セキュリティ文化と信頼概念についての考察

On Security Culture and Concept of Trust

杉野　隆　Takashi SUGINO
国士舘大学　情報科学センター
Center for Information Science，Kokushikan University

要旨

2005 年 11 月に発表されたセキュリティ文化専門委員会報告書は，日本におけるセキュリティ文化の普及策を提案している。セキュリティ，リスク，組織文化の概念，ルーマンの信頼概念をもとに，OECD ガイドライン及び本報告書におけるセキュリティ文化の捉え方を比較分析することによって，背景にある日本と欧米におけるセキュリティ文化，信頼概念の捉え方の違いを明らかにした。

1. はじめに

2002 年に OECD が「情報システム及びネットワーク（以下，ISN）のセキュリティのためのガイドラインーセキュリティ文化の普及に向けて」[1]を策定した。インターネットの世界的な普及を背景に，ネットワークへの参加者全員へのセキュリティ文化の浸透の重要性を指摘している。日本においてはこれに対応して，同年に制定された高度情報通信ネットワーク社会基本法の第 22 条では，「安全性及び信頼性」として情報セキュリティに言及している。また，2003 年に経済産業省が発表した「情報セキュリティ総合戦略」では三つの戦略を掲げているが，その第一番に「事故前提のしなやかな社会システムの実現」とある。この「事故前提」という考え方は，それまでの国の政策を大きく針路変更するものであった。一方，セキュリティ文化について，これまで政府レベルでの言及はなかった。

2005 年 7 月に情報セキュリティ政策会議に設置されたセキュリティ文化専門委員会（以下，委員会）は，日本においてセキュリティ文化を醸成するための基盤を検討し，同年 11 月に報告書[2]を作成した。セキュリティ文化の育成に関する望ましい取り組みといえるが，この報告書の分析を通して，日本におけるセキュリティ，リスクに対する捉え方と信頼との関係について考察する。

2. リスクとセキュリティの概念

2.1 リスクの概念

リスク(risk)の語源は，ラテン語の risicum（偶然的かつ不利な出来事）とされる。それがイタリア語に移入された後に，"risicare"（勇気を持って試みる），"risico"（ハザードや災い），"risco"（切り立った険しい岩礁）といった言葉を経て，遅くとも 17 世紀には英語に移入され“risk”になったようである。

確率に基づくリスクの概念は，1977 年英国の Richard Courtney が AFIPS においてリスクを定量的に規定しようとして提唱したのが最初である（諸説あり）。この概念は，その後 NIST にも採用され，「損失発生の（もしくは，予定した利益を得られない）可能性」とされている。ISO/IEC Guide 51:1999 では，人間の肉体的，精神的，経済的な福利に害（悪影響）を与える危害（ここでは“事象”とは表現されていない）が「起こる可能性の度合い」とその危害が引き起こす悪影響の「大きさ」という二つの要素が複合されたものと定義されている。実務的には，これら 2 要素の積によってリスクの「度合い」を評価することが多い。

関連する用語である危険は，リスクがある許容値以上の状態をいう。問題はこの許容値の決め方であるが，科学的合理性に基づいてのみ決定されるわけではなく，社会的合意として決定されることが多い。

2.2 セキュリティの概念

セキュリティとは，ある対象の安全性を確保することであり，安全な状態を示す概念ではない。ラテン語の securus を語源にしており，不安からの解放を意味していた。今日では，投資のリスクからの解放，窃盗，そしてコンピュータ事故からの解放といった意味で幅広く使われている。1960 年代には，オンライン技術が発達し，米空軍も，さまざまな機密度をもった情報を保存するコンピュータシステムを，さまざまなレベルの知る必要性 need-to-know をもった人々に共同利用させることになり，コンピュータセキュリティ，脆弱性について検討する必要性が生じてきた。このころから，セキュリティという言葉が情報システム分野で使われるようになった。

情報セキュリティの場合には，対象となる情報資産の管理者とその情報資産を管理される個人又は組織の双方が情報資産の安全性を確保するための規則を設定し，その規則をどのような技術を用いて実施するかが，主題となる。したがって，情報セキュリティとは，「情報資産の管理におけるさまざまな攻

撃などの脅威から情報資産を守り，その安全性を確保すること」を意味する。守るにふさわしい情報資産には，機密性，完全性，可用性の三つ（のいずれか）の特性が要求される。この三つは 1992 年に策定された OECD ガイドライン[3]で提唱され，現在では，情報セキュリティの特性として定着している。セキュリティが侵害されると，情報資産の三つの特性のいずれかが損なわれ，損害が発生する可能性がある。すなわち，情報資産にはリスクがあることになる。

3. 信頼概念

3.1 Luhmann のリスク概念

ある概念の内容は，その対立概念として何を措定するかによって明確になる。リスクに関しては，リスク／安全という対立概念の捉え方がなされている。何がリスクであり何が安全かという区分は，損害が発生しうる事象が存在するか否かという事実に基づいている。しかし，**2.** に述べたように，リスクは確率を含む概念であり，ある決定を行うには相応のリスクを伴うが，しかし，安全を確保するための決定にもやはりリスクを伴うわけであり，リスクと安全を対立概念として捉えることはできない。Luhmann は，損害の予期が誰によってどのように行われるかに注目して，リスク／危険という区別に概念上の転換を図った。リスクを取る者と決定者とは一致しないことが多い。そこで，損害を引き起こしうる事象に関して，「決定への帰責／非帰責」の構成を社会的側面に焦点を当てて観察する[4]。未来の損害の可能性は，自分がいくつかの選択肢から意識的に行った決定の帰結とみなされ，そのような決定に帰属されるという場合をリスク，未来の損害が自分以外の誰か（人や社会システム）によって引き起こされたものであり，他者に責任を負わせられる場合，すなわち自分自身のコントロールの及ばない原因に帰属される場合を危険とする。すなわち，未来の損害が，自分の決定に帰属されるか（自己帰属）／帰属されないか（他者帰属）が，リスク／危険を区別する重要な要因である[5]。上述のリスクの語源からも，航海の危険を回避したければできるがあえて損害の可能性をとることがリスクである。裏返せば，適切なリスクマネジメントを行うことにより，未来の損害を回避できることになる。

3.2 信頼概念

信頼が問題となるのは，他者との社会的相互作用が彼の行動についての不確実な知識に基づかねばならない状況においてである。これまで，生活世界におけるさまざまな社会行動において信頼について議論されてきたが，今日のネットワーク社会においても，信頼関係は重要である。

コンピュータウイルスの感染，ネット取引のトラブル，ネットワークの脆弱性を衝くさまざまな脅威，個人情報の漏えいなどによって個人，企業が大きな損害を蒙る可能性がある。各個人の PC や企業のサイトが常にセキュリティ確保に努めていないと，信頼できない PC・サイトからの攻撃によって，自らの情報資産を破壊したり，外部に流出させたりするばかりではなく，踏み台となって間接的に他者の PC・サイトに多大の被害を発生させることになる。企業にとっては社会的な信頼，評判を傷つけることにもありうる。

Luhmann によれば，人間は，「現実世界の複雑性を縮減する」ために信頼を必要とする[6]。相互作用のもつ二重の不確定性状態では，行為者にリスクが発生する。Luhmann はリスクと危険の対立を信頼の構造に持ち込み，リスクと信頼 trust，危険と確信 confidence をそれぞれ対応する概念と考えた。信頼は認識においてはリスク状況と，帰属においては自己帰属と結びつく。確信は認識においては危険と，帰属においては他者帰属と結びつく。また，Luhmann は，信頼を，人間に対する「人格的信頼」と，個人・社会間の契約関係というシステムが機能することにより支えられる「システム信頼」に分けている。匿名の個人間で行われる経済取引はシステム信頼に基づいており，システム信頼の代表例は，通貨システムである。

濱口は，社会的信頼のあり方に，自己依拠（self-reliance）を前提とした信頼と相互依存（inter-dependence）を前提とした信頼があるという[7]。前者は，各個人が自律性を確立し，自己責任と(合理的選択に基づく)自己利益を追求する，欧米型の信頼である。各人が合理的意思決定に従うのであるから，相互に相手の行動をほぼ予測でき，信頼関係が生まれる。しかし，個(自我)に徹すれば徹するほど，逆に他者不信の傾向を生み，法的契約によらなければ相手を信じられないことになりかねない。

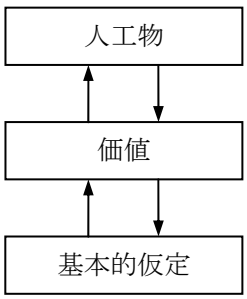
一方，後者の相互依存では，自ら個に徹するのではなく，互いに相手の気持ちや考え方を理解し，自分を相手に委ねる。これは，必ずしも，個を捨て，集団の意思決定に盲目的に従うことを意味するのではない。濱口は，これを間人主義と名付け，この意味での相互依存は，健全な社会を形成し，社会の効率性を実現するために重要な要素であるという。そして，後者は，Luhmann の「システム信頼」にも近いと述べている。ネットワーク社会における匿名個人間の社会秩序を確保し，社会効率を高めるためにはシステム信頼の確立が必要である。

4. セキュリティ文化

文化の概念はさまざまに捉えられている。ここでは，Giddens に従って，文化を，ドイツ流に「精神的に高次元のもの」と捉えるのではなく，（文化人類学に基づき）英米流に「社会の成員なり社会のなかの諸々の集団が生み出す生活様式」と包括的に捉える。

4.1 組織文化

Shein は，文化人類学における文化概念をもとに，レベルという考え方を持ち込み，組織文化を人工物，価値，基本的仮定の三つのレベルに分けた[8]。セキュリティ文化に関してもこの枠組みが使える。図に，各レベルの構成と，情報セキュリティにおける関連事項を示す。



目に見える組織構造及び手順（解読が困難，説明を要する）
セキュリティ実施手順書（パスワード，アクセス制御など），ガイドライン，リスク/セキュリティ意識キャンペーン，教育資料など

目に見え，意識するもの（標榜される正当な理由）
経営戦略，原則・基準，情報セキュリティポリシ，プライバシポリシ

無意識の当たり前の信念，認識，指向及び感情（組織文化の中核を形成し，価値観及び行動の源泉）
リスク，行動，態度の基本的理解

図　組織文化のレベルと情報セキュリティ関連事項

文物のレベルは具体的なセキュリティ行動について述べているが，組織成員は，なぜその行動が必要なのかについて十分に理解しているわけではない。十分に理解するためには，組織がなぜセキュリティ行動に価値をおくのかを納得することが必要である。さらに，価値観を共有するために，その背後にあって無意識のうちに行動を支配する信念，情報セキュリティ意識などに対する理解が必要である。また，これらのレベルは相互に関連しあっている。

4.2 セキュリティ文化の概念

[1]は，セキュリティ文化を「ISN を開発する際にセキュリティに注目し，また，ISN を利用し，情報をやりとりするに当たり，新しい思考及び行動の様式を取り入れること」と定義し，その普及を提唱した。また，その目的を「すべての参加者の間に、ISN 並びにそれらの提供及び利用の形態における一層大きな信頼 confidence を醸成すること」としている。思考・行動様式としての文化は，特定の社会の人々によって習得され，共有され，伝達される具体的な様式の体系であり，Schein の三層構造にも見られるようなさまざまな要素の集合体である。委員会では，OECD 関係者から，『飛行機に乗るときに携帯電話の電源を切る』といった行動を多くの人が無意識にとる状況がセキュリティ文化であると聞いたという挿話[9]が紹介された。これは基本的仮定のレベルに該当するが，当たり前の行動の定着のためには，その背景にある二つのレベルのセキュリティ文化の浸透が不可欠である。

4.3 セキュリティ文化専門委員会報告書

2005 年 11 月に発表されたこの報告書では，企業・個人のレベルにおける情報セキュリティ対策を強化するという共通認識を形成するために必要とされる方策をまとめている。提言の基本は次の二つである[2]。

①企業にとっては，企業の情報セキュリティ対策推進が企業の市場評価に繋がるような環境整備，情報セキュリティ人材の確保・育成

②個人にあっては，情報セキュリティ対策が「当たり前のこと」であると認識できる環境の整備（情報セキュリティリテラシ教育の推進とメディアの利用による啓発活動），情報関連製品・サービスを負担なく利用できる環境の整備

委員会では，OECD におけるセキュリティ文化の定義を翻訳して用いても正確に伝えることはできないので，日本の歴史，社会に即し，定着した言葉を用いて新たに定義すべきだと考えた。しかし，委員会議事録[9]を見る限り，12 名の委員から提出されたポジションペーパ中 9 名の文化の定義に関する意見が OECD の定義に近かったにもかかわらず，事務局は日本になじまないとして退けたようである。結果，企業，個人といった各主体が個々に醸成する思考・行動様式ではなく，「各主体のセキュリティに関する理解と役割分担の調整に基づき構築される，常識，マナーあるいは社会的慣習」という定義に落ち着いた。

ここで，主体の範囲は，企業と個人及び政府とされるが，[1]が ISN の開発・運用・利用という情報

システムのライフサイクルに沿って射程を捉えているのに比し，個別的であり恣意的である。また，文化は各主体の役割分担の「調整」によって構築されるものであり，自然調和にまかせるのでなく，政府の介入が必要であると主張している。この介入を新しい官民連携モデルと称しているが，従前と変わらない政策主導を目指しているにすぎない。[1]は，セキュリティ文化の構築の仕方は各国に任せているが，各主体の ISN への関与にはさまざまな側面があり，民主主義の原則に従った peer な文化の複合によって豊かな文化が形成されることを期待している。「常識，マナー，社会的慣習」は，基本的仮定，価値観に対応するが，二つの提言との関連は検討を要する。

一方，OECD が 2004 年に発表した文書[10]では，「単にその社会が文化的に高いレベルに到達すればよいということではなく，社会相互（筆者注：OECD 非加盟国も視野に入れている）間に一層大きな信頼と確信 trust and confidence を醸成することが目的である」と述べている。それぞれの社会が，自己に帰属するリスクに責任を持ち，他者社会に帰属する危険を最小限に抑制することにより，国際社会秩序が維持されるということが含意である。そのためには，基本的仮定だけでなく，Schein の第 2，3 層をも各社会が整備することによって始めてセキュリティ社会が実現することになる。しかし，委員会の定義したセキュリティ文化ではこの点については全く言及していない。ここではセキュリティ文化は，政府の進める情報セキュリティ政策と整合する共通基盤を形成するための方策でしかない。

5. セキュリティ文化の捉え方の相違

信頼は，健全な社会を形成し，社会の効率性を実現するための重要な要素である。

セキュリティは上述のように，（安全を確保する）技術という視点から生まれた概念であるが，生活世界における情報セキュリティの重要性が高まるとともに，技術の側面のみからは捉えられなくなり，社会，組織を支配する文化としての理解が必要になっている。

オーストラリア／ニュージーランドのリスクマネジメント規格 AS/NZS 4360:2004 のまえがきでは，「最も効率的であるためには，リスクマネジメントは組織の文化の一部になることがもっとも望ましい。それは別な活動と見なし実施されるよりも組織の哲学，方法及び事業プロセスに組み込まれることが望ましい。これが達成されると，組織のすべての人は，リスクのマネジメントに関与することになる。」と，リスク文化の重要性について明確に述べている。

この報告書は，政府の「第一次情報セキュリティ基本計画」策定の審議に供するために作成されたものであるが，2006 年 2 月に発表されたこの基本計画には，「セキュリティ文化」なる言葉はない。文化を思考・行動様式と捉えようとせず，セキュリティ文化と深い関わりを持つ信頼（システム信頼）概念に言及することもない。OECD 理事会勧告は，加盟国政府の政策策定の指針であり，強制力を持つものではないが，社会相互作用における信頼と確信の確立を通してセキュリティ文化を醸成するという OECD ガイドラインの理念は排除されたと言わざるを得ない。

6. まとめ

ネットワーク社会の秩序維持のためにはシステム信頼の確立が必要であり，そのもとにセキュリティ文化は醸成されることを明らかにした。日本におけるセキュリティ文化の定着を目指した報告書は，OECD の提言を換骨奪胎し，上からの政策にしてしまった。この背景には，個人・組織における人格的信頼を重視するが，システムとしての信頼を軽んずるという傾向があると見られる。

今後は，セキュリティ文化の醸成のための条件についてさらに検討を進めたい。

参考文献

[1] OECD　情報システム及びネットワークのセキュリティのためのガイドライン セキュリティ文化の普及に向けて，2002.

[2] 情報セキュリティ政策会議　セキュリティ文化専門委員会報告書－企業・個人の情報セキュリティ対策強化に向けて－，2005.

[3] OECD　情報システムのセキュリティのためのガイドライン，1992.

[4] 土方・ナセヒ編　リスク 制御のパラドクス，新泉社，2002.

[5] 小松丈晃　リスク論のルーマン，勁草書房，2003.

[6] ルーマン, N.（大庭・正村訳）　信頼 社会的な複雑性の縮減メカニズム，勁草書房，1990.

[7] 濱口恵俊　日本型信頼社会の復権，東洋経済新報社，1996.

[8] シャイン, E.H.（清水・浜田訳）　組織文化とリーダーシップ，ダイヤモンド社，1989.

[9] セキュリティ文化専門委員会第 1 ～4 回会合議事要旨

[10] OECD　Information Technology and Security, *Strengthening security and trust*, 2004.