IT 被害に遭いやすい心理的・行動的特性に関する調査

寺田剛陽[†1]　津田宏[†1]　片山佳則[†1]　鳥居悟[†1]

やり取り型の標的型メールや，水飲み場攻撃など，サイバー攻撃はユーザの心理・行動上の隙を突いた巧妙なものになってきている．こうした新たな攻撃に対抗するには，システム上の対策に加えてユーザ自身にも攻撃を見抜く力が必要となってきている．そこで我々は，組織の作業ログから近い将来にウイルス感染などの IT 被害に遭う可能性の高いユーザや部門を発見し，対策を配付するシステムの開発をめざしている．ここで，被害を削減するためにはユーザや部門の特性に合わせた対策の提供が必要だと我々は考えている．この実現に向けて今回の研究では約 1,000 名の IT 被害経験者に対してアンケート調査を行い，IT 被害経験者の心理・行動上の特徴を明らかにした．本結果は，組織における個人や部門のリスクの見える化や，きめ細かいサイバー攻撃対策に適用できると考えられる．

Investigation on Psychological and Behavioral Characteristics of Users Vulnerable to Cyber Attack

TAKEAKI TERADA[†1]　HIROSHI TSUDA[†1]　YOSHINORI KATAYAMA[†1]
SATORU TORII[†1]

1. 背景

標的型攻撃においては，業務上のやりとりを騙った標的型メールや，標的対象のユーザが日常よくアクセスするサイトを用いた水飲み場攻撃など，ユーザの心理的な特徴や行動上の隙をついた巧妙な攻撃が行われている[1]．こうした新たな攻撃に対抗するには，入口・内部・出口での監視や脆弱性対策などシステム上の対策に加えて，利用者にもこうした攻撃を見抜く力が必要となってきている[2][3]．

我々は，総務省「サイバー攻撃の解析・検知に関する研究開発」の一環として，サイバー攻撃などの IT 被害に遭いやすいユーザの心理や行動における特性を明らかにすることでリスクの高い利用者や組織の見える化を行い，リスクの大きさや種類に応じたセキュリティ対策につなげる研究を行っている．本論文では，IT 被害経験者に対して普段の考え方や行動に関するアンケート調査を行った結果，被害に遭いやすい因子をいくつか抽出したので報告する．

2. 関連研究

2.1 IT リスクに対するユーザ認知の研究

セキュリティにおける最大の弱点は人である．堅牢なシステムも適切に運用されなければその効果が活かされない．昨今，セキュリティに心理学や経済学などの社会科学の知見を活かそうとする動きが出てきている[4][5]．行動科学をサイバー攻撃対策に活かす研究[6]では，標的型攻撃メールに気付く力を養成する為には，対策を覚えやすくかつ，思い出しやすい形で提供することが必要であるとし，対策行動の促進にはインセンティブ（賞罰両方の意味で）を組織や個人に応じた形で提供するという議論を行っている．

セキュリティパッチの適用行動を効果的に促す研究[7][8]は，被害の恐ろしさを強調するよりも，対策自体の有効性を強調して伝える方が，パッチ適用の行動を促す効果があることが報告している．また，情報セキュリティ被害と個人属性（性別や年齢，ネット利用状況やセキュリティ知識など）の相関を調べた研究[9]では，フィッシング，ネット上の金銭被害の経験がある人は，自身のセキュリティ知識に過剰な自信を持っていると報告している．

2.2 ユーザの行動履歴に基づくセキュリティ対策

標的型攻撃メールの対象になりやすい職種を調べた研究[10]では，Symantec 社が収集したマルウェア付きメールのデータセットを学術研究者の専攻分野で分類したところ，「社会科学」や「東洋，アフリカ，アメリカ，オーストラリアの言語学，文学」カテゴリの研究者に標的型メールが多く届いていると報告している．

また，機密情報を含むメールが社外に流出することを防ぐ研究として，PC の利用実態や勤務状態といったユーザの個人属性と，機密情報を含むメールの社外発信数との相関を調べる研究があり[11]，情報漏洩を起こす社員の行動パターンを特定できる可能性を示唆している．

スマートフォンのアプリ権限の自動最適化に関する研究[12]では，コンピュータに関する専門知識を持たない一般ユーザにとって難解なアプリ権限付与の作業を，480 万人のユーザのアプリ権限設定のデータを分析し，最も属性の近いクラスタにユーザを分類することで，そのユーザに最適なアプリ権限設定テンプレートを提示できることを示

†1 富士通株式会社

している．

3. 課題

本研究の目的は，組織の従業員の作業ログから，近い将来にウイルス感染や標的型メールなどの IT 被害に遭う可能性の高いユーザや部門を検知し，対策を配付するシステムを構築することである．IT 被害を防ぐ実効性のある対策を提供するためには，ユーザや部門の特性に合わせた対策が必要だと考えている．つまり，検知対象になるようなログの値をユーザが残すようになった原因（作業環境や心理状態）を考慮して対策を検討し配付する必要があると考える．

そこで，セキュリティ意識に関する前記の従来研究[3][7][9]を参考に，IT 被害経験と，日頃の考え方・行動習慣の相関を調べるアンケート調査を実施した．この結果を分析することで IT 被害に関係する因子を抽出する．次に因子と作業ログの相関を求めることで，近い将来に被害に遭う可能性が高いユーザや部門を検知し，かつ彼らの特性に合わせた対策を提供するシステムを構築する．このシステムによって，被害に遭いやすいユーザ・部門を特定することができれば，彼らの心理や所属組織を考慮したより踏み込んだ対策が可能となる．逆にリスクの低いユーザ・部門に対しては対策を緩める検討も可能になる．

4. 被害因子を調べるアンケート調査の実施

4.1 調査のモデル

IT 被害に遭いやすいユーザが持つ心理的因子，行動的因子はどのようなものかを調べるため，図 1 に示すモデルを立てて分析することにした．

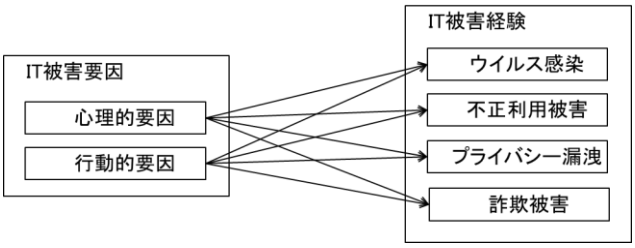


図 1　IT 被害モデル

Figure 1　The model that represents the relations between the damages on the Internet use and their cause.

調査票は IT 被害要因，IT 被害経験を調べる質問項目から構成し，分析では，回答データについて，回帰分析の手法を用いて，IT 被害経験の種類別にその因子を調べる．

4.2 調査票の作成

調査票の作成にあたっては，ヒューマンエラーや社会心理学におけるリスク回避行動に関する知見を援用して作成した．中谷内ら[13]によると，リスク回避行動をとるまでの意思決定プロセスにはさまざまな要因が作用することがわかっている．たとえばリスク認知（好ましくない事象が発生することに対する各個人の主観的な確率的判断）やコントローラビリティ（リスクを自分の知識やスキルでコントロールできるという認識の強さ）などの認知的要因，不安や後悔予期などの感情的要因，バイアスやヒューリスティックスなどの人間の情報処理の性質などである．

リスク回避行動に作用する要因はリスクの種類によって異なる一方で，共通する要因もある[13]．そこで，病気や事故などの身体的リスク，盗難や投資などの金銭的リスク，自然災害や原子力発電所のリスクなどに対する回避行動に作用する要因のなかには，ウイルス感染や標的型攻撃メールといった IT リスクに対する認知にも共通するものがあると考えた．また，標的型メール対策に関する我々の研究[3]において，標的型メールを模した「訓練メール」を開いた群と開かなかった群のアンケート回答データを比較したところ，開いた群は開かなかった群に比べて自信過剰でかつ，情報共有意思が低い傾向がわかった．表 1 にリスク回避行動に関係する要因の一覧を示す．

表 1 リスク回避行動に関係する要因

Table 1　The factors related to the risk evasion action.

リスク認知に関する因子	説明
リスク受容　安全志向因子	リスクを敬遠して安全な選択をする傾向
リスク受容　運命因子	被害に遭うのは不可抗力な部分があると考える傾向
自己効力感	直面する課題を自分で解決できるという自信
一般的信頼	他人を信頼する傾向
パーソナルな信頼	知人を信頼する傾向
用心深さ	人に対する用心深さ
権威主義	組織や目上の人、慣習に従う傾向
後悔予期	失敗を恐れる傾向
コスト認知	物事のリスクよりもリスク回避策に費やす労力を重視する傾向
ベネフィット認知	物事のリスクより利益を重視する傾向
ITに対するコントローラビリティ	ITを使いこなせる、ITに関するトラブルに対処できると思う傾向
現状維持傾向	変化を忌避する傾向
損失回避傾向	損をすることを敬遠する傾向

上記の知見のほか，IT 被害に関係がありそうな要因を検討して今回の調査票を作成した．質問項目数は回答者の負担が極力軽くなるよう約 50 項目とし，15 分程度で回答できる分量にした．今後，多くの従業員・組織に調査協力をお願いするためには必要な工夫であると考えている．IT 被害に関係しそうな因子を，できるだけ多く調査票に盛り込むため，質問項目の取捨選択において工夫を行った．被害因子と考えられる質問項目のなかには，社会心理学の知見

である心理測定尺度[14～19]を利用した項目があるが，心理測定尺度における質問項目は 4～10 項目で構成されているため，全項目を調査票に採用してしまうと，すぐに 50 項目を超えてしまい，調べたい被害因子の数が大幅に減ってしまう．そこで次善の策として，被害因子として選んだそれぞれの心理測定尺度について，その尺度を構成する質問項目のうち因子負荷量が高い上位 2 つの項目を採用した．このようにして被害要因約 25 項目を調査票に盛り込んだ．

また，IT 被害経験については[9]を参考に，4 種類の被害種別を用意し，それぞれの被害経験回数を答えてもらう形にした．調査票を構成する項目の一覧を表 2 に示す．ほとんどの項目で「まったくあてはまらない（1 点）」～「非常によくあてはまる（6 点）」の 6 段階尺度で回答してもらった．心理測定尺度から拝借した項目についても，6 段階尺度で統一することで回答者の負担を減らすようにした．

Q5，Q6 は情報共有意思に関する質問であり，「A に近い（1 点）」～「B に近い（6 点）」の 6 段階尺度で回答してもらった．Q10 では標的型攻撃に関するクイズを 3 問出題しており，「正しい」「正しくない」「わからない」の 3 択で回答してもらった．また，Q12 は PC 習熟度の自己評価をたずねる質問で「簡単な操作しかわからないレベル(1 点)」「メールやホームページ閲覧, PC を使って文章を書けるレベル(2 点)」「簡単なプログラミングや日常のトラブルを自分で解決できるレベル(3 点)」「専門的なプログラミングを行うことができるレベル(4 点)」の 4 段階尺度で回答してもらった．

表 2 アンケート調査項目一覧

Table 2　The list of the questionnaire items.

項番	質問意図	質問文
Q1_1	ウイルス感染経験	ウイルス感染（自分のパソコンに入っているセキュリティソフトが検出した場合も含む）
Q1_2	不正利用被害経験	不正利用（ユーザID、アカウント、オンラインゲームなどでの通貨やアイテム、クレジットカード、銀行口座、など）
Q1_3	プライバシー漏洩経験	プライバシーの漏洩（SNSや動画サイトなどにおける個人用設定が原因で、個人的な日記や閲覧履歴などが不特定多数に公開されてしまった、など）
Q1_4	詐欺被害経験	詐欺（なりすましメールに騙された、架空請求の支払いに応じた、偽のセキュリティソフトをインストールしてしまった、パソコンのシステムやファイルが書き換えられ元に戻すためにお金を支払った、など）
Q2_1	リスク受容 安全志向因子	危ない場所へは絶対近づかない
Q2_2	リスク受容 安全志向因子	何事も安全第一である
Q2_3	リスク受容 運命因子	危険と上手につきあうのが人生である
Q2_4	リスク受容 運命因子	危険と安全が混じり合っていることで、世の中は成り立っている
Q2_5	自己効力感の低さ	私にとって、最終的にはできないことが多いと思う
Q2_6	自己効力感の低さ	やりたいと思っても、私にはできないことばかりだと感じる
Q2_7	一般的信頼	ほとんどの人は基本的に正直である
Q2_8	一般的信頼	ほとんどの人は信頼できる
Q2_9	パーソナルな信頼	何をするにつけ、知らない人とするよりも、よく知った人とするほうが安心できる
Q2_10	パーソナルな信頼	一般に、長くつきあっている人は、必要なときに助けてくれることが多い
Q2_11	用心深さ	世の中には偽善者が多い
Q2_12	用心深さ	人々はふつう、口で言っているほどには、他人を信頼していない
Q3_1	権威主義	伝統習慣にしたがったやり方をとるべきだ
Q3_2	権威主義	先祖代々と同じやり方をとるべきだ
Q3_3	後悔予期	うまくいった場合のことよりも、失敗して後悔した場合のことを考える
Q3_4	後悔予期	最善のことをしたとしても、失敗した場合のことが気になってしまう
Q4_1	コスト認知の低さ	パソコンやスマートフォンなどで、アプリケーションをインストールする際やアップデートする際に表示される規約文や権限許可などの内容は、きちんと確認・理解してから先へ進む
Q4_2	コスト認知の低さ	前々から予定に入っていた大事な試験やプレゼンテーション（発表・企画提案・説明など）の日までには、自分として納得のいく準備（勉強量、資料内容、話す内容など）ができているのはいつものことだ ※　急な仕事の依頼などやむを得ない理由で準備不足になった場合は除く
Q4_3	ベネフィット認知	車がまばらに通っているが、車がまだずっと遠くにいれば、つまづく可能性も0ではないが、赤信号でも横断歩道を渡る
Q4_4	ベネフィット認知	つい、夜更かししたり、食べ過ぎ・飲み過ぎたりして、翌日以降の仕事や体調に影響が出てしまう
Q5	情報共有意思の低さ	Q5　仕事で、間違った情報を教えたり報告してしまったら、「A. ささいなことでもすぐに伝える」「B. よほどの支障が生じる心配がない限り伝えない」のどちらに近い対処をとりますか。 ※　お勤めの会社に、上記のような場合の対処マニュアルがないものとしてお答えください。
Q6	情報共有意思の低さ	Q6　仕事で、あなたは大事な顧客情報または社内機密情報を、まったく別の相手に送ってしまったら、「A. なるべく周りに相談して解決したい」「B. なるべく自分で解決したい」のどちらに近い対処をとりますか。（回答は1つ） ※　お勤めの会社に、上記のような場合の対処マニュアルがないものとしてお答えください。
Q7_1	ITに対するコントローラビリティ	わたしは、仕事上の大事なデータを誤って流出させたり、紛失したりすることはないと思う
Q7_2	ITに対するコントローラビリティ	わたしは、ブログやツイッター、掲示板などのインターネット上のコミュニケーションツールを正しく使えるので、不用意な発言で個人情報をもらしてしまったり、発言が広められて不特定多数の人間から非難を浴びることはないと思う

Q8_1	現状維持傾向	見たいTV番組が終わった後も、ずっとTVを見続けてしまったり、面白いwebサイトを読んだり見たりし終わった後も、ずっとネットサーフィンをしてしまうことが多い
Q8_2	損失回避傾向	欲しいものはできるだけ安く、お得に手に入れたい
Q8_3	所有欲	どうしても欲しいものは多少無理をしてでも手に入れる
Q8_4	楽観的傾向	わたしは、ふだんから気をつけているので、交通事故や犯罪に巻き込まれることはないと思う
Q8_5	流されやすさ	人から勧められたり、話を聞いて、その商品を手に入れたり、そのお店やイベントなどに行ってみたが、よくよく考えるとそんなに欲しくも行きたくもなかったなと思うことが多い
Q8_6	自制心の弱さ	街やインターネットで、その場でほしいと思った物を購入してみたが、あとで後悔することが多い

Q9	セキュリティ対策に対する心理的負担	セキュリティ対策は何をすればいいのかわからないし、面倒なのでしたくない
Q10_1	標的型攻撃についての知識（正解は○）	攻撃対象となるのは、不特定多数の一般ユーザではなく、特定の組織や特定の個人になる
Q10_2	標的型攻撃についての知識（正解は○）	攻撃者が用意したサーバから不正なプログラムをダウンロードさせるために、まずはそれを実行するため、必要なウイルスをパソコンに感染させるタイプがある
Q10_3	標的型攻撃についての知識（正解は×）	メールの差出人のアドレスや本文の内容から疑わしい要素を見つけやすいので、対策が比較的容易である
Q11_1	仕事量（自己評価）	1日でこなさなければならない案件がとても多く、残業が深夜に及ぶ
Q11_2	web接触時間その1	家に帰ってからの自由時間が少ないので、じっくりインターネットをする時間がない
Q11_3	web接触時間その2	家に帰ってからの自由時間が少ないので、インターネットよりも他のことに時間を使いたい
Q12	PC習熟度	Q12 あなたのパソコンの習熟度に近いものをお答えください。

表 2 において，Q2～Q3 が心理測定尺度を採用した項目である．Q2_1～2_4 は木下らのリスク受容尺度[14]，Q2_5，Q2_6 は三好らの自己効力感尺度[15]，Q2_7～Q2_12 は山岸らの一般的信頼尺度[16,17]，Q3_1，Q3_2 は敷島らの権威主義的伝統主義尺度[18]，Q3_3，Q3_4 は上市らの後悔予期尺度[19]から拝借した．

4.3 調査の実施

調査はリサーチ会社である株式会社インテージのモニター会員約 1,000 名に対し，web アンケートの形式で実施した．調査票は IT 被害経験回数および普段の考え方や行動習慣をたずねる内容から構成される．アンケート調査の概要を表 3 に示す．

表 3 アンケート調査の概要

Table 3 The attributes of the target on the questionnaire survey.

調査対象者	リサーチ会社が擁する国内のモニター約1000名
調査対象者の属性	全国の男女、20～60歳代、会社員でかつ、業務の半分以上で自分専用のパソコンを使用する、IT被害のいずれかに1回以上遭ったことがある
調査形式	webアンケート

モニターの男女比および年代比は，リサーチ会社のモニターの構成比に従っている．web アンケートページは各質問が 1 問ずつ提示する形式であり，一度回答すると次の質問のページが表示される．前の質問に戻って回答を訂正することはできない．

5. 調査結果

本節では，図 1 のモデルに基づいて，ロジスティック回帰分析を行った結果を示す．ロジスティック回帰分析とは，分析対象のデータを 2 つ以上の群に分け，どれか 1 つの群を基準に，それ以外の群について予測変数が基準変数に与える影響の強さをオッズで表現する回帰分析の一手法である．本調査では，以下の手順でロジスティック回帰分析を回答データに適用した．

1. 基準変数，予測変数を決める
   回答データのうち，IT 被害経験をたずねる質問項目のデータを基準変数（従属変数），被害因子を調べる各質問項目のデータを予測変数（独立変数）の素材とする．
2. データを 2 群に分ける
   IT 被害経験回数の度数分布に基づき，データを被害が少ない群と多い群の 2 群に分ける．
3. データを加工する
   被害因子を調べる質問項目のデータを回帰分析で利用できる形に加工する．
4. 予測変数を作る
   予測変数をどの質問項目を組合せて合成するかの判断基準を作るため，被害因子を調べる質問項目のデータの因子分析を行う．
5. ロジスティック回帰分析を行う
   被害が少ない群を基準の群（「ベースカテゴリ」とよばれる）として，ロジスティック回帰分析を行う．なお，分析は IT 被害経験の種類ごとに行う．
6. モデルを評価する
   求めたロジスティック回帰モデルがデータをどの程度説明しているかを，逸脱度残差のカイ二乗検定ならびに，各データが 2 群のどちらに属するかのモデルによる判別率で評価した．

5.1 データを 2 群に分ける

IT 被害経験回数の度数分布を IT 被害の種類ごとの被害経験回数の度数分布を表 4～7 に示す．いずれの表も 1021 名分のデータであり，横軸が被害経験回数，縦軸が人数を表す．

表 4 ウイルス被害回数の度数分布

Table 4 The frequency distribution of the viral infection experiences.

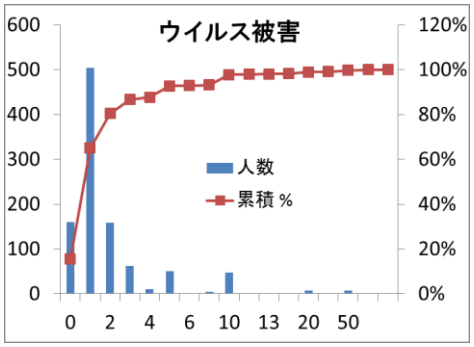


表 5 不正利用被害回数の度数分布

Table 5 The frequency distribution of the experiences damaged by unauthorized use.

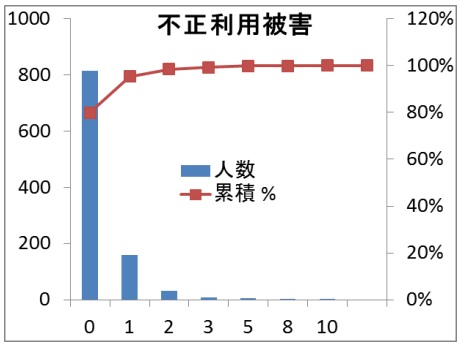


表 6 プライバシー漏洩被害の度数分布

Table 6 The frequency distribution of the experiences damaged by private information leakage.

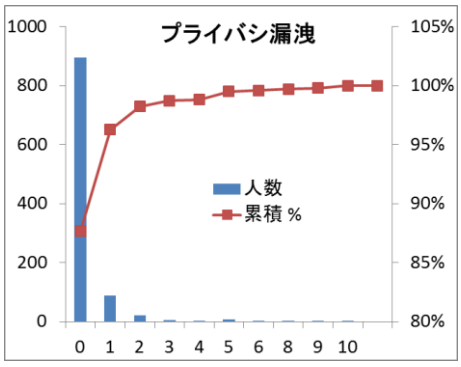
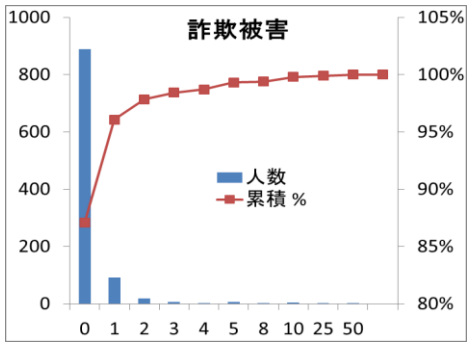


表 7 詐欺被害の度数分布

Table 7 The frequency distribution of the experiences damaged by fraud.



当初の分析では，これらの度数分布の対数をとった重回帰分析や，度数分布をポアソン分布とみなしてポアソン回帰分析を行ったが，回帰式のデータ予測力（決定係数，擬似決定係数など）が低かったため，度数分布に基づいてデータを複数の群に分け，これらの群を基準変数とするロジスティック回帰分析を行うことにした．

表から，ウイルス被害については被害回数 1 回が最も多く，その他の被害については被害 0 回が最も多いことがわかる．そこでウイルス被害については被害 1 回以下の人たちを「被害が少ない群」，2 回以上を「被害が多い群」，その他の被害については被害 0 回を「被害が少ない群」，1 回以上を「被害が多い群」としてデータを 2 群に分けてロジスティック回帰分析を行うことにした．

5.2 データを加工する

アンケートの Q2 以降の質問項目をロジスティック回帰分析の予測変数として利用するにあたり，各質問項目の正規性(データの分布が正規分布とみなせるか)を確認した．正規分布とみなせないデータを予測変数として回帰分析（ロジスティック回帰分析含む）で利用してしまうと，求まった回帰係数の検定が行えないため，その質問項目が IT 被害回数と有意に関係があるかを確認できない．正規性の確認は，平均値と標準偏差（Standard Deviation，SD）を求めて天井効果（平均値＋SD ＞ 最大値）または床効果（平均値－SD ＜ 最小値）があるかを調べることで行った．確認の結果，すべての質問項目について正規性を確認できた（表 8）．

表 8 質問項目の正規性の確認結果

Table 8 The frequency distribution of the questionnaire items from Q2 to Q12 can be considered as a normal distribution.

質問番号	最小値	最大値	平均値	標準偏差	平均+SD	平均−SD
Q2_1	1	6	4.3	1.2	5.5	3.1
Q2_2	1	6	4.3	1.1	5.5	3.2
Q2_3	1	6	3.6	1.2	4.8	2.3
Q2_4	1	6	4.0	1.1	5.1	2.8
Q2_5	1	6	3.9	1.2	5.1	2.6
Q2_6	1	6	3.6	1.2	4.9	2.4
Q2_7	1	6	3.4	1.2	4.6	2.2
Q2_8	1	6	3.3	1.2	4.5	2.2
Q2_9	1	6	4.3	1.1	5.4	3.2
Q2_10	1	6	4.0	1.1	5.1	3.0
Q2_11	1	6	4.0	1.1	5.0	2.9
Q2_12	1	6	4.2	1.0	5.2	3.2

Q3_1	1	6	3.6	1.0	4.6	2.6
Q3_2	1	6	3.3	1.0	4.3	2.3
Q3_3	1	6	3.8	1.1	4.9	2.6
Q3_4	1	6	3.7	1.1	4.8	2.5
Q4_1	1	6	3.4	1.2	4.6	2.2
Q4_2	1	6	3.9	1.1	5.0	2.8
Q4_3	1	6	3.5	1.3	4.9	2.2
Q4_4	1	6	3.5	1.2	4.7	2.3
Q5	1	6	3.2	1.3	4.5	1.9
Q6	1	6	3.4	1.4	4.8	2.0
Q7_1	1	6	3.9	1.2	5.0	2.7
Q7_2	1	6	3.8	1.3	5.0	2.5
Q8_1	1	6	3.7	1.3	5.0	2.4
Q8_2	1	6	4.5	1.1	5.6	3.3
Q8_3	1	6	3.9	1.1	5.0	2.8
Q8_4	1	6	3.3	1.1	4.4	2.2
Q8_5	1	6	3.4	1.1	4.5	2.3
Q8_6	1	6	3.3	1.1	4.4	2.2
Q9	1	6	2.8	1.3	4.2	1.5
Q11_1	1	6	2.8	1.3	4.1	1.5
Q11_2	1	6	2.9	1.3	4.3	1.6
Q11_3	1	6	3.2	1.3	4.4	1.9
Q12	1	4	3.0	1.0	3.9	2.0

また，Q10_1，Q10_2，Q10_3 については，3 問とも正解している回答者にダミー値 1，それ以外の回答者にダミー値 0 を割り当てた．

5.3 予測変数を作る

ロジスティック回帰分析を行うにあたり，多重共線性（データ数をわずかに増やしただけで分析結果である回帰式の係数や有意性が大きく変化する状態）を排除するため，項目間の相関係数を調べた．結果，0.7 を超える項目はなかった．よって多重共線性は起きにくいことを確認した．

次に，予測変数としてどの質問項目を組み合わせるかの判断基準を作るため，IT 被害因子の質問項目データを用いて因子分析を行った．ここで，心理測定尺度を利用した質問項目（Q2，Q3）については，それぞれの尺度を構成する 2 項目のデータをあらかじめ合算した．図 2 にスクリープロットのグラフ，表 9 に因子分析（最尤法，プロマックス回転, 統計ソフトは R のパッケージ psych の関数 fa を使用）の結果を示す．「Q3_3Q3_4」という表記は Q3_3 と Q3_4 のデータを合算したことを表している．

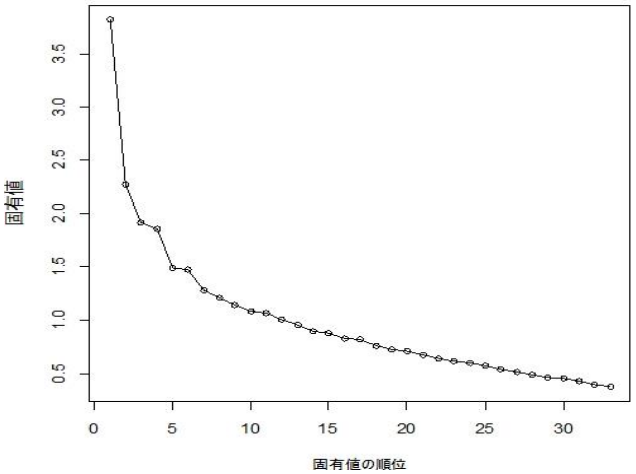


図 2 アンケート回答データのスクリープロット

Figure 2　The scree plot of the eigenvalues of the questionnaire answer data.

図 2 は各質問項目の固有値を大きい順にプロットしたものでスクリープロットとよばれる．因子分析を行う際は，あらかじめ因子数を決めておく必要があり，判断基準の 1 つとしてスクリープロットが使われる．折れ線グラフが急激に小さくなる 1 つ前までの点の数を因子数の目安として利用する．今回の分析では 6 因子で分析を行うことにした．

表 9　因子分析の結果

Table 9　The result of a factor analysis on the questionnaire answer data.

質問番号	因子						共通性
	1	2	3	4	5	6	
Q9	0.64	−0.05	0.02	0.00	−0.04	−0.16	0.39
Q8_6	0.60	0.02	0.05	−0.01	0.03	0.05	0.39
Q8_5	0.57	−0.05	0.13	−0.05	−0.03	0.04	0.34
Q5	0.44	−0.05	0.09	−0.05	0.02	−0.08	0.18
Q6	0.31	0.00	0.19	−0.06	0.01	−0.03	0.13
Q11_2	0.02	0.78	−0.08	−0.01	0.01	−0.05	0.61
Q11_3	0.00	0.61	0.05	0.00	0.02	−0.07	0.38
Q11_1	0.06	0.60	−0.06	0.02	0.00	0.03	0.39
Q4_1	−0.04	0.23	0.15	0.06	0.01	−0.08	0.09
Q7_2	−0.06	−0.06	0.67	−0.01	−0.02	−0.01	0.45
Q7_1	−0.18	−0.04	0.65	0.00	0.00	0.08	0.48
Q8_4	0.21	−0.02	0.44	0.07	−0.04	−0.06	0.23
Q4_2	−0.21	0.11	0.23	0.04	−0.01	0.11	0.13
Q3_3Q3_4	0.04	0.02	−0.02	0.71	−0.06	−0.03	0.50
Q2_5Q2_6	0.02	−0.05	0.03	0.57	0.02	0.01	0.34
Q3_1Q3_2	0.02	−0.01	0.03	0.37	0.22	−0.03	0.21
Q2_7Q2_8	−0.03	0.02	−0.02	−0.01	1.00	0.02	1.00
Q2_9Q2_10	0.01	−0.05	0.03	0.19	0.25	0.02	0.11
Q8_2	−0.16	−0.09	0.07	−0.04	0.00	0.65	0.44
Q8_1	0.15	0.03	−0.06	0.02	0.04	0.49	0.29
Q8_3	0.10	0.02	0.09	0.00	0.00	0.30	0.14
Q4_4	0.28	0.09	0.00	0.00	−0.01	0.29	0.22
Q4_3	0.14	0.03	0.08	−0.02	0.00	0.13	0.06
Q12	−0.23	0.15	0.03	−0.03	0.01	0.07	0.06
Q10	−0.01	−0.02	−0.01	−0.01	−0.02	0.07	0.01
Q2_11Q2_12	−0.01	0.01	−0.04	0.36	−0.33	0.05	0.21
Q2_1Q2_2	−0.09	−0.05	0.03	0.22	0.02	0.02	0.06
Q2_3Q2_4	0.01	−0.06	−0.04	0.18	0.04	−0.02	0.04

因子間相関	1	2	3	4	5	6
1	1.00	0.29	−0.01	0.00	0.07	0.16
2	0.29	1.00	0.13	0.05	0.00	0.11
3	−0.01	0.13	1.00	0.09	−0.01	0.22
4	0.00	0.05	0.09	1.00	0.10	0.08
5	0.07	0.00	−0.01	0.10	1.00	−0.01
6	0.16	0.11	0.22	0.08	−0.01	1.00

表 9 の結果を参照して，因子負荷量が高い質問項目どうしをさまざまな組合せで合算することで予測変数を合成し，ロジスティック回帰分析を行った．合成にあたっては因子負荷量の高さに加えて質問項目の意図も考慮した．たとえば，因子 1 には，Q9，Q8，Q5，Q6 が入っているが，Q5 と Q6 はどちらも情報共有意思を調べる質問項目であるので，Q5，Q6 を合成した予測変数，残りの Q9，Q8 を合成した予測変数を作るなどしてロジスティック回帰分析を行った．

5.4 ロジスティック回帰分析を行う

さまざまな予測変数でロジスティック回帰分析を行った（最尤推定法．統計ソフトは R のパッケージ VGAM の関数 vglm を使用）．その結果，質問項目を合成せずにそのまま予測変数として利用するほうが回帰係数の有意性が概

ね高い傾向になることがわかった．表 10 に IT 被害種別ごとのロジスティック回帰分析の結果を示す．表には，各質問項目の z 値（Wald 検定が定める，回帰係数を標準誤差で割った値）を記述している．|z| > 1.28 は 10%水準，|z|>1.64 は 5%水準，|z|>2.33 は 1%水準，|z|>3.09 は 0.1%水準で有意であることを示している．また，各質問項目を「影響度」が大きい順に列挙している．影響度は被害種別の z 値の最大値の絶対値で定義したが，あくまで分析結果を見やすくするために独自に導入した値であり，影響する被害種別が多い質問項目であれば，影響度が小さくとも IT 被害への影響が大きい因子といえる．

表 10　IT 被害種別ごとのロジスティック回帰分析の結果

Table 10　The result of a logistic regression of the questionnaire answer data for each type of the damages.

質問番号	被害種別の z 値				影響度
	ウイルス感染	不正利用	プライバシ漏洩	詐欺	
Q12	−0.17	3.09	1.48	0.61	3.09
Q9	−2.87	2.30	2.16	1.53	2.87
Q5	0.24	−2.37	−1.17	−1.15	2.37
Q7_1	−0.88	−0.34	−2.22	−0.86	2.22
Q4_1	−2.20	−1.08	0.94	1.47	2.20
Q2_7Q2_8	−1.27	2.19	−1.06	0.65	2.19
Q4_3	2.03	1.14	0.01	−1.25	2.03
Q2_1Q2_2	−1.66	−1.72	−1.96	−1.55	1.96
Q8_1	0.07	1.58	1.84	1.08	1.84
Q8_6	1.01	−1.72	−0.32	−0.01	1.72
Q10	0.07	−0.95	−0.99	1.50	1.50
Q6	0.45	1.21	1.40	0.76	1.40
Q11_1	0.65	−0.20	−0.44	1.31	1.31
Q3_3Q3_4	−1.25	−0.01	1.28	1.07	1.28
Q2_5Q2_6	−0.17	1.19	−1.18	−1.26	1.26
Q8_3	1.20	−0.68	−0.26	−0.91	1.20
Q8_2	0.00	0.71	−0.88	−0.21	0.88

表の結果から，ウイルス被害については，セキュリティ対策への心理負担度（Q9）やコスト認知の低さ（Q4_1）が被害を減らし（正確には被害の少ない群にユーザが振り分けられる確率が高まる），ベネフィット認知（Q4_3）が被害を増やす（被害の多い群にユーザが振り分けられる確率が高まる）ことがわかる．また，Q9 やリスク受容安全志向因子（Q2_1Q2_2）はすべての被害種別に対して有意に被害に影響する因子といえる．

5.5　モデルの評価

5.5.1 逸脱度残差のカイ二乗検定

ロジスティック回帰モデルによる IT 被害モデル（図 1）の適合度評価を，モデルに予測変数を全く投入しない場合（切片のみ）の逸脱度残差と投入した場合の逸脱度残差の差のカイ二乗検定で行った（表 11）．表の結果からモデルが有意であることがわかる．

表 11　ロジスティック回帰モデルのカイ二乗検定

Table 11　The result of a chi-square examination of the difference between the residual deviances on the logistic regression model

被害種別	切片のみ		質問項目投入		カイ二乗検定		
	自由度	逸脱度残差	自由度	逸脱度残差	χ ^2 値	累積確率 p	有意水準
ウイルス感染	1020	1321.7	1000	1292.0	29.7	0.07	p < 0.1
不正利用被害	1020	1024.0	1000	967.1	56.9	0.00	p < 0.01
プライバシ漏洩	1020	763.0	1000	673.4	89.6	0.00	p < 0.01
詐欺被害	1020	786.2	1000	715.4	70.8	0.00	p < 0.01

5.5.2 モデルによるデータの判別

表 12 は，IT 被害モデルを使って，1021 名の回答者が被害の少ない群と多い群のどちらに属するかを計算した結果である．

表 12　IT 被害経験の判別確率

Table 12　The correct answer rates of the logistic regression model for each type of the damages.

ウイルス被害

群分け	人数	モデルで予測した群		無作為判定
		2回以上群	1回以下群	
2回以上群	357	7.6%	92.4%	35.0%
1回以下群	664	3.0%	97.0%	65.0%

不正利用被害

群分け	人数	モデルで予測した群		無作為判定
		1回以上群	0回	
1回以上群	205	4.9%	95.1%	20.1%
0回	816	0.4%	99.6%	79.9%

プライバシ漏洩被害

群分け	人数	モデルで予測した群		無作為判定
		1回以上群	0回	
1回以上群	126	5.6%	94.4%	12.3%
0回	895	0.1%	99.9%	87.7%

詐欺被害

群分け	人数	モデルで予測した群		無作為判定
		1回以上群	0回	
1回以上群	132	2.3%	97.7%	12.9%
0回	889	0%	100%	87.1%

どの被害種別でも，被害回数が多い群に属する回答者を多い群に属すると正しく予測する確率は，無作為に予測する場合より低下したが，被害回数が少ない群に属する回答者を少ない群に属すると正しく予測する確率は向上した．

6.　考察

6.1　被害種別によって作用が逆の項目

表 10 の結果から，IT 被害因子といえる質問項目が抽出されたが，被害種別によって逆に作用する質問項目もある．セキュリティ対策への心理負担度（Q9）において，ウイルス感染被害は他の被害とは逆に，負担を感じている人の方が被害は少ない（正確には被害が少ない群にユーザが振り分けられる確率が高まる）ことを示している．この理由の仮説として，セキュリティ対策は面倒であるがウイルスの危険については世間の認知度が高まっており，また対策ソフトも比較的安価に入手できることから，負担に感じつつも対策は実施しているため被害が少ないことが考えられる．

コスト認知の低さ（Q4_1）においては，ウイルス感染に対しては被害を減らす方向に作用しており予想と一致する

一方，詐欺被害に対しては増やす方向に作用しており，現状ではうまく解釈できていない．ベネフィット認知（Q4_3）についても，ウイルス感染と詐欺で逆の結果となっており，うまく解釈できていない．

後悔予期（Q3_3Q3_4）に対してはウイルス被害を減らす一方でプライバシー漏洩が増える結果になっているが，プライバシー漏洩は因果が逆なのではないかと考えている．つまり漏洩被害に遭った結果，後悔予期が強くなったということである．自己効力感の低さ（Q2_5Q2_6）に対しては，不正利用被害と詐欺被害が逆の結果となっている．不正利用被害が予想に反してなぜ被害を増やすかはうまく解釈できていない．ただし有意水準 10%に満たないので偶然の可能性もある．

6.2 同じ質問意図であるが作用が逆の項目

情報共有意思をたずねる項目については Q5 と Q6 で結果が逆転している．寺田ら[3]の結果からすると，Q6 は予想に則した結果である一方，Q5 は逆の結果となった．理由として，Q5 と Q6 では共有する情報の質の違いが考えられる．Q5 で情報を共有しないと答えた人は大事でないと判断した情報を伝えないだけで大事な情報は共有する人たちであるという可能性がある．つまり Q5 は大事な情報とそうでない情報を判別できる自信があるかをたずねる質問になっていた可能性がある．一方で Q6 は確定した危険についての情報を共有するかという質問であったため，共有しないと答えた人たちは被害が多い傾向となったのではと考える．

6.3 予想と作用が逆の項目

また，標的型攻撃に関する知識（Q10）は予想に反して詐欺被害を増やす方向に作用しているがうまく解釈できていない．以上，今回の分析では，IT 被害の種別によって影響する因子やその作用の方向が異なることがわかった．サイバー攻撃手法は多様化しており，上記 4 種類を含むさまざまな被害を発端に攻撃者の侵入が始まる．よって対策を行う側としては被害種別にこだわらずに様々な因子を考慮する必要があると考える．

7. まとめ

本論文では，標的型攻撃のユーザ向け対策において，ユーザや部門に応じた対策を提供するシステムの構築を目的に，約 1,000 名の IT 被害経験者から被害の多いユーザを特徴づける因子を抽出した．結果，被害の種別によって因子やその作用が異なることがわかった．今後は，抽出した因子をもとに被害に遭いやすいユーザや部門の見える化を行い，リスクの大きさに応じた柔軟なサイバー攻撃対策につなげていく．

謝辞

本稿の内容には，総務省委託研究「サイバー攻撃の解析・検知に関する研究開発」の成果が含まれます．また，データ分析において多くの助言をいただいた東京大学の高木大資 助教に感謝いたします．

参考文献

1) Thonnard, O. et al.: Industrial Espionage and Targeted Attacks: Understanding the Characteristics of an Escalating Threat, Research in Attacks, Intrusions, and Defenses (RAID'12), LNCS Vol.7462, pp.64-85 (2012).
2) 情報セキュリティ白書 2013，独立行政法人情報処理推進機構 (IPA) (2013).
3) 寺田剛陽，鳥居悟，瀧澤弘和，安野智子，新真知：リスク認知に基づく標的型メール対策，情報処理学会研究報告, SPT-5 (2013).
4) McAfee Security Journal Fall 2008，マカフィー株式会社 (2008). http://b2b-download.mcafee.com/products/japan/pdf/threatreport/McAfee_SJ08F_J.pdf
5) Black Hat USA 2007 - セキュリティの心理学，攻撃者が利用する心の動き，マイナビニュース (2007). http://news.mynavi.jp/articles/2007/08/13/blackhat3/index.html
6) Pfleegar, S. L., Caputo, D. D., Johnson, M. E.: Workshop Report: Cyber Security Through a Behavioral Lens II, The Institute for Information Infrastructure Protection (the I3P) (2011). http://www.thei3p.org/docs/publications/442.pdf
7) リスク認知と実行に関する調査報告書，独立行政法人情報処理推進機構(IPA) (2012). http://www.ipa.go.jp/security/economics/report/behavior/index.html
8) 栗野俊一，吉開範章，高橋俊雄：コンピュータウイルス感染体験実験法の提案と構築，情報処理学会研究報告, CSEC-58 (2012).
9) 『情報セキュリティに関する被害と個人属性』のレポート，独立行政法人情報処理推進機構(IPA) (2012). http://www.ipa.go.jp/about/technicalwatch/20120913.html
10) Lee, M.: Who's Next ? Identifying Risk Factors for Subjects of Targeted Attacks, Virus Bulletin (2012). http://www.virusbtn.com/pdf/conference_slides/2012/MLee-VB2012.pdf
11) 池田利夫：企業内行動履歴解析による情報漏洩メール推定システムの検討，第 26 回 AI 学会全国大会 (2012).
12) Liu, B., Lin, J., Sadeh, N.: Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help ?, Proceedings of the 23rd International Conference on World Wide Web (WWW2014), pp.201-212 (2014). http://dl.acm.org/citation.cfm?id=2568035
13) 中谷内一也 編：リスクの社会心理学，有斐閣 (2012).
14) 木下冨雄，吉野絹子：リスク受容尺度(SRA)の 10 年間の変化(1)－受容得点と因子構造は変わったか，日本社会心理学会 第 48 回大会 (2007). http://www.wdc-jp.biz/cgi-bin/jssp/wbpnew/master/download.php?submission_id=2007-E-0398&type=1
15) 三好昭子：主観的な感覚としての人格特性的自己効力感尺度(SMSGSE)，発達心理学研究 14(2), pp.172-179, 2003.
16) 山岸俊男：信頼の構造－こころと社会の進化ゲーム，東京大学出版会 (1998).
17) 山岸俊男，小見山尚：信頼の意味と構造 －信頼とコミットメント関係に関する理論的・実証的研究－, INSS Journal, 2: pp.1-59 (1995). http://www.inss.co.jp/seika/pdf/2/001.pdf
18) 敷島千鶴ほか：権威主義的伝統主義の家族内伝達―遺伝か文化伝達か―，理論と方法(Sociological Theory and Methods), Vol.23, No.2, pp.105-126 (2008). https://www.jstage.jst.go.jp/article/ojjams/23/2/23_2_2_105/_article/-char/ja/
19) 上市秀雄：後悔予期尺度作成の試み，日本心理学会第 75 回大会, p.859 (2011). http://infoshako.sk.tsukuba.ac.jp/~ueichi/paper/2011_JPA_01_poster.pdf