情報処理学会論文誌 Vol.58 No.12 1890–1900 (Dec. 2017)

SNSにおける情報開示行動に関する要因分析

小川 隆一[1,a)] 安藤 玲未[2,b)] 島 成佳[2,c)] 竹村 敏彦[3,d)]

受付日 2017年3月13日, 採録日 2017年9月5日

概要：標的型攻撃では，攻撃対象（管理者など）に特化したなりすまし・偽装が行われ，それに気づいて未然に攻撃を防ぐことができる人もいるが，ある人はそれに気づかずに引っかかってしまうということが起こる．筆者らは，社会人がSNS上で「帰属組織に関する機密情報を開示する行動（以下，情報開示行動）」にいたる要因について行動科学的アプローチにより分析を試みる．本研究では，過去の情報漏えい事故などの知見から，「ユーザへの信頼」「情報開示範囲のコントロール」「コンプライアンス意識」「リスク認知」「自己顕示性」「情報管理に関する知識」「SNSでつながっている人数」「匿名・非匿名利用」の8つの要因からなる情報開示行動モデルを策定した．この行動モデルを検証するために，インターネットアンケート調査を実施した．その結果，「ユーザへの信頼」「情報開示範囲のコントロール」「リスク認知」「自己顕示性」「情報管理に関する知識」「SNSでつながっている人数」がSNS上での情報開示行動に影響する要因であること，「コンプライアンス意識」の情報開示行動に対する影響はないことを確認した．

キーワード：情報開示行動，SNS（social networking service），ソーシャルエンジニアリング，標的型攻撃

Analysis of Motivating Factors for Information Disclosure in SNS Services

Ryuichi Ogawa[1,a)] Remi Ando[2,b)] Shigeyoshi Shima[2,c)] Toshihiko Takemura[3,d)]

Received: March 13, 2017, Accepted: September 5, 2017

Abstract: APT attacks are often accompanied by spoofing and impersonation customized for cheating the target (such as administrators), so that some of them are not aware of the threat and get into the attackers' trap, while others are aware of it and escape the danger. Based on behavioral science approach, the authors have been analyzing key factors that trigger office workers' behavior such as "disclose confidential information in SNS" and "open APT emails." In this paper we present an information disclosure behavior model comprised by eight factors, based on experiences of the past: "Trust in users," "Information disclosure control," "Compliance awareness," "Risk recognition," "Self-display," "Information management knowledge," "Number of connected SNS users" and "Anonymous/non-anonymous usage." In order to evaluate the model, we performed an internet questionnaire. Its analysis shows that "Trust in users," "Information disclosure control," "Risk recognition," "Self-display," "Information management knowledge" and "Numbers of connected SNS users" are affecting factors for information disclosure behavior in SNS, while "Manners for internet services," "Compliance awareness" are not affecting the behavior.

Keywords: information disclosure, SNS (social networking service), social engineering, APT (advanced persistent threat)

1. はじめに

近年の標的型攻撃のような高度化したサイバー攻撃は，いくつかの攻撃プロセスを経て目的を達成するような複雑

[1] 情報処理推進機構
Information–technology Promotion Agency, Bunkyo, Tokyo 113–6591, Japan
[2] 日本電気株式会社
NEC Corporation, Kawasaki, Kanagawa 211–8666, Japan
[3] 佐賀大学
Saga University, Saga 840–8502, Japan
a) r-ogawa@ipa.go.jp
b) r-ando@ap.jp.nec.com
c) shima@ap.jp.nec.com
d) tosihiko@cc.saga-u.ac.jp

なものとなっている．また，システムのみだけでなく，人間も脆弱点と見なしており，攻撃手段としてソーシャルエンジニアリングも巧みに用いられる．

ソーシャルエンジニアリングは，人間の攻撃認知力の不備や錯覚を突き，システムの利用者や管理者の判断ミスや誤操作を誘発させて，情報窃取やマルウェア感染に用いられる．情報窃取では，攻撃者がターゲットの関係者になりすまし，ターゲットを関係者と誤解させて情報を入手する．また，マルウェア感染でも，攻撃者が関係者になりすまし，ターゲットに標的型攻撃メールを送り，関係者からのメールと信じこませてマルウェア付きの添付ファイルを開かせる．

組織は，ソーシャルエンジニアリングに対処するために，攻撃事例に基づく訓練や教育，注意喚起などの対策を一般的に講じている．しかし，攻撃者は防御側の状況を把握し，ソーシャルエンジニアリングの効果を確かめながら手口を変えて攻撃してくる．このように，ソーシャルエンジニアリングの攻撃では，攻撃側と防御側の間においていたちごっこの様相を呈している．攻撃側と防御側のいたちごっこを止めるには，攻撃者が防御側の状況を把握することを妨害したい．しかし，妨害するには，攻撃者の戦略や防御側の人の脆弱な特徴が明らかになっていない．このため，本研究では，攻撃者の戦略や防御側の人の脆弱な特徴を心理や行動の観点から分析するアプローチをとる．

本研究では，企業を狙う攻撃として標的型攻撃に注目し，ロッキードマーチンのサイバーキルチェーン [1] の攻撃手順を参考にして，攻撃シナリオの流れを作成した．標的型攻撃の攻撃手順では，攻撃者はまず偵察活動としてターゲットの組織の情報を収集する．情報収集の方法として，SNS やウェブサイト，あるいは廃棄される古紙・紙ごみから情報を収集することなどがある．とりわけ，SNS は企業自身がソーシャルメディアを導入しているとともに，企業の従業員なども個人として利用していることが多く，SNS 上での行動は十分な配慮がなされていないこともあわせて指摘されている [2]．そして，SNS を用いた方法は，攻撃者が狙った企業についての情報を提供してくれるだけでなく，コンテンツを投稿しているユーザを通じて個人的な接触の機会も与えてくれる．

このように，SNS を利用すればターゲット組織の情報を容易に収集できるため，SNS ユーザからの情報収集に注目し，偵察活動に SNS を利用するいくつかの記事[*1,*2,*3]を参考に攻撃シナリオを作成した．そして，その攻撃シナリオを基に攻撃対象となる人間が SNS などで不用意に組織の機密情報を開示してしまうケースを想定し，情報開示行動に影響を与える心理的な要因を分析した．ここで，情報開示行動を「不用意に SNS などで重要な情報を開示するなどの適切な範囲以外への情報を開示してしまう行為」と定義する．そして，分析結果から訓練や教育などの対策の一助となる情報を提供する．

本稿の構成は以下のとおりである．2 章では本研究の関連研究を紹介する．3 章では人間をターゲットとするサイバー攻撃の典型である標的型攻撃の攻撃シナリオをあげて，その中でソーシャルエンジニアリングへ対応するための情報開示モデルを示す．4 章では，情報開示モデルを検証するためのアンケート調査の概要について説明する．5 章では，アンケート調査の結果を示し，考察を行う．6 章において本研究のまとめと今後の展望を示す．

2. 関連研究

近年，人間を対象とするサイバー攻撃に対する対応や対策のあり方については，セキュリティエコノミクス（Economics of Information Security）と呼ばれる分野で議論されている．セキュリティエコノミクスは，経済学，社会学，社会心理学，行動科学など広く学際的な分野に知見を援用するアプローチを採用しており，情報セキュリティに関連する事象に対して，個人の利得や効用，社会制度や個人の振舞い，個人の意思決定や認知の観点など幅広いテーマを研究対象としているものである[*4]．日本においても，アンケート調査やインタビュー調査，実験などの手法を用いて，個人の情報セキュリティに関する行動や意識，心理的特性に関するデータを収集し，情報セキュリティに関する行動を規定している要因は何かを探索する試みが行われている．たとえば，リスク認知 [4], [5], [6]，セキュリティ行動・対策の実施状況 [7], [8], [9]，人間心理 [10], [11] などに関する調査や実験を介して，行動や意識に関する分析が行われている．そして，いずれの研究でも Stanton ら [12] が指摘したように，人間自身が脆弱性となっているために，人間（の心理やその不合理な振舞い）に対する対策の重要性が議論されている．また，SNS の利用については近年問題視されている炎上などへの企業としての対応もマネジメント（ソーシャルリスクマネジメント）の観点から議論されるようになっている [13], [14]．

本研究で取り扱う SNS 上での情報開示については，セキュリティエコノミクスの研究テーマの 1 つであるにもかかわらず，これまで注目を浴びてこなかった．しかしながら，この人間の心理につけ込んだ攻撃は増加の一途をたどっており，この問題について早急に解決すべきものであると考える．加えて，この問題はその個人が所属する企業・組織に対しても風評被害や金銭被害などを与えうるものである．特にインターネット上での信頼のあり方に対して 1 つの示唆を与えるものでもあると考える．そのため，本研

*1 http://www.terilogy.com/solution/apt/001a.html
*2 http://www.keyman.or.jp/kc/30006217/
*3 http://blog.trendmicro.co.jp/archives/11627

*4 詳細については，文献 [3] などを参照されたい．

究ではセキュリティエコノミックスでよく試みられるアンケート調査を採用して，研究を進めていく．

3. 標的型攻撃における情報開示

3.1 標的型攻撃

3.1.1 標的型攻撃の手順

標的型攻撃は，特定の相手をターゲットとして，いくつかのプロセスを経て，攻撃目標を達成する攻撃である．標的型攻撃のプロセスは，ロッキードマーチン社が，以下のように偵察から目的実行までを 7 つに分けたものを提唱している [1]．

(1) **偵察**：目的達成のために，ターゲットの組織の情報を収集する．
(2) **武装化**：攻撃に用いる悪意のあるソフトウェア（マルウェアなど）を作成する．
(3) **デリバリ**：ターゲットの組織と通信する手段（メールや Web など）を用いて，ターゲットの組織の情報システムに悪意のあるソフトウェアを送り込む．
(4) **エクスプロイト**：送り込んだ悪意のあるソフトウェアを情報システム上の OS やアプリケーションの脆弱性を利用して実行する．
(5) **インストール**：悪意のあるソフトウェアを情報システムにインストールする．
(6) **コマンド & コントロール**：悪意のあるソフトウェアは攻撃者が操る C2 サーバ[*5]と通信し，攻撃者の命令によってターゲットの組織内の情報システムにある秘密情報を探索する．
(7) **目的実行**：ターゲットの組織から機密情報を盗み出す．

3.1.2 攻撃シナリオ

図 1 は，標的型攻撃のいくつかの過去の事例から，3.1.1 項で示したサイバーキルチェーンに合わせて，標的型攻撃の始まりから発見までの攻撃シナリオを示したものである．

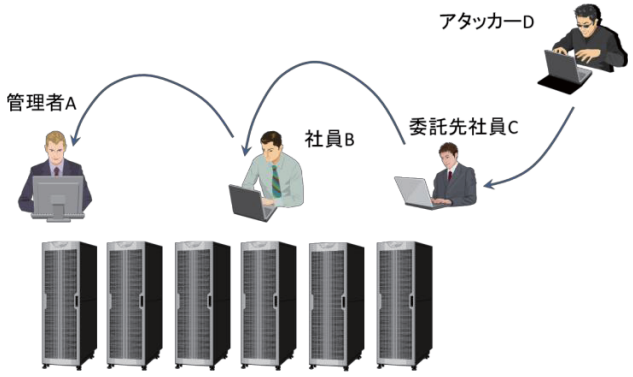


図 1 典型的な標的型攻撃
Fig. 1 Typical targeted attack.

[*5] C2 サーバとは，C & C サーバ（command and control server）を示す用語であり，外部からマルウェアに感染したコンピュータを制御したり命令したりするサーバのことである．

まず，以下に図 1 の攻撃シナリオの登場人物について説明する．

- 管理者 A：N 社のシステムの情報管理部門を統括する管理者
- 社員 B：N 社の社員
- 委託先社員 C：社員 B の部門サーバのソフト開発を請負う M 社の社員
- アタッカ D：N 社の機密情報を狙う攻撃者

次に，図 1 の攻撃シナリオを説明する．

(1) 委託先社員 C からの情報窃取（偵察）

アタッカ D は，N 社の機密情報窃取を目的とし，SNS や Blog，掲示板などを利用して N 社に関する情報を収集しながら，N 社の関係者を探す．そして，SNS 上で N 社の仕事をしていることを公開している委託先社員 C を発見する．

アタッカ D は，N 社の社員を装って委託先社員 C にコンタクトをとると，委託先社員 C はアタッカ D を知り合いである社員 B と勘違いし，アタッカ D と情報交換するようになる．その後，アタッカ D は，委託先社員 C から N 社の業務内容の情報を巧みに引き出す．

(2) 武装化，デリバリ，エクスプロイト，インストール

アタッカ D は，委託先社員 C から得た N 社の情報をもとに，マルウェアを仕込んだ添付ファイル付きの標的型攻撃メールを作成する．アタッカ D は，委託先社員 C になりすまし，社員 B のメールアドレス宛に標的型攻撃メールを送付する．社員 B は，標的型攻撃メールを委託先社員 C からのメールと思い込んで添付ファイルをクリックしてしまい，マルウェアを実行してしまう．そして，社員 B の PC がマルウェアに感染した後に，マルウェアはインターネット上の C2 サーバと通信を開始する．

(3) 管理者 A によるマルウェア感染の発見（コマンド & コントロール，目的実行）

アタッカ D は，C2 サーバから社員 B の PC 上のマルウェアをリモートで操作し，N 社の社内システムを把握しながら機密情報を探索する．そして，機密情報を見つけると C2 サーバに送信する．

管理者 A は，マルウェアから C2 サーバへの通信を Web プロキシのログから発見する．C2 サーバへの通信元である社員 B の PC を特定し，委託先社員 C になりすまして送られてきた標的型攻撃メールが感染原因であることを突き止める．

この攻撃シナリオでは，攻撃者が以下の 2 点でソーシャルエンジニアリングを用いている．

- (1) で，SNS 上で N 社の社員になりすまして，委託先社員 C から情報を引き出すとき．
- (2) で，委託先社員 C からのメールであるかのように標的型攻撃メールを装い，標的型攻撃メールのマルウェア付きのファイルをクリックさせるとき．

本研究では，(1) の偵察活動での対策を講じると，(2) の

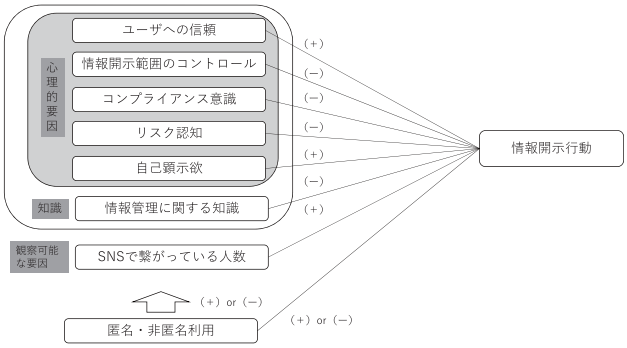


図 2 SNS における情報開示行動モデル
Fig. 2 Model for information disclosure in SNS services.

標的型攻撃メールによる攻撃につながる可能性が低くなり，標的型攻撃の予防になるものとし，(1) の偵察活動において，SNS 上で攻撃者に対して情報開示してしまう行動に注目する．

また，SNS では，ユーザが匿名と非匿名（実名）のどちらかの形態を選択してサービスを利用できる．匿名掲示板では様々な企業情報が書き込まれており，匿名性が情報開示しやすい環境を生んでいるのではないかと考えられる．このため，本研究では匿名と非匿名の環境で情報開示の傾向が異なると考え，匿名と非匿名が情報開示行動に与える要因に関して比較する．さらに，SNS では他の SNS ユーザとつながっている数が多い SNS ユーザほど情報発信を頻繁に行う傾向にあると考え，SNS でつながっている人数が情報開示行動に影響すると仮定する．

3.2 情報開示行動のモデル化

本ユースケースでは，アタッカ D が，攻撃を仕掛けたい N 社の関係者（委託先社員 C）に SNS で接近し，知り合いと信じ込ませて巧みに情報を聞き出すことを想定する．このため，アタッカは委託先社員 C に知り合いと信じ込ませ，委託先社員 C が自ら情報を開示するよう巧みに誘導できる状況にある．

Infosec が公開するコラムから過去の情報漏洩事故例 [15] を考察し，SNS で人が情報を開示する場合，**図 2** で示した 6 つの要因（「ユーザへの信頼」「情報開示範囲のコントロール」「コンプライアンス意識」「情報管理に関する知識」「リスク認知」「自己顕示性」）が以下のように影響すると仮定した．

- 「Twitter や SNS は，普段，自分の友人・知人とのやりとりが多いため，「自分の友人・知人向けに “ここだけの話” を書き込んでいる」と誤解しがちである」という記述から，情報開示の際に相手が信頼できるかどうかや，情報開示範囲を考慮していることがうかがえる．このことから，「ユーザへの信頼」「情報開示範囲のコントロール」を「情報開示行動」に影響する要因としてあげる．
- 「携帯電話キャリアについて『新機種のスマートフォンが発売される』という情報が Twitter に投稿された」という事例から，コンプライアンスの意識や情報管理の知識の欠如が関係していると考える．そして，その影響を認識できていなかったことも考えられる．このことから，「コンプライアンス意識」「情報管理に関する知識」「リスク認知」を「情報開示行動」に影響する要因としてあげる．

  また，誰も知らない新機種の情報を知っていることを示したい欲求を持っていたとも考えられる．このことから，「自己顕示性」を影響する要因としてあげる．

なお，図 2 の “+” は正の関係，“−” は負の関係があることを意味している．たとえば，「ユーザへの信頼」と「情報開示行動」の関係は “+” であると仮説を立てているため，ユーザへの信頼を高めることが情報開示行動をとりやすくさせているということを表している．この中で「情報管理に関する知識」「SNS でつながっている人数」は観察可能な要因，「ユーザへの信頼」「情報開示範囲のコントロール」「コンプライアンス意識」「リスク認知」「自己顕示性」は容易には観察できない心理的要因である．

以下，図 2 で用いている情報開示行動に影響を与える要因の簡単な説明と仮説を紹介する．

ユーザへの信頼

信頼（trust）とは，相手を信用し頼りにすることであり，信用よりも積極的な人間関係を表すとされている [16]．また，信頼（関係）はリスク研究などの分野でも重要な分析概念となっている．信頼関係が築かれることで「この人のことは信頼できる」「この人になら何でも話せる」といった期待感が生まれ，（相手を疑わない限り，善意で）情報を開示しやすくなる．とりわけ SNS において実名登録されている場合，信頼関係が構築されやすいと考えられている．それゆえに，「ユーザへの信頼が高い人ほど，情報開示行動が励起される」という仮説（**仮説 1**）を立てる．

情報開示範囲のコントロール

一般的な情報リテラシと同様に，ネットリテラシを高めることは情報セキュリティの観点から問題となる行動や情報セキュリティインシデント被害や事故に遭遇する可能性を低下させる効果が期待されている．本研究では，過去の情報漏えい事故の例において散見される（ネットリテラシの中でも）情報開示範囲のコントロールができていないこと（第三者に情報が伝わることを自覚していないこと）に注目する．そして，「情報開示範囲のコントロールを意識している人ほど，情報開示行動が抑制される」という仮説（**仮説 2**）を立てる．

コンプライアンス意識

コンプライアンス意識とは，法律や規則といったルールを守ることだけを指すのではなく，社会的規範やモラルを守ることも含んだ概念である [17]．

本研究で考えるような不要な情報開示行動を抑制するには，（形式的な）コンプライアンスの仕組みを整備するだけでは不十分であり，法律や倫理の積極的な遵守に向けた意識改革が必要となる [19]．それゆえに，「コンプライアンス意識が高い人ほど，情報開示行動が抑制される」という仮説（**仮説 3**）を立てる[*6]．

リスク認知

リスク認知とは望ましくない出来事の不確実性に関する主観的な見積り・確率である．これは，リスクは人の認知の仕方によって，見え方や扱い方が変わってしまうことを意味する．そこで，本シナリオで想定しているような自分が所属する企業がサイバー攻撃の標的になっている，あるいは，不特定多数のユーザが交流する SNS で攻撃者が情報を収集しているというリスクのとらえ方は 1 人 1 人異なる．それゆえに，「リスク認知が高い人ほど，情報開示行動は抑制される」という仮説（**仮説 4**）を立てる．

自己顕示性

SNS などにおいて，新技術などのトピックについて議論される場合など，自ら進んで企業内部の情報を開示することがありうる．この動機としては，議論を活性化するという善意と，議論を主導したいという自己顕示性があると考えられる．自己顕示性とは，自己の存在を多くの人の中でことさらにアピールしたいという欲求である [21]．それゆえに，こうした自己顕示的な情報開示は，たとえ企業で規則が存在していたとしても，ついうっかり他者に話してしまうということが起こりうる．そこで，「自己顕示性が強い人ほど，情報開示行動が励起される」という仮説（**仮説 5**）を立てる．

情報管理に関する知識

一般的に，十分な知識があると，理性的な行動が行えるため，情報セキュリティの観点から問題となる行動をとりにくいと考えられている．そのため，教育・トレーニングの充実がこれらの行動を抑止するためには必要とする研究が多く存在する．不要な情報開示行動もまた十分な情報管理に関する知識を持つことで抑制されると考えられる．本研究では，知識でもとりわけ SNS における情報管理に関する知識に注目し，「情報管理に関する知識を持っている人ほど，情報開示行動が抑制される」という仮説（**仮説 6**）を立てる．

SNS でつながっている人数

本研究ではコントロール変数として，SNS でつながっている人数を採用する．SNS でのつながりといっても，実際に面識のある友人などのつながりもあれば，インターネット上だけのものもある．また，上述した要因は観察することが必ずしも容易ではないが，SNS でつながっている人数はある程度観察することが可能となり，もし情報開示行動と関連性が認められれば対策を施す際に有用な情報となる．しかしながら，SNS でつながっている人数（規模）によって情報開示行動がとりやすくなるかとりにくくなるかについては不明である[*7]．そこで，「友人数の多少によって情報開示行動が異なる」という仮説（**仮説 7**）を立てる．

匿名・非匿名利用

SNS の利用が匿名と非匿名の違いにより，上述した要因が情報開示行動に対して与える影響の大きさが異なるか否かについても関心がある．そこで，「SNS の利用が匿名か非匿名かの違いにより，上述した要因が情報開示行動に対して与える影響の大きさが異なる」という仮説（**仮説 8**）を立てる．

4. アンケート調査

アンケート調査は SNS のようなオープンな空間で人が情報を開示する際，人の情報開示行動を把握することを目的としている．SNS 上で攻撃者の情報収集と分からずに，SNS ユーザが情報を開示することが考えられる．そこで，社会人の SNS ユーザが日常経験するケースとして，知人の要請に対して自分の業界に関する情報を開示するか否かを問うシナリオを作成した．

調査対象者は，週 1 回以上，Facebook，mixi，ブログなどを利用して情報の発信を行っている社会人としている．アンケート調査は，調査対象者であるかを調べるための事前調査を実施し，その中から条件を満たす 1,000 人を抽出し，本調査に回答してもらうという 2 段階の方式を採用している[*8]．調査期間は 2015 年 3 月 20 日から 3 月 21 日である．

アンケート調査は，調査会社が保有する Web アンケートシステムおよびモニタ会員を用いて実施した．今回，このインターネットアンケート調査手法を用いた理由は SNS やメールを利用している人を一定数確保するためである[*9]．回答者の構成は**表 1** に示すように，性別と年齢構成に偏りがないように等サンプルをとることとした．

本研究の分析で用いるアンケート調査の主要な質問内容は付録 A.1 に示している．質問内容は，ソーシャルメディアを介してつながる知人（同業種の会社社員）を前提としたシナリオに基づき，「情報開示行動」「ユーザへの信頼」「情報開示範囲のコントロール」「リスク認知」「自己顕示性」

[*6] 本研究ではコンプライアンスの仕組みの整備ではなく，個人のコンプライアンス意識に注目する．それは企業に属する個人の行動すべてをルールによって規定することはできないためである [18]．

[*7] その人数が多いということは面識のない不特定多数とつながっている可能性が高い．

[*8] 分析に際して，欠損値などがあったために，分析に用いることができる最終の観測数は 853 人である．

[*9] この調査形式はサンプルが無作為に抽出されていないなどの統計的な問題が指摘されている．しかしながら，調査の目的が個人や組織の意思決定の 1 つの有益な判断材料を提示することであれば，この方法を採用することに意義がある [20]．

表 1 調査対象者の構成
Table 1 Demographic information about the respondents.

	男性	女性
20–29 歳	125	125
30–39 歳	125	125
40–49 歳	125	125
50–59 歳	125	125
小計	500	500

に関する問いである[*10]．また，社会や会社への「コンプライアンス意識」に関する質問もある．これ以外にもオフラインやオンラインにおける情報の開示のしやすさなどに関する質問 [11] もあり，質問総数は 17 問である．これらの質問内容は文献 [4], [21] などで用いられているものに準拠して本アンケート調査のために一部カスタマイズを行った．

5. 分析

5.1 変数の加工・因子分析

本研究で用いる説明変数および被説明変数のいくつかは単項目ではなく，それらを適切に測定すると考えられる複数の質問項目によって構成されている．そのために，階層的重回帰分析（hierarchical multiple regression）を行う前に要因の作成および加工を行う必要がある．以下，簡単ではあるがその手順を示す．

被説明変数およびいくつかの説明変数（「情報開示行動」「ユーザへの信頼」「情報開示範囲のコントロール」「コンプライアンス意識」「リスク認知」「自己顕示性」）に関して，質問項目から作成される変数（構成概念）を作成するために因子分析を行う．

本アンケート調査で得られた質問項目のうち「情報開示行動」「ユーザへの信頼」「情報開示範囲のコントロール」「コンプライアンス意識」「リスク認知」「自己顕示性」（付録 A.1 参照）は，準拠した先行研究・調査にならい，5 段階のリッカード尺度で回答を求めている．これらの質問項目から構成される変数の信頼性を確認するため，因子分析に先駆けてクロンバックの α 信頼性係数を求めた（**表 2**）．その結果，表 2 に示したいずれの変数の α 信頼性係数も 0.60 を大幅に上回っており，信頼性を有していると判断できる[*11]．

[*10] いくつかの企業では，すでにソーシャルメディアに関するポリシやガイドラインにおいて第三者への情報開示行動自体を禁止しているところがある．このとき，情報提供を対面で行うと想定して回答しても，ソーシャルメディアを介して情報提供を行うことを想定して回答しても，その個人はその内容によってはコンプライアンス違反になりうる．アンケート調査では情報開示行動についての意識（この行動のとりやすさ）を測っているため，特に具体的な情報提供の方法（媒体）についての情報をシナリオ内では触れていない．しかしながら，情報提供の方法も行動意図に影響を与えうる可能性は否定できない．この点の改良については今後の課題としたい．

[*11] クロンバックの α 信頼性係数が 0.60 以上であればその変数の信頼性・再現性は高いと考えられている [22]．

表 2 クロンバックの α 信頼性係数
Table 2 Cronbach's coefficient α.

	質問項目数	α
情報開示行動	5	0.879
ユーザへの信頼	5	0.731
情報開示範囲のコントロール	3	0.704
コンプライアンス意識	4	0.854
リスク認知	3	0.855
自己顕示性	4	0.897

次に，これらの質問項目を用いて因子分析を行い，そこから各変数の因子得点を計算した．各変数は表 2 にあるその名前のとおり，計算された値が大きくなるほどその傾向が強い（程度が大きい）ことを表す．たとえば，「情報開示行動」の数値（因子得点）が大きいほど，情報開示をしやすいことを意味している．これらの因子分析の結果は付録 A.2 の**表 A·1** にまとめている．

「情報管理に関する知識」は，付録 A.1 に示した情報管理に関する 4 問のクイズの正答数でもって知識水準を表すものとする．この要因は 0 点から 4 点の範囲の値をとり，得点が高いほど情報管理に関する知識が高いことになる．なお，本アンケート調査から，情報管理に関する知識の平均値は約 1.65 点（中央値は 2 点）となっている．

本アンケート調査では，Facebook，mixi，ブログを利用してつながっている人数を質問しており，その回答人数を「SNS でつながっている人数」として分析に用いる．回答が得られたその人数の平均値は約 148.1 人（中央値は 50 人）となっている．なお，SNS でつながっている人数の分散が大きいため，SNS でつながっている人数の対数をとり，分析に用いることとした．また，人数が分からないもしくは覚えていないと回答した回答者は分析から除外している．

このほかにも，本アンケート調査では SNS を匿名で利用しているかどうかについても質問している．アンケート調査結果から，匿名で利用している回答者の割合は約 33%であることが分かった[*12]．本研究では，非匿名で利用している回答者には 1，そうでない回答者には 0 を付与するダミー変数を作成した．

5.2 階層的重回帰分析

階層的重回帰分析は，階層構造を持たせてモデルを構築することで，説明力が増加するかどうかや，変数間の媒介関係を検討することを目的としている回帰分析である（いい換えると，回帰分析を複数のステップに分けて実行し，追加のステップで説明力が増加するかどうかを検討するものである）．階層的重回帰分析については文献 [23] などが詳しいので参照されたい．

[*12] 複数の SNS を利用している回答者の中には匿名・非匿名両方で利用している者もいる．そのため，匿名・非匿名両方で利用している回答者は非匿名での利用意図を持っているということもあり，非匿名利用をしている回答者として取り扱っている．

表 3 階層的重回帰分析の結果
Table 3 Results of hierarchical multiple regression analyses.

	ステップ 1			ステップ 2		
	係数	t-value	β 係数	係数	t-value	β 係数
ユーザへの信頼	0.282***	7.130	0.254	0.276***	5.540	0.248
情報開示範囲のコントロール	−0.358***	−8.330	−0.297	−0.326***	−6.190	−0.271
コンプライアンス意識	0.018	0.500	0.017	0.011	0.270	0.010
リスク認知	−0.068*	−1.860	−0.063	−0.095**	−2.130	−0.087
自己顕示性	0.196***	5.400	0.190	0.150	3.330	0.146
情報管理に関する知識	−0.082***	−2.740	−0.076	−0.058	−1.560	−0.054
ln（つながっている人数）	0.030*	1.600	0.042	0.050**	2.130	0.071
匿名ダミー				0.290	1.510	0.137
匿名ダミー × ユーザへの信頼				−0.013	−0.160	−0.008
匿名ダミー × 情報開示範囲のコントロール				−0.101	−1.110	−0.052
匿名ダミー × コンプライアンス意識				0.025	0.300	0.012
匿名ダミー × リスク認知				0.077	0.960	0.040
匿名ダミー × 自己顕示性				0.104	1.370	0.065
匿名ダミー × 情報管理に関する知識				−0.064	−1.030	−0.061
匿名ダミー × ln（つながっている人数）				−0.040	−1.000	−0.076
（定数項）	0.022	0.230		−0.119	−0.970	
観測数	853			853		
F-value	$F(7, 845) = 87.10$***			$F(15, 837) = 41.62$***		
Adj R-squared	0.414			0.417		
R-squared	0.419			0.427		
Δ R-squared				0.0081		
(F-value)	2.58*			1.48		

*: $p < 10\%$, **: $p < 5\%$, ***: $p < 1\%$

情報開示行動を被説明変数とする回帰分析の結果を**表 3** に示している[*13]．表 3 の β 係数は平均 0，分散 1 と標準化したもので，係数間の比較を可能とする標準化係数，t-value は個別係数の有意性を検定するための t 値，F-value はモデルの有意性を検定するための F 値をそれぞれ表す[*14]．表 3 のステップ 1 は基本的な分析であり，ステップ 2 は匿名ダミー，さらに匿名ダミーと各変数の交差項をとっているものを追加した分析の結果を表している[*15]．

表 3 にある Δ R-squared はステップ 1 とステップ 2 での R-squared（決定係数）の変化量を表しており，その値は 0.0081 である．この変化量が有意であるかについては Δ R-squared の下の F 値を見てみると，10%水準で有意にならないことが確認できる．つまり，匿名ダミー，および匿名ダミーと各変数の交差項をとっているものを加えることは有意に説明力を高めることにつながらないことが分かる．

続いて，表 3 のステップ 1 における「ユーザへの信頼」「情報開示範囲のコントロール」「自己顕示性」「情報管理に関する知識」の係数は 1%水準，「リスク認知」「ln（SNS でつながっている人数）」の係数は 10%水準でそれぞれ有意である．また，ステップ 2 における「ユーザへの信頼」「情報開示範囲のコントロール」「自己顕示性」の係数は 1%水準，「リスク認知」「ln（SNS でつながっている人数）」の係数は 5%水準でそれぞれ有意である．「情報開示範囲のコントロール」「リスク認知」「情報管理に関する知識」の係数は負の値，これ以外の有意となった変数の係数は正の値をとっている．この結果は，たとえば「情報管理に関する知識」の係数は負なので，その水準が高いほど，情報開示行動をとりにくいことを意味する．

一方，「コンプライアンス意識」ならびに「匿名ダミー」と他の変数との交差項の係数はいずれのステップにおいても統計的に有意ではないことが分かった．

さらに，有意となった標準化係数の絶対値を見てみると，いずれのステップにおいても「情報開示範囲のコントロール」の係数が一番大きくなっている（その影響度はステップ 1 では 0.297，ステップ 2 では 0.271 である）．このことから「情報開示範囲のコントロール」が情報開示行動に最も大きな影響を与えうる要因であることが分かった．

*13 統計ソフトウェアとしては Stata MP 14.2 を用いた．
*14 β 係数や各統計量・検定方法などについては文献 [24] などを参照されたい．
*15 SNS の利用が匿名と非匿名のケースに分けて分析を行うことができるが，それでは推計された係数の大きさを直接比較することができない．本研究では仮説 8 を検証したいために，すべての要因について匿名ダミーとの交差項をとり，両者の大きさの違いを比較できるようにしている．

5.3 考察

分析結果から，3.2 節で立てた仮説 1 および仮説 2，仮説 4，仮説 5，仮説 6，仮説 7 は支持されたが，仮説 3 および仮説 8 は支持されなかった．以下，情報開示行動に大きな影響を与えている「ユーザへの信頼」（仮説 1），「情報開示範囲コントロール」（仮説 2）および「匿名・非匿名利用」（仮説 8）を中心として考察を行う．

- ユーザへの信頼

SNS ユーザはインターネット上の他のユーザを信頼する傾向が高いほど情報開示傾向が高くなることから，対策として他のユーザを安易に信頼しないことを認識させることが重要である．これを認識させるには，他のユーザを信頼して情報を提供してしまうと組織の機密情報漏えいにつながり，組織やユーザが不利益を受けてしまうことを理解させることが有効と考える．そして，総務省のインターネットトラブル事例集 [25] の「3. 誘い出し・なりすまし」や「4. 個人情報漏えい」を用いて，ユーザに不利益を受ける事例を示すことで理解が深まると考える．また，ユーザに不利益を認識させることは，「リスク認知」の向上の効果にも期待でき，情報開示行動の低減に高い効果があると考える．

また，SNS ユーザは，攻撃者がなりすましを行って信頼させてくることを考え，直接会った相手でなければ信頼しないぐらい気を付けるべきである．ただし，一般的に SNS 上で組織の機密情報をやりとりするべきではない．

- 情報開示範囲コントロール

SNS ユーザは，情報開示範囲のコントロールを意識している人ほど，情報開示行動が抑制されることから，対策として他のユーザに提供する情報を考慮すべきことを認識させることが重要である．

SNS の利用目的としては，「知人とのコミュニケーション」「趣味・嗜好を同じくする人を探す」の比重が大きいことが報告されている [26]．SNS ユーザは，知人や新たに知り合う人との情報交換などの交流を期待していることから，相手との交流を深めるために必要以上の情報を与えてしまう可能性が高い．このため，相手に悪意のあるかもしれないことを考慮し必要以上の情報を提供しないことを理解させるべきである．同時に，所属する組織の情報を開示させないために組織の情報管理のルールを作り，SNS 上で情報発信の際に気を付けることをユーザに徹底させる必要がある．

この 2 つの要因以外では，「自己顕示性」の高いユーザや「つながっている数」の多いユーザに対し，ユーザ自身が情報開示しやすい傾向があることを認識させて，日頃から情報管理を注意するように促すことが重要である．また，「リスク認知」「情報管理に関する知識」は「ユーザへの信頼」「情報開示範囲コントロール」と比べて情報開示行動への影響が小さいことから，「リスク認知」「情報管理に関する知識」を高める演習や教育は大きな効果が期待できないと考えられる．しかし，標的型攻撃の未然防止に関して少しでも貢献するためには，「リスク認知」や「情報管理に関する知識」を高める演習や教育を実施することが望ましい．

- 匿名と非匿名

分析結果は，仮説と異なり，情報開示に影響を与える要因に対して，匿名と非匿名の間で統計的な差が見られなかった．匿名は，機密情報を開示する際に情報発信者の特定を困難にする．匿名と非匿名で差がなかったことから，ユーザは SNS 上で機密情報を開示する際に，情報発信者を特定されることを気にしていないと考えられる．このことは，SNS ユーザがお互いに特定できたからこそ，機密情報を開示するのではないかとも推測できる．

6. おわりに

本研究では，標的型攻撃の攻撃シナリオをもとに仮説となる SNS 上のユーザの情報開示行動モデルを作成し，アンケート調査の結果から情報開示行動に影響を与える要因の探索を行った．その結果，図 2 において「コンプライアンス意識」「匿名・非匿名利用」は情報開示行動に影響を与えないが，「ユーザへの信頼」「情報開示範囲のコントロール」「リスク認知」「自己顕示欲」「SNS でつながっている人数」は情報開示行動に影響を与えることを確認した．図 2 で示したモデルの基本部分はある程度妥当性があると主張することができる．

本研究の仮説モデルの構築は攻撃シナリオに基づいており，攻撃シナリオの作り方によって本情報開示行動モデルを拡張することは可能である．たとえば，3.1.2 項で示した標的型攻撃メールの添付ファイルをユーザがクリックするシナリオにも適用可能である．また，フィッシングやランサムウェアを用いた攻撃でも攻撃シナリオを作成することで，本研究のように人間の脆弱な部分を分析できる．

最後に，今後の研究の展望について簡単に述べる．本研究ではアンケート調査から収集されたデータを用いて，情報開示行動の分析を行った．しかしながら，よりリッチなモデルの構築のためにはインタビュー調査や実験などの結果を用いた分析も必要である．その意味において本研究での分析は情報開示行動の分析の第 1 ステップであり，今後アンケート調査以外の調査手法を用いてさらなる分析を行っていきたい．加えて，今後もシステムの脆弱性に対しての対策が強化されていくことによって，攻撃者は人間の脆弱性を利用する攻撃を多用してくるのではないかと予想する．また，新たなシステムやデバイス，サービスなどが提供され使われることで，新たな人間への攻撃も発生すると予想する．このため，今後ソーシャルエンジニアリング対策の重要性がさらに増していくと考える．

参考文献

[1] Hutchins, E.M., Cloppert, E.M. and Amin, R.M.: Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chain (2010).
[2] クリストファー・ハドナジー：ソーシャル・エンジニアリング：最大の弱点 “人間” をハッカーの魔の手から守るためには，日経 BP 社 (2012).
[3] Anderson, R. and Moore, T.: Information Security: Where Computer Science, Economics and Psychology Meet, *Phil. Trans. R. Soc. A.*, Vol.367, pp.2717–2727 (2009).
[4] 独立行政法人情報処理推進機構：eID に対するセキュリティとプライバシーに関するリスク認知と需要の調査報告 2010 (2010).
[5] 熊谷洋子，島　成佳，小松文子，竹村敏彦：個人情報活用オンラインサービスに対する信頼感と利用意図に関する要因分析，日本セキュリティ・マネジメント学会誌，Vol.27, No.2, pp.3–15 (2013).
[6] 寺田剛陽，鳥居　悟，安野智子，瀧澤弘和，新　真知：リスク認知に基づく標的型メール対策の検討，情報処理学会グループウェアとネットワークサービス研究会技術報告，Vol.IPSJ-GN-88, No.9 (2013).
[7] 独立行政法人情報処理推進機構：リスク認知と実行に関する調査報告書 (2012).
[8] 小松文子，高木大資，松本　勉：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実験，情報処理学会論文誌，Vol.51, No.9, pp.1711–1725 (2010).
[9] 寺田剛陽，津田　宏，片山佳則，鳥居　悟：IT 被害に遭いやすい心理的・行動的特性に関する調査，DICOMO2014, pp.1498–1505 (2014).
[10] 小川隆一，島　成佳，福住伸一，角尾幸保：高度化したサイバー攻撃対策の心理学的アプローチについて，SCIS2015, 4D1–1 (2015).
[11] 安藤玲未，島　成佳，竹村敏彦：組織情報の外部提供に関する分析と考察，DICOMO2015 (2015).
[12] Stanton, J.M., Stam, K., Mastrangelo, P. and Jolton, J.: Analysis of End User Security Behaviors, *Computers and Security*, Vol.24, No.2, pp.124–133 (2005).
[13] 千葉直子，関　良明，橋元良明：従業員の Twitter 利用における情報漏えいリスクアセスメント：企業におけるリスク管理策の実態と有効性，電子情報通信学会技術研究報告，ライフインテリジェンスとオフィス情報システム，Vol.113, No.479, pp.131–136 (2014).
[14] 田村滋基，小川隆一，竹村敏彦：悪意のある投稿をする人の特性分析，SCIS2017 (2017).
[15] 田中　洋：「日常業務に潜むセキュリティの脅威」SNS 編「身近で起こるソーシャルメディアのセキュリティ事故—Twitter・SNS から情報漏洩!?」(2011)，入手先 ⟨https://www.infosec.co.jp/column/2011/⟩.
[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] 浜辺陽一郎：コンプライアンスの考え方—信頼される企業経営のために，中央公論新社 (2005).
[18] 竹村敏彦，三好祐輔，花村憲一：情報漏えいにつながる行動に関する実証分析，情報処理学会論文誌，Vol.52, No.12, pp.2191–2199 (2015).
[19] Siponen, M.: A Conceptual Foundation for Organizational Information Security Awareness, *Information Management and Computer Security*, Vol.8, pp.31–41 (2000).
[20] 労働政策研究・研修機構：インターネット調査は社会調査に利用できるか，労働政策研究報告書，No.17 (2005).
[21] 吉田富二雄，宮本聡介：心理測定尺度集 V：個人から社会へ〈自己・対人関係・価値観〉，サイエンス社 (2011).
[22] Hair, Jr., J.F., Anderson, R.E., Thatham, R.L. and Black, W.C.: *Multivariate Data Analysis*, Prentice-Hall International (1998).
[23] Greene, W.H.: *Econometric Analysis, 7th edition*, pp.639–641, Prentice Hall (2012).
[24] 永吉希久子：行動科学の統計学：社会調査のデータ分析，共立出版 (2016).
[25] 総務省：インターネットトラブル事例集（平成 28 年度版）(2016).
[26] 総務省：情報通信白書 平成 23 年度版, pp.155–181 (2011).

付　　録

A.1 アンケート調査の質問項目

本研究の分析で用いたアンケート調査の主要な質問項目を以下に示す．

情報開示行動

ソーシャルメディアを通して，久しぶりに昔からの知人（同業種の会社社員）から直接連絡がありました．その知人は競合他社状況に関する資料作りで困っているらしく，時間もないとのことで，同業種であるあなたに情報を教えてほしいとのお願いがありました．

困っている知人に以下の情報を提供しようと思うかについて，あなたの気持ちに最も近いものを「全くそう思わない」「あまりそう思わない」「どちらとも言えない」「まあそう思う」「とてもそう思う」のうちからそれぞれ 1 つだけお選びください．

(1) 会社の Web ページの公開情報
(2) 自分が調べた他社の情報
(3) 自社が調べた他社の情報
(4) 取引先関係者との情報交換により得た情報
(5) 自社の売上目標や製品計画等の情報

ユーザへの信頼

以下の主張に対して，あなたの考え方・気持ちに最も近いものを「全くそう思わない」「あまりそう思わない」「どちらとも言えない」「まあそう思う」「とてもそう思う」のうちからそれぞれ 1 つだけお選びください．

(1) インターネット上で，出会う人たちのほとんどは信頼できる．
(2) インターネット上で，出会う人たちについて信頼できる人と信頼できない人を見分ける自信がある．
(3) インターネット上では，困ったときにお互いに助け合うというルールが守られない．
(4) インターネット上で，世のため，人のために頑張ることは，自分が損をすることだ．
(5) インターネット上で，自分の利益を中心に行動することは，非難されることではない．

情報開示範囲のコントロール

以下の主張に対して，あなたの考え方・気持ちに最も近

いものを「全くそう思わない」「あまりそう思わない」「どちらとも言えない」「まあそう思う」「とてもそう思う」のうちからそれぞれ 1 つだけお選びください．

(1) 仮名を使って SNS を利用していれば，あなたが誰であるか本人を特定されることはないと思う．
(2) 自分の知人・友人同士であれば，その間で多くの情報をシェアしたいと思う．
(3) 公私関係なく多くの情報を知人・友人に提供したいと思う．

コンプライアンス意識

以下の主張に対して，あなたの考え方・気持ちに最も近いものを「全くそう思わない」「あまりそう思わない」「どちらとも言えない」「まあそう思う」「とてもそう思う」のうちからそれぞれ 1 つだけお選びください．

(1) 判断や行動をする際は，社会の価値基準を気にする．
(2) 社会のルールや手順を守って生活をしている．
(3) 私は社会的に誇りを持って生活している．
(4) 私は社会的責任をよく理解している．

リスク認知

以下の主張に対して，あなたの考え方・気持ちに最も近いものを「全くそう思わない」「あまりそう思わない」「どちらとも言えない」「まあそう思う」「とてもそう思う」のうちからそれぞれ 1 つだけお選びください．

(1) SNS では，自分の情報が意図せずに拡散してしまうかもしれない．
(2) SNS では，自分の書き込みによって，会社の情報や同僚のプライバシー情報が拡散してしまうかもしれない．
(3) 複数のサイトで ID・パスワードを同じにしていると，自分のアカウントが乗っ取られてしまうかもしれない．

自己顕示性

以下の主張に対して，あなたの考え方・気持ちに最も近いものを「全くそう思わない」「あまりそう思わない」「どちらとも言えない」「まあそう思う」「とてもそう思う」のうちからそれぞれ 1 つだけお選びください．

(1) SNS で注目を集めるために，事実よりもおおげさな表現にすることがある．
(2) SNS で派手な発言や写真で，人目を引こうとすることがある．
(3) SNS では，自分はちょっと目立ちたがり屋である．
(4) SNS で目立つことが，いやではない．

情報管理に関する知識

以下の項目について，概要や特徴に関する説明が「正しい」か「間違っている」かをお選びください．わからない場合は「わからない」をお選びください．

(1) インターネット上で広告をクリックしても個人情報 (名前，年齢，購入履歴，行動履歴等) は，収集されることがない．
(2) 写真を公開しても背景に気をつけていれば，撮影場所が特定されることがない．
(3) 個人情報を設定によって適切にコントロールすれば情報漏洩を防止できる．
(4) インターネット上に漏洩した情報は消すことが可能な技術はない．

SNS で繋がっている人数

Facebook，mixi，ブログを利用して，あなたが繋がっている人のおおよその人数をお書きください．なお，わからない・覚えていない場合は「わからない・覚えていない」をお選びください．

匿名・非匿名利用

あなたは，Facebook，mixi，ブログを匿名または非匿名のどちらで利用していますか．該当するものを「匿名」「非匿名」「どちらも」のうちから 1 つだけお選びください．

A.2 因子分析の結果

表 A·1 は，本研究で用いた因子分析の結果（因子負荷量と独自性）をまとめたものである．なお，因子負荷量とは質問項目に対して共通（潜在）因子がどれくらいの強さで影響を与えているかを示すものであり，また独自性は質問項目独自の変動を表すものである．因子分析について詳しくは文献 [24] を参照されたい．

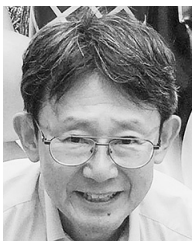
「ユーザへの信頼」において質問項目 (3)「インターネット上では，困ったときにお互いに助け合うというルールが守られない」の共通因子の値は 0.3935 と 0.40 を若干下回って低いものの，他の質問項目についてはおおむね因子負荷量の値は比較的大きなものとなっている．

表 A·1 に示した因子分析の結果を用いて因子得点を計算している．ユーザへの信頼については因子得点が高いほど，ユーザへの信頼が高いこと，また情報開示範囲のコン

表 A·1 因子分析
Table A·1 Results of factor analyses.

#	因子負荷量	独自性	#	因子負荷量	独自性
情報開示行動			ユーザへの信頼		
(1)	0.4157	0.8272	(1)	0.6744	0.5453
(2)	0.8168	0.3328	(2)	0.6319	0.6007
(3)	0.8998	0.1904	(3)	0.3935	0.8452
(4)	0.9001	0.1899	(4)	0.6296	0.6036
(5)	0.8601	0.2602	(5)	0.6057	0.6331
情報開示範囲のコントロール			コンプライアンス意識		
(1)	0.5542	0.6929	(1)	0.7111	0.4944
(2)	0.6231	0.6117	(2)	0.7867	0.3810
(3)	0.7189	0.4832	(3)	0.7354	0.4592
			(4)	0.7996	0.3606
リスク認知			自己顕示性		
(1)	0.8190	0.3293	(1)	0.8093	0.3450
(2)	0.7970	0.3648	(2)	0.8772	0.2305
(3)	0.7491	0.4388	(3)	0.8478	0.2812
			(4)	0.7510	0.4360

トロールについては因子得点が高いほど，情報開示範囲動のコントロールを意識していること，コンプライアンス意識については因子得点が高いほど，コンプライアンス意識が高いこと，リスク認知については因子得点が高いほど，リスク認知が高いこと，自己顕示性については因子得点が高いほど，自己顕示性が強いことを表している．



小川 隆一 （正会員）

1983 年東京大学理学系大学院修士課程修了．同年日本電気株式会社入社．画像データベース，システムセキュリティ，クラウド標準化の研究開発に従事．2015 年 10 月から情報処理推進機構にて調査分析事業に従事．電子情報通信学会，情報ネットワーク法学会各会員．

安藤 玲未 （正会員）

2012 年お茶の水女子大学大学院博士前期課程修了．同年日本電気株式会社入社．現在，セキュリティ研究所にて，セキュリティの研究開発に従事．

島 成佳 （正会員）

1997 年北陸先端科学技術大学院大学情報科学研究科博士課程前期修了．同年日本電気株式会社入社．2010 年（独）情報処理推進機構に研究員として出向．2012 年電気通信大学大学院情報システム学研究科博士課程後期修了．2013 年 4 月より日本電気株式会社に在籍．現在，セキュリティ研究所にて，サイバーセキュリティの研究開発に従事．博士（工学）．電子情報通信学会会員．

竹村 敏彦 （正会員）

1975 年生．1998 年関西大学総合情報学部卒業．2002 年大阪大学大学院修士課程修了．2006 年同博士課程修了．博士（応用経済学）．2005 年関西大学ポストドクトラルフェロー．2008 年関西大学助教．2013 年佐賀大学准教授．セキュリティエコノミックスの研究に従事．日本経済学会，日本経済政策学会，公益事業学会，日本情報経営学会各会員．