Cisco Prime Infrastructure サーバの強化

この付録では、Prime Infrastructure サーバの強化に関するチェックリストについて説明します。理想的には、サーバの強化の目的は、他の形式の保護を使用せずにサーバをインターネットに公開しておくことです。ここでは、公開する一部のサービスおよびプロセスが正常に機能することが求められる、Prime Infrastructure の強化について説明します。これは Prime Infrastructure のベスト プラクティスとして考えてください。Prime Infrastructure の強化には、不要なサービスの無効化、レジストリ キー エントリの削除と変更、ならびにファイル、サービスおよびエンド ポイントに対する適切な制限的権限の適用などが含まれます。

この付録の内容は、次のとおりです。

- 「Prime Infrastructure のパスワード処理」（P.B-11）
- 「SSL 認証の設定」（P.B-11）

Prime Infrastructure のパスワード処理

[Administration] > [AAA] > [Local Password Policy] ページで [Local Password Policy] パラメータを設定して追加の認証を設定できます。設定を有効にするには、チェックボックスをオンにします。

追加の認証では、次の設定が追加されます。

- パスワードの最小長が設定できます。
- ユーザ名またはユーザ名を逆にしたものをパスワードの一部として使用できるかどうかを設定できます。
- パスワードに、「cisco」、「ocsic」またはその中に大文字を使用した異形や、「i」の代わりに「1」、「|」、または「!」、「o」の代わりに「0」、「s」の代わりに「$」を使用したものを含められるかどうかを設定できます。
- ルート パスワードに **public** という語を使用できるかどうかを設定できます。
- パスワード内に 1 つの文字を 3 回よりも多く連続して繰り返せるかどうかを設定できます。
- パスワードに、大文字、小文字、数字、特殊文字の中から 3 種類の文字を含める必要があるかどうかを設定できます。

SSL 認証の設定

Secure Sockets Layer（SSL）認証は、Web サーバとブラウザ間のセキュアなトランザクションを保証するために使用されます。DoD 証明書をインストールすると、Web ブラウザでアイデンティティを信頼し、米国国防総省（DoD）によって認証されたセキュアな通信を提供できるようになります。

これらの証明書は、サーバまたは Web サイトのアイデンティティを確認するため、また SSL で使用する暗号キーを生成するために使用されます。この暗号化により、サーバとクライアント間で受け渡される情報が保護されます。

ここでは、次の内容について説明します。

- 「SSL クライアント認証の設定」（P.B-12）
- 「SSL サーバ認証の設定」（P.B-13）

SSL クライアント認証の設定

DoD 証明書を使用して SSL クライアント証明書の認証を設定するには、次の手順に従います。

（注） 前提条件として、SSL 証明書を作成するには、Keytool が必要です（JDK で使用可能）。KeyTool は、キーストアおよび証明書を管理するために使用するコマンドライン ツールです。

ステップ 1　次のコマンドを使用して、SSL クライアント証明書を作成します。

```
% keytool -genkey -keystore nmsclientkeystore -storetype pkcs12 -keyalg RSA -keysize 2048
-alias nmsclient -dname "CN=nmsclient, OU=WNBU, O=Cisco, L=San Jose, ST=CA, C=US"
-storepass nmskeystore
```

（注） キー アルゴリズムに RSA、キー サイズに 1024 または 2048 を指定します。

ステップ 2　次のコマンドを使用して、証明書署名要求（CSR）を生成します。

```
% keytool -certreq -keyalg RSA -keysize 2048  -alias nmsclient -keystore nmsclientkeystore
-storetype pkcs12 -file <csrfilename>
```

（注） キー アルゴリズムに RSA、キー サイズに 1024 または 2048 を指定し、証明書ファイル名を指定します。

ステップ 3　生成された CSR ファイルを DoD に送信します。DoD によって対応する署名証明書が発行されます。

（注） CSR 応答は、dod.p7b ファイルによって行われます。また、ユーザはルート CA 証明書も受信します。

（注） PKCS7 符号化された証明書を必ず取得するようにします。認証局では、PKCS7 符号化された証明書の取得のオプションを提供しています。

ステップ 4　次のコマンドを使用して、キーストアに CSR 応答をインポートします。

```
% keytool -import dod.p7b -keystore nmsclientkeystore -storetype pkcs12
-storepass nmskeystore
```

ステップ 5　受信したルート CA 証明書の形式が base 64 符号化であることを確認します。base 64 符号化でない場合、OpenSSL コマンドを使用して base 64 符号化形式に変換します。

```
% openssl x509 -in rootCA.cer -inform DER -outform PEM -outfile rootCA.crt
% openssl x509 -in DoD-sub.cer -inform DER -outform PEM -outfile rootCA.crt
```

（注）　受信したルート CA 証明書と下位の証明書の両方を変換します。

ルート CA 証明書と下位の証明書の両方を受信した場合は、次のコマンドを使用してこれらをバンドルする必要があります。

```
% cat DoD-sub.crt > ca-bundle.crt
% cat DoD-rootCA.crt >> ca-bundle.crt
```

ステップ 6　証明書を使用して SSL クライアント認証を設定するには、<NCS_Home>/webnms/apache/ssl/backup/ フォルダにある、**ssl.conf** ファイル内の Apache の SSL クライアント認証を有効にする必要があります。

```
SSLCACertificationPath conf/ssl.crt
SSLCACertificationFile conf/ssl.crt/ca-bundle.crt
SSLVerifyClient  require
SSLVerifyDepth 2
```

（注）　SSLVerifyDepth は、証明書チェーンのレベルにより異なります。ルート CA 証明書を 1 つだけ保持する場合は、これを 1 に設定する必要があります。証明書チェーンを保持する場合（ルート CA および下位 CA）、これを 2 に設定する必要があります。

ステップ 7　Prime Infrastructure に DoD ルート CA 証明書をインストールします。

ステップ 8　ブラウザに nmsclientkeystore をインポートします。

SSL サーバ認証の設定

DoD 証明書を使用して SSL サーバ証明書を設定するには、次の手順に従います。

ステップ 1　証明書署名要求（CSR）を生成します。

```
% keyadmin -newdn  genkey <csrfilename>
```

ステップ 2　生成された CSR ファイルを DoD に送信します。DoD によって対応する署名証明書が発行されます。

（注）　CSR 応答は、dod.p7b ファイルによって行われます。また、ユーザはルート CA 証明書も受信します。

（注）　PKCS7 符号化された証明書を必ず取得するようにします。認証局では、PKCS7 符号化された証明書の取得のオプションを提供しています。

ステップ 3　KeyTool で次のコマンドを使用して、署名証明書をインポートします。

```
% keyadmin -importsignedcert <dod.p7>
```

（注）　Prime Infrastructure は /opt/CSCOncs/httpd/conf/ssl.crt で自己署名証明書を保存します。インポートした証明書 / キーは /opt/CSCOncs/migrate/restore で保存されます。