CHAPTER 7

# セキュアなクライアント通信の設定

この章では、クライアント/サーバ通信を保護するように Cisco Data Center Network Manager（DCNM）を設定する方法について説明します。

この章では、次の内容について説明します。



## セキュアなクライアント通信に関する情報

ここでは、次の内容について説明します。



### クライアント/サーバ通信の暗号化

デフォルトでは、Cisco DCNM のクライアントとサーバ間の通信は暗号化されませんが、セキュアなクライアント/サーバ通信をイネーブルにすることができます。この通信では、Secure Sockets Layer（SSL）3.0 プロトコルをベースにしたプロトコルである Transport Layer Security（TLS）を使用します。具体的には、セキュアなクライアント通信をイネーブルにすると、Cisco DCNM クライアントと Cisco DCNM サーバの EJB ポートの間の通信が暗号化されます。

セキュアなクライアント通信をイネーブルにしても、ユーザがダウンロード、インストール、および Cisco DCNM クライアントへのログインを行う方法には影響しません。

### クライアント/サーバ通信に対するファイアウォールのサポート

Cisco DCNM は、ファイアウォールなどのゲートウェイ デバイスをまたぐクライアント/サーバ接続をサポートしていますが、クライアントが開始する必要がある Cisco DCNM サーバへの接続を許可するには、すべてのゲートウェイ デバイスを設定する必要があります。ゲートウェイ デバイスがトラフィックの到達を許可する必要がある Cisco DCNM サーバのポートについては、表 1-1 を参照してください。

デフォルトでは、Cisco DCNM サーバの起動時に、ランダムなポート番号がセカンダリ サーバのバインド ポートに割り当てられます。ゲートウェイ デバイスをまたぐクライアント/サーバ通信をサポートするには、セカンダリ サーバのバインド サービスで特定のポートが使用されるように、Cisco DCNM サーバを設定する必要があります。

# セキュアなクライアント通信の設定

ここでは、次の内容について説明します。



## クライアント/サーバ間の暗号化通信のイネーブル化

TLS をイネーブルにすると、クライアント/サーバ通信を暗号化できます。

Cisco DCNM の導入においてクラスタ化されたサーバを配置した場合は、クラスタ内の各サーバに対して次の手順を実行する必要があります。

### 手順の詳細

**ステップ 1**　Cisco DCNM サーバを停止します。サーバ クラスタでセキュアなクライアント通信をイネーブルにする場合は、stop-dcnm-cluster スクリプトを使用します。単一サーバを導入する場合は、次のいずれかを実行します。

- Microsoft Windows：[Start] > [All Programs] > [Cisco DCNM Server] > [Stop DCNM Server] を選択します。
- RHEL：Stop_DCNM_Server スクリプトを使用します。

Cisco DCNM の停止の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

**ステップ 2**　テキスト エディタで、次の場所にある jboss-service.xml ファイルを開きます。

*INSTALL_DIR*¥dcm¥jboss-4.2.2.GA¥server¥dcnm¥deploy¥ejb3.deployer¥META-INF¥jboss-service.xml

*INSTALL_DIR* は、Cisco DCNM のインストール ディレクトリです。Microsoft Windows のデフォルトのインストール ディレクトリは、C:¥Program Files¥Cisco Systems です。RHEL システムのデフォルトのインストール ディレクトリは、/usr/local/cisco です。

**ステップ 3**　ファイル内で次のセクションを探します。見つかったセクションが、次の各行と正確に一致していることを確認します。

```
<!--mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
  <depends>jboss.aop:service=AspectDeployer</depends>
  <attribute
name="InvokerLocator">sslsocket://${jboss.bind.address}:${cisco.dcnm.remoting.sslejbport:3
843}</attribute>
  <attribute name="Configuration">
    <handlers>
      <handler
subsystem="AOP">org.jboss.aspects.remoting.AOPRemotingInvocationHandler</handler>
```

```
    </handlers>
  </attribute>
</mbean-->
```

このセクションは、XML の標準のコメント記号（<!-- および -->）を使用してコメント アウトされています。

**ステップ 4**　次のようにして、このセクションをアンコメントします。

**a.** このセクションの先頭の行で、次の 3 文字を「mbean」の前から削除します。

```
!--
```

変更後、この行は次のようになります。

```
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
```

**b.** このセクションの最後の行で、次の 2 文字を「mbean」の後ろから削除します。

```
--
```

変更後、この行は次のようになります。

```
</mbean>
```

**ステップ 5**　jboss-service.xml ファイルを保存して閉じます。

**ステップ 6**　テキスト エディタで、次の場所にある jboss-service.xml ファイルを開きます。

*INSTALL_DIR*¥dcm¥jboss-4.2.2.GA¥server¥dcnm¥conf¥jboss-service.xml

**（注）**　このファイルは、ステップ 2 で開いた jboss-service.xml ファイルとは異なります。

**ステップ 7**　ファイル内で次のセクションを探します。

```
cisco.dcnm.remoting.transport=socket
cisco.dcnm.remoting.port=3873
cisco.dcnm.remoting.ejbport=3873
cisco.dcnm.remoting.sslejbport=3843
cisco.dcnm.remoting.client.invokerDestructionDelay=0
```

最後の 3 行の行末に記述されているポート番号は、Cisco DCNM サーバのインストール時にデフォルトのポート番号を変更したかどうかによって、この例とは異なる場合があります。

**ステップ 8**　cisco.dcnm.remoting.transport の値を sslsocket に変更します。変更後、この行は次のようになります。

```
cisco.dcnm.remoting.transport=sslsocket
```

**ステップ 9**　cisco.dcnm.remoting.port の値を、cisco.dcnm.remoting.sslejbport に指定されている値と一致するように変更します。たとえば、Cisco DCNM サーバがデフォルトの SSL ポートを使用するように設定されている場合、cisco.dcnm.remoting.sslejbport の値は 3843 であるため、変更後のこの行は次のようになります。

```
cisco.dcnm.remoting.port=3843
```

**ステップ 10**　cisco.dcnm.remoting.client.invokerDestructionDelay の値を 30000 に変更します。変更後、この行は次のようになります。

```
cisco.dcnm.remoting.client.invokerDestructionDelay=30000
```

**ステップ 11**　jboss-service.xml ファイルを保存して閉じます。

**ステップ 12**　次のいずれかを行います。

- Cisco DCNM の導入においてクラスタ化されたサーバを配置した場合は、クラスタ内の各サーバに対してこの手順を繰り返し実行します。その後、各サーバを起動します（マスター サーバを最初に起動します）。各サーバの起動間隔は、1 分以上あけてください。
- 単一サーバを導入する場合は、Cisco DCNM サーバを起動します。

単一の Cisco DCNM または Cisco DCNM サーバのクラスタの起動の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

# クライアント/サーバ間の暗号化通信のディセーブル化

セキュアなクライアント通信はディセーブルにできます。

Cisco DCNM の導入においてクラスタ化されたサーバを配置した場合は、クラスタ内の各サーバに対して次の手順を実行する必要があります。

### 手順の詳細

**ステップ 1**　Cisco DCNM サーバを停止します。サーバ クラスタでセキュアなクライアント通信をディセーブルにする場合は、stop-dcnm-cluster スクリプトを使用します。単一サーバを導入する場合は、次のいずれかを実行します。

- Microsoft Windows：[Start] > [All Programs] > [Cisco DCNM Server] > [Stop DCNM Server] を選択します。
- RHEL：Stop_DCNM_Server スクリプトを使用します。

Cisco DCNM の停止の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

**ステップ 2**　テキスト エディタで、次の場所にある jboss-service.xml ファイルを開きます。

*INSTALL_DIR*¥dcm¥jboss-4.2.2.GA¥server¥dcnm¥deploy¥ejb3.deployer¥META-INF¥jboss-service.xml

*INSTALL_DIR* は、Cisco DCNM のインストール ディレクトリです。Microsoft Windows のデフォルトのインストール ディレクトリは、C:¥Program Files¥Cisco Systems です。RHEL システムのデフォルトのインストール ディレクトリは、/usr/local/cisco です。

**ステップ 3**　ファイル内で次のセクションを探します。見つかったセクションが、次の各行と正確に一致していることを確認します。

```
<mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
  <depends>jboss.aop:service=AspectDeployer</depends>
  <attribute
name="InvokerLocator">sslsocket://${jboss.bind.address}:${cisco.dcnm.remoting.sslejbport:3
843}</attribute>
  <attribute name="Configuration">
    <handlers>
      <handler
subsystem="AOP">org.jboss.aspects.remoting.AOPRemotingInvocationHandler</handler>
    </handlers>
  </attribute>
</mbean>
```

このセクションは、XML の標準のコメント記号を使用してコメント アウトされています。

**ステップ 4**　XML の標準のコメント記号を使用して、このセクションを次のようにコメント アウトします。

**a.** このセクションの先頭の行で、次の 3 文字を「mbean」の前に追加します。

```
!--
```

変更後、この行は次のようになります。

```
<!--mbean code="org.jboss.remoting.transport.Connector"
name="jboss.remoting:type=Connector,transport=SslEjb3Connector,handler=ejb3">
```

**b.** このセクションの最後の行で、次の 2 文字を「mbean」の後ろに追加します。

```
--
```

変更後、この行は次のようになります。

```
</mbean-->
```

**ステップ 5**　jboss-service.xml ファイルを保存して閉じます。

**ステップ 6**　テキスト エディタで、次の場所にある jboss-service.xml ファイルを開きます。

*INSTALL_DIR*¥dcm¥jboss-4.2.2.GA¥server¥dcnm¥conf¥jboss-service.xml

**（注）**　このファイルは、ステップ 2 で開いた jboss-service.xml ファイルとは異なります。

**ステップ 7**　ファイル内で次のセクションを探します。

```
cisco.dcnm.remoting.transport=sslsocket
cisco.dcnm.remoting.port=3843
cisco.dcnm.remoting.ejbport=3873
cisco.dcnm.remoting.sslejbport=3843
cisco.dcnm.remoting.client.invokerDestructionDelay=30000
```

最後の 3 行の行末に記述されているポート番号は、Cisco DCNM サーバのインストール時にデフォルトのポート番号を変更したかどうかによって、この例とは異なる場合があります。

**ステップ 8**　cisco.dcnm.remoting.transport の値を socket に変更します。変更後、この行は次のようになります。

```
cisco.dcnm.remoting.transport=socket
```

**ステップ 9**　cisco.dcnm.remoting.port の値を、cisco.dcnm.remoting.ejbport に指定されている値と一致するように変更します。たとえば、Cisco DCNM サーバがデフォルトの EJB ポートを使用するように設定されている場合、cisco.dcnm.remoting.ejbport の値は 3873 であるため、変更後のこの行は次のようになります。

```
cisco.dcnm.remoting.port=3873
```

**ステップ 10**　cisco.dcnm.remoting.client.invokerDestructionDelay の値を 0 に変更します。変更後、この行は次のようになります。

```
cisco.dcnm.remoting.client.invokerDestructionDelay=0
```

**ステップ 11**　jboss-service.xml ファイルを保存して閉じます。

**ステップ 12**　次のいずれかを行います。

- Cisco DCNM の導入においてクラスタ化されたサーバを配置した場合は、クラスタ内の各サーバに対してこの手順を繰り返し実行します。その後、各サーバを起動します（マスター サーバを最初に起動します）。各サーバの起動間隔は、1 分以上あけてください。
- 単一サーバを導入する場合は、Cisco DCNM サーバを起動します。

単一の Cisco DCNM または Cisco DCNM サーバのクラスタの起動の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

# セカンダリ サーバのバインド ポートの指定

特定のセカンダリ サーバのバインド ポートを使用するように、Cisco DCNM サーバを設定することができます。

Cisco DCNM の導入においてクラスタ化されたサーバを配置した場合は、クラスタ内の各サーバに対して次の手順を実行する必要があります。

### 手順の詳細

**ステップ 1**　Cisco DCNM サーバを停止します。サーバ クラスタでセキュアなクライアント通信をイネーブルにする場合は、stop-dcnm-cluster スクリプトを使用します。単一サーバを導入する場合は、次のいずれかを実行します。

- Microsoft Windows：[Start] > [All Programs] > [Cisco DCNM Server] > [Stop DCNM Server] を選択します。
- RHEL：Stop_DCNM_Server スクリプトを使用します。

Cisco DCNM の停止の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

**ステップ 2**　テキスト エディタで、次の場所にある remoting-bisocket-service.xml ファイルを開きます。

*INSTALL_DIR*¥dcm¥jboss-4.2.2.GA¥server¥dcnm¥deploy¥jboss-messaging.sar¥remoting-bisocket-service.xml

*INSTALL_DIR* は、Cisco DCNM のインストール ディレクトリです。Microsoft Windows のデフォルトのインストール ディレクトリは、C:¥Program Files¥Cisco Systems です。RHEL システムのデフォルトのインストール ディレクトリは、/usr/local/cisco です。

**ステップ 3**　ファイル内で次のセクションを探します。見つかったセクションに、secondaryBindPort 行が含まれていることを確認します。

```
<!-- Use these parameters to specify values for binding and connecting control connections
to work with your firewall/NAT configuration
<attribute name="secondaryBindPort">xyz</attribute>
<attribute name="secondaryConnectPort">abc</attribute>
-->
```

デフォルトでは、このセクションは、XML の標準のコメント記号（<!-- および -->）を使用してコメント アウトされています。

セカンダリ サーバのバインド ポートを以前に指定した場合、このセクションはコメント アウトされていません。

**ステップ 4**　このセクションがコメント アウトされている場合は、次のように secondaryBindPort 行をアンコメントします。

**a.**　このセクションの 2 行目の行末で、次の 3 文字を「configuration」の後ろに追加します。

```
-->
```

変更後、この行は次のようになります。

```
to work with your firewall/NAT configuration-->
```

**b.** このセクションの 4 行目の行頭に、次の 4 文字を追加します。

```
<!--
```

変更後、この行は次のようになります。

```
<!-- <attribute name="secondaryConnectPort">abc</attribute>
```

アンコメント後のこのセクションは、次のようになります。

```
<!-- Use these parameters to specify values for binding and connecting control connections
to work with your firewall/NAT configuration-->
<attribute name="secondaryBindPort">xyz</attribute>
<!--<attribute name="secondaryConnectPort">abc</attribute>
-->
```

**ステップ 5**　secondaryConnectPort 行で、属性の開始要素と終了要素の間にポート番号を指定します。たとえば、ポート 47900 を指定する場合、secondaryBindPort 行は次のようになります。

```
<attribute name="secondaryBindPort">47900</attribute>
```

**ステップ 6**　remoting-bisocket-service.xml ファイルを保存して閉じます。

**ステップ 7**　次のいずれかを行います。

- Cisco DCNM の導入においてクラスタ化されたサーバを配置した場合は、クラスタ内の各サーバに対してこの手順を繰り返し実行します。その後、各サーバを起動します（マスター サーバを最初に起動します）。各サーバの起動間隔は、1 分以上あけてください。
- 単一サーバを導入する場合は、Cisco DCNM サーバを起動します。

単一の Cisco DCNM または Cisco DCNM サーバのクラスタの起動の詳細については、『*Cisco DCNM Fundamentals Configuration Guide, Release 5.x*』を参照してください。

# その他の関連資料

セキュアなクライアント通信に関する追加情報については、次のセクションを参照してください。

- 「関連資料」（P.7-7）
- 「標準規格」（P.7-8）

## 関連資料

| 関連トピック | 参照先 |
|---|---|
| 組織での Cisco DCNM の導入プロセス | 第 1 章「Cisco DCNM の導入」 |

## 標準規格

| 標準規格 | タイトル |
|---|---|
| SSL 3.0 | 「The SSL Protocol, Version 3.0」（http://tools.ietf.org/html/draft-ietf-tls-ssl-version3-00） |
| TLS 1.2 | 「The Transport Layer Security (TLS) Protocol, Version 1.2」（http://tools.ietf.org/html/rfc5246） |

# セキュアなクライアント通信機能の履歴

表 7-1 は、この機能のリリースの履歴です。

**表 7-1　セキュアなクライアント通信機能の履歴**

| 機能名 | リリース | 機能情報 |
|---|---|---|
| セキュアなクライアント通信 | 5.0(2) | この機能が導入されました。 |