統計数理(2006)
第 54 巻 第 1 号 105–122

特集「統計科学とリスク解析」
[原著論文]

階層ホログラフィックモデリング法の適用による リスクアセスメントプロセス改善の試み

下平 利和[1] ・Hua Xu[2]

(受付 2005 年 7 月 20 日; 改訂 2005 年 9 月 26 日)

要　　旨

従来のリスクマネジメントでは，各実務分野の観点で特化した独自の方法論が先行し，属人的要素に依存する内容も少なくない．本稿では，複雑なシステムにおけるリスク特定の手法として広く認められている階層ホログラフィックモデリング(HHM)法を用いたリスクアセスメントプロセスの改善へ向けた試みについて報告する．具体的にはIT システムセキュリティ分野を適用対象とした一連の試行における観察結果をもとに，リスクマネジメントレベル向上のための系統的な取り組みと，その成果について議論を行う．本手法の適用により，リスクに関する現実的な構造モデルを得ることができ，その後のプロセスを円滑に進めるための理論的根拠となり得る．またここでは参考として，今回の結果を用いた解析・評価の応用イメージ例を示す．

キーワード：システムズアプローチ，階層ホログラフィックモデリング法，IT-セキュリティ．

1. はじめに

リスクという概念が対象とする範囲は非常に広く，その定義や内容は適用する分野によって大きく異なる．過去，筑波大学経営システム科学専攻では，特定実務領域を対象として，現場の必要に応じて適用可能な既存の手法やツールを整理するとともに，課題の解決のための新しい方法やツールの開発，応用などについての各種研究が行われてきた．

そこでは特に，リスクやリスクマネジメントを，システム工学の観点から統合的に取り扱うための方法論，すなわちシステムズアプローチについて，

- プロジェクト参加メンバーが業務で関係している領域において，リスクに関して問題となっている事象について，ケース研究またはサーベイを通じて問題の本質を抽出し，その中から汎用的な手法若しくはガイドラインを抽出する．
- メンバーが業務で関係する領域の中で，リスクのアセスメントとマネジメントシステムに関して改善・解決すべき課題を発見し，これまでに培われてきた技法や理論を適用し，あるいはその技法や理論自身を改良していくことにより，発見された問題の解決を試みる．

という二つの取り組みを基本として，問題への接近を図ってきた．

[1] 東京工業大学大学院 総合理工学研究科知能システム科学専攻：〒226–8503 神奈川県横浜市緑区長津田町 4259
[2] 筑波大学大学院 ビジネス科学研究科経営システム科学専攻：〒112–0012 東京都文京区大塚 3–29–1

本論文では IT システムセキュリティ分野を具体的な適用対象としたシステムズアプローチによるリスクマネジメントの問題解決への試みについて報告する．本分野は現在，情報漏えい事件の多発や個人情報保護の観点から大きく注目を集めており，また急速な技術革新など周囲の各種環境変化の早さゆえに，リスクそのものも大きく変動し続けているという特徴を持つ．

本論文の目的は以下の通りである．

(1) リスクマネジメントにおいて重要な位置を占めるリスクアセスメントプロセスに対して，HHM 法の適用による現状の課題の改善について提案する．
(2) IT システムセキュリティ分野における，具体的な HHM 法適用の観察を通して，改善の有効性と解決すべき課題について報告する．
(3) HHM 法によるリスクアセスメントプロセスの改善に伴う，マネジメントレベル向上に資する副次的効果について報告し，その応用の可能性について述べる．

本論文の学術的貢献は，一連のシステムズアプローチによる方法論の適用が，未だ属人的な部分の多いリスクアセスメントプロセスの改善に役立つという知見を得ることである．

以下，本論文の構成は次の通りである．2 章では，リスクアセスメントプロセスとその課題について概説し，本研究の位置付けを示す．3 章では HHM 法の概略について紹介するとともに，4 章でリスク因子の特定への具体的な適用について述べ，結果について評価する．5 章では参考としてその結果を用いた解析・評価の応用イメージを示し，6 章で結論と課題をまとめる．

2. リスクアセスメントにおける現状と課題

近年，我が国でもようやくリスクマネジメントという言葉が一般的になって来たかに見える．しかしながら，一般に使われているリスクという言葉にはさまざまなレベルのものが混在しており，むしろ，漠然としたイメージとして捉えられていることも多い．リスクマネジメントについても，その定義や，対象とする範囲は非常にあいまいであり，実は使う人によって大きく異なっているということに注意しなければならない．

この背景には，リスクという概念が持つ普遍性と多様性という特質がある．リスクが対象となる範囲は非常に幅広く，リスクという概念の無い分野を探すことの方が難しい．既に金融，経営，IT，環境，安全衛生など，さまざまな分野において，それぞれ確立された独自の方法論が存在している．そしてこの結果，同じリスクとかリスクマネジメントという言葉を使いながら，その意味するところは微妙に異なるという事態が生じているのである．

このような抽象的な概念であったリスクを，Lowrance (1976) は，「好ましくない事象の発生可能性とその結果の大きさの測定」と定義した．また，日本規格協会 (2003) の TR Q 0008 (ISO/IEC GUIDE73：2002)「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」では，「事態の確からしさと，その結果の組み合わせである．または事象の発生の確率と事象の結果の組み合わせである」と記している．これらの定義はリスクを測定する尺度に焦点を絞って表現したものであり，その発生の可能性 L と，結果の大きさ (被害規模) X とから，リスクの期待値 R を計算する以下のような数学公式とも一致する．

$$R = LX \tag{2.1}$$

この計算式は非常にシンプルな分，リスクの取扱いが格段に楽になり，しかも応用性が高いことから一般的に用いられている．だが，3 章において後述するように，これだけではリスクの定義として十分とは言えないことに留意しておく必要がある (Kaplan and Garrick, 1981)．

図 1 に TR Q 0008 の定義によるリスクマネジメントに関する各用語間の関係を示す．ここでリスク因子とは，結果をもたらす可能性が潜在しているものごとや行動と定義されている．

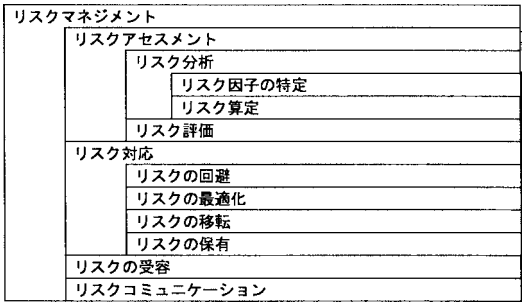

図 1.　TR Q 0008 **の定義によるリスクアセスメントの位置付け.**

リスクアセスメントを行う際には，まずリスク分析において，このリスク因子を特定し，続くリスク算定のプロセスにおいて，それら特定されたリスク因子の発生の可能性と，それによって引き起こされる事象の結果について検討する.

次いで，これらリスク分析プロセスで実施された原因と影響に関する因果関係モデルの内容，すなわち客観的あるいは主観的に予測された発生の可能性や大きさ，及び定量的あるいは定性的に定めた結果などについて，リスク評価のプロセスで正しく評価し，リスクマネジメントの目的から見た評価基準に基づいてランク付けを実施する．このリスク評価は，アセスメントとマネジメントの各プロセスのオーバーラップとして存在し，そこで決定した内容が，これ以降の判断における根拠として実際のリスク対策に連動していくため，非常に重要視されている.

この流れを見る限り，リスクアセスメントはシステマティックに処理されているように見受けられる．しかしながら実際の運用では，コストの都合などから簡便的・属人的な方法が採用されることも多く，しかも実施に当たっては，個人の勘や能力，あるいは過去の経験といった，組織化されていない属人的な対応に頼りきりというのが実状である.

例えばリスク因子の特定では，簡単に実施できるという理由で，規格や指針の記載内容などをもとに作成されたチェックリストを用いたヒアリングが一般的に採用されている．だがその場合，質問も回答も，画一的あるいは固定的なものになりやすいという欠点がある.

チェックリストは確かに効率的な手法ではあるが，基本的に内容が固定していることから，新しいインシデントへ柔軟に対応しきれず，また対象となる組織に固有の内容などの洗い出しについても，質問者の技量に依存する部分が非常に大きくなってしまう.

また，それを補完するために，関係者などによって実施されるブレーンストーミングも，非常に属人的な手法である．そして，本来は広く意見を集めることが目的のはずなのに，しばしば声の大きな人の主観的な発言に議論が左右されてしまったり，そのグループのオピニオンリーダー的な人物への追従が生じるといったことが起こりやすく，議論が広がらない，参加者間の情報の共有や公平な意見の提示が行えなくなるなどの問題が指摘されている(Vose, 2000**).**

一方，リスクには時間とともにその内容が変化するという特徴があるが，現状ではこうした変化への対応手段についても，ほとんど考慮できていない.

このような状況下では，せっかくリスク因子を特定しようとしても，網羅性などの点で十分な信頼度を確保することは不可能であり，有効なモデリングを行うことは出来なかった.

また，ほとんどの場合において，客観的な評価に十分なレベルの数値化は行われておらず，有効性評価のための数値化の手段についても未確立というのが現状である.

そもそもリスク分析を行う目的は，発生の可能性によってリスクを分け，リスクの評価及び

管理を支援するためのデータを提供することである．本来ならばリスクの算定は，存在する全てのリスク因子について個別に検討を行い，総合的に実施されなければならないはずである．

だが，これは非常に大変な作業であり，こうしたさまざまな因子について一つずつ検討していくといつまでもリスクを評価できないという理由で，通常は発生確率や規模について参加者によるブレーンストーミングなどによって大まかに評点を付け，(2.1)式を用いた簡便法により簡易的にリスクを評価していくのが現実的とされている．このような簡便法は，事前評価時のリスクアセスメントなどで普通に用いられているが，評価者の主観に影響されやすい．

このように，現状におけるリスクアセスメントは，基本的な概念とアプローチの考え方自体は間違っていないものの，実施の方法は洗練されておらず，しかも多くの場合かなり大雑把な形で運用されている．すなわち，実施時の詳細な内容にはかなり改善の余地が存在している．

3. 階層ホログラフィックモデリング(HHM)法によるリスクの特定

Haimes (1998)が提唱している階層ホログラフィックモデリング法(以下HHM法と略す)は，電力や上下水道のような大規模かつ複雑なシステムにおけるリスク特定のための一般的な方法として広く認められている手法である(Kaplan et al., 2001)．

通常，大規模で複雑なシステムは階層的な構造を有している．そしてそこにはシステム自体を構成する基本的な要素，例えば，目的や目標，制約条件，評価基準などに関係する階層的な構造とともに，社会的な要素，すなわち政治的，経済的，制度的，法律的，地域的要素などに関係した階層的な構造が互いに入り混じって存在し，それらが複数の部分システムを形成する．

こうしたシステムでは，リスクを単純かつ単一のプロセスと考えるのは現実的ではない．各階層の部分システムに潜在する個々のリスクが，部分システムに損害を与えるとともに，複合することにより，最終的にシステム全体へ重大な影響を及ぼしていくものと捉える必要がある．

当然そこでは，部分システムに潜在するリスクにいかに対処するか，という問題とともに，限られた資源を部分システム間でいかに効果的に配分するか，ということが最も重要な課題となる．その際，まず部分システムに潜在するさまざまなリスクを網羅的かつ効果的に特定するための，対象システムの構造モデルが重要となる．

このような複数の階層的構造が混在するシステムのモデル化では，多視点的な考え方が重要である．すなわち複数の視点からシステムを多面的に記述し，異なる視点から得られたモデルをオーバーラップさせていくことによって，全体システムのモデルを構築する．これはHHM法の基本的な考え方そのものである．

HHM法のアプローチでは，リスクマネジメントを対象システムの階層的な構造へ，うまく合致させることができるという点で非常に良い方法である．この結果，リスク特定にまつわる困難は大きく軽減され，対象システムをシンプルなモデルとして検討することが可能となる．

またHHM法では，(2.1)式の欠点を補う以下のような現実的なリスク定義に基づく期待値の算定式，すなわち可能性のある有限個のリスクシナリオの集合 S と，その発生の可能性 L，および結果の大きさ X の3つの要素の組み合わせとして検討するという考え方に対応している．そしてこの定義では，リスクマネジメントの初期段階では何を行うべきかが一目瞭然となる．

$$R=\{<S_\alpha, L_\alpha, X_\alpha>\}\,, \quad \alpha \in A \tag{3.1}$$

図2は階層ホログラフィックモデルの基本的なイメージをもとに，その作成と活用について概念的に示したものである．HHM法では，このような特殊なダイアグラムを用いる．ここで図の最上段，太枠のボックスにA-1，B-1，C-1,… と太文字で示されているのが，システムを記述するための切り口となる“視点”を表すヘッドトピックである．各ヘッドトピックは，その下に例えばA-1に対するa-1，a-2，a-3,… のように，細枠のボックスで表した複数のサブト

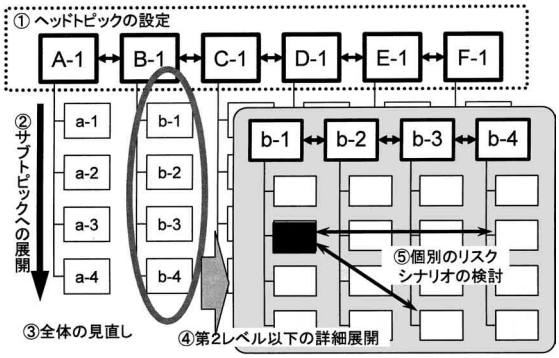

図 2.　階層ホログラフィックモデルと HHM 法によるリスク特定のイメージ.

ピックへと分解される．これらサブトピックはシステムを構成する部分システムあるいは要素と対応し，また，判断のための要求，条件，あるいは基準を表している．

ここで注目すべきは，これらダイアグラムの各縦列が，異なった視点から見た同一システムの持つ異なる属性を表現しているという点である．すなわち縦列を一つの組として見ることによって，リスクはかなりシンプルなモデルとして取り扱うことができるようになる．

また，それぞれの組は，個別の視点から得られたシステムのある側面のみを記述したものにすぎないが，これら各視点から得られたモデルを複合させることによって，各々のモデルが互いに補い合い，システムの全体像が総合的に表現されることになる．その結果，従来のアプローチからは分かりにくかった互いの関係性やそれぞれの位置づけも含めて，全体を俯瞰した形でリスクを本質的かつ弾力的に捉えられるようになるのである．

以下，HHM 法を用いてリスク特定を行う場合の，具体的な作業手順についてまとめておく．

step 1. **まず，参加者に全体の切り口となる視点についてのキーワードを出し合ってもらい，それについての意見交換を通してヘッドトピックの設定を行う．**
step 2. **各ヘッドトピックについて，それを構成する要素，あるいは関連する事項について自由に議論し，それぞれのサブトピックスへの展開を行う．**
step 3. **作成したモデルについて全体的な見直しを行い，修正する．**
step 4. **必要に応じて，サブトピックの組を基に第 2 レベル以下の詳細展開を行う．**
step 5. **個別のサブトピックやその関係性に着目することにより，具体的なリスクシナリオやリスクアイテムの特定作業を行う．**

このように，HHM 法を適正に用いるならば，対象システムの現実的な構造モデルを得ることが可能となる．それを基に，理論上は対象システムに関する大部分のリスクと不確実性の源を特定出来るはずであり，リスク解析や評価を効率的に行えるようになることが期待される．

一般に，現実の組織の多くは複数の異なるリスク要因を有しており，それらの要因が複雑なプロセスを経た後で，結果的にリスクへとつながっていく．実際，企業や事業体，政府などの組織は，階層的な構造を持った複雑なシステムとして捉えた方が適切なことが多く，HHM 法を用いたアプローチは，さまざまな面で広く適用していくことができるものと考えられる．

4. IT セキュリティ分野のリスクアセスメントにおける HHM 法の適用

以下，IT システムセキュリティ分野を適用対象とした一連の試行について述べる．具体的にはある民間企業で実施されたセキュリティポリシー構築プロジェクトでのアセスメント事例において，従来の一般的な手法による取り組みと平行して，HHM 法の適用など，システムズアプローチによる試行を行い，その過程で得られた成果物や，それぞれの手法の比較検討などを通して，その応用の有効性を探ることとした．

4.1 1 回目の試行における観察内容とその評価

今回，試行を実施した B 社は，一部上場の素材メーカー A 社の情報システム子会社である．従業員数約 60 名，その大部分を外部の協力会社の人材に頼っている．また，売上のほとんどは A 社およびグループ企業の情報システムの開発・保守・運用に係わるサービスが占めている．

親会社の A 社はいわゆる川上分野の企業であり，個人消費者との直接の接点が少ないということもあって，セキュリティについての意識は必ずしも高いとはいえない．これまで B 社は，外部からの脅威への対策を中心に必要なセキュリティ投資を行ってきたが，個人情報保護法対応などへの危機感から，今回，情報セキュリティポリシー導入に取り組むこととなった．

当初，リスク因子の特定は，チェックシートを用いたヒアリングおよびその結果を基にしたブレーンストーミングのみの予定であったが，ここでは，それに加えて HHM 法による試行を実施した．この際，理想的にはそれぞれ別のサンプルグループを用意し，並行に実施して比較することが望ましいが，対象組織の人数等の問題もあったため，HHM 法による試行を本来のチェックシートベースの作業から 1 週間先行して行うことにより，同一内容の繰り返しによる影響を，HHM 法への適用結果からは可能な限り排除できるように配慮した．

図 3 は，この HHM 法によるアプローチを現場で実際に試行した際に得られた成果物のうち，最初に作成されたベースモデルと，それに対する再検討後の修正モデルである．

最初に作成したモデルでは，サブトピックの数を無理やり 5 件にまとめるなど，やや形式にこだわり過ぎている部分がある．内容的にも重複する部分や，異なるレベルのものが混在する等，未成熟な部分が多く見受けられた．そこでメンバーに対し，全体の形式やサブトピックの数にはこだわらず，自由な発想で，本当に必要な内容が盛り込まれるように考えて欲しい旨を補足した．さらに次のステップでは，必要に応じてサブトピックをヘッドトピックとした詳細展開を実施するので，同じ内容のものはまとめて重複は避けるように検討すること，および，最終ステップでは，各サブトピックを互いに組み合わせてリスクシナリオを考えることを踏ま

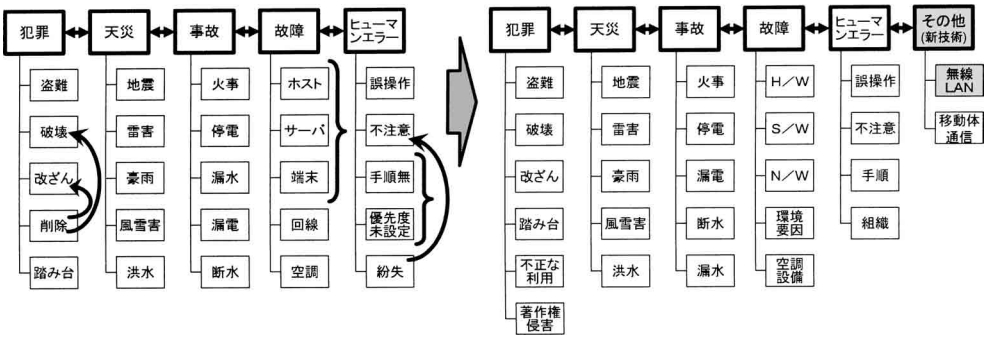

図 3. 議論を通した階層ホログラフィックモデルの洗練．

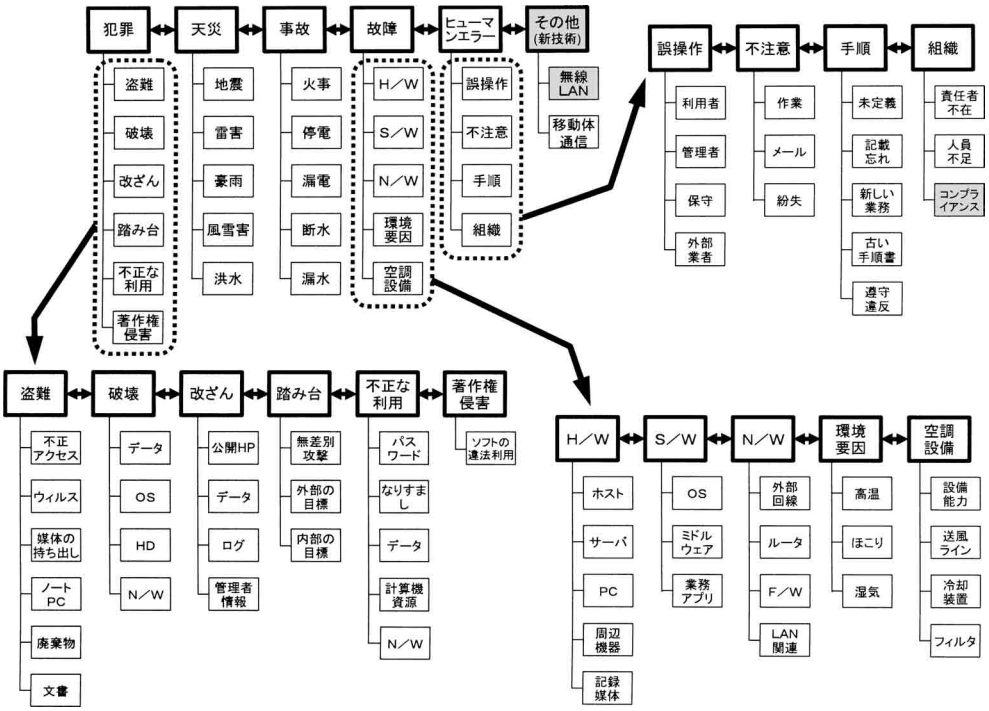

図 4.　階層ホログラフィックモデルの第 2 レベルへの詳細展開.

えて検討すると良いということを再説明した.

これを受け，このベースモデルを基に，さらに以下に抜粋したような議論が行われ，内容の重複や異なるレベルの混在などが整理された結果，修正モデルが作成されたのである.

- 「犯罪」の「削除」は「破壊」と「改ざん」のカテゴリーに含め，新たに 2 件を追加.
- 「故障」の分類は「ハードウェア(H/W)」,「ソフトウェア(S/W)」,「ネットワーク関連(N/W)」，それと「環境要因」,「空調設備」にする.
- 「ヒューマンエラー」の「紛失」を「不注意」に入れ，新たに「組織」起因を追加.
- その他のものとして「無線 LAN」等を追加．これは後に「新技術」とすることになった.

こうして完成した修正モデルであるが，その内容を見ると，例えば「天災」や「事故」などに関しては，かなり具体的なのに対し,「犯罪」,「故障」,「ヒューマンエラー」などについては，まだ分解が可能である．そこで以下のように，第 2 レベルへの詳細展開を行うことになった.
図 4 に，これらの検討結果から得られた第 2 レベルへの詳細展開の内容を示す.

以下に，この検討の過程で実際に行われた議論の一部を抜粋しておく.

＜「犯罪」に関する詳細展開における議論＞

- 「盗難」について，最近話題となっている「ノート PC」の盗難や「廃棄」PC からの情報漏えいという視点を付け加えるべき.
- 「破壊」については，対象についてまとめると，横展開も出来てよさそうである.
- 「改ざん」に関し,「ログ」や「管理者情報」の改ざんという内容を追加すべき.

＜「故障」に関する詳細展開における議論＞
- 「H/W」については，やはり対象についてまとめると，横展開も出来てよさそうである．
- 「環境要因」の中でも「高温」と「ほこり」による故障は非常に多い．

＜「ヒューマンエラー」に関する詳細展開における議論＞
- 「誤操作」については，誰が，何故，と考えて設定する方が分かりやすい．
- 「手順」が無いために起こるエラーは多い．その理由についてしっかり掘り下げるべき．
- 「組織」に関しては，各種ケースにもあるように「コンプライアンス」という観点を絶対に忘れてはならない．→ この議論を通して，“外部事例” という視点が重要であるという認識が醸成されたという点は特筆しておきたい．

こうして作成されたモデルをもとに，次ステップとしてリスクシナリオの抽出作業を行った．これまでの作業で情報の共有が出来ていたこともあってスムーズに進み，まず初めは具体的な事例から開始して，次第にモデル上の各アイテムの内容を相互に関連させながら（例えば図 4 右下の「H/W」の「サーバ」と「環境要因」の「高温」といった異なるリスクアイテム同士の関連付けから，「高温環境でサーバが暴走し，システムが停止する」というリスクシナリオが生成されるなど），結果としてかなり深いレベルまで議論を進めることが出来た．

こうして，HHM 法を用いた 3 日間にわたる作業の結果，合計で 141 件のリスクシナリオの抽出を行うことに成功した．以下に，その中から特徴的なものを抜粋しておく．

- 高速プリンタ装置の故障で，業務に深刻な影響が出る．
- 保管用 MT のリードエラーで，バックアップデータが消失する．
- OS のバグで例外処理が異常終了し，業務に影響が出る．
- 修正パッチのバグで，システムが停止する．
- 空調の給水管破裂による浸水で，設備にトラブルが生じる．

これら抽出されたリスクシナリオを見ると，参加メンバーそれぞれの実際の業務における経験や知識に基づいた内容が色濃く反映されたものとなっている．こうした内容は，その業務に関する実体験が無いと決して抽出されないものであり，このことから HHM 法によって良い形で情報が引き出されているということが分かる．しかも HHM 法の特性上，これらの情報は参加メンバーによる自発的な思考と積極的な行動の結果として提示されるものである．

このような環境でメンバーの参加度は高まる傾向があり，当然その結果として，作業の過程で得られる情報も，参加者間において強い印象を持つ形で共有されることが観察された．

一方，例えば以下のリスクシナリオに見られるように，特定のリスクアイテムに対する単一の視点による結果ではなく，複数のリスクアイテムとの関係性の中から抽出された，あるいは周辺のリスクアイテムの内容にインスパイアされたものが多く見られるという点も重要である．

- 火を消すための放水により，設備等が被害を受ける．
- 高温環境でサーバが暴走し，システムが停止する．
- 湿気とほこりでクラッキング現象が発生し，火災になる．
- 回線業者の保守時の誤切断により，バックボーン回線が断線．
- 移動体通信の使用により，正規ルートを経由しない外部との接続が可能となり，ウィルス等の脅威にさらされる．

これらのことは，HHM 法の適用によって特定の内容に固定されることなく，非常に柔軟で，かつ幅広い視点からの自由な議論が行われていることを示すものである．

さて，正規の手順によるチェックリストベースの作業によって得られたリスクアイテムと，

HHM 法によって得られた結果との比較結果からは,「盗聴」や「爆発物」,「煙」,「振動」などのように，チェックシートには含まれているが，HHM 法によるアプローチの中では出て来なかった項目もあるが，その一方で「無線 LAN」や「コンプライアンス違反」のように，HHM 法の試行により，通常の方法では抽出されなかったであろうと考えられるリスクアイテムが，少なくとも 2 件追加されていた．当初の目的としていた網羅性という点ではやや不十分な部分もあるが，リスクの対象範囲を拡大し得るという点では一定の効果はあることは確認できた．

このように一連の結果を見ると，今回は時間や準備が十分ではなかったこともあり，網羅性という点では必ずしも十分とは言えない部分もある．ただし，固定化されたチェックシートの枠組みを超えて，2 件とはいえリスクアセスメントの抽出対象を拡大しうるということが確認されたということは重要である．少なくともこの点だけでも，間違いなく HHM 法を適用する意味はあり，例えば詳細リスク分析などの実施手法として，期待できそうである．

ただし，対象範囲が広いと，実施に非常に大きな手間を要することも判明した．すなわち，通常のリスクアセスメントで本手法を適用するには，時間という要素が最大のネックとなる．

情報セキュリティポリシーの構築時，まず最初のステップでは，完璧なものを作るよりも，むしろ出来るだけ短期間で組織のレベルアップを果たすことこそが，より重要となる．従って，この段階におけるリスクアセスメントでは，効率性という点だけを見る限り，従来のチェックリストベースのアプローチの方が優位となる．試行後のアンケートで，時間が掛かりすぎるというものがあったが，そうした参加者の気持ちが大きく反映されている．

ただしこのことは，HHM 法の適用自体を否定するものではない．むしろ今回の結果からは，実務的な実施を考慮するならば，チェックシートベースでの従来の手法に対し，補完的に HHM 法を用いるやり方が，最も有効な結果をもたらすであろうと想定される．

ちなみに上記の試行後のアンケートでは， HHM 法に関して良くないと感じられた点として

- ともかく実施に時間がかかりすぎるように思われる．
- 全般的な内容だと範囲が広すぎて戸惑う．もっと狭い範囲に絞った方が議論しやすい．

という意見がある一方で，HHM 法の良い点として，

- 階層ホログラフィックモデルを見ながら議論をすると，リスク同士の関係や他の参加者の言いたいこととかが分かってくる．
- 意見が出しやすい．
- 体系的に考えられるので，セキュリティを行う目的や対策の位置付けとかがよく分かる．

という結果が得られている．この結果からも見て取れるが，階層ホログラフィックモデルは，参加者間のコミュニケーションのための共通言語としての役割を果たしている．そして，従来の単なるブレーンストーミングなどとは異なり，議論が拡散し難いという効果も観察された．

なお，HHM 法では対象範囲が狭いほど参加者の経験が活きてきて，有効な議論が行われるという傾向が見受けられる．また，実施の過程において高い教育的効果が得られるという点にも大いに着目すべきであると考える．

4.2　2 回目の試行における観察内容とその評価

現場において HHM 法を効果的かつ円滑に適用できるようにするため，1 回目の試行で得られた知見を活かし，実施方法について何点かの改善を加えることとした．

従来の HHM 法の適用では，通常，参加者はホワイトボードなどにダイアグラムの枠を描き，議論を行いながらそこに直接，各ヘッドトピックやサブトピックの内容を書き加え，また必要に応じて修正していた．このように，ホワイトボード等を作業用の媒体として用いると，

表1. 追加オプションにより機能向上を図った場合の使用媒体間の比較結果.

	内容の見易さ	更新の容易さ	結果の保存	参加者積極性	参加可能者	場所等の制限	備考（留意点）
ホワイトボード	○	○	×	○	大	有	設置の有無
大判の紙媒体＋ポストイットカード	○	○	○	○	大	無	
ノートパソコン＋プロジェクター	○	○	○	×	大	有	電源および装置の確保

i. **内容が見やすく，情報共有も行いやすい.**
ii. **内容の修正や追加が簡単に行える.**
iii. **図を大きく描くことにより，大人数でも参加可能.**

などの利点があるが，実際には，総ての場所にホワイトボードが設置されているわけではない.この結果，作業場所や時間帯が限定されてしまうなどの問題も発生した．また，通常のタイプでは結果の出力や保存は行えないため，作業の節目などでいちいち結果を書き写したり，デジタルカメラで画像に撮る等の手間が必要となり，特に複数日に渡って作業を継続的に行わなければならないような場合に，元と同じ状態に戻すために大きな手間が掛かっていた.

代替可能な媒体として大判の紙媒体やノートパソコンの使用が考えられたが，紙媒体は内容の追加・更新に難があり，またノートパソコンでは，実際に作業を行う際，画面や入力の制約から，参加者の積極性が大きく損なわれるということが観察された．このように機能面で見るといずれも一長一短であり，そのまま単独でホワイトボードを代替し得るものでは無かった.

一方，ブレーンストーミングなどに比べるとかなり改善されたとはいえ，HHM法でも，例えば消極的な性格の参加者などについては，必要な意見が提示されないという事態が起こり得た.

もちろん，こうしたことは各個人の性格に起因するものである．したがって，やはり何らかの“仕組み”として組み込む必要があるということは明らかであった．そこで，ここでは実務ケース研修などで一般的に採用されている手法を基に，以下のような改善を試みることとした.

A. **個人ワーク：各テーマについて個人で考える時間をとり，検討の結果をポストイットカードに記入させる.**
B. **グループワーク：各個人の記入したカードを集め，それらを用いて，KJ法ライクな進め方で議論を行っていく.**

この結果，言葉で意見を表現したり提示するのが不得手な参加者からも，必要な意見を吸い上げることができるとともに，また結果を整理する際にも，体系的に取り組むことが可能となる.

さらに，何度でも着脱可能なポストイットカードの使用により，応用の可能性が広がることが判明した．すなわち上記において，大判の紙媒体を使用する上で最大のネックとなっていた内容の追加・更新の問題が解決され，表1に示すようにこの組み合わせが優位となる.

ここではノートパソコンにプロジェクターを併用する案も検討したが，一連の流れとして全員参加で作業できる紙媒体と比較すると，操作者が特定されるデメリットは大きい．高価な装置を占有するという欠点もあり，やはり紙媒体を使うことが適当との結論に達した．さらにハンドリング性も考慮して，A3用紙にHHMダイアグラムをプレ印刷したものを用いることとした.

さて，2回目の試行は，B社の情報セキュリティポリシーの運用に伴う見直し作業への適用という形で，運用管理の部署を対象として「現場での情報漏えい」をテーマに実施した.

まず，HHM法の概要とそれを用いたリスク特定方法についての簡単なレクチャーの後，A3

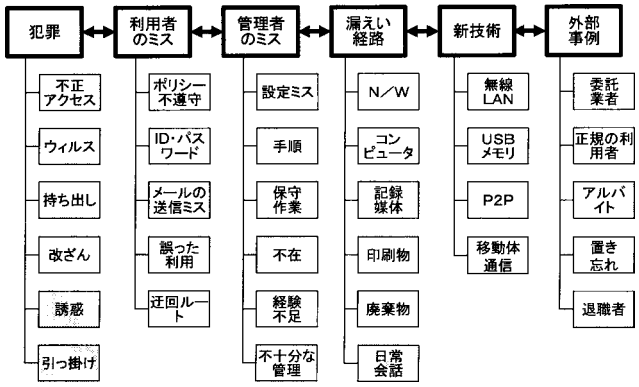

図 5.　内部からの情報漏えいに焦点を当てた階層ホログラフィックモデル.

の用紙に印刷した HHM 作業シートを提示し，ここではどこでも簡単に実施できるようにこの作業シートを用意した旨，ポストイットカード使用の利点と合わせて説明し，作業に入った．まず，話し合いによって，前提となる条件が以下のように決定された．

(1) **部門の性格上，外部からのアタックよりも内部からの漏えいを中心に作成する．**
(2) **視点となるヘッドトピックとして，ここでは，「犯罪」，「利用者のミス」，「管理者のミス」，「漏えい経路」，および「新技術」と「外部事例」を設定する．**

実施前には，内容的に高度な部分もあるということで，現場レベルでの試行を危ぶむ意見もあったが，実際に行ってみるとスムーズに作業が進み，その結果，今回の見直しにおける主要テーマである「現場での情報漏えい」に関する議論を図 5 のように展開することができた．

最終的に，「現場での情報漏えい」に関して，合計で 68 件のリスクシナリオが抽出されている．

これらの内容から，例えば「誘惑」や「引っ掛け」など心理面にも配慮した検討が行われた一方，「迂回ルート」や「P2P」のように，現場における実情も良く反映されており，ほぼ期待通りの議論が実施されていることが見て取れる．

ちなみに「外部事例」に関しては，作業時には事件や組織の名称を挙げて作業を行ったが，ここでは分かりやすくするために，リスクアイテムとしてはその事件の性格，リスクシナリオには，そこから発展した議論の内容も含めて表記するようにしてまとめた．その結果，「退職者」に関する議論が特に活発に行われ，「P2P」などとともに，追加視点の有効性も確認された．

また，HHM 法の効率的適用を目的とした各種改善策に関して，現場の反応は概ね好評であったが，アンケートでは，ポストイットによって意見が出しやすくなり，議論もそれを見ながら円滑に行えたという意見が多い一方，使用した A3 の作業用シートの大きさや，机に置いた時の作業者との位置関係などについての指摘もあり，細かい部分では改善の余地も残った．

今回は対象部門の参加者が少なかったこと，また，現場におけるグループ単位での適用では，通常，同様に少人数となる場合が多いとの想定から，ここではハンドリングの性能や準備のしやすさを第一に，A3 サイズのシートを用いることとした．だが，やはり実際に使ってみると，やや小さめという印象が強かったと思われる．ただし，作業用シートを使う時の作業者の向きなどについては，事前の段階ではまったく想定していなかったことも事実である．今後の課題として，そのような観点からの検討内容も併せて整理し，実施時におけるファシリテーターズ・マニュアルのようなものを作成しておくと役に立つのではないかと考えている．

なお今回の試行では，情報セキュリティポリシーの現場での運用に伴う作業において，内部からの情報漏えいに焦点を当てるというように，情報対象範囲を限定した形でHHM法を適用したわけだが，既に述べたように，これ自体についてはスムーズで活発な議論が行われており，やはり参加者の現場での経験や，業務における実情などが反映された非常に良好な結果が得られている．また，この過程で基本視点の提示による作業の効率化や，2つの追加視点(「新技術」と「外部事例」)に関する有効性についても確認することができた．

ただし，その結果を詳細にチェックすると，例えば図5などでも，内容的に荒削りな部分があることも事実である．ただし，できるだけ現場の自主運営に任せることによって効果を高めたいという意図もあるため，どのように実施していくのが良いかは，今後の課題となろう．

例えば基本視点や，そこから展開されるサブトピックについてもセットとして提供することにより，ある程度まではその後の議論をコントロールできるようにしておくべきかもしれない．全部の情報を提示するわけではないので，自由な議論が行われる余地は残せるが，制限されてしまう可能性もあり，これについても今後の課題の一つとして検討していきたい．

5. 解析・評価への応用イメージ例

前章までは主としてHHM法を用いたリスク因子の特定プロセスの改善について述べてきた．そこで作られた構造モデルは，リスク分析や評価を論理的に実施するための根拠となるものであるが，これまでの説明だけでは，具体的な解析・評価への応用についてのイメージはつかみにくいと思われる．そこで，ここでは4.2章で得られた構造モデルを用いた解析例を示す．

5.1 リスクランキングとフィルタリング法(RRF法)

これまで見てきたように，組織にはさまざまな種類のリスクが複合的に存在している．それぞれ，その特性や仕組みが大きく異なっており，すべてを同一の基準で評価することは事実上不可能である．また，そうした一元的な評価は意味が無いことについても既に述べた．

ここで必要となるのは，リスクマネジメントのスコープ，組織構造，意思決定者の権限などの観点から，優先的に対処すべきリスクシナリオのカテゴリーを選び，その上でリスクの優先順位付けを実現するということである．このための手法として，Haimes et al. (2002)が提唱している「リスクランキングとフィルタリング法(Risk Ranking and Filtering methodology／以下RRF法と略す)」が有効となってくる．

RRF法では特定されたそれぞれのリスクの組ごとに，必要なだけリスク評価のための基準を用意する．そして，特定したリスク全てについてリスクを算定し，それぞれのリスク基準に照らし合わせ，新たに対策を実施すべきリスクを明らかにし，そしてリスクの優先順位を決めるというアプローチをとる．特にこの手法は，多くの種類のリスクを含む大規模なシステムの場合におけるリスクの絞込み等に大きな効果を発揮する．

RRF法の特徴をまとめると図6のようになる．ここに示されるように，“テレスコーピングフィルタ”と“順序付け”という2つのフェーズから構成される．

(1) 5つぐらいの総合的な評価基準を用いてリスクランキングを行う．
(2) 測定可能な代理属性を用いて，リスクシナリオ・リスクアイテムを定量的に評価する．
(3) リスク指紋図で，クリティカルリスクシナリオ・リスクアイテムを見分ける．
(4) テレスコーピングフィルタで，リスクシナリオ・リスクアイテムをトップnまで削減．
(5) 階層分析法(AHP)によって得られた加重スコアを用いることにより，トップnまでのリスクシナリオ・リスクアイテムの順序付けを支援する．

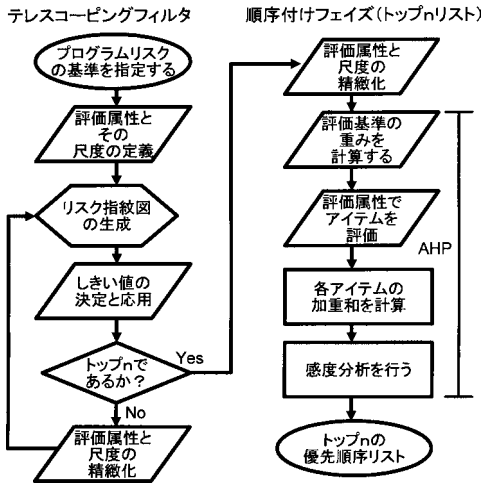

図 6.　RRF 法によるリスクの評価のフロチャート.

5.2　2 回目の試行結果に対する RRF 法の適用例

ここでは，適用時に白熱した議論が行われた「外部事例」を対象として，説明を行う.

なお，今回はあくまで説明のための参考イメージ例であるので，設定する評価基準は 4 個，各評価基準に対応する代理評価属性も 2 つにして，簡易的に実施することとする.

本来であれば各手段には有無のほかに難易度や費用も含まれ，もっと多い数の代理評価属性の定量的な数値を数理的に処理することによって評価基準の値を決定するが，ここではかなり簡便的なものとなっている.

i. **検出不能性**(Undetectability)**の視点 → きっかけを事前に発見することは可能か？**
   - **前兆情報(前兆となる事象はあるのか？　過去の事件データ等の蓄積度は？)**
   - **検出確認手段(事前に前兆を検出するための方法等は存在するのか？)**

ii. **制御不能性**(Uncontrollability)**の視点 → 被害を防止する手段は存在するのか？**
   - **モニタリング手段(状況をモニタリングするための方法等は存在するのか？)**
   - **防止手段(検知して緊急停止したり持ち出しを防止する方法等は存在するのか？)**

iii. **失敗への多数の経路**(Multiple paths to failure)**の視点 → 発生に至る経路が複数あるか？**
   - **経路の数(リスクの発生に至るルートの数は？　未知の方法が存在し得るか？)**
   - **迂回の容易さ(正規の方法をたやすく迂回する方法はあるのか？)**

iv. **撤回不能性**(Irreversibility)**の視点 → 発生前の状態に復旧できない可能性は？**
   - **最悪トラブルの発生可能性(最悪のトラブルが起こり得る可能性は？)**
   - **最悪トラブルの結果(最悪のシナリオが発生した場合の影響の大きさは？)**

これをもとに作成した評価基準モデルが，図 7 である.

今回の対象となる「外部事例」に関するリスクシナリオは次の 9 件である.

＜委託業者＞

a. **保守委託業者によって，個人情報が漏えいする.**

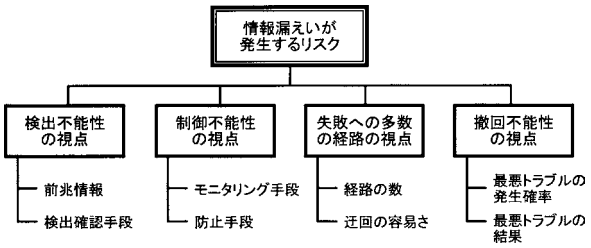

図 7. 話し合いによって作成した評価基準モデル.

表 2. 視点 ii の制御不能性に関する判断基準.

判断の根拠となる要素	重要度
モニタリングの実施レベル：低, 適用されている防止手段：無	5
モニタリングの実施レベル：低, 適用されている防止手段：有	4
モニタリングの実施レベル：中以下, 適用されている防止手段：無	3
モニタリングの実施レベル：中以下, 適用されている防止手段：有	2
モニタリングの実施レベル：高	1

b. **開発委託業者の不注意によって，情報が漏えいする.**

＜正規の利用者＞

c. **正規の利用者によって，個人情報が持ち出される.**

d. **興味本位の閲覧により，個人情報が漏えいする.**

＜アルバイト＞

e. **アルバイトの人間によって，個人情報が持ち出される.**

＜置き忘れ＞

f. **外出先で置き忘れたノートパソコンから，情報が漏えいする.**

＜退職者＞

g. **退職者により，情報が持ち出される.**

h. **退職者の嫌がらせにより，情報の改ざんが行われる.**

i. **退職者により，組織の脆弱性の情報が漏えいし，不正アクセスが発生する.**

これら各リスクシナリオについて定性的または定量的に評価するため，図 7 の評価基準モデルをベースに，例えば表 2 に示すような個別に設定された判断基準をもとにした関係者間の話し合いによって，それぞれ点数付けを行う.

この結果をもとに作成したリスク指紋図の例を図 8 に示す.

次に，これらの 9 件のリスクシナリオをトップ 4 まで削減するための方法として，ここでは，各評価基準に対応する重要度の平均値をそれぞれ計算したものをしきい値とし，図 8 右に示す様なしきい値指紋図を作成して使用するという方法を用いる.

ここで，しきい値指紋図によってテレスコーピングフィルタ処理を行うと，まず b のシナリオのみがリストから除かれる．だが，まだ数が多いので，しきい値を再計算して同様の処理を 2 回繰り返すことにより，さらに a，e，f，g の 4 つがリストから除かれ，最終的に表 3 に示すようなトップ 4 のリスクシナリオが求められる.

RRF **法の次のフェーズは順序付けフェーズである．ここではまず，各評価基準の値を個別に見て比較する．その結果，リスクシナリオ** c **はすべての値が** d **と等しいまたは大きく，これ**

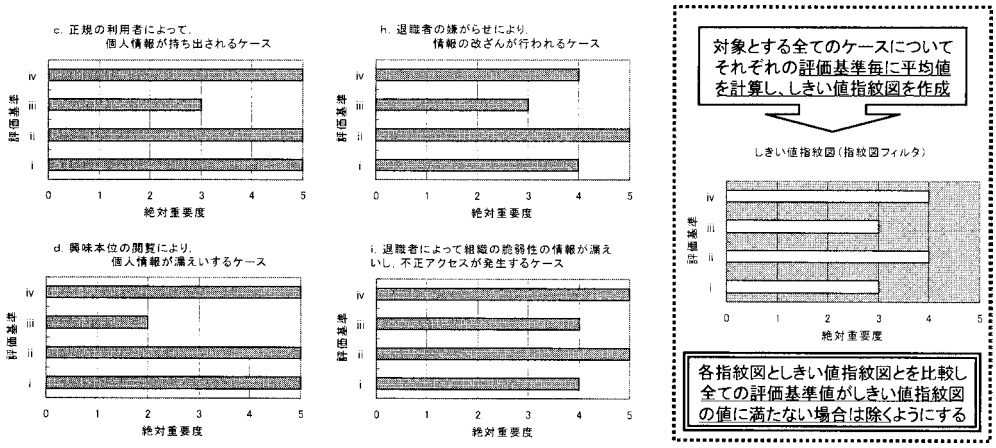

図 8.　リスクシナリオに関する指紋図としきい値指紋図の例.

表 3.　求められたトップ 4 リスクシナリオの内容.

リスクシナリオ	i	ii	iii	iv
c．正規の利用者によって，個人情報が持ち出される	5 点	5 点	3 点	5 点
d．興味本位の閲覧により，個人情報が漏えいする	5 点	5 点	2 点	5 点
h．退職者の嫌がらせにより，情報の改ざんが行われる	4 点	5 点	3 点	4 点
i．退職者による脆弱性情報の漏えいで，不正アクセスが発生	4 点	5 点	4 点	5 点

表 4.　求められた一対比較行列.

	i．検出不能性	ii．制御不能性	iii．多数の経路	iv．撤回不能性
i．検出不能性	1	3	5	1/3
ii．制御不能性	1/3	1	3	1/5
iii．多数の経路	1/5	1/3	1	1/7
iv．撤回不能性	3	5	7	1

よりcの方がdよりもランクが高いということが分かる．同様に，リスクシナリオcはhよりもランクが高く，またiもhよりランクが高いことが明らかである（すなわち，c＞d，c＞h，i＞hとなる）．しかしながらこの情報だけでは，d，h，iの順序関係までは決められないため，これらの間でAHPによるランク付け処理を実施する．

そこで，ここではまず実施時の参加者との話し合いによって，各評価基準間でどちらの影響がより重要であるかについての一対比較を行い，表4のような一対比較行列を求めている．

これより各評価基準の重み付けを決定するために，まず各行の要素の積を計算し，その値のn-th rootを求めて正規化した結果，それぞれの重みはiが0.263，iiが0.118，iiiが0.055，ivが0.564となる．すなわちここでは，ivの撤回不能性の影響が最も大きく，iiiの失敗への多数の経路の影響が最も小さいという結果が得られる．

最後に，以上のようにして求められた各評価基準の重みと，各リスクシナリオの指紋図とを用いて順序付けを行う．具体的には，以下のように各カテゴリーから見たそれぞれの重要度に，各評価基準の重みを掛けて，その加重和を求めている（図9）．

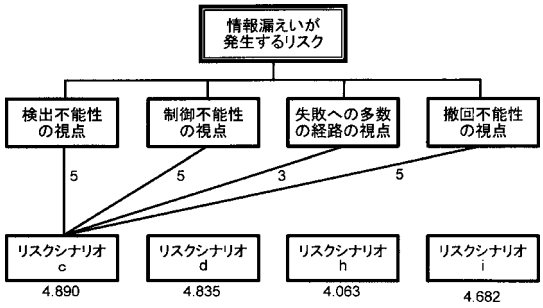

図 9. 加重和の計算例（リスクシナリオ c の場合）.

リスクシナリオ c：$5 \times 0.263 + 5 \times 0.118 + 3 \times 0.055 + 5 \times 0.564 = 4.890$
リスクシナリオ d：$5 \times 0.263 + 5 \times 0.118 + 2 \times 0.055 + 5 \times 0.564 = 4.835$
リスクシナリオ h：$4 \times 0.263 + 5 \times 0.118 + 3 \times 0.055 + 4 \times 0.564 = 4.063$
リスクシナリオ i：$4 \times 0.263 + 5 \times 0.118 + 4 \times 0.055 + 5 \times 0.564 = 4.682$

以上の計算から，これらのリスクシナリオ間の順序関係は c ＞ d ＞ i ＞ **h となることが分かる.**

6. おわりに

以上のように本試行によって，システムズアプローチによる方法論の適用が，まだ属人的な部分の多いリスクアセスメントプロセスの改善に役立つという知見を得るとともに，そこから得られる現実的な構造モデルは，解析・評価に役立ち，マネジメントレベルの向上に資するという確かな感触を得ることができた．これらは，大きな意義のあることだと考える.

何より，リスク因子の特定における HHM **法の適用を中心とする一連のアプローチは，従来のチェックシートとブレーンストーミングによる一般的な手法と比較して，議論への積極的な参加，多数の意見の提示，メンバー間の情報の共有，幅広い視点からの活発な議論が行われるなど，期待以上の効果が観察された．また，成果物についても新しいインシデントや，組織に固有の内容に関する洗い出しが良好に行われることを確認できた.**

また，特に注目すべきは，階層ホログラフィックモデルが参加者間のコミュニケーションのための，共通言語としての役割を果たすという副次効果についての観察結果である.

これは HHM **法の実施に伴って，その参加者に高い教育的効果が認められるという観察結果とともに非常に重要な知見として，今後に活かしていかなくてはならない内容である.**

これらの結果を受けて，現場において HHM **法を効率的に適用するための各種改善を加えた** 2 **回目の試行結果も改善策そのものは概ね好評であり，若干の改善の余地は残ったが，今後への展開についての自信を深めるものであった.**

ただし，実際の運用を考慮すると，現場のレベルに応じて実施形態を変えるというのが望ましい形であり，段階的にステップアップを図るべきであろうというのが現在の意見である.

なお， 5 **章では，この結果を解析・評価に応用させる場合のイメージとして，リスク評価における** RRF **法の適用イメージを示した．あくまで説明のための参考例であるため，本来の** RRF **法の定義から見ると，厳密な意味ではかなり簡易的な形での実施となっているが，複数の代理評価属性を考慮した評価基準の組み合わせを用いて，指紋図を使用するテレスコーピングフィルタによる絞込みの実施と，トップ** 4 **シナリオに対する** AHP **による順序付けという一連の処**

理からは，現実的な構造モデルの持つ可能性をつかむのには十分役立つものと思われる．

ちなみに，代理評価属性を厳密に適用する場合は，その尺度定義や根拠となるデータをどのように決めるかについてということが重要なポイントとなる．この点については，HHM 法において，各ヘッドトピックに対応するサブトピックス群が，基本的に同一の評価属性によって扱うことが出来るという点にも着目して欲しい．

この点に関連して，将来的に，基本視点―基本リスクアイテム―基準代理評価属性の 3 つをセットとして用意することにより，さらなる改善を加えたいと考えているが，そのためには，さらに体系的な取り組みを行っていく必要があり，今後の展開における最重点課題としたい．

謝　辞

今回の試行に当たって多大なる御協力を賜りました，B 社の情報セキュリティポリシー導入プロジェクトの関係者各位に，この場をお借りして深謝申し上げます．

参 考 文 献

Haimes, Y. Y.（1998）．*Risk Modeling Assessment, and Management*，John Wiley and Sons, New York.

Haimes, Y. Y., Kaplan, S. and Lambert, J. H.（2002）．Risk filtering, and management frame work using hierarchical holographic modeling, *Risk Analysis*, **22**(2), 383–397.

Kaplan, S. and Garrick, B. J.（1981）．On the quantitative definition of risk, *Risk Analysis*, **1**(1), 11–27.

Kaplan, S., Haimes, Y. Y. and Garrick, B. J.（2001）．Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk, *Risk Analysis*, **21**(5), 807–819.

Lawrance, W. W.（1976）．*Of Acceptable Risk*, William Kaufmann, Inc., Los Altos, California.

日本規格協会（2003）．『JIS TR Q0008（ISO/IEC GUIDE73: 2002），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』，日本規格協会，東京．

Vose, David（2000）．*Risk Analysis*: *A Quantitative Guide*, 2nd ed., John Wiley and Sons, Chichester.

122 Proceedings of the Institute of Statistical Mathematics Vol. 54, No. 1, 105–122 (2006)

Improvement of Risk Assessment Process through Hierarchical Holographic Modeling Method —A Practice in IT-security Policy Construction Project—

Toshikazu Shimodaira[1] and Hua Xu[2]

[1]Interdisciplinary Graduate School of Science and Engineering, Tokyo Institute of Technology
[2]Graduate School of Business Sciences, University of Tsukuba

Risk management has traditionally been performed for a special field of business through a specified method to the field. Moreover, performance of risk management depends very much on the people involved in the program. In order to overcome these drawbacks, we introduce a holistic approach called the Hierarchical Holographic Modeling (HHM) method to the risk assessment process. This method is a comprehensively recognized method for the identification of risk scenarios of a complex large-scale system.

In this paper, the HHM method is applied to a practical IT-system security management project, and a systematic procedure is proposed for the risk assessment process. As a result, HHM structural models are constructed, and a number of risk scenarios in the IT-system security problem are identified. The analytic aspects of the risk scenarios are also studied by using a risk ranking and filtering (RRF) method. Moreover, several issues in the application of the HHM method are discussed, and a series of measures are proposed that are believed to be useful for the effective use of the HHM method in the risk assessment process.

Key words: Risk assessment, Hierarchical Holographic Modeling, IT-system security.