個人情報漏えいインシデントを減らすためには

セキュリティ被害調査 WG
(株)NTTデータ　大谷　尚通

1. はじめに

2008年は、2007年と比較して、個人情報漏えいインシデント（以下、インシデントとする）の件数が大幅に増加し、1,373件（+509件）となった。これは、「教育・学習支援業」「金融・保険業」「サービス業」「運輸業」など、多くの業種において、全体的にインシデント件数が増加したことによる。図1のようにインシデント件数が過去最多にもかかわらず、漏えい人数は、723万人と個人情報保護法施行後では最も少なく、かつ、初めて減少に転じた。これは、漏えい人数が100万人を大きく超える大規模なインシデントが発生しなかったことが大きく影響している。詳細は、2009年7月に公開した「2008年情報セキュリティインシデントに関する調査報告書」をご覧いただきたい。

つまり2008年は、小規模なインシデントが多く発生し、公表された年である。

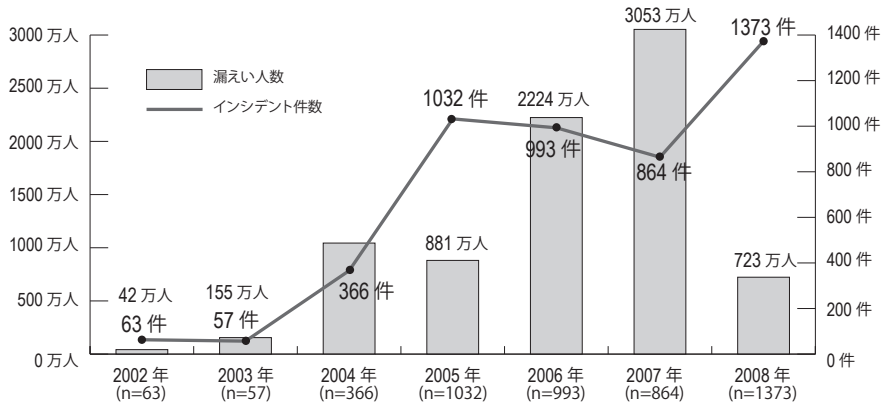

図 1：インシデント件数と漏えい人数（経年）

2. 小規模な個人情報漏えい件数

1件あたりの漏えい人数が100人未満の漏えい件数は、全体の約60%を占める。小規模なインシデントは公表されない場合もあるため、実際の件数と割合は、図 2よりも高いと予想される。一方、5000人以上の漏えい件数は、わずか6%である。

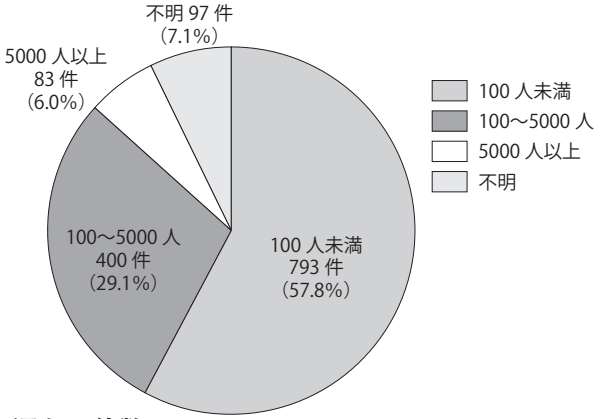

図 2：人数区分別の漏えい件数

業種別のインシデント件数の人数区分を図 3に示す。1件あたりの漏えい人数が100人以下の漏えい件数は、公務が469件中375件（80.0%）でもっとも多い。次いで、金融・保険業の159件中92件（57.9%）、教育・学習支援業の178件中72件（40.4%）である。公務は、100人以下のインシデント件数の占める割合も、他の業種と比べて最も高い。次に割合の高い電気・ガス・熱供給・水道業の66.7%（26件）との差も大きい。

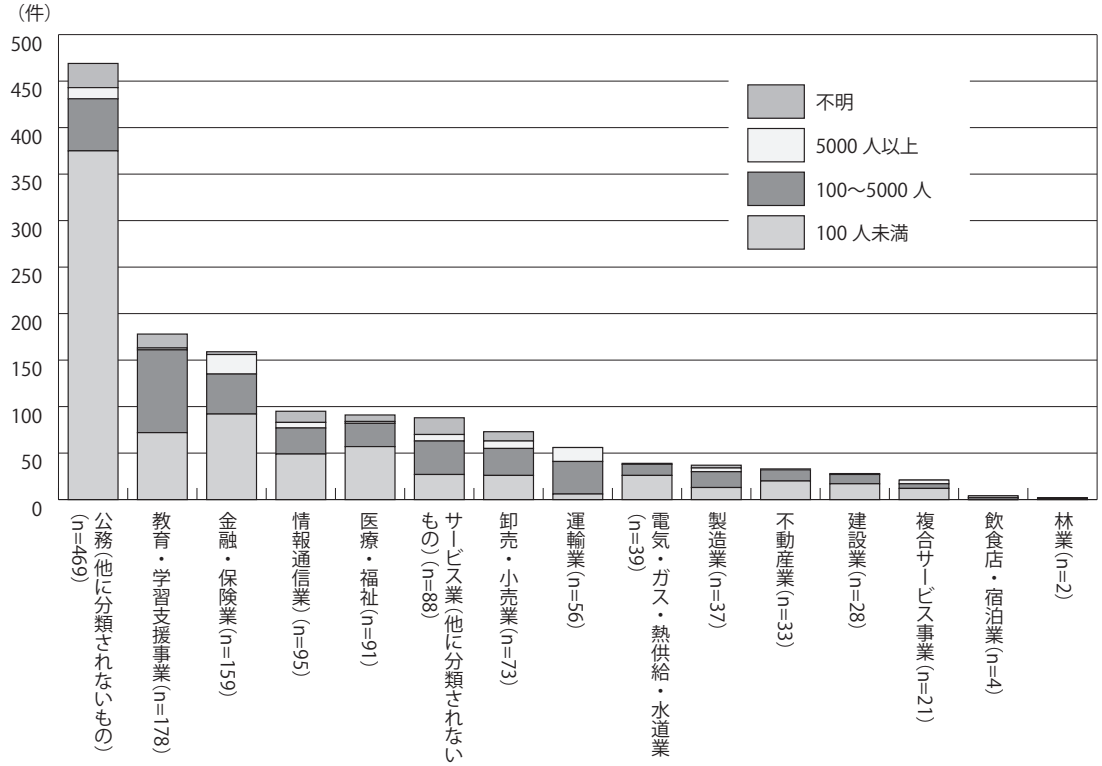

図 3：人数区分別の漏えい件数（業種別）

業種別によって、小規模なインシデントの発生確率に違いがあるのはなぜだろうか。各業種において、業種全体で扱う個人情報の総量、100人以下の個人情報を取り扱う業務を考察してみる。個人情報を取り扱う業務は、個人情報の授受や、持ち出す業務を想定した。これらの値を正確に見積もって比較することはできないため、それぞれの規模感を表現した。業種全体で扱う個人情報の量は、以下のように想定した。

- 公務：日本国民の人数に比例
- 金融・保険業：日本国民の人数に比例
- 電気・ガス・熱供給・水道業：世帯数
- 教育・学習支援業：就学者数

同様に、各業種において100人未満の個人情報を扱う通常業務の頻度を考察してみた。

- 公務：住民票の発行、税金、年金のお知らせなどの郵送、等
- 金融・保険業:窓口での振込手続き、口座開設手続き、等

- 電気・ガス・熱供給・水道業：検針、料金の通知、等
- 教育・学習支援業：テスト答案の保有、成績データの管理、等

業種全体で扱う個人情報の総量と100人未満の個人情報を扱う通常業務の頻度を総合的すると、公務と金融・保険業の個人情報の流量が最も多く、次いで電気・ガス・熱供給・水道業が多い。教育・学習支援業は、上位の2つのグループよりも少ない。公務と金融の個人情報の流量は同じぐらいであり、公務が、他の業種よりも飛び抜けて個人情報の流量が多いとは思えない。図3のように公務だけが小規模なインシデント件数、占める割合が多くなるには、別の理由がある。

過去5年間の調査結果によると、公務と金融・保険業は、常にインシデント件数の多い業種の1位と2位である。これらの業種には、個人情報保護に関する行政の指導が強く働いており、小規模のインシデントであっても公表することが多いため上位になっていると思われる。このように、小規模なインシデントを報告、公表する業種や組織には、偏りがあることが判明している。さらに、2008年の個人情報漏えいインシデントを分析したところ、ある人口の多い地方公共団体からのインシデントの公表件数が大幅に増加したことがわかった。特にこれまで報告されなかったような小規模なインシデントが、数多く報告されている。公務は、小規模なインシデントを報告、公表する体制、ルールが整備されていることが予想される。

3. 地方公共団体における情報漏えいインシデントの対応

各地方公共団体は、個人情報の取り扱いに関する条例を策定することになっている。総務省による各地方公共団体における情報セキュリティ対策の体制と規程整備に関する調査結果※を表 1に示す。

表 1：地方公共団体における情報セキュリティ対策の実施状況

団体区分別		団体数	情報セキュリティポリシーを策定		主要な情報資産について、情報セキュリティ対策実施手順を策定		情報セキュリティ研修を職員に対して実施	
都道府県		47	47	100.0%	42	89.4%	46	97.9%
指定都市		18	18	100.0%	17	94.4%	18	100.0%
市/特別区	50万人以上	15	15	100.0%	14	93.3%	15	100.0%
	10~50万人未満	251	251	100.0%	171	68.1%	240	95.6%
	5~10万人未満	267	266	99.6%	133	49.8%	242	90.6%
	5万人未満	255	248	97.3%	111	43.5%	185	72.5%
	小計	788	780	99.0%	429	54.4%	682	86.5%
町村	5万人以上	4	4	100.0%	1	25.0%	3	75.0%
	1~5万人未満	502	491	97.8%	183	36.5%	324	64.5%
	5千~1万人未満	254	241	94.9%	83	32.7%	118	46.5%
	5千人未満	234	213	91.0%	55	23.5%	89	38.0%
	小計	994	949	95.5%	322	32.4%	534	53.7%
合　計		1,847	1,794	97.1%	810	43.9%	1,280	69.3%

※「地方公共団体における行政情報化の推進状況調査結果　平成 21 年度資料編」 総務省
http://www.soumu.go.jp/denshijiti/chousah21.html

「情報セキュリティポリシーを策定」は、都道府県、指定都市、人口10万人以上の市、人口5万人以上の町村において、100%対応している。全体でも約97%の地方公共団体が対応できている。一方、「主要な情報資産について、情報セキュリティ対策実施手順を策定」と「情報セキュリティ研修を職員に対して実施」は、各地方公共団体の大きさによる実施率の差が大きい。「情報セキュリティ研修を職員に対して実施」は、都道府県、指定都市、人口10万人以上の市の約96%以上が対応できているのに対し、町村は平均50%程度である。「主要な情報資産について、情報セキュリティ対策実施手順を策定」も、都道府県、指定都市、人口50万人以上の市の93%以上が対応できているが、それ以外の地方公共団体となると実施率が大きく下がり、人口10〜50万人未満の市が約70%、町村になると約40%以下である。

前記の小規模なインシデントの公表件数が大幅に増加したある地方公共団体も、人口が多い都市であったことから、表1の3つの施策が実施されていたと思われる。このような情報セキュリティポリシーとそれに対応した実施手順の策定、さらにそれらを徹底させるための情報セキュリティ研修が実施されたことによって、それらの施策の実施率の高い地方公共団体内部には、情報セキュリティ関連知識を備えた人材が増え、そういった人材を中心に、全体としてセキュリティレベルの底上げが行われたのではないかと考えられる。その結果として、従来は業務現場から上がってこなかったような小さなインシデントなども、全て報告が上がるようになり、その地方公共団体における報告件数が大きく増えたと思われる。最終的に、それらの報告されたインシデントがすべて公表されたため、2008年の調査結果において件数が大幅増となった。

次に、個人情報漏えいインシデントの公表について考えてみる。

4. 個人情報漏えいインシデントの周知と公表

インシデントが発生し、個人や組織、社会に損害や迷惑などを及ぼす場合、またはその恐れがある場合、インシデントの発生元の組織は、なるべく早く対象者へインシデントに関する情報を周知しなければならない。個人情報漏えいインシデントの場合は、当該個人へ個人情報漏えいによるリスクが高まっていることを知らせて、個人情報の悪用による二次被害を防ぐことが必要になる。周知すべき項目は、いくつかある。以下に示すようにその目的も合わせて記述した。

表 2：周知の目的と項目

	目　的	項　目	例) *
1	被害拡大の阻止	対応策の周知	・想定されるリスク (※) ・悪用の手口 (※) ・対応方法 ・問合せ先
2	誤認の防止、不安の除去	経緯・状況説明	・個人情報漏えいの概要 ・漏えいしたと推察される期間 ・漏えいしたと推察される件数 ・漏えいしたと推察される個人情報の種類 (属性など)
3	謝罪	罪や過ちの謝罪	・謝罪 (※) ・補償内容 (※)
4	信用回復	対応体制 再発防止策 改善の報告	・漏えいの原因 ・調査報告 (※) ・再発防止策の提示 (※) ・改善状況 (※)

(※:本稿において追加した例)

＊参考：情報セキュリティ早期警戒パートナーシップガイドライン , 独立行政法人 情報処理推進機構
http://www.ipa.go.jp/security/ciadr/partnership_guide.html,p.16 Ⅴ．ウェブアプリケーションに係る脆弱性関連情報取扱

周知方法は、対象者に直接連絡する手段があるかどうかに依存する。郵送、電子メール、電話/FAXなど、対象者に直接かつ確実に連絡する手段があれば、それを使用すればよい。対象者に直接連絡する手段がない場合や対象者全員の連絡に時間が掛かる場合は、広告などを用いた周知、メディアへの公表を使用することになる。ただし、個人情報漏えいインシデントを公表する場合は、公表によって二次被害が拡大する恐れを考慮しなければならない。WinnyなどのP2Pファイル交換ネットワーク上へ個人情報が漏えいした場合は、公表によって漏えいした情報を興味半分に取得され、漏えいの範囲が拡大する恐れがある。漏えいした個人情報の悪用による二次被害のリスクと、個人情報の漏えいの範囲が拡大するリスクを見極めて、公表する内容やタイミングを決定することが求められる。可能ならば、P2Pファイル交換ネットワーク上の個人情報を消去してから、公表を行えば、リスクを低く抑えることができる。

前記の地方公共団体では、小規模なインシデントを積極的に公表していた。小規模なインシデントは、対象者に対する周知を問題なくおこなえるため、被害拡大の阻止を目的とした公表は不要である。前記の地方公共団体は、社会的立場や説明責任を重視して、公表を積極的に行っていたと思われる。

以上から、インシデントについて周知、公表する場合は、各組織において以下のような判断を行って欲しい。

- 周知、公表する目的は?(周知、謝罪)
- 周知、公表する相手(被害者、社会)は適切か?
- 周知、公表する手段は適切か?
- 公表する範囲(組織内/外)は適切か?
- 公表による二次被害の考慮は?

セキュリティ被害調査WGは、これまで多くのインシデントの公表の記事を調査してきた。全般的に経過報告、謝罪が多く、残念なことに注意すべきことや対応方法などの被害者のケアを記述したものは少ない。また、原因を究明して発表するとしながら、追加報告を行っていない組織も多い。インシデントの発生原因、被害状況などの情報は、公表するだけでなく、上手く活用すれば対策に大きく役立つ可能性がある。

次に、組織内でのインシデントの報告とインシデント情報の共有による効果について述べる。

5. インシデント報告による対策効果

■インシデント報告による対策効果

セキュリティ対策がある程度進んでいる現在の状況において、インシデントがなかなか無くならない理由を考えてみる。これまでの個人情報漏えいインシデントの調査結果から、セキュリティを保つための対策には、ルールや作業手順などの必ず人間が介在する部分が存在するため、ケアレスミスによって、ある程度、漏えいインシデントが発生してしまうことがわかっている。つまり、人間が介在する限り、インシデントは無くならないと思われる。このような人間の行為に基づくインシデントの確率的な考え方に「ハインリッヒの法則」がある。

ハインリッヒの法則は、米国の技師ハインリッヒ氏(H. W. Heinrich)が、労働災害の発生確率の研究から導いた経験法則であり、「1:29:300の法則」や「ヒヤリ・ハットの法則」とも呼ばれている。図 4に示すような海に浮かぶ氷山に例えられ、1件の重大な事故の発生の陰には29件の軽微な事故があり、さらに300件の事故未然のヒヤリとした経験が隠れているという法則である。海上に氷山として見える重大な事故と軽微な事故に

対して、海面下の見えない部分にはその10倍もの事故の兆候が存在している。

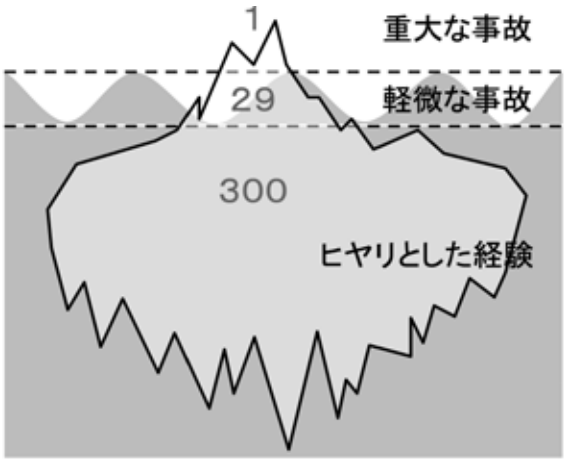

図 4：ハインリッヒの法則のイメージ

個人情報漏えいインシデントにハインリッヒの法則を当てはめてみると、1件の個人情報漏えいインシデント、29件の情報漏えいを伴わない紛失などのインシデント、300件の報告までに至らないちょっとした失敗やヒヤリとした体験が当てはまる。そして、この300件のヒヤリハットな事象は、重大な事故や軽微な事故の兆候といわれる。セキュリティ被害調査WGの調査からも、複数の小さなミスや無許可で機密情報を持ち出すなどのちょっとした故意の不正行為が重なって、個人情報漏えいインシデントの発生につながっていることがわかっている。このヒヤリハットな事象を適切に処置できれば、事故を未然に防止できたり、事故の影響を最小限にとどめたりすることができる。また、複数の原因が連なってインシデントが発生する場合は、より早い段階のちょっとした失敗やヒヤリとした体験レベルの原因に対処するほうが、対応しやすく、効果的な対策が行える。

これまで、情報セキュリティインシデント対策といえば、図 5の超高リスク、高リスク（影響度=3、発生確率=2）、中リスク（影響度=3、発生確率=1）、高リスク（影響度=2、発生確率=3）といった影響度の大きいリスクが優先的に取り組まれている。これからは、発生確率が高く、影響が小さいリスクについても、対策を行うことを推奨する。発生確率が高いヒヤリハットな事象への対応は、多くの現場の実務者に経験として蓄積されやすい。このように、インシデント以前のヒヤリハットな事象の対策は、一見、遠回りの対策に感じられるが、重大なインシデント対策の一環であり、効果がある。実際に医療現場では、このヒヤリハットのデータを収集し、データベースで分析、情報共有することによって、医療事故が削減されている。

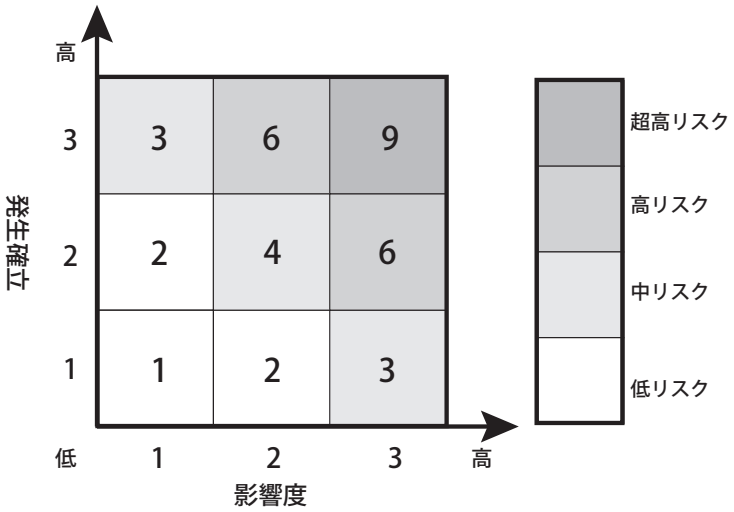

図５：リスク発生確率・影響度マトリクス

このように当WGは、医療分野や保険分野などで効果が確認されているハインリッヒの法則を情報セキュリティ分野に適用した対策方法を提案しようと考えている。これによって、これまで報告の対象としていなかったヒヤリハットな事象を収集し、その原因や状況などの情報を共有することによって、現在の対策方法では対処できていない問題を解決できる可能性がある。そのためには、報告すべきヒヤリハットな事象の基準や収集すべきインシデントの情報、インシデントの公表指針などを提示する必要もあると考えている。現在、各組織における重大な事故、軽微な事故、ヒヤリハットな事象の集計状況とその割合を把握するために、JNSA会員企業のインシデントの発生件数に関する調査と分析を開始している。今後、上記の仮説を調査や検証を通して確認していく予定である。