Web UI のセキュリティ強化

この付録では、次の項について説明します。

Web UI のセキュリティ強化

HTTPS を使用してセキュアソケットレイヤ（SSL）プロトコルで接続すると、Web UI は Java 仮想マシン（JVM）のデフォルトの暗号を使用します。これらの暗号には通常、弱い暗号セッションキーが含まれており、システムセキュリティに影響を与える可能性があります。システムを強化する場合は、次のように暗号を調整します。

（注） Cisco Prime Network Registrar 10.1 のデフォルトのインストールは、Transport Layer Security（TLS）1.2 で動作します。必要に応じて、古い TLS のバージョンで動作するように構成を変更できます。

ステップ 1 Cisco Prime Network Registrar インストールフォルダの *install-path*/tomcat/conf フォルダにある **server.xml** ファイルを開きます。

ステップ 2 次の例に示すように、HTTPS コネクタ文に暗号文を追加し、許可される暗号をリストします。

（注） **port**, **keystoreFile**, and **keystorePass** の値は、システムで設定した値と一致する必要があります。

```
<Connector port="8443"
maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
maxHttpHeaderSize="8192"
enableLookups="false"
disableUploadTimeout="true"
acceptCount="100" scheme="https" secure="true"
clientAuth="false"
```

Web UI のセキュリティ強化

```
ciphers="TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,

 TLS_RSA_WITH_AES_128_GCM_SHA256, TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256,
 TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
 TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384, TLS_RSA_WITH_AES_256_GCM_SHA384,
 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
 TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
 TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256,
 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,
 TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA,
 TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384,
 TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA"

 keystoreFile="conf/.keystore"

 sslProtocol="TLSv1.2"

 sslEnabledProtocols="TLSv1.2"/>
```

ステップ 3 Cisco Prime Network Registrar を再起動して、変更を有効にします。