

## 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ています。

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

EVENT LOG SEARCH RESULTS AT JUL 26 2005 02:26:59 PM GMT

First < Prev Displaying events 1 - 375 Next > (more recent events are shown at the top)

Time (GMT)	Description	Message GUID	Host	Component
Jul 26 2005 02:21:03.134 PM	W Returning a SOAP 1.1 Client Fault (in namespace http://schemas.xmlsoap.org/soap/envelope/) to client	000A49650000617A538491617E30005	seadiff	core
Jul 26 2005 02:21:03.134 PM	W Exception during processing of message HTTP POST SOAP request (SOAPAction: "http://oskinsurance.com/order/retrieveQuote") for /order from 10.0.4.57; problem type "Invalid message", problem message "Detected SQL command embedded in message -- blocking message transmission"	000A49650000617A538491617E30005	seadiff	core
Jul 26 2005 02:20:06.607 PM	N 'BeaglePartners', access OK for 'retrieveQuote': HTTP POST SOAP request (SOAPAction: "http://oskinsurance.com/order/retrieveQuote") for /order from 10.0.4.57	000A4965000061785383C4170C30814	seadiff	core
Jul 26 2005 02:19:33.087 PM	N 'BeaglePartners', access OK for 'retrieveQuote': HTTP POST SOAP request (SOAPAction: "http://oskinsurance.com/order/retrieveQuote") for /order from 10.0.4.57	000A496500006177538395610F51431	seadiff	core

## 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。

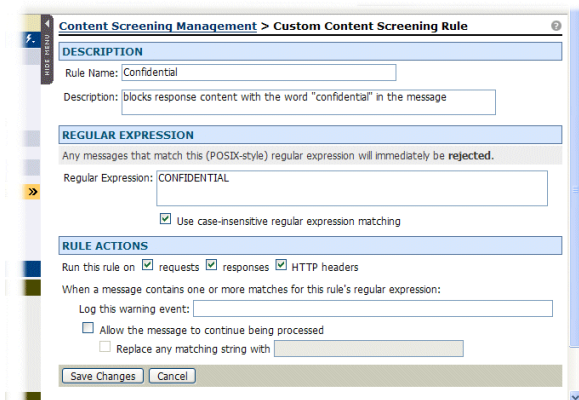
メッセージとステートメントを比較して合致した場合は、そのメッセージは遮断されます。

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規則を設定した例



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。