特集

インターネットというブランドイメージ

セキュリティの最新動向から考える

有限責任中間法人JPCERTコーディネーションセンター
運用グループ グループマネージャ
伊藤 求

「インターネットというブランドイメージが大きく低下した。」インターネットセキュリティという視点で2005年をふり返った時の筆者の感想である。フィッシング、ボットネット、スパイウェア、Winny・情報流出、ワンクリック詐欺などなど。テレビや新聞に出てくるこれらの“業界用語”は、なにやら“犯罪のニオイがぷんぷん”で、普通にインターネットを利用する人々が、「インターネットは危ない」というような印象を持っても不思議ではないという状況である。

数年前までのインターネットセキュリティの話題といえば、ウイルス・ワーム、ホームページ改ざん、DDoS攻撃など、自分のプログラミング能力やテクニックを誇示するための愉快犯的な行為が多数を占めていたのに対し、昨年からは先の例のような“金銭”にまつわる話がすっかり主役の座に上り詰めてしまった。

それもそのはずである。経済産業省が平成17年6月28日に発表した「平成16年度電子商取引に関する実態・市場規模調査※1」によると、日本における2004年度のB to C-EC（消費者向け電子商取引）の市場規模は5兆6,430億円。さらに、インターネットオークションなどのC to C（一般消費者間取引）についての流通総額は7,840億円。合わせると6兆円を超える金額がインターネット上で取引されていることになる。比較的オンラインショッピングなどの普及が遅れているとされる日本でさえこの規模である。世界マーケットとなるとこの数倍の市場規模がインターネット上に存在することになるわけだ。この巨大な市場を狙って、金儲けを狙う輩が現れても不思議ではない。要するに一般の人々にとっての「インターネットというブランドイメージ」は大きく低下した。しかし、お金儲けを狙う悪意のある人たちには「インターネットが美味しいブランド」になってしまったのだ。

フィッシング

直接“金銭”にまつわる話として、まず“フィッシング”が思い浮かぶ。

改めてフィッシングについて解説すると、「電子メールなどを用いて、銀行、クレジットカード会社、企業、オンラインショップなどを装ったホームページに消費者を誘導し、個人情報、社会保険番号などの信用情報、銀行口座番号やクレジットカード情報、オンライン用のアカウントやパスワードを詐取しようとする行為」となる。

このフィッシングでの“金銭”的被害は相当なものである。Gartner社とAnti-Phishing Working Group※2によると、2003年後半～2004年前半、全米で約5700万人がフィッシングメールを受信し、受信者の19%がサイトをクリック、そして、受信者の3%が個人情報を入力してしまった結果、被害額は銀行・クレジットカード会社を併せ約12億ドル(約1,400億円)。さらに、同じ調査で、2004年後半～2005年は全米で約7300万人がフィッシングメールを受信し、被害額は銀行・クレジットカード会社を併せ約9億3000万ドル(約1,100億円)といった結果が出ている。また、警察庁の資料※3によるとイギリスでは2003年の銀行の被害額が5,000万ポンド(約116億円)、さらに、オーストラリアでも2004年に発生したフィッシングでは、発生から1週間で1銀行あたり1,000万豪ドル(約12億円)の被害が出ているとの調査結果もある。

幸いなことに、日本ではフィッシングの被害はそれほど報告されていない。たとえば、2004年9月～10月にかけて発生した邦銀を対象とするフィッシングサイトの場合は、偽造されたカードが33名分で、うち8名のカードが不正使用され、被害総額が約150万円であった。また、偽ホームページでログイン情報を取得し、メールを盗み見た疑いで逮捕者が出ているというのが主なものであり、海外の例ほど被害(または規模)が大きなものはないようだ。

おそらく、日本でフィッシングの被害が大きくないのは、そもそもインターネット先進国で盛んであったオンラインバンクやオンライン納税といったものが一般に普及する前であったからと、“オレオレ詐欺”や“ATM盗撮”などのような物理セキュリティのスキを突いたものの方が効率よく簡単に行えたからであろうと想像できる。しかし、昨今の株価の上昇機運から急激に盛んになったオンライン株取引などが標的になった場合、新たな被害が発生しないとも限らない。いずれにせよ、技術的、運用的な安全対策が必要であることには違いない。

ボットネット

次に、直接“金銭”をイメージしにくいが、今後最も心配されるものが“ボット”や“ボットネット”である。

ボットとは、悪意のあるプログラムを電子メールやソフトウェアの脆弱性を用いてユーザーのパソコンなどに送り込み、遠隔操作可能なロボット端末(ボット)にしたもの。ボットネットとは、そのボットをネットワーク化したものである。

筆者の所属するJPCERTコーディネーションセンター（JPCERT/CC)とTelecom-ISAC Japan※4が共同で実施した調査によると、ボットの危険性は、“未対策のパソコンをインターネットに接続すると約4分でボット感染する”ということ、“既存のウイルス対策ソフトでは全てを検出できないこと”である。そのため、既に国内のISPユーザーの2～2.5％がボットに感染しているという結果も出ている。

“ボット”や“ボットネット”そのものは、プログラムやネットワークの技術がベースの問題である。しかし、迷惑メールが組み合わされると、“金銭”にまつわる話に変化してしまう。たとえば、迷惑メール送信業者などは、以前のように簡単にメールの大量送信が行えなくなってしまった。各ISPが迷惑メール対策としてOP25B（Out bound Port 25 Blocking：外向き25番ポート通信)などの導入を進めているし、送信元がばれるとすぐに営業停止処分を受ける可能性があるなど迷惑メールに対する法規制なども厳しくなっているからだ。一方、ボットネットは、他人のパソコンを自由自在に操れ、大量のメール送信もリモート操作で簡単に行える。ボットネット運用者と迷惑メール送信業者、お互いの利害が一致するところに市場が発生する。既に、ボットネットは時間あたり○○ドルなどでレンタル売買されているそうで、見事に“金銭”の話に変わってしまっている。

“ボットネット”が“金銭”と無縁でないのは、なにも迷惑メールだけではない。第3者のパソコンが遠隔からコントロール可能であるのだから、フィッシングの踏み台サイトにすることも可能だし、特定のサイトにDDoS攻撃を行うという脅迫行為にも利用することは可能だ。これらは、直接“金銭”に結びつく。このように、上記の例を取ってみても、インターネットセキュリティインシデントに関する傾向が、愉快犯から“金銭”目的に変化して来たことは(少々乱暴ではあるが)明白である。

今後のインターネットセキュリティインシデントの傾向

そこで、今後のインターネットセキュリティインシデントを少々想像してみよう。

筆者が“金銭”方向に向かっているインターネットセキュリティインシデントの代表的な例として“フィッシング”と“ボットネット”を示したのは、最近の技術動向であるからだけではなく、今後発生するであろうイ

※1 経済産業省「平成16年度電子商取引に関する実態・市場規模調査」
http://www.meti.go.jp/press/20050628001/20050628001.html
※2 Anti-Phishing Working Group
http://antiphishing.org/
※3 @police「phishingの現状と対策」
http://www.cyberpolice.go.jp/material/pdf/20040723phishing.pdf
※4 財団法人日本データ通信協会 テレコム・アイザック推進会議
https://www.telecom-isac.jp/

ンシデントは、おそらくこの2つの技術の応用や他の技術を組み合わせた発展型であると考えるからだ。

何しろ“金銭”目的の悪意のある人たちには、目の前に大きなマーケットが広がっている。日本の消費者だけがターゲットだとしても、6兆円。これが企業間電子商取引にまでおよぶとさらに大きい。2004年の狭義のB to B-EC（インターネット技術を用いたコンピュータ・ネットワークシステムを介しての企業間電子商取引行為）が102兆6,990億円。この統計では専用の閉鎖網IP-VPNを用いた取引額をも含むので、その全てがオープンなインターネット用いて行われているとは限らない。しかし、2004年度の日本のGDPが約500兆円※5（内閣府資料より）ということを考えると、この企業間電子商取引というのはかなり巨大なマーケットであることは確かだ。そのため、悪意のある人たちの標的は一般消費者だけでなく、企業間電子商取引に広がる可能性さえある。

たとえば、悪意のある人たちが企業の入札担当者を狙った場合。企業の入札を装ったWebページに“フィッシング”誘導し、彼の端末を“ボット”に感染させる。その端末にはおそらく他企業との電子商取引の情報も含まれているはずである。彼らは、まんまとそれらの情報を取得する。そして、“ボット化”された端末で、他の企業の入札に落札できるような価格で応札する。看板方式のようなジャストインタイムで納品されるような製品で、このような“偽の入札”が行われ、その工場はライン停止の被害が発生する、といったインシデントが発生するかもしれない。

「1台の端末が“フィッシング”や“ボット”の被害に遭うだけで大きなインシデントが発生する可能性」、それがこの予想の怖いところである。システム全体をセキュアな設計にしたとしても、一人のユーザーの何気ない行動で、全てを台無しにする可能性がある。それも通信回線と言ったインフラの事故ではなく、通常用いている端末パソコンのインシデントが原因で……。

対策

さて、このような悪意のある人たちにどのように対抗すればいいのだろうか？

まず、第一に重要なのは現場レベルでの情報共有である。アンチウイルスソフトにも引っかからない“ボット”、限りなく本物と見まがう“フィッシング”は、かなり熟練した技術者でも発見が困難なことが予想される。対策方法を学ぶために、雑誌やWebニュースだけでなく、セミナーや同業者の研究会に参加し、可能な限りの情報収集をする必要がある。しかし、個人や一企業でそれを続けることは時間的にも費用的にも困難が伴う。そのような時、同業の現場担当者レベルで情報を共有できるのであれば、より自分たちの環境の危機レベルが意識しやすい。なぜなら、インシデントには流行があり、比較的似通った環境が続けて被害に遭うことが多いからだ。

次に、経営者レベルでコンピュータセキュリティ対策を意識することが重要である。インシデントに遭って、慌てて対応を行い、取り返しのつかない事態にならないように、経営者主導のインシデントを想定したマニュアルなどの整備が必要である。マニュアルでは、インシデントが起こった時の連絡方法や行動指針、対処法を取り決め、指揮命令系統を明確にすることも必要であろう。そして、社内の情報流通のしくみができれば、先に集めた現場レベルの熱い情報を、必要な関係者に周知・共有できる体制の構築も可能になる。このように経営者レベルが現場の情報を意識するだけで、かなりセキュリティレベルが上がるはずである。

さいごに

我々 JPCERT/CCでは、現在の主要3業務（インシデントレスポンス、定点観測、脆弱性情報流通）に加え、最新のコンピュータセキュリティに関する脅威情報を提供する“早期警戒情報業務”を開始した。現在、従来の業務から集まったコンピュータセキュリティに関する“熱い情報”を、適切なタイミングで適切なユーザーに提供するための体制を構築中である。今後も、我々の発信する情報にご注目いただきたい。

※5 内閣府「平成15年度国民経済計算（93SNA）」
http://www.esri.cao.go.jp/jp/sna/h17-nenpou/17annual-report-j.html