VR/AR/MRセキュリティ・プライバシに対するユーザ認識の変遷調査

倉﨑 翔大[1,a)]　金岡 晃[1,b)]

概要：本研究では、VR/AR/MR HMD 利用におけるセキュリティやプライバシに対するユーザの認識の変遷を調査する。VR/AR/MR HMD の利用が増加する中、そこにあるセキュリティやプライバシ問題に対するユーザの認識やその変遷を把握することは、効率的にユーザへ対策行為を促す上で必要なことである。本稿では、VR/AR/MR HMD の利用者 100 名を対象とするクラウドソーシング調査を 2023 年の夏からおおよそ半年ごとに計三回行い、結果を分析した。分析結果より、ユーザの認識やその変遷が明らかになった。

キーワード：Virtual Reality, Augmented Reality, Mixed Reality

Survey of User Perception Transitions in VR/AR/MR Security and Privacy

Shodai Kurasaki[1,a)]　Akira Kanaoka[1,b)]

Abstract: This study surveys the transitions in user perceptions regarding security and privacy issues associated with the use of VR/AR/MR HMDs. As the usage of VR/AR/MR HMDs increases, understanding user perceptions and their transitions regarding security and privacy issues is essential for effectively promoting protective measures. This paper reports on a crowdsourced survey conducted three times, approximately every six months, starting in the summer of 2023, involving 100 users of VR/AR/MR HMDs. The analysis results revealed user perceptions and their transitions.

Keywords: CSS 2024, LaTeX, style files

1. はじめに

Virtual Reality(VR)/Augmented Reality(AR)/Mixed Reality(MR) 技術は、ヘッドマウントディスプレイ (HMD) と共に発展してきており、その用途はエンターテイメントにとどまらず、教育や専門的な分野での作業支援など多岐に拡大してきている。新たな IT 技術やその利用形態の誕生や発展は、利便性の向上をもたらす一方で、新たなセキュリティ上の脅威やリスクを生じさせてしまう。そのため、セキュリティ上の脅威やリスクについて十分に議論や対策をする必要が出てくる。

セキュリティの議論を行う中、ユーザにセキュリティ上の脅威やリスクへの対策を促すことは重要な課題の一つとなっており、そのためにはセキュリティ上の脅威やリスク、及びそれらへの対策に対するユーザの認識を把握することが必要不可欠である。著者らは昨年、VR/AR/MR に焦点を当ててセキュリティとプライバシの認識を図る網羅的な調査、およびその調査に用いる質問表の作成に参加した。

しかし、VR/AR/MR 技術の利用用途の拡大に伴い、ユーザの VR/AR/MR に対するセキュリティやプライバシの認識が変化してきている可能性がある。そこで本研究では、VR/AR/MR のセキュリティやプライバシに対するユーザの認識の変化はあるのか、あるとしたらどのようなものな

[1] 東邦大学
Toho University
[a)] 6523007k@st.toho-u.ac.jp
[b)] akira.kanaoka@is.sci.toho-u.ac.jp

のか、を Research Question として、調査を行った。調査は、昨年調査に用いた質問票を用いて約半年間毎に計 3 回実施した。

2. 関連研究

2.1 VR/AR/MR におけるセキュリティとプライバシ

VR/AR/MR に関するセキュリティやプライバシーの学術的なアプローチは, 2014 年頃より議論が始まった [1], [2]. 代表的な成果は Roesner と Kohno によるチームのものがあり、AR グラスにおけるプライバシーに焦点を置いた研究がされてきた [3], [4], [5]。

その後 2020 年代に入り研究は活発化し、VR において代表的な国際会議である IEEE VR では 2022 年に Security のセッションが設けられ、2023 年の USENIX Security でも Digital Reality に関するセッションが設けられ、続く 2024 年でもセッションが 1 つ設けられた。またヒューマンファクタとセキュリティを中心に扱う国際会議 SOUPS では併催ワークショップとして没入（immersive）をタイトルに掲げた Digital Reality に関連したワークショップが開催されるなど、コミュニティの拡大が見て取れる。

既存の計算機環境で起きてきた脅威の存在を VR/AR/MR デバイスでも発生することに着目した研究としては、アプリケーションによるセンサーやデータへのアクセス管理の不備を悪用した攻撃 [6], [7], [8]、そういったアクセス管理の不備を代表としてサイドチャネル攻撃を行うことでテキスト入力やユーザの行動、見ている映像を推定する攻撃 [9], [10], [11], [12], [13], [14], [15]、ユーザの識別や認証 [16], [17] がある。

VR/AR/MR 特有のセキュリティとプライバシーに関する研究は、ユーザの知覚の操作 [18], [19], [20] や、マルチユーザ環境における攻撃 [21], [22]、セキュリティ表示に関する研究 [23], [24]、ショルダーサーフィン攻撃 [25]、VR 空間におけるハラスメント [26], [27] などとともに、全般的なサーベイや課題の分類 [28], [29]、専門家によるユーザ認識検討 [30] などがある。本研究は、この中でもユーザの知覚を操作する攻撃について着目した。

2.2 ユーザに対するセキュリティやプライバシ認識調査

ユーザに対するセキュリティやプライバシーの認識に対する調査や検討は様々なアプローチが行われている。ユーザ全般に対するセキュリティ意識 [31], [32], [33] や、セキュリティツールに対する意識 [34]、パスワードポリシに対する意識 [35]、セキュリティメール利用者の意識 [36] などの研究が行われている。またそういった認識に対する評価尺度の研究 [37] や防護同期理論についてのアプローチも複数存在する [38], [39]。また、国内においてもいくつかの視点でアプローチが行われている [40], [41], [42]。

VR/AR/MR に対する認識については、MR 技術に対するユーザの不安や懸念に焦点を当てた研究 [43] や、著者らも参加した VR/AR/MR のセキュリティやプライバシに対する認識調査 [47] がある。

2.3 セキュリティやプライバシ認識の変遷調査

ユーザブルセキュリティ分野では、ユーザ実験にあたり異なる母集団や異なる分析手法によって得られる結果や知見が変わることが指摘されている。それに対して、ユーザブルセキュリティ分野に特化した国際会議である SOUPS では、2017 年より追試（Replication）研究を論文として募集し評価することを掲げている [44]。そこでは、同じ実験プロトコルで同じタイプのサンプルを用いる Full replication、1 つの設計変数が買えられている Variation、同じ実験目的だが違う設計を行う Triangulation といった細分化がされ、投稿が推奨されている。

Variation では例えば文化背景が異なる調査対象に対して同じ実験を行うなど異なる母集団に対するものもあれば、同じ母集団に対して実施する中で経年変化を評価する研究も対象となっている。いくつかの論文が経年変化を主眼に追試研究を行っている [45], [46]。これらは経年変化を深く分析しているものであるが、元の研究の数年後に再度実施といった経年変化であり、定期的な観測と分析を繰り返して経年変化を評価しているわけではない。

3. VR/AR/MR とセキュリティ・プライバシ

前章で紹介した通り VR/AR/MR においても他の IT 技術と同様にセキュリティやプライバシの問題が存在し、これらの問題について考えなければならない。また、VR/AR/MR 利用の増加は新たな脅威やリスクの発生につながる可能性があり、ユーザの VR/AR/MR のセキュリティやプライバシに対する意識を高めることはより重要なこととなってきている。

VR/AR/MR のセキュリティやプライバシの研究が増加傾向にあることから、セキュリティ研究者の VR/AR/MR のセキュリティやプライバシへの意識は高まっていると言えよう。一方で、それらに対する一般的なユーザの意識が高まってきているかどうかは、著者らの知る限り調査されておらず、わかっていない。

4. 調査に用いる質問票

VR/AR/MR のセキュリティに対するユーザの認識の変化を明らかにするため、約半年に一度の間隔で計三回アンケート調査を実施することで定量的に評価や分析を行った。アンケート調査には、著者らも参加したグループで以前、ユーザの VR/AR/MR に対するセキュリティやプライバシ認識調査を行った際に作成した質問票を用いた (**A.1**) 。

用いた質問票は、複数の質問項目から構成される以下の質問群から構成されている。

- VR/AR/MR のセキュリティへの脅威とリスクの認知状況 (Q1/Q4/Q7)
- VR/AR/MR の脅威やリスクへの対策方法の認知状況 (Q2/Q5/Q8)
- VR/AR/MR のセキュリティ対策実施状況 (Q3/Q6/Q9)
- パソコンのセキュリティ対策実施状況 (Q10)
- スマートフォンのセキュリティ対策実施状況 (Q11)
- セキュリティに対する認識 (Q12)
- セキュリティ上の被害経験 (Q13)

「パソコンのセキュリティ対策実施状況」の質問項目には、これを図るための既存尺度の一つである R-SeBIS[48], [49] を採用した。「スマートフォンのセキュリティ対策実施状況」の質問項目は、R-SeBIS の質問項目文中の「パソコン」や「タブレット」を「スマートフォン」に置き換えたものとした。また、「セキュリティに対する認識」には、これを図るための既存尺度である SA-6[50] を採用した。ただし、SA-6 は英語であったため、著者らも参加したグループで翻訳した。

5. 質問票によるセキュリティ・プライバシの認識調査

VR/AR/MR のセキュリティやプライバシに対するユーザ認識の変遷調査のために、ユーザ実験を三回、オンラインで実施した。一回目は 2023/06/22、二回目は 2024/02/10-11、三回目は 2024/08/09 に実施した。

5.1 実験条件

実験では、まず実験参加者に調査の目的と研究の内容を提示した。その際、調査にあたって VR/AR/MR のヘッドセットを利用した経験があるユーザだけが対象であることを提示した。ユーザが VR/MR/AR のヘッドセットを具体的にイメージすることが難しい可能性を考え、各ヘッドセットには具体的な製品名を付記した。2 回目以降のアンケート調査では MR の具体的な製品名の付記に、Magic Leap 2 と XREAL Air を追記した。

実験参加の同意を得たあと、提案質問票以外の質問として VR/MR/AR デバイスの利用経験を質問した。そこで VR/AR/MR の利用経験をそれぞれ機器、その回答にしたがって VR/MR/AR のどの質問に回答するかを選別した。MR の利用者が最も少ないと予想されたため、MR 利用経験があると回答した実験参加者には MR についての質問を行い、MR 利用経験がなく AR 利用経験がある実験参加者には AR についての質問、AR/MR ともに利用経験がなく VR 利用経験がある実験参加者には VR についての質問を行った。

VR/AR/MR のそれぞれの技術についての質問を行った後、VR/AR/MR 以外の質問は利用経験を問わず共通して質問した。

5.2 実験参加者

実験参加者はランサーズを利用して募集した。満 18 歳以上で日本語を理解することに加え、VR/AR/MR のヘッドセット利用経験があることを参加条件とした。事前に行ったパイロットテストにより回答終了までに費やす時間を計測し、回答時間と東京都の最低賃金をもとに報酬を 500 円と設定した。

VR/AR/MR の各質問について統計的な分析を行うために各技術に 30 名の回答を集めることを目標とし、各回ごとに 100 人を募集した。募集に対し各回共に 100 人がランサーズを介して実験に参加し、100 人全員が実験に同意し質問に回答した。第 2 回のアンケート調査に限り、1 人の回答不備データがあり分析対象から除外したが、それ以外の 299 件のデータは無事取得された。

第一回目の調査では、参加者の 69%が男性、年齢は 20 代から 50 代にわたった。第二回目の調査は、参加者の 74.7%が男性、年齢は 20 代から 60 代にわたった。第三回目の調査は、参加者の 75%が男性、年齢は 20 代から 70 代にまでわたった。三回とも、40 代の参加が最も多くなった。

利用経験の質問への回答では、VR の経験が第一回、第二回、第三回の調査でそれぞれ 90 人、82 人、81 人と最も多かった。VR の利用経験のあるデバイスとして、第一回と第二回の調査では HTC VIVE シリーズがあると答えた実験参加者はそれぞれ 3 人ずつだったのに対し、第三回の調査では 29 人と大きな差があった。同様に PICO シリーズの利用経験がある者も第一回、第二回、第三回のそれぞれ 4 人、2 人、28 人と第三回の調査の際は多くなった。逆に Meta Quest シリーズや Playstation VR シリーズの利用経験がある実験参加者数は、第三回の調査が最も少なかった。

6. ユーザ認識調査の結果

3 回の調査のすべてにおいて、AR と MR の質問群への回答数が適切な評価を行うには十分でなかったため、今回 AR と MR の質問群への回答は評価の対象外とした。そのため本章では、ユーザの VR セキュリティとプライバシ認識に対象を絞り、これの変遷を調査するために Q1, Q2, Q3 の 3 つの質問群に関する以下の内容の変化を示す。

- 各回の結果に対する因子分析の結果
- 各質問項目における平均値の変化

なお、結果の整理および因子分析では、Likert 尺度の各項目を 1 から 5 で数値化し、欠測値はその質問項目への回答の平均値で補完した。また、Q1, Q2 において数値の減

質問群	因子	質問項目番号
Q1	1	1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 13, 15, 18, 19, 26
	2	16, 17, 22
	3	23, 25
Q2	1	10,11, 12, 13, 14, 18, 19,20, 21, 24, 25, 27
	2	1, 2, 3, 4, 15
	3	5, 6, 7, 8, 9, 28
	4	22, 23, 26
Q3	1	8, 10, 11, 12, 13, 14, 20, 24, 25, 27, 28
	2	9, 15, 16, 17, 18, 19, 22, 23, 26
	3	1, 2, 3, 4
	4	5, 6, 7

表 1 第 1 回調査結果の因子分析により得られた因子構造

質問群	因子	質問項目番号
Q1	1	5, 6, 8, 10, 11, 12, 13, 14, 19, 22
	2	1, 2, 3, 9, 15, 18, 26
	3	16, 17, 23, 25
	4	20, 21
Q2	1	10, 11, 12, 14, 18, 25, 27
	2	1, 2, 3, 4
	3	5, 6, 7, 8, 17, 19, 22, 23, 26
	4	21, 28
Q3	1	1, 2, 3, 4, 8
	2	16, 17, 20, 22, 23, 26, 27, 28
	3	11, 12, 14, 18, 25
	4	5, 6, 7, 9, 15, 24

表 2 第 2 回調査結果の因子分析により得られた因子構造

少は認知度の向上を示し、Q3 においては実施度の高まりを示す。

6.1 各回の結果の因子分析

因子分析ではまず、各回、質問群ごとに質問項目の固有値を求めた。固有値を求めた後、スクリープロットにより各質問群の院指数を決め、院指数を固定し探索的因子分析 (EFA) を実施した。EFA の実施時、因子抽出法は最尤法を使い、プロマックス法 (Kappa=4) による回転を行った。EFA 実施後の各質問項目において、因子ごとの因子負荷量がいずれも 0.350 以上にならない質問項目と、共通性が 0.160 以上とならない質問項目を排除した。

第 1 回調査の結果に対して因子分析を行ったところ、質問群 Q1, Q2, Q3 の因子数は、それぞれ 3, 4, 4 となった。表 1 に各因子に該当する質問項目を示す。次に第 2 回調査結果の因子分析では、質問群 Q1, Q2, Q3 の因子数がすべて 4 となり、第一回調査結果に対する因子分析とは異なる結果となった。表 2 に各因子に該当する質問項目を示す。さらに第 3 回調査の結果の因子分析では、質問群 Q1, Q2, Q3 の因子数がそれぞれ 4, 3, 6 となり、本研究において行った 3 回の調査結果は因子分析の結果すべて異なる因子構造を持つことが明らかとなった。表 3 に各因子に該当する質問項目を示す。

質問群	因子	質問項目番号
Q1	1	1, 2, 3, 4, 8, 9, 10, 11, 12, 13, 15
	2	5, 6, 7, 18, 19, 22, 26
	3	14, 21, 23, 24, 25
	4	16, 17
Q2	1	5, 8, 9, 15, 16, 17,18, 20, 21, 22, 26
	2	6, 10,11, 12, 13, 14, 19, 24, 25, 27
	4	1, 2, 3, 4
Q3	1	1, 3, 8, 12, 14
	2	5, 6, 7, 9
	3	15, 16, 17
	3	13, 18, 20, 22, 27
	3	24, 25
	4	2, 4

表 3 第 3 回調査結果の因子分析により得られた因子構造

6.2 質問項目の平均値の比較

6.2.1 Q1 の質問項目ごとの平均値の比較

質問群 Q1 の質問項目において、第 1 回の調査から第 3 回の調査にかけて、平均値が上がったのは 7 問目と 26 問目のみで、他の質問項目の平均値は減少していた。平均値が下がった質問項目として、平均値が大きく下がった順に 5 問紹介する：

Q1-11：VR ヘッドセットに直接被害がなくても、接続したパソコンに悪影響のあるプログラムが存在する可能性がある。

Q1-19：コントローラーの認識や位置が正しくされていない場合、間違って写真を消してしまうなど、何か誤操作につながる可能性がある。

Q1-4：VR ヘッドセットについているカメラやマイクから周囲の情報が取得できる。

Q1-20：VR ヘッドセットの画面は他人から基本的には見えないため、トラブルの対処が難しい

Q1-12：実写を含む映像や写真を VR ヘッドセットで撮影する際に他人が写ってしまう等、肖像権の侵害になる可能性がある

逆に平均値が上がった 2 問の内容は以下の通りである：

Q1-7：バーチャル空間でのアバターは、データさえあれば見た目の完璧な再現が可能である。

Q1-2：VR 体験後、体験中の感覚が持続することがあり、数時間後に症状がより強く表れることもある。

6.2.2 Q2 の質問項目ごとの平均値の比較

質問群 Q2 の質問項目は、第 1 回から第 3 回の調査にかけて Q1 の質問項目程平均値が大きく変化した質問項目はなかった。平均値が下がった質問項目数は 19 問、上がった質問項目は 9 問であった。平均値が下がった質問項目として、平均値が大きく下がった順に 3 問紹介する：

Q2-23：バーチャル空間でハラスメントや迷惑行為の被害にあった場合、そのバーチャル空間サー

ビスに通報する。

Q2-3：カメラやマイクは、意図するアプリが必要とする時だけアクセスを許可する。

Q2-13：不用意に周辺の Wi-Fi には接続しない。

逆に平均値が大きく上がった質問項目の内容は以下の通りである：

Q2-28：VR 体験後に体験中の感覚が持続している場合は、症状が治まるまで車の運転をしてはいけない。

Q2-22：バーチャル空間では、その場にいない誰かに見聞きされている前提で過ごす。

Q2-20：VR ヘッドセットの操作確認は事前にしっかりと行っておき、思わぬ誤操作をしないようにする。

6.2.3 Q3 の質問項目ごとの平均値の比較

質問群 Q3 の質問項目も、第 1 回から第 3 回の調査にかけて Q1 の質問項目程平均値が大きく変化した質問項目はなかった。平均値が下がった質問項目数は 13 問、上がった質問項目は 15 問であった。平均値が下がった質問項目として、平均値が大きく下がった順に 3 問紹介する：

Q3-23：バーチャル空間でハラスメントや迷惑行為の被害にあった場合、そのバーチャル空間サービスに通報する。

Q3-24：VR ヘッドセットを利用する際は、周囲に誰もいない環境で利用するか、利用時に近寄らないでもらう。

Q3-27：VR 酔いなど、体調が悪くなったらすぐに利用を中止する。

逆に平均値が大きく上がった質問項目の内容は以下の通りである：

Q3-9：バーチャル空間で、自分が話していると思っている人が本人か否かを見た目以外からも併せて判断する。

Q3-5：普段インターネットで情報を集める時以上に、嘘や間違い情報を警戒する。

Q3-20：VR ヘッドセットの操作確認は事前にしっかりと行っておき、思わぬ誤操作をしないようにする。

7. 考察

3 回分のアンケート結果を因子分析した際の因子構造が一貫なものとならなかったことから、ユーザの VR/AR/MR セキュリティ、プライバシ認識が変化してきている可能性が考えられる。

また、Q1 において 26 の質問項目の中、24 問において平均値が下がったことから、ユーザによる VR のセキュリティ脅威やリスクの認知度が全般的に高まってきている可能性が明らかとなった。中でも、平均値が下がった上位 5 問の中に、VR HMD のカメラやマイクによるプライバシ問題が 2 問あることから、ユーザは VR の利用時にプライバシ問題について考えるようになってきている可能性が考えられる。一方で、第一回と第三回のアンケートでは VR デバイスの利用経験に大きな差があったことから、Q1-11 の内容の認知度は向上している結果となったが、実験参加者の利用経験による差である可能性も考えられる。

Q2 と Q3 において、バーチャル空間におけるハラスメントに関しての対策方法の認知度や対策実施度が実験結果では高まったことから、ユーザにとって VR 空間におけるハラスメントは身近な問題となってきている可能性が考えられる。

全体的な結果を見ると、VR のセキュリティへの脅威とリスクの認知状況や対策方法の認知状況に関する質問項目への回答の平均値が下がっているものの方が多い一方で、VR のセキュリティ対策実施状況に関する質問項目への回答の平均値が上がっているものがおおいことから、ユーザはまだ VR の利用において、セキュリティ対策行為を行う必要性をあまり感じていないか、労力のかかることだと考えている可能性が考えられる。

実験参加者の経験による差も考えられるが、第一回から第三回の調査にかけて結果が変わっていたことから、今後もユーザの VR/AR/MR セキュリティに対する認識の調査を続け、変遷を観察し続けることが必要である可能性が考えられる。

8. おわりに

本研究では、VR/AR/MR のセキュリティへのユーザ認識の直近の約 1 年での変遷について、調査を試みた。

調査においては著者らが昨年作成に参加した VR/AR/MR のセキュリティやプライバシ認識を調査するための調査票を用いて、約半年ごとにアンケート調査を実施した。調査結果に対して、因子分析や質問項目ごとの平均値計算を行い、各回の違いを観察した。

AR/MR については十分なサンプル数を得ることができず、評価の対象外となったが、因子構造の変化からユーザ意識が変わってきている可能性や、VR のセキュリティへの脅威とリスクの認知度が上がってきている可能性が明らかとなった。

謝辞 本研究は、JST、CREST、JPMJCR22M4 の支援を受けたものである。本研究の遂行にあたり、多大なご助言とご協力を頂いた KDDI 総合研究所の磯原隆将氏、佐野絢音氏の両名に深く感謝申し上げる。

参考文献

[1] Denning, T, et al.: In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and

Privacy-Mediating Technologies, ACM CHI'14, 2014
[2] Roesner, F., et al.: Security and Privacy for Augmented Reality Systems, Commun. ACM, Vol. 57, No. 4, p. 88–96, 2014
[3] Lebeck, K., et al.: Securing Augmented Reality Output, IEEE SP 2017, 2017
[4] Lebeck, K., et al.: Towards Security and Privacy for Multi-user Augmented Reality: Foundations with End Users, IEEE SP 2018, 2018
[5] Ruth, K., et al.: Secure Multi-User Content Sharing for Augmented Reality Applications, USENIX Security ' 19, 2019
[6] Farrukh, H., et al.: LocIn: Inferring Semantic Location from Spatial Maps in Mixed Reality, USENIX Security ' 23, 2023
[7] Kim, Y., et al.: Erebus: Access Control for Augmented Reality Systems, USENIX Security ' 23, 2023
[8] Slocum, C., et al.: Going through the motions: AR/VR keylogging from user head motions, USENIX Security ' 23, 2023
[9] Arafat, A. A., et al.: VR-Spy: A Side-Channel Attack on Virtual Key-Logging in VR Headsets, IEEE VR 2021, 2021
[10] Gopal, S. R. K., et al.: Hidden Reality: Caution, Your Hand Gesture Inputs in the Immersive VirtualWorld are Visible to All!, USENIX Security ' 23, 2023
[11] Luo, S., et al.: HoloLogger: Keystroke Inference on Mixed Reality Head Mounted Displays, IEEE VR 2022, 2022
[12] Meteriz-Yıldıran, C., et al.: A Keylogging Inference Attack on Air-Tapping Keyboards in Virtual Environments, IEEE VR 2022, 2022
[13] Zhang, Y., et al.: It' s all in your head(set): Side-channel attacks on AR/VR systems, USENIX Security ' 23, 2023
[14] Luo,S., et al.:Eavesdropping on Controller Acoustic Emanation for Keystroke Inference Attack in Virtual Reality, NDSS 2024, 2024
[15] Nguyen, A., et al.: Penetration Vision through Virtual Reality Headsets: Identifying 360-degree Videos from Head Movements, USENIX Security ' 24, 2024
[16] Nair, V., et al.: Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data, USENIX Security ' 23, 2023
[17] Zhu, H., et al.: Sound-Lock: A Novel User Authentication Scheme for VR Devices Using Auditory-Pupillary Response, NDSS 2023,, 2023
[18] Tseng, W-J.,et al.: The Dark Side of Perceptual Manipulations in Virtual Reality, ACM CHI '22, 2022
[19] Cheng, K., et al.: Exploring User Reactions and Mental Models Towards Perceptual Manipulation Attacks in Mixed Reality, USENIX Security ' 23, 2023
[20] Casey, P., et al.: Immersive Virtual Reality Attacks and the Human Joystick. IEEE Trans. on Dependable and Secure Computing 18, 2 (2021), 550-562 (2021).
[21] Su, Z., et al.:Remote Keylogging Attacks in Multi-user VR Applications. USENIX Security ' 24, 2024
[22] Slocum, C., et al.:That Doesn't Go There: Attacks on Shared State in Multi-User Augmented Reality Applications. USENIX Security ' 24, 2024
[23] Windl, M., et al.: Investigating Security Indicators for Hyperlinking Within the Metaverse, SOUPS 2023, 2023
[24] Cheng, K., et al.:When the User Is Inside the User Interface: An Empirical Study of UI Security Properties in Augmented Reality. USENIX Security ' 24, 2024
[25] Mathis, F., et al. : Virtual Reality Observations: Using Virtual Reality to Augment Lab-Based Shoulder Surfing Research, IEEE VR 2022, 2022
[26] Abhinaya S.B., et al.: Enabling Developers, Protecting Users: Investigating Harassment and Safety in VR, USENIX Security ' 24, 2024
[27] Abhinaya, S.B., et al.:Enabling Developers, Protecting Users: Investigating Harassment and Safety in VR. USENIX Security ' 24, 2024
[28] Huang, Y., et al.: Security and Privacy in Metaverse: A Comprehensive Survey, Big Data Mining and Analytics, Vol. 6, No. 2, pp. 234–247 (2023).
[29] Qamar, S., et al.: A systematic threat analysis and defense strategies for the metaverse and extended reality systems, Computers & Security, Vol. 128, p. 103127 (2023).
[30] Deldari, E., et al.: An Investigation of Teenager Experiences in Social Virtual Reality from Teenagers', Parents', and Bystanders' Perspectives, SOUPS 2023, 2023
[31] Alotaibi, F. and Alshehri, A.: Gender Differences in Information Security Management, Journal of Computer and Communications, Vol. 08, No. 03, pp. 53–60 (2020).
[32] Frik, A., Nurgalieva, L., Bernd, J., Lee, J., Schaub, F. and Egelman, S.: Privacy and Security Threat Models and Mitigation Strategies of Older Adults, SOUPS 2019, Santa Clara, CA, USENIX, pp. 21–40 (2019).
[33] Wash, R. and Rader, E.: Too Much Knowledge? Security Beliefs and Protective Behaviors Among United States Internet Users, SOUPS 2015, Ottawa, USENIX, pp. 309–325 (2015).
[34] Das, S., Kim, T. H.-J., Dabbish, L. A. and Hong, J. I.: The Effect of Social Influence on Security Sensitivity, SOUPS 2014, Menlo Park, CA, USENIX, pp. 143–157 (2014).
[35] Inglesant, P. G. and Sasse, M. A.: The True Cost of Unusable Password Policies: Password Use in the Wild, CHI ' 10, ACM, p. 383–392 (2010).
[36] Usman, W., Hu, J., Wilson, M. and Zappala, D.: Distrust of big tech and a desire for privacy: Understanding the motivations of people who have voluntarily adopted secure email, SOUPS 2023, USENIX, pp. 473–490 (2023).
[37] Huang, H.-Y., Demetriou, S., Hassan, M., Tuncay, G. S., Gunter, C. A. and Bashir, M.: Evaluating User Behavior in Smartphone Security: A Psychometric Perspective, SOUPS 2023, USENIX, pp. 509–524 (2023).
[38] Pahnila, S., Karjalainen, M. and Siponen, M. T.: Information Security Behavior: Towards Multi-Stage Models, Pacific Asia Conference on Information Systems (2013).
[39] Warkentin, M., Johnston, A. C., Shropshire, J. and Barnett, W. D.: Continuance of protective security behavior: A longitudinal study, Decision Support Systems, Vol. 92, pp. 25–35 (2016).
[40] 諏訪博彦, 原賢, 関良明：情報セキュリティ行動モデルの構築—人はなぜセキュリティ行動をしないのか，情報処理学会論文誌, Vol. 53, No. 9, pp. 2204–2212 (2012).
[41] 澤谷雪子，佐野絢音, 山田明, 窪田歩：個人のインターネット利用におけるセキュリティ対策行動開始のきっかけの分析，情報処理学会論文誌, Vol. 61, No. 12, pp. 1845–1858 (2020).
[42] 澤谷雪子, 山田明，半井明大，浦川順平，松中隆志，窪田歩：セキュリティリスク回避行動に影響を与えるユーザ要因間の構造の解析，情報処理学会論文誌, Vol. 57,No. 12, pp. 2696–2710 (2016).
[43] Katins, C., Woźniak, P. W., Chen, A., Tumay, I., Luu, V. T. L., Uschold, J. and Kosch, T.: Assessing User Ap-

prehensions About Mixed Reality Artifacts and Applications: The Mixed Reality Concerns (MRC) Questionnaire. In Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24). Association for Computing Machinery, New York, NY, USA, Article 604, 1–13 (2024).
[44] USENIX - SOUPS 2017 Call for Papers, https://www.usenix.org/conference/soups2017/call-for-papers, 2017
[45] Bird, S., Segall, I., Lopatka, M.:Replication: Why We Still Can't Browse in Peace: On the Uniqueness and Reidentifiability of Web Browsing Histories, SOUPS 2020, 2020
[46] Tang, J., Birrell, E., Lerner, A.:Replication: How Well Do My Results Generalize Now? The External Validity of Online Privacy and Security Surveys, SOUPS 2022, 2022
[47] 倉﨑翔大，佐野絢音，金岡晃，磯原隆将： VR/AR/MR に対するセキュリティとプライバシー認識に関する調査，Computer Security Symposium 2022 (CSS 2022)，2022.
[48] Sawaya, Y., Sharif, M., Christin, N., Kubota, A., Nakarai, A. and Yamada, A.: Self-Confidence Trumps Knowledge: A Cross-Cultural Study of Security Behavior, Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems, CHI ' 17, ACM, p.2202–2214 (2017).
[49] Serge Egelman and Eyal Peer. 2015a. The myth of the average user: Improving privacy and security systems through individualization. In Proceedings of NSPW.
[50] Faklaris, C., Dabbish, L. A. and Hong, J. I.: A Self-Report Measure of End-User Security Attitudes (SA-6), SOUPS 2019, Santa Clara, CA, USENIX, pp. 61–77 (2019).

付　　録

A.1 質問票の詳細情報

本研究において用いた質問票は Github 上 (https://github.com/kanaoka-laboratory/xrsec_questionnaire) に公開している。