Cisco ACE XML ゲートウェイ
スタートアップ ガイド
Software Version 5.1

Cisco Systems, Inc. | 170 West Tasman Drive | San Jose, CA 95134-1706 | 800 553-6387

Cisco ACE XML Gateway は、アプリケーション指向のネットワーキング製品です。

この製品には、Apache Software Foundation（http://www.apache.org/）が開発したソフトウェアが含まれています。

この製品には、OpenSSL Toolkit で使用する目的で OpenSSL Project（http://www.openssl.org/）が開発したソフトウェアが含まれています。

この製品には、LibCURL が含まれています。cURL is © 1996 - 2004, Daniel Stenberg, <daniel@haxx.se>. All rights reserved.

この製品には、Gnome プロジェクト用に開発された XSLT C ライブラリ libxslt、および libxml2 が含まれています。Libxslt は、Gnome プロジェクト用に開発された XML C ライブラリ libxml2 をベースとしています。

この製品には、OpenLDAP が含まれています。Copyright 1999-2003 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved.

この製品には、カーネギー メロン大学 Computing Services（http://www.cmu.edu/computing/）が開発したソフトウェアが含まれています [Net-SNMP]。

この製品には、カリフォルニア大学バークレー校とその協力者が開発したソフトウェアが含まれています。

正規表現のサポートは、Henry Spencer の POSIX 1003.2 準拠 regex パッケージをベースとしています。Copyright 1992, 1993, 1994 Henry Spencer. All rights reserved.

GS5.1-070523-2303-a

Cisco ACE XML ゲートウェイ スタートアップ ガイド

OL-13875-01-J

CONTENTS

第 1 部　最初の手順

この「最初の手順」では、Cisco ACE XML ゲートウェイ の設定と利用の際に基礎知識として役に立つ概念を紹介します。ここで説明するのは、XML Gateway の実装で最初に行う、ネットワーク環境へのセットアップ方法です。

内容は次のとおりです。

Cisco ACE XML Gateway ソリューションの概要

Cisco ACE XML ゲートウェイは Cisco Application Control Engine（ACE）ファミリー製品を構成し、ネットワークにアプリケーション インテリジェンスをもたらします。この製品は XML（Extensible Markup Language）と SOAP（Simple Object Access Protocol）をベースとする、安全で信頼性が高く、迅速な Web サービス環境の効率的な構築を実現します。XML Signatur、XML Encryption、SAML など、XML と SOAP をベースとする、技術の利用を簡素化するツールと機能を提供します。

このマニュアルでは、セキュリティ、メディエーション、高速化などの機能を含む、ACE XML Gateway のツールと機能を説明します。手順は段階を追って説明し、実稼働で利用できる ACE XML Gateway ポリシーを設定する方法を示します。このポリシーは、ACE XML Gateway がトラフィックの処理方法を決定するための、一連のルールと動作です。

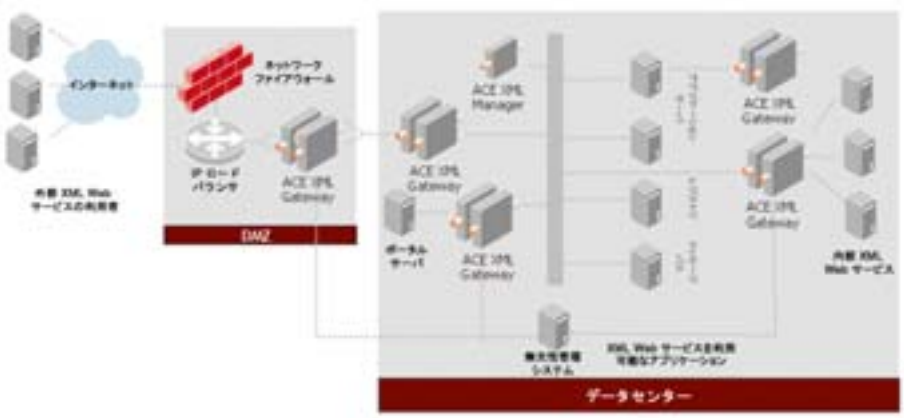
概要

図 3-1 に示すように、ACE XML Gateway は、必要に応じてネットワーク内の様々なロケーションで運用します。

主に DMZ 内に導入されますが、DMZ では、アクセス ルールやその他のセキュリティ ポリシー要件を外部ソースから流入するトラフィックに適用します。

保護されたネットワーク内では、アプリケーション トラフィックに対して集中的なルーティング ポイント兼メディエーション ポイントとして機能させることができます。また、プロセッサに負荷のかかる処理や XML 処理のタスクを、バックエンドのアプリケーション サーバから軽減します。

図 3-1　導入のトポロジ例



ACE XML Gateway は、どこに導入してもアプリケーションレベルでトラフィック管理と制御を行うことができるため、ネットワーク上のサービスで統一ポリシーを適用できます。

Cisco ACE XML ゲートウェイ システムの構成要素

Cisco ACE XML ゲートウェイは次の構成で導入します。

- ACE XML Gateway は、アプリケーション トラフィックのセキュリティと管理を担うエンタープライズクラスのアプライアンスであり、ネットワーク上のポリシー適用ポイントとして機能します。
- ACE XML Manager は、Cisco ACE XML ゲートウェイ ソリューションの管理用サーバであり、ポリシー作成とシステム監視のインターフェイスとなる Web コンソールを提供します。

マネージャ機能とゲートウェイ機能（スタンドアロン モードにおいて）を単一のアプライアンスで提供します。ただし、この構成はポリシー作成と評価が目的のため、実稼働での導入には推奨しません。

実稼働での導入では、一般的に 1 台の ACE XML Manager と 1 台または複数の ACE XML Gateway で構成されます。複数の ACE XML Gateway でクラスタを構成することができます。単一クラスタ内の XML Gateway はすべて同一のポリシーで機能する必要がありますが、別のクラスタでは別のポリシーを適用できます。つまり、個別のビジネス ニーズに特化させる場合、それぞれ独自のポリシーを持つ別個の ACE XML Gateway クラスタを設置したり、単一の ACE XML Manager を使用して開発、テスト、実稼働の各環境にポリシーの各バージョンを転送したりすることができます。

ACE XML アプライアンス製品は、フルサイズのラックマウント シャーシ、またはデスクトップ型である Gateway-D の形で提供されます。Gateway-D は設定の評価や開発向けですが、ラックマウント型のアプライアンスは実稼働環境に適しています。

XML Gateway のポリシー

ACE XML Gateway は、*ゲートウェイ ポリシー*が指定するとおりにトラフィックを処理します。ポリシーには DoS 攻撃への対応設定やコンテンツ スクリーニングのルール、あるいは、あるサービスに特化した設定など、ACE XML Gateway を通過するトラフィックに対するグローバルな設定が含まれます。

ポリシーは ACE XML Manager の Web コンソールで作成できます。Web コンソールから、ACE XML Gateway クラスタへポリシーを適用します。

ポリシーでは、次のような各種のメッセージ処理機能を設定できます。

- メッセージのコンテンツ、引数、その他の属性の確認

- メッセージ コンテンツの変換
- メッセージの属性またはコンテンツに基づいたサービス　ルーティングのダイナミックな選択
- ユーザ名 / パスワード、電子証明書、SAML 情報などの、ユーザ証明の確認
- XML Encryption によるコンテンツの暗号化と復号
- シグニチャの確認と生成

ポリシーは多数のポリシー オブジェクトとリソースで作成され、ACE XML Gateway のルールと動作を決定します。ポリシー内で重要なオブジェクトはサービス プロキシですが、これについては次で説明します。

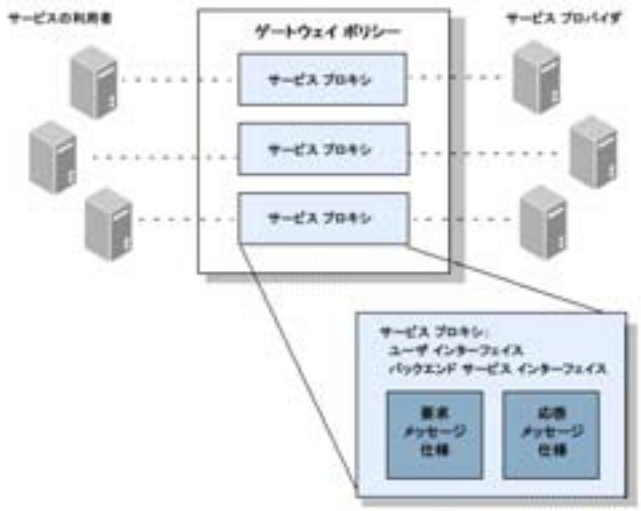
サービス プロキシの利用

ACE XML Gateway における外部サービスの定義で一番重要な要素は *サービス プロキシ*です。図 3-2 に示すように、ポリシーには多くのサービス プロキシを含めることができます。サービス プロキシはそれぞれ、ACE XML Gateway を経由して利用可能な特定のバックエンド リソースに対応しています。

サービス プロキシは、バックエンド サービス（そのサービス インターフェイス）の接続パラメータを認識し、サービスのサービス ユーザ（ユーザのインターフェイス）への表示方法を示します。

バックエンドの SOAP サービスに対しては、各サービス プロキシを特定の操作に対応させることができます。また、サービスが WSDL 文書のインポートで生成されている場合は、その WSDL 文書に記述されたすべての操作に対応させることができます。

図 3-2　ACE XML Gateway ポリシーの構成要素



サービス プロキシは、目的のサービスに到達する条件としてメッセージが適合すべき要件を定義します。このような要件には、メッセージ引数の有無や有効性といった、ユーザの資格証明や構成要件があります。メッセージは要件に合致すると ACE XML Gateway を通過します。合致しない場合は、XML Gateway がメッセージを遮断し、エラー応答を生成します。

このマニュアルでは、XML Manager を利用したサービス プロキシの作成および、ACE XML Gateway に到達した実際のトラフィックを用いたテストを学習します。このマニュアルに記載した手順により、上記の機能と概念を実際に経験することができます。

始める前に

次の各セクションで、このマニュアルの手順を実行するために必要な情報、ツール、システム要件を説明します。

必要な知識

このマニュアルは、ネットワーキング、セキュリティ、および XML の各技術に関連する概念を理解している読者を対象にしています。サービス指向アーキテクチャを実装すると、ネットワークとアプリケーション間の壁が低くなりますが、同時に組織上の各担当者にも相応した影響があります。そのため、ACE XML Gateway システムの実装ではほとんどの場合、経験の有無と関係なく、新しい作業が必要になります。

このマニュアルは ACE XML Gateway の背景知識を知っていただくために、実地作業を通して学習します。マニュアル セットには、ほかに『*Cisco ACE XML Gateway Installation and Administration Guide*』および『*Cisco ACE XML Gateway User's Guide*』が用意されていますが、これらも同様に背景的な情報を提供します。背景となる概念についてより詳細に把握する必要がある場合は、次の書籍を推奨します。

- Eric Rescorla 著、『*SSL and TLS*』― ネットワーク利用の際のセキュリティに関する一般的な情報と、特に PKI について学べます。
- Rosenberg、Remy 共著、『*Securing Web Services with WS-Security*』― WS-Security について学べます。

最小限必要なネットワーク構成の要件

このマニュアルで説明する最初の手順では、ACE XML アプライアンスを立ち上げてネットワーク上で動作させることを目的としています。この手順の実行に必要なものは次のとおりです。

- ACE XML アプライアンスに割り当てるスタティックな IP アドレス

  注： ACE XML Gateway と Manager を設定して単一のインスタンス（このマニュアルで説明されている構成）として実行する場合に必要なアドレスは 1 つだけです。ACE XML Gateway と ACE XML Manager を別個のアプライアンスに導入する場合は 2 つのアドレスが必要になります。

- ネットワークに用意されているデフォルト IP ゲートウェイの IP アドレス
- ネットワークに用意されているプライマリ DNS サーバの IP アドレス
- ローカル ネットワークの DNS サーバ（推奨）に登録するために ACE XML Gateway に与えるホスト名

- ACE XML Gateway アプライアンス上のルート アカウントに使用するパスワード

  今回が初めての導入で、ルート パスワードがわからない場合は、サポート担当者に問い合わせてください。

トラフィックを生成するための要件

このマニュアルにある手順でポリシーの設定が終了すると、そのポリシーを実際のトラフィックでテストすることができます。テストを行うには、XML Manager に組み込まれたテスト用ブラウザ、または Microsoft WFetch や Curl などの HTTP クライアント ツールを利用できます。

初期テスト用にサンプルのサービスがいくつか用意されています。このマニュアル中の手順を独自のサービスを使用して実施する場合は、次のものも必要になります。

- サーバ上で実行する Web サービス（.NET や AXIS などによる）
- 利用可能なサービスを記述する WSDL ファイル（ACE XML Gateway は WSDL ファイルを必要としませんが、セキュリティ ポリシーの作成が簡単になります）
- セキュリティ機能をテストするには、ACE XML Gateway 用およびクライアント認証用の公開鍵 / 秘密鍵ペアなどのリソースが必要です。
- 他のシステム（LDAP サーバなど）と同時に ACE XML Gateway をテストする場合は、それらのシステムのほかにも、関連するリソース（LDAP クエリーなど）を利用可能である必要があります。

初期セットアップ作業

次の手順では、ネットワークへの物理的な接続から基本的な各種のネットワーク設定まで、ACE XML アプライアンスの初期セットアップ方法を説明します。

インストールの準備

ACE XML Gateway アプライアンスまたは ACE XML Manager アプライアンスに対して行う基本的ネットワーク設定は、そのアプライアンスのオペレーティングシステム環境で行います。アプライアンスのシャーシ ポートはモデルにより様々なため、オペレーティングシステムにアクセスする手順も異なります。

アプライアンスのオペレーティングシステムにアクセスするには、モニタと USB キーボード、または KVM スイッチをそのアプライアンスに接続します。アプライアンスはシリアル コンソール接続もサポートします。この方法では、端末エミュレーション ソフトウェアまたはダム端末を備えた PC を、シリアル ケーブルでアプライアンスに接続できます。端末エミュレーション ソフトウェアまたはダム端末は VT-100 互換でなければなりません。

> **注：** アプライアンスへはシリアル接続でアクセスできますが、初期状態ではブート時のメッセージの出力先がシリアル出力ではなく、KVM 出力に設定されていることに注意してください。シリアル アクセスの詳細については「シリアル ケーブルによる接続」を参照してください。

初期セットアップ手順は次のとおりです。

1. 梱包からまだアプライアンスを取り出していない場合は取り出してください。

   > **注：** アプライアンスの評価試用中である場合は、返却に備えて梱包物を保存しておいてください。また、梱包には多くの場合、アプライアンスの返却に利用できる返送用配送伝票が含まれています。

2. モニタとキーボードをアプライアンス背面に接続します。シリアル ケーブルによる接続の詳細は「シリアル ケーブルによる接続」を参照してください。
3. アプライアンスの電源接続口に電源コードを差し込みます。
4. アプライアンスのバックパネルにあるネットワーク インターフェイス ポートにイーサネット ケーブルを接続します。ラックマウント型のアプライアンスにはイーサネット インターフェイス ポートが 5 つあります。バックパネルの上部左側の iLO（Integrated Lights-Out）コネクタ以外のコネクタのいずれかにケーブルを接続します。どのインターフェイスを使用しているかをメモしておいてください。

5. 電源ボタンを押してアプライアンスの電源を入れます。電源ボタンは Gateway-D ではフロントパネルに、ラックマウント型アプライアンスではバックパネルにあります。なお、旧型モデルでは、電源スイッチを使用するためにフェースパネルを外さなくてはならない場合があります。

システムが起動します。起動プロセスが終了すると、モニタにログイン プロンプトが現れます。

シリアル ケーブルによる接続

アプライアンスを直接 KVM に接続する代わりに、シリアル ケーブルを使用してラップトップなどの PC の DB-9 型シリアル コネクタに接続しても、アプライアンスに接続できます。

ラップトップなどの PC 側では、Microsoft HyperTerminal などの VT-100 互換端末エミュレーション ソフトウェアを装備している必要があります。

この接続は次のように設定してください。

- ビット / 秒：9600
- データビット：8
- パリティ：None
- ストップビット：1
- フロー制御：None

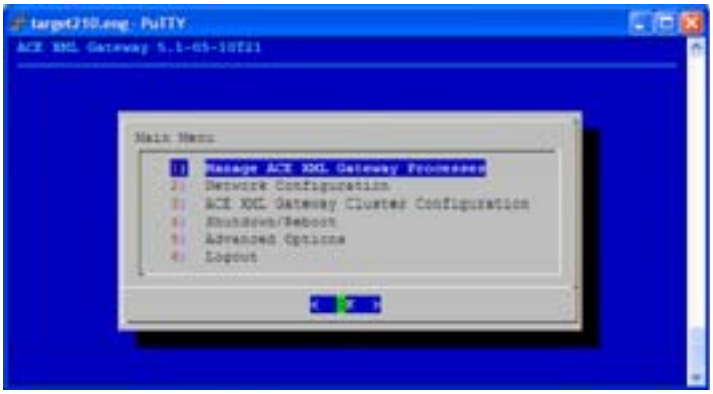
初期設定作業

アプライアンスに物理的接続を行ったあとに、基本的な設定を次のように行います。

1. アプライアンスのログイン プロンプトから `root` ユーザでログインします。パスワードは自分に割り当てられているものを使用してください。`root` のパスワードがわからない場合は、サポート担当者に問い合わせてください。
2. デフォルトのパスワードを使用してログインすると、パスワードを変更するように求められます。その場合は次のように操作します。
   a. **[OK]** をクリックするか、Enter キーを押します。
   b. **Please enter the new root password** という表示が出たら、新しいパスワードを入力して **[OK]** をクリックします。
   c. 次に現れた表示でパスワードを確認入力します。

   アプライアンス管理インターフェイスのメイン メニューが表示されます。

図 5-1　コマンドライン シェルのメニュー



3. 2 番めの項目 **[Network Configuration]** を選択して **[OK]** をクリックします。

   [Network Configuration] メニューが表示されます。

4. このメニューでネットワーク構成を次のように設定します。

   a. 最初の項目 **[Hostname]** を選択して **[OK]** をクリックします。

   b. ホスト名の画面で ACE XML Gateway の適正なホスト名の全体を入力します（`xmlgate.example.com` など）。入力を終えたら **[OK]** をクリックします。

      再び **[Network Configuration]** メニューが表示されます。

   c. **[IP Gateway]** を選択して、アプライアンスのネットワーク インターフェイスの接続先となるサブネットワークにおけるデフォルト ゲートウェイの IP アドレスを入力します。入力を終えたら **[OK]** をクリックします。

   d. **[Name Servers]** を選択して、利用しているネットワーク内の DNS サーバの IP アドレスを入力します。DNS サーバを 1 つ以上指定するには、複数の IP アドレスをスペースで区切って入力します。アプライアンスはリスト内で最初のサーバに問い合わせを行い、ネームサーバからの応答がない場合は以下順番に問い合わせを行います。入力を終えたら **[OK]** をクリックします。

   e. デフォルトでは、アプライアンス上の物理ネットワーク インターフェイスが無効になっています。**[Network Configuration]** メニューでネットワーク ケーブルを差し込んだインターフェイスを **Interface eth0** などの識別子で選択します。

      注： Gateway-D アプライアンスにはイーサネット ポートが 1 つしかないため、インターフェイス メニューの選択肢が 1 つ（**Interface eth0**）しかありません。フルサイズのアプライアンスでは、各ネットワーク インターフェイスに対応するインターフェイス メニューが現れます。

   f. ネットワーク インターフェイス メニューの最初の項目 **[enabled]** を選択します。

g. アプライアンスの IP アドレスを入力して **[OK]** をクリックします。

h. その IP アドレスに対するネットワーク マスク（netmask）を入力します。

i. 次に現れる入力画面で、そのインターフェイスのイーサネット速度を選択して **[OK]** をクリックします。

j. **[Edit Static Routes]** 画面で **[Accept settings]** を選択して **[OK]** をクリックするか、**[Cancel]** を選択してやり直します。

k. **[Network Configuration]** メニューで **[Test Network Settings]** を選択します。設定した内容に対して、ACE XML Gateway がいくつかの基本的なネットワーク テストを実行して結果を報告します。

5. クラスタ構成の設定を行うように求められた場合は、今回だけ [yes] を選択して設定します（要求されなかった場合は、**[Main Menu]** で 3 番めのオプション **[ACE XML Gateway Cluster Configuration]** を選択してください）。

   a. Gateway-D を使用している場合は、**[Both Gateway and Manager]** オプションを選択してアプライアンスをスタンドアロン モードで動作させてください。このモードでは、アプライアンスが XML Gateway と XML Manager の両方の機能を持ちます（システムの評価試用を行う際に通常使用されるモードです）。

      XML Gateway もしくは XML Manager として専用に利用する場合は、**[ACE XML Manager]** または **[ACE XML Gateway Cluster Member]** のいずれかの運用モードを選択してください。

   b. アプライアンスを ACE XML Gateway として動作するように選択した場合は、このアプライアンスを管理する ACE XML Manager のアドレスを指定してください。

   c. 要求された場合はアプライアンスのサービスを再起動して、設定変更を有効にします。その場合 **[yes]** を選択してください。

   d. アプライアンスを ACE XML Manager またはスタンドアロン マシンとして動作するように選択した場合は、ACE XML Manager の Web コンソールの、クラスタ数の追加または変更が必要という通知画面で **[OK]** をクリックします。

      スタンドアロン マシンについては、自身のゲートウェイ インスタンスを管理するように Manager が設定済みです。XML Manager 機能のみのマシンについては、管理対象の XML Gateway を Web コンソールの [Cluster Management] ページで設定する必要があります。

作業はこれで完了です。この ACE XML Gateway は設定が終了して、使用する準備が整いました。シェル インターフェイスを終了するには、メインメニューで [Logout] を選択します。

アプライアンスのネットワーク設定が終了したら、モニタとキーボードまたはシリアル ケーブルを外してもかまいません。ブラウザを使用して、ACE XML Manager の Web コンソールをローカル ネットワーク上で利用できます。アプライアンスのオペレーティングシステム環境に再度アクセスする必要がある場合は、PuTTY などのリモート SSH クライアントを使用できます。

XML Manager Web コンソールの使用

ACE XML Manager の Web コンソールは、ACE XML Gateway 用ポリシーの作成環境となります。ポリシー作成用の環境だけでなく、システム導入の監視ポイントとしても機能します。

ACE XML Manager の Web コンソールへのログイン

ACE XML Manager の Web コンソールは、最新バージョンのブラウザで利用できます。特に、Mozilla Firefox 1.5.0.*x* と 2.0.0.*x*、および Microsoft Internet Explorer 5.5 と 6 をサポートします。

ACE XML Manager の機能を適切に動作させるため、ブラウザの JavaScript 機能が有効になっている必要があります。

ブラウザから ACE XML Manager を利用するには、次のようにアクセスします。

1. ブラウザのアドレス欄にコンソールの URL を入力します。
   `https://<IP_Address>:8243`

   ここで、*<IP_Address>* は、前の章で ACE XML Manager に設定した IP アドレスです。ACE XML Manager Web コンソールへの接続は HTTPS（セキュリティの施された HTTP）を使用する必要があることに注意してください。また、ここに示すように、コンソールのデフォルトのリスニング ポートは 8243 です。
2. 一時的証明書を受け入れ、ログイン ページを表示します。

図 6-1　Manager へのログイン

3. ログイン欄には、ユーザ名として `administrator`（大文字と小文字の区別あり）と、administrator のパスワードを入力します。administrator のパスワードがわからない場合は、サポート担当者に問い合わせてください。

注： これは前の章「初期セットアップ作業」に記載の、アプライアンスのシェル インターフェイスへのアクセス時に使用するユーザ アカウントとは別のもの（通常はパスワードも別）であることを覚えておいてください。

実稼働レベルのプロジェクトの開始後、最初に行う作業の 1 つとして、プロジェクトの各メンバーまたは各グループに対してユーザ アカウントを Web コンソールで作成します。ただし、評価試用時には既存の `administrator` アカウントを使用することがあるかもしれません。

4. 使用しているシステムが有効なライセンスキーを*未設定*の場合は、メッセージが表示され、製品ライセンスの更新が必要であることを通知します。

   ライセンス ファイルを持っていない場合は、サポート担当者に問い合わせてください。ライセンス ファイルがある場合は、次の手順でライセンスを更新します。

   a. 提供されたライセンス ファイルを探し出し、テキスト エディタで内容をシステム クリップボードにコピーします。

   b. ライセンスをコピーしたら、ライセンス エラー ページ最下部にある **[License Management]** リンクをクリックします。

   c. ライセンスのテキストを **[License File]** 欄にペーストし、**[Save Changes]** をクリックします。

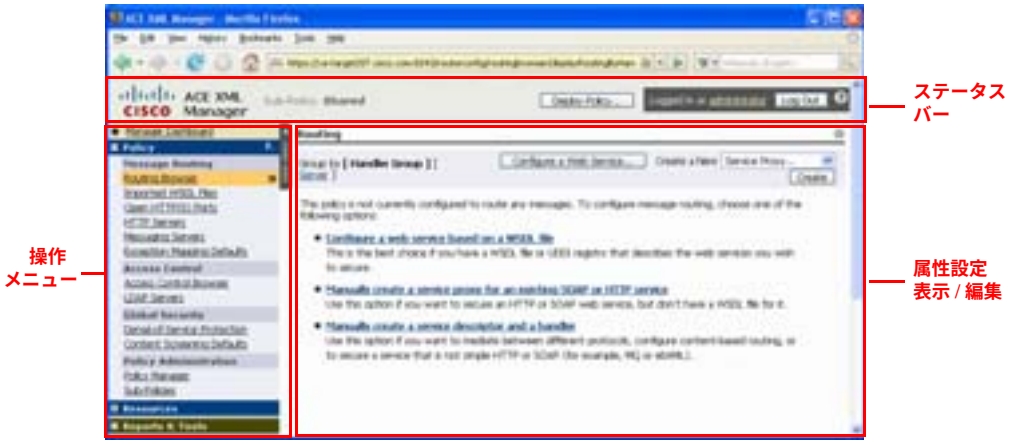
   正常に実行すると、「Your changes have been saved」という通知メッセージが表示されます。これで ACE XML Manager の Web コンソールを利用できるようになりました。

ACE XML Manager の Web コンソールの操作

*空*のポリシーを 1 つ持つ ACE XML Manager Web コンソールにログインすると、**Welcome** ページが表示されます。この **Welcome** ページから SOAP のトラフィック ルーティングの設定を開始できるほか、このページから出てポリシーの他の部分に対する作業を行ったり、他の種類のトラフィックに対してルーティングを設定することもできます。

図 6-2 に、ACE XML Manager Web コンソールで利用するインターフェイスの主要な構成を示します。

図 6-2　ACE XML Manager Web コンソール



このインターフェイスの主要な構成は、次のとおりです。

- *属性エディタ*には、システムの特定の状況や動作におけるステータス情報と設定が表示されます。
- コンソールの左側に表示される*操作メニュー*では、コンソールの様々な属性ページを開くリンクを利用できます。
- *ステータスバー*は、サブポリシー（1 つのポリシーは複数の部分に分けて構成することが可能で、その部分をサブポリシーと呼ぶ）の導入や切換えなどの、共通する操作を提供します。

このマニュアルでは、様々な設定作業を行うための詳細な手順を 1 つ 1 つクリックしながら進めることができます。しかし、ある作業を実行するためのコンソール操作方法は 1 つだけではありません。記載された手順を進める際は、ACE XML Manager Web コンソール インターフェイスを自由に試し、自分に適した操作手順を見つけて見ください。

第 2 部　ポリシーに関する作業

第 2 部では、ACE XML Gateway でサービスを保護するためのポリシー オブジェクトを定義する、一連の手順を説明します。最初に、ACE XML Gateway でのプロキシ処理の対象となるサービスを記述した WSDL 文書のインポートから始めます。次に、設定をテストしてから、システムが提供するログ作成ツールを実際に試します。

内容は次のとおりです。

サービスの仮想化

インストールの完了後、XML Manager と XML Gateway には空のポリシーが 1 つ用意してあります。最初の作業として、このポリシーに自分でルールと設定項目を追加することができます。プロキシ処理についての基本的設定をポリシー内に作成する作業は、手作業（外部サービスを表すポリシー オブジェクトを手で追加）または自動（WSDL 文書のインポート）で行うことができます。

WSDL 文書のインポートによる Web サービスの定義

ACE XML Gateway にサービス トラフィックを処理させるための設定では、最初の手順として、外部サービスから設定をカプセル化するポリシー オブジェクトを作成します。カプセル化は、そのサービスを記述した WSDL 文書をインポートすることで、一度に行うことができます。Manager は WSDL 文書の内容に基づいて、サービス プロキシを含むポリシー オブジェクトを生成します。このポリシー オブジェクトには、外部 Web サービスについての設定が記述されています。

WSDL 文書は、URL または UDDI レジストリからインポートできます。このマニュアルでは、URL から WSDL 文書をインポートする手順を説明します。

WSDL 文書のインポート手順は次のとおりです。

1. **Welcome** ページで **[Configure a Web Service]** ボタンをクリックします。

   注： Routing Browser を開く（操作メニューの **[Routing Browser]** リンクをクリックする）と、Web コンソールの他の場所からでもこのボタンを利用できます。

   一連の **[Configure a Web Service]** ページの最初のページは **[Locate Service]** です。図 8-1 に示すように、メニューにはポリシー内に Web サービスを定義するためのいくつかのオプションが用意されています。

図 8-1　インポートのオプション

Manager は UDDI レジストリへの問い合わせ、または WSDL 文書のインポートで得られた情報に基づいてサービス定義を生成できます。

2. このマニュアルでは、URL から WSDL 文書をインポートする手順を説明します。メニューでオプション **[Import WSDL File from URL or Disk]** を選択したら、オプション ボタン **[URL]** を選択します。
3. サンプルのリソース サイトをホストとするサービスの URL を **[URL]** ボタンの隣の入力欄に入力します。

   http://example.reactivity.com/service/order.asmx?WSDL

   注： 他のサービスについてのポリシーを作成する場合は、その URL を入力するか、使用したい WSDL ファイルを現在使用中のファイル システム上で **[File]** 欄に指定します。WSDL 文書のディレクトリを指定する代わりに、Manager に UDDI サーバ上でサービスを検索させるコントロールも使用できます。
4. **[Continue]** をクリックします。

   [Consumer Interface] 設定の中で、**[Exposed Port]** の選択肢が `[Default HTTP port [80, Insecure]]` になっていることに注意してください。あとで、サービスが SSL ポート 443 を使用するように設定することにします。それまではデフォルトの HTTP ポート 80 しか利用できません。
5. **[Exposed Path]** は、ユーザが ACE XML Gateway でサービスを指名するために使用する起動用パスです。デフォルト値を `/orders` に変更します。

   デフォルトとして、このポリシーは起動用パスを WSDL 文書から読み取ります。セキュリティ上の理由から、デフォルトの起動用パスは必ず変更しておくことを推奨します。このようにすると、パスにより外部に公開され、ハッカーによる攻撃にさらされる可能性のあるバックエンド インフラに関する詳細を隠すことができます（たとえば、拡張子 .asmx は .NET フレームワークであることを示唆します）。ユーザにとってさらに便利な呼び出しインターフェイスを公開することも可能で、ユーザをバックエンド サービスでの変更から解放することができます。
6. **[Access Control]** オプションでは **[Public]** を選択します。あとで、サービスへのアクセスを制御する条件を指定します。
7. **[Default Message Logging]** メニューから `[log bodies of inbound and outbound messages]` を選択します。

   ポリシーを導入する際は、メッセージ トラフィックのログ作成機能を起動しておくと良いでしょう。ACE XML Gateway を通過する実際のメッセージの中で設定変更の結果を確認できます。
8. エクスパンド コントロールをクリックして、**[Advanced Options]** を表示します。

   Manager はサービス プロキシと呼ぶポリシー オブジェクトを持つ外部サービスを提示します。サービス プロキシは WSDL 文書内の単一のオペレーション、または各サービス エレメントに対応させることができます。サービス エレメントの場合はサービス プロキシに複数のオペレーションを含めることができます。デフォルトでは、Manager は複数のオペレーション サービス プロキシを作成します。複数のオペレーションに対して各プロキシが単一の設定ポイントを提供するためです。ここでは、各オペレーションについて 1 つのサービス プロキシを生成します。

9. **[Condense SOAP Document operations into one service proxy per WSDL "Service" element, if possible]** と表示されているオプションのチェックボックスをクリックして無効化し、選択されないようにします。
10. このページ最下部にある **[Continue]** をクリックします。

    Deploy Policy ページが表示されます。このページのテキストが示すように、設定変更はそのポリシーを導入するまで ACE XML Gateway で有効になりません。有効になるまでは、XML Gateway での命令サービスに対して発行されたメッセージが遮断されます。ポリシーの導入はあとで実行します。最初に、WSDL 文書インポートの結果を確認します。
11. **[Return to Routing Browser]** をクリックします。

新規ポリシーの検査

ACE XML Gateway がメッセージ ルーティングの対象とするサービスを Routing Browser が表示します。図 8-2 に示すように、インポートされた WSDL 文書に基づいて、いくつかのサービス プロキシが生成されました。

図 8-2　新しいサービス プロキシを表示する Routing Browser

このポリシーにはサービス プロキシとして、`retrieveQuote`、`submitOrder`、`submitPayment` の 3 つが含まれています。いずれかのサービス プロキシの名前をクリックすると、詳しい設定内容を見ることができます。

たとえば、`RetrieveQuote` をクリックすると、このサービスの設定が表示されます。

図 8-3　サービス プロキシの情報ページ

このページは、このサービスに対するトラフィック処理について、要求と応答の検証と処理の要件を含む設定内容を表示します。この設定ページは１つ１つのサービスに対応しており、このマニュアルで説明されている設定作業のほとんどがこのページから行うことになります。

XML Gateway へのポリシー導入

ここまでは運用中のポリシー（ACE XML Manager 上で作成中のポリシー）の修正を行ってきました。このポリシーをネットワーク トラフィックに適用させるには、ACE XML Gateway に導入する必要があります。

ポリシー導入は、次のような複数の段階を経て行われます。

- XML Manager が現行のポリシーと提案されたポリシーの間を比較して、その違いを表示する。
- ユーザがポリシーの変更内容を承認すると、Manager がそのポリシーをコンパイルする。
- コンパイルされたポリシーが ACE XML Gateway に転送される。

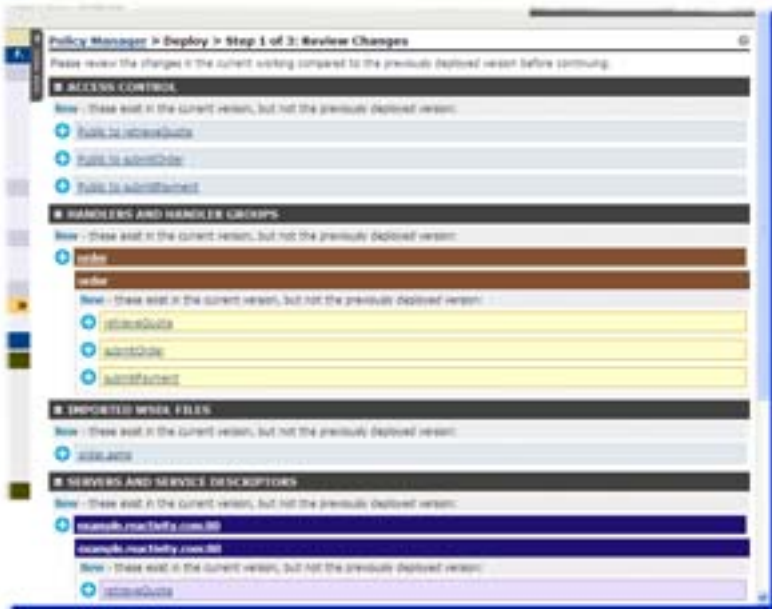
ポリシーを導入する手順

ポリシーを導入する方法は次のとおりです。

1. ACE XML Manager Web コンソール最上部の **[Deploy Policy]** ボタンをクリックします。

   最初の導入ページが新旧ポリシー間の変更点を表示します。この例では、WSDL 文書のインポートにより追加されたオブジェクトが変更点です。

図 9-1　導入手順 1/3 — 変更点の確認



2. ページ最下部にスクロールして **[Continue to Next Step]** をクリックします。

   Step 2 of 3, Basic Policy Review ページが表示されます。このページは導入するポリシー内の警告とエラーを示しています。ログ設定については、パフォーマンスに関する警告を表していることに注意してください。メッセージ本文のログ作成はパフォーマンスに影響するため、実稼働のシステムでは推奨しません。

3. **[Continue to next step]** をクリックします。

   Compile and Deploy ページが表示されます。このページは、その XML Manager が属す管理用ドメインに存在する ACE XML Gateway を示しています。ポリシーは特定の XML Gateway （複数可）を選んで導入することができます。一般的には、すべての XML Gateway で同じバージョンのポリシーを持たせるべきです。

   Out of date というステータスは、ACE XML Gateway 上のポリシーがコンパイルしたポリシーと相違していることを示します。

4. **[Policy Description]** 欄にポリシーの説明を入力します（「WSDL 文書からインポートした発注サービス」など）。

   デフォルトでは、ポリシーについての説明入力は任意です。一般的には、ポリシー バージョンの説明を加えることを推奨します。後日、ロールバックやポリシーの比較が必要になった場合に役立ちます。

5. **[Deploy to Selected Gateways]** をクリックして、コンパイルしたポリシーを ACE XML Gateway に導入します。

少し待つと、導入ページが再表示されます。再表示後は、ACE XML Gateway のステータスは **Up to date** となっています。

ポリシーの管理

ポリシーを導入すると、導入したバージョンが Policy Manager のポリシーバージョン履歴に記録されます。ACE XML Manager には多数の管理用ポリシーが用意されています。たとえば、ポリシーのバックアップ機能（さきほど導入したポリシーを含む）、以前のバージョンのポリシーへのロールバック（復元）機能、ポリシーのバージョン比較などが含まれています。

Policy Manager にアクセスするには、操作メニューの **[Policy]** エリアにある **[Policy Manager]** リンクをクリックします。

図 9-2　Policy Manager

このページ最下部のポリシー バージョン履歴では、さきほど導入したポリシーを含む、複数のバージョンが表示されます。

Policy Manager では、次の作業を行うことができます。

- 以前のバージョンのポリシーの*表示*、または*復元*。ロールバックを行うと、XML Manager 内で運用中の現行ポリシーが、前回 ACE XML Gateway に導入したものに置き換わります。ポリシーのロールバックを行ったあとは、そのバージョンを ACE XML Gateway へ伝達するためにそのポリシーの導入が必要になります。以前のバージョンのポリシーにロールバックするには、ポリシー履歴リストの中の **[Roll Back]** ボタンをクリックします。
- ポリシーのファイルへの*エクスポート*。別のシステム環境（たとえば開発環境から運用環境）へのポリシーの移動、バックアップ作成、サブポリシー間でのオブジェクトの移動などに便利な機能です。また、サポート担当者とポリシーを交換することが可能になるため、トラブルシューティングにも利用できます。
- [*Save to History*] は現在運用中のポリシーの複製を作成します。この複製はポリシー履歴リストに表示されます。ポリシー バージョンは、ポリシーを導入した際にも自動的に記録されることに注意してください。
- 現行ポリシーと ACE XML Gateway に導入されたポリシー間、または 2 つのバージョン間での差異を調べるための*ポリシー間の比較*。
- *ポリシーのリセット*による初期状態への復帰。Policy Manager の **[Reset Policy]** ボタンをクリックすると、インストール後に行われたポリシーへのあらゆる変更を取り消します。システムの学習に便利な機能です。ロールバックと同様に、ACE XML Gateway でリセットしたポリシーを有効にするには、そのポリシーの導入が必要です。

XML Gateway へのトラフィック送信

ポリシーの導入後、ACE XML Gateway に Order サービス要求を送信して設定のテストを行うことができます。ACE XML Manager Web コンソールにはテスト用ブラウザが用意されており、単純な要求を ACE XML Gateway のサービスに送信するために利用できます。

テスト用ブラウザから要求を送信すると、その要求は実際には ACE XML Gateway で始まります。サービス プロキシにアクセス要件が必要な場合、クライアントと同様に、この ACE XML Gateway もそれらを満たしている必要があります（ポリシーが特定のクライアントの IP アドレスへのアクセスを制限している場合、覚えておく必要があります）。

テスト用ブラウザは本来、ACE XML Gateway とバックエンド サービス間の接続をチェックするためのものですが、新規のサービス プロキシに対して最初に行うテストにも使えます。

テスト用ブラウザの使用

サービス プロキシをテスト用ブラウザから試す手順は次のとおりです。

1. **[Routing Browser]** で `retrieveQuote` サービス プロキシの名前をクリックします。

   サービス プロキシ情報のページが表示されます。

2. **[Test]** メニューが現れるまでページを最下部へスクロールします（このメニューにはデフォルトの選択肢 **-- Send Test Message --** が入っています）。

3. **[Test]** メニューから **[Test Consumer Interface]** を選択し、**[Test]** ボタンをクリックします。

   Send Test Message ウィンドウが表示されます。このサービス プロキシに適した SOAPAction ヘッダと本文があらかじめテキスト入力欄に記述されています。XML Manager が、スキーマから取り出した値を使用して要求の本文を記述します。次に例を示します。

   ```
   <ord:year>3</ord:year>
   ```

   自動的に生成された値は、より実際的な値へ任意に変更できます。ただし、このサービスはテスト用ブラウザが生成した値で機能するので、ここでは不要です。

4. 準備ができたら **[Send Test Message]** をクリックします。

正常に終了すると、正常終了の応答メッセージが HTTP 応答コード 200 として Response ページに表示されます。応答の中に `retrieveQuoteResponse` という名前のエレメントが現れることに注意してください。正常に終了できなかった場合は、応答ウィンドウにエラー メッセージが表示されます。

クライアント用テスト ツール

テスト用ブラウザは、XML Gateway サービスの最初のテスト ツールとしては役立ちますが、より実際的なテスト シナリオについては、HTTP クライアント用テスト ツールを使用する必要があります。無料で利用できる Microsoft WFetch、soapUI、Curl など、多数のテスト ツールがあります。

Curl はコマンドライン ツールですが、次のサイトから入手できます。

```
http://curl.planetmirror.com/
```

Parasoft SOAtest は、自動テストおよび負荷テストをサポートする SOAP クライアントのテスト ツールです。詳細は、次のサイトを参照してください。

```
http://www.parasoft.com
```

次に、Microsoft の WFetch を使用してサービスをテストする手順を紹介します。WFetch は IIS Diagnostics Toolkit の一部ですが、Microsoft Download Center で「WFetch」を検索して、入手できます。次のサイトを参照してください。

```
http://www.microsoft.com/downloads/search.aspx
```

WFetch を使用したポリシーのテスト

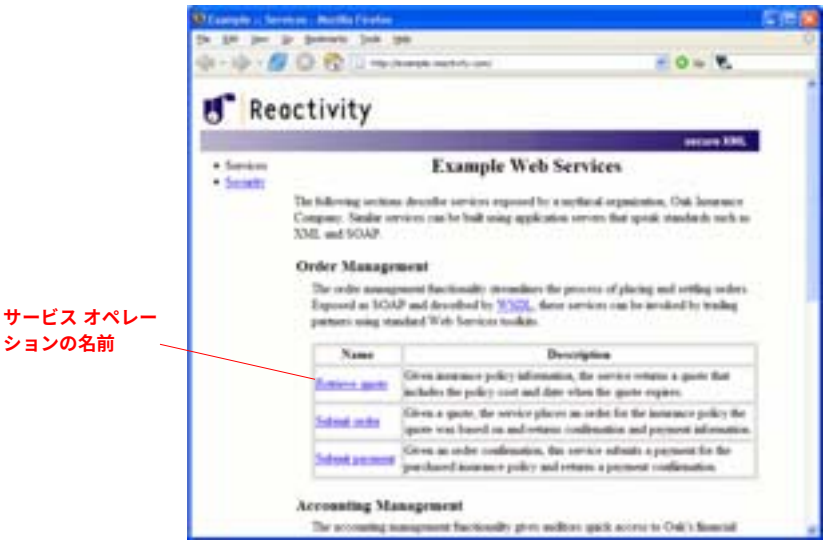
最初に WFetch をダウンロードしてインストールし、WFetch でサービスをテストします。詳細については、Microsoft の資料を参照してください。

Web コンソールのテスト用ブラウザが要求メッセージを生成しました。別のクライアントを使用する場合、テスト メッセージを手作業で作成する必要があります。テスト メッセージは、サービス例示サイトで公開されているメッセージ テンプレートを利用して作成することができます。

要求のテンプレート サイト：http://example.reactivity.com/

例示ページで **Retrieve quote** サービス オペレーションの名前をクリックします。

図 10-1　サービス オペレーションの情報



要求メッセージ テンプレートが応答例とともに表示されます。要求メッセージ テンプレートを利用してメッセージを作成し、HTTP クライアント ツールから ACE XML Gateway へ送信します。手順は次のとおりです。

1. WFetch を開き、メッセージ構成ページで **[Verb]** オプションを **[POST]** に設定します。
2. **[Host]** 欄に ACE XML Gateway のホスト名を入力します（`xmlgateway.organization.com` など）。
3. **[Port]** 欄に `80` と入力します。
4. **[Path]** 欄に、テストのために公開するサービスのローカル パスを入力します。「WSDL 文書のインポートによる Web サービスの定義」の「サービスの仮想化」で設定したように、**[Path]** 欄は `/orders` とします。

   [Ver]、**[Auth]**、**[Connect]** は、それぞれデフォルト値の `1.1`、`Anonymous`、`http` でかまいません。
5. **[Advanced Request]** オプションでは `[Add Headers&Body]` を選択します。
6. テキスト入力欄にテスト メッセージのヘッダと本文を追加します。出力例 10-1 を参照してください。HTTP ヘッダと本文は必ず空白行で区切ってください。

出力例 10-1　SOAP メッセージ

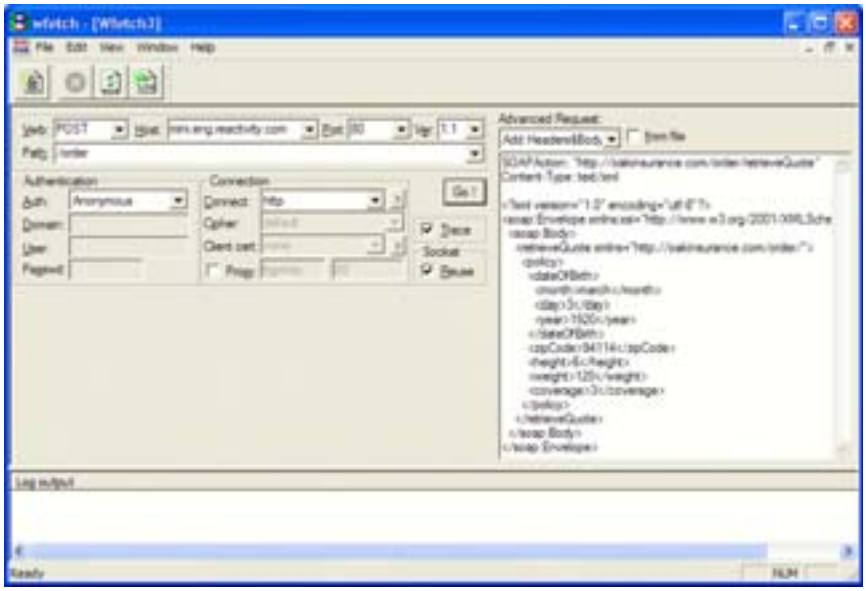
```
SOAPAction: "http://oakinsurance.com/order/retrieveQuote"
Content-Type: text/xml

<?xml version="1.0" encoding="utf-8"?>
 <soap:Envelope
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
   xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Body>
  <retrieveQuote xmlns="http://oakinsurance.com/order/">
    <policy>
      <dateOfBirth>
        <month>January</month>
        <day>1</day>
        <year>1960</year>
      </dateOfBirth>
      <zipCode>94002</zipCode>
      <height>52</height>
      <weight>150</weight>
      <coverage>402</coverage>
    </policy>
  </retrieveQuote>
 </soap:Body>
</soap:Envelope>
```

メッセージ テンプレートを example.reactivity.com からコピーする場合は、テンプレートのテキストをリストに示したサンプル値に必ず置き換えてください。

WFetch メッセージの設定ページが次のように表示されます。

図 10-2　WFetch メッセージ設定ページ



7. **[Go!]** ボタンをクリックして要求を送信します。

   図 10-3 にあるような応答が **[Log Output]** 欄に表示されるはずです。

図 10-3　WFetch の応答

この応答にはサンプルの価格、有効期限などともに、`retrieveQuoteResult` エレメントが含まれていることに注意してください。

WSDL 文書の自動生成と公開

XML Manager は、ポリシーで定義した SOAP サービスに対応する WSDL 文書を自動生成できます。WSDL 文書は様々なアプリケーションで便利に利用できます。一部の開発環境では、たとえばサービスのクライアント コードの生成に使用できます。テスト ツールの場合なら、テスト フレームワークの実装に使用できます。XML Manager から生成された WSDL 文書では、ポート定義において ACE XML Gateway をサービスの配置先として指定します。

WSDL 文書は、ポリシー内ではハンドラ グループに相当します。ハンドラ グループには任意の数のサービス プロキシ、ハンドラ、またはサービス記述を含めることができます。ただし、自動生成する WSDL 文書の中では SOAP ベースのサービスのみが記述されます。

ハンドラ グループとして WSDL 文書を作成する手順は次のとおりです。

1. ルーティング ブラウザ上で、発注サービスを要求するハンドラ グループの横にある **[generate WSDL]** リンクをクリックします。

   ブラウザのウィンドウに WSDL 文書が表示されます。

2. ブラウザの [Back] ボタンをクリックして、ルーティング ブラウザに戻ります。

3. ハンドラ グループとして WDSL 文書が生成されたあと、ルーティング ブラウザで **[generate WSDL]** リンクを右クリックし、メニューから **[Save Target As]** を選択すると、この WSDL ファイルをファイルシステムに保存できます。

   新規のサービス定義では、ポリシーを導入するか、上述のように WSDL 文書を手作業で作成しないかぎり、WSDL 文書を利用できません。

パートナーや顧客が WSDL 文書を利用できるように、制限付きの公開（ACE XML Gateway のサービス ディレクトリを利用）、または一般公開（ACE XML Gateway を通過して到達できる URL）が可能です。一般公開の場合、特定のハンドラ グループに対応する WSDL 文書は次のパスで公開できます。

`http://<gateway_hostname>:<port>/<service_path>?WSDL`

複数の WSDL 文書を 1 つの URL で公開するには、**System Management** > **Gateway Settings** ページで **[WSDL Publishing]** を設定します。特に、オプション **[Serve WSDL Files from the Gateway]** は有効にしてください。

次回以降のポリシー導入では、ACE XML Gateway が毎回自動的に、ポリシー内のすべてのハンドラ グループに対応する WSDL 文書を一般からアクセス可能な URL に公開します。

イベント ログとメッセージ ログの利用

ACE XML Gateway は、サービス指向環境におけるアクティビティの分析と監視を行うための幅広いツールと機能を提供します。これらのツールは ACE XML Gateway が行うアクティビティの管理とトラブルシューティングができるほか、ACE XML Gateway 外部のアクティビティのトラブルシューティングにも役立ちます。ACE XML Gateway のメッセージとイベント ログは、サービスのエンドポイント間での互換性問題やアプリケーション エラーの原因を特定する際にも非常に役立ちます。

次に、ACE XML Manager が提供するログ作成ツールを紹介します。

メッセージ トラフィックのログ情報の表示

「WSDL 文書のインポートによる Web サービスの定義」では、送受信するメッセージのログを記録させるために、`retrieveQuote` サービス プロキシに対してデフォルトのログ作成レベルを設定しました。このサービスへ「XML Gateway へのトラフィック送信」で説明したテストを実施すると、そのログの内容を表示させることができます。

ログを表示する手順は次のとおりです。

1. 操作メニューで **[Message Traffic Log]** リンクをクリックします。

図 11-1　メッセージ トラフィック ログへのリンク

このメッセージ トラフィックのログが表示されます。ログはメッセージを要求 / 応答の対で記録することに注意してください。

View カラムの下の **[events]** リンクをクリックするとそのメッセージ イベントに関する概要が表示されますが、ここではメッセージ本文を見ることにします。

2. View カラムにある **[req/resp pair]** リンクをクリックします。

図 11-2　イベントの表示

メッセージ交換一対についての情報を記載する新しいウィンドウが表示されます（受信要求、送信要求、受信応答、送信応答）。

3. このページの **Outgoing Response Attributes** エリアに向かって下方向へスクロールし、**Body** ラベルの隣のリンク、**[text/xml]** をクリックします。

メッセージの内容が表示されます。

図 11-3　送信応答のメッセージ本文

このウィンドウは送信応答メッセージの全テキストを表示しています。同様に、送信要求として送信されたメッセージや、受信した応答などのテキストも表示させることができます。

メッセージの仕様に複雑な設定を適用する際は、XML Gatesay を通過する 4 つの形式でメッセージを表示させると、メッセージへの設定の結果がわかりやすくなります。

ログの各種レベルについての理解

これまでの手順は、メッセージ トラフィック ログの中のメッセージ テキストを表示する方法でした。メッセージ ログはシステム導入の際に、メッセージ処理コンポーネントの理解とトラブルシューティングに役立ちます。

イベント ログはメッセージ処理について詳しい情報を提供します。その他にも、ポリシー変更をはじめ、ACE XML Gateway と ACE XML Manager のステート変化（再起動イベントなど）、保護されたサービスにより返されたアプリケーションの失敗、その他の種類のイベントといった、システムの他のアクティビティに関する情報も表示します。

図 11-4　イベント ログのテスト トランザクション

ログ上のすべてのイベントはログ レベルに関連付けられています。たとえば、さきほど実行したサービス テストから生じたアクセス イベントは、通知レベルでイベント ログに記録されていますが、これは記述カテゴリ *N* として示されています。

重大度には 6 つのレベルが設けられており、これを表 11-1 に示します。

表 11-1　ログの重大度レベル

名称	説明
アラート	システムが極めて危険な状態にあり、システム障害を防ぐために早急な対応が必要。
エラー	エラー状態にあり、システムが不適切な動作につながる可能性がある。
警告	エラー状態にあり、システムの予期しない動作につながる可能性がある（バックエンドの HTTP 応答コードが 500、XML Manager によるログインが失敗、メッセージの有効性チェックで失敗など）。

表 11-1　ログの重大度レベル（続き）

名称	説明
通知	正常だが、注意すべき状態（要求と応答が ACE XML Gateway を通過可能、要求メッセージがハンドラに合致しない、ユーザが XML Manager へのログインに成功など）。
情報	参考情報としてのメッセージ。メッセージの処理に重要な手順がある。
デバッグ	詳細情報のログ レベル。イベントに関して、システムの開発やトラブルシューティングの際に有用なレポートを含む。

システムは XML Manager で選択したログ レベルを反映するイベントのみを表示します。デフォルトでは通知レベルまたはそれ以上のレベルに設定されています。テストを行うためにデバッグまたはそれ以上のレベルに設定する必要のある可能性もあります。運用のための導入またはパフォーマンスのテストには、ログ レベルを通知またはそれ以上に設定することを推奨します。作成するログが詳細になると、システム パフォーマンスの低下が予想されます。

ログ レベルは System Management ページで変更できます。ログ レベルは、XML Manager と XML Gateway それぞれのアクティビティに対して別々に設定できます。XML Manager のイベントはシステム上の管理的アクティビティに集中しています。XML Gateway のイベントはトラフィック処理についての情報を詳細に提供します。ポリシーの作成とデバッグを目的とする場合、XML Gateway のログをデバッグ レベルに設定すると効果的です。

第 3 部　XML Gateway のセキュリティ機能

第 3 部では、WSDL 文書のインポートから得たポリシー設定に手を加える方法を説明します。システムのセキュリティ機能とメッセージ検証機能のセットアップ手順を見ることができます。

内容は次のとおりです。

- サービスへのアクセス コントロール
- SSL によるトラフィックの保護
- メッセージの検証
- コンテンツ スクリーニング ルールの利用
- 攻撃の防止
- XML コンテンツの暗号化と復号
- デジタル署名の作成と照合

サービスへのアクセス コントロール

ACE XML Gateway はサービスを保護するために、そのサービス要求に対してアクセス コントロールによる制限を適用します。ACE XML Gateway は、次のように、受信要求に組み込まれた幅広い種類の証明情報を評価できます。

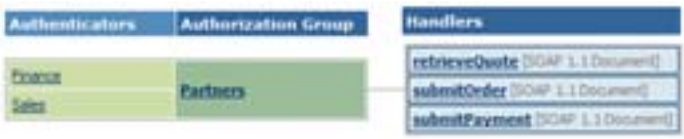
- 電子証明書
- Basic 認証 HTTP ヘッダ
- WSS UsernameToken
- WSS Password Digest
- XPath 表記法によりメッセージ内の場所を記されたユーザ名 / パスワードの組み合わせ
- Netegrity トークン
- SAML トークン
- IP アドレス
- 時刻

パスワード ベースの証明情報は ACE XML Gateway のポリシーが持つデータと照合するか、Netegrity SiteMinder、LDAP、Active Directory、あるいは何らかの SOAP サービスなどの外部の仕組みにより確認できます。

サービスへのアクセス条件は、オーセンティケータと呼ぶポリシー オブジェクトを使って定義します。要求がオーセンティケータにより許可されるには、オーセンティケータに格納されているすべての条件を満たさなければなりません。

1 つのオーセンティケータは、1 つの認証グループを介して 1 つのサービス プロキシに関連付けられます。認証グループは 1 つまたは複数のオーセンティケータを 1 つまたは複数のサービス定義に結び付けます（図 13-1 を参照）。

図 13-1　アクセス コントロール ポリシーの構成要素



1 つのサービスに関連付けられた複数のオーセンティケータが存在する場合は、要求がそのうちの 1 つに合致すればサービスにアクセスすることができます。ACE XML Gateway は証明情報の評価にいくつかの最適化手法を用います。1 つのサービスに関連付けられた複数のオーセンティケータが存在する場合、要求の評価は複雑な条件（暗号化など）のオーセンティケータよりも先に、すぐに確認できる条件（IP アドレスの規制など）のオーセンティケータを評価します。

もうひとつの最適化手法として、いったん要求がオーセンティケータに受け入れられると、ACE XML Gateway は他のオーセンティケータの条件を無視します。その結果として、イベント ログには実際にその要求を受け入れたオーセンティケータのみが表示されることに注意してください。受け入れる可能性のあったすべてのオーセンティケータが表示されるわけではありません。

IP アドレスによるアクセス コントロール

「サービスの仮想化」（p.19）でサービス プロキシを作成したあと、このマニュアルの手順どおりに実行している場合は、`retrieveQuote` サービス プロキシを *public* に設定しているはずです。このレベルでは、ACE XML Gateway が、受信要求をいずれかのサービス プロキシと一度一致すると、以降の証明確認は行いません。実際の導入では、ほとんどのサービスにおいて何らかの方法でアクセスを規制することになるでしょう。

次の手順では、ユーザの IP アドレスに基づいてオーセンティケータをセットアップし、それをサービス プロキシに関連付ける方法を説明します。

1. 操作メニューで **[Access Control Browser]** をクリックします。

   `retrieveQuote` サービスが Public の一覧表に表示されていることに注意してください。
2. **[Add an Authenticator]** ボタンをクリックします。
3. オーセンティケータの **Edit General Information** ページでオーセンティケータの名前を入力してください（`BeaglePartners` など）。
4. **[Authorization Group]** には、`Partners` など、新しい認証グループの名前を入力します（ドロップダウン メニューで **[Create in new authorization group named]** が選択されている必要があります）。
5. **[Create]** をクリックします。

   そのオーセンティケータの証明ページが表示されます。
6. **[Add Credential]** メニューに `[IP Address]` が選択された状態で **[Add]** をクリックします。
7. **[IP Address]** ページで、許容する IP アドレスの範囲を先頭と末尾の入力欄に入力します。

   ACE XML Gateway が認証されないクライアントを適切に遮断するかどうかを確認するため、まず最初にテスト要求を発行しようとしているコンピュータのアドレスを含まない範囲を入力します。
8. **[Save Changes]** をクリックします。

再び表示されたオーセンティケータのページには、REQUIRED CREDENTIALS（必要な証明情報）の下に IP アドレス要件が記載されています。

図 13-2　IP アドレスの要件

ここで、ハンドラを認証グループに関連付けるため、次の手順を行います。

1. オーセンティケータ ページ最下部にある **[Exit to Access Browser]** ボタンをクリックして、アクセス コントロールのブラウザに戻ります。

   オーセンティケータのほかに、さきほど作成した認証グループが表示されることに注意してください。

2. `retrieveQuote` サービス プロキシの名前をクリックします。この名前は Public 一覧表に記載されているはずです。

3. サービス プロキシのアクセス コントロール ページで、**[Access is restricted to the following authorization groups]** と記されたオプション ボタンをクリックします。

4. さきほど作成した認証グループ、Partners の横のチェックボックスをクリックします。

5. **[Save Changes]** をクリックします。

   アクセス　コントロール　ブラウザが再び表示されます。今回は `retrieveQuote` サービス プロキシに結びつけて作成した認証グループが記載されています。

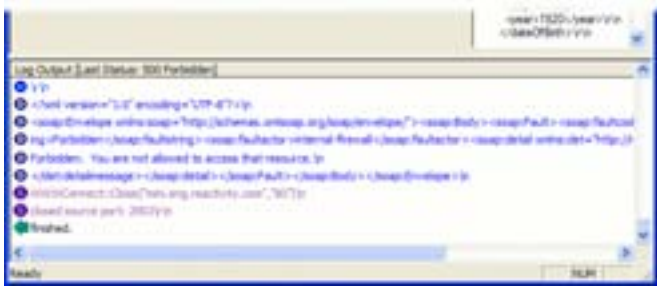
図 13-3　認証グループを与えられたサービス プロキシ

6. この変更を有効にするためにポリシーの導入を行います。

ポリシーの導入が終了したら、「XML Gateway へのトラフィック送信」で説明したようにテスト要求を発行します。

オーセンティケータに入力した IP アドレスの範囲外の IP アドレスを持つクライアントからテストを実行すると、図 13-4 に示すように、XML Gateway は「Forbidden」応答を返します。

図 13-4　不適格なアクセスへの応答



イベント ログがアクセス遮断のイベントをどのように記録しているかを確認するには、操作メニューの **[Event Log]** リンクをクリックします。

遮断されたアクセス試行がイベント ログの警告レベルで記録されていることに注意してください（次の図を参照）。

図 13-5　遮断アクセスのイベントを記録したログ

ユーザ名 / パスワードの認証によるアクセス コントロール

ACE XML Gateway は、パスワード ベースの柔軟な認証を行います。認証は、XML Gateway または LDAP ディレクトリなどの外部システムに保存したデータと照合することで有効になります。

次に、受信要求内のベーシック認証 HTTP ヘッダに対するパスワード チェックをセットアップ手順について説明します。

1. まだ開いていない場合は、操作メニューの **[Access Control Browser]** リンクをクリックします。

   前回作成した認証グループにもう 1 つの認証手順を加えることにします。
2. **[Add an Authenticator]** ボタンをクリックします。
3. **[Authenticator Name]** 欄に、このオーセンティケータの名前を入力します（Beagle Basic Auth など）。
4. **[Authorization Group]** メニューで、初めに作成した認証グループの名前、Partners を選択します。
5. **[Create]** をクリックします。

   オーセンティケータの証明情報ページが表示されます。
6. **[Add Credential]** メニューから **[HTTP(S) Basic Authentication]** を選択し、**[Add]** をクリックします。
7. **[HTTP(S) Basic Authentication]** ページで **[Verify Using]** メニューのデフォルトの選択肢 **[Fixed Values]** をそのまま維持します。

   このメニューのその他のオプションに、パスワードファイル認証（ユーザ名 / パスワードの組み合わせを持つ .htaccess 形式のファイル）と様々な LDAP 認証方式が含まれていることに注意してください。
8. このオーセンティケータが受け入れるユーザ名を **[Username]** 欄に入力します。
9. [Password] 欄には、受け入れるパスワードを入力します。
10. **[Save Changes]** をクリックします。

    Reqiured Credentials の下に **[HTTP(S) Basic Authentication]** という要件を記載するオーセンティケータ ページが表示されます。

    Identity Reporting 機能を利用すると、ユーザごとのサービス アクティビティを表示できます。新規オーセンティケータに対して Identity Reporting 機能を有効にします。
11. オーセンティケータ ページにある **Identity Reporting** ヘッダの横の **[Edit]** をクリックします。
12. **[Enable Identity Reporting]** チェックボックスをクリックします。
13. **[HTTP Basic Auth Username]** の横のチェックボックスを有効にします。これは、さきほど作成した認証要件の種別名です。
14. **[Save Changes]** をクリックします。

オーセンティケータ ページが再表示されます。**[Exit to Access Browser]** をクリックし、アクセス ブラウザで新しい設定の効果を確認します。

図 13-6　認証グループを与えられたサービス プロキシ

ユーザは 2 つのオーセンティケータで定義されている条件の *いずれか*に合致すれば retrieveQuote サービスにアクセスできることに注意してください（さきほど設定したパスワード要件、または IP アドレス要件）。IP アドレス要件を持つ BeaglePartners オーセンティケータにパスワード要件を加えると、ユーザがサービスにアクセスするには両方の条件を満たさなければなりません。

パスワード要件を適切にテストするには、テスト対象のホストを遮断するように IP アドレス要件を設定（またはそのポリシーからオーセンティケータを削除）する必要があります。

設定を最後まで完了させるためにポリシーを導入したあと、新しい認証要件をテストします。

前回と同様に、XML Gateway の retrieveQuote サービスに送信する要求を WFetch で用意します。ただし、認証用の証明情報には **Auth** 方式として **[Basic]** を選択し、**[User]** 欄および **[Passwd]** 欄には、オーセンティケータに入力したユーザ名とパスワードを入力します。

図 13-7　WFetch でベーシック認証の要求を設定

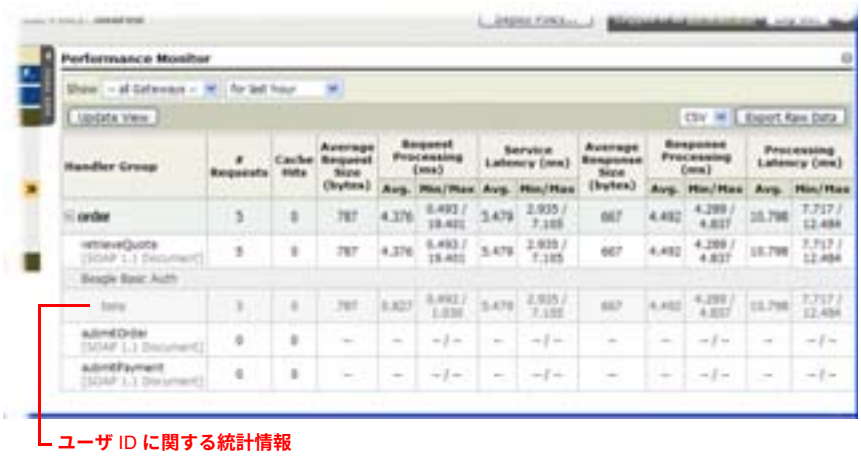
[Go!] をクリックします。これからサービスに対するパフォーマンス データの確認を行います。そのため、正常終了の応答を 1 回受け取ったあと、この要求を何回か繰り返して実行し、パフォーマンス データを蓄積してください。

これで、さきほど設定したユーザ証明に対するサービス アクティビティを参照できます。

1. XML Manager の Web コンソールで、操作メニューにある **[Performance Monitor]** をクリックします。
2. retrieveQuote サービスに対応するハンドラ グループの名前 order の横のエキスパンド コントロールをクリックします。

このサービス オペレーション全体についての合計値とともに、さきほど作成したユーザ ID に関する統計情報が表示されていることに注意してください。

図 13-8　パフォーマンス モニタに表示されたユーザのアクティビティ



この例では、オーセンティケータで認証するよう設定されている ID は 1 つだけです。オーセンティケータがパスワード ファイルや LDAP ディレクトリと突き合せてパスワードを確認するように設定されている場合、証明元に属する有効なアカウントからの要求は ID の数だけモニタに表示されます。

パフォーマンス モニタにおける統計情報の各項目についての詳細は、このページから呼び出すオンライン ヘルプで参照してください。

SSL によるトラフィックの保護

ACE XML Gateway は SSL/TLS を使用してユーザにセキュリティを保証するとともに、Gateway とバックエンド サービスの間のトラフィックを保護します。ここでは、ACE XML Gateway とユーザの間で SSL/TLS をセットアップする方法を説明します。

注： このマニュアルでは、以下 SSL/TLS を SSL と省略表記します。厳密にはバージョン 3.0 以下が SSL、バージョン 3.1 が TLS になります。

SSL の仕様では、SSL ハンドシェイクの一部として X.509 証明書の呈示がサーバに要求されます。多くの場合、呈示された証明書が一定の条件に合致しないと、クライアントは SSL ハンドシェイクを中断して通信を中止します。

接続を中断する条件はクライアントにより異なりますが、一般的には SSL 接続を確立するために ACE XML Gateway が呈示する証明書には、次の属性が必要です。

- 証明書が有効なこと（現在の日付が有効な「開始日」と「終了日」の間でなければならない）
- 「サーバ認証」用の拡張鍵があること
- ゲートウェイの DN には、サーバの IP アドレスに名前解決するホスト名と等しい CN があること
- クライアントはサーバ証明書の発行元 CA（認証局）を信頼するように設定されていること。また、サーバ証明書は CA の CRL（失効証明書リスト）に記載されていないこと

このシステムの実装では、ほとんどの場合、これらの要求に合致する CA 署名付きサーバ証明書の要求を組み込み、導入の際にはそれぞれの XML Gateway に証明書をインストールすることになります。

XML Manager コンソールには、証明書への署名要求を生成し、署名された証明書をアップロードするツールが備わっています。ただし、以降の説明では、ACE XML Gateway のサンプル リソース Web サイトから入手できるサンプルの証明書を使うことにします。

SSL 証明書による認証について

ACE XML Gateway はクライアントの証明書を確認しなくてもクライアントとの間で SSL セッションを確立できますが、たいていの場合、SSL ではクライアントの証明書の確認を行います。

ACE XML Gateway は、クライアント認証のために呈示された証明書を複数の方法で確認できます。最も単純な方法はサムプリントの合致によるものです。この方法では、ユーザから呈示された証明書と、ID 認証要件として設定されているものを ACE XML Gateway が比較します。サムプリントが合致すると、そのユーザが適格であると見なされます。

ACE XML Gateway は、クライアントの証明書を発行した認証局に基づいてユーザを認証することもできます。

ここでは、サムプリント照合による認証方法を説明します。この方法では、最初にその証明書の証明情報を定義する新しいオーセンティケータを作成します。次に、保護されたポートを待ち受けるハンドラをセットアップします。

必要な準備

評価用として利用できる証明書を持っていない場合は、次のリソース サンプル ページから証明書を入手できます。

http://example.reactivity.com/security.html

始める前に、Oak サーバ（このページの最下部）の 1 つで用いるサーバ用証明書を PKCS #12 形式でダウンロードします（次に行う手順では、Oak Server 証明書のうちの最初の P12 形式証明書、`maple.p12` を使用します）。PKCS #12 形式ファイルはパスワードで保護されていることがよくあります。このサンプルの証明書はパスワード `swordfish` で保護されています。

また、Oak セキュリティ チームの架空ビジネス パートナー（Beagle Partners, Inc. など）から PEM 形式のクライアント証明書と P12 形式の公開鍵 / 秘密鍵ペアも入手する必要があります。これにはサンプルの Web ページを使います。

XML Gateway の HTTPS ポートを開く

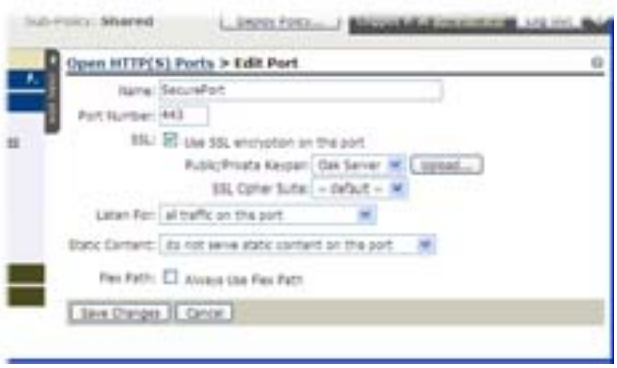
最初に ACE XML Gateway にリスニング ポートを開きます。このポートに SSL の使用を設定します。

1. 操作メニューで **[Open HTTP(S) Ports]** リンクをクリックします。
2. **Open HTTP(S) Ports** ページで **[Add a New Port]** ボタンをクリックします。
3. ポートの名前を入力します（`SecurePort` など）。この名前はリスニング ポートを識別するためのもので、この XML Manager でのみ使用されます。
4. **[Port Number]** として 443 と入力します。これは SSL 用として慣例となっている番号です。
5. **[SSL]** チェック ボックスを選択します。
6. **Public/Private Keypairs** ラベルの横に「public/private keypairs have been uploaded」というメッセージが表示されるはずです。このメッセージの横の **[Upload]** ボタンをクリックします。
7. [Upload Resorce] ウィンドウにリソースの名前を入力します（`Oak Server` など）。

8. **[Browse]** ボタンをクリックし、サンプルページ `maple.p12` からダウンロードした Oak サーバの P12 ファイルをファイル選択ダイアログで探します。
9. **[Password]** 欄に `swordfish` と入力します。
10. **[Public/Private Keypairs]** 欄の中の P12 ファイルに対して **[Upload]** をクリックします。

    次のような **Edit Port** ページが表示されます。

図 14-1　Edit Port ページ



11. **[Save Changes]** をクリックします。

このポート リストの中に新しいポートが現れます。

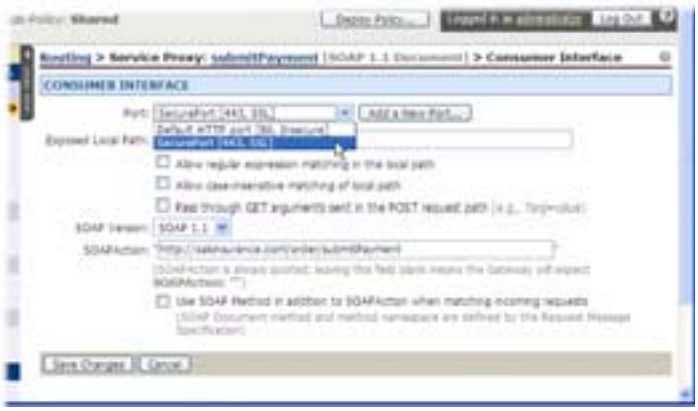
利用ポートの保護をサービス プロキシに設定

保護されたポートを利用するために、サービス プロキシを次のように設定します。

1. 操作メニューで **[Routing Browser]** リンクをクリックします。
2. `submitPayment` というサービス プロキシの名前をクリックします。

   `submitPayment` に対応した情報ページが表示されます。
3. **Consumer Interface** という見出しの横の **[Edit]** リンクをクリックします。
4. 作成した新しいポート SecurePort を **[Port]** ドロップダウン メニューから選択します。

図 14-2　ユーザ向けポートを変更する



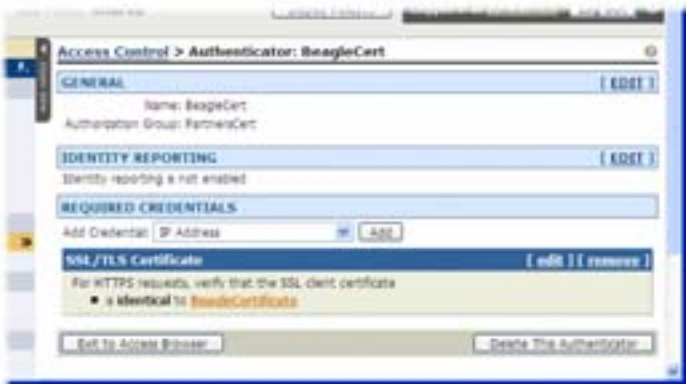
5. **[Save Changes]** をクリックします。

証明書のアクセス要件の作成

次の手順で新しいオーセンティケータを作成します。

1. 操作メニューで **[Access Control Browser]** をクリックします。
2. アクセス コントロール ブラウザで **[Add an Authenticator]** をクリックします。
3. オーセンティケータに名前をつけ（BeagleCert など）、新しい認証グループ PartnersCert に加えます。
4. **[Create]** をクリックします。
5. **Add Credential** メニューから **[SSL/TLS Certificate]** という項目を選択し、**[Add]** をクリックします。
6. **SSL/TLS Certificate** ページで、デフォルトの認証方法 **[SSL Certificate Fingerprint]** が選択された状態のまま、**[Upload]** をクリックして ACE XML Gateway に証明書ファイルをアップロードします。
7. **Upload Consumer Certificate Resource** ウィンドウで **[Resource Name]** 欄に名前を入力します（BeagleCert など）。ポリシー内の証明書をこの名前で識別します。
8. **[Local File]** 欄の横の **[Browse]** ボタンをクリックし、サンプルのセキュリティ リソース ページ `beagle.pem` からダウンロードした証明書ファイルを探します。
9. **[Local File]** 欄に証明書ファイルへのパスが入力された状態で **[Upload]** をクリックします。
10. **[Save Changes]** をクリックします。新しい証明書要件が証明情報リストに現れます。

図 14-3　証明情報リスト



11. **[Exit to Access Browser]** ボタンをクリックします。
12. アクセス コントロール ブラウザで Public 一覧表の右側の SubmitPayment サービス プロキシをクリックします。
13. Access Control for the Service Proxy ページで **[Access is restricted to the following authorization groups]** を選択し、さきほど作成したグループのチェックボックスを選択します。
14. **[Save Changes]** をクリックしてからこのポリシーを導入します。

それでは、このサービス プロキシへの要求を発行してみます。次に、要求とともに Beagle クライアントの証明書を渡す方法を説明します。

証明書アクセス要件のテスト

WFetch で要求の中の証明書を渡すには、最初に証明書を Internet Explorer にアップロードする必要があります（WFetch は要求だけでなく、IE の中にある証明書を渡すことができます）。証明書を Internet Explorer 6.0 にインポートする方法を次に説明します。別の方法として、Curl という HTTP クライアントのコマンド ライン ツールを使用して証明書の受け取りをテストできます。

必要であれば、次の URL から Beagle パートナーの P12 証明書 / 鍵ペアをサンプル ページからダウンロードしてください（まだ行っていない場合）。

http://example.reactivity.com/security.html

証明書をダウンロードしたら、次の手順に従ってください。

1. Internet Explorer で **[Tools > Internet Options]** をクリックします。
2. **[Content]** タブを選択してから **[Certificates]** ボタンをクリックします。
3. **[Import]** ボタンをクリックし、Certificate Import ウィザードを使用して `beagle.p12` ファイルを Internet Explorer にインポートします。
4. 要求された場合はそのファイルのパスワード swordfish を入力します。

要求を発行する前に、WFetch で次の変更を行います。

- **[Port]** として 443 を選択します。
- **[Connect]** 欄では `[https]` を選択します。
- **[cipher]** オプションは `[default]` のまま残します。
- Client cert には `[** cert from IE **]` を選択します。Internet Explorer に複数の証明書が存在する場合は、さきほどアップロードした証明書を選択してください。
- **[Headers and Body]** 欄に次のテキストをペーストしてください。

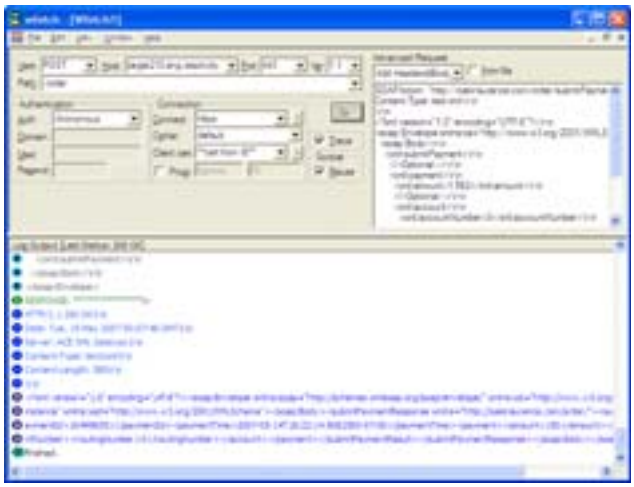
出力例 14-1　SubmitPayment 要求

```
SOAPAction: "http://oakinsurance.com/order/submitPayment"

<?xml version="1.0" encoding="utf-8"?>
 <soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
   <submitPayment xmlns="http://oakinsurance.com/order/">
   <payment>
    <amount>246.46</amount>
    <account>
      <accountNumber>123456</accountNumber>
      <routingNumber>789123</routingNumber>
    </account>
   </payment>
  </submitPayment>
 </soap:Body>
</soap:Envelope>
```

[Go!] をクリックすると、次のような応答が返ってきます。

図 14-4　証明書の設定を行った WFetch



Curl から送る要求に証明書を組み入れる

Curl を利用すると、次のコマンドでテスト メッセージを発行できます（コマンドライン上で一度にコマンド全体を入力する必要があります）。

```
curl -E beagle.pem:swordfish -k -v
  -H 'Content-Type: text/xml' -H
'SOAPAction: "http://oakinsurance.com/order/submitPayment"'
    --data-binary @- https://10.0.101.73/order
    < payment.xml
```

コマンドの中には Beagle の証明書である beagle.pem（この例では）とともにパスワードも含めることに注意してください。また、`payment.xml` には、サービスに渡す本文のコンテンツを含めなければなりません。コンテンツは次のようになります。

出力例 14-2　payment.xml のコンテンツ

```
<?xml version="1.0" encoding="utf-8"?>
 <soap:Envelope
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:xsd="http://www.w3.org/2001/XMLSchema"
xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
  <soap:Body>
   <submitPayment xmlns="http://oakinsurance.com/order/">
   <payment>
    <amount>246.46</amount>
    <account>
      <accountNumber>123456</accountNumber>
      <routingNumber>789123</routingNumber>
    </account>
   </payment>
  </submitPayment>
 </soap:Body>
</soap:Envelope>
```

メッセージの検証

メッセージの検証を ACE XML Gateway が行うことにより、無効な要求に対処する負荷がバックエンド リソースからなくなります。

ACE XML Gateway が行うメッセージの検証には次の種類があります。

- メッセージが XML スキーマまたは DTD に適合しているかの確認
- 形式的に適切な XML であるかどうかの確認（スキーマまたは DTD との照合確認は行わない）
- パラメータの存在と値の確認

メッセージが無効であると判断されると、ACE XML Gateway はこのイベントをログに記録し、選択されている場合は通知を送信します。

この章では、XSD と変数の検証によるメッセージ検証をセットアップする方法を説明します。詳細な情報が必要な場合は『*Cisco ACE XML ゲートウェイ User's Guide*』を参照してください。

メッセージ本文の検証

この章では、受信 SOAP 要求を XML スキーマに照合して検証する手順を説明します。スキーマによる検証は、ACE XML Gateway がメッセージに適用する処理タスクより前に行われます。

XML スキーマによる検証は次の手順でセットアップします。

1. 要求の検証を設定したいサービス　プロキシに対応する情報ページにアクセスします。
2. サービス プロキシの情報ページで、**Request Message Specification** の横の **[edit]** リンクをクリックします。

図 15-1　要求検証ページにアクセス

SOAP サービスに対しては、**[SOAP Message Validation]** オプションが表示されます。

3. XML スキーマでメッセージを検証するには、2 番めのオプション、**Content: require SOAP message validation with the specified XML schemas; reject invalid message** を選択します。
4. メッセージが Document-style SOAP の場合は、XML Manager が WSDL ファイルから XML スキーマ ファイルを抽出済みなので、手作業でスキーマをアップロードする必要はありません。

   サービスが Document-style SOAP のサービスではないが、XML コンテンツを処理するよう設定されている場合は、必要な XML スキーマ ファイルが XML Manager に保存されていない可能性が高くなります。**[Upload...]** ボタンをクリックして、XML スキーマを選択して読み込みます。
5. **[Save Changes]** をクリックします。

サービス プロキシ情報ページでは、要求メッセージの **XML schema-based content validation** に対する指定が SOAP Message Validation になっているはずです。

このポリシーを導入すれば、検証で無効とされたメッセージが遮断されます。スキーマによる検証をテストするには、オーダー要求の本文に対して、元のサンプル要求に含まれていないエレメントを XML 形式を壊さないようにして追加します。そのあとで ACE XML Gateway に要求を送信します。ACE XML Gateway は `faultstring` が「Validation Error」となっている SOAP 形式のエラー応答を返します。

引数の検証

ACE XML Gateway は、SOAP や HTTP/GET などの引数をサポートするプロトコルに対して、メッセージ内に含まれている引数を検証できます。メッセージ本文の検証と同様ですが、引数を検証すると、バックエンドに届くメッセージは、処理を行うアプリケーションが理解できるものに限定されます。

パラメータは次のように設定できます。

- 必要であるかどうか
- その値に求められるタイプ
- 値としてのコンテンツ要件

プロトコルが引数をサポートするサービスについては、サービス プロキシ情報ページからパラメータ エディタが利用できます。

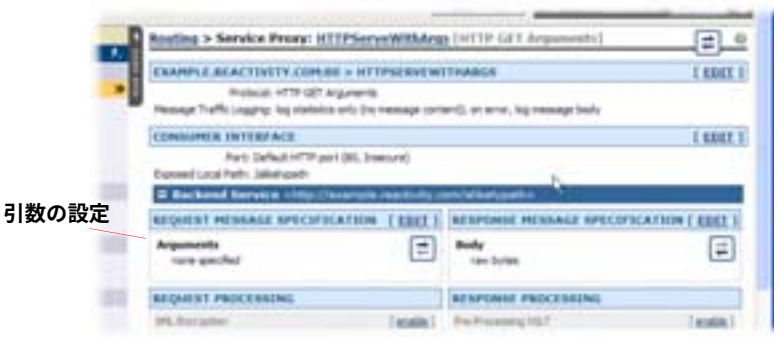
引数の要件を指定する手順は次のとおりです。

1. ルーティング ブラウザで引数の要件を設定したいサービス プロキシの名前をクリックします。

   サービス プロキシ情報のページが表示されます。

   サービスがパラメータをサポートする場合は、サービス プロキシ情報ページの **Request Message Specification** エリア、および **Response Message Specification** エリアに引数設定の表示が現れます。

図 15-2　サービス プロキシの引数への設定



2. **Request Message Specification** の横の **[Edit]** リンクをクリックします。
3. **[Add a New Row]** ボタンをクリックします。
4. **[Name]** 欄に、メッセージの中で確認できるパラメータの名前を入力します。
5. **Request Message Specification** ページの他のコントロールを使用して、必要な引数かどうか、そのタイプ、コンテンツまたはそのタイプを検証するかどうか、あるいはその両方を検証するかどうかを指定します。XML タイプのパラメータには、パラメータを検証する XML スキーマまたは DTD を追加指定できます。

   たとえば、要求に含まれていない可能性があるが、もし存在した場合にスキーマ検証により確認したい引数を追加する場合には、**[Req.]** チェックボックスを選択しない状態で残してもかまいません。
6. 確認を行いたいパラメータそれぞれに新しい行を追加します。
7. 終了後に **[Save Changes]** をクリックし、そのポリシーを導入して変更を有効にします。

ACE XML Gateway は、指定された引数が目的のサービスに届いたメッセージ内にあることを確認します。

コンテンツ スクリーニング ルールの利用

ACE XML Gateway は、メッセージの XML コンテンツに埋め込まれた特定の脅威を検出して遮断することができます。このような脅威の例としては、SQL 挿入攻撃があります。SQL 挿入攻撃では XML データに SQL コマンドを埋め込み、データベース攻撃の SQL コマンドをバックエンド サーバに実行させようとします。

このようなコンテンツを利用した脅威は、コンテンツ スクリーニング ルールで防ぐことができます。ACE XML Gateway には、あらかじめ定義されたスクリーニング ルールが多数用意されており、既知の脅威の多くに対処できます。また、自由にコンテンツ スクリーニング ルールを追加することができます。

コンテンツ スクリーニング ルールは有効化と無効化が可能なほか、**Content Screening Default** ページから新しいルールを作成できます。**Content Screening Default** ページはコンテンツ スクリーニング ルールの状況と、それぞれにおけるルール詳細を表示します。その例を次に示します。

- ルールを構成する表現形式
- ルールに合致すると自動生成されるログ イベント
- ルールのテキストが大文字小文字を区別するかどうか

コンテンツ スクリーニング ルールの有効化

コンテンツ スクリーニング ルールを有効化または無効化する手順は次のとおりです。

1. 操作メニューで **[Content Screening Defaults]** リンクをクリックします。
2. 特定のスクリーニング ルールに対して、**[disable]** から **[enable]** へ適用設定を変更します。このデフォルトのスクリーニング ルールは、特定のハンドラの設定で指定しないかぎり、すべてのハンドラに適用されます。
3. **[Save Change to Default Setting]** をクリックします。

グローバルなステータス設定では、サービス プロキシが特定のルールを上書きすることに注意してください（有効または無効）。サービス プロキシの特定のルール設定は、サービス プロキシ情報ページの **Content Screening** 設定エリアからアクセスできます。

コンテンツ スクリーニングのテスト

ACE XML Gateway にメッセージを送信して、コンテンツ スクリーニングをテストできます。たとえば、初めに作成した `retrieveQuote` ハンドラにスクリーニングを起動する手順は次のとおりです。

1. 操作メニューで **[Content Screening Defaults]** 項目をクリックします。
2. SQL Commands (v. 2) と記されたコンテンツ スクリーニングを有効化します。
3. **[Save Changes to Default Settings]** をクリックしてから導入します。

ここで、以下の要求を retrieveQuote サービスへ送信します。

出力例 16-1　SOAP メッセージ

```
<?xml version="1.0" encoding="utf-8"?>
 <soap:Envelope
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
 <soap:Body>
  <retrieveQuote xmlns="http://oakinsurance.com/order/">
    <policy>
      <dateOfBirth>
        <month>January</month>
        <day>DROP TABLE</day>
        <year>1960</year>
      </dateOfBirth>
      <zipCode>94002</zipCode>
      <height>52</height>
      <weight>150</weight>
      <coverage>402</coverage>
    </policy>
  </retrieveQuote>
 </soap:Body>
</soap:Envelope>
```

このメッセージには SQL-injection 攻撃を示すコンテンツ、DROP TABLE が含まれています。このメッセージは ACE XML Gateway に提示されると遮断されます。

遮断イベントにより生成されたログ エントリは、メッセージに埋め込まれた SQL コマンドを ACE XML Gateway が検出したことを示していることに注意してください。

図 16-1　遮断されたコンテンツのログ エントリ

コンテンツ スクリーニング ルールの作成

定義済みのコンテンツ スクリーニング ルールは、自分で作成したカスタム コンテンツ スクリーニング ルールで補うことができます。ルールは正規表現ステートメントで記述します。

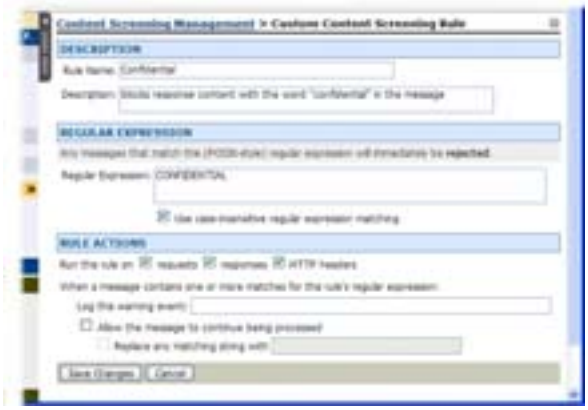
メッセージとステートメントを比較して合致した場合は、そのメッセージは遮断されます。

カスタム スクリーニング ルールを作成する手順は次のとおりです。

1. 操作メニューで **[Content Screening Defaults]** リンクをクリックします。
2. 画面に表示されていない場合は、**Custom Content Screening Rules** エリアが見えるまで下方向にスクロールします。
3. **[Define a New Rule]** をクリックします。
4. コンソールで識別できるようにルールに名前を付け、説明を加えます。
5. **[Regular Expression]** 欄に、スクリーニングしたいコンテンツに合致する正規表現を入力します。
6. **[Rule Actions]** 欄で、トラフィックにルールをどのように適用するかを指定できます。

   メッセージを遮断する代わりに、合致したコンテンツを指定文字列に置き換えて、メッセージを存続させることもできることに注意してください。送信メッセージでは便利な機能で、メッセージに含まれている機密情報やプライベート情報を隠すことができます。

図 16-2　コンテンツ スクリーニング ルールを設定した例



7. 終了したら **[Save Changes]** をクリックし、そのポリシーを導入して ACE XML Gateway でルールを実施させます。

攻撃の防止

ACE XML Gateway は、DoS 攻撃の疑いがある動きを検出します。特に Web サービスが受けやすい DoS 攻撃に属する XDos（XML Denial-of-Service）に有効です。

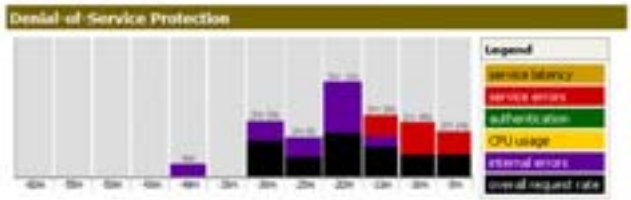
XDoS 攻撃はサービス プロバイダを悪用するために、XML メッセージの処理で発生するオーバーヘッドを利用しようとします。ACE XML Gateway はバックエンド インフラに対して障壁として機能し、DoS 攻撃が到達する前に阻止します。

XML Gateway アクティビティの表示

XDoS 攻撃が始まると、ACE XML Gateway はイベントのログを記録し、監視システムに通知します。そのほかに、そのトラフィックの出所となる IP アドレスから流れるトラフィックを一時的に遮断することもできます。

直前に検出された XDoS 攻撃を表示するには、Manager Dashboard を開きます。直前 1 時間の間に検出した XDoS 攻撃が **Denial-of-Service Protection** チャートに表示されます。

図 17-1　DoS 攻撃の防御



凡例で示されているように、このグラフは XDoS 攻撃の疑いのある動きを 6 種類の指標で情報提供します。

- **Service Latency（サービスの遅延）** — 許容範囲の遅延しきい値を超えるバックエンド サービスの遅延が繰り返し発生した場合に始動します（タイムアウトを含む）。
- **Service Errors（サービスのエラー）** — SOAP のエラーまたは HTTP 500 エラーなど、バックエンド サービスが異常な数のエラーを返したときに始動します。
- **Authentication（認証）** — 過剰な数の 401/403 エラーが返されたときに始動します（HTTP Unauthorized/Forbidden）。
- **CPU Usage（CPU 使用率）** — ACE XML Gateway で、メッセージの処理に極端な数値の CPU サイクルを必要としたときに始動します。たとえば 1 つのメッセージで検証する必要のあるシグニチャが何千もあるような場合です。

- **Service Errors（内部エラー）**— スキーマ検証エラー、悪意のあるコンテンツ、不正なデジタル署名などの、多数の内部エラーが検出されたときに始動します。
- **Overall request rate（総合要求レート）**— 受信要求の数が過度な場合に始動します。これは Web サイトやその他のネットワーク サーバに対する DoS 攻撃と類似した攻撃です。

DoS 攻撃検出しきい値の現在の設定は、**Denial-Of-Service Protection Settings** ページから確認、修正することができます。

DoS 攻撃防御の設定

DoS 攻撃を防御するためのトラフィックしきい値を変更する手順は次のとおりです。

1. 操作メニューの **Policy** セクションで **[Denial-of-Service Protection]** リンクをクリックします（**Global Security** サブヘッドの下）。
2. **Denial-Of-Service Protection Settings** ページで、DoS 攻撃の各カテゴリについて適切な設定変更を行います。
3. DoS 攻撃元と疑われる IP アドレスからのトラフィックを ACE XML Gateway に遮断させたい場合は、チェックボックス **[When an attack is detected, block the attacking IP address for at least 5 seconds]** をチェックしてください。
4. **[Save Changes]** をクリックしたあと、ポリシーを導入して ACE XML Gateway への変更を有効にします。

XML コンテンツの暗号化と復号

トランスポート層での暗号化を提供する SSL/TSL の暗号化とは異なり、XML での暗号化はメッセージ レベルで機能します。これにはいくつかの利点がありますが、そのひとつは、メッセージの特定の部分を暗号化できることです。この場合、メッセージのそれ以外の部分を人の読めるテキストのまま残すことができます。もうひとつの利点は、メッセージが宛先に到達したあとでも暗号化されたままであることです。こうすると、実際に必要になる時点まで保護しておくことができます。

送信 XML コンテンツの暗号化

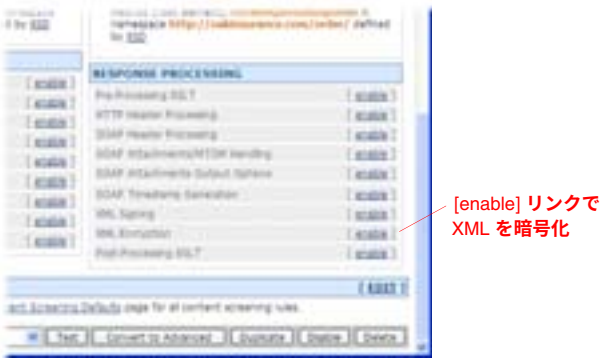
メッセージ コンテンツを暗号化するには、受信者の公開鍵を使用する必要があります（受信者がそのコンテンツを復号するには、対応する秘密鍵を必要とします）。

実際に XML 暗号化機能を利用するために最初に必要なことは、ユーザの証明書の読み込みです。ポリシーに入れるパートナーの公開鍵がこの証明書に含まれています。別の方法として、ACE XML Gateway は 受信要求の XML シグニチャに含まれている公開鍵でもメッセージを暗号化できます。この例では架空の Beagle Partners, Inc. の公開証明書を使用します。

メッセージの暗号化をセットアップする手順は次のとおりです。

1. ルーティング ブラウザで retrieveQuote サービス プロキシをクリックします。
2. **Response Message Specification** の下に見える **XML Encryption** の横の [enable] リンクをクリックします。

図 18-1　送信応答の暗号化



3. **XML Encryption** ページで **Transport with Public Key** の証明書リソース、beagle.cer を選択します。この証明書をまだアップロードしていない場合は、次の手順で行ってください。
   a. オプション メニューの横の **[Upload]** ボタンをクリックします。
   b. ポリシー内のリソースにつける名前を入力します。
   c. URL 欄には次の URL を入力してください。

      http://example.reactivity.com/pki/client/beagle.cer

   次のオプションの値はデフォルトのままでかまいません：**[For SOAP Role]**、**[Encryption Algorithm]**、**[Transport Cipher]**、**[Encryption Type]**

   実際には、要求を受け取るアプリケーションの都合により、これらのオプションをカスタマイズする必要があるかもしれません。
4. **[Element specified by these XPaths]** オプションを選択し、[XPath] 欄に次の値を入力します。

   ```
   //*[local-name()='price']
   ```

   応答メッセージのうち、`price` エレメントのみが暗号化されます。
5. **[Save Changes]** をクリックします。
6. retrieveQuote サービスにアクセス コントロールを設定している場合は、簡単にするため、この時点で公開アクセスにリセットします。それにより、イベント ログの中から暗号化に関連するイベントを見つけやすくなります。

   公開アクセスに設定するには、設定ページの最下部にある **[Edit Access Control]** リンクをクリックし、アクセス レベルとして **[Public]** を選択します。

   また、デフォルト（非暗号化ポート 80）設定に戻す必要があるかもしれません。ポートを変更するには、そのサービス プロキシに対するユーザ インターフェイスの設定を修正します。以前に説明した方法に従ってください。
7. 変更を保存したら、必ずポリシーを導入してください。

これで XML 暗号化のテストが可能になりました。

暗号化のテスト

メッセージの暗号化設定を終えたら、WFetch からサービスへメッセージを送信します。WFetch の設定は、再びデフォルトのポートと非同期認証を使用するように設定し直してください。次の例に類似したメッセージが応答として表示されます。

図 18-2　暗号化されている応答

この応答にはいくつか注意点があります。

- 暗号化されたデータを記述しているメッセージには WSSE セキュリティヘッダが追加されています。
- このヘッダに含まれているのは、暗号化された次のエレメントを識別する参照宣言です。
  `<DataReference URI="#RXFIDIXHYOTE"/>`
- 暗号化された `price` エレメントへの DataReference ポイント。暗号化されて次のように表示されます。

```
<EncryptedData
  Type="http://www.w3.org/2001/04/xmlenc#Element"
  Id="RXFIDIXHYOTE">
 <EncryptionMethod
    Algorithm="http://www.w3.org/2001/04/xmlenc#
      tripledes-cbc"/>
 <CipherData>
   <CipherValue>wuZ36uMfv7cqJvL2G/NI=</CipherValue>
 </CipherData>
</EncryptedData>
```

暗号化された応答に現れる設定オプションの結果に注意してください。インターフェイスにおける他のオプションについても自由にテストを行い、応答に現れる結果を確認してください。たとえば、**[Encrypt Element]** の選択肢として **[encrypt only the contents of the specified elements]** を試したり、XPath 行を設定に追加して、暗号化するエレメントを追加してください。

> **注：** メッセージの表示形式を改善するには、WFetch ではなく、メッセージ トラフィック ログのウィンドウで応答メッセージを開きます。

設定変更をテストすると、ACE XML Gateway により、複雑な技術が簡単に実行できます。XML 暗号化だけでなく、XML シグニチャ、SAML、UsernameToken など、他の Web Service 技術についても同様のことが言えます。

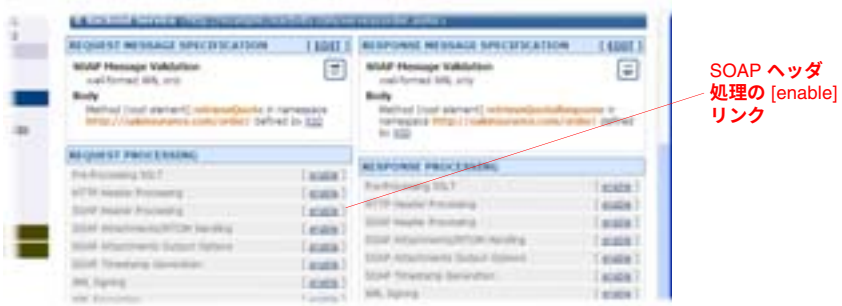
受信 XML コンテンツの復号

暗号化したコンテンツは、暗号化で使用した公開鍵に組み合わせる秘密鍵で復号する必要があります。これは、メッセージを送信した相手が ACE XML Gateway の公開鍵を持っていることが前提です。そのためコンテンツの復号設定では、復号に使用する鍵として ACE XML Gateway の秘密鍵を指定することになります。

サービス プロキシ上でメッセージ復号を設定する手順は次のとおりです。

1. ルーティング ブラウザ上で、暗号化したメッセージを発行するサービス プロキシをクリックします。
2. サービス プロキシ情報ページで、**Request Message Specification** 項目の **SOAP Header Processing** の横の **[enable]** リンクをクリックします。

図 18-3　受信要求の復号



3. 最初のチェックボックス **[Process header elements for SOAP Role]** にチェックを入れます。ドロップダウン メニューのオプションは `[no role]` のまま残します。

4. `WSS:XML Decryption` ヘッダの下にある **[Enable XML decryption using the selected keys]** にチェックを入れます。

   このオプションを有効化すると、暗号化された SOAP エレメントを ACE XML Gateway に復号できますが、リストに記載された鍵に限ります。

5. 復号に使用する秘密鍵を選択します（必要であれば **[Upload]** ボタンを利用して PKCS#12 形式の証明書 / 鍵ペアをアップロードできます）。

[Save Changes] を実行すると、設定の概要がサービス プロキシ情報ページの **Request Processing** エリアに表示されます。この変更を有効にするために必ずポリシー導入を行ってください。

デジタル署名の作成と照合

XML シグニチャを利用することにより、XML データの信頼性と完全性を保証することができます。つまり、データが特定の送信元から届き、シグニチャの生成以降に改変されていないことが保証できます。

ACE XML Gateway を利用すると、XML 暗号化のメッセージ処理への組み込みが簡単に行えます。送信メッセージの XML シグニチャの生成と、受信メッセージのシグニチャ確認をセットアップできます。

ACE XML Gateway は XML シグニチャを生成するために、秘密鍵を使用して指定コンテンツのダイジェストを作成します。その対象はメッセージの一部でも全体でもかまいません。XML シグニチャは、受信者が ACE XML Gateway の公開鍵を使用して処理します。公開鍵を使ってダイジェストを復号できれば、受信者は、公開鍵と対となる（ACE XML Gateway の）秘密鍵の持ち主によってそのメッセージが生成されたことを確認できます。同様に、シグニチャ照合を設定するには、送信者の公開鍵を使用します。

これから説明する手順は送信応答のコンテンツに署名する方法です。ここでは、サンプル リソース用 Web サイトに収容されているリソース ファイルを使用して署名の設定を行います。リソースを入手していない場合は、example.reactivity.com から入手してください。

応答メッセージへの署名

送信応答の XML 署名を設定する手順は次のとおりです。

1. ルーティング ブラウザで retrieveQuote サービス プロキシをクリックします。
2. **Response Message Specification** の下に見える **XML Signing** の横の [enable] リンクをクリックします。

図 19-1　送信応答への署名

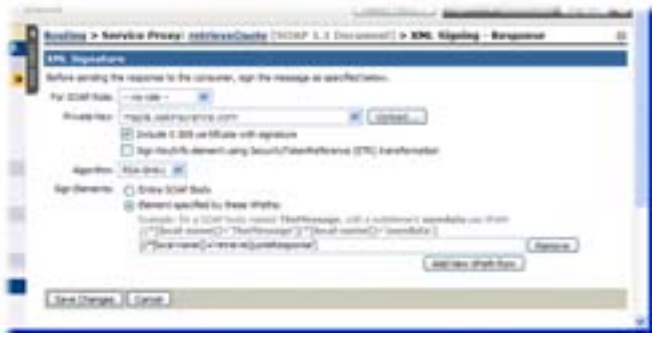
3. **XML Signature** ページ で **[Private Key]** オプションの横の **[Upload]** ボタンをクリックします。
4. **Upload Public/Private Keypair Resource** ウィンドウで名前を入力します。リソースはポリシーの中で使われるので、意味のわかる名前（`maple keypair` など）をつけます。
5. ファイル選択ウィンドウで **[Browse]** をクリックしてから、`maple.p12` ファイルを探して選択します。
6. パスワードとして `swordfish` と入力します。
7. **[Upload]** ボタンをクリックします。
8. **Private Key** メニューでそのリソースが選択されていることを確認します。

   次のオプションの値はデフォルトのままでかまいません：**[For SOAP Role]**、**[Include X.509 certificate with signature]**（有効化されていること）、**[Algorithm]**
9. **[Element specified by these XPaths]** オプションを選択し、[XPath] 欄に次の値を入力します。

   ```
   //*[local-name()='retrieveQuoteResponse']
   ```

   この設定は、署名を行った応答エレメント全体に対して有効です。

図 19-2　XML シグニチャの設定



10. **[Save Changes]** をクリックし、ポリシーを導入します。

以上の手順で、特定のエレメントに署名が行われました。実際にはほとんどの場合、SOAP メッセージ本文全体に署名が行われます。また、メッセージの安全性と完全性を保証するため、通常 XML シグニチャと XML 暗号化が一緒に使用されます。

XML シグニチャのテスト

メッセージの XML 署名を設定したら、WFetch からサービスへメッセージを送信します。結果は WFetch の出力表示ウィンドウに現れますが、メッセージをよりわかりやすく表示するには、次の手順でメッセージ トラフィック ログとして開きます。

1. 操作メニューで **[Message Traffic Log]** リンクをクリックします。
2. メッセージ エントリを表示するために **[req/resp pair]** リンクをクリックします。
3. **[Logged Message Content]** ウィンドウの **[Outgoing Response Attributes]** エリアで **[text/xml]** リンクをクリックします。

   次のようなウィンドウが表示されます。

図 19-3　署名されている応答

この応答の中で、次の部分に注意してください。

- Signatureエレメントが WSSE セキュリティ ヘッダに表示されています。図 19-3 では前の操作で設定した暗号化部分が省略されていますが、暗号化を有効に設定してあれば、Signature エレメントがセキュリティ ヘッダの中で EncryptedKey エレメントとともに表示されます。
- この図では BinarySecurityToken エレメントのコンテンツが省かれていますが、実際のテストでは非常に長いものになります。
- retrieveQuoteResponse エレメントには新しい属性がいくつか加わっています。wsu:Id 属性値は Reference エレメントの URI 値の対象としてのエレメントを示しています。

これらの機能により、受信したアプリケーションは署名付きエレメントに格納された情報の有効性と完全性を確認できます。

INDEX

さ

し

て

と

は

ひ

ほ

め

ら

ろ