セキュリティー・リスク・アセスメントにおける定性的評価の改善

松井 康宏

Remedy for the Qualitative Method of Security Risk Assessment

Yasuhiro Matsui

セキュリティーのリスク・アセスメントにおいては脆弱(ぜいじゃく)性などを定性的に評価する手法が使われることが多いが，その評価結果はゆらぎやすい．本論文では，すでに日本で広く利用されている ISMS（Information Security Management System) 関連の文献等を参照し，定性的評価の精度を向上させるための改善策を検討する．その改善策は，あるケースの ISMS 認証に適用し，その有効性を確認した．

In security risk assessment, we often use the qualitative method to evaluate vulnerability etc. But the results are likely to be different by each assessor individual. This paper discusses remedies to give accuracy the qualitative method, referring to documents related to ISMS (Information Security Management System) already used widely in Japan. These remedies were applied to ISMS certificate of a certain case, and checked the effectiveness.

Key Words & Phrases：セキュリティー，リスク・アセスメント，レイティング，定性的評価手法，ISMS
Security, Risk assessment, Rating, Qualitative method, ISMS

1．はじめに

これまでセキュリティー対策に向けて多くの文献が発表されてきた．まだセキュリティー対策への根本的な思想が黎明期(れいめいき)だった頃に，運用まで考慮した方法論［1］に始まり，上流工程でのメソドロジー［2］やモデリング・アーキテクチャーを活用した方法論［3］へと，議論が発展してきた．

一方，セキュリティー対策を講ずるにあたり，状況調査のために，よくリスク・アセスメントを行う．この作業レベルでのリスク・アセスメント手法に関する情報整理も進み［4］，後述する 2 つの手法がよく知られている．1 つは 1992 年にリチャード・コートニィの理論に遡る定量的評価手法であり，もう 1 つは，Guideline for the Management for IT Security（GMITS）［5］が紹介する詳細リスク分析等で用いられている定性的評価手法である．

GMITS は 1996 年から国際的な規格 ISO/IEC TR13335-1~5 となり，現在でも情報セキュリティー管理システム（Information Security Management System:ISMS）の国際認証規格 ISO/IEC27001［6］で参照規格とされている．そのため定性的評価手法は，ISMS 適合性評価制度［7］の後押しを受けて周知されている．世界的にみて，ISMS 認証事業者数の過半数は日本の事業者で占めている状況［8］にあり，定性的評価手法の課題点を検討するのは，今後の進展を考えれば重要な意味がある．

定性的評価手法では対象を相対的に評価する作業をする．これを「レイティング」と言う．この作業では，評価の仕方を標準化し，なるべく単純作業に落とし込むようにする．しかし，それでも個人の主観に作業は依存するので，評価基準の設定，評価者の理解と感覚差，実施時期の相違等で得られた成果の精度はゆらぐ．そのため作業レベルで，どのような問題に遭遇し，またそれらにどう注意して，精度を確保してゆくか知見の集積が求められている．

そこで本論文では，ISMS ユーザーズ・ガイド［9］等関連の文献を参照し，定性的評価の精度を向上させるための改善策を検討する．以下 2 章で定性的評価手法のレイティング・フェーズでの課題を整理し，3

提出日：2007 年 9 月 3 日，再提出日：2008 年 3 月 26 日

章で，その改善策を示す．4 章で，実際に利用した成果と考察を述べる．最後に 5 章で，主張点をまとめる．

2. 代表的な手法と課題

2.1 ２つの代表的手法

リスク・アセスメントには，大きく以下の 2 種類がある．

（1）定量的評価手法：資産価値，脅威の度合い，脆弱性等を評価し，それらから業務上用いられている単位（金額等の絶対的数量）でリスク値を示す手法．例えば脅威の発生頻度と顕在化した時の損失額の積から予想被害額でリスクを表現する式（1）がある（文献［10］等）．

ALE＝SLE×ARO　　（1）

ALE：年間予想被害額
　　（Annualized Loss Expectancy）
SLE：個別予想被害額（Single Loss Expectancy）
ARO：年間発生率
　　（Annualized Rate of Occurrence）

（2）定性的評価手法：資産価値，脅威，脆弱性を大中小のような相対的な段階値で評価し，それらからリスクを指標で導出する手法．例えば，資産価値，脅威，脆弱性の相対的評価値の積でリスク値とする式（2）がある（文献［9］等）．

R = A（c, i, a）× T × V　　（2）

R：リスク値（Risk）
A：資産価値（Asset）
T：脅威（Threat）
V：脆弱性（Vulnerability）

資産価値 A は，次の 3 点で相対評価される．

c：機密性（confidentiality）
i：完全性（integrity）
a：可用性（availability）

2.2 それぞれの特徴と傾向

定量的評価手法では，資産簿価に基づき SLE が客観的に把握され，ARO も統計的に十分確かな必要がある．これが故に，ゆらぎの少ない高精度な成果が得られ，コストに敏感な予算・投資の根拠，保険額算出向けなどが主用途になる．逆に評価対象資産の価値が絶対的な金額換算になじまないと精度の検証はしづらい．例えばデータベース上のデータの SLE を表すのに，損失価値，代替および回復作業費，信用失墜被害など，資産簿価にないものは客観的に額を確定するのは難しい．この手法はおのずと適用範囲が限られる．

一方，定性的評価手法は事前に用意しておく相対的な段階値を評価に使うので，客観的な統計データが揃っていなくとも着手できる敷居の低さがある．つまり絶対性と客観性を失う代償を払うことで，評価対象の特質にこだわらず広く展開できる簡便性を得る．そして，定量的評価手法より普及と定着のフィージビリティーは高くなる．しかしながら，以下に述べる課題も抱えることになる．

2.3 ISMS における定性的評価手法とその課題

ISMS ユーザーズ・ガイド（以下同ガイド）は，定性的評価手法を用いて，かつリスク・アセスメント実施者の立場で具体的に解説しており，共通理解を得やすい文献である．ISMS 確立の 10Step（図 1）のうち，リスク・アセスメントは Step3~5 にかけてあり，Step4~5 で，定性的評価手法の特徴であるレイティングのサンプルを示してくれている．

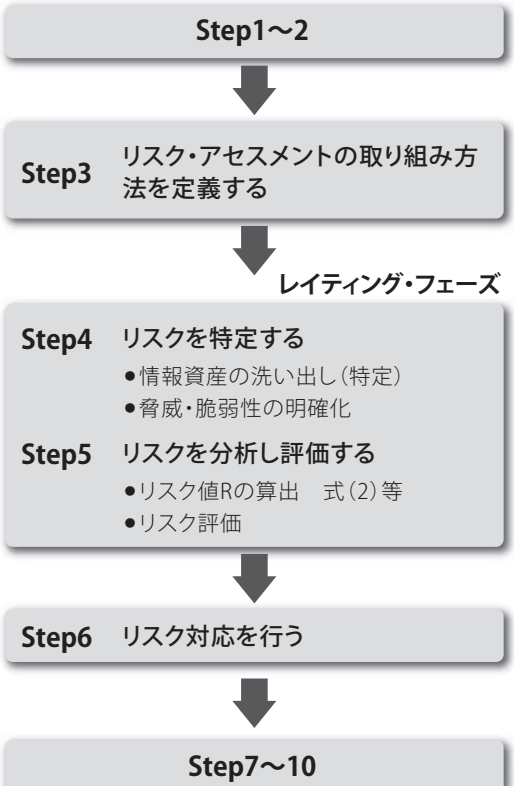


図 1. ISMS 確立の流れ

レイティング作業は，評価を段階的値のいずれかに振り分けるため，ゆらぎ要因を多く含む．これは式（2）

の単純さと相まって精度への影響をもたらす．以下に，レイティング・フェーズでの課題点を整理して述べる．

（1）評価値の段階数：評価値の設定を 3 段階，例えば 1，2，3 からの選択とすると，式（2）が積ゆえに，1 か 2 とするかで簡単に 2 倍差が生じ,ゆらぎを増幅する．これでは評価結果を想定して，レイティングに心理作用しかねない．また後から段階数を変えると，リスク評価基準の再設定に迫られ，年度対比もできなくなる．よって初めにどの程度の段階数を設定すべきか，あるいはどのように段階の増数が可能かが問題となる．

（2）主観による評価の個人差：レイティングは評価者の主観に委ねられるので，もともと個人差が出やすい．さらに同一対象物でも，立場が変われば人により差が出る．このことは同一評価者でも視点を変えれば，評価が変わることを意味する．

（3）状況の経年変化：評価対象や評価手法に変化がなくとも，評価対象が置かれた環境は，経年変化する．例えば，新しい脅威の出現や発生頻度の統計データ更新などである．資産価値も絶対的な変化がなくとも，法令改正で相対価値に影響する場合がある．

3. 対応する改善策

3.1 評価値の段階数

セキュリティー系監査では，High，Medium，Low の 3 値で報告する傾向がある．これは最終的に報告を受ける側に分かりやすくするためである.レイティング･フェーズでこれに倣う必要性はない．むしろ作業の容易性に対する精度の確保に注意すべきである．そのためには評価者に選択基準で迷わせないことが重要である．

これには，IT ガバナンスのフレームワークで有名な Control Objectives for Information and related Technology（COBIT）成熟度モデル［11］が参考になる．その自己評価アプローチによると，評価段階値として IT プロセスの不在（0）から最適化（5）までの 6 値を採用しているが，むしろ選択基準を明確に定義している点が参考になる．初めてリスク・アセスメントに取り組む場合は，そのまま採用することもできる．

すでに 3 値でレイティング作業している場合は 2.3（1）で述べたように，精度面で壁に当たる．レイティング結果にゆらぎが多く含まれたまま報告用に加工処理され,セキュリティー対策が講じられるのは好ましくない．

表 1. 小数値を用いた相対評価例

評価値	説明　(1),(2) は or で判断する
0.5	(1) 標準的な手順や手続きが整備，周知徹底され，守られている（実績が 1 年以上ある） (2) 合理的なコストや期間で実施可能な管理策はすべて実施している
1	(1) 標準的手順・手続きが整備され，守られている (2) 合理的なコストや期間で実施可能な管理策は実施している
1.5	(1) 手順や手続きはあるが，励行または徹底に改善すべきところがある (2) 合理的で実施可能な管理策は実施しているが，一部不足している
2	(1) 手順や手続きはあるが，励行または徹底がされていない (2) 一部の管理策のみ実施している
2.5	(1) 手続きや手順が未確立だが，口頭による指示や報告により業務遂行している (2) 管理策で未実施が多い
3	(1) 手順や手続きが確立されておらず，業務の遂行状況も不明 (2) 管理策がまったく行われていない

この場合，段階数を増やすには，小数値を採用する方法がある．

表 1 は，管理策の不備度合いの相対評価に使用した評価値の例である．当初 3 値を採用していたが，評価者から選択肢の少なさから選択に躊躇するという不評が出て，6 値に移行したものである．ただし 1，2，3 から 1，2，3，4，5，6 へマッピングしたわけではなく，0.5 刻みで 6 値にした．これには年度比較やリスク受容水準値の設定値が変わらないようにするため，0 以上 3 以下の範囲内でしか拡張が難しかった事情があった．この例では，少数値の利用により，全体のスケールを変更することはなく，評価結果のデータ処理はうまく収められている．

ちなみに同ガイド別冊　リスク・マネジメント編［12］p32 では「脅威やぜい弱性の分類数は概ね 3~5 である場合が多い様です」と紹介している．人間の感覚としては 1 桁が扱いやすい範囲なのは言うまでもない．それ以上は，際限がなく．定性的評価手法の特徴である簡便性を失うだけである．なお，式（2）を用いる場合，その特性から 0 の値は使えないことには注意する．

3.2 主観による評価の個人差

（1）用語理解の徹底と評価指標の導入:「リスク」,「脅威」,「管理策」等の言葉に対して，評価者の理解が不足していたり，一様にならないことがある．これには，該当具体例を列挙して評価者間で共有できる参照表

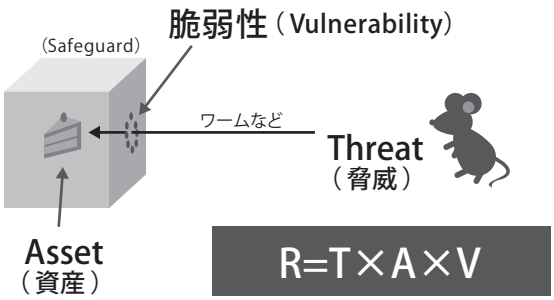
を用意しておくことが,「特定」作業には有効である. さらに必要なのは, レイティングの基準設定である. これには逆に一端抽象化して, 指標となる特徴を見出す方法があり, 簡易なモデリングである. 例えば同ガイド p44 で, 脅威を「情報システムや組織に損失や損害をもたらすセキュリティー事故の潜在的な原因」と定義しているが, これをもっと抽象化すると, 表 2 の意義欄にある「資産価値を損なう事象」にまで簡潔になる. その程度を測定するならば,(年間) 発生頻度を評価指標にできる. これを用語定義中に設けておくことで, 評価者間の理解は一定枠内にとどまり, レイティング作業に向いた準備とさせられる.

表 2. 用語の定義例

用語	意義	評価指標
資産価値	情報資産をセキュリティー面から見た価値	機密性 c, 完全性 i, 可用性 a
脅威	資産価値を損なう事象	年発生頻度
管理策	脅威からの保護策	(所定の表から選択)
脆弱性	脅威を顕在化させる増幅因子	現行管理策の不備度合→表 1 参照
リスク／リスク値	脅威が顕在化する可能性	確率同等／リスク値は指標値

評価者の視点を揃えるために, 脅威に対する管理策にも共有できる標準的なリスト (例えば ISMS 詳細管理策) を用意する. 従来の手順では, 管理策の適用はリスク・アセスメントの終わった後 (図 1 Step6) で検討していた. しかし, 現実には何らかの施策があるか無策であり, 標準との見比べを可能とするために用いる. さらに参照にとどまらず, 実際の運用実績データも用意しておく契機とする. この運用実績データについては (3) で述べる.

(2) 管理策による脆弱性の代替: 2.1 式 (2) では, 脆弱性がリスク値を決める一要素である. しかし, 脆弱性は脅威と混濁しやすく理解は一様には徹底しない. 例えば, あるシステムについて, 誤作動を脅威とした時, 設置場所が温湿度制御機能が低い環境なら, それが従来の脆弱性である. ただし, そんな設置環境を脅威ととらえることも可能であり, そのため人によりリスク・アセスメント結果が違ってくる. そこで脆弱性を評価者にとって, とらえやすいように変えた. まず 2.1 式 (2) から, 脆弱性を脅威の増幅係数とみなし, 表 2 の意義欄にあるように,「脅威顕在化の増幅因子」



(R:リスク　T:脅威　A:資産　V:脆弱性)

図 2. 脆弱性の概念図 (文献 [13] から引用)

と抽象化した. そして, 評価指標については「現行管理策の不備度合」とすることで, 従来の脆弱性の概念から切り替えた. ここでの脅威, 脆弱性および管理策の関係を図 2 で説明する. 従来, 脆弱性は評価対象固有の潜在的問題とされていたのに対して, 脅威の増幅因子を資産の周りにある箱 (セーフガード = 現行管理策) 上に見出し, そこに空いた穴こそが問題で, 穴の数や大きさを不備度合いと考えて評価指標としたのである. このように, 脆弱性を管理策側の問題に置き換えることで, 脅威と脆弱性の混濁を減らした. そして, 従来の分かりにくい脆弱性の意味は, レイティング作業では問わないようにした.

管理策を考慮して脆弱性を定性的に評価する考えは, 同ガイドのリスク・マネジメント編 pp.26-31 でも述べられている. これに対して本論文では, 主観性排除のために, さらに従来の脆弱性を測定可能な評価指標にまったく差し替え, さらに運用実績データを定量的に活用するアイディアを用いている.

(3) 管理策の運用実績データの活用: 管理策の不備度合いのレイティング作業は極力データに基づいて行う. それには管理状況の実績を裏付けるデータが必要となる. 一般に管理策には実施している以上, なんらかの運用実績データが付随する. 例えば PC 資産の「不正アクセス」の脅威に対して, PC 内のポリシー順守検査ツールの稼働やソフトウェア・レベルのタイムリーな更新を管理策としていれば, そのツール適用レポートや更新実績のデータがある. それらを用いて表 3 のような評価基準を作成し,これに従って,その不徹底度 (不備度合) をレイティングする. 管理策の運用実績データを用いたレイティングであるから, 主観の入る余地はかなり減る. つまり定性的評価手法の枠内でありながら, 定量的な手法が用いられていることになる. もちろん, データがないような管理策は不備度合いが高いと評価する.

表 3. 管理策の不備度合いレイティング例

	遵守率	評価値
ＰＣセキュリティーの例 管理下の全ＰＣで設定値が推奨値どおりになっている割合（定期点検結果）	１００％	０．５
	９９以上	１．０
	９５以上	１．５
	９０以上	２．０
	８０以上	２．５
	８０未満	３．０

3.3 状況の経年変化

ここでのゆらぎ要因は前二者と異なり，排除せず，むしろ利用することで精度を高められる．つまり避けられぬ状況の変遷を，あらかじめレイティング評価に反映されるようにしておくのである．以下に具体的に述べる．

（1）参照表の事前更新：社会や環境の変化は，情報資産や脅威の参照表類を用いて反映できる．具体例を示す参照表は必須であると上述した（3.2（3））とおりで，レイティング作業の着手前にタイムリーな更新をする必要がある.例えば可搬記憶媒体としてのUSBメモリーの脅威や脆弱性の参照表への追加等が相当する．これにより経年の変化を一律に反映でき，評価者間の認識差も回避できる．

（2）管理策の安定度評価：安定している管理策には安定度の評価点を設けるとよい．もともと脅威の発生頻度は他律的で確率的にもとらえにくい．例えば昨年地震がなければ今年は発生率が上がるとも，下がるとも言えない．これに対して，管理策は人為的なものである．複数年以上安定して機能してきた実績を評価するのは現実的に意味がある．いわゆる「枯れた技術」の評価である．具体的には**表1**で示すと,評価値 0.5 の（1）で，実績を加味しているとおりである．脆弱性を管理策の不備具合とするならば，有効な視点である．

（3）法規適合性：参照表の更新に際し，法規の創設改廃の影響事情があれば反映させておく．2005 年における個人情報保護法の施行は好例である．ただし，ISMS 適合性評価制度では法規適合性を一分野設けている［14］ように，まとめて吟味しておくのがよい．これはリスク・アセスメントとは別に定期的に行う方が確実である．

3.4 改善した手順

これまで上述の改善を施したものを**図３**に示す．（注:

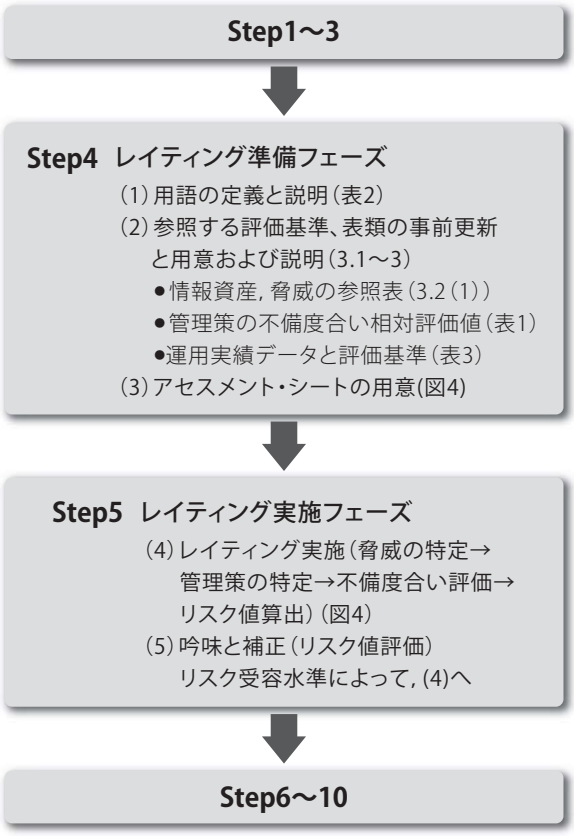


図 3. 改善を施した手順

カッコ内は本文中の参照先）

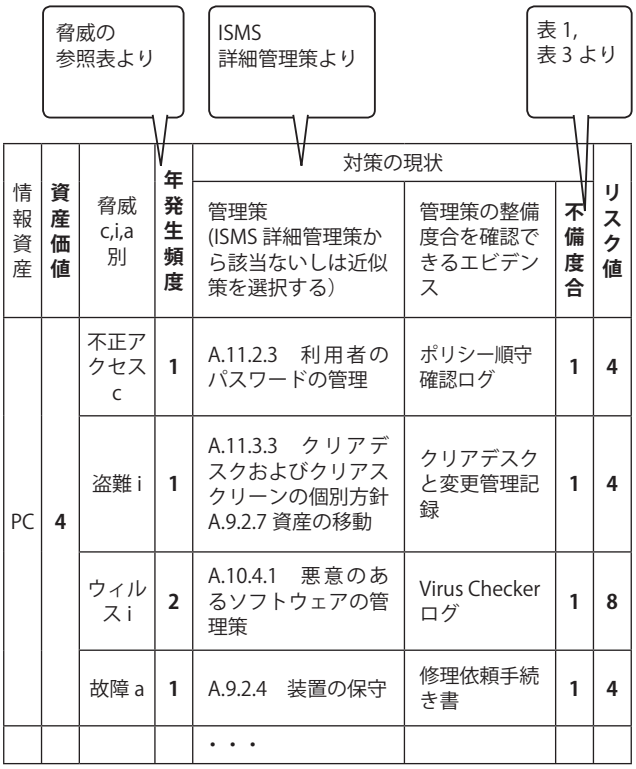
リスク・アセスメントで効果的なレイティングを実施するにあたり，準備が多いことが分かってきた．**図１**のレイティング・フェーズとの相違は，準備段階を明示的に手順中に設けて 2 フェーズ化した点である．**図１**の Step4 でも準備相当のことをしているが,必ずしもレイティング作業の課題解消を想定したものではない．これに対して**図３**の準備フェーズで用意する**表１**，**表２**，**表３**はレイティング作業にあたり，主観的判断をなるべく差し挟ませないための内容になっている．これにより実施フェーズでは，単純作業に落とし込まれたことを行えるようにした．

4. 実施例と考察

図３の改善手順を適用した実施例とその効果について考察する．

4.1 実施手順

図３の Step4 におけるレイティング準備フェーズで用意した表 1~3 は，すでに前章で掲げたとおりである．一度作成すれば年次で更新の手間がかかる程度である．



情報資産	資産価値	脅威 c,i,a 別	年発生頻度	管理策 (ISMS 詳細管理策から該当ないしは近似策を選択する)	管理策の整備度合を確認できるエビデンス	不備度合	リスク値
PC	4	不正アクセス c	1	A.11.2.3　利用者のパスワードの管理	ポリシー順守確認ログ	1	4
		盗難 i	1	A.11.3.3　クリアデスクおよびクリアスクリーンの個別方針 A.9.2.7 資産の移動	クリアデスクと変更管理記録	1	4
		ウィルス i	2	A.10.4.1　悪意のあるソフトウェアの管理策	Virus Checker ログ	1	8
		故障 a	1	A.9.2.4　装置の保守	修理依頼手続き書	1	4
				・・・			

図 4. リスク・アセスメント・シートの例（抜粋）

同 Step5 におけるレイティング実施フェーズで実際に使用したアセスメント・シートが**図 4** である．Step5 の順に左から右へ該当欄を記入して行けば，最後にリスク値が出る．シートに従えば評価者は，いずれも選択肢を与えられた形でのレイティング作業となる．主観的選択の余地が広がらないように選択肢は**表 2** の評価指標と**表 3** のような評価基準の値に従って選べるようにしてある．このような単純作業への落とし込みにより評価結果のバラつきが生じにくくなった．脆弱性を本質的に考えるのではなく，管理策の不備度合の評価をもって行うので，評価者からは，選択で迷わず楽になったというコメントがあった．

以上より**図 3** の改善された手順は，無理なく機能することが検証できている．

4.2 効率面

レイティングのフェーズを分けたことにより，かえって手間がかかっていないかの懸念がある．実施例でのリスク・アセスメント所要期間のデータを**表 4** に示す．ただし改善は一度に行ったのではなく，この間徐々に施されている．

2004 年は初めてのリスク・アセスメントで試行錯誤があり，手間がかかっている．実際のところ従来の方法では実施部門間の評価のゆらぎが生じていたため，レイティング作業後に全体の見直しを行わざるを得なかった．2005 年は**図 3** の手順がほぼ反映された下で，本格的にフェーズ分けしてレイティング作業をしている．2006 年は ISMS が ISO/IEC27001 へ移行する規格変更があったが，準備フェーズで，変化を吸収してリスク・アセスメントを行ったので，手戻りもなく遂行できた．この年の ISMS 認証の拡大・規格変更審査も良好に済んでおり［15］，決してワークロード増大は招いていない．

担当者の異動，サイトの拡大，規格変更，および年次の作業であることにより，繰り返しの熟練による効率化の要因は限りなく少ない．このような状況の中で，明確なフェーズ分けは，それぞれで変化の吸収をしてくれている．

表 4. リスクアセスメント実施期間

年度	サイト数	部門数	スケジュール上の期間
2004 年	3	10	約 4 ヵ月（初年度）
2005 年	4	13	約 1.5 ヵ月（拡大認証含）
2006 年	5	15	約 2 ヵ月（拡大／規格変更含）

4.3 留意点

ここでの改善策で定性的評価手法のすべての課題が解決したわけではない．依然以下の留意はいる．

（1）異なる評価対象間のリスク値：評価対象間の単純比較は要注意である．例えば PC100 台の包括評価とファクシミリ 1 台では定性的評価手法によるリスク値を対等比較できない．それぞれの絶対価値額が異なるからである．定量評価と異なり，それぞれがもともと別個に相対評価された以上，同一対象物を適用管理策により，どうリスク低減したか定点観測するにとどまる．これは精度を上げたとしても乗り越えられない．管理策を講ずる上で優先順位の検討材料として，経営者の参考資料となるにとどまる．

（2）同一の評価対象のリスク値：同一人物が同一対象を評価した時，毎回同じとは限らない．レイティングは相対評価である．評価対象が同一でも，情報資産の形態，脅威，法令等に更新があれば，それは評価対象の置かれている環境の変化を意味する．脅威等の特定作業用に例示する参照表は更新が必要であるとともに，クロス・チェックや全体の吟味は，いずれにせよ省けない．

(3) 事前更新：上記参照表類はレイティングの実施段階までには，更新と手配が済んでいなければならない．それにより精度が変わる．参照表は作るだけでなく徹底させることが肝要である.説明も十分しなければならない．

5. おわりに

本論文で目的とした改善策の提示は，**図 3** にまとめたとおりである．

ただし，この手順は PDCA サイクルを回し，3 年かけて改良してきたものである．常に改善してゆく不断の取り組みが，まさにマネジメント・システムであり，リスク・アセスメントを効果的プログラムにしている．

その意味でリスク・アセスメント過程に，ゆらぎ程度が分かる統計的技術を埋め込んだ手法の開発は今後の検討課題である．同一物の評価で評価者間の偏差が大きければ，警鐘を鳴らす指標の導入である．定性的評価であっても，数量的に有効性を可視化することで，早い段階でシステマティックな見直しが可能となる．レイティング作業はデータ処理になじむ作業であるから，工夫の余地はまだある．

謝辞

考え方の整理と情報提供において，データ・センター関係者の方々から積極的な協力を得られました．本論文の執筆に至れたことを，あらためて深謝いたします．

参考文献

［1］ 渡辺芳明: “セキュリティを確保したシステムを構築するための方法論,” ProVISION, No.29, pp.72-81（2001）.
［2］ 大西克己: “上流工程におけるセキュリティ･メソドロジーの実践,” ProVISION, No.42, pp.63-68（2004）.
［3］ 大津留史郎: “ ITセキュリティ要件の抽出手法 – オペレーショナル･モデリングとセキュリティ･メソッドの統合– , ” ProVISION, No.54, pp.80-87（2007）.
［4］ リスクアセスメント調査報告書ver1.0, 日本セキュリティ監査協会 http://www.jasa.jp/seika/pdf2003/dist_techwg3.pdf（2007）.
［5］ 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 – ,（TR X 0036-3:2001）,（GMITS: Guidelines for the Management for IT Security）, 日本工業標準調査会, http://www.jisc.go.jp（2008/2）.
［6］ Ted Humphreys and Angelika Plate: ISO/IEC 27001に基づくISMS認証の要求事項及び準備のための指針（英和対訳版）, 日本規格協会（2006）.
［7］ ISMS適合性評価制度の概要, 日本情報処理開発協会, http://www.isms.jipdec.jp/isms.html（2007/12）.
［8］ International Register of ISMS Certificates, Number of Certificates Per Country, http://www.iso27001certificates.com/（2008/1）.
［9］ ISMSユーザーズガイド – JIS Q 27001: 2006（ISO/IEC 27001:2005）対応 –, 日本情報処理開発協会（2008/1）.
［10］ 定量的セキュリティ測定手法および支援ツールの開発 – 調査報告書　別冊定量的セキュリティ尺度測定ガイドライン –, 情報処理推進機構, http://www.ipa.go.jp/security/fy15/development/metrics/documents/metrics_guideline.pdf（2004/4）.
［11］ COBIT 4.0 コントロール目標, マネジメントガイドライン, 成熟度モデル, IT ガバナンス協会, ISBN:1-933284-37-4, pp.22-23（2005）.
［12］ ISMSユーザーズガイド – JIS Q 27001: 2006（ISO/IEC 27001: 2005）対応– –リスクマネジメント編 –, 日本情報処理開発協会（2008/1）.
［13］ 郷間 佳市郎他：脆弱性定量化に向けての検討報告書, 日本ネットワークセキュリティ協会, p.6（2007/3）.
［14］ 法規適合性に関するISMSユーザーズガイド – ISMS認証基準（Ver.2.0）対応 –, 日本情報処理開発協会 http://www.isms.jipdec.jp/doc/JIP-ISMS115-10.pdf（2005/4）.
［15］ ISMS認証取得事業者一覧, 日本情報処理開発協会, http://www.isms.jipdec.jp/lst/ind/ISR001_JQA-IM0258.html（2008/2）

日本アイ・ビー・エム株式会社
ITD、セキュリティ / リスク管理、
ICP/ITA

松井 康宏 Yasuhiro Matsui

［プロフィール］
1986 年日本 IBM 入社．ネットワーク IT スペシャリストとして,インターネット系サーバー構築，e-business® ホスティングサービスのセキュリティ運用に従事．アウトソーシング部門で，データセンターの ISMS 認証取得を遂げ，現在アウトソーシング・プロジェクトのセキュリティ・チーム支援に従事．
ymatsui@jp.ibm.com