2013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 1.2 版

2014 年 12 月 25 日
2015 年　2 月 23 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

情報セキュリティ大学院大学
原田研究室 廣松研究室

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　損保ジャパン日本興亜リスクマネジメント株式会社
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
川上　昌俊　株式会社ラック
田中　洋　株式会社 インフォセック
広口　正之　リコージャパン株式会社
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

情報セキュリティ大学院大学
原田研究室
原田　要之助　教授
佐々木　崇裕　博士前期課程 2 年
福島　健二　博士前期課程 2 年
嶋作　泰洋　客員研究員
菅原　尚志　客員研究員
新原　功一　客員研究員
鈴木　宏幸　客員研究員
高梨　智治　客員研究員
根岸　秀忠　客員研究員
村上　靖　客員研究員
廣松研究室
廣松　毅　教授
情報セキュリティ大学院大学 修了生
小野　康史　2008 年度卒
高津　岳志　2006 年度卒

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、情報セキュリティ大学院大学 原田研究室、廣松研究室の協力をいただいて実施している。本調査もこれまでの調査方法を踏襲し、2013 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。インシデントの原因分析も含め、以下に 2013 年のインシデントの集計・分析結果、及び過去 9 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

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。

このことを踏まえ、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。

本報告書は、この目的のために、2013 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。

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 2013 年の個人情報漏えいインシデントの分析結果」「第 4 章 2013 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 2013 年の個人情報漏えいインシデントの分析結果」では、2013 年の単年データの分析結果、および蓄積された 12 年間分のデータから 2005 年から 2013 年までの 9 年間分のデータを用いた経年分析の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データの偏りが大きいため、分析対象から除外した。

「第 4 章 2013 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。掲載した損害賠償額に関する数値は、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、本編巻末に「インシデント一覧表」を収録した。

2.3 調査・分析方法

2013 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、JNSA の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　2013 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、1388 件（前年比 968 件減）であった。2012 年より大幅に減少している。近年は軽微な個人情報漏えいインシデントであっても公表するため、件数が多く、2008 年以降、2012 年を除いて 1500 件前後である。漏えい人数は、約 925 万人（前年比 46 万人減）と変化が少ない。2008 年以降、漏えい件数は多いが一件あたりの漏えい人数が 100 人未満の小規模なインシデントが占める割合が高いためである。想定損害賠償総額は、約 1,439 億円（前年比 694 億円減）となった。漏えい原因は、「誤操作」（485 件）が一番多く、「管理ミス」（449 件）、「紛失・置忘れ」（199 件）の 3 種類が大半を占めた。2013 年は、2012 年と比較して「管理ミス」の件数と割合が大きく減少した。2013 年は 100 万人以上の大規模なインシデントが発生し、かつ「情報通信業」の漏えい人数が突出して多い結果となった。

2013 年の集計結果の概要データは、以下の通りである。

表 3-1：2013 年 個人情報漏えいインシデント 概要データ

漏えい人数	**925 万 2305 人**
インシデント件数	**1388 件**
想定損害賠償総額	**1438 億 7184 万円**
一件あたりの漏えい人数※1	**7031 人**
一件あたり平均想定損害賠償額※1	**1 億 926 万円**
一人あたり平均想定損害賠償額※2	**2 万 7701 円**

※1：平均値は、被害者数が不明のインシデント 72 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。

2013 年は、一件あたりの漏えい人数が 100 万人を超える大規模なインシデントが 2 件発生した。インシデント・トップ 10 の原因は「不正アクセス」が多く、業種は「情報通信業」が多い。業種が「情報通信業」で、かつ原因が「不正アクセス」の場合のほとんどは、パスワードリスト攻撃による漏えいが原因であった。

表 3-2：インシデント・トップ 10

No.	漏えい人数	業種	原因
1	400 万人	情報通信業	不正アクセス
2	169 万 2496 人	情報通信業	不正アクセス
3	47 万人	卸売業，小売業	不正アクセス
4	42 万 6000 人	公務(他に分類されるものを除く)	紛失・置忘れ
5	24 万 3266 人	情報通信業	不正アクセス
6	17 万 5297 人	情報通信業	設定ミス
7	15 万 0165 人	卸売業，小売業	不正アクセス
8	12 万 0616 人	金融業，保険業	管理ミス
9	10 万 9112 人	情報通信業	不正アクセス
10	9 万 7438 人	情報通信業	不正アクセス

3.3 業種

(1) 単年分析(件数)

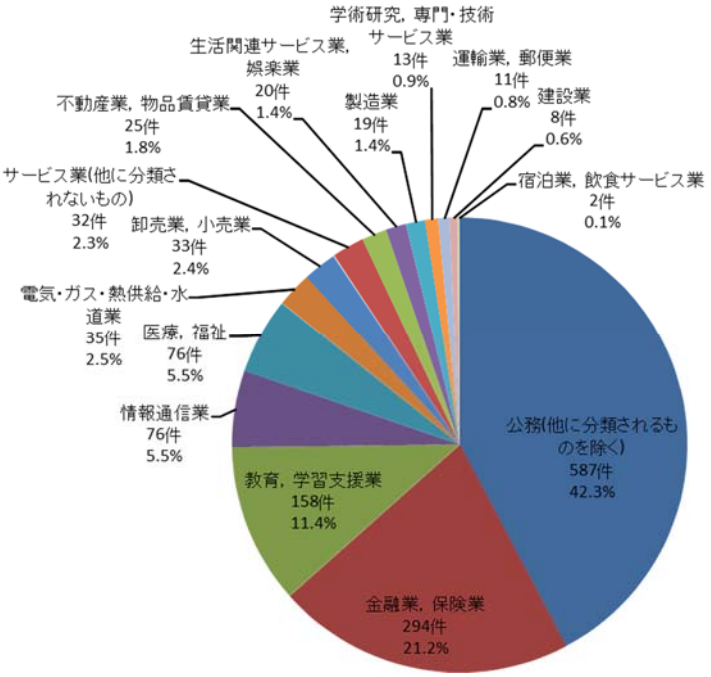

図 3-1：業種別比率（件数）

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」(42.3%)、「金融業，保険業」(21.2%)、「教育，学習支援業」(11.4 %)であり、全体の約 75%を占めている。

「公務」および「金融業，保険業」は 2004 年以降、「教育，学習支援業」「医療，福祉」は 2007 年以降、常に上位を占めている。これは、個人情報を取り扱うことが多いことに加え、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。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。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」からのインシデントの報告は稀であるが、それ以外はすべての業種で個人情報漏えいのインシデント報告がある。ほぼすべての業種において、個人情報を扱う限り、個人情報漏えいのインシデント発生のリスクがあると言える。

(2)　経年分析(件数)

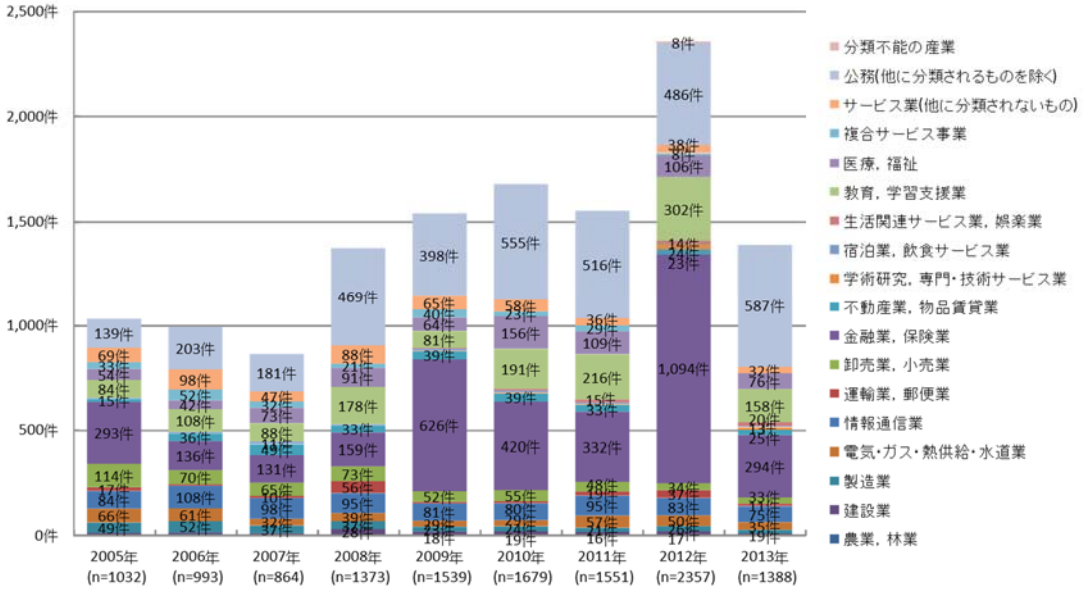

図 3-2：業種別件数の経年変化（件数）

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。2012 年に「金融業，保険業」のインシデント件数が大きく増加したが、2013 年は減少して例年通りの比率を占めている。インシデント件数が大きく増加した年は、そのタイミングで法律が変化したり行政の指導が行われたりなどの要因が働いたと思われる。「公務」は、2008 年以降、常に多くのインシデント件数を公表している。これは自治体が軽微なインシデントも積極的に外部へ公表しているためである。「教育，学習支援業」の件数も、2012 年よりは減少したが、3 番目に大きな比率となっている。「教育，学習支援業」も、インシデントを公表するようになってきたこと、校務で PC や USB メモリなどの使用が増加していることが原因と推定される。

(3)　単年分析（人数）

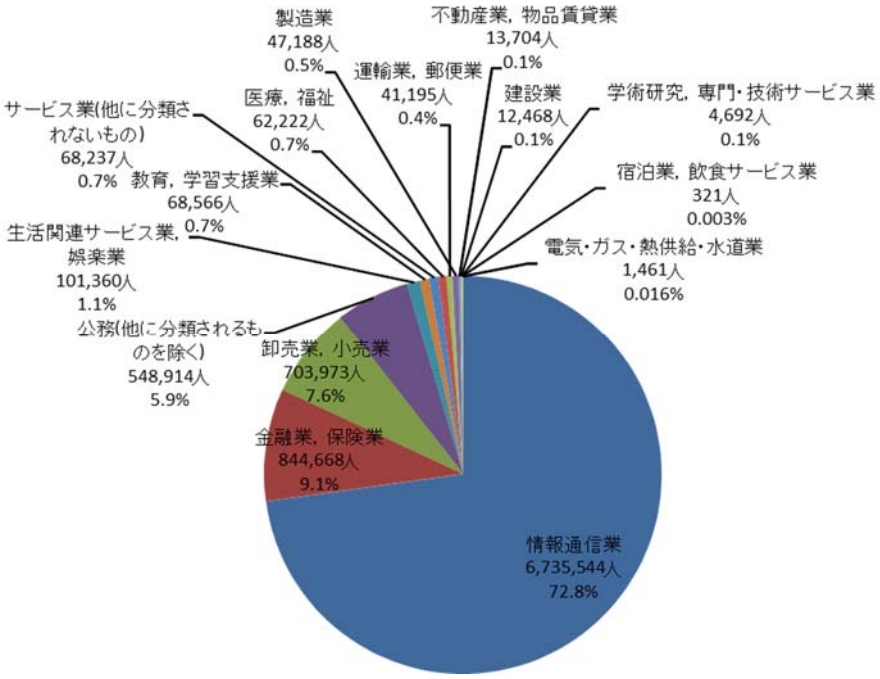

図 3-3：業種別比率（人数）

業種別での個人情報の漏えい人数の比率を図 3-3 に示す。上位から順に「情報通信業」(72.8%)、「金融業，保険業」(9.1%)、「卸売業，小売業」(7.6%)である。図 3-1 の件数比率のグラフでは、「公務」と「教育，学習支援業」の割合は合わせて 53.7%を占めたが、図 3-3 の人数比率のグラフでは 6.6%と少ない。これは、「公務」が扱う個人情報は住民票の交付など 1 人単位、「教育，学習支援業」の扱う個人情報はクラス単位で、一度に扱う個人情報の数が少ない。そのため、他の業種のインシデントと比較して、1 回のインシデントで漏えいする個人情報の数が少ないためである。

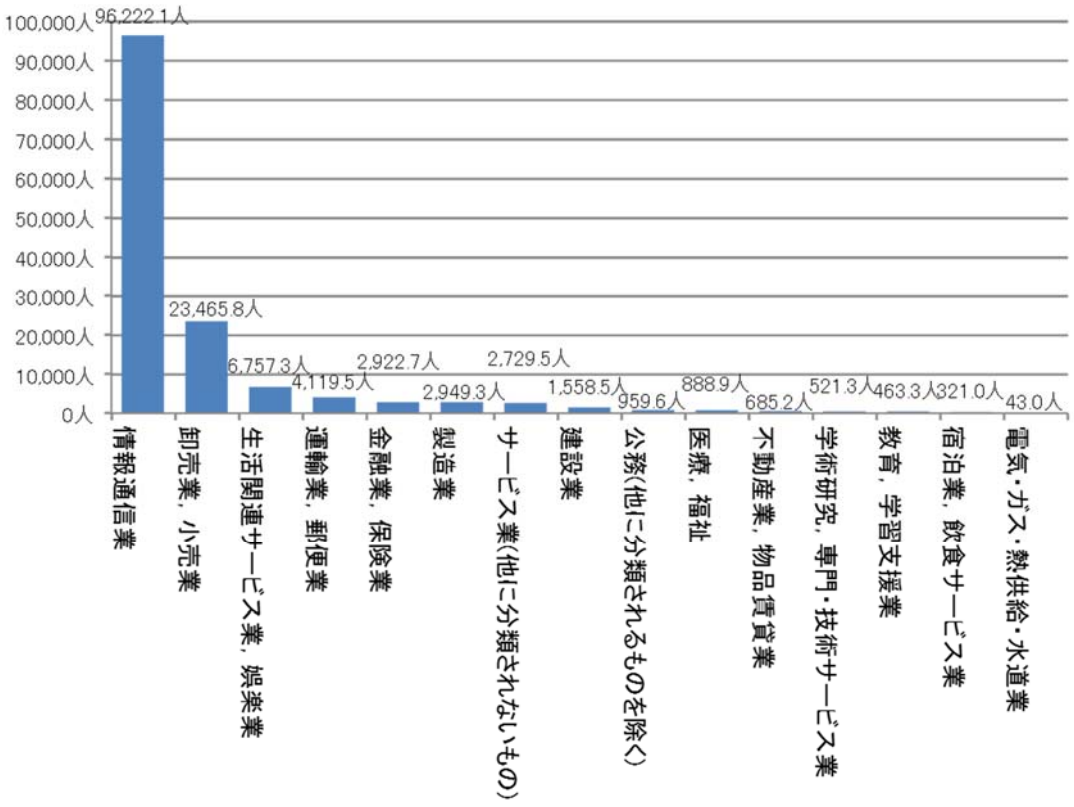

図 3-4：業種別の一件あたりの平均漏えい人数

インシデント一件あたりの漏えい人数（平均人数）を図 3-4 に示す。「情報通信業」（96,222 人）が突出しているが、これはインシデント・トップ 10（表 3-2 参照）のうち 1 位、2 位はじめ 6 件が情報通信業であり、これが情報通信業の平均漏えい人数を押し上げたためである。これにつづく上位の業種は「卸売業、小売業」（23,467 人）、「生活関連サービス業、娯楽業」（6,757 人）である。インシデントの件数が上位の「公務」は 960 人、「金融、保険業」は 2,923 人だった。「公務」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 587 件のうち、437 件は紙媒体の誤交付・誤送付による 10 人未満の小規模インシデントであった。

(4)　箱髭図(人数)

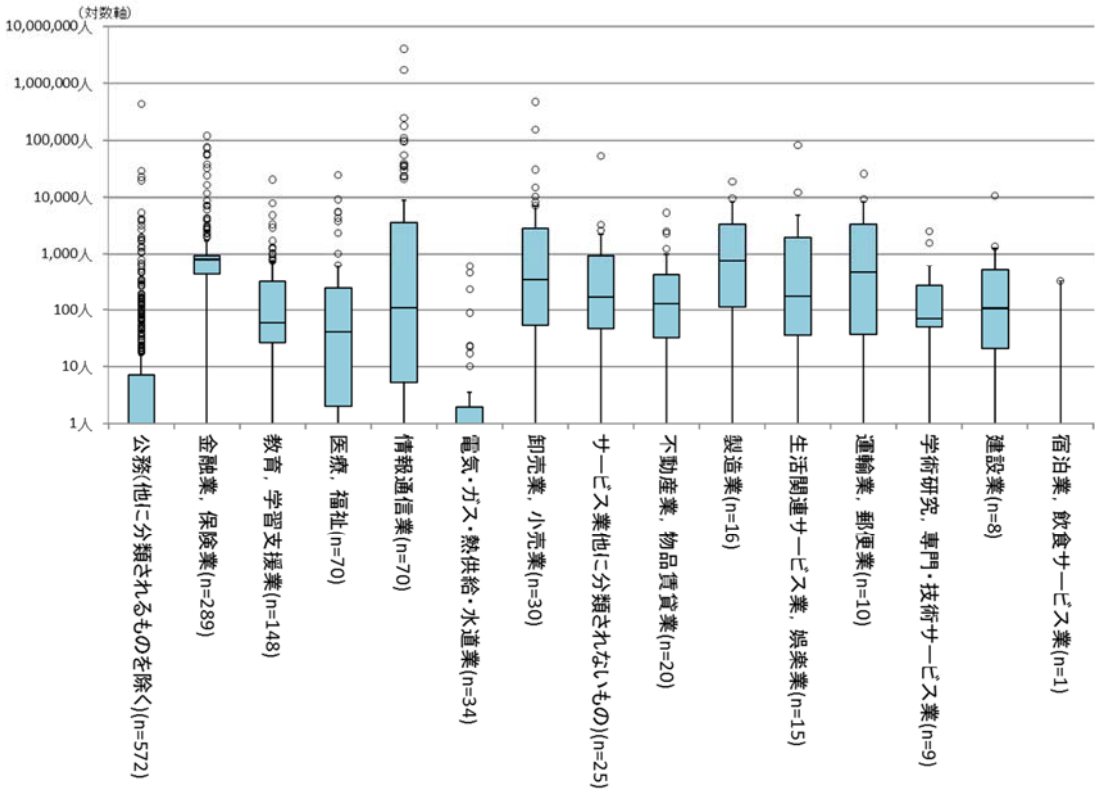

図 3-5：業種別の漏えい人数（箱髭図）

業種別のインシデント一件あたりの漏えい人数の箱髭図[1]を図 3-5 に示す。箱髭図を用いた表現は平均値とは異なり、分布を知ることができる。「公務」「電気・ガス・熱供給・水道業」は、箱髭図の長方形の部分（以下、「箱」という。）が 1 人から 10 人程度である。これはこの業種で発生した個人情報漏えいインシデントのほとんどが 1～10 人の小規模なインシデントであることを示している。一方「金融業，保険業」は、箱の位置が他の業種と比較して特に 1000 人に近いところに集中していることがわかる。またいくつかの業種において、漏えい人数が 1 万人以上の外れ値（丸印）が発生している。このことから、どの業種においても大量の個人情報を取り扱っていれば、まれにそれが漏えいする恐れを考慮しなければならない。

[1] 箱髭図の長方形の下辺は第 1 四分位数、中央の線は中央値、上辺は第 3 四分位数である。長方形の上辺から伸びる線の先端は「第 3 四分位数＋1.5×IQR」で、これより大きいデータは外れ値として 1 個ずつ点記号で表示される。IQR は、第 3 四分位数と第 1 四分位数の差である。「第 1 四分位数－1.5×IQR」より小さいデータと「第 3 四分位数＋1.5×IQR」より大きいデータは外れ値である。

(5)　経年分析(人数)

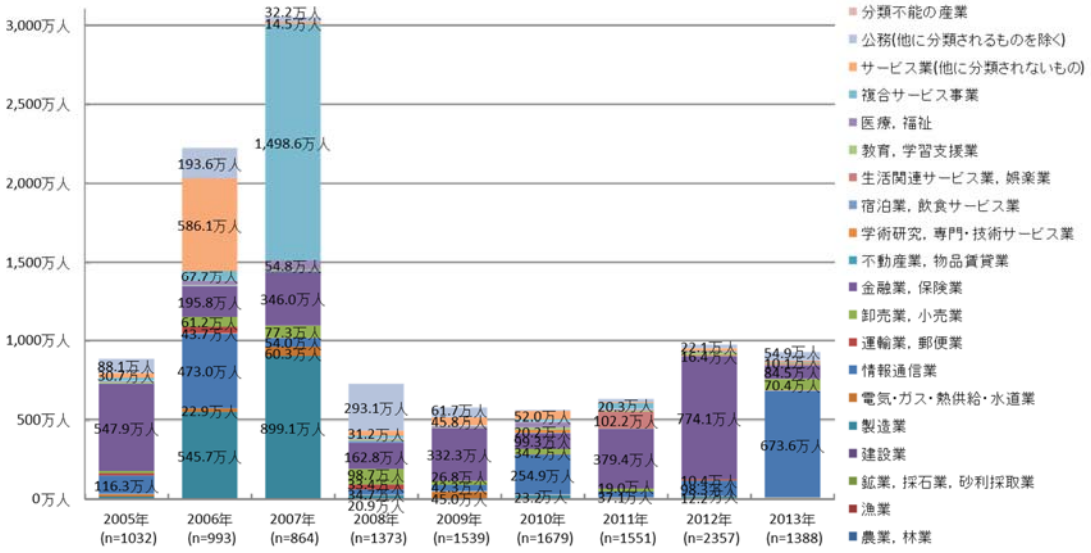

図 3-6：業種別漏えい人数の経年変化（合計）

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 年に情報通信業で、2007 年に複合サービス業で 100 万人以上の大規模なインシデントが多く発生した。そのため 2006 年と 2007 年は、漏えい人数が他の年よりも突出したグラフになっている。2013 年は「情報通信業」の漏えい人数が他業種より突出している。これは情報通信業を中心にパスワードリスト攻撃が多く発生し、大量の個人情報が漏えいしたためである。

(6)　相関分析

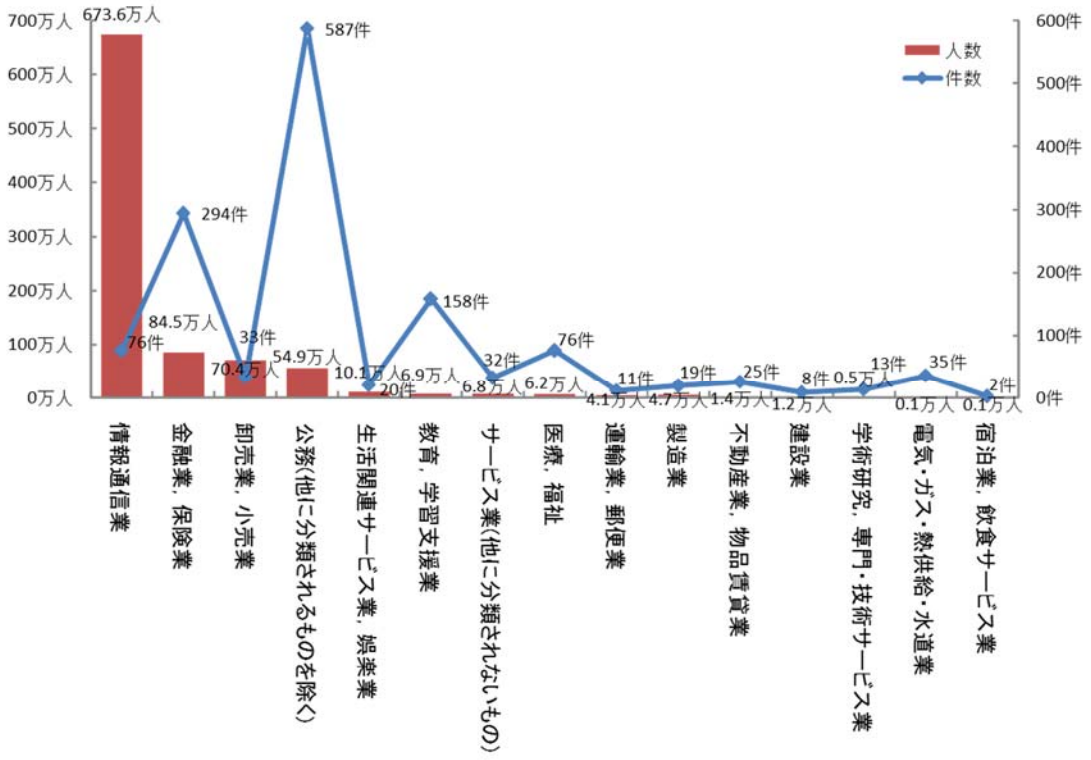

図 3-7：業種別のインシデント件数と漏えい人数

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。「情報通信業」のインシデント件数は少ないが、漏えい人数は最も多い。「公務」はインシデント件数が最も多いが、漏えい人数は上位から 4 番目である。これは、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反して漏えい人数の合計が少ない。

3.4 原因

(1) 単年分析(件数)

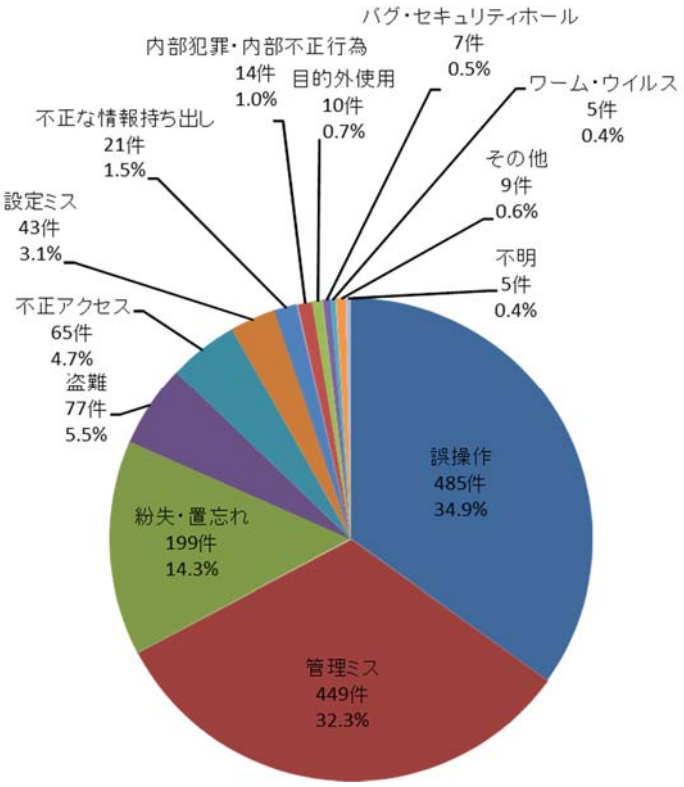

図 3-8：漏えい原因比率（件数）

個人情報漏えい件数の原因比率を図 3-8 に示す。2013 年は「誤操作」「管理ミス」「紛失・置忘れ」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、発見の遅れやインシデントに至る経緯が明確にならない場合が多い。

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、経緯も明確になりやすい場合が多い。発見の遅れや経緯が不明確なインシデントは被害を大きくする傾向にある。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効果が期待できる手順づく

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に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組み合わせるとより効果的である。

(2) 経年分析(件数)

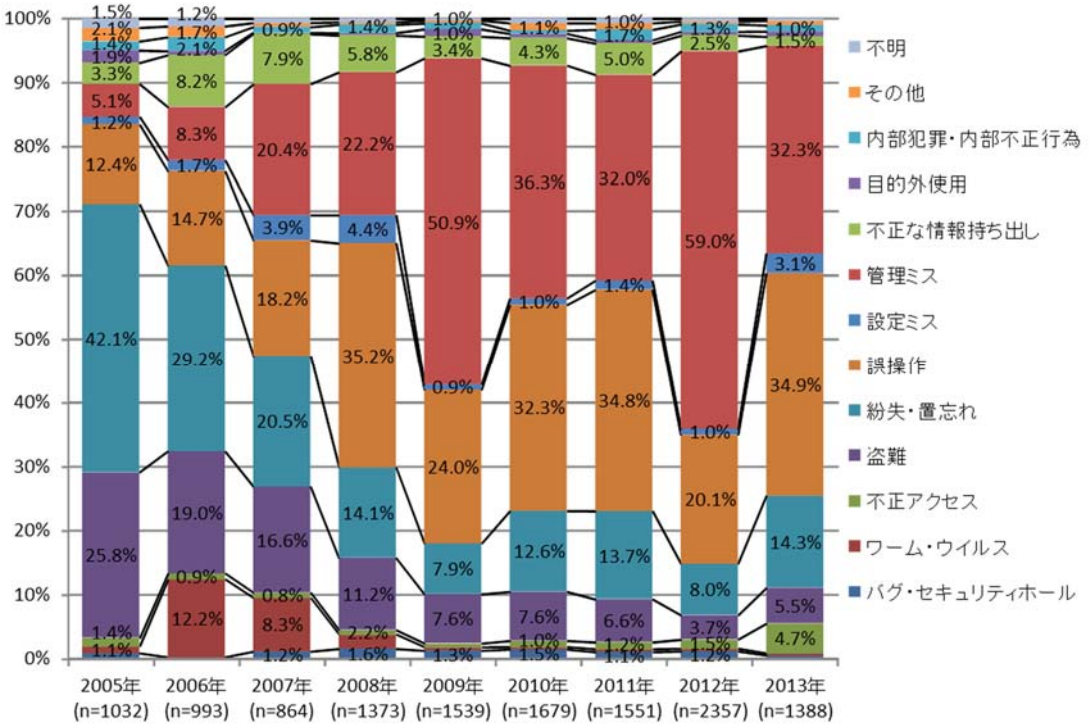

図 3-9：漏えい原因比率の経年変化（件数）

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。2011 年の 34.8%(539 件)から 2012 年に 20.1%(474 件)と減少した「誤操作」は、件数はほぼ横ばいだが、34.9%(485 件)と比率が増加している。一方で「誤操作」の増加により、「管理ミス」の比率は 2012 年の 59.0%(1391 件)から 32.3%(449 件)へ大きく減少している。

「管理ミス」及び「誤操作」、「紛失・置忘れ」はヒューマンエラーである。これらの増加は、個人情報を取り扱う担当者の意識低下と結びつけることもできる。今後も注視すべき点である。

なお、2009 年以降、「誤操作」「管理ミス」「紛失・置忘れ」が上位を占める傾向が続いている。

(3)　単年分析(人数)

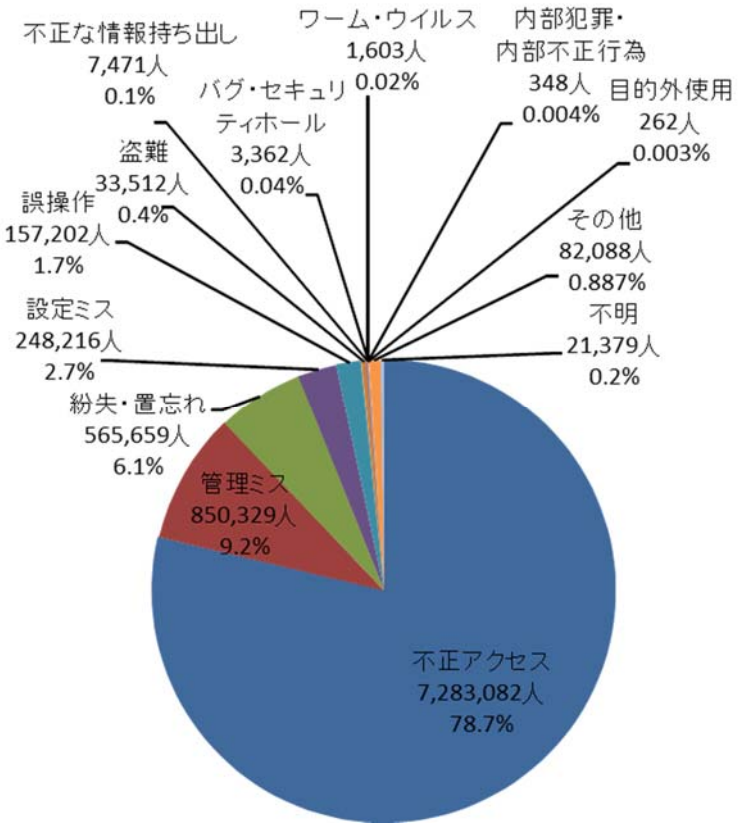

図 3-10：漏えい原因比率（人数）

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図 3-10 と前述した漏えい件数の原因比率である図 3-8 を比べると、傾向に若干の違いが見られる。図 3-8 のように件数で集計すると、「誤操作」「管理ミス」「紛失・置忘れ」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、第 2 位以下は「管理ミス」「紛失・置忘れ」など同様の原因となっている一方、「不正アクセス」が突出している。

「不正アクセス」は例年、一件あたりの被害が大きくなる傾向があり、それは 2013 年も同様であった。「管理ミス」に関しては、悪意がない原因にもかかわらず、件数とともに漏えい人数も多い。ここでも「管理ミス」への対策が重要であることが読み取れる。

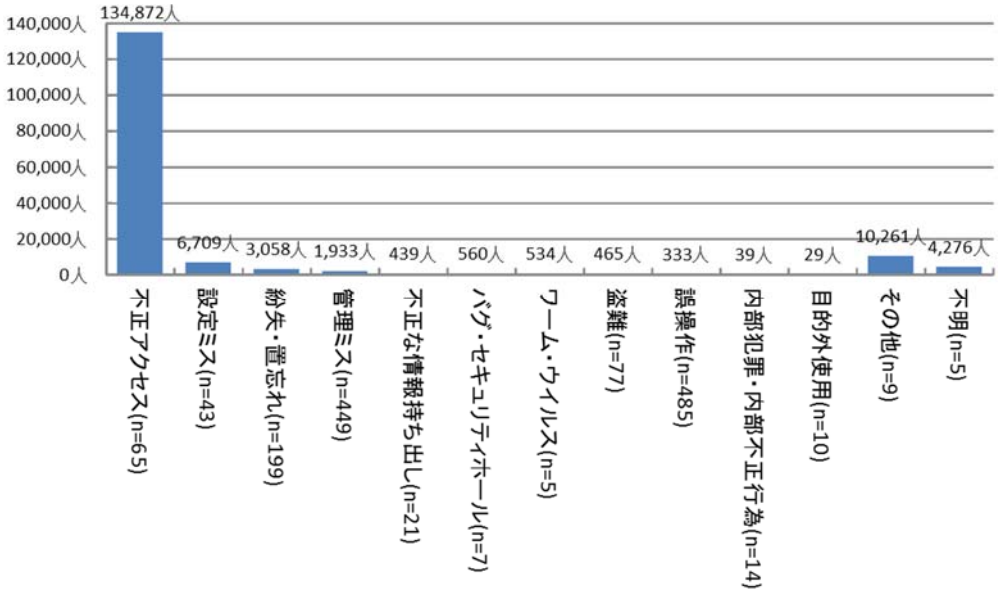

図 3-11：漏えい原因別の一件あたりの漏えい人数

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 では、「不正アクセス」「設定ミス」の一件あたりの漏えい人数が目立つ。

「不正アクセス」「設定ミス」の一件あたりの漏えい人数が多い要因は、インシデントの発生件数が少ないにも関わらず、インシデント・トップ 10 の上位に入るような規模のインシデントが発生しているためである。「不正アクセス」は、悪意のある者が個人情報の集積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件数が漏えいしていると推測される。

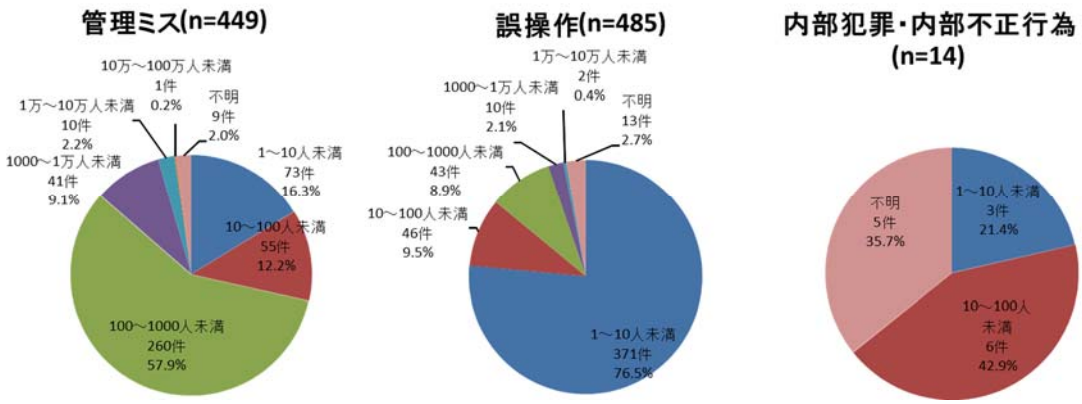

図 3-12：漏えい原因の人数区分（件数）

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。漏えい件数が第 1 位の「誤操作」は、10 人未満の情報漏えいインシデントが約 80%も占めており、1 件あたりの漏えい人数が少ないインシデントが目立つ。

一方、漏えい件数と人数ともに第 2 位の「管理ミス」は 100～1000 人未満の情報漏えいインシデントが多いが、大規模なインシデントもいくつも発生している。大量の個人情報を扱っている組織は、「管理ミス」によって大規模なインシデントが発生する恐れも考慮しなければならない。

「内部犯罪・内部不正行為」は、10～100 人未満の規模のインシデントが多い。「管理ミス」や「誤操作」に比べて、一件あたりの漏えい人数が多い。

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、被害が大きくなる傾向がある「内部犯罪・内部不正行為」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)　箱髭図(人数)

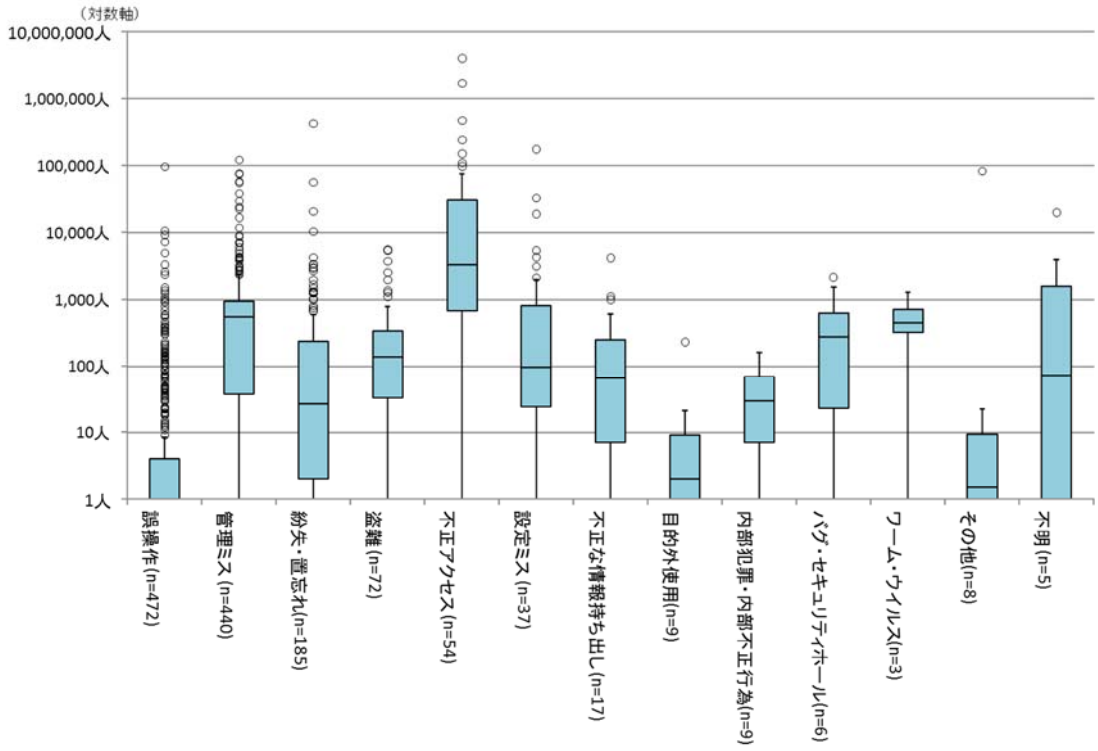

図 3-13：漏えい原因の漏えい人数（箱髭図）

漏えい原因別のインシデント一件あたりの漏えい人数の箱髭図を図 3-13 に示す。他の原因と比べて、「不正アクセス」「設定ミス」は、漏えい人数が大きな範囲にわたって分布している傾向にある。また、「紛失・置忘れ」「管理ミス」「誤操作」は、外れ値が広く分布している。特に「誤操作」は、数人規模のインシデントが多く発生している一方、10 万人規模のインシデントも発生するなど、漏えい人数が広く分布している。

(5)　業種別（件数）

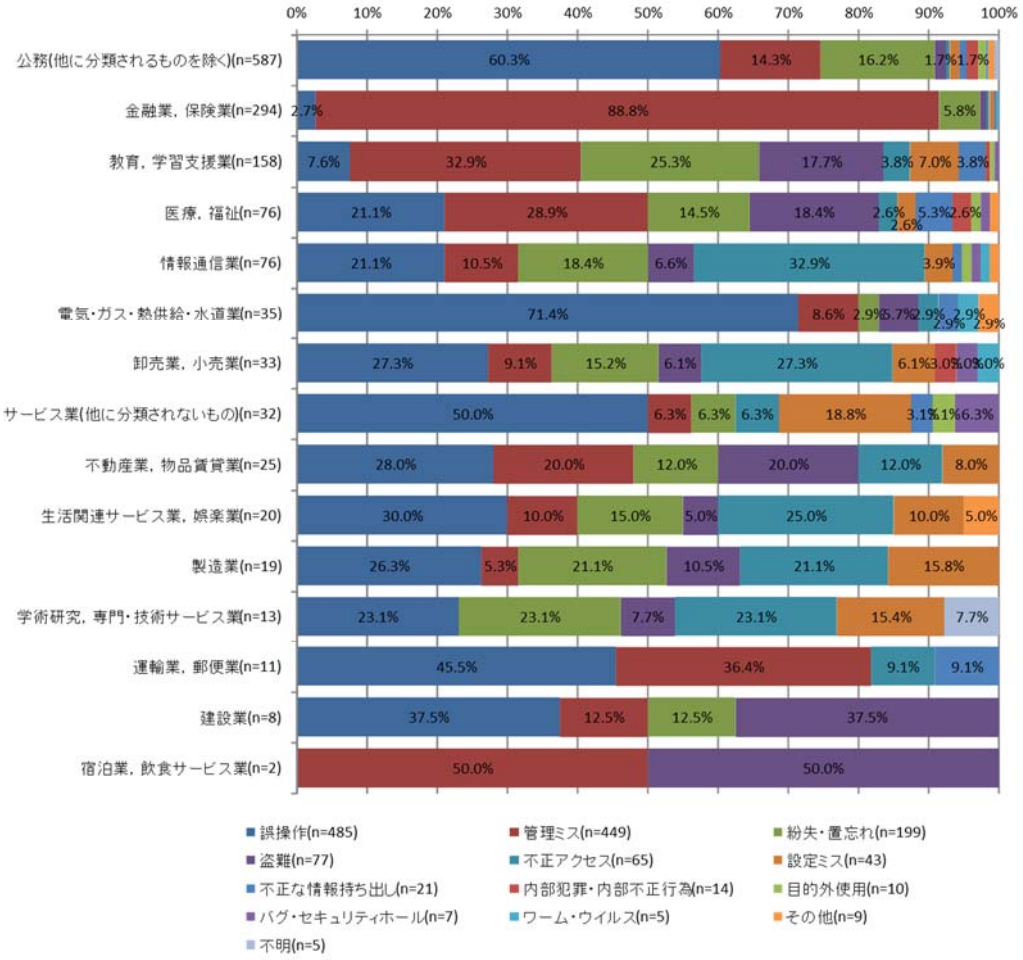

図 3-14：業種別の漏えい原因比率（件数）

業種別の漏えい原因比率を図 3-14 に示す。「金融業，保険業」は、「管理ミス」の占める比率が高く約 60%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、紛失や誤廃棄が判明したというケースが多い。

「公務」は、「誤操作」の占める比率が高く、公表された件数は 354 件となっている。2013 年の「誤操作」の全件数は 485 件であるため「誤操作」の約 73%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、日常業務の中で個人情報を送付するという作業が多いことに起因していると推測される。

「情報通信業」は、「不正な情報持ち出し」の比率が約 33%と、他の業種に比べて高い。件数は 25 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」が最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の実態がかい離し、形骸化している可能性もある。

3.5　漏えい媒体・経路

(1)　単年分析(件数)

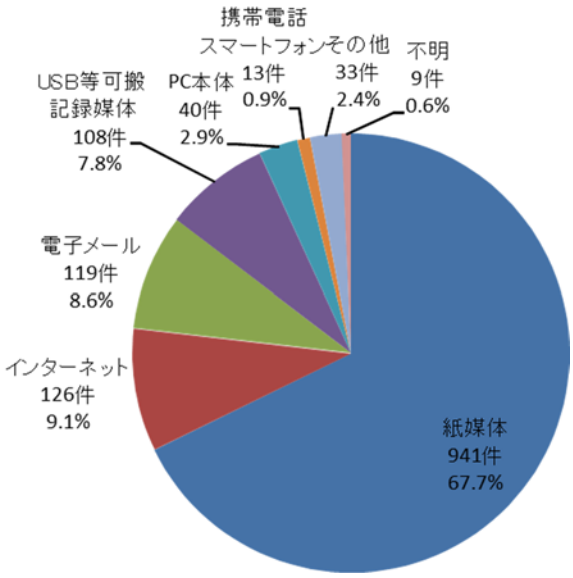

図 3-15：漏えい媒体・経路（件数）

漏えい媒体・経路別のインシデント件数を図 3-15 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 67.7%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。次に「インターネット」が 9.1%、「電子メール」が 8.6%を占める。

(2)　経年分析(件数)

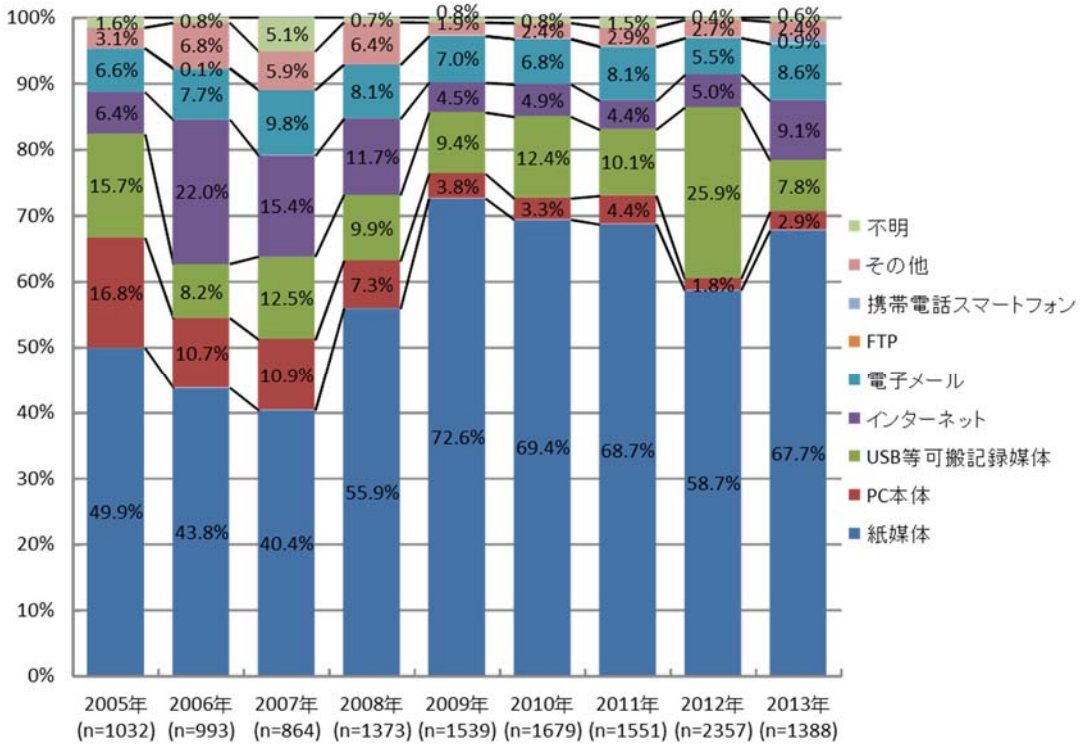

図 3-16：漏えい経路比率の経年変化（件数）

漏えい経路比率の経年変化について図 3-16 に示す。「紙媒体」による漏えい件数は、例年通りもっとも高い割合となっている。「紙媒体」は、2009 年以降、減少傾向にあったが、2013 年は 2012 年に比較し増加した。「紙媒体」の次に高い割合となったのは「インターネット」で、2009 年以降毎年 4%強～5%であったのに 2013 年度は 9.1%に増加した。2012 年は「USB 等可搬記録媒体」経由の漏えい件数割合が高かったが、2013 年は 2011 年以前の水準に戻った。

2014 年に割合が高かった「インターネット」経由の漏えい原因を見ると「不正アクセス」が約 48%で最も高く、2012 年の同約 29%と比較し約 1.7 倍に増加している。「不正アクセス」の割合が高くなった要因はパスワードリスト攻撃が増加したことが影響していると考えられる。

(3)　単年分析(人数)

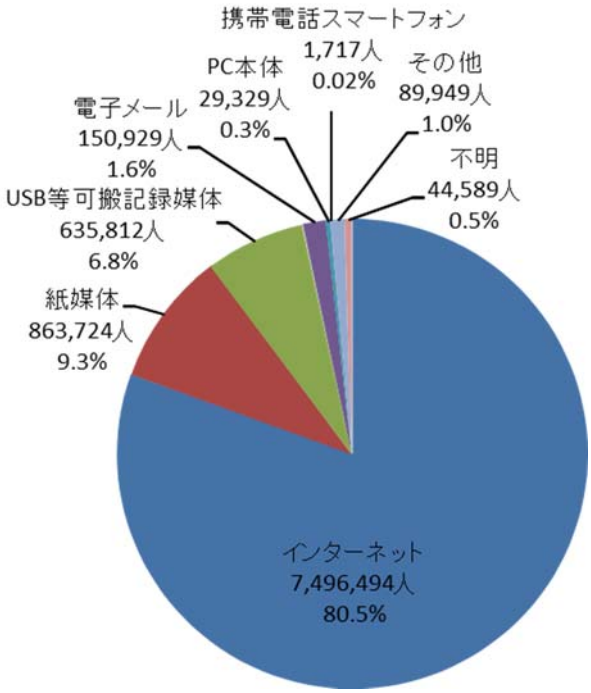

図 3-17：漏えい媒体・経路（人数）

漏えい媒体・経路別の漏えい人数を図 3-17 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 80.5%を占める。「表 3-2：インシデント・トップ 10」のうち、第 1 位～第 3 位、第 5 位～第 7 位、第 9 位、第 10 位の 8 件が「インターネット」であった。この 8 件のインシデントでは合計約 690 万人の被害となる。

2012 年に最も人数の多かった「USB 等可搬記憶媒体」が、2013 年は 6.8%で 3 番目であった。

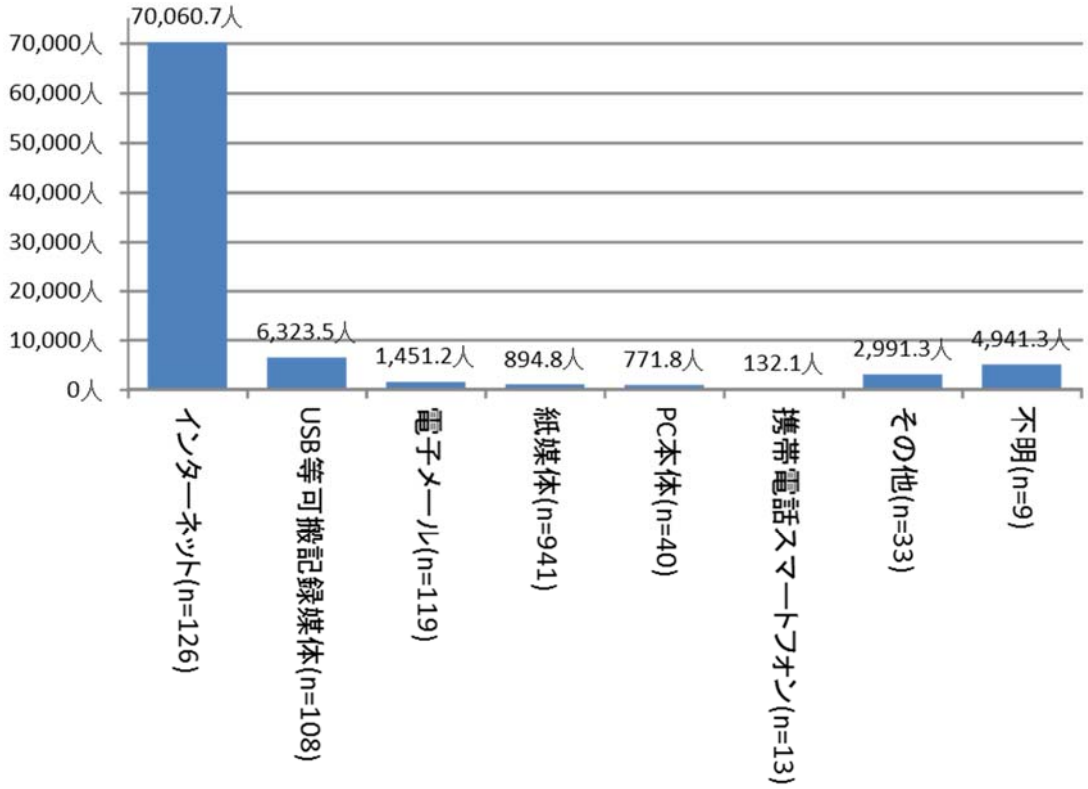

図 3-18：漏えい媒体・経路別の一件あたりの漏えい人数

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 3-18 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」が突出して多い。「インターネット」経由の漏えいの内、漏えい人数が大きい順の上位 5 件の漏えい原因は「不正アクセス」で、その 5 件の内 4 件がメールアドレスと、ID/PASSWD が窃取されている。この 5 件はパスワードリスト攻撃を受けた可能性が高く、盗まれたメールアドレス、ID/PASSWD は、別のパスワードリスト攻撃に利用されたり、なりすましによる詐欺に利用されたりといった二次被害に結び付いた可能性がある。

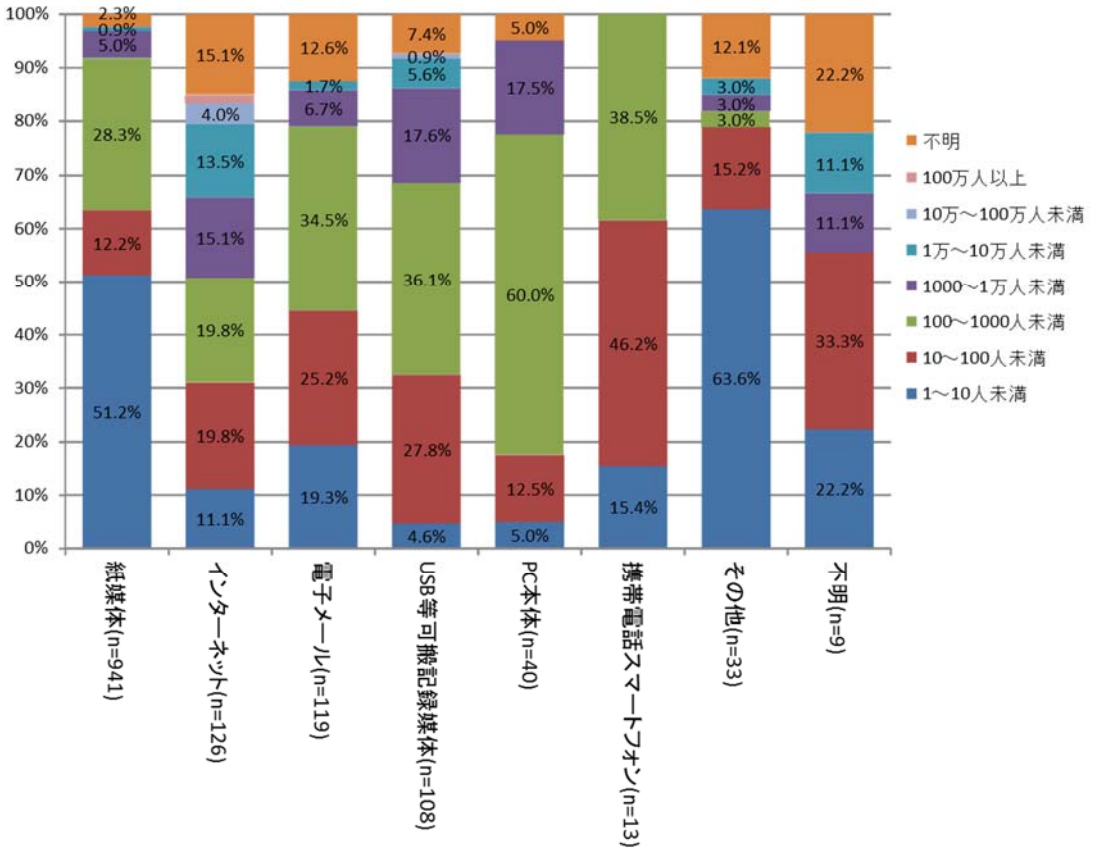

図 3-19：漏えい規模比率(件数)

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 3-19 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 90%以上を占め、とくに 1~10 人未満の小規模なインシデントの比率が約 51%と最も高い。「電子メール」「USB 等可搬記録媒体」「PC 本体」「携帯電話スマートフォン」も漏えい規模が 1000 人未満のインシデントの比率が高いが、その内訳は異なり、1000 人未満に限っては 1 人以上～10 人未満の比率が低く、10 人以上～1000 人未満の比率が高くなっている。

一方「インターネット」によるインシデントは、1000 人未満のインシデント比率が約 50%未満と他と比べ比較的低く、大規模のインシデントの比率が高い。

(4) 箱髭図(人数)

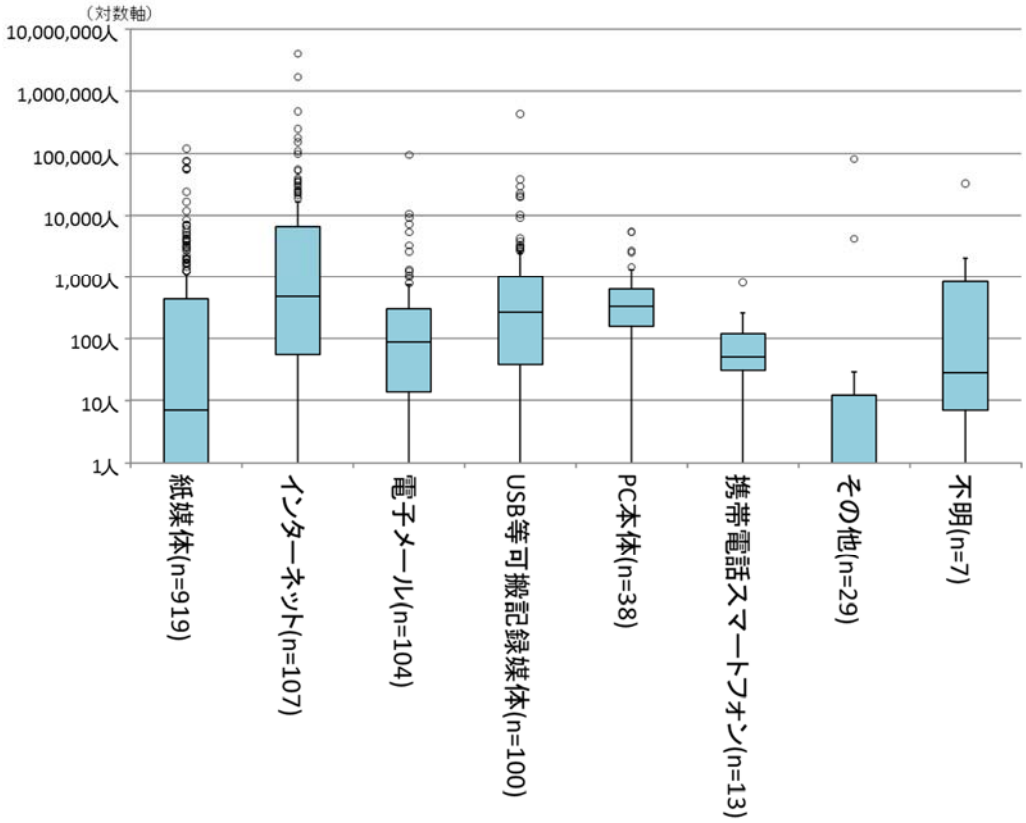

図 3-20：漏えい経路の漏えい人数（箱髭図）

漏えい経路別のインシデント一件あたりの漏えい人数の箱髭図を図 3-20 に示す。2013 年にインシデント件数が増加した「インターネット」経由の漏えいは、人数の分布が他の漏えい経路と比べて、若干漏えい人数が多い傾向を示している。「紙媒体」のインシデントは、その他を除いた他の経路によるインシデントと比べて、漏えい人数が 1 人から 1000 人未満の範囲に渡って広く分布している。

(5)　業種別（件数）

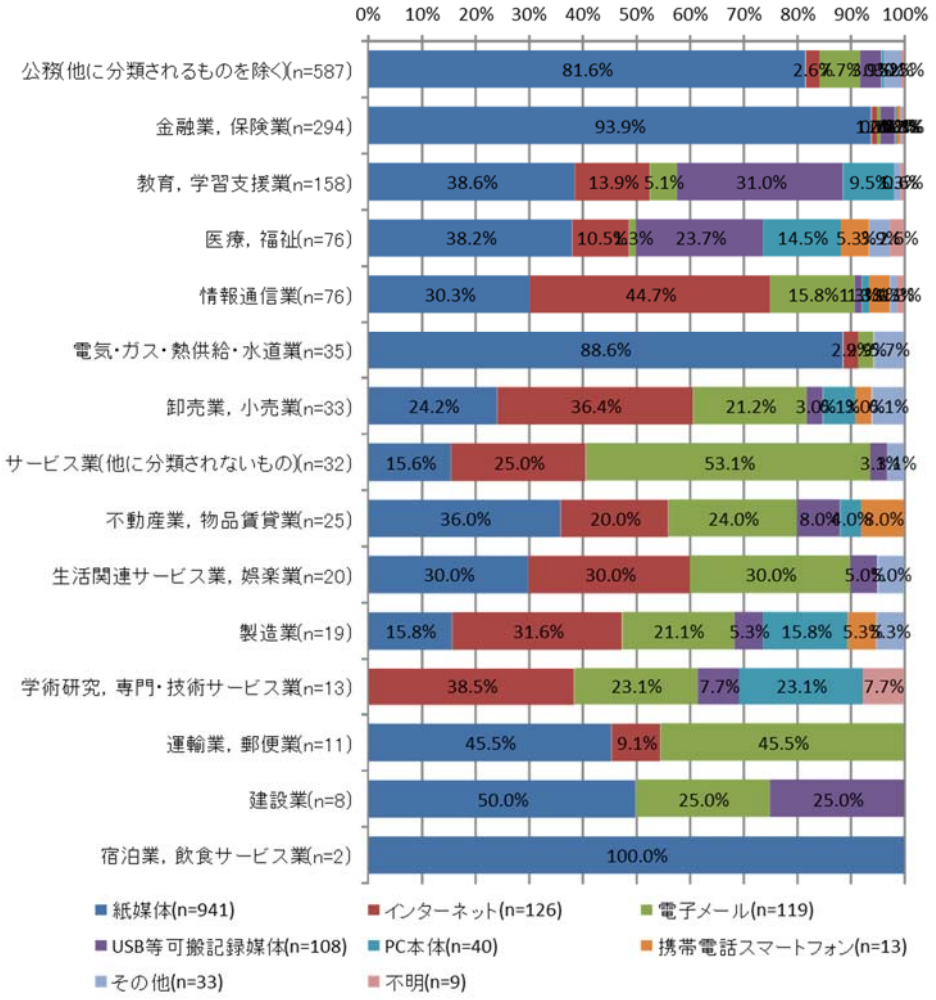

図 3-21：業種別の漏えい経路比率（件数）

漏えい媒体・経路の業種別比率（件数）について図 3-21 に示す。多くの業種で紙媒体によるインシデントが占める割合が高くなっているが、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ことが影響している。「公務」「金融業，保険業」「電気・ガス・熱供給・水道業」「宿泊業，飲食サービス」は、特に比率が高い。「情報通信業」「卸売業，小売業」「性格関連サービス業，娯楽業」「製造業」「学術研修，専門・技術サービス業」は「インターネット」の割合が 30%以上を占めている。「サービス業」「運輸業，郵便業」は「電子メール」の比率が高く、「教育学習支援」「医療，福祉」「建設業」は、「USB等可搬記録媒体」による比率が高い。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。業種毎に、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

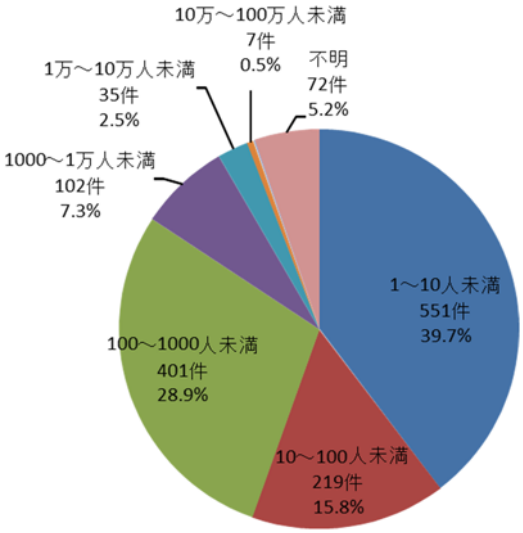

図 3-22：漏えい規模比率（件数）

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 3-22 に示す。全体的には、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。とくに「1～10 人未満」の比率が大きいのは、地方自治体、水道局などの公務や公共インフラの業種において、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方針の組織が増えていることが理由と見られる。

また「100～1000 人未満」の比率も比較的大きい。これは金融機関において多数の支店で発生した帳票の紛失を、支店別ではなく合計件数で公表されることが多いためである。本調査報告書ではそのような形式の公表に対し、合計件数を支店数で割った数字（平均値）を支店ごとの漏えい規模とみなして集計しているため、平均的な値である「100～1000 人未満」のインシデント件数が多くなる。

(2)　経年分析(件数)

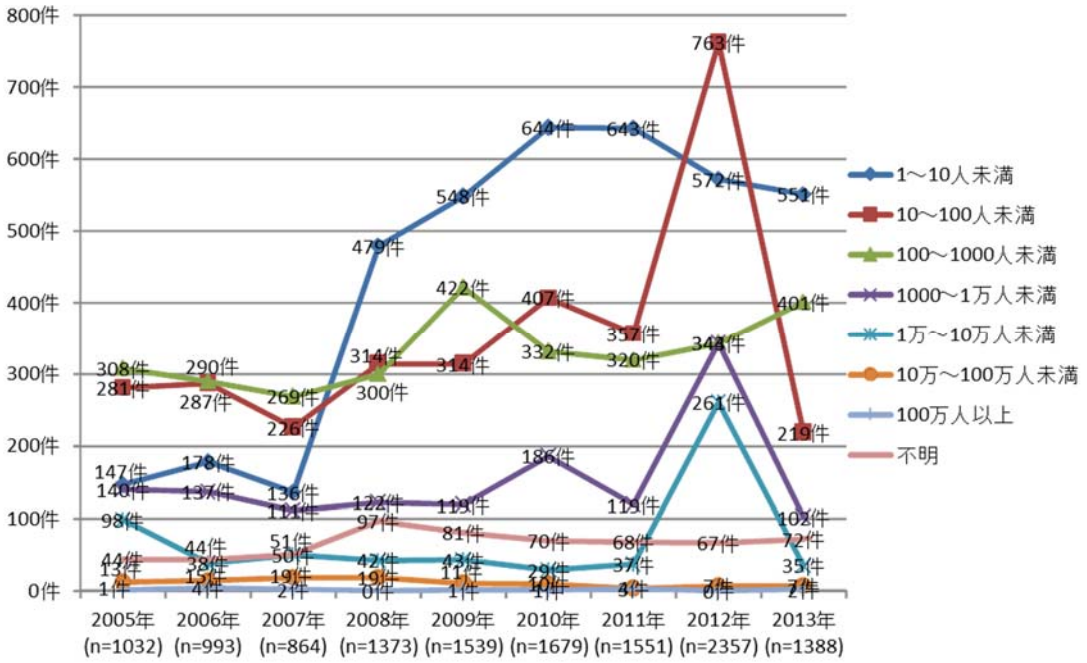

図 3-23：一件あたりの漏えい人数区分の経年変化（件数）

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 3-23 に示す。2013 年は、イレギュラーだった 2012 年を除けば、ほぼ 2008 年以降の例年通りの件数割合であったと言える。

(3)　業種別（件数）

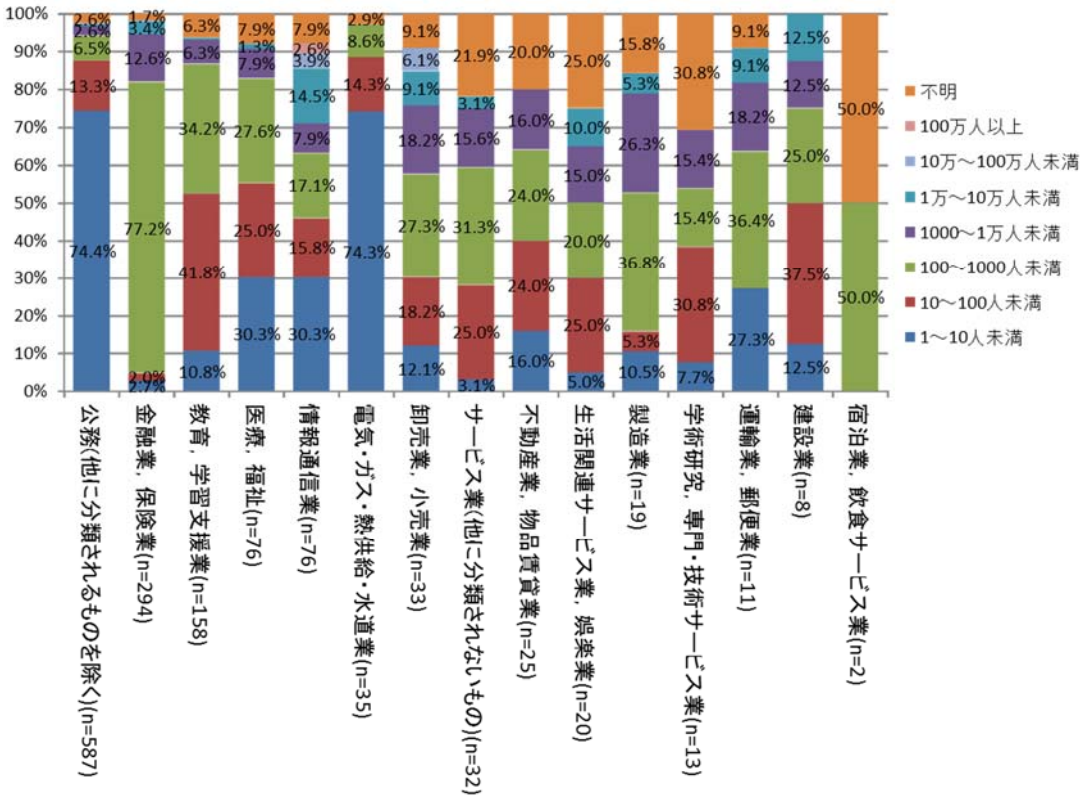

図 3-24：業種別の漏えい規模比率（件数）

業種別の漏えい規模（件数）の比率を図 3-24 に示す。「1～10 人未満」の小規模なインシデントの公表は「公務」「電気・ガス・熱供給・水道業」における比率が高い。また「100～1000 人未満」のインシデントの比率を押し上げているのは「金融，保険業」であることも見て取れる。

3.7　漏えい情報の価値

(1)　漏えい情報

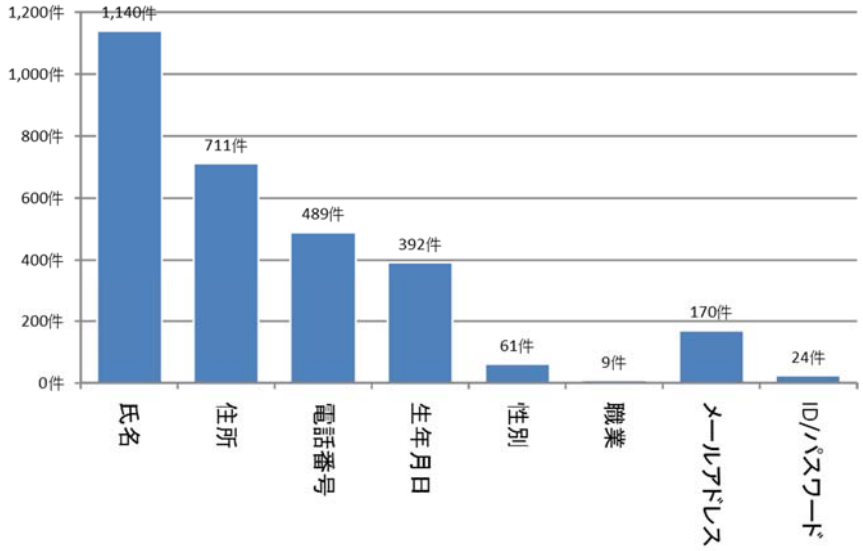

図 3-25：漏えい情報の出現確率

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	1140 件	82.1%
住所	711 件	51.2%
電話番号	489 件	35.2%
生年月日	392 件	28.2%
性別	61 件	4.4%
職業	9 件	0.6%
メールアドレス	170 件	12.2%
ID/PASSWD	24 件	1.7%

漏えい情報の出現確率を図 3-25、表 3-3 に示す。

「氏名」の出現率が 82.1%で高く、次いで住所（51.2%）、電話番号（35.2%）と続く。例年通り、「氏名」、「住所」などの基本的な個人情報の出現率が高いと考えられる。1.7%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)

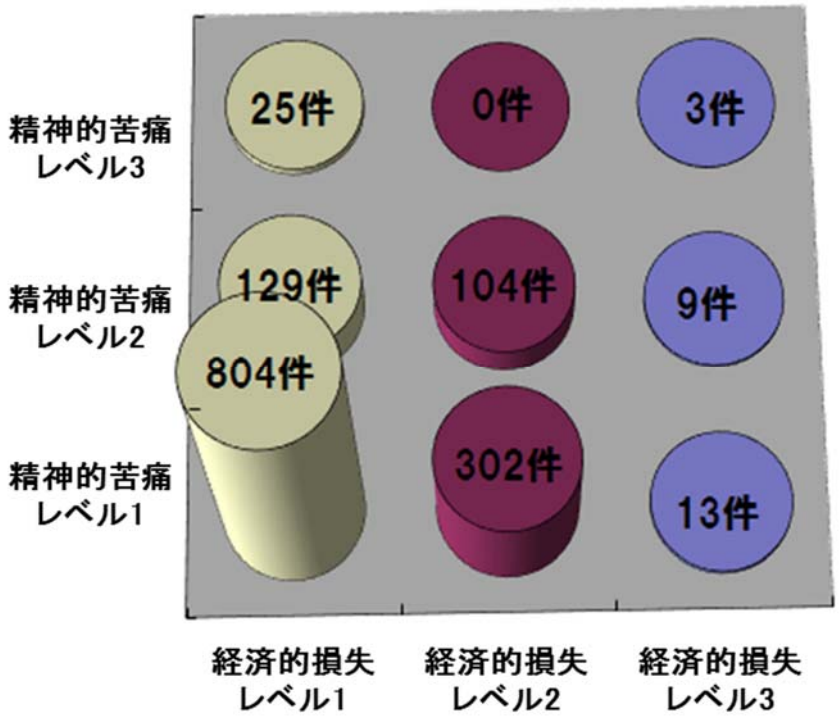

図 3-26：シンプル EP 図分布（件数）

2013 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 3-26 に示す。 シンプル EP 図については、P50～P51 を参照されたい。

2013 年の被害分布状況の特徴は、2012 年との比較し、精神的苦痛または経済的損失のレベルのいずれかが 2 であるフィールドの件数が減少し、かわって精神的苦痛と経済的損失がともにレベル 1 のフィールドが増加した点である。

(2)　業種別EP分布

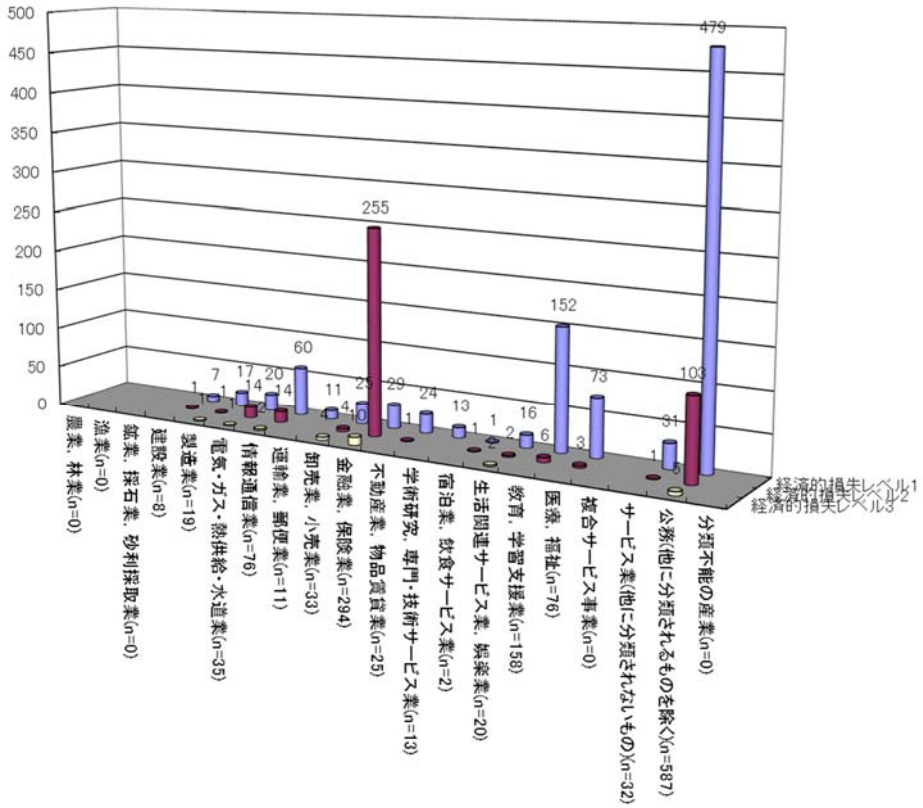

図 3-27：漏えい情報の経済的損失レベル分布（件数）

漏えい情報の経済的損失レベル分布（件数）を図 3-27 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」「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」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」、「金融業，保険業」であり、他は微少であった。

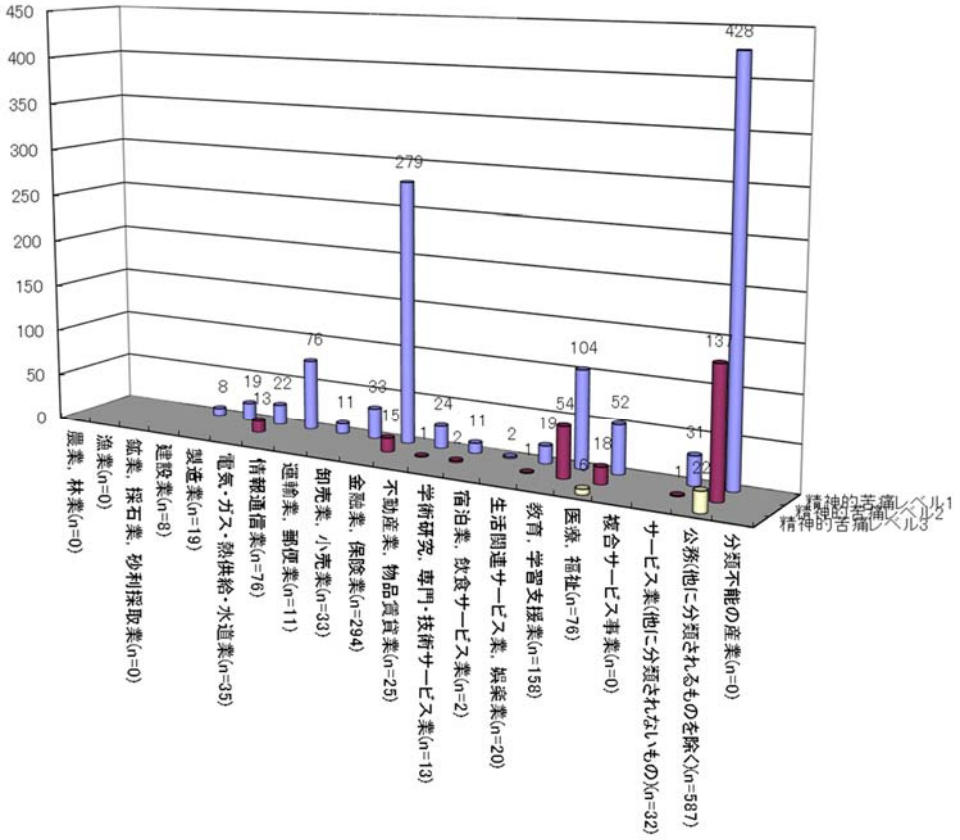

図 3-28：漏えい情報の精神的苦痛レベル分布（件数）

漏えい情報の精神的苦痛レベル分布（件数）を図 3-28 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」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。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 2013 年の間に収集した 9 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、2013 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	1032 件	881 万 4735 人	8922 人
2006 年	993 件	2223 万 6576 人	2 万 3432 人
2007 年	864 件	3053 万 1004 人	3 万 7554 人
2008 年	1373 件	723 万 2763 人	5668 人
2009 年	1539 件	572 万 1498 人	3924 人
2010 年	1679 件	557 万 9316 人	3698 人
2011 年	1551 件	628 万 4363 人	4238 人
2012 年	2357 件	972 万 65 人	4245 人
2013 年	1388 件	925 万 2305 人	7027 人

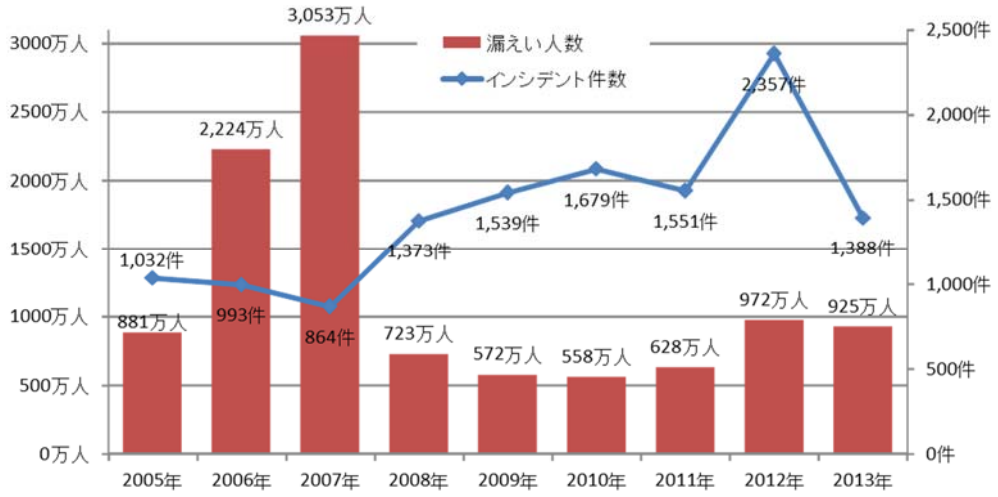

図 3-29：インシデント件数と漏えい人数の経年変化（合計）

2013 年のインシデント件数は、2012 年より大きく減少した。また、漏えい人数も 2012 年と比較してわずかに減少した。2013 年のインシデント件数は、2012 年より

※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 2013 年は 1,388 件から被害者数不明の 72 件を除いた 1,316 件で漏えい人数を除算した。

は減少したが 2008 年以降の例年とほぼ同じである。2013 年の漏えい人数は、2008 年以降では多いほうである。

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。一件当たり 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、2011 年が 3 件、2012 年が 0 件、2013 年が 2 件であった。2013 年は 2012 年と比較して、インシデント件数が大きく減少したものの、漏えい人数はわずかしか減少していない。これは 100 万人以上のインシデントが 2012 年の 0 件から 2013 年は 2 件に増加したことなどの影響によるものと考えられる。

また、内部犯罪・内部不正行為については、大規模なインシデントの影響によって変動するが、全体の傾向としては減少してきている。2013 年の内部犯罪・内部不正行為の比率は 0.004%であり、例年に比べても非常に少なかった。

表 3-5：内部不正による漏えい人数の経年変化の割合

	内部犯罪・内部不正行為	内部犯罪・内部不正行為以外
2005 年	10.2%	89.8%
2006 年	18.0%	82.0%
2007 年	28.3%	71.7%
2008 年	4.4%	95.6%
2009 年	29.1%	70.9%
2010 年	8.4%	91.6%
2011 年	7.1%	92.9%
2012 年	1.2%	98.8%
2013 年	0.004%	99.996%

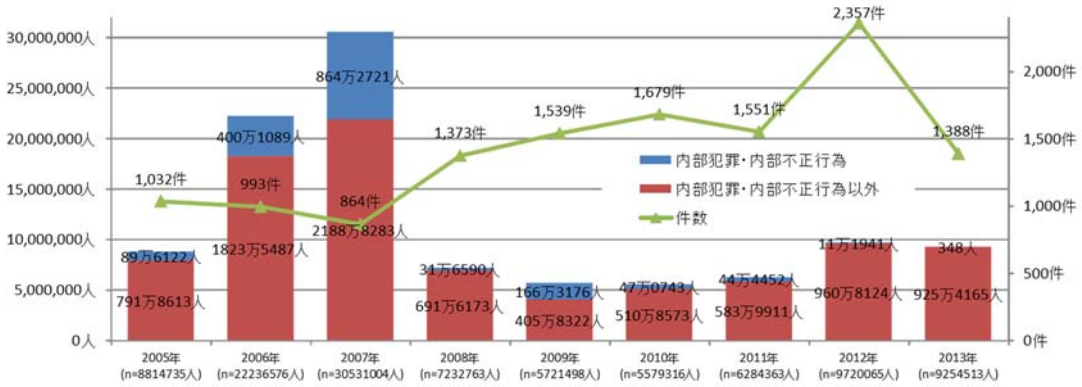

図 3-30：インシデント件数と内部不正による漏えい人数の経年変化（合計）

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 3-30 に示す。

個人情報保護法が完全施行された 2005 年以降、毎年 1000 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、2013 年は 1388 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おり、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。

2008 年以降は、インシデント件数は年間 1500 件前後で推移し、漏えい人数は 500 万人から 1000 万人の範囲で推移してきている。

図 3-2 のインシデント件数を見ると、年によって増減はあるものの「公務」と「金融業、保険業」の比率が高いことが分かる。図 3-7 の 漏えい人数の経年比較を見ると、「金融業，保険業」の比率が高い年と、「情報通信業」の比率が高い年があることが分かる。これは、その年に発生した大規模なインシデントが大きく影響するためと考えられる。

4　2013 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 5329 億円
2006 年	約 4570 億円
2007 年	約 2 兆 2711 億円
2008 年	約 2367 億円
2009 年	約 3890 億円
2010 年	約 1215 億円
2011 年	約 1900 億円
2012 年	約 2133 億円
2013 年	約 1439 億円

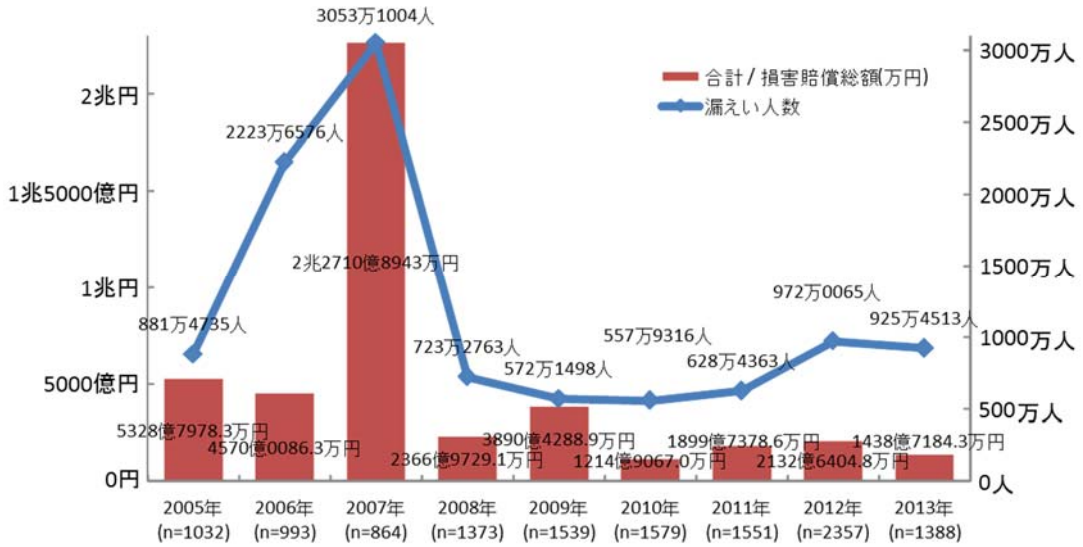

図 4-1：想定損害賠償総額と漏えい人数

想定損害賠償総額と漏えい人数の関係を図 4-1 に示す。2008 年以降、漏えい人数、想定損害賠償総額ともに低い値で推移している。2013 年は、漏えい人数、想定損害賠償総額とも、2012 年に比較して、微減した。

4.2　一人あたりの想定損害賠償額

(1)　単年分析

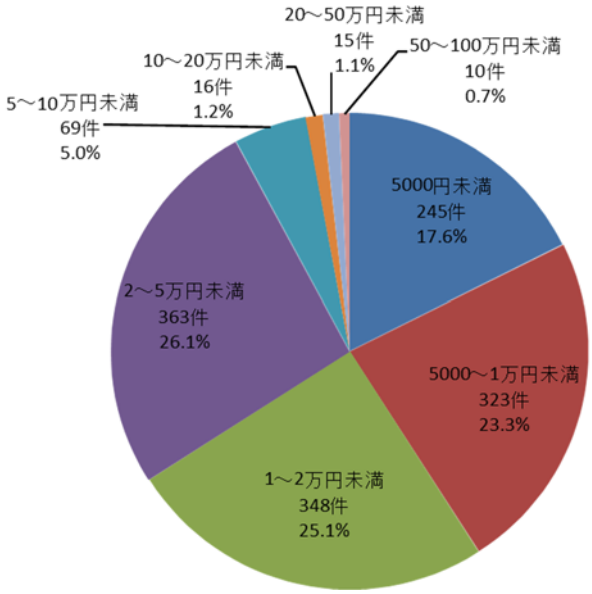

図 4-2：一人あたりの想定損害賠償額比率（件数）

一人あたりの想定損害賠償額を図 4-2 に示す。2013 年は、一人あたりの想定損害賠償額が「2～5 万円未満」のインシデント件数の占める比率が約 26%と最も多く、次いで「1～2 万円未満」の区分の約 25%が続く。両区分を合わせると、半数以上（約 51%）に達する。

(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
2011 年	4 万 8560 円
2012 年	4 万 4628 円
2013 年	2 万 7675 円

一人あたりの平均想定損害賠償額は、2 万円後半から 5 万円の範囲に収まっている。

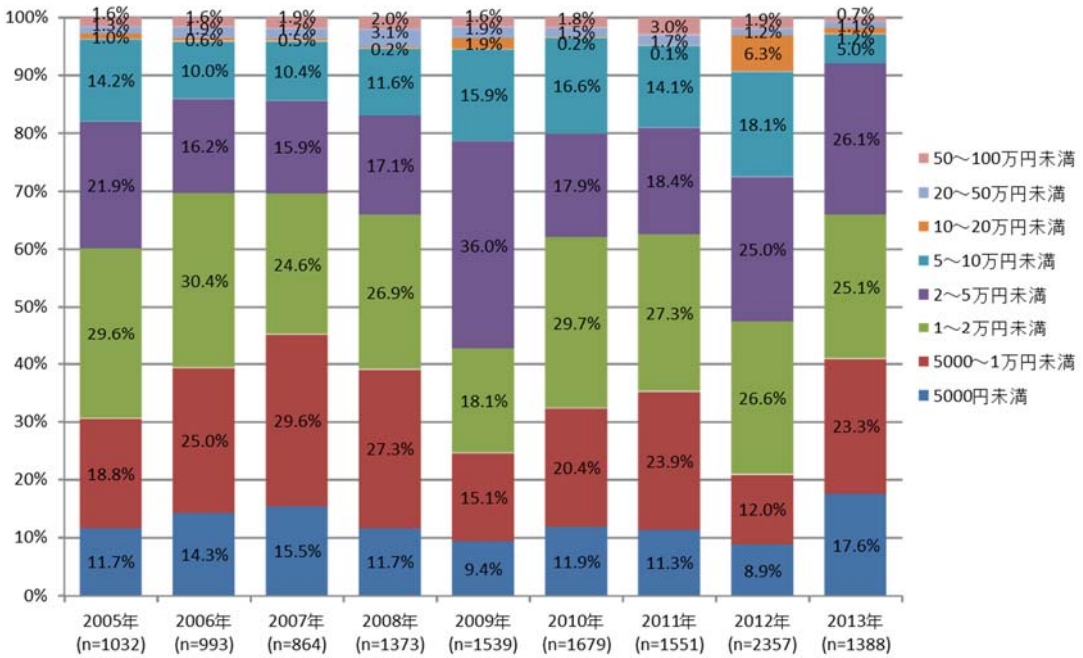

図 4-3：一人あたりの想定損害賠償額比率の経年変化（件数）

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。2013 年は、2012 年に比較して、「5000 円未満」と「5000～1 万円未満」の比率が増加し、「5～10 万円未満」の比率が減少した。全体的に俯瞰してみると、2009 年と 2012 年を除けば、ほぼ同様の傾向を示していることがわかる。

【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

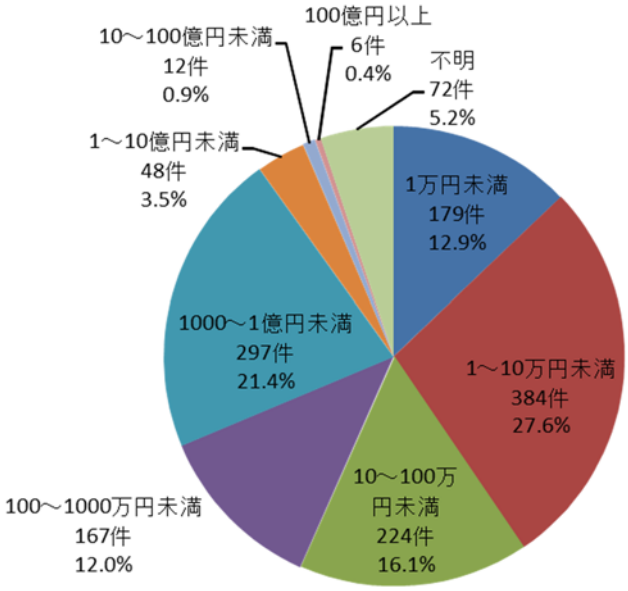

図 4-4：一件あたりの想定損害賠償額比率（件数）

一件あたりの想定損害賠償額を図 4-4 に示す。一件あたりの想定損害賠償額が 100 万円未満の区分を合わせると半数以上(約 57%)を占める。最も多い区分は「1 万円以上～10 万円未満」の比率で、約 28%である。また、2013 年は「1000 万円～1 億円未満」の比率が、前後の区分と比較して突出して高くなっているが、これは不正アクセス件数が増加したことの影響と考えられる。

(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
2011 年	1 億 2810 万円	約 1900 億円
2012 年	9313 万円	約 2133 億円
2013 年	1 億 6575 万円	約 1439 億円

2013 年は、2012 年に比較して、想定損害賠償の総額は減少したが、一件あたりの想定損害賠償額は増加した。これは、不正アクセスの件数が増加したことによる影響と考えられる。

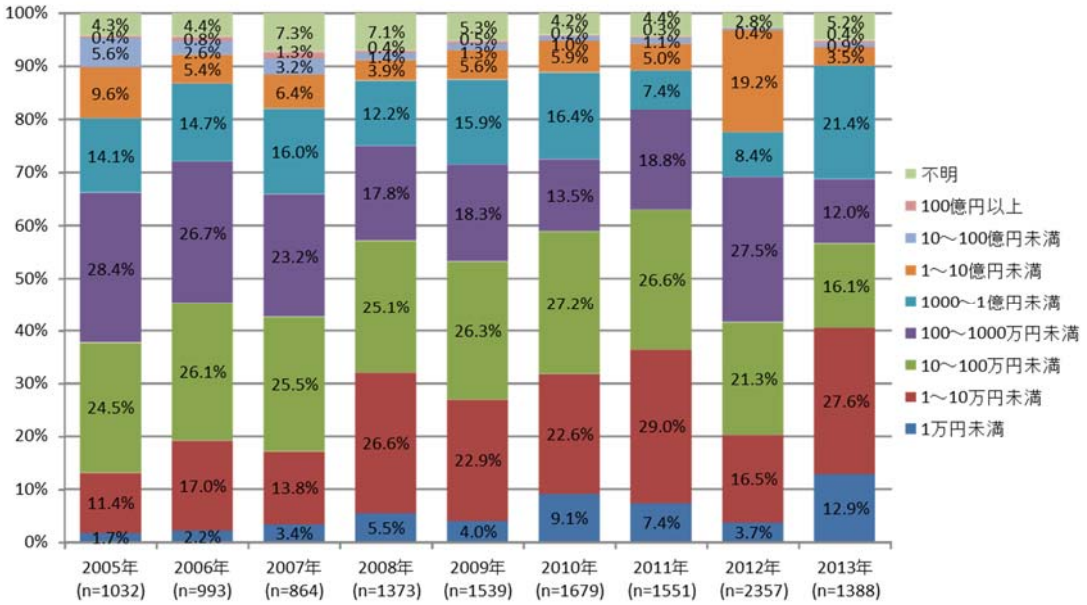

図 4-5：一件あたりの想定損害賠償額比率の経年変化（件数）

一件あたりの想定損害賠償額の経年変化を図 4-5 に示す。2013 年は、2012 年に比較して、「1～10 万円未満」と「1000 万～1 億円未満」などの比率が増加し、「100～1000 万円未満」と「1～10 億円未満」などの比率が減少した。2008 年以降は、2012 年を除き「1～10 万円未満」と「10～100 万円未満」の比率が高い傾向が続いている。

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、2012 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。想定損害賠償算定式の策定プロセスは図 5-1 に示す通りである。

5.2.1　想定損害賠償額算定式の策定プロセス

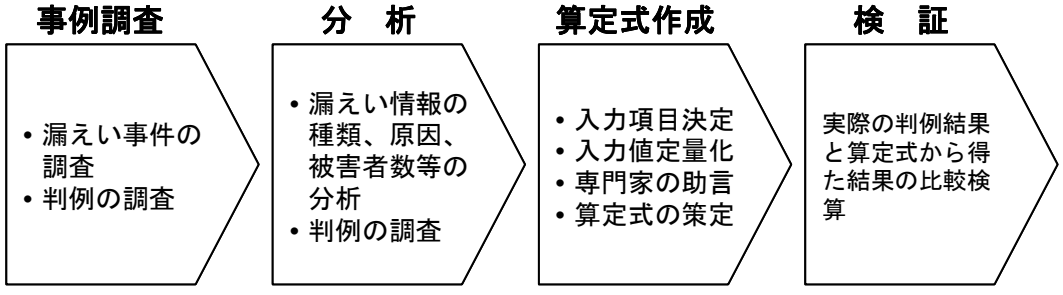

図 5-1：想定損害賠償額算定式策定のプロセス

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。2012 年の分析結果は「3. 2013 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。

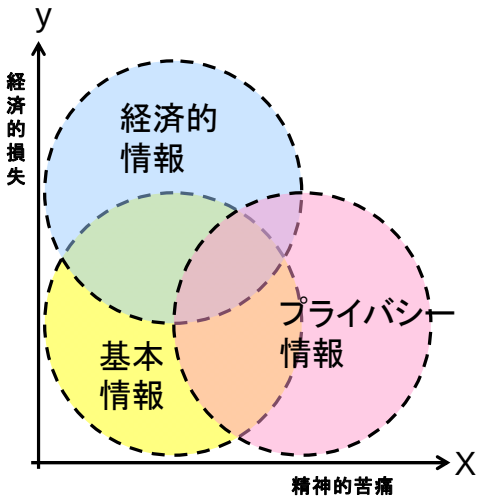

図 5-2：EP 図（Economic-Privacy Map）

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。

経済的損失レベル				
	3	口座番号＆暗証番号、クレジットカード番号＆カード有効期限、金融系Webサイトのログインアカウント＆パスワード、決済機能付きのサイトの顧客登録情報(アカウントにメールアドレスを使用する場合も含む。)	遺言書	前科前歴、犯罪歴、与信ブラックリスト
	2	パスポート情報、購入記録、ISPのアカウント＆パスワード(アカウントにメールアドレスを使用する場合も含む。決済機能のないサイトのアカウント＆パスワードも含む)、口座番号のみ、クレジットカード番号のみ、金融系Webサイトのログインアカウントのみ、印鑑登録証明書、ソーシャルセキュリティナンバー、サービス申込(加入申請)情報	年収・年収区分、所得、資産(固定資産税など)、建物、土地、残高、借金、所得(生活保護に関わる情報含む)、借り入れ記録、購入履歴(スタンプやポイントは除く)、給与額、賞与額、納税金額、寄付目的・金額、税や保険、保育費などの未納金額	
	1	氏名、住所、生年月日、性別、金融機関名、住民票コード、メールアドレス、健康保険証番号、年金証書番号、免許証番号、社員番号、会員番号、電話番号、ハンドル名、健康保険証情報、年金証書情報、介護保険証情報、会社名、学校名、役職、職業、職種、身長、体重、血液型、身体特性、写真、肖像、音声、声紋、体力測定値、家族構成、ISPアカウント名のみ、患者番号、受診科目・受診日、水栓番号、保険加入状況に関する情報、請求に係る金額(払戻しの請求金額など)	健康診断結果(結核検査記録など)、心理テスト結果、性格判断結果、病歴、手術歴、妊娠歴、看護記録、その他身体検査記録、治療法(治療に係る記録映像含む)、レセプト情報(治療に係る金額)、身体障がい者手帳情報、DNA情報、身体障がい情報、知的障がい情報、指紋、生体認証情報(静脈,声紋,虹彩,網膜,顔画像等)、スリーサイズ、人種、地方なまり、国籍、趣味、特技、嗜好、民族、賞罰(交通違反切符など)、職歴(求職に関する書類含む)、学歴(求職に関する書類含む)、成績(教務手帳を含む)、試験得点(解答用紙など含む)、日記、メール内容(内容によって、どの情報に該当するかを判断すべし)、位置情報、児童相談に関わる情報、高齢者医療保険や介護保険の還付金額、プライベート(恋愛)情報	加盟政党、政治的見解、加盟労働組合、信条、思想、宗教、信仰、本籍(戸籍附票、住民票に記載される本籍も含む)、病状(結核医療に関する情報など)、保有感染症、カルテ(エックス線写真も含む)、認知症情報、精神的障がい情報、性癖、性生活の情報、介護度、プライベート(不倫)情報(写真も含む)
		1	2	3
				精神的苦痛レベル

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

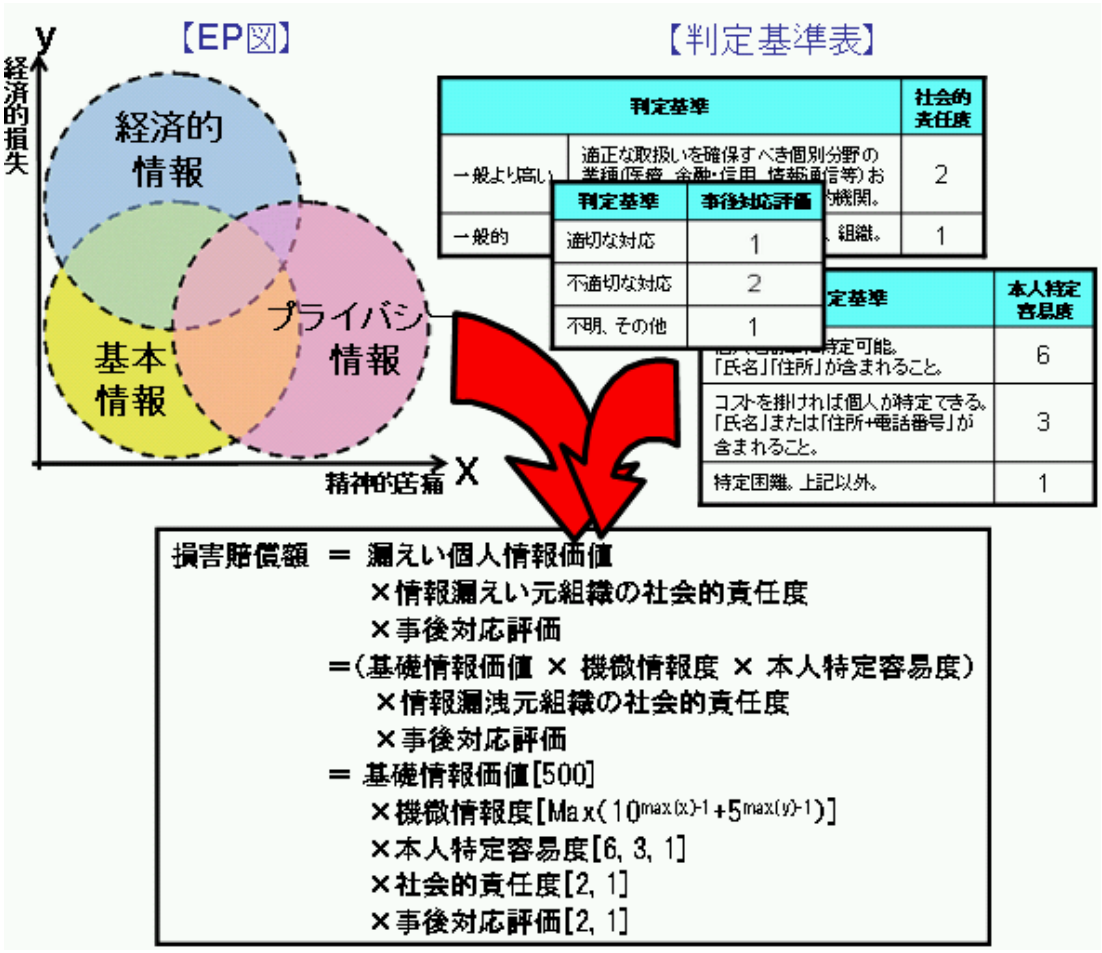

図 5-4：JO モデル

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

2013 年の個人情報漏えいインシデントを振り返って、以下に、「6.1 2013 年インシデントの特徴」「6.3 個人が気をつける個人情報漏えい」「6.2 パスワードリスト攻撃」「6.4 パーソナルデータの利活用に関する問題」についてまとめた。

2013 年は、これまでのインシデントとの違う結果が出た年でもあった。その一つに「不正アクセス」があげられる。まずは、2013 年インシデントの特徴でこれまでとの違いを触れる。また、スマートフォンの普及というプラットフォームの変遷とパスワードリスト攻撃という新しい脅威にも触れ、因果関係について考察する。さらに、情報漏えいの被害が複雑化する一方で、現在検討されているパーソナルデータの利活用についても触れる。

6.1　2013 年インシデントの特徴

2013 年は、2012 年に増加した漏えい件数 2,357 件が 1,388 件に減少し、平年並みの数値に戻った。また、インシデントの三大要因である管理ミス、誤操作、紛失・置忘れの件数も平年並みに戻った。これは、2012 年に行われた金融機関向けの点検による一時的な影響であったと推測できる。

一方で、情報通信業において漏えい件数の変化はないものの、1 件あたりの平均漏えい人数が 9,500 人と、非常に多い特徴があった。不正アクセスによる平均漏えい人数が 13 万 2000 人/件であり、主な原因となった。また、経路としてインターネットからの漏えい人数が 750 万人、人数比の割合が 80.5%と高く、1 件あたりの平均人数も約 7 万人と、非常に多かった。これは主に「パスワードリスト攻撃」という手法によるものである。

パスワードリスト攻撃については「6.2 **パスワードリスト攻撃**」で、パスワードリストの入手のリスクについては「6.3 **個人が気をつける個人情報漏**」で詳しく説明する。

6.2 パスワードリスト攻撃

2013 年は、パスワードリスト攻撃※による被害が多く発生した。パスワードリスト攻撃とは、漏えいした ID とパスワードなどを不正に入手して、これを使って別のサービスのアカウントへの不正ログインを試みる攻撃である。インターネット上のサービスのうち、ID を電子メールアドレスに固定しているサービスは ID を特定しやすく、ユーザがパスワードを使い回しているとパスワードリスト攻撃によって容易に不正ログインの被害を受けてしまう。2013 年に公表されたパスワードリスト攻撃は 34 件であった。「表 3-2：インシデント・トップ 10」のうち、パスワードリスト攻撃による大量の個人情報漏えいインシデントが 2 件含まれていた。2013 年に公表されたパスワードリスト攻撃 34 件について、業種別の発生件数と不正ログイン成功回数を「図 6-1：パスワードリスト攻撃の発生件数」と「図 6-2：不正ログイン成功回数」に示す。

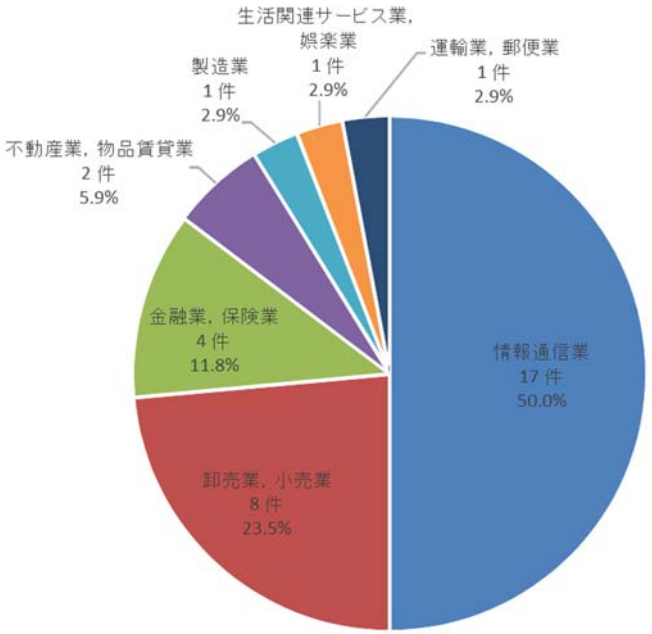

図 6-1：パスワードリスト攻撃の発生件数

パスワードリスト攻撃 34 件のうち、半分の 17 件が情報通信業で発生した。インターネット接続サービスやオンラインゲームのアカウントが攻撃されて被害が発生している。次の卸売業，小売業は、すべてオンラインショッピングサイトが攻撃されて被害が発生した。被害は、不正にログインされて個人情報が漏えいしたと報告されている。公表された情報からは、高価で換金性の高い商品を不正に購入された

※ 「パスワードリスト攻撃」「リスト型攻撃」「リスト型アカウントハッキング攻撃」「アカウントリスト攻撃」など、複数の呼び方が存在するが、本報告書では「パスワードリスト攻撃」とする。

被害は確認できなかった。金融業，保険業は、オンラインバンキングのアカウントで被害が発生した。

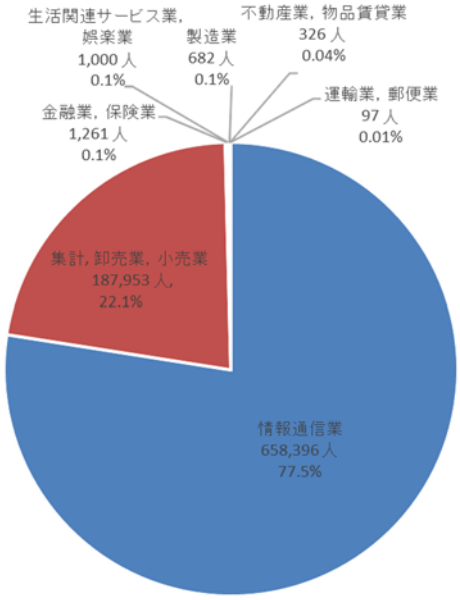

図 6-2：不正ログイン成功回数

不正ログイン回数は、情報通信業が約 80%を占めた。情報通信業は 1 件あたりの不正ログイン成功数が数万人規模の場合が多い。情報通信業のオンラインサービスはユーザ数が多く、パスワードリスト攻撃が成功する確率が高かった当予想される。

6.3　個人が気をつける個人情報漏えい

パスワードリスト攻撃のためには、アカウント情報が不可欠である。昨今のクラウドに代表されるインターネットサービスは、個人のメールアドレスが ID となるケースが多く、複数のインターネットサービスの ID が共通である利用者が少なくない。また、複数のパスワードを使いこなす利用者は珍しく、パスワードも共通にしてしまいがちである。攻撃者はそういった点を逆手に取り、不正に入手した ID とパスワードリストをつかってパスワードリスト攻撃を行う。

例えば、2013 年にコンピューターウイルスの機能を持たせたスマートフォン用の不正アプリを配布し、スマートフォンから電話帳データなどが抜き取られる事件が発生した。2013 年 9 月、京都府警サイバー犯罪対策課と山科署は、この不正アプリを配布した大分県の出会い系サイト運営会社元会長や東京都のＩＴ関連会社元社長ら 6 人を不正指令電磁的記録（ウイルス）作成や同供用などの疑いで逮捕した。男らが不正入手した個人情報は延べ約 6 億 5 千万件に上る疑いがあるという。

この他にも、2013 年からオンラインバンクで使用する個人情報を狙った「VAWTRAK」が猛威を奮っている。VAWTRAK の亜種は、オンライン銀行の認証情報も窃取するという。ウイルス対策ソフトベンダの報告によると、VAWTRAK は 2013 年 8 月に初めて存在が確認され、不正な活動は特に日本において顕著という。

これまで個人情報漏えいは、業務において大量の個人情報を収集、管理している企業、組織からの漏えいリスクが高かった。しかし、近年は個人のパソコンやスマートフォンがインターネットに常時接続されるようになったため、攻撃者が直接攻撃し、個人情報を搾取するようになった。また、個人によるオンラインバンキングやオンラインショッピング、個人を対象とした無料クラウドサービスの利用の増加により、個人情報がインターネット上に保存されるようになった。そのため、攻撃者はインターネット上のサービスも攻撃している。

つまり企業、組織が管理している個人情報とは別に、これらの個人が管理するパソコンやスマートフォン、インターネットサービス上の個人情報も攻撃の対象となってきたため、個人が自分自身で個人情報を管理し、情報漏えいに注意を払うことが重要になってきた。

6.4　パーソナルデータの利活用に関する問題

2013 年 6 月 27 日に Suica のデータを販売し、駅エリアのマーケティングに活用していくことが報道発表された。JR 東日本は、Suica の利用規約「第 19 条（個人情報の収集、保有、利用)」[2]で利用者情報を分析した結果から個人を特定できないように加工した情報の利用と提供を定めていた。しかし、Suica 利用者への事前説明や情報公開が不足したまま他社に提供した。そのため Suica 利用者が不安や不満を感じて、問い合わせや批判が多く発生した。この Suica のデータの第三者への販売において、問題だったと言われている点を以下に挙げる。

- 事前説明や情報公開の不足
- 情報提供の除外要望受付(オプトアウト)の手続きが無かった。周知が無かった
- 提供先企業からのデータの流出、悪用を防ぐ方法が説明不足
- 利用目的に対してデータの精度が不必要に高かった、匿名化が不十分

JR 東日本は、販売用の Suica のデータは個人情報に該当しないことの詳細な説明やオプトアウトの仕組み[3]を追加したが、データの販売は見合わせたままである。

個人情報保護法の施行以来、個人情報の利活用が難しくなった。しかし、個人情報保護法の施行から 10 年が経過し、ビックデータ関連ビジネス、特にビックデータを使ったマーケティングが活発化してきている。そこで、個人情報を匿名化して利活用できるようなルールの検討[4]が始まっている。またマイナンバー制度の導入にともない、個人と国や地方自治体、企業が、個人番号と紐付いた特定個人情報を取り扱う機会が発生する。今後、個人情報の利活用のルールが明確になり、個人情報の商用利用の実例が増えてノウハウが蓄積されれば、より安全な利活用方法が確立されるだろう。

[2] JR 東日本：Suica インターネットサービス 利用規約,
http://www.jreast.co.jp/suicainternetservice/rule/
[3]除外要望受付フォーム/Suica に関するデータの社外への提供,
http://www.jreast.co.jp/suica/procedure/suica_data.html
[4] パーソナルデータの利活用に関する制度改正大綱, 平成 26 年 6 月 24 日 高度情報通信ネットワーク社会推進戦略本部,
http://www.kantei.go.jp/jp/singi/it2/info/h260625_siryou2.pdf

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

【改訂履歴】

リリース日	修正箇所	修正内容
Ver. 1.0 2014 年 12 月 25 日		
Ver. 1.1 2015 年 1 月 8 日	p.30, 表 3-4 図 3-29	表 3-4、図 3-29：2013 年インシデント件数を修正
Ver. 1.2 2015 年 2 月 23 日	p.50, 図 5-4	図 5-4：JO モデルの数値を修正
	p.55, 6.4 パーソナルデータの利活用に関する問題	記述を一部修正