

NetScreen-IDP リリースノート

製品： IDP 10、100、500、1000

バージョン： NetScreen-IDP 3.0r1

パーツ番号： 093-1201-000-JP 改訂 A

日付： 7/8/04

目次：

1. バージョン要約	P. 2
2. 新しい機能と強化された機能について	P. 2
2.1 新しい機能	P. 2
2.2 強化された機能	P. 5
3. デフォルト動作の変更	P. 7
3.1 定義済み Log Viewer フィルタの変更は保存されません	P. 7
3.2 ハートビートは HA 設定中に有効になります	P. 7
3.3 攻撃オブジェクト更新	P. 7
3.4 デフォルトのセキュリティポリシールール	P. 7
4. 解決された問題	P. 7
5. 既知の問題	P. 8
5.1 機能の制限	P. 8
5.2 機能の問題	P. 8
5.3 既知の問題	P. 8
6. 更新のインストール	P. 13
6.1 始める前に	P. 13
6.2 インストール手順	P. 14
7. ヘルプの取得	P. 15

1. バージョン要約

NetScreen-IDP 3.0 は、IDP 10、100、500 および 1000 システムの最新リリースのソフトウェアです。このリリースには、IDP センサー、IDP ユーザーインターフェースおよび IDP 管理サーバーの更新が含まれています。既存の IDP 実装を修正、更新または変更する前に、すべての NetScreen-IDP 3.0 製品マニュアルを読んでおくことをお勧めします。

すべてのカスタマは、このリリースを実装してください。

2. 新しい機能と強化された機能について

このリリースには、以下の新しい機能と強化された機能が含まれています。

2.1 新しい機能

このリリースには、以下の新しい機能が含まれています。

2.1.1 動的グループ

サービス、重要度およびアプリケーションタイプなど、オブジェクト定義内のフィールドの値に基づいて、動的グループを定義できます。新しい攻撃オブジェクトを NetScreen-IDP システムに追加する場合、新しいカスタム攻撃オブジェクトを手動で作成しても、攻撃オブジェクトの自動更新中でも、IDP は、新しい攻撃オブジェクトをオブジェクト定義と一致する任意の動的グループのメンバとして自動的に追加します。

2.1.2 複合攻撃

複数のシグネチャ攻撃オブジェクトまたはプロトコルアノマリ攻撃オブジェクトを 1 つのセッションに結合する複合攻撃オブジェクトを作成できます。トラフィックが複合攻撃オブジェクトに一致するのは、シグネチャまたはプロトコルアノマリのすべてが一致する場合のみです。また、必要に応じて、トラフィックが特定の順序で各コンポーネントに一致するように指定することもできます。

2.1.3 プロファイルベースの検出

Profiler を使用して、ネットワークのトラフィック解析を支援できます。ネットワークのスナップショットを作成するには、最初に、Profiler が詳細情報を収集するホストおよびネットワークを識別します (Profiler は、このリストに含まれていないすべてのアドレスを 1 つの「外部」アドレスと見なします)。次に、Profiler は、センサーにより処理されるトラフィックで識別されるソース、宛先およびコンテキストのそれぞれ一意の組み合わせに対するレコードを記録します。Profiler がレコードをデータベースに追加すると、そのレコードに一致する後続のセッションが、新しい Profiler レコードを作成するのではなく、カウントおよびタイムスタンプを更新します。Profiler レコードは、ネットワークのデバイスおよび通常のアクティビティに関する包括的な詳細を提供します。

違反オブジェクトを設定して **Profiler** レコードをフィルタ処理し、ネットワークの不適切な、または危険な状況を識別して、脆弱性のあるホストまたはネットワークデバイスのセキュリティを確保するための適切な処置を取ることができます。一意のセッション（ソース、宛先およびコンテキスト）だけがレコードを生成するため、**Profiler** データベースは、数時以内でかなり安定した状態になります。次に、ネットワーク変更検出を有効にできます。これにより、**Profiler** が新しいホスト、ポートまたはプロトコルに関連するセッションを認識した場合、IDP ログレコードが生成されます。

2.1.4 ログの抑止

NetScreen-IDP を設定して、特定期間で特定のイベントが複数検出された場合それぞれに個別のログレコードを生成するのではなく 1 つのログレコード内でカウンタを増加させることができます。ログ抑止をグローバルに有効にして、レコードを抑止する前に受信するレコード数、および抑止の期間を指定します。

デフォルトのログ抑止設定を次に示します。

- ログ抑止はデフォルトで有効になっています。
- IDP は、ログ抑止用の一致イベントを判別するとき、宛先 IP アドレスを考慮しません。
- IDP は、ログレコードを 1 つ受け取った後にログ抑止を開始します。
- IDP は、16384 のログレコードでログ抑止を実行できます。
- IDP は抑止されたログを 10 秒後にレポートします。

たとえば、しきい値を 2 に設定して、期間を 5 秒に設定できます。この場合、IDP は、5 秒内で発生したイベントの最初の 2 つのインスタンスのログレコードを生成し、その 5 秒内の 3 つめ以降のイベントに関してはその数を追跡します。このイベントが 5 秒の制限を超えて繰り返される場合、IDP は、さらに 2 つのログレコードを生成します。

2.1.5 TruSecure 詳細情報

TruSecure 詳細情報が入手可能な場合、その情報を攻撃オブジェクトの新しい **Extended** タブで参照できます。TruSecure 情報には、影響を受けるベンダーや製品、イベントの詳細情報、パッチが入手できるかについての情報、および問題の回避策などが含まれます。

2.1.6 除外ルールベース

ログレコードを右クリックし、**Exempt** を選択することで、特定の攻撃オブジェクトの特定のソースと宛先のペアを**除外**できます。**除外**後にそのソースおよび宛先のペアのトラフィックが、メインルールベースの規則に指定されている攻撃オブジェクトに一致しても、ログレコードは生成されません。

除外ルールは、セキュリティポリシーエディターの**除外**ルールベースから作成、編集または削除できます。セキュリティポリシーエディターを作成すると、デフォルトの**除外**ルールには、任意のソース IP アドレス、任意の宛先 IP アドレスおよびすべての攻撃が含まれています。

除外ルールベースはターミナルです (メインルールベース以外のすべてのルールベースと同じです)。

2.1.7 カスタムレポート

カスタムレポートを作成できます。各カスタムレポートに関して、追加するコラム、表示するデータポイントの数、期間、およびフィルタ処理するコラム値を指定します。

2.1.8 クイックレポート

選択ログレコードに含まれる値に基づいてフィルタ処理された様々なログデータのグラフを表示する、クイックレポートを **Log Viewer** から表示できます。

2.1.9 RADIUS クライアント

NetScreen-IDP センサーを設定して、ACM または SSH を使用してセンサーに接続するユーザーの認証に RADIUS を使用できます。有効な場合、センサーは、最初に、ローカルユーザー認証をチェックし、失敗すると、RADIUS サーバーと通信してユーザー認証を行います。RADIUS サーバーを ACM で有効および識別します。

2.1.10 バイパスユニットは ACM で有効にされます

ACM にて NS-IDP-BYP (Bypass Unit) が NetScreen-IDP 10 または 100 で動作するように設定できます。詳しい設定は必要ありませんが、センサーはブリッジまたは透過モードで動作している必要があります。

2.1.11 ピアポートモジュレータ

ピアポートモジュレータは、NetScreen-IDP センサーインターフェースでダウン状態にあるリンクをチェックします。リンクがダウンしている場合、センサーは、同じ仮想ルーターの関連するネットワークインターフェースも強制的にダウン状態にします。この機能は、冗長性機構が IDP の両サイドを監視しているネットワークに適しています。ネットワークインターフェースがダウン状態にある場合、ネットワークは、IDP のトラフィックのルートを変更して、ネットワーク接続性を保守します。

ピアポートモジュレータを ACM で有効にできます。この機能は、VLAN インターフェースではサポートされていません。

2.1.12 透過モード

NetScreen-IDP センサーを透過モードで設定できます。これにより、NetScreen-IDP センサーは、非 IP/ 非 ARP トラフィックなどのトラフィックを、転送できるようになります。透過モードは、転送インターフェースのペアを独自の仮想ルーターに属する各ペアと使用します。透過モードでは、トラフィックがタグに関係なく転送されるので、VLAN タギングは必要ありません。透過モードは、外部高可用性 (HA) はサポートしていますが、スタンドアロン高可用性 (HA) はサポートしていません。透過モードでは、転送インターフェースの IP アドレス、VLAN 設定、および他のネットワークデバイスの設定の変更が必要ないので、透過モードはすぐに簡単に設定できます。

2.2 強化された機能

このリリースには、以下の強化された機能が含まれています。

2.2.1 追加サポートプロトコル

NetScreen-IDP は、以前のリリースでサポートされていたプロトコルのほか、LDAP、MySQL、NetBIOS 137/138、NTP、SSL、および Whois もサポートされるようになりました。

2.2.2 新しい定義済みレポート

IDP レポート構成要素に、23 の新しい定義済みレポートが追加されました。

2.2.3 ターミナルルールの新しい名前

セキュリティポリシーエディタのメインルールベースの Terminal コラムは、“Terminate Match” になりました。メインルールベースは、デフォルトではターミナルしないようになっています。他のすべてのルールベースは、デフォルトでターミナルです。

2.2.4 特殊なドメイン名

アルファベットではなく数値で始まるドメイン名など、標準定義から逸脱するドメイン名を指定できるようになりました。

2.2.5 長い SNMP コミュニティ文字列

ACM を使用して、最大 255 文字を含む SNMP 読取専用コミュニティ文字列を指定できるようになりました。

2.2.6 ACM で使用できるデバイスシリアルナンバー

IDP センサーのシリアルナンバーを ACM のメインページで参照できるようになりました。

2.2.7 sctop で表示される HA スタンバイ状態

sctop CLI コマンドをセンサーで実行する場合、**w** オプションを使用して、スタンドアロン高可用性 (HA) スタンバイ状態を表示できるようになりました。

2.2.8 転送インターフェースのハートビート静的ルート

デフォルトゲートウェイの代わりに ACM を使用してハードビートのルートを設定できるようになりました。

2.2.9 UI でハイライトされるトリガパケット

パケットビューアを IDP UI で開くと、ログエントリをトリガしたパケットは、内部パケットビューアで赤でハイライトされます。

2.2.10 TCP リセットのソースとしての非転送インターフェース

ACM を使用して、センサーをスニッファモードで設定して、TCP リセットを専用インターフェース上で送信できるようになりました。ただし、スニッファに使用されるインターフェースや管理インターフェースではなく、この目的のためにネットワークに接続されているインターフェースを使用する必要があります。

2.2.11 攻撃オブジェクト更新通知

IDP UI にログインしたとき、新しい攻撃オブジェクト更新が通知されるようになりました。この設定を変更するには (デフォルトでは有効になっています)、IDP UI メニューバーで、Tools → Preferences → User Settings をクリックして、**Check Update on Startup** チェックボックスをクリアします。

3. デフォルト動作の変更

このリリースでは、以下のデフォルト動作が変更されました。

3.1 定義済み Log Viewer フィルタの変更は保存されません

定義済み Log Viewer フィルタの変更は、現在の UI セッションのみで有効で、他の変更を保存するときには保存されません。

3.2 ハートビートは HA 設定中に有効になります

高可用性 (HA) を ACM で設定すると、ハートビート機構はデフォルトで有効になります。

3.3 攻撃オブジェクト更新

攻撃オブジェクトデータベースを更新すると、既存のグループに追加された新しい攻撃オブジェクトは、これらのグループを参照するルールで反映されます。この動作は、既存のグループに属している新しいカスタム攻撃オブジェクトを手動で追加した場合と同じです。また、攻撃オブジェクト名に影響を与えるような更新をしても、既存のセキュリティポリシールールは無効になりません。

3.4 デフォルトのセキュリティポリシールール

このリリースでは、セキュリティポリシールールの以下のデフォルト動作が変更されました。

3.4.1 デフォルトルールは None アクションを使用します

新しいルールをセキュリティポリシーで作成すると、デフォルトのアクションは “None” になります (以前は “Drop” でした)。

3.4.2 デフォルトルールはターミナルではありません

新しいルールをセキュリティポリシーで作成すると、Terminate Match フィールド (Terminal コラムの新しい名前) はデフォルトでは有効になりません。

4. 解決された問題

このリリースでは、以下の主なバグが修正されました。

- 00542 : オブジェクトエディタで、サービスオブジェクトに IP 構成要素オブジェクトが含まれていません。
- 00771 : ログインバスターの攻撃で “Zoom in” を選択すると、いくつかのレコードの Default Severity コラムに何も表示されないことがあります。

- 00802 : パケットビューアに、ポリシールールで設定されているパケット番号とは別の番号が表示されます。
- 00829 : ログインバスターゲータで、ズームインすると、間違ったタイム範囲がグラフタイトルに表示されることがあります。
- 00831 : ログインバスターゲータの「最新」の期間が、その日数が長い場合、正しく表示されないことがあります。
- 00875 : VLAN タグインターフェースで IDP 500 を介して送信される FTP および HTTP トラフィックが、すべての定義済み攻撃オブジェクトをアクション Ignore で指定するルールにより設定されている場合、センサーがクラッシュすることがあります。
- 00748 : 攻撃オブジェクト更新の完了前に、IDP UI がハングアップすることがあります。ハングアップした場合、Task Manager を介して IDP UI を停止し、UI を再起動して、更新を再実行してください。

5. 既知の問題

このリリースでは、以下の問題が報告されています。問題によっては、回避策があります。

以下の既知の問題に対する解決策および更新ソリューションについては、NetScreen サポートサイト、<http://www.netscreen.com/cso> にアクセスしてください。

5.1 機能の制限

なし。

5.2 機能の問題

IDP UI、IDP 管理サーバーおよび IDP センサーを IDP 3.0r1 にアップグレードする前に、IDP 2.1 にアップグレードする必要があります。

5.3 既知の問題

このリリースでは、以下の問題が報告されています。

- 00615 : 攻撃オブジェクト名をグラフ下部に表示するカスタムレポートは判読できません。
- 00765 : ログインバスターゲータで、ズームインすると、“timed out” メッセージが表示されることがあります。
- 00777 : Log Viewer で、Whois 詳細ペインからエラーが返されることがあります。
- 00781 : ACM Configure Routing Table セクションで、“Invalid IP address” エラーメッセージをトリガすることなく、無効な値をオプションルートの “Network”

フィールドに入力できます。また、ACMは無効なIPアドレスを有効なIPアドレスに不正に変換します。

- 00795 : 攻撃オブジェクトエディタで、**Extended** タブに、リンクフォーマットが正しくない壊れたリンクが含まれることがあります。
- 00882 : レポートで、**Log Viewer** フィルタは動的グループを正しく扱いません。
- 00919 : ACM が、**idpconf.cfg** ファイルを新しい (未設定の)IDP センサーにアップロードできないことがあります。
- 00932 : **Profiler** は、実行中でないセンサーをすぐに表示しません。解決策 : 実行中でないセンサーが **Profiler** に表示されるまで数秒待ちます。
- 00959 : カスタムレポートのリルダウンビューで使用されるフィルタが保存できません。
- 01002 : HA 構成のセンサーは、1つの転送インターフェースだけにしか **Verify-IP ping** を送信できないようです。IDP は、実際、**Verify-IP ping** を2つのインターフェースに送信しませんが、センサーは、両方の **ping** に同じ IP アドレスを使用します。これは、**Linux** カーネルルーティングテーブルが、同じソース IP アドレスから両方の **Verify-IP** アドレスを参照するからです。
- 01015/01601 : ログインベスティゲータで、カスタムレポートを作成すると、いくつかのフィルタが失われます。
- 01363 : **Profiler** で、IP アドレスのみを使用してフィルタリストに追加されるホストまたはネットワークは、保存されません。

解決策 : ホストまたはネットワークのネットワークオブジェクトを作成し、そのオブジェクトをフィルタリストに追加します。

- 01389 : IDP UI は、日本語 Windows 2000 でアンインストールできません。
- 01440 : ダッシュボードでのカスタムレポートの変更は、UI 全体には反映されません。
- 01472 : Log Viewer は、UI から削除されたセンサーから新しいログレコードを表示し続けます。
- 01487 : Log Viewer で、ログ抑止は宛先ポートを考慮しません。
- 01492 : センサーを透過モードで実行する場合、sctop はレイヤ 2 フレームをカウントしません。
- 01552 : Log Viewer で、カスタムビューは、IDP 2.1 から IDP 3.0 へのアップグレード中に保持されません。
- 01607/01565 : 右クリックメニューオプション“Show attack in security policy”を使用すると、攻撃オブジェクトを含む不正なグループ (静的または動的) が表示されることがあります。

解決策 : その攻撃オブジェクトに対して、Log Viewer から除外ルールを作成します。

- 01566/1574 : IDP 2.1 から 3.0 にアップグレードすると、更新通知が UI 基本設定に表示されていても、UI を開くと、攻撃オブジェクト更新ウィザードがトリガされます。

解決策 : ログイン時で今後の更新通知を無効にするには、IDP UI メニューバーで、Tool → Preferences → User Settings をクリックして、Attack Object Update セクションの Check Update on Startup チェックボックスを選択します。Apply をクリックして変更を保存し、Preferences ダイアログボックスを再び開き、Check Update on Startup チェックボックスをクリアします。Apply をクリックして、変更を保存します。

- 01570 : Log Viewer で、ログレコードのフィルタを作成し、フラグを大量のまたはすべてのログレコードに設定すると、フラグが間違ったログレコード、つまりフィルタと一致しないログレコードに適用されます。
- 01585 : 攻撃オブジェクトのフィルタは、定義済み動的グループの攻撃オブジェクトのすべてのインスタンスには適用されません。
- 01588 : ログインバステイゲータで、アドレス解決がホスト IP アドレスまたはホスト名で機能しません。
- 01605 : ベータプログラム中、NetScreen は、External-IP の名前を Non-Tracked IP に変更しました。IDP 3.0b1 (beta1) からアップグレードすると、External-IP をソース IP として使用する違反オブジェクトが Profiler に表示されます。違反オブジェクトには、オブジェクトエディタからアクセスできません。
- 01628 : レポートで、いくつかの定義済みレポートは、正しいデータポイントカウントを表示しません。

解決策：“set report options”を開き、OKをクリックして、定義済みレポートを正しいデータポイントカウントで更新します。

- **01633**：レポートで、フィルタが、名前に IP アドレスを使用するネットワークオブジェクトで機能しません。例えば、名前“192.168.1.1”を使用するネットワークオブジェクトです。

解決策：ネットワークオブジェクト名に IP アドレスを使用しません。

- **01647**：ACM で、Configuring RADIUS のオンラインヘルプが表示されません。
- **01527**：IDP UI を RHEL WS 3 にインストールするときにエラーメッセージが表示されます。これらのメッセージは無害なので無視してください。このエラーメッセージは次のとおりです。

```
Preparing to install...
tail: '-1' option is obsolete; use '-n 1'
Try 'tail --help' for more information.
install.bin: line 329: [: `)' expected, found -z
WARNING! The amount of /tmp disk space required and/or available
could not be determined. The installation will be attempted
anyway.
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer
archive...
Configuring the installer for this system's environment...
```

- **01573**：センサーを IDP 2.1 から IDP 3.0 にアップグレードするときにエラーメッセージが表示されます。これらのメッセージは無害なので無視してください。このエラーメッセージは次のとおりです。

```
/etc/lilo.conf has been changed to run the new kernel and
/sbin/lilo has been run
please remove the appropriate entries from /etc/lilo.conf and
rerun /sbin/lilo
please remove the appropriate entries from /etc/lilo.conf and
rerun /sbin/lilo
warning: /etc/ssh/ssh_config created as /etc/ssh/ssh_config.rpmnew
warning: /etc/ssh/sshd_config created as /etc/ssh/
sshd_config.rpmnew
warning: /etc/postfix/access created as /etc/postfix/access.rpmnew
warning: /etc/postfix/main.cf created as /etc/postfix/
main.cf.rpmnew
warning: /etc/postfix/transport created as /etc/postfix/
transport.rpmnew
```

- **01656**：Profiler を設定して起動すると、アクションオプションは、同期を実行するまで使用できません。

解決策：Profiler Configuration ダイアログボックスを開き、選択されている設定オプションのいずれかを変更して、OK をクリックします。プロファイリング処理を促すメッセージが表示されたら、OK をクリックして、Profiler Action ダイアログボックスを起動します。Profiler データを同期します。これで、Profiler Action オプションを使用できるようになります。

- 01657：ACM で、Intel Quad カードがインストールされているセンサーの“Configure Network Interface Hardware”セクションに、Quad カードインターフェースが Intel Gigabit インターフェースとして表示されます。これらのインターフェースには、“Please select auto mode for fiber card”という警告が含まれています。

解決策：警告を無視して、必要に応じて、各インターフェースの速度および二重オプションを設定します。設定は、正しく保存および適用されます。

- 01622：ACM で、IDP 2.1 から IDP 3.0 にアップグレードした場合、IDP 管理サーバー通信を設定、または ACM 設定をセンサーに適用すると、“permission denied”エラーメッセージが表示されることがあります。このエラーメッセージが表示されるのは、idpconf.cfg が ACM にアップロードされた場合、またはセンサーが ACM 実行前に再起動されていない場合です。

解決策：idp.cfg (/usr/idp/device/cfg の Sensor にあります) を編集するか、VIN 番号の属性を削除します (行を完全に削除します)。ACM 設定を再起動します。

- 01661：サービスフィールドでフィルタ処理するカスタム動的グループには、指定サービスに一致する複合攻撃オブジェクトがありません。
- 01525：オブジェクトエディタで、センサーネットワークオブジェクトを削除し、すぐに別のセンサーネットワークオブジェクトを削除すると、回避できないエラーメッセージが表示されます (UI クライアントは強制的にシャットダウンする必要があります)。

解決策：センサーネットワークオブジェクトを削除したら、砂時計アイコンが消えるまで待ち、その後で別のセンサーネットワークオブジェクトを削除します。

- 01547：Profiler ネットワークビューで、サービスは異なるがポート番号は同じである (DNS など) 2 つのプロトコルのビューを否定すると、データは返されません。
- 01552：IDP 3.0r1 にアップグレードすると、カスタム Log Viewer ビューは保存されません。
- 01644：IDP 3.0r1 にアップグレードしても、Sensor Settings Rulebase の既存のデフォルト値は、新しい IDP 3.0 デフォルト値で上書きされません。
- 01520：ACM で、仮想ルーターバインディングを切り替えると、設定がセンサーに適用されるときにエラーメッセージが表示されます。

- 01179 : IDP 3.0 ベータから IDP 3.0r1 にアップグレードすると、デフォルトの Profiler の最大データベースサイズは 500 ですが、範囲は 1 ~ 200 になります。妥当性検査エラーメッセージが UI に表示されます。

解決策 : IDP UI を閉じます。使用しているコンピュータの UI ディレクトリで `prefs.cfg` を探します。このファイルをテキストエディタで開き、Profiler の値を以下のように修正します。

```
profiler (  
  
:dblimit (value) <-- この値を 500 に変更します
```

変更を保存して、UI を開きます。

- ACM では、ピアポートモジュレータ (PPM) 機能は、VLAN インターフェースでサポートされていません。
- 攻撃オブジェクトデータベースが IDP 3.0 オブジェクトに更新される前に ACM から現在の設定を保存すると、いくつかのエラーメッセージが表示されます。

解決策 : 攻撃オブジェクトデータベースを ACM の実効前に更新します。

6. 更新のインストール

ソフトウェア更新は <http://www.netscreen.com/services> でダウンロードできます。

センサー、IDP 管理サーバーおよび IDP UI を IDP 3.0r1 にアップグレードする前に、IDP 2.1 を実行している必要があります。2.1 以前のリリースの IDP を実行している場合、3.0r1 にアップグレードする前に IDP 2.1 にアップグレードする必要があります。

また、NetScreen-IDP システムは、推奨されている順序でアップグレードしてください。詳細については、セクション 6.2 を参照してください。

6.1 始める前に

IDP 3.0r1 へのアップグレードを始める前に、以下のセクションの重要な情報をお読みください。

6.1.1 状態同期ケーブルを外す (HA 構成のみ)

HA 構成の IDP アプライアンスをアップグレードするには、アップグレードを実行する前に、各アプライアンスから状態同期ケーブルを外す必要があります。

6.2 インストール手順

NetScreen-IDP システムを 3.0r1 にアップグレードするには、システムの各階層を以下の順序でアップグレードする必要があります。

1. IDP センサーをアップグレードする
2. IDP 管理サーバーをアップグレードする
3. IDP UI をアップグレードする

以降のセクションでは、それぞれのアップグレードステップについて説明します。

6.2.1 センサーのアップグレード

IDP センサーをアップグレードするには：

1. IDP センサーリリース更新ファイルをターゲット IDP センサーにコピーします。
2. ターゲット IDP センサーにログイン (リモートまたはコンソール) します。root でログインしてスクリプトを実行する必要があります。IDP センサーが HA 構成の一部の場合、状態同期ケーブルがアプライアンスの状態同期ポートから外されていることを確認してください。
3. ステップ 1 でコピーしたリリース更新のターゲット位置に変更します。
4. **sh sensor_3_0r1.sh** を入力してリリース更新を実行します。
5. **reboot;reboot** を入力して、IDP センサープロセスを再起動します。

センサーが再起動したら、センサープロセスが自動的に開始されます。IDP センサーが HA 構成の一部の場合、状態同期ケーブルを再接続する前に、HA クラスタの他のセンサーもアップグレードします。

6.2.2 IDP 管理サーバーのアップグレード

IDP 管理サーバーをアップグレードするには：

1. IDP 管理リリース更新ファイルを IDP 管理サーバーにコピーします。
2. IDP 管理サーバーにログイン (リモートまたはコンソール) します。root でログインしてスクリプトを実行する必要があります。
3. ステップ 1 でコピーしたリリース更新のターゲット位置に変更します。
4. 以下の該当するコマンドを入力して、リリース更新を実行します。

Linux の場合：**sh mgtsvr_linux_3_0r1.sh**

Solaris の場合：**sh mgtsvr_solaris_3_0r1.sh**

6.2.3 UI のアップグレード

以下の指示に従い、NetScreen-IDP 3.0r1 UI をクライアントの現在の IDP UI ディレクトリにインストールできます。ただし、UI 更新を以前のバージョンの UI とは異なるディレクトリにインストールするには、最初に、以前のバージョンの UI をアンインストールし、以前の UI ディレクトリのすべてのファイルを削除する必要があります。

IDP 3.0 UI には、512 MB の RAM が必要です。UI をインストールするコンピューターに 512 MB の RAM があることを確認してください。

UI をアップグレードするには：

1. IDP UI リリース更新ファイルをクライアントマシンにコピーします。
2. UI 実行可能ファイルを開始します。
3. ダイアログボックスの指示に従って UI をインストールします。
4. UI インストールが完了したら、新しい UI を使用して、攻撃オブジェクトを更新します。

7. ヘルプの取得

詳細については、http://www.juniper.net/support/nscn_support/tao/contact.html までお問い合わせください。NetScreen 製品に関するサポートが必要な場合、以下にアクセスしてください。

www.netscreen.com/services/contact_tac

NetScreen は、ScreenOS ファームウェアのメンテナンスリリース (更新およびアップグレード) を提供することがあります。これらのリリースへのアクセス権を取得するには、以下のアドレスで、デバイスを NetScreen に登録する必要があります。

www.netscreen.com/cso

Copyright © 2004 NetScreen Technologies, Inc. All rights reserved. NetScreen、NetScreen Technologies、Neoteris、GigaScreen、NetScreen-Remote、NetScreen ScreenOS、NetScreen-Security Manager および NetScreen ロゴは、米国およびその他の国における NetScreen Technologies 社の登録商標です。その他のすべての商標および登録商標は、それぞれ各社に帰属します。本書の内容は予告無く変更することがあります。本文書のどの部分も NetScreen Technologies, Inc. の許可書なく、電子通信上ないしは機械上、如何なる目的にも如何なる形においても、あるいは如何なる手段においても、再生あるいは送信することはできません。

本文書のどの部分も 許可書なく、電子通信上ないしは機械上、如何なる目的にも如何なる形においても、あるいは如何なる手段においても、再生あるいは送信することはできません。許可書については、以下までお問い合わせください：

NetScreen Technologies, Inc.
Building #3
805 11th Avenue
Sunnyvale, CA 94089 U.S.A.
www.netscreen.com

Enterprise Security Profiler

ユーザーは、Enterprise Security Profiler の使用は国によって関連する法規制に違反しない限り、データ保護法なども含めて使えます。NetScreen はこの機能の使用が関連する法規制に適合することに関して一切表明および保証をしません。お客様がご自身の義務を理解するために、必要であれば、関連する法規制の下でアドバイスを受けてください。