不正アクセスとウイルス感染

鈴木 直美　フリーライター

ネットバンキングの不正送金が件数・被害金額とも激増
プラットフォーム広げるウイルス、脆弱性狙う標的型攻撃

2011年中に全国の都道府県警察のサイバー犯罪相談窓口などに寄せられた、不正アクセスに関する相談受理件数は、2年続いた減少傾向から一転し、前年から850件増えた4191件だった。一方、警察が検挙できた不正アクセス事件の数は103件、検挙人員は114件と、ここ数年間は大きな変化はない。

警察の検挙は、主に国内からの不正アクセス事件であるため、犯行を繰り返していた国内犯が検挙されると、検挙件数や認知件数が上昇する。2011年は、この手の検挙事件が少なかったようで、認知件数の多くを占めていた国内からのアクセスが前年の1755件から678件へ、容疑者の取り調べなどの警察活動による認知が前年の1488件から75件へと、それぞれ大幅な減少を見せている。

フィッシング多発～ネット銀行の不正送金激増

警察が認知した不正アクセス行為後の行為の内訳では、インターネットショッピングの不正購入が前年の12件から172件に、インターネットバンキングの不正送金が前年の22件から188件に跳ね上がっている。

前者に相当する検挙事例としては、ヤフーを装うフィッシングでカード情報などを入手し、インターネットショッピングで合計約1億円相当の商品をだまし取っていた詐欺グループの摘発が挙げられる。フィッシングによるカード情報の不正入手は割賦販売法違反になり、それを使って商品をだまし取ると詐取罪に相当する。不正使用時にクレジットカード会社の認証パスワードを使えば、カード会社のウェブサイトへの不正アクセスが問われる。

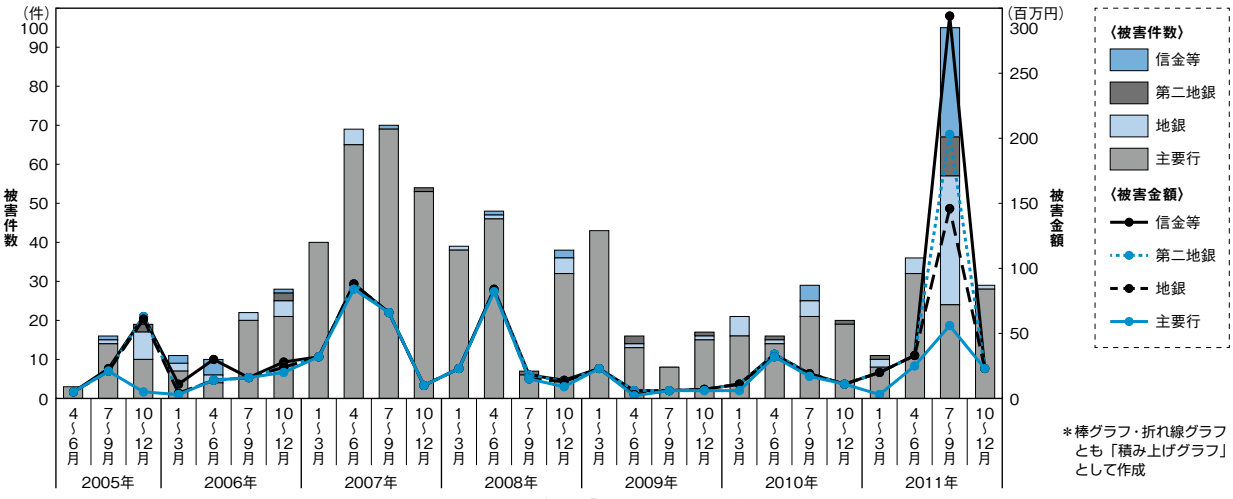
国内ユーザーを狙ったヤフーを装うフィッシングは、2004年にアカウント情報の詐取で始まり、やがてカード情報の詐取へとシフトする。2009年中盤からは、この手のフィッシングを頻繁に仕掛けるグループが次々に現れ、ヤフーのフィッシングが大量発生した。検挙者は、国内初のフィッシング摘発となった2005年以来、毎年出ており、2009年からの大量発生に関与したグループは、2010年から2012年にかけての摘発でほぼ一掃されたようだ。

インターネットバンキングの不正送金激増は、2011年6月下旬頃から始まったウイルスによるアカウント情報の窃取と、その後に続いた各行を標的としたフィッシングが大きな要因となっている。こうした攻撃は2004年秋ごろから見られるようになったが、これほどまでに大規模かつ執拗に行われた例はない。資料6-2-1は、金融庁が四半期ごとにまとめている被害発生状況だが、件数と被害金額は共に、2011年7～9月期が突出していることが見て取れる。地方銀行や信用金庫などでこれまでにない大きな被害が出ているのも特徴的だ。これは、同じサービスを使う地銀や信金のネットバンキングのアカウント情報が、何らかの方法でパソコン内に送り込まれたウイルスに盗み取られたためとみられる。

2011年の夏以降は、各行を装ったメールを不特定多数に送り、セキュリティー向上のためなどとして誘導先の偽サイトや添付したフォームにアカウント情報などを入力させようとするフィッシングが多発するようになる。標的となった銀行は、固定パスワードのほかに乱数表を使用しており、この乱数表の数字もすべて入力させようとするのが特徴だ。

一連の不正送金事件では、現金の引き出しなどに関わった国内在住の中国人が何人も検挙されているが、

資料6-2-1　インターネットバンキングによる不正払い戻し被害の発生状況



＊棒グラフ・折れ線グラフとも「積み上げグラフ」として作成

出所　金融庁「偽造キャッシュカード等による被害発生等の状況について」2005-2011年度版をもとに筆者が作成

全容はいまだ明らかになっておらず、2012年に入ってからも依然としてフィッシングが続いている。

カード情報の不正取得は2009年12月に施行された改正割賦販売法で処罰対象となり、2011～2012年の摘発には同法も適用されている。規定のなかったアカウント情報の不正取得に関しては、2012年5月に施行された改正不正アクセス禁止法に盛り込まれた。改正法では、不正取得や保管、要求する行為が禁止され、フィッシングサイトの開設やフィッシングメールの送信はそれ自体が処罰の対象となっており、被害の未然防止につながることが期待されている。

Mac、Andoroid狙うウイルスが拡大 政財界ターゲットに標的型攻撃

全国の警察が受理したコンピュータウイルス（マルウエア）に関する相談は3年連続で増加し、2011年は前年から101件増の428件だった。これまでウイルス自体を対象とした法律はなく、被害に応じて詐欺罪や不正アクセス禁止法違反などを適用していたが、2011年7月に施行された改正刑法に「不正指令電磁的記録に関する罪」（ウイルス罪）が新設され、同罪による検挙が2011年中に3件あった。

2011年のウイルス攻撃では、攻撃対象がMacやAndroid端末へと本格的に広がり始めた点と、特定の企業や機関を狙ったとみられる標的型攻撃が国内で大きな話題になった点が特筆される。

Macを狙ったこれまでの攻撃は、数も感染規模もそれほど大きなものではなかった。しかし、2011年春ごろからWindowsユーザーを標的としていた偽セキュリティーソフトにMac版が加わり、使用しているOSに応じた攻撃を展開、秋には、Flash Playerのインストーラーに偽装して実行させようとする「Flashback」が登場する。この「Flashback」は、年が明けてからは未修整の脆弱性を悪用した自動実行を併用するようになり、セキュリティー企業各社によると60万台という大規模な感染へと発展した。

スマートフォンの急速な普及に伴い、Andoroid端末が標的となるケースも目立ち始めている。こちらはもっぱらアプリケーションを装ってユーザーにインストールさせる手法だが、2011年末からはクリック詐欺での悪用が始まり、その後も国産のものがいくつか見つかっている。数も規模もパソコンウイルスの比ではないが、確実に広がりを見せているようだ。

標的型攻撃は、東日本大震災の発生後、震災や原発事故に関連した情報提供を装ったものが民間企業などを標的に、頻繁に送付されるようになった。警察庁が国内の企業4000社と共に立ち上げた、標的型メールの情報共有ネットワークの集計では、4月以降の2011年中に確認された標的型メールは1052件に上る。標的型メールの多くは、添付ファイルを開くとソフトウエアの脆弱性を突いて感染する手法を用いている。そのほとんどは、アップデートを欠かさなければ感染には至らないものばかりだったが、防衛関連企業や衆参議院など、感染被害が相次ぎ表面化し、大きな問題と認識されるようになった。

［インターネット白書ARCHIVES］ご利用上の注意

このファイルは、株式会社インプレスR&Dが1996年～2012年までに発行したインターネットの年鑑『インターネット白書』の誌面をPDF化し、「インターネット白書ARCHIVES」として以下のウェブサイトで公開しているものです。

http://IWParchives.jp/

このファイルをご利用いただくにあたり、下記の注意事項を必ずお読みください。

- 記載されている内容（技術解説、データ、URL、名称など）は発行当時のものです。
- 収録されている内容は著作権法上の保護を受けています。著作権はそれぞれの記事の著作者（執筆者、写真・図の作成者、編集部など）が保持しています。
- 著作者から許諾が得られなかった著作物は掲載されていない場合があります。
- このファイルの内容を改変したり、商用目的として再利用したりすることはできません。あくまで個人や企業の非商用利用での閲覧、複製、送信に限られます。
- 収録されている内容を何らかの媒体に引用としてご利用される際は、出典として媒体名および年号、該当ページ番号、発行元（株式会社インプレスR&D）などの情報をご明記ください。
- オリジナルの発行時点では、株式会社インプレスR&D（初期は株式会社インプレス）と著作権者は内容が正確なものであるように最大限に努めましたが、すべての情報が完全に正確であることは保証できません。このファイルの内容に起因する直接的および間接的な損害に対して、一切の責任を負いません。お客様個人の責任においてご利用ください。

お問い合わせ先 | 株式会社インプレスR&D | ✉ iwp-info@impress.co.jp