「マルチメディア，分散，協調とモバイル
(DICOMO2014)シンポジウム」 平成26年7月

IT リスクの動的特性を考慮した対策案組み合わせ最適化技術の提案

梅原悠平[†1]　安藤駿[†2]　佐々木良一[†3]

ＩＴリスクには，一つのリスクに対する対策が，別のリスクを生み出す多重リスクという問題がある．この問題を解決するために佐々木らが多重リスクコミュニケータ（以下，MRC）を開発した．MRC は，複雑化するリスクへの対応を定式化し，関与者間での合意形成を支援するシステムである．しかし，問題の解決には多重リスクの回避だけではなく，動的に変化する状況にも対応する必要がある．本稿で言う動的な変化とは対策を取ることによる相手の対応の変化である．対策の条件が厳しければ，対策に対する反発が大きくなり，リスクの上昇を招く可能性がある．よって，相手の動的な変化を考慮すべきだと考え，ＩＴリスクの動的特性を考慮した対策案組み合わせ最適化技術を開発した．本稿では特に攻撃者の「技術力」と「反発心」が重要だと考え，それらの特性の動的変化を考慮した上で定式化し解を求めた．この結果，従来の演算と今回提案した演算で取るべき対応が変わることなどが明らかになった．従来の演算と，今回提案した手法を用いた演算を行った場合では，対策を取った事によって変化するリスクに対応をした分，対策案の選定が状況に適したものとなったと考えられる．

The proposal of combinatorial optimization technology in consideration of dynamic characteristic of IT Risk.

YUHEI UMEHARA[†1]　HAYAKI ANDO[†2]　RYOICHI SASAKI[†3]

1. はじめに

近年，ＩＴシステムへの依存度の増大に伴い，セキュリティ意識が変化している． 従来のセキュリティでは，意図的な不正を防ぐことを目的としていたが，広義のセキュリティでは天災や故障・ヒューマンエラーといった原因にも対応ができる形に変化している．このような広義のセキュリティのことを著者らはＩＴリスクとして扱ってきた．ＩＴリスクには，一つのリスクに対する対策が，別のリスクを生み出す多重リスクという問題がある．例として，企業の情報漏えい問題を挙げると，情報漏えいを防ぐためにメールの監視をした場合，それは従業員のプライバシーの侵害となることが考えられる．これらの問題を解決するために佐々木らが多重リスクコミュニケータ（以下，MRC）を開発した[1]．MRC は，複雑化するリスクへの対応を最適化問題として定式化し，関与者間での合意形成を支援するシステムである．

従来の MRC は多重リスクを考慮しつつ対策案を選定することに対して秀でたものである．しかし，MRC の適用を重ねたことによって，次の２つの点を考慮することで MRC がより効果的になることがわかった．１つ目は「攻撃者の特性によるリスクの変化」で，２つ目は「対策指示内容による影響」である．

１つ目の「攻撃者の特性によるリスクの変化」とは，攻撃者が攻撃をどれだけ試みるのか，どれだけ攻撃を成功させるのかによってリスクが変化するということである．

２つ目の「対策指示内容による影響」とは，対策による対策関連者（対策を指示されてそれによって行動する者）の負担を考えるということである．例えば，情報漏洩対策のために内部の社員に向けて，ある対策を指示した場合に，対策関連者がその対策に対して大きな負担を感じれば，対策に反発をする可能性がある．反発することで対策を無視したりした場合は，対策に期待している効果が得られなく，結果的にリスクが上昇してしまう．これでは，対策として十分なものにはならない．つまり，対策指示による対策関連者の動向も加味した上で対策を決定する必要がある．

本研究では，上記の２つの点を考慮して反発心と技術力という要素に注目して攻撃者をパターン化する．対策の組み合わせによって対策関連者が負担を感じた場合，そのパターンの比率が変化するだろうという仮定の下で対策案選定方式を提案する．これにより，従来の MRC での対策案選定よりも，現実的で効果的な対策案群を選定することが可能となる．

本稿では，ＩＴリスクの動的特性を考慮した対策案組み合わせ最適化技術の提案をする．

†1 東京電機大学大学院
†2 東京電機大学大学院（現在，日本情報通信株式会社）
†3 東京電機大学　教授

2. 多重リスクコミュニケータ(MRC)

先行研究の多重リスクコミュニケータ（以下，MRC）について紹介する．MRC は，複数の意思決定関与者の合意形成を支援するために，目的関数や制約条件などの評価指標を考慮し，最適化問題として定式化し，対策案の最適な組合せを求める機能をもつ. MRC はこれまで個人情報漏洩問題や内部統制問題に適用されてきた[2].

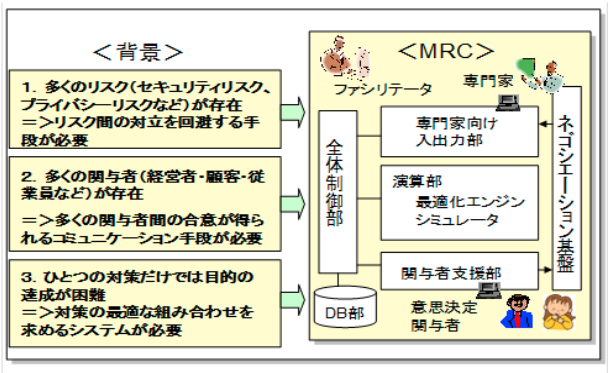

図１．　MRC 概要
Figure1.　Overview of　MRC

2. 1　MRC の目的

MRC が開発された背景と目的は以下の通りである．
（１）多くのリスク（セキュリティリスク，プライバシーリスクなど）が存在する．したがって，リスク間の対立を回避する手段が必要となる．
（２）多くの関与者（経営者・顧客・従業員など）が存在する．したがって，多くの関与者間の合意が得られるリスクコミュニケーション手段が必要となる．
（３）ひとつの対策だけでは目的の達成が困難である．したがって，対策の最適な組み合わせを求めるシステムが必要となる．

2. 2　MRC の評価指標

MRC は, 複数の意思決定関与者の合意形成を支援するために，下記に示すような評価指標を考慮しつつ，対策案の最適な組合せを求める機能を持つ．
（１）関与者
問題に関与する人たちのことを指す
（２）目的関数
最適な対策案を決定するために用いられる関数
（３）制約条件
組合せの中から，許容できるものを決定するための条件
（４）対策案
問題に対して考えられる対策
（５）リスク分析
MRC ではフォルトツリー分析法（以下，ＦＴ分析）でリスク分析が行われている．ＦＴ分析とは，頂上事象に好ましくない事象を置き，頂上事象から下位事象に向けて問題を展開し，その末端事象の発生確率を基に，頂上事象のリスクを求めるというものである．

2. 3　MRC の構成

MRC の構成は以下の通りである．
・専門家向け入出力部
専門家が，目的関数，制約条件式，対策案，係数，制約条件値を MRC プログラムに与えることを支援する．
・演算部
最適化エンジンとシミュレータより構成されている．最適化エンジンでは，組み合わせ最適化問題として定式化された問題の第 1 最適解から第 N 最適解を求める．シミュレータは最適解を求めた後，時間経過後の影響や地域的な変化などを意思決定者などに表示するために用いる．
・関与者支援部
意思決定関与者の合意形成のために必要なわかりやすく表現するためのものである．
・全体制御部
プログラム全体を制御する．
・データベース部
定式化結果や求解結果，関与者の意見などをデータベースとして整備し，必要に応じて取り出せるようになっている．
・ネゴシエーション基盤
各関与者が「制約条件値が違う」,「別の対策案がある」などの意見を言うと，この結果はこの部分を通して専門家に伝えられ，専門家によって変更された入力が MRC に与えられ，その結果が再表示される．
この MRC の利用者としては，専門家，複数の意思決定関与者，ファシリテータなどがいる．専門家は MRC を扱う人のこと指し，ファシリテータは議論の進行を補助する人のことである．

3. MRC の問題

従来の MRC は，組織内の多重リスクを回避しながら対策案を選定するということに焦点を当てたものである．したがって, 計画段階の多重リスク回避としては十分である．しかし，MRC の適用を重ねた事で，有効な対策案選定のためには，２つの問題が存在することが分かった．
（１）攻撃者の特性によるリスクの変化
（２）対策指示内容による影響
という問題である．このままでは，運用時を想定した場合に現実的で効果的な対策案選定が難しい．

3.1 攻撃者の特性によるリスクの変化

MRC ではリスク分析手法として, ＦＴ分析を用いている．著者らはＦＴ分析によるリスク分析でリスクに一種の傾向を発見した．それは，攻撃者の脅威に関するリスクに対してＦＴ分析を行い論理展開すると，末端事象が「攻撃を試みる確率」と「攻撃に成功する確率」の AND 演算であるという傾向である（図２）．攻撃者の特性によって問題を試みる確率や問題発生に成功する確率には差がある. つまり，同じ頂上事象であっても攻撃者が存在する場合はその頂上事象の発生確率は攻撃者によって変化するということである．従来の MRC ではその変化に対応をしていない．

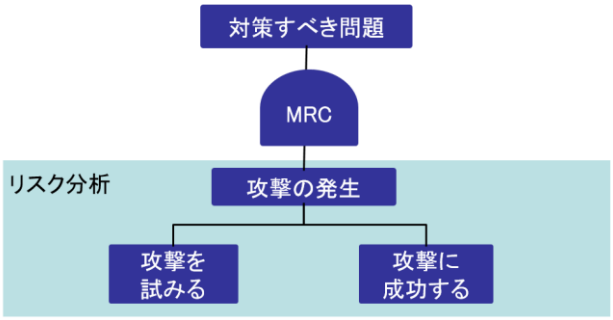

図２．リスク分析の傾向

Figure2.　Trend of risk analysis

3.2　対策指示内容による影響

対策を指示する事によって生じる影響も考慮しなければならないことが分かった．従来の MRC で選ばれる対策案は，対策による対策関連者への負担を考えていなかった．対策の負担によって対策関連者が反発心を持つと問題がある．対策と反発に関する問題の事例を挙げると，フランスでサルコジ大統領の経済政策に対して国中の労働組合が抗議を行い，全国規模のゼネラル・ストライキが発生するという事件があった．

このように，対策関連者は対策をただ受け入れるわけではない．対策の組み合わせによっては対策を負担に感じて，反抗する者を生み出す可能性がある．負担によって対策が受け入れられないと，期待していた対策の効果が得られない．従来の MRC では，このような対策指示による影響を考慮して選定されていない．

4.　MRC の要件

３章における問題点を踏まえた上で MRC に与えられる要件は以下の２つである．

（１）攻撃者の特性によるリスクの変化への対応

（２）対策指示内容による影響を考慮

これらの要件を考慮した分析を MRC で行うことで，より MRC を効果的なものにする必要がある．

4.1　攻撃者特性によるリスクの変化への対応

3.1 節で攻撃者が存在する場合は攻撃者によってリスクに変化があることを説明した．したがって，どのような攻撃者がどの程度の割合で存在するのか考慮することでこの問題を解決しようと考えた．しかし，攻撃者の性格や感情，行動パターンなどの特性と程度の組み合わせは多岐にわたる．

そこで，攻撃者の特性と程度を２つずつに絞り４つのパターンで攻撃者を分類し，そのパターンの比率によってリスクの変化に対応させることにした．先に説明した通り，攻撃者の特性によって実際に影響があるのはリスクの末端事象である「攻撃を試みる確率」と「攻撃に成功する確率」となる．したがって，これらに影響を与えるであろう特性を選ぶ．

本稿では，その特性を反発心と技術力とした（図３）．その理由は，反発心のある者と反発心のない者では，攻撃を試みる回数に変化があるためである．IPA の報告で，社内への不満が情報漏洩確率を上昇させるという問題があることが示されている[7]．このように，内部への反発心があれば内部者が内部犯罪者になるリスクが存在し，攻撃に試みる回数が上昇する．また，技術力のある者と技術力のない者では，攻撃の成功確率が変化する．これは，素人などの愉快犯から営利目的のプロ集団まで攻撃者が幅広く存在していることを考慮すると技術力の程度にバラつきがあり，それによって攻撃の成功確率が変化することが推測できる．よって，「反発心が有るか無いか」，「技術力が有るか無いか」の組み合わせで攻撃者をパターン化してその比率を基に分析を行う．

4.2　対策指示内容による影響を考慮

3.2 節で対策指示による影響を考慮した分析を行わなければならないことを説明した．対策の組み合わせが仮決定した後，対策全体として負担度がどの程度あるのかを決定する．その負担度を基にして対策関連者に反発がどのくらい存在するのか求めることで対策指示による影響を考慮することを考えた．そのために，負担度と反発の関係を対応表として作成する(図４)．その対応表から反発値を決定し，反発値を目的関数に反映することでリスクを決定する．負担度の値が閾値（図４のｂ１～ｂ５）を超えたり下回った場合は，その負担度に当てはまる反発値を目的関数に代入してリスクの再計算を行う．負担度の値が閾値をまたがらなければ，リスクの再計算の必要は無いので，そこで対策案の組み合わせを決定する．このように，目的関数に反発の値を反映させることで，対策指示による影響を考慮する．実際に反発を加味したシミュレーションを行うことで，運用時の効果がどの程度あるのかを把握することが出来る．

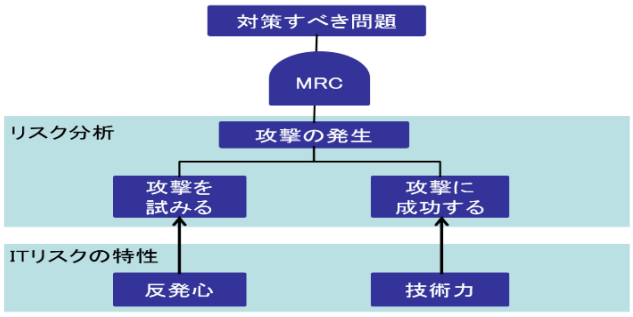

図３．　リスク分析の傾向と特性

Figure3.　Trend of risk analysis and dynamic characteristics

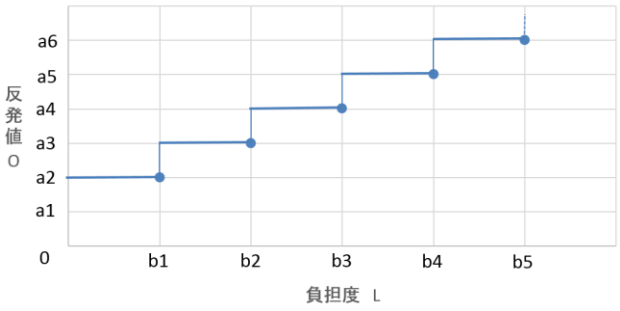

図４．　負担度と反発値の対応

Figure4.　Relationship between burden and opposition

5. 提案方式

従来の MRC の適用手順に，ＩＴリスクの動的な特性を考慮させ，対策を取る事による運用時の対策関連者の反応を考慮させる．図６の③～⑨の項目においてＩＴリスクの特性を考慮した分析を反映させ，⑤の「パターン化，分布」，⑥の「対応表の決定」という項目と⑬の「負担度，反発値の決定」を新たに加え，MRC の新たな分析方式を提案する．

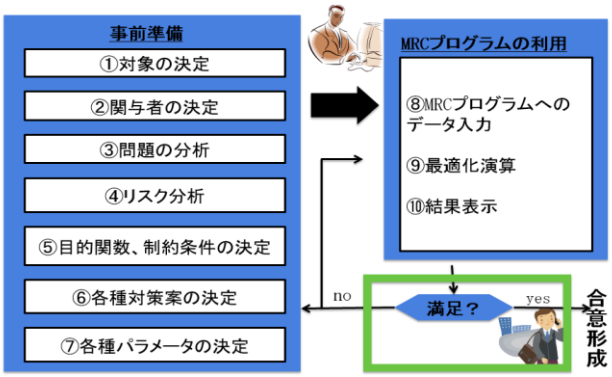

図５．　従来の MRC 適用手順

Figure5.　Application flow of conventional MRC

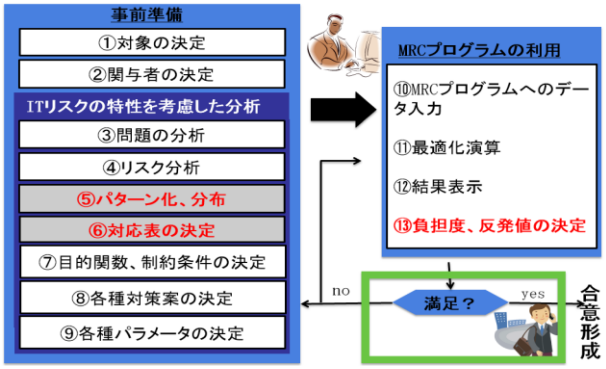

図６．　提案する MRC 適用手順

Figure6.　Application flow of proposed MRC

（１）対象の決定
対象とする問題を決定する．
（２）関与者の決定
問題に関与する者を決定する．
（３）問題の分析
問題の発生経路を明確にする．
（４）リスク分析
パターン毎にＦＴ分析でリスク分析を行う．図３から，パターンによって問題の発生確率が変化する．
（５）パターン化，分布
今回，要素は技術力と反発心である．選定したＩＴリスクの特性をそれぞれ特性の有無で４つのパターンに分類する（表１）．初期値となる分布はそれぞれのパターンの割合をアンケートやテストなどから求めて分布を決定する．
（６）対応表の決定
対策の負担度と反発値の関係を示す対応表を作成する．
（７）目的関数，制約条件の決定
目的関数と制約条件を決定する．目的関数に（４）で求めた分布を反映させる．
（８）各種対策案の決定
対策案を決定する．
（９）各種パラメータの決定
対策案の効果，制約条件の値などを決定する．
（１０）MRC プログラムへのデータ入力
事前準備で行った事項を MRC プログラムへ入力する．
（１１）最適化演算
事前準備で決定した条件で最適化問題として対策案の組み合わせを暫定的に決定する．
（１２）結果表示
対策案の組み合わせを表示する．
（１３）負担度，反発値の決定
最適化演算で得た対策案候補の負担度を求め，それを基にして対応表から反発値を決定する．負担度の求め方は，（負担度の合計）／（負担度を表す制約条件数）とする．閾値をまたがらなければ，合意形成の議論へ移る．閾値をまたがる場合は，その負担度に合った反発値を基に再度最適化演算を行う．
事前準備の後に，（１０）～（１３）の手順を合意形成するまで繰り返し，運用時を想定した対策案群を選定する．

表１．　パターン分類

Table 1.　Pattern Classification

	反発心あり	反発心なし
技術力あり	パターン１	パターン２
技術力なし	パターン３	パターン４

6. 提案方式を採用した MRC への適用

6.1 対象の決定

対象とする問題は，内部不正による情報漏えい問題を扱うことにした．内部が原因で起こる情報漏えいは被害が大きく，発生頻度が高いことが報告されている[6]．また，事前に個々のＩＴリスクの特性のパターンについて，入社時など定期的にアンケートやテストなどで調査を取る機会がある．この調査を基にして初期値となる分布を決定することが出来る．

6.2 関与者の決定

一般企業を想定し，関与者を決定した．関与者と関与者の主張をそれぞれ以下に示す．
（１）経営者
情報漏えい対策を促進し，情報漏えいの対策を優先するが，低コストで効果のある対策の組み合わせを希望する．
（２）従業員（対策関連者）
情報漏えい対策は，本来の業務とは関係がないため，本来の業務を優先する．また，対策による利便性やプライバシー侵害などの負担は強いられたくない．
（３）顧客
コストや従業員の業務効率などに関係なく，情報の保護を希望し，情報漏えい対策を最優先にする．

6.3 ＩＴリスクの特性を考慮した分析

6.3.1 問題の分析

JNSA による報告で，web・メール・記憶媒体・紙媒体の４つの経路が情報漏えい発生原因の上位４つとなっている[6]．そのため，この４つの経路を問題発生経路とした．

6.3.2 パターン化，分布

（１）パターン化

今回の適用ではＩＴリスクの特性として，技術力と反発心を選んだため提案方式より表１に示すように４つのパターンに分類する．

（２）分布

今回は分布を JTB モチベーションズが行った調査[8]とパレート法則を参考にして決定した．JTB モチベーションズによる調査では約 38%が会社に対して不満を持ち約 62%が会社に好感を持つ．またパレート法則より，20%が技術力があり 80%が技術力がないとすると，それぞれの割合の積をとり，パターン１は約 8%，パターン２は約 12%，パターン３は約 32%，パターン４は約 48%とする．今回は以上のように分布を決定した．分布を（表２）に示す．

表２．　４つのパターンの割合

Table2.　Rate of four patterns

	反発心あり	反発心なし
技術力あり	8%	12%
技術力なし	32%	48%

6.3.3 対応表の決定

今回は試験的に以下のような対応表を作成した．負担度を L とする．負担度を L とすると，反発値は

$$O = f(L) = [\frac{L}{2} + 1]$$ （[]：小数点以下切り捨て演算）

として与えることとした．

上記の式は負担度が 1.0 上がる毎に反発値が 1.0 から 0.5 ずつ上昇することを示す．負担度はある程度まで許容出来ると想定し，ある一定の負担を超えた場合に反発があると考えた．この対応表の負担度と反発値の関係が適切でないという場合は，リスクコミュニケーション時に話し合い，合意の下で変更することが出来る．

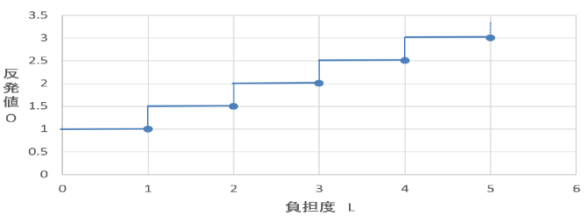

図７．　適用時の対応表

Figure7.　Table of burden and opposition

6.3.4 リスク分析

リスクを定量的に扱うためにＦＴ分析を行った．以下に分析を行ったリスクを示す．

・web からの情報漏洩発生

・メールからの情報漏洩発生

・電子媒体からの情報漏洩発生

・紙媒体からの情報漏洩発生

上記のリスクすべてに対して４つのパターン毎の分析をし，計 16 通りのＦＴ分析を行った．

6.3.5 目的関数，制約条件の決定

（１）目的関数

目的関数は，

$$\mathrm{Min}\{\sum_{j=1}^{4}\sum_{k=1}^{4} Q_j MP_{jk} + \sum_{i=1}^{12} Co_i X_i\}$$ （円）

とした．

j：パターンの種類

k：漏洩経路

Q：パターンの比率

M：情報漏洩被害額

P：漏洩確率

Co：対策コスト

Xi は０－１変数

Xi＝１　対策案 i を採用

Xi=0　　対策案 i を不採用

（２）制約条件

制約条件として以下を設定した．

・対策コスト

対策にかかるコストのことである．

$$\sum_{i=1}^{12} Co_i X_i \le Co_t$$

・漏洩確率

漏洩確率を示す値である．

$$\sum_{j=1}^{4}\sum_{k=1}^{4} P_{jk} Xi \le P_t$$

・利便性負担度

対策案を取ることによる利便性の負担度を示す値である．

$$\sum_{i=1}^{12} E_i X_i \le E_t$$

・プライバシー負担度

対策案を取ることによるプライバシーの負担度を示す値である．

$$\sum_{i=1}^{12} S_i X_i \le S_t$$

ここで，反発心を考慮するとP_{jk}が変化する．P_{jk}は図３の攻撃を試みる確率と攻撃に成功する確率からなる情報漏洩確率の数値であるが，攻撃を試みる確率をP_{jk1}，攻撃に成功する確率をP_{jk2}とすると反発値 O によって攻撃を試みる確率P_{jk1}に変化がある．よって，P_{jk}はOP_{jk1}とP_{jk2}によって変化する漏洩確率である．ただし，なにも対策候補のない最初の演算で目的関数に与えられる反発値 O は 1.0 である．

上記のような目的関数，制約条件の下で計算した Xi に対し、負担度 L は５章で述べた考え方により次式で計算することにした．

$$L = \sum_{i=1}^{12} (E_i + S_i) X_i / 2$$

Ei と Si は 6.3.7 節で示す表５の制約条件値を取る．

6.3.6 各種対策案の決定

以下に対策案の一覧を示す.

表３.　対策案一覧

Table3.　List of proposed measures

No.	対策案
#1	URLフィルタリングツールを導入し、 WEBフリーメールの使用や掲示板の書き込みを禁止する
#2	あらかじめ指定された管理ソフトウェアを使用し、管理者に許可されていないソフトウェアの使用を禁止する
#3	管理ソフトウェアの設定変更を禁止する
#4	メール送信時の制限を設ける(メール送信には上長の許可が必要)
#5	電子媒体への書き出し時に強制暗号化を行う(会社外のPCでは復元不可)
#6	印刷物へ強制的に印刷者の情報の透かしを挿入
#7	監視者の増員
#8	匿名性の減少(IDによる管理、持ち出し台帳による管理など)
#9	上司や同僚が相談を行うor相談できる環境を設ける
#10	指示を掲示する(個人情報管理策の掲示など)
#11	再教育の実施
#12	罰則の制定

6.3.7 各種パラメータの決定

以下に対策案の効果，制約条件の値，末端事象の値を示す．これらの値は「多重リスクコミュニケータの開発と適用」の値を基本的に参考にして，現在に沿うように値を決めた[1]．対策案効果の数値に関しては値が 0.4 のとき，フォルトツリーの末端事象の発生確率を 4 割下げることができることを意味している（表４）．今回は制約条件として，利便性負担度とプライバシー負担度設定したため表５にその値を示す．制約条件の値の指標は表６の通りである．なお，これらの値が適切でないという場合は，リスクコミュニケーション時に話し合い，合意の下で変更することが出来る．

表４.　対策案効果

Table4.　Effect of proposed measures

No	Web	メール	紙媒体	電子媒体
対策案1	0.7	0.5	0	0
対策案2	0.5	0.3	0	0
対策案3	0.5	0.2	0	0
対策案4	0	0.6	0	0
対策案5	0	0	0	0.8
対策案6	0	0	0.4	0
対策案7	0	0	0.7	0.5
対策案8	0.2	0.2	0.2	0.2
対策案9	0.5	0.5	0.5	0.5
対策案10	0.2	0.2	0.2	0.2
対策案11	0.5	0.5	0.5	0.5
対策案12	0.2	0.2	0.2	0.2

表５.　制約条件のパラメータの値

Table5.　Parameters values of constraints

No	利便性負担度 E	プライバシー負担度 S
対策案1	0.5	0.3
対策案2	0.6	0.2
対策案3	0.4	0
対策案4	0.6	0.6
対策案5	0.7	0.1
対策案6	0.1	0.2
対策案7	0	0.7
対策案8	0.4	0.5
対策案9	0.7	0.1
対策案10	0.1	0
対策案11	0.8	0.1
対策案12	0.4	0

表６.　制約条件値指標

Table6.　Index of constraint condition

利便性負担度	関与者の心理的負担
0～0.3	ほとんど不快とは感じない
0.3～0.6	やや不快
0.6～1.0	不快
プライバシー負担度	関与者の心理的負担
0～0.3	ほとんど不快とは感じない
0.3～0.6	やや不快
0.6～1.0	不快

6.4　MRC 演算による対策案最適化結果

以下に MRC 演算結果を示す．ここでは制約条件の漏洩確率 P を 1.0，利便性負担度 E を 2.5，プライバシー負担度 Pr を 1.5 として演算を行った．

表７.　１回目演算結果

Table7.　Result of first calculation

対策案	目的関数	漏洩確率 P	利便性負担度 E	プライバシー負担度 S
#1, #2, #3, #5, #10	35,173,200	0.86	2.3	0.6

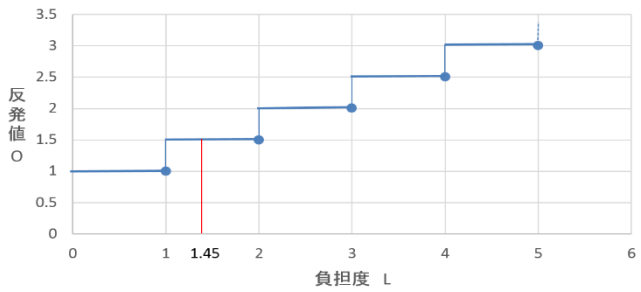

図８.　１回目の対応表

Figure8.　Relationship between burden and opposition at the first calculation

演算結果（表７）の対策案候補の利便性負担度 E とプライバシー負担度 Pr の合計は 2.9 である. 負担度 L を表す制約条件の数は２つなので，５章の説明に習い，負担度 L の値は 2.9／2 となる. したがって, 負担度 L は 1.45 である．対応表（図８）から負担度 L が 1.45 の場合は目的関数の反発値 O の値が 1.5 でなければならないため, 目的関数の反発値に 1.5 を代入して再計算を行った.

表８.　２回目演算結果

Table8.　Result of second calculation

対策案	目的関数	漏洩確率 P	利便性負担度 E	プライバシー負担度 S
#1, #2, #3, #4, #6, #10	35,681,200	0.91	2.3	1.3

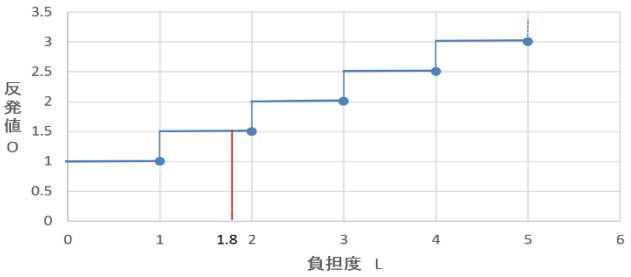

図９．　２回目の対応表

Figure9.　Relationship between burden and opposition at the second calculation

表８の結果から対策案候補の負担度Lを先ほどと同様にして求めると 1.8 である. 対応表（図９）から負担度 L が 1.8 の場合は目的関数の反発値 O の値は 1.5 となる．１回目の演算ですでに反発値 O を 1.5 として演算を行っているため, 反発によるリスクの差は存在しない. したがって, 今回の対策案候補は反発を考慮した上で目的関数が適切に設定されている．よって，ここで MRC の演算を終了した．

6.5　考察

従来の MRC であれば１回目の MRC 演算で, 合意形成への議論へと遷移していた．しかし，今回の適用では対策案の組み合わせによって，対策関連者の反発によるリスクの上昇が懸念された．よって，運用を想定した場合に適切な解として認められなかった．そこで，再度反発によるリスクを考慮した上で演算を行った結果，対策の組み合わせとリスクの兼ね合いが取れたため演算を終了した．

対策案に注目すると，「電子媒体書き出し時に強制暗号化」から「印刷物に透かしを挿入」といった具合に変化しており，負担度も考慮されている．

ＩＴリスクの動的特性を考慮することで，従来とは違った解が求まることになった．対策案選定がより詳細になったことからもＩＴリスクの動的特性による分析に基づきパターン毎に対応を変化させ，対策後の反応を考慮することの重要性を確認できた．

7.　おわりに

本稿では, MRC におけるＩＴリスクの特性を考慮した分析手法を提案した．従来の MRC では対策を取った事によって変化するリスクに対応をしていなかったが，それらを加味することでより対策案の選定が状況に適したものとなる見通しが得られた．

今後は，対応表の反発値と負担度の関係についてアンケート調査などを進め，現在よりもリスクの算出を厳密にする必要がある．

参考文献

1) 佐々木良一，　日高悠，　守谷隆史，　谷山充洋，　矢島敬士，八重樫清美，　川島泰正，　吉浦裕,「多重リスクコミュニケータの開発と適用」，情報処理学会論文誌 49(9)，3180-3190，2008-09-15
2) 谷山充洋，日高悠，荒井正人，甲斐賢，伊川宏美，矢島敬士，佐々木良一『多重リスクコミュニケータの企業向け個人情報漏洩問題への適用』情報処理学会論文誌 2007 年 10 号　2007 年
3) 芦野佑樹，間形文彦，西垣正勝，勅使河原可海，佐々木良一「AS-1-4 デジタルフォレンジック対策の組み合わせに関する合意形成のための多重リスクコミュニケータの適用」, 電子情報通信学会総合大会講演論文集 2009 年_基礎・境界，"S-27"-"S-28", 2009-03-04
4) 柿沼祐吾，谷山充洋，杉本尚子，矢島敬士，佐々木良一「多重リスクコミュニケータの青少年ネット規制法に関わる問題への適用」, 電気学会研究会資料. IS，情報システム研究会 2009(71), 25-30, 2009-12-11
5) 谷山充洋，日高悠，荒井正人「多重リスクコミュニケータの企業向け個人情報漏洩問題への適用」，日本セキュリティ・マネジメント学会誌 23(2), 34-51, 2009-09
6) JNSA，「2012 年情報セキュリティインシデントに関する調査報告書」，http://www.jnsa.org/result/incident/2012.html (2013 年 4 月 30 日)
7) IPA，「組織内部者の不正行為による インシデント調査」，http://www.ipa.go.jp/files/000014169.pdf (2012 年 7 月 17 日)
8) JTB モチベーションズ，「会社が好きですか　調査報告書」，http://www.jtbm.co.jp/wordpress/wp-content/uploads/2012/11/syasuki.pdf (2011 年 12 月)
9) 警察庁，「犯罪統計書　平成２４年の犯罪」，http://www.npa.go.jp/archive/toukei/keiki/h24/pdf/H24_ALL.pdf (2013 年 9 月 6 日)