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。

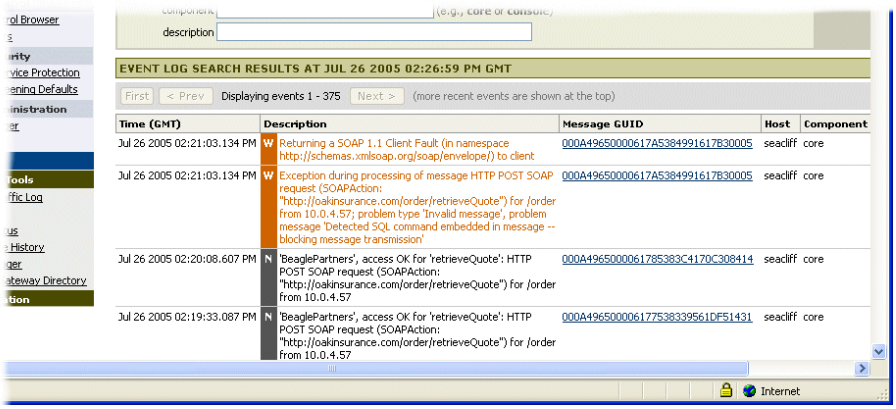
出力例 16-1　SOAP メッセージ

```
<?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。

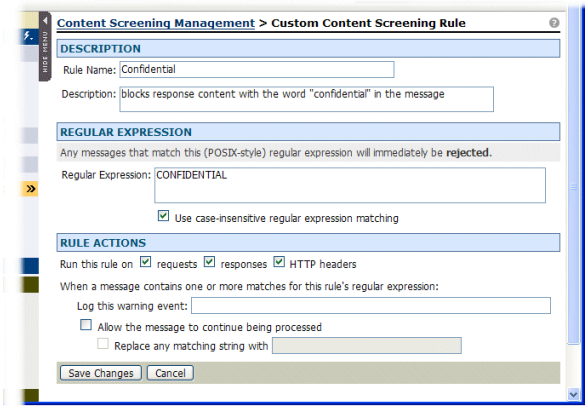
メッセージとステートメントを比較して合致した場合は、そのメッセージは遮断されます。

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。