



VRChatにおける リップティング対策の現実

暗号化ではなく、露出設計として考える

Soisina, くまめい

自己紹介

名前

Soisina

関心

VRChat・情報セキュリティ

X

<https://x.com/eyodonJJ>



今日扱わないこと / 今日話すこと

扱わない範囲

- リッピングの攻撃手順やツールの話
- 購入者ごとのフィンガープリントや透かし
- 権利主張、DMCAなどの法的手続き
- 個人の特定につながる話題

今日の主題

- 技術的に何が守れて、何が守れないのか
- VRChatの文化に合った現実的な設計
- 「誰に、どの版を、どの文脈で見せるか」
- という露出設計の考え方

アバターは単なる3Dモデルではない

VRChatでは、アバターは「他人からどう見えるか」だけでなく「自分をどう表現するか」でもある（VRChat公式ヘルプ）。

普通のゲームではキャラクタースキンはゲーム内アイテムの一種にすぎないが、VRChatでは異なる位置づけになる。



作者にとって

アバターは自分の作品であり、
創作活動の成果物として扱われる



販売者にとって

アバターは商品であり、
経済活動の対象になる



使用者にとって

アバターは自分の身体であり、
自己表現の手段になる



イベント主催者にとって

アバターは空間演出の一部であり、
場の設計に組み込まれる

実際に何が起きていたか



VRChat Security Update (2022)

VRChat公式が、改造クライアントの問題として「ripping and archiving avatars」を明記した。

リップpingを単発のいたずらではなく、改造クライアントネットワークによるプラットフォーム上の安全問題として位置づけている。

同文書で挙げられた問題：

- 毎月数千件のアカウント窃取（改造クライアント経由）
- キーロガーやボットネットとして振る舞う改造クライアント
- クリエイターが不具合対応に数時間～数日を費やし、原因が改造クライアントだったと判明するケース

被害は三層ある



第1層：アセット被害

アバターやワールドのデータが抜かれる。3Dモデル・テクスチャ・アニメーション等の流出。



第2層：アカウント・端末被害

改造クライアント経由でアカウントが乗っ取られる。端末の情報が抜かれる。キーロガーの被害。



第3層：創作環境への被害

このLTで一番重視したいのは第3層。リッピング対策は単にデータを守る話ではなく、創作文化をどう維持するかの話でもある。

なぜ完全防止が難しいのか

VRChatはローカル端末で3D空間を描画する。アバターやワールドを表示するには、メッシュ・テクスチャ・マテリアル・アニメーション等がクライアント側で使える形にならない。



Unity AssetBundle

モデル、テクスチャ、Prefab、音声等の非コードアセットを実行時にロードする仕組み

ネットワーク配信、キャッシュ、ランタイムロードを前提として設計されている

ダウンロード後にキャッシュされる場合がある（LZMAやLZ4圧縮）



OWASP Mobile Security

リバースエンジニアリング対策は耐性を上げるものであって、100%の効果を保証するものではない

攻撃者が端末を完全に制御できる場合、十分な時間と資源があれば、防御は最終的に迂回される

見せる以上、何らかの形で渡っている。

渡る以上、観測される可能性がある。

観測される以上、完全秘匿は難しい。

暗号化の効く場所・効かない場所



暗号化が有効な場面

- 通信経路の盗聴を防ぐ
- サーバー上の保管データを守る
- 正規ではないクライアントに鍵を渡さない
- 短命トークンでダウンロードURLを制御する



暗号化の限界

クライアントがアバターを表示するなら、最終的にクライアント側で復号される

復号鍵を一切渡さなければ表示できない

表示できるなら、表示に必要な情報はクライアント側に存在する

暗号化は「配送中や保存中」には有効だが、「正規ユーザーのクライアントが表示している瞬間」には弱い。VRChatの文脈では、暗号化は主役ではなく補助線になる。主役は「そもそも誰に、どの版を、どの場所で見せるか」。

DRMとリモートレンダリング



映像DRM (EME / CDM)

映像の場合は、再生パイプラインを比較的閉じやすい

しかし3Dアバターはメッシュ・テクスチャ・ボーン・表情・マテリアルがあり、リアルタイムに変形する

単なる動画ストリームより、クライアント側で扱うデータ構造がずっと豊か



リモートレンダリング

サーバー側で3D空間を描画し、クライアントには映像だけを送る方式

NVIDIA CloudXRのようなXRストリーミング基盤が例として挙げられる

元のメッシュやテクスチャをクライアントに渡さずに済む

VRChat日常利用での課題

遅延

VRはフレーム遅延への感度が高い

コスト

サーバーGPU資源のスケールが必要

互換性

既存クライアントとの整合が取れない

映像キャプチャ

映像として送っても画面録画は残る

VRChat公式の技術的対策



Easy Anti-Cheat (EAC)

抑止

改造クライアントをブロックする。アセットを暗号化して守る仕組みではなく、改造クライアントを使った不正行為のコストを上げる抑止策として機能する。



Secure Instances

露出制限

インスタンスの参加ルールをサーバー側で強制する。リンクを知っているだけでは入れず、実際に参加条件を満たしている必要がある。アセットそのものを守るというより、露出する相手を制限する対策になる。



規約 / Community Guidelines

文化的境界

リバースエンジニアリング、改造、コードインジェクション、anti-tamper回避、User Contentのharvest/mine/データ抽出等を禁止している。技術的防止ではないが、共同体の境界として機能する。

VRChatでやってはいけない対策

リッピング対策の名目で避けた方がよいこと

- クライアント改造に依存する対策を入れる
- 規約違反になりうるツールを使用する
- 他人に怪しいツールの導入を要求する
- アップロード後のアバターに、VRChatが想定しない実行時保護を無理に仕込む

なぜ危険なのか

- Community Guidelinesでアプリの改造やanti-tamper回避が禁止されている
- セキュリティのために規約違反に寄ると、守りたいはずのクリエイター自身が危険になる
- SDK更新・クライアント更新で壊れる。パフォーマンス悪化や購入者環境での動作不良が起きる
- 結果としてサポート負担が増え、長期運用に耐えない

対策 1 : Publicに置くものを減らす

Publicは文化的には開かれた場所で、出会い・拡散・イベント・展示といった良さがある。
しかしセキュリティ的には「知らない人に見せる場所」であり、かなり強い露出になる。

強い露出

高価値な完全版アバターをPublicに置く
全ギミック・高解像度テクスチャ・全パーツ
が揃った状態での公開

露出を下げる運用

Publicには宣伝用・試着用・軽量版・制限版を
置く
本番版や販売版はPrivateや限定インスタンスに
寄せる

この切り分けが一番効果が大きい対策になる。暗号化に比べて実装コストが低く、VRChatの標準機能だけで完結する。

対策 2：インスタンス設計で守る

Friends、Friends+、Invite、Group、Secure Instancesは単なる交流機能ではなく、露出制御の手段として使える。

インスタンス種別	参加条件	セキュリティ上の特性
Public	誰でも参加できる	露出が最も強い。高価値アセットには向かない
Friends+	フレンドのフレンドまで	範囲はやや広いが、Public より絞れる
Friends	直接のフレンドのみ	信頼関係のある範囲に限定できる
Invite+	招待＋リクエスト承認	主催者がゲートキーパーになれる
Group	グループメンバー限定	コミュニティ単位での制御が可能

「盗めないようにする」よりも「見せる相手を絞る」という発想が重要。
販売前の新作はInvite系やGroup系にする。イベント展示では見せる版を展示用にする。

対策 3： 見せる版の価値を分ける

アバターには完成版・試着版・Quest版・fallback版・宣伝用版など複数の形態がある。
これらを全部同じ価値にしない、という考え方。

完成版

全ギミック・高解像度テクスチャ・全パーツ

Private / 購入者のみ

試着版

一部ギミックを外す・機能を制限する

限定インスタンス

展示版

高解像度テクスチャや細かいパーツを減らす

イベント・展示会

宣伝用版

雰囲気は伝わるが、完全な製品価値は持たせない

Public

リッピングの被害は「盗まれたかどうか」だけでなく、盗まれたものにどれだけ価値が残っているかで変わる。

対策 4：標準機能に乗る

怪しいAntiRipツールよりも、VRChatの公式機能や文化的に受け入れられた運用の上で設計する。

EAC

改造クライアントの抑止

Secure Instances

露出範囲のサーバー側制御

Private avatar

公開範囲の制御

Creator Economy

プラットフォーム内の経済圏

Avatar Marketplace

標準導線での試着・購入

Group / Invite

コミュニティ単位の露出制御

プラットフォーム内販売 vs 外部販売

プラットフォーム内販売：自由度に制約はあるが、VRChatの標準導線に乗る。配布ファイル自体は渡らない。

外部販売：自由度は高いが、配布ファイルそのものが購入者に渡る。何を渡しているのかを理解する必要がある。

結論：暗号化ではなく露出設計として考える

対策の役割分担

暗号化	——— 配送の防御
EAC	——— 改造クライアントの抑止
Secure Instances	——— 露出範囲の制御
Private運用	——— 公開範囲の制御
試着版・展示版	——— 価値の制御

- 1 Publicに置くものを選ぶ。Publicは文化的には開かれた場所だが、セキュリティ的には強い露出になる。
- 2 試着会や展示会はインスタンス設計で守る。Friends、Invite、Groupは交流機能であると同時に露出制御になる。
- 3 見せる版の価値を分ける。完全版・試着版・展示版・Quest版・fallback版を同じ価値にしない。
- 4 怪しいAntiRipではなく、VRChatの標準機能に乗る。クライアント改造依存の防御は規約・互換性・サポートの面で問題がある。

誰に、どの版を、どの場で見せるかを設計する。それがVRChatに合ったリップニング対策の現実。