サイバー攻撃の脅威とセキュリティ対策

株式会社アイ・ティ・フロンティア
長久　浩三

はじめに

昨年は、政府機関や防衛産業などの企業がサイバー攻撃の被害を受け、日本中に警鐘を鳴らした年になったと言える。かつての、パソコンにウイルスを感染させて驚かせるようなイタズラや技術自慢などの愉快犯とは違い、社会的主張や利益を得るために、ターゲットを定めて、必要とする情報を盗む、あるいはシステムの制御を奪い被害を与えるなど、目的も大きく変わってきている。急速に進化する情報技術に合わせてセキュリティの脅威も進化しているのだ。この脅威から大切な情報やシステムを守るためには、サイバー攻撃の危険性を認識し、対策も進化させて行かなくてはならない。こうした状況で、私は自社の情報セキュリティを担当する立場から、既存の対策を改めて見直す必要があった。そのため、専門家の方々の意見やさまざまな情報機関から、脅威と攻撃の手口に関する情報を収集し、具体的な対策について研究を行った。その成果として、サイバー攻撃の脅威とセキュリティ対策について以下の通りまとめてみた。

1. サイバー攻撃の脅威と危険性

サイバー攻撃は、大きく2種類に分類できる。

一つはターゲットを特定せず、迷惑メールやセキュリティホールを悪用するウイルスなどを無差別に送りつけて、組織や個人に混乱をもたらす古典的なもの。

もう一つは、組織や個人にターゲットを絞り、あらゆる手段を用いて目的の情報を盗む、サービス機能を失わせる（DDoS攻撃）、システムの制御を奪ったりするものである。

後者が標的型攻撃と呼ばれ、2010年以降は「APT（Advanced Persistent Threat）攻撃」という言葉も使われている。APT攻撃の例として、2009年12月にGoogleをはじめとする複数の企業に被害を及ぼした「オーロラ攻撃」がある。ゼロデイアタックの手法によってIE（InternetExplorer）の脆弱性を利用し、知的財産やGmailアカウントを盗むなどの大きな被害を発生させた。

APT攻撃は情報を盗むだけではなく、スタックスネット（Stuxnet）と呼ばれる制御系システムを攻撃した例もある。手口はコンピュータに接続するUSBメモリによって感染を広げ、目的のシステムの制御を奪うというものだ。攻撃にはWindowsのショートカットファイルに存在する脆弱性を悪用しており、ショートカットファイルのアイコンを表示するだけで、任意のプログラムが実行される。

2010年9月に、イランの核燃料施設のウラン濃縮用遠心分離機が標的にされ、この攻撃で約8400台の遠心分離機の全てが稼働不能に陥ったとのニュースもある。また、このような攻撃に使われたソフトウェアは、ブラックマーケットで流通していると言われ、一般企業や個人を対象にした攻撃に広がる恐れもあり警戒が必要である。

制御系システムを狙った攻撃は、日本国内でも起きている。自動車や化学工場の製造ラインを管理する制御システムがウイルスに感染し、操業停止に追い込まれるなどの深刻な被害が、昨年3月までに少なくとも10件発生していることが経済産業省の調査で分かった。今やソフトウェアは、自動車、航空機、列車などの交通機関、水道、電気、ガスなどのライフラインを動かす殆どのシステムに使われており、制御系のシステムを狙った攻撃は、我々の生活や生命を脅かすほど危険性が高いことを認識する必要がある。

2. 標的型攻撃の手口

被害に遭わない為にも手口を認識しておく必要がある。近年の標的型攻撃は主に次のような手法が使われる。

（1）攻撃手法

①初期潜入段階

メールやUSBメモリ、Webサイトの閲覧を通じ

てウイルスに感染させる。
②攻撃基盤構築段階
浸入したPC内でバックドアを作成し、外部のC&Cサーバ（バックドアをコントロールする指令サーバ）と通信を行い、新たなウイルスをダウンロードする。
③システム調査段階
ターゲットの情報やシステムに関わる情報を調査・取得する。
④攻撃最終目的の遂行段階
調査した情報を基に攻撃専用のウイルスをダウンロードして攻撃を遂行し、ターゲットの情報を盗む、またはシステムの制御を奪う。

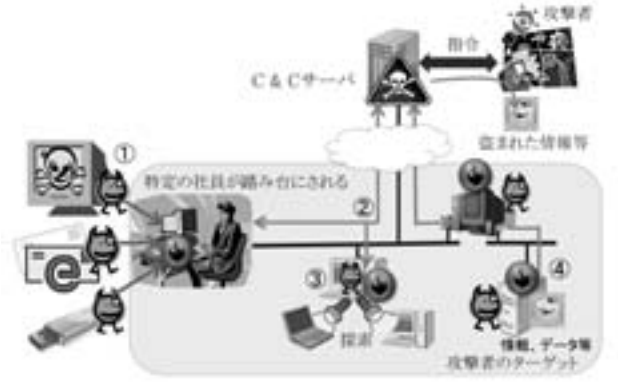


図 1 標的型攻撃の手法

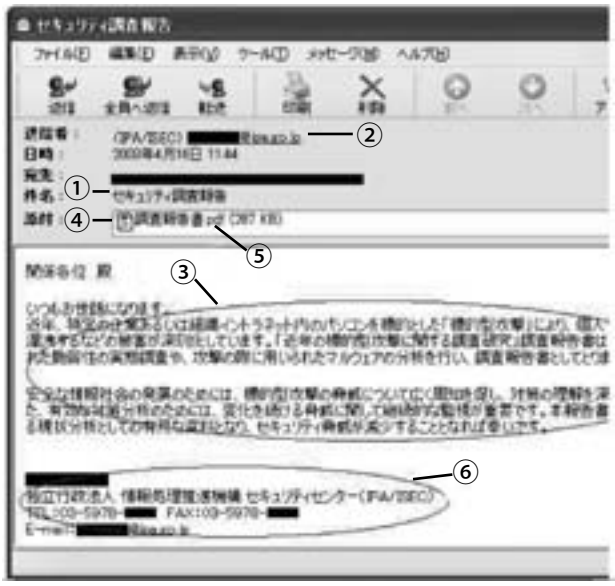
(3) 人の心理の弱点を突くメールなどの手口

これは一般的にソーシャルエンジニアリングとよばれ、人の心の隙間やミスにつけ
込むもので、例えば、ゴミ箱の紙屑などから攻撃の糸口を見つけ、ありとあらゆる
手段を使い情報を盗むなどの方法である。

メールは知人の名前を名乗り、内容もごく日常的なもので送られてくる。見分けるのは難しいが、これまで公開されているケースを見ると、内容はやや唐突感があり、添付ファイルやURLを開くよう誘導する文章が書かれている。不自然な気がしたら、安易に添付ファイルやURLをリクックせずに、電話で送信者に確認するなど、慎重な対応が必要である。

【ウェブ等で公表されている情報を加工して使用した事例】

IPA（独立行政法人情報処理推進機構）の「標的型攻撃メールの分析に関するレポート」から、「メール受信者をだますテクニック」の一部を紹介する。
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ド文書や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



引用：IPA「標的型攻撃メールの分析に関するレポート」

図2　IPA をかたって政府関係組織に送られたメール

【標的型攻撃メールの記載内容の傾向】

メールの内容は、受信者が興味を持ちそうな仕事関係のテーマが多い。例えば「研修会」「会議資料」「情報セキュリティの注意喚起」など、標的に合わせて使い分けられている。

分類	割合	テーマ事例（抽象化済）
イベント	38%	国際会議、シンポジウム、研修会、選挙、法令改正、VIP会合日程、役員人事異動、来訪者情報、社内ウイルス調査
報告書	32%	外交機密文書、国際情勢、海外資源、政府部局報告書、情報セキュリティ調査、ウイルス・不正アクセス届出状況、会議資料
ニュース・注意喚起	30%	東日本大震災、金融情勢、国際情勢、外交情報、政府予算、製品事故、情報セキュリティ注意喚起、新型インフルエンザ

表1　テーマによる分類

引用：IPA「標的型攻撃メールの分析に関するレポート」

(4) 攻撃の手口は進化する

攻撃者は潜入手口を進化させている。新たな手口ではメールにファイルは添付されておらず、Webサイトを案内するURLが添付されており、正規のWebサイトだと思って見ているうちにマルウェアに感染させるような、高度な隠蔽技術が使われる。裏では正規のWebサイトが複数改ざんされ、複数のサーバが乗っ取られて踏み台に使われる。Webアプリの開発担当者やサーバの構築担当者、運用担当者は、脆弱性対策を徹底するだけでなく対策を進化させて行く必要がある。

3. 中国からの攻撃に国際社会では警戒を強めている

中国では複数のグループで形成された「紅客連盟」というハッカー集団が存在する。また、中国政府は人民解放軍所属のハッカー部隊を保有しており、アメリカと中国近隣諸国ではサイバーテロの警戒を強めている。

図3の円グラフは、メールヘッダに記録されたIPアドレスを国別に集計したものである。約1/3が中国で管理するIPアドレスからのものだ。なお、不明の35%は、メールヘッダを入手できなかったものである。

アメリカ国防総省は、昨年5月「外国政府からのサイバー攻撃を『戦争行為』とみなし、サイバー攻撃を受けた際は武力行使も辞さない」と発表した。サイバー空間を陸、海、空、宇宙空間に次ぐ第5の新たな戦場と宣言し「サイバーコマンド」という部隊を創設し本格的な運用を開始している。台湾と中国では経済交流は進んでいるが、水面下では激しい攻防が行われており、台湾はサイバー部隊「老虎部隊」を設立し、中国をはじめとする海外からの攻撃に備えている。サイバー攻撃は、今や世界各国で深刻な問題として取り上げられており、多くの国で対策が進められている。

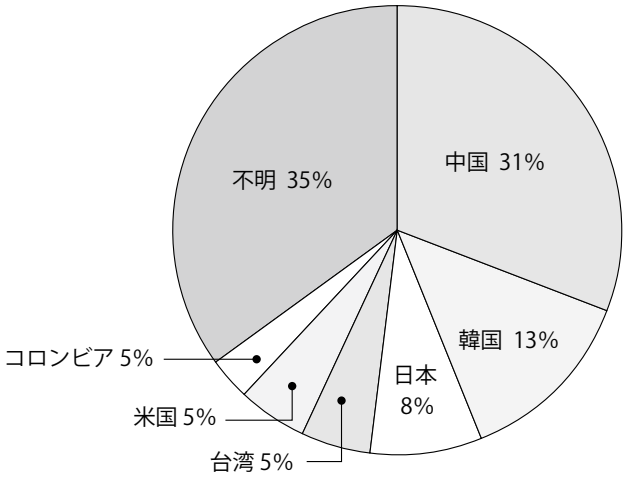


図3　標的型攻撃メール発信 IP アドレスの国別内訳

引用：IPA「標的型攻撃メールの分析に関するレポート」

4. 日本のサイバー攻撃への取り組み

政府は三菱重工業などへのサイバー攻撃をきっかけに、昨年10月に情報セキュリティ政策会議を開催し、政府と経済界を中心に官民が連携してサイバー攻撃の被害防止に取り組むことを決めた。今年1月には、各府省庁にCSIRT（情報セキュリティに即座に対応する組織）の保有を求めるとともに、国の最高情報セキュリティ責任者（CISO）を設置する方針を決めている。

また、今年1月1日の読売新聞で「防衛省が対サイバー兵器を開発」という記事が一面を飾った。防衛省がサイバー攻撃を受けた際に、攻撃経路を逆探知して攻撃元を突き止め、攻撃者のプログラムを無効化するというものだ。

しかし、日本では有事法制でサイバー攻撃が想定されておらず、サイバー兵器を対外的に使用できないばかりか、使用すると逆に刑法のウイルス作成罪などに抵触する可能性もある。また、こういった兵器や活動は、防衛省の自前のシステムを守るためのものであり、国民の生命と財産を守ることは想定されていない。従って、日本ではサイバー攻撃に対しては、自ら守るしかないのが実情だ。政府の一刻も早い法的整備と対策が望まれる。

5. サイバー攻撃への対策

対策は技術的なものだけでなく、組織的、人的といった多重防御で考えることが効果的である。これまでのセキュリティ対策の経験や専門家の意見、IPAなどの情報を基に、取り組むべき対策を以下の7点に纏めた。

(1) 従来の入口対策を見直す

既存の対策を見直し、入口で何を防ぎ、出口で何を防ぐかを考えて、ネットワークを設計することが重要である。そのため、メールゲートウェイやフィルタリング機能を見直す。Webアプリケーションの運用があれば、WAFを適用するなどを検討する。また、以下のようなフィルタリングやスパムメール、マルウェア対策機能を搭載したソリューションを利用するのも有効である。

a. 送られてきたメールの中身を分析し、送信元サーバのIPアドレスや送信者のドメインが悪意のあるものでないか評価する。
b. メールに添付されたファイル名の偽造をチェックしたり、ファイルの中身を解析して実行ファイルが含まれていないか調べる。
c. メールに記載されたURLが安全なサイトかを調べ、スパムメールかを判断し、一定の安全性をクリアーしたものだけを中に入れる。

(2) 出口対策を加える

ウイルスがLAN内に入り込んだ際の動きに注目し、その活動を最小限に抑え、万一浸入されても、情報を外に持ち出させないことがポイントである。

a. 内部プロキシ経由の外向け通信のみ許可し、プロキシを使わない端末からの直接通信を遮断する。
b. システムプロキシにJAVAスクリプトやMETAタグを利用したリダイレクト機能を実装し、リダイレクトに対する応答でウイルス通信を遮断する。
c. ネットワークをVLANなどで細分化し、ウイルスの感染範囲を狭める。
d. LAN内の通信を監視し、普段使われていないサービスの通信が発生したときはその原因を追究する。

(3) 監視の強化と発見時の対応手順を整備する

攻撃者がネットワークに侵入するためには、ターゲットに対して何度もアタックを繰り返す。そのため、普段からファイヤーウォールのログなどを監視し、不審な動きを捉えるようにする。また、不正アクセスやウイルス感染が発覚した際に、何をどうするのか手順を整備し、定期的に訓練を行っておく。

(4) 脆弱性対策を徹底する

攻撃の手口はさまざまだが、脆弱性対策の遅れや放置によって被害を受けた例をよく聞く。従って、いかに脆弱対策を徹底できるかが対策のカギを握る。

a. OSの適正なバッチ適用やウイルス対策ソフトを最新版にする。
b. AdobeやJava、Microsoftなどのアプリケーションソフトの脆弱性対策を徹底する。

c. 徹底するには、利用者から状況報告させ責任者がチェックするといった人間系の人的な対策も有効である。
d. パスワードの脆弱性対策として、パスワードは3種類の文字で8桁以上で類推しにくいものにし、定期的に変更するなどの運用を行う。
e. Webアプリケーションは、設計、開発、テストの各フェーズで脆弱性のチェックを行う。また、ツールなどで脆弱性診断を行うことも有効である。
f. Webサーバに対しては、セキュリティベンダーの脆弱性診断などを活用すると効果的である。
g. オープンソースを使用する場合は、サポートを受けられないケースが多いため、積極的に脆弱性情報を収集し必要な対策を取る。また、ソースは初期設定のままで使用しないことも重要である。
h. プログラムを台帳で管理し、脆弱なプログラムが見つかったら、ただちに影響範囲を特定し対応できるようにする。

(5) サーバを集約する

サーバの設置場所やシステム環境が異なるとセキュリティ対策のバラツキが起き、攻撃を受けた際の影響範囲の特定や対策を取ることが難しくなる場合がある。そのため、出来る限りサーバを集約したほうが監視や対策が容易になる。ただし、集約したことによるリスクもあるのでアセスメントを行うことが重要である。

(6) 重要情報を峻別する

自社にとって価値の高い情報資産は何か、守るべき情報は何処に有るのかを明確にする。重要な情報資産は、単純にWindowsのフォルダーに保管するのではなく、認証機能のある、文書管理ツールなどを使って管理するとよい。また、インターネットからの接続が無い場所に置くことも効果的である。さらに、利用者を限定するなどアクセス権限の管理も必要である。

(7) セキュリティ教育・意識啓発

攻撃者は、人の心の隙間や心理的な弱さを突いてくる。怪しいメールが届いたら添付ファイルやURLを簡単にクリックしない、業務に関係ないWebサイトを閲覧しないよう行動を正すなど、普段から意識を高めておくことが重要である。そのためにサイバー攻撃による危険性の理解、基本動作が出来るよう定期的な教育や確認テスト、掲示板などによる注意喚起、視覚に訴えるポスター掲示、自律的なセキュリティ活動に対する経営の評価など、意識が向上する活動を取り入れることが効果的である。

おわりに

今後も、サイバー空間を舞台にした不正行為は、さらに激しくなると予想される。特にモバイル端末への攻撃は、Androidの脆弱性を狙う攻撃が増える可能性が高い。モバイル端末のドライブバイ攻撃やモバイルボットネットが出現する可能性もある。さらに、水道、電気、ガスなど、日常生活に欠かせない産業システムへの脅威にも警戒が必要だ。また、世界的な経済不安から、標的は情報だけでなく金銭を目当てにする攻撃も増えてくると思われる。人の心理的な部分を突くよう、攻撃の手口はますます巧みになるだろう。脆弱性対策を怠ったり安易な行動は、自分だけでなく多くの人に被害を及ぼすことになる。サイバー攻撃を対岸の火事だと考えず、誰もが目の前にある脅威として認識することが重要である。そのためにも、日々の基本動作を確実にして、危機回避できるよう感度を高めて、対策に取り組むべきである。