Trend Micro InterScan for Cisco CSC SSM のトラブルシューティング

この章では、サポートについて TAC にお問い合わせになる前に、潜在的な問題を解決するための有益な情報を提供します。次の項で構成されています。

- インストール時のトラブルシューティング（P.8-3）
- インストールに失敗した場合の対処法（P.8-6）
- アクティベーションのトラブルシューティング（P.8-6）
- 基本機能のトラブルシューティング（P.8-7）
  - ログオンできない（P.8-7）
  - 失ったパスワードの回復（P.8-7）
  - 要約ステータスとログ エントリが同期していない（P.8-8）
  - HTTP 接続の遅延（P.8-8）
  - 一部の Web サイトへのアクセス速度が遅い、またはアクセスできない（P.8-9）
  - FTP ダウンロードが実行できない（P.8-9）
- スキャン機能のトラブルシューティング（P.8-10）
  - パターン ファイルをアップデートできない（P.8-10）
  - スパムが検出されない（P.8-10）
  - スパム スタンプ識別情報が作成できない（P.8-10）
  - 許容できない数のスパムの false positive が検出される（P.8-11）
  - スパムの false positive を許容できない（P.8-11）
  - 許容できない大量のスパムが検出される（P.8-11）
  - ウィルスは検出されるがクリーニングされない（P.8-11）
  - ウィルスのスキャンが動作しない（P.8-11）
  - 大容量ファイルのダウンロード（P.8-13）
  - スキャン サービスの再起動（P.8-14）
- パフォーマンスのトラブルシューティング（P.8-15）
  - CSC SSM コンソールがタイムアウトした（P.8-15）
  - ステータス LED が 1 分以上点滅する（P.8-15）
  - SSM が ASDM と通信できない（P.8-15）
  - ASDM を使用しないログイン（P.8-15）
  - CSC SSM のスループットが ASA よりはるかに低い（P.8-16）

- CSC SSM Syslog の概要（P.8-19）
  - SSM アプリケーションのミスマッチ [1-105048]（P.8-19）
  - CSC カードの障害のためにトラフィックが破棄された [3-421001]（P.8-19）
  - 適用外のトラフィックをスキップする [6-421002]（P.8-20）
  - 無効なカプセル化によって ASDP パケットが破棄された [3-421003]（P.8-20）
  - パケットを挿入できない [7-421004]（P.8-20）
  - アカウント ホスト数がライセンスの上限に近づいている [6-421005]（P.8-21）
  - 日単位のノード カウント [5-421006]（P.8-21）
  - CSC カードの障害のためにトラフィックが破棄された [6-421007]（P.8-21）
  - 新しいアプリケーションが検出された [5-505011]（P.8-22）
  - アプリケーションが停止した [5-505012]（P.8-22）
  - アプリケーションのバージョンが変更されている [5-505013]（P.8-22）
  - データ チャネルの通信障害 [3-323006]（P.8-23）
  - データ チャネルの通信は正常 [5-505010]（P.8-23）
- Knowledge Base の使用（P.8-16）
- Security Information Center の使用（P.8-17）
- CSC SSM Syslog の概要（P.8-19）
- Cisco TAC にお問い合わせになる前に（P.8-24）

インストール時のトラブルシューティング

次に、インストールを正しく実行するためのコマンドライン バージョンについて説明します。インストール中に問題が発生した場合は、P.8-6 の「インストールに失敗した場合の対処法」を参照してください。

コマンドライン インターフェイスを通じて CSC SSM をインストールするには、次の手順を実行します。

ステップ 1　コマンドライン プロンプトから次のように入力してインストールを開始します。

```
hostname# hw-module module 1 recover configure
```

次のような出力が表示されます。

```
Image URL [tftp://171.69.1.129/dqu/sg-6.0-1345-tftp.img]:
Port IP Address [30.0.0.3]:
VLAN ID [0]:
Gateway IP Address [30.0.0.254]:
hostname# 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
hostname#
hostname# debug module-boot
debug module-boot  enabled at level 1
```

ステップ 2　約 1 分後に、CSC-SSM の ROMMON が実行され、次のようなメッセージが出力されます。

```
hostname# Slot-1 206> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26 00:13:50
PST 2005
Slot-1 207>     morlee@bowmore:/pixab/biosbuild/1.0.10.0/boot/rommon
Slot-1 208> Platform ASA-SSM-AIP-10-K9
Slot-1 209> GigabitEthernet0/0
Slot-1 210> Link is UP
Slot-1 211> MAC Address: 000b.fcf8.01b3
Slot-1 212> ROMMON Variable Settings:
Slot-1 213>   ADDRESS=30.0.0.3
Slot-1 214>   SERVER=171.69.1.129
Slot-1 215>   GATEWAY=30.0.0.254
Slot-1 216>   PORT=GigabitEthernet0/0
Slot-1 217>   VLAN=untagged
Slot-1 218>   IMAGE=dqu/sg-6.0-1345-tftp.img
Slot-1 219>   CONFIG=
Slot-1 220>   LINKTIMEOUT=20
Slot-1 221>   PKTTIMEOUT=2
Slot-1 222>   RETRY=20
Slot-1 223> tftp dqu/sg-6.0-1345-tftp.img@171.69.1.129 via 30.0.0.254
```

ステップ 3　SSM は、イメージをダウンロードするために TFTP サーバに接続を試みます。数分後に、次のような出力が表示されます。

```
Slot-1 224>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 225>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 226>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 227>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 228>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
. . . [ output omitted ]. . .
Slot-1 400>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 401>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 402>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 403>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 404>
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 405> !!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Slot-1 406> Received 59501255 bytes
```

ステップ 4　TFTP のダウンロードが終了します。受信したバイト数に注意してください。このバイト数はユーザの CSC SSM イメージと同じサイズになるはずです。次に、ROMMON がこのイメージを起動します。

```
Slot-1 407> Launching TFTP Image...
```

ステップ 5　イメージが解凍され、インストールされます。数分すると、CSC SSM がリブートします。次のようなメッセージが表示されます。

```
Slot-1 408> Cisco Systems ROMMON Version (1.0(10)0) #0: Sat Mar 26 00:13:50 PST 2005
Slot-1 409>     morlee@bowmore:/pixab/biosbuild/1.0.10.0/boot/rommon
Slot-1 410> Platform ASA-SSM-AIP-10-K9
Slot-1 411> Launching BootLoader...
```

ステップ 6　1、2 分後に、CSC SSM がブートします。システムのブート時に次のように表示されることを確認してください。

```
hostname# show module 1
```

次のような出力が表示されます。

```
Mod Card Type                                    Model              Serial No.
--- -------------------------------------------- ------------------ -----------
  1 ASA 5520/5530 AIP Security Service Module-10 ASA-SSM-AIP-10-K9  P00000000TT

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ------------ ---------------
  1 000b.fcf8.01b3 to 000b.fcf8.01b3  1.0          1.0(10)0     CSC SSM 6.0
(Build#1345)

Mod SSM Application Name           Status           SSM Application Version
--- ------------------------------ ---------------- --------------------------
  1 CSC SSM                        Down             6.0 (Build#1345)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

Mod Status テーブル（出力の最終行）に「Up」というインスタンスが 2 つ表示されているかどうか検索してください。SSM Application Name テーブルの Status フィールドに「Down」と表示されている場合は、カードがまだアクティブ化されていないことを示しています。

インストールに失敗した場合の対処法

表 8-1 に、P.8-3 の「インストール時のトラブルシューティング」で説明したインストールに失敗した場合の対処法を手順別に示します。

表 8-1　インストールに失敗した場合の対処法

インストールの失敗が発生した手順	処置
ステップ 2	Cisco TAC にお問い合せください。
ステップ 3	1. ユーザの TFTP サーバが CSC SSM と同じ IP サブネットにある場合は、ゲートウェイの IP アドレスを 0.0.0 に設定したことを確認してください。 2. ルータまたはファイアウォールが CSC SSM とユーザの TFTP サーバとの間に存在する場合は、これらのゲートウェイで UDP ポート 69 を介して TFTP トラフィックが通過できることを確認してください。また、該当するルータがこれらのゲートウェイに正しく設定されていることも確認します。 3. イメージ パスが TFTP サーバ上に存在し、ディレクトリとファイルがすべてのユーザから読み取り可能であることを確認します。
ステップ 4	ダウンロードされた合計バイト数を確認します。このバイト数が CSC SSM イメージのサイズと異なる場合は、ユーザの TFTP サーバがイメージのサイズをサポートしていない可能性があります。この場合は、別の TFTP サーバを使用してください。
ステップ 5	イメージを再びダウンロードし、再度インストールします。2 度目もインストールできなかった場合は、Cisco TAC にお問い合わせください。
ステップ 6	イメージを再びダウンロードし、再度インストールします。2 度目もインストールできなかった場合は、Cisco TAC にお問い合わせください。

アクティベーションのトラブルシューティング

すべての処置を講じる前に、ASA にクロックが正しく設定されていることを確認してください。詳細については、『*Cisco ASA 5500 Series Adaptive Security Appliance Getting Started Guide*』および ASDM のオンライン ヘルプを参照してください。

次に、**show module**、**show module 1**、および **show module 1 details** コマンドを使用して CSC SSM のアクティブ化が正しく実行されていることを確認してください。これらのコマンドの出力を使用しても問題を解決できない場合は、Cisco TAC にお問い合わせください。

基本機能のトラブルシューティング

次の項では、ログオンまたはパスワードの回復といった、基本機能で発生する可能性のある問題の対処法について説明します。

- ログオンできない（P.8-7）
- 失ったパスワードの回復（P.8-7）
- 要約ステータスとログ エントリが同期していない（P.8-8）
- HTTP 接続の遅延（P.8-8）
- 一部の Web サイトへのアクセス速度が遅い、またはアクセスできない（P.8-9）
- FTP ダウンロードが実行できない（P.8-9）

ログオンできない

セットアップ ウィザードを使用して Trend Micro InterScan for Cisco CSC SSM をインストールしたときに、管理者パスワードを指定しています。ログインするには、インストレーション時に作成したこのパスワードを使用する必要があります。このパスワードは、ASDM にアクセスするのに使用するパスワードとは異なります。パスワードは大文字と小文字を区別するため、文字を正確に入力する必要があります。

パスワードを忘れた場合は、回復することができます。詳細については、P.8-16 の「Knowledge Base の使用」を参照してください。

失ったパスワードの回復

ASDM/CSC SSM を管理するには、次の 3 種類のパスワードを使用します。

- ASDM/Web インターフェイスのパスワード
- CLI パスワード
- ルート アカウント パスワード

この 3 種類のパスワードとも、デフォルトのエントリは「cisco」です。3 種類のパスワードすべてをなくした場合に、次の回復手順を実行します。

ステップ 1　CSC SSM を再イメージして、工場出荷時のデフォルト設定に戻します。再イメージすると、工場出荷時のデフォルトのソフトウェア イメージが SSM に転送されます。イメージを転送する場合の手順については、『*Cisco Security Appliance Command Line Configuration Guide*』の、「Managing AIP SSM and CSC SSM」の章の説明を参照してください。

ステップ 2　再イメージ後は、すべてのパスワードがデフォルト値に復元されます。これで、デフォルトのパスワード「cisco」を使用してログインし、ASDM/Web インターフェイス パスワードを新たに作成できるようになります。

ステップ 3　作成した新規 ASDM/Web インターフェイス パスワードを使用して、CSC SSM インターフェイスにアクセスします。**Administration > Configuration Backup** の順にクリックします。

ステップ 4　最新のコンフィギュレーションのバックアップをインポートして、コンフィギュレーション設定を復元します。

ステップ 5　デフォルトのパスワード「cisco」を使用して、コマンドライン インターフェイスおよびルート アカウントにアクセスし、デフォルトの CLI およびルート アカウント パスワードをアップデートします。

パスワードを、全部ではなく 1 つか 2 つだけなくす場合があります。次に、このような場合の対処法について説明します。

- ASDM/Web インターフェイス パスワードはあるが、シスコおよびルート アカウントのパスワードをなくした場合は、Web インターフェイスを通じて CSC SSM の管理を継続できますが、将来の必要時にコマンドライン インターフェイスまたはルート アカウントを使用できません。この 2 種類のパスワードを回復するには、前述の手順で再イメージと復元を行ってください。
- CLI パスワードしかない場合は、CSC SSM にログインして Restore Factory Defaults オプションに移動し、SSM をリセットしてください。これで再イメージと同じ効果があります。その後、保存済みのコンフィギュレーションをインポートします。Restore Factory Defaults オプションについては、P.A-12 の「工場出荷時のデフォルトの復元」を参照してください。
- ルート アカウント パスワードしかない場合は、ログインして **password** コマンドを使用して CLI パスワードを設定します。その後、前述と同様の手順を続行します。

要約ステータスとログ エントリが同期していない

場合によっては、Summary ウィンドウの Mail （SMTP）、Mail （POP3）、Web （HTTP）、および File Transfer （FTP）の各種タブに表示されるカウンタが、ログ レポートに表示される統計情報と同期していない場合があります。（CSC SSM コンソールで **Logs > Query** をクリックしてログにアクセスします）。この「不整合」は次の理由によるものです。

- デバイス　エラーまたはパッチ　インストール後のリブートのいずれかで発生したリブートによって、ログがリセットされている。
- SSM のメモリ ストレージの容量が足りないために、頻繁にログがパージされる。

HTTP 接続の遅延

CSC SSM で URL のフィルタリングをイネーブルにしている場合は、30 秒程度の遅延が発生することがありますが、CSC SSM はインターネットに接続するのに HTTP を使用しません。Trend Micro では、異なるカテゴリの URL を保管するオンライン データベースを維持しています。CSC SSM は、クライアントからの HTTP 要求を代行受信する場合に、URL データベースへのアクセスを試みます。インターネットへのアクセスが実行できない場合は（直接またはプロキシ経由で）、URL フィルタリングをディセーブルにしてください。

一部の Web サイトへのアクセス速度が遅い、またはアクセスできない

銀行やオンライン ショッピング サイトなどの Web サイトや、他の特定の用途のサーバでは、クライアントの要求に応答する前に、追加のバックエンド処理を必要とする場合があります。CSC SSM では、クライアント要求とサーバ応答の間に 90 秒のタイムアウトがハードコードされており、これによってトランザクションが CSC SSM のリソースを長時間占有することを防止します。これは、トランザクションの処理が長時間に及ぶと失敗することを意味しています。

これを回避するには、サイトをスキャンの対象から外します。コマンドライン インターフェイスでこれを行う場合は、たとえば、IP アドレスが 192.168.10.10 の外部ネットワークに対して、次のように実行します。

```
! exempt http traffic to 192.168.10.10
    access-list 101 deny tcp any host 192.168.1.1 eq http
    ! catch everything else
    access-list 101 permit tcp any any eq http
    class-map my_csc_class
          match access-list 101
    policy-map my_csc_policy
         class my_csc_class
             csc fail-close
    service-policy my_csc_policy interface inside
```

このように設定すると、192.168.10.10 までの HTTP トラフィックは CSC SSM からスキャンされなくなります。

パケット キャプチャの実施

CSC SSM を経由せずにアクセス可能なサイトはあるが、トラフィックがスキャンされているためにアクセスできない場合は、Cisco TAC にこの URL を報告してください。可能な場合は、パケット キャプチャを実施し、結果を TAC にも送信してください。たとえば、クライアントの IP が 10.1.1.1 だとすると、外部 Web サイトの IP は、次のように 10.2.2.2 になります。

```
access-list cap_acl permit tcp host 1.1.1.1 host 2.2.2.2
access-list cap_acl permit tcp host 2.2.2.2 host 1.1.1.1
capture cap access-list cap_acl interface inside
capture cap access-list cap_acl interface outside
```

FTP ダウンロードが実行できない

FTP にログインはできるが FTP 経由のダウンロードが実行できない場合は、**inspect ftp** 設定が ASA でイネーブルになっているか確認してください。詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』を参照してください。

スキャン機能のトラブルシューティング

次の項では、ウィルスまたはスパムのスキャンで発生する可能性のある問題の対処法について説明します。

- パターン ファイルをアップデートできない（P.8-10）
- スパムが検出されない（P.8-10）
- スパム スタンプ識別情報が作成できない（P.8-10）
- 許容できない数のスパムの false positive が検出される（P.8-11）
- スパムの false positive を許容できない（P.8-11）
- 許容できない大量のスパムが検出される（P.8-11）
- ウィルスは検出されるがクリーニングされない（P.8-11）
- ウィルスのスキャンが動作しない（P.8-11）
- 大容量ファイルのダウンロード（P.8-13）
- スキャン サービスの再起動（P.8-14）

パターン ファイルをアップデートできない

パターン ファイルが期限切れでアップデートできない場合は、ご使用の Maintenance Agreement が失効している可能性が高いです。**Administration > Product License** ウィンドウの **Expiration Date** フィールドを確認してください。過去の日付が表示されている場合は、Maintenance Agreement を更新するまではパターン ファイルをアップデートできません。

これ以外に考えられる原因は、Trend Micro ActiveUpdate サーバが一時的にダウンしていることです。数分後に、再度アップデートを試みてください。

スパムが検出されない

アンチスパム機能が動作していないように見える場合は、次の点を確認してください。

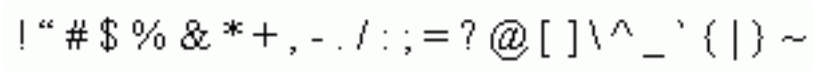
- この機能をイネーブルにしていても、アンチスパムのオプションはデフォルトではイネーブルになっていません（詳細については、P.3-9 の「SMTP および POP3 スパム フィルタリングのイネーブル化」を参照してください）。
- 着信メール ドメインを設定している（詳細については、P.3-7 の「SMTP メッセージ フィルタ、免責条項、および着信メール ドメインの設定」を参照してください）。

スパム スタンプ識別情報が作成できない

スパム スタンプ識別情報とは、電子メール メッセージの件名に表示されるメッセージです。たとえば、「Q3 Report」という見出しのメッセージに対して、スパム スタンプ識別情報で「スパム」と定義された場合、メッセージの件名には「Spam:Q3 Report」と表示されます。

スパム識別情報の作成で問題が発生している場合は、英字の大文字と小文字、数字の 0 ～ 9、図 8-1 に示す特殊文字の組み合わせのみを使用していることを確認してください。

図 8-1　スパム スタンプ識別情報で使用可能な特殊文字



指定以外の文字を使用しようとすると、SMTP および POP3 メッセージでスパム識別情報を使用できません。

許容できない数のスパムの false positive が検出される

スパム フィルタリングしきい値を、過度にアグレッシブな（高すぎる）レベルに設定している場合があります。しきい値を Medium または High に合わせている場合、**Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam** ウィンドウと **Mail (POP3) > Anti-spam > POP3 Anti-spam** ウィンドウで、しきい値のフィールドを低くしてみてください。また、**SMTP Incoming Anti-spam** ウィンドウと **POP3 Anti-spam** ウィンドウで、アンチスパムの「stamp message」機能をイネーブルにします。この 2 種類のウィンドウの詳細については、オンライン ヘルプを参照してください。

さらに、ネットワーク上のユーザがニュースレターを受信している場合は、この種のメッセージによって多数の false positive がトリガーされる傾向があります。承認済みの送信者リストにこのニュースレターの電子メール アドレスまたはドメイン名を追加して、これらのメッセージに対するスパム フィルタリングを省略してください。

スパムの false positive を許容できない

銀行や保険会社などの企業では、メッセージが false positive と識別されるようなリスクを負うことはできません。このような場合は、SMTP および POP3 に対するアンチスパム機能をディセーブルにしてください。

許容できない大量のスパムが検出される

スパム フィルタリングのしきい値を、低すぎるレベルに設定している場合があります。この場合は、**Mail (SMTP) > Anti-spam > SMTP Incoming Anti-spam** ウィンドウと **Mail (POP3) > Anti-spam > POP3 Anti-spam** ウィンドウのしきい値のフィールドで、設定を高くしてください。

ウィルスは検出されるがクリーニングされない

ウィルスに感染したすべてのファイルをクリーニングできるわけではありません。たとえば、パスワードで保護されたファイルは、スキャンもクリーニングもできません。

クリーニングに反応しないウィルスに感染したと思われる場合は、次の URL にアクセスしてください。

http://subwiz.trendmicro.com/SubWiz/Default.asp

このリンクからアクセスする Trend Micro Submission Wizard には、ウィルス感染が疑わしいファイルについて TrendLabs に評価を依頼する際の提出方法など、対処法に関する情報が含まれています。

ウィルスのスキャンが動作しない

SMTP Incoming、SMTP Outgoing、POP3、HTTP、および FTP Scanning の各ウィンドウで、ウィルスのスキャン機能をディセーブルにしているユーザがいないことを確認します。スキャンがイネーブルにも関わらずウィルスが検出されない場合は、カスタマー サポートにお問い合わせください。

また、P.2-3 の「アンチウイルス機能のテスト」の手順に従ってウィルスのスキャン機能をテストしてください。

不正な ASA ファイアウォール ポリシー設定のためにスキャンが動作しない

スキャンが動作しない原因として考えられるもう一つの原因は、ASA ファイアウォール ポリシー設定が正しくないために、ファイルがスキャンされていないことがあります。CLI で ASA **show service-policy csc** コマンドを使用して、SSM でトラフィックを処理するように設定します。次に例を示します。

```
show service-policy flow tcp host [clientIP] host [server IP] eq [proto]
```

次に例を示します。

```
hostname(config)# show service-policy flow tcp host 192.168.10.10 host 10.69.1.129 eq
http
Global policy:
Service-policy: global_policy
    Class-map: trend
        Match: access-lit trend
            Access rule: permit tcp any any eq www
        Action:
            Output flow: csc fail-close
            Input flow set connection timeout tcp 0:05:00
    Class-map: perclient
        Match: access-lit perclient
            Access rule: permit IP any any
            Action:
            Input flow: set connection per-client-max 5 per-client-embryonic-max 2
```

CSC SSM が失敗ステータスにあるためにスキャンが動作しない

CSC SSM がリブートのプロセス中か、ソフトウェアに障害が発生していると、syslog エラーの 421007 が生成されます。CLI で次のコマンドを入力して SSM カードのステータスを表示します。

```
hostname# show module 1
```

次の例に示すように、出力にはいくつかのテーブルが表示されます。3 番目のテーブル（SSM Application Name）にステータスが表示されます。この例では、SSM のステータスは「Down」です。

```
Mod Card Type                                    Model  Serial No.
--- -------------------------------------------- ------------------------------
1 ASA 5500 Series Security Services Module-10  ASA-SSM-10 JAB092400TX

Mod MAC Address Range                 Hw Version   Fw Version   Sw Version
--- --------------------------------- ------------ ---------------------------
  1 0013.c480.ae4c to 0013.c480.ae4c  1.0          1.0(10)0     CSC SSM 6.0
(Build#1345)

Mod SSM Application Name           Status            SSM Application Version
--- ------------------------------ ----------------------------------------
  1 CSC SSM                        Down              6.0 (Build#1345)

Mod Status             Data Plane Status     Compatibility
--- ------------------ --------------------- -------------
  1 Up                 Up
```

3 番目のテーブルの **Status** フィールドに表示可能なステータスは、次の 3 種類です。

- **Down**：無効なアクティベーション コードが使用された、ライセンスが失効している、ファイルが壊れている、などの永続的なエラーの場合に表示されます。
- **Reload**：パターン ファイルのアップデート中など、スキャンが再起動中の場合に表示されます。
- **Up**：通常の操作時を表すステータスです。

各プロセスのステータスを個別に表示するには、CLI で次のコマンドを実行してください。

```
hostname# show module 1 detail
```

次のような出力が表示されます。

```
Getting details from the Service Module, please wait...
    ASA 5500 Series Security Services Module-10
    Model:              ASA-SSM-10
    Hardware version:   1.0
    Serial Number:      JAB092400TX
    Firmware version:   1.0(10)0
    Software version:   CSC SSM 6.0 (Build#1345)
    MAC Address Range:  0013.c480.ae4c to 0013.c480.ae4c
    App. name:          CSC SSM
    App. Status:        Down
    App. Status Desc:   CSC SSM scan services are not available
    App. version:       6.0 (Build#1345)
    Data plane Status:  Up
    Status:             Up
    HTTP Service:       Down

    Mail Service:       Down

    FTP  Service:       Down

    Activated:          No

    Mgmt IP addr:       <not available>

    Mgmt web port:      8443

    Peer IP addr:       <not enabled>
```

CSC SSM のステータスは、**App.Status** フィールドに表示されます。前述の例ではステータスは「Down」です。このフィールドで可能なステータスは次のとおりです。

- **Not Present**：SSM カードは未検出
- **Init**：SSM カードはブート中
- **Up**：SSM カードは稼動中
- **Unresponsive**：SSM カードは応答していない
- **Reload**：SSM カードはリロード中
- **Shutting Down**：SSM カードはシャットダウンしている
- **Down**：SSM カードはダウン状態にあり、スロットから安全に取り外しが可能
- **Recover**：SSM カードは再イメージ中

大容量ファイルのダウンロード

非常に大きいサイズのファイルを扱うと、HTTP プロトコル、または FTP プロトコル上の問題が発生しやすくなります。HTTP Scanning ウィンドウ、および FTP Scanning ウィンドウの Target タブで設定した大容量ファイルの処理フィールドに、スキャンを遅らせるオプションが含まれています。

スキャンの遅延をイネーブルにしなかった場合は、InterScan for Cisco CSC SSM は、ファイル全体を受信およびスキャンしてから、要求しているユーザにファイル内容を渡す必要があります。ファイル サイズによっては、次のようになることもあります。

- 結局、ファイルはダウンロードされるが、最初は非常に低速でダウンロードが進むにつれて高速になる

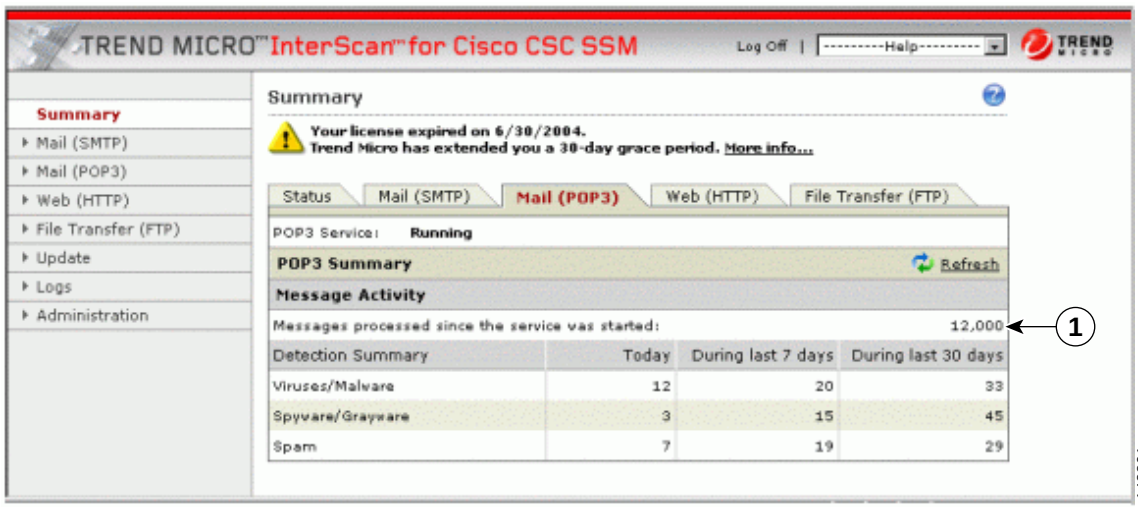
- ブラウザの自動タイムアウト時間が超過して、ユーザは結局ファイルの内容をまったく受信できない（ダウンロードが完了する前にブラウザがタイムアウトしたため）

スキャンの遅延をイネーブルにした場合は、タイムアウトになるのを防ぐため、大規模ファイルの一部の内容はスキャンされずに配信されます。それ以降の部分はバックグラウンドでスキャンされ、その後、脅威が検出されなければダウンロードされます。脅威が*検出された*場合は、残りのファイルはダウンロードされませんが、大規模ファイルのスキャンしていない部分はすでにユーザのマシンに保存されているため、セキュリティ リスクとなる可能性があります。

スキャン サービスの再起動

Summary ウィンドウの Mail （SMTP および POP3）タブでは、ウィンドウの Message Activity 領域に、**Messages processed since the service was started** のカウント数が表示されます。図 8-2 に、表示例を示します。

図 8-2　Summary ウィンドウの Mail（POP3）タブに表示されたメッセージ処理カウンタ



1	メッセージ アクティビティ カウンタ

イベントによってはこのカウンタをゼロにリセットするものがあります。次のようなイベントです。

- パターン ファイルまたはスキャン エンジンのアップデート
- コンフィギュレーションの変更
- パッチの適用

Detection Summary 領域はリセットされません。これらの統計情報は、上記のイベントに関わらず、トリガー イベントが発生するたびにアップデートし続けます。

カウンタがリセットされても問題はありません。カウンタがリセットされる理由を理解しておく必要があるだけです。ただし、**Messages processed...** フィールドでゼロの状態が続いた場合は、電子メール トラフィックがスキャンされていないことを示しているため、状況を調査する必要があります。

パフォーマンスのトラブルシューティング

次の項では、パフォーマンスについて発生する可能性のある問題について説明します。

- CSC SSM コンソールがタイムアウトした（P.8-15）
- ステータス LED が 1 分以上点滅する（P.8-15）
- SSM が ASDM と通信できない（P.8-15）
- ASDM を使用しないログイン（P.8-15）
- CSC SSM のスループットが ASA よりはるかに低い（P.8-16）

CSC SSM コンソールがタイムアウトした

CSC SSM コンソールをアクティブにしてから約 10 分間、アクティビティが 1 つも検出されない状態のままにしておくと、セッションはタイムアウトします。処理を続行するには再びログインしてください。保存していない作業上の変更は失われます。席を離れる場合は、作業内容を保存して戻るまでログオフすることを推奨します。

ステータス LED が 1 分以上点滅する

ステータス LED が 1 分以上点滅を繰り返している場合は、スキャン サービスが利用できない状態になっています。この問題を解決するには、システムを ASDM からリブートするか、カスタマー サポートにお問い合わせください。

注意　ダウンロードするファイルが **Do not scan files larger than...** フィールドの指定よりも大きいと、ファイルはスキャンされずに配信され、セキュリティ リスクとなる場合があります。

SSM が ASDM と通信できない

ポート アクセス制御をリセットすることで、この問題を解決できる可能性があります。手順については、P.A-16 の「管理ポートのアクセス コントロールのリセット」を参照してください。

ASDM を使用しないログイン

何らかの理由で ASDM が利用できない場合は、Web サーバから直接 CSC SSM にログインすることができます。ログインするには、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に、次の URL を入力します。

```
https://{SSM IP addresss}:8443
```

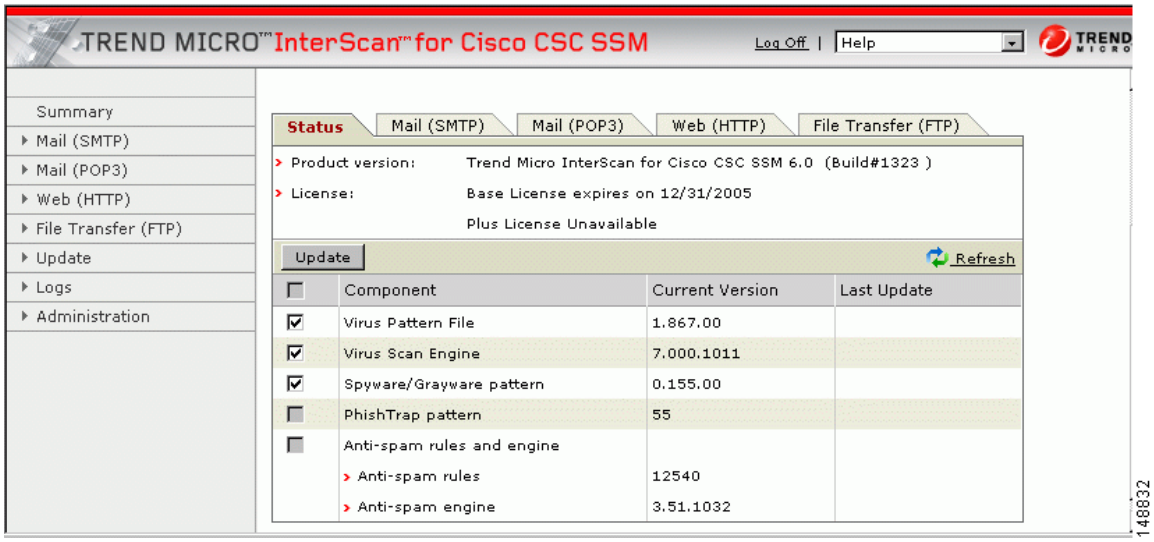
次に例を示します。

```
https://10.123.123.123:8443/
```

ステップ 2　**Logon** ウィンドウが表示されます。セットアップ ウィザードで **Password Configuration** インストール ウィンドウで作成したパスワードを入力し、**Log On** をクリックします。

ステップ 3　CSC SSM コンソールのデフォルト ビューは、次に示すように、**Summary** ウィンドウの Status タブです。

図 8-3　CSC SSM コンソールの Summary 画面に表示された Status タブ



CSC SSM のスループットが ASA よりはるかに低い

TCP 接続からファイルを復元してスキャンする処理は負荷が大きいため、ファイアウォールで通常実行されるプロトコル準拠チェックに比べ、はるかにオーバーヘッドが必要となります。対応策としては、スキャンが必要な接続だけを CSC SSM に誘導して、パフォーマンスのミスマッチを軽減する方法があります。

たとえば、HTTP トラフィックは、発信トラフィック（内部ユーザから外部 Web サイトへのアクセス）、着信トラフィック（外部ユーザから内部サーバへのアクセス）、イントラネット トラフィック（内部サイトと信頼済みパートナー間でのトラフィック）に分割することができます。発信トラフィックのみウィルスをスキャンして、着信トラフィックはスキャンしないように CSC SSM を設定することができます。

詳細については、『*Cisco Security Appliance Command Line Configuration Guide*』の「Managing AIP SSM and CSC SSM」の章を参照してください。

Knowledge Base の使用

Trend Micro のオンライン Knowledge Base を使用すると、より詳細な情報を検索することができます。Knowledge Base の URL は、次のとおりです。

http://esupport.trendmicro.com

Knowledge Base の検索エンジンでは、製品名、問題カテゴリ、キーワードを入力して検索を絞り込むことができます。Knowledge Base には、数千種類のソリューションが用意されており、毎週追加されます。

Security Information Center の使用

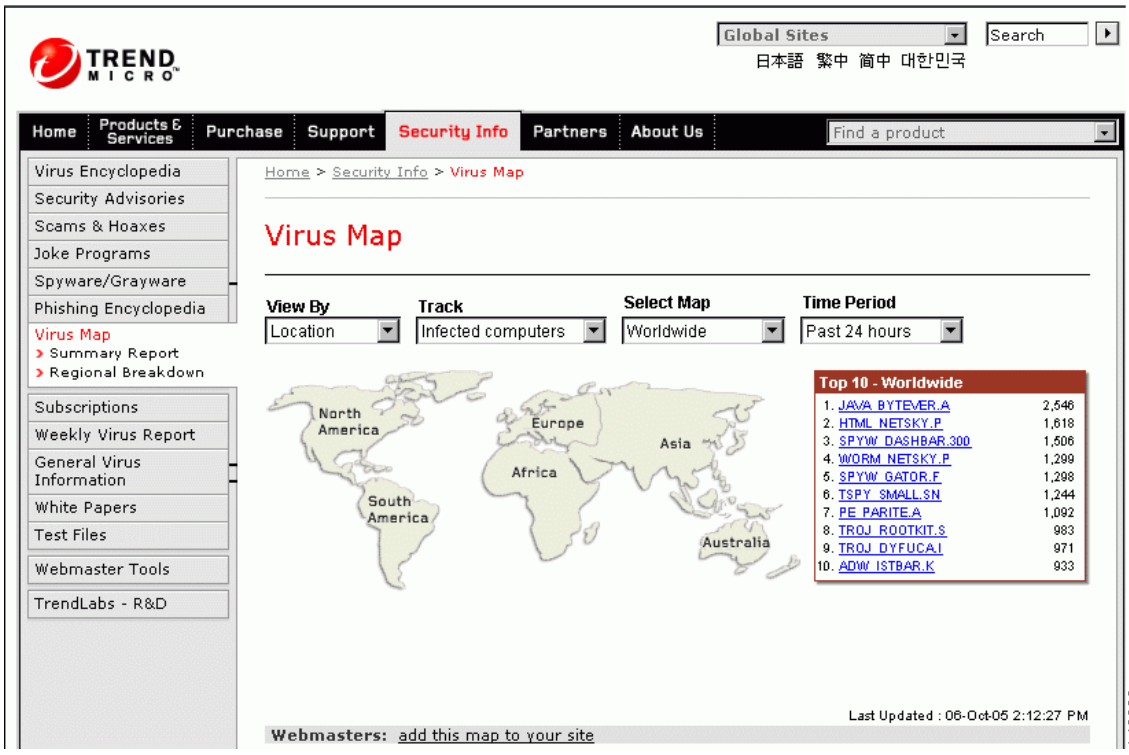
Trend Micro では、無料のオンライン リソースである Security Information Center から、包括的なセキュリティ情報が 24 時間週 7 日利用できます。Security Information Center の URL は次のとおりです。

http://trendmicro.com/vinfo/

Security Information Center では、次の情報を提供しています。

- **Virus Encyclopedia**：ウィルス、ワーム、トロイの木馬、その他すべての既知の脅威に関する知識をまとめたもの
- **Security Advisories**：マルウェアのアラート、最も顕著なリスクの危険度レーティング、最新のパターン ファイルとスキャン エンジンのバージョン、その他の有益な情報の表示
- **Scams and Hoaxes**：マルウェアによるデマ情報、チェーン メールまたは金銭的損失を与えるような詐欺情報、都市伝説などの情報
- **Joke Programs**：Trend Micro のスキャン エンジンで検出された、既知のジョーク プログラムに関する情報のリポジトリ
- **Spyware/Grayware**：検出されたスパイウェア / グレイウェア プログラムのトップ 10 情報、スパイウェア / グレイウェア プログラムの検索可能なデータベース
- **Phishing Encyclopedia**：既知のフィッシング詐欺のリストおよび犯行の手口の説明
- **Virus Map**：世界の地域別に脅威を表示

図 8-4　Virus Map



- **Weekly Virus Report**：その週に検出された脅威についての最新ニュース（Weekly Virus Report を購読すると、週に 1 度レポートが電子メールで自動配信されます）。
- General virus information に含まれる情報は次のとおりです。
  - **Virus Primer**：ウィルスの用語解説とウィルスのライフサイクルに関する説明
  - **Safe Computing Guide**：感染のリスクを減らすための安全基準
  - **Risk ratings**：マルウェアおよびスパイウェア / グレイウェアによる脅威を、グローバル IT コミュニティに対する危険度から Very Low、Low、Medium、または High とレーティング
- **White papers**：「*The Real Cost of a Virus Outbreak*」または「*The Spyware Battle—Privacy vs. Profits*」という見出しのセキュリティ概念を説明したドキュメントへのリンク
- **Test files**：Trend Micro InterScan for Cisco CSC SSM をテストするためのテスト ファイル、およびテストの実施手順
- **Webmaster tools**：Webmasters に関する無料の情報およびツール
- **TrendLabs**：ISO 9002 認定の、ウィルス調査および製品サポート センターである TrendLab に関する情報

CSC SSM Syslog の概要

CSC SSM 関連の syslog メッセージには 13 種類あります。この項では、メッセージごとに解説します。

SSM アプリケーションのミスマッチ [1-105048]

エラーメッセージ　`%ASA-1-105048: (unit) Mate's service module (application) is different from mine (application)`

説明　フェールオーバー プロセスで、アクティブ ユニットとスタンバイ ユニットのサービス モジュール間で、異なるアプリケーションが動作していることが検出されました。複数のサービス モジュールが使用されている場合、2 種類のフェールオーバー ユニットの間に互換性はありません。

unit：プライマリまたはセカンダリ。

application：InterScan Security Card などのアプリケーションの名前。

推奨処置　フェールオーバーを再度イネーブルにする前に、両ユニットに同一のサービス モジュールがインストールされていることを確認してください。

CSC カードの障害のためにトラフィックが破棄された [3-421001]

エラーメッセージ　`%ASA-3-421001: TCP|UDP flow from interface_name:ip/port to interface_name:ip/port is dropped because application has failed.`

説明　CSC SSM アプリケーションの障害のためにパケットが破棄されました。デフォルトでは、このメッセージは、10 秒に 1 回しか表示されないように制限されています。

interface_name：インターフェイス名。

IP_address：IP アドレス。

port：ポート番号。

application：CSC SSM が現在のリリースでサポートされている唯一のアプリケーションです。

推奨処置　すぐにサービス モジュールの問題を調査してください。

適用外のトラフィックをスキップする [6-421002]

エラーメッセージ　`%ASA-6-421002: TCP|UDP flow from` *interface_name*`:`*IP_address*`/`*port* `to` *interface_nam*`:`*IP_address*`/`*port* `bypassed` *application* `checking because the protocol is not supported.`

説明　サービス モジュールで使用するプロトコルがスキャンされないために、サービス モジュールのセキュリティ チェックの接続がバイパスされました。たとえば、CSC SSM は TELNET トラフィックのスキャンには適用されません。ユーザが TELNET トラフィックをスキャンするように設定している場合は、トラフィックがスキャン サービスをバイパスします。デフォルトでは、このメッセージは、10 秒に 1 回しか表示されないように制限されています。

IP_address：IP アドレス。

port：ポート番号。

interface_name：ポリシーが適用されているインターフェイス名。

application：CSC SSM が現在のリリースでサポートされている唯一のアプリケーションです。

推奨処置　サービス モジュールでサポートされているプロトコルのみを含めるように、設定を変更する必要があります。

無効なカプセル化によって ASDP パケットが破棄された [3-421003]

エラーメッセージ　`%ASA-3-421003: Invalid data plane encapsulation.`

説明　サービス モジュールで挿入されたパケットには、正しいデータ プレーン ヘッダーがありませんでした。シスコ専用プロトコルに準拠するデータ バックプレーンで交換されるパケットは、ASDP と呼ばれます。適切な ASDP ヘッダーのないパケットは破棄されます。

推奨処置　**capture** *name* **type asp-drop** [**ssm-asdp-invalid-encap**] コマンドを実行して有害なパケットをキャプチャし、Cisco TAC にお問い合わせください。

パケットを挿入できない [7-421004]

エラーメッセージ　`%ASA-7-421004: Failed to inject {TCP|UDP} packet from` *IP_address*`/`*port* `to` *IP_address*`/`*port*

説明　セキュリティ アプライアンスは、サービス モジュールで指示されたパケットを挿入できませんでした。これは、セキュリティ アプライアンスがすでに解放されたフローにパケットを挿入しようとして発生した可能性があります。

IP_address：IP アドレス。

port：ポート番号。

推奨処置　この状態は、セキュリティ アプライアンス がその接続テーブルをサービス モジュールに依存せず、独自に維持しているために発生した可能性があります。通常は、これによって問題は発生しません。セキュリティ アプライアンス のパフォーマンスに影響が生じた場合は、Cisco TAC にお問い合わせください。

アカウント ホスト数がライセンスの上限に近づいている [6-421005]

エラーメッセージ　`%ASA-6-421005: interface_name:IP_address is counted as a user of application`

説明　ホストがライセンスの上限に近づいているとカウントされました。指定されたホストは *application* のユーザであるとカウントされました。午前 0 時に、ライセンス検証のために、過去 24 時間分のユーザの合計数が計算されます。

interface_name：インターフェイス名。

IP_address：IP アドレス。

application：CSC SSM が現在のリリースでサポートされている唯一のアプリケーションです。

推奨処置　処置は不要です。ただし、全体のカウント数が購入したユーザ ライセンス数を上回る場合は、ライセンスのアップグレードについてシスコにお問い合わせください。

日単位のノード カウント [5-421006]

エラーメッセージ　`%ASA-6-421006: There are number users of application accounted during the past 24 hours.`

説明　過去 24 時間に *application* を使用したユーザの合計数を特定します。このメッセージは、サービス モジュールが提供するサービスを使用したホストの合計数を算出するために、24 時間ごとに生成されます。

推奨処置　処置は不要です。ただし、全体のカウント数が購入したユーザ ライセンス数を上回る場合は、ライセンスのアップグレードについてシスコにお問い合わせください。

CSC カードの障害のためにトラフィックが破棄された [6-421007]

エラーメッセージ　`%ASA-3-421007: TCP|UDP flow from interface_name:IP_address/port to interface_name:IP_address/port is skipped because application has failed.`

説明　このメッセージは、サービス モジュール アプリケーションに障害が発生し、フローがスキップされた場合に生成されます。デフォルトでは、このメッセージは、10 秒に 1 回しか表示されないように制限されています。

IP_address：IP アドレス。

port：ポート番号。

interface_name：ポリシーが適用されているインターフェイス名。

application：CSC SSM が現在のリリースでサポートされている唯一のアプリケーションです。

推奨処置　すぐにサービス モジュールの問題を調査してください。

新しいアプリケーションが検出された [5-505011]

エラーメッセージ　%ASA-5-505011: Module in slot *slot*, application detected *application*, version *version*.

説明　新しいアプリケーションが 4GE SSM 上に検出されました。このメッセージは、システムのブート時、4GE SSM のブート時、または 4GE SSM の新規アプリケーションの起動時に生成される可能性があります。

slot：アプリケーションが検出されたスロット。

application：検出されたアプリケーションの名前。

version：検出されたアプリケーションのバージョン。

推奨処置　記述されたアクティビティが正常または正常と予期される場合は、処置は不要です。

アプリケーションが停止した [5-505012]

エラーメッセージ　%ASA-5-505012: Module in slot *slot*, application stopped *application*, version *version*

説明　このメッセージは、アプリケーションが停止したか、4GE SSM から削除されるたびに生成されます。4GE SSM がアプリケーションをアップグレードしたか、4GE SSM 上のアプリケーションが停止またはアンインストールされた場合に発生する場合があります。

slot：アプリケーションが停止したスロット。

application：停止したアプリケーションの名前。

version：停止したアプリケーションのバージョン。

推奨処置　アップグレードが 4GE SSM で実行されなかったか、アプリケーションが予期せずに停止またはアンインストールされた場合は、4GE SSM のログを確認して、アプリケーションが停止した原因を特定してください。

アプリケーションのバージョンが変更されている [5-505013]

エラーメッセージ　%ASA-5-505013: Module in slot *slot* application changed from: *application* version *version* to: *newapplication* version *newversion*.

説明　このメッセージは、アップグレード後など、アプリケーションのバージョンが変更されるたびに生成されます。これはアプリケーションのソフトウェア アップグレードがモジュールで完了すると発生します。

slot：アプリケーションがアップグレードしたスロット。

application：アップグレードしたアプリケーションの名前。

version：アップグレードしたアプリケーションのバージョン。

slot：アプリケーションがアップグレードしたスロット。

application：アップグレードしたアプリケーションの名前。

version：アップグレードしたアプリケーションのバージョン。

newapplication：新規アプリケーションの名前。

newversion：新規アプリケーションのバージョン。

推奨処置　アップグレードが予期されていることと、新規バージョンが正しいことを確認します。

データ チャネルの通信障害 [3-323006]

エラーメッセージ　`%ASA-3-323006: Module in slot slot experienced a data channel communication failure, data channel is DOWN.`

説明　このメッセージは、データ チャネル通信に障害が発生して、システムが 4GE SSM にトラフィックを転送できなかったことを示します。この障害がフェールオーバー ペアのアクティブなアプライアンスで発生すると、フェールオーバーがトリガーされます。また、通常は 4GE SSM に送信される、設定済みのフェール オープンまたはフェール クローズのポリシーが強制的に実行されます。このメッセージは、システム モジュールと 4GE SSM との間で、セキュリティ アプライアンスのデータプレーンを介した通信上の問題が発生するたびに生成されます。これは 4GE SSM が停止、リセット、または削除されると発生します。

slot：障害が発生したスロット。

推奨処置　このメッセージが 4GE SSM のリロードまたはリセットの結果ではなく、また、4GE SSM のステータスが UP に戻った後に、対応するメッセージ 5-505010 が表示されない場合、**hw-module module 1 reset** コマンドでモジュールのリセットが必要な場合があります。

データ チャネルの通信は正常 [5-505010]

エラーメッセージ　`%ASA-5-505010: Module in slot slot data channel communication is UP.`

説明　このメッセージは、データ チャネルの通信が DOWN 状態から回復するたびに生成されます。このメッセージは、チャネル通信が正常に動作していることを示します。データ チャネル通信の失敗後、回復するとこのメッセージが表示されます。

slot：データ チャネル通信が確立されたスロット。

推奨処置　直前にデータ チャネル通信障害（メッセージ 3-323006）が発生した結果を受けこのメッセージが生成されたのでなければ、処置は不要です。通信障害の場合は、4GE SSM のメッセージを確認して、通信障害の原因を判定してください。

Cisco TAC にお問い合わせになる前に

Technical Assistance Center (TAC) にお問い合わせになる前に、マニュアルやオンライン ヘルプに必要な回答が記載されていないか確認してください。マニュアルや Knowledge Base を調べても回答が見つからない場合は、問題を効率良く解決するために、次の情報をお手元に用意してください。

- 製品のアクティベーション コード（複数の場合もあります）
- 製品のバージョン番号
- パターン ファイルおよびスキャン エンジンのバージョン番号
- ユーザ数
- エラー メッセージを受信した場合はその正確な文面
- 問題の発生手順

詳細については、P.-xv の「テクニカル サポート」を参照してください。