



# CHAPTER 18

## ebXML トラフィックに関する作業

この章では、ebXML データをやり取りするサービスでの作業方法について説明します。内容は次のとおりです。

- 「[ebXML について](#)」 (P.18-191)
- 「[ebXML サービス トラフィックの処理](#)」 (P.18-192)
- 「[ebXML ルックアップ テーブルの使用](#)」 (P.18-196)
- 「[Gateway をイネーブルにして SMTP トラフィックを受信するには](#)」 (P.18-198)
- 「[外部 MTA の設定](#)」 (P.18-199)

### ebXML について

Electronic Business XML (ebXML) は、システム間や組織間でビジネス プロセス情報のやり取りを行うために設計された標準機能セットです。実用面では、ebXML を使用すると、組織では、従来のメッセージ指向の方法で、注文書、請求書や、その他共有する必要がある情報をやり取りできます。

ebXML メッセージは、EbXML Message Service (ebMS) と呼ばれるプロトコルを使用して送信されます。ebMS は、SOAP および SOAP 添付ファイルに基づき、転送には HTTP または SMTP のいずれかが使用されます。

Cisco ACE XML ゲートウェイ では、ebXML サービスがサポートされます。これは、外部 ebXML サービスでハンドラおよびサービス記述子を作成できることを意味します。

ACE XML Gateway を使用すると、さまざまな方法で ebXML トラフィックを検証できます。また、アクセス コントロールやルーティング ルールなどの他のポリシー機能も、ebXML トラフィックに適用できます。

ACE XML Gateway では、これらの ebXML 固有の機能を検証できます。

- **ebXML ヘッダー** : ACE XML Gateway は、ebXML メッセージに MessageHeader SOAP ヘッダーがあることを検証します。この要素は、ebMS 2.0 の使用に従って形成する必要があります。使用から逸脱すると、妥当性に関する例外が発生します。
- **ebXML マニフェスト** : ebXML メッセージには、マニフェスト SOAP の本文が含まれている場合があります。この場合、ACE XML Gateway では、ebMS 2.0 仕様に従って確実に形成できます。
- **XML 署名** : 署名がヘッダーにあり、使用しているポリシーで署名のチェックが必要な場合、署名の妥当性がチェックされます。署名には、Content-Id (cid:xxx) URL スキームで 1 つまたは複数の SOAP 添付ファイルに対する参照が含まれていることがあります。

- **添付ファイル マニフェスト** : ebXML マニフェストがある場合、ACE XML Gateway では、ebXML マニフェストに各添付ファイルへの参照を含めるようにすることができます。添付ファイルがない参照がマニフェストに含まれる場合、妥当性に関する例外が通知されます。マニフェストに記述されていない添付ファイルがペイロードに含まれている場合、警告ログレベル イベントが生成されますが、添付ファイルは廃棄されます (ebMS 2.0 仕様で指定されている動作)。
- **添付ファイル スキーマ** : マニフェストにより、各添付ファイルのスキーマ ID が用意できます。ID が存在し、ポリシーによって ID が要求された場合、各添付ファイルでは、スキーマの妥当性がテストされます。

ACE XML Gateway では、同期および非同期の両方の ebXML メッセージのやり取りがサポートされます。ユーザが HTTP を介して SOAP メッセージを送信した場合、メッセージで ebXML の妥当性がテストされ、HTTP を介して ebXML サーバに送信されます。同期メッセージでは、サーバからの応答で ebXML の妥当性がテストされ、クライアントに戻されます。非同期メッセージでは、メッセージが正常に送信された場合、204 応答がクライアントに戻されます。

## ebXML サービス トラフィックの処理

ここでは、ebXML サービス トラフィックで ACE XML Gateway ポリシーを設定する方法について説明します。この手順は 2 つにわかれます。

- サービス記述子を作成します。サービス記述子には、バックエンド サービス プロバイダー (またはユーザが送信したメッセージの宛先) に対する ACE XML Gateway インターフェイスの設定が含まれます。
- サービス ハンドラを作成します。サービス ハンドラには、サービス ユーザが存在するインターフェイスの設定が含まれます。

## ebXML サービス記述子の作成

サービス記述子により、ACE XML Gateway とメッセージの受信者 (通常はサービス コンテナ) との間のインターフェイスが制御されます。

ebXML サービスのサービス記述子を作成するには、次の操作を実行します。

- 
- ステップ 1** Administrator ユーザまたは Routing ロールを持つ Privileged ユーザとして、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** ルーティングのページで、[Create a New] メニューから [Service Descriptor] を選択し、[Create] ボタンをクリックします。
- [Step 1 of 5: Service Protocol] ページが表示されます。
- ステップ 3** プロトコル メニューから、サービスで受信する ebXML メッセージ トラフィックのタイプを選択します。オプションは次のとおりです。
- **HTTP Post ebXML** : 同期 ebXML トラフィック用。この場合、ユーザは応答を待ちます。
  - **Asynchronous HTTP Post ebXML** : 応答が想定されない ebXML トラフィック用。
  - **Asynchronous URL Lookup-Based ebXML** : ACE XML Gateway で、宛先 URL ルックアップ テーブルに基づいてルーティングを決定。このメカニズムにより、SMTP メッセージと HTTP メッセージの両方の送信メッセージがサポートされます。

このオプションを使用するには、このセクションで説明されている手順に加え、[「ebXML ルックアップ テーブルの使用」 \(P.18-196\)](#) で説明されているようにルックアップ テーブルを設定する必要があります。

- ステップ 4** [Continue] をクリックします。
- ステップ 5** [Step 2 of 5: General Information] ページで、サービス記述子の固有名を入力します。この名前は、ポリシー内でだけ使用されます。
- ステップ 6** ebXML サービス タイプが (SMTP ではなく) HTTP に基づいている場合、[General Information] ページの [Server] メニューに追加の設定が表示されます。リストから宛先サーバを選択します。サーバがポリシーで HTTP サーバ リソースとして指定されていない場合、[Add a New Server] ボタンをクリックし、新しいサーバ設定を実行します。
- ステップ 7** [Continue] をクリックします。[Step 3 of 5: Service Interface] ページが表示されます。
- ステップ 8** サービス インターフェイス設定は、次のとおり、ebXML メッセージ サービスのタイプによってさまざまです。

*HTTP Post ebXML および Asynchronous Post ebXML:*

- [Path on Server] フィールドで、バックエンドサーバの実サービスに呼び出し URL を入力します。
- ebXML では、SOAP 1.1 のサポートだけが指定されているため、SOAP バージョンでは、デフォルト値の SOAP 1.1 が残されることがあります。SOAPAction は "ebXML" である必要があります。
- 必要に応じ、HTTP Basic 認証、Web Services Security (WSS) UsernameToken、または Security Assertion Markup Language (SAML) トークン値など、バックエンドサーバに対して ACE XML Gateway を認証するよう設定します。ここで設定されている値は、メッセージとともに渡されます。
- 必要な場合、サービス時間しきい値をミリ秒単位で指定します。ACE XML Gateway で、しきい値の時間内でバックエンドサーバから応答を受信しなかった場合、この事実を示すイベントが記録されます。これは、Quality Of Service の考慮時に効果的です。

*URL ルックアップが実行される ebXML メッセージについては、次のとおりです。*

- 「**ebXML ルックアップ テーブルの使用** (P.18-196) で説明されているようにルックアップテーブル ファイルをすでに ACE XML Manager にアップロードした場合、これをメニューから選択します。これ以外の場合、[Upload] をクリックし、画面上の説明に従ってテーブルをロードします。
- ルックアップ テーブルの URI マッピングに HTTPS の宛先がある場合、これらの宛先に対して、必要に応じ、証明書の検証や公開鍵または秘密鍵の設定を指定します。
- 必要な場合、サービス時間しきい値を指定します。

- ステップ 9** [Continue] をクリックします。

[Step 4 of 5: Request Message Specification] ページが表示されます。

- ステップ 10** (ebXML メッセージ ヘッダーの妥当性をチェックすることによって) ebXML の妥当性を確認するため、バックエンド サービスへのメッセージが自動的に検証されます。

[Request Message Specification] ページで、必要な検証オプションを追加で設定します。これらには、マニフェスト検証、添付ファイル、XML 署名チェックが含まれます。

次の項目が、これらの設定に適用されます。

- マニフェストでは、ebXML メッセージの添付ファイルが説明されます。マニフェストに一致する添付ファイルを検証する場合、ACE XML Gateway では、正確な数の添付ファイルがメッセージに含まれるかや、すべての ContentID が考慮に入れられているかなどが、チェックされます。
- マニフェストでは、URL の XML スキーマの場所が指定されます。該当する URL が含まれている XML スキーマが ACE XML Manager にすでにアップロードされていた場合、スキーマ検証はイネーブルにされており、ACE XML Gateway ではこのスキーマが使用されます。ACE XML Gateway では、ネットワークからダイナミックにスキーマが取得されません。

- メッセージの一部ではないが URI で参照される添付ファイルがマニフェストによって指定されている場合、ACE XML Gateway では、メッセージを拒否できます。セキュリティのため、ACE XML Gateway では、非ローカル リソースの使用は試行されません。URI ベースのリソースを許可するよう、ハンドラまたはサービス記述子を設定できますが、メッセージにないオブジェクトを参照するマニフェスト エントリがあるメッセージは拒否することが推奨されます。
- ebXML メッセージまたはメッセージの添付ファイルに対し、署名要求を指定できることに注意してください。ACE XML Gateway では、署名の検証前に、PKCS7 (S/MIME) 暗号化添付ファイルが復号化されます。メッセージの添付ファイルが暗号化されている場合、検証前にメッセージを復号化するためのキーを指定する必要があります。
- 署名する添付ファイルが必要な場合、すべての添付ファイルに署名する必要があります。ただし、添付ファイルへの署名が必要ではない記述子またはハンドラでは、エラーなしで署名された添付ファイルが受け付けられます。

**ステップ 11** HTTP Post メッセージ（非同期）では、[Response Message Specification] ページが表示されます。必要に応じ、サーバによって返されるメッセージの検証要求を設定します。発信要求では、応答の本文で、マニフェストの検証、添付ファイルの検証、および XML 署名のチェックを設定できます。

**ステップ 12** [Continue] をクリックし、サービス記述子を終了します。

この時点で、次に説明されているように、サービスのハンドラを作成できるようになっています。

## ebXML ハンドラの作成

ebXML サービスのハンドラを作成するには、次の操作を実行します。

- 
- ステップ 1** Administrator ユーザまたは Web コンソールの Operations ロールを持つ Privileged ユーザとして、操作メニューで Virtual Services ブラウザを開きます。
- ステップ 2** [Create a new] メニューで、[Handler] が選択された状態で [Create] ボタンをクリックします。
- ステップ 3** プロトコル リストから、サービスに適切な ebXML メッセージ トラフィックのタイプを選択します。オプションは次のとおりです。
- [HTTP Post ebXML]。非同期 ebXML トラフィック。この場合、本文が含まれた応答がバックエンド ebXML サービスから返されることが想定されます。
  - [Asynchronous HTTP Post ebXML]。バックエンド サービスからの応答が想定されない ebXML トラフィック。
  - [SMTP ebXML]。SMTP ベースの電子メールとして渡される非同期の ebXML トラフィック。このオプションを使用するには、「[Gateway をイネーブルにして SMTP トラフィックを受信するには](#)」(P.18-198) で説明されているように、ACE XML Gateway で SMTP MTA リスナーをイネーブルにする必要があります。
- ステップ 4** [Continue] をクリックします。ハンドラの設定ページが表示されます。
- ステップ 5** ハンドラの名前を入力し、ハンドラ グループを選択します。名前は内部でだけ使用されます。必要に応じ、このページで他のハンドラ オプションを設定できます。ポリシーの作成時には、メッセージ本文のログギングをイネーブルにすることを推奨します。
- ステップ 6** [Continue] をクリックします。[Consumer Interface] ページが表示されます。

**ステップ 7** サービスでのユーザのインターフェイスを、次の手順で設定します。

- ebXML over HTTP ハンドラでは、ポートと判明しているローカルパスを指定します。これは、ホスト名が含まれているパスで、ユーザがサービスの起動に使用する URI で構成されています。
- ebXML over SMTP ハンドラでは、ユーザがこのサービス用に起動する、宛先となる電子メールアドレスを指定します。電子メールは、`<name>@<domain>.<ext>` という標準形式である必要があります。ACE XML Gateway MTA では、このアドレスで指定されたドメイン宛での電子メールメッセージが受け入れられます。

他の設定は、ハンドラ ページのデフォルト値のままにすることができます。これらの設定について、簡単に説明します。

- ebXML では、この SOAP のみのサポートが指定されているため、[SOAP version] は SOAP 1.1 である必要があります。
- ebXML による指定どおり、SOAPAction は無視されます。ただし、値 "ebXML" (引用符付き) は検出されます。
- ebXML サービスでは、ハンドラの [SOAP Method] 設定と [SOAP Method Namespace] 設定は、Gateway には使用されません。

**ステップ 8** [Continue] をクリックします。

**ステップ 9** ハンドラでの着信メッセージは、デフォルトで、ebXML として検証されます。該当しない場合はドロップされます。[Request Message Specification] ページでは、マニフェスト検証、添付ファイル検証、XML 署名チェックなどの追加検証オプションを設定できます。詳細については、「[ebXML サービス記述子の作成](#)」(P.18-192) の手順 5 を参照してください。

**ステップ 10** [Continue] をクリックします。

**ステップ 11** 必要に応じ、[Response Message Specification] ページを設定します。ページの設定は、次のとおりです。

- 非同期メッセージ ハンドラでは、応答メッセージが想定されていないため、設定可能なプロパティはありません。
- 同期メッセージ タイプ (HTTP POST ebXML) では、[Response Message Specification] ページが表示されます。同期ハンドラ サービス ペアのオプション [Allow asynchronous delivery; this response can be an empty (HTTP 204) message] をチェックすることによって、HTTP を介して同期または非同期のトラフィックの混合モードをイネーブルにできます。
- メッセージは、204 応答などの空メッセージまたは本文付きの応答などの場合があります。ACE XML Gateway では、着信 ebXML メッセージと同様に応答本文を確認できます。つまり、マニフェスト検証、添付ファイル検証、および応答本文の XML 署名チェックも設定できます。

**ステップ 12** [Continue] をクリックします。

**ステップ 13** [Click Add a Route Now] をクリックし、このハンドラがルート メッセージの宛先とするサービス記述子を指定します (サービス記述子がまだ存在しない場合、ルートを追加せずに終了し、後で追加することができます)。

**ステップ 14** メニューから、作成したサービス記述子の名前を選択します。ebXML ハンドラでは、ハンドラの他のタイプと同様、複数のルートを使用でき、ルート設定ページで指定した基準に一致するものが選択されます。

**ステップ 15** [Save Changes] をクリックし、ポリシーが導入され、ACE XML Gateway の設定が使用されます。



## ebXML ルックアップ テーブルの使用

サービス記述子は、ACE XML Gateway によって仮想化されるサービス用のバックエンド設定を表す ACE XML Gateway のポリシー オブジェクトです。サービスのほとんどのタイプでは、サーバの IP アドレスまたはホスト名およびターゲット サービス URL を単に設定することによって、宛先サービスを指定できます。

ebXML サービスでは、同様に、メッセージの受信者を定義できます。ただし、ebXML サービス記述子により、URL ルックアップと呼ばれる追加のルーティング メカニズムが提供されます。

URL ルックアップでは、ACE XML Gateway により、キーの宛先値で構成されているテーブルを使用して、メッセージの宛先が動的に決定されます。ACE XML Gateway は、ebXML メッセージヘッダーの要素を組み合わせることによって、キーに到着します。次に、キーの一致について、ルックアップテーブルがチェックされます。キーが見つかった場合、メッセージは、キーに関連付けられている URL 経由でルーティングされます。



(注)

URL ルックアップは、非同期 ebXML サービス メッセージ タイプだけで動作します。

URL ルックアップ ルーティングを設定するには、キーの値と対応する宛先 をテキスト ファイルに入力します。ファイル名に関する要件はありません。アクセスする ACE XML Manager Web コンソールからコンピュータのファイル システムまたは URL にアクセス可能である必要があります。

宛先 URL は、HTTP、HTTPS、または電子メールアドレスの可能性がありますが、「[ebXML サービス記述子の作成](#)」(P.18-192) で説明されているように、HTTPS の宛先には、SSL クライアント キーペアおよびサーバ証明書を指定できます。

## ルックアップ キー

URI 一致キーを構成する ebXML メッセージ ヘッダーからのフィールドは、次のとおりです。

- Service
- Action
- CPAId
- To-PartyId

キーを構築するには、ルックアップ テーブル ファイルにある対応する URI の横に、フィールド値を指定します。フィールド値は、(空白なしで) カンマで区切って表示順に入力する必要があります。URI は、1 つのタブ文字によってキーと区切り、同じ行に入力する必要があります。

たとえば、[例 18-1](#) に示されているようなメッセージの構造について考えます。

### 例 18-1 サンプル メッセージ

```
<SOAP-ENV:Header>
<eb:MessageHeader>
  <eb:From>
    <eb:PartyId context="uriReference">
      urn:company.com
    </eb:PartyId>
  </eb:From>
  <eb:To>
    <eb:PartyId context="uriReference">urn:acme.com</eb:PartyId>
  </eb:To>
  <eb:CPAId>cpal</eb:CPAId>
```

```

    <eb:ConversationId>1234567.1953.react.nene</eb:ConversationId>
    <eb:Service>OrderProc</eb:Service>
    <eb:Action>ProcNewOrder</eb:Action>
    <eb:MessageData>
    ...
</eb:MessageData>
...
</eb:MessageHeader>
...
</SOAP-ENV:Header>

```

Service、Action、CPAId、および To-PartyId というキー フィールドの値に注目します。特定のアドレス宛てに送信するサンプルで示されているように、フィールドの値があるメッセージを使用するには、次のようにマッピングを構築します。

```
OrderProc,ProcNewOrder,cpa1,acme.com    mailto:jw@example.com
```

ここで示されているように、フィールド値はカンマで区切られています。宛先アドレスから最後のフィールドを分離するために、1 つのタブ文字を使用する必要があります。

この例では、URL はメールの宛先アドレスです。http または https の宛先もサポートされます。宛先として http アドレスまたは https アドレスを使用するには、例 18-2 のように、URL にプロトコル指定を含めます。

#### 例 18-2 サンプル URL ルックアップ項目

```
OrdProc,ProcOrder,cpa1,acme.com    mailto:user@sample.com
OrdProc,ProcOrder,cpa2,acme.com    http://sample.com/myservice
```

ルックアップ マッピングにはいくつかの追加の注意点があります。

- ルックアップ テーブルのマッピングには、Service、Action、CPAId、および To-PartyId のすべてのフィールドを指定する必要があります。
- キーに一致するメッセージでは、各キー フィールドが、メッセージ ヘッダーの対応する値に一致する必要があります。一致しない場合、メッセージはドロップされ、例外が発生します。
- メッセージは、1 つの宛先アドレスだけに一致させることができます。同じキーに 2 つのエントリが存在する場合、最後のエントリが使用されます。
- 行の先頭にハッシュ記号 (#) を入力することにより、コメントをファイルに追加できます。

## ルックアップ テーブルのアップロード

ファイルの作成後、次のとおり Web コンソールでテーブルをアップロードすることによって、ACE XML Gateway ポリシーでマッピングを使用できます。

- 
- ステップ 1** 操作メニューで [ebXML Lookup Tables] リンクをクリックします。
  - ステップ 2** テーブルの名前を指定します。この名前は、Web コンソールでだけ内部的に使用されます。
  - ステップ 3** ファイルの場所により、[Browse] をクリックしてファイル選択ダイアログでファイルを指定するか、ファイルの URL を指定します。
  - ステップ 4** [Upload] をクリックします。
- 

完了すると、SMTP ベース、ルックアップ ベースのサービスの ebXML サービス記述子の作成時に表示される設定にあるメニュー オプションとして、テーブルを使用できます。

# Gateway をイネーブルにして SMTP トラフィックを受信するには

ebXML メッセージは、HTTP または SMTP を介して送信できます。サービスで SMTP を使用している場合、使用環境にある各 Gateway で Mail Transport Agent (MTA) リスニング ポートをオープンする必要があります。ポートをオープンすると、着信 ebXML トラフィックを電子メール メッセージとして受信するよう、ACE XML Gateway がイネーブルにされます。



(注) 次に、ACE XML Gateway に含まれている MTA を設定する方法について説明します。「外部 MTA の設定」(P.18-199) で説明されているように、外部 MTA も設定できます。

着信電子メール リスニング ポートは、ACE XML Gateway では、デフォルトでクローズされています (ただし、ログ イベントの電子メール通知のシステム管理者への送信をイネーブルにするため、sendmail プロセスは、デフォルトでアクティブです)。

MTA リスニング ポートをオープンするには、Administrator アカウントを使用して、ACE XML Gateway アプライアンスでシェル インターフェイスにアクセスする必要があります。

MTA リスニング ポートをイネーブルにするには、次の操作を実行します。

- ステップ 1** セキュア SSH クライアントまたはコンソールからアプライアンスへの接続から、root ユーザとして ACE XML Gateway アプライアンスのシェル インターフェイスにログインします。[Main Menu] が表示されます。



(注) シェルへのアクセスの詳細については、『Cisco ACE XML Gateway Administration Guide』の「Logging Into the Shell Interface」を参照してください。

- ステップ 2** [Main Menu] から [Advanced Options] を選択します。シェル インターフェイスにより、[Advanced Options] 画面が表示されます。
- ステップ 3** [Advanced Options] ページから [MTA Configuration] を選択します。シェル インターフェイスにより、[MTA Menu] 画面が表示されます。
- ステップ 4** メニュー項目 [Open MTA Port] を選択します。リスニング ポートのステータスがトグル切り替えされる、この項目を選択します。メニュー項目の名前が、[Close MTA Port] に変更されます。
- これで、標準 SMTP サーバとしてポート 25 でリスンするよう、アプライアンスが設定されました。



(注) [MTA Menu] 画面の最初の項目が [Open MTA Port] ではなく [Close MTA Port] の場合、MTA ポートはすでにオープンされています。

- ステップ 5** リスニング ポートのオープン後、ACE XML Gateway MTA では、ポストマスタ メールボックスで電子メールを受信できます。ポストマスタ アドレスは、MTA の標準管理アドレスです (SMTP プロトコルに必要)。このアドレスは、Gateway の着信トラフィックと発信トラフィックのいずれにも影響を与えません。

必要な場合、ポストマスタへのメールが別の場所に送信されるようにアドレスを変更することも可能です。デフォルトのままにしておく場合、ポストマスタ メールボックスは ACE XML Gateway の root ユーザのメールボックスになります。これを行うには、[MTA Menu] から、2 つ目の項目 [Configure postmaster address] を選択し、画面上の説明に従ってポストマスタ メールボックスを設定します。



- ステップ 6** 完了したら、[MTA Menu] から 3 つ目のオプションを選択して [Advanced Options] メニューに戻り、コンソールセッションをクローズします。

この時点で、ACE XML Gateway では、電子メールの形式でサービス トラフィックを受信できるように設定されています。使用環境の各 ACE XML Gateway で、この手順を繰り返します。

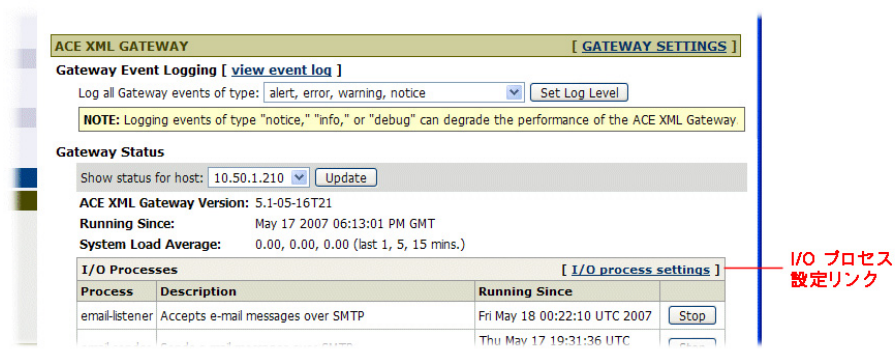
## 外部 MTA の設定

「Gateway をイネーブルにして SMTP トラフィックを受信するには」(P.18-198) で説明されているように、各 Gateway には、ACE XML Gateway で発着信する電子メール トラフィックを処理するため、内部 Mail Transport Agent (MTA) が含まれています。

また、ACE XML Gateway で使用する、Microsoft Exchange サーバなどの外部 MTA を設定できます。外部 MTA を設定するには、次の操作を実行します。

- ステップ 1** Administrator ユーザまたはコンソールの Operations ロールを持つ Privileged ユーザとして、操作メニューの [Administration] グループで [System Management] をクリックします。
- ステップ 2** ACE XML Gateway 設定で、[I/O Processes] の横に表示されている [I/O process advanced settings] リンクをクリックします。

図 18-1 外部 MTA 設定へのアクセス



- ステップ 3** [I/O Process Settings] ページで、SMTP サーバフィールドにある使用環境の MTA のホスト名と、SMTP リスニング ポート（通常は、ポート 25）を入力します。
- ステップ 4** Virtual Memory (VM; 仮想メモリ) サイズの制限は、ACE XML Gateway の電子メール送信者コンポーネントに適用されます。この設定により、電子メール攻撃によって使用されることからユーザを保護します。アプリケーションにより、この値を増やしたり、減らしたり、デフォルトを受け付けたりします。ほとんどの場合、デフォルトサイズの 512000 で十分です。
- ステップ 5** [Save Changes] をクリックします。

