SNS ユーザのパスワード管理に関する実証分析

竹村 敏彦† 田村 滋基‡ 児玉 弘†

†佐賀大学
840-8502 佐賀県佐賀市本庄町 1
tosihiko@cc.saga-u.ac.jp
hkodama@cc.saga-u.ac.jp

‡情報処理推進機構
113-6591 東京都文京区本駒込 2–28–8
s-tamura@ipa.go.jp

あらまし 近年, パスワード管理の不徹底に起因するインシデント被害の報告が増えている. そこで本研究では, 2015 年 3 月に SNS ユーザを対象に実施したアンケート調査の結果を用いて, 行動経済学・社会心理学の視点からパスワード設定・管理等に関する行動に影響を与えている要因を探索した. その結果, パスワード管理に影響を与える要因として「判断力」「プライバシー性に関する意識」があることが確認された. このことから, 判断力やプライバシー性に関する意識を向上させることで, 適切なパスワード管理を行うようになることが示唆された.

An Empirical Analysis on SNS Users' Password Management

Toshihiko Takemura† Shigeki Tamura‡ Hiroshi Kodama†

†Saga University.
1 Honjo-machi, Saga, 840-8502, JAPAN
tosihiko@cc.saga-u.ac.jp
hkodama@cc.saga-u.ac.jp

‡Information-technology Promotion Agency, Japan.
2–28–8 Honkomagome, Bunkyo–ku, Tokyo 113–6591, JAPAN
s-tamura@ipa.go.jp

Abstract Recently, it is reported that the number of security incident accident related to the inadequate password management have been increasing. In this article, we investigate the factors which have impacts on the password management from the viewpoint of behavioral economics and social psychology by using micro-data collected from the survey which we conducted. As a result, we confirmed that factors such as "capacity for judgment" and "awareness with regard to the privacy" influence on the password management. This result implies that improving capacity for judgment and/or heightening awareness with regard to the privacy lead to the adequate password management.

1 はじめに

近年, スマートフォンの登場とともに Facebook や Twitter などのソーシャル・ネットワーキング・サービス（Social Networking Service; SNS）やオンラインショッピング, オンラインバンキングの利用者数は増加傾向にある（文献 [1] など）. 誰でも簡単に SNS を利用できる環境が整う一方で, 文献 [2] などでも報告されているように, LINE の乗っ取り事件のような SNS のアカウント乗っ取りなどのインシデント被害が増

加している. このような被害に遭遇する一因として, SNS のアカウントおよびそのパスワードの設定・管理が適切でないことが挙げられる. つまり, ユーザが利用するネットワークサービス数が増えるほど, 管理すべきパスワードの数も同時に増えていき, ユーザは記憶の負荷を避けるために, パスワードを使い回ししてしまったり（文献 [3]）, 強度の高くないパスワード（誕生日や辞書に載っている単語などの類推しやすいものなど）を設定してしまったりする可能性が生まれてしまう. 言い換えると, パスワード環境の変化にともない, ユーザのパスワード管理が適切に行われにくい状況になりつつあるといえる. そのため, 適切なパスワード管理・設定が行われなければ, 類推攻撃やパスワードリスト攻撃などをはじめとするサイバー攻撃によるアカウント乗っ取り被害に遭遇するリスクを高めてしまうことになる.

本研究では, 行動経済学や社会心理学の視点からパスワード設定・管理に影響を与えている要因を探り, パスワードの使い回しなどを行うユーザに対して適切にパスワード管理をするためにはどのようなことをすればよいかについて考察することを目的とする. この目的を達成するために, 著者が 2015 年 3 月に実施したインターネット調査によって収集した個票データを用いた統計分析を行う.

2 関連研究

行動科学や社会心理学の視点から, パスワードの管理に関する行動特性について研究が行われているのでそのいくつかを紹介する[1].

文献 [5] はユーザのリスク認知がパスワードの文字長や更新回数といったパスワード管理に影響を及ぼしていることを明らかにしている. また, 文献 [6] は e コマースサイトのパスワードを対象に強度評価を行い, パスワードの文字長の平均は 7.37 字でその約 6 割はアルファベットのみで構成されていたことを明らかにしている. 文献 [7] はパスワードの管理には限界合理性や便宜主義（opportunism）といったヒューマンファクターなどがパスワード管理に影響を与えることを確認している.

この他にも, 文献 [8] では Yahoo!ユーザのパスワード約 7 千万件を収集したデータを用いて, パスワード強度とユーザの属性（性別, 年齢, 言語など）との関連を検討し, 若年者が年長者よりも簡単なパスワードを用いる傾向にあることを指摘している.

3 アンケート調査

本研究では, 2015 年 3 月に実施した「SNS ユーザの情報セキュリティ意識および行動に関する調査 2015」（以下, 「調査」と略す）と題したインターネットアンケート調査によって収集した個票データを用いて分析を行う. 本研究では, モニターパネルなどを利用し彼らの情報を基にサンプリングを行ってアンケートを実施する「クローズ型」のインターネット調査形式を採用した. この調査形式を採用した理由として, 調査環境の劇的な変化（回収率の低下, プライバシーや個人情報保護法への過剰反応による拒否率の上昇など）に加えて, 効率よく調査対象者を抽出するためである. この調査法はサンプルが無作為に抽出されていない等の統計的な問題が指摘されている. しかしながら, 文献 [9] でも述べられているように, 調査の目的が個人や組織の意思決定の一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. また, 本研究の結果は現時点では日本の SNS ユーザ全てに対して妥当性をもつとまでいえないが, 少なくとも調査会社にモニターとして参加している SNS ユーザに対して妥当性を有していることは主張できる. 勿論, 調査の正確性について議論する必要がある. この調査手法の詳細な利用可能性・妥当性については文献 [10] などを参照されたい.

この調査の目的は SNS ユーザの情報セキュリティ意識および行動を把握し, 情報セキュリティ教育のあり方などに関する情報を提供することにある. 調査対象者は Facebook や Twitter などの SNS を利用している個人である. そのた

[1] パスワードの管理と心理的特性の関係をまとめたものについては文献 [4] が詳しいので参照されたい.

表 1: 調査対象者の割付

職業	#	(%)
社会人		
20 代	155	12.5
30 代	155	12.5
40 代	155	12.5
50 歳以上	155	12.5
学生	309	25.0
主婦・主夫・無職	309	25.0

め, この調査は, まず調査対象者（SNS 利用者）であるかを調べるための事前調査を 2 万人に対して実施し, その中から職業・年齢別に割付を行い, 約 1,200 人を抽出した. 次に彼ら・彼女たちを対象に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. そして, 最終的に 1,238 人の有効回答を得ている. なお, 調査対象者の割付（構成）は表 1 のようになっている. さらに, 学生の内訳は 10 代が 261 人（21.1%）, 20 代が 48 人（3.9%）であり, 主婦・主夫・無職の内訳は 10 代が 8 人（0.6%）, 20 代が 97 人（7.8%）, 30 代が 96 人（7.8%）, 40 代が 51 人（4.1%）, 50 歳以上が 57 人（4.6%）である.

質問項目は, インターネット上での行動, パスワードの設定・管理, 悪意ある投稿経験, SNS の利用に関する意識, プライバシーに関する意識, SNS に関する知識などの一般的な質問に加えて, 情報活用の実践力や同調効果, リスク回避度, ネット依存度などをはじめとする心理に関する質問と多岐にわたっており, 質問総数は 60 問である. 質問項目の内容は, 文献 [11, 12] などで用いられているものを参考に作成されている. 質問項目から作成される要因（構成概念）などについては 4 節にて説明する[2].

ここで, 簡単に表 1 により分類した調査結果の一部を紹介する.

インターネットで利用している ID（アカウント）数について質問したところ, 図 1 のような結果が得られた. いずれの分類においても回

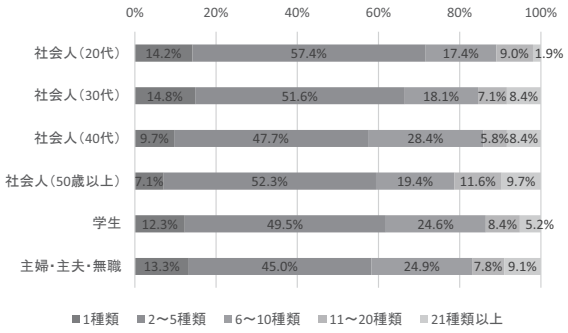

図 1: 管理アカウント（ID）数

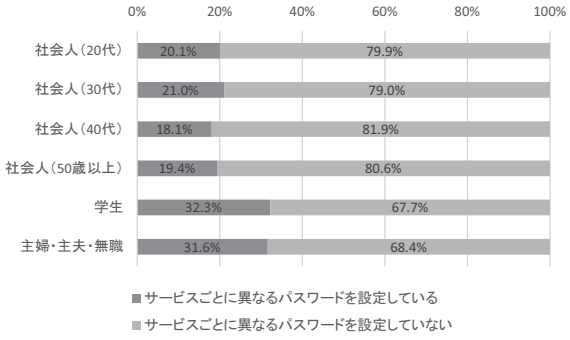

図 2: サービスごとの異なるパスワード設定

答者の 10%前後が 1 種類のアカウントしかないと回答している一方で, 21 種類以上のアカウント数を管理している回答者も 2〜10%の割合で存在していることがわかる. 3 割から 4 割の回答者が 6 種類以上のアカウントを持っていることから管理すべき複数のアカウントおよびパスワードの数が SNS の普及とともに増えていることがうかがえる.

図 2 は「サービスごとに異なるパスワードを設定しているかどうか」について質問した結果である. 図 2 を見てわかるように, 社会人は年代により若干の違いはあるものの平均して 20%前後の割合で異なるパスワードを設定しており, これらは学生や主婦などと比べて約 10 ポイント低いものとなっている.

また, 図 3 には「8 文字以上で記号を含むようなわかりにくい文字列でパスワードを設定しているかどうか」についての質問の結果を示している. これから約半数以上の回答者がわかり

[2]本研究で用いる要因は, 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. また, アンケート調査票は URL < http://ecolab.eco.saga-u.ac.jp/inf_sec/ >にて公開している.

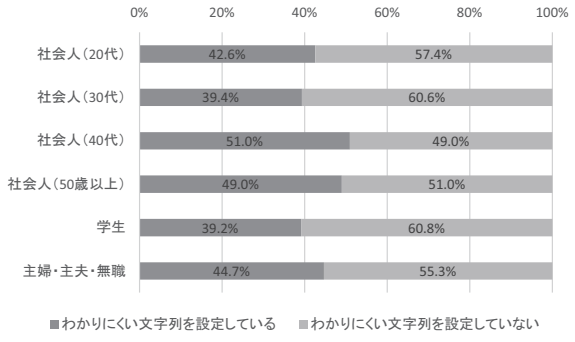

図 3: わかりにくい文字列の設定

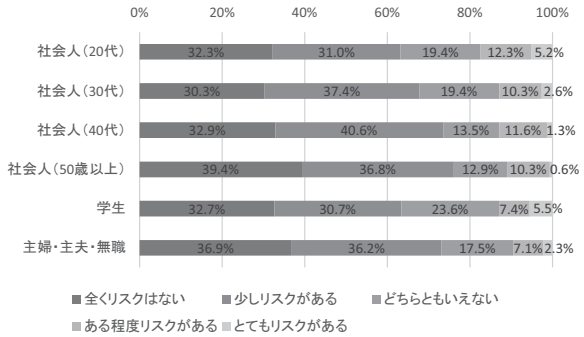

図 4: パスワードの詐取に対するリスク評価

にくい文字列でパスワードの設定をしていないことがわかる．

さらに, 図 4 には「パスワードの詐取がどれくらいリスクに感じるか」という質問をした結果を示している．この結果から 6 割以上の回答者がパスワードを詐取されることをリスクと感じていないことがわかる．

4 分析

本研究では, 文献 [7, 8] などにならい, パスワード管理に影響を与える要因として, 個人属性に加えて, 意識やリスク評価などの心理的な要因, 不合理な行動を引き起こすとされる要因（時間非整合性）, 知識などを考える．このモデルの検証を行うために, 多項ロジット回帰分析を行う．その前に, 説明変数および被説明変数のデータ加工について簡単に説明する．

4.1 変数の加工

4.1.1 被説明変数

パスワード管理 3 節で見たように, パスワード管理として考えるべきこととして「サービスごとの異なるパスワード設定」および「パスワードの強さ」がある[3]．本研究ではこの 2 つの側面をともに見ていきたいために, パスワード管理を表 2 のように変数として定義している．例えば, サービスごとに異なるパスワードを設定し, かつわかりにくい文字列でパスワードを設定している場合, この変数は 1 の値が付与される, と考える．つまり, パスワード管理の値が 1 と 4 を比較すると, 前者の方が適切にパスワード管理をしている一方で, 後者の方は適切にパスワード管理をしていないことになる．なお, 表 2 からも, 適切なパスワード管理ができている（サービスごとに異なるパスワードを設定し, かつわかりにくい文字列でパスワードを設定している）回答者の割合は 12.5%であるのに対して, 適切なパスワード管理ができていない（サービスごとに異なるパスワードを設定しておらず, かつわかりにくい文字列でパスワードも設定していない）回答者の割合は 45.9%である．このことから, 適切なパスワード管理があまりされていないことがうかがえる．

表 2: パスワード管理

値	サービスごとのパスワード設定	パスワードの強さ	#
1	YES	YES	155
2	YES	NO	386
3	NO	YES	129
4	NO	NO	568

4.1.2 説明変数

形式主義 形式主義とは社会的行動における暗黙の規則を強調し, 礼儀作法を特別に重視し, 身だしなみや話し方が適切であることに価値を置

[3] この他にも, パスワードの更新頻度も考えられるがこれについては賛否両論あるために今回の分析では取り扱っていない．

き, 体面を重視しようとするパーソナリティ特性の一つである（文献 [11]）. パスワードを適切に管理することはインターネット社会においては重要なことである. そのために, その行動に価値をおいていれば, 適切に管理されていると考えられる.

文献 [11] にならい, 形式主義を測る 10 問の質問群（「そう思わない」〜「そう思う」の 5 件法）を回答者に答えてもらい, その回答を用いて（一因子モデルとして）因子分析を行い, 変数を作成した. この変数は値が大きいほど, 形式主義的であると解釈する.

プライバシー性に関する意識　プライバシー性に関する意識とは, 氏名, 住所, 電話番号, 位置情報などのパーソナルデータのプライバシー（機微な情報や秘密の情報を本人の意思に反して第三者に知られない個人的権利）をどのように考えるかを表すものである. パスワード管理を徹底すると利便性が失われるために, そこにセキュリティやプライバシーを犠牲にしても仕方がないと考える可能性がある.

文献 [13] にあるパーソナルデータのプライバシー性に関する意識を問う 36 問の質問群（「プライバシー性がない」〜「極めて高い」の 4 件法）のうち本研究に関連する 25 問の回答を用いて（一因子モデルとして）因子分析を行い,「プライバシー性に関する意識」変数を作成した. この変数は値が大きいほど, プライバシー性に関する意識が高いと解釈する.

セキュリティインシデントに関する知識　一般的な情報セキュリティ対策の実施に関して, 情報セキュリティに関する知識が重要であることは文献 [14] などでも指摘されている. とりわけ, セキュリティインシデントに関する知識があれば, （その被害により自身に何らかの損害・損失が生じるため）被害に遭遇しないように事前対策を行うと考えられる.

調査では, 一般的な情報セキュリティ対策に関する知識についてではなく, 文献 [12] にある様々なインシデント（パスワードリスト攻撃やフィッシング, コンピュータウイルスなどの 7 種類）に関する質問項目がある（回答者はそれぞれのインシデントに対して 3 問からなるクイズでその内容が「正しい」「間違っている」「わからない」で答える形式である）. 本研究ではインシデントの中でもパスワード管理と関連があるパスワードリスト攻撃とフィッシングに関するクイズの正答数でもってセキュリティインシデントに関する知識とみなし, 変数を作成した. この変数は値が大きいほど, セキュリティインシデントに関する知識が高いと解釈する. 図 5 を見てわかるように, 4 割の回答者が全問不正解という結果が得られている.

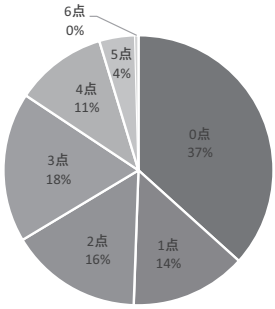

図 5: セキュリティインシデントに関する知識

判断力　文献 [15] によれば, 情報活用の実践力（一般的なリテラシー）は収集力, 判断力, 表現力, 処理力, 創造力および発信・伝達力の 6 つの側面から捉えられるとされている. 本研究ではこの中でもパスワードの管理と密接に関係している「判断力」に注目した. 判断力とは, 数多くある情報の中から必要なものを選択し, 内容を判断し, 適切な情報を引き出す能力のことである.

調査では, 文献 [15] にある情報活用の実践力における「判断力」を測る 7 問の質問群（「全くあてはまらない」〜「非常によく当てはまる」の 7 件法）を回答者に答えてもらっており, その回答を用いて（一因子モデルとして）因子分析を行い, 変数を作成した. この変数は値が大きいほど, 判断力が高いと解釈するものである.

時間非整合性　行動経済学でよく用いられる変数の一つとして時間割引率（time discount

rate）がある．時間割引率とは将来のモノの価値を現在の価値で割引く（置き換える）ときに用いられる概念であり, その大きさにより人のせっかち度や辛抱強さを測れるとされている．合理的な意思決定を行うとすればこの時間割引率はどのタイミングであろうと一致するが, 近年の研究ではこの時間割引率が時間の経過とともに変化すること（時間非整合性）が明らかになっている．この時間非整合性は人が後悔する原因の一つであるといわれている（文献 [16]）．

調査では文献 [16] にならい,「今, 10 万円もらう」（A）と「1 週間後に 11 万円もらう」（B）という選択と,「1 年後に 10 万円もらう」（A）と「1 年と 1 週間後に 11 万円もらう」（B）という選択をそれぞれ回答者にしてもらっている．本研究ではこの結果を比較し, ともに A もしくは B になっていればその回答者は時間整合的であると見なし、そうでなければ時間非整合的であると見なすことで時間非整合性の変数（時間非整合性であれば 1, そうでなければ 0 の値をとるダミー変数）を作成した．その結果, 約 20%の回答者は時間非整合的であることがわかった．

4.2 多項ロジット回帰分析

多項ロジット回帰分析とは, 順序性のないカテゴリーデータを被説明変数とするポピュラーな分析手法の一つである．本研究の被説明変数は 4.1.1 節で見た「パスワード管理」である．

一方で, 説明変数は 4.1.2 節で紹介したものに加えて,「年齢」「管理アカウント数」および「パスワードの詐取に対するリスク評価」（図 4）がある[4]．

多項ロジット回帰分析を行った結果をまとめたものが表 3 である[5]．管理アカウント数が 1 種類のみの回答者を分析から除外しているので, 分析対象となる回答者数は 1,088 人である．

表 3: 分析結果（多項ロジット回帰分析）

	Coef.	S.E.	z	p
Category 1				
(bese outcome)				
Category 2				
AGE	-0.010	0.007	-1.43	0.15
RSK	0.020	0.099	0.21	0.84
ID	-0.124**	0.060	-2.06	0.04
ID2	0.002	0.002	0.92	0.36
FORM	0.030	0.123	0.24	0.81
PRIV	-0.252**	0.124	-2.03	0.04
KNOW	-0.120*	0.067	-1.79	0.07
JDG	-0.332***	0.132	-2.52	0.01
TI	-0.246	0.270	-0.91	0.36
_cons	2.454	0.578	4.25	0.00
Category 3				
AGE	0.003	0.009	0.30	0.77
RSK	-0.007	0.123	-0.05	0.96
ID	-0.099	0.074	-1.34	0.18
ID2	0.003	0.003	0.98	0.33
FORM	-0.051	0.154	-0.33	0.74
PRIV	-0.352**	0.146	-2.42	0.02
KNOW	-0.012	0.082	-0.14	0.89
JDG	-0.520***	0.165	-3.14	0.00
TI	-0.211	0.335	-0.63	0.53
_cons	0.491	0.704	0.70	0.49
Category 4				
AGE	-0.017**	0.007	-2.35	0.02
RSK	-0.036	0.099	-0.37	0.71
ID	-0.215***	0.061	-3.52	0.00
ID2	0.005**	0.002	2.09	0.04
FORM	-0.055	0.124	-0.45	0.66
PRIV	-0.216*	0.124	-1.74	0.08
KNOW	-0.333***	0.068	-4.90	0.00
JDG	-0.556***	0.136	-4.09	0.00
TI	-0.085	0.264	-0.32	0.75
_cons	3.859	0.573	6.73	0.00

※ bese outcome（基準）は 1 である．

Number of obs = 1,088

LR chi2(27) = 191.38 Prob > chi2 = 0.00

Log likelihood = -1250.87 Pseudo R2 = 0.071

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

[4]「管理アカウント数」に関して図 1 で見たように 1 種類と回答している回答者は分析から除外した．つまり複数のアカウントを管理している回答者が分析の対象となっている．また, 管理アカウント数に関してはアカウント数を 2 乗したものも合わせて説明変数に用いている．

[5]本研究の分析には統計ソフトウェアとして Stata 14/MP2 を用いる．

表 3 の分析結果は基準をカテゴリー 1（サービスごとに異なるパスワードを設定し, かつ, パスワードにはわかりにくい文字列を設定している）としたものである.

全てのカテゴリーに共通して有意になった係数は「判断力」（JDG）と「プライバシー性に関する意識」（PRIV）であり, その値はいずれも負となっている. この結果は, 判断力が高い（プライバシー性に関する意識が高い）ほど, サービスごとに異なるパスワードを設定し, かつ, パスワードにはわかりにくい文字列を設定する傾向が強くなることを意味し, 適切なパスワードの管理に寄与することがわかる.

また,「管理アカウント数」（ID）および「セキュリティインシデントに関する知識」（KNOW）の係数はカテゴリー 2 とカテゴリー 4 において統計的に有意となり, その値はいずれも負となっている（カテゴリー 3 においてはいずれの変数の係数も統計的に有意ではない）. カテゴリー 4 においてのみ統計的に有意となったものは「年齢」（AGE）と「管理アカウント数の 2 乗」（ID2）の係数で, 前者の値は負, 後者の値は正となっている. これらの変数は全てのカテゴリーに共通してはいないが, パスワード管理の一方（もしくは両方）の設定に影響を与えることを意味している.

なお,「パスワードの詐取に対するリスク評価」（RSK）「形式主義」（FORM）「時間非整合性」（TI）の係数に関してはいずれのカテゴリーにおいても統計的に有意とならなかった. つまり, これらの要因はパスワードのそれぞれの設定をするか否かに影響を与えないことを意味している.

4.3 考察

ここで簡単に考察を行う. 多項ロジット回帰分析の結果, パスワード管理に影響を与える要因として「判断力」「プライバシー性に関する意識」があることが確認された. このことから, 判断力やプライバシー性に関する意識を向上させることで, 適切なパスワード管理を行うようになることが示唆される.

この他にも,「管理アカウント数」「セキュリティインシデントに関する知識」「年齢」などもパスワード管理に部分的ではあるが, 影響を与えることも確認された. 例えば,「セキュリティインシデントに関する知識」に即していえば, 情報セキュリティ教育の一環として, セキュリティインシデントに関する知識を身に着けさせることによって適切なパスワード管理を行うようになることが示唆される.

「年齢」に関しては文献 [8] と整合的な結果となっている. しかしながら「管理アカウント数」に関しては, 一部で管理アカウント数が増えれば, サービスごとに異なるパスワードを設定したり, パスワードにはわかりにくい文字列を設定する傾向が強くなるという結果が得られた. これは, 文献 [17] の「管理アカウント・パスワードの増大がパスワードのメモや安易なパスワード設定などの不適切なユーザ行動を招いている」という指摘とは異なるものである. しかしながら, 文献 [17] で指摘されていることは管理している平均アカウント数がかなり多い状況を想定しているが, 本研究では図 1 にあるようにそれほど管理しているアカウントの数は多くないので比較する際, 注意が必要である. なお, この点については今後更なる分析を試みたい.

本研究で採用した行動経済学的な要因および心理的な要因はパスワードのそれぞれの設定をするか否かに必ずしも影響を与えないことがわかった. 例えば, パスワードの詐取に対してリスクと捉えたとしても適切なパスワード管理を行うとは限らないことなどが示唆される. また, 行動経済学的な要因である時間非整合性に関して, 忍耐強さといった性格などはパスワード管理とは必ずしも関係ないといえる.

5 おわりに

本研究では, 2015 年 3 月に実施したインターネット調査によって収集された個票データを多項ロジット回帰分析を行うことにより, 行動経済学や社会心理学の視点からパスワード設定・管理に影響を与えている要因の探索を試みた. その結果, パスワード管理に影響を与える要因

として「判断力」「プライバシー性に関する意識」があることが確認された．この他にも，パスワード管理に部分的に影響を与える要因として「セキュリティインシデントに関する知識」なども確認され，情報セキュリティ教育などによりパスワード管理を適切に行わせることが可能であることが示唆された．

最後に，今後の展望について述べる．本研究では行動経済学的な要因（不合理な行動を引き起こす要因）の一つである時間割引率を分析に用いたが，それはパスワード管理に影響を与える要因でないことが確認された．調査にはこの他にも損失回避度やリスク回避度などがあるためそれらを用いて，適切なパスワード管理に影響を与える要因をさらに探索し，行動経済学の知見を援用し，ユーザが適切なパスワード管理ができるようになるための施策を考えていきたい．

謝辞　本研究は，日本学術振興会学術研究助成基金助成金「情報セキュリティ行動と有効な情報セキュリティ対策に関する実証研究」（課題番号 25380345・基盤研究 (C)・研究代表者 竹村敏彦）から助成を得て行った研究成果である．

参考文献

[1] 総務省: 平成 27 年度版情報通信白書, 日経印刷 (2015).

[2] 情報処理推進機構: 情報セキュリティ白書 2015, 情報処理推進機構 (2015).

[3] 情報処理推進機構: オンライン本人認証方式の実態調査報告書 (2014).

[4] 高橋優: パスワード生成・管理とユーザーの心理学的特性，埼玉工業大学教養紀要, No.32, 25-35 (2015).

[5] Gebauer, J., Kline, D., He, L.: Password Security Risk Versus Effort: An Exploratory Study on User-Perceived Risk and the Intention to Use Online Applications, Journal of Information Systems Applied Research, Vol.4, 52-62 (2011).

[6] Cazier, J.A., Medlin, B.D.: Password Security: An Empirical Investigation into E-commerce Passwords and Their Crack Times, Information Security Journal: A Global Perspective, Vol.15, 45-55 (2006).

[7] Campbell, J.,Ma, W., Kleeman, D.: Impact of Restrictive Composition Policy on User Password Choices, Behaviour and Information Technology, Vol.30, No.3, 379-388 (2011).

[8] Bonneau J.: The Science of Guessing: Analyzing an Anonymized Corpus of 70 Million Passwords. IEEE Symposium on Security and Privacy (2012).

[9] 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).

[10] 星野崇宏: 調査観察データの統計科学 – 因果推論・選択バイアス・データ融合, 岩波書店 (2009).

[11] Buzz, A.H.: 対人行動とパーソナリティ, 北大路書房 (1991).

[12] 情報処理推進機構: 2014 年度情報セキュリティの脅威に対する意識調査報告書 (2015).

[13] 総務省: ICT の進化がもたらす社会へのインパクトに関する調査研究 (2014).

[14] Schultz, E.: The human factor in security, Computers & Security, Vol.24, 425-426 (2005).

[15] 吉田富二雄・宮本聡介（編）: 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 282-289 (2011).

[16] 池田新介・大竹文雄・筒井義郎 : 時間割引率: 経済実験とアンケートによる分析, Discussion Paper Series, No.74 (2005).

[17] Adams, A., Sasse, M. A.: Users Are Not the Enemy, Communications of the ACM, Vol.42, No.12, 40-46 (1999).