社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2008－CSEC－43 (8)
2008／12／5

情報セキュリティ意識向上に向けた効果的なリスクアセスメント手法の提案

土井 智朗† 内田 勝也†

†情報セキュリティ大学院大学 情報セキュリティ研究科

あらまし 企業において、情報セキュリティの重要性は益々高まっている。業務の IT 化が進み、情報の活用抜きでは業務が立ち行かない現在においては、情報を取り扱う全ての従業員が情報セキュリティの重要性を認識し、それぞれの業務、立場においてその役割を正しく理解し実践することが求められており、情報セキュリティ意識の向上は重要な課題である。情報セキュリティ意識の向上には、従業員が自らの職務におけるリスクを評価する、すなわちリスクアセスメントの実施が不可欠である。しかし、現状のリスクアセスメントでは必ずしも情報セキュリティ意識の向上が図れていない。そこで、本論では、まず情報セキュリティ意識向上におけるリスクアセスメントの重要性を示したうえで、現状のリスクアセスメントの問題点を指摘する。さらに、その問題点の解決方法を検討し、情報セキュリティ意識向上に向けた効果的なリスクアセスメント手法を提案する。

キーワード 情報セキュリティ意識、リスクアセスメント

A Proposal of Effective Risk-Assessment for Improvement of Information Security Awareness

Tomoaki DOI† Katsuya UCHIDA†

† Graduate School of Information Security INSTITUTE of INFORMATION SECURITY

Abstract The importance of the information security is rising more and more in a company. The information technology is built into the business, and the business cannot be done without the use of information. Therefore all employees who handle information are requested to recognize the importance of the information security, and to practice each role in the information security. And the improvement of information security awareness is become an important problem for a company. The Risk-Assessment is indispensable for the improvement of the information security awareness. However the information security awareness has not necessarily improved in a current risk assessment. In this thesis, the importance of the risk assessment for the improvement of the information security awareness is first shown, and next, the problem of a current risk assessment is pointed out. In addition, the method of settlement of the problem is examined, and proposes an effective risk assessment method for the improvement of the information security awareness.

Keyword Information Security Awareness, Risk Assessment

1. はじめに

企業における情報セキュリティは、情報システムを保護することに主眼を置いて、情報システム部門を中心に取り組まれてきた。しかし、個人情報保護法の施行や昨今の内部統制議論の高まりにより、情報セキュリティは経営管理の一要素として、情報システム部門に閉じられたものではなく、情報を取り扱う全部門、全従業員が取り組むべき課題として認識されてきている。

こうした背景の中、ISMS 認証やプラーバシーマークなどのマネジメントシステムを導入するなど、情報セキュリティを全社的に取り組む企業がここ数年で急速に増加している。その一方で、セキュリティポリシーを違反したことによる情報漏洩事故の発生や、マネジメントシステムが組織に浸透しないなど、企業の従業員が情報セキュリティの重要性を正しく認識していない現状を指摘する声も聞こえてきており、情報セキュリティの意識をいかにして従業員に浸透させていくかが企業にとって喫緊の課題となっている。

情報の活用抜きでは業務が立ち行かない現在においては、情報を取り扱う全ての従業員が情報セキュリティの重要性を認識し、それぞれの業務、立場においてその役割を正しく理解し、実践することが求められる。そして、そのためには従業員が情報セキュリティのリスクを正しく認識するためのプロセスとしてのリスクアセスメントが重要なポイントとなってくるだろう。しかし、情報セキュリティマネジメントを導入し、既にリスクアセスメントを実施している企業においても情報セキュリティ意識が十分に浸透していない現状[1]を鑑みると、現状のリスクアセスメントの手法には何かしら問題があることが考えられる。

[1] 2007 年 2 月に情報セキュリティ大学院大学内田研究室で行った調査では、ISMS 認証取得事業者の約 70%（標本数 264 組織）が一般社員の認識・理解の強化を重点的な取組み課題であると回答している[1]。

そこで、本論では、従業員の情報セキュリティ意識の向上を目的に、現状のリスクアセスメントの課題を抽出し、課題に対する改善策を考察するとともに、情報セキュリティ意識向上に向けた効果的なリスクアセスメント手法を提案するものとする。さらに、提案した手法の有効性について検証し、残された課題について整理するものとする。

2. 情報セキュリティ意識向上の要件

2.1. 情報セキュリティ意識向上の目的

情報セキュリティの実践規範である JISQ27002[2]の管理策「8.2.2 情報セキュリティの意識向上、教育及び訓練」では、「各人が情報セキュリティの問題及びインシデントを認識でき、また、各人の役割分担の必要性に従って対応できるようになるために、組織のすべての従業員は、職務に関連する組織の方針及び手順についての適切な意識向上のための教育・訓練を受け、また、定めに従ってそれを更新することが望ましい」としており、さらに、「意識を高めるための教育・訓練は、各人が情報セキュリティの問題及びインシデントを認識でき、また、各人の役割分担の必要性に従って対応できるようになることを意図している」と示されている[2]。

このことから、情報セキュリティ意識向上の目的は「情報セキュリティマネジメントに携わる全ての従業員が、自らの情報セキュリティについての活動がもつ意味と重要性を認識し、各人の役割分担に応じて対応できるようにすること」と定義できるだろう。

2.2. 情報セキュリティマネジメントにおける従業員の役割

情報セキュリティマネジメントは、図1のような階層構造で成り立っており、下位の階層は上位の階層と協調して活動している。

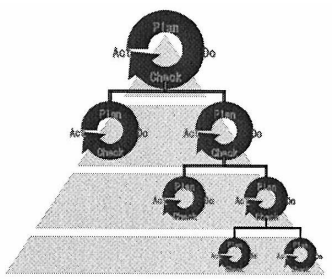

図 1 情報セキュリティマネジメントの階層構造[3]

これらの階層別の役割について、平成15年6月に経済産業省から公表された「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」[3]では、組織の階層構造について経営者、管理者、担当者の3階層に区分し、内部統制の構築・運用における各階層別の役割が示されている。そして、同指針に示されている管理者層、担当者層の役割について考察すると、従業員の役割として以下のように定めることができる。

①組織のセキュリティ目標に照らして、自らの職務におけるセキュリティ上のリスクを特定すること
②特定したリスクに対するリスク対策を検討し実施すること
③実施したリスク対策を評価し、必要な是正策を検討し実施すること

2.3. 情報セキュリティ意識向上の要件

ここまで述べてきたとおり、情報セキュリティ意識向上の目的は、情報セキュリティマネジメントに携わる全ての従業員が、自らの情報セキュリティについての活動がもつ意味と重要性を認識し、各人の役割分担に応じて対応できるようにすることである。そして、その役割が前述の通りであるならば、情報セキュリティ意識向上に必要な要件として、以下の2つが考えられる。

(1)「組織のセキュリティ目標を正しく理解していること」
従業員は、組織のセキュリティ目標に照らして自らの職務におけるセキュリティ上のリスクを特定するために、組織のセキュリティ目標や、セキュリティポリシーについて正しく理解していることが重要である。

(2)「自らの職務における情報セキュリティのリスクについて把握し理解していること」
従業員の役割は、情報セキュリティリスクに対してリスク対策を施し、それを評価、改善していくことである。そのためには、自らの職務における情報セキュリティリスクについて正確に把握している必要がある。

2.4. リスクアセスメントの重要性

では、これらの要件を満たすためには、具体的にどのような施策が必要だろうか。(1)「組織のセキュリティ目標を正しく理解していること」については、教育等を通じて従業員に周知することで達成することは可能だろう。しかし、(2)「自らの職務における情報セキュリティのリスクについて把握し理解していること」を満たすためには、自らの業務におけるリスクを評価する、すなわちリスクアセスメントの実施が重要となってくるだろう。これは、2002年8月にOECD（経済協力開発機構）が発表した「OECD Guidelines for the Security of Information Security System and Networks：Towards a Culture of Security（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）」[5]においても、参加者のセキュリティに対する認識の向上、セキュリティ文化を浸透していくためには、参加者全てがリスクアセスメントを実施することが重要である（リスクアセスメントの原則）とされていることからも明らかである。

では、情報セキュリティ意識向上に向けて、現状のリスクアセスメント手法にはどのような問題が存在するのだろうか。次節では、現状のリスクアセスメントの問題点について考察する。

---

[2] [2]p.26
[3] 出展：[4]5章 p.3

3. 現状のリスクアセスメントの問題点

3.1. 現状のリスクアセスメントのプロセス

ここでは、リスクアセスメントの手法として、JISQ27001[6]の要求事項に沿って、「ISMS ユーザーズガイド リスクマネジメント編」[7]で例示されている手法を示すものとする。

(1) リスクの識別

リスクアセスメントは、まず保護対象となる資産の特定及び資産の管理責任者を特定することから始まる。次に、特定した資産に対する脅威とぜい弱性を特定する。資産の管理責任者は、自らが管理する資産がさらされている脅威を識別したうえで、資産の性質等を踏まえて、識別した脅威に対するぜい弱性を特定することで、セキュリティ障害が資産に及ぼすかもしれない影響（＝リスク）について明確にする。

(2) リスクの分析及び評価

リスクの分析及び評価では、識別したリスクが顕在化した際の事業上の影響（損害）を算定する。具体的には特定した資産の機密性、完全性、可用性が損なわれた時に被る事業上の損害について評価することになる。そして、この評価は、組織のビジネスをよく理解した情報の管理責任者（ビジネスオーナー）が実施するものとされている。

次に、起こり得るセキュリティ障害などの現実的な発生可能性を評価するために、識別した脅威の発生頻度とぜい弱性の程度について評価する。そして、その評価結果を踏まえて、具体的にリスクレベル(リスク値）を算定する。そして、算定したリスクレベル（リスク値）が、組織が定めた受容基準を超えるものであった場合は、リスク対応を行うことになる。

3.2. 現状のリスクアセスメントの問題点

このように、JISQ27001 が示すリスクアセスメントでは、保護すべき資産と管理責任者を特定し、資産毎に脅威とぜい弱性の分析を行い、リスクを特定していくことになる。この手法では、保護対象となる資産を全て洗い出すことによって、組織がさらされているリスクを網羅的に把握できるメリットがある反面、以下のような問題点が指摘できる。

(1) 資産の利用者がリスクを認識できない

この手法では、資産の管理責任者がリスク分析を行うため、資産の管理責任を有さない従業員（資産を利用する者）はリスク分析に参加しないことが想定される。特に、脅威やぜい弱性の識別には専門知識を要するうえに作業が煩雑なため、特定の専門部署やコンサルタント等の外部の専門家を利用して行うケースも多く、一般の従業員にはリスクアセスメント自体が縁の遠いものとなってしまう。その結果、本来リスクを理解しなければならない資産の利用者に、識別されたリスクが自らの責任範囲にあることを認識されないのみならず、資産を利用する際に発生するリスクすら識別すらされないおそれがある。

(2) 業務プロセス上のリスクが把握しづらい

情報は本来伝達され共有されてこそ意味を持つものであり、一つの資産が様々な業務プロセスで使用されることも多いだろう。その場合、同一の資産であっても脅威やぜい弱性は業務プロセス（業務での資産の使用方法や頻度）によって異なることが想定される。しかし、この手法では業務プロセスではなく資産に焦点を当てて脅威やぜい弱性の分析を行うため、資産を使用する個々の業務の実態が反映されにくく、業務プロセスに沿ったリスクを把握することができない。その結果、リスクアセスメントで識別されたリスクが、情報の利用者であるユーザ部門の従業員には理解しづらいものになってしまう。

(3) 専門知識を有さない従業員では実施困難である

一般的に指摘されていることであるが、脅威やぜい弱性の識別には専門知識を要するうえに作業が煩雑なため、専門知識を有さないユーザ部門の従業員が実施するのは困難である。さらに、評価者が認識していないリスクについては特定されないため、評価者のスキルによって評価にバラツキが生じる。

このように、現状のリスクアセスメントの手法では、従業員のセキュリティ意識向上を図る上で問題点があることがわかる。そこで、次節ではこれらの問題を解決する方向性について検討する。

4. 問題点の解決に向けた考え方

4.1. 問題点解決の方向性

まず、「資産の利用者がリスクを認識できない」点については、資産の管理責任者のみならず、情報を利用する部門の従業員もリスクアセスメントを行える仕組みとすることで解決する。この検討には、業務に従事する者が自らリスクを評価する手法である自己統制評価（CSA：Control Self Assessment）を活用する。

次に、「業務プロセス上のリスクが把握しづらい」という問題点については、リスクアセスメントを業務プロセスに沿って行えるようにすることで解決を図る。これは金融庁「財務報告に係る内部統制の評価及び監査に関する実施基準」[8]に示されている、業務プロセスの内部統制の評価手法を活用することで実現する。

最後に、「専門知識を有さない従業員では実施困難である」点については、評価者の経験や知識によらない、容易に実施可能な仕組みとすることで解決する。ここでは、リスクアセスメントを困難にしている要因が、一般の従業員ではどのようなリスクがあるのか識別することが難しいことにあると考え、リスクの専門家と非専門家との間で生じるリスク認知のギャップを埋める手法として研究されているリスクコミュニケーションの考え方を活用する。

4.2. 統制自己評価(CSA)

(1)CSA の特徴[4]

CSA という手法は、従来、組織の独立した内部監査部門が客観的な視点で行ってきた評価プロセスを、業務に従事する者に自ら実施させる仕組みである。

CSA の最大の特徴としては、目的達成のためのリス

[4] [9][10]をもとに、論者が整理を行った。

クや、整備・運用されているコントロールの評定において、実際にその仕事に従事している人員を動員することである。そしてもう一つの特徴としては、CSAは「目的」、「リスク」、「コントロール」という3つの要素に焦点を当てており、業務に従事する者が、コントロールを検証・評価する過程で、その背後にあるリスクについても評価することが挙げられる。

このような特徴から、CSAには、実際に業務を行っている者が評価を行うことで、リスクとコントロールについて理解が深まるという利点がある。また、参加者が自ら評価し結論を出すので、当事者意識が高まり、不備の是正行動（コントロール）が効果的になるといったことも期待できる。さらに、当事者意識の向上に伴い、コントロールプロセスを設計、導入して、コントロールプロセスの運営を継続的に改善するように従業員のモチベーションを高める効果があるとされている。

(2) 統制自己評価手法の事例

このような自己評価として確立されている手法として、米国立標準技術研究所（NIST：National Institute of Standards and Technology）から公表されている「ITシステムのためのセキュリティ自己アセスメントガイド（NIST－SP800-26）」[11]がある。

このガイドは、評価者が情報セキュリティプログラムの現状を理解し、改善が必要な箇所を明らかにするための一つの手法として提唱されたものであり、管理面のコントロール、運用面のコントロール、技術面のコントロールの3つのコントロール分野を網羅した質問項目から構成されている詳細質問表が用意されており、質問には合計17のトピック225のコントロール項目が予め設定されている。評価者は対象となるITシステムについてこれらのコントロール項目について、その成熟度について評価することで、容易に自組織の現状を把握することができ、また、長期に渡って評価を継続することで、改善状況を評価することが可能となっている。

(3) 新リスクアセスメント手法への活用方法

新リスクアセスメント手法への活用方法としては、NISTが提唱するような、質問表を用いたコントロールの評価手法を用いて、業務に従事する者が自ら評価する仕組みとし、また、単にコントロールの実施状況をYES/NOで回答するだけではなく、コントロールの背景にあるリスクも同時に評価できる仕組みとすることで、リスクとコントロールに関する理解を深め、かつ当事者意識を醸成できるものとする。

4.3. プロセスアプローチを用いたリスクアセスメント手法

(1) 業務プロセスに係る内部統制の評価手法[5]

金融庁が公表している「財務報告に係る内部統制の評価及び監査に関する実施基準」では、業務プロセスの内部統制の評価手法として、以下のように示されている。

①取引の「開始」、「承認」、「記録」、「処理」、「報告」の5つのステップ（情報の変換点）を含め、取引の流れを把握し、取引の発生から集計、記帳といった会計処理の過程を把握する。

②各ステップにおけるリスクについて、財務情報を適切に作成するための要件（実在性、網羅性、権利と義務の帰属、評価の妥当性、期間配分の適切性、表示の妥当性）と照らして特定し、そのリスクに対する内部統制を評価していく。

(2) 新リスクアセスメント手法への活用の考え方

業務プロセスにおいてリスクの潜在するステップを識別し、そこで発生するリスクに対する統制の要件を明確にしたうえでリスクを評価する考え方は、業務プロセスに沿ってリスクを評価する際に有用な考え方である。そこで、情報セキュリティの観点でその活用方法を検討する。

まず、情報セキュリティ上の情報の変換点として考えられるステップは、情報のライフサイクル、すなわち「収集・取得」、「処理・利用」、「移動・移送」、「保管」、「廃棄」の各ステップだろう。そして、情報セキュリティの要件としては、「機密性」、「完全性」、「可用性」と定められるだろう。

このように“情報セキュリティにおける情報の変換点”における、“情報セキュリティの要件”を脅かすリスクについて、図のようなマトリクス表を用いてリスク評価を行うことで、業務プロセスにおけるリスクを網羅的かつ適切に把握することが可能となる。このような仕組みとすることで、業務プロセスにおけるリスクを評価することができ、「業務プロセス上のリスクが把握しづらい」問題点を解決することができるだろう。

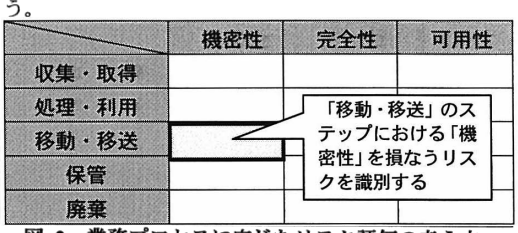

図 2　業務プロセスに応じたリスク評価の考え方

4.4. リスクコミュニケーション

(1) リスクコミュニケーションの効果[6]

米国の研究審議会（NRC：National Research council）の定義では、リスクコミュニケーションとは「個人、集団、組織間でのリスクに関する情報および意見の相互交換プロセスである」とされている。そして、リスクコミュニケーションの目的は、リスクの専門家と利害関係者との間で、リスクに関する情報を相互に交換、共有することで、リスクに関する理解の向上や相互の信頼のレベルを向上するとともに、リスク対応について最適な意思決定を図ることにある。つまり、利害関係者を含めたリスクに関係する人々が、リスクやリスク対応について十分に理解したうえでリスク対応を行うことで、リスク対応への納得性や実現可能性を高めることを目指すものである。

このようにリスクコミュニケーションを通じて多く

[5] [8]をもとに、論者が整理を行った。

[6] [12][13][14]をもとに、論者が整理を行った。

の関係者を関与させることの利点として、以下のような効果があるとされている。

① 民主的な意思決定を支援する
② 公益が確実に考慮される
③ より良い意思決定のために必要な理解を深める
④ 意思決定の基礎となる知見の改善に繋がる
⑤ 意思決定にかかる時間と費用を節約できる
⑥ リスク管理担当機関に対する信頼性を改善するかも知れない
⑦ より受け入れやすく、より容易に実行可能なリスク管理の意思決定を生み出す

これらの効果のうち、本論で注目するのは、③と④に挙げられる理解の促進効果である。通常、リスクの非専門家である利害関係者は、リスクについての正しい知識が不足しており、リスクを正しく評価することは困難である。そこで、リスクの専門家である送り手がリスク評価を行い、非専門家である受け手に対してそれらの情報を提供することで、非専門家である利害関係者のリスクに対する理解を深める（リスクを気づかせる）ことができ、リスクに対する知見を改善する効果が期待できるだろう。

⑵ 新リスクアセスメント手法への活用の考え方

新リスクアセスメント手法では、リスクの専門家（ISMS事務局等）が、予め想定されるリスクを特定し、リスク評価者に提示する仕組みとする。こうすることで、評価者は自らの業務でに、どのようなリスクがあるか特定することが容易に可能となり、リスク評価者の知識や経験等に左右されずにリスク識別を行うことができるようになる。また、この手法では評価者が認識していなかったリスクも自動的に識別されるため、リスクに関する教育的効果も期待でき、情報セキュリティ意識向上に向けた効果的なリスクアセスメント手法として活用できるだろう。

5. 新リスクアセスメント手法の提案

5.1. 特徴とねらい

現状のリスクアセスメントの手法では、資産の管理責任者がリスク分析を行い、資産の管理責任を有さない従業員（資産を利用する者）はリスク分析を行わないため、資産の利用者が資産を利用する際に発生するリスクを識別できないことが問題となっていた。そこで、本論で提案する新手法では、まず資産の利用者がリスクアセスメントを行う手法とした。また、新手法では、リスク評価を情報資産単位ではなく業務プロセス単位で行う。これは、現状のリスクアセスメントの手法では、資産を使用する個々の業務の実態が反映されにくく、業務プロセスに沿ったリスクを把握することができないという問題があるためである。そして、評価の対象を業務プロセス単位としたもう一つの理由は、評価対象の業務を実際に行っている者にリスク評価を行わせることで、評価者が自らの業務におけるリスクを認識できるようにすることである。

このように、評価者が自らの業務プロセスにおけるリスクを認識することで、情報セキュリティに対する意識を向上させることが、本手法の最大のねらいである。

5.2. 具体的な評価手法

本論で提案するリスクアセスメントでは、表1に示すような「リスク評価シート」を予めリスク管理部門が作成する。「局面」欄については、情報セキュリティ上のリスクが発生すると考えられるステップである、収集・取得、処理・利用、移動・移送、保管、廃棄の各局面が記載してあり、それらの局面における想定リスクを、リスク管理部門が予め識別して「想定されるリスク」欄に記載し、さらに「管理策案」欄に想定されるリスクに対する管理策案を記載しておく。

評価者は、評価対象となる業務プロセスを特定し、「リスク評価シート」の「想定されるリスク」に記載してあるリスクが当該業務プロセスの各局面において該当するかどうかを判断し、もし該当する場合はリスクとして特定する。また、「想定されるリスク」以外に、評価者が認識しているリスクがある場合はリスクを追加する。続いて、特定したリスクに対する管理策として、現状で実施している管理策を「管理策案」から選択する。その際、実施している管理策が複数ある場合は全て選択するものとする。また、リスクの特定時と同様に、部門独自で行っている管理策があればその内容を追加して記載する。最後に、想定されるリスクに対する現状の管理策を踏まえてリスクを評価し、残存リスクおよび必要な追加の管理策を策定する。

表 1　リスク評価シート

局面	No.	項目名	想定されるリスク	管理策案	リスク評価			残存リスク
					影響度	発生可能性	リスク値	追加の管理策
収集・取得	1	授受管理	自部署で情報を受入した際に、適切な授受管理を怠り、紛失等の認識が遅れる可能性がある。（対応策の遅れ、二次被害発生の可能性）	・情報を受領した場合、直ちに授受管理台帳に記載する。 ・情報の保管場所を特定する。 ・個人の机中には保管しない。				
	⋮	⋮	⋮	⋮				
処理・利用	⋮	⋮	⋮	⋮				
	⋮	⋮	⋮	⋮				
移動・移送	⋮	⋮	⋮	⋮				
	⋮	⋮	⋮	⋮				
保管	⋮	⋮	⋮	⋮				
	⋮	⋮	⋮	⋮				
廃棄	⋮	⋮	⋮	⋮				
	⋮	⋮	⋮	⋮				

6. 有効性の考察

本論で提案した新リスクアセスメント手法について、実際に企業において実施し、第3節で指摘した現状の問題点に対する効果について検証を行った。実施概要は以下の通りである。

【企業の概要と適用範囲】	
企業の業種	：クレジット産業
対象資産	：個人情報
対象部門	：個人情報を利用する各部門(40部署)
対象業務プロセス	：個人情報を利用する業務プロセス
業務プロセス数	：約３００プロセス
実施期間	：２００７年１２月～２００８年２月（３ヶ月間）

実際に実施した部門へのヒアリングを行った結果、「自らの業務のリスクが明確になった」、「自部門の業務に多くのリスクがあることが分かった」といったコメントが寄せられており、資産の利用者である業務従事者が自らの業務におけるリスクについて認識することができたと考える。また、「想定されるリスク」以外のリスクを特定している部門も多く、業務プロセスにおけるリスクについて改めて認識を深める契機となったことが窺える。さらに、約２０プロセスにおいて、５０近い残存リスクが発見された。これは現状では認識されていなかったことであり、今回の手法を導入したことで、改めて残存リスクを抽出することができたものである。また、今回のリスクアセスメントは、普段リスクアセスメントについて見識の無い従業員が行ったにもかかわらず、約３ヶ月間の間に４０部署、約３００業務プロセスについて評価することができた。さらに、実施結果について検証した結果、評価者による評価のゆらぎが生じることは無く、誰でも簡単かつ確実にリスク評価を行えたものと言える。

以上のことから、今回の手法により、業務プロセス上にどのようなリスクがあるかを業務従事者自らが把握することができ、現状の問題点に対して有効であったと言えるだろう。

このように、本論で提案した手法は、現状の問題点に対して有効であり、この手法は情報セキュリティ意識の向上に寄与できるものであると考える。特に、評価者やその上司である部門長がリスクを改めて認識できた点については、その対策である社内ルールについての理解を促進する効果も期待でき、従業員の意識を変えるための契機になったと考えている。

7. 今後の課題

今回の手法においては、予めリスクを想定する仕組みとしたため、その構造上、リスクの網羅性、リスク認識の妥当性に懸念が残る。この点については、今後内部監査との融合等を図り、網羅性やリスク認識の妥当性をチェックできるものとしたい。

また、今回は1社で1回実施したのみであることから、今後、広範かつ継続的に実施していくことで、改善を加え、より確実な手法としていきたい。

さらに、成熟度モデルの指標を組み込むことで、組織におけるセキュリティレベルの成長の把握に活用し、各部門、各担当者の自律的な改善を支援するツールとして、より効果的な手法となるようにしていきたい。

以　上

参考文献

[1] 財団法人ニューメディア開発協会、『ISMSの維持管理における実態調査』、2007年

[2] 『JISQ27002 情報セキュリティマネジメントの実践のための規範』、財団法人日本規格協会、2006年

[3] 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』、経済産業省、2003年

[4] 『ＩＳＭＳユーザーズガイド - JISQ27001:2006（ISO/IEC27001:2005）対応-』、財団法人日本情報処理開発協会、2006年

[5] 『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』、経済産業省、2002年

[6] 『JISQ27001 情報セキュリティマネジメントシステム - 要求事項』、財団法人日本規格協会、2006年

[7] 『ＩＳＭＳユーザーズガイド - JISQ27001:2006（ISO/IEC27001:2005）対応- リスクマネジメント編』、財団法人日本情報処理開発協会、2007年

[8] 企業会計審議会、『財務報告に係る内部統制の評価及び監査の基準』、金融庁、2007年

[9] Larry Hubbard、『統制自己評価　実践的ガイド』、眞田光昭訳、日本内部監査協会、2004年

[10] 山本祥司、『内部統制をどう捉えるか　他人任せにしてはいけない内部統制整備・評価～内部統制をどう捉えるか⑤～』、第一生命経済研レポート2006年9月号、第一生命経済研究所、2006年

[11] 米国標準技術研究所、『NIST Special Publication 800-26　IT システムのためのセキュリティ自己アセスメントガイド』独立行政法人情報処理推進機構、NRIセキュアテクノロジーズ訳、2001年

[12] 吉川肇子、『リスク・コミュニケーション』、福村出版、1999年

[13] 吉川肇子、『リスクとつきあう』、有斐閣、2000年

[14] 関澤純編著、『リスクコミュニケーションの最新動向を探る』、科学工業日報社、2003年

[15] 堀江正之、『成熟度モデルに基づく情報セキュリティ監査の新たな試み』、会計検査研究 第28号、会計検査院、2003年、171-186頁

[16] 土井智朗、星智恵、村上博、森貴男、山口健太郎、内田勝也、『ISMS 認証取得組織における現状と課題～認証取得組織へのアンケート調査から～』、日本セキュリティマネジメント学会第21回全国大会発表要旨、2007年、185-190頁

[17] 内田南、『内部統制実務講座 第10回 財務報告に係る内部統制評価の実務－プロセスレベル統制の有効性評価－』、情報センサー 2006年12月号、2006年、4-8頁