IDS 4.0/AIP-SSM/IPS 5.0 以降に関する FAQ

目次

概要

このドキュメントでは、Cisco Secure Intrusion Detection System（IDS）4.0、Advanced Inspection and Prevention Security Services Module（AIP SSM）、および Cisco Intrusion Prevention System（IPS）5.0 以降に関連する、最もよくある質問（FAQ）に回答しています。

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

IDS 4.0

Q. IDS MC と SecMon を新しいサーバにインストールしたので、古いサーバから新しいサーバにすべての設定（ユーザ、デバイスなど）をインポートしようとしています。 どうすればよいでしょうか。

A. これを行う最も簡単な方法は、新しい VMS サーバを起動し、この新しいボックスでセンサーを検出することです。

注: センサーを追加する場合は、手動で追加しないでください。 [検出設定] ボックスをオンにします。

センサーが検出されたら、それを SecMon にインポートします。 すべての設定は、センサーに保存されます。 シグニチャの設定やフィルタなどについては、新しいサーバを構築した後に作業を行います。 IDS MC は必ず、最新のシグニチャにアップデートしてください。

Q. IDS-4215 が、IDS リカバリ パーティションをアップグレードしようとしたときに [idsPackageMgr: invalid argument] エラー メッセージを受信します。 この問題を解決するには、どうすればよいですか。

A. これは、製造上の問題です。 一部のお客様は、悪い状態のベース イメージ（4.0）の IDS 4215 を受信しています。 次の手順を実行します。

1. リカバリ パーティション イメージ（登録ユーザ専用）をダウンロードします。
2. CLI を使用してリカバリ パーティション イメージのアップグレードを適用します。
   ```
   sensor#configure terminal sensor(config)#upgrade METHOD://USERNAME@SERVER/PATH/ IDS-4215-K9-r-1.1-a-4.1-1-S47.tar.pkg
   ```

3. リカバリ パーティション イメージが適用されたら、4215 が、正常に動作する 4.1(1) 4215 ベースに復元されます。 `sensor(config)#recover application-partition`

Q. 4.1(4) S99 から 4.1(4) S100 など、2 桁から 3 桁（S100 以降など）のシグニチャ レベル パッケージにアップグレードすると、自動アップデート機能に障害が発生します。 これはどのように解決すればよいですか。

注: Cisco VMS および CLI のお客様には、この問題は発生しません。

この問題の原因は、ファイル名が解析されたときに使用されるソートのロジックです。 このロジックでは、数字でのソートが必要な場合でも英数字ソートが実行されます。 回避策は、S100 以降などの 3 桁のシグニチャ レベルのパッケージにアップグレードする場合は、CLI（または VMS）を使用することです。 これを完了すると、自動アップデートが再び機能し始めます。 詳細については、Cisco Bug ID CSCef07999（登録ユーザ専用）を参照してください。

Q. [Authentication token manipulation error.] エラー メッセージの意味は何ですか。

A. この問題を解決するには、デフォルトのパスワード（cisco）を 2 回使用した後、設定モードからパスワードを変更します。 IDS では、デフォルトのパスワードを 2 回入力する必要があります。

次に、例を示します。

```
login:cisco
Password:cisco
Enter current password:cisco
Enter new password: ***
Re-enter new password: ***
```

Q. スイッチから IDSM を削除する方法を教えてください。

A. モジュールは、電源を切断した後で削除する必要があります。 次の手順を実行します。

1. センサーの CLI から **reset powerdown** コマンドを発行します。
2. センサーのシャットダウンが完了したら、スイッチ CLI から、**no power enable module (module_number)** コマンド（Cisco IOS の場合）または **set module power down (module_number)** コマンド（CatOS の場合）を発行します。
3. ブレードの shutdown ボタンを押します。
4. 物理的にシャーシの電源を落とします。 ステータス ライトが緑色に長く点灯したら、モジュールを安全に削除できます。

IPS 5.0 以降

Q. 回避を設定していますが、シグニチャにブロッキングを設定する方法がよくわかりません。 ホストのブロッキングと接続のブロッキングの違いは何ですか。

A. ホストのブロッキングは、その発信元アドレスからのすべてのパケットをブロックします。 接続のブロッキングは、発信元と宛先の IP/ポートに基づいて接続を 1 つだけブロックします。 PIX は、わずかに異なる方法で機能します。 自動回避の場合は、センサーが発信元 IP、宛先 IP、発信元ポート、および宛先ポートを送信します。 PIX は、その IP アドレスから送信されるすべて

のパケットをブロックします。 追加情報を使用して、PIX は、その 1 つの接続を接続テーブルから削除します。 接続が接続テーブルから削除されていない場合、理論的には、回避が適用後にすぐに削除されると、元の接続がタイムアウトされていないことがあり得ます。 この場合は、攻撃者が元の接続への攻撃を続行できます。 テーブルから接続を削除すると、回避の削除後は確実に、元の接続を使用して攻撃を続行できなくなります。 センサーは、1 つの接続を PIX で回避できません。PIX では、shun コマンドを使用して 1 つの接続を回避することをサポートしていないためです。 PIX shun コマンドは、追加の接続情報が提供されているかどうかにかかわらず、発信元アドレスを回避します。

Q. [Error: **Could not restart the network services. Fatal Error has occurred. Node MUST be rebooted to enable alarming]** エラー メッセージの意味は何ですか。

A. このエラーは、デフォルト ゲートウェイが正しくないことを意味しているか、または IP、ネットマスク、デフォルト ゲートウェイのいずれかが正しくないことを意味する一般的なエラー メッセージです。 メッセージの重大な部分は、最初に障害が発生した後に以前の設定が適用され、それが失敗したことを意味します。 センサーは ifconfig および route コマンドを発行し、そのいずれかまたは両方が失敗します。

Q. 自動アップデートが失敗し、[mainApp[343] Cid/E errSystemError http error response:500] というエラー メッセージが表示されます。 このエラー メッセージはどういう意味ですか。

A. この問題は、自動アップデート機能が、偶数時にダウンロードするように設定されているために機能しないことである可能性があります。 自動アップデートをランダムな時間に設定してみてください。 8 の小さなオフセットまたは夜間の時間でも、この問題が修正される場合があります。

通常、この問題は解決され、正時でない時間に取得時間を変更した場合は [Error: `http error response`: 500] エラー メッセージが表示されます。

注: IPS はシグニチャの自動アップデートに失敗すると、次のエラー メッセージを返します。

```
AutoUpdate exception: HTTP connection failed [1,110] name=errSystemError
```

この問題を解決するには、次の項目を確認します。

- センサーが Cisco.com に到達するのをファイアウォールが妨げているかどうかを確認します。
- ルーティングに問題があるかどうかを確認します。
- ダウンストリーム デバイス用のゲートウェイ デバイスで NAT が適切に設定されているかどうかを確認します。
- ユーザ クレデンシャルが正しいかどうかを確認します。
- アップデートの開始時刻を奇数時に変更します。

Q. [Error: **execUpgradeSoftware : AnalysisEngine is currently busy and unable to process this update. Please wait several minutes before attempting update again]** エラー メッセージの意味は何ですか。

A. この問題を解決するには、センサーをリロードするか、センサーのイメージを変更してみてください。

Q. エラー メッセージ [Cid/W Warning - DNS or HTTP proxy is required for global correlation inspection and reputation filtering but no DNS or proxy servers are defined.Add an HTTP proxy server or DNS server in the 'host' service configuration] を解決する方法を教えてください。

A. この問題を解決するには、次の手順を実行します。

- グローバル相関を無効にします。
- プロキシ/dns 設定を追加します。

Q. グローバル相関の状態の問題により IPS が受信する、次のエラーの解決方法を教えててください。 [23Jan2010 15:50:39.831 38.001 collaborationApp[655] rep/E A global correlation update failed: **Failed to open a TLS connection to HTTP server at X.X.82.127:443 :** TLS connection failed] および [collaborationApp[459] rep/E A global correlation update failed: **Failed download of ibrs/1.1/drop/default/1296529950 :** URI does not contain a valid ip address]

A. ポートの問題のために IPS がインターネットに接続できません。たとえば、パスのファイアウォールでインターネット アクセス用の正しいポートが開かれていないか、NAT に問題がある可能性があります。

グローバル相関が完全に機能するためにセンサーは、最初に https update-manifests.ironport.com を介して接続してユーザを認証し、次に HTTP 接続で GC のアップデートをダウンロードします。 センサーが HTTP (updates.ironport.com) からダウンロードするファイルは、グローバル相関で使用されるレピュテーション データです。 https update-manifests.ironport.com は X.X.82.127 アドレスに解決される必要がありますが、アクセスするインターネットに応じて、http updates.ironport.com の IP アドレスが変わる場合があります。 そのため、IP アドレスを確認する必要があります。 URL フィルタリングが有効な場合は、IPS がインターネットに接続できるように、URL フィルタの IPS 管理インターフェイス IP の例外を追加します。

次のエラーは、前の GC のアップデートが破損している場合に発生します。

```
collaborationApp[459] rep/E A global correlation update failed: Failed download of
ibrs/1.1/drop/default/1296529950 : URI does not contain a valid ip address
```

この問題は、通常、GC サービスの電源をオフにした後、オンにすると修正できます。 IDM で [Configuration] > [Policies] > [Global Correlation] > [Inspection/Reputation] を選択し、[Global Correlation Inspection] ([On] になっている場合は [Reputation Filtering] も) を [Off] にします。そして、変更を適用し、10 分待って、機能をオンにして監視します。

Q. [A global correlation update failed: **openConnection: Caught IpAddrException badAddrString. Unable to use the Global Correlation HTTP proxy and DNS settings. Verify connection and try again.]** エラー メッセージを、レピュテーション アップデートの失敗」のカテゴリで受信します。 この問題を解決するにはどうすればよいですか。

A. 次の項目を確認してください。

- グローバル相関の機能が動作するには、有効な IPS ライセンスが必要です。
- グローバル相関の機能が動作するには、HTTP プロキシ サーバまたは DNS サーバが設定されていることが必要です。

- グローバル相関のアップデートはセンサー管理インターフェイスを介して実行されるため、ファイアウォールで tcp 443/80 および udp 53 トラフィックを許可する必要があります。
- センサーがグローバル相関機能をサポートすることを確認します。 この機能が不要な場合は、IDM でグローバル コラボレーション機能を無効にしてください。[Configuration] > [Policies] > [Global Correlation] > [Inspection/Reputation] を選択し、[Global Correlation Inspection] ([On] になっている場合は [Reputation Filtering] も) を [Off] にします。

Q. グローバル相関の問題に対して IPS が受信する [A global correlation update failed: `openConnection`: Caught IpAddrException badAddrString] エラーを解決する方法を教えてください。

A. グローバル相関 (GC) を使用する場合は、その名前解決が機能することを確認してください。たとえば、DNS が到達可能であることを確認します。 また、ポート 53 をブロックするファイアウォールがあるかどうかを確認します。 そうでない場合は、GC の機能をオフにすると、このメッセージが表示されなくなります。

Q. ブラウザーから IME を起動すると受信する [Exception when initializing the connection to MySQL] エラー メッセージを解決する方法を教えてください。

A. この問題は、通常、サポートされていないオペレーティング システム (Windows 7 など) で IME を実行しようとすると発生します。

Q. IDM が受信する [Title: `IDM on 88-nsmc-c1 Vendor: Cisco Systems, Inc. Category: Launch File Error JAR resources in JNLP file are not signed by same certificate`] または [Error connecting to sensor, Failed to create sensor x.x.x.x:443 exiting idm] というエラーを解決する方法を教えてください。これは、アプリケーションの起動時に発生します。

A. この問題を解決するには、ブラウザ キャッシュをクリアしてください。

Q. GUI を使用する場合、IPS で非対称モードを設定できますか。

A. バージョン 6.0 では、IPS での非対称モードは、CLI を使用してのみ設定可能で、GUI では使用できません。 しかし、バージョン 6.1 では、この機能を GUI でも使用できます。

Q. どうすれば、IPS センサーでの遅延の問題を解決できますか。

A. この問題を解決するには、センサーが状態をフローと同期し、両方向を必要としないこれらのエンジンの検査を維持できるように、非対称モード処理を有効にします。 次の設定を使用ます。

```
IPS_Sensor#configure terminal IPS_Sensor(config)#service analysis-engine IPS_Sensor(config-ana)#virtual-sensor vs0 IPS_Sensor(config-ana-vir)#inline-TCP-evasion-protection-mode asymmetric
```

遅延の問題は、インライン拒否動作と拒否パケットが、VS0 のすべてのシグニチャに対して有効になっている場合に発生します。 すべてのシグニチャを有効にすると、通過するすべてのパケットを IPS が検査するため、遅延が発生します。 遅延の問題を解決するには、ネットワーク トラフィック フローに従って、必要な特定のシグニチャのみを有効にすることをお勧めします。

Q. AIP-SSM は Skype のブロックに役立ちますか。

A. 残念ながら、PIX/ASA は Skype トラフィックをブロックできません。 Skype には、ダイナミック ポートとネゴシエートし、暗号化されたトラフィックを使用する機能があります。 トラフィックが暗号化されているので、検索するパターンが存在せず、事実上 Skype を検出するのは不可能です。

最終的には、Cisco IPS（Intrusion Prevention System）/AIP SSM を使用できます。 これには、バージョンを同期させるために Skype サーバに接続する Windows Skype Client を検出できるいくつかの署名があります。 これは通常はクライアントが接続を開始するときに行われます。 センサーが最初の Skype 接続をピックアップするときに、そのサービスを誰が使用しているのかを発見でき、その IP アドレスから開始されたすべての接続をブロックすることができます。

Q. なぜ、IPS では、センシング インターフェイスがフラップしたり、頻繁にダウン状態になったりするのですか。

A. シグニチャ アップデートおよび再設定中には、sensorApp がアップデートの新しいシグニチャを処理するため、パケットの処理を停止します。 ネットワーク ドライバは、sensorApp が停止したことを検出し、バッファからの新しいパケットをプルします。 そして、ネットワーク ドライバはさまざまな処理を行いますが、これは、設定およびセンサー モデルによって異なります。

無差別インターフェイス - インターフェイスでリンクを停止し、sensorApp がモニタリングを再開すると、リンクを再起動します。

インライン インターフェイスまたはインライン VLAN ペア - バイパス設定によって異なります。

- **Bypass Auto**：ドライバはリンクを動作中のままにし、分析せずにパケットを通過させます。そして、sensorApp がモニタリングを再開すると、sensorApp を通過するパケット送信に戻ります。
- **Bypass Off**：ドライバは、無差別モードの場合と同様にインターフェイスでリンクを停止し、sensorApp がモニタリングを再開すると、リンクを再起動します。

したがって、センサー アプリケーションがバッファからパケットをプルしない場合、ドライバはインターフェイスをダウン状態にすることができます。これは、パケットを処理するように設定されているインターフェイスがないために発生する可能性があります。

次の口グは、センシング インターフェイスがフラップすると生成されます。

```
28Jun2011 09:03:09.483 6050.885 interface[409] Cid/W errWarning Inline
    databypass has started.
28Jun2011 09:03:13.639 4.156 interface[409] Cid/W errWarning Inline databypass
    has stopped.
28Jun2011 09:19:23.922 970.283 interface[409] Cid/W errWarning Inline databypass
    has started.
28Jun2011 09:19:27.486 3.564 interface[409] Cid/W errWarning Inline databypass
    has stopped.
```

Q. IDS または Intrusion Prevention System（IPS）センサーでは、パスワードの履歴が保持されますか。

A. いいえ、センサーではパスワード履歴は保持されません。 パスワードが表示されることはありません。

Q. IDS または Intrusion Prevention System（IPS）センサーでは、syslog サーバによる口グの送信がサポートされますか。

A. いいえ。

Q. IPS でイベントを保存できる最大容量はどれくらいですか。

A. センサーのローカル イベントが保存されるのは 30 MB までで、この 30 MB の制限に達すると、それ自体に上書きされます。 この制限は設定できません。

Q. すべての着信または発信電子メールで foto[a-z]\.zip ファイルを検出するシグニチャを書き込む方法を教えてください。

A. STRING.TCP を使用して、添付ファイルを検出するシグニチャを記述します。 次の記述に似た部分を探してください。

```
Engine STRING.TCP
Enabled True
Severity informational
AlarmThrottle Summarize
CapturePacket False
Direction ToService
MinHits 1
Protocol =TCP
RegexString [Ff][Ii][Ll][Ee][Nn][Aa][Mm][Ee][=]["][Ff][Oo]
            [Tt][Oo][a-zA-Z][.][Zz][Ii][Pp]["]
ResetAfterIdle 15
ServicePorts 25
StorageKey =STREAM
```

Q. FTP クライアントのタイムアウトの設定方法を教えてください。

A. 次のコマンドを発行します。

```
configure terminal
service host
networkParams
ftpTimeout 300 <timeout is in seconds>
```

Q. iplog-status の開始時刻と終了時刻を読み取り可能な形式に変換する方法を教えてください。

A. この出力は、UNIX エポックから現在までの時間を 10 進数で表したものです。 UNIX Date/Time Calculator サイトにあるような UNIX エポック計算ツールを使用してください。 最初の 10 桁を入力します。これは、この計算ツールで使用できるのは秒単位までであり、IDS ではナノ秒単位で保存されるためです。 つまり、最後の 9 桁は削除されます。 この出力にある開始時間は、1084798479 = Mon May 17 12:54:39 2004 (GMT) に変換されます。

CLI で **iplog-status** と入力すると、次の出力を受信します。

```
"
Log ID:             138343946
IP Address:         xxx.xxx.xxx.xxx
Group:              0
Status:             completed
Start Time: 1084798479512524000 End Time: 1084798510136582000 Bytes Captured: 2833 Packets
Captured: 14 "
```

Q. IOException when try to get certificate: **java.security.cert.CertificateExpiredException]** 」というエラー メッセージが表示されます。 どうすれば、これを解決できますか

。

A. このエラー メッセージを解決するには、AIP-SSM にログインし、次の例のように、特権 EXEC モードで tls generate-key コマンドを発行します。

```
sensor#tls generate-key
```

注: コマンド tls generate-key を使用するこの解決方法で、AIP-SSM が IME に接続できない問題も解決されます。

Q. [IOException: `connection refused: connect. IME IME server is not responding.` Please check if it is running] エラー メッセージが、IME で IPS を追加すると表示されます。 どうすれば、この問題を解決できますか。

A. このエラー メッセージを解決するには、[Control Panel] > [Admin Tools] > [Services] を選択し、IME サービスを再起動します。

Q. IME に IPS センサーを追加すると、[Could not verify config username/password[IOEXception - connect timed out] エラー メッセージを受信します。 どうすれば、この問題を解決できますか。

A. これは、IME と IPS センサーの間で通信が正しく行われていないことを示します。 SDEE をブロックするソフトウェアがないことを確認してください。

Q. [Error response from IME server: `Unknown error (check log file in installation's log directory)]` 」というエラー メッセージが表示されます。 どうすれば、この問題を解決できますか。

A. このエラー メッセージを解決するには、IME に IPS を追加するときに、正しい IP アドレスをしていることを確認します。また、接続を妨げる可能性があるソフトウェア ファイアウォールが IME コンピュータで動作していないことも確認します。

Q. IDS または Intrusion Prevention System（IPS）センサーは、電子メール アラートを送信できますか。

A. IDS センサーには、それ自体で電子メール アラートを送信する機能はありません。 IDS と併用しているセキュリティ モニタには、イベント ルールがセンサーによってトリガーされたときに電子メール通知を送信する機能があります。

セキュリティ モニタで電子メール通知を設定する方法の詳細については、「電子メール通知の設定」を参照してください。

Cisco IPS Manager Express（IME）は、イベント ルールが Cisco IPS センサーによってトリガーされたときに電子メール通知メッセージ（アラート）を送信するように設定できます。 詳細については、「IPS 6.X 以降： IME を使用した電子メール通知の設定例」を参照してください。

Q. Error: `Cannot communicate with mainApp (getVersion).` エラー メッセージが、センサーに接続しようとすると表示されます。 どうすれば、この問題を解決できますか。

A. この問題を解決するには、センサーをリブートします。

Q. 警告 [**Insufficient resources available to combine all currently active custom regexes. Some alerts will not fire. Consider retiring signatures until this message no longer occurs.]** エラーメッセージが、センサーでのシグニチャ調整時に表示されます。 どうすれば、この問題を解決できますか。

A. この問題を解決するには、使用中でないシグニチャを廃棄します。また、regex を持つお客様のシグニチャの数を減らすことも必要です。 さらに、**?** および **+** というメタ文字を regex で使用することもお勧めします。

Q. Cisco Intrusion Prevention System (IPS) センサーで遅延の問題が発生する理由は何ですか。 どうすれば、この問題を解決できますか。

A. 遅延の問題は、非対称ルーティングが原因で発生する可能性があります。 この問題を解決するには、シグニチャ 1330 を無効にしてみてください。

Q. Cisco Intrusion Prevention System (IPS) センサーで、SSHv1 をディセーブルにして、SSHv2 のみをイネーブルにしておくことはできますか。

A. SSHv1 をディセーブルにして、SSHv2 のみをイネーブルにすることはできません。 SSHv1 および SSHv2 の両方がイネーブルにされ、個別にディセーブルにすることはできません。

Q. [Error: **An error occurred at the sensor during the update, sensor message = The update requires 115000 KB in /usr/cids/idsRoot/var, there are only 110443 KB available.]** メッセージが、センサーをバージョン 4.1(5) にアップグレードすると表示されます。 どうすれば、この問題を解決できますか。

A. このエラー メッセージは、センサーのメモリ不足が原因で発生します。

この問題を解決するには、次の手順を実行します。

1. サービス アカウントにログインし、ルートになります。
2. 以下に示すように、次のディレクトリを削除します。 `# rm -rf /usr/cids/idsRoot/var/updates/files/S69`
   ```
   # rm -rf /usr/cids/idsRoot/var/updates/files/common
   # rm /usr/cids/idsRoot/var/virtualSensor/*
   # rm /usr/cids/idsRoot/var/.tmp/*
   ```
3. ここでセンサーをアップグレードします。 詳細については、Cisco Bug ID CSCsb81288 (登録ユーザ専用) を参照してください。

Q. ASA でログに [mainApp[396] cplane/E Error - accept() call returned -1] エラーメッセージが生成されます。 このエラーはどうすれば解決しますか。

A. [mainApp[396] cplane/E Error - accept() call returned -1] エラー メッセージは、Web サーバがファイルを読み取ることができず、TLS 接続が存在するときにファイル記述子を生成する accept() プログラムが失敗したことを示しています。 ただし、このファイルは、通常の動作には必要ではありません。 したがって、問題はありません。

Q. [tls/W errTransport WebSession:: sessionTask TLS connection exception: handshake incomplete] エラー メッセージの解決方法を教えてください。

A. このエラー メッセージは、モジュールで証明書が有効でなくなったことを示します。 この問題を解決するには、次の手順を実行します。

1. 次の手順で、CLI から証明書を再生成します。センサーのコマンドラインにログインします。**tls generate** コマンドを発行し、Enter キーを押します。 表示されたフィンガープリントに注意してください。
2. 次の手順で、新しい証明書を IME にプルします。IME を開き、ホーム ページにあるリストでセンサー名を見つけます。センサーを右クリックし、[Edit] をクリックします。[Edit Device] 画面が表示されたら、[OK] をクリックします。 センサーの時間を取得できないことに関する警告をバイパスします。新しいセキュリティ証明書（今、生成した）の確認を促されます。 フィンガープリントが一致することを確認し、[Yes] をクリックします。数秒後に、センサーの [Event Status] に再び [Connected] が表示されます。

Q. IPS にログインしようとすると、次のエラー メッセージが表示されます。[errSystemError-ct-sensorAPP.450 not responding, clientpipe failed.] このエラーを解決するにはどうすればよいのですか。

A. このエラーを解決するには、**reset** コマンドを使用して IPS をリブートします。

Q. AIP-SSM の時間が Cisco Adaptive Security Appliance（ASA）の時間と異なります。 どうすれば、この問題を解決できますか。

A. この問題を解決するには、NTP サーバを使用して、Cisco Adaptive Security Appliance（ASA）と AIP-SSM の時間を同期します。

詳細については、「IPS センサーでの NTP の設定」を参照してください。

Q. 複数の仮想センサーを AIP-SSM に適用する方法を教えてください。

A. AIP-SSM の仮想センサーは、インターフェイスごとに適用できません。これは、AIP-SSM のインターフェイスは 1 つだけであるためです。 複数の仮想センサーを作成する場合は、このインターフェイスを 1 つの仮想センサーにだけ割り当てる必要があります。 他の仮想センサーのインターフェイスを指定する必要はありません。

仮想センサーの作成後に、**allocate-ips** コマンドを使用して、センサーを Adaptive Security Appliance（ASA）のセキュリティ コンテキストにマッピングする必要があります。 複数のセキュリティ コンテキストを複数の仮想センサーにマッピングできます。 詳細については、「AIP-SSM の設定」の「*Adaptive Security Appliance コンテキストへの仮想センサーの適用*」セクションを参照してください。

Q. AIP-SSM でサポートされる仮想センサーの最大数はいくつですか。

A. 最大 4 台の仮想センサーをサポートできます。

Q. SSH または IDM を使用して IPS にログインしている場合は、

RADIUS/TACACS+ サーバに対して管理ユーザを検証するように IPS 4240/IDSM/IDSM2 を設定することができますか。

A. これは、TACACS+ サーバでは不可能ですが、RADIUS は IPS 7.0.(4)E4 からサポートされています。 詳細については、『Cisco Intrusion Prevention System 7.0(4)E4 リリースノート』の「*新機能と変更の情報*」および「*製薬と制限*」の各セクションを参照してください。 また、設定例については、「IPS 7.X： RADIUS サーバとして ACS 5.X を使用したユーザ ログイン認証の設定例」を参照してください。

Q. IPS 機能のライセンスの有効期限が切れると、どのような影響がありますか。

A. ライセンスの期限切れによるセンサーへの影響は、シグニチャのアップデートが停止されることだけです。

Q. IPS シグニチャ アップデートは、サービスまたはネットワーク接続に影響を及ぼしますか。

A. いいえ。 IPS シグニチャ アップデートは、サービスとネットワーク接続のどちらにも影響を及ぼしません。

Q. IPS モジュールを最新のシグニチャで自動的に更新するために入力する必要のある完全 URL は何ですか。

A. IPS モジュールを最新のシグニチャで自動的にアップデートするために必要なリンクは、https://198.133.219.25/cgi-bin/front.x/ida/locator/locator.pl です。

IPS モジュールの更新を完了するには、Cisco ユーザ ID とパスワードを使用する必要があります。

注: コードの 6.x トレインでは、Cisco.com からの自動アップデートはサポートされていません。 シグニチャ ファイルを手動でダウンロードし、センサーに適用する必要があります。 6.x コードには、自動アップデートの機能があります。 ただし、この機能を使用できるのは、ローカル ファイル サーバからだけです。このサーバにも、シグニチャ ファイルを手動でダウンロードする必要があります。

Q. IPS センサーには、X11 ポート フォワーディング セッションの乗っ取りへの脆弱性がありますか。

A. いいえ。 脆弱性がない理由は、次のとおりです。

- センサーには、X11 ライブラリがありません。 そのため、乗っ取られるセッションはありません。
- X11 ポート フォワーディングは、SSH 設定では有効になっていません。
- IPv6 は、センサーのカーネルにコンパイルされていません。 これは、脆弱性を利用するために必要なことです。

Q. ASA が多数の警告および攻撃ログを表示するときに、AIP-SSM がログを表示しないのは、なぜですか。

A. これは、ASA が何かをブロックしている場合は、検査が重複しないように、それを IPS に渡さないためです。 したがって、ASA と IPS で、重複するログは表示されません。

Q. ユーザが S518 シグニチャ セットを配置した後に [invalidValue: Editng string-xl-tcp sig XXXX has NO effect in this version] エラー メッセージが表示されます。 これは、なぜですか。

A. 完全なエラー メッセージは、次のとおりです。

```
evError: eventId=1284051856322985135 vendor=Cisco severity=warning
  originator:
    hostId: vbintestids03
    appName: sensorApp
    appInstanceId: 700
  time: offset=-240 timeZone=GMT-05:00 1286305251136551000
errorMessage: name=errWarning invalidValue:Editing string-xl-tcp
sig 21619 has NO effect
```

この問題は、string-xl-tcp または string-tcp-xl エンジンがハードウェアでサポートされていないために発生します。 詳細については、『IPS エンジン E4 リリース ノート』を参照してください。

Q. 自動アップデート機能を使用して ASA-SSM-10 でシグニチャを自動的に更新すると、次のエラー メッセージが表示されます。 [No installable auto update package found on server status=true.] 問題を解決するには、どうすればよいですか

A. 次の出力は、完全なエラー メッセージです。

```
autoUpgradeServerCheck:
    uri: https://XX.XX.XX.XX//cgi-bin/front.x/ida/locator/locator.pl
    packageFileName:
    result: No installable auto update package found on server  status=true
```

このエラーが生成されると、シグニチャは自動的にアップデートされません。これは、S479 より後のシグニチャ定義アップデートには E4 エンジンが必要であるためです。 これを解決するには、センサーを手動で 7.0(2) E4 にアップグレードする必要があります。

注: センサーは、自動的には E4 にアップグレードできません。7.0(2) が必要であり、センサーをリブートする必要があるためです。

Q. NIDS モジュールの IPS 5.0 の自動アップデート機能が動作していません。 問題を解決するには、どうすればよいですか

A. 次の出力は、完全なエラー メッセージです。

```
autoUpgradeServerCheck:
    uri: ftp://hfcu-inet01@192.168.1.12//ips-update/
    packageFileName:
    result: No installable auto update package found on server  status=true
```

この問題は、FTP サーバでの不適切なディレクトリ リスト表示形式が原因で発生します。 この問題を解決するには、既存の MS-DOS 形式のディレクトリ リスト表示から UNIX 形式のディレクトリ リスト表示に切替えてください。

ディレクトリ リスト表示設定を変更するには、[Start] > [Program Files] > [Administrative Tools] を選択して Internet Services Manager を開きます。 [Home Directory] タブに移動し、MS-DOS から UNIX にリスト表示スタイルを変更します。

Q. アップグレード中に IPS-4255 で [SensorApp fails in TcpRootNode:: expireNow()] エラー メッセージが表示されます。 この問題を解決するにはどうすればよいですか。

A. この問題は、分析エンジンの障害が原因で、Cisco Bug ID CSCtb39179（登録ユーザ専用）に記載されています。 この問題を修正するには、センサーをバージョン 7.0(4)E4 にアップグレードします。

Q. 新規ライセンスの購入後にライセンス アップデートを実行しようとすると、次のエラーがデバイスで報告されます。 **"[Failed to update license on sensor.] "[errExpiredLicense-The new license expire date is older than current license expire date.]** 問題を解決するには、どうすればよいですか

A. この問題は、受信したライセンス ファイルが無効な場合に発生します。 有効なライセンス ファイルを入手するには、登録ユーザとして Cisco.com にログインし、適切なライセンス ファイルをダウンロードします。 有効なライセンス ファイルを入手したら、センサーにインストールします。

新しいライセンス ファイルをインストールしてもエラーが表示される場合は、既存の無効なライセンス ファイルの問題である可能性があります。 この問題を解決するには、次の手順を実行して、既存の無効なライセンス ファイルを削除します。

1. サービス アカウント ユーザ名を入力して、サービス アカウントにログインします。サービス アカウントがない場合は、IPS コマンドラインを開き、コンフィギュレーション モードにして、次のコマンドを入力します。**username name privilege service password password**
```
ciscoasa# session 1
Opening command session with slot 1.

Connected to slot 1. Escape character sequence is 'CTRL-^X'.
login:
Password:

IPS#
IPS#conf t
IPS(config)# username name privilege service password password
```
2. サービス アカウントにログインしたら、**su** コマンドを入力して root に移動します（サービス アカウントと同じパスワードを使用します）。
3. /usr/cids/idsRoot/shared/ ディレクトリのファイルを削除します。**注:** host.conf ファイルは削除しないでください。**cd /usr/cids/idsRoot/shared/** コマンドを入力して共有ディレクトリに移動します。**ls** コマンドを入力して、ディレクトリにあるファイルを表示します。**rm file_name** コマンドを入力してファイルを削除します。**注:** host.conf ファイルは削除しないでください。
4. **/etc/init.d/cids restart** コマンドを入力してセンサーを再起動します。
5. 新しいライセンスをインストールします。

Cisco バグが、この動作に対処するために報告されています。 詳細については、CSCtg76339（登録ユーザ専用）を参照してください。

Q. [errorMessage: **IpLog 1712041197 terminated early due to lack of file handles.** name=ErrLimitExceeded] エラー メッセージの意味は何ですか。 この問題を解決するにはどうすればよいですか。

A. このエラーは、IP ロギングのパケット量が多すぎるために発生します。 この問題を解決するには、IP ロギング機能を無効にしてください。 IP ロギングの目的は、トラブルシューティングだけです。 シスコでは、すべてのシグニチャに対しては IP ロギングを有効にしないことをお勧めします。

Q. s550 から s551 にセンサーをアップデートすると、次のエラーが発生します。 [Cannot parse the current config for the component "signatureDefinition" and the instance "sig0".] 問題を解決するには、どうすればよいですか

A. この問題は、シグニチャ 23899.0 が原因で発生します。 詳細については、Cisco Bug ID CSCtn84552（登録ユーザ専用）を参照してください。

Q. センサーで、次のエラーが発生します。 `Error: autoUpdate successfully selected a package from the cisco.com locator service, however, package download failed:` Failed to receive the HTTP response.] 問題を解決するには、どうすればよいですか

A. autoUpdate をブロックしている URL フィルタリング、コンテンツ フィルタリング、またはプロキシ サーバがあるかどうかを確認します。 autoUpdate がブロックされていないことを確認し、提供されたユーザ クレデンシャルが正しいことも確認してください。

Q. バージョン 6.2(3)E4 で動作する IPS センサーで、次の XML エラー メッセージが表示されます。 `[errorMessage: IPS software attempted to write invalid XML data for (token).` Invalid XML character(s) were replaced with '*'.] 問題を解決するには、どうすればよいですか

A. この動作は、Cisco Bug ID CSCsq50873（登録ユーザ専用）で解決されています。 これは表面的な問題であり、受信される口グが多すぎることを除いては、運用上のオーバーヘッドは作成されません。 一時的な回避策は、センサーの NTP 関連の設定を削除することです。 根本的に解決するには、この不具合が修正されているバージョンにアップグレードします。

Q. クライアントが終了しているのに、IME ワークステーションが管理対象サーバに継続して接続するのはなぜですか。

A. IME は、2 つの Windows サービスと GUI クライアントとして動作します。 クライアントが終了したときに、2 つの Windows サービス（Cisco IPS Manager Express と MySQL-IME）は動作を続行し、管理対象センサーからイベントを収集し、ローカルの MySQL データベースに格納し続けます。 これにより、履歴レポートの作成が可能になります。

IME クライアントは、管理対象センサーへの単一の SDEE サブスクリプションを開き、後続のイベント取得アクティビティのために、それを再利用する必要があります。 IME ワークステーションから管理対象センサーへの継続する接続は正常な動作です。

Q. AIP-SSM モジュールは、SPAN ターゲットとして使用できますか。

A. いいえ。 AIP-SSM モジュールは、ASA インターフェイスを通過するトラフィック フローの監視だけに使用されるため、SPAN ターゲットとしては使用できません。

Q. IPS を E3 エンジンにアップグレードすると、CPU 使用率が高くなるのはなぜですか。

A. E3 エンジンの更新によって、IPS は、異なるアルゴリズムを使用してアイドル時間を管理し、パケットのポーリングのための時間を増やして遅延を減らします。 このように、増加した検査処理に対応して、使用率が上がることになります。 E3 で CPU を測定する適切な方法は、使用率ではなく、正しい CPU 使用率を示す**パケット負荷パーセンテージ**を使用することです。

Q. IPS アプライアンスのヘルス ステータス LED が赤で点滅しているのは、なぜですか。

A. これが発生する原因としては、CS-MARS、CSM、IEV、VMS-IDS/IPSMC などソフトウェアを実行するリモート管理ステーションの証明書が誤っていることが考えられます。この問題を解決するには、次の手順を実行します。

1. センサーの TLS 証明書をリモート管理ステーションに適用します。
2. 有効な DNS サーバを設定します。

Q. IPS によって、HTTP のトラフィックがインターフェイスの通過中に遅延しないようにする方法を教えてください。

A. 非対称モードで動作するようにセンサーを設定すると、問題が解決します。 非対称モード保護にセンサーを設定するには、次の手順を実行します。

1. [Configuration] > [Policies] > [IPS policies] に移動します。
2. **仮想センサー**をダブルクリックします。
3. **高度なオプション**に移動します。
4. 標準化モードで [Asymmetric mode protection] を選択します。
5. [OK] をクリックします。
6. 変更を有効にするために、装置をリブートします。

関連情報

- Cisco Secure Intrusion Prevention System に関するサポート ページ
- AIP-SSM のトラブルシューティング
- セキュリティ製品に関する Field Notice (CiscoSecure Intrusion Detection を含む)
- テクニカルサポートとドキュメント - Cisco Systems