使用する前に

この章では、IDM について説明し、IDM を使用するための情報を提供します。この章は、次の項で構成されています。

（注） 『*Installing and Using Cisco Intrusion Prevention System Device Manager Version 5.1* 』は、ASDM の IPS セクションにも適用されます。ASDM のパスは IDM よりも長く、Configuration > Features > IPS > Licensing などのようになっています。

勧告

この製品には、輸入、輸出、譲渡、使用を規制する米国またはその他の国の法律の対象となる暗号化機能が含まれています。シスコ暗号化製品の出荷は、暗号の輸入、輸出、配布、使用を行うサードパーティの権限を包含するものではありません。輸入者、輸出者、配布者、ユーザは、米国およびその他の国の法律を遵守する責任があります。この製品を使用すると、適用される法律および規則を遵守することに合意したことになります。米国およびその他の国の法律を遵守できない場合は、同封された品目をすぐに返品してください。

シスコ暗号化製品を規制する米国法の概要は、次の Web サイトで参照できます。

http://www.cisco.com/wwl/export/crypto/tool/stqrg.html

詳細な情報が必要な場合は、export@cisco.com に電子メールでお問い合せください。

IDM の概要

IDM は、センサーの設定と管理が可能な Web ベースの Java アプリケーションです。IDM の Web サーバはセンサーに常駐します。この Web サーバには、Internet Explorer、Netscape、または Mozilla Web ブラウザでアクセスできます。

IDM のユーザ インターフェイスは、File メニューと Help メニュー、Configuration ボタンと Monitoring ボタン（これらのボタンのメニューは左側の TOC ペインで開きます）、ページの右側にある Configuration パネルで構成されています。Configuration ボタンと Monitoring ボタンの横に、次の 4 つのボタンが表示されます。

- Back：前に表示していたパネルに戻ります。
- Forward：一度表示したことのある次のパネルに進みます。
- Refresh：現在のコンフィギュレーションをセンサーからロードします。
- Help：新しいウィンドウでオンライン ヘルプを開きます。

センサーを設定するには、**Configuration** をクリックし、左側のペインのメニューで該当するものを探します。**Monitoring** をクリックし、左側のペインのメニューでモニタリングを設定します。

新しい設定は、設定中のパネルの **Apply** をクリックすると有効になります。**Reset** をクリックすると、現在の変更が廃棄され、設定は以前のパネルの状態に戻ります。

システム要件

IDM のシステム要件を次に示します。

- Windows 2000、Windows XP
  - Java プラグイン 1.4.2 または 1.5 がインストールされている Internet Explorer 6.0。または Java プラグイン 1.4.2 または 1.5 がインストールされている Netscape 7.1。
  - Pentium III または 450 Mhz 以上で動作する同等品
  - 最小 256 MB、推奨 512 MB 以上
  - 解像度 1024 × 768、256 色（最小）
- Sun SPARC Solaris
  - Sun Solaris 2.8 または 2.9
  - Mozilla 1.7
  - 最小 256 MB、推奨 512 MB 以上
  - 解像度 1024 × 768、256 色（最小）
- Linux
  - Red Hat Linux 9.0 または Red Hat Enterprise Linux WS、GNOME または KDE を実行するバージョン 3
  - Mozilla 1.7
  - 最小 256 MB、推奨 512 MB 以上
  - 解像度 1024 × 768、256 色（最小）

（注） IDM で使用できるその他の Web ブラウザもありますが、サポートされているのはここに示したブラウザだけです。

Java プラグインのメモリ サイズの増加

IDM を正しく実行するには、Java プラグイン 1.4.2 または 1.5 がブラウザにインストールされている必要があります。デフォルトでは、Java プラグインは 64 MB のメモリを IDM に割り当てます。IDM は使用中にメモリを使い果たしてしまうことがあります。この場合、IDM は停止するか、空白の画面を表示します。**Refresh** をクリックした場合にも、メモリ不足になることがあります。メモリ不足になると、Java コンソールに `OutofMemoryError` メッセージが表示されます。

（注）　Sun Microsystems Java を使用することを推奨します。その他のバージョンの Java を使用すると、IDM に問題を引き起こすことがあります。

IDM を使用する前に Java プラグインのメモリ設定を変更する必要があります。必要最小メモリサイズは、256 MB です。

この項で取り上げる事項は次のとおりです。

Windows での Java プラグイン

Windows で Java プラグイン 1.4.2 と 1.5 の設定を変更するには、次の手順を実行します。

ステップ 1　Internet Explorer または Netscape のすべてのインスタンスを閉じます。

ステップ 2　**Start** > **Settings** > **Control Panel** をクリックします。

ステップ 3　Java プラグイン 1.4.2 がインストールされている場合は、次の手順を実行します。

a. Java プラグラインをクリックします。

Java Plug-in Control Panel が表示されます。

b. **Advanced** タブをクリックします。

c. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力します。

d. **Apply** をクリックして Java Control Panel を終了します。

ステップ 4　Java プラグイン 1.5 がインストールされている場合は、次の手順を実行します。

a. Java をクリックします。

Java Control Panel パネルが表示されます。

b. **Java** タブをクリックします。

c. Java Applet Runtime Settings の下で **View** をクリックします。

Java Runtime Settings Panel が表示されます。

d. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力して、**OK** をクリックします。

e. **OK** をクリックして Java Control Panel を終了します。

Linux と Solaris での Java プラグイン

Linux と Solaris での Java プラグイン 1.4.2 または 1.5 の設定を変更するには、次の手順を実行します。

ステップ 1　Netscape または Mozilla のすべてのインスタンスを閉じます。

ステップ 2　ControlPanel 実行可能ファイルを起動すると、Java Plug-in Control Panel が表示されます。

（注）　Java 2 SDK では、このファイルは <SDK インストール ディレクトリ >/jre/bin/ControlPanel にあります。たとえば、Java 2 SDK を /usr/j2se にインストールした場合、フルパスは /usr/j2se/jre/bin/ControlPanel です。

（注）　Java 2 Runtime Environment をインストールした場合は、ファイルは <JRE インストール ディレクトリ >/bin/ControlPanel にあります。

ステップ 3　Java プラグイン 1.4.2 がインストールされている場合は、次の手順を実行します。

a. **Advanced** タブをクリックします。
b. **Java RunTime Parameters** フィールドに `-Xmx256m` と入力します。
c. **Apply** をクリックして Java Control Panel を閉じます。

ステップ 4　Java プラグイン 1.5 がインストールされている場合は、次の手順を実行します。

a. **Java** タブをクリックします。
b. Java Applet Runtime Settings の下で **View** をクリックします。
c. Java Runtime Parameters フィールドに `-Xmx256m` と入力し、**OK** をクリックします。
d. **OK** をクリックして Java Control Panel を終了します。

センサーの初期化

この項では、センサーの初期化方法について説明します。取り上げる事項は次のとおりです。

概要

センサーをネットワークに設置した後、**setup** コマンドを使用してセンサーを初期化する必要があります。**setup** コマンドを使用して、ホスト名、IP インターフェイス、Telnet サーバ、Web サーバ ポート、アクセス コントロール リスト、時間設定、およびインターフェイスの割り当てとイネーブル化など、センサーの基本的な設定を行います。センサーを初期化すると、ネットワーク経由でセンサーと通信できるようになります。その後、侵入防御を設定できます。

センサーの初期化

センサーを初期化するには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して次のようにセンサーにログインします。

- シリアル接続、またはモニタとキーボードを使用して、アプライアンスにログインします。

（注）　IDS-4215、IPS-4240、または IPS-4255 では、モニタとキーボードは使用できません。

- IDSM-2 とのセッション：
  - Catalyst ソフトウェアの場合

```
cat6k> enable
cat6k> (enable) session module_number
```

  - Cisco IOS ソフトウェアの場合

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

- NM-CIDS とのセッション：

```
router# service-module IDS-Sensor slot_number/port_number session
```

- AIP SSM とのセッション：

```
asa# session 1
```

（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。

ステップ 2　センサーへの初回ログインでは、デフォルト パスワードの変更を求められます。

パスワードは 8 文字以上の長さとし、容易に推測できないもの、つまり辞書に出ていない単語にする必要があります。

注意　パスワードを忘れた場合、センサー イメージの再作成が必要になることもあります（『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照）。ただし、管理者特権を持つ別のユーザがいる場合を除きます。別の管理者がログインして、パスワードを忘れたユーザに新しいパスワードを割り当てることができます。または、サポートのためにサービス アカウントを作成している場合には、TAC でパスワードを作成してもらうことができます。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating the Service Account」を参照してください。

パスワードを変更すると、`sensor#` プロンプトが表示されます。

ステップ 3　**`setup`** コマンドを入力します。

System Configuration Dialog が表示されます。

（注）　System Configuration Dialog は対話型のダイアログです。デフォルトの設定が表示されています。

```
    --- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
User ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Current Configuration:

service host
network-settings
host-ip 10.1.9.201/24,10.1.9.1
host-name sensor
telnet-option disabled
ftp-timeout 300
login-banner-text
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
summertime-option disabled
ntp-option disabled
exit
service web-server
port 443
exit

Current time: Wed May 5 10:25:35 2004
```

ステップ 4　Space キーを押して次の質問を表示します。

```
Continue with configuration dialog?[yes]:
```

一度に 1 ページずつ表示するには Space キーを押します。一度に 1 行ずつ表示するには **Enter** キーを押します。

ステップ 5　`yes` を入力して続行します。

ステップ 6　ホスト名を指定します。

ホスト名は 64 文字までの文字列で、大文字と小文字が区別されます。数字、“_”、“-” は有効ですが、スペースは使用できません。デフォルトは sensor です。

ステップ 7　IP インターフェイスを指定します。

IP インターフェイスは、IP アドレス / ネットマスク、ゲートウェイ（X.X.X.X/nn,Y.Y.Y.Y）の形式で指定します。ここで、X.X.X.X（X は 0 ～ 255）は、32 ビット アドレスのセンサーの IP アドレスで、ピリオドで区切った 4 つのオクテットで記述されています。nn はネットマスクの番号です。Y.Y.Y.Y（Y は 0 ～ 255）は、32 ビット アドレスのデフォルト ゲートウェイで、ピリオドで区切った 4 つのオクテットで記述されています。

ステップ 8　Telnet サーバのステータスを指定します。

Telnet サービスは disable または enable に設定できます。デフォルトは disable です。

ステップ 9　Web サーバ ポートを指定します。

Web サーバ ポートは Web サーバが使用する TCP ポートです（1 ～ 65535）。デフォルトは 443 です。

（注）　Web サーバ ポートを変更した場合は、IDM への接続時にブラウザの URL アドレスでそのポートを指定する必要があります。指定する形式は `https://`*sensor_ip_address*`:port`（たとえば、`https://10.1.9.201:1040`）です。

（注）　デフォルトでは、Web サーバは TLS および SSL の暗号化を使用するように設定されています。ポートを 80 に設定しても、暗号化は無効になりません。

ステップ 10　`yes` を入力してネットワーク アクセス リストを修正します。

a.　エントリを削除する場合は、エントリの番号を入力して **Enter** キーを押すか、または **Enter** キーを押して Permit 行に進みます。

b.　アクセス リストに追加するネットワークの IP アドレスおよびネットマスクを指定します。

IP ネットワーク インターフェイスは、IP アドレス / ネットマスクの形式、つまり X.X.X.X/nn 形式で表されます。X.X.X.X には、ネットワーク IP アドレスをピリオドで区切った 4 オクテットで記述された 32 ビットのアドレスで指定します。X = 0 ～ 255 です。nn には、そのネットワークのネットマスクのビット数を指定します。

たとえば、10.0.0.0/8 は 10.0.0.0 ネットワーク上のすべての IP アドレス（10.0.0.0 ～ 10.255.255.255）を許可し、10.1.1.0/24 は 10.1.1.0 サブネット上の IP アドレスだけ（10.1.1.0 ～ 10.1.1.255）を許可します。

ネットワーク全体ではなく単一の IP アドレスへのアクセスを許可する場合は、32 ビット ネットマスクを使用します。たとえば、10.1.1.1/32 は 10.1.1.1 のアドレスだけを許可します。

c. アクセス リストに追加するネットワークの入力がすべて終わるまで、ステップ b を繰り返します。

d. 空白の Permit 行で **Enter** キーを押して、次の手順に進みます。

ステップ 11 システム クロックの設定値を修正するには、**yes** を入力します。

a. NTP を使用する場合は **yes** を入力します。

NTP サーバの IP アドレス、NTP 鍵 ID、および NTP 鍵値が必要です。これらがこの時点で存在しない場合は、後で NTP を設定できます。手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring the Sensor to Use an NTP Server as its Time Source」を参照してください。

b. サマータイム設定を修正するには、**yes** を入力します。

（注） サマータイムは DST とも呼びます。サマータイムを採用していない地域の場合は、ステップ n に進みます。

c. サマータイムの設定方法を指定するには、recurring、date、または disable を入力します。

デフォルトは recurring です。

d. recurring を選択した場合は、サマータイム設定の開始月を入力します。

有効な値は、january、february、march、april、may、june、july、august、september、october、november、および december です。

デフォルトは april です。

e. サマータイム設定の開始週を指定します。

有効な値は first、second、third、fourth、fifth、および last です。

デフォルトは first です。

f. サマータイム設定の開始曜日を指定します。

有効な値は、sunday、monday、tuesday、wednesday、thursday、friday、および saturday です。

デフォルトは sunday です。

g. サマータイム設定の開始時刻を指定します。

デフォルトは 02:00:00 です。

（注） デフォルトの定期的なサマータイム パラメータはアメリカ合衆国の時間帯用です。デフォルト値は、開始時刻が 4 月の第 1 日曜日午前 2 時、終了時刻が 10 月の第 4 日曜日午前 2 時と指定します。デフォルトのサマータイム オフセットは 60 分です。

h. サマータイム設定の終了月を指定します。

有効な値は、january、february、march、april、may、june、july、august、september、october、november、および december です。

デフォルトは october です。

i. サマータイム設定の終了週を指定します。

有効な値は first、second、third、fourth、fifth、および last です。

デフォルトは last です。

j. サマータイム設定の終了曜日を指定します。

有効な値は、sunday、monday、tuesday、wednesday、thursday、friday、および saturday です。

デフォルトは sunday です。

k. サマータイム設定の終了時刻を指定します。

l. DST ゾーンを指定します。

ゾーン名は、最長で 24 文字の文字列で、[A-Za-z0-9()+:,_/-]+$ を使用できます。

m. サマータイム オフセットを指定します。

世界標準時（UTC）からのサマータイム オフセットを分単位で指定します（負数は、グリニッジ子午線より西側の時間帯を示します）。

デフォルトは 0 です。

n. システムの時間帯を修正するには、**yes** を入力します。

o. 標準時の時間帯名を指定します。

ゾーン名は 24 文字までの文字列です。

p. 標準時のオフセットを指定します。

デフォルトは 0 です。

世界標準時（UTC）からの標準時間帯のオフセットを分単位で指定します（負数は、グリニッジ子午線より西側の時間帯を示します）。

ステップ 12 **yes** を入力して、仮想センサーの設定を修正します（vs0）。

現在のインターフェイス設定が表示されます。

```
Current interface configuration
  Command control: GigabitEthernet0/1
  Unused:
    GigabitEthernet2/1
    GigabitEthernet2/0
  Promiscuous:
    GigabitEthernet0/0
  Inline:
    None
  Inline VLAN Pair:
    None
```

ステップ 13 混合インターフェイスまたはモニタリング インターフェイスを追加するには、**yes** と入力します。

ステップ 14 たとえば **GigabitEthernet0/1** のように、追加するインターフェイスを入力します。

ステップ 15 **yes** と入力して、インライン インターフェイス ペアを追加します（プラットフォームがインライン インターフェイス ペアをサポートしている場合だけ表示されます）。

a. インライン インターフェイス ペアの名前を入力します。

b. インライン インターフェイス ペアの説明を入力します。

デフォルトは、`Created via setup by user <yourusername>` です。

c. インライン ペアの最初のインターフェイスの名前 **interface1** を入力します。

d. インライン ペアの 2 番目のインターフェイスの名前 **interface2** を入力します。

e. ステップ a から d を繰り返して別のインライン インターフェイス ペアを追加するか、または **Enter** キーを押して次のオプションに進みます。

ステップ 16 **yes** と入力して、インライン VLAN ペアを追加します（プラットフォームがインライン VLAN ペアをサポートしている場合だけ表示されます）。

インライン VLAN ペアで使用可能なインターフェイスのリストが表示されます。

```
Available Interfaces:
 [1] GigabitEthernet0/0
 [2] GigabitEthernet2/0
 [3] GigabitEthernet2/1
```

ステップ 17 インライン VLAN ペアに分割するインターフェイスの番号を入力します。

そのインターフェイスの現在のインライン VLAN ペア設定が表示されます。

```
Inline Vlan Pairs for GigabitEthernet0/0
  None
```

a. 追加するサブインターフェイル番号を入力します。

b. インライン VLAN ペアの説明を入力します。

c. 1 番目の VLAN 番号（vlan1）を入力します。

d. 2 番目の VLAN 番号（vlan2）を入力します。

e. ステップ a から d を繰り返して別のインライン VLAN ペアをこのインターフェイスに追加するか、または **Enter** キーを押して次のオプションに進みます。

ステップ 18 **yes** を入力して、別のインターフェイスを分割します。インライン VLAN ペアの追加を完了するには、**no** と入力するか、または **Enter** キーを押します。

設定した内容が次のオプションと共に表示されます。

```
[0] Go to the command prompt without saving this config.
[1] Return back to the setup without saving this config.
[2] Save this configuration and exit setup.
```

ステップ 19 **2** を入力して設定を保存します。

```
Enter your selection[2]: 2
Configuration Saved.
```

ステップ 20 システムの日付と時刻を修正するには、**yes** を入力します。

（注） このオプションは、モジュールでは使用できません。また NTP が設定されている場合も使用できません。このモジュールは、設置されているルータまたはスイッチ、あるいは設定済みの NTP サーバから時刻を取得します。

a. 現地日付を入力します（yyyy-mm-dd）。

b. 現地時間を入力します（hh:mm:ss）。

ステップ 21 センサーをリブートします。

```
sensor# reset
Warning: Executing this command will stop all applications and reboot the node.
Continue with reset? []:
```

ステップ 22 **yes** を入力してリブートを続行します。

ステップ 23 自己署名 X.509 証明書を表示します（TLS で必要です）。

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 24 証明書のフィンガープリントを書き留めます。

この情報は、Web ブラウザでこのセンサーへ接続した際に証明書の信頼性を確認するために必要になります。

ステップ 25 最新のサービス パックおよびシグニチャ アップデートを適用します。

最新版のソフトウェアを入手する方法については、P.12-2 の「Cisco IPS ソフトウェアの入手方法」を参照してください。最新のソフトウェア アップデートを適用する方法は Readme で説明されています。

これでセンサーの侵入防御設定を行う準備ができました。

初期化の確認

センサーが初期化されていることを確認するには、次の手順を実行します。

ステップ 1 センサーにログインします。

手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Logging In to the Sensor」を参照してください。

ステップ 2　設定を表示します。

```
sensor# show configuration
generating current config:
! ------------------------------
! Version 5.1(1)
! Current configuration last modified Wed Jun 29 19:18:14 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
virtual-sensor vs0
physical-interface GigabitEthernet0/0 subinterface-number 0
physical-interface GigabitEthernet2/1
exit
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.149.27/25,10.89.149.126
host-name sensor
telnet-option enabled
access-list 10.0.0.0/8
access-list 64.0.0.0/8
access-list 171.0.0.0/8
exit
time-zone-settings
offset 0
standard-time-zone-name UTC
exit
exit
! ------------------------------
service interface
physical-interfaces GigabitEthernet0/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/0
admin-state enabled
exit
physical-interfaces GigabitEthernet2/1
admin-state enabled
exit
bypass-mode auto
interface-notifications
missed-percentage-threshold 19
notification-interval 36
idle-interface-delay 33
exit
exit
! ------------------------------
service logger
exit
! ------------------------------
service network-access
exit
! ------------------------------
service notification
exit
! ------------------------------
service signature-definition sig0
signatures 2000 0
alert-severity high
```

```
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 2004 0
alert-severity low
status
enabled true
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3201 1
alert-frequency
summary-mode fire-all
exit
exit
exit
signatures 3301 0
status
enabled true
exit
exit
signatures 3401 0
status
enabled true
retired false
exit
engine string-tcp
event-action produce-alert|request-block-host
exit
alert-frequency
summary-mode fire-all
exit
exit
exit
exit
! ------------------------------
service ssh-known-hosts
exit
! ------------------------------
service trusted-certificates
trusted-certificates 10.89.149.227:443 certificate MIICJDCCAY0CCPy71vhtAwyNMA0GC
SqGSIb3DQEBBQUAMFcxCzAJBgNVBAYTAlVTMRwwGgYDVQQKExNDaXNjbyBTeXN0ZW1zLCBJbmMuMRIwE
AYDVQQLEwlTU00tSVBTMTAxFjAUBgNVBAMTDTEwLjg5LjE0OS4yMjcwHhcNMDUwNjE0MDUwODA3WhcNM
DcwNjE1MDUwODA3WjBXMQswCQYDVQQGEwJVUzEcMBoGA1UEChMTQ2lzY28gU3lzdGVtcywgSW5jLjESM
BAGA1UECxMJU1NNLUlQUzEwMRYwFAYDVQQDEw0xMC44OS4xNDkuMjI3MIGfMA0GCSqGSIb3DQEBAQUAA
4GNADCBiQKBgQCoOobDuZOEPudw63Rlt8K1YsymzR/D9Rlcnad/U0gjAQGfcUh3sG3TXPQewon1fH0+A
nBw8Jxv/ovSB1HJ3ujh5k7BrrB2QMv73ESsBDdxLY6SoX/yYANMf4zPcPCAORJ6DMQHFj44A+3tMZWsC
yaod23S1oYOxx7v5puPDYn3IQIDAQABMA0GCSqGSIb3DQEBBQUAA4GBAHfPM7jawvdfXkYyazqvy3ZOK
kHVwHji12vBLo+biULJG95hbTFlqO+ba3R6nPD3tepgx5zTdOr2onnlFHWD95Ii+PKdUxj7vfDBG8atn
obsEBJ1lAQDiogskdCs4ax1tB4SbEU5y1tktKgcwWEdJpbbNJhzpoRsRICfM3HlOEwN
exit
! ------------------------------
service web-server
exit
sensor#
```

（注）　また、**more current-config** コマンドを使用して設定を表示することもできます。

ステップ 3　自己署名 X.509 証明書を表示します（TLS で必要です）。

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 4　証明書のフィンガープリントを書き留めます。

この情報は、Web ブラウザでこのセンサーへ接続した際に証明書の信頼性を確認するために必要になります。

IDM へのログイン

この項では、IDM へのログイン方法について説明します。取り上げる事項は次のとおりです。

概要

同時 CLI セッションの数は、プラットフォームに応じて制限されています。IDS-4210、IDS-4215、および NM-CIDS の同時 CLI セッションの数は、3 つに制限されています。その他のプラットフォームは 10 の同時セッションを許容します。

前提条件

IDM は、バージョン 5.0 センサーの一部です。**setup** コマンドを使用してセンサーを初期化し、IDM と通信できるようにする必要があります。手順については、P.1-6 の「センサーの初期化」を参照してください。

サポートされるユーザのロール

次のユーザのロールがサポートされています。

- 管理者
- オペレータ
- ビューア

IDM へのログイン

IDM へログインするには、次の手順を実行します。

ステップ 1　Web ブラウザを開き、センサーの IP アドレスを入力します。

https://*sensor_ip_address*

（注）　IDM はセンサーにインストール済みです。

（注）　デフォルト アドレスは `https://10.1.9.201` です。センサーを初期化するときに、ネットワーク環境を反映するように変更します。Web サーバ ポートを変更した場合は、IDM への接続時にブラウザの URL アドレスでそのポートを指定する必要があります。指定する形式は `https://`*sensor_ip_address*`:port`（たとえば、`https://10.1.9.201:1040`）です。

Security Alert ダイアログボックスが表示されます。セキュリティと IDM の詳細については、P.1-18 の「IDM と証明書」を参照してください。

ステップ 2　Enter Network Password ダイアログボックスにユーザ名とパスワードを入力し、**OK** をクリックします。

（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。センサーの初期化のときに、パスワードを変更するプロンプトが表示されます。手順については、P.1-6 の「センサーの初期化」を参照してください。

Cisco IDM 5.0 Information ウィンドウが開き、IDM をロードしていることが示されます。別のブラウザ ウィンドウに IDM が表示されます。

Memory Warning ダイアログボックスに次のメッセージが表示されます。

```
Your current Java memory heap size is less than 256 MB. You must increase the Java
memory heap size before launching IDM. Click Help for information on changing the Java
memory heap size.
```

ステップ 3　**Help** をクリックし、Java メモリのヒープ サイズを変更する手順を確認します。

ステップ 4　Java メモリのヒープ サイズを変更する手順を実行します。

ステップ 5　開いているブラウザ ウィンドウをすべて閉じます。

ステップ 6　ブラウザ ウィンドウを開いてセンサーの IP アドレスを入力し、IDM を再起動します。

ステップ 7　Password Needed - Networking ダイアログボックスにユーザ名とパスワードを入力し、**Yes** をクリックします。

Warning ダイアログボックスに次のメッセージが表示されます。

```
There is no license key installed on the sensor. To install a new license, go to
Configuration > Licensing.
```

センサーのライセンスを入手する手順については、P.1-23 の「センサーのライセンスの入手」を参照してください。

Status ダイアログボックスに次のメッセージが表示されます。

```
Please wait while the IDM is loading the current configuration from the Sensor.
```

IDM のメイン ウィンドウが表示されます。

IDM と Cookie

IDM は Cookie を使用してセッションを追跡し、一貫性のあるビューを提供します。IDM はセッション Cookie（一時的）のみを使用し、保管された Cookie は使用しません。Cookie がローカルに保管されることはないため、ブラウザの Cookie ポリシーに反することはありません。Cookie はブラウザではなく、IDM Java アプレットによって処理されます。

IDM と証明書

この項では、IDM において証明書がどのように機能するかについて説明します。取り上げる事項は次のとおりです。

証明書について

IPS 5.1 には、IDM を実行し、VMS などの管理ステーションの接続先である Web サーバが含まれています。ブロッキング転送センサーは、マスター ブロッキング センサーの Web サーバにも接続します。セキュリティを提供するため、この Web サーバは TLS として知られる暗号化プロトコルを使用します。TLS は SSL プロトコルに密接に関連しています。Web ブラウザに `https://`*ip_address* から始まる URL を入力すると、Web ブラウザは TLS または SSL プロトコルを使用して応答し、暗号化セッションをホストとネゴシエートします。

注意　Web ブラウザは、IDM が提示する証明書を最初に拒否します。これは、認証局（CA）を信頼しないためです。

（注）　IDM は、デフォルトで TLS および SSL を使用できるようになっています。TLS および SSL を使用することを強く推奨します。

TLS での暗号化セッションのネゴシエーション プロセスは、クライアントとサーバ間で多数の協調的な交換が発生するため、「ハンドシェイク」と呼ばれます。サーバはクライアントに証明書を送信します。クライアントは、この証明書に対して、次の 3 つの部分で構成されるテストを実行します。

1. 証明書で識別される発行元は信頼できるか。

   Web ブラウザは、信頼されたサードパーティ CA のリストと共に出荷されます。証明書で識別された発行元が、ブラウザが信頼する CA のリストに含まれている場合、最初のテストに合格します。

2. 日付は、証明書が有効だと見なされる日付範囲内か。

   証明書には、日付のペアで構成される Validity フィールドがあります。日付がこの日付範囲内の場合、2 番目のテストに合格します。

3. 証明書で識別されるサブジェクトの共通名が、URL ホスト名と一致するか。

   URL ホスト名が、サブジェクトの共通名と比較されます。一致した場合、3 番目のテストに合格します。

IDM に接続するように Web ブラウザに指示すると、センサーは独自の証明書を発行しますが（センサーが自分自身の CA）、ブラウザが信頼する CA のリストにセンサーが含まれていないため、返される証明書は失敗します。

ブラウザのエラー メッセージが表示されたときに、3 つのオプションがあります。

- サイトから即座に接続解除する。
- 残りの Web ブラウザ セッション用に証明書を受け入れる。
- 証明書で識別される発行元を Web ブラウザの信頼 CA リストに追加して、有効期間が経過するまで証明書を信頼する。

最も便利なオプションは、発行元を永続的に信頼することです。ただし、発行元を追加する前に、アウトオブバンド方式を使用して、証明書のフィンガープリントを検査します。これによって、センサーを詐称した攻撃者から被害を受けることを防ぎます。Web ブラウザに表示される証明書のフィンガープリントが、センサーのフィンガープリントと一致することを確認します。

注意　センサーの組織名またはホスト名を変更した場合は、次にセンサーを再度ブートしたときに、新しい証明書が生成されます。次に Web ブラウザが IDM に接続するときに、手動上書きダイアログボックスが表示されます。Internet Explorer、Netscape および Mozilla で、証明書フィンガープリントの検証を再度実行する必要があります。

Internet Explorer での CA の検証

Internet Explorer を使用して証明書フィンガープリントを検証するには、次の手順を実行します。

ステップ 1　Web ブラウザを開き、センサーの IP アドレスを入力して、IDM に接続します。

https://*sensor_ ip_address*

Security Alert パネルが表示されます。

ステップ 2　**View Certificate** をクリックします。

Certificate Information パネルが表示されます。

ステップ 3　**Details** タブをクリックします。

ステップ 4　リストを下にスクロールして **Thumbprint** を検索し、選択します。

テキスト フィールドにサムプリントが表示されます。

（注）　Certificate パネルは開いたままにします。

ステップ 5　次のいずれかの方法で、センサーに接続します。

- センサーのコンソール ポートに端末を接続する
- センサーに直接接続されたキーボードとモニタを使用する
- センサーに Telnet 接続する
- SSH で接続する

ステップ 6　TLS フィンガープリントを表示します。

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 7　SHA1 フィンガープリントと、開いている証明書のサムプリント テキスト フィールドに表示されている値を比較します。

受け入れようとする証明書が本物であることが確認されました。

注意　フィンガープリントが一致しない場合は、原因を判別する必要があります。センサーの正しい IP アドレスに接続したことを確認します。正しい IP アドレスに接続していて、フィンガープリントが一致しない場合は、センサーが危険にさらされている可能性があります。

ステップ 8　**General** タブをクリックします。

ステップ 9　**Install Certificate** をクリックします。

Certificate Import Wizard が表示されます。

ステップ 10　**Next** をクリックします。

Certificate Store ダイアログボックスが表示されます。

ステップ 11　**Place all certificates in the following store** を選択して、**Browse** をクリックします。

Select Certificate Store ダイアログボックスが表示されます。

ステップ 12　**Trusted Root Certification Authorities** をクリックして、**OK** をクリックします。

ステップ 13　**Next** をクリックして、**Finish** をクリックします。

Security Warning ダイアログボックスが表示されます。

ステップ 14　**Yes** をクリックして、**OK** をクリックします。

ステップ 15　**OK** をクリックして、Certificate ダイアログボックスを閉じます。

ステップ 16　**Yes** をクリックして IDM を開きます。

Netscape での CA の検証

Netscape を使用して証明書フィンガープリントを検証するには、次の手順を実行します。

ステップ 1　Web ブラウザを開き、センサーの IP アドレスを入力して、IDM に接続します。

```
https://sensor_ip_address
```

New Site Certificate パネルが表示されます。

ステップ 2　**Next** をクリックし、**More Info** をクリックします。

View A Certificate パネルが表示されます。

ステップ 3　次のいずれかの方法で、センサーに接続します。

- センサーのコンソール ポートに端末を接続する
- センサーに直接接続されたキーボードとモニタを使用する
- センサーに Telnet 接続する
- SSH で接続する

ステップ 4　TLS フィンガープリントを表示します。

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 5　MD5 フィンガープリントと View A Certificate パネルに表示された値を比較します。

受け入れようとする証明書が本物であることが確認されました。

注意　フィンガープリントが一致しない場合は、原因を判別する必要があります。センサーの正しい IP アドレスに接続したことを確認します。正しい IP アドレスに接続していて、フィンガープリントが一致しない場合は、センサーが危険にさらされている可能性があります。

ステップ 6　**OK** をクリックして、View A Certificate パネルを閉じます。

ステップ 7　**Next** をクリックし、**Accept this certificate forever (until it expires)** オプション ボタンをクリックします。

ステップ 8　**Next** を 2 回クリックして、**Finish** をクリックします。

Mozilla の CA の検証

Mozilla を使用して証明書フィンガープリントを検証するには、次の手順を実行します。

ステップ 1　Web ブラウザを開き、センサーの IP アドレスを入力して、IDM に接続します。

```
https://sensor_ip_address
```

Website Certified by an Unknown Authority パネルが表示されます。

ステップ 2　**Examine Certificate** をクリックします。

Certificate Viewer パネルが表示されます。

ステップ 3　次のいずれかの方法で、センサーに接続します。

- センサーのコンソール ポートに端末を接続する
- センサーに直接接続されたキーボードとモニタを使用する
- センサーに Telnet 接続する
- SSH で接続する

ステップ 4　TLS フィンガープリントを表示します。

```
sensor# show tls fingerprint
MD5: C4:BC:F2:92:C2:E2:4D:EB:92:0F:E4:86:53:6A:C6:01
SHA1: 64:9B:AC:DE:21:62:0C:D3:57:2E:9B:E5:3D:04:8F:A7:FD:CD:6F:27
```

ステップ 5　MD5 フィンガープリントと Certificate Viewer General タブに表示された値を比較します。

受け入れようとする証明書が本物であることが確認されました。

注意　フィンガープリントが一致しない場合は、原因を判別する必要があります。センサーの正しい IP アドレスに接続したことを確認します。正しい IP アドレスに接続していて、フィンガープリントが一致しない場合は、センサーが危険にさらされている可能性があります。

ステップ 6　**Close** をクリックして、Certificate Viewer パネルを閉じます。

ステップ 7　**Accept this certificate permanently** を選択し、**OK** をクリックしてパネルを閉じます。

ログイン ダイアログボックスが表示されます。

ステップ 8　**Prompt** ダイアログボックスにユーザ名とパスワードを入力します。

ステップ 9　**Yes** をクリックして証明書を受け入れます。

センサーのライセンスの入手

この項では、センサーのライセンスの入手方法について説明します。取り上げる事項は次のとおりです。

概要

センサーはライセンス キーがなくても動作しますが、シグニチャ アップデートを取得するには、ライセンス キーが必要です。ライセンス キーを入手するには、IPS に関するシスコのサービス契約が必要です。契約を購入するには、代理店、シスコのサービス担当者または営業担当者にお問い合せください。詳細については、P.1-24 の「IPS 製品のサービス プログラム」を参照してください。

トライアル ライセンス キーも使用可能です。契約内容が不明なためにセンサーのライセンスを入手できない場合は、ライセンスが必要なシグニチャ アップデートをサポートしている 60 日のトライアル ライセンスを入手してください。

Cisco.com のライセンシング サーバから取得したライセンス キーは、センサーに送信されます。または、ローカル ファイルに含まれているセンサー ライセンス キーからセンサーのライセンス キーをアップデートすることもできます。ライセンス キーを申し込むには、http://www.cisco.com/go/license にアクセスして、**IPS Signature Subscription Service** をクリックします。手順については、P.1-26 の「ライセンス キーの取得とインストール」を参照してください。

ライセンス キーの取得には、IPS デバイスのシリアル番号が必要です。IDM で IPS デバイスのシリアル番号を見つけるには、**Configuration > Licensing** をクリックするか、CLI で **show version** コマンドを実行します。

ライセンス キーのステータスは、IDM の Licensing パネルで確認できます。IDM を起動するたびに、ライセンスのステータスが表示されます。ライセンス キーのステータスは、trial、invalid、または expired のいずれかです。ライセンス キーがない場合や、無効な場合、または期限が切れている場合でも、IDM を継続して使用できますが、シグニチャ アップデートはダウンロードできません。

CLI に入ると、ライセンス ステータスが通知されます。たとえば、ライセンスがインストールされていない場合は、次のメッセージが表示されます。

```
***LICENSE NOTICE***
There is no license key installed on the system.
The system will continue to operate with the currently installed
signature set. A valid license must be obtained in order to apply
signature updates. Please go to http://www.cisco.com/go/license
to obtain a new license or install a license.
```

このメッセージは、ライセンス キーをインストールするまで毎回表示されます。

IPS 製品のサービス プログラム

ライセンス キーをダウンロードしたり、最新の IPS シグニチャ アップデートを入手したりするには、IPS 製品の Cisco Services for IPS サービス契約を購入している必要があります。シスコシステムズと直接のお付き合いがある場合は、アカウント マネージャまたはサービス アカウント マネージャに連絡して、Cisco Services for IPS サービス契約を購入してください。シスコシステムズと直接のお付き合いがない場合は、1 ティアまたは 2 ティア パートナーからサービス アカウントを購入できます。

次の IPS 製品を購入する場合は、Cisco Services for IPS サービス契約も購入する必要があります。

- IDS-4215
- IPS-4240
- IPS-4255
- IDSM-2
- NM-CIDS

ASA 製品の場合、IPS を含まない次の ASA 製品のいずれかを購入したときは、SMARTnet 契約を購入する必要があります。

（注） SMARTnet は、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、およびオンサイトのハードウェア交換（NBD）を提供します。

- ASA5510-K8
- ASA5510-DC-K8
- ASA5510-SEC-BUN-K9
- ASA5520-K8
- ASA5520-DC-K8
- ASA5520-BUN-K9
- ASA5540-K8
- ASA5540-DC-K8
- ASA5540-BUN-K9

AIP SSM がインストールされた状態で出荷される次の ASA 製品のいずれかを購入した場合、または AIP SSM を購入してご使用の ASA 製品に追加した場合は、Cisco Services for IPS サービス契約を購入する必要があります。

（注） Cisco Services for IPS は、IPS シグニチャのアップデート、オペレーティング システムのアップデート、Cisco.com へのアクセス、TAC へのアクセス、およびオンサイトのハードウェア交換（NBD）を提供します。

- ASA5510-AIP10-K9
- ASA5520-AIP10-K9
- ASA5520-AIP20-K9
- ASA5540-AIP20-K9
- ASA-SSM-AIP-10-K9
- ASA-SSM-AIP-20-K9

たとえば、ASA-5510 を購入した後で IPS および購入済み ASA-SSM-AIP-10-K9 を追加する場合は、Cisco Services for IPS サービス契約を購入する必要があります。

Cisco Services for IPS サービス契約を購入したら、製品シリアル番号を入力してライセンス キーを申し込む必要があります。手順については、P.1-26 の「ライセンス キーの取得とインストール」を参照してください。

注意　お使いの製品に対して RMA を実行した場合、シリアル番号は変更されます。次に、新規シリアル番号用の新規ライセンス キーを取得する必要があります。

サポートされるユーザのロール

Licensing パネルにライセンス情報を表示したり、センサーのライセンス キーをインストールしたりするには、管理者である必要があります。

フィールド定義

Licensing パネルには、次のフィールドとボタンがあります。

フィールドの説明：

- **Current License**：現在のライセンスのステータスが表示されます。
  - **License Status**：センサーの現在のライセンスのステータスです。
  - **Expiration Date**：ライセンス キーの有効期限が切れる（または切れた）日付。
    ライセンス キーが無効な場合、日付は表示されません。
  - **Serial Number**：センサーのシリアル番号です。
- **Update License**：新しいライセンス キーの取得先を指定します。
  - **Cisco Connection Online**：ライセンス キーを取得するために、Cisco.com のライセンス サーバに接続します。
  - **License File**：ライセンス ファイルを使用するように指定します。
  - **Local File Path**：ライセンス キーが含まれているローカル ファイルを示します。

ボタンの機能：

- **Download**：IDM を実行しているコンピュータにライセンスのコピーをダウンロードし、ローカル ファイルに保存します。その後、紛失または破損したライセンスと置き換えたり、センサーのイメージの再作成後に再インストールしたりできます。
  センサー上に有効なライセンスがない場合、**Download** ボタンはディセーブルになっています。
- **Browse Local**：ライセンス キーを探すためのファイル ブラウザを起動します。
- **Update License**：選択したオプションに基づいて、新しいライセンス キーをセンサーに送信します。

ライセンス キーの取得とインストール

ライセンス キーをインストールするには、次の手順を実行します。

ステップ 1　管理者特権を持つアカウントを使用して IDM にログインします。

ステップ 2　**Configuration > Licensing** をクリックします。

Licensing パネルに現在のライセンスのステータスが表示されます。ライセンスがインストール済みの場合、必要に応じて **Download** をクリックして保存します。

ステップ 3　次のいずれかを実行してライセンス キーを取得します。

- Cisco.com からライセンスを取得するには、**Cisco Connection Online** を選択します。

  IDM は、Cisco.com のライセンス サーバに接続し、サーバにシリアル番号を送信してライセンス キーを取得します。これがデフォルトの方法です。ステップ 4 に進みます。
- ライセンス ファイルを使用するには、**License File** を選択します。

  このオプションを使用するには、www.cisco.com/go/license で、ライセンス キーを申し込む必要があります。

  ライセンス キーは、電子メールで送られてきます。送られてきたライセンス キーは、IDM がアクセスできるドライブに保存してください。コンピュータが Cisco.com にアクセスできない場合に、このオプションが役立ちます。ステップ 7 に進みます。

ステップ 4　**Update License** をクリックします。

Licensing ダイアログボックスが表示されます。

ステップ 5　**Yes** をクリックして続行します。

Status ダイアログボックスに、センサーが Cisco.com に接続中であることが示されます。Information ダイアログボックスで、ライセンス キーが更新されたことを確認できます。

ステップ 6　**OK** をクリックします。

ステップ 7　www.cisco.com/go/license にアクセスします。

ステップ 8　必須フィールドに入力します。

注意　IPS デバイスの正しいシリアル番号を用意しておく必要があります。これは、その番号のデバイスでだけライセンス キーが機能するからです。

ライセンス キーは指定した電子メール アドレスに送られます。

ステップ 9　ライセンス キーは、IDM を動作中のクライアントがアクセス可能なハードディスク ドライブまたはネットワーク ドライブに保存します。

ステップ 10　IDM にログインします。

ステップ 11 **Configuration > Licensing** をクリックします。

ステップ 12 Update License で、**Update From: License File** を選択します。

ステップ 13 **Local File Path** フィールドにライセンス ファイルへのパスを指定するか、または **Browse Local** をクリックしてライセンス ファイルを参照します。

Select License File Path ダイアログボックスが表示されます。

ステップ 14 ライセンス ファイルを参照して、**Open** をクリックします。

ステップ 15 **Update License** をクリックします。