2010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～

第 1.5 版

2011 年 7 月 1 日

2014 年 8 月 12 日 改訂

NPO 日本ネットワークセキュリティ協会

セキュリティ被害調査ワーキンググループ

目次

JNSA 調査研究部会 セキュリティ被害調査ワーキンググループ
ワーキンググループリーダー
大谷　尚通　株式会社 NTT データ
メンバー
井口　洋輔　NKSJ リスクマネジメント株式会社
猪俣　朗　トレンドマイクロ株式会社
大溝　裕則　株式会社 JMC
岡本　一郎　株式会社 インフォセック
佳山　こうせつ　富士通株式会社
北野　晴人　日本オラクル株式会社
佐藤　康彦　マイクロソフト株式会社
佐藤　耕太郎　日本オラクル株式会社
田中　洋　株式会社 インフォセック
馬鳥　雄也　日本オラクル株式会社
広口　正之　リコー・ヒューマン・クリエイツ株式会社
丸山　司郎　株式会社ラック
山田　英史　株式会社ディアイティ
吉田　裕美　株式会社ラック

1　はじめに

JNSA セキュリティ被害調査ワーキンググループ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）の調査分析は今回で 9 回目となる。

JNSA セキュリティ被害調査ワーキンググループでは、2009 年と同様に、これまでの調査方法を踏襲し、2010 年に新聞やインターネットニュースなどで報道された個人情報漏えいインシデント（以下、インシデントという）の情報を集計し、分析を行った。

この調査データにもとづいた、漏えいした組織の業種、漏えい人数、漏えい原因、漏えい経路などの情報の分類、JO モデル（JNSA Damage Operation Model for Individual Information Leak）を用いた想定損害賠償額などを分析した結果を報告書にまとめた。このような結果をもたらした原因分析も含め、以下に 2010 年のインシデントの集計・分析結果、及び過去 6 年間の蓄積されたデータを元にした経年変化の分析結果を報告する。

2　報告書について

2.1　報告書の目的

本報告書は、2010 年一年間に報道されたインシデントを調査・分析し、独自の観点から評価した結果である。

個人情報は個人情報保護法により保護を義務付けられた情報資産であり、個人情報漏えいは企業の経営者や組織の責任者が認知すべきリスクのひとつである。

当ワーキンググループでは、インシデントにおける「損害賠償の可能性」について、今後の議論の題材になることや、企業経営者が考えるべき情報セキュリティのリスク量の把握や、適切な情報セキュリティに対する投資判断の一助となることを目的として、検討、及び提案を行う。

2.2 報告書の構成

本報告書の本編は、さまざまな個人情報漏えいのインシデントを分析した「第 3 章 2010 年の個人情報漏えいインシデントの分析結果」「第 4 章 2010 年 想定損害賠償額の算定結果」と、個人情報漏えいによる想定損害賠償を算出するモデルを解説した「第 5 章 個人情報漏えいにおける想定損害賠償額の算出モデル」から構成される。

「第 3 章 2010 年の個人情報漏えいインシデントの分析結果」では、2010 年の単年の分析結果、9 年間の蓄積されたデータのうち、直近 6 年間のデータに基づく経年の分析結果の解説を行った。2002 年から 2004 年までのインシデント情報は公表件数が少なく、統計データとしては偏りが大きいため、2010 年の分析では、これらを除外した。

「第 4 章 2010 年 想定損害賠償額の算定結果」では、想定損害賠償額の算定結果とその考察結果を解説した。2002 年から 2010 年までの 9 年間の個人情報漏えいに関する数値は、新聞やインターネット上で報道された公開情報に基づいて、統計したものである。一方、想定損害賠償額は、当ワーキンググループが独自に開発した算定手法に基づいて算出した推定データであることに注意されたい。

また、2009 年の報告書と同様に「インシデント一覧表」を付録とした。

2.3 調査・分析方法

2010 年 1 月 1 日から 12 月 31 日の間に新聞やインターネットニュースなどで報道されたインシデントの記事、組織からリリースされたインシデントに関連した文書などをもとにインシデントの情報を集計した。まず、収集した情報を元に、これまでと同様に漏えいした組織の業種、漏えい人数、漏えい原因、漏えい経路などの分類・評価を行った。次に、独自の算定式（JO モデル）を用いて、想定損害賠償額を算出した。

本調査データは、インターネット上に公開されたインシデントに関する情報を手作業で収集し、記事や文書に書かれた内容から、インシデントの分析に必要な情報を取得している。よって、可能な限り多くの情報を収集するように努力しているが、公表された全てのインシデントの記事を収集できていないことを了承されたい。また、この報告書に対する読者の問い合わせに対応し、結果の一部が誤っていることが判明した場合には、随時これを訂正している。報告書を利用する場合には、ホームページ上に公開されている最新の報告書を利用していただきたい。

3　2010 年の個人情報漏えいインシデントの分析結果

3.1　概要

漏えい件数は、2007 年以降継続して増加しており、1,679 件（前年比＋140 件）と過去最高件数を更新した。これは、主に「公務」において漏えい件数が増加したことが影響しており、従来から積極的に情報漏えい事件を公表している特定の地方自治体に加え、2010 年から、もう 1 か所の特定の地方自治体が積極的に公表を始めたことが影響している。

漏えい人数は、約 558 万人（前年比－14 万人）と、2007 年以降継続して減少している。これは、漏えい件数が増加する一方で、一件あたりの漏えい人数が小さい 100 万人未満の事件が増加していることが影響している。

想定損害賠償総額も、漏えい人数と同様に減少し、過去最低の約 1,215 億円（前年比－2,675 億円）となった。これは総漏えい人数の減少と、1 件当たりの損害賠償額の減少の両面に起因する。

漏えい原因としては、引き続き「管理ミス」（610 件）、「誤操作」（543 件）が大半を占め 2010 年は、誤操作が増加（前年比＋174 件）している。

また、2010 年は特定の情報通信業において不正アクセスにより、大規模（約１７４万人）な事件が 1 件発生しているため、人数ベースの漏えい業種は「情報通信業」、漏えい原因は「不正アクセス」が突出した結果となっている。

2010 年の集計結果の概要データは、以下の通りである。

表 3-1：2010 年 個人情報漏えいインシデント 概要データ

漏えい人数	**557 万 9316 人**
インシデント件数	**1679 件**
想定損害賠償総額	**1215 億 7600 万円**
一件あたりの漏えい人数※1	**3468 人**
一件あたり平均想定損害賠償額※1	**7556 万円**
一人あたり平均想定損害賠償額※2	**4 万 3306 円**

※1：平均値は、被害者数が不明のインシデント 70 件を除いて算出している。
※2：この平均値は一件あたりのばらつきを吸収するため、まず、各インシデントの一人あたりの想定損害賠償額を算出し、そこから全てのインシデントの一人あたりの想定損害賠償額の平均額を算出している。よって、想定損害賠償総額を漏えい人数で割った値ではないことに注意されたい。

3.2　個人情報漏えいインシデント・トップ 10

表 3-2 に規模の大きいインシデント・トップ 10 を示す。2008 年は、漏えい人数が 100 万人を超える大規模なインシデントは 1 件も発生せず、2009 年と 2010 年は漏えい人数が 100 万人を超える大規模なインシデントが 1 件だけ発生した。

インシデント・トップ 10 の原因は、2008 年、2009 年と比較して「管理ミス」が減少し、「不正アクセス」「内部犯罪・内部不正行為」「不正な情報持ち出し」などの故意を含んだ原因が目立っている。

業種は、「金融業，保険業」「公務」が減少し、「情報通信業」が増加した。

表 3-2：インシデント・トップ 10

No.	漏えい人数	業種	原因
1	173 万 5841 人	情報通信業	不正アクセス
2	46 万 3360 人	情報通信業	内部犯罪・内部不正行為
3	31 万人	医療，福祉	不正な情報持ち出し
4	25 万 4122 人	卸売業，小売業	不正アクセス
5	20 万 1414 人	学術研究，専門・技術サービス業	管理ミス
6	19 万 7907 人	情報通信業	盗難
7	19 万 7077 人	製造業	設定ミス
8	19 万 5132 人	サービス業(他に分類されないもの)	不明
9	17 万 755 人	サービス業(他に分類されないもの)	不正アクセス
10	17 万 325 人	金融業，保険業	管理ミス

3.3　業種

(1)　単年分析(件数)

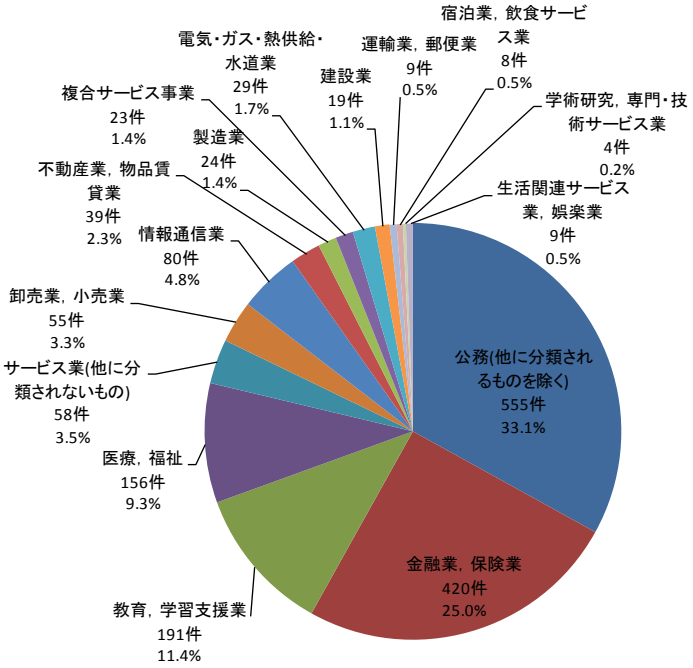

図 3-1：業種別比率（件数）

業種別のインシデント件数を図 3-1 に示す。インシデント件数の多い業種は、上位から順に「公務」(33.1%)、「金融業，保険業」(25.0 %)、「教育，学習支援業」(11.4 %)、「医療，福祉」(9.3%)であり、全体の約 80%を占めている。

「公務」及び「金融業，保険業」については、2004 年以降、常に上位を占める結果となっている。これは、個人情報を取り扱うことの多いことに加え、個人情報保護に関する行政の指導が強く働いている業種であり、小規模なインシデントであっても公表することが多いためと考えられる。また「教育，学習支援業」「医療，福祉」も 2007 年以降、上位をあげてきており、インシデントを積極的に公表する傾向が浸透してきていると考えられる。

インシデントが発生していないのは、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 業種だけである。その他のすべての業種で個人情報を利用しており、インシデント発生のリスクがあるという状況に変化は見られない。

(2)　経年分析(件数)

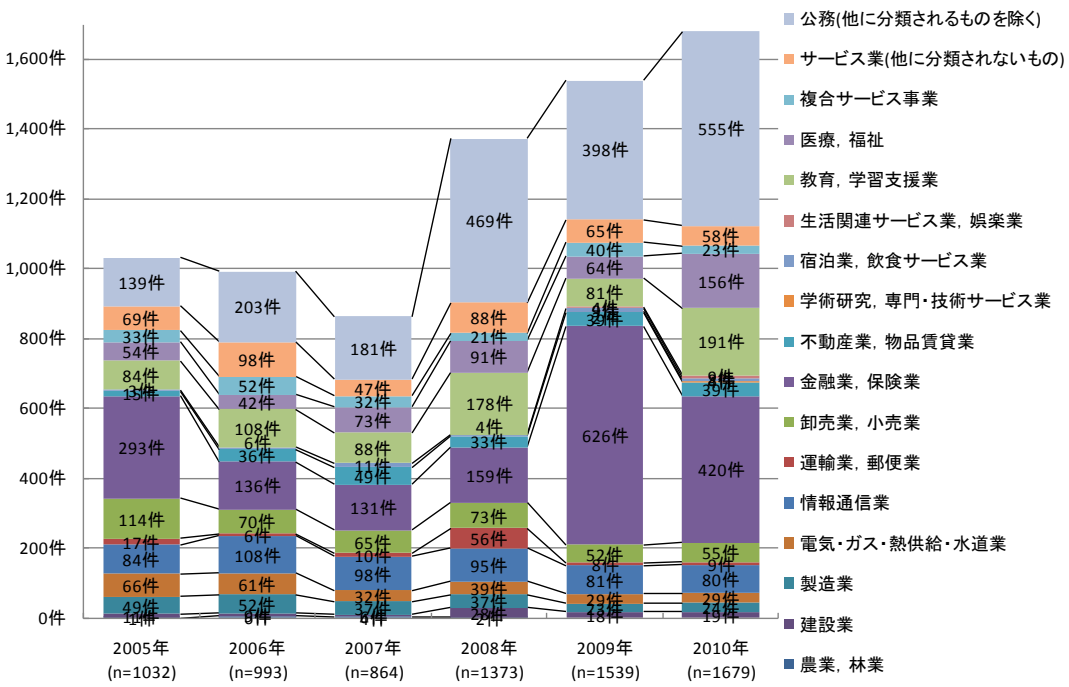

図 3-2：業種別件数の経年変化（件数）

業種別のインシデント件数を積み上げた棒グラフを図 3-2 に示す。2009 年に大きく増加した「金融業，保険業」は 2010 年には減少したが、依然として大きな件数を維持している。年毎の件数の変動が大きい理由は、そのタイミングでなにかしらの内外の要因が働いているためと思われる。

また 2008 年まで増加傾向にあり、2009 年に減少に転じたかに見えた「公務」及び「教育，学習支援業」の件数は、2010 年に再び大きな増加を見せた。

「公務」及び「教育，学習支援業」の増加傾向の要因としては、インシデントを公表するようになってきたこと、業務で PC や USB メモリなどの使用が増加していること、自治体などで臨時職員や派遣職員が増加しており、情報漏えいを防止するための教育が浸透していないことなどが挙げられるが、こうした傾向は引き続き進行していると考えられる。

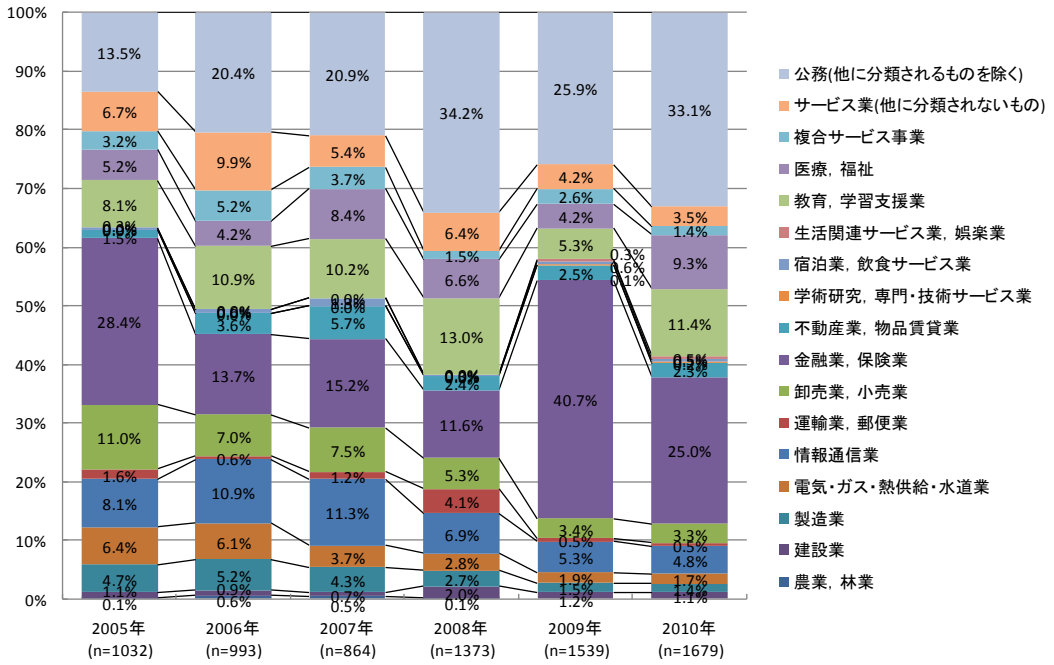

図 3-3：業種別比率の経年変化（件数）

業種別インシデント件数の比率の推移を図 3-3 に示す。2009 年に「公務」に代わり「金融業，保険業」が一番となったが、2010 年には再び「公務」が一番多くなった。これは「公務」の件数が増加した一方、「金融業，保険業」の件数が減少したことによる。

2009 年には減少した「教育，学習支援業」の割合が再び増加したほか、2008 年から減少傾向にあった「医療，福祉」が再び増加している。全体の件数が増加している中、いずれも割合が伸びているのは、大幅な件数の増加が反映されたことによる。

(3)　単年分析(人数)

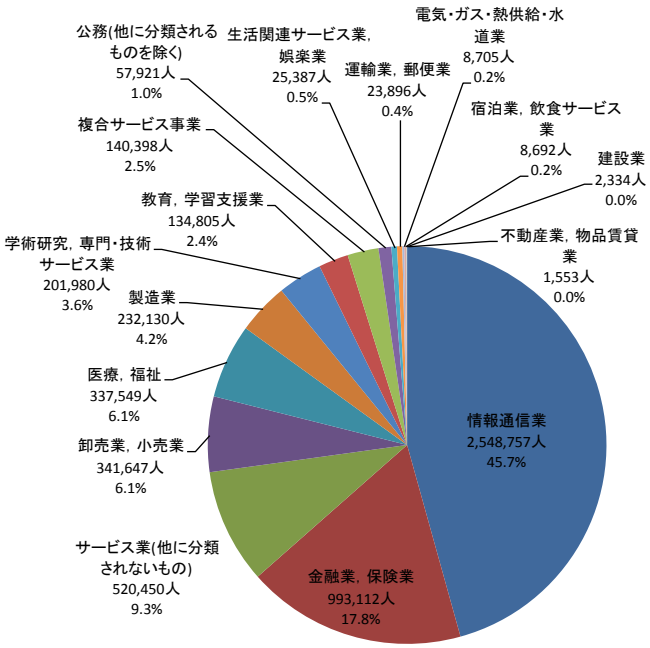

図 3-4：業種別比率（人数）

業種別での個人情報の漏えい人数を図 3-4 に示す。上位から順に「情報通信業」(45.7%)、「金融業，保険業」(17.8%)、「サービス業」(9.3%)であり、大量の個人情報を電子的に処理することの多い業種に集中した。

とくに「情報通信業」では漏えい人数 10 万人以上のインシデントが 4 件発生しており、この 4 件だけで合計人数は 2,497,108 人にのぼる。これは「情報通信業」の 98.0%、全業種合計の 44.8%を占める人数である。

「金融業，保険業」は 2009 年には突出した大規模なインシデントが多数発生したが、2010 年は大規模なインシデントが少なく、漏えい人数としては 2009 年の半分以下に減少した。

「教育，学習支援業」は、図 3-1 に示すように件数では全体の 11.4%を占めるが、図 3-4 に示すように人数では 2.4%と少ない。これは、「教育，学習支援業」において扱う個人情報にクラス単位などが多く、他の業種のインシデントと比較して規模が小さいためであると考えられる。

「公務」については、人数の比率はさらに少なく 1.0%でしかない。これは、「公務」の件数のほとんどを小規模インシデントが占めるためである。

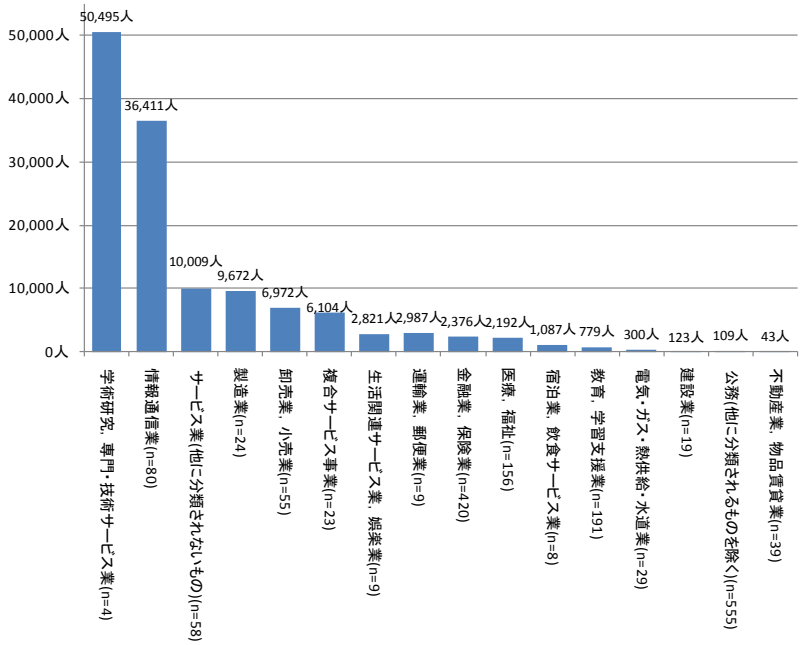

図 3-5：業種別の一件あたりの漏えい人数

インシデント一件あたりの漏えい人数（平均人数）を図 3-5 に示す。「学術研究，専門・技術サービス業」（約 5 万人）が突出しているが、これは 4 件のインシデントのうち 1 件が 20 万人以上の大規模インシデントであったためである（残りの 3 件は数十～数百件程度の小規模インシデントである）。

これにつづく上位の業種は「情報通信業」（約 3.6 万人）、「サービス業」（約 1 万人）、「製造業」（約 9,700 人）となっている。

インシデントの件数では 1 位だった「公務」の漏えい人数平均がわずかに 109 人であるが、これは前述のとおり小規模インシデントを多く含むためである。「公務」のインシデント 555 件のうち、395 件(71.2%)は 10 人未満の小規模インシデントである。こうしたインシデントの多くは、紙媒体の誤交付・誤送付などの誤操作、管理ミス、紛失・置き忘れによるものであった。

業種別での漏えい規模の比較は、「3.6 漏えい規模」の図 3-23 を参照されたい。

(4)　経年分析(人数)

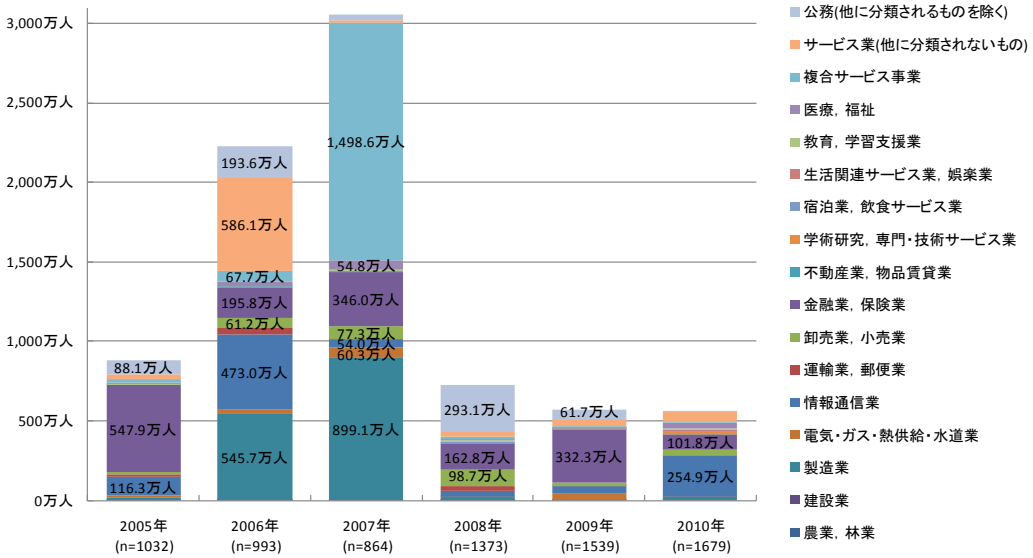

図 3-6：業種別漏えい人数の経年変化（合計）

業種別の個人情報漏えい人数を積み上げたグラフを図 3-6 に示す。2006 年、2007 年の漏えい人数が多くなっているが、いずれの年も 100 万人以上の大規模なインシデントが発生した年である。そのため、大規模なインシデントが発生した業種の人数が特異的に増えてしまい、2006 年は情報通信業が、2007 年では複合サービス業が突出したグラフになっている。同様に 2010 年は「情報通信業」が数としては他業種より突出している。つまり、業種別の個人情報漏えい人数に関しては、業種による特徴よりも、大規模な情報漏えいインシデントが発生した業種が目立つ傾向になっている。

(5)　相関分析

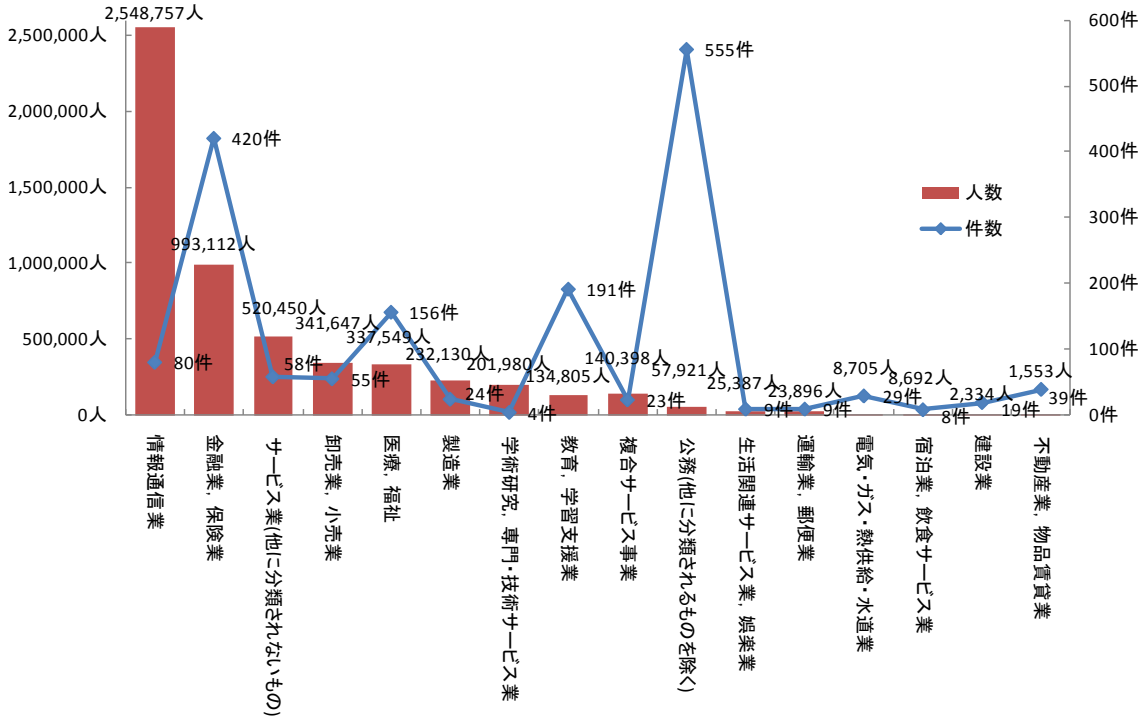

図 3-7：業種別のインシデント件数と漏えい人数

業種別のインシデント件数と漏えい人数の関係を図 3-7 に示す。2010 年に 10 万人以上の大規模インシデントが 4 件発生した「情報通信業」は、インシデント件数に比して漏えい人数が突出して多い。逆に、インシデント件数の多かった「公務」「金融業，保険業」「教育，学習支援業」「医療，福祉」は、小規模インシデントでも公表されることが多いため、インシデント件数に対して漏えい人数は少ない。

2009 年までの傾向として、一部の業種を除いて、インシデント件数と漏えい人数はほぼ正相関の関係にあった。これは多くの業種で共通して、ある程度以上の規模のインシデントしか公表しない風潮があったためと思われる。

しかし、2010 年にはこの相関関係が崩れつつあるように見える。複数の業種において小規模インシデントでも公表することが多くなり、業種間での差が開きつつあるのではないかと推測される。

3.4　原因

(1)　単年分析(件数)

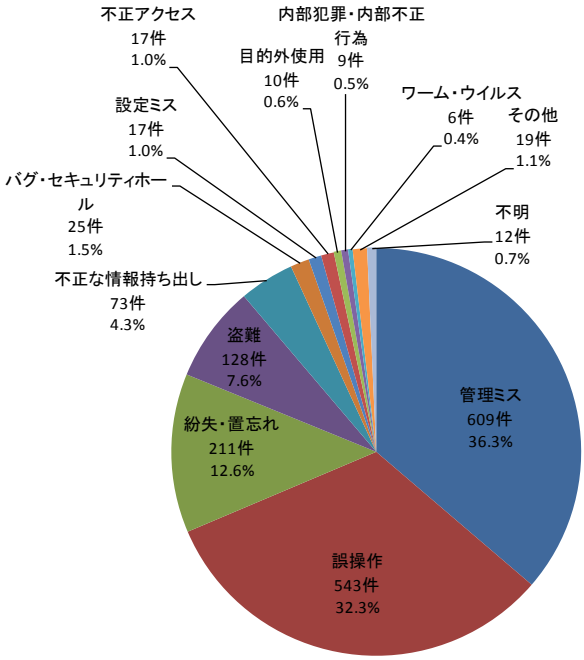

図 3-8：漏えい原因比率（件数）

個人情報漏えい件数の原因比率を図 3-8 に示す。

2010 年は「管理ミス」、「誤操作」、「紛失・置き忘れ」で約 80%を占めた。

「管理ミス」に区分されるインシデントは、組織としてルールが整備されていない、もしくはルールは存在しているものの遵守されていないために社内や主要な流通経路で発生するインシデントである。

組織としてルールが整備されていないことによるインシデントは、発見が遅れインシデントに至る経緯を明確できない場合も多い。一方、ルールが徹底されていないことによって発生するインシデントは、比較的早く発見され、経緯も明確にしやすい場合が多い。発見の遅れや不明確なままの経緯はインシデントの被害を大きくする。まずは個人情報を守るためのルール作りが望まれる。

「誤操作」及び「紛失・置き忘れ」はヒューマンエラーである。そのため対策としては、人的な対策として担当者へのセキュリティ教育(オペレーションの教育も含む)、及び組織的な対策としてヒューマンエラーを減らす予防対策として手順づくりが重要となる。ヒューマンエラーは必ず起こることを前提として暗号化などの漏えい対策や、紛失しても被害が拡大しない対策もあわせて行うとも検討する。

(2)　経年分析(件数)

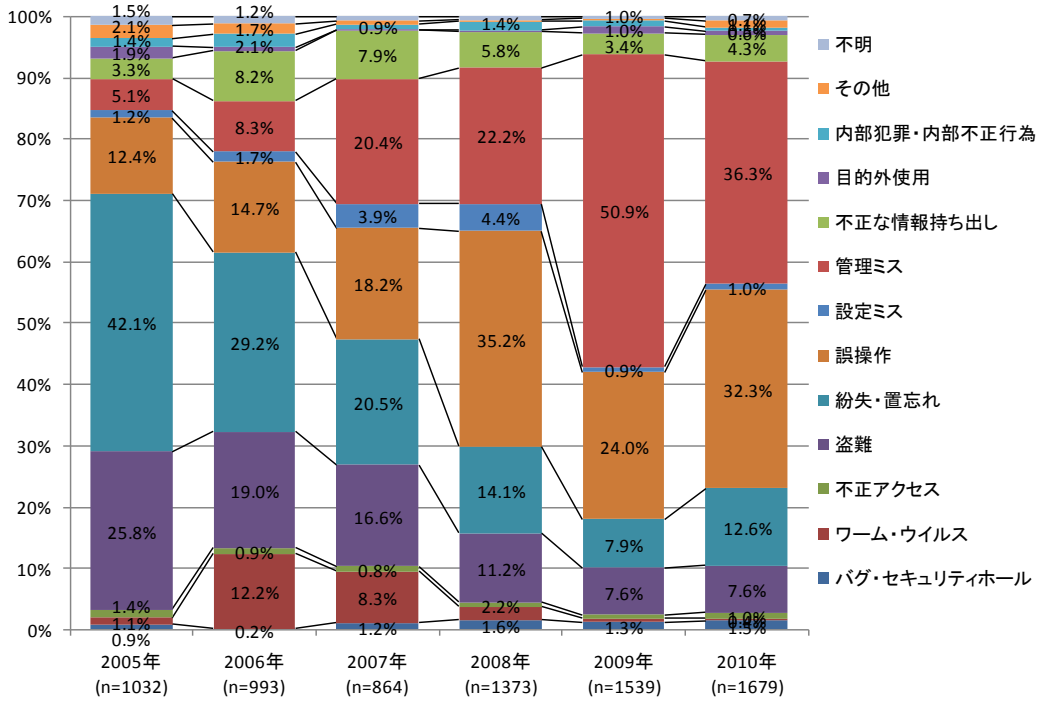

図 3-9：漏えい原因比率の経年変化（件数）

個人情報漏えい件数の原因比率の経年変化を図 3-9 に示す。

比率において 2009 年で 50.9%を占めていた「管理ミス」が 2010 年では 36.3%となり、件数では 784 件から 609 件となった。一方で、「誤操作」が 24.0%から 32.3%、件数では 369 件から 543 件、「紛失・置き忘れ」が 7.9%から 12.6%、件数では 122 件から 211 件に増加している。

管理ミス及び誤操作、紛失・置き忘れはヒューマンエラーである。これらの増加は、個人情報の取り扱いに関する担当者の意識低下と結びつけることもできる。今後注視する点である。

管理ミスの比率、件数に関しては、2010 年は 2009 年よりも減少しているが、2005 年からの変化でみると、全体的には増加傾向にあるといえる。

(3)　単年分析(人数)

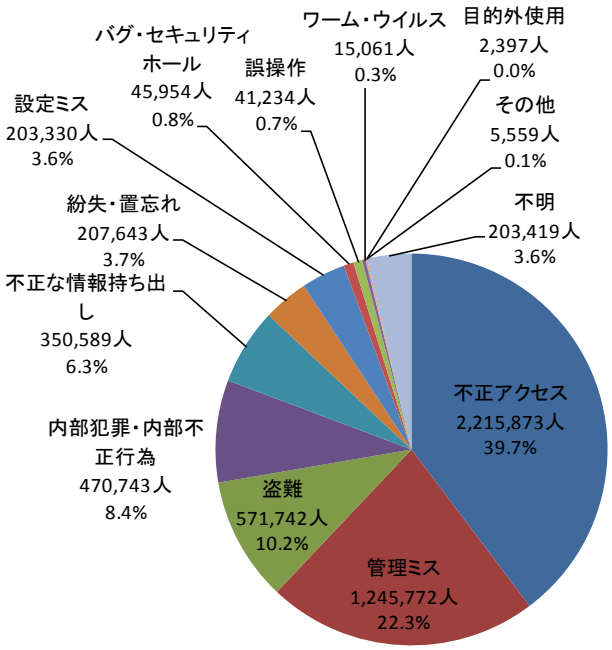

図 3-10：漏えい原因比率（人数）

個人情報漏えい人数の原因比率を図 3-10 に示す。

漏えい人数の原因比率を示す上記図 3-10 と前述した漏えい件数の原因比率である図 8 を比べると、傾向に違いが見られる。図 3-8 のように件数で集計すると、「管理ミス」、「誤操作」「紛失・置き忘れ」など当事者には悪意がない原因が並ぶが、図 3-10 のように人数で集計すると、「不正アクセス」「盗難」「内部犯罪・内部不正行為」など当事者に悪意が認められる原因が上位に入る。

漏えい人数が最も多かった「不正アクセス」は例年、1 件あたりの被害が大きくなる傾向があり、それは 2010 年も同様であった。そのため発生件数が少ない中で漏えい人数が最大となった。「内部犯罪・内部不正行為」は、際だって大きな漏えいインシデントが 1 件(約 46 万人)あり、それが漏えい人数を伸ばしている。

「管理ミス」に関しては、悪意がない原因にもかかわらず、件数とともに被害人数も多い。ここでも「管理ミス」への対策は重要であることが読み取れる。

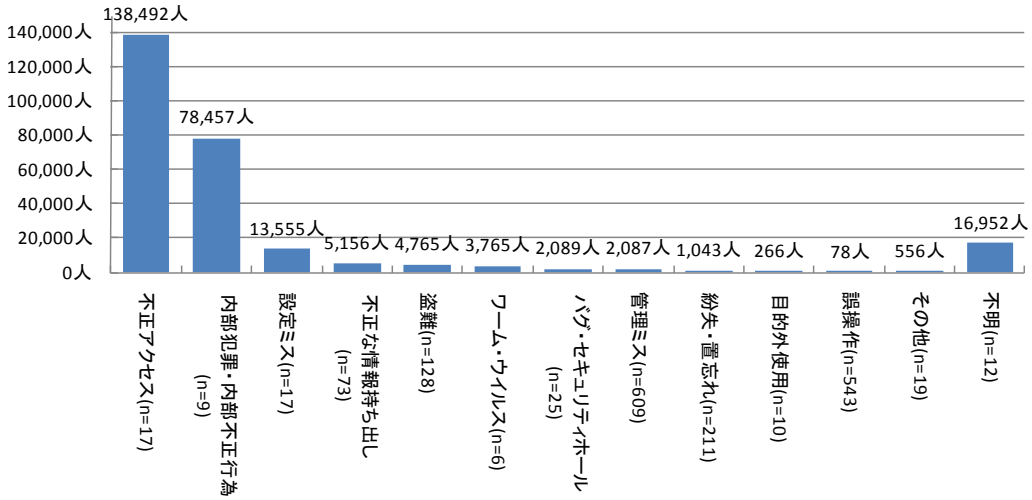

図 3-11：漏えい原因別の一件あたりの漏えい人数

漏えい原因別の一件あたりの漏えい人数を図 3-11 に示す。

図 3-11 からは、「不正アクセス」「内部犯罪・内部不正行為」の一件あたりの漏えい人数が目立つ。ただし「内部犯罪・内部不正行為」は前述したとおり突出した 1 件のインシデントによって平均人数をあげたものである。

「不正アクセス」に関しては毎年、一件のインシデントで大量の個人情報が漏えいする傾向にあるが、その傾向は 2010 年も同様である。2010 年の被害人数が多いインシデントの上位 10 位のうち 3 件が不正アクセスを原因としている。「不正アクセス」は悪意のある者が個人情報の集まりであるファイルやデータベースを対象にして行うため、発覚すると常にまとまった数の個人情報件数が漏えいすると推測される。

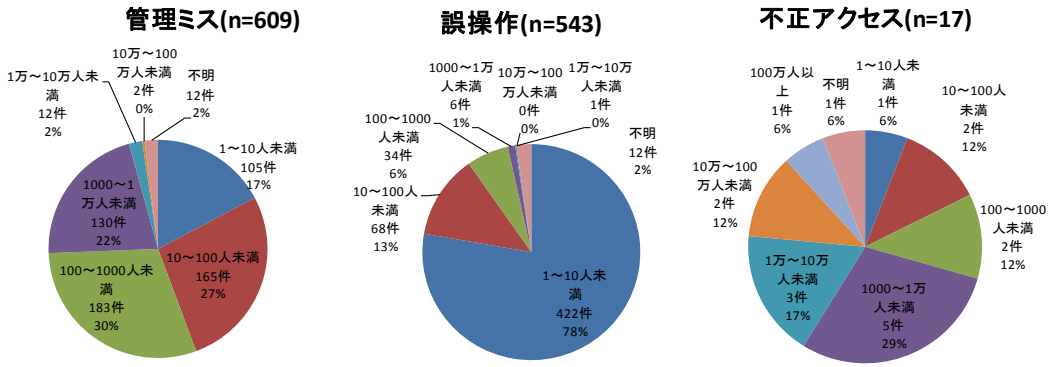

図 3-12：漏えい原因の人数区分（件数）

特徴的な漏えい人数区分を示す 3 つの原因を図 3-12 に示す。

件数では第 1 位、漏えい人数では第 2 位の「管理ミス」は 100 人未満と 1000 人未満の情報漏えいインシデントが多いと言えるが、漏えい人数の幅が広く少ない被害で収まらないことがわかる。

件数で第 2 位であった「誤操作」は、10 人未満の情報漏えいインシデントが 4 分の 3 以上を占めており、少ない人数の漏えいインシデントが目立つ。

漏えい人数で第 1 位であった「不正アクセス」は、1000 人以上～1 万人未満の規模のインシデントが最も多いが、10 万人以上の規模のインシデントを合計すると 6 件発生している。全体で 16 件しか報告されていない「不正アクセス」において、6 件の比率は大きく、ここでも「不正アクセス」が大規模なインシデントに結びつきやすい傾向がわかる。

これらの傾向から「管理ミス」に対する個人情報の管理対策を実施していくと同時に、被害が大きくなる「不正アクセス」への対策についても、優先順位を上げて検討しておく必要があると考えられる。

(4)　業種別(件数)

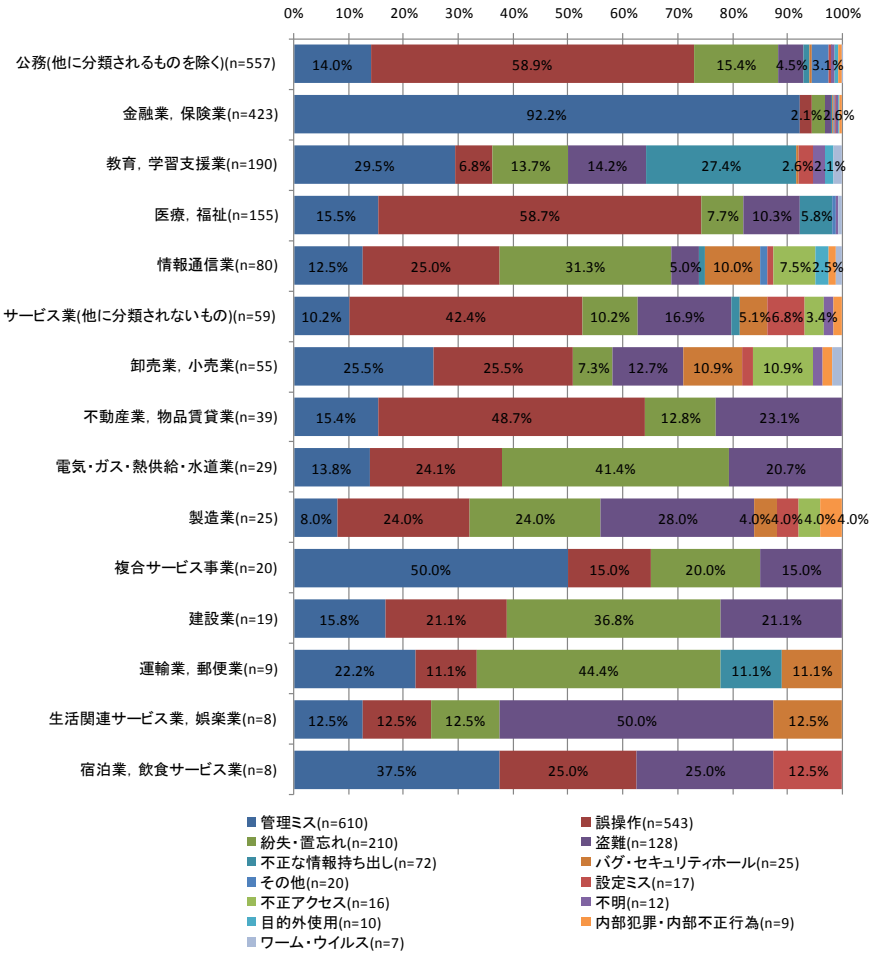

図 3-13：業種別の漏えい原因比率（件数）

業種別の漏えい原因比率を図 3-13 に示す。

「公務」は、「誤操作」の占める比率が高く、公表された件数は 328 件となっている。2010 年の「誤操作」の全件数は 543 件であるため「誤操作」の 60%を占めていることになる。内訳としては、郵送やメールの誤送付が多く、日常業務の中で情報送付という作業が多いことに起因していると推測される。「医療、福祉」においても「誤操作」の比率が高いが、「公務」と同じく郵送やメールの誤送付が多い。同様の背景があると思われる。

「金融業，保険業」は、「管理ミス」の占める比率が高く 90%を占める。インシデントの傾向としては個人情報の保管状況を再確認した結果、紛失、誤廃棄が判明したというケースが多い。複数の支店、支社の状況の確認を組織的に実施しているケースも多く、「金融業，保険業」の管理意識の高さが察せられる。

「教育・学習支援業」は、「不正な情報持ち出し」の比率が他の業種に比べて高い。件数は 57 件で、他の業種に比べて突出しており、「不正な情報持ち出し」がもっとも多い業種となっている。「不正な情報持ち出し」は当事者の意識の問題によるところが大きいが、まとまった件数が発生する場合は、業務特性と個人情報の持ち出しルールがかい離し、形骸化している可能性もある。ルールの形骸化は実質的には管理されていない状態であるためインシデントの発生を抑えることができない。現状の分析から、的を射た対策が求められる。

3.5　漏えい媒体・経路

(1)　単年分析(件数)

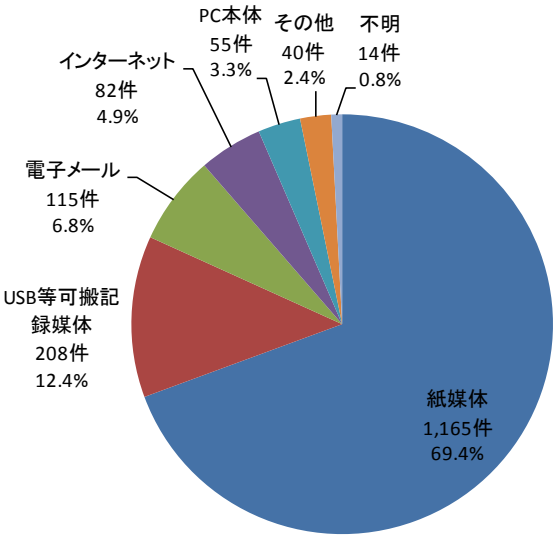

図 3-14：漏えい媒体・経路（件数）

漏えい媒体・経路別のインシデント件数を図 3-14 に示す。漏えい媒体・経路では、「紙媒体」がインシデント件数の 69.4%を占める。紙媒体は、業種や業務内容に関わらず、どんな場合においても多用される、使用機会の多い媒体であるため、それだけ漏えいすることが多い。また紙媒体によって漏えいした原因は、保管中の情報を誤廃棄するなどの「管理ミス」や、誤送付、誤交付といった「誤操作」によるものが多い。次に「USB 等可搬記録媒体」が 12.4%、「電子メール」が 6.8%を占める。

(2)　経年分析(件数)

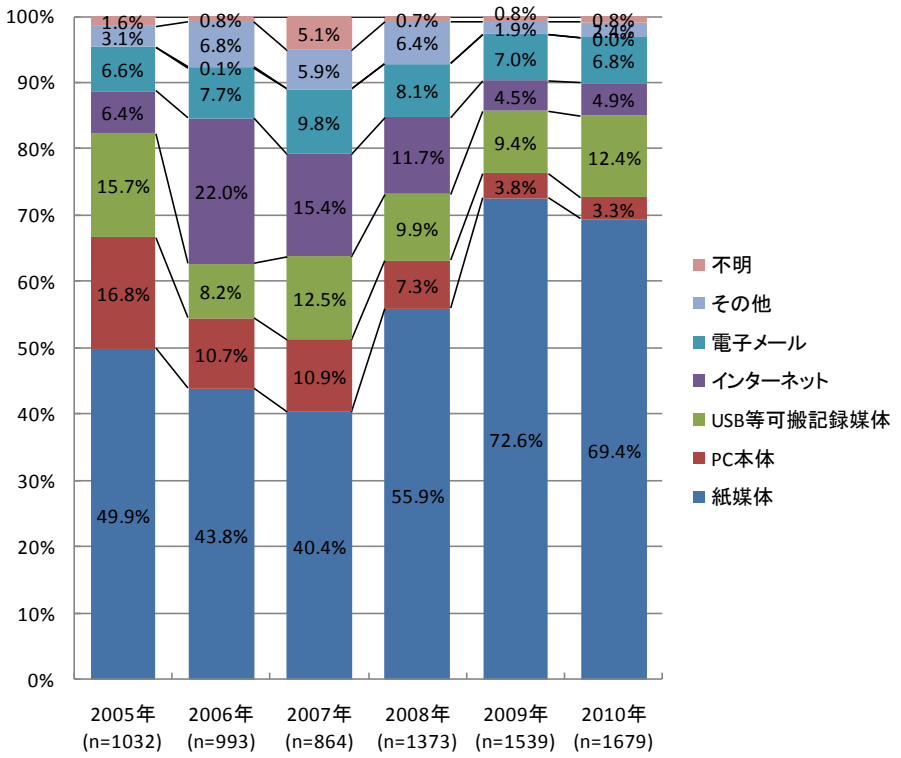

図 3-15：漏えい経路比率の経年変化（件数）

漏えい経路比率の経年変化について図 3-15 に示す。

「紙媒体」による漏えい件数は、2009 年に引き続き 2010 年も大幅に増加した。ただし、「USB 等可搬記録媒体」の件数は増加している。「PC 本体」、「インターネット」は 2008 年以前と比較すると減少している。

(3)　単年分析(人数)

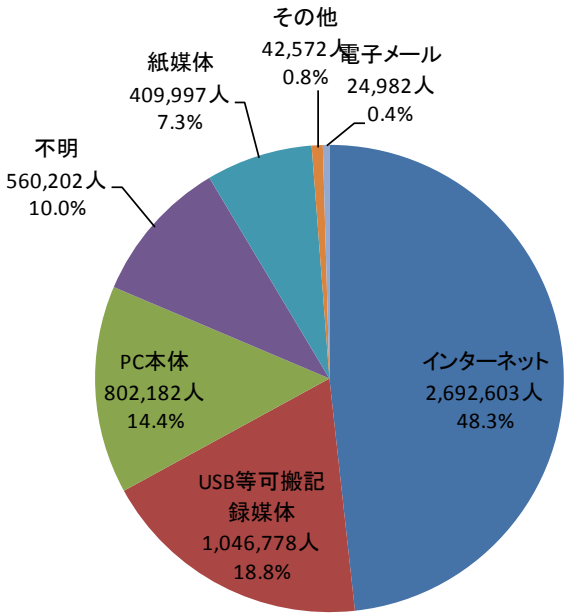

図 3-16：漏えい媒体・経路（人数）

漏えい媒体・経路別の漏えい人数を図 3-16 に示す。個人情報が漏えいした人数は、「インターネット」が約 48.3%を占める。図 3-16 に示すように「インターネット」はインシデントの件数は少ないが、1 件あたりの漏えい人数が多く、かつ、その中には、大規模なインシデントが数件含まれているため、このような結果となった。「表 3-2：インシデント・トップ 10」のうちの 5 件が昨年の「USB 等可搬記録媒体」に代わり「インターネット」よるものであり、この 5 件のインシデントだけで合計約 255 万人、漏えい人数の実に約 45%を占める。

一方、2009 年に最も人数の多かった「USB 等可搬記録媒体」は、18.8%であった。このように、大規模インシデントが人数の比率に大きく影響する。

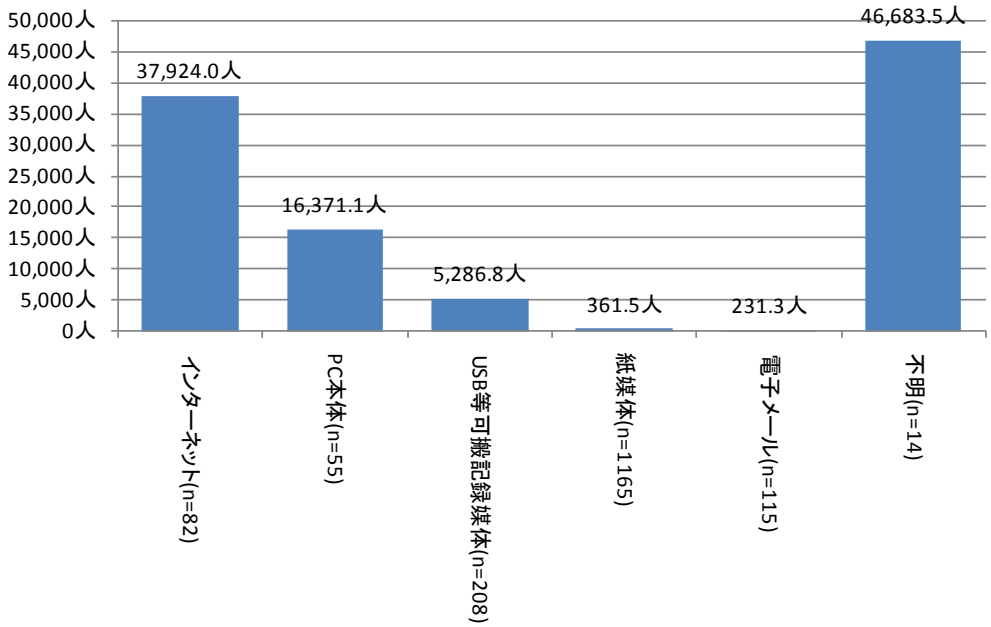

図 3-17：漏えい媒体・経路別の一件あたりの漏えい人数

漏えい媒体・経路別のインシデント一件あたりの漏えい人数を図 3-17 に示す。漏えい媒体・経路別の一件あたりの平均漏えい人数は、「インターネット」「PC 本体」「USB 等可搬記録媒体」が多い。「インターネット」の平均漏えい人数が多い理由は前述した数件の大規模インシデントが影響している面もあるが、これらの媒体・経路は、いずれも個人情報が扱い易い電子データ（ファイル）に保存されていること、個人情報が一度に大量に保存・管理されていることが関係している。

なお、漏えい媒体・経路が「不明」の平均漏えい人数が突出して大きい理由は、14 件のうちの 1 件が約 46 万人の大規模インシデントであったことによるものである。

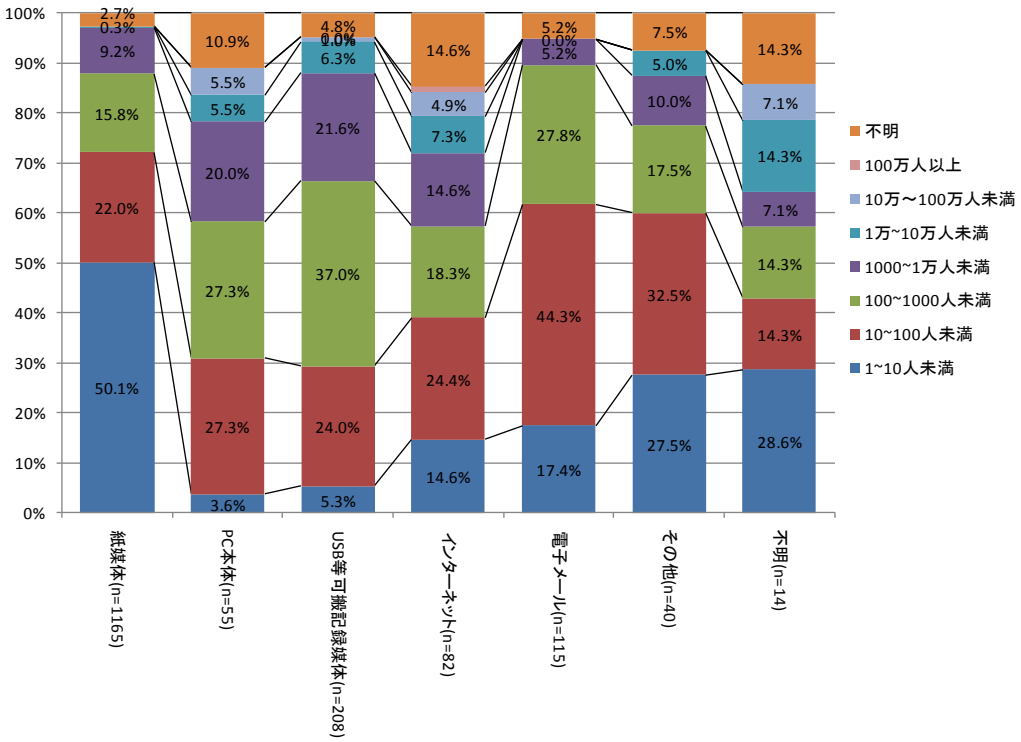

図 3-18：漏えい規模比率(件数)

漏えい媒体・経路別のインシデントの漏えい規模（件数）の比率を図 3-18 に示す。

「紙媒体」を媒体・経路とするインシデントは、漏えい規模が 1000 人未満のインシデントが約 90%を占め、とくに 1~10 人未満の小規模なインシデントの比率が約 50%と最も高い。「電子メール」も漏えい規模が 1000 人未満のインシデントの比率が約 90%を占めるが、その内訳は異なり、10～100 人未満のインシデントの比率が約 44%と高い。

一方で「インターネット」によるインシデントは、漏えい規模が 1000 人未満のインシデントの比率が低く、10 万人以上の比較的規模の大きいインシデントの比率が高い。100 万人以上の大規模なインシデントも発生している。

(4)　業種別(件数)

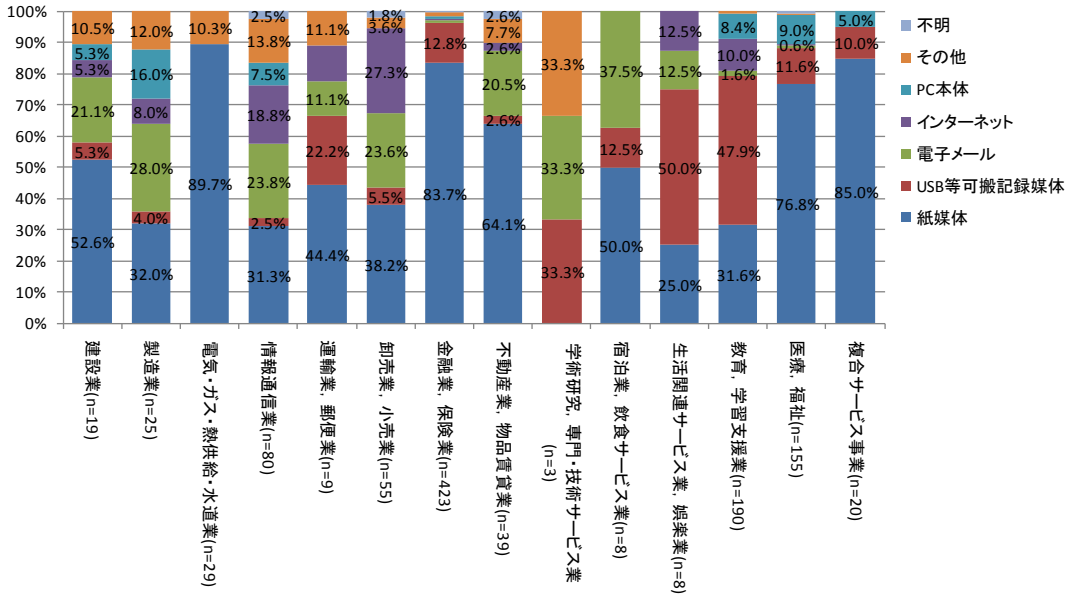

図 3-19：業種別の漏えい経路比率（件数）

漏えい媒体・経路の業種別比率（件数）について図 3-19 に示す。紙媒体は、業種、業務内容に関わらず、どんな場合においても多用される、使用機会の多い媒体であるため、紙媒体から漏えいする比率が高い業種が多い。「金融業，保険業」「複合サービス業」「公務(他に分類されるものを除く)」「医療，福祉」「電気・ガス・熱供給・水道業」は、特に比率が高い。「教育，学習支援業」は、「USB 等可搬記録媒体」による比率が高い。一方、「サービス業（他に分類されないもの）」「情報通信業」「製造業」「卸売業，小売業」は、「インターネット」および「電子メール」といったネットワークを介した漏えいインシデントの比率が高い。

業種によって、漏えいが発生しやすい媒体が異なっている。やはり、個人情報の移送・保管などに使用されることが多い媒体からの発生が多いと思われる。

3.6　漏えい規模

(1)　単年

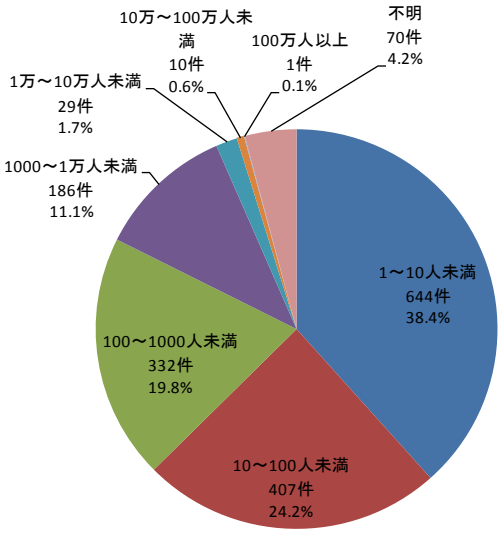

図 3-20：漏えい規模比率（件数）

インシデントの漏えい規模（人数）別のインシデント件数の比率を図 3-20 に示す。インシデントの漏えい規模が小さいほど、インシデント件数が多いことがわかる。漏えい人数 1000 人未満のインシデントを合計すると 82.4%になり、全体の 8 割以上を占めている。

一般的には、インシデントの漏えい規模が小さいほど公表されないケースが増えてくる。しかし最近は、漏えい人数が 1 件のインシデントでも積極的に公表する組織が増えてきている。

(2)　経年分析(件数)

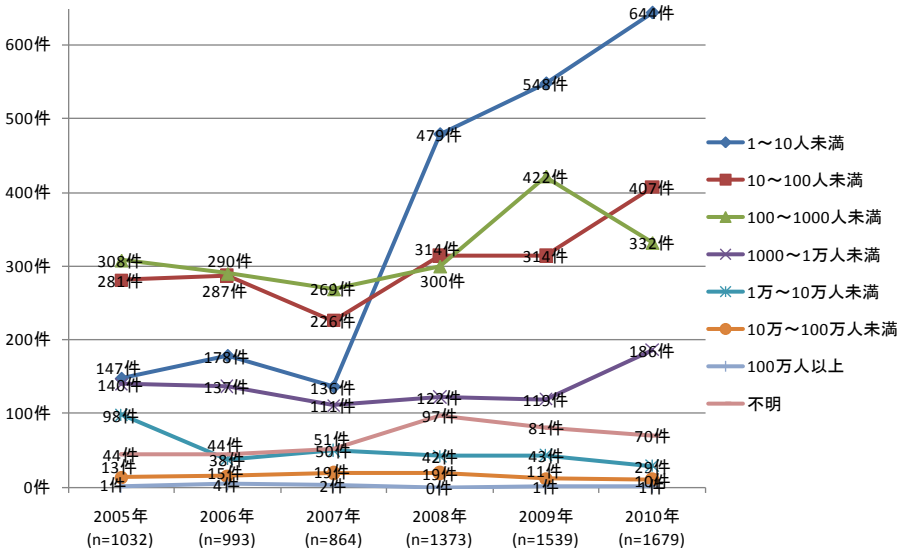

図 3-21：一件あたりの漏えい人数区分の経年変化（件数）

インシデントの漏えい規模（人数）別のインシデント件数の推移を図 3-21 に示す。2009 年に比べて、2010 年は、すべての漏えい規模の区分でインシデント件数が増加している。2008 年以降、最も漏えい規模の小さい「1~10 人未満」の区分が、最もインシデント件数が多い。これは、規模の小さいインシデントが実際に増加したということではなく、規模の小さいインシデントでも公表する組織が増えてきたためと考えられる。

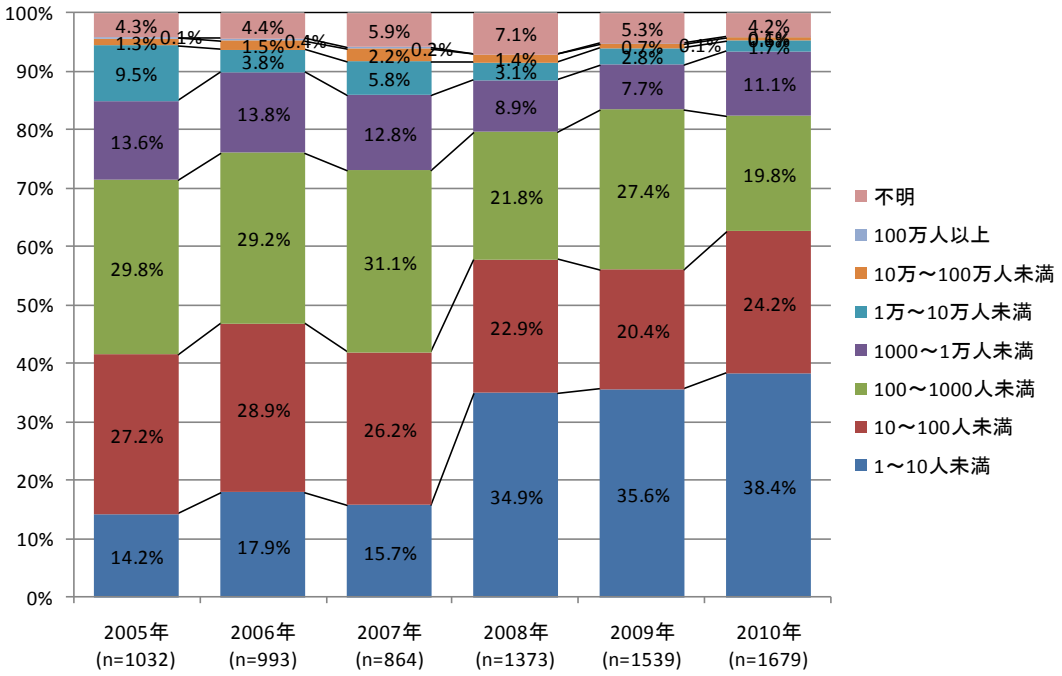

図 3-22：漏えい規模の比率の経年変化（件数）

図 3-22 は、インシデントの漏えい規模別のインシデント件数の比率の推移を棒グラフで表したものである。2008 年以降、最も漏えい規模の小さい「1~10 人未満」の区分が、最もインシデント件数が多い。2008 年以降、ほぼ同様の傾向である。

(3)　業種別（件数）

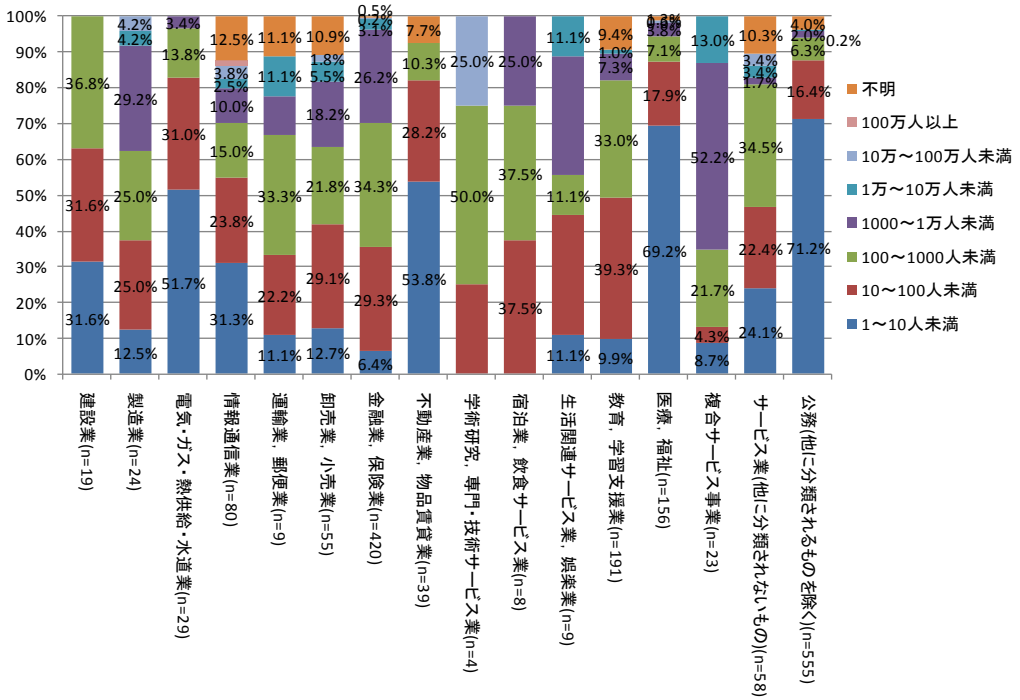

図 3-23：業種別の漏えい規模比率（件数）

業種別の漏えい規模（件数）の比率を図 3-23 に示す。小規模なインシデントとして、100 人未満までの合計で見てみると、「公務」、「医療、福祉」、「電気・ガス・熱供給・水道業」、「不動産業、物品賃貸業」の業種における比率が高く、いずれも 8 割を超えている。これは、これらの業種において、必ずしも大量の個人情報を保有していないわけではないが、窓口業務や現場業務において、比較的、人数の少ない個人情報を取り扱っているためと思われる。大規模なインシデントとして、100 人以上の合計で見てみると、「複合サービス事業」の業種における比率が高く、8 割に達している。数千枚の伝票を誤廃棄したインシデントなどがあった。

3.7　漏えい情報の価値

(1)　漏えい情報

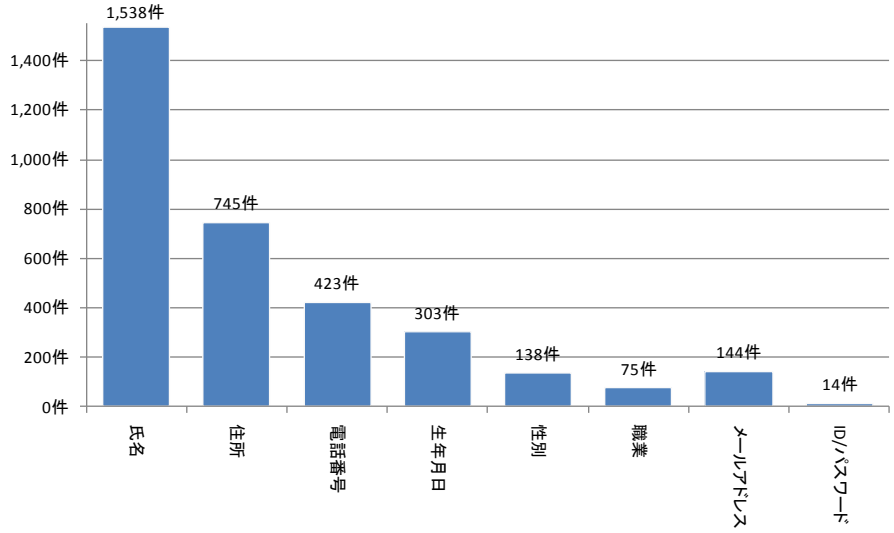

図 3-24：漏えい情報の出現確率

表 3-3：漏えい情報の出現確率

人数区分	件数	出現確率
氏名	1,538 件	95.6%
住所	745 件	46.3%
電話番号	423 件	26.3%
生年月日	303 件	18.8%
性別	138 件	8.6%
職業	75 件	4.7%
メールアドレス	144 件	9.0%
ID/PASSWD	14 件	0.9%

漏えい情報の出現確率を図 3-24、表 3-3 に示す。

「氏名」の出現率が 95.6%であり、2009 年（88.4%）までと同様、著しく高い。次いで住所（46.3%）、電話番号（26.3%）と続く。「氏名」、「住所」は基本的な個人情報であるため、出現率が高いと考えられる。

約 1 パーセントの確率で、ID とパスワードが漏えいしており、深刻な被害を及ぼ

す恐れがある個人情報が漏えいしていることが分かる。

(1)　漏えい情報の価値分布(EP図)

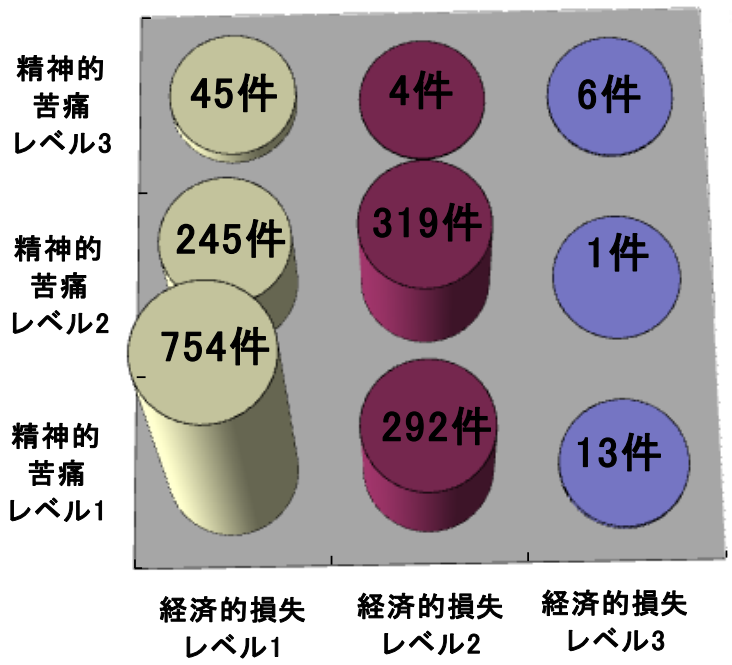

図 3-25：シンプル EP 図分布（件数）

2010 年のインシデントで漏えいした情報について、精神的苦痛レベルと経済的損失レベルの二つの評価軸を用いて機微度を評価し、シンプル EP 図上に表示した結果を図 3-25 に示す。

2010 年の被害分布状況の特徴としては、精神的苦痛と経済的損失のレベルが共に 1 であるフィールドが大幅に増加したことである。これは、「金融業，保険業」におけるインシデントが減少し、「公務」等で見られる小規模なインシデントが増加したことが要因と考えられる。

(2)　業種別EP分布

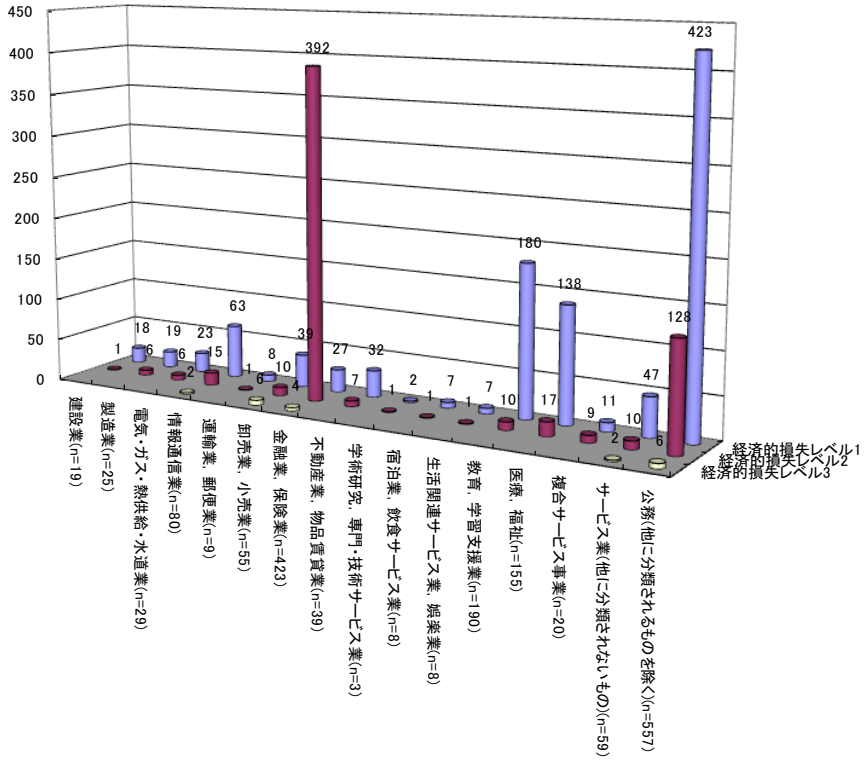

図 3-26：漏えい情報の経済的損失レベル分布（件数）

漏えい情報の経済的損失レベル分布（件数）を図 3-26 に示す。

経済的損失レベル 1 の個人情報が漏えいしたインシデント件数が多い業界は「公務」、「教育，学習支援」、「医療，福祉」である。

経済的損失レベル 2 の個人情報が漏えいしたインシデント件数が多い業界は、「金融業，保険業」、「公務」、「医療，福祉」、「情報通信業」である。「金融業，保険業」業界が特出しているが、これは預金残高等やクレジットカード情報が多いためだと考えられる。

経済的損失レベル 3 の個人情報が漏えいしたインシデント件数が多かったのは、「公務」、「卸売業，小売業」であり、他は 5 件未満であった。

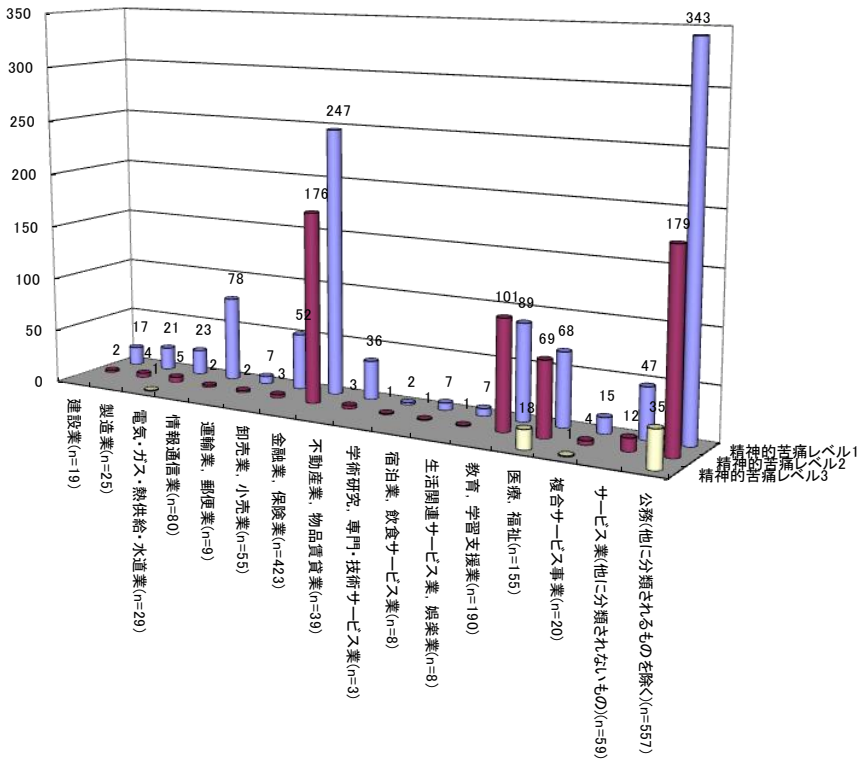

図 3-27：漏えい情報の精神的苦痛レベル分布（件数）

漏えい情報の精神的苦痛レベル分布（件数）を図 3-27 に示す。

精神的苦痛レベル 1 の個人情報が漏えいしたインシデント件数が多い業界は「公務」、「金融業，保険業」、「教育，学習支援業」である。

精神的苦痛レベル 2 の個人情報が漏えいしたインシデント件数が多い業界は、「公務」、「金融業，保険業」、「教育，学習支援業」、「医療，福祉」となっている。「金融・保険業」については経済的損失の場合と同様に預金残高、クレジットカード情報などが多いためである。また、「教育，学習支援業」、「医療，福祉」ではレベル 1 の件数より、レベル 2 の件数の方が多い。これは、主にテストの結果や健康診断の結果などの情報が漏えいしているためである。

精神的苦痛レベル 3 の個人情報が漏えいしたインシデント件数が多い業界は、「公務」、「医療，福祉」である。これは、「公務」では、本籍、犯歴などの情報が、「医療，福祉」では、病名、病歴などが漏えいしたためである。

3.8 経年分析

2005 年から 2010 年の間に収集した 6 年間分のインシデント情報をもとに様々な経年分析を行った。2002 年から 2004 年までのインシデント情報は公表件数が少なく、統計データとしては偏りが大きいため、2010 年の分析では、これらを除外した。

表 3-4：漏えい人数とインシデント件数の経年変化

	インシデント件数	漏えい人数	一件あたりの平均漏えい人数※
2005 年	1,032 件	881 万 4,735 人	8,922 人
2006 年	993 件	2,223 万 6,576 人	2 万 3,432 人
2007 年	864 件	3,053 万 1,004 人	3 万 7,554 人
2008 年	1,373 件	723 万 2,763 人	5,668 人
2009 年	1,539 件	572 万 1,498 人	3,924 人
2010 年	1,679 件	557 万 9,316 人	3,468 人

2010 年のインシデント件数は、2005 年以降において最多の 1,679 件となった。一方、漏えい人数は 2009 年からさらに減少し、2005 年以降において最少の約 556 万人となっており、2007 年以降、毎年減少する傾向にある。その結果、個人情報が漏えいした人は、日本の人口の約 23 人に 1 人の割合であった。

漏えい人数は、過去の集計分析から少数の大規模漏えいインシデントに影響されることが分かっている。1 件当たり 100 万人以上の漏えいインシデントは、2006 年が 4 件、2007 年が 2 件（内 1 件は 1000 万人超）、2008 年が 0 件、2009 年が 1 件、2010 年が 1 件であった。

インシデント一件あたりの平均漏えい人数も過去最少の 3,468 人／件となっている。これは、漏えい人数が 1000 人未満のインシデントが全体の 82.4%(1,383 件)を占めることからもわかるように、小規模なインシデントが多く公表されていることが大きく関係している。

※漏えい人数をインシデント件数（被害者数不明のインシデント件数を除く）で除算する。例えば 2010 年は 1,679 件から被害者数不明の 70 件を除いた 1,609 件で漏えい人数を除算した。

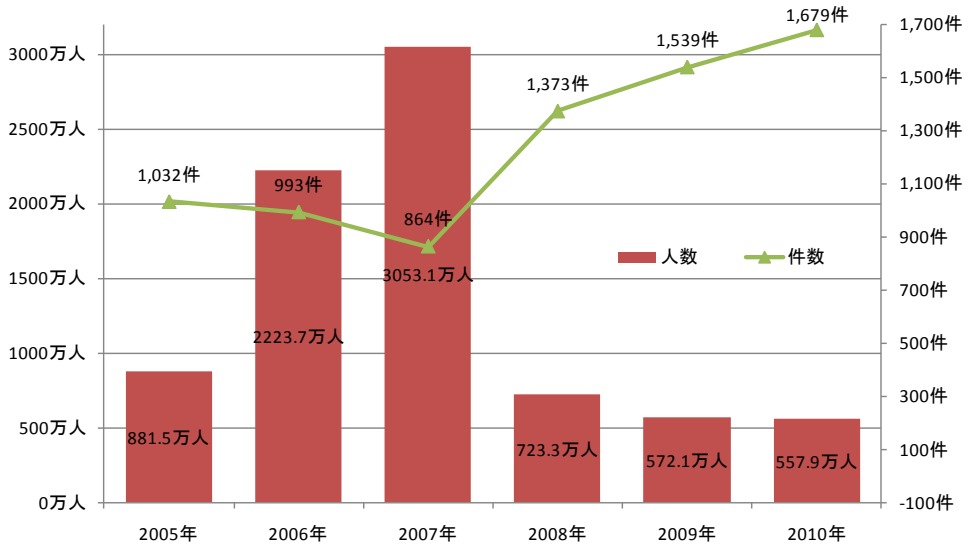

図 3-28 インシデント件数と内部不正による漏えい人数の経年変化（合計）

インシデント件数と内部不正による漏えい人数の経年変化を図 3-28 に示す。

個人情報保護法が完全施行された 2005 年以降、毎年 1,000 件程度の個人情報の漏えいインシデントが新聞やインターネットニュースで報道され続けており、2010 年は過去最多の 1,679 件となった。情報漏えいインシデントを起こしてしまった組織が、積極的にインシデントを公表する姿勢が定着してきているものと考えられる。

特に金融業，保険業や公務のように社会的影響の大きい業種は、漏えい人数が小規模のインシデントであっても公表している。一方漏えい人数は、2005 年から 2007 年まで増加傾向であったが、2008 年以降は明らかに減少している。これは、大規模なインシデントが減少し、小規模なインシデントの件数の割合が大きいためである。

表 3-5：内部不正による漏えい人数の経年変化の割合

原因	2005 年	2006 年	2007 年	2008 年	2009 年	2010 年
内部犯罪・内部不正行為	10.2%	18.0%	28.3%	4.4%	29.1%	8.4%
内部犯罪・内部不正行為以外	89.8%	82.0%	71.7%	95.6%	70.9%	91.6%

内部犯罪・内部不正行為による漏えい人数の割合は、2010 年は 8.4%であった。

この割合は、年によってまちまちであり、件数が少ない分 1 件当たりの漏えい規模（漏えい人数）によって大きく変化する。そのため、人数ベースでの分析では、特に決まった傾向はみられない。

内部犯罪や不正行為は、一時期の内部統制の推進によって、一定の対応が進んでいるはずだが、権限を持つ者による故意の不正については確実な解決策は無く、今後も単発的に発生するものと考えられる。

4　2010 年 想定損害賠償額の算定結果

4.1　想定損害賠償総額

表 4-1：想定損害賠償総額の経年変化

	想定損害賠償総額
2005 年	約 5,329 億円
2006 年	約 4,570 億円
2007 年	約 2 兆 2,711 億円
2008 年	約 2,367 億円
2009 年	約 3,890 億円
2010 年	約 1,215 億円

2010 年の想定損害賠償総額である約 1,215 億円は、平成 23 年度の高速道路無料化社会実験の予算額に相当する。

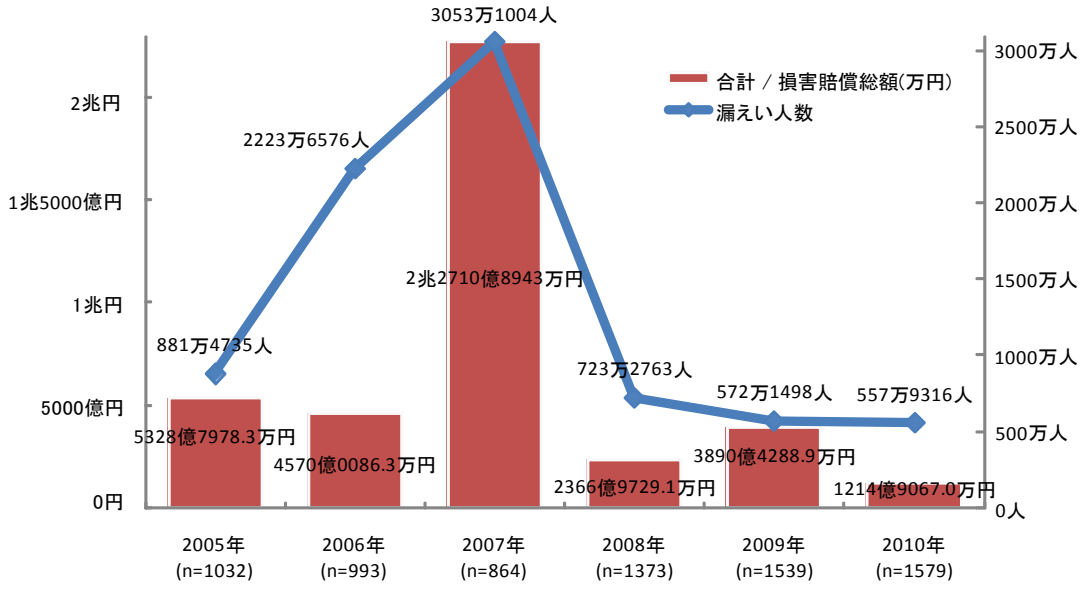

図 4-1：想定損害賠償総額と漏えい人数

想定損害賠償総額と漏えい人数の関係を図 4-1 に示す。

2010 年の漏えい人数と想定損害賠償総額を 2009 年と比較すると、漏えい人数、想定損害賠償総額ともに減少している。この原因は、単純に漏えい人数の減少による。2008 年以降、3 年間に渡って、漏えい人数、想定損害賠償総額が低い値であることから、対策の効果が現れているのかもしれない。

4.2　一人あたりの想定損害賠償額

(1)　単年分析

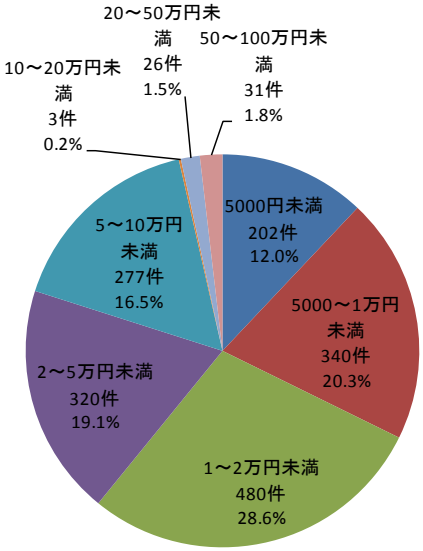

図 4-2：一人あたりの想定損害賠償額比率（件数）

一人あたりの想定損害賠償額を図 4-2 に示す。

2010 年は、一人あたりの想定損害賠償額が「1～2 万円未満」*のインシデント件数の占める比率が約 30%と最も多く、次いで「5000～1 万円未満」の比率が約 20%、合わせて約 50%となった。

* 一人あたりの想定損害賠償損害額が年々増加していることから、2009 年の報告書より金額の内訳単位を詳細に変更した。

(2)　経年分析

表 4-2：一人あたりの平均想定損害賠償額

	想定損害賠償総額
2005 年	4 万 547 円
2006 年	3 万 6743 円
2007 年	3 万 8228 円
2008 年	4 万 3632 円
2009 年	4 万 9961 円
2010 年	4 万 2662 円

一人あたりの平均想定損害賠償額は、3 万円後半から 5 万円の範囲に収まっている。

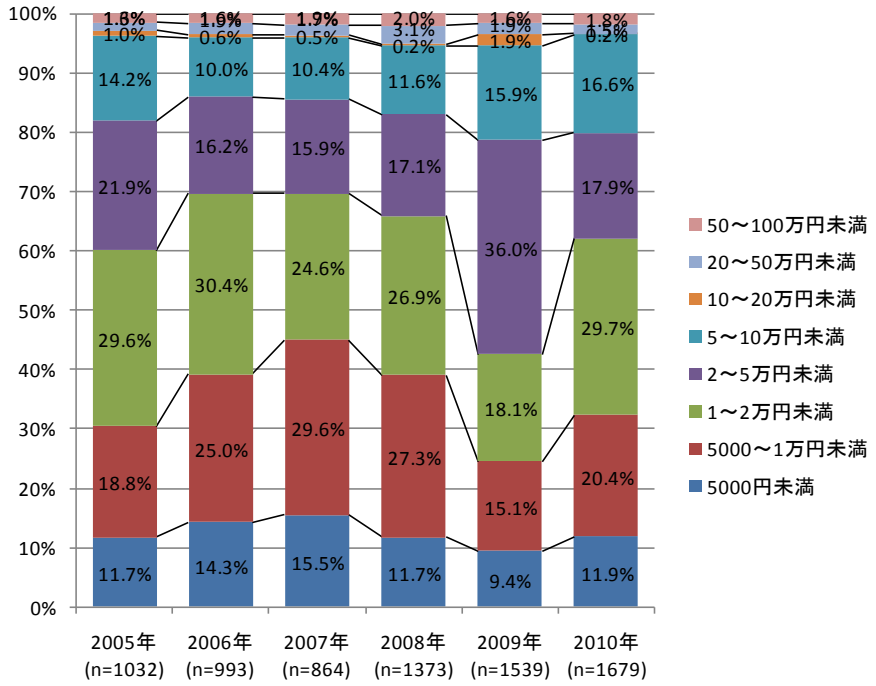

図 4-3：一人あたりの想定損害賠償額比率の経年変化（件数）

一人あたりの想定損害賠償額比率の経年変化を図 4-3 に示す。

2010 年は、2009 年と比べて「2～5 万円未満」のインシデント件数の割合が大きく減少し、「1～2 万円未満」インシデント件数の割合が大きく増加した。2005 年から 2010 年の経年変化を全体的に俯瞰してみると、実は 2009 年の「1～2 万円未満」と「2～5 万円未満」のインシデント件数の割合が、他の年と異なっている事がわかる。

【一人あたりの平均想定損害賠償額について】

「一人あたりの想定損害賠償額」は、インシデント毎に算出している。「一人あたりの平均想定損害賠償額」は、このインシデント毎の「一人あたりの想定損害賠償額」の平均金額を求めた。よって、全インシデントの「一人あたりの想定損害賠償額」を合計し、「インシデント総件数」で除算して、「一人あたりの平均想定損害賠償額」を算出している。「想定損害賠償額の合計」を「漏えい人数の合計」で、除算した値ではないことに注意されたい。

算出式、及び具体的な計算例は、以下の通りである。

インシデントが以下の 2 件の場合
A インシデントの一人あたり想定賠償額 ＝a 円
B インシデントの一人あたり想定賠償額 ＝b 円
一人あたりの平均想定損害賠償額 ＝(a 円＋b 円)÷2 件

■具体例

表 4-3：インシデント内容（具体例）

	漏えい人数	想定損害賠償総額	一人あたりの想定損害賠償額
A インシデント	1 人	100 万円	100 万円
B インシデント	100 人	100 万円	1 万円

表 4-4：一人あたりの想定損害賠償額（具体例）

	漏えい人数	一人あたりの想定損害賠償額
人数で除算した場合	101 人	200 万円÷101 人 ＝1.98 万円
本報告書の場合	101 人	(100 万円+1 万円)÷2 件 ＝50.5 万円

4.3　一件あたりの想定損害賠償額

(1)　単年分析

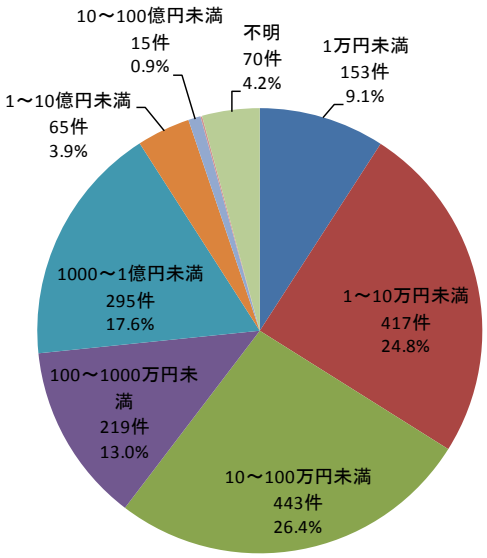

図 4-4：一件あたりの想定損害賠償額比率（件数）

一件あたりの想定損害賠償額を表 4-3 に示す。

一件あたりの想定損害賠償額が 100 万円未満のインシデントが半数以上(約 60%)を占め、そのうち「10 万円以上～100 万円未満」の比率が最も高く 26.3%である。

一件あたりの想定損害賠償額が 100 万円未満のインシデントは、一件あたりの漏えい人数が少なく、かつ漏えいした個人情報の価値があまり高くないインシデントであると考えられる。

(2) 経年分析

表 4-5：一件あたりの平均損害賠償額の経年変化

	一件あたりの平均想定損害賠償額	(参考) 想定損害賠償総額
2005 年	5 億 3935 万円	約 5329 億円
2006 年	4 億 8156 万円	約 4570 億円
2007 年	27 億 9347 万円	約 2 兆 2711 億円
2008 年	1 億 8552 万円	約 2367 億円
2009 年	2 億 6683 万円	約 3890 億円
2010 年	7551 万円	約 1215 億円

2010 年の一件あたりの想定損害賠償額は、これまでの想定損害賠償額のうちで、最も少ない。理由の一つは、漏えい人数が少ないことが挙げられる。理由のもう一つは、機微な個人情報が大規模に漏えいしたインシデントが少なく、一件あたりの想定損害賠償額が巨額になるインシデントがなかったことが挙げられる。

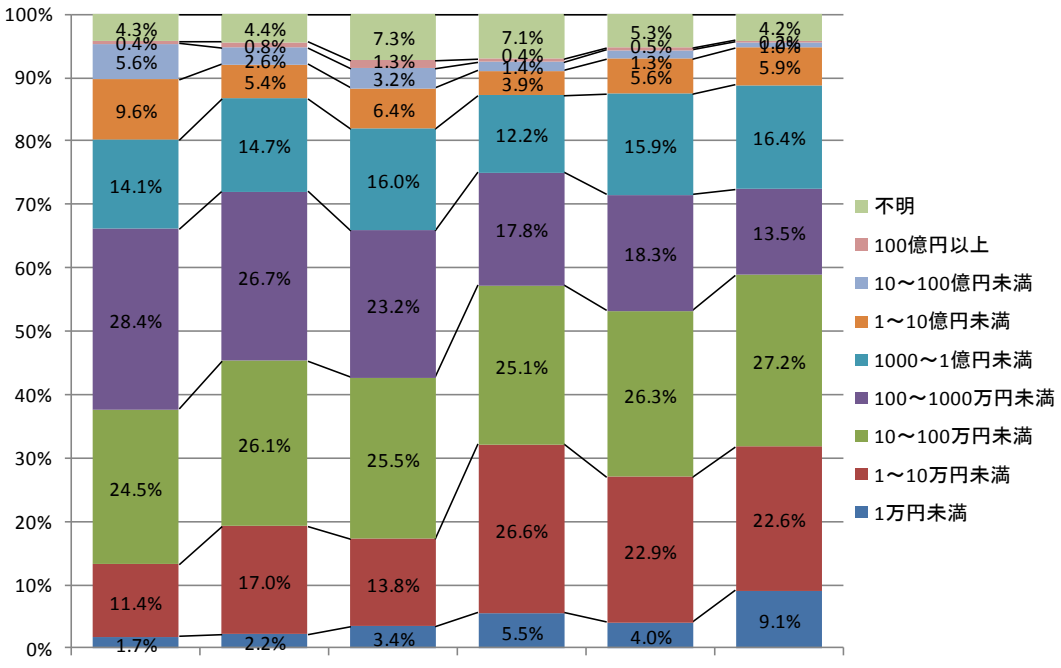

図 4-5：一件あたりの想定損害賠償額比率の経年変化（件数）

一件あたりの想定損害賠償額の経年変化を図 4-5：一件あたりの想定損害賠償額比率の経年変化（件数）に示す。

2007 年以前と比べて、2008 年以降は「1 万円以上～10 万円未満」の比率が高い。それに伴って、全体的に 100 万円未満の比率も、それまでの約 45%から約 55%へ、やや高くなっている。逆に「100 万円以上～1000 万円未満」の比率は、減少している。

2010 年は大規模インシデントが少なく、一件あたりの想定損害賠償額が 10 億円以上の高額なインシデントが占める比率は減少している。しかしながら、「100～1000 万円未満」、「1000 万～1 億円未満」の規模のインシデントが増加しており、今後の動向が気になる。

5　個人情報漏えいにおける想定損害賠償額の算出モデル

5.1　想定損害賠償額の算出の目的

想定損害賠償額の算定式の提案、及び算出式を実際のインシデントに適用した想定損害賠償額の算出は、当ワーキンググループの調査報告書の特徴である。

当ワーキンググループは、当初から実際に発生したインシデントの分析によるリスクの定量化と対策効果の定量化を目的に活動してきた。想定損害賠償額算定式の提案も、個人情報を取り扱う組織の潜在的なリスクを数値として把握することを目的にしている。よって、本算定式は各組織が所有する個人情報の潜在的リスクを把握するためのひとつの推定方法であり、被害者が漏えい元の組織に対して請求できる損害賠償額を示したものではない点を認識いただきたい。また、個人情報を保有している組織は、保有する個人情報について算定を試みていただきたい。

なお、以下に挙げる算定結果は、あくまでも「もし被害者全員が賠償請求したら」という“仮定”に基づくものであり、実際に各事例においてその金額が支払われたものではないことに注意していただきたい。

5.2　想定損害賠償額算定式の解説

想定損害賠償額の算定にあたっては、2010 年も 2003 年の調査方法を踏襲した。改定を行わなかった理由は、現実の判決による賠償額と本算定式による算定結果が許容できる範囲の差異に収まったことから、現行の算定式が十分使えるものと判断したためである。

想定損害賠償額の算定式の成り立ちについては、2003 年の報告書を参照いただきたい。ここでは簡単に概要を記述するに留める。

5.2.1　想定損害賠償額算定式の策定プロセス

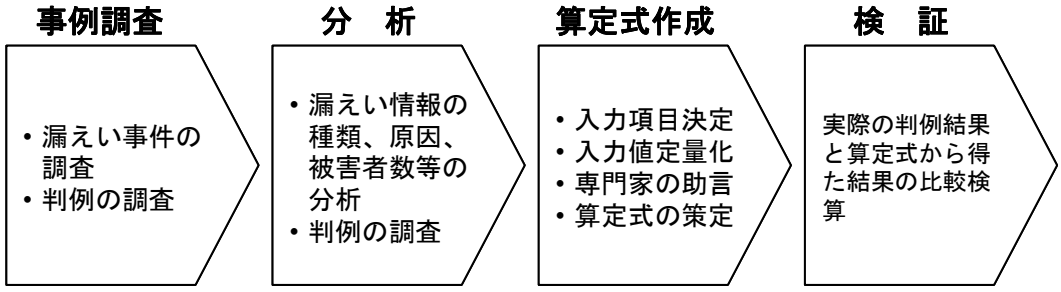

図 5-1：想定損害賠償額算定式策定のプロセス

図 5-1 に示す通りのプロセスで想定損害賠償算定式を策定した。

① 事前調査

報道されたインシデントを調査・集計する。同時に過去のプライバシー権侵害や名誉毀損の判例を調査する。ここでは 2003 年の報告書で説明した通り、「宇治市住民基本台帳データ大量漏えい事件控訴審判決 大阪高等裁判所 平成 13 年（ネ）第 1165 号 損害賠償請求控訴事件」を参考にした。

② 分析

集計したインシデントの被害者数、漏えい情報種別、漏えい原因、漏えい経路などを分析する。2010 年の分析結果は「3. 2010 年の個人情報漏えいインシデントの分析結果」の通りである。

③ 算出式作成

算出式の入力項目を決定し、算定式を策定。入力項目は、漏えい情報の価値、漏えい組織の社会的責任度、事後対応評価とした。また、弁護士など専門家の意見も取り入れた。

④ 検証

策定した算定式の信憑性をはかるため、先の宇治市の事例に当てはめ、算定式で得られた結果と実際の判決による損害賠償額と比較した。Yahoo! BB、及び TBC の判決との比較も行った。その結果、同程度の数値が得られた。

5.2.2 算定式の入力値の解説

当該算定式では以下の項目を入力値とした。

- 漏えい個人情報価値
- 情報漏えい元組織の社会的責任度
- 事後対応評価

実際の訴訟では、これらの項目以外にも、事前の保護対策状況、漏えいした情報の量、漏えい後の実被害の有無、事後対応の具体的な内容なども評価されると考えられる。しかし、当該算定式の策定において参考にする情報は公開情報であり、そこから読み取れる内容には限りがある。また、入力値や算出方法が複雑すぎて、セキュリティの専門家でなければ計算できなかったり、算出に必要な入力値が収集できなかったりすると、各組織が自ら所有する個人情報の潜在的リスクを算出するという目的に用いられなくなってしまう。よって、入力値をこれらに絞り、かつ値の算定が容易となるような計算方法を策定した。

以下に、それぞれの入力値を定量化して想定損害賠償額を算定する方法を解説する。

(1) 漏えい個人情報の価値

個人情報が漏えいした際に被害者に与える影響を、「経済的損失」と「精神的苦

痛」という 2 種類の尺度で分類した。影響の大きさを定量化するため、縦軸（y 軸）に「経済的損失」の度合いを、横軸（x 軸）に「精神的苦痛」の度合いを持たせたグラフを作成した。このグラフを便宜上 EP 図（Economic-Privacy Map）と名づける（図 5-2)。x 軸の正の方向の位置によって精神的苦痛の大きさを、y 軸の正の方向の位置によって経済的損失の大きさを表現する。

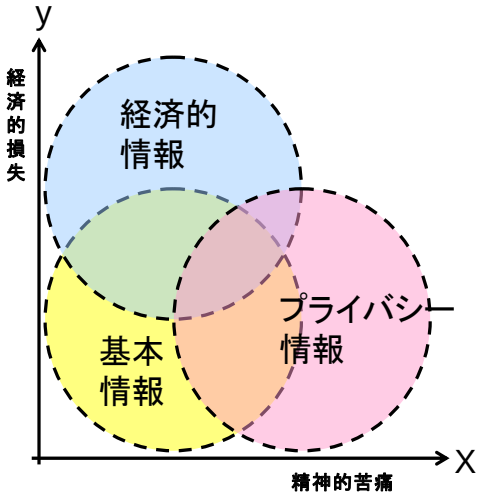

図 5-2：EP 図（Economic-Privacy Map）

この EP 図上へ、「個人情報の保護に関する法律（個人情報保護法)」、「個人情報保護に関するコンプライアンス・プログラムの要求事項（JIS Q 15001)」、及び過去の情報漏えいインシデントの調査分析で得られた漏えい情報の種類をプロットした。漏えいした情報がどのような影響をあたえるのか、つまり EP 図上の情報の位置により情報の価値を求めることができる。さらに、算出式への値の入力のしやすさ等を考慮し、EP 図の x 軸、及び y 軸をそれぞれ 3 段階に分け、漏えい情報の影響の度合いに応じて、漏えい情報を種類別に再配置した。再配置した図 5-3 が、シンプル EP 図である。

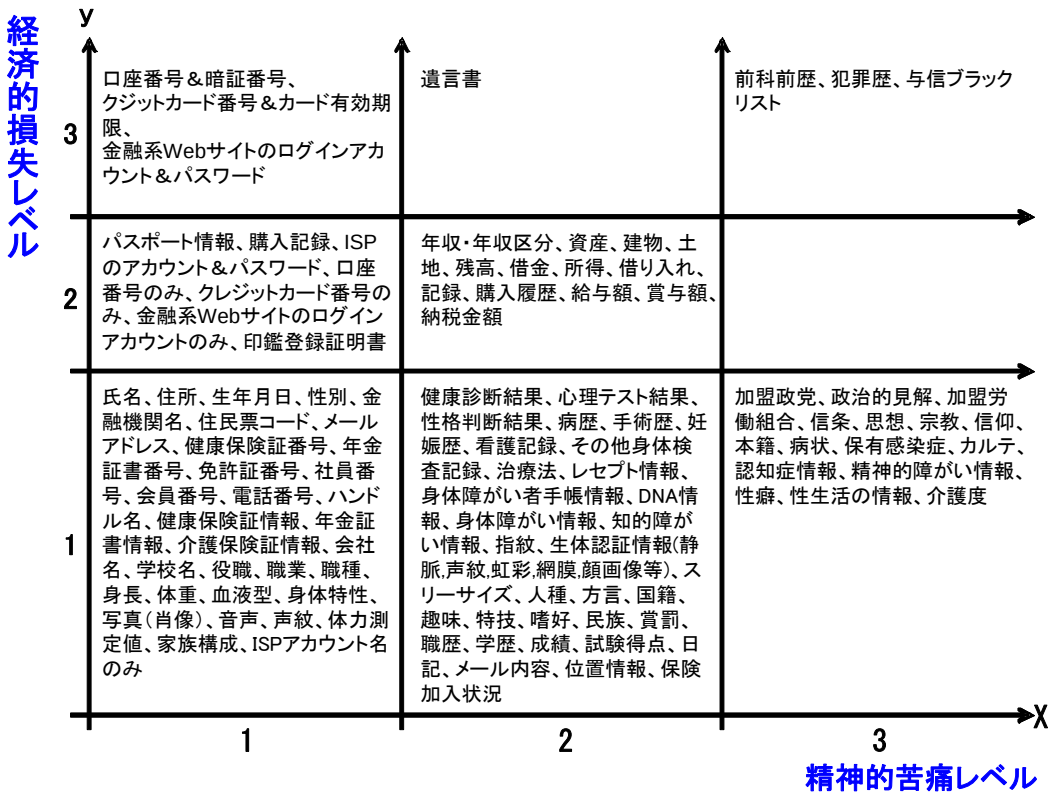

図 5-3：シンプル EP 図

ただし、単純に情報をシンプル EP 図上にあてはめて、その座標値（x 値、y 値）から漏えい情報の価値を推定するのではなく、実被害への結び付き易さを考慮して補正を加える必要があると考えた。その補正を加えた漏えい情報の価値を求めるための算出式を以下に示す。

漏えい個人情報価値 ＝ 基礎情報価値×機微情報度×本人特定容易度

各属性値の定義は、以下の通りである。

a. 基礎情報価値

基礎情報価値には、情報の種類に関わらず基礎値として、“一律 500 ポイント”を与えることとした。

b. 機微情報度

一般的に機微情報(センシティブ情報)とは、思想・信条や社会的差別の原因となる個人的な情報など、JIS Q 15001 で収集禁止の個人情報として定義されるような一部の情報に限定されることが多い。しかしこれら以外の情報でも精神的苦痛を感じる場合がある。本算出式では個人情報全体に対して 3 段階のレベルを設定し、その値からセンシティブの度合いを算定できるよう定義した。また経済的損害を被る情報についても機微情報度の算出式に含めた。

機微情報度は、対象となる情報のシンプル EP 図上の（x, y）の位置（=レベル値）を下記の式に代入して求める。

$$\text{機微情報度} = (10^{x-1}+5^{y-1})$$

漏えい情報が複数種類ある場合は、全情報のうちで最も大きな x の値と最も大きな y の値を採用する。例えば「氏名、住所、生年月日、性別、電話番号、病名、口座番号」が漏えいした場合、シンプル EP 図上の（x, y）は以下のようになる。

$$\text{「氏名、住所、生年月日、性別、電話番号」} = (1,1)$$
$$\text{「病名」} = (2,1)$$
$$\text{「口座番号」} = (1,3)$$

この例で最も大きい x 値は病名の“2”であり、最も大きい y 値は口座番号の“3”である。これらの値を前述の数式に当てはめると以下のようになる。

$$(10^{2-1}+5^{3-1}) = (10^{1}+5^{2}) = 35\text{ポイント}$$

c. 本人特定容易度

本人特定容易度は、漏えいした個人情報からの本人特定のし易さを表すものである。例えば銀行の口座番号が単独で漏えいしても、氏名などの本人を特定する情報が伴わなければ実被害に結び付きにくいことから、本人特定容易

度を本算出式に含めた。本人特定容易度は、以下の表 5-1 に示す判定基準を適用する。

表 5-1：本人特定容易度 判定基準

判定基準	本人特定容易度
個人を簡単に特定可能。 「氏名」「住所」が含まれること。	6
コストをかければ個人が特定できる。 「氏名」または「住所 ＋ 電話番号」が含まれること。	3
特定困難。上記以外。	1

(2) 情報漏えい元組織の社会的責任度

社会的責任度は表 5-2 に示すように、「一般より高い」と「一般的」の 2 つから選択する。社会的責任度が一般より高い組織は、「個人情報の保護に関する基本方針(平成 16 年 4 月 2 日 閣議決定)」に「適正な取り扱いを確保すべき個別分野」として挙げられている業種を基準とし、そこへ政府機関など公的機関と知名度の高い大企業を含めることとした。

表 5-2：情報漏えい元組織の社会的責任度 判定基準

判定基準		社会的責任度
一般より高い	個人情報の適正な取り扱いを確保すべき個別分野の業種（医療、金融・信用、情報通信など）、及び公的機関、知名度の高い大企業。	2
一般的	その他一般的な企業、及び団体、組織	1

(3) 事後対応評価

表 5-3 に基づいて、事後対応の評価値を求める。事後対応が「不明、その他」の場合、不適切な事後対応が露見しなかったと考え、適切な対応が行われた場合と同じ値とした。

表 5-3：事後対応評価 判定基準

判定基準	事後対応評価
適切な対応	1
不適切な対応	2
不明、その他	1

事後対応を評価する明確な基準がないため、過去の情報漏えいインシデントにおける事後対応行動を参考に作成した表 5-4 の対応行動例にあてはめて、事後対応の適切／不適切を判断する。

表 5-4：事後対応 行動例

適切な対応行動例	不適切な対応行動例
すばやい対応	指摘されても放置したままである
被害状況の把握	対応が遅い
インシデントの公表	繰り返し発生させている
状況の逐次公開(ホームページ、メール、文書)	対策を施したが、有効でない
被害者に対する事実周知、謝罪	虚偽報告
被害者に対する謝罪(金券の進呈を含む)	
顧客に与えるであろう影響の予測	
クレーム窓口の設置	
漏えい情報回収の努力	
通報者への通報のお礼と顛末の報告	
顧客に対する補償	
経営者の参加による体制の整備	
原因の追究	
セキュリティ対策の改善	
各種手順の見直し	
専門家による適合性の見直し	
外部専門家の参加による助言や監査の実施	

5.2.3　想定損害賠償額算出式

以上の定量化した「漏えい個人情報価値」、「情報漏えい元組織の社会的責任度」、「事後対応評価」の値を以下の算定式に代入することによって、想定損害賠償額が算出できる。算出式の全体像を図 5-4 に示す。

想定損害賠償額 ＝ 漏えい個人情報価値
× 情報漏えい元組織の社会的責任度
× 事後対応評価

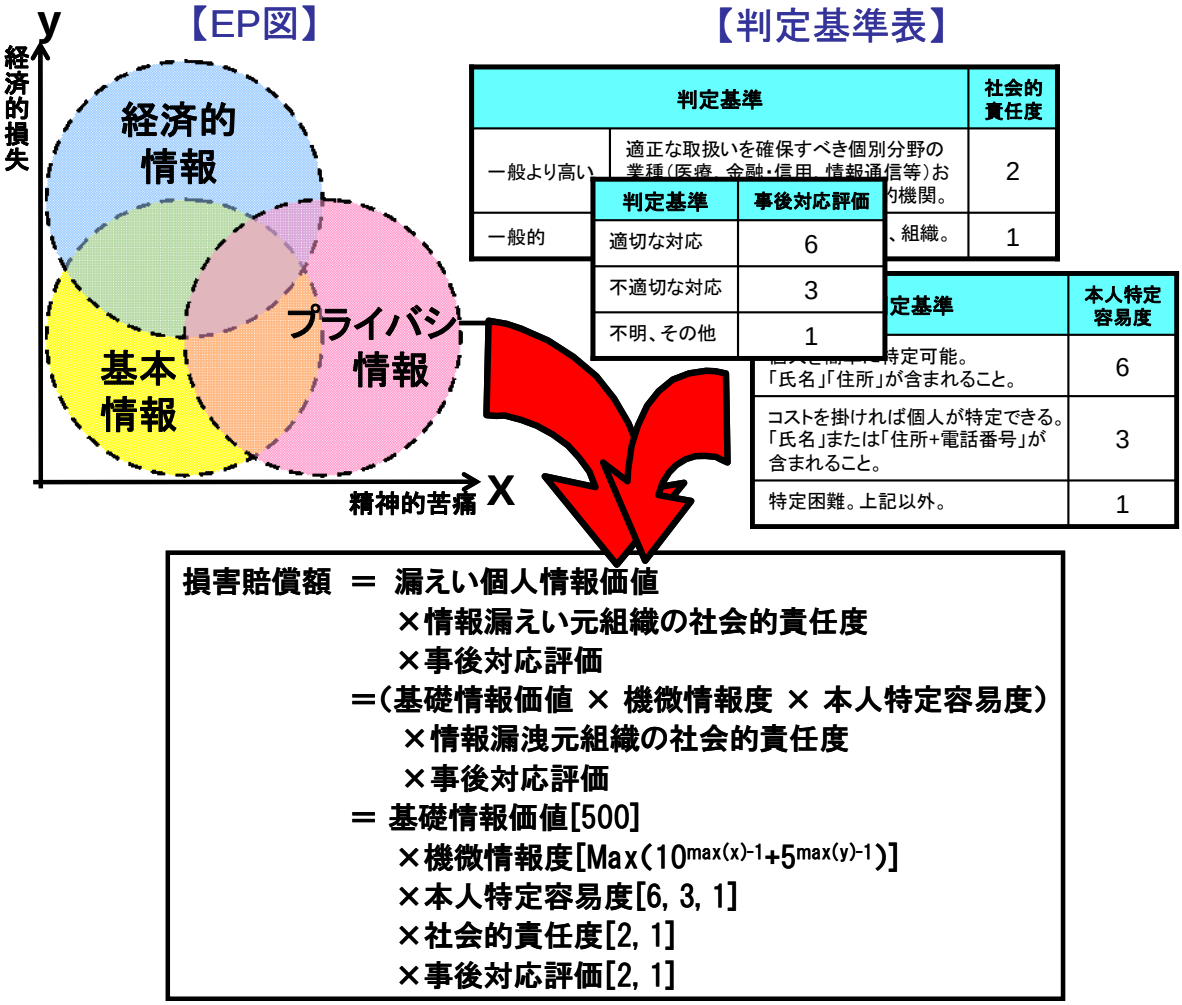

図 5-4：JO モデル

上記の想定損害賠償額算出式を、当ワーキンググループでは JO モデル（JNSA Damage Operation Model for Individual Information Leak）と名付けた。

6　最後に

これまで、漏えい人数が 100 人未満、10 人未満のインシデントは、公表されないことが多かった。近年は、小規模なインシデントであっても積極的に公表する組織が現れている。この小規模なインシデントの公表数が増加してきたことにより、分析結果が変化してきている。そこで、2010 年の調査結果から、以下のインシデントの規模と公表率の関係を考察した。

6.1　推定公表率について

一般的に、小規模な個人情報を取り扱う業務より、大規模な個人情報を取り扱う業務の方が、直接、人間が情報を取り扱う作業の頻度が少ないと考えられる。これは、そもそも大規模な個人情報ほど保有する組織が少なくなることや、その場合、組織がリスク低減のために、なるべく一度に大量の個人情報を取り扱わないように努力することなどによるものと考えられる。

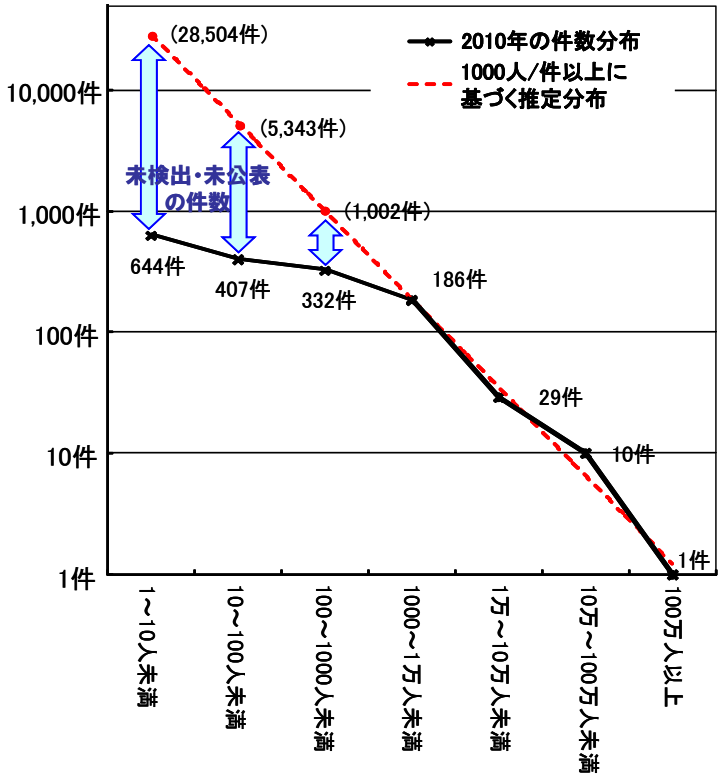

図 6-1：漏えい規模別のインシデント件数の分布（対数）

図 6-1 は、漏えい規模別に、インシデント件数を対数グラフで表したものである。当然、漏えい規模が大きいほど、インシデント件数は少ない。ただし、「1000 人～1 万人未満」を境界に、漏えい規模が小さいインシデントの減少率が鈍化して

いる。1000 人未満のインシデント件数は、実際のインシデント件数と公表されたインシデント件数が乖離している可能性がある。

そこで、2010 年に収集した小規模なインシデントの件数は、全ての小規模なインシデントの一部であると仮定し、図 6-1 の赤い点線に示す個人情報漏えいインシデントの件数の分布を推定した。この推定分布は、以下の考え方に基づいて導き出した。

1. ある自治体 A は、小規模なインシデントから大規模なインシデントまで、ありのままを公表している。自治体 A のみのインシデントの分布を分析した
2. 漏えい人数が 1000～1 万人/件以上のインシデントは、ほぼ隠さず公表されていると思われる。1000～1 万人/件以上のインシデントの分布を分析した。
3. 自治体 A のみのインシデントの分布と 1 万人/件以上のインシデントの分布が相似であることから、2 つの分布をもとに、個人情報漏えいインシデント全体の件数の分布（図 6-1 の赤い点線）を推定した。

実際の公表件数と推定した件数、推定公表率の関係を表 6-1 に示す。

表 6-1:漏えい規模別のインシデント件数

人数	公表件数	推定件数	推定公表率
1～10 人未満	644 件	28,504 件	2.3%
10 人～100 人未満	407 件	5,343 件	7.6%
100 人～1000 人未満	332 件	1,002 件	33.1%
1000 人～1 万人未満	186 件	（186 件）	（100%）
1 万人～10 万人未満	29 件	（29 件）	（100%）
10 万人～100 万人未満	10 件	（10 件）	（100%）
100 万人～	1 件	（1 件）	（100%）
合計	1,609 件	35,704 件	

注：推定件数のカッコ内の数字は、実際の件数である。
推定公表率のカッコ内の数字は、前提条件である。

この結果から、日本全体で発生しているインシデントの全件数は、3 万 5 千件を超えると推定される。平均すると、1 日に 98 件のインシデントが発生していると思われる。漏えい人数が 1 万人以上のインシデントが発生した場合は、ほとんどの組織で公表せざるを得ないが、1000 人未満のインシデントの場合は、公表しないことを選択する組織が増えてくるものと思われる。したがって、1000 人未満のインシデントの発生件数と公表件数に乖離が発生していると思われる。漏えい人数が

「1 人～10 人未満」のインシデントの公表率は、わずか 2.3%、「10 人～100 人未満」が 7.6%、「100 人～1000 人未満」が 33.1%である。

小規模なインシデントは、被害者へ個別対応できるため、その都度、公表する必要性は低い。よって、すべてのインシデントを公表すべきとは言えないが、漏えい人数が 100 人以上の場合は、連絡が付かない被害者がいる恐れがあるため、公表の可否を検討し、状況に応じて公表すべきである。また、人数が少ない場合であっても、すべての被害者に連絡が付かない場合は、メディアを利用して積極的に公表し、漏洩した情報が悪用される恐れなどを伝えることが望ましい。世間に対して説明責任を果たさなければならない場合や、公表によって類似インシデントの発生回避に役立つ場合も、公表することが望ましい。

各組織は、事前に公表の基準を設けること、公表しないインシデントであっても、きちんと報告させ、発生件数を把握するべきである。1 年間のインシデントの件数や、継続的な改善状況を情報セキュリティ報告書で報告すれば、組織のセキュリティに対する姿勢をアピールすることができる。

6.2　2010 年インシデントの特徴

2010 年は、政府関連の組織内部からの機密情報の漏えい事件が、相次いで大きく報道された。2010 年に発生した数万人分のクレジットカード情報が漏えいしたインシデントは、内部犯行であった。

このような悪意に基づくインシデントに立ち向かうには、どうしたらよいだろうか。内部から機密情報が漏えいする脅威には、システムによる対策だけでなく、組織面や運用面の対策と組み合わせなければ、効果がない。

まず、組織面や運用面においては、形骸化したルールではなく、誰でも順守できて効果があるルールを浸透させることである。例えば、セキュリティポリシーは組織全体が理解すべきセキュリティの方針であり、作業手順に組み込んで、実際の業務の安全性を向上できるような内容ではない。「お客様の情報は大事に扱いましょう」では、何をしたらよいのか、何をしてはいけないのか、わからない。また、業務を大きく阻害したり、大きな負担を強いるような内容も、実際の業務では遵守されない。現場の作業に合わせて、ルールを具体化して作業手順に組み込んでいれば、作業の実施と同時に、必ずその対策効果が発揮される。

システムによる対策は、具体化されたルールに合うように構築されていなければ、そもそも業務を実施したり、システムを運用することができない。外部へ送信する電子メールを暗号化するルールがあるのならば、暗号化機能があるメールソフトが備わったオフィス環境を提供し、サポートを充実させれば、システム面と運用面が組み合わさった効果的な対策となる。ルールだけでは対策できないケアレスミスも、ルールとシステム的な対策の組み合わせ（メールの暗号化の習慣化や平文メールの外部送信の拒否）により軽減される。

2010 年の個人情報漏えいインシデントの特徴は、以下の 3 点に整理できる。

【特徴 1】<u>業種別では、公務のインシデントがトップ</u>

昨年は「金融業、保険業」がトップであったが、2010 年は「公務」がインシデントの件数が 557 件で一番多かった。「公務」は過去 5 年で 3 回トップだったので、これ自体は大きな特徴とは言えない。ただし、「公務」の内訳を見てみると A 市が 203 件、B 市が 108 件と二つの自治体で過半数の件数を占めている。また、この二つの自治体のインシデント内容が、他の自治体と比較してセキュリティ対策に不備があったものとも考えられない。この二つの自治体は、公表することによる住民に対する説明責任を果たすとともに、同様な事故を起こさない抑止効果を狙っていると推測できる。実名は伏せるが、この二つの自治体の姿勢は称賛すべきことである。

【特徴 2】誤操作によるインシデントが増加

「誤操作」が原因によるインシデント件数が 2009 年の 24.0%から 2010 年は 32.3%と増加している。この「誤操作」は、封筒への封入ミスや FAX の誤送信などが多く 1 件当たりの個人情報の漏えい人数は、一人や二人などの少人数であることが多い。よって、件数では 32.3%であるが、漏えい人数では 0.7%と極端に少なくなっている。

【特徴 3】公表されたインシデント件数が最多で、漏えい人数が最少（※2005 年以降）

2008 年から 2010 年まで 3 年間この傾向が続いている。なおかつ、想定損害賠償額の総額も過去 6 年間で最少である。これは、日本という国の単位で考えると些細なインシデントも報告（公表）され、想定損害賠償額が大きくなるような価値の高い個人情報の漏えいが少なかったと言える。

6.3 まとめ

インシデントの分析はこれまでの章で説明されているため、ここでは、2010 年の分析結果を参考に考察してみたい。

(1) インシデントの公表について

2010 年のインシデント件数が一番多かった「公務」であるが、「2010 年インシデントの特徴」で書いたように、特定の自治体が多くの件数を公表していた。また、一人だけの個人情報の漏えいインシデントも 263 件と「公務」の 47%を占めていた。漏えいした個人情報の内容によっては、少人数の個人情報の漏えいであっても重大なインシデントになる可能性はあるので、すべてが小さなインシデントとは言えないし、小さなインシデントを公表する姿勢は評価に値する。

ただ、公表するための労力や経済性なども考えてみてはどうだろうか。数万人規模の組織の場合は軽微な漏えいインシデントが年に数百件以上になる場合もあるだろう。軽微なインシデントを都度公表するのではなく、情報セキュリティ報告書として年に一度公表するという方法も考えられる。

ここで、重要になるのが小さなインシデントと都度公表する必要がある大きなインシデントを区別する基準を組織が持つことである。決定した公表基準も情報セキュリティ報告書に記載すれば、組織の説明責任も果たせると考えられる。個人情報の漏えいインシデントを公表する件数の目安としては、本報告書の内容を読んで組

織として決定すれば構わないが、100 人から 1000 人の間で考えてみたらどうか。

インシデントの公表と漏えいした当事者に対する対応は、違うものであるから公表しない場合も、漏えいした当事者に対して素早く対応することは重要なことである。

(2) 誤操作の対策について

誤操作は、人が介在するため 100%事前に防ぐことは不可能に近いと考えられる。ただし、誤操作してしまった原因を分析することは重要である。例えば、BCC:で送信すべきところを、CC:で送信してしまった場合は、

① BCC:の使い方を知らなかった
② 複数の人にメールを送る時の規定がなかった
③ メールの規定はあったが、内容を知らなかった（または、周知していなかった）
④ BCC:で送ったつもりだったが、ミスして CC:で送ってしまった。

などの理由が考えられる。理由によって防止する対策が変わるので、重要な情報である。

また、個人情報を送付する場合は、電子データであれば暗号化して、万一誤送信しても内容を見えなくするなどの有効な対策がある。しかし、郵送や宅配便、FAX では、それができない。FAX でなければならない理由が無いならば、FAX に固執せずに、思い切って FAX 以外の代替手段へ切り替える判断も必要である。

7　お問い合わせ先

本報告書に関する引用・内容についてのご質問等は JNSA ウェブサイト上の引用連絡およびお問合せフォームからご連絡下さい。

※引用のご連絡に対する承諾通知はご返信しておりませんのでご了承下さい。

また報告書についての FAQ もございますので、引用・お問合せの際はご参照下さい。

http://www.jnsa.org/faq/incident.html

■お問い合わせフォーム

引用連絡および問合せフォーム

URL： https://www.jnsa.org/aboutus/quote.html