



## IBM Security Network Intrusion Prevention System (IBM Security Network IPS) FAQ

### 用語

1	<b>シグネチャ</b>
	パケットの特徴を記述したパターン。このシグネチャとパケットとを比較することにより通信内容を調査し、不正なアクセスかどうか判断します。
2	<b>XPU(X-Press Update)</b>
	IBM Security Network IPSに対するアップデートモジュールおよびシグネチャ。IBM Internet Security Systems のWebサイトからダウンロードして、IBM Security Network IPSに適用します。
3	<b>ポリシー</b>
	IBM Security Network IPSにおける検知や防御などの設定内容。また、IBM Security Network IPS導入時に設定したポリシーを、IBM Security Network IPSが検知したログに基づき最適な内容に変更することをポリシーチューニングと言います。
4	<b>イベント</b>
	IBM Security Network IPSが検知した項目です。
5	<b>バーチャルパッチ</b>
	セキュリティホールに対する攻撃を防ぐシグネチャのことです。インターネットセキュリティシステムズの研究機関X-Forceから提供される脆弱性を検知・防御するXPUを適用することで外部からの攻撃に耐えられる状態となり、パッチを適用しているのと同じ状態にすることができるためバーチャルパッチと呼んでいます。(IPSモードで動作させる必要があります。)
6	<b>IBM Security SiteProtector(TM) System</b>
	IBM Security Network IPSに対する各種の設定や、検知したイベントのリアルタイム表示を行うための管理システム。ひとつのIBM Security SiteProtector(TM) Systemで複数のIBM Security Network IPSを管理することもできます。
7	<b>LMI(ローカルマネジメントインターフェース)</b>
	WebブラウザによるIBM Security Network IPSの管理・設定を行う画面です。
8	<b>誤検知</b>
	IDS/IPSの誤検知には2種類あります。 1.不正アクセスではない通信を不正アクセスとして検知すること(False Positive) 2.不正アクセスの通信を検知しないこと(False Negative)  これらの要因は2つあります。 要因1. 初期のポリシー設定が適切でないために発生する誤検知です。IDS/IPSを設置したネットワークにとって脅威でない通信(Webサーバのないネットワークに対するHTTPを利用した攻撃等)を不正アクセスとして検知することは、IDS/IPSとしては正しい動作ですが、ユーザーの観点では誤検知と言えます。IDS/IPSの構築時にポリシーを十分に検討しますが、運用を開始してからわかる誤検知もあるため、ポリシーチューニングを行って誤検知を減らします。 要因2. 製品にXPUを適用していない場合や、製品に障害がある場合などに発生する誤検知です。XPUの適用によって改善されます。



機能

Q1	IDSとIPSの違いは何ですか。
A1	IDSは、Intrusion Detection Systemの略で、ネットワークへの不正なアクセスを検知するシステムです。検知した不正なアクセスをネットワーク管理者に伝えるとともに、調査・分析作業を支援するために必要な情報を保存することを目的としています。 IPSは、Intrusion Prevention SystemまたはIntusion Protection Systemの略で、IDSの機能に加え、不正な通信をドロップするなど、不正なアクセスからネットワークシステムを防御するシステムです。
Q2	ワームの亜種の侵入を防ぐことはできますか。
A2	IBM Security Network IPSではバーチャルパッチによりシステムを守っています。IBM Security Network IPSはワームの攻撃パターンで識別しているため、ワームの実行ファイルの一部が変わった亜種が来ても、攻撃パターンは同じなので、侵入を防ぐことができます。
Q3	ブロック設定が可能なシグネチャ数はどのくらいありますか。
A3	約3200あります。(2011年06月時点)
Q4	Winnyの通信を検知、遮断することができますか。
A4	可能です。WinMX、Napster、Kazaaなどのファイル交換ソフトに対応しています。
Q5	SoftEtherの通信を検知、遮断することができますか。
A5	可能です。
Q6	正常なアクセスを遮断してしまうことはありますか。
A6	インターネットセキュリティシステムズの研究機関X-Forceが作成した推奨ポリシーをベースに運用するため、正常なアクセスの遮断はほとんどありません。しかし、業務に及ぼす影響を考慮してポリシーを設計する必要があります。
Q7	IBM Security Network IPSをブリッジのように動作させることはできますか。
A7	インラインモードで使用するにより、リアルタイムに不正なパケットを検知し防御することができます。
Q8	IBM Security Network IPSのモニタリングポートにIPアドレスを付与する必要はありますか。
A8	インラインモードで使用する場合は、パケットをモニタリングするポートにIPアドレスを付与する必要はありません。
Q9	管理サーバは必要ですか。
A9	IBM Security Network IPSの集中管理やログの蓄積には、専用の管理サーバが必要です。管理サーバにはIBM Security SiteProtector(TM) Systemという管理システムを導入します。IBM Security Network IPSの集中管理やログの蓄積をしないなら、Webブラウザでの管理が可能です。(一部の機種では専用の管理サーバが必須です。)管理サーバはシステム要件にあわせて、別途購入が必要となります。
Q10	管理サーバが止まってしまったらどうなるのですか。
A10	IBM Security Network IPSが動作していれば、問題なく検知・防御できます。管理サーバが復旧し、IBM Security Network IPSと疎通がとれるようになった段階で、管理サーバが停止していた間に検知・防御した情報が管理サーバに送られます。
Q11	インラインモードでIBM Security Network IPSを使用しているときに、IBM Security Network IPSがハード故障で停止した場合、通信はどうなるのですか。
A11	IBM Security Network IPSでは、すべての通信を通すことができます(フェールオープン)(一部機種では別売オプションが必要)。別売オプションを使用することで、フェールオープンとフェールクローズ(すべての通信を止める)を選択することができます。
Q12	IBM Security Network IPSにUPSは必要ですか。
A12	IBM Security Network IPSはHDDを持っているので、UPSを設置することを推奨します。ただし、UPS制御ソフトには対応していません。
Q13	IBM Security Network IPSがあればアンチウイルスソフトは不要ですか。
A13	ウイルスはワームと異なり、正常な通信により侵入することがある(メールに添付されるなど)ため、IBM Security Network IPSでは防ぎきれません。そのため、IBM Security Network IPS以外にアンチウイルスソフトが必要です。
Q14	IBM Security Network IPSは海外製品ですが、マニュアルや画面表示は英語ですか。
A14	日本語のマニュアルが用意されています。画面表示は英語です。
Q15	IBM Security Network IPS自身は攻撃対象になりますか。
A15	モニタリングポートはIPアドレスを持たず、管理ポート(管理サーバと接続するためのポート)は内部ネットワークに接続しているため、IBM Security Network IPSが攻撃対象になることはありません。



構築

Q16	IBM Security Network IPSは設置したらすぐに使えますか。
A16	インターネットセキュリティシステムズが提供する推奨ポリシーを使えば、すぐにご利用いただけます。なお、SSLではIBM Security Network IPSの構築を行うサービス(不正侵入検知・防御サービス(IDS/IPS 構築サービス))をご提供しています。
Q17	構築に関する作業項目と作業期間について教えてください。
A17	SSLの構築サービスでは、ヒアリングから構築まで1~2ヶ月、運用開始後のポリシーチューニングが1ヶ月程度です。
Q18	IBM Security Network IPSは、どこに設置すればよいのですか。
A18	社内のどこを守りたいか、その目的により異なります。[IBM Security Network IPS概要]
Q19	IBM Security Network IPSのポリシーはカスタマイズできますか。
A19	IBM Security Network IPSでは、インターネットセキュリティシステムズが提供する推奨ポリシーまたはネットワーク環境にあわせてカスタマイズしたポリシーを使用することができます。カスタマイズの内容は、個々のシグネチャごとの監視/非監視、検知時のレスポンスの設定などです。
Q20	IBM Security Network IPSがあれば、ファイアーウォールは不要ですか。
A20	IBM Security Network IPSには、IPフィルターによる簡易的なファイアーウォール機能があります。NATやルーティング機能は無いため、一般的なファイアーウォールの代替には向きません。
Q21	IBM Security Network IPSの冗長構成はできますか。
A21	機種により異なります。 冗長構成ができるのは、IBM Security Network IPS GX5xxx, GX6xxx シリーズです。



運用

Q22	製品のアップデートは自動化されていますか。
A22	設定により自動化できます。 定期的に新しいアップデートモジュールがないかを確認し、モジュールがある場合は、設定した時刻にモジュールの適用を行ないます。
Q23	シグネチャのリリース頻度はどのくらいですか。
A23	毎月1～3回程度(緊急パッチがなければ月に1回)リリースされています。
Q24	XPUはどのように適用するのですか。
A24	インターネット経由で最新のXPUをダウンロードして適用します。インターネットに接続されていない場合は、接続している他のPCからXPUをダウンロードすることで適用が可能です。
Q25	XPUを適用するのにどれくらい時間がかかりますか。
A25	XPUに含まれるシグネチャの数によっても違いますが、100MbpsのLANの場合、5～10分程度かかります。
Q26	ワームがどこから侵入したのかを確認できますか。
A26	管理システムIBM Security SiteProtector(TM) Systemの画面で確認できます。
Q27	レポートの作成ができますか。
A27	可能です。また、スケジュール機能により、自動化することもできます。
Q28	ログがいっぱいになったときは、どうすればよいのですか。
A28	必要なログはバックアップして、不要になったログを削除して下さい。 ログがいっぱいにならないように、定期的にログを削除することを推奨します。
Q29	運用開始後にはどのような作業項目がありますか。
A29	大きく分けて6項目あります。 1. IBM Security Network IPSおよびIBM Security SiteProtector(TM) Systemの稼働監視 2. イベント対応(誤報かどうかの確認、ネットワークシステムの対処、イベントの傾向を分析など) 3. IBM Security Network IPSへXPUの適用 4. ポリシーチューニング 5. ログのデータベースのメンテナンス(Q28参照) 6. 管理サーバへXPUの適用
Q30	保存可能なログの量はどれくらいですか。
A30	保存できる量はハードディスクの容量に依存します。なお、1イベントあたりのログの大きさは2～4KBです。
Q31	IDS/IPSのログを解析をすることで何ができますか。
A31	IDS/IPSを設置したネットワークへのアクセスの傾向を調べ、不正アクセスの予防や対策に役立ちます。



## 保守

Q32	保守内容について教えてください。
A32	3つの保守メニューがあります。 ・「ソフトウェア&セキュリティコンテンツサービスおよびテクニカルサポート&ハードウェア故障時先出しセンドバックサービス(年間)」(必須) XPUのダウンロード、Q&A対応、ハードウェア交換を行います。 ・「ハードウェア故障時オンサイトサービスオプション(対応時間:平日10:00~17:00)(年間)」(オプション) ・「ハードウェア故障時オンサイトサービスオプション(対応時間:24時間365日)(年間)」(オプション) ハードウェア故障時にお客様先で製品交換を行います。
Q33	保守契約を更新しないとどうなるのですか。
A33	初年度の保守契約は必須です。 次年度以降は更新しないと、XPUのダウンロード、Q&A対応、ハードウェアの交換といったすべてのサポートが受けられなくなります。
Q34	保守契約期間を教えてください。
A34	保守契約期間は1年です。継続する場合には、期間終了前に更新手続きをして下さい。

## その他

Q35	バーチャルパッチを持たない他社のIPS/IDSとの違いは何ですか。
A35	他社のIPS/IDSでは、脆弱性発表後やワーム発生後にシグネチャが提供されるため、シグネチャを適用するまでの間はネットワークを守ることができません。また、攻撃一つ一つに対してシグネチャが作られるため、ワームの亜種などのような、同じ脆弱性に対する攻撃からネットワークを守ることができません。

※記載の内容は、2011年6月現在のものです。

shaping tomorrow with you

社会とお客様の豊かな未来のために

〈お問い合わせ〉

株式会社富士通ソーシャルサイエンスラボラトリ

〒211-0063 川崎市中原区小杉町1-403(武蔵小杉タワープレイス)

Tel:044-739-1251

E-mail:ssl-info@cs.jp.fujitsu.com