

## スペック一覧

	GX4004C v2-200	GX4004C v2	GX5008C v2 GX5008SFP v2	GX5108C v2 GX5108SFP v2	GX5208C v2 GX5208SFP v2	GX7412SFP-S GX7412SFP-10 GX7412SFP	GX7800SFP
パフォーマンス <sup>*1</sup>	200Mbps	800Mbps	1.5Gbps	2.5Gbps	4Gbps	5Gbps 10Gbps 15Gbps	23Gbps
遅延	< 200µsec	< 200µsec	< 200µsec	< 200µsec	< 200µsec	< 100µsec	< 100µsec
新規接続数 (1秒間あたり)	35,000	35,000	37,000	40,000	50,000	600,000	650,000
同時接続セッション数	1,300,000	1,300,000	1,500,000	1,700,000	2,200,000	12,500,000	12,500,000
インライン・モード時 防御セグメント数	2	2	4	4	4	8	4
バッチ・モード時 監視セグメント数	2	2	8	8	8	16	8
Virtual IPS (Granular Policy)	○ (VLAN IDごと、IPアドレスレンジごと、監視ポートごと)						
監視用インターフェース <sup>*2</sup>	Copper 10/100/1000 × 4	Copper 10/100/1000 × 4	Copper 10/100/1000 × 8 またはSFPポート × 8	Copper 10/100/1000 × 8 またはSFPポート × 8	Copper 10/100/1000 × 8 またはSFPポート × 8	10Gbps SFP+ (SR/LR) または1Gbps SFP × 4 1Gbps SFP × 12	10Gbps SFP+ (SR/LR) または1Gbps SFP × 8
管理用インターフェースCopper	1 (10/100/1000)						
Reset 送信用インターフェースCopper	専用または監視用インターフェースから出力 (10/100/1000)						
ハイ・アベイラビリティ対応	○ (非対称ルーティング・ネットワーク、ロード・バランシング・ネットワーク等への対応)						
IPv6 イベント検知・防御	○ IPv6プロトコルについては、シグネチャの検知、防御に対応します						
筐体サイズ	1U <ラック・マウント>		2U <ラック・マウント>		3U <ラック・マウント>		
本体外寸 (W×H×D) mm	432×44×382		430×88×515		前部 479、 後部 439×133×662		
電圧/周波数	100-240V 50/60Hz						
電流 (A)	5.0		8.4		10		
消費電力	0.141 kW		0.389 kW		0.592 kW		
発熱量	0.481 kBTU/時		1.328 kBTU/時		2.02 kBTU/時		
重量 (kg)	11		18		25		
記憶装置冗長化 (RAID1構成)	— ○						
電源冗長化	— ○						
ファイブ機能	内蔵 外付 (オプション)						
安全認証基準	UL 60950-1, CAN/CSA C22.2, NO. 60950-1, (CE Mark), IEC 60950-1, GB4943, GOST, UL-AR						
EMC認証基準	FCC Class A, Industry Canada Class A, AS/NZS CISPR 22 Class A, EN 55022 Class A (CE Mark), EN 61000-3-2 (CE Mark), EN 61000-3-3 (CE Mark), EN 55024 (CE Mark), VCCI Class A, KCC Class A, GOST Class A, GB9254 Class A, GB17625.1						
環境規制	RoHS, WEEE および REACH						
サポート & サービス							
サポート & サービス内容	テクニカルサポート、X-Press Updateの更新、Firmwareの更新、ハードウェア交換						
テクニカルサポート内容	平日10:00~17:00 (土日祝日、弊社休業日を除く) メールサポート/電話サポート (サポート・インシデント数の上限なし)、サポート・ナレッジベースの閲覧						
備考	<p>*1 この文書に含まれるすべて (GX7800以外) のパフォーマンス・データは、Firmware Update バージョン 4.1 を使用した場合の、ある特定条件の動作環境下でのデータを標準的な値として提示しています。他の動作環境におけるパフォーマンスは異なる場合がありますので、ご使用予定の環境で事前に検証することをお勧めしております。スループットの計測はRFC2544標準 (http://www.ietf.org/rfc/rfc2544.txt) に基づき実施しています。ベンチマーク・テスト環境: GX7800 はファクトのインラインモードで、「Trust X-FORCE」ポリシーを使用。Spirent Avalanche 3100 firmware 3.50 (またはそれ以上) をテスト機器として使用。通信の種別の比率: HTTP=41%, HTTPS=17%, SMTP=10%, POP3=5%, FTP=9%, DNS=15%, SNMP=3%; HTTP/HTTPS 通信は 44Kbyte のオブジェクト・サイズの標準 HTTP/S 1.1 GET 要求を使用。DNS 標準 A レコード・クエリを使用。FTP GET 要求による 15000 bytes を 2ms でバースト転送する通信、POP3 通信は 100KB オブジェクト・サイズでユーザーのメールボックス間の通信を使用。SMTP はオブジェクト無しの単純な接続を使用。SNMP ステータス・クエリーと応答を使用。他の動作環境におけるパフォーマンスは異なる場合がありますので、ご使用予定の環境で事前に検証することをお勧めしております。</p> <p>*2 接続する対向の機器はリンク・スピードと全/半二重を固定設定できる機器のみをサポートいたします。</p>						

\* IBM、IBMロゴ、ibm.com、およびVirtual Patch、X-FORCEは、世界の多くの国で登録されたInternational Business Machines Corp.の商標です。他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。現時点でのIBMの商標リストについては、<http://www.ibm.com/legal/copytrade.shtml>をご覧ください。  
\* Microsoft、WindowsはMicrosoft Corporationの米国およびその他の国における商標。  
\* 他の会社名、製品名およびサービス名等はそれぞれ各社の商標。



### 日本アイビーエム株式会社

〒103-8510 東京都中央区日本橋箱崎町19-21  
06-11 Printed in Japan  
<http://www.ibm.com/iss/jp>  
e-mail [issales@jp.ibm.com](mailto:issales@jp.ibm.com)

●このカタログの情報は2011年9月現在のものです。仕様は予告なく変更される場合があります。●記載のデータはIBM社内の調査に基づいたものであり、全ての場合において同等の効果が得られることを意味するものではありません。効果はおお客様の環境その他の要因によって異なります。●製品、サービスなどの詳細については、弊社もしくはビジネス・パートナーの営業担当員にご相談ください。  
©Copyright IBM Japan, Ltd. 2011 All Right Reserved

## IBMセキュリティー

# IBM Security Network Intrusion Prevention System (IPS)

ファイアウォールでは防御できない

社内外の不正アクセスからお客様のシステムを守ります



## IBM Security Network Intrusion Prevention System (IPS)

IBM Security Network IPSは、お客様のネットワーク帯域や可用性を損なうことなく、悪意を持った攻撃を自動的にブロックする不正侵入防御(IPS)アプライアンスです。IPS業界をリードしてきた高度なプロトコル分析技術と、セキュリティー研究開発組織 IBM X-FORCEによる脆弱性や攻撃の情報、世界9拠点のIBMセキュリティー運用監視センターからのリアルタイムな攻撃インシデント情報をベースに、最新の攻撃から未知の脅威までを防ぐことができるセキュリティー・アプライアンスです。IBM Security Network IPSシリーズには、お客様のネットワーク環境やスループットの要件に柔軟に合わせることが可能なモデルを幅広く用意しています。



### 導入効果

- 進化するさまざまな攻撃や不正侵入からお客様ネットワークを強固に防御
  - Webアプリケーション・ファイアウォール(WAF)機能が昨今の脅威を防御
  - セキュリティー・パッチを即時適用できない危険な状態のサーバーを保護
  - マルウェア(ウイルス/ワーム)による被害の拡散、帯域の無駄な消費、情報漏えいを防止
  - 急増する Web 改ざんや誘導型攻撃を防御
- ※ ハイパーリンクなどを利用して攻撃用サーバーにクライアントを誘導し不正なファイルをダウンロードさせるWebを利用した攻撃手法を「誘導型攻撃」といいます。

### おもな機能と特長

● **Webアプリケーション脅威の防御機能(WAF)**  
激増するWebアプリケーションの脆弱性に対する攻撃(クロスサイト・スクリプティングやSQLインジェクション、ファイル・インクルードなど)を効率的かつ高精度に検知・防御できるインジェクション・ロジック・エンジンとそれに対応する約140個のWAF(Web Application Firewall)関連シグネチャー(※2011年6月時点)を標準装備。GUIからウィザード形式で簡単に設定が可能です。

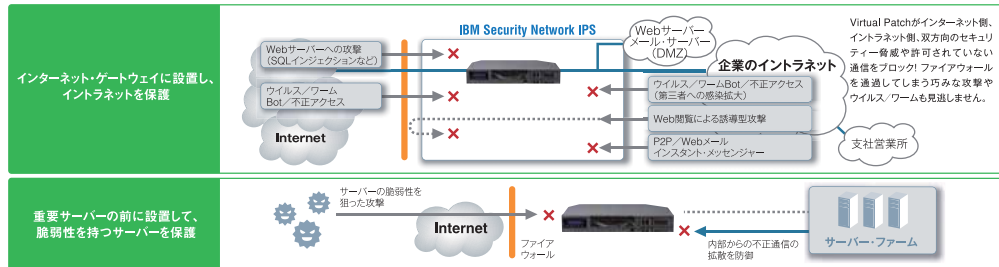
### ● PAM(プロトコル分析モジュール)

IBM Security IPSシリーズの中核をなす技術の一つであるPAMは、今日の大きな脅威とされている通信(ワーム、スパイウェア、P2P、DoS/DDoS、クロスサイト・スクリプティング、SQLインジェクション、パッファ・オーバーフロー、Webディレクトリートラバーサルなど)を検知、防御するために、240種類以上のネットワーク層、アプリケーション層のプロトコルや、ファイル形式の深層部分まで検査、防御することが可能です。

### ● セキュリティー・オペレーション・センター(SOC)によるIPSの監視と運用が可能

セキュリティー運用監視サービスIBM Managed Security Service (MSS)※を併せてご利用いただければ、監視センターSOCに常駐する専門に教育を受けたセキュリティー・エキスパートが、お客様のIBM Security Network IPSを24時間365日リモートで運用監視し、お客様のセキュリティー・アドバイザーとしてもサポートします。世界9拠点にあるSOCの情報連携で、迅速な対応を可能にします。

- ※ MSSは別途契約が必要です。
- 防御のための実装例



### X-FORCE

#### X-FORCEによる精度の高い検知・防御能力を実現

X-FORCEはIBMのグローバルなセキュリティー研究開発組織で、民間企業では世界最大級の規模を誇ります。主要なプロトコルやアプリケーションの脆弱性研究、攻撃や不正アクセス手法の調査をし、その分析成果を製品の防御エンジンやシグネチャーに反映させることで、非常に精度の高い攻撃検知、防御を実現しています。



### Virtual Patch

#### Virtual Patch(バーチャル・パッチ)による運行コスト削減

セキュリティー研究開発組織 IBM X-FORCEは、発見したOSやアプリケーションの脆弱性に関する分析結果を基に、その脆弱性を狙った攻撃を検知するシグネチャー(X-Press Update)を即座に開発してIBM Security Network IPSに反映させます。発見された脆弱性に対して仮想的にパッチが適用されている状態を作り出しバリエーションとして保護するVirtual Patch。セキュリティー・パッチが配布される前のゼロデイ攻撃を防御するとともに、システムに対するセキュリティー・パッチ適用計画を強力にサポートし、作業の軽減による運用コスト削減を実現します。



### Shell Code Heuristicエンジン

不正プログラムが使用するシェルコードを検知、防御するエンジンを搭載しており、未知の脆弱性を利用する攻撃による不正プログラムの実行を未然に防ぎます。

### 10Gbps 高速ネットワーク対応モデル GX7800

IBM Security Network IPS GX7800 モデルは、IBM Security Network IPSが持つ業界先進の事前防御機能のほか、次の特長を備えています。

- 10Gbps 以上の帯域の通信に対応
- 監視ポートに10Gbpsインターフェースを8個搭載可
- ネットワーク処理専用プロセッサを搭載し通信の遅延時間を劇的に低減
- PAM(プロトコル解析モジュール)バージョン2.0を搭載し解析パフォーマンスが大きく向上

## IBM Security SiteProtector(統合管理システム)

IBM Security SiteProtector(SiteProtector)は、IBM Security IPSシリーズを集中管理することができる統合管理システムです。各プロテクション・エージェントの設定・管理や検知・防御イベントの集積、リアルタイムな表示が可能です。さらに、複数の異なる種類のエージェントからの情報を相関分析したり、中長期的なイベント情報を、さまざまな視点から検索・解析することができます。SiteProtectorは、企業全体のセキュリティー・レベルを維持、向上させるための運用管理や意思決定を強力に支援します。



### おもな機能と特長

● **集中管理はもちろん、グループ管理も可能**  
論理的なグループを設定し、そのグループごとに IBM Security Network IPSシリーズの管理やイベントの表示、解析が可能です。

### ● ユーザー・アクセス管理

SiteProtectorを操作するユーザーに対し、標準のオペレーティング・システム権限モデルと同一の操作レベルを設定できます。また、このユーザー・アクセス権限は、論理的なグループに対して設定可能です。

### ● ポリシー管理

デフォルト・ポリシーおよびユーザーによるカスタマイズ・ポリシーを利用可能。カスタマイズ・ポリシーは、作成したグループ、もしくは個別のプロテクション・エージェントごとに適用できます。

● **シグネチャー X-Press Updateの自動更新とスケジューリング**  
SiteProtectorが、最新のX-Press Updateを自動でダウンロードし、各プロテクション・エージェントに自動配信、適用できます。この機能により、各プロテクション・エージェントを、常に最新の状態を保つことが可能。この自動更新機能は、もちろん、さまざまな操作・設定をスケジューリングすることができます。

### ● イベント・インシデント解析

デフォルトで提供している数十種類の表示方法以外に、必要に応じて柔軟にカスタマイズが可能です。例えば、ある時間までに検知されたイベント情報をベースラインとして登録し、時間経過に伴う検出イベントの変化を観察することもできます。

### ● グラフィカル・レポートと分析グラフの提供

グラフィカル・レポート、分析グラフ、さらに、レポートの定期的なジョブ・スケジューリングが可能。数十種類におよぶ解析情報を、HTML、PDF、CSV形式でレポート作成することができます。

### ● SiteProtector Web アクセス

Webブラウザ\*からセキュリティー・イベントを閲覧することができます。  
\* Microsoft Internet Explorer 7.0以上

### ● Microsoft Active Directoryとの統合

Microsoft Active Directoryのアセット情報と、SiteProtectorのアセット・グループを同期させ、セキュリティー・イベントとアセット、組織内のユーザーを迅速に関連付けることができます。

### ● セントラル・アラート機能

プロテクション・エージェントからのアラートを、いったんSiteProtectorにイベント通知し、しきい値または設定した条件によって、電子メールやSNMPレスポンスとして送信可能。例えば、1,000個の攻撃イベントを検知した際に、プロテクション・エージェントから1,000個の電子メールを送信するのではなく、SiteProtectorの条件に合致するイベントが1,000個通知された場合に、一通の電子メール、もしくは一つのSNMPレスポンスを送信できます。

### IBM Security SiteProtector 2.0 Service Pack 8.1

#### IBM Security Network IPS GXシリーズ・アプライアンスのサポートを強化

GXシリーズの認証サーバー、データ保護、SNMP、Webアプリケーション保護のポリシーのサポートを強化。Analysisビューでは、検出情報に対してマウスのシングル・クリックにより、攻撃元からの通信を継続的にブロック可能です。

#### 仮想サーバー保護製品IBM Security Virtual Server Protection for VMware(VSP)をサポート

VSPが保護する仮想マシンの詳細情報を、グルーピングしてAsset ビューに表示できます。

#### Analysis ビューでのスケジューリング・エクスポートやカテゴリが追加

カスタマイズした Analysis ビューを PDF、HTML、CSV および XLS 形式でスケジューリング・エクスポートできます。セキュリティー標準(CVE)、マイクロソフト社のセキュリティー・プレティン、IBM X-FORCEデータベースID、そして時間範囲(傾向分析用)など、ノートのための新しいカテゴリを追加しました。

#### Report ビューに2つのレポートが追加

- 1 仮想アセットのサマリー・レポートの追加。VSPで保護されている仮想マシン(VM)に関する情報のサマリー(ホスト名、DNS名、VM名、最終スキャン日、およびオペレーション・システム)を提供。
- 2 リスク評価ごとのイベント数レポートを追加。発信元、宛先、およびオブジェクト(高危険度、中危険度、低危険度および全イベント数)の数ごと、そしてリスク評価によってグルーピングし、システムに対する脅威情報を提供。

#### Microsoft Windows 7とIPv6をサポート

SiteProtectorは、エージェントとデュアル・スタックAgent ManagerとがIPv6で通信することをサポートします。IPv6を持つアセットとイベントを処理することもできます。IPv6のサポートは、発信元、宛先、およびオブジェクト(高危険度、中危険度、低危険度および全イベント数)の数ごと、そしてリスク評価によってグルーピングし、システムに対する脅威情報を示します。