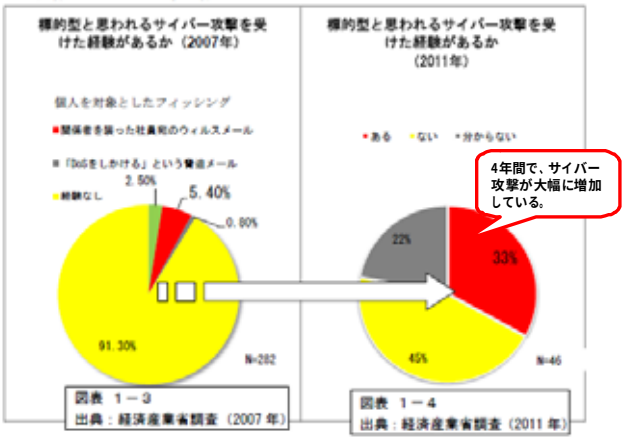
2011.12.1

情報セキュリティニュース ＜2011 No.4＞

忍び寄るサイバー攻撃、狙われる個人と企業

近年、海外では、企業のネットワークに対する攻撃だけでなく、一国の経済と国民生活が麻痺する事態につながりかねないサイバー攻撃が次々と発生している。
日本においても、今春以降、大手電機メーカーや総合機械メーカーをはじめとする名だたる企業や、総務省、地方自治体、衆参両議院などをターゲットにしたサイバー攻撃が続いている。
コンピュータウイルスを用いたサイバー攻撃は従来からあったものの、どちらかというと愉快犯であったり、また不特定多数を対象とするものが多かった。しかし、数年前から、特定の個人や企業の知的財産・重要情報を窃取することや、組織の活動を妨害することを主たる目的とする、プロの犯罪者による「標的型サイバー攻撃」と呼ばれる攻撃が増加している。
「標的型サイバー攻撃」が従来の「サイバー攻撃」と大きく異なるのは、標的者が確実にウイルスに感染するよう巧妙な手口を用いるうえ、「ゼロデイ攻撃（修正プログラム提供前の脆弱性を悪用してウイルス感染させる攻撃）」等を利用するなど、一度標的にされると、情報流出を引き起こすウイルスの感染を防ぐことが非常に困難になる点である。また、ウイルスに感染した後もそのことに気づかせない手法が用いられているため、長期間にわたって企業の主力製品等の機密文書を盗み出され、それを悪用されることによる競争力の低下、果ては企業の存続の危機などに直結する事態が発生しかねない。
本稿では、標的型サイバー攻撃の手法ならびに、その対応策について紹介する。



＜標的型サイバー攻撃の増加＞

（出典：経済産業省　サイバーセキュリティと経済研究会
報告書　中間とりまとめ（2011年8月5日））

＜2011年4月以降に国内で判明したサイバー攻撃＞

判明月	業　種	事　　案
5月	情報・通信業	会員のＩＤ／パスワードを用いた、なりすましによる不正アクセスがなされ、会員がサービスの利用料金に基づき付与されるポイントを不正に利用して商品交換を行った。
8月	金融業	当該金融業者を装い、取引の有無に関わらず不特定多数に不正なメールを送信し、ＩＤやパスワードを盗みとろうとした。
8月	機械製造メーカー	本社や生産拠点など11カ所において、パソコンやサーバ83台がウイルスへ感染していたことが判明した。製品や技術情報の外部流出は確認されていないとしている。
10月／11月	衆議院／参議院	衆院議員の公務用パソコンや衆院内のサーバが今年7月以降、外部からメールで送信されたコンピュータウイルスに感染し、議員ら衆院のネットワーク利用者のＩＤとパスワードが盗まれた。 参院議員の公務用パソコン計29台についても、同様の被害が確認され、情報を抜き取られた恐れがあるとしている。
11月	総務省	総務省の本省と地方の出先機関の業務用のパソコン23台がコンピュータウイルスに感染し、外部に情報が送信されていた。パソコンに保存されていた職員の個人情報や、総務省の業務に関する情報が流出した恐れがあるとしている。

１．標的型サイバー攻撃の現状

今年 7 月に衆議院へのサイバー攻撃が行われた。この事件では、議員用端末のユーザーが、攻撃者から送信された「標的型攻撃メール」の添付ファイルを開いたことから端末がウイルスに感染し、その端末から衆議院のネットワーク内にウイルス感染が拡大したことにより、約 1 ヶ月半の間、多くの情報が流出したと見られている。

ここでは、本件に関する報道や衆議院の議院運営委員会庶務小委員会での報告内容に基づき、このサイバー攻撃の概要を時系列で振り返るとともに、標的型攻撃メールによる攻撃方法について解説する。

＜時系列による衆議院へのサイバー攻撃＞

月　日	攻撃内容・漏洩項目・実行した対策等
2011 年 7 月 25 日	衆議院の3台の議員用貸与端末に、開くとウイルスに感染する添付ファイルをつけたメール(＝標的型攻撃メール）が送付される。 上記端末のうち、2台については、添付ファイルが開かれずに削除され感染はなかったが、1台の端末Ａにおいて添付ファイルが開かれたため、当該端末に「トロイの木馬型ウイルス（亜種)」が感染した。
7 月 25 日 ～26 日	端末ＡのＩＤおよびパスワード、衆議院のネットワークにアクセスするための証明書が窃取される。
7 月 25 日～ 9 月 7 日	端末Ａのメールを盗み見られた可能性あり。
8 月 22 日	サーバーと運用管理端末の管理者権限のＩＤおよびパスワードが流出する。 ＊管理者権限のＩＤおよびパスワードにより、議員用サーバー、運用管理端末および議員用の院内ＬＡＮ端末を操作できる。
8 月 23 日	端末Ａから、議員アカウントサーバー等に不正なプログラムが埋め込まれ、不正サイトへアクセスが発生した。これにより、運用管理端末からドキュメントが流出したと推測される。
8 月 24 日～ 9 月 7 日	すべての議員用貸与端末からのファイル流出の事実は確認されていないが、サーバー上に保存されたメールは盗み見られた可能性あり。
8 月 29 日	運用管理端末から、全議員のＩＤとパスワードのハッシュ値(注 1) 1,142 件が流出した。
9 月 7 日	サーバーと院内 LAN を切り離す。
9 月 16 日	部外への流出防止策が完了する。

（注１）ハッシュ値とは、あるデータ（数値）を、ハッシュ関数と呼ばれる関数で演算した結果のこと。暗号化と同等の効果が得られる。また、ハッシュ値とハッシュ関数が分かっていても、元のデータを算出できないという特徴がある。

1.1.標的型サイバー攻撃の特徴

標的型サイバー攻撃は、特定の組織や個人の端末を確実にウイルスに感染させ、その端末を踏み台にして組織のネットワークに侵入し情報を窃取したり、特定のシステムを破壊すること等を目的としている。インターネットを介した攻撃の場合、その目的を達成するために、一人当たりのウイルス感染率を高めるための工夫がなされている。具体的には、①ソーシャルエンジニアリング(注 2)の利用、②公知でない不正プログラムの利用、③ハードウェアの欠陥やソフトウェアのバグ等の脆弱性の利用などが挙げられる。通常、これらを複合的に組み合わせて攻撃することが多く、様々な攻撃パターンがあるが、上記事例のような標的型攻撃メールを利用する方法が代表的である。

なお、システムへの侵入に成功した後は、ウイルスが、感染したコンピュータを攻撃者が勝手に操作できるようなバックドア（裏口）を作成し、攻撃者が用意しているサーバとの通信経路を確保する。このバックドアを使い、システム内調査に必要な機能を追加して攻撃基盤を構築し、システム内情報の捜索を行う。そして、攻撃者との通信を継続的に行い、システム情報を確認しながら捜索を続け目的を果たすのである。

(注 2)ネットワークの管理者や利用者などから、話術や盗み聞き、盗み見などの「社会的」な手段によって、重要な情報を入手すること。具体的には、ゴミなどの廃棄物から目的の情報を取得する、パソコンのディスプレイ等に張り付けた付箋紙に記入してあるパスワードを見る、あるいはパスワードをキーボードに入力している場面を見るなどの手口がある。

1.2.標的型攻撃メールによる攻撃手法

標的型攻撃メールとは、送信者名の詐称やメールの表題・本文の巧妙な記述により、添付ファイルを開かせたり、本文に記載したリンク先のＵＲＬをクリックさせるよう工夫をされた、特定の個人をターゲットとするメールのことである。

以前から見受けられる不特定多数に送られて次々と感染拡大する大量配布型ウイルスメールと標的型攻撃メールには以下のような違いがある。

	大量配布型ウイルスメール	標的型攻撃メール
送信者	個人名や不明組織	攻撃対象が所属する組織や関係者を詐称
メールの件名・内容	一般的な用件	攻撃対象に関係のある内容や興味のある内容
ウイルス対策ソフトでの検知率	高い（公知の不正プログラム）	低い（公知ではない不正プログラム）
添付ファイルの形式	実行形式（拡張子が bin、exe 等）	文書形式（拡張子が doc、pdf 等）

ウイルス対策ソフトの多くは、世の中に発現しているウイルスを収集し、そのウイルスの情報を登録することでウイルスを検知している。しかし、特定のターゲットに対して限定的に送信されるウイルスについては、情報セキュリティ会社がその情報を収集する機会が少ないため、ウイルス対策ソフトへの登録に時間がかかることが多く、その間のウイルス対策ソフトによる検知には限界がある。

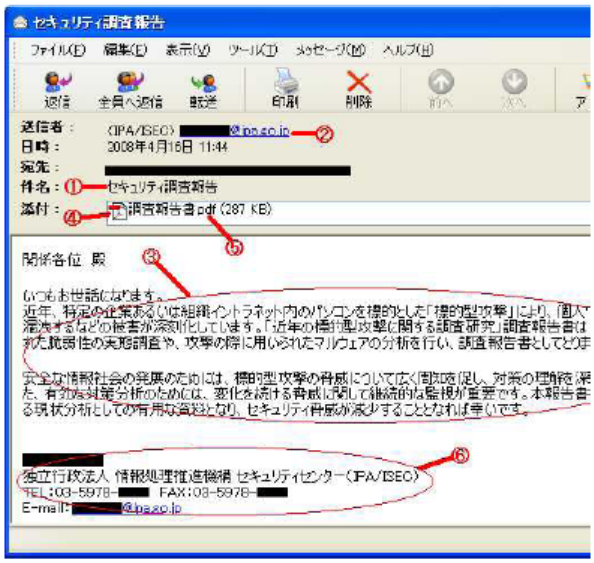
ウイルス対策ソフトでの検知が困難であっても、メールの受信者がそのメールを不審に思えば、添付ファイルを開かない、また、本文に記載されているリンク先に接続しないといった対応をとることができる。しかし、標的型攻撃メールでは、信頼できそうな組織や送信者から、自分に関係のありそうな表題や内容のメールが送られ、かつ、添付ファイルも PDF や Word などの文書形式であるため、ウイルスメールと気づかずに添付ファイルを開いてしまう可能性が高い。

そのうえ、ウイルスに感染しても、パソコン等に特に異常な症状が現れないケースが多く、感染に気づかないまま使用し続けてしまうことで、組織内のネットワークに感染が拡大し、より被害が広がってしまうのである。

以下は、2008 年 4 月に、IPA（独立行政法人情報処理推進機構）をかたって、政府関係組織に送信されたメールである。

このメールの本文や PDF ファイルは、2008 年 3 月に IPA のウエブに公開した報告書のプレスリリースの情報を利用しており、メール受信者をだます手口である以下の①～⑥の条件を満たしている。

＜2008 年 4 月 16 日に IPA をかたって送られたメール例＞



① メールの受信者が興味を持つと思われる件名
② 送信者のメールアドレスが信頼できそうな組織のアドレス
③ 件名に関わる本文
④ 本文の内容に合った添付ファイル名
⑤ 添付ファイルがワープロ文書や PDF ファイルなど
⑥ ②に対応した組織名や個人名などを含む署名

なお、この事例でメールに添付されていた PDF ファイルは、2008 年 2 月 7 日に修正プログラムが提供された Adobe Reader と Acrobat の脆弱性を悪用していた。

（出典：IPA テクニカルウォッチ　標的型攻撃メールの分析に関するレポート）

２．標的型サイバー攻撃の対策

これまでの企業におけるセキュリティ対策は、ファイアウォールやウイルス対策ソフト等によってインターネットを介したウイルス感染を防止する「入口対策」が主体であったが、標的型サイバー攻撃に対しては、入口対策だけでは万全とは言えない。なぜなら前述した事例でもわかるように、組織に属する個人の端末やＵＳＢメモリ等を介してネットワークにウイルスが侵入するリスクが高いからである。このため、入口対策に加えて、万が一ウイルスに感染した場合に情報流出を防ぐための出口対策も必要となる。

2.1.入口対策（ウイルス侵入防止策）とユーザー教育

組織のシステムの入口で技術的対策を徹底しても、ユーザーが悪意のある添付ファイルを誤って開いてしまう、または悪意のあるウエブサイトに接続してしまう等の行動により、ウイルスに感染してしまう可能性を完全に払拭することはできない。

このため、ウイルス感染につながる行動を避けるよう、ユーザーを教育することが必要となる。①事例による怪しいメールの見分け方、②怪しいメールを受信した際の対応、等を平時よりユーザーに周知するとともに、標的型メール攻撃を想定した訓練を繰り返し実施することなどで、ユーザーのレベルアップを図ることが効果的である。

2.2　出口対策（情報流出防止策）

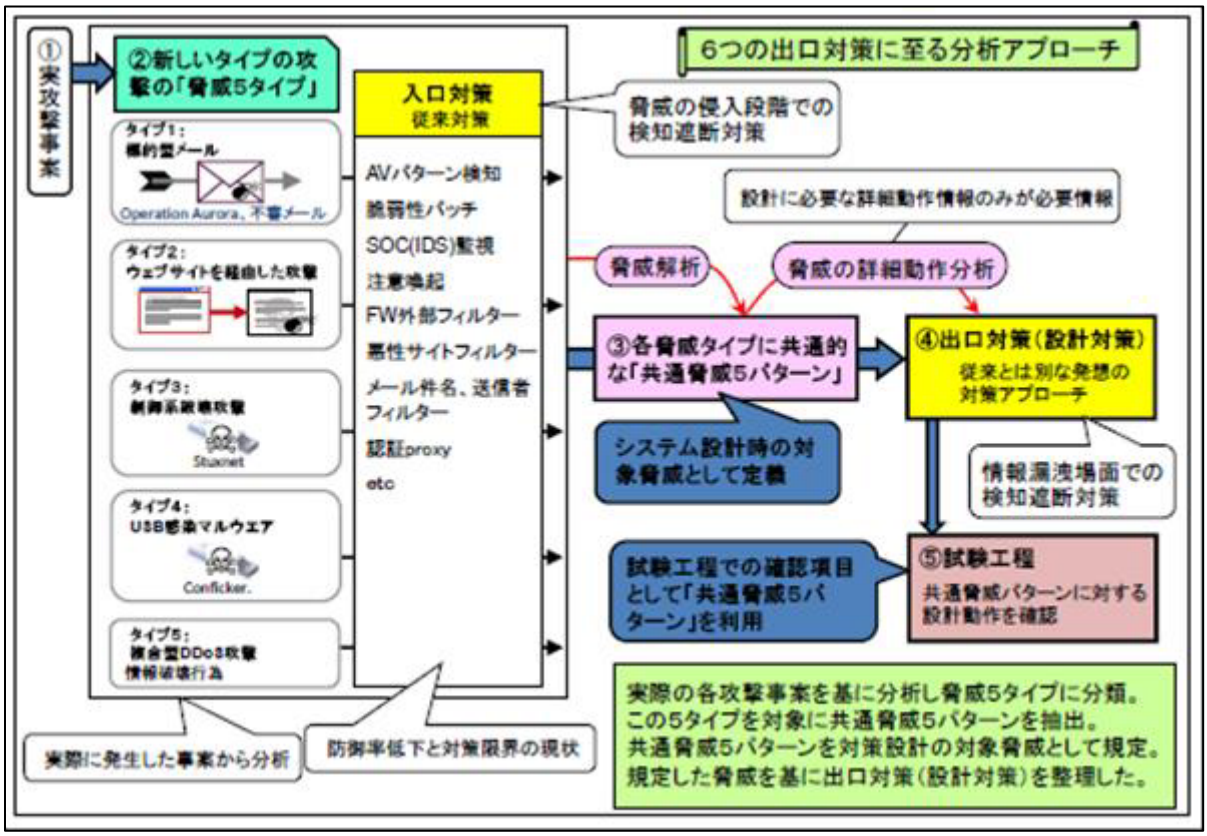
組織として最も大きな被害は、重要な情報が窃取されることや重要なシステムの稼動に障害を与えられることであり、これらの被害を回避することが最も重要な課題になる。

「1.1.標的型サイバー攻撃の特徴」で解説したように、ウイルスがシステムに侵入すると、ウイルスは、上記で記載した被害を目的とした攻撃を行うために、バックドア（裏口）を作成し、攻撃者と通信を行う。よって、通信経路を遮断する「出口対策」は非常に有効である。

この出口対策を実施するうえでは、システムのネットワーク・フロー設計の視点から考える必要があり、出口対策とはシステム設計面での対策手法と言える。

ＩＰＡでは、実際の事案の解析を基に、６つの出口対策を策定している。ここでは対策を策定するまでの考え方と対策の概略を、次頁に参考までに掲載する。

＜「出口対策」策定のアプローチの全体像＞



＜共通脅威５パターンと６つの「出口対策」の関連図＞

（出典：IPA「新しいタイプの攻撃」の対策に向けた設計・運用ガイド）

2.3.クローズ系システムに対する対策

従来、サイバー攻撃はインターネットを介して攻撃する手口が主流であり、インターネットにつながっているオープン系システムを狙う。しかしながら、昨年、原子力発電所においてクローズ系システムである制御システムにウイルスが侵入し攻撃を行う、という事件が発生した。これが、2010 年 7 月に発見された「Stuxnet（スタックスネット）」という名前のウイルス攻撃である。

電力やガス等のインフラの制御システムに限らず、製造業の製造ラインや金融業のＡＴＭ端末を結ぶシステム等の制御・プラント系システムもクローズ系システムであり、常時ネットワークにはつながっていない。そのため、クローズ系システムでは、サイバー攻撃の影響を受けることは考えにくいとされてきた。しかし、オープン系システムとクローズ系システムとの間で情報をやり取りする際にＵＳＢメモリ等を利用するため、このＵＳＢメモリ等がウイルスに感染すると、これを介してクローズ系システムにウイルスが侵入し、情報の窃取や破壊攻撃を受けてしまう。

ただし、情報窃取にかかわるこれらの活動は、オープン系システムを介して行われるため、このような攻撃においても、前述した出口対策の実施とユーザー教育が有効的であると言える。

現時点において、国内では、このような攻撃による情報窃取等の被害が発生したとの報告はないが、海外での発生状況から、いつ同様の事態が発生してもおかしくない状況となっている。

３．おわりに

近年、企業へのサイバー攻撃は、情報を不正に取得し、これを売買することにより金銭を得ることを目的としており、その目的を達成するために、攻撃方法がますます巧妙になっている。残念ながら、ある企業がその標的とされた場合、自社のネットワークを守ることは極めて難しいと言える。例えば、本年 3 月 31 日、福島第一原子力発電所の事故による放射線汚染の恐怖が広まる中、「3 月 30 日放射線量の状況」という件名の添付ファイルがついたウイルスメールが、警察やインフラなどの基幹産業の関係者に送信され、ウイルスに感染する事件が起こっている。

Ｍ＆Ａ・企業提携などのインサイダー情報や研究・開発をはじめとする製品関連の秘密情報、顧客情報等が窃取・悪用されると、計り知れない損失を被りかねない。これを防ぐためには、最新の対策を常に手当てし続けていくことが望まれるが、人的・物的資源を無限に投入することもできない。社会におけるサイバー攻撃の動向、一般に推奨されている対策、自社で保有する情報の種類、自社で実施済みの対策のレベルなどを考慮した上で、自社にとって最適な実行策を検討・実行することが重要である。

インターリスク総研 コンサルティング第二部　ＢＣＭ第二グループ
アソシエイト　沖　　歩　(オキ　アユミ)