CHAPTER 22

センサーへのログイン

（注） IPS SSP を搭載した Cisco ASA 5585-X は、現在、Cisco IPS 7.1 をサポートする唯一のプラットフォームです。他の Cisco IPS センサーは、いずれも現在 IPS 7.1 をサポートしていません。

（注） IPS SSP を搭載した Cisco ASA 5585-X は、ASA 8.2(4.4) 以降および ASA 8.4(2) 以降でサポートされています。ASA 8.3(*x*) ではサポートされていません。

（注） IPS プラットフォームでは、10 個の CLI セッションを同時に確立することができます。

この章では、さまざまな Cisco IPS プラットフォームにログインする方法について説明します。内容は次のとおりです。

サポートされるユーザ ロール

次のユーザ権限を使用してログインできます。

- 管理者（Administrator）
- オペレータ（Operator）
- ビューア（Viewer）
- サービス（Service）

サービス ロールでは、CLI に直接アクセスできません。サービス アカウント ユーザは、bash シェルに直接ログインします。このアカウントは、サポートおよびトラブルシューティング目的でのみ使用します。無許可の変更はサポートされず、正しく動作することを保証するには、センサーでイメージを再作成することが必要になります。サービス ロールでは、1 ユーザのみ作成できます。

サービス アカウントにログインすると、次の警告が表示されます。

```
****************************** WARNING ****************************************
UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED.
This account is intended to be used for support and troubleshooting purposes only.
Unauthorized modifications are not supported and will require this device to be re-imaged
to guarantee proper operation.
*******************************************************************************
```

（注） サービス ロールは、必要に応じて CLI をバイパスできる特殊なロールです。管理者権限を持つユーザだけが、サービス アカウントを編集できます。

詳細情報

- サービス アカウントの詳細については、「サービス アカウントについて」（P.6-23）を参照してください。
- ユーザの追加および削除を行う手順については、「認証およびユーザの設定」（P.6-18）を参照してください。

アプライアンスへのログイン

（注） コンソールからアプライアンスを初期化（**setup** コマンドを実行）する必要があります。ネットワークを設定すると、SSH および Telnet が有効になります。

アプライアンスには、コンソール ポートからログインできます。

アプライアンスにログインするには、次の手順を実行します。

ステップ 1　アプライアンスにログインするため、コンソール ポートをセンサーに接続します。

ステップ 2　ログイン プロンプトに対してユーザ名とパスワードを入力します。

（注） デフォルトのユーザ名とパスワードはどちらも **cisco** です。初めてアプライアンスにログインするとき、このユーザ名とパスワードを変更するように求めるメッセージが表示されます。最初に、UNIX パスワード（**cisco**）を入力してください。次に、新しいパスワードを 2 回入力します。

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.
```

```
A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
ips-4240#
```

詳細情報

- アプライアンスをターミナル サーバに接続する手順については、「ターミナル サーバの設定」（P.22-3）を参照してください。
- **setup** コマンドを使用してアプライアンスを初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

ターミナル サーバの設定

ターミナル サーバは複数の低速非同期ポートを持つルータです。この複数のポートは、他のシリアル デバイスに接続されています。ターミナル サーバを使用して、アプライアンスを含むネットワーク機器をリモートで管理することができます。

RJ-45 接続またはヒドラ ケーブル アセンブリ接続を使用して Cisco ターミナル サーバをセットアップするには、次の手順を実行します。

ステップ 1　次のいずれかの方法で、ターミナル サーバに接続します。

- RJ-45 接続を行うターミナル サーバの場合、180 ロールオーバー ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。
- ヒドラ ケーブル アセンブリの場合、ストレート パッチ ケーブルをアプライアンスのコンソール ポートからターミナル サーバのポートに接続します。

ステップ 2　ターミナル サーバで、ラインとポートを設定します。イネーブル モードで次の設定を入力します。ここで、# は設定するポートの回線番号です。

```
config t
line #
login
transport input all
stopbits 1
flowcontrol hardware
speed 9600
exit
exit
wr mem
```

ステップ 3　アプライアンスへの不正アクセスを防ぐため、ターミナル セッションは確実に正しく終了してください。

ターミナル セッションが正しく終了されていない場合、つまり、セッションを開始したアプリケーションから exit(0) 信号が受信されていない場合、ターミナル セッションは開いたままです。ターミナル セッションが正しく終了していない場合、そのシリアル ポート上で開かれる次のセッションでは、認証が実行されません。

注意　接続を確立するために使用したアプリケーションを終了する前に、必ずセッションを終了してログイン プロンプトに戻ってください。

注意　誤って接続が切断されたり終了した場合は、接続を再確立し、正しく終了して、アプライアンスに対する不正なアクセスを防ぎます。

AIM IPS へのログイン

ここでは、AIM IPS へのセッションを確立する方法について説明します。内容は次のとおりです。

AIM IPS およびセッション コマンド

ルータ コンソールから AIM IPS へのセッションを確立します。AIM IPS は外部コンソール ポートを備えていないため、AIM IPS へのコンソール アクセスは、ルータで **service-module ids-sensor** *slot*/*port* **session** コマンドを発行したとき、または AIM IPS ポート番号に対応するスロット番号を使用してルータへの Telnet 接続を開始したときにイネーブルになります。外部コンソール ポートがないことは、初期ブート設定がルータを通じてのみ可能であることを意味します。

service-module ids-sensor *slot*/*port* **session** コマンドを発行すると、v との間にコンソール セッションが作成されます。このセッションで任意の IPS コンフィギュレーション コマンドを発行できます。セッションでの作業を完了し、IPS CLI を終了すると、Cisco IOS CLI に戻ります。

session コマンドを使用すると、IDS-Senso インターフェイスの IP アドレスを使用して逆方向の Telnet 接続が開始されます。IDS-Sensor インターフェイスは、AIM IPS とルータの間のインターフェイスです。**session** コマンドを起動する前に、IDS-Sensor インターフェイスに IP アドレスを割り当てる必要があります。ルーティング可能な IP アドレスを割り当てると、IDS-Sensor インターフェイス自体が攻撃に対して脆弱になります。これは、ルーティング可能な IP アドレスを通して、ネットワーク上で AIM IPS を確認できるようになるためです。つまり、ルータ外部にある AIM IPS と通信できるようになるためです。この脆弱性に対処するため、IDS-Sensor インターフェイスにアンナンバード IP アドレスを割り当てます。こうすると、AIM IPS IP アドレスはルータと AIM IPS 間でローカルにのみ使用されるようになり、AIM IPS との間にセッションを確立しようとする試みから隔離されます。

（注）　アプリケーション ソフトウェアのインストールまたはモジュール イメージの再作成を行う前にセッションを開始すると、ブートローダが起動します。ソフトウェアのインストール後、アプリケーションを始動するセッションを開始します。

注意　モジュールへのセッションを確立してコンソールから大規模な転送処理を実行する場合、ホスト コンソールのインターフェイス速度を 115200/bps 以上に設定しないと、文字のトラフィックが失われることがあります。速度が 115200/bps に設定されていることを確認するには、**show running config** コマンドを使用します。

詳細情報

アンナンバード IP アドレスを設定する手順については、「Using an Unnumbered IP Address Interface」を参照してください。

AIM IPS へのセッション接続

（注） ルータから AIM IPS を初期化（**setup** コマンドを実行）する必要があります。ネットワークを設定すると、SSH および Telnet が有効になります。

AIM IPS からルータへのセッションを確立するには、**service-module ids-sensor** *slot*/*port* **session** コマンドを使用します。セッション プロンプトをルータ プロンプトに戻すには（AIM IPS プロンプトからルータ プロンプトに戻るには）、**Ctrl キーと Shift キーを押した状態で 6 キー**を押し、続いて **x** を押します。セッション プロンプト（ルータ プロンプト）に戻るには、空白行で **Enter** を押します。ルータ コマンドを実行した後でこのセッションに戻る場合は、ルータに対するセッションを一時停止する必要があります。AIM IPS セッションに戻る予定のない場合は、セッションを一時停止するのではなく閉じてください。

セッションを閉じると、AIM IPS CLI から完全にログアウトします。ログインするには、新しいセッション接続を確立するためにユーザ名とパスワードを入力する必要があります。セッションを一時停止した場合は、CLI にログインしたまま残ります。**session** コマンドを使用して接続した場合は、ユーザ名とパスワードを入力せずに同じ CLI に戻ることができます。

（注） Telnet クライアントには多くの種類があります。クライアントによっては、**Ctrl キーを押した状態で 6 キーを押してから x キー**を押す必要があります。制御文字は、^^、Ctrl-^、または ASCII 値 30（16 進数では 1E）で表されます。

注意 **disconnect** コマンドを使用してセッションを終了しても、そのセッションは残ります。この開いている状態のセッションは、残った接続を利用しようとしている人間に悪用されるおそれがあります。

AIM IPS へのセッションを開始または終了するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　AIM IPS のステータスをチェックし、実行中であることを確認します。

```
router# service-module ids-sensor 0/1 status
Service Module is Cisco IDS-Sensor0/1
Service Module supports session via TTY line 322
Service Module is in Steady state
Getting status from the Service Module, please wait..
Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.2(1)E3
  Model:             AIM IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.196
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

ステップ 3　ルータから AIM IPS へのセッションを開始します。

```
router# service-module ids-sensor 0/1 session
Trying 10.89.148.196, 2322 ... Open
```

ステップ 4　モジュール セッションを終了するか、または一時停止して終了します。

- `sensor# exit`

（注）　IPS CLI のサブモードにいる場合は、すべてのサブモードを終了する必要があります。センサーのログイン プロンプトが表示されるまで、**exit** と入力します。

注意　セッションを適切に終了しないと、残っているセッションを別のユーザが乗っ取ることが可能になります。Cisco IOS セッションを完全に終了するため、必ず `router#` プロンプトで **exit** と入力してください。

- AIM IPS へのセッションを一時停止して終了するには、**Ctrl キーを押した状態で Shift キー**を押し、**6** を押します。すべてのキーから指を放してから、**x** を押します。

（注）　セッションでの作業が終了したら、ルータに戻ってセッション（IPS アプリケーション）とモニタ対象のルータ インターフェイスの間の関連付けを確立する必要があります。

ステップ 5　ルータから接続解除します。

```
router# disconnect
```

ステップ 6　**Enter** キーを押して接続解除を確認します。

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

詳細情報

AIM IPS を初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

AIP SSM、AIP SSC-5、および IPS SSP へのログイン

（注）　ASA モジュール（AIP SSM、AIP SSC-5、および IPS SSP）を初期化すると、SSH と Telnet が有効になります。

適応型セキュリティ アプライアンスから ASA モジュールにログインします。

適応型セキュリティ アプライアンスから ASA モジュールへのセッションを確立するには、次の手順を実行します。

ステップ 1　適応型セキュリティ アプライアンスにログインします。

（注）　適応型セキュリティ アプライアンスがマルチモードで動作している場合は、続行する前に **change system** コマンドを使用して、システム レベルのプロンプトを表示させます。

ステップ 2　ASA モジュールとの間にセッションを確立します。

```
asa# session 1
Opening command session with slot 1.
Connected to slot 1. Escape character sequence is 'CTRL-^X'.
```

ログインするためのセッション タイムアウトは 60 秒です。

ステップ 3　ログイン プロンプトに対してユーザ名とパスワードを入力します。

（注）　デフォルトのユーザ名とパスワードはどちらも **cisco** です。初めてモジュールにログインするとき、このユーザ名とパスワードを変更するように求めるメッセージが表示されます。最初に、UNIX パスワード（**cisco**）を入力してください。次に、新しいパスワードを 2 回入力します。

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
aip-ssm#
```

ステップ 4　セッションからエスケープして適応型セキュリティ アプライアンス プロンプトに戻るには、次のいずれかの手順を実行します。

- **exit** と入力します。
- **Ctrl キーと Shift キーを押した状態で 6 キーを押し、続いて x** を押します（**CTRL^X** と表されます）。

詳細情報

- **setup** コマンドを使用して AIP SSM を初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

- **setup** コマンドを使用して IPS SSP を初期化する手順については、「IPS SSP の高度なセットアップ」（P.23-26）を参照してください。
- ASDM を使用して AIP SSC-5 を初期化する手順については、「ASDM での AIP SSC-5 のセットアップ」（P.23-8）を参照してください。

IDSM2 へのログイン

（注） スイッチから IDSM2 を初期化（**setup** コマンドを実行）する必要があります。ネットワークを設定すると、SSH および Telnet が有効になります。

スイッチから IDSM2 にログインします。

IDSM2 へのセッションを確立するには、次の手順を実行します。

ステップ 1　スイッチから IDSM2 へのセッションを確立します。

- Catalyst ソフトウェアの場合

```
console> (enable) session slot_number
```

- Cisco IOS ソフトウェアの場合

```
router# session slot_number processor 1
```

ステップ 2　ログイン プロンプトに対してユーザ名とパスワードを入力します。

（注） デフォルトのユーザ名とパスワードはどちらも **cisco** です。初めて IDSM2 にログインするとき、このユーザ名とパスワードを変更するように求めるメッセージが表示されます。最初に、UNIX パスワード（**cisco**）を入力してください。次に、新しいパスワードを 2 回入力します。

```
login: cisco
Password:
***NOTICE***
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable laws and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
idsm-2#
```

詳細情報

setup コマンドを使用して IDSM2 を初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

NME IPS へのログイン

ここでは、NME IPS へのセッションを確立する方法について説明します。内容は次のとおりです。

NME IPS およびセッション コマンド

ルータ コンソールから NME IPS へのセッションを確立します。NME IPS は外部コンソール ポートを備えていないため、NME IPS へのコンソール アクセスは、ルータで **service-module ids-sensor** *slot*/*port* **session** コマンドを発行したとき、または NME IPS ポート番号に対応するスロット番号を使用してルータへの Telnet 接続を開始したときにイネーブルになります。外部コンソール ポートがないことは、初期ブート設定がルータを通じてのみ可能であることを意味します。

service-module ids-sensor *slot*/*port* **session** コマンドを発行すると、NME IPS との間にコンソール セッションが作成されます。このセッションで任意の IPS コンフィギュレーション コマンドを発行できます。セッションでの作業を完了し、IPS CLI を終了すると、Cisco IOS CLI に戻ります。

session コマンドを使用すると、IDS-Senso インターフェイスの IP アドレスを使用して逆方向の Telnet 接続が開始されます。IDS-Sensor インターフェイスは、NME IPS とルータの間のインターフェイスです。**session** コマンドを起動する前に、IDS-Sensor インターフェイスに IP アドレスを割り当てる必要があります。ルーティング可能な IP アドレスを割り当てると、IDS-Sensor インターフェイス自体が攻撃に対して脆弱になります。これは、ルーティング可能な IP アドレスを通して、ネットワーク上で NME IPS を確認できるようになるためです。つまり、ルータ外部にある NME IPS と通信できるようになるためです。この脆弱性に対処するため、IDS-Sensor インターフェイスにアンナンバード IP アドレスを割り当てます。こうすると、NME IPS IP アドレスはルータと NME IPS 間でローカルにのみ使用されるようになり、NME IPS との間にセッションを確立しようとする試みから隔離されます。

（注） アプリケーション ソフトウェアのインストールまたはモジュール イメージの再作成を行う前にセッションを開始すると、ブートローダが起動します。ソフトウェアのインストール後、アプリケーションを始動するセッションを開始します。

注意 モジュールへのセッションを確立してコンソールから大規模な転送処理を実行する場合、ホスト コンソールのインターフェイス速度を 115200/bps 以上に設定しないと、文字のトラフィックが失われることがあります。速度が 115200/bps に設定されていることを確認するには、**show running config** コマンドを使用します。

詳細情報

アンナンバード IP アドレスを設定する手順については、「Setting Up Interfaces on NME IPS and the Router」を参照してください。

NME IPS へのセッション接続

（注）　ルータから NME IPS を初期化（**setup** コマンドを実行）する必要があります。ネットワークを設定すると、SSH および Telnet が有効になります。

NME IPS からモジュールへのセッションを確立するには、**service-module ids-sensor** *slot*/*port* **session** コマンドを使用します。セッション プロンプトをルータ プロンプトに戻すには（NME IPS プロンプトからルータ プロンプトに戻るには）、**Ctrl キーと Shift キーを押した状態で 6 キー**を押し、続いて **x** を押します。セッション プロンプト（ルータ プロンプト）に戻るには、空白行で **Enter** を押します。ルータ コマンドを実行した後でこのセッションに戻る場合は、ルータに対するセッションを一時停止する必要があります。NME IPS セッションに戻る予定のない場合は、セッションを一時停止するのではなく閉じてください。

セッションを閉じると、NME IPS CLI から完全にログアウトします。ログインするには、新しいセッション接続を確立するためにユーザ名とパスワードを入力する必要があります。セッションを一時停止した場合は、CLI にログインしたまま残ります。**session** コマンドを使用して接続した場合は、ユーザ名とパスワードを入力せずに同じ CLI に戻ることができます。

（注）　Telnet クライアントには多くの種類があります。クライアントによっては、**Ctrl キーを押した状態で 6 キーを押してから x キー**を押す必要があります。制御文字は、^^、Ctrl-^、または ASCII 値 30（16 進数では 1E）で表されます。

注意　**disconnect** コマンドを使用してセッションを終了しても、そのセッションは残ります。この開いている状態のセッションは、残った接続を利用しようとしている人間に悪用されるおそれがあります。

NME IPS へのセッションを開始または終了するには、次の手順を実行します。

ステップ 1　ルータにログインします。

ステップ 2　NME IPS のステータスをチェックし、実行中であることを確認します。

```
router# service-module ids-sensor 1/0 status
Service Module is Cisco IDS-Sensor1/0
Service Module supports session via TTY line 130
Service Module is in Steady state
Service Module heartbeat-reset is disabled
Getting status from the Service Module, please wait..

Cisco Systems Intrusion Prevention System Network Module
  Software version:  6.2(1)E3
  Model:             NME IPS
  Memory:            443508 KB
  Mgmt IP addr:      10.89.148.195
  Mgmt web ports:    443
  Mgmt TLS enabled:  true


router#
```

ステップ 3　ルータから NME IPS へのセッションを開始します。

```
router# service-module ids-sensor 1/0 session
Trying 10.89.148.195, 2322 ... Open
```

ステップ 4　モジュール セッションを終了するか、または一時停止して終了します。

- `sensor# exit`

（注）　IPS CLI のサブモードにいる場合は、すべてのサブモードを終了する必要があります。センサーのログイン プロンプトが表示されるまで、**exit** と入力します。

注意　セッションを適切に終了しないと、残っているセッションを別のユーザが乗っ取ることが可能になります。Cisco IOS セッションを完全に終了するため、必ず `router#` プロンプトで **exit** と入力してください。

- NME IPS へのセッションを一時停止して終了するには、**Ctrl キーを押した状態で Shift キー**を押し、**6** を押します。すべてのキーから指を放してから、**x** を押します。

（注）　セッションでの作業が終了したら、ルータに戻ってセッション（IPS アプリケーション）とモニタ対象のルータ インターフェイスの間の関連付けを確立する必要があります。

ステップ 5　ルータから接続解除します。

```
router# disconnect
```

ステップ 6　**Enter** キーを押して接続解除を確認します。

```
router# Closing connection to 10.89.148.196 [confirm] <Enter>
```

詳細情報

NME IPS を初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。

センサーへのログイン

（注）　**setup** コマンドを使用してセンサーを初期化し、Telnet をイネーブルにすると、SSH または Telnet を使用してセンサーにログインできます。

センサーにログインするには、次の手順を実行します。

ステップ 1　SSH または Telnet を使用して、ネットワーク経由でセンサーにログインします。

```
ssh sensor_ip_address
telnet sensor_ip_address
```

ステップ 2　ログイン プロンプトに対してユーザ名とパスワードを入力します。

```
login: ******
Password: ******
***NOTICE***
```

```
This product contains cryptographic features and is subject to United States and local
country laws governing import, export, transfer and use. Delivery of Cisco cryptographic
products does not imply third-party authority to import, export, distribute or use
encryption. Importers, exporters, distributors and users are responsible for compliance
with U.S. and local country laws. By using this product you agree to comply with
applicable law s and regulations. If you are unable to comply with U.S. and local laws,
return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at:
http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

If you require further assistance please contact us by sending email to export@cisco.com.

***LICENSE NOTICE***
There is no license key installed on the system.
Please go to http://www.cisco.com/go/license to obtain a new license or install a license.
sensor#
```

詳細情報

センサーを初期化する手順については、「センサーの基本的なセットアップ」（P.23-5）を参照してください。