情報処理学会論文誌 Vol.53 No.9 2160–2170 (Sep. 2012)

教員用PCで発生したセキュリティ事例の分析 ―組織のITセキュリティ対策推進モデルを用いた分析

杉浦 昌[1,a)] 諏訪 博彦[2] 太田 敏澄[2]

受付日 2011年11月30日, 採録日 2012年6月1日

概要：組織のセキュリティ対策の推進と実施を定量的に表したモデルが提案されている．このモデルは，ゲーム理論を用いて組織がどのような状態のとき従業員がセキュリティ対策を実施し，どのような状態のとき実施しないかを明らかにしている．本論文では，実際に発生したセキュリティインシデントの事例を用いてこのモデルを検証した．事例は，実際に学校の教員用 PC で発生したものを用いた．公開されている統計データや調査データを用いて事例のモデルにおけるパラメータを定量的に算出した．事例がモデル上のどの状態にあるのかを明らかにし，事例においてジレンマ状態が発生していることを確認した．これにより，モデルがこの事例を適切に表現していることを示した．さらに，モデル上のどのようなパラメータの変化がセキュリティ上で効果があるかを求め，セキュリティ対策の改善を定量的に検討した．組織をセキュリティ上望ましい状態とする方策の条件を見出し，本モデルが組織のセキュリティ対策の実施を適切に表現することができる可能性を示した．結論として，検証したモデルの実用の可能性が示された．

キーワード：セキュリティ，組織，インシデント，モデル，ゲーム理論

Analysis of an Actual IT-security Incident Occurred with a PC Used by Teachers: Using IT-security Implementation Model in an Organization

Masashi Sugiura[1,a)] Hirohiko Suwa[2] Toshizumi Ohta[2]

Received: November 30, 2011, Accepted: June 1, 2012

Abstract: A quantitative model based on the game theory of IT-security promotion and implementation in organizations has been proposed. This model clarifies what state an organization is in and then determines which security measures an employee should or should not perform. In this study, we examined this model using an actual IT-security incident that occurred with a PC used by teachers at a school. Using public statistics and survey data, we calculated the parameters of the example in the model quantitatively and were able to clarify in what kind of state the example was and identify the state of the example within the dilemma state. By these, we showed that the model expressed this example appropriately. Furthermore, we determined what changes to the parameters were effective and examined the subsequent improved IT-security measures quantitatively. We pinpointed the optimal conditions for IT-security measures within an organization and showed the possibility that this model can express the IT-security implementation of an organization appropriately. The results showed that this model has the potential for practical use.

Keywords: security, organization, incident, model, game theory

1. はじめに

組織におけるセキュリティ対策の推進と実施を，ゲーム理論を用いて定量的に表したモデルが提案されている．このモデルは，組織がモデル上のどのような状態のときに従

[1] 日本電気株式会社
NEC Corporation, Minato, Tokyo 108–8001, Japan
[2] 電気通信大学
University of Electro-Communications, Chofu, Tokyo 182–8585, Japan
[a)] m-sugiura@fine.biglobe.ne.jp

業員がセキュリティ対策を実施し，どのような状態のときにそれを実施しないかを明らかにしている．そこで本論文では，公開されている種々の情報をもとに，実際に発生したセキュリティインシデントの事例を用いてこのモデルを定量的に検証した．

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推進に関する先行研究を述べる．3 章で組織の IT セキュリティ対策推進モデルについて述べ，4 章で実際のセキュリティ事例の分析を行う．5 章で考察を行い，モデルの妥当性を吟味し，本分析に基づいたセキュリティの改善策を検討する．6 章で結論を述べ，最後に 7 章で今後の課題を述べる．

2. 先行研究

組織におけるセキュリティ対策の推進と実施に関し，事象を定量的に調査・検討した先行研究について述べる．

(1) 学校や教育機関で発生したセキュリティ事件・事故の発生状況の調査

学校，教育機関，関連組織で発生したセキュリティ事件・事故の発生状況を調査した報告がある [1]．この調査は，実際に発生した児童・生徒・教員などの個人情報を含む情報の漏えい事故を調査したものとして貴重である．しかし，本調査は，学校や自治体が発表・公開した情報を集計したものであるため，各事例において発生した被害額は分からない．また，どれだけの母集団に対してどれだけ発生したかの検討もできないため，事故の発生確率も不明である．

(2) 一般利用者が感じるインターネット利用の危険性に関する調査

一般のインターネット利用者に対し，その利用の習熟度とインターネット利用の危険性に対する認識との関連について調査した報告がある [2]．利用者の習熟の程度と危険性の認識についての関係を調べたものとして価値がある．しかし，インターネットの利用に関する不安を数値で示すよう求める問いであるため，その数値の意味が明確ではなく，定量的な考察に用いることはできない．

(3) セキュリティ・アセスメントにおける被害額の検討

企業や組織でセキュリティ対策を行うには多大な費用がかかるため，すべての対策を同時に行うことはできず，対策に優先順位をつけて可能なものから実行していくのが普通である．このため，守るべき情報資産を明らかにしたうえでそれらの情報資産に対するリスクの大きさを見積もる，いわゆるセキュリティ・アセスメントの重要性が認識されつつある．しかしそれを実行する手法はまだ確立されておらず，さまざまな研究と提案がなされている段階である．

たとえば実効的なセキュリティ・アセスメントの実施を検討した研究として，不正アクセスによる被害を正確かつリアルタイムに求めることを目的として，システムや組織が所有するソフトウェア，ハードウェア，人員，業務といったリソースの情報を，その依存関係とともに記述するリソース依存モデルとそれによる被害予測の手法を提案した研究がある [3]．

さらに，この方法に基づいて実際の個人情報漏えいの事件・事故について損害額を算出した研究がある [4]．この研究では，漏えいした個人情報の損害賠償額に加え，情報漏えいにより課される法的な罰則や信用失墜などを含めて定量化するため，情報の価値を

漏えい個人情報価値
= 基礎情報価値 × 機微情報度 × 本人特定度

としている．各値は，アセスメントを行う際の評価者の主観的な判断が，係数の重み付けの形で含まれている．この研究ではこれを JO モデルと名付けている．

これらの研究は，組織を守るべきセキュリティ推進者が自組織内の数多くの情報資産のそれぞれの価値を算出しそれを比較し評価する方法としては有効と考えられる．しかし，セキュリティ推進者はセキュリティ技術や情報資産の価値，セキュリティリスクの大きさについてある程度の正しい知識や経験，判断力を持っているのに対し，一般の従業員に対してはそれは期待できない．実際，多くの事件・事故においては，従業員がセキュリティ推進者の想定と異なる判断をして行動したことによる場合が多く，セキュリティ推進者の判断する各種の値と従業員の判断する値とは大きく異なる可能性がある．このため，従業員がセキュリティ対策を実施しない事象を取り扱うものとはなっていない．

(4) 情報セキュリティインシデントに関する調査報告

個人情報の漏えい事件・事故について継続的に調査を行っている報告がある [5]．この調査は，1 年間の間に新聞やインターネットニュースで報道された記事や，組織が公表した文書などをもとに，(3) で紹介した JO モデルに基づいて漏えい 1 件あたりの想定損害賠償額を求めたものである．具体的な金額が判明している，宇治市における個人情報漏えいの裁判や Yahoo における情報漏えいの謝罪費用など，過去の個人情報漏えい事件の賠償金額や謝罪金額をもとにしている．セキュリティ事件・事故の具体的な被害額を見積もった調査報告として貴重であり，毎年継続的に調査報告が行われている点も価値がある．

しかし，その算定方式は (3) で述べた JO モデルに基づいているため，セキュリティ推進者の判断によって見積もられており従業員の認識とは異なる．また，個人情報の漏えいという，裁判にまで至った深刻なセキュリティ事件・事故の事例における被害額であるという限定された条件での検討である．さらに，事件・事故に関係した従業員がその発生確率をどのように認識したかの調査はされていない．

(5) 海外の関連研究

海外におけるセキュリティ事象の定量的，数値的な研究の

表 1 パラメータの一覧
Table 1 The parameters.

推進部門のパラメータ	
記号	値の意味
G_1	推進部門のペイオフ
P_1	推進部門が認識する事故の発生確率
Sp	事故が発生した場合の事後対策にかかる費用
M	セキュリティ対策を指示することの利得
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
Y_2	事故が発生したときの損失量
Ca	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
V	従業員が受けるペナルティの量

発表の場として，2002 年から開催されている WEIS（Workshop on the Economics of Information Security）[20] がある．表題の「セキュリティエコノミクス」が示すように，経済学的，社会科学的，ビジネス的な視点の研究などが発表されている．たとえば，偽のアンチウイルスソフトの金銭の流れと動作を分析した研究 [21]，セキュリティ対策を判断するにあたり，情報の価値をどのように見積もるかを数学的に分析した研究 [22] などがある．WEIS では高度なモデル化や定量化，精緻な解析がなされているが，事例を用いて組織内におけるセキュリティ対策の推進と実施の基本的な構造を分析しようとするものはない．また，本モデルによる分析に用いることができるような定量的なデータを求めたものもない．

3. 組織の IT セキュリティ対策推進モデル

特定の条件下でお互いに影響を与えあう複数の主体の間で生じる相互関係を研究する手法として広く用いられているものにゲーム理論がある [6], [7], [8], [9]．ゲーム理論では，複数の主体である「プレーヤ」が，自分が得られるペイオフ（利得）が最大となる行動となる「戦略」を選択する．このとき，別のプレーヤの選択する戦略によって自分のペイオフの大きさが変わる場合には，その相互作用によって各プレーヤの選択する戦略が変わってくる．各プレーヤのペイオフの大小関係により，パレート最適やナッシュ均衡などの特徴的な状態が発生し，それを分析することにより，各プレーヤ間の状態が安定的なものか不安定なものかが分かる．このゲーム理論を組織内のセキュリティ対策に適用したモデルが提案されている [10]．本論文では，この提案の「組織のセキュリティ対策推進モデル」を用いる．

モデルの内容を簡単に説明する．このモデルは，組織内でセキュリティ対策を指示し推進する立場の「推進部門」とセキュリティ対策を実行する立場の「従業員」の 2 者からなる．推進部門はセキュリティ対策の「指示」と「非指示」のいずれかの戦略をとり，従業員は，セキュリティ対策について「実施」と「非実施」のいずれかの戦略をとる．このとき，x を推進部門が「非指示」のときの従業員の「実施」戦略のペイオフと「非実施」戦略のペイオフの差，y を推進部門が「指示」のときの従業員の「実施」戦略のペイオフと「非実施」戦略のペイオフの差とすると，組織の状態は

$$x = -Y_d + P_2 Y_2 \tag{1}$$

$$y = -Y_d - C_a + P_2(Y_2 + V) \tag{2}$$

さらに

$$y = x - C_a + P_2 V \tag{3}$$

と表される．

ここで Y_d，P_2，C_a などのパラメータの意味は**表 1** に示した内容である．

組織の状態は，各パラメータの値によって，(1) 常時実施ゲーム，(2) 指示実施ゲーム，(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いずれかのゲームをとる．各ゲームの状態を**図 1** に示す．

5 つのゲームの状態は以下の性質を持つ．

(1) 常時実施ゲーム（$x \geqq 0$，$y \geqq 0$ のとき）

推進部門と従業員の戦略の組合せを考えると，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．推進部門の戦略にかかわらず，従業員はつねにセキュリティ対策を実施するので，セキュリティマネジメント上最も望ましい状態である．

(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．推進部門がセキュリティ対策を指示すれば従業員は実施するので，セキュリティマネジメント上

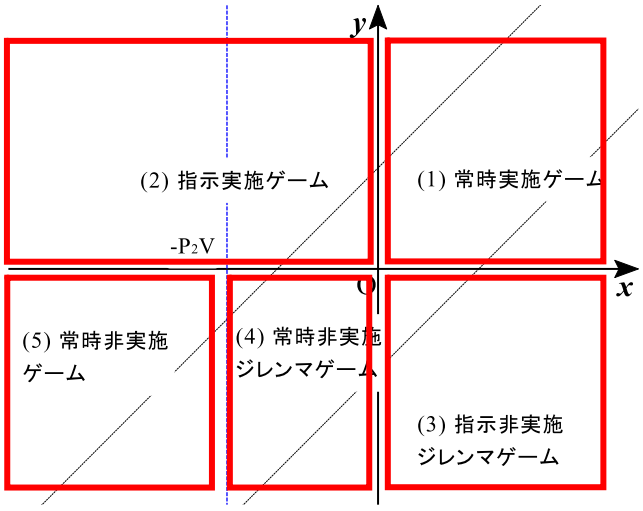

図 1 ゲームの種類
Fig. 1 Five games between promotion section and employee.

は望ましい状態である．

(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．ジレンマ状態が発生しているうえ，推進部門がセキュリティレベルを向上させようとしてセキュリティ対策の実施を指示すると，従業員はそれに反して実施をやめてしまうので，組織全体のセキュリティレベルは低下することになる．セキュリティマネジメント上，特に望ましくない状態である．

(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．ジレンマ状態が発生しているうえ，従業員がセキュリティ対策を実施しないので，セキュリティマネジメント上望ましくない状態である．

(5) 常時非実施ゲーム（$x < -P_2V \leqq 0$，$y < 0$ 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．従業員がセキュリティ対策を実施しないので，セキュリティマネジメント上望ましくない状態である．

4. セキュリティ事例の分析

4.1 用いるセキュリティ事例

ある学校の教員用 PC で発生したセキュリティ事例に着目する [11]．

事例において，この PC は，セキュリティ対策のため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，利用者である教員が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た．漏えいした情報の中には理解度試験が含まれていたため，理解度試験の再作成とその実施が必要となった．その教員は以前はパスワードを記憶していたが，それを忘れたため推進部門に依頼して取り消し・再発行の手続きをしたことがあり，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．

この事例では，セキュリティ推進部門のとった推進策は「パスワードを 1 週間ごとに変える」であった．すなわち，セキュリティ推進部門のとりうる戦略は，「パスワードを 1 週間ごとに変える」と「パスワードを 1 週間ごとに変えない」である．戦略「パスワードを 1 週間ごとに変えない」をとった場合，パスワードの変更は従業員（本事例では教員）の判断に任されることになる．

推進部門が「変える」の戦略を選択した場合，従業員は，システムにより強制的に 1 週間ごとの変更を強いられる．このため，従業員がとりうる戦略は，「決めたパスワードを覚える（紙に書きとめない）」か「決めたパスワードを覚えない（紙に書きとめる）」のいずれかとなる．

4.2 公表されたデータからのパラメータの算出

従業員のペイオフを構成するパラメータの値を種々の公表値をもとに求める．共通の評価尺度とするため，ペイオフの値はすべて金額に換算して算出する．

2 章で述べたように，実際のセキュリティ事例における損害額や対応費用，従業員が認識するセキュリティ事故の発生確率などを具体的に求めた先行研究は見当たらない．また，セキュリティという特殊性のため，事故の発生自体の公表がなされない場合もある．公表された場合でもその詳細については明らかにされないことが多く，部外者が追調査を行うこともまた困難である．

本事例のような教育現場におけるセキュリティ事象も，詳細な情報の公開や分析を行った例は見当たらない．そこで本研究では，公表されている各種の調査データや統計データを用い，妥当と思われる推定を行って計算する．セキュリティ施策は継続的に行われるため，単位時間あたりの値で考える．単位時間は 1 年とする．

(1) 従業員の時間あたりのコスト

総務省の調査 [12] によれば，高等学校教育職の月額平均

給与は 430,111 円とされている．月の労働時間 20 日，1 日 8 時間とすると，

$$430{,}111\text{ 円} \div (20\text{ 日} \times 8\text{h}) \fallingdotseq 2{,}688\ [\text{円/h}] \tag{4}$$

が，従業員の時間あたりのコストとなる．本研究では今後この金額を従業員の時間あたりのコストの値として用いる．

(2) セキュリティ対策実施による業務効率の低下量 Y_d

従業員がセキュリティ対策を行うことによる業務効率の低下量 Y_d は，1 つのパスワードを作成し記憶するのに必要な時間となる．十分なセキュリティ強度を持ついわゆる「良いパスワード」の必要性や生成方法は，政府・公共機関や一般の雑誌などで取り上げられており，多くの組織でも従業員に対する教育が行われている [13], [14], [15], [16]．従業員は，これらに従って，パスワードを考案し，それを記憶にとどめるよう暗誦し，パソコンのパスワード変更画面でそれまでのパスワードを入力した後に新たなパスワードを入力し，確認のため同一のパスワードを入力する．これらの作業は通常は数分で完了する．ここでは，その時間を 3 分とする．時間あたりのコスト式 (4) から，

$$Y_d = 2{,}688\text{ 円/時} \times (3/60) \fallingdotseq 134.4\ [\text{円}] \tag{5}$$

となる．

(3) セキュリティ対策に従うための対応コスト C_a

セキュリティ推進部門が戦略「パスワードを 1 週間ごとに変更する」を選んだ場合，従業員は，最初のパスワード設定に加え，さらに 51 回のパスワードの作成と記憶を年間に行う必要がある．この 51 回分の作業は，従業員から見れば推進部門から指示されそれに従うのに必要なコスト C_a となる．式 (3) から，

$$C_a = 134.4\text{ 円} \times 51\text{ 回} = 6{,}854\ [\text{円}] \tag{6}$$

となる．

(4) 事故が発生したときの損失量 Y_2

推進部門が 1 週間ごとのパスワード変更を指示せず，従業員もそれを行わなかった場合には，ある確率でセキュリティ事故が発生し，業務上の損失が生じる．本事例の場合は，実際に漏えいが発生して理解度試験の再実施が必要となった．よって，理解度試験の再作成，再実施，再採点，再集計などの手間が事故発生時の損失 Y_2 となる．理解度試験の再作成，再実施の準備と実施，再採点と再集計に合計 2 日間分の手間がかかると想定する．時間あたりのコストから，

$$Y_2 = 2{,}688\ (\text{円/h}) \times 2\text{ 日} \times 8\text{h} = 43{,}008\ [\text{円}] \tag{7}$$

となる．

(5) ペナルティ V

推進部門から 1 週間ごとのパスワードの変更を指示されたとき，従業員がその指示に従わずにパスワードを紙に書きとめる戦略をとった場合には，ランダムな文字列を紙に記載するだけの作業で済むので，それに必要なコストはほとんどかからない．しかし，それにより事故が発生した場合には，従業員はペナルティを受ける．

民間企業の人事労務担当者に対して行った，従業員に対する処分内容の調査 [17] によると，提示した 12 の違反事項のモデルケースのうち，意図的かつ悪質な 2 つのケース「社内機密データを勝手に持ち出し，インターネット上で公開した」と「上司のパスワードを使って，アクセス権のない社内機密データに不正にアクセスし，コピーした」以外は，最も多かった処分は譴責（始末書提出）であった．これは，最も処分が重い場合を想定しての回答である．よって，ここでは従業員がパスワードを紙に書きとめ，それが事件事故となった場合に受けるペナルティ V を，始末書の作成と上司や関係者への謝罪とする．これには半日の時間がかかると想定する．時間あたりのコストから，

$$V = 2{,}688\ (\text{円}) \times 4\text{h} = 10{,}752\ [\text{円}] \tag{8}$$

となる．

(6) 従業員が認識する事故の発生確率 P_2

従業員が認識するセキュリティ事故の発生確率の数値を算出する．

2 章で述べたように，セキュリティ事故において従業員が事故の発生確率をどの程度の値と認識していたかの報告例はない．本事例の従業員に対して新たに調査を行うのもきわめて困難である．また，広く一般のインターネットユーザに対して行ったアンケートはあるが，「現在のインターネットの安全性は，100%中，平均 54.8%」に感じているという漠然とした評価結果であった [2]．一方，広くリスクについてその実際の発生頻度を報告した例 [18] はあるが，人口 10 万人あたりの年間の死亡者の数であり，重大とはいえ命に関わるようなことの少ないセキュリティ事故の確率とは，状況が異なっていると思われる．

そこで本研究では，学校における情報漏えいの発生状況の調査結果から，発生件数の率を従業員の認識する事故の発生確率と見なして算出する．

本研究では，経済産業省が実施した調査 [19] に着目した．この調査は無作為に抽出した全国の小中高等学校 206 校に対して行われたもので，回収 99 部（回収率 48%），回答校 105 校であった．この中に，情報セキュリティ事故の経験の有無を尋ねた問いがある（問い (29) 番）．情報漏えいの経験は 8 件なので，回答した学校の総数 105 件から，従業員が認識する事故の発生確率 P_2 は

$$P_2 = 8 \div 105 \fallingdotseq 0.0762 = 7.62\ [\%] \tag{9}$$

となる．

以上，算出した本セキュリティ事例のパラメータの値をまとめたものを**表 2** に示す．

表 2 本セキュリティ事例のパラメータの値
Table 2 The parameters of the actual security incident.

パラメータ	値	単位	意味
Y_d	134.4	円	セキュリティ対策実施による業務効率の低下量
C_a	6,854	円	セキュリティ対策に従うための対応コスト
Y_2	43,008	円	事故が発生したときの損失量
V	10,752	円	ペナルティ
P_2	7.62	%	従業員が認識する事故の発生確率

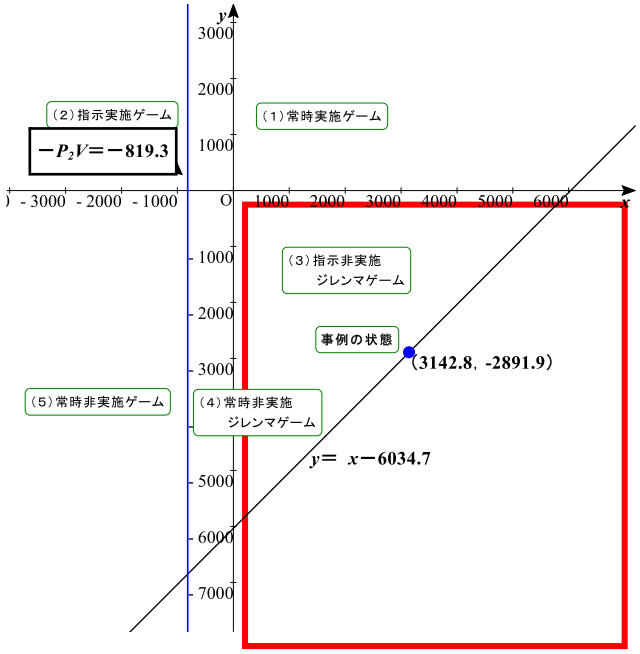

図 2 本事例の状態
Fig. 2 The state of the actual security incident.

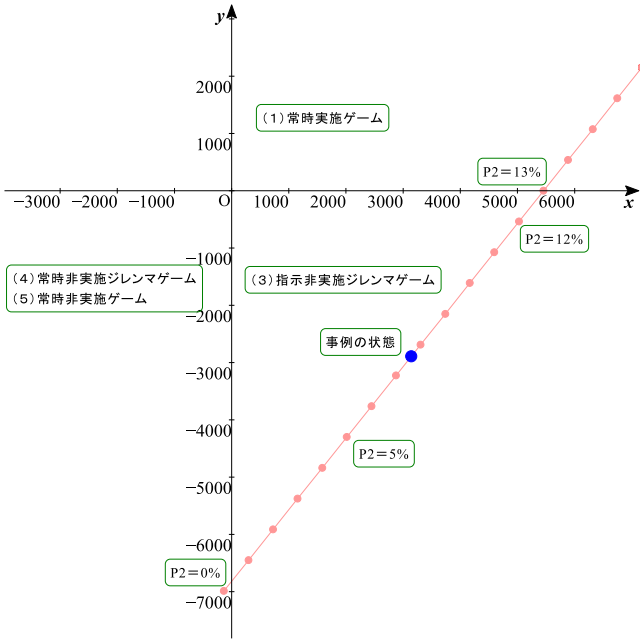

図 3 P_2 の値と状態
Fig. 3 The value of P_2 and the state.

4.3 事例のゲームの状態

(1) ゲームの種類

4.2 節で求めたパラメータの値により x, y を計算してその数値を求める．

式 (1)，式 (3) に各パラメータの値を入れると

$$x = -Y_d + P_2 Y_2 = 3142.8 \tag{10}$$

$$y = x - C_a + P_2 V = -2891.9 \tag{11}$$

となる．これは $x \geqq 0$，$y < 0$ の領域にあるので，本事例は**図 2** の「(3) 指示非実施ジレンマゲーム」の状態であることが分かる．

(2) 従業員が認識する事故の発生確率による状態の変化

従業員が認識する事故の発生確率は，人により大きく異なる可能性がある．そこで，従業員が認識する事故の発生確率 P_2 の値がどのような値をとるとセキュリティ事象がどのような状態に変化するのかを分析する．

「(4) 常時非実施ジレンマゲーム」は，y 軸と $x = -P_2 V$ に挟まれる領域なので，その存在には

$$-P_2 V < x < 0 \tag{12}$$

という条件が発生する．

式 (12) の後項の条件は「(2) 指示実施ゲーム」もしくは「(3) 指示実施ジレンマゲーム」との境界と一致する．式 (10) の前項の条件は，変形して整理すると

$$Y_d/(V + Y_2) < P_2 \tag{13}$$

となる．

これにより，従業員の認識する事故の発生確率 P_2 が 0%から 0.25%の場合「(5) 常時非実施ゲーム」になり，0.25%から 0.31%の間で「(4) 常時非実施ジレンマゲーム」になり，0.31%から 13%の間で「(3) 指示非実施ジレンマゲーム」になり，13%以上では「(1) 常時実施ゲーム」となる．

このときの P_2 の値を 0%から 1%刻みで計算した状態を，**図 3** に赤い点としてプロットする．P_2 の値が大きい場合，状態は右上の「(1) 常時実施ゲーム」の方向にあることが分かる．

5. 考察

5.1 事例の状態から見たモデルの妥当性

本事例の場合，当初，従業員（教員）はパスワードを紙に書きとめず記憶していたが，その後それを忘れたという経

表 3 C_a を改善したときのパラメータの値
Table 3 The value of the parameters at improved C_a.

パラメータ	値	単位	意味
Y_d	134.4	円	セキュリティ対策実施による業務効率の低下量
C_a	1,478	円	セキュリティ対策に従うための対応コスト
Y_2	43,008	円	事故が発生したときの損失量
V	10,752	円	ペナルティ
P_2	7.62	%	従業員が認識する事故の発生確率

緯がある．これは，もしも推進部門が 1 週間ごとのパスワードの変更を指示しなかったならば，そのパスワードをそのまま記憶して使っていたことを示している．つまり，推進部門が戦略「パスワードを 1 週間ごとに変えない」を選択すれば従業員は戦略「決めたパスワードを覚える（紙に書きとめない)」を選択し，逆に推進部門が「パスワードを 1 週間ごとに変える」をとった場合に従業員は「決めたパスワードを覚えない（紙に書きとめる)」を選択してしまったことになる．すなわち，「指示非実施ジレンマゲーム」が発生していることが現象面からも示される．本モデルはこれを定量的に示している．

また，モデルによる分析の結果は，従来から経験的に得られている実際の組織のセキュリティ対策の特徴とも合致している．すなわち，従業員が事故の発生確率をゼロもしくは非常に小さなものと認識している場合には，推進部門からどれだけセキュリティ対策を指示されても実際には実施しない．反対に，事故の発生確率が非常に大きいと認識している場合には，従業員は推進部門の指示の有無にかかわらず自らセキュリティ対策を実行して自己防衛を行う．そして，さほど発生確率が高くないと思われる状況では，多少の手間で済むものなら従業員は自発的に対策を行うが，推進部門からの指示どおりに行うと煩雑な作業をしなければならないような場合には，そのセキュリティ対策を実行しないことがある．本モデルにより得られた分析結果はこれらの経験と合致する．

5.2 改善策

一般に行われているいくつかのセキュリティ対策を本事例に適用し，それらが本事例をどのように改善するかを検討する．

対策がモデルの各パラメータの値の変化とどのように関連するかを明らかにし，それらを本事例に適用した場合にどのような効果があるかを，モデル上で考える．そして，従来の経験と比較して，その妥当性を検討する．

(1) 推進時の従業員の対応コスト C_a の低減

事例では，推進部門がパスワードを 1 週間ごとに変更していたが，これを 1 カ月に 1 度変更する場合を考える．パスワードの変更は，最初の 1 回に加え年間に 11 回の変更となるので，従業員の対応コスト C_a は，

$$C_a = 134.4\text{ 円} \times 11\text{ 回} = 1{,}478\text{［円］} \tag{14}$$

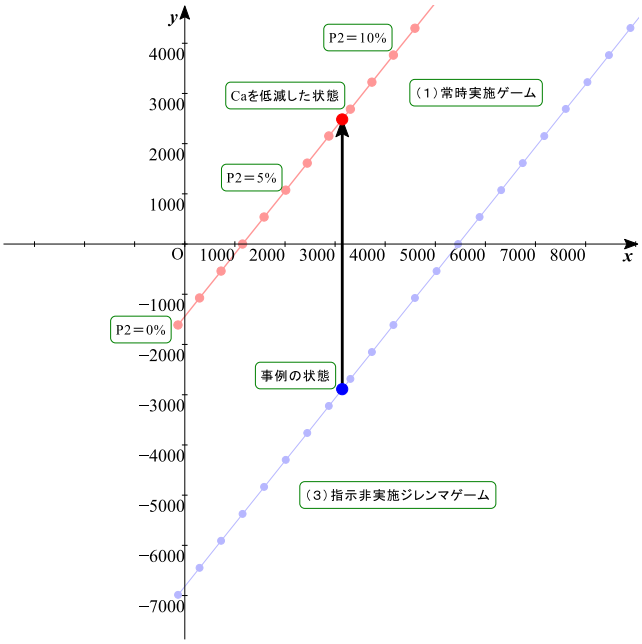

図 4 パスワード変更期間の延長による C_a の低減
Fig. 4 A decrease in C_a by the extension of the password change period.

に減少する．

なお，パスワードの変更期間は本来はそれが解読される時間をもとに技術的に算出して設定されるべきであるが，本論文ではこの問題には立ち入らないこととする．

各パラメータを**表 3** に示す．

この場合，ゲームの位置は

$$x = -Y_d + P_2 Y_2 = 3142.8 \tag{15}$$

$$y = x - C_a + P_2 V = 2484.1 \tag{16}$$

となる．これは，「(1) 常時実施ゲーム」である．もとの状態が「(3) 指示非実施ジレンマゲーム」であったものから「(1) 常時実施ゲーム」となるので，セキュリティ対策上望ましい方策である．

さらに，P_2 の値をいくつかに変化させた場合の x と y の値を図示したものをあわせて**図 4** に示す．このとき，従業員の認識する事故の発生確率 P_2 が 0%から 0.25%の場合「(5) 常時非実施ゲーム」になり，0.25%から 0.31%の間で「(4) 常時非実施ジレンマゲーム」になり，0.31%から 3.0%の間，「(3) 指示非実施ジレンマゲーム」に，3.0%以上で「(1) 常時実施ゲーム」となる．もとの状態では従業

表 4 ペナルティ V を法定内で増加させたときのパラメータの値
Table 4 The value of the parameters by the increase in the legality of penalty V.

パラメータ	値	単位	意味
Y_d	134.4	円	セキュリティ対策実施による業務効率の低下量
C_a	6,854	円	セキュリティ対策に従うための対応コスト
Y_2	43,008	円	事故が発生したときの損失量
V	21,504	円	ペナルティ
P_2	7.62	%	従業員が認識する事故の発生確率

員の認識する事故の確率が 13%以上で「(1) 常時実施ゲーム」だったものが，本方策では，3.0%以上で「(1) 常時実施ゲーム」となる．すなわち，従業員がセキュリティ対策をより実施することになり，その点からも，本方策はセキュリティ対策上望ましいといえる．

これは，セキュリティ対策を実施するための負担が少ない方策であれば多くの従業員がそれを実施するという，従来から経験的に得られている組織のセキュリティ対策の実情とも合致している．

(2) ペナルティ V の増加

従業員が施策に従うよう，従業員に対するペナルティを増加させることがある．ペナルティの代表的なものは，懲戒処分の 1 つである減給である．日本においては労働基準法 91 条の定めにより，1 回の額が平均賃金の 1 日分の半分を超え，総額が 1 賃金支払期における賃金の総額の 10 分の 1 を超えてはならないという規定がある [24]．

これに従うと，従業員の追加のペナルティは半日分の減給となる．よって，元の状態の半日程度の始末書の作成と謝罪に加え，1 日分の給与額がペナルティ V となる．

時間あたりのコストから，

$$V = 2{,}688\text{（円）} \times 8\text{h} = 21{,}504\text{［円］} \tag{17}$$

となる．

各パラメータを**表 4** に示す．

この場合，ゲームの位置は

$$x = -Y_d + P_2 Y_2 = 3142.8 \tag{18}$$

$$y = x - C_a + P_2 V = -2072.6 \tag{19}$$

となる．これは「(3) 指示非実施ジレンマゲーム」の状態である．

さらに，P_2 の値をいくつかに変化させた場合の x と y の値をあわせて図示したものを**図 5** に示す．

従業員の認識する事故の発生確率 P_2 が 0%から 0.21%の場合「(5) 常時非実施ゲーム」になり，0.21%から 0.31%の間で「(4) 常時非実施ジレンマゲーム」になり，0.31%から 11%の間「(3) 指示非実施ジレンマゲーム」に，11%以上で「(1) 常時実施ゲーム」となる．

4.3 節で述べた元の状態よりは改善されているが，「(1) 推進時の従業員の対応コスト C_a の低減」の改善策と比較すると，5.2 節の「(1) 推進時の従業員の対応コスト C_a の低減」ではゲームの状態が「(1) 常時実施ゲーム」に移行したものがこの策では「(3) 指示非実施ジレンマゲーム」にとどまっている点，また，「(1) 常時実施ゲーム」となるための従業員の認識する事故の発生確率が，「(1) 推進時の従業員の対応コスト C_a の低減」では 3.0%以上であるものが本方策では 11%である点から，効果の薄い方策であることが分かる．

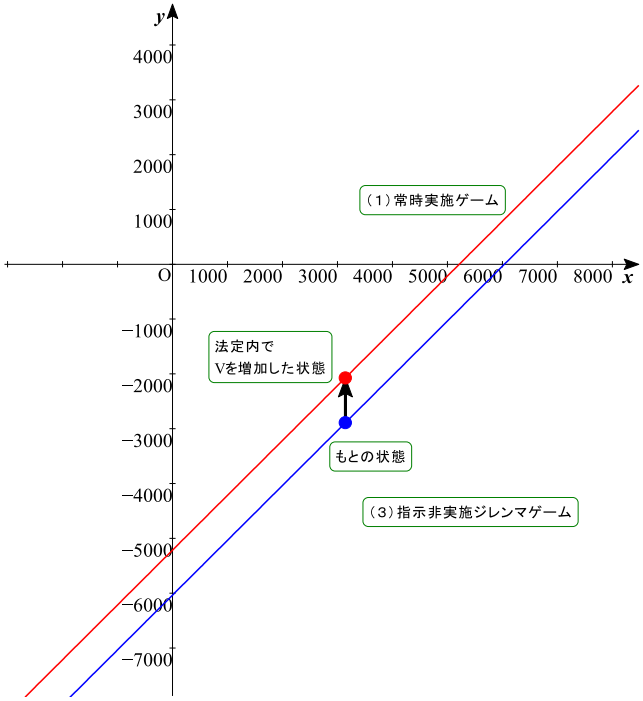

図 5 ペナルティ V の増加による変化
Fig. 5 The change of the state by the increase of penalty V.

さらなる分析のため，法律の定めを超えてさらにペナルティ V の値を大きくすることを検討する．(1) の推進時の従業員の対応コスト C_a の低減では，従業員の認識する事故の発生確率 P_2 が 3.0%以上で「(1) 常時実施ゲーム」となった．そこで，同じ P_2 の値で「(1) 常時実施ゲーム」となるようなペナルティ V の値を計算すると，

$$V = 189{,}938\text{［円］} \tag{20}$$

という高い値にする必要があることが分かる．

(3) 暗号化ソフトウェアの使用とパスワードの変更期間の延長による，推進時の従業員の対応コスト C_a と事故が発生したときの損失量 Y_2 の低減

暗号化ソフトウェアを利用することによって，たとえ不

表 5 暗号化ソフトウェアの使用とパスワードの変更期間の延長を行った場合のパラメータの値
Table 5 The value of the parameters by using encryption software and the extension of the password change period.

パラメータ	値	単位	意味
Y_d	134.4	円	セキュリティ対策実施による業務効率の低下量
C_a	134	円	セキュリティ対策に従うための対応コスト
Y_2	4,301	円	事故が発生したときの損失量
V	10,752	円	ペナルティ
P_2	7.62	%	従業員が認識する事故の発生確率

正に PC 内のファイルにアクセスされてもそれによる被害を最小限にとどめることが可能である．そこで，暗号化ソフトウェアの使用と PC のパスワードの変更期間の延長の 2 つの方策を同時にとる場合を考える．

暗号化ソフトウェアを実際の組織内で利用することによりどの程度セキュリティの被害が低減されるかを数値的に示した先行研究は見当たらない．そこで，本研究では，ファイルの暗号化ソフトウェアを利用することによって事故が発生した際の従業員の損失量 Y_2 が 1/10 になると仮定する．また，パスワードの変更期間を半年，すなわち，最初の 1 回以外に半年後にもう 1 回変更するものとする．このときの各パラメータを**表 5** に示す．

この場合，ゲームの位置は

$$x = -Y_d + P_2 Y_2 = 193.3 \tag{21}$$

$$y = x - C_a + P_2 V = 878.6 \tag{22}$$

となる．これは，「(1) 常時実施ゲーム」となる．従業員が自発的にセキュリティ対策をとるので，セキュリティ対策を推進するうえでは，非常に望ましい状態である．

さらに，P_2 の値をいくつかに変化させた場合の x と y の値を図示したものを**図 6** に示す．従業員の認識する事故の発生確率 P_2 が 0%から 0.89%の場合「(5) 常時非実施ゲーム」になり，0.89%から 1.8%の間で「(4) 常時非実施ジレンマゲーム」になり，1.8%から 3.1%で「(2) 指示実施ゲーム」に，3.1%以上で「(1) 常時実施ゲーム」となる．

本施策をとった場合，事例のもとの状態やこれまで述べた他の施策では存在した「(3) 指示非実施ジレンマゲーム」が存在しなくなる点が大きな特徴で，セキュリティ対策として非常に望ましいといえる．また，もとの状態では従業員の認識する事故の確率が 13%以上で「(1) 常時実施ゲーム」だったものが，本方策では，3.1%以上で「(1) 常時実施ゲーム」となる．この点からも，本対策は非常に望ましい方策といえる．

この対策は，新技術の投入による積極的な利便性の向上と，マネジメントの見直しによる負担の軽減という，実際にセキュリティ対策の現場で行われている方策が効果があることを示しており，これは広く経験と合致する．

5.3 事例の選定根拠と意義

本論文で用いた事例は，実際に発生が報告されたセキュリティインシデントである．この事例は，従業員が，セキュリティ対策の負担感が大きい場合に推進部門の指示に従わずにそれを実行せず，その結果セキュリティ事故に至った代表例である．事例の発生の原因や経緯が公開されており，客観性，信憑性がある．モデルのパラメータを算出する際に用いたその他の情報も，客観性や信憑性のある公開情報である．

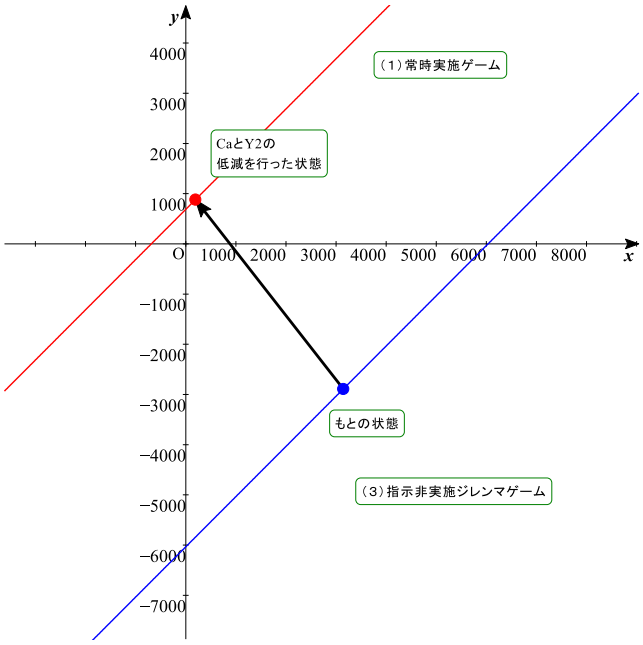

図 6 暗号化ソフトウェアの使用とパスワードの変更期間の延長による変化
Fig. 6 The change of the state by using encryption software and the extension of the password change period.

これらを用い，本事例をモデルに適用してモデルの各パラメータを算出した．そして，パラメータの値とモデルの状態を吟味し，本事例に関してはモデルが現実の姿を適切に表していると考えられることが分かった．すなわち，本事例によってモデルとモデルの各種のパラメータの妥当性を定量的に検証することができた点で重要である．

また，本事例のように，セキュリティ対策の負担感が大きい場合に従業員が推進部門の指示やルールに従わずに事故に至った事例はほかにも発生している．本事例が報告された教育現場における情報セキュリティ事故の報告 [11] でも多くの事例が報告されている．教員の利用が集中するため，定められた専用 PC 以外の一般利用 PC で生徒の成績

データの処理を行ってしまい，その結果，成績ファイルがそのPCの内部に保存されてしまった事例，PCを用いた授業を進行させるためIDとパスワードを忘れた生徒に他の生徒からそれらを借用するよう教員が指示した事例，作業を行う教員の負担が大きいため校内のPCのセキュリティパッチの適用を怠ってウイルス感染した事例，個別にアクセス権限を設定することが負担となるため利用者に一律にフルアクセスの権限をあたえてしまった結果，他のクラスの生徒の誤操作によってすべてのファイルが別のフォルダに移動してしまった事例，などが報告されている．すなわち，これらの事例からすれば，本事例が，モデルで用いた変数やパラメータに関して，代表的な事例であると位置づけることができると考えられる．

5.4 改善策の有効性について

考察した改善策が本当に有効であるかどうかを検証するためには，インシデントの場に立ち戻って実際にその施策を実施して調査する必要がある．しかし本事例においてそれを行うのはきわめて困難であるため，本論文では，一般的と思われる過去の経験と比較してその妥当性の検証とした．経験との比較なので客観性についてはさらなる検討の余地があるが，モデルとパラメータの現実妥当性の検証を行うことができたと考える．今後，アンケート調査や社会実験などでさらに深く検証できる可能性があり，本研究はその基礎検討になると考えられる．

5.5 事例の時期の妥当性

従業員が認識する事故の発生確率P_2の算出に用いた事例の調査[19]は2003年のものである．この調査は2003年以降は行われていない．このため，これ以上新しい調査結果を用いることは不可能である．

一方，教員用PCのセキュリティ事例は2007年に報告[11]されたものであるが，2004年から2006年の間に個別に学校を訪問し，ヒアリングを行って収集した調査データを用いている．これには2003年から2006年の間に発生した事例が報告されており，発生時期が明記されていない事例も一部に含まれるがこれらも同時期に発生した事例であると考えるのが妥当である．本研究で用いた教員用PCのセキュリティ事例も，正確な発生時期は不明であるが，同時期と考えられる．

また，セキュリティ事件・事故は，1999年の宇治市における情報漏えい事件や，2000年の官公庁のWebサイトの書き換え事件のころから頻繁に報道されている．このため，2003年当時から，セキュリティは多くの従業員にとって重要な関心事であったと予想される．セキュリティに対する初等中等教育機関の組織的な取り組みも，組織のセキュリティポリシの作成やセキュリティ責任者の配置のようなその後の進展はあるものの，取り組みの姿勢や体制の概要はこれも大きく変化していない．

さらに，平成22年3月付の事例集[23]が公開されており，その中に教員用PCのセキュリティ事例が再録されている．よって，教育現場における推進部門や従業員の置かれた状況に大きな変化があったわけではないと考えられる．

このため，2003年当時の調査データを用いたことによって，P_2の値の精度が低下してそれが分析結果の数値に影響を与える可能性はあるものの，それが本研究の分析の枠組みや手法に大きな影響を与えるものではないし，検証対象としたモデルの現実妥当性の吟味を不可能とするものでもないと思われる．したがって，これらの調査結果を用いるのは，現実的で妥当であると判断される．

6. 結論

本論文では，組織のセキュリティ対策推進モデルを用いてセキュリティ事件・事故の事例を，定量的に分析した．パラメータ値を算出し，事例がモデルのどの状態に相当するのかを明らかにした．事例の状況とモデルが表す特性とを比較して，モデルが実際の事象を適切に表現していることを確認した．

さらに，モデルの各パラメータの値を変化させるいくつかのセキュリティ対策を検討し，それにより，本事例においてどのようなセキュリティ対策を行うのがセキュリティ対策の推進のうえで効果があるかをモデルのうえから求めるとともに，それらのセキュリティ対策を従来からの経験と比較してその妥当性を検証した．

これにより，用いたモデルが現実の組織のセキュリティ対策の推進を表現できる可能性があること，また，本モデルによる組織のセキュリティ対策の推進の分析が，セキュリティ対策を検討する際に有用な手法となる可能性があることを示した．

7. 今後の課題

本論文では，公表された事例をもとにモデルのパラメータを算出した．このため，いくつかの仮定をおき，妥当と思われる数値を求めてそれを適用した．今後，セキュリティ事例をより詳細に調査することによって，各パラメータの値をより厳密に求め，それを用いて分析することが必要である．特に，従業員が認識する事故の発生確率については，行動経済学や社会心理学などの社会科学の分野で行われているアプローチなども用いて研究を進める必要がある．

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くだ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] 教育ネットワーク情報セキュリティ推進委員会：平成22年度学校・教育機関の個人情報漏えい事故の発生状況・教

員の意識に関する調査 (2010).
[2] さくらインターネット（株）：インターネット使用に関する習熟度と危機管理意識調査 (2009).
[3] 大谷尚通，桑田喜隆，小迫明徳，井上　潮：依存モデルを用いたセキュリティ・アセスメントのための被害予測システムの検討 (2002).
[4] 山田英史，大谷尚通，山本　匡：インシデント調査に見る現状と情報漏洩の想定被害額—個人情報漏洩における想定損害賠償額の算定 (2004).
[5] 日本ネットワークセキュリティ協会：2010 年情報セキュリティインシデントに関する調査報告書—個人情報漏えい編 (2010).
[6] 武藤滋夫：ゲーム理論入門，日本経済新聞社 (2001).
[7] 鈴木光男：新ゲーム理論，勁草書房 (1994).
[8] 鈴木一功：MBA ゲーム理論，ダイヤモンド社 (1999).
[9] Taylor, M.: *Possibility of Cooperation: Studies in Rationality and Social Change*, Combridge University Press (1987). 松原　望（訳）：協力の可能性, 木鐸社 (1995).
[10] 杉浦　昌，諏訪博彦，太田敏澄：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，情報処理学会論文誌，Vol.52, No.6, pp.2019–2030 (2011).
[11] 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).
[12] 総務省：平成 21 年年地方公務員給与実態調査結果 (2009).
[13] 警察庁：セキュリティ講座　入門講座　ID・パスワード管理編，入手先 ⟨http://www.npa.go.jp/cyberpolice/downloads/begin_07_031217.zip⟩ (2003.12.17 更新).
[14] （独）情報処理推進機構：IPA 対策のしおりシリーズ (4)，「不正アクセス対策のしおり—大丈夫ですか，あなたのパソコン？（パソコン利用者向け）」，2008 年 5 月 16 日第 3 版 (2008).
[15] 日経パソコン：2008.6.23，大事な秘密の守り方 (2008).
[16] 日経パソコン：2010.4.12，強いパスワードの現実解 (2010).
[17] 労務行政研究所編集部：企業における情報管理の最新実態，労政時報，No.3777, pp.51–77 (2010).
[18] 武田篤彦：いろいろな事項についての 10 万人あたりの年間死亡数（2006 年版），（財）体質研究会，入手先 ⟨http://www.taishitsu.or.jp/risk/risk2006.html⟩ (参照 2011-09-21).
[19] 経済産業省：初等中等教育現場における情報セキュリティに係る現状調査報告書 (2003).
[20] WEIS2012, available from ⟨http://weis2012.econinfosec.org/index.html⟩.
[21] Stone-Gross, B., Abman, R., Kemmerer, R.A., Kruegel, C. and Steigerwald, D.G.: The Underground Economy of Fake Antivirus Software (2011), available from ⟨http://weis2011.econinfosec.org/papers/The%20Underground%20Economy%20of%20Fake%20Antivirus%20Software.pdf⟩.
[22] Grossklags, J., Johnson, B. and Christin, N.: The Price of Uncertainty in Security Games (2009), available from ⟨http://weis09.infosecon.net/files/161/index.html⟩.
[23] 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 (平成 22 年 3 月) 入手先 ⟨http://www.isef.or.jp/rd/jirei.html⟩ (参照 2012-05-23).
[24] 渡邊　岳，加藤純子：不祥事発生から懲戒処分までの対応ステップと法的留意点，労政時報，No.3774, pp.60–82 (2010).

杉浦 昌　（正会員）

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．2012 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（工学）．ネットワークおよびサーバのセキュリティ対策，セキュリティコンサルティング，国・自治体・民間団体のセキュリティポリシ作成と運用の推進，ISMS 適合性評価制度の推進，セキュリティ標準規格の作成等，セキュリティマネジメントの研究と実践，普及啓発に従事．現在，日本電気（株）勤務．

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，ソーシャルメディアの研究に従事．『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）』，社会情報学会（SSI），日本ソフトウェア科学会，経営情報学会，日本 OR 学会，IEEE 等．