2014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 1.0 版

2016 年 6 月 16 日
2016 年 7 月 11 日 改定

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

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、2014 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 2014 年のインシデントの集計・分析結果、及び過去 10 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、2014 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 2014 年の個人情報漏えいインシデントの分析結果」「第 4 章 2014 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 2014 年の個人情報漏えいインシデントの分析結果」では、2014 年の単年データの分析結果、および蓄積された 13 年間分のデータから 2005 年から 2014 年までの 10 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 2014 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

2014 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　2014 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、1591 件（前年比 202 件増）であった。2013 年より微増である。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 5000 万人（前年比 4075 万人増）と大幅に増加した。想定損害賠償総額は、約 1 兆 6642 億円（前年比 1 兆 5203 億円増）となった。大規模なインシデントが 1 件発生したためである。漏えい原因は、「管理ミス」（696 件）が一番多く、「誤操作」（491 件）、「紛失・置忘れ」（200 件）の 3 種類で約 90%を占めた。原因の上位 3 種類の 2014 年の比率は、ここ数年の平均的な比率であった。2014 年は 4000 万人以上の大規模なインシデントが発生したため漏えい人数が突出して多い結果となった。

2014 年の集計結果の概要データは、以下の通りである。

表 3-1：2014 年 個人情報漏えいインシデント 概要データ

漏えい人数	**4999 万 9892 人**
インシデント件数	**1591 件**
想定損害賠償総額	**1 兆 6642 億 3910 万円**
一件あたりの漏えい人数※1	**3 万 2616 人**
一件あたり平均想定損害賠償額※1	**10 億 8561 万円**
一人あたり平均想定損害賠償額※2	**5 万 2625 円**

※1：平均値は、被害者数が不明のインシデント 58 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。

2014 年は、一件あたりの漏えい人数が 1000 万人を超える大規模なインシデントが 1 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、業種は「公務」がやや多い。「内部犯罪・内部不正行為」が原因のインシデントは、発生頻度が低いが被害は大きい。管理ミスや紛失・置忘れ、誤操作といった人為的ミスは、例年より少なめであった。

表 3-2：インシデント・トップ 10

No.	漏えい人数	業種	原因
1	4858 万人	教育，学習支援業	内部犯罪・内部不正行為
2	16 万 4650 人	情報通信業	誤操作
3	13 万 1646 人	製造業	不正アクセス
4	9 万 4359 人	情報通信業	不正アクセス
5	6 万 1977 人	製造業	不正アクセス
6	5 万 6780 人	公務(他に分類されるものを除く)	誤操作
7	4 万 1477 人	公務(他に分類されるものを除く)	盗難
8	4 万人	金融業，保険業	管理ミス
9	4 万人	公務(他に分類されるものを除く)	内部犯罪・内部不正行為
10	3 万 9585 人	金融業，保険業	紛失・置忘れ

3.3 業種

(1) 単年分析(件数)

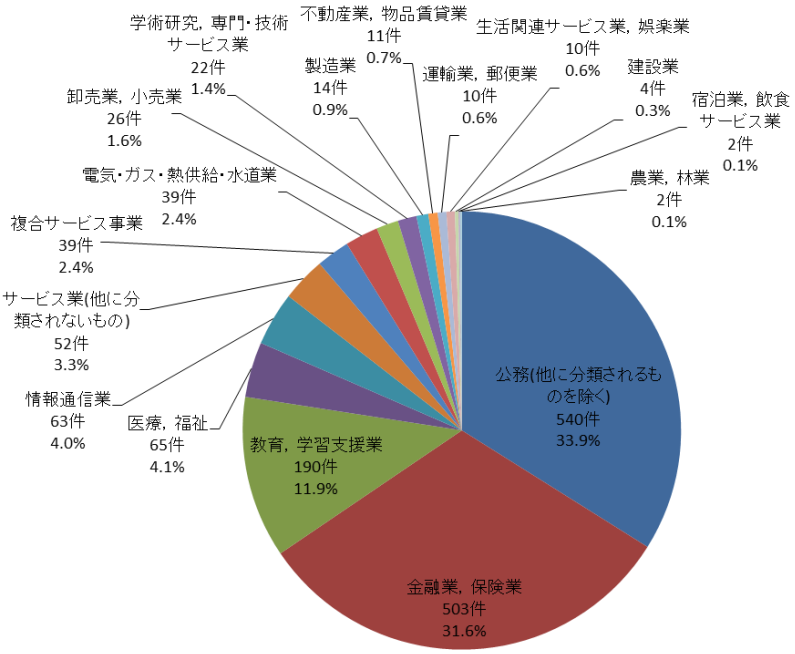

図 3-1：業種別比率（件数）

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」(33.9%)、「金融業，保険業」(31.6%)、「教育，学習支援業」(11.9 %)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」「教育，学習支援業」「医療，福祉」が、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、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ため、小規模なインシデントであっても公表することが多いからである。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)

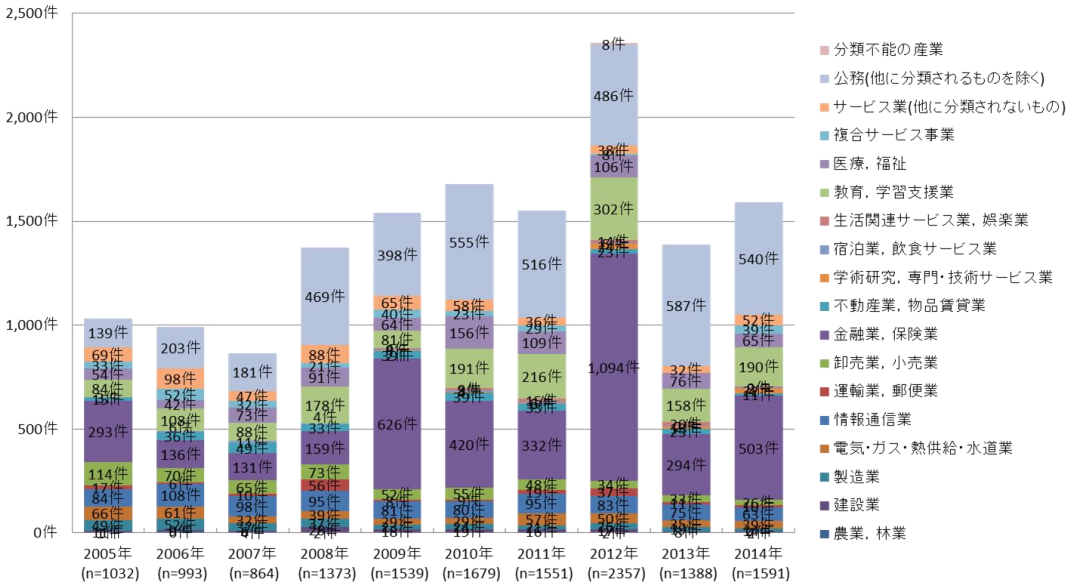

図 3-2：業種別件数の経年変化（件数）

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。

「金融業，保険業」のインシデント件数が大きく増加した 2012 年以外の 2008 年から 2014 年は、発生件数や比率は類似している。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といった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）

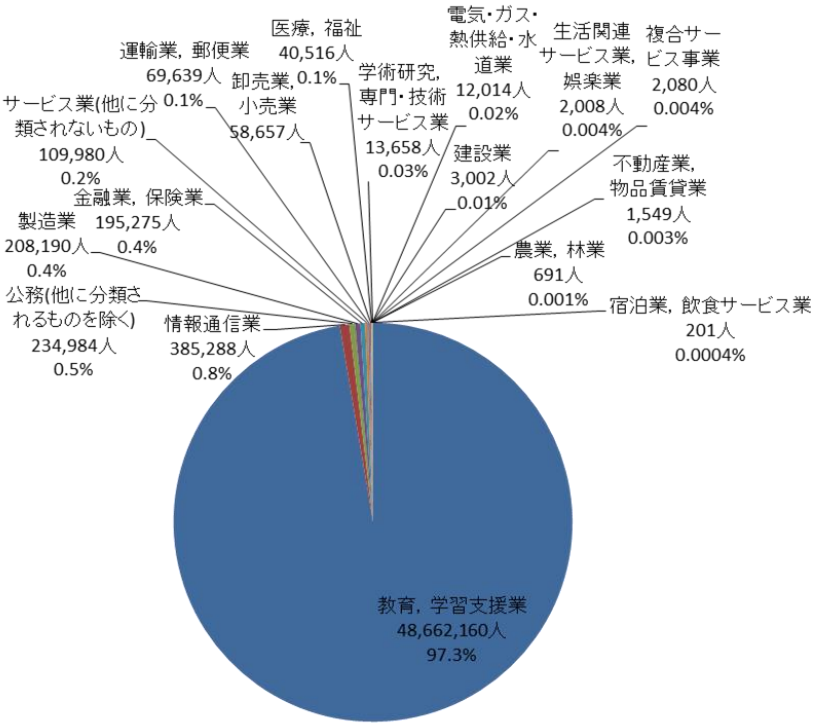

図 3-3：業種別比率（人数）

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。大規模なインシデント1件が影響し、「教育，学習支援業」が 97.3%を占めた。

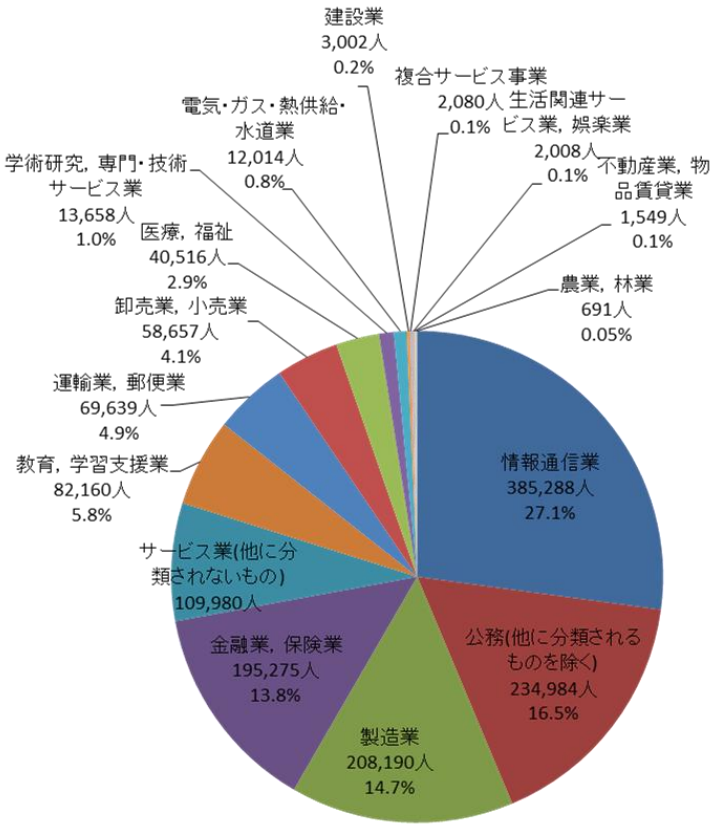

図 3-4：業種別比率（人数）

大規模なインシデント 1 件を除いた業種別での個人情報の漏えい人数の比率を図 3-4 に示す。

上位から順に「情報通信業」(27.1%)、「公務」(16.5%)、「製造業」(14.7%)、「金融業，保険業」(13.8%)であった。突出して人数が多い業種はなく偏りは見られない。

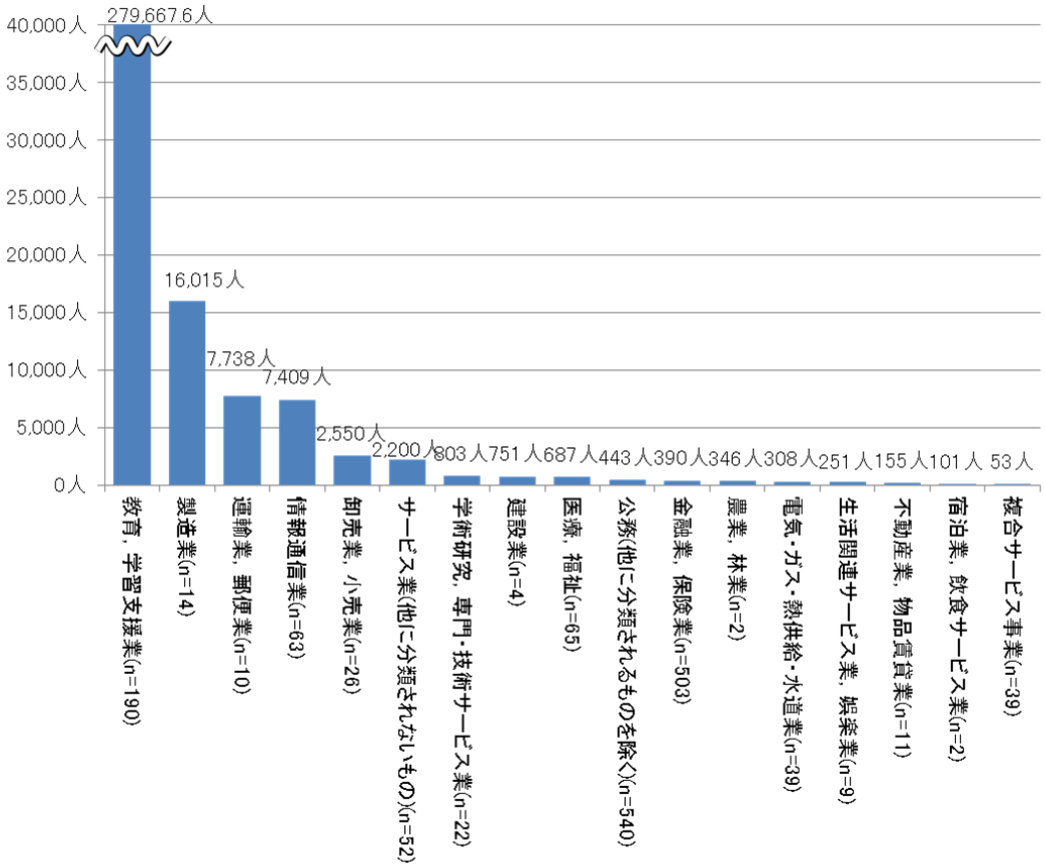

図 3-5：業種別の一件あたりの平均漏えい人数

インシデント一件あたりの漏えい人数（平均人数）を図 3-5 に示す。大規模なインシデント 1 件が影響し、「教育，学習支援業」(279,668 人)が最も多い。

大規模なインシデント 1 件を除いた場合、「製造業」(16,015 人)、「運輸業,郵便業」(7,738 人)、「情報通信業」（7,409 人）の順であった。「製造業」(16,015 人)、は、製造業のインシデント数が 14 件と少ないが、インシデント・トップ 10（表 3-2 参照）の 5 位のインシデント(6 万 1977 人)が発生して、平均漏えい人数を押し上げたためである。インシデントの件数が上位の「公務」は 443 人、「金融、保険業」は 390 人、大規模なインシデント 1 件を除いたあとの「教育，学習支援業」は 475 人であった。

(4)　箱髭図(人数)

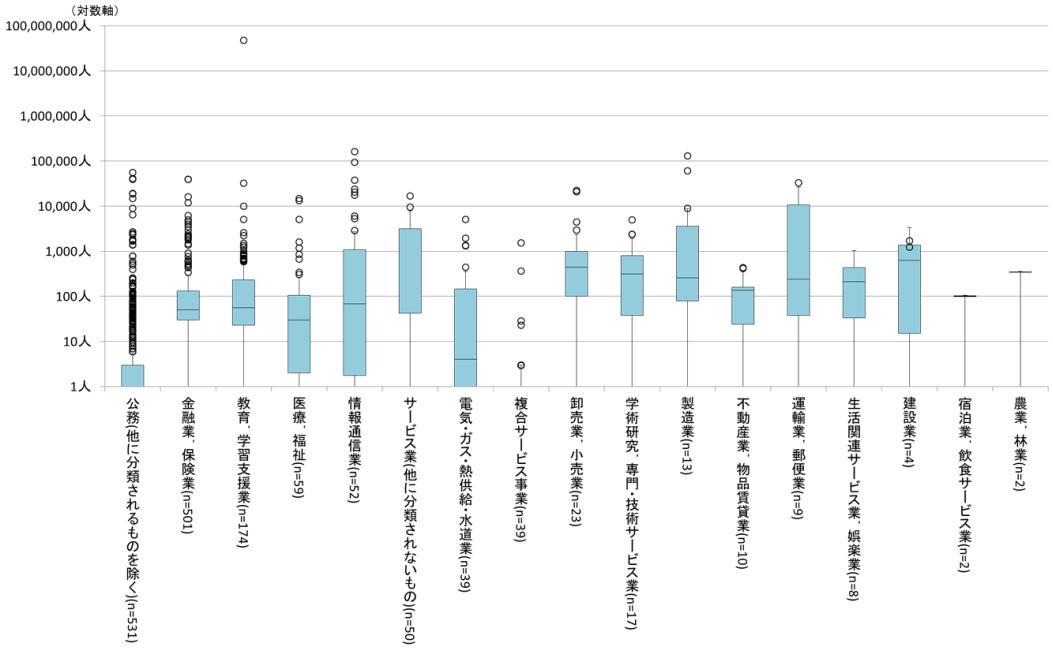

図 3-6：業種別の漏えい人数（箱髭図）

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 3-6 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」は、箱髭図の長方形の部分（以下、「箱」という。）が 1 人から 10 人の中に収まっている。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「製造業」は、箱の位置が他の業種と比較して高く、100 人から 5000 人の範囲であった。

「教育，学習支援業」の漏えい人数 1000 万人以上の丸印（外れ値）は、大規模なインシデント 1 件である。「情報通信業」と「製造業」にも、漏えい人数が 10 万人以上の外れ値が発生している。

[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。同様に「第 1 四分位数－1.5×IQR」より小さいデータは外れ値である。

(5)　経年分析（人数）

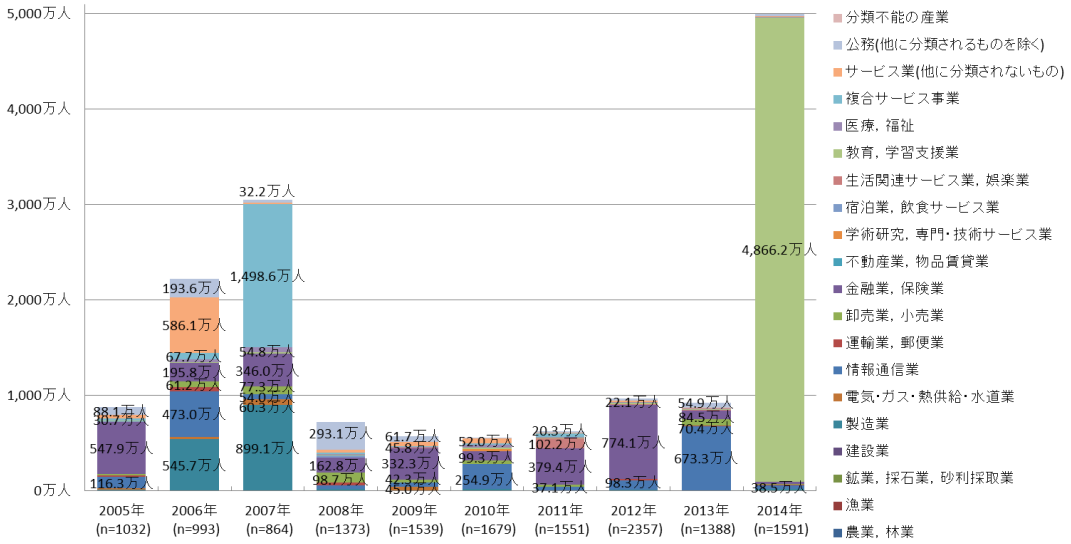

図 3-7：業種別漏えい人数の経年変化（合計）

業種別の個人情報漏えい人数を積み上げたグラフの経年変化を図 3-7 に示す。

大規模なインシデント 1 件の影響により、2014 年が他の年よりも突出したグラフになっている。他にも 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ため、他の年よりも突出している。

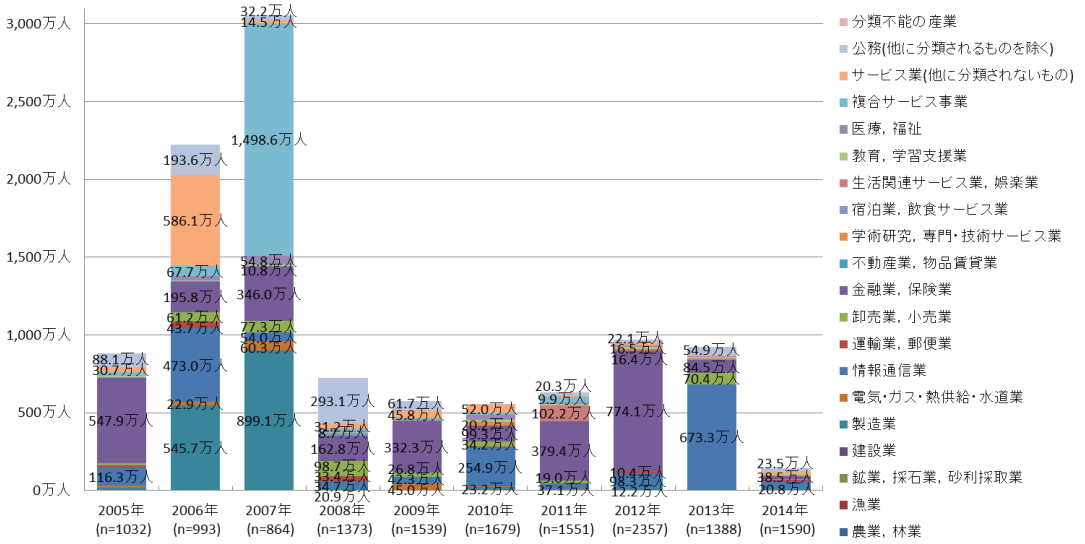

図 3-8：業種別漏えい人数の経年変化（合計）

大規模なインシデント 1 件を除いた業種別の個人情報漏えい人数を積み上げたグラフの経年変化を図 3-8 に示す。2014 年は、大規模なインシデント 1 件を除くと、漏えい人数の合計は、例年よりも大幅に減少している。

(6)　相関分析

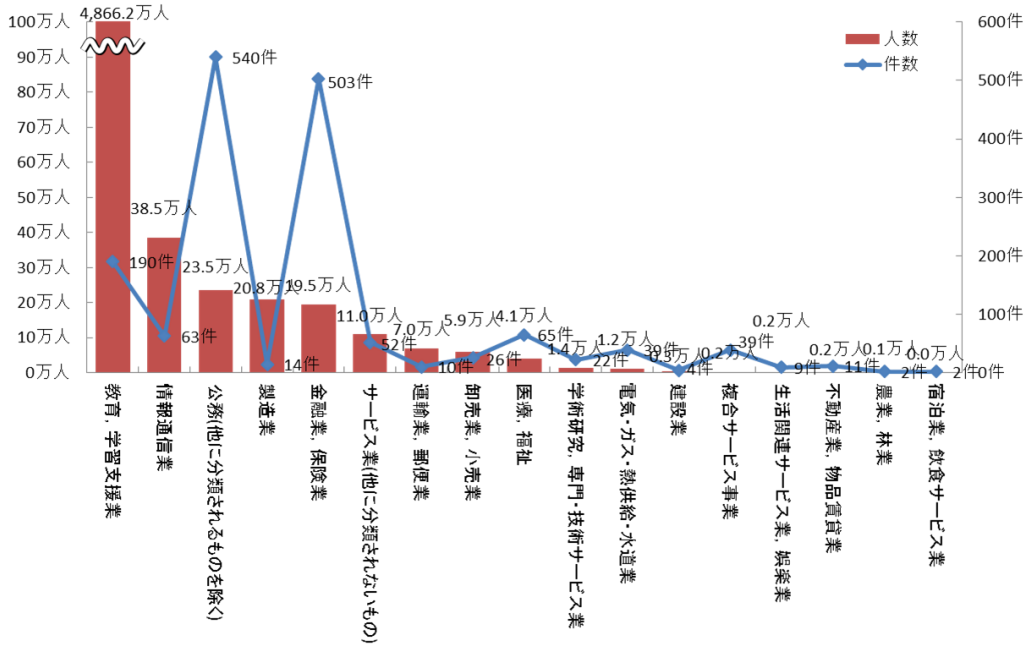

図 3-9：業種別のインシデント件数と漏えい人数

業種別のインシデント件数と漏えい人数の関係を図 3-9 に示す。

大規模なインシデント１件の影響により、「教育，学習支援業」の人数が突出している。

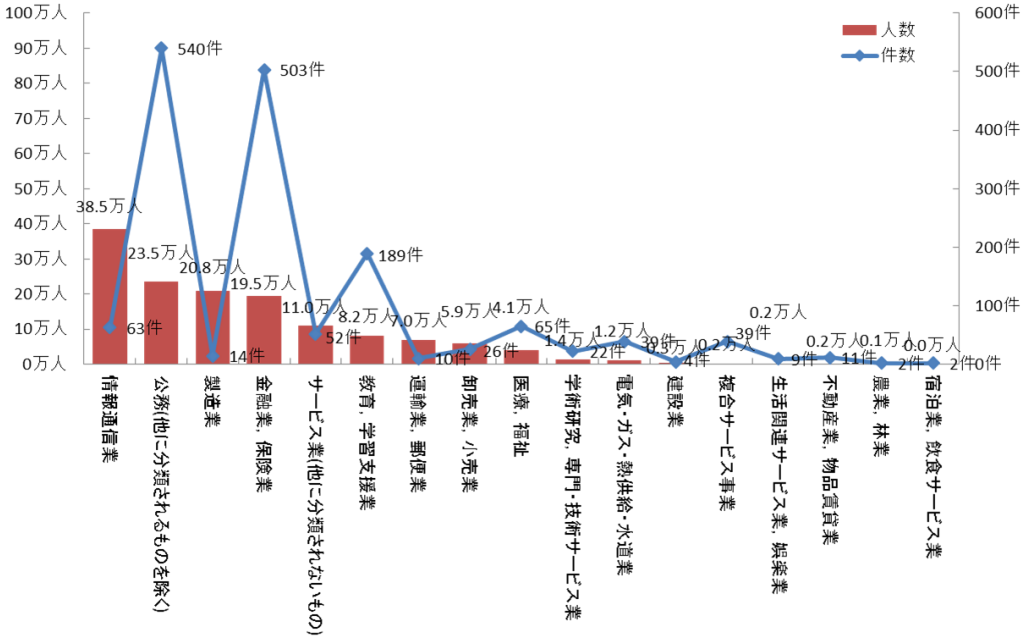

図 3-10：業種別のインシデント件数と漏えい人数

大規模なインシデント１件を除いた業種別のインシデント件数と漏えい人数の関係を図 3-10 に示す。

「情報通信業」は、インシデント件数が少なく漏えい人数が最も多い。「公務」や「金融業、保険業」は、インシデント件数が他の業種と比べて非常に多い。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である。

3.4 原因

(1) 単年分析(件数)

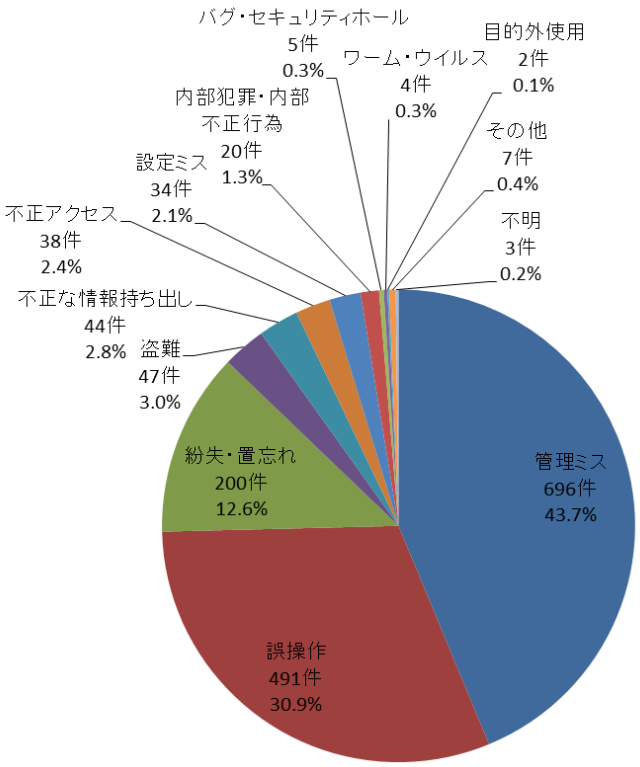

図 3-11：漏えい原因比率（件数）

個人情報漏えい件数の原因比率を図 3-11 に示す。

2014 年は「管理ミス」「誤操作」「紛失・置忘れ」で約 90%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。

(2)　経年分析(件数)

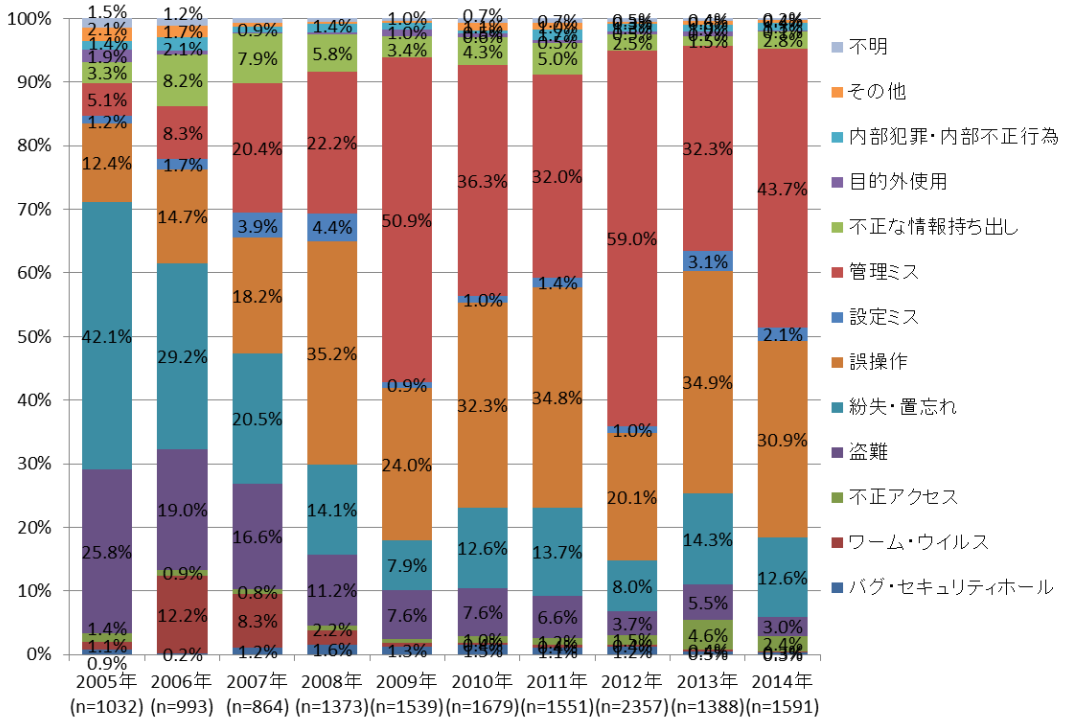

図 3-12：漏えい原因比率の経年変化（件数）

個人情報漏えい件数の原因比率の経年変化を図 3-12 に示す。

2014 年の原因比率は、2008 年以降の「管理ミス」「誤操作」「紛失・置忘れ」が上位を占める傾向と類似している。2008 年以降の変化に注目すると、2008 年と 2012 年は、他の年とくらべて「管理ミス」の割合が高く、それ以外の原因の割合がやや異なる。「管理ミス」の割合は、59.0%から 32.0%と変化の幅が大きい。「誤操作」の割合は 35.2%から 20.1%、「紛失・置忘れ」の割合は 7.9%から 14.3%と、「管理ミス」と比較して変化の幅は少ない。

(3)　単年分析(人数)

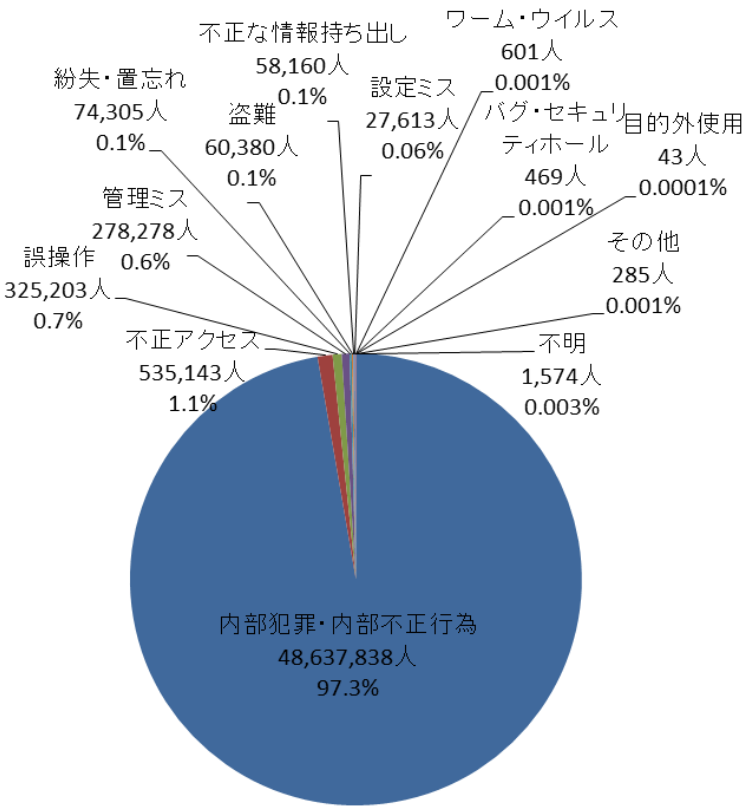

図 3-13：漏えい原因比率（人数）

個人情報漏えい人数の原因比率を図 3-13 に示す。

大規模なインシデント 1 件の影響により、「内部犯罪・内部不正行為」の人数が突出している。「内部犯罪・内部不正行為」や「不正アクセス」は例年、一件あたりの漏えい人数が多くなる傾向がある。

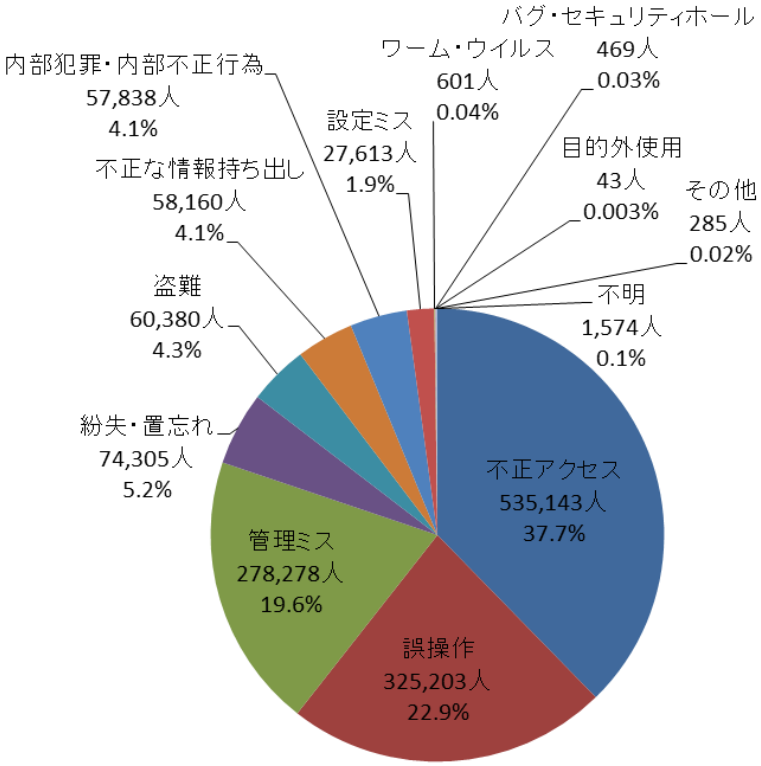

図 3-14：漏えい原因比率（人数）

大規模なインシデント 1 件を除いた個人情報漏えい人数の原因比率を図 3-14 に示す。

前述した漏えい件数の原因比率を表した図 3-11 と比べると、件数では 1.3%の「不正アクセス」が、漏えい人数の原因比率では 37.7%と突出している。「不正アクセス」は例年、一件あたりの漏えい人数が多くなる傾向がある。

続いて、インシデント件数が多い「誤操作」「管理ミス」「紛失・置忘れ」が、漏えい人数でも上位に並んでいる。「内部犯罪・内部不正行為」は、大規模なインシデント 1 件以外のインシデントは漏えい人数が多くなかったため、上位ではなかった。

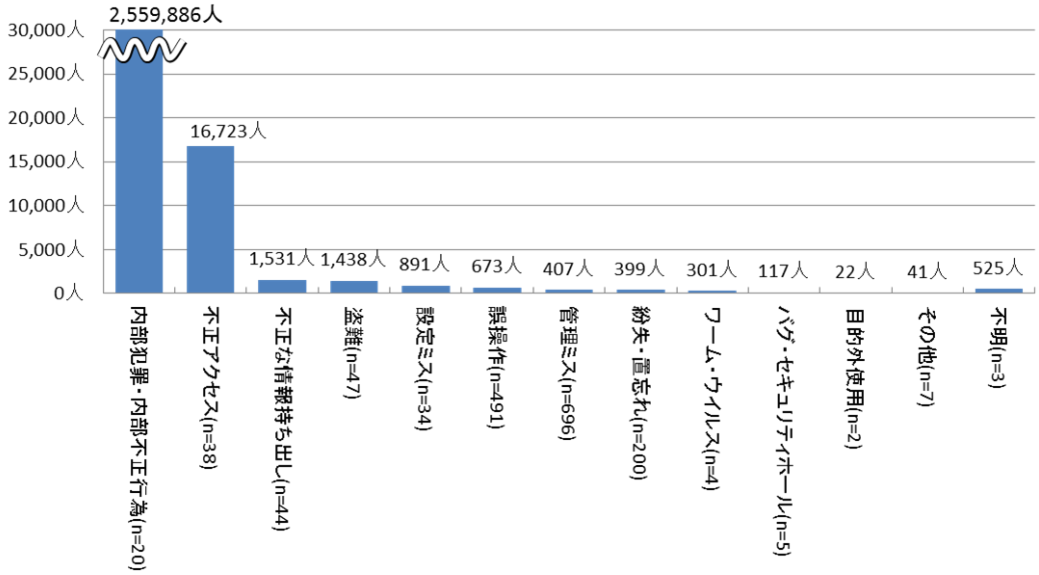

図 3-15：漏えい原因別の一件あたりの漏えい人数

漏えい原因別の一件あたりの漏えい人数を図 3-15 に示す。大規模なインシデント 1 件が影響し、「内部犯罪・内部不正行為」が突出している。

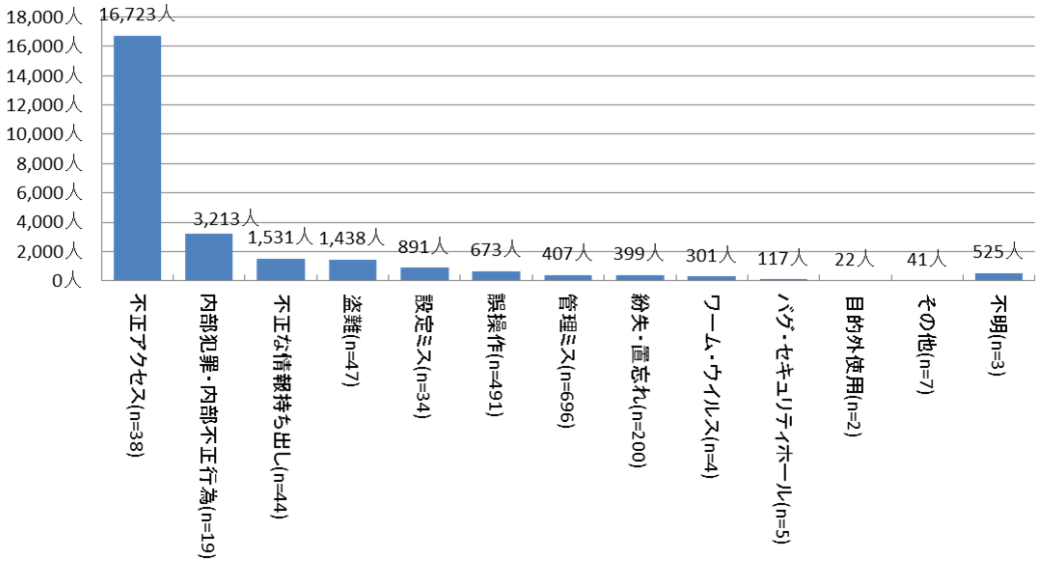

図 3-16：漏えい原因別の一件あたりの漏えい人数

大規模なインシデント 1 件を除いた業種別のインシデント件数と漏えい人数の関係を図 3-16 に示す。「不正アクセス」の一件あたりの漏えい人数が目立っている。「不正アクセス」は、3 件のインシデントがトップ 10 に入っているなど、漏えい人数が 1 万人以上のインシデントが約 3 分の 1 を占めている。悪意のある者による「不正アクセス」は、メールアドレスやアカウント情報の不正取得が目的のため、

発覚すると常にまとまった件数が漏えいしている。

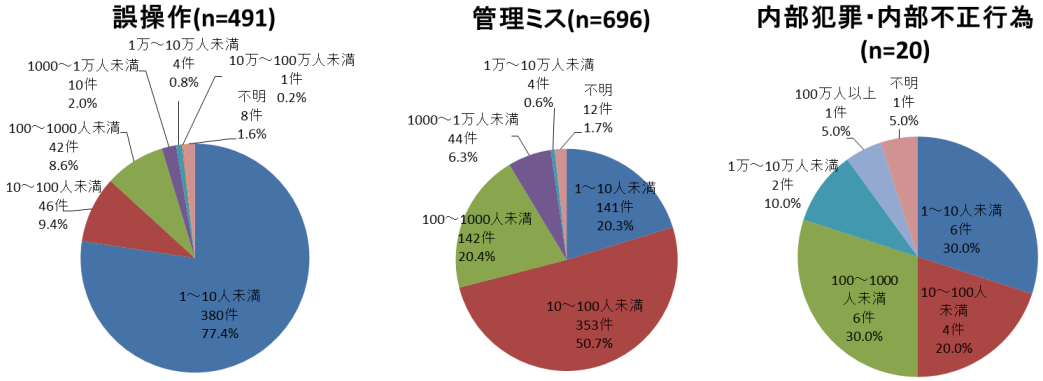

図 3-17：漏えい原因の人数区分（件数）

特徴的な漏えい人数区分を示す 3 つの原因を図 3-17 に示す。

漏えい件数が第 1 位の「管理ミス」は 10～100 人未満の情報漏えいインシデントが多い。漏えい件数が第 2 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。「内部犯罪・内部不正行為」は全体の件数が少なく、すべての人数区分でまんべんなくインシデントが発生している。全体のインシデント件数が少ないにも関わらず、100 万人以上のインシデントも 1 件発生している。

(4)　箱髭図(人数)

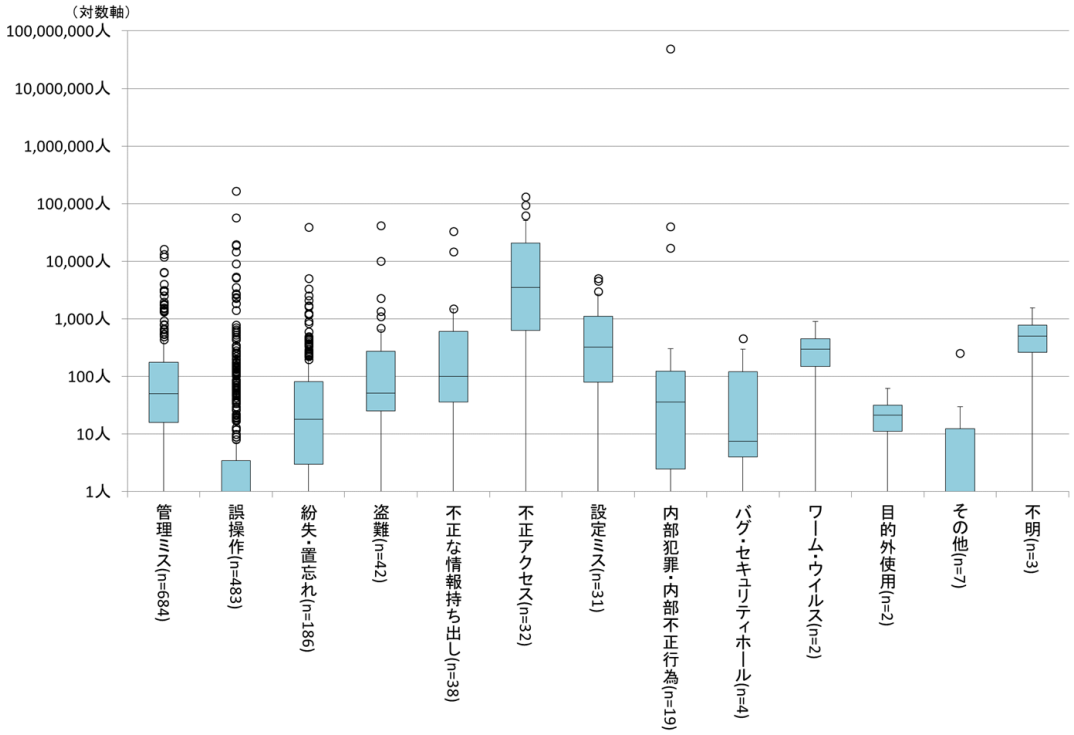

図 3-18：漏えい原因の漏えい人数（箱髭図）

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 3-18 に示す。他の原因と比べて「不正アクセス」は、箱の位置が 1000 人～1 万人とインシデントの規模が大きい。一方「誤操作」は、箱の位置が 10 人未満でインシデントの規模が小さい。「誤操作」と「内部犯罪・内部不正行為」は、外れ値が広く分布している。

(5)　業種別（件数）

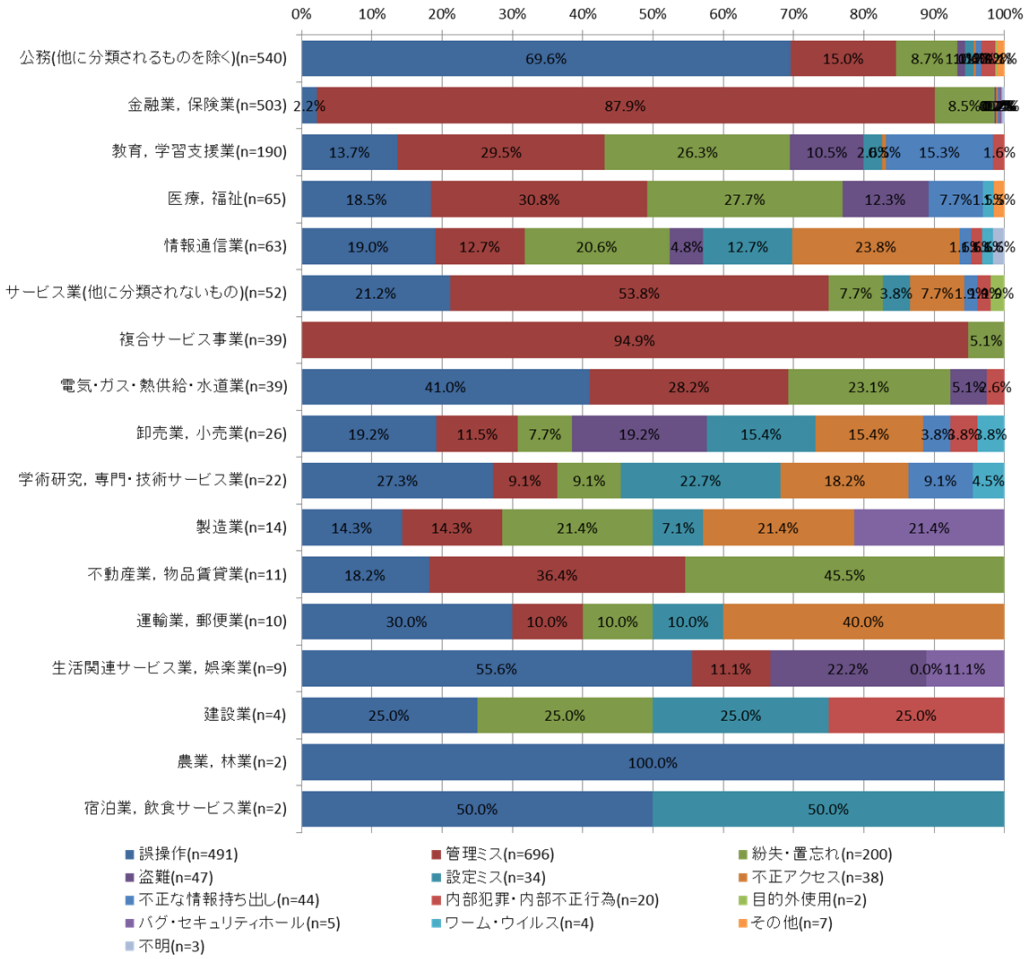

図 3-19：業種別の漏えい原因比率（件数）

業種別の漏えい原因比率を図 3-19 に示す。

「公務」と「生活関連サービス業，娯楽業」は、「誤操作」の占める比率が高い。公務の誤操作の原因の内訳は、紙媒体の送信が多い。公務における日常業務において、紙媒体の個人情報を取り扱う作業が多いことに起因していると推測される。

「金融業、保険業」と「複合サービス事業」は、「管理ミス」の占める比率が高く、約 90%を占める。管理ミスの原因の内訳も、紙媒体の誤廃棄が多い。「情報通信業」と「運輸業，郵便業」は「不正アクセス」の比率が高い。「教育，学習支援業」は「不正な情報持ち出し」が最も多い業種である。「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、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が考えられる。

3.5　漏えい媒体・経路

(1)　単年分析(件数)

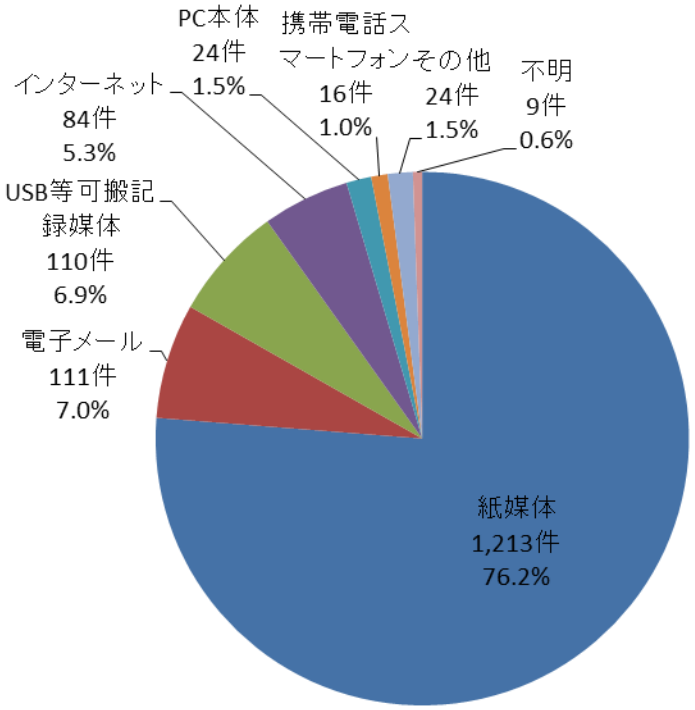

図 3-20：漏えい媒体・経路（件数）

漏えい媒体・経路別のインシデント件数を図 3-20 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 76.2%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「電子メール」が 7.0%、「USB 等可搬記録媒体」が 6.9%を占める。

(2)　経年分析(件数)

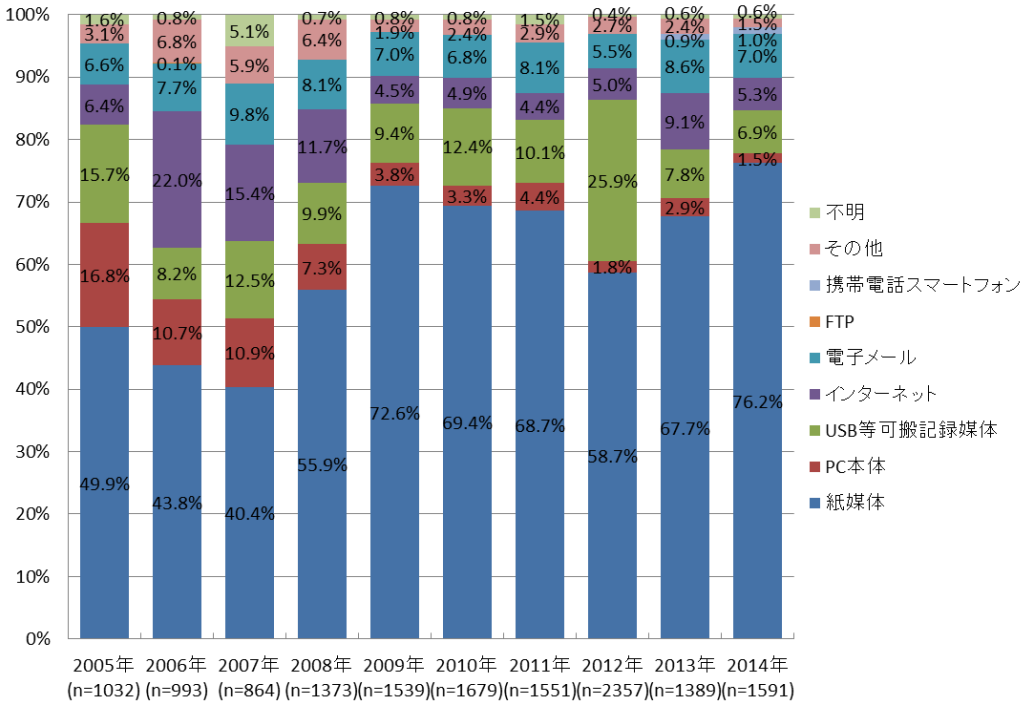

図 3-21：漏えい経路比率の経年変化（件数）

漏えい経路比率の経年変化について図 3-21 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、2012 年から 2014 年にかけて増加している。「紙媒体」の次に高い割合となったのは「電子メール」と「USB 等可搬記録媒体」で約 7%である。「USB 等可搬記録媒体」は、割合の変動が大きい。「インターネット」経由の漏えい原因の内訳を見ると「不正アクセス」が約 44%を占める。「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）

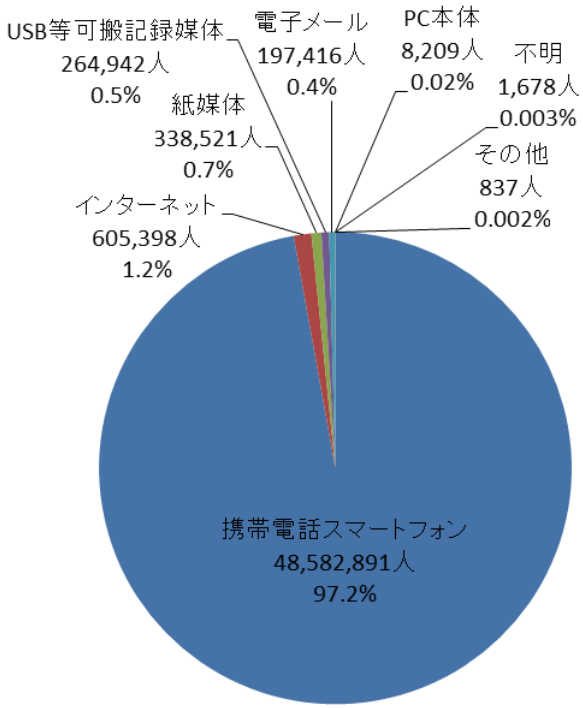

図 3-22：漏えい媒体・経路（人数）

漏えい媒体・経路別の漏えい人数を図 3-22 に示す。

大規模なインシデント 1 件の影響により、「携帯電話，スマートフォン」の占める割合が 97.2%と突出している。これまで「携帯電話，スマートフォン」によって漏えいした個人情報の人数は少なく、大規模インシデントの発生リスクとしては、あまり注目されていなかった。

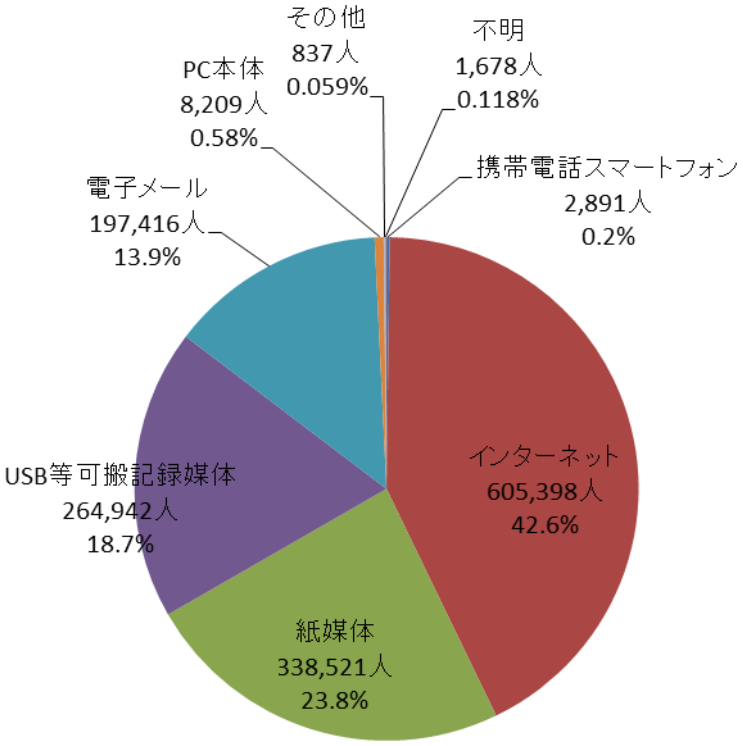

図 3-23：漏えい媒体・経路（人数）

大規模なインシデント 1 件を除いた漏えい媒体・経路別の漏えい人数を図 3-23 に示す。「インターネット」が 42.6%を占める。

例年は、「インターネット」のような電子データによる漏えい人数の占める割合が高いが、2014 年は「USB 等可搬記憶媒体」や「電子メール」よりも、「紙媒体」のほうが高い割合を占めた。

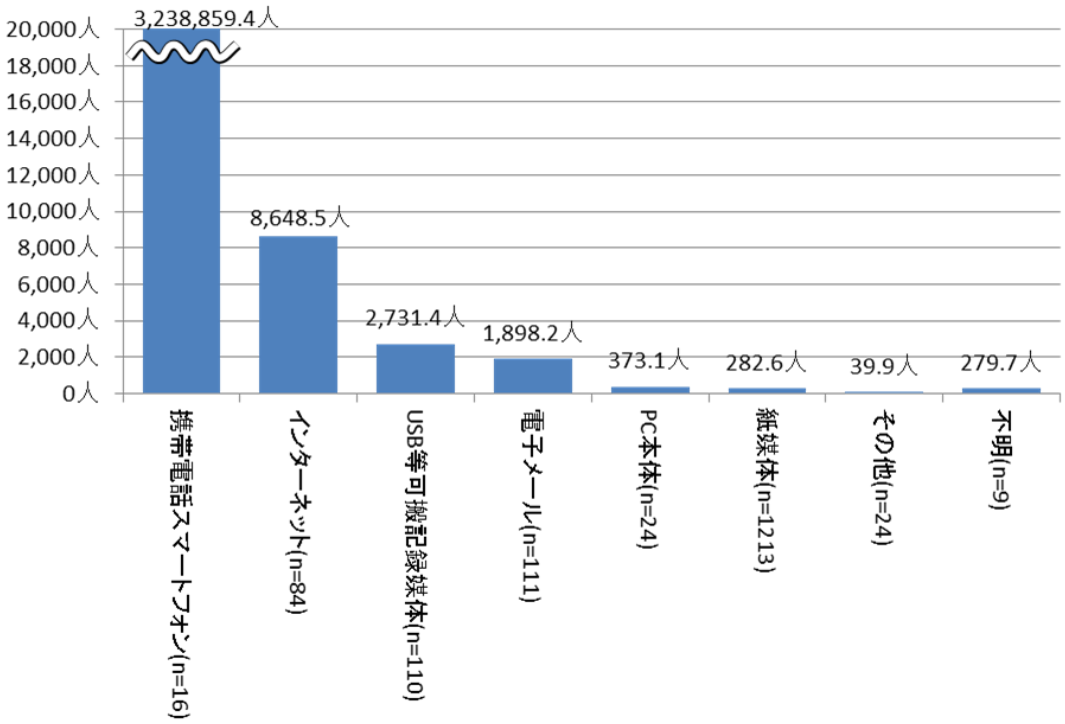

図 3-24：漏えい媒体・経路別の一件あたりの漏えい人数

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 3-24 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、大規模なインシデント 1 件の影響により、「携帯電話，スマートフォン」が突出して多い。

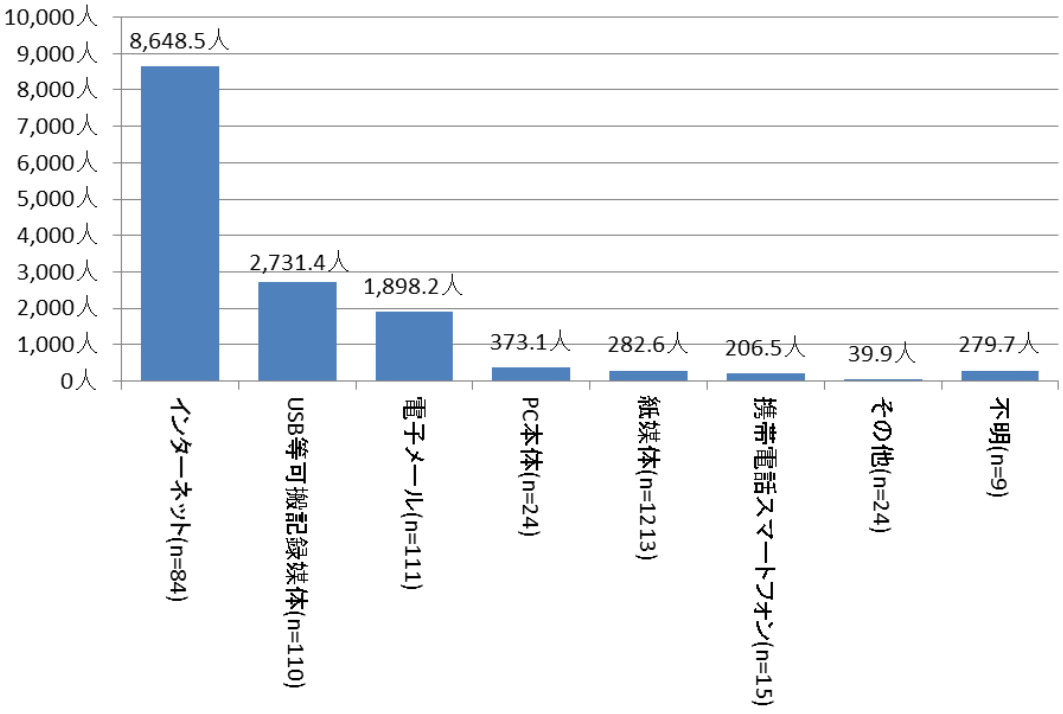

図 3-25：漏えい媒体・経路別の一件あたりの漏えい人数

大規模なインシデント 1 件を除いた漏えい媒体・経路別のインシデント一件あたりの漏えい人数を図 3-25 に示す。「インターネット」経由のインシデントが、1 件あたり 8648.5 人と最も多い。「インターネット」経由の漏えいのうち、人数が多いインシデントの原因は「不正アクセス」がほとんどを占める。

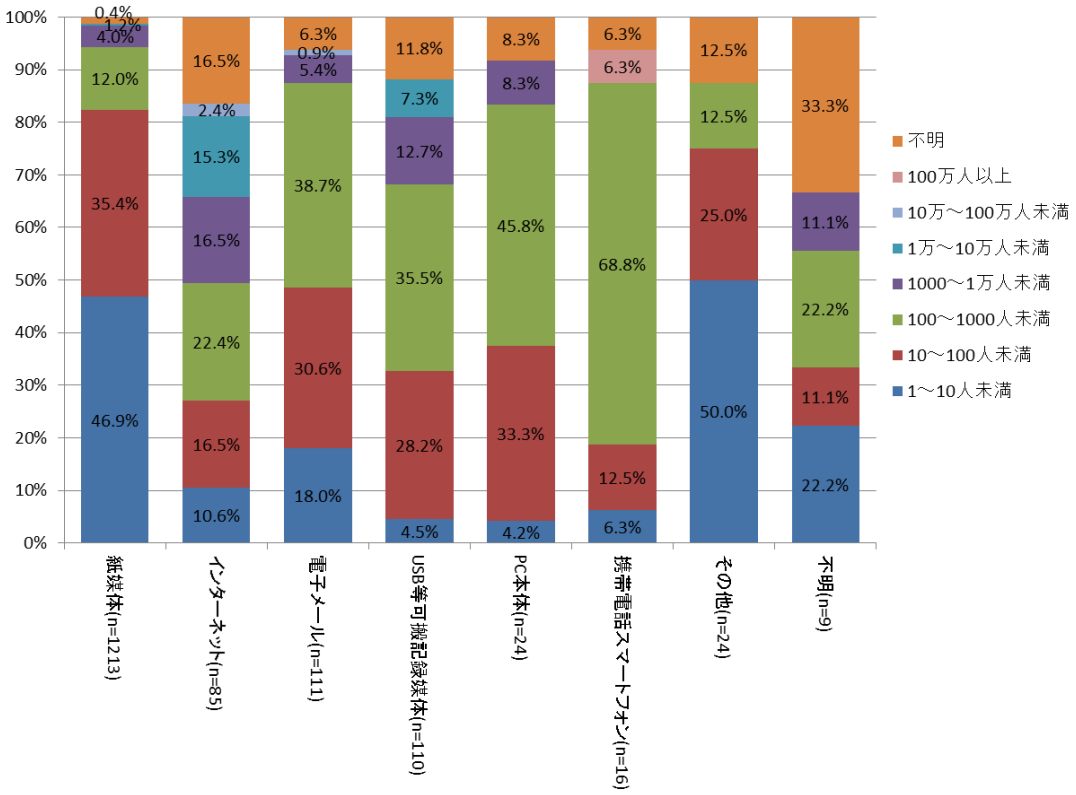

図 3-26：漏えい規模比率(件数)

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 3-26 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、1～10 人未満の小規模なインシデントの比率が高い。「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「紙媒体」の場合と異なる。「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」は、1 人以上～10 人未満の比率は低く、10 人以上～1000 人未満の比率が高い。「インターネット」は、1000 人未満のインシデント比率が約 50%未満と他と比べて低く、大規模のインシデントの比率が高い。

(4)　箱髭図(人数)

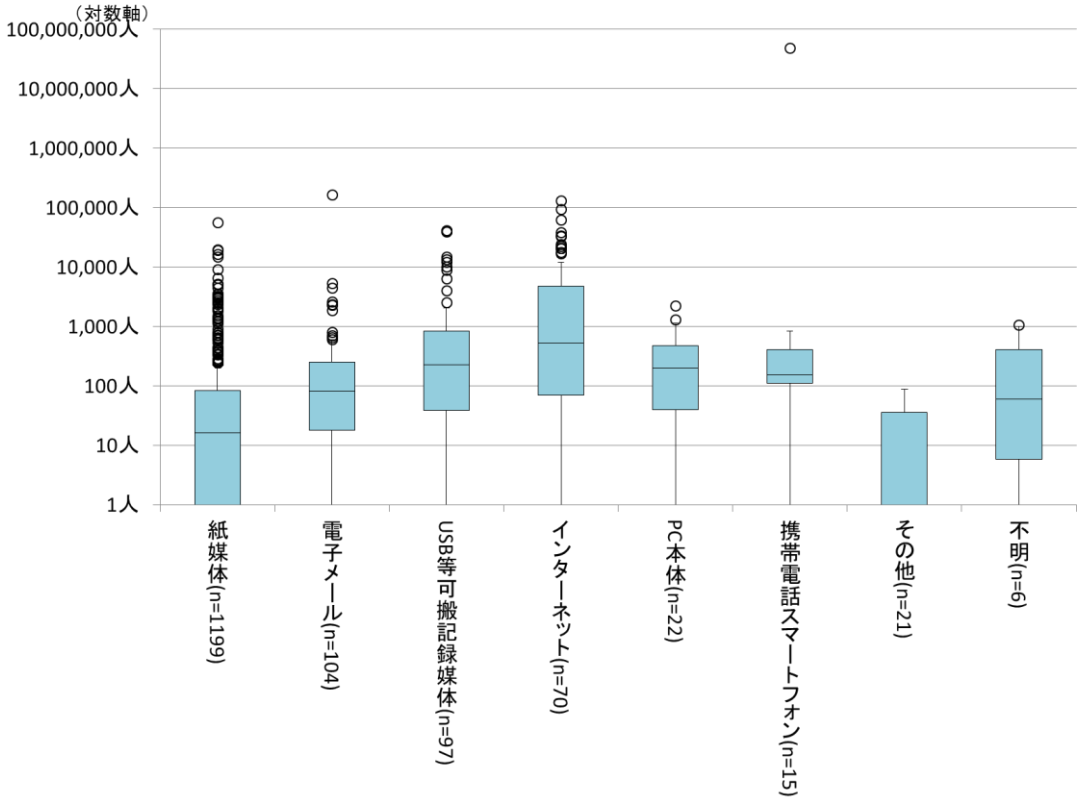

図 3-27：漏えい経路の漏えい人数（箱髭図）

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 3-21 に示す。「インターネット」経由の漏えいは、箱の部分が他の漏えい経路と比べて、若干、位置が高い。つまり、他の漏えい経路よりも漏えい人数がやや多い。「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、漏えい人数が少なく、1 件あたりの漏えい人数が 1 人～1000 人未満の広い範囲に分布している。

(5)　業種別（件数）

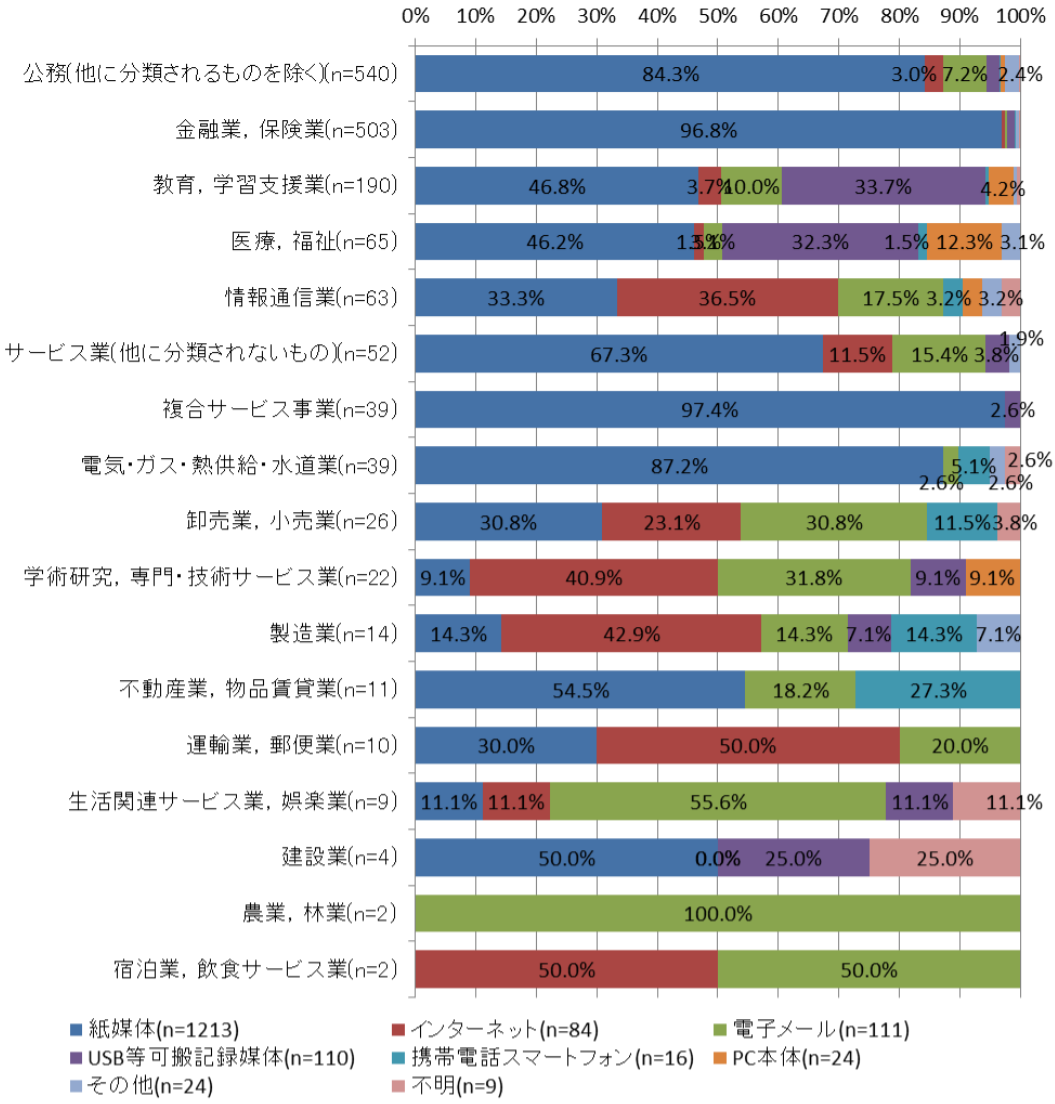

図 3-28：業種別の漏えい経路比率（件数）

漏えい媒体・経路の業種別比率（件数）について図 3-28 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、特に「公務」「金融業,保険業」「複合サービス事業」「電気・ガス・熱供給・水道業」において占める割合が高い。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。「情報通信業」「学術研究,専門・技術サービス業」「製造業」「運輸業，郵便業」「宿泊業,飲食サービス」は「インターネット」の割合が 30%以上を占めている。「卸売業,小売業」「学術研究,専門・技術サービス業」「生活関連サービス業,娯楽業」は「電子メール」の比率が高

く、「教育,学習支援業」と「医療,福祉」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。これは、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の違いによると思われる。

3.6　漏えい規模

(1)　単年

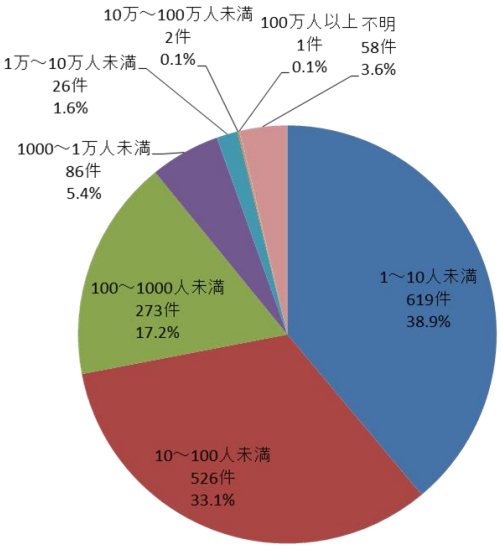

図 3-29：漏えい規模比率（件数）

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 3-29 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)

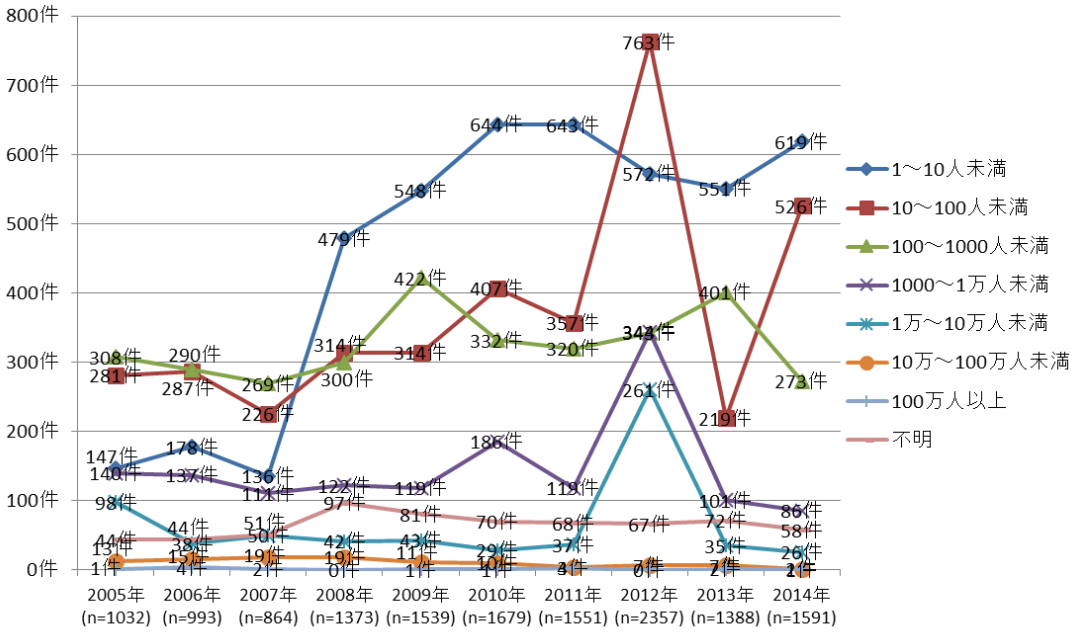

図 3-30：一件あたりの漏えい人数区分の経年変化（件数）

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 3-30 に示す。2012 年は、全体的に件数がイレギュラーである。2012 年以降は、10～100 人未満の件数の変化が大きい。2014 年は、100～1000 人未満の件数が減少し、10～100 人未満の件数が大きく増加している。

(3)　業種別（件数）

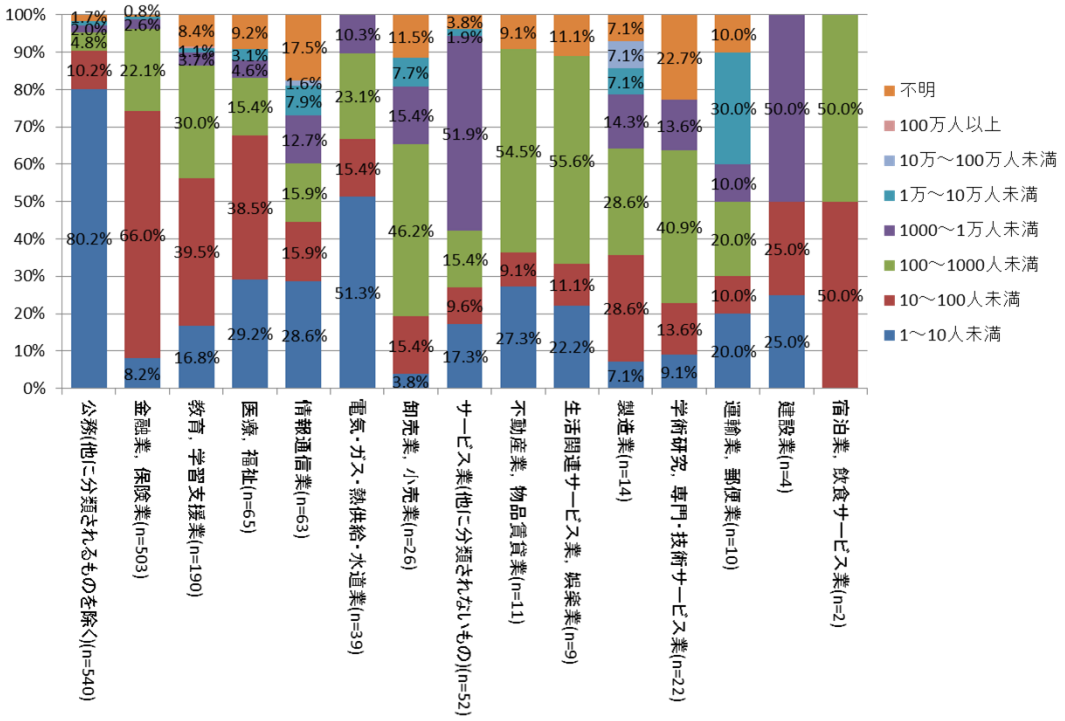

図 3-31：業種別の漏えい規模比率（件数）

業種別の漏えい規模（件数）の比率を図 3-31 に示す。「1～10 人未満」の小規模なインシデントは「公務」「電気・ガス・熱供給・水道業」で割合が高い。また「金融業，保険業」は「10～100 人未満」の割合が高い。「卸売業，小売業」「不動産業，物品賃貸業」「生活関連サービス業,娯楽業」「宿泊業,飲食サービス業」は「100～1000 人未満」の割合が高い。「サービス業」「建設業」は、「1000～1 万人未満」の割合が高い。

3.7　漏えい情報の価値

(1)　漏えい情報

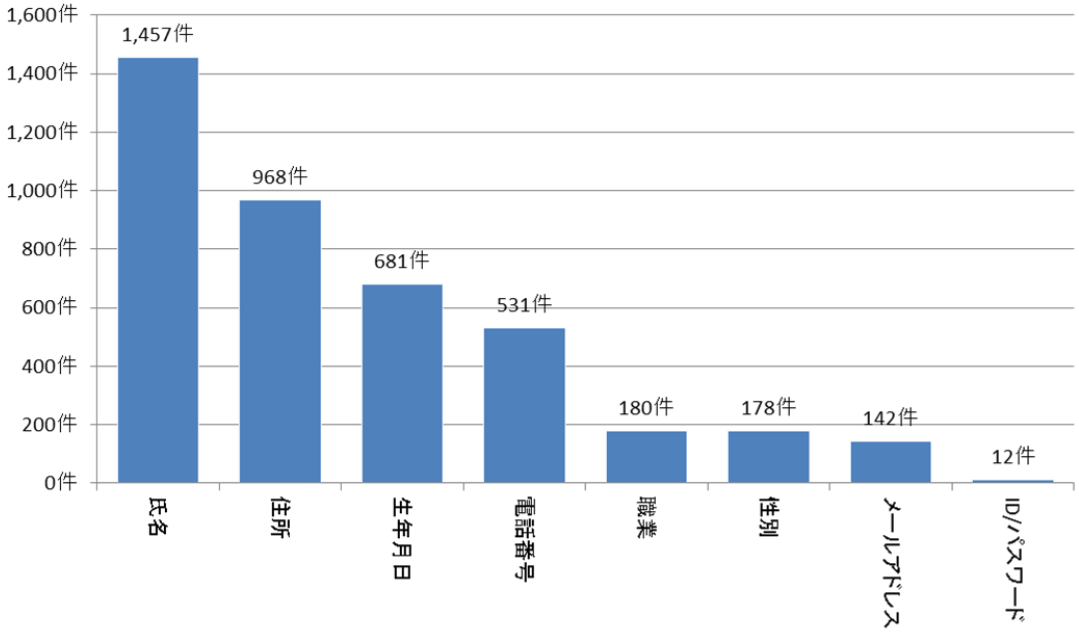

図 3-32：漏えい情報の出現確率

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	1,457 件	91.6%
住所	968 件	60.8%
生年月日	681 件	42.8%
電話番号	531 件	33.4%
性別	180 件	11.3%
職業	178 件	11.2%
メールアドレス	142 件	8.9%
ID/PASSWD	12 件	0.8%

漏えい情報の出現確率を図 3-32、表 3-3 に示す。

「氏名」の出現率が 91.6%で高く、次いで住所（60.8%）、生年月日（42.8%）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) 漏えい情報の価値分布(EP図)

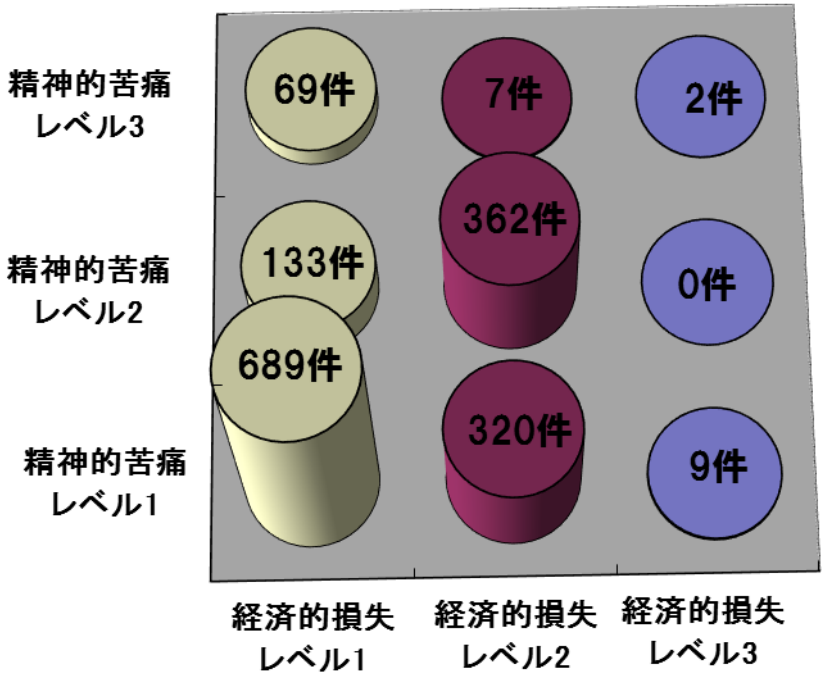

図 3-33：シンプル EP 図分布（件数）

2014 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 3-33 に示す。 シンプル EP 図については、P52～P53 を参照されたい。

2014 年の被害分布状況は、2013 年と比較して精神的苦痛と経済的損失がともにレベル 1 のフィールドの件数が減少し、かわって精神的苦痛または経済的損失のレベルのいずれかが 2 であるフィールドが増加した点である。

(2)　業種別EP分布

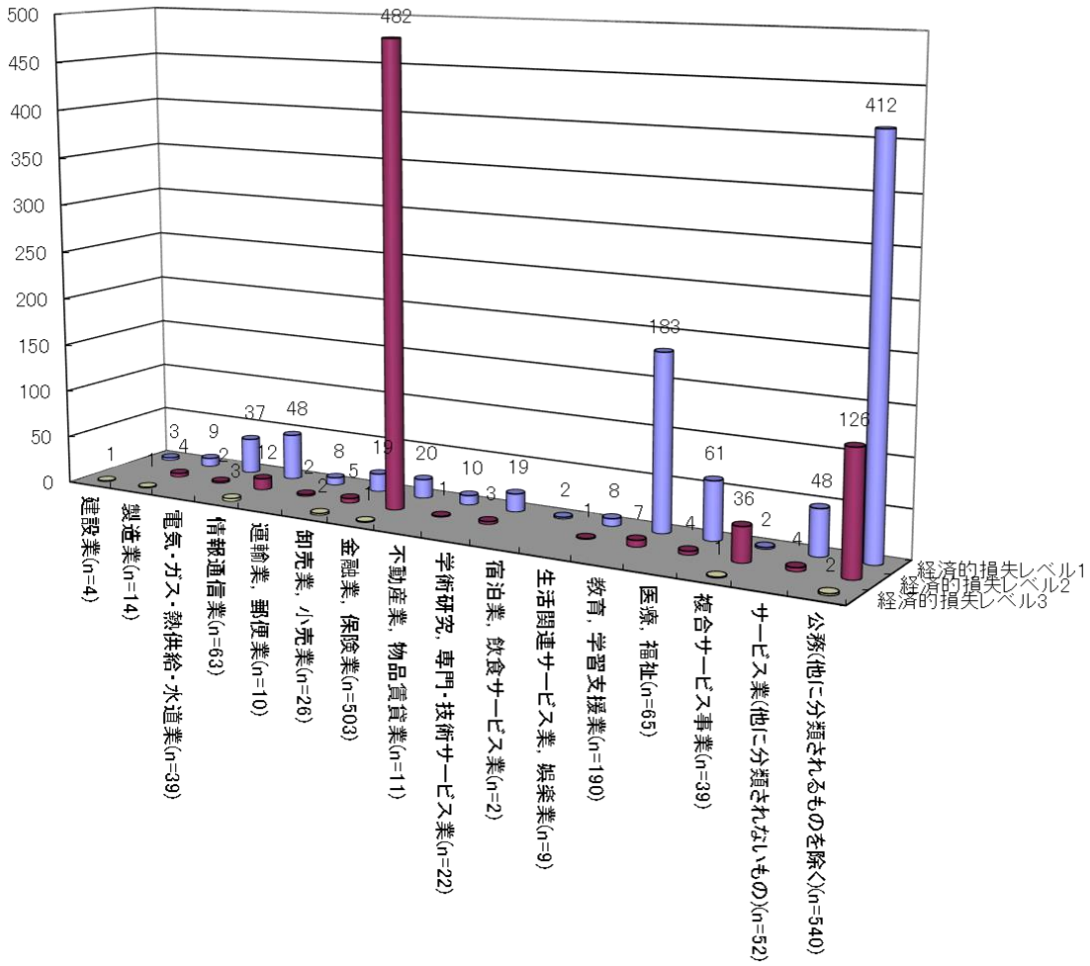

図 3-34：漏えい情報の経済的損失レベル分布（件数）

漏えい情報の経済的損失レベル分布（件数）を図 3-34 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，学習支援業」「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」が特出しているが、これは預金残高やクレジットカード情報等の情報漏えいが多いためと考えられる。

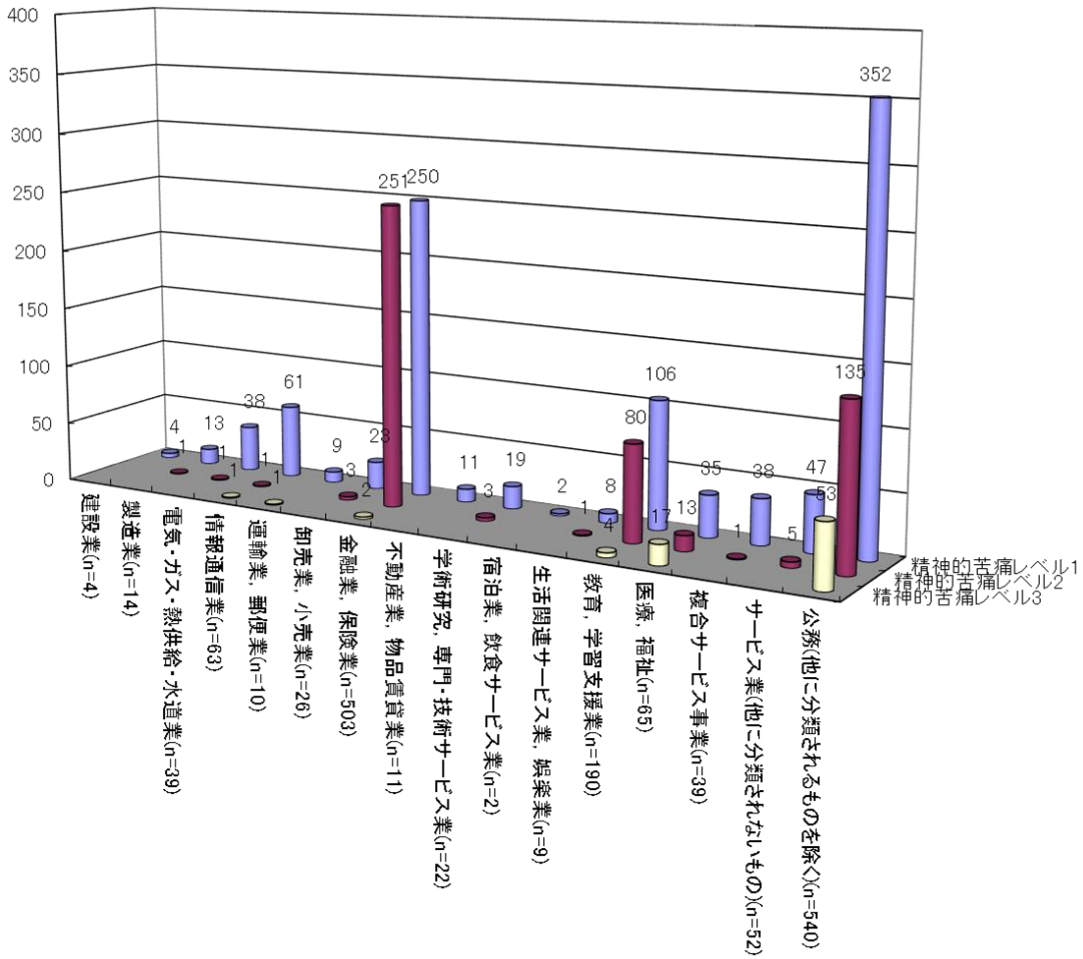

図 3-35：漏えい情報の精神的苦痛レベル分布（件数）

漏えい情報の精神的苦痛レベル分布（件数）を図 3-35 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、「金融業，保険業」「公務」「教育，学習支援業」である。「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の漏えいが多いためである。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 2014 年の間に収集した 10 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、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	3,698 人
2011 年	1,551 件	628 万 4,363 人	4,238 人
2012 年	2,357 件	972 万 65 人	4,245 人
2013 年	1389 件	925 万 4513 人	7027 人
2014 年	1591 件	4999 万 9892 人	3 万 2797 人

2014 年は 2013 年と比較して、インシデント件数がやや増加し、漏えい人数が大幅に増加した。これは、一件あたりの漏えい人数が 4000 万人を超える大規模なインシデントが 1 件発生したためである。

インシデント件数は、2013 年より増加した。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。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、2014 年が 1 件（4000 万人超）であった。

※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 2014 年は 1,591 件から被害者数不明の 58 件を除いた 1,539 件で漏えい人数を除算した。

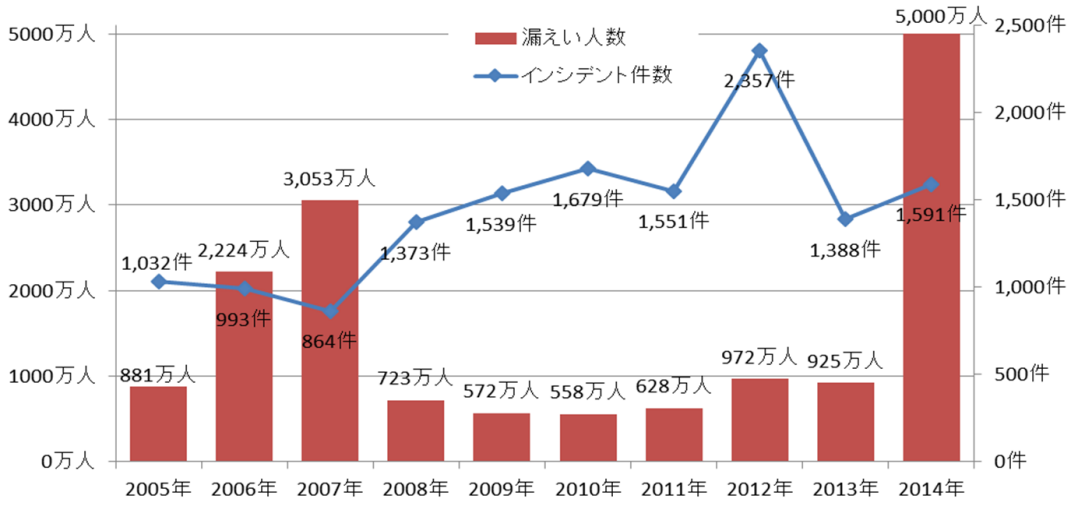

図 3-36：インシデント件数と漏えい人数の経年変化（合計）

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%
2014 年	96.7%	3.3%

内部犯罪・内部不正行為の漏えい人数の割合は、大規模なインシデントの影響によって変動し、その変動幅も大きい。2014 年の内部犯罪・内部不正行為の比率は 2013 年と比べて、正反対となった。

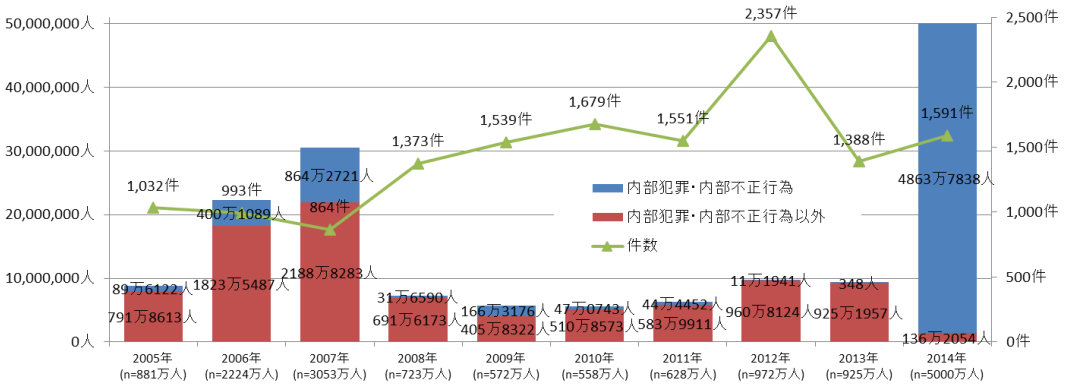

図 3-37：インシデント件数と内部不正による漏えい人数の経年変化（合計）

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 3-37 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、2014 年は 1,591 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 1,500 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 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 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　2014 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
2011 年	約 1,900 億円
2012 年	約 2,133 億円
2013 年	約 1,439 億円
2014 年	約 1 兆 6,642 億円

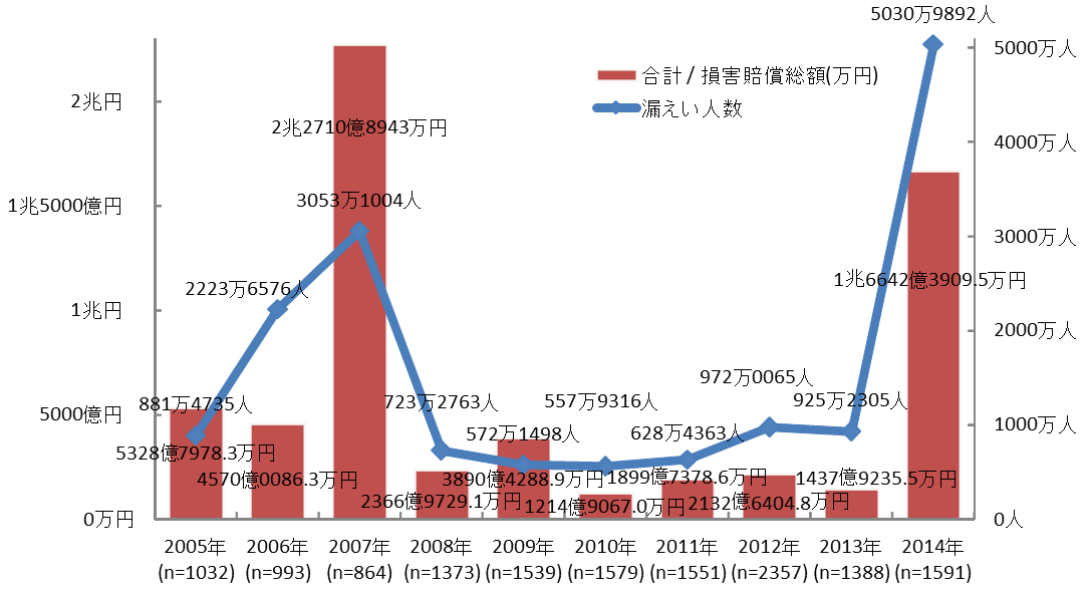

図 4-1：想定損害賠償総額と漏えい人数

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。2014 年は、漏えい人数、想定損害賠償総額とも、2013 年と比較して大幅に増加した。

4.2　一人あたりの想定損害賠償額

(1)　単年分析

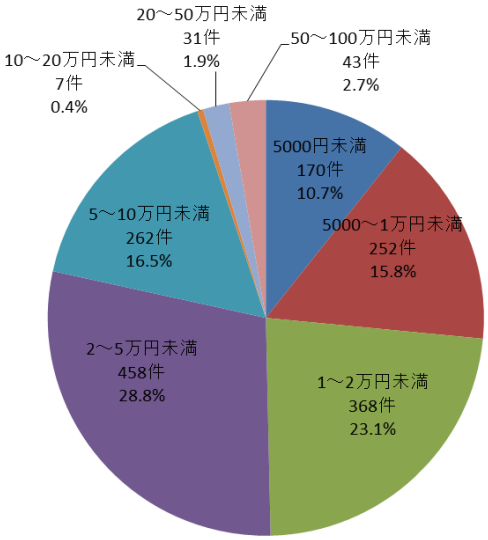

図 4-2：一人あたりの想定損害賠償額比率（件数）

一人あたりの想定損害賠償額を図 4-2 に示す。2014 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 29%と最も多く、次いで「1～2 万円未満」の区分の約 23%が続く。両区分を合わせると、半数以上（約 52%）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 6,743 円
2007 年	3 万 8,228 円
2008 年	4 万 3,632 円
2009 年	4 万 9,961 円
2010 年	4 万 2,662 円
2011 年	4 万 8,560 円
2012 年	4 万 4,628 円
2013 年	2 万 7,675 円
2014 年	5 万 2,625 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。

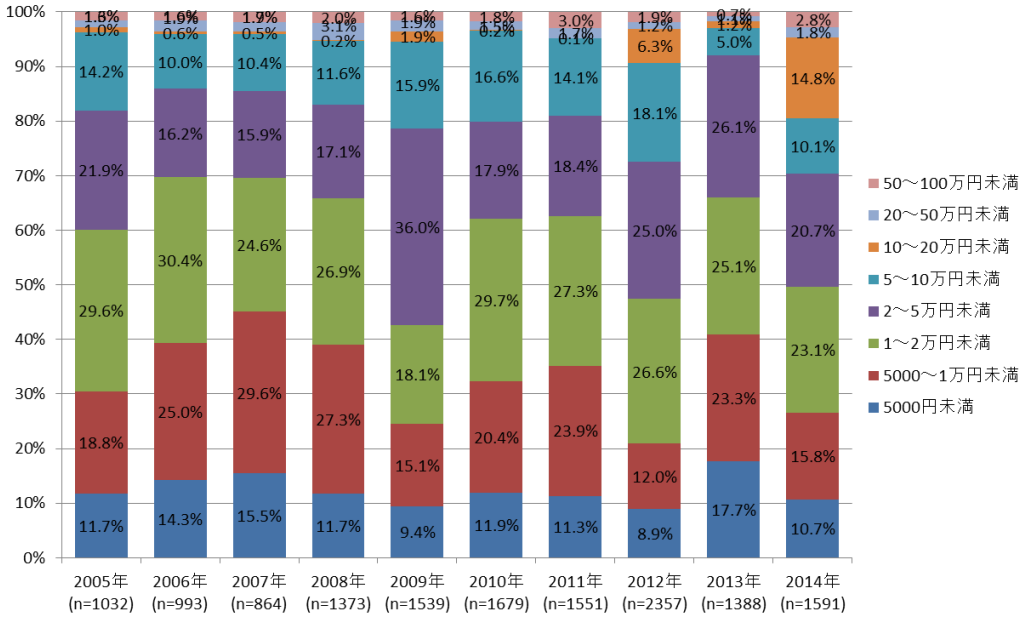

図 4-3：一人あたりの想定損害賠償額比率の経年変化（件数）

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。2014 年は、2013 年に比較して、5 万円以上の比率が増加した。特に「10～20 万円未満」の比率が増

加した。全体的に俯瞰してみると、2009 年と 2012 年以降に傾向が変化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

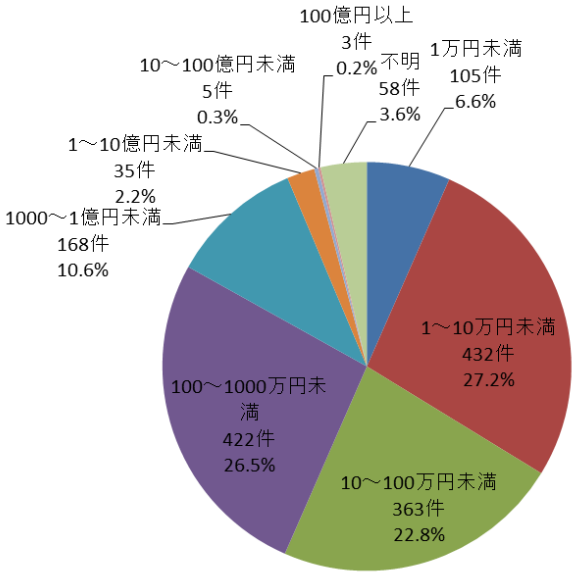

図 4-4：一件あたりの想定損害賠償額比率（件数）

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 27%である。また、2014 年は「1000 万円～1 億円未満」の比率が高くなっているが、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
2014 年	10 億 8561 万円	約 1 兆 6,642 億円

2014 年は、2013 年に比較して、想定損害賠償の総額、平均想定損害賠償額ともに大幅に増加した。これは、一件あたりの漏えい人数が 4000 万人を超える大規模なインシデントが 1 件発生したことによる影響である。

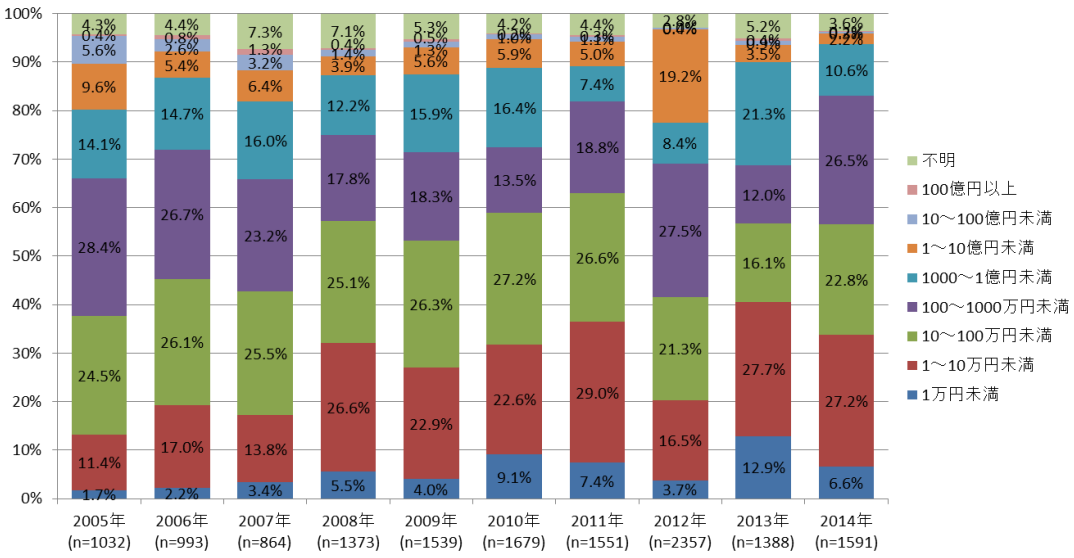

図 4-5：一件あたりの想定損害賠償額比率の経年変化（件数）

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。2014 年は、2013 年と比較して「10～100 万円未満」と「100～1000 万円未満」の比率が増加した。2008 年以降は、2012 年を除き 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、2014 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

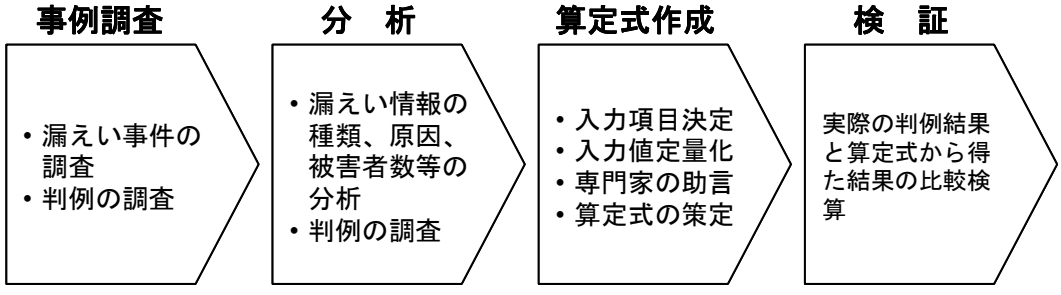

図 5-1：想定損害賠償額算定式策定のプロセス

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。2014 年の分析結果は「3. 2014 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。

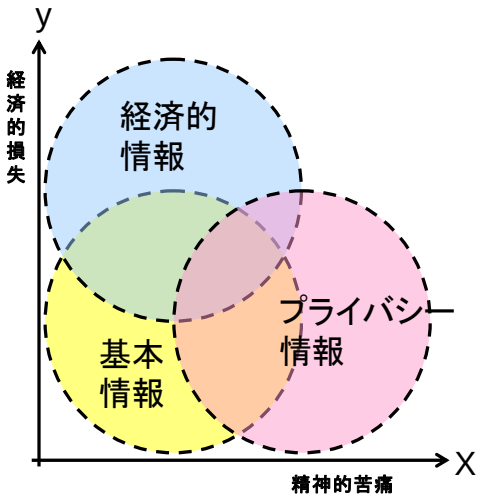

図 5-2：EP 図（Economic-Privacy Map）

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）」、「個人情報保護マネジメントシステム－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

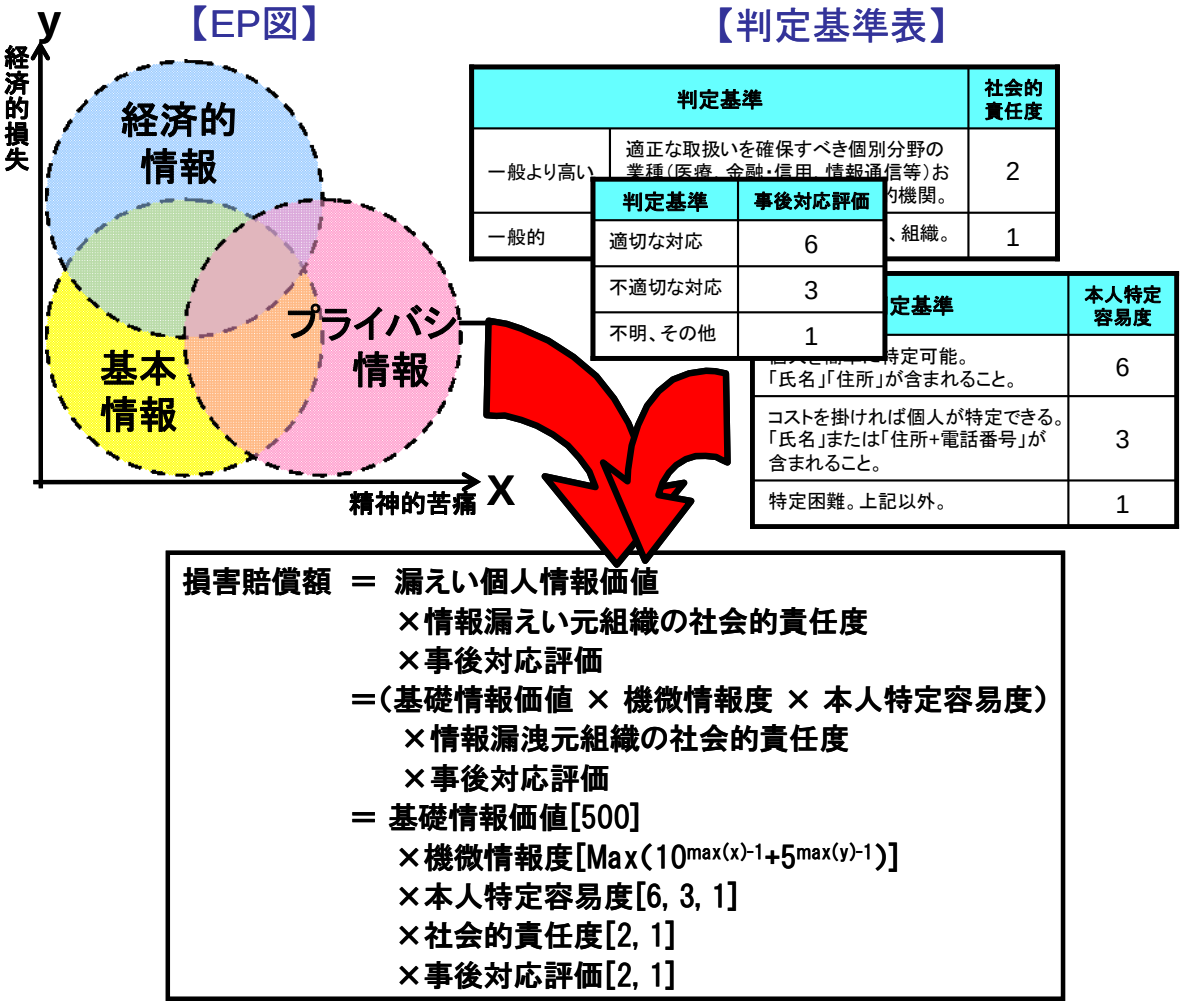

図 5-4：JO モデル

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

2014 年は、これまで個人情報漏えいインシデントの調査を行った中で、漏えい人数が最も多い。その原因は「内部犯罪・内部不正行為」であった。この「内部犯罪・内部不正行為」は、過去に発生した大規模インシデントの上位 10 件の原因のうち、最も多い 4 件を占める。いかに「内部犯罪・内部不正行為」が、大規模インシデント発生につながるリスクが高い原因であることがわかる。この「内部犯罪・内部不正行為」は、相変わらず対策が難しいリスクである。

また「携帯電話，スマートフォン」を経由して 4000 万人以上の個人情報が漏えいしたことも大きな特徴である。これまで「携帯電話，スマートフォン」に関係した個人情報漏えいインシデントは、「携帯電話，スマートフォン」自体の「紛失・置忘れ」が多く、「携帯電話，スマートフォン」を悪用したインシデントは注目されていなかった。スマートフォンの記憶容量が増加し、PC と容易に接続できるようになったことで、新たに発生したインシデントである。このように技術の進歩によって発生する新しいリスクも、セキュリティ対策を講じる際に考慮しなければならないポイントである。

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