

「被害額算出モデル」報告書

2003年 3月

情報処理振興事業協会

セキュリティセンター

目次

1. 調査の背景と目的	1
1.1 調査の背景	1
1.2 調査の目的	2
2. 調査の概要	3
2.1 調査項目	3
2.2 調査手段	4
3. 被害額算出モデルの設計に関する検討	6
3.1 昨年度モデルからの改良の視点	6
3.2 本年度モデルの新機軸	7
3.3 本年度モデルの構造（算式）	12
3.4 モデルの妥当性の検証	15
4. 各種パラメータ等の導出	18
4.1 表面化被害額関連	18
4.2 潜在化被害額関連	21
4.3 業種別・事業所規模別グループ分類	24
5. 業種別・事業所規模別の被害推計モデル構築と被害額試算	26
5.1 業種別・事業所規模別のモデル構築	26
5.2 インシデント被害の規模に着目した推計	29
5.3 有効回答事業所ベースの被害額試算	30
6. 国内被害総額の推計と比較検証	31
6.1 国内被害総額の推計	31
6.2 推計結果の比較検証	33
6.3 残された課題	35
付属資料	37

付.1 業種・事業所規模グループ別セキュリティインシデント被害額.....	37
付.2 ヒアリング調査結果.....	40

1. 調査の背景と目的

1.1 調査の背景

2001年9月に米国で発生した同時多発テロ等を契機として、サイバーテロの防止あるいは重要インフラのセキュリティに対する関心が世界規模で高まっている。これに伴い、我が国の基幹産業に携わっている企業やIT関連企業におけるセキュリティインシデント（コンピュータウイルスによる被害）に係る実態把握の必要性が、ますます強く認識されるようになってきている。

実態把握の第一歩として、セキュリティインシデントによる被害額の把握が重要であることは言を待たない。被害の大きさを適切に金額評価することなしには、経済社会に対するその影響の度合い（深刻度）を把握することができず、その結果として、セキュリティインシデントへの対応策にどれだけの労力とコストが必要かを判断することができないからである。

適切な被害額の推計には、より精緻な推計モデルが必要とされる。ここでいうモデルとは、セキュリティインシデントの発生からシステム復旧及び業務正常化までの事態の流れを現実に即して再現し、その過程で発生し得る各種コスト（損失）を多面的に把握・算定する仕組みを指す。モデルの構築は、言い換えれば、セキュリティインシデントの発生、それへの対応、及びそこで発生するコストの内容を主要なファクターに還元し、簡潔に表現することである。よって、その作業を通じて、セキュリティインシデントの実態を的確に把握するための着眼点や知見が整理された形で抽出されることになる。これは、セキュリティインシデントに係るリスクマネジメントを確立する上で不可欠の情報である。

ところが、これまで我が国ではこうした情報の蓄積が必ずしも十分でなかったことから、セキュリティインシデントによる国内被害額について信頼に足る推計値が得られなかった。そのため、情報処理振興事業協会は平成13年度に「情報セキュリティインシデントに関する調査」（以下「昨年度調査」と略記する）を実施し、国内被害に関する情報収集と、被害額算出モデルの試作と検討を行った。この調査は、セキュリティインシデントの国内実態把握の端緒として非常に大きな意味をもつものであった。そして現在、より詳細な事態把握と、それを踏まえた被害額算出モデルの精緻化が求められているところである。

1.2 調査の目的

本調査は上述の「調査の背景」を踏まえて実施されるものであり、その目的は次の 2 点である。

IT ユーザー事業所が自己のセキュリティインシデント被害額を簡便に事後算定あるいは予測することを可能とするために、昨年度調査で作成された被害額算出モデルをベースとして、より精緻化されたモデルを構築すること。
構築したモデルを用いて、実際に、我が国のセキュリティインシデント被害額（国内被害総額）を推計すること。

なお、被害額算出モデルの精緻化に関しては、その妥当性を客観的かつ的確に評価するため、実際にセキュリティインシデントを経験した事業所を中心としたヒアリング調査を実施することとした。

また、被害額の推計に必要な各種原単位・パラメータについては、国内事業所に対するアンケートを通じて得られたデータより推計することとした。

2. 調査の概要

2.1 調査項目

2.1.1 被害額算出モデルの設計に関する検討（→ 第3章）

昨年度調査の被害額算出モデルの設計をベースとして、本調査で構築するプロトタイプモデルの構造について、「モデル構築目的の明確化」及び「推計精度の向上」という観点から検討する。その上で、本調査における被害額算出モデルの具体的な構造を提案する。

なお、モデルは業種別・事業所規模別（事業所の従業員規模別）のグループごとに作成する。グループ分けの基本的な根拠は業種別・事業所規模別のアンケート回収数であり、各グループに一定のサンプル数が確保されるようにグルーピングする。ただし、この場合、被害額の推計に用いるパラメータ（後述）がグループごとに顕著に異なる保証はない。パラメータ計算の結果、たとえあるグループと別のグループのパラメータが比較的近い値となることが判明した場合でも、業種別・事業所規模別の被害額を個別に推計した上でそれらを合計して総額を出すというプロセスを重視する立場から、グループは統合せず当初のグルーピングをそのまま推計に用いることとする。

2.1.2 アンケートからの各種原単位・パラメータの導出（→ 第4章）

被害額算出モデルによる推計に必要な各種の原単位あるいはパラメータを、アンケートで得られたデータから算定する。原単位・パラメータとは、被害額の積み上げ推計を行う際にモデルに与える、時間当たり人件費単価やシステム停止時間、IT依存業務割合等のことである。

本調査では、便宜上、事業所（あるいは企業）ごとに設定する数値を「原単位」と呼び、事業所（あるいは企業）を問わず業種別・事業所規模別グループに共通の数値として与えるものを「パラメータ」と呼ぶこととする（よって、厳密な概念定義に基づく用語の使い分けではない）。

2.1.3 業種別・事業所規模別の被害額算出モデルの構築と被害額推計（→ 第5章）

ここまでの作業で設定したグループ、原単位、パラメータ等に基づき業種別・事業所規模別の被害額推計モデルを構築し、実際に被害額の推計を行う。例えば、業種区分×事業所規模区分の組み合わせ（すなわちグルーピング）が計9パターンであれば、被害額算出

モデルも 9 パターンを用意することとなる（後述のように、実際には 4 パターンのモデルを構築することとなった）。

アンケートでは、客体に対して、セキュリティインシデントに係るデータを大規模（事業所全体に及ぶ被害）、中規模（部署または課全体に及ぶ被害）、小規模（少数のパソコンに及ぶ被害）の別に返答するよう求めている。そのため、どのパターンのモデルにおいても、大・中・小の規模別に被害額を推計することができるようにした。

2.1.4 国内被害総額の推計と比較検証（→ 第 6 章）

上述の業種別・事業所規模別被害額の推計結果に基づいて、国内被害総額の推計を行う。推計手順は、基本的には、年間のセキュリティインシデント 1 事業所当たりの被害額に、別途算定される年間のセキュリティインシデント発生割合と、国内事業所総数を乗じることによる膨らまし推計である。

膨らまし推計によって国内被害総額の推計値が得られたら、それを米国等で公表されている類似の調査結果と比較し、その妥当性に関する検討を行う。

最後に、セキュリティインシデント被害額推計のさらなる精緻化に向けた課題について、ヒアリングの結果等を踏まえて整理する。

2.2 調査手段

2.2.1 アンケート調査（国内ウイルス被害状況調査の一部として同時に実施）

目 的

上述の 2.1.2 ~ 2.1.4 までの作業、すなわち、アンケートからの各種原単位・パラメータの導出、業種別・事業所規模別の被害額算出モデルの構築と被害額推計、及び国内被害総額の推計と比較検証に必要な各種データ・情報を収集すること。

対 象

事業所規模別に層化無作為抽出された国内の 4,000 事業所。

調査期間

平成 15 年 2 月

調査方法

調査票による郵送回収・郵送回収調査方式。

回収実績

有効回答数：1,096（有効回収率 27.4%）

2.2.2 ヒアリング調査

目的

被害額算出モデルの構造が、セキュリティインシデントの発生からシステム復旧及び業務正常化までの事態の流れにマッチしているかどうかについて、実際にセキュリティインシデントを経験した事業所等のコメントを踏まえて検証すること。

さらに、セキュリティインシデントの管理・報告体制、発生・被害状況に関する業種別・事業所規模別の違いについて分析すること。

対象

下記の5事業所とした。

- 1) A事業所（建設・製造業、99名以下）
- 2) B事業所（建設・製造業、100名以上）
- 3) C事業所（第3次産業、99名以下）
- 4) D事業所（第3次産業、100名以上）
- 5) E事業所（経営多角化、100名以上）

実施期間

平成15年2月

3. 被害額算出モデルの設計に関する検討

3.1 昨年度モデルからの改良の視点

3.1.1 モデル構築目的の明確化

昨年度調査では、被害額算出モデル構築の目的に関する検討が必ずしも具体的ではなく、特に、誰が、何のために利用するモデルであるかという点がやや曖昧であった。この点に関して、本調査は次のように考える。

「IT ユーザー事業所が被害額推計モデルの利用を通じて比較的簡便に、自己で発生した情報セキュリティインシデントの被害額を測定あるいは予測することを可能とすることにより、各社の情報セキュリティ対策（リスクマネジメント）の立案に寄与すること。」

昨年度調査の報告書においても指摘されているとおり、モデル利用の目的に応じて、モデルの構造や被害額の推計に必要なデータ（原単位・パラメータ）は異なる。本調査では、被害額推計モデル構築の目的を上記のように定めた上で、その達成に向けたモデルのあり方を検討し、実際にプロトタイプモデルを構築する。

本調査のセキュリティインシデント被害額算出モデルの基礎となるのは、昨年度調査で試作的に開発された被害額算出モデルである。本調査では、これに以下で述べる観点からの再検討と改訂を加え、より精緻化されたプロトタイプモデルの構築を目指す。

3.1.2 推計精度の向上

昨年度報告書では、昨年度調査を「セキュリティインシデントに係る被害額・投資額の調査の第一歩として行われたもの」と位置づけており、推計方法の確立に向けた端緒を作ることにより重点が置かれていた。本年度調査では、昨年度の成果をベースとして、被害額推計モデルをユーザにとって使い勝手の高いものへと改良していくことが求められる。そのためには、昨年度調査において残された課題である、(1) 推計方法の精度向上、(2) 調査対象業種の偏りと調査対象企業数の少なさの是正、及び(3) 調査負荷の軽減が必要となる。

以下に、被害額算出モデルの推計精度向上に向けた具体的な対応策（新機軸）を述べるが、これらは上記(1)～(3)へのアプローチを念頭に置いたものである。

3.2 本年度モデルの新機軸

3.2.1 昨年度モデルの構造

本調査で構築する被害額算出モデルは、基本的に、昨年度モデルをベースとする。そこで、本年度モデルの改良点（新機軸）について検討する前に、昨年度モデルの構造を確認する。概略は以下のとおりである。

なお、昨年度モデルが推計対象としたのは、セキュリティインシデントの1次的（直接的）被害であったことから、以下でも1次的被害に限定して述べる。

基本算式

$$\text{インシデント被害額（1次的被害額）} = \text{表面化被害額（円）} + \text{潜在化被害額（円）}$$

「表面化被害額」とは、インシデント被害の結果として生じる損失ないしは出費であり、その規模が金額として明確に認識できるものである。

他方、「潜在化被害」とは、インシデントによる被害ではあるものの、その影響が具体的な損失・出費の金額としては表出しにくいものを指す。システムダウンによる業務効率の低下等がこれに該当する。

表面化被害額

$$\text{表面化被害額} = \text{逸失利益（円）} + \text{復旧に要したコスト（円）}$$

「逸失利益」とは、システムないしはネットワークがインシデントにより停止していなければ得られていたであろう利益金額であり、次の算式で示される。

$$\text{逸失利益} = \text{時間当たり利益（円/時間）} \times \text{システム停止時間（時間）}$$

ここで、「時間当たり利益」は、1時間あたりに換算した利益額である。また、「システム停止時間」とは、インシデントによりシステムないしはネットワークが停止していた時間の長さである。

他方、「復旧に要したコスト」とは、セキュリティインシデントに見舞われたシステムの復旧に要する出費（人件費、ハードウェア、ソフトウェア）を指すが、昨年度モデルでは具体的な算式は示されなかった。

$$\boxed{\text{復旧に要したコスト}} = \boxed{\text{人件費・ハードウェア・ソフトウェア}} \text{ (円)}$$

潜在化被害額

$$\boxed{\text{潜在化被害額}} = \boxed{\text{固定費（人件費）}} \text{ (円/人・時間)} \times \\ \boxed{\text{インシデントによる影響を受けた人数}} \text{ (人)} \times \boxed{\text{システム停止時間}} \text{ (時間)} \times \\ \boxed{\text{IT 感応度（業務依存度）}}$$

「固定費（人件費）」とは、インシデントによる影響を受けた従業員 1 人当たり、かつ 1 時間当たりの人件費単価である。

「インシデントによる影響を受けた人数」とは、インシデントの被害を受けたのがクライアント PC であれば、その台数を該当データとする。インシデント被害を受けたのがメールサーバやファイルサーバ等のサーバ類の場合には、そのサービスを利用している人数を該当データとする。

「IT 感応度」とは、インシデントを受けたシステムないしネットワークが、業務に対してどれだけの影響度をもつかを、0~1 の範囲で表す係数である。システムやネットワークへの業務の依存度が高いほど、この係数の値は高まることから、業務のシステム依存度と言い換えてもよい。例えば、システムやネットワークを利用すれば 1 時間で 100 件処理できたものが、利用しなかったときに 80 件しか処理できなかった場合、この業務のシステム依存度（IT 感応度）は 0.2 と考える。

3.2.2 本年度モデルの新機軸

上述の昨年度モデルの構造に対して、本年度調査における新しい被害額算出モデルについては、以下の点からその基本構造を見直し、改良することとしたい。その概要は図表 3 - 1 に図示されているとおりである。

表面化被害に関する改善

表面化被害については、昨年度と同様に推計対象を 1 次的被害（直接的被害）に限定す

る。改善点としては、システム復旧コストについて、昨年度モデルがただ「復旧に要したコスト」としていたのに比べて、本調査では「時間当たり人件費」、「システム復旧時間」及び「復旧に携わった IT 担当者数」の積に、代替ハード購入費を加えた額として定式化していることが挙げられる。

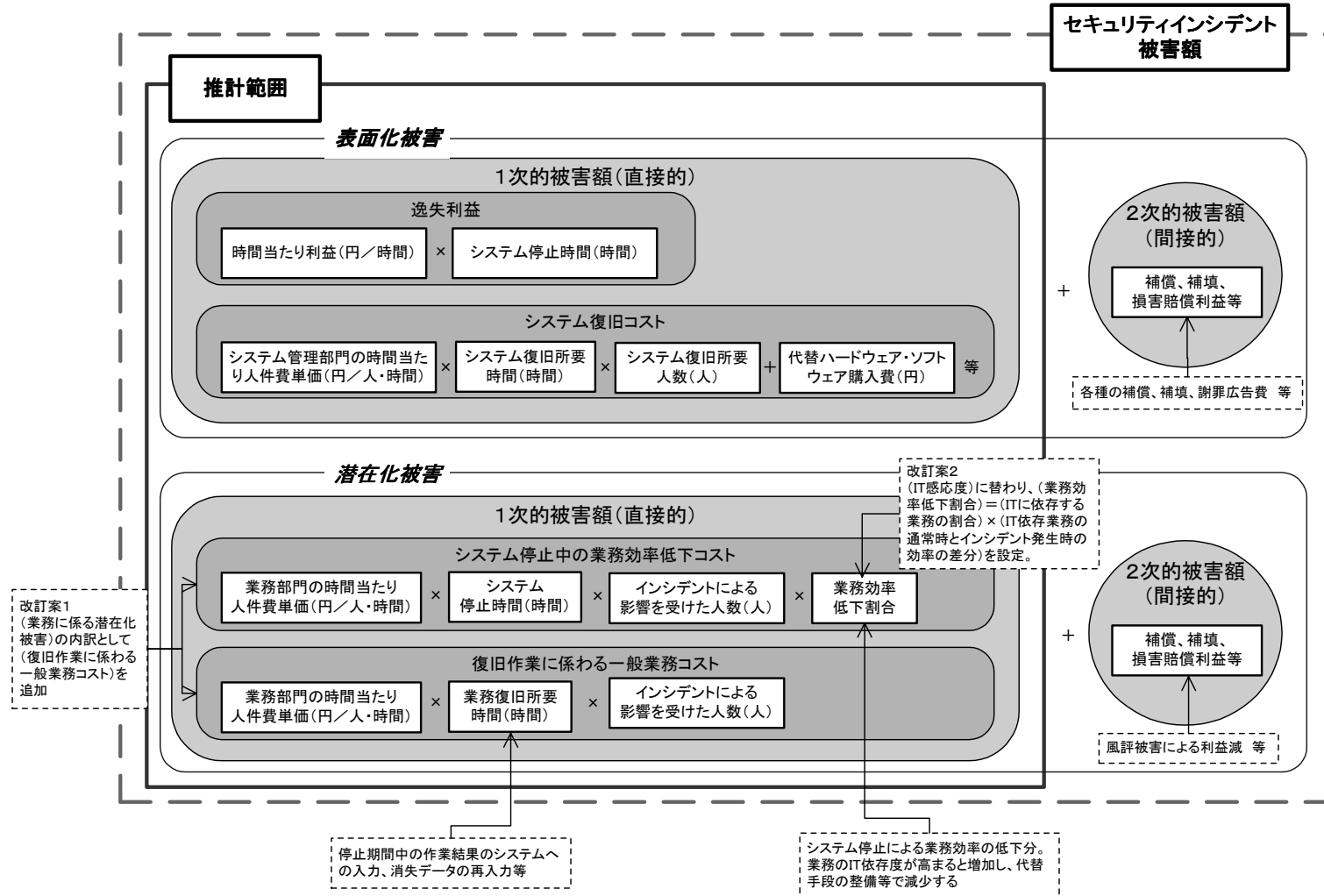
潜在化被害に関する改善

1) 復旧に係わる一般業務コストの追加

昨年度調査の特徴点は、ビジネス機会の損失や追加人件費の発生等でコストが明らかに目に見える表面化被害にとどまらず、業務効率（生産性）の低下等目に見えにくい潜在化被害までも推計の対象としたところにある。本年度調査でもこの方向性を重視し、潜在化被害のより詳細な把握に努めることとする。具体的には、推計対象を 1 次的被害に限る点では昨年度モデルと同様であるが、1 次的被害に「復旧に係わる一般業務コスト」を追加する点が新機軸である（図表 3 - 1 中の改訂案 1）。

これは、システム停止時間中におけるコンピュータによらない（マニュアル）作業の結果のシステム入力や、システム停止に伴う消失データの再入力等によって発生するコストである。金融機関（銀行）のシステムダウンの事例に見られるように、システム停止中においても企業は顧客に対して電話やファクス等を用いてサービスを提供する。本年度モデルは、この復旧に係わる一般業務コストを、「時間当たり人件費」、「業務復旧時間」及び「インシデントによる影響を受けた人数」の積として求める。

図表3-1 本年度モデルの基本構造と改良点



2) システム停止中の業務効率低下コストの推計における「業務効率低下割合」パラメータの新規導入

他方、潜在化被害におけるシステム停止中の業務効率低下コストについては、昨年度調査で被害額推計に用いられていた「IT 感応度」に替わって、本調査では「業務効率低下割合」を用いることとした（図表3 - 1中の改訂案2）。

IT 感応度については、比較的簡便に信憑性の高いパラメータを算定することが困難であった。信憑性を高めるための手段としては、パラメータの算定ベース（すなわちサンプル数）を増やし、より統計的に厳密な平均値を求めることが挙げられる。そのためには、アンケートにおいて回答者（事業所）が回答しやすいように工夫してパラメータ算定用データを多く入手することが肝要である。昨年度調査における IT 感応度という回答しづらい概念を、「IT に依存する業務の割合」と「IT 依存業務の通常時とインシデント発生時の効率の差分（効率低下幅）」に要因分解した上で、個別に事業所からの回答を求めることにより、回答をより容易にすることが可能となる。

業務効率低下割合は、上記の IT 依存業務割合と IT 依存業務のインシデント発生時の効率低下幅の積として求められる。その考え方（根拠）は下記【参考】のとおりである。

【参考：業務効率低下割合の考え方】

事業所内の業務を IT に依存した業務と依存しないものに分けて考えると、IT に依存した業務の場合は、システム停止中は電話やファクス等システムを使用しない方法を選択して業務を継続せざるを得ず、その分効率は低下してしまう（通常時の効率を A とし、インシデント発生時の効率を B とすれば、 $B < A$ となる）。

一方、IT に依存しない業務の場合はシステムの有無とは無関係なので、通常時もインシデント発生時も業務効率は不変となる。

	通常時の効率	インシデント発生時の効率
IT に依存した業務	A	B (< A)
IT に依存しない業務	C	C

ここで、事業所の業務全体のうちの IT 依存割合を α とおくと、下記のようなになる。

$$\text{通常時の業務効率} = A \times \alpha + C \times (1 - \alpha) \dots\dots\dots (1)$$

$$\text{インシデント発生時の業務効率} = B \times \alpha + C \times (1 - \alpha) \dots\dots\dots (2)$$

求めたい業務効率の低下比率は、通常時の業務効率に対するインシデント発生時の業務

効率低下分であるから、

$$\text{業務効率の低下比率} = \frac{\text{通常時の業務効率} - \text{インシデント発生時の業務効率}}{\text{通常時の業務効率}}$$

となり、式(1)及び(2)より、下記のようになる。

$$\begin{aligned}\text{業務効率の低下比率} &= \frac{\{A \times \alpha + C \times (1 - \alpha)\} - \{B \times \alpha + C \times (1 - \alpha)\}}{\{A \times \alpha + C \times (1 - \alpha)\}} \\ &= \frac{A \times \alpha + C - C \times \alpha - B \times \alpha - C + C \times \alpha}{\{A \times \alpha + C \times (1 - \alpha)\}} \\ &= \frac{A \times \alpha - B \times \alpha}{\{A \times \alpha + C \times (1 - \alpha)\}} \dots\dots\dots (3)\end{aligned}$$

また、最終的に求めたいのは通常時の業務効率がインシデント発生時にどの程度低下するかの割合であり、必ずしも通常時の業務効率の水準を求める必要は無い。

したがって、通常時の業務効率を1 (= 100%) とおくと、(3)式より、

$$\text{業務効率の低下比率} = \alpha \times (A - B)$$

となる。

すなわち、「業務効率低下割合」は、「IT に依存する業務の割合」と「IT 依存業務の通常時とインシデント発生時の効率の差分」を乗じたものであると定義することができる。

3.3 本年度モデルの構造（算式）

昨年度モデルの構造を踏まえた本年度モデルに関するここまでの検討を踏まえて、本年度モデルの構造を以下のように定式化することとした。

3.3.1 基本算式

$$\boxed{\text{インシデント被害額 (1 次的被害額)}} = \boxed{\text{表面化被害額}} (\text{円}) + \boxed{\text{潜在化被害額}} (\text{円})$$

基本算式は昨年度モデルと同様である。すなわち、まず「表面化被害額」は、インシデント被害の結果として生じる損失ないしは出費であり、その規模が金額として明確に認識

できるものである。他方、「潜在化被害額」は、インシデントによる被害ではあるものの、その影響が具体的な損失・出費の金額としては表出しにくいものを指す。

なお、推計対象を 1 次的被害（直接的被害）額に限定しているという点でも、本年度モデルは昨年度モデルと同様である。

3.3.2 表面化被害額

$$\text{表面化被害額} = \text{逸失利益} (\text{円}) + \text{システム復旧コスト} (\text{円})$$

「逸失利益」は、システムないしはネットワークがインシデントにより停止していなければ得られていたであろう利益金額であり、次の算式で示される。

$$\text{逸失利益} = \text{時間当たり利益} (\text{円/時間}) \times \text{システム停止時間} (\text{時間})$$

ここで、「時間当たり利益」は、1 時間あたりに換算した利益額である。また、「システム停止時間」とは、インシデントによりシステムないしはネットワークが停止していた時間の長さである。

他方、「システム復旧コスト」は、本年度モデルにおける新しい定式化部分である。システム復旧コスト自体は、昨年度モデルにおける「復旧に要したコスト」と同義であり、セキュリティインシデントに見舞われたシステムの復旧に要する出費（人件費、ハードウェア、ソフトウェア）を指す。今年度モデルの特徴は、それを、下記の算式で計測する点にある。

$$\begin{aligned} \text{システム復旧コスト} = & \text{システム管理部門の時間あたり人件費単価} (\text{円/人・時間}) \times \\ & \text{システム復旧所要時間} (\text{時間}) \times \text{システム復旧所要人数} (\text{人}) + \\ & \text{代替ハードウェア・ソフトウェア購入費} (\text{円}) \end{aligned}$$

ここで、「システム管理部門の時間あたり人件費単価」とは、インシデントによるトラブルを解消する（つまりシステムを復旧する）ための作業に投入されるシステム管理部門スタッフ 1 人当たり、かつ 1 時間当たりの人件費単価である。

「システム復旧所要時間」は、インシデントによるシステムの停止からそのリスタートまでの時間の長さである。

「システム復旧所要人数」は、インシデントによるトラブルを解消する（つまりシステムを復旧する）ための作業に投入されるシステム管理部門スタッフの延べ人数である。

「代替ハードウェア・ソフトウェア購入費」は、システム復旧に際して新たに購入しなければならなかったハード及びソフトの購入コストである。

3.3.3 潜在化被害額

$$\text{潜在化被害額} = \text{システム停止中の業務効率低下コスト} (\text{円}) + \text{復旧作業に係わる一般業務コスト} (\text{円})$$

この算式に示されているように、本年度モデルでは、潜在化被害額が「システム停止中の業務効率低下コスト」と「復旧作業に係わる一般業務コスト」の2つからなっている。昨年度調査における潜在化被害額は、前者（システム停止中の業務効率低下コスト）のみであったが、本年度モデルでは新たに「復旧作業に係わる一般業務コスト」を推計対象に追加する。

まず、「システム停止中の業務効率低下コスト」の算式は次のとおりである。

$$\text{システム停止中の業務効率低下コスト} = \text{業務部門の時間あたり人件費単価} (\text{円} / \text{人} \cdot \text{時間}) \times \text{システム停止時間} (\text{時間}) \times \text{インシデントによる影響を受けた人数} (\text{人}) \times \text{業務効率低下割合}$$

ここで、「業務部門の時間あたり人件費単価」とは、インシデントによるトラブルに見舞われた業務部門（現場）のスタッフ1人当たり、かつ1時間当たりの人件費単価である。また、「システム停止時間」は、インシデントによりシステムないしはネットワークが停止していた時間の長さである。

「インシデントによる影響を受けた人数」の定義は、昨年度モデルのそれと異なっている。昨年度の定義では、インシデントの被害を受けたのがクライアントPCであれば、その台数を該当データとし、被害を受けたのがサーバであれば、それを利用している人数を該当データとした。本年度モデルにおける「インシデントによる影響を受けた人数」は、インシデントの発生により通常業務の実施が困難ないしは不可能となった、業務部門（現場）スタッフの人数である。その具体的な推計方法については、次章で説明される。

「業務効率低下割合」は、上記の【参考：業務効率低下割合の考え方】で説明したとおり、「IT に依存する業務の割合」と「IT 依存業務の通常時とインシデント発生時の効率の差分」の積として定義されるパラメータである。このパラメータの導入が本年度モデルの新機軸の 1 つであることは既に述べたとおりである。

次に、これも本年度モデルの新機軸の 1 つである「復旧作業に係わる一般業務コスト」について説明する。これは次の算式で求められる。

$$\boxed{\text{復旧作業に係る一般業務コスト}} = \boxed{\text{業務部門の時間あたり人件費単価}} (\text{円/人・時間}) \times \boxed{\text{業務復旧所要時間}} (\text{時間}) \times \boxed{\text{インシデントによる影響を受けた人数}} (\text{人})$$

ここで、「業務部門の時間あたり人件費単価」とは、インシデントによるトラブルに見舞われた業務部門（現場）のスタッフ 1 人当たり、かつ 1 時間当たりの人件費単価である。また、「業務復旧所要時間」は、インシデントによるシステム停止に係る復旧作業を開始してからシステムが完全正常化するまでの時間の長さである。

「インシデントによる影響を受けた人数」は、インシデントの発生により通常業務の実施が困難ないしは不可能となった、業務部門（現場）スタッフの人数である（具体的推計方法は次章で説明される）。

3.4 モデルの妥当性の検証

事業所へのヒアリング調査により、下記項目に関する妥当性の検証を行った。

- ・ モデルの概念・推計対象
- ・ モデルの設計・推計式

その結果、ヒアリング調査対象となったすべての事業所が、モデルの概念や設計について「妥当である」と回答した。

3.4.1 モデルの概念・推計対象

表面化被害

被害が把握しやすい「表面化被害」に関する項目として、「逸失利益」と「システム復旧コスト」が存在することについて、すべての調査対象事業所から同意が得られた。

事業所において把握しているあるいは把握可能な被害額は、セキュリティインシデント発生時の復旧に要するシステム部門と現場部門の人的費用が主であり、本モデルで言う「表面化被害」の「システム復旧コスト」に該当する。一方、「逸失利益」については、電子商取引を行っていない、基幹システムが被害を受けたことがない事業所では生じないとの回答も見られるが、ネットワークセキュリティ関連製品・サービスの顧客となっている、セキュリティ意識の高い事業所を中心に、「逸失利益」(機会損失)は必ず生じるもので、その防止や一環としての被害額の把握への努力がなされていることが指摘された。

潜在化被害

被害が把握しにくい「潜在化被害」として、「システム停止中の業務効率低下」と「復旧作業に係る一般コスト」が存在することについては同意が得られた。

潜在化被害は、認識はされているものの、推計・把握に向けた試みはあまりなされていないのが現状である。その原因は、現場における復旧に要するコストは、本社では正確には把握しにくいことにある。

その他

2 次的被害についても認識がされているが、当面、より把握が望まれる 1 次的被害を調査対象とし、2 次的被害については将来の課題とすることについて、すべての調査対象事業所から同意が得られた。

3.4.2 モデルの設計・推計式

表面化被害

「表面化被害」に関する推計式については、すべての調査対象事業所から同意が得られた。

潜在化被害

「潜在化被害」に関する推計式については、すべての調査対象事業所から同意が得られた。ただし、「システム停止中の業務効率低下」の「業務効率低下割合」については、本来ならば、数ある現業部門から情報を収集すべきだが、事実上正確な値の算出は不可能であることが指摘され、「定義を明確にしないと感覚的なものになるが、定義を厳密にしすぎる

と回答不能になる」、「部門、職種により数値が異なるが、感覚的な数値、大まかな数値を見積もるしか方法がない」等の意見が見られた。

【参考：モデルの妥当性に関する事業所からの意見】

ヒアリング調査結果から、モデルの概念・推計対象、モデルの設計・推計式に対して、以下のような意見が出された。

図表 3 - 2 モデルの妥当性に関する事業所からの主な意見

	表面化被害	潜在化被害
モデルの概念・推計対象	<ul style="list-style-type: none"> ・同社で把握している被害は、システム部門と現業部門が対応する人件費であり、本モデルですべて網羅される。 ・推計範囲等は概ね妥当。 ・ネットワークセキュリティ関連製品・サービスの顧客は、機会損失（モデル中の「逸失利益」の部分）は必ずあると認識しており、その防止に注力している。 	<ul style="list-style-type: none"> ・「業務効率低下割合」は定義を明確にしないと感覚的なものになるが、定義を厳密にしすぎると回答不能になる点に留意する必要がある。
モデルの設計・推計式	<ul style="list-style-type: none"> ・推計式は概ね妥当。 	<ul style="list-style-type: none"> ・本来ならば、数ある現場部門から情報を収集すべきだろうが、事実上不可能と思われるので、大まかな推計になるのは致し方ないだろう。 ・部門、職種により、「ITに依存する業務の割合」や「通常時とインシデント発生時の効率の差分」は異なるが、大まかな平均値を推測することが可能。 ・特に「復旧作業に関わる一般業務コスト」はシステム部門では正確に把握できない。ただ、大規模事業所になるほど、業務復旧作業量の割合は大きくなる傾向があるだろう。

4. 各種パラメータ等の導出

前章ではモデル構造について示したが、モデル推計に際しては、モデル構造に基づき、アンケート調査や既存統計調査等から、原単位やパラメータを抽出する必要がある。本章では、本モデル推計において活用するデータ群に関する詳述を行う。

4.1 表面化被害額関連

前述の通り、表面化被害額の推計においては、「逸失利益」と「システム復旧コスト」を算出する必要がある。以下に、両要素に関し、設定すべき原単位等を示す。

4.1.1 逸失利益

逸失利益は、下式により推計される。

図表4 - 1 逸失利益の推計式

$$\boxed{\text{逸失利益}} = \boxed{\text{時間当たり利益}} \times \boxed{\text{システム停止時間}}$$

売上総利益額 ÷ (年間規定営業日数 × 1日当たり規定営業時間)

逸失利益の推計に必要な原単位等とその入手・算出方法を下表に示す。

図表 4 - 2 逸失利益の推計に必要な原単位等と入手・算出方法

原単位等	入手・算出方法
売上総利益額	<p>アンケート調査、問D 2</p> <p>未記入の場合は、下記方法により、業種別・事業所規模別にグループを分類（グループ分類方法については 1.3 節参照）、各グループの平均売上総利益額を算出し、属するグループの値を代用した。</p> <p>方法論</p> <ul style="list-style-type: none"> 業種が相対的に比較できる「経常利益」を売上総利益額に代替させた。 <p>金融業以外については、平成 13 年法人企業統計より得られる各業種別の「経常利益」を、平成 13 年事業所・企業統計調査から得られる「企業数」で除し「(a)1 社当たり経常利益」を算出。</p> <p>金融業の「経常利益」については全国銀行の決算状況（13 年度決算、日本銀行発表）より平成 13 年度の値が著しく負の値となるため、「営業純益」を代用し、同じく平成 13 年事業所・企業統計調査から得られる「企業数」で除し「(a)1 社当たり経常利益」を算出した。</p> <p>次に「企業数」と「事業所数」から「(b)1 社当たり事業所数」を算出。</p> <p>$(a) \div (b)$より各業種別の「(c)1 事業所当たり経常利益」を得る。</p> <p>(c)を各業種の事業所数による加重平均値を計算、グループの平均とした。</p> <p>注)「経常利益」において、「電気・ガス・熱供給・水道業」は法人企業統計「電気業」、「卸売・小売業、飲食店」は「卸・小売業」の値を使用。そのため、「企業数」「事業所数」において、「電気・ガス・熱供給・水道業」は事業所・企業統計「35 電気業」の値、「卸売・小売業、飲食店」は「48～53 卸売業」と「54～59 小売業」の合計値、また「金融業」は銀行と信託銀行等のみの決算状況であるので、事業所・企業統計「62 銀行・信託業」を使用した。</p>
年間規定営業日数	<p>アンケート調査、問D 3（前）</p> <p>未記入の場合は、属する業種別・事業所規模別グループ内の回答の平均値を代用した。</p>
1 日当たり規定営業時間	<p>アンケート調査、問D 3（後）</p> <p>未記入の場合は、属する業種別・事業所規模別グループ内の回答の平均値を代用した。</p>
システム停止時間	<p>アンケート調査、問D 4 - B</p>

4.1.2 システム復旧コスト

システム復旧コストは下式により推計される。

図表 4 - 3 システム復旧コストの推計式

$$\boxed{\text{システム復旧コスト}} = \boxed{\text{時間当たり人件費}} \times \boxed{\text{システム復旧時間}} \\ \times \boxed{\text{復旧に携わったIT担当者数}} + \boxed{\text{代替ハード・ソフト購入費}}$$

各原単位等の入手・算出方法を下表に示す。

図表 4 - 4 システム復旧コストの推計に必要な原単位等と入手・算出方法

原単位等	入手・算出方法
時間当たり人件費*	<p>= システム管理部門の時間当たり人件費単価。</p> <p>平成 13 年厚生労働省賃金構造基本統計調査の職種別分類「システム・エンジニア」「プログラマー」「電子計算機オペレーター」の「年間給与総額」「年間労働時間」を「労働力人口」による加重平均値を「システム部門」とした。</p> <p>「年間給与総額」÷「年間労働時間」÷「労働力人口」により、「時間当たり人件費」を算出した。</p> <p>注) 業種別の値がないため、グループ 1、3 は賃金構造基本統計調査の事業所規模「10～99 人」の値、グループ 2、4 は事業所規模「100～999 人」と「1000 名以上」の「労働力人口」による加重平均値により計算した。</p>
システム復旧時間	アンケート調査、問 D 4 - C
システム復旧所要人数	アンケート調査、問 D 4 - D
代替ハード・ソフト購入費	アンケート調査、問 D 4 - E

注) *印のある原単位・パラメータは、事業所ごとにではなく、業種・事業所規模グループごとに設定するものを示す。

4.2 潜在化被害額関連

潜在化被害額の推計においては、「システム停止中の業務効率低下」と「復旧作業に係る一般業務コスト」を算出する必要がある。以下に、両要素に関し、設定すべき原単位等を示す。

4.2.1 システム停止中の業務効率低下コスト

システム停止中の業務効率低下コストは、下式により推計される。

図表4 - 5 システム停止中の業務効率低下コストの推計式

$$\begin{aligned} \boxed{\text{システム停止中の業務効率低下}} &= \boxed{\text{時間当たり人件費}} \times \boxed{\text{システム停止時間}} \\ &\times \boxed{\text{インシデントによる影響を受けた人数}} \\ &\underbrace{\times \text{システム復旧所要人数} \times \text{業務復旧作業量対システム復旧作業量比率}} \\ &\times \boxed{\text{業務効率低下割合}} \\ &\underbrace{\times \text{IT依存業務割合} \times \text{IT依存業務のインシデント発生時の効率低下幅}} \end{aligned}$$

システム停止中の業務効率低下コストの推計に必要な原単位等とその入手・算出方法を下表に示す。

図表 4 - 6 システム停止中の業務効率低下コストの推計に必要な原単位等と入手・算出方法

原単位等	入手・算出方法
時間当たり人件費*	<p>= 業務部門の時間当たり人件費単価。</p> <p>平成 13 年厚生労働省賃金構造基本統計調査より業種別、事業所規模別に「年間給与総額」「年間労働時間」を「労働力人口」による加重平均値で算出した。</p> <p>「年間給与総額」÷「年間労働時間」÷「労働力人口」により、「(a)時間当たり人件費」を算出した。</p> <p>業種別、事業所規模別に得られた (a)から「労働力人口」により加重平均値を計算、グループごとの値とした。</p> <p>注)「金融・保険・不動産業」は賃金構造基本統計調査の産業分類「J 金融・保険業」と「K 不動産業」の「労働力人口」による加重平均値より計算、グループ 1、3 は事業所規模「10～99 人」の値、グループ 2、4 は事業所規模「100～999 人」と「1000 名以上」の「労働力人口」による加重平均値により計算した。</p>
システム停止時間	アンケート調査、問 D 4 - B
システム復旧所要人数	アンケート調査、問 D 4 - D
業務復旧作業量対システム復旧作業量比率	アンケート調査、問 D 5 - 2
IT 依存業務割合	アンケート調査、問 D 6 - B (「その他業務部門」)
IT 依存業務のインシデント発生時の効率低下幅	アンケート調査、問 D 6 - 2 - B (「その他業務部門」)

注) *印のある原単位・パラメータは、事業所ごとにではなく、業種・事業所規模グループごとに設定するものを示す。

4.2.2 復旧作業に係る一般業務コスト

復旧作業に係る一般業務コストは、下式により推計される。

図表 4 - 7 復旧作業に係る一般業務コストの推計式

$$\begin{aligned}
 & \boxed{\text{復旧作業に係る一般業務コスト}} = \boxed{\text{時間当たり人件費}} \\
 & \quad \times \boxed{\text{業務復旧時間}} \times \boxed{\text{インシデントによる影響を受けた人数}} \\
 & \underbrace{\hspace{15em}} \\
 & \text{システム復旧所要時間} \times \text{システム復旧所要人数} \times \text{業務復旧作業量対システム復旧作業量比率}
 \end{aligned}$$

復旧作業に係る一般業務コストの推計に必要な原単位等とその入手・算出方法を下表に示す。

図表 4 - 8 復旧作業に係る一般業務コストの推計に必要な原単位等と入手・算出方法

原単位等	入手・算出方法
時間当たり人件費*	= 業務部門の時間当たり人件費単価。 平成 13 年厚生労働省賃金構造基本統計調査より業種別、事業所規模別に「年間給与総額」「年間労働時間」を「労働力人口」による加重平均値で算出した。 「年間給与総額」÷「年間労働時間」÷「労働力人口」により、「(a)時間当たり人件費」を算出した。 業種別、事業所規模別に得られた (a)から「労働力人口」により加重平均値を計算、グループごとの値とした。 注)「金融・保険・不動産業」は賃金構造基本統計調査の産業分類「J 金融・保険業」と「K 不動産業」の「労働力人口」による加重平均値より計算、グループ 1、3 は事業所規模「10～99 人」の値、グループ 2、4 は事業所規模「100～999 人」と「1000 名以上」の「労働力人口」による加重平均値により計算した。
システム復旧所要時間	アンケート調査、問 D 4 - C
システム復旧所要人数	アンケート調査、問 D 4 - D
業務復旧作業量対システム復旧作業量比率	アンケート調査、問 D 5 - 2

注) *印のある原単位・パラメータは、事業所ごとにではなく、業種・事業所規模グループごとに設定するものを示す。

4.3 業種別・事業所規模別グループ分類

ヒアリング調査結果から把握した業種及び事業所規模間のセキュリティインシデントへの対応状況の差異等に基づき、さらにアンケート調査のサンプル数分布も勘案して、グループ化を行った。具体的には、業種を「建設・製造業」と「第3次産業」に、また事業所規模の大小により「99名以下」と「100名以上」に分類し、4つのグループを形成した。

図表4-9 業種別・事業所規模別グループ分類とサンプル分布
(単位：上段はサンプル数、下段は%)

	N	99名以下	100名以上
合計	377 100.0	150 39.8	227 60.2
建設・製造業	166 100.0	グループ1 66 39.8	グループ2 100 60.2
第3次産業	211 100.0	グループ3 84 39.8	グループ4 127 60.2

注) 上記は、有効回答のうち、セキュリティインシデント被害を受け、当該被害についての情報提供を頂いた事業所のサンプル分布。

従業員数が多い事業所から構成されるグループ2、4で、従業員数が少ないグループ1、3よりも、被害を受けた事業所のサンプル数が多くなっている。

【参考：業種・事業所規模別セキュリティインシデントへの対応状況】

ヒアリング調査結果から、業種・事業所規模別に、セキュリティインシデントへの対応状況に関し、以下の差異がある傾向があることが分析された。

<業種による差異>

- ・ 製造業等の業種では、工場・流通センターにおいて非 WINDOWS マシンが利用されており、ウイルス定義ファイルが一括管理できないなど、セキュリティ対策が弱くなりがち傾向がある。
- ・ 情報サービス業等の PC への依存度が高い業種ほど、セキュリティインシデントの被害が大きくなる傾向がある。

<事業所規模の大小による差異>

- ・ 大規模事業所ほど、システム管理部門等でセキュリティインシデントに関する対策を一括管理する傾向がある。
- ・ 大規模事業所ほど、ウイルス定義ファイルの更新やバックアップの頻度が高い傾向がある。
- ・ 大規模事業所ほど、インシデントに関する報告を蓄積・調査・分析する体制が整備されている傾向がある。
- ・ PC への依存度も高い大規模事業所ほど、セキュリティインシデントの被害が大きくなる傾向がある。

図表 4 - 1 0 業種・事業所規模によるセキュリティインシデントへの対応上の差異

業種・事業所規模等により差異が見られる要素	
セキュリティ管理・報告体制	・エンドユーザ数が多い規模の大きい事業所等を中心に、エンドユーザの負担削減や被害件数削減等を目的に、メールサーバを設置し、サーバレベルでウイルス定義の更新を行い、ウイルスの発見・駆除を行う事業所が増えている。
セキュリティインシデントの発生・対応	・十分なシステム管理要員を抱える大企業や情報サービス産業において、ウイルス定義ファイル更新やバックアップの頻度が高い、報告事例を蓄積・分析する傾向が見られる。 ・規模の大きい事業所では、インシデントに関する報告を蓄積・調査・分析する体制が整備されている。規模が小さい事業所では、報告を受け対応したままのところも見られる。 ・製造業等においては、工場・流通センターにおいて、WINDOWSでないマシンが利用されており、ウイルス定義ファイルの一括管理が対応できない場合もある。ネットワーク接続をしている場合、これらが感染被害となりやすい。工場・流通センターにはシステム管理についての組織・人員が十分でない傾向もある。
セキュリティインシデントがもたらす被害	・情報サービス産業やオフィスワーカーが増大する大企業等のPC依存度が大きい産業において、「システム停止中の業務効率低下」を中心に、被害が大きくなる傾向がある。

5. 業種別・事業所規模別の被害推計モデル構築と被害額試算

5.1 業種別・事業所規模別のモデル構築

5.1.1 業種及び事業所規模に応じた4種類のモデル構築

上述のとおり、本調査では、業種及び事業所規模に基づく下記の4つのグループを設けている。したがって、被害額推計モデルも、これら4グループのそれぞれについて構築される。すなわち、計4種類のモデルが用意されることとなる。

-	グループ1	: 建設・製造業	99名以下
-	"	2 : "	100名以上
-	"	3 : 第3次産業	99名以下
-	"	4 : "	100名以上

これら4グループは、ヒアリング調査結果から把握した業種及び事業所規模間のセキュリティインシデントへの対応状況の差異等に基づきつつ、さらにはアンケート調査での回答サンプル数の分布をも勘案して設定されたものである。

5.1.2 業務効率低下割合

グループ別の被害額算出モデルの構造自体はまったく同一である。すなわち、モデルは個別サンプルのセキュリティインシデント被害額を逸失利益や効率化低下コストといった被害種類ごとに積み上げて総額を得るという仕組みになっている。したがって、基本的には、個別サンプルからの個々の回答内容の正確さが、モデルの推計精度を規定していることができる。

ただし、「システム停止中の業務効率低下コスト」の推計に用いられるパラメータである「業務効率低下割合」については、個別サンプルの回答データではなく、グループごとの平均値を用いることとした。これは、このパラメータに係る個別サンプルの数値にはばらつきが大きい(すなわち推計結果に誤差やバイアスを生みやすい)と想定されたからである。より信憑性の高い業務効率低下割合を得るためには、このパラメータの算定ベースすなわち回答サンプル数をできるだけ多くして、統計的により信頼できる平均値を求めることが必要と考えられた。

図表 5.1.1-1 には、グループ別の平均値に基づく業務効率低下割合（ただし業務部門）を示している。既に説明したとおり、業務効率低下割合は「IT に依存する業務の割合」と「IT 依存業務の通常時とインシデント発生時の効率の差分」の積として定義される。図表 5.1.1-1 には、IT に依存する業務の割合、IT 依存業務の通常時とインシデント発生時の効率の差分、及び両者の積である業務効率低下割合のそれぞれについて、平均値、分散及び最頻値を示している。

まず、業務効率低下割合の構成要素である IT 依存割合と 効率の差分をみると、いずれについても、建設・製造業に比べて第 3 次産業の方がサンプルごとのデータのばらつき（分散）が大きいことがわかる。また、建設・製造業では事業所規模の大きい方でデータのばらつきが相対的に大きいのに対して、第 3 次産業では事業所規模の小さい方でばらつきが大きい。最も分散が大きいのはグループ 3（第 3 次産業、99 名以下）である。このグループ 3 のみ、最頻値が 35 と、他グループの最頻値（= 55）と異なっている。

次に、業務効率低下割合をみる。上述のと でみたグループ別のデータのばらつきの違いは、両者の積である業務効率低下割合にも反映されている（つまりグループ 3 のばらつきが最も大きい）。しかしながら、モデルの推計に用いられる平均値を見る限り、グループ間での顕著な差異は認められない。このように、結果的には、グループ間での業務効率低下割合に格差は確認されなかった。

ただし、このことは、業種別・事業所規模別のグルーピングに基づいてセキュリティ被害額の推計を行うことの意味を必ずしも否定するものではない。今回の調査では、サンプル数の制約もあり、業種と事業所規模をきめ細かく分類したグルーピングができなかった。より詳細なグルーピングに基づく分析を行うことができれば、グループ間の IT 依存割合、効率差分、引いては業務効率低下割合の差異が浮き彫りとなる可能性はあると考えられる。

図表 5.1.1 - 1 グループ別の業務効率低下割合（業務部門）

IT に依存する業務の割合（％）

	グループ 1： 建設・製造業 99 名以下	グループ 2： 建設・製造業 100 名以上	グループ 3： 第 3 次産業 99 名以下	グループ 4： 第 3 次産業 100 名以上
平均値	56.1	53.7	56.0	59.3
分散	452	499	789	586
最頻値	55	55	35	55

IT 依存業務の通常時とインシデント発生時の効率の差分（％）

	グループ 1： 建設・製造業 99 名以下	グループ 2： 建設・製造業 100 名以上	グループ 3： 第 3 次産業 99 名以下	グループ 4： 第 3 次産業 100 名以上
平均値	50.4	44.0	45.1	48.8
分散	660	752	846	775
最頻値	55	55	55	55

業務効率低下割合 = () ÷ 100) × () ÷ 100)

	グループ 1： 建設・製造業 99 名以下	グループ 2： 建設・製造業 100 名以上	グループ 3： 第 3 次産業 99 名以下	グループ 4： 第 3 次産業 100 名以上
平均値	0.310	0.263	0.287	0.308
分散	0.050	0.047	0.070	0.053
最頻値	0.303	0.193	0.123	0.303

(注) 1. グループ 1 ~ 4 のサンプル数はそれぞれ、66、100、84、127 である。

2. のデータはアンケート調査の問 D 6 から、 は問 D 6 - 2 から、それぞれ得られた。いずれも一定の幅をもった選択肢を 1 つだけ選択する設問である。例えば、 について「10%」という選択肢を選んだ場合には、0% ~ 10% の中央値である 5% を推計に用いた。同様に、 について「90 ~ 100%」を選んだ場合は、95% を推計に用いた。

5.2 インシデント被害の規模に着目した推計

本年度モデルにおいては、業種別・事業所規模別のグルーピングに加えて、各グループにおいて、大、中、小という被害規模別で被害額を推計することとした。各被害規模の定義は下記のとおりである。

- 大規模被害：事業所全体に及ぶ被害
- 中規模被害：部署または課全体に及ぶ被害
- 小規模被害：少数のパソコンに及ぶ被害

被害規模の観点を導入した理由は次のとおりである。すなわち、同じ 1 件のセキュリティインシデントでも、その規模が違えば、事業所ないしは事業所の利益や業務効率に及ぼす影響は異なると考えられる。大規模被害 1 件当たりの被害額は、小規模被害 10 件の被害額に相当する可能性がある。

こうした問題意識を踏まえて、今回、逸失利益の推計に際して、小規模及び中規模被害を算入しない（すなわち小・中規模被害では逸失利益は発生しないとの想定を設ける）こととした。その理由は次のとおりである。

ヒアリング調査の結果等を踏まえると、小規模被害においては、システム部門、業務部門（現場）においてシステム復旧コストのみが発生するケースがほとんどと想定されること。著しく多数の業務用ファイルがウイルスの感染した場合（＝大規模被害）でなければ、現場における復旧コスト（特に「復旧作業に関わる一般業務コスト」）もさほど発生しないと推察される。

複数のクライアント PC がウイルスに感染した程度では、「システム復旧コスト」は多少発生するものの、他の被害項目のコストはほとんど計上されないと推測される。他方、基幹システムに被害があった場合には、すべての項目で大きな被害が計上されると考えられる。基幹システムの被害は、概して、本調査でいうところの大規模被害に該当する。

常識的に考えても、中小規模被害にけるシステム停止が会社の利益ロスに直結するとの想定を設けることは現実的でない。実際、そうした前提でモデル推計を実施したところ、逸失利益が異常に大きく算定される結果となった。こうしたことから、本調査では、逸失利益の推計に際して、小規模及び中規模被害を算入しないこととした。

5.3 有効回答事業所ベースの被害額試算

アンケートへの有効回答事業所のデータを基に、業種別・事業所規模別グループごとに被害総額を試算したところ、下表のような結果が得られた。

図表 5 - 1 業種別・事業所規模別被害総額（単位：円）

	被害サンプル数	被害総額	大規模被害	中規模被害	小規模被害	1事業所当たり被害額
グループ1： 建設・製造業、99名以下	66	18,033,347	3,763,074	4,823,729	9,446,544	273,233
グループ2： 建設・製造業、100名以上	100	98,963,643	58,477,293	14,462,958	23,887,340	969,636
グループ3： 第3次産業、99名以下	84	16,767,411	828,465	640,420	15,263,167	199,612
グループ4： 第3次産業、100名以上	127	47,763,964	19,833,265	20,471,570	7,459,130	376,094

試算結果では、グループ1の被害総額が約1.8千万円（1事業所当たりの被害額約27万円）、グループ2が約1億円（同約100万円）、グループ3が約1.6千万円（同約20万円）、グループ4が約5千万円（同約38万円）となっており、1事業所当たりの被害額はPCユーザーが多い（従業員数が多い）大規模事業所が属するグループにおいて大きい一方で、グループ当たりの被害額は事業所数が多い中小規模事業所が属するグループにおいて多くなっていることが読み取れる（図表6-2参照）。

なお、各グループの被害額に関する詳細は、付属資料を参照されたい。

6. 国内被害総額の推計と比較検証

6.1 国内被害総額の推計

本節では、前章で求められた各グループ別被害額に基づき、国内の総被害額を推計する。

6.1.1 推計手順

以下の手順にしたがって、国内総被害額の推計を行った。

前章で試算した有効回答事業所ベースの被害総額の業種・事業所規模グループ別集計を利用し、グループ別にそれぞれ国内の事業所ベースの被害総額を算定し、その和を国内被害総額とすることとした。

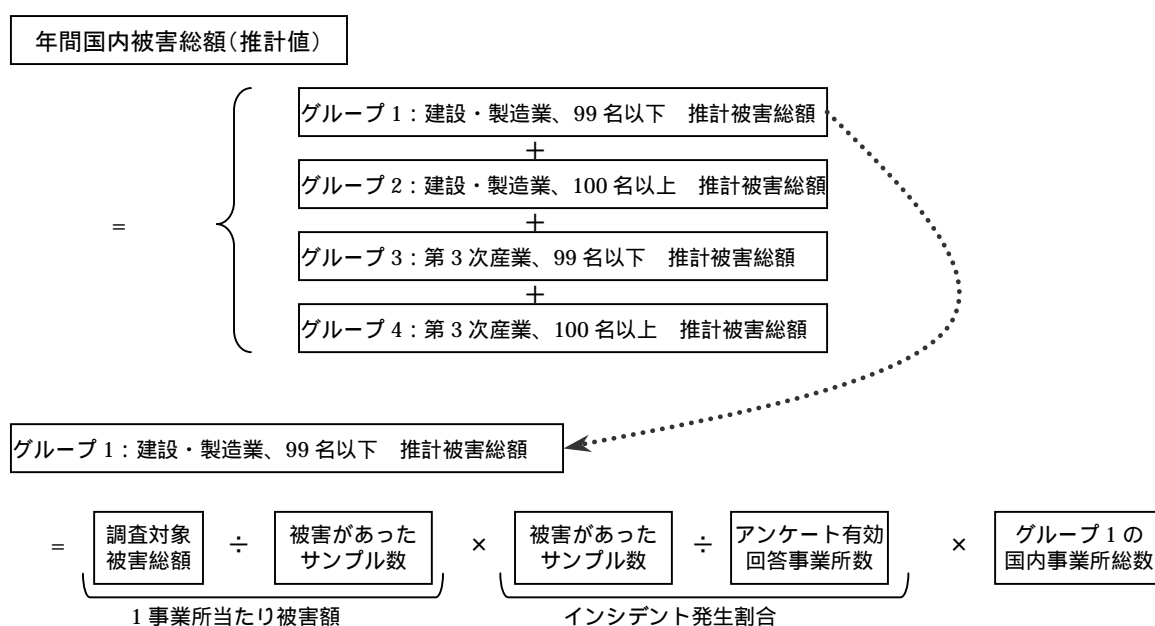
アンケート結果から試算した「調査対象被害総額」を「被害があったサンプル数」で除し(a) 1事業所当たり年間被害額を算定する。

別途、アンケート結果から「被害があったサンプル数」を「アンケート有効回答事業所数」で除して、(b) 年間インシデント発生比率を算定する。

(a) × (b) × 業種別・事業所規模別国内事業所総数により、年間業種別・事業所規模別国内被害総額を得る。

業種別・事業所規模別の年間国内被害総額を合計することにより、年間国内総被害額を得る。

図表 6 - 1 国内被害総額の推計手順



6.1.2 推計結果

上記推計手順により推計された、2002年1月～12月の国内セキュリティインシデントの被害総額は、約4,392億円に達した。

図表6-2 業種別・事業所規模別被害総額

	(a)推計 被害総額(円) (a)=(b)×(c)×(d)	(b)1事業所当 たり被害額 (円)	(c)インシデント 発生割合	(d)グループ内 国内総 事業所数
グループ1： 建設・製造業、99名以下	85,605,402,377	273,233	0.253	1,238,983
グループ2： 建設・製造業、100名以上	5,746,323,265	969,636	0.316	18,727
グループ3： 第3次産業、99名以下	340,939,607,907	199,612	0.344	4,961,366
グループ4： 第3次産業、100名以上	6,883,916,188	376,094	0.462	39,634
合計	439,175,249,736	---	---	6,258,710

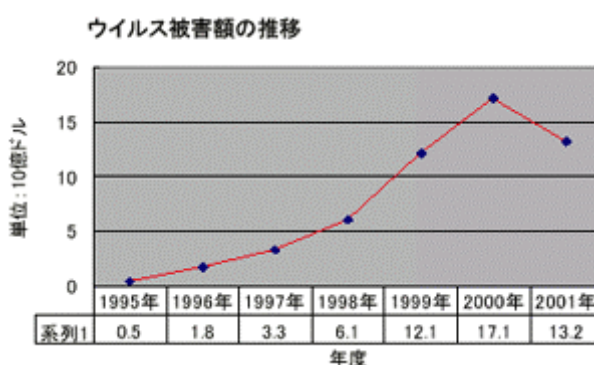
注) 四捨五入された値があるため、厳密には(a)=(b)×(c)×(d)とならない。

6.2 推計結果の比較検証

6.2.1 他の試算結果との比較等による検証

米国民間調査会社 Computer Economics 社の試算によれば、世界で発生したウイルス被害額は、図表 6 - 2 のとおりとなっている。2000 年度で 17.1 億ドル、2001 年度で 13.2 億ドル、日本円に換算すると、およそ 1.5 兆円から 2 兆円の間で推移している。2000 年は「love letter」ウイルスが猛威を振るったため一時的に被害額が増加したものと考えられる。

図表 6 - 2 世界のウイルス被害額の推移



資料：米国 Computer Economics 社発表資料をもとにコンピュータアソシエイツ社が作成したデータを引用

なお具体的な推計範囲や推計方法は公開されていないので、本調査の試算結果が妥当かどうか単純に両試算結果を比較することで判断することは必ずしも妥当ではないが敢えて、検証のため比較する。

- 他の推計結果との比較検証

$$\begin{aligned} & \text{Computer Economics 社の年間推計値} \times \frac{\text{日本のパソコンの出荷台数}}{\text{世界のパソコンの出荷台数}} \\ &= 1.58 \text{ 兆円} (13.2 \text{ 億ドル} \times 120 \text{ 円 / ドル}) \times \frac{13,169 \text{ (千台)}^*}{133,642 \text{ (千台)}^*} \\ &= 1,560 \text{ 億円} \quad (\text{本調査試算結果の約 } 1 / 3) \end{aligned}$$

*パソコン白書 2000-2001, pp244、「パソコン出荷台数の推移実績および予測」より

- 1 事業所当たり被害額による検証

$$\begin{aligned} 1 \text{ 事業所当たり被害額} &= \text{推計被害総額} \div \text{日本の総事業所数} \div \text{インシデント発生割合} \\ &= 439,175,249,736 \text{ 円} \div 6,258,710 \text{ 事業所} \div 0.343^* \\ &= 70,170 \text{ 円 / 1 事業所当たり (年間)} \times 2.92 \\ &= 204,896 \text{ 円} \end{aligned}$$

*今回の調査結果、G1～G4のインシデント発生割合の単純平均値

6.2.2 考察

Computer Economics 社との比較では、本調査の試算結果がおよそ3倍の総被害額となった。さらに日本のコンピュータウイルスへの遭遇率と世界平均の遭遇率との割合を乗じると、日本の遭遇率が高いと一般にいわれていることから、3倍の開きはやや縮まるものと考えられる。あくまで推計方法、推計範囲の一致を考慮しない前提での比較ではあるが、その前提で妥当性について一定の枠内であると考えられる。

また、1事業所当たりの年間被害額については、インシデントに遭遇した場合、1事業所が被害の規模（大・中・小規模）や遭遇回数を押し並べて1年間で被る金額である。あくまでも感覚的な枠にとどまるが、妥当性について一定の枠内であると考えられる。

6.3 残された課題

6.3.1 逸失利益に関する精緻化

セキュリティインシデントを大規模、中規模、小規模に区分する際の定義に、曖昧さがある。その影響を直接的に受けたのが「逸失利益」の推計であり、中規模と小規模では利益ロスが生じないという仮定を設けざるを得なくなっている。あるインシデントが利益ロスに直結するかどうかという観点で考えると、インシデントを基幹システム関係被害、オンライン（受注システム）関係被害等に分けることも一案であろう。オンライン（受注）関連の被害は、クライアントPCレベル（＝小規模）のインシデントでありながら、利益ロスに直結する可能性もある。よって、今後は、大・中・小という分け方に必ずしも固執せず、利益に直結するかどうかという観点からのインシデントの類型化が必要であろう。

6.3.2 業務部門に関するデータの精緻化

「業務効率低下割合」については、本来ならば、数ある現業部門から情報を直接収集すべきだが、本調査では、多くのサンプル数を得ることを重要視し、システム管理部門に対するアンケート調査により、現業部門の業務効率低下割合について、推察してもらう手順をとった。業務効率低下割合においては、正確な数値を算出することは技術上困難であるが、複数サンプル事業所におけるモニター調査等、フィジビリティ及び費用対効果の高い調査手法を用いて数値を推計することが考えられる。

6.3.3 事業所を調査対象とする際の留意点

調査対象の単位を企業ではなく事業所としたことについては、被害がどこでどれだけ発生したかをきめ細かく把握するという点では有効であったが、他方で、利益額は企業単位でなければ回答しづらいという実査上の問題を引き起こした（利益額に無回答のサンプルが多かった）。たとえ利益額を回答してもらっても、時間当たり利益額を事業所ごとに計算してみると、同一業種内においてもかなりのばらつきがあることがわかる。回答サンプルに業績好調な事業所ばかりが含まれていたり、逆に業績の悪い事業所が多く含まれていたりすると、被害額の推計に上方ないしは下方バイアスを生むことになる。よって、よほど大きな回答サンプル数（例えば何千というオーダー）を確保しない限り、非常に正確な推計は難しいといえる。それが困難な場合、利益額はアンケートではなく既存統計等から推計することが妥当であろう。

6.3.4 インターネット上で企業・事業所が自己のセキュリティインシデント被害額を推計できるようにする

ヒアリング調査において、多くの事業所がセキュリティインシデントによる被害を感じていながらも、被害額については試算・推計していない状況が読み取れた。一方、システム部門においては、今後のセキュリティ関連対策の充実に際して、自己が受けたセキュリティインシデントの被害を定量的に把握することの重要性が指摘された。また、インターネット上等で簡易にセキュリティインシデントの被害額を算出することができるシステムへのニーズが確認された。

付属資料

付.1 業種・事業所規模グループ別セキュリティインシデント被害額

付.1.1 グループ1（建設・製造業、99名以下）のセキュリティインシデント被害額算出結果

図表付. - 1 業種別・事業所規模別被害総額（単位：円）

集計対象サンプル数 = 66	合 計			
	大規模被害	中規模被害	小規模被害	
インシデント発生件数（件）	116	11	17	88
平均業務効率低下割合（業務部門）	0.31	---	---	---
1次的（直接的）被害総額（円）	18,033,347	3,763,074	4,823,729	9,446,544
表面化被害	17,984,128	3,738,891	4,817,611	9,427,626
逸失利益	316,814	316,814		
システム復旧コスト	17,667,314	3,422,078	4,817,611	9,427,626
潜在化被害	49,219	24,183	6,118	18,918
システム停止中の業務効率低下コスト	27,354	8,438	6,118	12,798
復旧作業に係わる一般業務コスト	21,865	15,744	0	6,120

注）集計対象サンプル数ベースの計算結果であり、日本全体の被害額を示すものではない。

付.1.2 グループ2（建設・製造業、100名以上）のセキュリティインシデント被害額算出結果

図表付 - 2 業種別・事業所規模別被害総額（単位：円）

集計対象サンプル数 = 100	合 計			
		大規模被害	中規模被害	小規模被害
インシデント発生件数（件）	636	15	58	563
平均業務効率低下割合（業務部門）	0.26	---	---	---
1次的（直接的）被害総額（円）	96,963,643	58,477,293	14,517,888	23,968,463
表面化被害	96,818,779	58,468,482	14,462,958	23,887,340
逸失利益	53,185,119	53,185,119		
システム復旧コスト	43,633,660	5,283,363	14,462,958	23,887,340
潜在化被害	144,864	8,811	54,930	81,123
システム停止中の業務効率低下コスト	122,969	8,515	35,702	78,752
復旧作業に係わる一般業務コスト	21,895	296	19,228	2,371

注）集計対象サンプル数ベースの計算結果であり、日本全体の被害額を示すものではない。

付.1.3 グループ3（第3次産業、99名以下）のセキュリティインシデント被害額算出結果

図表付 - 3 業種別・事業所規模別被害総額（単位：円）

集計対象サンプル数 = 84	合 計			
		大規模被害	中規模被害	小規模被害
インシデント発生件数（件）	210	5	9	196
平均業務効率低下割合（業務部門）	0.29	---	---	---
1次的（直接的）被害総額（円）	16,767,411	828,465	640,420	15,298,526
表面化被害	16,720,842	825,667	632,008	15,263,167
逸失利益	706,319	706,319		
システム復旧コスト	16,014,523	119,348	632,008	15,263,167
潜在化被害	46,569	2,798	8,412	35,359
システム停止中の業務効率低下コスト	37,046	2,094	5,504	29,448
復旧作業に係わる一般業務コスト	9,523	704	2,908	5,912

注）集計対象サンプル数ベースの計算結果であり、日本全体の被害額を示すものではない。

付.1.4 グループ4（第3次産業、100名以上）のセキュリティインシデント被害額算出結果

図表付 - 4 業種別・事業所規模別被害総額（単位：円）

	集計対象サンプル数 = 127			
	合 計	大規模被害	中規模被害	小規模被害
インシデント発生件数（件）	726	21	91	614
平均業務効率低下割合（業務部門）	0.31	---	---	---
1次的（直接的）被害総額（円）	47,763,964	19,833,265	20,471,570	7,459,130
表面化被害	47,325,691	19,821,293	20,398,385	7,106,013
逸失利益	4,941,991	4,941,991		
システム復旧コスト	42,383,700	14,879,303	20,398,385	7,106,013
潜在化被害	438,273	11,972	73,185	353,117
システム停止中の業務効率低下コスト	384,186	11,972	53,752	318,463
復旧作業に係わる一般業務コスト	54,087	0	19,433	34,655

注）集計対象サンプル数ベースの計算結果であり、日本全体の被害額を示すものではない。

付.2 ヒアリング調査結果

付.2.1 ヒアリング実施要領

目 的

被害額算出モデルの構造が、セキュリティインシデントの発生からシステム復旧及び業務正常化までの事態の流れにマッチしているかどうかについて、実際に過去にセキュリティインシデントを経験した事業所等のコメントを踏まえて検証すること。

さらに、セキュリティインシデントの管理・報告体制、発生・被害状況に関する業種別・事業所規模別の違いについて分析すること。

対 象

下記の5事業所とした。

- 1) A事業所（第3次産業、100名以上）
- 2) B事業所（第3次産業、99名以下）
- 3) C事業所（建設・製造業、100名以上）
- 4) D事業所（建設・製造業、99名以下）
- 5) E事業所（経営多角化、100名以上）

実施期間

平成15年2月中。

調査項目

- ・ セキュリティ管理・報告体制
- ・ セキュリティインシデント事例（発生経緯・内容・対応方法、被害構造）
- ・ セキュリティインシデント被害額算出モデルに対する意見

付.2.2 ヒアリング総括

	業種・事業所規模等に関わらず 共通性が高い要素	業種・事業所規模等により 差異が見られる要素
セキュリティ管理・報告体制	<ul style="list-style-type: none"> ウイルス感染等のセキュリティインシデント発生時には、ユーザから本社システム管理部門及び支社・営業所等のシステム担当へと電話及びメール等による報告が行われる。 報告を受けたシステム管理部門及びシステム担当が（直接もしくは遠隔地において）対応指示を行う。 システム管理部門及びシステム担当の指示を受け、感染者（もしくはシステム管理部門及びシステム担当）による対応がなされる。 システム管理部門から、ウイルス等のセキュリティインシデントに関わる事項につき、周知・啓発・注意喚起の連絡がなされている。 	<ul style="list-style-type: none"> エンドユーザ数が多い規模の大きい事業所等を中心に、エンドユーザの負担削減や被害件数削減等を目的に、メールサーバを設置し、サーバレベルでウイルス定義の更新を行い、ウイルスの発見・駆除を行う事業所が増えている。
セキュリティインシデントの発生・対応	<ul style="list-style-type: none"> メールの添付ファイル開封による感染がほとんど。 ウイルス感染の場合には、システム部門1~2名と現業部門1~2名で対応され、通常1台当たり数時間で発見・駆除・スキャン・ファイル修復等の一連の作業が完了する。 ウイルス感染の場合には、追加のソフト・ハード購入や、OS及びソフトの再インストールはほぼ見られない。 	<ul style="list-style-type: none"> 十分なシステム管理要員を抱える大企業所や情報サービス産業において、ウイルス定義ファイル更新やバックアップの頻度が高い、報告事例を蓄積・分析する傾向が見られる。 規模の大きい事業所では、インシデントに関する報告を蓄積・調査・分析する体制が整備されている。規模が小さい事業所では、報告を受け対応したままのところも見られる。 製造業等においては、工場・流通センターにおいて、WINDOWSでないマシンが利用されており、ウイルス定義ファイルの一括管理が対応できない場合もある。ネットワーク接続をしている場合、これらが感染被害となりやすい。工場・流通センターにはシステム管理についての組織・人員が十分でない傾向もある。
セキュリティインシデントがもたらす被害	<ul style="list-style-type: none"> 通常のウイルス感染である限り、多数のPCが同時に影響されることは少なく、システム部門1~2名と現業部門1~2名による「システム復旧コスト」「システム停止中の業務効率低下」が中心である。 基幹システムが被害に遭う場合、「逸失利益」「復旧作業に関わる一般業務コスト」へと被害範囲が飛躍的に拡大し、その対応コストも増大する。しかし、基幹システムが被害に遭う事例はほとんど見られていない。 	<ul style="list-style-type: none"> ECを行っている/いないで、「逸失利益」の大小は変わってくる。 情報サービス産業やオフィスワーカーが増大する大企業所等のPC依存度が大きい産業において、「システム停止中の業務効率低下」を中心に、被害が大きくなる傾向がある。