3. 脆弱性問題を解決するための多重リスクコミュニケータ

東京電機大学
佐々木 良一　sasaki@im.dendai.ac.jp

インターネット社会の進展につれて，脆弱性やリスクが増大してきており，それら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ー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．

はじめに

社会や企業はいろいろな脆弱性（Vulnerability）を抱えている．ここで，脆弱性とは，日本工業規格によると，「脅威によって影響を受ける資産または資産グループの弱さ」と定義されている[1]．一方，リスク（risk）は，「ある脅威が，資産または資産グループの脆弱性を利用して，資産への損失，または損害を与える可能性」と定義されている[1]．したがって，社会や企業はいろいろなリスクを抱えているということもできる．

たとえば，企業においては，図-1 に示すような，さまざまなリスクがある[2]．

そこには，利益を上げるために積極的にとるべきリスク以外に，情報セキュリティリスクや，プライバシーリスク（個人情報漏洩リスクなど），コンプライアンスリスクなどのような派生的リスクもある．

脆弱性の影響を無視できるようにし，脆弱性問題を解決するためには，これらのリスクを低減するための対策を実施していくことが必要になるが，1 つの対策だけでは，通常，各種のリスクを十分小さくすることはできない．また，それぞれの対策は，これらのリスクに対し，プラスに作用する場合もあれば，マイナスに作用する場合もある．したがって，いくつかの対策の最適な組合せを求める手法が必要になってくる．

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（Risk Communication）に関する関心も高まってきている[3]．従来は，このリスクを 1 つのものと考えてきたが，上記の例に示すように多くのリスクがある．したがって，リスクコミュニケーションも，多重のリスクを考慮しつつ，最適な対策組合せに関する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られる．

上記のような目的を達成するため，著者らは「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）」の開発構想をまとめ試適用を行った[4]．多重リスクコミュニケータは，情報化社会の脆弱性の問題を解決するのに役立つと思うので，

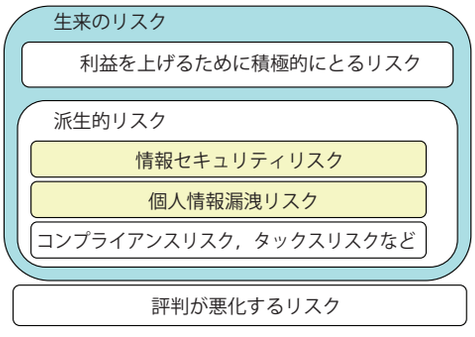

図-1　企業経営と種々のリスク

その構想や試適用の結果，脆弱性問題の解決方法の検討などを述べる．

多重リスクコミュニケータの必要性

◆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 [5]．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 [5]．

リスクの定義はいろいろあるが，確率の概念を含むのが特徴であり，「事象の発生確率と事象の結果の組合せ」という定義もある（文献 6）の p.15）．

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，リスクの受容およびリスクコミュニケーションを含む」とされている（文献 6）の p.16）．

ここで，リスクコミュニケーションとは，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または共有」と定義されている（文献 6）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 7）の p.21. 原典は文献 8））．

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．

◆対立するリスク

セキュリティとプライバシーの関係を概念，対策，技術のそれぞれで表すと図 -2 に示すようになると考えられる [4]．

セキュリティ対策とプライバシー対策の関係は，「両立」，「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．

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

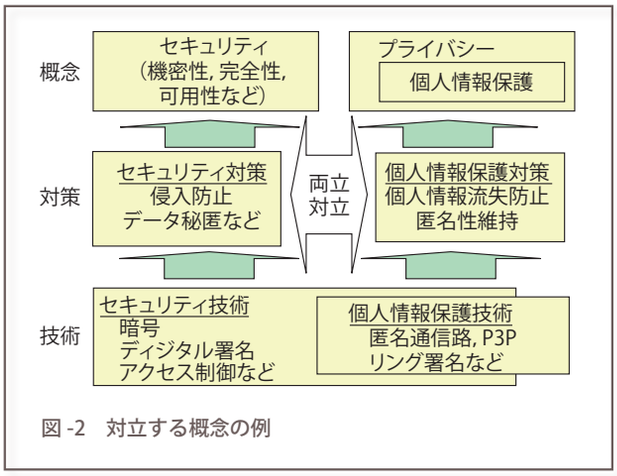

図 -2　対立する概念の例

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．

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）セキュリティ対策のための暗号化やディ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得る．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ー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 -3 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ー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ー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，プライバシー，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ーにコストや使いやすさも含め，最適な対策の組合せを意思決定者と

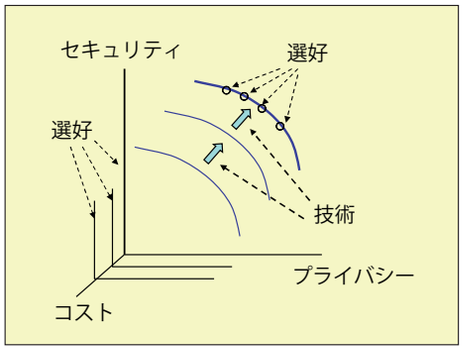

図 -3　対立概念解決方法のイメージ

の合意を取りつつ決定していくためのツールは不可欠となる．

多重リスクコミュニケータの開発構想

◆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．

◆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 -4 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) 専門化向け表示部
(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）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

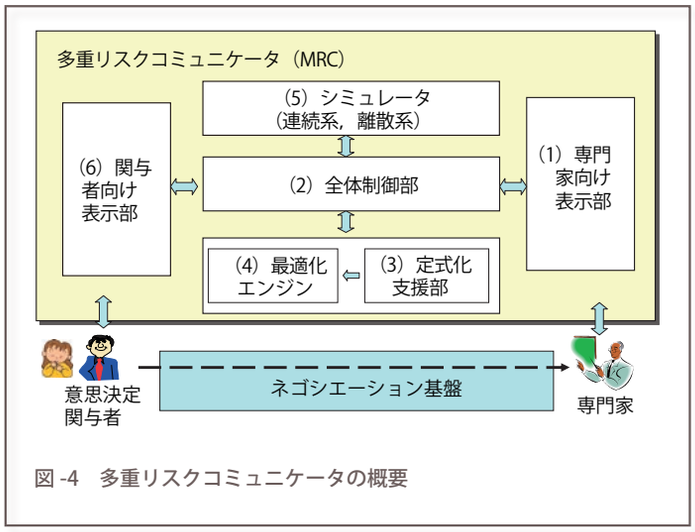

図 -4　多重リスクコミュニケータの概要

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．

◆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）専門化向け表示部，（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 -5 に示すようにコストやプライバシー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, …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上で，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，プライバシーリスク関数は，フォルトツリー分析法 [10] などを用いて個々の対策案を求めた上で，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 の組合せが第 1 最適解，1 と 4 の組合せが第 2 最適解など）．

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 [11]．

Min (1－L)　$T(x_i \mid i = 1, 2, n)$
s.t. $P(x_i \mid i = 1, 2, n) \leqq Pt$
　$S(x_i \mid i = 1, 2, n) \leqq St$
　$C_k(x_i \mid i = 1, 2, n) \leqq C_{kt}$ $(k = 1, 2, \ldots, K)$
　$x_i = 1$ or 0
X_i : i番目の対策案
T : ソーシャルトータルコスト
S : セキュリティリスク関数
P : プライバシーリスク関数
C_k : K番目の関与者のコスト関数
Min (1－L) は第1最適解から第L最適まで求める処理を意味する

図 -5　定式化結果のイメージ

- 総当り法（ブルートフォース法）：対策案の数が少ない場合．
- 厳密解法：対策案の数が比較的多い場合．辞書式枚挙法などがある．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得ないものを効率よくスキップしていこうとするものである．
- 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よ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 [12] 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）関与者間で合意を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られる」などの意見を言う．

ステップ⑤

この結果は，ネゴシエーション基盤（二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．

試適用と考察

◆適用対象

ここでは「個人情報漏洩問題」を扱うこととし，以下の前提で適用を行うこととした．

(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 件当たり 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．

また，関与者は①企業経営者，②企業の従業員，③顧客，とした．

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」というトータル社会コスト

制約条件：

（a）個人情報漏洩確率≦ Pt
（b）対策コスト≦ Ct
（c）従業員の負担≦ Dt

ここでは，目的関数を最小にするものだけではなく 2 番目，3 番目に小さくするものも求めるようにしている．

対策案は，(1) ファイアウォールの設置，(2) IDS（侵入検知システム）の設置，(3) 外部へのメールの監視，(4) PC ソフトのセキュリティパッチ，(5) 隔離エリア内での外部媒体への保存の管理，(6) 隔離エリア内への入退出管理システム，(7) 人手による隔離エリア内での持ち物検査などを選択した．

この具体的適用方法と適用結果については，文献 9) を参照願いたい．この適用により，多重リスクコミュニケータの基本的な有効性が確認でき，情報化社会の脆弱性問題などの解決に適用できるだろうと考えている．具体的には以下の 2 つの場面で利用できると考えるようになった．

- 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．
- 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．

おわりに

以上，「多重リスクコミュニケータ」のあるべき機能や，「個人情報漏洩問題」への試適用結果などを述べた．

今後，不正コピー防止対策や，住民基本台帳システムの計画問題など，意見の対立の強いものに適用するとともに，リスクコミュニケーションの過程を，ロールプレイヤーを設け実験していく予定である．

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)「JIS ハンドブック 67-1　情報セキュリティ」，日本規格協会 (2004).
2) 石井　至：リスクのしくみ，東洋経済新報社 (2002).
3) http://web.sfc.keio.ac.jp/~hfukui/class/riskmg/risk.pdf
4) 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.
5) 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).
6)「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).
7) http://web.sfc.keio.ac.jp/~hfukui/class/riskmg/risk5_23.files/frame.htm
8) http://www.nrc.gov/reading-rm/doc-collections/nuregs/brochures/br0308/#chapter_1
9) 日高　悠，石井真之，佐々木良一：多重リスクコミュニケータの開発構想と試適用（その 2），電子情報通信学会，SCIS2005.
10) McCormic, N. J.: Reliability and Risk Analysis, Academic Press Inc. (1981).
11) Gerfinkel, R. S. et al.: Integer Programming , Wiley and Sons (1972).
12) 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).

（平成 17 年 3 月 30 日受付）