スマートフォンパケットの増加に伴う不正アクセス対策の見直し

Sniper® IPS

SecureSoft Sniper IPS

キヤノンITソリューションズ

http://www.canon-its.co.jp/

キヤノンMJ ITグループのキヤノンITソリューションズ（以下、キヤノンITS）の提案する不正侵入検知・防御アプライアンス「SecureSoft Sniper IPS（セキュアソフト スナイパー IPS。以下Sniper IPS）」。最近のスマートフォンパケットの増加に伴う、データセンターにおける不正アクセス対策の見直しについて聞いた。

不正アクセスの広がりとスマートフォンパケットで増加する検査量

2011年は、特定の企業や官庁に対する「標的型」の不正アクセスがニュースをにぎわせた。キヤノンITS・セキュリティソリューション事業部の五十嵐氏は「近年は、特定のハッカーが不正アクセスを試みるだけでなく、インターネット上に公開された不正アクセスの手法やツールを入手して、不正アクセスを試みる攻撃者が増えているため、結果的に集団的な行為となります」と、不正アクセスが広がっている背景を説明した。

ソーシャルネットワークサービスを提供する大手企業が、2011年10月に公表したデータによると、同社サービスへのアクセス件数は1日あたり10億件で、そのうち不正アクセスは60万件を超えるという。五十嵐氏は、「全体のアクセス件数の比率から見ると不正アクセスの件数は少ないですが、個人情報の漏えいやサービス停止などの事故が起きた場合、損害や信用に大きく影響します。安全・安心なサービスを提供するためには、不正アクセスの兆候を早期に検知し、未然に防ぐ備えを見直すことが必要です」と、不正侵入検知・防御システムの重要性を述べた。

最近では、どこでも容易にインターネットへアクセスできるスマートフォンやタブレットPCが急速に普及している。通信パケット量も膨大になり、データセンター事業者やコンテンツプロバイダーは、それに応じたレスポンスでのサービス提供が求められる。

スマートフォンパケットの多くは、文字データや情報の更新データなど、64byteまたは128byteの“ショートパケット”のデータである。「1500byteのデータを正常なパケットか不正なパケットか判断する場合、従来なら検査は1回ですむところ、ショートパケットの場合はおよそ20倍以上の検査量が必要になり、検査プロセスには大きな負担がかかります。今後さらに増大するショートパケットに対し、安定したスループットを維持できる不正侵入検知・防御システムの選定が必要になります」と五十嵐氏は語る。

高速性と高い検出率に加え日本語対応で運用性にも配慮

こうした状況のなか、同社が提案するのが、セキュアソフト社の不正侵入検知・防御システムの「Sniper IPS」だ。セキュアソフト社の森下氏は、「携帯電話向けコンテンツを提供する事業者さまにSniper IPSと、他社製品を含む3種のIPS製品についてスループット評価を行っていただいたところ、64byteや128byteといったショートパケットに対して、Sniper IPSが最も高いスループットを維持しました」と、その処理速度の高

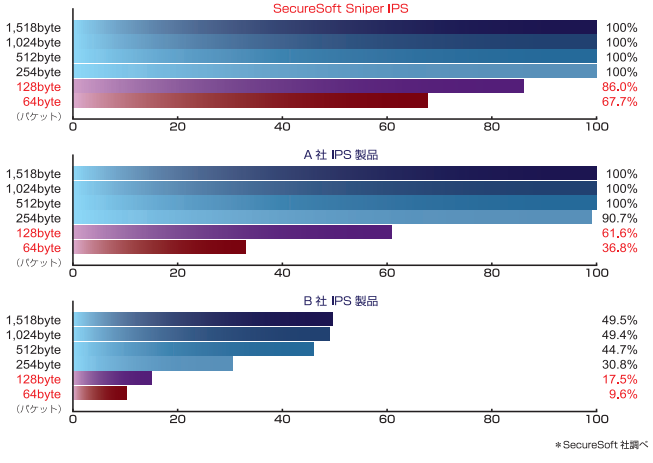

図1　各社IPS製品のスループット評価テスト（2Gbpsのスループット環境）

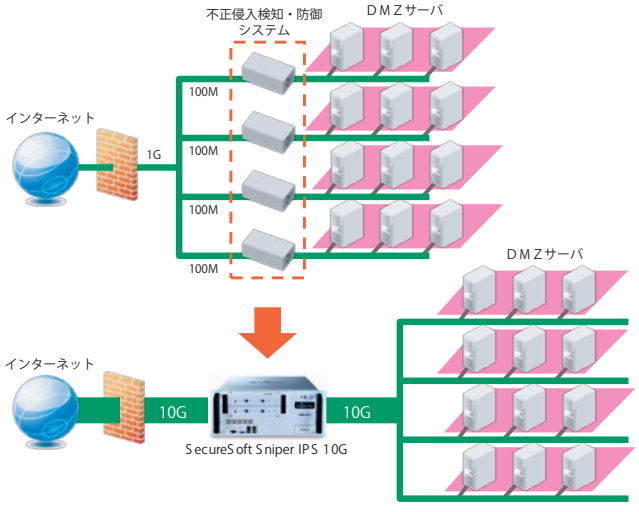

図2　システムを集約することで、管理・運用コストの削減が期待できる

さを説明した（図1）。

Sniper IPSには、ハードウェアスペックによりいくつかのバリエーションがある。なかでも、データセンター事業者など、大容量ネットワーク向けの最上位モデル「Sniper IPS10G」は、業界最速クラスの最大20Gbpsのスループットを実現。64byteのショートパケットでも19Gbps、128byteは20Gbpsと高いパフォーマンスを示した。

同様に、検知率について競合製品と比較検証を実施したところ、Sniper IPSが最も高い検知率を示した。「不正アクセスには、パケットを分割し（パケットのフラグメント化）、不正侵入検知・防御システムを回避する試みがあります。不正侵入検知・防御システムは、分割される前のパケットを再構築しないと検知できません。また、不正侵入検知・防御システムのなかには、分割されたパケットの再構築に負荷がかかるため、不正アクセスを検知できない機器もあり、その場合、検知率が低下してしまいます。Sniper IPSは、パフォーマンスに大きな影響もなく、分割されたパケットの検知をすることができます。」と森下氏は語る。Sniper IPSは、処理能力と共に検知能力も高い製品であることがわかる。

Sniper IPSなら、1つの筐体で検知・防御機能と管理機能を提供するため、管理サーバーが不要という手軽さも魅力の1つ。管理サーバーが別売となる他社製品と比較すると、導入やアップデート、保守の費用を抑えることができるという。

森下氏は、「Sniper IPS は、ネットワークの一番外側に設置しつつ、そこから枝分かれした複数のセグメント単位でポリシーを分けることもできます」と説明する。複

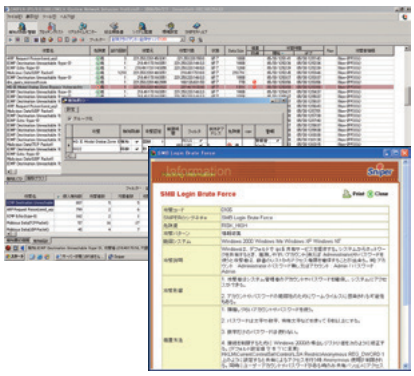

図3　管理画面や検出したイベントは完全日本語化対応されており、わかりやすい

キヤノンITソリューションズ
セキュリティソリューション事業部
セキュリティ企画部 セキュリティ商品開発課
課長　五十嵐謙知氏

セキュアソフト
営業本部
営業グループ
課長　森下渡氏

数のネットワークごとに不正侵入検知・防御システムを導入しているような環境であれば、Sniper IPS10Gだけにシステムを集約することで、管理・運用コストの削減も期待できるのだ（図2）。

またすべてのモデルで、電源やファンも標準で冗長化しており、電源故障、システムダウンなどにより、正常に起動しないといったハードウエア障害時にも、L2レベルですべての通信をバイパスできる安心の設計になっている。

さらに五十嵐氏が強調するのが、日本語に対応していること。Sniper IPSが選ばれる理由の1つだ。「一般的に不正侵入検知・防御システムは、管理ツールや検出した不正アクセスの解説が英語表記である場合が多く、専門的な用語を理解するのに時間がかかります。専任の技術者がいるデータセンターでは、従来のIPSでの運用経験があり英語表記の運用でも問題ないのかもしれませんが、直感的にわかる日本語表記のほうが、迅速に対応できるのではないでしょうか。データセンター事業者さまにおいては、お客さまに不正侵入検知・防御サービスを提供する上で、運用しやすく、わかりやすい解説のある製品が有効であると考えます」と五十嵐氏。

Sniper IPSは、検知した攻撃についてわかりやすい日本語で解説してくれる。これなら、担当者が急に変更になった場合でも迅速な対処が可能だ（図3）。

ユーザーのニーズに応えたセキュリティソリューションの提案を

不正アクセス対策は、2000年の初め頃から不正侵入検知システム（IDS）が主流だったが、2005年頃には不正侵入検知・防御システム（IPS）が主流になってきた。

「現在の市場は不正侵入検知システム（IDS）から始まって10年が経過し、リプレイスの需要が多くあります。導入をご検討されているお客さまが重視するのは実績と運用性です。Sniper IPSは、国内外で多くの実績があり、お客さまのニーズに応えることができる製品であると思います。今後も不正アクセスに対する品質の良い製品をセキュアソフトに求めていきたいと思います」と五十嵐氏は語る。

森下氏は、「新たに、DDoS攻撃対策の専用機『Sniper DDX』をリリースしました。DDoS攻撃は、ボットウイルスなどに感染し、外部からコントロールされた多数のゾンビPCが、インターネット上のサーバーに一斉に攻撃を行い、サービスを遅延させ、さらにサービスをダウンさせます。DDoS攻撃の場合、“攻撃”なのか"多数のアクセス"なのかを判断することが難しいとされていますが、Sniper DDXは、専用の解析エンジンで的確な検知・防御を実現します」と、専用機だからより効果的に防御できることを強調した。

最後に五十嵐氏に今後の展開について聞くと、「キヤノンITSでは、新たに西東京市に都市型次世代データセンターを建設中です。2012年10月にサービス開始を予定しています。最新鋭のファシリティとセキュリティ設備でお客さまのニーズに応えられるサービスを提供します。今後もSniper IPSをはじめ、安全・安心なサービスやソリューションをお客さまへ提案していきたいと思います」と語った。

問い合わせ先
キヤノンITソリューションズ
セキュリティソリューション事業部
電話番号　03-6701-3441
URL　http://canon-its.jp/product/ips/

インプレスビジネスメディア刊「データセンター完全ガイド2012年冬号」より転載