トラブルシューティング

この付録では、センサーとソフトウェアのトラブルシューティングのヒントと手順を示します。この章は、次の項で構成されています。

- 予防保守（P.C-2）
- 障害リカバリ（P.C-3）
- パスワード リカバリ（P.C-4）
- 4200 シリーズ アプライアンスのトラブルシューティング（P.C-5）
- IDM のトラブルシューティング（P.C-41）
- IDSM-2 のトラブルシューティング（P.C-46）
- AIP SSM のトラブルシューティング（P.C-54）
- 情報の収集（P.C-56）

予防保守

次のアクションは、センサーの保守に役立ちます。

- 適切なコンフィギュレーションをバックアップします。現在のコンフィギュレーションが使用できなくなった場合に、バックアップ バージョンに置換できます。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating and Using a Backup Configuration File」を参照してください。
- バックアップ コンフィギュレーションをリモート システムに保存します。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Copying and Restoring the Configuration File Using a Remote Server」を参照してください。
- 手動でアップグレードする前に、必ずコンフィギュレーションをバックアップしてください。自動アップグレードを設定してある場合は、定期的なバックアップを実行してください。
- サービス アカウントを作成します。

  サービス アカウントは、パスワードのリカバリや、TAC によって指示されたその他の特別なデバッグ状況に必要です。

  手順については、『*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。

注意　サービス アカウントを作成するかどうかは慎重に検討してください。サービス アカウントは、システムへのシェル アクセスを提供します。これにより、システムは脆弱になります。しかし、サービス アカウントを使用すると、管理者パスワードを喪失した場合に新規パスワードを作成することができます。状況を分析して、サービス アカウントをシステム上に存在させるかどうかを決定します。

（注）　AIP SSM へのシェル アクセスを取得できないので、AIP SSM でパスワード リカバリ用のサービス アカウントを使用することはできません。AIP SSM へのシェル アクセスを取得するには、ROMMON を使用する必要があります。

障害リカバリ

この項では、障害の後にセンサーを復旧する必要がある場合の推奨事項と実行すべきステップを示します。

障害が発生した場合に備えて、これらの推奨事項に従ってください。

- コンフィギュレーションに CLI または IDM を使用している場合は、変更を加えるたびに現在のコンフィギュレーションをセンサーから FTP または SCP サーバへコピーします。

  手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating and Using a Backup Configuration File」を参照してください。

  （注）　そのコンフィギュレーションの特定のソフトウェア バージョンをメモしておく必要があります。コピーしたコンフィギュレーションは、同じバージョンのセンサーにしか適用できません。

  （注）　また、そのセンサーで使用したユーザ ID のリストも必要です。ユーザ ID とパスワードのリストは、コンフィギュレーションに保存されません。現在のセンサー上のユーザのリストを取得する手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Viewing User Status」を参照してください。

- IDS MC を使用している場合、現在のコンフィギュレーションは IDS MC データベースに保存されるので、別のコピーは必要ありません。

  （注）　ユーザ ID のリストは、IDS MC データベースには保存されません。ユーザ ID をメモしておく必要があります。

  （注）　そのコンフィギュレーションの特定のソフトウェア バージョンをメモしておく必要があります。コピーしたコンフィギュレーションは、同じバージョンのセンサーにしか適用できません。

障害が発生し、センサーを回復する必要がある場合は、次の手順を実行します。

1. センサーのイメージを再作成します。

   アプライアンスとモジュールの場合の手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。

2. デフォルト ユーザ ID とパスワード cisco を使用してセンサーにログインします。

   （注）　cisco パスワードを変更するよう求めるプロンプトが表示されます。

3. **setup** コマンドを実行します。

   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。

4. コンフィギュレーションが最後に保存されコピーされたときの IPS ソフトウェア バージョンにセンサーをアップグレードします。

   IPS ソフトウェアのバージョンを確認し、それらをインストールする方法の詳細については、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。

警告　センサーを障害前と同じ IPS ソフトウェア バージョンに戻さずに、保存したコンフィギュレーションをコピーしようとすると、コンフィギュレーション エラーが発生する可能性があります。

5. 最後に保存したコンフィギュレーションをセンサーにコピーします。

   手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1* 』の「Creating and Using a Backup Configuration File」を参照してください。

6. センサーの新しい鍵と証明書を使用するようにクライアントをアップデートします。

   イメージを再作成すると、センサーの SSH 鍵と HTTPS 証明書が変更されます。手順については、P.2-12 の「既知のホスト鍵の定義」を参照してください。

7. 前のユーザを作成します。

   手順については、P.2-28 の「ユーザの設定」を参照してください。

パスワード リカバリ

次のパスワード リカバリ オプションが存在します。

- 別の管理者アカウントが存在する場合、もう一方の管理者はパスワードを変更できます。
- サービス アカウントが存在する場合は、サービス アカウントにログインし、コマンド **su - root** を使用してユーザ root に切り替えることができます。CLI 管理者アカウントのパスワードを変更するには、**password** コマンドを使用します。たとえば、管理者のユーザ名が「adminu」である場合、コマンドは **password adminu** になります。新規パスワードを 2 度入力するよう求めるプロンプトが表示されます。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。

リカバリ パーティションまたはシステム イメージ ファイルを使用して、センサーのイメージを再作成することができます。詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。

4200 シリーズ アプライアンスのトラブルシューティング

この項では、4200 シリーズ アプライアンスのトラブルシューティングについて説明します。

ヒント　アプライアンスをトラブルシューティングする前に、センサーにインストールしたソフトウェアバージョンの Readme で警告の項を調べて、既知の問題を確認してください。

この項で取り上げる事項は次のとおりです。

- 通信の問題（P.C-5）
- SensorApp およびアラート（P.C-11）
- ブロッキング（P.C-19）
- ロギング（P.C-28）
- センサーが NTP サーバと同期していることを確認する（P.C-34）
- シグニチャに対して TCP リセットが実行されない（P.C-35）
- ソフトウェア アップグレード（P.C-37）

通信の問題

この項では、4200 シリーズのセンサーでの通信の問題のトラブルシューティングについて説明します。取り上げる事項は次のとおりです。

- Telnet または SSH を使用してセンサー CLI にアクセスできない（P.C-5）
- 設定が誤っているアクセス リスト（P.C-8）
- 重複する IP アドレスによりインターフェイスがシャットダウンする（P.C-9）

Telnet または SSH を使用してセンサー CLI にアクセスできない

Telnet（すでにイネーブルにしてある場合）または SSH でセンサー CLI にアクセスできない場合は、次の手順を実行します。

（注）　センサーで Telnet をイネーブルまたはディセーブルにする手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Enabling and Disabling Telnet」を参照してください。

ステップ 1　コンソール、端末、またはモジュール セッションからセンサー CLI にログインします。

センサー上で CLI セッションを直接開くさまざまな方法については、『*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　センサーの管理インターフェイスがイネーブルになっていることを確認します。

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 944333
   Total Bytes Received = 83118358
   Total Multicast Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 397633
   Total Bytes Transmitted = 435730956
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

管理インターフェイスは、ステータス行 `Media Type = TX` が記述されたリスト内のインターフェイスです。Link Status が `Down` である場合はステップ 3 に進んでください。Link Status が `Up` である場合はステップ 5 に進んでください。

ステップ 3　センサーの IP アドレスが固有であることを確認します。

```
sensor# setup
--- 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 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

ネットワーク上の別のデバイスが同じ IP アドレスを持っていることを管理インターフェイスが検出した場合、管理インターフェイスは起動しません。

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing the IP Address, Netmask, and Gateway」を参照してください。

ステップ 4　管理ポートがアクティブなネットワーク接続に接続していることを確認します。

管理ポートがアクティブなネットワーク接続に接続されていない場合、管理インターフェイスは起動しません。

ステップ 5　センサーに接続しようとしているワークステーションの IP アドレスがセンサーのアクセス リストで許可されていることを確認してください。

```
sensor# setup
--- 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 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no login-banner-text
exit
--MORE--
```

ワークステーションのネットワーク アドレスがセンサーのアクセス リストで許可されている場合は、ステップ 6 に進みます。

ステップ 6　ワークステーションのネットワーク アドレス用に許可エントリを追加し、コンフィギュレーションを保存し、接続を再試行します。

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing the Access List」を参照してください。

ステップ 7　ネットワーク　コンフィギュレーションでワークステーションがセンサーに接続できるようになっていることを確認します。

ファイアウォールの後ろでセンサーが保護されていて、ワークステーションがファイアウォールの前にある場合は、ワークステーションがセンサーにアクセスできるようにファイアウォールが設定されていることを確認します。あるいは、ワークステーションの IP アドレスでネットワーク アドレス変換を実行しているファイアウォールの後ろにワークステーションがあり、センサーがファイアウォールの前にある場合は、センサーのアクセス リストにワークステーションの変換済みアドレス用の許可エントリが含まれていることを確認します。

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing the Access List」を参照してください。

設定が誤っているアクセス リスト

設定が誤っているアクセス リストを訂正するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　コンフィギュレーションを表示してアクセス リストを確認します。

```
sensor# show configuration | include access-list
access-list 10.0.0.0/8
access-list 64.0.0.0/8
sensor#
```

ステップ 3　許可されたネットワークのリストにクライアントの IP アドレスがあることを確認します。ない場合は、追加します。

```
sensor# configure terminal
sensor(config)# service host
sensor(config-hos)# network-settings
sensor(config-hos-net)# access-list 171.69.70.0/24
```

ステップ 4　設定を確認します。

```
sensor(config-hos-net)# show settings
   network-settings
   ------------------------------------------------
      host-ip: 10.89.149.238/25,10.89.149.254 default: 10.1.9.201/24,10.1.9.1
      host-name: qsensor-238 default: sensor
      telnet-option: enabled default: disabled
      access-list (min: 0, max: 512, current: 3)
      ------------------------------------------------
         network-address: 10.0.0.0/8
         ------------------------------------------------
         network-address: 64.0.0.0/8
         ------------------------------------------------
         network-address: 171.69.70.0/24
         ------------------------------------------------
      ------------------------------------------------
      ftp-timeout: 300 seconds <defaulted>
      login-banner-text: <defaulted>
   ------------------------------------------------
sensor(config-hos-net)#
```

重複する IP アドレスによりインターフェイスがシャットダウンする

同じ IP アドレスで新しくイメージが作成されたセンサーが 2 つあり、それらが同じネットワーク上で同時に起動すると、インターフェイスはシャットダウンします。Linux は、別のホストとのアドレスの競合を検出すると、コマンド / コントロール インターフェイスがアクティブ化するのを妨げます。

該当するセンサーにネットワーク上の別のホストとの IP アドレスの競合がないことを確認するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　インターフェイスが起動しているかどうかを判別します。

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1822323
   Total Bytes Received = 131098876
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 219260
   Total Bytes Transmitted = 103668610
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

コマンド/コントロール インターフェイスのリンク ステータスがダウンであることが出力で示されている場合は、ハードウェアの問題または IP アドレスの競合があります。

ステップ 3　センサーの配線が正しいことを確認します。

『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』のセンサーの章を参照してください。

ステップ 4　**setup** コマンドを実行して、IP アドレスが正しいことを確認します。

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。

SensorApp およびアラート

この項では、SensorApp およびアラートでのトラブルシューティングの問題について説明します。取り上げる事項は次のとおりです。

- SensorApp が動作していない（P.C-11）
- 物理接続、SPAN、または VACL ポートの問題（P.C-12）
- アラートが表示されない（P.C-14）
- センサーがパケットを検出しない（P.C-16）
- 破損した SensorApp コンフィギュレーションの削除（P.C-18）
- IDS-4250-XL の不良なメモリ（P.C-18）

SensorApp が動作していない

センシング プロセスの SensorApp は、常に動作している必要があります。動作していない場合は、アラートを受信しません。SensorApp は分析エンジンの一部なので、分析エンジンが動作していることを確認する必要があります。

分析エンジンが動作し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　CLI にログインします。

ステップ 2　分析エンジン サービスのステータスを判別します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1)S149.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: ASA-SSM-20
Serial Number: 021
No license present
Sensor up-time is 19 days.
Using 505495552 out of 1984704512 bytes of available memory (25% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 37.7M out of 166.6M bytes of available disk space (24%
usage)
boot is using 40.5M out of 68.5M bytes of available disk space (62% usage)


MainApp          2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Running
AnalysisEngine   2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Not
Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149

sensor#
```

ステップ 3　分析エンジンが動作していない場合は、それにつながるエラーを検索します。

```
sensor# show events error fatal past 13:00:00 | include AnalysisEngine
evError: eventId=1077219258696330005 severity=warning

originator:
hostId: sensor
appName: sensorApp
appInstanceId: 1045
time: 2004/02/19 19:34:20 2004/02/19 19:34:20 UTC
errorMessage: name=errUnclassified Generating new Analysis Engine configuration file.
```

（注）　最後の再起動の日付と時刻がリストされます。この例では、最後の再起動は 2004 年 2 月 19 日の 7 時 34 分でした。

ステップ 4　最新のソフトウェア アップデートを持っていることを確認してください。

```
sensor# show version
Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149
```

最新のソフトウェア アップデートを持っていない場合は、Cisco.com からそれらをダウンロードします。手順については、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。

ステップ 5　ソフトウェア アップグレードに付属している Readme を参照して、SensorApp または分析エンジンの既知の DDTS を確認してください。

物理接続、SPAN、または VACL ポートの問題

センサーが適切に接続されていない場合は、アラートを受信しません。

センサーが適切に接続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　CLI にログインします。

ステップ 2　インターフェイスが起動していることと、パケット カウントが増加していることを確認します。

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 1830137
   Total Bytes Received = 131624465
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 220052
   Total Bytes Transmitted = 103796666
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

ステップ 3　Link Status がダウンである場合は、センシング ポートが適切に接続されていることを確認します。

a.　センシング ポートがアプライアンスで適切に接続されていることを確認します。

『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』のアプライアンスの章を参照してください。

b.　センシング ポートが IDSM-2 で正しい SPAN または VACL キャプチャ ポートに接続されていることを確認します。

『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の IDSM-2 の章を参照してください。

ステップ 4　インターフェイス コンフィギュレーションを確認します。

a.　インターフェイスが正しく設定されていることを確認します。

手順については、P.3-10 の「インターフェイスの設定」を参照してください。

b. Cisco スイッチで SPAN および VACL キャプチャ ポート コンフィギュレーションを確認します。

手順についてはスイッチのマニュアルを参照してください。

ステップ 5 インターフェイスが起動していることと、パケット　カウントが増加していることを再び確認します。

```
sensor# show interfaces
```

アラートが表示されない

アラートが表示されない場合は、次のことを試してください。

- シグニチャがイネーブルになっていることを確認します。
- シグニチャが非アクティブになっていないことを確認します。
- Produce Alert がアクションとして設定されていることを確認します。

（注） Produce Alert を選択した後、戻って別のイベント アクションを追加し、Produce Alert を新規コンフィギュレーションに追加しないと、アラートはイベント ストアに送信されません。シグニチャを設定するたびに、新規コンフィギュレーションが古いコンフィギュレーションを上書きするので、各シグニチャに必要なイベント アクションをすべて設定してあることを確認してください。

- センサーがパケットを検出していることを確認します。
- アラートが生成中であることを確認します。

アラートが表示され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 CLI にログインします。

ステップ 2 シグニチャがイネーブルになっていることを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# status
sensor(config-sig-sig-sta)# show settings
   status
   -----------------------------------------------
      enabled: true <defaulted>
      retired: false <defaulted>
   -----------------------------------------------
sensor(config-sig-sig-sta)#
```

ステップ 3　Produce Alert が設定されていることを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine ?
normalizer     Signature engine
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert
sensor(config-sig-sig-nor)# show settings
   normalizer
   ----------------------------------------------
      event-action: produce-alert default: produce-alert|deny-connection-inline
      edit-default-sigs-only
      ---------------------------------------------
sensor#
```

ステップ 4　センサーがパケットを検出していることを確認します。

```
sensor# show interfaces FastEthernet0/1
MAC statistics from interface FastEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 267581
   Total Bytes Received = 24886471
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 57301
   Total Bytes Transmitted = 3441000
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 1
   Total Transmit FIFO Overruns = 0
sensor#
```

ステップ 5　アラートをチェックします。

```
sensor# show statistics virtual-sensor
SigEvent Preliminary Stage Statistics
    Number of Alerts received = 0
    Number of Alerts Consumed by AlertInterval = 0
    Number of Alerts Consumed by Event Count = 0
    Number of FireOnce First Alerts = 0
    Number of FireOnce Intermediate Alerts = 0
    Number of Summary First Alerts = 0
    Number of Summary Intermediate Alerts = 0
    Number of Regular Summary Final Alerts = 0
    Number of Global Summary Final Alerts = 0
    Number of Alerts Output for further processing = 0alertDetails: Traffic Source:
int0 ;
```

センサーがパケットを検出しない

センサーがネットワーク上のパケットを検出していない場合は、インターフェイスのセットアップが正しくない可能性があります。

センサーがパケットを検出していない場合は、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　インターフェイスが起動し、パケットを受信していることを確認します。

```
sensor# show interfaces GigabitEthernet0/1
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Down
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

ステップ 3　インターフェイスが起動していない場合は、次の手順を実行します。

a.　配線を確認します。

センサーが適切にインストールされているかどうか確認する手順については、『*Installing Cisco Intrusion Prevention System Appliances and Modules 5.1*』のセンサーの章を参照してください。

b. インターフェイスをイネーブルにします。

```
sensor# configure terminal
sensor(config)# service interface
sensor(config-int)# physical-interfaces GigabitEthernet0/1
sensor(config-int-phy)# admin-state enabled
sensor(config-int-phy)# show settings
   <protected entry>
   name: GigabitEthernet0/1
   ----------------------------------------------
      media-type: tx <protected>
      description: <defaulted>
      admin-state: enabled default: disabled
      duplex: auto <defaulted>
      speed: auto <defaulted>
      alt-tcp-reset-interface
      ----------------------------------------------
         none
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
   ----------------------------------------------
sensor(config-int-phy)#
```

ステップ 4　インターフェイスが起動し、パケットを受信しているかどうかを確認します。

```
sensor# show interfaces
MAC statistics from interface GigabitEthernet0/1
   Media Type = TX
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 3
   Total Bytes Received = 900
   Total Multicast Packets Received = 3
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0 ...
```

破損した SensorApp コンフィギュレーションの削除

SensorApp コンフィギュレーションが破損し SensorApp を実行できない場合は、コンフィギュレーションを完全に削除して SensorApp を再起動する必要があります。

SensorApp 設定を削除するには、次の手順を実行します。

ステップ 1　サービス アカウントにログインします。

ステップ 2　su で root になります。

ステップ 3　IPS アプリケーションを停止します。

```
/etc/init.d/cids stop
```

ステップ 4　仮想センサー ファイルを置換します。

```
cp /usr/cids/idsRoot/etc/defVirtualSensorConfig.xml
/usr/cids/idsRoot/etc/VS-Config/virtualSensor.xml
```

ステップ 5　キャッシュ ファイルを削除します。

```
rm /usr/cids/idsRoot/var/virtualSensor/*.pmz
```

ステップ 6　サービス アカウントを終了します。

ステップ 7　センサー CLI にログインします。

ステップ 8　IPS サービスを開始します。

```
sensor# cids start
```

ステップ 9　管理者特権でアカウントにログインします。

ステップ 10　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? [yes]:yes
Request Succeeded.
sensor#
```

IDS-4250-XL の不良なメモリ

IDS-4250-XL の中には、問題のある DIMM を XL カードに搭載して出荷されたものがあります。問題のある DIMM によって、センサーが停止したり、SensorApp が機能を停止してコア ファイルを生成したりすることがあります。

IDS-4250-XL のメモリに問題があるかどうかを確認する手順については、Partner Field 52563 を参照してください。

ブロッキング

この項では、ブロッキングと ARC サービスのためのトラブルシューティングのヘルプを提供します。取り上げる事項は次のとおりです。

- ブロッキングのトラブルシューティング（P.C-19）
- ARC が動作していることを確認する（P.C-20）
- ARC 接続がアクティブであることを確認する（P.C-20）
- デバイス アクセスの問題（P.C-22）
- ネットワーク デバイスのインターフェイスと方向を確認する（P.C-24）
- ネットワーク デバイスへの SSH 接続をイネーブルにする（P.C-25）
- シグニチャに対してブロッキングが実行されない（P.C-25）
- マスター ブロッキング センサーのコンフィギュレーションを確認する（P.C-26）

ブロッキングのトラブルシューティング

ARC を設定した後、**show version** コマンドを使用して、ARC が適切に動作するかどうかを確認できます。ARC がネットワーク デバイスに接続されていることを確認するには、**show statistics network-access** コマンドを使用します。

（注）ARC は、以前は Network Access Controller と呼ばれていました。IPS 5.1 から名前は変更されましたが、IDM と CLI では引き続き Network Access Controller、**nac**、および **network-access** として示されています。

ARC をトラブルシューティングするには、次の手順を実行します。

1. ARC が動作していることを確認します。

   手順については、P.C-20 の「ARC が動作していることを確認する」を参照してください。

2. ARC がネットワーク デバイスに接続していることを確認します。

   手順については、P.C-20 の「ARC 接続がアクティブであることを確認する」を参照してください。

3. Event Action が特定のシグニチャの Block Host に設定されていることを確認します。

   手順については、P.C-25 の「シグニチャに対してブロッキングが実行されない」を参照してください。

4. マスター ブロッキング センサーが適切に設定されていることを確認します。

   手順については、P.C-26 の「マスター ブロッキング センサーのコンフィギュレーションを確認する」を参照してください。

（注）ARC アーキテクチャの説明については、P.A-12 の「ARC」を参照してください。

ARC が動作していることを確認する

ARC が動作していることを確認するには、**show version** コマンドを使用します。MainApp が動作していないと、ARC は実行できません。ARC は MainApp の一部です。

ステップ 1　CLI にログインします。

ステップ 2　MainApp が動作していることを確認します。

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(1.1)S152.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
Sensor up-time is 3 days.
Using 734863360 out of 3974291456 bytes of available memory (18% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 35.6M out of 166.8M bytes of available disk space (23%
usage)
boot is using 40.5M out of 68.6M bytes of available disk space (62% usage)


MainApp          2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600   Not
Running
AnalysisEngine   2005_Mar_18_12.53   (Release)   2005-03-18T13:03:21-0600   Running
CLI              2005_Mar_04_14.23   (Release)   2005-03-04T14:35:11-0600


Upgrade History:

  IDS-K9-sp-5.0-1.1-   12:53:00 UTC Fri Mar 18 2005

Recovery Partition Version 1.1 - 5.0(1.1)

sensor#
```

ステップ 3　MainApp が `Not Running` と表示した場合、ARC は動作していません。TAC に連絡します。

ARC 接続がアクティブであることを確認する

ARC 統計情報で State が `Active` でない場合は、問題が生じています。

統計情報内で State が Active であ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　CLI にログインします。

ステップ 2　ARC が接続していることを確認します。

出力の State セクションを調べて、すべてのデバイスが接続中であることを確認します。

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
   NetDevice
      Type = Cisco
      IP = 10.89.147.54
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = fa0/0
         InterfaceDirection = in
State
   BlockEnable = true
   NetDevice
      IP = 10.89.147.54
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
sensor#
```

ステップ 3　ARC が接続していない場合は、繰り返し発生するエラーを検索してください。

```
sensor# show events error hh:mm:ss month day year | include : nac
```

例

```
sensor# show events error 00:00:00 Apr 01 2005 | include : nac
```

ステップ 4　最新のソフトウェア アップデートを持っていることを確認してください。

```
sensor# show version
Upgrade History:

  IDS-K9-maj-5.0-1-   14:16:00 UTC Thu Mar 04 2004

Recovery Partition Version 1.1 - 5.0(1)S149
```

最新のソフトウェア アップデートを持っていない場合は、Cisco.com からそれらをダウンロードします。手順については、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。

ステップ 5　ソフトウェア アップグレードに付属している Readme を参照して、ARC の既知の DDTS を確認してください。

ステップ 6　各デバイスのコンフィギュレーション設定が正しいことを確認します（ユーザ名、パスワード、IP アドレス）。

手順については、P.C-22 の「デバイス アクセスの問題」を参照してください。

ステップ 7　各ネットワーク デバイスのインターフェイスと方向が正しいことを確認します。

手順については、P.C-24 の「ネットワーク デバイスのインターフェイスと方向を確認する」を参照してください。

ステップ 8　ネットワーク デバイスが SSH-DES または SSH-3DES を使用している場合は、デバイスへの SSH 接続がイネーブルになっていることを確認します。

手順については、P.C-25 の「ネットワーク デバイスへの SSH 接続をイネーブルにする」を参照してください。

ステップ 9　制御されている各デバイスのインターフェイスと方向がそれぞれ正しいことを確認します。

手順については、P.C-24 の「ネットワーク デバイスのインターフェイスと方向を確認する」を参照してください。

デバイス アクセスの問題

ARC が管理対象のデバイスにアクセスできない場合があります。管理対象デバイスの IP アドレス、ユーザ名、およびパスワードが正しいことと、インターフェイスおよび方向が正しく設定されていることを確認します。

（注）　SSH デバイスが SSH 1.5 をサポートしている必要があります。センサーは SSH 2.0 をサポートしていません。

デバイス アクセスの問題をトラブルシューティングするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　管理対象デバイスの IP アドレスを確認します。

```
sensor# configure terminal
sensor (config)# service network-access
sensor(config-net)# show settings
   general
   ----------------------------------------------
      log-all-block-events-and-errors: true <defaulted>
      enable-nvram-write: false <defaulted>
      enable-acl-logging: false <defaulted>
      allow-sensor-block: false <defaulted>
      block-enable: true <defaulted>
      block-max-entries: 250 <defaulted>
      max-interfaces: 250 <defaulted>
      master-blocking-sensors (min: 0, max: 100, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      never-block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-hosts (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
      block-networks (min: 0, max: 250, current: 0)
      ----------------------------------------------
      ----------------------------------------------
   ---------------------------------------------
   user-profiles (min: 0, max: 250, current: 1)
   ---------------------------------------------
      profile-name: r7200
      ----------------------------------------------
         enable-password: <hidden>
         password: <hidden>
         username: netrangr default:
      ----------------------------------------------
   ---------------------------------------------
   cat6k-devices (min: 0, max: 250, current: 0)
   ---------------------------------------------
   ---------------------------------------------
   router-devices (min: 0, max: 250, current: 1)
   ---------------------------------------------
      ip-address: 10.89.147.54
      ----------------------------------------------
         communication: telnet default: ssh-3des
         nat-address: 0.0.0.0 <defaulted>
         profile-name: r7200
         block-interfaces (min: 0, max: 100, current: 1)
         ----------------------------------------------
            interface-name: fa0/0
            direction: in
            ----------------------------------------------
               pre-acl-name: <defaulted>
               post-acl-name: <defaulted>
            ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
   ---------------------------------------------
   firewall-devices (min: 0, max: 250, current: 0)
   ---------------------------------------------
   ---------------------------------------------
sensor(config-net)#
```

ステップ 3　デバイスに手動で接続して、ユーザ名、パスワード、およびイネーブル　パスワードが正しいことと、デバイスがセンサーから到達可能であることを確認します。

a. サービス アカウントにログインします。

b. ネットワーク デバイスに Telnet または SSH で接続して、コンフィギュレーションを確認します。

c. デバイスに到達できることを確認します。

d. ユーザ名とパスワードを確認します。

ステップ 4　各ネットワーク デバイスのインターフェイスと方向がそれぞれ正しいことを確認します。

手順については、P.C-24 の「ネットワーク デバイスのインターフェイスと方向を確認する」を参照してください。

ネットワーク デバイスのインターフェイスと方向を確認する

管理対象のデバイスごとに各インターフェイスと方向が正しいことを確認するために、偽のホストに手動ブロックを送信し、ルータの ACL 内にブロックされたアドレスに対応する deny エントリがあるかどうかを確認できます。

（注）　また、**Monitoring > Active Host Blocks** をクリックして、IDM から手動ブロックを実行することもできます。

偽のホストに対する手動ブロックを開始するには、次の手順を実行します。

ステップ 1　ARC 汎用サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
```

ステップ 2　偽のホスト IP アドレスに対する手動ブロックを開始します。

```
sensor(config-net-gen)# block-hosts 10.16.0.0
```

ステップ 3　汎用サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:? [yes]:
```

ステップ 4　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は `no` と入力します。

ステップ 5　ルータに Telnet 接続し、ブロックされるアドレスの拒否エントリがルータの ACL 内に存在することを確認します。

手順についてはルータのマニュアルを参照してください。

ステップ 6　手動ブロックを削除するために、ステップ 1 ～ 4 を繰り返します。ただし、ステップ 2 ではコマンドの前に **no** を入れます。

```
sensor(config-net-gen)# no block-hosts 10.16.0.0
```

ネットワーク デバイスへの SSH 接続をイネーブルにする

SSH-DES または SSH-3DES をネットワーク デバイスの通信プロトコルとして使用している場合は、それがデバイスでイネーブルになっていることを確認する必要があります。

ネットワーク デバイスへの SSH 接続をイネーブルにするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　コンフィギュレーション モードに入ります。

```
sensor# configure terminal
```

ステップ 3　SSH をイネーブルにします。

```
sensor(config)# ssh host blocking_device_ip_ address
```

ステップ 4　デバイスを受け入れるかどうかを確認するプロンプトで、**yes** と入力します。

シグニチャに対してブロッキングが実行されない

特定のシグニチャに対してブロッキングが実行されない場合は、イベント アクションがホストをブロックするように設定されていることを確認します。

特定のシグニチャに対してブロッキングが実行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　CLI にログインします。

ステップ 2　シグニチャ定義サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)#
```

ステップ 3　ホストをブロックするようにイベント アクションが設定されていることを確認します。

（注）　アラートを受け取る場合は、イベント アクションの設定時に必ず **produce-alert** を追加する必要があります。

```
sensor(config-sig)# signatures 1300 0
sensor(config-sig-sig)# engine normalizer
sensor(config-sig-sig-nor)# event-action produce-alert|request-block-host
sensor(config-sig-sig-nor)# show settings
   normalizer
   -----------------------------------------------
      event-action: produce-alert|request-block-host default: produce-alert|deny
-connection-inline
      edit-default-sigs-only
      ----------------------------------------------
         default-signatures-only
         ----------------------------------------------
            specify-service-ports
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            specify-tcp-max-mss
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
            ----------------------------------------------
            specify-tcp-min-mss
            ----------------------------------------------
               no
               ----------------------------------------------
               ----------------------------------------------
--MORE--
```

ステップ 4　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-nor)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 5　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

マスター ブロッキング センサーのコンフィギュレーションを確認する

マスター ブロッキング センサーが適切にセットアップされていることを確認したり、適切にセットアップされていないマスター ブロッキング センサーをトラブルシューティングしたりするために、**show statistics network-access** コマンドを使用できます。リモート マスター ブロッキング センサーが Web アクセスに TLS を使用している場合は、転送センサーが信頼できる TLS ホストとしてセットアップされていることを確認します。

センサーのマスター ブロッキング センサー コンフィギュレーションを確認するには、次の手順を実行します。

ステップ 1　ARC の統計情報を表示して、マスター ブロッキング センサー エントリが統計情報内にあることを確認します。

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 122.122.122.44
         ShunMinutes = 60
         MinutesRemaining = 59
```

ステップ 2　マスター ブロッキング センサーが統計情報内にない場合は、追加する必要があります。

手順については、P.8-37 の「マスター ブロッキング センサーの設定」を参照してください。

ステップ 3　マスター ブロッキング センサーが確実にブロックを開始するように、偽のホスト IP アドレスに対する手動ブロックを開始します。

```
sensor# configure terminal
sensor(config)# service network-access
sensor(config-net)# general
sensor(config-net-gen)# block-hosts 10.16.0.0
```

ステップ 4　ネットワーク アクセス汎用サブモードを終了します。

```
sensor(config-net-gen)# exit
sensor(config-net)# exit
Apply Changes:? [yes]:
```

ステップ 5　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ステップ 6　ブロックが ARC の統計情報に表示されることを確認します。

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 100
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes =
```

ステップ 7　マスター ブロッキング センサーのホストの CLI にログインし、**show statistics network-access** コマンドを使用して、マスター ブロッキング センサーの ARC の統計情報にブロックが表示されることを確認します。

```
sensor# show statistics network-access
Current Configuration
   AllowSensorShun = false
   ShunMaxEntries = 250
   MasterBlockingSensor
      SensorIp = 10.89.149.46
      SensorPort = 443
      UseTls = 1
State
   ShunEnable = true
   ShunnedAddr
      Host
         IP = 10.16.0.0
         ShunMinutes = 60
         MinutesRemaining = 59
```

ステップ 8　リモート マスター ブロッキング センサーが Web アクセスに TLS を使用している場合は、転送センサーが TLS ホストとして設定されていることを確認します。

```
sensor# configure terminal
sensor(config)# tls trust ip master_blocking_sensor_ip_address
```

ロギング

TAC は、トラブルシューティングの目的でユーザにデバッグ ロギングを有効にするように要請する場合があります。LogApp は、さまざまなロギング ゾーンのロギングの重大度を制御することによって、各アプリケーションによってどのログ メッセージが生成されるかを制御します。デフォルトでは、デバッグ ロギングはオンになりません。

個々のゾーン制御をイネーブルにすると、各ゾーンはそれが設定されているロギングのレベルを使用します。それ以外の場合は、すべてのゾーンに対して同じロギング レベルが使用されます。

この項で取り上げる事項は次のとおりです。

- デバッグ ロギングをイネーブルにする（P.C-28）
- ゾーン名（P.C-33）
- SysLog への cidLog メッセージの転送（P.C-33）

デバッグ ロギングをイネーブルにする

注意　デバッグ ロギングをイネーブルにするとパフォーマンスに大きく影響するため、TAC によって指示された場合にだけイネーブルにしてください。

デバッグ ロギングをイネーブルにするには、次の手順を実行します。

ステップ 1　サービス アカウントにログインします。

ステップ 2　log.conf ファイルを編集して、追加のログ ステートメントを格納できるようにログのサイズを増やします。

```
vi /usr/cids/idsRoot/etc/log.conf
```

ステップ 3　`fileMaxSizeInK=500` を `fileMaxSizeInK=5000` に変更します。

ステップ 4　ファイルのゾーンおよび CID セクションを見つけて、デバッグの重大度を設定します。

```
severity=debug
```

ステップ 5　ファイルを保存し、vi エディタを終了し、サービス アカウントを終了します。

ステップ 6　管理者として CLI にログインします。

ステップ 7　マスター コントロール サブモードに入ります。

```
sensor# configure terminal
sensor(config)# service logger
sensor(config-log)# master-control
```

ステップ 8　すべてのゾーンに対してデバッグ ロギングをイネーブルにするには、次の手順を実行します。

```
sensor(config-log-mas)# enable-debug true
sensor(config-log-mas)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: false <defaulted>
   ----------------------------------------------
sensor(config-log-mas)#
```

ステップ 9　個々のゾーン制御をオンにするには、次の手順を実行します。

```
sensor(config-log-mas)# individual-zone-control true
sensor(config-log-mas)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
sensor(config-log-mas)#
```

ステップ 10　マスター ゾーン制御を終了します。

```
sensor(config-log-mas)# exit
```

ステップ 11 ゾーン名を表示します。

```
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: false <defaulted>
      individual-zone-control: true default: false
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: warning <defaulted>
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ----------------------------------------------
sensor(config-log)#
```

各ゾーン名の参照先リストについては、P.C-33 の「ゾーン名」を参照してください。

ステップ 12 特定のゾーンの重大度レベル（デバッグ、タイミング、警告、またはエラー）を変更します。

```
sensor(config-log)# zone-control IdsEventStore severity error
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: warning <defaulted>
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ----------------------------------------------
sensor(config-log)#
```

ステップ 13 特定のゾーンのデバッグをオンにします。

```
sensor(config-log)# zone-control nac severity debug
sensor(config-log)# show settings
   master-control
   ----------------------------------------------
      enable-debug: true default: false
      individual-zone-control: true default: false
   ----------------------------------------------
   zone-control (min: 0, max: 999999999, current: 14)
   ----------------------------------------------
      <protected entry>
      zone-name: AuthenticationApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: Cid
      severity: debug <defaulted>
      <protected entry>
      zone-name: Cli
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdapiCtlTrans
      severity: warning <defaulted>
      <protected entry>
      zone-name: IdsEventStore
      severity: error default: warning
      <protected entry>
      zone-name: MpInstaller
      severity: warning <defaulted>
      <protected entry>
      zone-name: cmgr
      severity: warning <defaulted>
      <protected entry>
      zone-name: cplane
      severity: warning <defaulted>
      <protected entry>
      zone-name: csi
      severity: warning <defaulted>
      <protected entry>
      zone-name: ctlTransSource
      severity: warning <defaulted>
      <protected entry>
      zone-name: intfc
      severity: warning <defaulted>
      <protected entry>
      zone-name: nac
      severity: debug default: warning
      <protected entry>
      zone-name: sensorApp
      severity: warning <defaulted>
      <protected entry>
      zone-name: tls
      severity: warning <defaulted>
   ----------------------------------------------
sensor(config-log)#
```

ステップ 14 ログ サブモードを終了します。

```
sensor(config-log)# exit
Apply Changes:?[yes]:
```

ステップ 15 変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ゾーン名

表 C-1 にデバッグ ログ ゾーン名を示します。

表 C-1　デバッグ ログ ゾーン名

ゾーン名	説明
AuthenticationApp	認証ゾーン
Cid	汎用ロギング ゾーン
Cli	CLI ゾーン
IdapiCtlTrans	すべての制御トランザクション ゾーン
IdsEventStore	イベント ストア ゾーン
MpInstaller	IDSM-2 マスター パーティション インストーラ ゾーン
cmgr	Card Manager サービス ゾーン[1]
cplane	Control Plane ゾーン[2]
csi	CIDS サーブレット インターフェイス[3]
ctlTransSource	送信制御トランザクション ゾーン
intfc	インターフェイス ゾーン
nac	ARC ゾーン
SensorApp	AnalysisEngine ゾーン
tls	SSL および TLS ゾーン

1. Card Manager サービスは、シャーシ内のモジュール間で制御および状態の情報を交換するために、AIP SSM で使用されます。
2. Control Plane は、Card Manager によって AIP SSM で使用されるトランスポート通信レイヤです。
3. CIDS サーブレット インターフェイスは、CIDS Web サーバとサーブレットの間のインターフェイス レイヤです。

SysLog への cidLog メッセージの転送

syslog に cidLog メッセージを転送すると役に立つ場合があります。

cid ログ メッセージを syslog へ送信するには、次の手順を実行します。

ステップ 1　idsRoot/etc/log.conf ファイルへ移動します。

ステップ 2　次の変更を加えます。

a. [logApp] `enabled=false` と設定します。

`enabled=false` がデフォルトであるため、`enabled=true` のコメント化を解除します。

b. [drain/main] `type=syslog` を設定します。

次の例は、ロギング コンフィギュレーション ファイルを示しています。

```
timemode=local
;timemode=utc

[logApp]
;enabled=true
;-------- FIFO parameters --------
fifoName=logAppFifo
fifoSizeInK=240
;-------- logApp zone and drain parameters --------
zoneAndDrainName=logApp
fileName=main.log
fileMaxSizeInK=500

[zone/Cid]
severity=warning
drain=main

[zone/IdsEventStore]
severity=debug
drain=main

[drain/main]
type=syslog
```

syslog 出力が、syslog メッセージの優先度への次の通信とともに syslog ファシリティ local6 に送信されます。

```
LOG_DEBUG,        //   debug
LOG_INFO,             //    timing
LOG_WARNING,   //    warning
LOG_ERR,             //    error
LOG_CRIT             //     fatal
```

（注） /etc/syslog.conf　でそのファシリティが適切なプロパティでイネーブルになっていることを確認します。

注意 syslog は、logApp よりずっと低速です（毎秒約 1000 メッセージに対して、約 50 メッセージ）デバッグ重大度は一度に 1 つのゾーンでイネーブルにすることをお勧めします。

センサーが NTP サーバと同期していることを確認する

IPS 5.1 では、無効な NTP 鍵値や ID など、正しくない NTP コンフィギュレーションをセンサーに適用することはできません。正しくないコンフィギュレーションを適用しようとすると、エラーメッセージが表示されます。NTP コンフィギュレーションを確認するには、**show statistics host** コマンドを使用してセンサーの統計情報を収集します。NTP 統計情報セクションには、NTP サーバとのセンサーの同期に関するフィードバックを含む NTP 統計情報があります。

NTP コンフィギュレーションを確認するには、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。

ステップ 2　ホスト統計情報を生成します。

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
         11.22.33.44     CHU_AUDIO(1)     8 u   36   64    1    0.536    0.069   0.001
         LOCAL(0)        73.78.73.84      5 l   35   64    1    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f014   yes   yes   ok     reject   reachable  1
          2 10373  9014   yes   yes  none    reject   reachable  1
        status = Not Synchronized
     ...
```

ステップ 3　数分後にホスト統計情報を再び生成します。

```
sensor# show statistics host
     ...
     NTP Statistics
             remote           refid      st t when poll reach   delay   offset  jitter
        *11.22.33.44     CHU_AUDIO(1)     8 u   22   64  377    0.518   37.975  33.465
         LOCAL(0)        73.78.73.84      5 l   22   64  377    0.000    0.000   0.001
        ind assID status  conf reach auth condition  last_event cnt
          1 10372  f624   yes   yes   ok   sys.peer   reachable  2
          2 10373  9024   yes   yes  none    reject   reachable  2
        status = Synchronized
```

ステップ 4　ステータスが引き続き `Not Synchronized` である場合は、NTP サーバ管理者と一緒に、NTP サーバが正しく設定されていることを確認します。

シグニチャに対して TCP リセットが実行されない

リセットするように設定されたイベント アクションがない場合は、特定のシグニチャに対して TCP リセットが実行されません。

特定のシグニチャに対してリセットが実行されないことをトラブルシューティングするには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　イベント アクションが TCP リセットに設定されていることを確認します。

```
sensor# configure terminal
sensor(config)# service signature-definition sig0
sensor(config-sig)# signatures 1000 0
sensor(config-sig-sig)# engine atomic-ip
sensor(config-sig-sig-ato)# event-action reset-tcp-connection|produc-alert
sensor(config-sig-sig-ato)# show settings
   atomic-ip
   ----------------------------------------------
      event-action: produce-alert|reset-tcp-connection default: produce-alert
      fragment-status: any <defaulted>
      specify-l4-protocol
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-payload-length
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-header-length
      ----------------------------------------------
         no
         ----------------------------------------------
         ----------------------------------------------
      ----------------------------------------------
      specify-ip-tos
      ----------------------------------------------
--MORE--
```

ステップ 3　シグニチャ定義サブモードを終了します。

```
sensor(config-sig-sig-ato)# exit
sensor(config-sig-sig)# exit
sensor(config-sig)# exit
Apply Changes:?[yes]:
```

ステップ 4　変更を適用する場合は **Enter** キーを押し、変更を廃棄する場合は **no** と入力します。

ステップ 5　正しいアラームが生成されていることを確認します。

```
sensor# show events alert
evAlert: eventId=1047575239898467370 severity=medium
originator:
hostId: sj_4250_40
appName: sensorApp
appInstanceId: 1004
signature: sigId=20000 sigName=STRING.TCP subSigId=0 version=Unknown
addr: locality=OUT 172.16.171.19
port: 32771
victim:
addr: locality=OUT 172.16.171.13 port: 23
actions:
tcpResetSent: true
```

ステップ 6　スイッチでセンサーからの着信 TCP リセット パケットが許可されていることを確認します。

手順についてはスイッチのマニュアルを参照してください。

ステップ 7　リセットが送信されていることを確認します。

```
root# ./tcpdump -i eth0 src host 172.16.171.19
tcpdump: WARNING: eth0: no IPv4 address assigned
tcpdump: listening on eth0
13:58:03.823929 172.16.171.19.32770 > 172.16.171.13.telnet: R 79:79(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
13:58:03.823930 172.16.171.19.32770 > 172.16.171.13.telnet: R 80:80(0) ack 62 win 0
```

ソフトウェア アップグレード

この項では、ソフトウェア アップグレードのトラブルシューティングについて説明します。取り上げる事項は次のとおりです。

- ソフトウェア アップグレードの間、IDS-4235 および IDS-4250 が機能停止する（P.C-37）
- 適用するアップグレードとそれらの前提条件（P.C-37）
- 自動アップデートの問題（P.C-38）
- センサーに保存されているアップデートでセンサーをアップデートする（P.C-39）

ソフトウェア アップグレードの間、IDS-4235 および IDS-4250 が機能停止する

IDS-4235 および IDS-4250 の BIOS が A03 の場合は、最新の IPS ソフトウェアを適用する前に、BIOS を A04 にアップグレードする必要があります。アップグレードしないと、ソフトウェア アップグレードのプロセス中にアプライアンスが機能停止します。BIOS をアップグレードする手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1* 』の「Upgrading the BIOS」を参照してください。最新の IPS ソフトウェアを適用する手順については、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。

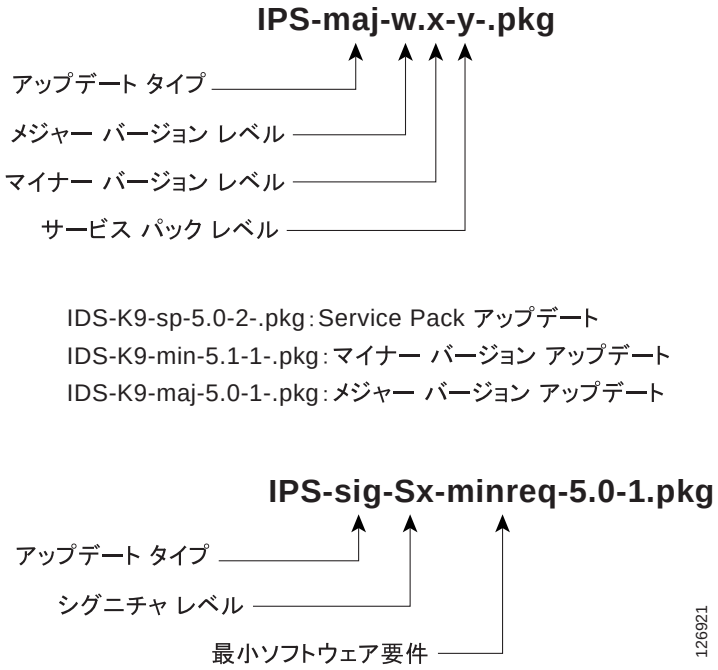
適用するアップグレードとそれらの前提条件

ソフトウェアの正しいサービス パック、マイナー バージョン、およびメジャー バージョンを用意する必要があります。新規ソフトウェアの適用でトラブルが発生した場合は、適切な前提条件で正しいアップデートを適用していることを確認してください。

- シグニチャ アップデートには、ファイル名にリストされた最小バージョンが必要です。
- サービス パックを適用するには、正しいマイナー バージョンが必要です。
- マイナー バージョンには正しいメジャー バージョンが必要です。
- メジャー バージョンには前のメジャー バージョンが必要です。

図 C-1 は、IPS ソフトウェアのファイル名の解釈方法を示しています。

図 C-1　IPS ソフトウェアのファイル名



自動アップデートの問題

自動アップデートの推奨されるトラブルシューティング方法は次のとおりです。

- tcpDump の実行
  - サービス アカウントを作成します。センサーと FTP サーバの間でパケットを取得するには、su で root になり、コマンド / コントロール インターフェイスで tcpDump を実行します。

    手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Creating the Service Account」を参照してください。
  - **upgrade** コマンドを使用して、手動でセンサーをアップグレードします。

    手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。
  - tcpDump 出力で、FTP サーバから戻されるエラーを検索します。
- センサーが正しいディレクトリ内にあることを確認します。

  ディレクトリが正しく指定されている必要があります。これを行わないと、Windows FTP サーバで問題が発生します。ディレクトリ名の前にもう 1 つまたは 2 つの「/」が必要な場合があります。

  これを確認するため、ご使用の FTP 接続による tcpDump 出力で表示される同じ FTP コマンドを使用します。
- カスタム プロンプトを使用するために FTP サーバを変更していないことを確認してください。

  たとえば、FTP プロンプトを変更してセキュリティ警告を提供するようにすると、センサーがハードコード化された応答のリストを期待するため、問題が発生します。

（注） プロンプトを変更しないことは、4.1(4) より前のバージョンにのみ当てはまります。

- Windows FTP サーバ セットアップ オプションを使用して、UNIX ファイル構造と非 MS-DOS ファイル構造をエミュレートする必要があります。
- SCP を使用している場合は、既知のホスト リストに SSH ホスト鍵を追加したことを確認してください。

  手順については、P.2-12 の「既知のホスト鍵の定義」を参照してください。

自動アップデートを実行する前に、手動で **upgrade** コマンドを実行してみます。**upgrade** コマンドでは動作したが、自動アップデートでは動作しない場合には、次のことを試しています。

- センサーの IPS ソフトウェア バージョンを調べます（手順については、P.C-59 の「バージョン情報」を参照してください）。

  バージョン 4.0(1) には、自動アップデートに既知の問題があります。自動アップデートの設定と使用を試行する前に、4.1(1) へ手動でアップグレードします。
- 自動アップデート用にパスワードが設定されていることを確認します。手動アップデートに使用したパスワードと一致することを確認します。
- FTP サーバ内のファイル名が、大文字小文字の区別も含め、Cisco.com の Downloads に表示されるものと完全に一致することを確認します。

  Windows FTP サーバの中には、大文字小文字の区別が正しくないファイルへのアクセスを許可するものもありますが、最終的にはセンサーが名前の変更を理由にそのファイルを拒否します。

必要に応じて、自動アップデートで tcpDump を実行します。成功した手動アップデートと失敗した自動アップデートを比較して、そこからトラブルシューティングすることができます。

センサーに保存されているアップデートでセンサーをアップデートする

アップデート パッケージをセンサーの /var ディレクトリに保存し、必要に応じてそのアップデートを使用してセンサーをアップデートできます。

センサーに保存されているアップデートでセンサーをアップデートするには、次の手順を実行します。

ステップ 1　サービス アカウントにログインします。

ステップ 2　Cisco.com からアップデート パッケージ ファイルを取得します。

手順については、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。

ステップ 3　アップデート ファイルをセンサーの /usr/cids/idsRoot/var ディレクトリへ FTP または SCP で送信します。

ステップ 4　ファイル許可を設定します。

```
chmod 644 ips_package_file_name
```

ステップ 5　サービス アカウントを終了します。

ステップ 6　管理者特権を持つアカウントを使用してセンサーにログインします。

ステップ 7　センサーのホスト鍵を保存します。

```
sensor# configure terminal
sensor(config)# service ssh
sensor(config-ssh)# rsa1-keys sensor_ip_address
```

ステップ 8　センサーをアップグレードします。

```
sensor(config)# upgrade scp://service@Sensor_ip_address/upgrade/ips_package_file_name
Enter password: *****
Re-enter password: *****
```

IDM のトラブルシューティング

この項では、IDM のトラブルシューティング手順を示します。

（注）　これらの手順は、ASDM の IPS セクションにも適用されます。

この項で取り上げる事項は次のとおりです。

- Java プラグインのメモリ サイズを増やす（P.C-41）
- IDM を起動できない - Java アプレットのロードに失敗（P.C-43）
- IDM を起動できない - 分析エンジンがビジー状態（P.C-44）
- IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできない（P.C-44）
- シグニチャがアラートを生成しない（P.C-45）

Java プラグインのメモリ サイズを増やす

IDM を正しく動作させるには、ブラウザに Java プラグイン 1.4.2 または 1.5 をインストールする必要があります。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** をクリックしたときに、メモリが使い果たされてしまうこともあります。メモリが使い果たされるたびに、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（P.C-41）
- Linux および Solaris での Lava プラグイン（P.C-42）

Windows での Java プラグイン

Java プラグイン 1.4.2 および 1.5 に対応した Windows で Java プラグイン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、**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 および Solaris での Lava プラグイン

Linux および Solaris 上で Java プラグイン 1.4.2 および 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** 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。

IDM を起動できない - Java アプレットのロードに失敗

症状　ブラウザに、`Loading Cisco IDM.Please wait ...` と表示されます。ウィンドウの左下隅に、`Loading Java Applet Failed` と表示されます。

考えられる原因　この状態は、IDM を起動するマシンに複数の Java プラグイン（1.4.*x* および / または 1.3.*x*）がインストールされている場合に発生します。

推奨処置　Java キャッシュをクリアして temp ファイルを削除し、使用しているブラウザの履歴をクリアします。結果として、これらのプラグインのどれもデフォルトでは使用されません。各アプレットは正しいプラグインを使用する必要があります。

キャッシュをクリアするには、次の手順を実行します。

ステップ 1　ブラウザのウィンドウをすべて閉じます。

ステップ 2　Java プラグイン 1.3.*x* 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. **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.3.x** をクリックします。

b. **Advanced** タブをクリックします。

c. Java Runtime Environment の下で、ドロップダウン メニューから **JRE 1.3.x** を選択します。

d. **Cache** タブをクリックします。

e. **Clear** をクリックします。

ステップ 3　ava プラグイン 1.4.*x* 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. **Start** > **Settings** > **Control Panel** > **Java Plug-in 1.4.x** をクリックします。

b. **Advanced** タブをクリックします。

c. Java Runtime Environment の下で、ドロップダウン メニューから **JRE 1.3.x** を選択します。

d. **Cache** タブをクリックします。

e. **Browser** タブをクリックします。

f. ブラウザのチェックボックスをすべて選択解除します。

g. **Clear Cache** をクリックします。

ステップ 4　temp ファイルを削除し、ブラウザ内の履歴をクリアします。

IDM を起動できない - 分析エンジンがビジー状態

エラー メッセージ `Error connecting to sensor. Failed to load sensor-errNotAvailable-Analysis Engine is busy. Exiting IDM.`

考えられる原因　この条件は、センサー内の分析エンジンがタスクを実行する準備のためにビジー状態で、IDM に応答しない場合に発生する可能性があります。

推奨処置　しばらく待ってから、接続を再試行してください。

IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできない

IDM、リモート マネージャ、または検知インターフェイスがセンサーにアクセスできないが、SSH または Telnet（イネーブルの場合）を使用してセンサーの CLI にアクセスできる場合には、次の手順を実行します。

（注）　センサーで Telnet をイネーブルまたはディセーブルにする手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Enabling and Disabling Telnet」を参照してください。

ステップ 1　ネットワーク コンフィギュレーションが、センサーで設定されている Web サーバ ポートにアクセスできることを確認します。

```
sensor# setup


    --- 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 10.89.130.108/23,10.89.130.1
host-name sensor
telnet-option enabled
access-list 0.0.0.0/0
ftp-timeout 300
no 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
```

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing Web Server Settings」を参照してください。

ステップ 2　ルータ、スイッチ、またはファイアウォールなどのネットワーク　デバイスがセンサーとワークステーションの間にある場合は、これらのデバイスが、ワークステーションによるセンサーの Web サーバ ポートへのアクセスを許可するように設定されていることを確認します。

リモート管理通信はすべてセンサーの Web サーバによって実行されます。

詳細については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Changing Web Server Settings」を参照してください。

シグニチャがアラートを生成しない

シグニチャが反応したときにアラートが表示されない場合は、Produce Alert がイベント アクションとして設定されていることを確認してください。

注意　イベント アクションを設定するたびにその他のアクションを追加することはできません。実際には、イベント アクションを設定するたびに、そのリストを置換しているので、イベント アクションを設定するたびに必ず Produce Alert を選択してください。

たとえば、Produce Alert を選択したが、-後から別のイベント アクションを追加し、Produce Alert を新規コンフィギュレーションに追加しないと、アラートはイベント ストアに送信されません。

アラートを確実に受け取るようにするには、仮想センサーとイベント ストアの統計情報を使用します。

IDSM-2 のトラブルシューティング

IDSM-2 のソフトウェア アーキテクチャは、4200 シリーズのセンサーと同じです。P.C-5 の「4200 シリーズ アプライアンスのトラブルシューティング」で説明されているのと同じトラブルシューティング ツールを使用できます。

この項では特に IDSM-2 のトラブルシューティングについて説明します。取り上げる事項は次のとおりです。

- IDSM-2 問題の診断（P.C-46）
- トラブルシューティング用の switch コマンド（P.C-47）
- ステータス LED がオフになっている（P.C-47）
- ステータス LED がオンだが IDSM-2 がオンラインにならない（P.C-50）
- IDSM-2 コマンド / コントロール ポートと通信できない（P.C-51）
- TCP リセット インターフェイスの使用方法（P.C-52）
- シリアル ケーブルを IDSM-2 に接続する（P.C-53）

IDSM-2 問題の診断

次のリストに照らし合せて、IDSM-2 問題を診断します。

- IDSM-2 とマザーボードの間のリボン ケーブルがゆるくなっています。

  モジュールを物理的に処理しているときに、コネクタがベース カードから外れ、ドーター カードとベース カードの接触が失われる場合があります。コネクタのリボン ケーブルがゆるむと、ポート 7 と 8 でオンライン診断エラーが発生します。この条件が存在する場合、モジュールは動作できません。

  詳細については、Partner Field Notice 52816 を参照してください。

- IDSM-2 の中に、出荷時に障害のある DIMM が同梱されているものがありました。

  IDSM-2 のメモリに問題があるかどうかを確認する手順については、Partner Field 52563 を参照してください。

- ハードディスク ドライブが読み取りまたは書き込みを実行できません。

  ハードディスク ドライブを長期（2 週間以上）にわたって連続使用すると、次のようないくつかの症状が現れる場合があります。

  - ログインできない
  - 読み取り / 書き込み操作の実行時のコンソールへの I/O エラー（**ls** コマンド）
  - コマンドが正しく実行されない（実行可能ファイルへのパスが見つからない）

  スイッチはモジュールが良好であることを報告しますが、サービス アカウントにログインしてコマンドを実行しようとすると、問題が存在することが表示されます。4.1(4) サービス パックを使用すると、この問題は軽減されますが、4.1(4) アプリケーション パーティション イメージで IDSM-2 のイメージを再作成する場合は、4.1(4b) パッチを適用する必要があります。詳細については、CSCef12198 を参照してください。

- ストリームベースのシグニチャ（1300 シリーズ）に対して IP ロギングをイネーブルにすると、SensorApp はクラッシュするか、CPU の 99% を消費します。回避策については、CSCed32093 を参照してください。

- IDSM-2 はロックアップされると思われます。リモート アクセスは禁止されます（SSH、Telnet、IDM、イベント サーバ、制御トランザクション サーバ、および IP ログ サーバ）。

  この障害は、SWAP の使用に関連しています。IDSM-2 は ping に応答します。この問題を解決するには、4.1(4) サービス パックを適用します。詳細については、CSCed54146 を参照してください。

- IDSM-2 をアップグレードした直後、またはシグニチャを VMS で調整した直後に、IDSM-2 が応答しなくなり、多くの場合、SensorApp コア ファイルを生成します。この問題を修正するには、4.1(4b) パッチを適用します。

- サポートされるコンフィギュレーションが IDSM-2 にあることを確認します。

  『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Supported IDSM-2 Configurations」を参照してください。

IDSM-2 に上記の問題のいずれも発生していないことを確認し、それでも応答しないように見える場合、たとえば、SSH または Telnet からログインできない場合やスイッチに対してセッションを開始することができない場合などは、IDSM-2 が ping に応答するかどうかと、サービス アカウントからログインできるかどうかを確認してください。ログインできる場合は、cidDump およびコア ファイルを取得して、TAC に連絡してください。

トラブルシューティング用の switch コマンド

IDSM-2 のトラブルシューティングには、次の switch コマンドが役に立ちます。

- **show module**（Cisco Catalyst ソフトウェアおよび Cisco IOS ソフトウェア）
- **show version**（Cisco Catalyst ソフトウェアおよび Cisco IOS ソフトウェア）
- **show port**（Cisco Catalyst ソフトウェア）
- **show trunk**（Cisco Catalyst ソフトウェア）
- **show span**（Cisco Catalyst ソフトウェア）
- **show security acl**（Cisco Catalyst ソフトウェア）
- **show intrusion-detection module**（Cisco IOS ソフトウェア）
- **show monitor**（Cisco IOS ソフトウェア）
- **show vlan access-map**（Cisco IOS ソフトウェア）
- **show vlan filter**（Cisco IOS ソフトウェア）

ステータス LED がオフになっている

IDSM-2 のステータス インジケータがオフになっている場合は、電源を入れて IDSM-2 をオンにする必要があります。

IDSM-2 のステータスを判別するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　IDSM-2 がオンラインであることを確認します。

Catalyst ソフトウェアの場合、次のように入力します。

```
cat6k> enable

Enter password:
cat6k> (enable) show module
Mod Slot Ports Module-Type                Model                Sub Status
--- ---- ----- ------------------------- ------------------- --- --------
1   1    2     1000BaseX Supervisor      WS-X6K-SUP1A-2GE    yes ok
15  1    1     Multilayer Switch Feature WS-F6K-MSFC         no  ok
2   2    48    10/100BaseTX Ethernet     WS-X6248-RJ-45      no  ok
3   3    48    10/100/1000BaseT Ethernet WS-X6548-GE-TX      no  ok
4   4    16    1000BaseX Ethernet        WS-X6516A-GBIC      no  ok
6   6    8     Intrusion Detection Mod   WS-SVC-IDSM2        yes ok

Mod Module-Name          Serial-Num
--- -------------------- -----------
1                        SAD041308AN
15                       SAD04120BRB
2                        SAD03475400
3                        SAD073906RC
4                        SAL0751QYN0
6                        SAD062004LV

Mod MAC-Address(es)                         Hw     Fw          Sw
--- -------------------------------------- ------ ---------- ----------------
1   00-d0-c0-cc-0e-d2 to 00-d0-c0-cc-0e-d3 3.1    5.3.1      8.4(1)
    00-d0-c0-cc-0e-d0 to 00-d0-c0-cc-0e-d1
    00-30-71-34-10-00 to 00-30-71-34-13-ff
15  00-30-7b-91-77-b0 to 00-30-7b-91-77-ef 1.4    12.1(23)E2 12.1(23)E2
2   00-30-96-2b-c7-2c to 00-30-96-2b-c7-5b 1.1    4.2(0.24)V 8.4(1)
3   00-0d-29-f6-01-98 to 00-0d-29-f6-01-c7 5.0    7.2(1)     8.4(1)
4   00-0e-83-af-15-48 to 00-0e-83-af-15-57 1.0    7.2(1)     8.4(1)
6   00-e0-b0-ff-3b-80 to 00-e0-b0-ff-3b-87 0.102  7.2(0.67)  5.0(0.30)

Mod Sub-Type                Sub-Model           Sub-Serial  Sub-Hw Sub-Sw
--- ----------------------- ------------------- ----------- ------ ------
1   L3 Switching Engine     WS-F6K-PFC          SAD041303G6 1.1
6   IDS 2 accelerator board WS-SVC-IDSUPG       .           2.0
cat6k> (enable)
```

Cisco IOS ソフトウェアの場合

```
cat6k#show module
Mod Ports Card Type                              Model              Serial No.
--- ----- ------------------------------------- ------------------ -----------
  1   48  48 port 10/100 mb RJ-45 ethernet       WS-X6248-RJ-45     SAD0401012S
  2   48  48 port 10/100 mb RJ45                 WS-X6348-RJ-45     SAL04483QBL
  3   48  SFM-capable 48 port 10/100/1000mb RJ45 WS-X6548-GE-TX     SAD073906GH
  5    8  Intrusion Detection System             WS-SVC-IDSM-2      SAD0751059U
  6   16  SFM-capable 16 port 1000mb GBIC        WS-X6516A-GBIC     SAL0740MMYJ
  7    2  Supervisor Engine 720 (Active)         WS-SUP720-3BXL     SAD08320L2T
  9    1  1 port 10-Gigabit Ethernet Module      WS-X6502-10GE      SAD071903BT
 11    8  Intrusion Detection System             WS-SVC-IDSM2       SAD05380608
 13    8  Intrusion Detection System             WS-SVC-IDSM-2      SAD072405D8

Mod MAC addresses                       Hw    Fw           Sw           Status
--- ----------------------------------- ------ ------------ ------------ -------
  1  00d0.d328.e2ac to 00d0.d328.e2db   1.1   4.2(0.24)VAI 8.5(0.46)ROC Ok
  2  0003.6c14.e1d0 to 0003.6c14.e1ff   1.4   5.4(2)       8.5(0.46)ROC Ok
  3  000d.29f6.7a80 to 000d.29f6.7aaf   5.0   7.2(1)       8.5(0.46)ROC Ok
  5  0003.fead.651a to 0003.fead.6521   4.0   7.2(1)       5.0(1.1)     Ok
  6  000d.ed23.1658 to 000d.ed23.1667   1.0   7.2(1)       8.5(0.46)ROC Ok
  7  0011.21a1.1398 to 0011.21a1.139b   4.0   8.1(3)       12.2(PIKESPE Ok
  9  000d.29c1.41bc to 000d.29c1.41bc   1.3   Unknown      Unknown      PwrDown
 11  00e0.b0ff.3340 to 00e0.b0ff.3347   0.102 7.2(0.67)    5.0(1.1)     Ok
 13  0003.feab.c850 to 0003.feab.c857   4.0   7.2(1)       5.0(1)       Ok

Mod Sub-Module                  Model               Serial        Hw     Status
--- --------------------------- ------------------ ------------ ------- -------
  5 IDS 2 accelerator board     WS-SVC-IDSUPG      07E91E508A    2.0    Ok
  7 Policy Feature Card 3       WS-F6K-PFC3BXL     SAD083305A1   1.3    Ok
  7 MSFC3 Daughterboard         WS-SUP720          SAD083206JX   2.1    Ok
 11 IDS 2 accelerator board     WS-SVC-IDSUPG      .             2.0    Ok
 13 IDS 2 accelerator board     WS-SVC-IDSUPG      0347331976    2.0    Ok

Mod Online Diag Status
--- -------------------
  1 Pass
  2 Pass
  3 Pass
  5 Pass
  6 Pass
  7 Pass
  9 Unknown
 11 Pass
 13 Pass
cat6k#
```

（注） IDSM-2　を初めて取り付けたときに、ステータスが　other　を示すのは正常な動作です。IDSM-2 が診断ルーチンを完了してオンラインになった後で、ステータスは ok を示します。IDSM-2 がオンラインになるまでの時間としては、最長で 5 分間みてください。

ステップ 3　ステータスが ok でない場合は、モジュールをオンにします。

```
router# set module power up module_number
```

ステータス LED がオンだが IDSM-2 がオンラインにならない

ステータス インジケータがオンになっているが、IDSM-2 がオンラインにならないという場合は、次のトラブルシューティング ヒントを試してください。

- IDSM-2 をリセットします。
- IDSM-2 がスイッチに適切にインストールされていることを確認します。
- ハードディスク ドライブのステータスが失敗した場合は、アプリケーション パーティションのイメージを再作成します。

IDSM-2 をイネーブルにするには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　IDSM-2 がイネーブルになっていることを確認します。

```
router# show module
```

ステップ 3　ステータスが ok でない場合は、IDSM-2 をイネーブルにします。

```
router# set module enable module_number
```

ステップ 4　IDSM-2 がそれでもオンラインにならない場合は、リセットしてください。

```
router# reset module_number
```

IDSM-2 がオンラインになるまで 5 分ほど待ってください。

ステップ 5　IDSM-2 がそれでもオンラインにならない場合は、ハードウェアとオペレーティング システムが良好であることを確認してください。

```
router# show test module_number
```

ステップ 6　port ステータスが fail の場合は、IDSM-2 がスイッチ内でしっかり接続されていることを確認します。

ステップ 7　hdd ステータスが fail の場合は、アプリケーション パーティションのイメージを再作成する必要があります。

手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Upgrading, Downgrading, and Installing System Images」を参照してください。

IDSM-2 コマンド / コントロール ポートと通信できない

IDSM-2 コマンド / コントロール ポートと通信できない場合は、コマンド / コントロール ポートが正しい VLAN に配置されていない可能性があります。

IDSM-2 のコマンド / コントロール ポートと通信するには、次の手順を実行します。

ステップ 1　コンソールにログインします。

ステップ 2　その他のシステムからコマンド ポートを ping できることを確認します。

ステップ 3　IP アドレス、マスク、およびゲートウェイ設定が正しいことを確認します。

```
router# show configuration
```

ステップ 4　コマンド / コントロール ポートが正しい VLAN に置かれていることを確認します。

Catalyst ソフトウェアの場合

```
cat6k> (enable) show port 6/8
* = Configured MAC Address

# = 802.1X Authenticated Port Name.

Port  Name                 Status     Vlan       Duplex Speed       Type
----- -------------------- ---------- ---------- ------ ----------- ------------
 6/8                       connected  trunk        full        1000 IDS


Port  Status      ErrDisable Reason    Port ErrDisableTimeout  Action on Timeout
----  ----------  -------------------  ----------------------  -----------------
 6/8  connected                      -  Enable                  No Change

Port  Align-Err  FCS-Err    Xmit-Err   Rcv-Err    UnderSize
----- ---------- ---------- ---------- ---------- ---------
 6/8           0          0          0          0         0

Port  Single-Col Multi-Coll Late-Coll  Excess-Col Carri-Sen Runts     Giants
----- ---------- ---------- ---------- ---------- --------- --------- ---------
 6/8           0          0          0          0         0         0         -

Port  Last-Time-Cleared
----- --------------------------
 6/8  Wed Mar 2 2005, 15:29:49

Idle Detection
--------------
   --
cat6k> (enable)
```

Cisco IOS ソフトウェアの場合

```
cat6k#show intrusion-detection module 5 management-port state
Intrusion-detection module 5 management-port:

Switchport: Enabled
Administrative Mode: dynamic desirable
Operational Mode: static access
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Vlans allowed on trunk:1
Vlans allowed and active in management domain: 1
Vlans in spanning tree forwarding state and not pruned:
   1
Access Vlan = 1


cat6k#
```

ステップ 5　コマンド / コントロール ポートが正しい VLAN に置かれていない場合は、正しい VLAN に置いてください。

手順については、『*Configuring the Cisco Intrusion Prevention System Sensor Using the Command Line Interface 5.1*』の「Configuring the Catalyst 6500 Series Switch for Command and Control Access to the IDSM-2」を参照してください。

TCP リセット インターフェイスの使用方法

IDSM-2 には TCP リセット インターフェイス（ポート 1）があります。IDSM-2 は、センシング ポートに TCP リセットを送信できないので、専用の TCP リセット インターフェイスが用意されています。

IDSM-2 において TCP リセット上の問題が発生した場合は、次の手順を試してください。

- センシング ポートがアクセス ポート（1 つの VLAN）である場合、TCP リセット ポートが同じ VLAN に存在するように設定する必要があります。
- センシング ポートが dot1q トランク ポート（マルチ VLAN）である場合、このセンシング ポートと TCP リセット ポートはすべて同じネイティブ VLAN を持つ必要があり、TCP リセット ポートは両方のセンシング ポートによってトランク接続されている VLAN すべてにトランク接続されている必要があります。

シリアル ケーブルを IDSM-2 に接続する

シリアル ケーブルを IDSM-2 のシリアル コンソール ポートに直接接続することはできません。直接接続すると、スイッチおよびモジュールのネットワーク インターフェイスがバイパスされます。

IDSM-2 にシリアル ケーブルを接続するには、次の手順を実行します。

ステップ 1　IDSM-2 で 2 つの RJ-45 ポートを見つけます。

マザー ボードの中央あたりにあります。モジュールの前面プレートを見ている場合は、右側の RJ-45 ポートがシリアル コンソール ポートです。

ステップ 2　IDSM-2 で右側のポートにストレート ケーブルを接続してから、端末サーバ ポートにケーブルのもう一方の端を接続します。

ステップ 3　端末サーバ ポートを 19200 ボー、8 ビット、パリティなしに設定します。

これで、IDSM-2 に直接ログインできるようになります。

（注）　ケーブルはシャーシの前面から出てくる必要があるので、シリアル ケーブルを IDSM-2 に接続するのは、スイッチ シャーシ内で IDSM-2 の上にモジュールがない場合だけです。

AIP SSM のトラブルシューティング

AIP SSM のソフトウェア アーキテクチャは、4200 シリーズのセンサーと同じです。P.C-5 の「4200 シリーズ アプライアンスのトラブルシューティング」で説明されているのと同じトラブルシューティング ツールを使用できます。

次の項では、AIP SSM のトラブルシューティングに特有のコマンドを示します。

AIP SSM の一般的な健全性情報を確認するには、**show module 1 details** コマンドを使用します。

```
asa# show module 1 details
Getting details from the Service Module, please wait...
ASA 5500 Series Security Services Module-20
Model:              ASA-SSM-20
Hardware version:   0.2
Serial Number:      P2B000005D0
Firmware version:   1.0(10)0
Software version:   5.1(0.1)S153.0
Status:             Up
Mgmt IP addr:       10.89.149.219
Mgmt web ports:     443
Mgmt TLS enabled:   true
asa#
```

出力には AIP SSM がアップとして示されます。ステータスが Down の場合は、**hw-module module 1 reset** コマンドを使用して AIP SSM をリセットすることができます。

```
asa# hw-module module 1 reset
The module in slot 1 should be shut down before
resetting it or loss of configuration may occur.
Reset module in slot 1? [confirm]
Reset issued for module in slot 1
asa(config)# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Shutting Down
****************************************************
asa(config)# show module

Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  0 ASA 5520 Adaptive Security Appliance         ASA5520            P2A00000014
  1 ASA 5500 Series Security Services Module-10  ASA-SSM-10         P2A0000067U

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  0 000b.fcf8.7bdc to 000b.fcf8.7be0  0.2          1.0(10)0     7.0(1)
  1 000b.fcf8.0176 to 000b.fcf8.0176  0.2          1.0(10)0     5.1(0.1)S153.0

Mod Status
--- ------------------
  0 Up Sys
  1 Up
asa(config)#
```

AIP SSM のリカバリで問題が生じた場合は、**debug module-boot** コマンドを使用して AIP SSM の起動時の出力を確認できます。TFTP サーバの IP アドレスが正しいことと、TFTP サーバ上のファイルが正しいことを確認します。その後、**hw-module module 1 recover** コマンドを使用して、再度、AIP SSM をリカバリします。

```
asa(config)# hw-module module 1 recover configure
Image URL [tftp://0.0.0.0/]: tftp://10.89.146.1/IPS-SSM-K9-sys-1.1-a-5.1-0.1.i$
Port IP Address [0.0.0.0]: 10.89.150.227
VLAN ID [0]:
Gateway IP Address [0.0.0.0]: 10.89.149.254
asa(config)# debug module-boot
debug module-boot  enabled at level 1
asa(config)# hw-module module 1 recover boot
The module in slot 1 will be recovered.  This may erase all configuration and all data
on that device and attempt to download a new image for it.
Recover module in slot 1? [confirm]
Recover issued for module in slot 1
asa(config)# Slot-1 140> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25
23:02:10 PST 2005
Slot-1 141> Platform ASA-SSM-10
Slot-1 142> GigabitEthernet0/0
Slot-1 143> Link is UP
Slot-1 144> MAC Address: 000b.fcf8.0176
Slot-1 145> ROMMON Variable Settings:
Slot-1 146>   ADDRESS=10.89.150.227
Slot-1 147>   SERVER=10.89.146.1
Slot-1 148>   GATEWAY=10.89.149.254
Slot-1 149>   PORT=GigabitEthernet0/0
Slot-1 150>   VLAN=untagged
Slot-1 151>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 152>   CONFIG=
Slot-1 153>   LINKTIMEOUT=20
Slot-1 154>   PKTTIMEOUT=4
Slot-1 155>   RETRY=20
Slot-1 156> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
Slot-1 157> TFTP failure: Packet verify failed after 20 retries
Slot-1 158> Rebooting due to Autoboot error ...
Slot-1 159> Rebooting....
Slot-1 160> Cisco Systems ROMMON Version (1.0(10)0) #0: Fri Mar 25 23:02:10 PST 2005
Slot-1 161> Platform ASA-SSM-10
Slot-1 162> GigabitEthernet0/0
Slot-1 163> Link is UP
Slot-1 164> MAC Address: 000b.fcf8.0176
Slot-1 165> ROMMON Variable Settings:
Slot-1 166>   ADDRESS=10.89.150.227
Slot-1 167>   SERVER=10.89.146.1
Slot-1 168>   GATEWAY=10.89.149.254
Slot-1 169>   PORT=GigabitEthernet0/0
Slot-1 170>   VLAN=untagged
Slot-1 171>   IMAGE=IPS-SSM-K9-sys-1.1-a-5.1-0.1.img
Slot-1 172>   CONFIG=
Slot-1 173>   LINKTIMEOUT=20
Slot-1 174>   PKTTIMEOUT=4
Slot-1 175>   RETRY=20
Slot-1 176> tftp IPS-SSM-K9-sys-1.1-a-5.1-0.1.img@10.89.146.1 via 10.89.149.254
```

情報の収集

問題が発生した場合には、次の CLI コマンドとスクリプトを使用して、情報を収集し、センサーの状態を診断できます。**show tech-support** コマンドを使用してすべてのセンサーの情報を収集することもできれば、この項にリストしたその他の個々のコマンドを使用して特定の情報を収集することもできます。

この項で取り上げる事項は次のとおりです。

- テクニカル サポート情報（P.C-56）
- バージョン情報（P.C-59）
- 統計情報（P.C-61）
- インターフェイスの情報（P.C-71）
- イベント情報（P.C-72）
- cidDump スクリプト（P.C-76）
- Cisco FTP サイトのファイルのアップロードとアクセス（P.C-77）

テクニカル サポート情報

すべてのセンサーのステータスおよびコンフィギュレーション情報を取得する場合は、**show tech-support** コマンドが役に立ちます。

この項で取り上げる事項は次のとおりです。

- 概要（P.C-56）
- テクニカル サポート情報の表示（P.C-57）
- Tech Support コマンドの出力（P.C-58）

概要

show tech-support コマンドは、センサーのステータスおよびコンフィギュレーション情報をすべて収集します。収集した情報には、現在のコンフィギュレーション、バージョン情報、および cidDump 情報が含まれます。出力が 1 MB を超えるなど、大きい可能性があります。出力はリモート システムに転送できます。出力をリモート システムにコピーする手順については、P.C-57 の「テクニカル サポート情報の表示」を参照してください。

（注）Monitoring > Support Information > System Information をクリックすることによって、IDM から同じ情報を収集できます。

（注）TAC に問い合せる前に、必ず、**show tech-support** コマンドを実行してください。

テクニカル サポート情報の表示

show tech-support [**page**] [**password**] [**destination-url** *destination-url*] コマンドを使用して、システム情報を画面に表示したり、特定の URL へ送信したりすることができます。この情報は、TAC でトラブルシューティング ツールとして使用できます。

次のパラメータはオプションです。

- **page**：一度に 1 ページずつ、情報の出力を表示します。

  次の出力行を表示するには **Enter** キーを押し、次のページの情報を表示するには Space キーを押します。
- **password**：パスワードとその他のセキュリティ情報を出力に残します。
- **destination-url**：情報を HTML としてフォーマットし、このコマンドの後に続く宛先に送信するよう指示します。このキーワードを使用した場合、出力は画面に表示されません。
- *destination-url*：情報を HTML としてフォーマットすることを示します。URL は、情報の送信先を指定します。このキーワードを使用しない場合は、情報が画面に表示されます。

テクニカル サポート情報を表示するには、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 CLI にログインします。

ステップ 2　画面に出力を表示します。

```
sensor# show tech-support page
```

システム情報が、一度に 1 ページずつ画面に表示されます。次のページを表示するには Space キーを押し、プロンプトへ戻るには **Ctrl+C** キーを押します。

ステップ 3　ファイルへ出力を送信する（HTML 形式で）には、次の手順を実行します。

a. 次のコマンドを入力し、その後に有効な宛先を入力します。

```
sensor# show tech-support destination-url destination-url
```

次の宛先タイプを指定できます。

- **ftp:**：FTP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、
  `ftp:[[//username@location]/relativeDirectory]/filename` または
  `ftp:[[//username@location]//absoluteDirectory]/filename` です。
- **scp:**：SCP ネットワーク サーバの宛先 URL。このプレフィクスの構文は、
  `scp:[[//username@]location]/relativeDirectory]/filename` または
  `scp:[[//username@]location]//absoluteDirectory]/filename` です。

たとえば、ファイル `/absolute/reports/sensor1Report.html` へテクニカル サポート出力を送信するには、次の手順を実行します。

```
sensor# show tech support dest
ftp://csidsuser@10.2.1.2//absolute/reports/sensor1Report.html
```

`password:` プロンプトが表示されます。

b. このユーザ アカウントのパスワードを入力します。

`Generating report:` メッセージが表示されます。

Tech Support コマンドの出力

次は、**show tech-support** コマンドの出力例です。

（注）　この出力例は、コマンドの最初の部分と、インターフェイス、ARCm および cidDump サービスに関する情報を示しています。

```
sensor# show tech-support page

System Status Report
This Report was generated on Fri Feb 21 03:33:52 2003.
Output from show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2208534
   Total Bytes Received = 157390286
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239437
   Total Bytes Transmitted = 107163351
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0

Output from show statistics networkAccess
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = true
   BlockMaxEntries = 250
   MaxDeviceInterfaces = 250
```

```
State
   BlockEnable = true

Output from cidDump

cidDiag
CID Diagnostics Report Fri Feb 21 03:33:54 UTC 2003
5.0(1)
<defaultVersions>
<defaultVersion aspect="S">
<version>149.0</version>
<date>2005-03-04</date>
</defaultVersion>
</defaultVersions>
1.1 - 5.0(1)S149
Linux version 2.4.26-IDS-smp-bigphys (csailer@mcq) (gcc version 2.96 20000731 (R
ed Hat Linux 7.3 2.96-112)) #2 SMP Fri Mar 4 04:11:31 CST 2005
 03:33:54 up 21 days, 23:15,  3 users,  load average: 0.96, 0.86, 0.78
--MORE--
```

バージョン情報

センサーの一般的な健全性情報を確認するには、**show version** コマンドが役に立ちます。この項で取り上げる事項は次のとおりです。

- 概要（P.C-59）
- バージョン情報の表示（P.C-59）

概要

show version コマンドは、センサーの一般的な健全性情報を表示し、障害が発生している場所を示すことができます。次の情報を提供します。

- どのアプリケーションが実行中か
- アプリケーションのバージョン
- ディスクおよびメモリの使用量
- アプリケーションのアップグレード履歴

（注）　**Monitoring > Support Information > Diagnostics Report** をクリックすることで、IDM または ASDM から同じ情報を収集できます。

バージョン情報の表示

show version コマンドを使用して、インストールされているすべてのオペレーティング システム パッケージ、シグニチャ パッケージ、およびシステム上で稼働している IPS プロセスのバージョン情報を表示することができます。システム全体のコンフィギュレーションを表示するには、**more current-config** コマンドを使用します。

バージョンとコンフィギュレーションを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　バージョン情報を表示します。

```
sensor# show version
```

次の例に、アプライアンスと NM-CIDS のバージョン出力のサンプルを示します。

アプライアンスのバージョン出力のサンプル

```
sensor# show version
Application Partition:

Cisco Intrusion Prevention System, Version 5.0(0.29)S135.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: IPS-4255-K9
Serial Number: JAB0815R017
No license present
Sensor up-time is 5 days.
Using 722145280 out of 3974291456 bytes of available memory (18% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 36.3M out of 166.8M bytes of available disk space (23%
usage)
boot is using 39.4M out of 68.6M bytes of available disk space (61% usage)


MainApp          2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
AnalysisEngine   2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600   Running
CLI              2005_Feb_18_03.00   (Release)   2005-02-18T03:13:47-0600


Upgrade History:

  IDS-K9-maj-5.0-0.29-S91-0.29-.pkg   03:00:00 UTC Mon Feb 16 2004

Recovery Partition Version 1.1 - 5.0(0.29)S91(0.29)

sensor#
```

NM-CIDS のバージョン出力のサンプル

```
nm-cids# show version
Application Partition:
Cisco Intrusion Prevention System, Version 5.0(0.27)S129.0

OS Version 2.4.26-IDS-smp-bigphys
Platform: NM-CIDS
Serial Number: JAD06490681
No license present
Sensor up-time is 1 day.
Using 485675008 out of 509448192 bytes of available memory (95% usage)
system is using 17.3M out of 29.0M bytes of available disk space (59% usage)
application-data is using 31.1M out of 166.8M bytes of available disk space (20%
usage)
boot is using 39.5M out of 68.6M bytes of available disk space (61% usage)
application-log is using 529.6M out of 2.8G bytes of available disk space (20% usage)


MainApp          2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600   Running
AnalysisEngine   2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600   Running
CLI              2005_Feb_09_03.00   (Release)   2005-02-09T03:22:27-0600


Upgrade History:

  IDS-K9-maj-5.0-0.27-S91-0.27-.pkg   03:00:00 UTC Thu Feb 05 2004

Recovery Partition Version 1.1 - 5.0(0.27)S91(0.27)

nm-cids#
```

（注）　--MORE-- プロンプトが表示されたら、Space キーを押して次の情報を表示するか、**Ctrl+C** キーを押して出力をキャンセルし、CLI プロンプトに戻ります。

ステップ 3　コンフィギュレーション情報を表示します。

（注）　**more current-config** または **show configuration** コマンドを使用できます。

```
sensor# more current-config
! ------------------------------
! Version 5.0(0.26)
! Current configuration last modified Wed Feb 16 03:20:54 2005
! ------------------------------
display-serial
! ------------------------------
service analysis-engine
exit
! ------------------------------
service authentication
exit
! ------------------------------
service event-action-rules rules0
exit
! ------------------------------
service host
network-settings
host-ip 10.89.147.31/25,10.89.147.126
host-name sensor
access-list 0.0.0.0/0
login-banner-text This message will be displayed on banner login.
exit
time-zone-settings
--MORE--
```

統計情報

センサーのサービスの状態を調べるには、**show statistics** コマンドが役に立ちます。

この項で取り上げる事項は次のとおりです。

- 概要（P.C-61）
- 統計情報の表示（P.C-62）

概要

show statistics コマンドは、センサーのサービスの状態のスナップショットを提供します。次の統計情報を提供します。

- 分析エンジン
- 認証
- 拒否された攻撃者
- イベント サーバ
- イベント ストア

- ホスト
- ロガー
- ネットワーク アクセス
- 通知
- SDEE サーバ
- トランザクション サーバ
- トランザクション ソース
- 仮想センサー
- Web サーバ

（注）　**Monitoring > Support Information > Statistics** をクリックすることによって、IDM から同じ情報を収集できます。

統計情報の表示

show statistics virtual-sensor [**clear**] コマンドを使用して、仮想サーバの統計情報を表示できます。**show statistics [analysis-engine** | **authentication** | **denied-attackers** | **event-server** | **event-store** | **host** | **logger** | **network-access** | **notification** | **sdee-server** | **transaction-server** | **transaction-source** | **web-server**] [**clear**] コマンドを使用して、各センサー アプリケーションの統計情報を生成できます。

（注）　**clear** オプションは、分析エンジン、ホスト、またはネットワーク アクセス アプリケーションには使用できません。

センサーの統計情報を表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　仮想センサーの統計情報を表示します。

```
sensor# show statistics virtual-sensor
Virtual Sensor Statistics
   Statistics for Virtual Sensor vs0
      Name of current Signature-Definition instance = sig0
      Name of current Event-Action-Rules instance = rules0
      List of interfaces monitored by this virtual sensor = fe0_1
      General Statistics for this Virtual Sensor
         Number of seconds since a reset of the statistics = 1675
         Measure of the level of resource utilization = 0
         Total packets processed since reset = 241
         Total IP packets processed since reset = 12
         Total packets that were not IP processed since reset = 229
         Total TCP packets processed since reset = 0
         Total UDP packets processed since reset = 0
         Total ICMP packets processed since reset = 12
         Total packets that were not TCP, UDP, or ICMP processed since reset = 0
         Total ARP packets processed since reset = 0
         Total ISL encapsulated packets processed since reset = 0
         Total 802.1q encapsulated packets processed since reset = 0
         Total packets with bad IP checksums processed since reset = 0
         Total packets with bad layer 4 checksums processed since reset = 0
         Total number of bytes processed since reset = 22513
```

```
   The rate of packets per second since reset = 0
   The rate of bytes per second since reset = 13
   The average bytes per packet since reset = 93
Denied Address Information
   Number of Active Denied Attackers = 0
   Number of Denied Attackers Inserted = 0
   Number of Denied Attackers Total Hits = 0
   Number of times max-denied-attackers limited creation of new entry = 0
   Number of exec Clear commands during uptime = 0
Denied Attackers and hit count for each.
The Signature Database Statistics.
   The Number of each type of node active in the system (can not be reset)
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   The number of each type of node inserted since reset
      Total nodes inserted = 28
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 6
   The rate of nodes per second for each time since reset
      Nodes per second = 0
      TCP nodes keyed on both IP addresses and both ports per second = 0
      UDP nodes keyed on both IP addresses and both ports per second = 0
      IP nodes keyed on both IP addresses per second = 0
   The number of root nodes forced to expire because of memory constraints
      TCP nodes keyed on both IP addresses and both ports = 0
Fragment Reassembly Unit Statistics for this Virtual Sensor
   Number of fragments currently in FRU = 0
   Number of datagrams currently in FRU = 0
   Number of fragments received since reset = 0
   Number of fragments forwarded since reset = 0
   Number of fragments dropped since last reset = 0
   Number of fragments modified since last reset = 0
   Number of complete datagrams reassembled since last reset = 0
   Fragments hitting too many fragments condition since last reset = 0
   Number of overlapping fragments since last reset = 0
   Number of Datagrams too big since last reset = 0
   Number of overwriting fragments since last reset = 0
   Number of Initial fragment missing since last reset = 0
   Fragments hitting the max partial dgrams limit since last reset = 0
   Fragments too small since last reset = 0
   Too many fragments per dgram limit since last reset = 0
   Number of datagram reassembly timeout since last reset = 0
   Too many fragments claiming to be the last since last reset = 0
   Fragments with bad fragment flags since last reset = 0
TCP Normalizer stage statistics
   Packets Input = 0
   Packets Modified = 0
   Dropped packets from queue = 0
   Dropped packets due to deny-connection = 0
   Current Streams = 0
   Current Streams Closed = 0
   Current Streams Closing = 0
   Current Streams Embryonic = 0
   Current Streams Established = 0
   Current Streams Denied = 0
Statistics for the TCP Stream Reassembly Unit
   Current Statistics for the TCP Stream Reassembly Unit
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   Cumulative Statistics for the TCP Stream Reassembly Unit since reset
      TCP streams that have been tracked since last reset = 0
      TCP streams that had a gap in the sequence jumped = 0
      TCP streams that was abandoned due to a gap in the sequence = 0
```

```
      TCP packets that arrived out of sequence order for their stream = 0
      TCP packets that arrived out of state order for their stream = 0
      The rate of TCP connections tracked per second since reset = 0
SigEvent Preliminary Stage Statistics
   Number of Alerts received = 491
   Number of Alerts Consumed by AlertInterval = 0
   Number of Alerts Consumed by Event Count = 0
   Number of FireOnce First Alerts = 6
   Number of FireOnce Intermediate Alerts = 480
   Number of Summary First Alerts  = 0
   Number of Summary Intermediate Alerts  = 0
   Number of Regular Summary Final Alerts  = 0
   Number of Global Summary Final Alerts  = 0
   Number of Alerts Output for further processing = 491
SigEvent Action Override Stage Statistics
   Number of Alerts received to Action Override Processor = 0
   Number of Alerts where an override was applied = 0
   Actions Added
      deny-attacker-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
      reset-tcp-connection = 0
SigEvent Action Filter Stage Statistics
   Number of Alerts received to Action Filter Processor = 0
   Number of Alerts where an action was filtered = 0
   Number of Filter Line matches = 0
   Actions Filtered
      deny-attacker-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 0
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 0
      request-snmp-trap = 0
      reset-tcp-connection = 0
SigEvent Action Handling Stage Statistics.
   Number of Alerts received to Action Handling Processor = 491
   Number of Alerts where produceAlert was forced = 0
   Number of Alerts where produceAlert was off = 0
   Actions Performed
      deny-attacker-inline = 0
      deny-connection-inline = 0
      deny-packet-inline = 0
      modify-packet-inline = 0
      log-attacker-packets = 0
      log-pair-packets = 0
      log-victim-packets = 0
      produce-alert = 11
      produce-verbose-alert = 0
      request-block-connection = 0
      request-block-host = 5
      request-snmp-trap = 0
      reset-tcp-connection = 0
   Deny Actions Requested in Promiscuous Mode
      deny-packet not performed = 0
```

```
            deny-connection not performed = 0
            deny-attacker not performed = 0
            modify-packet not performed = 0
         Number of Alerts where deny-connection was forced for deny-packet action = 0
         Number of Alerts where deny-packet was forced for non-TCP deny-connection
action = 0
      Per-Signature SigEvent count since reset
         Sig 2004 = 5
         Sig 2156 = 486
sensor#
```

ステップ 3　分析エンジンの統計情報を表示します。

```
sensor# show statistics analysis-engine
Analysis Engine Statistics
   Number of seconds since service started = 1999
   Measure of the level of current resource utilization = 0
   Measure of the level of maximum resource utilization = 0
   The rate of TCP connections tracked per second = 0
   The rate of packets per second = 0
   The rate of bytes per second = 13
   Receiver Statistics
      Total number of packets processed since reset = 290
      Total number of IP packets processed since reset = 12
   Transmitter Statistics
      Total number of packets transmitted = 290
      Total number of packets denied = 0
      Total number of packets reset = 0
   Fragment Reassembly Unit Statistics
      Number of fragments currently in FRU = 0
      Number of datagrams currently in FRU = 0
   TCP Stream Reassembly Unit Statistics
      TCP streams currently in the embryonic state = 0
      TCP streams currently in the established state = 0
      TCP streams currently in the closing state = 0
      TCP streams currently in the system = 0
      TCP Packets currently queued for reassembly = 0
   The Signature Database Statistics.
      Total nodes active = 0
      TCP nodes keyed on both IP addresses and both ports = 0
      UDP nodes keyed on both IP addresses and both ports = 0
      IP nodes keyed on both IP addresses = 0
   Statistics for Signature Events
      Number of SigEvents since reset = 491
   Statistics for Actions executed on a SigEvent
      Number of Alerts written to the IdsEventStore = 11
sensor#
```

ステップ 4　認証の統計情報を表示します。

```
sensor# show statistics authentication
General
   totalAuthenticationAttempts = 2
   failedAuthenticationAttempts = 0
sensor#
```

ステップ 5　システム内で拒否された攻撃者の統計情報を表示します。

```
sensor# show statistics denied-attackers
Denied Attackers and hit count for each.
sensor#
```

ステップ 6　イベント サーバの統計情報を表示します。

```
sensor# show statistics event-server
General
   openSubscriptions = 0
   blockedSubscriptions = 0
Subscriptions
sensor#
```

ステップ 7　イベント ストアの統計情報を表示します。

```
sensor# show statistics event-store
Event store statistics
   General information about the event store
      The current number of open subscriptions = 2
      The number of events lost by subscriptions and queries = 0
      The number of queries issued = 0
      The number of times the event store circular buffer has wrapped = 0
   Number of events of each type currently stored
      Debug events = 0
      Status events = 9904
      Log transaction events = 0
      Shun request events = 61
      Error events, warning = 67
      Error events, error = 83
      Error events, fatal = 0
      Alert events, informational = 60
      Alert events, low = 1
      Alert events, medium = 60
      Alert events, high = 0
sensor#
```

ステップ 8　ホストの統計情報を表示します。

```
sensor# show statistics host
General Statistics
   Last Change To Host Config (UTC) = 16:11:05  Thu Feb 10 2005
   Command Control Port Device = FastEthernet0/0
Network Statistics
   fe0_0     Link encap:Ethernet  HWaddr 00:0B:46:53:06:AA
             inet addr:10.89.149.185  Bcast:10.89.149.255  Mask:255.255.255.128
             UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
             RX packets:1001522 errors:0 dropped:0 overruns:0 frame:0
             TX packets:469569 errors:0 dropped:0 overruns:0 carrier:0
             collisions:0 txqueuelen:1000
             RX bytes:57547021 (54.8 MiB)  TX bytes:63832557 (60.8 MiB)
             Interrupt:9 Base address:0xf400 Memory:c0000000-c0000038
NTP Statistics
   status = Not applicable
Memory Usage
   usedBytes = 500592640
   freeBytes = 8855552
   totalBytes = 509448192
Swap Usage
   Used Bytes = 77824
   Free Bytes = 600649728

   Total Bytes = 600727552
CPU Statistics
   Usage over last 5 seconds = 0
   Usage over last minute = 1
   Usage over last 5 minutes = 1
Memory Statistics
   Memory usage (bytes) = 500498432
   Memory free (bytes) = 894976032
Auto Update Statistics
   lastDirectoryReadAttempt = N/A
   lastDownloadAttempt = N/A
   lastInstallAttempt = N/A
   nextAttempt = N/A
sensor#
```

ステップ 9　ロギング アプリケーションの統計情報を表示します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 11
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 35
   TOTAL = 99
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 64
   Warning Severity = 24
   Timing Severity = 311
   Debug Severity = 31522
   Unknown Severity = 7
   TOTAL = 31928
sensor#
```

ステップ 10 ARC の統計情報を表示します。

```
sensor# show statistics network-access
Current Configuration
   LogAllBlockEventsAndSensors = true
   EnableNvramWrite = false
   EnableAclLogging = false
   AllowSensorBlock = false
   BlockMaxEntries = 11
   MaxDeviceInterfaces = 250
   NetDevice
      Type = PIX
      IP = 10.89.150.171
      NATAddr = 0.0.0.0
      Communications = ssh-3des
   NetDevice
      Type = PIX
      IP = 10.89.150.219
      NATAddr = 0.0.0.0
      Communications = ssh-des
   NetDevice
      Type = PIX
      IP = 10.89.150.250
      NATAddr = 0.0.0.0
      Communications = telnet
   NetDevice
      Type = Cisco
      IP = 10.89.150.158
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = out
         InterfacePostBlock = Post_Acl_Test
      BlockInterface
         InterfaceName = ethernet0/1
         InterfaceDirection = in
         InterfacePreBlock = Pre_Acl_Test
         InterfacePostBlock = Post_Acl_Test
   NetDevice
      Type = CAT6000_VACL
      IP = 10.89.150.138
      NATAddr = 0.0.0.0
      Communications = telnet
      BlockInterface
         InterfaceName = 502
         InterfacePreBlock = Pre_Acl_Test
      BlockInterface
         InterfaceName = 507
         InterfacePostBlock = Post_Acl_Test
State
   BlockEnable = true
   NetDevice
      IP = 10.89.150.171
      AclSupport = Does not use ACLs
      Version = 6.3
      State = Active
      Firewall-type = PIX
   NetDevice
      IP = 10.89.150.219
      AclSupport = Does not use ACLs
      Version = 7.0
      State = Active
      Firewall-type = ASA
   NetDevice
      IP = 10.89.150.250
      AclSupport = Does not use ACLs
      Version = 2.2
```

```
      State = Active
      Firewall-type = FWSM
   NetDevice
      IP = 10.89.150.158
      AclSupport = uses Named ACLs
      Version = 12.2
      State = Active
   NetDevice
      IP = 10.89.150.138
      AclSupport = Uses VACLs
      Version = 8.4
      State = Active
   BlockedAddr
      Host
         IP = 22.33.4.5
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 21.21.12.12
         Vlan =
         ActualIp =
         BlockMinutes =
      Host
         IP = 122.122.33.4
         Vlan =
         ActualIp =
         BlockMinutes = 60
         MinutesRemaining = 24
      Network
         IP = 111.22.0.0
         Mask = 255.255.0.0
         BlockMinutes =
sensor#
```

ステップ 11 通知アプリケーションの統計情報を表示します。

```
sensor# show statistics notification
General
   Number of SNMP set requests = 0
   Number of SNMP get requests = 0
   Number of error traps sent = 0
   Number of alert traps sent = 0
sensor#
```

ステップ 12 SDEE サーバの統計情報を表示します。

```
sensor# show statistics sdee-server
General
   Open Subscriptions = 0
   Blocked Subscriptions = 0
   Maximum Available Subscriptions = 5
   Maximum Events Per Retrieval = 500
Subscriptions
sensor#
```

ステップ 13 トランザクション サーバの統計情報を表示します。

```
sensor# show statistics transaction-server
General
   totalControlTransactions = 35
   failedControlTransactions = 0
sensor#
```

ステップ 14 トランザクション ソースの統計情報を表示します。

```
sensor# show statistics transaction-source
General
   totalControlTransactions = 0
   failedControlTransactions = 0
sensor#
```

ステップ 15 Web サーバの統計情報を表示します。

```
sensor# show statistics web-server
listener-443
   number of server session requests handled = 61
   number of server session requests rejected = 0
   total HTTP requests handled = 35
   maximum number of session objects allowed = 40
   number of idle allocated session objects = 10
   number of busy allocated session objects = 0
crypto library version = 6.0.3
sensor#
```

ステップ 16 ロギング アプリケーションなどのアプリケーションの統計情報をクリアするには、次の手順を実行します。

```
sensor# show statistics logger clear
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 141
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 142
   TOTAL = 156
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 14
   Warning Severity = 1
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 28
   TOTAL = 43
```

統計情報が検出され、クリアされました。

ステップ 17 統計情報がクリアされたことを確認します。

```
sensor# show statistics logger
The number of Log interprocessor FIFO overruns = 0
The number of syslog messages received = 0
The number of <evError> events written to the event store by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   TOTAL = 0
The number of log messages written to the message log by severity
   Fatal Severity = 0
   Error Severity = 0
   Warning Severity = 0
   Timing Severity = 0
   Debug Severity = 0
   Unknown Severity = 0
   TOTAL = 0
sensor#
```

統計情報はすべて 0 から始まります。

インターフェイスの情報

検知インターフェイス、コマンド / コントロール インターフェイスに関する情報を収集するには、**show interfaces** コマンドが役に立ちます。

この項で取り上げる事項は次のとおりです。

- 概要（P.C-71）
- インターフェイス コマンドの出力（P.C-72）

概要

show interfaces コマンドを使用して、次の情報を学習できます。

- インターフェイスが起動しているか停止しているか
- パケットが表示されているかどうかと、どのインターフェイスに表示されているか
- パケットが SensorApp によってドロップされているかどうか
- パケットのドロップにつながるエラーがインターフェイスによって報告されているかどうか

show interfaces コマンドは、すべてのシステム インターフェイスの統計情報を表示します。また、個別のコマンドを使用して、コマンド / コントロール インターフェイス（**show interfaces** *command_control_interface_name*）、検知インターフェイス（**show interfaces** *interface_name*）のそれぞれの統計情報を表示することもできます。

インターフェイス コマンドの出力

次は、**show interfaces** コマンドの出力例です。

```
sensor# show interfaces
Interface Statistics
   Total Packets Received = 0
   Total Bytes Received = 0
   Missed Packet Percentage = 0
   Current Bypass Mode = Auto_off
MAC statistics from interface GigabitEthernet0/1
   Media Type = backplane
   Missed Packet Percentage = 0
   Inline Mode = Unpaired
   Pair Status = N/A
   Link Status = Up
   Link Speed = Auto_1000
   Link Duplex = Auto_Full
   Total Packets Received = 0
   Total Bytes Received = 0
   Total Multicast Packets Received = 0
   Total Broadcast Packets Received = 0
   Total Jumbo Packets Received = 0
   Total Undersize Packets Received = 0
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 0
   Total Bytes Transmitted = 0
   Total Multicast Packets Transmitted = 0
   Total Broadcast Packets Transmitted = 0
   Total Jumbo Packets Transmitted = 0
   Total Undersize Packets Transmitted = 0
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
MAC statistics from interface GigabitEthernet0/0
   Media Type = TX
   Link Status = Up
   Link Speed = Auto_100
   Link Duplex = Auto_Full
   Total Packets Received = 2211296
   Total Bytes Received = 157577635
   Total Multicast Packets Received = 20
   Total Receive Errors = 0
   Total Receive FIFO Overruns = 0
   Total Packets Transmitted = 239723
   Total Bytes Transmitted = 107213390
   Total Transmit Errors = 0
   Total Transmit FIFO Overruns = 0
sensor#
```

イベント情報

show events コマンドを使用して、SensorApp によって生成されたアラートとアプリケーションによって生成されたエラーを表示できます。

この項で取り上げる事項は次のとおりです。

- センサー イベント（P.C-73）
- 概要（P.C-73）
- イベントの表示（P.C-73）
- イベントのクリア（P.C-76）

センサー イベント

イベントには、次の 5 つのタイプがあります。

- evAlert：侵入検知アラート
- evError：アプリケーション エラー
- evStatus：IP ログを作成中など、ステータスの変化
- evLogTransaction：各センサー　アプリケーションによって処理される制御トランザクションのレコード
- evShunRqst：ブロック要求

イベントは、新しいイベントに上書きされるまでイベント ストア内に残ります。

概要

イベント ビューアやセキュリティ モニタでイベントが表示されないなどのイベント取り込み問題をトラブルシューティングする場合には、**show events** コマンドが役に立ちます。**show events** コマンドを使用すると、センサー上でどのイベントが生成されたかを判断し、生成されたイベントと障害がモニタリング側にあることを確認できます。

clear events コマンドを使用して、イベント ストアのすべてのイベントをクリアできます。

show events コマンドのパラメータは次のとおりです。

```
sensor# show events
<cr>
alert          Display local system alerts.
error          Display error events.
hh:mm[:ss]     Display start time.
log            Display log events.
nac            Display NAC shun events.
past           Display events starting in the past specified time.
status         Display status events.
|              Output modifiers.
```

イベントの表示

show events [{[**alert** [informational] [low] [medium] [high] [**include-traits** ***traits***] [**exclude-traits** ***traits***]] | **error** [warning] [error] [fatal] | **log** | **NAC** | **status**}] [*hh:mm:ss* [*month day* [*year*]] | **past** *hh:mm:ss*] コマンドを使用して、イベント ストアのイベントを表示できます。

開始時刻から、イベントが表示されます。開始時刻を指定しない場合は、現在時刻から、イベントが表示されます。イベント タイプを指定しない場合は、すべてのイベントが表示されます。

（注）　イベントは、**Ctrl+C** キーを押して要求をキャンセルするまで、ライブ フィードとして表示されます。

次のオプションが適用されます。

- **alert**：アラートを表示します。攻撃が進行中であること、または攻撃が試みられたことを示している可能性のある不審なアクティビティを通知します。

  レベル（informational、low、medium、または high）が選択されていない場合は、すべてのアラート イベントが表示されます。
- **include-traits**：指定した特性を持つアラートを表示します。

- **exclude-traits**：指定した特性を持つアラートを表示しません。
- **traits**：10 進数（0 ～ 15）で表した特性ビットの位置。
- **error**：エラー イベントを表示します。エラー イベントは、エラー条件が発生したときにサービスによって生成されます。
- **log**：ログ イベントを表示します。ログ イベントは、トランザクションが受信され、アプリケーションの応答があったときに生成されます。トランザクションの要求、応答、および成功または失敗に関する情報が含まれています。
- **NAC**：ARC（ブロック）要求を表示します。
- **status**：ステータス イベントを表示します。
- **past**：指定された時間数、分数、秒数の間に開始されたイベントを表示します。
- *hh:mm:ss*：表示を開始する過去の時、分、秒。

（注）　**show events** コマンドは、指定されたイベントが使用可能になるまで待機します。**Ctrl+C** キーを押して終了するまで、イベントの待機と表示は継続します。

イベント ストアのイベントを表示するには、次の手順を実行します。

ステップ 1　CLI にログインします。

ステップ 2　現在開始されているすべてのイベントを表示します。

```
sensor#@ show events
evError: eventId=1041472274774840147 severity=warning vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 12075
  time: 2003/01/07 04:41:45 2003/01/07 04:41:45 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown

evError: eventId=1041472274774840148 severity=error vendor=Cisco
  originator:
    hostId: sensor2
    appName: cidwebserver
    appInstanceId: 351
  time: 2003/01/07 04:41:45 2003/01/07 04:41:45 UTC
  errorMessage: name=errTransport WebSession::sessionTask(6) TLS connection exce
ption: handshake incomplete.
```

フィードは、**Ctrl+C** キーを押すまですべてのイベントを表示し続けます。

ステップ 3　2005 年 2 月 9 日の午前 10 時から、ブロック要求を表示します。

```
sensor#@ show events NAC 10:00:00 Feb 9 2005
evShunRqst: eventId=1106837332219222281 vendor=Cisco
  originator:
    deviceName: Sensor1
    appName: NetworkAccessControllerApp
    appInstance: 654
  time: 2005/02/09 10:33:31 2004/08/09 13:13:31
  shunInfo:
    host: connectionShun=false
      srcAddr: 11.0.0.1
      destAddr:
      srcPort:
      destPort:
      protocol: numericType=0 other
    timeoutMinutes: 40
  evAlertRef: hostId=esendHost 123456789012345678
sensor#
```

ステップ 4　2005 年 2 月 9 日の午前 10 時から、警告レベルのエラーを表示します。

```
sensor# show events error warning 10:00:00 Feb 9 2005
evError: eventId=1041472274774840197 severity=warning vendor=Cisco
  originator:
    hostId: sensor
    appName: cidwebserver
    appInstanceId: 12160
  time: 2003/01/07 04:49:25 2003/01/07 04:49:25 UTC
  errorMessage: name=errWarning received fatal alert: certificate_unknown
```

ステップ 5　45 秒前からのアラートを表示します。

```
sensor# show events alert past 00:00:45

evIdsAlert: eventId=1109695939102805307 severity=medium vendor=Cisco
  originator:
    hostId: sensor
    appName: sensorApp
    appInstanceId: 367
  time: 2005/03/02 14:15:59 2005/03/02 14:15:59 UTC
  signature: description=Nachi Worm ICMP Echo Request id=2156 version=S54
    subsigId: 0
    sigDetails: Nachi ICMP
  interfaceGroup:
  vlan: 0
  participants:
    attacker:
      addr: locality=OUT 10.89.228.202
    target:
      addr: locality=OUT 10.89.150.185
  riskRatingValue: 70
  interface: fe0_1
  protocol: icmp


evIdsAlert: eventId=1109695939102805308 severity=medium vendor=Cisco
  originator:
--MORE--
```

ステップ 6　過去 30 秒間に始まったイベントを表示します。

```
sensor# show events past 00:00:30
evStatus: eventId=1041526834774829055 vendor=Cisco
  originator:
    hostId: sensor
    appName: mainApp
    appInstanceId: 2215
  time: 2003/01/08 02:41:00 2003/01/08 02:41:00 UTC
  controlTransaction: command=getVersion successful=true
    description: Control transaction response.
    requestor:
      user: cids
      application:
        hostId: 64.101.182.101
        appName: -cidcli
        appInstanceId: 2316


evStatus: eventId=1041526834774829056 vendor=Cisco
  originator:
    hostId: sensor
    appName: login(pam_unix)
    appInstanceId: 2315
  time: 2003/01/08 02:41:00 2003/01/08 02:41:00 UTC
  syslogMessage:
    description: session opened for user cisco by cisco(uid=0)
```

イベントのクリア

イベント ストアをクリアするには、**clear events** コマンドを使用します。

イベント ストアのイベントをクリアするには、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 CLI にログインします。

ステップ 2　イベント ストアをクリアします。

```
sensor# clear events
Warning: Executing this command will remove all events currently stored in the event
store.
Continue with clear? []:
```

ステップ 3　**yes** を入力してイベントをクリアします。

cidDump スクリプト

IDM または CLI へのアクセス権限がない場合は、root としてログインして /usr/cids/idsRoot/bin/cidDump を実行することによって、基盤となるスクリプト cidDump をサービス アカウントから実行できます。cidDump ファイルのパスは /usr/cids/idsRoot/htdocs/private/cidDump.html です。

cidDump は大量の情報を取り込むためのスクリプトです。この情報には、IPS プロセス リスト、ログ ファイル、OS 情報、ディレクトリ リスト、パッケージ情報、設定ファイルなどがあります。

cidDump スクリプトを実行するには、次の手順を実行します。

ステップ 1　センサー サービス アカウントにログインします。

ステップ 2　su と入力し、サービス アカウント パスワードを使用して root になります。

ステップ 3　cidDump /usr/cids/idsRoot/bin/cidDump と入力します。

ステップ 4　結果として生成される /usr/cids/idsRoot/log/cidDump.html ファイルを圧縮します。

```
gzip /usr/cids/idsRoot/log/cidDump.html
```

ステップ 5　問題が発生した場合は、結果として生成される HTML ファイルを TAC または IPS 開発者に送信します。

手順については、P.C-77 の「Cisco FTP サイトのファイルのアップロードとアクセス」を参照してください。

Cisco FTP サイトのファイルのアップロードとアクセス

サイズの大きいファイル、たとえば、cidDump.html、show tech-support コマンドの出力、コア ファイルなどを ftp-sj サーバにアップロードできます。

Cisco FTP サイトでファイルのアップロードやアクセスを実行するには、次の手順を実行します。

ステップ 1　anonymous として ftp-sj.cisco.com にログインします。

ステップ 2　/incoming ディレクトリに移動します。

ステップ 3　ファイルをアップロードするには、**put** コマンドを使用します。

バイナリ転送タイプを使用していることを確認します。

ステップ 4　アップロードされたファイルにアクセスするには、ECS にサポートされたホストとしてログインします。

ステップ 5　/auto/ftp/incoming ディレクトリに移動します。