2012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 7 月 7 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

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
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	デロイト トーマツ リスクサービス株式会社
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

※2013 年当時の所属

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
嶋作	泰洋	博士前期課程 1 年
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
菅原	尚志	客員研究員
鈴木	宏幸	客員研究員
高梨	智治	客員研究員
新原	功一	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

修了生

小野	康史	2008 年度 修了
髙津	岳志	2006 年度 修了

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、2012 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 2012 年のインシデントの集計・分析結果、及び過去 8 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。

本来、2013 年度中に発行すべき報告書だが、作業者の都合によりまる 1 年遅れとなってしまいました。期待してお待ちいただいていた皆様には大変申し訳ございませんでした。調査は今後とも継続してまいりますので、引き続き宜しくお願いいたします。

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、2012 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 2012 年の個人情報漏えいインシデントの分析結果」「第 4 章 2012 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 2012 年の個人情報漏えいインシデントの分析結果」では、2012 年の単年データの分析結果、および蓄積された 11 年間分のデータから 2005 年から 2012 年までの 8 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 2012 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

2012 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　2012 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、2357 件（前年比＋806 件）であった。2011 年より大幅に増加している。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、件数が多い。漏えい人数も、約 972 万人（前年比＋345 万人）と、2011 年よりも大きく増加したが、全体的には 2007 年以降減少傾向にある。これは、漏えい件数が増加する一方で、全インシデントのうち、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 2133 億円（前年比＋332 億円）となった。

漏えい原因※1は、「管理ミス」（1391 件）が一番多く、「誤操作」（474 件）、「紛失・置忘れ」（189 件）の 3 種類が大半を占めた。2012 年は、2011 年と比較して「管理ミス」の割合が増加し「誤操作」の割合が減少した。また、2012 年は 100 万人以上の大規模なインシデントが発生しなかったが、「金融業，保険業」の漏えい人数が突出した結果となっている。

2012 年の集計結果の概要データは、以下の通りである。

表 3-1：2012 年 個人情報漏えいインシデント 概要データ

漏えい人数	**972 万 65 人**
インシデント件数	**2357 件**
想定損害賠償総額	**2132 億 6405 万円**
一件あたりの漏えい人数※2	**4245 人**
一件あたりの平均想定損害賠償額※2	**9313 万円**
一人あたりの平均想定損害賠償額※3	**4 万 4628 円**

※1 図 3-9：漏えい原因比率（件数）参照
※2 平均値は、被害者数が不明のインシデント 67 件を除いて算出している。
※3 この値は、インシデントごとに一人あたりの想定損害賠償額を推定し、その後、全てのインシデントの一人あたりの想定損害賠償額を用いて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。

近年は、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の発生件数が少なく、2009 年と 2010 年は 1 件、2011 年は 3 件、2012 年は発生しなかった。

インシデント・トップ 10 の原因は「管理ミス」が多いが、「不正アクセス」「不正な情報持ち出し」「内部犯罪・内部不正行為」といった故意を含んだ原因も目立っている。業種は、「金融業，保険業」が多い。

表 3-2：インシデント・トップ 10

No.	漏えい人数	業種	原因
1	76 万人	情報通信業	設定ミス
2	40 万 6632 人	金融業，保険業	管理ミス
3	17 万 1518 人	情報通信業	不正アクセス
4	12 万 4471 人	金融業，保険業	管理ミス
5	12 万 1191 人	公務(他に分類されるものを除く)	不正な情報持ち出し
6	11 万人	サービス業(他に分類されないもの)	不正アクセス
7	10 万人	金融業，保険業	管理ミス
8	9 万 6000 人	金融業，保険業	管理ミス
9	9 万 5689 人	製造業	内部犯罪・内部不正行為
10	8 万人	運輸業，郵便業	管理ミス

3.3　業種

(1)　単年分析(件数)

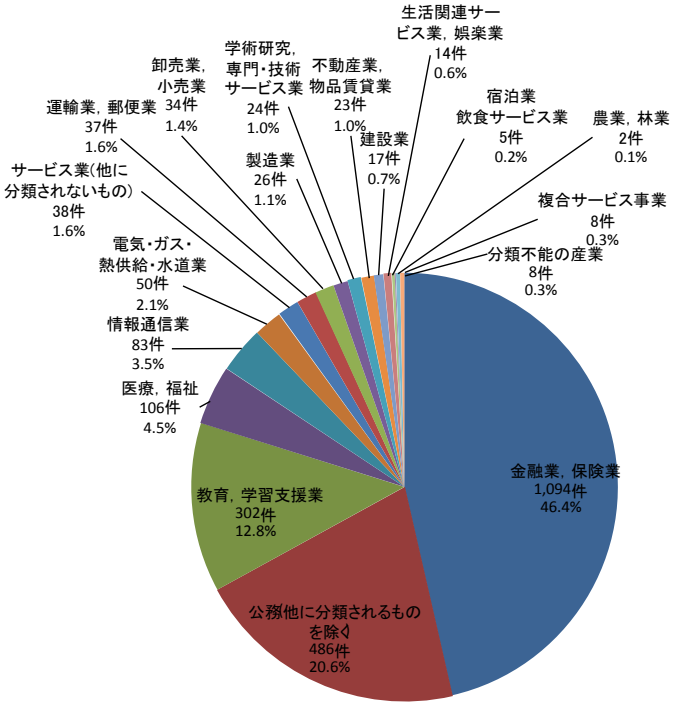


図 3-1：業種別比率（件数）

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「金融業，保険業」(46.4%)、「公務」(20.6%)、「教育，学習支援業」(12.8 %)であり、全体の約 80%を占めている。

「公務」および「金融業，保険業」は、2004 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。また「教育，学習支援業」「医療，福祉」も 2007 年以降、順位を上げてきており、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「漁業」「鉱業，採石業，砂利採取業」の 2 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)

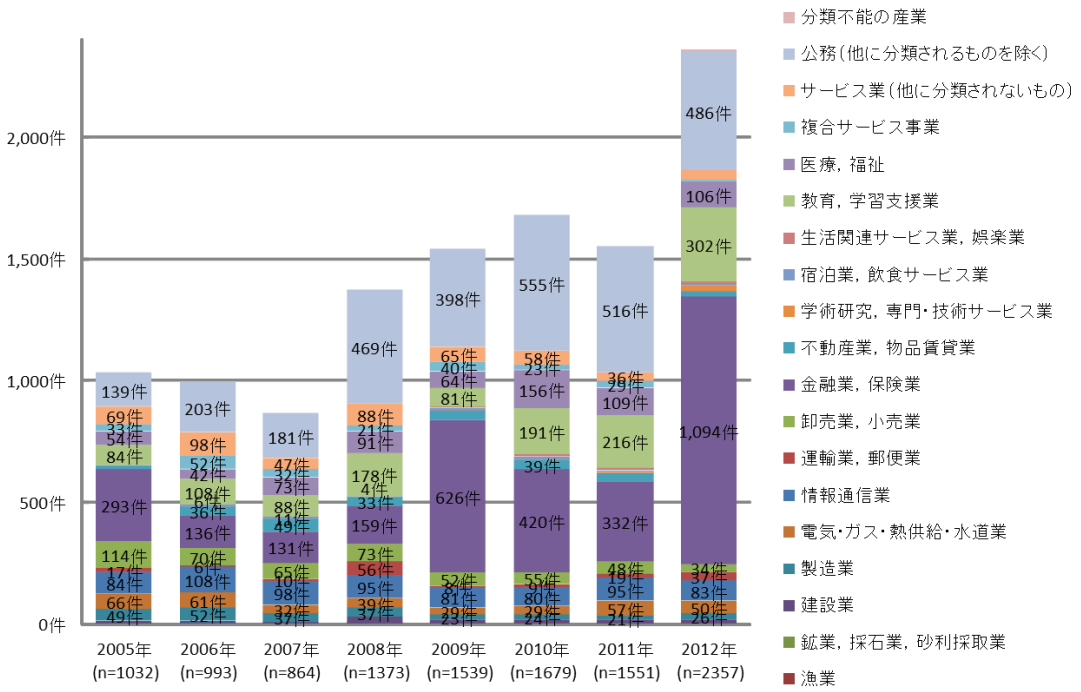


図 3-2：業種別件数の経年変化（件数）

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 年にインシデント件数が大きく増加した「金融業，保険業」は、2012 年も大幅に増加している。これは 2012 年に複数の金融機関から、多数の支店でのコムフィッシュ*等帳票の紛失が公表されたことが影響している。

「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、増加している。「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、教育用だけでなく校務用で PC や USB メモリなどの使用が増加していることが原因であると推定される。

*情報保存媒体として使用されるシート状の薄膜フィルム

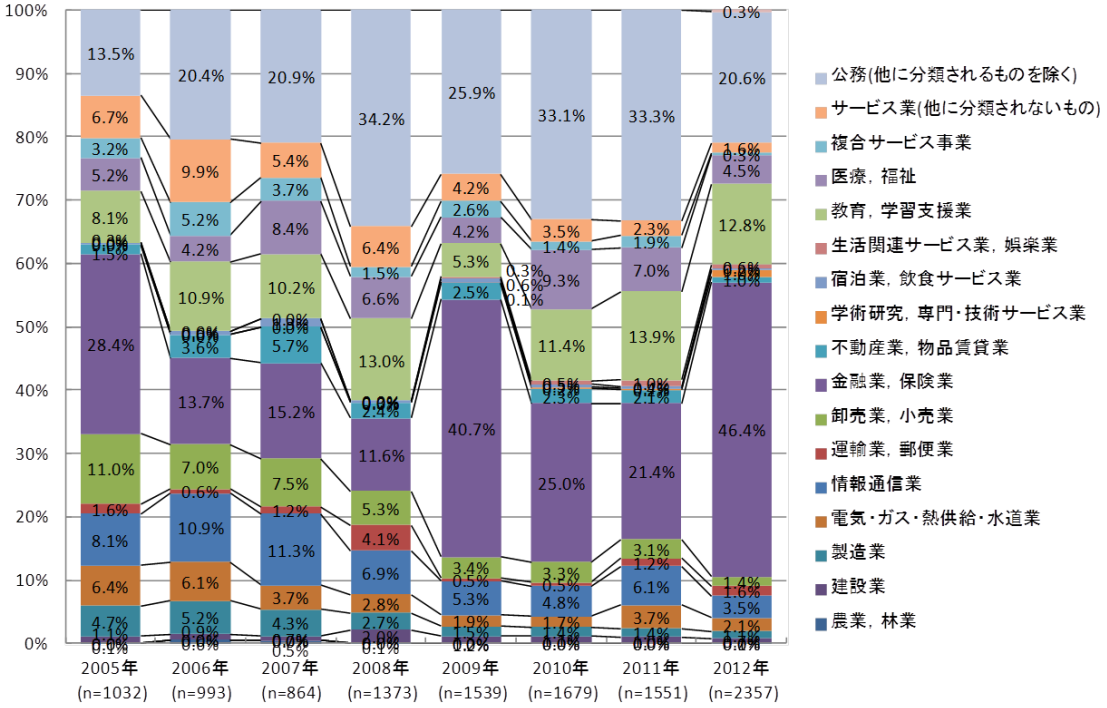


図 3-3：業種別比率の経年変化（件数）

業種別インシデント件数の比率の推移を図 3-3 に示す。「サービス業」「卸売業，小売業」「情報通信業」「製造業」の割合が徐々に減少している。継続的に情報漏えい対策が行われていると思われる。

(3)　単年分析(人数)

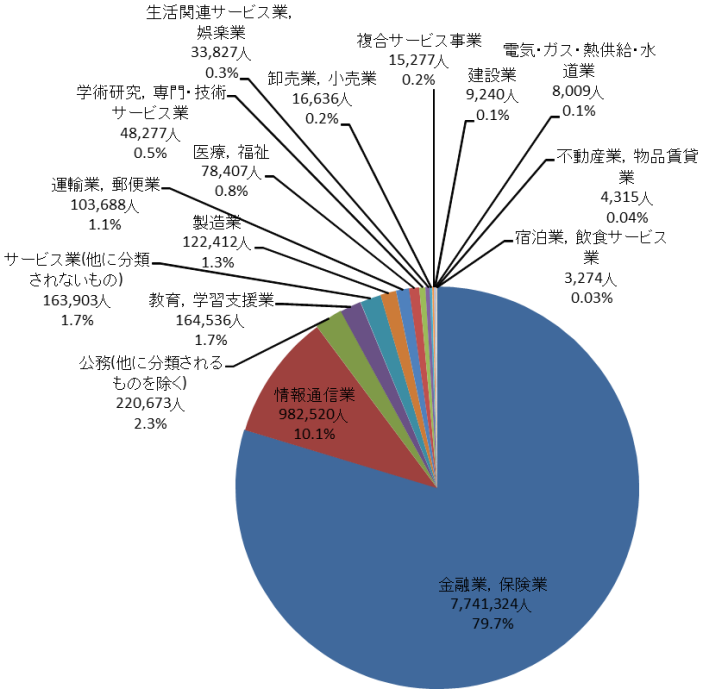


図 3-4：業種別比率（人数）

業種別での個人情報の漏えい人数をその比率を図 3-4 に示す。上位から順に「金融業，保険業」「情報通信業」の漏えい人数が前年に比べて大幅に増加しているが、この原因は特定の金融機関から、240 店において合計 560 万人分の個人情報が記録されたコムフィッシュの誤廃棄が公表されたことによる。「公務」と「教育，学習支援業」の合計値は、図 3-1 の件数比率では 33.4%を占めるが、図 3-4 の人数比率では 4.0%と少ない。これは、「公務」は住民票の交付など 1 人単位、「教育，学習支援業」はクラス単位など、一度に扱う個人情報の数が少なく、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。

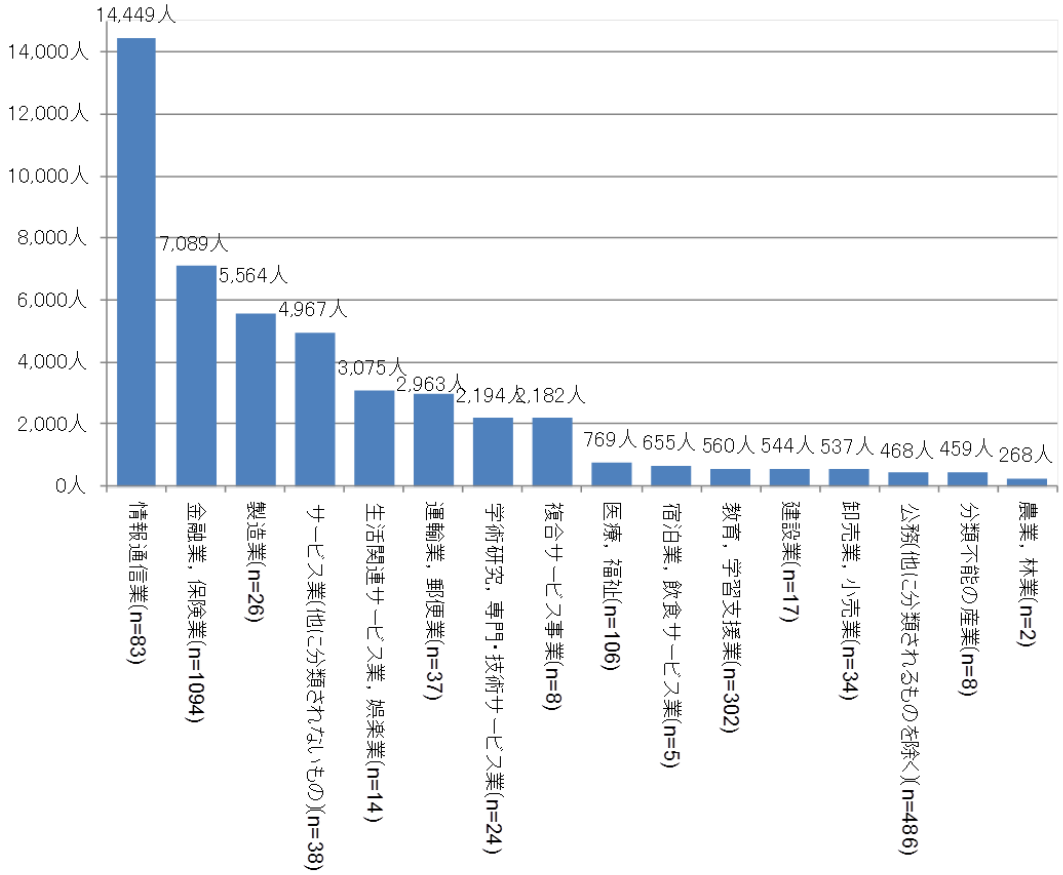


図 3-5：業種別の一件あたりの漏えい人数

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。「情報通信業」（約 14,000 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 位と 3 位が情報通信業であり、これが平均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「金融業，保険業」（約 7,000 人）、「製造業」（約 5,500 人）となっている。

インシデントの件数が上位の「公務」は 468 人、「教育，学習支援業」は 560 人だった。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 486 件のうち、330 件(67.9%)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・誤送付によるものであった。

(4)　箱髭図(人数)

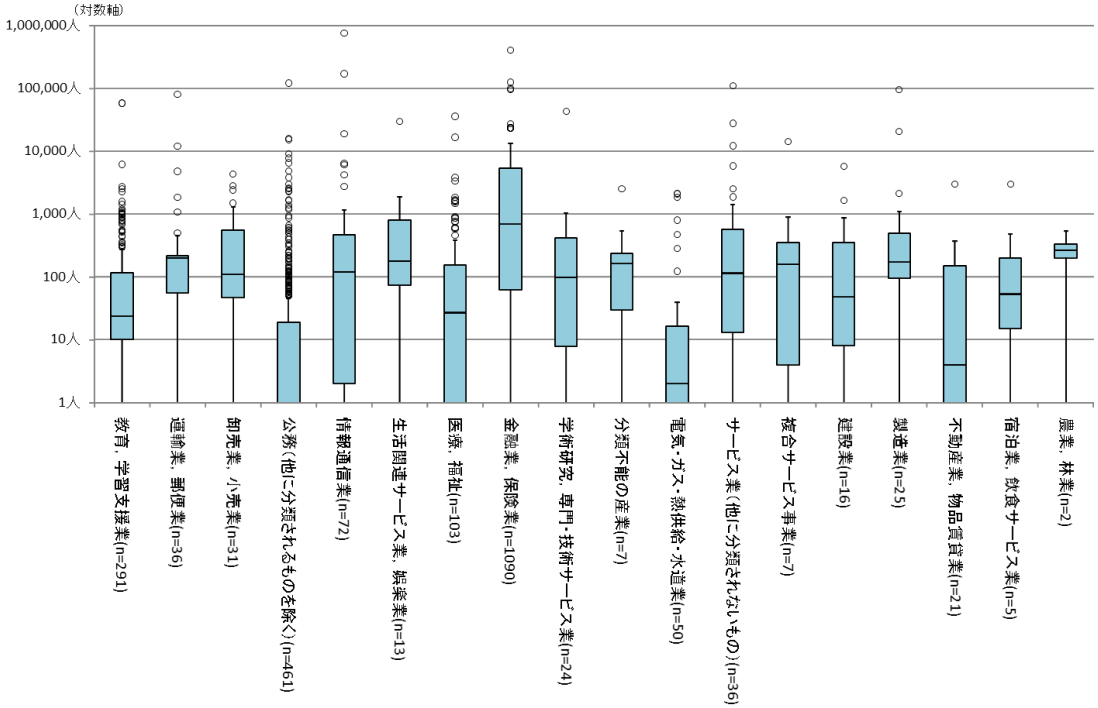


図 3-6：業種別の漏えい人数（箱髭図）

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*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」「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、箱髭図の箱の部分の位置から、1 件あたりの漏えい人数が 100 人から 1 万人と他の業種と比較して特に多いことがわかる。「製造業」と「生活関連サービス業，娯楽業」も漏えい人数が 100 人から 1000 人程度と比較的規模が大きい。

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。

---

* 箱髭図の箱の下辺は第 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。箱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)

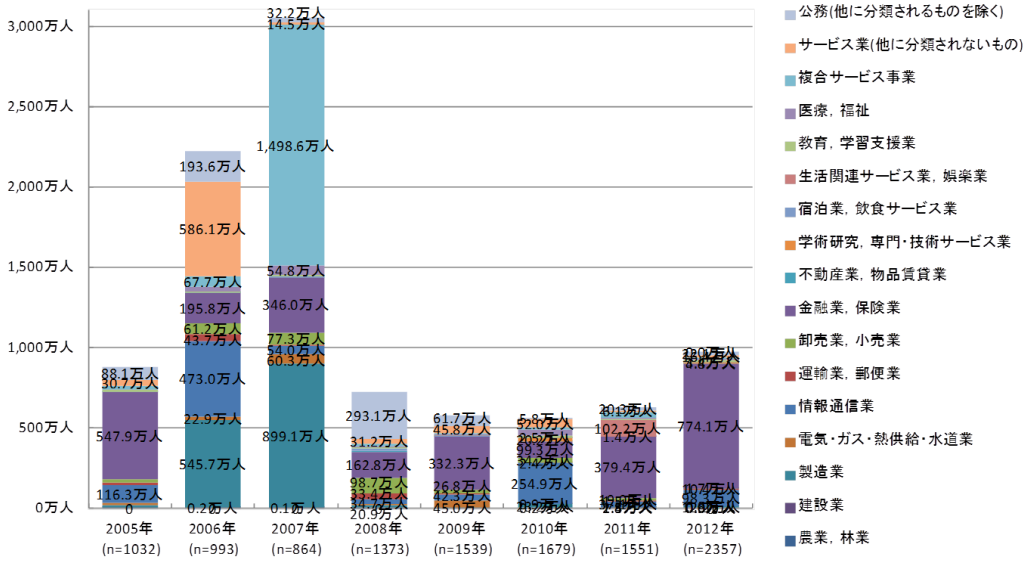


図 3-7：業種別漏えい人数の経年変化（合計）

業種別の個人情報漏えい人数を積み上げたグラフを図 3-7 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。

2012 年は「金融業，保険業」の漏えい人数が他業種より突出している。前述したとおり複数の金融機関から多数の帳票の紛失が公表されており、とくにそのうちの１つの金融機関が約 560 万人分の個人情報を含むコムフィッシュを紛失したためである。

(6)　相関分析

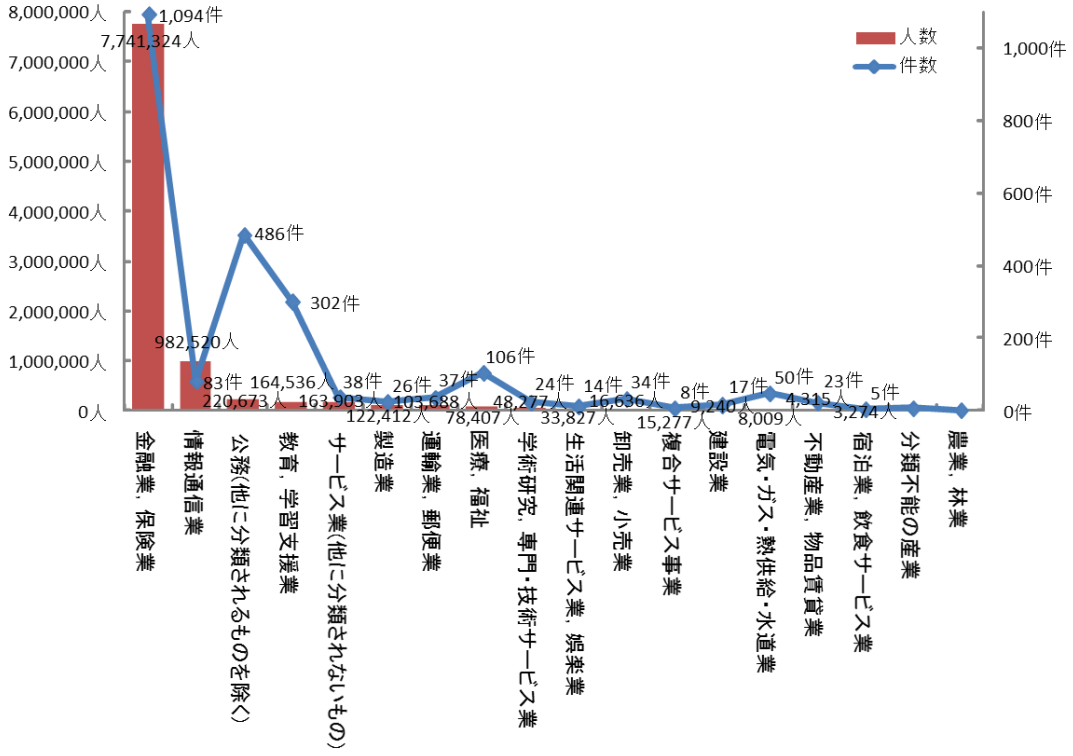


図 3-8：業種別のインシデント件数と漏えい人数

業種別のインシデント件数と漏えい人数の関係を図 3-8 に示す。「情報通信業」は 2012 年に発生したインシデント件数が比較的少ないにも関わらず 10 万人単位の大規模インシデントが 2 件発生したため、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、「公務」「教育，学習支援業」「医療，福祉」「電気・ガス・熱供給・水道業」は、個人単位の帳票が多い業種であることに加え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。

3.4　原因

(1)　単年分析(件数)

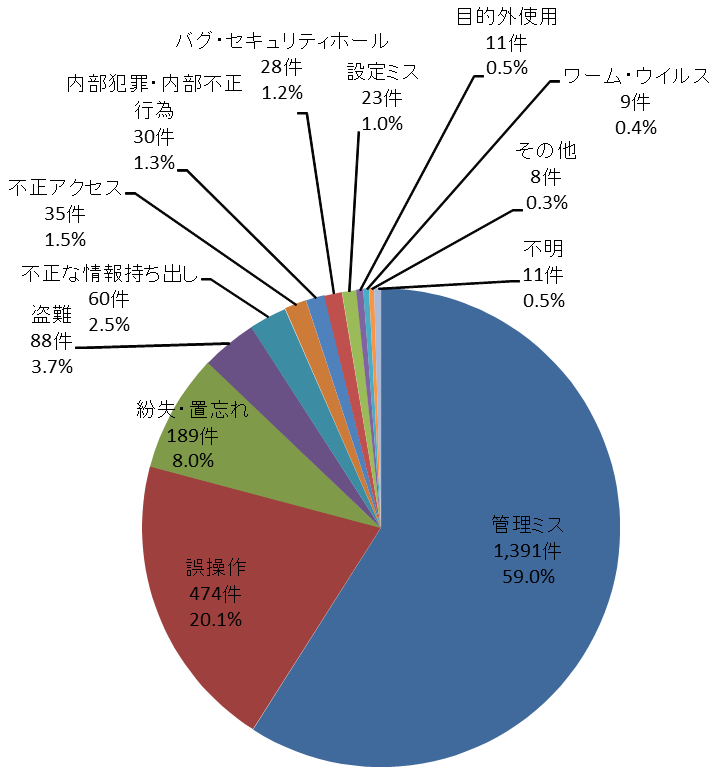


図 3-9：漏えい原因比率（件数）

個人情報漏えい件数の原因比率を図 3-9 に示す。2012 年は「管理ミス」「誤操作」「紛失・置き忘れ」で約 90%を占めた。「管理ミス」の約半分は、信用金庫や信用組合、地方銀行での紛失や誤廃棄であった。

「誤操作」および「紛失・置き忘れ」はヒューマンエラーである。その対策としては、担当者へのセキュリティ教育、および業務や操作の手順づくりとその遵守が効果的である。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、漏えいしても被害が拡大しない対策もあわせて行うことも検討に値する。

(2)　経年分析(件数)

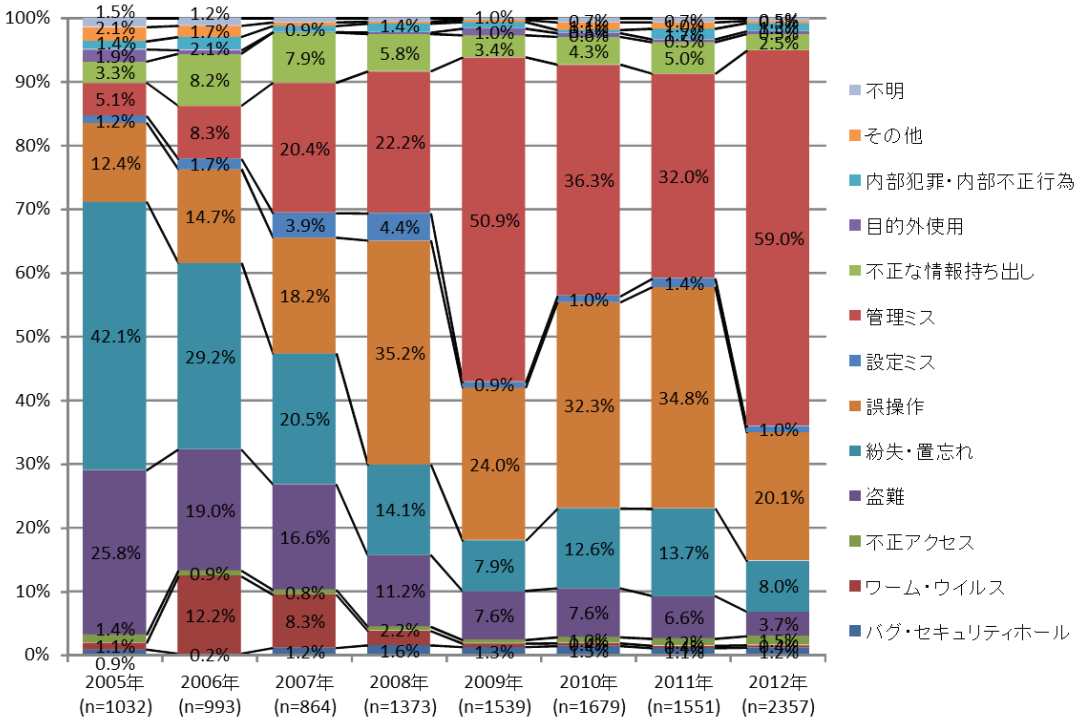


図 3-10：漏えい原因比率の経年変化（件数）

個人情報漏えい件数の原因比率の経年変化を図 3-10 に示す。2012 年は、2009 年から減少していた管理ミスが増加している。

総件数も 2009 年から 2011 年は 1500~1600 件程度で推移していたが、2012 年では約 800 件増加し、2357 件にまで増えている。

2012 年の件数をみると、管理ミスが 2011 年から約 900 件(全体の 59.0%)増加している。その一方で他の原因の件数はやや減少している傾向が見受けられる。これらのことから管理ミスの増加が総件数を増やしたと読み取れる。

先に述べたように、管理ミスはヒューマンエラーによって発生することが多い。管理ミスの増加は、個人情報の取り扱いに関する担当者・関係者の意識低下が引き起こす場合も多いため留意が必要である。翌年(2013 年)の原因比率・件数には注視したい。

(3)　単年分析(人数)

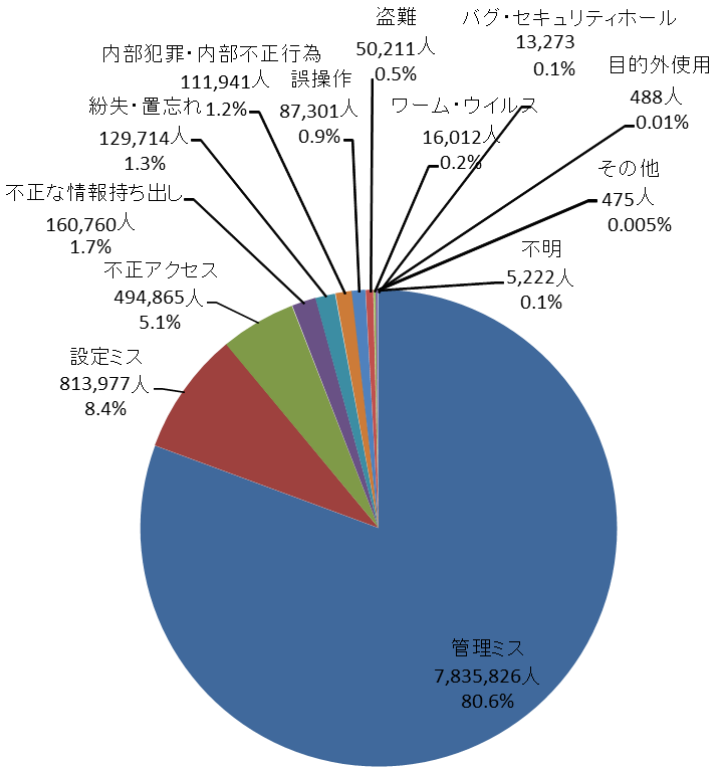


図 3-11：漏えい原因比率（人数）

個人情報漏えい人数の原因比率を図 3-11 に示す。

「管理ミス」による漏えい人数が 80%を超える。2012 年における「管理ミス」の影響の大きさが読み取れる。

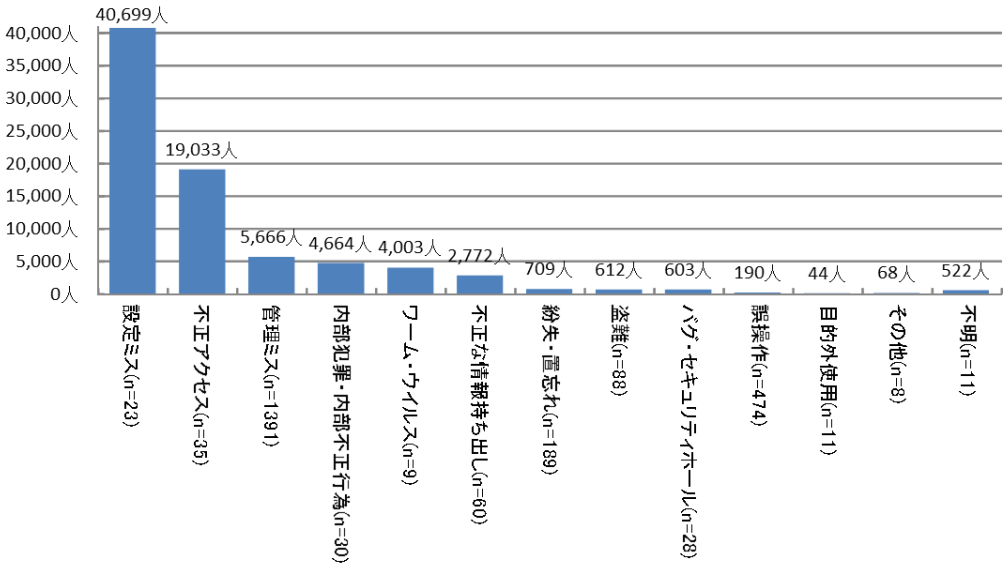


図 3-12：漏えい原因別の一件あたりの漏えい人数

漏えい原因別の一件あたりの漏えい人数を図 3-12 に示す。図 3-12 では、「設定ミス」「不正アクセス」の一件あたりの漏えい人数が目立つ。「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。

これは「内部犯罪・内部不正行為」にも当てはまる。2012 年の「内部犯罪・内部不正行為」は、目立つ件数を示していないが前年は上位に挙がっていたものであり悪意のある者が引き起こすインシデントとして認識しておく必要がある。

設定ミスについては、スマートフォン用の電話番号検索アプリ「全国電話帳」によるインシデントによる漏えい人数が 76 万人となり、1 件あたりの人数を押し上げている。これまで設定ミスによる漏えい人数を大きく上回っており、翌年以降の動向をみて 2012 年の特有のインシデントであったかどうかを確認したい。

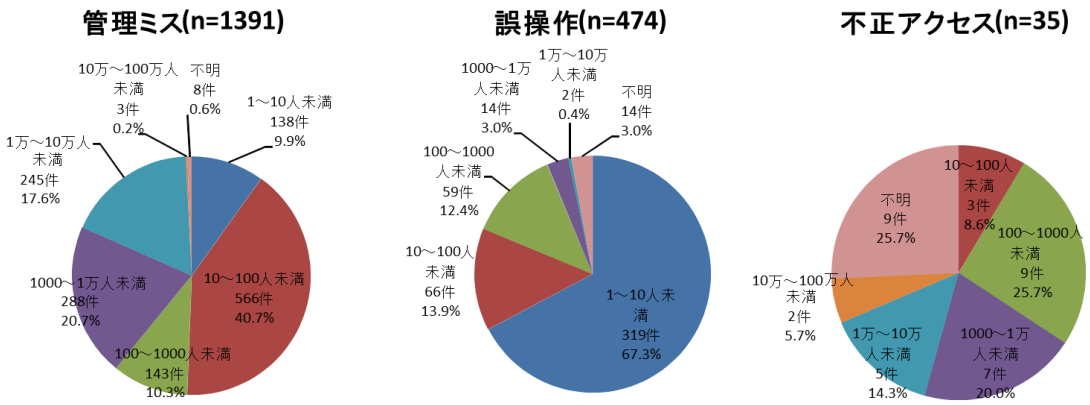


図 3-13：漏えい原因の人数区分（件数）

特徴的な漏えい人数区分を示す 3 つの原因を図 3-13 に示す。件数、漏えい人数ともに第 1 位の「管理ミス」は 10～100 人未満が最も多いが、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。

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おおよそ 4 分の 3 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。

「不正アクセス」は、1000 人以上のインシデントが多く、10 万~100 万人未満のインシデントも 2 件発生している。同規模のインシデントは「管理ミス」では 3 件発生しているが総件数を考慮にいれると「不正アクセス」の一件あたりの漏えい人数が多くなる傾向が見えてくる。

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」のような悪意のある者が引き起こすインシデント対策についても、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)

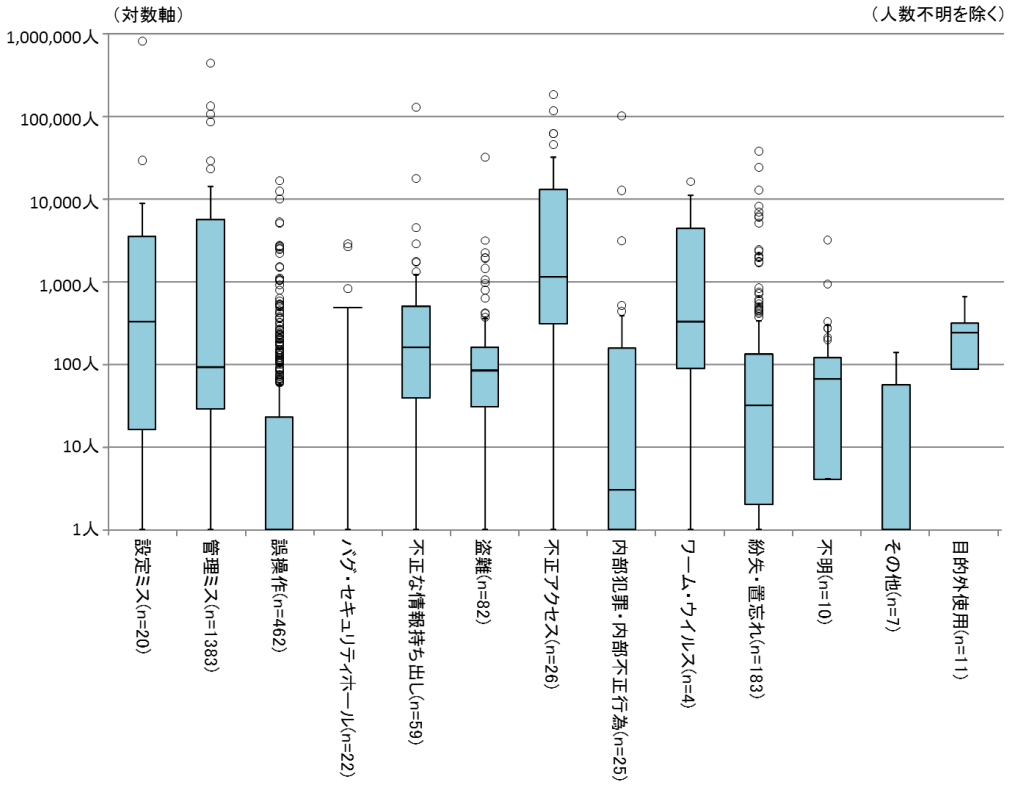


図 3-14：漏えい原因の漏えい人数（箱髭図）

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 3-14 に示す。他の原因と比べて、「不正アクセス」「ワーム・ウイルス」の漏えい人数は、箱髭図の箱の部分が 100 人から 1 万人の範囲に分布し、漏えい人数の規模が他の原因と比較して多いことがわかる。また「設定ミス」「管理ミス」の 1 件あたりの漏えい人数は大きい外れ値があり、まれに大規模なインシデントが発生することがわかる。

「誤操作」「紛失・置忘れ」は、外れ値の数が多い。特に「誤操作」は箱のほとんどの部分が 10 人以下に分布しているにもかかわらず、外れ値が 100 人から 1 万人まで広く分布している。また、「不正な情報持ち出し」「内部犯罪・内部不正行為」は、分布自体は少ない範囲を示しているが大きい外れ値が分布している。

(5)　業種別（件数）

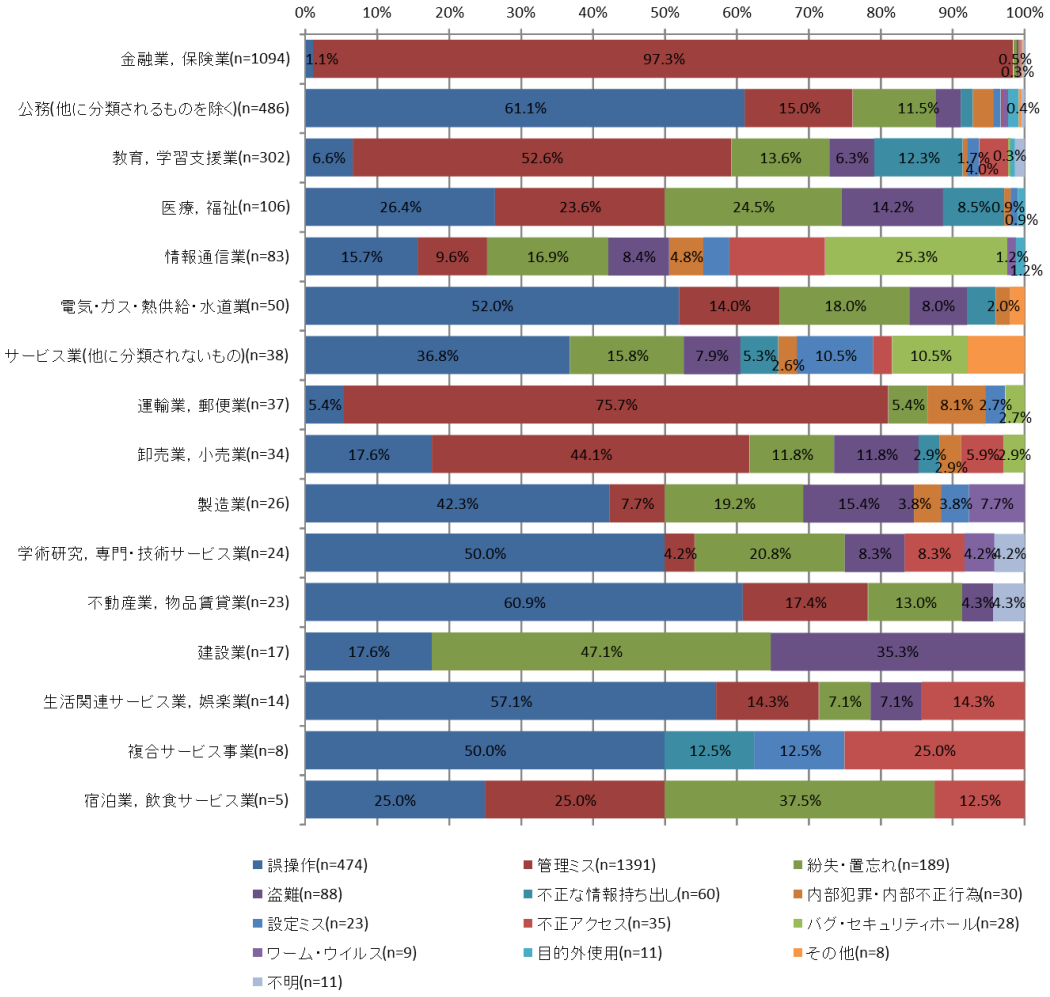


図 3-15：業種別の漏えい原因比率（件数）

業種別の漏えい原因比率を図 3-15 に示す。2012 年の業種別の漏えい原因比率は、おおむねこれまで同様の傾向が見られた。「公務」「不動産業，物品賃貸業」「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。2012 年の「誤操作」の全件数 474 件のうち、「公務」の「誤操作」は 62.7%(297 件)を占める。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。

「金融業，保険業」は、「管理ミス」の占める比率が高く、97.3%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。「教育・学習支援業」は、「不正な情報持ち出し」の比率が 12.3%と、他の業種に比べて高い。件数も 37 件で、もっとも多い業種となっている。「教育・学習支援業」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がある。

3.5　漏えい媒体・経路

(1)　単年分析(件数)

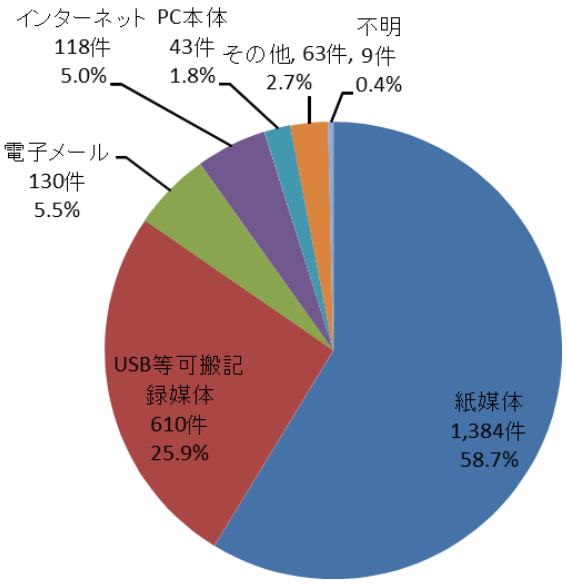


図 3-16：漏えい媒体・経路（件数）

漏えい媒体・経路別のインシデント件数を図 3-16 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 58.7%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「USB 等可搬記録媒体」が 25.9%、「電子メール」が 5.5%を占める。

(2)　経年分析(件数)

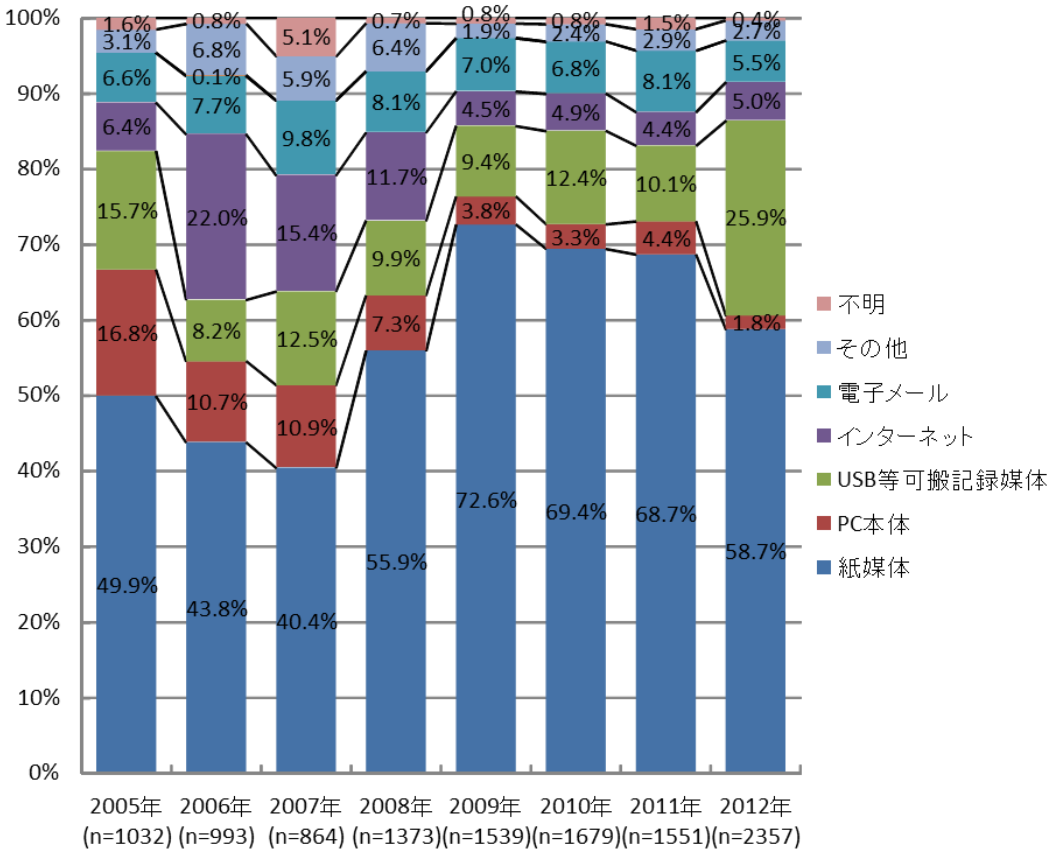


図 3-17：漏えい経路比率の経年変化（件数）

漏えい経路比率の経年変化について図 3-17 に示す。原因の大半を占める「紙媒体」による漏えい件数は、2009 年以降、減少傾向にある。2012 年の「USB 等可搬記録媒体」による漏えい件数は 2011 年比 2.5 倍以上となっている。

(3)　単年分析(人数)

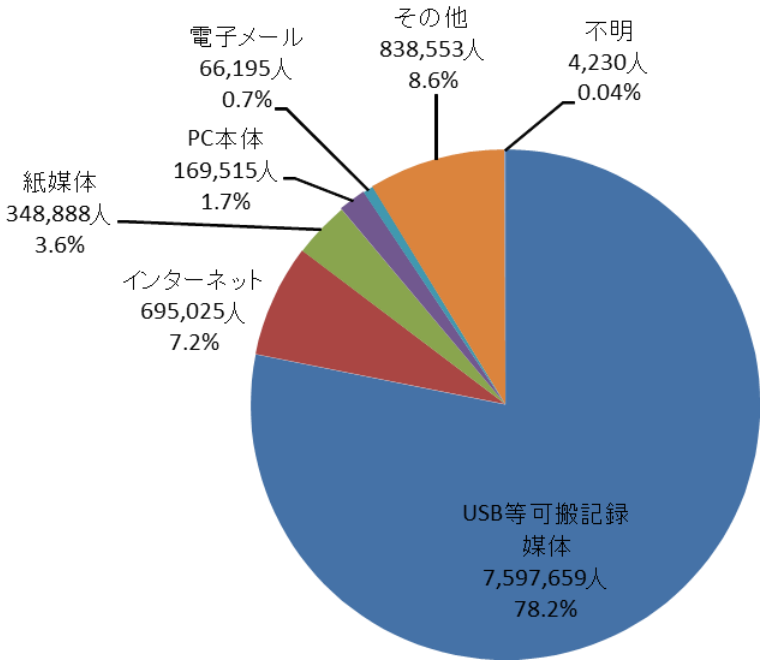


図 3-18：漏えい媒体・経路（人数）

漏えい媒体・経路別の漏えい人数を図 3-18 に示す。個人情報が漏えいした人数は、「USB 等可搬記録媒体」が 78.2%を占める。「表 3-2：インシデント・トップ 10」のうち、第 2 位、第 7 位、第 8 位、第 10 位の 4 件が「USB 等可搬記録媒体」であった。この 4 件のインシデントでは合計約 68 万人、2011 年に比べ、上位集中ではない傾向がうかがえる。

2010 年に最も人数の多かった「インターネット」は、その後に減少し、2012 年は 7.2%で 2 番目であった。「インターネット」経由のインシデントも、「表 3-2：インシデント・トップ 10」の第 3 位、第 6 位、第 9 位の 3 件も発生している。

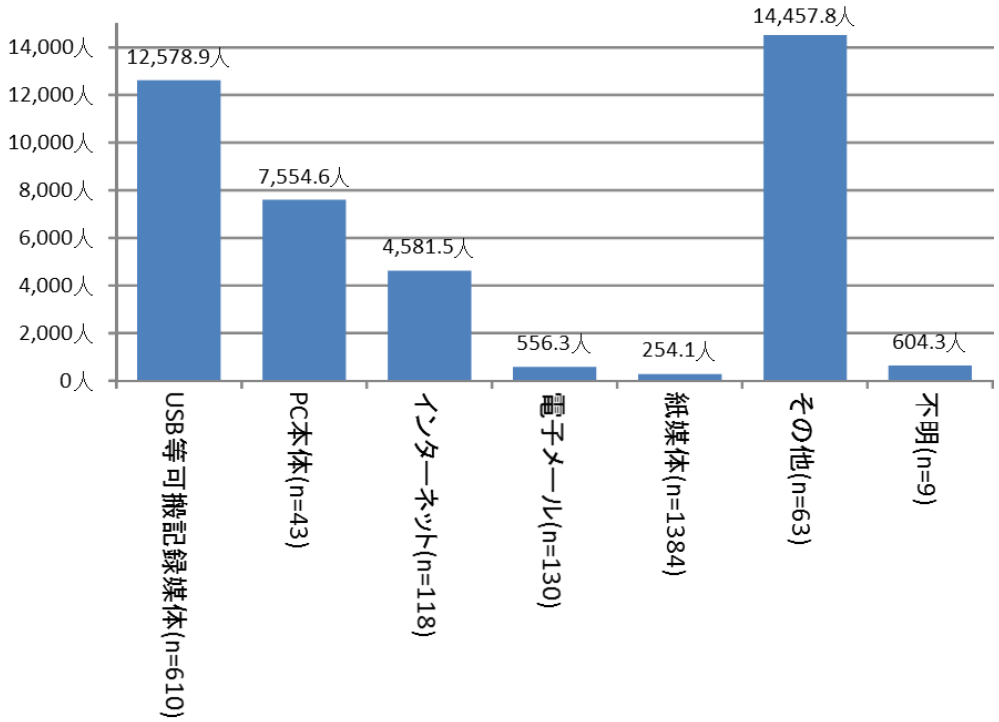


図 3-19：漏えい媒体・経路別の一件あたりの漏えい人数

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 3-19 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、「USB 等可搬記録媒体」「PC 本体」「インターネット」が多い。「USB 等可搬記録媒体」「PC 本体」「インターネット」の平均漏えい人数が多い理由は、いずれも個人情報が扱い易い電子データ（ファイル）に保存されており、一度に大量の個人情報が操作できることから、USB メモリ、インターネット、PC 本体を経由して漏えいしたと思われる。

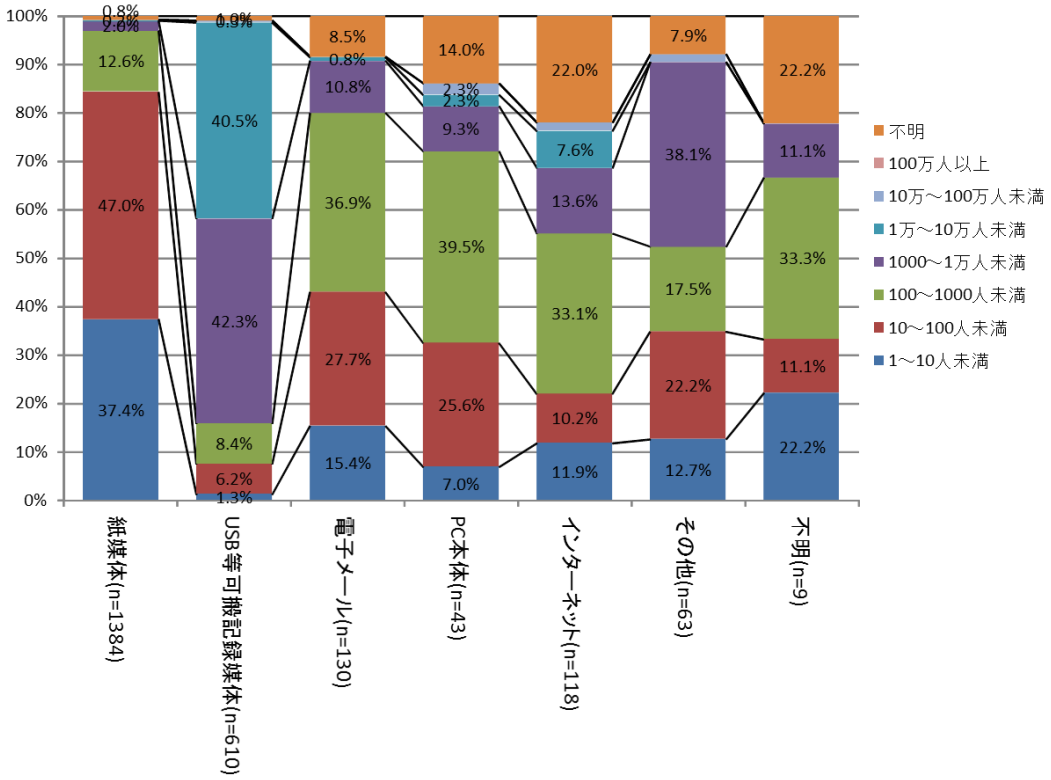


図 3-20：漏えい規模比率(件数)

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 3-20 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 10~100 人未満の小規模なインシデントの比率が約 47%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 80%を占めるが、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、10 人以上～100 人未満、100 人以上～1000 人未満と規模が大きくなるにしたがってインシデントの比率も徐々に増加している。

一方で「USB 等可搬記録媒体」によるインシデントは、1000 人未満のインシデント比率が 20%未満と他と比べ圧倒的に低く、大規模のインシデントの比率が高い。

(4)　箱髭図(人数)

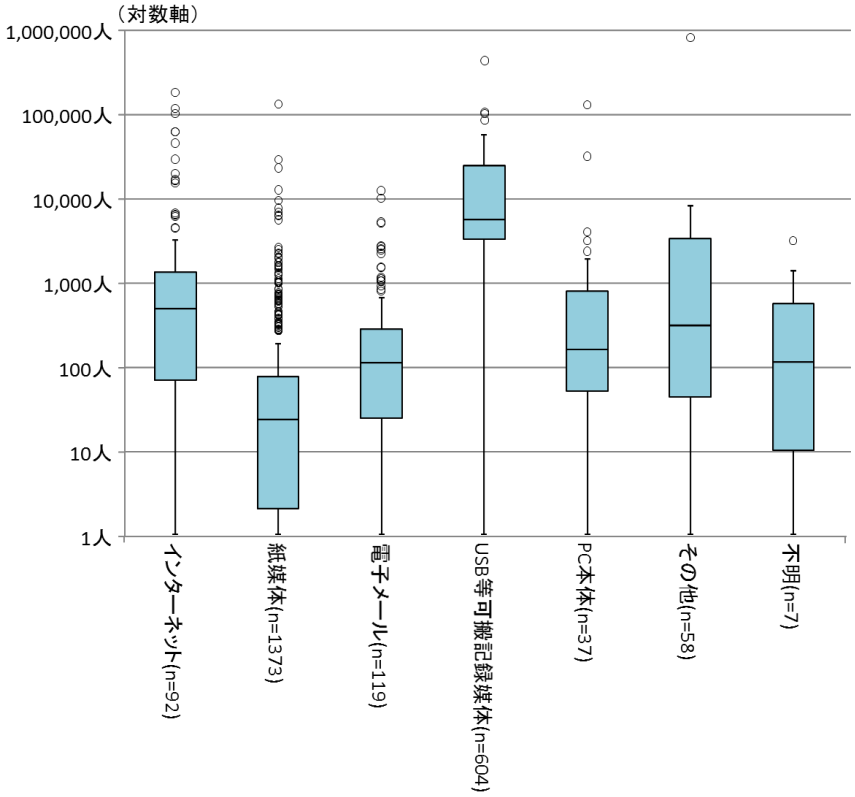


図 3-21：漏えい経路の漏えい人数（箱髭図）

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。「USB 等可搬記録媒体」の漏えい人数の分布は 1 件あたりの漏えい人数が 1 万人前後で、他の漏えい経路と比較して多いことがわかる。「紙媒体」のインシデントは、箱髭図の箱の部分が 100 人未満と小規模だが、10 万人以上のインシデントも発生している。

(5)　業種別(件数)

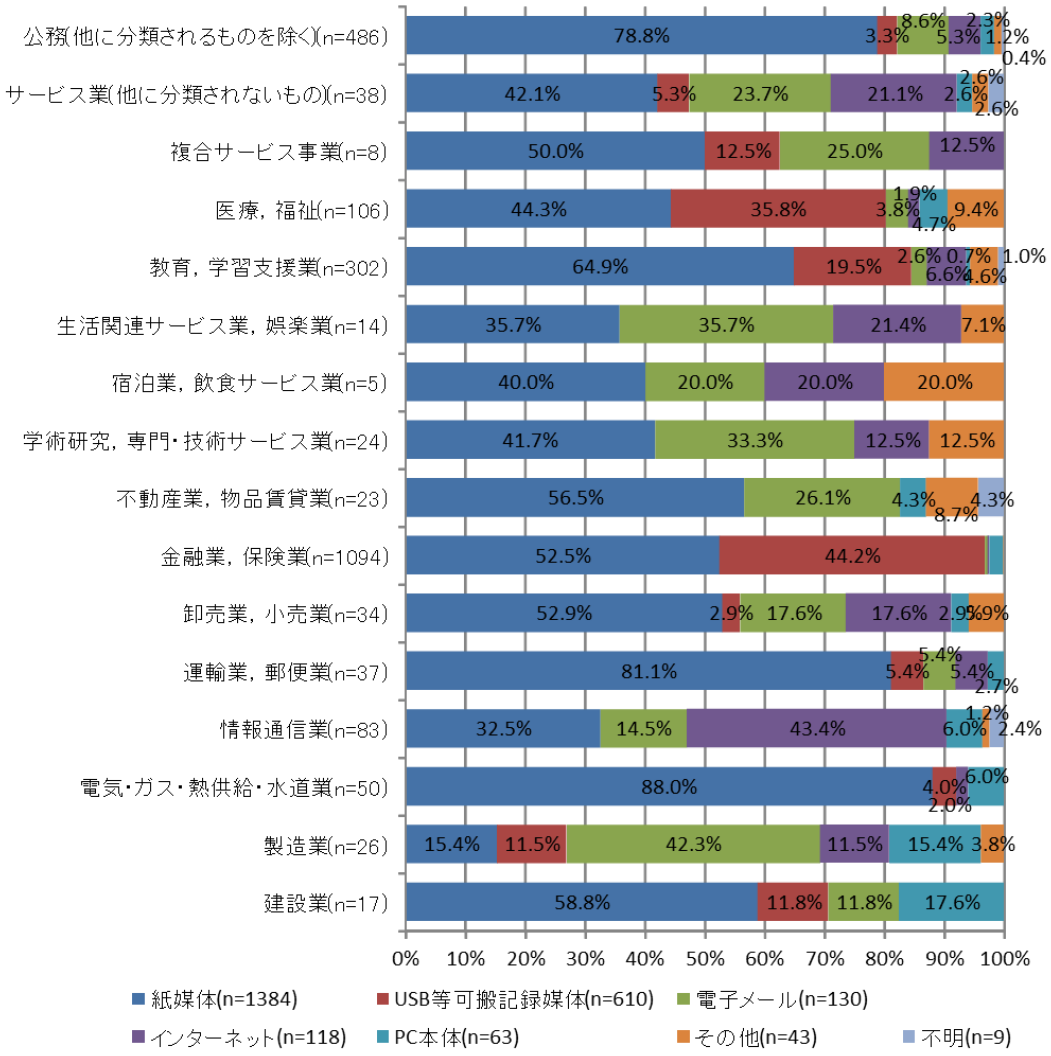


図 3-22：業種別の漏えい経路比率（件数）

漏えい媒体・経路の業種別比率（件数）について図 3-22 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、紙媒体によるインシデントが占める割合が高い業種が多い。「教育,学習支援業」「電気・ガス・熱供給・水道業」「公務」「運輸業,郵便業」は、特に比率が高い。「医療，福祉」「金融業，保険業」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。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

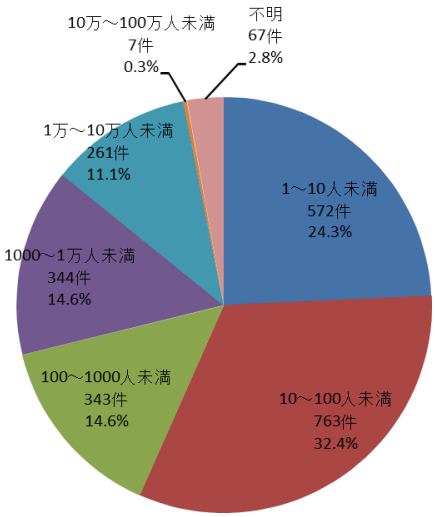


図 3-23：漏えい規模比率（件数）

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 3-23 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。しかし、隣接する区分と比較してみると、相対的に「1 万～10 万人未満」、「1000～1 万人未満」および「10～100 人未満」の比率が大きいことがわかる。これは、金融業・保険業におけるインシデントの漏えい規模の影響と見られる。漏えい人数が 1000 人未満のインシデントを合計すると 71.3%になり、全体の 7 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が、組織によっては、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方針のところもある。

(2)　経年分析(件数)

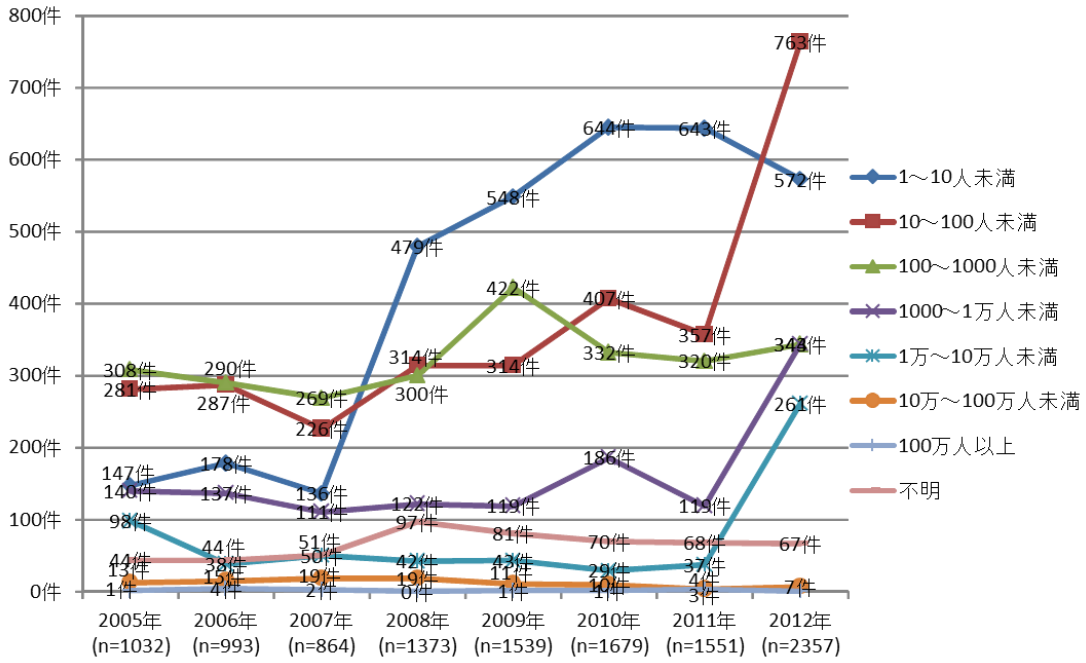


図 3-24：一件あたりの漏えい人数区分の経年変化（件数）

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 3-24 に示す。2012 年は、2011 年と比べて、「1 万～10 万人未満」、「1000～1 万人未満」および「10～100 人未満」が大きく増加している。これは、前述したように、金融業・保険業におけるインシデントの影響と見られる。

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状況が続いていたが、2012 年は「10～100 人未満」が最も多くなった。

(3)　業種別(件数)

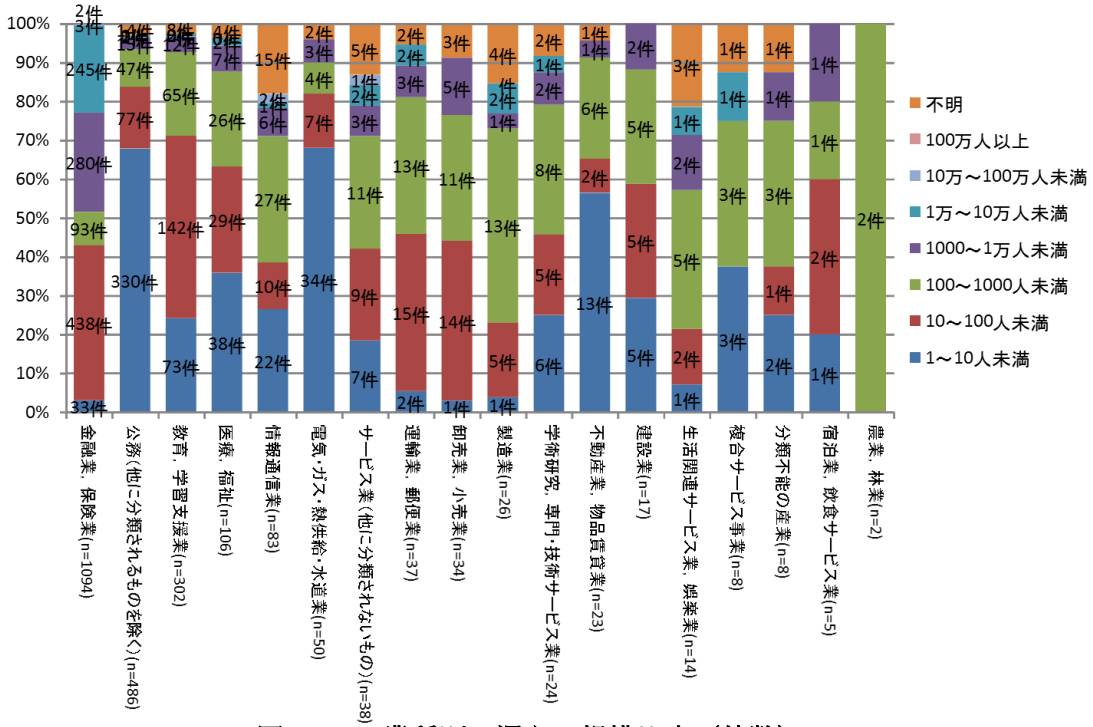


図 3-25：業種別の漏えい規模比率（件数）

業種別の漏えい規模（件数）の比率を図 3-25 に示す。100 人未満までの小規模なインシデントの合計で見てみると、「公務」「電気・ガス・熱供給・水道業」「教育・学習支援業」における比率が高く、約 80～90%である。これらの業種は、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。「金融業・保険業」と「公務」のインシデント件数が多いので、全体的な傾向にも大きな影響を与えている。

3.7　漏えい情報の価値

(1)　漏えい情報

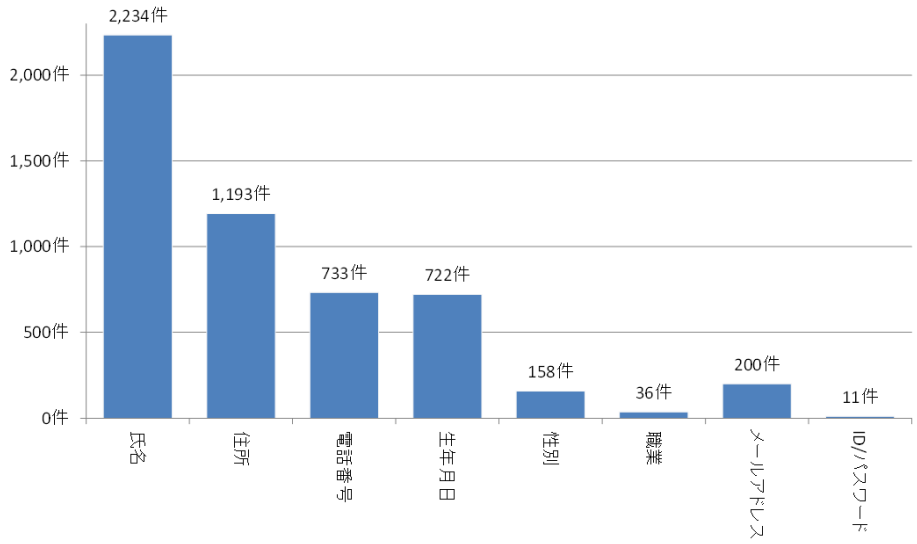


図 3-26：漏えい情報の出現確率

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	**2234 件**	**94.8%**
住所	**1193 件**	**50.6%**
電話番号	**733 件**	**31.1%**
生年月日	**722 件**	**30.6%**
性別	**158 件**	**6.7%**
職業	**36 件**	**1.5%**
メールアドレス	**200 件**	**8.5%**
ID/PASSWD	**11 件**	**0.5%**

漏えい情報の出現確率を図 3-266、表 3-3 に示す。

「氏名」の出現率が 94.8%であり、著しく高い。次いで住所（50.6%）、電話番号（31.1%）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)

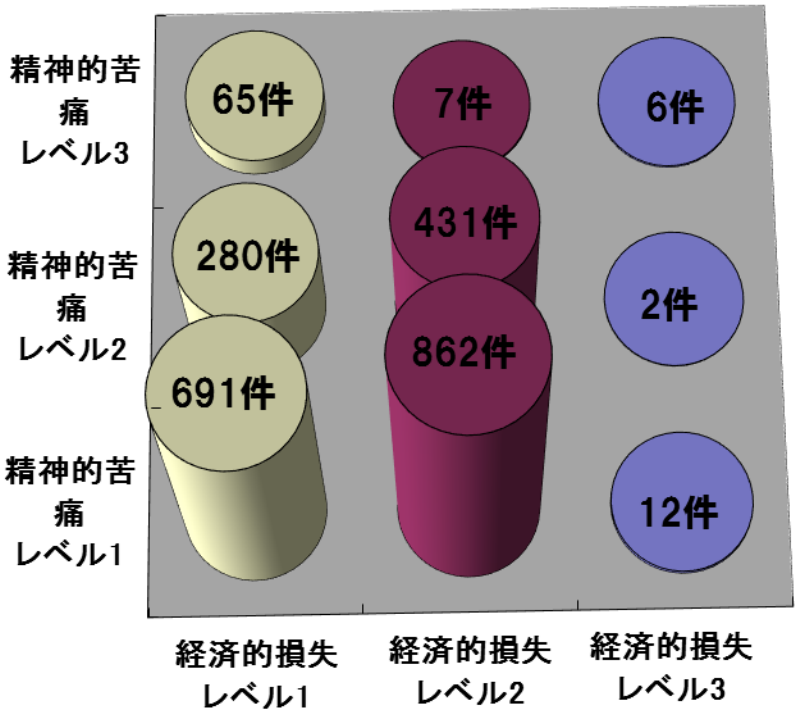


図 3-27：シンプル EP 図分布（件数）

2012 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 3-27 に示す。

2012 年の被害分布状況の特徴は、2011 年と比較して、精神的苦痛と経済的損失のレベルが共に 2 であるフィールド、および精神的苦痛のレベル 1 と経済的損失のレベル 2 のフィールドが大幅に増加した点である。

* シンプル EP 図とは、個人情報が漏えいした時に被害者へ与える精神的苦痛の度合いを横軸(x 軸)に、経済的損失の影響度合いを縦軸(y 軸)に対応させて、それぞれの影響の大きさを 3 段階で表現したもの。詳細は、p.47、p.48 を参照。

(2)　業種別EP分布

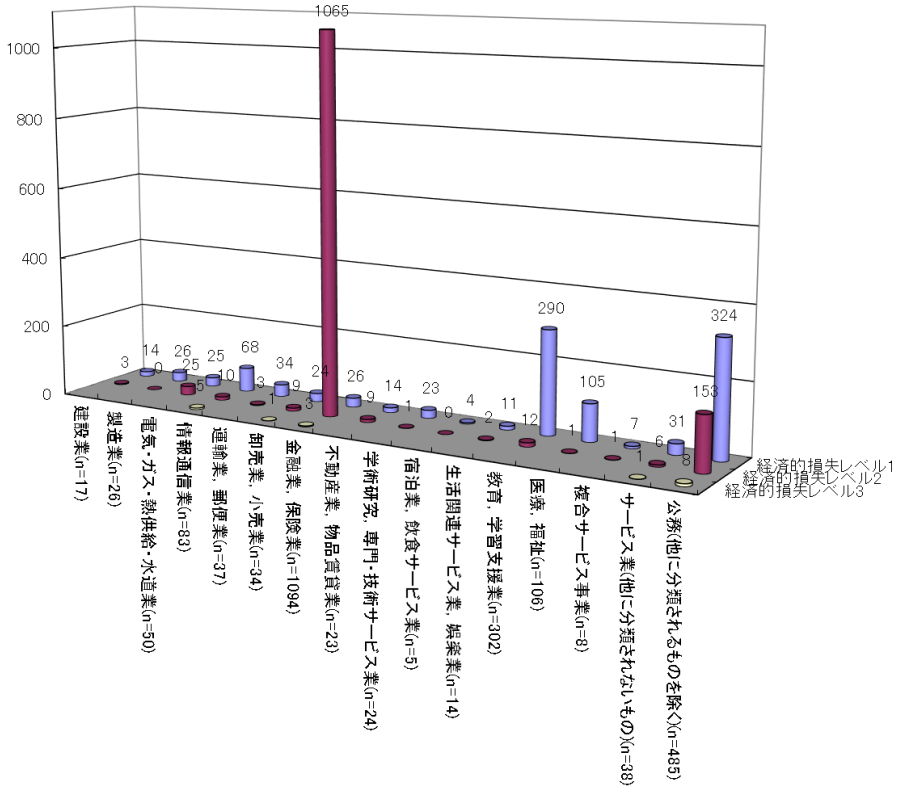


図 3-28：漏えい情報の経済的損失レベル分布（件数）

漏えい情報の経済的損失レベル分布（件数）を図 3-28 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」である。「金融業，保険業」業界が特出している理由は、預金残高等やクレジットカード情報の漏えいが多いためと考えられる。

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 5 件未満であった。

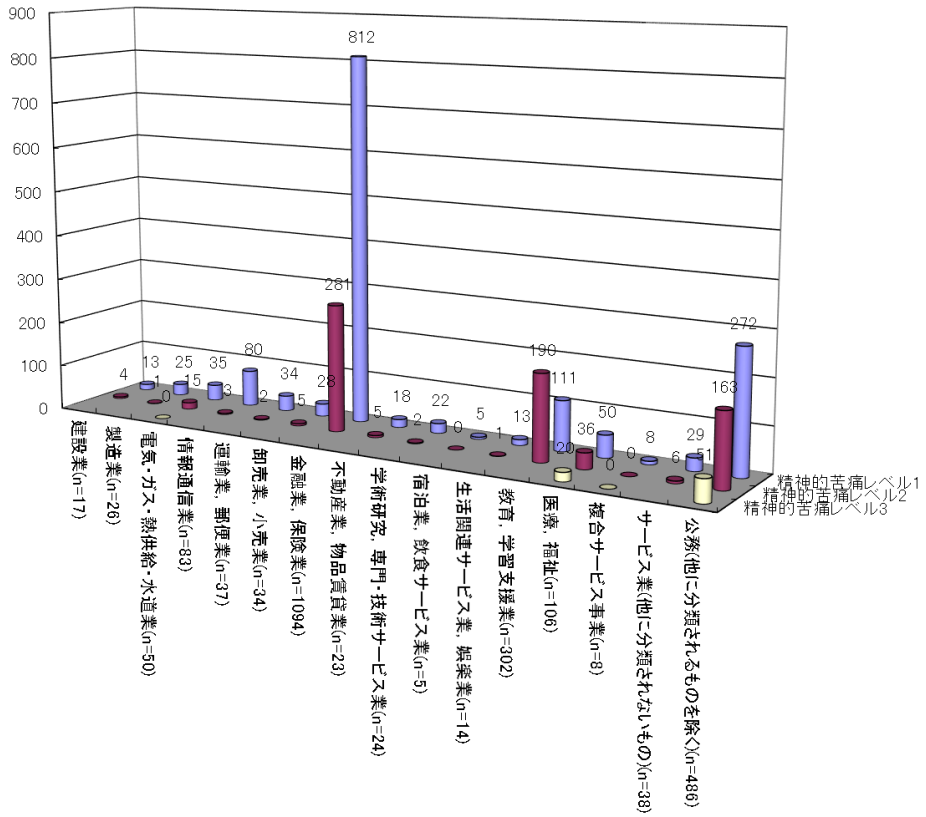


図 3-29：漏えい情報の精神的苦痛レベル分布（件数）

漏えい情報の精神的苦痛レベル分布（件数）を図 3-29 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」「情報通信業」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」「教育，学習支援業」「公務」となっている。「金融・保険業」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 2012 年の間に収集した 8 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、2012 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	3468 人
2011 年	1551 件	628 万 4363 人	4238 人
2012 年	2357 件	972 万 65 人	4245 人

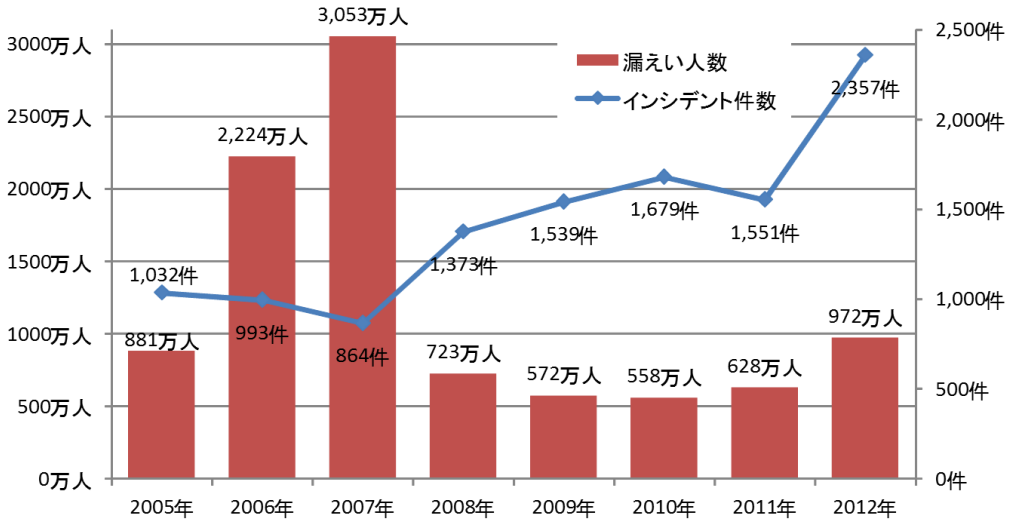


図 3-30：インシデント件数と漏えい人数の経年変化（合計）

2012 年のインシデント件数は、2011 年より増加した。また、漏えい人数も 2011 年と比較して増加した。2012 年は、2008 年以降では、インシデント件数と漏えい

※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 2012 年は 2357 件から被害者数不明の 67 件を除いた 2290 件で漏えい人数を除算した。

人数共に目立って増加した。結果、個人情報が漏えいした人は、日本の人口の約 13 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。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 件であった。2012 年は 100 万人以上の漏えいインシデントが 0 件であったのに、合計の漏えい人数が 2011 年より増加したのは、インシデント件数が増加したことと相関関係にあるからである。2011 年と 2012 年を対比すると、2012 年のインシデント件数は 2011 年に比較すると約 1.5 倍となり、同様に 2012 年の漏えい人数は 2011 年に比較すると約 1.5 倍で同じ比率で増加していることがわかる。

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%

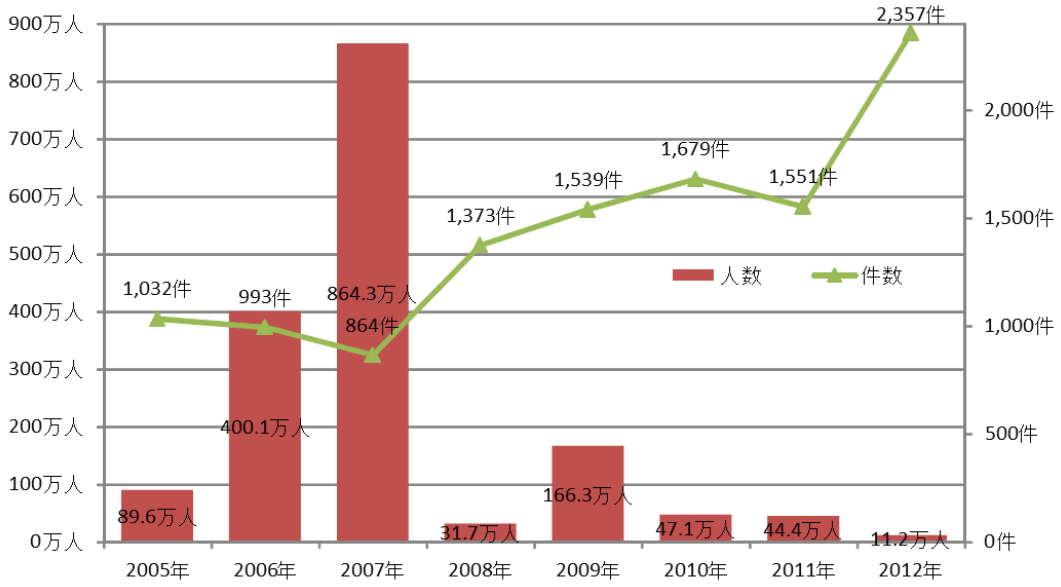


図 3-31：インシデント件数と内部不正による漏えい人数の経年変化（合計）

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 3-31：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、2012 年は 2,357 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 件程度で推移し、漏えい人数は減少傾向にあったが、2012 年は、インシデント件数と漏えい人数が共に増加している。

図 3-2 インシデント件数と図 3-7 漏えい人数の経年比較を見ると「金融業，保険業」が大きく増加していることが分かる。増加原因を裏付ける直接的な情報は無いが、金融・保険業界で個人情報管理の状況調査の対象がより小さな組織にも拡大された等の動きがあった可能性がある。

4　2012 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

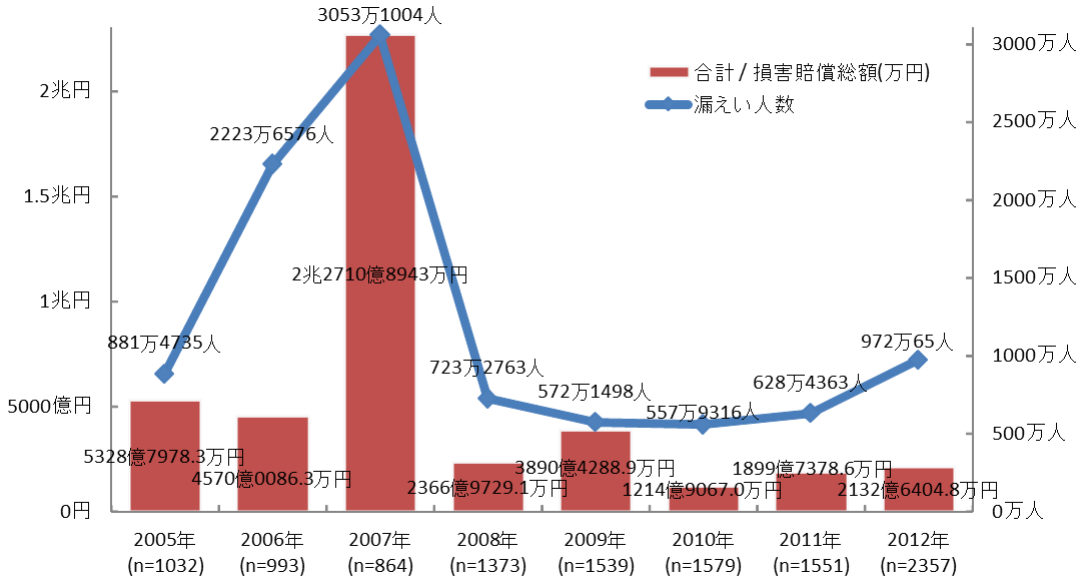


図 4-1：想定損害賠償総額と漏えい人数

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。2012 年は、漏えい人数、想定損害賠償総額ともに微増した。

4.2　一人あたりの想定損害賠償額

(1)　単年分析

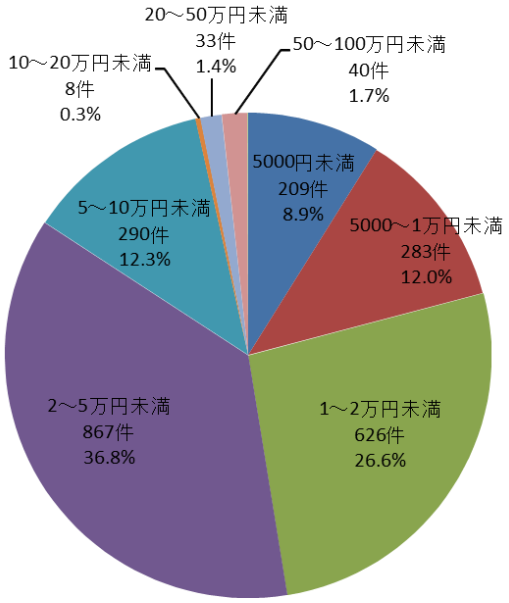


図 4-2：一人あたりの想定損害賠償額比率（件数）

一人あたりの想定損害賠償額を図 4-2 に示す。

2012 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 36.8%と最も多く、次いで「1～2 万円未満」の比率が 26.6%、合わせて約 63%となった。

(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
2011 年	4 万 8560 円
2012 年	4 万 4628 円

一人あたりの想定損害賠償額は、ほぼ 4 万円から 5 万円の範囲に収まっている。

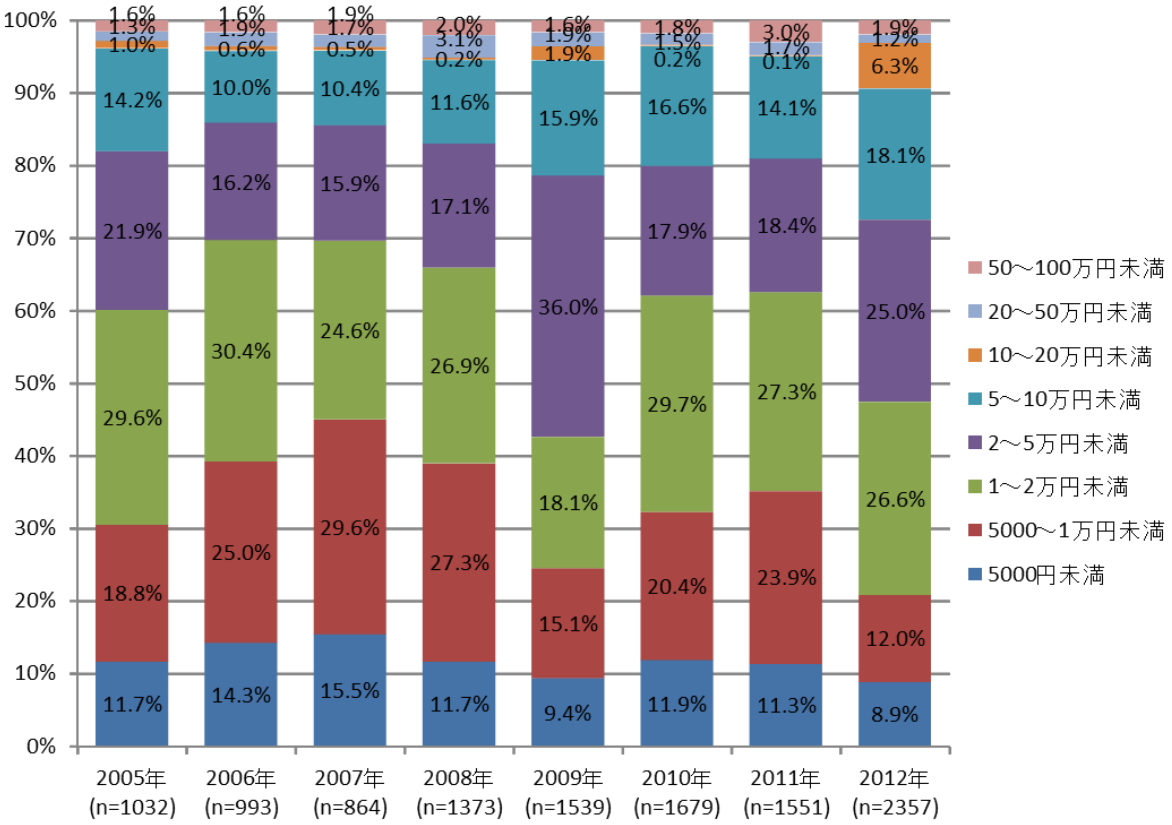


図 4-3：一人あたりの想定損害賠償額比率の経年変化（件数）

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。

2012 年は「1～2 万円未満」「2～5 万円未満」「5～10 万円未満」「10～20 万円未満」の割合が増加した。

【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 JO モデルを用いて算出している。全てのインシデントの「一人あたりの想定損害賠償額」を合計し、インシデント件数で除算した金額が、インシデント一件あたりの「一人あたりの平均想定損害賠償額」である。「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

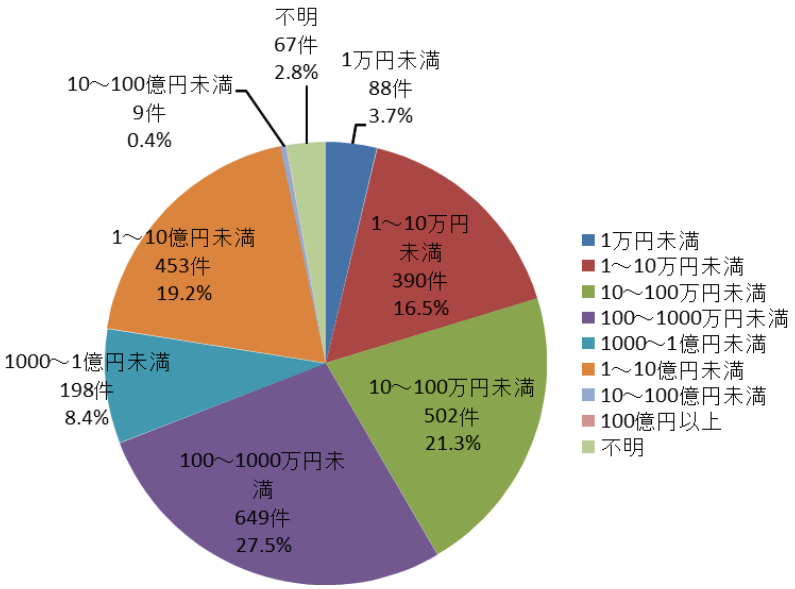


図 4-4：一件あたりの想定損害賠償額比率（件数）

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 100～1000 万円未満のインシデントが最も多く、27.5%を占めた。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 100 万円未満のインシデントは、41.5%だった。

(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

2012 年は、想定損害賠償総額は増加したが、一件あたりの平均想定損害賠償額は減少した。

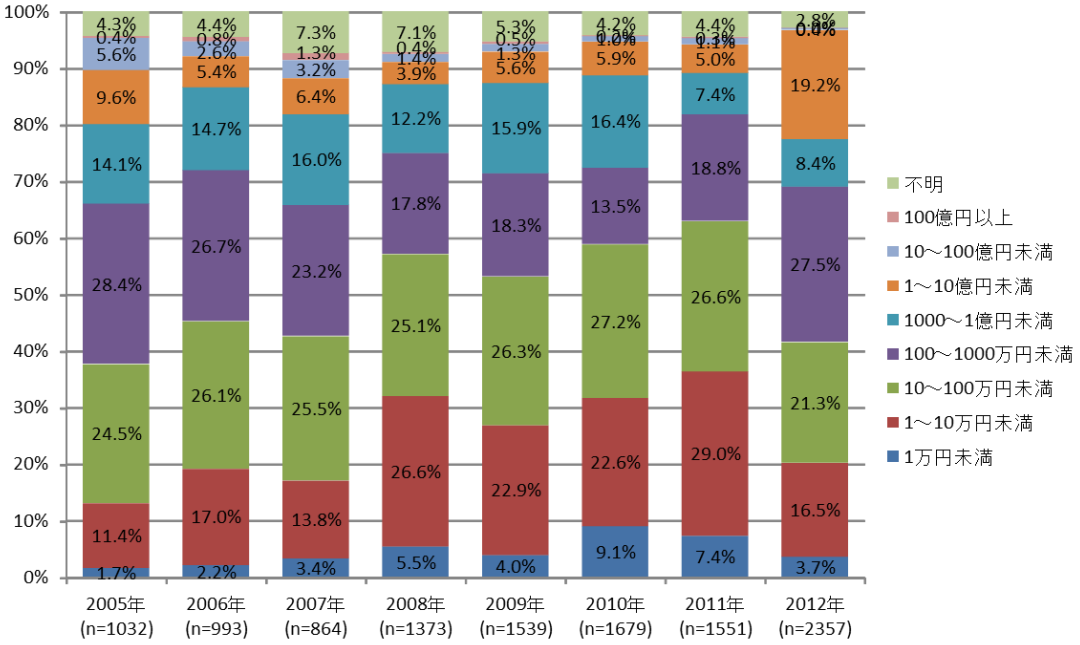


図 4-5：一件あたりの想定損害賠償額比率の経年変化（件数）

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。

2008 年から 2011 年までは、100 万円未満の割合が約 60%前後を占めていた。2012 年は「100 万円以上～1000 万円未満」と「1 億円以上～10 億円未満」の割合が大幅に増加し、それにともなって 100 万円未満の割合が約 40%へ減少した。

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

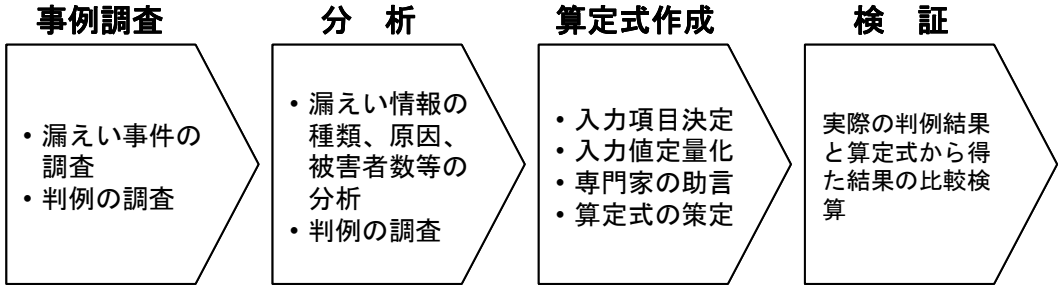


図 5-1：想定損害賠償額算定式策定のプロセス

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. 2012 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。

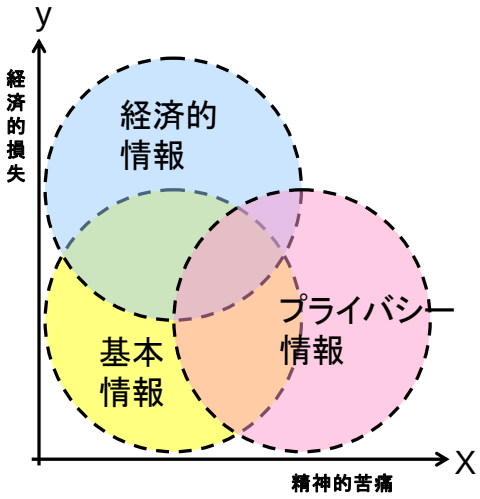


図 5-2：EP 図（Economic-Privacy Map）

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。

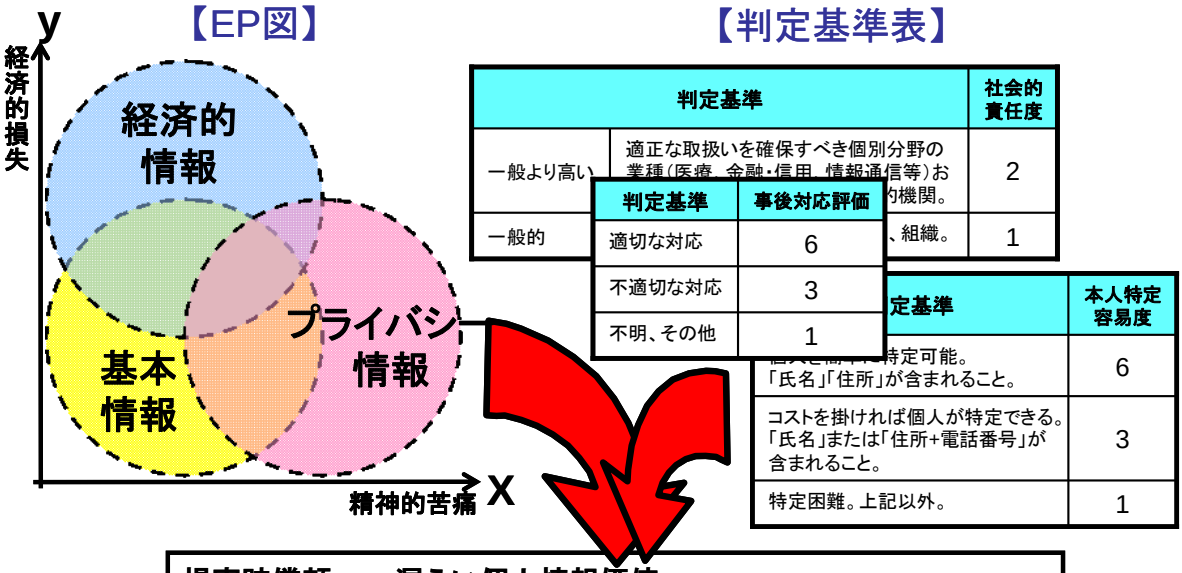
表 5-4：事後対応 行動例

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



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
＝(基礎情報価値 × 機微情報度 × 本人特定容易度)
×情報漏洩元組織の社会的責任度
×事後対応評価
＝ 基礎情報価値[500]
×機微情報度[Max($10^{max(x)-1}+5^{max(y)-1}$)]
×本人特定容易度[6, 3, 1]
×社会的責任度[2, 1]
×事後対応評価[2, 1]

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　まとめ

2012 年の個人情報漏えいインシデントの調査結果の考察を以下にまとめた。

6.1　2012 年インシデントの特徴

2012 年は、報道や公表されたインシデント件数が大きく増加した。この要因は「金融業，保険業」の公表件数が大きく増加したためである。「金融業，保険業」からの個人情報漏えいインシデントは、口座に関係する機微な個人情報が含まれ、インシデントの件数が多く、インシデント 1 件あたりの平均漏えい人数も多い。そのため、全体の統計結果へも影響が現れている。2012 年に「金融業，保険業」の件数増加によって、大きく変化したポイントを以下に示す。

- USB 等可搬記録媒体の件数、人数の増加
  (156 件→610 件, 371 万人→760 万人)
  ただし、USB メモリではなく、コムフィッシュの紛失によるもの
- 「管理ミス」の件数と割合の大幅増加
  (497 件→1391 件, 32.0%→59.0%)
- 一件あたりの想定損害賠償額が 100～1000 万円未満のインシデントの増加
  (18.8%→27.5%, 292 件→649 件)

さらに、この「金融業，保険業」のインシデント件数のほとんどが信用金庫や信用組合、地方銀行での紛失や誤廃棄であった。特に金融業でインシデント件数が増加した理由は、信用金庫や信用組合、地方銀行において、書類の保管状況などを一斉に点検するなどの動きがあったためと思われる。

その一方で、相変わらず、個人情報を取り扱うことが多く、かつ個人情報保護に関する行政の指導が強く働いている「公務」「教育，学習支援業」から、小規模なインシデントの公表が多い。その原因は「誤操作」「管理ミス」「紛失・置き忘れ」といったヒューマンエラーが大半を占める。日常業務において少人数の個人情報を扱う作業が多い上記の業種は、行政の指導が強く働いているにもかかわらず、漏えい件数がなかなか減少しない。

6.2 個人情報の詐取方法の変化

個人情報を保有、管理する組織からの漏えいではなかったため報告書には掲載しなかったが、2012 年は不正アプリによって個人情報が不正に大量取得される事件がいくつか発生した。いずれも、スマートフォンへアプリケーションをインストールすると、勝手にスマートフォン上の電話帳情報が抜き出されてしまう不正アプリケーションであった。正常な動作に見せかけてその裏で電話帳情報を抜き出したり、アプリケーションのダウンロード先を Google Play から別のリンクへ変更して騙したり、アップデート機能を用いて電話帳情報を抜き出す不正な機能を後から追加したりして、アプリケーションの利用者が気づきにくい手法を用いている。またスマートフォンを操作、管理している個人の意識思考判断では、「人気アプリが無料」といったうたい文句に騙され易い。

このように近年は個人の IT 環境上に蓄積された個人情報が攻撃者に狙われ始めている。これまで攻撃者はインターネットに常時接続された企業のサーバを狙い、そこに蓄積されている個人情報を一気に大量詐取していた。しかし、スマートフォンやクラウドサービスの個人利用の普及に従い、個人の IT 環境に個人情報が蓄積されるようになると、攻撃者はセキュリティ対策を強化した企業のサーバよりも、セキュリティ対策が弱く、騙されやすい個人のスマートフォンを狙い始めた。

これまでは、企業の IT 環境から個人情報が漏えいするリスクが大きかった。これからは、それに加えて個人の IT 環境に蓄積された個人情報が漏えいするリスクも、考慮しなければならない。そのためには、以下のようなスマートフォン利用者の情報セキュリティリテラシーの向上が必要である。

- スマートフォンに関する情報セキュリティ教育
- スマートフォン関連の不正アプリ、不正アクセスなどのセキュリティリスクの情報提供
- スマートフォンに蓄積されている自分の個人情報、知人の個人情報の把握

ただし、スマートフォンの普及によって利用者の拡大が続いているため、スマートフォン利用者間の情報セキュリティリテラシーの情報格差が顕在化している。IT 業界、セキュリティ業界は一丸となり、スマートフォン利用者にとって安心安全なインターネット環境を提供しなければならないと思う。

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