Cisco Secure Intrusion Detection System (バージョン3.1およびそれ以前) FAQ

目次

概要

このドキュメントでは、以前 NetRanger と呼ばれていた Cisco Secure Intrusion Detection System (IDS) バージョン 3.1 以前に関する FAQ を記載しています。

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。

一般

Q. Cisco Secure IDS についての追加情報はどこにありますか。

A. Cisco Secure IDS の詳細については、製品ドキュメント全編を参照してください。

Q. IDS システム全体 (IDS センサー + IDS Management ソフトウェア) のシグニチャを更新するにはどうすればよいですか。

A. センサーと管理プラットフォームのシグニチャを個別にアップグレードする必要があります。管理ソフトウェアはセンサーから署名を学習できないため、管理ソフトウェアも更新する必要があることに注意してください。 各アプリケーションの最新のシグニチャ更新を、Cisco Secure Downloads (登録ユーザ専用) からダウンロードします。 同じ場所にある readme ファイルにアップグレード手順の説明が含まれています。

Q. シグニチャの完全なリストをどのように確認できますか

A. IDS シグニチャのリストは Cisco Secure Encyclopedia (登録ユーザ専用) から入手できます。

Q. UNIX IDS センサーとスタンドアロン センサーのユーザのデフォルト パスワードは何ですか。

A. UNIX IDS スタンドアロン センサーおよび IDS 管理ソフトウェアでは、ユーザ **netrangr** およ

び root のデフォルト パスワードは「attack」です。 **su コマンド**を発行して root ユーザになった場合、デフォルト パスワードは「attack」です。 Intrusion Detection System Module（IDSM）ブレードで、ユーザ名 **ciscoids** のデフォルト パスワードは「attack」です。

Q. Intrusion Detection System Module（IDSM）ブレードの設定をどのようにダンプできますか

A. 設定をアップロードするためにローカル FTP サーバが必要です。

1. ブレードの diag モードで次のコマンドを入力します。
   report systemstatus site *<ftp_target_ip_address>* **user** *<ftpusername>* **dir** *<directoryname>*
2. 「Continue generating the System Repor」と尋ねられた場合、続行するには **y** と入力します。
3. プロンプトが表示されたら、指定されたユーザの FTP パスワードを入力します。 プロセスが完了すると、プロセスが失敗したか、またはファイルが送信されたかを伝えるメッセージを受信します。

Q. IDS のインストールやアンインストール時に、ログ ファイルはどこにありますか

A. インストール/更新のログは次の場所にあります。

- Director のインストール ログは /var/adm/nrInstall.log にあります。
- センサー サービス パック更新のログは /usr/nr/sp-update/ にあります。
- シグニチャ更新のログは /usr/nr/sig-update/ にあります。

Q. PIX for IDS ではどんなシグニチャを使用できますか

A. IDS は PIX 6.0 以降でのみ使用可能です。 シグニチャは syslog メッセージ 400000 から 400051 までに含まれており、これらを Cisco Secure IDS シグニチャ メッセージといいます。 各シグニチャの詳細については、「PIX システム ログ メッセージ」を参照してください。

Q. シグニチャ更新がリリースされたとき、通知を受け取ることはできますか

A. Cisco Secure IDS 関連製品のニュースを電子メールで受信するには、Cisco IDS Active Update Notifications にサインアップします。

Q. IDS センサーを制御するにはどんなアプリケーションを使用できますか。また、各アプリケーションの違いは何ですか。

A. バージョン 3.1 よりも前では、管理オプションとして Cisco Secure Policy Manager（CSPM）または UNIX Director を使用できます。 この 2 つの主な違いは、CSPM が Windows Server 上の独立したアプリケーションとして動作するのに対し、UNIX Director は UNIX Solaris サーバの HP OpenView 上で実行されることです。 IDS 3.1 ではこれに加えて、PC にインストールされた IDS Event Viewer（IEV）を使用したり、バージョン 3.1 センサーに含まれる IDS Device Manager を使用して、センサーを管理することもできます。 Device Manager は、センサーを設定した後、Secure Socket Layer（SSL）を使用してデフォルトで有効になります。

Q. ソフトウェア開発キット（SDK）ソフトウェアはどこで入手できますか

A. SDK ソフトウェアは一般に公開されていません。

IDS センサー

Q. センサーのバージョン 3.x と 4.x の違いは何ですか

A. バージョン 4.0 にはいくつかの新機能があります。 最も顕著な新機能は Cisco IOS® に似たコマンドライン インターフェイス（CLI）です。

Q. IDS でインターフェイス速度をどのようにハードコードしますか

A. 3.X および 4.0 コード内の速度/デュプレックスのハード設定はサポートされておらず、機能リクエストに関するバグが報告されています（Cisco Bug ID CSCdy43054（登録ユーザ専用））。 この機能は、「インターフェイスの設定」で入手可能な 5.0 コードで使用できます。

Q. センサー ソフトウェアをバージョン 3.0 から 3.1 にどのようにアップグレードできますか

A. お客様はバージョン 3.1 の更新ファイルを Cisco Secure Downloads（登録ユーザ専用）からダウンロードできます。

Q. センサー ソフトウェアをバージョン 2.5 から 3.0 にどのようにアップグレードできますか

A. お客様はバージョン 3.0 の更新ファイルを Cisco Secure Downloads （登録ユーザ専用）からダウンロードできます。 バージョン 2.5 でサービス パックとシグニチャ更新をインストールしたのと同じ方法で、ソフトウェア更新をインストールします。 手順の詳細は、「Cisco IDS センサー設定の注意点バージョン 3.0」を参照してください。

Q. センサー ソフトウェアをバージョン 2.2 から 3.0 にアップグレードするにはどうすればよいですか。

A. 3.0 アップグレード ファイルは Cisco Secure Downloads（登録ユーザ専用）からダウンロード可能ですが、このファイルは 2.5 より前のバージョンを更新できません。 Product Upgrade Tool（登録ユーザ専用）から入手可能な更新/リカバリ CD を使用して、ソフトウェア バージョン 2.2 から 3.0 にアップグレードする必要があります。 この CD の製品番号は IDS-SW-U です。

注: 更新/リカバリ CD を注文するには、有効なサポート契約が必要です。

Q. センサーにキーボードとモニタを接続しましたが、正常にブートしません。 どうすればよいのですか。

A. サポートされているキーボードとモニタを使用していることを確認します。 一部のブランドおよびモデルは Cisco Secure IDS と互換性がなく、IDS センサーが正しくブートしません。 ブランドの詳細については、「Cisco Secure IDS アプライアンスのブート障害」を参照してください。

Q. Cisco Secure Downloads の IDS セクションには 2 種類の更新ファイルがあります (サービス パックとシグニチャ) 。 これらの違いは何ですか。

A. これらのファイルにはそれぞれ、特定のソフトウェア更新/追加のセットが含まれています。これらの命名規則は次のとおりです。

- IDS センサー アプライアンス ソフトウェアのサービス パック更新には、IDS センサー コア アプリケーション ソフトウェアの改善とバグ修正含まれています。 たとえば、**IDSk9-sp-3.0-5-S17.bin** という名前のファイルには、ソフトウェア バージョン 3.0(5) の更新に加えて、シグニチャ セット番号 17 が含まれています。
- シグニチャ更新ファイルにはシグニチャ (攻撃フィンガープリント) の更新のみが含まれます。 たとえば、**IDSk9-sig-3.0-5-S18.bin** という名前のファイルには、3.0(5) センサー ソフトウェア用のシグニチャ セット番号 18 が含まれています。

お客様はこれらのファイルを Cisco Secure Downloads (登録ユーザ専用) サイトからダウンロードできます。

Q. ルータを回避するようセンサーが正しく設定されているかどうか、どのように確認できますか

A. センサーにユーザ **netrangr** としてログインし、次のコマンドを実行します。

nrgetbulk *<appID> <sensorHostID> <sensorOrgID> <priority> <token>*

「*<IP_address>* Active」のような応答を受信します。これは、攻撃のブロックに使用されている回避デバイスの IP アドレスを示しています。 この出力は、コマンド構文と期待される応答の例を示しています :

```
netrangr@sensor:/usr/nr
>nrgetbulk 10003 38 1000 1 NetDeviceStatus
10.48.66.68 Active
Success
```

また、ルータにログインして **who コマンド**を発行することで、センサーにログインしているかどうか確認できます。

Q. nrconns コマンドを発行すると、「値が設定されていない」というエラー メッセージが表示されます。 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 メッセージは、センサーの /usr/nr/etc/routes や /usr/nr/etc/hosts ファイルに問題がある可能性を示しています。 .../routes ファイルは、センサーと Director の間のポストオフィス通信を定義します。 … /hosts ファイルは、センサーおよび Director の名前と IP アドレスを定義します。

また、ユーザ root としてログインし、**sysconfig-sensor コマンド**を実行して、IDS 通信インフラストラクチャ情報を再び入力することもできます。

Q. FTP を使用してセンサーのログ ファイルをコピーし、それを他の場所に保存するにはどうすればよいですか

A. その手順の詳細については、「表示用に IP ログ ファイルをコピーする」を参照してください。

Q. センサー ソフトウェア バージョン 2.5 および 3.1 の configd デーモンはどうなりましたか

A. configd は、2.2.x コード ベースのセンサーと UNIX Director の両方ですべてのコマンドを処理するデーモンです。 2.5 および 3.0 コード ベースではこの機能が他のデーモンに吸収され、configd デーモンは存在しなくなりました。

Q. センサーのシグニチャを更新すると、「ERROR: `Could not determine the type of NetRanger from daemons file.` Unable to update.」というエラー メッセージが表示されます。 どう対処すればよいですか。

A. センサーの /usr/nr/etc/daemons ファイルを編集して nr.packetd がデーモン リストに含まれるようにしてください。 それから、サービスを停止し、再起動します。

Q. IDS 4210 では、どれがコントロール インターフェイスで、どれがスニフィング インターフェイスですか

A. 最も上のコントロール インターフェイスは **iprb1:** で、 最も下のスニフィング インターフェイスは **iprb0:** です。

Q. センサーで ifconfig -a コマンドを発行したときに、インターフェイスが 1 つだけ表示されるのはなぜですか。

A. **Ifconfig コマンド**は、コントロール インターフェイスのみを表示します。 他方のインターフェイス（スニフィング インターフェイス）もセンサーで使用されますが、ユーザには表示されないようになっています。 このインターフェイスを確認する必要がある場合は、root としてログインし、**ifconfig -a コマンド**を発行してインターフェイス名を判別します。 **ifconfig <interface> plumb** コマンドを発行して、特定のインターフェイスのステータスを確認します。

Q. センサーでインターフェイス速度をどのようにハードコードできますか

A. センサーでインターフェイス速度をハードコードする必要はなく、シスコ テクニカル サポートではこれがサポートされていません。 スイッチが自動ネゴシエーション用に設定されると、インターフェイスは接続先のスイッチとの間で速度をネゴシエートします。 ネットワークからセンサーへのトラフィックは単方向です（つまりセンサーは受信側）。 したがって、（スイッチ ポートが 100 M であると想定すると）100 半二重でネゴシエート済みとスイッチで表示されたら、一般的には十分です。

UNIX Director

Q. 新しい 3.0 センサーを 2.2.x バージョンの Director で使用できますか

A. はい。ただし Director ソフトウェアをバージョン 2.2.3 以降にアップグレードする必要があります。 登録済みのお客様はこれらのファイルを Cisco Secure Downloads（登録ユーザ専用）からダウンロードできます。

Q. 使用している Director デーモンのバージョンをどのように確認できますか

A. **cat /usr/nr/VERSION** コマンドを発行し、出力に含まれるバージョン番号を確認します。

注: Director での **nrvers コマンド**の出力には、その Director で実行されているデーモンのバージョンが示されますが、Director ソフトウェア自体のバージョンは示されません。

Q. Director の設定をダンプするにはどうすればよいですか

A. ユーザ **netrangr** としてログインし、スクリプト /usr/nr/bin/director/nrCollectInfo を実行して、/usr/nr/var/tmp/Report_For_Director.html という名前のファイルに設定情報を送ります。

Q. HP OpenView ディスプレイに多数のエラー (おそらく 1,000 個以上) が表示されます。 それらを削除しても、また表示されます。 これは、なぜですか。

A. IDS Director が エラーでいっぱいになり、それらすべてを表示できない場合、ファイルへのバッファリングが開始します。 IDS デーモンを停止し、開いている OpenView マップをすべて終了して、ファイルを削除します。 ファイル **/usr/nr/var/nrDirmap.buffer.default** を削除した後、IDS デーモンおよび OpenView マップを再起動します。

Q. HP OpenView マップにアラームが出る問題が発生しています。 /usr/nr/var/errors.nrdirmap でエラーが発生し続けます。 どうすればよいのですか。

A. 2.2.2 より前のバージョンの IDS では、OpenView データベースを消去するのが最も簡単な方法です。 データベースは /var/opt/OV/share/databases/openview にあります。 次のステップを実行して、OpenView データベースを削除します。

1. **Ovstop コマンド**を使用して、開いているすべての OpenView マップを閉じた後、**nrstop コマンド**を使用して IDS サービスを停止します。
2. ユーザ root としてログインし、**/usr/nr/bin/director/nrDeleteOVwDb** を発行します。
3. すべての「error.*」ファイルを /usr/nr/var ディレクトリの中から削除します (errors.configd など) 。
4. **nrstart コマンド**を使用してサービスを再起動した後、**ovstart コマンド**を使用して OpenView を再起動します。 **注:** Director バージョン 2.2.2 では、データベース全体ではなく、OpenView データベースの IDS 部分のみを削除できます。 この手順は『IDS Director Configuration Guide』で説明されています。

Q. OpenView マップのアラームが表示されません。 Director の /usr/nr/var/errors.postofficed ファイルに、このマシンで nrdirmap を実行するライセンスがないというメッセージが表示されます。 これはどのように解決すればよいですか。

A. 次のコマンドを実行してください。

```
cp /usr/nr/etc/.lt/license-all.lic /usr/nr/etc/licenses
```

ユーザ **netrangr** がファイルを所有していることを確認して、IDS サービスを再起動します。

Q. nrConfigure ユーティリティを実行して Director をダブルクリックすると、次のメッセージが表示されます。 「Unable to find the type of the sensor for *<director_name>*. Please check that Postoffice and packetd are running」 どうすれ

ばよいのですか。

A. この問題が発生する理由は、nrConfigure が Director のデーモン ファイル内に（不必要な）packetd プロセスを検出するためです。 nrConfigure が Director に対して（Sensor であるかのように）バージョンを問い合わせると、Director はセンサー バージョンを応答できません。

この問題を解決するには、次の手順を実行します：

1. /usr/nr/etc/daemons ファイルを編集して nr.packetd、nr.sensord、および nr.managed のエントリを削除します（これらのプロセスはセンサーでのみ実行されるべきです）。
2. **nrstop コマンド**を使用してサービスを停止し、**nrstart コマンド**を使用してサービスを再起動します。
3. nrConfigure がシャットダウンされたことを確認します。
4. **Ovw コマンド**を使用して OpenView を起動します。
5. [Security] > [Advanced] > [nrConfigure DB] > [Delete] を選択して、破損した nrConfigure データベースを削除します。
6. プロンプトが表示されたら、**yes** と入力して続行します。
7. OpenView のメイン ウィンドウで、Director およびすべてのセンサーを強調表示します。
8. [Security] > [Advanced] > [nrConfigure DB] > [Create] を選択し、マシンの現在の設定バージョンを使って新しい nrConfigure データベースを作成します。

Q. OpenView マップで nrdirmap アプリケーションがデフォルトで有効にならないようにするには、どうすればよいですか

A. UNIX Director で IDS アプリケーションを実行するユーザは、OpenView で他のアプリケーションも実行できます。 これは推奨されませんが、状況によっては避けることができません。 問題は、すべての OpenView マップで nrdirmap がデフォルトで有効になることです。他のアプリケーションが OpenView で動作する場合には、これは望ましくありません。

UNIX Director で次の手順を実行して、nrdirmap を有効にするマップを選択できるように、デフォルトを変更してください。

1. ユーザ **netrangr** としてログインします。
2. **cd $OV_REGISTRATION/C** と入力します（OV_REGISTRATION は環境変数の一部です。通常のパスは /etc/opt/OV/share/registration/C です。）
3. **su root** と入力します。
4. nrdirmap ファイルを編集し、「Command」行を次の出力例のように変更します。
```
Command -Shared -Initial "nrdirmap";
!--- Changes to: Command -Shared -Initial "nrdirmap -d";
```
5. nrdirmap ファイルを保存します。
6. OpenView を終了し、再起動します。 今度は、**ovw コマンド**でマップが表示されたときに **ps -ef | grep dirmap** と入力すると、次に示すような出力が表示されるはずです。 nrdirmap に -d スイッチを含めていることに注意してください。 `>ps -ef | grep dirmap`
```
netrangr 7175 6820 0 09:50:47 pts/2 0:00 grep dirmap
netrangr 7158 7152 0 09:50:21 ? 0:00 nrdirmap -d
```

これで、OpenView で作成される新しいマップでは、nrdirmap がデフォルトで有効にならなくなります。 nrdirmap がインストールされたマップを作成するには、この手順で説明するように OpenView GUI から作成する必要があります。

1. OpenView のメイン メニューから [Map] > [New] と選択し、新しいマップの名前を入力しま

す。
2. 設定可能なアプリケーションとして NetRanger/Director が表示されるはずです。 [NetRanger/Director] を選択し、[Configure For this Map] をクリックします。
3. 「Should nrdirmap be enabled for this map?」というオプションに対して、nrdirmap を有効にする場合は [True] を選択します。
4. [Verify] を選択し、[OK] をクリックします。

Q. Director バージョン 2.2.3 にアップグレードした後、イベントの重大度を 5 より高いレベルに設定できません。旧バージョンでは設定できていました。 なぜでしょうか。

A. Director バージョン 2.2.3 では重大度レベルが変更され、1 ~ 5 の範囲のみサポートされるようになりました。

IDS Cisco Secure Policy Manager（CSPM）

Q. IDS センサーを管理するにはどのバージョンの CSPM を使用する必要がありますか

A. 現在、CSPM バージョン 2.3i だけが IDS センサーを管理でき、CSPM 3.0 では管理できません。 CSPM を使用してセンサーおよび他のシスコ セキュア デバイス（PIX、ルータなど）を管理する場合は、2 つの別々の Windows サーバに 2 つの異なるバージョン（2.3i および 3.x）の CSPM をインストールする必要があります。 それぞれのサーバを使用して、対応するデバイスを次のように管理できます： センサー用には CSPM 2.3i を使用し、PIX、ルータなどには CSPM 3.x を使用します。

Q. IDS センサーを管理して通信を確実に機能させるには CSPM をどのように設定できますか

A. IDS センサーを管理して通信を確実に機能させるよう CSPM を設定する方法について、詳しくは「CSPM での Cisco Secure IDS センサーの設定」を参照してください。

Q. CSPM でアプライアンスのシグニチャを調整できますか

A. 「調整」とはシグニチャの起動条件（たとえばスイープのホスト数）の変更などを指しますが、アクションや重大度レベルを設定するという意味ではありません。

（どのバージョンの）CSPM も、アプライアンスのシグニチャを調整できません。 シグニチャのアクションと重大度だけを設定できます。 つまり、CSPM ではどの重大度とアクションをシグニチャに関連付けるかを設定できますが、シグニチャの起動条件は設定できません。 センサーを調整するにはセンサーの SigWizMenu を使用する必要があります。 SigWizMenu と CSPM は異なる部分の設定を行うため、両方を同じセンサーの設定に使用できます。

注: UNIX Director バージョン 2.2.3 以降をご使用の場合は、SigWizMenu で設定するすべての項目を nrConfigure ユーティリティで設定できます。 2.2.3 にアップグレードした後は、シグニチャを調整するために SigWizMenu ではなく nrConfigure を使用してください。

関連情報

- Cisco 侵入防御システム製品のサポート
- Cisco Secure Intrusion Detection System に関する文書
- Cisco Secure Intrusion Detection System に関するフィールド通知
- テクニカルサポートとドキュメント - Cisco Systems