CHAPTER 2

SSHD プロトコルの設定

Secure Shell Daemon （SSHD）プロトコルは、保護されていないネットワーク経由で通信する 2 つのホスト間で、通信内容を暗号化して保護します。CSS では、OpenSSH を実装して、通信を保護することができます。SSHD では、CSS のログイン プロンプトでユーザ名とパスワードを入力する、標準の CSS ログイン シーケンスを使用します。

CSS の SSHD では、SSH v1 プロトコルと v2 プロトコルの両方がサポートされます。SSH v1 では、3DES や Blowfish などの暗号化方式で通信が暗号化されます。SSH v2 では、128 ビットの AES、Blowfish、3DES、CAST128、Arcfour、192 ビットの AES、または 256 ビットの AES が使用できます。

注意 SSHD を使用する場合は、リモート システムにある、ネットワーク マウントしたファイル システムから CSS をブートするような環境（ディスクレス環境）に設定されていないことを確認してください。CSS をネットワーク マウントしたファイル システムからブートする場合は、SSHD プロトコルがサポートされないことに留意してください。

ネットワーク マウントしたファイル システムから CSS がブートされた場合は、SSHD プロトコルにより初期化が行われるときに、次に示す SSHD からのエラー メッセージが記録され、初期化動作が終了します。

```
Unable to initialize sshd; failure to seed random number generator
```

この章の主な内容は次のとおりです。

- SSH の有効化
- SSH アクセスの設定
- CSS での SSHD の設定
- SSHD を使用する場合の Telnet アクセスの設定
- SSHD 設定の表示

SSH の有効化

CSS の SSH 機能を有効にするには、セキュア管理ソフトウェア オプションを購入する必要があります。セキュア管理ソフトウェア オプションを購入した場合は、権利証明書が次の方法でお手元に届きます。

- CSS の注文の際に購入した場合は、アクセサリ キットに権利証明書が同封されています。
- CSS をすでに購入している場合、権利証明書は郵送によりお手元に届きます。

（注） セキュア管理オプションの権利証明書がアクセサリ キットにない場合は、製品をお買い上げの弊社販売代理店にお問い合わせください。

権利証明書の指示に従って、セキュア管理ソフトウェア ライセンス キーを入手します。

セキュア管理ライセンス キーをインストールして SSH を有効にするには、次の操作を実行します。

1. CSS にログインして、**license** コマンドを実行します。

```
# license
```

2. セキュア管理ライセンス キーを入力します。

```
Enter the Software License Key (q to quit): nnnnnnnnnnnn
```

セキュア管理ライセンス キーはこれで正常にインストールされ、SSH 機能がアクティブになります。

SSH アクセスの設定

SSH による CSS へのアクセスは、**no restrict ssh** コマンドによりデフォルトで有効になっています。SSH アクセスの選択状態は、running-config ファイル内で調べることができます。

SSHD 使用時にセキュリティを強化するには、Telnet アクセスを無効にします（Telnet アクセスはデフォルトで有効に設定されています）。第 1 章「CSS のアクセス制御」の説明に従って、**telnet-access disable** コマンドを使用します。

SSH による CSS へのアクセスを有効にするには、次のコマンドを入力します。

```
(config)# no restrict ssh
```

SSH によるアクセスを無効にするには、次のように入力します。

```
(config)# restrict ssh
```

CSS での SSHD の設定

CSS に SSHD を設定するためのコマンドは、次のとおりです。

- **sshd keepalive** ：TCP キープアライブ メッセージを有効にする。
- **sshd port** ：SSHD ポートを指定する。
- **sshd server-keybits** ：エフェメラルなプロトコル サーバ キーのビット数を設定する（SSH v1 だけ）。
- **sshd version** ：CSS でサポートされる SSH プロトコルのバージョンを設定する。

SSHD から CSS へのアクセスが有効化され、SSHD が SSH クライアントからの接続を受信できることを確認します。デフォルトでは、SSH アクセスは、**no restrict ssh** コマンドによってグローバルに有効化されています。

SSHD キープアライブの設定

CSS では、クライアントに TCP キープアライブ メッセージを送信して、サーバからクライアントへの SSHD 接続が機能しているかどうか（たとえば、ネットワークが停止しているか、または、クライアントが応答不能になっているか）を確認できます。クライアントへの SSHD キープアライブの送信を無効にすると、サーバ上でセッションが無期限に停止し、システム リソースを大量に使用することがあります。

SSHD キープアライブを有効にするには、**sshd keepalive** コマンドを使用します。SSHD キープアライブは、デフォルトで有効に設定されています。

クライアントへの SSHD キープアライブの送信を有効にするには、次のコマンドを入力します。

```
(config)# sshd keepalive
```

SSHD キープアライブの送信を無効にするには、次のように入力します。

```
(config)# no sshd keepalive
```

SSHD ポートの設定

SSH のデフォルト ポート番号は 22 です。サーバがクライアントからの接続を監視するポート番号を指定するには、**sshd port** コマンドを使用します。22、または 512 ～ 65535 のポート番号を入力します。

（注） 新しい sshd ポートを設定すると、ポートが無効または使用不可であることを通知するメッセージが表示される場合があります。このメッセージが表示されるのは、ポートが CSS の内部で使用中の場合です。このメッセージが表示された場合は、別のポート番号を入力してください。

たとえば、ポート番号 65530 を SSHD ポートとして設定するには、次のように入力します。

```
(config)# sshd port 65530
```

ポート番号をデフォルトの 22 に戻すには、次のように入力します。

```
(config)# no sshd port
```

SSHD サーバキービットの設定

エフェメラルなプロトコル サーバ キーのビット数を指定するには、**sshd server-keybits** コマンドを使用します。**sshd server-keybits** コマンドは、SSH v1 の接続だけを対象としています。512 ～ 1024 （有効な範囲）のビット数を入力します。デフォルトは 768 です。

（注） このコマンドの有効な範囲は 512 ～ 1024 です。ただし、CSS では、バージョン 5.00 との下位互換性を維持するために、512 ～ 32768 の値を入力することができます。1024 を超える値を入力した場合、値はデフォルトの 768 に変更されます。CSS を再度ブートしたときに、有効な範囲を知らせる次のエラー メッセージが表示されます。

```
NETMAN-3: sshd: Bad server key size <configured value>; range 512 to
1024; defaulting to 768
```

たとえば、サーバ キーのビット数を 1024 に設定するには、次のように入力します。

```
(config)# sshd server-keybits 1024
```

ビット数をデフォルトの 768 に戻すには、次のように入力します。

```
(config)# no sshd server-keybits
```

SSHD バージョンの設定

デフォルトでは、CSS は SSH v1 と v2 の両プロトコルをサポートします。SSH v1 と v2 をサポートするように CSS を設定するには、**sshd version** コマンドを使用します。このコマンドのシンタックスは次のとおりです。

sshd version v1|v2

キーワードの意味は次のとおりです。

- **v1** ：SSH v1 プロトコルだけをサポートするように CSS を設定
- **v2** ：SSH v2 プロトコルだけをサポートするように CSS を設定

たとえば、SSH v1 プロトコルだけをサポートするように CSS を設定するには、次のように入力します。

```
(config)# sshd version v1
```

SSH v2 プロトコルだけをサポートするように CSS を設定するには、次のように入力します。

```
(config)# sshd version v2
```

SSH v1 と v2 の両プロトコルをサポートするデフォルト設定に CSS をリセットするには、次のように入力します。

```
(config)# no sshd version
```

SSHD を使用する場合の Telnet アクセスの設定

デフォルトでは、CSS への Telnet アクセスが有効に設定されています。SSHD を使用する場合は、CSS への 安全でない Telnet アクセスを無効にすることができます。SSHD 使用時のセキュリティ強化のため、Telnet アクセスを無効にすることをお勧めします。CSS への Telnet アクセスを無効にするには、グローバルな **restrict telnet** コマンドを使用します。

Telenet アクセスを無効にするには、次のように入力します。

```
(config)# restrict telnet
```

CSS への Telnet アクセスを有効に戻すには、次のコマンドを入力します。

```
(config)# no restrict telnet
```

SSHD 設定の表示

SSHD の設定を表示するには、**show sshd** コマンドを使用します。このコマンドには、次のオプションがあります。

- **show sshd config** ：SSHD の設定を表示する。
- **show sshd sessions** ：現在アクティブな SSHD サーバ セッションの要約を表示する。このコマンドでは、SSH クライアントが設定されている場合だけ、データが表示されます。
- **show sshd version** ：CSS で現在動作中の SSHield パッケージを表示する。

SSHD 設定を表示するには、次のように入力します。

```
# show sshd config
```

表 2-1 に、**show radius config** コマンドで表示されるフィールドを示します。

表 2-1　show sshd config コマンドのフィールド

フィールド	説明
Maximum Sessions Allowed	同時に実行できる SSHD セッションの最大数（最大 5 セッション）
Active Sessions	現在アクティブな SSHD セッションの数
Log Level	現在のログ レベル
Listen Socket Count	SSHD が現在監視しているソケットの数。このバージョンでは設定できません。デフォルト値は 1 です。
Listen Port	SSHD がクライアントとの接続の監視に使用するポート番号。ポート番号を指定するには、**sshd port** コマンドを使用します。デフォルト値（SSH 用のデフォルト ポート）は 22 です。指定できるポート番号は、22、または 512 ～ 65535 の値です。
Listen Address	SSHD がクライアントの接続の監視に使用するアドレス。このバージョンでは設定できません。デフォルト値は 0.0.0.0 です。

表 2-1　show sshd config コマンドのフィールド（続き）

フィールド	説明
Server Key Bits	SSHv1 サーバ キーの生成に使用するサーバ キーのビット数。デフォルトは 768 です。範囲は 512 ～ 1024 です。
RSA Protocol (SSH1)	SSHv1 アクセスの状態。このバージョンでは設定できません。デフォルトで有効に設定されています。
Empty Passwords	使用不可。ユーザ名には、必ずパスワードを関連付ける必要があります。
Keepalive	クライアントへの TCP キープアライブ送信の状態（Enabled または Disabled）。SSHD キープアライブは、デフォルトで有効に設定されています。
SSH2 Cipher List	クライアントとサーバの間で認証、暗号化、およびデータ保全性の確保に使用される SSHv2 暗号スイートのリスト

SSHD セッションを表示するには、次のように入力します。

```
# show sshd sessions
```

表 2-2 に、**show sshd sessions** コマンドで表示されるフィールドを示します。

表 2-2　show sshd sessions コマンドのフィールド

フィールド	説明
Session_ID	セッションの ID
Conn_TID	接続を処理する SSHD サーバの接続タスク ID（tSshConn）
Login_TID	接続を処理するログイン タスク ID （tSshCli）
PTY_FD	ログイン タスクが CSS CLI とやり取りするために使用するファイル記述子。 PTY_FD ファイル記述子を使用すると、SSH クライアント セッションを、**show lines** コマンドの実行結果で Line フィールドに表示されるセッションと関連させることができます。たとえば、**show sshd sessions** コマンドを実行すると、PTY_FD32 に関連する SSH クライアント セッションが表示されます。**show lines** コマンドを入力すると、sshc32 （SSH クライアントの場合は pty_fd32）を含む行が表示されます。この関係によって、**show lines** コマンドで、SSH セッションのログイン時刻、アイドル時間、およびクライアントの場所を確認できます。
Remote IP/Remote Port	SSHD セッションのリモート IP とポート番号

SSHD バージョンを表示するには、次のように入力します。

```
# show sshd version
SSHield version 1.5, SSH version OpenSSH_3.0.2p1
```