2009年情報セキュリティインシデントに関する調査結果の追加分析

セキュリティ被害調査WG
(株)NTTデータ　大谷　尚通
リコー・ヒューマン・クリエイツ(株)　広口　正之
(株)ディアイティ　山田　英史

はじめに

今年も、セキュリティ被害調査WGによる個人情報漏えい事件・事故(以降「インシデント」という)の調査分析結果をまとめた報告書を7月に公開した。すでに多くの方が、報告書から個人情報漏えいを多く公開している業種や、漏えいの原因などをご覧いただいていると思う。本稿では、「調査データから見える特徴」で2009年の傾向を振り返ったあと、WGメンバが独自に解析した2つの成果「インシデントの事例分析」と「中小企業における個人情報漏えいの傾向」をご紹介する。

1. 調査データから見える特徴

1-1. 概要

2009年の集計結果の概要データを表 1-1に示す。2009年は、2008年から引き続いて、漏えい件数が1539件(＋166件)に増加し、漏えい人数が約572万人(－152万人)に減少した。漏えい人数が減少しているにもかかわらず、想定損害賠償総額は、3,890億4,289万円(＋1,523億1,760万円)と増加した。これは、「口座番号」「クレジットカード番号」等の情報を所有する「金融業，保険業」の漏えいインシデントが増加していることが起因する。2009年は、「金融業，保険業」の漏えいインシデントの発生元として地方銀行や都市銀行の地方支店からの公表が増加している。2009年に金融庁が中小・地方銀の情報セキュリティ管理の強化を方針として打ち出し、それを受けて地方銀行および都市銀行の地方支店でセキュリティ監査を強化したために、誤廃棄などの管理ミスが多く発見されたことが背景にあると推測される。

表 1-1:2009年個人情報漏えいインシデントの概要

漏えい人数	572万1,498人
漏えい件数	1,539件
想定損害賠償総額	3,890億4,289万円
一件当たりの漏えい人数	3,924人
一件当たり平均想定損害賠償額	2億6,683万円
一人当たり平均想定損害賠償額	4万9,961円

1-2. 漏えい媒体の経年変化

情報漏えいインシデントが最も多い媒体は、図 1-1に示すように紙媒体である。これは、インシデントを多く公表している「金融業・保険業」「公務」において、紙媒体を使用する頻度が高いことも影響している。紙媒体の占める割合は、紙媒体の持ち出し禁止などの一般的な対策によってしばらくは減少したが、2007年以降、増加に転じている(矢印①)。これは、紙媒体からの漏えいに対して決定的な対策が無いことと、紙媒体以外のUSB等可搬記録媒体、電子メール、インターネット等のシステム的な対策が進み、これらの占める割合が減少した(矢印②)ことで、紙媒体の割合が相対的に増加したと考えられる。

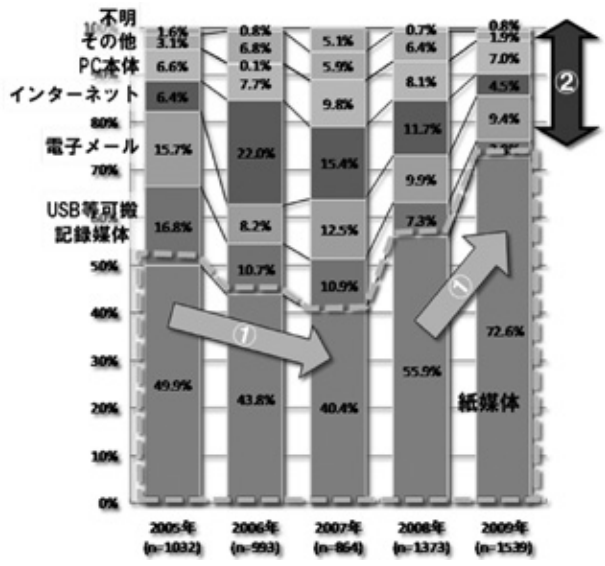

図 1-1: 媒体・経路別の漏えい件数(経年)

1-3. 漏えい原因の経年変化

図 1-2からは、漏えい原因の特徴的な経年変化を見ることができる。紛失・置き忘れと盗難による漏えいは、毎年着実に減少している(矢印①)。これは、不必要な情報の持ち出しが減少したこと、情報を持ち出した時は行動に注意する姿勢が浸透したことによる効果が表れていると推察する。反対に、管理ミスと誤操作の比率は、増加の一途をたどっている(矢印②)。これは、監査や組織内統制の強化に伴い、管理ミスによる誤廃棄や紛失が判明したこと、前記の原因の対策が進んだ事によって、対策が難しい誤操作による漏えいが顕在化したことが、影響していると考えられる。

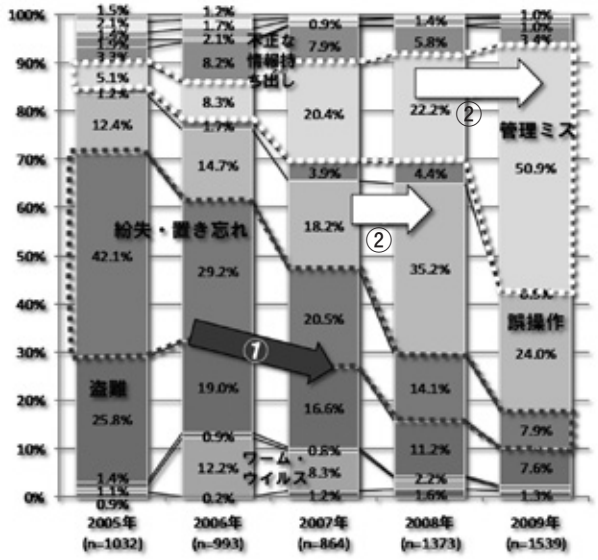

図 1-2: 原因別の漏えい件数(経年)

1-4. まとめ

漏えい原因のうち、高い割合を占める「管理ミス」と「誤操作」への対策が重要である。「管理ミス」の対策は、組織として、法令や契約、慣習に照らして情報の保管期限と廃棄方法を決めること、保管が義務付けられた情報を廃棄する場合は、廃棄内容、廃棄日、廃棄方法、実施者等を記録する手続きを決めることなど、情報の管理に関するルールを明確に定めて、実践することが求められる。「誤操作」対策は、各個人による手続き的な対策と、組織的・システム的な対策がある。例えば、電子メールの誤送信の対策は、各人が送信前に再度、宛先を見直す手続きを習慣づける方法と、送信ボタンを押した後でも誤送信を取り消せるシステムを導入する方法がある。

今後は、対策の難しい誤操作のようなケアレスミスと、悪意のある有権限者による内部犯行・内部不正行為への対応が、漏えい対策のポイントになると思われる。

2. インシデントの事例分析

「2009年 情報セキュリティインシデントに関する調査報告書」では、漏えい原因を、管理ミス、誤操作、紛失・管理ミス、盗難、不正な情報持ち出しなどに分類して報告している。しかし、実際のインシデントを教訓として、具体的な対策の要否を検討しようとする場合などにおいては、インシデント事例をもう少し詳細に分析する必要がある。

2-1. ウイルス感染

ウイルス感染によって、個人情報や機密情報が漏えいするのは、ファイル共有ソフトウェアを使用していて、暴露系のウイルスに感染した場合である。2009年のインシデント1,539件中、ファイル共有ソフトに関連した漏えいインシデントは27件あり、そのうち、ウィニーが16件、シェアが7件である。残り4件では、ファイル共有ソフトウェアの名称を公表していない。

ファイル共有ソフトウェアを使用していた場所は、ほとんどが自宅である。会社で使用していたのは、1件のみである。使用していた人は、社員、元社員、配偶者、子供などである。自宅に個人情報や機密情報を持ち帰っていた理由は、バックアップのため、業務実施のためなどである。

自宅に待ち帰ることを禁止するだけでなく、自宅に持ち帰った場合に、どのような経緯で漏えいするかも含めて従業者に教育する必要があると思われる。

2-2. 誤交付

誤交付とは、書類を誤って手渡してしまった事例である。次のような場合がある。

(1) 本人の書類を、別人に手渡した。
(2) 本人に、別人の書類を手渡した。
(3) 本人と別人の書類を取り違えて、手渡した。
(4) 本人の書類の他に、別人の書類がまざっていた。

本人であるかどうかの確認と、書類が間違っていないかの確認が必要である。まれではあるが、同姓や同姓同名の場合もあるので細心の注意が必要である。

2-3. 誤送付

誤送付とは、書類を誤って送付してしまった事例である。次のような場合がある。

(1) 本人の書類を、別人に送付した。
(2) 本人と別人の書類を取り違えて、送付した。
(3) 本人の書類の他に、別人の書類がまざっていた。

誤交付と比較すると、「本人に別人の書類を送付した」事例が存在しないが、これは、本人の情報が何もない場合には、本人に送付されようがないためと考えられる。

窓付き封筒は、宛先と内容物の相違を無くす手段として有効であるが、(3)のような事例には有効でない。封筒の数と、内容物の数をあらかじめ数えておく方法は、過不足なく封筒に入れたことを確認する手段として有効であるが、その方法だけでは(2)のような事例には有効でない。

2-4. メールの誤送信

メールの誤送信には、次のような場合がある。

(1) 一斉送信時にBCCでなく、TOで送信した。
(2) 一斉送信時にBCCでなく、CCで送信した。
(3) 誤ったファイルを添付した。

BCCを間違えてTO、CCにした事例では、TOが27件、CCが11件であり、TOに入れる事例のほうが多い。添付ファイルを間違えた事例は、3件あった。この中にも、一斉送信用のファイルを間違って添付した事例があり、多くの人に一斉送信する場合には、細心の注意が必要である。

2-5. FAXの誤送信

FAXの誤送信には、次のような場合がある。

(1) FAX番号を押し間違えた。
(2) FAX番号を押すときに参照していた情報が間違っていた。
(3) 古いFAX番号をそのまま使用していた。
(4) FAX番号を登録するときに間違えた。
(5) 「0」発信すべきであったが、0を入力しなかった。

(1)のFAX番号を押し間違えた事例がほとんどであるが、その他にもさまざまな間違え方が見られる。こうした間違え方について知ることが、間違いを減らすための第一歩であると考える。

2-6. USBメモリの紛失

USBメモリの紛失の事例については、次のような場合がある。

(1) カバンに入れていて、カバンごと紛失した。
(2) ポケットに入れていたが、いつの間にか無くなった。
(3) カバンに入れていたが、いつの間にか無くなった。
(4) 勤務先で、いつの間にか無くなった。

(1)のカバンごと紛失した事例が最も多いが、小さいために、いつの間にか紛失する事例が多いのが、USBメモリ紛失の特徴である。

2-7. 車上荒らし

車上荒らしの事例には、次のような場合がある。

(1) 窓ガラスを割られた。
(2) ドアの鍵を壊された。
(3) 車両ごと盗難にあった。

(1)の窓ガラスを割られる事例が11件と最も多いが、ドアの鍵を壊された事例が2件、車両自体が盗難にあった事例も2件ある。カバン等を外から見えないところにおくだけでは防ぎきれないという認識が必要である。自宅駐車場での被害もあるので、自宅といえども油断は禁物である。

2-8. 情報の誤公開

情報の誤公開は、意図せずに個人情報などを公開してしまった事例である。次のような場合がある。

(1) ウェブサーバでファイルが閲覧可能な状態に

なっていた。
(2) ウェブコンテンツに誤って掲載した。
(3) アプリケーションの誤りで公開された。

2008年には、グーグルマップの機能で誤って公開された事例が24件あったが、2009年には改善され、同様の事例は見られなかった。

以上のように、インシデントのパターンを細分化することによって、自分の会社、組織における危険な状態が浮き彫りになり、具体的な対策が見えてくるのではないだろうか。実際に発生したインシデントを単にニュースとして聞き流してしまうのではなく、他山の石として教訓にすることが重要である。

3. 中小企業における個人情報漏えいの傾向

過去の情報漏えいインシデントを見ると、報道機関への公表元は大企業や自治体であっても実際には委託先から漏えいしたという事例が散見される。委託先の多くは中小企業であり、多くの業種においてサプライチェーンの中に何らかの形で中小企業が含まれると考えられる。中小企業における情報漏えいの傾向のようなものが見つかれば、今後のサプライチェーン全体の統制の一助になるのではないかと考え「2009年 情報セキュリティインシデントに関する調査報告書」の中から、漏えい元が中小企業の事例を抽出し集計した。

3-1. 中小企業の抽出方法

中小企業基本法第２条の定義にしたがい、2009年の集計結果から漏えい元が中小企業に該当するインシデントを抽出した。報道等において公表元が大企業等の場合であっても直接の漏えい元が中小企業と判明した場合は分析対象に含めた。

【除外した業種】
公務、銀行・信金、公共の電気・ガス・水道、独立行政法人、建設業、社団法人、学校法人、公立小中高、医療・福祉

3-2. 集計結果

(1). インシデント件数と漏えい人数規模

全業種1,539件の内中小企業に該当する組織は56件で、総漏えい人数は54万7,331人となった。全業種の中に占める割合は、件数で3.6％、人数で9.5%となった。

表 3-1:【中小企業】インシデント件数と漏えい人数規模

	全業種	中小企業
インシデント件数	1,539件	56件
漏えい人数	573万1,498人	54万7,331人
一件当たりの漏えい人数	3,924人	11,170人(※1)
想定損害賠償総額	3,894億1,144万円	144億8,471万円
一人当たりの平均想定損害賠償額	4万9,961円	1万6527円

※中小企業の「一件当たりの漏えい人数」は被害者数不明を除き、母数を49件とした。

(2). 業種分布

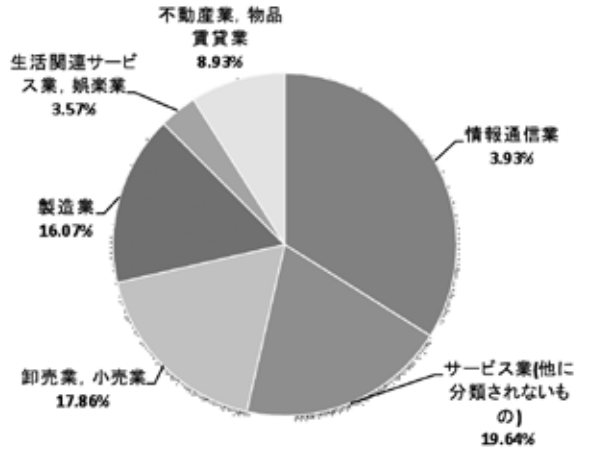

図 3-1:【中小企業】個人情報漏えいの業種別割合(件数)

図 3-1の中小企業における漏えいインシデント件数の業種別割合は、全業種から「金融・保険業」「公務」「教育・学習支援」を除いたため、当然の結果「情報通信」「卸売業・小売業」が上位に来た。また、同図から全業種に比較して中小企業は「製造業」の割合が高くなっていることがわかる。

(3). 漏えい原因

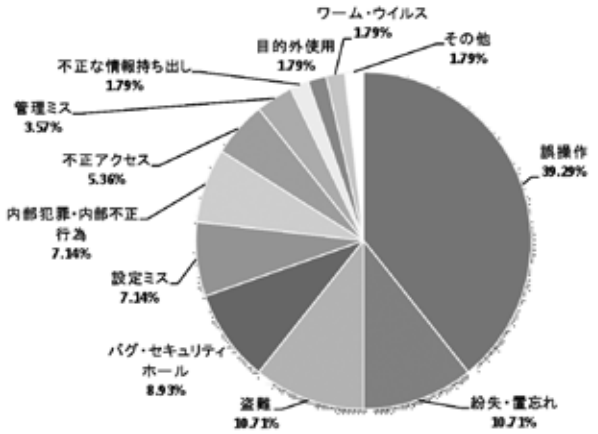

図 3-2:【中小企業】個人情報漏えいの原因別割合(件数)

漏えい原因については全業種と中小企業では差異が見られる。中小企業の集計からは「金融業・保険業」が除外されているため、それに伴って全業種で原因の1位であった「管理ミス」の割合が低くなっている。

中小企業の集計では「誤操作」が1位になっているが、具体的な内容は電子メールに関連するものが多く、宛先アドレスを間違った事例や「Bcc:」に入れるべき宛先を「To:」や「Cc:」に入れてアドレスを露呈したという事例が見られる。なお、全業種でも「誤操作」は2位と上位であるが、全業種では「公務」における郵送物の誤配送が占める割合が多く、中小企業の集計からは「公務」を除外しているため、同じ「誤操作」でも内訳は異なる。

(4). 漏えい媒体・経路

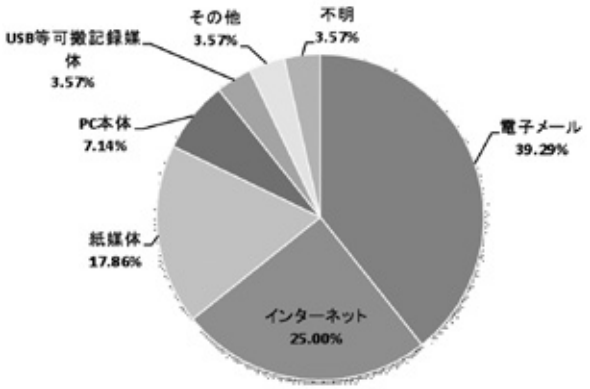

図 3-3:中小企業】個人情報漏えいの経路別割合(件数)

漏えい媒体・経路になると全業種と中小企業では大きく構成が変わる。全業種で「紙媒体」の割合が高かったのに対し、中小企業で「電子メール」の割合が高くなっている。これは、原因の「誤操作」における電子メールの誤送信と連動しているためである。2位の「インターネット」の多くは、会員用ホームページの設定ミスで、他人の登録情報が閲覧できる状態にあったというケースである。

中小企業は、人手とコストをかけずに広く販路を開拓するために電子メールやホームページを積極的に活用することから「電子メール」「インターネット」の割合が高くなっていると解釈することもできる。

この結果だけでは判断できないが、中小企業においてはITのセキュリティリテラシーの向上が大きな課題と考えられる。また、会員用ホームページの作成・運用を外注しているケースも多くあるはずだが、セキュリティを考慮した業者選定も課題の一つである。

3-3. 留意点

当ワーキンググループの集計は、インターネットニュース等に公表された情報に基づくため、積極的に公表する方針を持つ行政関係と、マスコミが取り上げやすい大手企業に母集団が偏る傾向がある。したがって、上記集計においても母数が56件と小さく、そのまま世の中の中小企業の平均像とは言い難いところもあるが、販路として積極的にITを活用する姿など大企業とは異なった特性を持つことが垣間見られ、今後も何らかの形で中小企業におけるインシデントの実態を調査することにも意味があると想像させる。そのためには現在のアプローチとは違った調査方法を考えなくてはならないが、当ワーキンググループの課題の一つとしてとらえ引き続き検討していきたい。