

媒体名	発行部数	掲載日	掲載面
テレコミュニケーション (1/4)	38,000部	2007年10月	p. 58~p.61

簡単導入で注目 通信系販売店の新商材UTM

通信系販売店の今後の重要商材として注目されているUTMアプライアンス。構築が容易な反面、提案時には、ユーザー企業の既存のセキュリティ環境や重視するポイントの事前確認が必須となる。

文◎藤田 健(本誌)

ファイアウォールやVPN、IDS/IPS(不正侵入検知/防御)、アンチウイルス等の複数のセキュリティ機能を1つの筐体に統合したUTM(統合脅威管理)アプライアンスが、通信系販売店の「電話プラスワンの商材」として注目を集めつつある。

電話のIP化の進展により、通信系の販売店はネットワークに取り組まざるを得なくなっている。だが、まだまだ二の足を踏む販売店が多いのが実情だ。

UTMアプライアンスを扱うある販売代理店の営業部長は「通信系販売店がネットワークに取り組む取っ掛かりとしてUTMは最適な商材」と語る。理由は、導入と運用が簡単だからだ。

「UTMを拠点間のVPN装置としても機能させる場合には、VPN上でのようなパケットが流れるか等、ある程度ネットワークのスキルが必要だ。しかし、ルーターやファイアウォールの裏側でセキュリティアプライアンスとして動作させるだけなら、IPアドレス等のネットワークの最低限の知識があれば構築できる」と前出の営業部長はいう。

例えば、フォーティネットの「FortiGate」などは管理画面が日本語化されているため(写真)、一度メ

ーカーの講習会に参加すれば、ほとんどの販売店は自社で導入できるようになる。

参考までに紹介すれば、現在、UTMアプライアンスのVPN機能を活用した導入事例はほとんど見かけない。UTMのメインユーザーである中小企業がVPNを利用する時は、VPN機器をキャリアからレンタルで導入している割合が多いからだ。

J-SOX法の影響は中小企業にも

導入する企業にとってUTMアプライアンスはどのような位置づけになってきているだろうか。

一般的にUTMは「中小企業向けの商材」といわれている。大企業の場合は、情報システム部門がしっかりしているうえ、セキュリティ対策に十分なコストがかけられるため、各機能に特化した製品を個別に導入し、運用管理を実施している。だが、中小企業では、人的にもコスト的にもそのような導入・運用形態は採れない。

他方で、徐々に中小企業にもきちんとしたセキュリティ対策が求められるようになってきた。複数の販売店が口を揃えるのが「J-SOX法の影響」だ。

J-SOX法は、相次ぐ会計不祥事やコンプライアンス(法令遵守)の欠如等を防止するため、米国のサーベンス・オクスリー法(SOX法)に倣って整備されたものだ。上場企業とその連結子会社に、会計監査制度の充実と企業の内部統制強化を求めている。

J-SOX法は本来、未上場の中小企業は対象外だが、対策は上場企業の取引先にも求められる。このため、今回取材した販売店各社も「メーカーから確認文書が来るので、セキュリティ対策を実施しなければならないという雰囲気になっている」という。

多くの中小企業が上場企業と取り引きしていることから、セキュリティ対策を実施していない企業は今後、ビジネスができなくなる可能性がある。

UTMアプライアンスは、導入・運用の容易さから、このような中小企業に適したセキュリティ商材とされている。

先進的な販売店は大きな実績

では、現状でUTMアプライアンスを扱っている通信系販売店はどれくらいあるだろうか。

主要UTMベンダーの一次代理店の話を総合すると、日常的に取り引きしている二次代理店のうち、扱っているのは1割にも満たないようだ。やはり、まだまだ「セキュリティは難しい」という意識が通信系販売店には

媒体名	発行部数	掲載日	掲載面
テレコミュニケーション (2/4)	38,000部	2007年10月	p.58~p.61

根強いことの表れだろう。

こうした状況に対して各一次代理店は、セミナーや勉強会の開催頻度を増やして「セキュリティはさほど難しくない」という啓蒙活動を実施するとともに、案件にSEを同行させ、導入支援を行っている。

ちなみに、数少ないUTMに積極的な販売店はすでになんかの実績をあげている。なかには、導入だけに留まらず、監視とメンテナンスからなるマネジメントサービスまで提供しているところもあるという。

これまで通信系の販売店には、このようなサービスで食べていこうという発想はなく、IP時代を迎えた通信系販売店の意識変革のよい事例といえるだろう。

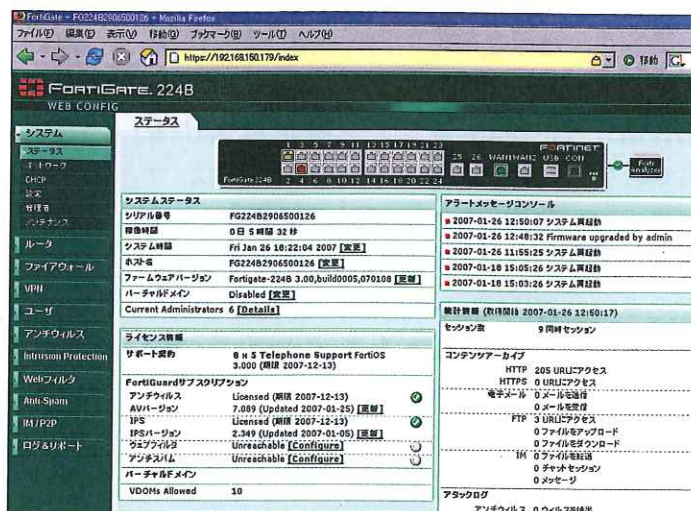
顧客先でのデモで受注増

まだセキュリティに取り組めていない通信系販売店の参考になる販社がある。キヤノンシステムアンドサポート(キヤノンS&S)だ。

同社はキヤノンマーケティングジャパンの100%子会社であり、コンサルティングから保守サービスまで一貫して提供している。特に、47都道府県・200カ所以上の拠点を通じ、24時間365日体制で保守を手掛けてきた実績がユーザーに評価されている。

キヤノングループということで、当初はMFP(複合機)の取り扱いからスタートし、徐々にPCやアプリケー

ションソフトウェア等の情報システム系の商材を扱うようになった。さらにIP電話にも進出。NECインフロンティアのIP対応ビジネスホン「Aspire」とNECのIP-PBX「APEX」も扱っている。



日本語化されたフォーティネットの「FortiGate-224B」の管理画面

マーケティング本部ITソリューション販売推進部ITソリューション販売推進第一課の猪狩伸也課長は「ネットワーク構築を手掛けるようになると、セキュリティ商材の扱いも必須になった」と語る。

そうした折、グループ会社のキヤノンネットワークコミュニケーションからフォーティネットの紹介を受けた。「当社が求めていた“簡単に導入でき、すぐに効果が出る商材”に合致したので取り扱うことにした」という。

同社のユーザーのうち、従業員10~20名の企業は7~8割を占める。この層のユーザー企業は、コスト削減効果が短期間でハッキリと数字に表れるシステムへの投資には前向きだが、そうではないセキュリティ機器の導入には総じて腰が重い。このため、

UTMの必要性を実感してもらうための取り組みが必要となる。

同社は提案に際してまず、UTMアプライアンスをユーザー企業に持ち込んでデモを実施するようにしている。「不正攻撃やスパムメール

等、実際に何がどれくらい起きているかを見てもらうことで、顧客が被害者や加害者にならないためにはUTMの導入が必要だということを訴求している。デモを実施すればほとんどの企業で納得してもらえる」と猪狩課長は語る。

その後、具体的な商談に入るが、必ずしもすべての機能を利用するわけではなく「どの機能を

使うかは、顧客とよく話し合っている」という。

営業マンの教育もユニークだ。セキュリティ関連の情報は、日々刻々と変化するが、最新の情報を常に全員が共有しなければならない。前述のように同社は、全国に200拠点以上を構えている。

同社では毎朝15分間、各拠点で営業マンが集まって勉強会を開催している。具体的には1枚の用紙にポイントを絞って最新情報を整理し、それを営業マンに伝える。勉強会で得た情報は、その日に回るユーザー企業へのトークにも利用でき、UTM未導入のユーザーには必要性を説く材料にもなる。

キヤノンS&Sでは、UTMアプライアンスは単体ではなく、他の情報シ

媒体名	発行部数	掲載日	掲載面
テレコミュニケーション (3/4)	38,000部	2007年10月	p. 58~p.61

ステム系商材と一緒に導入するケースがほとんどだが、これまで紹介してきた取り組みにより、「最近には月に200~300セットは出るようになった」(猪狩課長)という。

GWサーバー撤廃でコスト削減

丸紅ソリューション・ITソリューション事業部インテグレーション営業部プロダクト&マーケティング課の作間健司課長は、「今年になってようやく、ユーザーがUTMという言葉に敏感になり始めた」と実感している。

同社は1999年1月からソニックウォールのセキュリティ製品を販売しており、UTMアプライアンスもメーカーが市場投入した約3年前から取り扱っている。

丸紅ソリューションが直販するケースはほとんどなく、商社などの流通、SI、ISPをそれぞれ経由して販売している。流通経由は小規模の企業が多く、SI経由は比較的中規模層が多いという。

ソニックウォールは自社でカスタマサポートセンターを用意しているが、丸紅ソリューションでもサポート部隊を用意している。

作間課長は「流通のサポートはソニックウォールに一任しているが、SIのサポートは従来から当社で実施している」と説明する。「UTMアプライアンス単体だけでなく、複合的なネットワーク構築、セキュリティ構築の観点からサポートできる点が強み」と語っている。

ユーザー企業がUTMアプライアンスを導入するタイミングについては「ミドルレンジ層は毎年のゲートウエ

イアンチウィルススのライセンス更新時が多い」という。

この層のユーザーの更新時のキーワードは「ゲートウェイアンチウィルスサーバーを省く」だ。

ソニックウォールの小規模企業向け製品「SonicWALL TotalSecure」は主要セキュリティ機能を統合したいわゆるUTMアプライアンスだが、ミドルレンジ層が導入する「SonicWALL PRO」シリーズは、ファイアウォール/VPNアプライアンスにUTMファンクションを追加する製品だ。このため、UTMファンクションを投入する以前は、SonicWALL PROとともに他社のゲートウェイアンチウィルスサーバーを導入するのが一般的だった。

だが現在は、アンチウィルスソフトやIPSを自由に追加できる。このため、ゲートウェイアンチウィルスサーバーを撤去してこれらを付加したほうが、費用対効果が高い。

「クライアントにもアンチウィルスソフトは入れるので、ゲートウェイは“一次的な関所”という割り切り運用が増えた。ゲートウェイアンチウィルスサーバーを省いて浮いた予算で、他のセキュリティ機能を追加したり、ネットワークの投資に充てるようになった」と作間課長は説明している。

小規模企業では、前述のようにセキュリティ対策には腰が重いという課題がある。これに対して丸紅ソリューションでは、被害対応にかかる費用や個人情報漏えいで1件当たりに支払った金額等、セキュリティ被害の具体的な事例を用いている。「セキュリティ対策は一種の保険だ。保険

をかけていない時、実際にどれくらいの損失になるのかをトップに説明することが小規模企業には効果的(作間課長)という。

マネジメントサービスを提供

NTTPCコミュニケーションズ(NTTPC)は、トータルセキュリティマネジメントサービスのブランド「Security BOSS」を立ち上げ、その第1弾として独アスタロー社のUTMアプライアンスを活用した「ゲートウェイ・セキュリティ運用監視サービス」を開始している。

同社はアスタロー社の国内販売代理店であり、当初はSIとして販売・保守を手掛けていた。だが、運用に手間がかかり、継続できないユーザーが多かったことから、サービスとしての提供に踏み切った。

「UTMアプライアンスは運用が容易」といわれているが、オンデマンド事業部プロダクト部商品開発担当の尾崎文則課長代理は「IPSやファイアウォールはチューニングが大変であり、スパムやURLフィルタはホワイトリスト、ブラックリストの追加と削除が頻繁に起こる。特に小規模企業では専任の情報システム担当がいないので、運用ができなくなるところが多い」と説明する。

UTMは、個別にセキュリティ機器を導入するケースに比べると一元管理ができるために運用が容易だが、やはり管理者にはある程度のセキュリティに対する知識が求められるようだ。

サービスの概要だが、UTMアプライアンスをユーザー企業にレンタル

媒体名	発行部数	掲載日	掲載面
テレコミュニケーション (4/4)	38,000部	2007年10月	p. 58~p.61

し、NTTPCのセキュリティオペレーションセンタのマネジメントサーバーとIPsecVPNで結び、24時間365日体制でリモート監視・運用する。これにより、ユーザー企業には管理担当者が不要になる。

提供されるセキュリティ機能は「ファイアウォール運用」「24時間365日侵入検知防御」「メールアンチスパム運用」「メールアンチウイルス運用」「WEBアンチウイルス運用」「アンチスパイウェア運用」「アンチフィッシング運用」「URLフィルタリング運用」「ファイル転送アプリケーション制御」の9つ。

「ライト」「ライト+」「スタンダード」「ハイエンド」の4つのサービスプランがあり、スタンダード以上で9つのセキュリティ機能が提供される。

月額料金はスタンダードで18万9000円、ライトなら3万1500円。尾崎課長代理は「このようなサービスを提供しているベンダーは他にもあるが、月額60万円、80万円という価格設定。当社は機器のレンタル料や保守を含んでもこの料金」と価格優位性を強調している。

顧客の重視ポイント把握を

UTMアプライアンスをユーザー企業に提案する時、注意しなければならないことがある。メリットだけでなく、デメリットもきちんと把握しておかなければならないという点だ。図表にUTMの主なメリットとデメリットを示した。

ジュニパーネットワークスの製品を取り扱っているCRCシステムズ・ソリューションサービス本部ソリュ

図表 UTMアプライアンスのメリットとデメリット

メリット		デメリット	
1	1台で主要セキュリティ機能を利用可能	1	障害発生時には単一障害点になる
2	導入作業が容易	2	各機能ごとに最適なパフォーマンスを持つ製品を選択できない
3	導入・管理コストがリーズナブル	3	拡張性が制限される
4	運用・管理工数が軽減	4	複数の機能を同時に使用するとスループットの低下を招く
5	省スペースを実現		
6	優れた耐障害性による信頼性向上		

提案時にメリットとデメリットの両方をきちんとユーザーに説明したうえで導入の可否を選択してもらう

ーションサービス部の笠井貴一技術担当部長は「UTMは何でもできる」と説明すると誤解を招く。UTMに1~10まですべてを求めるのは難しいということをユーザーに理解してもらったうえで導入しないと、トラブルの原因になる」と指摘する。つまり、ユーザーが何を最重要視するかを事前にきちんと把握しておくことが必要なのだ。

UTMを導入すれば、必要最低限のセキュリティは守れる。しかし、高レベルでセキュリティを守りたいなら、運用の煩雑さとコスト高を覚悟してでも、大企業のように各機能に特化した製品を組み合わせるしかない。

他方で、工夫次第でUTMのセキュリティレベルを上げることも可能だ。例えば、アンチスパムやアンチウイルス機能はISPのサービスとしても提供されているので、それと組み合わせると導入すればより強固になる。

UTMアプライアンスは今までまったくセキュリティ対策を実施していなかったユーザーには提案しやすい商材だ。逆にいえば、すでに何らかの

セキュリティ装置を導入しているユーザーへの提案は慎重になるべきだろう。「現在何のセキュリティ装置を導入していて、どのように運用しているのか」「UTMに切り替えて大丈夫なのか」「今と比較してコストはどうなるのか」等々、確認すべき事項は多い。

CRCの笠井担当部長は「当社が扱うジュニパーネットワークスの製品は、機能ごとにライセンスが分かれているため、欲しい機能だけを選ぶことも可能」と語っている。

このほか、現在のUTMには複数のセキュリティ機能を同時に使用すると、ネットワークのスループット低下を招くという課題もあるので、スループット重視のユーザーに提案する時にはこの点も考慮しなければならない。

UTMアプライアンスは今後、通信系の販売店にとって欠かすことのできない重要なプラスワンの商材になる可能性がある。だが、ここまで述べてきたように、導入に際して注意しなければならない点が多く、これまで以上にユーザーとの事前の話し合いが求められる商材といえる。