Vol.2013-EIP-60 No.8
2013/5/16

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—

菅原尚志† 原田要之助†

個人情報を漏えいした企業・組織は数々の対応をしなければならないが、そのひとつに補償が挙げられる。近年の個人情報漏えい事故を見ると、漏えいした個人情報の人数が事故 1 件で 1,000 万人にのぼることもある。したがって、たとえ 1 人あたりの補償額が少ないとしても、総補償額は巨額になり得る。

訴訟に発展する前に、被害者に対してお詫び金を支払う場合がある。特に日本では事故を起こした際にお詫び金を送る習慣がある。個人情報漏えい事故を起こした企業・組織は少額のお詫び金を送る場合があり、訴訟を避ける目的と考えられるが、お詫び金の支払いに関する規定やガイドラインはなく、企業・組織毎に支払いの判断がされているのが現状である。

本研究では、過去の事例を挙げて、どのようにしてお詫び金が送付されたかを検証する。また、アンケートを用いてお詫び金について分析し、個人情報漏えいのリスクマネジメントについて考察する。

A study on the compensation by company/organization when privacy and personal information are compromised - Focusing on the money compensation -

TAKASHI SUGAWARA† YONOSUKE HARADA†

The companies and organizations which leaked privacy information of customers need to take necessary actions, and compensate loss of privacy protection. Among many privacy information leakage incident cases, even an incident with victim over 10 million will happen. The total amount of compensation can be big, even if each amount of personal compensation is small.

Before developing to a lawsuit, the companies and organizations pay compensation to potential victims. In Japan, people give a gift for reconciliation when they encounter troubles. In cases, companies and organizations have paid small money compensation than actual court trials. This conduct may reduce the actual court trials. However, companies and organizations do not develop any rules and procedures for compensation, and they decide case by case.

In this study, the past privacy information leakage incidents are analyzed how the money compensation are paid. And, by using a questionnaire, the tendency of the money compensation in Japanese companies and organizations make clear, and aspects of risk management for privacy information incident are considered.

1. はじめに

企業や組織において個人情報漏えい事故が起きた場合、企業・組織には損害賠償責任が発生する場合がある。NPO 日本ネットワークセキュリティ協会（JNSA）と情報セキュリティ大学院大学の「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」[1]によると、個人情報漏えい事故は年間で 1,551 件発生しており、1 件あたりの平均想定損害賠償額は 1 億 2,810 万円とされ、企業や組織にとって事業継続上の重大なリスクと捉えるべきである（表 1 参照）。

表 1　2011 年個人情報漏えいインシデント概要データ[1]

漏えい人数	628 万 4,363 人
インシデント件数	1,551 件
想定損害賠償額	1,899 億 7,379 万円
1 件あたりの漏えい人数	4,238 人
1 件あたり平均想定損害賠償額	1 億 2,810 万円
1 人あたり平均想定損害賠償額	4 万 8,533 円

† 情報セキュリティ大学院大学　情報セキュリティ研究科
Institute of Information Security

また、損害賠償以外にも、謝罪広告やお詫び状の郵送による費用の支出が必要な場合がある。さらに、適切な対応がとられない場合、顧客を軽視し、コンプライアンス意識が低い会社であるという印象を社会に植え付けてしまう可能性がある。その結果、企業への信用が大きく悪化するため、顧客の離反や新規採用への悪影響、株価、格付けの低下、ブランドイメージの毀損、資金調達コストの増加など、事業者の経営にも広く悪影響を及ぼす風評リスクが発生する可能性がある[2]。

近時の傾向として、企業が大量の個人情報漏えい事件を起こした場合、お詫びに加えて 1 人当たり 500 円の金券を配布する例が見受けられる。宇治市住民基本台帳データ漏えい事件判決で認定された慰謝料 1 人当たり 1 万円という基準や TBC 事件で認定された 3 万円に比べれば、それぞれ 20 分の 1、60 分の 1 という額ではあるものの、数十万人、数百万人という被害者がいる場合にはそれでも巨額のコストがかかることになる。被害者人数が多く、プライバシー侵害の程度が大きい場合には、謝罪に巨額のコストをかけても、それによって損害賠償請求を行ってくる被害者の数をできる限り減らすことができ、最終的には少ないコスト

で済むことも起こり得る。なかには、500 円の金券を配布するのではなく、500 円の金券への引換券を配布し、実際に引換所に現れた被害者に対してだけ金券を渡す方法をとり、コストを抑えた企業もあった。しかしながら、このような金券の配布は、被害者への損害賠償請求権自体がすべて消滅するものではない。

2. 個人情報漏えい事故における損害賠償

個人情報保護法には、個人情報漏えいの結果発生した損害の賠償に関する規定は存在しない。しかし、漏えい事故を発生させた企業は、被害者から訴訟を起こされ、損害賠償請求を受けるケースもある。この場合、精神的損害を被ったとして、慰謝料を請求されることになる。また、訴訟を起こされたとしても、和解によって解決するということもあるようだ[4]。近年の漏えい事故を見ると、漏えいした個人情報の人数が事故 1 件あたり 1,000 万人にのぼることもある。したがって、たとえ 1 人あたりの支払額が少ないとしても、訴えた被害者の人数によっては、企業・組織の総支払額は理論上巨額になり得る。

過去に損害賠償金が支払われた事例を以下に挙げる。

- 宇治市住民基本台帳データ大量漏えい事件[3]

1998 年 4 月、宇治市の乳幼児健診システムの開発を担当していた民間のシステム会社のアルバイト従業員が、住民基本台帳データ 21 万 7,617 件分のデータを不正にコピーして持ち出し、名簿業者に売却した事件である。漏えいしたデータは、個人の住民番号・住所・氏名・性別・生年月日・転入日・転出先・世帯主名・世帯主との続柄等であった。名簿業者がさらにこのデータを他に販売するなどしたことに関して、宇治市の住民数名が、データの流出によって精神的苦痛を被ったと主張して、宇治市に対し、プライバシー権侵害を理由とした損害賠償請求（慰謝料及び弁護士費用）の支払を求めた。請求額は、1 人あたり慰謝料 30 万円、弁護士費用 3 万円であった。京都地方裁判所は市役所に 1 人あたり 1 万円の慰謝料と弁護士費用の 5.000 円を科す判決を下し、市は控訴した。大阪高等裁判所は京都地裁と同様、個人情報漏えいの責任が使用者である宇治市にあると判断し、宇治市に対し提訴者に損害賠償をするよう命じた。その損害賠償額は 1 人当たり 1 万 5,000 円と認定され、その内訳は慰謝料 1 万円、弁護士手数料 5,000 円というものであった。実際に訴訟を起こした提訴者は 3 人であったため、賠償額は結果として 4 万 5,000 円と高額ではない。仮に漏えいした約 22 万人全員から集団訴訟されたりすると賠償額は 30 億円になったと考えられる。なお、個人情報漏えい事故に関する損害賠償支払い命令が出た判決としては初めての判例とされ、後述の個人情報漏えい事故の裁判やお詫び金に大きく影響していると考えられる。

以上のような判決が出たものの、現実的には多数の被害者が提訴することは現在の日本では考えにくい。1 人当たり 1 万 5,000 円の損害賠償額では、たとえ勝訴しても弁護士費用やその他の裁判費用の方が高額となり、費用超過になる可能性が高い。したがって、多数の被害者が損害を覚悟して訴訟に踏み切る可能性は低いと考えられる。これまでに起きた日本での個人情報漏えい事件を見ても、一度に多数の被害者が同時に訴訟に踏み切った事例はない。これは、日本にアメリカのような集団訴訟制度aが存在しないことも影響していると考えられる。

3. 個人情報漏えい事故におけるお詫び金

個人情報漏えい事故が起き、被害者側から損害賠償に関する訴訟へ発展する前に、被害者に対してお詫び金を支払うケースがある。お詫び金として商品券等を送付する時には直接的なコストに加え、郵送料金やダイレクトメール作成、人件費といった間接的なコストも発生する。なお、お詫び金の支払いに関する規定やガイドラインは定められておらず、企業・組織に支払いの判断が委ねられている。

個人情報漏えい事故を起こした際に被害者から訴訟を起こされた場合、事故を起こしてしまったことによる信用の低下だけでなく、さらに、企業・組織のブランドイメージの毀損が懸念される。たとえば、株式会社ローソン（以下、ローソンとする）では、個人情報流出発覚後に約 115 万人の会員全員にお詫び状と 500 円分の商品券を送付した。送付コストなどを含めて 5 億円以上の経費がかかったとされている。また、株式会社アプラス（以下、アプラスとする）も約 8 万人の被害者に、お詫び状と 1,000 円分のギフト券を送付したとされる。このアプラスの事件では、氏名、住所、電話番号、生年月日などの基本情報に加えて、顧客の職業区分や年収区分も流出した。送付したギフト券の総額は 8,000 万円になったとされる。

個人情報流出の被害者に商品券などを送付し謝罪することは、企業の信頼性低下を最小限にとどめ、社会の当該企業に対する信頼の回復を図る、という意味を持つ。さらに、ブランドイメージの棄損を防止するといった理由も挙げられる。一方で、被害者となった本人に対して謝罪の姿勢をアピールすることにより、個人情報漏えいの被害者による提訴の率を下げ、大量の被害者による集団訴訟に基づく巨額の損害賠償額のリスクを回避するという側面も考えられる。事故を起こした企業・組織は、同業他社で同様な個人情報漏えい事故が起きお詫び金を送付していたとしたら、同様の、またはそれ以上の経営判断をすることになる。過去の個人情報漏えい事故と公表されているお詫び金など

a クラスアクションとも呼ばれる。アメリカ民事訴訟において、同等な被害を被った多くの消費者の権利を一括して行使する権限が認められ、被害救済の目的を持つ。

の支払いを付録に示す。

なお、お詫び金支払いについて被害者以外に開示されていないケースも想定される。そのため、付録に示した事例は過去の事例全てを網羅できているわけではなく、実際にはさらに多い事例があると推想される。また、公表されてはいないものの、例えばオンラインゲーム分野においてはゲーム上の仮想的な金銭をお詫び金の代わりにしていることも考えられる。すなわち、実際に金券としてのコストとするのではなく、自社でのみ使うことができるポイント等にすることによって、自社での売上に計上できる。つまり、マーケティングのためのツールとしてお詫び金を用いているとも言える。

また、日本国内と海外では、お詫びに対する考えが異なるであろう。2011 年 4 月、外部からの不正アクセスを受け、海外のソニーグループの企業から個人情報が流出した。日本国内だけでも被害者数は 740 万人以上となった。この事件では氏名、住所、国名、性別、生年月日、電話番号メールアドレス、オンライン ID、ログインパスワード が漏えいした。この事件では、ネットワークサービスが止まったことに対する補償として特定コンテンツの無料ダウンロードなどを提供した。これは、文化や訴訟などの仕組みの違う海外の事例であり、「個人情報漏えいに関するお詫び金」といった捉え方をせずに「ネットワークサービス停止に対する補償」という判断をしたものと考察され、国によってお詫びや補償に対する考えが異なると考えられる。アメリカでは集団訴訟制度が存在するため、可能な限り訴訟を避けるための補償を提供していると考えられる。

4. 個人情報漏えいに関する保険

個人情報漏えいを防ぐために情報セキュリティ対策を実施することは不可欠であるが、いかに対策を実施したとしても、対策に万全はあり得ないため、完全に防ぐことは不可能である。個人情報漏えい事故が発生した場合の企業・組織の被害を低減（転嫁）する手段としての保険（リスクの共有）がリスクマネジメントにおける重要な役割を担うことになる。

個人情報漏えい事故が発生した場合、加害者である企業・組織は、損害賠償金の支払いやお詫び金の送付を余儀なくされるだけでなく、長年かけて築いてきた信用や消費者からの信頼、ブランドイメージを失いかねない。個人情報漏えい事故が発生した際には、信頼を回復すべく説明責任の遂行や広報宣伝活動を行う必要がある。個人情報漏えいに関する保険は、こうした事業者が負担する損害賠償金や各種費用を補償することにより、事業活動を支援することを目的としている。この保険は、賠償責任保険bに属し、その担保範囲としては、法的な賠償責任に関する部分から争訴に応じるための弁護士費用、謝罪広告やお詫び状郵送に関する費用に至るまでの広範な損害を補償する。補償内容は一般に保険会社が定めたいくつかのパターンから選択できる。また、保険料の算定にあたっては、会社の規模、取り扱う個人情報の件数および内容等から一般的な算定式に基づく査定を行った上で、プライバシーマークや ISMS 適合性評価制度における認証を受けていることなど、個人情報保護体制の確立状況に応じて保険料を減額する場合がある。

現在、多くの損害保険会社から個人情報漏えいに関する損害保険が提供されている。多くの個人情報漏えい保険は大きく 2 つの補償内容から構成されている。ひとつは賠償責任担保部分であり、これは個人からプライバシー侵害などで損害賠償請求された場合の、法律上の賠償金や訴訟になった場合の費用（弁護士費用等）を補償する。もうひとつは費用損害担保部分である。損害賠償請求まで至らない場合でも、お詫び状の送付や謝罪広告費用など多くの費用が発生することが想定される。賠償責任担保部分では、法律上の賠償金ではない費用損害については補償の対象とならないため、費用損害担保部分でこのようなお詫び状の発送費用などを補償する。

各社で多少の違いはあるが、補償する対象・費用はほぼ共通している。細かな違いとしては、自社従業員による個人情報漏えい時も補償対象か、委託先での情報漏えい時も補償対象としているか、等が挙げられる。なお、年間保険料の算出式や、業種・売上高毎の費用の違いについて公表しているかどうかは各社で異なっている。

5. 損害賠償金とお詫び金に関する先行研究

5.1 想定損害賠償額算出式

JNSA では個人情報漏えいにおける損害賠償の定量化に関して、過去の情報漏えい事件・事故の分析、プライバシー権や名誉棄損の判例の分析、および専門家の助言に基づき、独自に算出式を作成している[5]。各組織が保有する個人情報が漏えいした場合の想定損害賠償額（情報の価値）を独自に算定し、セキュリティ対策費用の目安が得ることを目的としている。損害賠償額を 1 人あたりの個人情報の社会的価値と置き換えて考えることにより、組織が保有する個人情報の件数に基づいて、その組織が個人情報を保有することの潜在的なリスクを定量化できるとしている。

また、JNSA の想定損害賠償額算出式では、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 種類の尺度で分類する。影響の大きさ

b 個人または企業に過失があるとき、場合によっては過失がないときにも、他人に加えた損害について賠償責任を負わされる場合がある。被保険者が契約に基づき、第三者に対して一定の財産的給付をなすべき法的責任を負うことによって被る損害を填補することを目的とする損害保険である。企業で所有する施設への損害に対する施設賠償や、業務の遂行上で発生する製造物責任に関する賠償がある、

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」の度合いを示すグラフ（EP 図：Economic-Privacy Map）を作成する。 x 軸の正の方向に対して精神的苦痛の大きさが、y 軸の正の方向に対して経済的損失の大きさが対応する（図 1 参照）。

また、個人情報を以下の 3 つの属性に大別する。

- 基本情報：個人情報保護法による個人を特定する基本四情報
- プライバシー情報：漏えいした場合、他人に知られることにより個人に対して精神的苦痛を与え得る情報
- 経済的情報：利用することにより、個人の持つ資産に直接的に影響を与え得る情報

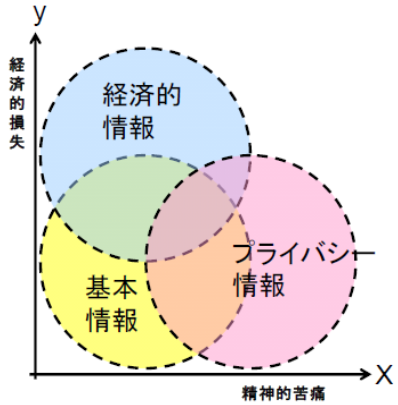

図 1　EP 図[1]

これらの 3 つの属性は互いに重なり合うこともあり得る概念であるが、経済的損失と精神的苦痛の 2 軸の座標でその概念を示し、かつ具体的な個人情報の種別をその座標の中にプロットすると以下の図に示す S-EP 図のようになる。

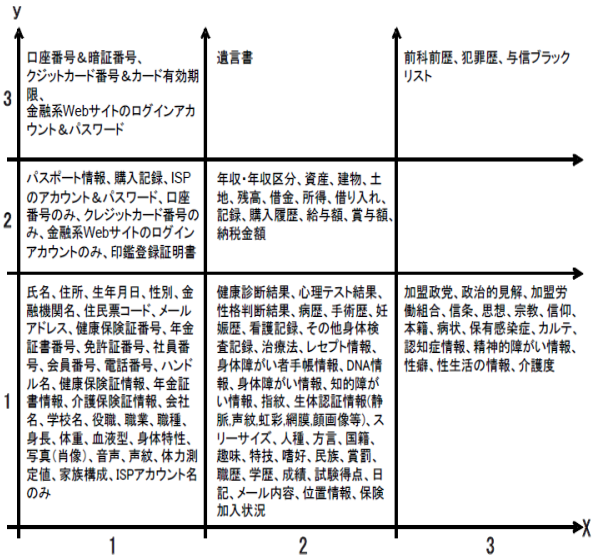

図 2　S－EP 図[1]

この S-EP 図は、EP 図上へ過去の個人情報漏えい事件・事故の調査分析で得られた漏えい情報の種類をプロットしている。漏えいした情報がどのような影響を与えるのか、つまりどの程度の価値を持つのかが図 2 の EP 図上のプロット位置により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、図 2 の S-EP 図の x 軸と y 軸を影響度合いに応じてそれぞれ 3 段階に分け、漏えい情報の種類を再配置している。

さらに、基礎情報価値、機微情報度、本人特定容易度、情報漏えい元組織の社会的責任度、事後対応評価をそれぞれ判定し、算出式に当てはめることにより、想定損害賠償算出額を求めることができる。

想定損害賠償額算出式では、算定を簡易化するために、「漏えいした情報の種類」「個人特定の容易さ」「漏えいを起こした組織の社会的責任度」「事後対応の善し悪し」といった限定された要因のみで損害賠償額を求めている。しかし、実際の裁判では上記の要因の他、「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」など様々な要因や背景が吟味されるため、より現実に近い答えを得ることは難しいであろう。

5.2　被害者から見た損害賠償金とお詫び金に関する調査

個人情報漏えい事故に対する損害賠償金について、インターネット利用者がどのように評価するかを定量的に計測したアンケート調査がある[6]。2007 年に Web アンケートによる全国のインターネット利用者 1,386 人から回答が得られている。設問として以下の 3 つのケースを挙げ、設定された損害賠償金としての慰謝料が妥当であるか否かを質問している。

①身体的特徴が漏えいしたケース
精神的被害（不安感が続く）、実被害（重大な被害）、企業対応（ホームページで謝罪）、慰謝料 3 万 5 千円
②メールアドレスが漏えいしたケース
精神的被害（不安感が続く）、実被害（被害あり）、企業対応（500 円の金券）、慰謝料 6 千円
③基本情報（氏名・住所・性別・生年月日）が漏えいしたケース
精神的被害（心配のみ）、実被害（被害あり）、企業対応（詫び状）、慰謝料 1 万円

この調査結果について、以下の図 3 に示す。

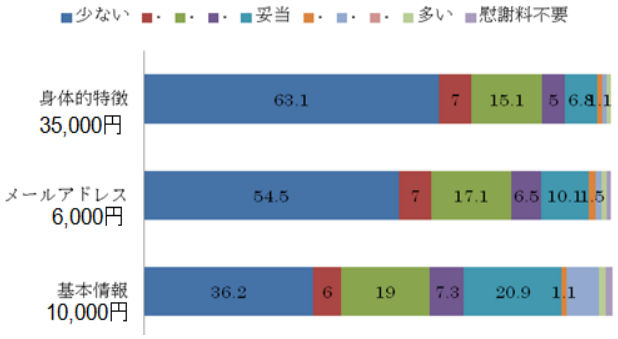

図 3　アンケート回答結果[6]

①の身体的特徴においては、インターネット利用者の多くは 3 万 5 千円の慰謝料が少ないと感じている。この①～③の 3 つのケースはそれぞれ過去に起きた事例を参考とし、設問を設定している。そのため、実際に支払われた慰謝料を参考に設定されているのだが、①の身体的特徴に関する情報については慰謝料以上の損害を与えられていると感じる一般者は少なくないということになる。なお、この調査は被害者目線での調査となっているため、加害者（企業や組織）目線では異なる結果が得られると予測される。

6. 企業・組織から見たお詫び金

筆者らは企業・組織の立場からのお詫び金に関する認識を把握するために、アンケートを用いて分析した。2012 年 7 月から 8 月に、日本国内のプライバシーマーク取得企業、ISMS 認証取得企業、官公庁、教育機関などから、ランダムに選んだ 4,500 の情報セキュリティシステム担当者を対象とした「情報セキュリティ調査」を実施した[7]。この調査では、個人情報漏えい事故のお詫び金についてアンケート形式での調査を行っている。調査結果を以下に示す。

個人情報漏えい事故発生時のお詫び金に関して、事前に基準を定めているのは 4%にとどまっており、ほとんどの企業ではお詫び金に関する規定を定めていない（図 4 参照）。また、定めていると回答した企業は、過去に事故などの経験がある企業など、一部の企業にとどまっていると考えられる。

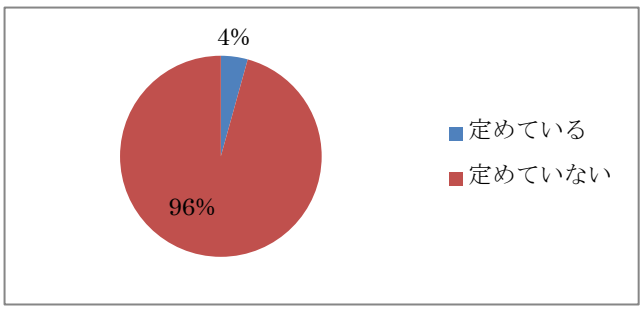

図 4　お詫び金支払額についての基準策定状況（N=325）

電話番号、購入に関する情報といった基本的な個人情報については、比較的低い金額であり、1,000 円以内が半数以上を占めている（図 5 参照）。これは、被害者に対して金銭的な損害や、精神的な被害を負わせる可能性が低いため、企業・組織としては低い金額を想定していると考えられる。

一方、遺言書や与信ブラックリスト、口座番号、カルテといった個人情報については比較的高い金額が設定されており、5,000 円以上が半数以上を占めている。これは、被害者に対して金銭的な損害や、精神的な被害を負わせる可能性が高く、お詫び金の金額として表れていることがわかる。

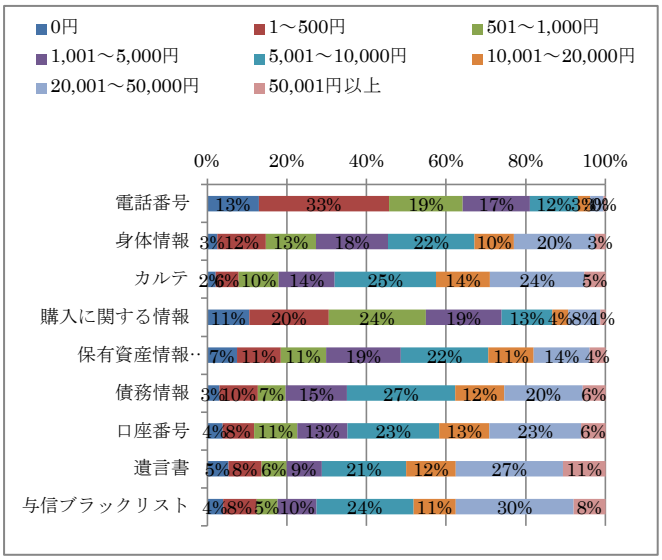

図 5　想定お詫び金支払額
（上から N=232、N=231、N=228、N=226、N=228、N=228、N=230、N=226、N=226、単位：円）

また、調査では 50,000 円以上と回答した場合については具体的な金額を記入してもらっているが、遺言書については 100,000 円と記載されている例もあり、最高金額は 1 千万円であった。

すなわち、お詫び金支払い額については、漏えいした個人情報の種別が影響を与えると考えられる。特に、口座番号などの二次被害に繋がり得る個人情報や、機微なプライバシー情報に関わるカルテが漏えいすると、お詫び金額に反映される必要があるという結果がアンケート調査より得られた。

また、調査では自由記入欄を設定しており、以下のようなコメントが得られた。

- 相場を知らないためわからない
- 予測できない
- お詫び金(小規模)の情報が少ない
- ニュースになるのは大企業が多く、小規模事業者の妥当なお詫び金等の情報が少なく感じる
- 相場感が全く分からないのが不安に感じている

ここでは、他社で支払われたお詫び金についての情報を

求めている企業・組織が見受けられ、他社の事例を参考にして支払額を決定していると考えられる。もちろん、他社の事故対応等の情報を得ることは重要であるが、自社での事故を詳細に把握した上で、自社の責任（過失）と被害者への被害の程度から、被害者への補償方法を考えるべきであると考える。たとえば、付録に示すように多くの小売業ではお詫び金を受け取りに店へ来店したり、自社の商品やサービスを利用することを期待しているが、卸売業や製造業では異なった対応が取られると考えられるためだ。

7. まとめ

個人情報漏えい事故を起こすと、加害者側である企業・組織はプライバシー侵害を理由とした損害賠償金の支払いをすることがある。氏名、住所、性別、生年月日といった個人情報に加え、プライバシーに関する情報が漏えいした場合、高額な賠償金の支払い対象となり得る。また、1 人あたりの賠償額が少額な場合でも、電子的なデータのときは大量に漏えいすることがあるため、さらに多額の賠償になる可能性もある。

このため、被害者が訴訟に持ち込む前に企業側の誠意を示すことで顧客からの信頼を回復し、また、企業のブランドを回復するために、お詫び金を支払うケースは少なくない。この場合、企業独自の判断でお詫び金の額を定めるが、企業毎にお詫び金に関する基準があいまいである。また、過去の個人情報漏えい事故発生時に支払われた金額を参考とし、同様の金額と設定されることも少なくない。

損害賠償額を予測するために、JNSA では独自の算出式を提唱している。個人情報の価値等を判断することにより個人情報の重み付けを行っている。しかしながら、損害賠償金のみを対象としている。また、櫻井は、一般者に対する損害賠償金やお詫び金に関するアンケート調査を実施している。そのため、一般者のみを対象としており、加害者側である企業・組織については触れられていない。

自社特有の経営環境等も考慮する必要があると考えられる。事業体系として、BtoB の場合と BtoC の場合では補償方法が異なる。BtoB の場合は契約等で事前に定められているが、BtoC では定められていないことがほとんどであろう。また、補償の方法としても、金券等を直接送付することに限らず、Web サービス上でポイントを配布するなど、自社の環境を考慮した上でより効果的な補償方法を考える必要がある。しかしながら、一部の企業に見られるようにお詫びをマーケティングと組み合わせているケースがある（付録参照）。あくまでも「お詫び」の形として支払いを考えることが重要であろう。

また、独占的に展開している企業（インフラ業など）においては、顧客離れが起きにくく、お詫び金を支払うということを全く想定していないということも考えられる。お詫び金等を支払わないとしても、謝罪文をホームページ上に公開するだけでなく、何かしらの形で被害者である顧客への補償をすることが重要であると考える。

本研究では、アンケート調査を用いることによって企業・組織が支払うお詫び金について分析した。漏えいした個人情報に基本的な情報が含まれている場合に比べ、金銭的な損害につながる個人情報やプライバシー侵害に関わる情報が含まれていた場合の方が高いお詫び金を払うという傾向が見られた。また、過去の事例等より、金融系の業種や金融に関する情報を取り扱う企業では資産情報や口座番号などの情報に対して高いお詫び金を想定していることがうかがえる。しかしながら、アンケートに記載されたコメントから読み取れるように、過去の事例を参考とし、500 円から 1,000 円といった同様な金額を支払う企業・組織は少なからず存在する。お詫び金という概念については重要であると考えるが、自社での事故を詳細に把握した上で、被害者への補償方法を適切に判断すべきであると考える。

個人情報漏えい事故を起こした企業や組織は、事故の復旧に関する対応策だけでなく、被害者への補償方法についても事前に考えておく必要があるであろう。たとえば、実際には流出していなかった被害者に対してもお詫び金が送付されている事例が過去にはある。主な理由としては、漏えいした個人情報全体を把握できていない段階でお詫び金送付を決定してしまった、ということにある。そのため、お詫び金送付に至るまでの過程等についても事前に考えておき、備える必要があるであろう。

また、リスクファイナンスとして、保険等に加入することも有効な策であろう。近年の個人情報漏えいに関する保険は従前と異なり、自社に過失があった場合でも補償の対象となる保険プランも用意されている。また、加入方法についてはオプションとして自社に必要な部分にのみ加入することも可能となっており、自社への脅威に対して必要最低限の保険を利用するなど、有効に活用していくことが重要である。

参考文献

[1] NPO 日本ネットワークセキュリティ協会・情報セキュリティ大学院大学、2011 年情報セキュリティインシデント調査報告書
[2] 東京海上日動リスクコンサルティング、「個人情報保護とリスクマネジメント」、ソフト・リサーチ・センター、2005 年 6 月
[3] 大阪高判 2001・12・25 別冊 NBL79 号 190 頁
[4]淵邊善彦・五十嵐敦、「個人情報管理ハンドブック第 2 版」、商事法務、2008 年 4 月
[5] 山田英史・大谷尚通・山本匡、「インシデント調査に見る現状と情報漏洩の想定被害額」、信学技報 2004-17、2004 年
[6] 櫻井直子、「情報セキュリティの価値と評価」、文眞堂、2011 年 12 月
[7]根岸秀忠・菅原尚志・村山厚・平木健士・佐藤栄城・原田要之助「企業・組織における情報セキュリティ調査」、2013 年暗号と情報セキュリティシンポジウム、2013 年 1 月

付録

表 2　お詫び金が支払われた事例（著者作成）

対応年月	企業名	対象者数	お詫び金額	送付されたお詫び金
2003 年 6 月	ローソン	560,000	500 円	商品券
2003 年 8 月	アプラス	79,110	1,000 円相当	商品券
2003 年 8 月	ジェーシービー	6,923	1,000 円相当	商品券
2003 年 11 月	ファミリーマート	182,780	1,000 円相当	クオカード、または、ファミマ・ポイントを 100 ポイント
2003 年 12 月	東武鉄道	131,742	5,000 円相当	東武動物公園または東武ワールドスクエア招待券 2 枚
2004 年 1 月	ソフトバンク BB	4,517,039	500 円	金券
2004 年 3 月	サントリー	75,000	500 円	郵便為替
2004 年 5 月	ツノダ	16,000	500 円相当	金券
2004 年 6 月	コスモ石油	923,239	50 マイル分	ガソリンマイル
2004 年 7 月	DC カード	478,000	500 円	商品券
2005 年 1 月	オリエンタルランド	121,607	500 円	金券
2005 年 3 月	JR 東日本	300	1,000 円相当	GALA 湯沢場内利用券
2005 年 10 月	小田急電鉄	6,203	500 円相当	金券
2007 年 3 月	大日本印刷	8,640,000	500 円	金券（43 社の業務委託元毎に対応が異なる。NTT ファイナンスやジャックスカードなどが送付）
2007 年 12 月	NTT ドコモ関西	339	1,000 円	QUO カード
2008 年 3 月	インデックス・コミュニケーションズ	186	500 円相当	金券
2008 年 4 月	サウンドハウス	122.884	1,000 円相当	サウンドハウスで使用できるクレジット
2008 年 6 月	相鉄ホテル	1,760	1,000 円相当	商品券（１組分）
2008 年 6 月	アイリスプラザ	28,105	1,000 円相当	ポイント
2009 年 2 月	NHN Japan	399	500 円	WebMoney
2009 年 5 月	三菱 UFJ 証券	49,159	10,000 円相当	ギフト券
2009 年 8 月	アリコジャパン	18,184	10,000 円（流出した人）、3,000 円（流出しなかった人）	商品券
2009 年 8 月	アミューズ	148,680	500 円相当	クオカード
2010 年 12 月	東村ジャパン	722	500 円または 1,000 円、300 円（流出したメール受信者）	定額小為替証券または電子書籍製品の割引クーポン、割引クーポン
2012 年 10 月	ジャム・ティービー	169	1000 円相当	Web ポイント