中堅・中小企業向けネットワークセキュリティソリューション

Network Security Solution for Mainstay SMEs

● 高橋　晃　　● 三浦崇久

あらまし

標的型攻撃などのサイバー攻撃は日々巧妙化しており，情報漏えいが社会問題化して久しい。しかし，株式会社富士通マーケティング(以下，富士通マーケティング)の主要なお客様である中堅・中小企業においては，主にICT投資予算の不足やICT専任者の不在により，セキュリティ対策の導入が進んでいないのが実情である。富士通マーケティングはこの状況を改善するため，富士通製品のみならず広く他社製品を組み合わせ，お客様の規模や商談パターン別に費用対効果を最適化したセキュリティソリューションを提案してきた。それらは，中堅・中小企業の商談ケースに応じてスモールスタートから始めることができるセキュリティ対策が主な特徴となっている。

本稿では，中堅･中小企業に向けたネットワークセキュリティ対策について，富士通マーケティングの取り組みを紹介する。

Abstract

Cyber attacks are becoming increasingly skillful as in targeted attacks and the like, and information leakage has been a social issue for some time. However, many small- to medium-sized enterprises (SMEs), which are the main customers of Fujitsu Marketing Limited (hereafter “Fujitsu Marketing”), have not been able to introduce adequate security measures due mainly to a lack of budget for investing in information and communications technology (ICT) and dedicated ICT engineers. Fujitsu Marketing has been striving to address these difficulties. It is offering security solutions that are optimized for better return on investment (ROI) for its customers according to their business size and commercial style by allowing Fujitsu products to be combined with components provided by other vendors. These solutions are characterized by their scalability because they can be installed in a small package to start with, depending on the needs of each SME. This paper explains how Fujitsu Marketing has been developing the network security solutions for SMEs.

ま え が き

近年，日本国内へのサイバー攻撃が増加している。警察庁広報資料によると，日本へのサイバー攻撃のうち標的型メール攻撃の件数は2013年から急増し，2014年には前年の3倍以上の1,723件へと増加した。[(1)] 例えば2015年6月には，この標的型攻撃によって日本年金機構から少なくとも125万人の個人情報が漏えいした事件は記憶に新しい。

これらの攻撃はますます巧妙化しており，トレンドマイクロ社が発表した「国内標的型サイバー攻撃分析レポート2015年版」[(2)] によると，国内の標的型攻撃において，日本国内に設置されたC&C(注1) サーバが利用された事例の割合は，2013年と比較して2014年は7倍以上になっている。これは，日本国内の正規サイトを改ざんしてC&Cサーバとして動作させ，正規のWeb通信に偽装させるケースが増加していることを意味する。

また標的型攻撃では，攻撃を受けてから気付くまでに時間がかかることが多く，攻撃を受けたことにさえ気付かないケースもある。実際，日本年金機構の場合は，内閣サイバーセキュリティセンター（NISC）が検知したことによって発覚しており，これ以降に公表されたマルウェア(注2) 感染事例の多くは，外部組織からの指摘によって発覚している。このような事件を受け，情報処理推進機構（IPA）はウイルスに感染したことを前提にセキュリティ対策を行う必要があると改めて注意喚起している。

特に，株式会社富士通マーケティング（以下，富士通マーケティング）の主要なお客様である中堅・中小企業は，大企業に比べてセキュリティ対策が十分でない場合があり，情報窃取以外に大企業への標的型攻撃の踏み台にされることも多い。

本稿では，クライアント端末に対する標的型攻撃において，まず中堅・中小企業におけるネットワークセキュリティ対策の現状を分析し，そのパターンに対応した製品群の選定について述べ，最後に富士通マーケティングの提供するセキュリティ運用サービスを紹介する。

（注1） Command and Controlの略。マルウェアに感染してボット化したコンピュータに指令（command）を送り，制御（control）すること。その役割を担うサーバをC&Cサーバ，その通信をC&C通信と呼ぶ。

（注2） 不正かつ有害な動作を行う意図で作成された悪意のあるソフトウェアや悪質なコードの総称。

標的型攻撃の概要

本章では，標的型攻撃について簡単に説明する。

標的型攻撃は，複数の攻撃手法を組み合わせ，戦術的な攻撃手順に沿って遂行されるという特徴がある。攻撃者は「初期潜入の段階」で標的をマルウェア感染させる。攻撃手法を変化・巧妙化させ，執拗にマルウェアを送りつけることが多い。メールをやり取りした後にマルウェアを送る手法（やり取り型攻撃）や，頻繁にアクセスするWebサイトを改ざんしマルウェアをダウンロードさせる手法（水飲み場攻撃）などが知られている。手口を巧妙化させ，マルウェア自体も亜種を作るなどしてウイルス対策ソフトでは検知できないように工夫している。

標的とする端末をマルウェアに感染させると，RAT(注3) によってC&Cサーバから遠隔操作を確立させる。これが端末制御の段階である。従来は独自プロトコルを使用していたが，最近ではHTTP/HTTPSを使用し，認証プロキシサーバ経由でも通信可能なツールを使用するように進化している。

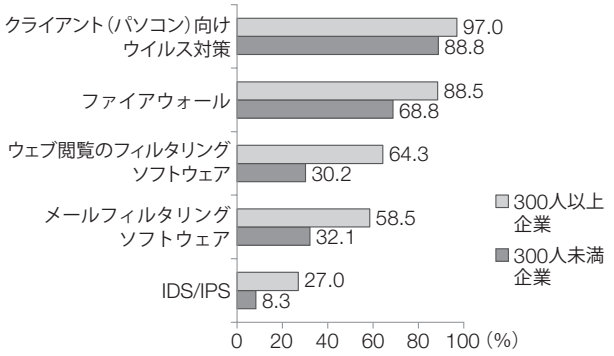
次に，感染した端末の遠隔操作が可能になると，ツールによってLAN内の情報を探索し，有益と思われる情報の収集に取り掛かる。そして実データを取得し，外部への送信を行う。以上の一連の動作が，概ね標的型攻撃の概要となる。

中堅・中小企業の現状分析

本章では，中堅・中小企業におけるネットワークセキュリティ対策の現状を分析する。

IPAが発表した「2014年度 情報セキュリティ事象被害状況調査－報告書－」[(3)] からネットワークセキュリティに関する項目を抜粋し，その導入状況を従業員300人以上の企業と300人未満の企業において比較した結果を**図-1**に示す。この図に基づき，300人未満の中堅・中小企業におけるセキュリティ対策の実施状況について簡単に解説する。

（注3） Remote Administration Toolの略。管理者権限を持ってコンピュータを遠隔操作できるようにするツールのこと。



出典：情報処理推進機構（IPA）
「2014年度 情報セキュリティ事象被害状況調査－報告書－」

図-1　情報セキュリティ関連製品やソリューションの導入状況

（1）ウイルス対策

300人未満の企業においても，クライアント端末のウイルス対策についてはほぼ実施されており，本項目は改善対象から除外する。

（2）ファイアーウォール（FW）

300人未満の企業では約68％が導入しているが，導入率は十分とは言えない。また後述するが，中堅・中小企業の多くが導入している従来型FWでは防御できないマルウェアも多いため，本項目を主な改善対象とする。なお，ここで従来型FWとは，セキュリティ対策として「あらかじめ設定したIPアドレスとプロトコルによる通信制御を実施しているFW」を指す。

（3）Webフィルター・メールフィルター（アンチスパム）

300人未満の企業で対策を実施している企業は，約1/3にとどまっている。したがって本項目も改善対象とする。

（4）IPS/IDS(注4)

300人未満の企業ではほとんど導入されていない。したがって，本項目も併せて改善対象として扱う。

次に，富士通マーケティングがこれまで関わってきた中堅・中小企業のお客様の典型的なネットワーク構成を**図-2**に示す。この図に示したとおり，

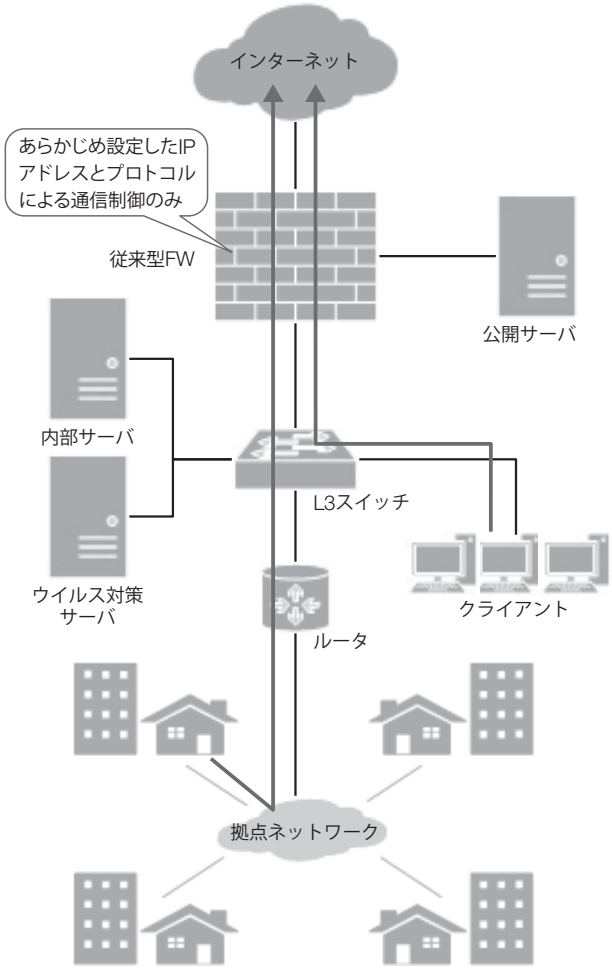


図-2　中堅・中小企業の典型的なネットワーク構成

中堅・中小企業ではたった1台の従来型FWのみで社内ネットワークが防御されているケースが多い。

この背景には，主に二つの原因がある。一つは，専任のICT管理者が不在で，何をすればよいか分からないためである。もう一つは，中堅・中小企業にとって高価なセキュリティ製品は，予算化すら難しいという事情である。富士通マーケティングは，このような背景を理解した上でソリューションを提供している。

中堅・中小企業のセキュリティ対策の課題

現状の一般的な中堅・中小企業のネットワークに設置されている従来型FWで防御可能な内容を**表-1**に示す。この表にまとめたように，一般的な中堅・中小企業では，パターンファイルやシグネチャが存在する既知のマルウェアや，既知の脆弱性に対する攻撃への対策が不十分であることが分かる。

(注4)　Intrusion Prevention System/Intrusion Detection Systemの略。不正アクセスを監視する装置で通信遮断を行うものをIPS，検知のみ行うものをIDSという。通常の行動パターンを定義し逸脱したら異常と判断する方式をアノマリ型，異常な行動パターンを定義し一致したら異常とみなす方式をシグネチャ型という。

表-1　従来型FWの防御可能内容

攻撃フェーズ	対策カテゴリ	防御すべき内容★	防御可否
初期潜入	ウイルス対策	マルウェアダウンロード	可
	Webフィルター	不正サイトアクセス	不可
	アンチスパム	マルウェアダウンロード	一部可
	IPS/IDS	OSの脆弱性への攻撃	不可
端末制御	FW	独自プロトコルによるC&C通信	可
	Webフィルター	不正サイト（C&Cサーバ）アクセス	不可
	IPS/IDS	マルウェアの振る舞い	不可

★：パターンファイルやシグネチャが既知である場合に限る。

「標的型攻撃の概要」の章で述べたように，初期潜入の段階で攻撃者はまず標的対象組織の内部へ潜入を試みる。このようにして既存マルウェアの亜種を送り込まれた場合，ウイルス対策ソフトでは防ぐことはできない。また，次の端末制御の段階において，最近のC&C通信ではプロトコルにHTTP/HTTPSを使用するため，従来型FWでは防ぐことができない。更に，正規のWebサイトを改ざんしてC&Cサーバを設置している場合は，Webフィルター機能でも防ぐことはできない。

中堅・中小企業の標的型攻撃対策

これまでに述べた課題からも分かるように，中堅・中小企業の標的型攻撃対策には少なくとも今までのセキュリティ対策に加え，C&Cサーバとの通信を検知できるソリューションが必須となる。また，中堅・中小企業のニーズ（分かりやすさと扱いやすさ）と，限られた予算に合致した製品を選定しなければならない。標的型攻撃に対するネットワークセキュリティ製品は，各ベンダーから最近ようやく市場に投入され始めた。その数ある製品群から製品を選定する前に，まず中堅・中小企業の現状のネットワーク状況や対策レベルに応じた商談ケースごとに対応が必要となる。

特に中堅・中小企業の場合は，前述したように「たった1台の従来型FWのみで守られている状況をいかに改善するか」から始めるべきである。まさにスモールスタートによる改善が必要とされる。この主な改善方法を以下に二つ挙げる。一つは，お客様の現行FWにIPS/IDS機能を付加する「単体アドオンケース」である。もう一つは，FW製品を丸ごと標的型対策に対応した製品へ交換する「FWリプレースケース」である。

以下では，まず現状のネットワーク構成に機器を単体で追加する単体アドオンケースについて述べる。

（1）単体アドオンケース

本ケースは，様々な理由で現行のFWを廃棄できないため，現行FWにIPS/IDS機能のみを追加したいというお客様に適している。このような場合，C&Cサーバとの通信検知精度を向上させ，マルウェア対策を実施できるマカフィー社のMcAfee NSPシリーズをアドオンケースとして提案している。本シリーズは比較的導入しやすい価格帯から選定可能であり，C&C通信の検知や，シグネチャレスエンジンの採用によって標的型攻撃で使用されるゼロデイマルウェアの検知も可能である。

次に，FWリプレースケースについて述べる。FWリプレースケースは，1台でFWとIPS/IDSなどの複数機能を実現するため，お客様の規模別に以下の二つの製品群を選定し，パフォーマンスの確保にも十分留意する。

（2）FWリプレースケース1（中規模企業向け）

中堅・中小企業の中でも比較的規模が大きく，高いパフォーマンスを求められる場合は，次世代FWの先駆者として，市場で高い評価を得ているPalo Alto Networks社のPAシリーズを採用する。

本製品は，UTM(注5) とアプリケーション識別の機能のほかに，ボットネットレポート機能でC&C通信を検知できる。この機能は，トラフィックログ，脅威ログ，URLログなどの情報から，ボットネット感染が疑われるホストをリストアップするものである。また，WildFireと呼ばれるクラウド型サンドボックス(注6) 環境を別途追加することで，マルウェアの振る舞いも検知可能である。

（3）FWリプレースケース2（中・小規模企業向け）

FWリプレースケースにおいて，チェック・

（注5）Unified Threat Managementの略。FWをベースに，アンチウイルス，IPS/IDS，Webコンテンツフィルタリングなど複数のセキュリティ機能が統合された機能群のこと。UTM機器のことを指す場合もある。

（注6）保護された領域内でプログラムを動作させることで，不正な挙動や外部への送信がないかといったことを事前にチェックし，外部への悪影響が及ぶのを防止するセキュリティ手法のこと。

ポイント・ソフトウェア・テクノロジーズ社のCheckPointApplianceシリーズは比較的低コストで機種を選定できるため，中堅・中小企業に適している。既存FWを交換してIPS/IDS機能を追加することによって，マルウェア対策とC&Cサーバとの通信検知性能を向上させる。本製品は，Webとメール通信を1台で監視し，下位機種においてもログレポートが充実して分かりやすいため，特に専任のICT管理者が不在の中堅・中小企業に適している。また，クラウド型サンドボックスを別途追加することが可能で，スモールスタートから始めて最終的に高度なサンドボックス分析までを実現できる。

これらの製品群へのリプレースを実施すると，中堅・中小企業のネットワークを概ね**表-2**のレベルまで向上できる。

中堅・中小企業向けセキュリティ運用サービス

本章では，富士通マーケティングが提供するセキュリティ運用サービスについて述べる。

一般的に，標的型攻撃対策の運用サービスは導入機器が高価で，かつ高度なサンドボックス分析などを含むため，運用にかかる費用も非常に高価である。中堅・中小企業のお客様に一般的なセキュリティ運用を提案すると，その見積もり額の大きさに落胆されるケースが多い。これに対し，富士通マーケティングはトラフィック分析やログ

表-2　標的型対策製品導入後の防御可能内容

攻撃フェーズ	対策カテゴリ	防御すべき内容★	防御可否
初期潜入	ウイルス対策	マルウェアダウンロード	可
	Webフィルター	不正サイトアクセス	可
	アンチスパム	マルウェアダウンロード	可
	IPS/IDS	OSの脆弱性への攻撃	可
端末制御	FW	独自プロトコルによるC&C通信	可
	Webフィルター	不正サイト（C&Cサーバ）アクセス	可
	IPS/IDS	マルウェアの振る舞い	一部可

★：パターンファイルやシグネチャが既知である場合に限る。

表-3　中堅・中小企業向けセキュリティ運用サービスの型決め（案）

●：24時間　○：平日9時～17時対応

項番	運用項目			運用深さ	要件パターン組み合わせ		
	大分類	小分類	作業項目		小	中	大
1	シグネチャ管理	デフォルト管理	メーカーデフォルトシグネチャ	浅	○		
2		カスタマイズ管理	限定事象範囲シグネチャ適用			○	
3			システム構成ベースのシグネチャ			○	○
4			顧客固有シグネチャ				○
5			システム構成/脆弱性診断シグネチャ	深			○
6	データ管理	シグネチャ	最新シグネチャバックアップ	浅	○	○	○
7		検知ログ	ログバックアップ	深			○
8	発生事象への対応	事象の検知・遮断処理	事象の検知のみ	浅			
9			事象の遮断のみ		●		
10			事象の検知および遮断	深		●	●
11		事象通知	自動通知	浅	●	●	●
12			誤遮断シグネチャの解除（お客様要求時）		●	●	●
13			カスタマイズ通知	深		●	●
14		事象分析	事象の真偽判定	浅		○	●
15			事象のシステム影響度判定			○	●
16			事象の対策案提示			○	●
17		ポリシーチューニング	事象分析後シグネチャ調整	深			○
18		マルウェア分析	通信の振る舞い分析				○
19	問い合わせ対応	問い合わせ対応	問い合わせ回答		○	○	●
20	報告書管理	機器運用報告書	通知情報，シグネチャ更新情報などの運用履歴	浅			○
21		分析報告書	攻撃別分析，トピックス運用履歴	深		○	○

検索の操作性に優れたMcAfeeNSP，PaloAlto，CheckPointApplianceを選定し，かつ運用内容を中堅・中小企業向けに特化したセキュリティ運用サービスを提供していく。また，この三つの製品が持つデフォルトでの遮断機能を組み合わせ，比較的安価な定型運用サービスとして型決めすることで効率化を図っていく（**表-3**）。

なお，本サービスは上記の機器が持つマルウェア対策機能によって不正アクセスを遮断できるが，難易度の高いサンドボックス分析などの運用作業はオプションとしている。それは，専任のICT管理者がいない中堅・中小企業に対して，サンドボックス分析などはコストが高く，ニーズにマッチしないからである。

富士通マーケティングは，マルウェア対策とC&Cサーバ対策に特化するとともに，コストの低減も併せて行い，中堅・中小市場への普及を図ることを第一の目的とする。少ない投資で必要最低限のセキュリティ対策を提供し，お客様には本来の業務に集中していただくのが狙いである。ただし，こうした対策には限界があり，それを正しくお客様に伝えていくのも富士通マーケティングの役割である。

む　す　び

富士通マーケティングは，中堅・中小企業の予算と商談ケースに合わせ，必要最低限な1台を既存環境にアドオンあるいはリプレースし，お客様のセキュリティ対策をスモールスタートから支援していく。一般的に高度な分析を伴い複雑になりがちなセキュリティ運用サービスを，専任のICT管理者が不在の中堅・中小企業のニーズにマッチさせ，必要最低限のシンプルな運用に特化したサービスを展開していく。

こうした取り組みを踏まえ，将来的に富士通マーケティングのサービス商品であるAZSERVICEシリーズのラインナップに加えていきたい。

富士通マーケティングは，これからも主要なお客様である中堅・中小企業の発展と安全な社会の実現に貢献していく。

参考文献

(1) 警察庁：平成27年におけるサイバー空間をめぐる脅威の情勢について.
https://www.npa.go.jp/kanbou/cybersecurity/H27_jousei.pdf
(2) トレンドマイクロ株式会社：国内標的型サイバー攻撃分析レポート2015年版．2015年4月．p.15-18.
(3) 独立行政法人 情報処理推進機構（IPA）：2014年度 情報セキュリティ事象被害状況調査－報告書－．2015年1月．p.49-50.
https://www.ipa.go.jp/files/000043418.pdf

著者紹介

高橋　晃（たかはし　あきら）
（株）富士通マーケティング
システム本部
ネットワークソリューションセンター
ネットワークセキュリティのフィールドSE業務に従事。

三浦崇久（みうら　たかひさ）
（株）富士通マーケティング
システム本部
ネットワークソリューションセンター
ネットワークセキュリティのフィールドSE業務に従事。