光学的透過型HMDにおける映像の予期せぬ移動が与える影響とリスク

倉﨑 翔大[1]　金岡 晃[1,a)]

概要：光学的透過型 AR/MR HMD は様々な分野での作業支援やエンターテイメントなど、利用用途が拡大してきており、同時にそこにあるセキュリティやプライバシ問題への対策がより重要になってきている。様々なセキュリティやプライバシ問題が考えられている中、本研究では映像が予期せぬ移動をすることによる影響とリスクに着目した。映像の予期せぬ移動は、支援対象である作業の妨害や視線誘導によるプライバシ侵害などにつながる可能性が考えられる。映像の予期せぬ移動による影響やリスクを明らかにするため、本稿ではユーザ実験及びそのデザインを行い、その結果の分析をした。

キーワード：Virtual Reality，Augmented Reality，Mixed Reality, 知覚操作攻撃

Effects and Risks of Unexpected Image Movement in Optical See-Through HMD

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

Abstract: Optical see-through AR/MR HMDs are increasingly being used in various fields for task support and entertainment, which has concurrently raised the importance of addressing security and privacy issues. Among the various security and privacy issues, this study focuses on the impact and risks associated with unexpected image movement. Unexpected image movement can potentially lead to the interference with the supported tasks or privacy invasion through gaze guidance. To clarify the effects and risks of unexpected image movement, we designed and conducted user experiments, followed by an analysis of the results.

Keywords: Virtual Reality，Augmented Reality，Mixed Reality, Perceptual Manipulation Attack

1. はじめに

光学的透過型 AR/MR ヘッドマウントディスプレイ（HMD）は、物理的な現実世界とデジタル情報をシームレスに融合させる技術として、エンターテインメントから産業業界まで幅広い分野で急速に普及している。このようなHMD の普及に伴い、作業効率の向上や新しい体験の提供といったメリットが享受される一方で、新たなセキュリティとプライバシーの脅威が顕在化しつつある。特に、ユーザの意図しない形で映像が移動する現象、いわゆる「映像移動攻撃」は、これまでのセキュリティ研究において十分に考慮されてこなかったリスク領域であり、その影響は未解明の部分が多く残されている。

既存の VR/AR/MR に関するセキュリティ研究は、2020年ころから研究が増えつつあるが、それらは主にユーザのデータ保護やアクセス制御、ショルダーサーフィン攻撃の防御といったテーマに集中してきた。一方で、従来の計算機環境と比較してより強く知覚に訴えかける VR/AR/MR について、ユーザの知覚に対する直接的な操作を通じた攻撃、すなわち知覚操作攻撃（Perceptual Manipulation Attacks, PMA）については十分に掘り下げられていない。特に、最も知覚として影響が強いと考えれれる視覚情報に焦点を当てた攻撃については、従来の研究が限られており、

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

視覚的な干渉や改ざん、そして本研究で取り上げる映像の予期せぬ移動がどのようにユーザに影響を及ぼすかについては、未だ明確な理解が進んでいないのが現状である。

映像移動攻撃とは、HMD の表示領域において、ユーザが意識しないまま HMD 上に表示される映像が予期せぬ方向へ移動することにより、ユーザの注意や視線を操作する攻撃を指す。この攻撃は、ユーザの視線誘導を通じて作業を妨害したり、視線を操作されることで視線の先にある特定の情報を悪意ある第 3 者に不正に取得される可能性があるため、作業効率の低下やプライバシ侵害といった深刻なリスクを引き起こす可能性がある。例えば、作業支援アプリケーションを使用しているユーザが、重要な情報を見逃すことで作業ミスを誘発されるリスクや、攻撃者がユーザの視線を操作して意図的にプライバシー情報や作業環境周辺の機密情報を収集するリスクが考えられる。

本研究の目的は、光学的透過型 HMD における映像移動攻撃がユーザに与える影響とリスクを体系的に評価し、その具体的な脅威を明らかにすることにある。具体的には、映像が予期せぬ形で移動した場合に、ユーザがどの程度その移動に気付き、また気付かずに作業を継続した場合にどのようなリスクが生じるかを実験的に検証する。これにより、視覚情報操作攻撃の一形態である映像移動攻撃が実際にユーザに与える影響の実態を解明し、今後のセキュリティ対策の基礎となるデータを提供することを目指す。

研究の目的に対し、Research Question として以下の 2 つを設定した。

RQ1：光学的透過型 HMD における映像移動攻撃による影響はどのようなものか

RQ2：ユーザに気づかれず映像移動攻撃をすることはできるのか

本研究では、2 つの RQ に答えるために 22 名の実験参加者を対象に光学的透過型 HMD である Magic Leap 1 を用いたユーザ実験を実施したした。実験では、映像移動攻撃が実施された際に参加者がどのように反応するかを観察し、映像移動が作業効率やプライバシーに与える影響を明らかにすることを狙った。実験参加者に対しては、移動攻撃が行われたことを認識させる前後でインタビューを行い、移動の認識とその影響についての定性的なデータを質的研究のアプローチを採用し分析した。

実験と分析の結果、映像が連続的に移動した場合に多くの実験参加者がその移動に気づかず、特に連続的な映像移動が気付かれにくいことが判明した。この結果は、ユーザが知らない間に視線や注意を操作されるリスクが現実のものであることを示しており、特に産業用や医療用の HMD 利用環境においては重大なセキュリティリスクとなり得ることを示唆している。

本研究は光学的透過型 HMD における新たなセキュリティリスクを明らかにし、今後のセキュリティ研究において映像移動攻撃の防御策や検知手法の検討が必要であることを示している。

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 年と 2024 年の USENIX Security でも Digital Reality に関するセッションが設けられた。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。

既存計算機環境の脅威の存在を 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]、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 [8], [9], [10], [11], [12]、ユーザの識別や認証 [13], [14] がある。

VR/AR/MR 特有の研究は、ユーザの知覚操作 [15], [16], [17] や、マルチユーザ環境における攻撃 [18], [19]、セキュリティ表示に関する研究 [20], [21] 、VR 空間におけるハラスメント [22], [23] などとともに、全般的なサーベイや課題の分類 [24], [25] などがある。

2.2 知覚操作攻撃（PMA）

ユーザの知覚を操作する攻撃は知覚操作攻撃（Perceptual Manipulation Attacks、PMA）と呼ばれており、Tseng らによって VPPM（Virtual-Physical Perceptual Manupulation）がユーザ同意なしに無意識にユーザに適用される攻撃として整理され [15]、その一部については Cheng ら [16] や Casey ら [17] によってユーザ実験を行われてきた。

Cheng らは、MR 環境における PMA について、視覚と聴覚に対する攻撃を、3 つのシナリオ及び攻撃に分けてユーザ実験を行った。まず 1 つ目は、誤った情報を HMD 上に表示することでユーザを誤認させる視覚的な攻撃である。2 つ目は、通知音や着信音を流すことによって、ユーザの注意をそらし、タスクのミスを誘発することを目的とした聴覚的な攻撃である。最後に 3 つ目は、HMD 上の映像及

びタスクに集中させることにより、物理的な世界での出来事を認識させないことを目的とした攻撃である。これらの攻撃は一定の効果を表し、ユーザが敵対的な MR コンテンツによって操作される可能性が示された。

Casey らは、VR HMD ユーザをユーザ自身に気づかれることなく移動させる攻撃を Human Joystick Attack（HJA）と呼び、ユーザ実験を行った。このユーザ実験では 5 つの VR ゲームが用意され、VR コンテンツ全体を 1cm/s で移動させることで HJA を行い、94.4%のユーザが初期位置から前方 1.9m の位置まで無意識のうちに誘導された。

3. 視覚情報操作攻撃

3.1 過去研究による攻撃分類と実験における課題

Tseng らにより整理され Cheng らによりユーザ実験がされた PMA ではあるが、Cheng らの実験で扱った知覚は視覚に対するものと聴覚に対するものに別れ、さらに視覚に対するものも色の違いによるものと、視線の集中によるものの 2 点に限定された実行であった。それは Tseng らが整理した攻撃分類のすべてを網羅しているわけではない。また、Tseng らは VPPM について攻撃分類をしたが、それらの VPPM を引き起こす各種知覚についてさらに詳細に分類を行っているわけではなかった。しかし、視覚に対してユーザに与えうる影響は他の近くに比べて強く、かつ広範であることが予想される。そこで、本節では Tseng らの分類や Cheng らの実験を踏まえ、視覚情報に焦点をあて PMA がどう行われるかをさらに詳細に考察した。

3.2 視覚情報操作攻撃とその分類

Tseng らは、VPPM が同意なしに無意識のうちにユーザに適用される攻撃を指摘し、Cheng らはそれを PMA と呼んだ。本稿では、その PMA をさらに視覚に限定したものを視覚情報操作攻撃と呼ぶことにする。視覚情報操作攻撃は、悪意のあるユーザが起こす行動により以下に分類ができる

- 視覚干渉オブジェクトの不正挿入：ユーザが見ている環境に対して、悪意のあるユーザが不正なオブジェクトを挿入しユーザ行動に干渉をすることで、誤った認識や行動を引き起こす攻撃
  - 視覚干渉オブジェクトを正規オブジェクトの手前や覆うように配置することでユーザの視界を遮る攻撃
  - 視覚干渉オブジェクトを周辺視野に配置することでユーザの意識や集中を逸らせ干渉をする攻撃
- 視覚情報の消去：ユーザが見ている環境に本来存在するべき視覚情報を意図的に消去することで、ユーザに対する重要な情報を隠し、誤った認識や行動を引き起こす攻撃
- 視覚情報の改ざん：ユーザが見ている環境に存在する視覚情報を他の情報に置き換えることで、ユーザに誤った認識や行動を引き起こす攻撃
- 視覚情報の位置変更：ユーザが見ている環境に存在する視覚情報の位置を変更することで、ユーザに誤った認識や行動を引き起こす攻撃

本研究ではこれらの攻撃のうち Casey らが HJA として行った「視覚情報の位置変更」に着目し、それらをあらためて「映像移動攻撃」と呼ぶことする。Casey らが没入型の環境で実験していたことに対し、パススルーにより物理的な周辺情報が視覚に提供される環境において悪意のある視覚情報の位置変更がどのようにユーザに影響を与えるかを検証する。

4. 映像移動攻撃

4.1 映像移動攻撃による脅威やリスク

映像移動攻撃による具体的な脅威やリスクとしては、以下のようなものがあると考えられる。まず 1 つ目は、攻撃により映像の視認性が低下して作業効率が低下することである。その結果、作業支援として表示位置に重要な意味合いがあった場合には作業ミスが誘発されてしまう可能性がある。2 つ目は、視線誘導を用いたプライバシ侵害などの悪意のある行為の助長である。攻撃者が HMD のカメラ情報を取得していた場合、視線誘導によってより多くの周辺情報を攻撃者は取得することが可能になる。

しかし、映像を移動させることでユーザの視線を無意識に誘導できるかどうかは、一概には言えない。移動が明確に実施されたケースでは、移動はユーザに認知され違和感を持たれ、リスクを回避する行動を取る可能性が高くなる。そのため、映像移動攻撃のリスクが顕在化するにはユーザ自身の気付きが重要な要素となる。

4.2 映像の移動

映像移動攻撃が行われる場合の映像移動は多くのパターンがある。本節では映像移動攻撃による映像の移動について整理し、どの移動がユーザに気付かれにくいかを検討する。

4.2.1 方向や回転

映像の表示位置の移動を直線、もしくは円軌道に沿うような単純な移動に絞った場合、前、後ろ、左、右、上、下の 6 方向への移動と、ロー、ヨー、ピッチの 3 種の回転における移動がある。ユーザが注目すべき映像に対し、ユーザは視点だけでなく顔の向きも移動させると仮定すると、映像移動攻撃に気が付く要因は視覚によるものだけでなく、首のねじれや前庭感の変位によるなど複数の要因が関係すると考えられる。前述した映像の移動のほとんどは、映像に対して顔を向けるために首を動かす必要がある。しかし、前と後ろへの映像の移動は、他の移動ほど首を動かす必要

性がない。また、映像は近くに来るほど視野における締める割合の変化が大きくなるため、気付く可能性が高いと考えられる。これらから、映像の移動は前方への移動だと仮説を立てた。

4.2.2 速度

映像の移動を速度で考えると滑らかな移動である連続的移動と瞬間移動である非連続的移動に分けられる。

映像の連続的移動と非連続的移動のどちらが気付きにくい移動かを検討したが、条件により気付きやすさが変わり判断は難しいため仮説を立てなずに実験の評価対象に含めることとした。

4.3 前提となる攻撃者モデル

本研究では、AR/MR HMD 上の映像を操作することのできる強力な攻撃者モデルを前提として議論を行う。これは Tseng らが示した攻撃者モデル [17] に沿うものであり、Tseng らや Cheng らの研究と同様に本稿の焦点が視覚情報操作攻撃の技術的な実現性や防御策などの議論にに先立つ攻撃の影響やリスクの明確化にあるためである。

5. ユーザ実験のデザイン

本研究では、2 つの RQ に答えるため、ユーザ実験を行った。ユーザ実験では、映像移動攻撃による影響を観察するために、まず実験参加者にタスクを課し実験参加者がタスクを実施している間に映像移動攻撃を行う。その後、映像移動攻撃による影響や実験環境について柔軟かつ深く理解し評価を行うため、半構造化インタビューを行った。

5.1 実験シナリオ

実験では、実際に MR HMD を用いた作業支援を実験参加者に受ける体験を提供し、体験中に映像移動攻撃を行うことで、攻撃の影響を生態学的妥当性の確保を図りつつ観察しインタビューをする。今回行ったユーザ実験で支援の対象とするタスクは、ルービックキューブの盤面を 6 面揃えることとした。

支援対象のタスクは、実環境に近い実験環境の構築のため、次の 2 つを満たすことが必要であった。1 つ目は、MR HMD 等を用いた支援を行うことが自然になるため、多くの人によって自力では遂行が困難な作業であることである。2 つ目は、PC やタブレットなどよりも MR HMD を用いて支援する方がより効果的であることや、支援環境が本来の作業を阻害しないことである。ルービックキューブの盤面を 6 面揃えることは、これらの条件を満たす作業であると考え、ユーザ実験におけるタスクと設定した。

5.2 実験環境

実験環境には机と椅子を用意し机上に未完成のルービックキューブを置いた。実験参加者は椅子に座り机上の未完成ルービックキューブを 6 面揃えるタスクを実施する。その際に MR HMD を装着し、揃えるための支援を受ける。

MR HMD には実験用に開発したアプリケーションを導入した。実験用アプリケーションでは、ディスプレイ上部に 3D オブジェクトのルービックキューブを表示し、物理的に手元にあるルービックキューブからあと何手で 6 面が揃えられるかの数字と、現在何手目であるかの情報、さらにはキューブ盤面を進める／戻すといった操作の説明が表示されている（図 1)。

実験には光学的透過型 MR HMD である Magic Leap 1 を用いた。Magic Leap 1 は光学的透過型の HMD を持ち、PC と接続せずに稼働するスタンドアローン型のデバイスである。ディスプレイが表示する視野（Field of Vision、FoV）は水平 40 度、垂直 30 度、対角 50 度の性能を持つ。

5.3 実験全体の流れ

ユーザ実験ではまず、実験の目的やタスク、映像移動攻撃を行うこと、取得する情報とその管理、謝礼、中断についての説明を実験参加者に行い、実験参加への同意を得た。実験参加への同意を得たのちに、インタビューの分析や映像移動攻撃による影響の観察のため、実験風景の撮影と録音を開始する。

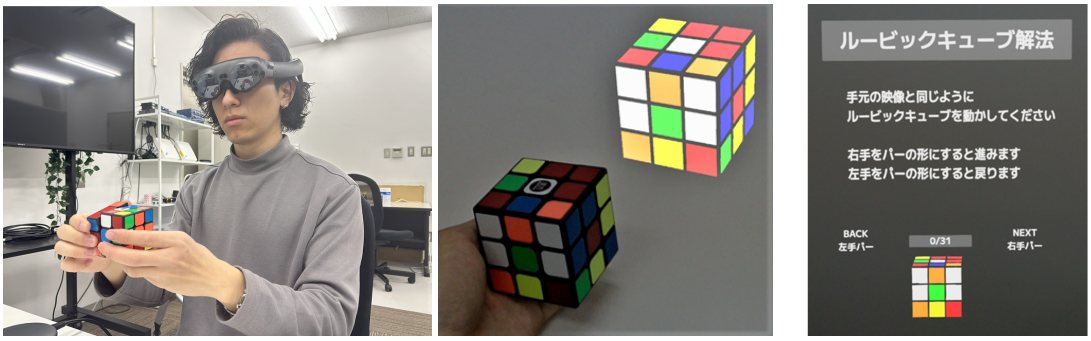
撮影開始後、改めてタスクの説明を行い、タスクのチュートリアルを受ける時間を設けた。タスク開始後、タスク実施中に映像移動攻撃を行う。

タスク終了後、実験参加者には HMD を装着してもらったまま、一度インタビューを行う。次に HMD を外し、実験参加者にアンケートへの回答を依頼し、その後再度インタビューを行い、謝礼を渡して実験終了とした。

5.4 本ユーザ実験における映像移動攻撃

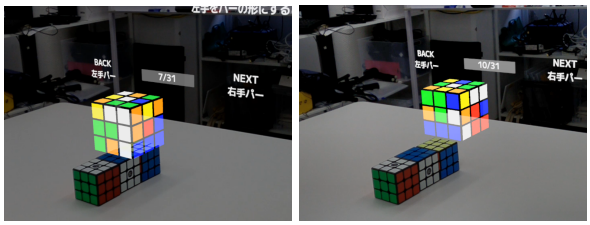
攻撃としての映像移動は前方への移動を、移動は連続的移動と非連続的移動の両者を採用し、2 パターンの映像移動攻撃を行う。連続的移動と非連続的移動の移動距離は、映像のルービックキューブの物理的な 1 個分のサイズである 7.5cm とした。

また、非連続的移動の移動速度の設定は 0.5cm/s とした。Casey らの HJA[17] では映像全体の表示位置を 1cm/s で移動させていたが、Casey らの実験で用いられた非透過の完全没入型の VR デバイスではなく光学的透過型の HMD であるため物理的環境も視界に入ることで移動に気付きやすいこと、さらには Casey らの実験では実験参加者は立って作業をしていたことに対して本実験では椅子に座って作業をしていることから 1cm/s での移動への認知が容易であると考え、そこで、半分の速度である 0.5cm/s で映像の表示位置を移動させることとして実験した。



(a) 実験で利用する Magic Leap 1　(b) ユーザが視認する情報　(c) ディスプレイ表示される情報

図 1: 実験に用いられたデバイスとアプリケーション



(a) 移動前　(b) 移動後

図 2: ディスプレイに表示される情報の移動

5.5　インタビュー

ユーザ実験では半構造化インタビューを 2 回に分けて行った。ここでは 1 度目のインタビューを「タスク直後のインタビュー」、2 度目のインタビューを「アンケート後のインタビュー」と呼ぶこととする。

インタビューの結果分析は、録音されたインタビュー音声を文字起こしし著者らでコーディングを行い、コーディング結果をもとに考察を行った。コーディングは著者ら 2 名でそれぞれ帰納的コーディングを行い、信頼性担保としてコードの一致とその議論に加えてコードを割り当てたインタビューの文字起こしテキストデータに対して質的研究支援ソフトである NVivo を用いて Cohen の kappa 係数の計算を行い、係数が Fleiss ら [26] が示す 0.75 を超えるまで議論とコードの再検討とコードの再割り当てを実施した。最終的な kappa 係数は 0.77 であった。

5.5.1　タスク直後のインタビュー

タスク直後のインタビューでは、まず最初に映像移動攻撃に気が付いたかどうかを質問した。回答に応じ、気付いた移動の詳細情報や、違和感の有無など他の気付きの存在についての質問を追加して行った。

その後、映像移動攻撃前と後の映像の表示位置を交互に示し、それにより気が付いたことや感想などを質問した。

5.5.2　アンケート後のインタビュー

アンケート後のインタビューでは、大きく分けて 3 種の質問をした。

1 つ目は、映像移動攻撃に気が付いていた場合に攻撃が気になったか、どの様に攻撃に気づいたのか、いつ頃気が付いたのか、について質問を行った。また、事前に映像移動攻撃を行うと言われていなかった場合にも気付けたと思うかどうかについても質問した。

2 つ目は、映像移動攻撃以外による違和感やストレスがあったかどうかの質問や、支援用アプリケーションの自然さについての質問を行った。

3 つ目は、実験参加者のルービックキューブを揃える技術や経験について質問を行った

5.6　実験参加者の募集

実験参加者は、著者らが所属する大学の学部、もしくは大学院研究科の学生を対象に募集を行った。実験は 2023/12/25 から 2024/01/25 で行い、22 名の実験参加者が実験に参加した。

参加にあたり実験参加者に裸眼の視力が 0.7 以上であることを条件とした。Magic Leap 1 は眼鏡を着用したままでは利用ができない。また、映像の移動による影響を評価する研究であるため映像を一定の明瞭さで視認できる状況が必要であるために条件を設定した。

報酬は、所要時間の目安が 45 分程度であることと著者らが所属する大学が所在する県の最低賃金を勘案し、1,000 円分の図書カードの進呈とした。

5.7　倫理配慮

ユーザ実験は著者らが所属する大学の倫理審査を通過した上で行った。

取得した情報についてはいずれも個人の特定につながる情報は結びつけず、研究室で厳重に管理を行った。また、実験はいつでも中断することができ、中断した場合でも謝礼を受け取ることができることを実験参加者に伝えた。

6.　結果

本章では、コーディング結果に基づき、それぞれのコードに関するユーザの特徴を示し、RQ1 と RQ2 への答えを

得る。

6.1 映像移動攻撃について

6.1.1 移動の認知

タスク直後のインタビューにおいて、実験参加者のうち 50% (11/22) が何らかの映像移動攻撃に気が付いたと回答した。この回答には、映像移動の内容を正しく認識したかどうかを問わずに気が付いたと回答した実験参加者だけを抽出したため、移動の認識が異なっている実験参加者が含まれている。

6.1.2 移動詳細の認識

何らかの映像移動攻撃に気が付いた実験参加者の 11 人のうち、映像の前方への連続的移動と非連続的移動の両方に気が付いたのは 1 人 (P20) であり、映像の連続的移動に気が付いた言及をしたのは 1 人、非連続的移動に気が付いたよう言及をしたのは 5 人であった。

残りの 4 人の内 3 人は、映像が前方に移動したことには気が付いたが、どの様に移動したのかはわからないと回答した。

> “(実験実施者：どういう感じで奥に行きましたか？) そんなに、気づいたら、みたいな。” (P14)

また、実験参加者の内 2 人 (P2, 20) は、映像が前方に移動した後に手前にも移動したと回答し、1 人 (P22) はそもそも手前 (後方) にのみ移動したと回答するなど、移動自体を認知したものの誤った認識をしていた。

6.1.3 ダイアログとルービックキューブの表示の関係性

移動の認知はしているものの正確な認識がされていないケースとして、HMD に表示される操作方法ダイアログとルービックキューブの位置関係変化について言及する実験参加者もあった。実際にはこれらは位置関係を保持したまま移動が行われていたために誤った認識ではあるものの、移動についての一定の認知を示していた例と言える。これらの位置関係の変化についての言及は実験参加者のうち 5 人が行っていた。

> “キューブは、変わらずで、説明文だけこう、前後したのかなと思いました。” (P22)

6.1.4 移動認知の方法や難易度

タスク中に移動や異変に気が付いた実験参加者のうち 3 人は見える範囲の変化に言及した。これらも移動の認知はしているものの正確な認識がされていないケースと言える。

> “でも結構明らかに瞬間的に変わったので、その視界、自分が見える範囲から見える、何、情報が増えたので、はい、そう思いました。” (P11)

6.1.5 映像の見た目の変化

移動の認識についての直接的な言及ではないののの HMD に表示されるコンテンツの見た目の変化に言及した回答が多くあった。実験参加者のうち 11 人が、少なくとも 1 回以上映像の見える範囲について言及した：

> “あいや、さっきよりもちょっと近くなって、これが見づらくなっている要因というか、さっきより近くなって見づらくなり、見づらくっていうか、全体が見えなくなりました。” (P9)

また、攻撃による異変には気付いていたにもかかわらず、そのとき映像の表示位置は変わっていないと思っている発言した実験参加者が二人 (P5, 15) いた：

6.1.6 移動による意識の分散

映像移動が自身のタスクに影響したことを言及するケースが複数あった。実験参加者 P17 は、映像移動によって一時的にタスクに対する意識が分散したことを言及した：

> “は、そうですね、移動した瞬間は気になりました。一回ルービックキューブを回す手が止まるぐらいには気になりました。”
>
> “一瞬、そうですね、奥の文字に目を向けたので、まあ 1, 2 秒だったかなと思います。” (P17)

また、少し不安を感じたものの、タスク実施前に攻撃を行うことを聞いていたためあまり気にしなかったと発言した実験参加者 (P4) もいた：

> “あ、パって動いたので、「あ、私、今なにかしたかな」ってちょっと不安にはなりました。でもあとは、まあでも動くって言ってたしなって思ったので、はい。(P4)

6.2 タスクに対する意識

タスクへの集中が移動の認識に関わることも考えられるため、実験参加者がタスク実施における意識に関する言及があった場合にはその意識についての詳細をさらに質問するなどを行った。集中している等の言及をした実験参加者が 4 人、失敗への不安当の言及をした実験参加者は 4 人いた。

> “なんか、前に移動してることに全く私気づかなかったと思います、なんか、こっちに一生懸命になりすぎて、多分、そうですね、なんか、そうですね、一生懸命になっちゃってたんで、そんなに気づかなかったです、はい。” (P13)

6.3 支援用アプリケーションの完成度

インタビュー中、支援用アプリケーションへの違和感やストレスについて 10 人の実験参加者から言及があった。それらの違和感やストレスの原因として多くを占めたのは映像全体が初期位置だと欠けることとアプリケーションの誤作動であった：

7. 考察

7.1 攻撃による影響と実験参加者の行動 (RQ1)

7.1.1 攻撃を認知した際の影響

移動を認識した際に一時的にタスクが止まった実験参加者がいたことや不安を感じた実験参加者がいたことから、攻撃による影響として一時的な作業の中断や不安の誘発がある可能性が示された。今回の実験環境では作業の中断はタスクの成否に大きな影響を与えないが、AR/MR 適用先には航空や外科手術利用など短時間の作業中断が大きなリスクとなるケースが多く存在するため、作業の中断を誘発させる可能性が示されたことは重要であると考える。

また、タスク実施前に映像の移動があることが伝えられていたことから、移動を認識した実験参加者で移動を気に留めなかった参加者の中には実験であるという認識が働いたために中断や不安の想起がなかった可能性がある。

7.1.2 攻撃を認知しなかった際の影響

実験参加者の全員が完遂までタスクに取り組んだことから、全員が映像移動攻撃後も映像を見続けており、視線が攻撃によって移動させられたと考えることができる。

実験参加者は物理的なキューブ本体と HMD 上のキューブを交互に見比べながら操作をしているケースが多く、視線が物理オブジェクトとデジタルオブジェクトの交互に動き、視線移動も多く起きる利用環境であった。

操作支援や訓練用途など透過型の HMD を利用する主な環境においてはそういった視線移動が多いケースが一般的であることが予想される。透過型の HMD が利用される環境全般においては映像移動攻撃によりユーザ操作される可能性を示す結果であると言えよう。

7.2 攻撃への気づき (RQ2)

7.2.1 攻撃の気づかれにくさ

映像が前方への連続的移動を行ったことに気付いた実験参加者が 2 人であったことから、連続的移動を行う映像移動攻撃はユーザに認知されず実行することができる可能性の高さが示された。

また、非連続的移動の方が連続的移動よりも多くの実験参加者 (5/22 人) に気が付かれたことから、映像移動攻撃としては非連続的移動の方が気が付かれやすい可能性も考えられる。

7.2.2 映像の内容による気が付きやすさの違い

HMD 上のダイアログ表示位置が移動したと気が付いたにもかかわらず、HMD 上のキューブ表示位置が移動したとは考えていなかった、あるいは認識していなかった実験参加者がいた。操作方法等のダイアログとキューブの違いは、頻繁に視線が向かう操作主体のキューブと、タスクが進むにつれ操作に慣れ視線が向かわなくなるダイアログ、という視線の頻度差がある。さらに本研究で用いたアプリケーションでは、ダイアログ等は 3D 空間上の 2D オブジェクト、キューブが 3D オブジェクトという違いと、キューブが多色使いである一方でダイアログ等はグレースケールの表示であることの違いがある。こういった違いが移動の気付きに与える影響も予想される。

7.2.3 見える範囲の変化による気づき

見える範囲の変化による気づきが多かったが、Magic Leap1 より広い視野角を提供する HMD を用いた場合や映像の初期位置が遠い場合、見える範囲に変化が現れず、 気付きが発生しない可能性が考えられる。

7.2.4 映像の変化には気が付いても移動には気が付かない

：実験参加者の 2 人が、映像の変化には気が付いていたものの表示位置の変化には気が付いていなかった。このことから映像移動攻撃を受けた際、ユーザは異変を感じたとしても映像が移動したことを必ず認知できるとは限らないことが示唆される。

7.3 ユーザ実験

7.3.1 タスクに対する意識

インタビューでルービックキューブを揃えることに集中していたり失敗したくないなどの発言をし、映像移動攻撃に気が付かなかった実験参加者が 6 人いたことから、タスクの難易度や特性が異なれば、違う結果となった可能性が考えられる。

7.3.2 支援用アプリケーションの完成度

支援用アプリケーションへの具体的な違和感やストレスについて発言しなかった実験参加者が 22 人中 12 人いたことから、作成したルービックキューブの支援用アプリケーションの完成度は一定以上であると考えられる。

7.4 対策の検討

本稿では主に光学的透過型 HMD に対する映像移動攻撃の可能性を示したが、攻撃の検知手法や防御策についても議論を行う必要がある。大きく分けて、OS レベルとアプリケーションレベルの両方におけるアプローチがあるだろう。OS レベルでは情報の入力部分や処理部分に対するアプローチを、アプリケーションレベルでは情報の表示部分に対するアプローチをとることが考えられる。

8. 本研究における制約

本研究で行った実験には、いくつかの制約がある。ここではその制約を挙げ、それらが結果に与える影響や結果が示すものの範囲を議論する。

ユーザ実験で募集されたのは著者らが所属する大学の学生であった。情報系やコンピュータサイエンス系より広い募集ではあったものの、理系学生という偏りがある。それ

らが結果に及ぼす影響の議論は困難であるが、新たな技術の進取性が高い影響が考えられる。

実験の目的説明といった事前の説明において研究の目的が映像移動攻撃にあることと、実験において HMD 上の映像が移動することは通知済みであったために、結果に影響を与える可能性がある。本来の目的を伝えずにユーザ実験を行う Deception Study を採用することも考えられるが、倫理的な問題が指摘されていることに加え、Deception Study の有無による結果の違いに疑問符を投げる研究結果もあることなどから本研究では採用しなかった。

ユーザ実験に用いた HMD は光学的透過型 HMD であったが、物理的な環境をそのまま視覚に届けるといった利点がある一方で画角が狭く表示域の限定性よりオブジェクトが欠けることがあり、その画角が実験の結果に影響する可能性がある。近年では、Meta 社の Quest 3 や Apple 社の Vision Pro など、光学的な透過ディスプレイを持たないが外部向けの高精細な RGB カメラを複数搭載することで映像として透過機能を提供する映像透過型 HMD が広まっている。これらの画角は光学的透過型 HMD より広いことに加え、没入環境を利用することでユーザが実際に感じる画角は 360 度にわたるなどユーザがオブジェクトの欠損を感じることがない。こういった画角の差による影響も今後の研究課題となるだろう。

本研究で評価した映像移動は、前方移動に限定されていた。4.2.1 で示したように、映像の移動を考えた場合、6 方向の移動に加え 3 種の回転といった軸が考えられる。これらそれぞれの軸が移動の認識に与える影響とその比較や、組み合わせた効果なども議論されるべきであろう。

9. おわりに

本研究では、光学的透過型 MR HMD における映像移動攻撃がユーザに与える影響とリスクを評価した。ユーザ実験の結果、映像が前方に移動する連続的な攻撃は多くのユーザに気づかれにくいことが判明した。このことは、AR/MR 環境においてユーザが知らぬ間に視線や注意を操作される可能性があることを示唆しており、特に作業支援やセキュリティが求められる場面では重大なリスクとなり得る。

謝辞 本研究は、JST、CREST、JPMJCR22M4 の支援を受けたものである

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, 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] Slocum, C., et al.: Going through the motions: AR/VR keylogging from user head motions, USENIX Security ' 23, 2023
[8] Arafat, A. A., et al.: VR-Spy: A Side-Channel Attack on Virtual Key-Logging in VR Headsets, IEEE VR 2021, 2021
[9] Meteriz-Yıldıran, C., et al.: A Keylogging Inference Attack on Air-Tapping Keyboards in Virtual Environments, IEEE VR 2022, 2022
[10] Zhang, Y., et al.: It' s all in your head(set): Side-channel attacks on AR/VR systems, USENIX Security ' 23, 2023
[11] Luo,S., et al.:Eavesdropping on Controller Acoustic Emanation for Keystroke Inference Attack in Virtual Reality, NDSS 2024, 2024
[12] Nguyen, A., et al.: Penetration Vision through Virtual Reality Headsets: Identifying 360-degree Videos from Head Movements, USENIX Security ' 24, 2024
[13] Nair, V., et al.: Unique Identification of 50,000+ Virtual Reality Users from Head & Hand Motion Data, USENIX Security ' 23, 2023
[14] Zhu, H., et al.: Sound-Lock: A Novel User Authentication Scheme for VR Devices Using Auditory-Pupillary Response, NDSS 2023,, 2023
[15] Tseng, W-J.,et al.: The Dark Side of Perceptual Manipulations in Virtual Reality, ACM CHI '22, 2022
[16] Cheng, K., et al.: Exploring User Reactions and Mental Models Towards Perceptual Manipulation Attacks in Mixed Reality, USENIX Security ' 23, 2023
[17] 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).
[18] Su, Z., et al.:Remote Keylogging Attacks in Multi-user VR Applications. USENIX Security ' 24, 2024
[19] Slocum, C., et al.:That Doesn't Go There: Attacks on Shared State in Multi-User Augmented Reality Applications. USENIX Security ' 24, 2024
[20] Windl, M., et al.: Investigating Security Indicators for Hyperlinking Within the Metaverse, SOUPS 2023, 2023
[21] 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
[22] Abhinaya S.B., et al.: Enabling Developers, Protecting Users: Investigating Harassment and Safety in VR, USENIX Security ' 24, 2024
[23] Abhinaya, S.B., et al.:Enabling Developers, Protecting Users: Investigating Harassment and Safety in VR. USENIX Security ' 24, 2024
[24] 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).
[25] 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).
[26] Fleiss, J.L., et al.: Statistical methods for rates and proportions. John Wiley & Sons, 2013.