情報セキュリティマネジメントシステム (ISMS) における効率的な詳細リスクアセスメント実施手法の提案と情報処理センターへの適用

Proposal of an efficient risk-assessment method for Information Security Management Systems (ISMSs) and its application to an Information Processing Center

市川 哲彦 †, 永井 好和 †, 長谷川 孝博 ‡, 伊藤 賢 §, 三池 秀敏 †

Ichikawa, Y.†, Nagai, Y.†, Hasegawa, T.‡, Itou, K.§, Miike, H.†

ichikay@yamaguchi-u.ac.jp, ynagai@yamaguchi-u.ac.jp, miike@yamaguchi-u.ac.jp,
cithase@ipc.shizuoka.ac.jp, itouken@itsc-ltd.co.jp

山口大学大学情報機構メディア基盤センター †
静岡大学総合情報処理センター ‡
株式会社 ITSC§
Media and Information Technology Center, Yamaguchi University†
Information Processing Center, Shizuoka University‡
ITSC Ltd.§

概要

近年情報セキュリティの重要性が認識され，情報セキュリティを組織的にかつ継続的に維持するための情報セキュリティマネジメントシステム (Information Security Management System, 以下 ISMS) の構築・運用が重要視されるようなった．山口大学メディア基盤センターでも平成 18 年度から本格的な構築作業に取りかかった．ISMS を構築する上で最も工数のかかる作業の一つが資産のリスクアセスメントであるが，本センターにおける構築では，関係スタッフの教育レベルや経験にばらつきがあり，一般的なリスクアセスメントの概念や脅威・脆弱性の例を説明しただけは，どのような脅威や脆弱性を考えたらら良いかの判定ができず，リスクアセスメント作業が進まないという問題が発生した．そこで，本研究では特に初期段階のリスクアセスメントプロセスを効率よく進めるための手法を提案し，また，この手法を実際の ISMS 構築に適用した結果について報告を行う．本手法では，まず各資産管理者が適用済み対策と懸念事項を書き下し，次に構築担当者が機械的な置き換えを行う．最後に再度資産管理者と構築担当者で話し合いながら脆弱性識別とリスク値の評価を進める，この手法に従ってリスクアセスメントを進めた結果，約 4ヶ月で完了することができたため，大学の情報処理センターのように，人数に比して資産が多く，また，スタッフが多忙でインタビューに時間をかける余裕が無いケースでは有効であると考えられる．

キーワード

ISMS, リスクアセスメント

1 はじめに

情報セキュリティの重要性が認識され，また数々の情報漏洩事故などが報道されるにつれ，情報セキュリティを組織的にかつ継続的に維持するための情報セキュリティマネジメントシステム (Information Security Management System, 以下 ISMS) の構築・運用が重要視されている．また，一般企業だけではなく大学のような教育・研究機関においても個人情報保護やセキュリティ教育の観点から ISMS が重要視されるようになっている [1] [2].

ISMS は国際標準 ISO/IEC 27001 [3] に従って構築・運用するのが一般的であり，その場合，適用範囲の決定，基本方針の策定，資産の識別，リスクアセスメントおよび対応計画策定，というステップを踏むことになる．なお，ISMS では資産は「組織にとって価値をもつもの」と定義されており，人，物，情報，サービスなどが全て含まれる．資産の識別については，業務フロー図や業務手順書の中から，授受するデータ，操作・加工するデータ，保存・保管するデータ，またそれらを行う上で利用される装置や機器を洗い出すという手法が知られている．また，資産管理に必要な人的コストを軽減するために，価値，用途，使用する場所，リスクが同等なものをグルーピングすることで管理項目を減らすという指針も知られている [4]．そのため，これを足がかりにして資産認識の作業を開始することが可能である．

リスクアセスメント手法の分析については文献 [5] に詳しいが，現在では TR X 0036-3[6] のリスクアセスメント手法 (詳細リスク分析) が一般的である．この手法では，資産の機密性，完全性，可用性のそれぞれの側面について次の 4 つのステップを踏んで進められる:

1. 資産価値を定める;
2. 考えられる脅威を特定しそのレベルを定める;
3. 実装されている管理策を考慮して脅威に対しての脆弱性を識別しそのレベルを定める;
4. 資産価値，脅威レベル，脆弱性レベルの乗算によってリスク値を算出し，受容レベル[1] 内にあるかどうかを判定する．

ISMS 認証規格 ISO/IEC 27001 の 4.2.1 d) e) を満たす上にはこの手法をマニュアル化することで十分であると認識されている．しかしながら，脅威や脆弱性の例は TR X 0036-3 や BS 7799-3[7] に挙げられてはいるものの，実際に各ステップを進めようとすると，どのような脅威を考え，どのような脆弱性を考えれば良いのかが大きな障害となることが山口大学メディア基盤センターにおける ISMS 構築の過程で判明した．

山口大学メディア基盤センターでは 2007 年 4 月より本格的に ISMS 構築に取り組んでおり，外部のコンサルティング会社による ISMS 構築講習会を実施し，ISMS 構築演習にはほぼ全てのスタッフを参加させている．従って，TR X 0036-3 で述べられている手法については各スタッフは十分に理解をしており，また，資産の管理状況についてもそれぞれの資産管理者は十分に把握している．しかしながら，いざ自分たちがもっている資産に対してリスクアセスメントを実施しようとしても構築作業が思うように進まないという状況に陥った．一部の資産管理者に意見を聞いたところ，脅威や脆弱性の識別手順が明確ではないために，どこから手をつけて良いのか見当が付かず，また，例として TR X 0036-3 や BS 7799-3 中のものを提示されても，逆に，全てを網羅的にチェックしなくてはならないように感じ，心理的な負担となっているということが次第に明らかになった．

本研究では上記の問題に鑑み，TR X 0036-3 に従ってリスクアセスメントを実施するための具体的な手法について提案を行う．既存の手法としては JRMS (JIPDEC Risk Management System) [8] があるが，ベースラインアプローチであることとインタビュー項目が多岐にわたり職員負担が大きいという問題がある．また，資産の設置場所，担当者，接続ネットワークの属性を用いて詳細リスク分析を効率良く進める手法 [9] もあるが，これでは資産についての脅威や脆弱性をどのように識別するのかについては解決ができない．同様に詳細リスク分析を用いるものとしては，CRAMM (CCTA Risk Analysis and Management Methodology) が英国のデファクトスタンダードであり支援ツールの販売も行われている．詳細は調査中であるが，文献 [5] では全てのプロセスを完了するまで長期間を要する点が指摘されており，我々の要求に応えることは難しいと考えられる．

以下，第 2 節では提案手法の概略について，また，第 3 節では本学で実施したケーススタディについて報告する．続いて議論ならびに今後の課題を述べる．

2 リスクアセスメント実施手法

本手法の目的は，TR X 0036-3 の手法を理解しているスタッフに対して，リスクアセスメント実施のより詳細な手順を与えることで，短期間に，少ないスタッフでリスクアセスメントを終えられるようにすることである．まずこのような手法の検討に至った経緯について述べる．

本学メディア基盤センターにおける ISMS 構築は，通常の構築手順に従い，資産の一通りの洗い出しが終了し

[1] 受容レベルは ISMS 基本方針や業務内容に基づいて経営陣が決定を行う．

た後に，リスクアセスメントのフェーズへと移行した．本フェーズには，資産洗い出しの過程で各資産毎の管理者責任者・管理者が明確になっているので，各資産の管理者に適宜資産のリスクアセスメント業務を振り分け，また，1 名のスタッフがリスクアセスメント結果をとりまとめるという体制で臨んだ．しかしながら，当初の予定に比して作業が遅々として進まないという事態が発生した．資産のリスクアセスメント担当者から意見を聞いたところ,「どのような管理策が適用済みであるかを列挙することは可能であるが，それらを，脅威，脆弱性という言葉で表すことが難しい」，また,「考えられる脅威や脆弱性にはさまざまなものがあるが，どこまで検討すれば十分なのかが判らない」というコメントが寄せられた．また，脅威レベルや脆弱性レベルについては 4 段階で数値化するようリスクアセスメント手法を定めたが，この定量化作業もリスクアセスメントの負担感につながっていたと考えられる．[2]

脅威の例としては，コンサルティング会社から入手したものや，TR X 0036-3 付属書 C に含まれるものや BS 7799-3 に含まれるものなどをリストアップして提示したのであるが,「代表的なものだけを挙げておりこれだけにとどまらないという」という説明が，逆にどこまで考えれば良いのかわからないという意見につながったものと思われる．本来であれば，同文書の付属書 D や BS7799-3:2006 付属書 C を提示し，さらに脆弱性のリストや脆弱性と管理策との関係も提示する予定であったが，逆効果と判断して情報提供を停止し，より簡便で作業に入りやすい方法を検討することとした．

インタビューやディスカッションを実施した結果，現状適用済みの管理策については，それが ISO/IEC 27001 付属書 A のどこに分類されるかを明示的に意識しているわけではなくても容易に列挙できること，また，現在計画されているリスク対応計画については担当者自身は容易に説明することができることから，これらの情報を収集することを足がかりとしてリスクアセスメントを行うこととした．本来であれば，リスクアセスメントがあり，その結果として適用する管理策の決定とリスク対応計画の立案がなされるのであるが，ある程度独自に管理策の適用が進んだ状態から ISMS 構築に向かう際には，逆向きに情報収集をした方が実施が容易であるという判断に基づいている．

まず，現状の把握においては Microsoft Excel, MindManager 等のツールを使うことはせず，項目だけを決めて自由形式で「メモ書き」として記述する方法を採用した．各種ツールを用いたり XML 等の機械可読な形式を用いることで，以降の処理を自動化するという選択肢も検討されたが，作成者の負担感を払拭することが第一と判断したためである．収集した情報がリスクアセスメントの第一次情報になる．

これらのメモ書きには次の項目を含めた:

- 資産名称
- 資産管理担当者
- メモ書き作成者[3]
- 資産価値と判断根拠
- 現在行っている管理策と対処する脅威
- 懸念事項
- 対応計画

なお，懸念事項と対応計画については，項目としては別に設定せずに現在の管理策を列挙する時にに補助的なコメントとして記載をするようにしている．

一次情報の例を図 1 に示す．これは教室用のパーソナルコンピュータ (PC) と，教室システムを統括しているサーバ類について記述したものである．資産管理者にはこの形式で例示を行い，多少形式を変更しても構わない旨を伝えた上で，それぞれが担当する資産について記述を依頼した．

この形式での情報収集の後に，形式変換，担当者への提示，インタビューとディスカッションを経てリスクアセスメント結果が構成される．例文はこの作業を進めやすくするため，意識的に文体をかなり統一してあり,「対策 c: t による p の喪失の防止」としてある．[4] 資産を a としたとき，(a, p, t, c) をエントリとして表形式にすると，先の例では表 1 のようになる．ただしこの表では，後の操作がしやすいように懸念事項は管理策とは別な列にしてある．さらにこの表を特性，脅威でグルーピングすると表 2 となる．

ここまでは資産の管理者以外のスタッフが機械的に進めることができる．ここからは管理者との共同作業となる．まず，管理策は脆弱性の “裏返し” であるため，先の表を編集して脆弱性記述を加えていく．結果は表 3 の通りである．この段階では対策と懸念事項は一つにまとめている．ある程度は管理策から脆弱性の名称は推測できるため，初期段階では取り纏めの担当者や一部のスタッフがまとめて行い，その上で資産管理者に確認を求めることで管理者の負担を軽減することができる．

さらに管理者へのインタビューによって資産価値，脅威レベル，脆弱性レベを加え，これらの乗算値をリスク値とする．結果を表 4 に示す．なお，ここでは，資産価

[2]後に再現性を担保するたに各レベル毎の例を盛り込む形に変更しているが，本質的な問題は各レベル分けについての共通認識が形成されていなかったことであると考えている．

[3]オプション．担当者とは別に協力者が作成した場合に用いる．

[4]自由形式であることは伝えてあるので，この構造以外の情報提供も想定されたが実際には例外は無かった．

```
============================================================
資産名称: 教室 PC
担当者 (作成者): 市川

資産価値
- C: 2. システム内容が漏れても関係者への影響は少ない
- I: 2.
  完全性が損なわれると講義・演習に影響があるが, 代替機を用いることで対処可能.
- A: 2. 可用性が損なわれると講義・演習に影響があるが, 代替機を用いることで対処可能.

現在行われている策と対処する脅威
- セキュリティワイヤ
    盗難による可用性の喪失
    なお, マウス・キーボードの盗難対策は一部の教室のみで実施.
- 一般ユーザと管理者とを区別する
    誤用による完全性の喪失
    悪用による完全性の喪失
- ウィルス対策ソフトウェア
    ウィルス感染による完全性の喪失
    ウィルス感染による可用性の喪失
- ハードディスク保護
    誤用による完全性の喪失
    悪用による完全性の喪失
============================================================
資産名称: 教室 PC 用サーバ
担当者 (作成者): 市川

資産価値
- C: 2. システム内容が漏れても関係者への影響は少ない
- I: 3. 完全性が損なわれると講義・演習に影響がある
- A: 3. 可用性が損なわれると講義・演習に影響がある.

現在行われている策と対処する脅威
- サーバ室内への設置
   盗難, 破壊による機密性の喪失.
   盗難, 破壊, 空調エラーによる完全性の喪失.
   盗難, 破壊, 空調エラーによる可用性の喪失.
- UPS
   不安定な電源による可用性な喪失
   停電による故障による可用性の喪失
- アクセス制限 (ssh はかかっている. http はかかっていない. )
    誤用による完全性の喪失
    悪用による完全性の喪失
- 故障対策
  *教室がまるまる止まるけどまったくしていない.
  *バックアップについては要確認

リスク対応計画
  今のところ無し
```

図- 1: リスクアセスメント一次情報の例

表- 1: セキュリティ対策テキストを表データに変換した結果．a, p, t, c は本文中の説明と対応している．

資産名 (a)	特性 (p)	脅威 (t)	対策 (c)	懸念事項
教室 PC	可用性	盗難	セキュリティワイヤ	マウス・キーボードは未実施
	完全性 完全性	誤用 悪用	利用権限の区別 利用権限の区別	
	完全性 可用性	ウィルス ウィルス	ウィルス対策ソフトウェア ウィルス対策ソフトウェア	
	完全性 完全性	誤用 悪用	ハードディスク保護 ハードディスク保護	

表- 2: セキュリティ対策テキストを表データに変換し再編成したもの

資産名	特性	脅威	対策	懸念事項
教室 PC	完全性	誤用	利用権限の区別 ハードディスク保護	
		悪用	利用権限の区別 ハードディスク保護	
		ウィルス	ウィルス対策ソフトウェア	
	可用性	盗難	セキュリティワイヤ	マウス・キーボードは未実施
		ウィルス	ウィルス対策ソフトウェア	

表- 3: セキュリティ対策テキストを表データに変換し脆弱性記述を加えたもの

資産名	特性	脅威	脆弱性	対策・懸念事項
教室 PC	完全性	誤用	保護策の不備	利用権限の区別 ハードディスク保護
		悪用	保護策の不備	利用権限の区別 ハードディスク保護
		ウィルス	ウィルス対策の不備	ウィルス対策ソフトウェア
	可用性	盗難	盗難防止措置の不備	セキュリティワイヤ マウス・キーボードは未実施
		ウィルス	ウィルス対策の不備	ウィルス対策ソフトウェア

表- 4: セキュリティ対策テキストを表データに変換しリスク値評価を加えたもの

資産名	特性	脅威	脆弱性	リスク値	対策・懸念事項
教室 PC	機密性 (2)	—	—	–	–
	完全性 (2)	誤用 (3)	保護策の不備 (1)	6	利用権限の区別 ハードディスク保護
		悪用 (3)	保護策の不備 (1)	6	利用権限の区別 ハードディスク保護
		ウィルス (3)	ウィルス対策の不備 (2)	12	ウィルス対策ソフトウェア
	可用性 (2)	盗難 (3)	盗難防止措置の不備 (3)	18	セキュリティワイヤ マウス・キーボードは未実施
		ウィルス (3)	ウィルス対策の不備 (2)	12	ウィルス対策ソフトウェア

値，脅威レベル，脆弱性レベル共に 1 から 4 までの 4 段階評価とし，値が大きいものほど高い，とした．基本的なリスク分析とリスク評価は以上で終了である．

このようなステップを踏むことで，テキストレベルで収集した一次情報からリスク評価結果を得ることができる．以降は，

1. リスク評価値が受容基準内に入るか否かの判定，
2. 受容できないリスクについて低減・受容・回避・移転のいずれかの対策を選択，
3. 低減について適切な管理策を選択し計画を立案する，

というステップが続き，リスクアセスメントが完了する．

3 適用事例

前節で述べた手法を山口大学メディア基盤センターの ISMS 構築に利用した．資産の洗い出しには，各スタッフが担当業務を分析し，授受するデータ，操作・加工するデータ，保存・保管するデータ，またそれらを行う上で利用される装置や機器を挙げるというプロセスを経たのち，業務・サービスという観点からグルーピング行うことで実施をしている．業務手順書が完備していなかったため，各業務やサービスの担当者自身がこの作業を行っている．資産はグルーピングを行った結果約 40 である．ここで，サービスの単位で資産はグルーピングされている．例えば先ほどの例で上げた教室用サーバシステムであれば，DHCP(dynamic host configuration protocol) サーバ，ウィルス対策サーバ，ActiveDirectory サーバなどの複数のサーバが含まれているし，また，データベースサービスであれば，内訳として，Oracle9i, PostgreSQL, MySQL，FreeBSD といったソフトウェア，サーバ 3 台分のハードウェア，利用申請書のような情報などがすべて含まれている．技術的には異なる管理策を適用することができるが，資産数を減らすためにこのようにグルーピングしてリスクアセスメント担当者を割り当て，必用に応じて適宜担当者が分割を行うものとした．

リスクアセスメントは適用範囲に含まれる専任教育職員 9 名，技術職員 2 名，技術補佐員 1 名，事務補佐員 3 名および兼任教育職員 1 名が分担して行った．担当したスタッフのうち 1 名を除く全員が事前または実施途中で外部コンサルタントによってなされた ISMS 構築についての二日間の講習会を受講しており，そのため，ISMS の基礎概念を理解している．

当初は前節で述べたような手順を明示せず，脅威のサンプルと脆弱性のサンプルを示して作成を依頼したが，第 1 節で述べたとおり，どのような脅威を考えればよいのかわからない，評価をするに当たって脆弱性や管理策としてどこまで検討すれば良いのかわからない，というような理由によりリスクアセスメント作業が進まないという問題が発生した．前節で述べたような手順の概略を示して一次情報を収集したところ，作成依頼から数日で約半数の情報が得られた．最終的には 1ヶ月程度でほぼ情報の収集が行われた．

一次情報の収集の後のリスクアセスメント作業は，文書管理担当の非常勤職員のサポートの下で各担当者によって行われた．ISMS 構築のコンサルタントを交えて適宜議論しながら進めた結果，全体としては約 4ヶ月でリスク評価が終了した．その他の業務をすべて行いながら進めたことや，途中に年度の境界が含まれているため，実質的にはさらに短期間で進めることができると考えられる．

問題点と考えられる事項もある．まず，管理者はどのような管理策を適用しているのかを想起するのは容易ではあるが，その一方で，どこまでを列挙すれば良いのかがわからないという意見が出された．例えば，要求事項 [3] の附属書 A の管理策の中にある「A.11.2.2 特権管理: 特権の割当て及び利用は，制限し，管理されなくてはならない」というようなアクセス制限は，システム設定においては極めて一般的であるため，敢えて適用した管理策として書くべきかどうかが問題となる．現時点では明示的な判断基準を出すことが難しいため，主要なものを列挙し，意見交換と議論の過程で見直すこととした．

次に，ボキャブラリーの統一が難しいことが挙げられる．管理策の記述や，脅威・脆弱性を記述する際に用いる言葉を統一することでリスクアセスメント結果の可読性が向上すると共に，他者の行ったリスクアセスメント結果を参考にする際にも有用であると考えられる．当初の予定では脅威や脆弱性の一覧から選択することを検討していたが，負担感が増すということと，脅威や脆弱性の記述に用いる言葉の解釈について共通認識を持つことが難しいことから，今回は特に制約を設けず，記述者の感覚に合う言葉を用いることを認めている．結果としてリスクアセスメント結果にやや統一感を欠いている感が否めないが，今後徐々に改善がなされるものと考えている．

また， 本手法に固有の問題では無いが，リスク対応計画を “先取り” する例が発見されたので報告しておく．ISMS 導入当初，全管理策を実施しなくてはならないのか，という質問が寄せられた．そのため，当時検討を進めていた ISMS 構築ワーキンググループでは，「認証取得時には要求される管理策がすべて実装されていなくても，対応計画が作成されていれば良い」，という説明をしていた．これは，ISMS 構築の一連のプロセスを踏まえていたのであるが，リスクアセスメントの過程で意見交換をした結果，この説明を「対応計画があれば対処済みとして扱っても良い」というように誤解する職員が

居ることが判明した．例えばネットワーク等の利用申請書の管理状況に若干問題があると考えられるが，より安全な保管場所に変更することが計画されているため脆弱性無し，という判断をしたり，ネットワーク装置の防塵対策に問題があると考えられるが，おおむね改善がされておりまた改善計画があるため脆弱性無しとして判断したという例があった．現状では，リスクアセスメント，リスク対応計画の立案，経営陣の承認という基本的なステップが実施されておらず，リスク認識，経営陣の承認，リスク対応計画の立案という異なったステップを踏んでいることからの混乱でもあると考えている．他の大学においても ISMS 構築と通常業務実施中の各種改善が平行して進められる可能性は高いと考えられ，ISMS 構築を推進する ISMS 事務局のスタッフへの説明の方法など，工夫が必要であると言える．

4　まとめ

本稿では，リスクアセスメントを進めるための手法について提案を行った．この手法は，対策として何をしているのか，また，それらは何を防ぐためなのか，を列挙するステップからスタートする．資産の管理者が実施済み管理策を列挙するのは容易であるため，リスクアセスメントの第 1 ステップをこのような簡便な方法にすることで，短期間に必要な情報を収集することができる．また，収集された情報からある程度機械的に資産価値，脅威，脆弱性の表にまとめることができるため，リスクアセスメント作業を効率良く進める事ができる．依然として，第 1 ステップで基本情報を集める作業は，資産担当者以外が作成するのは困難であり，また，リスク評価の最終ステップである脅威や脆弱性のレベル判定も担当者以外が行うことは難しいものの，この中間のステップは機械的に実施できるために，他のスタッフによる分担も可能となるからである．

この手順を本学メディア基盤センターの ISMS 構築の一部に適用した．一般的なリスクアセスメント手法についてのみ説明を行って作業を依頼していた状況では評価結果がなかなか集まらなかった．しかしながら，本手順を示したうえで，適宜分担および情報交換をしながら進めた結果，文書管理担当の非常勤職員のサポートはあるものの，約 4ヶ月で資産のリスクアセスメントを行うことができた．年度末・年度頭の多忙な時期が含まれているため，実施時期をうまく設定すればさらに期間を短縮できるものと考えられる．

本手順では，ほぼ自由形式で記述を与えることを第 1 ステップとしているが，実際には記述パターンが想定されており，「(資産 a に対する) 対策 c: t による p の喪失の防止」という形式になっている．従って，XML のようなタグ付けを支援するアプリケーションを用意すれば，中間ステップのかなりの部分を自動化することも可能と考えている．テキスト形式での入力にこだわらないのであれば Web アプリケーションとしてシステムを構築することで記述パターンを自動的に強制することも考えられる．ただし，適用している管理策の説明から脆弱性を特定する作業が必要であり，技術的にはこの処理をどのように支援するのかが課題となる．あらかじめ対策としてどのようなものがあるかを列挙することができ，かつ，それらについてスタッフ間の共通認識が得られれば，Web アプリケーションでメニューから選択させるようにすることで対策の語彙を制限することができる．さらに，脆弱性と対策との関係をあらかじめデータベース化しておくことができれば，選択された対策から脆弱性の候補を絞り込み，そのメニューの中から脆弱性を選択させることができる．あまりリストが長いと負担感につながる可能性があるが，使用する語彙の統一という意味でも効果が期待できるので，今後検討する価値があるものと考えている．また，リスクアセスメントの再現性を担保する方法としても有効ではないかと考えられる．

謝辞

本研究は山口大学大学情報機構メディア基盤センタースタッフの多大なる協力のもとに行われました．ここに記して謝意を表します．

参考文献

[1] 八巻, 藤本, 長谷川, 館野, 小林, 野崎, 中山, 岡田, 井上：“大学の IT コンプライアンス”, 静岡学術出版 (2007).

[2] 電子情報通信学会編：“情報セキュリティハンドブック第 5 編第 4 章”, オーム社 (2004).

[3] JIS Q 27001: 2006 (ISO/IEC 27001:2005): “情報技術 – セキュリティ技術 – 情報セキュリティマネジメントシステム要求事項”, 日本規格協会 (2006).

[4] 日本情報セキュリティ認証機構：“BS7799 情報セキュリティマネジメントシステム基礎コース”, 日本情報セキュリティ認証機構 (2005).

[5] 日本セキュリティ監査協会：“リスクアセスメント調査報告書”, 日本セキュリティ監査協会 (2004).

[6] TR X 0036-3:2001: “IT セキュリティマネジメントのガイドライン－第 3 部: IT セキュリティマネジメントのための手法”, 日本規格協会 (2001).

[7] BS 7799-3:2006: “情報セキュリティマネジメントシステム－第 3 部: 情報セキュリティリスクマネジメントの指針”, 日本規格協会 (2001).

[8] 日本規格協会：“JIPDEC リスクマネジメントシステム解説書”, 日本規格協会 (2004).

[9] 長谷川, 伊藤, 渡邊, 八巻：“詳細リスク分析法に基づく新しい情報セキュリティリスクアセスメント手法”, 経営情報学会 2007 年秋期全国研究発表大会, 浜松, pp. 334–337 (2007).