2011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 1.4 版

2012 年 12 月 7 日

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	NKSJ リスクマネジメント株式会社
猪俣	朗	トレンドマイクロ株式会社
大溝	裕則	株式会社 JMC
岡本	一郎	株式会社インフォセック
佳山	こうせつ	富士通株式会社
北野	晴人	日本オラクル株式会社
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
菅原	尚志	博士前期課程 1 年
新原	功一	客員研究員
鈴木	宏幸	客員研究員

廣松研究室

廣松	毅	教授
齋藤	肇	博士前期課程 2 年

情報セキュリティ大学院大学 修了生

星	智恵	2008 年度卒
小野	康史	2008 年度卒
髙津	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）の調査分析は今回で 10 回目となる。

JNSA セキュリティ被害調査ワーキンググループと情報セキュリティ大学院大学 原田研究室、廣松研究室では、2010 年と同様に、これまでの調査方法を踏襲し、2011 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 2011 年のインシデントの集計・分析結果、および過去 7 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識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、世の中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、および提案を行う。

本報告書は、この目的のために、情報セキュリティ大学院大学 原田研究室、廣松研究室と協同で、2011 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 2011 年の個人情報漏えいインシデントの分析結果」「第 4 章 2011 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 2011 年の個人情報漏えいインシデントの分析結果」では、2011 年の単年の分析結果、10 年間の蓄積されたデータのうち、直近 7 年間のデータに基づく経年の分析結果の解説を行った。2002 年から 2004 年までのインシデント情報は公表件数が少なく、統計データとしては偏りが大きいため、分析に際しては、これらを除外した。

「第 4 章 2011 年 想定損害賠償額の算定結果」では、想定損害賠償額の算定結果とその考察結果を解説した。2002 年から 2011 年までの 10 年間の個人情報漏えいに関する数値は、新聞やインターネット上で報道された公開情報に基づいて、統計したものである。一方、想定損害賠償額は、当ワーキンググループが独自に開発した算定手法に基づいて算出した推定データであることに注意されたい。

また、2010 年の報告書と同様に「インシデント一覧表」を付録とした。

2.3 調査・分析方法

2011 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 2011 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、1551 件（前年比-128 件）であった。2010 年よりやや減少しているが、2008 年以降、主に「公務」における漏えい件数が増加したことが影響して、1500 件程度の件数が続いている。

漏えい人数は、約 628 万人（前年比＋70 万人）と、2010 年よりは増加したが、全体的には 2007 年以降減少傾向である。これは、漏えい件数が増加する一方で、一件あたりの漏えい人数が小さい100 人未満の事件が増加していることが影響している。想定損害賠償総額は、約 1,900 億円（前年比＋685 億円）となった。

漏えい原因は、「誤操作」（539 件）が一番多く、「管理ミス」（497 件）、「紛失・置忘れ」（213 件）の 3 種類が大半を占めた。2011 年は、「誤操作」がやや減少し（前年比－4 件）、「管理ミス」も減少（前年比－112 件）している。また、2011 年は「金融業，保険業」において 100 万人以上の大規模なインシデントが 2 件発生しているため、人数ベースの漏えい業種は「金融業，保険業」が突出した結果となっている。

2011 年の集計結果の概要データは、以下の通りである。

表 3-1：2011 年 個人情報漏えいインシデント 概要データ

漏えい人数	**628 万 4363 人**
インシデント件数	**1551 件**
想定損害賠償総額	**1899 億 7379 万円**
一件あたりの漏えい人数※1	**4238 人**
一件あたり平均想定損害賠償額※1	**1 億 2810 万円**
一人あたり平均想定損害賠償額※2	**4 万 8533 円**

※1：平均値は、被害者数が不明のインシデント 68 件を除いて算出している。
※2：この平均値は一件あたりのばらつきを吸収するため、まず、各インシデントの一人あたりの想定損害賠償額を算出し、そこから全てのインシデントの一人あたりの想定損害賠償額の平均額を算出している。よって、想定損害賠償総額を漏えい人数で割った値ではないことに注意されたい。

3.2 個人情報漏えいインシデント・トップ 10

表 3-2 に規模の大きいインシデント・トップ 10 を示す。2008 年は、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は 1 件も発生せず、2009 年と 2010 年は各 1 件ずつ発生した。2011 年は、3 件も発生した。

インシデント・トップ 10 の原因は、「内部犯罪・内部不正行為」「不正アクセス」「不正な情報持ち出し」といった故意を含んだ原因が目立っている。

業種は、「公務」が 2010 年と同様に件数が多く、「金融業，保険業」は件数が多いものの、減少傾向を示している。

表 3-2：インシデント・トップ 10

No.	漏えい人数	業種	原因
1	165 万 7131 人	金融業，保険業	不正な情報持ち出し
2	136 万 8307 人	金融業，保険業	管理ミス
3	100 万 7052 人	生活関連サービス業，娯楽業	不正アクセス
4	20 万 3731 人	情報通信業	不正アクセス
5	15 万 8248 人	金融業，保険業	内部犯罪・内部不正行為
6	12 万 8307 人	金融業，保険業	管理ミス
7	12 万 4900 人	金融業，保険業	管理ミス
8	9 万 2408 人	金融業，保険業	内部犯罪・内部不正行為
9	7 万 3000 人	卸売業，小売業	内部犯罪・内部不正行為
10	7 万人	情報通信業	誤操作

3.3 業種

(1) 単年分析(件数)

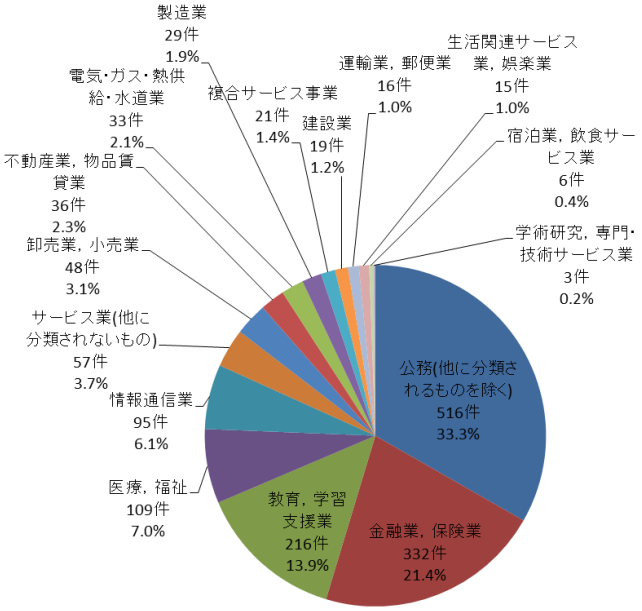

図 3-1：業種別比率（件数）

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」(33.3%)、「金融業，保険業」(21.4%)、「教育，学習支援業」(13.9 %)、「医療，福祉」(7.0%)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」については、2004 年以降、常に上位を占める結果となっている。これは、個人情報を取り扱うことが多いことに加え、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「農業、林業」「漁業」「鉱業，採石業，砂利採取業」の 3 業種だけである。その他のすべての業種で個人情報を利用しており、インシデント発生のリスクがあるという状況に変化は見られない。

(2)　経年分析(件数)

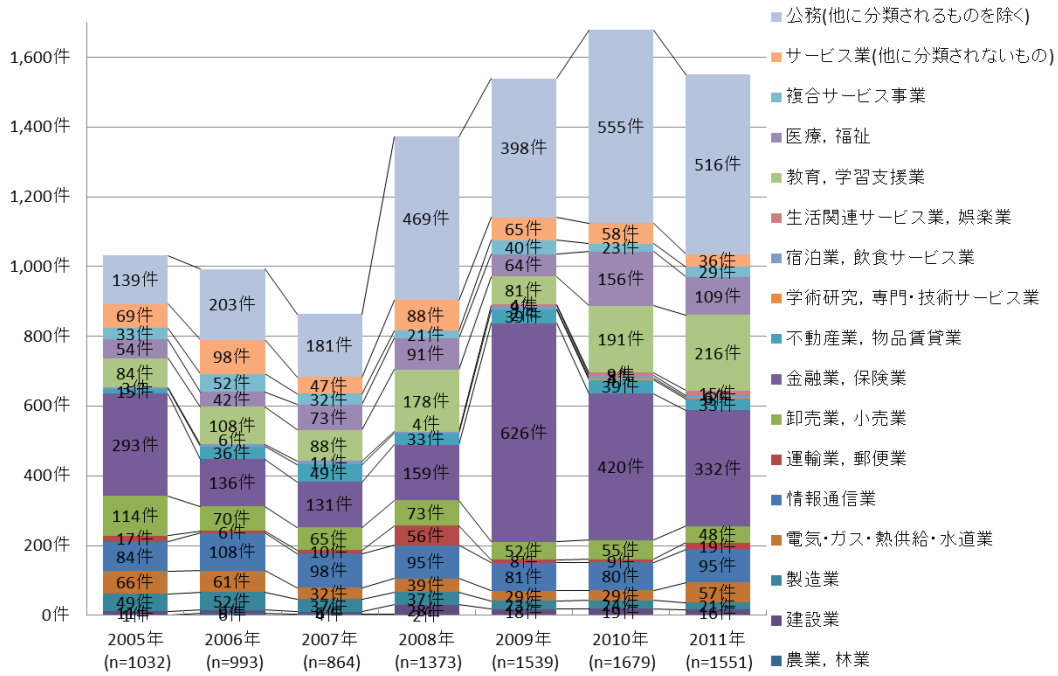

図 3-2：業種別件数の経年変化（件数）

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

「公務」は、2008 年以降、常に多くの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報告しているためである。

2009 年に減少に転じたかに見えた「教育，学習支援業」の件数は、2010 年以降、大きく増加している。「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。

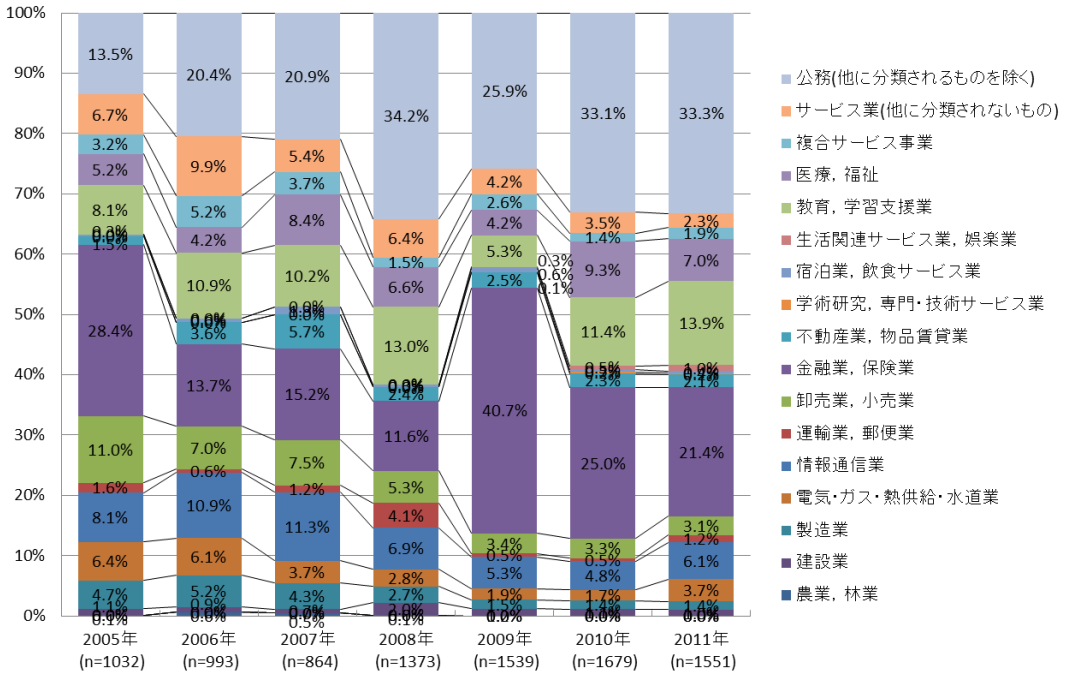

図 3-3：業種別比率の経年変化（件数）

業種別インシデント件数の比率の推移を図 3-3 に示す。2011 年は、2010 年とよく似た比率である。「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)

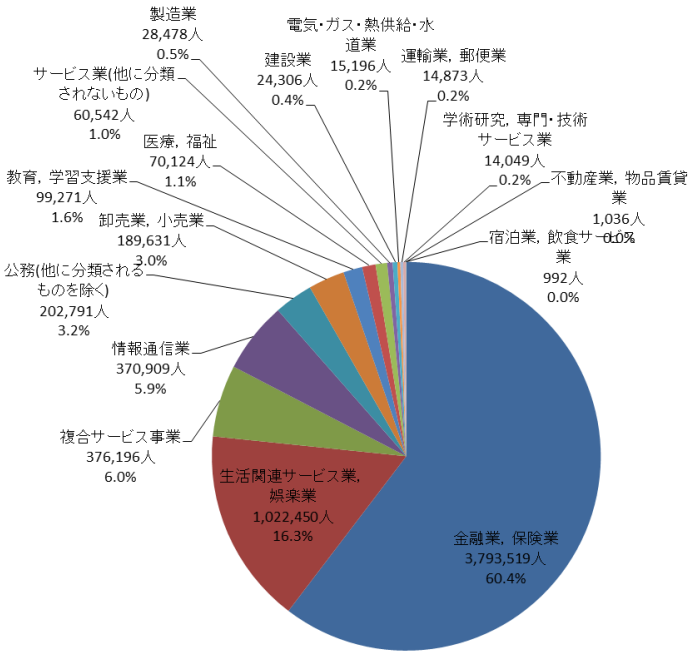

図 3-4：業種別比率（人数）

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」(60.4%)、「生活関連サービス業，娯楽業」(16.3%)「複合サービス業」(6.0%)である。大量の個人情報を電子的に処理することの多い業種に集中した。「金融業，保険業」は、「表 3-2：インシデント・トップ 10」に含まれるインシデントが 6 件発生しており、うち 2 件のインシデントが 100 万人を越えている。インシデント・トップ 10 に含まれるインシデントだけで、約 350 万人にのぼる。

「生活関連サービス業，娯楽業」は、インシデント 1 件のみであるが、漏えい人数が約 100 万人であったため、2 番目に多い 16.3%を占めた。

「公務」「教育，学習支援業」は、図 3-1 に示すように件数では全体の 47.2%を占めるが、図 3-4 に示すように人数では 4.8%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。

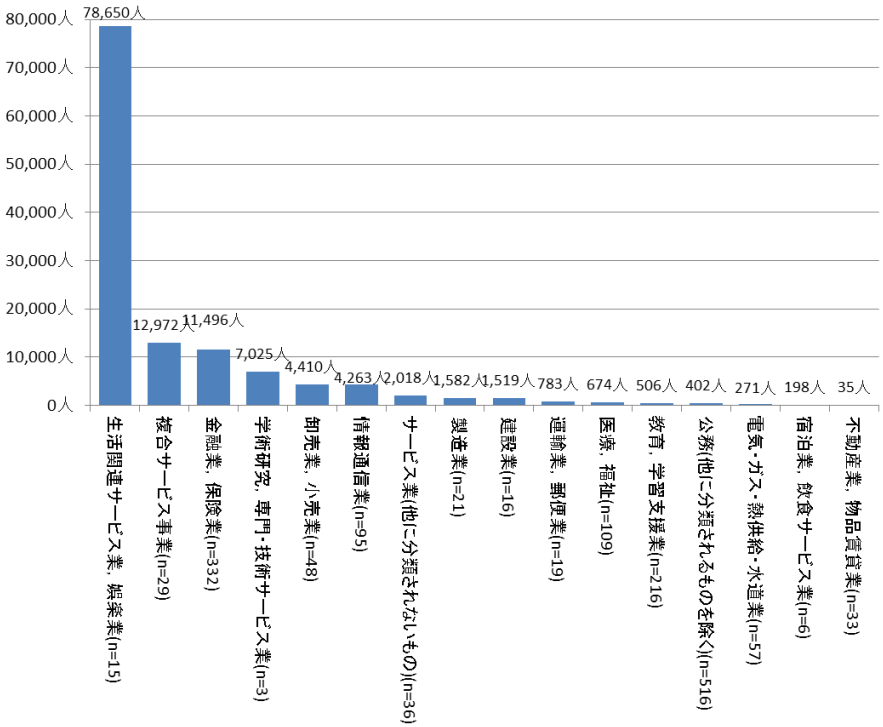

図 3-5：業種別の一件あたりの漏えい人数

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。「生活関連サービス業，娯楽業」（約 8 万人）が突出しているが、これは 15 件のインシデントのうち 1 件が 100 万人以上の大規模インシデントであったためである。

これにつづく上位の業種は「複合サービス業」（約 1.3 万人）、「金融業，保険業」（約 1.1 万人）、「学術研究，専門・技術サービス業」（約 7,000 人）となっている。

インシデントの件数では 1 位だった「公務」の一件あたりの平均漏えい人数は 402 人である。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 516 件のうち、396 件(76.7%)は 10 人未満の小規模インシデントである。こうしたインシデントの多くは、紙媒体の誤交付・誤送付などの誤操作、管理ミス、紛失・置き忘れによるものであった。業種別での漏えい規模の比較は、「3.6 漏えい規模」の図 3-25 を参照されたい。

(4)　Box-Whisher Diagram（箱髭図）（人数）

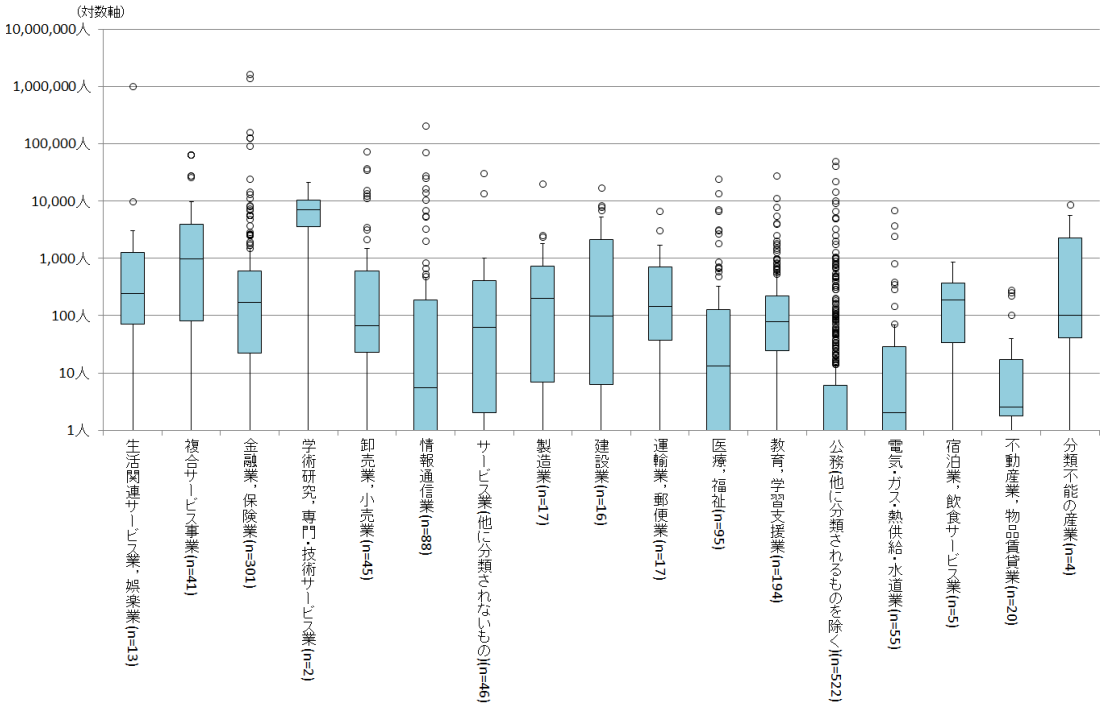

図 3-6：業種別の漏えい人数（箱髭図）

業種別のインシデント一件あたりの漏えい人数の Box-Whisher Diagram（箱髭図）[*1] を図 3-6 に示す。

「情報通信業」「サービス業」「製造業」「建設業」「医療，福祉」は、箱髭図の長方形の部分が 10 人未満から 1000 人程度の範囲に長く伸びており、主なインシデントの漏えい人数が数人から数百人の比較的少人数の範囲でばらついていることがわかる。一方、「金融業，保険業」は、箱髭図の長方形の部分が 1 万人付近にあり、主なインシデントの規模が最も大きいことがわかる。「公務」は、箱髭図の長方形の部分が 1 人から 14 人である。主なインシデント[*2] のほとんどが、小規模なインシデントであることがわかる。

またほとんどの業種において、漏えい人数の大きい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個人情報を取り扱っている場合は、まれに大量の個人情報漏えいインシデントが発生する恐れを考慮しなければならないと思われる。

[*1] 箱髭図の長方形の下辺は第 1 四分位数、中央の線はメディアン（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＋3×（1/2×（第 3 四分位数－第 1 四分位数）」である。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。長方形の下辺から伸びる線の先端は「第 1 四分位数－3×（1/2×（第 3 四分位数－第 1 四分位数）」であり、これより小さいデータも外れ値となる。これらの外れ値は、正規分布でいう 3 シグマに相当するものと等価である。

[*2] 「公務」はメディアン（中央値）が 1 人であり、かつ最小値が 1 人であるため、図 3-6 の長方形の下半分は描画されない。

(5)　経年分析(人数)

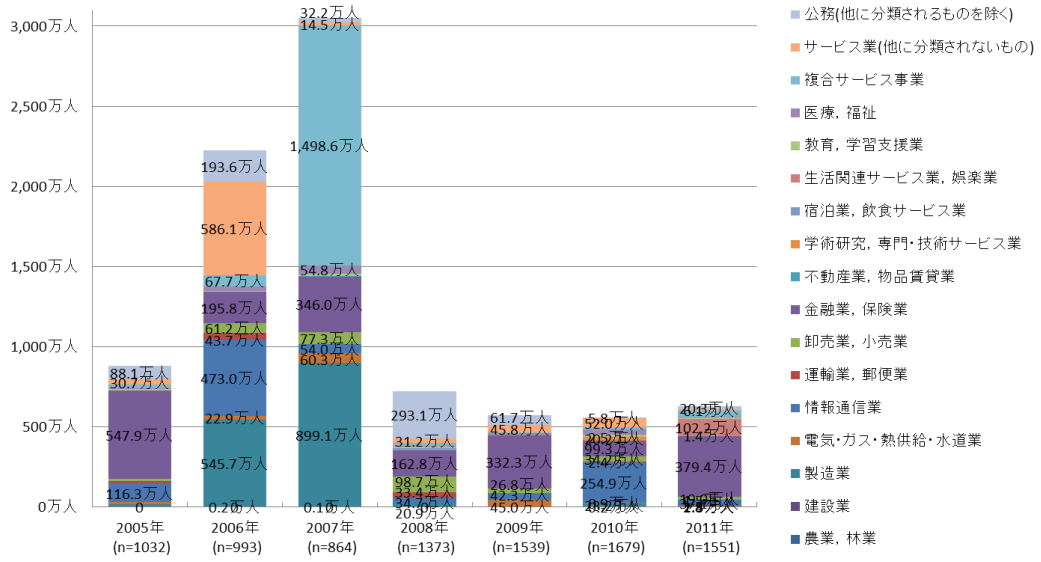

図 3-7：業種別漏えい人数の経年変化（合計）

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、2007 年の漏えい人数が多くなっているが、いずれの年も 100 万人以上の大規模なインシデントが多く発生した年である。そのため、大規模なインシデントが発生した業種の人数が特異的に増えてしまい、2006 年は情報通信業が、2007 年では複合サービス業が突出したグラフになっている。同様に 2011 年は「金融業，保険業」が数としては他業種より突出している。つまり、業種別の個人情報漏えい人数に関しては、業種による特徴よりも、大規模な情報漏えいインシデントが発生した業種が目立つ傾向になっている。

(6)　相関分析

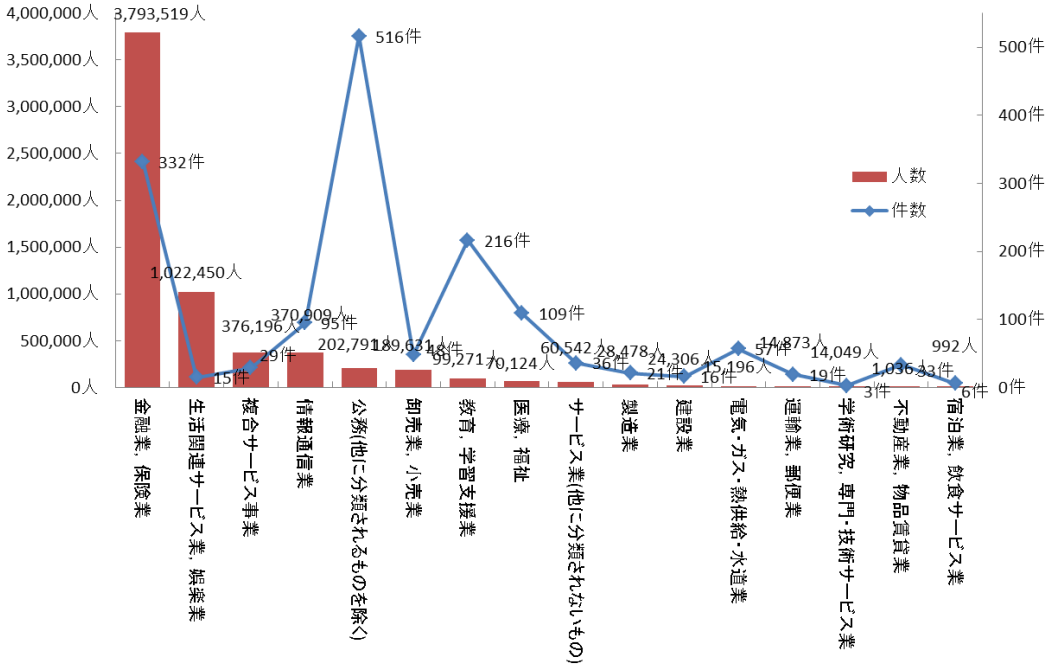

図 3-8：業種別のインシデント件数と漏えい人数

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。2011 年に 100 万人以上の大規模インシデントが 1 件発生した「生活関連サービス業，娯楽業」は、インシデント件数に比して漏えい人数が突出して多い。

逆に、インシデント件数の多かった「公務」「教育，学習支援業」「医療，福祉」は、小規模インシデントでも公表されることが多いため、インシデント件数に対して漏えい人数は少ない。

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

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

3.4 原因

(1)　単年分析(件数)

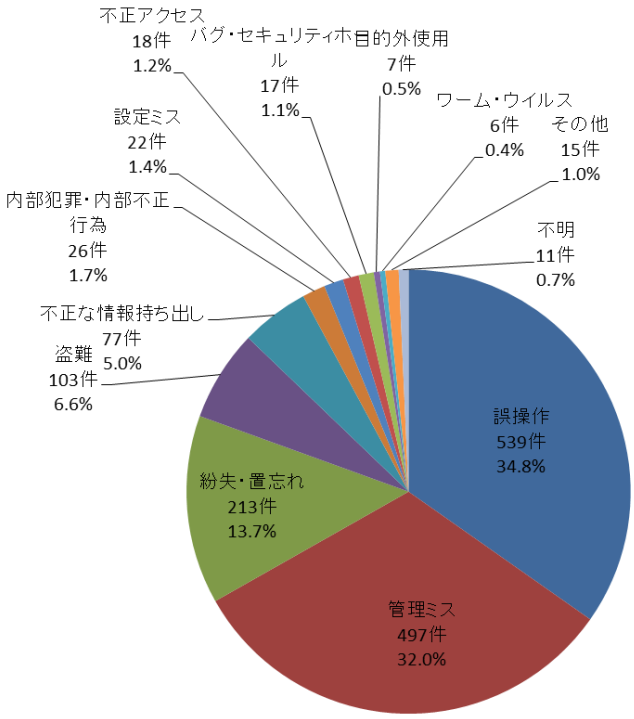

図 3-9：漏えい原因比率（件数）

個人情報漏えい件数の原因比率を図 3-9 に示す。2011 年は「誤操作」、「管理ミス」、「紛失・置き忘れ」で約 80%を占めた。「管理ミス」に区分されるインシデントは、組織としてルールが整備されていない、もしくはルールは存在しているものの遵守されていないために社内や主要な流通経路で発生するインシデントである。組織としてルールが整備されていないことによるインシデントは、発見が遅れインシデントに至る経緯を明確できない場合も多い。

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

「誤操作」および「紛失・置き忘れ」はヒューマンエラーである。そのため対策としては、人的な対策として担当者へのセキュリティ教育(オペレーションの教育も含む)、およ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として暗号化などの漏えい対策や、紛失しても被害が拡大しない対策もあわせて行うことも検討に

値する。

(2)　経年分析(件数)

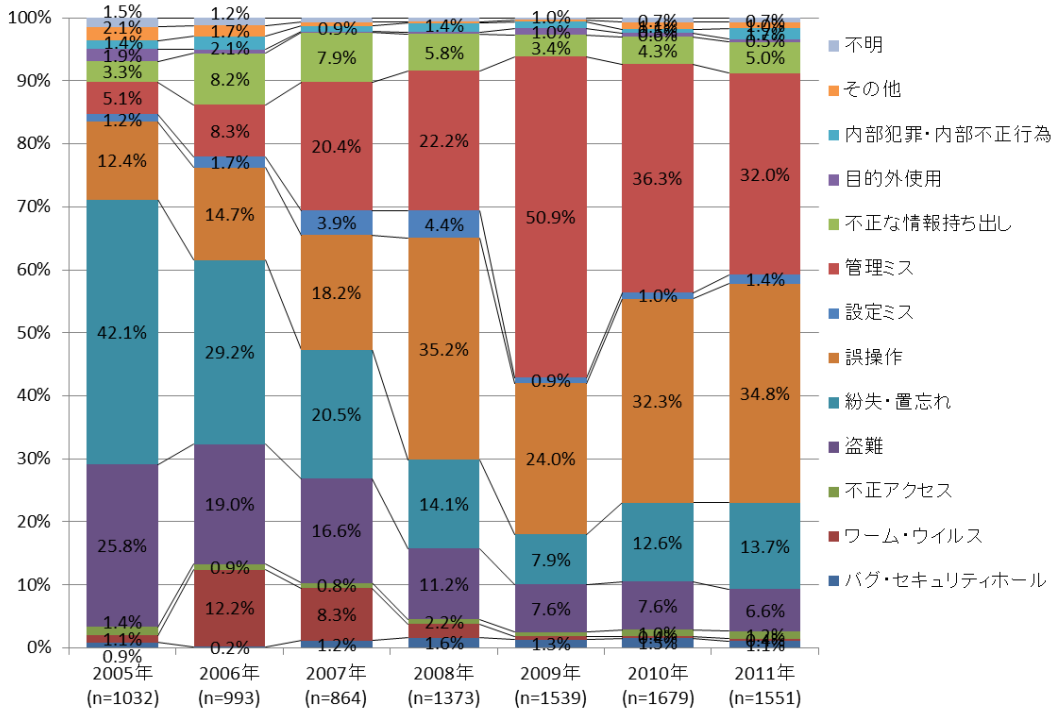

図 3-10：漏えい原因比率の経年変化（件数）

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。2011 年は、2010 年とよく似た比率である。2009 年で 50.9%(784 件)を占めていた「管理ミス」は、2010 年が 36.3%(609 件)、2011 年が 32.0%(497 件)と減少している。一方で「誤操作」の比率は、2009 年が 24.0%(369 件)、2010 年が 32.3%(543 件)、2011 年が 34.8%(539 件)、「紛失・置き忘れ」の比率は、2009 年が 7.9%(122 件)、2010 年が 12.6%(211 件)、2011 年が 13.7%(213 件)へ増加している。

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

2005 年以降、管理ミスと誤操作が増加傾向にあったが、2010 年と 2011 年は、その増加が止まった傾向がみえる。

(3)　単年分析(人数)

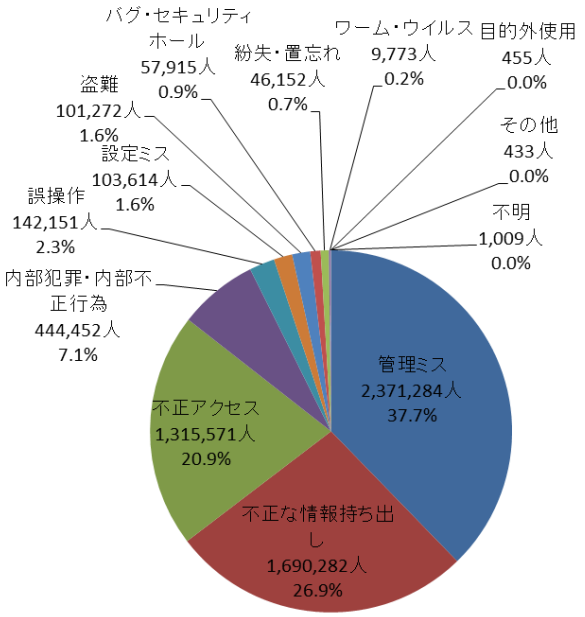

図 3-11：漏えい原因比率（人数）

個人情報漏えい人数の原因比率を図 3-11 に示す。

漏えい人数の原因比率を示す上記図 3-11 と前述した漏えい件数の原因比率である図 3-9 を比べると、傾向に違いが見られる。図 3-9 のように件数で集計すると、「誤操作」「管理ミス」「紛失・置き忘れ」など当事者には悪意がない原因が並ぶが、図 3-11 のように人数で集計すると、「不正な情報持ち出し」「不正アクセス」「内部犯罪・内部不正行為」など当事者に悪意が認められる原因が上位に入る。

「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 2011 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」への対策は重要であることが読み取れる。

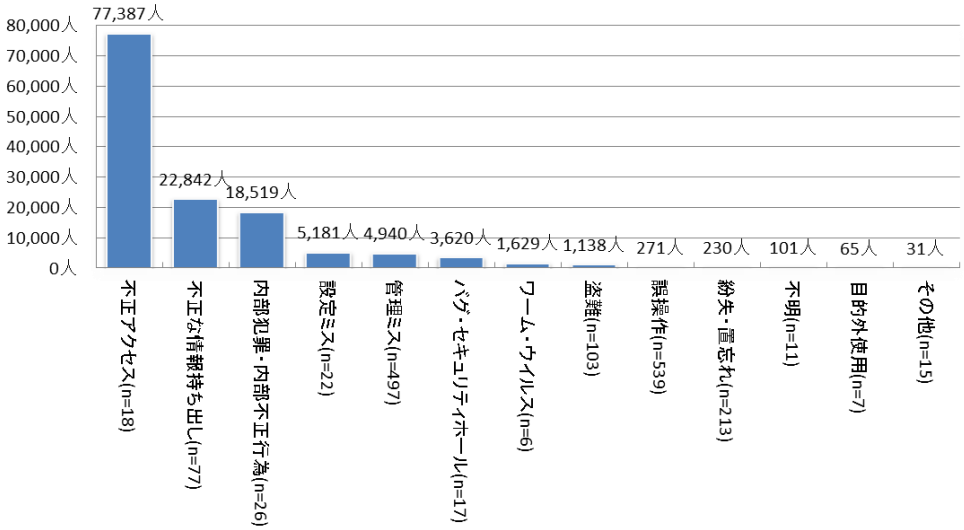

図 3-12：漏えい原因別の一件あたりの漏えい人数

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、「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」の一件あたりの漏えい人数が目立つ。「不正アクセス」の一件あたりの漏えい人数が多い要因は、インシデント・トップ 10 の第 3 位と第 4 位に 2 件のインシデントによって平均人数が増加したためである。「不正アクセス」は、悪意のある者が個人情報の集まりであるファイルやデータベースを対象にして行うため、発覚すると常にまとまった数の個人情報件数が漏えいすると推測される。

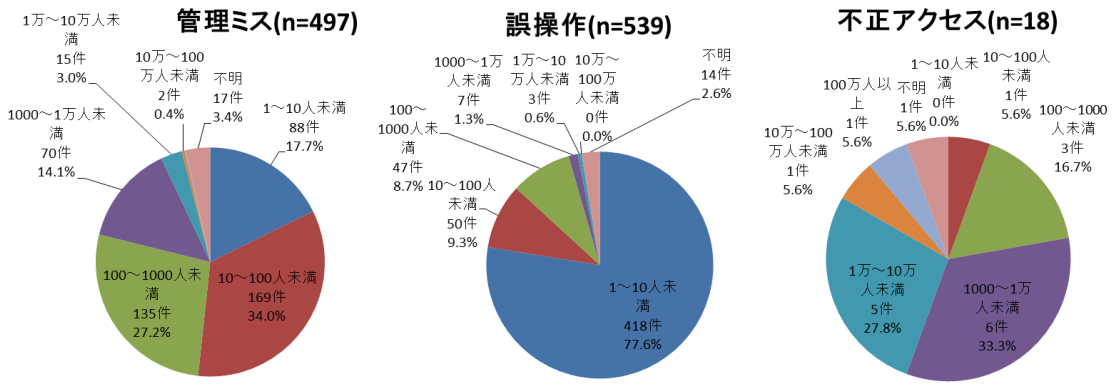

図 3-13：漏えい原因の人数区分（件数）

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。件数では第 2 位、漏えい人数では第 1 位の「管理ミス」は 10～100 人未満と 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。

件数で第 1 位であった「誤操作」は、10 人未満の情報漏えいインシデントが 4 分の 3 以上を占めており、少ない人数の漏えいインシデントが目立つ。

「不正アクセス」は、1000 人以上～1 万人未満と 1 万人以上～10 万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「不正アクセス」への対策についても、優先順位を上げて検討しておく必要があると考えられる。

(4) Box-Whisher Diagram(箱髭図)(人数)

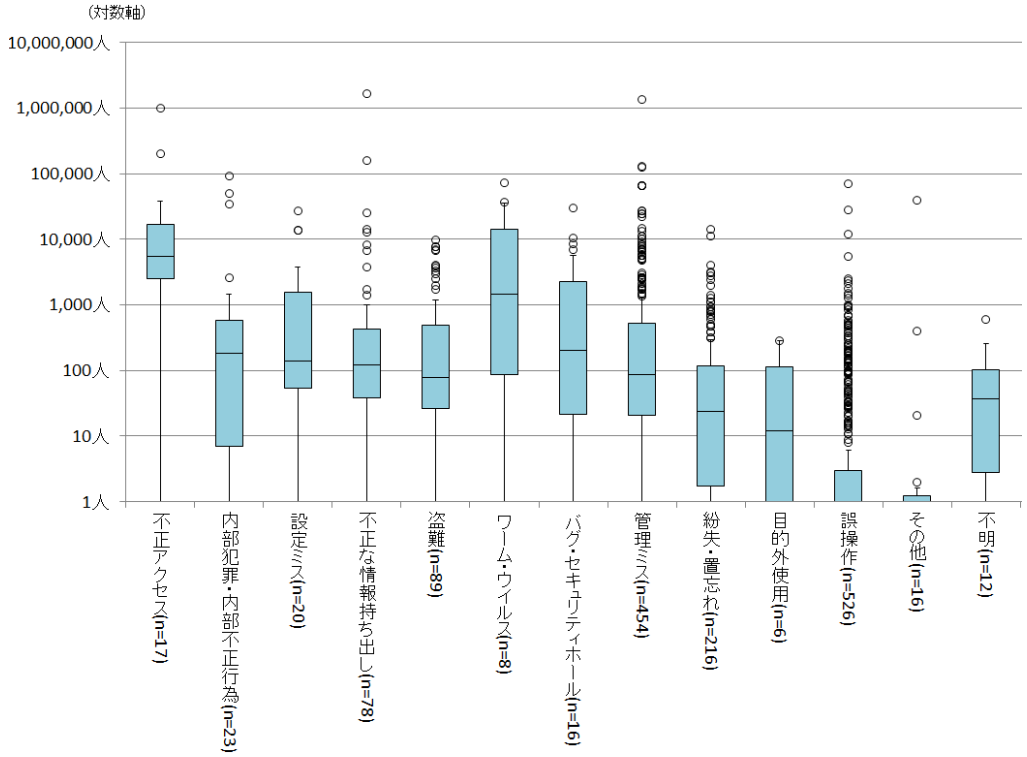

図 3-14：漏えい原因の漏えい人数（箱髭図）

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 Box-Whisher Diagram(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」は、漏えい人数が大きい範囲に分布している傾向にある。また、「不正な情報持ち出し」「管理ミス」「誤操作」は、大きい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。

* 「誤操作」はメディアン（中央値）が 1 人であり、かつ最小値が 1 人であるため、図 3-14 の長方形の下半分は描画されない。

(5)　業種別(件数)

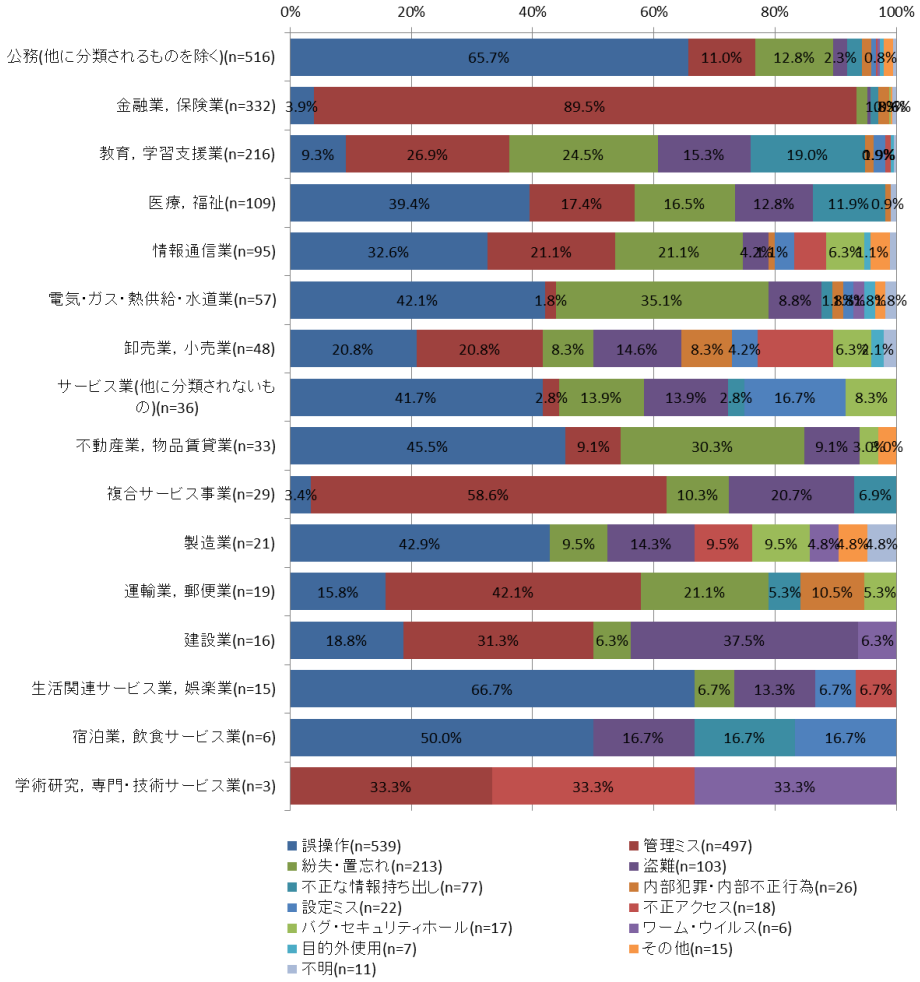

図 3-15：業種別の漏えい原因比率（件数）

業種別の漏えい原因比率を図 3-15 に示す。「公務」は、「誤操作」の占める比率が高く、公表された件数は 339 件となっている。2011 年の「誤操作」の全件数は 516 件であるため「誤操作」の 66%を占めていることになる。内訳としては、郵送やメールの誤送付が多く、日常業務の中で情報送付という作業が多いことに起因していると推測される。

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

「教育・学習支援業」は、「不正な情報持ち出し」の比率が 19%と、他の業種に比べて高い。件数は 41 件で、他の業種に比べて突出しており、「不正な情報持ち出し」がもっとも多い業種となっている。「不正な情報持ち出し」は当事者の意識の問題に

よるところが大きいが、まとまった件数が発生する場合は、業務特性と個人情報の持ち出しルールがかい離し、形骸化している可能性もある。

3.5 漏えい媒体・経路

(1) 単年分析(件数)

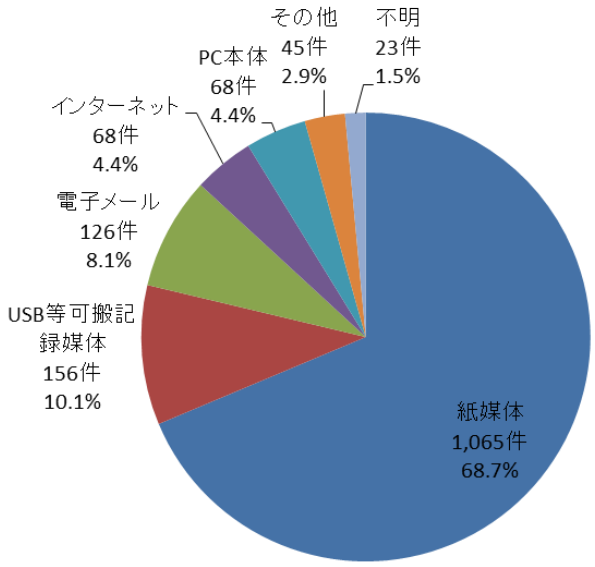

図 3-16：漏えい媒体・経路（件数）

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 68.7%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 10.1%、「電子メール」が 8.1%を占める。

(2)　経年分析(件数)

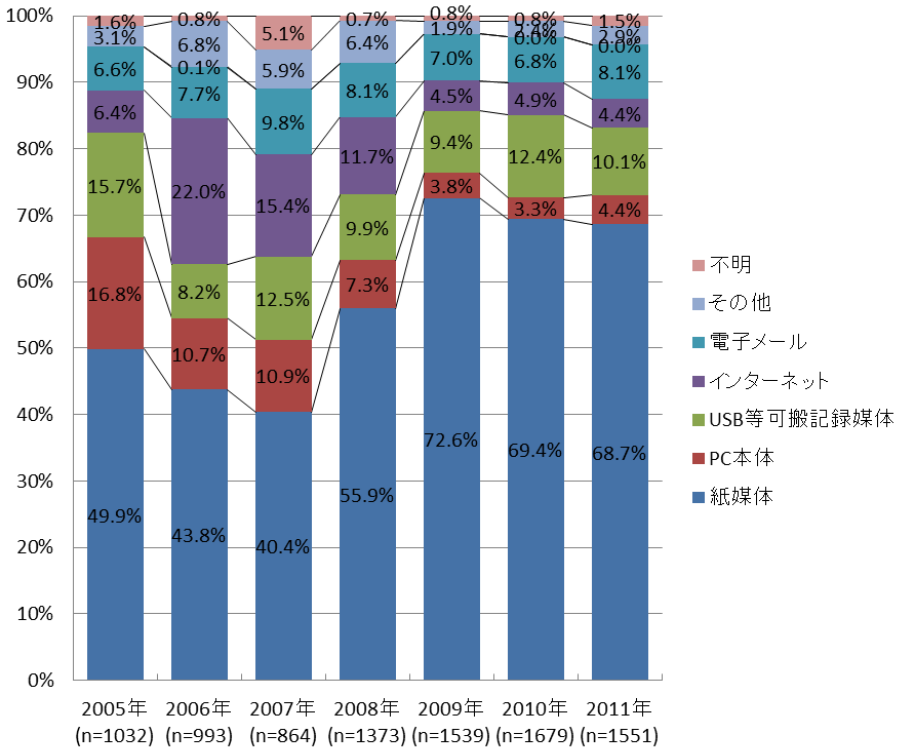

図 3-17：漏えい経路比率の経年変化（件数）

漏えい経路比率の経年変化について図 3-17 に示す。

「紙媒体」による漏えい件数は、2009 年に引き続き 2010 年、2011 年と原因の大半を占める。2009 年以降、件数の割合に大きな変化はない。

(3)　単年分析(人数)

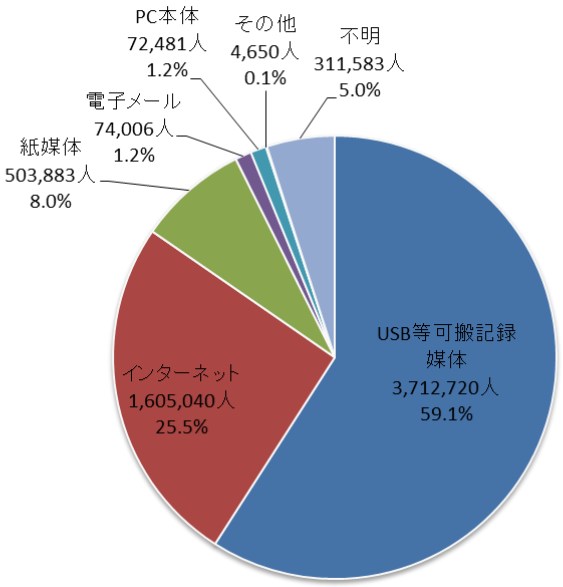

図 3-18：漏えい媒体・経路（人数）

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」が約 59.1%を占める。「表 3-2：インシデント・トップ 10」のうち、第 1 位、第 2 位、第 6 位の 3 件が「USB 等可搬記録媒体」であった。この 5 件のインシデントだけで合計約 315 万人、漏えい人数の実に約 50%を占める。

2010 年に最も人数の多かった「インターネット」は、25.5%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、4 位、第 9，10 位の 4 件も発生している。

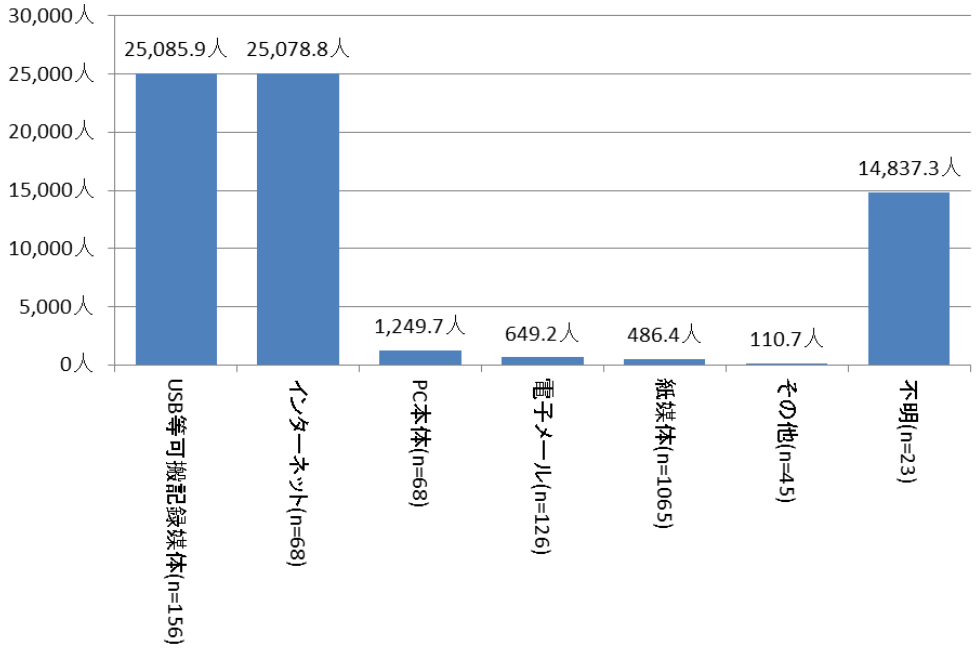

図 3-19：漏えい媒体・経路別の一件あたりの漏えい人数

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」「インターネット」が多い。「USB 等可搬記録媒体」と「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、それらのデータを受け渡しやすい USB メモリやインターネットを経由して漏えいしたと思われる。

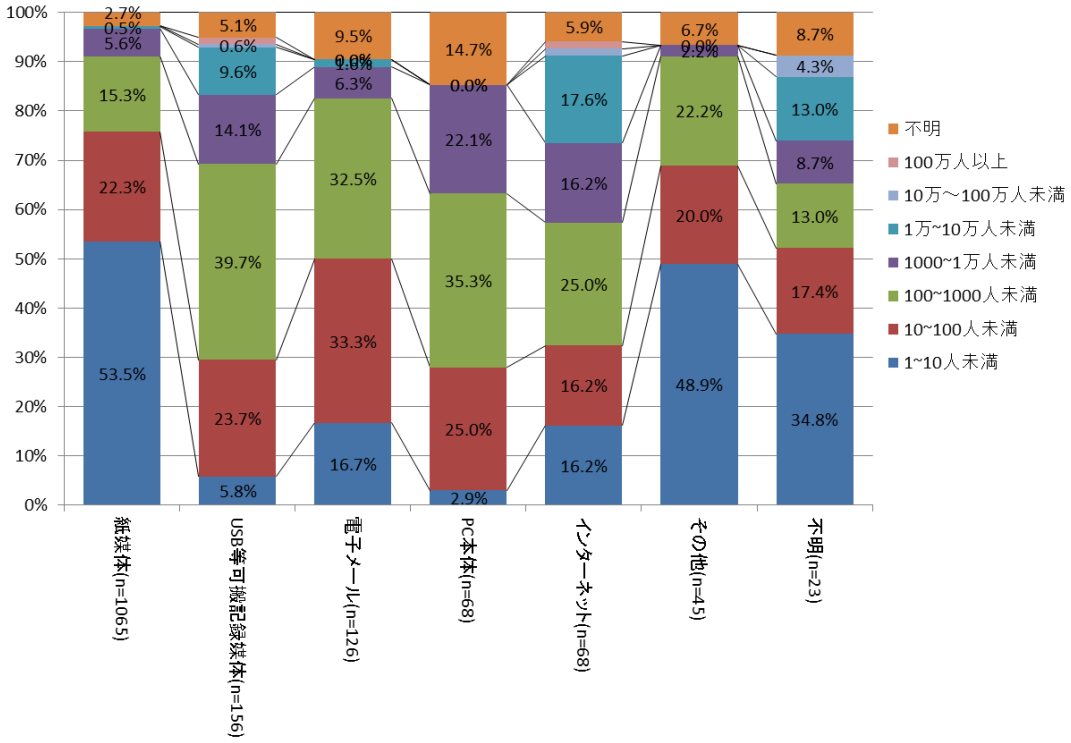

図 3-20：漏えい規模比率(件数)

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約 90%を占め、とくに 1~10 人未満の小規模なインシデントの比率が約 55%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、10 人以上～100 人未満と 100 人以上～1000 人未満のインシデントの比率がいずれも約 33%と高い。

一方で「インターネット」によるインシデントは、漏えい規模が 10 万人未満のインシデントがまんべんなく発生している。「インターネット」の場合、1 万人以上～10 万人未満の比較的規模の大きいインシデントの比率が高い。

(4) Box-Whisher Diagram(箱髭図)(人数)

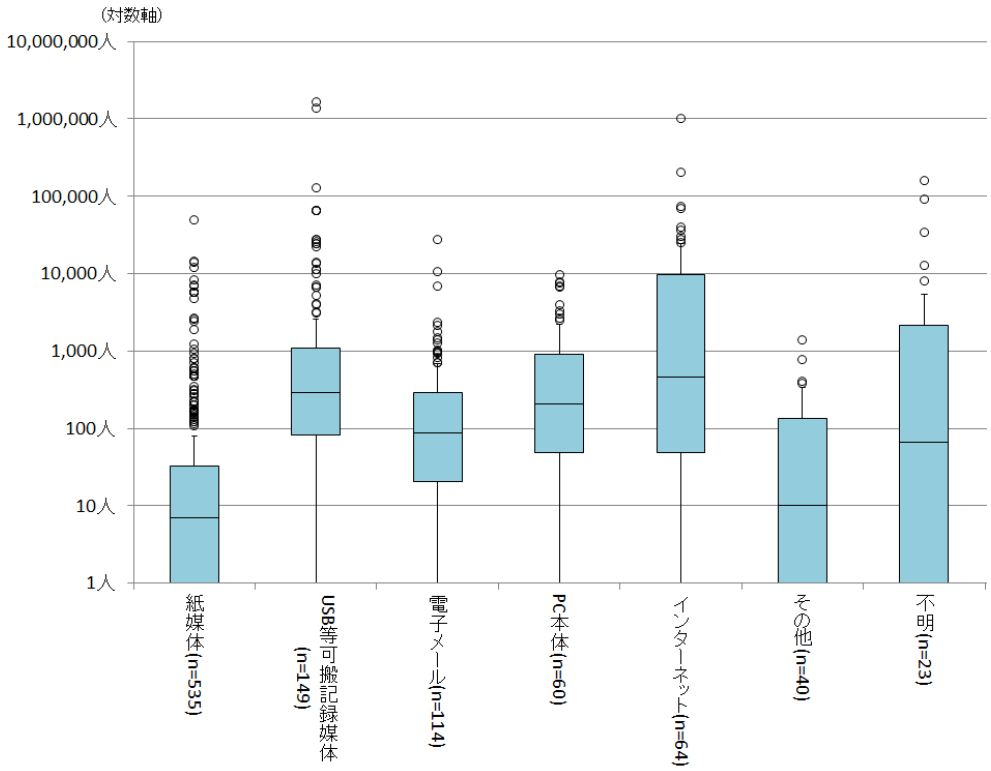

図 3-21：漏えい経路の漏えい人数（箱髭図）

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 Box-Whisher Diagram(箱髭図)を図 3-21 に示す。「インターネット」の漏えい人数の分布は、ほかの漏えい経路と比べて、やや漏えい人数が多い傾向にあることがわかる。また、「紙媒体」のインシデントだけは、他のインシデントと分布が異なり、75%以上のインシデントが漏えい人数 100 人未満である。ただし、5 万人規模のインシデントも発生している。

(5)　業種別(件数)

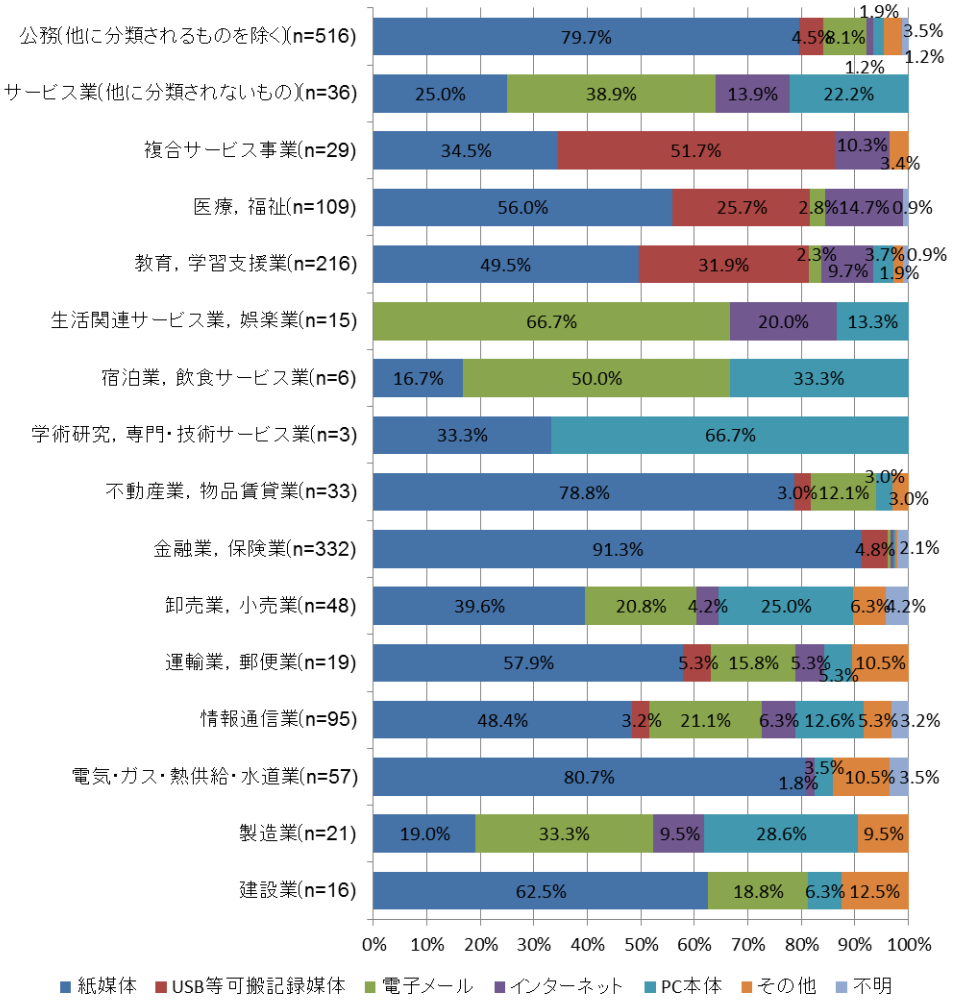

図 3-22：業種別の漏えい経路比率（件数）

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。「金融業，保険業」「電気・ガス・熱供給・水道業」「公務」「不動産業，物品賃貸業」は、特に比率が高い。「複合サービス業」「医療，福祉」「教育，学習支援業」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

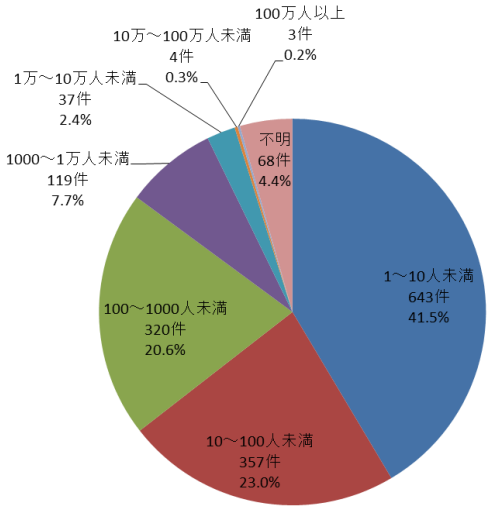

図 3-23：漏えい規模比率（件数）

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。インシデントの漏えい規模が小さいほど、インシデント件数が多いことがわかる。漏えい人数 1000 人未満のインシデントを合計すると 85.1%になり、全体の 8 割以上を占めている。

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

(2)　経年分析(件数)

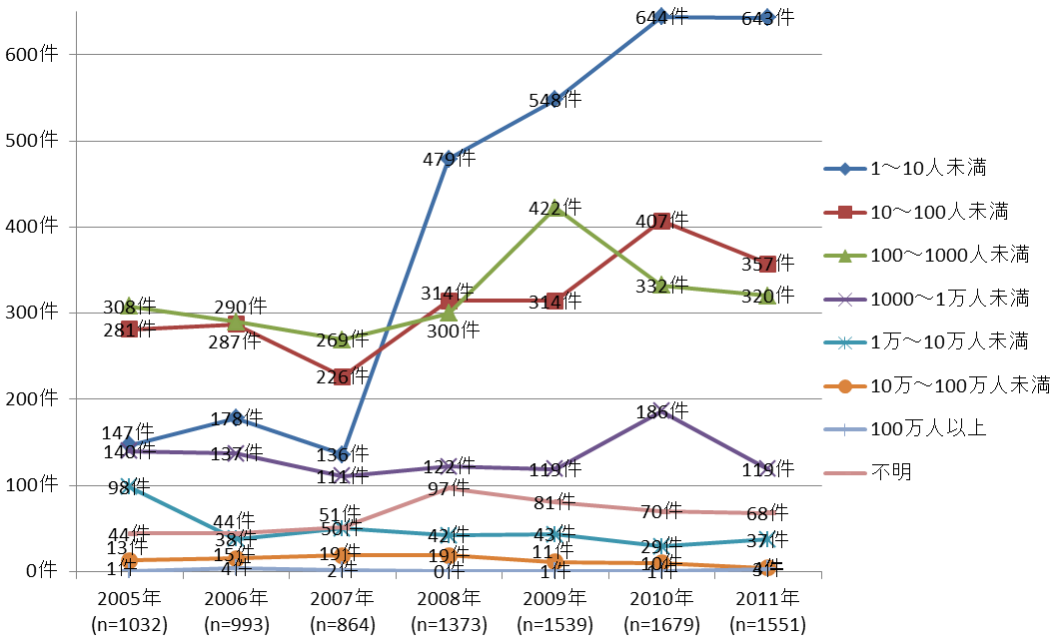

図 3-24：一件あたりの漏えい人数区分の経年変化（件数）

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。2011 年は、2010 年と比べて、10～100 人未満と 1000～1 万人未満の件数がやや減少した以外は、あまり変化がない。

2008 年以降、最も漏えい規模の小さい「1~10 人未満」の区分が、最もインシデント件数が多い。これは、規模の小さいインシデントが実際に増加したということではなく、規模の小さいインシデントでも公表する組織が増えてきたためと考えられる。

(3)　業種別（件数）

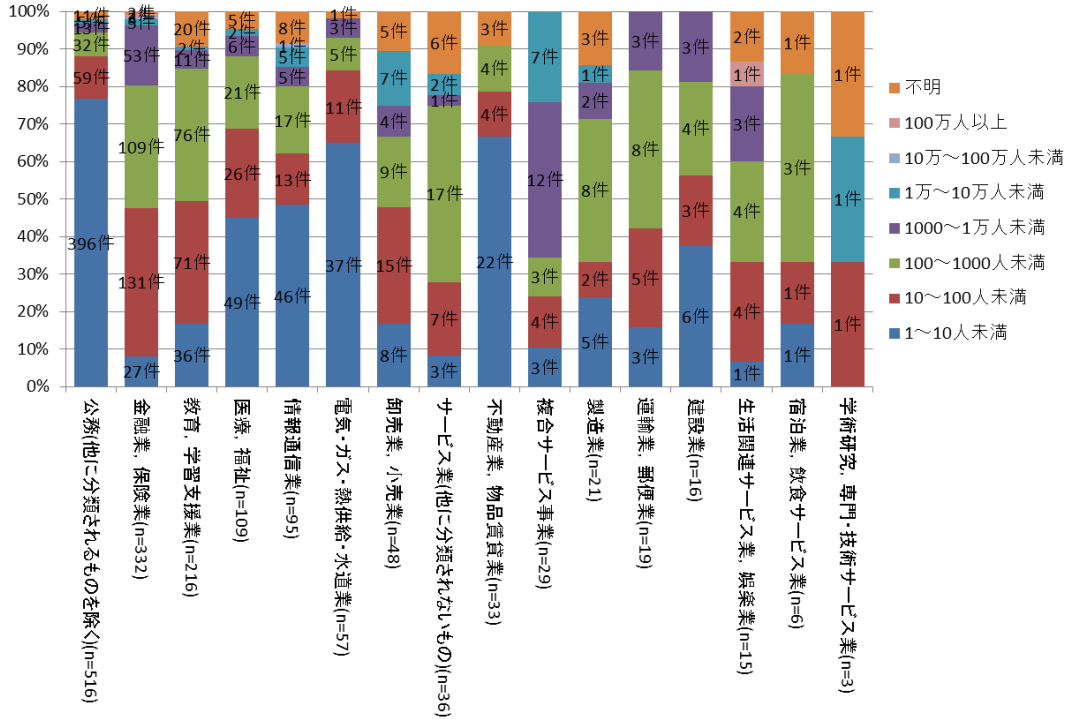

図 3-25：業種別の漏えい規模比率（件数）

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」「不動産業、物品賃貸業」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。

3.7 漏えい情報の価値

(1) 漏えい情報

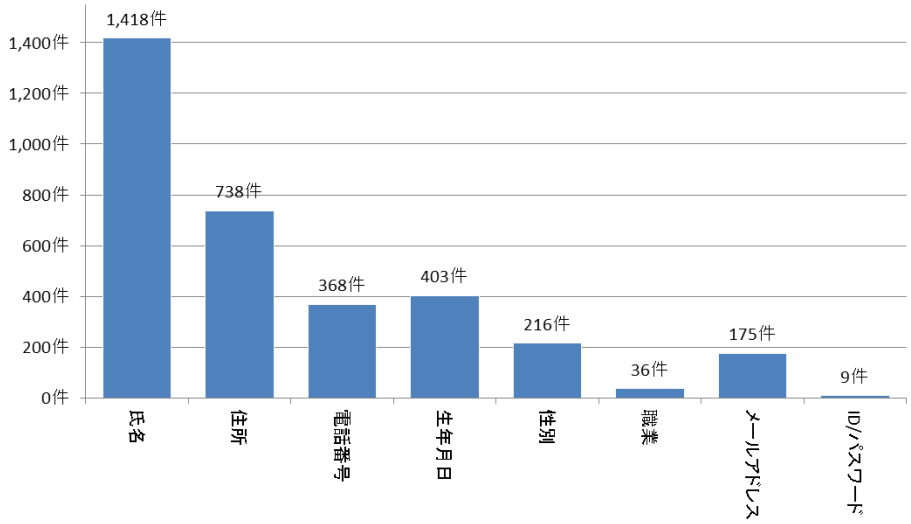

図 3-26：漏えい情報の出現確率

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	1,418 件	88.2%
住所	738 件	45.9%
電話番号	368 件	22.9%
生年月日	403 件	25.1%
性別	216 件	13.4%
職業	36 件	2.2%
メールアドレス	175 件	10.9%
ID/PASSWD	9 件	0.6%

漏えい情報の出現確率を図 3-26、表 3-3 に示す。

「氏名」の出現率が 88.2%であり、著しく高い。次いで住所（45.9%）、電話番号（22.9%）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)

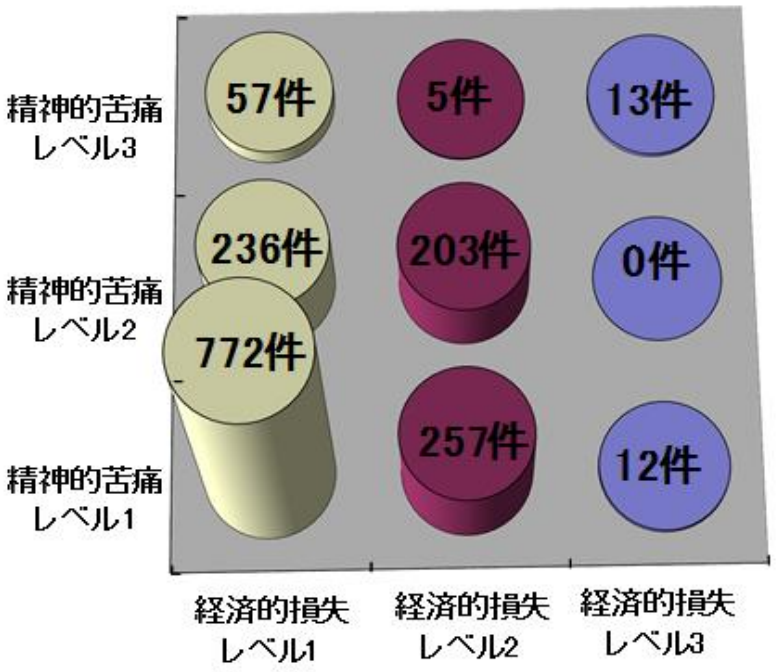

図 3-27：シンプル EP 図分布（件数）

2011 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。 シンプル EP 図については、P46～P47 を参照されたい。

2011 年の被害分布状況の特徴は、2010 年と類似している。2010 年との違いは、精神的苦痛と経済的損失のレベルが共に 2 であるフィールドが大幅に減少した点である。

(2)　業種別EP分布

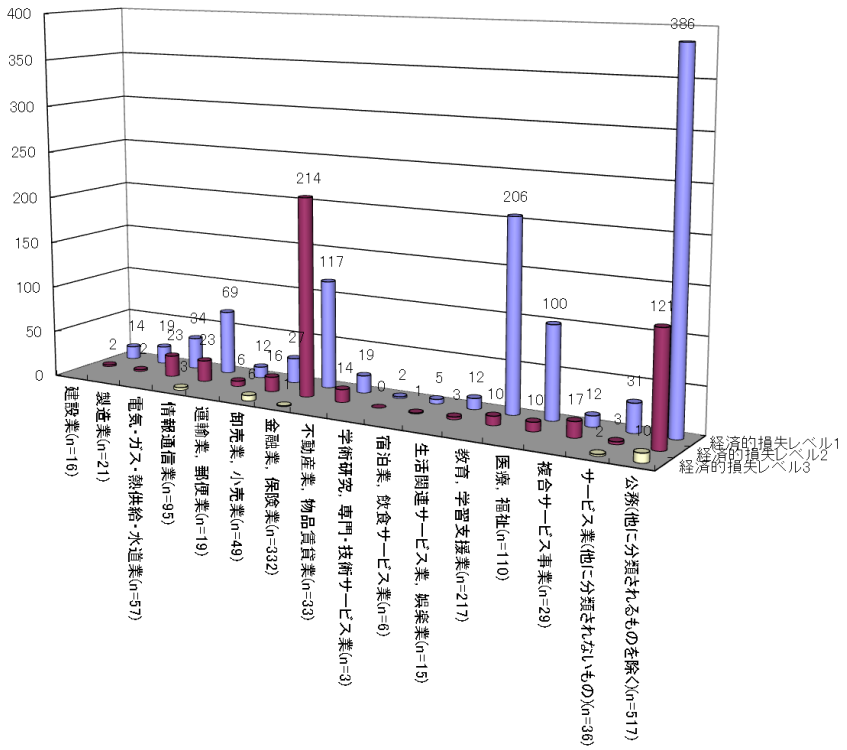

図 3-28：漏えい情報の経済的損失レベル分布（件数）

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が、これは預金残高等やクレジットカード情報が多いためだと考えられる。

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

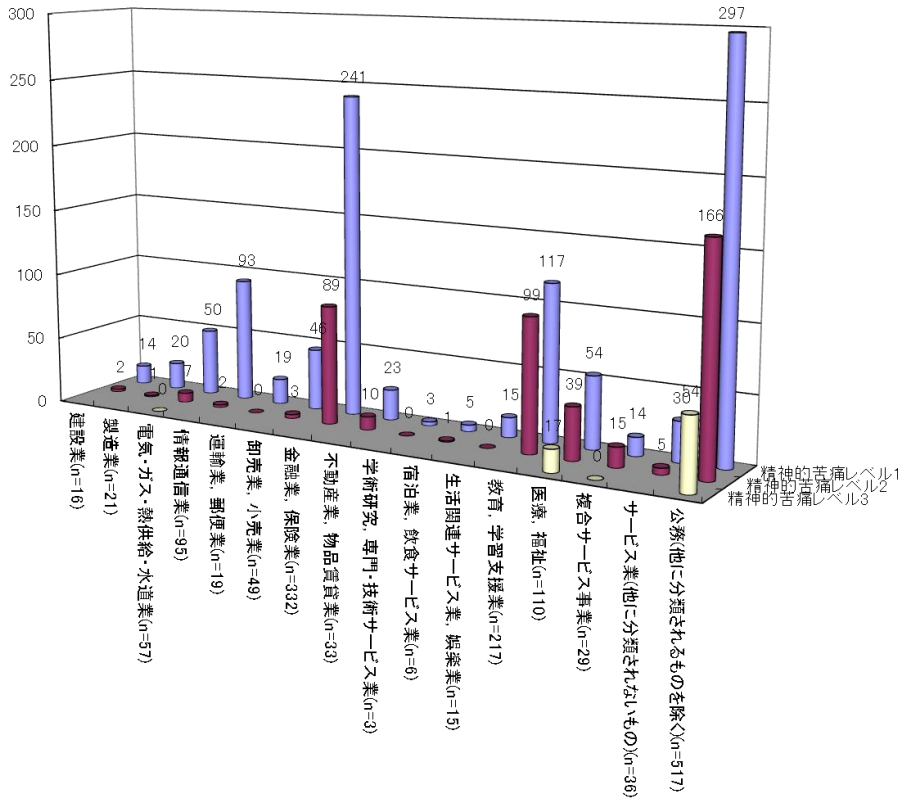

図 3-29：漏えい情報の精神的苦痛レベル分布（件数）

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、「公務」「教育，学習支援業」「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 2011 年の間に収集した 7 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、2011 年の分析では、これらを除外した。

表 3-4：漏えい人数とインシデント件数の経年変化

	インシデント件数	漏えい人数	一件あたりの平均漏えい人数※
2005 年	1,032 件	881 万 4,735 人	8,922 人
2006 年	993 件	2,223 万 6,576 人	2 万 3,432 人
2007 年	864 件	3,053 万 1,004 人	3 万 7,554 人
2008 年	1,373 件	723 万 2,763 人	5,668 人
2009 年	1,539 件	572 万 1,498 人	3,924 人
2010 年	1,679 件	557 万 9,316 人	3,468 人
2011 年	1,551 件	628 万 4,363 人	4,238 人

2011 年のインシデント件数は、2010 年よりやや減少した。一方、漏えい人数は 2010 年より増加した。2008 年以降、2006 年や 2007 年のような漏えい人数が非常に多い状況は発生していない。結果、個人情報が漏えいした人は、日本の人口の約 20 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 2011 年は 1551 件から被害者数不明の 68 件を除いた 1483 件で漏えい人数を除算した。

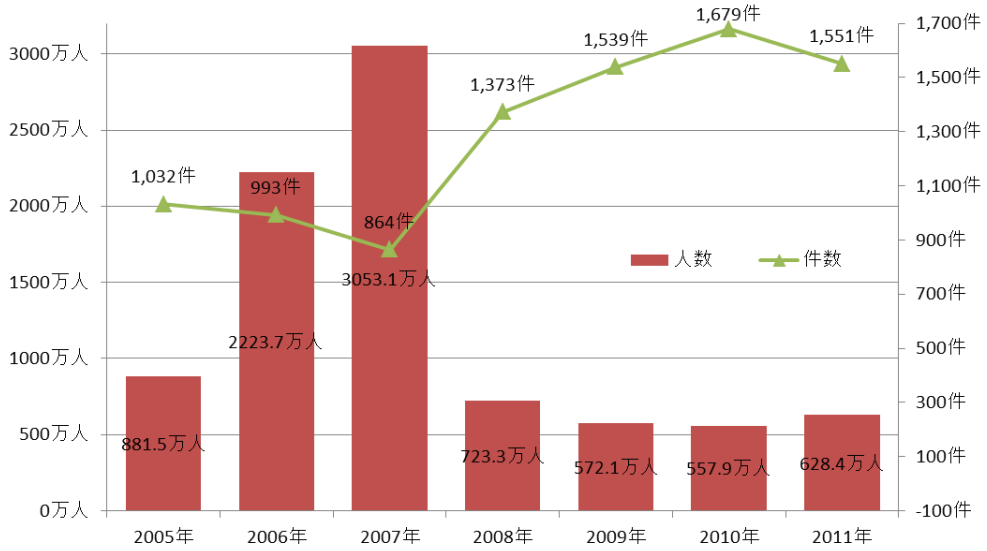

図 3-30 インシデント件数と漏えい人数の経年変化（合計）

インシデント件数と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 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、2011 年は 1551 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、毎年 1500 件程度のインシデントが公表されている。

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

表 3-5：内部不正による漏えい人数の経年変化の割合

原因	2005 年	2006 年	2007 年	2008 年	2009 年	2010 年	2011 年
内部犯罪・内部不正行為	10. 2%	18. 0%	28. 3%	4. 4%	29. 1%	8. 4%	7. 1%
内部犯罪・内部不正行為以外	89. 8%	82. 0%	71. 7%	95. 6%	70. 9%	91. 6%	92. 9%

内部犯罪・内部不正行為による漏えい人数の割合は、2011 年は 7.1%であった。

内部犯罪・内部不正行為の件数が少ないため、1 件の漏えい規模（漏えい人数）によって表 3-5 の割合は大きく変化する。そのため、人数ベースでの分析では、特に決まった傾向はみられない。

4　2011 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

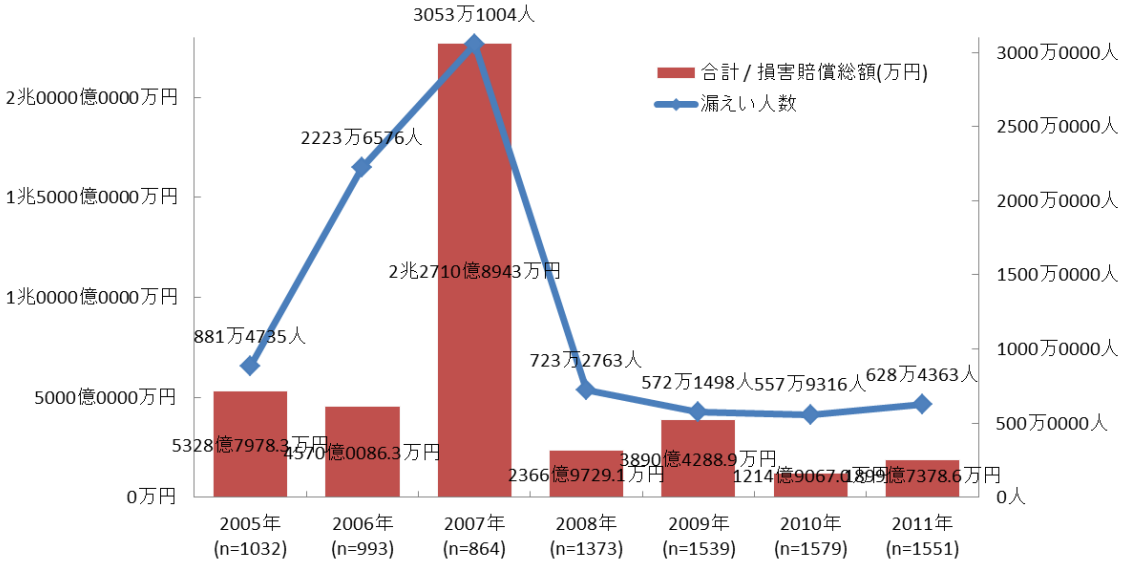

図 4-1：想定損害賠償総額と漏えい人数

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。その中で 2011 年の漏えい人数と想定損害賠償総額を 2010 年と比較すると、漏えい人数、想定損害賠償総額ともに微増している。

4.2 一人あたりの想定損害賠償額

(1) 単年分析

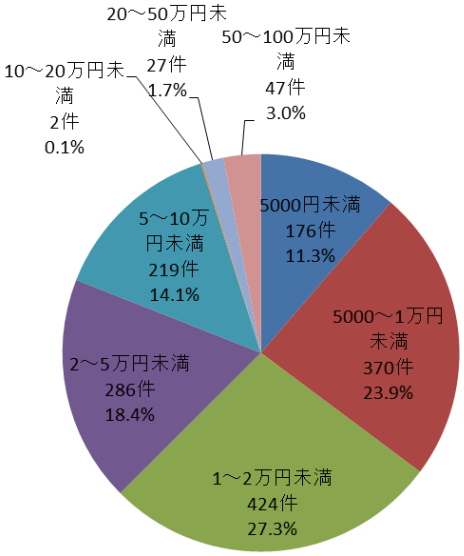

図 4-2：一人あたりの想定損害賠償額比率（件数）

一人あたりの想定損害賠償額を図 4-2 に示す。

2010 年は、一人あたりの想定損害賠償額が「1～2 万円未満」のインシデント件数の占める比率が約 27%と最も多く、次いで「5000～1 万円未満」の比率が約 24%、合わせて約 50%となった。

(1)　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

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

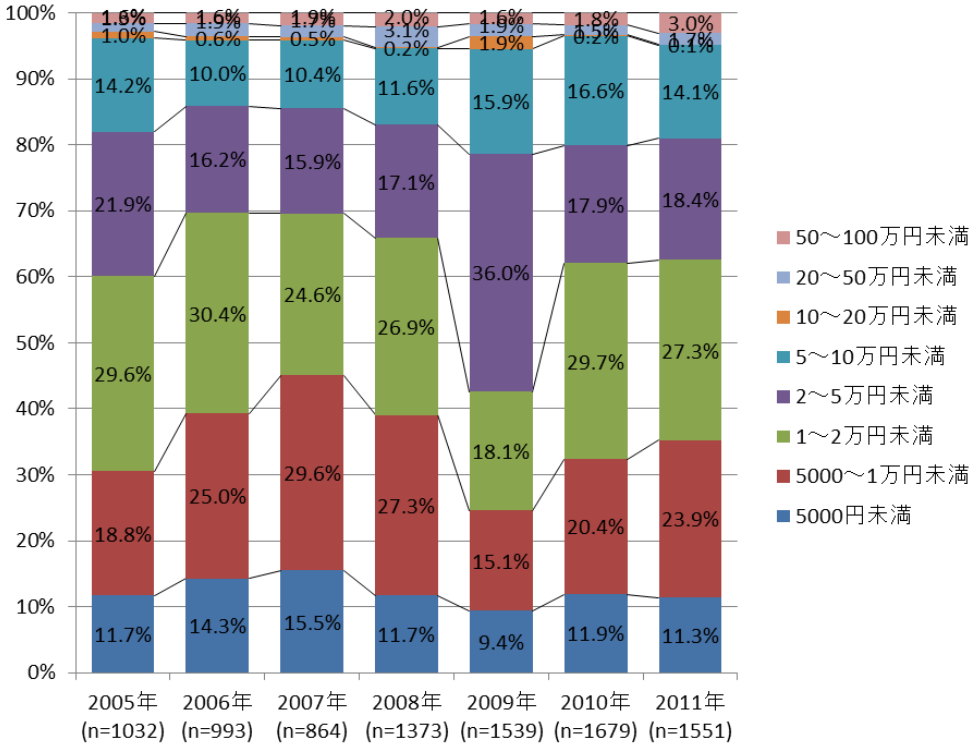

図 4-3：一人あたりの想定損害賠償額比率の経年変化（件数）

一人あたりの想定損害賠償額比率の経年変化を図 4-3 に示す。

2011 年は、2010 年と類似した傾向を示している。2005 年から 2011 年の経年変化を全体的に俯瞰してみると、2009 年の「1～2 万円未満」と「2～5 万円未満」のインシデント件数の割合が、他の年と異なっている事がわかる。

【一人あたりの平均想定損害賠償額について】

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

算出式、およ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

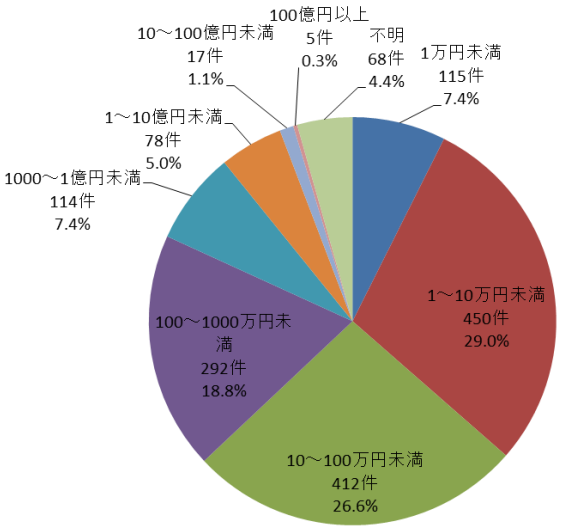

図 4-4：一件あたりの想定損害賠償額比率（件数）

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 万円未満のインシデントが半数以上(約 63%)を占め、そのうち「1 万円以上～10 万円未満」の比率が最も高く 29.0%である。一件あたりの想定損害賠償額が 100 万円未満のインシデントは、一件あたりの漏えい人数が少なく、かつ漏えいした個人情報の価値があまり高くないインシデントであると考えられる。

(2) 経年分析

表 4-5：一件あたりの平均損害賠償額の経年変化

	一件あたりの平均想定損害賠償額	(参考) 想定損害賠償総額
2005 年	5 億 3935 万円	約 5329 億円
2006 年	4 億 8156 万円	約 4570 億円
2007 年	27 億 9347 万円	約 2 兆 2711 億円
2008 年	1 億 8552 万円	約 2367 億円
2009 年	2 億 6683 万円	約 3890 億円
2010 年	7551 万円	約 1215 億円
2011 年	1 億 2,810 万円	約 1900 億円

2011 年は、2010 年よりもインシデント件数は減少したが、一件あたりの漏えい人数は増加しており、そのため、一件あたりの想定損害賠償額は増加した。理由の一つは、インシデント・トップ 10 に「金融業，保険業」のインシデントが 6 件も含まれ、想定損害賠償額が 100 億円以上のインシデントが増加したことが原因と思われる。

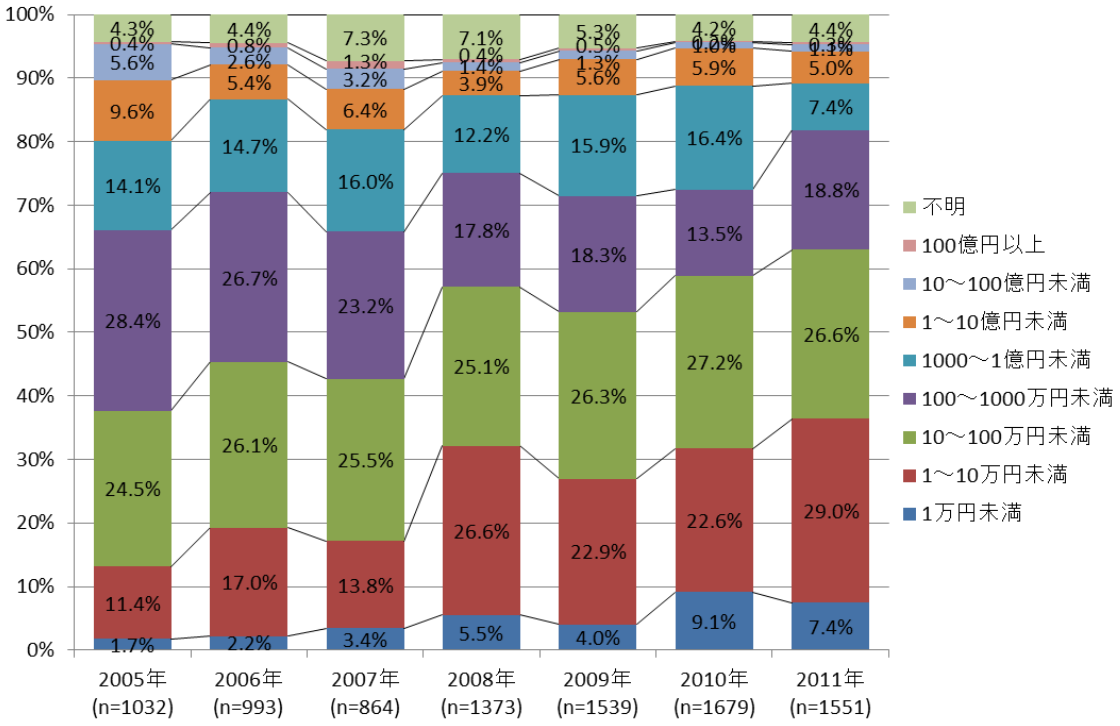

図 4-5：一件あたりの想定損害賠償額比率の経年変化（件数）

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

2007 年以前と比べて、2008 年以降は「1 万円以上～10 万円未満」の比率が高い。それに伴って、全体的に 100 万円未満の比率も、それまでの約 45%から約 60%前後へ、やや高くなっている。

経年変化を全体的に俯瞰してみると、2011 年は、想定損害賠償額が 1000 万円未満のインシデントの割合が高くなっており、想定損害賠償額が低いインシデントの割合が徐々に増えている。

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、およ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、2011 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

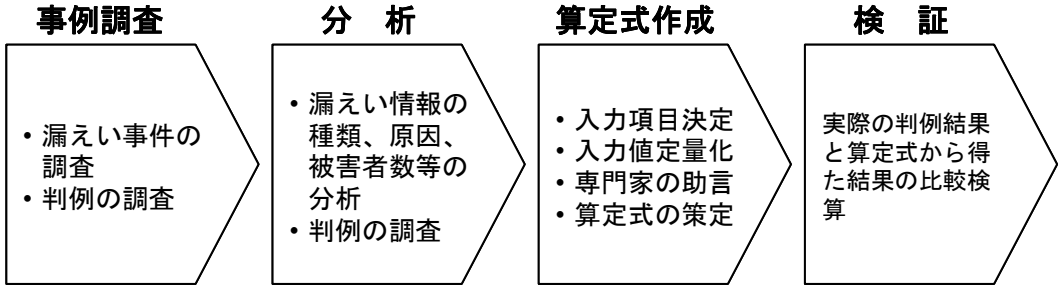

図 5-1：想定損害賠償額算定式策定のプロセス

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。2011 年の分析結果は「3. 2011 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、および 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。

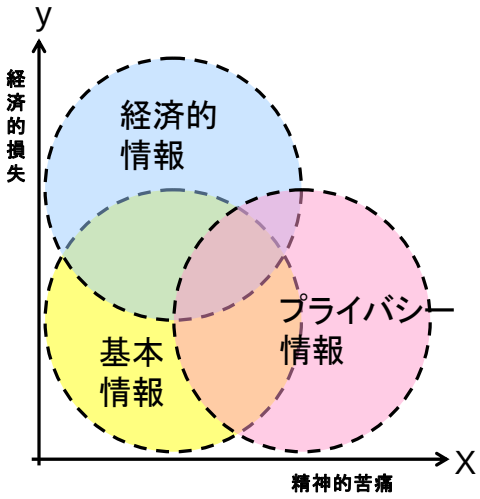

図 5-2：EP 図（Economic-Privacy Map）

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）」、およ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、および 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

(3) 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）、および公的機関、知名度の高い大企業。	2
一般的	その他一般的な企業、および団体、組織	1

(4) 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

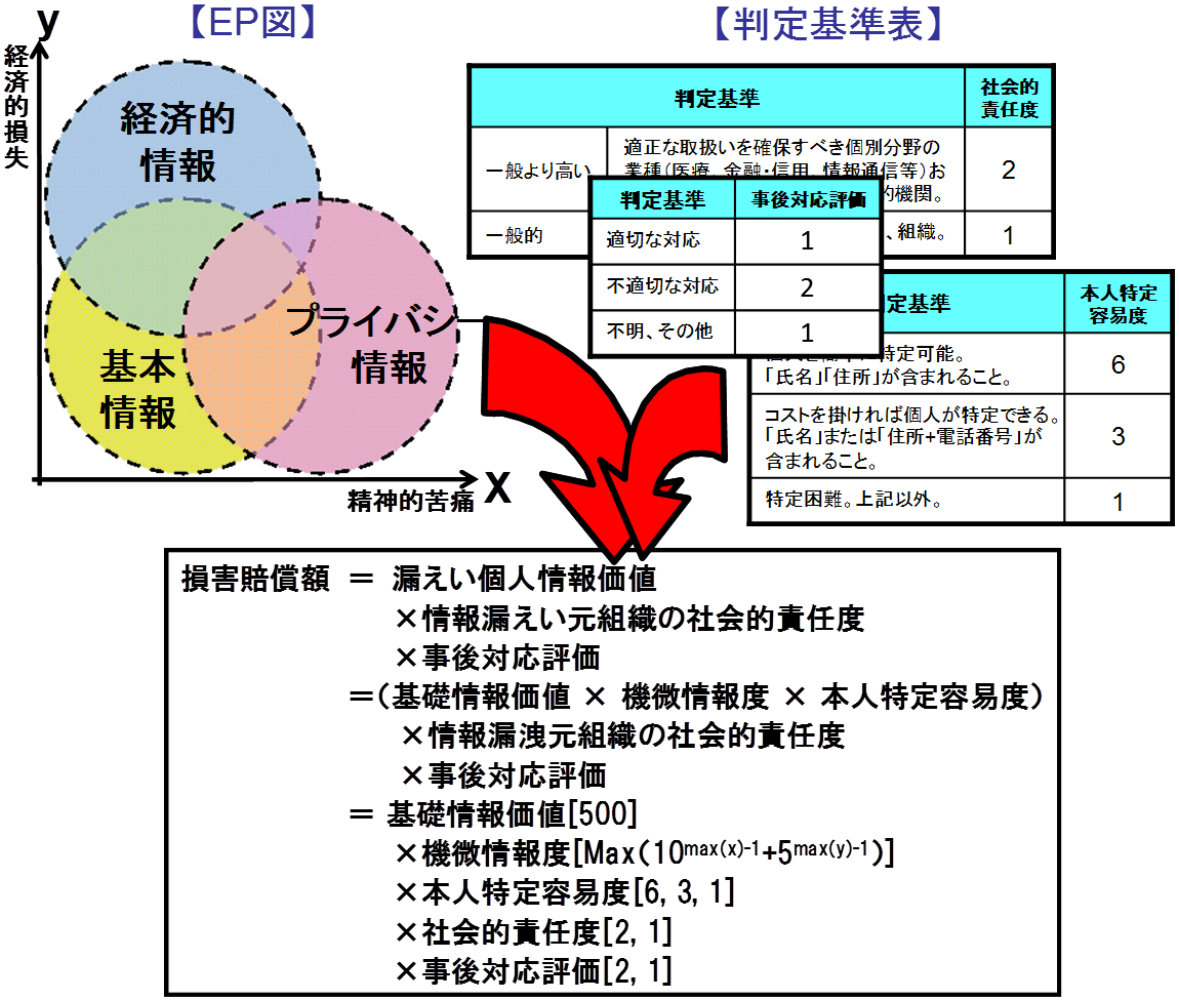

図 5-4：JO モデル

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

2011 年の個人情報漏えいインシデントを振り返って、以下の「6.1 2011 年インシデントの特徴」「6.2 電子メールの誤送信対策と影響について」「6.3 電子証明書の不正発行事件」「6.4 海外グループ会社からの個人情報漏えい」についてまとめた。

6.1 2011 年インシデントの特徴

2011 年は、業種、原因、漏えい経路、漏えい規模などの傾向が、2010 年とよく似た年であった。また、ここ数年間、上記の各構成の変動も少ない。

ここ数年の原因を分析すると、その特徴は、「管理ミス」および「誤操作」「紛失・置き忘れ」といった、ヒューマンエラーが原因の大半を占めていること、「管理ミス」と「誤操作」が特に多く、「紛失・置き忘れ」の比率が継続的に減少している点である。一方、「盗難」「ワーム・ウイルス」「不正アクセス」などの外的要因は、低い割合が続いている。

漏えい件数の特徴は、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、毎年 1500 件程度のインシデントが公表されていることである。特に「金融業，保険業」や「公務」のように社会的影響の大きい業種は、漏えい人数が小規模のインシデントであっても公表している。

一件あたりの想定損害賠償額は、経年変化を全体的に俯瞰してみると、想定損害賠償額が低いインシデントの割合が徐々に増えていることがわかる。上記の漏えい人数が小規模のインシデントが増えていることが、関係していると予想される。

6.2 電子メールの誤送信対策と影響について

電子メールの誤送信がなくなる方法について、問い合わせを受けることがある。電子メールの誤送信は、宛先誤り、本文や添付の内容自体の誤った入力、不適切な電子メールアドレスの To/Cc 指定の 3 種類である。これらは、ケアレスミスが原因である。ケアレスミスは、人が介在することによって発生するため、完全に発生をゼロにすることは非常に難しい。よって、誤送信がなくなるまで、いつまでも対策を追加し続けるのは、セキュリティ投資に対する効果が悪い。個人情報などの機密性の高いデータは、必ず暗号化して、誤送信しても情報が漏えいしないよう対策し、誤送信自体は許容する方法が、合理的である。

電子メールの誤送信の規模は、一件あたり平均約 650 人と紙媒体に次いで少なく（図 3-19 参照）、一人あたりの想定損害賠償額も 1 万円未満の割合が約 93%を占める。結果的に一件あたりの想定損害賠償額は、他の漏えい媒体・経路の一件あたりの想定損害賠償額よりも低いインシデントが多い。

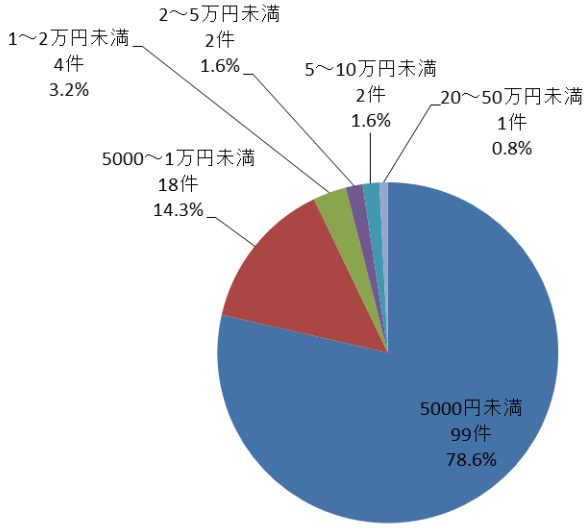

図 6-1：一件あたりの想定損害賠償額（メール誤送信）

個人情報の漏えいにおいて、漏えい範囲を特定し、適切な事後対応を行うことが肝要である。その点において、電子メールの誤送信は、誤送信先が明確であり、影響範囲の特定および追跡が容易である。メーリングリストで誤送信が発生した場合であっても、個人情報が広範囲に提供されてしまうが、その公開範囲を特定し、誤送信先へ連絡し対処できる。つまり、電子メール誤送信は、自体の収拾が困難ではない。誤送信先がビジネス上の常識的な取引相手であれば、影響はより最小限に留めることができる。

6.3 電子証明書の不正発行事件

2011 年は、電子証明書の発行元が不正アクセスを受けて、不正な電子証明書が発行さるインシデントがいくつも判明した。

米国グーグル社の電子メール「Gmail」のユーザーに対する中間者攻撃と呼ばれる不正な成りすましが発見されたことを契機に、オランダの認証局（電子証明書の発行元）の DigiNotar 社の認証局インフラが不正アクセスを受け、管理者権限でアクセスされて 513 枚の電子証明書が不正に発行されていたことが判明した。DigiNotar 社以外には、COMODO、米 GlobalSign、StartCom なども攻撃を受け、不正に電子証明書が発行されていたことが判明した。

不正に証明書が発行された問題は、さまざまなところに影響を及ぼしている。不正な電子証明書の中には、google.com, skype.com, twitter.com, www.facebook.com, windowsupdate.com, windowsupdate.com, wordpress.com など、広く利用されている著名なドメインも含まれていた。電子証明書は、自分の通信相手が本物であることを確認するためのかなめである。不正に発行された電子証明書が不正な Web サイ

トで使用されれば、ユーザーへ上記のような本物のサイトへアクセスしていると思わせて、ID やパスワードを入力させたり、マルウェアをインストールさせたりできてしまう恐れがある。

電子証明書は、さまざまなセキュリティ対策をきちんと備えた発行元が、申請書をしっかり審査した上で発行しており、不正アクセスされて、不正に電子証明書が発行されることはないと考えられていた。電子証明書の不正発行事件は、認証局の信頼性が崩壊したショッキングな出来事であった。

6.4 海外グループ会社からの個人情報漏えい

2011 年は、日本企業の海外グループ会社より、個人情報が漏えいするインシデントが多く発生した。表 6-1 に日本企業の海外グループ会社で発生した個人情報漏えいインシデントの一部を掲載した。これらのインシデントは、個人情報保護法がどこまで適用されるのか、明確に判断できないため、2011 年のリストから除外した。

表 6-1：日本企業の海外グループ会社でのインシデント(一部)

No.	業種	漏えい人数
1	情報通信業	7700 万人
2	情報通信業	2462 万 3400 人
3	情報通信業	2 万 5350 人
4	製造業	129 万 755 人
5	製造業	28 万 3000 人
6	情報通信業	3 万 7500 人
7	情報通信業	8500 人
8	情報通信業	2000 人

■ 個人情報漏えいの原因

表 6-1 のインシデントは、全て海外グループ会社において、ハクティビズム*を掲げた攻撃者による不正アクセスを受けて、個人情報が漏えいしたインシデントである。攻撃者は、ハクティビズムにもとづいて攻撃を行っているが、アクセス制御や認証システムなどのセキュリティ機構の不備や脆弱性の放置を突いて攻撃したり、ソーシャルエンジニアリングにより、マルウェアを動作させてバックドアを仕掛け、外部から操作して顧客情報や機密情報を抜き出したりと、攻撃の手法は、他の愉快目的や金銭目的の場合と違いはない。つまり、上記の被害にあったグローバルに事

* ハッキングとアクティビズム（積極行動主義）を合わせた造語。サイバー攻撃によって、自らの主張を認めさせようとすること。

業を展開している日本企業は、国内の Web サイトやインターネットに接続されたシステムはセキュリティ対策が施されていたが、海外グループ会社の Web サイトやシステムのセキュリティ対策が不十分であったため、それを攻撃者に発見され、インシデントが発生したと思われる。このように、国内からは目が届きにくい海外グループ会社のシステムや、その委託先のシステムが、企業全体のセキュリティ上の弱点になってきている。2011 年の日本企業の海外グループ会社からの個人情報漏えいインシデントは、海外グループ会社へ情報セキュリティ対策の指示が行き届いていないという問題点を浮き彫りにした。この問題点は、国内グループ会社に対しても、同様に当てはまる。また、ハクティビズムにもとづいた攻撃だけでなく、標的型攻撃と呼ばれる、事前に攻撃対象組織の弱点を綿密に調査して攻撃を仕掛けてくる場合も、同様に弱点が多く存在するグループ会社が狙われる。

■ グループ会社の情報セキュリティガバナンス

これからは、顧客情報を海外のクラウドサーバ上へ蓄積したり、顧客情報の収集から管理、分析などの情報活用までを国内および海外グループ会社へ委託することが、ますます増加するであろう。特にグローバル展開を進める日本企業にとって、海外グループ会社による情報漏えいインシデントは、これからより気を付けなければならない重要事項である。

グループ会社では、たとえば、情報セキュリティに対する意識が低い、セキュリティ対策に必要十分なリソースが確保されていない、セキュリティ対策が計画的に実施されていないなどの理由から、セキュリティ対策が不十分であることが多い。その原因の一つとして、グループ会社へセキュリティ対策を全て任せていることが挙げられる。そのため、本社―グループ会社間、国内―海外グループ会社間のセキュリティ対策に大きな格差が発生し、セキュリティ対策が不十分なグループ会社が攻撃者に狙われてしまう。

グローバル展開を目指す日本企業は、海外グループ会社全体に対して、情報セキュリティ対策のための活動を横断的に展開し統制することをより重視して、統一的な情報セキュリティガバナンスを構築するべきである。しかし、海外グループ会社全体へ、情報セキュリティガバナンスを浸透させることは、容易ではない。グループ会社へ情報セキュリティガバナンスの適用を開始する場合、たとえば、以下の項目をグループ会社へ適用するところから始める。

- セキュリティ対策の方針や目標とする対策の提示
- セキュリティ対策の現状と格差の把握
- 各グループ会社にあった実施計画の策定
- 実施状況のモニタリングと評価

情報セキュリティガバナンスは、もとは米国から広まった情報セキュリティもコーポレート・ガバナンスの１つとして組み込むことを目指した概念である。グローバル展開を目指す日本企業の場合、米国方式の情報セキュリティガバナンスの構築方法がよいとは限らない。米国や欧州だけでなく、中国やインド、東南アジア、南アジアなどの海外グループ会社を対象とする場合、それぞれ地域の法令だけでなく、商習慣や地域性などの違いも考慮して、展開方法を工夫しなければならないであろう。

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