APPENDIX **B**

Cisco VXC Manager のセキュリティについて

この付録には、Cisco VXC Manager のセキュリティに関する詳細情報が記載されています。

Cisco VXC Manager では、不正な Cisco VXC Manager インストールがデバイスを管理することを防止するよう Device Manager を設定できます。[Enable Device Security] オプションを設定すると、Cisco VXC Manager Agent および Cisco VXC Manager Web サービスは 1 対 1 の関係になります。この関係では、デバイスと Web サービスの両方が共通の固有のセキュリティ証明書を共有します。Cisco VXC Manager の要求を処理する前に、デバイスの Cisco VXC Manager Agent が証明書を確認します。Web サービスの証明書が Cisco VXC Manager Agent の証明書と一致する場合、Cisco VXC Manager Agent は、デバイスによる要求された関数または命令の実行を許可します。証明書が一致しない場合、Cisco VXC Manager Agent は、デバイスによるどの要求への対応も防止します。

（注） Cisco ThreadX デバイスではデバイス セキュリティはサポートされません。

注意 **デバイス セキュリティをイネーブルにする場合**：デバイス セキュリティをイネーブルにする場合は、必ず証明書番号を書き留めて、安全な場所に保持してください。何らかの理由で Cisco VXC Manager インストールが破損して、Cisco VXC Manager の再インストールが必要になった場合は、新しい証明書番号を取得します。ただし、元の証明書番号がないと、デバイスを管理できません。Cisco VXC Manager では、セキュリティ証明書を新しい証明書に変更するか、古い証明書を復元するオプションが示されます。

デバイス セキュリティをディセーブルにする場合：デバイス セキュリティをディセーブルにすると、既存のデバイスは、次のチェックインまでセキュリティ証明書を解放しません。サーバは証明書を提示しなくなるため、証明書を更新または再検出できません。間隔の間にチェックインする必要があります（つまり、プッシュではなくプル）。

Cisco VXC Manager のセキュリティをイネーブルにするには、次の手順を実行します。

デバイスでの証明書のインポート

Cisco VXC Manager のコンポーネント間のセキュアな通信を開始する前に、証明書をデバイスにインポートします。証明書をインポートするには、2 つの方法があります。1 つは、証明書が含まれるパッケージを作成して配置する方法です。もう 1 つは、証明書が含まれる DDC を作成して、DDC が証明書をすべてのデバイスに自動的に配置できるようにする方法です。インポート手順は、デバイスの OS によって異なります。

ヒント　証明書認証：証明書パッケージをデバイスに配置した後で、サーバで証明書を認証する必要があります。サーバとクライアント間の証明書を認証するための基準は、証明書を発行した認証局、証明書の作成日、および証明書の名前に基づいています。証明書認証が正常に行われると、サーバとクライアントは相互のセキュアな通信を開始します。

WTOS

WTOS が実行されているデバイスで証明書をインポートするには、（Cisco VXC Manager で登録するその他のパッケージと同様に）2 つのパッケージを登録する必要があります。1 つのパッケージは、証明書を追加するためのもので、もう 1 つは、証明書をデバイスから削除するためのパッケージです。証明書の追加または削除を行う場合は、wnos.ini ファイルを変更して、2 つの別個のパッケージを登録する必要があります。

証明書パッケージのフォルダ構造は VXC-M Package¥CADeployment で、CADeployment という名前のフォルダには wnos という名前のフォルダが 1 つ含まれています。wnos という名前のフォルダには、cacerts という名前のフォルダと wnos.ini という名前のファイルが格納されています。cacerts という名前のフォルダには実際の証明書ファイルが含まれています。

次に、証明書を追加するための wnos.ini の例を示します。

```
# Bypass the user log in to the local device
signon=0
# Set the Privilege to high
Privilege=high
# Command to Import the certificate to WTOS devices
AddCertificate= CA certificate file name
```

次に、証明書を削除するための wnos.ini の例を示します。

```
# Bypass the user log in to the local device
signon=0
# Set the Privilege to high
Privilege=high
# Command to delete the certificate in WTOS devices
DelCertificate= CA certificate file name
```

次に、WTOS デバイスに証明書を追加するための rsp ファイルの例を示します。

```
[Version]
Number=CADeployment
Description=CA Certificate Deployment
OS=BL
Category=Images
ImageSize=
[Script]
```

Windows XPe

（注）　この項は、Cisco VXC デバイスには適用されません。サードパーティ クライアントの管理にのみ適用されます。

Windows XPe が実行されているデバイスで証明書をインポートするには、（Cisco VXC Manager で登録するその他のパッケージと同様に）2 つのパッケージを登録する必要があります。1 つのパッケージは、証明書を追加するためのもので、もう 1 つは、証明書をデバイスから削除するためのパッケージです。

証明書パッケージを追加するためのフォルダ構造は「¥VXC-M Packages¥CertificateAdd」で、フォルダ「¥VXC-M Packages¥CertificateAdd」には別の「CertificateAdd」フォルダとファイル「CertificateAdd.rsp」が含まれています。フォルダ「CertificateAdd¥ CertificateAdd」には、「root_cert.pem」という名前の実際の証明書ファイルが格納されます。

次に、Windows XPe が実行されているデバイスに証明書を追加するための rsp ファイルの例を示します。

```
[Version]
Number=CertificateAdd
Description=Installs a root CA Certificate
OS=XP
Category=Other Packages
[Script]
;
;-------------------------------------------------------------------------
;Check Operating System and Confirm free space
;-------------------------------------------------------------------------
CO "XP"
CF "C" "200"
;-------------------------------------------------------------------------
;Query User and Lockout
;-------------------------------------------------------------------------
LU
;-------------------------------------------------------------------------
;Copy over certificate file
;-------------------------------------------------------------------------
SF "<regroot>¥root_cert.pem" "c:¥Program Files¥VXC-M¥root_cert.pem"
;-------------------------------------------------------------------------
;Update Registry & End Lockout
;-------------------------------------------------------------------------
SV "HKEY_LOCAL_MACHINE¥SOFTWARE¥RAPPORT¥HAGENT¥CAValidation" "1" "REG_DWORD"
SV "HKEY_LOCAL_MACHINE¥SOFTWARE¥RAPPORT¥HAGENT¥CAPath" "c:¥Program
Files¥VXC-M¥root_cert.pem"
EL
```

証明書パッケージを削除するためのフォルダ構造は「¥VXC-M Packages¥CertificateRemove」で、フォルダ「¥VXC-M Packages¥CertificateRemove」には別の「CertificateRemove」フォルダとファイル「CertificateRemove.rsp」が含まれています。

次に、Windows XPe が実行されているデバイスから証明書を削除するための rsp ファイルの例を示します。

```
[Version]
Number=CertificateRemove
Description=Removes a root CA Certificate
OS=XP
Category=Other Packages
[Script]
;;
```

```
;--------------------------------------------------------------------------
;Check Operating System and Confirm free space
;--------------------------------------------------------------------------
CO "XP"
CF "C" "200"
;--------------------------------------------------------------------------
;Query User and Lockout
;--------------------------------------------------------------------------
LU
;--------------------------------------------------------------------------
;Delete certificate file
;--------------------------------------------------------------------------
DF "c:¥Program Files¥VXC-M¥root_cert.pem"
;--------------------------------------------------------------------------
;Update Registry & End Lockout
;--------------------------------------------------------------------------
DR "HKEY_LOCAL_MACHINE¥SOFTWARE¥RAPPORT¥HAGENT¥CAValidation"
DR "HKEY_LOCAL_MACHINE¥SOFTWARE¥RAPPORT¥HAGENT¥CAPath"
EL
```

注意　デバイス レジストリで CA 検証フラグが 1 に設定されている場合、証明書の検証が行われます。このフラグが 1 に設定されていない場合は、クライアント側では証明書の検証は行われません。

Windows CE .NET

（注）　この項は、Cisco VXC デバイスには適用されません。サードパーティ クライアントの管理にのみ適用されます。

Windows CE .NET が実行されているデバイスで証明書をインポートするには、（Cisco VXC Manager で登録するその他のパッケージと同様に）証明書ファイルが含まれているパッケージを登録する必要があります。たとえば、証明書パッケージのフォルダ構造は「VXC-M Package¥CE_CertInstall」で、フォルダ「CE_CertInstall」には、「CE_CertInstall」という名前のフォルダが 1 つとファイル「CE_CertInstall.rsp」が含まれています。フォルダ「CE_CertInstall¥ CE_CertInstall」には、「CRC.txt」という名前のテキスト ファイルと「root_cert.cer」という名前の実際の証明書ファイルの 2 つのファイルが格納されています。

次に、Windows CE が実行されているデバイスに証明書をインストールするための rsp ファイルの例を示します。

```
[Version]
Number=CE_CertInstall
Description=Installs a Certificate to a CE .NET device
OS=CEN
Category=Other Packages
[Script]
;
;--------------------------------------------------------------------------
;Check Operating System and Confirm free space
;--------------------------------------------------------------------------
CO "CEN"
;--------------------------------------------------------------------------
;Query User and Lockout
;--------------------------------------------------------------------------
LU
```

```
;-------------------------------------------------------------------------
;Update Registry & End Lockout
;-------------------------------------------------------------------------
SV "HKEY_LOCAL_MACHINE¥SOFTWARE¥Cisco¥AutoLoadCert¥AutoLoadCert" "1" "REG_DWORD"
SV "HKEY_LOCAL_MACHINE¥SOFTWARE¥Cisco¥AutoLoadCert¥CertFiles¥Root" "root_cert.cer"
SF "CECert" "<regroot>¥root_cert.cer" "¥flash1¥root_cert.cer"
EL
RB
```

次に、Windows CE .NET デバイスの証明書の検証をオンまたはオフにするための .rsp ファイルの例を示します。

```
[Version]
Number=CE_CertValOff
Description=Turns Certificate Validation OFF for a CE .NET device
OS=CEN
Category=Other Packages
[Script]
;DATE: 26 Sept 2008
;
;-------------------------------------------------------------------------
;Check Operating System and Confirm free space
;-------------------------------------------------------------------------
CO "CEN"
;-------------------------------------------------------------------------
;Query User and Lockout
;-------------------------------------------------------------------------
LU
;-------------------------------------------------------------------------
;Update Registry & End Lockout
;-------------------------------------------------------------------------
SV "HKEY_LOCAL_MACHINE¥SOFTWARE¥RAPPORT¥HAGENT¥CAValidation" "0" "REG_DWORD"
EL
RB
```

セキュアな通信（HTTPS）の使用

Cisco VXC Manager では、Cisco VXC Manager のコンポーネント間のセキュアな HTTPS 通信がサポートされます。

セキュアな通信は、次の 2 つの方法で開始できます。

- HAgent で開始される HTTPS 通信
- Cisco VXC Manager Administrator Console で開始される HTTPS 通信

HAgent で開始される HTTPS 通信

HAgent は、クライアントデバイスの起動中に HServer との通信を開始できます。クライアントの HAgent が起動すると、DHCP サーバまたはプロキシ サーバから次の情報を要求します。

- サーバ IP アドレス
- 通信に使用される HTTPS ポート番号

HAgent が DHCP オプション タグから HTTPS ポート番号を取得できる場合は、IP アドレスとポート番号を使用して、HTTPS を介して HServer と通信します。

HAgent が DHCP オプション タグから HTTPS ポート番号を取得できない場合は、次の順序に従います。

1. HAgent は、ポート 443 と 8443 を使用して HTTPS を介して通信しようとします。
2. HAgent が HTTPS を介して通信できない場合は、ポート 80 と 280 を使用して HTTP を介して接続しようとします。
3. HAgent が HServer との通信を正常に開始した場合は、使用される通信メカニズム、IP アドレス、およびポート番号をキャッシュに入れて、後続の要求にその情報を使用します。
4. 起動中に HTTPS 通信が失敗した場合、HAgent は HTTPS プロトコルを再試行しません。

Cisco VXC Manager Administrator Console で開始される HTTPS 通信

Administrator Console が、HServer との通信に使用するポート番号とプロトコルを判別できるようにネットワークを設定できます。

ポート番号の判別

Administrator Console が通信用のポート番号を判別できるようにするには、次のようにします。

手順

ステップ 1　必要なポート番号を使用して HServer をホストする IIS を設定します。

ステップ 2　IIS および WWW サービスを停止します。

ステップ 3　HServerInit サービスを起動します。

Administrator Console が開始すると、HServer との通信に使用するポート番号と IP アドレスを取得するためにデータベースに照会します。¥

プロトコルの判別

Administrator Console が通信用のプロトコルを判別できるようにするには、次のようにします。

手順

ステップ 1　HServer をホストする IIS を TCP、SSL、または TCP、および SSL ポートとバインドします。

ヒント　SSL ポートの場合は、証明書をインストールする必要があります。

ステップ 2　IIS および WWW サービスを停止します。

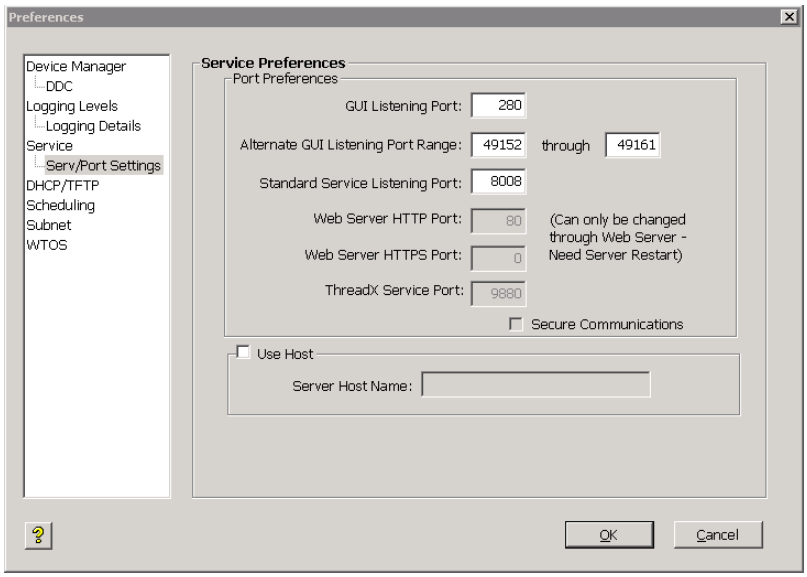
ステップ 3　HServerInit サービスを起動します。

ポート番号と IP アドレスは、Cisco VXC Manager Database に格納されます。

要求が SSL を介して行われた場合は、Cisco VXC Manager 設定全体がセキュアに設定されます。

Administrator Console での設定は必要ありませんが、通知のために [Secure Communications] チェックボックスが [Serv/Port Settings Preferences] ダイアログボックスに表示されます。

図 B-1　Serv/Port Settings Preferences



IIS で SSL ポートが設定されている場合は、[Secure Communications] チェックボックスはオンになります。設定されていない場合はオフになります。

セキュアな通信を開始する前に、すべての設定が行われていることを確認します。

ヒント　セキュアな通信のフラグは、リモート リポジトリとマスター リポジトリの両方に適用されます。

Cisco VXC Manager デバイス セキュリティのイネーブル化

Cisco VXC Manager では、不正な Cisco VXC Manager インストールがデバイスを管理することを防止するよう Device Manager を設定できます。

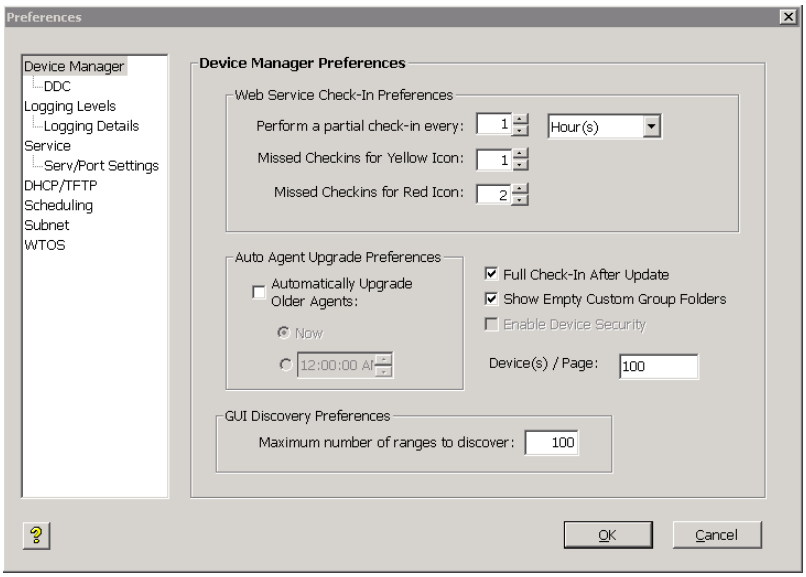
デバイス セキュリティをイネーブルにするには、次のようにします。

手順

ステップ 1　Administrator Console のツリー ペインで、[Configuration Manager] を展開して、[Preferences] を選択して、[Cisco VXC Manager Preferences] のカテゴリが表示された詳細ペインを表示します。

ステップ 2　[Device Manager Preferences] をダブルクリックして、[Device Manager Preferences] ダイアログボックスを開きます。

図 B-2　Device Manager Preferences



ステップ 3　[Enable Device Security] を選択して [OK] をクリックしてから、[Yes] をクリックして確認します。

これ以降、デバイスがセキュリティ証明書をまだ保持していない場合は、次回のデバイスの再検出またはチェックイン時に、Cisco VXC Manager は、デバイスの Cisco VXC Manager Agent と Cisco VXC Manager インストール間の 1 対 1 の関係を確立します。この関係は、不正な Cisco VXC Manager インストールがデバイスを管理することを防止します。

ヒント　デバイス セキュリティを適用すると、Cisco VXC Manager は、Web サービスと Cisco VXC Manager Agent 間の通信をすべて自動的に暗号化します。ただし、暗号化は、デバイス セキュリティとは関係なくオンにできます（「Service Preferences」（P.7-17）を参照）。

Cisco VXC Manager セキュリティ証明書の変更

Cisco VXC Manager セキュリティ証明書を変更する前に、デバイス セキュリティをディセーブルにしたことを確認してから、Cisco VXC Manager セキュリティ証明書を変更してください。証明書番号の変更後に、デバイス セキュリティを再度イネーブルにできます（「Cisco VXC Manager デバイス セキュリティのイネーブル化」（P.B-7）を参照）。

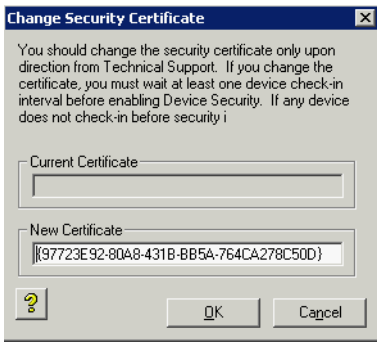
Cisco VXC Manager 証明書番号を変更するには、この手順を使用します（証明書を新しい番号に変更するか、古い証明書を復元できます）。

Cisco VXC Manager セキュリティ証明書を変更するには、次のようにします。

手順

ステップ 1　[Configuration Manager] を展開して、[Licensing] ノードを右クリックし、[New] > [Certificate] を選択して [Change Security Certificate] ダイアログボックスを開きます（Cisco VXC Manager によって、[New Certificate] ボックスに新しい証明書番号が作成されることに注意してください）。

図 B-3　Change Security Certificate



ヒント　デバイス セキュリティをディセーブルにしていない場合は、警告メッセージが表示されます。

ステップ 2　新しい証明書を受け入れるかどうかによって、次のいずれかを実行します。

- 受け入れる場合は、[OK] をクリックします。この手順はこれで完了です。
- 受け入れない場合は、復元するセキュリティ証明書を入力して（デバイスは前の Cisco VXC Manager インストールのこの証明書を共有している可能性があります。セキュリティ証明書を復元することによって、デバイスのコントロールを再度取得します）、[OK] をクリックします。

注意　セキュリティ証明書を変更する前に、すべてのデバイスがチェックインして、現在の証明書を解放できるように、1 回のチェックイン間隔の間待機します。現在の証明書を使用するデバイスが、この時間内にチェックインしない場合に、新しい証明書のセキュリティをイネーブルにすると、チェックインしなかったデバイスは管理不能になります（まだ古い証明書を保持しているため）。