります。

名前によるヘッダーの定義に加えて、ヘッダーが必須であるかどうか、および、発信メッセージで送信するかどうかを設定できます。拡張ヘッダーを使用することで、ACE XML Gateway がヘッダーの「must understand」アトリビュートをどのように扱うかも設定できます。

SOAP ヘッダー仕様を含む WSDL を使用して WSDL のインポートから生成したサービス定義の場合、WSDL にあったカスタム SOAP ヘッダーはすべて、自動的にユーザ指定ヘッダーとして指定されます。

XML Stylesheet Language Transformations（XSLT）をヘッダーに適用する

XSLT は、ACE XML Gateway がヘッダーを処理する前または後にヘッダーに適用できます。SOAP ヘッダーに適用する XSLT を作成するときは、次の点に注意してください。

- XSLT は、ヘッダー エレメントだけではなく、SOAP メッセージ全体に対して適用されます。したがって、XSLT の XPath は、root Envelope document root エレメント、つまり、`/soap:Envelope` を基準にドキュメント内でパスを参照する必要があります。

  これによって、たとえばヘッダーに出力されるなど、メッセージの本文の内容にアクセスできます。

- XSLT の出力は、`<soap:Header>` エレメントの直接の子としてメッセージに入れられます。したがって、結果が `<wsse:Security>` ヘッダーの子であることを意図する場合は、XSLT は `<wsse:Security>` ヘッダーをルート エレメントとして出力する必要があります。これによって、必要に応じてヘッダーの名前、名前空間、アトリビュートなどを変更できます。

- XSLT の結果は、有効な XML である必要があります。ヘッダーは任意の数の子エレメントを持てますが、次のようにルート ノードを 1 つだけ持つ必要があります。

  ```
  <sampleHeader>
    <element1>...</element1>
    <elementN>...</elementN>
  </sampleHeader>
  ```

  結果に複数のピア ルート ノードが含まれる（次の例のような）場合は、最初のピア ルート ノードだけが使用されます。

  ```
  <element1>...</element1>
  <elementN>...</elementN>
  ```

SOAP 名前空間の設定

ACE XML Gateway が SOAP メッセージの発信 WS-Security エレメントおよび WS-Utility エレメントに使用する名前空間を設定できます。名前空間の設定は、System Management ページの Gateway Settings ページに表示されます。設定フィールドは、そのページの SOAP XML Namespace Configuration 設定エリアにあります。発信メッセージに必要な名前空間をフィールドに入力します。この変更の後に、ACE XML Gateway は SOAP メッセージの WS-Security エレメントおよび WS-Utility エレメントに名前空間を適用します。

Gateway がこれらの値を適用する方法は、受信要求がすでに名前空間を使用しているかどうかによって異なることに注意してください。

- 受信要求が名前空間を使用するが、管理者が設定した名前空間ではない場合は、ACE XML Gateway は、管理者が入力した名前空間を発信要求に適用します。しかし、対応する応答を受け取った場合は、応答をユーザに送信する前に、オリジナルの要求によって指定された名前空間を使用します。この方法で、ユーザはオリジナルの要求と同じ名前空間を使用するメッセージを受け取りますが、一方で、保護されたサービスは設定された名前空間を参照します。
- 受信要求が名前空間を指定しない場合、ACE XML Gateway は、保護されたサービスへの発信要求と、ユーザに送信される発信要求の両方に、管理者が指定した名前空間を使用します。

これらのルールは、WS-Security エレメントおよび WS-Utility エレメントに別々に適用されます。たとえば、受信応答が WS-Security 名前空間を指定し、WS-Utility 名前空間を指定しない場合、ユーザは要求から WS-Security 名前空間を参照しますが、ACE XML Manager 設定から WS-Utility 名前空間を参照します。

大きいメッセージの処理

Flex Path サービスの場合、ACE XML Gateway は、非常にサイズの大きいメッセージの処理を可能にする特別の処理技術を使用します。ACE XML Gateway は、最大 400MB までのサイズの SOAP 添付ファイルおよび HTTP Post XML メッセージを処理できます（標準ハードウェア設定の場合）。

デフォルトで、Flex Path は 10MB を超えるメッセージを大きいメッセージとして扱います。大きいメッセージの処理には、ストリーム型処理手法およびハードディスク利用率を含む特別の処理技術があります。

（注）　Reactor 処理は、大きいメッセージを特別の取り扱いなしに処理できます。Reactor 内のメッセージのサイズは、単一プロセスに使用できる機器の メモリの量（大部分のハードウェア設定では、2GB 以下）だけから制限されます。しかし、Reactor メッセージ処理に適応可能なデフォルトの脅威防御設定があり、デフォルトでメッセージ サイズを 10MB に制限します。I/O プロセス拡張設定ページでこの値を変更できます。

大きいメッセージのトラフィックに適応できるオペレーションの種類には、スキーマ検証、適格性のチェック、および、コンテンツ スクリーニングがあります。ACE XML Gateway は、大きいメッセージ添付ファイルの XML 署名も確認できます（署名が、メッセージの SOAP 部分にあり、大きい添付ファイル内にはない場合）。ACE XML Gateway Software Development Kit（SDK）を使用すると、プログラムが大きいメッセージ添付ファイルの内容へアクセスできるため、カスタム検証やカスタム処理を添付ファイルの内容に適用できます。

（注）　メモリ内でのメッセージの処理を必要とするオペレーション（XML 暗号化や復号化、XPath の解決を必要とする機能など）は、大きいメッセージには適用できません。

大きいメッセージは、しばしば、SOAP 添付ファイルの形式を取ります。しかし、ACE XML Gateway での大きいメッセージのサポートは、HTTP Post XML メッセージなどの他のフォーマットにも適用されます。HTTP Post または HTTP Get への応答で受信された大きい XML メッセージもサポートされます。

SOAP エンベロープのサイズは 10 MB に制限されているため、大きい SOAP ペイロードは、SOAP エンベロープ内ではなく、添付ファイルとして転送されなければなりません。添付ファイルの合計サイズは、最大 400 MB に制限されています。ACE XML Gateway が SOAP メッセージを検証する方法から、この制限は SOAP メッセージに適用され、XML ペイロードや SOAP 添付のある他の種類のメッセージには適用されません。

大きいメッセージのサポート有効にするための特別な手順はありません。大きいメッセージはデフォルトでサポートされます。しかし、大きいメッセージの処理を決定するパラメータは、要件に従って変更できます。特に、大きいメッセージの処理を示すメッセージ サイズは、ACE XML Gateway が参照するトラフィックの種類と必要に応じて変更できます（最も強く関係する要因は、大きいメッセージのトラフィックの同時発生の可能性）。

ACE XML Gateway の大きいメッセージの処理の調整については、Cisco のサポート担当者に問い合せてください。

（注）　クライアントへ送信される大きい応答の自動圧縮を設定できます。これは、要求内にある GZIP 圧縮データを受け入れることを意味します。ゲートウェイが応答を圧縮する、応答サイズしきい値は設定可能です。詳細については、15-170 ページの「応答の圧縮」セクションを参照してください。

SOAP 添付ファイルの処理

SOAP メッセージは、MIME または DIME エンコード データ形式のメッセージ添付ファイルを含むことがあります。添付ファイルは、一般に、画像や PDF ファイルなどのネイティブ ASCII ではないデータの転送に使用されます。

ACE XML Gateway は、SOAP 添付ファイルを認識し、検証することができます。その他のタスクの中で、次のタスクを実行できます。

- 受信メッセージの添付ファイルを要求する、または、禁止する。
- 添付ファイルを制限する最小サイズと最大サイズを強制する。
- 添付ファイルを圧縮する、または、復元する。
- DIME 形式から MIME 形式にまたは逆に、添付ファイルを変換する。
- 添付ファイルに SDK 拡張を通じてカスタム処理を行う。

ACE XML Gateway は、Message Transmission Optimization Mechanism（MTOM）メッセージ エンコードを使用するメッセージを処理します。MTOM、および、それに関係する仕様、XML-binary Optimized Packaging（XOP）は、大きい Base64 エンコード部分を含む SOAP Document メッセージを最適化する方法です。

（注）　SOAP 添付データに関する情報については、W3C Note「SOAP Messages with Attachments」（http://www.w3.org/TR/SOAP-attachments）を参照してください。

受信 SOAP 添付ファイルの処理

SOAP Attachments/MTOM Handling エディタを使用して、受信添付ファイルの処理方法を指定できます。このエディタでは、添付ファイルが必要であるかどうか、添付ファイルサイズの制約、内容を検証するかどうかなどを指定できます。

受信 SOAP 添付ファイルの処理を設定するには、次の作業を実行します。

ステップ 1　Web コンソールに `Administrator` ユーザ、または、`Routing` ロールまたは `Access Control` ロールを持つ `Privileged` ユーザとしてログインしているときに、アクティブ サブポリシーを編集するハンドラまたはサービス記述子を提供するサブポリシーに設定します。

ステップ 2　操作メニューで [Virtual Services] リンクをクリックします。

ステップ 3　編集する仮想サービス オブジェクトの名前をクリックします。

ステップ 4　指定したハンドラまたはサービス記述子の情報ページの [Incoming SOAP Attachments] バナーで [Edit] リンクをクリックします。

基本仮想サービスの場合、[Request Processing] または [Response Processing] の下の [SOAP Attachment Validation] の横にある [edit] リンクをクリックします。

ステップ 5　[Edit SOAP Attachments] ページで、SOAP 添付ファイルを受け入れるかどうかを指定します。

- SOAP 添付ファイルを搬送するメッセージを拒否する（デフォルト）には、[Edit SOAP Attachments] ページの上部に表示されるメニューで [Reject SOAP messages with attachments] アイテムを選択します。
- SOAP 添付ファイルを受け入れるには、[Edit SOAP Attachments] ページの上部に表示されるメニューで、[Accept...] アイテムを選択します。

メニューには選択されたアイテムが表示されます。SOAP 添付ファイルの受け入れを選択した場合、エディタは、グローバル添付ファイル処理の設定およびタイプ固有の添付ファイル仕様の設定に使用できる追加のコントロールを表示します。

ステップ 6　受信添付ファイルにコンテンツ スクリーニング ルールを適用するには、[Apply content screening rules to attachments] チェックボックスをクリックします。

このオプションを使用すると、ACE XML Gateway は、[Content Screening Defaults] ページで有効にされたコンテンツ スクリーニング ルールを受信 SOAP 添付ファイルに適用します。

ステップ 7　受信添付ファイルを復元するには、[Decompress any compressed attachments] チェックボックスをクリックします。

有効にされると、ACE XML Gateway は、圧縮された受信 SOAP 添付ファイルを復元します。ACE XML Gateway は添付ファイルを ZIP または GZIP 形式に圧縮または復元できます。

ステップ 8　ハンドラが受け入れるそれぞれの種類の SOAP 添付ファイルに対して、次のように添付ファイル仕様を作成します。

a. [Add Another Attachment Specification] ボタンをクリックします。

[Attachments with Content-Type] ペインが表示されます。

b. [Attachments with Content-Type] メニューから添付ファイルの種類を選択します。

メニューに表示されない添付ファイルの種類を指定するには、[custom attachment] タイプを選択し、メニューの横のフィールドに添付ファイルの種類の名前を入力します。カスタム タイプを指定する場合、リストにある他の種類に似た形式を使用します。

任意の種類の添付ファイルを受け入れるには、[any unspecified MIME type attachment] タイプを選択します。

c. [Require at least] フィールドに、受信メッセージが持つことができる SOAP 添付ファイルの数の最小値と最大値を入力します。

無制限の添付ファイルを指定するには、両方の値に（デフォルトの）0（ゼロ）を入力します。

d. [Limit attachment size] フィールドに、個々の SOAP 添付ファイルのサイズに認められる最小値と最大値をキロバイト（KB）で入力します。

ページの下部にある [Add Another Attachment Specification] ボタンを使用して、必要な数の添付ファイル仕様を追加できます。添付ファイル仕様を削除するには、[Remove] ボタンをクリックします。

[Add Another Attachment Specification] ボタンは利用できません。次の手順に進みます。

ステップ 9　[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。

発信 SOAP 添付ファイルの圧縮

ACE XML Gateway は、発信メッセージの添付ファイルを圧縮できます。発信 SOAP 添付ファイルを圧縮するには、次の手順を実行します。

ステップ 1　Web コンソールに `Administrator` ユーザ、または、`Routing` ロールまたは `Access Control` ロールを持つ `Privileged` ユーザとしてログインしているときに、アクティブでない場合は、アクティブなサブポリシーを、仮想サービスを含むサブポリシーに設定します。

詳細については、「サブポリシーの使用」（P.30-306）を参照してください。

ステップ 2　操作メニューで [Virtual Services] リンクをクリックします。

ステップ 3　編集する仮想サービス オブジェクトの名前をクリックします。

ACE XML Manager Web コンソールに、サービスの設定ページが表示されます。

ステップ 4　指定されたハンドラまたはサービス記述子の情報ページの [Outgoing SOAP Attachments] 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 オブジェクトの場合、[Request Processing] または [Response Processing] の下にある [SOAP Attachments Compression] の横の [Edit] リンクをクリックします。

ステップ 5　ACE XML Gateway がメッセージの送信の前に SOAP 添付ファイルを圧縮するようにするには、[Edit SOAP Attachments] ページの [Compress...] チェックボックスをクリックします。

ステップ 6　[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。

MTOM メッセージの処理

標準 SOAP ドキュメント メッセージでは、バイナリ メッセージ コンテンツは、Base64 エンコード形式のメッセージのエンベロープ内にあります。MTOM（Message Transmission Optimization Mechanism）を使用すると、バイナリデータはデータ表現に必要なバイト数を削減できる raw バイトに処理され、メッセージ添付ファイルとして、エンベロープの外に出されます。

最適化された MTOM メッセージを受信したとき、ACE XML Gateway は、データを再構成し、Base64 データとして再度エンコードし、メッセージのエンベロープ内に戻します。XML 暗号化や復号化、XML 署名検証などの通常の SOAP 検証および処理手法をデータに適用します。MTOM エンコード要求を送信したクライアントへの応答は、MTOM エンコードされます。

MTOM コンテンツをこの方法で処理する代わりに、Gateway は単に次のように実行します。

- MTOM データのあるメッセージをブロックします。
- MTOM 最適化データをパススルーします。

（注）　別の種類の例外にはマッピングできませんが、バックエンド サービスからの MTOM 関連の例外はクライアントにパススルーされます。

デフォルトで、添付ファイルおよび MTOM エンコードされたメッセージはブロックされます。MTOM エンコード メッセージを許可する、または、処理する代わりに、次の手順を実行します。

ステップ 1　[Virtual Services] ページで、MTOM の処理を設定する仮想サービスの設定ページを開きます。

ステップ 2　[SOAP Attachments/MTOM Handling] 見出しの横にある [enable] リンク（または、すでに設定がデフォルトから変更されている場合は [edit]）をクリックします。

ステップ 3　[SOAP Attachments/MTOM Handling] ページで、次のオプションから選択します。

- [Accept and Decode MTOM messages] : Gateway が MTOM 最適化メッセージのコンテンツを Base64 形式に再構成するようにします。この設定の変更が適用されて導入されると、仮想サービスの他の処理および検証の設定はデコードされた MTOM コンテンツに適用可能です。
- [Accept both MIME- and DIME-encoded SOAP messages with attachments] : Gateway は、最適化された MTOM を受け入れますが、デコードしません。添付ファイル仕様を追加し、次のうちのいずれかを選択することで、MTOM 添付ファイルのあるメッセージだけが受け入れられるように、メッセージがスクリーニングされます。
  - [any unspecified MIME type] は、MTOM および他の任意の添付ファイルの種類を指定します。
  - [application/xop+xml] は、MTOM エンコードされた添付ファイルだけを受け入れます。

（注）　添付ファイルのある MTOM メッセージを完全な状態のままパススルーするには、SOAP 添付ファイル出力は、仮想サービスに対して有効でなければなりません。

ステップ 4　**[Save Changes]** をクリックします。

設定を導入すると、ACE XML Gateway は、MTOM メッセージを設定どおりに処理します。特に、[Accept and Decode MTOM messages] が選択されている場合、ACE XML Gateway は、この仮想サービスへの受信メッセージの SOAP エンベロープの `<xop:Include>` エレメント（最適化 MTOM コンテンツが存在することを示す）をチェックします。見つかった各エレメントに対して、ACE XML Gateway は添付ファイルのリストから、その Content-ID が XOP include エレメントの「href」アトリビュート値（「cid」識別名の後ろ）に合致する添付ファイルを探します。

次に、エレメントの例を示します。

<xop:Include href="cid:mygif"/>

Would match an attachment that had the header:

Content-ID: <mygif>

一致するものが見つかった場合、添付ファイルのコンテンツは Base-64 エンコード化されており、SOAP エンベロープの <xop:Include> エレメントの置き換えに使用され、それに応じて添付ファイルが削除されます。

ダイナミック サービス ルーティング WS-Addressing

このセクションでは、WS-Addressing と ACE XML Gateway の使用方法について説明します。内容は次のとおりです。

WS-Addressing の概要

WS-Addressing は、SOAP メッセージ内へのアドレッシング情報組み込みのための W3C 仕様です。WS-Addressing は、SOAP ヘッダーとしてアドレッシング情報を組み込むための形式を定義します。

WS-Addressing の目的は、SOAP と特定のネットワーク プロトコルの間の依存関係をなくすことです。このような依存関係の例は、SOAPAction ヘッダーです。SOAPAction は HTTP ヘッダーであり、SOAP 1.1 では SOAP メッセージに SOAPAction があることが要求されます（最新仕様では任意です）。

WS-Addressing を使用すると、SOAPAction およびその他のアドレッシング情報は、SOAP エンベロープ内で搬送されます。したがって、アドレッシング情報は完全にメッセージ コンテンツの中に入れられ、HTTP ヘッダーには依存しません。その結果、メッセージは特定の転送プロトコルには依存せず、宛先へのルートにおいて複数の転送メカニズムを横断できます（たとえば、E メール メッセージを HTTP 要求または応答としてなど）。

次のリストに、WS-Addressing ヘッダーの例を示します。

例 11-1　WS-Addressing ヘッダーの例

```
<?xml version="1.0" encoding="UTF-8"?>
<soap:Envelope
  ...
  xmlns:wsa="http://www.w3.org/2005/08/addressing"
>
 <soap:Header>
   <wsa:MessageID>urn:uuid:...</wsa:MessageID>
   <wsa:ReplyTo>
      <wsa:Address>
         http://beagle.example.com/customer/oak
      </wsa:Address>
   </wsa:ReplyTo>
   <wsa:To>https://oakinsurance.com/service/order.asmx</wsa:To>
   <wsa:Action>http://oakinsurance.com/retrieveQuote</wsa:Action>
   </soap:Header>
 <soap:Body>
  ...
 </soap:Body>
</soap:Envelope>
```

この例は、WS-Addressing 名前空間の宣言で始まっています。ACE XML Gateway は WS-Addressing ヘッダーに対して次の名前空間をサポートします。

- http://www.w3.org/2005/08/addressing
- http://schemas.xmlsoap.org/ws/2004/08/addressing

ACE XML Gateway WS-Addressing 機能は、特に、To および Action ヘッダー エレメントに依存しています。

- To は、メッセージのエンドポイントを特定します。
- Action は、要求の宛先であるアクターの Uniform Resource Identifier（URI; ユニフォーム リソース識別子）が含まれます。これは、SOAPAction HTTP ヘッダーと等価です。

受信要求が WS-Addressing ヘッダーを含む場合、Gateway は、ヘッダーに To エレメントおよび Action エレメントが含まれることを要求します。ReplyTo や FaultTo などの別のヘッダーが存在した場合は、それらに対しても検証を行います。

他の種類の SOAP ヘッダーとは異なり、WS-Addressing ヘッダーは、デフォルトで発信メッセージへパススルーされます。

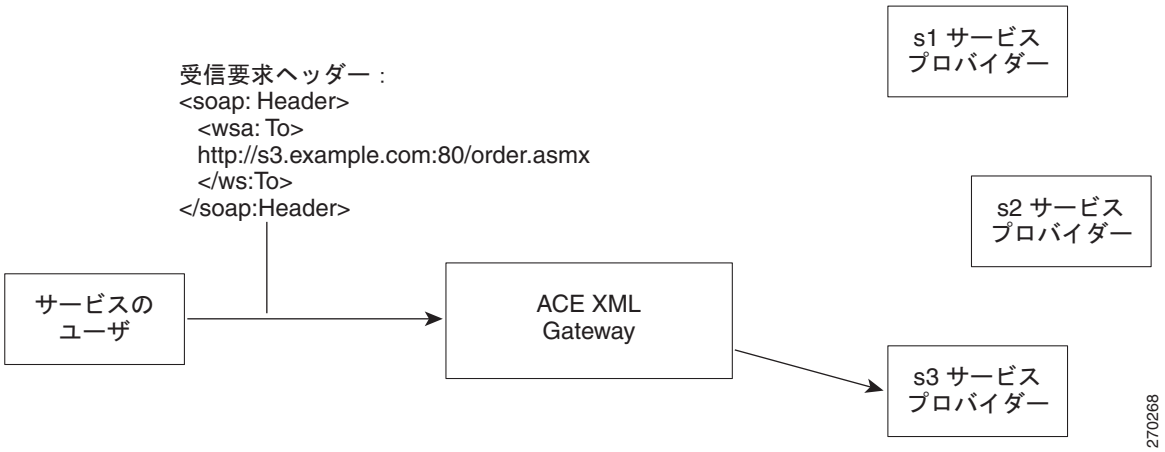
ACE XML Gateway での WS-Addressing サポート

ACE XML Gateway は複数の方法で WS-Addressing をサポートします。標準 SOAP サービス定義では、WS-Addressing ヘッダー処理を有効にできます。ACE XML Gateway は、バックエンド サービス インターフェイスに適切な情報で、ヘッダーの値を書き換えます。

このルーティング設定では、分岐したルーティングによって複数の代替宛先が可能であるときでも、仮想サービスの宛先はスタティックであり、宛先 Universal Resource Locator（URL）はポリシー設定に設定されます。WS-Addressing を使用してメッセージをルーティングするもう 1 つの方法は、ACE XML Gateway が WS-Addressing ヘッダーのコンテンツに基づいて、バックエンド宛先に動的にルーティングすることです。バックエンド サービス宛先をポリシーで指定する必要はありません。受信 To 値の内容で厳密に定義されています。

この例を 図 11-1 に示します。

図 11-1　WS-Addressing ダイナミック ルーティング



WS-Addressing ヘッダーのあるメッセージを受信した場合、ACE XML Gateway は、ヘッダーの To フィールドで特定されるリソースへ処理した要求を転送します。Gateway は、HTTP または HTTPS アドレスである To エレメントから抽出した宛先だけをサポートします。mailto などの別の種類のプロトコルのアドレスはサポートされません。

たとえば、HTTPS 宛先、または、特定のドメインへの宛先だけが（正規表現照合によって）許可されるように、Gateway がトラフィックをルーティングする宛先に制限を課すことができます。

スタティック ルーティングによる WS-Addressing の使用

ACE XML Gateway ポリシーの任意の SOAP サービス定義に、WS-Addressing ヘッダー処理を設定できます。そのためには、SOAP サービス設定の要求または応答に対する拡張 SOAP ヘッダー処理設定を使用します。WS-Addressing ヘッダー オプションは、[Known Header] タイプの下に表示され、`To` エレメントに対するオプションがあります。さらに、要求設定には `Action` エレメントに対するオプションがあります。

他の種類の SOAP ヘッダーと同様に、ヘッダーを必須、任意、または、禁止に設定できます。XSLT によって、ヘッダーの変換を指定することもできます（詳細については、「SOAP ヘッダー拡張設定」（P.11-120）を参照してください）。

Gateway には、要求に対して `To` エレメントおよび `Action` エレメントに次のカスタム処理オプションがあります。

- [Rewrite with the destination service URL] は、To エレメントのコンテンツを、サービス記述子のサービス インターフェイス設定から抽出した宛先 URL に置き換えます。アドレスは、サービスのホスト名とサービス パスから構成されます。
- [Rewrite with the destination SOAP Action] は、Action エレメントのコンテンツを、サービス記述子のサービス インターフェイス設定で指定された SOAPAction に置き換えます。

`To` 宛先および `Action` 値が発信メッセージ内で書き換えられる場合、受信メッセージは WS-Addressing ヘッダーのある状態で到着しなければなりません。そうでない場合は、この設定は効果がありません。

ダイナミック ルーティングでの WS-Addressing の利用

ダイナミック アドレッシングを実現するには、サービス定義に WS-Addressing サービス記述子を使用します。SOAP RPC ハンドラおよび SOAP ドキュメント ハンドラは、WS-Addressing ベースの SOAP サービス記述子にルーティングできます。

図 11-2　WS-Addressing サービス記述子へのルーティング

WS-Addressing サービス記述子の設定は、バックエンド サービス URL を含みません。その代わり、宛先 URL は、受信要求の `To` エレメントから得られます。URL が指定した要件に一致する限り、Gateway はメッセージを URL に送信します。

（注） デフォルトで、WS-Addressing サービス記述子でメッセージのルーティングに使用される SOAP ヘッダーは、発信メッセージ内に保持されます。

ACE XML Gateway で WS-Addressing ダイナミック ルーティングを使用するための一般的な手順は次のとおりです。

ステップ 1　[Virtual Services] ブラウザで、WS-Addressing サービスのユーザ インターフェイスを定義するハンドラを作成します。ハンドラは、SOAP Document プロトコル ハンドラまたは SOAP RPC プロトコル ハンドラのいずれかでなければなりません。

（注）　基本仮想サービス オブジェクトを使用して WS-Addressing を実装することはできません。仮想サービスは、ハンドラとサービス記述子のペアで構成される必要があります。

ステップ 2　サービス記述子を作成します。プロトコルに対して、次のいずれかを選択します。

- [SOAP Document with WS-Addressing Routing]、SOAP Document ハンドラからルーティングする場合。
- [SOAP RPC with WS-Addressing Routing]、SOAP RPC ハンドラからルーティングする場合。

ステップ 3　[Name] フィールドでサービス記述子の記述的な名前を入力します。名前は、サービス記述子で一意である必要があります。

ステップ 4　WS-Addressing サービス記述子のサービス インターフェイスを設定します。次の設定を除き、設定は他の SOAP サービス記述子と同様です。

- [SOAPAction] は、Gateway が発信要求の SOAPAction HTTP ヘッダーを生成する方法を制御します。このヘッダーに対して、ACE XML Gateway に次を実行させるようにできます。
  - [pass through incoming SOAPAction value] : 受信要求に SOAPAction HTTP ヘッダーが含まれる場合、その値は発信要求の SOAPAction HTTP ヘッダーへパススルーされます。
  - [use value from WS-Addressing Action element] : WS-Addressing Action エレメントは、URL によって、要求の対象であるサービスを指定します。受信要求に存在する場合、その値は SOAPAction HTTP ヘッダーへの代入に使用されます。
  - [use fixed value] : ポリシーで指定される値を使用します。オプションが選択されたときに表示されるテキスト フィールドに値を入力します。
  - [use value from XPath] : XPath 特定される受信要求のロケーションから抽出される値を使用します。
  - [use value from HTTP header] : 受信要求の名前付き HTTP ヘッダーから得られる値を使用します。
- [Destination] 設定は、Gateway が要求をルーティングする、許可されたバックエンド宛先を制限するために使用されます。次のオプションを使用して宛先を制御します。
  - [Only allow HTTPS destinations, regardless of any other restrictions] : Gateway に、To 値が HTTPS アドレスではないメッセージをブロックするように指示します。さらに制約事項を調整するには、[Restrict to destinations] オプションを指定してさらに要件を指定します。
  - [Restrict to destinations] : Gateway がメッセージをルーティングするバックエンド宛先に関する制限を指定します。受け入れ可能な宛先を URL によってまたはパターンマッチの正規表現を使用して示すことができます。正規表現が宛先値に一致する場合、メッセージはその宛先にルーティングされます。
  - [Forbid Destinations] は、WSA ヘッダーによって指定される宛先値にかかわらず、Gateway が決してメッセージを送信しないバックエンド サービスを特定します。たとえば、メッセージ ループ シナリオの可能性を防ぐために、WSA 設定の中で localhost を禁止アドレスとして設定することが想定されます。
- [Remote Server Cert] は、バックエンド サーバへの接続を作成するときに Gateway が受け入れるサーバ証明書の要件を設定します。したがって、たとえば、信頼される証明書を提供するバックエンド サーバだけにダイナミック ルーティングを制限できます。Certificate Authority（CA; 認証局）証明書リストから、証明書署名者として受け入れられる CA の証明書を選択します。

タイムアウト、SOAP バージョン、および、サービスタイムしきい値設定は他の種類の SOAP サービス記述子と同様です。

ステップ 5　**[Continue]** をクリックします。

ステップ 6　必要に応じて、要求メッセージおよび応答メッセージの要件を設定します。詳細については、「サービス記述子の作成」（P.5-43）を参照してください。

完了したら、サービス記述子設定ページが表示されます。ハンドラから新しい WS-Addressing サービス記述子へのルーティングが設定可能です。他の SOAP 機能では多くの場合有効にされますが、このハンドラは SOAP ヘッダー処理を有効にする必要がありません。

その要求の [Advanced SOAP Header Processing] 設定ページで受信ヘッダーの要件を設定できます。このハンドラがヘッダーのないメッセージが受け入れないように、このページで WSA ヘッダー オプション（`To` および `Action`）を必須に設定できます。サービス記述子によって、そのコンテンツが書き換えられるため、`To` エレメントまたは `Action` エレメントの書き換えを設定しないでください。これらの設定値の設定は、ポリシー コンパイル エラーを生じます。

完了したら、ポリシーを導入して、Gateway でサービスを利用可能にします。WS-Addressing サービスに関連付けられたイベントは、イベント ログの中で「WSAddress」という用語で特定されることに注意してください。