Vol.2010-CSEC-49 No.1
2010/5/11

組織の IT セキュリティ推進のゲーム理論による分析 ー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ー

杉浦昌[†]　諏訪博彦[††]　太田敏澄[††]

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．分析により，以下の知見を得た．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．

IT-security Implementation Game in Organizations - A Game between Promotion Section and Employee -

MASASHI SUGIURA[†]　HIROHIKO SUWA[††]
TOSHIZUMI OHTA[††]

We develop a model of IT security implementation game in organizations based on game theory. Two players are the members of game; i.e. an IT security section that promotes implementation of IT security in an organization, and the employee who implements IT security in his/her business in the organization. We formulate the costs and benefits of implementation for their strategies in the game. Results in our analysis find the five types of game, which are a regular implementation game, a promotion-implementation game, a promotion-non-implementation dilemma game, a regular non-implementation dilemma game, and a regular non-implementation game.

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．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[1]．このため，セキュリティポリシーの制定や組織内教育の充実，セキュリティ監査の実施等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．例えば，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る P2P ファイル共有ソフト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．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．

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．セキュリティ対策の指示に対する従業員のふるまいのメカニズムをあきらかにした上で対応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．

本論文の構成は以下の通りである．2 節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 節で実際の組織で実施されているセキュリティ対策について整理し，4 節でその状況をセキュリティ対策推進ゲームとしてモデル化する．5 節でモデル化したゲーム構造を分析し，6 節でゲームの特性を考察する．最後に 7 節で結論を述べる．

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，宮崎らの研究[2]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得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

[†] 電気通信大学，情報処理推進機構（IPA）
University of Electro-Communications,　Information-Technology Promotion Agency ,JAPAN
[††]電気通信大学
University of Electro-Communications

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の研究[3]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み合わ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 らの研究[4]や松浦の研究[5]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の研究[6]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．

3. 組織のセキュリティ対策

実際の組織で行なわれているセキュリティ対策について述べる．

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．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もつ．

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ものであれば，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．ここでは，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

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は個別に利用部門に要求する場合は少なく，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た上でセキュリティ推進部門がそれを用いて活動する場合が多い．セキュリティ推進部門は用意された予算のなかからそれを適切に活用して組織のセキュリティ対策を行う．

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 [7])は，企業や組織が選択し得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，全ての対策を一律，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．

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上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[8]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ーガイドライン[9]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 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等を加味し，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ため，本論文では，対象とするセキュリティ対策のリスクアセスメント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 節で述べ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あらわす．ゲームは，あるひとつのセキュリティ対策の推進について考える．本論文では繰り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 & Ohta[10]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．

4.1 プレーヤ

本論文では，3.1 で述べたように，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その組織内へ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 で述べたように，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，ある一つのセキュリティ対策について推進部門が取り得る戦略は，その対策の実施についての「指示」と「非指示」の二つとなる．

一方，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

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．この M の値は報酬や賞罰のような数値であらわされるものばかりでなく心理的なものや数値化しにくいものもあるが，それら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

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，$M-P_1S_p$ のコストを負担する．

(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取る戦略の組み合わせにより変わる．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，前記「（１）推進部門の任務職責」，「（２）事故が発生したときの対処コストの負担」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み合わ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．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[11]．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，その時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例がある．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等の作業が普通であ

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等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出来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，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常に正確に把握する事は容易ではない．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わからず，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．

(5) 従業員のペイオフ G2 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取る戦略の組み合わせにより変わる．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．上記「（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」から「（４）推進部門が従業員に与えるペナルティ」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)

4.5 セキュリティ対策推進ゲームの利得構造

4.3，4.4 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．

次節で，このゲームの構造を考える．

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. 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．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.(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．さらに，セキュリティ対策を実施することはセキュリティレベルの向上につながるため，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した場合のペイオフは，セキュリティ対策を指示したにもかかわらず実施しなかった場合のペイオフよりも大きい．以上をまとめて整理すると，推進部門のペイオフ G_1 は次の大小関係となる．

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）…(9)

(2) 従業員のペイオフ G2 の大小関係

従業員のペイオフ G_2 の大小関係は，(5)式，(7)式，及び(6)式，(8)式より，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） …(10)

G_2（非指示：非実施）>G_2（指示：非実施）…(11)

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(9)式であるため，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．

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」のペイオフと「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」のペイオフと「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（非指示：実施）－G_2（非指示：非実施）　＝－Y_d＋P_2Y_2　…(12)

y＝G_2（指示：実施）－G_2（指示：非実施）

　＝－Y_d－C_a－｛－P_2Y_2－P_2V｝　＝x－C_a＋P_2V　…(13)

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≧0，y≧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≧0，y≧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≧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≧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≧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，従業員は常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≧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≦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≦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．

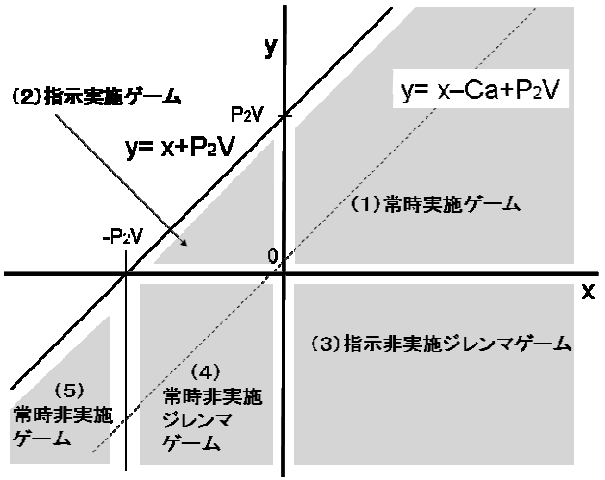

図 1　ゲームの種類と空間

Figure 1　Five games between promotion section and employee.

6.　考察

各ゲームにおけるセキュリティ事象を考察する．

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≧0 かつ y≧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．(12)式，(13)式で考えると，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．本ゲームでは，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それを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況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上でも望ましくない状態である．

実際の事例としては，「4.4. 従業員のペイオフ G_2」の「（３）推進部門の指示に従う際の従業員コスト」で述べたような，大きな管理コスト C_a がかかる場合にこのゲームになる．

（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．

6.2 セキュリティ対策を推進する上で望ましいゲームの状態と x，y の値

状態が $x=X$, $y=Y$ の値のとき，X，Y は(13)式 $y = x - C_a + P_2V$ の関係をとる．よって，X の値を増加させていけば Y の値も増加していく．X，Y は (13)式であらわされる線分上を図 1 の破線の右上の方向に進んで行く．6.1 で論じたように，セキュリティ対策を推進する上では（１）の常時実施ゲームの状態となるのがもっとも望ましく，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(13)式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，(12)式より，$Y_d + P_2Y_2$ の値を増加させればよい．第一項の，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進むのは，経験的な結論と一致する．第二項の，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進むのも，経験的な結論と一致する．

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況を分析し，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セキュリティ対策推進ゲームを提案した．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ことを示した．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出来るかを明らかにした．

1 経済産業省：情報セキュリティ総合戦略，pp38-41（2003）．
2 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，pp1871-1879（2005）．
3 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），pp249-256（2003）．
4 Gordon, L.A. and Loeb, M.P.: The Economics of Information Security Investment, *ACM Trans.* On Information and System Security, Vol.5, No.4, pp438-457(2002).
5 松浦幹太：情報セキュリティと経済学，SCIS2003，pp475-480（2003）．
6 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, pp13-18（2007）．
7 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）．
8 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）．
9 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，pp13-17（2000）．
10 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 TRANSACTIONS on SMC*; PART A, Vol.39, No.2, pp.321-330 (2009).
11（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）．