情報処理学会論文誌 Vol.55 No.9 1946–1955 (Sep. 2014)

招待論文

ITリスク学の提案と最近の動向

佐々木 良一[1,a)]

受付日 2014年6月11日, 採録日 2014年6月17日

概要：社会のITシステムへの依存の増大にともない，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システムが扱うや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，それらに関する著者らの研究成果を報告する．最後にITリスク学に関する世の中の最近の研究動向の紹介を行う．

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

Proposal and Recent Trend of IT Risks Science

Ryoichi Sasaki[1,a)]

Received: June 11, 2014, Accepted: June 17, 2014

Abstract: With increase of the dependency of society on IT system, it is becoming difficult to solve safety issue of IT system 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 system but also IT system itself and services treated by IT system. 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 presents our research activities on the IT risks science. Last of all, the recent research trends on the IT risk science are shown.

Keywords: IT risk, risk management, risk communication, IT risks science

1. はじめに

金融，航空，鉄道，電力，ガス，政府・行政サービス，医療，水道，物流などは社会の重要インフラがIT（Information Technology）システムに大きく依存するようになってきており，IT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た．このような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な時代になりつつある．

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，②ITシステムが扱う情報だけでなくITシステム自体やITシステムが扱うや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．

[1] 東京電機大学
Tokyo Denki University, Adachi, Tokyo 120–8551, Japan
[a)] sasaki@im.dendai.ac.jp

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．最後に IT リスク学に関する著者らや世の中の最近の研究動向の紹介と今後の展望を行う．

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．たとえば，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，攻撃箇所の増加にともな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的な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行われている [3], [4]．

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	リライアビリティ、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

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つねに不確実性をともな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え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必ずしもつながらないことを指摘している．

三上は，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えず，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と対応方針

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紹介されるように「被害の予期がだれ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」その正当性を考察するだけでよいだろう．しかし，当事者はつね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分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うる．

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その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，不確定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え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注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」は計算可能かもしれないが，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ともな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をしようと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

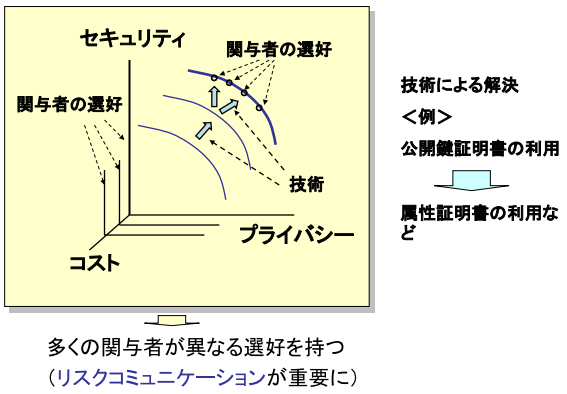

図 1 多重リスクへの対応法
Fig. 1 Method of resolving opposing risks.

うと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．したがって合理的プライオリティ付をしようとすれば，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良くすることはできる．たとえば，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わた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合せが不可欠である．

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合せが不可欠である．

(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ク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合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（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お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

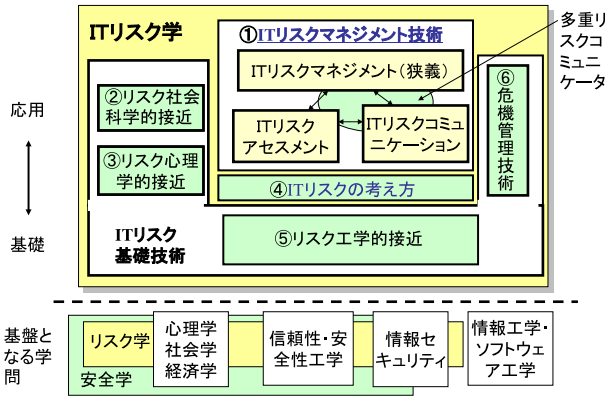

図 2 IT リスク学の構成
Fig. 2 Structure of IT risk science.

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タ 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．④ IT 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) リスクにきわ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，日本人は不可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ということを忘れてはならないだろう．②，③，⑤，⑥ 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

すでに述べたように 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する．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) 企業などの組織，(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決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．

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タ 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

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タ 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，専門家はつね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．このような状況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 1 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とらえ方をしている．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」といわれている．また，文献 [17] ではベネットは (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いわれている．

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うえで，多くの関与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タ 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

ここでは多重リスクコミュニケータ MRC [13], [21] について説明を追加する．Social-MRC の構想については文献 [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文献 [22] を，機能の強化と適用結果については文献 [23] を参照願いたい．

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決めるフェーズが重要であり，定量的分析・評価と

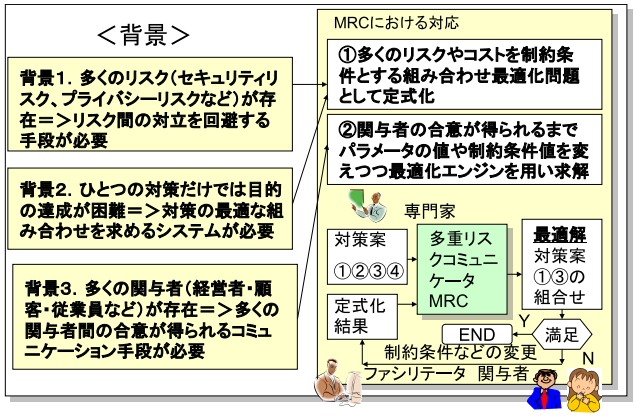

図 3 多重リスクコミュニケータ（MRC）の概要
Fig. 3 Overview of multiple risk communicator.

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与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合せ最適化問題（最適組合せ問題ともいう）として定式化し，（要求 3）に対応するため関与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，その結果を分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，制約条件を各関与者の評価指標（たとえば，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の組合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うえで，各主観確率に基づく対策案の最適な組合せを知ったうえ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，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，複数の意思決定関与者と，それらの人たちの仲立ちをするファシリテータがいる．

著者らは MRC を，各種の個人情報漏洩問題 [24] や，内部統制問題 [25]，証拠性保全問題 [26] 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と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合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分かったことが影響していると考えられる．

5. 最近の動向と今後の展望

IT リスク学を構成する種々の技術の最近の研究状況を本章では紹介する．

図 2 の ① の部分については，問題解決のためのいろいろなアプローチが必要となり，研究が始まりつつある．たとえば，太田敏澄らは，ゲーム理論や社会心理学などに基づく「モデル・ベースド・アプローチ」を提唱している [27]．

著者らも図 2 の ① の部分については，MRC や Social-MRC の実適用の増加と改良を通じてさらに便利なものにしていきたい．もっと簡単にリスクアセスメントを行い，合意形成を行って行く方法の確立も今後の課題である．さらに，今回開発したツールは Plan 用のものであるが，Do-Check-Act と連携したツールの開発も必要になるだろう．たとえば，いろいろなタイプの攻撃者がある比率でいる前提で PLAN 用に最適な対策案の組合せを求めておき，攻撃を受けている段階で，攻撃者のタイプが推定できたらその攻撃者に最適な対策の組合せに変更しながら対応していくというようなアプローチも考えられる．最近，内部犯罪対応にこのようなアプローチの試みを開始した [28]．

これらの作業を行う中から，図 2 の ④ の IT リスク学概念のさらなるブラッシュアップを行う予定である．最近，「集合知」の有用性が強く認識されており [29]，集合知の活用という面からリスクコミュニケーション問題の解決を図っていきたいと考えている．

IT リスク関連基礎技術の部分（図 2 の ②，③，⑤，⑥ に相当）についても実施すべきいろいろな項目があり，関係者の研究の推進を期待したい．特に次のような項目については，図 2 の ① において必要となるものなので IT リスク学の研究の一環として，重要性が高いものであると考えている．

(a) リスク心理学的接近法（図 2 の ②）：内部犯罪対策などにおいて対策の犯罪者に与える心理的効果の推定法の確立など．このような研究は国内では独立行政法人情報処理推進機構や岩手県立大学，京都産業大学などで進められている（たとえば文献 [30]）．国外でも文献 [31] などいろいろな研究が行われている．

(b) リスク社会科学的接近法（図 2 の ③）：東京大学で

は情報セキュリティの経済学的研究（http://www.isl.im.dendai.ac.jp/itrisk2010/2010.09.18.matsuura.pdf）が実施されてきた．独立行政法人情報処理推進機構ではセキュリティエコノミクスという名で情報セキュリティに対する社会科学的アプローチ（http://www.ipa.go.jp/security/economics/）が実施されてきた．また，情報セキュリティ大学院大学では経済学・経営学・法学などを総合的に組み合わせた研究が行われており注目に値する（文献 [16] の 7 章）．海外でも国際会議 WEIS（Workshop on the Economics of Information Security）などでいろいろな研究成果が発表されている．

(c) リスク工学的接近（図 2 の ⑤）：セキュリティ技術と安全性工学を組み合わせた対策案の創出と評価方法の確立など．IEEE Transactions on Dependable and Secure Computing などに種々の関連論文が掲載されている．また，Telecommunication Systems には文献 [32] のような論文も発表されている．

(d) 危機管理技術（図 2 の ⑥）：障害が発生した場合の自律的復旧ともいうべきレジリエンス対策に関する研究はさかんになりつつある（たとえば文献 [33]）．著者らもリスク対策だけでなく事象発生後の被害拡大防止対策も考慮した対策案の最適な組合せを求める研究を開始した [34]．

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 リスク対策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となり，研究も増加すると考えられる．

なお，この学問は「情報セキュリティ理論の体系化/調査研究」という名で内閣官房の情報セキュリティセンターの「情報セキュリティ研究開発戦略（改訂版）」において 16 の重要なテーマの 1 つにもなっている [35]．

6. 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，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．

そのうえで IT リスク学を構成する種々の技術の最近の動向を紹介するとともに，今後の展望を行った．

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厚く御礼申しあげる．

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, *Comm. 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 (2006).
[5] ウルリヒ・ベック（著），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). 入手先 ⟨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).
[11] 池田信夫 blog：存在論的ブラックスワン，入手先 ⟨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，入手先 ⟨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 (2011).
[19] 佐々木良一，杉本尚子，矢島敬士，増田英孝，吉浦　裕，鮫島正樹，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 (2011).
[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] Sasaki, R.: Consideration on Risk Communication for IT Systems and Development of Support Systems (Invited Paper), *Journal of Information Processing*, Vol.20, No.4, pp.814–822 (2012).
[22] 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摘用と考察，日本セキュリティ・マネジメント学会誌，Vol.25, No.3, pp.15–23 (2012).

[23] 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．
[24] 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，日本セキュリティ・マネジメント学会誌，Vol.23, No.2, pp.34–51 (2009).
[25] 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，Vol.22, No.3, pp.3–14 (2008).
[26] 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の適用，日本セキュリティ・マネジメント学会誌，Vol.26, No.1, pp.3–14 (2012).
[27] 太田敏澄，諏訪博彦：モデル・ベースド・アプローチに基づくセキュリティ・マネジメント，日本セキュリティ・マネジメント学会，Vol.27, No.1, pp.27–33 (2013).
[28] 梅原悠平，佐々木良一：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，情報処理学会，DICOMO2014 (2014).
[29] 西垣 通：集合知とは何か ネット時代の「知」のゆくえ，中公新書 (2013).
[30] 上田昌史：行動科学から見た情報セキュリティとプライバシーに関する研究について，電子情報通信学会誌，Vol.96, No.8, pp.656–661 (2013).
[31] Crosslera, R.E., Johnstonb, A.C., Lowryc, P.B., Hud, Q., Warkentina, M. and Baskervillee, R.: Future directions for behavioral information security research, Computers & Security, Vol.32, pp.90–101 (Feb. 2013).
[32] Sterbenz, J.P.G., Çetinkaya, E.K., Hameed, M.A., Jabbar, A., Qian, S. and Rohrer, J.P.: Evaluation of network resilience, survivability, and disruption tolerance: Analysis, topology generation, simulation, and experimentation, *Telecommunication Systems*, Vol.52, No.2, pp.705–736 (2013).
[33] Wolter, K., Avritzer, A., Vieira, M. and van Moorsel, A. (Eds.): Resilience Assessment and Evaluation of Computing Systems, Springer (2012).
[34] 松永一朗，佐々木良一：情報システムの継続的運用計画支援システムの開発と適用，情報処理学会 CSS2013 (2013).
[35] 内閣官房情報セキュリティセンター「情報セキュリティ研究開発戦略（改訂版）」(2014 年 7 月 10 日)，入手先 ⟨http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf⟩.

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．平成 13 年 4 月より東京電機大学教授．工学博士（東京大学）．平成 10 年電気学会著作賞受賞．平成 14 年情報処理学会論文賞受賞．平成 19 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．平成 25 年 IFIP Outstanding Service Award．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），『IT リスク学 情報セキュリティを超えて』（共立出版，2013 年）等．日本セキュリティ・マネージメント学会会長，デジタル・フォレンジック研究会会長，内閣官房情報セキュリティ補佐官，国立情報学研究所客員教授．