2012.12.3

情報セキュリティニュース ＜2012 No.3＞

個人情報漏洩事故の最新動向と対策 ～ JNSA の最新の調査結果を中心に ～

1. はじめに

2012 年 9 月 20 日、日本ネットワークセキュリティ協会(以下「JNSA」)から「2011 年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編」が公表された。

本調査は、2011 年に発生、公表された個人情報漏えい事故を集計したもので、今回で 10 回目となる。

本稿では、この調査報告書を元に、近年の個人情報漏洩事故の傾向、特徴を解説すると共に、企業が取り得る対策について考察する。

なお、特に記載が無い場合、文中の表、グラフ等の出典は「2011 年 情報セキュリティインシデントに関する調査報告書 ～個人情報漏えい編（JNSA)」である。

2. 2011 年の個人情報漏洩事故の特徴

2.1. 概要

2011 年の個人情報漏えいインシデントの概要は、表 1 の通りである。

表 1　2011 年 個人情報漏えいインシデント 概要データ

	2011 年	(参考)2010 年
漏洩人数	6,284,363 人	5,579,316 人
インシデント件数	1,551 件	1,679 件
一件あたりの漏洩人数[1]	4,238 人	3,468 人

前年 2010 年の調査結果と比較すると、件数は 128 件減、人数は 705,047 人増となった。すなわち、件数は減っているが漏えい人数は増加していることが分かる。これは 100 万人以上の大規模な情報漏えいインシデントが前年(1 件)比で 2 件増加したことが影響している。単純平均での一件あたりの漏えい人数は表 1 に示した通りであるが、実際の各インシデントでの漏えい人数は、100 万人漏れた事故もあれば、5 人だった事故もある。

個人情報漏えいの対応策の検討にあたっては、こうした各インシデントの特徴をとらえて検討する必要がある。よって次章より、情報漏えいの媒体、漏えい経路、漏えい原因などの視点から、2011 年の傾向とその対策を考えていく。

[1] 被害者数が不明のインシデント 68 件を除いて算出

2.2. 情報漏えい媒体・経路

まず、どのような媒体で個人情報が漏えいしているかを表 2 に示す。

表 2　2011 年 個人情報漏えいインシデント媒体別漏えい状況

媒体	漏えい件数	漏えい人数	1 件あたりの漏えい人数
紙媒体	1065 件	503,883 人	486.4 人
USB 等可搬媒体	156 件	3,712,720 人	25,085.9 人
電子メール	126 件	74,006 人	649.2 人
インターネット	68 件	1,605,040 人	25,078.8 人
PC 本体	68 件	72,481 人	1,249.7 人

分析の結果、漏えい事故の件数としては紙媒体が依然としてトップである。業務上、紙媒体を利用する頻度が高く、また紛失しやすい媒体であることが窺える。
一方で、漏えいした人数では、「USB 等可搬媒体」が群を抜いて多い。電子可搬媒体には、大量の情報を格納して利用するため、事故が起こった際の被害が大きくなりやすい。

このデータから企業が考えるべきことは、組織が対策を考える際に「起こりやすさ」と「1 件あたりの被害の大きさ」のどちらを重要視するかである。いずれを重要視するかによって対策が異なってくる。

「起こりやすさ」に着目し、紙媒体による漏えいを防ぐためには、まず紙媒体への出力自体を減らすことが第一である。内容の確認などはパソコンなどの画面上で行い、不必要な紙出力を減らすことで、情報の紛失リスクを大きく低減させることが可能である。また、クリアデスク活動など、整理整頓を心がけることも、紛失リスクの低減に役立つ。

他方、「1 件あたりの被害の大きさ」を重視して対応策を検討する場合には、電子可搬媒体への 1 回あたりの格納情報量を削減する、利用が終了した媒体のデータ消去をつど確実に行う、などが重要である。

2.3. 漏えい原因と漏洩人数の関係

次に、漏えい原因と漏えい人数の関係を表 3 に示す。

表 3　2011 年 個人情報漏えいインシデント原因別漏えい状況

媒体	漏えい件数	漏えい人数	1 件あたりの漏えい人数
誤操作	539 件	142,151 人	263.7 人
管理ミス	497 件	2,371,284 人	4,771.1 人
紛失・置き忘れ	213 件	46,152 人	216.6 人
盗難	103 件	101,272 人	983.2 人
不正な情報持ち出し	77 件	1,690,282 人	21,951.7 人
不正アクセス	18 件	1,315,571 人	73,087.2 人

漏えいの要因別では、「誤操作」が件数トップとなり、次いで「管理ミス」が 2 番目に多い状況である。漏えい人数では、「管理ミス」によるものが最も多く、1 件あたりの漏えい人数でも、意図的な漏えいである「不正な情報の持ち出し」や「不正アクセス」を除くと、最も漏えい数が多い結果となった。前記した「起こりやすさ」「1 件あ

たりの被害の大きさ」どちらの対策に重きを置くとしても、「管理ミス」への対処が重要なポイントであるといえる。

「管理ミス」によるインシデントは、組織にマニュアルが整備されていない、あるいは整備されているマニュアルが遵守されていないために発生する。

JNSA の調査報告書では、ルールがない状況で発生したインシデントよりも、ルールが整備されている状況で発生したインシデントの方が早期に発見される傾向があり、まずは個人情報を守るためのルール作りが必要としている。企業としてどのように個人情報を管理・活用していくのか、と言う軸をしっかり定めることが対策の第一歩となる。

1 件あたりの被害を小さくするための対策としては、「物理的に分散して管理する」「管理者の権限を分割し、作業に必要な権限に限る」などが挙げられる。

3. 企業が取る対策のポイント

3.1. 情報漏えい対策は人的ミスの低減が課題

JNSA の報告書では、単年分析と共に経年分析も合わせて行っている。(図 1, 2)

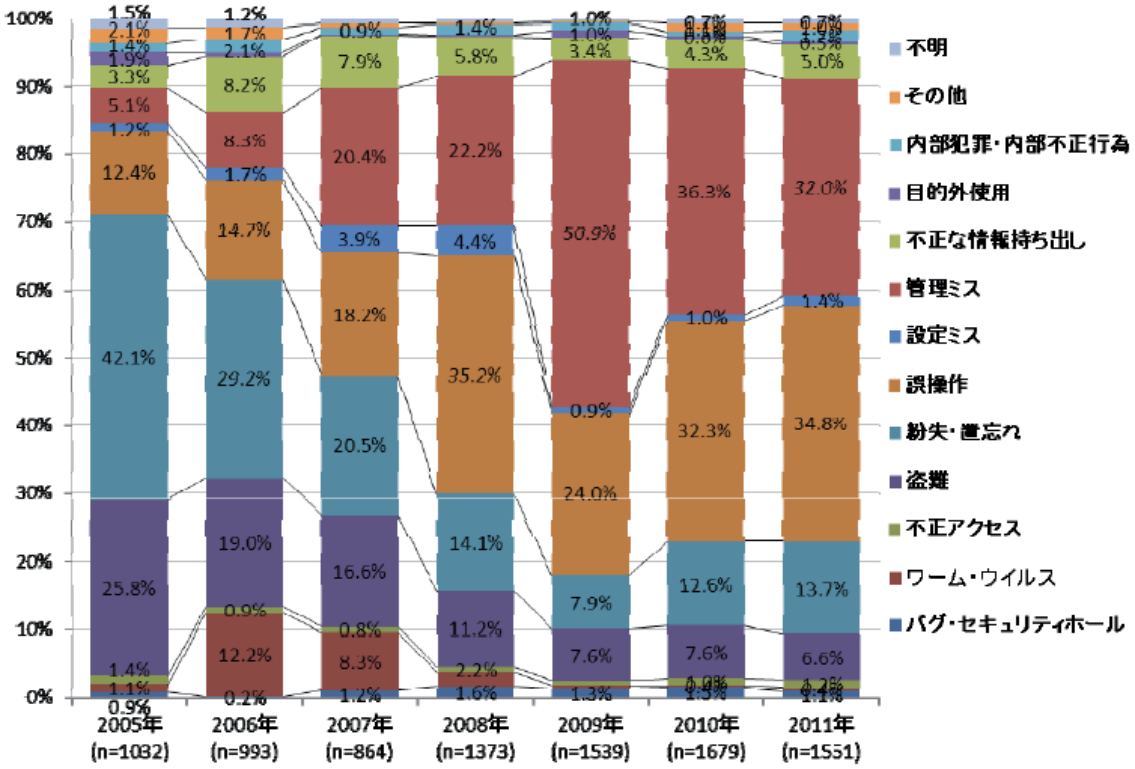

図 1 漏えい原因比率の経年変化(件数)

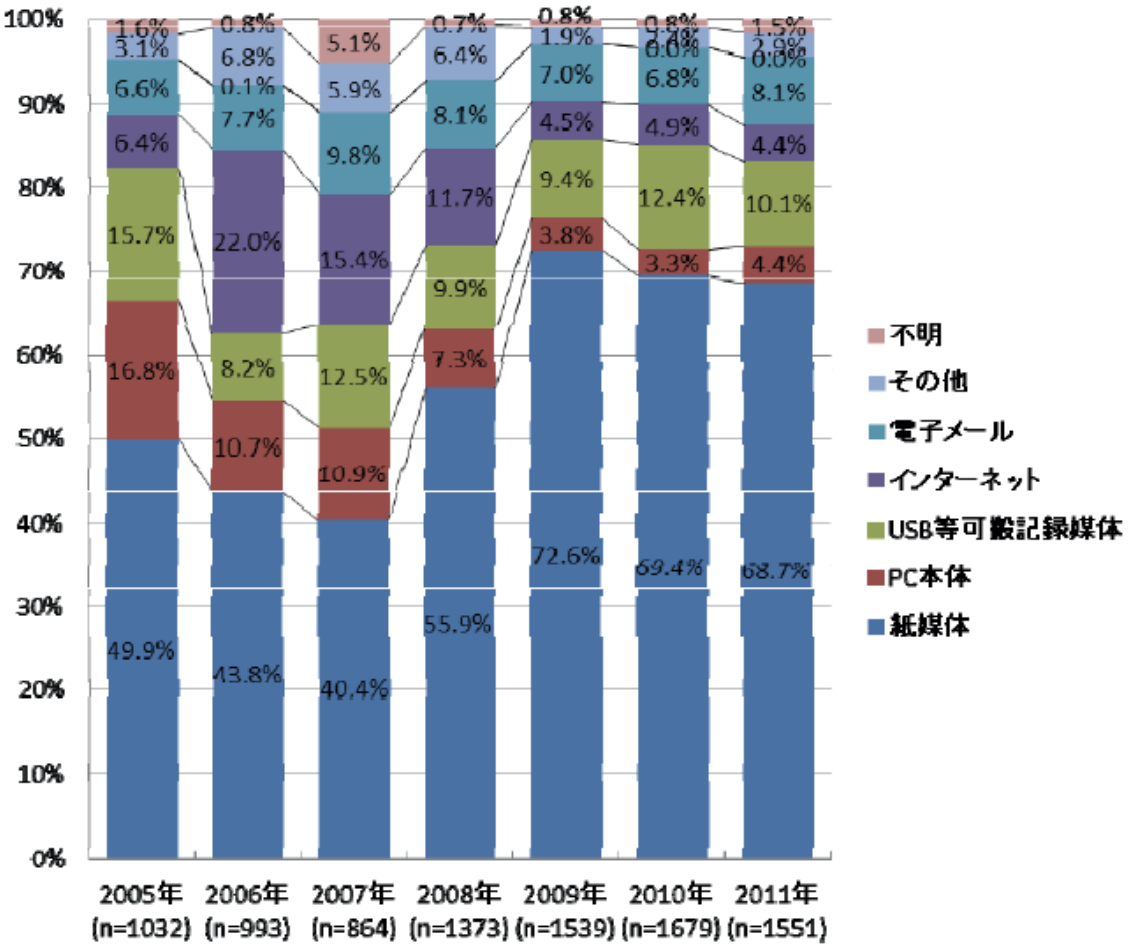

図 2 漏えい経路比率の経年変化(件数)

2008 ～ 2009 年頃から、漏えい原因の上位が「バグ・セキュリティホール」から「管理ミス」、「誤操作」へと移り、漏えい経路でも紙媒体の比率が上昇している。これはシステム化などの対策が進み、静的に保管されている情報の漏えいが減少してきたことで、結果的に人的リスクが浮かび上がったと言うことが出来る。2010 年代はシステムから人間に情報が渡った後の情報管理こそが重要になってきたと言えるだろう。

対策のポイントとしては、まず業務プロセスを明らかにすることである。その上で、プロセス毎にどのような情報を扱うか、またその情報がどのように移動するか、情報を扱う主体は人かシステムか、など、リスクポイントを確認していき、各ポイントに最適な対策を打っていく必要がある。

3.2. 事故は起こるものだという認識を

2011 年に個人情報インシデントが発生していない業種は第一次産業にあたる「農業、林業」「漁業」「鉱業、採石業、砂利採取業」の 3 業種だけであり、それ以外の全ての業種ではインシデントが発生している。二次産業、三次産業に携わる企業では、個人情報を持つ限り、情報漏えいのリスクをゼロにすることはできないと覚悟する必要がある。

もちろん事故を未然に防ぐ努力を怠ってはならないが、事故発生後に迅速に復旧することで、被害を最小限に食い止めることができ、また場合によっては事故対応の早

い企業という評価を受けることも可能となる。情報漏えい事故が起こったあとの対応は、非常事態への対処と同様であり、災害対応同様、行動指針を事前に定めマニュアルを作成しておくこと、加えて定期的に訓練・演習を行い、認識を高めておくことが肝要といえる。

3.3. 対策の自動化には限界があり、人的統制が必要になること

前述したとおり、情報漏えいの原因としては「誤操作」、「置き忘れ」などヒューマンエラーに起因するものが多く、外部からのアタックなどは一回のダメージは大きいものの、頻度は低い。これは言いかえれば「人間の手を介したときに情報漏えいが起こりやすい」ということである。情報管理、アクセス管理のシステム化、扉のオートロックなど、自動化で出来るものも多いが、業務を遂行する以上、どこかのプロセスで人間が情報を扱うことになる。つまりどこかで人間を統制(人的統制)する必要がある。

人的統制を行う上での大きなポイントは、手順を複雑化しないこと、業務上の動線を乱さないことである。手順が複雑だったり、普段行かないようなところに行かせたり、余りにやり慣れない手順をやらせるような手順を作ってしまえば、当然望んだような管理はされなくなり、形骸化へ向かってしまう。普段の業務プロセスから大きく乖離しないようなルールを定めることが肝要である。

4. おわりに

本稿では、2011 年までの状況を踏まえて、現状行っていくべき個人情報漏えい対策について述べた。

個人情報保護の意識が高まったこの数年間に情報管理のシステム化は大きく進み、大規模な情報漏えい事故や、社内システム内部から大量に情報が流出する事故は減少傾向にある。その一方、人による事故は減少しておらず、報告数ではむしろ増加している状況である。

近年スマートフォンが急速に普及するなどモバイル端末の性能が飛躍的に向上し、また様々なワークスタイルが広がりつつある現在、個人が扱う情報は今後、質・量ともに向上していくことは間違いない。先述したように、企業の業務における情報の動きや位置付けを確実に把握し、各リスクポイントに最適な対策を一層きめ細かく打っていく必要があるだろう。

以上

インターリスク総研 コンサルティング第二部　BCM 第一グループ
主任コンサルタント 頼永　忍