

システム提案活動の確度を上げる最終兵器

# 「次世代セキュリティテストアプライアンス」

企業が活動するために利用する情報システムは、常に変化の連続だ。システムインテグレータは、その変化の兆候をいち早く見越してシステム提案、企業の競争力向上を導くのが使命といえる。近年では、プラットフォームにクラウドという選択肢が生まれ、モバイルワーカーのワークスタイルを一新するスマートフォンやタブレット端末が登場し、システム提案の現場も様相が一変しつつある。

ソフトウェア分野も例外ではなく、Facebook や Skype などの新しいコミュニケーションツールの登場は、業務のあり方を大きく変革している。しかし、その一方でこうしたアプリケーションにより新しい脅威が生まれているのも確かだ。こうした脅威をどう可視化し、防御すべきか。また、こうした技術をシステムインテグレータはどう顧客に伝えるべきか。世界レベルの測定技術提供で定評のある東陽テクニカを訪ねて取材した。



INTEROP TOKYO  
2013  
セキュリティ部門  
特別賞  
Spirent Studio



**「Skype は許可したいけど、禁止したくもある」**  
情報システム部門の矛盾する  
悩みに Sler はどう応えるべき？

今日、Twitter や Facebook、YouTube、Skype、LINE などといったソーシャルメディアを始めとする革新的なアプリケーションが続々と登場、これらは個人の生活のみならず、今や企業の情報発信や情報収集、コミュニケーションのあり方に大きな影響を与えている。

たとえば Skype は、そのビデオ通話機能によって、相手を訪問することなしに会話や

お会議をすることが可能になった。実際、これ出張費を削減している企業も多いようだ。しかし、その一方で新しい脅威も生んでいる側面もある。この点について、株式会社東陽テクニカ 情報通信システム営業部 課長 野村周一氏は次のように語る。

「このアプリケーションにはファイル送信機能があり、文書や画像などのファイルを通信用相手に送ることができます。これまで情報システム部門は、情報漏えい対策として主に電子メール環境や USB メモリなど外部機器を監視してきましたが、それだけでは間に合わなくなってきました」

そう、情報システム部門は、大きな葛藤を抱えている。

“競争優位を維持するために、業務の生産性を向上させる新しい道具はどんどん使ってもらいたいが、脅威は抜け漏れのない形で徹底して封じたい”

システムインテグレータとして、このような情報システム部門の思いにどのような最適解を示すべきだろうか。

**こうしたニーズに対応して  
次世代セキュリティ製品が  
市場に続々登場**

幸いなことに、この分野にはこれまでにはなかったセキュリティ製品が登場し始めてい

る。次世代ファイアウォールや UTM (Unified Threat Management、統合脅威管理)、MPS (Malware Protection System、マルウェア防御システム) と呼ばれるものがそれらだ。

次世代ファイアウォールは、次世代といいつつも、提供する解決策はすでに現実的だ。従来のファイアウォールは通信ポートの開閉制御のみだったが、この新しいファイアウォールは、通信ポート内のアプリケーションを詳細に識別し、可視化し、制御することが可能だ。ゆえに、これを利用すれば、“Skype のビデオ通話機能は許可するけれども、ファイル送信機能は許可しない”といったきめ細かいセキュリティポリシーがそのとおり実行できる。

一方、UTM は、一台に複数のセキュリティ機能を搭載することをコンセプトにした製品である。ベースとなっているのはファイアウォールと VPN (Virtual Private Network) 機能で、そこに、アンチウイルス、不正侵入防御、Web コンテンツフィルタリングといった機能も含まれている。増加する一方のさまざまな脅威に対して、一台で効率よく対応できるのが大きな特徴だ。

MPS というのは、近年とみに悪質化している標的型攻撃に特化したセキュリティ機器だ。この攻撃に対応すべく構築したアルゴリズムに基づいて、これを検知し、被害が発生する前に除去を行う。



情報通信システム営業部 課長 野村周一氏

こうした新ジャンルのセキュリティ製品は、ITと脅威の進化に日々対峙する企業の情報システム部門にとって大きな希望であり、システムインテグレータにとっても新規案件を生み出す有力な提案商材だ。

### それらのカタログ値を Sler として自信を持って担保できるか？

しかし、コンセプトはすばらしいものの、いやコンセプトが画期的だからこそ、これらは決して安価ではない。また、新しく登場しただけに参考にできる実績も限られている。また、株式会社東陽テクニカ 情報通信システム営業部 SE グループ 課長 有地博幸氏は、こう語る。

「製品カタログに記載されている機能や性能値、導入効果は、入念に調整された環境で計測された最良値を示しています。自社の環境でその数値が実際に発揮されるかどうかは、また別の話になります」

そういう事情を知っているシステムインテグレータが「カタログ値比較では、A社、B社、C社、それぞれこうなっています」と顧客に対してただ告げるわけにはいかない。あるいは、それがいやなら、そうした製品が一定の導入実績を積みまで提案を控えるというのも一つの見識かもしれない。しかし、参入が遅くなればなるほど、製品に関する技術ノウハウ蓄積の機会も失うことになる。

### 次世代セキュリティテスト アプライアンス 「Spirent Studio」というソリューション

それでは、これらの製品を、自信を持って顧客へ提案するにはどうしたらいいか。この課題を解決するのが次世代セキュリティテストアプライアンス「Spirent Studio」だ。この製品は、新時代のセキュリティ製品をテストするために米国 Spirent Communications 社が開発した。

米国 Spirent Communications 社は、有線から無線、そして衛星に至るまで、キャリアサービスを利用するあらゆる顧客企業の QoE(Quality of Experience) を高める

ため、必要なソリューションを幅広く提供している通信用測定器専門メーカーである。1980年に設立以来、通信機器の性能試験器のパイオニアとして業界をリード、高速化を続けるイーサネット通信、VoIP、VPN、マルチプレイサービス、クラウドネットワーク & サービス、IPv6 ネットワークなどの各種有線 IP サービス導入において強力なイニシアチブを發揮している。

そうした中、同社は「Spirent Studio」を、多様化・高度化するサイバー攻撃を疑似し、ネットワークセキュリティの堅牢性を評価する専用アプライアンスとして開発した。製品体系として大きく「Spirent Studio Security」と「Spirent Studio Performance」の2つがある。

これらは、ネットワーク上の脆弱性を誘発するファジング試験、Malwareを含む既知の脆弱性攻撃、DDoS 攻撃に対応しており、次世代ファイアウォール、UTM、MPSなどのセキュリティ製品を効率よく評価することが可能だ。また、Skype や YouTube などのアプリケーショントラフィックを自ら生成し、IP パケットのデータ部分の情報から、フィルタリングの是非を判断する DPI (Deep Packet Inspection) 機能の検証やセキュリティポリシーの最適化など多様な試験が行える。

### 数千もの攻撃パターン、試験パターンに対応、被試験対象機器の実力を実測定で把握可能

具体的に機能を見ていこう。まず「Spirent Studio Security」だが、この製品は各種攻撃トラフィックの生成、被試験対象機器の振る舞いの監視を行う。標準で 75 種類以上のプロトコル・ファジングに対応しており、Unix 系 OS や Windows OS の pcap(packet capture) ファイルをインポートすることでカスタム・ファジングも可能で、アプリケーションに内在する脆弱性を強力にあぶり出す。

また、2,300 種類以上の既知の脆弱性、2,900 種類以上のシグネチャを含む攻撃、さまざまなネットワーク階層への DDoS 攻撃について熟知、詳細な試験・分析が可能である。

さらに、昨今ますます巧妙化している標的型攻撃に備え、Malware 感染経路を疑似することもできる。

他方、「Spirent Studio Performance」は、トラフィックが混在した現実のシステム環境を想定しながらアプリケーションの振る舞いをリアルに疑似、被試験対象機器の監視を行ったり、性能を試験することができる。その数、初期導入時で 3,500 シナリオ以上。リアルなアプリケーショントラフィックを作り出すことができる。

また、1,000 種類以上の Malware に感染した PC の振る舞いをエミュレーションしたり、Malware を始めとしたセキュリティ脅威の感染経路の疑似を行うことも可能だ。

### 最新パターンがアップデートされ続ける 「Spirent TestCloud」

これらに加えてこの製品の大きな魅力は、「Spirent TestCloud」の存在だ。有地氏は語る。

「このクラウドは、Spirent Communications 社が「Spirent Studio」のために立ち上げたサービスで、セキュリティテクノロジーの最前線で日々活躍する同社の精鋭エンジニアが厳選した最新攻撃パターンや最新試験コンテンツの定期的なアップロード、サポート契約を結んだ「Spirent Studio」ユーザーはこれをいつでもダウンロードできます」

そのため初期導入でも数千、来年予定されているアップデートでは数万種類を超え



情報通信システム営業部 SEグループ 課長 有地 博幸氏



る攻撃パターンや試験パターンを装備することが可能だ。また、このアップデートではC&C(Command&Control)サーバとのCall Backなどを疑似する機能も含まれる。このクラウドサービスがあるからこそ、「Spirent Studio」ユーザーは企業情報システムの実態に即したセキュリティ機器性能試験が行えるというわけだ。

「Spirent Studio」は、アプライアンスとして高い製品完成度を誇っている。たとえばMalware スキャンングテストでは、「Spirent Studio Security」のクライアントポートから被試験対象機器を経由して「Spirent Studio Security」のサーバポートへ HTTP リクエストを出す。すると、「Spirent Studio Security」のマネジメントポートが外部 Web サーバから Malware 検体を取得、それをサーバポートから再び被試験対象機器を経由してクライアントポートへサーバからの応答として返す。企業情報システム環境をリアルに疑似して試験が行えるため、試験環境の構築が非常に容易だ。



図 1 最新コンテンツを提供する「Spirent TestCloud」

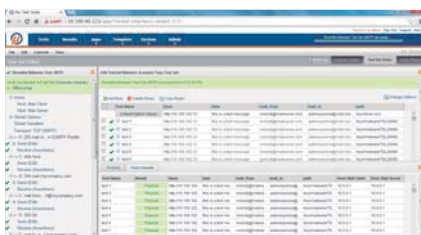


図 2 「Spirent Studio Security」を使用した Malware スキャンング試験実行例

管理用 GUI も業務効率に配慮して極めて視覚的に設計されており、Malware の検知率など試験結果は一目で把握できるようになっている。また気にかかる問題点は思考の流れに沿って次々ブレークダウンすることが可能だ。レポートもグラフやチャートを多用して視認性の高いものとなっており、加工の手間をかけることなく会議や提案の場へ提出することが可能である。

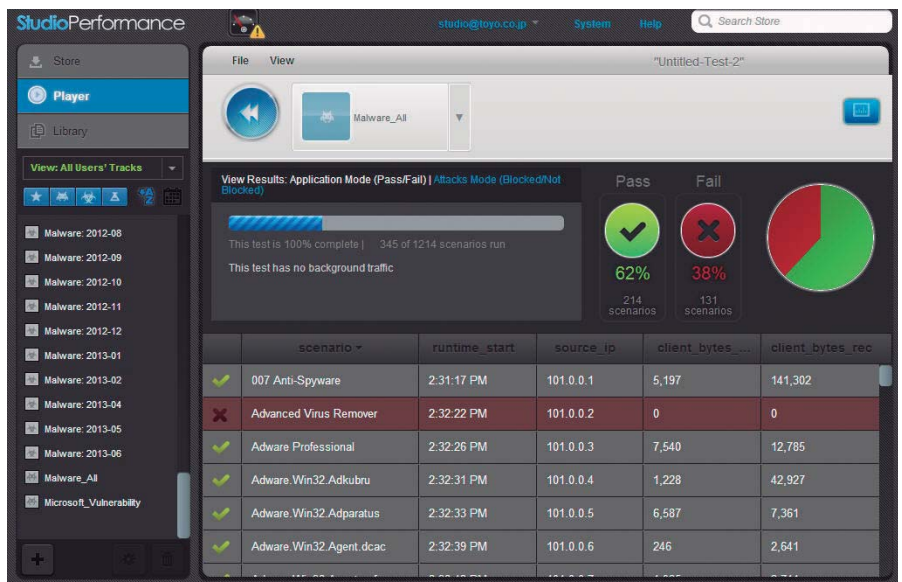


図 3 「Spirent Studio Performance」を使用した Malware 検知率測定試験実行例

### 顧客企業それぞれの実情に合わせた製品選定と推奨で信頼度を上げる

つまり、「Spirent Studio」を利用することによって、次世代セキュリティ製品の実質的な性能を測定することが可能になる。それも、システム提案しようという顧客企業の情報システム環境に焦点を合わせた設定で機能を測ることができる。野村氏は、この点について次のように語る。

「根拠に乏しい“一般的な評価”ではなく、「こういう結果が出ましたので、御社の環境で一番性能を発揮するのは〇〇社製品です」と裏付けとなる測定値を示しながら自信を持って訴求できます。どの顧客企業にも同じソリューションを提案して反応を見るのではなく、それぞれ適切なソリューションを提案できるので、案件受注の確度も大きく上がります」

さらに、この製品はセキュリティ製品を販売した後のアフターサービスでも、末永く活用できる。企業で活用されるソーシャルメディア系アプリケーションはバージョンアップも早く、そのたびに新たなセキュリティポリシーを確立する必要があるが、そうしたタイミングに、顧客企業に対してこの製品を使ったアドバイスやコンサルティングをタイムリーに展開することが可能だ。

結果として、この製品を基に顧客企業との間に内容の充実した対話の機会が増え、システムインテグレータとしての技術力を証

明するとともに、それが信頼度向上にもつながる。このビジネスは今後ますます、自らの実力を定量的にアピールする必要がある増えてくるだろうが、「Spirent Studio」はその意味で格好の道具となるように思った。

東陽テクニカでは、このアプライアンスを実地に見てみたいという顧客向けに、有償貸出しおよびサポートサービスキャンペーンを展開しているが、好評につき現在、期間を延長して実施している。「Spirent Studio 8010 モデル (1G&10G 共にマルチモードファイバ対応)」を、2週間から1ヶ月間 (詳細は別途) を機器使用中のサポートを含めて特別価格 (50万円～) で貸し出す。機器台数に限りがあるためすべての申し出に答えることはできないが、最先端のワークスタイルとセキュリティ対策の両立を検討する絶好のチャンスである。前向きに応募してみてはいかがだろうか。

株式会社 東陽テクニカ 情報通信システム営業部  
Spirent Communications社製品窓口  
〒103-8284 東京都中央区八重洲1-1-6  
TEL.03-3245-1250 (営業直通) FAX.03-3246-0645  
URL. http://www.toyo.co.jp/spirent/studio/  
E-mail. studio@toyo.co.jp

Spirent Studio C100 シリーズ



東陽テクニカ