



# CHAPTER 15

## ポートおよびホスト名に関する作業

ここでは、ACE XML Gateway でポートをオープンして、クライアント HTTP または HTTPS の要求をリスンする方法について説明します。内容は次のとおりです。

- 「HTTP ポートについて」 (P.15-165)
- 「ポートのオープン」 (P.15-166)
- 「仮想ホスト名でのリスニング」 (P.15-168)
- 「静的コンテンツ応答の設定」 (P.15-168)
- 「応答の圧縮」 (P.15-170)

### HTTP ポートについて

クライアントでは、そのユーザ インターフェイスで指定されたポート番号に要求を送信することによって、ACE XML Gateway でプロキシされているアプリケーションにアクセスします。ポート オブジェクトを使用すると、ACE XML Gateway の HTTP リスニング ポートをオープンし、その設定を管理できます。ポート オブジェクトは、新しい仮想 Web アプリケーションを定義するときか、または Web Services Description Language (WSDL) インポート プロセスを介して仮想 Web サービスを定義するときに、作成されます。ただし、手作業でこれらを作成したり、既存の定義を変更したりすることもできます。

ACE XML Gateway ポリシーには、HTTP ポート 80 の組み込みリスニング ポートが含まれています。HTTP ポートのポリシー オブジェクトを使用して、追加のリスニング ポートをオープンできます。たとえば、SSL セキュア接続（一般的にポート 443 を使用）のために、追加ポートをオープンする必要があることがあります。リスニング ポートの追加後、これを仮想サービスまたは仮想 Web アプリケーションに適用すると、サービスへの要求がポートで処理されます。



(注)

特定の内部システム プロセスによって使用されるため、組み込みデフォルト HTTP ポート (80) は削除できません。ただし、[Open HTTP(S) Ports] ページから、組み込みポート オブジェクトの名前、ポート番号、または他の値を変更することによって、組み込みポート オブジェクトを編集できます。

ポート オブジェクトには、ACE XML Gateway の名前ベースまたは IP ベースの仮想ホストを設定できる設定が含まれています。ポートは、特定のホスト名または IP アドレスに送信されるトラフィックをリスンするよう、設定できます。

ポートは、静的な応答メッセージとともに特定の URL で要求に応答するよう、設定できます。この機能は、アップストリームロード バランサまたは他のネットワーク ホストによって、ACE XML Gateway のヘルス モニタリングをイネーブルする場合に、しばしば使用されます。

ポート定義で応答の圧縮がイネーブルの場合、ACE XML Gateway では、設定されたサイズのしきい値を超える応答は圧縮されます。クライアントでは、圧縮された応答を受け入れる着信要求で、Accept-Encoding ヘッダーによって示す必要があります。



(注)

ACE XML Gateway では、チャンクされた要求は、Reactor によってのみ処理できます。つまり、Flex Path では、チャンクされた要求（チャンクされた転送エンコードを示す要求）はサポートされません。チャンクされた要求を受信した場合、ACE XML Gateway により、411 エラー応答コードで応答が返されます。バックエンドサーバからのチャンクされた応答はサポートされますが、Flex Path で処理されるメッセージについては、Gateway により、クライアントへの配信前にチャンクされた応答が構成されます。Reactor によって処理されるチャンクされた応答は、チャンクされた状態で渡されます。

## ポートのオープン

ACE XML Gateway でリスニング ポートをオープンするには、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 Routing ロールを持つ Privileged ユーザとして Web コンソールにログイン中に、使用するポートに対してアクティブなサブポリシーを設定します。
- ステップ 2** 操作メニューで [HTTP Ports & Hostnames] リンクをクリックします。
- ステップ 3** [Open HTTP(S) Ports] ページで [Add a New Port] ボタンをクリックします。
- ステップ 4** [Edit Port] ページにある [Name] フィールドで、新しいポート定義に対してわかりやすい名前を入力します。この名前により、ACE XML Manager のコンソールでポートが特定されます。名前は、ポリシー内のポート オブジェクトで固有である必要があります。
- ステップ 5** [Port Number] フィールドにリスニング ポートの番号を入力します。



(注)

システムが適切に動作するようにするには、ACE XML Gateway および Manager によって管理目的で予約されているポート番号の使用は避けます。これらには、8200 から 8299 の範囲および 514 のポートが含まれます。システムによって使用されている可能性があるポートのリストについては、『Cisco ACE XML Gateway Administration Guide』を参照してください。

- ステップ 6** ACE XML Gateway で、ポートのトラフィックに対してトランスポート レイヤ セキュリティを適用するには、[SSL] チェックボックスを選択します。  
[Public/Private Keypairs] メニューおよび [Upload] ボタンがイネーブルにされます。
- ステップ 7** SSL がイネーブルの場合、[Public/Private Keypair] メニューから項目を選択し、この接続の暗号化に使用される公開鍵と秘密鍵のペアを指定します。  
正しいキーのペアがメニューに表示されない場合、[Upload] ボタンを使用してポリシーにアップロードする必要があります。SSL の詳細については、「[SSL/TLS によるトラフィックの保護](#)」(P.19-201)を参照してください。
- ステップ 8** オプションで、このポートにあるクライアントとの SSL 接続のネゴシエーションを受け付ける暗号を、[SSL Cipher Suite] メニューで指定します。接続を使用するには、セキュア接続のネゴシエーションで、ACE XML Gateway およびクライアントによって暗号スイートで合意できる必要があります。ここで指定された暗号がクライアントでサポートされていない場合、接続は許可されません。  
接続では、デフォルトで、[System Management] > [I/O Settings] ページで設定されているように、ACE XML Gateway の HTTP サーバプロセスに対して、SSL 暗号スイート設定が使用されます。このオプションを使用すると、このポートに対して、より詳細な設定を適用できます。

<http://www.openssl.org/docs/apps/ciphers.html> で説明されているように、[SSL Cipher Suite] メニューからカスタム設定を選択して暗号スイートを指定し、表示されるフィールドで、OpenSSL 暗号文字列形式で受け付けられる暗号スイートを入力します。



(注) 暗号スイート文字列を入力する際には、注意してください。ACE XML Manager Web コンソールインターフェイスでは、入力値は検証されません。無意味な値を誤って入力した場合、ACE XML Gateway では、サーバとの SSL 接続をオープンできないことがあります。

**ステップ 9** ポートは、すべてのトラフィックまたは特定のホスト名または IP アドレスに送信されるトラフィックだけをこのポートでリッスンするよう、設定できます。この設定を使用すると、ホスト名または IP アドレスのいずれかによって、ACE XML Gateway で仮想ホスト (vhosts) を設定できます。

[Listen For] メニューの次のオプションから、このポートで監視する要求を指定します。

- [All traffic on this port] : このポートの Gateway に宛てて送信されるすべてのトラフィックが、このポートでリッスンされます。
- [Requests to a hostname] : このポートの Gateway およびこのホスト名に宛てて送信されるすべてのトラフィックが、このポートでリッスンされます。ホスト名の文字または POSIX 1003.2 正規表現を [Hostname] フィールドに入力することによって、1 つまたは複数のホスト名を指定します。正規表現を使用するには、[Allow regular expression matching in the hostname] チェックボックスをクリックします。
- [Requests to specific IP addresses] : ポートでは、この IP アドレスに宛てて送信されたすべてのトラフィックがリッスンされます。1 つまたは複数の IP アドレスを [IP Addresses] フィールドに入力します。各アドレスがそれぞれの行にあるよう、複数の IP アドレスを分割するパラグラフを使用します。

入力するすべての IP アドレスは、各 Gateway アプライアンスのネットワーク インターフェイスでも設定する必要があります。詳細については、『Cisco ACE XML Gateway Administration Guide』を参照してください。

**ステップ 10** [Static Content] メニューから [serve the following static page on this port] オプションを選択することによって、このポートの特定の URL で静的な応答メッセージを用意できます。

詳細については、「静的コンテンツ応答の設定」(P.15-168) を参照してください。

**ステップ 11** 必要に応じ、[Compression] オプションをイネーブルにすることによって、このポートでの応答の圧縮がイネーブルにされます。圧縮されるメッセージの最小サイズも指定します。デフォルトは 2KB です。詳細については、「応答の圧縮」(P.15-170) を参照してください。

**ステップ 12** このサーバでのメッセージ処理で、Reactor プロセスを回避する場合、[Flex Path] オプションを選択します。Gateway サービスに対して定義されたタスクが Reactor によってサポートされない場合 (プロトコル メディエーションなど)、Reactor では、要求メッセージが自動的に Flex Path 処理に渡されます。サービスへのラウンドトリップの可能性を含む、応答による処理の完了後、クライアントに戻す配信のため、Reactor に戻されます。

外部クライアントとの互換性を保つため、このオプションを使用することによって、ポート上で Reactor をディセーブルにする必要が生じることがあります。一般的には、クライアントとの相互運用性について注意深くテストした後でだけ、実稼動システムで Reactor を使用することを推奨します。また、パフォーマンスの理由で、Reactor では Flex Path より少ないロギングが実行されます。このため、初期ポリシー作成の間には、Reactor をディセーブルにする必要が生じることがあります。



(注) リリース 5.0 にアップグレードされたシステムでは、アップグレード前にポリシーに存在したポート オブジェクトは、デフォルトでイネーブルにされています。

**ステップ 13** [Save Changes] をクリックします。

これで、ポートは、仮想サービス設定ページの [HTTP Port] メニューに表示されるようになりました。

## 仮想ホスト名でのリスニング

ACE XML Gateway では、IP ベースと名前ベースの仮想ホスティングがサポートされます。このサポートにより、Gateway は、複数のアドレスサブルなホストに予約されるプロキシの役割を果たすことができます。ACE XML Gateway の仮想ホスト名の設定は、ポリシーのポート オブジェクト設定に表示されます。

ポート上の仮想ホスト名により、ACE XML Gateway は、指定されたホストに宛てられたサービス要求に誘導されます。ポリシーにある複数のポートを、それぞれ、異なるホスト名または IP アドレスで、1 つのポート番号でリッスンするよう、設定できます。

ACE XML Gateway の仮想ホスト名を設定するには、次の手順に従います。

- 
- ステップ 1** ホストの要求をリッスンする ACE XML Gateway で、ポート オブジェクトを作成または変更できます。ポート オブジェクトの作成に関する詳細については、「[ポートのオープン](#)」(P.15-166) を参照してください。
- ステップ 2** [Listen For] メニューで、名前ベースの仮想ホスティングの場合は [requests to a hostname] を、IP ベースの仮想ホスティングの場合は [requests to specific IP addresses] を、選択します。
- ステップ 3** IP アドレスに対する要求をリッスンするようポートを設定する場合は、テキスト フィールドに IP アドレスを指定します。入力する IP アドレスは、ACE XML Gateway アプライアンスのネットワーク インターフェイスでも設定する必要があります。詳細については、『*Cisco ACE XML Gateway Administration Guide*』を参照してください。
- ステップ 4** ホスト名に対する要求をリッスンするようポートを設定する場合は、テキスト フィールドにホスト名を入力します。次のように、ホスト名ボックスの [Allow] 正規表現照合でチェックして、正規表現としてホスト名を入力することによって、正規表現照合を使用できます。
- ^example\$ | example:80 | example.cisco.com |
- この場合、example.cisco.com、または example:80 など、(全体一致の場合に) example として誘導されるホストで、ポートによって要求が受け入れられます。正規表現照合がイネーブルの場合、単に "example" のホストにある値は、サブストリングとして "example" が表示される要求 URL に一致し、これは、意図とは異なる場合があります。
- ステップ 5** 完了したら [Save Changes] をクリックし、ポリシーを導入して ACE XML Gateway への変更を有効にします。
- 

## 静的コンテンツ応答の設定

ACE XML Gateway は、ポート上の特定の URL で、静的な応答メッセージの役割を果たすよう、設定できます。他のネットワーク要素（ロード バランサなど）では、このメカニズムを使用して、ACE XML Gateway に対してヘルス チェックを実行できます。HTML ページ、SOAP 応答、テキストだけの応答や、その他の形式で、静的な応答を設定できます。

静的な応答ページについては、次のようないくつかの注意点があります。

- ポートの仮想ホスト設定（つまり、[Listen For] オプションの特定の設定）は、静的なページ応答には影響を及ぼしません。つまり、たとえば、ホスト名 "mygateway" に対する要求だけをリッスンするようポート 8080 を設定する場合、静的コンテンツ ページは、要求されたホスト名に関係なく、ポート 8080 で設定された URL パスに対する要求の役割を果たします。
- ロード バランサは、バランスされるデバイス上のヘルス チェックに HEAD 方式の要求を送信することがあります。ポート上の応答ページは、HEAD 方式の要求および GET 要求に、自動的に応答します。
- ポート上で圧縮をイネーブルにする場合、圧縮は、静的な応答には適用されません。

静的な応答を設定するには、次の操作を実行します。

**ステップ 1** 「ポートのオープン」(P.15-166) に説明されているように、ポート オブジェクトを作成または編集します。

**ステップ 2** [Static Content] メニューから、オプション [serve the following static page on this port] を選択します。

**ステップ 3** [Path] で、応答の送信先の URL パスを指定します。

**ステップ 4** 次の [Content-Type] メニューから、応答のタイプを選択します。

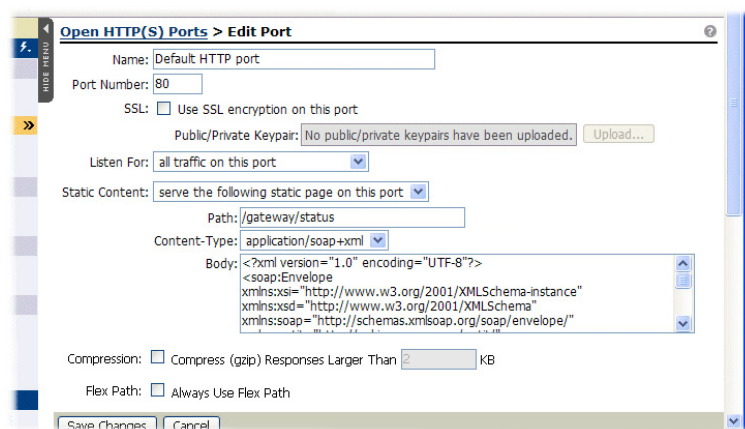
- HTML
- XML
- SOAP
- Text
- または、カスタム応答

該当する応答コンテンツ タイプに適切な本文コンテンツを入力します。たとえば、HTML では、適切なマークアップ タグが応答に含まれることを意味します。

**ステップ 5** [Body] フィールドで、応答メッセージの本文を入力します。

本文には、必要に応じ、選択するコンテンツ タイプに応じたマークアップ タグが含まれる必要があります。たとえば、SOAP メッセージでは、次の図のように、XML 要素およびエンベロープ マークアップが本文に含まれる必要があります。

図 15-1 静的コンテンツ メッセージの設定



**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。

ポリシーの導入時に、次のような ACE XML Gateway アドレスで、ページを使用できます。

`http://xmlgate.example.com:80/gateway/status`

## 応答の圧縮

ACE XML Gateway では、設定されたサイズを超える発信応答を圧縮することによって、トラフィックが最適化されます。ポート上で応答の圧縮がイネーブルの場合、Gateway では、次のサンプルヘッダーのように、要求の HTTP [Accept-Encoding] ヘッダーで圧縮された応答の受信を示すクライアントで、応答が圧縮されます。

```
Accept-Encoding: compress, gzip
```

ACE XML Gateway では、GZIP 圧縮形式を使用して、該当する応答が圧縮されます。

Flex Path 処理が使用される仮想サービスの応答のみ、圧縮が可能です。つまり、Reactor では、応答の圧縮はサポートされません。別な方法で Reactor 処理が許可されるポートで応答の圧縮をイネーブルにする場合（つまり、[Flex Path] オプションがイネーブルの場合）、圧縮で Reactor 処理を使用する仮想サービスかどうかをチェックする必要があります。この場合で、応答の圧縮が使用しているアプリケーションで重要な場合、サービスの "Always use Flex Path" 設定を選択することによって、サービスに Flex Path 処理を使用する必要が生じることがあります。



**(注)** Reactor および Flex Path 処理の詳細については、[第 20 章「Reactor 処理の設定」](#)を参照してください。

ACE XML Gateway では、バックエンドシステムから圧縮された形式ですでに返された応答については、追加の圧縮は適用されません。ACE XML Gateway で圧縮を開始する場合だけ、このオプションをポリシーでイネーブルにする必要があります。



**(注)** Gateway ではなくバックエンドシステムで応答の圧縮を実行するには、要求の Accept-Encoding HTTP ヘッダーでパススルーを設定する必要があります。発信要求に対する仲介を特に設定しない場合、このヘッダーは ACE XML Gateway で要求から削除されます。

応答の圧縮を設定するには、次の操作を実行します。

- ステップ 1** [Open HTTP(S) Ports] ページで、圧縮を設定するポートの [edit] リンクをクリックします。
- ステップ 2** [Compression] チェックボックスをオンに設定します。
- ステップ 3** 必要に応じ、応答の圧縮をトリガーするデフォルトのメッセージサイズを変更します。このサイズより小さい応答は、圧縮されません。デフォルトは 2 キロバイトです。
- ステップ 4** [Save Changes] をクリックした後、ポリシーを導入して Gateway への変更を有効にします。

応答メッセージが圧縮されるときには、イベントが通知レベルでイベント ログに示されます。情報レベルのイベント ログ項目は、メッセージが圧縮しきい値より小さいか大きいを示します。圧縮された応答では、次のように、圧縮の前後でメッセージのサイズがイベント ログに示されます。

```
Returning response 200 for request message to client; 379 bytes  
Compressed Response From 1802 bytes to 379 bytes  
This message will be compressed on its way out  
Message size is larger than or equal to compression threshold (1KB)
```

応答が圧縮されたサービスでメッセージ ロギングがイネーブルの場合、メッセージは圧縮前の形式で記録されます。つまり、メッセージ ログには、メッセージは圧縮された形式では表示されません。

