2002年度情報セキュリティ被害調査報告について

株式会社損保ジャパン・リスクマネジメント
山本　匡
株式会社NTTデータ
大谷　尚通

情報セキュリティ被害調査ワーキンググループでは、前年に引き続き、情報セキュリティインシデントの被害調査をプロジェクトとして行った。
今年は、昨年の調査及び被害モデルのみならず、情報漏洩事故による被害の影響についての考察を加え、２部構成とした。各部の概要は「2.目的」の通りである。(なお、本報告では、紙面の構成上、第一および二部をまとめて報告する。)

1. 目　的

サイバーテロや重要インフラセキュリティに対する関心は、益々高まり、今まで以上に重要インフラである情報システムにおけるセキュリティインシデントに関する過去の事例や現状についても関心が高まっている。

しかし、これらセキュリティインシデントに関する具体的な事例や被害額についてのまとまった情報は殆ど無い。インシデントの性質上、一般に公表されることが稀であるということに加え、そもそも被害の定義が曖昧であることも、情報が得られない大きな原因となっている。

また、同様なことは、対策の面でも生じており、対策定義の曖昧さにより、対策コストの情報は、まだ不足している。

そこで＜第１部＞では、昨年同様にアンケートやヒアリングによって、国内におけるサイバーテロや重要インフラセキュリティインシデントに関する現状を把握するための情報収集を行った。この情報から得られる結果を基に、昨年度提案したセキュリティインシデントの被害額や情報セキュリティの対策投資額を推計するモデルに対し、情報セキュリティマネジメントにおける「リスクの大きさ(被害規模)」と「対策規模」の把握と効果の計測、効率的なマネジメントの実現において、更に精緻なモデルとするため検討を加え、2002年度モデルとして提案する。

また、＜第２部＞では、社会的な反響があり、関連者も非常に多数に上る事故種類の一つとして、今回「情報漏洩」を取り上げた。この「情報漏洩事故」は、どの企業にも共通の脅威であり、個人情報保護法案の進捗を踏まえると、経営者としては当然認知すべきリスクの一つである。

本ワーキンググループでは、「情報漏洩事故」における「損害賠償の可能性」や「株価への影響」について、今後の議論の題材になることや、企業経営者が考えるべき情報セキュリティのリスク量の把握や行うべき投資判断の一助となることを目的として、検討および提案を行った。

1 第1部の概要

情報セキュリティのインシデントに関する調査および被害算出モデルについて、下記の内容をまとめている。

(1)「情報セキュリティインシデントに係る被害額・対策の投資費用に関する調査」

アンケートやヒアリングにて調査すべき項目を設定し、実際の企業においてインシデント発生や発生で要した費用(被害額)を調査した。

また、情報セキュリティインシデントの対策として実施されている取り組みへの投資額についても調査した。

(2)「被害額算出モデルの提案」

前年作成した情報セキュリティインシデントに関する被害額の算出モデルについて、更なる検討を加えたモデルを作成した。

具体的には、システム対応者の労務費用だけでなく、損害賠償に要した費用、復旧等に要した人件費、ハードウェア等物理的被害、イメージダウンによる被害、業務の停止による逸失利益などを想定し、被害額を算出するモデルの再検討と提案を行った。

(3)「情報セキュリティインシデント対策の標準モデルと対策費用」

前年調査との対比を交えた現時点で考えられる被害抑制のための標準的なモデルや望まれる対策レベルや予算規模などの提案を行った。

2 第2部について

情報漏洩による被害想定と考察について、当ワーキンググループの一案として、下記内容をまとめている。

(1)「情報漏洩による損害賠償被害額の想定」
2002年に発生した、情報漏洩事件について調査を実施し、そのインシデント内容を分析した。本分析結果を元に、当ワーキンググループとして、個人情報の価値およびその情報が漏洩した際における賠償金額等について、いくつかの仮定に基づいて被害額を算出した。
(2)「情報漏洩による企業価値への影響(株価面での考察)」
情報漏洩による企業価値低下の一端を探るため、2002年に情報漏洩事件を生じた企業について、情報漏洩の事故発生と当該企業の株価の動きについて、どの様な関係があるのかを調査し、本結果を元に、当ワーキンググループとして影響額を算出した。

2. 調査の概要 (以降、第1部について記述)

1 調査対象
・セキュリティ被害調査WGメンバーにて調査を依頼し、了解頂いた日本のインフラや基幹産業を構成する企業や組織。
・JNSAメンバー企業を中心とするIT関連企業。(一部に非IT企業含む)

2 調査方法
・対象企業に対して、アンケート及びヒアリングにより調査。
・アンケートは、昨年度の調査用紙をより簡便かつ詳細な回答ができるように大幅に修正したアンケート用紙を使用。
・JNSAメンバーへのアンケートは、JNSA事務局長の依頼文章と共に送付し、記入後、事務局へ返送、集計を行った。
・JNSAメンバー以外へのアンケートは、ヒヤリング担当者より先方へ個別依頼にて収集。

3 調査の結果
3.1 ヒヤリング調査の結果
(詳細は報告書参照)
3.2 アンケート調査の結果(集計表)
(詳細は報告書参照)
3.3 アンケート回収率とヒアリング引受率
アンケートの回答率37%(昨年比▲6%)であるが、回答件数は12件増加している。ヒアリング承諾18件、承諾率50%程度は、ほぼ昨年同レベルである。
3.4 アンケート拒否の主な理由
自社の情報セキュリティに対する取り組み方の詳細を答えることがポリシーに反する場合や、セキュリティ内容の回答に対する抵抗があげられる。

4 調査結果の分析と特徴
今回の調査内容について、情報セキュリティに関連が大きい部分を中心に分析を行うとともに、昨年の調査結果との比較も行った。
4.1 本年調査の調査結果と考察
詳細は報告書参照。概要は下記の通り。
・業種:JNSA会員企業中心であり、情報系が多い。
・対策状況:基本対策はほとんど実施済み。
4.2 前年度調査結果と今年度調査結果の比較
詳細は報告書参照。概要は以下の通り。
・規定の制定が10%増加。
・取引契約における対策の強化が増加。
・パッチ適用の増加。
・教育関連の予算増加。
・ウイルスチェックは、95%以上普及。

5 被害状況の概要
前年2001年度の被害報告は調査対象55件中33件(61%)あったが、本年2002年度は同66件中11件(17%)と前年の約1/4に大きく減少した。また、被害範囲も低く留まり、被害金額は12万円程度と低い。
一定水準のセキュリティ対策は実施されているため、被害の拡大をもたらすのは外部要因ではなく、故障など不可抗力的なものや運用手順上の問題に起因する場合に限定された結果となった。

6 調査結果の分析と特徴(総括)
今回のアンケートによると各社のセキュリティ対策については、ファイアウォールやコンピュータウイルス対策

は約100%が配備し、侵入検知システム（IDS）も43.9%が導入しているという結果となった。また、パッチの適用も100%が実施している。

ファイアウォール、ウイルスチェック、IDSなどの導入により、不正侵入・コンピュータウイルスへの技術的対策は定着してきたが、昨今問題になっている情報漏洩については設定ミスや関係者による不正といった人的要素が高く、技術的対策よりも管理・運用面の対策が求められる傾向にある。

運用面については、ポリシー等規定を設定している企業は87.9%になり、連絡体制の整備、教育の実施も高い比率で実施している。このように、技術面・運用面の整備が進んだことが今回の調査で被害額が低く抑えられる結果に結びついたと考えられる。

しかし反面、被害を受けたと回答した企業も同様に技術的対策やポリシーの策定は実施しており、教育の徹底やチェック機能の強化に再考の余地があることを明らかにした。利便性とのバランスを考慮しながらも、罰則規定など強制力を伴う運用ルールや管理体制の強化が企業にとって今後の課題となるだろう。

予算面に関しては、65.2%の企業が情報セキュリティに割り当てる予算を情報システム関連予算の一部として計上しており、また、売上高に占めるセキュリティ予算の割合も非常に低く、企業活動の中でセキュリティ対策が優先順位の低い位置にあることを示唆している。

セキュリティ対策は効果が見えにくいというのも予算が確保できない理由のひとつと考えられるが、今後のアンケートおよびヒアリング内容については、導入しているセキュリティ技術がインシデント発生率にどのような影響を与えているのか、また、連絡体制などの対策が被害発生後の対応にどれだけ効果を発揮しているのかを、定量的にまたコスト的に把握するような質問項目を検討していく必要があるだろう。

3. 情報セキュリティインシデント対策の標準モデルと対策費用

1 被害発生を抑止している情報セキュリティインシデント対策の状況

本年度の「情報セキュリティインシデントが発生した企業のグループ」と「被害にあわなかった企業のグループ」について、「情報セキュリティを確保するために導入しているシステム」項目のアンケート結果をもとに対策などの差異を把握するために分析を行った。

しかしながら、ファイアウォールやウイルスチェックソフトなどのセキュリティ対策システムの導入比率との相関関係は、残念ながら特に見出せなかった。

ただし、情報セキュリティインシデント被害を受けた後に、すぐにシステム的な対策を実施したことも考えられるため一概に無関係とは結論付けられない。

2 抑止モデルの情報セキュリティ関連予算の実際

本年度の調査で、情報セキュリティインシデントが「発生した企業」と「発生しなかった企業」を二つのグループに分けて、その中で「情報セキュリティ関連予算」について、アンケート回答のある企業のみを取り出し、傾向を分析したところ、インシデント被害の「発生した企業」と「発生しなかった企業」の各グループの従業員数とセキュリティ予算を合計して「一人あたりのセキュリティ予算」を比較すると、「被害にあわなかったグループ」の一人あたりの情報セキュリティ予算が15,991円に対し「被害にあったグループ」の予算は5,327円と3倍の差が出た。

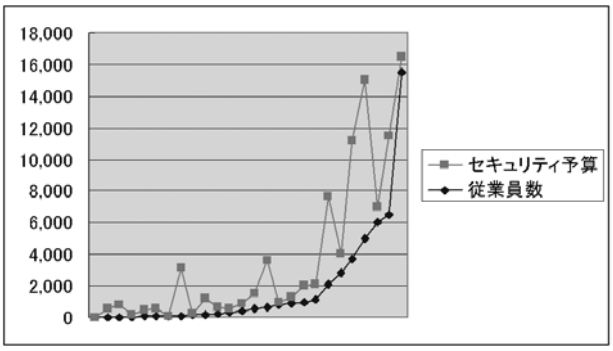
「情報セキュリティ予算」は、企業規模が大きくなれば一人あたりの金額は少ない傾向があり、情報セキュリティ予算の定義が明確ではない点を考慮すると、今回表れた「3倍の差」を単純に判断できないが、来年度以降の調査においても継続的に傾向を分析していきたい結果となった。

3 望まれる対策レベルと予算規模の提案

ハード面での対策はほぼ完了している企業も多かった。しかし、運用面を要因とする事故は多く、人的部分の教育までが、被害拡大を防止するための対策に含むべきとの結論となった。

対策レベル		具体例
対策レベル１	技術的対策	アンチウイルスソフト
		メール監視ソフト
		ファイアウォール
		IDS
		認証デバイス
対策レベル２	運用上対策	入退室管理
		セキュリティ管理責任者の任命
		情報セキュリティに関する規程作成
		セキュリティ事故対応マニュアル
対策レベル３（推奨レベル）	情報セキュリティ教育・啓発	コンピュータウィルス教育
		パスワード管理教育
		機密情報保護教育
対策レベル４	セキュリティ監査・第三者認証	ISMS ・ BS7799
		Ｐマーク

今回のアンケートでは、情報システム予算における情報セキュリティ関連予算の割合は、最大65%（従業員数140名）から最小0.1%（従業員数15,470名）まで多岐にわたり、平均で14.5%になった。



4. 2002年度情報セキュリティインシデント被害額算出モデルに関する検討

昨年度モデルをもとに、今年度の情報セキュリティインシデントに関する被害額の算出モデルを作成した。

昨年との変更点は、営業継続費用や喪失情報資産、機会損失などの追加や文言の修正を中心としており、詳細は報告書を参照願いたい。

また、これらの項目をアンケートの調査票としてまとめており、今後の被害調査時の記入表として活用いただければと考える。

D－1事故状況

1	被害コード→			
	＜事故状況＞			
2	発生日時	年　月　日（　：　）		
3	被害システムについて	事故時の対策について		
4	被害システムの種類について（該当システムの右欄に○をお付け下さい。）			
	(1) インターネット（DMZを含む）		(4) 社内専用ネットワーク	
	(2) イントラネット		(5) E C (B to B)	
	(3) エクストラネット		(6) E C (B to C)	
5	停止時間			時間
6	影響を受けた従業員の人数			人
7	システム停止時の業務処理量の低下割合			%
8	システムの年間売り上げ（EC関連の場合）			円
9	システムの年間収益（EC関連の場合）			円
10	被害を受けたサーバーの数			台
11	被害や影響を受けたクライアントの数			台
12	営業継続費（代替システム設置、人手の処理など）			円
	代替手段 ＜対応方法をご記入下さい＞			
13	逸失利益（システム売上×停止時間、確実な利益の逸失分等）			円
14	喪失した情報資産			円
15	機会損失（見込み利益で逸失分、売上増分の逸失など）			円
16	賠償・補償金額			円
17	その他関連出費（ブランド価値の維持費用について）			
	(1) お詫び広告			円
	(2) 謝罪出状			円
	(3) お詫び行脚			日人工
18	復旧作業量（システム部門他）			日人工
19	復旧費用（業者等への支払額）			円
20	貴社従業員の一日当たりの人件費			円／日

5. モデルおよび調査の今後の課題

1 モデルの課題

1.1 情報セキュリティインシデント被害額算出モデルの課題

モデルについては、昨年から課題となっている「IT感応度」については、今年度の見直しで十分な材料が無く、前回提案と特に大きな進歩を遂げることができなかった。今後は、企業毎に大きく異なるシステムの導入状況や業種などの情報で、ある程度数値化できる仕組みが本モデルの幅広い利用のために必要と考える。

また、対策の標準モデルについては、被害の有無を中心に考えたが、大きな差は無かった。しかし、事故の発生時期とアンケート時期のタイムラグにより、事故発生と対策の相関を掴むためには、対策の導入時期までも踏まえたものにする必要も考えられる。

2 調査の課題

2.1 アンケートの課題

今回の調査では、昨年の冗長なアンケート項目を見直し、十分な議論を重ねてポイントを絞ったアンケートの作成を行った。

しかしながら、今年のアンケートにおいても、記入のし易さなどの課題は残っている。

2.2 ヒアリングの課題

今回のヒアリング調査先も全般的に協力的であった。しかしながら、ヒアリング作業には人手が必要であり、件数増加を行う場合には、大きな課題となる。

6. 情報漏洩による損害賠償被害額の想定（以降、第2部について記述）

2002年は、個人情報保護法案と住民基本台帳ネットワーク(住基ネット)の運用開始に代表されるように、個人情報漏洩に注目された年(注：報告書の執筆時点では、個人情報保護法案は成立前だった)である。そこで本章では、不正アクセス等による情報漏洩事件について調査を実施し、そのインシデント内容を分析した。本分析結果を元に、個人情報の価値およびその情報の漏洩による賠償金額等について、いくつかの仮定のもとに被害額を算出した。

1 国内の情報漏洩

2002年1月から12月の間に発生した、ネットワーク経由での不正アクセス等による情報漏洩事件は、当ワーキンググループの調査結果によると、インターネット上で公に報道されたものだけでも計63件にものぼり、被害者の合計人数は、41万8,716人（1件平均 6,646人）であった。そのほとんどが、個人情報（メールアドレスのみの場合も含む）の漏洩である。

1.1 漏洩情報の分析

表1に情報漏洩事件の漏洩情報を分析した結果を示す。出現確率は、それぞれの漏洩情報の項目が、各調査対象の情報漏洩事件に含まれていた割合を示す。「氏名」は、情報漏洩事件うちの86％に含まれており、最も流出する可能性が高い情報である。さらに「氏名」、「住所」、「メールアドレス」、「電話番号」までの上位4つの情報が、他の情報に比べて高い確率で漏洩している。これは、これらの情報がホームページ上のアンケート、会員情報の記入などにおいて、ひとまとめの情報として頻繁に収集されているためと考えられる。

表1において、出現頻度が少ないため「その他」に分類した情報は、スリーサイズ、顔写真、趣味、年収、学歴、企業名、部署名、クレジットカード番号、プリペイドカード番号など、より個人の私的な情報が含まれている。これら情報は、漏洩する確率が高い上位4種類の情報よりも、より個人的な情報を含んでおり、情報漏洩による被害が大きく、深刻である。

表1：情報種別毎の漏洩件数と出現確率

漏洩情報名称	件数 (出現確率)
氏名	54件 (86%)
住所	38件 (60%)
メールアドレス	29件 (46%)
電話番号	28件 (44%)
生年月日	10件 (16%)
職業	6件 (10%)
性別	5件 (8%)
ユーザID	4件 (6%)
パスワード	2件 (3%)
アンケート関連	11件 (17%)
その他	21件 (33%)

2 情報漏洩元の分析

情報漏洩元の組織は、企業が約8割を占める。これは、企業が公共機関や教育機関に比べて、インターネットを利用したメーリングリストやアンケート募集、顧客への付加サービスを活発に行っているからであり、想定された結果である。今後は、e-Japan計画に代表されるように、政府、自治体がインターネット上におけるサービス提供を進めるため、情報漏洩事件に占める公共機関の割合が増加することが懸念される。図2に示す情報漏洩原因のうち、「設定ミス」、「誤操作」、「管理ミス」といった人為的なミスに由来した原因は、あわせて67％である。情報漏洩原因の「バグ・セキュリティホール」「不正アクセス」は、人為的なミスに直接関係していないが、最新のパッチを適用したり、Webシステムをより強固な構造へ変更したりすることにより、回避可能であったと思われる。つまり、人的要因に対する対処不足によって発生

した情報漏洩は、前述の2つの原因らを合わせて、全体の88%にもおよぶ。

情報の漏洩経路は、Web経由が84%、Email経由が13%であり、この2つで漏洩経路の大半を占める。どちらも、現在のインターネットの利用において、最も普及し、利用されているサービスである。

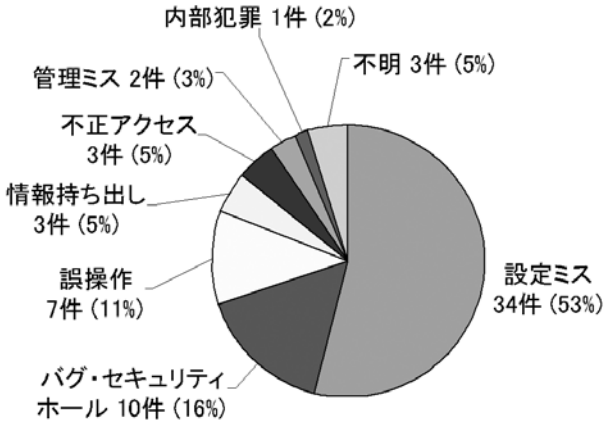


図2：情報漏洩原因

2.1 情報漏洩の原因

「Web経由」「Email経由」「FTP経由」が代表的な情報漏洩経路である。その中でも「設定ミス」が原因となって「Web経由」において情報漏洩に至るケースがもっとも多い。事件発生時の情報から、このWeb経由による情報漏洩の原因は、以下のような「設定ミス」、「バグ・セキュリティホール」とその他要因が、重なったことによって発生したと考えられる。

- web serverの設定ミス。ディレクトリ・リスト表示の許可設定ミスなど。
- ファイルパーミッションの設定ミス
- cgi等プログラムの設計ミス
- 推測しやすいファイル/ディレクトリ名の利用

（これらの複合要因の場合が多い）

Web(HTTP)は、CG/SSI、JavaScript/PHP、JPS/ASPなど双方向性サービスの手段として発達した。Webは、システム構築が容易で、便利なインタラクティブ・サービスを提供できる反面、システムの複雑化によりセキュリティホールを含みやすい。その結果、不正アクセスや設定ミスなどによる情報漏洩に結びつきやすいと想定される。

3 情報の種類と賠償額

3.1 宇治市住民基本台帳データ大量漏洩事件

漏洩した情報の価値をもとに、情報漏洩事件に対する賠償額が算出できると考える。そこで、宇治市住民基本台帳データ大量漏洩事件の控訴審判決より、漏洩した情報と損害賠償額との関係を参考とした。

表2：宇治市情報漏洩件数

情報名	漏洩件数
住民記録	18万5800件
外国人登録関係	3297件
法人関係	2万8520件
合計	21万7617件

・賠償額

被害者（住民）らに対し、慰謝料として1人当たり1万円、弁護士費用は、被害者（住民）1人当たり5000円。よって、1人当たりの賠償額は、1万5000円。

参考文献：http://www.law.co.jp/cases/uji2.htm

宇治市住民基本台帳データ大量漏洩事件で漏洩した個人情報は、「氏名」、「住所」、「性別」、「生年月日」の一般的な個人情報に加え、「世帯主名」、「世帯主との続柄」といったプライバシー度の高い情報が含まれていたという特徴がある。これに加えて、個人情報の情報源は、宇治市(自治体)の管理する住民基本台帳であることから、情報として最も信頼性・正確性が高い。上記の内容と、事件発生後にデータ回収、市民に対する説明、防止策の実施などの真摯的な対応姿勢が見られたことなどを考慮した結果から、慰謝料として被害者(住民)1人当たり1万5000円が言い渡された。もし、情報漏洩件数の約22万件より約22万人が訴訟をおこした場合、損害賠償額の合計は、約33億円となる。

式1：宇治市裁判における損害賠償額

15,000円×217,617件=32億6,425万5,000円

3.2 情報漏洩事件における損害賠償額の算出式

個人情報漏洩事件における損害賠償の実例はまだ少なく、賠償金額の基準が明らかになるには、今後発生する訴訟判決の事例の積み重ねが必要である。しかしながら、多発している情報漏洩事故を考えると、賠償金額に対する何らかの指標や想定モデルが必要と考えられる。本ワーキンググループでは、前述の判例や弁護士先生の意見

などを考慮し、あくまでも今後の議論の題材とするため、式2の算出式を設定した。
算定対象の情報漏洩事件について、式2の各項目に当てはまるポイントを表3から選択し、評価ポイントを算出する。表4の対応表を用いて、評価ポイントから漏洩情報1件当たりのおおよその損害賠償額を算定する。

式2：情報漏洩元組織の損害賠償額の算出式

情報漏洩元組織の損害賠償額 (評価ポイント)
= 漏洩情報の内容に基づく慰謝料 →表3:①の和
× 個人情報提供の同意の有無 →表3:②から選択
× 情報提供者との関係 →表3:③から選択
× 情報漏洩元組織の社会的信頼度 →表3:④から選択
× 事件後の対応姿勢 →表3:⑤から選択

表3：評価ポイント表

算式項目	状況別ポイント
①被害者に対する慰謝料(複数選択可)	基本的な個人情報 = 100
	特徴的な個人情報(3種類以下) = 500
	特徴的な個人情報(それ以上) = 1000
	メールアドレスのみ = 10
	個人を特定するID,パスワード関係 = 300
②個人情報提供の同意の有無	同意有り = 2.0
	同意無し = 1.0
③情報提供者との関係	顧客 = 2.0
	アンケート、プレゼント応募者 = 1.0
④情報漏洩元組織の社会的信頼度	一般より高い = 1.5
	一般的 = 1.0
⑤事件後の対応姿勢	良い = 1.0
	普通 = 2.0
	悪い = 4.0

表4：評価ポイントと想定慰謝料の対応表

1件当たりの評価ポイント	想定慰謝料
1000ポイント未満	0～5,000円
1000～2000ポイント未満	～10,000円
2000～5000ポイント未満	～50,000円
5000ポイント以上	50,000円以上

4 情報漏洩による損害賠償被害額想定

2002年の情報漏洩事件一覧および算出式(式2)を用いて算出した損害賠償額を表5、表6(次ページ)に示す。

2002年の国内におけるインターネット上の情報漏洩による損害賠償額は、推定の結果、以下のようになった。

表5：2002年 情報漏洩 総損害賠償額(推定)

総損害賠償額(推定)：
151億4,270万円(418,716人)

1件当たりの平均損害賠償額(推定)：
2億4,036万円(1件平均：6,646人)

図6に算出式(式2)で求めた2002年情報漏洩事件の評価ポイントの分布を示す。情報漏洩事件全体に対して、漏洩情報が基本的な個人情報やメールアドレスのみの情報漏洩事件が多いため、1件当たりの想定慰謝料が5000円以下(評価ポイントが1000ポイント未満)の漏洩事件が、全体の約70%を占めた。宇治市裁判例の損害賠償額(3600ポイント相当)以上にあてはまる情報漏洩事件は、10件(16%)であった。いずれも特徴的な個人情報が漏洩した事件であった。

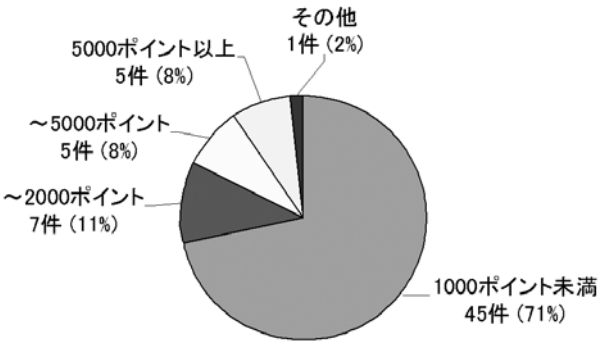


図6：情報漏洩事件の評価ポイント分布

情報漏洩の被害者全員が、損害賠償訴訟を起こすとは限らないが、損害賠償金額および、情報漏洩事件によるブランドイメージの低下等による売上への影響などを含めれば、情報漏洩による損害は、コンピュータウィルス等によるインシデント被害同様、その損害額は大きい。個人情報を収集・管理している場合は、情報漏洩によるリスクを平均損害賠償額(表5)ではなく、収集・管理している情報の内容と件数から算出式(式2)を用いて推定可能である。よって、アンケートや顧客サービスを実施するにあたり、その情報内容と件数から、情報漏洩リスクとして損害賠償額を算定し、セキュリティ投資額の参考とすることが可能である。

表6：2002年 情報漏洩事件一覧

企業・団体 No.	区分	漏洩情報 基本情報	特徴情報	メールアドレス	パスワード	評価ポイント	想定慰謝料	被害人数（人）	想定損害賠償総額（万円）
A	企業			○		200	5,000	1,900	950
B	企業	○				200	5,000	10,000	5,000
C	企業	○				600	5,000	1,388	694
D	企業	○				400	5,000	2,972	1,486
E	企業	○			○	800	5,000	68,471	34,236
F	企業	○				1,200	10,000	900	900
G	企業	○				400	5,000	22	11
H	企業	○				800	5,000	370	185
I	企業			○		100	5,000	1,462	731
J	企業			○		200	5,000	不明	不明
K	企業	○				1,200	10,000	4,300	4,300
L	企業	○				600	5,000	730	365
M	企業	○				200	5,000	4,000	2,000
N	企業	○				800	5,000	4,000	2,000
O	企業	○				400	5,000	10,000	5,000
P	企業	○				400	5,000	368	184
Q	企業	○				800	5,000	60	30
R	企業	○				400	5,000	1,303	652
S	企業	○			○	1,600	10,000	不明	不明
T	企業	○				600	5,000	800	400
U	企業	○				400	5,000	350	175
V	企業	○				400	5,000	1,000	500
W	教育機関	○				400	5,000	1,800	900
X	企業	○	◎			4,400	50,000	37,000	185,000
Y	企業	○				400	5,000	45,000	22,500
Z	企業	○				200	5,000	1,500	750
AA	企業	○				800	5,000	340	170
AB	企業	○				400	5,000	4,700	2,350
AC	その他	○				400	5,000	14,000	7,000
AD	企業	○				400	5,000	242	121
AE	企業	○				800	5,000	2,000	1,000
AF	企業	○				800	5,000	700	350
AG	企業	○				400	5,000	280	140
AH	公共機関	○				1,200	10,000	6,541	6,541
AI	企業	○				400	5,000	不明	不明
AJ	企業	○				400	5,000	1,100	550
AK	企業	○				800	5,000	5,000	2,500
AL	企業	○				1,600	10,000	1,600	1,600
AM	企業	○				400	5,000	1,200	600
AN	企業	○				400	5,000	2,093	1,047
AO	企業	○				400	5,000	不明	不明
AP	企業	○	◎			8,800	100,000	100,000	1,000,000
AQ	企業	○				1,600	10,000	不明	不明
AR	企業					算出不能	5,000	不明	不明
AS	企業	○				800	5,000	1,700	850
AT	教育機関	○	○			4,800	50,000	304	1,520
AU	企業	○	○		○	7,200	100,000	17,000	170,000
AV	公共機関			○		600	5,000	350	175
AW	企業	○				400	5,000	398	199
AX	企業	○				400	5,000	3,244	1,622
AY	企業	○			○	6,400	100,000	235	2,350
AZ	企業	○				200	5,000	1,200	600
BA	企業	○				400	5,000	50,000	25,000
BB	企業	○	○			2,400	50,000	400	2,000
BC	企業	○				400	5,000	335	168
BD	公共機関			○		600	5,000	59	30
BE	その他	○	○		○	7,200	100,000	不明	不明
BF	公共機関	○				1,200	10,000	483	483
BG	企業	○	○			7,200	100,000	65	650
BH	公共機関	○				600	5,000	154	77
BI	公共機関	○				600	5,000	190	95
BJ	教育機関	○	○			4,800	50,000	3,107	15,535
BK	企業				○	4,800	50,000	不明	不明
合計	63						合計	418,716	1,514,270
							平均	6,646	24,036

7. 情報漏洩事故による企業価値への影響(株価面での考察)

企業は、広報活動やＩＲ活動を行い企業価値の創造を行っている。これに対し、情報漏洩事故の発生は、信頼感の失墜および企業価値の低下を招く事故の一つと考えられる。

しかしながら、企業価値の指標が数多くあるのと同様に、情報漏洩などの不祥事によって、「どれくらい企業価値が低下したか？」を把握することは非常に難しい。

この点について、情報漏洩による企業価値低下の一端を垣間見るため、情報漏洩の事故発生と当該企業の株価の動きについて、どの様な関係があるのかを調査した。

1 情報漏洩事故発生後の株価変動の把握方法について

情報漏洩事故が発生した株式上場企業(もしくは密接な関連上場企業)について、事故発生後の短期及び中期における株価の動きを検討した。

株価の動きは、株式相場全体との連動性もあり、単純に金額を比較せず、株式相場全体＝日経平均とし、「事故発生の前日(前月末)」における「日経平均値と当該企業株価」との割合を基準とし、「事故発生後の日経平均と値と当該企業株価」割合の変化について、＜短期＞と＜中期＞に分けて調査した。

2 実例による株価変動の調査

2.1 短期影響額

企業毎に影響の有無や大小があるものの、「全社集計」においては、わずか8社の合計額で約150億円を示している。そして、企業によっては、1社のみで100億を超える数値も見られる。

8社の短期影響額の合計＝150億円

2.2 中期影響額

短期と比較し、より大きな影響が出ている。企業毎に影響の有無や大小があるものの、「全社集計」においては、わずか8社の合計額で約220億円を示している。そして、企業によっては、1社のみで250億を超える数値も見られる。

8社の中期影響額の合計＝220億円

3 企業における情報漏洩事故の株価への影響想定とその利用

企業経営者のリスク管理の一つとして、情報漏洩事故を想定し、自社株価への影響を考える場合への利用が考えられる。具体的には、下記の様な算式による影響額の試算が考えられる。

① 各社の「前日株価に対する差額割合」である「0～9％程度」数値の利用の場合

影響額＝自社株価×（0～9％）×発行株数

② 全社集計の「一株当たり差額」である「6～9円程度」の利用の場合

影響額＝6～9円×発行株数

これらの数値や算式を用い、情報漏洩事故の株価への影響額を事前想定することは、経営者における予防的なリスク管理として重要と考える。

今回の結果による影響の大きさを考えると、「情報セキュリティ対策費用」を単なる「システムコスト」ではなく、「企業価値の低下を防ぐためのＩＲ費用の一つ」として、積極的に捉え直すことも必要である。

4 算出基準値の課題

今回は、算出の基準値として「日経平均」を利用したが、株価の動きには業種毎のトレンドがあり、「日経平均」と「業種平均」が乖離する事は日常的に起こっている。

企業経営者の立場としては、同業他社との優劣も重要であり、今後は影響の把握をより精緻にするため、算出の基準値に「業種平均」を取り入れることも検討すべきである。

8. 最後に

今回2部構成で報告書を作成した。第2部においては、今後の各方面での議論の題材とするため、公表された情報漏洩事故について検討を加え、賠償による被害額の想定や企業価値の一端を示す株価への影響について、本ワーキンググループとして数値を示した。これは、メンバー内での討議・検討の結果であり、法律問題など我々の専門分野以外の要素が多く、現時点ではトライアル的な数値であることは否めない。

しかしながら、これらの被害の数値算出および算出課程を明示したことで、専門家を巻き込んだ今後の議論の題材を示すことができた。

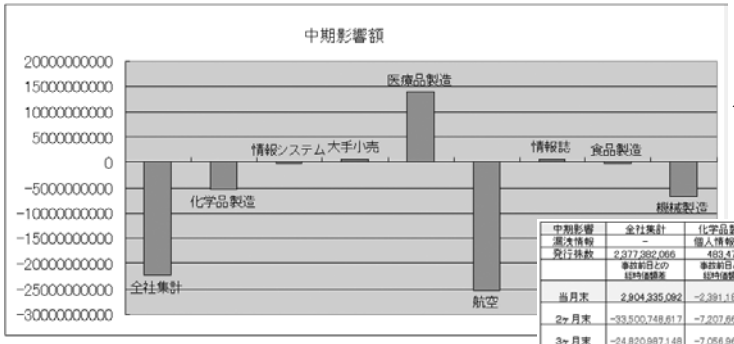
各異分野の専門家における共通の話題として取り上げられ、情報システムのリスクアセスメントで必要な「リスク量の把握」における把握モデルの構築が前進し、安全な情報化社会の形成に役立つことを期待したい。

報告掲載URL

http://www.jnsa.org/active1a.html

9. 2003年度の活動

誰もが興味のある被害について調査を行っているが、これらの事故情報収集は、容易ではない。しかしながら、本ワーキンググループならではの自由な発想による被害算出を、アンケートやヒアリングと共に今年度も引き続き行っていく予定である。



←中期影響額のグラフ

↓影響状況一覧

中期影響	全社集計	化学品製造	情報システム	大手小売	医療品製造	航空	情報誌	食品製造	機械製造
漏洩情報	－	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	個人情報漏洩	社内文書
発行株数	2,377,382,066	483,478,398	6,079,200	7,707,085	21,076,260	1,536,082,686	57,606,628	19,018,565	56,533,234
	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差	事故前日との総時価額差
当月末	2,904,335,092	-2,391,186,437	385,046,116	228,968,428	35,552,585,519	-30,089,363,254	992,471,666	361,720,517	-2,135,907,464
2ヶ月末	-33,500,748,617	-7,207,661,195	34,112,062	733,372,351	17,875,262,835	-40,587,241,253	383,916,817	-46,604,046	-4,685,906,189
3ヶ月末	-24,820,887,148	-7,056,943,701	53,223,297	1,000,553,392	568,067,968	-5,931,163,173	148,204,325	-163,011,541	-13,439,897,715
4ヶ月末	-33,659,566,285	-4,798,506,294	-925,642,464	540,858,539	1,623,993,216	-24,069,485,182	1,025,077,127	-1,072,899,642	-6,082,961,582
4ヶ月間累積	-89,076,966,959	-21,454,317,627	-353,260,990	2,503,752,711	55,619,909,539	-100,677,252,861	2,549,669,936	-920,794,712	-26,344,672,954
1ヶ月当り	-22,269,241,740	-5,363,579,407	-88,315,247	625,938,178	13,904,977,385	-25,169,313,215	637,417,484	-230,198,678	-6,586,168,239
一株当り差額	-9.4	-11.1	-14.5	81.2	65.9	-16.4	11.1	-12.1	-116.5
前月株価に対する金額割合	－	-4.40%	-1.29%	9.44%	3.97%	-4.50%	5.40%	-1.66%	-14.26%