Web3時代に向けたメタバース等の利活用における研究会

資料５－３

メタバースにおける サイバーセキュリティの 検討について

2022年12月2日

日本スマートフォンセキュリティ協会（JSSEC）
技術部会 部会長 兼 メタバースセキュリティWG 仲上竜太
（ニューリジェンセキュリティ株式会社）

メタバースにおけるサイバーセキュリティの検討について

アジェンダ

- JSSECのご紹介
- メタバースにおけるサイバーセキュリティの考え方
- 諸外国および国内における代表的な取り組み
- まとめ

※本資料に記載の内容は個人の見解に基づくものです。

JSSECのご紹介

日本スマートフォンセキュリティ協会

Japan Smartphone SECurity association / https://jssec.org/

「人との接点となるスマートフォンを中心に、新たな社会での更なるセキュリティの重要性について普及啓発すること」を目的に10年前に発足。現在、幹事企業14社、正会員51社のほか、特別会員、団体、オブザーバが参加し、利用部会／技術部会／パブリックリレーション部会／啓発事業部会の4つの部会が活動している。

JSSEC技術部会

部会長 兼 メタバースセキュリティWGリーダー
仲上竜太（ニューリジェンセキュリティ株式会社）

JSSEC技術部会では、5G時代のスマートフォンの新たな利活用方法として2018年よりVR/AR等XRコンテンツ開発におけるサイバーセキュリティの研究を開始。2022年10月にメタバースセキュリティWGを設立し、各団体と連携してメタバースにおけるサイバー脅威およびセキュリティ対策の研究を行っている。

2019年5G環境に向けたコンテンツトレンドセミナー開催
2022年セキュリティフォーラム2022オンラインメタバースセキュリティ講演
2022年JSSEC10周年記念イベント・キャリア3社によるパネルディスカッション開催
2022年Japan Security Summit 2022 メタバースセキュリティ講演

メタバースにおけるサイバーセキュリティの考え方

メタバースにおけるサイバーセキュリティを検討するにあたって生ずる「メタバース」の定義の問題

サイバーセキュリティは従来情報の「機密性」「完全性」「可用性」を担保する取り組みと定義されてきましたが、昨今では、デジタル技術の社会への浸透により、利用者のプライバシーの保護や人格・権利に対する保護も含む文脈となりつつあります。
あわせて「メタバース」は現在のところ明確な定義が存在せず、広義のサイバーセキュリティを検討する際の諸条件の整理として以下の構成要素を有するデジタル空間をメタバースとして設定します。

仮想空間表現

- 複数のユーザが同時に空間に存在できる
- 3Dオブジェクトを組み合わせた空間表現ができる
- アバターを通して干渉可能なオブジェクトが設定できる
- バーチャルリアリティによるアバター視点ができる

自己投射性・身体表現

- アバターによる見た目・外見のカスタマイズ
- モーショントラッキングによる頭・手足・腰などの動作の反映。仕草、ふるまいなど。
- 音声や加工音声による会話
- エモート（3D版絵文字や固定的な動き）

コミュニティ・社会基盤

- ユーザ同士のソーシャルなつながりの実現
- 空間へのアクセス制御
- 情報やメッセージのやり取り
- アイテムの所有・権利の保障
- 金銭もしくはトークンを介した取引の実現

これらの要素を部分的にも備えたデジタル空間をメタバースと設定

※3D仮想空間以外もメタバースとして認識する

メタバースにおけるサイバーセキュリティの考え方

デジタル技術の発展に伴って進化したメタバース上のコミュニケーション

テキストチャット
アバター

ボイスチャット
エモート

身体コミュニケーション
アバター視点

- **映像技術やデバイスの普及による空間表現の進化**
- **時代と共にコミュニケーションの手段や解像度が向上し没入度が増加**
- **VR技術によって現実の体験に大幅に近づいている**

“富士通Habitat” https://pr.fujitsu.com/jp/news/1997/Sep/habitat/habitat2_concept.html
“Fortnite” 2022, Epic Games, Inc. Epic、Epic Games
“バーチャル渋谷, cluster” https://cluster.mu/w/79347fb9-05f5-429e-ab5f-8951ee8cd966

メタバースにおけるサイバーセキュリティの考え方

メタバースを考える上で、人間の能力をもとに整理すると…

自分という人間
(アイデンティティ)

デジタル空間での
- 容姿・外見（アバター）
- 名前・呼び名
- 視覚・聴覚・皮膚感覚
- 表情や手足などの
  身振り・身体表現
- 声・話し方

センサーや装置で再現される
デジタル上の自分
（デジタルツイン）

メタバースにおけるサイバーセキュリティの考え方

現実の自分のアイデンティティと自分のデジタルツインが存在する空間＝メタバース

- メタバースごとに自分のアイデンティティとデジタルツインが存在
- メタバースごとに提供される機能・実現される内容・表現が異なる
- 現実の自分によってすべて結合されている

なぜメタバースにおけるサイバーセキュリティを考える必要があるのか？

メタバースに広がる活動領域

- 自分のデジタルツインを伴う豊かなコミュニケーション
- 空間での行動記録や交流記録、発言、視線、触れたものなどの記録
- 視界を覆うHMDやモーションセンサーなど物理身体とデジタルとの深い結合
- インターネットへの接続を前提としたサービス設計

現実空間においては記録・アクセスできなかった現象が
デジタル化によって悪用されるリスクが生じている

インターネットを通じて物理的身体へのアクセスが可能

メタバースにおけるサイバーセキュリティの考え方

JAPAN SMARTPHONE SECURITY ASSOCIATION

システムへの不正

- ウェブアプリケーションやクライアントアプリケーションの脆弱性を悪用したユーザへの情報窃取・不正行為
- 運営ネットワークを通じた、サーバへの侵入などのデータ侵害
- DDoSなどのサービスそのものへの攻撃
- 視界やVR機器への攻撃
- 身体フィードバックへの攻撃

ユーザへの不正

- プラバシーや個人特定
- ストーキング
- 人格のなりすまし
  - アバターの盗用
  - アバターの再現
  - Deepfakeによる声の模倣
- 盗聴・盗撮
- ハラスメント

システム的セキュリティとともに空間における治安維持の観点があります

メタバースにおけるサイバーセキュリティの考え方

VRソーシャルメタバースサービスを仮定した場合の、サービスに対する脅威分析の一例

STRIDE分類	メタバースにおける脅威例
Spoofing（なりすまし）	攻撃者が正規の利用者を装うなりすまし。認証情報の窃盗による、アバターモデルの悪用、Deepfakeによる音声の偽装。
Tampering（改ざん）	悪意を持ってデータを書き換える改ざん。ワールド(空間)データや表示アセット、ユーザプロファイルデータの改ざん。
Repudiation（否認）	サービス上での操作履歴などの隠滅により不正行為の証拠を無くし、攻撃者の特定をできなくする脅威。サービス内に保存されている行動履歴の改ざん、操作ログの改ざん、メッセージの改ざんなどによる否認など。
Information disclosure（情報漏洩）	秘匿すべき情報を窃取または暴露する情報漏洩。見えないアバターによる空間内の発言や行動の盗聴・盗撮。
Denial of Service （サービス拒否）	サービスを止めてしまい使えなくする攻撃。メタバースサービスそのものへの妨害やプレイヤーのパソコン・スマホやVR機器の破壊、無効化、表示妨害。
Elevation of Privilege（権限昇格）	管理者の権限を不正の奪い悪用する権限昇格。権限昇格は、一般のプレイヤーのアカウントを不正な方法によって管理者に昇格し、通常では使用できない管理機能の使用をプロフィール改ざんによる等により可能にする脅威。

メタバースにおけるサイバーセキュリティの考え方

アプリケーションサービスとしてのメタバースへの対応策は、オンラインゲームへのサイバーセキュリティ対策手法が有効。

①脆弱性診断によるアプリケーション脆弱性の対応
多くのメタバースプラットフォームサービスはウェブサービスまたはサーバ＋クライアントアプリケーションの形態で提供されており、アプリケーション脆弱性診断による未然防御対策が有効。
メタバースプラットフォームの多くがUnityなどのゲーム制作エンジンで開発されています。

②チート対策による正常系仕様を悪用した不正行為の抑制
実装上の脆弱性や正常系機能や仕様を悪用した不正課金や不正プレイを抑制する、チート対策による脅威分析と不正対策の実施。

③サービス運営によるゲーム内（メタバース内）コミュニティ維持
ゲーム空間内のもめごとやハラスメントに対する仲裁、判断などを実施するGM（ゲームマスター）と同様の機関によるコミュニティの健全性維持。
現状のメタバースサービスの多くではユーザ自身の判断によるブロック・報告により対処可能。

諸外国および国内における代表的な取り組み

メタバースにおけるアイデンティティ、プライバシー、サイバーセキュリティの調査検討については、
日本および諸外国において様々な取り組みが進められています。
ここでは、代表的な取り組みについて紹介します。

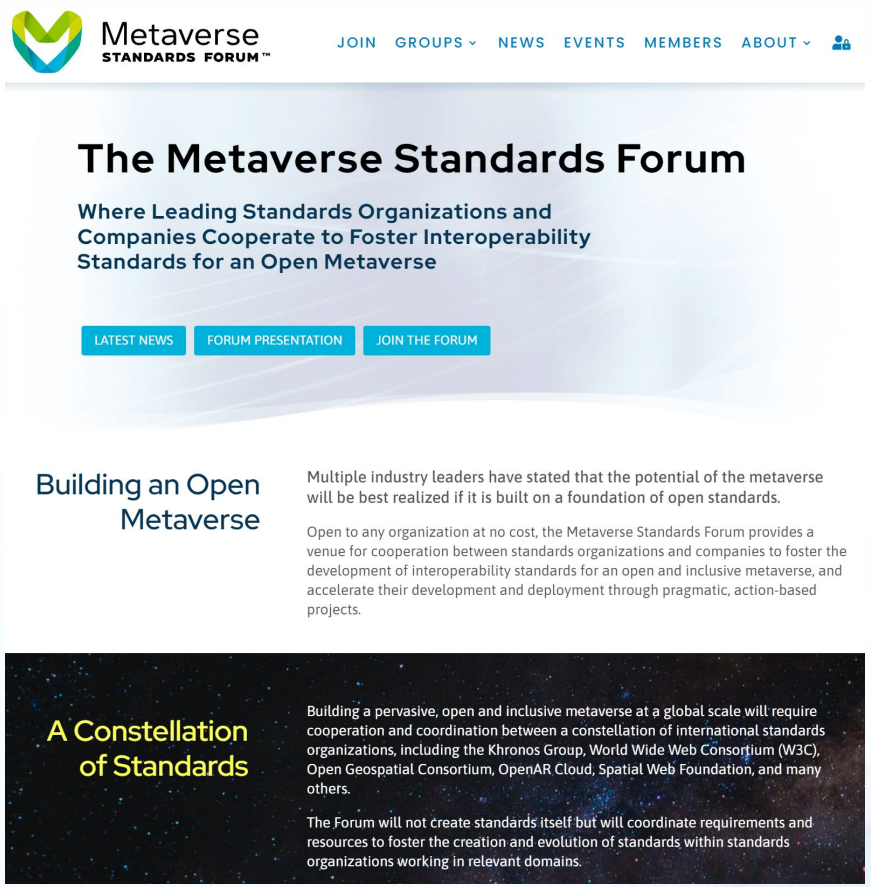
諸外国および国内における代表的な取り組み

The Metaverse Standards Forum

https://metaverse-standards.org/

Adobe, Autodesk, avataar, EPIC Games, Unity, Meta, nVidia, Qualcomm, SIE, Huawei,W3C, Web3d Consortiumなど37団体が中心となり2022年6月に設立。現在2000団体が加盟。
3D技術、アセット管理、アバター互換性、デジタルファッション、現実世界との統合などメタバースに関する技術と仕様のオープンな標準化を進める。
プライバシー、セキュリティ、アイデンティティに関する取り組みも行われている。

“Recommendations for responsible innovation that mitigates human and societal harm from objective and subjective privacy risks – including cybersecurity and identity risk management”



諸外国および国内における代表的な取り組み

XR Security Initiatives (SanFrancisco,USA)

https://xrsi.org/

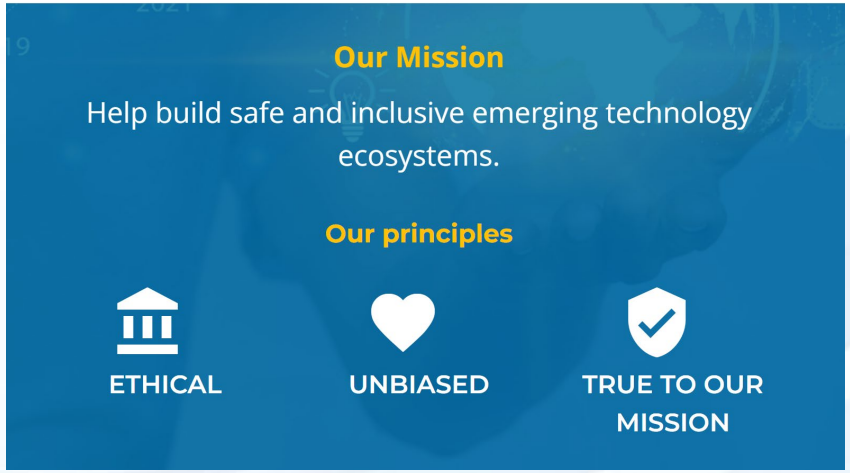
XR Safety Initiative（XRSI）は、没入型環境におけるプライバシー、安全、セキュリティ、倫理を促進するグローバルな非営利の標準化団体（SDO）。没入型技術や新興技術に深い関心を持ち、受賞歴のあるサイバーセキュリティの専門家である「サイバーガーディアン」と呼ばれるKavya Pearlmanによって2019年に設立された。
サンフランシスコのベイエリアに本社を置くXRSIには、現在、世界中から150人以上の多様で学際的なアドバイザーが集まっている。

12月10日～15日にMETAVERSE SAFETY WEEKが開催される。

XR Safety Initiative (XRSI) is a global non profit Standards Developing Organization(SDO) that promotes privacy, safety, security, and ethics in immersive environments.

Founded in 2019 by Kavya Pearlman, known as the "Cyber Guardian," an award-winning cybersecurity professional with a deep interest in immersive and emerging technologies.

Headquartered in San Francisco Bay Area, XRSI currently has over 150 diverse and multidisciplinary advisors from around the globe.



バーチャルシティコンソーシアム

http://shibuya5g.org/research/

渋谷区公認の配信プラットフォーム「バーチャル渋谷」の運営に基づくさまざまな知見をもとに、今後の他都市での類似モデル展開や新規ビジネス・技術開発など、日本発メタバースの発展に向けて、オープンに議論・調査研究を行い、ガイドラインの策定や情報発信することを目的とした組織です。

発起企業：KDDI株式会社、東急株式会社、みずほリサーチ&テクノロジーズ株式会社、一般社団法人渋谷未来デザイン

「バーチャルシティガイドライン ver.1.5」(2022年11月)

都市連動型メタバースにおける諸課題について権利関係、個人情報、電気通信事業法、独禁法、各種事業法の整理と準拠を記載。

9.個人情報の取り扱い

(1)ユーザーデータの収集と所有（個人情報の管理）

“メタバースの仮想環境内においては、実社会と異なり、プラットフォーマーはユーザーのあらゆる活動に関する情報が取得しうる立場となるため、ユーザーの個人特定につながる粒度の細かい（さらには個人の経歴や内面に係るセンシティブな）情報を取得することができる可能性が高いと考えられる。”

一般社団法人日本デジタル空間経済連盟

https://jdsef.or.jp/

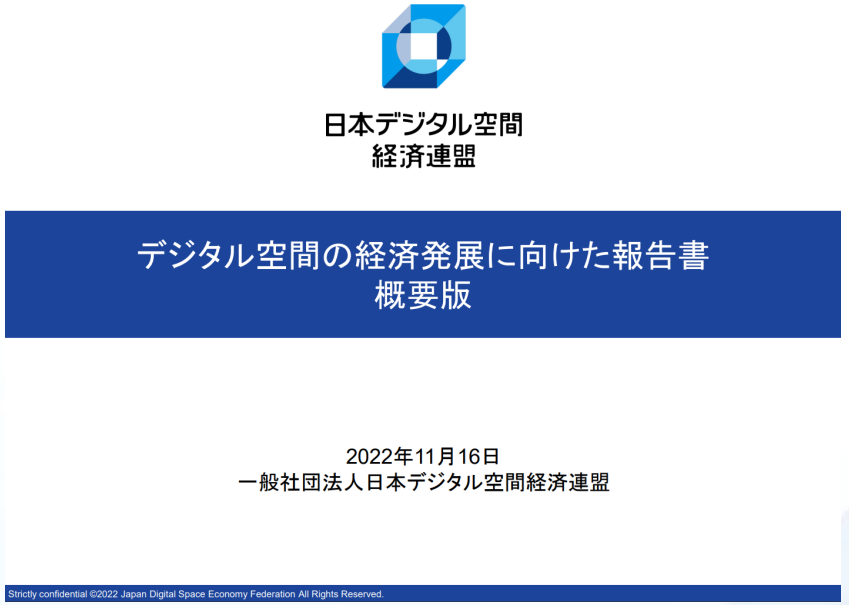
業界横断の総合経済団体として、デジタル空間における経済活動を活性化し、日本経済の健全な発展と豊かな国民生活の実現に寄与することを目的に、デジタル空間の経済発展が日本の経済発展に資するよう、政策提言や情報発信、様々な関係団体との対話等を行う団体として、2022年4月にSBIホールディングスが設立。

デジタル空間の経済発展に向けた報告書(2022年11月)

デジタル空間を活用した事業推進にあたり現在の課題や今後顕在化するであろう課題について弁護士、公認会計士、大学教授等の専門家と議論を行いその対応方針をまとめたもの。

知的財産、デジタル金融、プラットフォームの3カテゴリによって構成され、情報セキュリティについては①デジタル空間における個人情報の取り扱い、② デジタル空間を前提としないビジネスとの情報セキュリティに関する違い/差分の有無について言及。

検討の方向性が示されています。



諸外国および国内における代表的な取り組み

一般社団法人メタバース推進協議会

https://jmpc.jp/

メタバース空間内での生活文化・コミュニティの形成、ビジネスの普及・促進のためのルールメイク(ガイドライン整備、ルールメイキング戦略、標準化)を目的として2022年3月に設立。

現実社会連動メタバースガイドラインにおけるセキュリティガイドラインの策定(2022年11月)

メタバース推進協議会セキュリティ分科会（セキュリティ分科会(セキュアIoTプラットホーム協議会・日本音楽事業者協会・片岡法律事務所と共同)で作成。
11月に骨子を発表し、現在有識者による検討を進めている。

セキュリティガイドライン

■ ガイドライン策定にあたり、「現実社会連動メタバース」の存在意義や考え方の方針を基に、特にセキュリティ領域においては以下を宣言する。※セキュリティ分科会(セキュアIotプラットホーム協議会様・日本音楽事業者協会様・片岡法律事務所様)と共同で作成

宣言		必要なアクションプラン/対応		
		ルール	運用	技術
社会的観点	➢ 仮想世界を現実世界と同様に過ごすようになる環境整備 例）長時間利用における心身の健康リスク ➢ 公共性/匿名性のアバターや空間の在り方 例）公共性が高く直接的影響力のある政治、芸能、医療などにおけるなりすましなどのリスク	・メタバース運用事業者に対するセキュリティポリシーの整備 ・利用者に対するメタバース利用ルールの策定 ・メタバース組成各段階の法律的視点からの検討と法的留意点リストの策定	・メタバーズ運営事業者に対するセキュリティポリシーに基づくチェックシートの整備 ・メタバース運営事業者に対する脆弱性診断の提供 ・利用者に対するセキュリティ手引書の整備	・脅威分析に基づく具体的な技術的ソリューションの提示(認証をベースにしたなりすましや改ざん防止、情報漏洩対策、デバイスへのDOS攻撃対策など) ・最新技術動向の発信
経済的観点	➢ 適切な利用デバイスの普及に向けた環境整備 例）不適切な規格デバイスの流通におけるデータ流出などのリスク ➢ 適切な利用場所の環境整備 例）公共性の高い利用場所におけるデバイス攻撃などのリスク			
倫理的観点	➢ 将来的な五感連動を見据えた人間拡張の検討 (人間の物理的精神的な存在の限界を取払うアップデート) ➢ 仮想世界/現実世界の相互連動を見据えたモラルや規範 例）表現の自由による誹謗中傷発生のリスク			
文化的観点	➢ 新たな生活文化の形成と醸成に向けた環境整備 例）仮想オブジェクトの肖像権やパブリシティ権の乱用のリスク			

諸外国および国内における代表的な取り組み

NPO法人バーチャルライツ

https://www.npovr.org/

バーチャルリアリティー空間における表現の自由とプライバシー保護の擁護を図るとともにバーチャルリアリティー文化の発展を図り、もって互いの個性と人格を尊重しあえるインターネット空間の実現に寄与することを目的として2021年に3月に代表の國武悠人氏が設立。

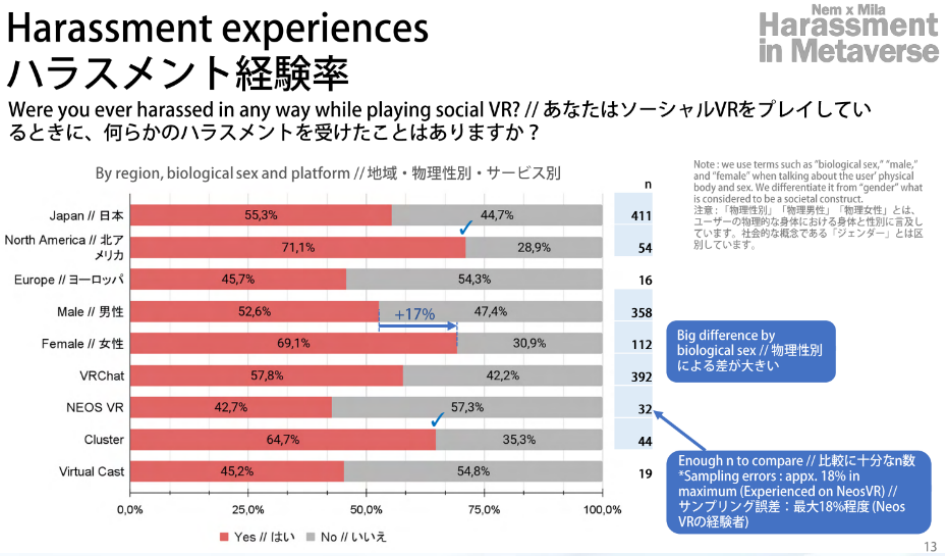
・国際メタバース協議会
メタバースが国際的に拡大していく中で、各国のアドボカシー団体の政策提言や事業推進等に国際的な視点を取り入れる必要性などから設立。
韓国におけるメタバースにおけるハラスメントの実態や法令による規制に対しての調査や、プライバシーを含む提言を採択。

諸外国および国内における代表的な取り組み

「Harassment in Metaverse - メタバースにおけるハラスメント(Nem x Mila)」調査報告

https://note.com/nemchan_nel/n/n60fd28b43b3a

急速なユーザー数の増加により注目が集まるメタバースでのハラスメントの実態を明らかにするため、全世界のソーシャルVRユーザーを対象に、メタバース文化エバンジェリストのバーチャル美少女ねむ氏・人類学者のミラ氏によって行われた国際的な大規模調査。
VRデバイスを用いた没入度の高いメタバース体験者におけるハラスメント経験、種類、強度、現実世界に与える影響など利用者視点での実態調査とともに法令・プラットフォームへの要望についての考え方についても調査されている。



まとめ

- メタバースにおけるサイバーセキュリティについては、メタバースの利活用形態の定義ごとに課題整理を行う必要がある
- 多くのメタバースプラットフォームがゲームエンジンまたはオンラインゲームと同等の構造であることから、多くのセキュリティ対策については既存のオンラインゲームで培われた技術やサービスの活用が可能である
- 行政サービスやビジネス利用など、現実空間でのアイデンティティとの結合が密なメタバースにおいては、健全なデジタル空間の維持のためある程度の利用者権限制限や抑制などが必要と考えられる
- 一方、既存のVRメタバースコミュニティにおいてはハラスメントの実態は見られるものの、自由な空間によって生まれる文化の側面もあることから、一律の規則化・規定化は求められていない
- 利用形態・利用実態にあわせたサイバーセキュリティやプラットフォーマが参照可能なガイドラインの在り方の検討が望まれる