

費用対効果に優れ 利便性も充実

毎年夏になると、米国アラスカ州では蚊の大群が発生し、住民たちの悩みの種となっているが、アラスカ大学アンカレッジ校のネットワーク環境は夏だけでなく年中と云っていいほど、ウイルス感染とクラッキング攻撃の嵐にさらされている。

同校でCIOを務めるリチャード・ホイットニー氏にとって、ネットワークに打撃を与えるクラッカーたちは人を料子敷と同じくらいに（いや、それ以上に）憎らしい存在である。そこで、同氏は、殺虫剤ならぬ「多機能な統合型セキュリティ・ゲートウェイ（ISG：Integrated Security Gateway）」を導入することによって、うるさいクラッカーたちからネットワークを積極的に防御することにした。

ホイットニー氏に限らず、今、ネットワーク環境を守るためにISGを採用するCIOが急激に増加している。その人気の秘密は、「1台のマシンで、侵入検知からファイアウォール、アンチウイルスまですべての対策をカバーできる」（ホイットニー氏）という手軽さにあるようだ。

ISGとは、IDS/IPS（侵入検知/防止）、ウイルス・スキャン、スパム・メール（迷惑メール）排除、Webコンテンツ・フィルタリングなど、多くのセキュリティ機能を1台の筐体に搭載したアプライアンスである。最近の製品では、ファイアウォール機能やVPN（Virtual Private Network）機能もサポートされるようになっており、セキュリティ対策における便利な“よろず屋”としての地位を確立しつつある。

昨今、企業のセキュリティ対策において費用対効果と利便性という2つの要素が強く求められる傾向にあること



ISGは 企業セキュリティの 救世主となるか

多機能なシングル・ボックスのメリットと意外な落とし穴

今、セキュリティ市場では、あらゆる機能を“1つの箱”の中に詰め込んだ統合アプライアンス製品が次々と発表されている。導入のしやすさ、単機能アプライアンスと比較した場合の新設費など、そのメリットは数多い。本稿では、今、まさにブームとなりつつある統合型セキュリティ・ゲートウェイ（ISG）製品のメリット、ならびにそこに潜む落とし穴を検証することで、この種の製品を遊ぶ際にCIOが考慮すべき事項を明らかにしたい。

ジョン・エドワーズ

net by John Edwards

を検討しているという。

「我々は、ネットワーク環境をつい先日、ギガビット・クラスにアップグレードしたばかりだ。そのため、近いうちにISGがパフォーマンス上のボトルネックになるだろう。1つのアプライアンスのためにネットワーク全体のパフォーマンスを落とすことは、あってはならないことだ」と語る。

ネットワークのゲートウェイ層で稼働するISGは、とりわけパフォーマンスに影響を与えやすい。ユーザーの中には、ISGを導入したところ、ネットワークのパフォーマンスが急激に落ちたため、結局、その利用をあきらめてしまったというようなところも出てくる。

ゴートナーのベスカートル氏は、こうした問題や、運用管理の煩雑さを解決するためにも、業界標準に準拠したISGを利用することを勧めている。この分野の国際規格として有名なものとしては、米国政府の認可を受けた研究機関によって与えられる「情報技術セキュリティ評価基準（Common Criteria Certification）」などがある。こうした標準を製品選びの1つの指針とすれば、カタログ・スペックと明らかに異なるようなパフォーマンス上の問題を回避できる可能性が高まることになる。

ISGは確かに、成長期にありがちないくつかの課題を抱えてはいる。だが、総合的に見て、セキュリティ対策で悩むCIO、CSOの“切り札”になりうるだけの可能性を秘めているのも事実だ。業界では、今後数年のうちに、ISGは単機能のセキュリティ・アプライアンスを押し分け、標準技術として定着するとも目されているのだ。

このISGといかにつきあうかが、これからのCIOにとっては、避けては通れないテーマとなってきそうだ。■

電子メールにご用心

スパムとウイルスの撃退にも威力を発揮するISG

統合型セキュリティ・ゲートウェイ（ISG）ベンダーには、2人の“良き”いや、正確に言うところ“信頼できない”友人がいる。ウイルス作成者とスパム・メール業者である。こうした被害の温床となる電子メールのセキュリティ対策は、今やCIOにとって脅威することのできない問題となっている。とはいえ、従来のクライアント・ベースのツールで、この問題を解決するのは難しい。そこで、ユーザー企業が“切り札”として期待を寄せるのがISGなのである。

非営利の産産機関、パブリック・ヘルスケアでCIOを務めるデブ・ギャレット氏は、近ごろ、このやっかいな問題に真正面から挑んだ。一元的かつ総合的に電子メール保護を担うために、数々のツールを試した同氏は、「問題解決のためにはISGを導入するしかない」という結論に達したという。

「当初は、市販されているデスクトップ・ツールをいくつか試してみた。だが、細粒的には十分でも、それらをまとめて管理し、すべてのデスクトップを最適な状態に保っておくのは至難の業であることが分かった。そこで、1つのボックスですべてを担うISGの有効性に目を向けるようになったのだ」（同氏）

ギャレット氏は、1日に平均で4,000通の外部からの電子メールを受信するパブリック・ヘルスケアのネットワーク上に、サイファートラストのISG [IronMail] を導入した。その効果は絶大で、現在、同製品は1日に1,500通のスパム・メールをゲートウェイ層で遮断することに成功しているという。

最新のISG製品は、暗号化やセキュリティ・ポリシーの管理、ウイルスの侵入防止にも威力を発揮する。そのうえ、それらすべての機能を単一のコンソール上から一元管理することも可能だ。これはつまり、エンドユーザーの手を一切離らせることなく、セキュリティ上の負担に対応できるということである。「ISGの効果は予想していたよりもはるかに大きい。心のつかえが1つとれたような思いだ」と、ギャレット氏は目を細める。

金米で住宅リフォーム・サービスを提供するアメリカン・レジデンシャル・サービスのセキュリティ管理者、ジェソン・ソリンスキ氏も、ボーダーウェアのISG [MXsense] を利用して、同社の2,500人のエンドユーザーをスパム・メールから隔離することに成功している。

1日に数千電子メールの半分がスパム・メールとされる米軍にあって、さまざまな機能を詰め込んだ“小さな箱”は、なくてはならない存在となりつつある。

多層なセキュリティ・インフラを維持・管理する必要がまったく消滅するわけではないということも、押さえておきたいポイントだ。フロスト&サリバンのライト氏は、こう警告する。

「ネットワークの境界で1台のマシンにすべてを任せておくと、悪意のあるクラッカーはそのマシンを通りさえすれば、内部に侵入できることになる。ホストやサーバ、デスクトップに別種の保護技術を装備しておかなければ、ネットワーク全体を守ることはできないと考えておいたほうがよい」

かねてから、企業では、セキュリティ・レベルを高めるために、ファイアウォール・システムをネットワーク上の複数の場所に配置するというような対策を講じてきた。では、ISGを複数台配置するという手は有効なのだろうか。残念ながら、その効果はほとんどないというのが真相のようだ。パートナー・グループのシャクター氏は次のように注意を促す。

「ISGは、あくまでもネットワークのゲートウェイ層で効力を発揮するように設計されているため、ほとんどの機能は2重化の恩恵を受けない。したがって、ファイアウォールを2重化するような旧来型の手法も、決して意味を失ったわけではない」

一方、昨今、平凡な製品ではCIOの支持を得られないと考えた多くのISGベンダーは、他社製品との差別化を図るため、最先端の機能を自社製品に組み込むことに躍起になっている。つまり、「すべての機能で75点」を実現するのはもはや当たり前であり、そこにどれだけ「100点の機能」を搭載し、付加価値を付けられるかという戦いを繰り広げているのである。

ベスコートル氏は、「ISGの導入にあたって、CIOが選りすぐりの技術を使うのをあきらめる必要はなくなるだろ

う。CIOは少なくとも搭載機能の1つがその分野で最高峰のものであることを求めるべきだ」と主張する。「多機能」であることによって新たな市場を開拓したISGだが、今後は「多機能かつ高性能」でなければ生き残れないわけだ。

最後に、ISGが単機能セキュリティ機器よりも明らかに不利だと思われるのが、アップグレードの問題である。セキュリティ・アプライアンスの多くは、通常、特定のタスクを処理する機能を回路に組み込んだASIC（特定用途向け集積回路）を採用し、パフォーマンスの向上を図っている。だが、このASICは高価で、しかもソフトウェアによって機能を変更することができないため、機能をアップグレードしようとするには、ISGもしくは、ASIC自体を買い換える必要があり、それなりの出費が必要だ。また、ISGは複数の機能を持つがゆえに、その分（ある機能が）隔離化するのも早いと予想される。それゆえ、アップグレードのコストは、単機能型アプライアンスよりも大きくなる可能性があるということを覚悟しておくべきであろう。

パフォーマンスを確保するか

ISGを導入時に最後先すべき事項が「ネットワークを完全に防御できること」であるのは明白だ。だが、パフォーマンスもそれと同じくらい重要な条件である。というのも、セキュリティ製品を導入したせいでネットワークの速度が低下すると、人々はたいてい、それを使わずに済ませる方法を見つけ出してしまふからだ。

最大データ転送レートが900MbpsのISG製品を2年近くにわたって利用してきたアラスカ大学のハイットニー氏は、早くもより高速なモデルへの置き換え



Illustration by Francesco Landini

「何と言っても、新しいISGの導入に伴い、それまで利用していたウイルス・スキャン、Web/電子メール・フィルタリング・ソフトウェアのライセンス料金を大幅に削減できたことが大きい」(岡氏)

アントン氏は、定常的に発生するソフトウェアのサポート料やライセンス料を考慮に入れた場合、ISGへの移行に伴うROIは、2004年には118%、2005年には177%、2006年には213%に達すると予測している。

「カスタマイズが難しい」といった課題も

一方で、よいことづくめに思えるISGの導入だが、CIO諸氏もご存じのとおり、特定の製品によって得られる

固有のメリットには、必ずと言っていいほど、それと相反するデメリットが内包されているものである。ISGの場合も決して例外ではない。

ガートナーのインターネット・セキュリティ・アナリストであるジョン・ベスカートル氏は、ISGがもたらすデメリットの1つとして、カスタマイズ性の乏しさを挙げる。

「ISGを導入すれば、確かに管理作業は軽減されよう。しかしながら、それは同時に、自分のコントロールをある程度あきらめるということでもある」(ベスカートル氏)

フロスト&サリバンのライト氏も、その点を要する専門家の1人だ。岡氏は、「ISGには微調整を加える手段が欠けているため、ネットワーク・トラフィックと完全に同期して機能させる

というような高度な運用は不可能だ」と指摘する。

また、ISGの最大のメリットの1つとも言える一元的な管理機能にも、実は落とし穴の一面がある。ネットワーク・セキュリティ機能を1か所に集約すれば、確かに管理プロセスは簡素化できるが、真を返せば、それは、突然の障害によってネットワーク環境が一気に異質化してしまうということを意味している。

「例えば、1か所の電源が落ちただけで、4~5種類のセキュリティ機能が一気に停止してしまうといった危険がある。したがって、ユーザーには、ISGの冗長化対策を万全なものにしておくことを強く勧めたい」と、ベスカートル氏は力説する。

また、ISGを導入したからといって、

した情報を別のコンポーネントに適用することができれば、複数のコンポーネントを連携させて防御の壁を厚くすることが可能だからである。例えば、IDSコンポーネントが不正な電子メールを検知した場合、その情報を自動的にスパム・フィルタに反映できれば、スパム・メールのブロック率は飛躍的に向上する。もちろん、複数のコンポーネントの情報を集約できれば、管理者の負担も大幅に軽減される。

ISGベンダーの1つ、フォーティネットでは、モジュール間の連携を支援する「ポリシー・エンジン」を同社の製品「FortiGate」に搭載し、ファイアウォール、VPN、侵入検知、アンチウイルスの各モジュール間のデータ共有を可能にしている。こうした連携機能の詳細を把握することも、製品選びにおいてはきわめて重要なステップとなる。

高いROIを達成

では、冒頭に登場したアラスカ大学のホイットニー氏は、いかにしてISG製品を選定したのであろうか。

当時、ホイットニー氏がセキュリティ上最大の課題と認識していたのは、ウイルス/ワームの防御、不正アクセスの排除であったが、2万人以上のネットワーク・ユーザーを抱える同大学にとって、クライアントごとにインストールされた従来型のソフトウェアの運用継続は、パフォーマンスと管理性の2つの側面から限界に達しつつあった。

「我々は、2002年の春から、システムとネットワーク・セキュリティのあり方について検討を始め、同時に、市場に出回っているさまざまな製品について調査を行った。その結果、アプライアンス型のISGが、最もROI（投資

利益率）の高い選択肢であるとの結論に至ったのだ」（ホイットニー氏）

製品の比較検討を行った結果、同氏は、ファイアウォール、アンチウイルス、侵入検知、コンテンツ・フィルタリング、VPNの各機能を備えたシマンテックの「Symantec 5300 Gateway Security Appliance」（1台4万ドル）に白羽の矢を立てた。決定の決め手となったのは、同価格帯の製品の中でパフォーマンスが優れていたことと、直感的な管理インタフェースを有していたことであった。

すでに導入から2年近くが経過しているが、ホイットニー氏は、ISGの導入によって、アラスカ大学のネットワークのセキュリティ・レベルを確実に向上させることができたことを誇る。

「もし、ISGの導入に踏み切っていなければ、当大学の限られたITスタッフでは、対応しきれないような状況が生まれていたはずだ。メインの大規模サーバも、はたして稼働し続けることができていたかどうか分からない。もはや、ISGのようなツールなくして、大規模ネットワークを安全に運用していくのは不可能なのではないだろうか」（同氏）

一般に、セキュリティ・ツールはその投資効果が見えにくいとされるが、実は、ISGの導入が企業収益に明らかにプラス効果をもたらしたという例も報告されている。

産業機械/システム・メーカーのイリノイ・ツール・ワークスは、スパム・メールならびにウイルス対策のためにミラポイントの「Message Director」を導入した。同社戦略調達担当副社長、ゲイリー・アントン氏によれば、初年度の2003年には、同製品で5,000人のネットワーク・ユーザーをカバーし、26%のROIを達成したという。

からすれば、ISGに対する期待の高まりも十分に納得のいくところだ。第1の要素である費用対効果で見ると、ISGは、各種の機能に特化したアプリケーションを組み合わせて利用するよりはるかに安上がり導入することができる。また利便性の面でも、スタンダードなさまざまなハードウェア/ソフトウェア製品を組み合わせて使う場合に比べ、ネットワークのボトルネックが発生しにくいし、単一のインタフェースですべての機能を管理できるというメリットもある。

言ってみれば、現在のISGは、長らくCIOが待ちわびてきた「理想の」セキュリティ・ツールなのである。

“シングル・ボックス・ブーム”の到来

業界の専門家たちも、ここ数年のISG人気に注目している。IT調査会社、バートン・グループの副社長兼ディレクター/セキュリティ戦略サービス担当ディレクター、フィル・シクスター氏は、「ISGは、今やIT市場の中でも1、2を争う成長市場となった」と評価する。

市場の拡大を当て込んで、この分野に参入するベンダーも後を絶たない。現在、この分野の大手ベンダーとしてはボーダーウェア・テクノロジーズ、フォードネット、インクラ・ネットワークス、インターネット・セキュリティ・システムズなどがある。また、サイファートラスト、ミラポイント、ネットスクリーン・テクノロジーズ(ジュニアネットワークスが買収)、シマンテックなども有力どころとして挙げられる。

現在、世に出ているISGの価格は、機能や性能に応じて1万~5万ドルの間で設定されている。スタンダードの

ファイアウォール/VPN装置の価格がエントリー機種ですら3,000~1万ドルであることを考えると、その“お買い得感”はかなりのものである。

また、最近、CIOならびにCSO(最高セキュリティ責任者)の間で、セキュリティの確保のためには総合的な対策が不可欠であるとの認識が確立されつつあることも、ISGベンダーにとっては願ってもない追い風となっている。セキュリティ対策では、ある特定の分野の防御が弱いと、それが他の分野にも悪影響を与えてしまうケースが少なくない。例えば、いくら高性能なアンチウイルス・ツールを導入していても、スパム・フィルタの機能が弱ければ、ネットワークをウイルス攻撃から完全に防御することは難しいといったことが言えるのだ。こうした点からしても、あらゆる機能を過不足なく備えるISGの優位性は高いと言える。

通常、「あらゆる機能を詰め込んだ製品は、特定の機能に特化した製品と比べてパフォーマンスで見劣る」というのが相場だが、ISGにはこの常識も当てはまらない。むしろ、その逆で、単機能のセキュリティ機器よりも高いパフォーマンスを発揮できる可能性を有しているのである。その理由を、シクスター氏はこう説明する。

「単機能のセキュリティ製品を複数組み合わせ、それらをネットワークに直列に接続して順番にトラフィックを流そうとすると、どうしてもパフォーマンスに問題が生じてしまう。その点、ISGなら拠点が1つで済むため、影響を最小限に抑えることができるのだ」

ソフトウェア・ベースのセキュリティ・ツールと比較した場合も、ISGの優位性は崩れない。筐体が独立しているため、サーバやクライアントのCPUパワーを奪うことなく、機能を実行することが可能だからである。

IT調査会社 Frost & Sullivan のセキュリティ業界アナリスト、ジェーン・ライト氏は、こう指摘する。

「あらゆるデータのパケットをスキャンし、適切なものだけを通すというような処理をソフトウェアで行おうとすれば、どうしても他のITリソースに影響が出てしまう。その点、アプリケーション型の製品は、機能が独立して存在するため、一定の処理速度を安定して保つことができる。企業にとってみれば、そのメリットはきわめて大きい」

「ISG製品」選択のポイント

以上のことからしても、セキュリティ対策において、ISGの導入がきわめて有効な選択肢であることは明らかである。だが、「数ある製品の中から、どれを選ぶか」という段階になると、CIOはかなりの重荷を悩ますことになる。というのも、現在、市場に出回っているISGは、いずれもが多様な機能を搭載しているが、機能的な特徴は製品によって大きく異なっているからである。

例えば、インターネット・セキュリティ・システムズの「Proventia」は、VPN、ファイアウォール、アンチウイルス、侵入検知/防止、コンテンツ/スパム・フィルタリングなどのネットワーク・セキュリティ機能をフル装備しているが、電子メール向けの機能は限定されたものとなっている。一方、不正な電子メールの防御に特化したISGの1つであるミラポイントの「Message Director」は、ウイルスとスパムの対策に重点を置いている。

また、多くのISG製品では、統合的な運用管理を支援するために、何らかのかたちでコンポーネント間の通信機能が用意されている。これも、ISGにとってはかなり重要な機能である。ある特定のコンポーネントが収集