セキュリティ対策への大いなる誤解、2つの図で理解する投資対効果を最大化する方法

企業向けのセキュリティ製品には、さまざまな種類がある。それぞれに特徴があるが、確実にいえることは、単体ですべてをカバーできる製品は存在しないということだ。したがって、企業には限られた予算内で複数の製品を選び、組み合わせて、セキュリティを高めることが求められる。では、どのように組み合わせるのがベストなのか。考え方のポイントを探った。

セキュリティのROIを考えるには「順番」が重要

企業が導入すべきセキュリティ製品には、さまざまな種類がある。ウイルス対策やファイアウォールはもちろん、不正侵入を検知・防御するIDS/IPS、Webアプリケーション対策としてのWAF、DDoS対策のアプライアンスやクラウドサービス、さらにはサイバー攻撃をリアルタイム監視するSIEMなど。1つの製品ですべてを守りきることは難しく、さまざまな製品を組み合わせて「多層防御」をとることが当たり前になっている。

もちろん、潤沢な資金を持つ一部の大企業であれば、こうした製品をすべて導入し、セキュリティを高めることは可能だろう。しかし、ほとんどの企業には、そんな余裕はない。限られた予算をやりくりしながら、セキュリティを最大限に高めなければならない。

ここで以下の図1を見てほしい。この図の縦軸はセキュリティ強度（不正アクセスからの防御効果）、横軸は導入するセキュリティソリューションへの投資金額を表している。

各セキュリティソリューションは、多層防御のもとに累積的に導入することになる。このことから、各セキュリティソリューションの投資金額と効果範囲をイメージした円を、グラフの右上にずらしながら記載している。

右側にあるものほど、投資金額の割に、セキュリティ強度の上昇が抑えられる傾向にあると気づかれると思う。これは右側にあるものほど、その箇所より左側にある累積されたソリューションからすり抜ける攻撃をとらえるものとしてリリースされたものであり、脅威の対象が減ってくることから、おのずと防御効果も抑えられるという考え方に沿ったものである。

効果が抑えられてしまうからといって、たとえばサンドボックスやSIEMの導入を、ウイルス対策そしてIPSよりも先に検討することは控えたい。これらは基本的に導入・運用工数がかかるものである。

このため、ウイルス対策やIPSによるフィルタリングが十分にされていない状況下で、これらのソリューションを導入すると、運用工数が飛躍的に上昇し、扱いきれなくなる懸念が出る。

つまり、ここでのポイントは、コストパフォーマンスを考えた場合、「導入するセキュリティ製品には正しい順番がある」ということだ。

次に導入範囲の視点でみてみよう。ほとんどの一般企業においてはインターネットをはじめとしたネットワークに接続して業務を行うスタイルであることからも、ファイアウォール、ウイルス対策、そしてIPSを最低限導入する範囲としている。そして大企業や機密情報を取り扱う企業であるほど、SIEMまでを含んだセキュリティソリューションの導入検討が望まれる。より高度な、すり抜ける攻撃に対応するためだ。

そしてコストパフォーマンス曲線のグラフについて、2点注目する箇所がある。1点目はセキュリティ効果の上昇がIPSを境に鈍化すること。2点目はコストパフォーマンスの曲線そのものが、2つある点だ。

1点目については脅威の侵入経路を考えてみた場合に、ウイルス対策による保護経路とIPSによる保護経路の2経路があることが要因となる。それぞれの経路の保護を行うソリューションの導入により、セキュリティ強度は順調に上

セキュリティソリューションへの投資対効果のイメージ

●右にあるセキュリティソリューション程、その箇所より左側にある累積されたソリューションからすりぬける攻撃をとらえるものとしてリリースされたもの
●左にあるセキュリティソリューション程、成熟しており価格も落ち着いている

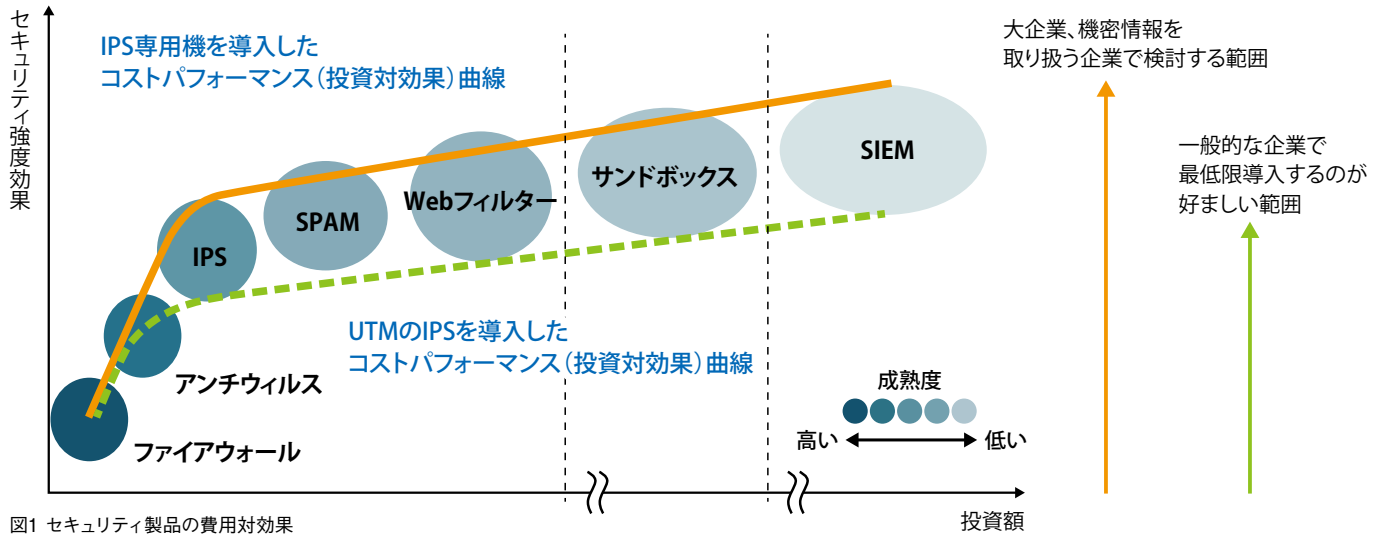


図1 セキュリティ製品の費用対効果

セキュリティ対策への大いなる誤解、2つの図で理解する投資対効果を最大化する方法

セキュリティソリューションの導入状況からみる危機的状況

ウィルス対策	回答数	導入済み	導入予定	予定なし	知らない	導入済み%	未導入%
大企業(1,000人以上)	1102	829	134	93	46	75.2%	8.4%
中堅業(300～999人)	674	502	68	82	22	74.5%	12.2%
中小業(300人未満)	870	714	42	87	27	82.1%	10.0%
ファイアウォール/UTM	**回答数**	**導入済み**	**導入予定**	**予定なし**	**知らない**	**導入済み%**	**未導入%**
大企業(1,000人以上)	1102	765	135	132	70	69.4%	12.0%
中堅業(300～999人)	674	442	102	86	44	65.6%	12.8%
中小業(300人未満)	870	572	79	158	61	65.7%	18.2%
スパム/フィッシング対策	**回答数**	**導入済み**	**導入予定**	**予定なし**	**知らない**	**導入済み%**	**未導入%**
大企業(1,000人以上)	1102	647	182	183	90	58.7%	16.6%
中堅業(300～999人)	674	357	102	157	58	53.0%	23.3%
中小業(300人未満)	870	388	80	297	105	44.6%	34.1%

どの企業層にも安定的に導入されているセキュリティソリューション

IDS / IPS	回答数	導入済み	導入予定	予定なし	知らない	導入済み%	未導入%
大企業(1,000人以上)	1102	478	195	252	177	43.4%	22.9%
中堅業(300～999人)	674	229	109	224	112	34.0%	33.2%
中小業(300人未満)	870	166	84	431	189	19.1%	49.5%
標的型攻撃対策	**回答数**	**導入済み**	**導入予定**	**予定なし**	**知らない**	**導入済み%**	**未導入%**
大企業(1,000人以上)	1102	558	202	213	129	50.6%	19.3%
中堅業(300～999人)	674	262	133	194	85	38.9%	28.8%
中小業(300人未満)	870	199	101	405	165	22.9%	46.6%

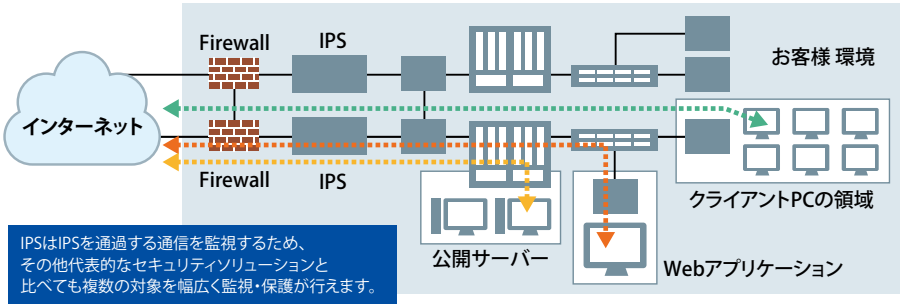
企業層にて導入率に差があるセキュリティソリューション

出典：ITR「IT投資動向調査2017」

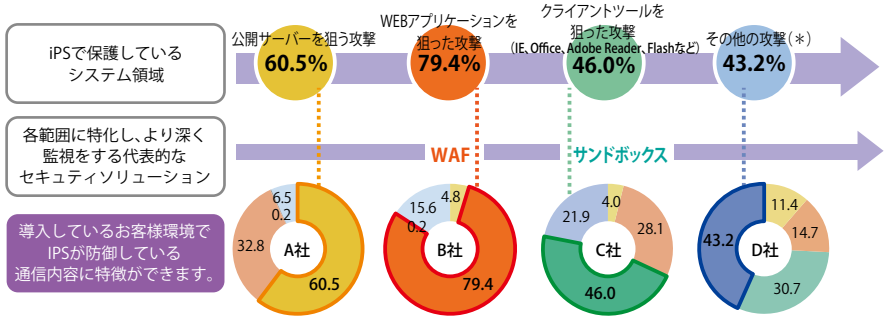
特にIDS/IPSの非導入状況は、クライアントPCへの攻撃が盛んになっている現状からも危険な状況であるといえます。

図2 セキュリティ製品別の導入状況

IPSの魅力（広範囲N不正アクセスに対応しているIPSの具体例）



IBMの監視サービスMNSSでのお客様における
特定顧客の1ヶ月間でIPSにて防御した通信の種類とその割合（単位：%）



通信の種類の項目は検出イベント名より分類分けをしています。割合は防御した通信件数より算出しています。
（*）情報収集関係や通信バイパスなど（本来HTTPである通信をSMTP通信に入れ込むなど）

図3 IDS/IPSの効果は公開サーバ、Webアプリケーション、クライアントPCのすべてにおよぶ

昇するが、それ以降のソリューションについては、同じ経路の保護を厚くするものであるため、上昇傾向が鈍化されることになる。

2点目はUTMに搭載されているIPSの使用時における強度上昇が抑えられる点である。

それぞれの詳細については後述する“IDS/IPSの導入率が低い理由とIDS/IPSを導入しないと危険である理由”、“無料やおまけのIDS/IPSでは不十分な理由”の項で伝えることにする。

では実際のセキュリティ製品の導入率はどうなっているのか。図2は「国内IT投資動向調査報告書2017」によるセキュリティソリューションの導入状況についてたずねた結果だ。これによると、ウイルス対策やファイアウォールなど、従業員規模で高い導入率を示しているものもあるが、IDS/IPS、標的型攻撃対策などは、企業規模別で大きな差がみられた。こうした「ギャップ」のあるものについては、本来入れておくべきものを入れていない傾向にある製品と言える。

IDS/IPSの導入率が低い理由とIDS/IPSを導入しないと危険である理由

次に、図1と図2を合わせて見ていただくと、導入するセキュリティの順番が誤っているのが、「IDS/IPS」だということがお分かりいただけるのではないだろうか。日本アイ・ビー・エム セキュリティー事業本部 セキュリティー・システムズ事業部 落合宏俊 氏は「IDS/IPSは非常にコストパフォーマンスの高い製品です」と胸を張る。

IDS/IPSの歴史は長く、もともとファイアウォールやウイルス対策の弱点を補う対策として登場した。IPSは「Intrusion Prevention System」の略で、サーバやネットワークの外部との通信を監視し、侵入の試みなどの不正アクセスを検知して攻撃を未然に防ぐシステムだ。また、IDSは「Intrusion Detection System」で、検知を主目的としている点が異なる。

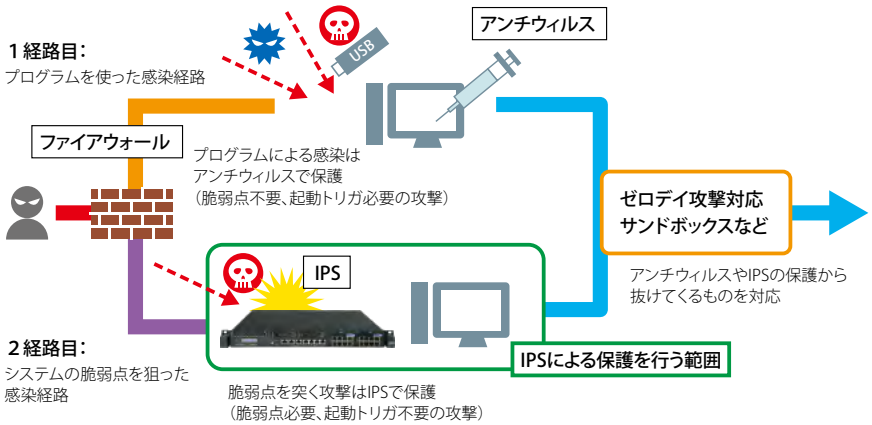
IDS/IPSのメリットの1つは、ネットワークのすべてのデータを監視するため、カバー範囲が広いということ。したがって、単に成熟度が高く、価格がこなれているからというだけではなく、カバーエリアの広さからもコストパフォーマンスが高くなるのである（図3）。

「たとえば、クライアントPCに対する未知の攻撃を防ぐうえで、サンドボックスは非常に効果の高いソリューションです。ただし、その役割は、既存のセキュリティ対策をすり抜けてきた未知のマルウェアを検知することがメインであり、価格も決して安いとはいえません。一方のIDS/IPSは、システムの手前でネットワークのデータを監視するため、クライアントPCの保護に加えて、サーバやWebアプリケーションの保護も行え、カバー範囲も広いです。またIPS独自の仕組みにて未知のマルウェアを検出できるケースもあります。これらのことからも、IDS/IPSはその必要性を、もっと見直されるべきだと思います」（落合氏）

では、考えるべきはコストの面だけなのかというと、もちろんそうではない。そこで考える

セキュリティ対策への大いなる誤解、2つの図で理解する投資対効果を最大化する方法

2経路ある標的型攻撃（IPS未導入時は2経路目が、ガラ空き状態）



1経路目:
ウィルスなどメール添付にあるようなプログラムを使った経路。プログラムであるために添付ファイルを開くなどのユーザーによるトリガーが必要だが、稼働環境があれば脆弱点のないシステムであっても活動する。この経路はアンチウィルスやアンチスパムがシステムの保護を担当する。

2経路目:
システムの脆弱性を突いて管理者権限をとる攻撃であるため、ユーザーによるトリガを必要としない。脆弱点はクライアントPCが使うInternet ExplorerやAdobe Acrobat ReaderやFlashまで及ぶ。この経路をIPSにて保護を担当する。なお、IPSは独自の仕組みでゼロデイ対応を行っている。

図4 標的型攻撃は2経路あり、IPS未導入時は2経路目がガラ空きになる

UTM保護における懸念

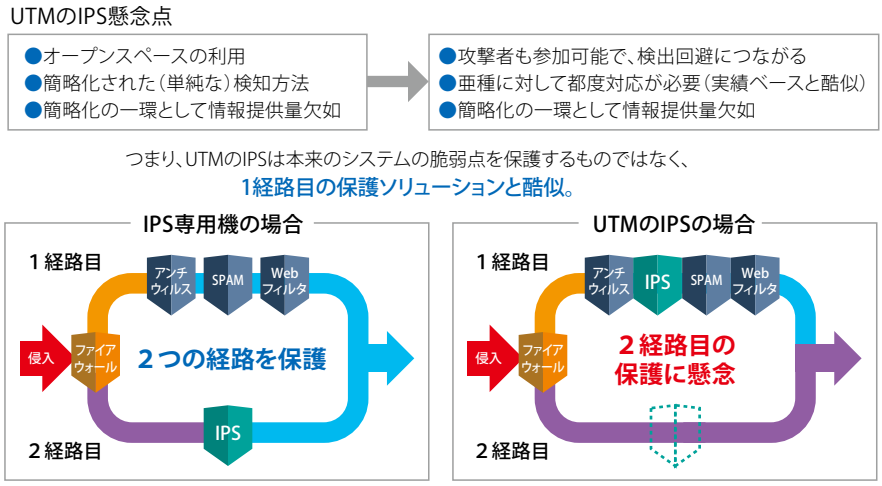


図5 UTMによる保護が十分ではない理由

べきが、セキュリティインシデントの「2つの経路」だ（図4）。

「標的型攻撃の経路は大きく2つあります。1つは、ウイルスなどの『プログラム』を使った経路です。プログラムであるため、添付ファイルを開くなどのユーザーによるトリガーが必要ですが、まったく脆弱性のないシステムでも攻撃が可能です。もう1つは、システムの『脆弱性』を突いた攻撃です。こちらは、ユーザーによるトリガーを必要とせず、脆弱性がいきなり侵入を許してしまいます。前者で有効なのがウイルス対策、後者で有効なのがIDS/IPSで、これらは相互に補完する関係なのです」（落合氏）

IDS/IPSはネットワークを流れるデータを監視して、シグネチャに基づいて不正アクセスを検出・防御する。また、脆弱性を埋める「パッチ」をメーカーに代わって提供することもあるため、高度な製品を導入しなくても「ゼロデイ攻撃」にも対応できることがある。このように、脆弱性を狙う攻撃をシステムの手前で防ぐのである。

無料やおまけのIDS/IPSでは不十分な理由

とはいっても、ユーザーによっては「いまはUTMの中に備わっているIDS/IPSを利用しているから大丈夫」「オープンソース（OSS）のIDS/IPSを導入しているから問題ない」と考えているかもしれない。しかし、落合氏は「そこには大いなる誤解があります」と説く。図5を見てもらいたい。

「複数のセキュリティ機能を1つのハードウェアに統合したのがUTMですが、UTMに含まれるIDS/IPS機能は、あくまで付加的なもので、本来の脆弱性を保護する仕組みやゼロデイ攻撃への対応という点で、決して十分とはいえません。これはOSSについても同様です。また、ネットワークの間に立つため、パフォーマンス劣化を恐れて、機能をオフにしているようなケースもあります。このようにみますと、これらはあくまでも攻撃の実績ベースを元にした保護であるため、攻撃経路の2経路のうちアンチウイルスによる保護がメインとなる1経路目しかカバーできないのです。そしてUTMでみますと、複数のセキュリティ機能があっても、結局は攻撃の実績ベースの保護となる1経路目の厚みを増すものばかりで、2経路目の対応がしきれていない結果となりかねないのです」（落合氏）

なぜこれらのIDS/IPSが、アンチウイルスによる保護がメインとなる1経路目と同一視されるのか。理由は以下のようになる（図6）。

IDS/IPSによる脆弱点の保護手法は大別して2種類ある。1つ目はシステムの脆弱点を狙う個々の攻撃に対応するシグネチャを都度追加して保護を行うもの。2つ目は脆弱点そのものに対応したシグネチャによって保護を行うものである。

1つ目の保護手法である攻撃ごとのシグネチャ対応というのは、アンチウイルスでいう亜種への対応に酷似している。つまり、実際の攻撃が確認できた上での都度の対応になり、この視点から実績ベースとする1経路目の保護と同じになるのである。

さらにOSSのIDS/IPSの場合は、その特徴から攻撃者もOSSコミュニティに参加しており、リリースされるシグネチャを回避する攻撃が出てくる懸念がある。

「これら重要な内容が、導入を検討するユーザー企業に伝わらない要因の1つとして、セキュリティソリューションの評価を行っている第三機関である NSSの評価結果があります。最近のIPSの評価結果では、ほとんどのメーカーのIPSにおける検出率の結果が90%台です。IPSの提案を行う企業が、この検出結果のみを導入検討するユーザーに伝えます。するとユーザーも検出性能の結果として、90%台であれば性能面は了解できるものとして、コストを意識したUTMのIPSを選択しがちです。こうなると1経路目のみの対応となるソリュー

セキュリティ対策への大いなる誤解、2つの図で理解する投資対効果を最大化する方法

亜種に依存しないパターンの提供により、亜種を使った脅威に事前対応する例

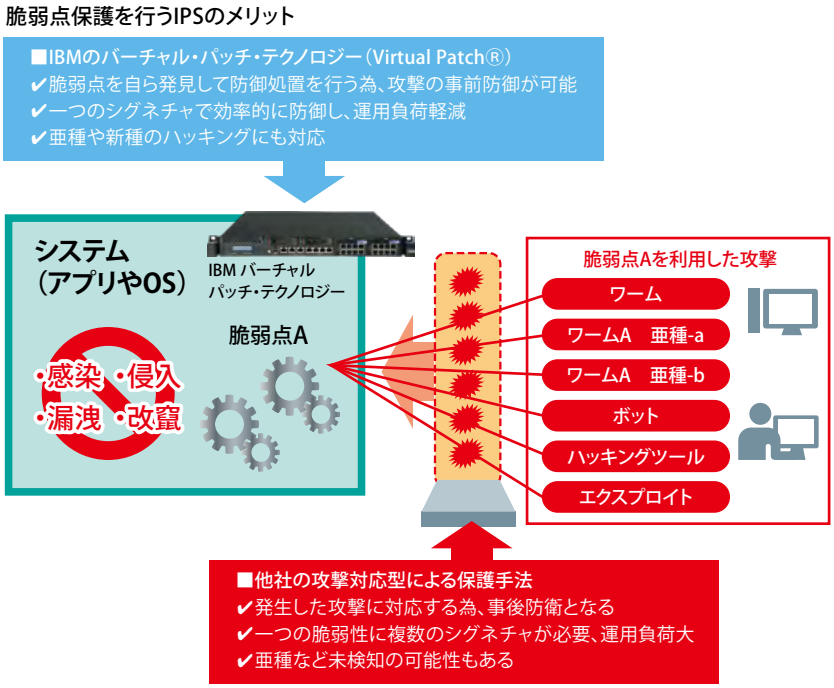


図6 IDS/IPSによる保護手法の違い

標的型攻撃に使用される代表的なクライアントツールへのIBM IPSの対応状況

2010年から2014年の5年間における以下クライアントツールへの対応（実績ベース）
－Internet Explorer / Adobe Acrobat Reader , Adobe Flash

ワンポイント

外部から攻撃を持ち込む経路となりうる Internet Explorer、そして具体的な情報が詰まっている Adobe Acrobat Reader や Adobe Flash への脆弱点対応は非常に重要です。

Internet Explorer への対応（競合他社と比べても圧倒的です）

IBM IPS は、独自の強力な検出技術にて、
97.9% のセキュリティパッチに対応（＊1）。さらに 56.8% が事前対応（＊2）。

公開情報にて 競合A社 での同一条件における実績ベースの結果は
72.7% のセキュリティパッチに対応。さらに、9.1% が事前対応。

Adobe Acrobat Reader , Adobe Flash への対応（公開他社情報はありません）

Adobe Acrobat Reader に関しては Internet Explorer と同一算出方法で
88.5% のセキュリティパッチに対応。さらに 30.8% が事前対応。
Adobe Flash に関しては
78.9% のセキュリティパッチに対応。さらに 33.3% が事前対応。

＊1：セキュリティパッチに対応
公開情報によるIBM調査結果。該当するセキュリティパッチにIPSシグネチャがある場合にカウント対象としています。
本ページ内容のセキュリティパッチに対応という記載では共通の算出法がとられています。
＊2：事前対応
公開情報によるIBM調査結果。該当するセキュリティパッチの公開1週間以上前にIPSシグネチャがある場合にカウント対象としています。本ページ内容の事前対応という記載では共通の算出法がとられています。

図7 代表的なクライアントツールへのIBM IPSへの対応状況

ションを導入することになりかねません」（落合氏）

その一方、脆弱点に対応するシグネチャを使用するIDS/IPS専用機では、2経路目本来の動きに沿って稼動できることに加えて、各々の亜種に対応するシグネチャを都度作成する必要がなくなる。その結果、IDS/IPSが使用する全体のシグネチャ数も少なくなり、過剰検出も少なくなる傾向がある。

これらのことからも専用のIDS/IPSが必要になるのだが、その中でもIBMのIDS/IPSは不正アクセスの検出率が圧倒的に高いのが特長だ。

「たとえば、Internet Explorerの場合、97.7%のセキュリティパッチに対応するシグネチャを用意しているだけでなく、マイクロソフトがそのセキュリティパッチを公開する1週間以上前 に、脆弱性を保護するIPSシグネチャがある割合が56.8%でした（ものによっては5年以上前など、年単位でパッチの公開よりも早く対応できているケースがあります）。

つまり万が一、セキュリティパッチが公開される前の段階も含めて、セキュリティホールをパッチでふさぐ前の攻撃があったとしても、弊社のIPSの導入にて、多くの攻撃に対応できるものと期待が持てます。同じ他IPS専用製品であっても、これらの数字は72.7%と9.1%にすぎません（図7）」（落合氏）

これだけ高い検出率を実現できる背景には、IBMが持つ世界最大規模のセキュリティ研究機関「X-Force」がある。全世界10拠点の監視センターでは、1日に200億件のデータを分析し、その知見をIDS/IPS製品にも活かしている。

「さらに、弊社では、24時間365日、不正なアクセスを監視するマネージド・セキュリティー・サービスも提供しています。IDS/IPS製品、セキュリティ研究機関、監視サービスの3つを持っており、前身となる ISS社（Internet Security Systems社）の時より15年継続して提供し続けているのは、弊社だけです」（落合氏）

現在、多くの企業は高度化・複雑化するサイバー攻撃への対応に苦慮している。それに対し、多くのセキュリティベンダーが「当社の製品を導入すれば保護できます」とアピールする。

しかし、すべての攻撃を防御できる製品は存在しない。いずれも、どこかを守れれば、どこかは守れない。ユーザーは、限られた予算内でそれを見極め、守れない箇所がないように、複数の製品を組み合わせなければならない。こう考えると、そのポートフォリオに専用のIDS/IPSを含めることは、非常に効果的だとわかるだろう。

ウイルス対策やファイアウォールと並んで古い歴史を持つIDS/IPS。それだけに技術も成熟し、かつ価格も十分にこなれてきたコストパフォーマンスに優れた製品だ。その導入効果は非常に高いという事実に、多くの企業は今こそ気づくべきではないだろうか。

■お問い合わせ先
日本アイ・ビー・エム株式会社
フリーダイヤル　0120-550-210
受付時間　9:00～17:00（土、日、祝日を除く）
メール　http://ibm.biz/ContactSec

※本記事は、2016年12月20日に掲載されたビジネス+ITからの転載です。