情報処理学会論文誌 Vol. 49 No. 9 3180–3190 (Sep. 2008)

推薦論文

多重リスクコミュニケータの開発と適用

佐々木 良一[†1,†2] 日高 悠[†3] 守谷 隆史[†1]
谷山 充洋[†1] 矢島 敬士[†1,†2] 八重樫 清美[†4]
川島 泰正[†5] 吉浦 裕[†6]

企業や社会はいろいろなリスクをかかえており，最近では1つのリスク対策（たとえばセキュリティ対策）が，新しいリスク（たとえばプライバシリスク）を発生させるということも多く「リスク対リスク」の時代を迎えているともいえよう．この問題を解決するために，いろいろなリスクやコストを考慮しつつ，望ましい対策案の組合せに関し，経営者や顧客，従業員など意思決定関与者の合意を形成していくことが必要となっていることを指摘した．あわせて，この機能の実現は支援ツールなしでは容易ではないため「多重リスクコミュニケータ（MRC）」の構想を提案してきた．今回，(1) 専門家入出力部や，(2) 最適化エンジン，(3) 合意形成用の関与者支援部などを持つ MRC プログラムの開発を行うとともに，個人情報漏洩問題，不正コピーによる著作権侵害問題，内部統制問題などに適用することにより，その有効性を確認するとともに残された課題が明確になったので報告する．

Development and Applications of Multiple Risk Communicator

Ryoichi Sasaki,[†1,†2] Yuu Hidaka,[†3] Takashi Moriya,[†1]
Katsuhiro Taniyama,[†1] Hiroshi Yajima,[†1,†2]
Kiyomi Yaegashi,[†4] Yasuhiro Kawashima[†5]
and Hiroshi Yoshiura[†6]

Businesses and society face various risks, and measures to reduce one risk often cause another risk. It may be said that nowadays is the times of the risk vs. the risk. For this reason, the risk communication for forming agreement among decision-making persons, such as manager, customers, and employees, is becoming important. However, it is not easy to search for the combinations of the optimal measures, reducing the risk based on the concept which is opposed to each other, such as security, privacy, and development cost, and taking agreement. This situation requires development of the "multiple risk communicator (MRC)" with the functions of which are (1) Modeling support part for expert, (2) optimization engine, and (3) displaying the computed result to decision-making persons. In this paper, after describing a developments design of MRC, we explain the implemented MRC program and its application results to personal information leakage problems, illegal copying problems, and inner control problems with evaluation on the usefulness and issues to be solved in future.

1. はじめに

企業や社会はいろいろなリスクをかかえており，最近では1つのリスク対策（たとえばセキュリティ対策）が，新しいリスク（たとえばプライバシリスク）を発生させるということも少なくない．すなわち，「リスク対リスク」の時代を迎えているともいえよう．たとえば，セキュリティ対策として暗号化やデジタル署名のために公開鍵証明書を利用するが，そこに書かれた住所や生年月日が，個人情報の流出につながり，プライバシ上の問題となるとも考えられる．

セキュリティの喪失とプライバシの喪失という多重のリスクがある場合に，それらのリスク間の対立を解決するのに，**図1** に示すように技術は十分貢献でき，1つの対策でセキュリティもプライバシもよくすることはできる．たとえば，公開鍵証明書が個人情報漏洩の原因となりプライバシが問題になるならば，属性だけを記述した属性証明書を渡すようにすることで，セキュリティとプライバシの両方に望ましくすることはできる．しかし，やはり，公

†1 東京電機大学
Tokyo Denki University
†2 独立行政法人科学技術振興機構社会技術研究開発センター
Researcher of RISTEX JST
†3 IT 働楽研究所
IT DORAKU RESEARCH LAB. Ltd.
†4 ピンポイントサービス
PinpointService, Inc.
†5 アドイン研究所
AdIn Research, Inc.
†6 電気通信大学
The University of Electro-Communications
本論文の内容は 2007 年 10 月のコンピュータセキュリティシンポジウムにて報告され，CSEC 研究会主査により情報処理学会論文誌ジャーナルへの掲載が推薦された論文である．

開鍵証明書を使う場合に比べて，安全性や使い勝手では，やや劣るといえよう．

したがって，セキュリティ，プライバシ，コストなどの指標のどれを重要視するかは，意思決定関与者の選好の問題となる．さらに，意思決定に関与する人たちは多く，これらの人たちが合意を形成するのは容易ではなく，リスクコミュニケーションの過程が必要となる．ここで，リスクコミュニケーションとはリスクについて直接・間接に関係する人たちが意見を交換し，合意を形成する過程であり，原子力施設の設置時に電力会社，住民などの意思決定関与者間の合意形成などに用いられてきたものである．

著者らは，こうした問題を解決するために，いろいろなリスクやコストを考慮しつつ，望ましい対策案の組合せに関し，経営者や顧客，従業員など意思決定関与者の合意を形成していくことを支援するためのツールが必要と考え，「多重リスクコミュニケータ（Multiple Risk Communicator: MRC）」の開発構想を固めてきた（文献 1)，2) など）．リスク分析用の方法としては，ベースラインアプローチや詳細リスク分析，組合せアプローチなどが知られているが[13]，いずれもリスク対リスクの問題を解決する機能や，リスクコミュニケーションの機能を持つものではない．

その後，(1) 専門家入出力部や，(2) 最適化エンジンなどを含む演算部，(3) 関与者支援部などを持つ MRC プログラムの開発を行った．意思決定支援にプログラムを利用する例は多いが[14]，リスク分析やリスクコミュニケーションを支援するプログラムは一般に少ない．特に MRC プログラムのような機能を持つものはない．この MRC プログラムを，個人情報漏洩問題，不正コピーによる著作権侵害問題，内部統制問題などに適用することにより，基本的有効性を確認するとともに今後の課題が明確になった．

本論文では，MRC の開発目的，MRC プログラムの概要，適用結果，今後の課題などについて報告する．

2. MRC の開発目的と概要

MRC を開発した背景と目的を整理すると以下のようになる（**図 2** 左側参照）．

(1)　多くのリスク（セキュリティリスク，プライバシリスクなど）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コミュニケーション手段が必要となる．

(3)　1 つの対策だけでは目的の達成が困難である．したがって，対策の最適な組合せを求めるシステムが必要となる．

このような目的のために考案した MRC は，いろいろ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ベースに，複数の意思決定関与者の合意を形成するのを支援する機能などを持つものである．このような機能を持たせるため図 2 の右側に示すように，専門家向け入出力部，演算部，関与者支援部，全体制御部，データベース部，ネゴシエーション基盤などから構成することとした．この MRC の利用者としては，専門家や，複数の意思

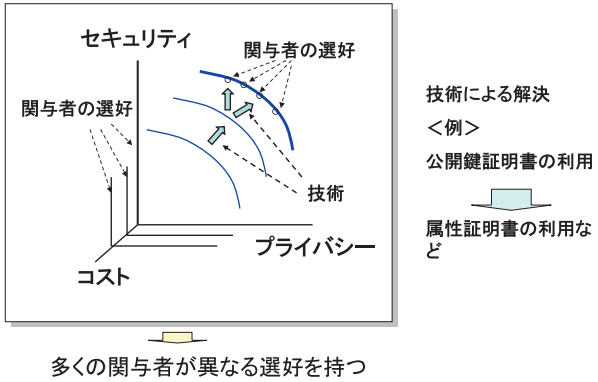

図 1　対立するリスクの解決方法のイメージ
Fig. 1　Image of method for solving the conflict between risks.

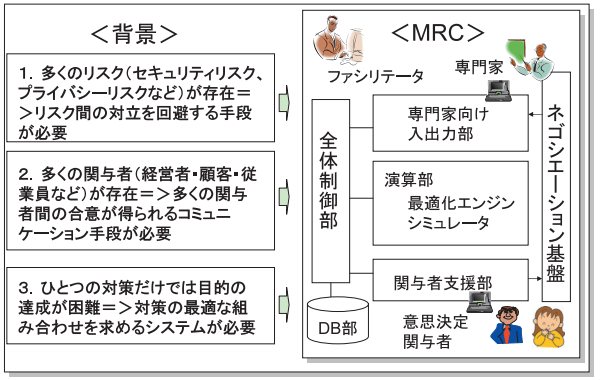

図 2　MRC の開発目的と概要
Fig. 2　Development objectives and characteristics of MRC.

決定関与者と，それらの人たちの間の仲立ちをするファシリテータがいる．

この MRC を適用するにあたっては，事前に専門家が次のような対応を行うことを想定している．

① **対象の決定**：問題を解決したい人の依頼などにより，扱う問題を決定する．たとえば，ある地方自治体における個人情報漏洩問題などがこれにあたる．

② **問題の分析**：対象問題が生じる原因や不正の方法などの分析を行う．たとえば個人情報の持ち出し経路や，方法を明確化する．

③ **対象とする関与者の決定**：意思決定に影響を及ぼす関与者をリストアップする．たとえば，地方自治体の場合は，関与者としては，自治体の幹部や住民，職員などが考えられる．これらの関与者にはリスクコミュニケーションの過程で，意見を言ってもらう．

④ **目的関数・制約条件の項目の決定**：対策案の最適な組合せを求めるため組合せ最適化問題として定式化する際の目的関数と制約条件の項目を決定する．ここでは，目的関数としてトータルソーシャルコストを最小化することとし，制約条件として，関与者ごとに興味のある項目を設定することとした．たとえば，目的関数は，（個人情報漏洩の発生確率 × 損害額 + 対策費用）とし，制約条件としては，自治体の幹部向けに対策費用，住民向けに個人情報漏洩確率，職員向けにプライバシ負担度，利便性負担度を設置する．

⑤ **対策案のリストアップと関連パラメータの推定**：有効と考えられる対策案をリストアップする．次に，各対策案の対策費用や，プライバシ負担度，利便性負担度などを積み上げ計算や，アンケートによって決定し，表の形で整理する．また，対策を施した場合の個人情報漏洩確率などの発生確率については，フォルトツリー分析法（FTA）[11] を用いるが，それに必要なデータも準備する．ここでの，表のイメージは**表 1** に示すとおりであり，フォルトツリーは，**図 3** に示すようになる．

表 1 で「従業員へのプライバシ負担度」や，「従業員への利便性負担度」の値は，プライバシや利便性に関する新たな負担がまったくない場合は 0，負担が耐えられないほど大きい場合は 1 であるとして，従業員へのアンケートによって得ている．

このようにして得られたものを MRC に入力することになるが，この MRC は，すでに述べたように次の 6 つの部分で構成することにしている．

（1）専門家向け入出力部

専門家が**図 4** に対応するような（a）目的関数，（b）制約条件式，（c）対策案，（d）係数，（e）制約条件値を多重リスクコミュニケータに与えるのを支援する．

ここで，X_i は対策案 i の採用，不採用を表す 0-1 変数であり，C_i や D_{i1}，D_{i2} は，表 1 など

表 1　対策案とパラメータの値の例
Table 1　Examples of the countermeasures and the values of parameters.

対策案	対策効果 $\Delta P_{\alpha 1 i}$ 内部1	対策効果 $\Delta P_{\alpha 2 i}$ 内部2	対策効果 $\Delta P_{\beta i}$ 外　部	コスト Ci （万円）	従業員へのプライバシー負担D_1i	従業員への利便性負担 D_2i
1:外部へのメール監視(コンピュータ制御による自動監視)	0.8	0.8	0.8	390	0.6	0
2:外部へのメール監視(人手による監視)	0.95	0.95	0.95	3000	1	0
3:ファイアウォール	0.9	0.9	0.9	75	0	0.4
4:IDS(侵入検知システム)	—	0.7	0.7	1300	0	0
5:個人情報サーバの脆弱性の管理	—	0.8	0.9	300	0	0.2
6:隔離エリア内での外部媒体への保存の管理	0.9	0.9	0.9	2500	0	0.7
7:隔離エリア内への入退出管理システム	—	0.8	0.9	800	0.1	0.4
8: 隔離エリア内への持ち物検査	0.8	0.8	0.9	3000	0.8	0.6

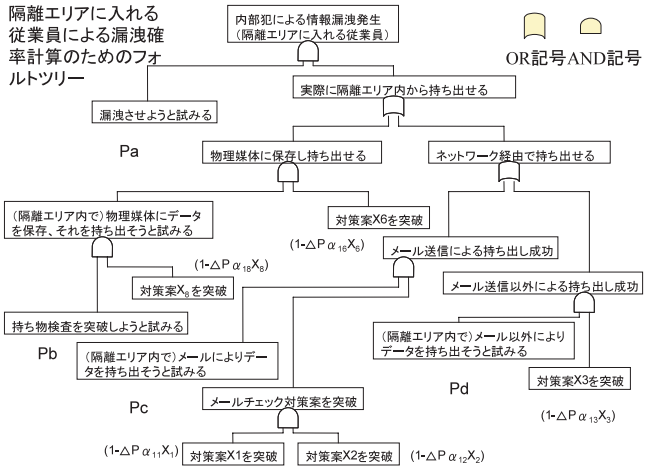

図 3　内部の不正者による個人情報漏えいに関するフォルトツリー
Fig. 3　Example of fault tree for information leakage by injustice person in inside.

どから得られるものである．また，$P_{\alpha 1}$，$P_{\alpha 2}$，P_β などは，表 1 の対策効果の値をベースにし，図 3 のようなフォルトツリーを用いて求めるものである．また，C_t，D_1，D_2，P_t は，専門

家によって最初与えられその後，意思決定関与者によって変更することが可能なものである．

この過程で，リスク計算の基礎となる事故などの発生確率を計算できるようにするためフォルトツリー分析を行うことが多いが，この分析を支援する機能も持たせる．

(2) 全体制御部

プログラム全体を制御する．

(3) 演算部

最適化エンジンやシミュレータなどよりなる．最適化エンジンは，組合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 L 最適解を求める．この求解には総当たり法や辞書式枚挙法を採用する．

シミュレータは，最適解を求めた後，対策結果の予測を詳細に行い，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．

(4) 関与者支援部

住民や従業員などの意思決定関与者の合意形成のために必要な情報を分かりやすく表現するためのものである．ここでは，(a) 各関与者が，満足する解に導くための表示内容や，表示順序とともに，(b) 関与者間で合意が形成しやすくする表示方法の工夫が必要となる．

(5) 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する．

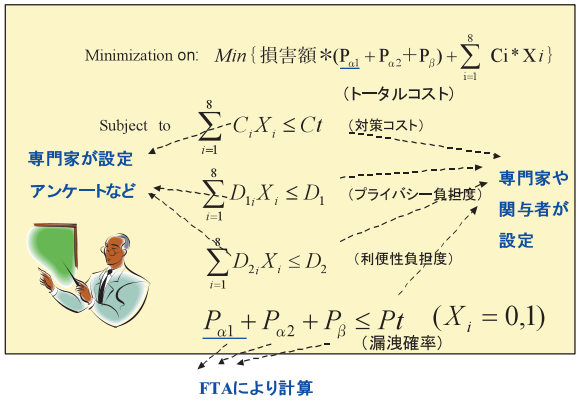

図 4　定式化結果のイメージ
Fig. 4　Image of formulated result.

(6) ネゴシエーション基盤

それぞれの関与者が，「もっと別の対策案を考える」とか「制約条件値が違う」とかの意見を言うと，この結果は，ネゴシエーション基盤（2 者間で情報交換するためのツールがベースとなる）を利用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多重リスクコミュニケータに与えられ，その結果が再表示される．この仲立ちをファシリテータが行い，プロジェクト管理用のソフトや関与者支援部のソフトを利用する．また，ファシリテータが専門家として作業を行うことがあってもよい．

3. MRC プログラムの開発

今般開発した MRC プログラム（バージョン 1）の構成は**図 5** に示すとおりである．

このようにしたのは，次のような条件を満足したかったからである．

(1)　インターネットにつなげるところなら，専門家やファシリテータ，一般関与者が同じところにいる場合だけでなく，異なるところにいる場合にでも MRC 機能を利用できるようにしたい．

(2)　専門家向け PC を除き，ファシリテータ向け PC や一般関与者向け PC は特別なソフトを必要としないようにしたい．

ここで，MRC プログラムは，4 種類のコンピュータ上に実現されている．図 2 の全体制御部は，これらの PC 上のソフトに分散して実現していると考えることができる．

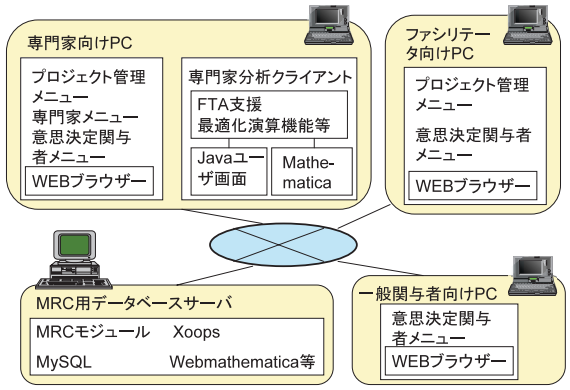

図 5　MRC システムの構成
Fig. 5　Structure of MRC program.

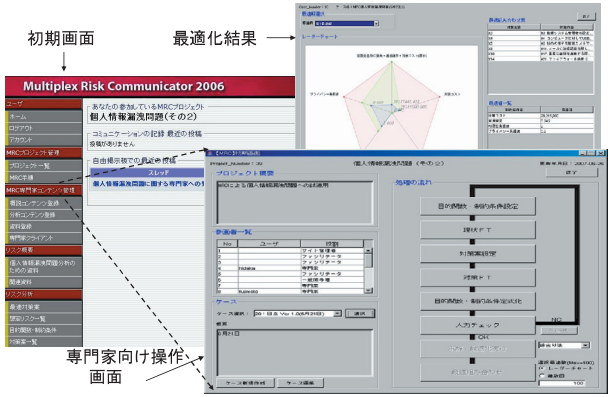

図 6　MRC プログラムの専門家向け入出力部の画面イメージ
Fig. 6　Image of display for experts in MRC program.

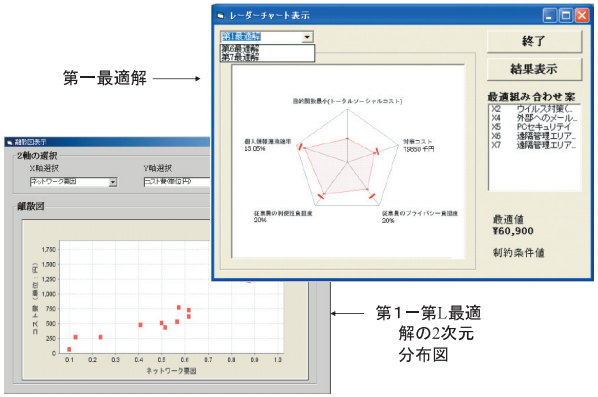

図 7　一般関与者向け画面
Fig. 7　Display for individuals involved in decision making.

専門家向け PC 上には，専門家向け入出力部の機能と最適化エンジンの機能が実現されている．専門家向け入出力部については，2 章の「**(1) 専門家向け入出力部**」で述べた構想にそって開発を行っている．また，最適化エンジンで扱える対策案の最大数は，最初は 15 個，現状では，32 個とし，求解法として，総当たり法と辞書式枚挙法[12] を実装し選択できるようにした．定式化に必要な数式を効率良く記述するため Mathematica[9] を組み込んだ．

また，シミュレータについては，既存のシミュレーションプログラムの MRC からの立ち上げ支援機能を実現した．専門家向け PC からは，(1) プロジェクト管理メニュー，(2) 専門家メニュー，(3) リスク関与者メニューを扱うことができるようになっている．(1)，(2) のメニューから見られる画面の概要は，**図 6** に示すとおりである．

関与者支援部やネゴシエーション基盤については，今回は必要最小限の機能とした．適用を通じて必要な機能を明確化し，バージョン 2 で機能を追加する予定である．バージョン 1 の関与者支援部は，一般関与者向け PC の中に実現されており，**図 7** に示すような画面イメージを持つリスク関与者メニューを見ることができる．ここでは，第 1 最適解から第 L 最適解（バージョン 1 では最大 100）までをいろいろな形で分かりやすく表示できるようにしている．

また MRC 用データベースサーバや一般の WEB にある，解を求める前提や対応するフォルトツリー，関連情報などを 1 つの画面（ポータルサイトと呼ぶ）から，容易にたどれるようにしている．さらに，掲示板機能をネゴシエーション基盤として利用して，専門家やファシリテータに種々の連絡を行うことも可能である．あわせて，このメニューから制約条件を変更した場合の解を求めて表示できるようになっている．

ファシリテータ用 PC からは，プロジェクト管理メニューとリスク関与者メニューを見ることができる．

MRC 用データベースサーバには，プロジェクトごとの分析結果や，関与者間のやりとりの記録が保存されるようになっている．ファシリテータが許可した専門家向け PC，一般関与者向け PC から，インターネットを経由してこのデータベースにプロジェクトごとにアクセスすることができる．

4. MRC の適用と評価

4.1 MRC の適用結果

4.1.1 適用結果の概要

MRC プログラムを試適用する目的は次の 3 点である．

(1)　各問題において満足すべき定式化が可能かどうかの確認
(2)　そのような定式化結果に対し MRC により解を求めることが可能かどうかの確認
(3)　ロールプレイヤによりリスクコミュニケーションを行うことにより合意の形成の可能性が高いかどうかの検討

そして，可能性が高い場合には，本物の意思決定関与者に参加いただき合意形成できるかどうかを確認するとともに実際の対策に役立てるようにしたいと考えた．

表 2　適用結果の概要
Table 2　Applied results of MRC.

	対象	目的	関与者	分析手法 プログラム	備考
1	個人情報漏洩への適用	従業員の負担も考慮した対策案の合意形成	経営者 顧客 従業員	FTA PR，V1	表3参照
2	不正コピーによる著作権侵害問題への適用	対策後の不正者の行動を想定した効果予測に基づく合意形成	レコード会社 消費者	FTA PR	[4]参照
3	内部統制問題への適用	大学における公的資金の適切な運用に関する内部統制対応	センタ 教授 学生	ETA V1	[7]参照
4	暗号の危殆化対策への試適用	暗号危殆化時の署名つき文書の安全対策に関する合意形成	政府 署名者 検証者	ETA PR	[5]参照

分析手法:FTA: Fault Tree 分析法 ETA:Event Tree 分析法
適用したプログラム　PR:プロトプログラム、V1:バージョン1プログラム

MRC については，類似のアプローチがほとんどないので，最初からすべての必要機能を盛り込んだプログラムを作るのではなく，バージョンに分けてプログラムを作り，それを複数の対象に適用しつつ，方式自体の改善を図り，次のプログラムを作るというアプローチを採用した．具体的には，最初に最適解を求める機能を中心とするプロトプログラムを作り適用し，次に 3 章で述べた MRC プログラム（バージョン 1）を開発し適用してきた．

適用結果は**表 2** に示すとおりである．表 2 で PR はプロトプログラムを表し，V1 はバージョン 1 のプログラムを表している．適用が一番多いのが個人情報漏洩対策であり，不正コピー防止対策や，内部統制対策，公開鍵暗号の危殆化対策などにも適用した．個人情報漏洩対策への適用結果については，4.1.2 項で少し詳しく述べることとし，ここでは，その他の適用結果について言及する．

1）不正コピーによる著作権侵害問題への試適用[4)]

不正コピーによる著作権侵害が，音楽業界，音楽に関連する流通業界，消費者といった社会全体にどのような影響を与えるかについて分析を行うとともに，最適な不正コピー対策の組合せを求める．

分析における特徴は，不正者を関与者として意見を聞くことができないので，その部分をシミュレータで代行させた点である．ここでの，関与者は，学生などがロールプレイヤとして参加し，意見を述べたものである．

2）J-SOX 法など内部統制整備への MRC の適用[7)]

J-SOX 法や新会社法などの誕生により内部統制が強化される中で，組織がどのような制度的・技術的対策をとっていくのがよいかの合意を形成することを目的とする．

近年，大学における公的研究費の不正利用が問題になっており，「大学における公的研究費の運用体制構築」を具体的には採用することにした．ここで，対策効果の分析などには，実施とチェックの間に時間の経緯があることから，そのような状況での分析に適した ETA（イベントツリー分析法）を用いた．

この結果，物品購入・旅費精算・給与精算のすべてのケースにおいて，財務リスクだけでなく効率性低下リスクなども考慮した最適な対策案が得られるなどの知見が得られた．

ここでの，関与者は，学生などがロールプレイヤとして参加し，意見を述べたものである．

3）暗号の危殆化時の対策への MRC の適用[5)]

公開鍵暗号などが危殆化した場合に，すでに存在する署名付きデジタル文書に及ぼす影響を十分小さくするための対策案の組合せに対する合意の形成を行うことを目的とするものである．電子借用書への対策を対象に実施した．対策効果の分析などには，暗号危殆化に対し，いろいろな対策が時間の経過とともに考えられることから，そのような状況での分析に適した ETA（イベントツリー分析法）を用いた．

この結果，次のようなことが明らかになった．

(1)　CRYPTREC[10)] を今後，より強化することが望ましい．
(2)　危殆化時対応ポリシを早急に策定し，それに沿って対応することを強制できるよう制度化する必要がある．
(3)　署名付き文書を扱う人たちに，危殆化に関する情報を，認証局経由ではなく，広く確実に伝達する仕組みが必要である．
(4)　署名付き文書の再処理方法について今から検討しておく必要がある．

ここでの，関与者は，暗号や法律，保険システムの実際の専門家であり，パラメータの値などについて意見を述べたものである．

(1)〜(3) のいずれの場合も，各問題において満足すべき定式化が可能であると確認できるとともに，そのような定式化結果に対し MRC により解を求められることが確認できた．また，ロールプレイヤによりリスクコミュニケーションを行うことにより合意の形成に成功しているが，さらに多くのケースでの実験が必要であると考えている．

4.1.2　個人情報漏洩対策への適用

個人情報漏洩対策については，**表 3** に示すようにいろいろなケースに適用してきた．

個人情報漏洩への対策は，1）プロバイダからの情報漏洩対策，2）一般企業からの情報漏洩対策，3）区役所からの情報漏洩対策の 3 種類実施した．1），2）は，関与者が一部，ロー

表 3　個人情報漏洩問題への適用状況
Table 3　Applied results to private information leakage problems.

No	対象問題	関与者	現在の状況	備考
1	プロバイダーからの個人情報漏洩対策	管理者 顧客 従業員	3つのケースでロールプレイ	[2][8]参照
2	一般企業からの個人情報漏洩対策	情報管理センタ 社員	1つのケースでロールプレイ	[6]参照
3	小中学校の校務システムからの個人情報漏洩対策	電算課 教育委員会担当 教師	MRCシステムを実適用。対策実現予定。	世田谷区役所

ルプレイヤであるが，3）は関与者も含め実際の適用である．以下，それぞれについて簡単に説明を行う．

1）プロバイダからの個人情報漏洩対策[2),8)]

ここでの対策案の数は 8 個であり，ソーシャルコスト最小化を目的関数とし，対策コスト，個人情報漏洩確率，プライバシ負担度，利便性負担度を制約条件とした．

ここでは，3 組のロールプレイヤで合意形成実験を行った．専門家が最初に与えた制約条件で解を求めた後，関与者が望む制約条件の値をそれぞれ入れ，何回か演算したのち，第 3 回を除きいずれの場合も合意に達した．たとえば，第 1 回の場合は以下のようなものである．

① 専門家によって与えられた制約条件は，漏洩確率：年間 0.15 回以下，対策コスト：8,000 万円以下，従業員のプライバシ負担度：0.30 以下，従業員の作業負担度：0.30 以下であった．ここで，プライバシ負担度，作業負担度に関する制約条件値は，すべての対策案を採用した場合の負担度を 1 とした場合の比率をいう．

② この結果をベースに，個人情報漏洩対策やセキュリティなどに関し十分知識のある学生を，経営者，住民，従業員のロールプレイヤとし，合意形成の実験を行い，以下のような結果を得た．

(1) 顧客のロールプレイヤが，漏洩確率を年間 0.1 回以下にすべきと主張した．そこで，専門家が，再度最適解を求めたが，結果は同じであった．

(2) 次に，従業員のロールプレイヤは，従業員のプライバシ負担度は，0.15 にすべきであると主張した．その結果，専門家がプライバシ負担度を，0.15 にして，漏洩確率を年間 0.1 回以下にし，求解した最適解を全員が受け入れ，合意形成が得られた．

合意が得られなかったロールプレイヤの第 3 組目は，パラメータの値について，どうしても合意が得られず，最適解が求められなかったものである．

2）一般企業からの個人情報漏洩対策[6)]

企業における「個人情報漏洩問題」を MRC の適用の対象とし，リスク分析とリスクコミュニケーションを行った．ここで対象とする組織では，サーバルームに入れない従業員がサーバルームの外から個人情報を業務上入手できるようになっており，従業員からの申請があると管理者が許可を出し，サーバから個人情報を入手できるような運用スタイルとなっている．

対策案の数は，15 個であり，ソーシャルコスト最小化を目的関数とし，対策コスト，個人情報漏洩確率，プライバシ負担度，利便性負担度を制約条件とした．

合意形成実験は学生と社員をロールプレイヤとする実験を行い，結果を関与者に見せ，制約条件をいろいろ変え最適解を求めている過程で，5 回目で関与者の合意が得られた．

1），2）いずれの場合にも，各問題において満足すべき定式化が可能であると確認できるとともに，そのような定式化結果に対し MRC により解を求められることが確認できた．また，ロールプレイヤによりリスクコミュニケーションを行うことにより合意形成の可能性が高いことが確認できた．

3）小中学校の校務システムからの個人情報漏洩対策

世田谷区内の小中学校の校内ネットワークシステム（校務システム）に対する個人情報漏洩対策に MRC プログラムを適用した．対策案の数は 13 個で，ソーシャルコスト最小化を目的関数とし，対策コスト，個人情報漏洩確率，利便性負担度を制約条件とした．

市役所の電算機部門の責任者，教育委員会の設備担当者，学校の教員を意思決定関与者とし，3 回の会合で，12 通りのケースにおける最適解を示す中で，対策案組合せの合意を形成することができた．世田谷区役所では，この結果を実際の行政に反映する方向で準備を進めている．

4.1.3　処理時間の測定結果

上記の適用においては，MRC プログラムを用いて結果を表示するまでの時間は，最大でも 2 分程度であり，実用上問題がなかった．

ここでは，処理時間の確認のため，4.1.2 項の 2）のケースについて，変数の数を変化させ，総当たり法と辞書式枚挙法を用いた場合の求解時間を測定した．2 回測定し平均した結果は，**表 4** に示すとおりである．当然ではあるが 2 回の測定による差はほとんどなく平均値に示す測定結果が 2 回えられた．

表 4　処理時間
Table 4　Processing time.

解法＼変数の数	5個	10個	15個	20個
(1)総当り法	0.1秒	4.3秒	151.5秒	5445.6秒
(2)辞書式枚挙法	0.1秒	3.5秒	34.6秒	1125.9秒
(2)／(1)	1.0	0.81	0.23	0.21

変数の数が大きくなるにつれて，総当たり法と辞書式枚挙法による処理時間の差は大きくなる傾向にある．しかし，辞書式枚挙法を採用することによって計算時間を短くしても，変数の数の増加による処理時間の増加が大きく，変数の数を数個大きくすると，総当たり法を用い元の変数の数で計算したのと同じぐらいの計算時間になってしまう．

したがって，リアルタイムで MRC を利用する場合には，変数の数は 15 個以下程度にしておくことが望ましいといえる．計算結果を出す間，別の議論をするなどの対策を立てることにより，変数の数が 20 程度までなら何とか適用できるのではないかと考えている．

変数の数が 15 個でも，適用経験からかなりの範囲の実際的問題を扱えると考えているが，さらに大きな問題に適用したい場合に備えて，高速近似解法などの検討をしていくことが望ましい．

4.2　適用結果の検討

これらの適用結果から次のようなことがいえる．

(1) MRC に必要な定式化は，プロトタイププログラム，バージョン 1 プログラムのすべての適用対象によって可能であり，MRC からすべてのケースにおいて解が得られることが明らかになった．なお，通常の安全解析には FTA が適切で，対策に時間的推移があるものには ETA が適切であることも確認できた．

(2) また，個人情報漏洩問題を中心にリスクコミュニケーションを行うことにより，ロールプレイヤの場合も実際の意思決定者の場合も合意を形成できる場合が多いことが明らかになった．これらの適用により，MRC は多重リスク下のリスクコミュニケーションの支援に基本的に有効である見通しが得られた．

(3) プロトプログラムを利用して適用を行う中から，基本的機能は問題ないが，最適化結果を分かりやすく表示する機能や，インターネット上から必要に応じて意思決定関与者が MRC にアクセスできる機能が必要であることなどが明らかになった．

(4) これらの結果を受けて開発したバージョン 1 を利用することにより，最適化結果を図 7 に示すようにグラフの形で表示できるようになるとともに，インターネットに接続できるところならどこでもリスクコミュニケーションが可能となり，関与者の意見の反映が容易となった．また，変数の数が 15 個ぐらいなら，実用上問題がない時間で求解が可能であることが明らかになった．

(5) 試適用の結果を，いろいろな利用可能性がある人たちに見ていただくことによって，当初予想した（a）政府機関から委託を受けたシンクタンクなどが，政府機関に対し，提案を行う場合以外に，（b）企業のシステムの受注を取るため SI 会社がリスクを考慮したシステムを提案する場合や，（c）企業が新製品を出す場合に既存製品がある中で，社会的に受け入れられるかどうかを検討する場合にも利用しうるという意見をいただいた．

(6) しかし，次のような問題点も明確になった．

（a）制約条件値を決めるのが簡単でない場合がある：意思決定関与者やそのロールプレイヤより対策費用などの制約条件値は比較的決めやすいが，個人情報漏洩確率などの制約条件値を答えるのが困難であるという意見が聞かれた．しかし，対策を行わない場合との比や，他社との比などの比率で与えるようにすることで，比較的容易に制約条件値を与えてもらえるようになった．

（b）専門家が対象を理解し，分析し，リーズナブルな入力をできるようにするのに時間がかかる：学生が初めて適用する場合，これらの分析に 3 カ月以上かかることも少なくない．これは，ある程度仕方のない問題ではあるが，時間を短縮できることが望ましい．個人情報漏洩問題など，同じような対象に繰り返し適用することにより，作業の効率化を図ることが可能であり，2 回目からは 1–2 週間で MRC の適用が可能となった例もある．

（c）専門家の示す結果を意思決定関与者が理解するのに時間がかかる：結果が何を示しているかや，前提条件を理解するのに時間がかかる．現在も，3 章で述べたように解を求める前提や対応するフォルトツリー，関連情報などを 1 つの画面（ポータルサイトと呼ぶ）から，容易にたどれるようにするなど情報獲得のための支援機能が関与者支援部にあるが[3]，さらに良いものにしていきたい．

（d）リスクコミュニケーションで関与者が自説を強く主張し，パラメータの値について

合意が得られない場合もある：この点については，どうしようもない場合もあるが，効用関数の導入などによる関与者支援機能の強化[3] により解決がつく場合もあると考えており，この機能をバージョン 2 に入れ，実験を行う予定である．

（e）扱える変数の数が 15 個程度である：対策案の数（変数の数）は試適用においては，8 から 15 であった．前にも述べたように変数の数がこのぐらいなら，最適化エンジンを用いることにより実用上問題がない時間で求解が可能であることが明らかになった．採用すべきかどうかを検討する対策案の数を 15 ぐらいに絞っておくのは困難なことではなく，多くの実際的問題を扱えると考えられる．しかし，さらに大きな問題に適用したい場合に備えて，高速近似解法などの検討をしていきたいと考えている．

5. おわりに

本論文では，先に提案した「多重リスクコミュニケータ」の基本概念に基づき，プログラム（バージョン 1）を開発し，個人情報漏洩防止問題などに適用することにより有効性を確認するとともに残された課題を示した．

今後，次のような改良を図っていきたいと考えている．

(1)　種々の合意形成支援機能の充実

(2)　高速近似解法の開発と MRC プログラムへの組み込み

リスクコミュニケーションの研究自体は国内外で増加の傾向にあるが，情報システムを対象としたものは少なく，支援ツールの開発も少ない．本論文と類似のアプローチは，私たちの知る限りでは存在しない．

謝辞　本研究は，科学技術振興機構社会技術研究開発センター「情報と社会」研究開発領域計画型研究開発「高度情報化社会の脆弱性の解明と解決」の中で実施したものである．研究を進める中で，貴重なご意見をいただいた中央大学土居範久教授をはじめとする関係者の方々に感謝申し上げる．

参考文献

1) 佐々木良一，石井真之，日高　悠，矢島敬士，吉浦　裕，村山優子：多重リスクコミュニケータの開発構想と試適用，情報処理学会論文誌，Vol.46, No.8, pp.2120–2128 (2005).
2) Sasaki, R., et al.: Development Concept for and Trial Application of a “Multiplex Risk Communicator”, *IFIP I3E2005*, pp.607–621 (2005).
3) 渡部知浩，山本裕志，矢島敬士，佐々木良一：多重リスクコミュニケータにおける関与者情報獲得支援方式の評価，電気学会論文誌 C 分冊，pp.310–317 (Feb. 2008).
4) 岡田祐司，吉浦　裕，佐々木良一，矢島敬士，村山優子：不正者のモデルを用いた多重リスクコミュニケータの拡張，情報処理学会 CSS2006 (Nov. 2006).
5) 藤本　肇，上田祐輔，佐々木良一：公開鍵暗号危殆化のデジタル署名付き文書への影響分析と対策案の提案，情報処理学会論文誌，Vol.49, No.3, pp.1105–1118 (2008).
6) 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 CSS2007 (Nov. 2007).
7) 守谷隆史，千葉寛之，佐々木良一：多リスク・多関与者を考慮した内部統制構築法の提案と一適用，情報処理学会 CSS2007 (Nov. 2007).
8) 日高　悠，藤本　肇，矢島敬士，佐々木良一：多重リスクコミュニケータの個人情報漏洩問題への適用性の評価，電子情報通信学会 SCIS2006 (Jan. 2006).
9) http://www.hulinks.co.jp/software/mathematica/
10) http://www.cryptrec.jp/
11) McCormic, N.J.: *Reliability and Risk Analysis*, Academic Press Inc. (1981).
12) Gerfinkel, R.S., et al.: *Integer Programming*, Wiley and Sons (1972).
13) JIS TR X 0036-3:2001：セキュリティマネジメントのガイドライン第 3 部「セキュリティマネジメントのための手法」(2001).
14) たとえば新村秀一：意思決定支援システムの鍵―有り余るコンピュータ・パワーをどう使う，講談社 (1993).

(平成 19 年 11 月 29 日受付)
(平成 20 年 6 月 3 日採録)

推薦文

インターネット社会の進展とともにリスクが増大しており，リスク低減のための対策方法を選択する際に，関係者が客観性を持ったデータを示して判断することが重要になってきている．本研究では，客観性を持ったデータを用いて，意思決定者との間で合意を形成するためのリスクコミュニケーションを促進する機能について提案している．さらに，分析手法を基に，多重リスクコミュニケータを開発し，実際に適用して評価している．取り組み内容についても新規性が高く，また様々な問題に適用させ，知見が得られており，開発したツールの効果も高く，有効性も高いことから推薦する．

（コンピュータセキュリティ研究会主査　寺田真敏）

佐々木良一（フェロー）

1971 年 3 月東京大学卒業．同年 4 月日立製作所入社．システム開発研究所にてシステム高信頼化技術，セキュリティ技術，ネットワーク管理システム等の研究開発に従事．2001 年 4 月より東京電機大学工学部教授，2007 年 4 月より未来科学部教授．工学博士（東京大学）．1998 年電気学会著作賞受賞．2002 年情報処理学会論文賞受賞．2007 年総務大臣表彰（情報セキュリティ促進部門）．平成 19 年度「情報セキュリティの日」功労者表彰．著書に，『インターネットセキュリティ』（オーム社，1996 年），『インターネットセキュリティ入門』（岩波新書，1999 年），『IT リスクの考え方』（岩波新書，2008 年）等．情報処理学会コンピュータセキュリティ研究会顧問．日本セキュリティ・マネジメント学会会長，情報ネットワーク法学会理事長，日本学術会議連携会員，日本ネットワークセキュリティ協会会長．

日高　　悠（正会員）

2005 年東京電機大学工学部情報通信工学科卒業．同年同大学大学院情報メディア学修士課程入学．この間主に情報セキュリティ，多重リスクコミュニケータの研究に従事．2007 年同大学院修了．同年株式会社 IT 働楽研究所に入社．

守谷　隆史

2006 年 3 月東京電機大学工学部情報メディア学科卒業．同年 4 月同大学大学院工学研究科情報メディア学専攻修士課程入学．リスクコミュニケーションを支援する多重リスクコミュニケータの研究に従事．2008 年 3 月同修士課程修了．同年 4 月新日鉄ソリューションズ入社．

谷山　充洋（学生会員）

2007 年 3 月東京電機大学工学部情報メディア学科卒業．同年 4 月同大学大学院工学研究科情報メディア学専攻修士課程入学．現在，多重リスクコミュニケータの新たな適用問題を検討中．

矢島　敬士（正会員）

1950 年 10 月 5 日生．1975 年 3 月京都大学大学院精密工学専攻修了．（株）日立製作所に入社し，同社システム開発研究所勤務．1982 年 MIT 客員研究員．1999 年から 2003 年まで東京工業大学客員教授．2004 年 4 月から東京電機大学情報メディア学科教授．グループウエア，コミュニケーション・インタフェース等の研究に従事．IEEE，電気学会，HI 学会会員．工学博士．

八重樫清美

1957 年 4 月 10 日生．1976 年 3 月岩手県立黒沢尻工業高等学校機械科卒業．（株）アイエックスナレッジに入社し，ユーザ運用等従事．1977 年（株）アルタスに入社し，SE としてプラント，3D グラフィックスシステム開発等に従事．1988 年（株）アドイン研究所に入社し，SE として AI，ロボット，ヴァーチャルモールシステム等の研究・開発に従事．発明特許に “ファジィパターン型ヒューマンインターフェースシステム” がある．1997 年同社にて営業に転属し，受託顧客・パートナ開拓，商品企画等に従事．2005 年（株）ピンポイントサービスを設立，代表取締役に就任．AI 技術を中心としたコンサルティング，研究開発等を事業展開．日本セキュリティ・マネジメント学会会員．

川島　泰正（正会員）

1983 年北海道大学大学院工学研究科精密工学専攻修了．株式会社日立製作所日立研究所（茨城県日立市）において，三次元 CAD/CAM・CG・設計知識管理システム等の研究開発に従事．2001 年より株式会社アドイン研究所（東京都千代田区）においてグローバルマーケティング支援・リスコミュニケーションシステム等の開発・コンサルティングに従事．博士（工学）．

吉浦　　裕（正会員）

1981 年東京大学理学部情報科学科卒業．日立製作所を経て，2003 年より電気通信大学電気通信学部人間コミュニケーション学科勤務．現在，同教授．自然言語処理，知識処理の研究を経て，現在，情報セキュリティ，著作権保護の研究に従事．理学博士．電子情報通信学会，日本セキュリティ・マネジメント学会，システム制御情報学会，人工知能学会，IEEE 各会員．2000 年日立製作所社長技術賞，2005 年情報処理学会論文賞，2005 年システム制御情報学会産業技術賞，2006 年 IEEE International Conference on Intelligent Information Hiding and Multimedia Signal Processing，Best Paper Award 各受賞．