情報セキュリティ・マネジメントの制度設計

*田中　秀幸[#]
松浦　幹太[##]

要旨

本稿は、情報セキュリティ技術と社会制度の相互連関に着目しつつ、社会基盤に関する施策を提示する。具体的には、保険と監査制度の活用によって情報セキュリティ投資の動機付けを確保する情報セキュリティ・マネジメントのあり方を理論的に示す。相互依存性という情報セキュリティの特徴はただ乗り問題などを招来するため、ユーザーのセキュリティ投資をいかに誘因するかが重要になる。本稿は、政府規制によるのではなく、ユーザーの経済合理的な活動を前提とした制度設計を示すとともに、情報セキュリティ・リスク定量化等の今後の課題を明らかにする。

キーワード

動機付け、所有権ルール、責任ルール、保険、情報セキュリティ監査、経済的定量化

1　はじめに

情報セキュリティ技術が進歩しているにもかかわらず、セキュリティ水準は向上していないと指摘されている（Fisk[2002], Larochelle and Rosasco[2003]）。情報セキュリティの確保には、技術の問題だけではなく、情報セキュリティ・システムを普及させる動機付けの問題が重要になっている(Anderson[2001])。このため、近年、情報セキュリティに関する動機付けの研究が増加しつつあり（松浦[2003], Matsuura[2003]）、（１）攻撃者に攻撃を控えさせるための動機付け（Dwork and Noar[1993], Dwork and Noar[1995], Matsuura and Imai[1998], Juels and Brainard[1999], Matsuura and Imai[2000], Yemini and Dailianas[1998]）、（２）標準化によるコスト削減のセキュリティ導入技術後押し効果 (Fox[2002])、（３）プライバシー関連技術の費用対効果(Feigenbaum et al.[2002])、（４）責任(liability)の動機付け効果（Fisk[2002], Yahalom[2002], Varian[2002], Larochelle and Rosasco[2003]）などの研究が進められている。こうした先行研究を踏まえて、本稿では、セキュリティ水準を確保するために、どのような動機付けがあり得るのかを俯瞰した上で、損害賠償責任の動機付けと保険・監査制度の活用を軸とする、情報セキュリティ・マネジメントが重要であることを示す。

本稿の構成は次のとおりである。最初に、情報セキュリティ・マネジメントの制度設計に当たり、情報セキュリティの相互依存性という特徴に注目する。相互依存性があるがゆえに、情報セキュリティへの取り組みは、他のユーザーの取り組みに依存することになる。

[#] 東京大学社会情報研究所
[##] 東京大学生産技術研究所

インターネットの普及によって多様なユーザーが参加する中では、情報セキュリティを確保するために要する費用とセキュアな情報ネットワーク環境から得られる便益は、ユーザーによってバラツキが生じるようになる。情報セキュリティの相互依存性という特徴を踏まえると、費用対便益比率の低いユーザーが経済合理的に行動すると、セキュリティ確保の上で問題が生じることを明らかにする。

次に、こうした問題への対応として、伝統的な安全確保対策である政府規制の導入について検討を加える。政府規制は、一定の基準を設定することが前提となるが、情報セキュリティ分野においては、政府が基準を設定して、規制を運用することが困難であることを明らかにする。

政府規制以外の措置としては、民間ベースの動機付けがあげられる。そこで、本稿では、その枠組みを所有権ルール(property rules)と責任ルール(liability rules)に分けて検討する。前者は、何らかの権原(entitlement)を取引の対象とするものであり、環境分野における排出権取引がその例となる。本稿では、情報セキュリティ分野においても、所有権ルールで動機付けをし得る可能性を示す。ただし、グローバル、かつ、分散的に展開するインターネットでは、何らかの方法で権原を管理することは困難である。そこで、損害賠償を基にした責任ルールについて検討を加える。損害賠償という事後的な調整スキームによっても、セキュリティ投資に対する事前の動機付けが可能である誘因構造を示した上で、責任ルールに付随する問題点を明らかにする。

続いて、責任ルールの問題点を軽減する制度に検討を移し、保険制度を取り上げる。保険の持ついくつかの機能を上げながら、特に行政的規制を代替して、一定のセキュリティ基準を担保するとともに、監視機能も有することを明らかにする。さらに、保険制度を有効に機能させるためには、情報セキュリティに関する専門的知見を有する第三者のサービスの活用であることを示しながら検討を加える。その上で、保険と監査制度との組合せによって動機付けることで、民間ベースで自律的にセキュリティ投資が進むことを明らかにする。

本稿では、以上のとおり、情報セキュリティ・マネジメントの制度設計の全体像を提示した上で、こうした民間ベースの動機付けを機能させるためには、次なる課題として情報セキュリティの経済的定量化などが必要であることを示す。

2　情報セキュリティの相互依存性とその問題

2.1　相互依存セキュリティとしての情報セキュリティ

全く独立した情報システムであれば、そのセキュリティは相当程度自己の管理内容に依存する。しかしながら、インターネットの普及等によって、ネットワーク化が進む中にあっては、情報セキュリティの相互依存性は高まっている。コンピュータ・ウィルスの被害や踏み台問題に見られるように、自らのセキュリティ水準は自らの管理努力だけではなく、ネットワークで接続された相手方がどれだけの情報セキュリティ・マネジメントをしているかが大いに関係するようになる。いかにセキュリティ投資をして水準を高めていても、他のユーザーのセキュリティ水準が低ければ意味がなくなることがある。一つの例として、２００３年１月のＳＱＬスラマー・ワーム(the Sapphire/Slammer Worm)によって、韓国のネットワークが半日近くダウンしたことが上げられる。このケースでは修正プログラムを当てていないＳＱＬサーバの存在が一因となって、それ以外のユーザーがネットワーク・ダ

ウンの影響を受けている（総務省[2003]）。負の外部経済効果が発生しているのである。このような相互依存関係にあるセキュリティ (interdependent security, Kunreuther and Heal[2003])においては、セキュリティ確保に対する投資額の決定は、他の主体がどのような行動を取るかに依存することになる。情報セキュリティ問題の動機付けの検討に当たっては、こうした相互依存性という外部経済効果を前提として検討することが必要となる。

2.2 ユーザーの貢献とセキュリティ水準の問題

2.2.1 セキュリティ水準決定の3つの型 (プロトタイプ)

それでは、相互依存関係にあるユーザーがセキュリティ水準にどのように貢献することができるであろうか。個々のユーザーの情報セキュリティ管理とセキュリティ水準の関係について考察したい。公共財の供給水準を分析した Hirshleifer[1983]に倣えば、この関係は次の三つの型に分けることができる。

(1) $X = \sum_{i=1}^{n} x_i$ 総和型(Summation)

(2) $X = \min_i(\chi_i)$ 最小努力依存型(Weakest-link)

(3) $X = \max_i(\chi_i)$ 最大努力依存型(Best-shot)

（X はセキュリティの水準、x_i は構成主体 i によるセキュリティ投資水準（人的投入を含む）。）

第一は、総和型で、各ユーザーの管理努力の合計によって、セキュリティ水準が定まるタイプである。各ユーザーの貢献が水準の向上をもたらすことになる。第二は、最小努力依存型で、最小の努力しかしないユーザーの努力水準に依存するという考え方である。他のユーザーがいかに努力しようとも、セキュリティの水準は最小努力者の水準によって決まってしまう。第三は、最大努力依存型で、最も努力したユーザーの水準によって、セキュリティ水準が定まる[1]。

2.2.2 相互依存性に伴う問題

Varian[2002]は、この分類を情報セキュリティ投資とセキュリティ水準の関係に当てはめて、ナッシュ均衡と社会的最適解についての考察を行っている。本稿では、その考察に基づき、総和型と最小努力依存型について、それぞれ、ＳＱＬスラマー・ワームと踏み台の問題を例に当てはめながら、セキュリティ投資に特段の動機付けがないままでは、どのような問題が生じ得るのかを明らかにする。

(1) 総和型

セキュリティ水準が総和型で決まる場合であっても、相互依存関係にあるためにあるユーザーの投資水準は他のユーザーの投資水準に依存することになる。もし、他のユーザーの投資によって十分なセキュリティ水準が確保されるのであれば、自分は投資する必要がなくなるからである。ＳＱＬスラマー・ワームの例で言えば、パッチを当てているユーザーが十分存在すれば、自分がパッチをあてていなくても輻輳によるネットワーク・ダウンのリスクは低くなるので、輻輳問題の回避という観点からはわざわざパッチを当てようとはしなくなる。

このような場合には、費用対便益比率の高いユーザーがセキュリティ投資を行うことがナッシュ均衡となり、同比率の低いユーザーは、そうしたセキュリティ投資にただ乗りすることになる。公共財に関しては、欲求度の高いユーザーが不釣り合いなほど多くの負担

を引き受けると指摘されているが(Olson[1965], p.35)、情報セキュリティについても該当する場合がある。事業活動でインターネット等の情報ネットワーク・システムが必要なユーザーほど、セキュリティ水準を確保することに伴う便益が大きくなるのでセキュリティ投資を積極的に行う一方で、情報ネットワーク・システムの必要度がそれほど高くないユーザーは、セキュリティ投資を積極的に行わず、前者のユーザーによって実現したセキュリティ水準にただ乗りするというケースである。

ただ乗りの問題が生じても、一部ユーザーの投資によってセキュリティ水準が確保されれば問題ないとも考えられる。しかしながら、社会的最適解と比較すると、このようなナッシュ均衡は必ずしも適当とは言えなくなる。なぜなら、社会的最適解は費用の少ないユーザーによるセキュリティ投資によって実現されるからである。費用対便益比率の低いユーザーの方が費用の絶対値が少ない場合、費用対便益比率の高いユーザーによって実現しているナッシュ均衡のセキュリティ水準は、社会的最適解のセキュリティ水準よりも低くなってしまうという問題が生じる。

こうした問題を回避して、できるだけ多くのセキュリティ投資を実現するには、ただ乗りをする、費用対便益比率の低いユーザーにセキュリティ投資を行わせるような仕組みが必要となる。

(2) 最小努力依存型

最小努力依存型では、セキュリティ水準はセキュリティ投資の最も低いユーザーによって決まってくる。情報セキュリティへの攻撃が最もセキュリティ投資の低い（すなわち最も脆弱な）ユーザーを踏み台にして行われる場合が、これに該当し得る。自己のセキュリティ投資の水準が高くても、セキュリティが脆弱な取引の相手方によって、自己のセキュリティ水準が引き下げられてしまうことが考えられるからである。

このような最小努力依存型のナッシュ均衡では、費用対便益比率の低いユーザーによってセキュリティ水準が決まる[2]。費用対便益比率の高いユーザーがいくらセキュリティ投資を行っても、セキュリティ水準には反映されず、無駄になってしまうのである。費用対便益比率の低いユーザーは、情報セキュリティが確保されることにそれほど魅力を感じていないか、セキュリティを確保するための負担感が大きく、いずれにせよ、何も仕組みがなければ、セキュリティ投資を積極的に行う可能性は低い。

したがって、最小努力依存型の場合でも、セキュリティ水準を高めるには、総和型と同様に、費用対便益比率の低いユーザーにセキュリティ投資を行わせるような仕組みが必要となる。

2.3 問題解決の必要性と対策の対象

以上のとおり、情報セキュリティの相互依存性という特徴を踏まえると、セキュリティ水準が総和型で決定される場合であっても､最小努力依存型で決定される場合であっても、セキュリティ水準を高めるには、特に、情報セキュリティに関する費用対便益比率の低いユーザーを対象に、何らかの仕組みが必要になることが明らかになった。

ところで、費用対便益費用比率の高い、あるいは低いユーザーとはどのようなケースが考えられるであろうか。大企業と中小企業を比較しながら考察したい。まず、便益の面であるが、図表１の調査結果が示すとおり、大企業と中小企業の間では、インターネット接続という点ではそれほどの差異はないので、それだけを見れば、大企業と中小企業がセキュリティの確保されたネットワークから得られる便益に差はない。ところが、外部へのコンピュータの公開や業務上の外部から内部ネットワークへの接続の必要性では大きな差が見られる。後者の実態を踏まえると、社会全体の情報ネットワーク・セキュリティからの

便益は大企業の方が中小企業よりも享受していることがわかる。次に、費用の面であるが、情報セキュリティの確保には管理業務を行う担当者・部署の設置など一定の固定費用が必要になり、必ずしも事業規模に比したものとはならない。このため、大企業に比較して中小企業の方が事業規模に対する費用負担の割合が高くなるおそれがある。図表１の調査結果でも担当者不在の割合が大企業に比して中小企業の方が多いことに、固定的費用負担の重さが表れている。以上のとおり、便益面、費用面のいずれを見ても、大企業よりも中小企業の方が費用対便益比率が低くなる要素を持っている。概して、費用対便益比率の高いユーザーは大企業に多く、低いユーザーは中小企業に多いことがわかる。

（図表１）情報システムに関する大企業と中小企業の比較

	大企業（N=490）	中小企業(N=111)
６０％以上のコンピュータがインターネット接続可能な企業の割合	６６．３％	７６．６％
Web サーバ等外部に公開しているコンピュータがある企業の割合	８１．３％	５４．１％
外部から内部ネットワークへの接続が業務上必要ない企業の割合*	１５．１％	３３．３％
セキュリティ管理担当者(専任・兼任)がいないの企業の割合	１３．５％	２９．７％

*現在接続を行っておらず計画もない回答者の内数（大企業 N=93, 中小企業 N=42）
（出典）三菱総合研究所[2002]のデータに基づき作成。

従来から中小企業の情報セキュリティ投資の低さの問題は指摘されている。こうした中小企業のセキュリティ水準の低さは、個々の事業者にとっての問題のみならず、他のユーザーの情報セキュリティ水準の確保という点からも問題になる。社会全体の情報セキュリティを確保するためには、中小企業に代表されるような情報ネットワークの費用対便益比率の低いユーザーの動機付けが必要となる。次章では、どうしたらユーザーのセキュリティ投資を促すことができるかについて検討する。

3　情報セキュリティ確保のための政府規制の可能性

セキュリティ水準を確保するための一つの仕組みは、政府規制である。安全確保を目的とする規制は、健康や環境を目的とする規制と並んで社会的規制の一つとして、政府によってその仕組みが提供されている(横倉[1997])。伝統的には、政府が一定の基準を設定して、それを基準･認証や資格制度などによって強制してきた(井手[1997], 八代[2003, p.245-268])。果たして、情報セキュリティという安全を確保するために、伝統的な政府規制は有効であろうか。そのような措置が基本的には導入されていないことを踏まえると、伝統的な政府規制の有効性は疑問視されるが、本章では、その理由について検討を加え、政府規制とは異なる新たな仕組みが必要であることを明らかにする。

3.1　基準に関する二つの態様

政府規制で設定される基準は、仕様基準（technology-based regulation）と性能基準(performance-based regulation)の二つに大別される（八代[2003, pp.245-268], Coglianese and

Lazer[2002])。前者は、既に存在する規格に基づき、製品や設備の具体的な材料や構造等の仕様や数値が基準として定められているものである。これに対して、後者は、こうした具体的な材料や構造などを特定するのではなく、一定の性能（例えば「割れない」「滑らない」）を基準として求めるものである。したがって、後者においては、一定の性能を満たしさえすれば、どのような材料や構造等の仕様（技術）を用いるかは自由になっている。

近年、仕様基準については過剰な規制になるおそれがあるとして見直しの気運が高まっているが、一概に否定されるものではなく、仕様基準にも性能基準にもそれぞれ合理性がある(Coglianese and Lazer[2002])。その合理性を、規制対象の同質性と性能の計測のしやすさという二つの軸で見ると、次のとおりとなる（図表２参照)。まず、仕様基準であるが、性能の計測が困難で、規制対象の同質性が高い場合には、有効な場合がある。すなわち、同質性が高く技術変化が激しくなければ、結果的に安全を実現する仕様（技術）が大差ないことが十分考えられ、そのような場合には、各事業者が別々に工夫のために時間と費用を費やすよりも、ベスト・プラクティスに見習うことが最も安上がりで効果的になる。

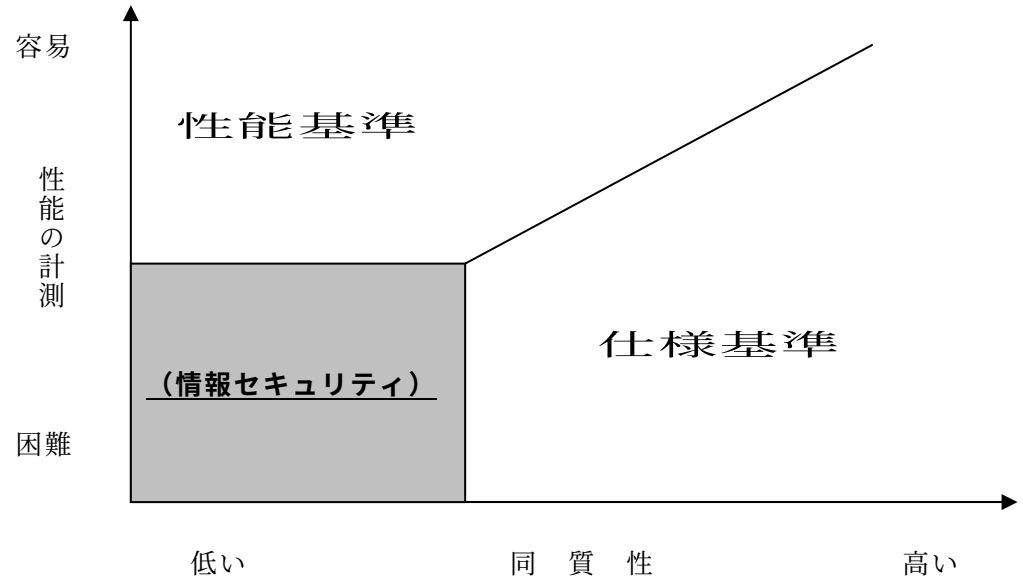
性能基準については、性能が計測しやすければ、効果的となる。特に規制対象の同質性が低い場合には、異なる技術を用いても、同じ性能を満たすことが可能になる可能性が高くなるので、事業者の創意工夫を活かせるという効果がある。また、技術変化が激しい場合にも、新たな技術を取り入れることが可能となるので、既存の規格を前提とせざるを得ない仕様基準と比較して性能基準は効果的である。ただし、性能基準も万全ではない。性能が第三者によって計測しづらければ、基準として機能しなくなるからである。

3.2　情報セキュリティに関する基準の可能性

さて、情報セキュリティに関する基準は、図表２の二つの軸で見るとどうなるであろうか。まず、同質性の軸であるが、情報セキュリティの管理態様は極めて多様である。業種、事業規模、情報システムの依存度などによって異なっており、同質性は低い。図表２の横軸で見れば、左方に位置する。

次に、性能の計測の軸であるが、情報セキュリティの計測は困難である。情報セキュリティは、一旦それが確保されれば自動的に維持されるものではなく、日々の管理・運営によって変化する動態的な性質を有している。また、新たな脆弱性の発見や新たな技術導入

（図表２）　政府規制の基準の態様



出典：Coglianese and Lazer[2002], p.207 に加筆修正して作成

など外的要因によって、セキュリティ水準が影響を受ける。性能基準で典型的に言われるような、「割れない」や「滑らない」のように容易に計測できるものではない。図表２の縦軸でみれば、下方に位置する。また、情報セキュリティを巡って急速に技術が進歩していることを踏まえると、一定のセキュリティ水準（＝性能）を達成するために必要な技術を絶えず見直す必要があり、技術進歩に応じて性能が動態的に変化するという点も性能計測の難しさにつながる。

以上のように情報セキュリティを二つの軸で検証すると、仕様基準又は性能基準といった従来の政府規制の基準では対応できない範囲にある（図表２の灰色部分）ことがわかる。伝統的な安全規制である、基準・認証や資格制度といった直接規制を実現するには、政府によって一定の基準を設定することが必要となる。しかし、情報セキュリティの場合にはいずれの基準も適用できないことから、これまで、直接規制が基本的には講じられていなかったものと考えられる。

他方で、第二章で論じたとおり、情報セキュリティの相互依存性を踏まえると、何らかの仕組みを導入しなければ、セキュリティ投資を促すことは困難である。同質性が低く、かつ、性能の計測が困難であるという制約の下で、どのような制度設計を行うかを検討することが必要となる。

4　民間ベースの動機付け

4.1　所有権ルールと責任ルール

政府による直接規制が有効ではない場合には、民間ベースでの動機付けの枠組みが重要となるが、セキュリティ確保の動機付けの場合には、相互依存性という外部経済効果をどのようにコントロールするのかが重要となる。民間ベースで外部経済効果をコントロールする方法は、所有権ルール(property rules)と責任ルール(liability rules)の二つがある（Kaplow and Shavell[1996]）[3]。前者は、外部性をコントロールする権原(entitlement)を取引の対象とすることによって外部性を内部化するもので、環境分野における排出権取引がその例になる[4]。これに対して、後者は、（負の）外部性が発生した場合に事後的に発生者に賠償責任を負わせるルールで、公害訴訟がその例となる[5]。

4.2　所有権ルールと情報セキュリティ

民間ベースの動機付けとして、情報セキュリティにこの二つのルールを当てはめるとどうなるであろうか。所有権ルールに基づけば、一定のセキュリティが確保された情報ネットワーク・システムに参加する権原に所有権を設定することが考えられる。この権原の活用策の一つは、差止請求である。特に最小努力依存型のセキュリティの場合、一定のセキュリティ水準を維持できないユーザーの参加は認めない、又は、そのようなユーザーが参加していたら、システムの利用を差し止めることは、セキュリティ水準を維持するためには有効な手段となり得る。また、差止請求以外にも活用方法はあり得る。例えば、総和型のセキュリティにおいて、費用対便益比率の高いユーザーのセキュリティ投資へのただ乗りを防ぐ手段として、セキュリティ投資の水準に応じてネットワーク・システムの参加料金に差を設けることがあげられる。セキュリティ投資の水準が高い場合には参加料金を低くし、そうでない場合には同料金を高く設定することで、ただ乗りを防ぐことが可能となる。

差止請求によって、情報システム・ネットワークへの参加が禁止されている実例は既にある。ＮＴＴドコモ迷惑メール送信禁止仮処分事件（横浜地決平成１３・１０・２９，判例時報１７６号１８頁）である。この事件では、架空の電子メール・アドレス宛に営利目的の電子メールを送信するなどして、ＮＴＴドコモの所有する電気通信設備の機能低下もしくは停止をもたらすような行為を対象に、その禁止が命じられている（丸橋[2003]）。この事件は、本稿がこれまで論じてきた例とは異なり、意図的な行動の結果セキュリティに障害を来しているものではあるが、民間ベースで情報セキュリティ水準を確保するための手段として、所有権ルールを適用する可能性があることが示されている。

所有権ルールに基づく解決手法の問題は、セキュリティの確保されたネットワーク・システムへのアクセスという権原をどうやって管理するかにある。前述の迷惑メール事件の場合には、ＮＴＴドコモが一元的に管理しているため、差止請求という所有権ルールを適用することが可能であった。しかし、グローバルかつオープンに展開するインターネットの場合、ＮＴＴドコモのようにネットワーク全体を排他的に管理する主体が存在しないのみならず、国の政府による管理が期待できないので、問題が難しくなる。ただし、インターネットの管理においても、セキュリティへの対応の動きはある。インターネット上のドメイン・ネームなどを管理するグローバルな非営利機関である ICANN(Internet Corporation for Assigned Names and Numbers)では、インターネット上のセキュリティ問題を扱う委員会 SECSAC(Security and Stability Advisory Committee)を発足させ、ルート・ネーム・サーバのセキュリティにとどまらず、ＰＣを含めた末端を対象としたセキュリティ問題についても検討されるようになってきている（Vixie[2002]）。インターネットを対象としては、前述の通信事業者のような強力な所有権管理は困難であろうし、インターネットの参加者をセキュリティ投資水準で差別的に取り扱うことの是非を含め相当慎重な検討は必要であろうが、非営利組織によって所有権ルールに基づく何らかの対応の余地はある。

4.3　責任ルールと情報セキュリティ

次に責任ルールの可能性について検討する。伝統的には、外部経済効果を内部化するためには、所有権を市場で取引する費用が低ければ、所有権ルールの方が責任ルールよりも効率的であると考えられている（Coase[1960]）。したがって、責任ルールの適用に合理性があるのは、市場で取引する費用が高い場合となる。市場取引費用の問題を情報セキュリティに当てはめて考えると、前節の NTT ドコモのようにネットワーク・システムを一元管理している場合には、取引費用が禁止的に高くなるわけではないので、所有権ルールを適用することは一つの解決策となり得る。これに対して、現在のインターネットのようにネットワーク・システムのセキュリティが一元的に管理されていない場合には、そもそも取引する相手を探す段階から膨大な費用がかかるおそれがあり、取引費用は極めて高くなると見込まれる。したがって、事前に所有権を設定する所有権ルールではなく、事後的に調整する責任ルールの方が適当となる。

近年では、取引費用が低い場合でも、責任ルールの方が所有権ルールよりも優れているとの考え方が示されている（Kaplow and Shavell[1996]）。所有権を割り当てる主体が潜在的被害者のリスク回避費用について十分な情報を持っていない場合がそれに該当する。所有権ルールに基づき不正確な情報に基づいて管理者が事前に所有権を割り当てるよりも、責任ルールに基づき事後的な損害賠償で担保した方が、潜在的被害者のリスク回避費用に関する正確な情報を利用できる。したがって、事前に権原を割り当てる所有権ルールよりも事後的に調整する責任ルールの方が優れているというのである。この考え方を情報セキュリティに当てはめるとどうなるであろうか。情報セキュリティの水準は外形的な基準で一

義的に明らかになるものではなく、むしろ如何なる管理を行うかに大きく依存することになる。このため、情報セキュリティを確保・維持するための情報については、管理者よりも潜在的被害者たるユーザーの方が優位となる。したがって、情報セキュリティの確保を民間ベースの動機付けで図るためには、取引費用が低い場合であっても、所有権ルールよりも責任ルールに基づいて行う方が適当になる。

責任ルールに関しても、所有権ルールと同様に、情報セキュリティに関する損害賠償請求の実例はある。報道で扱われることの多い事例としては、企業の情報ネットワーク・システムの障害に伴うものと、個人情報の管理に関するものに類型化される。近年のシステム障害の例としては、金融機関の統合に伴うものがあり、図表３のような損害賠償請求が行われている。後者の個人情報管理に関するものとしては、最高裁まで争われたものとして、宇治市の住民基本台帳データ流出に関する損害賠償請求があげられる（北岡[2003], 藤原[2003]）。さらに、以上の二つの類型以外にも、コンピュータ・フォレンジックへの関心の高まりが示すとおり、最近では、これまで責任を問われることのなかった踏み台のケースについても、損害賠償のリスクが高まっているとの指摘がある（藤田[2003]）。情報セキュリティ分野においては、責任ルールに基づく問題解決、処理が行われるようになっているのである。

（図表３）金融統合の際のシステム障害に伴う損害賠償請求額

みずほフィナンシャルグループ （２００２年４月システム統合）	ＵＦＪ銀行 （２００２年１月システム統合）
○東京電力：約５千万円* ○九州電力：約６６０万円 （データ変換のためのプログラム開発費６１０万円、4,100 件の領収書郵送費用など５０万円）** ○東京都水道局：約１千７百万円 （特例処理のプログラム作成･運営経費１３百万円、郵送費２百万円、職員超過勤務手当３百万円）***	総額：数億円*

（出典）*日本経済新聞[2002], **日経金融新聞[2002], ***東京都水道局[2002]

4.4　責任ルールの誘因構造と問題点

これまで述べてきたとおり、責任ルールは、直接には、問題が発生した後に損害賠償によって事後的に、被害者を救済する効果を持つ。しかし、それだけではなく、将来の問題を抑止する効果も持っている（内田[2003, p.303]）。そこで、本節では、責任ルールの誘因構造について、Shavell[1987, pp.9-21]に基づき、情報セキュリティの問題に即して、明らかにしておきたい。

（想定するリスク）

Ａ社のコンピュータ・システムが原因となって、Ｂ社のコンピュータ・システムのセキュリティに問題が生じて、その結果Ｂ社で損害が発生[6]。

○　Ａ社に損害賠償責任がない場合

この場合には、損害が発生したＢ社がすべて負担することになる。一定の損害発生を予測するＢ社は期待損害額を減らすよう動機付けられ、セキュリティ投資を行う。他方、何ら責任を伴わないＡ社は、動機付けがないのでセキュリティ投資を行わない。

○　Ａ社に損害賠償責任がある場合（無過失責任ルール）

無過失責任ルールの下では、過失の有無に関係なく、Ａ社がすべての損害額を補償しなければならなくなる。一定の損害賠償を予測するＡ社は期待損害賠償額を減らすよう動機付けられ、セキュリティ投資を行う。他方、何ら自己負担の伴わないＢ社は、動機付けがないのでセキュリティ投資を行わなくなる。

○ Ａ社に損害賠償責任がある場合（過失責任ルール）

過失責任ルールの下では、Ａ社は適切なセキュリティ管理を行っていれば、損害賠償が免責されることになる一方で、そのような管理を行っていなければ賠償責任を負うことになる。Ａ社は免責されるよう動機付けられ、セキュリティ投資を行う。Ｂ社は、Ａ社が合理的に判断すればセキュリティ投資を行うことが予想されるので、自らの期待損害額を減らすよう動機付けられ、セキュリティ投資を行う。

以上は、損害賠償責任原則に関する簡単な類型化であるが、賠償責任の所在を明確にすることによって、事前のセキュリティ投資が動機付けられることがわかる。

ただし、どのような相手に対しても損害賠償責任の割り当てが、動機付けとして機能するわけではない。例えば、次の例である。

○ 損害賠償額がＡ社の資産を大幅に上回るため、Ａ社が全資産を投じてもＢ社に対して賠償できない場合。

この場合、Ａ社は、セキュリティ投資の成果として期待損害賠償額が自分の全資産を下回らない限りは、一旦損害が発生してしまえばすべての資産を失って倒産することは変わらない。したがって、セキュリティ投資を行う動機付けは失われ、損害賠償責任が割り当てられても、事前にリスクを削減しようとはしなくなる。

ブロードバンドの普及などによって、中小企業や個人にも常時接続が増えており、ネットワークに接続された他の情報システムへのセキュリティ要因となる可能性が高まっている。中小企業や個人では、セキュリティの脆弱性が問題となって大企業に巨額の損失を与えたとしても、賠償できるだけの資産は見込めないおそれが高い。このため、中小企業や個人にとっては、賠償責任が割り当てられても、事前のセキュリティ投資の動機付けとしては機能しなくなる。その結果、潜在的被害者である大企業だけでセキュリティ投資が行われることになり、中小企業や個人によるただ乗りの問題が発生する。

他にも、損害賠償請求には問題がある。損害賠償が訴訟に持ち込まれた場合にかかる費用の問題である。環境分野に関する研究ではあるが、米国におけるアスベスト訴訟に関する実証分析では、損害賠償に要した費用のうち、実際の補償に充当されるのは４割程度に過ぎず、６割程度は訴訟費用など直接の補償以外の費用に充当されていることが明らかになっている(Freeman and Kunreuther[1997, pp.26-29])。責任ルールは、損害賠償があるが故に事前の動機付けとして機能するものの、一旦、損害が発生した場合には、補償以外にも費用を要するという問題が発生するのである。

5　保険制度と監査制度

5.1　責任ルールと保険

4.4 節後段で述べたような損害賠償に伴う問題に対応する一つの方法が保険制度である。第一が、保険制度の持つリスク分担機能によるものである（Freeman and Kunreuther[1997, p.23]）。保険は、個々の事象（セキュリティ事故）による経済的影響を、より広範なグル

ープ（多くの企業）に分担させることができる。それによって、一個人や一企業では負担しきれない損害への賠償を可能にする。損害賠償額が資産を上回る際の問題を回避することが可能になるのである。第二は、損害賠償における保険の効率性である。訴訟では、実際の補償に充当される額は全体の４割程度であったのに対し、米国の実証研究では、損害賠償保険を活用した場合には、三分の二が補償に充当されることが示されている（Freeman and Kunreuther[1997, p.29]）。損害賠償制度の効率性の問題を保険制度によってある程度カバーすることが可能なのである。

保険制度の機能は以上の二つにとどまらない。保険制度には、行政的規制の代替として機能する側面も有するのである（小早川ほか[2003]）。具体的には、一定の基準を担保する機能と事後的な監視の機能である。こうした機能は、保険に伴う二つの問題、すなわち逆選択とモラルハザードの問題に関係している(Freeman and Kunreuther[1997, p.24-25])。

まず、基準の担保であるが、保険会社は、高リスクな被保険者ほど保険を利用したがる逆選択の問題に対応するため、引き受け時点で低リスク者と高リスク者を分別する必要がある。これに対して、低リスクでなければ付保されない、又は安価な保険料を享受できないため、被保険者は、低リスク者としての基準を満たすようにリスク削減措置を講じるようになる。また、保険会社の側でも、保険引き受けの過程で、被保険者に対しリスク削減対策を推奨する。例えば、東京海上火災保険株式会社が提供する e-リスク保険（ＩＴリスクを補償する商品）では、引き受けの前に業務内容のヒアリングやリスク評価が行われ、基幹業務を担当するサーバがバックアップされている等の一定の条件を満たす場合には、割引の対象となっている。こうして、保険は一定のセキュリティ基準の実施を担保する機能を提供することになる。

もう一つの監視機能であるが、保険会社は保険契約後の被保険者によるモラルハザードを防ぐために、被保険者を監視する。保険引き受け時点で、一定のセキュリティ基準を満たしても、付保されたことで、かえってセキュリティ基準を維持しなくなるというモラルハザードの問題に、保険会社は対応する必要がある。このため、保険会社は、保険引き受け後に被保険者が一定のセキュリティ基準を維持しているかを、監視することになる。こうして、被保険者のセキュリティ水準が一定に保たれるようになるのである。

以上の保険制度による行政的規制代替機能によって、3.2 節で述べた情報セキュリティに関する基準の困難な点、すなわち、同質性が低く、性能の計測が困難である点に起因する問題の解決が可能になる。第一に、同質性の低さとの関係であるが、情報セキュリティを維持する仕様（技術）は多種多様に渡るため、一定の安全性を満たすかどうかの確認はきめ細かに行う必要がある。仮に、政府がその確認を行おうとすれば、行政の肥大化の問題を伴うことになる。これに対して、保険制度を活用すれば、保険会社という民間ベースでセキュリティ基準の確認を行うことが可能となる。保険会社は確認のためのコストをある程度、被保険者に転嫁することになるので、最終的には、被保険者の負担でセキュリティ基準の確認が行われるという仕組みが組み込まれることになる(Kunreuther[2001])。政府が安全確認を行えば、何らかの形で国民全体に負担が及ぶ可能性が生じるという問題を、保険制度によって関係者の負担のみで実現できるようになるのである。

第二に、性能の計測との関係であるが、情報セキュリティは管理の実態に依存するために、一旦、一定の水準を満たしたからと言って自動的に維持されるわけではない。水準の維持のためには、監視は重要な役割を果たす。前段と同様に、政府が監視を行えば、行政コストが嵩むことになるが、保険制度の中に組み込まれることで、被保険者は自己負担で監視を受けることが動機付けられることになる。

5.2　第三者サービスとしての監査制度の活用

保険制度による基準の担保機能と事後的監視の機能を実現するためには、被保険者のリスク水準を判断できる能力が必要となるが、保険会社が自らリスク水準を計測し、判断するのは必ずしも効率的ではない。なぜなら、第一に、情報セキュリティに関する高度な専門性が必要になるからである。情報セキュリティ・リスクの測定が保険会社の中核事業でない場合には、そのような専門家を内部で確保することは、保険会社の事業戦略的として問題となる。第二に、情報セキュリティの管理態様の多様性によってその問題が加速される。業種、事業規模、情報システムへの依存度等によって、情報セキュリティの管理態様は異なる。保険会社として引き受けリスクを分散するには、できるだけ多様な管理態様を対象にした方がいいが、他方で、引き受けるリスクが多様になれば、さらに多くの専門家を確保することが必要となり、より費用が嵩むことになる。

そこで、保険会社は第三者の機能を活用することになるが、その方法は３つに類型化される。第一は、特定のセキュリティ・ソフトウェア導入等のリスク削減措置がある場合には保険料を割り引く方法である。この方法は、簡便な方法ではあるが、セキュリティ水準は、ハードウェアやソフトウェアの単なる導入にとどまらず、どのような管理がなされているかに依存することを踏まえると、メルクマールとしての実効性は限られたものになる。第二は、ハードウェア又はソフトウェア企業が保険会社と提携する方法である。例えば、AT&T と Marsh 社の提携により、AT&T のインターネット・データ・センターやウェブ・ホスティング・サービスを利用する場合に Marsh 社の保険が付保されるものや(Gordon et al[2003])、インターネット・セキュリティ・システムズ社（ISS 社）と東京海上火災保険社の提携によって、ＩＳＳ社によるセキュリティ・サービスを利用する場合には、自動的に東京海上火災保険社の e-リスク保険が付保されるものなどがある[7]。このような方法であれば、保険会社と提供する企業がセキュリティ管理を行うことになるので、そのサービスを受けている範囲では実効性が期待される。

第三は、監査制度と保険の組合せである(Kunreuther[2001], Kunreuther and Heal[2003])。監査制度との組合せについては、前述の二つの方法と比較して、以下の４つの利点がある。第一に、対象の一般化である。特定のソフトウェアや企業に依存することなく、第三者監査が提供する範囲であれば、あらゆるセキュリティ水準を対象にできる。第二に、マネジメントを対象に水準を判断できる点である。特定の製品・サービスの導入だけでは、実際に所期の目的を達成するように運用されているかわからない。情報セキュリティで重要なことはいかに管理されているかであり、それは、監査によらなければ把握することは困難である。第三に、判断の一層の正確性の確保である。第三者監査はそれぞれ得意な分野や業種がある。得意分野の第三者監査を活用することで、リスク水準の判断がより正確になる。第四に、被害発生時の負担の削減である。一つの企業の製品・サービスに依存した場合、同製品・サービスの脆弱性が顕在化した場合、保険事故が同時に発生する可能性が高まる(Schechter and Smith[2003])。多様な第三者監査を用いることで、このような同質性に起因する問題を回避することが可能となる。

日本では、情報セキュリティ監査制度が整えられているが(経済産業省[2003])、同制度と保険制度を補完的に活用することで、効率的な付保が実現できる。それと同時に、監査を受けることで、保険会社から一定の優遇措置を受けられることを踏まえると、e-Japan 重点計画 II に盛り込まれている、情報セキュリティ監査制度の普及にも寄与することになる。

5.3　保険の活用と経済的定量化

以上のとおり、保険と監査制度の組合せは、民間ベースの情報セキュリティ投資の動機

付けとしての可能性を有しているが、事業として保険制度が成り立つためには、情報セキュリティに関する経済的リスクをどれほど負っているのかの定量化（経済的定量化）が必要となる(Freeman and Kunreuther[1997, pp.51-53.])。損失発生確率又は損失規模の期待値に応じて、引受保険料が決定されることになるが、そのために、定量化が前提になるからである。現在引き受けられている情報セキュリティに関する保険について見れば、事業規模や業種によって大まかに区分するか、又は特定の商品と組み合わせることによって、大まかなリスクの定量的把握を実現している状況である。このため、現状では、各ユーザーの実態に即したきめ細かな情報セキュリティ・マネジメントの動機付けとしては、必ずしも保険制度は十分に期待できる段階にはない。今後、前節で述べたように監査制度等第三者サービスとの組合せにより、よりきめ細かな情報セキュリティ・マネジメントが行われる可能性はあるが、それを実現するためには、ユーザーの管理実態に即した形できめ細かくリスクを定量化する必要がある。

情報セキュリティ・リスクの定量化に関しては、米国商務省標準局（当時）が１９７９年に示した年間予想損失額（ALE: Annual Loss Expectancy）の一般的枠組以来、第二世代としてのシナリオ分析アプローチなどが試みられているほか、保険制度での活用が困難だった第二世代までの手法の限界を超えるべく、最近では、決定分析（decision analysis）を取り入れた手法の研究が進められているところである（Soo Hoo[2000, 2002]）。決定分析アプローチについては、保険制度との接合が試みられてはいるが、基本的な枠組みの段階にとどまっており、新たな枠組みに基づく分析に必要なデータの収集と当該データに基づくモデルの実用化という課題が残されている。いずれにせよ、技術進歩やビジネス環境に応じて動態的に変化する情報セキュリティ・マネジメントに対応できる動機付けとして、保険及び監査制度を一層効果的に活用するためには、情報セキュリティ・リスクの経済的定量化を実用的水準で実現することが必要となる。

6　むすび

相互依存性のある情報セキュリティに関しては、各ユーザーの経済合理的な判断にセキュリティ投資を委ねるだけでは、ただ乗りなどの問題が生じ、必ずしも社会的な最適解が達成されるわけではない。このため、ユーザーにセキュリティ投資を行わせるような、何らかの仕組みが必要になる。安全確保の分野では伝統的な手法である、政府規制の導入については、情報セキュリティ基準の設定と規制の執行という観点で、問題があることがわかった。そこで、民間ベースの動機付けについて検討を加えたところ、所有権ルールに基づく動機付けも可能性はあるものの、当面の実効性を確保するには、責任ルールに基づく枠組みを設定することが適当であることが示された。責任ルールに伴う諸問題を軽減するには、情報セキュリティ分野では保険制度と監査制度を組み合わが有効であるが、実効性を確保するためには、情報セキュリティ・リスクの経済的定量化が必要であることを明らかにした。本稿では、以上のとおり、情報セキュリティの相互依存性に着目しながら、セキュリティ水準を確保するためには、保険と監査制度の活用による民間ベースでの動機付けを基本とした情報セキュリティ・マネジメントの制度設計が重要であることを理論的に提示した。

情報セキュリティ・マネジメントの制度設計を進めるための今後の課題としては、第一に、リスクの経済的定量化があげられる。5.3 節で述べたとおり、具体的なデータに基づいて、実用的な定量化に向けて研究を進めることが必要である。第二の課題としては、中小企業や個人ユーザーの取り扱いに関する更なる検討である。こうした費用対便益比率の

低い主体を動機付けるには、保険や監査制度だけでは十分な効果を期待できるかどうか慎重に見極める必要があるからである。中小企業や個人ユーザーの問題に関しては、インターネット・サービス・プロバイダ（ISP）に責任を割り当てることで、情報セキュリティが確保されるとの提案もなされている（Varian[2000]）。しかしながら、プロバイダ責任制限法（「特定電気通信役務提供者の損害賠償責任の制限及び発信者情報の開示に関する法律」（平成１３年法律第１３７号））制定時に、慎重な検討が行われるなど（郵政省[2000]）、ユーザーと ISP の責任関係については検討すべき論点は多い。中小企業や個人ユーザーの情報セキュリティ・マネジメントに関しては、ISP の位置づけを含めて、責任ルールや所有権ルールの適用について一層の研究が必要である。今後は、以上のような課題に重点を置きながら、情報セキュリティ・マネジメントの制度設計を進めることが求められる。

---

[1] 実際は、Hirshleifer[1983]が指摘するとおり、いずれか一つのケースによって定まるとは限らず、３つのケースの中間や組み合わせも想定される。

[2] 正確には、ナッシュ均衡の投資水準としては、まったくセキュリティ投資を行わない場合から費用対便益比率の低いユーザーの投資水準までの幅があるが、ここでは、ナッシュ均衡かつパレート支配的なものをあげている。

[3] これら二つのルールに加えて、Calabresi and Melamed[1972]は不可譲な権原ルール (inalienable entitlements rules)を挙げているが、このルールでは権原の売買が政府によって予め規制されることになるので、本稿では除外して検討を進める。

[4] 所有権ルールの典型例は政府による規制となる。また排出権取引は責任ルールに近い性格も有している。

[5] 政府による課税（例：炭素税）も、責任ルールに含まれる。

[6]Ａ社とＢ社のいずれも、セキュリティ投資を行うことで、セキュリティ・リスクを減少させることができると想定する（いわゆる、バイラテラル・ケース）。なお、これと対照されるのは、一方の投資だけがセキュリティ・リスクを減少させることができる、ユニラテラル・ケースとなる。

[7] ISS 社ウェブ・ページ参照（http://www.isskk.co.jp/）。

参考文献

Anderson, Ross[2001] “Why Information Security is Hard -- An Economic Perspective,” in *17th Annual Computer Security Applications Conference (ACSAC)*, December 2001.

－[2002] “Unsettling Parallels Between Security and the Environment,” in *Workshop on Economics and Information Security*, May 2002.

Calabresi, Guido and A. Douglas Melamed[1972] “Property Rules, Liability Rules and Inalienability: One View of the Cathedral,” *Harvard Law Review*, 85, pp.1089-1128.

Coase, Ronald H[1960] “The Problem of Social Cost,” *the Journal of Law and Economics*, vol.3, pp.1-44.

Coglianese, Cary and David Lazer[2002] “Management-Based Regulatory Strategies,” in Donahue , John D. and Joseph S. Nye Jr. ed., *Market-based Governance : Supply Side, Demand Side, Upside, and Downside*, Cambridge, Mass. : Visions of Governance in the 21st Century, pp.201-224.

Dwork, C. and M. Nor[1993] “Pricing via Processing or Combating Junk Mail,” in E.F. Brickell ed. *Advances in Criptology-CRYTO’92*, Lecture Notes in Computer Science 740, pp.139-147, August 1993, Springer-Verlag.

－and－[1995] “Pricing via Processing or Combating Junk Mail,” *Technical Report CS95-20*, Faculty of Mathematical Sciences, The Weizmann Institute of Science.

Feigenbaum, J.; M. J. Freedman; T. Sander and A. Shostack[2002], “Economic Barriers to the Deployment of Existing Privacy Technologies,”in *Workshop on Economics and Information Security*, May 2002.

Fisk, Mike[2002] “Causes and Remedies for Social Acceptance of Network Insecurity, “ in *Workshop on Economics and Information Security*, May 2002.

Fox, B.[2002] “Internet TAO: The Microeconomics of Internet Standards Setting,” in *Workshop on Economics and Information Security*, May 2002

Freeman, Paul K. and Howard Kunreuther[1997] *Managing Environmental Risk through Insurance*, Boston : Kluwer Academic Publishers.

Gordon, Lawrence A.; Martin P. Loeb and Tashfeen Sahail[2003] “A Framework for Using Insurance for Cyber-Risk Management,” *Communication of the ACM*, vol.46, No.3, pp.81-85.

Hirshleifer, Jack[1983] “From Weakest-link to Best-shot: The Voluntary proposition of Public Goods,” *Public Choice*, vol.41, pp.371-386.

Juels, A. and J. Brainard[1999] “Client Puzzles: A Cryptographic Defense Against Connection Depletion Attacks, “ in S. Kent ed., *Proc. Of NDSS’99(Networks and Distributed Security Systems)*, pp.151-165, 1999.

Kaplow, Louis and Steven Shavell[1996] “Property Rules versus Liability Rules: an Economic Analysis,” *Harvard Law Review*, vol.109, no. 4, pp.713-790.

Kunreuther, Howard[2001], “Third-Party Inspection as an Alternative to Command-and-Control Regulation,” in Orts, Eric W. and Kurt Deketelaere ed., *Environmental Contracts : Comparative Approaches to Regulatory Innovation in the United States and Europe*, London : Kluwer Law International, pp.389-406.

－and Geoffrey Heal[2003], “Interdependent Security,” *the Journal of Risk and Uncertainty*, vol. 26, no.2/3, pp.231-249.

Larochelle, David and Nicholas Rosasco[2003] “Towards a Model of the Costs of Security, “ *UVa CS Technical Reports*, CS-2003-13, pp.1-11

Matsuura, Kanta[2003] “Information Security and Economics in Computer Networks: An Interdisciplinary Survey and a Proposal of Integrated Optimization of Investment”, *The 9th International Conference of Computing in Economics and Finance (CEF 2003)*, Seattle, July 2003.

－ and H. Imai[1998] “Protection of Authenticated Key-Agreement Protocol against a Denial-of-Service Attack,” *Cientifica*, vol.2, no. 11, pp.15-19.

－and －[2000] “Modified Aggressive Modes of Internet Key Exchange Resistant against Denial-of-Service Attack,” *IEICE Transactions on Information and Systems*, vol.E83-D, no.5, pp.972-979, May 2000.

Olson, Mancur[1965] *The Logic of Collective Action: Public Goods and the Theory of Groups*, Cambridge, Mass. : Harvard University Press.

Schechter, Stuart E. and Michael D. Smith[2003] “How Much Security is Enough to Stop a Thief?” in *the Seventh International Financial Cryptography Conference*, January 2003.

Shavell, Steven[1987] *Economic Analysis of Accident Law*, Cambridge, Mass. : Harvard University Press.

Soo Hoo, Kevin J.[2000] “How Much is Enough?: A Risk-Management Approach to Computer Security,” *Working Paper, Consortium for Research on Information Security and*

Policy(CRISP), Stanford University, pp.1-88, at http://citeseer.nj.nec.com/505332.html on August 30, 2003.

－[2002] “How Much is Enough?: A Risk-Management Approach to Computer Security,” in *Workshop on Economics and Information Security*, May 2002.

Varian, Hal R.[2000] “Managing Online Security Risks,” *New York Times*, June 29, 2000.

－[2002] “System Reliability and Free Riding,” in *Workshop on Economics and Information Security*, May 2002, at http://www.cl.cam.ac.uk/users/rja14/econws/49.pdf on August 25, 2003.

Vixie, Paul[2002] “Securing the Edge,” SECSAC/SAC004, October 17, 2002, at http://www.icann.org/committees/security/sac004.txt, on September 10, 2003.

Yahalom, R.[2002] “Liability Transfers in Network Exchanges,” in *Workshop on Economics and Information Security*, May 2002.

Yemini, Y.; Dailianas, D; D. Florissi and G. Huberman[1998] “Market Net: Market-Based Protection of Information Systems,” in *Proceedings of First International Conference on Information and Computation Economics(ICE’98)*, October 1998.

井手秀樹[1997] 「社会的規制の手段」，植草益編，『社会的規制の経済学』，東京：ＮＴＴ出版，pp.50-79.

内田貴[2003] 『民法 II: 債権各論』（第１８刷），東京：東京大学出版会.

北岡弘章[2003] 『漏えい事件、Ｑ＆Ａに学ぶ個人情報保護と対策』東京：日経ＢＰ.

経済産業省[2003] 『情報セキュリティ監査研究会報告書』.

小早川光郎＝川出敏裕＝城山英明＝廣瀬久和＝山本隆司[2003]「現代における安全問題と法システム（下)」,『ジュリスト』，no. 1248，pp.92-117.

総務省[2003] 「インターネット障害に関する韓国訪問調査の結果及び今後のインターネット・セキュリティ対策の充実・強化」，２月１０日報道発表資料 at http://www.soumu.go.jp/s-news/2003/030210_2.html on August 25, 2003.

東京都水道局[2002] 「みずほ銀行に対する損害賠償請求について」，at http://www.metro.tokyo.jp/INET/CHOUSA/2002/08/60C8N100.HTM on August 25.

日経金融新聞[2002] 「みずほの障害、九電が賠償請求、開発費用など６６０万円」，２００２年９月，p.11

日本経済新聞[2002] 「みずほ、東電に５０００万円賠償」，２００２年８月２４日朝刊，p.3.

藤田憲治[2003] 「”踏み台”にされた企業に賠償責任？高まる訴訟リスクに新対策、カギはポリシーとフォレンジック」，Nikkei Internet Solutions, 2003.9, pp.53-55.

藤原静雄[2003] 「宇治市住民基本台帳データ不正漏えい事件」，岡村久道編『サイバー法判例解説，別冊ＮＢＬ　No.79』東京：商事法務，pp.190-191.

松浦幹太[2003] 「情報セキュリティと経済学」, The 2003 Symposium on Cryptography and Information Security, January 2003.

丸橋透[2003] 「ＮＴＴドコモ迷惑メール送信禁止仮処分事件」，岡村久道編『サイバー法判例解説，別冊ＮＢＬ　No.79』東京：商事法務，pp.22-23.

三菱総合研究所[2002] 『情報セキュリティの市場動向に関する調査報告書』，at http://it.jeita.or.jp/infosys/committee/security/pdf/02-kei-1furoku1.pdf on August 25,

2003.
八代尚宏[2003] 『規制改革：「法と経済学」からの提言』東京：有斐閣.
郵政省[2000] 『インターネット上の情報流通の適正確保に関する研究会報告書』, pp.1-78, at http://www.soumu.go.jp/joho_tsusin/pressrelease/japanese/denki/001220j601.html on August 30, 2003.
横倉尚[1997] 「社会的規制の対象」, 植草益編,『社会的規制の経済学』, 東京：ＮＴＴ出版, pp.22-49.