ヘルスケアアプリのインストール同意におけるプライバシー保護技術の効果について

菊池 浩明[1,a)]　金森 祥子[2,b)]　荒井 ひろみ[4,c)]　森 由希子[3,d)]　野島良[5,e)]

概要：ヘルスケア情報などの機微な情報を取得するアプリは，将来の疾病罹患などを予見して生活習慣を改善することが期待できる一方，自分の個人情報が漏洩したり，支持しない製薬開発などに無断で用いられたりすることに懸念がある．識別子や特異な値を削除することでデータから本人が識別できないようにする匿名化技術や機微な値に対してランダムなノイズを加えて真の値が分からないようにする差分プライバシー技術などのプライバシー保護技術 PETs が研究されている．しかしながら，技術を説明する同意文書が難解で判断できないユーザや技術全般に対して不信頼感を持つユーザが一定数存在する．そこで，本研究では，複数の同意文書を用意して，被験者実験を行い，どの様な条件や説明文書によってユーザの不安を取り除き，利用に対する同意が得られるのか明らかにすることを試みる．

キーワード：局所差分プライバシー，ヘルスケア

Is a choice of privacy-enhancing technologies significant for user consent to the installation of a healthcare app?

Hiroaki Kikuchi[1,a)]　Sachiko Kanamori[2,b)]　Hiromi Arai[4,c)]　Yukiko Mori[3,d)]　Ryo Nojima[5,e)]

Abstract: Healthcare applications helps improve lifestyle habits by predicting future disease risks. At the same time, however, there are concerns that such personal information may leak or be misused without consent for purposes pharmaceutical development that the user does not support. Privacy-enhancing technologies (PETs) have been studied to mitigate these risks, including anonymization techniques that prevent individual identification by removing identifiers and outliers, and differential privacy techniques that add random noise to sensitive values so that the true values cannot be inferred. Nevertheless, there remains a certain number of users who find consent documents explaining these technologies too complex to understand, or who harbor distrust toward the technologies in general.
In this study, we prepared multiple versions of consent documents and conducted user experiments to examine what conditions and with what types of explanations users' concerns can be effecrtive, and consent to the use of such applications can be installed.

Keywords: Local differential privacy, healthcare

1. はじめに

近年，スマートフォンやウェアラブル端末の普及に伴

[1] 明治大学総合数理学部
School of Interdisciplinary Mathematical Sciences, Meiji University
[2] 情報通信研究機構サイバーセキュリティ研究所
National Institute of Information and Communications Technology Cyber Security Research Institute
[3] 京都大学・医学部附属病院
Kyoto University Hospital
[4] 理化学研究所・革新知能統合研究センター
RIKEN/ AI Safety and Reliability Unit
[5] 立命館大学情報学部
Ritsumeikan University, Faculty of Informatics
[a)] kikn@meiji.ac.jp
[b)] kanamori@nict.go.jp
[c)] hiromi.arai@riken.jp
[d)] yukimori@kuhp.kyoto-u.ac.jp
[e)] ryo.nojima@gmail.com

い，ヘルスケアアプリを通じて日常的に健康関連データを収集・解析することが一般化しつつある．これらのアプリは，生活習慣の改善や将来の疾病罹患リスクの予見に寄与する可能性を有しており，公衆衛生や個人の健康増進に大きな役割を果たすことが期待されている．一方で，アプリ利用者の中には，自らのセンシティブな個人情報が第三者に漏洩したり，意図しない研究や製薬開発に無断で利用されたりすることへの懸念から，インストールや利用を見送るケースも少なくない．

こうした懸念に応える技術として，プライバシー保護技術（Privacy-Enhancing Technologies: PETs）が研究・導入されている．識別子や特異値を除去する匿名化技術や，個々のデータにランダムなノイズを加えることで真の値を秘匿する差分プライバシー（Differential Privacy; DP）が代表的である．特に DP は，理論的に堅牢なプライバシー保証を提供できることから注目され，プラットフォーマーや研究機関での採用が進んでいる．しかしながら，その数理的背景やリスク・利点の説明は一般利用者にとって理解が困難であり，また技術全般に対する不信感から同意判断が容易ではないという課題がある．

これらの課題に対して，Xion らは [2] ユーザがデータの共有の意思決定を行う際に，DP をどの様に説明すると効果的であるかを，同意文書の例を複数用意したユーザ実験により明らかにしている．Nanayakkara ら [3] は，DP における中心的パラメータであるプライバシー費用 ϵ の説明可能性に焦点を当て，リスクを具体的に提示した説明がユーザの理解度と納得感を高めることを明らかにした．中川らの [4] は，匿名加工情報や仮名化加工情報といった制度が，市民にどのように受け止められているかを明らかにしている．市民は個人データの利用に対して一律に拒否的ではなく，利用目的や提供先によって許容度が大きく変化すること，および，公共的・公益的な目的での活用には一定の理解が得られる一方，営利目的の利用には強い慎重さが見られた．

そこで，先行研究の知見を元にして，本研究ではヘルスケアアプリに関する利用者の同意形成に焦点を当てる．複数の同意文書を準備し，クラウドソーシングによる大規模なユーザ実験を通じて，どのような条件や説明の仕方がユーザの不安を軽減し，インストールや利用に対する同意を促進するかを明らかにすることを目的とする．これにより，PETs の理論的有効性と実際のユーザ受容性とのギャップを埋め，プライバシー配慮型ヘルスケアサービスの普及に資する知見を得ることを目指す．

本研究のリサーチクエスチョンは次のとおりである．

RQ1.差分プライバシーによる機微情報の保護機構は，ユーザの安心感を高めてアプリのインストール同意率を向上させるか？

RQ2.ユーザは同意書から，正しくプライバシー保護の仕組みやリスクを理解できるか？（どのように説明するのが効果的か）

RQ3.ユーザの不信感や不安を高めている原因は何か？

2. 関連研究

2.1 Xiong らの DP の説明に関する研究

Xiong らは [2], ユーザがデータの共有の意思決定を行う際に，DP をどの様に説明すると効果的であるかを，同意文書の例を複数用意したユーザ実験により明らかにしている．特に，LDP と DP の違いに焦点を置き，ユーザがリスクの違いを正しく理解できるかを調査している．

彼らは，ロールプレイにより，アプリをインストールした状況を想定し，正確な診断のためにアプリが取得する個人データの種類や取得方法を調査している．DP を数理的に説明するよりも，比喩的かつ直感的に説明することで，ユーザの理解度が有意に向上することが示された．また，ユーザは「どの程度データが保護されるか」という定性的な情報を重視しており，ϵ の数値そのものよりもリスクの具体的な解釈に基づいて意思決定を行う傾向が明らかとなった．さらに，効果的な説明は単に理解度を高めるだけでなく，ユーザの不安を軽減し，データ共有に対する信頼と積極性を高めることにもつながることが確認された．

2.2 Nanayakkara らの ϵ の説明可能性調査

Nanayakkara らの研究 [3] は，DP における中心的パラメータであるプライバシー費用 ϵ の説明可能性に焦点を当てている．理論的には ϵ が小さいほどプライバシー保証は強くなることが知られているが，非専門家にとって数値の意味を理解することは極めて難しい．従来の同意文書やプライバシーポリシーでは，ϵ を単に「プライバシー予算」として提示するのみであり，ユーザはその数値が自らのリスクや利便性にどう影響するかを判断できない．プライバシー費用の概念をユーザに直感的かつ実用的に理解させ，差分プライバシーの採用やデータ提供の意思決定を支援する説明方法を確立することを目的にしている．

そこで，彼らはまず理論的背景を整理し，ϵ がどのようにリスクの度合いと対応するかを可視化する複数の説明デザインを設計した．リスクを生起確率と非生起の比であるオッズで定量化し，それをテキストによる説明，グラフに可視化した説明，具体的な数値例にした説明などを提供し，比較対象とした．クラウドソーシングによる大規模なユーザ実験を行い，参加者に異なる説明を提示した上で，理解度・安心感・意思決定への影響を測定した．さらに，参加者の属性や背景知識を考慮し，説明方式ごとの効果の差異も分析した．

単に「ϵ が小さいとプライバシーが強い」と説明するよりも，リスク（オッズ) の形で具体的に提示した説明がユーザの理解度と納得感を高めることが明らかになった．また，

数値の大きさだけでなく「自分のデータがどの程度識別され得るか」といった確率的直感を与えることが，ユーザの同意判断に強く影響することが示された．さらに，解釈を工夫することで，技術的背景を持たないユーザでも差分プライバシーを理解しやすくなり，DP 技術に対する信頼を高められる可能性があることを示した．

2.3 中川らによる社会調査

中川らのの研究 [4] は，匿名加工情報や仮名化加工情報といった制度が，市民にどのように受け止められているかを明らかにすることを目的としている．改正個人情報保護法により匿名加工情報が制度化されたものの，その作成方法や安全性に関する理解は一般の事業者や利用者に十分浸透していない．さらに，技術的に高度な匿名化の競技会である PWSCUP の成果があっても，「法制度で定義される匿名加工や仮名化が，一般市民にとって望ましい形態なのか」という社会的受容性は未解明であった．この研究は，制度と技術のあいだにある「社会的合意形成のギャップ」を埋めることを狙っている．

彼らは 全国 1045 名の一般市民を対象にした大規模なアンケート調査を実施した．調査では，匿名加工情報や仮名化加工情報といった概念をわかりやすく提示した上で，それらがどの程度受容可能か，どのような利用条件なら許容されるのかを質問した．また，利用目的や提供先の種類ごとに，市民が感じるリスクや許容度の差を定量的に把握できるよう設計されていた．これにより，法律上の制度と市民の意識の間にある認識のズレをデータとして明らかにした．

主要な結論として，市民は個人データの利用に対して一律に拒否的ではなく，利用目的や提供先によって許容度が大きく変化することが示された．特に，公共的・公益的な目的での活用には一定の理解が得られる一方，営利目的の利用には強い慎重さが見られた．また，匿名化や仮名化といった技術的枠組みによってプライバシーリスクが軽減されることは理解されているが，その安全性や実効性への信頼は十分でないことも浮き彫りになった．この結果は，制度設計や事業者による説明責任において，市民のリスク認知を前提とした丁寧な情報提供が必要であることを示唆している．

3. 調査方法

糖尿病罹患リスクを予測するアプリを想定し，複数の条件の同意書を用意してユーザ調査を行う．表 1 にアンケート概要を示す．本調査にはクラウドソーシングサービス Cloudworks [*1] を用いた．実際に用いたアンケート文と同意書の例を，付録 A.1 と A.2 に示す．

[*1] https://crowdworks.jp/public/jobs/12369085

表 1 アンケート調査概要

項目	値
日時	2025 年 8 月 11 日（月） 8:35 – 11:30
被験者	クラウドワークス契約ワーカー (作業承認率が 95%以上)
仕事量	20 問 (10 分程度)

リスクの高さに関して，次の 2 種類を設定する．

(1) 低リスク

$\epsilon = \ln 2 (0.69)$

「貴方が糖尿病の罹患リスクがある時，このアプリは 2/3 の確率でリスクあり，1/3 の確率でリスクなしと回答します.」(正直に回答する頻度が低い)

(2) 高リスク

$\epsilon = \ln 4 (1.38)$

「貴方が糖尿病の罹患リスクがある時，このアプリは 4/5 の確率でリスクあり，1/5 の確率でリスクなしと回答します.」(正直に回答する頻度が高い)

プライバシー費用 ϵ の説明に関しては，次の 2 種類を用意する．

(1) 加工方法の説明

「差分プライバシーは，機微な値に確率的なノイズを加えることで真の値を分からなくすることを理論的に保証しています.」「貴方が糖尿病の罹患リスクがある時，このアプリは 2/3 の確率でリスクあり，1/3 の確率でリスクなしと回答します．罹患リスクがない時は，2/3 の確率でリスクなし，1/3 の確率でリスクありと回答します」真の値 x の摂動化 y は，$\epsilon = \ln 2$ の時，

$$Pr[y = 1|x = 1] = \frac{e^{\epsilon}}{e^{\epsilon} + d - 1} = \frac{2}{3}$$

(2) 漏洩リスクの説明

「差分プライバシーは，機微な値に確率的なノイズを加えることで真の値を分からなくすることを理論的に保証しています.」「このアプリで差分プライバシーでノイズを加えて「リスクあり」と回答した時，100 名中 15 名は貴方が本当に糖尿病の罹患リスクがあると確信します．日本における成人の糖尿病有病率は 8%です.」摂動化 y が与えられた時，真の値 x が露見する確率は，$\epsilon = \ln 2$ の時，

$$Pr[y = 1|x = 1] = \frac{e^{\epsilon}}{e^{\epsilon} + d - 1} = \frac{2}{3}$$

この組み合わせ 2×2 に差分プライバシー適用なしを加えて，被験者集合を表 2 の 5 つのグループに分ける．

4. 調査結果

4.1 被験者

表 3 に被験者のデモグラフィック情報を示す．図 1 に，被験者集合の年齢の分布を表す．表 4 に，被験者の業種分布を示す．平均年齢 42 歳，男女比もほぼ等しく，一般的

表 2　被験者グループ

	低リスク $\varepsilon = \ln 2\,(0.69)$	高リスク $\varepsilon = \ln 4\,(1.38)$	差分プライバシー無 $\varepsilon = \infty$
加工方法説明	維持確率 $p = \frac{2}{3}$ A	維持確率 $p = \frac{4}{5}$ C	（説明なし） E
リスク説明	真のリスク漏えい $\Pr[x = 1 \mid y = 1] = 0.148$ B	真のリスク漏えい $\Pr[x = 1 \mid y = 1] = 0.258$ D	

表 3　被験者属性

項目	値	
年齢	平均 42.9	最小 20 歳，最大 77 歳
性別	男性 147 名	女性 112 名
治験経験	あり 13 名	なし 244 名

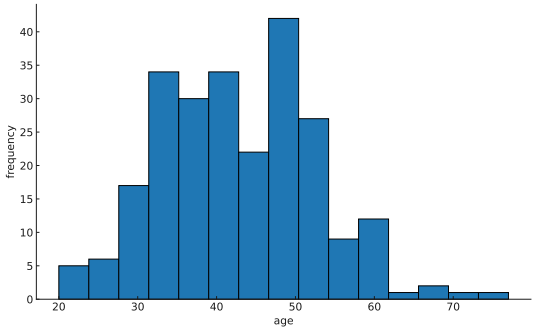

図 1　被験者の年齢分布

表 4　業種の頻度分布

業種	人数
その他	89
専業主婦	31
製造業	30
会社員（情報・通信業）	30
教育	20
医療福祉	14
飲食業	14
会社員（金融保険業）	11
建築業	9
会社員（電気・ガス，インフラ）	7
宿泊業	3
農業・林業	1

なユーザを代表したサンプリングになっている．

図 2 に，血圧や血糖値などの個人情報に対して気にしている頻度を表す．身長などの外見的から観測される個人情報と異なり，血圧などの検査データは直ぐに回答できる人は少なく，血圧，中性脂肪，コレステロールの順に認識している人が多い．

これらの個人情報セキュリティや二次利用に対しての許容度を図 3 に示す．アプリに登録して個人で管理するのは

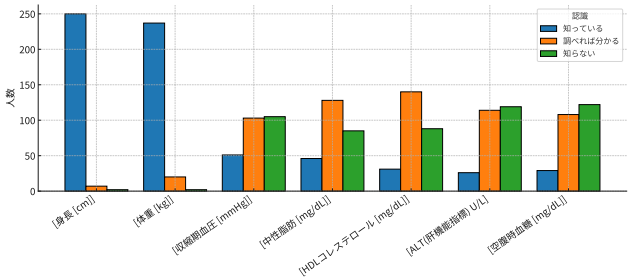

図 2　個人情報の認識分布

良いが，サーバに管理したり，二次利用されたりすることに対しては消極的である．

4.2　アプリのインストール同意

表 5 に，各グループにおけるアプリのインストール同意数を示す．その積み上げグラフを図 4 にて可視化する．

直ぐに削除する人も含めてインストールに同意する人は，グループ B（低リスク，リスクによる説明）が最も多い．従って，加工方法よりもリスクの大きさで説明したほうが，正しく理解を行い同意をした人が増えた可能性がある．しかし，どのグループも 80%で推移しており，それらの差は大きくない．

そこで，自由度 2 によるカイ二乗検定で有意差を検定した．表 6 にリスクの大きさによる検定，表 7 に DP の説明方法による検定結果を示す．いずれも，p 値は有意水準に達せず，統計的には有意ではないことが示された．

同意の原因を明らかにするために，いくつかの質問を行っている．表 8 には，インストールに同意しない理由の分布（複数回答あり），表 9 に，同意する理由の分布をそれぞれ示す．不同意の西田の理由は，情報漏洩に対する恐れや他人に知られることに対する嫌悪である．同意を決定する要素として提供先も大きな要因である．表 10 には，提供先ごとの同意の頻度を示す．学術機関，官庁，民間の順に同意が増えている．表 11 には，DP と匿名加工のクロス集計を示した．2 つの PETs 技術の間に差はなく，DP による二次利用に同意する人は匿名加工についても同意している．

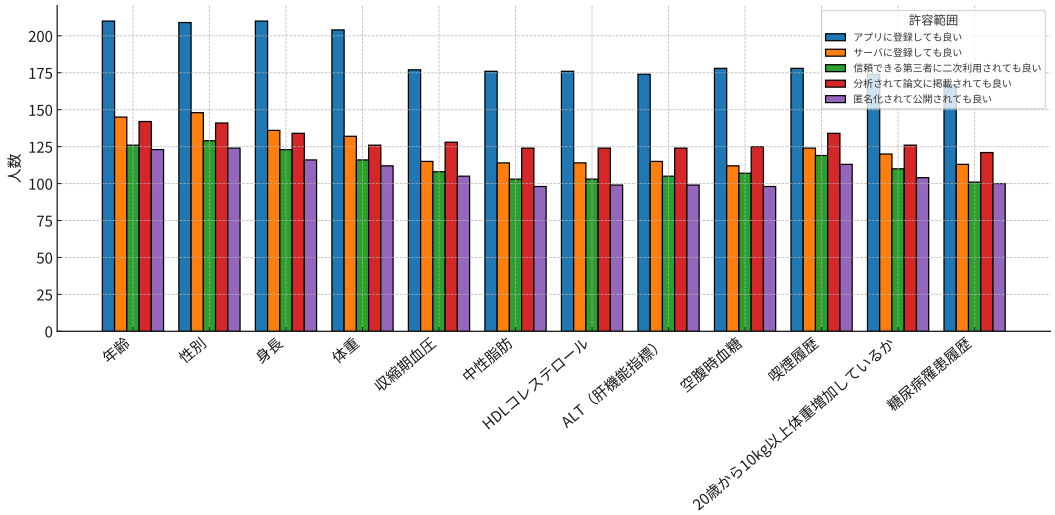

図 3　個人情報の提供許容度分布

表 5　type 別のアプリインストール同意状況

type	同意しない	[%]	同意するが直ぐ削除	[%]	同意する	[%]
A	9	(15.3)	7	(11.9)	43	(72.9)
B	4	(7.4)	10	(18.5)	40	(74.1)
C	7	(14.3)	7	(14.3)	35	(71.4)
D	8	(18.6)	3	(7.0)	32	(74.4)
E	8	(14.8)	8	(14.8)	38	(70.4)

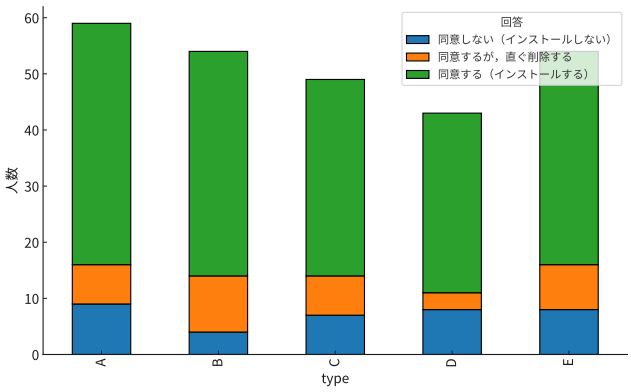

図 4　アプリのインストール同意数分布

表 6　リスクと同意についてのカイ二乗検定 (DF = 1)

group	同意する	[%]	同意しない	[%]
$A+B$ (低リスク)	100	(38.6)	13	(5.0)
$C+D$ (高リスク)	77	(29.7)	15	(5.8)
χ^2	0.63			
p-value	0.429			

4.3　客観的理解度

被験者が同意書を正しく読み，記載されている内容を理解しているかどうか表 12 による理解度テストを行った．

表 7　差分プライバシーの説明方法と同意についてのカイ二乗検定 (DF = 1)

group	同意する	[%]	同意しない	[%]
$A+C$ (摂動化説明)	92	(85.2)	16	(14.8)
$B+D$ (リスク説明)	85	(87.6)	12	(12.4)
χ^2	0.093			
p-value	0.760			

表 8　インストールに同意しない理由

理由	人数
アプリから情報漏洩することが怖いから	33
プライバシー情報を人に知られたくないから．	24
登録した情報が無断で利用されることが嫌だから	13
情報を提供しても自分に見返りが無い	11
情報を提供しても謝礼がない	9
同意した	7
該当なし	2

表 9　インストールに同意する理由

理由	人数
自分にあった生活習慣に活かせるから	171
新しい治療法の開発や今後の予測につながる可能性があるから	118
万が一情報が持ち出されても，匿名化処理されているために安心だから	79
嫌になっても，いつでも削除要求できるから	70
同じ症状の患者間でつながることができるから	14

概ね正答率は 75%程度で推移しているおり，Q3 （インストール直後に削除できる）と Q6 (匿名化されたデータから個人が特定されない) の理解度が最も高く，Q7 （匿名加工の停止要求可能 *2）が最も低かった．

*2　匿名加工情報は特定の個人が識別できない状態になっているの

表 10　提供先による同意の頻度

提供先	同意数 （複数回答)
大学病院 （学術機関)	183
厚生労働省（官庁）	157
製薬会社 (民間)	108
無条件に同意	63

表 11　差分プライバシーと匿名加工のクロス集計

		匿名加工情報の提供に同意しない	匿名加工情報の提供に同意する
差分プライバシー	同意する	4	0
	同意する	0	259

アプリのインストールに同意しない人は，個人情報保護の制度に対する知識が不足し，同意書の内容を誤読していることが考えられる．そこで，表 13 に，同意の有無と正解数との分割表を求めた．平均値で 0.472, 中央値で 0.5 の差が生じており，最大値の 10%に相当する．差は生じているが，平均値の検定を行うと，t 値 1.33, 自由度 48.7, p 値 0.190 となり，0.05 より大きいため統計的な有意性ではない．

ユーザの同意を左右する他の因子の影響を検討する．

表 14 は，目的の異なる各種ヘルスケアアプリに対する利用者の受容頻度を示す．学術目的のものが営利目的のものよりも高く受容されている．表 15 に，取得されることに受容性の高い個人データの一覧を示す．歩数，心拍数に対しては他の情報よりも数倍高い．既にサービスされているスマートフォンなどの例があることが影響していると考えられる．

表 16 は，スクリーンタイム（スマートフォンの累積利用時間）の統計量に対してどのような加工が望まれているかを示している．利用時間を合計する，上位 5 件のみにする，の 2 つの処理が顕著に選択されている．一方，ランダムなノイズなどの処理に対しては受容が多いとは言えない．

4.4　リスク志向度

ユーザがリスクを正しく知覚しているかどうかを測定するための質問を行った．表 17, 表 18, 表 19 に，それぞれ, 2 択の事象を与えて高リスクであるのはどちらか回答してもらった結果を示す．高リスクな事象には*をつけており，いずれも，最頻度で選択されている．ただし，表 18 に関しては正解はなく，メールアドレス（匿名性）とアプリ利用時間（属性のプライバシー）の優先度については意見が別れている．前者を保証するものが匿名化技術，後者を保証するものが DP に対応している．

で，オプトアウトが出来ない．作成していることを通知公表していれば，本人の同意を取る必要もない．

5.　おわりに

本研究では，糖尿病リスク予見アプリの利用を例題として，インストールの同意とその背後にある情報理解度との関連を分析した．アンケート調査を通じて，アプリのインストールに同意する参加者は，同意書に記載された情報に対する理解度が相対的に高いことが示された．一方，同意しない参加者は理解度が低い傾向を示し，プライバシーリスクに対する懸念や誤解が，インストール意思に影響を与えている可能性が明らかとなった．

差分プライバシーのプライバシー保護の強さ（リスク）と方式やリスクの大きさ（説明方法）を変えた A–E のグループ比較や同意群間の統計的検定を通じて，グループ間で顕著な有意差は確認されなかったものの，リスクを説明するほうが効果的である傾向が見られた．アプリを利用に対する同意については，利用者の持つ情報リテラシーやプライバシー志向度合い，個人情報保護制度に関する理解度，および，二次利用される用途や提供先など，多くの条件に依存することが明らかになった．

本研究の意義は，プライバシーに配慮したアプリ導入の成否が，利用者の理解度や説明の分かりやすさに大きく左右されることを明らかにした点にある．特に，差分プライバシーや匿名加工情報といった専門的な仕組みを適切に説明し，誤解を解消することが，ユーザーの同意形成に不可欠である．

本研究には限界がある．調査は限定的な対象集団に基づくものであり，広範なユーザ層を代表するものではない．また，回答は自己申告に基づくため，実際の行動とは乖離する可能性がある．

今後は，多様な対象集団を含む大規模調査や，実際の利用行動データを組み合わせることで，同意形成のメカニズムをより実証的に検討することが望まれる．さらに，説明文言やインターフェース設計の改善を通じて，利用者が安心してアプリを利用できる環境を整備することが課題である．

謝辞　本研究は，JST, CREST Grant Number JPMJCR21M1 と JSPS 科研費 23K11110 の助成を受けている．

参考文献

[1] ライフログテクノロジー, “カロミル　プライバシーポリシー”, (2025 年 8 月参照，https://www.calomeal.com/ppolicy.html).

[2] A. Xiong, T. Wang, N. Li and S. Jha, “Towards Effective Differential Privacy Communication for Users’ Data Sharing Decision and Comprehension,” 2020 IEEE Symposium on Security and Privacy (SP), pp. 392-410, 2020.

[3] Priyanka Nanayakkara, Mary Anne Smart, Rachel Cummings, Gabriel Kaptchuk, and Elissa M. Redmiles,

表 12　設問ごとの正解と誤答数

設問	正解	正答	誤答
Q1. 登録したヘルスケア情報をアプリの管理者は知ることができる。	正しい	141	46
Q2. アプリに登録したヘルスケア情報を委任先に削除依頼できる。	誤り	151	45
Q3. アプリをインストールした個体に登録したヘルスケア情報を削除依頼できる。	正しい	201	22
Q4. 登録したヘルスケア情報は共同研究先の大学病院でも参照される。	誤り	162	33
Q5. 第三者に提供された機微なデータから真の値が漏洩することがある。	誤り	166	36
Q6. 第三者に提供されたデータから自分のデータが特定されることがある。	誤り	201	23
Q7. 自分のデータが匿名加工情報として加工されることを停止要求できる。	誤り	77	102

表 13　同意有無によるスコア統計量

区分	n	平均	標準偏差	中央値
同意する	223	4.372	1.730	5.0
同意しない	40	3.900	2.122	4.5

表 14　ヘルスケアアプリに対する受容度 (複数回答可)

回答	人数
活動量と疾病の関係を明らかにする学術目的のアプリ	142
自分の将来の健康寿命を予測するアプリ	135
製薬会社が健康な生活習慣を助言するアプリ	121

表 15　取得されてもよい個人情報

回答	人数
平均歩数	230
心拍数	200
脳波	89
スクリーンタイム	48
位置情報	24
ウェブサイトの閲覧履歴	16
毎月の預金残高	2

表 16　スクリーンタイムの提供条件

回答	人数
決して許可しない	93
全アプリの一日の合計利用時間にする	91
上位 5 件以下を削除する	35
利用時間に 1 時間までの正負のランダムなノイズを足す	30
何もしない（無条件に取得を許す）	25
確率 1/2 でランダムな時間に置き換える	20
閲覧アプリの組み合わせが同じ人が 20 名以下の時は削除する	15

表 17　高リスクなのはどちらか (1)

回答	人数
2/3 の確率で正しい履歴を答え，1/3 の確率でランダムな履歴を答える*	120
分からない（同じ）	90
1/3 の確率で正しい履歴を答え，2/3 の確率でランダムな履歴を答える	47

表 18　高リスクなのはどちらか (2)

回答	人数
メールアドレスが知られているが，どのアプリを何時間使ったかは不正確に知られている	127
メールアドレスは秘匿されているが，どのアプリを何時間使ったかは正確に知られている	78
分からない（同じ）	54
無回答 (NaN)	4

表 19　高リスクなのはどちらか (3)

回答	人数
どのアプリを何時間使ったかの履歴はクラウド（サーバ）にのみ格納されている*	144
分からない（同じ）	59
どのアプリを何時間使ったかの履歴はスマートフォン（アプリ）にのみ格納されている	56

“What are the chances? explaining the epsilon parameter in differential privacy”, In Proceedings of the 32nd USENIX Conference on Security Symposium (SEC 23), USENIX Association, USA, Article 91, pp. 16131630, 2023.

[4] 中川 裕志, 菊池 浩明, “個人データの利用に対する許容度に関する社会調査”, コンピュータセキュリティシンポジウム 2022 論文集, 情報処理学会, pp. 1222-1229, 2022.

[5] P. Kairouz, K. Bonawitz, and D. Ramage, “Discrete distribution estimation under local privacy,” in Proc. 33rd Int. Conf. Mach. Learn., vol. 48, Jun. 2016, pp. 24362444.

[6] J. C. Duchi, M. I. Jordan, and M. J. Wainwright, “Minimax optimal procedures for locally private estimation,” Journal of the American Statistical Association, vol. 113, no. 521, pp. 182201, 2018.

付　　録

A.1　アンケート文

あなたは健康診断で，5 年以内に糖尿病に罹患するリスクが 60%と診断されました．空腹時における血糖値は，健康な成人の場合 90mg/dL ですが，あなたの値は 180mg/dL でした．そこで，あなたの検査項目や属性情報を元に，貴方の糖尿病罹患リスクを予測し，生活習慣の改善に役立てるアプリの利用を推められました．

アプリの同意書を読み，以下の質問にお応えください．

A.2　同意書 (*A* の例)

本アプリは，ユーザーのヘルスケアデータをもとに糖尿病の罹患リスクを予見し，生活習慣の改善に役立てることを目的としています．本アプリは診断を行うものではなく，高リスク判定が出た場合は必ず医師の診察を受けてください．

取得する情報は以下の通りです．

- 属性情報：年齢，性別，身長，体重
- 履歴情報：喫煙，糖尿病罹患，20 代からの体重変化
- バイタル・検査項目：血圧，中性脂肪，コレステロール，ALT（肝機能），空腹時血糖値
- 端末情報：識別子，IP アドレス

利用目的は，糖尿病罹患リスクの算出と表示，健康状態に応じたアドバイスの提供，アプリ改善・品質向上のための分析，および法令に基づく匿名加工情報の作成と二次利用です．

第三者提供は法令に基づく場合や安全性情報収集のためを除き行いません．ただし，厚生労働省の担当部署，大学病院，民間製薬会社と共同利用する場合があります．各共同利用先の管理責任者・窓口・利用範囲は当社 Web サイトにて公表します．

また，機微情報を第三者に提供する際には差分プライバシーを適用し，値を特定できないように確率的に加工します．例えば，リスクありと判定された場合でも 2/3 の確率で「リスクあり」，1/3 の確率で「リスクなし」と回答し，逆の場合も同様です．さらに，個人識別情報は匿名加工情報に変換し，再識別できない形にします．

安全管理措置として，通信や保存の暗号化，アクセス制御，多要素認証，改ざん検知などの技術的対策，権限管理や委託先監督・監査などの組織的対策を実施します．取得データは最終利用日から 3 年間保存します．匿名加工情報および差分プライバシー処理済みデータは削除請求の対象外ですが，適法かつ公正な範囲でのみ利用します．

利用者は登録済みデータの開示・訂正・削除を請求でき，同意はいつでも撤回可能です（撤回前の適法性に影響はありません）．

連絡先は以下の通りです．個人情報窓口：個人情報管理者 情報 守 電話 03-5343-1234．共同利用先の詳細は当社 Web サイト「共同利用先一覧」を参照してください．