個人情報漏えいインシデントの変遷と挑戦

大谷 尚通 †‡

† 株式会社 NTT データ
135-8671　東京都江東区豊洲 3-3-9
ootanihs@nttdata.co.jp

‡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 WG
105-0003　東京都港区西新橋 1-22-12 JC ビル 3F

あらまし 個人情報保護法が施行されて 10 年が経過し, 施策の見直しや個人情報に対する個人や組織の意識の変化が現れてきている. そこでこれまでに蓄積した国内で公表された 13 年間分の個人情報漏えいインシデントのデータを元に個人情報漏えいに関するセキュリティインシデントや対策の変化を振り返る. また, これまでのセキュリティ対策を評価するとともに問題点を明らかにし, セキュリティ対策の次のステップを考える.

Change and challenge for an incident of personal information leakage

Hisamichi Ohtani†‡

†NTT DATA Corporation
ootanihs@nttdata.co.jp

‡NPO Japan Network Security Association

Abstract ”Act on the Protection of Personal Information” is carried out, and has passed 10 years. The law was revised, and consciousness to personal information is changing. So I look back to a change in a personal information leakage and a change in a measure based on data for 13 years which were published in the country. A security measure of existence is estimated and the problem is made clear. I think and propose a step next to the security measure.

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は, 情報セキュリティ分野における被害の定量化や投資対効果の考え方の普及と発展を目的に活動を行っている. 情報セキュリティ対策を効果的に実施するためには, 経験やノウハウだけでなく, リスク大きさや対策の効果を定量的に評価しなければならない. そのためには, 業務やシステムに内在する情報セキュリティリスクや情報セキュリティインシデントが発生した時の被害を算定できなければならない.

当 WG は,2005 年の個人情報保護法の施行に向けて,2002 年より企業における個人情報を保有するシステムのリスク, および個人情報漏えい事件・事故（以下,「インシデント」という）を調査, 分析する活動を始めた. この時, セキュリティ対策の選定やインシデント発生時の意思決定の指標になる数値として, 被害額を定量的に示す試みを取り入れた. 本稿では, インシデント被害調査 WG が蓄積した 13 年間分の個人

情報漏えいインシデントの調査データを使って, 業種による発生インシデントの傾向の違いやセキュリティ対策の導入によるインシデント件数の変遷などを示す. またインシデントの公表に対する組織の意識や取り組みの変化, セキュリティインシデント被害額の考え方に対する認知向上など, 報告書の執筆を通して得られた知見も示す.

2 個人情報漏えいインシデントの分析

2002 年から 2014 年までの公表された個人情報漏えいインシデントを分析した結果と, 分析結果から得た個人情報漏えいインシデントのさまざまな特徴を述べる.

2.1 インシデント概要 (2002 年〜2014 年)

2002 年 1 月 1 日から 2014 年 12 月 31 日の 13 年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収集した. これらの情報を元に, 漏えいした組織の業種, 漏えい人数, 漏えい原因, 漏えい経路などのさまざまな分類・評価と, 独自の個人情報漏えいの被害額算出式を用いた想定損害賠償額の算出を行った. その結果を表 1 に示す.

表 1: 2002 年〜2014 年の集計データ

漏えい件数	1 万 4798 件
漏えい人数	1 億 6815 万 6124 人
想定損害賠償総額	6 兆 7043 億 6748 万円
平均漏えい人数/件	1 万 1923 人
平均想定損害賠償額/件	4 億 7535 万円
平均想定損害賠償額/人	4 万 4913 円

13 年間に漏洩した個人情報の件数は約 1 万 5000 件, 漏えい人数は日本の人口よりも多い 1 億 6815 万 6124 人であった. インシデント 1 件あたりの漏えい人数は約 1 万人であった. 漏えい人数が 1 万人のインシデントは, 企業にとって重大なインシデントであり, 適切に対応しなければならないレベルである.

2.1.1 業種別分析

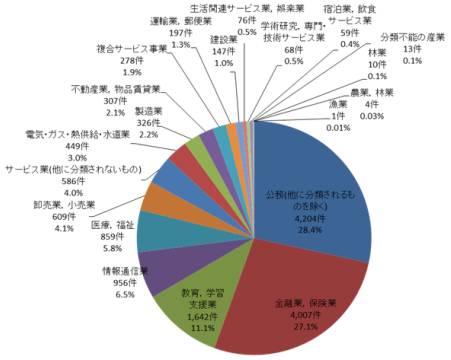

図 1: 業種別のインシデント件数

「公務」,「金融業, 保険業」,「教育, 学習支援業」の件数が多い. 特に「公務」や「金融業, 保険業」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ため, インシデント件数が多い. さらにこれらの業種は, 監督官庁の指導により 100 人以下の小規模なインシデントも積極的に公表しているためである.

漏えい人数が 100 人以上の場合は, 連絡がつかない被害者が発生するおそれがある. また二次被害が発生するおそれがある場合は, 被害者へ早急に連絡しなければならない. そのような場合は, 漏えい元組織は, インシデントを公表する場合が多い. 100 人以上のインシデント 5,681 件に限定すると,「金融業, 保険業 (2,169 件)」,「教育, 学習支援業 (678 件)」,「公務 (616 件)」,「情報通信業 (434 件)」の順に多い. 情報漏えいインシデントを起こしてしまった組織が, 積極的にインシデントを公表する姿勢が定着してきている.

図 2 から, 業種毎の漏えい経路/媒体の特徴がわかる. 「公務」,「金融業, 保険業」,「電気・ガス・熱供給・水道業」は, 紙媒体からの漏えいが多い. 「情報通信業」はインターネット経由,「教育, 学習支援業」と「医療, 福祉」は USB 等可搬記録媒体からの漏えいが多い. このように一部の業種にはインシデントが多発する経路/媒体があり, 重点的に対策を行うべきだと言える.

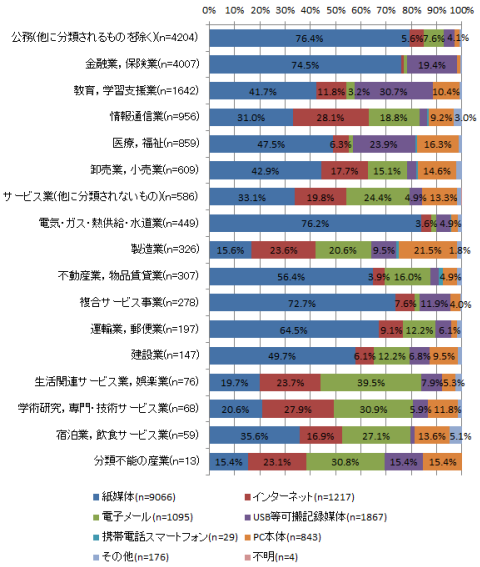

図 2: 業種と漏えい経路/媒体の関係 (件数)

2.1.2 原因分析

インシデントの原因は,「管理ミス (5,021 件)」,「誤操作 (3,876 件)」,「紛失・置忘れ (2,310 件)」の順に件数が多い. 管理ミスの内訳は, 誤廃棄が多い. つまり件数の多い上位 3 つの原因はヒューマンエラーである. 一方, 原因別の漏えい人数を集計すると, 図 3 のように「内部犯罪・内部不正行為 (212 件)」の漏えい人数が最も多い. 内部犯罪・内部不正行為は, 一度に大量の個人情報漏えいが発生するためである.

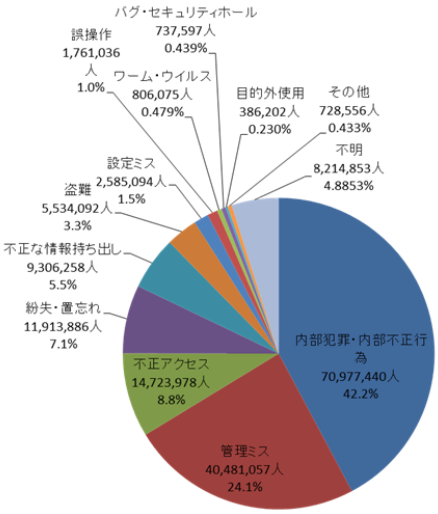

図 3: 原因別の漏えい人数

2.1.3 漏えい経路の分析

個人情報は, 紙媒体で漏えいする場合が最も多い. 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. 住民票などの公的な個人情報は, 書類として管理される機会が多く, 誤廃棄などの管理ミスや誤送付, 誤交付といった誤操作が発生しやすい.

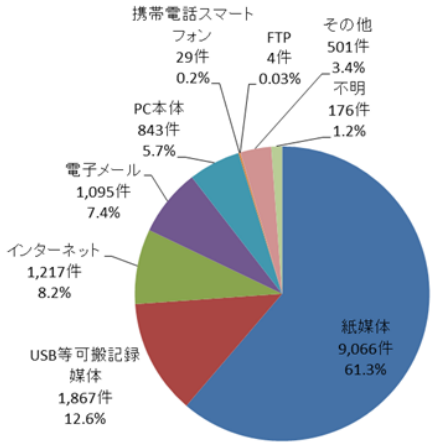

図 4: 漏えい経路 (件数)

3 個人情報漏えいインシデントの経年変化

個人情報保護法の施行前の 2002 年から 2004 年までは, 個人情報漏えいインシデントの公表数が少なく, インシデントを公表した業種や漏えい人数のデータの偏りが大きかった. そのためインシデントの経年変化の分析では,2002 年から 2004 年までのデータは分析対象から除外し,2005 年以降の 10 年間分のデータを用いた.

3.1 経年変化とインシデント件数の収束の関係

2005 年の個人情報保護法の施行以降, 毎年 1,000 件程度の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るようになった.2008 年以降, 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 1,000 万人の範囲で推移してきている (図 4). 2008 年以降, 一

年間に発生するインシデント数が, ほぼ一定になっている (図 5).

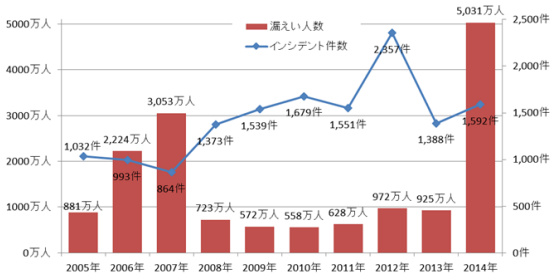

図 5: インシデント件数と漏えい人数の経年変化

インシデント件数と漏えい人数がほぼ一定になった要因は, 以下の 2 つが考えられる.

- 一般的な個人情報漏えいのセキュリティ対策が完了し, 一定の効果が出ている. ただし, これ以上の追加対策が行われていない
- 監督官庁の指示によりインシデントを公表する体制を確立し, 積極的にインシデントを公表する姿勢が定着した. 特に社会的影響の大きい業種である「金融業, 保険業」「公務」「医療, 福祉」は, 小規模のインシデントであっても公表する.

しかし,2012 年と 2014 年だけは, インシデント件数 (2,357 件) と漏えい人数 (5,031 万人) が非常に多い. 2012 年は,「金融業, 保険業」の業界全体で点検などの指示があったため, 同業界からのインシデント報告が増加し, 全体の件数が増加したと思われる.2014 年は, ベネッセの大規模インシデント発生により漏えい人数が増加した. このように, 基本的には一年間に発生するインシデント件数と漏えい人数はほぼ一定だが, このように監督官庁の管理方針が大きく変化した場合や大規模なインシデントが発生した場合などは, 例年とは異なる傾向が現れる年があることがわかった.

3.2 個人情報漏えいインシデント年表

個人情報漏えいインシデントの考え方や対策に大きな影響を与えた, 注目されたインシデントを表 2 に挙げる.

表 2: 個人情報漏えいインシデント年表

年	企業名	漏えい人数	原因
1999	宇治市	22 万人	内部犯
2002	TBC	3.7 万人	設定ミス
2003	ローソン	56 万人	その他
2003	ファミリーマート	18 万人	不明
2004	Yahoo BB	452 万人	内部犯
2004	ジャパネットたかた	51 万人	内部犯
2007	大日本印刷	864 万人	内部犯
2009	三菱ＵＦＪ証券	149 万人	内部犯
2011	ソニー (※)	7700 万人	不正アクセス
2014	ベネッセ	4858 万人	内部犯

※海外事例のため集計対象には含まれない
内部犯＝内部犯罪・内部不正行為

宇治市 個人情報漏えいによるプライバシー侵害で, 初めて損害賠償請求の裁判が行われた事例. 個人情報を名簿売買目的で盗み出したが, 現行法では情報が財物に該当しないために窃盗罪に問えなかった

TBC 個人を特定できる情報と身体的特徴の情報が漏えいしたことで, 被害者が精神的な被害を受けた事例. 裁判で高額な損害賠償額が決定した

ローソン 情報を漏えいしてしまった組織が, 初めて被害者へお見舞金 500 円相当の引換券を配布した事例. お詫びとしてお見舞金を支払うことだけが目的ではなく, 被害者が店舗で引換券を使用した際にローソン側が直接謝罪する目的があったといわれている

Yahoo BB 漏えい人数が 452 万人と大規模な事例. 会員へ 500 円相当の金券送付した. 個人情報を盗んだ Yahoo BB 代理店の役員は恐喝未遂で逮捕. 裁判により 5 名へ 6,000 円を損害賠償した

ジャパネットたかた 個人情報漏えい発覚時に再発を懸念して, サービスを全面停止した事例

三菱ＵＦＪ証券 高い権限を持った人 (部長代理) による内部犯. 不正アクセス禁止法違反と窃盗罪で逮捕. 高額のお見舞金 (商品券 1 万円) を 5 万人へ配布した

ソニー 攻撃者が特定組織を狙って不正アクセスし, 個人情報の漏えいに成功した事例

ベネッセ 過去最大の個人情報の漏えい人数.3504 万世帯へ金券 500 円分を配布し, 特別損失約 260 億円を計上. 不正競争防止法違反 (営業秘密の複製) で逮捕

表 2 の原因は内部犯が多い. 内部犯によるインシデントは, 機微な情報を含む個人情報が大量に漏えいするため, 被害額も高額になり, 報道に至る場合が多い. その場合, 社会的影響が大きいため, 漏えい元組織や警察, 監督官庁から, 漏えいの原因や過程, 問題点などのより詳細なインシデントの内容が公表される. これらの他のインシデントよりも詳しい情報は, 新しいセキュリティ上の問題を明らかにし, 個人情報漏えいのリスクの考え方やセキュリティ対策に影響を与えた.

3.3 インシデントの調査方法の問題点

個人情報漏えいインシデントの調査は, インターネット上に公開されたニュース記事, 広報記事を手作業で収集し, 記事や文書の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. 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. ましてや, 国内で発生した未公表のインシデントも含め、すべてのインシデント情報を収集することはできない. よって, 収集できるインシデントの件数や本調査のカバー率は, 報道機関がニュースへ取り上げる基準や漏えい元組織の公表の基準に左右される. ニュース性の高い大規模なインシデントほど, 報道, 公表されるため, 漏れなく収集できる.

小規模インシデントの件数は, 業種や組織毎の公表基準の違いによる差が大きい. 監督官庁から小規模インシデントであっても公表するよう指示されている「金融業, 保険業」「公務」「医療, 福祉」は, 小規模インシデントの情報も集まりやすい. たとえば「卸売業, 小売業」,「サービス業」は企業数が多く, 個人情報も扱う機会が多いはずだが, インシデント件数が少ない. 図 6 からも, 前者よりも後者のほうが, 報道, 公表された漏えい人数が多いことがわかる.

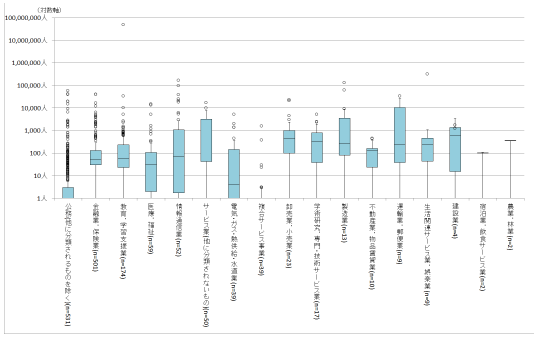

図 6: 2014 年の業種別の漏えい人数（箱髭図）

このようにインターネットニュースなどで報道された記事や組織から公表された文書などから, インシデントのデータを収集して分析する方法は, 収集できるデータ自体に偏りがあるため, 統計的な分析には不向きである.

4 効果的な対策に向けた挑戦

4.1 個人情報漏えいの想定損害賠償額算出モデル

個人情報保護法の施行に向けて, 各組織は個人情報を扱うシステムや業務に対してリスク分析を行い, セキュリティ対策を実施しなければならない. しかし, 個人情報自体の価値の算出は難しく, アンケートデータやカスタマーサービス用の顧客情報を蓄積しているデータベースシステムは利益を産み出さないため, 資産価値も定めにくい. 個人情報を扱うシステムや業務のうち, 資産価値を算定しにくい場合は, 被害額を基準にリスクの大きさを判断する.

既存の情報セキュリティインシデントの被害額算出モデル [1] は, さまざまな情報セキュリティインシデントを表面化被害額と潜在化被害額の 2 つに分けて計算する汎用的な算出モデルである. それぞれの 2 つの被害額の計算には, インシデントに関係する多くの情報が必要である. 実際に被害額を算出しようとすると, 計算に必要な情報をすべて集められず, 算出モデルが複雑で計算が大変なことがわかった.

そこで個人情報漏えいインシデントの調査の経験と集計したデータをもとに, 想定損害賠償額を算出する独自のモデル「JNSA Damage Oper-

ation Model for Individual Information Leak」(以下,「JO モデル」と言う) を作成した.JO モデルは, 以下の 3 つの特徴がある.

- プライバシー侵害の裁判事例などの実例にもとづいた経験的なモデル
- 式の項数を極力減らして入手が容易な情報を使った簡単なモデル. 誰でも想定損害賠償額を算出できる
- 被害は, 一般的な値, 検証しやすい値へ定量化する. もっとも認識されやすい被害額 (金額）へ換算する

JO モデルは, 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として作成したが, 実際に発生したインシデントの想定損害賠償額の算出にも応用できる. その場合は, 個人情報の潜在的リスクの推定値であり, 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ことに注意する

4.1.1 JO モデルと想定損害賠償額の算出式

JO モデルにもとづく想定損害賠償額の算出式 (1) は, 定量化した「漏えい個人情報価値」と「情報漏えい元組織の社会的責任度」,「事後対応評価」の値を用いる.

$$\begin{aligned}\text{想定損害賠償額} &= \text{漏えい個人情報価値}\\ &\quad \times \text{情報漏えい元組織の社会的責任度}\\ &\quad \times \text{事後対応評価} \qquad (1)\end{aligned}$$

4.1.2 漏えい個人情報価値

個人情報の価値は,「基礎情報価値」と「機微情報度」,「本人特定容易度」の値を用いる. 基礎情報価値は, 情報の種類に関わらず一律 500 ポイントとした.

$$\begin{aligned}\text{漏えい個人情報価値} &= \text{基礎情報価値}\\ &\quad \times \text{機微情報度}\\ &\quad \times \text{本人特定容易度} \qquad (2)\end{aligned}$$

機微情報度の定量化には, 個人情報が漏えいした場合に被害者へ与える 2 種類の影響「経済的損失」と「精神的苦痛」を用いる. 縦軸 y に「経済的損失」の度合いを, 横軸 x に「精神的苦痛」の度合いを持たせた Economic-Privacy Map(以下,「EP 図」という)(図 7) を定義した. 漏えいした個人情報の種別の EP 図上の座標から, 影響の大きさを数値化し, 機微情報度を算出する.

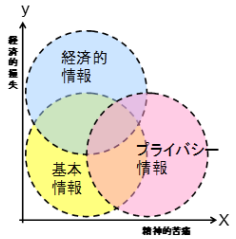

図 7: EP 図

EP 図の x,y 軸を 3 段階に分け, 個人情報の保護に関する法律（個人情報保護法）[3], 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）[4], 及び調査から得た漏えい情報の種類を図上へプロットした図 8 をシンプル EP 図という. シンプル EP 図は, 漏えいした個人情報の種別の EP 図上の位置（x, y）を 3 段階から選択するだけのため, 求めやすい.

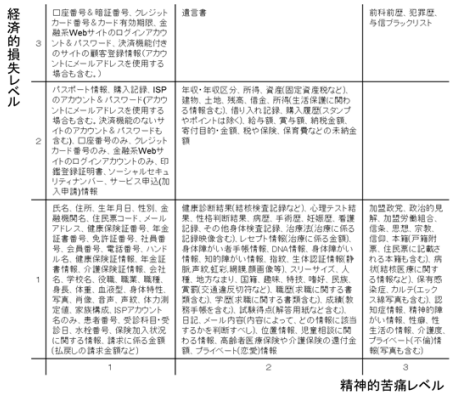

図 8: シンプル EP 図

機微情報度の算出は, 式 (3) を用いる. 式 (3) は, 過去のプライバシー侵害の裁判の損害賠償額のデータとクレジットカードの不正利用の被害額のデータにもとづいて作成した. 漏えいした個人情報の種別の位置（x, y）をシンプル EP 図から求めて, 式 (3) へ代入すれば, 機微情報度を算出できる. 漏えい情報が複数種類ある場合

は, 全漏えい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.

$$機微情報度 = 10^{x-1} + 5^{y-1} \qquad (3)$$

本人特定容易度は, 漏えいした個人情報からの本人の特定のし易さを表す値である. たとえば, 病状のデータが単独で漏えいしても, 氏名と住所がセットになった情報が伴わなければ, 本人の特定および連絡がおこなえないため, 実被害に結び付きにくい. 本人特定容易度は, 表 3 に示す判定基準を適用する.

表 3: 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	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	3
特定困難. 上記以外	1

以上より JO モデルでは, 個人に関係する全ての情報は個人情報と定義し, 漏えいした全ての個人情報をひとまとめにして, その機微情報度と本人特定容易度を決定して, 漏えい個人情報価値を算出する. 漏えいした情報を 1 つ 1 つ個人情報か否か, 判断する必要はない. パーソナルデータに関する検討会が作成した「識別特定個人情報」や「非識別非特定個人情報」の考え方 [5] に類似している.

4.1.3 情報漏えい元組織の社会的責任度

情報漏えい元組織の社会的責任度は表 4 のように「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へ政府機関などの公的機関を含めたものとした.

4.1.4 事後対応評価

事後対応評価の値は表 5 を用いる. 収集したインシデント情報には, ほとんど事後対応の情報がない. 事後対応が「不明, その他」の場合は, 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. また, 事後対応を評価する明確な基準がないため, 過去のインシデントにおける事後対応行動を参考に作成した対応行動例 [6] にあてはめて, 事後対応の適切／不適切を判断する.

表 4: 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

表 5: 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

4.2 個人情報漏えいの費用の試算

個人情報漏えいによって発生する費用は, 前述の想定損害賠償だけではない. そこで, 架空の企業における個人情報漏えいのシナリオを作成し, 全費用の算出を行った [9]. 費用の算定に使用した企業のプロファイルとシナリオ, 試算結果を図 9 に示す.

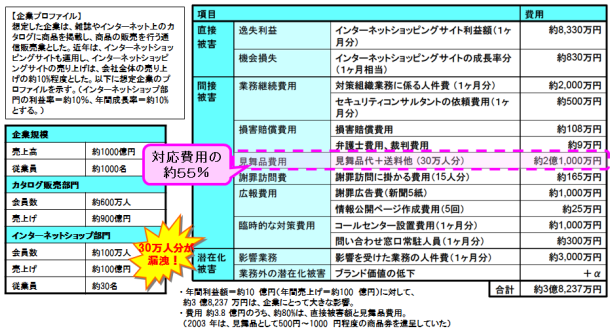

図 9: 個人情報漏えいの費用の試算

想定したシナリオに基づく個人情報漏えいインシデントの全費用の試算結果は, 約 3 億 8,237 万円＋α となった. この試算により, 個人情報漏えいは損害賠償額だけでなく, 業務停止による

逸失利益やその他の対応費用が, 被害額と費用となって表れることがわかった. 売上げが約100億円で利益が10億円のインターネットショップ部門において, 突然の約3億8,237万円の費用発生は, 経営に大きな影響を与える.

費用のうち, 見舞品の費用が全体の約半分を占める. 見舞品を送付することは, 企業側から被害者（顧客）に対する謝罪表現のひとつであり, 必ずしも必須ではない. 被害者にとっては, 見舞品による一時的な謝罪表現よりも, 被害者への対応や漏えい情報の回収, 再発防止対策などに費用をかけて, それによって得られる安心感や信頼感のほうが価値が高い.

個人情報を大量に扱う組織は, 組織が保有している個人情報とその個人情報を利用している業務を調査し, 個人情報漏えいによる費用を事前に試算すべきである. その費用を考慮して適切なセキュリティ投資や社内制度の策定, インシデント発生後の対応費用を軽減するための保険加入など, リスクの未然回避と損害軽減策を講じるべきである.

4.3 公表の必要性と判断基準

個人情報の保護に関する法律施行令 [7] や改正前の個人情報の保護に関する法律は, 個人情報が5,000人以下の組織であれば個人情報取扱事業者から除外していた. その影響により, 漏えい元組織は小規模のインシデントを公表しないことが多い.

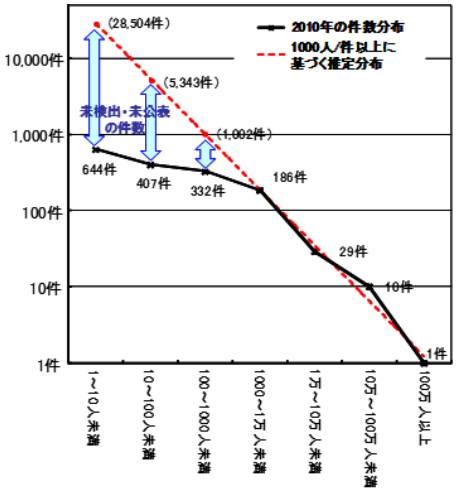

図 10: 2010年 インシデント件数の分布（対数）

2010年のデータを元に漏えい規模別のインシデント件数を集計して対数グラフで表した (図10). 漏えい人数が1000人～1万人以上の中規模から大規模のインシデントは, ほぼすべて報道や公表されていると思われる. そこで小規模インシデントの件数の分布を推定し, 図10に赤い点線で示した. 図10のように1000人未満のインシデントの発生件数 (推定) と公表件数には乖離があると思われる. インシデントの公表率は, 漏えい人数が「1人～10人未満 (2.3%)」,「10人～100人未満 (7.6%)」,「100人～1000人未満 (33.1%)」と推定された [8]. 漏えい人数が1万人以上のインシデントが発生した場合は公表せざるを得ないが,1000人未満のインシデントの場合は公表しないことを選択する組織が増えてくるものと思われる.

小規模インシデントの場合は, 漏えい元組織が被害者へ個別に連絡を行い, インシデントの状況説明や謝罪, 二次被害への注意などの対応できる. そのため小規模インシデントの場合は, 公表する必要性は低い. しかし, たとえば漏えい人数が100人以上の場合は, 被害者へ連絡がつかない場合が増え, 個別に対応することが困難になる. 被害者が少人数であっても, すべての被害者に連絡がつかない場合は, 報道機関やインターネットを利用して積極的にインシデントを公表し, 漏えいした情報が悪用されるおそれなどを伝えることが望ましい. 世間に対して説明責任を果たさなければならない場合や, 公表によって類似インシデントの発生回避に役立つ場合も, 公表することが望ましい.

各組織は事前に公表の基準を設け, インシデントの状況に応じて, 前記の基準にもとづいて公表の可否を検討し, 対応するべきである. また公表しないインシデントであっても, きちんと報告させて, 発生件数を把握するべきである.

4.4 情報セキュリティ報告書の活用

小規模インシデントであっても積極的に逐次公表する行為は, 被害者が, 漏えい元組織によってインシデントが隠蔽されていないことを確認できるため, 好ましい行動である. しかし, 大規模な組織は軽微な漏えいインシデントが多数発

生する. そのため, 公表する労力やコストなどを考慮すると, 被害者へ個別対応できている小規模なインシデントを逐次公表する作業は, 費用対効果が悪い.

小規模なインシデントを都度公表するのではなく, 情報セキュリティ報告書で年に一度公表する方法が有効である. 小規模なインシデントと中規模以上のインシデントを区別する基準を定義し, その公表基準は毎年の情報セキュリティ報告書に記載する. この方法により, 小規模なインシデントも公表して組織の説明責任を果たすとともに, 公表にかかる作業と費用を削減できる. 1 年間のインシデントの件数や継続的な改善状況を情報セキュリティ報告書で継続して報告すれば, 組織のセキュリティに対する姿勢をアピールすることもできる.

5 まとめ

セキュリティ被害調査 WG が蓄積した 13 年間分の個人情報漏えいインシデントのデータを分析した結果, 2005 年の個人情報保護法の施行以降, インシデント件数が一定の割合まで減少し, 定常値で遷移していることが確認できた. これは個人情報漏えいの基本的な対策が普及してインシデント件数が減少したあと, 基本的な対策では防止しきれないインシデントが一定の割合で発生している状態と推測される.

2008 年以降の定常的な状態のデータから, 漏えいの原因や経路の普遍的な傾向や業種別の特徴が判明した. 漏えいの原因はヒューマンエラーが大部分を占め, 漏えいの媒体/経路は紙媒体が最も多い. 個人情報を取り扱う業務が, 紙媒体を手作業で扱う場合が多いと推測される.

本調査の方法や収集データ, 想定損害賠償額の算出式は,2003 年に作成した方法を 2014 年までそのまま踏襲した. 前年の調査結果や考察結果にもとづいて, 収集データや JO モデルを変更することも検討した. しかし実際の個人情報漏えいインシデントの裁判の賠償額と, 本算出式による想定損害賠償額の算出値の誤差が, 許容できる範囲に収まっていることから, 現行の算出式で問題ないと判断して変更しなかった.

個人情報漏えいの調査報告を 13 年間続けることによって, この想定損害賠償額を算出して, 個人情報を取り扱う組織の潜在的なリスクを把握したり, 実際のインシデントの被害の大きさを推定したりする方法を, 情報セキュリティ分野に浸透させることができた.

5.1 課題と今後の予定

当 WG は, さまざまな情報セキュリティインシデントのリスクや被害, 対応費用を定量化し, 投資対効果の考え方にもとづいた合理的なセキュリティ対策方法の構築と普及を目指している.

近年国内でも,2011 年に米国証券取引委員会（SEC）が公表した「サイバーセキュリティの侵害やリスクの情報開示に関するガイドライン (CF Disclosure Guidance: Topic No. 2 Cyber security)」 [10] が注目されはじめている [11]. 同ガイドラインは, 株式公開企業は, 自社のビジネスリスクになるおそれのあるサイバー攻撃を識別し, そのサイバー攻撃を受けた場合の業績への影響を投資家へ開示するよう記述している. 米国の上場企業は, 自社のサイバー攻撃のリスクや想定被害を詳しく開示したり, 被害事例を開示したりしている. そこで今後は, 個人情報漏えいインシデントだけでなく, ウイルス感染や不正アクセス, 標的型攻撃, 水飲み場型攻撃, その他のサイバー攻撃などのインシデント別の被害モデルを構築し, それらの状況に特化した被害額や対応費用の算定式を作成し, 普及させる予定である.

さらに今後, 経営層は, 経営戦略に情報セキュリティ対策を組み込み, セキュリティリスクの軽減や回避, サイバー攻撃の早期検知と早期対応による被害の最小化のために, 適切なセキュリティ対策投資を行っていることをステークホルダーへ示さなければならない. セキュリティ投資対効果「Security Return On Investment（SROI）」の算出モデル構築や, 適切なセキュリティ対策投資のベストプラクティスの提案なども検討したい.

参考文献

[1] IPA,2006 年国内における情報セキュリティ事象被害状況調査報告書,http://www.ipa.go.jp/security/awareness/johorouei/index2.html

[2] 上国忠弘, コンピュータ・セキュリティ, 近代科学社,1981

[3] 個人情報の保護に関する法律,http://www.caa.go.jp/planning/kojin/houritsu/index.html

[4] 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）,http://www.kantei.go.jp/jp/it/privacy/houseika/dai11/JISQ15001.pdf

[5] パーソナルデータに関する検討会 決定等,https://www.kantei.go.jp/jp/singi/it2/pd/index.html

[6] JNSA セキュリティ被害調査 WG,2013 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～,http://www.jnsa.org/result/incident/

[7] 個人情報の保護に関する法律施行令（平成十五年十二月十日政令第五百七号）,http://law.e-gov.go.jp/htmldata/H15/H15SE507.html

[8] JNSA セキュリティ被害調査 WG,2010 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～,http://www.jnsa.org/result/incident/

[9] JNSA セキュリティ被害調査 WG,2003 年度情報セキュリティインシデントに関する調査報告書 第 2 部 情報漏洩による被害想定と考察,http://www.jnsa.org/result/incident/

[10] サイバーセキュリティの侵害やリスクの情報開示に関するガイドライン (CF Disclosure Guidance: Topic No. 2 Cyber security), http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm,2011

[11] 内閣サイバーセキュリティセンター（NISC）, 我が国のサイバーセキュリティ戦略,https://www.nic.ad.jp/ja/materials/after/20150320/20150320-fujita.pdf,2015