



INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

2005 年 企業における 情報セキュリティ事象被害額調査

報告書

2006 年 11 月

ウイルス被害額算出モデル研究会
独立行政法人 情報処理推進機構

目 次

| | |
|--|----|
| 1. 検討の概要 | 1 |
| 1.1. 目的 | 1 |
| 1.2. 体制 | 2 |
| 1.3. 検討の経緯 | 3 |
| 2. ウイルス被害額算出の基本的考え方 | 4 |
| 2.1. 被害事象の分類 | 4 |
| 2.2. 被害額算出モデルの方向性 | 4 |
| 2.2.1. 被害額算出の基本単位 | 4 |
| 2.2.2. ウイルス被害の収支への影響 | 5 |
| 3. ウイルス被害額算出モデル | 7 |
| 3.1. モデルの構造 | 7 |
| 3.2. 復旧に要したコスト | 8 |
| 3.2.1. システム復旧コスト | 8 |
| 3.2.2. データ復旧コスト | 8 |
| 3.3. ウイルス被害による逸失売上 | 9 |
| 3.3.1. EC 停止による売上減分 | 9 |
| 3.3.2. 重要システム停止による売上減分 | 9 |
| 4. モデルの評価と今後の課題 | 11 |
| 4.1. 被害額算出モデルの評価 | 11 |
| 4.2. ウイルス被害額モデルに関する今後の課題 | 14 |
| 5. その他の情報セキュリティ事象に関する被害額の実態把握 | 15 |
| 5.1. SQL インジェクションによる被害実態について | 15 |
| 5.2. Winny を通じたウイルス感染による情報漏えいの被害実態について | 19 |
| | |
| 別紙 1 重要システム停止による売上への影響度の考え方 | |
| 別紙 2 コンピュータウイルスに関する被害状況調査アンケートの概要 | |
| 別紙 3 国内の被害総額の推計方法 | |

1. 検討の概要

1.1. 目的

ネットワークを軸とする IT（情報技術）は、今やわが国の社会・経済の基盤を支える極めて重要な社会インフラを担っている。そのため、IT システムがコンピュータウイルス（以下、「ウイルス」という）に感染すると、単に従業員やグループの業務に支障を来すだけでなく、例えば、Winny ネットワークを介してなど、個人情報をはじめとする機密情報の流出事故や、全社あるいは取引先を含むバリューチェーン全体の事業中断をも招きかねない。さらに、取引先や提供サービスのエンドユーザへの感染拡大、トラフィックの急増によるネットワーク障害といった IT 社会への悪影響も発生する可能性がある。

つまり、ウイルス対策は、企業の事業継続性確保や果たすべき社会的責任の遂行に不可欠な取組みの一つと言える。したがって、政府は、企業に対策実施の動機を与える定量的なデータの提供と、その取組みを促す適切な施策の実施を通じて、企業のウイルス対策を推進することが求められている。

しかし、情報セキュリティ対策の実施にはコストを要するため、企業が十分な予算を確保するのに有効な客観的データと、セキュリティインシデントが及ぼす社会的影響の度合いを提示し、その取組みの重要性を啓発していく必要がある。IPA では従来、被害額算出モデルを開発しその試算を行ってきた。ただし、これまでのモデルは、事業所単位・インシデント単位のデータを積み上げる形で、インシデントの規模に応じた被害実態を明示できるメリットが得られた反面、企業単位の経営指標が利用できない、平均的なインシデントの規模の設定が回答者の判断に依存するため、企業の被害額を検討する際の振れ幅が大きくなるといった問題も見られた。そこで、回答しやすさを向上し主観的判断を減らす改善を行うことによって、回答者の負担を軽減するとともに、回答の振れ幅を抑制し被害額を安定的に計測する手法を開発することが望まれる。

このため、IPA では、「ウイルス被害額算出モデル研究会」を設置し、ウイルスの被害額算出モデル（ウイルスにより企業の重要システムなどの能力低下・停止といったインシデントによる被害額算出）を確立することをめざす。また、別途行われる国内におけるコンピュータウイルス被害状況調査の結果を踏まえ、被害額算出モデルを用い、国内企業の被害ケースを試算し、今後の参考とする。

また、2005 年は、不正アクセスによる商用 Web サイトへの攻撃（SQL インジェクションによるもの）や Winny ネットワークを介した情報漏えいインシデントといったものが、情報セキュリティ関連の重大事件として捉えることのできる年であった。これらによる事業への影響は、ウイルス被害によるシステムの停止といった従来から調査研究してきたインシデントと同様に、非常に大きなものと考えられる。また、こうしたインシデントによる影響についての調査研究は重要になりつつある。一方で、こうしたことについては、これまで十分な調査研究はなされておらず、単にアンケートなどによって傾向を捉えるといったことは難しいと考えられた。このため、公表された事例などを対象に、今後の情報セキュリティ関連インシデント対応における参考情報として提供すべく、ヒアリング等による方法によって事例研究も行った。

1.2. 体制

(1) 研究会

IPA では、被害額算出モデルを策定するため、有識者による「ウイルス被害額算出モデル研究会」(以下、研究会という)を設置した。以下に研究会の委員構成を示す。

ウイルス被害額算出モデル研究会 委員構成 (敬称略・順不同)

(委員長)

元橋 一之 東京大学 大学院工学系研究科 教授

(委員)

五井 孝 株式会社大和総研
システムソリューション事業本部ソリューション推進部次長
早乙女 真 株式会社NTTデータ経営研究所
ソーシャル・イノベーション・コンサルティング本部 チーフコンサルタント
重松 孝明 日本アイ・エス・ティ株式会社 第二システム部 部長
長嶋 潔 東京海上日動火災保険株式会社 情報産業部 eリスクプロジェクトリーダー
山田 英史 株式会社ディアイティ セキュリティガバナンスビジネス部 マネージャー

(事務局)

三角 育生 独立行政法人情報処理推進機構 セキュリティセンター センター長
小門 寿明 独立行政法人情報処理推進機構 セキュリティセンター
ウイルス・不正アクセス対策グループ グループリーダー
石井 茂 独立行政法人情報処理推進機構 セキュリティセンター
普及グループ グループリーダー
花村 憲一 独立行政法人情報処理推進機構 セキュリティセンター
情報セキュリティ技術ラボラトリー 研究員
川口 修司 株式会社三菱総合研究所 情報セキュリティ研究グループ 主任研究員
井上 信吾 株式会社三菱総合研究所 情報セキュリティ研究グループ 研究員
江連 三香 株式会社三菱総合研究所 情報セキュリティ研究グループ 研究員

(2) 全体のフレームワーク

IPA の研究会では、被害額算出モデルの確立に向けた検討を行った。また、IPA では、「国内におけるコンピュータウイルス被害状況調査」として株式会社三菱総合研究所(以下、「MRI」という)にアンケート調査を委託しており、その一環として、本研究会で策定した被害額算出モデルに基づき、アンケートの結果を踏まえた被害額を試算した。ウイルス被害額算出に関し、研究会での検討と国内におけるコンピュータウイルス被害状況調査のフレームワークを図 1-1 に示す。

加えて、不正アクセス(SQL インジェクション)及び Winny を介した情報漏えい関連のインシデントについて、事務局にてヒアリング等を実施した。

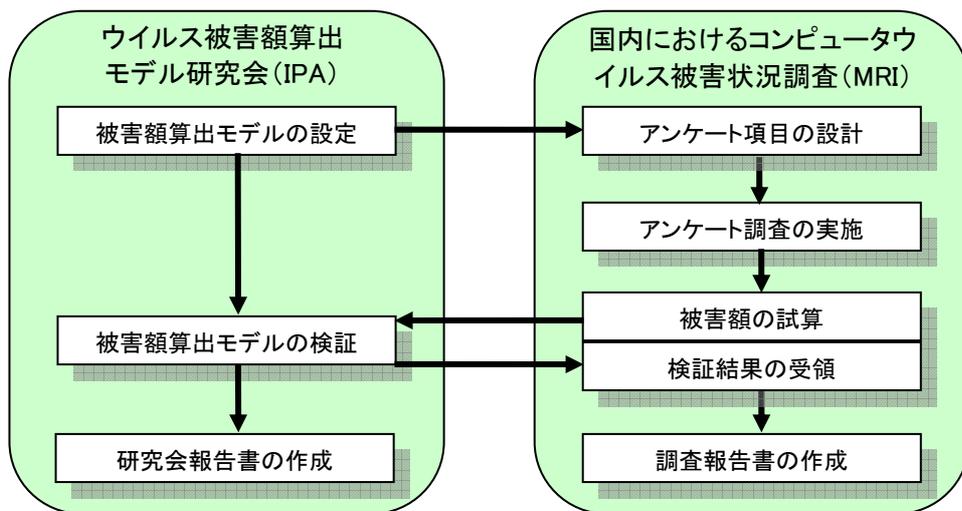


図 1-1 ウイルス被害額調査のフレームワーク

1.3. 検討の経緯

研究会は、以下の日程で計4回開催した。

平成18年1月25日（水）平成17年度第一回会合

平成18年2月9日（木）平成17年度第二回会合

平成18年4月6日（木）平成17年度第三回会合

平成18年5月9日（火）平成18年度第一回会合

その他、追加的な審議をメールベースで行った。

2. ウイルス被害額算出の基本的考え方

2.1. 被害事象の分類

ウイルス被害額¹を算出するためには、金額換算可能な「被害」を対象とする必要がある。被害事象は、ウイルスの感染が直接的に引き起こす一次的被害と、その波及効果として間接的に発生する二次的被害に分類できる。また、これらの被害事象を金額換算する場合、例えば、感染により発生した支出と、本来得られるはずであったが感染により得られなかった売上（機会損失による逸失売上）の2つに整理する方向が考えられる。これらの整理に基づき、ウイルス感染による被害事象を表 2-1に例示する。

表 2-1 ウイルス感染による主な被害事象の例示

| 被害額の性質 | 被害のタイプ | |
|----------------|---|---|
| | 一次的被害（直接的） | 二次的被害（間接的） |
| 感染により発生した支出 | <ul style="list-style-type: none">・機器の性能低下～停止・データの破壊、流出 | <ul style="list-style-type: none">・補償、補填、損害賠償・謝罪広告・訴訟費用 |
| 感染により得られなかった売上 | <ul style="list-style-type: none">・EC等サービスの遅延～不能化・業務プロセスの遅延～停止 | <ul style="list-style-type: none">・風評被害 |

2.2. 被害額算出モデルの方向性

2.2.1. 被害額算出の基本単位

被害額の推計に力点を置いた被害額算出モデルは、全体をいくつかのグループ（カテゴリ）に分類して、カテゴリ毎に被害額合計を算出できるように設計する。その際、なるべく分散が少なくなるようにカテゴリの分類を定めること、またカテゴリの合計額が正確かつ容易に算出できるようにカテゴリ内の算出単位（被害額を算出する最小単位）を設定することが望まれる。

(1) カテゴリ

被害額を算出する際には、何らかの区分に基づくカテゴリ毎に算出単位を導出し、それぞれの母数を乗じる。例えば、ITやインターネットへの依存度合いは業務プロセスの構造によって異なること、企業規模によってウイルス対策の実施状況や被害を受けうる端末数に差があることなどを考慮すれば、業種や企業規模による分類がウイルスの被害規模の把握に有効と考えられる。

なお、実査の実施にあたっては、カテゴリ毎に統計的に見て適正な規模の回収数を確保できるようにカテゴリを設定することも重要である。

¹ ここでの被害額算出対象は、ウイルスによりシステム機能低下、停止等のインシデントを生ぜしめたものを想定。Winnyネットワークを介したインシデントについては、別途、事例研究によって調査した。

(2) 算出単位

被害額算出モデルの算出単位は、事業所単位とする場合と企業単位とする場合が考えられる。事業所単位の場合、対象範囲が狭いため、システム管理者が個々のインシデントの状況を把握しやすく、アンケートによって比較的精緻な被害実態を導出することが可能である。しかし、企業の事業に対するインパクトなどの検討にあたって、企業の経営指標²をそのまま適用することができないため、回答者に指標値を調整するなどの負担をかけることになる。一方、企業単位の場合、企業の経営指標を活用することが可能だが、回答部署が企業全体としての被害を集約していることが企業あたりの正確な被害額を推計する前提となる。

また、被害規模算出の考え方として、インシデント一回あたりを単位にする方法と、年ベースで発生したインシデントの累計を単位にする方法が考えられる。前者は、インシデント一回あたりの被害規模算出に有効であるが、個々のインシデントに幅があるため、代表値が回答者の主観的な判断に左右される可能性がある。一方、後者は、年ベースの延べ作業工数に集約するためインシデントの発生頻度や規模のばらつきに影響されにくいと考えられるが、インシデント一回あたりの被害規模は通年化されるため現場の実感に合わない値となる可能性もある。

本研究会の被害額算出モデルでは、回答しやすさを向上し回答者の主観的判断を減らすことによって、回答者の負担を軽減するとともに、回答の振れ幅を抑制し被害額を安定的に計測できるように、企業毎の、年ベースの累計単位で見た被害額を把握するものとする。

2.2.2. ウイルス被害の収支への影響

(1) 感染による営業機会逸失の金額換算

感染による営業機会の逸失を金額換算する場合、業務停止が影響する割合を売上に乗じたものとするか、利益に乗じたものとするかは重要な問題である。

企業の実被害という観点で見ると、ウイルス感染が発生して業務が停止し、売上が低下したとしても、調達した部材や商品の資産価値が低下するわけではない³ので、実際に逸失するのは売上分全額ではなく利益相当分のみと考えることができる。損害保険の観点からも、損失を利益相当分と考えるのが妥当とする意見もあった。

一方、数値の信頼性の観点で見ると、利益にはコスト削減などの企業努力や産業環境などの要素も含まれるため、ウイルス被害額の実態に合わないという考え方もある。BSE（狂牛病）やSARSといったトラブルの事象がもたらす社会的影響の規模を金額で表現する場合には、売上ベースの金額が用いられることも少なくない。

本研究会の被害額算出モデルでは、経年比較を念頭に置いた統計の安定性も鑑み、感染による営業機会逸失の金額換算を、業務停止が影響する割合を売上に乗じたものとする。

² 経営指標は、決算書で提示される売上高等の業績データ。企業単位で算出される。

³ 食材のように鮮度が重視される部材や商品は、資産価値が低下する可能性がある。

(2) 感染による二次的被害

例えば、ウイルスをきっかけとして電子商取引（EC）サイトが改ざんされたり、ウイルスに感染したサイトを閲覧した顧客がウイルスに感染したりした場合、既存顧客が離反したり新規顧客から敬遠され、売上を大幅に落とす可能性がある。そうした風評被害による損失は復旧に要する費用より大きいとする分析もある⁴。

ただし、そのような二次的被害は、他の影響因子を除いて計測することが困難である⁵ため、感染の直接的な被害である一次的被害と同列に扱うことは適当でないと考えられる。

⁴ 高橋正和, “事故発生時の損失額は?”, 日経情報ストラテジー 2004年08月号 pp260-263

⁵ 例えば、営業活動の自粛などの影響や、流出した情報の種類による影響などを取り除くことが難しい。

3. ウイルス被害額算出モデル

3.1. モデルの構造

2章の検討を踏まえ、本研究会では、ウイルス被害額算出モデルの位置付けを、「一企業における年間の一次的被害額（円／年）」を算出するものとし、その概要を以下のように設定する。

- ・ 被害額算出の対象は一次的被害に限定する。
- ・ 被害額の算出単位は、企業毎の、年ベースで発生したインシデントの累計とする。
- ・ 感染による営業機会の逸失分は、売上ベースで算出する。

今回策定したウイルス被害額の算出モデルの構造を図 3-1に示す。具体的には、ウイルス感染からの復旧に要したコストと、ウイルス被害の発生による逸失売上で構成される。

$$\boxed{\text{ウイルス被害額}} = \boxed{\text{復旧に要したコスト}} + \boxed{\text{ウイルス被害による逸失売上}}$$

モデルの積算範囲

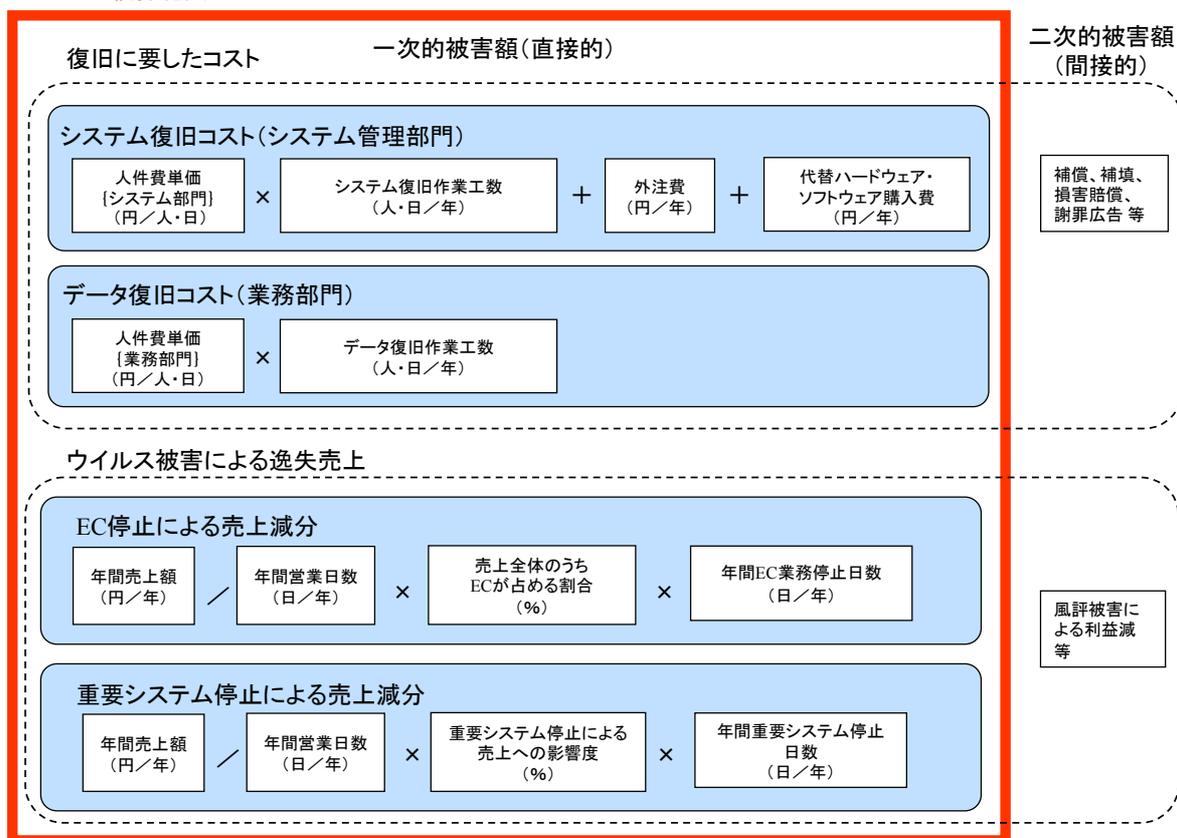


図 3-1 ウイルス被害額算出モデルの構造

3.2. 復旧に要したコスト

復旧に要したコストは、システム復旧コストとデータ復旧コストで構成される。

$$\boxed{\text{復旧に要したコスト}} = \boxed{\text{システム復旧コスト}} + \boxed{\text{データ復旧コスト}}$$

「システム復旧コスト」とは、システム部門のスタッフがウイルスに感染したコンピュータの復旧に要した費用である。また、「データ復旧コスト」とは、業務部門のスタッフがウイルス感染により消失・破壊されたデータの復旧にかけた費用である。

3.2.1. システム復旧コスト

システム復旧コストは、システム復旧にかかる人件費、復旧に関する外注費、代替ハードウェア・ソフトウェア購入費の総和で構成される。

$$\begin{array}{c} \text{システム復旧にかかる人件費} \\ \boxed{\text{システム復旧コスト}} = \boxed{\text{人件費単価(システム部門)}} \times \boxed{\text{システム復旧作業工数}} \\ \quad + \boxed{\text{外注費}} + \boxed{\text{代替ハードウェア・ソフトウェア購入費}} \end{array}$$

- ・ 「システム復旧にかかる人件費」は、人件費単価（システム部門）とシステム復旧作業工数から算出される。このうち、「人件費単価（システム部門）」（円/人・日）は、被害を受けたシステムを復旧するための作業に投入されるシステム部門スタッフ1名・1日あたりの人件費単価である。また、「システム復旧作業工数」（人・日/年）は、システム復旧に要した年間の延べ作業工数である。
- ・ 「外注費」（円/年）は、システム復旧に際して、外部セキュリティ業者等に業務を発注した際の費用である。
- ・ 「代替ハードウェア・ソフトウェア購入費」（円/年）は、システム復旧に際して、新たに購入したハードウェアおよびソフトウェアの購入費用である。

3.2.2. データ復旧コスト

データ復旧コストは、データ復旧にかかる人件費である。

$$\boxed{\text{データ復旧コスト}} = \boxed{\text{人件費単価(業務部門)}} \times \boxed{\text{データ復旧作業工数}}$$

- ・ 「業務部門の時間あたり人件費単価」（円/人・日）は、被害を受けたデータを復旧するための作業に投入される業務部門スタッフ1名の1日あたりの人件費単価である。
- ・ 「データ復旧作業工数」（人・日/年）は、業務部門においてデータ復旧に要した年間の延べ作業工数である。

3.3. ウイルス被害による逸失売上

ウイルス被害の影響が売上にまで及ぶのは、電子商取引（EC）をはじめインターネット上での事業を支えるシステムや、社内の業務プロセスを支えるネットワークや重要サーバが感染し停止した場合に代表されると考えられる。そこで、ウイルス被害による逸失売上は、電子商取引（EC）停止による売上減分と重要システム停止による売上減分で構成されるものとする。

$$\boxed{\text{ウイルス被害による逸失売上}} = \boxed{\text{EC 停止による売上減分}} + \boxed{\text{重要システム停止による売上減分}}$$

なお、重要システムとは、インターネットに公開している業務遂行上重要なサーバ（EC サーバは除く）、及び社内のネットワークや基幹システムなどの事業活動に深く関係する重要サーバを指す。

3.3.1. EC 停止による売上減分

本モデルでは、EC 業務の場合はシステム停止時間がそのまま売上減に直結すると仮定する。そこで、「EC 停止による売上減分」（円/年）は、一日あたりの EC 売上額（円/日）と EC 業務停止日数（日/年）から算出できる。

$$\boxed{\text{EC 停止による売上減分}} = \frac{\text{年間売上額}}{\text{年間営業日数}} \times \frac{\text{売上全体のうち EC が占める割合}}{\text{EC 業務停止日数}}$$

一日あたりの EC 売上額

- ・ 「一日あたりの EC 売上額」（円/日）は、年間売上額（円/年）、年間営業日数（日/年）、売上全体のうち EC が占める割合（%）から導出する。
- ・ 「EC 業務停止日数」（日/年）は、ウイルス感染の影響で EC 業務が停止した期間（年ベース）である。

3.3.2. 重要システム停止による売上減分

重要システム停止による売上減分は、一日あたりの売上額（円/日）、重要システム停止による売上への影響度（%）、年間の重要システム停止日数（日/年）から算出する。

ここで考慮すべきは、EC サービスのように、重要システムの停止が即売上に影響するとは限らない点である。すなわち、重要システムの停止時間がどの程度になると売上に影響するか（許容停止時間）と、許容停止時間を越えて重要システムが停止した場合に売上が被るダメージの大きさ（売上への影響度）を勘案して、売上減分を導出する必要がある。

$$\begin{array}{c}
 \text{重要システム停止による売上減分} = \overbrace{\text{年間売上額} / \text{年間営業日数}}^{\text{一日あたりの売上額}} \\
 \times \text{重要システム停止による売上への影響度} \times \text{重要システム停止日数}
 \end{array}$$

- ・ 「一日あたりの売上額」(円/日)は、年間売上額(円/年)、年間営業日数(日/年)から導出する。
- ・ 「重要システム停止による売上への影響度」(%)は、許容停止時間を考慮した売上への影響度である(別紙1参照)。
- ・ 「重要システム停止日数」(日/年)は、ウイルス感染の影響で重要システムが停止した期間(年ベース)である。

4. モデルの評価と今後の課題

4.1. 被害額算出モデルの評価

(1) ウイルスに感染し被害を受けた1企業あたりのウイルス被害額

ウイルス被害額算出モデルに基づき、「コンピュータウイルスに関する被害状況調査」アンケート結果（2006年3月実施、発送総数6,561件・有効回答1,701件；別紙2参照）や既存の公表データを用いると、ウイルスに感染し被害を受けた1企業あたりの算出項目毎のウイルス被害額（年ベース）が算出可能である。

表4-1に示す通り、算出項目は「復旧に要したコスト」と「ウイルス被害による逸失売上」に大別され、さらに各算出項目は詳細化される。本モデルでは、「感染」と「被害」を別にして捉え、各算出項目の被害額は、全感染企業の平均ではなく「各被害が発生した企業」の平均を各項目において算出する。その理由は、全ウイルス感染企業を対象として平均値を求めた場合、被害の発生していない企業が平均値を下げるために、実際に企業が被害に遭った場合の被害額の大きさに対して、統計で示された平均値が乖離してしまうためである。

なお、本文では、従業員数300名未満の企業を「中小企業」、従業員数300名以上の企業を「大手・中堅企業」と定義する。

表 4-1 算出項目一覧

| 算出項目 | 算出項目と アンケートによる算出対象企業数 | | |
|--------------------|--------------------------|--|--|
| | 項目 | 中小企業 | 大手・ 中堅企業 |
| 復旧に要したコスト | | | |
| システム復旧コスト | | | |
| システム復旧に係る人件費 | システム復旧作業発生企業 | 95社 | 110社 |
| 外注費 | 外注費発生企業 | 1社 | 0社 |
| 代替ハードウェア・ソフトウェア購入費 | 代替機器購入企業 | 7社 | 4社 |
| データ復旧コスト | データ復旧作業発生企業 | 95社 | 110社 |
| ウイルス被害による逸失売上 | | | |
| EC停止による売上減分 | ECサーバが停止し、売上に影響した企業 | 3社 | 2社 |
| 重要システム停止による売上減分 | 重要システムが停止し、売上に影響した企業 | 17社 ^{*1} 24社 ^{*2} | 21社 ^{*1} 41社 ^{*2} |

※ 1) サーバ停止やネットワーク停止により売上に影響を受けた企業数

※ 2) 重要サーバ停止により売上に影響を受けた企業数

例えば、1社あたりの「システム復旧に係る人件費」は、3章で示したモデル式に当てはめると下記の通りとなる。

$$\begin{aligned} \text{システム復旧に係る人件費} &= \text{人件費単価(システム部門)} \times \text{システム復旧作業工数} \\ &= (\text{人件費単価/時} \times \text{1日あたり営業時間}) \times \text{システム復旧に要した作業工数} \\ \text{※中小企業の場合} &= (1,659 \text{ 円/時} \cdot \text{人} \times 8.6 \text{ 時間/日}) \times 2.6 \text{ 人} \cdot \text{日} \\ \text{※大手・中堅企業の場合} &= (1,659 \text{ 円/時} \cdot \text{人} \times 9.4 \text{ 時間/日}) \times 4.1 \text{ 人} \cdot \text{日} \end{aligned}$$

【データ出典】

人件費単価（システム部門）：「厚生労働省賃金構造基本統計調査 平成16年」より
「電子計算機オペレーター」の金額を企業規模・業種に依らず一律に適用。

1日あたり営業時間：アンケート調査結果より平均値を算出

システム復旧に要した作業工数：アンケート調査結果より平均値を算出

このように、算出項目毎のウイルス被害額の算出式は、下記の通りとなる。

$$\text{算出項目毎のウイルス被害額 (円/年・社)} = \sum_{i=1}^{Xk} Ck_{(i)} / Xk$$

Ck: 項目Kの被害額

Xk: 算出項目 k における被害額発生企業数 (算出項目によって異なる)

ウイルスに感染した場合でも、全ての算出項目に該当する被害が発生する訳ではないため、各算出項目によって算出対象企業数が異なる。

アンケート調査結果を見ると、システム復旧コストやデータ復旧コスト等、復旧に要したコストは全ての企業で発生するが、ECや重要システムが停止し、逸失売上として被害が発生するだけの大きな影響を受ける企業は限られている。しかし、復旧コストと逸失売上が同時に発生した場合は多額の被害額が発生している。

中小企業、大手・中堅企業それぞれについて、次の考え方で、被害額が生じた企業の平均的な被害額を参考値として計算すると、それぞれ以下のとおりとなった。

| | | |
|-----------|---------------------|-------------------------|
| | 中小企業 (被害発生企業数 95 社) | 大手・中堅企業 (被害発生企業数 110 社) |
| 被害額 (参考値) | 約 4.3 百万円/社 | 約 130 百万円/社 |

【考え方】

復旧に要したコストの1社あたりの平均値は

$$C = \sum_{j=1}^k \sum_{i=1}^X C_{(j,i)} / X$$

ただし、 $C_{(j,i)}$ は、被害額が生じた企業*i*における、復旧に要したコストの個別項目*j*に係るコスト（被害額）である。 k は、復旧に要したコストの個別項目の総数（＝4項目）、 X は中小企業又は大手・中堅企業それぞれのカテゴリにおける被害額が生じた企業の総数である。例えば、ある企業*m*における個別項目*n*についてはコスト（被害額）が生じていない場合は $C_{(nm)} = 0$ として計算する。

| | 中小企業 (復旧コスト発生企業数 95 社) | 大手・中堅企業 (復旧コスト発生企業数 110 社) |
|-----------|---------------------------|-------------------------------|
| 復旧に要したコスト | 約 172 千円／社 | 約 153 千円／社 |

同様に、逸失売上の1社あたりの平均値は

$$L = \sum_{j=1}^1 \sum_{i=1}^Y L_{(j,i)} / Y$$

ただし、 $L_{(j,i)}$ は、逸失売上が生じた企業*i*における、逸失売上の個別項目*j*に係る売上減分である。 1 は、逸失売上の個別項目の総数（2項目）、 Y は中小企業又は大手・中堅企業それぞれのカテゴリにおける逸失売上が生じた企業の総数である。例えば、ある企業*m*における個別項目については売上減が生じていない場合は、 $L_{(nm)} = 0$ として計算する。

| | 中小企業 (逸失売上発生企業数 35 社) | 大手・中堅企業 (逸失売上発生企業数 46 社) |
|------|--------------------------|-----------------------------|
| 逸失売上 | 約 4,136 千円／社 | 約 129,497 千円／社 |

※大手・中堅企業、46社の内訳には、売上高1,000億円を超える企業が数社含まれており、当該企業において2日を越えるネットワーク停止の被害が発生すると、逸失売上は約3億円～4億円が計上される。これらにより、1社あたりの逸失売上が1億を超える額となっている。

仮に1企業において「復旧に要したコスト」及び「ウイルス被害による逸失売上」が発生したとした場合、平均的な被害額＝ $C + L$ （中小企業、大手・中堅企業別）となる。

| | 中小企業 (被害発生企業数 95 社) | 大手・中堅企業 (被害発生企業数 110 社) |
|--------------------|------------------------|----------------------------|
| 1企業あたり被害額 (参考値) | 4,308 千円／社 | 129,649 千円／社 |

注) なお、逸失売上についての有効数字は百万円単位だが、計算の便宜上千円単位を用いた。

国内総被害額の計算手法と算出のための基礎データは別紙に記載する。

4.2. ウイルス被害額モデルに関する今後の課題

ウイルス被害額算出モデル（ウイルスにより企業の重要システムなどの能力低下・停止といったインシデントによる被害額算出モデル）の課題として、以下の項目が挙げられる。

(1) 企業を算出単位とすることのメリットとリスク

本研究会のモデルでは、算出単位を「インシデント」「事業所」から「年間」「企業」に変更した。これにより、企業の売上高等の経営指標や各種調査を試算に適用することが可能となり、モデルの精度を向上させることができたと考えられる。

ただし、本モデルでは、企業の情報セキュリティ担当部署が、各事業所で発生したトラブルを企業という単位ですべてを把握していることが前提となる。そこで、複数の事業所を有する回答企業において、ネットワーク的に外部接続点を絞り複数の事業所を企業単位で管理している、または復旧が必要な規模のトラブルについては情報セキュリティ担当部署への報告が義務付けられていることを確認することが望まれる。

(2) 外注費、代替ハードウェア・ソフトウェア購入費等のデータの安定性

システム復旧のための外注や代替ハードウェア・ソフトウェアの購入はモデル構成上必要と考えられるが、アンケート調査の場合、このように必ず発生するわけではない項目は、そのときの回答票の傾向によってデータの安定性を損なう要因となる可能性がある。こうした項目についても安定的にデータを確保するためには、アンケートの回収票をさらに増やすことが望まれる。

(3) 二次的被害額のモデル化

本研究会のモデルには、ウイルス被害が取引先やエンドユーザに悪影響を及ぼした場合の補償・補填、損害賠償、謝罪広告、訴訟費用、また風評被害による機会損失といった二次的被害額は含まれていない。しかし、ウイルス被害が社会的に大きな影響を及ぼした場合、その風評による機会損失は極めて大きくなる可能性がある。他の影響因子を除くことが困難であるため、一次的被害額と同列に扱うことは適当ではないが、そうした影響規模についても将来的にはモデルの一環として検討することも考えられる。

5. その他の情報セキュリティ事象に関する被害額の実態把握

情報セキュリティインシデントには、ウイルスにより企業の重要システムなどの能力低下・停止といったインシデント以外にも様々な要因があり、不正アクセスによりホームページを改ざんされたり、P2P ファイル交換ソフトなどを介した個人情報を含む機密情報が漏えいしたといったインシデントが多数報道されている。

特に、2005 年は、不正アクセスによる商用 Web サイトへの攻撃（SQL インジェクションによるもの）や Winny ネットワークを介した情報漏えいインシデントといったものが、情報セキュリティ関連の重大事件として捉えることのできる年であった⁶。このようなインシデントが起きた場合、原因調査や復旧作業にどれほどの人的資源を要するのか、金銭的被害が発生するのかについて、インシデント対応を実施した企業に対し実態調査を行った。

※実態調査は、被害を受けたことが公表されている企業を対象に IPA（事務局）がヒアリング等を行い、計 10 社に協力を頂き対応状況等につき調査したものである。

5.1. SQL インジェクションによる被害実態について

SQL⁷インジェクションとは

データベースと連携したウェブアプリケーションの多くは、利用者からの入力情報を基にデータベースへの命令文を組み立てる。ここで、命令文の組み立て方法に問題がある場合、攻撃によってデータベースの不正利用を招く可能性がある。この問題を悪用した攻撃手法は、一般に「SQL インジェクション」と呼ばれている。データベースが不正利用されると、データが書き換えられたり、機密情報が漏えいしたりする危険性がある。

2005 年には、氏名、住所、電話番号、生年月日、メールアドレスなど大量の情報が流出した事件や、攻撃を受けたウェブサイトへアクセスした利用者がウイルスに感染するようにウェブページを改ざんされた事件など、SQL インジェクションによる事件の報道が多数あった。このような状況を踏まえ、報道のあった企業のうち数社に対してヒアリング等により、被害の状況、対応状況等につき調査を実施した。

⁶ 情報セキュリティ白書 2006 年版では、2005 年の 10 大脅威として、「第 1 位 事件化する SQL インジェクション」および「第 2 位 Winny を通じたウイルス感染による情報漏えいの多発」を挙げている。

⁷ Structured Query Language

以下に、ヒアリング等の結果に基づき、インシデントの発生から、対応開始、事態の収拾までを時系列に整理することとし、得られた情報などを基に、事例の平均的な被害額についても推計を行うこととする。

(1) インシデントの顕在化・初動対応

インシデントの発生については、

- ・自社のホームページが改ざんされていることを自ら又はウェブサイト管理外注先が発見
- ・アクセスログに異常(大量)なアクセスが残っていることから発見

など、自ら又は管理外注先が、なんらかの不正アクセス被害が発生していることを確認。

今回調査したいずれのケースも、ウェブページが改ざんされるなどにより、ウェブサイトを通じた事業の継続が困難となり、被害発生の確認後、直ちに、被害原因の調査及び被害拡大防止のため、ウェブサイトを通じたサービスの提供を全面的に停止している。

(2) 被害状況の調査

ウェブサイト管理会社やセキュリティ専門業者などにより、当該のウェブサーバおよびウェブアプリケーションについて、被害原因の追究を実施。ウェブサーバのログ調査などの結果、SQLインジェクションのぜい弱性が存在しており、これを突かれたためと判明。また、ウェブサイトを通じて会員登録を行ったユーザのメールアドレス等が漏えいしていた事実も明らかとなった。これらの調査により、被害原因および被害範囲を特定に至る。

インシデント発生確認後、被害状況の調査には、平均数日間を要している。

(3) 復旧作業

SQL インジェクションのぜい弱性を解消するため、ウェブアプリケーションの利用者からの入力情報を基にデータベースへの命令文を組み立てる部分を全てチェックし、また、データベース操作・管理ソフトについても点検を実施している。その結果を踏まえて、保有するウェブアプリケーションの改修作業およびサーバの再構築を実施。ウェブサイトの公開に向けて、改修作業を行ったものについて、ぜい弱性やその他の問題の有無をチェックするため、セキュリティ専門企業におけるセキュリティ診断を実施。

閉鎖していたウェブサイトの復旧にあたっては、

- ・全てのページを対象に必要な改修の実施及びセキュリティ診断が終了してから公開したケース
 - ・一部のコア事業から改修・診断を経てサイト公開したといった復旧を段階的に行ったケース
- の両者があった。いずれのケースも、全面復旧までには3、4ヶ月を要したところが多かった。

セキュリティ強化の観点から、メール情報等の暗号化、データベース管理等の再設定なども行っている。

また、ヒアリングしたケースでは、いずれの場合にも、復旧作業では、単にウェブアプリケーションの改修・診断といったソフトウェア面での対応のみならず、不正アクセスを防止するために有効と判断したハードウェア（ファイアウォール、IDS⁸、IPS⁹）の導入・設置などのセキュリティ対策の強化も行っている。

(4) 対外説明

インシデントに関する対外発表は、被害原因及び被害状況を把握の後、実施している。

個人情報を漏えいしてしまった顧客に対しては、個別に謝罪の連絡を送り、謝罪の告知を新聞等のメディアや自社のホームページを通じて実施。加えて、外部からの問い合わせ対応のために窓口を設置するなどの対応を行った。

外部からの問い合わせ対応のために、専用のコールセンターを設置したケースもあった。その内容は、派遣職員を含む対応要員を一定数確保し、部屋を用意、フリーダイヤル設置などである。問い合わせ体制については、段階的に縮小しているが、半年程度継続したところもある。

また、ウェブサイトの有償で情報等を掲載していた社におけるインシデントでは、当該事業のクライアントに対して個別に説明を行い、ウェブサイト停止期間における損害を補償したケースもあった。

(5) 社内体制の整備

すべての復旧作業・対外説明が終了した後、社内にセキュリティ対策部署の設置や情報の管理体制の見直しなど、必要な社内体制を充実させた。

推計される被害額について

直接的な被害額として計上される支出項目として、以下の対策などが挙げられる。

- ・ サーバの再構築作業（OSの再インストール、各種設定等）
- ・ Webアプリケーションの改修作業
- ・ 第三者によるセキュリティ検査（ぜい弱性検査）
- ・ セキュリティ対策システム機器（ファイアウォールやIDS等）の導入

ヒアリング対象となった社（複数社）のケースをみると、使用されていたサーバの台数（数台～数十台）・プログラム本数（数百本～数千本）であった。これらを踏まえて、復旧作業に要したウェブアプリケーション等の改修費用・検査等の外注費およびファイアウォール等の機器の購入費を推計すると、約4,800万円～1億円程度を要するものと考えられる。

⁸ Intrusion Detection System

⁹ Intrusion Prevention/Protection System

推計根拠

プログラムの改修・検査工数 約3人日/本 (ヒアリングしたケースから推定)

約3万円/人・日 (ソフトウェア開発技術者単価¹⁰) ×プログラム改修・検査工数×プログラム本数 (500本のケース、1,000本のケース) = 約4,500万円~9,000万円

ファイアウォール等の機器の導入コスト 約300~1,000万円 (ヒアリングしたケース)

合計 約4,800万円~1億円

また、社内での人件費については、インシデント発生時から対応を完了するまで、様々な時点で組織としての意志決定を必要とされる。この決定には、組織のトップを含めた専門チームが非常に多くの時間を費やしており、概ね100~200人日を要しているケースがほとんどであった。この人件費を平均の労働賃金で計算すると、およそ以下の金額となる。

$100\sim 200 \times 17,976 \text{円}^{11} (\text{人/日}) = 180 \text{万円} \sim 360 \text{万円}$

顧客情報が漏えいしたケースや、サイト閉鎖による広告主への保証など、対外的に説明・保証が必要な場合がある。こちらについても以下のとおり、金銭的な被害が発生することとなる。

- ・情報が漏えいしてしまった方へのお詫び (電子メールや郵便)
- ・問い合わせ窓口の設置 (フリーダイヤルの設置や専任スタッフの配置)
- ・サイト閉鎖期間における広告費の返還や保証

これらの幅はおおよそ数百万円~5千万円を要したという結果を得ることができた。

不正アクセスによりサイトに多大なダメージを受けた場合、売上の停止、復旧作業、顧客対応など、様々な損害が発生することとなり、総額1億円を超える被害額が発生することも稀ではないことが判明した。

なお、これらの推計値には、ウェブサイトの閉鎖による売上減 (逸失売上) を含んでいない。ウイルス被害額推定のように、これまで勘案するためには、単純に計算した場合に、企業のウェブサイトを通じた年間売上額に、閉鎖期間 (月数) / 12の値を乗じた規模と考えられる。

今回ヒアリングをした企業においては、ウェブサイトを通じた年間売上額は数億円から数十億円まで様々で、閉鎖期間は数ヶ月であったが、平均的なケースとして年間売上額20億円、3ヶ月間閉鎖したとした場合には、5億円規模の逸失売上があったことになる。

注：段階的に復旧・公開を実施した企業は特定のケースであったため、サイト閉鎖後、完全に復旧が完了してから公開したケースを取り上げている。

¹⁰ 月刊 積算資料 (財団法人 経済調査会) におけるソフトウェア開発技術者3の単価

¹¹ 平成16年厚生労働省賃金構造基本統計調査における全従業者の人件費単価 (詳細は別紙3を参照)

5.2. Winny を通じたウイルス感染による情報漏えいの被害実態について

Winny とは、P2P ファイル交換ソフトであり、同ソフトウェアを利用するユーザ間でファイルを共有できるものである。近年、Winny を悪用して情報漏えいを引き起こすウイルス (W32/Antinny) により、組織から顧客情報や技術情報などが漏えいした事件が多数報道され、大きな社会問題となった。

このような状況を踏まえ、報道のあった企業のうち数社に対してヒアリング等により、被害の状況、対応状況等につき調査を実施した。

以下に、ヒアリング等の結果に基づき、インシデントの発生から、対応開始、事態の收拾までを時系列に整理することとし、得られた情報などを基に、事例の平均的な被害額についても推計することとする。

(1) 情報漏えいの顕在化・初動対応

第三者から Winny のネットワークに企業情報が流れているとの通報を受け、情報漏えいが発覚。提供された情報を元に、当該データを Winny ネットワーク上で検索し、事実確認を行う。同時に、漏えい元となった PC の特定作業を行い、当該 PC に保存されているデータを確認。特定後、Winny ネットワーク上のデータと当該 PC のデータを照合し、流出しているデータの範囲を特定。また、流出したデータがもたらす影響範囲・対応策について社内で緊急体制を構築し、検討を開始。

(2) 被害状況の調査

流出元となった PC について解析を行い、感染した時期を特定し、データが Winny ネットワーク上に公開されていた期間を把握。また、Winny ネットワークの監視を行い、データの拡散範囲を調査。

流出したデータについては、内容を詳細に分析し、個人情報を中心とする重要情報の有無、範囲について精査した。

(3) 対外説明

漏えいしたデータに顧客情報が含まれていた場合、該当する法人・個人への謝罪対応を実施。法人であれば、営業担当が直接謝罪に出向き、個人へは郵送やメールを使い、事実を通知して謝罪した。

また、外部からの問い合わせに対応する専用窓口を設置するケースもあった。

(4) 再発防止策

社員およびグループ会社など、関係する組織の社員すべてに自宅 PC をチェックさせ、業務データが保存されていないかを確認。情報の持ち出しルールの再徹底を実施。

当然、業務 PC 及び自宅 PC において、Winny 等のファイル交換ソフトの使用を自粛または禁止する通知を発信した。

また、自宅 PC で業務を行うことを完全に禁止するようにしたケースや、情報漏えい時の被害を最小限にするため、持ち出し PC や自宅 PC で扱うデータを暗号化して保存するようにしたといった対策を講じたケースがあった。暗号化ソフトについては、新規に導入したり、運用方針の変更により、業務データが保存された自宅 PC まで適用範囲を拡大したといったケースがあった。

被害額の推計について

ヒアリングの結果、Winny 等による情報漏えい時の対応として、漏えいしたデータの調査分析作業および対外説明や問い合わせ対応に要する人件費が各社に共通して発生していた。

漏えいしたデータの精査には、10 数名～100 名の規模で、1 日～1 週間程度、照合作業およびデータの影響範囲の特定を実施しており、50 人日～100 人日を要したケースがほとんどであった。

$50 \sim 100 \times 17,976 \text{ 円} \times (\text{人/日}) = \text{約 } 90 \text{ 万円} \sim \text{約 } 180 \text{ 万円}$

また、流出元となった PC の解析作業及び Winny ネットワークにおけるデータの拡散状況について、外部業者に依頼しているケースもあり、これらの調査費の合計が約 5～600 万となっているものもあった。

顧客情報が漏えいしたケースの謝罪対応には、

- ・すべての法人（数十社）への謝罪対応に 2～3 名の営業担当が回り、約 200 人日を要した
 - ・個人（数百名）に、電話や郵送等による謝罪対応を実施し、約 25 人日を要した
- といったものがあった。

$200 \times 17,976 \text{ 円} \times (\text{人/日}) = \text{約 } 360 \text{ 万円}$

$25 \times 17,976 \text{ 円} \times (\text{人/日}) = \text{約 } 45 \text{ 万円}$

問い合わせ窓口を設置して対応したケースでは、漏えいの事実を公表してから約 3 ヶ月間、10 名体制で対応したケースなど、多大な人件費が発生しているものがあった。

$900 \times 17,976 \text{ 円} \times (\text{人/日}) = \text{約 } 1,620 \text{ 万円}$

※平成 16 年厚生労働省賃金構造基本統計調査における全従業員の人件費単価（詳細は別紙 3 を参照）

不正アクセスの被害で取り上げたケースと異なり、Winny による情報漏えい被害では、社員が対応する作業がほとんどであり、外部業者に発注する作業は限定されていた。本来、被害額として計上すべきではないかもしれないが、社員が対応した人件費を積み上げると、最大で約 2,100 万円もの費用がかかるケースがあることが明らかとなった。

また、調査を外注する場合は、約 5～600 万円の費用が必要となるケースもあり、さらに対応費用が追加される可能性があることも判明した。

なお、これらの数値には、Winny による情報漏えいによる二次的な被害額は含んでいない。

ヒアリングを通じて

インシデントに係る事例のヒアリング等を10社に実施したところ、次の実態が判明した。まず、自社が当事者になる事態を想定している企業は少ない、セキュリティ対策を実施してはいたが、十分ではなく、被害が発生する余地を残してしまっていたという点である。

誰もがそうであるが、自分が事故に遭うと思って自動車を運転しているドライバーはほとんどいないだろう。ところが、事故に遭って初めて保険のありがたさを感じるように、対策の重要性を認識するようになる。

情報セキュリティにおいても、経営上、予算を割り当てるのが困難なケースもあるが、誰もが不正アクセスを受ける危険性と隣り合わせである現状を鑑みると、必要最低限のセキュリティ投資は必要であるし、企業の存続に関わる事業であれば、相応の投資を行い、セキュリティレベルを高めておくことは必須である。

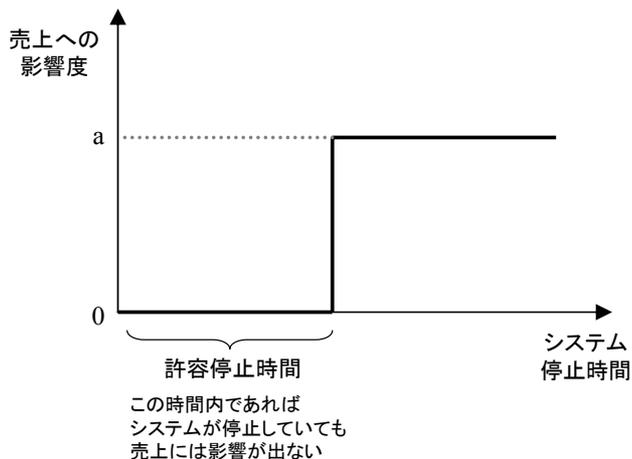
ヒアリングを実施した企業にあった共通点として、あらかじめセキュリティ対策への意識をさほど高く置いていなかったこと、今回のインシデント対応を行った結果、セキュリティ対策への意識に変化が生まれたことが挙げられる。特に、今後のセキュリティ対策を向上させていく上で必須である、経営層の理解が得られるようになった、経営層が牽引し、組織としてセキュリティ対策に取り組むようになったとの声が聞かれた。

インシデントが発生すると、金銭的被害もさることながら、企業イメージの失墜、対応する従業員の精神的苦痛など、想像もしなかった（二次的な）損害が発生することとなる。セキュリティ対策に完璧なものは存在しないが、必要な対策は実施すべく、経営層には適切な判断をしていただけるようお願いしたい。

謝辞：本調査を実施するにあたり、多くの企業のご担当者様に多大なご理解とご協力をいただきました。ここに、感謝の意を表します。

別紙1 重要システム停止による売上への影響度の考え方

企業において重要な情報システムが停止しても、ただちに売上がすべてなくなるわけではなく、その時間が短かければ売上には全く影響しない可能性もある。そこで、システムが停止していても売上減少を及ぼさないですむ時間を「許容停止時間」として、システム停止時間が許容停止時間を超過すると、売上への影響度（売上減少額／売上額）がゼロから a に推移すると仮定し、a を「重要な情報システム停止時の売上への影響度」とする。売上への影響度はその後さらに変動する可能性もあるが、簡略化のため、ここでは a のまま一定とする。



システム停止時間 ≤ 許容停止時間 の場合

$$\text{売上減少分} = 0 \quad \rightarrow \quad \text{売上減少分} = 0$$

システム停止時間 > 許容停止時間 の場合

$$\text{売上減少分} = \text{売上} \times a \quad \rightarrow \quad \text{売上減少分} = \text{売上} \times a$$

a の算出にあたっては、「情報セキュリティ対策の取組状況に関するアンケート調査」¹²（経済産業省）の回答企業における「主要な情報システムが 24 時間停止した時の売上への影響度」の平均値を用いることとした。その結果、大手・中堅企業は 38.0%、中小企業は 34.0%と設定した。

また、同経済産業省調査によると、それぞれの「システム停止時間」のケースにおいて「許容停止時間」を超えると回答した企業の比率は次の表のようになる。例えば、大手・中堅企業において 1 時間以内のシステム停止で売上に影響がある企業は 15.3%となる。

表 付 1-1 「システム停止時間」が「許容停止時間」を超えると回答した企業の比率

| システム停止時間 | 1 時間以内 | 半日以内 | 1 日以内 | 数日以内 | それ以上 |
|----------------------|--------|-------|-------|-------|--------|
| 大手・中堅企業 (300 人以上) | 15.3% | 45.9% | 76.4% | 98.7% | 100.0% |
| 中小企業 (300 人未満) | 12.7% | 37.3% | 66.5% | 95.8% | 100.0% |

¹² http://www.meti.go.jp/policy/netsecurity/sec_gov-TopPage.html

同調査を踏まえると、許容停止時間が数日超で売上に 100%の影響があることから、「重要な情報システム停止時間毎の売上への影響度」を、表付 1-1 の値に a を乗じて下記のとおり設定した。なお、数日 = 3 日と仮定した。

表 付 1-2 重要な情報システム停止時間毎の売上への影響度

| システム停止時間 | ～半日以内 | 半日超～1 日以内 | 1 日超～3 日以内 | 3 日超～ |
|----------------------|-------|-----------|------------|-------|
| 大手・中堅企業 (300 人以上) | 5.8% | 17.4% | 29.0% | 38.0% |
| 中小企業 (300 人未満) | 4.3% | 12.7% | 22.6% | 34.0% |

本研究会のモデルでは、表 付 1-2 をもとに、個票ごとにシステム停止時間から売上への影響度を設定し、逸失売上を算出した。

別紙2 コンピュータウイルスに関する被害状況調査アンケートの概要

3章に示したウイルス被害額算出モデルを踏まえ実施された、企業等を対象としたアンケート調査の概要を以下に示す。アンケート調査の詳細については、「国内におけるコンピュータウイルス被害状況調査報告書」を参照のこと。

(1) 調査対象

本調査は、全国の企業及び自治体 6,561 件を調査対象として実施した。その内訳は、全国の企業 5,500 件、全国の自治体 1,061 件となっている。

| | |
|------|---|
| 標本数 | 6,561 件 (うち、企業 5,500 件、自治体 1,061 件) |
| 標本台帳 | ①企業 ・「情報処理実態調査」対象機関 ・株式会社 東京商工リサーチ (上記の抽出機関の補足) ②自治体 ・財団法人地方自治情報センター |
| 抽出方法 | ①企業 業種別、従業員規模別無作為抽出 ②自治体 都道府県 (47 都道府県) 特別区 (東京 23 区) 市町村 人口規模別無作為抽出 |

(2) 調査期間

調査実施期間：2006 年 3 月

調査対象期間：2005 年 1 月～12 月

(3) 調査方法

郵送調査法 (郵送留置、郵送回収)

(4) 回収結果

発送総数 6,561 件に対し、企業 1,206 件、自治体 495 件、計 1,701 件の有効回答 (25.9%) が得られた。

なお、アンケートにおける企業の有効回答 1,206 件のうち、ウイルスに感染したケースは大手・中堅 110 件、中小 95 件、計 205 件 (18%) であった。

別紙3 国内の被害総額の推計方法

参考までに、ウイルス被害額算出モデルを用いた国内の被害総額の算出方法を示す。

国内総被害額は、以下の式の通り、カテゴリ（本調査では従業員規模）別に、ウイルスに感染した1企業あたりの算出項目毎の平均被害額を、国内の総インターネット利用企業数に乘じ、さらにウイルス感染時のECシステムや重要システムの停止などの被害率を算出項目毎に乘じて被害額を推計し、その総計をとることで算出可能である。

$$\boxed{\text{国内ウイルス被害総額}} = \sum_{\text{算出項目}} (\boxed{\text{算出項目毎ウイルス被害額}})$$

$$\boxed{\text{算出項目毎のウイルス被害総額}}$$

$$= \sum_{\text{カテゴリ}} (\boxed{\text{1企業あたり算出項目毎平均被害額}} \times \boxed{\text{インターネット利用企業数}} \times \boxed{\text{被害率}})$$

$$= \sum_{\text{カテゴリ}} (\boxed{\text{1企業あたり算出項目毎平均被害額}} \times (\boxed{\text{国内企業数}} \times \boxed{\text{インターネット利用率}}) \times \boxed{\text{被害率}})$$

ウイルス被害額算出モデルに基づき、アンケート調査結果（別紙2参照）や既存の公表データから試算した結果、ウイルスに感染し被害を受けた1企業あたりの算出項目毎の平均ウイルス被害額（年ベース）は下記の通りである。

表付3-1 ウイルスに感染した1企業あたりの算出項目毎の平均ウイルス被害額（年ベース）

| カテゴリ | 中小企業 (従業員300人未満) | 大手・中堅企業 (従業員300人以上) |
|---------------------|---|--|
| 費目 | | |
| 復旧に要したコスト | | |
| システム復旧コスト | | |
| システム復旧に係る人件費 | 37千円 (95社) | 64千円 (110社) |
| 外注費 | 3,000千円 (1社) | 0円 (0社) |
| 代替ハードウェア・ソフトウェア購入費 | 1,143千円 (7社) | 1,750千円 (4社) |
| データ復旧コスト | 19千円 (95社) | 25千円 (110社) |
| ウイルス被害による逸失売上 | | |
| EC停止による売上減分 | 15,461千円 (3社) | 72,531千円 (2社) |
| 重要システム停止による 売上減分 | (サーバ停止) 3,929千円 (17社) (ネットワーク停止) 1,316千円 (24社) | (サーバ停止) 27,456千円 (21社) (ネットワーク停止) 130,880千円 (40社) |

注1) () 内は、算出対象企業数

注2) なお、逸失売上についての有効数字は百万円単位だが、計算の便宜上千円単位を用いた。

「重要システム停止による売上減分」は、大手・中堅企業の方が売上額が大きい上に、IT・ネットワークへの依存が進んでいてシステム停止による売上への影響度が高いため、大手・中堅企業の逸失売上が中小企業を大きく上回る結果となった。

なお、参考までに、国内企業数、インターネット利用率および被害率（アンケート回答企業における被害発生企業の割合）、人件費単価のデータを以下に掲載する。

表 付 3-2 国内企業数・インターネット利用率

| カテゴリ | 中小企業 (従業員 300 人未満) | 大手・中堅企業 (従業員 300 人以上) |
|------------------|-----------------------|--------------------------|
| 国内企業数 (注 1) | 1,517,978 社 | 11,638 社 |
| インターネット利用率 (注 2) | 77.2% | 98.4% |

注 1) 総務省「平成 16 年事業所・企業統計」より導出

注 2) 総務省「平成 16 年通信利用動向調査」および中小企業金融公庫「中小企業の情報化と電子商取引」(2005 年 12 月)よりインターネット利用率を導き、業種に依らず一律に適用

表 付 3-3 算出項目毎のウイルス被害率

| カテゴリ | 中小企業 (従業員 300 人未満) | 大手・中堅企業 (従業員 300 人以上) |
|------------------------|---------------------------------|---------------------------------|
| 復旧に要したコスト | | |
| システム復旧コスト | | |
| システム復旧に係る人件費発生率 | 14.2% | 22.3% |
| 外注費 発生率 | 0.1% | 0.0% |
| 代替ハードウェア・ソフトウェア購入費 発生率 | 1.0% | 0.8% |
| データ復旧コスト 発生率 | 14.2% | 22.3% |
| ウイルス被害による逸失売上 | | |
| EC 停止 被害率 | 0.4% | 0.4% |
| 重要システム停止 被害率 | (サーバ停止) 2.5% (ネットワーク停止) 3.6% | (サーバ停止) 4.3% (ネットワーク停止) 8.1% |

表 付 3-4 時間あたり人件費単価

| カテゴリ | 中小企業 (従業員 300 人未満) | 大手・中堅企業 (従業員 300 人以上) |
|---------------------------------------|-----------------------|--------------------------|
| 時間あたり人件費単価 (システム管理部門) (円/時間) (注 1) | 1,659 円 | 1,659 円 |
| 時間あたり人件費単価 (全従業者) (円/時間) (注 2) | 2,247 円 | 2,247 円 |

注 1) 「厚生労働省賃金構造基本統計調査 平成 16 年」より「電子計算機オペレーター」の金額を企業規模・業種に依らず一律に適用。

「厚生労働省賃金構造基本統計調査 平成 16 年」より全労働者に関する金額を企業規模・業種に依らず一律に適用。