多重リスクコミュニケータの開発構想と試適用

佐々木 良一[†1,†4] 石井 真之[†1] 日高 悠[†1]
矢島 敬士[†1] 吉浦 裕[†2] 村山 優子[†3]

インターネット社会の進展につれて，リスクが増大してきており，そのリスクをどの程度どのように低減するかが重要な課題になっている．このため，住民などの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が重要になりつつある．しかし，一口にリスクといってもセキュリティやプライバシや開発コストなどお互いに対立する概念に基づくリスクを低減する必要があり，関与者の合意を取りつつ最適な対策の組合せを求めるのは容易でない．このような問題を解決するために，(1) シミュレータや，(2) 最適化エンジン，(3) 合意形成用の表示部などを持つ「多重リスクコミュニケータ」が必要であると考えた．そして，その開発構想を固め，個人情報漏洩防止問題に試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が明確になったので報告する．

Developments Design on "Multiplex Risk Communicator" and Its Trial Application

Ryoichi Sasaki,[†1,†4] Saneyuki Ishii,[†1] Yuu Hidaka,[†1]
Hiroshi Yajima,[†1] Hiroshi Yoshiura[†2] and Yuuko Murayama[†3]

Along with progress of an Internet society, the risk is increasing and it has been an important subject how the risk is reduced and how much. For this reason, the risk communication for forming agreement among decision-making persons, such as residents, is becoming important. However, it is not easy to search for the combination 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 "multiplex risk communicator" with the function of which are (1) simulator, (2) optimization engine, and (3) displaying the computed result to decision-making persons. Developments design of "multiplex risk communicator" and its application to private information leakage issue is shown in this paper.

1. はじめに

DDoS（Distributed Denial of Service）攻撃や各種ワームの被害などによりセキュリティ対策に対する関心が高まっている．また，個人情報保護などのためのプライバシ対策も強い関心を呼んでいる．

セキュリティ対策というとプライバシ対策そのものと思い込んでいる人も少なくない．しかし，セキュリティ対策とプライバシ対策は，文献 1) で明らかにしたように，(1) 両立，(2) 対立の 2 つの関係があり，特に，対立する場合は，セキュリティやプライバシに，コストや使いやすさも含め，最適な対策の組合せを検討する必要がある．

一方，最近，リスクについて直接間接に関係する人々が意見を交換し，合意を形成する過程であるリスクコミュニケーションに関する関心も高まってきている[2)〜5)]．従来は，リスクコミュニケーションで扱われるリスクを 1 つのものと考えてきたが，セキュリティとプライバシが対立する場合の例でも分かるように，セキュリティが失われるリスクと，プライバシが失われるリスクの両方を考慮する必要がある．また，使いやすさを運用リスク，開発コストを経済リスクの 1 つと見られないこともない．したがって，リスクコミュニケーションも，これらの多重のリスク（セキュリティが失われるリスクと，プライバシが失われるリスク，運用リスク，経済リスクなど）を考慮しつつ，合意を形成できるようにすることが必要になっていくと考え

†1 東京電機大学
Tokyo Denki University
†2 電気通信大学
The University of Electro-Communications
†3 岩手県立大学
Iwate Prefectural University
†4 社会技術研究システムミッション II 研究員
Researcher of RISTEX Mission 2

られる．

上記のような目的を達成するため，「多重リスクコミュニケータ（Multiple Risk Communicator：以下MRCと略記する場合もある）」の開発構想を固めた．本稿では，「多重リスクコミュニケータ」のあるべき機能，開発計画，試適用結果などを述べる[7]．

2. 多重リスクコミュニケータの必要性

2.1 リスク関連の用語

英語のRiskが登場するのは1660年代でハザードや災いを意味するイタリア語risicoからの転用であるといわれている[2]．なお，risico自体はガリオン船に乗るスペイン人の水夫が険しい岩礁をriscoといったことから生じた言葉のようである[2]．

リスクの定義はいろいろあるが，危険やハザードが「被害や損害そのもの，またはそれが起こりうる状態（文献3)のp.1)」と確定的な状態を表すのと異なり，確率の概念を含むのが特徴である．日本工業規格によると次のように定義している．

「リスク（Risk）：事象の発生確率と事象の結果の組み合わせ.」（文献13)のp.15）

特に，原子力工学などの分野では，不安全事象の発生確率とそれによって生じる損害の大きさの積をリスクという場合が多い（文献4)のp.21）．

また，リスクマネージメント（Risk Management）とは，日本工業規格によると「リスクに関して組織を指揮し管理する調整された活動である」とし，「一般にリスクアセスメント，リスク対応，リスクの受容及びリスクコミュニケーションを含む」とされている（文献13)のp.16）．

ここで，リスクコミュニケーション（Risk Communication）とは，同じく日本工業規格によると「意思決定者と他のステークホルダーの間における，リスクに関する情報の交換又は共有」と定義されている（文献13)のp.17）．また，U.S.NRCの定義によるとリスクマネージメントの一部をなし「個人とグループ，そして組織の間で情報や意見を交換する相互作用的過程である.」とされている（文献11)のp.21．原典は文献12)）．

リスクコミュニケーションが重要になってきた背景には，市民および行政・事業者における，(1) 民主主義を支える公民権，(2) 自己決定権，(3) 知る権利，(4) 説明責任，(5) インフォームドコンセント (6) 情報公開などの思想や機運の高まりがあるといえるだろう．

2.2 対立するリスク

セキュリティとプライバシの関係を概念，手段，技術のそれぞれで表すと**図1**に示すようになると考えられる[1]．

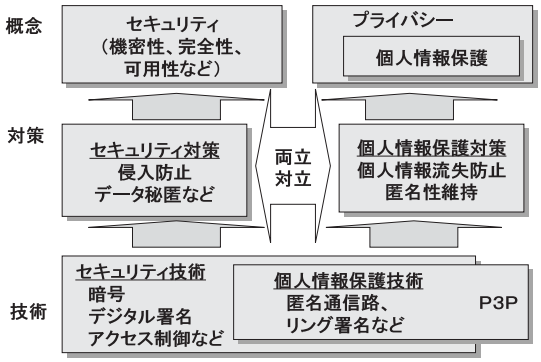

図1 セキュリティとプライバシー
Fig. 1 Security and privacy.

表1 セキュリティ対策と個人情報保護の関係
Table 1 Security measure and personal information protection.

No	関係		例
	分類	説明	
1	両立	セキュリティ対策が個人情報保護の手段	FWなどの不正侵入対策が個人情報の流失を保護
2	対立	セキュリティ対策と個人情報の保護の一方を実現しようとすると他方の成立が困難	(a)個人情報の保護が不正者の追跡を困難にする (b)暗号化メールを許すことが、個人情報の流失を見逃す (c)デジタル証明書の情報から個人情報が知られる

セキュリティ対策とプライバシ対策の関係は，**表1**に示すように，(1) 両立，(2) 対立に大別することが可能であろう．

以下それぞれについて説明を加えていく．

(1) 両立：個人情報流出防止対策の場合は通常，侵入防止やデータ秘匿などのセキュリティ対策を行うことが個人情報の保護につながる．たとえば，第三者が外部から不正侵入して個人情報を持ち出すのに対し，ファイアウォールを設置するなどのアクセス制御技術を用いることにより個人情報の流出を保護できる．また，ネットワーク上での個人情報の盗み見を防止するためにデータを秘匿するなどの対策も考えられるさらに，入退出管理などの物理的セキュリティ対策を実施することにより，内部の人間が個人情報を不正に持ち出すのを防止しできるこれらは，いずれも基本的なセキュリティ対策である

(2) 対立：セキュリティ対策の実施が個人情報の保護を困難とする場合であり，従来あまり検討されてこなかったものである．たとえば，(a) セキュリティ対策

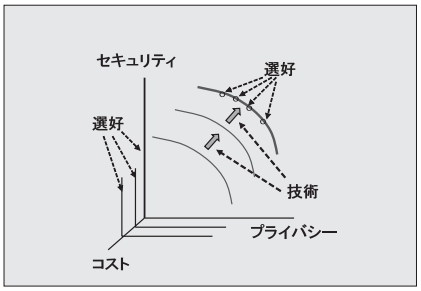

図 2 対立概念解決方法のイメージ
Fig. 2 Image of method to solve opposing concept.

のための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，こ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るとの指摘もある．また，(b) 第三者からの脅威に対するセキュリティ対策として暗号化メールを許すことが，個人情報の流出のチェックを不可能にする場合もありうる[6] さらには，(c) 個人情報保護対策を採ることが，不正侵入の追跡性をなくさせ，社会としてのセキュリティを弱めることになる可能性がある．

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 2** に示すように技術は十分貢献できる．

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，公開鍵証明書を使う場合に比べて，安全性や使い勝手では劣るといえよう．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，意思決定者の選好の問題となる．

このように，セキュリティやプライバシにコストや使いやすさも含め，最適の対策の組合せを意思決定者との合意をとりつつ決定していくためのツールは不可欠となる．

3. 多重リスクコミュニケータの開発構想

3.1 多重リスクコミュニケータへの要求

上記のような理由から，開発することとした多重リスクコミュニケータであるが，次のような要件を満足する必要がある．

(要求 1) 対立する多様なリスクがあり，それらを考慮しつつ対策を考える必要がある．

(要求 2) 個別のリスクに対しても多様な対策が必要であり，1 つの対策ですべてを解決することはできず，多くの対策の最適な組合せを求める機能が不可欠である．

(要求 3) 意思決定を行うためには多くの関与者（たとえば，経営者，市民，顧客，従業員）が満足するものであることが望ましい．したがって，多関与者間で行うリスクコミュニケーションを支援する機能が不可欠である．

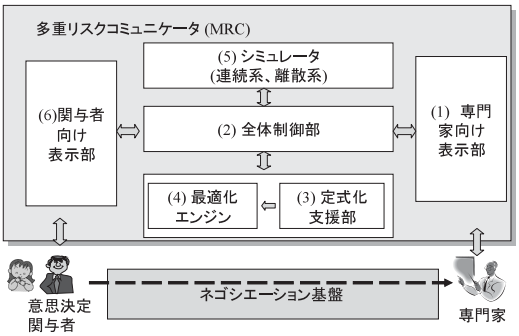

図 3 多重リスクコミュニケータの概要
Fig. 3 Overview of multiple risk communicator.

3.2 多重リスクコミュニケータの構想

このような要件を満足する多重リスクコミュニケータとして，**図 3** に示すようなものを開発することとした．

多重リスクコミュニケータは，次の 6 つの部分で構成すべきであると考えた．

(1) 専門家向け表示部
(2) 全体制御部
(3) 定式化支援部
(4) 最適化エンジン
(5) シミュレータ
(6) 関与者向け表示部

多重リスクコミュニケータへの（要求 1）「対立する多様なリスクがあり，それらを考慮しつつ対策を考える必要がある」と（要求 2）「個別のリスクに対しても多様な対策が必要であり，1 つの対策ですべてを解決することはできず，多くの対策の最適な組合せを求める機能が不可欠である」を満足するための基本機能を実現するのが，(3) 定式化支援部と (4) 最適化エンジンである．ここでは，各種対策案を $0-1$ 変数とする離散型最適化問題（$0-1$ 計画問題ともいう）[9] として定式化し，求解することを前提としている．

また，(要求 3)「意思決定を行うためには多くの関与者が満足するものであることが望ましい．したがって，多関与者間で行うリスクコミュニケーションを支援する機能が不可欠である」を満足するためのものが，(1) 専門化向け表示部，(5) シミュレータ，(6) 関与者向け表示部である．シミュレーションなどを行い，対

策結果を詳細に示すとともに，専門家や，関与者が判断しやすく表示することができるようにしなければならない．

そして，これらの各部分の処理をつなぐのが，(2) 全体制御部である．

なお，著者らの当初の検討[7] では，(1) の専門家向け表示部を明示的に扱っていなかったが，その後の検討で適切な定式化を行うために，重要であると考え導入したものである．

3.3 多重リスクコミュニケータの利用イメージ

（ステップ①）専門家が，(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，最適化問題として定式化する．((1) 専門家向け表示部，(2) 全体制御部，(3) 定式化支援部を利用)．

ここでは，各種対策案を 0－1 変数とする最適化問題として定式化することを前提とする．各対策案の最適な組合せを求めるためには，このような方法が，最も定式化が容易だからである．

具体的な定式化は対象によって異なるが，たとえば，**図 4** に示すようにコストやプライバシセキュリティに関するリスク制約の下にソーシャルトータルコストを最小化する方法などがよいと考えている．

そして，ここでは，第 1 最適解だけでなく，第 2，第 3，$\cdots$ 第 L 最適解も求めるように定式化している．これは，どうしても定量化できない要因を考慮しつつ，第 1 から第 L 最適解の中から，関与者が満足できる解を選択できるようにするためである．

コストに関する制約式はコストモデルを作成し，個々の対策案のコストを求めたうえで，以下のように表現することにより記述できる．

$$\sum_{i=1}^{n} C_i \cdot X_i \leqq C_t \qquad (1)$$

ここで，C_i は対策案 i のコスト，C_t はトータルコストの制約値を表している．また，X_i は 0－1 変数であり，1 ならば対策案 i を採用，0 ならば不採用であることを表している．

また，セキュリティリスク関数や，プライバシリスク関数は，フォルトツリー分析法[8] などを用いて個々の対策案を求めたうえで，それらの関数として表現すればよいと考えている．

（ステップ②）対策案の第 1 －第 L 最適組合せを (4) 最適化エンジンを用いて求める（例：対策案 1 と 3 の組み合わせが第一最適解，1 と 4 の組み合わせが第二最適解など）．

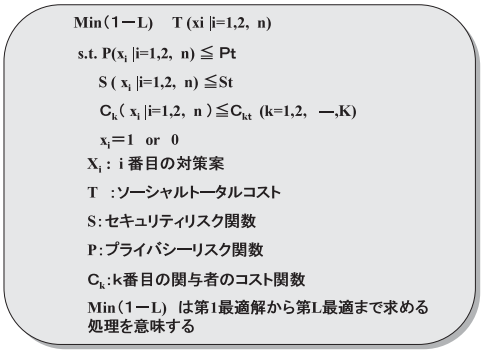

図 4 定式化結果のイメージ
Fig. 4 Image of formulated result.

ここで，(4) 最適化エンジンは，定式化された問題の最適解を効率的に求めるための機能を実現する部分であり，以下のような手法の採用が考えられる[9]．

(a) 総当り法（ブルートフォース法）：対策案の数が少ない場合．

(b) 厳密解法（辞書式枚挙法など）：対策案の数が比較的多い場合．この方法は，総当り法をベースにし明らかに最適解になりえないものを効率良くスキップしていこうとするものである．

(c) 近似解法：対策案の数が多い場合．最適解である保証はないが最適解に限りなく近いものを効率良く求める解法である．

いずれも，従来は第 1 最適解を求めるためだけに開発されたものであるが，少し工夫することによって，第 1 －第 L 最適解を求めるようにできると考えている．

（ステップ③）この結果を (5) シミュレータや (6) 関与者向け表示部を用いて分かりやすく表示する．

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．

このようなシミュレーションを実施するのに最も使いやすいと考えられるシステム・ダイナミックス[10] をベースにプログラムを開発する予定である．

(6) の関与者向け表示部は，住民や従業員などの意思決定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順序の工夫が必要となる．

（ステップ④）それぞれの関与者が，「制約条件値が違う」とか「もっと別の対策案が考える」などの意見をいう．

（ステップ⑤）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．

以上の過程を繰り返すことにより，複数のリスクを考慮しつつ，複数の関与者の意見を導入しつつ，お互いが満足できる解に到達する可能性が増大すると考えられる．

3.4 解決すべき課題

多重リスクコミュニケータを現実に適用していくには次のような課題を解決する必要があると考えられる．

(1) 専門家側
- (1 – a) 定式化の困難性
- (1 – b) 効果の不確実性

(2) 意思決定者（一般市民など）側
- (2 – a) 制約条件のあいまい性
- (2 – b) 非定量的要因の勘案
- (2 – c) 1 人の関与者が満足する解に早く到達させる方法
- (2 – d) グループ間の解の不一致の解消

これらはいずれも困難な課題である．しかし，大切な課題であり，試適用を通じて少しずつ解決していく必要がある．

4. 試適用と考察

4.1 適 用 対 象

多重リスクコミュニケータについては，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，簡単なプロトプログラムを作り，それを複数の対象に適用しつつ，方式自体の改善を図り，次のプロトプログラムを作るというアプローチを採用した．

多重リスクコミュニケータの適用手順は，**図 5** に示すとおりであり，若手研究者が適用を実施した．ここで，事前準備というのは，3.3 節のステップ①で述べた多重リスクコミュニケータ内で定式化を行うための準備作業である．

ここでは「個人情報の漏洩問題」を扱うこととし，以下の前提で適用を行うこととした（図 5 の①，②に対応）．

(1) 個人情報漏洩が起こる会社の組織概要は大手プロバイダサービス会社．
(2) 所有する個人情報は百万件とする．
(3) 個人情報の価値は 1 件あたり 1 万円．
(4) 個人情報は (a) 内部不正者により漏洩する場合と，(b) 外部不正者により情報漏洩する場合および (c) ウイルスによって漏洩する場合の 3 つのパターンを考える．内部不正者ならびに外部不正者の情報の持ち出し方法は，**図 6** に示すとおりとした．
(5) 現状はほとんど対策がなされていないと仮定した．

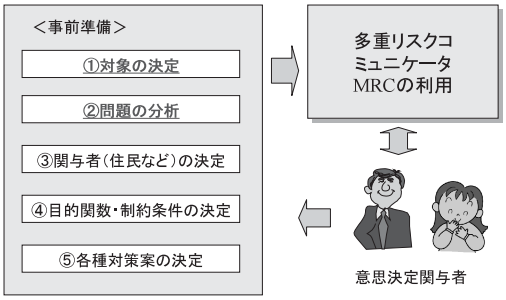

図 5 MRC の個人情報漏洩対策への適用
Fig. 5 Application of MRC to personal information leakage measures.

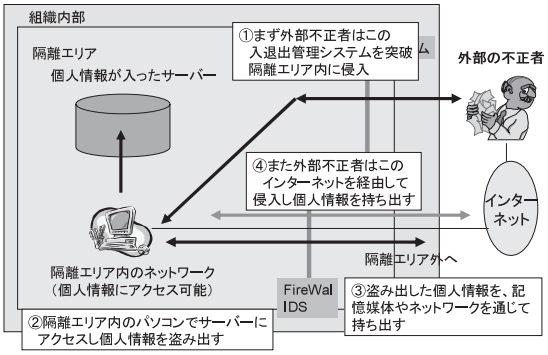

図 6 外部不正者の行動パターン
Fig. 6 Behavior pattern of external unjust person.

4.2 適 用 方 法

図 5 にそって以下，適用を行っていった．③の関与者は，①企業経営者，②企業の従業員，③顧客とした．

④の目的関数，制約条件の決定結果は以下のとおりである．

目的関数：個人情報漏洩リスクと対策コストの和の大きさが，制約条件を満足しつつ 1 番目から 2 番目に小さい対策案の組み合わせを選択する．

制約条件：
(a) 個人情報漏洩確率 $\leqq Pt$
(b) 対策コスト $\leqq Ct$
(c) 従業員の負担 $\leqq Dt$

⑤の対策案は，**表 2** に示す 8 つを選択した．ここでの対策案ごとのコストなどの値は，適用者が表 2 に示すようなものをとりあえず与えた．従業員の負担は，監視などによりプライバシなどが侵されたり，新しい作業などにより手間が増たりする，などによって生じるものであり相対値で与えている．本来は，従業員の

表 2 対策などの決定
Table 2 List of proposal measures.

対策案	ΔP_{oi} (外部)	ΔP_{Ii} (内部)	コスト費(万円) Ci	従業員への負担 Di
1:ファイアウォール(内部から外部へのFTP、Telnetなどの禁止も含む)	0.9	0.9	100	5
2:ウイルス対策(ワクチン)	0.99	--	300	6
3:IDS(侵入検知システム)	0.95	0.95	300	1
4:外部へのメール監視	0.8	0.8	100	8
5:PCセキュリティ(脆弱性の管理)	0.9	0.8	100	1
6:隔離エリア内での外部媒体への保存の管理	0.8	0.8	100	6
7:隔離エリア内への入退出管理システム	0.9	0.1	300	3
8: 隔離エリア内への持ち物検査	0.9	0.5	700	10

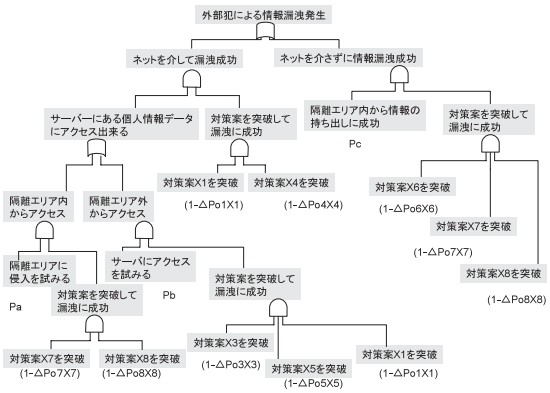

図 7 外部の不正者による情報漏洩に関するフォルトツリー
Fig. 7 Fault tree for personal information leakage caused by external unjust person.

アンケート結果などを用いるべきものである．

外部不正者による情報漏洩が起こるケースは，フォルトツリー[8] を用いて表現すると**図 7** に示すとおりである．この結果に基づき，外部不正者による個人情報漏洩確率は次のように表現できる．

外部不正者による個人情報漏洩確率

$$Po=\{P_{oa}(1-\triangle P_{o7}X_7)(1-\triangle P_{o8}X_8)+ P_{ob}(1-\triangle P_{o1}X_1)(1-\triangle P_{o3}X_3)(1-\triangle P_{o5}X_5)\} *(1-\triangle P_{o1}X_1)(1-\triangle P_{o4}X_4) +P_{oc}(1-\triangle P_{o6}X_6)(1-\triangle P_{o7}X_7)(1-\triangle P_{o8}X_8)$$

ここで，$\triangle P_{oi}$ は，外部からの不正に対する対策案 i の対策効果を表し，X_i は，対策 i を採用するなら 1，しないなら 0 となる 0 − 1 変数である．

内部不正者による個人情報漏洩確率 P_I も同様に以下のように定式化可能である．

$$P_I=\{P_{Ia}(1-\triangle P_{I7}X_7)(1-\triangle P_{I8}X_8)+ P_{Ib}(1-\triangle P_{I1}X_1)(1-\triangle P_{I3}X_3)(1-\triangle P_{I5}X_5)\} *(1-\triangle P_{I1}X_1)(1-\triangle P_{I4}X_4) +P_{Ic}(1-\triangle P_{I6}X_6)(1-\triangle P_{I7}X_7)(1-\triangle P_{I8}X_8)$$

$$Min\,(1-2)\quad 損害額*(\mathrm{Po}+\mathrm{P_I}+\mathrm{P_V})+\sum_{i=1}^{8}\mathrm{Ci}*\mathrm{X}i$$

$$\sum_{i=1}^{8} C_iX_i \le Ct$$

$$\sum_{i=1}^{8} D_iX_i \le Dt$$

$$Po+P_I+P_V \le Pt \qquad (X_i=0,1)$$

係数の値は表2 などで示すとおり

図 8 定式化結果
Fig. 8 Formulated results.

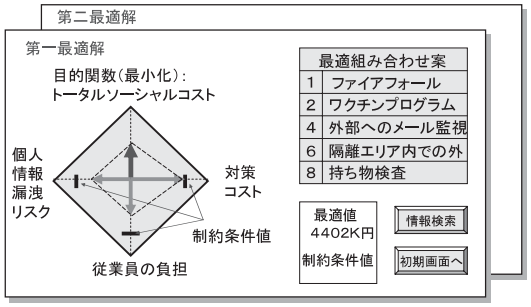

図 9 求解結果の表示イメージ
Fig. 9 Image of displaying obtained solution.

ウイルスによる漏洩確率 P_V は以下のように定式化することができる．

$$P_V = P_d(1-\triangle P_2X_2)(1-\triangle P_5X_5)$$

この結果得られる定式化結果は，**図 8** に示すとおりである．

4.3 Excel を用いた多重リスクコミュニケータ簡易版の開発

これらの定式化結果に基づき，Excel を用いて，制約条件を満足しつつ，目的関数を最も小さくするもの，2 番目に小さくするもの，3 番目に小さくするものの組合せを総当り法により求められるようにした．

ある項目の値（たとえば目的関数値）を小さい順にならべる機能などは，Excel がもともと持っており，制約条件を満足しないものはフィルタリングすることのできるので，Excel を用いて容易に 2 つ以上の最適解を求めることができた．

また，制約条件値を変えて容易に再計算できるので，いろいろなケースで最適解を求めそれを容易に，関与者に示せることも分かった．さらに，Excel は，図の表現機能も充実しているので，比較的分かりやすく表現できると考えられる．

結果の表示については，数値だけであるが，今後，**図 9** のように，目的関数値と制約条件値を図示でき

るようにしようと考えている．

Excel をベースとする場合の第 1 の問題は，対策案の数が多くなった場合の求解時間である．また，今回はシミュレータを使わなかったが，使う場合はシミュレータと組み合わせたい場合の対応方法が問題となる．

4.4 適用結果と考察

Excel ベースの簡易多重リスクコミュニケータを使い，制約条件対策コスト $Ct = 1{,}800$ 万円，従業員の負荷 $Dt = 35$（相対値），個人情報漏洩確率 $Pt = 2\%$の場合の求解結果は，以下のとおりである．

第 1 最適解は，

対策案 1，2，4，6，8 の組合せ

（最適値は 4402180）

第 2 最適解は，

対策案 1，2，3，6，7，8 の組合せ

（最適値は 6228045）

実際に実施したのはここまでである．今後，関与者の意見を入れつつ，全体として満足する解が得られるか検討していく必要がある．

なお，研究者が，それぞれのロールプレイヤとして試験的に考えたところ，次のような反応があった．

(1) 顧客：「賠償額は 1 万円ではなく 10 万円だ」

(2) 従業員：「負担の増大が大きすぎる．原案の半分に」

(3) 企業経営者：「こんなに対策費用は出せない」など

これらに対し，種々に条件を変えて，演算し，たとえば，最終的に次のような皆が満足する解に行き着くことが望ましい．

＜最終的な対策組合せ決定までのイメージ＞企業経営者の「対策費用を 3 割増やすので，従業員の負担も原案の 2 割減で了解してくれ」という申し出に，そのケースを，多重リスクコミュニケータを用いて演算し，その表示結果を見て従業員が納得する．

どういう結論に結びつくかの実験は今後の課題である．

以上の適用ならびに検討結果から多重リスクコミュニケータに関し，次のようなことがいえると考えられる．

(1) 3.4 節の課題 (1 – a) 定式化の困難性への対応：定式化などは容易ではないが多重リスクコミュニケータは適用できそうであり，最適解は間違いなく求められそうであるとの意見が適用者から得られた．

(2) 課題 (1 – b) 効果の不確実性，(2 – a) 制約条件のあいまい性への対応：対策効果の不確実性や，制約条件のあいまい性の問題は，関与者がいろいろな意見を言う中で，これらの値を変化させて解を求めることにより，適用者もある程度解消できそうな印象を持ったが，これも今後の実験を通じて確認していく必要がある．

(3) 課題 (2 – b) 非定量的要因の勘案への対応：第 1 最適解だけでなく，第 2—第 L 最適解まで得られる機能は，定式化しきれなかった要因を考慮しつつ，第 1—第 L 最適から解を選択できるので望ましいという意見は，適用者からも得られたが，この点は，多くの利用者に対する実験を通して確認していく必要がある．

(4)(2 – c)1 人の関与者が満足する解に早く到達させる方法，(2 – d) グループ間の解の不一致の解消への対応：条件を変え，すぐに結果を表示できる機能が満足解の収束に有効であるとの意見は強いが，どのような順序でどう見せていくかについては，まだまったく分かっておらず今後の課題である．また，最適解を求めた前提を関与者は知りたがると考えられるが，どのように効率的に見せるかも今後の課題である．

今回，多重リスクコミュニケータの試適用を行う中で以下のような具体的な 2 つの場面で利用できると考えるようになった．

(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．日本全体を対象としたマクロモデルになることが多い．

(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．企業環境を中心としたミクロなモデルとなることが多い．

また，本来はすべての必要機能を盛り込んだ多重リスクコミュニケータプログラムを作ることが望ましいが，Excel をベースとする簡易版でも，かなりのことはできそうであり，Excel ベースの開発の検討も引き続き行うこととした．

5. 終わりに

以上,「多重リスクコミュニケータ」のあるべき機能や開発計画，試適用結果などを述べた．

今後次のようなことを行っていく予定である．

(1) 多重リスクコミュニケータを他の 2，3 の応用例に試適用し，多重リスクコミュニケータが持つべき機能を検証する．

(2) 複数の関与者が納得するための情報の開示の順序や方法の検討を，実験を行いつつ実施する．

(3) Excel を用いた簡易版の適用範囲拡大と，本格版の開発の検討を行う，など．

大変難しい研究テーマであるが，今後対応が不可欠なテーマでもあるので意欲的に進めてゆきたい．

本研究は，応用セキュリティフォーラム（ASF）の安全・安心ワーキンググループの活動の中で着想した

ものであり，科学技術振興機構社会技術研究システムミッションプログラム II「高度情報化社会の脆弱性の解明と解決」の中で検討を深めたものである．

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：セキュリティと個人情報保護の関係に関する考察，電子情報通信学会，信学技報 SITE2003-14, pp.1–6 (2003).
2) ジョン・F・ロス：リスクセンス―身の回りの危険にどう対処するか，集英社新書 (2001).
3) http://web.sfc.keio.ac.jp/~hfukui/class/riskmg/risk.pdf
4) 佐々木良一：インターネットセキュリティ入門，岩波新書 (1999).
5) 日本リスク研究学会（編）：リスク学事典，TBS ブリタニカ (2000).
6) 安 健司，赤羽泰彦，佐々木良一：個人情報不正送出チェック機能を持つ暗号メールの構想と基本部の開発，コンピュータセキュリティシンポジウム CSS (Oct. 2003).
7) 佐々木良一：多重リスクコミュニケータの開発構想，電子情報通信学会，SCIS2004 (2004).
8) McCormic, N.J.: Reliability and Risk Analysis, Academic Press Inc. (1981).
9) Gerfinkel, R.S., et al.: Integer Programming, Wiley and Sons (1972).
10) 小玉陽一：システム・ダイナミックス入門―複雑な社会システムに挑む科学，講談社ブルーバックス (1984).
11) http://web.sfc.keio.ac.jp/~hfukui/class/riskmg/risk5_23.files/frame.htm
12) http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0308/#chapter_1
13) JIS ハンドブック 58-4 リスクマネージメント 2005，日本規格協会 (2005).

(平成 16 年 11 月 25 日受付)
(平成 17 年 6 月 9 日採録)

佐々木良一（フェロー）

昭和 46 年 3 月東京大学卒業．同年 4 月日立製作所入所．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．同研究所第 4 部長，セキュリティシステム研究センタ長，主管研究長等を経て平成 13 年 4 月より東京電機大学工学部教授．工学博士（東京大学）．平成 10 年電気学会著作賞，平成 14 年情報処理学会論文賞など受賞．著書に，『インターネットセキュリティ』（オーム社，1996 年），『情報セキュリティ事典』（代表編，共立出版，2003 年），等．IEEE，電子情報通信学会等の会員．情報処理学会フェロー．日本セキュリティ・マネージメント学会常任理事，IFIP TC11 日本代表．

石井 真之（正会員）

平成 15 年東京電機大学工学部一部情報通信工学科卒業．平成 17 年同大学大学院工学研究科情報通信工学専攻修士課程修了．同年日本電気株式会社入社．現在，ユビキタスソフトウェア事業部に勤務．

日高 悠（学生会員）

平成 17 年東京電機大学工学部一部情報通信工学科卒業．現在，同大学大学院工学研究科情報メディア学専攻修士課程に在籍．情報セキュリティに関する研究に従事．

矢島 敬士（正会員）

昭和 50 年京都大学大学院工学研究科修士課程精密工学専攻修了．同年（株）日立製作所システム開発研究所入所．昭和 56 年から 1 年間 MIT 客員研究員．平成 11 年同社同研究所主管研究員兼情報センター長．平成 16 年東京電機大学大学院工学研究科情報メディア学専攻教授（工学博士）．平成 11〜14 年まで，東京工業大学客員教授．知識応用システム，ユーザ・インタフェース，ネットワーク上のコミュニーション・システムの研究に従事．現在，IEEE Reliability Society Technical Operations (IndustrialSystems) chair，ヒューマンインタフェース学会理事．

吉浦　裕（正会員）

昭和 56 年東京大学理学部情報科学科卒業．同年日立製作所入社．日立研究所，システム開発研究所勤務．平成 15 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助教授．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，システム制御情報学会，人工知能学会，IEEE 各会員．平成 2 年情報処理学会学術奨励賞，平成 16 年度情報処理学会論文賞，平成 17 年システム制御情報学会産業技術賞受賞．

村山　優子

津田塾大学学芸学部数学科卒業．三菱銀行および横河ヒューレット・パッカード社に勤務．昭和 59 年 University College London 大学院理学部計算機科学科修士課程修了．平成 2 年同大学大学院博士課程修了．Ph.D.（ロンドン大学）．慶應義塾大学環境情報学部非常勤講師を経て，平成 6 年 4 月より広島市立大学情報科学部情報工学科講師，平成 10 年 4 月より岩手県立大学ソフトウェア情報学部助教授．平成 14 年 4 月より教授．現在に至る．インターネット，ネットワークセキュリティの研究に従事．IEEE，ACM，電子情報通信学会，映像情報メディア学会，日本 OR 学会，情報知識学会各会員．