IBM Security Network Protection XGS シリーズのご紹介

2016年1月15日
日本アイ・ビー・エム株式会社

実績を重ねてきたIBM Security IPS製品群の3大ポイント

IBM Security IPS製品群のIBMの強みは以下の3点です。

IBMの強み① IBM X-Force の脆弱性研究

- IBM X-Forceは世界的に有名なセキュリティー研究機関
- 多くの脆弱性を発見してきた実績
- このナレッジを製品に投入することで、新たな脅威にいち早く対応

IBMの強み② PAMによる高度な解析能力

- 独自のプロトコル分析ベースの複合解析技術により深いレベルまで通信を解析
- パターンマッチングや振る舞い分析に頼らないため、高い精度で攻撃からの防御を実現

※ PAM：Protocol Analysis Module(プロトコル分析モジュール)

研究 & 情報力

高い解析能力

IBMの強み③ 事前防御を実現するVirtual Patch® Technology

- 「X-Forceのナレッジ」と「PAMの解析力」の相乗効果により、攻撃手法や亜種の出現による影響を受けない保護を実現
- 脆弱性そのものを保護するため、Virtual Patch Technology を実現

比類のないグローバルカバレッジとセキュリティーナレッジ

IBMの強み①

- Security Operations Centers
- Security Research Centers
- Security Solution Development Centers
- Institute for Advanced Security Branches

IBM Research

IBM Institute for Advanced Security
Enabling cybersecurity innovation and collaboration

契約中のデバイス数: 20,000 超

世界中の管理対象顧客数: 3,700 超

1 日に管理されるイベント件数: 130 億超

モニター対象の国 (MSS) の数: 133

セキュリティー関連の特許件数: 3,000 超

X-FORCE

分析されたWebページ&イメージ数: 200 億

スパム & フィッシング攻撃件数: 4,500 万

文書化された脆弱性の数: 76,000

1 日あたりの侵入試行件数: 数十億

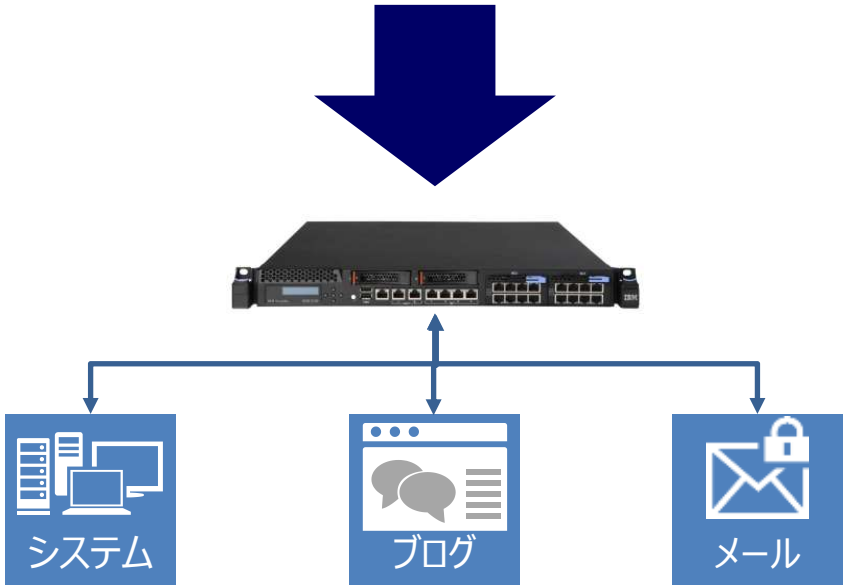
固有のマルウェア・サンプルの数: 数百万

X-Forceによる脅威に対するインテリジェンス

IBMの強み①

X-Force Threat Intelligence Cloud

- **X-Force データベース** – 広範囲な脆弱性のカタログ
- **WebフィルターDB** –悪質な感染したWebサイト
- **IPレピュテーション** – ボットネット、匿名プロキシ、悪意のユーザ
- **アプリケーションの識別** – Webアプリケーションの情報
- **脆弱性の研究**–最新の脆弱性と保護
- **セキュリティー・サービス** – 3000を超える顧客のIPS監視



複合解析技術　PAM(プロトコル解析モジュール)

IBMの強み②

IBM Security IPS 製品群の中核を構成する技術
- ●非常に軽く、超高速かつ正確な解析エンジン
- ●脆弱性を狙った攻撃そのものを検知
- ●ネットワーク・トラフィックの全てのレイヤーを検査するディープ・インスペクション
  - ➢ネットワークとアプリケーション層のプロトコル、データやファイル・フォーマットを解析し攻撃から防御

PAMに含まれる検出手法

脆弱性のモデル化とアルゴリズム解析	RFC準拠検査
ステートフル・パケット・インスペクション	TCPリアセンブル&フロー・リアセンブル
プロトコル・アノーマリー検知	統計分析
ポート非依存解析	ホスト・レスポンス分析
ポート・アサイメント解析	IPv6ネイティブ・トラフィック分析
ポート追随解析	IPv6トンネル分析
プロトコル・トンネリング解析	SITトンネル分析
アプリケーション・レイヤー・プリプロセッシング解析	ポートプローブ検知
シェルコード・ヒューリスティック解析	パターン・マッチング
コンテキスト・フィールド分析	カスタム・シグネチャー
コンテンツ分析	インジェクション・ロジック・エンジン、等

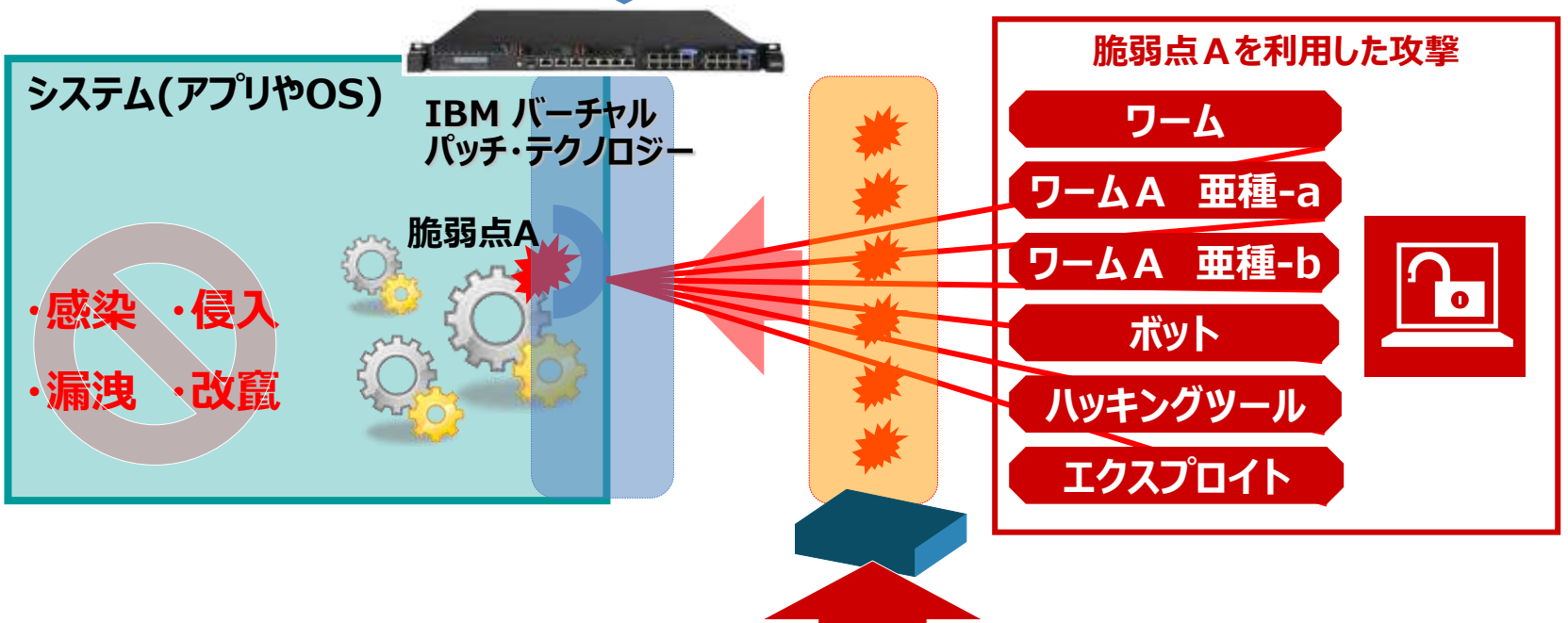
■ プロトコル認識・分析
・480以上のプロトコルとファイルフォーマットを分析可能

■ トラフィック分析
・5500以上のアルゴリズムに基づく脆弱性ベースの保護技術
※2015年7月時点

脆弱性視点だから実現できる バーチャルパッチ(Virtual Patch)

IBMの強み③

■ IBMのバーチャル・パッチ・テクノロジー(Virtual Patch)
- ✓ 脆弱点を自ら発見して防御処置を行う為、攻撃の事前防御が可能
- ✓ 一つのシグネチャーで効率的に防御し、運用負荷軽減
- ✓ 亜種や新手のハッキングにも対応



■ 他社 Patch (攻撃対応型)
- ✓ 発生した攻撃に対応する為、事後防御となる
- ✓ 一つの脆弱性に複数のシグネチャーが必要、運用負荷大
- ✓ 亜種など未検知の可能性もある

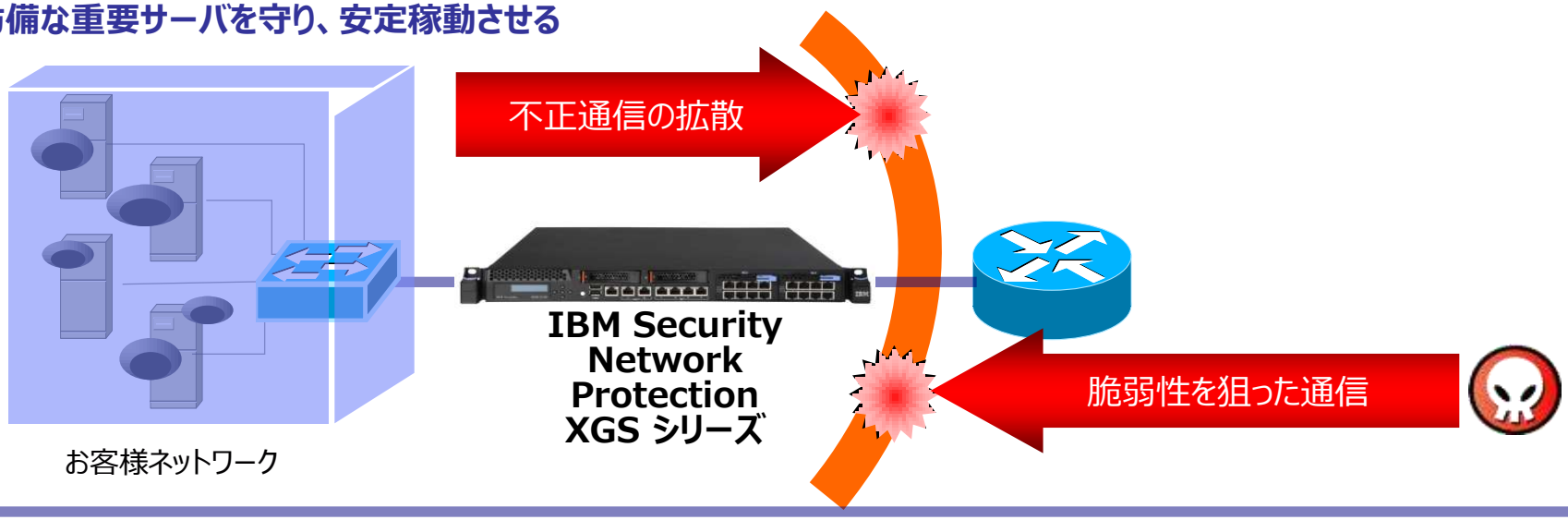
Virtual Patch® がバリア効果で保護を実現します

IBMの強み③

IBM Security Network Protectionが、脆弱性に対する攻撃を検知、防御することで、脆弱性が存在するサーバーに対して、仮想的にセキュリティー・パッチが適用されている状態を作ります。これがIBM の Virtual Patch テクノロジーです。
このテクノロジーは、IBM X-Force の脆弱性研究結果を反映させる事で、非常に高い検出精度を実現しています。

バーチャル・パッチによるバリア効果

無防備な重要サーバを守り、安定稼動させる



セキュリティーパッチ適用のタイムコントロールが可能です。

次世代型ネットワークセキュリティー・ソリューション
IBM Security Network Protection の特徴

実績を重ねてきたIBM Security Network IPS(旧名称：Proventia®シリーズ)の技術を継承しつつ昨今の脅威や利用形態にも対応するための様々な拡張を行っています

多段的な監視による保護
- ユーザー・グループ単位でアプリケーションを制御し不正通信の削減を実現
- トラフィック監査により悪用を素早く特定
- IPレピュテーション& Geo Location の活用
- FireEyeとの連携機能による保護

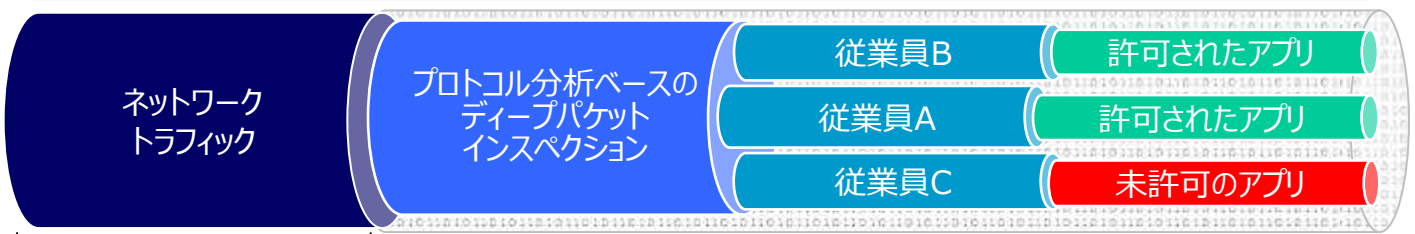
柔軟な拡張と操作性の改善
- フレキシブル・パフォーマンス・ライセンス
- ネットワーク・インターフェイス・モジュール
- SSL復号化機能
- 日本語化された管理インターフェイス
- QRadar 連携によるセキュリティー・インテリジェンス

Proventiaで実績を重ねてきた不正侵入防御技術の継承
- 独自のプロトコル分析の手法により脆弱性を狙った攻撃そのものを検知し防御を実現
- X-Forceの分析力と連携することでVirtual Patchを実現する中核機能

IBM Security Network Protection - ネットワークの可視化とコントロール

XGSは 既存の感染、不正なアプリケーション、および企業のポリシー違反 など、ブロックするコンテキストアウェアアクセス制御ポリシーを強制することができます。

IBM Security Network Protection XGS シリーズ



ネットワーク・フロー・データ

異常なアクティビティーのリアルタイム認識と、分析と相関を強化した QRadar 統合機能を提供します。

ディープ・パケット・インスペクション

アドレスやポートあるいはプロトコルに限定されずに、IP、ポート、プロトコル、アプリケーションを完全に分類します。

完全なID認識

ユーザーおよびグループと、ネットワークの利用、アプリケーション使用および活動を関連付けます。

アプリケーション認識

アドレス、ポート、プロトコル、アプリ活動 またはセキュリティ・イベントに関係なく、ネットワーク・トラフィックを完全に分類します。

当製品についてのお見積り･ご購入についてのお問い合わせはこちら

http://ibm.biz/Kiyohara

お問い合わせはこちら

清原 俊継

（きよはら としつぐ）

デジタル・セールス事業

RLM第一営業部