

生体情報保護の可視性がユーザ体験と セキュリティ意識に及ぼす影響

菅沼 弥生¹ Vo Ngoc Khoi Nguen¹ 成田 惇¹ 奈良 成泰² 一色 寿幸² 岡村 利彦² 大木 哲史¹

概要：生体認証が普及するにつれ、より安全な生体認証システムを構築する重要性が高まってきている。テンプレート保護型生体認証は、伝送路上や保管される生体情報の安全性を保ちつつ認証を可能とする技術であり、生体認証のセキュリティにおける重要な要素技術である。一方、ユーザビリティの観点からは、利用者のユーザビリティのために、これらのセキュリティメカニズムを可視化すべきか、またはブラックボックス化すべきかという問題が存在する。そこで本研究では、生体認証のテンプレート保護の文脈において、生体情報保護の可視性がユーザ体験に与える影響を分析することを目的とする。生体認証における登録および認証の2つの段階を対象とし、生体情報保護の可視化状態が異なる2つのアプリケーションを設計し、標準化された評価尺度および半構造化インタビューを用いてUXに関する調査を行った。本調査によって、テンプレート保護型生体認証の利用を促進する上でのUX設計の重要性や、生体情報提供への懸念が与える影響などを明らかにした。

キーワード：生体認証, バイオメトリクス, テンプレート保護, ユーザビリティ

Impact of Biometric Protection Visibility on User Experience and Security Awareness

YAYOI SUGANUMA¹ VO NGOC KHOI NGUEYN¹ JUN NARITA¹ MASAHIRO NARA² TOSHIYUKI ISSHIKI²
TOSHIHIKO OKAMURA² TETSUSHI OHKI¹

Abstract: As biometrics becomes more and more popular, it becomes more important to build a more secure biometric authentication system. Template-protected biometrics is one of the elemental technology in biometric security. It enables authentication while maintaining biometric data security in transmission and storage. On the other hand, from the usability point of view, there is a problem of whether these security mechanisms should be visible or black-boxed for users' usability. Therefore, this study aims to analyze the impact of the visibility of biometric protection on user experience in the context of biometric template protection. We designed two applications with different biometric protection visibility for two biometric authentication stages: enrollment and authentication. We investigated their UX using standardized rating scales and semi-structured interviews.

Keywords: Biometrics, Template Protection, Usability

1. はじめに

生体認証が普及するにつれ、より安全な生体認証システ

ムを構築する重要性が高まってきている。従来は本人拒否率や他人受入率といった認証精度を安全性の評価基準とすることが一般的であったが、近年では認証精度だけでなく、ネットワークを介した生体認証システム（リモート生体認証）までを対象とし、入力される生体情報の安全性から、伝送路上や保管される生体情報の安全性といった、より多

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

² 日本電気株式会社, 神奈川県川崎市中原区下沼部 1753 番地, NEC Corporation, 1753 Shimonumabe, Nakahara-ku, Kawasaki, Kanagawa, Japan

くの脅威に対応した安全性が求められている。これらのうち、伝送路上や保管される生体情報の安全性は、文献 [1] 等において提案されたテンプレート保護型生体情報の枠組みで捉えられ、これまでも多くの研究が進められてきた。

一方、生体認証はセキュリティと可用性の両立を目指した技術の 1 つであり、認証精度の向上やテンプレートの保護だけでなく、そのユーザビリティや社会的受容性に関する研究もまた多く行われてきた [2][3]。2008 年には NIST が生体認証とユーザビリティに関するハンドブック、Usability & Biometrics^{*1} を出版しており、生体認証システムにユーザ中心の設計プロセスを採用する際に必要となる主要なコンセプトを、ユーザおよび組織要件の決定、デザインソリューションの開発、および評価の実施といった項目に整理している。特に近年では、モバイル端末をはじめとする個人所有の端末での生体認証が急速に普及したことによって、個人所有の端末ロック解除や、モバイルペイメントにおける本人確認など、利用するユーザ層や利用環境が急速に多様化しつつある。このような状況において、主にモバイル端末を対象としたユーザビリティに関する研究が多く行われている。文献 [4] では顔・音声・ジェスチャーといった生体認証のモダリティを例に挙げ、モダリティごとに異なる認知的・身体的負荷がユーザビリティへ与える影響を明らかにしている。文献 [5] では部屋の明るさや把持方法、移動状態といった環境要因が生体認証のユーザビリティに与える影響を明らかにしている。文献 [6], [7] では、既存システムの認証手段を生体認証へ置き換えた際のユーザビリティの変化を調査している。

上記のような生体認証のモダリティや環境要因、あるいは既存認証手法との比較などのユーザビリティ研究が多く進められている一方で、テンプレート保護に代表される生体認証のプライバシー保護機能がユーザビリティに与える影響については、これまでほとんど議論がされてこなかった。そこで本研究では、以下の 2 つのリサーチクエスチョンを定義し、これらに関する調査を実施する。

[RQ1] 生体情報が保護されていることを利用者に可視化することによる影響とは何か？

[RQ2] 生体情報提供に関する懸念はユーザ体験にどのような影響を与えるか？

これらの調査結果から、生体認証に生体情報の保護プロセスを組み込む際に考慮すべきユーザビリティ上の課題が明らかとなり、利用者にとって安全性の高い生体認証アルゴリズムが、より高い受容性をもって利用可能となることが期待できる。

本リサーチクエスチョンに対する調査として、著者らは Distler らの電子投票における暗号化プロセスのユーザビリティ調査 [8] を参考に、生体認証における登録および認証

の 2 つの段階を対象とし、生体情報保護の可視化状態が異なる 2 つのアプリケーションを設計し、標準化された評価尺度および半構造化インタビューを用いて UX に関する調査を行った。

本稿における貢献は以下の通りである。

- (1) 2 種類のアプリケーションを用いたタスク調査およびアンケートを実施し、生体情報保護の可視性がユーザ体験とセキュリティ意識に与える影響を調査した
- (2) UX 評価尺度に関する回答を、生体情報保護の可視性と関連付けて分析し、生体情報保護の状態をユーザに提示することが、セキュリティ意識およびアプリケーションのユーザ体験に強い影響を与えていることを明らかにした。
- (3) 生体情報が保護の可視化によりアプリケーションから得られる一部のユーザ体験が向上する傾向を確認した。
- (4) 生体情報提供に関する懸念が高いユーザは可視化によりユーザ体験が向上しやすい傾向を確認した。

2. 関連研究

生体情報の保護とユーザ体験に関連する研究としては、文献 [8] や文献 [9] があげられる。Venkatraman らは、オンラインバンキングへの生体認証導入にあたる課題抽出を目的としたケーススタディを行い、導入に向けた重要な課題の 1 つが利用者のプライバシーに関する懸念であることを指摘した [9]。Distler らは、電子投票アプリケーションを対象に、暗号化アルゴリズムによる投票プロセスや検証プロセスの可視化がアプリケーションの UX 向上に寄与するかを調査した [8]。文献 [8] の調査では、セキュリティ関連情報を利用者に提示するバージョン、および提示を行わないバージョンの 2 つのバージョンのアプリケーションを作成し、38 名の参加者によりそれぞれのバージョン間における UX の違いを検証した。これにより、セキュリティ関連情報を提示することが全体的な UX 向上に寄与することを示した。

本稿では、主に Distler らの調査手法を参考に、生体認証のテンプレート保護プロセスの可視化が UX に与える影響を調査することを目的とする。生体認証のユーザビリティ研究分野ではこれまで行われていなかったテンプレート保護を対象とし、生体情報漏えいに対する意識がユーザ体験に与える影響を含めた分析を行う点で、既存研究と異なる目的を持つ。

3. 調査方法

本章では、前章で述べた仮説を検証するためのタスク調査について述べる。本調査は 2021 年 1 月 7 日から 2021 年 1 月 15 日にかけて実施された。参加者は大学内で募集し、全ての参加者から実験参加への同意を得た。

^{*1} https://www.nist.gov/system/files/usability_and_biometrics_final2.pdf

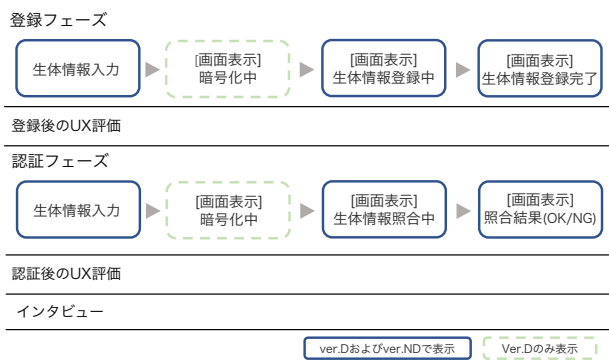


図 1 実験の構成図

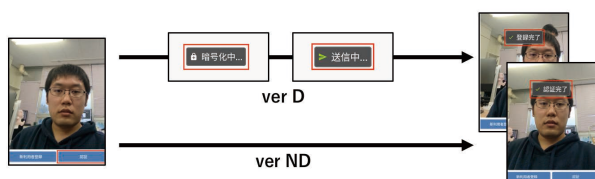


図 2 作成した顔認証アプリケーションの概要

3.1 参加者

本調査では 18 人の参加者を募集し、18 人が参加した。18 人中 14 人が男性、4 人が女性であった。

3.2 手順

本調査は 5 つの手順により構成される。実験の構造を以下、および図 1 に示す。

[手順 1]登録:参加者はアプリケーションを介して自身の顔画像を撮影し、システムへ登録する

[手順 2]登録後の UX 評価:[手順 1] の UX を質問紙を用いて評価する

[手順 3]認証:参加者は、再度自身の顔画像を撮影し、登録した顔画像間との認証を行う。

[手順 4]認証後の UX 評価:[手順 3] の UX を [手順 2] と同様の質問紙を用いて評価する。

[手順 5]インタビュー:テンプレート保護型生体認証の利用がユーザに与える影響を評価する。くわえて、参加者の生体情報を提供することに対する懸念を測定する。

実験指示者は参加者に、実験の概要説明および質問紙回答用のパソコンおよびアプリケーション操作用の端末を渡した。参加者は、実験の概要およびアプリケーションの操作方法についての説明を受けた。その後、アプリケーション操作端末を操作し、アプリケーションの動作を確認した。アンケートの回答にあたっては、LimeSurvey^{*2}によって作成されたアンケートに匿名で回答した。参加者は、2 種類のアプリケーションで、それぞれ [手順 1] から [手順 4] を 1 回ずつ実施し、最後に [手順 5] のインタビューおよび生体情報を提供することに関する質問項目に回答しても

^{*2} <https://www.limesurvey.org>

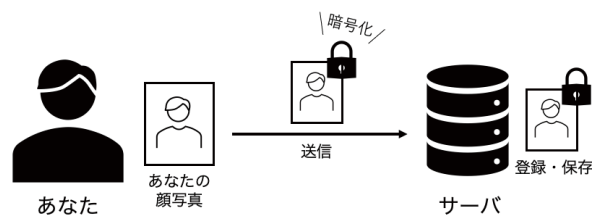


図 3 テンプレート保護型生体認証の説明 (登録過程)

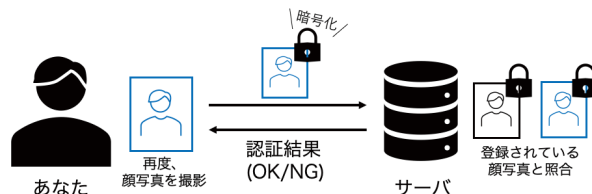


図 4 テンプレート保護型生体認証の説明 (認証過程)

らった。1 人あたりの調査時間はおおよそ 30 分であった。

3.2.1 アプリケーション

本調査では、生体認証において生体情報が保護されていることを利用者に可視化することによる影響を分析するため、調査用にテンプレート保護型生体認証機能によるリモート生体認証機能を模した 2 種類の Android アプリケーションを開発した。開発したアプリケーションの概要を図 2 に示す。

2 つのアプリケーションは、共通して Facenet[10] を用いた顔認証機能を搭載している。顔認証機能は、顔画像の登録および顔画像の認証の 2 つの機能から構成されており、調査の各フェーズに応じて登録と認証を指定し、アプリケーションを操作することができる。2 つのアプリケーションの相違点を以下に示す。

ver.D 顔画像を登録および認証後、「暗号化中」という単語が表示され、2 秒程度の待ち時間が発生する。(図 1 の登録フェーズおよび認証フェーズにおいて、生体情報を入力後にすべての動作がユーザに表示される)

ver.ND 顔画像を登録および認証後、「暗号化中」という単語が表示されず、待ち時間は発生しない。(図 1 の登録フェーズおよび認証フェーズにおいて、生体情報を入力後に青枠の動作のみがユーザに表示される)

参加者には、テンプレート保護型生体認証の説明として、図 3 および図 4 を用いた説明を受けた後、今回利用するアプリケーションにこの技術が用いられ、コンビニエンスストア等の店舗での決済や入退室管理等に今回のアプリケーションが利用される場面を想定するように指示した。なお、参加者には ver.D もしくは ver.ND のいずれのバージョンを利用する場合においても、今回使用するアプリケーションにはテンプレート保護型生体認証が利用され、送信・保管する生体情報が安全に保護されることを説明した。

表 1 UX 評価尺度を構成する下位尺度の概要

下位尺度	用語	概要
UEQ/Hedonic	快楽性	ユーザ体験における快楽的な品質
UEQ/Pragmatic	実用性	ユーザ体験における実用的な品質
UEQ/Attractiveness	視覚性	ユーザ体験における視覚的な品質
Needs/Competence	能力	自らが置かれている環境において能力を発揮できている感覚
Needs/Autonomy	自律性	自らの意思で判断を下している感覚
Needs/Security	セキュリティ	自らに及ぶ脅威や不安をコントロールできている感覚

3.3 評価尺度

[手順 2] および [手順 4] の UX 評価を、2 つの既存の評価尺度を用いて評価した。1 つ目は、Laugwitz らによって提案された魅力 (Attractiveness)、実用性 (Pragmatic)、快楽性 (Hedonic) の 3 つの観点から構成されるユーザ体験の質を測定する尺度 (UEQ) [11] である。本調査では、Laugwitz らによって翻訳された日本語版の評価尺度をそのまま使用した*3。質問項目は 26 個の対照的な単語のペアにより、参加者は 7 段階 (-3 から +3 の範囲) でより自身のユーザ体験を表す単語に近い選択肢を回答した。2 つ目は、Lallemant らによって提案された能力、自律性、セキュリティ、喜び、関連性、影響力、自己実現の必要性を測定する尺度 (UXneeds) [12] である。本調査では、下位尺度のうち、文献 [8] で分析の対象となっていた、能力、自律性、セキュリティの 3 つの下位尺度を修正および日本語化し、使用した。参加者は、(全くそう思わない (1) ~ とてもそう思う (5)) で回答した。以上で挙げた、本調査で使用した UX 評価尺度を構成する下位尺度の概要を表 1 に示す。[手順 5] の生体情報を提供することに対する懸念は、Malhotra らによるプライバシー情報提供へのリスク理解、不安を測定する尺度 (IUIPC) [13] の一部を本調査用に修正および日本語化し、使用した。参加者は、自身が提供する生体情報がサービス提供者のもとから漏洩する可能性に関して (漏洩する可能性は半々 (1) ~ どちらかと言えば漏洩する (7)), (低い (1) ~ 高い (7)), (かなり低い (1) ~ かなり高い (7)), (ほぼありえない (1) ~ ほぼ確実 (7)) の 4 つの尺度に答えた。

3.3.1 インタビュー

テンプレート保護型生体認証が利用されることにより、ユーザ体験がどのように変化するかを評価するため、インタビューを実施した。インタビューでは、アプリケーション内で印象に残った機能の特徴や利用する中で直面した困難性といったアプリケーション全体の印象に関する質問項目、通常の生体認証とテンプレート保護型生体認証への認識と利用体験に関する質問項目、アプリケーションへのセキュリティやプライバシーへの懸念に関する質問項目および「暗号化中」という単語を表示することがユーザのセキュリティ、プライバシー懸念に与える影響に関する質問

表 2 UX 評価の要約

	ver.D		ver.ND		d		p
	M	SD	M	SD			
UEQ/Overall	1.29	0.78	1.05	0.70	0.31	< 0.01	
UEQ/Hedonic	0.14	1.09	-0.16	0.97	0.29	0.02	
UEQ/Pragmatic	2.01	0.70	1.88	0.60	0.20	0.13	
UEQ/Attr.	1.37	1.03	1.03	1.04	0.33	< 0.01	
Needs/Competence	3.72	0.59	3.82	0.62	0.17	0.17	
Needs/Autonomy	3.60	0.83	3.46	0.77	0.17	0.11	
Needs/Security	4.12	0.53	3.96	0.68	0.27	0.03	

項目について、ユーザに回答してもらった。

4. 結果および分析

[RQ1] および [RQ2] を検証するため、D/ND 各バージョンの UX 評価尺度の値に違いがあるかを検証する。分析には、実験に参加した 18 名 (男性 14 名、女性 4 名) の回答結果を使用した。

4.1 生体情報が保護されていることを利用者に可視化することによる影響

生体情報が保護されていることを利用者に可視化することによる影響を検証するため、登録・認証全てのプロセスに共通した ver.D および ver.ND 間の UX 評価尺度値を分析する。まず、表 2 に登録時および認証時に評価された UEQ および UXneeds 全てから算出した平均値および標準偏差を示す。効果量は Cohen の d に従った。

表 2 より、UEQ の観点から、登録時の ver.D および ver.ND に差があるかについて分析する。まず、UEQ/Overall は UEQ/Hedonic, Pragmatic, Attractiveness の平均から求められる総合的ユーザ体験 (UEQ/Overall) について分析した。UEQ/Overall は ver.D が ver.ND よりも高い値を示し、有意差が認められた ($t(35) = 3.150$, $p = 0.003$)。このことから、生体情報が保護されていることが参加者に可視化されている場合には、総合的なユーザ体験が高く評価されることがわかった。

次に、UEQ/Overall を構成する 3 つの下位尺度について分析した。ユーザ体験における快楽性 (UEQ/Hedonic) は ver.D が ver.ND よりも高い値を示しており、有意差が認められた ($t(35) = 2.558$, $p = 0.015$)。ユーザ体験における実用性 (UEQ/Pragmatic) は、ver.D の方が ver.ND よりもわずかに高い値を示しているが、有意差は現れなかった ($t(35) = 1.560$, $p = 0.128$)。ユーザ体験における視覚性 (UEQ/Attractiveness) は、ver.D の方が ver.ND よりも高い値を示しており、有意差が認められた ($t(35) = 3.420$, $p = 0.002$)。

以上から、生体情報が保護されていることが参加者に可視化されている場合には、参加者がユーザ体験における快楽性および視覚性を特に高く評価し、またユーザ体験の総合的品質においても高い評価をすることがわかった。

*3 <https://www.ueq-online.org>

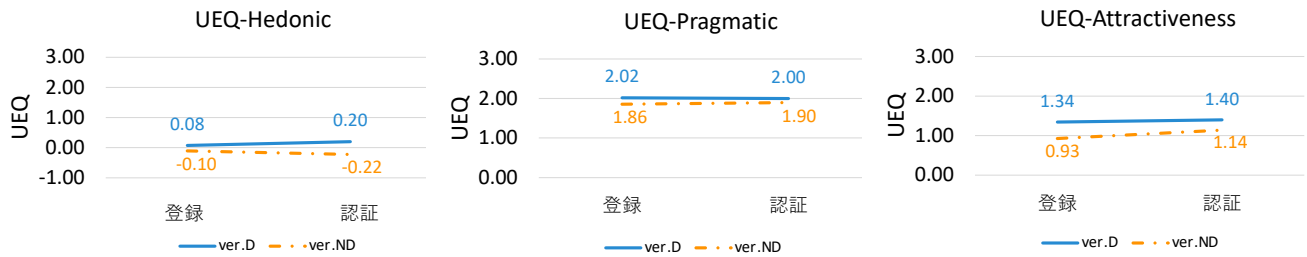


図 5 UEQ の評価結果

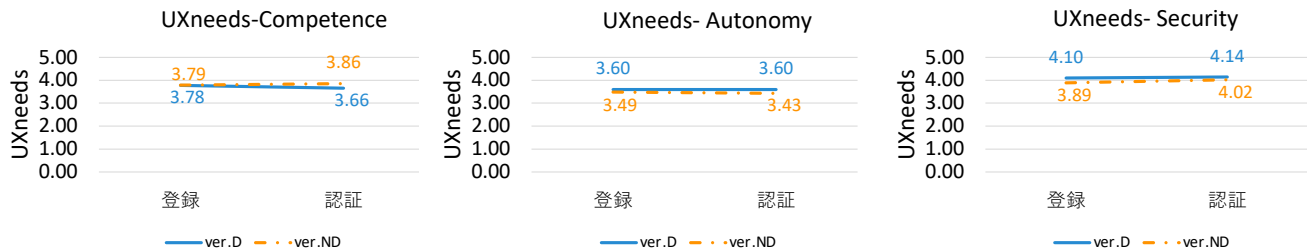


図 6 UXneeds の評価結果

次に、UXneeds の観点から、登録時の ver.D および ver.ND に差があるかについて分析する。表 2 より、能力 (Needs/Competence) は ver.D の方が ver.ND よりもわずかに低い値を示しているが、有意差は現れなかった ($t(35) = -1.416, p = 0.166$)。自律性 (Needs/Autonomy) は、ver.D の方が ver.ND よりもわずかに高い値を示しているが、有意差は現れなかった ($t(35) = 1.638, p = 0.110$)。セキュリティ (Needs/Security) は、ver.D の方が ver.ND よりもわずかに高い値を示しており、有意差が認められた ($t(35) = 2.211, p = 0.034$)。このことから生体情報保護に関する表示がある場合に、より強く自らに及ぶ脅威や不安をコントロールできる感覚を得ていることがわかった。

最後に、登録時と認証時の UX 評価値の違いを調査するために、UEQ および UXneeds の下位尺度ごとの平均値を登録、認証ごとに算出し、図 5 および図 6 に示した。これらの図から、UXneeds-Competence を除く全ての評価値に関して ver.D が登録-認証いずれの場合にも大きな値をとることがわかる。

4.2 生体情報提供に関する懸念が UX 評価に与える影響

生体情報提供に関する懸念と UX 評価との関係进行分析するため、生体情報提供に関する懸念に対する回答を用いて、ユーザを高懸念群 (PH) と低懸念群 (PL) の 2 群に分割した。分割基準には全回答の中央値を用いた。各群の UEQ/Overall および UXneeds の平均値を図 7 に示す。図 7 より、UEQ, UXneeds とともに ver.D のほうが ver.ND よりも高い値を示すことがわかる。

ここで、懸念ごとに評価値の差分値に着目すると、UEQ に関しては、PL における ver.D, ver.ND 間の差分値 ($1.28 - 1.15 = 0.13$) よりも PH の差分値 ($1.25 - 0.97 = 0.28$) が大きくなっている。この差分値は可視化による UX の向上と考えられることを踏まえれば、生体情報提供への懸念の大きい参加者はより可視化されたインターフェースをより強く好む傾向にあること、また懸念の小さい参加者に対しては可視化による効果が薄いことが言える。一方、UXneeds に関しては、ver.D と ver.ND 間での評価値の差はほとんど見られなかった。

5. 議論

4.1 節で述べたように、表 2 においては、ver.ND より ver.D の UX 評価値が高い。この結果から、ユーザは生体情報が保護されたことを可視化された際に、アプリケーションからより良いユーザ体験を得ていることがわかる。これらを踏まえれば、テンプレート保護型生体認証の受容性を高めるためには、処理性能や保護性能の向上だけでなく、保護プロセスを明示的に利用者に示すことが有効な手段の 1 つであると言える。参加者へ実施したインタビューにおいては、「目に見える形で暗号化と出てくると、既存の顔認証より安心できる」、「暗号化中の表示がでて、はっとした、出た方が安心感がある。表示される強く、よりセキュリティを意識した。」といった指摘があった。また生体情報保護の処理過程を明示的に示すことを目的に設定された 2 秒程度の待ち時間に関して、指摘を行ったユーザは少数であった。指摘を行ったユーザの中には、「(暗号化中



図 7 生体情報の提供に関する懸念の大きさによる UEQ および UXneeds の評価結果

と表示されると) 待ち時間に起きている処理がわかるためよりアプリを信頼できる」点が指摘されており、これらの結果も可視化の有効性を示している。

また、4.2 節で述べたように、生体情報提供に関する懸念と UX 評価値との関係を分析した結果、生体情報提供への懸念が大きい参加者は、懸念が小さいユーザと比較して、可視化を好みやすい傾向にあることがわかった。しかし、この事実は UEQ に関してのみ観測されており、UXneeds に関しては関連性が見出されていない。また、低懸念群のユーザはいずれのバージョンに対しても可視化による効果が薄く、このようなユーザにも効果的に働きかけるインターフェースの開発が求められる。

5.1 制限事項

本調査で使用したアプリケーションは、調査用に作成しており、調査は実験室で行なったため、参加者に安心感を与え、UX 評価に影響を与えた可能性がある。また、今回の調査に参加した学生は情報学を専攻する学生であり、情報セキュリティやプライバシーに対する懸念が一般ユーザより強い傾向があった可能性がある。これらの要因により、セキュリティをはじめとする UX 評価に影響を与えた可能性がある。

5.2 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。

6. まとめ

本研究は、テンプレート保護型生体認証において、生体情報が保護されたことを可視化した場合、ユーザ体験にどのような影響を与えるのかを調査および分析した。調査結果

から、生体情報が保護されたことを可視化したアプリケーションの方がユーザ体験に関する評価は高く、特に、生体情報提供に関する懸念を抱いているユーザには効果があることを示唆する結果が得られた。この結果に基づく技術、たとえば、利用者の生体情報提供への懸念の高さを適切に把握するとともに、懸念の高さに応じて保護状態の表示を適切にコントロール可能な技術などを開発することで、生体認証時のユーザビリティを向上させ、かつ利用者にとって安全性の高い生体認証アルゴリズムが、より高い受容性をもって利用可能となる可能性がある。本調査は制限事項でも述べた通り、参加者属性の偏りなど多くの課題が残るものであった。今後はより大規模な調査を通して、本分析で得られた知見の確認を進める予定である。

参考文献

- [1] Ratha, N. K., Connell, J. H. and Bolle, R. M.: Enhancing security and privacy in biometrics-based authentication systems, *IBM Syst. J.*, Vol. 40, No. 3, pp. 614–634 (2001).
- [2] Toledano, D. T., Fernández Pozo, R., Hernández Trapote, Á. and Hernández Gómez, L.: Usability evaluation of multi-modal biometric verification systems, *Interacting with Computers*, Vol. 18, No. 5, pp. 1101–1122 (2006).
- [3] Furnell, S. and Evangelatos, K.: Public awareness and perceptions of biometrics, *Computer Fraud & Security*, Vol. 2007, No. 1, pp. 8–13 (2007).
- [4] Trewin, S., Swart, C., Koved, L., Martino, J., Singh, K. and Ben-David, S.: Biometric authentication on a mobile device: a study of user effort, error and task disruption, *Proceedings of the 28th Annual Computer Security Applications Conference*, pp. 159–168 (2012).
- [5] Bhagavatula, R., Ur, B., Iacovino, K., Kywe, S. M., Cranor, L. F. and Savvides, M.: Biometric authentication on iphone and android: Usability, perceptions, and influences on adoption (2015).
- [6] Tassabehji, R. and Kamala, M. A.: Evaluating biometrics for online banking: The case for usability, *Int. J. Inf. Manage.*, Vol. 32, No. 5, pp. 489–494 (2012).
- [7] Mayron, L. M., Hausawi, Y. and Bahr, G. S.: Secure, Usable Biometric Authentication Systems, *Universal Access in Human-Computer Interaction. Design Methods, Tools, and Interaction Techniques for eInclusion*, Springer Berlin Heidelberg, pp. 195–204 (2013).
- [8] Distler, V., Zollinger, M.-L., Lallemand, C., Roenne,

- P. B., Ryan, P. Y. and Koenig, V.: Security-Visible, Yet Unseen?, *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, pp. 1–13 (2019).
- [9] Venkatraman, S. and Delpachitra, I.: Biometrics in banking security: a case study, *Inf. Manage. Comput. Secur.*, Vol. 16, No. 4, pp. 415–430 (2008).
- [10] Schroff, F., Kalenichenko, D. and Philbin, J.: FaceNet: A unified embedding for face recognition and clustering, *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, pp. 815–823 (2015).
- [11] Laugwitz, B., Held, T. and Schrepp, M.: Construction and evaluation of a user experience questionnaire, *Symposium of the Austrian HCI and usability engineering group*, Springer, pp. 63–76 (2008).
- [12] Lallemand, C. and Koenig, V.: Lab testing beyond usability: challenges and recommendations for assessing user experiences, *Journal of Usability Studies*, Vol. 12, No. 3, pp. 133–154 (2017).
- [13] Malhotra, N. K., Kim, S. S. and Agarwal, J.: Internet users’ information privacy concerns (IUIPC): The construct, the scale, and a causal model, *Information systems research*, Vol. 15, No. 4, pp. 336–355 (2004).