個人情報漏洩補償に関する一検討

石川 朝久† 櫻井 幸一‡

†scientia.admin@gmail.com

‡九州大学
819-0395 福岡市西区元岡 744
sakurai@inf.kyushu-u.ac.jp

個人情報漏洩インシデントが発生した企業は原因調査・情報漏洩対象者の報告・お詫び・補償、メディア対応やお問い合わせ窓口の設置など多様な対応が必要とされる。特に、昨今メディアでも情報漏洩インシデントが大きく取り上げられることから、組織のインシデント対応の着目度は高い。その一方、個人情報漏洩インシデントへの費用対効果がわかりづらいことも指摘されている。また、個人情報漏洩補償を明確に定められたガイドライン・基準がなく、民事裁判による判例も多くないことから、各組織が過去事例を参照しているケースがほとんどある。本研究では、インシデント対応を計画する上で役立つフレームワークについて整理を行い、特に個人情報漏洩補償に着目して、分析・考察を行う。

A Study of Compensation in Personal Information Leakage

Tomohisa Ishikawa† Kouichi Sakurai‡

†scientia.admin@gmail.com
‡Kyushu University
744 Motooka Nishi-ku, Fukuoka 319-0395, JAPAN
sakurai@inf.kyushu-u.ac.jp

Abstract: The organizations and companies that have personal information leakage should take a lot of necessary actions such as investigation, public relations, and compensation for customers. Especially, in Japan, since mass media attempt to broadcast these information leakage incidents in daily news, the organizations or companies are also interested in incident handling planning. On the other hand, it is pointed out that there is the difficulty of understanding cost-benefit of security incident preparation investments. Also, the compensation for the victims in personal information leakage is not prescribed in regulation or guidelines, and there are only few cases of the civil trials for the compensation of information leakage incidents. Therefore, current compensations are determined by past examples. In this study, frameworks for planning incident handling are overviewed, and the compensation of incident handling is analyzed.

1　はじめに

Web サービスの発展に伴い、各種サービスの利用時には個人情報の登録が促されることが一般的である。登録によりサービス提供者、サービス利用者双方が利便性を得る一方、Web サービスのセキュリティレベルが十分でないことから個人情報が漏洩するインシデントは後を絶たない。NRI セキュアテクノロジーズ株式会社の 2014 年度の調査「サイバーセキュリティ:傾向分析レポート 2014」[1]によれば約 28%の Web サイトに重要情報に不正にアクセス可能な問題が発見されている。日本企業、組織に対してもこれらの攻撃は継続して行われてきたが、2011 年グローバル企業に大規模攻撃が報道されたことをきっかけに、インシデント対応、個人情報漏洩への検討が、各企業の課題の一つとなっている。

本稿では、現在のインシデントに対する検討モデルを整理した後、想定個人情報賠償金額の算出モデルに焦点を当てて考察を行う。

2　関連研究

インシデントに関連する検討モデルは、定量的、定性的モデル[2]としていくつか提唱されている。定量的モデルについて 3 つ例示する。

2.1　ROSI フレームワーク

第一のフレームワークは、ROSI（Return On Security Investment）[3]である。これは、セキュリティ投資対効果を考えるためのフレームワークである。このフレームワークの目的は、費用対効果の高いセキュリティを目指すことであり、現在のセキュリティ投資の基礎となる考え方である。考え方としては、SLE（個別予想被害額）、ARO（年間発生率）から、ALE 年間損失額)を算出し、セキュリティ投資の費用対効果を考えるアイディアであり、定量的アプローチとし他の研究にも取り入れられている [4] 。本モデルは概念として広く採用されている一方、各数値の算出が難しいことが指摘されている。

2.2　CyberTab フレームワーク

第二に、米エコノミスト社インテリジェンス部門が作成したフレームワーク、CyberTab[5]が挙げられる。このフレームワークは、特定の想定脅威に対するインシデントレスポンス費用と必要経費を計算することができる。このフレームワークを利用することにより、一回のインシデントにかかる費用が計算できるため、ROSI フレームワークを考えるための一助になると考えられる。本フレームワークの最大の特徴は、インシデントに対してどのような費用を考慮すればよいか明示してくれる点であり、インシデントレスポンス時の考慮で見逃されやすい法務部、広報部との稼働も考慮されている。その点で、実際にインシデントにかかる費用をシミュレーションするためには有益なモデルと考えられる。

2.3　JO モデル

第三に挙げるモデルは、個人情報漏洩時の想定賠償額を算出することに焦点を置いたモデル、JO モデル(JNSA Damage Operation Model for Individual Information Leak)[6]である。JNSA（日本ネットワークセキュリティ協会）が考案したこのモデルは、個人情報価値・組織の社会的責任度・事後対応評価の3点より想定損害賠償額を算出するモデルである。今回、個人情報漏洩賠償費用の考察に焦点を当てるため、事象にてモデルの整理を行う。

3　JO モデルによる算出方法

JO モデルによれば、想定損害賠償額は**「個人情報価値×社会的責任度×事後対応評価」**の3パラメータの積にて決定する。

3.1　個人情報価値

第一のパラメータは、「個人情報価値」である。

計算できるよう工夫されており、「**基礎情報価値×機微情報度×本人特定容易度**」の積にて定義されている。

第一のパラメータは、「基礎情報価値」であり、個人情報の基礎となる金額を意味する。JO モデルでは、2003 年に発生したローソンカード会員 56 万人の個人情報漏洩を参考に、500 円と定義された。

第二のパラメータは、機微重要度とは、漏洩個人情報に含まれた機微重要性を決めるパラメータで以下のように定義される。

$$[\max(10^{x-1}+5^{y-1})]$$

- X： 精神的苦痛レベルの最大値
- Y： 経済的損失レベルの最大値

この定義式について、JO モデルを作成したワーキンググループは、次のような理論的分析を行っている。個人情報を「経済的損失」と「精神的損失」の２種類の尺度で分類し、EP 図（Economic Privacy Map）というマッピングを作成した。以下図は、ワーキンググループの報告書[7]からの引用である。

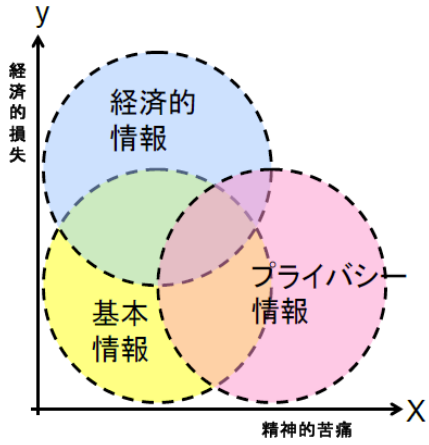

図 1 EP 図（参考文献[7]より引用）

その後、ワーキンググループは、各個人情報を EP 図にマッピングして簡素化を行い、S-EP 図を作成して利用しやすい形にまとめている。ここでは、代表的な漏洩情報について著者にて整理を行い、まとめた図を示す。（原本は、参考文献[7] を参考のこと。）

図 2 S-EP 図（参考文献[7]より筆者作成）

JO モデルの運用では、上記のような漏洩情報の分類をもとに、漏洩した情報の「経済的損失レベル」と「精神的苦痛レベル」を決めて、上記計算式に当てはめて計算を行う。

第三は、「本人特定容易度」である。「氏名+住所」が含まれていれば、個人を簡単に特定できるとして賠償額 6 倍、「氏名」または「住所 + 電話番号」があればコストをかければ個人を特定できるとして賠償額 3 倍、その他の場合 1 倍という形で定義されている。

3.2 社会的責任度

「社会的責任度」とは、組織が個人情報漏洩に果たす責任度を意味し、「一般より高い」と「一般的」の二種類から選択を行い、社会的責任度が一般より高い企業は、2 倍の補償費用を負担する形で定義されている。ここでいう「社会的責任度が一般より高い企業」とは、「個人情報の保護に関する基本方針」で指定された産業分野に加え、公的機関、大企業などが含まれている。

3.3 事後対応評価

事後対応評価とは、インシデント発生後の組織の対応評価を意味して、不適切な対応を行っ

たと判定される場合には、2 倍の補償費用を払うように計算式が作られている。適切対応有無については、JO モデルのワーキンググループで、「対応速度」、「お問い合わせ窓口の設置有無」など定性的な判断基準が用意されている。

3.4 JO モデルの適用事例

2013 年 3 月に発生した JINS クレジットカード情報漏洩事故を例に JO モデルで計算を行う。本事件で、カード名義人名・カード番号・セキュリティコード・有効期限などが漏洩した[8]。当初 12,036 人分の情報漏洩の可能性があると指摘されていたが、最終報告で 2,059 人分の情報流出にとどまる旨が報告された[9]。株式会社ジェイアイエヌは、漏洩可能性を含む 12,036 人に対して 1000 円分の QUO カードとクレジットカード再発行手数料を負担する形で賠償を行った。仮に、クレジットカード再発行手数料を 500 円とすると、1 人当たり 1500 円程度の賠償、1800 万円以上の支出となる。その他にも、郵送費、調査費用などが想定される。特に、クレジットカード情報漏洩の場合、PCI SSC(Payment Card Industry Security Standard Council)にて PFI 認定(PCI Forensic Investigator)されたフォレンジックベンダーによる調査が必要など、その他にも様々なコストがかかると推測される。今回の事例を JO モデルで計算すると、一人当たり 39,000 円の賠償額が想定される。

- 個人情報価値　　39,000

$$500 \times \max(10^{1-1} + 5^{3-1}) \times 3$$

- 社会的責任度　　1
- 事後対応評価　　1

規範例としての賠償額としては非常に有益であるが、1,000 円という実際の金額との間には大きな差があり、改善課題があると考えられる。

4 保険制度

最近では、個人情報漏洩に対する保険等も登場している。Latham & Watkins 社のホワイトペーパー[10]では、サイバー攻撃の最終防衛ラインとして保険が有効であると指摘し、統合的なリスク管理として保険は有益なツールであると述べている。また、日本の各保険会社も個人情報漏洩に関連する保険サービスを始めている。その一例としては、東京海上日動の「個人情報漏えい保険」[11]、損保ジャパン「個人情報取扱事業者保険」[12]などが挙げられる。両保険ともに、インシデント対応費用と賠償費用の2種類をカバーするように設計されており、発生するインシデント費用の一部を保険料によりカバーできる。ただし、保険はあくまでインシデント発生時の特定の費用を規定額までカバーしてくれないため、特定の保険加入だけで十分か否かは上記で紹介したフレームワークを使いながら分析していく必要はあると考えられるが、発生時期、コストの予想が難しいインシデントに対して、保険料という形で固定費用化できることは非常に有益だと考えられる。

5 個人情報漏洩事故賠償の実際

現在、Web サービスにおいて個人情報漏洩が発生した場合、現在明確な指針が存在していない。また、個人情報保護を目的に成立した個人情報保護法にも該当する規定は存在しない。そのため、個人情報漏洩事故の金額は民事訴訟による判例、もしくは企業が独自に算出した賠償金額のいずれかにより決定される。菅原・原田[13]は、各企業に対してアンケート調査を試み、「電話番号、購入に関する情報といった基本的個人情報については、比較的低い金額であり、1000 円以内が半数を占めている」と報告している。

筆者が、2002 年から 2013 年における公開事例 31 件を調査したところ、平均的な賠償金額は 3138 円であった。しかしながら、実際にグラフ化(図 3)してみると、その多くは 500 円~1000 円に偏っていることがわかる(グラフの都合上、1 万円以上は 1 万円としてプロットしている)。実際、筆者が調査した事例の中で 1 万円以上の

事例は以下の 4 事例のみで、そのうち 2 事例は民事裁判により定められた補償額である。

- TBC (2002)　35,000 円 [14]
- JAL 労働組合(2007)　10,000 円 [15]
- 三菱 UFJ 証券(2009)　10,000 円 [16]
- アリコジャパン(2009)　10,000 円 [17]

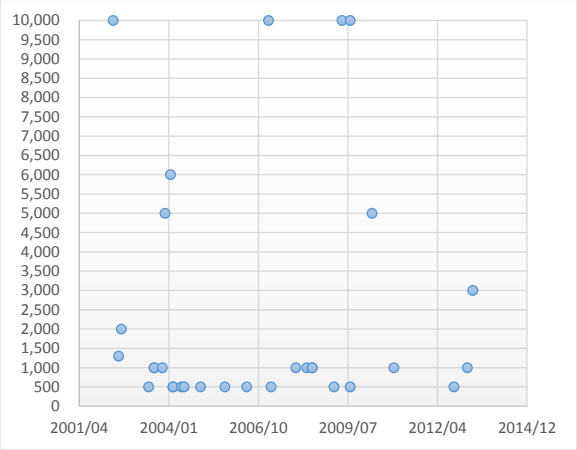

図 3　企業が提示した補償額分布

企業が提示する補償額が 500 円～1000 円にとどまる理由は、JO モデルでも利用された 2003 年に発生したローソンカード会員情報漏洩事件の賠償額（一人あたり 500 円）がベンチマークとして機能していると考えられる。逆に、民事裁判で損害賠償を求めた事例に着目すると、1998 年の宇治市住民基本台帳データ漏洩事件の 15,000 円[14]、早稲田大学講演会参加者名簿流出事件(1998 年)の 5000 円[18]、Yahoo!BB の情報漏洩事件(2004 年)の 6000 円[14]といった金額などが挙げられる。言い換えれば、補償金額として 5000 円以上の賠償を求めるのであれば、民事裁判に持ち込まないと難しいと現在のデータから推察される。

さらに、上記 31 事例について JO モデルを当てはめて分析を行い、そのギャップについてグラフ化を行った。（ブルーの棒グラフは実際に企業が提示した補償額を意味し、オレンジの棒グラフは同事例について JO モデルで算出した想定損害賠償額を意味している。グラフの便宜上、50,000 円以上はすべて 50,000 円としてプロットした）

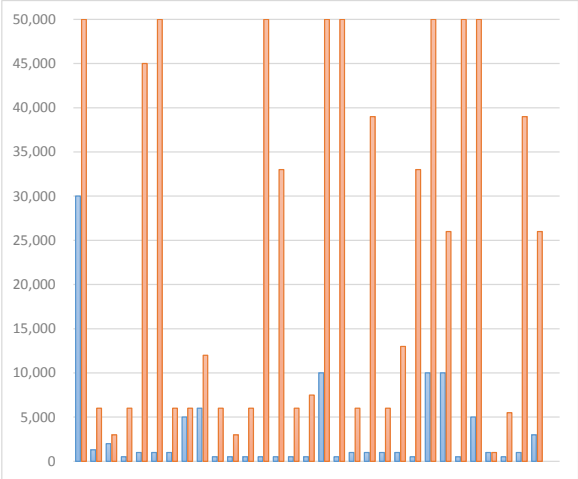

図 4　企業補償額と JO モデルのギャップ

上図をみてわかる通り、JO モデルと実際の企業が提示する補償額には大幅なギャップがあることがわかり、多くの事例において 2 倍以上の差異が見受けられる。上記のことから、JO モデルが現実的な補償額を割り出す点では改善の余地があると考えられる。

6　課題

本テーマを考える上での課題は以下のように抽出できる。

課題の一つとして、JO モデルが提示する金額が個人情報漏洩賠償額の規範例を示す一方、個人情報漏洩が実際に発生した場合とのギャップが指摘できる。特に、個人賠償金額が仮に 1000 円だとしても、賠償対象者が 10 万人いれば 1 億円になる。

その一方、規範的な個人情報漏洩賠償金額モデルとしての精緻化である。JO モデルが開発された 2003 年度に比べて外部環境が変化していると考えられ、そのことも考慮に入れるべきだと考えられる。特に SNS（Social Network Service）などを利用して個人情報を収集可能である。OSINT（Open Source Intelligence）技術の発展、あるいは攻撃方法の多様化などにより、サイバー空間上に存在する個人情報数、攻撃技術に変化が生じている。その意味で精緻化の余地があると考えられる。具体的には、特に考慮すべきだと考えるべき点として３点を

挙げる。

第一に、「検索容易性」が挙げられる。現在では SNS などに挙げられている情報をもとにさらなる個人情報を引き出すことが可能である。当然、SNS 上に存在する個人情報は、個人の自由意思に基づいて記載されている反面、記載情報と漏洩情報がリンクすることは想定されていない可能性が多い。実際に、個人を特定可能な情報(メールアドレス)などがあればあるほど別の情報へリンクしやすい。そのため、漏洩する情報次第では攻撃者により二次情報漏洩をしてしまう可能性がある。

第二に「変更容易性」(Cancelability)が挙げられる。例えば、パスワード情報の漏洩については騒がれることが多い反面、SYK 型認証情報(Something You Know)[19]ついては通常オンライン上で変更できる場合が多い。その一方、生年月日・住所などについては変更したくてもできないケースが多く、それらの情報を秘匿したい人にとっては非常に困る可能性がある。

第三に「回収容易性」が挙げられる。会員サイトからの情報漏洩の場合、PasteBin[20]などに張り付けられてしまうと多くの人にダウンロードされ、別のサイトなどで公開されてしまうなど回収が困難である。また、Winny による情報漏洩で明らかになったように、一度サイバー空間に漏洩した情報を根本的に回収することは難しい [21] 。その一方、内部犯行の事例などでは、その多くが金銭的動機による犯罪であり、漏洩先は名簿業者などに限定されている。公的機関により調査により流出先をある程度限定できるため、この観点でも想定賠償被害額のモデルに組み込まれるべき指標であると考えられる。

7 まとめ

情報漏洩事故が発生した場合、企業・組織はメディア対応、被害者への補償、原因究明など様々なことに気を配りながら、対応を進める必要がある。その一方、それらのインシデントにはどれぐらいの費用が想定され、それに対する投資額としてはいくらが妥当なのか各企業・組織で把握することは非常に困難である。

本論文では、まず企業が実際にインシデント対応を計画・シミュレーションするためのフレームワークを整理した。観点とすると、ROSI フレームワークが提示するように費用対効果を意識すること、またインシデントかかるコストを算出する CyberTab フレームワーク、そして想定賠償額を算出する JO モデルを例に挙げた。汎用的な指標ではあるが、どのような観点に注意しながら想定コストを考えればよいか分析が可能になると思われる。また、個人情報漏洩補償について実際に企業が支払う事例を研究し、その多くが 500 円~1000 円程度に収まることが分かった。さらに、JO モデルで算出可能な想定賠償額との比較を行い、少なくても 2 倍以上のギャップが存在することが分かった。このことから、JO モデルは個人情報漏洩時の賠償額を考える上で規範的指標となりつつも、実際の企業は 2003 年のローソンカードの事例(補償額 500 円)を基に補償額を決めていると考えられる。その後、筆者は JO モデルについて以下の 3 点を提言した。JO モデル策定時と比較し外部環境が変化していることから、「検索容易性」、「変更容易性」、「回収容易性」の 3 点をモデルに組み込むことを提言した。今後は、各企業の補償額と他の要素(補償額の支払方法、情報公開速度)との連関性、および他の指標(株価、検索エンジン上のキーワード注目度)にどのような関連性が見えるか、定量的分析を試みる予定である。また、JO モデルの精緻化モデルの提案なども行いたいと考えている。

参考文献

[1] サイバーセキュリティ:傾向分析レポート 2014, NRI セキュアテクノロジーズ株式会社, http://www.nri-secure.co.jp/news/2014/0820_report.html

[2] セキュリティー・リスク・アセスメントにおける定性的評価の改善, 松井 康宏 http://www-06.ibm.com/ibm/jp/provision/no57/pdf/57_paper4.pdf

[3] Introduction to Return on Security Investment, ENISA,
http://www.enisa.europa.eu/activities/cert/other-work/introduction-to-return-on-security-investment/at_download/fullReport
[4] 定量的セキュリティ測定手法および支援ツールの開発 - 調査報告書 別冊 定量的セキュリティ尺度測定ガイドライン, 情報処理推進機構
http://www.ipa.go.jp/files/000013701.pdf
[5] CyberTab, The Economist Intelligence Unit Ltd
https://cybertab.boozallen.com/
[6] 情報漏えいインシデントの調査結果から学ぶセキュリティ対策, NPO 日本ネットワークセキュリティ協会
http://www.jnsa.org/seminar/2008/0822/080822_incident.pdf
[7] 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, NPO 日本ネットワークセキュリティ協会
http://www.jnsa.org/result/incident/data/2012incident_survey_ver1.1.pdf
[8] 不正アクセスによるお客様情報流出の可能性に関するお知らせとお詫び, 株式会社ジェイアイエヌ
http://www.jins-jp.com/illegal-access/info20130315-1600.pdf
[9] 不正アクセス（JINS オンラインショップ）に関する調査結果（最終報告）, 株式会社ジェイアイエヌ
http://www.jins-jp.com/illegal-access/info.html
[10] Cyber Insurance: A Last Line of Defense When Technology Fails, Latham & Watkins
http://www.lw.com/thoughtLeadership/lw-cybersecurity-insurance-policy-coverage
[11] 東京海上日動 個人情報漏えい保険
http://www.tokiomarine-nichido.co.jp/hojin/baiseki/roei/
[12] 損保ジャパン 個人情報取扱事業者保険
http://www.sompo-japan.co.jp/hinsurance/risk/relief/infomation/index.html
[13] 企業・組織における個人情報漏えい事故の補償について-お詫び金に着目した考察-,情報処理学会 EIP 研究会
http://lab.iisec.ac.jp/~harada_lab/lab/2013/20130516.pdf
[14] 過去最高の賠償金となったTBCの情報流出, ITPro
http://itpro.nikkeibp.co.jp/article/COLUMN/20070215/262166/
[15] JAL 監視ファイルで考えてしまうプライバシーの範囲と企業倫理, 新倉 茂彦
http://blogs.itmedia.co.jp/niikura/2010/11/jal-7f45-1.html
[16] 顧客情報流出による損失 70 億円超と試算、三菱 UFJ 証券, ITPro
http://itpro.nikkeibp.co.jp/article/NEWS/20090909/336929/
[17] “見えない”が最も怖い, ITPro
http://itpro.nikkeibp.co.jp/article/NC/20100702/349899/
[18] 最終回 個人情報漏えい プライバシ侵害の損害賠償の根拠, ITPro
http://itpro.nikkeibp.co.jp/article/COLUMN/20110412/359332/
[19] 利用者認証の種類 --- SYK, SYH, SYA, ITPro
http://itpro.nikkeibp.co.jp/article/COLUMN/20060324/233215/
[20] PasteBin
http://pastebin.com/
[21] Winny、Antinny に関する FAQ, 情報処理推進機構
https://www.ipa.go.jp/security/virus/faq/winny_qa.html