VR/ARにおける認知的リスクの可視化：セキュリティ意識向上のためのデモンストレーション

金岡 晃[1,a)]　手老 陽南[1]　大塚 航世[1]　藤田 真由[1]　倉﨑 翔大[1]

概要：本研究では、VR/AR 技術に特有のセキュリティリスクを体験的に理解できるデモンストレーションを開発した。ネットワーク構築業務を支援する AR アプリをモデルとし、視覚干渉オブジェクトや聴覚干渉オブジェクト、不正なオブジェクトの偽装による攻撃を再現した。さらに、攻撃発生時に解説モードへ切り替える仕組みを導入し、ユーザに攻撃の詳細や影響を直感的に伝える設計とした。

1. はじめに

近年、Virtual Reality（VR）および Augmented Reality（AR）技術の発展は著しく、エンターテインメント分野を超えて、産業用途にも広がりを見せている。特に、医療、製造、航空、宇宙、設計、軍事における支援用途や訓練用途など、多岐にわたる分野での利用が進んでおり、日常業務や重要なワークフローに組み込まれる事例も増加している。

しかしながら、VR/AR 技術の普及に伴うセキュリティリスクについては、十分に認識されているとは言い難い。これらのリスクに関する認識と技術の導入の間には大きなギャップが存在しており、産業界や学術界においても、その解消が急務となっている。このギャップを埋めるため、近年では VR/AR に特化したリスクの特定や分析に取り組む学術研究が進みつつあり、徐々に活発な研究領域として注目を集めている。

VR/AR セキュリティは、VR/AR が高い没入感や実在性を提供することにより従来のコンピューティング環境と異なるユーザ認知特性を与えることもあり、ハードウェア、ソフトウェア、ユーザの認知特性という複数の要素の交点に位置する点で特徴的である。そのため、セキュリティ分野に限らず、VR/AR 分野、HCI 分野、さらには認知科学の分野の研究者と技術者にも理解が広がる必要がある。しかし、現時点では多くの VR/AR リスクが現実的な問題として受け入れられていないのが現状である。

本研究では、関連分野の研究者や技術者、さらには一般のユーザを対象に、VR/AR 技術のセキュリティリスクを具体的に示すデモンストレーションを開発した。デモでは、VR/AR 環境特有のリスクが顕在化する具体的なシーンを想定し、これを再現するためのデモアプリケーションを開発した。

本デモのアプリケーションとして、ネットワーク構築業務を顧客先環境で行う際に、非熟練作業者が効率的かつミスなく作業を進められるよう支援する AR アプリ（以下、作業支援アプリ）をモデルとした。このアプリは、現実世界の物理環境と重ね合わせて作業手順を提示したり、接続状況を視覚化することで、作業の円滑化を目指すものである。

デモ内ではこの作業支援アプリが悪意のある第 3 者によって既に侵入され、攻撃用スクリプトが混入されているというシナリオを設定した。ユーザが作業支援アプリの支援を受けつつネットワーク構築業務を進める中で複数の攻撃が実行される。具体的には、「視覚干渉オブジェクトの不正挿入」「聴覚干渉オブジェクトの不正挿入」「オブジェクトの偽装」の 3 種類の攻撃シナリオが含まれている。

本デモでは、作業支援アプリに攻撃が実行されるたびに、作業支援アプリでの通常作業を中断し、「デモとしてのリスク・攻撃解説モード」に移行する仕組みを採用している。この解説モードでは、攻撃の内容やリスクの詳細をわかりやすく伝えることを目的としており、ユーザが攻撃の影響を客観的に振り返ることができる。また、解説モードへの移行時には、視覚的および体験的な工夫を施している。具体的には、周囲を暗くすることで没入感を高めるとともに、フォントや UI デザインを通常の作業支援アプリとは異なるものに変更することで、ユーザが直感的に「解説モードに切り替わった」と認識できるようにしている。

これらの攻撃をデモ内で実際に体験することにより、VR/AR 環境におけるリスクを直感的に理解し、その重要

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

性を認識してもらうことを目指す。

2. 関連研究

2.1 VR/AR セキュリティ

VR/AR に関するセキュリティやプライバシ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]．代表的な成果として、AR グラスにおけるプライバシに焦点を置いた研究がされてきた [3], [4], [5]。

既存のコンピューティング環境の脅威の存在を VR/AR 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]、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。

一方、VR/AR 特有の研究は、ユーザの知覚操作 [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] 、オブジェクトの偽装攻撃 [26] 、VR 空間におけるハラスメント [27], [28] などとともに、全般的なサーベイや課題の分類 [29], [30] 、専門家によるユーザ認識検討 [31] などがある。また、VR/AR に対するセキュリティだけではなく、VR/AR デバイスを用いた既存セキュリティ事象への対応手法も検討がされている [32]。しかし全体を見ると既存のコンピューティング環境と同等のリスクや脅威を分析する研究が多くを占めており、VR/AR 特有のセキュリティやプライバシの研究はまだ充実しているとは言い難い。

2.2 VR/AR リスクの体系的整理

前節で示した通り、VR/AR のセキュリティに関する議論は始まりつつあるものの、脅威や攻撃対象領域についての体系的な分析はまだ十分に行われていなかった。 金岡らは、この課題を解決するために、VR/AR 環境におけるセキュリティ脅威を体系的に整理した。そしてその分析を基に、VR/AR 技術に固有の攻撃対象領域を分類し、潜在的な攻撃の攻撃対象領域を明確化させた。さらに、これらを実現する攻撃者のモデルを構築し、その能力および手法を体系的に検討した [33]。本研究ではこれらで示された脅威と攻撃者モデルの一部を利用し、デモのシナリオを構成した。

3. VR/AR デモアプリ開発の目的と要件

3.1 目的

本研究の目的は、VR/AR 技術におけるセキュリティリスクを具体的に示し、その重要性を広く認識してもらうことである。この目的を達成するため、セキュリティ分野のみならず、VR/AR 分野や HCI 分野、さらには認知科学分野の研究者や技術者、そして一般のユーザを対象にしたアプローチが必要である。特に、産業用途における利用が増加する中で、これらのリスクを正確に理解し、予防策を講じるための認識を深めることが重要となる。

3.2 要件

この目的を達成するために、デモアプリケーションには以下の要件が求められる。

(1) VR/AR 環境特有のリスクが顕在化する具体的なシーンを示すこと
- 実際の産業用途を想定した環境で、視覚干渉、聴覚干渉、オブジェクト偽装といった攻撃がどのように発生し、ユーザに影響を与えるかを再現

(2) ユーザが体験できるインタラクティブな設計であること
- 単なる説明にとどまらず、ユーザが攻撃を体感できる仕組みを持つことにより、リスクの理解が深まり、実際の脅威を直感的に認識可能

4. VR/AR セキュリティリスクデモアプリの設計

前章で示した要件を満たすため、本研究ではネットワーク構築業務を支援する「作業支援アプリ」をモデルにしたデモアプリケーションを設計・開発した。このアプリケーションは、非熟練作業者が効率的に作業を進められるよう支援する一方で、悪意のある第 3 者による侵入を受けた状況を想定している。具体的には、視覚や聴覚を悪用した攻撃が作業環境でどのように影響を及ぼすかを再現し、ユーザがその影響を実際に体験できるように設計されている。

さらに、作業中に攻撃が発生すると、通常の作業支援アプリから「デモとしてのリスク・攻撃解説モード」へと移行する。この解説モードでは、周囲を暗くし没入感を高めるとともに、フォントや UI デザインを変更することで、通常の作業支援環境とは異なる体験を提供するよう工夫している。このように、ユーザが単に攻撃を受けるだけでなく、その内容と影響を詳細に理解できる仕組みを備えたインタラクティブなデモとする。

4.1 作業支援アプリモード

本デモの作業支援アプリは、ネットワーク構築業務を支援する AR アプリケーションとして設計した。産業用途での実用性を意識し、作業者が自然に操作を行えるよう、操作方法としてハンドジェスチャを採用した。これにより、物理的なコントローラを必要とせず、作業環境に適応した直感的なインターフェースを提供する。

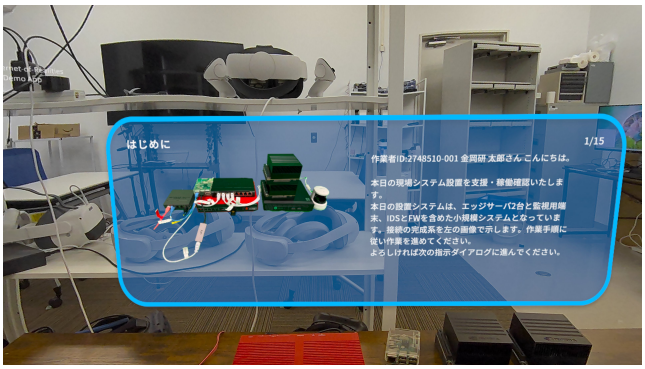

図 1: 作業支援アプリの表示例：作業内容指示

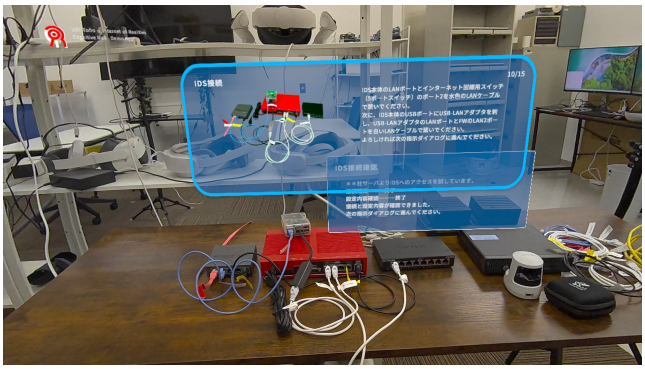

図 2: 作業支援アプリの表示例：機器接続確認

作業支援アプリでは、複数の作業手順を順にダイアログとして表示する仕組みを備えている（図 1）。作業者は画面に表示された手順を確認しながら、作業を進めることができるよう設計されている。また、作業内容に加えて、対象デバイスや接続ケーブルの情報を写真付きで表示することで、視覚的な理解を補助する。これにより、非熟練作業者であっても誤操作を減らし、作業効率を高めることが期待される。

さらに、いくつかの機器においては、接続後に企業側のネットワークシステムが自動的に接続確認を行う機能も組み込まれている（図 2）。この機能は、接続状態の適正さをリアルタイムに評価し、作業者に対してその結果をフィードバックする役割を果たす。これにより、作業者が迅速かつ正確に次の作業に移行できるよう支援する。

4.2 攻撃の発生

デモ内ではこの作業支援アプリが悪意のある第 3 者によって既に侵入され、攻撃用スクリプトが混入されているというシナリオを設定した。ユーザがネットワーク構築業務を進める中で攻撃用スクリプトが動き、複数の攻撃が実行される。

具体的には、以下の 3 種類の攻撃シナリオが含まれている。1 つ目は、「視覚干渉オブジェクトの不正挿入」である（図 3）。攻撃者により、視界内に不正なオブジェクトが挿入され、ユーザの視線が意図的に誘導されたり、作業が中

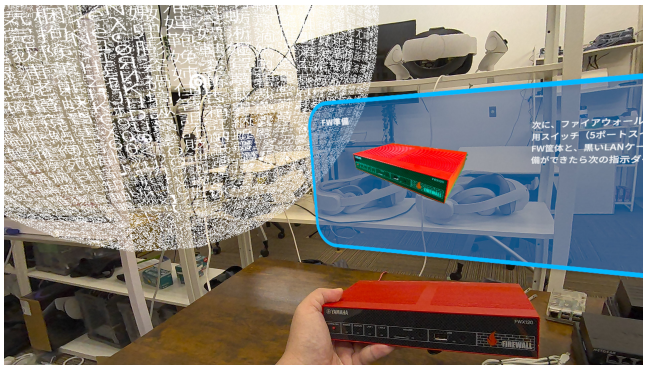

図 3: 攻撃シナリオ 1：視覚干渉オブジェクトの不正挿入（アプリ UI と独立しているケース）

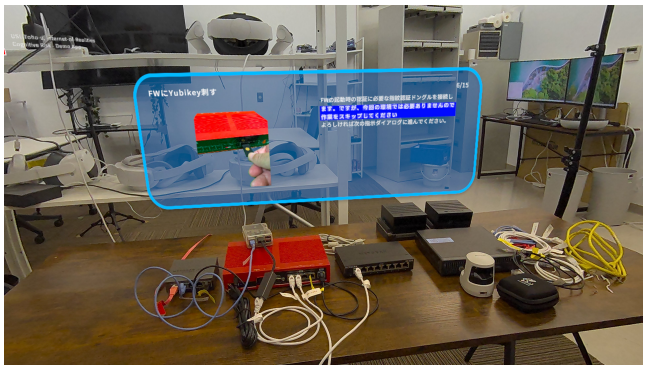

図 4: 攻撃シナリオ 3：オブジェクトの偽装

断される状況が再現される。こちらはさらに攻撃状況下でフォアグラウンドで動作しているアプリに UI が類似している（文脈に沿っている）か、独立している（文脈に沿っていない）かにより 2 つの攻撃が行われる。図 3 は、不正挿入オブジェくとしてアプリ UI の文脈には沿っていない形で文字が多数記載された球体オブジェクトがユーザ視界の左側に表示された攻撃を示している。これによりユーザの視界誘導や作業中断を引き起こす。

2 つ目は、「聴覚干渉オブジェクトの不正挿入」である。特定の方向から意図的に挿入された音声刺激により、ユーザの注意が逸れ、作業効率や正確性が損なわれる。

3 つ目は、「オブジェクトの偽装」による攻撃である。本来の作業対象物の外見が不正に変更され、ユーザが誤った操作を行うよう誘導される。図 4 では、作業指示パネルの文章に重なるように偽装パネルが配置されており、本来の指示とは異なる指示文章が記載されている。

4.3 デモとしてのリスク・攻撃解説モード

本デモでは、作業支援アプリを利用した業務中に発生するリスクを体験した直後に、専用の「リスク・攻撃解説モード」に移行する設計を採用している。このモードを導入することで、攻撃がどのように発生し、作業にどのような影響を与えたかを詳細に解説することが可能となり、ユーザがリスクの本質を深く理解できることを狙いとしている。

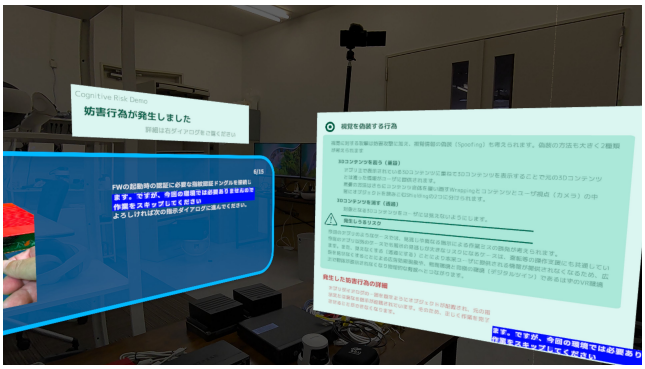

図 5: リスク・攻撃解説モードの表示例：オブジェクト偽装後の解説

リスク・攻撃解説モードでは、通常の作業支援アプリとは異なる UI デザインを採用しており、作業支援アプリの一部ではないことをユーザに直感的に認識させる工夫が施されている（図 5）。具体的には、周囲を暗くすることで没入感を高め、フォントや UI デザインを変更することで視覚的な切り替えを明確化している。このデザイン変更により、ユーザは通常の作業環境から一歩離れた客観的な視点を持つことが可能となる。

さらに、このモードでは、発生したリスクの具体的な内容や、その背後にある攻撃手法をユーザに伝えることを重視している。視覚的な強調やアニメーションを用い、攻撃の影響を分かりやすく示す設計となっている。これにより、ユーザ体験をより深く、かつ学習効果の高いものにすることを目指している。

5. 知覚操作攻撃デモの開発

5.1 デバイスとアプリケーションの選定

本デモは、現時点で最もポピュラーなデバイスの一つであり、ビデオパススルー機能を備えた Meta Quest 3 を使用して実現した。このデバイスのビデオパススルー機能を活用することで、現実世界の映像を背景に重ねて AR アプリケーションを動作させる構成を採用している（図 6）。

5.2 作業支援アプリの UI 設計

作業支援アプリのユーザインタフェース（UI）は、VR/AR でよく見られる半透明なパネルとエッジのあるデザインを採用した。作業手順が表示されるパネルには、対象デバイスやケーブルの写真を添えることで、視覚的な補助を提供し、作業者が情報を直感的に把握できるよう工夫している。

5.3 リスク・攻撃解説モードの UI 変更

リスク・攻撃解説モードでは、作業支援アプリの通常の UI から切り替わることを視覚的に明確化するため、フォントや色使いを変更した。また、実際に攻撃に使用されたオブジェクトを小さく表示することで、攻撃部分を強調

図 6: デモアプリケーションをインストールした Meta Quest 3 を装着し作業支援を受けつつネットワーク構築作業を実施

(a) 作業支援アプリの通常 UI

(b) リスク・攻撃解説モードへの変更後 UI

図 7: 攻撃発生後の作業支援アプリからリスク・攻撃解説モードへの移行

し、ユーザがその影響範囲を直感的に理解できるようにした。図 7 は、モード切替前の作業支援アプリの通常 UI からリスク・攻撃解説モードの UI に切り替わった前後のスクリーンショット画像を示している。

5.4 操作インタラクションの設計

本アプリでは、作業者が実際に機器の接続や設定作業を行う際、物理的なコントローラを用いず、自然なハンドジェスチャを使用する設計を採用した。具体的には、人差し指と親指を 1 秒以上つまむジェスチャー（Pinch Gesture）を操作トリガーとして利用した。このジェスチャーは、Meta Quest 3 のハンドトラッキング機能を活用することで、直

感的な操作感を実現している。

6. 議論

本研究では、VR/AR 環境におけるセキュリティリスクを体験的に理解できるデモアプリケーションを開発し、攻撃がどのようにユーザ体験に影響を与えるかを提示した。本デモは、特に視覚や聴覚を悪用した攻撃が作業環境に与える影響を直感的に認識できるよう設計されている。しかしながら、デモの目的がリスクの認知向上に重点を置いているため、現実の攻撃に比べ、攻撃がユーザに気付かれやすい形で提示されている。この点は、本デモが持つ限界の 1 つと考えられる。

実際の攻撃は、本デモで示したものよりもさらに巧妙で、ユーザに気付かれにくい形で実行される可能性が高い。そのため、次のバージョンのデモでは、気付かれにくい攻撃を再現するモードを搭載することが課題の 1 つである。また、こうしたモードを通じて、リスクの「潜在性」や「検知の困難さ」を強調し、ユーザにより現実的な脅威を認識させることが期待される。

さらに、現行のデモでは、VR/AR 技術に特有のリスクに焦点を当てているが、従来のコンピューティング環境でも生じうる一般的なリスクをデモに導入することも重要である。これにより、VR/AR 環境と従来環境のリスクの共通点と相違点を明確にし、セキュリティ対策の全体像を示すことが可能となる。こうした幅広いリスクの表現が、セキュリティに対する包括的な認識の向上につながると考えられる。

最後に、防御策を視覚化したデモンストレーションも今後の課題として挙げられる。本デモでは、リスクを体験的に認識させることを目的としているが、攻撃をどのように検知し、無効化できるのかを示す防御策のデモは、技術的・教育的な側面で大きな意義を持つ。このような防御策の導入により、リスク認識から具体的な解決策へと視点を広げ、セキュリティ対策の実装に向けた議論をさらに深めることが期待される。

7. まとめ

本研究では、VR/AR 環境特有のセキュリティリスクを可視化し、ユーザが体験的に理解できるデモアプリを開発した。今後は、気付かれにくい攻撃や防御策を取り入れたデモの実装に加え、一般的なリスクも表現可能な包括的なデモへと発展させることで、セキュリティ意識のさらなる向上を目指す。

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] 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 In-

terface: 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] Fujita, M., Kurasaki, S., & Kanaoka, A. (2023, November). Securing Cross Reality: Unraveling the Risks of 3D Object Disguise on Head Mount Display. In Proceedings of the 13th International Conference on the Internet of Things (pp. 281-286).
[27] Abhinaya S.B., et al.: Enabling Developers, Protecting Users: Investigating Harassment and Safety in VR, USENIX Security ’ 24, 2024.
[28] Abhinaya, S.B., et al.:Enabling Developers, Protecting Users: Investigating Harassment and Safety in VR. USENIX Security ’ 24, 2024.
[29] 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).
[30] 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).
[31] Deldari, E., et al.: An Investigation of Teenager Experiences in Social Virtual Reality from Teenagers’ , Parents’ , and Bystanders’ Perspectives, SOUPS 2023, 2023
[32] Kanaoka, A., & Isohara, T. (2024, March). Enhancing Smishing Detection in AR Environments: Cross-Device Solutions for Seamless Reality. In 2024 IEEE Conference on Virtual Reality and 3D User Interfaces Abstracts and Workshops (VRW) (pp. 565-572). IEEE.
[33] 金岡晃、森亮太、大塚航世、倉﨑翔大、大木哲史、大東俊博、磯原隆将：VR/AR 環境におけるセキュリティ脅威と攻撃対象領域の体系的分析、2025 年暗号と情報セキュリティシンポジウム（SCIS2025）