情報処理学会論文誌 Vol.58 No.3 745–753 (Mar. 2017)

情報セキュリティリスク環境下における自身の管理する情報の開示に関する意思決定モデルの提案

藤田 邦彦[1,a)]

受付日 2016年4月25日, 採録日 2016年12月1日

概要：自分自身の個人情報や所属する組織の秘密情報など，自身の管理する情報を不適切に開示する事例が増えつつある．不適切な開示を防止する対策の実施は，当該情報を管理する主体の行動に依存する部分が大きい．本研究では，開示する主体は，開示によって得られる利得と損失をそれぞれの量と確率を勘案して比較し，開示するか否かを意思決定すると仮定しモデル化を行う．このモデル化により，自身の管理する情報の不適切な開示の防止の対策実施に資する貢献が期待できる．本研究ではモデル化に際し，行動経済学において人がどのようにリスクをともなう決定を行うかを説明する理論であるプロスペクト理論を援用する．そして，本研究で提案するモデルを，電子商取引サイトの決済手段の選択の例と，組織の秘密情報を持ち出すか否かの意思決定の例に適用し，適用の結果と，他のアンケート調査の結果の整合性を検討することにより，提案モデルの有効性を評価する．

キーワード：情報セキュリティ，プライバシ，プロスペクト理論，リスク

Proposing Decision Making Model for Disclosure of Information Being Managed by Oneself against Information Security Risk

Kunihiko Fujita[1,a)]

Received: April 25, 2016, Accepted: December 1, 2016

Abstract: The cases of inappropriate disclosure of information being managed by oneself such as personal information of one's own and secret information of organizations are increasing. Preventing inappropriate information disclosure depends on the behavior of the subject who manage the information. In this paper, I assume that the subject who discloses the information compares quantity and probability with respect to gains and losses by disclosing the information and makes a decision. This modeling can be expected to contribute preventing inappropriate information disclosure. In this paper, I apply the prospect theory, which models how people make decisions with monetary risk. I apply the proposed model to two case examples. One is to decide means of settlement in electric commerce cite, and the other is to to decide whether or not taking the secret information outside of the office. I evaluate the effectiveness of the proposed model by considering the consistency between the result of applying the model to two cases and the result of questionnaire surveys being conducted by other organizations.

Keywords: information security, privacy, prospect theory, risk

1. 序論

文献 [1] によると，2013 年末の国内のインターネット利用者数は 10,044 万人（前年比 4.1%増）にのぼり，人口普及率は 82.8%（前年差 3.3 ポイント増）に及ぶ．このような現代日本において，企業や学校などの組織が主体となって行う情報セキュリティ対策はもちろん，情報セキュリティの知識や意識の高い人や低い人を含んだ幅広いインターネット利用者が情報セキュリティに関する行動を行うことが，スマートな社会を実現するために重要である [2]．インターネット利用者の情報セキュリティに関する行動を分析

[1] 文京学院大学
Bunkyo Gakuin University, Bunkyo, Tokyo 113–8668, Japan
[a)] kfujita@bgu.ac.jp

するためには，その前段の情報セキュリティに関する意思決定の構造を分析する必要がある．近年，この分析を社会科学的にアプローチする様々な研究が進められている [3]．本研究では，人が，自分自身の個人情報や所属する組織の秘密情報など，自身が管理する情報を，情報セキュリティリスク環境下で開示する状況を分析対象とし，開示するか否かの意思決定をシミュレートするモデルを提案する．

まず，個人情報の開示・漏洩に係る本研究の意義について述べる．インターネット利用者数が増大するにつれ，ネットワーク上での個人情報のやりとりも増加し，これに比例して個人情報が漏洩する可能性も増えている．安易な個人情報の開示を防ぐため，たとえば，総務省による情報セキュリティ意識を啓発するサイト [4] では，以下のような注意喚起を行っている．

> クレジットカード番号や住所、氏名、電話番号などの重要な情報や、電子メールの内容、商品の購買履歴といった利用者の行動に関する多くの情報が、ネットワーク上をデータとして流れるようになっています。これらの情報は、事故や悪意のある攻撃によって、漏えいしたり、悪用されたりする危険性があることを認識しておく必要があります。
>
> （中略）
>
> さらに、個人のインターネット利用において問題となっているのが、個人情報の公開です。ブログやソーシャルネットワーキングサービス（SNS）を使って、個人が情報発信をする機会が増えていますが、自分の写真や連絡先をインターネット上に公開することには、危険も伴います。また、インターネット上の電子掲示板やホームページなど、誰でも見られる場所に他人の個人情報を公開することは、たとえ事前に許可を得たとしても、プライバシー保護の観点から慎重になった方がよいでしょう。

個人情報の漏洩を防止する対策の実施は，当該個人情報を管理する人の行動に依存する部分が大きいため，上記のような注意喚起を各人に対して呼びかけることは重要である．しかし一方で，人が個人情報を開示する際に，どのように情報セキュリティリスクを認知し，その結果に基づきどのような意思決定を行うかをモデル化することは，個人情報漏洩防止の対策実施に示唆を与えると期待され，有意義である．

次に，所属する組織の秘密情報の開示・漏洩に係る本研究の意義について述べる．企業などの組織で，不正アクセスやウイルス感染，情報漏洩などの情報セキュリティの事故（以下「インシデント」という）の発生が連日のように報道されている．インシデントは，発生場所の観点から，組織外部からのサイバー攻撃と組織内部における不正行為（以下「内部者の脅威」という）の大きく 2 つに分類できる．内部者の脅威の典型的な例は，組織の秘密情報の持ち出しである．内部者の脅威においては，内部者は情報や情報システムにアクセスする権限を持つ場合が多く，価値のある重要な情報の保管場所を知っているため，発生件数に比して被害の規模や被害額が大きい傾向にあり [5]，対策を講じなければならない重要な課題であることは明らかである．また，上記の理由によりアクセス制御などによる技術的な対策のみでは限界があるため，不正行為を誘発する環境要因や，秘密情報の持ち出しという行動をとるに至った意思決定について分析することには意義がある [6]．

本研究では，情報セキュリティを行動科学的にアプローチする．これは，情報セキュリティに関与する主体の態度・行動や振舞いに焦点を当てるものである [7]．行動や振舞いを決定するための，意思決定のメカニズムや要因などを探求するために，本研究では特に，行動経済学において人がどのようにリスクをともなう決定を行うかをモデル化したプロスペクト理論を援用したアプローチを採用し，情報セキュリティリスクの認知と意思決定のモデル化を試みる．行動経済学では，リスク環境下において迫られた選択について，その利得の大小から合理的に意思決定する状況に対し，個人の認知的バイアスが意思決定に反映されることが分かっている．本研究は，これをリスク環境下の情報セキュリティに関する行動においても適用しようという試みである．そのうえで，提案モデルをクレジットカードを利用した消費者購買行動に適用した例と，組織の秘密情報を持ち出すか否かを意思決定する例を示す．

本稿の構成は以下のとおりである．2 章では関連研究について述べる．3 章ではプロスペクト理論を概観する．特に価値関数と確率加重関数というプロスペクト理論を構成する重要な関数について説明する．4 章では，人が情報セキュリティリスク環境下で，自身の管理する情報を開示するか否かの意思決定のモデルを提案する．また，提案モデルの適用例を示し，提案モデルの有効性についての考察を加える．最後に 5 章で結論と今後の課題について述べる．

2. 関連研究

本研究は，自身の管理する情報を開示するか否かの意思決定のモデルを構築する際に，プロスペクト理論という経済学の成果を援用するものである．提案モデルの適用例の 1 つは，組織の内部情報の持ち出しという犯罪における，人間の行動のモデル化である．しかし，犯罪を実行するか否かを経済学的アプローチでモデル化する研究は古くから行われている．以下ではまず，そのような研究の歴史を概観し本研究の位置づけを述べ，次に，情報セキュリティに係る意思決定の問題を対象とした近年の研究について説明

し本研究との違いを述べる．

2.1 犯罪への経済学的アプローチ

Becker は文献 [8] において，経済学において中心的な役割をしている経済合理性を犯罪行為にも応用した研究を発表した．この研究は，犯罪を実行するか否かを，合理的な意思決定プロセスとしてモデル化したものである．このモデルでは，犯罪から得る利益がその機会費用（刑罰や罰金）を上回る限り，犯罪を実行することになる．この場合，刑罰や罰金は犯罪行為に対する対価であり，この対価を支払う能力（所得）が高い者は利益や効用が上回る限り犯罪を実行する．

Becker の研究における意思決定の主体は，いわゆる合理的経済人[*1]である．しかし，実際の人間の行動はそれほど経済合理的ではなく，心理的な影響を受けることが，実験を通じて明らかになった．この実験結果を理論的に説明できる，期待効用仮説に対して心理学的により現実的な理論がプロスペクト理論 [9] である．

本研究では，自身の管理する情報を開示するか否かの意思決定モデルを構築するに際しては，心理的な影響を加味することが妥当と考え，プロスペクト理論を援用することとした．

2.2 情報セキュリティに係る意思決定の研究

従来の情報セキュリティ対策は，技術的対策やルールの策定に重点が置かれていた．しかし，情報システムを利用・管理・運用するのが人間であることから，人のリスク情報の認知や意思決定のメカニズムを解明する社会科学的アプローチの必要性が認識されつつある [3]．

情報セキュリティリスク下での意思決定に関する研究としては，小松らの研究 [10] と杉浦らの研究 [11] があげられる．

小松らの研究 [10] では，ボット対策などの情報セキュリティ対策の状況を社会的ジレンマ状況[*2]と仮定し，個人が合理的選択に基づき行動することを前提に，集団の成員の IT ネットワークという公共財に対する貢献をゲーム理論で定式化したモデルに，アンケートによる社会調査データを適用し，情報セキュリティ対策を実施する個人の意思決定の要因を分析している．

杉浦らの研究 [11] では，組織において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ている．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．

このように，小松らの研究 [10] と杉浦らの研究 [11] の両者とも，分析の対象は情報セキュリティ対策を実施するか否かの意思決定についてであり，分析の手段としてゲーム理論を用いている．一方，本研究は，分析の対象は自身の管理する情報を開示するか否かの意思決定についてであり，分析の手段はプロスペクト理論を用いており，分析の対象と手段が両者の研究と異なる．

また，文献 [12] では，人の情報セキュリティに関する認知と意思決定がプロスペクト理論に基づき，行動が期待効用仮説に基づくという仮説から，セキュリティ対策を実施するべきなのにしない場合や，セキュリティ対策を実施しないでいるべきなのにする場合など，齟齬が生じる状況を分析している．プロスペクト理論を情報セキュリティの分野に適用するという点で本研究と類似しているが，情報セキュリティ投資を対象にするという点で，自身の管理する情報を開示するか否かの意思決定を対象とする本研究とは異なる．

3. プロスペクト理論

本章では，本研究の提案モデルを構築する際に援用したプロスペクト理論について解説する．

プロスペクト理論は，人が宝くじや株式投資など結果が確実ではない，リスクが存在するような商品を購入する際に，そのリスクに対してどのように認知し，どのような行動をとるかについて説明するモデルである [9]．プロスペクト理論は，期待効用理論の代替理論として考案されたものである．

リスクを確率的に含む事象に対して，意思決定主体者が，その価値を数値化し評価したものを効用といい，その期待値を期待効用という．期待効用理論では，発生する可能性のある結果 x によって人がどの程度の効用を得られるかを，効用関数 $u(x)$ によって表す．効用関数は，単調増加（x が大きいほど得られる効用も大きい）と限界効用の逓減（x が 1 単位増加した場合の効用の増分は逓減する）という性質を持つ．また，x の発生確率を p とおくと，期待効用は $p \cdot u(x)$ と表すことができる．

選択を迫られたとき，期待効用が最大化される選択を決定する，といった合理的な個人の選択を期待効用理論という．しかし，個人の選択は必ずしも合理的ではなく，フレーミングと呼ばれるリスク環境下における人の認知の違いに左右されることが確かめられている [13]．フレーミングは，個人のリスク認知に対するバイアスであり，情報セキュリティにおいても，情報資産のリスクを分析する際や対策を実施する際に考慮が必要と考えられる．

このフレーミングを数理的に説明するものが，プロスペクト理論である．プロスペクト理論は 2 つの関数から構成

[*1] もっぱら経済的合理性のみに基づいて行動する個人主義的な人間像．
[*2] 社会が最適とする現象と，個人が合理的と判断する現象が乖離している状況．

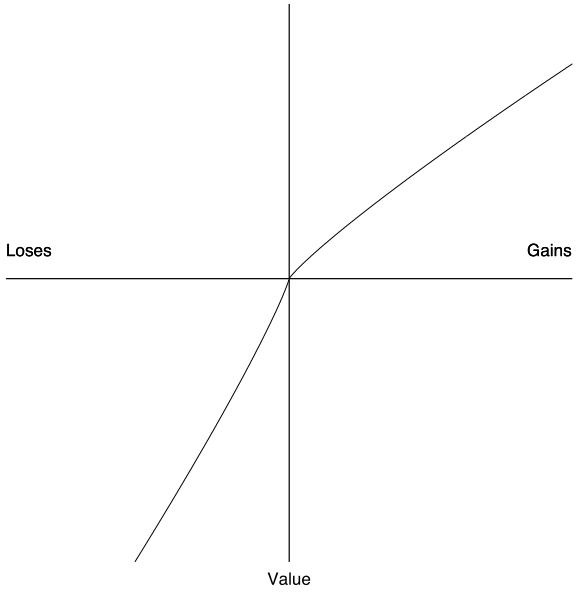

図 1 価値関数
Fig. 1 Value function.

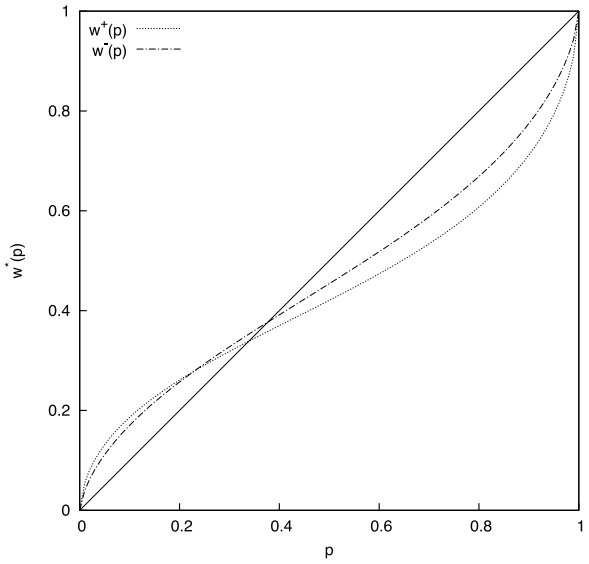

図 2 確率加重関数
Fig. 2 Probability weighting function.

される．1 つは，発生する可能性のある結果それぞれ（たとえば，宝くじの場合は賞金，株式投資の場合は収益率）に対して人がどの程度の満足を得るかを示す価値関数 $v(x)$ である．価値関数は期待効用理論における効用関数に対応する．もう 1 つの関数は，確率に非線形の重み付けをつける確率加重関数 $w(p)$ である．プロスペクト理論における期待効用に対応するものを期待価値と呼ぶとすると，これは $w(p) \cdot v(x)$ と表すことができる．

3.1 価値関数

価値関数は，下式により与えられる [14]．また，これをグラフにプロットしたものが，**図 1** である．

$$v(x) = \begin{cases} x^{\alpha} & \text{if } x \geq 0 \\ -\lambda(-x)^{\beta} & \text{if } x < 0 \end{cases} \quad (1)$$

ただし，x は利得（正の値）または損失（負の値）の量である．文献 [14] によると，被験者実験の結果，$\alpha = \beta = 0.88$，$\lambda = 2.25$ が，最もよく実験結果を近似できる．

価値関数 $v(x)$ は以下の 3 つの特徴を有する．

参照点依存性 価値は参照点（原点）からの変化またはそれとの比較で測られ，絶対的な水準が価値を決定するものではない，という性質．たとえば期待効用理論では 100 万円の効用は一意に決定されるが，プロスペクト理論では，1 万円が 100 万円になったのか，1,000 万円が 100 万円になったのかで，その価値は異なる．この価値判断の基準となる 1 万円や 1,000 万円のことを参照点といい，（主観的な）価値が参照点に従って決まるという特徴を参照点依存性という．

感応度逓減性 利得も損失も，それが小さいうちは変化に敏感だが，大きくなるにつれ，その変化に鈍感になっていく，という性質．利得の局面においては，これは期待効用理論における限界効用逓減の法則と同じことを意味する．一方，プロスペクト理論では，損失局面においても同様に感応度逓減を示すとしているので，人は，利得に関してはリスク回避的，損失に関してはリスク追求的であるということになる．このことは実験によって確かめられている [9]．

損失回避性 人は利得よりも同じ規模の損失を価値ベースでより深刻に感じるというもの．多くの実証研究は，損失回避性のマグニチュード（式 (1) の λ）が 2〜2.5 倍であることを明らかにしている．

3.2 確率加重関数

確率加重関数は，下式により与えられる [14]．また，これをグラフにプロットしたものが，**図 2** である．

$$w^{+}(p) = \frac{p^{\gamma}}{(p^{\gamma} + (1-p)^{\gamma})^{1/\gamma}}$$

$$w^{-}(p) = \frac{p^{\delta}}{(p^{\delta} + (1-p)^{\delta})^{1/\delta}}$$

ただし，$w^{+}(p)$ は利得，$w^{-}(p)$ は損失が予想される場合に適用される関数である．実際の確率 p について，人はそれをどのように評価するかを表すのが，確率加重関数である．文献 [14] によると，被験者実験の結果，$\gamma = 0.61$，$\delta = 0.69$ が，最もよく実験結果を近似できる．

確率加重関数は，人がリスクのある状況で自分にとっての価値を評価する際，個々の事象が発生する確率 p を額面どおり受け取るのではなく，心理的な確率の評価値 $w(p)$ に変換する，ということを表す関数である．

確率加重関数は，確率が 0 と 1 ならびに約 0.35 のときにはそのとおりに評価され，確率が約 0.35 より小さいときには過大評価され，確率が約 0.35 より大きいときは過小評価

されることを表す．

4. リスク環境下の情報開示の意思決定モデル

プロスペクト理論では，リスク環境下において迫られた選択について，その利得の大小から合理的に意思決定する状況に対し，人の認知的バイアスが意思決定に反映されることが分かっている [7]．人は，自身が管理する情報を開示するか否かの意思決定をする際には，情報の開示によって発生する利得と損失を勘案していると考えることができる．損失を発生させる事象（損失事象）は必ず発生するわけではないが，発生する可能性はつねにあり，このような可能性がある状況は，リスク環境下にあるといえる．利得や損失の量と発生確率については，それぞれ判断する主体が認知した結果が，情報開示をするか否かの意思決定の判断材料となる．したがって，自身が管理する情報を開示するか否かの意思決定をモデル化する際にプロスペクト理論を援用することは妥当であり，利得や損失の量については価値関数，利得や損失の確率については確率加重関数を適用することが適切である．

本章では以上の考え方をふまえ，まず最初に損失事象についてモデル化する．次に，利得事象についてモデル化する．そして，リスク環境下の情報開示の意思決定モデルを示し，具体例をあげて当該モデルについて説明を加える．

4.1 損失事象のモデル化

損失事象は，利得を発生させる事象（利得事象）をともなうものとともなわないものに分類できる．例として，電子商取引サイトで商品を購入する際に，クレジットカードを決済手段として用いる場合について検討する．決済が完了した時点で利得事象（たとえばポイントの付与など）が発生するものとする．クレジットカード番号が通信経路上で盗聴された場合は，盗聴という損失事象は発生したが，決済は完了できるため利得事象も発生する（**図 3** 参照）．一方，フィッシングサイトに誘導されてクレジットカード番号を詐取された場合は，詐取という損失事象が発生し，決済は完了できないため利得事象は発生しない（**図 4** 参照）．本研究では，利得事象をともなう損失事象を非排他的損失事象，ともなわない損失事象を排他的損失事象と呼ぶ．

以上の概念を整理し，損失事象についてモデル化する．ある情報を開示する手段 $\mathcal{M}$ において，排他的損失事象の集合を $A^{\mathcal{M}}_{ex} = \{a^{\mathcal{M}}_{ex_1}, a^{\mathcal{M}}_{ex_2}, \ldots, a^{\mathcal{M}}_{ex_n}\}$，非排他的損失事象の集合を $A^{\mathcal{M}}_{nox} = \{a^{\mathcal{M}}_{nox_1}, a^{\mathcal{M}}_{nox_2}, \ldots, a^{\mathcal{M}}_{nox_m}\}$ とする．各事象は独立でない可能性がある．ある複数の独立でない事象が同時に発生した場合，損失の量は累積されるものとする．事象 a の量を $R(a)$ とし $R(a) < 0$ が成り立ち，発生確率を $P(a)$ とし $0 \leq P(a) \leq 1$ が成り立つとすると，情報開示の判断の際に認知される損失の期待価値は，下式のように表せる．

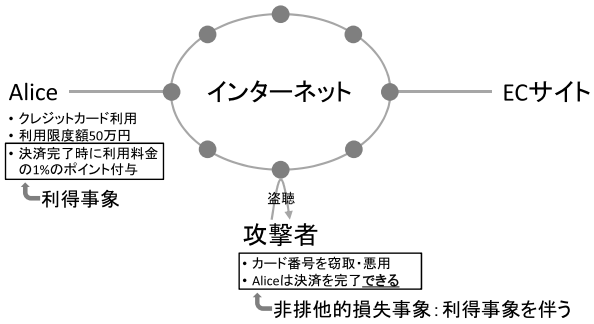

図 3 非排他的損失事象の例

Fig. 3 The example of the nonexclusive loss event.

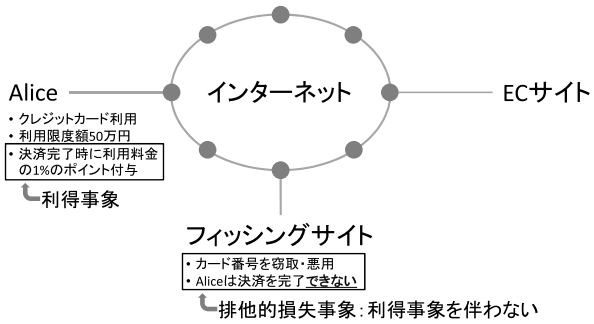

図 4 排他的損失事象の例

Fig. 4 The example of the exclusive loss event.

$$
\begin{aligned}
&Loss(A^{\mathcal{M}}) \\
&\quad = \sum_{i=1}^{n} w^{-}(P(a^{\mathcal{M}}_{ex_i}))v(R(a^{\mathcal{M}}_{ex_i})) \\
&\qquad + \sum_{j=1}^{m} w^{-}(P(a^{\mathcal{M}}_{nox_j}))v(R(a^{\mathcal{M}}_{nox_j}))
\end{aligned}
$$

ただし，v と w は各々 3 章で説明した価値関数と確率加重関数である．また，$0 \leq w^{-}(P(a))$ と $v(R(a)) \leq 0$ より，$Loss(A^{\mathcal{M}}) \leq 0$ である

4.2 利得事象のモデル化

次に利得について検討する．ある情報を開示する手段 $\mathcal{M}$ において，利得事象の集合を $B^{\mathcal{M}} = \{b^{\mathcal{M}}_1, b^{\mathcal{M}}_2, \ldots, b^{\mathcal{M}}_t\}$ とする．排他的損失事象が発生しなかった場合のみ，すべての利得事象が発生するものとする（**図 5** 参照）．事象 b の量を $R(b)$ とし $R(b) > 0$ が成り立つとすると，情報開示の判断の際に認知される利得の期待価値は，下式のように表せる．

$$
\begin{aligned}
&Gain(B^{\mathcal{M}}) \\
&\quad = w^{+}\left(1 - P\left(\bigcup_{i=1}^{n} a^{\mathcal{M}}_{ex_i}\right)\right)\sum_{k=1}^{t} v(R(b^{\mathcal{M}}_k))
\end{aligned}
$$

4.3 リスク環境下の情報開示の意思決定モデル

以上の 2 つの式を用いると，情報開示に関する意思決定をモデル化できる．たとえば，損失が利得を上回る可能性が高い行動は回避する，ということは，

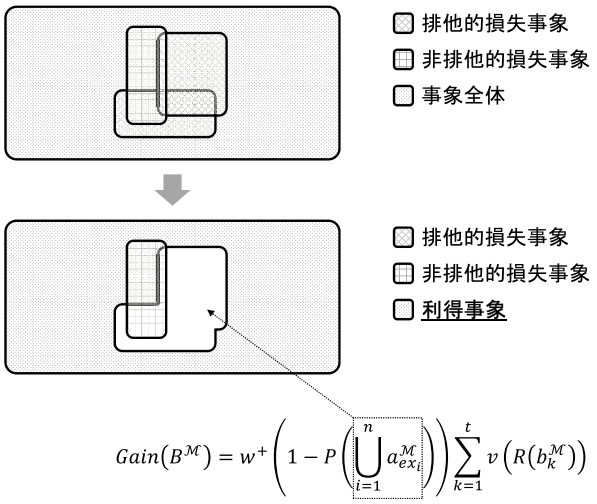

図 5 利得事象の考え方
Fig. 5 The concept of the gain event.

$Gain(B^{\mathcal{M}}) > \left|Loss(A^{\mathcal{M}})\right|$ の条件を満たさなければ，該当する行動をとらない，と表すことができる．また，ある目的を達成するための手段が複数ある場合，それぞれの手段 $\mathcal{M}_1,\ldots,\mathcal{M}_h$ のうち，情報セキュリティの観点からどれを選択するか，という意思決定問題についてもモデル化できる．各々の手段をとった場合に損失を発生させる事象の集合を $A^{\mathcal{M}_1},\ldots,A^{\mathcal{M}_h}$，利得を発生させる事象の集合を $B^{\mathcal{M}_1},\ldots,B^{\mathcal{M}_h}$ とすると，情報セキュリティの観点から選択されるべき手段は，下式のように表せる．

$$max(Gain(B^{\mathcal{M}_1}) + Loss(A^{\mathcal{M}_1}),\ldots, Gain(B^{\mathcal{M}_h}) + Loss(A^{\mathcal{M}_h})) \quad (2)$$

4.4 提案モデルの適用例

4.4.1 決済手段の選択

文献 [15] によると，2013 年末時点でのインターネットで購入する際の決済方法は，「クレジットカード払い」が 63.7%と最も多く，次いで，「代金引換」(43.8%)，「コンビニエンスストアでの支払い」(38.9%)，「銀行・郵便局の窓口・ATM での振込・振替」(30.8%) となっている．このうち，上位 2 つを占める「クレジットカード払い」と「代金引換」を例に取り上げて，電子商取引サイトで商品を購入する場合を想定し，提案モデルの適用を試みる．以下の前提条件を仮定する．

(1) 決済手段はクレジットカード $\mathcal{M}^{Card}$ または代金引換（代引）$\mathcal{M}^{COD}$ とする．
(2) クレジットカードを利用した場合は，利用料金の 1%のポイントが付与されるものとする．また，当該ポイントの交換比率は，1 ポイント = 1 円とする．ポイントの付与は利得事象である．
(3) クレジットカード利用限度額は 50 万円とする．
(4) クレジットカードを利用した場合の，カード番号の漏洩による被害額は，クレジットカード利用限度額とする．また，フィッシングによるカード番号の詐取という排他的損失事象が発生する確率を $P(a_1^{Card})$ とする．
(5) 代引き手数料は 300 円とする．
(6) 代引では損失事象は発生しないものとする．

以上の前提条件に基づき，s 円の商品を購入する際に，決済手段にクレジットカードと代引のどちらを選択するか，という意思決定問題は，下式で表すことができる．

$$max(w^{+}(1 - P(a_1^{Card}))v(0.01s)+ w^{-}(P(a_1^{Card}))v(-500000), v(-300)) \quad (3)$$

式 (3) を，「利用金額」と「フィッシングによるカード番号の詐取が発生する確率」と「利得の期待価値と損失の期待価値の和」を軸にとり，$0 \le P(a_1^{Card}) \le 1$ の範囲でプロットしたものが**図 6** で，$0 \le P(a_1^{Card}) \le 0.0013$ の範囲でプロットしたものが**図 7** である．購入金額 s が大きくなればなるほど，カード番号の漏洩の確率 $P(a_1^{Card})$ が高くても，クレジットカードで購入する傾向を示す．

以下では，提案モデルの結果が以上のとおりになったことと，他の調査結果との整合性について検討する．文献 [16] では，インターネットで商品を購入する際の，購入金額と決済手段について，アンケート調査を実施している．アンケート調査の結果の内のクレジットカードと代引につ

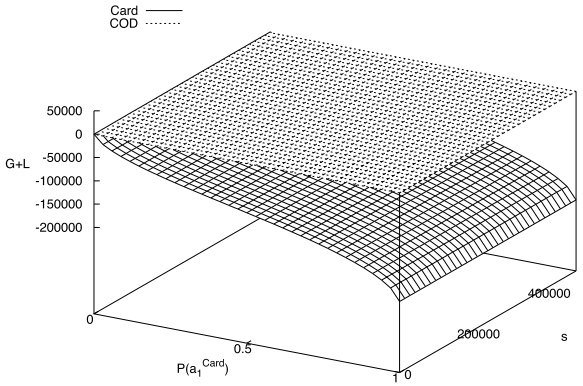

図 6 全体 ($0 \le P(a_1^{Card}) \le 1$)
Fig. 6 The whole ($0 \le P(a_1^{Card}) \le 1$).

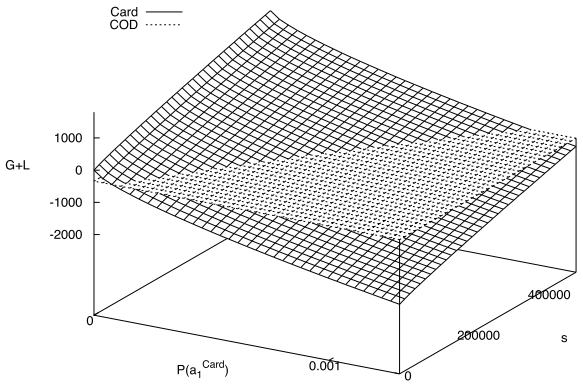

図 7 詳細 ($0 \le P(a_1^{Card}) \le 0.0013$)
Fig. 7 The details ($0 \le P(a_1^{Card}) \le 0.0013$).

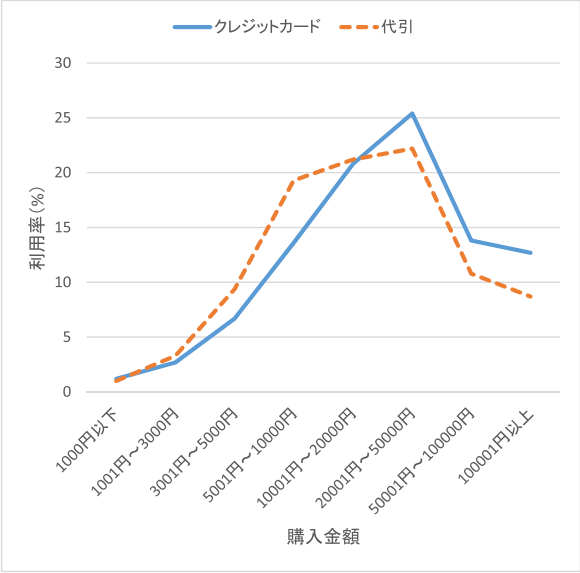

図 8 クレジットカードと代引の，購入金額ごとの利用率
Fig. 8 The utilization rate of credit card and cash on delivery by purchase price.

いて，購入金額と利用率をグラフで表したものが，**図 8** である．図 8 によると，購入金額が 10,000 円以下の場合は代引の利用率が高いが，それを超えるとクレジットカードの利用率が逆転している．この結果は，提案モデルの適用例の結果と傾向が一致している．

残念ながら文献 [16] では，それぞれの決済手段を選んだ理由については調査されておらず，本モデルに組み入れていない他の要因で図 8 のような結果になった可能性もある．しかし，提案モデルで分析した結果と文献 [16] で報告されたアンケート結果は整合するため，提案モデルの有効性の裏付けとなりうる．

4.4.2 組織内部の秘密情報の持ち出し

内部者が，自身の管理している秘密情報を不正に持ち出すか否かの選択について，提案モデルの適用を試みる．まず，文献 [17] を参考に，以下の前提条件を仮定する．

(1) 内部者が秘密情報を持ち出したことが事後的に発覚する確率を q とする．
(2) 発覚した場合の内部者のペナルティは，解雇かつ賠償金 c の支払いが発生する．これは排他的損失事象である．
(3) 秘密情報を持ち出したことによる報酬を d とする．これは利得事象である．
(4) 内部者が将来にわたって組織から受け取る賃金の総額を L とする．これは利得事象である．
(5) 内部者は，持ち出したことが発覚しなかった場合は，d と L の両方を得られる．一方，発覚した場合は，何も得られず，賠償金 c（> 0）の支払いが発生する．
(6) 内部者は，発覚確率を勘案したうえで，秘密情報を持ち出したときと持ち出さないときの利得の大小をもとに合理的に意思決定をする．

以上の前提条件に基づき，内部者が，自身の管理している秘密情報を不正に持ち出すか，という意思決定問題は，下式で表すことができる．

$$max(w^{+}(1-q)v(L+d)+ w^{-}(q)v(c), v(L)) \quad (4)$$

上式について，実際のデータを用いて分析する．分析に際し，以下の前提条件を追加する．

(6) 報酬 d は内部者の年収 l の 2 倍とする．これは，持ち出せる情報の価値が年収に比例することを反映させた仮定である．
(7) 賠償金 c は 1,000 万円とする．
(8) 内部者の年収 l は，厚生労働省の賃金センサスにおける標準労働者（産業計，大卒・男子，企業規模 1,000 人以上）[18] から算出する．
(9) 内部者が将来にわたって組織から受け取る賃金の総額 L は，文献 [18] をもとに DCF（Discounted Cash Flow）法[*3]を用いて算出する．
(10) L を算出する際に必要な退職金額は，厚生労働省の退職給付の支給実態調査 [19] に基づき，2,572 万円とする．

そして，式 (4) を，上記の仮定に基づき，x 軸を発覚の確率，y 軸を内部者の利得とし，内部者が 25 歳，35 歳，45 歳，55 歳のときの様子をプロットしたものが**図 9** である．

図 9 では，実線が秘密情報を「持ち出す」場合の利得であり，破線が秘密情報を「持ち出さない」場合の利得である．すべての年代において，発覚の確率が高いと賠償金を支払う可能性が高まるため，「持ち出す」場合の利得が下がる様子が表されている．また，年齢が低い内部者より高い内部者の方が，「持ち出す」場合の利得が「持ち出さない」場合の利得を上回る範囲が広いことが分かる．換言すると，年齢が高い内部者の方が低い内部者よりも，「持ち出す」インセンティブが強いということである．

以下では，提案モデルの結果が以上のとおりになったことと，他の調査結果との整合性について検討する．文献 [6] では，アンケート調査を実施している．回答者を属性ごとのグループに分け，各グループの不正行為への気持ちの高

[*3] DCF 法とは，将来のキャッシュフローを割り引いて現在価値に換算する手法である．たとえば現在の 10,000 円と 5 年後の 10,000 円では，現在の 10,000 円の方が価値が高い．これは，10,000 円を年利 $r \geq 0$ で運用した場合，5 年後には $10{,}000 \times (1+r)^5$ 円になるからである．この逆算が DCF 法で，5 年後の 10,000 円を現在価値に割り引くと，$\frac{10{,}000}{(1+r)^5}$ 円である．毎年度キャッシュフローが発生する場合の割引現在価値は下式で求められる．

$$L = \sum_{j=1}^{m} \frac{l_j}{(1+r)^j}$$

ただし，m は現在の年度を 0 としたときの将来キャッシュフローの発生する最終年度とする．

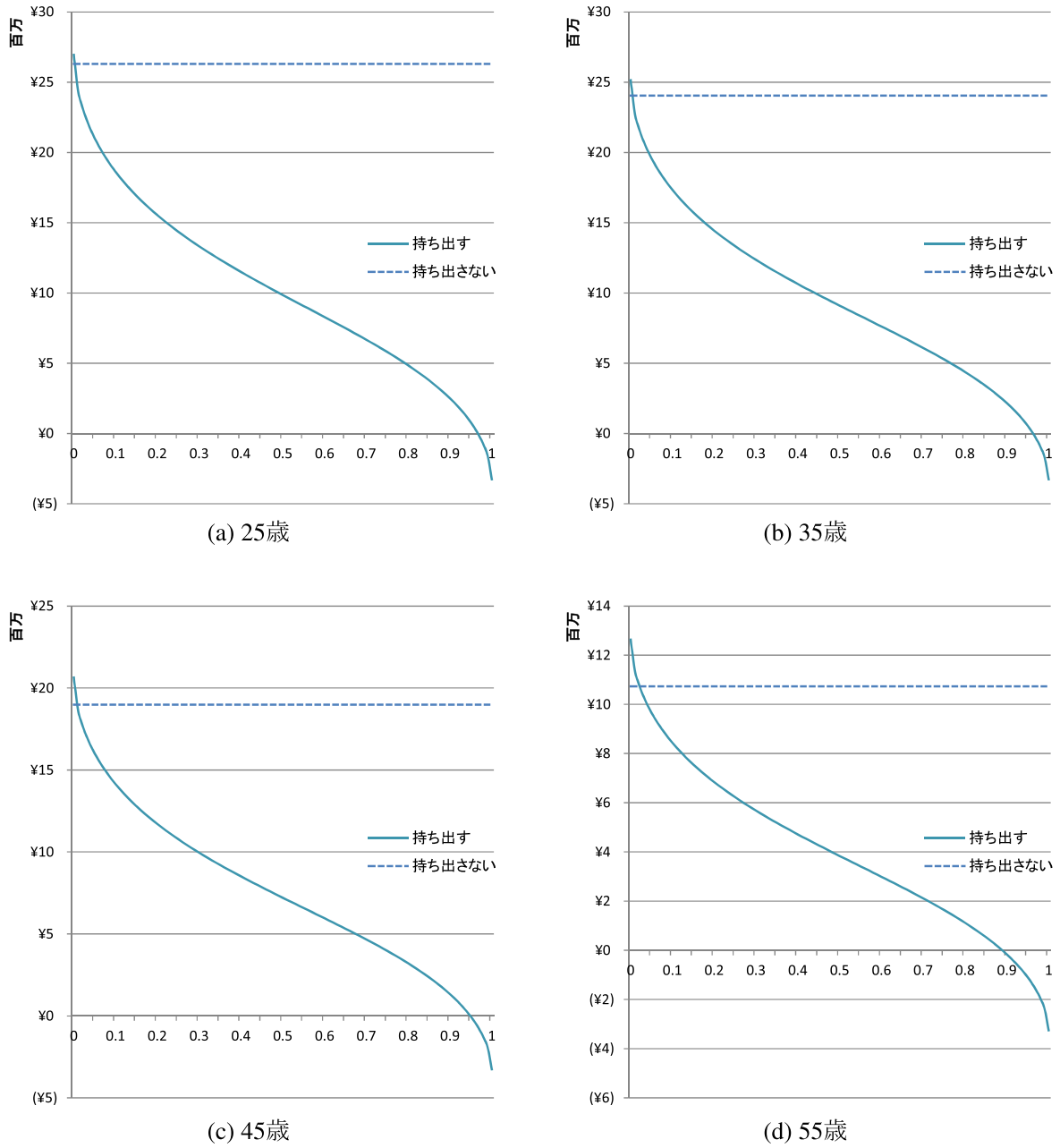

図 9 年齢ごとの，秘密情報を持ち出すか否かのグラフ

Fig. 9 The graph whether or not taking the secret information outside of the office by age.

まり/低下の程度について分析している．属性のうち年齢についても，20 歳代，30 歳代，40 歳代，50 歳代，60 歳以上の 5 つのグループに分類し，「動機・プレッシャ」「環境・機会」「知識・経験」の 3 つのカテゴリについて，それぞれのカテゴリに属する設問に対する平均を算出している．その結果についての全体的な傾向を示した部分を以下に引用する．

> 大まかな傾向として，全年代の中で，不正行為に対する気持ちが最も高まりにくいのは 30 代で，最も高まりやすいのが 60 代以上であることが分かる．
>
> 年代が高くなるにつれて，（単調にというわけではないが）平均値が増加している．つまり不正行為への気持ちの高まり具合が大きくなるケースが，少なからず見受けられる．そこで，そのような傾向がほんとうにあるのか確認したところ，「知識・経験」においてはすべてのケースで，「動機・プレッシャ」「環境・機会」に関しても半分以上のケースで，そのような傾向があることが分かった．

文献 [6] では，そのような傾向が生じる理由については記述がないが，本モデルを適用することにより以下のとおり説明できる．図 9 の示す「年齢が高い内部者の方が低い内部者よりも，「持ち出す」インセンティブが強い」ということは，秘密情報を持ち出すという不正行為に踏み切

る障壁が低いということであり，上で引用した「不正行為に対する気持ちが高まる」ということとほぼ同じ意味である．したがって，文献 [6] のアンケート結果である，年代が高くなるにつれて，不正行為に対する気持ちが高まる傾向を，本モデルが裏付けていることを図 9 は示している．

5. 結論

本研究では，プロスペクト理論を応用し，人の情報セキュリティリスクに関する認知と意思決定がプロスペクト理論に基づくと仮定した場合に，自身の個人情報や所属する組織の秘密情報を開示・漏洩するか否かを決定するモデルを提案した．また，提案モデルを電子商取引サイトの決済手段の選択の例と，組織の秘密情報を持ち出すか否かの意思決定の例に適用し，どのような場合にどのような意思決定がなされるかを明らかにできることを示した．

今後は，提案モデルの評価と精緻化へのフィードバックのため，提案モデルが様々な状況に適用できるかを確認することにより，提案モデルの提供範囲と適用限界を明確にしたい．また，提案モデルに基づき，人がある状況でどのように行動するかを予測し，その予測結果から，必要な情報セキュリティ対策をあらかじめ実施する，などの応用についても検討したい．

謝辞 多くのご助言をいただいた，NTT コミュニケーション科学基礎研究所情報基礎理論研究グループの塚田恭章氏に感謝いたします．

参考文献

[1] 総務省：第 2 部 第 5 章 第 3 節 1 (2) インターネットの利用状況，情報通信白書，日経印刷 (2014).
[2] 諏訪博彦，原 賢，関 良明：情報セキュリティ行動モデルの構築 — 人はなぜセキュリティ行動をしないのか，情報処理学会論文誌，Vol.53, No.9, pp.2204–2212 (2012).
[3] 持永 大，杉浦 昌，小松文子，村野正泰，赤井健一郎，上田昌史：情報セキュリティ事象の社会科学的アプローチによる研究の動向，情報処理学会研究報告，Vol.2009-CSEC-46, No.41 (2009).
[4] 総務省：国民のための情報セキュリティサイト（オンライン），入手先 ⟨http://www.soumu.go.jp/main_sosiki/joho_tsusin/security/intro/security/02.html⟩.
[5] Computer Emergency Response Team (CERT): 2012 CyberSecurity Watch Survey (online), available from ⟨http://www.cert.org/archive/pdf/CyberSecuritySurvey2012.pdf⟩.
[6] 情報処理推進機構（IPA）：組織内部者の不正行為によるインシデント調査（オンライン），入手先 ⟨http://www.ipa.go.jp/files/000014169.pdf⟩.
[7] 小松文子：行動科学的アプローチ，セキュリティマネジメント学，松浦幹太（編），pp.105–122, 共立出版 (2011).
[8] Becker, G.: Crime and Punishment: An Economic Approach, *Journal of Political Economy*, Vol.66, No.2, pp.169–217 (1968).
[9] Kahneman, D. and Tversky, A.: Prospect Theory: An Analysis of Decision under Risk, *Econometrica*, Vol.47, No.2, pp.263–292 (1979).
[10] 小松文子，赤井健一郎，上田昌史，松本 勉：情報セキュリティ対策は社会的ジレンマか？ — ボットネット対策への適用，情報処理学会研究報告，Vol.2009-CSEC-46, No.20 (2009).
[11] 杉浦 昌，諏訪博彦，太田敏澄：組織の IT セキュリティ推進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，情報処理学会研究報告，Vol.2010-CSEC-49, No.1 (2010).
[12] Verendel, V.: A prospect theory appraoch to security, Technical report, Department of Computer Science and Engineering, Chalmers University of Technology, Goteborg University, Sweden (2008).
[13] Tversky, A. and Kahneman, D.: The Framing of Decisions and the Psychology of Choice, *Science, New Series*, Vol.211, pp.453–458 (1981).
[14] Tversky, A. and Kahneman, D.: Advances in prospect theory: Cumulative representation of uncertainty, *Journal of Risk and Uncertainty*, Vol.5, No.4, pp.297–323 (1992).
[15] 総務省：第 2 部 第 5 章 第 3 節 1 (4) インターネットで購入する際の決済方法・購入最高金額，情報通信白書，日経印刷 (2014).
[16] 総務省：平成 25 年通信利用動向調査（オンライン），入手先 ⟨http://www.e-stat.go.jp/SG1/estat/List.do?bid=000001048692&cycode=0⟩.
[17] 藤田邦彦：内部者の脅威のゲーム理論を用いた分析，2014 年暗号と情報セキュリティシンポジウム予稿集，No.2B1-1 (2014).
[18] 厚生労働省：賃金構造基本統計調査（全国）（オンライン），入手先 ⟨http://www.mhlw.go.jp/toukei/list/chingin_zenkoku.html⟩.
[19] 厚生労働省：平成 20 年 就労条件総合調査退職給付（一時金・年金）の支給実態（オンライン），入手先 ⟨http://www.e-stat.go.jp/SG1/estat/List.do?bid=000001016267&cycode=0?⟩.

藤田 邦彦 （正会員）

1999 年北陸先端科学技術大学院大学情報科学研究科情報処理学専攻博士後期課程修了．同年日本電信電話株式会社入社．現在，文京学院大学経営学部准教授．情報セキュリティ，アクセス制御，フォーマルメソッド，デジタル著作権管理の研究に従事．博士（情報科学）．人工知能学会，電子情報通信学会各会員．