不正アクセスの動向

鈴木 直美　フリーライター

増加の一途をたどる検挙件数とオークション不正操作
サイト改ざんはSQLインジェクションからガンブラーへ

2009年中に都道府県警察から警察庁に報告があった不正アクセス行為の「認知件数」は前年から506件増えて2795件あり、「検挙件数」は前年より795件増えて2532件あった。

大規模化するオークションの不正アクセス

検挙した個々の事件で行われた犯罪行為の総件数を示す「検挙件数」は、過去5年間にわたって増加を続け、約9倍にまで膨れ上がった。ところが、事件数や検挙者数にはそれほど大きな変化はない。事件数は前年の101件から95件に、検挙者は135人から114人へ共に減少しているほどだ。つまり1つの事件に含まれる犯罪行為数が多いということで、不正アクセスの大規模化が見てとれる。

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、前年から747件増の2245件。次いで「好奇心を満たすため」が148件増の165件、「オンラインゲームの不正操作」が57件減の63件と続く。検挙件数を押し上げている要因は、桁違いに多い「不正に金を得るため」という動機にほかならない。金銭目的の動機はこの5年間で約13倍に増えた。動機全体に占める割合は約3割増え、2009年は9割（88.7%）に達している。

不正アクセス行為後に行われた行為は、なりすまし出品などのインターネットオークションの不正操作が最も多く、過去最多だった前年の1559件をさらに上回る2152件。検挙件数と歩調を合わせるように、5年間にわたって増加の一途をたどっている。次いでオンラインゲームの不正操作が345件、情報の不正入手が185件と続く。

以上を考え合わせると、金銭を目的としたインターネットオークションの不正操作が、年々大規模化している様子が鮮明に浮かび上がってくる。

不正アクセスの手口は大きく変動

検挙事件における不正アクセスの手口は、前年1368件に激増したパスワードの設定や管理の甘さにつけ込んだものが、58件へと大幅に後退。代わって、前年88件に激減していたフィッシングによる入手が2084件と再び最多となった。次いで、共犯者などからの入手167件、他人から購入したもの92件、識別符号を知り得る立場にあった元従業員や知人などによるもの61件と続く。

手口の極端な増減から推察できるのは、フィッシングとパスワードクラッキングが、大規模なインターネットオークションの不正アクセスの主な手口であることだ。そして、犯人あるいは犯人グループによって手口に偏りがあり、その年の検挙者によって件数が大きく変動するということである。

SQLインジェクションからガンブラーへ

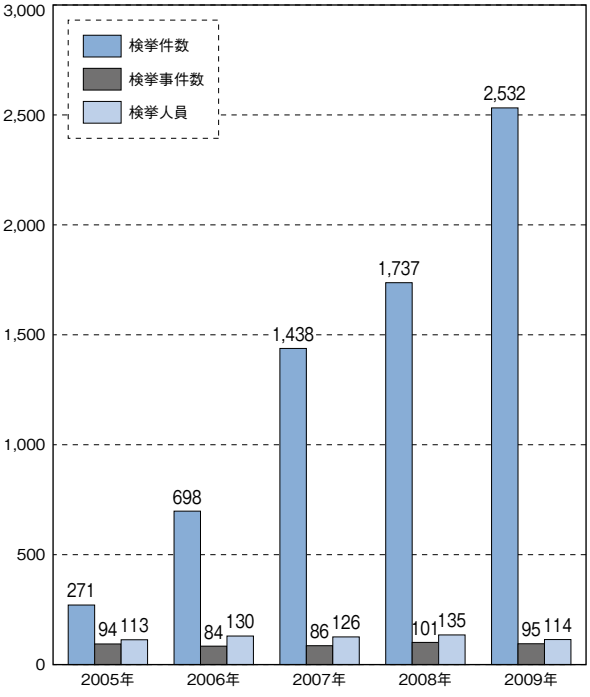
ウェブサーバーの脆弱性を突くSQLインジェクションという手法を使ったサイト改ざん攻撃が、2008年春から国内でも多発した。年末から2009年の年明けにかけては、それまでの数百倍という凄まじい数の攻撃が集中し、著名な企業やサービス、自治体など、多数の正規サイトが改ざん被害を受けた。

SQLインジェクションによるサイト改ざんは、閲覧者

インターネット白書／ ©1996-2012 Impress R&D

検挙件数は急増、検挙事件数などはほぼ一定～事件の大規模化示す

資料6-2-6 不正アクセス行為の検挙件数、検挙事件数、人員数の推移



出所　国家公安委員会ほか「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」2010年3月
http://www.npa.go.jp/cyber/statics/h21/pdf53.pdf

検挙件数（1つの事件で行われた犯罪行為の総数）は増加を続けているが、事件数や検挙者数に大きな変化はない。どころか、2009年は事件数・検挙者数とも前年より減少している。これらは個々の事件が大規模化していることを示している。

不正アクセス行為の動機は9割が「金のため」

資料6-2-7 不正アクセス行為「動機」の内訳

	2008年	2009年
不正に金を得るため（件）	1,498	2,245
好奇心を満たすため	17	165
オンラインゲームで不正操作を行うため	120	63
嫌がらせや仕返しのため	52	34
顧客データの収集等情報を不正に入手するため	12	19
料金の請求を免れるため	3	4
その他	35	2
計	**1,737**	**2,532**

出所　国家公安委員会ほか「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」2010年3月

動機の「不正に金を得るため」は、2005年から2009年の5年間で約13倍に増えている。2009年は2245件（前年から747件増）で、動機全体の9割（88.7%）に達した。

をウイルスに感染させるための、不正なタグの埋め込みに用いられた。改ざんされたページを閲覧するだけで、ブラウザーやプラグインなどの脆弱性を突く攻撃コードが実行され、自動的にウイルスに感染してしまう、ドライブバイダウンロードと呼ばれる攻撃である。

SQLインジェクションによる改ざん攻撃は、年末年始をピークに急速に減退したが、4月からは別の改ざん攻撃が国内のウェブサイトを襲った。ウイルスに感染したパソコンからサイト更新用のFTP情報を盗み取り、それを使って不正アクセスして改ざんするという手法だ。目的はドライブバイダウンロードを仕掛けるための改ざんであり、被害が拡大した5月の連休頃に使われていた攻撃サイトのドメイン名から、後にGumblar（ガンブラー）と呼ばれるようになった。詳しくはコンピュータウイルスの項に譲るが、このガンブラーに端を発する新たな攻撃の連鎖が、秋から国内サイトで爆発的に広がり始め、2010年にかけてパンデミック状態を引き起こした。

手口は「管理の甘さ」「フィッシング」が極端に増減

資料6-2-8 不正アクセス行為「犯行の手口」内訳

	2008年	2009年
識別符号窃用型（件）	1,736	2,529
フィッシングサイトにより入手したもの	88	2,084
共犯者等から入手したもの	7	167
他人から購入したもの	24	92
識別符号を知り得る立場にあった元従業員や知人等によるもの	163	61
利用権者のパスワードの設定・管理の甘さにつけ込んだもの	1,368	58
言葉巧みに利用権者から聞き出した又はのぞき見たもの	26	12
スパイウェア等のプログラムを使用して識別符号を入手したもの	48	8
ファイル交換ソフトや暴露ウイルスで流出した識別符号を含む情報を利用したもの	6	0
その他	6	47
セキュリティ・ホール攻撃型	**1**	**3**

出所　国家公安委員会ほか「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」2010年3月

「パスワードの設定・管理の甘さにつけ込んだもの」は、2008年は前年から激増して1368件になったが、2009年には58件に激減。「フィッシングサイトにより入手したもの」は2008年は前年から激減して88件になったが、2009年には2084件に激増。手口の極端な増減から、犯人グループの手口に偏りがあること等が推察できる（本文参照）。

インターネット白書／ ©1996-2012 Impress R&D

Internet White Paper ARCHIVES
インターネット白書
ARCHIVES
1996,1997,1998,1999,2000

［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

©1996-2012 Impress R&D, All rights reserved.