

企業における情報セキュリティガバナンスの
あり方に関する研究会 報告書
参考資料

リスク定量化に関する検討資料

1. リスク定量化が求められる背景

企業において情報セキュリティ対策が進展しない理由の一つとして、IT事故発生リスクが明確でなく、適正な情報セキュリティ投資の判断が困難であるとの指摘がある。企業経営者の視点から情報セキュリティ対策を考えると、どの程度セキュリティ投資を行えばよいかという判断基準がない状況であり、企業にとって適切な水準での情報セキュリティ対策の実施の指標とするためにも、リスクの定量化が求められている。

2. リスク定量化に関する検討事例

現在、セキュリティ関連機関等においてリスク定量化手法の開発が検討されている。また、金融機関では新BIS規制¹（バーゼルⅡ）により「オペレーショナルリスク」（情報システム障害等含む）の定量化に関する検討が進展している。ただし、現段階では、検討は進みつつあるものの、確立した手段はないと考えられる。

（1）コンピュータウイルス被害総額（独立行政法人情報処理推進機構（IPA））²

我が国におけるコンピュータウイルス被害総額を推計するもの。推計に必要なパラメータは事業者アンケートから得られたデータから算出。

インシデント被害額 = ①「表面化被害額」 + ②「潜在化被害額」

①「表面化被害額」 = 逸失利益 + システム復旧コスト

▼「逸失利益」 = 時間当たり利益 × システム停止時間

▼「システム復旧コスト」 = システム管理部門の時間当たり人件費単価 × システム復旧所要時間 × システム復旧所要人数 + 代替ハードウェア・ソフトウェア購入費

②「潜在化被害額」 = システム停止中の業務効率低下コスト + 復旧に関わる一般業務コスト

▼「システム停止中の業務効率低下コスト」 = 業務部門の時間当たり人件費単価

× システム停止時間 × インシデントによる影響を受けた人数 × 業務効率低下割合

※業務効率低下割合の考え方：「ITに依存した業務」と「依存しない業務」とに分けて考え、「ITに依存した業務」の場合は効率低下割合が大きい。

【2003年度国内のウイルス被害総額推計】

国内のウイルス被害総額推計結果 = 約3,025億円（2003年度）

調査対象 被害総額	÷	被害があった サンプル数	×	被害があった サンプル数	÷	アンケート有効 回答事業所数	×	国内事業所総数
1事業所当たり被害額				インシデント発生割合				

（2）インシデント被害額・情報漏えい被害額（NPO 日本ネットワークセキュリティ協会（JNSA））³

¹ BIS（Bank for International Settlements：国際決済銀行）が定めた、国際業務を行う民間銀行の自己資本比率に関する国際統一基準。バーゼル合意とも呼ばれる。これが達成できない銀行は、国際業務から事実上の撤退を求められる。新BIS規制は、リスクの計測方法としてオペレーショナルリスクが導入される方向で、2006年末に適用される予定。

² IPA「国内・海外におけるコンピュータウイルス被害状況調査 被害額推定報告書」（2004年4月）
http://www.ipa.go.jp/security/fy15/reports/virus-survey/documents/2003_calc_model.pdf

①情報セキュリティインシデント被害額算出モデル

逸失利益や損害賠償等表面化する被害と、ブランド価値低下等潜在する被害を算出し加算。

I P A被害算出モデルをベースに策定。

➤ **インシデント被害額** = a. 表面化被害 + b. 潜在化被害

a. 表面化被害 = 直接被害 + 間接被害

b. 潜在化被害額 = 業務にかかわる潜在化被害 + 業務外の潜在化被害 (ブランド価値の低下)

▼ 業務にかかわる潜在化被害 = 固定費 (人件費) × インシデントによる影響を受けた人数 × IT 感応度 (業務依存度) × 停止時間 + 業務外の潜在化被害 (風評被害など)

※IT 感応度 (業務依存度) : システムないしネットワークの業務に対する影響度を 0 ~ 1 の範囲で設定。システムやネットワークへの業務依存度が高い → 感応度も高い、業務に全く影響無し → ゼロ。実施の調査・検証の結果、一般企業における実務上の参考値としては、「IT 感応度 0.2」を推奨。

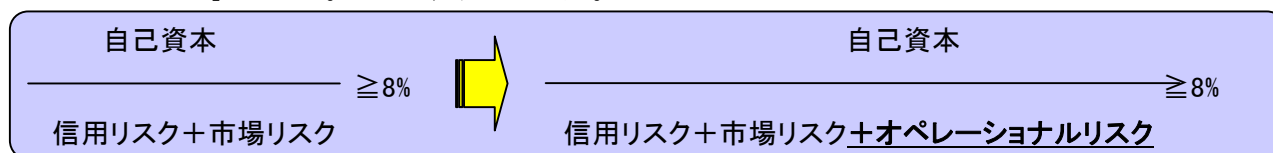
②情報漏えいによる被害想定

「経済的損失」と「精神的苦痛」の2つの観点からリスクを分析し、個人情報価値を定量化。判定基準表を用いて算出式の各項の数値を求めやすくする改良を実施。

➤ **損害賠償額** = 基礎情報価値 × 機微情報度 × 本人特定容易度 × 情報漏えい元組織の社会的責任度 × 事後対応評価

(3) 新 BIS 規制に伴う「オペレーショナルリスク」定量化

自己資本比率を計算する式の分母に、従来の信用リスクと市場リスクに加え、新たに「オペレーショナルリスク」が追加。2006 年末より適用。



「オペレーショナルリスク」は、内部または外部の者による不正行為、また過失による誤入力、コンピュータシステムの障害などの事務事故によって損失が発生するリスクを含む。金融業務における IT 依存度の高まりに伴い、IT 事故によるリスクが増大していることに対応。「新 BIS 規制」では、オペレーショナルリスクが大きいほど、より多くの自己資本を準備しなければならないため、金融機関は対策を講じる必要がある。

計量方法としては基礎的指標手法、標準的手法、先進的手法から選択。先進的手法には、損失分布手法、内部計測手法、リスクシナリオ手法などが挙げられており、今後オペレーショナルリスク定量化手法及びツール開発が進展することが見込まれる。

【ex. 損失分布手法】

年間の事故発生率 (頻度分布、ex.ポアソン分布など) や、事故 1 件あたりの損失額 (損失額分布、ex.実分布、対数正規分布など) を基に、モンテカルロシミュレーションを実施する手法。

³ JNSA 「2003 年度情報セキュリティインシデントに関する調査報告書」 (2004 年 3 月)
http://www.jnsa.org/active2003_1a.html

3. 被害量算定モデル

(1) 被害量算定モデルの基本的考え方

2.の検討事例を踏まえ、今回実施した企業アンケート調査の結果（参考②③）を活用する形で、リスク定量化ツールの骨格となる被害量算定モデルについて、WGにおいて検討を行った。本モデルでは、IT事故により企業の情報システムが停止した場合に、企業の収益に直接的に与える影響を算出する。算出のための指標としては、企業アンケート調査結果及びその他の調査などから抽出したデータと、各企業が記入する自社のデータがあり、それらを組み合わせて算出することにより、各企業のリスク値が明確化される。ただし、本モデルは暫定的なイメージであり、実際のツールとして整備するためには適切な係数の設定や更なる精緻化が必要と考えられる。

また、情報セキュリティ対策ベンチマークのセルフチェックツールと連動して利用することにより、リスク評価結果をもとに、対策実施の必要性の有無を検討する際に参考とすることができる。そのため、被害量算定モデルは、情報セキュリティ対策ベンチマークが公開されるサイトと同じサイトで提供されることが望まれる。

(2) 被害量算定方法の概要

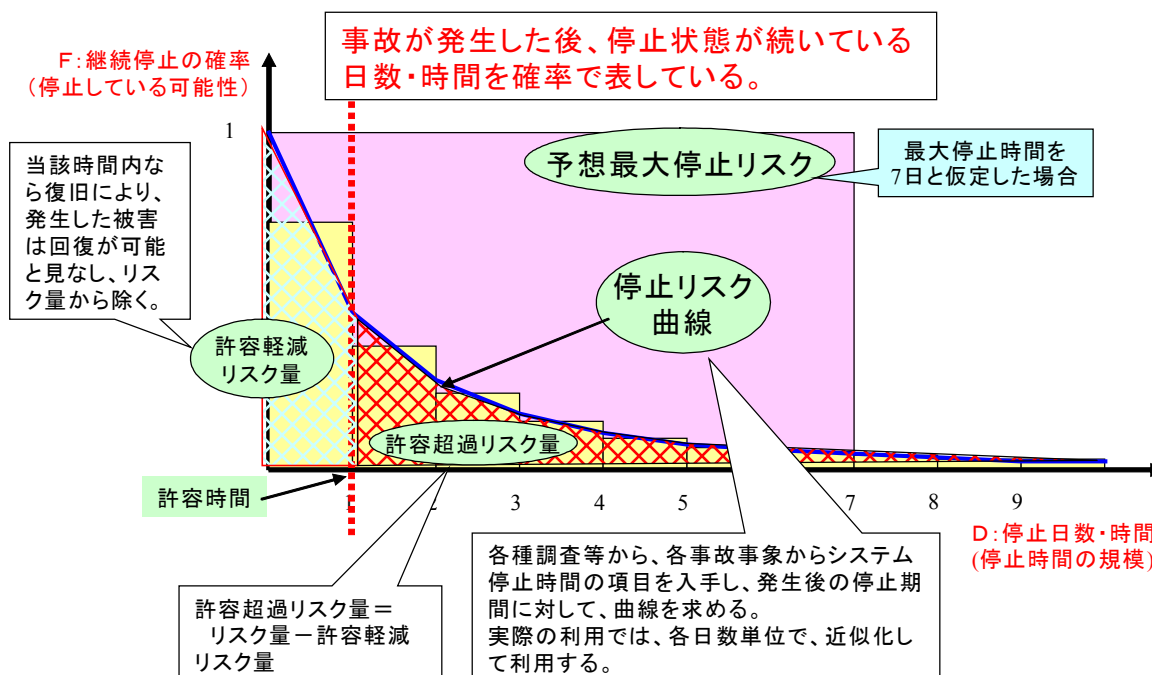
情報システムがある時点で停止している確率を、各種調査等から各事故事象でのシステム停止時間の項目を入手して求める（停止リスク曲線）。この積分値がリスク量であるが、これに企業毎の1日の利益に与える影響度、事故の年間発生確率、セキュリティ対策を講じることにより低減されるリスクの比率を掛け合わせ、年間の被害量を概算する。

(3) 停止リスク曲線

停止リスク曲線とは、情報システムが停止するなどの事故が発生した後、ある時点で停止状態が続いている確率を表した相関図である。この相関図から得られる積算値（面積）が、事故が発生した場合のリスク量として算出される。

一般的に、停止日数（時間）が短い事故の発生割合が高く、1週間以上長期にわたって停止する事故の発生割合は低いため、停止日数・時間とともに逓減する二次曲線が想定される。

【図表1 停止リスク曲線イメージ】



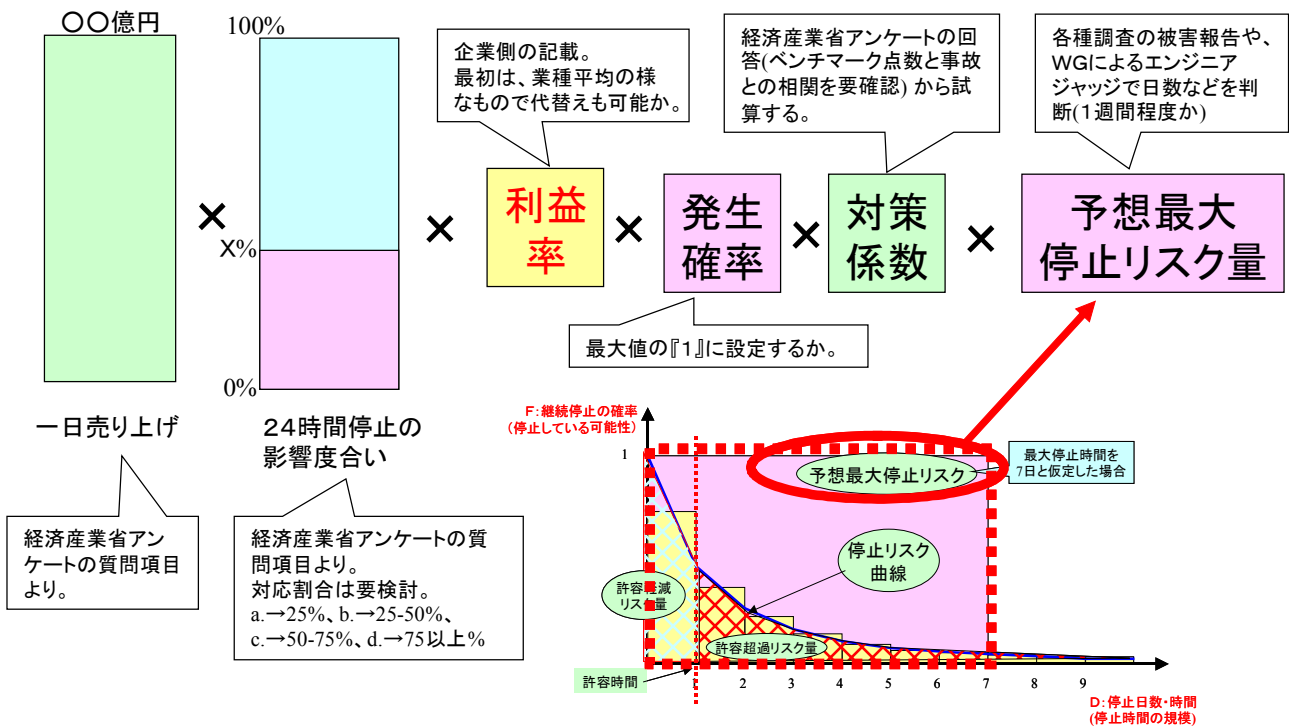
(5) 予想最大停止リスク量

予想最大停止リスク量とは、企業が許容しうるリスク量を除き、年間あたりに企業が抱える停止リスク量を算出するもの。統計等をもとに設定した予想しうる最大停止時間のリスク量に、企業毎の1日の利益に与える影響度、事故の年間発生確率、セキュリティ対策を講じることにより低減されるリスクの比率を掛け合わせ、年間の被害量を概算する。

予想最大停止リスク量(年間)

$$= \text{売上高(一日)} \times \text{24時間停止の影響度合い} \times \text{利益率} \times \text{発生確率} \times \text{対策係数} \times \text{予想最大停止リスク量}$$

【図表3 予想最大停止リスク量の算定イメージ】



【用語の解説】

- ①売上高：企業の1日あたりの売上高。企業が記入。
- ②24時間停止の影響度合い：主要な情報システムが営業日に「24時間」停止した場合の売上高への影響度を企業が選択（25%未満、25-50%未満、50-75%未満、75%以上）。
- ③利益率：当期売上高に占める当期利益の割合。企業が記入。ゼロ若しくはマイナスの可能性もあるため、業種別平均値等も検討。
- ④発生確率：過去1年間に事業に影響を及ぼすシステム停止が発生する確率。
(a)経済産業省調査より算出、(b)その他調査結果より算出
- ⑤対策係数：企業のセキュリティ対策とリスクとの相関関係（の強さ）を表す係数。
- ⑥許容超過リスク量：停止リスク曲線から得られる停止のリスク量から許容軽減リスク量を除したものの。