WebView のセキュリティ：Active Directory および Secure Socket Layer

この章では、WebView レポーティングにおける 2 つのセキュリティ機能について説明します。この章の内容は、次のとおりです。

Active Directory について

Microsoft Active Directory(R)（AD）サービスでは、アプリケーション、ファイル、データベース、およびその他のリソースへのアクセス権に関する情報を管理することで、ネットワーク環境における保全性およびセキュリティを確保します。

リリース 7.0(0) の認証モデルは、受け入れられた Microsoft の青写真に従って Active Directory と連携しています。ICM WebView で必須の特権は、AD 標準に従って制限されています。

Active Directory の詳細については、『*Staging and Active Directory Guide for Cisco ICM/IPCC Enterprise & Hosted Editions*』を参照してください。

WebView 管理者のドメイン権限

ICM のセットアップの WebView レポーティング コンポーネントをインストールするには、WebView 管理者は ICM ドメインのローカル管理およびセットアップ権限を持っている必要があります。

その他の設定およびレポーティング機能では、全体的なドメイン管理機能は必要ありません。

WebView ドメイン ローカル セキュリティ グループにおけるユーザ メンバシップ

以前のリリースでは、各ユーザ アカウントは個別に作成されていました。個々のユーザは、ICM コンフィギュレーション マネージャ ユーティリティの User List ツールを使用してユーザ アカウントを作成していました。

これは引き続き、ユーザ アカウントを追加する方法として有効です。

お客様では、任意の AD ユーザを WebView Domain Local Security Group（DLG; ドメイン ローカル セキュリティ グループ）のメンバにすることにより、その AD ユーザに WebView 特権を割り当てることもできるようになりました。

リリース 7.0(0) では、この方法でユーザを追加します。

WebView ユーザ認証モデル

このセクションでは、WebView ユーザ認証が ICM Active Directory モデルとどのように連携しているかを説明します。

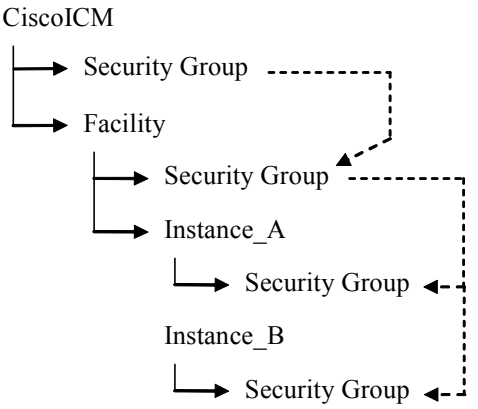
ICM 導入環境における AD Organizational Unit（OU; 組織ユニット）および Domain Local Security Group（DLG; ドメイン ローカル セキュリティ グループ）の階層は、次のとおりです。

```
<Root>
    CiscoICM_<function>
<Facility>
    <facility_name>_<function>
<Instance>
    <facility_name>_<instance_name>_<function>
```

WebView ユーザ アカウントは、それぞれの「<Instance>」OU 内で「<facility_name>_<instance_name>_WebView」DLG のメンバシップを持つ AD 内のアカウントになります。

したがって、リリース 7.0(0) では、WebView ユーザ アカウントの認定要件は、USER_GROUP テーブル内にエントリを持つ Windows NT ドメイン アカウントから、対象のインスタンスに対するそれぞれの Organizational Unit（OU; 組織ユニット）内で WebView Domain Local Security Group（DLG; ドメイン ローカル セキュリティ グループ）のメンバシップを持つ Active Directory アカウントに変わります。

図 9-1　Active Directory



AD 管理者は、標準の Active Directory ツール、User List ツール、または ICM Domain Manager ツールを使用して、任意の AD ユーザを WebView Domain Local Security Group（DLG; ドメイン ローカル セキュリティ グループ）のメンバにすることで、そのユーザに WebView 特権を割り当てることができます。

ファシリティおよび ICM ルートの OU では、WebView DLG のメンバに特殊な特権は割り当てられません。

ユーザ名

WebView にログインするには、次の方法でユーザ名を入力します。

- <domain>\<user>
- <domain>/<user>
- ユーザのプリンシパル名（user@domain.com）
- \user（デフォルトでは、WebView サーバ マシンに関連付けられているドメイン）
- /user（デフォルトでは、WebView サーバ マシンに関連付けられているドメイン）
- user（デフォルトでは、WebView サーバ マシンに関連付けられているドメイン）

SSL について

Secure Socket Layer（SSL）は、Web ブラウザと Web サーバ間のセキュアな通信を可能にするプロトコルです。

Microsoft Internet Information Services（IIS）バージョン 6.0 が動作する Windows 2003 サーバ環境に WebView サーバがインストールされている場合、WebView リリース 7.0(0) では、SSL 3.0 に対して 128 ビットの暗号化をサポートしています。

Windows 2000 サーバおよび IIS 5.0 からアップグレードするお客様では、SSL オプションは ICM のセットアップでグレー表示され、インストール時に無効になります。

ICM のセットアップ時の SSL の設定

ICM のセットアップの［WebView Node Properties］画面には、WebView 用に SSL 3.0 暗号化を設定するためのグループ ボックスが表示されます。

このグループ ボックスには、次の管理項目があります。

- 暗号化（128 ビット）を有効にするためのチェックボックス（デフォルトで選択されています）
- セッションを暗号化するためのチェックボックス

管理者は、ICM のセットアップからデフォルトの設定を変更できます。また、SSL 暗号化ユーティリティを呼び出すことで、いつでも設定を変更することが可能です。このユーティリティの使用法については、「SSL 暗号化ユーティリティ」（P.9-7）を参照してください。

デフォルトをそのまま使用した場合：

- （OpenSSL を使用して）自己署名証明書が生成され、その証明書がローカル マシン ストアにインポートされ、IIS Web サーバ上にインストールされます。

  自己署名証明書とは、外部の認証局による署名のない証明書のことです。これにより、暗号化された Web 接続が確実に行われるようになります。
- WebView　にログインする際に入力される認証情報（ユーザ名およびパスワード）が確実に暗号化されるようになります。

管理者が複数の WebView サーバをインストールする場合は、それぞれを独自の証明書で設定し、SSL を個別に設定できます。

別の証明書がすでにインストールされている場合は、ICM のセットアップではその証明書が置換されることはなく、既存の証明書が上書きされることもありません。

以後、管理者は、企業の認証局または信頼できるサードパーティ認証局（Verisign など）によって署名されている証明書を取得してインストールできます。これを行う場合、管理者は、その認証局によって提示された手順に従うか、または Microsoft Knowledge Base の手順を参照して IIS を直接設定できます。

ユーザのログイン時における変更

このセクションでは、SSL が有効になっているときのレポート ユーザに対する 2 つの小さな変更について説明します。

URL

SSL が認証に対して有効になっている場合、レポート ユーザは `http` で始まる WebView URL を入力します。

SSL がセッション全体に対して有効になっている場合、各ページの URL は `https` で始まります。

セキュリティの警告

レポート ユーザが初めて SSL 対応ページを開いたとき、サーバの証明書を受け付けるように求めるセキュリティの警告が表示されます。

このメッセージのオプションは、[はい]、[いいえ]、または [証明書の表示] です。

- [はい] を選択すると、このブラウザ セッションに関してだけの証明書が受け付けられます（信頼されます）。ユーザが WebView に次回アクセスしたときには、セキュリティの警告が表示されます。
- [いいえ] を選択すると、WebView アクセスが禁止されます。ブラウザには空白ページが表示されます。
- [証明書の表示] を選択すると、証明書をインストールするオプションがある画面が開きます。[インストール] をクリックすると証明書がローカルに保存され、以後、セキュリティの警告が表示されることはありません。

SSL 暗号化ユーティリティ

SSL 暗号化ユーティリティとは、WebView サーバ上の任意のローカル管理者が使用できるスタンドアロン アプリケーションで、ICM のセットアップを起動せずに SSL 設定の変更ができます。

ユーティリティの起動

WebView サーバがディストリビュータ アドミン ワークステーション上にある場合、管理者はこのユーティリティを AW プログラム グループから実行できます。

WebView サーバが別のマシン上にある場合、管理者はこのユーティリティを WebView サーバから実行できます（/icm/bin/sslutil.exe）。

ユーザ インターフェイス

SSL 暗号化ユーティリティには、次の 2 つのタブがあります。

- ［Configuration］タブには、使用している環境で検出された ICM Web ベースのアプリケーションに対して SSL が現在有効になっているかどうかが示されます。これらのアプリケーションは、WebView、Dynamic Reskilling/WebConfig、および Internet Script Editor です。

  このタブで変更を行うには、ICM インスタンスを選択します。次に、そのインスタンスに対して［SSL 3.0 Encryption］を選択または選択解除します。

  WebView に対して［Enable Encryption］を選択すると、2 つのオプション ボタン、［Authentication］と［Session］が有効になります。

  - ［Authentication］では、ユーザ名およびパスワードがあるログイン ページが暗号化されますが、セッションは暗号化されません。
  - ［Session］では［Authentication］が想定され、ユーザと WebView サーバ間で送信されるすべてのページ（クエリー、レポート、ヘルプなど）が暗号化されます。
- ［Certificate Authentication］タブには 1 つのボタン、［Execute］があります。

  これをクリックすると、証明書があらかじめ作成されているかどうかが確認されます。証明書が存在する場合、管理者に上書きするか、あるいは実行を取り消すよう求めるメッセージが表示されます。

  証明書が存在しない場合、ユーティリティによって <installDrive>\icm\ssl\host.crt 内に自己署名証明書が作成されます。

変更を適用すると、adminui.properites 内の暗号化の値が（none、auth、または session に）更新されます。

変更を有効にするために管理者が IIS を再起動する必要はありません。