Vol.2021-SPT-41 No.44
2021/3/2

SNSユーザの適切なプライバシー開示行動を促すナッジの検討

伊藤 詩歩[1]　成田 惇[1]　菅沼 弥生[1]　西垣 正勝[1]　大木 哲史[1]

概要：SNS を通じて誰もが自身や身の回りの環境に関する情報を自由に発信することが可能である．一方で，旅行中の写真投稿や書き込みによる空き巣被害や，投稿から個人が特定されたことによるストーカー行為被害，プライバシー情報を引き換えとした脅迫被害に遭遇する等，SNS ユーザが自身のプライバシー情報を公開することに起因するトラブルが生じている．そこで，本研究は SNS ユーザがトラブルに遭遇することを未然に防ぐため，ナッジにより SNS ユーザの適切なプライバシー開示行動を促すことを目的とする．これまで提案されたナッジは，ナッジの種類や提示方法による効果の違いが検証されてきた一方で，これらの効果がユーザによって異なる可能性を考慮していなかった．本研究では，特に SNS 利用者のプライバシー保護への関心の程度を考慮し，SNS ユーザのプライバシー開示におけるナッジの有効度と，プライバシー志向の関係について調査した．調査の結果から，ナッジを考えるにあたり，プライバシー懸念の程度を考慮することの重要性を明らかにし，また，SNS 利用の具体的なリスクを提示するナッジによりユーザの SNS 利用事体が脅かされる可能性を示した．

A Nudge Improving Decision about Privacy-Disclosure in Social Networks

Shiho Ito[1]　Jun Narita[1]　Yayoi Suganuma[1]　Masakatsu Nishigaki[1]　Tetsushi Ohki[1]

Abstract: Through social networking services (SNS), anyone can freely transmit information about themselves and their environment. On the other hand, there are some troubles caused by SNS users disclosing their privacy, such as burglary due to posting photos and messages during a trip, damage due to personal identification from posts, and threats in exchange for private information. In order to prevent SNS users from encountering these troubles, this study aims to encourage SNS users to manage their private information appropriately by using nudges. While the existing nudges have been verified to have different effects depending on the type of nudge and the presentation method, they have not taken into account the possibility that these effects may differ among users. This study investigated the relationship between the effectiveness of nudges in disclosing SNS users' privacy and their privacy intention, taking into account the degree of privacy concern of SNS users. The results show the importance of considering the degree of privacy concern when considering nudges. We also have shown that nudges that present specific risks of SNS use may threaten users' SNS use itself.

1. はじめに

インターネットやスマートフォンの普及に伴い，SNS を通じて誰もが自身や身の回りの環境に関する情報を自由に発信することが可能になってきている．また，SNS 利用者数は年々増加しており，総務省統計局の調査 [1] によると，平成 30 年の日本国民全体に対する LINE 利用者数の割合は約 60%となっている．

一方で，総務省総合通信基盤局の調査 [2] によると，旅行中の写真投稿や書き込みによる空き巣被害や，SNS 投稿から個人が特定されたことによるストーカー被害，プライバシー情報を引き換えとした脅迫被害に遭遇する等，SNS 利用をきっかけとするトラブルが発生している．これらのトラブルは，ユーザが SNS を利用する際に自身のプライ

[1] 静岡大学, 浜松市中区城北 3 丁目 5-1, Shizuoka University, 3-5-1 Jo-hoku, Naka-ku, Hamamatsu City, Shizuoka, Japan

バシー情報を公開することに起因しており，ユーザ自身がプライバシー情報の取り扱いに関する知識を身に付け，実践する必要性が高まっていると言える．しかし，SNS は誰でも容易に利用を開始することが可能であるため，SNS 利用によって生じ得るプライバシー上のリスクや，その適切な対策についての教育を SNS 利用を開始する前に全てのユーザに対して行うことは困難である．そのため，現在の SNS ユーザの多くは適切なプライバシー開示行動ができていない状態で SNS を利用していると考えられる．そこで，適切なプライバシー開示行動ができていない状態の SNS ユーザが，SNS 利用をきっかけとしたトラブルに遭遇することを未然に防ぐため，SNS ユーザに適切なプライバシー開示行動を促す必要がある．ここで，適切なプライバシー開示行動を，ユーザがプライバシー情報を公開するリスクを理解し，公開するプライバシー情報の内容と公開範囲を考慮した上で，プライバシー開示の判断を行うことと定義する．

本研究では SNS ユーザのプライバシー開示行動を促すためのアプローチとしてナッジに着目する．ナッジとは，行動の選択肢を設計することで人々が自分自身にとって良い選択を自発的にとる手助けをする手法である [3]．SNS におけるナッジに関する既存研究では，ナッジの種類や提示方法による効果の違いが検証されており，SNS ユーザへ SNS 利用に関する知識を与えるナッジを用いることで，ユーザのプライバシー情報開示における適切な意思決定のサポートが可能になることが示されている [4–6]．しかし，いずれの既存研究においても SNS ユーザによってナッジから受ける影響および影響の強さが異なる可能性について十分に調査がなされておらず，全てのユーザに対して有効なナッジ手法は未だに発見されていない．

そこで本研究では，ユーザごとの特性を考慮したナッジを検討することで，SNS ユーザへ SNS 利用時のプライバシー情報を管理する方法を改善する機会を与えることを目的とする．ここで，プライバシー保護への関心が高いユーザはプライバシー保護への関心が低いユーザに比べて，プライバシー情報開示をしにくい等，SNS 利用方法はユーザのプライバシー志向によって異なる [7] 点に着目し，ユーザごとの特性として特にプライバシー志向を考慮する．そして，アンケート調査を通してナッジの有効度とプライバシー志向の関係を明らかにする．この結果を用いて，ユーザのプライバシー志向に応じたナッジを提示することで，ユーザに対する負担が少ない形で SNS の利用方法を改善する機会が与えられ，これにより，プライバシー漏えいへの不安のない SNS 環境が実現されることが期待できる．

2. 関連研究

2.1 プライバシーナッジ

情報セキュリティとプライバシーの分野において，人々がより安全な行動や自身のプライバシーを重視した行動を促すことを目的としたナッジに関する研究が数多く行われてきた．モバイルデバイスの利用時に個人が情報を開示する可能性が高いと推測される場面における過度なプライバシー情報の開示を防ぐ研究 [5] では，ユーザが書いた電子メールをスキャンし，不要そうな箇所を検出，通知したり，自身が発信した情報を見ることが可能なユーザの存在を思い出させたりする手法を提案している．これらの手法は，ユーザが不適切に情報を発信するのを思いとどまらせることに有効であった．また，若年層ユーザが SNS を利用する際，プライバシー情報を含む投稿や，知らない人とコミュニケーションを取る等のリスクの高い行動をとることを防止するために有効なナッジを検討した研究が存在する [8]．若年層 SNS ユーザが行動を選択するようなシナリオにおいて，「55%の人は（SNS で知り合った人と 1 対 1 で）会わないそうだよ」といった否定文のナッジを提示した時の方が，「45%の人は会うそうだよ」といった肯定文のナッジを提示した時と比較して，実験参加者を望ましい回答の選択に誘導する効果があるということを明らかにした．また，プライバシーや安全促進の目的で肯定文のナッジは使用すべきではないと結論づけている．

これらの研究から，人々へより安全な行動やプライバシーを保護する行動を促すためにナッジが有効であることが分かる．しかし，これらの手法はユーザごとにナッジの有効度が違う可能性について考慮されておらず，全ての人に対して必ずしも有効な手段であるとは限らない．そこで本研究では，ユーザごとのナッジ有効度の差を考慮した SNS ユーザの適切なプライバシー開示行動を促すナッジを検討する．

2.2 安全な行動を促すためのユーザ特性を考慮した手段

これまで，人々のセキュリティ行動やプライバシー保護行動に影響を与えるユーザ要因の存在が示され，ユーザ毎に有効なセキュリティ対策が異なる可能性について検討されてきた．

Wisniewski らは，SNS ユーザを実際のプライバシー行動とプライバシー保護メカニズムの認識を基にクラス分けを行い，各クラスの性質に合致したプライバシー教育やナッジについて議論している [9]．また，佐野らは OS 更新を促すため有効なメッセージは，ユーザのセキュリティ対策の実施状況や経験要因により異なることを示している [10]．同様に，Briggs らは人々のセキュリティの習熟度や衝動制御能力の違いがナッジの効力に及ぼす影響について調査しており，調査の結果，公共の場で接続する wifi を選択するというシナリオにおいて，セキュリティの習熟度が高い人は低い人よりもナッジの効力が高く安全な wifi を選択する傾向があること，衝動制御能力が高い群は低い群に比べてナッジの効力が高く，安全な wifi を選択する傾向があるこ

とを明らかにした [6].

これらの研究は，より安全な行動やプライバシーを保護する行動を促すための手段は，ユーザ毎にその有効度が異なることを示している．そこで本研究では，SNS におけるユーザ毎に異なるプライバシーへの意識（プライバシー志向）が，プライバシー保護行動に影響を与えると仮定し，ユーザのプライバシー志向の違いがナッジの効力に及ぼす影響を調査する．これにより，ユーザのプライバシー志向に応じたナッジを提示することで，ユーザに対する負担が少ない形で SNS の利用方法を改善する機会を与え，プライバシー漏えいへの不安のない SNS 環境が実現されることが期待できる．

3. リサーチクエスチョンと仮説

本研究におけるリサーチクエスチョンを定義する:

[**RQ1**] SNS ユーザへ適切なプライバシー開示行動を促すことが可能なナッジはどのようなものか

[**RQ2**] SNS ユーザによってナッジの有効度に差は生じるのか

本研究におけるリサーチクエスチョンへの仮説を定義する:

[**H1**] SNS ユーザのプライバシー志向を考慮したナッジを提示することで適切なプライバシー開示行動を促すことが可能となる

[**H2**] SNS ユーザのプライバシー志向によってナッジの有効度に差が生じる

本研究ではユーザをプライバシー志向によってクラス分けして，各クラスのユーザに同じナッジを提示した場合の有効度の差を調査・分析することにより H1 および H2 を検証する．

4. 調査方法

本章では，前章で述べた仮説を検証するためのアンケート調査について述べる．本調査は 2021 年 1 月 15 日から 16 日にかけて実施した．参加者はクラウドソーシングサービスの lancers.jp[*1]を用いて募集し，仮説検証のため作成したアンケートの回答を依頼した．

4.1 参加者および手順

本調査では 1000 人の参加者を募集し，1000 人が参加した．また，参加者にはアンケート調査の参加報酬として 100 円を支払った．参加者は lancers.jp のアカウントを登録し，タスクに記載されているアンケート URL から LimeSurvey[*2]によって作成されたアンケートの回答ページに移り，匿名でアンケートに回答した．アンケート終了後，参加者には固有のタスク完了パスワードが表示され，パスワードを lancers.jp のタスク依頼フォームに入力することで，タスクは完了する．1 人あたりのアンケート想定所用時間はアンケート概要の説明からタスク完了パスワードの入力完了までであり，15 分程度である．

4.2 アンケートの構成

アンケート調査は「アンケートの概要」「SNS 利用場面を想定した 4 つのシナリオとその質問項目」「プライバシー懸念に関する質問」「SNS 利用方法に関する質問」の 4 項目により構成した．[*3] SNS 利用場面を想定した 4 つのシナリオとその質問項目では，1 つのシナリオに対しナッジがない場面とナッジが 1 種類提示される場面を用意し，参加者へ 4 つのシナリオすべてに対して回答を求めた．提示するナッジは 4 種類の中からランダムで選ばれるように設計した．各場面では「〜する」,「〜しない」という 2 択の選択肢を示し,「〜する」という選択肢を潜在的にリスクの高い選択肢とし,「〜しない」という選択肢をプライバシーや安全に配慮した選択肢とした．本稿ではこれ以降，参加者が「〜する」,「〜しない」のいずれかの選択を行うことを選択行動と呼ぶ．その後，ナッジに対する印象を問う質問，選択行動時にナッジがどの程度判断材料となったかとその理由についての質問への回答を求めた．このとき，判断材料になったか否かの理由への回答は自由記述形式，その他の質問への回答は (1)〜(5) の 5 段階リッカート尺度を用いた．なお，本調査では「全く当てはまらない (1)」のように数値を合わせて示すことで，参加者間での尺度間隔を一定としている．また，シナリオが表示される順序は，順序効果の影響を回避するため，参加者によりランダムに表示されるように設計した．

また，プライバシー懸念に関する質問項目の中に,「この質問には ”やや当てはまる (4)” を選択してください.」といった注意力テスト [11] を加えた．これにより 17 名の参加者が除外された．

アンケートの作成にあたっては，Lancers を通して計 100 名に対して実施したパイロット調査の結果を用いて質問紙の質を向上させた．なお，パイロット調査・本調査ともに参加した参加者が存在していたが，これらの参加者は本調査での回答へバイアスがかかることを考慮して除外した．

4.2.1 調査シナリオおよびナッジ

本調査が対象とする SNS 利用において一般的に用いられるいくつかの用語を以下にまとめる．

フォロワー

自身の投稿を（積極的に）閲覧するアカウントを指す．

[*1] https://www.lancers.jp
[*2] https://www.limesurvey.org
[*3] 本調査で使用したアンケート用紙は，下記の Web サイトに掲載する．https://github.com/ohkilab/improving-decision-nudge/

フォロワーが SNS にログインすると，フォロワーの SNS 利用ページに自身の投稿が表示される．

公開アカウント

自身の投稿を誰でも閲覧できる状態にしているアカウントを指す．公開アカウントの投稿は，フォロワー以外でも（検索等を行うことで）閲覧することができる．

非公開アカウント

自身の投稿を自身がフォローリクエストを許可したユーザ（フォロワー）のみ閲覧できる状態にしているアカウントを指す．

本調査では，先行研究 [4] における 9 つのシナリオからプライバシー情報の管理を行う場面を想定した 4 つのシナリオを選択し，調査設定に合致するよう一部変更した．

S1：友達との自撮り写真の投稿

友達と外出先で撮影した自撮り写真を SNS へ投稿しようとしている場面において，友達の許可無しに自撮り写真を SNS へ投稿するか否かの判断を仰ぐシナリオである．このシナリオではユーザのアカウントは公開アカウントとした．これは，自分以外の人物のプライバシー情報の管理を行う場面を想定している．本人の許可なく写真を投稿すると，本人の予期せぬプライバシー情報悪用による被害が生じる場合や，肖像権の侵害にあたる場合があるため，本人へ投稿の許可を得てから投稿することが望ましい．

S2：自身の顔が写っている写真の投稿

SNS へ自身のプライバシー情報を含む投稿をするか否かの判断を仰ぐシナリオである．このシナリオではユーザのアカウントは公開アカウントとした．また，投稿を試みている写真として，自身の顔が写っている写真を想定するよう参加者に指示した．これは，自身の顔情報の管理を行う場面を想定している．自身の顔を含む写真を投稿をすることは，出会い系サイトへの無断使用等の悪用リスクがあるため，顔を隠したり，公開範囲を限定することが望ましい．

S3：自身の居場所が特定できる写真の投稿

旅行先で撮影した写真をその場で SNS へ投稿するか否かの判断を仰ぐシナリオである．このシナリオではユーザのアカウントは公開アカウントとし，投稿により自身の現在の居場所が特定できる場面を想定するよう参加者に指示した．これは，自身の位置情報の管理を行う場面を想定している．自身の居場所が特定できる写真やテキストを投稿をすることは，居住地が特定されたり，家の不在が知られ空き巣被害に遭遇するリスクがあるため，位置情報の特定を困難にする工夫をしたり現在地のリアルタイムな投稿を控えることが望ましい．

S4：面識のないユーザからのフォローリクエストの許可

共通の趣味を持ったユーザからフォローリクエストがきた場合に，リクエストを許可するか否かの判断を仰ぐシナリオである．このシナリオではユーザのアカウントは非公開アカウントとした．これは，自身の情報の公開範囲の管理を行う場面を想定している．面識のない第三者からのフォローリクエストを許可することは悪意を持ったユーザがプライバシー情報を悪用するリスクがあるため，面識のないユーザからのフォローリクエストは許可しないか，フォローリクエストを送信してきたアカウントを吟味した上で許可することが望ましい．

ナッジを考慮するにあたり，既存研究において提案されてきた様々なナッジ [12] の中から，SNS のインターフェイスを大きく変更する必要がなく，今回のシナリオに当てはめた際に違和感のないナッジを 3 つ選択し，調査用に一部修正してアンケートに用いた．シナリオと対応するナッジメッセージを表 1 に示す．なお N1，N2 は同じナッジを使用しているがメッセージが異なる．N1 は他のユーザが自身の投稿へアクセスできることについて，N2 は他のユーザ投稿に含まれる情報を入手できることについて，それぞれ「〜する」とした場合の結果を示している．知らせる行動の結果によって反省を促せるか否かが異なることを考慮し，2 つのメッセージを用意した．

N1，N2：Reminding of the consequences

個人に自身の行動の結果をあらかじめ知らせることで行動に対する反省を促すナッジ

N3：Reducing the distance

今後起こり得るリスクの重要さを知らせることで，未来のリスクを想定した行動をすることを促すナッジ

N4：Providing multiple viewpoints

新たな行動の選択肢を提示することで，行動に対する反省を促すナッジ

4.2.2 プライバシー懸念の評価

本研究では，プライバシー情報開示におけるユーザが提供するプライバシー情報に対するプライバシー懸念を測定するため，PCIA（Privacy Concerns related to Information Abuse）および PCIF（Privacy Concerns related to Information Finding）[13,14] を使用した．PCIA は自身の情報を第三者が入手し悪用することをどの程度懸念しているかを測定する尺度である．PCIF とは自身の情報を第三者が入手すること自体をどの程度懸念しているかを測定する尺度である．それぞれを測定するための質問項目は全てを利用し，それぞれの質問項目は「全く当てはまらない (1)」〜「非常に当てはまる」(5) の 5 段階のリッカート尺度で回答してもらうよう設計した．

5. 結果および分析

[H1] および [H2] を検証するため，ユーザのプライバシー志向ごとのナッジの有効度，ユーザのプライバシー志向がナッジ判断に与える影響，ナッジの内容がナッジ有効度に与える影響について分析する．ここで，ナッジが有効で

表 1 シナリオと対応するナッジメッセージ

シナリオ	ナッジ	
S1	N1	あなたをフォローしていないユーザのタイムラインにもこの投稿が表示されるかもしれません
	N2	一緒に写っているあなたの友達はこの投稿を見て初めて自身の顔が公開されていることに気付きます
	N3	本人の許可なく本人の画像を投稿した際にプライバシー情報を悪用されるトラブルや肖像権の侵害をめぐる裁判が起きています
	N4	自分の許可なく自分の写真を投稿されることを不快に思うユーザも存在します
S2	N1	あなたをフォローしていないユーザのタイムラインにもこの投稿が表示されるかもしれません
	N2	この記事へアクセスした人はあなたの顔を知ることができます
	N3	顔写真が広告や出会い系サイトの画像に無断で使用されたり悪意のある加工をして拡散される事件が数多く起きています
	N4	顔が写っている画像の投稿に危険を感じるユーザも存在します
S3	N1	あなたをフォローしていないユーザのタイムラインにもこの投稿が表示されるかもしれません
	N2	この記事へアクセスした人はあなたの現在の居場所を知ることができます
	N3	リアルタイムな居場所を公開することで家の不在が知られ空き巣の被害が起きています
	N4	テキストや写真の撮影日時・場所の情報から投稿者の現在の居場所が推測できる投稿に危険を感じるユーザも存在します
S4	N1	リクエストを許可されたユーザのタイムラインにあなたの投稿が表示されるようになります
	N2	リクエストを許可されたユーザはあなたの投稿から情報を入手できるようになります
	N3	悪意を持った人物が自身を偽って他ユーザに接近し入手した情報を悪用する事件が起きています
	N4	顔見知りでないユーザのフォローリクエストを許可することに危険を感じるユーザも存在します

あった，とはナッジの観測により参加者がプライバシー開示の意思決定を変更したこと，すなわちナッジが無い場合に「〜する」と回答した参加者が，ナッジを提示した場合に「〜しない」と回答したことを意味する．またナッジ有効数を，ナッジを観測した参加者のうちナッジが有効であった参加者の数として定義する．プライバシー志向の評価には，PCIA 値および PCIF 値を用いる．PCIA 値は PCIA に関する 4 つの質問項目の回答を平均した値とする．PCIF 値は，PCIF に関する 3 つの質問項目の回答を平均した値とする．3 つ目の質問項目の回答の値は，3 つ目の質問項目を構成する 6 つのサブ質問項目の回答の平均値である．

本稿において，ナッジ有効度は，特定のナッジを観測したユーザのうちそのナッジが有効であったユーザの割合として定義する．一方本調査では，シナリオ間およびナッジ間の参加者割り当て数はほぼ均一，すなわち特定のナッジを観測したユーザ数は全てのナッジ間でほぼ均一である．このため結果の分析においてはナッジ有効数をナッジ有効度の指標として扱っている．

分析には，本調査に参加した 1000 人の回答のうち，注意力テストに誤答した，またはパイロット調査に参加していた参加者を除いた計 928 名の回答結果を使用した．また本調査では，参加者 1 人当たり 4 つのシナリオへ回答したため，回答の総数は参加者数の 4 倍である 3712 となる．参加者 1 人あたりのアンケート実施時間は，アンケート概要の説明からタスク完了パスワードの入力完了までであり，およそ 15 分であった．

5.1 ユーザのプライバシー志向とナッジ有効度の関係

ユーザのプライバシー志向ごとにナッジ有効度が異なるかどうかを確認するため，χ^2 検定を実施した．検定は，ナッジが有効であった参加者から構成される群を有効群，それ以外を無効群とした．また，参加者の PCIA 値の平均値を算出し，平均値よりも高い PCIA 値の参加者を PCIAH 群，平均値よりも低い PCIA 値の参加者を PCIAL 群とした．同様に，参加者の PCIF 値の平均値を算出し，平均値よりも高い PCIF 値の参加者を PCIFH 群，平均値よりも低い PCIF 値の参加者を PCIFL 群とした．PCIAH 群と PCIAL 群の間にナッジ有効数の差があるか，PCIFH 群と PCIFL 群の間にナッジ有効数の差があるかを χ^2 検定により検証した．検定の結果を表 2 に示す．有意確率 $p < 0.05$ で有意差がある場合は灰色で強調される．表 2 より，PCIAH 群と PCIAL 群には有意差があり，PCIAH 群の方が PCIAL 群よりもナッジ有効数が多く，ナッジの有効度が高いことがわかる．同様に，PCIFH 群と PCIFL 群には有意差があり，PCIFH 群の方が PCIFL 群よりもナッジ有効数が多く，ナッジの有効度が高いことがわかる．これらの結果から，自身の情報を第三者が入手することへの懸念の程度や，自身の情報を第三者が入手し悪用することへの懸念の程度といった参加者のプライバシー志向がナッジを考慮した選択を行うかどうかの要因となっていることが確認できた．

表 2 ナッジ有効数と PCIA・PCIF の高低群に対する χ^2 検定の結果
($\text{PCIA}: p < 0.01, \chi^2 = 57.443$/ $\text{PCIF}: p < 0.05, \chi^2 = 4.818$)

	PCIAH	PCIAL	PCIFH	PCIFL
ナッジ有効数	**383**	200	**318**	265

5.2 ユーザのプライバシー志向がナッジ判断に与える影響

5.1 節では，ナッジにより選択行動に変化があったユーザの数を有効数として評価を行った．一方で，潜在的には選択に変化がなかった参加者にも，ナッジを判断基準とした参加者が存在すると考える．ここでは，ナッジを観測した参加者のうち「表示されたメッセージは〜するか否かの判断材料になりましたか」という質問に対して「少しなった (4)」または「かなりなった (5)」と回答した参加者

表 3 ナッジ判断基準数と PCIA・PCIF の高低群に対する χ^2 検定の結果（PCIA:$p < 0.01$,$\chi^2 = 249.043$/PCIF:$p < 0.01$,$\chi^2 = 76.787$）

	PCIAH	PCIAL	PCIFH	PCIFL
ナッジ判断基準数	**1637**	850	**1462**	1025

の数をナッジ判断基準数とし，5.1 節と同様 PCIAH 群と PCIAL 群の間にナッジ判断基準数の差があるか，PCIFH 群と PCIFL 群の間にナッジ判断基準数の差があるかを χ^2 検定により検証した．検定の結果を表 3 に示す．有意確率 $p < 0.05$ で有意差がある場合は灰色で強調される．表 3 より，PCIAH 群と PCIAL 群には有意差があり，PCIAH 群の方が PCIAL 群よりもナッジ判断基準数が多く，ナッジの有効度が高いことがわかる．同様に，PCIFH 群と PCIFL 群には有意差があり，PCIFH 群の方が PCIFL 群よりもナッジ判断基準数が多く，ナッジの有効度が高いことがわかる．以上より，[H1] および [H2] を支持する結果が得られた．

5.3 ナッジの内容がナッジ有効度に与える影響

ナッジごとの有効度の差を明らかにするため，N1 から N4 でペアを作り χ^2 検定を行った．また，プライバシー志向の差が各ナッジに対する有効度に差をもたらすのかを明らかにするため，PCIA 値と PCIF 値の高低群に分割した．検定の結果を表 4 に示す．有意確率 $p < 0.05$ で有意差がある場合は灰色で強調される．表 4 より，N1 から N4 の中で N3 がもっとも有効数が多く，ナッジの有効度が高いことがわかる．

6. 議論

6.1 ユーザのプライバシー志向とナッジの有効度の関係

5.1 節の結果から，ユーザのプライバシー志向によってナッジ有効度に差が生じることが確認された．このことから，PCIA や PCIF によって計測されるユーザのプライバシー志向はナッジの有効度に影響を与え，プライバシー開示行動を促すためには全ての SNS ユーザに同じナッジを提示するのではなく，ユーザごとのプライバシー懸念の程度の違いを考慮したナッジを提示する必要があると言える．

また，5.2 節より，選択行動に変化が無かった参加者にも，潜在的にはナッジを判断基準とした参加者が存在することが明らかになった．自由記述による回答では，これらの参加者がナッジを判断基準とした理由として，「ナッジによりプライバシーリスクを改めて強く意識したから」や「自身の意思が正しかったことを再認識できたから」など自身が既に認識していた懸念事項でも，ナッジにより改めて指摘されることでその重要性を再認識したり，より強く意識することが可能になったことが挙げられていた．更に，もともとプライバシー情報開示への抵抗感を感じていた参加者の中には，自身の投稿にアクセスできる第三者の存在を知らされるナッジ (N1) により「自身のプライバシー情報が第三者に取得される」ということを強く意識するようになった参加者が存在した．このことから，PCIA 値や PCIF 値が高く，普段からプライバシーリスクを認識している，または漠然とプライバシーリスクを意識しているユーザにも，投稿に含まれる具体的なプライバシー情報の存在を知らせるナッジ (N2) や，プライバシー情報を悪用される具体的な場面を知らせるナッジ (N3) を用いることで，既に認識している事項の再認識，あるいはより強い認識を促し，より適切なプライバシー開示行動へと結びつけることができると考える．

6.2 ナッジの内容がナッジ有効度に与える影響

5.3 節より，N3 はナッジ有効数およびナッジ判断基準数が，N1 から N4 の中で最も多い．このことから N3 は 4 種類のナッジの中で最も有効度が高いナッジであることが分かる．しかし，N3 が有効だった参加者には，自由記述による回答において，N3 に対し「SNS 利用に恐怖を覚えた」や「リスクが具体的に示されて怖くなり何もできなくなった」と回答した参加者が存在した．ナッジを提示する際は，利用者にとっての負担が少ない形で適切なプライバシー開示行動を促す必要があるが，N3 は SNS 利用に伴うリスクを直接的に示しており，参加者によっては SNS 利用に恐怖を感じ，SNS 利用自体を躊躇したりしてしまうことがあった．したがって，SNS 利用に伴うリスクを直接的に示すナッジは，必ずしも適切なプライバシー開示行動を促すナッジとして適当ではないと言える．

N3 以外のナッジに関しては，PCIA 値および PCIF 値の高低にかかわらずナッジ間の有効数および判断基準数に違いは見られず，ナッジの有効度には差が無かった．

よって，今回のナッジには PCIA 値や PCIF 値が低い参加者にはリスクを直接的に伝える以外の手法でプライバシー開示行動を促す手法がないと言える．これはナッジにより与えられた情報を事実として認識しても，自身に置き換えて考慮しないなど重要視しないためだと考えられる．このような PCIA 値や PCIF 値が低い参加者に対しても，直接的にリスクを伝える以外の方法でプライバシー開示行動を促すには，どのようなナッジが有効であるかを検討する必要がある．

6.3 制限事項

今回の調査では，プライバシー志向によるナッジの有効度の差を明らかにすることに焦点を当てているため，検討したナッジの種類は限定的であった．また，実際の SNS 利用を想定したアンケート調査であるため，ユーザごとに異なるはずである SNS の利用方法や投稿内容の違いは考慮

表 4　ナッジと PCIA・PCIF の高低群に対するナッジ有効数およびナッジ判断基準数の χ^2 検定の結果

	ナッジ有効数				ナッジ判断基準数			
	PCIAH	PCIAL	PCIFH	PCIFL	PCIAH	PCIAL	PCIFH	PCIFL
N1-N2	74-91	41-46	58-75	57-62	389-409	205-213	352-361	242-261
N1-N3	**74-137**	**41-82**	**58-121**	**57-98**	**389-446**	**205-248**	352-399	**242-295**
N1-N4	74-81	41-31	58-64	57-48	389-393	205-184	352-350	242-227
N2-N3	**91-137**	**46-82**	**75-121**	**62-98**	409-446	213-248	361-399	261-295
N2-N4	91-81	46-31	75-64	62-48	409-393	213-184	361-350	261-227
N3-N4	**137-81**	**82-31**	**121-64**	**98-48**	**446-393**	**248-184**	399-350	**295-227**

できていない．そのため，普段投稿を全く行わないユーザへは，普段用いない SNS の利用方法を想定して回答を仰いでしまっている．

今回の分析では，ユーザを PCIA 値・PCIF 値それぞれに対して高いか，低いかの 2 群に分けている．しかし，より詳細なユーザごとのナッジ有効度の差を調査するためには，さらにユーザのクラス分けを細分化する必要がある．

6.4　研究倫理

本研究において実施したアンケートは，内容や実施手順がアンケート実施者の所属組織の倫理委員会が定めた基準に照らし，審査を要する事例には該当しない範囲内であることを確認の上，実施された．実施にあたって，実験参加者は事前にアンケート内容について知られされており，自由意志に基づいた同意のもと参加している．また，個人情報の取り扱いは，日本国の個人情報保護法に準拠した方法に基づいている．

7.　まとめ

本研究では，SNS ユーザのプライバシー開示に起因するトラブルを未然に防ぐことを目的として，SNS ユーザへ適切なプライバシー開示行動を促すためのユーザのプライバシー思考を考慮したナッジを検討した．アンケート調査の結果から，SNS ユーザのプライバシー志向によりナッジ有効度に差があり，PCIA 値や PCIF 値が高いユーザは PCIA 値や PCIF 値が低いユーザに比べてナッジ有効度が高いことが明らかになった．また，SNS 利用におけるプライバシー開示行動に伴うリスクを直接的に提示するナッジは利用者へ恐怖を与え，SNS 利用そのものまで脅かしてしまう可能性があることを示した．この結果は，SNS 利用時にユーザのプライバシー志向に応じたナッジの提示を実現し，ユーザにとっての負担が少ない形で SNS 上でのプライバシー漏えい対策を行う一助となると考えられる．

今後の課題は，PCIA 値や PCIF 値が低いユーザに対してリスクを直接的に示す以外で有効度が高いナッジを検討，提案することである．これにより，全てのユーザに対してユーザにとっての負担が少ない形で SNS の利用方法を改善する機会を与え，プライバシー漏えいへの不安のない SNS 環境を実現することが期待される．

参考文献

[1] 総務省統計局：平成 30 年版情報通信白書ソーシャルメディアの利用状況 (2019). https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd142210.html.
[2] 総務省：インターネットトラブル事例集 (2020 年版) (2020). https://www.soumu.go.jp/main_content/000681954.pdf.
[3] Thaler, R. H. and Sunstein, C. R.: *Nudge: Improving decisions about health, wealth, and happiness*, Penguin Books (2009).
[4] Masaki, H., Shibata, K., Hoshino, S., Ishihama, T., Saito, N. and Yatani, K.: Exploring Nudge Designs to Help Adolescent SNS Users Avoid Privacy and Safety Threats, *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems*, pp. 1–11 (2020).
[5] Balebako, R., Leon, P. G., Almuhimedi, H., Kelley, P. G., Mugan, J., Acquisti, A., Cranor, L. F. and Sadeh, N.: Nudging users towards privacy on mobile devices, *Proc. CHI 2011 Workshop on Persuasion, Nudge, Influence and Coercion*, Citeseer, pp. 193–201 (2011).
[6] Briggs, D. J. L. C. P. and van Moorsel, A.: Nudging whom how: IT proficiency, impulse control and secure behaviour, *Networks*, Vol. 49, p. 18 (2014).
[7] Taddei, S. and Contena, B.: Privacy, trust and control: Which relationships with online self-disclosure?, *Computers in Human Behavior*, Vol. 29, No. 3, pp. 821–826 (2013).
[8] Kroll, T. and Stieglitz, S.: Digital nudging and privacy: improving decisions about self-disclosure in social networks, *Behaviour & Information Technology*, pp. 1–19 (2019).
[9] Wisniewski, P. J., Knijnenburg, B. P. and Lipford, H. R.: Making privacy personal: Profiling social network users to inform privacy education and nudging, *International Journal of Human-Computer Studies*, Vol. 98, pp. 95–108 (2017).
[10] 佐野絢音，澤谷雪子，　山田明，　窪田歩：セキュリティ行動変容ステージに応じた OS 更新を促すメッセージの提案，*Symposium on Cryptography and Information Security* (2020).
[11] 三浦麻子，小林哲郎：オンライン調査における努力の最小限化 (Satisfice) 傾向の比較: IMC 違反率を指標として，メディア・情報・コミュニケーション研究 (2016).

[12] Caraban, A., Karapanos, E., Gonçalves, D. and Campos, P.: 23 ways to nudge: A review of technology-mediated nudging in human-computer interaction, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–15 (2019).
[13] Preibusch, S.: Guide to measuring privacy concern: Review of survey and observational instruments, *International Journal of Human-Computer Studies*, Vol. 71, No. 12, pp. 1133–1143 (2013).
[14] Dinev, T. and Hart, P.: Internet privacy concerns and their antecedents-measurement validity and a regression model, *Behaviour & Information Technology*, Vol. 23, No. 6, pp. 413–422 (2004).