

ネット社会における安全と安心

— 情報セキュリティ論から IT リスク学へ —

Safety and Confidence in Net-Society

From Information Security to IT Risk Science —

佐々木良一

社会の IT システムへの依存の増大に伴い、IT システム関連の安全の問題を従来の情報セキュリティ技術だけで解決するのは困難な時代になりつつある。このため、著者らは不正によるものだけでなく、天災や故障ならびにヒューマンエラーも対象とし、IT システムが扱う情報だけでなく IT システム自体や IT システムが扱うサービスに関連して発生する安全の総合的問題を「IT リスク」と呼び、それを解決するための学問を「IT リスク学」と名づけ、研究を進めてきた。本論文では、最初に IT リスクへの対策が重要となった背景を説明したのち、他のリスクと比べた IT リスクの特徴に関する分析結果を示す。次に、IT リスク学の定義を明確にするとともに、IT リスク学を構成する要素技術を明らかにし、著者らが行っている最近の研究動向を紹介する。

キーワード：IT リスク、リスクマネジメント、リスクコミュニケーション、IT リスク学

With increase of the dependency of society on IT systems, it is becoming difficult to solve safety issues of IT systems based on the conventional information security approach. Therefore, we proposed the concept of “IT risks science” and continued the studies to solve comprehensive safety issues caused by not only the injustice but also a natural disaster, failure of hardware and human error, and having the effect not only to information treated by IT systems but also IT systems itself and services treated by IT systems. This paper explains the necessary background of measurers against IT risk, and then shows analytical results of the IT risk characteristics compared with other risks. Next, the author makes the definition of IT risks science clear, clarifies the elemental technologies to constitute IT risks science, and introduces the recent trend of the IT risks science.

Key Words: IT Risk, Risk management, Risk Communication, IT Risks Science

1. はじめに

IT (Information Technology) システムの機能が失われると社会活動に大変な影響を与えるようになって来ている現状で IT システム関連の安全の問題を従来の「情報セキュリティ」の概念だけで解決するのは 2.1 節に述べるような理由により困難になりつつある。

このため、著者らは①不正によるものだけでなく、天災や故障ならびにヒューマンエラーも対象とし、② IT システムが扱う情報だけでなく IT システム自体や IT システムが扱うサービスに関連して発生する安全の総合的問題を「IT リスク」と呼び、それを解決するための学問を「IT リスク学」と名づけた。そして、「IT リスク学」の発展のために、日本セキュリティ・マネジメント学会の中に「IT リスク学研究会」を 2008 年 5 月に設立し、IT リスク学の定義を明確にするとともに、IT リスク学を構成する要素技術を明らかにし、リスクコミュニケーションを中心に技術開発や支援システムの開発を行ってきた。

リスクそのものに関する研究は国内外で広く行われてきた⁽¹⁾。しかし IT リスクに関する研究は少なく、それを IT リスク学として確立しようという試みは海外にもなかった。そのため、海外の類似のアプローチを調査し、それを日本に適合するようにしていくというアプローチができず独自に確立していく必要があった。

本論文では、最初に IT リスクへの対策が必要な背景や、IT リスクの特徴、必要となる対応方法に関する考察結果を報告する。次に IT システムの安全を確保するための学問である IT リスク学の定義や、IT リスク学を構成する要素技術を明確にする。そして最後に著者らが行っている IT リスク学の最近の研究動向の紹介を行う。

2. IT リスクに関する考察

2.1 なぜいま IT リスクか

社会全体が IT システムに大きく依存する現在、IT システム関連の安全の問題を従来の「情報セキュリティ」の概念だけで扱うのは次に述べるような理由により困難な時代になりつつある。

- (1) IT システムの安全性は、意図的な不正だけでなく、天災やハードウェアの故障、ソフトウェアのバグ、ヒューマンエラーによっても脅かされるが、従来の情報セキュリティではこれらの意図的でない脅威は、ほとんど扱ってこなかった。IT システムに恩恵を受けている人からすると、原因が何であれその機能が失われることの影響は大きい。また、それらの脅威が相互に影響を与える場合もあり、統一的な対応が期待されている。例えば、システムの信頼性をあげるためにデータを 2 重化して保持することが、攻撃箇所が増加に伴うセキュリティの低下につながったりするためこれらを統一的に扱うことが必要になる。
- (2) IT システムの安全の問題は、文献⁽²⁾で指摘するように階層化して検討すべきであり、ここでは次の 3 つの階層に分けて考えることにした (表 1 参照)。

第 1 階層 IT システムそのものの安全

第 2 階層 IT システムが扱う情報の安全

第 3 階層 IT システムが行うサービスの安全

しかし、従来の情報セキュリティでは、第 2 階層が中心で、第 1 階層の IT システムそのものの安全性のうちハードウェアの安全性はほとんど扱われてこなかった。またネットショッピングの安全などの第 3 階層の IT システムが行うサービスの安全問題もほとんど対象外であった。社会を構成する各種のサー

ビスの大部分がITシステムで構成されるようになってきており、ITシステムの安全にとって第3階層を扱うことは不可欠である。ITシステムのサービスの安全まで扱おうとすると、従来の工学的アプローチだけではなく、心理学的なアプローチや社会科学のアプローチも不可欠となる。

以上により、ITシステムの安全の問題に関し、従来と違ったアプローチが必要であるのは確実であり、トラストやニューディペンダビリティという名で研究がおこなわれている⁽³⁾⁽⁴⁾。

このような、ITシステムにおいて広い意味での安全が失われる可能性を、後で詳しく説明する用語である「ITリスク」と呼ぶことにした。

リスクという概念は、「将来の帰結に対する現在における予測」という見方が下敷きになっており、「危険が生じる可能性」を意味する。それなるがゆえにリスクには常に不確実性を伴うという特徴がある。このため「事故や被害や損失の規模だけでなくその発生確率の概念」も入れてリスクの評価を行うことが多い。

著者が、トラストやニューディペンダビリティという概念ではなく、「ITリスク」という名称を採用することにしたのは、安全の問題を扱うには、リスクという概念がもともと持つ不確実性への配慮が不可欠であり、発生確率の概念を積極的に取り入れていかざるを得

ないと考えたからである。

2.2 リスクをめぐる状況

ドイツの社会学者ウルリヒ・ベックが指摘するように、かつて人類は地震などの自然災害や病気などを恐れていたが、現在ではそれらのリスクをコントロールするために開発した科学技術そのものが新たなリスクとして問題になってきている⁽⁵⁾。このような新たなリスクに覆われた社会をベックは「リスク社会」と呼んだ。

また、ドイツの社会学者であるニコラス・ルーマンは文献⁽⁶⁾や⁽⁷⁾によると「コントロールのあるところリスクも増大する」といい、リスク対策を施すことがリスクを低減することにつながることを指摘している。

三上剛史は、原発や新型インフルエンザなどの新しいリスクが損害の深刻さ、補償不可能性ゆえに損失を最小限に抑え保障するというアプローチではなく、潜在的リスクを洗い出し、あらかじめ排除する「警戒」型アプローチが必要となるという。そして、その「警戒」の行為ゆえにリスクと向かいあわざるを得ず、リスク恐怖症を招きがちであり、さらにそれが監視社会を作り出すと指摘する⁽⁸⁾。

ITシステムにおいても、最近の標的型攻撃はスパイ活動を目的とするものであり、米国などはこれを防止するためいかなる報復攻撃も辞さないと言っており、リスクへの対応がここでも新たなリスクを生み出している。

2.3 リスクへの対応困難性に対応方針

リスク社会学者などが指摘するようにリスクを制御するのは限りなく難しい。これはITシステムにおいても同様であり、新しい攻撃方法が次々に出現する中でそれを事前に予測し、制御し、守りきるのは本当に困難である。福島第一原発の事故を経験した今、その難しさを痛感する。これこそが、「リスク問題」は21世紀の最大の課題の1つであるというゆ

表1 ITシステムの安全の階層化
Table 1 Layering of IT System Safety

階層	対象	扱う事故・障害	従来の学問・技術分野	指標
3	ITシステムが行うサービスの安全	発券サービスの停止、プライバシーの喪失など	システム工学 リスク学 社会科学など	プライバシー、ユーザビリティ
* 2	ITシステムが扱う情報の安全	情報のCIA(機密性、完全性、可用性)の喪失	情報セキュリティ	セキュリティ(機密性、完全性、可用性)
1	ITシステムそのものの安全	コンピュータや通信機器の故障	信頼性工学 情報セキュリティ	リアイアビリティ、アベイラビリティ

* 従来情報セキュリティが扱っていた範囲

えんであろう。

しかし、そこにリスクがあるなか、何もしないのが正しい道なのだろうか。第三者であれば、文献⁽⁶⁾でルーマンが言ったとされるように「被害の予期が誰によってどのようになされるかという点に着目し観察を行い」判断すればよいだろう。しかし、当事者は常に決定を要求されるのである。また、ITシステムにおいてはリスクへの対策をしないとわかるとさらに厳しい攻撃が行われ、リスクの増大につながるということもありえる。

したがって、リスク対策が作り出す新しいリスクを考慮しつつ波乗りのような形でリスクマネジメントを実施し続けるしかないのだろうと思う。リスクマネジメントを行う上で大切なのがリスクアセスメントであり評価結果に基づき採用すべき対策を明確にして行く必要がある。リスクアセスメントにあたっては、通常、リスクを「損害の大きさ×損害の発生確率」として定義し、評価するが、これに対しては以下のような批判がある。

- (1) 人はリスクの存在そのものを認識できないのではないのか。
- (2) フランク・ナイトが、確率によって予測できる「リスク」と、確率的事象ではない「不確実性」とを明確に区別すべきである⁽⁹⁾としているように、不確実な状況を認識できたとしてもその事象の発生確率は測定できない場合が多い。
- (3) 事象の発生確率やその損害の大きさを推定できたとしてもそれらの値そのものに不確実性や曖昧性が残る。
- (4) リスクは「損害の大きさ×損害の発生確率」で定義してよいのか。損害が非常に大きなものは発生確率が低くてもその確率に不確実性があるので重点的に対策を考えるべきではないのか。

いずれももっともな指摘である。しかし、先に述べたように人はリスクに直面し判断せざるを得ない場合は少なくない。そして、人

知を超える判断はいずれにしろできないのである。だとすれば(1)の批判にこたえるためにはどのように人知を集めるかが重要になる。これがリスクに関する合意形成を支援する手段であるリスクコミュニケーションが目される背景でもあろう。リスクコミュニケーションにおいてはまず多くの人知を集め、事実を可能な限り確認することが大切である。

しかし、ナイトが指摘したように事故などの発生確率などについて不確実が大きい場合は多い。その場合には事故の発生確率や影響の大きさなどに不確実性が残り客観確率を求めることは困難である。これに関連し「ブラック・スワン」⁽¹⁰⁾の著者であるナシーム・ニコラス・タレブは、「ナイトのリスクと不確実性の区別は本質的ではない。たとえば世界貿易センタービルで働いていた人にとって9・11は確率ゼロのブラック・スワンだったが、そこに突っ込む飛行機に乗っていたテロリストにとっては確率1に近い出来事だった。両者を知っている神がいれば「存在論的リスク」は計算可能かも知れないが、神はいないので、すべての社会現象はナイトの意味で不確実なのだ。」⁽¹¹⁾という。これは卓越した見解であろう。すなわち、すべての確率は各人の主観確率であるといっているのである。

だとすれば事象ごとの発生確率を主観確率として意識的に扱い、この確率などをリスクコミュニケーションによって調整しながら合意を形成していくことによってしかリスクに対応することはできないと思う。したがって、客観的なデータがないことや不確実性を伴うということによって生じる批判(2)–(4)に対しては、リスクコミュニケーションを適切に進めることにより対応していこうというのが私たちの基本的立場である。

ここでリスクに関連する合意形成を行う目的には次の3つがあると考えている。

(目的①) 個人的選択

(目的②) 組織内合意形成

(目的③) 社会的合意形成

これらの目的はITシステムのリスクコミュニケーションにおいても同様である。

2.4 ITリスクの特徴

ITリスクを食品医薬品リスク、廃棄物リスク、放射線での健康リスク、環境リスク、自然災害リスクなどの他のリスクと比べて見てみよう。ここでITリスクとしては2000年問題、個人情報漏洩問題、サイバーテロ、暗号の危殆化、大規模情報システムの故障などを取り上げ分析を行った⁽¹²⁾。この結果、ITは電力やガス、水道、金融などの社会の重要インフラのさらにインフラになっており、ITリスクへの対応の重要性は高いことが明らかになった。また、ITシステムのリスクは、他のリスクと同様に次のような特徴があることが分かった。

(1-1) ゼロリスクは存在しないため、対策のプライオリティ付けをしようとするすると定量的評価が必要となる。

あらゆるものにリスクがあるのでゼロリスクを実現しようとするすると無限のリスク対策が必要となり資金やマンパワーなどの制約から現実的でない。従って合理的プライオリティ付けをしようとするれば、定量的評価が必要となる。特に社会的合意形成のように説明責任の大きいものでは不可欠となる。

(1-2) 多重リスクへの対応が必要である。

エネルギー対策のためにバイオエタノールを採用することが食糧危機につながったように1つのリスクへの対応が別のリスクを引き起こすということ、すなわち「リスク対リスク」あるいは「多重リスク」への配慮がITシステムにおいても不可欠である。

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ーもよくすることはできる。例えば、セキュリティ対策のために用いられる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、公開鍵証明書の代わりに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、やや劣るといえよう。したがってどのような解をとるかについては最終的には意思決定関与者の選好が問題となる。

(1-3) 多くの関与者とのリスクコミュニケーションが大切である。

図1において意思決定関与者が複数おり、それらの間の利害の対立が大きい場合にはリスクコミュニケーションがITリスクに関しても重要となる。たとえば個人情報漏洩対策の場合は、経営者、顧客、従業員など多くの関与者が存在し、顧客のために個人情報漏洩対策を行うことが従業員のプライバシーや労働環境を犠牲にして実施される場合が少なくない。したがって対策に関しそれらの人たちが互いに合意を形成することが望ましい。

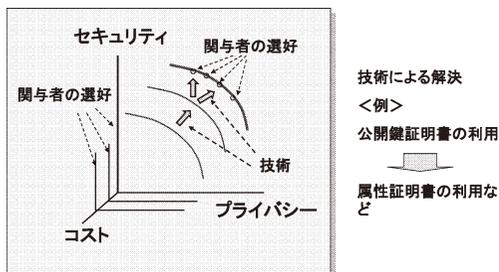
次にITシステムのリスクは他のリスクと比べ次のような特徴があることが分かった。

(2-1) ITリスク対策は1つの対策だけで対応するのは困難であり、いろいろな対策の組み合わせが不可欠である。

ITシステムはソフトウェアにより多様な機能を実現されているため、障害時の影響も多様である。また、ITリスクには意図的な不正も含むため、不正の高度化により、脅威がどんどん大きくなり、対応が難しくなっていく。したがって、1つの対策だけで防止するのは困難であり、いろいろな対策の組み合わせが不可欠である。

(2-2) 組織内合意への適用の重要性が高い。

原子力発電所などを稼働させている組織は限られるのに対し、ITシステムはほとんどの組織が利用しているのも1つの特徴であろう。したがって原子力プラントに関するリス



多くの関与者が異なる嗜好を持つ
(リスクコミュニケーションが重要に)

図1 多重リスクへの対応法

Figure 1 Method of Resolving Opposing Risks

コミュニケーションにおいて組織内合意を必要とする組織は少ないのに対し、ITシステムに関するリスクコミュニケーションは、組織内合意形成へのニーズは広い範囲で存在する。

(2-3) 動的リスクへの対応が重要となる。

個人の不正を対象とするITリスクにおいては、攻撃側の対応が防御側の対応を変え、防御側の対応が攻撃を変化させるといったように相互依存性があり、リスクが動的に変化する。したがってこれらの動的リスクを考慮した評価ができることが望ましい。

3. ITリスク学の提案

3.1 ITリスク学の定義

著者らは、このような問題を解決するため2.4節で述べた特徴(1-1) (1-2) (1-3) (2-1) (2-2) に対応し、対策案の最適組み合わせに関する合意形成を支援するための多重リスクコミュニケーター(以下MRC)を開発し、個人情報漏洩対策などに適用することによって、その有効性を確認することができた⁽¹³⁾。

ITリスクの問題を扱う上でMRCのようなアプローチも必要であるが、MRCでは特徴(2-3)の動的リスクの問題を扱ってはならず研究のさらなる進展も必要となる。またMRCとは違ったアプローチや、その周辺知識も不可欠であると考えるにいたった。一方、ITリスク問題解決のアプローチは既存の単

独の学問領域からだけのアプローチでは不十分であり、学際的アプローチが不可欠であると考えられた。そこで「ITリスク学」という「ITリスク」に関する問題の解決のための学問分野を立ち上げ、多くの研究者の協力の下に問題解決の早期化・効率化を図りたいと考えた。このため2008年5月に日本セキュリティ・マネジメント学会の中に「ITリスク学」研究会を設立した。

リスクそのものに関する研究は国内外で広く行われている⁽¹⁾。国内においては日本リスク研究学会、日本リスクマネジメント学会、日本リスク・プロフェッショナル学会などの学会もあり、統計数理研究所ではリスク研究ネットワークを立ち上げリスク研究者間の討論の場を提供している⁽¹⁴⁾。しかし、ITリスクに関する研究は少なく、それをITリスク学として確立しようという試みは海外にもなかった。そのため、海外の類似のアプローチを調査し、それを日本に適合するようにしていくというアプローチができず独自にITリスク学を確立していく必要があった。

ここで提案する「ITリスク学」は、従来の「情報セキュリティ」、「安全性工学・信頼性工学」、「ソフトウェア工学」などを統合する総合科学であるといえよう。「情報セキュリティ」自体が総合科学と言われており、「ITリスク学」はより広い概念であるので非常に広大なものとなっている。このため、中心的に扱う部分を明確にしていく必要がある。

そこで著者らはITリスク学研究会の中で検討を行い、ITリスク学を、下記のように定義した。

定義「不正によるものだけでなく、天災や故障ならびにヒューマンエラーによって生ずるITシステムのリスクならびにITシステムが扱う情報やサービスに関連して発生するリスクに対し、リスク対策効果の不確実性や、リスク対リスクの対立、関与者間の対立などを考慮しつつ適切に対処し、ITシステムに関

連する安全を確保していくための学際的学問]

(注1) ITシステムのサービスに関するリスクを含むので、セキュリティだけでなく、プライバシー、ユーザビリティなども含む

(注2) 一般的に扱うとあまりにも広くなるので、ITリスクの特徴である「リスク対リスクの対立、関与者間の対立を考慮しつつ」を入れることにより研究範囲を明確にした。

(注3) 「制御する」ではなく「対処していく」にしたのはリスクの完全な制御は不可能であるとの認識に基づく。

(注4) ITリスク学は現実世界において役立つものでなければならないという思いから「ITシステムに関連する安全を確保していく」というのを入れた。

3.2 ITリスク学の構成要素

この定義に基づくITリスク学の構成は、試行錯誤的検討の結果、図2のように考えるのがよいのではないかと現状では思っている。

中心になるのが①「ITリスクマネジメント技術」である。これは狭義のITリスクマネジメント、ITリスクアセスメント、ITリスクコミュニケーションをリスク対リスクの対立、関与者間の対立を考慮しつつ実施し、社会や組織にとって安全なシステムの構築と運用を可能とするためのものである。著者らが開発した多重リスクコミュニケーション MRC はここに含まれるツールである。この部分については、今後も技術開発や適用を積極的に行っていく予定である。

① ITリスクマネジメント技術を支援するものとして、④「ITリスクの考え方」と、「ITリスク基礎技術」がある。④ITリスクの考え方は、ITリスクの特徴や対策の基本的方策に関する検討を行うためのものである。

ITリスク基本技術は、リスク一般への

種々の対応技術に関するものであり、主に、②「リスク社会科学的接近」、③「リスク心理学的接近」、⑤「リスク工学的接近」、⑥「危機管理技術」からなると考えている。

② リスク社会科学的接近には、「リスク社会学的接近」、「経済学的接近」、「経営学的接近」「法学的接近」などがある。リスク社会学的接近には、(イ)ITリスクと社会、(ロ)ITリスクとメディアなどがある。一方、経済学はリスクを積極的に取り込んできた学問であり、リスクのマイナスの側面だけでなくプラスの側面も扱うのが特徴である。経済学の中で最も重要なのは期待効用理論であり、これはITリスク学においても利用しうるものである。その他、経営学的接近や、リスク対策と法やコンプライアンスの問題はこのリスク社会科学的接近に含まれるものであろう。

③ リスク心理学的接近は、人間はITリスクにいかに対応できるかや、適切に対応できるようにするためにはどうすべきかを扱うもので、(イ)ITリスクと人間、(ロ)ITリスクと心理、(ハ)ITリスクの認識、(ニ)ITリスクと過誤などが主要なテーマとなる。奈良由美子によると日本人は、(a)リスクに極めて敏感でゼロリスクを求める傾向、(b)安全よりも安心を重視する傾向、(c)リスクに対しあきらめてしまう傾向があるという⁽¹⁵⁾。(a)(b)と(c)は矛盾するがこのようなリスク感を形成する要因として、日本人は不確実性を回避する傾向が高い、現状肯定的心情があるとしている。このような日本人のリスクに対する特徴も考慮しながら対処していく必要があるだろう。

⑤ リスク工学的接近には、(a)情報セキュリティ技術、(b)安全性・信頼性技術のうちITシステムに関連が深いもの、(c)ソ

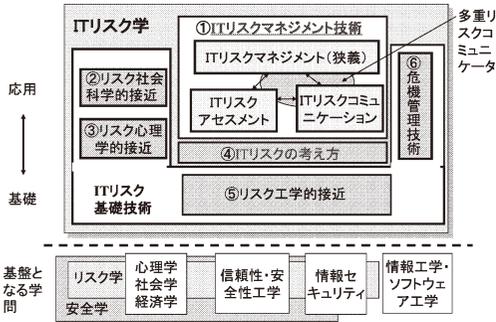


図2 ITリスク学の構成

Figure 2 Structure of IT Risk Science

フトウェア工学のうちソフトウェアの信頼性に関連するもの、(d) IT システムのプロジェクト管理技術を利用するものがある。

- ⑥ 危機管理技術はリスク対策がうまくいかなかった場合に備えるためのものである。障害時に事業を継続するためのBCP (Business Continuity Plan) やBCM (Business Continuity management) などがここに含まれる。この部分をITリスクマネジメント技術に含めることも可能であるが重要性が高く今後発展が期待される分野であるので別の項目とした。

以上、ITリスク学の構成について説明したが、あくまで①を研究の中心に据えるべきであると考えている。④も大切であり、広い視野に立った検討が必要であるが、①の方向づけを適切に行うために実施していくことを忘れてはならないだろう。②③⑤⑥は、研究開発状況をよく把握した上で、①を実現するために必要な範囲で技術開発や接近法の確立を行っていくべきものであると考えている。

4. ITリスク学に関する著者らの研究

4.1 研究の経過

既に述べたように2008年5月に日本セキュリティ・マネジメント学会の中に「ITリスク学」研究会を立ち上げ、以下のような研

究を実施してきた。

- (1) ITリスク学の定義
- (2) ITリスク学の全体像と構成要素の明確化
- (3) 構成要素の概要と研究課題の明確化
- (4) 研究課題の解決に向けての活動
- (5) 「ITリスク学 情報セキュリティを超えて」⁽¹⁶⁾の出版(2013年2月)

このうち、(1)–(3)については3章で説明したとおりである。(5)は研究の中間的成果をまとめたものである。本節では(4)の研究課題の解決に向けての活動を紹介します。特に、図2の①「ITリスクマネジメント技術」のうち著者らが行った研究結果を中心に報告する。

4.2 ITリスクマネジメント技術に関する研究の進展

ITシステムのリスクマネジメントは、(1)政府や地方自治体、(2)企業等の組織、(3)家庭などで必要となる。特に(1)(2)においてリスクマネジメントの重要性が高い。リスクマネジメントは各組織においてPlan-Do-Check-ActのPDCAサイクルの中で運用されている。いずれの過程も大事であるが特に重要となるのがPlanの過程であり、これを適切に行うためには関与者間での合意形成が重要であると考えられる。このうち(1)で必要となるのが社会的合意形成、(2)で必要となるのが組織内合意形成、(3)で必要となるのが個人的選択であろう。

広義のリスクマネジメントは、リスクアセスメント、リスクコミュニケーションそして狭義のリスクマネジメントからなる。本研究では、このうち、2.3節に示した理由によりリスクコミュニケーションが特に重要であると考えており、Planの過程におけるリスクコミュニケーションの研究を中心に行ってきた。

文献⁽¹⁷⁾によるとリスクコミュニケーション自体の研究は1980年代から本格的に実施

されるようになってきたといわれ、米国のナショナル・リサーチ・カウンシルは1989年にリスクコミュニケーションを、「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」と定義しているという。民主主義を支える公民権、自己決定権、知る権利 説明責任、インフォームドコンセント、情報公開と同じ根を持つもので、住民などに情報をきちんと伝えることではじめて、適切な合意が得られるという理念に基づくものであろう。

ここで、リスクコミュニケーションの目的は、すでに述べたように個人的選択、組織内合意、社会的合意の3つに分類される。一方、リスクコミュニケーションにおけるマネジメント主体側の実施項目は次の3つに分類することができるのではないかと考えている。

(実施項目1) 対象となる事象や対象システムそのものの情報やそのリスクに関連する一般的情報の提供

(実施項目2) 対象となる事象や対象システムが受け入れられうるものかどうかの検討のための情報のやり取り

(実施項目3) そのままでは受け入れられないとすれば、どのような対策をとるべきかを定めるための情報のやり取り

ここで、個人的選択では実施項目1が重要

となり、組織内合意では実施項目3が、社会的合意では実施項目2と3が重要になると考えられる。

4.3 ITシステムにおけるリスクコミュニケーションの対象の分類

リスクコミュニケーションの目的（個人的選択、組織内合意、社会的合意）とITシステムの安全の対象（「ITシステム自体の安全」、「ITシステムが扱う情報の安全」、「ITシステムが提供するサービスの安全」）ごとのリスクコミュニケーションの例の検討を行った。その一例は表2に示すとおりである。また、著者らは、個人的選択向けにE-Learningコンテンツ作成支援ツールELSEC⁽¹⁸⁾、組織内合意形成支援用に多重リスクコミュニケーションMRC⁽¹³⁾、社会的合意形成用にSocial-MRC⁽¹⁹⁾を開発してきた。MRCとSocial-MRCについては4.5節で説明を追加する。

4.4 リスクコミュニケーションの課題と対応策

ITシステムを含め各対象のリスクコミュニケーションをうまく実施するためには次のようないろいろな課題を克服していく必要がある。

課題① 専門家の知識への疑問：アスベス

表2 ITシステムのリスクコミュニケーションの対象
Table 2 Objects of Risk Communication for IT System

	ITに関するリスクコミュニケーション例			支援システム	他分野のリスクコミュニケーションの例
	ITシステム自体	ITシステムが扱う情報	ITシステムが行うサービス		
目的① 個人的選択	自己PCのセキュリティホール対策	SNSにおける自己情報の秘匿対策	ネットショッピングのリテラシー	E-Learning 支援 ツール ELSEC	禁煙の実施 インフルエンザワクチン接種
目的② 組織内合意	BCPのためのITのバックアップ対策	オフィスにおける個人情報漏洩対策	ネットショッピング対象の品質維持対策	多重リスクコミュニケーション MRC	工場の環境対策 オフィスの省エネ対策
目的③ 社会的合意	ウイルス作成罪の可否	情報フィルタリングの可否	薬のネット販売の可否	社会的合意形成支援システム Social-MRC	原発再稼働の可否 BSE対策のための全頭検査

ト被害や福島第一原子力発電所の事故に見られるように、多くの専門家が気付かないような災害が起こりうる。これは、ITシステムにおいても同様であり、専門家は常に正しいのかという疑問でもあるだろう。この問題に対しては評価に参加する専門家は最善を尽くすということしかない。

課題② リスク管理者への不信：リスク管理者は、リスクに関する情報をすべて流しているのか、すべて公言したとおりにリスクを管理しているのかという点への疑問の形で現れる。リスク管理者が信頼を獲得するには、中谷内一也が指摘するように自らの意思で自分を他者の目にさらし、何か不誠実な行いが発覚した場合には致命的な処分を自らに課すことを公約する以外にないのだろう⁽²⁰⁾。

課題③ リスクアセスメントの評価基準に関する疑問：リスクアセスメントの評価指標として何を取るかや、指標間のトレード・オフをどのように扱うかは簡単ではない。このようなことであっても合意形成が容易に行える仕組みが必要になる。このための仕組みの一例である MRC を 4.5 節で記述する。

課題④ 客観確率への不信：以下のような理由で客観確率に基づく確率論的アプローチは不毛ではないかという意見もある。

- (1) 未来は過去のように起こるか疑問である。確率は通常、過去のデータに基づいて計算されている。しかし、今後も同じように起こるか疑問である。過去のデータが得られた環境と現状は異なっている場合が少なくない。
- (2) 確率計算のためのデータは得られない場合が多い。このため、条件の異なるデータも確率計算に用いる場合がある。たとえばある疾病の死亡率は年齢によって大幅に異なるが、データ量が少ないと年齢群別ではなく、全体としての死亡率を用いる場合がある。このため無理をして求めた確率が対象となる人に適切なもので

あるかどうか分からない場合がある。

- (3) 上記のような問題が解決されたとしても、個人にとっては、手術の成功率のような確率は直感的に理解しにくい。たとえば、成功確率が 90%だといわれても、患者にとって自分は一人しかおらず、手術が成功するか失敗して死んでしまうかのどちらかである。90%の部分は生き、10%の部分は死ぬというのではない。したがって、客観確率に基づく定量的評価は信じるに値しないという意見もある。

たしかに、これらの意見に見られるように、完全な客観確率は存在しないのだと思う。しかし、定量的評価が有効でないということではない。大切なことは次の 3 点だろう。

- (a) 専門家はできるだけ客観的と思われる事象の発生に関するデータを集める。
- (b) それらをベースに各人は得られたデータをよく検討し自分にとっての事象の発生に関する主観確率を決めていく。
- (c) そして、各人ごとに違った主観確率であっても全体として合意がとれるようなリスクアセスメントやリスクコミュニケーションの方法を確立する。このための方法の一例についても 4.5 節で記述する。

課題⑤ 情報の受け手のバイアスの問題：ここでは、情報の送り手は適切な情報を持っていて、それらの情報を送るが、住民などの受け手が主観的な判断により、バイアスが生じるという考え方をしている。すなわち、住民などの人々のリスク認知は、文献⁽¹⁷⁾によると「主観的な枠組みの中でリスク事態を理解し、個人や社会にもたらすかもしれない危害について予想をかたちづくる心理的なプロセス」であるといわれている。このため、「客観的なリスク情報（客観リスク）は、個人や社会に到達した段階でスクリーニングされる。その過程を経た後個人や社会に受容されたリスク情報（主観リスク）は一定のゆがみ

(バイアス)を持つ。」とされている。また、文献⁽¹⁷⁾によるとベネットは、(1)非自発的なリスクにさらされる場合、(2)不公平に分配されている場合、(3)個人的な予防行動では避けることができない場合、(4)よく知らないもの、あるいは新奇なものなどは、リスクを過大評価し、怖いと思うことが多いと言っているという。

しかし、このような主観的な判断を客観的でないという理由により否定するのは適切ではない。粘り強い情報提供を続けたいうえで、多くの関係者の主観的判断をベースに合意形成できるようにして行く必要がある。このための方法についても4.5節で記述する。

4.5 リスクコミュニケーション支援システムの開発

ITシステムのリスクコミュニケーションを支援するために著者らは次の2つのツールの開発を行った。

- ① 組織内合意形成支援用：多重リスクコミュニケーション MRC (Multiple Risk Communicator)
- ② 社会的合意形成支援用：社会的合意形成支援システム Social-MRC

4.5.1 多重リスクコミュニケーション MRC の概要

ここでは多重リスクコミュニケーション MRC⁽¹³⁾⁽²¹⁾について説明を追加する。MRCの適用対象としてはすでに述べたように(a)BCPのためのITバックアップ対策、(b)オフィスにおける個人情報漏洩対策、(c)ネットショッピングにおける品質維持対策などが考えられる。ここではどのような対策をとるべきかを定めるフェーズが重要であり、定量的分析・評価と結び付ける要求が強く、リスクコミュニケーションは組織内の関係者とユーザなどの外部の人の代表あるいはロールプレイヤーの間で行われることが多いと考える。

MRCの開発の要求と対応については、図

3に示すとおりであり(要求1)(要求2)に対応するため、多くのリスクやコストを制約条件とする組み合わせ最適化問題(最適組み合わせ問題ともいう)として定式化し、(要求3)に対応するため関係者の合意が得られるまでパラメータの値や制約条件値を変えつつ最適化エンジンを用い求解を行い、その結果をわかりやすく表示できるような機能を持たせることとした。

なお、MRCは、4.4節の課題③-⑤に以下のように対応したものとなっている。

課題③ リスクアセスメントの評価基準に関する疑問：目的関数をトータルコスト、制約条件を各関係者の評価指標(例えば、個人情報漏洩対策なら経営者にとっての対策コスト、顧客にとっての情報漏えい確率、従業員にとっての利便性指標)で表し、それぞれの制約条件を変化させた場合の対策案の最適な組み合わせを求められるようにすることによって、基準の変化を考慮しつつ合意形成を容易にしている。

課題④ 客観確率への不信：すべては客観データに基づく主観確率であるという前提の上で、各主観確率に基づく対策案の最適な組み合わせを知った上で合意を形成するので客観確率である必要がない。

課題⑤ 情報の受け手のバイアスの問題：バイアスがあるというのを前提に、お互いの主観的意見を出し合うことにより合意形成を行うので、バイアスがあることが問題にならない。

このためのプログラムはWindows-XP上に実装されており、JAVAやPHPで約1万ステップからなる。そして、専門家向け入力部、演算部、関係者支援部、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されている。このMRCの利用者としては、MRCの専門家や、複数の意思決定関係者と、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。

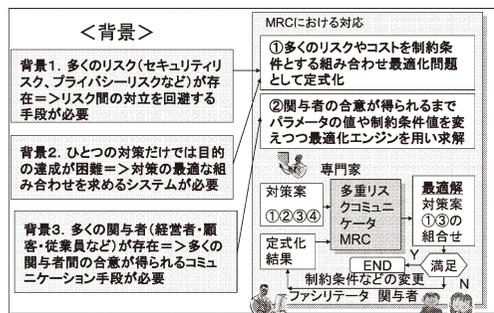


図3 多重リスクコミュニケーター (MRC) の概要
Figure 3 Overview of Multiple Risk Communicator

著者らは MRC を、各種の個人情報漏洩問題⁽²²⁾や、内部統制問題⁽²³⁾、証拠性保全問題⁽²⁴⁾など 10 件に適用し、基本的有効性を確認することができた。10 件の適用中 9 件は合意に達しており予想以上に合意が取れることが確認できた。議論の過程における参加者同士の信頼感の向上や、個別の意見は違っても採用される対策案の組み合わせに含まれる対策案は共通のものが多いことなどが参加者にわかったことが影響していると考えられる。

4.5.2 Social-MRC の概要

社会的合意を形成するためには、より多くの人が合意形成に参加できるようにするとともに、できるだけその人たちの意見が反映できるようにすることが必要である。したがって、数千人以上が直接 MRC を使えるようにすることが望ましいが、非常に困難である。そこでここでは、現実の政治と同様に間接民主主義的な方法をとることとした。すなわち、対象とする問題に関し、オピニオンリーダに意見を戦わせてもらい、それを見て一般関係者が意見を言ったり、誰を支持するかを言ってもらおうというものである。このようにすることによって、次のような長所が生じる。

- (1) 一般関係者の意見の動向をリアルタイムに知るにより、それぞれのオピニオンリーダが自分の意見に固執していつまでたっても合意が形成できないという

問題を回避しやすくなる。

- (2) 一般関係者の中のすぐれた意見を意思決定に反映し、もともとの各オピニオンリーダの意見による解よりもよいものが得られやすくなる。

上記の目的を達成するため、オピニオンリーダ間のコミュニケーションと一般関係者参加型のコミュニケーションの 2 階層のリスクコミュニケーションを統合的に支援する Social-MRC システムの構想を固めプログラムの開発と青少年のための情報フィルタリング問題に適用を行った。このシステムの概要は図 4 に示すとおりである⁽¹⁹⁾。

ここで、オピニオンリーダというのは対象とする問題に関しそれぞれの立場の意見を代表する人であり、ファシリテータというのは、会議の運営を行い参加者の合意形成を支援する人である。また、MRC の専門家というのは対象問題を分析し、最適組み合わせ問題として定式化するとともに、MRC を動かし解を求め、その結果をオピニオンリーダやファシリテータ、さらには一般関係者に表示する人である。一般関係者は、対象とする問題に関心がある人で、これらの会議に参加する資格のある人である。誰でも参加可能であるという設定にすることも可能である。

第 1 階層 (オピニオンリーダ間のコミュニケーション) では、既開発の MRC をベースに必要な機能を追加することとし、これを MRC-Studio と呼ぶことにした。また第 2 階層 (一般関係者の議論参加) では、MRC-Plaza を用い一般関係者にオピニオンリーダたちの討議の様態を UStream などの動画共有サービス機能を取り込み中継するとともに、オピニオンリーダたちも見ている MRC-Studio の出力を提示することにした。そして、一般関係者に Twitter の機能などを通じて意見を言ってもらい、一般関係者フィードバックシステムを用い、その意見をわかりやすくオピニオンリーダたちに提示できるようにし

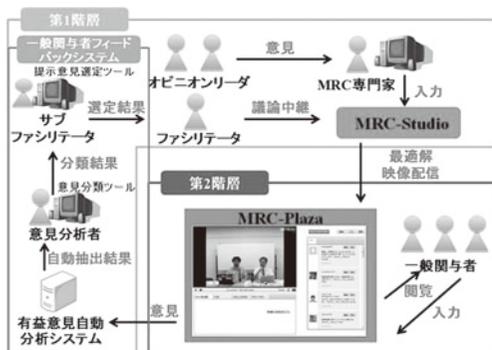


図4 Social-MRCの概要
Figure 4 Overview of Social-MRC

た。

Social-MRCで扱うに適した問題としては、青少年のための情報フィルタリング問題以外に、(a)国民IDの付与の問題やウイルス作成罪の可否、(b)電子署名法の法的有効性やさらに、(c)監視カメラとプライバシー問題、(d)幼児ポルノのブロック問題などがあると考えられる。また、利用場面はWEB利用公聴会や、コンセンサス会議、テレビの討論番組などが考えられる。

従来よりもより深い議論と早い合意形成を可能にしたい場合に適用しようとするものである。そこでは一方的なやり取りではなく住民などの関係者からの意見を入れて双方向で情報交換を行ったり、何かの制約条件やパラメータを変えたら全体にどのように影響が及ぶかを確認したりしながら方針を決定するのに役立つのではないかと考えている。

Social-MRCの構想についてさらに詳しくは⁽¹⁹⁾⁽²¹⁾を、青少年のための情報フィルタリング問題への試適用結果については⁽²⁵⁾を、機能の強化と適用結果については⁽²⁶⁾を参照願いたい。

5. 終わりに

本論文では、最初にITリスクへの対策が必要な背景を述べたのち、他のリスクと比べたITリスクの特徴を明確にした。次に、ITリスク学の定義を明確にするとともに、ITリ

スク学を構成する要素技術を示したのち、著者らがやっているリスクコミュニケーションを中心とするITリスクマネジメント技術について詳しく紹介した。

社会のITシステムへの依存度は今後ますます増大していくことが予想される以上、ITリスクの問題の重要性は上がることはあっても下がることはないだろう。したがって、それを他の人々がITリスク学と呼ぶかどうかは別にしてITリスクの問題解決のための学問はますます重要になってくると考えられる。

ITリスク学がさらに充実したものになるためには、やらなければならないことはまだまだ多く残されている。この分野の研究に多くの方々が参加いただくことを期待するとともに、著者らも引き続き粘り強く研究を続けていきたいと考えている。

謝辞

ITリスクのあり方に関する討議に参加いただき、貴重な意見をいただいた日本セキュリティ・マネジメント学会ITリスク学研究会の皆様には厚く御礼申し上げます。

参考文献

- (1) 日本リスク研究学会編「リスク学事典 増補改訂版」阪急コミュニケーションズ、2006
- (2) 林紘一郎、田川義博、浅井達雄「セキュリティ経営 ポスト3.11の復元力(レジリエンス)」勁草書房、2011
- (3) Hoffman, L. J., et al.: Trust beyond security: an expanded trust model, Communications of the ACM, Vol.49, No.7, pp.94-101 (2006)
- (4) 戦略イニシャティブ「情報化社会の安全と信頼を担保する情報技術体系の構築——ニュー・ディペンダビリティを求めて——」科学技術振興機構、研究開発戦略センター、CRDS-FY2006—SP-07

- (5) ウルリヒ・ベック(東廉/伊藤美登里訳)「危険社会 新しい近代への道」法政大学出版局, 1998
- (6) 山口節郎「現代社会のゆらぎとリスク」新曜社, 2002
- (7) 土方透, アルミン・ナセヒ(編著)「リスク 制御のパラドックス」新泉社, 2002
- (8) 三上剛史「社会の思考 — リスクと監視と個人化 —」学文社, 2010
- (9) フランク・ナイト著(安達貴教訳)「リスク, 不確実性および利潤」(1921)http://www.soec.nagoya-u.ac.jp/~adachi.t/translation_ch1_completed.pdf
- (10) ナシーム・ニコラス・タレブ著(望月衛訳)「ブラック・スワン(上・下)」ダイヤモンド社, 2009年
- (11) 池田信夫 blog「存在論的ブラックスワン」<http://ikedanobuo.livedoor.biz/archives/51352999.html>(ナシーム・ニコラス・タレブ著(望月衛訳)「強さと脆さ」ダイヤモンド社, 2010年にも同様な記述が分散して書かれているがここでは池田氏による紹介を引用した)
- (12) 佐々木良一, 「IT リスクの考え方」岩波新書, 2008
- (13) 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ーの開発と適用」, 情報処理学会論文誌, Vol.49, No.9, pp.3180-3190, 2008
- (14) 統計数理研究所リスク研究ネットワーク <http://www.ism.ac.jp/risk/contents/noe.html>
- (15) 奈良由美子「生活とリスク」放送大学教育振興会, 2007
- (16) 佐々木良一編著「IT リスク学 情報セキュリティを超えて」共立出版, 2013
- (17) 吉川肇子「リスクとつきあう」有斐閣選書, 2000
- (18) 川上昌俊, 安田浩, 佐々木良一「情報セキュリティ教育のためのeラーニング教材作成システム ELSEC の開発と評価」情報処理学会論文誌 VOL.52, No.3, pp.1266-1278
- (19) 佐々木良一, 杉本尚子, 矢島敬士, 増田英孝, 吉浦 裕, 鯨島正樹, 船橋誠壽「IT リスク対策に関する社会的合意形成支援システム Social-MRC の開発構想」情報処理学会論文誌 Vol. 52, No.9, pp.2562-2574
- (20) 中谷内一也「リスクのモノサシ 安全・安心生活はありうるか」NHK ブックス, 2006
- (21) Ryoichi Sasaki, “Consideration on Risk Communication for IT Systems and Development of Support Systems (Invited Paper)” Journal of Information Processing, Vo.20 (2012)-4, pp.814-822
- (22) 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ー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, VOL.23, No.2, pp.34-51
- (23) 守谷隆史, 千葉寛之, 佐々木良一, 「内部統制のための多リスク・多関与者を考慮した費用対効果の評価法の提案と適用」, 日本セキュリティ・マネジメント学会学会誌, 第22巻第3号, pp.3-14, 2008.12
- (24) 土方広夢, 間形文彦, 西垣正勝, 勅使河原可海, 佐々木良一「デジタル・フォレンジクスを考慮した個人情報漏洩対策に関する合意形成のための多重リスクコミュニケーターの適用」日本セキュリティ・マネジメント学会誌, 26巻第1号 2012年5月 pp.3-14
- (25) 大河原優, 高草木一成, 矢島敬士, 増田英孝, 小林哲郎, 佐々木良一「IT リスク対策に関する社会的合意形成支援システム Social-MRC の情報フィルタリング問題への試適用と考察」日本セキュリティ・マネジメント学会誌 25巻第3号 2012年1月 pp.15-23
- (26) 安藤 駿, 増田英孝, 矢島敬士, 佐々木良一「社会的合意形成支援システム Social-MRC の拡張と100人規模の実験への適用」JSSM 第27回全国大会研究報告会