情報セキュリティーにおけるインセンティブ制御*

田村知嗣　　加茂知幸

要旨

本論文の目的は、組織における情報ネットワーク上において、組織内の機密情報が組織外へ漏えいするリスクに対して、論理的にセキュリティーが担保できるような相互チェックシステムを提示し、その性能について、①インセンティブ、②フォールト・トレランス性、③効率性の３つ視点から評価することである。本研究で得られた結果および含意は以下のとおりである。第一に、チェックを行うことのコストが存在する場合、プレイヤーがチェック活動を実施するインセンティブが十分ではないため、誰もチェックを行わない。第二に、上述の問題に対して、適切な罰則規定を導入すると、いずれのシステムでも情報漏えいを防ぐことができる。第三に、故障ノードが存在しない場合であれば、チェック・コストが少なくて済むという意味で、全員一致ルールが望ましい。第四に、故障ノードの存在を前提とすると、全員一致ルールでは、適切な情報であっても送信されない事態が発生し、ネットワーク・システム自体が機能しなくなる恐れがある。一方、多数決ルールであればそのような事態を避けることができる。したがって、システムのフォールト・トレランス性の観点からは、多数決ルールを採用することが望ましい。

キーワード：情報セキュリティー、フォールト・トレランス性、インセンティブ

1. はじめに

近年、情報セキュリティーに関して社会的に大きな注目が集まっている。これはコンピュータ技術の革新により大容量の電子データを手軽に取扱うことができるようになり、さらにインターネットをはじめとする情報通信のためのネットワークへの接続が普及したことによって、善意のユーザの意図しない動作、または悪意のユーザの恣意的な行動、さらには自然災害等が、個人や所属する組織またはそれ以上の規模におけるコミュニティーに対して人的影響や金銭的被害等をもたらす、またはそのおそれのある事案が増えたことによるものである。

このため情報セキュリティー対策は大きな社会的課題となっており、前述のような事案

*本論文は田村が京都産業大学経済学研究科に提出した特定課題研究報告書を加筆・修正したものである。論文を作成するにあたり飯田善郎教授（京都産業大学）から大変有益な助言を受けた。ここに記して感謝する。もちろん、本稿に残された誤りはすべて筆者たちの責任である。

を未然に防ぎ、または影響や被害を最小限にするために個人や組織は多大な費用と労力を必要とすることになる。コンピュータ技術のさらなる進歩やネットワーク利用の高度化及び犯罪手口の巧妙化などによって、今なおセキュリティー・インシデントの発生は後を絶たない状況である。特に昨今では、先に述べたように国や自治体等の行政機関やいわゆる大企業における組織的な事案が数多く起こっている。またこのような組織では上に挙げたようなセキュリティー対策を一見十分に実施しているにもかかわらず、その運用や管理（マネジメント）に不備があったためインシデントに至ったケースが多いとみられる。

このため、今後の情報セキュリティー対策においては、個別の対策を強化するだけでなく、これらのマネジメントを適切に行い、有機的な繋がりをもってその効果を発揮できるように運用することが求められる。

このような状況を踏まえると、今後ますますネットワークの活用が進むとみられるが、これに伴い情報セキュリティーに関する脅威やリスクも同様にますます増大するものと考えられる。また個人や組織は電子情報のさらなる厳格な取り扱いが求められていくことになるであろう。

そこで、本研究の目的は、組織における情報ネットワーク上において、組織内の機密情報が組織外へ漏えいするリスクに対して、論理的にセキュリティーが担保できるような相互チェック・システムを提示し、その性能について、①インセンティブ、②フォールト・トレランス性、③効率性の３つ視点から評価することである。

本研究の特色は以下の点にある。第一に、本研究では、チェック活動を行う主体は機械ではなく人間であるとの立場から、チェックを行うことによるコストの存在を明示的に導入する点である。したがって、チェック・システムが正常に機能するかについて、チェック主体のインセンティブを詳細に検討する必要がある。この点は従来の計算機科学的なアプローチとは異なる。第二に、ゲーム理論を応用した分析を行うことである。チェックを行う主体が複数存在する場合、各主体のインセンティブが複雑に絡み合うことになる。このような状況を分析するにはゲーム理論を応用することが有用である。第三に、システムのフォールト・トレランス性を考慮した分析を行う点である。チェック・システムにおいて、その構成員の一部が正常に行動しなくても、システム全体としては正常に処理を続行することが可能であることが望ましい。このような性質のことをフォールト・トレランス性（故障耐性）という。フォールト・トレランス性は、計算機科学の分野ではよく知られた性質であるが、ゲーム理論を制度設計問題に応用したメカニズム・デザイン論では、ほとんど意識されなかった性質である[1]。本研究の分析は、メカニズム・デザイン論にフォールト・トレランス性を導入する試みとしてみることもできる。

次節では、情報セキュリティーに関する問題およびその対策についての概観を与える。第３節では、情報漏えいリスクに対して、クライアントが相互にチェックするシステムを提案

[1] フォールト・トレランス性を考慮したメカニズム・デザインの研究として Eliaz(2002)がある。

し、その性能を分析するためのモデルを構築する。第４節では、第３節のモデルを用いて、チェックシステムの性能を比較検討する。具体的には、ゲームのナッシュ均衡点を計算して、均衡において情報漏えいを防ぐことが可能であるか、またシステムのフォールト・トレランス性および効率性について議論する。第５節では、本研究で得られた結果をまとめて、今後の課題についても簡単に述べる。

2.　情報セキュリティー問題とその対策

2-1　情報セキュリティーとは

情報セキュリティー（*information security*）とは、JIS Q 27002（すなわち ISO/IEC 27002）によって、次の三つの性質を維持することと定義されている。

(I)　**機密性**（*confidentiality*）情報へのアクセスを認められた者だけが、その情報にアクセスできる状態を確保すること

(II)　**完全性**（integrity） 情報が破壊、改ざん又は消去されていない状態を確保すること

(III)　**可用性**（*availability*）情報へのアクセスを認められた者が、必要時に中断することなく、情報及び関連資産にアクセスできる状態を確保すること

また情報セキュリティーに関する概念として、次の用語が挙げられる。

(i)　**脆弱性**（*vulnerability*）脅威が付け入ることができる、資産が持つ弱点。すなわちリスクを発生させる潜在的な原因。

(ii)　**脅威**（*threat*）脆弱性を利用して、リスクを現実化させる手段。すなわち資産に損害を与える可能性がある直接的な要因。

(iii)　**リスク**（*risk*）脅威の大きさと脆弱性のそれを掛け合わせたもの。すなわち何かしらの損失を発生させる事象の発生確率。

(iv)　**情報セキュリティー・インシデント**（*information security incident*）望まないまたは予期しないシステム、サービスまたはネットワークにおける特定の状態（事象）の発生であって、事業運営を危うくする確率および情報セキュリティーを脅かす確率が高いもの。

情報資産を情報セキュリティー・インシデントの脅威から守り、前述の情報セキュリティーを確保するための対策としてさまざまなものがある。これらは大きく３つに分類され、それぞれの性質と主な対策を次に示す。

（１）技術的対策

ソフトウェア、データ、ネットワークなどに技術的な機構を組み込むことで，システム機器や端末，データなどに被害が発生することを防ぐ対策のこと。対策例として、アクセス制御、ファイアウォール、ウイルス対策ソフト、侵入検知システム、暗号化などが挙げられる。

（２）人的対策

人間による過誤，盗難，不正行為のリスクなどを軽減するための教育や訓練，及び情報セ

キュリティー・インシデントに対して被害を最小限にするための対策のこと。対策例として、情報セキュリティーに対する責務の明確化、就業規則への運用ルールの明記、定期的な教育、事故対応マニュアルの作成などがある。

（3）**物理的対策**

外部からの侵入による盗難や破壊，自然災害や火災による損壊や停電などから情報システムや情報資産を保護し，安全を確保するための対策のこと。対策例として、サーバ室の設置、空調管理、入退室管理、電源や通信回線及び機器の二重化、盗難防止器具などがある。

2-2　分散コンピューティングとフォールト・トレランス性

フォールト・トレラント・システム（*fault tolerant system*）は、その構成部品の一部が故障しても正常に処理を続行が可能となるシステムである[2]。すなわち障害が発生した場合、単純な設計のシステムでは少しの障害でも全体が停止するが、フォールト・トレラント・システムでは完全に機能を保ったまま処理を続行するか、障害の重大性に応じて機能を低下させながらも処理を続行する。フォールト・トレランス性は連続稼働が求められるシステムや人命に関わるシステムで特に要求される。またフォールト・トレランス性は個々のマシンの特性というのみではなく、マシン間の連携（多重化や分散処理）についての規則の特性でもある。

フォールト・トレラント・システムに求められる基本的特性は以下の通りである。

(1)　単一障害点（single point of failure）がないこと（障害に対して全体の障害とならないよう対策が施されていること）

(2)　単一故障点（single point of repair）がないこと（ハードウェア故障についても前号と同様であること）

(3)　障害部品の隔離ができ、障害の伝播を防ぐこと

(4)　代替モードがあること

また、二重化（多重化や冗長化）によるフォールト・トレランス性は三つに分類される。

(1)　**レプリケーション**：同じシステムを複数稼動し、それら全部に同じ処理を並列に実行させて定足数を満足した結果を正しい結果として採用する。

(2)　**冗長性**：同じシステムの複製を複数用意し、障害が発生した場合は予備のシステムに切り替える。

(3)　**多様性**：同じ仕様であるが異なる実装のシステムを複数稼動させ、レプリケーションと同様にこれらを運用する。この場合、各システムが同じ障害を発生することがないと考えられるが開発や保守のコストが大きい。

ビザンチン将軍問題（*Byzantine Generals Problem*）とは、相互に通信しあう何らかのオブジェクト群において、通信及び個々のオブジェクトが故障または故意によって偽の情

[2] 分散システムにおけるフォールト・トレランス性の詳細についてはタネンバウム（2003）第 7 章を参照せよ。

報を伝達する可能性がある場合に、全体として正しい合意を形成できるかを問うものである。またフォールト・トレラント・システムにおいては、多数決の妥当性や分散処理の妥当性に関する問題とされる。

なおビザンチン将軍問題に帰結される故障や障害を**ビザンチン故障**（*Byzantine Failure*、あるいは**ビザンチン障害**）と呼び、ビザンチン将軍問題が発生しても全体として正しく動作するシステムを**ビザンチン・フォールト　・トレランス性**（*Byzantine Fault Tolerance*）があるという。

ビザンチン将軍問題は、東ローマ帝国（ビザンチン帝国）の将軍達がそれぞれ軍団を率いてひとつの都市を包囲しており、彼らが都市攻撃計画について合意したいと考えている状況において発生する。ここで最も単純な形では、将軍達は攻撃するか撤退するかのみを合意決定するが一部の将軍達は攻撃したいと思い、他は撤退を望むかもしれない。しかし重要な点は、将軍達は一つの結論に合意しなければならないということであり、一部の将軍だけで攻撃を仕掛けても敗北することは明らかであるため、全員一致で攻撃か撤退かを決めなければならない。なお、彼らはそれぞれ離れた場所に各軍団を配置しており、メッセンジャーを相互に送ることで合意を目指す。さらに前提条件として、彼らのうちの一部の将軍は裏切り者であり、最適でない戦略に票を投じて混乱させることがある。

例えば、5 人の将軍が投票して 2 人が攻撃で 2 人が撤退に票を投じたとすると、5 人目の裏切り者でもある将軍は一部の将軍達には撤退票を送り、他の将軍達には攻撃票を送るかもしれない。この結果 5 人目から撤退票を受けた将軍達は撤退し、残りの将軍達は攻撃を開始して敗走することになる。ここで裏切り者でない誠実な将軍達が全員一致で攻撃または撤退に同意しているとき、ビザンチン・フォールト・トレランス性は達成可能であるという。

ビザンチン故障とは、分散処理システムにおいてアルゴリズムを実行中に発生する故障や障害である。**不作為障害**（*omission failures*）と**作為障害**（*commission failures*）が含まれる。ここで不作為障害とは、クラッシュまたは要求の受信に失敗することや、応答の送信に失敗することなどを指す。また作為障害とは、要求を不正に処理することや、要求に対して不正または一貫しない応答を返すことなどを指す。

このためビザンチン故障を前提とした実環境のモデルでは、ハードウェアの故障やネットワーク輻輳または切断やソフトウェアのバグまたは悪意ある攻撃によってコンピュータやネットワークが予期しない動作をする。ビザンチン・フォールト・トレランス性アルゴリズムは、このような故障や障害に対処し、仕様で解決するよう指定された問題を解決できなければならない。このようなアルゴリズムは一般に、ビザンチン故障の状態にあるプロセスを何個まで許容し対処できるかで特徴付けられる。これを**回復力**（*resilience*）　t で表す。前述の将軍の例では A、B、C の三人のうち A が裏切り者であるとき、A が B には攻撃すると伝えるが C には撤退すると言い、B と C が相互にやりとりして A からの伝達内容を確認し合った場合、B も C も誰が裏切り者であるかを判断できないのである。（B か

C が裏切り者だった場合でも内容が食い違う。）すなわち将軍の人数を n、裏切り者の人数を t としたとき、解決策が存在するのは n が（3 × t + 1）以上の場合のみである。

なおビザンチン将軍問題も含めた古典的な合意問題の多くは、システムのプロセス数を n としたとき、n > 3t を満たさない場合の解が存在せず、障害が全プロセスの 3 分の 1 未満である状況でないと正しい動作を保証できない。すなわちメッセージに嘘があったとしても、障害プロセスが全プロセスの 3 分の 1 未満であればビザンチン・フォールト・トレランス性は達成される。

2-3　経済学的観点での情報セキュリティー問題[3]

近年、情報セキュリティーの機能不全はその悪い設計と同じくらいの頻度で悪い誘因（インセンティブ）によって引き起こされるとされてきた。また情報システムは特に、これを管理する者がミスをしてもその被害者にならない（責任を負わない）場合に失敗する傾向にある。すなわちミクロ経済学の理論及び手法やゲーム理論は、セキュリティー技術者にとっての暗号化理論と同じくらい重要となっている。

前述の誤ったインセンティブの例として、かつて人々はウイルスにより自分のパソコンが駄目になるのを防ぐためには費用を掛けたが、ウェブサイトに対するサービス不能攻撃に加担しないために金を使うことはなく、これはモラルハザードに当たるものである。また法学的には責任はリスクをいちばん管理できる側に割り当てられるべきであることが、ネットワーク上のリスクはこれがうまく分配されていないために、結果としてプライバシーの侵害等が起こる。さらにネットワークにおいては経済学の理論における、双方が取引することを望んでいるが片側が結果に影響する観察できない行動をとるときに発生する「情報の非対称性」といった側面も伴い、例えばファイル共有システムの利用者は他人と共有することを選んだかどうかを隠すことができるので、これらの中にはそのシステムの運営に協力するよりもむしろ「**ただ乗り（フリーライド）**」する者が存在するということも起こり得る。

情報産業は、個別の動作が他への副作用を持つ点で多くの異なる外部性を持つことが特徴であり、例えばソフトウェア業界については互換性という便益のために支配的な安定の方へ向かうことが挙げられる。経済学ではこれをネットワーク外部性と呼び、これにより大規模ネットワークあるいはソフトウェア利用者のコミュニティーはそれの各メンバーにとってより価値があるものとなる。またこれは OS の進歩や支配だけでなく、セキュリティーの欠点の特徴を説明することも可能とする。すなわち、プラットフォームのベンダは市場での位置を構築しているとき、概して初めにはセキュリティーを無視し、後にいったん利益のある市場を捕らえると厳重に顧客を確保するために過大なセキュリティーを追加する。

さらにこの外部性として、経費は一般に個々の投資の成果への変化に依存するが、セキュリティー投資の影響はしばしば投資者自身の決断だけでなく他者の決定にも依存すること

[3] 本節の説明は Varian(2004)に依拠している。

が挙げられる。例えばソフトウェアプログラムの正確さは作成する者のうち最小限の努力に依存する一方、そのソフトウェアの有効性と攻撃への強さは全員の努力の合計（最大限の努力）に依存する。すなわちある単純なモデルでは、各プレイヤーのコストは防御に費やされた努力である一方、プレイヤーへの期待される便益はシステムが故障を避ける確率である。そしてこの確率が個々の努力の合計の関数であるとき、システムの信頼性はいちばん高い費用対便益の比率をもつプレイヤーに依存し、この結果他のすべてのプレイヤーはフリーライドとなる。また別のモデルでは、セキュリティー投資は戦略の補完物になり得ることを示しており、個々の取る安全のための措置は他人が自分の投資を思いとどまらせる正の外部性を生むことが挙げられる。

また、一般的にネットワーク外部性をもつ技術は初期の緩やかな普及から、いったんユーザの数がある臨界量に達するとその率が急増するという古典的な S 字曲線となる。しかしこの逆の例として、セキュリティー技術において費用は最小限の数のプレイヤーが採用するまでは便益よりも大きいかもしれないが、もし誰もが最初に行く他人を待つならその技術は決して展開しないというブートストラップ問題がある。

近年の主流である積極的なソフトウェアの脆弱性の公表は社会的に望ましいかどうかについて、ソフトウェアベンダとセキュリティー研究者の間における議論がある。それはある研究者が、ソフトウェアへの攻撃はセキュリティパッチまたは公表により推測される脆弱性に基づいているため、その脆弱性が一般によって発見される可能性がなければ公表や頻繁なパッチに反対したというものであり、一方、脆弱性の公表はベンダに次の製品の発売において脆弱性を塞ぐインセンティブを与えるのを助けるといった意見もある。

またベンダはもっと安全なソフトウェアを作ることができるが、ソフトウェア業界の経済学は彼らにそうするためのインセンティブをほとんど与えないという側面がある。これは、消費者は一般に機能を追加することや市場で初めてであること、そして特にネットワーク外部性を伴うプラットフォーム市場で最も有力になることに対してベンダを報いるからである。そしてベンダの動機付け不足のもう 1 つの局面は、ソフトウェア市場が「レモン市場」であることである。すなわちベンダは自身の製品のセキュリティーについて対価を求めるが、消費者は彼らを信用する理由を持っておらず、さらに多くの場合ベンダでさえ自身のソフトウェアがどのくらい安全であるかを知らない。このため消費者はそのセキュリティーのために経費を掛ける理由を持ち合わせず、これによりベンダはセキュリティーに投資することに消極的になる。

以上のように情報セキュリティーの負の側面は、個人と組織に直面しているインセンティブの点と、市場の失敗の点からも説明可能である。

3. ゲーム・モデル

本論文では企業等における組織活動のひとつについて、情報セキュリティーに関する課題の解決を目指して論理的な改良を想定する。すなわち、情報資産に対する脅威のうち当該

組織における秘密情報の流出が電子メールの送信によって発生する場合を考える。なおこの事象の発生要因として、次のようなものが挙げられる。

- 電子メールの利用者（ユーザ）に悪意を持った者がいる。
- 悪意を持たないユーザが過って標的型メールに返信してしまう。

これらにより、従来のメール送信のための手順（図１）では情報の機密性が維持できなくなり、情報漏えいのリスクを伴うことになる。そこで、この送信手順（システム）に次に示す変更を加えることとする。

送信しようとするメールが送信者（クライアントノード）からメールサーバに到達するまでに複数のノード（例えば同僚や上司）を経由して、これら各中継ノードにおいてメールの内容の正当性（外部に送信しても良いか）をチェックする。ただし各中継ノードも１つのクライアントであるため、悪意を持つユーザであるか、または故障しているために正しくチェックできない場合がある（不正なメールを正当なものであると偽る）。このとき、本システムを維持するために故障ノードは全ノードのうち何個まで許容できるか、という問題は第２節で述べたビザンチン将軍問題の類似として捉えることができる。

上述したとおり、組織内のあるクライアントから送出されたメールは外部に送信されるまでにメールサーバを除くいくつかの中継ノードを経由する。ここでメールを発信するクライアントノードは、外部に送信しても良いもの（Good mail, G メール）と送信してはいけないもの（Bad mail, B メール）を確率的に送出する。各中継ノードは自身に到達した他ノードからのメールの正当性をチェックし、この結果を付加して次のノード（またはサーバ）に転送する。最後に、メールサーバは、到達したメッセージに付加された各中継ノードの判定結果から、あるルールに従って、メールを送信するか否かの最終的な判断を行う。

クライアントノードが B メールを発信する確率を p とする（G メールが発信される確率は $1-p$）。発信されたメールをチェックする中継ノード（クライアント）をプレイヤーとする。プレイヤーの数（中継ノードの数）を N で表す。議論の簡単化のため、N は奇数であるとする（$N \geq 3$）。各プレイヤーは対象メールを「チェックする（Yes）」か「チェックしない（No）」かを決める。Yes を選択すると、G メールには「OK」、B メールには「NG」のメッセージが対象メールに付加される。No を選択すると、メールの内容はチェックされず、G メールにも B メールにも「OK」のメッセージが付加される。Yes を選択するコストを c とする。各プレイヤーは他のプレイヤーが付加したメッセージを観察できないものとする。

メールサーバは、各プレイヤーによって付加されたメッセージのプロファイルを確認し、事前に定めた送信ルールに従って、対象メールを送信するかどうかを決める。G メールが送信されると、すべてのプレイヤーは a の利得を得る。B メールが送信されると、すべてのプレイヤーは d の損害を被る。

ここで、利得に関するパラメーターについて以下を仮定する。

仮定１：$a < d, c > pd, a(1-p) > c$

この仮定の意味は次のようなものである。B メールが送信されて被る損害は十分大きいが、それがクライアントから発信される確率が十分小さいので、期待値で見るとチェックを行うコストよりも小さい。また、G メールが正常に送信されることの便益は、チェック・コストに比して十分大きい。

メールサーバの送信ルールとして、本稿では以下の２つを考える。

（1）**全員一致ルール**（*unanimity rule*）すべてのプレイヤーのメッセージが OK であったときのみ送信する。

（2）**多数決ルール**（*majority rule*）過半数のプレイヤーのメッセージが OK であったときのみ送信する。

次章では、上記 2 種類の相互チェックシステムの性能について、プレイヤーのインセンティブおよびフォールト・トレランス性の観点から詳細に分析する。

4. 均衡分析

前章で設定したモデルを用いて、全員一致ルールと多数決ルールとの比較を行う。すなわち、それぞれのルールのもとで、各プレイヤーの行動をインセンティブの観点から検討し、その結果としていかなるナッシュ均衡が実現するかについて分析する。[4]4-1 節では故障ノードが存在しないケースを取り扱う。4-2 節では、4-1 節の議論を拡張して、中継ノードがビザンチン故障する可能性を考慮した分析を行う。

4–1　故障ノードが存在しないケース

この節では、プレイヤーは故障ノードを含まないケースの分析を行う。故障ノードが存在しない場合、いずれのルールにおいても、故障しているプレイヤーがいない場合、G メールは必ず送信される。したがって、B メールの送信を防ぐことができるかが重要となる。

まず、全員一致ルールにおける各プレイヤーのインセンティブをチェックする。全員一致ルールでは、1 人でも Yes を選択していれば B メールは送信されないことを注意しておく。プレイヤーA が、A 以外で Yes を選択しているプレイヤーがいる場合、A が Yes を選ぶことの期待利得は

$$(1-p)a - c$$

であり、No を選ぶことの期待利得は

$$(1-p)a$$

であるから、No を選ぶことが最適である。A 以外で Yes を選択しているプレイヤーがいない場合、Yes を選ぶことの期待利得は

[4] ゲーム理論の基礎については岡田(2011)、岡田他(2015)を参照せよ。

$$(1-p)a-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a-pd$$

である。仮定より $c>pd$ であるから、No を選ぶことが最適となる。すなわち、どのプレイヤーにとっても No が支配戦略となる。したがって、メールは誰もチェックしない結果となる。

次に、多数決ルールにおける各プレイヤーのインセンティブをチェックしよう。プレイヤーA 以外のプレイヤーで Yes を選択している者が$(N+1)/2$人以上いる場合、A の選択とは関係なく B メールは送信されない。このとき、A が Yes を選ぶことの期待利得は

$$(1-p)a-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a$$

であるから、No を選ぶことが最適である。A 以外に Yes を選択しているプレイヤーが$(N-3)/2$人以下しかいない場合、A の選択とは関係なく B メールは送信される。このとき、A が Yes を選ぶことの期待利得は

$$(1-p)a-pd-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a-pd$$

であるから、No を選ぶことが最適である。A 以外に Yes を選択しているプレイヤーがちょうど$(N-1)/2$人いる場合、A が Yes を選ぶことの期待利得は

$$(1-p)a-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a-pd$$

である。仮定より $c>pd$ であるから、No を選ぶことが最適となる。すなわち、どのプレイヤーにとっても No が支配戦略となる。したがって、メールは誰もチェックしない結果となる。以上を命題としてまとめておこう。

命題１　*仮定１が満たされるとき、全員一致ルールでも多数決ルールでも、すべてのプレイヤーにとって No が支配戦略となる。したがって、メールは全くチェックされず、B メールは送信されることになる。*

いずれのルールであっても、プレイヤーがメールをチェックするコストのため、チェックしないインセンティブが大きくなり、結果として誰もチェックしない事態となる。したがって、プレイヤーにチェックするインセンティブを与える必要がある。そこで、以下のような罰則規定を導入する。もし、B メールが送信されてしまった場合、No を選択した（すなわち B メールに OK メッセージを付加した）プレイヤーには利得単位で b だけの

ペナルティーが課されるものとする。ここで、ペナルティーの大きさは以下の条件を満たすほど十分に大きいことを仮定する。

仮定２：$b > \frac{c-pd}{p}$

上記の罰則制度を導入した上で、２つのルールにおけるプレイヤーのインセンティブをチェックする。

まず全員一致ルールを考える。プレイヤーA を任意に固定する。A 以外に Yes を選択しているプレイヤーがいる場合、A が Yes を選ぶことの期待利得は

$$(1-p)a-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a$$

であるから、No を選ぶことが最適である。A 以外で Yes を選択しているプレイヤーがいない場合、A が Yes を選ぶことの期待利得は

$$(1-p)a-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a-p(b+d)$$

である。仮定２より $c<p(b+d)$ であるから、Yes を選ぶことが最適となる。以上より、全員一致ルールの下でのナッシュ均衡点は次のように特徴付けられる。

命題２　*全員一致ルールに仮定２を満たす罰則規定が導入されるものとする。このとき、任意の１人のプレイヤーだけが Yes を選び、残りのプレイヤーは No を選択するような戦略の組はナッシュ均衡点であり、また純戦略ナッシュ均衡点はこのタイプのものに限られる。*

次に多数決ルールを考える。あるプレイヤーA 以外で Yes を選択しているプレイヤーが $(N+1)/2$人以上いる場合、A の選択とは関係なく B メールは送信されない。このとき、A が Yes を選ぶことの期待利得は

$$(1-p)a-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a$$

であるから、No を選ぶことが最適である。A 以外で Yes を選択しているプレイヤーがちょうど$(N-1)/2$人いる場合、A が Yes を選ぶことの期待利得は

$$(1-p)a-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a-p(b+d)$$

である。仮定２より $c<p(b+d)$ であるから、Yes を選ぶことが最適となる。A 以外で Yes を選択しているプレイヤーが$(N-3)/2$人以下しかいない場合、A の選択とは関係なく B メールは送信される。このとき、A が Yes を選ぶことの期待利得は

$$(1-p)a-pd-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a-p(b+d)$$

である $c<pb$ であれば Yes を選ぶことが最適であり、$c>pb$ であれば No を選ぶことが最適である。以上より、多数決ルールの下でのナッシュ均衡点は次のように特徴付けられる。

命題３　*多数決ルールに仮定２を満たす罰則規定が導入されるものとする。このとき、*$(N+1)/2$ *人だけが Yes を選択し、残りは No を選択するような戦略の組はナッシュ均衡点となる。さらに* $b>c/p$ *であれば、ナッシュ均衡点はこのタイプのものに限られる*[5]*。*

命題２より、適切な罰則規定が導入されると、全員一致ルールのナッシュ均衡点では、1 人のプレイヤーがメールをチェックすることになる。命題３より、多数決ルールの下では、$(N+1)/2$ 人だけがメールをチェックするようなナッシュ均衡点が存在する。したがって、いずれのルールであっても、B メールの送信を防ぐことがナッシュ均衡点において可能である。

命題４　*仮定２を満たす罰則規定が導入されるとする。全員一致ルールのナッシュ均衡点では、G メールは送信され、B メールは送信されない。多数決ルールでは、G メールは送信され、B メールは送信されないようなナッシュ均衡点が存在する。*$b>c/p$ *であれば、ナッシュ均衡点はそのようなものに限られる。*

最後に２つのルールの効率性について議論しておく。複数均衡の問題を避けるために、$b>c/p$ を仮定する。命題２と４より、全員一致ルールでのナッシュ均衡点では 1 人のプレイヤーだけが Yes を選び、G メールは送信されるが B メールは送信されない。このとき、プレイヤーの均衡利得の総和は

$$\{a(1-p)-c\}\times 1+a(1-p)\times(N-1)=a(1-p)N-c$$

である。一方、命題３と４より、多数決ルールでのナッシュ均衡点では、$(N+1)/2$ 人だけが Yes を選択し、G メールは送信されるが B メールは送信されない。このとき、均衡利得の総和は

[5] $c>pb$ のときは全員が No を選択することもナッシュ均衡点となる。

$$\{a(1-p)-c\}\times\frac{N+1}{2}+a(1-p)\times\frac{N-1}{2}=a(1-p)N-c\frac{N+1}{2}$$

である。すなわち、全員一致ルールのほうが多数決ルールよりも均衡総利得が大きい。これは、どちらのルールであっても、G メールは送信されて B メールは送信されないが、全員一致ルールのほうが Yes を選ぶ人数が少ないので、その分だけチェックのコストを節約することができるためである。以上を命題としてまとめておく。

命題５　$b>c/p$ *であるとき、全員一致ルールのほうが多数決ルールよりも均衡総利得が大きいという意味で効率的である。*

４−２　故障ノードが存在するケース

本節では、プレイヤーの一定数が故障等により正常に機能しない可能性を考慮に入れて、システムのフォールト・トレランス性を検討する。本稿では、プレイヤーの故障はビザンチン故障（任意故障）である場合を考える。故障プレイヤーは、G メールには NG、B メールには OK のメッセージを付加するものとする。メールサーバはどのプレイヤーが故障しているのかは判別できないものとする。当然のことだが、すべてのプレイヤーが故障していればシステムの安全性は全く期待できない。そこで、本稿では、故障プレイヤーの数にある上限がある場合でのシステムのパフォーマンスについて分析する。故障プレイヤーの数について以下を仮定する。

仮定３：故障プレイヤーの数は$(N-3)/2$以下である。

さらに、以下の分析においては、最悪のケースを想定して、どのプレイヤーも故障プレイヤーの数はちょうど上限の$(N-3)/2$であると認識して行動するものとして議論を進める。

まず、全員一致ルールから検討する。ここで最初に注意すべきことは、故障プレイヤーが存在する場合、全員一致ルールでは G メールは全く送信されない、ということである（故障プレイヤーは G メールに NG のメッセージを付加する)。プレイヤーA を任意に固定して、A 以外に Yes を選択しているプレイヤーがいる場合、A が Yes を選ぶことの期待利得は $-c$ であり、No を選ぶことの期待利得は 0 であるから、No を選ぶことが最適である。A 以外で Yes を選択しているプレイヤーがいない場合、A が Yes を選ぶことの期待利得は $-c$ であり、No を選ぶことの期待利得は $-p(b+d)$ である。仮定２より $c<p(b+d)$ であるから、Yes を選ぶことが最適となる。つまり、このゲームのナッシュ均衡点では、1 人だけが Yes を選び、残りのプレイヤーは No を選ぶことになる。したがって、均衡において G メールも B メールも送信されない。以上を命題としてまとめておく。

命題６　*全員一致ルールにおいて仮定２と３が満たされるとする。任意の１人のプレイヤ*

ーだけが Yes を選び、残りのプレイヤーは No を選択するような戦略の組はナッシュ均衡点であり、また純戦略ナッシュ均衡点はこのタイプのものに限られる。

次に、多数決ルールを検討しよう。プレイヤーA を任意に固定する。A 以外で Yes を選択しているプレイヤーが$(N-3)/2$人以下しかいない場合、A の選択とは関係なく B メールは送信される。このとき、A が Yes を選ぶことの期待利得は

$$(1-p)a-pd-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a-p(b+d)$$

である。$c<pb$ であれば Yes を選ぶことが最適であり、$c>pb$ であれば No を選ぶことが最適である。A 以外で Yes を選択しているプレイヤーがちょうど$(N-1)/2$人いる場合、A が Yes を選ぶことの期待利得は

$$(1-p)a-c$$

であり、No を選ぶことの期待利得は

$$(1-p)a-p(b+d)$$

である。仮定２より $c<p(b+d)$ であるから、Yes を選ぶことが最適となる。つまり、このゲームのナッシュ均衡点では、故障していないプレイヤーはすべて Yes を選択することになる。したがって、均衡では G メールは必ず送信されるが B メールは決して送信されない。

命題７　*多数決ルールにおいて仮定２と３が満たされるとする。故障していないプレイヤーは全員 Yes を選択するような戦略の組はナッシュ均衡点となる。さらに $b>c/p$ であれば、ナッシュ均衡点はこのタイプのものに限られる。*

命題６より、全員一致ルールのナッシュ均衡点では、１人のプレイヤーが Yes を選択するので、B メールは送信されない。すでに注意したように、故障プレイヤーが存在する場合、全員一致ルールでは G メールは全く送信されない。これに対して多数決ルールでは、命題７より、過半数のプレイヤーが Yes を選択するようなナッシュ均衡点が存在する。このとき、故障プレイヤーの存在の有無にかかわらず、G メールは送信されるが B メールは送信されない。さらに $b>c/p$ であれば、均衡はそのようなものに限られる。以上を命題としてまとめておく。

命題８　*仮定２と３が満たされるとする。全員一致ルールのナッシュ均衡点では B メールは送信されない。さらに、故障プレイヤーが存在するときは G メールも送信されない。多数決ルールでは、故障プレイヤーの存在の有無にかかわらず、G メールは送信されて B メールは送信されないようなナッシュ均衡点が存在する。$b>c/p$ であれば、ナッシュ均衡*

点はそのようなものに限られる。

最後に２つのルールの効率性について議論しよう。４−１節と同様、複数均衡の問題を避けるために、$b > c/p$ を仮定する。比較の基準としてマクシミン基準を採用する。すなわち、各ルールの利得総和を考えるときにもっとも悲観的な状況を想定し、その最小値を比較してどちらのほうがより大きいかを考える。本稿ではシステムのフォールト・トレランス性に注目するので、マクシミン基準で比較することは妥当であると思われる。したがって、以下では故障プレイヤーの数はちょうど$(N-3)/2$であると仮定して、故障していないプレイヤーの利得の総和を比較する。

命題６と８より、全員一致ルールでのナッシュ均衡点では１人のプレイヤーだけが Yes を選び、故障プレイヤーが存在するなら G メールも B メールも送信されない。このとき、故障していないプレイヤーの均衡利得の総和は

$$(-c) \times 1 + 0 \times \frac{N-3}{2} = -c$$

である。一方、命題７と８より、多数決ルールでのナッシュ均衡点では、故障していないプレイヤー全員（$(N+1)/2$ 人）が Yes を選択し、G メールは送信されるが B メールは送信されない。このとき、均衡利得の総和は

$$\{a(1-p) - c\}\frac{N+1}{2}$$

である。仮定１より、この値は$-c$よりも大きい。すなわち、多数決ルールのほうが全員一致ルールよりも均衡総利得が大きい。これは、どちらのルールであっても、B メールは送信されないが、全員一致ルールでは G メールが送信されない可能性があるためである。以上を命題としてまとめておく。

命題９　$b > c/p$ *であるとする。マクシミン基準では、均衡総利得に関して多数決ルールのほうが全員一致ルールよりも望ましい。*

5. 結語

本稿では、情報漏えいリスクに関して、クライアントがメール等の送信内容を相互にチェックするシステムの性能について検討した。従来の情報工学的なアプローチと異なり、チェックする中継ノードは機械ではなく人間であるとの立場から、チェックを行うことによるコストの存在を明示的に導入した上で、各ノードのインセンティブの観点から、チェックシステムとして全員一致ルールと多数決ルールのパフォーマンスの比較を行った。その結果、適切な罰則規定を導入すれば、いずれのシステムでも情報漏えいを防ぐことができることが示された。故障ノードが存在しない場合であれば、チェック・コストが少なくて済むという意味で、全員一致ルールが望ましい。一方、故障ノードの存在を前提とすると、全員一致

ルールでは、適切なメールであっても送信されないことになり、メール・システム自体が機能しなくなる恐れがあるが、多数決ルールであればそのような事態を避けることができる。

本稿では、検討を簡単にするためにゲームにおけるプレイヤーの数やノードの故障確率等に限定した値を用いた。しかし現実的にはこれよりも様々な条件が考えられ、情報漏えいによるセキュリティー・インシデントを効率的に防止するために、さらに実世界に近付けた条件を取り入れることが今後の課題として挙げられる。

引用文献

アンドリュー・S・タネンバウム、マーデル・ファン・スティーン（2003）『分散システム ── 原理とパラダイム』ピアソンエデュケーション

岡田章（2011）『ゲーム理論（新版）』有斐閣

岡田章、加茂知幸、三上和彦、宮川敏治（2015）『ゲーム理論ワークブック』有斐閣

Anderson, R. and Moore, T (2006) “The Economics of Information Security,” *Science* **314.**

Eliaz, K (2002) “Fault Tolerant Implementation,” *Review of Economic Studies* **69**.

Hirshleifer, J. (1983) “From weakest-link to best-shot: the voluntary provision of public goods.” *Public Choice*, **41.**

Varian, H.R. (2004) “System Reliability and Free Riding.” In L. Camp and S. Lewis (ed.), *Economics of Information Security* (Advances in Information Security, Volume 12), pp.1-15. Kluwer Academic Publishers.