情報的側面からの企業評価指標

永田　清

1．はじめに

企業活動を大きく分けて経営分野、会計分野、情報分野の３分野から見た評価指標を作成するというプロジェクトにおいて、我々の担当は情報分野であるが、情報システム全般をどのように捕らえるかがまず問題になる。一般に情報システムといった場合、扱う範囲は非常に広く、場合によると会計システムや経営判断の意思決定システムにまで至るであろう。しかし、本プロジェクトにおいては、まず各分野における固有の評価指標を作成し、それらを持ち寄りすり合わせ、全体的な評価指標システムに仕上げていこうという趣旨であるから、我々の考察すべき範囲も自ずと限られてくる。

範囲をあまり大きくせずに企業における情報資産を中心に考察することとする。この場合に、もう一つ考慮しなければならない問題が生ずる。企業が情報を扱うシステムには、情報資産の効率的な運用により利益を最大限に発揮するといった目的がある一方、情報資産に関係するリスクを最小限に留めるといった面も考慮されなければならない。後者に関しては消極的な印象が強く、場合によると軽視されてきたのが現実であろう。しかし、今回の報告で述べるようにさまざまな標準や認証が行われている今日、必ずしもマイナスを押さえるといった消極的な事柄ではなく、認証取得などによる積極的な企業戦略としても成り立つ可能性を持っている。ここで我々は、情報システムに係わるリスク評価を情報システム評価の一部分として扱うか、それとも独立に扱いそれらのバランスにより全体の評価をすべきなのか、といった問題に突き当たる。“リスク”という言葉を使ったが、この言葉自体はかなり広範囲の意味を持ち、情報システムのリスクなどといえばそのシステムがもたらすさまざまな結果まで含むことになってしまうだろう。セキュリティ評価と言えば良いのかもしれないが、ここで紹介する基準や認証の中には“リスク評価”を行うというものがあるので、敢えて“リスク”を使った。

情報の効率性やリスク、セキュリティをどのように扱うにせよ、最終的には情報システム分野としてまとまったものを出すことになるが、現段階では情報システムのセキュリティやリスクを独立して扱うこととする。また、今回の報告では、情報資産の効率性や利便性などではなく、リスクに係わるさまざまな評価システムを概観する。

2．さまざまな情報セキュリティ評価

我々の目的は、個々の企業の情報システムを評価することであるから、内部のアンケートや外部に出た客観的な情報などをインプットとして処理し、評価値となるアウトプットを得るより良い方法を模索する必要がある。そのためにまず、既存の評価システムを研究することが必要になる。

セキュリティ評価またはリスク評価システムには、さまざまなものが存在しそれぞれの対象とする範囲や用途が規定されている。ここで取り上げるのは、BS7799に由来するISO17799とISMS認証、Common Criteria(CC)とCEM、我が国のリスクマネージメントシステムであるJRMS、およびその他のセキュリティ(リスク)評価システムである。これらの多くは非常に大きなシステムであり、その由来、評価対象や方法などにも違いがあるが、例えばリスク分析などの個別の分析、評価には共通のツールを用いることもありうる。また、アンケートには1000を超える質問項目が存在し、各部門から4、5人の回答者を必要とするなど、中小企業に対して適用するにはかなり困難なシステムだと思われる部分があるが、その考え方、セキュリティ評価方法、アプローチの仕方などは十分参考になる。

3. BS7799、ISO17799

1993年に「Code of Best Practice, Information Security Management」として、英国で発行された情報セキュリティに関する基準が、1995年には「BS7799; 1995 A Code of Practice, For Information Security Management」として英国標準となった。このBS7799は、

・情報セキュリティ管理実施基準(Part1)

・情報セキュリティ管理システム仕様(Part2)

の2つからなっている。Part1では、さまざまな事柄に関し英語の“should(すると良い)”といった表現が使われているのに対し、Part2では“shall(しなければなら)”といった表現で必要要件を明確に規定している。

ISO(International Organization for Standardization;国際標準化機構)がBS7799 Part1を標準化したものが「ISO/IEC 17799:2000 Information Technology－Code of Practice for Information Security Management」であり、情報セキュリティ対策実施のためのガイドラインと位置づけられている。そこでは、大項目として次のような10項目が要求されている。

(1) 情報セキュリティポリシー
(2) セキュリティ推進組織
(3) 情報資産の分類および脆弱性分析
(4) 人的セキュリティ
(5) 物理的環境的セキュリティ
(6) 運用管理
(7) アクセス制御
(8) 開発およびメンテナンス
(9) 業務継続計画
(10) 準拠

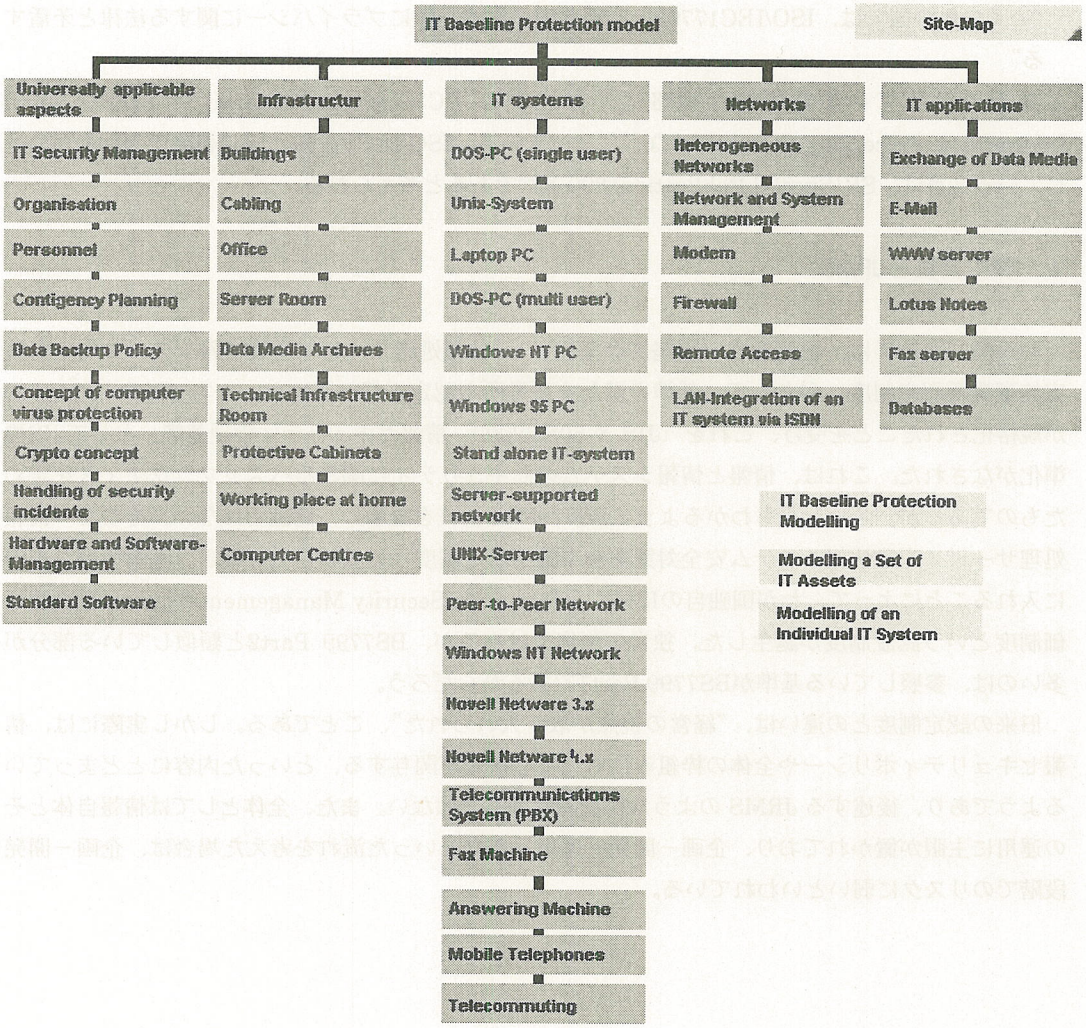
ISOは国際標準化を目指す組織であるが、ISO/IEC 17799を自国の規格とするかどうかは、それぞれに国が判断する事柄である。2002年3月時点で国家規格として採用している国は、英国、オランダ、オーストラリア、ニュージーランド、ブラジル、チェコ、フィンランド、アイスランド、アイルランド、スウェーデン、ノルウェーなどがあり、わが国もその中に入っている。これらの国の

ほとんどは、まだ国際規格化されていない BS7799 Part2も取り入れ、自国の認証規格としている。

一方米国、カナダ、ドイツなどの国々では、独自の規格を持ち、それらがISO/IEC 17799に勝っているといった主張を展開している。以下にドイツと米国の規格を概観する。

ドイツ：1991年に BSI 法に基づき設立された BSI(Bundesamts für Sicherheit in der Informationstechnik)(英国の BSI は、認証などの業務も行う企業である[1])が作成した「IT ベースライン・プロテクション・マニュアル」がある。ホームページ[2]上には、図1に示すようなプロテクション・モデルの構成図があり、各項目をクリックすることにより詳しい内容が表示される。

図1



[1] http://www.bsi-global.com/

[2] http://www.bsi.bund.de/gshb/english/menue.htm

この図からもわかるように、構成はハードウェアなどの機器、ソフトウェアの種類といった“部品”や、組織・場所などの区分からなり、それらの安全性をどのように確保するかが示されている。

米国：商務省の技術管理本部であるNIST(National Institute of Standards and Technology)がISO/IEC17799に対し、批判的な文章を公表している。以下に、㈶日本情報処理開発協会(JIPDEC)による訳[3]からいくつかを引用する。

“詳細な組織上のセキュリティレビュー、もしくは認証プログラムをサポートするに足る情報を提供していない”

“技術上の規格ではなく、IT システムの導入に関連して非技術的な課題を評価するマネジメント規格”

“いくつかの国では、ISO/IEC17799の一部が国の法律、特にプライバシーに関する法律と矛盾する”

2番目で触れている技術的な規格は、後述するCC(Common Criteria)やFIPS(Federal Information Processing Standards)などによっている。ISO/IEC17799と同じ範疇でNISTが公表している文書は、SP(Special Publication)800-XX[4]であると考えられる。

4．ISMS認証とJRMS

わが国においては、旧通産省（現経済産業省)の「情報処理サービス産業情報システム安全対策実施事業所認定制度」があって、基準を満たす事業所の認定を行っていた。一方でISO/IEC17799が規格化されたことを受け、これを「JIS X 5080:2000　情報セキュリティ管理基準」としてJIS標準化がなされた。これは、情報と情報システムのセキュリティに関わるベストプラクティスを定めたものであるが、名称からもわかるようにBS7799のPart1を継承し、認証ではない。そこで「情報処理サービス産業情報システム安全対策実施事業所認定制度」の流れを受け継ぎ、国際標準を視野に入れることによって、わが国独自のISMS(Information Security Management System)適合性評価制度という認証制度が誕生した。独自の制度ではあるが、BS7799 Part2と類似している部分が多いのは、参照している基準がBS7799 Part1であるからだろう。

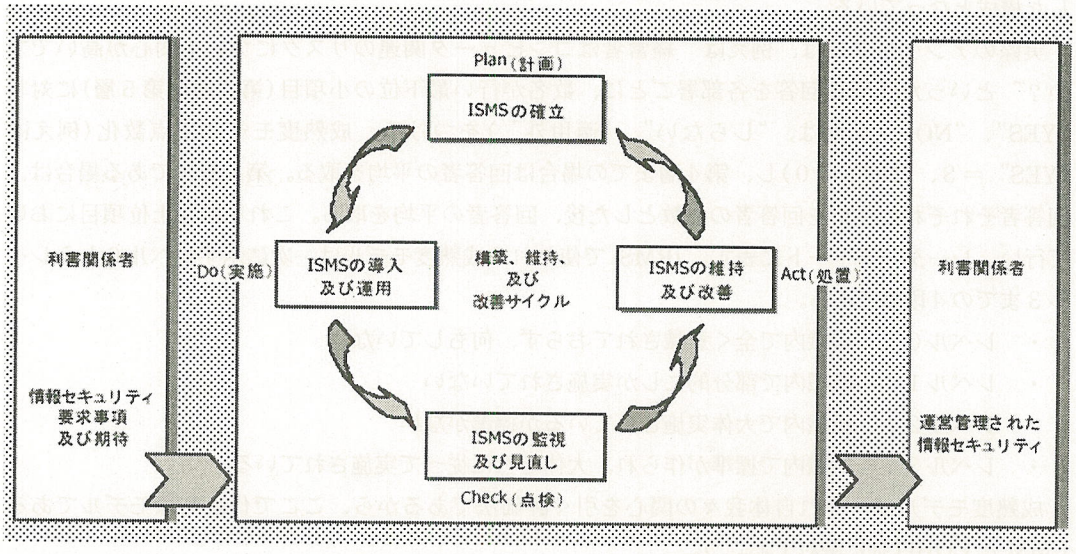
旧来の認定制度との違いは、“経営の視点が取り入れられた”、ことである。しかし実際には、情報セキュリティポリシーや全体の枠組みにおいて経営者が関与する、といった内容にとどまっているようであり、後述するJRMSのような積極的な関与ではない。また、全体としては情報自体とその運用に主眼が置かれており、企画－開発－運用－破棄といった流れを考えた場合は、企画－開発段階でのリスクに弱いといわれている。

---

[3] ㈶日本情報処理開発協会，“情報セキュリティマネジメントシステム(ISMS)の国際動向と取り組みの実際”，平成14年9月，pp. 34-36

[4] http://csrc.nist.gov/publications/

図２　出所：㈶日本情報処理開発協会、“ISMS 認証基準(Ver.2.0)”



ISMS の要求項目は、ISO/IEC17799の大項目10の下に連なる約1000の小項目である。マネジメント・システムとして、図２に示す PDCA(Plan-Do-Check-Act)のサイクルが確立しているかを認証の要件として取り入れている。

経営的な要素を強く出した情報システムに関わるリスクマネジメントシステムが、JIPDEC(日本情報処理開発協会)による JRMS(JIPDEC Risk Management System)である。 JIPDEC によるリスク分析の方法論であり、JRMS の母体とも言える JRAM(JIPDEC Risk Analysis Method)(1992)では、

・事故分析による被害の定量的把握

・質問票による情報システムの脆弱性分析

という２つの方法でリスク解析を行うことを提唱している。

2001年に公表された「JIS Q 2001: 2001 リスクマネジメントシステム構築のための指針」をベースとして、JRAM における第２の手法である“質問票による情報システムの脆弱性分析”に基づき JRMS が構築された。

第１の手法である“事故分析による被害の定量的把握”は、過去に発生した被害による損失を金額などで定量的に測定する方法であり、それ自体興味深いがここでは JRMS の項目や評価の仕方などを見ていくこととする。

2002年度に JIPDEC から公表された“情報化社会におけるリスクと JRMS”によると、質問項目数は1004項目で、それらが４または５階層の中・小項目に分類されている。表１で上位階層のみを示す。そこで示された内容、キーワードに関する質問を、経営者、リスクマネジメント部門、情報システムリスクマネジメント組織、ユーザ部門の複数人に対し行うが、部門によって回答するものとしないものがある。また、ⅠとⅡは全社的組織関連と位置付けられ、リスクマネジメント担当役員(CRO)が運営する。ⅢとⅣに関しては、情報システムマネジメント組織の長である情報システム担当役員(CIO)など運営に当たる。このように、JRMS は情報や情報システムと経営的な視点と

を併せ持ったマネジメントシステムである。また、前述のように企画、開発段階でのリスクに配慮した構成となっている。

実際のアンケートでは、例えば“経営者はコンピュータ関連のリスクについて関心が高いですか？”といった質問の回答を各部署ごとに、数名が行い最下位の小項目(第４層か第５層)に対し“YES”、“NO”(または、“しらない”、“適用外”)をつける。成熟度モデルで点数化(例えば“YES”＝3、“NO”＝0)し、第４層までの場合は回答者の平均を取る。第５層まである場合は、回答者それぞれの平均を回答者の点数とした後、回答者の平均を取る。これを順次上位項目において行い、レーダーチャートに表す。JRMS で使われる成熟度モデルは、次に示すレベル０からレベル３までの４段階である。

- レベル０：　組織内で全く意識されておらず、何もしていない
- レベル１：　組織内で部分的にしか実施されていない
- レベル２：　組織内で大体実施されているが標準がない
- レベル３：　組織内で標準が作られ、大体それに従って実施されている

成熟度モデルは、それ自体我々の関心を引く評価法であるから、ここで代表的なモデルであるCMM と COBITⅢに触れておこう。

CMM(Capability Maturity Model)は、米国防総省の依頼により Carnegie Melon 大学のSEI(Software Engineering Institute)が開発した、組織のソフトウェア開発能力評価を行うモデルである。ソフトウェア開発プロセスの成熟度をレベル１(Initial)、レベル２(Repeatable)、レベル３(Defined)、レベル４(Managed)、レベル５(Optimizing)の５段階に分類している。

ソフトウェア開発を対象とする CMM を情報システム全体に広げ、成熟度評価を行ったものがCOBITⅢである。開発プロセスを“企画・計画と組織(PO)”、“調達と開発(AI)”、“運用と支援(DS)”、“モニタリング(M)”の４つの管理プロセスから成るとし、それぞれを PO1～PO11、AI1～AI6、DS1～DS13、M1～M4の合計34の IT プロセスに分類している。評価は“有効性”、“効率性”、“機密性”、“完全性”、“可用性”、“準拠”、“信頼性”の７つの情報基準と、“人間”、“業務システム”、“技術”、“設備”、“データ”の５つの IT 資源に対し行われる。レベルは CMM の５段階に最低位のレベル０を加えた６段階である。

表1.

Ⅰ	経営とリスクの関係	
	1 経営環境とリスクマネジメント	経営者の関心，経営レベルによるリスク範囲，リスクマネジメントポリシー等々
Ⅱ	JRMSにおけるリスクマネジメント計画	
	1 JRMSの計画	
	2 JRMSの実行組織	全社的リスクマネジメント，情報システムリスクマネジメント，ユーザの各組織に分類
	3 JRMSの維持	
	4 JRMSのリスク分析	リスク分析の仕組み，体制，実施，および災害，事故，情報システム，経営，政治・経済・社会それぞれのリスク分析をキーワードとする質問
	5 JRMSのリスク対策	リスク対策の分析，財務的対応，リスク対応のための組み合わせ，テロ，人命損失などをキーワードとする質問
Ⅲ	情報システムのリスク分析	
	1 情報セキュリティポリシーのリスク分析	
	2 情報システムのリスク分析	情報システムのリスク分析，システム開発，システム運用，アウトソーシング
	3 情報システムの個別リスク分析	Ⅳ - 3，4，5に関する項目
Ⅳ	情報システムにおけるリスク対策	
	1 リスク対策における情報セキュリティ	
	2 情報システムのリスク対策	情報システム総合企画，システム開発，システム運用，アウトソーシング，システム監査
	3 不正アクセス・コンピュータウィルス関連	コンピュータ犯罪，不正アクセス，コンピュータウィルス，e-Commerce，電子メール
	4 災害対策	
	5 障害対策	
	6 その他の関連事項	
	7 バックアップ	
	8 緊急時対策	

5．CCとISO TR 13335

NSA(National Security Agency)におけるNCSC(National Computer Security Center)が、コンピュータの安全評価の基本的標準として作成し、1985年に改訂版がDoD(Department of Defense)標準 DoD 5200.28-STD として発表されたのがTCSEC(Trusted Computer System Evaluation Criteria)である。そこでは、製品が提供する保護レベルを区分Aから区分Dまでの4つに区分けしている。区分Dは最小保護、区分Cは任意型保護クラス(C1、C2)、区分Bは必須保護クラス(B1、B2、B3)、区分Aは検証型保護である[5]。TCSECの影響を受けカナダは、機能上の基準をサービスに分解し、異なった強度レベルを与えたCTCPEC(Canadian Trusted Computer Product Evaluation Criteria)ver.3.0を1993年に発表した。一方EUでは、TCSECの保証要件から多くの特徴を分離し、機能要求クラスの導入、商用評価ファシリティという概念の採用などによっ

[5] アーサー E.ハット他著 “[翻訳版]ワイリー コンピュータセキュリティハンドブック”，㈱富士テクノシステム，p25

て、政府と商用のセキュリティ要件両方を満たすことを目標とした ITSEC(Information Technology Security Evaluation Criteria)を1991年に発表している。これら米国、カナダ、欧州の動きがひとつになり、1996年には共同評価基準 CC(Common Criteria ver.1.1)が生まれた。CC は情報処理製品のみでなく、情報処理システム全体の信頼性まで認証する制度である。2000年には、ISO/IEC 15408として国際標準化され、我が国でも JIS X 5070として JIS 化されている。CC には次に示す９つの機能要件、10の保証クラス、７層の評価保証レベルがある。

機能クラス：

監査、通信、ユーザデータ保護、識別と認証、プライバシ、TOE(Target of Evaluation)、セキュリティ機能保護、資源利用、TOE アクセス、高信頼性パス

保証クラス：

「セキュリティ基本設計書」の評価、「セキュリティ設計ガイドライン」の評価、構成管理、配布と運用、開発、ガイダンス文書、ライフサイクルサポート、テスト、脆弱性評価、保証の維持

評価保証レベル：

EAL1(一般向け機能のテスト確認)...EAL7(公式検証方法に基づく設計とテスト確認)

ここで我々は、特に保証クラスの“脆弱性評価”を参照し、分析する必要があるかもしれない。また、CC を基にした評価に関するガイドとして CEM(Common Methodology Information Technology Security Evaluation)があり、リスク分析手法を含んでいる。

CC は上述のように信頼性認証制度であるが、セキュリティポリシーの作成、情報システムの運用に係わる人や情報処理機器の管理に関する参照情報として ISO TR(Technical Report) 13335がある。ここに含まれるリスク分析手法は、情報資産の脆弱性分析として ISMS においても用いられる。

6．その他

・OCTAVE^{SM}(Operationally Critical Threat, Asset, and Vulnerability Evaluation System)

CMM 開発でも知られる Carnegie Melon 大学の SEI が開発したセキュリティ評価システムであり、資産ベースの評価を行う。組織内の小さなチーム(Analysis Team)によりすべての情報解析と次の３つの手順の管理が行われる。

フェーズ１：　資産ベースの脅威プロファイルを作成

フェーズ２：　基盤脆弱性の特定

フェーズ３：　セキュリティ戦略の計画と発展

・BIA(Business Impact Analysis)

中心的業務機能やその実行性に対する情報システム障害の影響力を評価する。具体的には、“組織に影響を及ぼしかねない崩壊や災害によって引き起こされる問題を洗い出す”、“問題の数量化や質の評価”、“重要な機能、復旧の優先順位、相互依存関係などを明確化することによって復旧時間目標を定める”などを、５つのキー要素(Time Criticality, Health and Safety, Customer

Satisfaction, Embarrassment, Financial)を考慮しながら行う。

・FIPS(Federal Information Processing Standards)

NIST と NSA が作成する“設計、開発、高信頼性情報システムや製品の評価”の必要条件を定式化するための基準であり、TCSEC にとって代わろうとするプロジェクトの中で実現した。FIPS PUB No65ではリスク分析ワークシートにより、定量的なリスク分析が行われる。

図3はワークシートの例であり、年間の予想損失額を1から8までレベル化された“予想損失発生頻度(f)”と“1回当たりの予想損失額(i)”を基に式 $ALE = C^{(f+i-3)}$ (C はある定数)によって計算している。

図3

システム/アプリケーションデータファイル (SYSTEM/ APPLICATION Data Files)	データインテグリティ (DATA INTEGRITY)		データ機密性 (DATA CONFIDENTIALITY)	可用性 (PROCESSING AVAILABILITY)			コメント (COMENTS)
	Modification	Destruction		2hrs	24hrs	72hrs	
	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	(i) (f) (ALE)	
アプリケーション870	6 3 $300K	4 2 $300K	7 4 $30M	–	–	–	
AgPlans	5 3 $30K	4 2 $300	6 3 $300K	–	–	–	
CurrProg	4 2 $300	–	–	–	–	–	
ProgHist	4 3 $3K	4 2 $300	4 3 $3K	–	–	–	ALE:年間推定損失
WWWMod	4 2 $300	4 2 $300	4 2 $300	–	–	–	K: 1000
PFiles							M: 100万

(出典：FIPS PUB NO.65より)

7. おわりに

今回は、情報セキュリティやリスク評価を中心に、既存の基準や方法などを調査し簡単な比較・分析を試みた。細部にわたるものではないが、全体としてどのような状況になっているのかがはっきりしてきたと思う。今後は、より詳しい分析を行い我々の目的に合う評価方法の開発に役立てたい。また、情報システム全般の評価方法としてどのように仕上げていくかも今後の課題である。

[参考文献]

[1] アーサー E.ハット他著“[翻訳版] ワイリー コンピュータセキュリティハンドブック”、㈱富士テクノシステム

[2] 江村潤朗監、“情報セキュリティとシステム監査”、中央情報教育開発協会

[3] 情報処理振興事業協会、“情報技術セキュリティのための共通評価方法論 パート1 概説と一般モデル”、1997年1月

[4] 情報処理振興事業協会、“情報技術セキュリティのための共通評価方法論 パート2 評価方法論”、1999年8月

[5] 田辺雄史、“IT セキュリティ評価・認証制度について”、経済産業省商務情報政策局情報セキュリティ政策室、2002年3月

[6] ㈶日本情報処理開発協会、“JIPDEC リスクマネジメント(JRMS) のあり方に関する研究(JRAM2002)”、2002年3月

[7] 堤 裕司、“COBIT の概要、CMM の概要”、ITC 総研、2002年7月

[8] ㈶日本情報処理開発協会、“情報セキュリティマネジメント(ISMS)の国際動向と取り組みの実際”、2002年9月

[9] ㈶日本情報処理開発協会、“情報化社会におけるリスクと JRMS －リスク対策検討委員会 調査研究報告書”、2003年3月

[10] ㈶日本情報処理開発協会、“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)－”、2003年4月