SECURITY REPORT

2022

JULY

メタバース拡散による
サイバーセキュリティ戦略

CyberFortress

このレポートは、株式会社サイバーフォートレスの独自の調査にて収集されたデータに基づき作成しています。

メタバース拡散によるサイバーセキュリティ戦略

01. 概要

新型コロナウィルスの拡散でオンライン・オフラインの境界が崩れることによって映画や想像の中だけに存在すると思った仮想世界が急激に現実へ広がっている。2020年第3四半期、代表的なメタバースプラットフォームであるロブロックス(Roblox)の月間利用者数は約1億5000万人、月別累積利用時間は30億時間に達するなどメタバースに対する興味と人気が爆発的に増加した。

2020年アメリカの大統領民主党選挙候補であったジョー・バイデンとカマラ・ハリスはEpic Gamesの有名なゲームであるフォートナイト(Fortnite)を活用して選挙キャンペーンを起こった。経済回復公約をゲーム内のクエストとして提供して現場に新たな研究施設を建てたり、5Gブロードバンド通信ができるタワーを建てるなどの経済計画を見せた。またグーグルは自社の3次元マップである「グーグルアース」から土地を横10m、縦10mで分けて売っている。現実に存在する土地の持ち主とグーグルアースで販売している仮想土地の持ち主は違うけど、自分が欲しがる地域の土地を仮想環境からいくらでも取得できる。このようにメタバースは我々に巨大な変化の波を見せながら近づいている。

メタバース拡散によるサイバーセキュリティ戦略

02. メタバースとは？

メタバース(Metaverse)の概念は今までに固定されていたり定義されていない。しかし、一般的に仮想、抽象を意味する「メタ(meta)」に現実の世界を意味する「ユニバース(universe)」の合成語として使用される。
つまり、現実と仮想境界が曖昧な「第3の境界地域」を意味する。アメリカ電気電子学会はメタバースを「知覚される仮想世界と連結された永久的な3次元仮想空間で構成されたインターネット」だと定義した。

今の仮想環境(VR)、拡張現実(AR)、複合現実(MR)を合わせるエクステンデッドリアリティ(XR)が普遍化され、メタバースは多様な分野でで幅広く、迅速に我々周辺のものを仮想環境に置き換えている。もはやミレニアル世代・Z世代はメタバースで自分のアバターを利用して友達を作ったり、ものを買ったりなどゲーム・対話・集まりを超えて、経済・社会・文化的な多様な活動をしている。しかも非対面社会が拡散されオンライン活動か拡大された現在、新型コロナウィルで疲れた大勢の人たちが現実世界と似たようになったサイバー空間から外出して得られる楽しみなどをを疑似的に得ている。

03. メタバースの特徴

現実の世界と仮想の世界を繋ぐメタバースには仮想世界だけ発生しうる様々な特性が複合的に存在するため、多様な特徴が存在する。その中で、メタバースに対する一般的な重要特性を整理したのが下記である。

1. 持続的である (Be persistent)
- リセット(reset)、中止または終了されず無限に続く。

2. 同時的でリアルタイム的である (Be synchronous and live)
- (事前に計画された個別のイベントが発生する可能性はあるが)メタバースは全ての人にリアルタイムで、そして一貫的に存在する躍動感がある。

3. 同時的な参加に制限がない (Have no real cap to concurrent participations with an individual sense of “presence”)
- 全ての人がメタバースの構成員になって同時に特定の催し、場所、活動に参加できる。

4. 完全に機能する経済である (Be a fully functioning economy)
- 個人と企業は創作し、所有し、投資し、販売ができ、他の人に認められる価値を作り続ける多様な作業(work)に対して報酬をもらえる。

メタバース拡散によるサイバーセキュリティ戦略

5. 現実的な仮想世界を体感できる (Be an experience that spans)

- デジタル環境と現実の世界、私的で公的な繋がりと体験、解放及び閉鎖されたプラットフォームに繋がる体験がある。

6. これまでにない相互運用性（インターオペラビリティ）を提供する (Offer unprecedented interoperability)

- データ、デジタルアイテム/資産、コンテンツなど多様な連携を基に相互運用性が確保される。

7. 多種多様な人によってコンテンツと利用価値が生成され運用される (Be populated by “content” and “experiences” created and operated by an incredibly wide range of contributors)

- 一部は個人で、他の一部は非公式的な組織か、商業的企業である可能性がある。

全世界的にメタバースの先駆けと言われるロブロックス(Robolox)のCEOであるDave Baszuckiが説明したRobloxメタバースの特徴と、説明したメタバースの一般的な重要特性を比較してみると大きな違いはない。多様な主体が相互作用して共進化(coevolution)し、その中で社会・経済・文化活動が行われて価値を創出するデジタル世界の意味である。

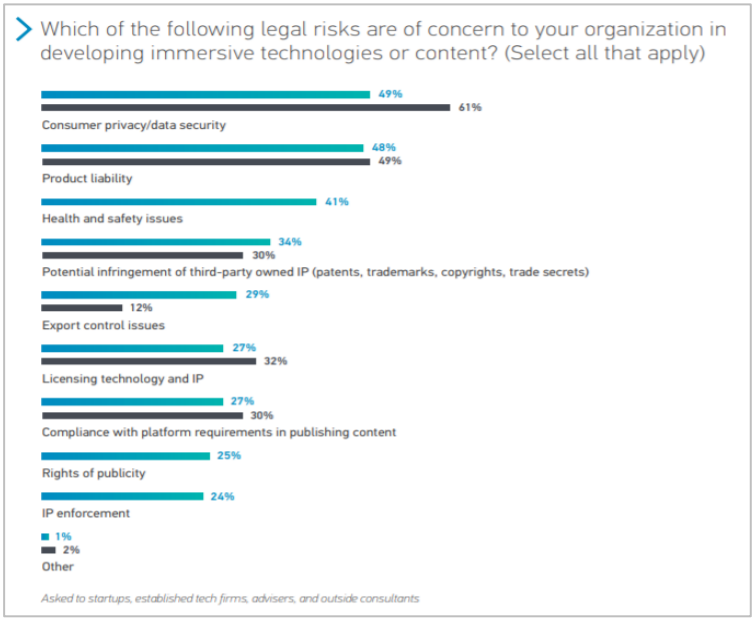
【▲ メタバースを作るとき考慮する特性 (参考 : Roblox)】

04. メタバースの主なセキュリティ脅威

メタバースは仮想のデジタル空間で、違う「自分」であるデジタルアイデンティティ(identity)を作り出す。仮想の空間で作られた自分のアバターで色々な活動をすると現実の世界とつながる。例えば仮想世界で取り引きをすると現実の電子金融取り引きに繋がる。金融ITサービスのように金融取り引きを成功させるためには使用者は自分の身分を証明しなければならないし、支払いしたサービス/商品及び取り引きが履歴を改ざんされる脅威から守らなければならない。

つまり、メタバースサービス業者は仮想世界に対するデータ/コンテンツ保護及び利用者プライバシー保護を最優先で考慮すべきである。

これを補足するのが最近情報セキュリティコミュニティのアンケートでメタバース実現技術及びコンテンツ開発業界が法的リスクの部門で最優先で考慮するものが製品(サービス)品質保障(Production Liability)ではなく、顧客のプライバシーとデータ保護(Consumer Privacy/Data Security)であると結果がでた。



【▲ 没入型技術、コンテンツの法的リスクアンケート (参考： Perkins Coie LLP)】

メタバースは新たな仮想現実のサービスタイプだと考えられるが、そのプラットフォームの構成は既存IT共有サービス(例：Cloud Service, Open API)と比べて大きな違いはない。上記にあるメタバースの運用上に現れる潜在的な脅威であるデータ保護や**顧客の**プライバシー**漏出保護**は我々が思っている典型的なサイバーセキュリティ脅威**対策**の定義と似ている。

メタバース拡散によるサイバーセキュリティ戦略

ただし、メタバースは現実の世界を反映し、多様な相互作用が行われる特性が存在するため、これを考慮して本コラムでは色々なメタバースコミュニティ記事とコラムを参考に下記のように2つのメタバースセキュリティ脅威に対して定義した。

1) データ保護脅威(Data Security Threat)

メタバースから仮想空間経済体系を実現するためにブロックチェーンは重要な役割を担っている。メタバースからのアバターはブロックチェーン技術を基盤とした非代替性トークン(NFT, Non-Funglible Token)で仮想世界の不動産取り引き、商品取引など様々な経済活動ができる。

しかし、メタバースアバターの全ての経済活動、情報交換などは仮想世界のことだけではなく現実の世界と繋がっているため、ハッキングによるデータの改ざん脅威が常に存在する。

2020年8月アメリカオンラインゲームであるロブロックス(Roblox)でハッカー達はシステムをハッキングし、煽情的なイメージと人種差別のメッセージを出したり、ゲームキャラクターがわいせつな行為をするようにさせた事件が発生し、利用者は公憤を発した。事件発生直後、ゲーム会社側は安全で安心なプラットフォームを作るため努力すると声明をだしたがその後にも似たような事例が数回発生した。

このようにまだハッキング犯罪の脅威から解放されておらず、基本的なメタバースの運用の安全性とデジタル資産の安全な管理が必要となっている。

2) データプライバシー脅威 (DATA Privacy Threat)

第一番に、個人情報データのプロファイリング

メタバース実現の重要技術であるエクステンデッドリアリティ(XR, Extended Reality)をサポートするための機器は膨大な個人情報がリアルタイムで自動的に収集されて処理される。利用者の運動動作、目の動きのパターンが収集・分析されて単純に2D画面での視線分析を超えて仮想世界で何を見て、誰と交流しているのかをより深層的に分析できる。現実でメタバースの中の特定の人の生活を立体的に観察して一挙手一投足が監視できれば、これは深刻なプライバシー侵害になる。

第二番に、デジタルツイン - 意図していない利用者の生活の公開

デジタルツイン(Digital Twin)に対するセキュリティの対策が不明である。メタバースからのデジタルツインとは言葉通りデジタルで作り出した双生児である。単純に外見や構造だけではなく、物理的法則まで適用して現実に発生しうる全ての状況を仮想空間でシミュレーションする技術を意味する。

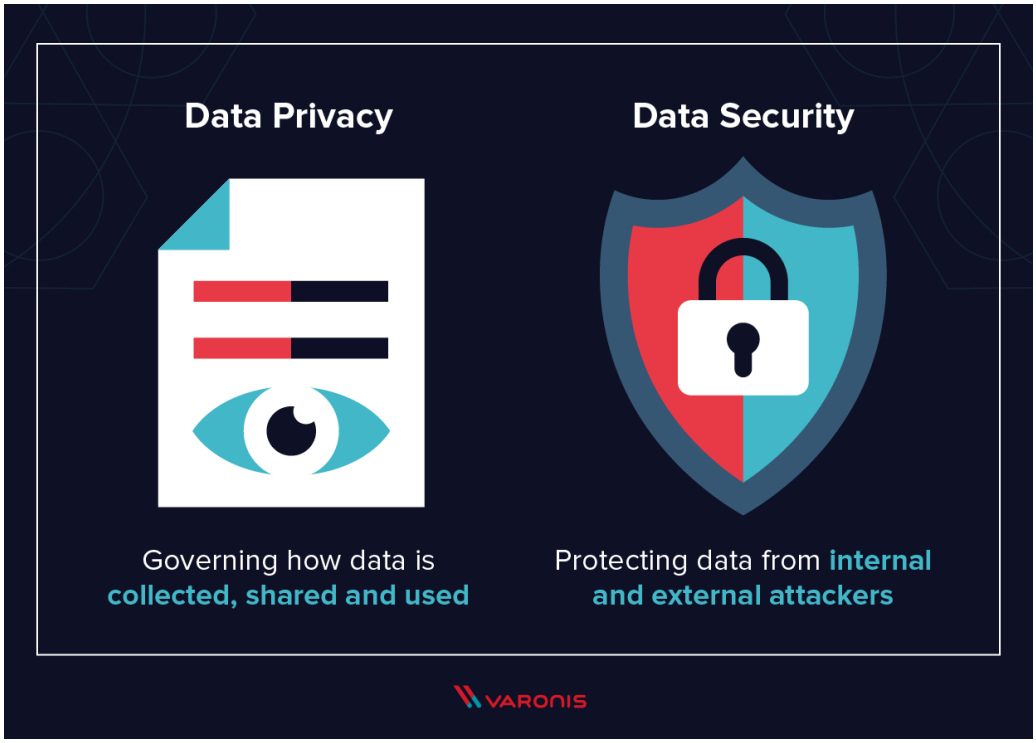
メタバース拡散によるサイバーセキュリティ戦略

メタバースからは利用者の建物、家にあるもの、販売店の商品など全てがデジタルツインで実現される。つまり、違う自分の姿、環境がメタバースの仮想世界にそのまま投影されて存在する。メタバースは明確な境界を持っている現実とは違って利用者の生活が投影されたデジタルツインに制限なく実現できるため、個人のプライバシーなどを守ることはとても大変だと考えられる。残念ながらこれを保護するために必要な基準が今のところ明確ではない。

第三番に、複雑でリアルタイム的な個人情報の処理

今のオンライン基盤のITサービスの個人情報が提供及び共有される時点は比較的に明確だが、メタバースでは自分の個人情報がどのタイミングでだれに共有されているのか確認するのは難しい。メタバースの複合的なサービスは利用者の消費習慣、位置情報、生体情報などのような新たなタイプの個人情報を特定の時点ではなくリアルタイムで使用・共有する。

従って、メタバースからは個人情報に対する強制権を行使するために必要な情報を正確に確認するためには既存のITサービスと比べられないぐらい複雑で難しい。



【▲ Difference Between Data Security and Data Privacy (参考：VARONIS)】

05. メタバース保護のためのサイバーセキュリティ戦略

メタバースはIT共有サービスプラットフォームと同じく情報セキュリティの問題点(データセキュリティ、プライバシー)を持っているが、既存情報セキュリティ対策よりメタバースの特性に合わせた戦略の樹立が必要である。

1) Content Protection - デジタルコンテンツ及び知的資産権保護戦略

「仮想世界で作られた創作物に対する著作権はどのように保護されるべきなのか？」

代替不可能な特性を持っているNFT(Non-Fungible Token)を利用して現実・仮想世界での所有権を証明する。
しかし、創作者ではない他の人が先に創作物をNFTを利用して所有権を主張したり２次創作物のNFT所有権が現著作物の著作権を侵害する場合がある。

メタバース上で作られて流布されるコンテンツの不法コピー及び流通問題は他のITオンラインサービスの問題と同一である。ただし、現実の世界の全ての姿がデジタルツインに投影されたメタバースには実際に存在する特定のブランド品を無断複製して使用される可能性がある。企業の立場としてはこれはブランド及び商標に対する知的資産権を侵害である。

従って、NFTの偉作・著作権の問題に対応する保証システム、検証及び認証システムが必要である。ブランドや商標の知的資産権の侵害に対して企業は持続的にモニタリングする必要がある。これのためにコンテンツ生産者(企業もしくはクリエイター)は技術的な対応としては既存コンテンツ保護技術であるDRM技術を活用しメタバースコンテンツの保護と無断複製に対するモニタリング手段を整えなければならない。

また、管理的な戦略でコンテンツ生産者はメタバース環境で自分のコンテンツの流通及び著作権侵害に対する新たな規定を迅速に樹立し、持続的に反映する必要がある。

2) Consumer Privacy Protection - 個人情報プライバシー保護戦略

「メタバース業者の広範囲で不法的な個人情報プロファイリング行為はどのように防ぐのか？」

メタバースに接続すると多様な生体認識情報が収集される。単純にマウスのクリックとキーボード入力などで手動的に特定のデータを収集することではなく、HMDのような機器で脳波、血圧、呼吸など生体情報(Biometric Data)を含めて個人の行動情報及び感情情報まで全てを収集し、分析(プロファイリング)できる。

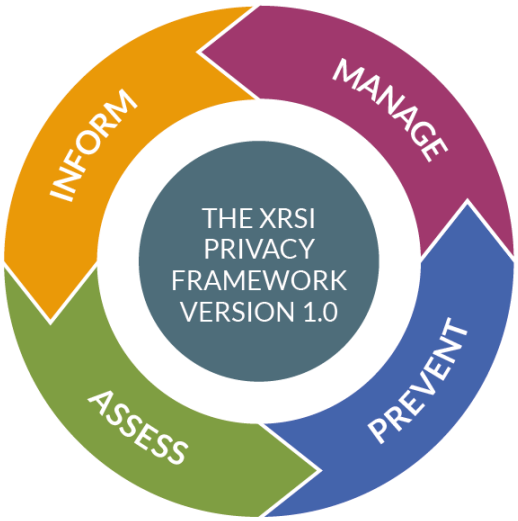
メタバース拡散によるサイバーセキュリティ戦略

GDPR(General Data Protection Regulation, EU一般データ保護規則)第9条によると、このような処理には個人データを特別な範疇で取り扱われるため格別な注意が必要であると述べている。従ってデータの暗号化及び追加的に収集される個人情報を認識して統制できる範囲のデータ保護が必須である。

技術的な措置戦略としてメタバースサービス使用者の動き及び身体的な特性など生体情報を安全に保護する方法を求めなければならない。AR/VR環境から使用するメタバース機器(ARグラス、ホログラム装置、HMD(Head Mounted Display))は製造段階からプライバシーセキュリティ政策を樹立し、ファームウェアアップデート及びデータ暗号化で安全な環境を維持しなければならない。また、データの物理的なセキュリティ、施設/人材セキュリティ、ネットワークセキュリティ、システム強化、暗号セキュリティ、エンドポイント保護など法的な要求事項を満たすための政策及びセキュリティ手段を求めて実現する必要がある。

一方、 技術的な措置戦略以外のセキュリティ戦略としては個人情報全般に対する責任が強化されたメタバース個人情報保護規定及び管理体系を構成しなければならない。単純に指定された個人情報類型と安全性の確保措置を定義した既存の個人情報保護活動ではなく、生体情報及び行動情報収集、分析及び処理する全ての統合的な管理体系の設計が必要である。

良い事例として最近、XR世界からの私生活、セキュリティ及び倫理的な問題全てを扱う国際的非営利団体であるXRSIは2020年9月プライバシー保護フレームワークを公開した。XRプラットホームで個人情報保護の作業領域を4つに(Access-Infrom-Manage-Prevent)分けて各領域ごとに保護措置方法を定義した。



【▲ XRSI Privacy Framework概要 (参考： XRSI.org)】

06. 最後に

このよに既存のシステム保護措置及び管理政策はメタバースの仮想環境を適切に保護するためには足りないため、これをメタバースの特徴に合わせて改善する必要がある。メタバースの発展のためには規制の不明な情報を含む認識論的な状況（不確実性）が必要だからである。メタバースの領域が拡大・発展され、価値が高くなるほど各種規制と綿密な調査が行われると思うが、このような規制が投資者に信頼を与えて消費者には安心を与える肯定的な要素として作用する。

07. 参考資料

https://www.kisa.or.kr/public/library/IS_View.jsp?mode=view&p_No=158&b_No=158&d_No=503&cPage=4&ST=T&SV=
https://clink.social/what-is-the-metaverse/
https://www.matthewball.vc/all/themetaverse
https://arteco.legal/66
https://spri.kr/posts/view/23197?code=issue_reports
https://www.seoul.co.kr/news/newsView.php?id=20201009027001
https://www.boannews.com/media/view.asp?idx=98450&page=1
https://www.cityam.com/the-metaverse-real-world-laws-give-rise-to-virtual-world-problems/
https://www.gamesindustry.biz/articles/2021-06-08-new-world-old-rules-the-rise-of-the-metaverse
https://xrsi.org/definition/the-xrsi-privacy-framework