Special
“情報＝資産”価値に応じた情報漏洩対策とは？

情報漏洩の現実と傾向

NPO 日本ネットワークセキュリティ協会
主席研究員　安田直義（㈱ディアイティ）

インターネットは、社会基盤として使われるコミュニケーション手段として、市民生活になくてはならないものになっている。しかし、普及につれて、新しいメディアが定着する際に特有な問題点も現れてきている。情報が資産であることは今も昔も変わりないが、情報漏洩の量的規模、地域性、実行容易性などの面で、コンピュータとインターネットは、今までになかった問題点を提示してきてもいる。

情報を取り巻く環境

情報はお金になるという意味で「価値」がある。「情報＝資産」なのである。企業活動の基礎情報としての価値はもちろんだが、情報自体が売買されている。名簿屋さんに卒業生名簿や在校生名簿、社員名簿などが「売れる」のである。情報は、今までは「紙」にプリントされた形が主流だったが、パソコンやインターネットの普及とともに、デジタルデータが使われるようになってきた。これに伴い、まず量的な爆発が起こっている。紙では1,000人分のデータもあれば、かなり嵩張るだろうが、デジタルデータでは数百万人分のデータでもUSBメモリひとつに収まってしまうのである。データ量の多寡は、データが予期しない不生な移動を行う際の、大きな制約事項とはならなくなってきているのである。

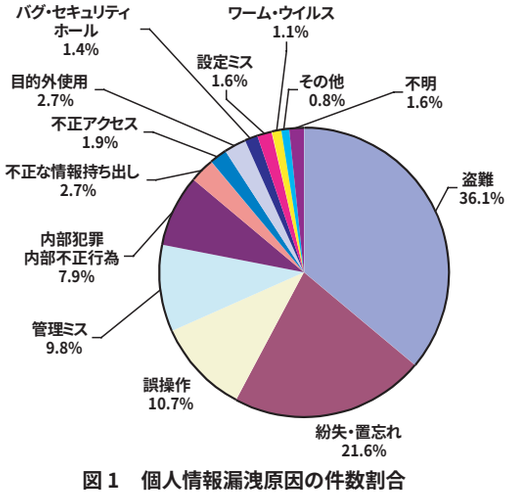

図１　個人情報漏洩原因の件数割合

No.	要素	原因	%	対応する原因
1	技術的	人為ミス	22.1	設定ミス、誤操作、管理ミス
2	技術的	対策不足	4.4	バグ・セキュリティホール、ウイルス、不正アクセス
3	非技術的	人為ミス	24.3	置忘れ、目的外利用
4	非技術的	犯罪	46.7	内部犯罪、情報持ち出し、盗難
5	その他	その他、不明	2.4	その他、不明

図２　個人情報漏洩原因の分類

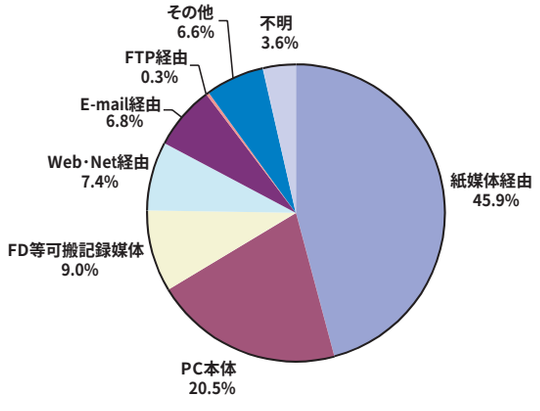

図３　個人情報漏洩経路の件数割合

No.	要素	%	経路
1	インターネット	14.5	Web・Net経由、E-mail経由、FTP経由
2	媒体	75.4	紙媒体、FD等可搬記録媒体、PC本体
3	その他、不明	10.2	その他、不明

図４　個人情報漏洩経路の分類

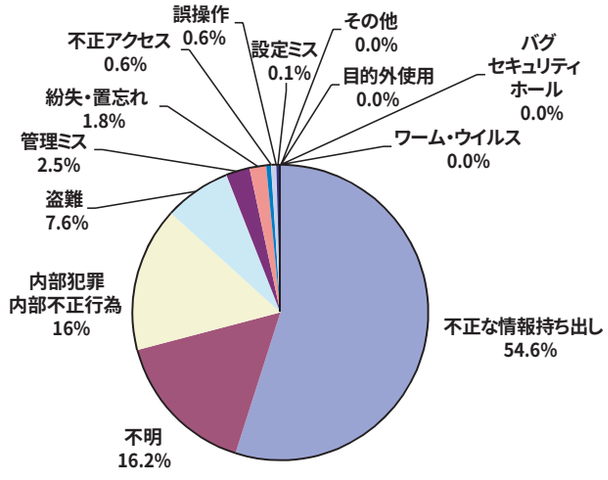

図５　原因別の情報漏洩件数（人数）

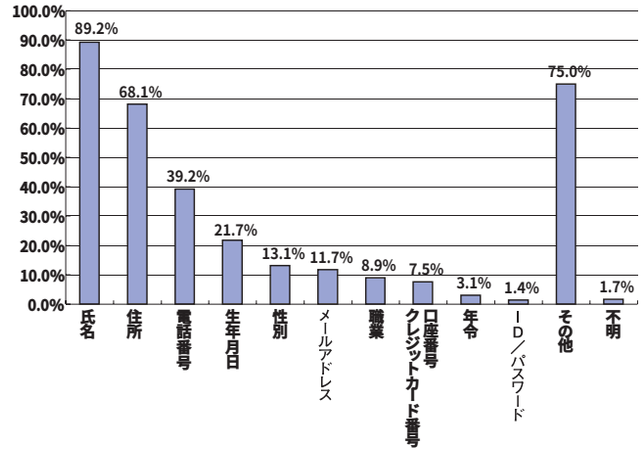

図６　漏洩情報の内訳

インターネットの利用により、地域性もなくなってきている。物理的な漏洩であれば、その場所に行かなくてはならないが、ネットワーク経由のデータ転送であれば、地球のどこにいるかよりも、どの程度高速なネットワークで接続されているかの方が重要になってくる。とはいえ、言われるほど地域性がなくなっているわけではないようである。これについては後述する。

情報漏洩は、今に始まったことではない。多分、ここだけの話、と言うのは人間の歴史とともにあったに違いないし、書類を盗み出すのはスパイの大切な役目でもあった。重要なものであればあるほど、手に入れるための費用や労力を惜しまないものである。内容についての興味のある無しだけではなく、お金になるかどうかも大きな要素になっている。情報の価値は、持主が決めるのではなく、欲しい人が決めるのだ、とよく言われる。繰り返すが情報は売れるのである。

個人情報とプライベート情報は違いがあると言われる。いずれも持主である個人が所有するものであり、特にプライベート情報は、個人の許可があって初めて他人に知らされるべきものである。ただ、医療情報などでは、癌など本人にも知らされていないものもある。氏名、住所、生年月日、性別、電話番号のような基本的な情報であろうとも、教えたくないことはある。このような個人情報を教えてもらったとしても、他の用途に自由に使っても良いわけではない、ということを言っているのが個人情報保護法である。ただ、何をすると罰せられるのかは、監督省庁や主務大臣が最初に判断することになっているので、色々な判断や選択肢がある場合、どうしても一番安全側の対処で準備をせざるを得なくなり、ともするときつい制限側の対策を取らなければ安心できないという問題点も指摘されている。

情報漏洩の原因と経路

少し具体的な数字を見てみよう。日本ネットワークセキュリティ協会（JNSA）の調査[1]によると、報道されている情報漏洩事故の約70％は技術的なネットワーク経由ではなく、物理的なパソコンの盗難や紛失によるものだそうである（図１、２参照）。技術的な原因は約25％程度だが、バグ・セキュリティホール、ウイルス、不正アクセスなどの対策不足が原因となったのは、4.4％程度しかない。ともするとネットワークを通した技術的な面が注目されやすいが、実際には伝統的な人間の活動に基づいた事故による場合が多いのである。

また、どのような媒体で漏洩したかをみると（図３、４参照）、約46％が紙媒体である。ITを使っていようと無かろうと、件数でみるとやはり誰でも読める紙媒体なのである。さらにUSBメモリやCD-ROM、DVDなど

の物理的な媒体、PC本体から漏洩した件数は、約75%以上になっている。一方、インターネットを経由して漏洩した件数は約15%弱でしかない。思ったより少ないと感じる方が多いのではないだろうか。

ところで、情報漏洩の原因を図１では事件件数で見たが、漏洩人数という観点で見たのが図５である。不正な情報持ち出しによるものが何と54.6%にも上っている。内部犯罪、内部不正行為も16%に上る。よく、情報漏洩の７～８割は内部犯行だと言われるが、不正な持ち出しも内部の人間である場合が多いので、まとめ方によっては確かに70%程度という数字がでても不思議ではない。

図１の事件件数の不正な情報持ち出しは2.7%でしかないが、図５の漏洩人数では54.6%に上っている。不正な情報持ち出しと内部犯罪・内部不正行為の合計で見ると、漏洩件数の10.6%に対して漏洩人数は70.6%になる。これは、不正な情報持ち出しや内部犯罪・内部不正は、発覚している事件件数では１割程度だが、漏洩人数で見ると、実に全体の７割を占めていることになる。このように不正操作や内部犯罪は、一度起こるとその影響が大きいことが窺える。事情を知っている人間が関係すると、根こそぎ持っていかれ、規模が大きくなり易いことは、たぶん経験則でもあるだろう。IT関係でも今までと同じ傾向はそんなに変わらないのである。

さて、情報漏洩した個人情報の内容を見てみよう（図６参照）。多いのは、氏名、住所、電話番号、生年月日、性別、という基本的な情報がほとんどである。報告書[1]にはこれらの組み合わせについての状況も書かれているので、参照していただきたい。これらの情報を人に見せたいかどうかは、ケースバイケースであろう。Aさんには見せたけど、Xさんには教えたくない、というのは普通にあるケースだと思われる。このような情報の流通のコントロールが大切なことである。多分、一般的な傾向で考えるのではなく、医療情報や犯罪履歴など、プライベート情報を扱う場合については、一般とは異なる特別な配慮と技術的な手立てを考えなければならないだろう。これはリスク管理にも通ずる考え方であり、どんなものにも同じ扱いをすればよいのではない、ということでもある。

情報資産価値のリスク評価

情報漏洩対策に取り組むことが社会から信用される重要な証にもなっているが、産業界におけるセキュリティ対策の温度差は、依然として大きいようである。例えば、2004年に警察庁が行った全国の企業、医療・教育・行政機関等へのアンケート調査[4]によると、情報セキュリティポリシーを策定済みの団体は、金融機関が74.6%、エネルギー関連企業が93.3%に対して、教育機関は21.0%、医療機関においては8.0%しか策定されていない。これが、扱う情報資産のリスク評価の結果であれば問題は無いのであるが、そうでもないのが見て取れることが悩ましい。

本誌の2005年７月号の企画特集「より強固に確実に！これからの情報セキュリティ対策」の総論に、個人情報資産のリスク評価額算出モデルを紹介させていただいた。算出方法の詳細は本誌やJNSAの報告書[1]を見ていただきたいが、年間の想定損害賠償額の総計を見ると下記のようになる。

◆2002年度　189億2,201万円
◆2003年度　280億6,936万円
◆2004年度　4,666億9,250万円

これは実際に支払われた金額ではなく、もし全ての事例で想定損害賠償額の全額が支払われたら、という仮定の金額であるが、2004年度は前年に比べ16倍以上に増えている。これは、個人情報保護法の実施などで、世間の関心が高まり、報道された事件が増えたこととも無関係ではないだろう。

組織名	国名	漏洩人数	漏洩情報	漏洩原因	漏洩経路
AOL（America Online）	米国	93,000,000	スクリーンネーム、メールアドレス、電話番号、郵便番号、クレジットカード名	内部犯罪・内部不正行為	不明
金融機関や電話会社の社員などのグループ	台湾	15,000,000	氏名、住所、電話番号、収入など	内部犯罪・内部不正行為	不明
カリフォルニア州立大学バークレイ校（University of California, Berkley）	米国	1,400,000	氏名、住所、電話番号、社会保障番号、生年月日、プロバイダ名	不正アクセス	Web・Net経路
バンク・オブ・アメリカ（Bank of America）	米国	1,200,000	クレジットカード番号や口座データ、氏名、住所、社会保障番号	紛失	FD等可搬記録媒体

図７　海外における情報漏洩事件の一部

諸外国と日本

「どこまでやればよいのか？」という疑問は依然として大きいだろう。すぐには結論が出ないようだが、世の中の方向性を見るうえで、日本以外での状況を見ておくことは意味があるだろう。

海外で報道された個人情報漏洩の事例から、件数の大きいものを図７に上げてみた。過去最大規模と見られる米国AOLの例と、台湾の個人情報を不正に集めて詐欺グループに売り渡していたグループは、いずれも何らかの形で内部犯行を伴っている。しかも、目的は金銭目的である。腕試しや愉快犯、怨恨の比率は少なくなり、仕事として情報漏洩に加担し、ブラックマーケットを作っているといえるだろう。

個人情報保護法の公式な英訳が無いそうであるが、米国では2003年に、ある法律事務所が試訳を行い、その一部がビジネスにおける対策用として、2005年１月に公開されている[6]。また、PRIVACY & AMERICAN BUSINESS誌[7]の2003年11月号は、日本の個人情報保護法関係の特集が組まれているが、目次ページにある挿絵が意味深長である（図８）。このように見られているのだろうか。国際標準に倣えば全て由とは思わないが、結局、日本からの議論が出ていないことの証しかもしれない。もっと日本固有の事情を含めて、世界に向けた情報発信と情報交換を行なわなければならないのだろう。

図８　日本の個人情報保護法を欧米から見たイメージと思われる挿絵[7]

前回も『技術だけでは解決しない。しかし、技術の裏付けがなければ対策は取れない。』と書いた。セキュリティも、自動車、飛行機、原子力発電所などと同様に、事故前提で考えなければならない。全てに対して絶対完全は求められないのである。何を守り、何から守り、どのように守るか、をもっと身近に議論していきたいものだと思う。

【参考資料】

[1]「2004年度 個人情報漏洩インシデント調査報告書」.JNSAセキュリティ被害調査WG

情報漏えいによる被害想定と考察（賠償額および株価影響額）

図1~6 は本資料から引用されている。

http://www.jnsa.org/active/2004/active2004_1a.html

[2]「情報セキュリティプロフェッショナル総合教科書」JNSA教育部会スキルマップ作成WG. 秀和システム. ¥3,990. 2005/04/29.

情報セキュリティに関するスキルを16分類し、各々に関して専門家としての初学者を対象とした教科書。

http://www.shuwasystem.co.jp/cgi-bin/detail.cgi?isbn=4-7980-0880-X

[3]「個人情報保護法対策セキュリティ実践マニュアル 2005年度版」. JNSA個人情報保護法ガイドライン作成WG. インプレス. ¥3,675. 2005/03/08.

http://www.jnsa.org/active7_050307.html

[4]「不正アクセス行為対策等の実態調査」. 警察庁. 2005/03/31

http://www.npa.go.jp/cyber/research/h16/countermeasures.pdf

[5]「アクセス制御機能に関する技術の研究開発の状況等に関する調査」. 警察庁. 2005/03/31

http://www.npa.go.jp/cyber/research/h16/research.pdf

[6] Japan 's Personal Information Protection Act.

2003 Law No. 57. 2003 Law No. 57.

Translation of Provisions Relevant to Business.

Center for Social and Legal Researchによる個人情報保護法の試訳
http://www.privacyexchange.org/japan/JapanPIPA2003v3_1.pdf

[7] PRIVACY & AMERICAN BUSINESS誌Vol 10. Num 8 (Nov. 2003)

Special Issue on Consumer Privacy in Japan and the New National Privacy Lawの挿絵

http://www.privacyexchange.org/pab_japanissue.pdf