メタバースセキュリティガイドライン(第２版)

～安心安全なメタバース空間の実現に向けて～

令和５年 12 月 14 日

メタバース推進協議会

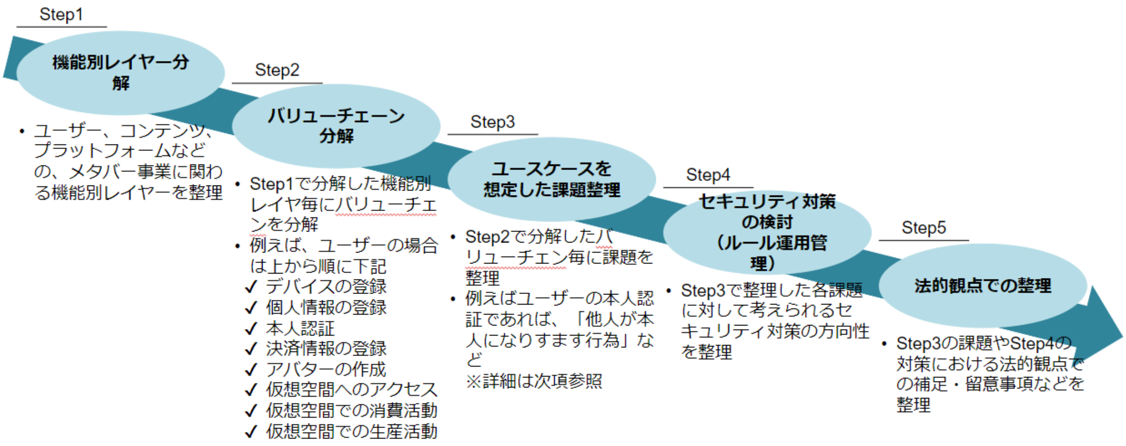
目次

0. はじめに

【メタバース推進協議会の背景・目的】
現実社会では、未来のために解決しておきたい多くの課題が複雑に絡み合い、いまでは、人々が望む平穏で"普通"の生活や営みさえ、"有難い"とされています。日本には、特有の自然観や倫理観、美意識があり、加えて近年は科学や技術の分野で目覚ましい進歩を遂げています。しかし、いまの現実社会には、様々な課題を解決できる社会の構造や整備が追いついていないケースも散見されます。このような時代にメタバースという新しい世界をどのように描いていくか、それを後世にどの様に残していくべきか、現実社会を構成しているより多くの人々と連携し、生活者が主体となるメタバースの可能性を探求するために、メタバース推進協議会が発足しました。
メタバース推進協議会では、日本の生活文化、科学、技術、経済などに関わる有識者と企業を結集し、日本人の自然観や倫理観、美意識を元にしたメタバースの世界に、現実社会の課題を連動させて描き、後世に伝えていきます。

【メタバース推進協議会のガイドライン】
メタバース推進協議会では、協議会の目的に向けた活動の根幹となる「現実社会連動メタバースガイドライン」を策定いたします。また、その中の一つが本ガイドラインである「セキュリティガイドライン」であります。
「セキュリティガイドライン」では、ユーザー・プラットフォーム事業者・コンテンツ事業者などの、メタバースに関わる全ての関係者に対して、情報セキュリティや利用環境上の課題と解決策を解説するとともに、安心安全にメタバースを利用・運用するために必要な要件を示しております。これらの情報に基づき、広く安心安全なメタバースの世界が浸透することを目的としております。

【本ガイドラインの作成方法・構成】
本ガイドラインの作成に向けて、個別のセキュリティ脅威や課題を考える以前に、まずは、メタバースにおけるあらゆるユースケースの洗い出しから始めました。未だメタバースそのものが世界で浸透していない現状では、どのようなセキュリティ脅威・課題があるかを直接導くことは難しいと考えたためです。従って、どの様なプレイヤーがどのようにメタバースに関わるのかの整理から始めました。
具体的にはまずは、ユーザー・コンテンツ・プラットフォームなど、メタバース事業に関わる機能別レイヤの洗い出しから始めました。その上で、各機能別レイヤのバリューチェーンを分解いたしました。例えばユーザーという機能別レイヤであれば、デバイスの登録・個人情報の登録・本人認証/確認などのバリューチェンに分解できると考えます。ここで整理したバリューチェンの一つ一つに対し、セキュリティ脅威・課題を洗い出しました。最後にそれぞれのセキュリティ脅威・課題に対するセキュリティ対策、法的観点での補足・留意事項を検討いたしました。
上記のように整理・検討を進めたため、本ガイドラインでも同様の構成で作成しております。



【今後に向けて】

本ガイドラインはメタバースが世界に浸透し、新たなユースケースの抽出やセキュリティ技術の開発が進む過程で随時更新される予定です。

また、本協議会では、ガイドライン策定と並行し、各種メタバースの実証実験を進めて参ります。実証実験を通じて抽出された新たな課題も、本ガイドラインに反映して参ります。

この活動を通じて、本協議会の目的である、メタバースの世界と現実社会の課題を連動させ、後世へ伝えていくことに繋がることを願います。

1. ユーザー

1-1 デバイス情報・個人情報の登録

【ユースケース】

- デバイスが不正登録される
- 他者デバイスの不正な登録によるなりすましがおこる
- 登録した個人情報の目的外利用、同意のない第三者提供
- 登録した個人情報の流出

【課題・留意点】

- 生活者保護の視点として、デバイスを不正に登録されないようにセキュリティ設定等に留意が必要。
- 生活者保護の視点として、利用目的や情報の提供先を確認して、想定外の情報利用がなされないように留意が必要。
- IT インフラの視点として、デバイス情報が「個人情報」や「個人関連情報を個人データとして取得」することが想定される場合には、個人情報保護法に留意が必要。
- デバイス情報（種類、バージョン、通信回線、OS 等の情報）を取得する場合にも、遵守すべきルールがないかについて、確認が必要。
- 法的な視点として、「個人情報」「個人データ」に該当するものは、他のデータと区別して個人情報保護法に基づく安全管理措置その他法令上の義務を遵守することへの留意が必要。
- （プライバシーポリシーの策定、利用目的の公表等）
- メタバースプラットフォームに保存されているユーザーに関する個人情報保護への留意が必要。

【対策】

- 氏名、生年月日、メールアドレス、性別、住所、IP アドレス、端末識別番号等個人情報を登録する際には、正しい登録先であることを確認の上、入力することが必要。
- 利用用途によっては、プラットフォーム側でも、より厳格なデバイス認証の仕組みが必要。
- 機密情報が求められるものは、デバイス自体を特定して、間違いなく確認、認証することが必要。

1-2 本人確認・本人認証

【ユースケース】

- 第三者がメタバース上で、本人になりすましてアバターの登録をする
- 第三者がメタバース上でアバターをのっとり、本人になりすまして行動・取引等をする

【課題・留意点】

- IT インフラの視点として、ユーザーがメタバースに接続する際の本人確認・認証に関する課題がある。HMD を被っている場合に MFA（多要素認証）など、従来の方法が困難となる場合が考えられ、システムとして認証強化を行う手段が複雑になる懸念がある。
- 本人認証・本人確認の対象となる取引（行為）によって、「認証（同一性確認）」（及び実在性確認）だけで足りるのか、真正性の確認（本人性、身元確認）を要するのかは、空間設計や対象取引（行為）によって異なるため、それぞれ必要な確認の水準に合わせた方法を選択する必要がある。

- 法的な視点として、犯罪収益移転防止法に定められる「特定取引」の場合、同法に基づく「取引時確認」のタイミング、確認すべき事項や方法、記録事項等、同法の詳細な定めを遵守する必要がある。
- 反社会的勢力の排除として、各事業者が提供する空間や取引に合った方法を検討すべき。

【対策】

- 認証方式として、利便性の高い本人確認およびセキュアな認証が必要。
- 一般に情報システムにおける本人認証では、パスワードによる認証に加え MFA（多要素認証）によって認証を強化が図られている。MFA には、個人情報として登録されたメールアドレスや電話番号による確認や、スマートフォンデバイス上のアプリを利用する方法や、指紋・虹彩などの生体認証を行うものがある。
- 認証方式として、スマートフォンや PC、HMD を装着した状態でも容易に利用可能な認証方式の採用が推奨される。HMD を装着した状態でメールや SMS を通じたパスコードの確認は容易ではないため、別の方法が必要と考えられる。例えば複数の認証方式を許容し、デバイスに応じて最適な認証方式が採用できるなどが望ましい。
- 高い機密性が求められる利用用途では、プラットフォーム側でも、マイナンバーカードによる公的個人認証の仕組み等、より厳格な本人確認・認証の仕組みの実装が必要。

1-3 決済情報の登録

【ユースケース】

- 登録した決済情報の流出
- 第三者に決済情報を不正に登録され、利用される

【課題・留意点】

- IT インフラの視点として、メタバースに接続する際の認証に関する課題がある。例えば、MFA 等は、HMD を被っていると IT 構築が複雑になる懸念がある。

【対策】

- 自己の保有する決済情報（アカウント ID、カード番号、PW、セキュリティコード等）について、第三者に取得されないように管理する。
- 第三者の決済情報が不正に登録されることのないように、（１）現実社会の決済手段、メタバース内の決済手段の登録時、（２）現実決済手段のメタバース内決済手段への連携時に、空間、サービス提供側として適切な防止措置を講じる。
- 高い機密性が求められる利用シーンでは、プラットフォーム側でも、マイナンバーカードによる公的個人認証の仕組み等、より厳格な本人認証の仕組みの実装が必要。

1-4 アバターの作成

【ユースケース】

- 他人が本人になりすましてアバターを作成
- 作成したアバターの悪用

【課題・留意点】

- 生活者保護の視点として、他人の著作権、商標権、肖像権等を侵害しないように留意が必要。
- また、現実世界と異なる点として、アバターの相貌による認識はデジタルによって簡単にコピーできてしまう。一意性をどう見るか、アバターの顔による顔認識は可能か。カスタマイズで同じアバターを作れてしまうことは問題か等の検討が必要。

【対策】

- メタバース空間の設計時に、アバターについて、（１）各ユーザーが著作権等を保有するか、（２）事業者が著作権等を有するアバターを提供し、自由に利用できることとするのか、それぞれの空間の目的に沿ったルール作りや運営が必要となる。

1-5 仮想空間へのアクセス

【ユースケース】

- アクセス時のハッキング

【課題・留意点】

- 不正アクセス禁止法に基づき、アクセス管理者のアクセス防御措置（努力義務）に留意が必要。

【対策】

- MitM、認証情報のフィッシング等、既存サービスにおける認証のリスクモデルの構築が必要。

1-6 仮想空間内での消費活動

【ユースケース】

- 決済時の情報流出
- なりすましによる不正利用
- 購入物が偽物、何らかの理由で所有できない

【課題・留意点】

- 購入物に問題がある場合、民法の契約内容不適合責任が適用される可能性がある点に留意が必要。

【対策】

- メタバース空間で行われる消費行動の種類によって、（１）メタバース空間に登録時の本人確認、消費行動の当事者や決済情報の利用時の認証（実在性や本人の決済情報であることの確認）をどこまで厳格に行うかのルールづくり、（２）消費行動の当事者と決済手段提供者、空間提供者等各当事者間に適用される、不正が起きた場合のルールづくりが求められる。
- 他人に自らのアカウントや決済情報を不正に利用して消費行動されないように、情報管理する。
- 既存システムにおける決済サービスのリスクモデルを構築する。

1-7 仮想空間内でのコミュニケーション

【ユースケース】

- 虚偽の情報等による勧誘、売買

- 誹謗中傷、名誉棄損の被害

【課題・留意点】

- 法的な視点として、メタバース空間内でユーザー間のメッセージ交換を媒介したり、ウェブ会議のような特定のユーザーが参加できるシステムを提供したりする場合等、電気通信事業法に基づく登録又は届出が必要となる点に留意が必要。
- また、公開の掲示板等の場合、登録や届出が不要となるケースであっても、通信の秘密の保護や、検閲の禁止の規制はかかるので注意が必要。

【対策】

- プロバイダー責任制限法が適用される場合には、名誉棄損等、権利侵害を受けた者から当該権利の侵害に係る発信者情報の開示請求等に対応が求められることとなる。
- 空間内コミュニケーションが公開されるものか、クローズなものか、各々のルールに従って投稿する。

1-8 仮想空間内での生産活動

【ユースケース】

- 購入された生産物の対価が入金されない

【課題・留意点】

- 商取引的観点とともに、決済サービスの不備や記録情報の書き換えリスク等への留意が必要。

【対策】

- 購入者からの検収通知を受けて入金する仕組み（エスクロー）を導入する等、空間を運営する事業者が防止措置を講じることも必要。

2. コンテンツ（サービス）

2-1 コンテンツの設計・制作

【ユースケース】

- 著作権を侵害したコンテンツが生成・投入されてしまう
- ポイントや空間内通貨などの不正の生成

【課題・留意点】

- 法的な視点として、コンテンツが著作権、商標権、肖像権等の侵害をしないように留意する。

【対策】

- 著作権侵害について規約で利用者に対して制限を課すとともに、メタバース上と接続されたショップやアイテム販売サイトで販売されているものの定期的なパトロールによって実態把握を行う。

2-2 ユーザーへの販売

【ユースケース】

- 作成コンテンツが偽物の空間へデリバリーされてしまうリスク
- 悪意を持ったコンテンツがデリバリーされてしまうリスク

【課題・留意点】

- 生活者保護の視点として、空間内で売買等を行う場合には、偽の空間でないか、空間内の表示等に不自然な点がないかを注意する必要がある。
- IT インフラの視点として、仮想空間におけるフィッシング、コピー、偽物についてのリスクがある。フィッシングとは、悪意をもった行為者があたかも正規のサービスのような見た目で利用者のログイン情報や個人情報、クレジットカード情報などを窃取する目的でサイトなどを設置するものであり、メタバースにおける仮想空間においても著名な空間コンテンツの類似的なものまたはコピーを作成して誘導することで、個人情報などを窃取するものが考えられる。その結果、重大な個人情報漏洩や不正決済などのリスクが発生する恐れがある。
- 複数の空間でコンテンツを提供する場合、空間をまたいだ取引を許容するのか、その場合の本人認証、アバターの流用はどうするのか、事業者側でルールを設定する必要がある。
- 偽物の空間（フィッシングサイトのような空間）で取引を防止し、本物の空間での取引の安全性を確保するため、事業者側で偽物の空間への誘導防止に関して、注意喚起をする等の工夫も必要である。
- メタバースプラットフォーマー側において、コンテンツを登録する際に、制作者の実在性やコンテンツ自体の安全性に対する審査が不十分であると、利用者に損害を与えるコンテンツが流通してしまう恐れがある。

【対策】

- 空間コンテンツの真正性担保については以下の方法が考えられる
  - メタバースプラットフォーマーが空間に対して審査・認証を行って保護する方法
  - 利用者による主体的な安全性確認を可視化し投票等によって健全性を保つ方法
  - 認証局の発行する証明書を空間に対して発行可能なものとし、悪意を持った開発者による空間の発行を困難にする方法
- 取引については可視性を担保し、プラットフォームを超えたトラッキングを可能にすることで不正に利用された場合の証明とすることが求められる。その際にパブリックチェーンの活用などは有用である。

2-3 ユーザーへの販売

【ユースケース】

- 作成コンテンツが偽物の空間へデリバリーされてしまうリスク
- 悪意を持ったコンテンツがデリバリーされてしまうリスク

【課題・留意点】

- 生活者保護の視点として、空間内で売買等を行う場合には、偽の空間でないか、空間内の表示等に不自然な点がないかを注意する必要がある。
- IT インフラの視点として、仮想空間におけるフィッシング、コピー、偽物についてのリスクがある。フィッシングとは、悪意をもった行為者があたかも正規のサービスのような見た目で利用者のログイン情報や個人情報、クレジットカード情報などを窃取する目的でサイトなどを設置するものであり、メタバースにおける仮想空間においても著名な空間コンテンツの類似的なものまたはコピーを作成して誘導するこ

とで、個人情報などを窃取するものが考えられる。その結果、重大な個人情報漏洩や不正決済などのリスクが発生する恐れがある。

- 複数の空間でコンテンツを提供する場合、空間をまたいだ取引を許容するのか、その場合の本人認証、アバターの流用はどうするのか、事業者側でルールを設定する必要がある。
- 偽物の空間（フィッシングサイトのような空間）で取引を防止し、本物の空間での取引の安全性を確保するため、事業者側で偽物の空間への誘導防止に関して、注意喚起をする等の工夫も必要である。
- メタバースプラットフォーマー側において、コンテンツを登録する際に、制作者の実在性やコンテンツ自体の安全性に対する審査が不十分であると、利用者に損害を与えるコンテンツが流通してしまう恐れがある。

【対策】

- 空間コンテンツの真正性担保については以下の方法が考えられる
- メタバースプラットフォーマーが空間に対して審査・認証を行って保護する方法
- 利用者による主体的な安全性確認を可視化し投票等によって健全性を保つ方法
- 認証局の発行する証明書を空間に対して発行可能なものとし、悪意を持った開発者による空間の発行を困難にする方法
- 取引については可視性を担保し、プラットフォームを超えたトラッキングを可能にすることで不正に利用された場合の証明とすることが求められる。その際にパブリックチェーンの活用などは有用である。

3. コンテンツ（アバター）

3-1 アバター設計・制作

【ユースケース】

- 制作したアバターのデータ流出

【課題・留意点】

- 法的な視点として、アバターの権利について、各空間運営者がどのようなルールを策定するか留意が必要。他の空間にアバターを持ち出すことを許容するかどうかも、空間運営者やアバターの権利者との契約によるものの、そもそもアバター作成者（ユーザー）に著作権等が残る場合、当該アバターの利用者（著作権者から許諾された者）が他の空間に持ち出せるかどうかは許諾の範囲かどうかによる。
- アバターに付随する情報（購入したメタバース空間内の財産や決済情報等）の流出は、一時的には「個人データの流出」するかどうかが問題となる（個人データかどうかは、アバターと実在する個人との結びつき等による）。二次被害として、当該情報を不正に利用された場合は、財産の消失や決済情報の不正利用等が考えられる。
- また、現実世界と異なる点として、アバターの相貌による認識はデジタルによって簡単にコピーできてしまう。一意性をどう見るか、アバターの顔による顔認識は可能か。カスタマイズで同じアバターを作れてしまうことは問題か等の検討が必要。

【対策】

- 空間上に展開されたアバターデータをメモリ上などから抜き取れないような仕組みの構築
- アバターの認識符号（ＩＤ）などの流用により、他人が所有するアバターデータを取得できないような仕組みの構築
- 自分で制作、カスタムして制作したアバターについては、データ制作者の権利として著作権による保護が有用
- プラットフォーム上で提供されるアバター編集ツールによるカスタマイズは、同一の組み合わせが生じることを念頭に、認証等の識別に適さないことに留意

3-2 ユーザーによる利用

【ユースケース】

- コピーされたアバターによる不正利用、なりすまし

【課題・留意点】

- アバターや決済情報の本人認証の問題への留意が必要。
- また、現実世界と異なる点として、アバターの相貌による認識はデジタルによって簡単にコピーできてしまう。一意性をどう見るか、アバターの顔による顔認識は可能か。カスタマイズで同じアバターを作れてしまうことは問題か等の検討が必要。

【対策】

- 利用規約などによるアバター外見の模倣に関する行為の制限

4. コンテンツ（空間）

4-1 空間設計・制作

【ユースケース】

- アクセス導線の設計によるセキュリティ脅威
- 空間自体が偽物（フィッシングサイトのようなもの）

【課題・留意点】

- 法的な視点として、不正アクセス禁止法に基づき、アクセス管理者のアクセス防御措置（努力義務）に留意が必要。
- 偽物の空間（フィッシングサイト）への誘導を防止する措置（注意喚起等）も検討課題となる。
- IT インフラの視点として、仮想空間におけるフィッシング、コピー、偽物についてのリスクがある。

【対策】

- プラットフォームによる空間の認証と認証の可視化（公式マークなど）
- 利用規約などによる他社の著作物や商標を使用したワールドの作成の制限

4-2 空間へのデータ残留

【ユースケース】

- 空間自体がデータで構成されていることから、空間での活動データが残留してしまうケース

- 本来記録されるべきでないデータの保存など

【課題・留意点】

- 記録データの取り扱いやデータの記録方法について留意する必要がある

【対策】

- データの保存期間、閲覧範囲等の開示
- 保存データに対するセキュリティ対策の実施

4-3 空間内での体操デザイン

【ユースケース】

- 現実世界での動きで意図的/非意図的に関わらずケガを誘発

【課題・留意点】

- HMD を装着した状態で身体的行動（コントローラの大きな操作や歩行）を求める場合には、現実世界の周辺環境に問題がないか（HMD 装着時の一時に限らずサービス利用途中も）留意が必要。

【対策】

- 身体的行動を求める場合には周辺に危険がないかの確認を事前に促す
- HMD 前面カメラで外界情報を読み取り危険があると判断した場合にはサービスを一時中断しパススルーで現実世界の状況確認を促す

4-4 ユーザーにより利用

【ユースケース】

- アバター間による誹謗中傷、名誉棄損

【課題・留意点】

- 法的な視点として、プロバイダー責任制限法が適用される場合には、名誉毀損等、権利侵害を受けた者から当該権利の侵害に係る発信者情報の開示請求等に対応が求められることとなる。
- また、コミュニティにおけるプレイヤー同士でのモラル／ハラスメントに関するリスクへの留意が必要。

【対策】

- 利用規約によるハラスメントの定義と防止
- プラットフォームサービス内での紛争解決

5. プラットホーム

5-1 プラットホームの設計・制作

【ユースケース】

- 過度なユーザーの個人情報の取得と独占

【課題・留意点】

- 法的な視点として、デジタルプラットフォーム透明化法の適用対象となる場合がある点、独占禁止法の優越的地位の濫用に留意が必要。
- ユーザーやコンテンツ提供者の情報を大量に取得することから、どの情報をどの範囲で利用、管理すべきなのか適切な仕分けと安全管理措置が必要となる（個人情報保護法、プライバシーの観点だけでなく、コンテンツ提供者との秘密保持契約や営業秘密等）。

【対策】

- ユースケースによっては、マイナンバーカードによる公的個人認証の仕組み等より厳格な本人認証の仕組みの実装が必要。

5-2 プラットフォーム間のインターオペラビリティ

【ユースケース】

- 認証の連携
- プロビジョニング

【課題・留意点】

- 協議中

【対策】

- 協議中

5-3 プラットホームの提供

【ユースケース】

- プラットフォームの乗っ取り、なりすまし
- プラットフォームへのサイバー攻撃

【課題・留意点】

- プラットフォームサービス管理者権限や DDoS 対策等、クラウドセキュリティリスクへの考慮が必要。

【対策】

- プラットフォーム運営事業者の実在確認等メタバース空間の真正性の確保のため SSL/TLS 証明書の導入等の対策が必要。

6. デバイス

6-1 デバイスの設計・制作

【ユースケース】

- デバイスの脆弱性を踏み台とした DOS 攻撃の発生
- スパイチップの混入などによるプライバシー情報の流出
- 不適切なデバイスによる健康被害

【課題・留意点】

- 脆弱性を排除した上で製品出荷する必要がある

- 脆弱性が見つかった段階で速やかにファームウェアのアップデートができる仕組みが必要
- デバイスが取得できる情報に網膜情報など個人情報に資する情報があるためその取扱いに留意する必要がある
- HMD を始めとしたデバイスに記録された個人情報の削除について留意が必要
- センサーの小型化により身体のポジション、身体形状、身体的特徴、利用者の位置情報などプライバシーに関する情報の取得が可能となることが考えられる
- セーフティの観点から、視覚や聴覚およびクロスモーダルな領域への非侵襲的な身体のリスクがあることに留意したデバイスの開発が求められる

【対策】

- セキュリティバイデザインに基づく設計・製造が必要
- 出荷前の脆弱性診断の実践が必要
- デバイスの設計製造から利用、リユース/廃棄にいたるまで、プロダクトライフサイクル全体を考慮したセキュリティ対策が必要
- 安全にファームウェアをアップデートする仕組みの実装が必要
- 利用用途によっては、より厳格なデバイス認証の仕組みが必要
- 非侵襲的な身体および精神面への影響等のリスクが考えられるため、厚生労働省などによる安全基準が求められる可能性もある。

6-2 ユーザーによる利用

【ユースケース】

- デバイスへのサイバー攻撃

【課題・留意点】

- デバイスへの DOS 等への留意が必要
- 表示される画像や映像の改ざん
- センサーで取得されるデータ、デバイスで取得可能なデータの窃取

【対策】

- デバイスのファームウェアにおけるサイバー攻撃対策の実装
- デバイス上で実行されるソフトウェアにおけるデバイスへのサイバー攻撃に至る脆弱性対策

7.インフラ

7-1 通信回線の接続

【ユースケース】

- 通信網へのサイバー攻撃

【課題・留意点】

- 通信インフラに対するリスクについては、一般の事業と同等と考えて良い。

【対策】

- 電気通信事業法の適用を受けることが必要。

7-2 通信回線の利用

【ユースケース】

- 通信網へのサイバー攻撃

【課題・留意点】

- 協議中

【対策】

- 協議中

８.デベロッパーサポート

【ユースケース】

- 協議中

【課題・留意点】

- 協議中

【対策】

- 協議中

【作成者】

・一般社団法人 メタバース推進協議会

【作成協力※五十音順】

・一般社団法人 セキュア IoT プラットフォーム協議会
・一般社団法人 日本音楽事業者協会
・片岡総合法律事務所
・一般社団法人 日本スマートフォンセキュリティ協会(JSSEC)
<JSSEC 技術部会 メタバースセキュリティ WG 参加企業>
ニューリジェンセキュリティ株式会社
株式会社ラック
KDDI 株式会社
アルプスシステムインテグレーション株式会社
日本電気株式会社
PwC
東京システムハウス株式会社
サイバートラスト株式会社
・経済産業省
・総務省