情報処理学会論文誌 Vol. 52 No. 6 2019–2030 (June 2011)

組織のITセキュリティ対策のゲーム理論による分析 —セキュリティ推進部門と従業員間の指示と実施のゲーム

杉浦 昌[†1,†2,†3] 諏訪博彦[†1]
太田敏澄[†1]

本論文は，組織内でセキュリティ対策を指示する立場のセキュリティ推進部門とその指示を受けて実施する立場の従業員の行動をモデル化し，組織内のセキュリティ対策をゲーム理論を用いて分析したものである．推進部門と従業員の2プレーヤからなる非協力の戦略型ゲームを考え，それぞれのペイオフにより形成されるゲームの構造を明らかにした．常時実施ゲーム，指示実施ゲーム，指示非実施ジレンマゲーム，常時非実施ジレンマゲーム，常時非実施ゲームの5種類のゲームが存在することを明らかにし，いくつかのセキュリティ対策の事象を5種類のゲームの空間上に位置づけた．どのようなセキュリティ対策上の変数に着目して施策を変化させればゲームの種類が変化してセキュリティ対策の効果があるかを分析した．従来経験的にいわれてきた変数の変更が有効であることをモデル上で理論的に示すとともに，経験上あまり知られていなかった現象についても分析した．最後に，本モデル化による分析の有効性と今後の可能性を考察した．

Analysis of IT Security Implementation in an Organization by Using Game Theory: A Game between IT Security Section and Implementing Employee

Masashi Sugiura,[†1,†2,†3] Hirohiko Suwa[†1] and Toshizumi Ohta[†1]

We have developed a model based on game theory of IT security implementation in organizations. The game has two players: one works in the IT security section, which promotes implementation of IT security, and one who implements IT security in his/her section. Their strategies in the game are formulated on the basis of the expected costs and benefits of implementation. Analysis of the model revealed five types of games: regular implementation, promotion-implementation, promotion-non-implementation dilemma, regular non-implementation dilemma, and regular non-implementation. The regular implementation and promotion-implementation type games occurred depending on the cost of the employee to be directed by the promotion section and on the value of the penalty and the probability felt by the employee. We observed some examples of IT security implementation, classified them into five types of games, and analyzed which changes in security parameters are effective. We showed theoretically that certain changes in parameters which were reported from experiences are effective, and analyzed the effects that were not understood well in experiences. Finally, we showed the effectiveness and the possibility for future extension of this model.

1. はじめに

セキュリティ事件・事故は，発生すると大きな損害につながる場合が多い．1999年に発覚した宇治市での漏えい事件の場合，住民への実際の賠償額は1人あたり1万5,000円であった[⋆1]．NPO日本ネットワークセキュリティ協会の調査報告書[1)]によれば，個人情報が漏えいした事故の1人あたりの平均想定損害賠償額は4万3,632円，事故の1件あたりの平均想定損害賠償額は1億8,552万円となっている．

このため，組織におけるITセキュリティ対策は大きな課題となっており，多くの組織ではセキュリティ対策に多大な費用と労力を注いでいる．しかし，技術的な対応だけでは限界があり，技術と並んでマネジメントも重要であることが，車輪の両輪になぞらえて指摘されている[2)]．このため，セキュリティポリシの制定や組織内教育の充実，セキュリティ監査の実施などの方策が多くの組織で進められている．

それにもかかわらず，実際には，定められた方策が守られずに事件・事故に至った例が数多く発生している．たとえば，持ち出しが禁止されているデータを持ち出してそれを紛失もしくは盗難被害にあって情報漏えい事件となったり，使用を自粛するよう強く求められてい

†1 電気通信大学
University of Electro-Communications
†2 独立行政法人情報処理推進機構
Information-Technology Promotion Agency, JAPAN
†3 日本電気株式会社
NEC Corporation

⋆1 2002年7月11日，1人あたり慰謝料1万円，弁護士費用5,000円の判決が確定．

る P2P ファイル共有ソフト[⋆1]がインストールされた個人用 PC で業務を行っている中で暴露ウイルスに感染して情報漏えいとなったりする事件・事故が続いている．2009 年 1 月から 7 月の間をみても，教育・福祉関係者による児童の情報の紛失や盗難の事故[⋆2]，会社員や医療関係者，団体職員などによるファイル共有ソフトを介したネットワークへの情報漏えい事故[⋆3]などが数多く報道されている．

同様のセキュリティ事故はすでに過去数年にわたり新聞やテレビ，ラジオなどで数多く報道され大きな話題になっているうえ，事故を起こした本人の所属組織のセキュリティ管理部門は注意喚起や禁止行為の通達を出していたケースが多い．したがって，事故を引き起こした本人がその危険性をまったく知らないまま実行して事故が発生したとは考えにくく，本人はある程度は危険性を認識していたと思われる．

データを持ち出した理由が自宅で業務を行う目的であったケースも多い．多少の危険性を感じつつも業務の必要性を優先させた結果の可能性がある．

このように，従業員が自らの判断で組織のセキュリティ管理者の指示に従わない場合，従来よくいわれている教育や普及啓発の徹底だけではこれらのセキュリティ事故を防ぐことはできない．従業員の振舞いのメカニズムをあきらかにしたうえでセキュリティ対策を考える必要がある．

そこで本論文では，組織内のセキュリティ対策の推進と実施の構造をモデル化し，ゲーム理論を用いて分析することにより，これらに対する解決策を検討する．

なお，金銭詐取の行為や遺恨などによる意図的なセキュリティ違反は，通常の行動とは異なり利益追求や悪意を持って積極的に違反を犯す行為なので，本論文では検討の対象外とする．また，対象とするセキュリティ対策は，サーバの OS やアプリケーションプログラムの脆弱性対策や DB 連携 Web サーバの SQL インジェクション対策などのような，専門性の高いものおよびその対応を行う者が専門家に限られるものは除外する．一般の従業員にそのセキュリティ対策の内容や効果が理解されていないものも除外する．前者は専門家のセキュリティ対策技術の問題であり，後者はセキュリティリテラシの普及啓発の問題だからである．

本論文の構成は以下のとおりである．2 章で組織内のセキュリティ対策の選定とその遂行に関する先行研究を紹介する．3 章で実際の組織で実施されているセキュリティ対策を分析し，4 章でその状態をセキュリティ対策推進ゲームとしてモデル化する．5 章でモデル化したゲーム構造を分析し．6 章でゲームの特性に基づきセキュリティ対策の推進を改善する方策について考察する．最後に 7 章で結論を述べる．

2. 先行研究

組織のセキュリティ対策の選定と遂行に関する先行研究について述べる．

セキュリティ対策の実施にゲーム理論を適用した研究として，宮崎ら[3] の研究がある．電子署名技術の利用において署名者が債務超過状態の債権者であるような場合を例にあげ，署名鍵の自己暴露が債権者に対する攻撃となりうることをゲーム理論を用いて分析している．しかし，特定の条件下での分析を試みたものであり，組織内のセキュリティ対策実施の構造を明らかにするものではない．

セキュリティ対策の選定を定式化した研究としては兵藤ら[4] の研究がある．資産，脅威，対策のそれぞれを構成要素単位で取り扱い，選択した対策案の組合せごとに平均残存資産と対策コストの差分の期待値を最大化するモデルを考え，セキュリティ対策案選定問題を離散最適化問題として定式化している．セキュリティ対策の投資効果を定量化して最適投資を求める研究としては，Gordon ら[5] の研究や松浦[6] の研究がある．定量的にリスクの分析とセキュリティ対策の検討を行った研究としては，実際の情報流出事故のデータをもとにリスク解析を行って評価基準に重み付けを与え効果的なセキュリティ対策を求めた弓削ら[7] の研究がある．しかし，これらの研究は，従業員がセキュリティ対策の指示に従わない現象を説明するものではない．これを説明するためには，組織がセキュリティ対策を推進する部門と実行する部門とから構成されていることを考慮して，検討を行う必要がある．

⋆1 2006 年 3 月 15 日，安倍官房長官（当時）が記者会見で P2P ファイル共有ソフトを使わないよう国民に呼びかけ．

⋆2 2009 年 7 月佐賀市の幼稚園で園児の個人情報が記録された USB メモリを許可なく持ち出し紛失，2009 年 4 月福岡市で児童の個人情報を許可なく持ち出して盗難．

⋆3 2009 年 7 月生保社員が自宅で作業中に持ち出し禁止の業務データ・従業員の個人データを漏えい，同 6 月佐賀県の病院職員が自宅で作業中に持ち出し禁止の患者個人データを漏えい，同 6 月福岡県のガス会社職員が自宅で作業中に持ち出し禁止の顧客個人データを漏えい，同 5 月退職した信金職員が自宅で顧客個人データを漏えい，同 4 月東京の病院職員が自宅で作業中に持ち出し禁止の患者個人データを漏えい，同 4 月広島の教育関係者が自宅で作業中に持ち出し禁止の生徒個人データを漏えい，同 4 月熊本県の職員が自宅で作業中に持ち出し禁止の業務データ・職員個人データを漏えい，同 2 月埼玉の警察官が自宅で作業中に持ち出し禁止の職員データを漏えい，同 2 月名古屋の学会運営会社社員が自宅で作業中に持ち出し禁止の個人情報データ・業務データを漏えい，同 1 月東京のレンタルサーバ会社従業員が自宅で作業中に持ち出し禁止の顧客個人データを漏えい，同 1 月環境庁の委託を受けた調査会社社員が自宅で作業中に持ち出し禁止の調査対象の個人データを漏えい，同 1 月イベント会社元社員が自宅で持ち出し禁止の顧客個人データを漏えい，同 2 月北海道の電力関係団体職員が自宅で作業中に持ち出し禁止の顧客データ・業務データを漏えいした件の最終調査結果公表．

3. 組織のセキュリティ対策の分析

実際の組織で行われているセキュリティ対策の推進について考察し，その基本的な構造を明らかにする．

3.1 セキュリティ推進の体制

セキュリティ対策の選定には専門知識が必要であり，その判断を組織内の個々人にまかせていては効率が悪い．組織としての統一がとれなかったりセキュリティ対策が組織の方針と齟齬をきたしたりするおそれもある．また，現実の組織では，経営層をはじめさまざまな部門があるためそれぞれが勝手に対策を決定するのでは混乱が大きい．このため，多くの組織では，スタッフ部門にセキュリティ対策の推進部門を作ったり組織内 IT の推進者と兼任させたりして組織全体のセキュリティ対策の選定と推進活動を行い，組織内の従業員はその指示を受けて実際のセキュリティ対策を実行する例が多い．

組織における情報セキュリティマネジメントの導入，実施，維持および改善のための指針および一般的原則について規定した規格 ISO/IEC27002（JIS Q27002）[8] をみると，「6. 情報セキュリティのための組織」において「（組織内の情報セキュリティを管理するため）組織内において情報セキュリティを導入し，その実施状態を統制するための管理上の枠組みを確立することが望ましい」として，セキュリティ対策を推進する部門もしくは機能について述べている．つまり，セキュリティ対策を管理する立場と管理を受ける立場の二者からなる構成の考え方が示されている．よって本論文では，セキュリティ対策推進部門と従業員の二者からなる構造を考える．

3.2 セキュリティ対策推進部門と従業員の目的の違い

セキュリティ対策推進部門は，組織内のセキュリティ対策の推進が自らに与えられた任務職責である．このため，可能な限りセキュリティ対策を指示し推進したいという意志を持つ．

一方，組織内の一般の従業員は，セキュリティ対策の必要性について理解はしているものの，本来の職務は与えられた業務の遂行である．したがって，業務の遂行に大きな影響が出ないのであれば，推進部門の指示に従ってセキュリティ対策を実行するが，そうでない場合には指示に従わない方が自らの得となる．

従業員が推進部門の指示に従わない事態を避けるため，セキュリティ推進部門は，指示に従わない従業員に対してペナルティを与え，実行を強制する場合が多い．ペナルティの付与は ISO/IEC27002（JIS Q27002）でも「8.2.3 懲戒手続き」の管理策として「セキュリティ違反を犯した従業員に対する正式な懲戒手続きを備えることが望ましい」と規定されており，従業員就業規則の一部として規定されている場合などを含め，多くの組織で実施されている．

ペナルティは，従業員にとっては負担となるため，指示に従わないことに対する抑止力の役割を果たすが，推進部門にとっては直接の利益とならないのが普通である．実際のペナルティの内容は賠償のような計量可能なものである場合もあるが，組織内の就業規則や規定，ルールのような，数値化しにくいものもある．本論文では，従業員が感じる負担をコストに換算したものをペナルティの値とする．

3.3 セキュリティ対策に必要な費用の負担

実際の組織では，セキュリティ対策に必要な費用や事故が発生した場合の対応の費用を個別に利用部門に要求することは少なく，あらかじめ組織内の共通の賦課費用として各部門に拠出を割り振って得られた予算のなかからセキュリティ推進部門がそれを適切に活用して組織のセキュリティ対策を行う場合が多い．よって本論文では，対策に直接必要な設備投資の費用や事故が発生した場合の対応の費用はセキュリティ推進部門が負担するものとする．

3.4 実施するセキュリティ対策

セキュリティ対策にはさまざまなものがある．ISO/IEC27002（JIS Q27002）は，企業や組織が選択しうるセキュリティの方策として 11 のカテゴリに分類した 133 個の管理策（Controls）をあげている．この管理策は一般的原則であるため，組織において実際のセキュリティ対策として実行するにはさらに具体化する必要がある．このため，実際のセキュリティ対策はさらに多種多様なものとなる．

組織の特性や実態にあわせて管理策をより具体化した例として，地方公共団体における情報セキュリティポリシに関するガイドライン[9] がある．本ガイドラインは，総則，情報セキュリティ基本方針，情報セキュリティ対策基準の 3 章構成からなる．情報セキュリティにおける基本的な考え方を定めたものが基本方針で，これに基づく共通の情報セキュリティ対策の基準を定めたものが対策基準である．さらに本ガイドラインの内容をふまえ，組織内で実際にそれが正しく適用されているかどうかを確認するためのものが情報セキュリティ監査のガイドライン[10] である．平成 15 年 12 月に発行された初版では監査項目が 975 項目と多く，内容を整理した平成 19 年の改版後も 317 項目となっている．

このように，具体的な情報セキュリティ対策は非常に多岐にわたり数が多いため，すべての対策を一律，同時期に実施するのは不可能である．このため，セキュリティ推進部門は，さまざまな条件を考慮に入れながら，自組織においてどの対策の実施を指示しどの対策は指示しないかの取捨選択の判断を行う．よって本論文では，セキュリティ推進部門は，1 つ

1 つのセキュリティ対策ごとに，その実施を指示するかしないかの二者択一の選択を行うものとする．

3.5　リスクアセスメント

セキュリティ対策のあるべき姿としては，組織が自組織が持っている情報資産を洗い出し，それに対する脅威の大きさとそれが発生する確率とを考え，対策を施した場合にどこまでリスクが減って残存リスクが許容リスクを下回るかを検討したうえでセキュリティ対策を決定することが望ましい．これは，JIS Q 13335-1 [11] の「3.6 リスク」「3.9 セキュリティ要素の関係」や 2000 年 7 月に出された政府の情報セキュリティポリシガイドライン[12] にも，セキュリティ対策として望ましいリスクアセスメントの進め方として記載されている．

実際の組織では，ISO/IEC27002（JIS Q27002）や 3.4 節で述べたガイドラインなどに示されたセキュリティ対策を参考としつつ，自組織における過去の事例から得られた経験などを加味し，可能なセキュリティ対策の候補を先に決める．そしてそのセキュリティ対策ごとにリスクアセスメントを行い，対策を決定していく．

セキュリティ対策は，大きな投資額が必要なかわりに得られる効果が及ぶ範囲が広いものや，逆に投資額が小さいかわりに範囲が狭いものなどがある．このため，本論文では，対象とするセキュリティ対策は単位費用あたりで考えるものとする．

4. セキュリティ対策推進ゲーム

3 章で考察したセキュリティ対策の状況をモデル化し定式化するため，組織内でのセキュリティ対策の推進と実施をゲームとして表す．ゲームは，ある 1 つのセキュリティ対策の推進について考える．本論文では繰返しや混合戦略を考えない非協力の戦略型ゲームを考える．

本論文では，Umehara ら[13] が迷惑施設や原子力施設などのリスク情報の開示を行政と住民とをプレーヤとするゲームとして分析した手法をベースとして議論を展開し，定式化を行う[⋆1]．

4.1　プ レ ー ヤ

本論文では，3.1 節で考察したように，セキュリティ対策を指示し推進する立場である「推進部門」とセキュリティ対策を実行する「従業員」との 2 プレーヤのゲームを考える．推進部門はセキュリティ対策の選定と組織内への実施の指示を行う立場であり，従業員は自らの業務の遂行を目的としつつ推進部門からのセキュリティ対策を実施するよう求められる立場である．

実際の組織では，推進部門が階層構造となっていたり個々の従業員によって判断が異なったりグループを形成したりして，三者以上のプレーヤが相互に影響を及ぼしあう形態もあるが，それらの分析は今後の課題とする．

4.2　戦　　略

3.4，3.5 節で考察したように，現実の組織では，個々のセキュリティ対策の採用を個別に判断する．すなわち，ある 1 つのセキュリティ対策について推進部門がとりうる戦略は，その対策の実施についての「指示」と「非指示」の 2 つとなる．

一方，3.2 節で考察したように，一般の従業員は，そのセキュリティ対策の業務への影響や実施の手間，指示の有無を勘案し，自らの判断により対策を実施するか実施しないかを選択する．すなわち一般の従業員の戦略は，セキュリティ対策の「実施」と「非実施」である．

4.3　推進部門のペイオフ G_1

推進部門のペイオフ G_1 について考える．

(1)　推進部門の任務職責

3.2 節で考察したように，推進部門は，組織内のセキュリティ対策の推進が自らに与えられた任務職責である．このため，セキュリティ対策を指示することにより，推進部門は組織から利得を得る．この利得の値を M とする．M は正の値である．指示しない場合は利得は 0 である．利得を金額に換算したものを M の値とする．

(2)　事故が発生したときの対処コストの負担

3.3 節で考察したように，従業員がセキュリティ対策を行わず，その結果セキュリティ事故が発生したとき，推進部門は業務の一環として事後対策を行う．推進部門が認識しているセキュリティ事故が発生する確率を P_1，事後対策にかかる費用を S_p とすると，事故が発生した場合に推進部門は P_1S_p のコストを負担することになる．このとき，もしも推進部門がセキュリティ対策の実施を指示したにもかかわらず従業員が実行しなかった場合，推進部門は任務職責は果たしたものの事故が発生した際に事後対策のコストを負担することになり，$M - P_1S_p$ の負担となる．

この $M - P_1S_p$ の値は通常は負の値となる．なぜなら，対策をすすめるために推進部門に与えられる利得 M よりもセキュリティ事故による損害 P_1S_p が小さいのであれば，その

⋆1 Umehara らは，迷惑施設や原子力施設などに関するいわゆる「リスク情報」を行政が住民に開示するかどうかを，住民と行政とをプレーヤとするリスク情報開示ゲームで表現し，行政がプロスペクト理論に従った場合にはリスク追及行動をとって開示しない場合があることを示した．本論文ではこのゲーム化の手法をセキュリティ対策推進部門と従業員間の指示と実施に適用し，分析を行う．

セキュリティ対策を指示したほうが全体としての出費が大きい，すなわち，何も対策をしないほうが損失が少ない状態となり，そもそもその施策自体の意味がないからである．また，これが正の値であるとすると，それは，セキュリティ推進部門が，その組織において実際のセキュリティ被害が出ることよりも，推進部門がセキュリティ対策の指示を行うこと自体のほうに大きな利得を感じる，すなわち，事故の発生を防ぐことよりも，自らが指示を行うことのほうを重要と判断するということであり，このような，セキュリティ対策の指示そのものの利得が大きく，指示自体が自己目的化してしまっているような状態は，明らかに正常な組織のあり方ではない．

そこで本論文では，利得 M よりも P_1S_p の値のほうが大きい，すなわち，$M - P_1S_p$ が負の値である状況を考える．

(3)　推進部門のペイオフ G_1 の値

推進部門のペイオフの値は推進部門自身のとる戦略と従業員のとる戦略の組合せにより変わる．あるセキュリティ対策に関する推進部門のペイオフ G_1 を，

G_1（推進部門の戦略：従業員の戦略）

で表記する．G_1 は，4.3 節 (1)，4.3 節 (2) の議論より，従業員がとる戦略と推進部門がとる戦略の組合せによって以下のようになる．

G_1（非指示：実施）$= 0$ (1)

G_1（非指示：非実施）$= -P_1S_p$ (2)

G_1（指示：実施）$= M$ (3)

G_1（指示：非実施）$= M - P_1S_p$ (4)

4.4　従業員のペイオフ G_2

従業員のペイオフ G_2 について考える．

(1)　セキュリティ対策を実施することによる業務効率の低下

本来セキュリティ対策は通常の業務に影響を与えないのが理想である．しかし，現実にはセキュリティ対策を行うことにより業務効率の低下を招くことが多い．たとえば，USB メモリの利用を禁止したりノート PC の持ち出しを禁止したりすることは，データの受け渡しの利便性の低下やモバイルコンピューティングの活用による業務の効率化を阻害することになる．実際，情報セキュリティを強化すると業務効率が下がるとの意見がそれを否定する意見やその他の意見を上回ったという上場企業の従業員へのアンケート調査の結果も報告されている[14]．

本論文では，セキュリティ対策を実施したときのそれによる業務効率の低下をコストとして金額に換算したものを Y_d とする．

(2)　セキュリティ対策を実施しないときのペイオフ

従業員は，セキュリティ対策を実施しないとある確率で事故が発生し，そのときに自分の業務に損失が発生すると考える．この従業員が考える事故の発生確率を P_2，損失の値を Y_2 とする．セキュリティ対策を実施しないときに従業員が感じるコストは P_2Y_2 である．

(3)　推進部門の指示に従う際の従業員のコスト

推進部門がセキュリティ対策を指示した場合，従業員がそれに従う際には対応に必要なコストが発生する．

たとえば，実際の対策として，外部に持ち出すノート PC や USB メモリを貸し出し制にしてそのつど借用と返却を管理するルールを制定したり，職場への出入りに際してのノート PC の守衛への届出を行うルールを制定したりする例がある．これらは従業員にとって負担となり，コストとして認識される．ノート PC や USB メモリの管理を推進部門からの指示によらずその部門内で行っている場合，通常は貸し出しノートへの記帳などの作業が普通であり，そのような方策でもセキュリティ対策として効果がある．しかし，推進部門がそれを推進する場合，組織内での統一書式の制定や推進部門への報告書の作成，部門の上司や責任者の承認印などを求めることが多いため，従業員にとって手間がかかったり上司の不在の間は承認が受けられず持ち出しができなかったりして負担となり，コストとして認識される．

この推進部門がセキュリティ対策を指示した際に従業員がそれに従うのに必要な従業員の負担，すなわち従業員にとっての推進部門に指示されマネジメントされるコストを，対応コスト C_a とする．

(4)　推進部門が従業員に与えるペナルティ

推進部門は組織内のセキュリティ対策推進の責任と権限を負っている．このため，3.2 節で考察したように，実施を指示したにもかかわらず従業員が実施しなかった場合，従業員に対してペナルティを与えることがある．従業員に対するペナルティは推進部門にとって直接の利益とはならないため，推進部門のペイオフには影響しないが，従業員にとってはコストとなる．この推進部門が従業員に与えるペナルティを金額に変換したものを V とする．

しかし，ペナルティ V は，従業員にそのままかかるわけではない．一般に，従業員が指示を正しく守っているかどうかを推進部門がつねに正確に把握することは容易ではない．多くの場合，従業員が指示に従わなくてもそれは推進部門には分からず，実際に事故が発生してからそれが判明する．つまり従業員からみれば，ペナルティ V によるコストは，事故発生の確率 P_2 を乗じた値 P_2V となる．

表 1　セキュリティ対策推進ゲーム
Table 1　Game between promotion section and employee.

利得表		従業員(G_2)	
		実施	非実施
推進部門(G_1)	非指示	0，$-Y_d$	$-P_1Sp$，$-P_2Y_2$
	指示	M，$-Y_d-C_a$	$M-P_1Sp$，$-P_2Y_2-P_2V$
前項は推進部門のペイオフG_1，後項は従業員のペイオフG_2			

(5)　従業員のペイオフ G_2 の値

従業員のペイオフの値も，推進部門自身のとる戦略と従業員のとる戦略の組合せにより変わる．あるセキュリティ対策に関する従業員のペイオフ G_2 を，G_1 の場合と同様に，

G_2（推進部門の戦略：従業員の戦略）

で表記する．4.4 節 (1) から (4) までの議論により，従業員のペイオフ G_2 は以下のようになる．

G_2（非指示：実施）$= -Y_d$ (5)

G_2（非指示：非実施）$= -P_2Y_2$ (6)

G_2（指示：実施）$= -Y_d - C_a$ (7)

G_2（指示：非実施）$= -P_2Y_2 - P_2V$ (8)

（以上の議論で用いた変数を表にしたものを付録に示す.）

4.5　セキュリティ対策推進ゲームの利得構造

4.3，4.4 節で議論した G_1，G_2 のペイオフの値から，セキュリティ対策推進ゲームの利得表は**表 1** のようになる．

このゲームの構造は 5 章で考える．

5. ゲームに基づくセキュリティ対策の分析

5.1　ペイオフの大小関係

ゲームの構造を明らかにするため，推進部門と従業員のペイオフの大小関係を考える．

(1)　推進部門のペイオフ G_1 の大小関係

推進部門のペイオフ G_1 の大小関係を，その意味と式 (1) から式 (4) に基づいて考える．

推進部門の戦略が「指示」「非指示」のいずれの場合でも，従業員がセキュリティ対策を実施しなかった場合にはその組織に P_1S_p の損失が発生し，それは推進部門の負担となる．よって，推進部門にとっては，「指示」「非指示」のいずれの戦略に対しても従業員が戦略「実施」をとったときのほうが，ペイオフが大きい．ここで，M は 4.3 節 (1) で述べたように正の値なので，以下の大小関係が成り立つ．

G_1（指示：実施）$> G_1$（指示：非実施） (9)

G_1（非指示：実施）$> G_1$（非指示：非実施） (10)

また，推進部門は可能な限りセキュリティ対策を進めるのが任務職責であり，このとき 4.3 節 (1) で議論したように利得 M を得るので，推進部門は「指示」が支配戦略である．すなわち，以下の関係が成り立つ．

G_1（指示：実施）$> G_1$（非指示：実施） (11)

G_1（指示：非実施）$> G_1$（非指示：非実施） (12)

ここで，G_1（非指示：実施）と G_1（指示：非実施）の大小関係を考える．「4.3 節 (2) 事故が発生したときの対処コストの負担」で述べたように，$M - P_1S_p$ の値は負の値であるため，G_1（非指示：実施）は，G_1（指示：非実施）よりも大きい．よって，以下の関係が成り立つ．

G_1（非指示：実施）$> G_1$（指示：非実施） (13)

これは，セキュリティ対策を指示しなかったにもかかわらず従業員が対策を実施することが，セキュリティ対策を指示したにもかかわらず従業員が実施しないことよりも望ましいことを示しており，セキュリティ対策の実際の判断状況とも合致する．

以上，式 (9) から式 (13) をまとめて整理すると，推進部門のペイオフ G_1 は，式 (14) に示すとおりの大小関係がつねに成立する．

G_1（指示：実施）$> G_1$（非指示：実施）
$> G_1$（指示：非実施）$> G_1$（非指示：非実施） (14)

(2)　従業員のペイオフ G_2 の大小関係

従業員のペイオフ G_2 の大小関係は，式 (5)，式 (7)，および式 (6)，式 (8) より，従業員から見るとそれぞれ以下のようになる．

G_2（非指示：実施）$> G_2$（指示：実施） (15)

G_2（非指示：非実施）$> G_2$（指示：非実施） (16)

5.2　ゲームの種類と境界条件

推進部門のペイオフ G_1 の大小関係は式 (14) であるため，このゲームは従業員のペイオフ G_2 の大小関係によって変化する．

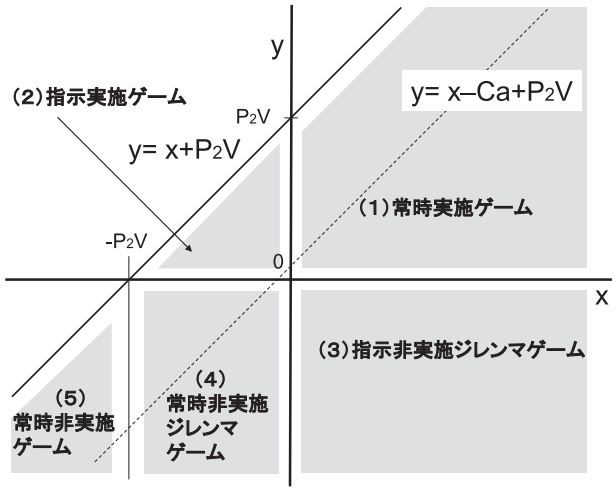

図 1　ゲームの種類と空間
Fig. 1　Five games between promotion section and employee.

ゲームの特性と境界条件を明らかにするため，推進部門の戦略が「非指示」の場合の従業員の「実施」と「非実施」のペイオフの差 G_2（非指示：実施）$-$ G_2（非指示：非実施）を x，「指示」の場合の「実施」と「非実施」のペイオフの差 G_2（指示：実施）$-$ G_2（指示：非実施）を y とおく．

$$x = G_2\text{（非指示：実施）} - G_2\text{（非指示：非実施）} = -Y_d + P_2Y_2 \tag{17}$$

$$\begin{aligned} y &= G_2\text{（指示：実施）} - G_2\text{（指示：非実施）} \\ &= -Y_d - C_a - \{-P_2Y_2 - P_2V\} = x - C_a + P_2V \end{aligned} \tag{18}$$

よって，x と y の値により以下の 5 種類のゲームの状態が存在する．x，y の空間とこれら 5 つのゲームを**図 1** に示す．

(1)　常時実施ゲーム

（$x \geqq 0$，$y \geqq 0$ のとき）

ナッシュ均衡は（指示：実施）で，このときパレート最適となる．推進部門の戦略にかかわらず，従業員は，「実施」が優位な戦略となる．図 1 の $x \geqq 0$，$y \geqq 0$ における x 軸，y 軸，$y = x + P_2V$ で囲まれた (1) の領域が，このゲームの空間である．

(2)　指示実施ゲーム

（$x < 0$，$y \geqq 0$ のとき）

ナッシュ均衡は（指示：実施）で，このときパレート最適となる．従業員の戦略は，推進部門の戦略が「指示」の場合には「実施」が，「非指示」の場合には「非実施」が，優位な戦略となる．図 1 の $x < 0$，$y \geqq 0$ における x 軸，y 軸，$y = x + P_2V$ で囲まれた (2) の領域が，このゲームの空間である．

(3)　指示非実施ジレンマゲーム

（$x \geqq 0$，$y < 0$ のとき）

ナッシュ均衡は（指示：非実施）であるが，このときパレート最適ではなく，ジレンマ状態となる．推進部門の戦略が「非指示」の場合には従業員にとって「実施」が優位であるものの，推進部門が「指示」を選択すると「非実施」が優位となるため，従業員はつねに推進部門の戦略と逆の行動をとるのが優位な戦略となる．図 1 の $x \geqq 0$，$y < 0$ となる (3) の領域が，このゲームの空間である．

(4)　常時非実施ジレンマゲーム

（$-P_2V \leqq x < 0$，$y < 0$ のとき）

ナッシュ均衡は（指示：非実施）だがこのときパレート最適ではなく，ジレンマ状態となる．これ以外の戦略はすべてパレート最適となる．推進部門の戦略にかかわらず従業員にとっては「非実施」が優位な戦略となる．図 1 の $-P_2V \leqq x < 0$，$y < 0$ となる (4) の領域が，このゲームの空間である．

(5)　常時非実施ゲーム

（$x < 0$，$x < -P_2V$，$y < 0$ のとき）

ナッシュ均衡は（指示：非実施）でこのときパレート最適となる．他のすべての戦略もパレート最適となる．このときも，推進部門の戦略にかかわらず従業員は「非実施」が優位な戦略となる．図 1 の $x < 0$ かつ $x < -P_2V$，$y < 0$ と $y = x + P_2V$ で囲まれた (5) の領域が，このゲームの空間である．

6. 考　　察

提案したモデルの各ゲームにおけるセキュリティ事象を考察し，組織内のセキュリティに関連する環境をどのように変化させればセキュリティ対策の効果が高まるかを検討する．

6.1　各ゲームのセキュリティ事象

各ゲームのセキュリティ事象について考察する．

(1) の常時実施ゲームは，$x \geqq 0$ かつ $y \geqq 0$ が成立するときに発生する．これは，推進部門がセキュリティ対策の実施を指示する場合としない場合のいずれの場合でも，従業員にとってはセキュリティ対策を実施したほうがペイオフが大きいと判断される場合である．式 (17)，式 (18) で考えると，この状態は，セキュリティ対策の実施による業務効率の低下 Y_d が小さく，事故が発生した際の損失 P_2Y_2 が大きく，セキュリティ対策実施の指示に従うのに必要な負担 C_a が小さく，従業員が考える事故が発生した場合のペナルティによる負担 P_2V が大きい場合である．実際のセキュリティ対策では，それを遂行するのに必要な従業員の手間や作業時間を減らして利便性を高めるとともに，管理部門が従業員に与えるマネジメント作業の量を減らし，それを実施しなかった場合の被害の大きさを従業員に正しく認識させるとともに罰則を設けることが推進に効果があると考えられているが，本ゲームの状態はそれとよく一致する．本ゲームは，推進部門がとくに指示しなくても従業員はセキュリティ対策を実施するので，セキュリティ対策を推進するには望ましい状態である．

(2) の指示実施ゲームは，$x < 0$，$y \geqq 0$ が成立するときに発生する．推進部門がセキュリティ対策を指示しないときには従業員は実施しないほうがペイオフが大きいが，指示したときには実施したほうがペイオフが大きくなる状態である．これは，セキュリティ対策の実施による業務効率の低下 Y_d は事故が発生した際の損失 P_2Y_2 よりも大きいものの，セキュリティ対策実施の指示に従うのに必要な負担量 C_a が小さく，事故が発生した場合のペナルティ P_2V が大きいような場合である．従業員は推進部門からの指示がなければセキュリティ対策を実行したくはないが，指示されるならば仕方なく実行するという状態がこのゲームに相当する．推進部門が「非指示」の戦略をとると従業員は「非実施」が優位な戦略となるため，セキュリティ対策を推進するには推進部門は「指示」を選択する必要がある．

(3) の指示非実施ジレンマゲームは，$x \geqq 0$，$y < 0$ が成立するときに発生する．推進部門がセキュリティ対策を指示しないときは，セキュリティ対策の実施による従業員の業務効率の低下 Y_d が小さく事故が発生した際の損失 P_2Y_2 が大きいが，セキュリティ対策の実施を指示した場合にはそれに従うのに必要な負担量 C_a が大きく，それに比べれば事故が発生した場合のペナルティ P_2V が小さい場合である．

推進部門は指示を，従業員は非実施を選択するのがナッシュ均衡の戦略であるが，それはパレート最適な戦略とならないため，ジレンマ状態が発生する．従業員が推進部門の意図と反する行動をとることになるので，セキュリティ推進の面だけでなく，組織のセキュリティマネジメントを遂行するうえでも望ましくない状態である．

実際の事例としては，企業の製品開発部門におけるファイル保存の例がある．装置やプログラムの開発部門では，技術資料や設計書など，業務の中で多くの資料が作成される．開発が終了したあとも，メンテナンスを行ったり，市場で発生した障害に対応したり，次の業務の参考としたりするため，これらの技術資料はある一定期間，手近なところに置いて保存する必要がある．このとき，セキュリティの管理策を強化するため，資料を推進部門の管理下の鍵のかかる保管庫に保管したりマイクロフィルム化したりするよう，推進部門が指示する例がある．しかしこのような施策は，必要なときに取り出すのに時間がかかるうえ，受益者負担の原則でその利用に費用がかかることが多いため，業務効率が低下したり，課金によってその業務プロジェクトの採算性が悪化したりする．このため，これらの施策は開発者にとっては推進部門により強制される負担と感じ，この負担があまりに大きいと感じた場合には，開発者は設計資料を推進部門の目のとどかない場所，たとえば自宅に持ち帰ったり自分のロッカに隠して保存したりする場合があり，資料を安全な場所で保管するというセキュリティ策が実行されなくなる．この場合，開発者にとって，資料を製品開発部門のフロア内で正しく管理することによる業務効率の低下が Y_d で，保管庫に保存したりマイクロフィルム化したりすることにより発生する対応コストが C_a である．この例の場合は，開発者にとって C_a が Y_d に比べて大きな値となり，本ゲームの状態となったと考えられる．これは，著者が調査した事例である．

他の事例として，自宅の私有 PC 内に業務データが存在しないことを確認するソフトウェアを従業員に配布して実行させるような施策を行った例がある．この事例では，実行してそれを報告するだけであれば必要な負担量はさほど大きくないため指示に従ったものが，実行を指示するだけでなく出力結果のファイル一覧をその内容の説明をつけて提出させるような施策をとったため，私有 PC の内容を職場に提出するという心理的に大きな負担や作業の手間が発生した．その結果，指示非実施ジレンマゲームの状態となって，自宅に私有 PC は存在しないなどと従業員が嘘の報告をして確認ソフトウェアの実行自体を行わず，結果，セキュリティ対策がとられないことになった．この事例の場合，確認ソフトウェアを実行する手間が Y_d で，その結果を詳細に報告する手間が C_a である．単に確認ソフトウェアの実行を報告するだけであれば C_a は小さいが，ファイルの一覧を出力したうえその内容の説明を記述するような施策にすると，C_a は大きくなる．従業員に対して大きな対応コスト C_a を強いたために本ゲームの状態になったと考えられる．これも，著者が調査した事例である．

他の公表された事例としては，学校の教員用 PC で起こったセキュリティ事故の例がある［a］．この学校の教員用 PC は，セキュリティ推進部門であるシステムの管理者によって，パスワードを利用するよう設定されており，かつその際には週 1 回のパスワードの変更

が必要となるよう設定されていた．しかし，利用者である教員はそれを覚えきれないため，パスワードを記した紙を机の引き出しに保存し，それが学生に知られて PC 内の情報が漏えいし理解度試験の再実施が必要となった．教員は，過去に，覚えていたパスワードを忘れシステム管理者に依頼して取り消し・再発行の手続きを行ったことがあり，そのときの経験からパスワードを紙に書いて記録していた．

本事例の場合，教員は当初，パスワードを記憶して毎回それを入力することによる業務効率の低下を許容して PC を使っていた．しかし，システム管理者が週 1 回のパスワードの変更のような大きな負担となる指示を出したため，パスワードを記憶せず紙に書いて PC を使うようになった．通常，パスワードの設定はセキュリティ対策としてよく知られているが，それを 1 週間ごとに変えるというのは一般のシステムにおいてはきわめて異例な運用である．このため，教員は，パスワードを設定することによる負担はセキュリティ対策の実施にともなう業務効率の低下 Y_d と認識したものの，それを毎週変更することによる負担は推進部門の指示に従うのに必要な対応コスト C_a であると認識し，その結果，指示非実施ジレンマゲームが発生したと考えられる．

これらの事例によれば，セキュリティ対策の変更により，本モデルにおける従業員の対応コスト C_a の値やペナルティ P_2V の値は，変化させることができると考えられる．そこで，**図 2** に示した各ゲームの状態に関し，たとえば，あるセキュリティ対策で生じている指示非実施ジレンマ状態を，従業員の対応コスト C_a の値やペナルティ P_2V の値の異なるセキュリティ対策に変更することによって，指示実施ゲームの状態ないし常時実施ゲームの状態に移行させることができると考えられる．従業員の対応コスト C_a の値やペナルティ P_2V の値の推定は，容易ではないと考えられるが，代理変数を見出すなどの方法を用いることによって，途をひらくことができるものと考える．

(4) の常時非実施ジレンマゲームと (5) の常時非実施ゲームは，$x < 0$，$y < 0$ が成立するときに発生する．推進部門がセキュリティ対策の実施を指示する場合としない場合のいずれの場合でも，従業員にとってはセキュリティ対策を実施しないほうがペイオフが大きいと判断される場合である．$-P_2V \leqq x < 0$ のときは推進部門は指示を，従業員は非実施を選択するのがナッシュ均衡の戦略であるが，それはパレート最適な戦略とならないため，ジレンマ状態が発生する．$x < -P_2V$ のときは推進部門は指示を，従業員は非実施を選択するのがナッシュ均衡の戦略で，これはパレート最適な戦略ともなり，ジレンマ状態は発生しない．しかし，いずれのゲームも従業員はセキュリティ対策をとらないので，セキュリティ対策を推進するには望ましくない状態である．

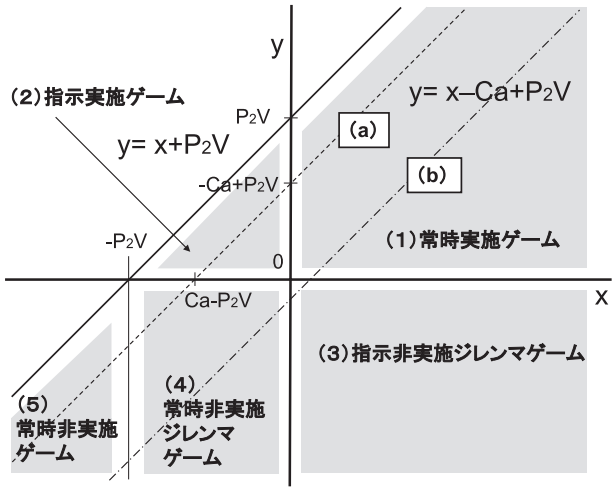

図 2　P_2V と C_a の値によりとりうるゲーム
Fig. 2　Games that can be taken by the value of P_2V and C_a.

6.2　セキュリティ対策を推進するうえで望ましいゲームの状態と x，y の値

x，y は式 (18) で表される線分上を図 1 の破線の右上の方向に進んで行く．6.1 節で論じたように，セキュリティ対策を推進するうえでは (1) の常時実施ゲームの状態となるのが最も望ましく，次いで (2) の指示実施ゲームの状態が望ましい．よって，セキュリティ対策を進めるには，状態 $x = X$，$y = Y$ を，この式 (18) の線分上をそれぞれ増大する方向に進めていくことが必要である．X を増やすには，式 (17) より，$Y_d + P_2Y_2$ の値を増加させればよい．すなわち，第 1 項のセキュリティ対策を実施したときの業務効率の低下 Y_d の値を下げるとセキュリティ対策が進む方向に状態が変化し，第 2 項の従業員が感ずる事故の発生確率 P_2 とそのときの損失 Y_2 との積が増加すると，同じくセキュリティ対策が進む方向に状態が変化することが分かる．従来，セキュリティ対策による業務効率の低下を最小限にとどめることやセキュリティ事故に対する従業員の危機感，恐怖感を高めることがセキュリティ対策の推進に効果があると経験的にはいわれていたが，本モデルによる分析では，このように，これらは理論的に説明できる．

6.3　各ゲームの状態となる条件

従業員の対応コスト C_a とペナルティ V の値を変えることによりゲームの種類が変わる．

どのような状況でこれらのゲームの状態となるのかを調べる．x，y は式 (18) の値をとるが，P_2V と C_a の値によって，図 2 のようにとりうるゲームが変わる．

図 2 中の破線 (a) のように，$P_2V > C_a$ のとき (1) 常時実施ゲーム，(2) 指示実施ゲーム，(4) 常時非実施ジレンマゲーム，(5) 常時非実施ゲームの 4 つのゲームをとるが，(3) の指示非実施ジレンマゲームはとらない．$P_2V = C_a$ で (1) 常時実施ゲーム，(4) 常時非実施ジレンマゲーム，(5) 常時非実施ゲームの 3 つのゲームをとり，$P_2V < C_a$ で図中の一点鎖線 (b) のように，(1) 常時実施ゲーム，(3) 指示非実施ジレンマゲーム，(4) 常時非実施ジレンマゲーム，(5) 常時非実施ゲームの 4 つのゲームをとる．6.1 節で論じたように，セキュリティ対策を推進するうえでは (3) の指示非実施ジレンマゲームは組織のマネジメント上望ましくないので，$P_2V \geqq C_a$ とするのが望ましい．すなわち，セキュリティ対策の推進には，従業員の対応コスト C_a による負担を小さくする施策をとると効果があることが分かる．

従業員の負担を減らすことがセキュリティ対策を推進するうえで重要であることは，従来から経験的に知られている．しかし，本研究によって，従業員の負担には，セキュリティ対策の実施による業務効率の低下 Y_d とセキュリティ対策を指示されることによる従業員の対応コスト C_a の 2 つがあり，これらはセキュリティ対策の推進において異なった効果を及ぼすことが明らかになった．

Y_d を減らすセキュリティ対策は，6.2 節で述べた状態 $x = X$，$y = Y$ を式 (18) の線分上で正の方向に動かす．このため，たとえば現在の状態が (4) 常時非実施ジレンマゲームだったとき，Y_d を減らすセキュリティ対策を行った場合，$P_2V < C_a$ であるときには，セキュリティ対策を推進していくと (3) 指示非実施ジレンマゲームに突入してしまい，これは施策として好ましくない．一方，C_a を小さくするセキュリティ対策を行った場合には，図 2 の一点鎖線 (b) を破線 (a) のように，とりうるゲームの空間を y 軸に沿って平行に正の方向に動かすことになるので，(2) 指示実施ゲームに突入し，この場合はセキュリティ対策として好ましい．

このように，本研究のモデルに基づいて，あるセキュリティ対策について，従業員の対応コスト C_a の値やペナルティ P_2V の値を推定することによって，その対策がもたらすゲームの状態を把握することや，これらの変数の値を変化させる代替的なセキュリティ対策について，ゲームの状態の移行を検討することなどが考えられる．本モデルは，組織にとって適切なセキュリティ対策を検討する場合に，その基礎的なモデルとして活用することができるものと考える．

6.4　ペナルティ V の効果の減少

4.4 節 (4) で議論したように，推進部門が設定したペナルティ V は，従業員にとっては自らが認識している事故発生の確率 P_2 を乗じた値として感じられる．これは，従業員が，事故の発生確率 P_2 を推進部門が考える P_1 よりも小さく認識した場合，事故の発生によってあたえられるペナルティによる損失を，推進部門が考えるよりも低く見積もることを示している．

人が発生確率を低く認識するメカニズムを明らかにしたものとして，Kahneman らの「プロスペクト理論」がある[16]．この中で，人は損失フレームにおいてリスク選好の意思決定をする傾向があることが示されている．これをセキュリティ対策における従業員の認識にあてはめて考えると，セキュリティ対策を行うことが自らの業務の遂行における損失であると認識した場合には損失フレームの状態となり，従業員が事故の発生確率を小さく認識する可能性があると考えられる．1 章で紹介した持ち出し禁止データの持ち出しによる紛失・盗難被害の事件や P2P ファイル共有ソフトを使っている中での暴露ウイルスへの感染による情報漏えいの事例でも，事件・事故となる可能性を本人が正しく認識していたとは考えにくい．発生する可能性がゼロではないとの認識はあったであろうが，それが自分に発生するとは思っていなかった，すなわち，その危険性に関しては，発生する確率は非常に小さな値であると認識していた可能性が考えられる．

このように，本モデルの分析によると，ペナルティ V は従業員の認識によって値が減少するため，その効力が小さなものとなる可能性があることが分かる．これは，従来行われていたような，罰則の強化により組織のセキュリティ対策を進める施策は，実は効果を発揮しない場合があることを示している．

6.5　インセンティブを導入した場合の効果の減少

従業員が指示に従った場合に，従業員に対して報酬のようなインセンティブを与える方策も行われている．しかし，多くの場合，指示内容の実施を正しく確認するのは手間がかかるため，本当に実施したのかどうか，また，確認できたとしてその後も継続的に実施しているかどうかまでは正しく分からない場合がある．たとえば，自宅での P2P ファイル共有ソフト利用の自粛のような指示は，組織がその指示が守られているかどうかを継続して確認するのは難しい．USB メモリの業務利用禁止のような施策も，物理的に USB ポートを塞いだり接続を禁止するソフトウェアを導入したりしない限り，継続的にその施策が実行されていることを確認するのは困難である．

このような場合，インセンティブを R とすると，従業員にとって「実施」の戦略のペイ

オフに R が，「非実施」のペイオフに $(1-P_2)R$ が見込まれるので，

$$y = -Y_d - C_a + R - \{-P_2Y_2 - P_2V + (1-P_2)R\} = x - C_a + P_2V + P_2R \quad (19)$$

となり，従業員は，インセンティブを，ペナルティ V と同じく P_2 のかかった値 P_2R と認識することになる．よって，従業員の感じる発生確率 P_2 が推進部門が考える発生確率 P_1 より小さい場合には，ペナルティ V と同様，従業員がセキュリティの指示に従うことを促進するインセンティブの効果は弱まる．この現象は，経験的にはあまり知られていないと思われるが，本モデルによる分析で理論的に説明される．

6.6　本モデルの有効性と今後の可能性

本セキュリティ対策推進ゲームのモデル化では，3 章のセキュリティ対策の分析において，主要と思われる要素を盛り込んでその構造を決定した．これにより，セキュリティ推進上の種々の事象が整理され，対策や効果をゲームの空間上に位置づけることができた．さらに，どのような変数に着目してそれをどのように施策として変化させればゲームの種類が変化してセキュリティ推進が進むかを論理的に分析することができ，本モデルの有効性が確認された．

また，推進部門が行うセキュリティ推進の施策とそれが従業員に与える影響，およびセキュリティ対策推進上のさまざまな事象は，いずれも推進部門にとってのペイオフと従業員にとってのペイオフとに分解して考えることができる．よって，本論文には盛り込まなかった細かな影響や事象なども，それぞれのペイオフに分解して基本となる本モデルに追加していけば，今後さらにモデルを精緻化して表現し分析することが可能となる．

7. 結　　論

本論文では，実際の組織で行っているセキュリティ対策の状態を分析し，IT セキュリティ対策の推進部門と組織内の従業員とをプレーヤとするモデルを作成し，セキュリティ対策推進ゲームを提案した．ゲーム理論によりゲームの構造を分析し，従業員のペイオフにより 5 種類のゲームが存在するという知見を得た．各ゲームの特性を分析し，どのような方策をとればセキュリティ対策を推進することができるかを明らかにした．分析により，従来経験的にいわれてきた，セキュリティ対策を実施することによる業務効率の低下量の低減と，推進部門の指示を受けることによるコストの低減の 2 つがセキュリティ対策の推進に有効であることを理論的に示すとともに，推進部門が従業員に与えるペナルティやインセンティブは従業員が事故の発生確率を実際よりも小さく認識した場合には効果が少なくなることがあるという，従来の経験上ではあまり知られていなかった現象を明らかにした．さらに，本モデル化による分析の有効性と今後の可能性を確認した．

8. 今後の課題

一般にセキュリティ事象は詳細が明らかにされることは少なく，議論に用いた各種の変数を定量的に計測した研究例はほとんどない．今後，事例の調査や社会科学的な実験を行うことによって要因と特性を実測して定量的に表すとともに，各要因の状態がどのようなものであればセキュリティ対策が推進されるのか，どのような値であれば組織のセキュリティ対策推進の状態を評価する指標となりうるのかを検討することが課題である．

また，本論文ではセキュリティ対策を指示し推進する立場である推進部門とセキュリティ対策を実行する従業員との 2 プレーヤを考えたが，実際の組織では，推進部門が階層構造となっていたり，個々の従業員によって判断が異なったりグループを形成したりして三者以上が相互に影響を及ぼしあう形態もある．n 人ゲームへの拡張や，複数のプレーヤからなる構造の分析，モデルのさらなる精緻化は今後の課題である．

謝辞　本論文の作成と改良に際し，多数の有益なコメントを下さった査読者ならびに関係各位に謹んで感謝の意を表します．

参　考　文　献

1) NPO 日本ネットワークセキュリティ協会：2008 年情報セキュリティインシデントに関する調査報告書，Ver.1.2, p.3 (2009).
2) 経済産業省：情報セキュリティ総合戦略，pp.38–41 (2003).
3) 宮崎邦彦，岩村　充，松本　勉ほか：交渉ゲームにおける鍵自己暴露戦略のインパクト—電子署名技術の利用に係る新たな課題，情報処理学会論文誌，Vol.46，No.8，pp.1871–1879 (2005).
4) 兵藤敏之，中村逸一，西垣正勝ほか：セキュリティ対策案選択問題のモデル化，情報処理学会研究報告，2003-CSEC-22 (35), pp.249–256 (2003).
5) Gordon, L.A. and Loeb, M.P.: The Economics of Information Security Investment, *ACM Trans. on Information and System Security*, Vol.5, No.4, pp.438–457 (2002).
6) 松浦幹太：情報セキュリティと経済学，*SCIS2003*, pp.475–480 (2003).
7) 弓削哲史，柳　繁：情報流出事故の定量的解析，信学技報 IEICE Technical Report, R2007-16, pp.13–18 (2007).
8) 日本規格協会：JIS Q 27002:2006（ISO/IEC27002:2005），情報技術—セキュリティ技術—情報セキュリティマネジメントの実践のための規範，日本規格協会 (2006).
9) 総務省：地方公共団体における情報セキュリティポリシーに関するガイドライン（平成 18 年 9 月版）(2006).

10) 総務省：地方公共団体における情報セキュリティ監査に関するガイドライン（2007 年 7 月 6 日全部改定）(2007).
11) 日本規格協会：JIS Q 13335-1 情報技術—セキュリティ技術—情報通信技術セキュリティマネジメント—第一部：情報通信技術セキュリティマネジメントの概念及びモデル，日本規格協会 (2006).
12) 高度情報通信社会推進本部 情報セキュリティ対策推進会議：情報セキュリティポリシーに関するガイドライン，pp.13–17 (2000).
13) Umehara, E. and Ohta, T.: Using Game Theory to Investigate Risk Information Disclosure by Government Agencies and Satisfying the Public; The Role of the Guardian Agent, *IEEE Trans. on SMC; Part A*, Vol.39, No.2, pp.321–330 (2009).
14)（株）富士通総研経済研究所：日本における内部統制の現状に関するアンケート調査 (2007).
15) NPO 情報セキュリティフォーラム：教育現場における情報セキュリティ事故・対応事例の研究事例集，p.13 (2007).
16) Kahneman, D. and Tversky, A.: Prospect Theory: An Analysis of Decision Under Risk, *Econometrica*, Vol.47, pp.263–291 (1979).

付　　録

変数一覧

推進部門のパラメータ			
記号	値の意味	記号	値の意味
G_1	推進部門のペイオフ	S_p	事故が発生した場合の事後対策にかかる費用
P_1	推進部門が認識する事故の発生確率	M	セキュリティ対策を指示することの利得(金額換算)

従業員のパラメータ	
記号	値の意味
G_2	従業員のペイオフ
P_2	従業員が認識する事故の発生確率
Y_d	セキュリティ対策実施による業務効率の低下量（金額換算）
Y_2	事故が発生したときの損失量（金額換算）
C_a	セキュリティ対策を指示された時にそれに従う従業員の対応コスト（金額換算）
V	従業員が受けるペナルティの量（金額換算）
R	従業員が受けるインセンティブの量（金額換算）

ゲームの値		
記号	意味	値
x	G_2（非指示：実施）$-G_2$（非指示：非実施）	$-Y_d+P_2Y_2$
y	G_2（指示：実施）$-G_2$（指示：非実施）	$x-C_a+P_2V$

(平成 22 年 5 月 26 日受付)
(平成 23 年 3 月 7 日採録)

杉浦　　昌（学生会員）

1983 年電気通信大学大学院電子工学専攻修士課程修了．同年日本電気（株）入社．画像圧縮・画像処理装置，ネットワークシステムの研究開発等を経て，IT セキュリティおよびセキュリティマネジメントのコンサルティングビジネスの推進，ならびに，公的団体・業界団体の委員会活動および規格標準化活動に従事．（独）情報処理推進機構非常勤研究員．電気通信大学大学院情報システム学研究科社会知能情報学専攻．

諏訪　博彦（正会員）

1998 年群馬大学社会情報学部卒業．2006 年電気通信大学大学院情報システム学研究科博士後期課程修了．博士（学術）．現在，電気通信大学大学院情報システム学研究科社会知能情報学専攻社会情報システム学講座助教．ソーシャルメディアに関する研究に従事．

太田　敏澄（正会員）

1970 年東京工業大学経営工学科卒業，1972 年同大学院理工学研究科修士課程修了．1977 年工学博士．現在，電気通信大学大学院情報システム学研究科教授．社会情報システム学，組織知能工学の研究に従事．『社会の中の企業（共著）』，『都市と環境の公共政策（共著）』，『環境としての情報空間（共著）』，『社会情報システム学・序説（共著）』，『Creative and Innovative Approaches to the Science of Management（共著）』，日本社会情報学会（JASI），日本ソフトウェア科学会，経営情報学会，日本 OR 学会，IEEE 等．