

スマートフォンでつながる デジタル空間の安心と安全

～JSSECとメタバースセキュリティの取り組み～

一般社団法人 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 仲上竜太
(ニューリジエンセキュリティ株式会社)

自己紹介

仲上 竜太 ,CISSP

JSSEC技術部会 部会長

ニューリジェンセキュリティ株式会社

CTO,クラウドセキュリティ事業部副部長

ソフトウェアオフショアベンチャーのち株式会社ラックに入社。サイバー・グリッド研究所長、ネットエージェント株式会社取締役、デジタルペンテストサービス部長を経て、現在は野村総合研究所とラックの合併企業であるニューリジェンセキュリティ株式会社にてCTOを務める。

研究分野：ゼロトラストセキュリティ・xR・メタバース

所属団体：

- ・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
- ・日本ネットワークセキュリティ協会(JNSA)
- ・日本バーチャルリアリティ学会

委員会：

- ・総務省「Web3時代のメタバース等の利活用に向けた研究会」構成員
- ・内閣官房「デジタル市場競争会議ワーキンググループ」オブザーバー

連載：

- ・@IT「働き方改革時代のゼロトラストセキュリティ」



メタバースについて



出典：バーチャルマーケット2021
メタバース上で開催される世界最大のVRイベント『バーチャルマーケット2021』会場&出展企業
第1弾を発表!! | 株式会社HIKKYのプレスリリース
<https://prtimes.jp/main/html/rd/p/000000140.000034617.html>



出典：Everything Facebook revealed about the Metaverse in 11 minutes - YouTube
<https://www.youtube.com/watch?v=gElfo6uw4g>

近年注目を集める「メタバース」を取り巻く様々なイメージ

- ・アバターでコミュニケーションが可能な3Dバーチャル空間
- ・よりリッチなショッピング体験が可能なビジネス空間
- ・ブロックチェーンやNFTでアイテムの所有や売買
- ・メタバースの土地を所有して投資運用

→メタバースの特性が様々な切り口で切り取られている状況

メタバースの構成要素

見た目・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）

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

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がメタバース

※3D仮想空間以外もメタバースとして認識する

メタバースに広がる活動領域

- 自分のコピーを伴う豊かなコミュニケーション
- 視界を覆うHMDやセンサーなど、より深い身体とデジタルとの結合
- インターネットへの接続を前提としたサービス設計



これまでデジタル化されにくかった活動情報が
メタバースでは記録が可能になります

メタバースにおける新たなプライバシーについて



デジタル化された生活空間における

- ・ 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
- ・ 訪問した場所
- ・ 購入したもの
- ・ 会話した相手
- ・ 人間関係など

ウェブサイトと比較して、
より多くの個人の属性や情報が取得可能

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

- 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

システムのセキュリティだけでなくコミュニティ維持や治安維持の観点が必要

これから考えること：メタバースにおける脅威の類型化

脅威分析手法STIRDEによる分類

- （１）Spoofing（なりすまし）：悪意のある攻撃者が正規の利用者を装うなりすまし。特に認証情報の窃盗による、アバターモデルの悪用など。
- （２）Tampering（改ざん）：悪意を持ってデータを書き換える改ざん。特にワールドデータやプロフィールデータの改ざん
- （３）Repudiation（否認）：攻撃の証拠を隠滅し身元を隠す否認。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。
- （４）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。見えないアバターを通してVR空間内の発言や行動が盗聴・盗撮される恐れ。
- （５）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DoS攻撃：プレイヤーのパソコンやVR機器へのDoS攻撃。
- （６）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。

これから考えること：脅威への対応策

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

メタバースプラットフォームサービスはサーバ+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、サーバまたはアプリケーションに対する攻撃界面となる脆弱性は、一般的なアプリケーション診断で対策が可能。

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る。

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、不正課金や不正プレイを抑制するチート対策によるセキュリティ対策の実施。

③サービス運営によるゲーム内（メタバース内）治安維持

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）と同様にメタバース空間内の治安を維持する機関が必要。現状多くのメタバースではユーザ同士のブロック・報告に依存している。

これから考えること：相互運用性とデジタル資産への脅威

現在メタバースの多くが互いに独立して運用されている。

今後、相互運用性が確保された場合にクローズド・中央集権的メタバースにおける管理統制から非中央集権的（De-centralized）への移行が考えられる。

また各メタバース間で共通の資産管理（アバターや衣装などのアイテムや保有するデジタル資産）をブロックチェーン上に記録する仕組みが用いられることが考えられる。

これらの資産はブロックチェーンに紐づくウォレットで管理すると推測される。

ウォレットや暗号資産に対してはかねてより暗号資産取引所へのサイバー攻撃や、個人ユーザへのフィッシング詐欺・暗号通貨詐欺・NFT詐欺などで窃取や詐取が問題視されており、メタバースにおけるアイテムや保有資産に対しても同様の懸念が生じる。

また、複数のメタバースでの挙動を追跡し、デジタル上の人格から現実の人物特定が行われるリスクも考えられる。

JSSECのメタバース セキュリティの取り組み

JSSEC技術部会メタバースセキュリティWGの設置

NEW



JSSEC技術部会にメタバースにおけるセキュリティの諸課題を議論するメタバースセキュリティWGを設立しました。

背景：

スマートフォンの新たな活用方向として、メタバースに接続、利用するためのデバイスとしての役割が期待されている。JSSECでは、スマートフォンのセキュリティについて各キャリアやアプリ事業者・技術者・利用者を対象に多面的なセキュリティの議論を基にガイドラインの制定や普及啓発活動を推進してきた。

現在新たなネットの利用形態として注目されているメタバースにおいては、スマートフォンやスマートフォンOSを使用したデバイスがその接続に際して中心的なデバイスになりつつある。

スマートフォンが活用されるメタバースについてセキュリティ上の課題やプライバシーについて技術的な観点から議論を行うべく、技術部会にメタバースセキュリティWGを設置する。

活動体制：

技術部会の下にメタバースセキュリティWGを設置。

JSSEC技術部会

部会長 仲上竜太（ニューリジェンセキュリティ）

副部会長 宮崎力（ラック）

副部会長 佐藤導吉（東京システムハウス）

セキュアコーディングWG 宮崎力（兼任）

ネットワークWG 佐藤導吉（兼任）

マルウェア対策WG 小笠原徳彦（Shift Security）

→メタバースセキュリティWG 仲上竜太（兼任）

活動計画(2022年度)：

総務省「Web3時代に向けたメタバース等の利活用に関する研究会」委員参加

メタバースセキュリティ勉強会

事業者とのディスカッション

随時オンライン会合を開催

JSSECとメタバースセキュリティの取り組みについて



- 2022年10月 メタバースセキュリティWGを設置
- 2022年8月～ 総務省「Web3時代のメタバース等の利活用に関する研究会」委員
- 2022年12月～ メタバース推進協議会セキュリティ分科会に、
セキュアIoTプラットフォーム協議会と共同参画
- 2023年2月17日 メタバース推進協議会メタバースセキュリティガイドライン一部抜
粋発表

総務省「WEB3時代に向けたメタバース等の利活用に関する研究会」への参加

メタバース等の様々な利活用 ①

7

- オンラインゲーム・ソーシャルVRでのコミュニケーション、イベント等でのメタバース等の利用が進みつつある。
- ビジネス向けにメタバース空間を提供する事業者や、「メタバース」という名前を冠してテレワーク用のバーチャルオフィス※を提供する事業者も出現。

※ 企業ネットワークへの負荷の上昇を避け、またビジネス用の端末でも安定的な利用を確保する観点から、2次元空間の形をとることもある。

①コミュニケーション・イベント

イベントの様子



“VR飲み会”の様子



(出典: パーチャル美少女ねむ著『メタバース進化論』技術評論社 2022年)

事務局資料から引用

https://www.soumu.go.jp/main_sosiki/kenkyu/metaverse/index.html

②ビジネス利用、テレワーク

ビジネス向けメタバース空間 (バーチャル住宅展示場の例)



(出典: 凸版印刷株式会社Webサイト https://www.toppan.co.jp/news/2022/02/newsrelease220221_1.html)

バーチャルオフィス



(画像提供: oVice株式会社)

メタバース等の様々な利活用 ②

8

- 現実の街をメタバースとして仮想空間上に再現し、その空間でイベント等を実施し、リアル空間への訪問を促す試みが、複数の地域で進展している。
- 国土交通省では、現実の都市空間を仮想空間上に再現する「デジタルツイン」/「リアルメタバース」の取組として、自治体が保有する情報をもとに都市の3次元情報を整備し、オープンデータ化を推進する「Project PLATEAU (プロジェクト プラトール)」を進めている。

③ 街を再現したメタバース・デジタルツイン

バーチャル秋葉原



(画像提供: 合同会社AKIBA観光協会、大日本印刷株式会社)

Project PLATEAU



(出典: PLATEAU VIEW (<https://www.mlit.go.jp/plateau/app/>) より、さいたま市浦和区東部の3Dモデル)

メタバース等の様々な利活用 ③

9

- 一部の大学等では、メタバース上での講演やVR空間での授業等を実施。
- 製造業や建設業をはじめ、様々な産業分野でのデジタルツイン・メタバース等の仮想空間の利用も進みつつある。

④講演、教育

東大総長メタバース講演



オンラインVR講義



(画像提供: 東京大学 高宮 智浩 准教授)

⑤産業分野での活用

コマツ社のデジタルツインの事例



(出典: 2022年3月22日 AI経済検討会 座長ヒアリング(第2回) 資料3
コマツ講演資料 https://www.soumu.go.jp/main_content/000004091.pdf)

製造現場でのMRの利活用イメージ



(画像提供: 日本マイクロソフト株式会社)

総務省「WEB3時代に向けたメタバース等の利活用に関する研究会」



(1) 今後、多くのユーザがメタバース等を利用していくこととなった場合に、そうしたユーザがメタバース等の特性を理解し、不利益なく使えるようにするためにはどのような点に留意すべきか。

キーワード (例)

- ・没入感、主観的な視点
- ・アバター的人格/見られ方
- ・契約時の説明責任
- ・身体への侵襲
- ・管理者のルールメイキング
- ・個人情報を含むデータの管理
- ・セキュリティ
- ・Web3 (サービス) の活用 等

(2) 社会のデジタルトランスフォーメーション (DX) が進んでいく中で、今後、メタバース等の利活用が進展すると考えられるユースケースにはどのようなものがあるか。また、こうした仮想空間を構築・利活用する者は、その用途を踏まえてどのような点に留意すべきか。

キーワード (例)

<ユースケース>

- ・公共/準公共分野のDX
- ・テレワーク
- ・教育/研修/訓練
- ・地域活性化
- ・産業利用

<留意すべき点>

- ・現実世界での権利との関係
- ・プラットフォームとの責任分界
- ・利用者のデジタル環境
- ・ (ログ等の) データの管理
- ・既存アバターの利用

(3) 今後、メタバース等の利活用の進展に伴い、社会や経済にどのような影響があり、デジタルインフラやその利用環境等はどのように変わっていくのか。

キーワード (例)

- ・5G/Beyond 5G
- ・データセンター/クラウド
- ・インターネットトラフィック
- ・モバイル市場 (通信・端末・アプリ等)
- ・消費電力/CO2排出量
- ・個人の可処分時間

メタバース推進協議会・セキュアIoTプラットフォーム協議会との連携



一般社団法人メタバース推進協議会 セキュリティ分科会

<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を発表(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プラットフォーム協議会・日本スマートフォンセキュリティ協会・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。

メタバースセキュリティガイドライン総論の一部項目を公表(2023年2月)

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プラットフォーム協議会・日本音楽事業者協会・片岡法律事務所)と共同で作成

宣言

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
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などのリスク
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

必要なアクションプラン/対応

ルール	運用	技術
・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的視点からの検討と法的留意点リストの策定	・メタバース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きの整備	・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

さいごに...最近のメタバース状況と日本の産業について

- HMDやモーションセンサーなどのハードウェア、アニメ・ゲームなどのデジタルコンテンツの活用が見込まれるメタバース周辺産業では、日本企業の活躍が進んでいます。



SONY mocopi
モバイルモーション
キャプチャー



Shiftall
MeganeX / Flip VR



SANRIO
Virtual Festival 2023
in Sanrio Puroland

ありがとうございました