

個人情報漏えいに対する補償についての考察

—お詫び金と賠償金—

田中 智大^{†1} 原田要之助^{†2}

概要: 企業や組織等は個人情報の漏えい防止対策として、プライバシーマークや ISMS 認証を取得してきた。しかしながら、数百万件の個人情報漏えいが 毎年報告されており、プライバシーマークや ISMS 取得組織も含まれる。事前対策だけでは不十分で、漏えいを前提とした事後対策も必要であると考 えられる。また事後対策の 1 つとして日本ではお詫び金という対応がある。しかし、お詫び金の支払いに関する法律はない。そのため、お詫び金に関する基準は各組織の裁量に委ねられている。今回の研究では、アンケート調査を通して、企業や組織におけるお詫び金・補償の基準などについて分析した。

キーワード: 個人情報漏えい, お詫び金, 事後対策

Consideration about the compensation for the personal information leak

- Compensation and indemnity -

TANAKA TOMOHIRO ^{†1} YONOSUKE HARADA ^{†2}

Abstract: Companies or organization have been certified with privacy mark or ISMS to prevent from personal information leakage. However, leakage incidents, containing millions of personal information, are reported every year. Organizations certified with privacy mark or ISMS are included. Those measurements for prevention may be insufficient. Therefore, it is necessary to prepare post leakage measurements. Compensation is considered as one of post leakage measures. There is no legal regulation to define the amount of compensation. Individual organization has to decide the amount. In this report, I carried out questionnaire survey and analyzed it about the compensation systems in a company or organization.

Keywords: personal information leakage, Compensation,

1. はじめに

近年、様々な情報のデータ化などにより情報漏えいといったインシデントが問題になっている。それに対して企業や国には個人情報保護法やサイバーセキュリティリテリテ基本法を制定して、企業や組織に義務を課してきている。一方、企業や組織も情報セキュリティ対策技術の向上、個人情報保護法への対応、プライバシーマーク取得、ISMS 認証取得などによって、情報漏えいの対策を行ってきた。

日本ネットワークセキュリティ協会(以下 JSNA)の情報セキュリティインシデントに関する調査報告書[1]の 2005 年から 2013 年までの調査結果によると大きな事件によって著しく漏えい人数が多い年があるがそれらを除けば、ほぼ横ばいで 600 万件から 900 万件ほどの漏えい人数が毎年報告されている。このことから企業や組織が対策をとっているにもかかわらず情報漏えいインシデントが減っていない現状がある。これに対して、事前対策はもちろんのこと、情報漏えい事件への事後対応も重要になってくると考えられ

る。

とくに情報漏えいなどのインシデントの事後対応では、被害者に対するすばやい連絡や対応、インシデントの事実公表、顧客に対する補償などが考えられる。日本では、補償の 1 つにお詫び金という形で 500 円から 1000 円相当の金券などを配る対応がこの 10 年ほどにおいて、一般的に行われてきている。海外ではこのような対応は少なく、損害への賠償や訴訟になるケースが多い。本稿では、このお詫び金や補償金について調査、アンケート結果をもとに考察した。なお本稿におけるお詫び金には損害賠償や慰謝料といった法律や判決で決まるいわば補償金とは別に、謝罪や誠意をしめす意味合いで金券などを配布することを指す。

2. お詫び金・補償金に関する先行研究

2. 1 企業・組織からみたお詫び金

菅原の研究[2]では、個人情報漏えいに関してプライバシーマーク、ISMS 認証を取得している企業にアンケート調査を行ったところ、事前にお詫び金支払額に関して基準を定めているかの調査結果を図 1 に示す。

^{†1} 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY
^{†2} 情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

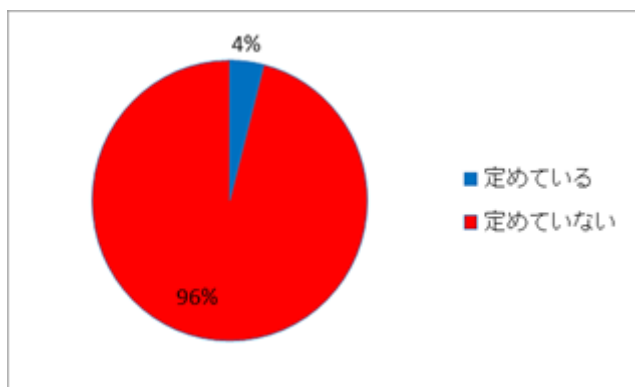


図1. お詫び金支払額についての基準策定状況(2012年度)(n=325)

結果は4%の企業・組織がお詫び金に関する基準を定めていた。

その図1で定めている企業に漏えいした個人情報の種類毎のお詫び金支払い額の基準を策定しているかどうか調査した結果を図2に示す。

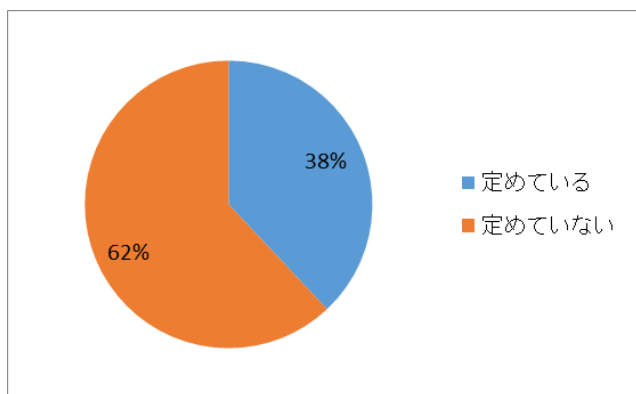


図2. 漏えいした個人情報の種類(レベル)ごとのお詫び金支払額の基準の策定(2012年度)(N=14)

結果は38%の企業・組織が個人情報の種類ごとにお詫び金の支払金額を策定していた。

またお詫び金に関する基準を定めていない企業も含めた想定でのお詫び金支払額を調査したところ、氏名・住所・性別・生年月日といった個人情報に関する基本的な情報が含まれている場合に比べ、2次被害につながる機微な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報告されている。

また、お詫び金は被害者が損害賠償の訴訟に持ち込む前に企業側の誠意を示すことで、顧客からの信頼回復や企業のブランドを早く回復できるように、お詫び金を支払うケースは少なくないと述べられている。この場合には、企業や組織では独自に決めた判断でお詫び金の額を決めている。しかしこのお詫び金に関する基準があいまいであると述べている。なお菅原は、アンケートでの自由回答の内容などから、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と分析している。

2. 2 被害者からみた損害賠償金

櫻井の研究[3]の中にある個人情報漏えい事故に対する被害者目線での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結果がある。これは2007年に全国のインターネット利用者に対して、Webアンケートを行ったもので1,386人から回答が得られている。

このアンケート回答の中で個人情報漏えい時に、企業に対して求める態度の調査結果(N=1,386)では、「慰謝料を請求する」35.4%、「慰謝料ほどでないが、詫言程度はほしい」25.7%、「漏洩した企業の商品、サービスを購入したくない」19.8%であり、「謝罪してくれればよい」12.4%、「何も必要ない」3.3%という結果である。すなわち、個人情報を漏えいした企業に対して、約35%の回答者が賠償金を、また、約26%の人が企業に対してお詫び金を求めているという結果になった。

次に、企業が取るべき対応の調査結果(N=1386)では、「事故の公表」26.6%、「謝罪文を送る」19.4%、「対応窓口の設置」17.3%、「慰謝料を払う」14.4%、「お詫びの品を送る」9.8%、「謝罪に行く」9.8%、「何も必要ない」2.1%という結果になり、約10%の「お詫び品を送る」というのが、本稿で述べているお詫び金に相当すると考えられる。

また実際の漏えいインシデントを想定とした質問もしており、設問としては身体情報、メールアドレス、基本情報の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。このケースで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問が設定されているのだが、全体的に少ないと感じている回答者が多い結果となっている。

また設問の企業対応に対して年代や性別での属性ごとに分析したところ、全体的に「ホームページで謝罪」が幅広い年代に対して効果があることが述べられている。また「詫言状」、「金券」による対応も男女による効用の違いはあるものの、全体的に効果があるとのべられている。櫻井の研究からも、お詫び金による効果があることがわかる。

3. 企業・組織によるお詫び金などの配布事例

3. 1 国内での事例

主に個人情報漏えい事後にお詫び金を支払った(企業によってはお詫び金と述べていないケースもある。本稿では、筆者が判断した)事例について公表されたデータを調査し

た。個人情報保護法が2004年に制定された時点では、支払われたお詫び金としては、1,000円の商品券が多かった。ローソンでは、自社の商品券であり、一般の金券に比べ自社の経営に与える影響は小さかった。一方、2004年に起きたソフトバンク BB の個人情報漏えい事件では、漏えいの規模が大きく、マスコミなどの報道もさかんに行われた結果として、500円の商品券となった。この事件以降、お詫び金の額が500円で、金券となった。ただし、三菱UFJ銀行のケースでは、内部犯行による漏えい事件であり、故意によるもので悪質と見なされたことから、10,000円となり、事件の大きさや漏れた情報による重大性なども考慮したお詫び金が支払われるようになった。2014年のベネッセの事件までは、情報漏えい事件では、500円から1,000円のお詫び金が支払われるのが一般的であったと考えられる。

3. 2 ベネッセによる個人情報漏えい事件

最近の事例ではベネッセによる個人情報漏えい事件が注目を集めた[4][5][6]。ベネッセは個人情報流出後の対応として当初「金銭的謝罪は考えていない」としながら、その後「200億円の原資を準備し、お客様に謝罪する」と態度を変化させた。そして最終的な対応は被害者が「500円分の選べる電子マネーギフト」、「500円分の全国共通図書カード」、「ベネッセこども基金へのご寄付」の3つの選択肢から1つ選ぶという形になった。この事件では経済産業省からは是正勧告が出るという個人情報漏えい事件では異例の事態となった。流出件数については、はじめに「最大で約2070万件まで増える可能性あり」としていながら、その後、約2300万件となり、さらに増える可能性についても言及しており、最終的には3504万件（実態件数約2895件）にのぼる流出件数となった。またお詫び状に関しても外側から個人情報がみえていたことやお詫び金の金額、お詫び金の代わりに寄付などの対応から、「誠意が感じられない」、「子供の情報が漏えいしたのに500円で済まそうとしている」などといった様々な批判があった。

これらの批判などから多くの被害者が集団訴訟を起こし、過去の同種事例と比較しても重大だとして5万5千円の損害賠償請求をしている。

また、お詫び金に関して500円が多いのは2004年頃に個人情報漏えい相次いで起こったことにより業界への批判が高まり、その中でソフトバンクがお詫びとして500円の商品券を配布したのが始まりだと考えられる。

公表されたニュースをもとに調査したので、サービス停止時や緊急メンテナンスが起こった際、頻繁にポイントなどでお詫びをするオンラインゲーム業界をより詳しく調べていけばより多くの事例があると考えられる。

3. 3 海外の事例

2011年4月のプレイステーションネットワークにおける不正アクセスによる個人情報漏えい[7]では補償として特定コンテンツの無料配布などの対応をとった。

2013年3月のXbox Entertainment Awards 2013の公式サイトにて、一時的に投票者の個人情報が閲覧可能な状態となっていた事故[8]では、対象者にはお詫びとして1600マイクロソフトポイント（約2400円相当）が無料で配布された。

海外の場合、お詫びとして金券やポイントを配るといった対応ではなく、被害者に対してモニタリングサービスや1年間ほどのIDの保護や自社のサービスを無償で行うといった補償としての対応多く見られた。

これはアメリカの場合、集団訴訟制度があるためにお詫びというよりも補償という対応が多いのではないかと考えられる。

4. 1 個人情報の価値

個人情報に関する価値の1つの指標としてJNSAの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[1]で公開されている漏洩個人情報の価値を経済的損失・精神的苦痛それぞれ3つのレベルに分類し図に示したシンプルEP図というものがあり図3に示す。

経済的損失レベル	1	2	3
3	□口座番号・暗証番号、クレジットカード番号とカード有効期限、金融系WebサイトのログインアカウントIDとパスワード、決済機能付きのサイトの顧客登録情報(アカウントIDとメールアドレスを使用する場合も含む)	遺失書	前科前歴、犯罪歴、身元ブラックリスト
2	パスポート情報、購入記録、ISPのアカウントIDとパスワード(アカウントIDと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IDとパスワード(アカウントID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、印刷履歴証明書、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・年齢区分、所得、資産固定資産税など、建物、土地、預金、借入、生活保護に関する情報を含む、借入れ記録、購入履歴(スタンプやポイントは除く)、給付額、賞与額、前払金額、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、学級名、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、SPAアカウント名のみ、患者番号、受診科目・受診日、年齢番号、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)、心電図結果、性格診断結果、病歴、手術歴、妊娠歴、看護記録、その他身体検査記録、治療法(押印に係る記録除く含む)、レセプト情報(治療に係る金額)、身体障がい者手帳情報、DIN情報、身体障がい情報、知的障がい情報、認知、生体認証情報(静脈・声紋・虹彩・網膜・顔面像等)、スリープ・サイズ、人種、地方なまり、国籍、趣味、特技、嗜好、民族、賞状・交通違反切符など、職業に関する書類(含む)、学歴(求職に関する書類含む)、成績表(含む)、履歴書(含む)、試験科目(解題用紙など含む)、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)、血書情報、犯罪記録に関する情報、高齢者医療保険/介護保険の選付金額、プライバシー(恋愛)情報	加害状況、政治的見解、加害者組合、位階、思想、宗教、位階、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、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、性生活会の履歴、介護歴、プライバシー(不倫)情報(含む)
	1	2	3

図3. シンプル EP 図

これをもとに個人情報の価値を算出しているが、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りとしており、その補正を加えた漏えい情報の価値を求めるために「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」といった計算式を用いている。

しかし、漏えいした生年月日や電話番号といった個人情報別では区別しているが、同じ生年月日といった個人情報でも大人と子供といった背景別では区別されていない。ベネッセ事件では、過去のお詫び金の金額やこの計算式を考慮して「500円のお詫び金」が判断されたと考えられる。しかし、子供の生年月日を固定したものと考えた点や名簿屋に情報が漏えいしている点で、被害者の被害意識とすれ違った一因と考えられる。EP 図や被害金額の計算式も見直す必要があると考える。

4. 2 ユーザー側からみた個人情報の価値

IoT時代のセキュリティ、プライバシーに関する意識調査2015[9]によると個人情報の価値に関して、約6割の人が個人情報は自分を含め、人々の販促活動につながるため価値があると回答しており、半数の人が自分に関する個人情報は商品や通貨、日用品と同じように金銭的価値があると回答している。

また信頼できる会社がユーザーから個人情報を入手する際にユーザー側にいくら支払うべきかという質問では、同じ氏名でも自分自身の氏名より友人や家族の氏名の方が5倍以上高い金額を回答している。このことから同じ情報(氏名)でも、その自分や知人といった属性などによってユーザー側の認識が違うといえる。

5. 先行研究・調査まとめ

先行研究などから、一部の企業・組織でしかお詫び金に関する規定がなく、大部分の企業・組織ではお詫び金に関する規定がなかった。

日本には、他人にものを頼む場合や挨拶代わりに粗品を送る日本固有の文化的風習がある。この観点からも詫び料やお詫び品といったお詫び金にあたる要求が一定数ある。櫻井の研究においてもお詫び目的の「金券」はプラスの効用が見られていることからお詫び金に関する規定を定め、効果的に利用することが望まれる。

しかしベネッセの情報漏えい事件では色々な要因があるが、お詫び金を配布するタイミングや金額、被害にあった顧客の被害意識の取り違えなどによってマイナスに働いて集団訴訟に発展したと考える。さらに名簿屋に漏えいした個人情報が流れていて、今後も被害の可能性があることから、他の事例のように被害の期間や範囲が限定的ではない。これは漏えいした情報内容が名簿屋に流れていて、子供の個人情報という今後長い間被害にあう可能性が高いという特殊性を十分に考慮しなかったためのすれ違いによる。

以上のことから、企業が今後事後対応としてお詫び金を払うとしても、過去の事例から500円の金券を安易に配布

するのではなく、漏えいした情報の再流通やどのような場面で利用されるかなどについても考慮する必要がある。これらを加味して、お詫び金の金額や方法、手順を考える必要があるといえる。また個人情報の価値に関しても子供などの特殊性や年齢などの背景によっては同じ個人情報でも漏えいした場合のお詫び金の金額に差をつけることも考える必要がある。

6. アンケート調査 (暫定)

6. 1 アンケートの概要

原田研究室では2015年8月に「情報セキュリティ調査」アンケートを郵送にて実施した。対象は、日本国内のプライバシーマーク取得組織、ISMS認証組織、BCMS認証取得組織、官公庁、教育機関などから、4500組織である。本稿では、先着50件のデータについて分析した。今後、全データの集計結果によっては分析結果が変わる可能性はある。

6. 2 仮説

ベネッセの個人情報漏えい事故では過去のお詫び金配布事例から言えば500円相当のお詫び金にあたるといえる。

しかし、今回の事故では様々な要因があるが、金額などに多くの批判があった。今回の事故から、今後は過去の事例をただ参考にするのではなく、お詫び金を払う際には、子供や家族の情報といった属性を考慮する必要が出てきたと考えられる。そこで以下の仮説をたて、アンケート調査を行った。

仮説1. 2012年度よりも2015年度調査ではお詫び金に関する規定を定めている企業が増えているのではないか。

6. 3 アンケート結果

お詫び金の基準を定めているかどうかの調査結果を図4に示す。

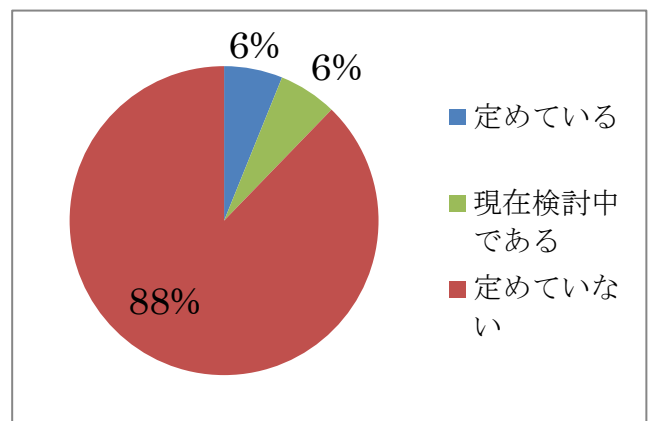


図4. お詫び金の基準の策定状況 (2015年度 n=50)

結果、定めている企業が6%、検討中の企業が6%、定めていない企業が88%であった。また定めていると回答した企業の中に個人情報に種類ごとに金額を定めている企業はいなかった。

また、ベネッセの個人情報漏洩事故を受けてお詫び金に関する規定の改定や作成に影響があったかどうか調査した結果を図5に示す。

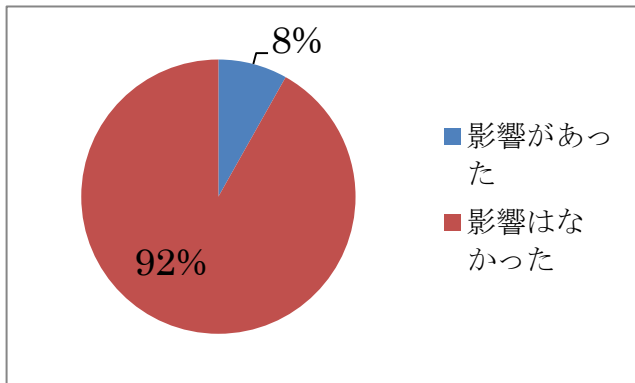


図5. ベネッセにおける個人情報漏えい事故による、お詫び金の規定の改定、策定に対する影響の有無(n=50)

8%の企業が影響があったと回答した。

次に、個人情報を漏洩してしまった場合、どのような対応を考えているかを複数回答で調査した結果を図6に示す。

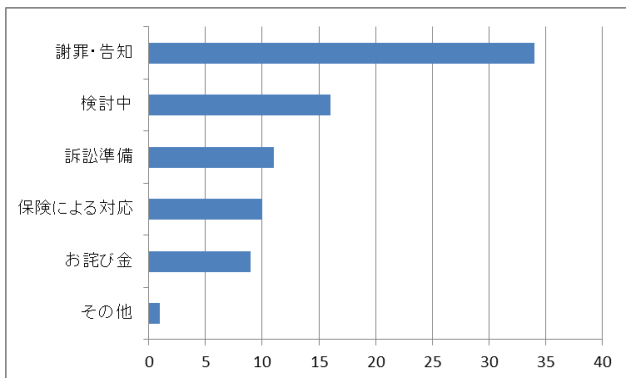


図6. 個人情報漏えい時に考えている対応 (複数回答) (n=50)

多い順から謝罪・告知、検討中、訴訟に対する準備、保険による対応、お詫び金での対応であった。

また、個人情報が漏えいしてしまった場合の想定でのお詫び金配布金額を子供とそうでない場合で回答してもらい平均値を図7に示す。

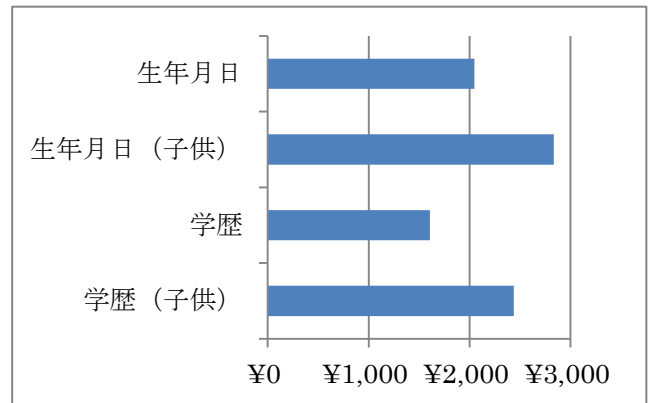


図7. 想定でのお詫び金の平均配布金額

結果、生年月日が約2048円、生年月日(子供)が約2835円、学歴が約1607円、学歴(子供)が約2439円という結果であった。

7. 考察

仮説ではベネッセにおける事故前の2012年度調査より事故後である2015年の調査では基準を策定している企業が増えていると仮説を立てたが、図4からお詫び金に関する基準を定めている企業が2012年度から増えているとは言えない結果であった。

しかし図4で6%の企業がお詫び金の基準の策定について検討中と回答していることから、ベネッセにおける集団訴訟結果によっては増えていくことは考えられる。

そして図6でも約30%の企業で漏えい時に考えている対応では検討中と回答しており、今回のベネッセにおける集団訴訟の結果次第では何らかの対応策を考えている企業が多いのではないかと考える。また保険による対応とお詫び金での対応を考えている企業がほぼ同数いる回答結果になっており、お詫び金に関する規定を定めている企業が少ないのは、保険で対応しているためとも考えられる。

次に図7から想定でのお詫び金配布金額において、企業は子供の情報が漏えいした時の方が、高い金額を配布する結果になっており、過去のお詫び金配布事例で子供の情報で区別された例は見つからなかったが、今後はそういった事例が出てくると考えられる。

謝辞

本研究にご協力いただいた情報セキュリティ大学院大学の教授等関係者、原田研究室、アンケート調査にご協力いただいた企業・官公庁の皆様様に謹んで感謝の意を表す。

参考文献

- [1] 情報セキュリティインシデントに関する調査報告書
2013 2015年8月20日アクセス
http://www.jnsa.org/seminar/2014/0610/data/A4_incident.pdf
- [2] 菅原尚志・原田要之助 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―
- [3] 櫻井 直子 (2009) 情報セキュリティ価値の定量化に関する実証的研究- ネットワーク利用者の視点による -
- [4] ベネッセ、情報漏洩 3504 万件に補償は 500 円の金券 2015年8月20日アクセス
http://www.nikkei.com/article/DGXLASDZ10H6I_Q4A910C1000000/
- [5] ベネッセ個人情報流出被害者の会
<http://no-benesse.jp/> 2015年8月20日アクセス
- [6] ベネッセに対する集団訴訟ブログ ベネッセ個人情報漏えい被害対策弁護団
<http://vsbenesse.exblog.jp/>
2015年8月20日アクセス
- [7] ソニー「PSN」の情報漏えい―補償拡大を求める声の高まり
<http://japan.cnet.com/news/commentary/35002928/> 2015年8月20日アクセス
- [8] Xbox Awards の個人情報流出問題をマイクロソフトが謝罪、お詫びとして対象者に 1600MSP を配布
<http://www.gamespark.jp/article/2013/03/23/39726.html> 2015年8月20日アクセス
- [9] IoT時代のセキュリティ、プライバシーに関する意識調査 2015 2015年9月5日アクセス
<http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20150423011206.html>