CHAPTER 7

Video Administration と Video Integration 間の通信のセキュリティ保護

Cisco Unified MeetingPlace Video Integration と Video Administration for Cisco Unified MeetingPlace 間に存在する通信には 2 つの形式があります。1 つは SOAP over HTTP を使用し、もう 1 つは固定 TCP ソケット上の独自の XML プロトコルを使用します。セキュリティ攻撃を防ぐために、これらの 2 つのサーバ間の通信をセキュリティ保護することをお勧めします。

Video Integration では、デフォルトで一組のサーバおよびクライアント証明書がインストールされます。これらの証明書は、OpenSSL を使用して生成される認証局キーによって署名されます。Video Integration のインストール後、SSL はデフォルトでオフになります。

OpenSSL を使用した基本セキュリティ レベルの設定

Video Administration サーバと Video Integration がインストールされた Web Conferencing サーバとの間の通信を暗号化するには、デフォルトでインストールされている OpenSSL 設定ファイルを使用できます。

両方で、次の手順を実行する必要があります。

- Video Administration サーバに基本セキュリティを設定する（P.7-2）
- Cisco Unified MeetingPlace Video Integration サーバに基本セキュリティを設定する（P.7-5）

注意　編集する前に、すべてのファイルをバックアップしておくことが重要です。デフォルト ファイルのバックアップがないと、既知の動作設定に戻すことが困難な場合があります。

Video Administration サーバに基本セキュリティを設定する

ステップ 1　**vcs-core.properties** という名前のファイルを検索します。このファイルは、\Program Files\Cisco\Video Admin\VA\jboss-3.2.5\bin にあります。

ステップ 2　ファイルのバックアップ コピーを作成します。

ステップ 3　Notepad でファイルを開き、**#for MCU proxy XML API** で始まるセクションを検索します。

ステップ 4　vcs-core.properties ファイル内で、#for MCU proxy XML API 行の下に、次の 6 行があることを確認します。これらの行がない場合は、追加します。# で始まっている場合は、# を削除します（#for MCU proxy XML API 行の # はそのままにしておきます）。

```
com.radvision.icm.dciproxy.server.useSystemKeyStore=false
com.radvision.icm.mcuproxy.useSSL=true
com.radvision.icm.dciproxy.server.keystore=..\\server\\all\\conf\\icmservice.keystore
com.radvision.icm.dciproxy.server.keystorePassword=radvision
com.radvision.icm.dciproxy.server.trustKeystore=..\\server\\all\\conf\\icmservice.
keystore
com.radvision.icm.dciproxy.server.trustKeystorePassword=radvision
```

（注）　2 行目は、com.radvision.icm.mcuproxy.useSSL=false から com.radvision.icm.mcuproxy.useSSL=true に変更する必要が生じることがあります（この変更により SSL が有効になります）。

ステップ 5　**server.xml** という名前のファイルを検索します。このファイルは、\Program Files\Cisco\Video Admin\VA\jboss-3.2.5\server\all\deploy\jbossweb-tomcat50.sar にあります。

ステップ 6　ファイルのバックアップ コピーを作成します。

ステップ 7　server.xml ファイルを編集するために Notepad で開き、ファイル内に次の 8 行があることを確認します。これらの行がない場合は、追加します。

```
<Connector port="8443" address="${jboss.bind.address}"
                maxThreads="100" minSpareThreads="5" maxSpareThreads="15"
                scheme="https" secure="true" clientAuth="false"
                keystoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
                keystorePass="radvision"
                truststoreFile="${jboss.server.home.dir}/conf/icmservice.keystore"
                truststorePass="radvision"
           sslProtocol = "TLS" />
```

（注）　通常は、server.xml ファイルを変更する必要はありません。

ステップ 8　**web.xml** という名前のファイルを検索します。このファイルは、Files\Cisco\Video Admin\VA\jboss-3.2.5\server\all\deploy\icmservice.war\WEB-INF にあります。

ステップ 9　ファイルのバックアップ コピーを作成します。

ステップ 10　web.xml ファイルを編集するために Notepad で開き、ファイル内に次の行があることを確認します。これらの行がない場合は、追加します。

```
<!--
  <security-constraint>
   <web-resource-collection>
    <web-resource-name>ScheduleService</web-resource-name>
    <description>ScheduleService</description>
    <url-pattern>/1.0/ScheduleService/*</url-pattern>
<http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>SvrAdmin</role-name>
  </auth-constraint>
  </security-constraint>
<security-constraint>
   <web-resource-collection>
    <web-resource-name>ResourceService</web-resource-name>
    <description>ResourceService</description>
    <url-pattern>/1.0/ResourceService/*</url-pattern>
<http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>SvrAdmin</role-name>
  </auth-constraint>
  </security-constraint>
<security-constraint>
   <web-resource-collection>
    <web-resource-name>ControlService</web-resource-name>
    <description>ControlService</description>
    <url-pattern>/1.0/ControlService/*</url-pattern>
<http-method>POST</http-method>
  </web-resource-collection>
  <auth-constraint>
    <role-name>SvrAdmin</role-name>
  </auth-constraint>
  </security-constraint>
<login-config>
    <auth-method>CLIENT-CERT</auth-method>
    <realm-name>icmservice</realm-name>
  </login-config>
<security-role>
```

```
    <role-name>SvrAdmin</role-name>
  </security-role>
-->
```

ステップ 11 この例の 1 行目と最終行（「<!--」および「-->」）を削除し、保存してファイルを閉じます。

ステップ 12 **login-config.xml** という名前のファイルを検索します。このファイルは、\Program Files\Cisco\Video Admin\VA\jboss-3.2.5\server\all\conf にあります。

ステップ 13 ファイルのバックアップ コピーを作成します。

ステップ 14 login-config.xml ファイルを編集するために Notepad で開き、ファイル内に次の 10 行があることを確認します。これらの行がない場合は、追加します。

```
</application-policy>
<application-policy name="icmservice">
    <authentication>
     <login-module code="com.radvision.icm.service.security.ICMServiceCertLoginModule"
                          flag="required">
        <module-option name="password-stacking">useFirstPass</module-option>
        <module-option
                 name="securityDomain">java:/jaas/SecurityDomainICMService</module-option>
        <module-option name="rolesProperties">roles.properties</module-option>
     </login-module>
    </authentication>
</application-policy>
```

（注）　通常、login-config.xml ファイルを変更する必要はありません。

ステップ 15 **jboss-service.xml** という名前のファイルを検索します。このファイルは、\Program Files\Cisco\Video Admin\VA\jboss-3.2.5\server\all\conf にあります。

ステップ 16 ファイルのバックアップ コピーを作成します。

ステップ 17 jboss-service.xml ファイルを編集するために Notepad で開き、ファイル内に次の 8 行があることを確認します。これらの行がない場合は、追加します。

```
<mbean code="org.jboss.security.plugins.JaasSecurityDomain"
                name="jboss.web:service=SecurityDomain">
            <constructor>
                <arg type="java.lang.String" value="SecurityDomainICMService"/>
            </constructor>
            <attribute name="KeyStoreURL">resource:icmservice.keystore</attribute>
            <attribute name="KeyStorePass">radvision</attribute>
   </mbean>
```

（注）　通常、jboss-service.xml ファイルを変更する必要はありません。

Cisco Unified MeetingPlace Video Integration サーバに基本セキュリティを設定する

ステップ 1　**Cisco Unified MeetingPlace Web Conferencing** マスター サービスを停止します。Cisco Unified MeetingPlace Video サービスが自動的に停止します。

ステップ 2　Windows の [Control Panel] で、**[MeetingPlace Gateways]** をダブルクリックします。

ステップ 3　**[Video Security]** タブをクリックします。

ステップ 4　**[Encrypt Video Administration Communication]** チェックボックスをオンにします。ポートを 8443 に変更するかどうかの問い合せに対して **[Yes]** をクリックします（[Video] タブの [Video Administration Port] の設定が変更されます。この操作は手動で実行することもできます）。

ステップ 5　**[Verify Server Certificates]** チェックボックスはオンにしないでください。

ステップ 6　**[Use Client Certificates]** チェックボックスをオンにします。

ステップ 7　**[OK]** をクリックします。

ステップ 8　Cisco Unified MeetingPlace Web Conferencing マスター サービスを再起動します。Cisco Unified MeetingPlace Video サービスが自動的に再起動します。

ステップ 9　Cisco Unified MeetingPlace Video Integration がインストールされているサーバごとに、ステップ 2 ～ ステップ 8 を繰り返します。