情報セキュリティにおける負荷の少ない効果的なリスク分析手法の提言

㈱オリエントコーポレーション

■ 執筆者Ｐｒｏｆｉｌｅ ■

1987 年　㈱オリエントコーポレーション入社
　　営業店勤務（営業推進担当）
1991 年　システム開発部
1997 年　事務システム統括室
2000 年　グローバルフォーカス㈱出向
　　ISMS 構築・運営管理担当
2004 年　㈱オリエントコーポレーション
　　システム企画部
　　情報セキュリティ管理担当

■ 論文要旨 ■

情報通信技術の発達した現代の IT 社会において，企業の所有する情報資産は，その安全性を脅かす多くのリスクに曝されている．このような環境において，増大するリスクに適切に対応し，事業を持続的に発展させるためには企業における効果的な情報セキュリティ対策の実装は必要不可欠なものである．
しかしながら，企業に対する各種の調査結果からは，情報セキュリティ対策の実装レベルについて適切に判断できていない状況が伺える．そして，その原因の一つとして，リスクに対する適切な分析方法が分からないということが言われている．
そこで，本稿では，情報セキュリティにおける現状のリスク分析手法を調査し，その特徴及び内在する問題点を整理する．そして，筆者が経験してきたリスク分析の実践結果から得られた経験値を踏まえ，それらの問題点を解決する新たなリスク分析手法を提言する．

目　次

図表一覧

１．はじめに

１．１　企業における情報セキュリティの取組み

ここ数年，企業の情報セキュリティをめぐるインシデント（Incident；情報漏洩事件，システム事故など）の発生が増加傾向にある．頻発する個人情報漏洩事件，コンピュータウィルスによるシステムダウン，不注意によるオペレーションミスに伴う情報の誤更新など，一度セキュリティインシデント（Security Incident）が発生するとその影響は一時的な損失に収まらず，企業経営の存在そのものを危うくする場合もある．

一方，2005年4月に全面施行された個人情報保護法や，2006年6月に制定された金融商品取引法（日本版SOX（Sarbanes Oxley）法[1]）など，法令などの適合性（Compliance）の観点から，企業の社会的責任（Corporate Social Responsibility：CSR）[2]を問う流れも加速してきており，（社）日本経団連は2004年5月18日に改定した企業行動憲章[１]の中で，「企業は利害関係者との対話を重ねつつ，法令順守を基本として社会的責任を果たすことにより，社会における存在意義を高めていかねばならない．」としており，企業自らが，自らの責任において社会的責任性に配慮する姿勢を示している．

こうした動きを受けて，企業においては，これまでのように，まず対策ありきで場当たり的に，ITセキュリティ対策（ファイアウォールやウィルス対策ソフト，IDS（不正侵入検知システム）など）を導入するだけではなく，法令などの適合性(Compliance)や利害関係者への説明責任を意識した経営戦略上のリスクマネジメント(Risk management)の観点から，情報セキュリティを捉える動きも増えてきている．

このことを物語る事例として，日本においては，2002年に運用開始された「情報セキュリティマネジメントシステム（ISMS）適合性評価制度」におけるISMS認証を取得する企業が増えてきている．[3][２]このISMSにおいて，費用対効果のある効果的な情報セキュリティ管理策を実装するためには，リスク分析（risk analysis）は必須プロセスであるが，現状では，日本におけるリスク分析の実施状況に関して，「不正アクセス対策に関するアンケート報告書；平成12年度警察庁調査」[３]の結果から，全体の約90%もの企業がリスク分析を実施していないことが判る．

それらの企業においてリスク分析を実施していない理由の約50%は，「コストや時間が掛かり過ぎる」ことが挙げられており，そのほか「適切な手法がない」，「分析のためのデータが乏しい」，「分析の効果がわからない」が各30%近くを占めている．

これらのアンケート結果から，企業においては，高い作業負荷やセキュリティに関する専門的スキルの不測が原因で，リスク分析が実施されていないことが推測できる．

その後，平成15年度に同様に実施された，「不正アクセス行為対策などの実態調査：平成15年度警察庁調査」[４]においても，企業において効果的な情報セキュリティ対策

---

1 日本版 SOX（Sarbanes Oxley）法；米国の SOX 法に倣って、会計監査制度の充実と企業の内部統制強化を求める日本の法規制。米国の SOX 法と異なる点として、COSO フレームワークの 5 つの構成要素に加えて IT の利用（IT 統制）が加えられている．

2 企業の社会的責任（Corporate Social Responsibility）；企業の責任を，従来からの経済的・法的責任に加えて，企業のステークホルダー（社内外の利害関係者，従業員，消費者，取引先に加え地域社会も含める）にまで広げる考え方のこと．

3 日本情報処理開発協会（JIPDEC）の発表によると，2005 年 8 月時点で日本の ISMS 認証取得事業者数は，1，014 件となっている．

を実施するうえでの問題点として，「コストがかかり過ぎる（50.6%）」，「費用対効果が見えてこない（50.6%）」，「どこまで行えばよいのか基準が示されていないため判断できない（50.2%）」との結果が出ており，その状況はあまり改善されていない．

１．２　当社の情報セキュリティへの取組み

当社においても，顧客の個人情報保護の観点から情報セキュリティの重要性は早くから認識されており，平成13年には，情報セキュリティポリシーを策定し，ポリシーに基づき様々な情報セキュリティ対策を継続的に実施してきている．

また，情報子会社であった，グローバルフォーカス㈱（現，富士通クレジットソリューションズ(FCSOL)社，以下GF社という）において，2003年に情報セキュリティ管理のグローバルスタンダードであるBS7799の認証取得した．その後，もう一つの情報子会社である，㈱システムオリコ社においても2006年5月にISMS認証とBS7799認証を同時取得し，システム部門における情報セキュリティマネジメントの推進について積極的に取り組んでいるところである．

筆者は，当時のGF社において，情報セキュリティ管理の業務に携わっており，BS7799に基づいた情報セキュリティマネジメントシステム（以下ISMSという）の構築に関ってきた．当時は，ISMS認証取得企業の数も少なく，解説本などもあまり存在しない状況であり，リスク分析の実施についても，１．１節の企業におけるリスク分析実施に関する調査結果で述べたような同様の悩みを抱えつつ，手探りでの試みであった．

本稿では，筆者が経験してきたISMSにおけるリスク分析活動の試行錯誤の実践経験を踏まえ，企業のリスク分析における問題点及び課題を整理したうえで，その実施負荷（時間，労力）を極小化しつつ，経営者及びその関係者が納得できる結果を享受できる新たなリスク分析手法の確立を目指すこととする．

なお，本稿で述べるリスク分析の範囲は，「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TR Q 0008：2003（ISO/IEC GUIDE 73：2002）」[５]の定義における，「リスクアセスメント」，「リスク対応」，「リスクの受容」までを，その対象範囲とする．

２．リスク分析手法の種類とその特徴

２．１　情報セキュリティにおけるリスク分析

情報セキュリティにおけるリスク管理において，リスク分析は，組織の情報資産に影響を及ぼすリスク因子を特定し，そのリスクの程度を評価したうえで，経営判断に基づきリスクに対する対応方針を選択，リスクの受容可否を決定するプロセスである．

国際標準ガイドラインとして，ITセキュリティ管理の標準手法を提供するISO/IEC TR 13335（以下GMITS）[６]では，ITセキュリティマネジメントにおけるリスク管理プロセスの中でのリスク分析の位置づけについて，効果的，効率的なセキュリティ対策を選択するための判断尺度として，リスクを評価，特定するプロセスであるとしている．

また，リスク分析手法の4つの戦略的アプローチとして，「ベースラインアプローチ(Baseline Approach)」，「非形式アプローチ(Informal Approach)」，「詳細リスク分析アプローチ(Detail Approach)」，「組み合わせアプローチ(Combined Approach)」を

提示しており，その特徴及び長所，短所を含めて具体的に述べている．【表１】

手法	特徴	長所	短所
ベースライン アプローチ (Baseline Approach)	予め決めた一定の確保すべきセキュリティレベルを満たすために必要な対策を選択し適用する手法	大規模対象でも時間や負荷がかからない	対象が過度や不十分になる可能性がある
非形式アプローチ (Informal Approach)	組織や担当者の経験や判断によってリスクを評価する手法	詳細リスク分析に比べ時間や負荷が少ない	見落としや見方の偏りの可能性がある
詳細リスク分析 (Detail Approach)	情報資産に対して「価値」「脅威」「脆弱性」を個々に識別し，リスクの程度を評価する手法	対称個々に適したセキュリティ対策を特定できる	相当な時間，労力，専門知識が必要
組み合わせ アプローチ (Combined Approach)	複数のアプローチを併用し，それぞれのアプローチの長所･短所を相互に補完，作業の効率化や分析精度の向上を図る手法	重要な部分を厳密に分析しつつ，全体も適切に保護でき費用対効果が高い	厳密な分析の部分とほかの部分の特定の適切さに依存

表 1：リスク分析の種類と特徴

（出典：ISO/IEC TR 13335）

これらのリスク分析における一連のプロセスのうち，「リスクの評価」は，効果的，効率的なセキュリティ管理策を選択し，組織として受容するリスクを決定するために必須のプロセスである．そして，この「リスクの評価」の手法として，一般的にリスクの程度を評価する方法の違いにより，「定量的リスク分析手法」と「定性的リスク分手法」の二つの手法が存在する．次に，それぞれの方法の特徴について整理する．

２．２　定量的リスク分析手法

企業経営者の視点から考えると，IT投資において最適な情報セキュリティへの投資を実施するためには，情報セキュリティリスクを一定の指標に基づき定量的に評価することが求められている．

「定量的リスク分析手法[4]」は，通常，リスクを財務的数値指標にて評価するもので，リスクの計算は一般的には，事象の発生頻度（確率）と発生した場合の損失（金額）に基づき以下のように算出する．

“リスク（金額/年）”＝“予想損失額（金額）”×“発生頻度（回数/年）”

ここで，リスク（金額/年）が客観的な納得性を持つためには，“発生頻度（回数/年）”及び“予想損失額（金額）”について信頼性のあるデータが必要となるが，これらの数値について現状では，客観的な数式または明確に定義された保険数理データセットから導き出された信頼性の高いデータを使用することは困難であるとされている．[７]

このため，情報セキュリティにおけるリスク分析手法として日本では，まだ一般化されていないようである．そこで，次にもう一つの分析手法である定性的分析手法について見てみる．

[4] 現在，利用されている定量的リスク分析手法としては，アメリカの NIST（National Institute of Standards and Technology）推奨の方法や FTA（Fault Tree Analysis）法などがある．

２．３　定性的リスク分析手法

「定性的リスク分析手法」は，「定量的リスク分析手法」が確立されていない現状においては，情報セキュリティにおけるリスク分析手法として一般的に広く用いられている．前出のGMITSにおいては，【表１】で見てきたように４つの戦略的手法が紹介されていて，それぞれ長所・短所がある．

リスク分析を実施しようとする組織は，リスク分析を実施する業務システムの範囲（情報資産の保護に責任を有する範囲）及び規模，組織の環境，情報セキュリティマネジメントの成熟度[5]を考慮して最適な手法を選択することになる．

２．４　リスク分析手法の特徴の整理

以上，リスク分析の手法のうちリスク評価の観点の違いから，「定量的リスク分析手法」及び「定性的リスク分析手法」について，分析手法の種類と特徴及び使用状況について整理してきた．ここで，両分析手法の長所及び短所について整理すると以下のようにまとめられる．【表２】

	長所	短所
定量的リスク分析	a)リスクを財務的な数値によって経営陣に示すことができる	a)信頼できる結果と合意に達するプロセスに専門性と時間が必要
定性的リスク分析	a)リスクランクを認知しやすい b)合意に達するのが容易	a)セキュリティ投資の正当化が困難 b)重要リスクが十分識別されない

表 2：定量的・定性的リスク分析の長所・短所

(出典：Microsoft セキュリティリスク管理ガイド)

このように両手法とも分析時間，専門性，精度の点において一長一短があるが，日本のISMS適合性評価制度においては，「ISMSユーザーズガイドーリスクマネジメント編ー（以下，ISMSガイドと呼ぶ）」[８]の中で，ISMS認証基準に準拠した標準的な手法として「詳細リスク分析アプローチ」に基づいたリスク分析手順が紹介されており，日本のISMS認証取得企業において広く採用されている．[９]

そこで，次にこの「ISMSガイド」に記載されている「詳細リスク分析手法」のプロセスを見ていきながら，リスク分析手法の問題点について考察してみる．

３．リスク分析手法のプロセスとその問題点

「詳細リスク分析手法」は，リスク分析を実施する対象範囲における情報資産を洗い出し，資産に対する脅威と脆弱性を識別することでリスクを評価する手法である．ここでは，この詳細リスク分析について「ISMSガイド」に基づいたうえで，筆者のリスク分析経験も交えて考察し，その問題点を抽出する．

３．１　保護資産の識別

[5] 情報セキュリティマネジメント成熟度；現状の情報セキュリティ対策が，どの程度のレベルに到達しているかを，成熟度モデルを使用し，ある程度数値化して示したもの．代表的な成熟度モデルとしては，IT ガバナンスの成熟度モデルである COBIT（Control Objectives for Information and related Technology）がある．COBIT では，レベル０（存在しない）からレベル５（最適化されている）までの 5 段階のレベルで評価が行われる．

情報セキュリティに投資可能な経営資源は限られている．リスクに対して不必要に対策実装の範囲を広げることは，投資効率の観点から望ましくない．そこで，リスク分析において，リスクに対して情報資産の保護が最も必要となるような範囲を明確にした上で，その範囲において保護する必要がある情報資産を特定する必要がある．

保護資産の識別では，リスク分析の対象範囲において，何処に，どれくらいの価値の，どのような資産が存在し，それらの資産は業務において，どのような環境で使用されているのかを調査する．通常，情報資産には，業務上，資産を扱う処理環境（ライフサイクル）が存在している．情報の場合を例にすると，入力－処理－保管－出力－転送－持出－廃棄などが考えられ，情報の処理環境は，それぞれのライフサイクルごとに異なるものである．【表３】

このような場合，保護資産に影響を与える脅威や，脅威が利用する環境上の脆弱性もライフサイクルごとに固有のものが想定されるため，リスク分析における保護資産の識別作業では，このライフサイクル分析は大変重要となる．

資産名称	資産価値	資産内容	設置場所	処理環境（ライフサイクル）					
				入力	処理	保管	出力	転送	廃棄
会員マスタ	４：重要	会員情報全般を保有	電算センタ内サーバ	許可者が業務端末で入力	アプリにて更新・削除処理	MTにて定期バックアップ	プリンタ出力後，配送	なし	運用管理者が定期的削除
営業情報管理マスタ	１：公開	営業店の基本情報を保有	〃	〃	〃	〃	なし	〃	なし

表 3：情報資産の識別表（情報の例示）

しかし，この保護資産の識別作業は，業務の規模や範囲にもよるが，業務システムに精通した担当者達の協力を得たうえで，数百種類もの情報資産について具体的に資産の存在場所や処理環境を分析しなければならず，大変時間と労力のかかる作業となる．

３．２　脅威と脆弱性の識別

保護資産の識別が出来たら，各保護資産の業務処理環境（ライフサイクル）ごとに保護資産にセキュリティ上影響を与える脅威と，その脅威が利用する脆弱性（セキュリティ管理の弱点）を識別する．リスク分析を実施する業務システム環境の専門性や複雑さにもよるが，これらの脅威と脆弱性の詳細な識別は，リスク分析を実施する業務システム（業務環境，情報システム全般）についての相当な専門知識が必要とされる．

例えば，「不適切なパスワード及びアクセス制御の欠如」の脆弱性による「不正アクセス・情報漏洩」の脅威の発生は，情報セキュリティの専門化でなくても識別が可能だが，「業務サーバ内の重要情報が，外部からの不正な第三者によって攻撃，侵入されることにより重要情報が改竄または漏洩する．」というようなケースにおいて，具体的な脅威内容とその脆弱性内容については，ネットワークキングやソフトウェア構造に関する技術的な知識や攻撃に関する専門知識が不足していると，リスクを具体的かつ的確に識別することは容易ではない．せっかく資産が洗い出されても，内在する脅威及び脆弱性に気付かなければ，重大なリスクを見過ごすことになる．そこで，情報セキュリティ

の専門知識を持った要員の確保が必要となり，場合によっては外部のコンサルタントや専門化の力を借りる必要もある．

３．３　リスクの評価

リスクを評価するためには，３．１節及び３．２節で識別した保護資産及び脅威と脆弱性について，それぞれ“資産の価値”，“脅威の発生度合い”，“脆弱性の程度”を階層的に数値化し，それらの値を用いてリスク値を計算し，その結果に基づき組織として受容できるリスクかどうかを判断することになる．

３．３．１　資産価値の評価

「ISMSガイド」では，資産価値の評価について，情報資産の機密性，完全性，可用性が損なわれた時の事業上の影響を評価するとしており，例として【表４】のような評価基準が紹介されている．しかしながら，このような事業上の影響の評価は管理責任者の主観に基づくものであり，２．２節の定量的リスク分析手法の問題点でも述べたとおり，事業上の損害を定量的に見積もるのは難しいため，評価結果は常にぶれやすい．

資産価値	クラス	説明
1	低	情報の内容が漏洩，改竄されても業務への影響が少ない
2	中	情報の内容が漏洩，改竄された場合，業務への影響が大きい
3	高	情報の内容が漏洩，改竄された場合，業務への影響が深刻かつ重大

表 4：完全性の評価基準例

（出典：ISMS ガイド）

３．３．２　脅威・脆弱性の評価

次に，脅威及び脆弱性の評価について見てみると，「ISMS ガイド」では“脅威発生の度合い”や“脆弱性によるリスク顕在化の度合い”などにより，レベル分けする基準が紹介されている．しかしながら，資産価値の評価と同様で，脅威や脆弱性の程度についてレベルを分ける評価基準は，結局，評価者の主観的判断にならざるを得ない内容である．そのため，評価者の脅威及び脆弱性に関する専門的知識が不足していると，リスクの程度について現実的な判定をすることは容易ではない．【表５】

レベル	脅威の程度	脆弱性の程度
1	3 年以内には発生しない	最高程度の対策を実施済
2	3 年に一度発生	通常の利用状況では殆どリスクは顕在化しない
3	1 年に一度発生	専門能力ある者の不注意によりリスクが顕在化
4	1ヶ月に一度発生	一般者の不注意により，リスクが顕在化
5	1ヶ月に一度以上発生	常にリスクが顕在化する（対策なし）

表 5：脅威の評価基準例

（出典：ISMS ガイド）

３．３．３　リスクの評価

以上のよう方法で算出された“資産価値”，“脅威の度合い”，“脆弱性の度合い”に基づき，リスクは以下のような計算式で算出される．

“リスク値”　＝　“資産価値”　×　“脅威の度合い”　×　“脆弱性の度合い”

このように算出されたリスク値について，組織のリスク評価基準と比較し，組織として受容可能なリスクを識別していくことになるが，このリスク値は，これまで述べてきたように評価者の主観的判断により評価された“資産価値”，“脅威の度合い”，“脆弱性の度合い”から求められた値であるため，特に受容リスク値の前後（図１のリスク値＝４の前後）では，リスク値が受容レベル未満でも，ほかの要因（例えば法令からの要求事項や社会的責任性）により実際にはリスク対応が必要と判断される場合もあり，逆に受容レベル以上でも，利便性が優先された場合や投資可能コストとの比較などにより，リスク対応が不要と判断される場合も発生するのである．

また，リスク値が明らかに低い（リスク値＝０，１，２）場合は，資産に対する脅威と脆弱性の内容から管理策が不要と判断可能な場合が多く，逆にリスク値が明らかに高い（リスク値＝６，７，８）場合は，無条件に管理策実施の必要があると判断可能である．例えば，数十年に１回程度発生する地震に対して十分な耐震対策を施した電算センタ内にある情報資産への可用性低下リスクを想定した場合，リスク値は明らかに低いと判断可能であろうし，重要な情報が格納されているサーバへのアクセス制御がされてない状態における機密性低下リスクを想定した場合には，リスク値は明らかに高いはずであり，リスク値をわざわざ算出する必要はない．

すなわち，多くの時間と労力をかけて，主観に基づいたリスク評価プロセスを経て定性的なリスク値を算出しても，実際の管理策選定は，保護資産に対する脅威及び脆弱性と対策実施後の残留リスクの内容や，利便性への影響度合いや投下可能コストの程度に基づき，関係者の判断により決定される場合が多いのである．【図１】

	脅威の発生度	低			中			高		
	脆弱性の程度	低	中	高	低	中	高	低	中	高
資産価値	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

リスク値が明らかに高いまたは低いリスクは，リスク値を算出して判断しなくてもリスクの内容だけで判断できる！

リスク受容値の前後は，リスク値以上でも未満でも対策要否判断は分散することが多い！（リスク受容の程度≧４の例）

図 １：リスク値によるリスク評価

３．４　リスク対応

以上のように主観的判断により算定されたリスク値に基づき，リスクを変更させるための方策を選択することになる．リスク対応の選択肢としては，「リスクの減少（risk reduction）」，「リスクの保有（risk retention）」，「リスクの回避（risk avoidance）」，「リスクの移転（risk transfer）」の４つが一般的である．

上記の各リスク対応のうち，通常は「リスクの減少」が最も多く採用される．これは，リスクに対して適切な管理策を適用することで，リスクの発生頻度及び影響を減少させるのだが，実際にはリスクの完全な除去は不可能であるため，対策実施後でも残存するリスクについて「リスクの保有」をすることとなる．

また，保有できないリスクについては，「リスクの回避または移転」を選択し，リス

ク自体を取り除くことになる．ここで，これらのリスク対応により，最終的に「どの程度リスクが低減されたのか？」，「残留リスクは受容リスク基準を満たしているのか？」について，算出したリスク値に基づき経営者が承認することになる．

しかしながら，これまで見てきたようにリスク値は，便宜的に付けられた値（レベル）に基づいて算出されたものであり，理論的根拠のあるものではないため，その判断は曖昧なものとなりやい．例えば，「コンピュータウィルス感染による情報改竄」に対するリスク値が“10”であるとき，「ウィル対策ソフトの導入」管理策により受容リスクレベルまでリスクが低減されるかどうかを数値で客観的に判断することは困難である．

このように，リスク評価によるリスク対応の選択は，常に不確実な要素を含んでおり，最終的には，経営者を含む意思決定に係わる関係者間での調整で決定するしかなく，組織としての判断を組織の責任に基づき行うことになる．

３．５　リスク分析手法における問題点の整理

ここまで，日本の企業におけるリスク分析実施の現状，リスク分析手法の種類及びその特徴，それらの手法のうち「定性的リスク分析手法」の一つである「詳細リスク分析手法（アプローチ）」について，その特徴と問題点を見てきた．

ここで，それらの問題点について纏めると以下【表６】のようにリスク分析の“作業の負荷”及び“分析の効果”の２つの観点にて整理される．

観点	内容
作業の負荷	リスクを具体的に分析するためには詳細リスク分析が望ましいとされるが，その実施のためには，膨大な保護資産の識別作業などの労力や分析のための専門知識（具体的な脅威や脆弱性及び適切な管理策の知識）が必要となり負荷が高い．
分析の効果	多くの作業負荷（時間，労力）をかけて詳細リスク分析を実施しても，現状ではリスクの定量化に限界があるため，結果的に経営者を含む関係者の主観的判断（知識・経験・理論）に頼るしかなく，分析結果に対する納得性に乏しい．

表 6：リスク分析における問題点の整理

これらの問題について，２．１節【表１】で述べたGMITSの各リスク分析手法について実施負荷と実施結果の精度の関係を整理すると【図２】のようにまとめられる．

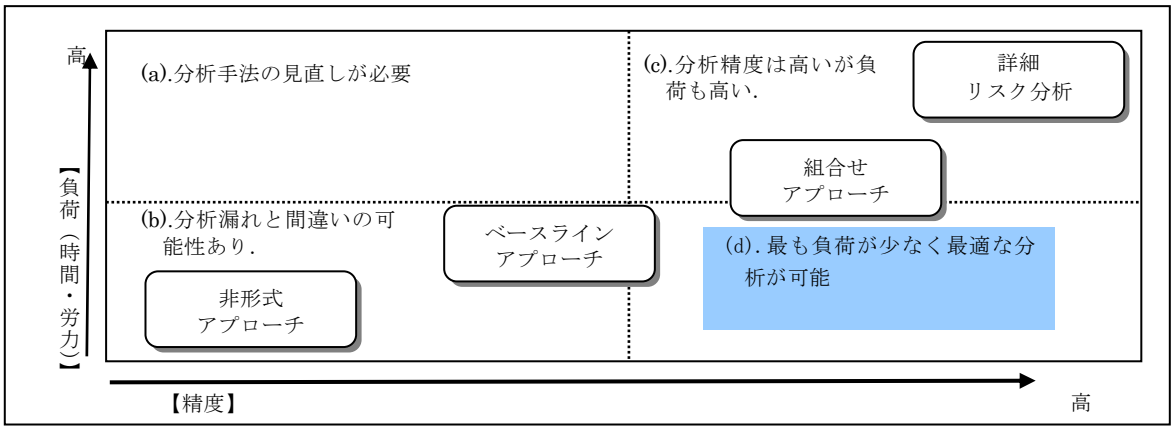


図 2：リスク分析手法の負荷と精度

この図から（a）のエリアは，最も非効率な分析手法であり，分析手法自体の見直しが

必要であると考える．（b）のエリアは，一定の知識を持った担当者の経験や判断，あるいは，一定レベルのセキュリティ対策一覧などを基準（ベースライン）とし，現状を分析する方法であり，分析負荷が少ないが，分析漏れや過不足な対策実施になりやすい．また，（c）のエリアは，基本的に重要な情報資産を識別した上で，情報資産に対するリスクを分析していく手法であり，ある程度，精度の高いリスク分析が実施できるが，情報資産個々のリスクを分析評価するため，比例して作業負荷も高い．

そこで，（d）のエリアが最も負荷が少なく適切な分析が可能であるが，【図２】からも明らかなように現状では適切な手法が存在していないことが判る．そこで，次章より，図の（d）のエリアの条件を満たすことのできる新たなリスク分析手法について，考察を進める．

４．新リスク分析手法の考察

４．１　問題解決の方向性

３．５節で見てきたように，現状ではリスク分析の問題点を解決する負荷が少なく効果的なリスク分析手法は存在していない．しかしながら，既存の各分析手法は，一長一短ではあるが，それぞれに長所（強み）を持っている．

そこで，まず，4 つのリスク分析手法のうち，「組み合わせアプローチ」を除く，３つのリスク分析アプローチの各長所について，リスク分析手法の問題点に対する効果の観点で整理してみると，以下【表７】に整理できることが解かる．

問題点	リスク分析アプローチ	各アプローチの長所（強み）
作業負荷の問題（時間・労力）	非形式アプローチ (Informal Approach)	情報セキュリティに関する専門家のスキルを活用して，リスク分析における専門知識不足を補い短時間の分析を可能とする
	ベースラインアプローチ (Baseline Approach)	あらかじめ精査された情報セキュリティ管理策（ベースライン）を用意し，これを参照することで短時間に一定レベルの精度を確保した分析を可能とする．
分析結果の問題（納得性）	詳細分析アプローチ (Detail Approach)	リスクの評価に必要な要素（業務システム環境・脅威・脆弱性）を体系的に識別することで，納得性のある分析を可能とする．

表 7：リスク分析の問題点と適用分析アプローチ

そこで，上記【表７】の結果から，3 つのアプローチの長所（強み）をバランスよく融合することで，リスク分析の問題点を解決する新たなリスク分析手法について考察してみる．

４．２　新リスク分析手法の要件

４．１節での問題解決の方向性を踏まえ，３．５節で述べた「リスク分析手法における二つの問題点」，すなわち，「問題点１：作業の負荷が高い」，「問題点２：分析の効果が見えない」について，これらの問題点を解決するために以下の三つの要件を設定する．

《問題点１》：作業の負荷（分析のための労力や専門知識が必要）

①要件１（分析負荷の極小化）

分析負荷のかかる，資産（資産内容と資産価値）と業務システム環境を詳細に洗い出さなくても，リスク環境（業務システム環境・脅威・脆弱性）について，あらかじめ体系化された分析モデルに従うことで，リスク分析を実施できるようにする．

②要件２（専門知識の排除）

リスク分析に必要な専門知識（脅威と脆弱性及び管理策の内容）や，リスク分析手法を知らなくても，専門家によって精査され確立された分析モデル（ベースライン）を使用することで，適切なリスク分析の実施を可能とする．

《問題点２》：分析の効果（作業負荷に見合った分析結果が得られない）

③要件３（分析結果の納得性向上）

定性評価を前提にし，リスクの判断に必要な情報（脅威や脆弱性など）を具体的かつ充分に提示することで，リスク値の計算を行わなくても，関係者が納得性を持てる管理策の抽出を可能とする．

４．３　要件に対する仮説とその検証

これらの要件に対して，それぞれ次のような仮説を立てるとともに，自身が経験してきた実環境における詳細リスク分析結果について分析することで，それらの仮説を検証してみる．なお，仮説の検証に使用するリスク分析結果は，筆者が関わった ISMS 構築時（2003 年 2 月，認証取得）に，実際に実施したリスク分析のデータを使用する．

４．３．１　仮説の設定

①要件１に対する仮説

リスクの識別は，資産個々ではなく資産の存在場所と処理環境の単位で集約して実施することで，分析作業の負荷を大幅に軽減できる．（これによる脅威や脆弱性の抽出漏れは発生しない．）

②要件２に対する仮説

情報セキュリティ管理策の国際標準である「ISMS 詳細管理策」をベースラインとして使用することで，専門知識がなくても一般的に想定されうるリスクに対して必要十分な管理策を実装できる．

③要件３に対する仮説

管理策の決定は，主観により算出されたリスク値により機械的に判断されず，“リスクの内容（脅威と脆弱性の詳細)”，“対策に必要なコスト”，“利便性の低下内容（業務の効率化・迅速化の低下)”，“管理策実施後の残留リスク内容”で総合的に判断される．

４．３．２　仮説の検証

①要件１に対する仮説の検証

942 種類の保護資産を識別し，保護資産個々に対して脅威・脆弱性を抽出した．この内容を一覧にして分析してみると，資産（資産内容と資産価値）が異なっていても資産の存在場所と処理環境が同一であれば，脅威・脆弱性もほぼ同一となっていることが判った．例えば，個人情報を含む業務マスタと内部の業務管理情報マスタの資産内容と資産価値は異なるが，どちらのマスタも電算センタ内の本番サーバに

格納されており，入出力などの処理環境は同一であるため，脅威と脆弱性の内容も同一となった．すなわち，リスクの原因となる脅威及び脆弱性は，資産（資産内容と資産価値）によって変わるわけではない．（よって資産個々の評価は不要.）
そこで，この資産の存在場所と処理環境を Key にして資産を集約したところ，195 分類に集約されパターン化された．つまり，資産及び脅威と脆弱性の分析作業量は資産個々で実施した場合の約 79%減(195 / 942)となった．

②要件２に対する仮説の検証

詳細リスク分析結果に基づき，選択された管理策は 53 種類（管理策の内訳は，セキュリティ管理ツールの導入など技術的または物理的管理策が７種類で，残りはルール及び規約の強化や監視などの運用管理策）であったが，それらはすべて「ISMS 詳細管理策」で網羅されていた．また，既存の管理策についても，ほぼ「ISMS 詳細管理策」で網羅されていた．すなわち，想定したリスクに対して，国際標準が提供している管理策は充分に対抗出来ていると判断できる．

③要件３に対する仮説の検証

詳細リスク分析結果から算出されたリスク値に基づきリスク受容可否を判定するが，リスク値が受容レベルを満たしていても管理策を適用した（リスクの内容から判断して経営者からの指示により管理策を適用した），あるいは受容レベルを満たしていなくても管理策を適用しなかった（利便性低下による業務影響度合いを考慮し，現状の管理策でもリスクに対応可能と判断したケースなど）件数は全体で 48 件（全リスクの 24%）あった．これらのケースでのリスク受容可否は，リスク値による算術的な判断（受容リスク値の以内か以外か）ではなく，業務処理環境，脅威と脆弱性の内容，管理策実施後の残留リスクの内容，そしてセキュリティ強化により低下する利便性の度合いと必要コストに基づき，経営者を含む関係者の総意で判断されていた．

以上のことから，筆者が経験してきた実際のリスク分析実施結果に基づく検証により，４．２節で述べた新リスク分析手法に必要な３つの要件について実証できたものと考える．そこで，次章において，これら３つの要件を具体化することによる，新たなリスク分析手法の作成方法について考えてみる．

５．新リスク分析手法作成の考え方

５．１　新リスク分析手法作成の基本方針

４章の仮説検証結果を踏まえて，４．２節で述べた３つの要件を実現した新リスク分析手法を作成するために，まず，以下のような基本方針を設定する．

《新リスク分析手法作成の基本方針》
『情報セキュリティ管理のベストプラクティス（Best Practice）である「ISMS 詳細管理策」をベースラインとした「リスク分析モデル」を構築し，この「リスク分析モデル」を使用することで，専門知識がなくても分析負荷をかけずに一定の納得性を確保したリスク分析が実施できる手法とする.』

ここで，この基本方針における「リスク分析モデル」のベースラインとなる「ISMS

詳細管理策」は，「10の管理分野」と，「36の管理目的」，「133の管理策及び952の詳細管理策」から成り立っており，情報資産の安全性について，どのような管理策を実施すればよいのか，ある程度，網羅的に提示している．

しかし，リスク分析手法の観点からは，それらの管理策がどのような業務システム環境における情報資産に対して，どのような脅威・脆弱性の存在を想定しているのかについては体系的には示していないため，リスクを具体的に把握できない．

そこで，次に，基本方針に掲げたリスク分析の実施を可能とするような，「リスク分析モデル」の構築方法について考えてみる．

５．２　新リスク分析手法におけるリスク分析モデルの構築

まず，「ISMS 詳細管理策」から，リスク分析に必要となる要素（業務システム環境，脅威・脆弱性）について，具体的に洗出す．そして，それらの要素におけるリスクについて対抗する詳細管理策を抽出し，それらを「詳細リスク分析アプローチ」の手法で具体化していくことで，国際標準に準拠したリスク分析モデルを構築していく．

この具体化においては，情報セキュリティの専門家の知識を加えることで，この分析モデルを使用したセキュリティ管理策選定の判断に必要となるリスク分析の要素について，より多くの精錬された情報を提供するようにする．【図３】

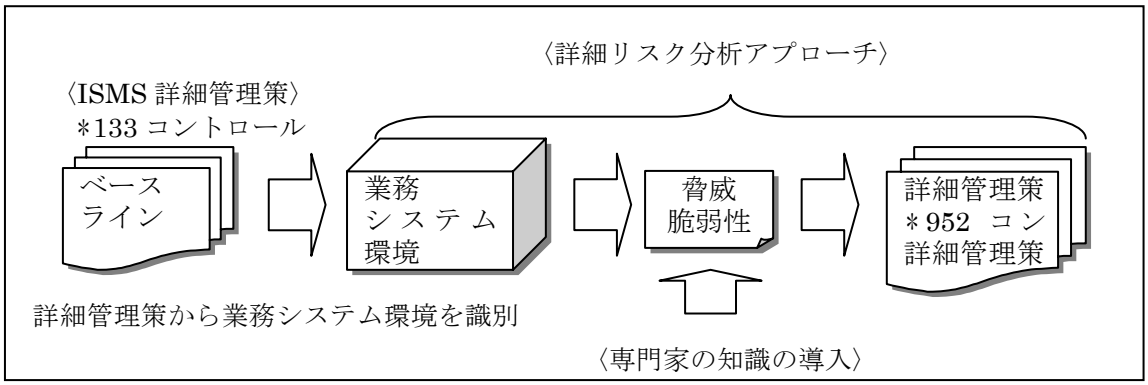


図 3：新リスク分析モデルの構築方法

このようにリスク分析に必要な情報が，体系的かつ詳細に提供されることで，どのような情報システム環境に，どのような脅威や脆弱性（つまりリスク）が内在していて，それらリスクには，どのような管理策が必要とされるのかということについて，リスク評価に関係する人達の理解が深まり，これによりリスク分析の結果についての納得性が高まると考える．[6][10]

６．リスク分析モデルの構築手順

５章で述べた新リスク分析手法作成の考え方に基づき，以下の手順で新リスク分析モ

[6] この点について，Microsoft 社の「セキュリティリスク管理ガイド」の中で，Microsoft 社における情報リスクアセスメントにおける経験値として，リスクに関係する人たちが，リスクに関するより多くの詳細な情報を得ることで，リスク評価結果に対する理解が深まることが体験的に証明されているとしている．

デルを構築していく．

６．１　業務システム環境の抽出（リスク分析範囲の設定）

まず，各「ISMS 詳細管理策」が保護することを想定している，業務システム環境を抽出する．ここで，「ISMS 詳細管理策」は，その管理策実施により，達成すべき「管理目的」があり，また，「管理目的」は業務システムにおける情報資産の安全性を維持するために必要な「管理分野」を想定している．

そこで，この管理の対象となる業務システム環境の概要を抽出することを考える．以下に「ISMS 詳細管理策」からの事例を示す．（「JIS X 5080：2002」より例示）[11]

①管理分野：8.　　通信及び運用管理

②管理目的：8.7　情報及びソフトウェアの交換

③管理策　：8.7.3 電子商取引におけるセキュリティ

８．７．３．「電子商取引におけるセキュリティ管理策（認証，暗号化，否認防止，電子署名，決済保護など)」は，「インターネット通信における電子データ交換）の利用，電子メールの利用，オンライン商取引などの利用及び運用管理業務」を想定していることから，以下のような業務システム環境を抽出する．

④組織内の公開ネットワーク上に Web サーバ，メールサーバを配置し，インターネットを介して Web ブラウザによりアクセスする不特定多数の利用者と売買及び決済情報などの授受を行う業務システム環境

６．２　脅威・脆弱性環境の抽出（リスクの識別）

６．１節で抽出した業務システム環境について，その業務システムの安全性を脅かす脅威を洗い出し，それらの脅威が利用すると想定される脆弱性も洗い出す．脅威の抽出においては，“どの程度の知識・能力を持った利用者”が“どのような手段，方法”を用いて，また“どのような脆弱性を利用して”発生させるのかを具体的に洗い出す．

例えば，外部の不正利用者による脅威であれば，「セキュリティに関する高度な専門知識を保有する攻撃者が，パッチが適用されていない既知の Web サーバ OS または mail サーバ OS のセキュリティホールを利用して，DOS（Denial of Service：サービス不能）攻撃により，サーバを機能停止させることで，サーバの管理者権限を奪い，情報を漏洩または改竄する.」のように，あるいは，内部の不正利用者による脅威であれば，「システムの専門知識を有するシステム運用者が，ネットワーク盗聴機器を不正に設置し，ネットワーク上を流れる暗号化されていない利用者の権限情報を不正にキャプチャ（盗聴）し盗み取ることで，正規の利用者に成りすまして情報漏洩または改竄する.」などのように具体的に抽出する．これによりリスク発生度合いを客観的かつ具体的に識別できるようにしておく．

６．３　セキュリティ管理策の抽出（セキュリティ必要条件の識別）

６．１節，６．２節で識別したリスク環境（業務システム環境及び脅威，脆弱性）に対して，リスクに対応するために必要となる「ISMS 詳細管理策」を抽出する．

あらゆるリスクは，回避または移転しない限りリスクを“零”にすることはできない．そこで，管理策の抽出において，あらかじめ想定したリスクへ備える事前対策としての

「抑止・予防」の管理策に加えて，リスクが発生した場合の事後対策である「検知・回復」の管理策を組み合わせることにより，リスクの影響をできるだけ低く抑えることを考える．これにより，効果的にリスクを低減することが可能となる．【表８】[12]

脅威	セキュリティ管理策			
	抑止	予防	検知	回復
記憶媒体の不正持出による漏洩	建屋の物理管理（記憶媒体の持出管理）	データの秘匿（データ暗号化）	建屋の物理管理（記憶媒体の保管管理）	有効期間管理（漏洩データの無効化）

表 8：セキュリティ脅威とセキュリティ管理策
（出典：田渕治樹「国際セキュリティ標準 ISO/IEC15408 入門」）

一方，セキュリティ管理策は，そのコントロール階層（Layer）によって，人的・組織的管理策，技術的管理策，物理的・環境的管理策に分けても考えることができる．

《リスク管理策の階層（Layer)》

①人的・組織的管理策　：組織における人や組織全般を管理運営する管理策
②技術的管理策　　：ソフトウェアやネットワークなどでの技術的管理策
③物理的・環境的管理策：建物やハードウェア・設備を対象にした管理策

そこで，「ISMS 詳細管理策」について管理策の階層（Layer）で分類分けしたうえで管理策種別（抑止・予防・検知・回復）とのマトリックスで整理してみると，【表９】のように体系化できる．このように，セキュリティ管理策について管理策種別及び管理策 Layer で分類分けし体系化することで，リスクに対して必要となる管理策を洩れなく効果的に識別できるようになる．

	抑止	予防	検知	回復
人的・組織的管理策	■セキュリティ規程 ■セキュリティ委員会 ■外部委託 ■資産の分類 ■職務の分離 ■利用者責任 ■教育・訓練 ■法的適合	■ 脆弱性診断 ■ 定期保守 ■ 操作手順書 ■ 事件事故管理 ■ 情報取扱手順 ■ 利用者登録・管理 ■ 暗号鍵管理 ■ 契約	■監視カメラ ■監査ログ ■システム監査 ■ポリシー準拠の点検 ■アクセス権の見直し	■ 運用記録 ■ 復旧手順 ■ 事業継続管理
技術的管理策	■ アクセス制御 ■ 識別・認証 ■ 記録の保護 ■ ディジタル署名 ■ 否認防止	■ ウィルス管理策 ■ 暗号化 ■ 電子メール管理 ■ 公開情報保護 ■ メッセージ認証 ■ 入力データ検証	■技術的適合検査 ■メッセージ認証 ■入力データ検証 ■出力データの妥当性検証	■ バックアップ ■ 時刻同期
物理的・環境的管理策	■ 物理的セキュリティ境界 ■ ネットワークの分離 ■ 入退室管理 ■ 開発・運用の分離	■ 保守管理 ■ 変更管理 ■ 廃棄管理 ■ 容量・能力計画 ■ システムの受入 ■ 媒体管理	■システム使用状況の監視 ■モバイル PC の管理	■ 多重化 ■ 無停電装置

表 9：ISMS セキュリティ管理策の分類（主な管理策を抽出）

６．４　セキュリティ管理策のレベル設定（セキュリティ十分条件の識別）

ここまでで，実装する情報セキュリティ要求が定義され，情報セキュリティの必要条件（想定されるリスクに対して，「必要なセキュリティ対策」を選択しているか）が明

らかになる．しかし，実装する情報セキュリティ対策は，リスクに対して有効なのか，すなわち，リスクへの情報セキュリティ対策の十分性は識別できていない．そこで，次に情報セキュリティ対策の十分条件（どの程度まで実施するのか）について検討する．

納得できる情報セキュリティ対策の実装のためには，実装する対策が，リスクに対し，どの程度対抗できるのかを明らかにする必要がある．しかしながら，２章で見てきたように，受容リスクレベルについて統計的数値を用いて客観的に評価することは現状では困難であるため，主観的判断に頼らざるを得ない．そこで，以下の事例のようにセキュリティ管理策の実装レベル（十分性）を判断するための具体的な評価指標を予め設定する方法を考える．[7]

「情報セキュリティ管理策の十分性評価指標の設定」

■情報セキュリティ管理策例

・ 悪意のあるソフトウェア（コンピュータウィルスなど）に対する管理策

■情報セキュリティ管理策の十分性評価要素例

《管理策詳細》	《セキュリティレベル評価要素（高 ＞ 中 ＞ 低）》
▶パターンファイル更新頻度	▶Daily ＞ weekly ＞ monthly
▶パッチ対策実施頻度	▶随時 ＞ 年１回 ＞ 不定期
▶ウィルスソフト多重度	▶ゲートウェイ導入 ＞ サーバー導入 ＞ PC のみ
▶ソフトウェア導入管理	▶ソースコードチェック＞ 提供元検証 ＞ 未実施
▶システム情報改竄検知	▶自動検知 ＞ 定期的検証管理 ＞ 未実施
▶利用者ウィルス対策習熟度	▶専門化を設置 ＞ 全員が熟練 ＞ 一部不徹底

上記のように情報セキュリティ管理策の十分性（どのレベルまで実施するのか）を客観的に評価する要素を抽出し，各評価要素に重み付けすることで，情報セキュリティ管理策の十分性を定性的に評価するものとする．【表 10】【表 11】

レベル	定義情報更新頻度	パッチ対策実施頻度	ウィルスソフト多重度	改竄検知実施管理	利用者習熟度
最小	monthly	不定期	PC のみ	未実施	一部不理解
基本	weekly	年１回	サーバ導入	年１回	全員が習熟
最高	anytime	随時	ゲートウェイ導入	自動検知	専門化設置

表 10：セキュリティ管理策の十分性の評価指標事例

レベル	レベル内容
最小	既知のウィルスにも感染するレベル
基本	既知のウィルス感染を防御するレベル
最高	新種（亜種）のウィルス感染を防御するレベル

表 11：セキュリティ管理策の十分性の評価レベル事例

同様の方法で，ほかのセキュリティ管理策についても評価指標を設定し，定性的評価を実施していくことで，情報セキュリティ管理策のレベルを設定していく．

[7] この点に関しては，同様の研究が ECOM（電子商取引推進協議会）において進められており，情報セキュリティにおける対策要求に対する具体策の選択基準と対策の十分性を評価するための方法論として「セキュリティ対策評価技法」が策定されている．[13]

６．５　利便性への影響設定

ISMS 詳細管理策を実施した場合の利便性の影響を識別する．利便性の影響については，「業務に影響あり」，「許容範囲」，「全く影響がない」などのレベルを区別しておく．また，具体的な低減内容についても，セキュリティ強化により業務の効率性・迅速性が低下する内容についてできるだけ具体的に設定する．

例えば，“情報の持出制限により，情報の持ち出しに管理者承認が必要となり時間がかかる”や，“暗号化により端末操作レスポンスが低下する”など低減度合いが判るように具体的に設定する．利便性への影響内容を具体的に設定することで，業務における利便性への影響を意識した実現性のある管理策レベルを決定できるようになる．

６．６　リスク分析データの関連付け

６．１節～６．５節で抽出・設定した以下のデータについて，詳細リスク分析手順に沿って体系的に関連付ける．その関連付けにおいては，管理策の強度と利便性の低減度に関するバランスを十分に考慮する．

①リスク発生環境

「業務システム環境（資産設置場所，業務処理環境）」

「脅威内容（主体，種別，内容）」，「脆弱性内容」

②セキュリティ管理策セット

「管理策種別（“抑止・予防”or“検知・回復”）」，「ISMS 詳細管理策」

「管理策実装レベル（最高，基本，最小）」，「利便性の影響内容」

通常，セキュリティ対策の強度と利便性は相反する関係であり，利便性を大きく損なわない一定レベルまではセキュリティを強化するとリスク（この場合，損失）の低減により資産価値は高まると考えられるが，強化のレベルが限度を超えると逆に利便性の著しい低下により資産価値が低下していくものと考える．【図４】

よって，極端にセキュリティ強度を高くしたため業務の実施がままならない，あるいは，極端にセキュリティ強度を弱めたために，リスクが高いような管理策の組合せは，分析モデル構築において始めから除外するものとする．

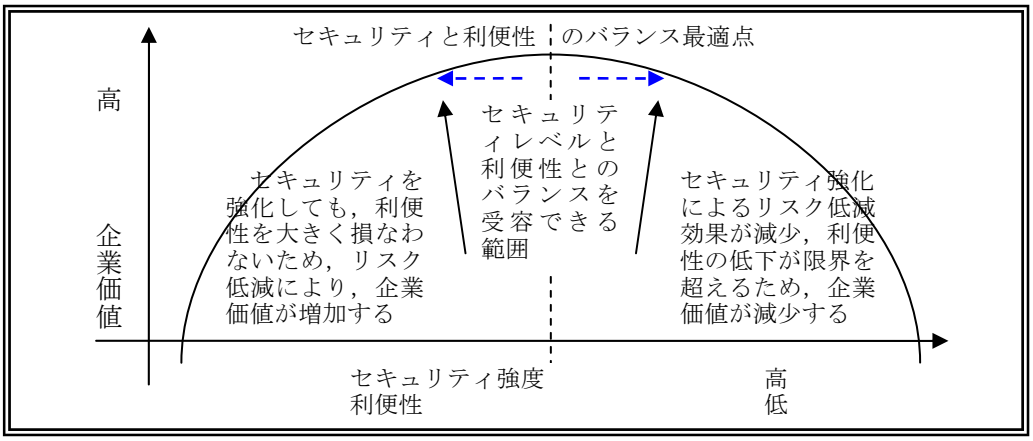


図 4：セキュリティと利便性のバランスの概念

以上のような手順で，予め ISMS 詳細管理策から想定されるリスク分析データセットを作成する．【図５】このとき，リスク分析データセットの作成には専門家の意見を加えることで，リスク発生の可能性（脅威及び脆弱性の内容から評価）を考慮して，必要となるセキュリティ管理策セット（セキュリティレベルと利便性のバランスを考慮した組み合わせ）を設定しておく．これにより，このモデルを使用したリスク分析実施において，分析結果の納得性を確保しやすくなる．

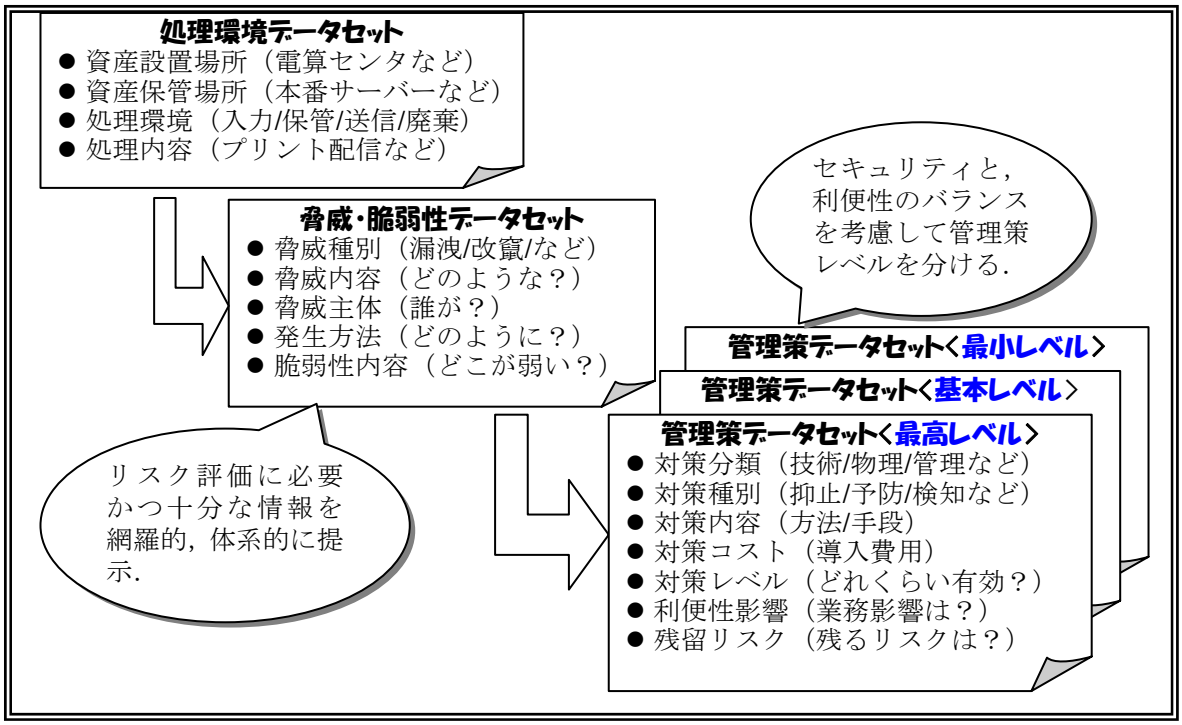


図 5：リスク分析データセットの概念

７．新リスク分析手法によるリスク分析

６章で構築したリスク分析モデルを使用した，新リスク分析手法の実施手順について以下に述べる．リスク分析を実施する組織は，「新リスク分析実施フロー」【図６】のように，このリスク分析モデル(データセット)を使用し，この分析モデルが提示する条件にしたがって必要なセキュリティ管理要件及びその実装レベルを選択する方法で行う．

以下に，電子商取引システムを想定した業務システムにおいて，本リスク分析モデルを使用したリスク分析手順の事例を説明する．なお，選定するセキュリティ管理策はコンピュータウィルス対策を事例として説明する．

７．１　セキュリティレベル（目標）の設定

リスク分析を実施する組織は，まずリスク分析を実施する業務システムにおけるセキュリティ目標を組織決定する．セキュリティ目標については，情報セキュリティの三要素（機密性・可用性・完全性）について，どの要素を，どのレベル（抑止・予防・検知・回復）の目標とするのかの観点で決定する．

この点については，2005 年 3 月に発表された「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」[14]の中で，ベンチマークに基づいた要求されるセキュリティ水準の考え方が提示されており参考にすることができる．以下にセキュリティ目標の設定例について述べる．

《セキュリティ目標の設定例》

『当該リスク分析対象システムは，インターネットを介して不特定多数の利用者との間で 24 時間 365 日での信用取引を行う情報システムである．扱う情報は，顧客の信用情報であり，個人情報保護法などコンプライアンスの観点からも最高レベルの機密性と完全性の確保が要求される．また，このシステムは事業の規模（利用顧客数，取引高）及び情報システムへの依存性（24 時間 365 日サービス稼動）から，その社会的責任性が高く，可用性レベルもまた最高レベルが必要とされる．よって情報セキュリティにおける機密性・完全性・可用性の全レベルにおいて，“High（最高）レベル”を，そのセキュリティ目標とする.』【表 12】

レベル	要素	目標	目標レベル
最小 レベル (minimum)	機密性 完全性	防止	■一般利用者(*1)の不正を防御可能 (*1：システムの特別な知識を持っていない主体) ■偶発的なセキュリティ侵害（漏洩・改竄）を防御する
		検知	■不正検知に 1 ヶ月程度を要する
	可用性	回復	■24 時間以内での業務復旧可能
基本 レベル (basis)	機密性 完全性	防止	■熟練者(*2)による不正アクセスを防御可能 (*2：製品レベルでの専門的なシステム知識を有する主体) ■意図的なセキュリティ侵害（漏洩・改竄）を防御する
		検知	■不正検知に 1 週間程度を要する
	可用性	回復	■１時間以内での業務復旧可能
最高 レベル (high)	機密性 完全性	防止	■エキスパート(*3)による不正アクセスを防御可能 (*3：セキュリティに関する高度な専門知識を有する主体) ■計画的・組織的セキュリティ侵害（漏洩・改竄）を防御する
		検知	■不正検知をリアルタイムに実施可能
	可用性	回復	■基本的にノンストップ運用可能

表 12：セキュリティ目標レベルの考え方

７．２　リスク分析環境の識別

リスク分析を実施する業務システム構成（情報資産の環境）の概要を把握し，その範囲における最重要資産を識別する．次に，その資産の「設置場所・保管場所・処理環境」について分析モデルから該当データを選択する．【表 13】

Key	設置場所	保管場所	情報資産	処理	処理内容
E - 1	電算センター	Mail サーバ Web サーバ	会員情報	更新 保管	会員からの E メール情報をダウンロードし保管
					会員からの Web リクエストをアプリケーションで受付処理

表 13：情報資産処理環境データセットの事例

７．３　リスクの識別

最重要資産の業務処理環境に存在する「脅威（脅威種別・脅威主体・発生方法・発生内容)」と現状の「脆弱性（弱点内容)」のデータセットを分析モデルから選択し，その

資産に影響を及ぼすリスク（脅威と脆弱性）をすべて選択する．例では，「Web サーバが，サーバソフトのセキュリティホールを利用して不正プログラムに侵入され情報漏洩，改竄される」脅威に対して，「サーバソフトに最新パッチを適用していない」，「サーバへのウィルス対策ソフトが未導入」，「情報の改竄検知の仕組みがない」脆弱性（網掛けの脆弱性）を識別している．【表 14】

Key		脅威				脆弱性
		種別	内容	主体	方法	内容
E - 1	R - 1	侵入 改竄	Web サーバが，不正プログラムに侵入され，情報改竄，情報漏洩	不正なプログラム	サーバソフトのセキュリティホールを利用，不正なリクエスト送信により侵入	定義情報更新遅延 最新パッチ未適用 ウィルスソフト多重度 改竄検知未実施 利用者の無知

表 14：脅威・脆弱性データセットの事例

7．4　セキュリティ管理策の選択

選択したリスクに対して，予め組織決定したセキュリティ目標を満たす管理策データセット（管理策詳細とその管理策実装レベル）を選択する．

セキュリティ管理策の選択，導入においては，どれほどのセキュリティ管理策を導入しても，リスクが“零”になるわけではなく，セキュリティ管理策によりリスクを低減するといっても，どの程度までリスクを低減させるべきであるのかということが問題になってくる．例では，あらかじめ組織決定したセキュリティ目標レベル“High”を満たす管理策データセットを選択したうえで，選択したデータセット（High レベル）より，前記【表 14】において「脅威・脆弱性データセット」から識別した「内在する脆弱性」を改善する管理策として，以下の詳細管理策を選択している．【表 15】

①「パッチ管理」，「Antivirus（ウィルス対策ソフト）の導入」，「改竄検出」

そして，それらの管理策の実装レベルとして，「利便性への影響内容」，「実装コスト」を考慮したうえで，次のような管理策実装レベルを選択することで，セキュリティ目標レベル“High”の条件を達成するようにする．

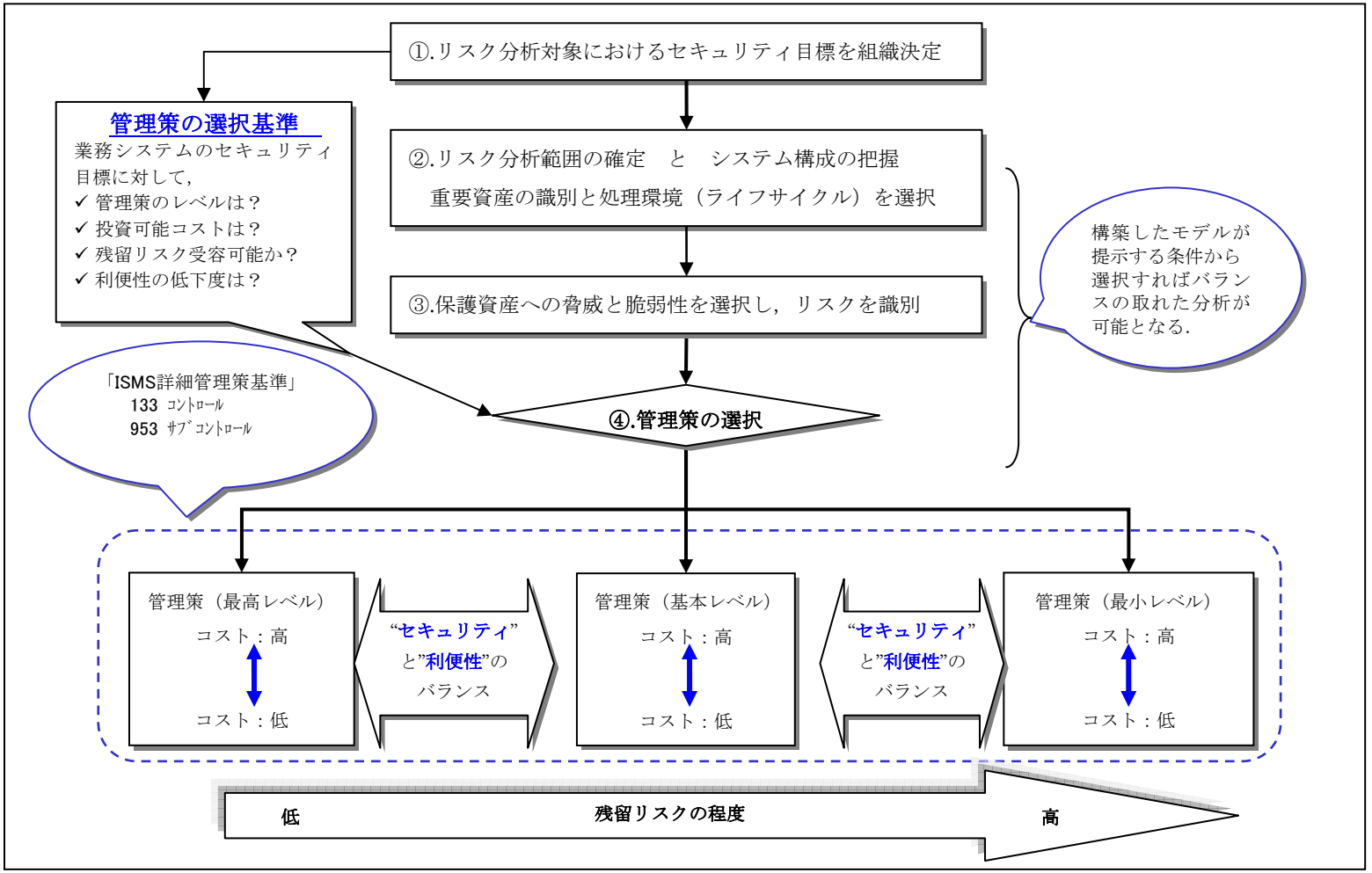
②「最新パッチの常時更新実施」，「ゲートウェイへの Antivirus 導入」，
「改竄自動検知システムの導入」

Key		種別	管理策	管理策詳細	レベル	管理策実装レベル
E - 1	R - 1	抑止 予防	悪意のあるソフトウェアに対する管理策	定義情報の更新管理	High：未知のウィルスに対抗するレベル	常に最新状態を維持
				パッチ管理		常時最新パッチ適用更新
				Antivirus の導入		ネットワーク境界での導入
		検知 回復		改竄検出		自動改竄検知
				利便性影響度レベル内容	コスト	残留リスク
				利用者訓練		定期的・教育訓練実施
				・フィルタリング(URL，mail など)強化による情報収集制約の増加 ・定義情報更新の負荷増大 ・パッチ適用による管理負荷増大	市場価格にて算定	最新定義情報の配布の前に攻撃される

相当な業務の負荷を伴う

表 15：セキュリティ管理策データセットの事例（レベル High の選択例）

図 6：新リスク分析実施フロー



８．まとめ

８．１　新リスク分析手法の特徴

以上，ここまで，情報セキュリティを取り巻く状況の整理と，情報セキュリティへの取り組みにおいて必須のプロセスであるリスク分析手法の種類と特長及び，その抱える問題点について整理をしてきた．そのうえで，筆者が経験してきたISMS構築及び運用における試行錯誤の実践活動の中から得た経験値を踏まえ，それらの問題点を解決する新たなリスク分析手法として，「ISMS詳細管理策」をベースラインとしたリスク分析モデルを使用した分析手法について述べてきた．

本稿で提案した新リスク分析手法は，現状では定量化が難しい情報セキュリティにおけるリスク分析作業において，リスクを定量化することに拘らず，GMITS の４つの戦略的リスク分析手法の特徴及び長所をバランスよく取り入れることで，現状のリスク分析手法の問題を解決する新たな分析手法の構築をねらったものである．

これまで述べてきたように，このリスク分析モデルを使用したリスク分析手法においては，詳細な保護資産の洗出し，及び個々の資産価値の評価や，一からの脅威や脆弱性の抽出，及びそれらの指標からのリスク値の算出作業は発生しない．リスク分析作業は，このリスク分析モデルが提示する分析パターンに沿って，組織のセキュリティ目標に適合する管理策を，リスク分析作業に関わる関係者の合意に基づき選択していくだけである．

これにより，負荷のかかる情報資産と処理環境の識別を詳細に実施する工程を簡略化することができ，脅威や脆弱性に関する専門知識がなくても洩れなくリスクを識別し，組織のセキュリティ目標に適合する納得性のある管理策を選択できるものと考える．

この分析手法の特徴は，以下の諸点となる．

①リスク分析に必要となる情報（情報処理環境，脅威，脆弱性）を専門家の知識により体系的にデータベース化するので，過度の時間と労力や専門知識を必要とせずに実施できる

②モデルに実装する管理策は，あらかじめ，セキュリティと利便性のバランスを考慮し，過度または過少にならないように組み合わせるので，納得できる管理策の選択ができる．

③情報セキュリティ管理策の国際標準から想定したリスク分析モデルであり，管理策の見落としや偏りが少なく，分析対象の規模に関わらず比較的バランスのとれた対策が選定できる．

８．２　新リスク分析手法と今後の課題

2005年7月25日のOECD理事会の勧告として採択された「情報システム及びネットワークのセキュリティのためのガイドライン～セキュリティ文化の普及に向けて～」[15]において，ネットワークのすべての「参加者」が講じるべき措置（9 つの原則）のなかで，『責任（Responsibility)』と『リスクアセスメント（Risk assessment)』が掲げられている．

これは，『すべての「参加者」が，情報システム及びネットワークのセキュリティに対する自らの責任を理解すること.』，そして，『自らの責任においてリスクアセスメン

トを行うこと』を求めている．また，『リスクアセスメントは，脅威と脆弱性を識別するものであり，保護すべき情報の性質と重要性に照らして，リスクの許容できるレベルの決定を可能にし，情報システム及びネットワークに対する潜在的な損害のリスクを管理するために，適切な制御を選択することを支援する.』としている．

このように，現在の IT 社会において，情報セキュリティを適切に実装していくためには，リスクアセスメント（リスク分析）は，避けては通れない重要なプロセスであることが認識されている．しかしながら，本稿で見てきたように，リスク分析の実施は，負荷が高く，リスクの定量化が困難なために分析結果に対する納得性にも問題を抱えており，ゆえに，情報セキュリティ対策の実装において，どこまでやれば安全なのか（安全と保証されるのか）が判断できずにいる．また，（社）日本経団連「企業の情報セキュリティのあり方に関する提言（2005 年 3 月 15 日）」[16]においても，企業の情報セキュリティ対策を更に進めるうえで，「あるリスクに対しては，このレベルの対策が必要という合理的なセキュリティ水準の目安について，官民が協力し，何らかの具体的な水準を共有できるようにする必要がある.」と謳っている．

このような現状において，本稿で提案したリスク分析の考え方は，定性的評価を前提にして，リスク分析に必要な諸条件を体系的かつ網羅的に整備した分析モデルを提示することにより，リスク分析に必要な要素を可視化することができ，これによって，リスク分析に関わる組織の関係者が，リスク分析の結果について容易に理解でき納得することができる方法であると考える．このように，リスク分析結果について納得性が得られることによって初めて，自らの情報セキュリティレベルについて自信を持つことができ，有効なリスク管理を実現できるのである．

本稿で述べたリスク分析手法は，現在，当社における正式なリスク分析手順として取り入れ，実際のリスク分析作業への適用を開始しているところである．

今後，リスクの異なる様々な情報システムにおけるリスク分析作業への適用を進め，その結果を評価し，リスク分析データセットを継続的に改善していくことで，有効なリスク分析モデルへと発展できるものと考えている．

以　上

[参考文献]

[1] 日本経済団体連合会「企業行動憲章：社会の信頼と共感を得るために」（2004 年 5 月 18 日）
http://www.keidanren.or.jp/japanese/policy/cgcb/charter.html
[2] 報道資料「ISMS認証取得者数が1，000件を超える」
http://www.isms.jipdec.jp/doc/press20050826.pdf
[3] 警視庁：不正アクセス対策に関するアンケート報告書（平成 12 年度）
http://www.npa.go.jp/cyber/research/h12/fusei_ac4/4_c04.html
[4] 警視庁：不正アクセス行為対策などの実態調査（平成 15 年度）
http://www.npa.go.jp/cyber/research/h15/image/H16countermeasures.pdf
[5] リスクマネジメントー用語ー規格において使用するための指針 TR Q 0008：2003（ISO/IEC GUIDE73：2002）
[6] ITセキュリティマネジメントのガイドラインのガイドラインー第3部：ITセキュリティマネジメントの手法　TR X0036-3（ISO/IEC TR 13335-3）
[7] Microsoft セキュリティリスク管理ガイド第 2 章：セキュリティリスク管理方法概観
http://www.microsoft.com/japan/technet/security/guidance/secrisk/srsgch02.mspx
[8] JIPDEC「ISMS ユーザーズガイドーリスクマネジメント編ー」（2004 年 7 月）
http://www.isms.jipdec.jp/doc/JIP-ISMS113-10.pdf
[9] JIPDEC「ISMS構築事例集～情報セキュリティへの取り組み事例～」（2005年10月28日）
http://www.isms.jipdec.jp/doc/const/001top.PDF
[10] Microsoft セキュリティリスク管理ガイド第 4 章：リスクの評価
http://www.microsoft.com/japan/technet/security/guidance/secrisk/srsgch04.mspx
[11] 日本規格協会「JIS X 5080：2002）情報セキュリティマネジメントガイド（2003 年 7 月）
[12] 田渕治樹「国際セキュリティ標準 ISO/IEC15408 入門」オーム社（2001 年 5 月 20 日）
[13] ECOM「セキュリティ対策評価モデル」（2005 年 2 月）
http://www.ecom.or.jp/en/results/results2004/2004_10.pdf
[14] 経済産業省「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」
[15] OECD 情報セキュリティ及びネットワークのセキュリティのためのガイドライン
http://www.meti.go.jp/policy/netsecurity/OECD020917set.htm
[16] 日本経団連「企業の情報セキュリティのあり方に関する提言」
http://www.keidanren.or.jp/japanese/policy//2005/015/honbun.html