情報処理学会論文誌　Vol. 51　No. 9　1711–1725 (Sep. 2010)

情報セキュリティ対策における個人の利得と認知構造に関する実証研究

小松文子[†1,†2]　高木大資[†3]　松本勉[†4]

情報セキュリティ対策は，安全なネットワークを使用するうえで必須である．これまで情報セキュリティ対策は，技術対策と組織などのマネジメントの局面から推進されてきたが，実行主体である利用者の実行がともなわないという現象が見られる．これを解決するためには，個人の意思決定のメカニズムを明らかにすることが有効であると考えられる．本研究では，情報セキュリティ対策を必要とするネットワークを社会的ジレンマ状況ととらえ，利得構造と個人の認知構造について実証調査分析をした．この結果，利得構造では，協力率が低い状況を説明できず，認知構造の調査では，社会的ジレンマ状況であることを支持する結果は得られなかった．しかし，利得構造は対策実行意図と整合し，また認知構造では特定の要素が実行意図へ影響を与えていることが分かったので報告する．

Experimental Study on Individual Gain and Cognitive Structure in Information Security Measures

Ayako Komatsu,[†1,†2] Daisuke Takagi[†3] and Tsutomu Matsumoto[†4]

The information security measures are indispensable to use the secure network. Though the information security measures have been promoted from the aspect of management and technological measures. However, it is reported that the entity who has to do actually does not carry out the information security measures. It is thought it is effective to clarify the mechanism of the individual decision making to solve this. As a result of social survey, it was understood that the gain structure adjusted to the measures execution intention though it was not able to explain the assumed situation. It also observed that a specific cognitive element has influenced the execution intention.

1. はじめに

ネットワークを利用する利用者が，情報セキュリティ対策を実行に移すことが，ネットワーク全体の品質を向上させるために必要である．これまで，ISMS（Information Security Management System）などのマネジメントの観点からの取り組みや，技術対策を適用することなどにより，情報セキュリティ対策が図られてきた．しかし情報セキュリティ対策が，個人によって実施されることを考えれば，個人が情報セキュリティ対策を実行する意思決定の研究が，対策実行の効果をあげるために明らかに有効であろう．実例として，経済産業省と総務省が多くのISPと共同で推進しているCCC（サイバークリーンセンター）が実施する“ボット対策事業”がある[14]．この事業では，CCCがボットに感染しているユーザを検知し，感染したユーザへメールで感染事実を知らせるとともに，ボット駆除ツールを無償で提供している．しかし，対策を実行したのは，年間を通じて感染を知らせたユーザのうちわずか30%程度である．このような状況がなぜ起きているのか，どのようにすれば，この状況を改善できるか，を課題とし，この現象が，「環境配慮行動」に類似していることを参考に，社会学，数理社会学，経済学，社会心理学などの領域で研究されている社会的ジレンマ状況の研究を援用し，個人の意思決定状況の分析を試みた．

本論文では，個人が情報セキュリティ対策を実行することにより，個人の利得をどのように感じているかについて，またどのような認知状況におかれているかについて質問紙調査を行い，情報セキュリティ対策の状況が社会的ジレンマ状況にあるかを分析した．本論文の構成は以下のとおりである．2章で社会的ジレンマ状況の定義と関連研究についてのべ，3章で情報セキュリティ対策を社会的ジレンマ状況と想定し，その利得構造と認知要素を定義し，質問紙調査の概要と結果を述べる．4章で調査結果を分析・考察し，5章で今後の課題を述べる．

†1 横浜国立大学大学院環境情報学府環境メディア情報学専攻
Graduate School of Environment and Information Sciences, Yokohama National University
†2 独立行政法人情報処理推進機構
Security Economics Laboratory, Information-Technology Promotion Agency
†3 東京大学大学院人文社会系研究科
Graduate School of Humanities and Sociology, The University of Tokyo
†4 横浜国立大学大学院環境情報研究院
Research Institute of Environment and Information Sciences, Yokohama National University

2. 社会的ジレンマ状況と関連研究

ここ数年，情報セキュリティに関連する事象に対して，経済学，社会学，社会心理学など社会科学的な観点によりモデル化，事象の構造研究などを行う「セキュリティエコノミクス」という領域が知られるようになってきた[3),5)]．さらに，情報セキュリティ対策を推進するうえでの心理要因に注目した研究も進められている[4)]．これらの研究をふまえて，本論文で扱うボット対策事業が社会科学的に見るとどのような状況にあるかを明らかにするために，個人の意思決定にかかわる個人と社会の利得に注目する．本章では，合理的選択理論に基づく社会的ジレンマの定式化と個人の意思決定に対する誘因についての社会数理学における既存研究と，個人の認知に注目した社会心理学，社会学における実証研究を紹介する．

2.1 社会的ジレンマ状況の定義

社会的ジレンマ状況は，「個人の合理性と社会の最適性がかい離する状況」[2)] といわれる．社会的ジレンマ状況は，社会のあらゆる面に見ることができる．たとえば，大気汚染を例にとると，排ガスの性能が高い自動車を，性能やコストの面から購入せず，結果として大気汚染が進み，個人にも悪影響を及ぼすといった状況である．社会心理学者のドウズは，次の 2 つの条件を満たす社会状況を，社会的ジレンマ状況と定義した[1)]．

a) 社会的に非協力な行動をとる各個人の行為への結果（payoff）は，他のだれが協力していようが，協力行動をとる個人の行為への結果（payoff）よりも高い．

b) しかし，全員が非協力の場合の，1 人ひとりの行為への結果（payoff）は，全員が協力した結果（payoff）より小さい．

また，ドウズは，社会的ジレンマ状況を N 人囚人のジレンマゲームとして定式化した．ゲーム理論は，個人が他者との関係において，なんらかの意思決定を行う場合，その意思決定の選択それぞれに利得を設定し，いかなる選択が可能であるかを検討する手段の 1 つである．社会的ジレンマ状況に関しては，個人と他者（社会）との関連における意思決定を解明するという観点で文献 1)，8) をはじめとしてゲーム理論を使用する研究がある．これは，個人が，ある選択を迫られたとき，その選択がもたらす利得の大小のみによって行動を選択する「合理的選択理論」で意思決定することを前提とする．利得とは，個人がある行為を行った結果，個人が得られる益を指す．ここでは，金銭ではかられるものだけでなく，使いやすさなども含まれる．

N 人からなる集団において，条件 a）で述べた他人に迷惑をかける選択行為を「非協力」，迷惑をかけない選択行為を「協力」とし，それぞれ C，D とする．集団において m 人が協力を選択している場合，$C(m)$ を協力を選択した個人が受ける利得，$D(m)$ を非協力を選択した個人が受ける利得とする（$0 \leqq m \leqq N$）．受ける利得は全員が m により一定であるとする．Dawes は，以下の式 (1)，(2) が成り立つ状況を社会的ジレンマ状況と定義した．

$$D(m-1) > C(m) \tag{1}$$

かつ

$$D(0) < C(N) \tag{2}$$

式 (1) は，個人が協力を選択したときに得られる利得は，非協力を選択したときに得られる利得よりもつねに少ないことを表す．このため，他者との関係において，利得を最大化しようとすると，個人は非協力を選択することになる．しかし，式 (2) は，全員が協力を選択する状況での個人の利得は全員が非協力であるときの利得よりも大きいことを示す．ここに，個人の選択が社会としては望ましくない状況がおき，社会的ジレンマと称される状況となる．

表 1　社会的ジレンマの類型化
Table 1　Type of social dilemma.

	社会的トラップ	社会的フェンス
環境から何かを取る	資源管理問題 （「共有地の悲劇」）	環境汚染物質の除去
環境に何かを投入する	環境汚染 （負の公共財の共有）	集合財（公共財）の供給

社会的ジレンマ状況は，**表 1** に示すように類型化される[8)]．表 1 で，環境とは社会的ジレンマ状況が発生する対象の環境をいう．社会的トラップは，合理的な選択を取り続けていると社会的な “わな” にはまってしまうこと．社会的フェンスは，合理的な選択を取り続けていると目標を達成することが困難であるような状況をそれぞれ指す．牛飼いが個人の利得のみを追求した結果，放牧地が荒廃してしまうことを取り上げた共有地の悲劇[2)] や，公共財の供給問題は，それぞれ社会的トラップや社会的フェンスととらえられている．

個人による情報セキュリティ対策を，ウイルスや悪性プログラムであるマルウエアなどによって汚染されたネットワーク環境への協力行動であると想定し，環境配慮行動を援用し，このような状況を社会的ジレンマ状況ととらえようとする試みは，文献 6) で報告されている．本論文では，情報セキュリティ対策に類似した “環境汚染物質の除去” についての定式化を紹介する[8)]．

集団の成員が共有している環境が汚染されているとき，コストをかけて汚染物質を取り除

くことを協力とし，何もしないことを非協力とする．このときの利得関数は，全員が非協力を選択している状態を初期状態とし，以下で表される（文献 8) で記述されている記号をそのまま用いた）．

$$C(m) = D(0) + \gamma(m) - \delta(m) \qquad (1 \leqq m \leqq N) \tag{3}$$

$$D(m) = D(0) + \gamma(m) \qquad (0 \leqq m \leqq N-1) \tag{4}$$

ただし，$\gamma(m)$ は，m 人が協力行動をした場合に，集団の成員 1 人ひとりが受ける正の外部性の大きさを表す関数（$\gamma(m) \geqq 0$，$\gamma(0) = 0$）である．なお，外部性とは経済活動における意思決定が市場を通さずに他の経済主体へ影響を及ぼすことをいう．$\delta(m)$ は，協力行動を m 人がした場合に，それぞれ負担するコストの大きさを表す（$\delta(m) > 0$）．

経済学では，インターネットのように，財の排除性がなく，競合的でない財である公共財を実現するために，集団の成員がコストを負担し協力しなければならない状況において，フリーライダ（ただのり）とよばれる問題が生じることが知られている．フリーライダとは公共財を実現する目標があるとき，他者のコスト負担により，自分自身は協力しなくても，その恩恵により自分も利得を得ている個人を指す．これも，社会的ジレンマ状況を表すといわれる．

2.2　意思決定における誘因値

個人が協力行動・非協力行動をとったときのそれぞれの利得を表したが，合理的選択理論によれば，集団における成員が，協力か非協力を選択するための誘因は，それぞれの利得の差によって表すことができる．木村は，「集団の目標とする集合財の供給が集団規模が大きいと実現されにくい」というオルソン問題を社会的ジレンマの現象の 1 つとしてそのモデル化を試みているが，その中で，意思決定における誘因値を以下に示すように定義している[7]．

自分が協力すると協力者が m 人になるとしたとき，利用者が協力行動を選択する誘因値 $t(m)$ は以下で表される．

$$t(m) = D(m-1) - C(m) \tag{5}$$

$t(m) < 0$ であれば，協力行動のほうが，非協力行動よりも利得が大きいことを表す．したがって，協力行動をとる．$t(m) = 0$ であれば，特に行動を起こさない初期状況のままとする．$t(m) > 0$ であれば非協力行動のほうが協力行動よりも利得が大きいことを表す．したがって非協力行動をとる．

2.3　社会調査による認知状況についての実証研究

次に，個人の認知の観点から社会的ジレンマ状況を定義しようとする試みについて述べる．2005 年海野ら[12] は，国内 3 つの市の住民に対する「家庭廃棄物（ごみ）に関する住民の意識と行動による調査」を実施し 1,772 名の回答を得て，社会的ジレンマ状況を社会調査によって定義する研究を実施した．この調査は社会的ジレンマ状況の社会調査として知られている．ごみの分別廃棄が，各家庭にとって手間がかかるものであるが，社会全体としては，分別廃棄をすることによって，環境資源の節約になる，という状況を想定して実施されたものである．調査では住民がごみの分別廃棄についてどのように認知しているかを，以下の 3 つの認知要素を定義し認知の状況を類型化し，これらの関係を分析している．

1. コスト性
2. 危機性
3. 無効性

上記 1. のコスト性とは，ドウズの a）に対応し，協力行動にコストがともなうという性質である．2. の危機性とは，b）に対応し，社会の構成員がコスト回避行動すなわち非協力行動を選択した場合，社会構成員にとって望ましくない状態をもたらすという性質をいう．3. 無効性とは個人の協力行動が社会状態に及ぼす結果は無限に小さいという性質で，海野らによって追加された．3 つの認知要素によって認知状況を類型化すると，ごみの分別廃棄問題を社会的ジレンマ状況ととらえている人は，全体の 1 割強で，大多数の人にとって状況は社会的ジレンマ状況ではないという結果が示された．この調査において，対象となる現象は，社会的ジレンマ状況として可能性がある状況であるが，実際は異なる状況である可能性もあることを示し，なんらかの社会的仕組みなどにより，社会的ジレンマ状況を解決する手段がすでに社会に存在する可能性があることを示している．海野らは，このような社会的ジレンマ状況への解決の手段をも含めて社会的ジレンマ状況を研究すべき，ということを主張する．また，POSA（部分尺度分析：Partial Order Scalogram Analysis）による分析を試みて，個人がどの認知要素をどのような順序で獲得するかを分析し，危機感，有効感（無効感の反対）の順に獲得し，コスト感を脱却するとき，環境配慮行動を行う傾向が大きくなることを示した．また，海野らは社会的ジレンマ状況について，社会調査の方法を論じている[18]．これによると，社会調査における認知状況を研究した他の研究のうち，オランダのペリカーン，長谷川の調査は，認知要素については他人との行動を与件として行動意図と選好を尋ねるものとして紹介されている．

2.4　社会的ジレンマ状況の解決

これまで述べたように，社会的ジレンマ状況は，大きく 2 つの領域にて研究されている．1 つは，個人の選択誘因と社会全体の利得の観点からで，もう一方は個人の認知の状況を明らかにすることである．このような社会的ジレンマ状況を解決するということは，協力行動の選択率（協力率）を上げることである．これには，やはり 2 つのアプローチがあると考え

られている[15]．1つは，「構造的解決」で，なんらかの形でジレンマの構造を変化させジレンマそのものを解消させることである．2.2節で述べたような，個人を協力行動へ誘因する誘因関数を定義し，個人と社会の利得構造を解明してその構造を変化させることは，構造的解決のうちの1つである．もう一方は，「個人の認知の解決」である．2.3節で述べたような個人の認知の構造を解明し，その状況を変化させることにより協力行動を選択する集団を増やすことである．個人の選好は，リスクに直面したときとそうでないときで，同じ価値でも異なる選好傾向があるとするプロスペクト理論[13]や，協力行動をとる際に，他者の協力の程度に影響され協力率が変化するといった研究がある[15]．

3. 情報セキュリティ対策と社会的ジレンマ状況

本章では，情報セキュリティ対策の状況について述べ，社会的ジレンマ状況と想定した理由を，2章で述べた関連研究による定義を参照して述べる．また，情報セキュリティ対策における個人の利得の構造と認知の構造について，関連研究をもとに定義する．次に，社会的ジレンマ状況という観点から情報セキュリティ対策を見たときの仮説を設定し，これを実証するための質問紙調査についての概要と結果を述べる．

3.1 情報セキュリティ対策の状況

最近では，新聞などのマスメディアやISPなどは，情報セキュリティ対策が利用者にとって安全にネットワークを使用するために必要であると積極的に注意喚起するようになった[16]．しかし，対策を怠ったことによるセキュリティ事故は延々として発生し続けている．日本ネットワークセキュリティ協会の調査によれば，2009年上半期のインシデント件数は，2008年の1,373件に対して1,528件と予想されている[17]．ここで，個人にとって情報セキュリティ対策をとることがどのような状況であるかを考えてみる．対策ソフトの購入や設定など，費用や手間がかかることが必要であり，一方で自分にセキュリティ対策をしないことで本当に不便や障害が起きるかを想像しにくい状況かもしれない．あるいは，自分だけ対策をとらなくても，それほどネットワークの安全性への影響はないと思っているかもしれない．このように個人が自己の手間などの“コスト”を優先して対策をしなければ，ネットワークには脅威による障害が増加してしまい，その結果，ネットワークに被害が蔓延し，ネットワークの品質が低下することとなり，個人がネットワークから受ける利益が低下し，ネットワーク全体として“安全な”ネットワークを実現できない状況ではないかと考える．情報セキュリティ対策は，対策を迫られる個人にとって合理的であると考えられる選択が，その個人が利用するネットワーク全体にとって最適でない状況ではないだろうか．このような状況は，

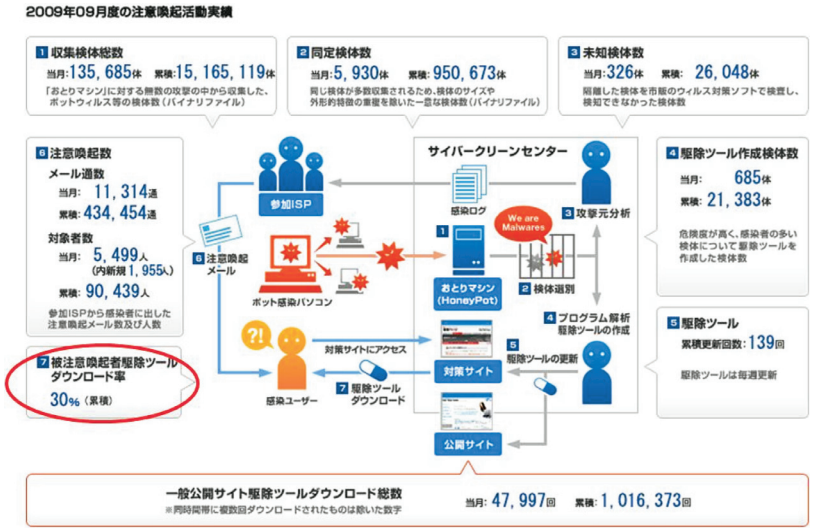

図1　CCCのボット対策事業 [https://www.ccc.go.jp/report/200909/0909monthly.html] より引用
Fig. 1　Anti-Bot countermeasures project.

2.2節表1で述べた社会的ジレンマ状況の類型のうち「社会的フェンス」と見なすことができる．なお，本論文で“ネットワーク”とは，インターネットやインターネットを介して構築したシステムを含めた1つの共同体としての社会システムをさす．

3.2 ボット対策事業への適用

ボットウイルスとは，コンピュータを悪用することを目的に作られた悪性プログラムで，コンピュータに感染すると，インターネットを通じて悪意を持った攻撃者が，感染したコンピュータを外部から遠隔操作し，インターネットの他の利用者へ迷惑メールや攻撃することが知られている[14]．このため，利用者は自分自身への被害を認知することなく，ネットワーク全体へ被害を引き起こしているという状況が想定される．CCCでは，ISPの協力を得て，ボット感染利用者に対して注意喚起メールを送付し，駆除ツールをCCCのサイトで提供している．感染を知らされた利用者は，駆除ツールをダウンロードし，自己のPCにインストールして対策をとることが期待される（**図1**）．この活動は，効果をあげており，世界的に見れば相対的に日本がボットウイルスへの感染が低いという結果を表している．ただし，CCCでの注意喚起における個人の対策実施の現状は，クリーナとよばれる対策ツール

をダウンロードしたユーザは，年間を通じて約 30%の低さにとどまっており，この値をさらに向上させることが望ましい．

ボット対策を迫られた，感染を知らされた個人がなぜ 30%という低い割合でしか対策を実行しようとしないのか．駆除ツールをダウンロードし利用者の PC に設定することは，手間が生じると考えられる．他方，駆除ツールをダウンロードせず対策をとらずにいることは手間はかからないが，現状の利得をそのまま受けられる．しかし将来ネットワークの安全性が低くなり，現状の利得も受けられなくなることが想定できる．この状況も社会的フェンスといえるのではないかと考える．

本研究では，情報セキュリティ対策の状況が，社会的ジレンマ状況として説明できるかを考察するために，ボット対策事業を実証対象とし，まず個人の利得構造や認知構造をモデル化し，実証のための質問紙調査を実施することとした．

3.3　情報セキュリティ対策における利得構造モデル

情報セキュリティ対策を社会的ジレンマ状況とした場合の，解決のための 2 つの方策のうち，構造的解決のための利得の構造について，まず，ネットワークの利用者が情報セキュリティ対策を迫られた場合の，対策コスト，得られる利得などを用いて，対策実施のための誘因関数を導く．次にフリーライダの存在について述べる．

3.3.1　情報セキュリティ対策実施のための誘因関数

N 人からなるネットワークにおけるネットワーク利用者の集団（$N \geqq 3$）があるとする．だれも情報セキュリティ対策を実施していない状況を初期状態とすると，情報セキュリティ対策を実施すると，ネットワーク利用者にはなんらかの利得が得られるとする．この場合，利得とは，金銭的な利得だけでなく，利便性なども含む．ネットワークにとっては，利用者が情報セキュリティ対策をとることがネットワークを安全に提供できることである．ここで，情報セキュリティ対策を実施することを「協力」行動とし，対策をとらないままでいることを「非協力」行動とする．

今，協力者の数を m 人とすると（$0 \leqq m \leqq N-1$），協力者と非協力者の利得をそれぞれ，$C(m)$，$D(m)$ で表す．また，ネットワーク利用者は，初期状態において，全員が一定の値 B（$D(0)=B$，$B \geqq 0$）の利得を受けている状態とする．また，対策をとるコストを一定とし，K（$K>0$）とする．

だれも協力しない初期状態から，情報セキュリティ対策を実施することを迫られ，m 人が協力行動をとったとする．このとき，式 (3)，(4) に，情報セキュリティ対策の状況を適用すると，以下の式 (6)，(7) がいえる．

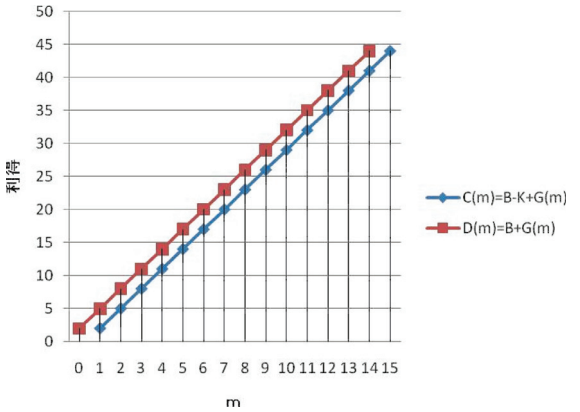

図 2　$C(m)$ と $D(m)$（$N=15$，$B=0$，$K=3$，ただし，$G(m)$ は，式 (10) から，$G(m)=G(1)+(m-1)K$ としたとき）
Fig. 2　$C(m)$ and $D(m)$ ($N=15$, $B=0$, $K=3$, when $G(m)=G(1)+(m-1)K$).

$$C(m) = B - K + G(m) \tag{6}$$

$$D(m) = B + G(m) \tag{7}$$

ただし，$G(m)$ は，m 人が協力を選択した場合に，ネットワーク利用者 1 人ひとりが受ける利得の増分を表す関数とする（$G(m) \geqq 0$，$G(0)=0$）．

m 人が協力した場合の 1 人あたりの式 (5) で示される誘因値は，以下の式 (8) となり，個人は，この値によって，協力行動を選択するか否かを判断する．

$$t(m) = G(m) - G(m-1) - K \tag{8}$$

すべての 1 以上の m について，$t(m)>0$ である協力行動をとる場合は，以下が成り立つ．

$$G(m) - G(m-1) > K \tag{9}$$

$$G(m) - G(1) > (m-1)K$$

$$G(m) > G(1) + (m-1)K \tag{10}$$

図 2 に，$C(m)$，$D(m)$ を表した．セキュリティ対策を迫られた個人にとって，誘因値がどのような値になっているか，その誘因値と選択行動の関連についてを調査すれば，協力率を上げるための要因を分析することができる．

3.3.2　フリーライダの状況と脅威の理解

情報セキュリティ対策の状況において，フリーライダの存在について検討する．フリーライダは，コストのかかる協力をとらず，他者の協力による恩恵を受け，非協力のままでいる

利用者をさす．自己が協力しなくても，利得を受けられる構造である．式 (6)，(7) で式 (1) が成り立つ状況であるから，以下で表される．

$$G(m) - G(m-1) < K \tag{11}$$

m 人が協力したときの利得から $m-1$ 人が協力したときの利得の差がコストよりも小さいときである．これは，誘因値 $t(m) < 0$ を示している．つまり，協力の誘因値があるが，協力しない個人をフリーライダと見なせる．

また，情報セキュリティ対策の状況では，個人が情報セキュリティ対策のリスクを理解する程度が，既存研究のゴミの分別行動などとは異なる．たとえば，個人は，環境問題の影響をマスコミや映像で見る機会が多く，被害の状況や対策の効果を知る機会が多い．しかし，情報セキュリティの場合は，近辺に被害者が存在することは少なく，その状況を理解する機会は明らかに低い．セキュリティ対策の効果や脅威について理解していなければ，（経済）合理的な判断ができない，と考えられる．しかし，理解度が高い場合は，合理的な判断が可能で，フリーライダになる可能性もある．したがって，協力誘因があっても協力をしないもの，また情報セキュリティにおける脅威の理解が行動にどのような影響があるかの状況について調査し，フリーライダの存在を説明することができるか，を調査する．

3.4　情報セキュリティ対策における認知の状況

次に，社会的ジレンマ状況を解決する 2 点目の方策である「個人の認知構造を変化させる」ためには，「個人の認知」の状況を知らなければならない．大規模な社会調査を実施したこと，ごみの分別問題という情報セキュリティに類似した対象について調査したもの，という理由から 2.3 節で述べた環境配慮行動の「ゴミの分別」行動について調査した既存研究[12] で使用した認知要素の調査を参考とする．ただし，本論文では，社会的ジレンマ状況の定義により，個人と社会との関連が重要であるとの考えから，既存研究における認知の 3 要素の「危機性」について，社会と個人の区別がつきにくいため，新たに個人への危機性か社会を構成する他人への危機性かの区別をつけた．したがって，認知要素として，「コスト性」，「危機性（個人）」，「危機性（他人）」，「無効性」の 4 つを考えた．これらの認知要素が，個人が情報セキュリティ対策を迫られる状況におかれたときどのような状況であるかを調査する．

3.5　質問紙調査と仮説

CCC のボット対策事業における注意喚起メールを受けたユーザの対策の低さを説明するために，ボット対策状況が社会的ジレンマ状況ではないかという仮定する．すでに述べたように，情報セキュリティ対策が，インターネットという公共財的な財を対象とし，社会的ジレンマ状況の類型の 1 つである，社会的フェンスの状況に類似しているからである．社会的ジレンマ状況を解決するためには，利得構造と認知構造を知らなければならない．そのためには，現実にボット感染した利用者に直接質問することが最も効果的であるが，統計処理する対象数を確保することが困難であることや，ボット感染を検知された利用者への直接の接触は，通信の秘密を守らなければならないという法制度上制限されていることもあり，調査手法は，インターネットのアンケートモニタに対する質問紙調査とした．質問紙調査では，ボット感染をしたという一律の状況を想定した状況に回答者をおくことが可能である．この方法は，モニタを利用したことから，一般市民や一般ユーザを対象としたことにはならないことに留意が必要である．

調査にあたって，以下の仮説をたてた．

［仮説 1］　CCC のボット対策事業の低い対策率を考慮すると，ボット対策は，個人にとっては手間がかかり，得る利得は手間に比較すると少ない．したがって，対策しない個人が多く，誘因値は非協力を示す．本仮説が検証されれば，利得構造上，ボット対策事業の状況は社会的ジレンマ状況であることが分かる．また，分析において，誘因値に依存した対策実行意図を持つ状況であることが分かるからボット対策を向上させるには，コストや利得で表される誘因値を制御することによって協力率を上げることができる．

［仮説 2］　利用者は，協力誘因があったとしても，手間を嫌がり，フリーライダとなる．また，このような利用者はボットの脅威について理解度が高い．本仮説が検証され，フリーライダの存在が明らかになれば，利得構造を制御しても，協力しないグループが存在することを意味する．誘因値によって協力率を向上させる場合の効果の限度を知ることができる．

［仮説 3］　4 つの認知要素による認知タイプは，「協力行動にコストを感じ」，「自分に危機性を持たない」が，「他人に危機性を感じ」「協力行動には無効感がある」の社会的ジレンマ状況である．この認知タイプの回答者は，情報セキュリティ対策実行の意図を持つ割合が低い．本仮説が検証されれば，現実の CCC における対策状況を説明することができる．なお，本仮説を検証する調査において，認知要素と対策実行意図との関係を分析することができ，協力率を上げるためにどの認知要素を獲得すれば，協力行動に態度を変容させることができるかも明らかにすることができる．

3.6　質問紙の設計

3.6.1　質問の流れ

回答者がおかれている状況を，CCC が実施しているボット対策に近づけるため，注意喚起メールを利用者に送付したと想定し，そのメールに対する個人の意識や行動について設問

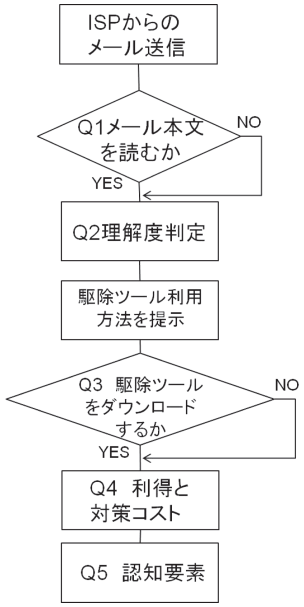

図 3　質問紙構成，手順
Fig. 3　Flow of questionnaire.

した．質問紙の構成を**図 3** に示す．

以下に設問順を示す．

- 注意喚起メールを受信した場合にメールを読むか，読まないか（Q1）．
- 注意喚起メールを読んだ後に，メールで書かれた内容について，3 問のクイズを出す．正解数によって，理解度を 0（正解数 0）〜3（正解数 3）の 4 段階に分類した（Q2）．
- 駆除ツール利用手順を提示した後，ボット駆除対策ツールをダウンロードするつまり対策を実施するか対策実行意図を問う（Q3）．
- 個人が対策をとることへのコスト感と，対策をとらないでいる場合の利得を，それぞれ現在のインターネットから得ている利益を 100 として（Q4）問う．
- 2.3 節で述べた社会的ジレンマ状況に対する 4 つの認知要素（コスト感，危機感（自分），危機感（他人），無効感）（Q5）を，4 件法により質問した．4 章以降の調査分析においては，はい，いいえの 2 件のデータのみを利用している．2 件法でなく 4 件法にした理由は多くの情報を収集することで他の分析に利用することの可能性を残しておいたからである．

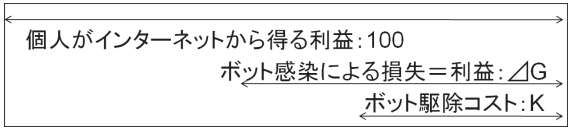

図 4　想定した ΔG と K
Fig. 4　Assumed ΔG, K.

Q2，Q3 は注意喚起メールを読んだ回答者に対して聞く．設問本文は付録を参照のこと．

3.6.2　利得と対策コスト

回答者に，駆除ツール対策手順を提示した後，その対策のコストとボット対策をすることによって得られる利益を Q4 で質問した．ボットは，3.2 節で述べたように，PC 利用者はその被害を認知することが困難であるため，対策した結果の利得を実感できないことが多い．このため，逆説的に損失として質問した．回答者がインターネットから得る利益を 100 として，利得構造は，インターネット全体の利得を 100 と仮定し，**図 4** に示すような構造を想定した．これらの値は，式 (8) で表される協力行動である情報セキュリティ対策実行に対する誘因値を算出するために使用する．

3.7　調 査 結 果

調査は，Goo リサーチを利用したインターネット調査で行った．アンケートに先立ち，アンケート項目についての妥当性を検討するためフォーカスグループによる事前アンケートを実施した．調査期間は，3/19〜3/24 で，総回答数は 5,136 であった．収集データは，年代別，男女別に均等割付けとしている．

3.7.1　注意喚起メールとその理解度

注意喚起メールを読むと答えた回答者は，5,136 人中 4,164 人であった．注意喚起メールを読んだ回答者のうち，理解度 0，1，2，3 は，それぞれ 1,743 人，78 人，1,900 人，447 人であった．

3.7.2　利 得 構 造

誘因値を算出する対象とした回答者は，注意喚起メールを読むとしたもののうち，図 4 で示した利得構造を満足するものを抽出した．現在の利益を 100 としているとき，感染による損失（ボット対策をすることによる利益）が現状の 100 以上であるものを除いた．そのうえで，コストを過大に回答したものをはずれ値として除外し，全体の回答のうち 3,714 を

有効回答とした．協力行動をとる必要十分条件は，協力者が $m-1$ 人から m 人になったとき，すなわち 1 人分の利得の増分がコストより大きいときである．したがって，誘因値は，Q4 で得た個人の利得の増分（ΔG）とコスト（K）の差である．**図 5** に誘因値の分布を示した．あきらかに，誘因値ゼロの場合が突出しており，特異点と考えられる．

3.7.3　認知の状況

メールを読むと答えたもののうち，認知の 4 つの要素について集計したものを**表 2** に示す．コスト感，危機感（自己）に対しては，肯定するものが多いが，危機感（他人），無効感については否定的である傾向があることを示している．

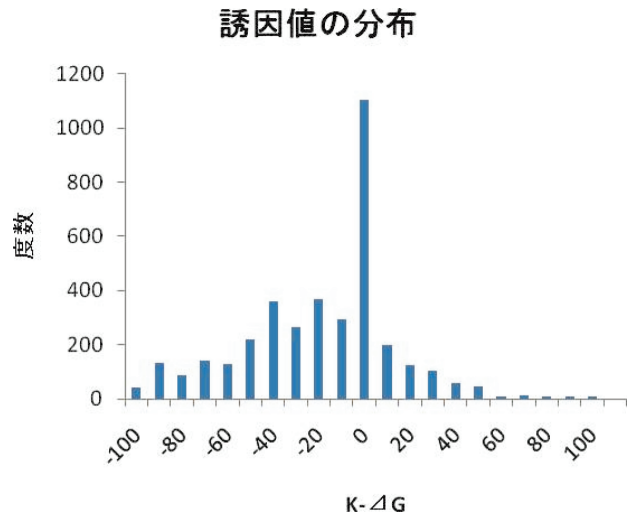

図 5　誘因値の度数分布
Fig. 5　Histgram of incentive value.

表 2　認知要素の調査結果
Table 2　Result of cognitive elements.

認知の程度(n=4164)	コスト感	危機感（自己）	危機感（他人）	無効感
そう思う	1169	1779	167	157
どちらかといえばそう思う	1841	1799	860	891
どちらかといえばそう思わない	647	496	1753	1685
そう思わない	507	90	1384	1431

3.7.4　実 行 意 図

メールを読んだ回答者に対し，対策手順を提示し，指定された対策を実施するかとの問いに，実施すると回答したのは 3,254 人，実施しないと回答したのは 910 人で，それぞれ 78%，22%であり，実際の CCC の事業における対策率 30%とは異なる結果となった．

4.　分析と考察

質問紙調査で得た結果に基づいて，利得構造と認知の状況について分析し考察する．

4.1　利 得 構 造

表 3 に，ΔG，K，誘因値 t（$\Delta G - K$）の平均値，中央値，最頻値と対策実行意図あり（C），なし（D）の割合を理解度別に示す．図 5 に示すように誘因値 t は正規分布ではないため，代表値として中央値を見る．まず，誘因値 t は，-10 であり協力行動への誘因があることを示している．この場合の実行意図あり，なしの全体における比率は，それぞれ 0.78 と 0.22 であり，高い比率で協力行動をとると回答しており，誘因値と整合する．次に，誘因値は，ゼロの特異点があることから，ゼロとそれ以外のデータを分類して分析した．その度数と平均値，中央値，最頻値と協力（C），非協力（D）の分布を**表 4** に示す．これによ

表 3　誘因値と理解度，協力/非協力行動割合
Table 3　Incentive value, understanding level and rate of C/D.

	全体			理解度0			理解度1			理解度2			理解度3		
	3714			1580			69			1682			383		
	平均	中央値	最頻値	平均	中央値	最頻値	平均	中央値	最頻値	平均	中央値	最頻値	平均	中央値	最頻値
⊿G	52.66	50.00	50.00	50.60	50.00	50.00	56.65	50.00	50.00	53.76	50.00	50.00	55.63	50.00	50.00
K	33.49	30.00	50.00	35.10	30.00	50.00	37.28	30.00	30.00	32.67	30.00	50.00	29.81	20.00	10.00
t	−19.17	−10.00	0.00	−15.50	−9.00	0.00	−19.38	−10.00	0.00	−21.09	−15.00	0.00	−25.81	−20.00	0.00
C	0.78			0.70			0.78			0.82			0.90		
D	0.22			0.30			0.22			0.18			0.10		

⊿G: 利得, K:対策コスト, t:誘因値, C:協力者割合 D:非協力者割合

表 4　誘因値 0 を境界とした協力・非協力率
Table 4　Rate of C/D on incentive value of 0 boundary.

K−⊿G		全体			t<0			t=0			t>0		
	n	3714			2131			1007			576		
	平均値	−19.17			−40.71			0			27.01		
	中央値	−10			−40			0			20		
	最頻値	0			−20			0			10		
		度数	割合	平均値	度数	割合	平均値	度数	割合	平均値	度数	割合	平均値
	C	2885	0.78	−21.8	1769	0.83	−41.31	720	0.71	0	396	0.69	25.86
	D	831	0.22	−10.3	362	0.17	−37.76	287	0.29	0	180	0.31	29.51

t:誘因値, C:協力者 D: 非協力者

表 5　誘因値と認知要素との関係
Table 5　Relation of incentive value and cognitive element.

	危機感（自己）		危機感（他人）		有効感		非コスト感	
	あり	なし	あり	なし	あり	なし	あり	なし
度数	3165	549	963	2751	2720	994	998	2716
t 平均値	−21.04	−8.41	−9.03	−22.72	−22.52	−9.99	−29.71	−15.30

全体n=3714

表 6　誘因値と認知要素との数量化 1 類の結果
Table 6　Result of quantification theory type 1 on incentive value and cognitive element.

	レンジ	単相関	偏相関
非コスト感	12.5594	0.1892	0.1659
危機感（自己）	7.7568	0.1328	0.0785
危機感（他人）	7.0413	0.1778	0.0721
有効感	4.2139	0.1644	0.0436

重相関係数	0.2596
重相関係数の2乗	0.0674

れば，全体で，協力（C），非協力（D）とした回答者の誘因値は，それぞれ −21.8，−10.3 と大きな差がついていることが分かる．また，誘因値が 0 以下，すなわち合理的選択理論に従えば，協力（C）をとるはずのグループの誘因値の平均は，C で −41.31，D で −37.76 である．一方，誘因値 (t) が 0 以上のグループの誘因値の平均は，C で 25.86，D で 29.51 となった．誘因値 (t) < 0 のグループは，相対的に協力傾向があり，また誘因値 (t) > 0 のグループは相対的に協力傾向が低いことを表し，誘因値と整合している．誘因値 ($t = 0$) のグループは，初期状態，すなわち非協力状態であるのが自然であると考えられるが，特に D が高い値を示してはいない．次に，認知の 4 要素が誘因値にどのような影響を持つかを分析する．**表 5** に認知の 4 要素と誘因値の平均値を示す．“非コスト感がある” すなわち対策にコストを感じないグループが最も誘因値の平均が低く，協力への誘因が高い．さらに，誘因値に認知要素がどのように関連するかを見るために，数量データである誘因値に対して数量化 1 類によって分析した．その結果を**表 6** に示す．重相関係数の 2 乗である決定係数が 0.0674 と低く，その結果を採用することは困難であるが，4 要素のうち誘因値に対して最も貢献している要素は，コスト感である可能性を示している．

以上をまとめると，ボット対策を想定した調査では，回答者の意識は対策コストよりも利得が上回り対策を実行する意図が高い傾向を示す．ボット対策の状況は，個人の誘因値が低く協力率が低い傾向にあるという仮説 1 は却下された．ただし，個人が意思決定する際に，利得関数から導出する誘因値の状況に整合することが分かった．すなわち情報セキュリティ対策の推進には，個人が対策するためのコストとしての手間などを減らし，コストよりも対策をすることで得られる利得を大きくすることが効果的である．また，誘因値 0 については，以下のように考える．誘因値 0 が意味するのは，ボット対策をとることの利得とコストが等しいということである．今回の調査では，対策をとることを損失で聞いているため，対策コストが損失値と同じ，とする回答者が多かった（27%）．個人は，損失値を認識した場合，その対策コストと損失値（対策による利益）を区別して考えにくい傾向があり，その値を同値としたのではないかと考える．

4.1.1　フリーライダの存在

仮説 2 の，フリーライダの存在が認められる状況を確かめるために，理解度別の誘因値と実行意図との関係を表 3 で見る．理解度が高くなると，実行意図の割合も明らかに多い．理解度と実行意図との相関係数を算出したところ 0.17 であり，弱い相関が認められた．理解度を高めることが実行意図を高めることにつながる．また表 4 より，協力行動への誘因がある，$t < 0$ のグループの協力率は，他グループと比較し高い．このことから，他の $t = 0$，$t > 0$ と比較して，特にフリーライダの存在が多いとは認められない．理解度が高い場合も協力率が高いので，フリーライダの存在の根拠とはならない．ただし，$t < 0$ のうち非協力を選択した 17%がフリーライダでない，と断言はできないため，仮説 2 のフリーライダの存在を検証することはできなかった．

4.2　認知要素と実行意図の関係

4.2.1　認知要素の類型化と実行意図

社会的ジレンマ状況の 4 つの認知要素について，4 件法で質問したが，その回答の「そう思う」「どちらかといえばそう思う」を 1，「どちらかといえばそう思わない」「そう思わない」を 0 として，各要素を表す．この認知要素の状況は，16 のタイプに分類できる．認知要素の 16 のタイプと，それぞれの全体における割合，それぞれの実行意図ありの割合を**表 7** に示す．このとき，タイプの分け方として，能動的なタイプを基準として分けることとし，認知要素の「無効感」は「有効感」，「コスト感」は非コスト感として表現している．なお，認知要素については，アンケートで ISP からのメールを読まない回答者を除いており，そのため標本数は 4,164 である．

表 7 より，以下のことがいえる．

- 最も大きな割合であるのは，タイプ 4 で，43.6%である．自己危機感，他人危機感，有効感があり，コスト感を感じるタイプであった（順に○○○×）．次に，タイプ 3 の

表 7　社会的ジレンマの 4 要素の認知タイプと実行意図の割合
Table 7　Recognitive types and rate of coorperation.

タイプ	危機感 :自己	危機感 :他人	有効感	非コスト感	全体の割合%	実行意図 %
言語表現	自分に被害が及ぶ	他人に被害が及ぶ	有効である	手間がかからない		
1	○	○	×	○	1.3	80.8
2	○	○	×	×	4.5	76.1
3	○	○	○	○	20.7	91.7
4	○	○	○	×	43.6	83.3
5	○	×	×	○	1.4	78.9
6	○	×	×	×	9.0	67.1
7	○	×	○	○	1.2	75.5
8	○	×	○	×	4.5	47.6
9	×	○	○	○	1.9	69.2
10	×	○	○	×	2.6	72.0
11	×	○	×	○	0.3	76.9
12	×	○	×	×	1.0	43.9
13	×	×	○	○	0.2	80.0
14	×	×	○	×	0.8	53.1
15	×	×	×	○	1.0	47.6
16	×	×	×	×	5.9	37.2

20.7%であり，タイプ 4 との違いは，コストを感じない，である．

- 社会的ジレンマ状況であるとされる，タイプ 12（自己に被害が及ばず，他人に被害が及び，対策の効果は有効でなく，コストを感じる）割合はわずか 1.0%である．情報セキュリティ対策の認知状況が社会的ジレンマであるという仮説 3 は却下された．
- 最も実行意図が高いタイプは，すべての認知要素を保持しているタイプ 3（自己危機感，他人危機感，有効感，コスト感がない）で，全体の割合は 20.7%であるが，実行意図は最も高く，91.7%である．
- 最も実行意図が低いタイプは，すべての認知要素を保持していないタイプ 16（自己危機感なし，他人危機感なし，有効感なし，コストを感じる）で，37.2%であり，次に低いのは，社会的ジレンマタイプの 12 である．したがって，ジレンマ状況にある回答者は実行意図が低い傾向にあるといえる．

表 8　実行意図と 4 要素の二項ロジスティック回帰分析結果
Table 8　Result of regression analysis on intention.

従属変数:	実行意図（1=実行意図あり）
独立変数	B
切片	−0.58***
性別（男=1, 女=0）	0.12
年齢	0.00
危機感（自己）（1=危機感あり）	1.13***
危機感（他人）（1=危機感あり）	0.45***
有効感（1=有効感あり）	0.56***
非コスト感（1=コスト感なし）	0.63***
pseud-R^2	.15
N	4164

† p<.10 *p<.05 ** p<.01 ***p<.001

4.2.2　認知要素の実行意図へ与える影響

次に，従属変数である実行意図があり，なしの 2 値であり，認知要素である独立変数のどの要素が実行意図に大きな影響を与えているかを分析するために，2 項ロジスティック回帰分析を行った．求めた結果を**表 8** に示す．

これによると，危機感（自己）が，他の認知要素に比較して最も実行意図に高い影響を与えていることが分かる．危機感（自己）に続き実行意図に高い影響を与える要素は，非コスト感，有効感，危機感（他人）であった．また，各要素について，交互作用は見られなかった．

4.2.3　認知要素獲得の順序について

各認知要素に注目し，探索的な手法である POSA（部分尺度分析：Partial Order Scalogram Analysis）による分析を試みる．POSA は，ゴミ分別行動を対象とした社会的ジレンマの認知構造の分析でも使用されているが[12]，ある対象に対して（本調査の場合は，回答者）セキュリティ対策意図の有無について問われているなかで，各認知要素が累積的な関係を持つかを明らかにすることができる．認知要素間で類似しているものを近くに配し，認知要素間の並びを設定する．認知要素間の類似性を決める手法として，数量化 III 類を利用して要素間の類似度を調べる方法や，連関係数を使用するが，類似性の高い認知要素ほど獲得順も近くなると思われるため，認知要素の獲得の順番を図示する POSA の中での提示順をジャッカード係数によって決めた[10]．ジャッカード係数は，集合の類似度を測るのに使われ，2 変数 A，B があるとき，以下で表される．2 変数が同時に発生する度数 $a \times b$，2 変数のうち A だけが発生する度数を a，B だけが発生する度数を b とすると，

表 9　各認知要素間のジャッカード係数
Table 9　Jaccard coefficient of each cognitive element.

	(X,Y)	(X,Z)	(X,W)	(Y,Z)	(Y,W)	(Z,W)
ジャッカード係数	0.76	0.76	0.27	0.83	0.30	0.30

X:危機感（自己），Y：危機感（他人），Z:有効感，W:非コスト感

ジャッカード係数は，以下である．

ジャッカード係数：　$a \times b/\{(a \times b) + a + b\}$

X：危機感（自己），Y：危機感（他人），Z：有効感，W：非コスト感としたとき，それぞれの要素間のジャッカード係数を**表 9** に示す．

数値が大きいほうが類似度が高いから，X，Y，Z，W の順番で POSA を実施する．これは，文献 12) における POSA と同様の順序となる（ただし，文献 12) では，認知要素は 3 種類である）．

次に，POSA による具体的な手順を示す．まず，4 つの各要素のすべてを持たないタイプ 16（0000）から開始し，1 つずつ認知要素を獲得したタイプへ順に進み，最後にすべての要素を持つタイプ 1111 に至る図形を描く．この結果，4 つの認知要素に関するタイプと協力行動の頻度を POSA ダイアグラムに図示すると**図 6** のようになる（$n = 4{,}164$）．各タイプ名の下に記載されている数字は，上段がそのタイプに分類された回答者数と全体の中での比率，下段がそのタイプの回答者の中で協力行動を行う人の数とその比率である．また，POSA は図の描き方により，図中に載らないタイプが 5 つ存在する．そのようなタイプを**表 10** に示す．図 6 中に表現された 11 個のタイプに分類される度数（再現率）は全体の 90.6%であった．また，各タイプに分類される度数から，図の左側のルートに位置するタイプの回答者が多いことが分かる．つまり，認知要素の獲得の過程に順序性があるとすれば，最も協力行動を行いにくいと考えられるタイプ 6 から最も多く協力行動を行うと考えられるタイプ 3 への経路をつなぐと，タイプ 16 → タイプ 6（「危機感（自己）」の獲得）→ タイプ 2（「危機感（他人）」の獲得）→ タイプ 4（「有効感」の獲得）→ タイプ 3（「非コスト感」の獲得）という経路が最も自然であると考えられる．このルート上に配置される回答者数は全回答者数の 83.7%であり，十分に高いといえる数値であった．

次に，認知タイプによる協力行動の多寡の違いについてであるが，どの認知要素も獲得していないタイプ 16 から 1 つずつ認知要素を獲得するにつれ協力行動を行う回答者は増加し，タイプ 3 では図中で最大の 91.7%になるということが示されている．このルートのタ

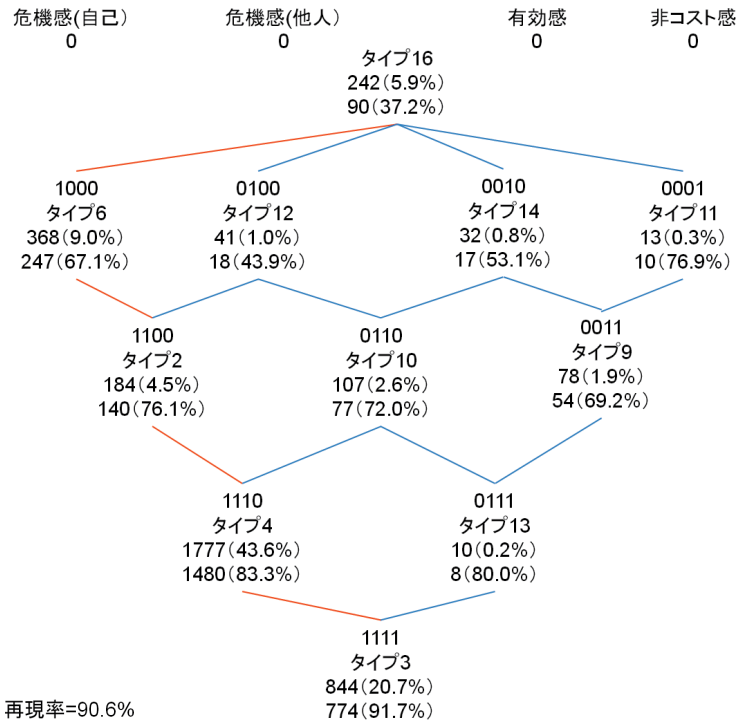

図 6　認知要素の POSA 図
Fig. 6　POSA diagram of cognitive elements.

表 10　POSA に載らなかったタイプ
Table 10　Elements not on POSA diagram.

タイプ	度数	全体の中の比率	「行う」人の度数	「行う」人の比率
1	52	1.3	42	80.8
5	57	1.4	45	78.9
7	47	1.2	41	87.2
8	184	4.5	139	75.5
15	42	1.0	20	47.6

イプ間において，協力行動を行う回答者の増加する割合は，タイプ 16 からタイプ 6 が最も多い．これは，タイプ 6 の「危機感（自己）」を得ることが，このルート上でタイプ 3 へ到達するうえで最も効果的であるといえる．これは，4.2.2 項で示した実行意図と認知要素の関係と整合する．また，先述した最も多くの回答者が配置されている左側のルート上ではこの状況を社会的ジレンマとして認知するタイプは出現しない．しかし，図中に表示されなかったタイプ 7（「危機感（自己）」=○，「危機感（他人）」=×，「有効感」=○，「非コスト感」=○）における協力行動を選択する回答者の比率は全タイプ中 2 番目に高い 87.2%であり，このことから，協力行動を促進させるためだけなら必ずしも「危機感（他人）」を認知している必要はないということも示された．

結果を簡単にまとめると，まず，各認知要素を 1 つずつ獲得していくにつれ，タイプ中の協力行動を意図する者の比率が上昇することが示された．また，本論文であげた 4 つの認知要素に順序性があると仮定すると，「危機感（自己）」→「危機感（他人）」→「有効感」→「非コスト感」の順に獲得されていくことが示されたといえる．

4.3　モデルと調査の妥当性

社会的ジレンマ状況の利得構造を表すモデルのうち，社会的フェンスにおける誘因値をボット対策事業に適用し，協力行動時と非協力行動時の利得関数を定義した．また認知状況を明らかにするために認知要素を調査した．以下にモデルに対応した調査の妥当性について述べる．

4.3.1　利得構造の調査

誘因値に従う合理的選択理論を前提としたモデルでは，すべての個人が，協力者が m であるとき，同一の値の誘因値を前提としている．したがって，調査では，代表値による評価を実施した．しかし，実際には誘因値は個人ごとに相当の違いがあり，代表値による分析では，その実態を説明するには不足があると考える．これについては，5.1.2 項の今後の課題で述べる．

4.3.2　認知構造の調査

既存研究が使用した認知要素を危機感，コスト感，無効感の 3 つから危機感を自己と他人に分類し，4 要素に拡張して質問紙調査に使用した．

本論文は，社会的ジレンマそのものの類型化や適切な認知要素を知るための調査ではなく，情報セキュリティ対策の状況が社会的ジレンマ状況であるかという仮定に対して，その認知の構造を追及するものであることと，情報セキュリティ対策において，他者の状況を知る機会や与えられる機会が少ないであろうと想定した．また，海野らの方式は，ゴミの分別問題を対象としており，情報セキュリティ問題に類似した現象を対象として調査したものであり，認知の観点からも情報セキュリティと類似の要素を持つのではないかと考え，採用した．結果として，自己への危機感が実行意図に高い影響が見られた．社会的ジレンマ状況の既存研究において，社会調査については，すでに述べたように本論文が参考とした条件構成認知類型といわれる海野らの方式のほかに状況選択型類型といわれるオランダのペリカーン，長谷川らの要素がある．状況選択型類型では，他者の状況を与えることによって自己の行動の選好順序を選ぶといった設問方式を使用している．海野らの 3 要素に対して本調査では危機感（他人）の要素を加えたことは，他者の状況についての要素を考慮することであり，この意味では，状況選択型類型の調査とも共通点があると考える．

調査の結果では，ゴミ廃棄物の状況と同様に，認知類型において社会的ジレンマ状況であるタイプは 1 割であり，海野の調査と同様の「社会的ジレンマ状況にない」を追認する結果となった．なお，認知類型においてはタイプ 3，4 に大きな偏りが見られた．この原因として，質問紙調査において，直接的な問いをしているため，問いに対して素直に「はい」と答えてしまう「イエス・テンデンシ」が存在していた可能性がある．質問の回答を確定するためには，類似の質問を設けることや，間接的な質問方式をとるなどをする必要があったと考える．

5.　今後の課題

環境配慮行動に関する既存研究を参考とし，情報セキュリティ対策のボット対策事業を例として，人間が行動を選択する際の基準である利得構造を定義し，質問紙調査による大規模な実証検証を試みた．また，同時に認知構造について，既存研究での認知の要素を拡張したうえで調査した．利得構造と認知構造を同時に調査するような試みは，著者の知る限り，数理社会学など社会的ジレンマ状況を研究する他領域にも例がないものである．以下に今後の課題を述べる．

5.1　利得構造と認知の融合

5.1.1　誘因値の分析と認知要素の分析のまとめ

既存研究における社会的ジレンマ状況の構造的解決については，すべての個人が利得の大小による合理的な選択をとる，という前提で定式化されている．利得の定式化は，理論上の定義であり，筆者らの知る限り大規模集団に対する検証はされていない．また，各個人の利得が協力者数 m によってすべての個人が同一であることや，合理的選択理論の前提をおいたうえでの理論である．このため，現実の事象をそのまま説明することは困難であったと考

えられる．今後は，個人の多様性に注目した定式化が必要とされる．また，誘因値が 0 であるケースが多かった現象は注目に値する．個人は，対策することの手間などのコストを，ボット対策をしない場合に認識する損失と同等に見なす傾向がある．このため，対策の手間などを軽減しても，誘因値は変わらないことが想定できる．このようなグループに対しては，誘因値による協力率の向上は効果がなく，他の手法が必要であることが予想される．

認知要素については，以下のように考える．既存研究の認知の要素を援用し，4 つの認知要素を使った調査を実施した．社会的ジレンマ状況にある認知タイプは全体のわずか 1%であり，ほとんどの回答者が社会的ジレンマ状況を認知していないということが分かった．4 つの認知要素のうち，実行意図に最も大きな影響を与えるのは，危機感（自己）であり，また，POSA の分析によって，危機感（他人）はかならずしも，実行意図に必要とは考えられなかった．認知の要素に順序性を仮定すると，認知要素は，危機感（自己）→ 危機感（他人）→ 有効感 → 非コスト感の順を考えることができ，これを獲得順とすると，自己の危機感を獲得することが，実行意図を高くするために重要であることが示された．これらから，「注意喚起メール」にて自己の危機感を喚起することを想定した情報セキュリティ対策が有効であることが考えられる．今後は，個人に恐怖感などを喚起し実行させる脅威認知の理論として，「防護動機理論」を考慮し，この有効性を評価していくことが必要と考える[11]．また，情報セキュリティ対策が対象とした公共財に対する目標については，公共的な「規範意識」や「責任感」などが実行意図に影響を与えるのではないかと考える．4.3.2 項で述べた状況選択型類型の，他者の状況を所与として個人の判断を質問することとともに，「規範意識」や「責任感」を加えた質問で調査することも，有効ではないかと考える．

次に，脅威の理解度であるが，情報セキュリティ対策が他の社会的ジレンマ状況の事例と大きく異なるのは，その脅威の理解度であると考える．本調査では，脅威の理解度が高いほど対策実行意図が高いという結果を得られた．この状況は，意思決定のプロセスのモデルとして，二重プロセスモデルにより説明できる可能性がある．二重プロセスモデルの 1 つの精緻化見込みモデルでは，人間がリスクを判断する際，中心ルートと周辺ルートの 2 通りのプロセスで決定することが確かめられており，リスクの内容を正確に理解できなくても，周辺情報によって判断し実行する，というものである．かならずしも脅威の理解が高くなくても協力行動をとる可能性を示唆している．今後は，調査において，周辺情報といわれる対策指示をした主体への信頼感や自己の経験，情報セキュリティに対する知識の程度などを考慮した調査が必要と考える．

5.1.2　価値評価関数による誘因値と認知要素の融合

本論文では，誘因値と認知要素について，数量化 I 類の分析を実施した．決定係数が低いため，結果として採用はできない．誘因値が各個人のそれぞれの基準に従って評価された結果である，と考えると，実態に適合する誘因値を算出するには，認知要素と誘因値の融合が必要である．たとえば，自己への危機感が誘因値へどのように作用するか，今回調査しなかった要素についても，誘因値への評価関数として定義できることが重要であると考える．すなわち，個人が考える利得は，個人が持つ評価関数により規定されるものである．このため，個人の多様性を考慮した価値関数などを考慮することが，必要であると考えられる．

5.1.3　実行意図と実行のギャップ

本研究の目的は，ボット対策事業に見られるような情報セキュリティ対策の低い対策率を向上することである．ボット対策事業を想定した質問紙調査での対策実行意図は高く，現実を表していなかった．これは，「実行意図」と実際の「実行」は異なる，ということを表す．ゴミの分別問題の社会調査でも，実行意図がないところに実行することはない，という前提で調査できたのは，「実行意図」であり，実際の「実行」ではない．また，実際の「実行」を確認するための社会調査を実施することは，現実的ではなく，この点での調査をいかに実態に合わせて実施するか，は重要な課題である．ボットネット対策の実態を見る限り，「実行意図はあっても，実行しない」状況である可能性が高い．本状況をさらに解明するためには，実際の感染者に対する調査，もしくは実験室での疑似環境を設置しての大規模な実験であろう．前者は，制度上，実施が困難であるため，今後は，実験室での実験を実現可能とし，実行意図と実行のギャップを解明したいと考える．

6. おわりに

情報セキュリティ対策として技術，組織のそれぞれの観点から取り組まれてきたが，セキュリティ事象は発生し続けている．これらから，個人が対策を実施するという点で，個人の意思決定にかかわる研究が情報セキュリティ対策の推進に有効であると考えた．情報セキュリティ対策がゴミ分別行動などの環境配慮行動と類似していることから，社会的ジレンマ状況に関する既存研究を援用し，協力行動を誘因する誘因関数と認知要素を定義し，情報セキュリティ対策における個人の利得構造と認知の状況を明らかにするための質問紙調査を実施した．調査では，情報セキュリティ対策が利得構造上の誘因値が，非協力を表す状況であること，フリーライダが存在することと理解度が関係すること，認知の状況として社会的ジレンマ状況であることを仮説とした．

調査の結果，約 80%の回答者が実施対策を実行する意図を持ち，協力行動への意図が高いことが分かった．そして，個人が誘因値に整合して利得を評価していることが分かった．したがって，コストと利得について，協力行動をとるよう誘因値を制御することは，実行意図を向上させることにつながることが明らかになった．次に，認知要素の調査結果であるが，社会的ジレンマ構造を表すタイプは，1%程度であり，認知上は，社会的ジレンマ状況を表していない．また，自己への危機感の認知が，情報セキュリティ対策実行意図に他の認知要素に比べて大きな影響があること，4 つの認知要素に順序性があると仮定すると，「危機感（自己）」→「危機感（他人）」→「有効感」→「非コスト感」の順に獲得されていくことが明らかになった．

今後さらに，研究が必要であると考えられるのは以下である．誘因値が 0 である回答者が 27%存在し，コストを損失値と同等であるとする傾向があり，誘因値の制御は協力率向上に貢献しない状況が存在すること．次に，CCC でのボット駆除ツール対策率の低さを，利得構造の調査，認知の調査では，実行意図と実際の実行の間にギャップが存在し，「意図はあるが，実行しない/できない」状況であることから，今後は，この状況を想定した研究が必要となろう．さらに，実証研究として利得構造に個人の認知による価値変換関数を定義すること，認知の二重プロセスや防護動機理論などの個人の認知の研究と数理的に社会をとらえる研究とを融合した研究として進めていく．

謝辞　本論文の調査は，（独）情報処理推進機構における「情報セキュリティ事象の社会科学的分析に関する調査」によって実施されたデータを使用している．納税者に感謝する．本調査の社会心理学分野の調査に助言いただいた東京大学池田謙一教授に感謝する．また，多くの示唆をいただいた匿名査読者に感謝する．

参　考　文　献

1) Dawes, R.: Social Dilemmas, *Annual Review of Psychology*, Vol.31, pp.169–193 (1980).
2) Hardin, G.: The Tragedy of Commons, *SCIENCE*, Vol.162, pp.1243–1248 (1968).
3) Anderson, R. and Moore, T.: The Economics of Information Security, *SCIENCE*, Vol.314, pp.610–613 (2006).
4) 日景奈津子，カール・ハウザー，村山優子：情報セキュリティ技術に対する安心感の構造に関する統計的検討，情報処理学会論文誌，Vol.48, No.9, pp.3193–3203 (2007).
5) 杉浦　昌，小松文子，上田昌史，山田安秀：情報セキュリティエコノミクスの挑戦，*Proc. CSS2008*, pp.725–730 (2008).
6) 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適用，IPSJ 研究報告，IPSJ-SIG-SPT-40(109), pp.265–280 (2009).
7) 木村邦博：大集団のジレンマ，ミネルヴァ書房 (2002.5).
8) 木村邦博：環境汚染問題の 3 つのモデル，土場　学，篠木幹子（編）：個人と社会の相克，pp.53–75, ミネルヴァ書房 (2008).
9) 小松　洋：環境問題はいかに認知されているか，土場　学，篠木幹子（編）：個人と社会の相克，pp.77–104, ミネルヴァ書房 (2008).
10) 横田賀英子：侵入窃盗犯のリスク対処行動に関する分析，木村通治，真鍋一史，安永幸子，横田賀英子（著）：ファセット理論と解析事例，pp.51–61, ナカニシヤ出版 (2002.6).
11) 木村堅一：脅威認知・対処認知と説得：防護動機理論，深田博巳（編著）：説得心理学ハンドブック，pp.374–417, 北大路書房 (2004.8).
12) 海野道郎：誰が社会的ジレンマを定義するのか?，社会学研究，東北社会学研究，No.80, pp.1–28 (2006.6).
13) Kahneman, D. and Tversky, A.: Prospect Theory: An Analysis of Decision under Risk, *Econometrica*, Vol.47, No.2, pp.263–292 (1979).
14) サイバークリーンセンター．https://www.ccc.go.jp/ (Last visited, 2009.11)
15) 藤井　聡：社会的ジレンマの処方箋，p.193, ナカニシヤ出版 (2003.10).
16) Yahoo! ネットの安全対策．http://special.security.yahoo.co.jp/
17) JNSA：2009 年情報セキュリティインシデントに関する調査報告書上半期速報版 Ver1.0 (2010.3.8).
http://www.jnsa.org/result/incident/data/2009fp_incident-survey_sokuhou_v1.0.pdf
18) 海野道郎，篠木幹子：社会調査における社会的ジレンマの測定について：方法論的検討，日本行動計量学会大会発表論文抄録集，Vol.34, pp.296–299 (2006.08).

付　　録

アンケート設問文

1. 注意喚起メールが送付されたとき，内容を読むかどうか（Q1）．
Q1：あなたが利用しているインターネットサービスプロバイダから［重要なお知らせ］と件名に書かれた電子メールが送信されてきたとします．あなたはその電子メールの本文を読みますか？[SA, N=5136]（はい/いいえの 2 択）
2. 対策をする手順を提示した後，ボット駆除対策ツールをダウンロードするつまり対策を実施するか（Q2）．
Q2：あなたは，次に示される電子メールが，インターネットサービスプロバイダから送信されたときに，指定されたサイトに示される「ボットの駆除手順」を行いますか．当てはまるものを 1 つ選んでください．[SA, N=4164]（行う，行わない，の 2 択）

3. 個人が対策をとることへのコスト感と，対策をとらないでいる場合の利得を，それぞれ現在のインターネットから得ている利益を 100 として（Q3，Q4）問う．
   Q3：今，あなたがインターネットから得られている利益を 100 とします．ボットに感染した場合，あなたが受ける損失は，インターネットから得られている利益 100 と比べてどのくらいですか．0 以上の半角・整数で入力してください．
   Q4：「ボットの駆除手順」にかかるコストは，インターネットから得られる利益を 100 としたときと比べてどのくらいですか．0 以上の半角・整数でお答えください．
4. 2.2 節で述べた社会的ジレンマ状況に対する 4 つの認知要素（コスト感，危機感（自分），危機感（他人），無効感）（Q5）．
   Q5-1（コスト感）：ボット駆除手順を行うことについて，あなたは面倒だと思いますか？
   Q5-2（危機感：自己）：ボットの駆除手順を行わないと，自分が被害を受けることはあると思いますか？
   Q5-3（危機感：他人）：ボットの駆除手順を行わなくても，インターネット上で他の人にさし障りが出ることはほとんどないと思いますか．
   Q5-4：（無効感）自分がボットの駆除手順を行わなくても，インターネット全体への影響はほとんどないと思いますか．

(平成 21 年 11 月 30 日受付)
(平成 22 年 6 月 3 日採録)

小松　文子（正会員）

日本女子大学卒業．NEC にて，汎用計算機の OS 開発，ネットワークプロトコル国際標準化活動を経て，JEIDA（現 JEITA）にてセキュリティ評価認証制度の導入に従事．NEC に復帰し，PKI 関連の製品開発・サービス開発・技術支援を経て後，中央研究所にて，効果的なセキュリティ対策についての研究に取り組む．2005 年 NEC 上席システムズアーキテクトに認定．2008 年より（独）情報処理推進機構情報セキュリティ分析ラボラトリーラボラトリー長．おもな著書に『PKI ハンドブック』（ソフトリサーチセンター）．

高木　大資

1982 年香川県に生まれる．2008 年明治学院大学大学院心理学研究科修士課程修了．現在，東京大学大学院人文社会系研究科博士課程（心理学修士）・日本学術振興会特別研究員（DC2）．おもな論文「他者の目撃記憶に関する情報と再認の遅延が他者への同調的な目撃記憶に及ぼす影響」社会心理学研究，24(3)，189–199，「地域コミュニティによる犯罪抑制：地域内の社会関係資本および協力行動に焦点を当てて」社会心理学研究，26(1)（印刷中）．

松本　　勉（正会員）

1986 年 3 月東京大学大学院工学系研究科電子工学専攻博士課程修了，工学博士．同年 4 月横浜国立大学講師．2001 年 4 月より同大学院環境情報研究院教授．現在，同大学教育研究評議員，日本学術会議連携会員，国際暗号学会 IACR 理事．暗号アルゴリズム・プロトコル，耐タンパ技術，生体認証，人工物メトリクス等の「情報・物理セキュリティ」の研究教育に 1981 年より従事．1982 年にオープンな学術的暗号研究を目指した「明るい暗号研究会」を 4 名で創設．1994 年第 32 回電子情報通信学会業績賞，2006 年第 5 回ドコモ・モバイル・サイエンス賞，2008 年第 4 回情報セキュリティ文化賞，2010 年文部科学大臣表彰・科学技術賞（研究部門）受賞．