サイバー攻撃の現状と対策について

株式会社NTTデータ経営研究所
シニアスペシャリスト　早乙女　真
NTTデータ先端技術株式会社
シニアエキスパート　天野　寛生

はじめに

寄稿にあたって、自分の身の回りの情報セキュリティについて、少し整理をしてみた。その結果、改めて感じたことは、自分が未だ情報セキュリティインシデント(注1)に見舞われていないことは、極めてラッキーだということである。このラッキーは、所属する企業のセキュリティ対策が充実しているおかげか？はたまた自分がセキュリティに関する環境構築やルール遵守などに努めているが故か？答えはどちらも否。正解は、自分の持っている情報に攻撃するほどの価値がないか、または単なる偶然で情報の価値が知られていないかのいずれかである。

企業や組織の情報セキュリティを取り巻く外的、内的環境は高速度で変化している。大局的には、情報技術の進化に伴い、コンピュータやネットワークに関する機能、機器が巷に氾濫し、その利用範囲や利用形態が多様化していることがある。特にインターネットやスマートフォンに代表される携帯機器のインパクトは極めて大きい。こうしたことでセキュリティインシデントにおいて発生する事象や攻撃ルートは急激に多様化している。

もう1つの視点として、デジタル情報の価値の高騰がある。パソコンの実用化から数十年を経て、DBソフトや表計算ソフト、またはこれらと同等に情報のリストアップ機能をもったアプリケーションソフトの利用が日常化し、それらを使ううちに様々な有価値のデジタル情報がコンピュータや電子機器内に自然に蓄積されている。企業の戦略や業績に関わるような目的をもって作られた情報でなくとも、自然に価値の芽生えてしまった情報はどこにでもあり、やっかいなセキュリティ事故の対象となり得るのである。

こうした変化の帰結として、サイバー攻撃に対する防御の無力化が進行している。発生する事象、攻撃ルートの多様化に対して守るべき対象が散乱していることにより、これまでの常識では有効となっていた防御手段が、必ずしも効果の期待できないものと化している。ここに攻撃側の進化が追い打ちをかける。

情報技術の進化の黎明期には、言ってみれば攻撃側も遊び半分であり、攻撃によって得られる価値などにはあまり頓着せず、自己の存在を誇示する目的でホームページの改ざん

(注1)情報管理やシステム運用に関して保安上脅威となる現象や事象

02-14_地銀08月号 特集-1.indd 2　13.8.21 1:52:46 PM

をしてみたり、電子文書やシステムを壊して利用者の混乱を楽しむようなことが行われていた。それから数年、何のせいかはともかくとして、世の中は悪質化している。標的型攻撃という言葉はかなりスタンダードになったので、少なくとも一度くらいは耳にしたことがあるだろう。長期にわたり攻撃の標的について研究し、計画的に情報を得て攻撃ポイントを練り、価値の高い標的にとって影響の大きい情報を盗み出すような攻撃。しかも、じわじわと張り付いて情報を取得し続けるために、以前のように攻撃が成功したことをこれ見よがしに公表したりはしない。映画や小説の世界におけるスパイ活動のようなことが、現実に行われているのである。

なあに、当社は立派なファイアウォールを設置しているし、マニュアルも整備し、ウイルス対策もソフトの最新化も行っているから大丈夫と思われる方。冗談ではない。ちょっとした技術者ならこれくらいの環境を攻撃する手段はいくつでも考えられる。簡単にいえばソフトウェアでできる防御は、仕組みを知ればソフトウェアで破れるのである。ましてや、人がルールで守っている部分などには、ミスか故意かはともかく簡単に攻撃目標となる隙ができる。

つまり、攻撃者に動機さえあれば、そして、あなたやあなたの組織に盗んで価値のある情報があれば、またはあなたやあなたの組織が失うことによって世間や他の誰かが利するような情報を持つのであれば、その対価を目当てに攻撃者が活動を始める可能性は十分にあり、その攻撃から身を守ることは極めて困難であるということを認識すべき状況なのである。

前置きがいささか長くなったが、本稿はこのような状況認識に立って、今日的な、サイバー攻撃等の情報セキュリティ上の脅威からあなたやあなたの組織の身を守る術について、解説を試みるものである。

セキュリティインシデントの変化

セキュリティインシデントの変化について、公知の情報をもとにして追ってみようと思う。2005年３月に経済産業省を中心としたコンピュータ・セキュリティ検討会の発信で「コンピュータ・セキュリティ～2004年の傾向と今後の対策～」という資料が公開されている。その後は、情報処理推進機構（IPA）のセキュリティセンターが引き継ぎ、毎年「10大脅威」という資料が発行されている。

2004年時点で資料(注２)に示される主な脅威は以下のとおりである。

＜利用者向けの脅威＞

◆ボット(注３)

◆コンピュータウイルス

◆フィッシング詐欺(注４)

＜管理者向けの脅威＞

◆個人情報の漏えい

◆複数製品にまたがる脆弱性の脅威

◆ウェブサイトの改ざん

これを見ると、ある意味で安心された方が多いかもしれない。この時点の脅威は、情報

（注２）「コンピュータ・セキュリティ～2004年の傾向と今後の対策～安全なインターネットの利用を目指して」2005年３月31日コンピュータ・セキュリティ協会より引用

（注３）コンピュータに潜伏して組織的な攻撃を行うプログラム

（注４）偽のウェブサイトで人を騙し、情報を盗み取る詐欺的行為

02-14_地銀08月号 特集-1.indd 3 13.8.21 1:52:46 PM

セキュリティに多少明るい人であれば、想像できる範囲にあるもので、対策も以下のように基本的なものが紹介されている。

◆ソフトウェアを安全に保つ

◆信頼できないソフトウェアやデータを使わない

◆対策ソフトウェアの導入

◆利用者自身の対策

ちなみに「利用者自身の対策」では、不審なメールを開かない、不審なウェブサイトを信用しないといった利用者の行動を規定することが有効な対策であることが述べられている。

さて、時計を数年進めてみる。2010年版10大脅威(注5)には、「あぶり出される組織の弱点」と副題がついている。１位から10位の脅威の内容は以下のとおり。

① 変化を続けるウェブサイト改ざんの手口

② アップデートしていないクライアントソフト

③ 悪質なウイルスやボットの多目的化

④ 対策をしていないサーバ製品の脆弱性

⑤ あわせて事後対応を！情報漏えい事故

⑥ 被害に気付けない標的型攻撃

⑦ 深刻なDDoS攻撃(注6)

⑧ 正規のアカウントを悪用される脅威

⑨ クラウド・コンピューティングのセキュリティ

⑩ インターネットインフラを支える製品の脆弱性

タイトルの表現に「変化を続ける」、「多目的化」といった変化や多様性を示すキーワードが増えているが、大まかに捉えれば、まだこの時点の脅威は2004年の脅威の延長上で辿ることができる。ちなみにこの年の大きな話題は①位に記されているガンブラーウイルスであり、このウイルスにより有名企業や公共機関のウェブサイトを閲覧しただけで感染する可能性があることが、新聞やテレビで報道され話題となった。この事件は、対策側の意識も変わらなければいけないことを関係者に突きつけたと考えることもできる。また、標的型攻撃も新種の脅威として⑥位にランクされている。こうした傾向の変化が副題で示される「あぶり出される組織の弱点」にも反映されていて、セキュリティ対策を経営課題として扱うことなど、組織としての取り組みの強化が求められている。

さらに時計を進めて2012年版(注7)を見てみる。筆者の感覚では、このあたりで「悪質化」という意味では大きな変化があったように感じられる。副題は「変化・増大する脅威！」。

① 機密情報が盗まれる⁉新しいタイプの攻撃

② 予測不能の災害発生！引き起こされた業務停止

③ 特定できぬ、共通思想集団による攻撃

④ 今もどこかで…更新忘れのクライアントソフトを狙った攻撃

⑤ 止まらない！ウェブサイトを狙った攻撃

⑥ 続々発覚、スマートフォンやタブレットを狙った攻撃

(注５)「2010年版10大脅威『あぶり出される組織の弱点！』」2010年３月独立行政法人情報処理推進機構セキュリティセンターより引用

(注６)サーバやルータ等の機能を麻痺状態にさせる攻撃の一種

(注７)「2012年版10大脅威～変化・増大する脅威！～」2012年３月独立行政法人情報処理推進機構セキュリティセンターより引用

02-14_地銀08月号 特集-1.indd 4 13.8.21 1:52:46 PM

⑦　大丈夫⁉電子証明書に思わぬ落とし穴
⑧　身近に潜む魔の手…あなたの職場は大丈夫？
⑨　危ない！アカウントの使いまわしが被害を拡大！
⑩　利用者情報の不適切な取扱いによる信用失墜

タイトル表現の変化は、執筆者の状況感によるものとも思われるが、「狙った攻撃」という言葉で示される恣意性の存在や「予測不能」、「特定できぬ」、「止まらない」、「危ない！」などという危険性や防御困難性の強調により、攻撃者の「悪質化」が想起される記述となっている。また、新しい脅威として、「スマートフォンやタブレットを狙った攻撃」が無視し難いものになってきたことが現れている。①位の新しいタイプの攻撃については、副題として「情報窃取を目的とする標的型の諜報攻撃（APT(注8)）」との記述があり、標的型攻撃の一種として企業や国家機関の重要な機密情報の諜報を目的とした攻撃が取り上げられている。

さて、現時点で最新となる2013年版(注9)を見てみよう。

①　クライアントソフトの脆弱性を突いた攻撃
②　標的型諜報攻撃の脅威
③　スマートデバイスを狙った悪意あるアプリの横行
④　ウイルスを使った遠隔操作
⑤　金銭窃取を目的としたウイルスの横行
⑥　予期せぬ業務停止
⑦　ウェブサイトを狙った攻撃
⑧　パスワード流出の脅威
⑨　内部犯行
⑩　フィッシング詐欺

2013年版は、タイトル表現が前年と変化しているが、項目は比較的前年と共通する要素が多い内容と思われる。「クライアントソフトの脆弱性を突いた攻撃」や「フィッシング詐欺」など、改めて対策の原点回帰を促すような項目と共に、警察の捜査が撹乱される困難な犯罪事件として記憶に新しい「遠隔操作」などの新しい脅威が記されている。さらに、個々の内容を見ると、脅迫行為なども伴う標的型諜報攻撃に加え、ウイルスや様々な技術を駆使した金銭搾取を目的とした攻撃など、悪意ある攻撃者の存在が時間とともに鮮明になってきているという印象は拭えない。

このようなセキュリティ脅威の変化を見てくると、脅威の傾向としては、時間を経ても同種のものがなくならないこと。言いかえれば、対策を徹底し、守りを固めることが難しいことに加えて、新種や亜種の発生による多様化が進んでいること。そして、悪質な攻撃者の存在が鮮明になり、金銭的価値を執拗に狙うとともに、既存対策をすり抜けるよう周到に戦術を練った標的型攻撃のような脅威が、目前まで迫ってきていることなどが読み取れる。

セキュリティ対策の面からは、基本的対策で手を抜くことも許されないと同時に、悪質な攻撃者を意識した新たな高度な対策もまた必要という難局に追い込まれているということもできるのである。

図らずも暗いことばかり述べることになり

（注８）持続的標的型攻撃（Advanced Persistent Threat）
（注９）「2013年版10大脅威～身近に忍び寄る脅威～」2013年３月独立行政法人情報処理推進機構セキュリティセンターより引用

02-14_地銀08月号 特集-1.indd 5　13.8.21 1:52:46 PM

恐縮している。次章以降では、対策者に光を与える対策の方向性などに触れてみたい。

セキュリティ対策の方向性

ここでは、近年のセキュリティトピックの中心になり、メディアで目にすることも多い標的型攻撃と類似する攻撃等を例にとって、ひと通りのおさらいも含めつつ、その対策方針の方向性について述べることにする。

標的型攻撃の源流は意外に深い。もともとサイバー攻撃はインターネット黎明期から国家間の諜報活動の一環として軍事関連施設に対して継続的に行われ続けており、2000年代の中盤から、このような軍のネットワークに侵入し、機密データを盗み出す攻撃に対して、米軍が「APT」という言葉を用いるようになった。こうした軍事関連施設をターゲットとするような攻撃手法が、政府機関や民間企業、一般市民まで対象にするようになったのがここ数年の変化といえる。

実際の標的型攻撃においては、ソフトウェアの未知の脆弱性を悪用するような高度な技術が用いられることももちろんあるが、組織の構成員の人的な脆弱性を狙ったソーシャルエンジニアリング的(注10)な要素を含む場合もある。なかには技術的な手段をほとんど用いずに遂行されることすらある。言いかえれば、標的を狙い定めた攻撃者が、明確な意図を持って、あらゆる手段を講じて目的を遂行しようとしているということでもある。また、防御する側からはこうした単純な方法のほうが、案外対策が施しにくいといった事情もある。

例えば、現在では「標的型攻撃」といえば、電子メールを用いた攻撃がほぼ代名詞といえるほど、多くのケースで電子メールシステムが悪用される。被害者は一見正常に見える電子メールを受け取り、それが攻撃者からのものとは気づかないまま、悪意のあるWebサイト（フィッシングサイトや、マルウェア(注11)を見えないようにダウンロードさせるサイト）への誘導リンクをクリックしたり、不正なPDFドキュメントやWordファイルを開くことでマルウェアの侵入を許す。

こうした電子メールは、伝統的なスパムメール(注12)とは異なり、受信者組織の内部関係者でしか知り得ない情報が含まれていたり、心理的なトリックを用いて開封を促すような表現を用いたりして、情報セキュリティについてある程度知見をもった受信者であってもうっかり開いてしまうような作りになっている。部外者がこのような内部情報を含んだメール文面を作成することは難しそうに思えるかもしれないが、この手の細工に慣れた攻撃者にとっては、普段使われているメールの内容を盗み見ることができれば、作成はさほど困難なことではない。まして、取引相手など関係者のコンピュータをウイルスに感染させ、大量に文面を入手できるような事前準備を行えば、なおさらのことである。

もっと原始的な手法も未だに使われる。攻撃者が標的とする組織の駐車場にマルウェアや不正なドキュメントファイルを書き込んだUSBメモリを放り出しておき、何の気なしに拾った関係者が確認のため自分のコンピュータに接続するとマルウェアに感染してしま

(注10)特定の人を狙い心理的に相手をだますような手法
(注11)コンピュータウイルスなど悪意をもったソフトウェアの総称
(注12)旧来の一般的迷惑メールの通称

02-14_地銀08月号 特集-1.indd 6 13.8.21 1:52:46 PM

う、などという方法である。

標的型攻撃では、このようにさまざまな手法を駆使してマルウェアを組織内に送り込む段階を「初期潜入段階」と呼ぶ。一旦組織内部に入り込んだマルウェアは、次の攻撃フェーズに入っていく。「攻撃基盤構築段階」と呼ばれる段階である。この段階でマルウェアは主に以下のようなことを行う。

①内部拡散

ネットワーク上に存在する他のコンピュータに自分のコピーを拡散させ、感染を拡大する。

②バックドアの構築

攻撃者の用意したコマンド＆コントロールサーバ（C&C サーバ）とのバックドア通信経路(注13)を確保し、C&C サーバからの指示通りの動作ができるようにする。C&C サーバとの通信は多くの場合、ユーザのインターネットアクセスに紛れて、http のような一般的な通信プロトコル(注14)を用いて行われるため、ファイアウォールをすり抜けることができる。

③自己アップデート

マルウェアは、ずっとそのままでいればいずれアンチウイルスソフトに検知される可能性がある。このため、用意したサーバから自分の亜種をダウンロードして、自分自身を少し異なるファイルに置き換える。こうすることでパターンマッチ方式(注15)でウイルスを検知するタイプのアンチウイルスソフトに検知されることを防ぐ。アンチウイルスソフトのウイルスパターン情報は随時アップデートされるが、それよりも早く自分自身をアップデートし続けることで、長期間にわたり検知されないままの状態を維持することを可能にする。

次なる段階は「システム調査段階」と呼ばれる。ここまでのフェーズを経てネットワーク内に居座ったマルウェアは、そのネットワーク上にどんなサーバが存在し、どんな機密情報があるのかを時間をかけて調査する。この段階では既に C&C サーバとの通信を通じて、攻撃者がマルウェアを自由にコントロールできる状態になっており、手探り的な情報の検索だけでなく、攻撃者が直接ファイル名を見て判断できる程度の精度を持って情報探査を行っていると考えたほうがよい。

さて、いよいよ「攻撃最終目標の遂行段階」である。ファイルサーバ上の機密データにたどり着いたマルウェアは、最終的に C&C サーバに向けてこれらのデータを送信することで攻撃目的を達成する。

ここまでの攻撃段階を見てくると、攻撃には必ずしも革新的な新技術が用いられているわけではないことがわかる。

それぞれの技術は決して目新しいものではなく、昔から用いられてきたものであるが、これらの技術が合わせ技で用いられた場合に防御が困難になる。端的にいえば、ソーシャルエンジニアリングの要素が含まれているという時点で、システム的な対策で完全に防ぐことは不可能といえる。しかも、攻撃者というものはターゲットにした組織に10の攻撃を仕掛けたとしたら、そのうち９つが失敗したとしても、１つ成功すればよいのである。

だからといって、投げやりになり初期潜入

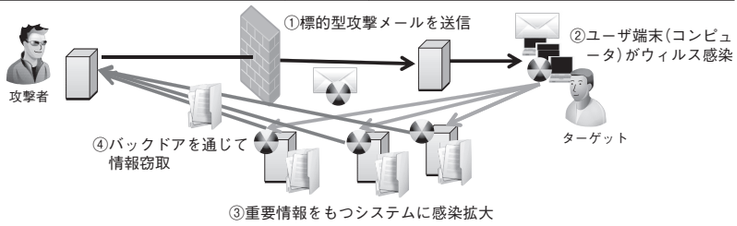
(注13)正規の手続きを踏まずに侵入を可能にする「裏口」
(注14)ネットワーク上での通信に関する規約や手順
(注15)過去のウイルス等に関するパターン情報との照合によりウイルスを見分ける方式

02-14_地銀08月号 特集-1.indd 7 13.8.21 1:52:46 PM

図表１　標的型攻撃のフェーズ

攻撃の進行

フェーズ	従来の手法との違い	概要
初期潜入段階 （既存の対策をくぐり抜けた侵入）	大	**標的型**攻撃メール添付ウィルス Web 改ざんによるダウンロードサーバ誘導 外部メディア（USB 等）介在ウィルスなど
攻撃基盤構築段階 （情報を盗み出す仕組みの構築）	小	バックドアの構築 ウィルスの一斉バージョンアップ機能追加 システム内部への攻撃基盤構築
システム調査段階 （情報を盗み出す対象の調査と選定）	中	システム情報の取得 時間を掛けた重要情報の存在箇所特定
最終目的の遂行段階 （情報の持ち出し）	小	重要情報の窃取 組織情報（アカウント等）を元に、目標を再設定



図表２　各攻撃フェーズと用いられる技術

フェーズ	技術
初期潜入段階	ソーシャルエンジニアリング
	電子メールに添付されたマルウェア
	アプリケーションの脆弱性を突く攻撃
攻撃基盤構築段階	C&C サーバとの http 通信
	http 通信を利用した自己アップデート
	ネットワーク経由での自己増殖
システム調査段階	C&C サーバとの http 通信
攻撃最終目標の遂行段階	C&C サーバとの http 通信

段階でのセキュリティ対策を行う意味がない、すなわち行う必要がないなどと考えるのはいささか早計である。サイバー攻撃は標的型攻撃だけではない。初期潜入段階を想定した当然行っておくべき基本的なセキュリティ対策は、広くさまざまな脅威に対して有効なものであるから、継続的に対策の維持・強化を行いながら、不足している部分を適切に補っていくことが必要と考えられる。

初期潜入段階を想定したセキュリティ対策は、マルウェアの侵入に対する対策ということで「入口対策」と呼ばれる。対して、C&C サーバとの通信による最終目標達成、すなわち情報の窃取を防ぐための対策は「出口対策」と呼ばれている。

システム全体のセキュリティレベルを維持しながら、標的型攻撃への耐性を高めるためには、「入口対策」と「出口対策」にバランスのとれた投資を行って対策を強化していくことが重要である。そのうえで、入口での完全な攻撃排除は難しいことを念頭に置き、マルウェアが内部に侵入してしまった場合に最終目的の遂行を阻止するための「出口対策」が最後の砦になることを意識し、多層的な対策を施すことが有効性の鍵になる。

02-14_地銀08月号 特集-1.indd 8　13.8.21 1:52:47 PM

今日的な対策の手法と有効性

標的型攻撃のような進化する脅威に対して、今日的な防御で大切になってくるのは、数多ある対策手法への投資バランスを考えることだと思われる。ここではそうした防御の手法について述べるとともに、費用対効果からどのような対策を優先的に行えばよいかについて説明する。

A） 入口対策における手法

入口対策は、文字通りマルウェアの侵入を水際で防ぐための入口における対策である。最近の標的型攻撃の傾向をもとに、入口対策としてどんな手法が有効かについて考えてみる。

①送信者詐称を見破る手法

標的型攻撃で用いられるメールは、内部関係者や政府機関などを詐称している例が多いことは先に述べた。このことを逆手に取り、メールの差出人を詐称した場合に現れる特徴をつかんで標的型メールを見破る方法がある。SPF（Sender Policy Framework）と呼ばれる技術がそれである。

どんな組織でも、メールを送信するときには組織のメールサーバを利用するのが普通である。ある会社から送られてくるメールは必ずその会社のメールサーバを発信源としているはずである。しかし、攻撃者はもちろんその組織に属しているわけではないので、異なる発信源から標的型メールを送らざるを得ない（攻撃者が送信元の組織に既に侵入済みで、メールサーバを掌握してしまっているようなケースは除く）。

SPF はその組織の送信メールサーバを登録して公開することで、受信者が正しいメールサーバから送られたメールかどうかを判断することを助けるためのものである。受信者側（すなわち、攻撃を受ける側）が SPF に対応したメール受信サーバを利用していれば、自動的に受け取ったメールの正統性をチェックし、結果によってはそのまま破棄したり、メールヘッダに判定結果を書き込んだりすることができる。

政府機関ドメインは早々に SPF の導入を進めていたこともあって、go.jp ドメインのメールシステムはほぼ100％に近い割合で SPF 登録をすませている。SPF を適切に活用することで、政府機関を騙ったメールはほぼ見分けることは可能といえる。

しかしながらこの方式には弱点もあり、送信側の組織が自分たちの送信メールサーバを登録していない場合には、そもそも判定が行えない。現在 SPF は徐々に普及しつつあり、今後の有効性への期待は高まるものの、政府機関以外を対象とした場合の有効性は現時点では限定的である。

②未知のマルウェアを検出する手法

標的型攻撃で用いられるマルウェアは、そのターゲットに合わせて作成されたマルウェアであることが多く、たまたま良く似たマルウェアの情報が得られている場合などを除き、ウイルス対策ソフトメーカーがマルウェアの情報を入手できないことが多い。マルウェアの情報が入手できない場合は、当然ウイルスパターンファイルには反映されないので、標的型攻撃で用いられるマルウェアは、ウイルス対策ソフトでは検知できないことが多いということになる。

また、検知の可能なマルウェアだったとし

02-14_地銀08月号 特集-1.indd 9 13.8.21 1:52:47 PM

ても、前述したように自分自身をアップデートするなどして、絶え間なく姿を変え続ける機能を持っており、やはりウイルス対策ソフトでの検知には限界がある。

このようなマルウェア対策として有効なのがサンドボックスと呼ばれる検知技術である。

サンドボックス方式のウイルス対策ソフトは、ウイルスのパターンファイルに依存せず、隔離された空間を用意して、実際に疑わしいファイルを動作させてみる。サンドボックスという名称は、子供がどれだけ遊んでも大丈夫な砂場、というところから来ており、サンドボックス内でのプログラムのさまざまな挙動から、マルウェアなのか、正常なファイルなのかを判定する。

例えば、「起動と同時にインターネット接続を試み、何かのファイルをダウンロードしようとする」といった標的型攻撃で用いられるマルウェアに特有の挙動があるが、サンドボックス方式のウイルス対策ソフトは、このような挙動のパターンを多数の事例情報として蓄積しておくことで、マルウェア判定を行う。

サンドボックス型は現時点で未知のマルウェア検知における有望な手法ではあるが、残念ながらこの方式も万能とはいえない。マルウェアの中には自分自身が本当のコンピュータ上にいるのか、それともサンドボックス上にいるのかを判断して、サンドボックス上にいると判定した場合にそのまま動作を停止してしまうものなどが存在するし、そもそも検知側が想定していないような新しい挙動をするものもあり、絶対に検知漏れが発生しないとは言い切れない。

入口対策に限らず、攻撃側と対策側がいたちごっこを繰り返すのが常である。が、確率的に言ってしまえば、既存のアンチウイルスソフトでは検知し切れないウイルス等の８割近くを検知できる製品なども生まれており、複数のアンチウイルスソフトを検討するうえでこうした製品を多層防御を構成する候補として検討する方法も考えられる。

B） 出口対策における手法

出口対策では、情報の窃取、すなわち送信を思い通りに行わせないことに主眼を置くことになる。出口対策についてもどんな手法が有効かについて考えてみる。

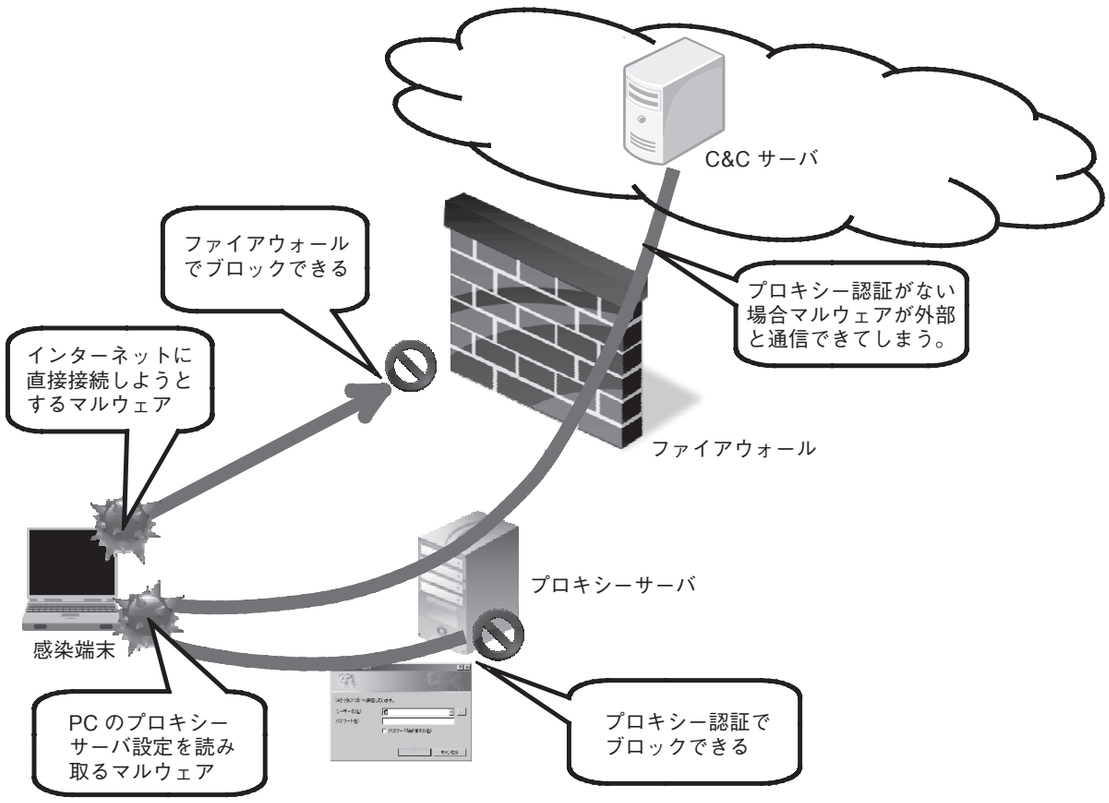
③ Web アクセスの制御による手法

出口対策において一番重要なポイントは、情報伝達の手段であるインターネットへのWWW アクセスの制御である。攻撃基盤構築段階、攻撃最終目標の遂行段階のいずれにおいても、マルウェアは攻撃者の意図に操られて C&C サーバとの WWW 通信を行う。つまり、WWW 通信が意図せぬ送信等を行わないようきちんと制御することができれば、攻撃者の目的遂行を阻害できる可能性は十分に高まるのである。

具体的には、ユーザのコンピュータが直接インターネットへ接続するような構成は避け、制御を行うためのプロキシーサーバを設置することがこれにあたる（図表３）。ただし、単にプロキシーサーバを設置しても、コンピュータのプロキシー設定を読み取りプロキシーサーバ経由で WWW 通信を行うようなマルウェアも存在しているので、プロキシーサーバを設置するだけではなく、プロキシー認証(注16)を有効にすることが大事である。プロキシー認証を利用すれば、マルウェアが行おうとする通信のかなりの部分をブロックする

02-14_地銀08月号 特集-1.indd 10 13.8.21 1:52:47 PM

図表３



ことができる。

あえて述べれば、極めて高度なマルウェアを想定した場合、例えば、内部ネットワークの通信を盗聴され、別のシステムの認証情報がマルウェアに知られて、同じパスワードを使用していたプロキシー認証が破られるケースやユーザのキーボード入力をそのまま横合いから盗み取る、いわゆるキーロガーの機能を持っているマルウェアによって認証情報が盗まれるケースなどでは、プロキシー認証とても絶対とは言い切れない。しかしながら、攻撃者としても高度な技術とかなりの努力をもって攻めない限り破り難い仕組みは構築できるのである。

ここまで述べてきたとおり、残念ながら、どのような対策を施しても100％の標的型攻撃防御を保証できることにはならない。しかし、複数の対策を実施して多層的に防御することで、対策の効果は飛躍的に上がるのが事実である。肝心なことは、まず「これさえやっておけば大丈夫」、「この製品を使えば問題ない」といったことはありえないと考えること、そして、利用しているシステムの弱点を十分に認識し、それらに対応する対策を塗り重ねることである。こうすることで、必ずしも高価な製品を導入しなくても十分に効果の高い対策が施せると考えられる。

(注16) WWW 通信時にユーザ名とパスワードを要求する仕組み

02-14_地銀08月号 特集-1.indd 11 13.8.21 1:52:49 PM

これからのセキュリティ対策

情報セキュリティ対策の考え方が世の中で広く認知されてきたのは、たかだかこの10年程度のことだと思われ、それから現在に至るまで、情報セキュリティ対策の主流を占めていたパラダイムは「既知の攻撃への対策」であった。ウイルスの検知も、不審な通信の検知も、攻撃側が過去に行った実例に対応する形で、その「パターン」に対応するための「対策」として進歩してきた。攻撃の実例を整理し、その対策を打つという考え方は極めて実直であり有効な方法と考えられるので、今後においても主流であることは疑いようもない。

しかし、標的型攻撃のような脅威が登場してくることにより、こうした「既知の攻撃への対策」だけでは限界が見えてきていることも事実である。こうした状況を今後打開していくにあたって、考えられるひとつの方向性は、自律的予測による検出の手法になる。例えば、先に説明した「サンドボックス」のように、「マルウェアの振る舞いや挙動から、攻撃かどうかを検出する技術」の考え方を推し進め、未知の攻撃に対しても、より迅速に対応できるような自律的な機能を備えたセキュリティ製品が新たな主流になってくると考えられる。

もう一つの方向性は、防御の観点を変えて対処より目的達成の阻止を重視するという方向性である。自戒を含めて、これまで攻撃を受ける側の目線は常に攻撃そのものにばかり向いていたのではないかと思う。攻撃に対処する、という考え方が最優先で検討されるべきなのは間違いない。しかし、観点を変えてその攻撃が本当は何を目論んでいるのかという最終目的をあらためて考えてみると、例えば情報の搾取であり、これを阻止して攻撃者の思惑を達成させないのが、標的型攻撃対策における「出口対策」である。

出口対策を重視するということは、マルウェアの侵入への対処に限界があることを認めつつ、仮にマルウェアに侵入されても、攻撃者の最終目的を達成させなければよいという考え方に基づいている。入口対策が100％攻撃を防ぐことができないとすれば、「入口対策」よりも「出口対策」のほうが投資価値があるという考え方も全体を俯瞰したて対策方針と考えることができる。情報セキュリティ対策も、個々の問題対処の目線から、経営観点からの全体最適を目指す方向性に変える転機に差し掛かってきたといえるのではないだろうか。

終　わ　り　に

代表的な情報セキュリティに関するスタンダードである金融情報システムセンターの「安全対策基準」において標的型攻撃に触れている箇所がある。

ここに記載されている内容は標的型攻撃対策に関する一般的な記述と考えられる。対策で述べられていることは、前章までと重複する部分も多いが、入口対策、出口対策を組み合わせた多層防御、定期的な対策の見直し、訓練や教育、さらには専門性組織を整備して迅速かつ適切な対応と早期警戒体制や関係者間情報共有を整備することなど種々の対応が有効とされている。

若干整理する。本編の主旨のひとつは、お読みなったら伝わると思うが技術対策が非常に難しいややこしい話になってきたということである。言ってしまえば、技術力を持った

02-14_地銀08月号 特集-1.indd 12 13.8.21 1:52:49 PM

安全対策基準における標的型攻撃の記述の抜粋(注17)

標的型攻撃は、特定の組織や個人、あるいは特定のシステムや情報を標的とした攻撃である。主な攻撃手法として、コンピュータウイルスが添付された電子メールや、USB メモリ等の可搬型記録媒体を介して対象に侵入する手法がある。

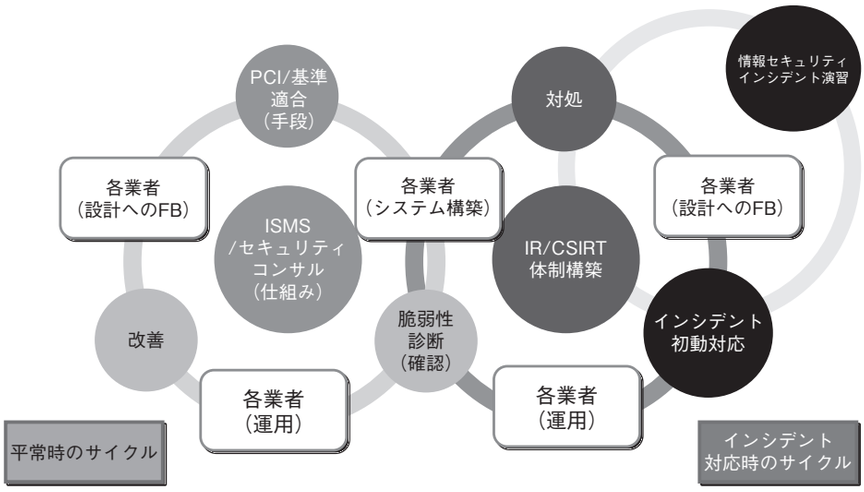
標的型攻撃への対策には、外部からの攻撃の予防・防御を目的とした入口対策（ファイアウォール、抗ウイルスソフトの導入等）のほか、侵入したウイルスの検知、バックドアの構築防止や機密情報の流出防止等を目的とした出口対策（通信ログ、イベントログ等の分析による、不適切な通信の検知・遮断等）があるが、具体的対策を講じる際には、これらを組み合わせた多層防御の形を取ることが有効である。

標的型攻撃は絶えず高度化するため、情報（組織内外のインシデント）収集に努め、定期的に対策を見直し、上記の技術的対策のほか、組織（関係先等も含む）においても標的型メール訓練や各種教育等を定期的に実施することが望ましい。

＜中略＞

また、組織内 CSIRT（Computer Security Incident Response Team）を整備することも、迅速かつ適切な対応や、収集した情報の一元化による早期警戒体制の構築、及び関係者間での情報共有に有効と考えられる。

図表４　CSIRT の持つべき機能



部隊との連携なしにはサイバー攻撃への対処はできない。

また、防御に絶対がないことを認識してもらいたいということも重要で、出口対策はもとより、何かされてしまったことを敏感に迅速に察知して対応に走れる体制が必要になる。具体的には、安全対策基準では CSIRT と紹介されている社内専任（常勤）組織を立ち上

(注17) 出所：「金融機関等コンピュータ・システムの安全対策基準・解説書　（第８版追補）」【技43】（参考３）

02-14_地銀08月号 特集-1.indd 13　13.8.21 1:52:49 PM

げ、最新技術や対処方法等を教示し支援する技術的専門部隊（外部でもやむなし）との連携を確立することになる。

最後に強調したいのは、情報通信システムのすべての利用者がサイバー攻撃や情報セキュリティの概況を理解し、何かおかしければ、即座に専門家に相談するという行動を身につけること（そのための教育・訓練を受けること）が、もろもろの対策を機能させるためのベースとして重要であることを、組織の個々の所属員（銀行であれば一人一人の行員）はもちろん組織全体が認識することが必要だということである。

早乙女　真（さおとめ　まこと）
株式会社NTTデータ経営研究所　シニアスペシャリスト
大手コンピュータメーカーで公共・金融系大規模システム、端末等制御システム、業務パッケージ開発等様々なシステムの開発・企画・移行等に従事した後、2000年より現職。公共機関、大手企業等を中心にITリスクマネジメント、システム監査、情報セキュリティ、アウトソーシング等に関するコンサルティングを行っている。
●資格：特種情報処理技術者、情報処理システム監査技術者
●委員等：IPAソフトウェア高信頼化センター連携委員会委員、JISA技術委員会標準化部会健全性評価指標WG委員

天野　寛生（あまの　ひろお）
NTTデータ先端技術株式会社　シニアエキスパート
2000年から大規模Webメールサービスや検索サービス等様々なシステムの設計・開発に従事した後、2007年より公共機関、大手企業等の情報システムのセキュリティ設計やセキュリティ評価などを中心に、セキュリティ対策全般に携わる。2011年より現職。
●資格：CISSP

02-14_地銀08月号 特集-1.indd 14　13.8.21 1:52:49 PM