

不正アクセスの動向

鈴木直美 ●フリーライター

金銭目的がさらに増え、手口はパスワードクラッキングへ SQLインジェクション攻撃による不正アクセス多発

2008年に都道府県警察のサイバー犯罪相談窓口等に寄せられた、不正アクセス、コンピューターウイルスに関する相談は、前年より50.5%増加し4522件。2年連続の減少から一転し、過去最高の件数となった。不正アクセス行為の認知件数は、前年比25.9%増の2289件、検挙件数は20.7%増の1740件と、ともに増加を続けている。検挙した1740件の事件数は前年の86件から101件に(17.4%増)、検挙者は126人から137人(8.7%)となっており、何人かのグループによる大規模な不正アクセス行為が、その多くを占めている様子が見えてくる。

ますます増える金銭目的の不正アクセス

検挙件数のうち、不正アクセスの動機として「不正に金を得るため」を挙げたものは、1498件(312件・26.3%増)と、激増した前年をさらに上回る結果となった。金銭目的の傾向はますます強くなり、全体の86.2%を占める。次いでオンラインゲームの不正操作が13件減の120件、嫌がらせや仕返し10件減の52件、好奇心を満たすための38件減の17件と続く。

フィッシングからパスワードクラッキングへ

検挙事件における不正アクセスの手口は、前年最多だったフィッシングによる入手が、1157件から88件へと大きく減少。変わって、パスワードの設定や管理の甘さにつけ込んだものが、前年の139件から1368件へと激増。全体の8割近くを占めている。次いで、パスワード等を知りうる立場にあった元従業員や知人等によるものが、前年の39件から163件に。減ってはいるものの、フィッシングが88件、スパイウェア等のプログラムを使用しての入手が48件(前年55件)と、巧妙な手口によるものも依然として発生している。

SQLインジェクション攻撃による不正アクセス多発

2007年5月に滋賀県の企業支援サイトに脆弱性を突いて侵入し、出会い系サイトの宣伝などを書き込んだとして、

大阪の出会い系業者らが2月に検挙された。2008年に検挙されたセキュリティホール攻撃型の不正アクセスは、この1件のみだが、通販サイトを攻撃してクレジットカード情報などを盗み取り、不正に使用される被害が多発した。

4月に千葉の業者が9万7500件、5月に都内の業者が2万件、7月に仙台の業者が2万8000件、9月に都内の業者が1万8000件の顧客情報流出を公表。いずれも、データベースアプリケーションの脆弱性を狙う、SQLインジェクションと呼ばれる手法が使われた海外からの攻撃で、クレジットカードの不正使用に気づいたカード会社からの指摘で発覚した。また、カード番号の下4桁を保存していなかったため不正使用には至らなかったが、8月には大阪の業者が65万3000件の流出を公表。これも、カード会社からの指摘で発覚した。カードが不正に使われた被害者らは、オンラインゲームのアイテムなどが購入されたこと証言しており、オンラインゲームのアイテムや通貨を売買するRMT(リアルマネートレーディング)での換金を目論んだ犯行とみられる。

このSQLインジェクションによる不正アクセスには、閲覧者をウイルス感染させるためのコードがサイトに埋め込まれる、改ざん被害も多発した。

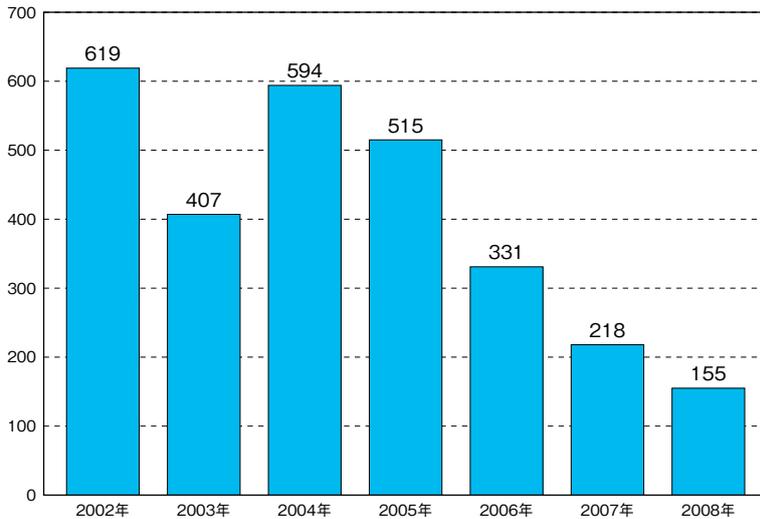
フィッシング被害は偽サイトのホストにも注視

フィッシングがらみの不正アクセスには、情報を詐取された側の被害と、ホームページなどにフィッシングサイトが設置された側の被害がある。前者については、検挙事件は激減し、金融庁発表のネットバンキングによる不正引き出し被害も減少方向にある。が、2008年も銀行やクレジットカードなどの金融機関に加え、ポータルサイトのアカウントを盗み取ろうとするフィッシングメールとサイトがいくつか出現した。

国内でホストされたフィッシングサイトは、RSAセキュリティによると年間で1000件余り。ほとんどは海外ブランドのフィッシングで、国内の利用者に直接被害が及ぶものではないが、一般の国内サイトが外部から侵入され、偽サイトを構築されるというケースが多数を占めるという点に注

■ 届出件数、実害件数ともに減少

資料 6-2-3 不正アクセス届出件数の推移

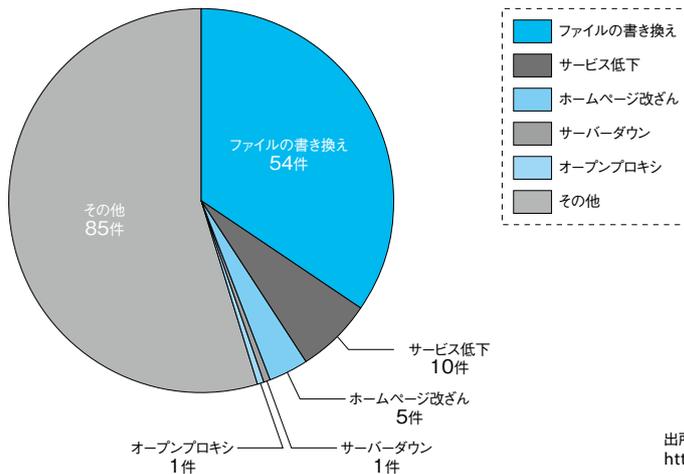


2008年にIPA（情報処理推進機構）に届出のあった不正アクセスの件数は、前年の218件から155件（28.9%減）に。このうち実際に被害があったケースは、前年の162件から120件（25.9%減）と、ともに大幅な減少となった。本年は、法人や機関からの届出の減少が顕著で、個人からの届出が45%を占める。

出所 IPA「2008年のコンピュータ不正アクセス届出状況」2009年1月
<http://www.ipa.go.jp/security/txt/2009/documents/2008all-cra.pdf>

■ 被害内容はファイルの書き換えが多数を占める

資料 6-2-4 実際に被害があった届出件数と被害の種別



届出のうち実際に被害が生じたケースの被害内容の分類では、例年どおりプログラムの埋め込みを含むファイルの書き換えが多く寄せられた。不正アクセスを許した原因として、IDやパスワード管理不備や古いバージョンのソフトウェアの使用、パッチの未導入など、基本的なセキュリティ対策がなされていないサイトが狙われていると、IPAでは推測している。

出所 IPA「2008年のコンピュータ不正アクセス届出状況」2009年1月
<http://www.ipa.go.jp/security/txt/2009/documents/2008all-cra.pdf>

視したい。また、ボットと呼ばれるウイルスの一種に感染したPCのネットワーク「ボットネット」を操り、感染PCに偽サイトをホストさせるフィッシングも多数出現。ボットネットには、国内の利用者のPCも頻りに登場している。フィッシング対策には、自身がだまされないための対策とともに、こうした偽サイトをホストしないための、不正アクセス対策やボット対策にも注意を払う必要がある。

参考文献

- ・警察庁「平成20年中のサイバー犯罪の検挙状況等について」2009年2月
<http://www.npa.go.jp/cyber/statics/h20/pdf46.pdf>
- ・国家公安委員会、総務省、経済産業省「不正アクセス行為の発生状況及びアクセス制御機能に関する技術の研究開発の状況」2009年2月
<http://www.npa.go.jp/cyber/statics/h20/pdf47.pdf>
- ・金融庁「インターネット・バンキングによる預金等不正払戻し（被害発生状況・補償状況）」2009年3月
<http://www.fsa.go.jp/news/20/ginkou/20090318-2/04.pdf>



[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。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