コンジョイント分析による SNS アカウント情報の価値の測定*

竹腰 智 [1,†]　小川 隆一 [1,††]　竹村 敏彦 [2,†††]

概要：SNS（Social Networking Service）の急速な進展にともなって，膨大な個人のプライベートな情報がインターネット上で流通されるようになり，その情報を活用した様々なサービス提供され始めている．一方で，SNS に関して炎上やプライバシー侵害，不正ログインといった問題も近年注目されており，多くの人々の中では情報漏えいに対する懸念や不安を抱いていることも指摘されている．このような状況において，本研究では多くの個人情報が紐づく SNS アカウント情報（ID やパスワードなど）に着目し，コンジョイント分析を通じて，これらの経済学的価値の測定を行った．その結果，精神的被害よりも実被害に対して金銭的にも大きな評価をしていることなどが明らかになった．続けて，プライバシー・パラドックスの存在の検証を試みるために，SNS の利用の有無，SNS 実名利用の有無，悪意ある投稿経験の有無といった個人属性別に，SNS などのアカウント情報の価値の測定を合わせて行ったところ，プライバシー・パラドックスが存在する可能性が示唆する結果が得られた．

キーワード：コンジョイント分析，　SNS アカウント情報，プライバシー情報の価値，プライバシー・パラドックス

Measuring Economic Value of SNS Account Information via Conjoint Analysis

Satoshi Takekoshi[1,†]　Ryuichi Ogawa[1,††]　Toshihiko Takemura [2,†††]

Abstract: In accordance with the progress of SNS (Social Networking Service), many individuals/firms exchange enormous quantity of data involved their private information and we have various kinds of the services using the data in the world. On the other hand, recently social problems such flaming, invasion of privacy and fraud login as to SNS are confirmed, and many of individuals experience a worry about divulging of information. Under such situation, in this article we focused on the SNS account information such as IDs and/or passwords, and attempted to measure the economic value of the privacy information via conjoint analysis. As a result, we confirmed that they would assess higher monetary value of actual damage rather than mental damage. Next, we tested whether there was "privacy paradox" according to individual attributes such as the presence or absence of SNS usage/experience of posting malicious messages. As a result, we could approximately confirm the existence of the privacy paradox in Japan.

Keywords: Conjoint analysis, SNS account information, Economic value of privacy information, Privacy paradox

1. はじめに

SNS（Social Networking Service）において人々が情報発信や情報共有などのコミュニケーションをとることにより，新たなライフスタイルが生まれ，社会にとって SNS は便利なツールとなっている．また，SNS の急速な進展にともなって膨大な個人のプライベートな情報がインターネット上で流通されるようになり，その情報を活用した様々なサービス提供され始めている．その一方で，SNS に関して炎上やプライバシー侵害，不正ログインといった問題も近年注目されており，多くの人々の中では情報漏えいに対する懸念や不安を抱いていることも珍しくない．実際に，近年 SNS などのサービスアカウントへのログインに必要な情報（ログイン ID，パスワード）や，これに関連する個人情報の漏えい被害も多数発生している[1].

また，インターネット上におけるプライバシー不安と実際の自己開示行動の間に乖離が見られるという「プライバシー・パラドックス（Privacy Paradox）」の存在が指摘されている（第 2 章を参照されたい）．この現象の解釈については行動経済学におけるプロスペクト理論から与えられていることもあるが，個人が自身のプライバシー情報の（経済学的）価値を把握していないこともその理由として考えられる[a]．プライバシー情報の価値を把握せずに，SNS をはじめとするインターネット上のサービスに提供していること

* 本研究の意見は，著者たち個人に帰属し，所属機関の公式見解を示すものではないことをことわっておく．

1 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan
2 城西大学
Josai University
† s-takeko@ipa.go.jp
†† r-ogawa@ipa.go.jp
††† tkmrtshk@josai.ac.jp

a 個人情報の価値の認識という点において，情報処理推進機構では，ネットワークサービス利用のために収集・蓄積される個人情報に対して，利用者がセキュリティとプライバシーに関するリスクをどのように認識・受容しているかを調査している[2]．この調査から，日本人利用者はプライバシーが重要であると認識している一方で，プライバシー侵害のリスク回避意識が低いことなどが明らかにされている．

は，今後より一層進展していく DX（デジタル・トランスフォーメーション）[b]社会におけるパーソナル情報（プライバシー情報）の利活用に悪影響を与えることが予想される[c]．その意味において，本研究のようにプライバシー情報の経済的・マーケティング評価を行うことはこの課題を解決することにつながる第一歩につながると考えられる．

本研究では，多くの個人情報が紐づく SNS アカウント情報（ID やパスワードなど）に着目し，コンジョイント分析を通じて，これらの経済学的価値の測定を行う．具体的には，文献[4, 5]にならい，近年利用が進んでいる SNS などのパスワードや ID などのアカウント情報の価値をどのように評価しているかについて分析を行う．SNS は一般的に無料で利用できるものの，SNS を利用している個人は，そこに様々な個人情報を紐づけるという行動をとっている．これらの情報は，文献[4, 5]で取り上げているプライバシー情報よりも，より多くの情報を含んでいると考えられる．これらの情報がどれくらいの価値があるのかを測定することは実務的にも学術的にも興味深いことである．

本研究の構成は以下の通りである．第 2 章において関連研究を紹介する．第 3 章ではフレームワーク（コンジョイント分析の概要および手順）について説明する．第 4 章ではアンケート調査について説明し，第 5 章では分析結果および考察を与える．最後に第 6 章にて，本研究のまとめと今後の展望などについて示す．

2. 関連研究

ここでは，簡単に本研究と関連するものを紹介する．

個人情報の価値の測定を行っている研究として文献[4, 5]などがある．文献[4]は，ネットワーク利用者が情報セキュリティおよび個人情報に対して，どのような価値評価をするかを求めるための客観的・定量的な評価フレームワーク（コンジョイント分析や CVM など）を用いた分析を行っている．その中で，ネットワーク利用者に対する調査からネットワーク利用者の便益測定を行うとともに，実証的に得た金銭的評価について議論を展開している．また，文献[5]は文献[4]と同様に，何らかの理由で自らのプライバシー情報が漏えいしたときに，金銭的な実被害額を全額保証した上で，支払われる慰謝料をどの程度要求するかという仮想的な状況（シナリオ）の下で，個人のプライバシー情報（氏名・住所・性別・生年月日）の価値の測定をコンジョイント分析によって試みている．その結果，精神的被害を貨幣価値で測ると約 15,486 円，実被害については約 37,407 円になることなどを明らかにしている．加えて，企業の対応について見てみると，500 円の金券を送るよりも，詫び状を送ったりする方が個人にとって高い評価をしていることなども明らかにしている．

これらは日本ネットワークセキュリティ協会（JNSA）などが行っているアプローチと異なり，主として消費者が考える個人情報の価値に着目した研究である．この他にも，携帯電話の GPS 測位位置情報（ビッグデータとしての位置情報）に着目し，コンジョイント分析によって個人情報の価値の測定を行っている．そして，パーソナルデータの市場の成立可能性などについて議論を行っているものなどもある[6]．

これらの研究と密接に関連することとして「プライバシー・パラドックス」と呼ばれるものがある．プライバシー・パラドックスとは，大多数の個人はプライバシーに対する様々な不安や懸念を日頃から持っているにもかかわらず，SNSをはじめとするインターネット上では個人情報の開示を進んで行っているという現象（プライバシー不安と実際の自己開示行動の間に見られる乖離現象）のことをいう[7]．このプライバシー・パラドックスの存在は国内外の多くの研究において確認されている[8,9,10]．日本において，文献[11]は，プライバシーに関するパラドックスの存在を確認し，プライバシーの財としての価値の認識するために，携帯電話の電子マネー機能に関してコンジョイント分析を行っている．その結果，プライバシー的情報についての重要度の高さなどについて指摘している．

3. フレームワーク

3.1 コンジョイント分析

コンジョイント分析は，1960 年代に計量心理学の分野で誕生し，その後はマーケティングリサーチや経済学の分野で発展してきた SP（Stated Preferences）データ（仮想的な状況下での選好意識等に関するデータ）を用いて評価する表明選好法の代表的な手法の一つである．コンジョイント分析の詳細は文献[12]などを参照されたい．

コンジョイント分析における回答者の効用関数に多属性効用関数を想定する多属性アプローチは文献[13]により開発され，文献[14]などにより精緻化されたものであり，個人は財・サービスを消費する際，財・サービスを構成する様々な属性から効用を得るというものである．財・サービスの持つ性質・特性を多数の属性に分割し，各属性の水準を変化させることで，仮想的な商品を作成するものである．すなわち，ある商品の選好を測るために，選考に影響を及ぼす複数の具体的な特徴（属性）を組み合わせたカード（プロファイル）を回答者に提示し，商品全体での効用（全体効用）をたずね，その全体効用と属性ごとの効用（部分効用）をともに分析する手法である．言い換えると，個々の属性の重要性についての質問は行わず，プロファイルに対する評価を観察することで，個々の属性の重要性を明らかにする点に特徴があるといえる．

b DX とは，IT の浸透が「人々の生活をあらゆる面でより良い方向に変化させる」という概念である[3]．

c 厳密にいうと，プライバシー情報とパーソナル情報は異なる概念であるが，本研究ではこれらを同義として扱うこととする．

コンジョイント分析を用いることで，各属性の 1 単位が効用を変化させる度合いを示した値，つまり各属性の限界効用を推定することができる．各属性の限界効用の比からは，属性間の限界代替率を求めることができる．また，属性に金銭的属性が含まれている場合には，その金銭的属性と他の属性の限界効用の比から，各属性の評価額が求められる. この評価額は, ある属性を 1 単位増加させるために，個人が支払っても構わないと考える最大の金額であり，各属性に対する限界支払意思額（Willing to Pay）と解釈することができる．

このように，コンジョイント分析では，個人が日常の行動の中で直観的に判断している内容を，多くの被験者で代表される集団の平均的な考え方として評価するものである．

3.2 コンジョイント分析の手順

文献[15]ではコンジョイント分析を行う手順を 7 つの段階に分けている（1. 分析目的の設定, 2. 属性・水準の決定, 3. 全選択肢集合の作成, 4. 調査票の作成, 5. データ収集, 6. モデルの推定と検定，7. 計画評価）．以下，簡単にこの手順について説明を行う．なお，5. データ収集については第 4 章にて説明する．

(1) 分析目的の設定

本研究で取り上げる SNS などのパスワードや ID などのアカウント情報が漏えいすることによって, その SNS 内にある様々なタイプのプライバシー情報まで漏洩することになる（さらにはパスワードの使いまわしなどをしている場合，他の SNS などにも被害が及ぶことが予想される）．その意味において文献[4, 5]が想定しているプライバシー情報よりもセンシティブなものがこの情報に含まれているといえる．

本研究では，SNS などのパスワードや ID などのアカウント情報を個人がどのように評価しているかについて明らかにする．そのために，仮想的な状況として，これらの個人のプライバシー情報が何らかの理由で情報漏えいされたときに，金銭的な実被害額全額を保証した上で，支払われる慰謝料についての評価をアンケート調査において求めることとした．

(2) 属性・水準の決定

様々な属性が分析の対象とする行動に影響するとしたとしても，全ての属性を選択実験において変化させることはできない．プロファイルを構成する属性と水準に関しては，人間の情報処理能力の限界を考慮する必要がある．一般的に，コンジョイント分析を用いた調査において，属性は最大でも 6 つが限界であるとされている[15].

本研究では，文献[4, 5]に従ってプロファイルの属性および水準を表 1 のように設定した. 属性として「精神的被害」があるのは，謝料は本人の精神的苦痛に応じて金額が算定されるものであるからとしている[4]．また，企業の対応は事例として散見された企業の対応を反映したものである．

表 1　プロファイルの属性および水準

Table 1　Profile of Conjoint cards

属性	水準	内容				
精神的被害	重大な心労	病院に行くほど眠れない日が何日も続き、日常生活に支障をきたした				
	不安感が続く	日常生活に問題はないが、二次被害の心配と不安感が長く続いた				
	心配のみ	漏えいがわかった当初は心配したが、すぐになくなった				
	なし	知らなかったなど被害はないに等しい				
実被害	重大な被害	架空請求、掲示板への誹謗中傷、いたずら電話、迷惑メールなどがあった				
	被害あり	二次利用された事実はないが、漏えいしていることを他人に知られた				
	被害なし	すぐに回収されたため、被害はないか、ないに等しい				
企業の対応	金券	企業から500円の金券が届いた				
	詫び状	企業からお詫び状またはお詫びメールが届いた				
	HP	企業のホームページ上に謝罪文が掲載された				
	対応無し	企業から誠意ある対応はなかった				
慰謝料		20000円	40000円	60000円	80000円	100000円

慰謝料の金額としては，下限を 2 万円，上限を 10 万円とした．なお，文献[5]では，2 万円，4 万円，8 万円，10 万円としていたが，本研究ではこれに 6 万円を追加している．JNSA によれば, 2005 年から 2011 年にかけての一人当たりの平均想定損害賠償額は 3 万円後半から 5 万円の範囲である[16]. これに比べると, 本研究における金額の設定は高く設定されている．

(3) 全選択肢集合の作成

属性および水準を組み合わせたプロファイルの作成において，総当たり法では膨大な組み合わせができる．しかしながら，これらすべてに対して回答を求めることは不可能である．そこで，これらのプロファイルの効率的な組み合わせを実現することが求められる．ここでいう効率的とは，ある一定の統計的信頼性を持った結果を，最も少ないサンプルで得ることを意味する．

一般的に用いられているプロファイルデザインの手法として直交配列と呼ばれるものがあり，本研究でもこの手法を採用する．さらに，表 1 に従って具体的な選択肢の作成に加えて,「どちらも選ばない」という選択外オプション（opt-out option）を設定し，全選択肢集合を作成することにする．

(4) 調査票の作成

文献[5]にならい，調査票には，上述した手順で作成したプロファイルの組み合わせに対して「ある企業が，あなたのSNSなどのパスワードやIDなどの個人情報をインターネット上に漏えいしたと仮定します．以下は，被害の状況と企業の対応がそれぞれ設定されています．それぞれの条件において支払われる慰謝料について，あなたがより納得出来るものとして，条件Aもしくは条件Bのいずれか1つをお選びください．なお，この慰謝料は，金銭的な実被害額全額を保証した上で，支払われる金額と考えてください．条件として設定される言葉の意味は，おおよそ以下のイメージと考えてください.」というリード文ならびに表2の属性・水準の説明を示した後に, 表2のような質問例を提示し回答者に選択してもらうという形式をとっている．

本研究では，表2のような質問を20問作成した．これらの作成には，統計ソフトウェアであるR version3.5.4を用いた．

表 2　質問例

Table 2　One example of questionnaires

	A	Aの方が納得できる	どちらも納得できない	Bの方が納得できる	B
精神的被害	心配のみ	□	□	□	重大な心労
実被害	重大な被害	□	□	□	被害なし
企業の対応	HP	□	□	□	金券
慰謝料	40000円	□	□	□	60000円

(5) モデルの推定と検定

選択実験のための質問から得られたデータは，確率効用理論という個人の意思決定モデルを理論的基礎とした離散選択モデルによって分析される．本研究では，離散選択モデルの中でも基本的な選択型ロジットモデルを取り上げる．なお，選択型ロジットモデルなどの理論的説明ならびに検定方法などについては文献[17]を参照されたい．

(6) 計画評価

分析した結果の評価については，1 つの属性の水準を（限界的に）変更したときの評価と複数の属性の水準を同時に変更したときの評価などがある．本研究では主として，前者の（経済学的）評価を試みる（経済学的評価の詳細は文献[18]を参照されたい）．上述したように，貨幣単位での評価に関する 1 つ目の指標は，限界支払意思額（WTP）である．WTP は属性を 1 単位増加させることによる確定効用の増分を求め，それを相殺するだけの貨幣単位の属性を引き上げるものとして考えられる．

4. アンケート調査

本研究では，2019 年 3 月にクローズ型のインターネットアンケート調査形式により実施された「労働者の情報セキュリティ意識および行動に関する調査 2019」（以下，「2019 年調査」と称す）によって収集した個票データを用いて分析を行う．

「2019 年調査」の目的は，一般労働者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や情報セキュリティマネジメントを行う際の情報を提供することにある．調査対象者は 2 年以上同一の企業で働いており，日常業務でパソコンや電子メールなどを利用している一般的な労働者である．この調査は，オーバーサンプリングや，計測している回答時間から一般的な回答者と比べて回答時間が早い者を不良回答者として取り扱いサンプルから外すなどして，最終的に 1,032 人の有効回答数を得ている．調査対象者の構成は表 3 のようになっている．

質問項目は，情報セキュリティ意識，情報セキュリティ行動，情報リテラシーに加えて，職場環境，行動経済学で用いられる指標（例えば，リスク回避度など）に関するもの，本研究で行うコンジョイント分析のためのものなど多岐にわたっている．

表 3　回答者のデモグラフィック属性

Table 3　Demographic attributes of respondents

		#	(%)
性別	男性	491	47.58
	女性	541	52.42
年齢	20～29歳	87	8.43
	30～39歳	280	27.13
	40～49歳	307	29.75
	50～59歳	260	25.19
	60歳以上	98	9.50
年収	400万円未満	517	50.10
	400～600万円未満	178	17.25
	600～800万円未満	81	7.85
	800～1000万円未満	47	4.55
	1000万円以上	33	3.20
	答えたくない	176	17.05
居住地域	北海道・東北	98	9.50
	関東（東京都除く）	267	25.87
	東京都	133	12.89
	中部	169	16.38
	近畿	186	18.02
	中国・四国	74	7.17
	九州・沖縄	105	10.17
上場・非上場	上場	516	50.00
	非上場	516	50.00
正規・非正規	正規	516	50.00
	非正規	516	50.00
従業員数	300人未満	482	52.74
	300人以上	432	47.26

以下，本研究で用いる属性について簡単に見ていく．「2019 年調査」では，SNS 利用状況（閲覧や書き込みなどのアクセス状況）についてサービス（Facebook や Twitter など）ごとに質問している．この質問に対して「アカウント，ID を作成（登録）しただけ」「1 か月に 1 回程度以下での利用」「1 か月に数回程度での利用」「1 週間に数回程度での利用」「毎日数回程度の利用」「毎日かなりの頻度で利用」「利用していない」の選択肢を提示して回答を求めている．ここで，「アカウント，ID を作成（登録）しただけ」と「利用していない」を選択した個人はそのサービスを利用していない，それ以外のものを選択していればサービスを利用していると見なした．そして，少なくともいずれかのサービスにおいて利用経験があれば SNS を利用していると本研究では判断する．その結果，SNS を利用していない個人が 414 人（40%），SNS を利用している個人が 618 人（60%）いることがわかった．

また，「2019 年調査」では，SNS 利用者（#=618）を対象として，利用している SNS は何か，これまで悪意ある投稿をした経験があるか否かなどについても質問している．

同じ SNS でも実名と匿名を併用していたり，SNS によって使い分けていたりするケースがある[d]．本研究では，基本的に実名で利用が行われる Facebook と LinkedIn を利用していれば，その個人は「実名で SNS を利用している」と見なしている．その結果，実名で SNS を利用している個人は 346 人（56%），実名で SNS を利用していない個人は 272 人

d 「2019 年調査」では，回答者に直接 SNS を実名・匿名で利用しているか否か，について質問をしていない．そのため，本研究におけるこのグルーピングについては今後よく吟味する必要がある．

（44%）であることがわかった．

「2019 年調査」では，Facebook や Twitter など 8 種類の SNS に対して個別に，情報処理推進機構が毎年実施している「情報セキュリティに対する意識調査」で用いられている「他人や企業の悪口」「他人の発言を非難する内容」などを含む 13 の悪意ある投稿をしたかどうかについて質問している[19]．ここでは，13 項目のうち少なくとも 1 つでも該当するものがあればその回答者はその SNS で悪意ある投稿を行った経験があると判断する[20]．本研究では悪意ある投稿をした SNS を個別に分析するのではないため，8 種類の SNS において 1 つでも悪意ある投稿をした経験があるか否かについて知ることができる．この結果，これまで悪意ある投稿経験がない個人は 526 人（85%），投稿経験がある個人は 92 人（15%）であることがわかった．

5. 分析結果

5.1 分析結果 I

表 4 には，「2019 年調査」の回答者全員を対象として行ったコンジョイント分析の結果を示している[e]．なお，文献[5]にならい，慰謝料，精神的被害，実被害に関しては水準に順序性があると判断した．しかしながら，企業の対応は必ずしも順序性が保証されていないために，ダミー変数として分析に用いた．そのために，企業対応は水準ごと（「対応なし」を基準としている）の推定された係数値が示されている．また，ASC は選択肢固有定数を表している．つまり，表 2 で A もしくは B のいずれかを選択していれば 1，「どちらも納得いかない」を選択していれば 0 が付与されるものである．

表 4 にある Likelihood ratio test（尤度比検定）は推定されたすべての係数値がゼロであるという帰無仮説を統計的検定するためのものである．この検定の p 値から，この帰無仮説は棄却されることがわかる．後述の分析結果に関しても同様のことがいえる．

表 4 の係数の p 値を見てわかるように，「精神的被害」の係数は 5%水準で有意となっており，それ以外の係数はいずれも統計的に 1%水準で有意となっている．つまり，本研究で用いた属性（変数）のいずれもそれぞれの選択肢の効用に影響を与えることがわかる．また，「精神的被害」「実被害」の係数はいずれも負の値をとっている．このことから，例えば精神的被害の程度が大きくなるほど，精神的被害が設定されている選択肢の効用が小さくなることを意味する．逆に，係数の値が正の値をとっている「慰謝料」および企業の対応（「金券」「詫び状」「HP」）については，それぞれの変数の値が大きくなるほど，その変数が設定されている選択肢の効用が大きくなる．とりわけ，企業の対応については，「対応無し」と比べて何らかの対応をすることで個人の効用を高めることになることを意味している．この結果は SNS などのパスワードや ID といったアカウント情報に関するものであるが，個人のプライバシー情報（氏名・住所・性別・生年月日）の価値の測定を試みている文献[4,5]の結果と整合的である．

表 4　分析結果 I

Table 4　Result I

		coef	exp(coef)	se(coef)	z	p
ASC		-0.927	0.396	0.053	-17.53	<2.00E-16
慰謝料		0.007	1.007	0.000	17.07	<2.00E-16
精神的被害		-0.025	0.976	0.011	-2.29	0.022
実被害		-0.310	0.734	0.015	-21.09	<2.00E-16
企業の対応	金券	0.266	1.305	0.036	7.31	2.69E-13
	詫び状	0.298	1.347	0.033	8.96	<2.00E-16
	HP	0.281	1.324	0.036	7.84	4.47E-15
	対応無し	0.000				

Likelihood ratio test=5565 on 7 df, p=< 2.2E-16

n= 61920, number of events= 20640

次に，表 4 の分析結果を用いて限界支払意思額（属性の価格評価）を行う．

精神的被害などのような非金銭的属性（変数）の限界支払意思額は，簡単に第 3.2 節でも説明したように，非金銭的属性が 1 単位変化したときの評価額となる．本研究のように，線形モデルを想定している場合，非金銭的属性の推定された係数値を金銭的属性（慰謝料の金額）の推定された係数値で除したものの絶対値をとることで計算できる．そこで，非金銭的属性である精神的被害，実被害，企業の対応に関する限界支払意思額をそれぞれ計算した結果が表 5 である．

表 5　限界支払意思額 I

Table 5　Calculated willing to pay I

要因		WTP
精神的被害		3516.35　円
実被害		44013.65　円
企業の対応	金券	37852.67　円
	詫び状	42413.11　円
	HP	39896.05　円

表 5 を見ると，精神的被害を貨幣価値で測ると約 3,516 円，実被害については約 44,014 円になることがわかる．精神的被害よりも実被害に対して金銭的にも大きな評価をしていることがうかがえる．また，企業の対応について見てみると，500 円の金券を送るよりも，詫び状を送ったりする方が個人にとって高い評価をしていることが読み取れる．違う見方をすると，企業のホームページ上に謝罪文を掲載することと 500 円の金券を送ることにそれほど評価に大きな違いがないことがわかる．この結果は，評価額は異なるものの，文献[5]の結果とは整合的であるといえる．

e 本研究における統計分析には，統計ソフトウェアである R version3.5.4 を用いた．

5.2 分析結果 II（SNS 利用の有無）

第 4 章で見たように，SNS を利用していない個人が 414 人，SNS を利用している個人が 618 人存在している．

第 2 章で紹介したプライバシー・パラドックスの存在を考えると，SNS を利用しているか否かによって，SNS などのパスワードや ID といったアカウント情報の価値の評価が異なることが予想される．本研究では，精神的被害や実被害についてはこれらの評価額を SNS 利用者の方が SNS 非利用者よりも高く見積もっているのではないかという仮説を立てる．これにより，（間接的ではあるが）プライバシー・パラドックスが存在するか否かについて検証することも可能であると考える．表 6 には SNS の利用状況によってグループ分けしたコンジョイント分析の結果を示している．

表 6　分析結果 II（SNS 利用の有無）

Table 6　Result II (SNS no-users/users)

SNS非利用者		coef	exp(coef)	se(coef)	z	p
ASC		-0.989	0.372	0.085	-11.621	<2.00E-16
慰謝料		0.008	1.008	0.001	11.420	<2.00E-16
精神的被害		-0.036	0.964	0.017	-2.086	0.037
実被害		-0.330	0.719	0.024	-13.958	<2.00E-16
企業の対応	金券	0.285	1.330	0.058	4.881	1.05E-06
	詫び状	0.305	1.357	0.054	5.677	1.37E-08
	HP	0.272	1.313	0.058	4.719	2.37E-06
	対応無し	0.000				
Likelihood ratio test=2633 on 7 df, p=< 2.2E-16 n= 24840, number of events= 8280						
SNS利用者		coef	exp(coef)	se(coef)	z	p
ASC		-0.885	0.413	0.068	-13.105	<2.00E-16
慰謝料		0.007	1.007	0.001	12.729	<2.00E-16
精神的被害		-0.017	0.983	0.014	-1.268	0.205
実被害		-0.297	0.743	0.019	-15.859	<2.00E-16
企業の対応	金券	0.254	1.289	0.047	5.456	4.87E-08
	詫び状	0.294	1.342	0.042	6.935	4.07E-12
	HP	0.286	1.331	0.046	6.262	3.80E-10
	対応無し	0.000				
Likelihood ratio test=2963 on 7 df, p=< 2.2E-16 n= 37080, number of events= 12360						

表 6 の SNS 非利用者のケースを見てみると，「精神的被害」の係数は 5%水準で有意となっており，それ以外の係数はいずれも統計的に 1%水準で有意となっている．一方で，SNS 利用者のケースでは「精神的被害」の係数は統計的に有意な結果は得られていないものの，それ以外の係数はいずれも統計的に 1%水準で有意となっている．このことから，SNS を利用しているか否かによって SNS などのパスワードや ID といったアカウント情報に関する「精神的被害」の評価が異なることがわかる．表 7 には SNS 非利用者と SNS 利用者のそれぞれの要因に関する限界支払意思額をまとめている．表 7 を見てわかるように，有意となった「実被害」や企業の対応について，「HP」は SNS 非利用者と SNS 利用者の評価額の差は約 6,800 円となっているが，それ以外のものについてはそれほど大きく異なることはなかった．

表 7　限界支払意思額 II

Table 7　Calculated willing to pay II

		WTP	
要因		SNS非利用者	SNS利用者
精神的被害		4776.45 円	
実被害		43487.97 円	44400.16 円
企業の対応	金券	37609.25 円	37990.27 円
	詫び状	40210.83 円	43971.84 円
	HP	35886.88 円	42714.94 円

5.3 分析結果 III（SNS 実名利用の有無）

第 4 章で見たように, SNS を利用している個人（618 人）の中で，実名で SNS を利用している個人は 346 人，実名で SNS を利用していない個人は 272 人存在している．

第 5.2 節と同様に，プライバシー・パラドックスの存在を考えると，SNS を実名で利用しているか否かによって，SNS などのパスワードや ID といったアカウント情報の価値の評価が異なることが予想される．本研究では，精神的被害や実被害について，これらの評価額を実名で SNS を利用している個人の方がそうでない個人よりも高く見積もっているのではないかという仮説を立てる．表 8 には SNS の利用状況によってグループ分けしたコンジョイント分析の結果を示している．

表 8 の SNS の非実名利用のケースを見てみると，「精神的被害」の係数は 10%水準で有意となっており，それ以外の係数はいずれも統計的に 1%水準で有意となっている．一方で，SNS の実名利用のケースでは「精神的被害」の係数は統計的に有意な結果は得られていないものの，それ以外の係数はいずれも統計的に 1%水準で有意となっている．このことから，SNS を実名で利用しているか否かによって SNS などのパスワードや ID といったアカウント情報に関

表 8　分析結果 III（SNS 実名利用の有無）

Table 8　Result III（Anonymous/ autonym usage of SNS）

非実名利用		coef	exp(coef)	se(coef)	z	p
ASC		-0.821	0.440	0.101	-8.094	5.77E-16
慰謝料		0.008	1.008	0.001	10.277	<2.00E-16
精神的被害		-0.038	0.962	0.021	-1.862	0.063
実被害		-0.330	0.719	0.028	-11.737	<2.00E-16
企業の対応	金券	0.242	1.274	0.070	3.460	0.001
	詫び状	0.309	1.362	0.063	4.872	1.10E-06
	HP	0.306	1.357	0.068	4.465	8.00E-06
	対応無し	0.000				
Likelihood ratio test=1269 on 7 df, p=< 2.2E-16 n= 16320, number of events= 5440						
実名利用		coef	exp(coef)	se(coef)	z	p
ASC		-0.937	0.392	0.091	-10.348	<2.00E-16
慰謝料		0.006	1.006	0.001	7.860	3.83E-15
精神的被害		-0.001	0.999	0.019	-0.029	0.977
実被害		-0.270	0.763	0.025	-10.757	<2.00E-16
企業の対応	金券	0.263	1.301	0.062	4.220	2.45E-05
	詫び状	0.283	1.327	0.057	4.950	7.41E-07
	HP	0.270	1.310	0.061	4.412	1.02E-05
	対応無し	0.000				
Likelihood ratio test=1708 on 7 df, p=< 2.2E-16 n= 20760, number of events= 6920						

表 9　限界支払意思額 III

Table 9　Calculated willing to pay III

		WTP	
要因		非実名利用	実名利用
精神的被害		4745.85 円	
実被害		40765.98 円	48692.21 円
企業の対応	金券	29875.31 円	47514.93 円
	詫び状	38096.67 円	50983.97 円
	HP	37714.65 円	48729.35 円

する「精神的被害」の評価が異なることがわかる．表 9 には SNS の非実名利用者と SNS の実名利用者のそれぞれの要因に関する限界支払意思額をまとめている．表 9 を見てわかるように，有意となった要因の評価額はいずれも両者で大きな差があることが確認できる．

5.4 分析結果 IV（悪意ある投稿経験の有無）

第 4 章で見たように，SNS を利用している個人の中で，これまで悪意ある投稿経験がない個人は 526 人，これまで悪意ある投稿経験がある個人は 92 人存在している．

本研究では，悪意ある投稿経験があるか否かによって，SNS などのパスワードや ID といったアカウント情報の価値の評価が異なることと考える．具体的には，悪意ある投稿をする個人は（自らのプライバシー情報でさえ）それほど高く評価していないのではないかという仮説を立ててそれを検証する．表 10 には SNS の利用状況によってグループ分けしたコンジョイント分析の結果を示している．

表 10　分析結果 IV（悪意ある投稿経験の有無）

Table 10　Result IV (Experience of posting malicious messages)

悪意ある投稿経験なし		coef	exp(coef)	se(coef)	z	p
ASC		-0.858	0.424	0.073	-11.680	<2.00E-16
慰謝料		0.007	1.007	0.001	12.647	<2.00E-16
精神的被害		-0.027	0.974	0.015	-1.790	0.0734
実被害		-0.327	0.721	0.020	-16.025	<2.00E-16
企業の対応	金券	0.263	1.301	0.051	5.190	2.11E-07
	詫び状	0.306	1.358	0.046	6.628	3.40E-11
	HP	0.316	1.371	0.050	6.361	2.00E-10
	対応無し	0.000				
Likelihood ratio test=2625 on 7 df, p=< 2.2E-16 n= 31560, number of events= 10520						
悪意ある投稿経験あり		coef	exp(coef)	se(coef)	z	p
ASC		-1.046	0.351	0.172	-6.068	1.29E-09
慰謝料		0.004	1.004	0.001	2.754	0.006
精神的被害		0.036	1.037	0.035	1.031	0.303
実被害		-0.133	0.876	0.048	-2.779	0.005
企業の対応	金券	0.204	1.226	0.118	1.730	0.084
	詫び状	0.226	1.254	0.107	2.103	0.036
	HP	0.118	1.125	0.116	1.018	0.309
	対応無し	0.000				
Likelihood ratio test=359.8 on 7 df, p=< 2.2E-16 n= 5520, number of events= 1840						

表 10 の悪意ある投稿経験がないケースを見てみると，「精神的被害」の係数は 10%水準で有意となっており，それ以外の係数はいずれも統計的に 1%水準で有意となっている．一方で，悪意ある投稿経験があるケースでは「精神的被害」「HP」の係数は統計的に有意な結果は得られていないものの，それ以外の係数はいずれも統計的に 1%水準で有意となっている．このことから，悪意ある投稿経験があるか否かによって，SNS などのパスワードや ID といったアカウント情報に関する「精神的被害」「HP」の評価が異なることがわかる. 表 11 には悪意ある投稿経験がない個人と悪意ある投稿経験がある個人のそれぞれの要因に関する限界支払意思額をまとめている．表 11 を見てわかるように，有意となった要因の評価額はいずれも両者で大きな差があることが確認できる．

表 11　限界支払意思額 IV

Table 11　Calculated willing to pay IV

		WTP	
要因		悪意ある投稿経験無し	悪意ある投稿経験あり
精神的被害		3714.73 円	
実被害		45215.54 円	35762.20 円
企業の対応	金券	36439.70 円	54945.27 円
	詫び状	42363.97 円	60936.37 円
	HP	43707.94 円	

5.5 考察

第 5.1 節では「2019 年調査」の回答者全員，また第 5.2 節から第 5.4 節では回答者個人の属性でもってグルーピングした統計結果を示した．ここでは，これらの結果についての考察を行う．

「2019 年調査」の回答者全員を対象とした結果は，属性として用いた「慰謝料」「精神的被害」「実被害」および企業の対応（「金券」「詫び状」「HP」）の係数がいずれも統計的に有意となり，それぞれのコンジョイントカードで設定されている選択肢の効用に影響を与えていることがわかった．また，同様の分析を行っている文献[5]の結果と比較すると，精神的被害に対する評価は 12,000 円程度安くなっている一方で，それ以外の要因はいずれも評価金額が高くなっている．勿論，対象としている情報や調査対象が異なることもこの結果に影響を与えていると考えられるが，興味深い結果である．

続いて，SNS の利用の有無，SNS 実名利用の有無，悪意ある投稿経験の有無といった個人属性別に，SNS などのアカウント情報の価値の測定を合わせて行ったところ，SNS 利用者，SNS の実名利用，悪意ある投稿経験があるグループにおける「精神的被害」の係数はいずれも統計的に有意とならなかった. SNS 利用グループと SNS 非利用グループで「精神的被害」の評価が異なることについて，一つの可能性として，SNS 非利用者は個人情報を漏らしたくないと考えており，SNS 利用者は個人情報が流出するリスクをある意味で受容しているものと考えることもできる．この点については更なる分析が必要になると思われる．一方で，「実被害」に関して, SNS を利用していない個人よりも SNS

を利用している個人方がその評価を高くなっていることがわかった．また，SNS 利用者の中でも実名で利用している個人の方がそうでない個人よりも高い評価を行っていることも確認できた．このことから，プライバシー・パラドックスが存在する可能性が示唆していると考えることができる．そして，悪意ある投稿経験に関しては，悪意ある投稿経験がある個人の方が投稿経験のない個人よりも「実被害」の評価額が低いことも確認できた．このことについては，悪意ある投稿経験がある者は自分自身の個人情報の価値も低く捉えて，悪意ある投稿経験が無い者よりも限界支払意思額が低くなったと推測される．

企業の対応についてはいずれの分析結果についても同じ傾向があることが読み取れた．例えば，企業のホームページ上に謝罪文を掲載することと 500 円の金券を送ることにそれほど評価に大きな違いがないことなどが確認された．

6. おわりに

本研究では，仮想的な状況を想定し，コンジョイント分析を通じて，SNS などのパスワードや ID などのアカウント情報の価値の測定を試みた．その結果，精神的被害よりも実被害に対して金銭的にも大きな評価をしていることなどが明らかになった．続けて，プライバシー・パラドックスの存在の検証を試みるために，SNS の利用の有無，SNS 実名利用の有無，悪意ある投稿経験の有無といった個人属性別に，SNS などのアカウント情報の価値の測定を合わせて行った．その結果，プライバシー・パラドックスが存在する可能性が示唆された．また，企業の対応についても対応をしないよりも，何らかの対応をすることが個人に評価されることも概ね確認された．とりわけ，企業の対応について見てみると，500 円の金券を送るよりも，詫び状を送ったりする方が個人にとって高い評価をしていることは興味深い結果であった．

最後に，本研究の限界と今後の展望を示す．本研究では，限られた情報（例えば，アンケート調査対象者が労働者に限定されていることなど）によってプライバシー情報の価値の測定を行っていたため，一般化することが必ずしも容易ではない．しかしながら，この種の市場が存在しない情報財（プライバシー財）の価値を個人が認識するに至ることの一助になると思われる[5, 6, 11]．今後，この種の研究が日本においても積極的に行われていくことを期待したい．

謝辞

本研究成果の一部は，独立行政法人日本学術振興会の科研費（17K03827，17K00463）の助成を受けて行ったものである．

参考文献

[1] 情報処理推進機構『情報セキュリティ白書 2019～新しい基盤，巧妙化する攻撃：未知のリスクに対応する力を』情報処理推進機構, 2019 年

[2] 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に関するリスク認知と受容の調査報告」, 2010 年（https://www.ipa.go.jp/files/000011765.pdf）

[3] Stolterman, E., Fors, C.A.: Information Technology and Good Life. Kaplan, B., Truex, D.P., Wastell, D., Wood-Harper, A.T., DeGross, J. (Eds) Information Systems Research. Relevant Theory and Informed Practice. Kluwer Academic Publishers, pp.687-692, 2004

[4] 櫻井直子『情報セキュリティの価値と評価～消費者が考える個人情報の値段』文眞堂, 2011 年

[5] 竹村敏彦・片山佳則・鳥居悟・古川和快「プライバシー情報の価値の測定」, SCIS2019 Proceedings, 3C2-3, 2019 年

[6] 高口鉄平『パーソナルデータの経済分析』勁草書房, 2015 年

[7] Barnes, S.: A Privacy Paradox: Social Networking in the United States, 2006（https://firstmonday.org/article/view/1394/1312_2）

[8] Debatin, B., Lovejoy, J.P., Hom, A.K., Hughes, B.N.: Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences. Journal of Computer-Mediated Communications, vol.25, no.1, pp.83-108, 2009

[9] Dienlin, T., Trepte, S.: Is the Privacy Paradox a Relic of the Past? An In-depth Analysis of Privacy Attitudes and Privacy Behaviors. European Journal of Social Psychology, vol.45, pp.289-297, 2014

[10] 三上俊治「SNS における自己開示とプライバシー・パラドックス」，東洋大学社会学部紀要, vol.53, no.1, pp.65-77. 2015 年

[11] 岡田仁志・高橋郁夫「コンジョイント方式によるプライバシー分析－携帯電話電子マネーの位置情報の認知の実証的検証を例に－」，情報通信政策レビュー, 2, 55-65, 2011 年

[12] Louviere, J.J., Hensher, D.A., Swait, J.D.: Stated Choice Methods: Analysis and Application. Cambridge University Press, 2000

[13] Lancaster, K.J.: A New Approach to Consumer Theory. Journal of Political Economy, vol.74, pp.132-157, 1966

[14] Rosen, S.: Hedonic Prices and Implicit Markets: Product Differentiation in Pure Competition. Journal of Political Economy, vol.82, pp.34-55, 1974

[15] 合崎英男『農業・農村の計画評価～表明選好法による接近』農林統計協会, 2005 年

[16] 日本ネットワークセキュリティ協会「2011 年情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～Ver.1.4」, 2012 年（https://www.jnsa.org/result/incident/data/2011incident_survey_ver14.pdf）

[17] Train, K. Discrete Choice Methods with Simulation, Second Edition. Cambridge University Press, 2009

[18] Bennett, J., Adamowicz, V.: Some Fundamentals of Environmental Choice Modeling, Bennett, J., Blamey (edit) The Choice Modelling Approach to Environmental Valuation. Edward Elgar, pp.37-69, 2001

[19] 情報処理推進機構「2018 年度情報セキュリティに対する意識調査」, 2018 年（https://www.ipa.go.jp/security/fy30/reports/ishiki/index.html）

[20] 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 Proceedings, 1F1-6, 2017 年