情報セキュリティにおけるリスクの定量化手法

Quantification Technique of Risk in Information Security

岡 本 卓 馬

要 約 情報セキュリティ対策を考える上で，リスクマネジメントは不可欠である．これは，リスクアセスメント，リスク対応，リスク受容，リスクコミュニケーションを含む概念である．

リスクマネジメントの結果を踏まえて具体的な対策を検討するが，現在のリスク評価の多くは，リスクの大きさを相対的な数値として算出するため，対策に要する費用の妥当性を判断するのは困難である．

対策に要する費用の投資対効果を計る上では，リスクが顕在化する確率やリスクが顕在化することで被ると予想される損失額を算出し，リスクを定量化することが有効である．

本稿では，リスクを定量的なデータとして算出するための方法例と，留意点について記述する．

Abstract In the idea of the information security measures, the risk management is indispensable. This is a concept including the risk assessment, the risk receipt for the risk, and the risk communications.

It is difficult to judge the validity of costs required for measures so that many of present risk evaluations may calculate risky as a relative numerical value though concrete measures are examined based on the result of the risk management.

In the measurement of investment/effect of costs required for measures, it is effective to calculate the amount of loss expected receiving by actualizing the probability and the risk that the risk is actualized, and to quantify the risk.

This paper discusses the example of the method and the note to calculate the risk as quantitative data.

1. はじめに

昨今，OSの脆弱性を突いたコンピュータウィルス，企業の個人情報・機密情報の漏洩事故などがメディアでも話題になり，企業の情報セキュリティへの関心はかつてないほど高まっている．今や情報セキュリティ対策は企業経営における重要課題の一つである．

しかしながら，情報セキュリティ対策と一言でいっても，その範囲は非常に広い．ウィルス対策ソフトやファイアウォールといった技術的な対策から，情報セキュリティポリシーの策定や従業員の情報セキュリティ教育といった組織的な対策，そしてバイオメトリクス認証による入退管理や災害対策のような物理的な対策まで，情報セキュリティ対策という言葉で括られる製品，サービスは数多く存在する．

このような状況の中で，日本ユニシスでは1998年から，情報セキュリティに関する製品・サービスを網羅的に統合したセキュリティサービスメニュー「iSECURE」として提供している．

筆者が，このサービスメニューの提案支援活動を通じて顧客からよく受けた質問は「数ある製品・サービスの中で，最も投資対効果の高い情報セキュリティ対策は何か」というものであ

った．

情報セキュリティ対策の多くは，想定されるリスクの顕在化を予防するための事前措置である．そのため，一般的には，SCM[*1],ERP[*2]，会計システムなどに代表される情報システムのように，売上増，業務効率の改善によるコスト削減といった投資対効果の観点では説明しにくいとされている．

しかしながら，情報セキュリティ対策にもそれ相応のコストがかかる．投資額の妥当性を判断し，数ある対策に優先順位をつけて，より投資対効果の高い情報セキュリティ対策を迅速に実施するためには，守るべき情報資産に対するリスクを評価することが有効である．

一般的なリスク評価では，あるリスクを他のリスクとの相対的数値で表すことが多い．しかしながら，この手法ではリスクの大きさを認識することはできても，そのリスクに対して妥当な投資額を判断することは難しい．

本稿では，リスクマネジメントの全体像を記述した上で，より投資対効果を計りやすい数値としてリスクを定量化するための手法を記述する．

2. 情報セキュリティにおけるリスクマネジメント

2.1 情報セキュリティにおけるリスクの考え方

情報セキュリティ対策を考える上で，リスクをどのように捉えるかは非常に重要である．そのため，本節ではリスクに関連する用語とその定義について述べる．

システム管理者向けの情報技術セキュリティ管理指針に関する報告書である「ISO/IECTR 13335（通称 Guidelines for the Management of IT Security，略称 GMITS)」の邦訳として経済産業大臣より公表された報告書「TR X 0036」[1]では，リスクを次のように定義している．

リスク：ある脅威が，資産または資産グループの脆弱性を利用して，資産への損失，または損害を与える可能性
脅威　：システムまたは組織に危害を与える，好ましくない偶発的事故の潜在的な原因
脆弱性：脅威によって影響を受け得る資産または資産グループの弱さ

（「TR X 0036-1 : 2001」 用語及び定義より抜粋）

この定義に基づくと，脅威，脆弱性，資産価値のいずれかが増加するとリスクが増大することになる．そのため，脅威，脆弱性，資産価値を識別し，それに適切な対策を施すことがリスクを低減させるための方策であるといえる．

「TR X 0036」ではリスクを脅威，脆弱性，資産との関係で説明している．これに対し，リスクを事業との関係で説明したものとして，2003 年 6 月に経済産業省が設置したリスク管理・内部統制に関する研究会が発表した報告書「リスク新時代の内部統制～リスクマネジメントと一体となって機能する内部統制の指針～」[2]がある．

この報告書では，リスクを事象発生の不確実性と捉えた上で，損害の発生の可能性のみでなく，例えば新規事業進出などによる利益又は損失の発生可能性も含むものであるとしている．

「BS 7799-2 : 1999」を基に，財団法人日本情報処理開発協会が公表した規格である，情報セキュリティマネジメントシステム適合性評価制度「ISMS 認証基準（Ver 2.0)」[3]ではリスクの考え方として「TR X 0036」における定義を基礎としている．本稿においても「TR X 0036」における定義を基礎とする．

2.2 リスクマネジメントの概要

「ISMS 認証基準（Ver 2.0）」では，リスクマネジメントの用語として，リスク一般の用語を定義した標準情報である「リスクマネジメント−用語−規格において使用するための指針（以下 TR Q 0008 : 2003）」[4]の定義を採用している．

「TR Q 0008 : 2003」によると，リスクマネジメントとは，「リスクに関して組織を指揮し管理する調整された活動」と定義されており，リスクマネジメントは，

① リスクアセスメント
② リスク対応
③ リスクの受容
④ リスクコミュニケーション

を含む概念であると説明されている．

次節以降で，リスクアセスメント，リスク対応，リスクの受容，リスクコミュニケーションそれぞれの概要を記述する．

2.3 リスクアセスメント

リスクアセスメントとは，リスクの分析から評価までの過程を指すものである．具体的には，情報資産を識別し，それにまつわる脅威，脆弱性を識別する．そして，リスクが発生する可能性及び，リスクが発生した場合の損害額を算定する「リスク分析」と，リスク分析で算定したリスクをどのように評価するかの「リスク評価」までの過程である．リスクアセスメントについては 3.1 節以降でさらに詳細に記述する．

2.4 リスク対応

「TR Q 0008 : 2003」では，リスク対応の選択肢として，

① リスクの最適化
② リスクの保有
③ リスクの回避
④ リスクの移転

の四つが挙げられている．

「リスクの最適化」とは，言い換えれば適切な対策を実施してリスクを低減することである．リスクを完全になくすことは不可能なため，投資対効果や利便性を考えた上で情報セキュリティ対策を実施し，受容可能な水準までリスクを低減させることになる．リスクの低減については，リスクが発生する確率を低減させることと，リスクが発生した場合の影響を低減させる方法に分けられる．対策実施後の残存リスクについては，リスクの保有の対象として管理する．

「リスクの保有」の対象となるリスクは，一般的に識別されたリスクと識別されずに組織に内在しているリスクの 2 種類に分けられる．識別されていないリスクも含めて，リスクが発生した際の損失及び利益に対して内部留保をおこなう場合もあるが，「ISMS 認証基準（Ver.2.0）」では識別されたリスクのみを対象としている．

「リスクの回避」は，リスクへの対応を検討した際に，投資対効果の観点から対策の実施が妥当ではない場合や，有効な対策がない場合などに採られる．具体的には，事業からの撤退，情報資産の廃棄といった方法が挙げられる．

「リスクの移転」は，契約等によりリスクを他者に移転することである．アウトソーシングとして情報資産や情報システムの運用を外部委託する方法と，保険等を利用する方法の大きく2種類に分けられる．リスクを移転した際には，移転したリスクと移転しなかったリスク，そしてリスクを移転したことにより新たに発生するリスクの3点を明確にする必要がある．

2.5　リスクの受容

リスクの受容とは，リスクアセスメントの結果識別されたリスクの中で，様々な要因から対策を見送ったリスクを経営陣が確認し，適切と判断し承認する意思決定である．そのためには，リスクアセスメントにおけるリスクの評価基準の確立と共に，リスクをどこまで許容するかという受容リスク水準の明確化が必要である．

2.6　リスクコミュニケーション

リスクコミュニケーションとは，意思決定者と他のステークホルダーの間におけるリスクに関する情報の交換または共有のことである．ここでいうステークホルダーとは，リスクに対して影響を与えるもしくは受けると認識される個人やグループ又は組織を指す．

ステークホルダーの具体例としては，顧客や組織内の従業員，労働組合といった利害関係者が挙げられる．また，広義の意味のリスクコミュニケーションでは，組織内における経営陣と事業部門間のコミュニケーションも含まれる．

3.　リスクアセスメントの詳細

3.1　リスク分析とリスク評価

リスクアセスメントは，リスクの分析から評価までの過程を指すものであるが，3章では，「ISMS認証基準（ver 2)」に基づいて，リスクの分析を

① 情報資産の洗い出し
② 脅威の識別
③ 脆弱性の識別

の三つに分けて述べる．また，リスクの評価についても，

① 損害の評価
② 脅威の評価
③ 脆弱性の評価

の三つに分けて解説する．

3.2　情報資産の洗い出し

情報資産の洗い出しでは，情報資産の保有状況を確認すると共に，情報資産の属性や価値(機密性，完全性，可用性)を明確にする必要がある．属性とは具体的には，保管形態，保管期間，用途等を指す．また，それぞれの情報資産に対して管理責任者を特定することが望ましい．

情報資産の洗い出し作業は非常に負荷の高いものであるが，作業実施の際に情報資産のグループ化を実施すると，作業負荷軽減及び今後の分析作業の効率化が図れる．情報資産のグループ化とは，例えば同じ属性（保管形態，保管期間，用途等）や同じ重要性を持つ情報資産を一つのグループとすることである．属性や重要性が同じで，結果的に適用されるセキュリティ対

策が同じであれば，同じグループとしてまとめて管理することが効率的である．

3.3　脅威の識別

脅威とは，情報システムや組織に損失や損害をもたらすセキュリティ事故の潜在的な原因である．脅威は次節で記述する脆弱性により誘引され，顕在化するものである．

「TR X 0036」では，脅威を人為的脅威と環境的脅威に大別した上で，さらに人為的脅威を，意図的（計画的）脅威と偶発的脅威に分けている．脅威を識別するためには，まずこのように脅威を大別することが必要である．そして，例えば意図的脅威であれば，攻撃者の動機，攻撃に要するスキル，利用可能なリソースを考慮に入れ，さらに，情報資産の特性，脆弱性などからどのような要因が脅威であるかを識別することが有効である．

3.4　脆弱性の識別

脆弱性とは，脅威の顕在化を誘引する情報資産が持つ弱点やセキュリティホールのことである．脆弱性は脅威を顕在化させ，損害や障害を発生させる可能性を持っている．脅威が存在しない脆弱性については，損害や障害を発生させる可能性がないため，あまり重要視する必要はない．

脆弱性は情報資産の性質や属性と関連付けて検討すると識別が容易である．例えば，ノートパソコンであれば，「持ち運びし易い」，「衝撃に弱い」といった性質が挙げられるが，それと同時にその性質は，「盗難や置き忘れ」，「故障」という脅威に対する脆弱性にもなるのである．そのため，脆弱性は脅威と関連付けて整理することが重要である．

3.5　リスク分析手法の紹介

「ISMS 認証基準（ver 2)」に基づいてリスク分析における作業を個別に記述してきた．それ以外の手法として，「TR X 0036」で述べられている四つのアプローチに関して記述する．

「TR X 0036」ではリスク分析の手法として，以下の四つを紹介している．

① ベースラインアプローチ
② 詳細リスク分析
③ 組み合わせアプローチ
④ 非形式的アプローチ

ベースラインアプローチとは，一定のセキュリティレベルを設定した上で，必要な対策を選択し，対象となる情報資産に一律に適用することである．

詳細リスク分析とは，情報資産ひとつひとつに対して，資産価値，脅威，脆弱性やセキュリティ要件を識別し，評価することである．

組み合わせアプローチとは，複数のアプローチを組み合わせ，それぞれの長所短所を補完し，作業の効率化や分析精度の向上を図る手法である．

非形式的アプローチとは，担当者の経験や判断によってリスクを評価する手法である．

これらのアプローチのどれを採用すべきかは，情報資産に求められるセキュリティ要求事項（事業，法律，契約など）に依存するので一概に判断できるものではない．「TR X 0036」ではどのアプローチが適切であるかを確定するための方法として，上位リスク分析を紹介している．

「TR X 0036-3 9.1　上位リスク分析」では，どのアプローチが適切であるかを決定するため

の要素として，以下を挙げている．

① IT システムを使って達成するべきビジネスの目的
② 組織のビジネスが IT システムに依存している度合い
③ システムの開発，保守，又は変更という点での，この IT システムへの投資レベル
④ 組織が直接価値を認めている IT システムの資産

これらの項目を評価することで，自社にどのアプローチを採用するかを決定するのである．

3.6 損害の評価

「ISMS 認証基準(ver 2)」における損害の評価では，情報資産の価値を評価するのではなく，情報資産の機密性（confidentiality），完全性（integrity），可用性（availability）が損なわれた場合の影響度を評価する．一般的には，要素ごとに 3〜5 段階にレベル分けする等の方法が採られる．この際，機密性，完全性，可用性の平均値を評価すると誤った対策を実施してしまう危険性がある．そのため，可用性はあまり求められないが，機密性が求められる情報資産など，情報資産の特性を考慮する必要がある．

3.7 脅威の評価

脅威の評価では，リスク分析の結果，作成した脅威一覧に基づき，業務上の経験や過去の統計データを加味して脅威のレベルを評価することになる．一般的には「低い」,「中程度」,「高い」の三つの区分に分ける場合が多いが，自社の環境に合わせて評価区分を変えていくことが重要である．

3.8 脆弱性の評価

脆弱性の評価では，情報資産の持つ弱点，セキュリティホールがどの程度であるかを評価する．脆弱性の評価区分についても脅威の評価と同様に「低い」,「中程度」,「高い」といった区分に分けることが多い．

脆弱性の評価では，現在実施されている対策を考慮する．例えば，十分な対策が施されている場合は，脆弱性は少なくなる．そのため，脆弱性の評価に当たっては，情報資産に対して実施している対策をリストアップする必要がある．

4. リスク評価の課題と損失予想額の算出

4.1 リスク評価の課題

リスクアセスメントの結果に基づいて，対策を実施するリスク，受容するリスクを決定していく．一般的におこなわれているリスク評価の多くは，情報資産の価値，脅威，脆弱性を相対的にレベル分けしている．例えば，「ISMS 認証基準（ver 2)」では，リスクの大きさであるリスク値の計算式として以下の式を紹介している．

リスク値＝「情報資産の価値」×「脅威」×「脆弱性」

「情報資産の価値」,「脅威」,「脆弱性」の各々のレベルの乗算から求めたリスク値を参考にしてリスクの大きさを判断し，より優先度の高い対策を実施していくことが可能である．

しかしながら，このリスク値のみでは，自社における相対的なリスクの大きさを認識することはできても，リスク対策に要する費用が適正かどうかの判断は難しい．

例えば，リスク値 24 のリスクに対して 1000 万円の投資が妥当かどうかという投資対効果を計るためには，リスクを相対的数値ではなく，予想損失額というセキュリティ対策の投資対効果をより計りやすい形で定量化する必要があると言える．

特に個人情報漏洩など，顕在化した場合の影響が大きいリスクについては，予想損失額という形でリスクを定量化し，情報セキュリティ対策の投資対効果を見極め，迅速な経営判断を下すための一助とすることが望ましい．

4.2 リスク定量化手法の概要

本稿ではリスクを定量化するための手法として，Annual Loss Expectation（以下 ALE）によるリスク定量化の手法を採りあげる．ALE とは，何らかのセキュリティ事故によって，企業が 1 年間に被ると予測される損失額のことである．この手法では，まず自社の現状に基づいて識別された個別のリスクに対して，以下の計算式で年間の予想損失額を算出する．

ALE（年間予想損失額）＝年間発生頻度×予想損失額

予想損失額とは，個別のリスクが 1 回顕在化するごとに被る被害額の予測値である．また，年間発生率は，リスクが 1 年間に顕在化すると予測される回数を指す．

リスクが顕在化する確率及び予想される損失額は，実施する情報セキュリティ対策によって変化する．ALE を活用して情報セキュリティ対策の投資対効果を計るためには，修正 ALE という数値を算出する必要がある．修正 ALE とは，対策実施によるリスク顕在化の確率及び予想損失額の変化を反映させて，ALE を算出し直した数値である．

ALE と修正 ALE を比較することで，特定の情報セキュリティ対策の実施によってどの程度の年間予想損失額の低減が見込めるのかを明確にすることが可能となる．

5. リスク定量化の算出方法例

5.1 リスク定量化のステップ

リスクの定量化をおこなうためにはまず，リスクアセスメントを実施し，自社が保有しているリスクを明確にすることが不可欠である．

ALE によるリスク定量化では，洗い出した個別のリスクに対して，リスク顕在化の確率，及びリスクが顕在化した場合に被ると予想される予想損失額を見積もり，その乗算から年間予想損失額を算出する．次節以降で，リスク顕在化の確率及び予想損失額の算出方法例について記述する．

5.2 リスク顕在化の確率の算出

リスクが顕在化する確率を正確に算定することは困難であるが，統計的データや経験的データからある程度の数値を算出することは可能である．具体的には，自社における過去の実績データ（システム障害や社内犯罪など），システム利用者の状況（情報リテラシー，利用者数，利用頻度など），また，公的機関が発表している情報などを利用する．

リスク顕在化の確率を算出する上で使用するデータは，想定するセキュリティ事故によって異なってくる．

例えば，現在，社会の関心が最も高いと言える個人情報の漏洩について考えてみると，一般的に個人情報の漏洩は個人情報データベースに対して正規のアカウントを持つユーザによる漏

洩と，不正アクセスによる漏洩との 2 種類に分けられる．

正規のアカウントを持つユーザによる個人情報の漏洩については，情報セキュリティに関する犯罪発生率を表す適切なデータが現在のところ存在しない．そのため，犯罪白書といった公的データを参考に推察する必要があるであろう．例えば，法務省の「犯罪白書平成 15 年版」[5] によると，日本における窃盗の発生率は，10 万人当たり 1437 件であり，1 年あたりの発生確率は 1.4% である．あくまでデータからの推察であるが，利用者が 100 人いれば，年間およそ 1 回の割合で個人情報が漏洩してしまう計算になる．

正規のアカウントを持たない者の不正アクセスによって個人情報が漏洩してしまう確率を算出する際には，現在公表されているデータが参考になる．例えば，独立行政法人情報処理推進機構（IPA）のセキュリティセンターが毎月公表している不正アクセス届出状況が挙げられる．これによると，2005 年上半期（1 月〜6 月）では，不正アクセスの届出件数は 319 件であり，その内実際に侵入やメール不正中継などの被害に遭ったケースは 89 件に及び，前年比約 2.5 倍の増加となっている．届出は任意のため，直接このデータから個人情報が漏洩する確率を計算するのは難しいが，自社の状況に照らし合わせて大まかな傾向をつかむことは可能である．

また，最近では，「1 : 29 : 300 の法則」を使用して，情報漏洩の発生確率を推定する方法も挙げられている．「1 : 29 : 300 の法則」は米国のハインリッヒ氏が労働災害の事例の統計を分析した結果導き出されたもので，「ハインリッヒの法則」とも呼ばれている．これによれば，1 件の重大災害の裏には 29 件のかすり傷程度の軽災害があり，その裏にはケガはないがヒヤリとした 300 件の体験があるとしている．つまり，不正アクセスに当てはめると，330 件の悪意ある攻撃があるとすると，そのうちの 30 件が事故につながり，その中の 1 件は重大な事故であるという試算である．不正アクセス検知を行っている企業であれば，この法則を参考に，情報漏洩事故の発生確率を概算することは可能であると言える．

このように，想定するセキュリティ事故の発生原因を考慮して，それに適合するデータや分析手法を利用することで，リスク顕在化の確率を見積もることが可能である．

5.3　予想損失額の算出

予想損失額を算出するためには，個別のリスクが顕在化した際に被ると予想される損失の構成要素を洗い出す必要がある．損失には，復旧などに要した人件費や業務停止による逸失利益，損害賠償費用など様々な要素が考えられるが，本稿ではこれらの構成要素を大きく二つに分類する．

まず一つ目として，復旧に要するコスト，事故対応に要するコスト，システム停止による逸失利益を，リスクが顕在化することで生じる 1 次的な損失額である「直接損失額」とする．次に二つ目として，各種の補償や損害賠償請求費用などの 2 次的な損失額を「間接損失額」とする．

実際にセキュリティ事故が発生してしまった場合，一般的に，企業には再発防止策を実施することが求められる．この際，外部にコンサルティングを依頼するコストや対策実施にかかるコストなどが発生すると考えられるが，ALE によるリスク定量化は，あくまで対策を実施することによって，どの程度年間予想損失額を軽減できるかを計るための手法である．そのため，再発防止対策コストについては予想損失額を算出する上では対象外とする．

直接損失額は，以下のような式で算出することができる．

直接損失額＝逸失利益＋復旧に要するコスト＋事故対応に要するコスト
＝（年間想定売上高÷365×業務停止日数）
＋（復旧対応をおこなう人数×原価×復旧にかかる日数＋
ハードウェア・ソフトウェア費用）
＋（事故対応をおこなう人数×原価×事故対応にかける日数）

復旧にかかる日数については，想定するリスクを，自社の過去の事例やシステム構成などと照らし合わせて見積もる必要がある．また，暫定的対応としてハードウェア・ソフトウェアが必要となる可能性にも留意すべきである．事故対応については，例えば，個人情報が漏洩した際の顧客からの問い合わせ窓口設置や，取引先への営業的対応のそれぞれに必要とされる人数及び日数を見積もる必要がある．

間接損失額を算出するためには，2 次的に発生すると想定されるコストを洗い出す必要がある．2 次的なコストの例としては，補償，損害賠償費用，謝罪広告費用などがある．間接損失額については以下のような式で算出できる．

間接損失額＝補償・補填費用＋損害賠償費用＋謝罪広告費用

補償，補填費用の具体例としては，個人情報漏洩事故事例に見られるような，お詫び金が挙げられる．昨今の個人情報漏洩事故事例では，個人情報が漏洩した企業がその被害者に対して，お詫び金として 500 円〜1000 円の金券を配布するケースが見られる．このような事例を参考にして費用を見積もることが有効である．

損害賠償費用の見積もりについても個人情報漏洩事故事例から考える．個人情報漏洩事故から損害賠償請求訴訟に発展した場合，企業が被る損失は莫大なものになると予想される．想定損害賠償額を見積もる上でよく参考にされるのは，京都府宇治市の住民情報漏洩事件である．この事件では，「基本 4 情報（氏名，住所，性別，生年月日）を漏洩した場合，慰謝料は 1 人につき 1 万円とする」という判例が出ている．漏洩した個人情報の内容によって想定される損害賠償額は異なってくるため，判例から想定損害賠償額を見積もるには，自社の保有する個人情報の内容と合致する個人情報漏洩事故の判例を参考にする必要がある．

想定損害賠償額を見積もる手法としては日本ネットワークセキュリティ協会から「2004 年度　セキュリティインシデントに関する調査報告書　ver 1.0」[6]が公開されている．この報告書では，個人情報漏洩事故を漏洩個人情報価値，情報漏洩元組織の社会的責任度，事後対応評価の三つの要素で分析してレベル分けし，想定損害賠償額をこの 3 要素の乗算で求めている．

また，顕在化した場合の影響が甚大であると推測されるリスクについては，謝罪広告費用についても考慮する必要がある．

このようにして算出した直接損失額と間接損失額の和が予想損失額となる．

予想損失額＝直接損失額＋間接損失額

5.4　ALE の算出と修正 ALE

算出したリスク顕在化の確率と予想損失額から，現状での年間予想損失額（ALE）を算出する．ALE は 1 年間にリスクが顕在化する頻度と，リスクが顕在化した場合に被ると予想される予想損失額の乗算で求められる．

当然のことながら，リスクが顕在化する確率及び予想される損失額は実施する情報セキュリティ対策によって変化する．ALE を活用して，情報セキュリティ対策の投資対効果を計るた

めには，対策実施による変化を反映させて，修正 ALE を算出する必要がある．

修正 ALE の算出には，実施する情報セキュリティ対策を，リスクが顕在化する確率を低減させる対策，リスクが顕在化した際の被害を低減させる対策，両方の効果が見込める対策のように分類することが有効である．

例えばリスクアセスメントの結果からリスクを分析したところ，リムーバブルメディアを利用した内部からの個人情報漏洩というリスクの予想損失額が 5000 万円，1 年間にリスクが顕在化する頻度が 0.5，つまり 2 年に 1 回であるとすると，ALE は以下のように計算できる．

ALE＝5000 万円×0.5＝2500 万円

このリスクに対して，暗号化などによるデータ保護ソフトを導入した場合，リスク顕在化の頻度を 0.1，つまり 10 年に 1 回まで低減させることができるとすると，修正 ALE は，

修正 ALE＝5000 万円×0.1＝500 万円

となる．この場合，データ保護ソフトの導入に必要な費用が 1000 万円だと仮定すると，実際には，可用性や運用方針なども考慮に入れる必要があるが，投資対効果の面では導入を検討する余地は十分にある．

このように，年間予想損失額としてリスクを定量化することは，情報セキュリティ対策への投資対効果を計る上で有効である．しかし，リスクアセスメントが的確におこなわれていなければ，情報資産の脅威，脆弱性からリスク顕在化の確率や予想損失額を信頼できるデータとして算出することは難しい．リスクを定量化するためには，リスクアセスメントは必要不可欠なのである．

5.5　リスク定量化の留意点

年間予想損失額としてリスクを定量化することは，情報セキュリティ対策への投資額を考える上で有効である．しかし，リスクアセスメントの結果洗い出した全てのリスクに対して定量化を実施することは，必要となる人的コストから考えても現実的ではない．

リスクを定量化する目的は，経営者が情報セキュリティ対策の投資対効果を計るための指標を提供することである．そのため，定量化を実施するリスクの対象は，リスクアセスメントの結果を踏まえ，自社に重大な損失を与える可能性があるリスクに絞るべきである．

また，一般的に投資対効果を計るための指標を算出する際には，より精密な数値を算出しようとする傾向が強い．しかしながら，情報セキュリティにおけるリスクは日々刻々と変化している．精密な数値を算出するために時間を費やしている間にリスクが変化してしまう可能性もある．予想損失額が 1000 万円であるか，1100 万円であるかというデータはあまり重要ではない．重要なのは精密な数値ではなく，自社の環境に即した正確な数値を経営者に提供し，より迅速な意思決定を可能とすることなのである．

6.　お　わ　り　に

情報セキュリティ対策を適切に実施していなければ，莫大な損失につながるような事故・事件が発生してしまう可能性がある．しかし，どの程度の確率で，どれほどの損失が発生するのかが分からなければ，具体的な対策をどのレベルまで実施すべきかを迅速かつ的確に決定することは極めて難しい．そのため，リスクを相対的なレベル分けだけではなく，予想損失額という，より投資対効果を計りやすい数値として定量化することは極めて重要であろう．

しかしながら，予想損失額を元に，有効な対策を的確に実施したとしても，その対策が永久に有効なものであるとは言えない．情報セキュリティを考える上で忘れてはならないのは，情報セキュリティ対策は一過性のものではないということである．リスクは不変のものではない．実施時は有効であった対策が，リスクの変化と共に全く意味を成さないものになってしまう可能性がある．

リスクの変化を想定し，計画的に対策を実施できるようになることが理想ではあるが，日々刻々とリスクが変化している現状ではそれは難しい．そのため，情報資産のセキュリティを確保するには，常に変化するリスクを定期的に分析し，それに即した対策を迅速かつ継続的に実行していくことが必要なのである．

＊1　SCM：Supply Chain Management の略．原材料の調達，製造，流通，販売までの一連の流れを管理して，サプライチェーン全体の動きを見ながら，経営判断の迅速化を図る意思決定システム．

＊2　ERP：Enterprise Resource Planning の略．企業全体を経営資源有効活用の観点から統合的に管理し，経営の効率化を図る業務横断型のソフトウェア．

参考文献

［1］ 日本工業標準調査会 「TR X 0036-1」 1996 年

［2］ リスク管理・内部統制に関する研究会 「リスク新時代の内部統制～リスクマネジメントと一体となって機能する内部統制の指針～」 2003 年

［3］ 財団法人日本情報処理開発協会 「ISMS 認証基準（Ver 2.0）」 2003 年

［4］ 日本工業標準調査会「リスクマネジメント-用語-規格において使用するための指針」2003 年

［5］ 法務省「犯罪白書　平成 15 年版」2003 年

［6］ 日本ネットワークセキュリティ協会 「2004 年度　セキュリティインシデントに関する調査報告書　ver 1.0」 2005 年

［7］ 小見志郎 「情報資産のリスクマネジメント」 株式会社ぎょうせい　2005 年

［8］ 塚田孝則 「企業を守るセキュリティポリシーとリスク評価-組織的対策と技術的対策」 日経 BP 社　2001 年

［9］ 情報処理推進機構　セキュリティセンター 「情報セキュリティインシデントに関わる調査報告書　Ver 1.0」 2002 年

執筆者紹介　岡　本　卓　馬 （Takuma Okamoto）

2003 年日本ユニシス(株)入社．情報セキュリティ関連サービスの提案及びビジネス企画を経て，2004 年より流通向けシステムサービスに従事．現在，日本ユニシス・ソリューション(株)産業流通第一サービス本部に所属．