

技 術 的 保 護 格 差

— 非映像デジタルアセットの保護基盤に関する調査と政策提言 —

令和 8 年 8 月

デジタルアセット保護基盤検討委員会

Lycoris Studio

※本書の本文は、原則として 2026 年 8 月 28 日までに確認した資料に基づいています。

国際標準の策定状況、行政組織名、事業名、予算額は、その後変更されている場合があります。

※本書は、オンラインでのみ公開する文書です。書籍としての刊行は行いません。

※本書の利用条件、免責事項、更新履歴は、巻末の奥付に記載しています。

※本書に関するお問い合わせは、下記のお問い合わせフォームまでご連絡ください。

デジタルアセット保護基盤検討委員会公式ホームページ：<https://dcapic.jp/contact/>

※お問い合わせはデジタルアセット保護基盤検討委員会のお問い合わせフォームよりお願いいたします。

※運営元（Lycoris Studio）へ直接ご連絡いただいた場合、対応いたしかねますのでご了承ください。

目 的

本書は、日本のデジタルクリエイター産業において、コンテンツの種類と利用環境によって、権利者が現実利用できる技術的保護の厚みに体系的な差が生じている状況を検証し、その縮小に向けた政策提言を行うものです。

主な対象は、一般 Web 環境で表示、操作、流通又は提供される静止画像、イラスト、Live2D モデル、汎用 3D モデル、アバター、テクスチャ、モーション、ゲームアセット等の非映像デジタルアセットです。映像分野は、保護の仕組みがどのように接続され、運用されているかを比較する対象として扱います。

映画・映像の分野では、暗号化形式、標準 API、DRM 固有実装、信頼された実行環境、保護された媒体経路、鍵・ライセンス管理、出力保護、認証・適合性制度等が複数主体の運用を通じて接続されています。ただし、映像分野においてもコピーの完全防止が実現しているわけではなく、保護の保証は単一規格ではなく複数の実装、契約及び運用の組合せに依存します。

非映像分野にも保護技術は存在します。静止画像向けの暗号化・セキュリティ規格、権利・来歴メタデータ、アクセス制御、透かし、ネイティブ GPU の保護機構に加え、電子出版、積層造形、電子設計 IP 等には、暗号化、ライセンス又は利用制御を組み合わせた用途別の保護基盤があります。

本書が確認した課題は、一般 Web 環境において複数の非映像形式を横断し、形式、標準 API、信頼された実行・描画境界、鍵・ライセンス運用、保護出力及び適合性ガバナンスを接続する共通層を、本調査で確認した公開一次資料の範囲では確認できないことです。

本 書 の 中 心 概 念

本書は、技術的保護格差を次のように定義します。

技術的保護格差とは、コンテンツの種類と利用環境によって、権利者が利用できる技術的保護、信頼された実行・描画経路、ライセンス運用、適合性制度の厚みに体系的な差がある状態をいいます。

この格差は、暗号技術、透かし又は GPU 機能といった個別技術の有無だけを指すものではありません。保護に必要な複数の層がエンドツーエンドで接続され、個人クリエイターや小規模事業者を含む権利者が、費用と運用の面でも現実利用できる状態にあるかどうかの差を指します。

本書の検討は、当初の広い仮説から出発し、先行する規格、技術及び用途別基盤の存在を確認するたびに修正してきました。そのため、「非映像デジタルアセットには保護技術が存在しない」又は「非映像分野には統合的な保護基盤が一切存在しない」という主張は採用していません。仮説修正の経緯と最終的な中心命題は、第 1 章及び第 7 章に記載しています。

本書が提案しないこと

誤解を避けるため、本書が提案しないことを明示します。

1. すべての作品又はサービスに対する DRM の義務化
2. コピー又は不正利用の完全防止
3. 特定の製品、事業者、暗号方式又は実装方式の行政による指定
4. 開放的なファイル形式、既存ツール又は相互運用性の排除
5. 用途別に成立している既存の保護基盤の一律な置換
6. 保護技術へ参加しない権利者又は利用者の不利益な取扱い
7. 技術的対策だけによる法的救済、契約、削除要請又は事後対応の代替
8. 生成 AI と著作権をめぐる論点又は個別の著作物利用の適法性に関する一括評価

本書が求めるのは、任意参加、比例原則、相互運用性、透明性、プライバシー、アクセシビリティ、研究可能性及び長期保存を前提として、用途とリスクに応じて選択できる保護手段を増やすことです。正規利用への副作用、実装費用、運用費用及び社会的影響を、保護効果と同時に評価します。

五つの政策提言

本書は、特定技術の採用を先に決めず、次の順序で段階的に検討することを提案します。

1. 不正取得・再利用と対策費用の実態調査
2. 既存の保護基盤、技術的選択肢、限界の調査研究
3. 権利・来歴メタデータの相互運用と識別子照合の整備支援
4. 一般 Web・複数形式横断の要件定義と実証支援
5. 国際標準化と継続運用への参画支援

各段階では、必要性、既存基盤で対応できる範囲、実証結果及び社会的影響を判断します。被害又は対策費用が政策資源の投入に見合わない場合、既存基盤の適用で対応できる場合、効果と互換性を両立できない場合、又は副作用が比例的でない場合は、高介入の施策を拡大しません。提言の具体的内容、提言先、時間軸及び評価指標は第 9 章に記載しています。

調 査 の 方 針

本書は、政府・行政機関、国際標準化機関、標準化団体、仕様策定主体、公式レジストリ、事業者の公式技術文書及び査読付き学術論文を優先して確認しました。主要な事実関係には、各章の末尾で出典と URL を記載しています。

「確認できない」という記述は、調査基準日までに公開されていた仕様、公式レジストリ、政府資料、標準化団体の資料及びその他の公開一次資料を対象とします。非公開システム、契約者限定機能、未索引資料又は将来の仕様まで含む不存在を意味しません。

公開資料で確認できる事実と、本書が比較から導いた分析は区別しています。第 7 章の形成要因は、第 3 章で整理した成立条件と、第 4 章から第 6 章までの事例を用いて構成した説明仮説です。各要因の寄与を数量的に実証したのではなく、枠組みの外にある要因を網羅したものでもありません。

また、市場規模の拡大は、被害額又は将来の被害増加を直接証明しません。本書は、現時点で把握できない被害、対策費用及び正規利用への影響を、共通の方法で調査すること自体を第一の提言としています。

規格の状態、製品仕様、行政組織名、部署名、事業名及び公開 URL は変更される場合があります。提出、公開又は引用の時点で、最新の状態を再確認してください。

想 定 す る 読 者

読者	推奨する読み方
行政機関、政策担当者	第 1 章、第 7 章、第 8 章、第 9 章、第 10 章 上記章を読み、必要な根拠を第 2 章から第 6 章で確認する
クリエイター、権利者 サービス事業者	第 1 章、第 5 章、第 6 章、第 8 章、第 9 章を読む
技術者、研究者 標準化関係者	第 3 章、第 4 章、第 6 章、第 7 章、第 8 章、第 9 章 上記の章を中心に読む
時間の限られた読者	本ファイル、第 1 章、第 9 章、第 10 章を読む

本書の構成

第1章は、問題設定、調査結果、中心命題及び五つの政策提言の全体像を示します。

第2章は、市場、流通、権利者、Web プレビュー、被害統計及び生成 AI に関する調査範囲を整理します。

第3章は、映像分野において、暗号化、標準 API、信頼境界、ライセンス及び適合性運用がどのように接続されているかを検証します。

第4章は、静止画像、汎用規格、GPU 保護機構、電子出版、積層造形、電子設計 IP、Live2D モデル、3D モデル等について、既存技術と用途別基盤を棚卸しします。

第5章は、Web プレビューに必要な表示と、再利用可能な構造データの保護を両立する難しさを事例から検討します。

第6章は、データ最小化、アクセス制御、信頼された実行環境、透かし、監視等の既存対策について、それぞれが防げるものと防げないものを整理します。

第7章は、技術的保護格差を定義し、コンテンツ類型間の比較と形成要因の分析を行います。

第8章は、任意参加と相互運用性を前提とする次世代保護基盤の設計原理、機能層及び段階的な実現経路を示します。

第9章は、実施原則、判断ゲート、五つの政策提言、提言先及び評価指標を示します。

第10章は、調査で確認できた結論と、各主体が取り得る行動を整理します。

第11章は、本書で用いる主要な概念、規格、技術及び政策用語を整理します。

第12章は、第1章から第10章までで参照した資料を横断的に一覧化します。

第13章は、本書に掲載する図及び主な整理項目の掲載箇所を示します。

第14章は、書誌情報、利用条件、免責、訂正方針、連絡先及び更新履歴を示します。

用語と出典の読み方

本書は、暗号化、DRM、アクセス制御、電子透かし、権利・来歴メタデータ、ライセンス管理、信頼された実行環境及び適合性制度を、目的と保証範囲の異なるものとして区別します。例えば、来歴情報の目的をコピーの完全防止として評価したり、伝送時の暗号化だけで復号後の利用まで保護できると評価したりしません。個別の用語と技術的な責任分界は、主に第3章、第4章、第6章及び第11章で説明しています。

出典番号は各章のファイル内で完結しています。番号が同じでも、別の章では異なる資料を指す場合があります。各章末の「出典」と「本章の記述に関する注記」は、確認範囲、推論の限界及び例外を示すため、本文と一体として参照してください。

内容

第1章 エグゼクティブサマリー	12
要旨	12
1-1 問題の所在	12
1-2 なぜ今か	12
1-3 検証の結果 — 当初の仮説は修正されました	13
1-4 空白の所在	13
1-5 なぜ個別対応で解決しないのか	14
1-6 五つの提言	14
1-7 本書が求めないこと	15
1-8 日本にとっての意義	15
出典（第1章）	16
本章の記述に関する注記	17
第2章 デジタル著作物を取り巻く環境	18
2-1 クリエイターエコノミーと非映像デジタルアセット市場	18
イラスト・Live2D モデル・3D モデルの流通	18
この市場の担い手	18
日本が先行する領域	18
2-2 WEB インタラクティブプレビューの普及	18
なぜプレビューが必要か	18
技術的な前提	19
現行の運用	19
2-3 海賊版被害の現状と、統計上の空白	19
全体の被害規模	19
対象カテゴリに含まれないもの	19
他の統計でも確認できません	19
政策文書における言及	20
この空白が意味すること	20
統計の非対称性 — 類型によって「見えている度合い」が違います	20
海外における認識	20
2-4 生成 AI 時代における原本データの価値の変化	21
出典（第2章）	21
本章の記述に関する注記	22
第3章 映像分野における技術的保護基盤	23
3-1 まず用語を区別する	23
3-2 共通暗号化 — CENC は DRM ではない	23
3-3 標準 API と信頼境界 — EME と CDM	24
EME 標準化への異論	24
3-4 ハードウェアによる隔離	25
3-5 それでも防げないもの	25
3-6 この基盤の成立を支えた七つの条件	26
出典（第3章）	28

本章の記述に関する注記	29
第4章 非映像デジタルアセットにおける保護の現状	30
4-1 配信アーキテクチャの共通構造	30
4-2 既に存在する規格の棚卸し	30
4-2-1 静止画像には複数の現行規格が存在します	30
4-2-2 メディア形式に依存しない汎用の保護規格も存在しました	31
4-2-3 GPU レベルの保護機構も存在します	32
4-2-4 用途別には統合された保護基盤が存在します	32
4-2-5 小括 — 部品と用途別基盤は存在します	32
4-3 なぜ接続されなかったのか	33
4-3-1 条件②標準インターフェース — 形式規格と Web API の分離	33
4-3-2 条件③厳密な信頼境界 — 実装側へ委ねられた領域	33
4-3-3 条件⑥適合性ガバナンス — 制度は設けられたが、保存公開一覧に登録項目が表示されていない	34
4-3-4 条件⑤経済的アンカー — 横断的な要求主体を確認できない	34
4-3-5 小括 — 空白の所在	35
4-4 類型別の現状	36
4-4-1 静止画像 — 表示物と原本の距離が近い類型	36
4-4-2 Live2D モデル — 事業者の設計努力と、その先にある構造的限界	37
4-4-3 3D モデル・アバター — オープン性という設計思想との緊張	38
4-4-4 ゲーム・制作アセット — 公式ドキュメントが認める限界	39
4-5 原本と表示物 — 映像との本質的な差異	40
4-5-1 原本は生産財である	40
4-5-2 映像との比較	40
4-5-3 表示物の層に関する留意点	41
4-6 空白の所在	41
出典（第4章）	42
本章の記述に関する注記	46
第5章 ケーススタディ — WEB プレビューの構造的ジレンマ	47
5-1 プレビューは、欠かすことのできない機能です	47
5-2 先進事例 — 目的別のデータ分離という設計	47
5-3 「DRM 機能はありません」という明示	48
5-4 個社の努力が届かない領域	48
5-5 本章の結論	49
出典（第5章）	50
本章の記述に関する注記	50
第6章 既存対策の効果と限界	51
6-1 六つの分類	51
6-2 各分類の検討	51
A 渡さない	51
B 価値を下げる	52
C 取得主体を限定する	52
D 実行環境を信頼する	52
E 事後に追跡する	53

F 異常を検知する	54
6-4 本章の結論	1
出典（第6章）	1
本章の記述に関する注記	2
第7章 「技術的保護格差」の定義と分析	3
7-1 定義	3
7-2 コンテンツ類型別の比較	1
表 1-A 保護層の充足状況	1
表 1-B 保護の便益に関わる性質	2
7-3 なぜ格差が生じたのか	1
7-3-1 技術的困難だけでは説明できません	1
7-3-2 要因1 需要側アンカーの有無	2
7-3-3 要因2 利用環境の集中と分散	2
7-3-4 要因3 標準化における設計選択	2
7-3-5 要因4 制度運用層を支える主体の有無	2
7-3-6 要因5 オープン性という設計思想との緊張	3
7-4 本章の結論	3
出典（第7章）	4
本章の記述に関する注記	4
第8章 次世代デジタルアセット保護基盤の構想	6
8-0 本章が提案しないこと	6
教訓1 CCCD の失敗	6
教訓2 EME 標準化への異論	6
教訓3 開放性をもたらしてきた便益	6
8-1 五つの設計原理	7
原理1 既存の層を分離して捉え、必要な接続だけを標準化する	7
原理2 任意参加と比例原則を採用する	7
原理3 相互運用性、可搬性、フォールバックを確保する	7
原理4 保護水準を段階化し、多層防御として組み合わせる	7
原理5 制度運用、透明性、プライバシーを技術と同時に設計する	7
8-2 一般 WEB・複数形式横断の共通層	8
層1 暗号化と安全なパッケージング	8
層2 識別子、権利・利用条件、来歴	8
層3 Web 標準 API	8
層4 信頼された実行・描画と出力制御	8
層5 ライセンス、適合性、失効、ガバナンス	8
8-3 段階的な実現の道筋	9
第1段階 低介入の相互運用基盤	9
第2段階 対象別プロファイルと実証	9
第3段階 国際標準化と継続運用	9
8-4 多層防御という考え方	9
8-5 構想が実現しない場合への備え	11
8-6 本章の結論	11

出典（第8章）	11
本章の記述に関する注記	12
第9章 政策提言	13
9-1 なぜ政策の関与が必要か	13
理由1 判断の基礎となるデータと共通指標が不足しています	13
理由2 相互運用と制度運用は個社だけでは形成されにくい課題です	13
理由3 Web 標準と国際標準は国内の個社だけでは成立しません	13
9-2 標準化と継続運用から得られる示唆	13
JPSEC 登録制度の変遷	13
ISO/IEC 24216-1:2026 の経験	14
9-3 政策実施の原則と判断ゲート	14
9-4 五つの提言	14
表3 政策提言の全体像	14
提言1 不正取得・再利用と対策費用の実態調査	15
提言2 既存の保護基盤、技術的選択肢、限界の調査研究	15
提言3 権利・来歴メタデータの相互運用と識別子照合の整備支援	15
提言4 一般 Web・複数形式横断の要件定義と実証支援	16
提言5 国際標準化と継続運用への参画支援	16
9-5 提言先別の役割	16
内閣・知的財産戦略本部	16
経済産業省	17
文化庁	17
文部科学省	17
総務省・デジタル庁等	17
9-6 政策評価指標	17
9-7 想定される反論への応答	17
反論1 CCCD の失敗を繰り返すのではないか	17
反論2 保護機構は開放的な 3D エコシステムを損なうのではないか	17
反論3 3D データの技術的保護は原理的に不可能ではないか	18
反論4 政府が技術を選ぶべきではないのではないか	18
反論5 法的救済と削除要請を優先すべきではないか	18
9-8 本章の結論	18
出典（第9章）	19
本章の記述に関する注記	20
第10章 結論	21
10-1 本書が明らかにしたこと	21
1 非映像分野にも技術要素と用途別の統合基盤があります	21
2 空白は、一般 Web・複数形式を横断する共通保護層にあります	21
3 技術的保護格差は、技術の有無ではなく接続と利用可能性の差です	21
4 格差の要因は、技術だけでは説明できません	21
5 原本又は再利用可能な構造データが配信される領域では、別の設計が必要です	22
10-2 放置した場合に残る課題	22
10-3 それぞれの立場で可能なこと	22

クリエイターと権利者	22
サービス事業者	22
標準化団体と実装者	23
研究者	23
行政	23
10-4 本書が求めるもの	23
出典（第 10 章）	24
本章の記述に関する注記	24
第 11 章 用語集	25
11-1 目的の異なる技術	25
11-2 本書の中心概念	25
11-3 映像分野の保護技術	26
11-4 静止画像、権利情報及び来歴	27
11-5 用途別及び形式非依存の保護基盤	28
11-6 WEB、3D 及び GPU	29
11-7 LIVE2D 及び WEB プレビュー	29
11-8 個別の対策技術	30
11-9 政策及び標準化	31
第 12 章 参考文献一覧	32
12-1 政府・行政機関	32
12-2 国際規格・標準仕様・業界仕様	33
12-3 企業・サービス・実装資料	39
12-4 学術論文・研究資料	44
12-5 保存資料・その他	45
12-6 原典確認と参照上の留保	46
第 13 章 図表一覧	47
13-1 図	47
13-2 番号付きの表	47
13-3 本文中の主な整理項目	47
13-4 図の利用上の注意	48
13-5 表の利用上の注意	48
第 14 章 奥付	49
14-1 利用条件	49
14-2 引用・紹介に関するお願い	49
14-3 免責及び調査上の限界	49
14-4 訂正方針	50
14-5 お問い合わせ	50
14-6 関連文書	50
14-7 更新履歴	50
14-8 書誌情報	50

第1章 エグゼクティブサマリー

要旨

映画・映像の分野では、暗号化、標準 API、セキュアな実行環境、ライセンス管理、適合性審査、法的裏付けを組み合わせた成熟したコンテンツ保護のエコシステムが成立しています。

一方、本書が主な対象とする一般 Web 環境では、静止画像、Live2D モデル、汎用 3D モデル、アバター、テクスチャ、モーション、ゲームアセットを横断する同等の共通保護層を、本調査で確認した公開一次資料の範囲では確認できませんでした。

ただし、非映像分野全般に保護基盤がないわけではありません。電子出版、積層造形、電子設計 IP、企業内情報保護等には、暗号化、ライセンスまたは利用制御を組み合わせた用途別の基盤が存在します。また、暗号化の国際規格、権利表現の国際規格、GPU レベルの保護機構も確認できました。

課題は、用途や実装環境を越えて利用できる形で、形式、Web 標準 API、信頼された実行・描画境界、鍵・ライセンス運用、保護出力、適合性ガバナンスが接続されていないことにあります。本書の分析では、その要因は技術だけでなく、需要側主体、費用負担、継続運用等の経済的・制度的条件にも及びます。

本書は、この状態を「技術的保護格差」と定義し、その解消に向けた五つの政策提言を行います。

1-1 問題の所在

現在一般的な Web ブラウザやアプリケーション上でデジタルアセットを表示・操作する場合、レンダリングに必要な構造データをクライアント環境で処理する必要があります。3D モデルのスキニングや物理演算、Live2D モデルの表情変形は、モデルの構造データを参照しなければ実行できないためです。

商用映像配信では、視聴アプリケーションが復号後のフレームを直接操作しなくても再生を成立させられます。EME は HTMLMediaElement と鍵システムを接続する標準 API であり、強い信頼境界は、DRM 固有の CDM、User Agent による制約、TEE や secure media pipeline、出力保護、堅牢性規則等を組み合わせた実装によって形成されます。EME 単体が復号後データの隔離を一律に保証するわけではありません[8][21]。

これに対し、一般 Web 環境で複数形式のインタラクティブなアセットを同じ保護経路へ接続する標準 API と、エンドツーエンドの信頼境界は、本調査で確認した公開一次資料の範囲では確認できませんでした。

そして、この差は単なる技術的な差に留まりません。映像を画面から取得して得られるのは、通常、配信用データからさらに変換された視聴用のコピーです。一方、本書が対象とするデジタルアセットには、制作・販売に用いる原本データと、表示・プレビューに用いる派生データという区別があります。プレビュー用データが販売用データから分離・縮退される場合もありますが、Live2D モデルの構造、3D モデルのメッシュやリグ、テクスチャ等、表示と操作に必要な再利用可能データをクライアント側で処理する点は変わりません。これらは、取得後に改変し、別の作品へ組み込み、再演し、再販売できる素材になり得ます。

映像にも、撮影素材や保存用マスターといった制作原本は存在します。しかし、一般的な映像配信において、それらを視聴者の端末へ渡す必要はありません。送られるのは配信用に符号化された断片であり、原本は制作側に留まります。

差は「原本が存在するか」ではなく、「利用目的を達成するために、再利用可能な構造データをクライアント側で処理する必要があるか」です。映像は制作原本を渡さずに視聴を成立させられます。インタラクティブなアセットでは、表示・操作に必要な構造データを処理経路から完全に外すことができません。

再利用可能な構造データがクライアント側の処理経路に現れるにもかかわらず、一般 Web・複数形式を横断する共通保護層を確認できないこと。これが本書の中心的な問題意識です。

1-2 なぜ今か

第一に、市場が急速に拡大しています。ピクシブが公表した資料によれば、BOOTH の 3D モデルカテゴリにおける 2025 年の取扱高は約 104 億円、注文件数は約 774 万件であり、2023 年の約 31 億円から 2 年間で 3 倍以上に拡大しています[1]。

第二に、被害の実態を示すデータを確認できません。経済産業省が 2026 年 1 月に公表した日本発コンテンツの海賊版被害額調査において、デジタルコンテンツの区分は映像、出版、音楽、ゲームの四つです[2]。静止画像素材、Live2D モデル、3D モデル、アバター、テクスチャ、モーションは、独立したカテゴリとして設けられていません。なお同調査は、2025 年の回においてオンライン上の偽キャラクターグッズを新たな調査対象に加えており、調査対象の拡張には前例があります[2]。

第三に、政策文書における明示的な位置づけを確認できません。知的財産推進計画 2026 について、本調査の範囲では「アバター」「デジタルアセット」「技術的保護手段」「電子透かし」「3D モデル」といった語の使用を確認できませんでした[3]。「メタバース」の語は 2 箇所で使用されていますが、いずれも技術的保護の文脈ではありません。

第四に、日本はこの領域で国際的に先行する立場にあります。2026 年 5 月、日本が主導したアバターに関する国際規格 ISO/IEC 24216-1:2026 が発行されました[4]。国際標準化の場において、日本がこの分野で議論を主導し得ることは既に実証されています。

市場は拡大し、日本は先行しています。しかし、何がどれだけ失われているかを示すデータがありません。この状態が、判断と対応の遅れを生んでいます。

1-3 検証の結果 — 当初の仮説は修正されました

本書の検討は、「非映像デジタルアセットには保護のための技術も規格も存在しない」という広い仮説から出発しました。

調査の結果、この仮説が事実と反することが判明したため、仮説を修正しました。

- 映像分野の共通暗号化規格である CENC は、2023 年発行の第 4 版において画像アイテムを対象に含めています[5]
- JPSEC (Secure JPEG 2000) は、静止画像符号化方式である JPEG 2000 向けのセキュリティ規格であり、2023 年に改訂された第 2 版が現行版です[6]
- JPEG ファミリー全般を対象とする ISO/IEC 19566-4 も現行規格として存在します
- 積層造形には 3MF Secure Content と Materialise Identify3D があり、暗号化した製造データを認可された機器やワークフローへ接続する実装が存在します[13][15]
- 電子出版には Radium LCP があり、出版物の暗号化、ライセンス文書、利用条件、署名、状態管理等を組み合わせています[14]
- 電子設計 IP には IEEE 1735-2023 があり、設計情報の暗号化、利用権、ライセンス検証、信頼モデルを規定しています[16]
- 形式に依存しない標準 DRM として、写真とゲームを明示的に対象に挙げた OMA DRM が実在し、日本の端末にも実装されていました
- MPEG にも知的財産管理保護と権利表現言語の規格があり、いずれも廃止されていません
- GPU レベルでは、Vulkan 1.1 以降のコア仕様に保護メモリ機構が含まれます。ただし、実装による対応はオプションです[7]

したがって、非映像分野全般について保護技術や統合例の不在を主張することはできません。用途別の基盤と構成要素は既に存在します。（詳細は第 4 章）

1-4 空白の所在

用途別の基盤が存在する一方、一般 Web 環境で静止画像、Live2D モデル、汎用 3D モデル、アバター、テクスチャ、モーション、ゲームアセットを横断する共通保護層は、本調査で確認した公開一次資料の範囲では確認できませんでした。

不足を、暗号アルゴリズムまたは GPU 能力の不在だけに還元することはできません。個別の暗号化形式やネイティブ GPU 機構は存在しますが、複数形式に共通する保護形式または接続方式、Web 標準 API、信頼された実行・描画境界、鍵・ライセンス運用、保護出力、経済的アンカー、適合性ガバナンスが、エンドツーエンドの仕組みと

して接続されていません。

これは抽象的な指摘ではなく、公開仕様上の境界として示すことができます。W3C の Encrypted Media Extensions における鍵システム的能力指定は audioCapabilities と videoCapabilities で構成され、画像・3D メッシュ・汎用アセットに対応する能力項目は、2026 年時点の Working Draft に定義されていません[8]。また、WebGL の現行拡張一覧と glTF の正式・開発中拡張一覧にも、保護メモリ、暗号化資産、DRM またはライセンス管理を共通化する拡張を確認できませんでした[17][18]。

そして、この空白は認識されてこなかったのではありません。W3C には関連するコミュニティグループが三つ存在しましたが、いずれも閉鎖されています[19]。Khronos のコミュニティフォーラムには議論が残り、OpenUSD 側では 2026 年 5 月に知的財産保護に関する Draft 提案が提出されました。ただし、同提案は 2026 年 8 月 28 日時点で審議中であり、DRM、暗号方式、具体的なアクセス制御をスコープ外としています[20]。

問題は繰り返し認識され、複数の場で検討されてきましたが、本書が対象とする一般 Web・複数形式横断の共通保護層としては結実していません。（詳細は第 4 章、第 7 章）

1-5 なぜ個別対応で解決しないのか

事業者は、既に利用可能な対策を組み合わせています。目的別のデータ分離、プレビュー用データの縮退、アクセス制御、利用条件の明示等です。

しかし、個社が到達できる範囲には限界があります。標準 API、信頼境界、ハードウェア隔離は、ブラウザ、OS、GPU の各ベンダーの領域であり、一事業者が単独で構築できるものではありません。

そして、本書の分析で重要な仮説の一つが、一般 Web・複数形式横断の共通実装を継続的に求める需要側アンカーを確認できないことです。

映像分野では、コンテンツを供給する側や DRM 事業者が保護要件を仕様・契約として策定し、端末・プラットフォーム側が対応を進めてきました。非映像デジタルアセットの権利者は、個人クリエイター、小規模スタジオ、中小事業者に広く分散しています。その総体が相当規模の市場を形成していても、それだけで共通要件を形成し、実装を継続的に促す主体が成立するとは限りません。

便益が広く分散し、実装・運用費用が特定の主体に集中し得る構造です。この仮説を検証するには、便益、費用、需要主体を対象とする実態調査が必要です。（詳細は第 5 章、第 9 章）

1-6 五つの提言

#	提言	主な提言先	時間軸
1	不正取得・再利用と対策費用の実態調査	経済産業省、文化庁	短期
2	既存の保護基盤、技術的選択肢、限界の調査研究	文化庁、経済産業省	短期
3	権利・来歴メタデータの相互運用と識別子照合の整備支援	文化庁、経済産業省 知的財産戦略本部	短中期
4	一般 Web・複数形式横断の要件定義と実証支援	経済産業省、文部科学省	中期
5	国際標準化と継続運用への参画支援	経済産業省 知的財産戦略本部	長期

提言 1 がすべての前提となります。被害額が不明であること自体が政策課題です。現状では、この分野に政策資源を投入すべきか否かを判断するための基礎データが欠けています。

提言 3 は、DRM の導入を求めません。文化庁は 2026 年 2 月から、分野横断権利情報検索システム及び個人クリエイター等権利情報登録システムを運用しています[9]。提言 3 は新たな中央データベースの創設を直ちに求めるものではなく、既存の公的基盤、民間サービス、ファイル内メタデータの関係を確認したうえで、必要な相互運用と識別子照合を検討するものです。

（詳細は第 9 章）

1-7 本書が求めないこと

誤解を避けるため、明示します。

本書は、デジタルアセットへの DRM の義務化を求めています。

2000 年代前半、日本の音楽業界はコピーコントロール CD を導入し、正規購入者の利便性を損なった結果、市場から排斥されました。この結末は、文化審議会著作権分科会の中間整理（2007 年）に記録されています[10]。利便性と相互運用性を損なう技術的保護は、市場によって排斥される。本書は、この教訓を無視した提案を行いません。

また、自由に読み書きできる仕様が普及したことが、制作環境の多様性と流通の拡大を支えてきたことも事実です。3D アセットの分野において、glTF に代表される開放性の思想が果たしてきた役割は、その最も明確な例です。本書は、開放性を制限すべきだと主張していません。開放性の便益とクリエイターの負担を、データに基づいて比較できる状態にすべきだと主張しています。

さらに、「コピーを完全に防止する技術」を求めるものでもありません。そのような技術は存在せず、成熟した映像分野においても、画面の撮影による取得は防げません。目指すべきは、不正取得の技術的・経済的コストを引き上げ、流出時に追跡可能とし、商業的な不正流通の誘因を削ぐことです。（詳細は第 8 章）

1-8 日本にとっての意義

この分野において、日本には二つの経験があります。

2000 年代、日本の特定非営利活動法人 Intellectual Resource Initiative（IRI）が、JPEG 2000 のセキュリティ規格である JPSEC の登録機関（JPSEC RA）を引き受けました。ISO による正式な指定を受け、登録の受け皿も整備されました[11]。一方、2023 年承認の ITU-T T.807 第 2 版では、登録機関に関する第 7 条が非推奨とされました[12]。公開資料だけから、登録の全期間の実績又は制度変更の原因を確定することはできません。

2026 年 5 月、日本は産業技術総合研究所を中核とする体制で、アバターに関する国際規格を成立させました[4]。継続的な検討体制と、それを支える組織が置かれていました。

JPSEC の事例は、仕様と登録機関の制度に加えて、利用状況、更新及び撤退を継続的に検証できる運用が必要であることを示します。ただし、公開資料から利用実績及び制度変更の原因を確定できないため、担い手の体制との因果関係をこの事例だけから断定することはできません。必要なのは、仕様の策定に加えて、需要、実装、費用負担、適合性確認、更新を継続的に支える体制です。

日本は、アバター、Live2D モデル、同人流通という、世界に先行する領域を持っています。その制作を担っているのは、多くの場合、個人か小規模な事業者です。

だからこそ、この課題は構造的であり、公共的です。

本書が求めるのは、用途別基盤と既存の技術要素を踏まえ、一般 Web・複数形式横断で必要な接続を検証し、その運用を継続的に支える主体を検討することです。

出典（第 1 章）

[1]:「BOOTH 3D モデルカテゴリ 取引白書 2026」ピクシブ株式会社, 2026 年 2 月 6 日.

<https://www.pixiv.co.jp/2026/02/06/110000>

「BOOTH 3D モデルカテゴリ取引白書 2025」ピクシブ株式会社, 2025 年 2 月 19 日（2023 年の取扱高に関する公式資料）. <https://inside.pixiv.blog/2025/02/19/114500>

[2]:「日本発コンテンツの海賊版被害額調査の結果を取りまとめました」経済産業省（委託：一般社団法人コンテンツ海外流通促進機構、再委託：PwC コンサルティング合同会社）, 2026 年 1 月 26 日公表（2026 年 5 月 22 日更新）.

<https://www.meti.go.jp/press/2025/01/20260126001/20260126001.html>

[3]:「知的財産推進計画 2026」知的財産戦略本部, 2026 年 6 月 12 日決定.

https://www.cas.go.jp/jp/seisakukaigi/titeki2/260612/keikaku_all.pdf

[4]:「アバターに関する国際規格が発行されました」経済産業省, 2026 年 6 月 29 日. 対象規格は ISO/IEC 24216-1:2026（ISO/IEC JTC 1/SC 35、2026 年 5 月発行）.

<https://www.meti.go.jp/policy/economy/hyojun-kijun/is/20260629.html>

[5]: ISO/IEC 23001-7:2023（第 4 版）, 2023 年 8 月 8 日発行. 序文（画像アイテムを対象に含める旨）。規範的条項の本文は無償公開の対象外のため未確認. <https://www.iso.org/standard/84637.html>

[6]: Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認.

<https://www.itu.int/rec/T-REC-T.807>

[7]: Protected Memory, Vulkan Documentation Project, Khronos Group.

<https://docs.vulkan.org/guide/latest/protected.html>

[8]: Encrypted Media Extensions 2, W3C Working Draft, 2026 年 7 月 7 日.

<https://www.w3.org/TR/encrypted-media-2/>

[9]:「『分野横断権利情報検索システム』及び『個人クリエイター等権利情報登録システム』の運用開始について」文化庁, 2026 年 2 月 26 日.

https://www.bunka.go.jp/koho_hodo_oshirase/hodohappyo/94333101.html

[10]: 文化審議会著作権分科会 私的録音録画小委員会「中間整理」文化庁, 2007 年 10 月 12 日. 第 49 頁および脚注 32.

https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/h1910_rokuon_chukan.pdf

[11]: Statement of IRI, JPSEC RA（特定非営利活動法人 Intellectual Resource Initiative）.

<https://www.jpsec-ra.jp/statement-of-iri/>

[12]: Recommendation ITU-T T.807 (V2), ITU-T, 2023 年. 第 7 条における JPSEC 登録機関への登録機構が非推奨とされたことを確認. <https://www.itu.int/rec/T-REC-T.807>

[13]: 3MF Secure Content Extension 1.0.2, 3MF Consortium.

https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf

[14]: Radium Licensed Content Protection 1.0.

<https://readium.org/lcp-specs/releases/lcp/latest>

[15]: Materialise Identify3D, Materialise.

<https://www.materialise.com/en/industrial/software/identify3d>

[16]: IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE 1735-2023. <https://standards.ieee.org/ieee/1735/7237/>

[17]: WebGL Extension Registry, Khronos Group. <https://registry.khronos.org/webgl/extensions/>

[18]: glTF Extensions, Khronos Group.

<https://github.com/KhronosGroup/glTF/tree/main/extensions>

[19]: Past Community Groups, W3C. <https://www.w3.org/community/groups/past/>

[20]: Separation of Concerns for IP Protection in USD, OpenUSD-proposals PR #107, 2026 年 5 月 14 日.
<https://github.com/PixarAnimationStudios/OpenUSD-proposals/pull/107>

[21]:MovieLabs Specification for Enhanced Content Protection, Version 1.4, MovieLabs.
https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.4.pdf

本章の記述に関する注記

- 本章は第 2 章から第 10 章までの内容を要約したものです。各主張の詳細な根拠は、該当する章を参照してください。
- 出典[2]、[3]、[9]、[12]は原典で確認済みです。ただし[3]については、特定の語の不使用を根拠とする記述を含みます。「確認できなかった」ことは「存在しない」ことと同義ではありません。
- 1-5 の要因分析は、第 3 章 3-6 で構成した七条件を分析枠組みとして用いた結果です。枠組みの外にある要因は、本書の検討範囲に入っていません。
- 1-8 の JPSEC に関する記述について、利用実績及び制度変更の原因は公開資料から確定できません。本書は、担い手の体制と制度変更との間に因果関係があると主張していません。
- 行政組織名、部署名、事業名は変更される可能性があります。提出時点での再確認を要します。

第2章 デジタル著作物を取り巻く環境

本章では、本書が対象とするデジタルアセットの流通環境と、その市場規模、被害の実態を確認します。

あらかじめ述べておくべきことがあります。本章で最も重要な発見は、市場規模を示す数値ではなく、被害の実態を独立して示す公的なデータを、本調査の範囲では確認できなかったことです。この点は2-3で詳述します。

2-1 クリエイターエコノミーと非映像デジタルアセット市場

イラスト・Live2D モデル・3D モデルの流通

日本では、個人クリエイターが制作したイラスト・静止画像素材、Live2D モデル、3D モデル、アバター、テクスチャ、モーションといったデジタルアセットが、オンラインマーケットプレイスを通じて日常的に取引されています。

その規模は、既に無視できない水準にあります。ピクシブが公表した資料によれば、同社が運営する BOOTH の 3D モデルカテゴリにおける 2025 年の取扱高は約 104 億円、注文件数は約 774 万件でした[1]。同カテゴリの取扱高は、2023 年に約 31 億円、2024 年に約 58 億円と推移しており、2 年間で 3 倍以上に拡大しています[1]。

関連する市場として、VTuber 市場があります。矢野経済研究所の調査によれば、VTuber 関連事業を展開する企業の売上高ベースで、2023 年度が 800 億円、2024 年度が 1,050 億円の見込み、2025 年度が 1,260 億円の予測とされています[2]。

なお、これらの数値を合算することはできません。BOOTH の数値はマーケットプレイスにおける取扱高であり、矢野経済研究所の数値は VTuber 関連事業を展開する企業の売上高です。算出の基準と対象範囲が異なります。本書は、両者を合わせた「非映像デジタルアセット市場の規模」を示す統計を確認できていません。

この市場の担い手

重要なのは規模だけではありません。この市場の担い手の構成が、後の章の議論に直結します。

イラスト、Live2D モデル、3D モデル、アバターの制作を担っているのは、多くの場合、個人のクリエイター、あるいは数名規模のスタジオです。流通を担うマーケットプレイスも、映像配信事業者のような巨大プラットフォームとは規模が異なります。

第7章では、この分散した構造を、一般 Web・複数形式を横断する共通保護層が形成されにくかった要因の一つとして分析します。これは公開資料から直接確認できる因果関係ではなく、本書の分析枠組みに基づく仮説です。

日本が先行する領域

イラスト、Live2D モデル、アバター、バーチャルキャラクターといった領域において、日本は国際的に先行する立場にあります。

このことは、国際標準化の場でも確認できます。2026 年 5 月、アバターに関する国際規格 ISO/IEC 24216-1:2026 が発行されました。経済産業省の発表によれば、同規格の原案は産業技術総合研究所内に設置された拡張体験デザイン協会および同協会が運営する国内検討委員会での議論を経て開発され、ISO/IEC JTC 1/SC 35 において国際規格化されたものです[3]。

日本がこの領域で国際規格を主導し得ることは、既に実証されています。

2-2 Web インタラクティブプレビューの普及

なぜプレビューが必要か

インタラクティブなアセットの品質は、静止画では伝わりません。

Live2D モデルであれば、表情がどう変化するか、口の開閉が自然か、髪や衣服の物理演算が破綻しないか、目線の追従が滑らかかといった要素が価値を決めます。3D モデルであれば、ポリゴンの流れ、リグの品質、モーション適用時の挙動が問題になります。これらは、実際に動かしてみなければ判断できません。

そのため、マーケットプレイスはブラウザ上で動作するプレビュー機能を提供しています。Live2D 社が運営する nizima では、作品詳細ページでモデルを表示するためのプレビュー用データが、販売用データとは別に用意される仕組みが公式に説明されています[4]。

技術的な前提

ブラウザ上で Live2D モデルを表示し、表情やモーションを動かすためには、その計算に必要なデータがクライアント環境に存在する必要があります。Cubism SDK for Web の公式解説は、モデルデータをバイト列として読み込んでモデルを生成する処理の流れを示しています[5]。

3D モデルについても同様です。頂点データ、テクスチャ、スキニング情報を参照しなければ、レンダリングも操作もできません。

ここに、本書が扱う構造的な問題があります。プレビューは品質確認に必要ですが、提供すればレンダリングに必要なデータをクライアント環境で処理することになります。販売用原本をそのまま配信する必要はなく、プレビュー用データの分離や縮退は可能です。それでも、表示と操作に必要な再利用可能データがクライアント側の処理経路に現れるという条件は残ります。この点は第 5 章で詳しく検討します。

現行の運用

こうした状況のもとで、事業者は利用可能な手段を組み合わせ対応しています。nizima では、販売用データとは別にプレビュー用データを用意する仕組みが説明されています[4]。また、ダウンロード可能な確認用データについては、確認用途に限定し、解像度を下げる等の対策をとることが推奨されています[6]。

一方で、BOOTH の公式ヘルプは、同サービスが DRM 機能を提供していないことを明記しています[7]。3D モデルカテゴリだけで年間 100 億円規模に達する取引が、プラットフォームによる DRM 機能を伴わずに行われています。

ここで区別が必要です。非映像分野全般に保護基盤がないわけではありません。電子出版の Radium LCP、積層造形の 3MF Secure Content および Materialise Identify3D、電子設計 IP の IEEE 1735 等、用途別の基盤は存在します[12][13][14][15]。本書が問題とするのは、一般 Web 環境において、イラスト、Live2D モデル、汎用 3D モデル等を横断して利用できる共通保護層を、本調査で確認した公開一次資料の範囲では確認できないことです。これは個別事業者の怠慢ではなく、一社の実装だけでは解消できない標準化と運用の課題です。

2-3 海賊版被害の現状と、統計上の空白

全体の被害規模

日本発コンテンツの海賊版被害については、経済産業省が調査を実施しています。2026 年 1 月に公表された調査によれば、デジタル分野における被害額は相当規模に達しており、前回調査から大きく拡大しています[8]。

しかし、本書にとって重要なのは、その金額ではありません。

対象カテゴリに含まれないもの

同調査のデジタルコンテンツの区分は、映像、出版、音楽、ゲームの四つです[8]。なお同調査は、2025 年の回においてオンライン上の偽キャラクターグッズを新たな調査対象に加えており、調査対象の拡張には前例があります[8]。

すなわち、次のものは独立したカテゴリとして存在しません。

- 静止画像素材、イラスト
- Live2D モデル
- 3D モデル、アバター
- テクスチャ、モーション
- 単体で流通するデジタル制作素材

「ゲーム」の区分に、単体で流通する 3D モデルやアセットが含まれるかどうかは、公開資料からは確認できません。含まれていると推定すべきではありません。

他の統計でも確認できません

本書の調査では、政府統計、警察統計、業界団体の公表資料を横断的に確認しましたが、非映像デジタルアセットの不正取得・無断再配布・無断再利用について、独立した公的統計または業界統計を確認できませんでした。これは公開資料を対象とした本調査の結果であり、非公開の事業者データまで含めた不存在を意味しません。

政策文書における言及

日本の最上位の知財政策文書である知的財産推進計画 2026 についても、本調査の範囲では、「アバター」「デジタルアセット」「技術的保護手段」「電子透かし」「3D モデル」といった語の使用を確認できませんでした[9]。「メタバース」の語は 2 箇所で使用されていますが、仮想空間のデザインを意匠制度でどう保護するかという検討と、人工知能や VR 等と並記された技術動向への言及であり、本書が対象とする技術的保護の文脈での言及は確認できませんでした。「3D」については、都市モデルに関する記述が確認できます[9]。

なお、本書はこれを政策の怠慢として批判するものではありません。被害の実態を示すデータを確認できない現状では、政策文書に明示的に位置づけられにくいことは、むしろ自然な帰結です。

この空白が意味すること

以上を整理します。

BOOTH の 3D モデルカテゴリは、2023 年から 2025 年までの 2 年間で取扱高が 3 倍以上に拡大しました。しかし、その市場を含む非映像デジタルアセットについて、何がどれだけ失われているかを独立して示す公的なデータは、本調査の範囲では確認できません。

独立した被害データを確認できないため、他分野との比較も、政策的な優先順位の判断も、その基礎を欠いています。そして、政策文書に位置づけられない領域は、調査の対象にもなりにくくなります。

この空白こそが、第 9 章で示す提言 1「不正取得・再利用と対策費用の実態調査」の直接的な根拠です。

統計の非対称性 — 類型によって「見えている度合い」が違います

ここで、本書自身の記述に関わる重要な事実を述べておきます。

本章で提示できた市場規模の数値は、BOOTH の 3D モデルカテゴリと、VTuber 関連事業を運営する企業の売上高の 2 点だけです。

イラスト・静止画素材の市場規模も、Live2D モデルの市場規模も、本調査では確認できませんでした。公的統計に加え、本調査で確認した事業者の公表資料にも、独立した市場規模を示す数値は見当たりませんでした。

この非対称性には理由があります。3D モデルについては、ピクシブが取引白書を公表し、Khronos Group や AOUSD といった標準化団体が保護をめぐる議論を公開し、VRChat が不正抽出について公式に言及し、中国では司法判断が公表されました。議論の材料が、外部から観測できる形で存在しています。

一方、イラストと Live2D モデルについては、Live2D 社と nizima の公式ドキュメントという一次資料はあるものの、市場規模の統計、被害の統計、標準化の議論、判例を、本調査の範囲では確認できませんでした。

この差は、実際の市場規模や被害の大きさを反映したものではありません。観測されているかどうかの差です。

そして、この状況は本書のような文書に構造的な偏りをもたらします。証拠のある類型について多く書き、証拠のない類型について少なく書くことになるためです。書き手が意識しなければ、「調べられていないものは論じられない」という循環が、文書の中で再生産されます。

本書はこの点を自覚し、以下の方針を採ります。

- 統計の不在を、記述量の少なさに反映させません。構造的な議論において、イラスト、Live2D モデル、3D モデル、ゲームアセットを同格に扱います
- 統計を確認できない場合は、その旨を明記します。推計や類推で埋めません
- 統計の不在それ自体を、政策課題として提示します

この非対称性は、第 9 章の提言 1（実態調査）の根拠の一部を構成します。海賊版被害額調査に非映像デジタルアセットの独立カテゴリがないことに加え、市場規模の統計すら類型によって偏在しているという事実は、この分野が政策的な観測の外に置かれてきた可能性を示唆します。

海外における認識

被害の実態が統計として把握されていないことと、問題が認識されていないこととは、別のことです。

VRChat は 2022 年のセキュリティ更新において、改造クライアントが利用者に無断でアバターの不正抽出とアーカイブ化を行っている実態を公式に指摘し、対策を導入しました[10]。プラットフォーム運営者自身による公式

の言及です。

司法判断も現れています。北京インターネット法院が公表した典型事例によれば、同法院は仮想デジタルヒューマンの形象について、制作チームによる独自の美学的選択と判断を体现するものとして独創性を認め、美術作品を構成すると判断しました。3D モデル販売サイトで実質的に類似するモデルを公開・販売した行為について、情報ネットワーク伝播権の侵害が認定されています[11]。

2-4 生成 AI 時代における原本データの価値の変化

最後に、近年の環境変化について限定的に触れます。

本書は、生成 AI と著作権をめぐる論争そのものには踏み込みません。この論点は独立した検討を要するものであり、本書の主題である技術的保護基盤の構造とは、扱うべき射程が異なるためです。

ただし、一点だけ指摘しておく必要があります。

第4章で述べるとおり、イラストの原本や、Live2D モデル、3D モデル、テクスチャ、モーション、ゲームアセットの原本データは、視聴して消費される映像とは異なり、改変し、別の作品に組み込み、再演し、再販売できる素材です。すなわち生産財としての性格を持ちます。

生成 AI の普及は、生産財としての用途に、新たな一つが加わりました。学習用データとしての利用です。

無断で取得されたアセットが学習データセットへ混入する可能性については、本書の調査範囲では、公的機関による定量的な把握を確認できませんでした。したがって本書は、その規模や影響について推測を述べません。

しかし、原本データが従来より広い用途で価値を持つようになったことは、実態調査の必要性を高める方向に作用します。第9章の提言1において、AI 学習用データセットへの取り込みの実態を調査対象に含めるべきとしているのは、この理由によります。本書は、AI 開発・学習段階における著作物利用の適法性について評価を行いません。著作権法第30条の4等をめぐる論点は、独立した検討を要するためです。調査すべきは、取得経路、許諾の有無、技術的なアクセス制限の回避の有無、および権利者の認識と負担です。

出典（第2章）

[1]:「BOOTH 3D モデルカテゴリ 取引白書 2026」ピクシブ株式会社, 2026 年 2 月 6 日.

<https://www.pixiv.co.jp/2026/02/06/110000>

「BOOTH 3D モデルカテゴリ取引白書 2025」ピクシブ株式会社, 2025 年 2 月 19 日（2023 年の取扱高に関する公式資料）. <https://inside.pixiv.blog/2025/02/19/114500>

[2]:「VTuber 市場に関する調査」株式会社矢野経済研究所, 2025 年 4 月 28 日（プレスリリース No.3806）.

https://www.yano.co.jp/press-release/show/press_id/3806

[3]:「アバターに関する国際規格が発行されました」経済産業省, 2026 年 6 月 29 日.

<https://www.meti.go.jp/policy/economy/hyojun-kijun/is/20260629.html>

[4]:「Live2D 作品の投稿」nizima (Live2D Inc.) . <https://docs.nizima.com/guide/item-upload/live2d/>

[5]:「モデルについて (Web)」Live2D Inc., Cubism SDK Manual.

<https://docs.live2d.com/4.2/en/cubism-sdk-manual/model-web/>

[6]:「クリエイター向けオーダーメイドガイド」nizima (Live2D Inc.) .

<https://docs.nizima.com/guide/creator-ordering/>

[7]:「DRM 機能（デジタル作品保護機能）はありますか？」BOOTH（ピクシブ株式会社）.

<https://booth.pixiv.help/hc/ja/articles/231284508>

[8]:「日本発コンテンツの海賊版被害額調査の結果を取りまとめました」経済産業省（委託：一般社団法人コンテンツ海外流通促進機構、再委託：PwC コンサルティング合同会社）, 2026 年 1 月 26 日公表（2026 年 5 月 22 日更新）.

<https://www.meti.go.jp/press/2025/01/20260126001/20260126001.html>

[9]:「知的財産推進計画 2026」知的財産戦略本部, 2026 年 6 月 12 日決定.

https://www.cas.go.jp/jp/seisakukaigi/titeki2/260612/keikaku_all.pdf

[10]:VRChat Security Update, VRChat Inc., 2022 年 7 月.

<https://hello.vrchat.com/blog/vrchat-security-update>

[11]:北京インターネット法院公表事例（一審：（2024）京 0491 民初 4936 号、二審：北京知識産権法院（2025）京 73 民終 603 号）の専用ページ。

https://english.bjinternetcourt.gov.cn/2025-10/29/c_819.htm

[12]:3MF Secure Content Extension 1.0.2, 3MF Consortium.

https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf

[13]:Radium Licensed Content Protection 1.0.

<https://readium.org/lcp-specs/releases/lcp/latest>

[14]:Materialise Identify3D, Materialise.

<https://www.materialise.com/en/industrial/software/identify3d>

[15]:IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE 1735-2023. <https://standards.ieee.org/ieee/1735/7237/>

本章の記述に関する注記

- 出典[2]の市場定義は原典で確認済みです。同調査の「VTuber 市場」は、国内の VTuber 事務所・プロジェクト運営企業の当該事業売上高（海外事業を含む）ベースで算出されたものであり、個人で活動する配信者の収益や、モデル制作素材の流通額を含むものではありません。
- 出典[8]および[9]は原典で確認済みです。ただし[9]については、特定の語の不使用を根拠とする記述を含みます。「確認できなかった」ことは「存在しない」ことと同義ではありません。
- 出典[8]について、同調査が 3D モデル・アバター等を独立した被害額カテゴリとして扱っていないことは原典で確認できますが、「ゲーム」区分の内訳にこれらが一切含まれていないことまでは確認できません。
- 出典[11]について、判決書の全文は一般に公開されておらず、当事者名は匿名化されています。本文の記述は、法院が公表した典型事例の紹介に基づくものです。
- 出典[4]および[6]からは、データ分離と解像度低減を確認しました。本調査が確認した nizima の現行公式資料では、SAMPLE 透かしや表示位置の時間変化を裏づける記述を確認できなかったため、同サービスの実装として本文に記載していません。
- 出典[12]から[15]は、非映像分野全般に保護基盤がないという意味ではないことを示す用途別先行事例です。本書の対象である一般 Web・複数形式横断の共通保護層と同一視しません。
- 2-1 で述べたとおり、本章に記載した各市場規模の数値は算出基準が異なるため、合算することはできません。
- 2-4 で述べたとおり、本書は生成 AI と著作権をめぐる論争そのものを検討対象としていません。

第 3 章 映像分野における技術的保護基盤

本章では、映画・映像配信の分野で成立している技術的保護の仕組みを整理します。これは映像分野を賞賛するためではなく、後の章で非映像デジタルアセットの状況を検討するための「比較の物差し」を用意するためです。

先に結論を述べます。映像分野の保護は、単一の優れた暗号技術によって成り立っているものではありません。暗号化の形式、標準 API、クライアント内の信頼境界、ハードウェアによる隔離、ライセンス管理、契約による適合性の強制、そして法的裏付けという複数の層が、それぞれ別の主体によって担われ、一つのエコシステムとして接続された結果として成立しています。この「層の分業と接続」という構造こそが、本書の中心的な観察対象です。

3-1 まず用語を区別する

コンテンツ保護をめぐる議論では、性質の異なる技術が「DRM」という一語にまとめられがちです。しかし政策を論じる際には、これらは目的も評価指標も異なるため、厳密に区別する必要があります。本書では以下のとおり用語を使い分けます。

用語	定義	何を達成するか
DRM	利用条件をクライアント側でも技術的に強制する仕組み	再生期限、出力解像度、デバイス数などの条件を実際に守らせる
暗号化	伝送中・保管中のデータを鍵なしには読めない形にする処理	秘匿。 ただしそれ自体は利用条件を強制しない
アクセス制御	データを取得できる主体を限定する仕組み	権限のない者による取得の防止
ウォーターマーク (電子透かし)	識別情報をコンテンツに埋め込む技術	流出後の追跡と抑止。 コピーの防止ではない
Provenance 来歴管理	出所・作成者・改変履歴を証明する仕組み	真正性の検証。 コピーの防止ではない
ライセンス管理	利用許諾条件を表現・記録・管理する仕組み	権利条件の機械可読な表現

この区別は形式的なものではありません。たとえば Provenance の成果を「防止できたコピーの件数」で評価することは、技術の目的を取り違えた誤りです。後の章で扱う各技術についても、この区分を常に明示します。

3-2 共通暗号化 — CENC は DRM ではない

映像分野の相互運用性を支える基礎は、MPEG Common Encryption (CENC) です。ISO/IEC 23001-7 として国際標準化されており、現行は 2023 年 8 月 8 日発行の第 4 版です[1]。

CENC について最初に確認すべきは、この規格自体は DRM システムを定義していないという点です。ISO による規格の説明は、複数のデジタル著作権管理・鍵管理システムが同一の共通暗号化ファイルまたはストリームにアクセスできるようにするためのメタデータを規定するものであり、「本文書は DRM システムを定義しない」と明記しています[1]。

では何を共通化したのか。暗号アルゴリズム (AES-128)、メディアサンプルへの暗号化の適用範囲、復号に必要な鍵識別子と初期化ベクトルの格納方法、そしてそれらを記述するメタデータ構造です[1]。

この共通化がもたらした帰結は決定的でした。従来、各 DRM システムは独自の暗号化形式を用いていたため、配信事業者は DRM ごとに別々の暗号化ファイルを作成・保管する必要がありました。CENC の導入により、一つの暗号化済みファイルに対して複数の DRM システムがそれぞれの方法で鍵を取得し、同じデータを復号できる構造が可能になりました。「コンテンツの暗号化」と「DRM 固有のライセンス取得・権限制御」がアーキテクチャ上分離されたのです。

CENC には複数の保護スキームがあり、実運用では cenc (AES-CTR モード) と cbcs (AES-CBC モードによるパターン暗号化) が中心です。パターン暗号化は第 3 版で追加されたもので、規格自体がその動機を、デバイスが

ビデオトラックを復号するために必要な計算能力の削減であると説明しています[1]。

この2方式は、同一の CMAF Presentation 内では相互に排他的です[2]。配信サービスが cenc 版と cbcs 版を併存させることは可能です。そして cbcs への収束は、各主体の対応の積み重ねとして進みました。Apple は HLS において FairPlay との互換性を保証するには METHOD=SAMPLE-AES を使う必要があり、これは CENC における cbcs 保護スキームに相当すると公式に説明しています[3]。Microsoft は、PlayReady 1.X~3.X が CTR モードのみを保護できたのに対し、4.0 以降で CBC モード (cbcs) に対応したとしています[4]。DASH Industry Forum は相互運用性ガイドラインで CMAF 対応のため cbcs を追加し、可能な場合は両方式で暗号化することを推奨しています[2]。CTA WAVE は再生互換性のため、cbcs 適用時のパターンを 1:9 とすることを必須要件としています[5]。

配信形式としては、MPEG-DASH (ISO/IEC 23009-1)、HLS (RFC 8216) [6]、そして両者の分断を統合するために策定された CMAF (ISO/IEC 23000-19) が用いられます。CENC と CMAF により、同一の暗号化メディア資産を複数の DRM で共用する構成が可能になりました。ただし、cenc と cbcs の対応差、レガシー機器、配信プロトコル、DRM 固有シグナリングの差が残るため、単一ファイルセットで主要 DRM を一律にカバーできるとは一般化できません。

なお、業界全体がいつ cbcs を既定としたかを宣言した単一の文書は存在しません。上記は各組織が個別に cbcs を追加・推奨・必須化していった記録の集積です。

3-3 標準 API と信頼境界 — EME と CDM

暗号化形式が共通化されても、それだけでは何も起きません。Web ブラウザがその暗号化コンテンツを扱えなければならず、そのための標準インターフェースが必要になります。それが Encrypted Media Extensions (EME) です。

EME は 2017 年 9 月 18 日に W3C 勧告となりました[7]。仕様は自らの位置づけを、HTMLMediaElement を拡張し、暗号化コンテンツの再生を制御する API を提供するものと説明しています[7]。

ここで二点、正確に理解すべきことがあります。

第一に、EME もまた DRM そのものではありません。EME は HTMLMediaElement と Key System を接続し、鍵システムの選択、セッション、ライセンスメッセージ、鍵状態を共通化する標準 API です。W3C は特定の商用 DRM を必須化せず、共通のベースラインとして Clear Key への対応のみを User Agent に求めました[8]。Clear Key は暗号化メディアを平文鍵で復号する簡易 Key System であり、追加のクライアント側保護を要求しません。

第二に、EME 単体が強い信頼境界を一律に保証するわけではありません。商用 DRM では、アプリケーションが DRM 固有メッセージを通常は解釈せずに転送し、鍵を CDM 内部で扱う構成が一般的です。一方、Clear Key では JSON/JWK と平文鍵がアプリケーション経路を通ります。復号後フレームを隔離する強い信頼境界は、DRM 固有 CDM、User Agent の制約、ライセンス条件、TEE、secure media pipeline、出力保護、適合性・堅牢性規則の組合せによって形成されます[7][8]。

したがって本書では、EME が担う標準 API の層と、個別 DRM・OS・ハードウェア・運用規則が形成する信頼境界の層を区別します。

なお、EME は 2017 年の勧告以降も保守・拡張が続いており、後継仕様「Encrypted Media Extensions 2」が策定作業中です。最新の Working Draft は 2026 年 7 月 7 日付です[9]。ただし 2017 年以降に追加された主な機能は暗号化スキームの能力検出 (encryptionScheme) と HDCP ポリシーに関する鍵状態の問い合わせ (getStatusForPolicy()) であり、対象範囲は一貫して HTMLMediaElement、すなわち音声と映像のままです。鍵システムの能力指定は audioCapabilities と videoCapabilities として定義されており、これ以外の種類のコンテンツに対応する項目は定義されていません[9]。この点は第 4 章で改めて取り上げます。

EME 標準化への異論

EME の標準化は、技術的には合理的でしたが、社会的には強い異論を伴いました。この経緯は、本書が政策を論じるうえで無視できません。

電子フロンティア財団 (EFF) などは、オープンであるべき Web 標準にクローズドな DRM 技術を組み込むこと

への正式な異議を提出しました。主な論拠は、米国 DMCA 等の技術的保護手段の回避禁止規定により、セキュリティ研究者による脆弱性調査や、新規参入者による互換実装の開発が法的に制限されうるという点でした[10]。EFF は、セキュリティ研究者や相互運用性を追求する開発者を提訴しないという誓約を W3C 会員に義務付けることを求めました[10]。

W3C は、会員投票（賛成 108、反対 57、棄権 20）を経て、誓約の義務化を退け EME を勧告化しました[8]。W3C が示した論拠は二点でした。第一に、プラグインに委ねられていた暗号化コンテンツとの通信をブラウザの管理下へ統合し、CDM のアクセスを必要最小限に制約することで、利用者のセキュリティとプライバシーを改善できるという点です。第三者 CDM をサンドボックス内で実行することは、仕様が挙げる実装方法の一つであり、CDM 一般の必須構成ではありません。第二に、W3C が EME を拒絶した場合、利用者はブラウザを離れ完全にクロードなネイティブアプリへ移行せざるを得ず、結果として Web というプラットフォームの価値が損なわれるという点です[8]。

この論争が示すのは、コンテンツ保護の標準化が純粋な技術問題ではなく、相互運用性・セキュリティ研究の自由・プラットフォームの開放性との間の政策的な選択を伴うということです。第 8 章および第 9 章で本書が提言を行う際も、この論点は回避されるべきではありません。

3-4 ハードウェアによる隔離

高価値の映像を保護する場合、ソフトウェアによる保護だけでは不十分とされ、ハードウェアレベルの隔離が要求されます。

Trusted Execution Environment (TEE) は、メインの OS から論理的・物理的に隔離されたプロセッサ内の安全な実行環境です。鍵の取扱い、ライセンスポリシーの検証、メディアの復号がこの内部で行われるため、メイン OS が侵害された状態でも鍵の漏洩を防ぐことが企図されています[11]。

Secure Video Path は、復号後の非圧縮映像データを保護されたメモリ領域に置き、一般のアプリケーションから読み取れない状態のままハードウェアデコーダを経てディスプレイへ転送する経路です[11]。HDCP は、デバイスから外部ディスプレイへ物理的に出力される際のケーブル上の暗号化を担い、DRM ポリシーは再生条件として一定の HDCP リンクの確立を要求できます[11]。

保護の強度は段階的に定義されます。ここで注意すべきは、公開されている一次資料の充実度が事業者によって大きく異なるという事実です。

Microsoft は、PlayReady のセキュリティレベルとして、ハードウェア手段によって資産と鍵が保護される SL3000、ソフトウェアまたはハードウェア手段で秘密情報を保護する SL2000、開発・テスト環境向けの SL150 を公式に定義しています[11]。Android は MediaDrm API において、鍵管理・暗号処理・デコード・メディア処理をすべてハードウェア裏付けの TEE 内で実行する SECURITY_LEVEL_HW_SECURE_ALL から、鍵管理にソフトウェアのホワイトボックス暗号を用いる SECURITY_LEVEL_SW_SECURE_CRYPTO まで、複数の水準を公式に定義しています[12]。

一方、業界で広く言及される Google Widevine の「L1/L2/L3」については、Android の計測 API に DRM_TYPE_WIDEVINE_L1 等の識別子が存在することは確認できるものの[13]、各水準の技術的要件を明文で定義した Google/Widevine の公開一次資料は、本調査の範囲では確認できませんでした。ただし、公開契約には secure boot、鍵と平文経路の保護、出力保護、TEE 等の堅牢性要件が記載されています[22]。これらを L1/L2/L3 へ個別に割り当てることはできません。

この事実自体が、映像分野の保護エコシステムの性格を示しています。すなわち、この仕組みは公開仕様だけで動いているのではなく、契約と適合性審査によって維持されているということです。実際、Microsoft は PlayReady のデバイス統合において、OEM に対しプラットフォーム移植、暗号アクセラレータ、ビデオ経路の実装、デバイス固有の秘密情報の設定、そしてコンプライアンスおよび堅牢性規則への適合検証までを要求しています[14]。

3-5 それでも防げないもの

映像分野の保護基盤を「完全なコピー防止」と理解することは誤りです。本書は、この点を明確にしておきます。

第一に、アナログホールです。画面に表示された映像をカメラで撮影する行為、スピーカーから出る音声を録音する行為に対して、デバイス内部の暗号化やハードウェア保護は構造的に無力です。

第二に、出力保護の回避です。HDCP はケーブル上の暗号化を提供しますが、これを解除して平文の映像信号を出力する機器が流通する場合があります。

第三に、ソフトウェア保護水準の解析です。ハードウェア TEE を用いない保護水準では、鍵や復号ロジックがソフトウェア層に存在するため、解析の対象となります。実際、Widevine の実装や EME 標準に関する形式的な安全性解析、およびブラウザ実装のプライバシー影響を検証した査読付き学術論文が公表されています[15][16]。

したがって、映像分野の保護基盤について正確な表現は以下のとおりです。

技術的保護手段は、無劣化かつ大量の不正複製を完全に防止する仕組みではありません。しかし、暗号化とハードウェア隔離の組み合わせにより、一般の利用者による安易な複製を著しく困難にし、不正取得に要する技術的・経済的コストを大きく引き上げることで、商業的な不正流通の誘因を削ぐ、相対的かつ実効性の高い防御層として機能しています。

3-6 この基盤の成立を支えた七つの条件

以上を踏まえ、映像分野で保護エコシステムが成立するために必要だった条件を七点に整理します。これは他分野への移植可能性を評価するための基準であり、第 4 章以降で繰り返し参照します。

- ① 共通暗号化フォーマット。単一の暗号化データに対して複数の DRM が共存できること。暗号化規格と DRM ロジックが分離されている状態を指します。CENC がこれを担いました。
- ② 標準インターフェース。プラットフォームに依存しない形で、アプリケーション層と保護モジュールの間の通信規約が標準化され、開発者が個別の DRM の内部実装を意識せずに済むこと。EME がこれを担いました。
- ③ 厳密な信頼境界。DRM 固有 CDM、User Agent の制約、OS、ハードウェア保護経路、ライセンス条件、堅牢性規則を組み合わせ、鍵と復号後データを非認可主体から隔離できること。
- ④ ハードウェア隔離。OS が侵害されても鍵が漏れず、復号後のデータが利用者領域のメモリに露出しない隔離実行環境が、民生用デバイスに標準搭載されていること。
- ⑤ 経済的アンカー。共通の保護水準を要求し、それを満たさない実装には価値を認めない主体が、継続的に存在したこと。

この条件については、記録が二つの側面を示しています。

一方では、コンテンツを供給する側が保護要件を策定し、公表しました。映画スタジオが設立した MovieLabs が公開する仕様は、高度なコンテンツ配信において、各スタジオが配信の前提条件となる機能要件を個別に決定する旨を明記しています[17]。W3C の Web & TV Interest Group がまとめた要件文書も、コンテンツ所有者は自らの権利が保護されなければ高価値コンテンツを制作・提供しなくなると述べ、権利保護を機能要件として列挙しています[18]。

他方では、この要件を満たさないプラットフォームが、市場での競争力を失う構造がありました。Mozilla は 2014 年、DRM で保護されたコンテンツがトラフィックの 3 割以上を占めるなかで、EME に対応しなければ利用者が他のブラウザへ移らざるを得なくなるとして、実装に踏み切った経緯を公式に説明しています[19]。Google が公開した技術文書も、EME をプレミアムコンテンツの配信者が自社の動画を保護できるようにするものとして説明しています[20]。

すなわち、供給側の要求とプラットフォーム側の投資は、対立する説明ではありません。要件が公表され、それを満たさない実装が市場から選ばれなくなるという構造を通じて、両者は接続されていました。

- ⑥ 適合性ガバナンス。厳格な適合性要件を伴うライセンス契約構造を通じて、コンプライアンスおよび堅牢性規則のような実装・運用の要件を、契約ベースで強制できたこと。
- ⑦ 法的裏付け。技術的保護手段の回避行為そのものを規制する法制度が存在したこと。

これらのうち、①と②は標準化団体が、③はブラウザベンダーが、④はチップセットと OS のベンダーが、⑤と⑥はコンテンツホルダーとプラットフォーマーが、⑦は各国の立法が担いました。七つの層が、それぞれ異なる主

体によって担われながら、一つのエコシステムとして接続されたのです。この全体の構造を図1に示します。

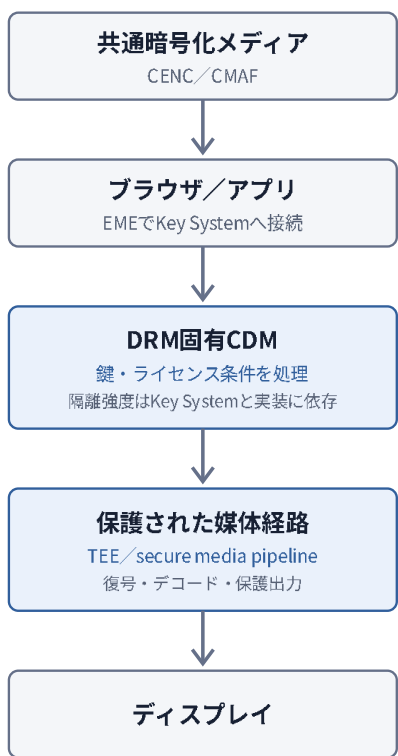
なお、これらの条件が成立した時期は様々ではありません。CENCの第1版は2012年2月[1]、EMEの最初のWorking Draftは2013年5月[21]、MovieLabsの保護要件仕様の初版は2013年9月です[17]。暗号化規格の策定が、供給側の要件文書の公表に先行しています。したがって、供給側の要求が先にあり、それに応じて規格が作られたという単純な順序では説明できません。本書は、これらが並行して進み、相互に参照されながら一つの基盤を形成したものと整理します。

次章では、この七つの条件を物差しとして、画像、Live2Dモデル、3Dモデル、アバター、ゲームアセットといった非映像デジタルアセットの現状を検討します。そこで見えてくるのは、「技術が存在しない」という単純な欠如ではなく、部品は存在するのに接続されなかったという、より複雑な構造です。

図1 映像分野における保護の構造

標準APIと、DRM・OS・ハードウェア・運用制度が形成する信頼境界を区別して示す

保護されたデータの経路



接続される七つの条件

- ① 共通暗号化フォーマット
CENC：暗号化資産を複数DRMで共用可能にする
- ② 標準インターフェース
EME：HTMLMediaElementとKey Systemを接続する
- ③ 厳密な信頼境界
DRM固有CDM・User Agent制約・ライセンス条件・堅牢性規則
鍵・復号後データの隔離は、Key Systemと実装の堅牢性に依存
- ④ ハードウェア隔離と保護出力
TEE・secure media pipeline・HDCP
- ⑤ 経済的アンカー
権利者・配信事業者・DRM事業者が保護要件を形成する
- ⑥ 適合性ガバナンス
契約・認証・堅牢性規則・失効・更新
- ⑦ 法的裏付け
技術的保護手段の回避を規制する法制度

注：七層が接続されても完全なコピー防止にはならず、画面の撮影等は防止できない。

図1 映像分野における保護の構図

出典（第 3 章）

[1]:ISO/IEC 23001-7:2023, Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files, ISO/IEC, 2023 年 8 月 8 日発行（第 4 版）。

<https://www.iso.org/standard/84637.html>

[2]:DASH-IF Interoperability Guidelines Part 6: Content Protection and Security, v5.0.0, DASH Industry Forum.

<https://dashif.org/docs/IOP-Guidelines/DASH-IF-IOP-Part6-v5.0.0.pdf>

[3]:Using content protection systems with HLS, Apple Inc.

<https://developer.apple.com/documentation/http-live-streaming/using-content-protection-systems-with-hls>

[4]:PlayReady Content Encryption, Microsoft.

<https://learn.microsoft.com/en-us/playready/packaging/content-encryption>

[5]:CTA-5001-E, Web Application Video Ecosystem — Content Specification, Consumer Technology Association.

<https://cdn.cta.tech/cta/media/media/resources/standards/pdfs/cta-5001-e-final.pdf>

[6]:RFC 8216, HTTP Live Streaming, IETF, 2017 年 8 月.

<https://www.rfc-editor.org/rfc/rfc8216.html>

[7]:Encrypted Media Extensions, W3C Recommendation, 2017 年 9 月 18 日.

<https://www.w3.org/TR/2017/REC-encrypted-media-20170918/>

[8]:W3C Publishes Encrypted Media Extensions (EME) as a W3C Recommendation, W3C, 2017 年 9 月 18 日.

<https://www.w3.org/press-releases/2017/eme-recommendation/>

[9]:Encrypted Media Extensions 2, W3C Working Draft, 2026 年 7 月 7 日.

<https://www.w3.org/TR/encrypted-media-2/>

[10]:Notice to the W3C of EFF's appeal of the Director's decision on EME, Electronic Frontier Foundation, 2017 年 7 月 12 日.

<https://lists.w3.org/Archives/Public/public-html-media/2017Jul/0005.html>

[11]:セキュリティ レベル (PlayReady) , Microsoft.

<https://learn.microsoft.com/ja-jp/playready/overview/security-level>

[12]:MediaDrm, Android Developers API Reference, Google.

<https://developer.android.com/reference/android/media/MediaDrm>

[13]:PlaybackMetrics, Android Developers API Reference, Google.

<https://developer.android.com/reference/android/media/metrics/PlaybackMetrics>

[14]:Integrating PlayReady in Devices, Microsoft（最終更新 2018 年 2 月 1 日）。

<https://learn.microsoft.com/en-us/playready/overview/integrating-in-devices>

[15]:Stéphanie Delaune, Joseph Lallemand, Gwendal Patat, Florian Roudot, Mohamed Sabt, Formal Security Analysis of Widevine through the W3C EME Standard, USENIX Security Symposium, 2024 年 .

<https://www.usenix.org/conference/usenixsecurity24/presentation/delaune>

[16]:Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME, Proceedings on Privacy Enhancing Technologies, 2023 年, Volume 2023, Issue 4, pp.306-321. DOI: 10.56553/popets-2023-0112.

<https://doi.org/10.56553/popets-2023-0112>

[17]:MovieLabs Specification for Enhanced Content Protection, Version 1.4, Motion Picture Laboratories, Inc. (MovieLabs), 2024 年 8 月.

https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.4.pdf

[18]:MPTF Requirements for Content Protection, W3C Web and TV Interest Group, Media Pipeline Task Force, W3C Editor's Draft, 2012 年 8 月 16 日. <https://www.w3.org/2011/webtv/MPTF/cpreq.html>

[19]:Reconciling Mozilla's Mission and W3C EME, Mozilla, 2014 年 5 月 14 日.

<https://hacks.mozilla.org/2014/05/reconciling-mozillas-mission-and-w3c-eme/>

[20]:Moving to HTML5 Video, Google, 2016 年.

<https://developers.google.com/media/pdf/2016-HTML5-Video-Whitepaper.pdf>

[21]:Encrypted Media Extensions, W3C First Public Working Draft, 2013 年 5 月 10 日.

<https://www.w3.org/TR/2013/WD-encrypted-media-20130510>

[22]:Widevine Mobile License Agreement, Exhibit A, Google.

<https://developers.google.com/widevine/contact/widevine-mobile-license-use>

本章の記述に関する注記

- Widevine のセキュリティレベル「L1/L2/L3」の各要件を明文で定義した Google/Widevine の公開一次資料は、本調査の範囲では確認できませんでした。このため本章では、公式定義が公開されている Microsoft PlayReady および Android MediaDrm を主たる例として用いています。
- CENC における cenc 方式から cbcs 方式への業界的な移行について、その完了時期を宣言した単一の一次資料は確認できませんでした。本章の記述は各組織による個別の対応記録に基づいています。
- 3-6 の条件⑤について、コンテンツを供給する側が「保護要件を満たさなければ供給しない」と表明した契約、公式声明、議会証言は、本調査の範囲では確認できませんでした。確認できたのは、保護要件が仕様として策定・公表されていること、および要件に対応しなかった場合の市場上の帰結を、プラットフォーム側が公式に説明していることです。本文の記述は、この範囲に限定しています。
- 3-6 に整理した七つの条件は、映像分野の到達点を他分野と比較するために本書が構成した枠組みです。この枠組みの外にある要因は、本書の検討範囲に入っていません。

第4章 非映像デジタルアセットにおける保護の現状

前章では、映像分野の保護基盤が七つの条件の接続によって成立していることを確認しました。本章では同じ物差しを、画像、Live2D モデル、3D モデル、アバター、ゲームアセットといった非映像デジタルアセットに当てます。

はじめに、本書が避けたい誤解を明示します。

「非映像デジタルアセットには技術的保護の手段が存在しない」というのは、事実に反します。

暗号化の国際規格、権利表現の国際規格、GPU レベルの保護機構に加え、電子出版、積層造形、電子設計 IP 等の用途別基盤も存在します。したがって、非映像分野全般について統合例がないともいえません。一方、本調査で確認した公開一次資料の範囲では、一般 Web 環境で複数形式を横断する共通保護層は確認できませんでした。

本章では、用途別の基盤と個別技術を認めたうえで、一般 Web・複数形式横断の経路において、どの接続が不足しているかを特定します。

4-1 配信アーキテクチャの共通構造

はじめに、対象となるアセットに共通する配信の流れを確認します。静止画像であれ、Live2D モデルであれ、3D モデルであれ、利用者の端末で表示・操作される限り、次の経路をたどります。

サーバー／CDN ↓ アセットデータの送信 ブラウザ／アプリケーション ↓ 読み込み・デコード ランタイム (JavaScript、WebGL／WebGPU、ゲームエンジン等) ↓ 計算・変形・合成 GPU ↓ ディスプレイ

映像との違いは、この経路の途中で何が起きているかにあります。

映像の場合、暗号化されたストリームは、DRM 固有 CDM、User Agent、TEE、secure media pipeline、出力保護等を組み合わせた実装により、復号後フレームをアプリケーションから隔離したまま再生できます。EME は HTMLMediaElement と Key System を接続する標準 API であり、単体でこの信頼境界を保証するものではありません。

一方、インタラクティブなアセットでは事情が異なります。Live2D モデルであれば、表情パラメータの変化に応じて頂点を変形させる計算が必要です。3D モデルであれば、スキニング、物理演算、衝突判定、ライティングの計算が必要です。これらの計算は、モデルの構造データそのものを参照しなければ実行できません。

したがって、クライアント側でレンダリングを行うアーキテクチャを選ぶ限り、レンダリングに必要な構造データが、計算可能な形でクライアント環境に存在しなければならないという制約が生じます。これは Web 固有の弱点ではありません。ネイティブアプリケーションでも、実行環境が解釈できる形でデータが存在する必要があるという点では同じです。

なお、この制約は「暗号化しても無意味である」ことを意味しません。暗号化は伝送中・保管中の秘匿として有効に機能し、取得のコストを引き上げます。制約が意味するのは、暗号化だけでは復号後の状態をどう扱うかという問題が残ることです。本章の中心的な問いは、一般 Web で複数形式を扱う場合に、標準 API、保護された実行・描画境界、鍵・ライセンス運用、適合性制度をどう接続するかです。

4-2 既に存在する規格の棚卸し

ここでは、非映像デジタルアセットに適用可能な既存の国際規格・技術を確認します。この節は、本書の主張が「規格が存在しない」という誤った前提に立っていないことを示すために不可欠です。

4-2-1 静止画像には複数の現行規格が存在します

第一に、映像分野の共通暗号化規格である CENC 自体が、静止画像を対象に含んでいます。

これは意外に知られていない事実です。ISO/IEC 23001-7 の第3版 (2016 年) における適用範囲は「ファイル、トラック、およびトラックフラグメントのメタデータ」でしたが[1]、2023 年発行の第4版では「ファイル、アイテム、トラック、およびトラックフラグメントのメタデータ」へと改められています[2]。

第4版の序文は、第3版からの主な変更点として「アイテム暗号化。これにより画像アイテムがメディアトラック向けに定義された保護スキームを利用できるようになる」を挙げています[2]。規格本体には、アイテム暗号化が

ックス ('ienc') およびアイテム補助情報ボックスの規定が追加されています[2]。ISO Base Media File Format において静止画像はアイテムとして格納されるため、HEIF や AVIF 等の画像に対して、映像と同じ保護スキーム(cenc、cbcs 等)を適用する道が規格上は開かれているということです。

第二に、静止画像専用のセキュリティ規格が現行規格として存在します。

JPEG 2000 の Part 8、通称 JPSEC です。ISO/IEC 15444-8 として標準化され、ITU-T 勧告 T.807 としても発行されています。2007 年 4 月に初版が発行され[3]、2008 年には file format security を扱う追補が加わり、2023 年には第 2 版が発行されました[4]。ITU-T 版は 2023 年 2 月 13 日に承認され、現在も有効です[5]。

「JPSEC は過去に存在したが廃止された規格」という理解は誤りです。2007 年版が廃止されたのは事実ですが、それは 2023 年版への置換に伴うものです。

JPSEC が扱う範囲は、単なる暗号化に留まりません。ITU-T はその対象として、機密性、完全性検証、送信元認証、条件付きアクセス、セキュアなスケーラブルストリーミング、セキュアなトランスコーディングを挙げています[5]。しかも、画像全体だけでなく、空間領域、解像度レベル、色成分、品質レイヤーといった単位ごとにセキュリティサービスを適用できる設計です[5]。JPEG 委員会は 2013 年の文書で、JPSEC の用途として、低解像度のプレビューのみを許可し高解像度へのアクセスを制限する例を明示しています[6]。

つまり、後の章で「プレビュー専用データによる原本保護」として論じる考え方は、20 年近く前に国際規格として設計されていたということです。

第三に、JPEG ファミリー全般を対象とするセキュリティ規格も存在します。

ISO/IEC 19566-4「JPEG systems — Part 4: Privacy and security」が 2020 年 3 月に発行されています[7]。これは JPEG 2000 に限らず、ボックス構造を持つ JPEG ファイル形式全般に適用可能なプライバシー・セキュリティ機能と、その存在を通知するシグナリング構文を規定するものです[7]。策定の背景には、ソーシャルネットワークやクラウド環境における画像メタデータの保護、プライバシー、そして権利情報の保全という要求がありました[8]。

ここで注意が必要です。この規格は保護と来歴の双方を扱っており、要求文書では W3C PROV を用いた来歴情報の埋め込みと完全性検証が挙げられています[8]。来歴管理はコピー防止ではありません。同一の規格が複数の目的を扱うからといって、両者を混同してはなりません。

4-2-2 メディア形式に依存しない汎用の保護規格も存在しました

第一に、写真とゲームを明示的に対象とする標準 DRM が、かつて存在しました。

Open Mobile Alliance の OMA DRM です。バージョン 2.1 の仕様は、メディアオブジェクトの形式、OS、実行環境に依存しないことを明記したうえで、対象例としてゲーム、着信音、写真、音楽クリップ、動画クリップ、ストリーミングメディアを列挙しています[9]。DRM Agent、Rights Issuer、Content Issuer、Rights Object といった役割を明確に分離し、利用者が保護コンテンツを他のデバイスへ渡した先で受領者が別途権利を取得する「Superdistribution」まで定義していました[9]。

日本でも実装されています。ソフトバンクの公式アーカイブに残る Vodafone 804N の取扱説明書には、メディアプレイヤーの対応形式として「DRM OMA DRM(S/D).dcf」が明記され、ダウンロードした画像等について再生回数・期間・転送の制限があり、権利がなければコンテンツキーを取得する旨が記載されています[10]。

したがって、「非映像デジタルアセットについて、形式非依存の標準 DRM が作られたことはない」という主張は誤りです。

第二に、MPEG にも保護のための標準が存在します。

MPEG-4 の Part 13 (ISO/IEC 14496-13:2004) は「Intellectual Property Management and Protection (IPMP) extensions」として知られ、通称 IPMP-X と呼ばれます[11]。MPEG の公式解説文書は、当時の DRM 市場の問題を相互運用性の欠如と更新可能性の欠如と診断し、それを改善するために交換可能な保護ツール、ツールリスト、セキュアメッセージング枠組み等を導入したと説明しています[12]。

MPEG-21 にも、Part 4「Intellectual Property Management and Protection Components」(ISO/IEC 21000-4:2006) と、Part 5「Rights Expression Language」(ISO/IEC 21000-5:2004) があります[13][14]。REL は、許可・禁止・

義務・制約を用いて権利条件を機械可読に表現する言語です。

これら三つの規格は、いずれも 2026 年 8 月時点で ISO カタログ上「Published」であり、廃止されていません[11][13][14]。旧 MPEG 公式サイトで標準化活動の状態が「Closed」と表示されることがありますが、これは活動の状態であって規格の廃止ではありません。

4-2-3 GPU レベルの保護機構も存在します

「3D データは復号された状態で GPU メモリに置かれざるを得ないため、映像のような保護は原理的に不可能である」という説明を目にすることがありますが、これは正確ではありません。

Khronos Group の Vulkan は、バージョン 1.1 以降のコア仕様に保護メモリ機構を含みます[15]。保護対象は画像に限られず、バッファにも適用できます。ただし protectedMemory への対応はオプションであり、実装ごとに機能照会が必要です。EGL_EXT_protected_content と Direct3D 12 の Protected Resource Session にも、保護された GPU 資源を扱う機構があります[19][72]。これらも拡張または実装依存であり、単独で DRM 要件やエンドツーエンドの保護を保証するものではありません。

したがって、頂点データを保護メモリ上で扱う仕組みは、仕様として既に存在します。「原理的に不可能」と書くことはできません。

Khronos は、保護メモリへアクセスするパイプラインが少数であるとの設計前提を示し、パイプライン単位で保護アクセスを制御する機構を整備しました[16]。当初の拡張は Vulkan 1.4 へ昇格しています。本調査で確認した公開一次資料の範囲では、汎用 3D アセット保護としての広範な商用実装は確認できませんでした。ただし、これは市場全体で利用されていないことを意味しません。

2026 年 8 月 28 日時点の公開 WebGPU 仕様、WebGL 仕様および登録拡張には、ネイティブ GPU の保護資源を汎用 3D アセット向けに利用する標準の保護セッション、保護キューまたは保護リソース API を確認できませんでした[17][18][73]。GPUExternalTexture は外部映像をサンプリングする機構であり、汎用 3D アセットの暗号化、鍵管理、利用条件、非読出し保証を提供するものではありません。

WebGPU の origin-clean 等の制約は、利用者と他オリジンを悪意ある Web コンテンツから守るための境界です。正規利用者から権利者のアセットを隔離する信頼境界とは目的が異なります。

4-2-4 用途別には統合された保護基盤が存在します

非映像分野には、複数の技術層を接続した用途別基盤も存在します。

- 電子出版の Radium LCP は、出版物の暗号化、ライセンス文書、利用条件、署名、状態管理、認証クライアントを組み合わせています[74]
- 積層造形の 3MF Secure Content は、3MF パッケージ内の部品・資源の暗号化を規定します。Materialise Identify3D は、製造データの暗号化、認可機械での復号、数量・機械条件の執行、監査を一つの製造ワークフローへ接続します[75][76]
- 電子設計 IP の IEEE 1735-2023 は、設計情報の暗号化、利用権、ライセンス検証、信頼モデルを規定します[77]

これらは、「非映像分野に統合基盤は存在しない」という広い主張を反証します。一方、対象形式、業界、認証アプリ、ネイティブ環境または特定ベンダーに依存します。本書が対象とする一般 Web・複数形式横断の共通層とは区別が必要です。

4-2-5 小括 ー 部品と用途別基盤は存在します

以上を整理します。

層	非映像側で確認できるもの	判定
共通暗号化フォーマット	CENC のアイテム対応、JPSEC、ISO/IEC 19566-4	存在する
利用条件の技術的強制 (DRM)	OMA DRM 2.x、MPEG-4 IPMP-X	歴史的に存在した
権利条件の表現	MPEG-21 REL、後述の VRM メタデータ等	存在する

GPU レベルの保護実行環境	Vulkan 保護メモリ、Direct3D 12、EGL	存在する（ネイティブ機能。対応はオプションまたは実装依存）
用途別の統合基盤	Radium LCP、3MF Secure Content、Identify3D、IEEE 1735	存在する （対象分野・実装環境に限定）
標準 API と信頼境界	—	次節で検討

「規格も統合例も存在しない」という主張は成り立ちません。問うべきは、一般 Web 環境で複数形式を横断する共通層として、なぜ接続されなかったのかという点です。

4-3 なぜ接続されなかったのか

前章で整理した七つの条件を物差しとして、順に検討します。ここで浮かび上がるのは、一般 Web・複数形式横断の経路では、暗号技術そのものより、標準 API、信頼境界、経済的アンカー、適合性ガバナンス等の接続が不足しているという点です。

4-3-1 条件②標準インターフェース — 形式規格と Web API の分離

MPEG-4 IPMP-X は、相互運用性の欠如を明確に問題として認識し、その解決を目指した規格でした。ではなぜ、EME のような形にならなかったのか。

MPEG の公式解説文書には、IPMP-X が「機能インターフェースを定義するというアプローチを採らなかった（did not choose the approach of defining functional interfaces）」と明記されています[12]。代わりに採用されたのは、メッセージルーターを介したセキュアなメッセージ通信でした[12]。

つまり、IPMP-X では、機能インターフェースではなくメッセージ通信を中心とする設計が選択されました。ただし、この記録だけから、後の Web API や現在の実装状況との因果関係まで断定することはできません。

JPSEC と ISO/IEC 19566-4 についても同様のことが言えます。これらはコードストリームやファイル形式の側にセキュリティ構文を規定する規格であり、Web アプリケーションが保護モジュールを利用するためのブラウザ API ではありません[5][7]。OMA DRM も、デバイス上の DRM Agent とネットワークプロトコルを規定しましたが、Web プラットフォームの標準ではありませんでした[9]。

一般 Web・複数形式横断の経路については、本調査で確認した公開一次資料の範囲で、この層を担う共通 API を確認できませんでした。前章で述べたとおり、EME における鍵システム的能力指定は audioCapabilities と videoCapabilities として定義されており、画像・3D メッシュ・汎用アセットに対応する第三の項目は、2026 年 8 月時点の現行 EME 2 仕様にも定義されていません[20]。

同じ Working Draft のステータス欄は、2017 年の勧告以降に追加された機能として、暗号化方式の能力検出と、HDCP ポリシーに関連する鍵状態の照会の 2 点を挙げたうえで、その他の機能を含めることは Media Working Group のスコープ外である旨を明記しています[20]。

4-3-2 条件③厳密な信頼境界 — 実装側へ委ねられた領域

MPEG-21 の IPMP Components は、Digital Item に保護情報や統制対象部分を組み込む方法を規定します。しかし ISO による規格の説明は、この規格が保護手段、鍵、鍵管理、信頼管理、暗号アルゴリズム、認証基盤を規定しないことを明記しています[13]。

Rights Expression Language も同様です。権利表現の構文と意味論、および認可モデルを定めますが、信頼されたシステムのセキュリティ対策は規定せず、権利表現をいつ参照しなければならないかも規定しません[14]。

これらの規格は、権利表現や保護情報の構造を定める一方、信頼されたクライアントの具体的な構築を各実装者へ委ねています。この分離は規格の欠陥を意味しませんが、運用基盤を成立させるには別の実装主体と制度が必要です。

映像分野では、この領域をブラウザベンダー、OS ベンダー、チップセットメーカー、CDM ベンダー、コンテンツ権利者の実装・契約・適合性制度が担っています。一方、MPEG-21 については、その統合を担う横断的主体を、本調査で確認した公開資料の範囲では確認できませんでした。

4-3-3 条件⑥適合性がバナンス — 制度は設けられたが、保存公開一覧に登録項目が表示されていない

七条件のうち、非映像側の状況を最も象徴的に示すのが、この層です。

JPSEC は、保護ツールを登録して相互運用の基盤とする Registration Authority を規格上に持っていました。ISO/IEC 15444-8:2007 の説明は、規定内容の一つとして「固有識別子を付与する登録機関に JPSEC ツールを登録するための規範的プロセス」を挙げています[21]。未知のツール識別子がコードストリーム中に現れた際、登録機関に照会して当該ツールの情報を取得する、という設計思想です。

この登録機関は、実際に設置されました。そして日本に置かれました。

運営主体は、特定非営利活動法人 IRI (Intellectual Resource Initiative) です。同法人の Web サイトは、JPSEC RA を、JPSEC 項目を登録したい者のためにインターネット上の場を提供し、審査・維持・配布・連絡窓口を担う組織と説明しています[22]。単なる自称ではありません。同サイトは、ISO によって JPEG 2000 Part 8 の Registration Authority として指定されたことを表示できる旨を記載しています[23]。登録のためのアカウント発行手続きや、登録資格を国内外の標準化委員会等に限定する規定も整備されていました[24]。

IRI 自身の声明は、その動機をこう述べています。デジタルアーカイブや図書館サイトの構築が急速に普及するなかで、JPEG 2000 が提示するセキュリティ技術が新たな社会基盤として不可欠であると認識し、この技術の普及を助けるために登録機関を引き受けることを決めた、と[25]。

2025 年 2 月 9 日付の保存公開一覧には、登録項目が表示されていません[26]。ただし、これは保存時点の公開状態を示すものであり、全期間にわたり登録がなかったことを証明するものではありません。

ITU-T の 2023 年版 T.807 では、JPSEC registration authority に関する第 7 条が非推奨化されています[27]。

また、IRI の声明には、特定非営利活動法人として、登録機関業務に起因する経済的・事業的活動への責任を負わず、関連活動への恒久的な関与も保証できない旨が記載されています[25]。

この一文と、映像分野の対応する層を並べてみてください。

Microsoft は、PlayReady のデバイス統合において、OEM に対しプラットフォーム移植、暗号アクセラレータ、ビデオ経路の実装、デバイス固有の秘密情報の設定、そしてコンプライアンスおよび堅牢性規則への適合検証までを要求しています[28]。実装後も、契約と適合性プロセスによって信頼境界が維持される仕組みです。

一方、画像分野の登録機関を担った非営利法人は、関連活動への恒久的な関与を保証できない旨を表明していました。

ここには、技術仕様だけでなく、制度を継続運用する主体と費用負担を検討する必要性が現れています。ただし、公開資料から利用実績及び制度変更の原因を確定できないため、これらを運営主体の法人形態や当該声明だけに帰することはできません。

4-3-4 条件⑤経済的アンカー — 横断的な要求主体を確認できない

次に、共通実装を継続的に求める需要側主体の違いを検討します。

第 3 章 3-6 の条件⑤で述べたとおり、映像分野では、コンテンツを供給する側や DRM 事業者が保護要件を仕様・契約として策定し、端末・プラットフォーム側が対応を進めました。公開契約には secure boot、鍵と平文経路の保護、出力保護等の堅牢性要件がありますが、保護レベルごとの全要件を体系的に示す公開公式資料は確認できていません。

非映像側はどうだったか。

OMA DRM には、通信事業者と端末ベンダーという実装主体が存在し、日本の携帯端末への実装も確認できます[10]。ただし、その対象と運用体系は、本書が検討する一般 Web・複数形式横断の共通層とは異なります。

JPSEC、MPEG IPMP、ISO/IEC 19566-4 については、OS・ブラウザ・チップセット・アプリケーションの各ベンダーに共通実装を要求できるだけの需要側主体を、公開資料から確認することはできません。映像分野における MovieLabs の仕様に相当する、供給側が策定・公表した保護要件の文書も、これらの分野では確認できませんでした。JPEG の Privacy & Security 活動には、写真通信社の団体や画像権利情報の団体といった関係者が参加していましたが[8]、これらは画像の権利情報とプライバシーにとって重要な関係者ではあっても、業界共通の保護要件を

策定し、その実装をプラットフォームに促す立場ではありませんでした。

さらに、利用環境の分散があります。映像配信では、媒体形式、再生 API、DRM、保護出力等の役割分担が比較的標準化されています。これに対し非映像デジタルアセットは、画像ビューア、3D エンジン、DCC ツール、ゲームエンジン、WebGL/WebGPU アプリケーション、OS のファイルビューア等、多様な環境で扱われます。この分散が共通要件の形成にどう影響したかは分析仮説であり、因果関係を直接実証したものではありません。

4-3-5 小括 ― 空白の所在

七条件に照らした評価を整理します。

条件	非映像側の状況
① 共通暗号化フォーマット	部分的に達成。CENC、JPSEC、IPMP の各枠組みに類似の思想はあった
② 標準インターフェース	用途別の仕組みは存在するが、一般 Web・複数形式横断の EME 相当 API は確認できない
③ 厳密な信頼境界	用途別・個別実装には存在するが、一般 Web・複数形式横断の共通境界は確認できない。MPEG-21 では実装を規定しない
④ ハードウェア隔離	ネイティブ GPU 機構は存在するが、対応はオプションまたは実装依存。現行 Web 仕様に汎用アセット向けの標準接続経路は確認できない
⑤ 経済的アンカー	用途別には存在するが、一般 Web の共通実装を継続的に要求する横断的主体は確認できない
⑥ 適合性ガバナンス	用途別には存在する。一般 Web・複数形式横断の制度は確認できない。JPSEC には旧登録制度があり、保存公開一覧に項目は表示されていないが全期間の履歴は不明
⑦ 法的裏付け	映像専用ではない。日本法についても非映像著作物に関係し得る（第 9 章で詳述）

個別の暗号化規格、GPU 機構、用途別基盤は存在します。一般 Web・複数形式横断の経路で確認できないのは、形式、標準 API、信頼された実行・描画境界、鍵・ライセンス運用、保護出力、経済的アンカー、適合性ガバナンスを一体として接続する共通層です。

そして重要なのは、これらのうち⑤と⑥が技術ではなく制度の問題だという点です。暗号アルゴリズムを新しく発明しても、これらの層は埋まりません。法的裏付けを除く六条件の対比を図 2 に示します。

以下では、この構造を踏まえたうえで、静止画像、Live2D モデル、3D モデル・アバター、ゲームアセットという類型別の現状を検討します。あわせて、映像と非映像を分ける本質的な差異——取得されたデータが消費されるのか、再び生産に用いられるのかという違いについて論じます。

図2 非映像デジタルアセットにおける保護の構造

用途別の統合基盤と技術部品は存在する。未接続なのは、一般Web・複数形式横断の共通層である。



図 2 非映像デジタルアセットにおける保護の構造

4-4 類型別の現状

4-4-1 静止画像 — 表示物と原本の距離が近い類型

静止画像は、本書が扱う類型のなかで、やや特殊な位置にあります。

まず事実関係を正確に述べます。画面に表示された画像を撮影・キャプチャしても、それは原本と同一ではありません。元ファイル固有のメタデータ、非表示情報、元の圧縮表現、表示解像度を超える画素、元のビット深度や色管理情報は、通常回収できません。「スクリーンショットは原本の完全なコピーである」という説明は不正確です。

しかし、用途によっては実用上の代替物になり得ます。閲覧、SNS への再投稿、画面上での鑑賞が目的であれば、表示解像度のキャプチャで足りる場合が少なくありません。この性質は、配信経路をどれだけ強固に保護しても変わりません。正規の利用者に表示した視覚情報は、表示装置に現れるからです。

したがって静止画像では、閲覧用途に限れば、配信経路の保護を強化することによる便益が相対的に小さくなります。この点を認めずに「画像にも DRM を」と主張することは、本書の説得力を損ないます。

ただし後述する 4-5 のとおり、これは静止画像に固有の弱点ではありません。3D モデルであっても、鑑賞用途に限ればレンダリング動画で代替され得ます。表示物の層が鑑賞用途に対して代替可能であることは、類型を問わない共通の性質です。

一方で、便益が小さいのは「閲覧用途で代替可能な範囲」に限られます。高解像度印刷、出版、商品制作、素材

としての再販売、レタッチ用の中間データ、AI 学習用の原本といった用途では、表示用画像と高解像度原本の価値差は依然として大きいままです。この構造は、後述する 4-5 の二層モデルにおいて、他の類型と共通のものとして整理します。

実務上、この差に対応する設計は既に一般的です。高解像度の原本を非公開領域で管理し、Web には縮小・再圧縮した閲覧用の派生データのみを提供するという方式です。これは DRM ではなく、価値の高い原本をそもそもクライアントへ渡さないというデータ最小化の考え方です。4-2-1 で述べたとおり、JPSEC が 2000 年代に設計していたのは、まさにこの考え方の規格化でした。

配信側のアクセス制御としては、署名付き URL や短寿命トークンが広く用いられます。ここで重要なのは、これらがアクセス制御であって DRM ではないという区別です。この区別は標準文書自体が明示しています。CDN 相互接続における URI 署名を規定する RFC 9246 は、URI 署名がコンテンツ保護スキームではなく、コンテンツ自体の保護には DRM 等の別の仕組みが必要である旨を明確に述べています[29]。署名付き URL が防げるのは権限のない取得であり、権限を持つ利用者に一度提供した内容の再取得は、別の脅威モデルです。

来歴管理については、近年めざましい進展があります。C2PA (Content Credentials) は、暗号学的に検証可能な形で作成者や編集履歴をコンテンツに結び付ける仕様であり、調査基準日時点の現行版は第 2.4 版です[30]。カメラ、編集ソフト、プラットフォームの各層に商用実装が存在します[78][79][80]。ISO/IEC 21617 (JPEG Trust) シリーズも、Part 1「Core foundation」が 2026 年版として発行され[31]、Part 2「Trust profiles and reports」および Part 3「Media asset watermarking」の開発が進んでいます[32]。

ただし、これらをコピー防止の解決策として扱うことは誤りです。C2PA が公開する FAQ は、Content Credentials は DRM ではなく、DRM が利用を制限するのに対して Content Credentials は制限を伴わず透明性を提供するものであると明記しています[33]。来歴管理は「これが誰の、どのような由来の作品か」を証明する技術であり、「複製を止める」技術ではありません。両者は補完的ですが、代替関係にはありません。

電子透かしについても、限界を正確に把握する必要があります。画素レベルに情報を埋め込む方式の不可視電子透かしについては、生成モデルを介した再構成によって検出が大きく損なわれ得ることが、理論と実験の双方から示されています[34]。JPEG 再圧縮や縮小、一定範囲の切り抜きに耐えることと、生成 AI によって視覚内容を再構成された場合にも同じ識別子が残ることは、別の要件です。

ただし、方式による差があります。生成過程そのものに情報を埋め込む方式については、同種の攻撃下でも検出が維持されたとする報告があります[35]。この方式は生成される画像の見え方に影響するため、既存の画像へ後から適用する用途には向きませんが、「電子透かしは生成 AI によって無効化される」という一般化は、本調査の範囲では成立しません。

4-4-2 Live2D モデル — 事業者の設計努力と、その先にある構造的限界

Live2D モデルは、本書が扱う問題を最も明瞭に示す類型です。

Live2D 社の公式ドキュメントによれば、組み込み用途のデータは、モデル本体である .moc3、関連ファイルを結び付ける .model3.json、テクスチャ、そして必要に応じて物理演算の .physics3.json、モーションの .motion3.json 等から構成されます[36]。

Cubism SDK for Web の公式解説は、ブラウザ上で .model3.json を取得してバイト列として読み込み、そこから .moc3 のデータをメモリへ展開してモデルを生成する処理の流れを示しています[37]。モーションについても同様に、.motion3.json を取得してバイト列として渡す処理が示されています[38]。

したがって、ブラウザ内で Live2D モデルをレンダリングし、表情やモーションを動かす構成では、その計算に十分なデータがクライアント環境に存在する必要があります。

ただし、ここで重要な留保が必要です。これは「編集原本をブラウザへ渡さなければならない」という意味ではありません。Web 版 SDK が必要とするのは実行用データであり、Cubism Editor の編集ファイルや、販売用のアーカイブそのものではありません。

この区別を実装に落とし込んでいる例が、Live2D 社が運営するマーケットプレイス nizima です。公式ガイドに

よれば、Cubism Editor からの出力により、編集できないモデルデータである export.zip、編集可能なデータである original.zip、そして作品詳細ページで表示するプレビュー用の preview.zip の三種類が生成されます[39]。プレビュー用のテクスチャは販売用データより小さくできること、そして公開用の preview.zip 自体はダウンロード提供の対象ではないことも公式に説明されています[40]。

ダイレクトメッセージで確認用データを送る場合には、受信者がダウンロード可能であるため、解像度を落とした確認用データを用いることが推奨されています[42]。

本調査が確認した現行の Live2D プレビュー操作ガイド[41]では、SAMPLE 透かしや表示位置の時間変化を裏づける記述を確認できなかったため、同サービスの実装として扱いません。

これらは、多層防御の実践として評価に値します。データ分離、アクセス制御、データ縮退、利用条件の組み合わせであり、事業者の設計努力として先進的です。第 5 章では、この事例をより詳しく検討します。

ただし、二点を正確に述べておく必要があります。

第一に、これらをすべて「DRM」と呼ぶことは技術的に不正確です。分離、アクセス制御、縮退は、いずれも利用条件を技術的に強制する仕組みではありません。

第二に、プレビュー用データがダウンロード提供の対象でないことと、ブラウザレンダリング用データが渡らないこととは、同義ではありません。前者はサービス上のアクセス制御であり、後者は Web 版 SDK の動作原理に関わります。

なお、Cubism SDK には整合性を確認する MOC3 Consistency Checker が公式提供されていますが[43]、これは不正な変更が疑われる状態を検出するための機能であり、コピー防止の DRM ではありません。本調査の範囲では、Cubism SDK 標準として購入者単位の利用条件を技術的に強制する仕組みは確認できませんでした。

ここに構造が現れます。個々の事業者は、利用可能な手段を組み合わせることで相当に高度な設計を実現しています。しかしそれは各社が個別に設計したものであり、業界横断で共有された標準ではありません。第 3 章で整理した七つの条件のうち、②標準インターフェース、③信頼境界、④ハードウェア隔離を一社が業界横断の仕組みとして成立させることは難しく、①⑤⑥についても、一社の取組だけで業界横断の基盤になるとは限りません。

4-4-3 3D モデル・アバター — オープン性という設計思想との緊張

3D アセットの領域では、事情がやや異なります。主要な交換形式に利用条件の技術的強制が組み込まれていないことには、相互運用性を重視する設計思想が関係しています。

glTF は Khronos Group が策定し、ISO/IEC 12113:2022 として国際標準化された 3D アセット配信形式です[44]。同規格は PAS 手続により、Khronos の仕様を技術的変更なく国際規格として採択したものです。その設計思想は、特定のグラフィックス API に依存しないランタイム非依存性、機能追加を許容する拡張可能性、そして伝送効率にあります。相互運用性の最大化が最優先されています。

仕様および公式の拡張レジストリを調査した範囲では、コア仕様にも公式拡張にも、暗号化、アクセス制御、利用条件の技術的強制に関する規定は確認できませんでした。

関連する拡張として、XMP に準拠したメタデータを埋め込む KHR_xmp_json_ld があります。これにより作成日、帰属表記、ライセンス条件といった情報をファイルに内包できます。しかし仕様原文は、メタデータがアセットの外観やレンダリングに対して規範的な影響を与えないと明記しています[45]。すなわち、権利条件を記述することはできても、それを強制する仕組みではありません。

VRM も同様の構造を持ちます。VRM 1.0 の仕様は、VRMC_vrm.meta において詳細な利用許諾表明を定義しており、アバターとして操作できる者の限定、商用利用の可否、改変の可否、暴力・性的・政治的・反社会的表現への利用可否といった項目が規定されています[46]。

これは、権利者の意思を機械可読な形で表明する優れた仕組みです。しかし仕様上、これらの条件に反する利用が行われた際に、ソフトウェア側にレンダリングの停止等を要求する技術的強制の規定は存在しません[46]。VRM コンソーシアムのアプローチは、暗号化や DRM による技術的防止ではなく、権利者の意思をファイルに明記することによる社会的・規範的な抑止に依拠しているといえます。

MPEG は別のアプローチを取っています。MPEG-I Scene Description (ISO/IEC 23090-14) は、glTF 2.0 を基礎としつつ MPEG 拡張によってメディアとの統合機能を追加する構造で、現行版は 2025 年 11 月発行の第 2 版です[47] (2023 年の第 1 版は撤回されています)。ここには Media Access Function (MAF) が取得・復号・デコードしたメディアを、シーングラフ側のバッファへ渡すアーキテクチャが存在します[48]。しかも対象メディアには動的メッシュや点群も含まれるため、「3D ジオメトリは対象外」と断ずることはできません。

ただし、これは EME 型の信頼境界ではありません。公開アーキテクチャとの比較による評価では、MAF の出力は復号済みのデータとしてプレゼンテーションエンジンへ渡されます[48]。EME のように、鍵システムを標準 API から選択し、ライセンス要求と応答を不透明なメッセージとして仲介し、復号後のアセットを非信頼のアプリケーションから隔離する、という構造とは異なります。また、シーングラフ内の静的ジオメトリそのものを DRM 保護する標準ではありません。

現在進行中の動きもあります。glTF 2.1 は 2026 年 8 月時点でプレビュー段階にあり、Khronos Registry の現行版は glTF 2.0 です。策定中のバイナリ形式にはチャンクの符号化フィールドが予約され、将来のバージョンや拡張が圧縮や暗号化に用い得る場所として設計上確保されています[49]。ただし、glTF 2.1 自体は暗号化を定義していません。OpenUSD 側の「Separation of Concerns for IP Protection in USD」は、2026 年 8 月 28 日時点で Open から Draft の提案です。DRM、暗号方式、具体的なアクセス制御の実装を明示的にスコープ外としており、採択済み仕様ではありません[50]。

被害の実態については、プラットフォーム運営者による公式の言及があります。VRChat は 2022 年のセキュリティ更新において、改造クライアントが利用者に無断でアバターの不正抽出とアーカイブ化を行っている実態を公式に指摘し、対策としてアンチチート技術を導入しました[51]。これは実行プロセスの監視によるアクセス制御であり、アセットデータを暗号化して利用条件を強制する DRM ではありません。

学術研究では、3D メッシュへの電子透かしに研究の蓄積があります。2009 年に公表されたサーベイ論文は、メッシュの簡略化や非一様リメッシュによって埋め込みに用いた接続情報が失われやすいこと、頂点順序の変更や別の表現形式への変換が最も破壊的な操作であり、当時は有効な防御策が報告されていないことを整理しています[52]。近年は深層学習を用いた手法により、ガウスノイズ、回転・拡大縮小、切り取り、頂点の並べ替え、圧縮といった攻撃に対する耐性の向上が報告されています[53]。

ただし、本書が対象とする用途に照らすと、未解明の領域が残ります。リギングのやり直しや UV 展開の変更に対する耐性を扱った研究は、本調査の範囲では確認できませんでした。事後追跡としての価値は認められますが、想定される編集操作の全体に対して耐性が実証されているわけではありません。

4-4-4 ゲーム・制作アセット — 公式ドキュメントが認める限界

ゲームエンジンの領域では、開発元自身が保護の限界を明示的に述べている点が特徴的です。

Unity の現行マニュアルは、AssetBundle の配信について HTTPS の使用と CRC による完全性検証を説明しています[54]。HTTPS は伝送路の暗号化、CRC は整合性の確認であり、いずれも保存済みデータのコピー防止ではありません。

より踏み込んだ記述は、Unity 5.4 の公式マニュアル「Protecting Content」にあります。同文書は独自暗号化の適用方法を説明すると同時に、クライアントがデータを受け取った後は、十分な動機を持つ第三者による取得を暗号化だけで防ぐことは困難であるという趣旨を明示しています[55]。開発元自身による、この問題に関する率直な記述です。

Addressables についても、特定バージョンの公式 API にカスタム暗号化を実装するためのインターフェースが記載されていますが[56]、現行の一般向けパッケージで同等の API が標準機能として維持されているかは確認できませんでした。「設定画面のスイッチ一つで有効化できる標準 DRM がある」という理解は、公式資料からは支持されません。

Unreal Engine では、プロジェクト設定に Pak の暗号化キー、インデックスの暗号化、アセットの暗号化といった項目が公式に用意されています[57]。ただし公式ドキュメントは、Pak 暗号化の目的をデータ抽出や改変を妨げ

るものとして説明しており、不可能にするとは表現していません[58]。また、復号のためには実行時にクライアントが鍵を利用できる必要があり、公式 API には埋め込み鍵の概念と実行時の鍵登録の仕組みが存在します[59]。

Anti-Tamper 技術についても、対象範囲の区別が必要です。Denuvo Anti-Tamper は、バイナリに加えて実行時メモリの不正操作、コード注入、リバーズエンジニアリング等を対象としています[60]。しかし、レンダリング中にメモリ上へ展開されたアセットデータの秘密性を維持し、その取得を防止する機能であるという公式の説明は確認できませんでした。実行ファイルの保護とアセットの保護は、別の問題です。

流通側の状況を最も端的に示すのは、日本最大級の同人・素材マーケットプレイスである BOOTH の公式ヘルプです。同ヘルプは、DRM 機能を提供していないことを明記しています[61]。すなわち、3D モデルカテゴリだけで年間 100 億円規模に達する取引が[62]、技術的強制ではなく契約とアクセス制御によって運営されているということです。

これは同社の怠慢を示すものではありません。本章で見てきたとおり、本調査で確認した公開一次資料の範囲では、一般 Web・複数形式を横断して利用できる共通保護層を確認できないためです。

4-5 原本と表示物 — 映像との本質的な差異

ここまでの検討を踏まえ、映像と非映像を分ける本質的な差異を定式化します。

しばしば「映像もスクリーンレコーディングで録画できるのだから、非映像だけが特別に脆弱なわけではない」という指摘がなされます。この指摘は、防止の可否という観点では正しいものです。しかし、取得されたデータがその後どう使われるかという観点を欠いています。

4-5-1 原本は生産財である

映像を録画した場合、得られるのは劣化した視聴用のコピーです。それは再び視聴されるだけであり、新たな作品を作る材料にはなりません。映像作品の商業的価値は視聴体験そのものにあり、録画物はその代替品として競合しますが、生産の手段にはなりません。

一方、本書が対象とするデジタルアセットの原本は違います。これらは改変し、別の作品に組み込み、再演し、再販売できる素材です。取得されたデータは、消費されるだけでなく、再び生産に用いられます。

この構造は、類型を問わず共通しています。重要なのは種類の違いではなく、同じ作品に「原本」と「表示物」という二つの層が存在することです。

類型	原本（生産財）	表示物（消費物）
静止画像・イラスト	高解像度原本、レイヤー付きデータ、線画、素材データ	Web 表示用に縮小・再圧縮された画像
Live2D モデル	.moc3、テクスチャ、物理演算設定、モーション	画面上で再生される動き
3D モデル・アバター	メッシュ、リグ、テクスチャ、スキニング情報	レンダリングされた映像
ゲーム・制作アセット	プロジェクトファイル、素材一式、モーション	ゲーム画面、再生結果

いずれの類型でも、原本を取得されれば、それは新たな制作の材料になります。イラストの高解像度原本は、印刷、商品化、素材としての再販売、他作品への流用、AI 学習用データという用途を持ちます。Live2D モデルの.moc3 とテクスチャは、別のキャラクターへの改変や無断配信に用いられます。3D モデルのメッシュとリグも同様です。

4-5-2 映像との比較

この観点から、映像と非映像を対比すると次のようになります。

	映像	非映像デジタルアセット
配信経路に現れるもの	配信用に符号化された断片	原本またはそれに近い実行用データ
端末で参照される必要があるもの	復号後の映像フレーム	構造データそのもの
取得物の主な用途	視聴（消費）	改変・組み込み・再演・再販売（生産）
経済的損害の性質	視聴機会の逸失	制作労働の成果の横取り、競合品の出現
保護対象と配信経路の関係	保護対象は経路の外に留められる	保護対象が経路上に現れる

ただし、映像に原本の層が存在しないわけではありません。映像制作にも、撮影素材、編集プロジェクト、VFX アセット、保存用マスターといった制作原本が存在します。京都市立芸術大学芸術資源研究センターが文化庁事業として公開する映像資料の保存ガイドは、保存用マスターと展示用・プレビュー用データを明確に区別しています[63]。ストックフッテージ市場では、映像素材が他作品の材料としてライセンス販売されており[64]、映像もまた生産財として流通しています。

差は、原本が存在するかどうかではありません。原本を利用者の端末へ渡さずにサービスが成立するかどうかです。

一般的な映像配信では、端末へ送られるのは配信用に符号化された断片であり、制作原本は制作側に留まります[65]。視聴という目的が、原本を渡さずに達成できるためです。第3章で見た EME や Secure Video Path は、この前提の上に成り立っています。

インタラクティブなアセットでは、これが成立しません。glTF は、メッシュ、スキン、アニメーションの各データをバッファに格納し、クライアント側がそれを参照して頂点変形を計算する形式として設計されています[66]。表示と操作の計算そのものが構造データを必要とするため、原本またはそれに極めて近い実行用データが、クライアント環境に置かれる必要があります。

表示の経路を保護する仕組みは、この差を埋めません。保護すべきデータが、保護された経路の外側で参照されるためです。

4-5-3 表示物の層に関する留意点

ただし、表示物の層については、類型ごとに性質の差があります。

静止画像では、表示物と原本の距離が相対的に近くなります。4-4-1 で述べたとおり、閲覧や SNS への再投稿といった用途であれば、表示解像度のキャプチャで足りる場合が少なくありません。

ただし、これは静止画像に固有の弱点ではありません。3D モデルであっても、鑑賞用途に限れば、レンダリング動画を録画すれば目的は達せられます。表示物は、いずれの類型でも「鑑賞」という用途に対して代替可能です。

したがって正確な整理は、次のとおりです。

表示物の層は、類型を問わず、鑑賞用途に対して保護の便益が小さい。

原本の層は、類型を問わず、生産財としての価値を持ち、保護の便益が大きい。

類型による差は、この二層がどれだけ離れているかの程度差であって、構造の違いではない。

この整理により、本書は静止画像を例外として扱いません。イラストも、Live2D モデルも、3D モデルも、ゲームアセットも、同じ二層構造を持つ対象として扱います。

なお、この整理は本書が構成した分析枠組みです。調査の当初は、静止画像と 3D アセットを別個の類型として扱う方針でしたが、4-4-1 と本項の検討を経て、両者を同格に扱う整理へ変更しています。第2章 2-3 で述べた統計の非対称性を、本書自身が再生産しないためです。第6章で対策を検討する際も、第9章で提言を行う際も、この整理を維持します。

4-6 空白の所在

以上を統合し、本章の結論を述べます。

空白は非映像デジタルアセット全般ではなく、一般 Web・複数形式を横断する共通保護層にあります。

これは抽象的な指摘ではありません。具体的に指し示すことができます。前章で述べたとおり、EME における鍵システムの能力指定は audioCapabilities と videoCapabilities として定義されており、画像・3D メッシュ・汎用アセットに対応する第三の項目は、2026 年 8 月時点の現行 EME 2 仕様にも定義されていません[20]。

そして重要なのは、この空白が「誰にも思いつけなかった」ものではないということです。

WebGPU Explainer は、cross-origin または DRM データを現行 WebGPU では扱えないと説明し、将来の候補として JavaScript から読み戻せない保護キューを挙げています[67]。これは実装済み機能ではありません。2018 年の議事録にも、WebGL と DRM コンテンツの関係で読み戻し権限のない GPU リソースを検討した記録があります[68]。

W3C には関連するコミュニティグループが複数存在しました。Web メディアへのアクセス・利用制限を議論する Restricted Media Community Group は 2023 年 4 月に、ストック写真や動画等のライセンスされたコンテンツを扱う Licensed Content Community Group は 2019 年 8 月に、クリエイター向けの保護・追跡を含むメディアコンテンツを探索する MFX Media Community Group は 2023 年 2 月に、いずれも閉鎖されています[69]。

Khronos のコミュニティフォーラムには 2020 年に「Asset protection for glTF」と題する議論が存在します[70]。Metaverse Standards Forum には Digital Asset Management を扱うグループが存在し、活動しています[71]。OpenUSD 側では 2026 年 5 月に IP 保護に関する提案が提出され、2026 年 8 月 28 日時点で Open かつ Draft の状態です[50]。

つまり、この問題は繰り返し認識され、複数の場で検討されてきました。それでも、本書が対象とする一般 Web・複数形式横断の共通保護層としては結実せず、いくつかの検討の場は閉鎖されました。

4-3 で確認した未接続部分のうち、経済的アンカーと適合性ガバナンスは制度の問題です。JPSEC では登録機関が設けられましたが、公開資料から登録項目を確認できず、2023 年版では登録機関に関する条項が非推奨化されました[26][27]。その原因は公開資料から確定できないため、担い手の属性だけに帰属させることはできません。

したがって、本書の中心的な主張は次のとおりです。

非映像デジタルアセットの技術的保護における課題は、暗号技術や GPU 能力そのものの不足ではありません。暗号化の規格、権利表現の規格、GPU レベルの保護機構、用途別の統合基盤が存在します。

本調査で確認した公開一次資料の範囲では、一般 Web 環境において、静止画像、Live2D モデル、汎用 3D モデル、アバター、テクスチャ、モーション、ゲームアセットを横断し、形式、標準 API、信頼された実行・描画境界、鍵・ライセンス運用、保護出力、適合性ガバナンスを一体として提供する共通層を確認できませんでした。

この接続は、個々のクリエイターやサービス事業者の努力だけで実現できるものではありません。標準化団体、プラットフォーム事業者、権利者、実装事業者、政策主体の協調を要する構造的課題です。

次章では、この構造がマーケットプレイスの現場でどのように現れるかを、ケーススタディとして検討します。

出典（第 4 章）

[1]:ISO/IEC 23001-7:2016, Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files（第 3 版）. <https://www.iso.org/standard/68042.html>

[2]:ISO/IEC 23001-7:2023（第 4 版）, 2023 年 8 月 8 日発行. 序文（画像アイテムを対象に含める旨）。目次上、第 8.3 項および第 8.4 項の存在を確認。規範的条項の本文は無償公開の対象外のため未確認。

<https://www.iso.org/standard/84637.html>

[3]:ISO/IEC 15444-8:2007, Information technology — JPEG 2000 image coding system: Secure JPEG 2000, 2007 年 4 月発行. <https://www.iso.org/standard/37382.html>

[4]:ISO/IEC 15444-8:2023（第 2 版）. <https://www.iso.org/standard/82566.html>

[5]:Recommendation ITU-T T.807 (V2), Information technology – JPEG 2000 image coding system: Secure JPEG 2000, ITU-T, 2023 年 2 月 13 日承認. <https://www.itu.int/rec/T-REC-T.807>

[6]:Call for contributions to JPEG Privacy, JPEG Committee, 2013 年 1 月 21 日.

https://jpeg.org/items/20130121_4.html

[7]:ISO/IEC 19566-4:2020, Information technologies — JPEG systems — Part 4: Privacy and security, 2020 年 3 月発行. <https://www.iso.org/standard/73607.html>

[8]:Draft Call for Proposals on JPEG Privacy & Security, ISO/IEC JTC 1/SC 29/WG 1 (JPEG), 文書番号 WG1N74015, 2017 年 1 月. https://jpeg.org/downloads/privacy_and_security/wg1n74015_Draft_CfP.pdf

[9]:OMA DRM Architecture V2.1, Open Mobile Alliance, 文書番号 OMA-AD-DRM-V2_1-20070724-C, 2007 年 7 月 24 日. https://www.openmobilealliance.org/release/drm/V2_1-20070724-C/OMA-AD-DRM-V2_1-20070724-C.pdf

[10]:Vodafone 804N 取扱説明書（英語版）, ソフトバンク公式アーカイブ.

<https://www.softbank.jp/en/mobile/set/data/support/users-guide/shared/sb804n/804n-e-manual.pdf>

[11]:ISO/IEC 14496-13:2004, Information technology — Coding of audio-visual objects — Part 13: Intellectual Property Management and Protection (IPMP) extensions, 2004 年 9 月発行.

<https://www.iso.org/standard/39110.html>

[12]:MPEG-4 Intellectual Property Management and Protection Extension (IPMP-X), MPEG 文書 N7505, 2005 年 7 月. <https://mpeg.chiariglione.org/standards/mpeg-4/ipmp-extensions.html>

[13]:ISO/IEC 21000-4:2006, Information technology — Multimedia framework (MPEG-21) — Part 4: Intellectual Property Management and Protection Components, 2006 年 4 月発行.

<https://www.iso.org/standard/41836.html>

[14]:ISO/IEC 21000-5:2004, Information technology — Multimedia framework (MPEG-21) — Part 5: Rights Expression Language, 2004 年 4 月発行. <https://www.iso.org/standard/36095.html>

[15]:Protected Memory, Vulkan Documentation Project, Khronos Group.

<https://docs.vulkan.org/guide/latest/protected.html>

[16]:VK_EXT_pipeline_protected_access, Vulkan Documentation Project, Khronos Group.

https://docs.vulkan.org/features/latest/features/proposals/VK_EXT_pipeline_protected_access.html

[17]:WebGPU, W3C Candidate Recommendation Draft, 2026 年 8 月 20 日. <https://www.w3.org/TR/webgpu/>

[18]:WebGL 2.0 Specification, Khronos Group, Editor's Draft, 2026 年 6 月 30 日.

<https://registry.khronos.org/webgl/specs/latest/2.0/>

WebGL Extension Registry, Khronos Group. <https://registry.khronos.org/webgl/extensions/>

[19]:EGL_EXT_protected_content, Khronos Group, Version 13, 2021 年 12 月 6 日.

https://registry.khronos.org/EGL/extensions/EXT/EGL_EXT_protected_content.txt

[20]:Encrypted Media Extensions 2, W3C Working Draft, 2026 年 7 月 7 日.

<https://www.w3.org/TR/encrypted-media-2/>

[21]:ISO/IEC 15444-8:2007 の適用範囲に関する ISO 公式カタログの記述.

<https://www.iso.org/standard/37382.html>

[22]:What is JPSEC RA?, JPSEC RA (特定非営利活動法人 Intellectual Resource Initiative) .

<https://www.jpsec-ra.jp/whatisra/>

[23]:Duties of JPSEC RA, JPSEC RA. <https://www.jpsec-ra.jp/duties/>

[24]:Contact information, JPSEC RA. <https://www.jpsec-ra.jp/contactinfomation/>

[25]:Statement of IRI, JPSEC RA. <https://www.jpsec-ra.jp/statement-of-iri/>

[26]:List of registered items, JPSEC RA, 2025 年 2 月 9 日保存版. 保存時点では登録項目が表示されていない。全期間の登録履歴を証明するものではない。

https://web.archive.org/web/20250209211023id_/https://www.jpsec-ra.jp/items/

[27]:Recommendation ITU-T T.807 (V2), Information technology — JPEG 2000 image coding system: Secure JPEG 2000, 2023 年 2 月. 2023 年版では JPSEC registration authority に関する第 7 条が非推奨化されています。

<https://www.itu.int/rec/T-REC-T.807>

[28]:Integrating PlayReady in Devices, Microsoft, 2018 年 11 月 6 日.

<https://learn.microsoft.com/en-us/playready/overview/integrating-in-devices>

[29]:RFC 9246, URI Signing for Content Delivery Network Interconnection (CDNI), IETF, 2022 年.

<https://www.rfc-editor.org/rfc/rfc9246.html>

[30]:Content Credentials: C2PA Technical Specification, Version 2.4, Coalition for Content Provenance and Authenticity.

https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA_Specification.html

- [31]:ISO/IEC 21617-1:2026, Information technology — JPEG Trust — Part 1: Core foundation.
<https://www.iso.org/standard/91405.html>
- [32]:ISO/IEC 21617-2 および ISO/IEC 21617-3 (いずれも開発中。2026 年 8 月確認) . ISO/IEC 21617-2
<https://www.iso.org/standard/89038.html>
ISO/IEC 21617-3. <https://www.iso.org/standard/90209.html>
JPEG Trust ワークプラン. <https://jpeg.org/jpegtrust/workplan.html>
- [33]:Are Content Credentials a form of DRM?, C2PA FAQ. (仕様本文ではなく FAQ における記述です。
<https://c2pa.org/faqs/>
- [34]:Xuandong Zhao et al., "Invisible Image Watermarks Are Provably Removable Using Generative AI," NeurIPS 2024.
https://proceedings.neurips.cc/paper_files/paper/2024/hash/10272bfd0371ef960ec557ed6c866058-Abstract-Conference.html
- [35]:Yuxin Wen et al., "Tree-Ring Watermarks: Fingerprints for Diffusion Images that are Invisible and Robust," NeurIPS 2023. <https://arxiv.org/abs/2305.20030>
- [36]:「組み込み用データ」Live2D Inc., 最終更新 2025 年 8 月 26 日.
<https://docs.live2d.com/cubism-editor-manual/export-moc3-motion3-files/>
- [37]:「モデルについて (Web)」Live2D Inc., Cubism SDK Manual.
<https://docs.live2d.com/4.2/en/cubism-sdk-manual/model-web/>
- [38]:「モーションについて」Live2D Inc., 最終更新 2026 年 1 月 29 日.
<https://docs.live2d.com/en/cubism-sdk-manual/motion/>
- [39]:「Live2D 作品の投稿」nizima (Live2D Inc.) . <https://docs.nizima.com/guide/item-upload/live2d/>
- [40]:「nizima に投稿できる作品の種類 nizima」 (Live2D Inc.) .
<https://docs.nizima.com/en/guide/item-upload/>
- [41]:「Live2D プレビュー操作ガイド」nizima (Live2D Inc.) . <https://docs.nizima.com/guide/preview-guide/>
- [42]:「ダイレクトメッセージの使い方」nizima (Live2D Inc.) . <https://docs.nizima.com/en/guide/direct-message/>
- [43]:「MOC3 Consistency Checker」Live2D Inc., 最終更新 2025 年 8 月 26 日.
<https://docs.live2d.com/en/cubism-editor-manual/moc3-consistency-checker/>
- [44]:ISO/IEC 12113:2022, Information technology — Runtime 3D asset delivery format — Khronos glTF™ 2.0, 2022 年 7 月 26 日発行. <https://www.iso.org/standard/83990.html>
- [45]:KHR_xmp_json_ld 拡張仕様, Khronos Group.
https://github.com/KhronosGroup/glTF/blob/main/extensions/2.0/Khronos/KHR_xmp_json_ld/README.md
- [46]:VRM 1.0 仕様 VRMC_vrm.meta, VRM コンソーシアム.
https://github.com/vrm-c/vrm-specification/blob/master/specification/VRMC_vrm-1.0/meta.ja.md
- [47]:ISO/IEC 23090-14:2025 (第 2 版) , Information technology — Coded representation of immersive media — Part 14: Scene description, 2025 年 11 月発行. <https://www.iso.org/standard/90191.html>
- [48]:MPEG Extends and Integrates glTF 2.0 into MPEG-I Scene Description ISO/IEC 23090, Khronos Group, 2024 年 7 月 26 日.
<https://www.khronos.org/blog/mpeg-extends-and-integrates-gltf-2.0-into-mpeg-i-scene-description-iso-iec-23090>
- [49]:[glTF 2.1] 64-bit upgrade to binary format, KhronosGroup/glTF Issue #2594, 2026 年 5 月 27 日. <https://github.com/KhronosGroup/glTF/issues/2594>
- [50]:Separation of Concerns for IP Protection in USD, PixarAnimationStudios/OpenUSD-proposals PR #107, 2026 年 5 月 14 日. <https://github.com/PixarAnimationStudios/OpenUSD-proposals/pull/107>
- [51]:VRChat Security Update, VRChat Inc., 2022 年 7 月.

<https://hello.vrchat.com/blog/vrchat-security-update>

[52]:Kai Wang et al., "A Comprehensive Survey on Three-Dimensional Mesh Watermarking," IEEE Transactions on Multimedia, 第 10 卷第 8 号, 2008 年 12 月. <https://ieeexplore.ieee.org/document/4694850/>

[53]:Xingyu Zhu et al., "Rethinking Mesh Watermark: Towards Highly Robust and Adaptable Deep 3D Mesh Watermarking," AAAI 2024. <https://ojs.aaai.org/index.php/AAAI/article/view/28613>

[54]:「AssetBundle Download Integrity and Security」 Unity Technologies.

<https://docs.unity3d.com/2023.1/Documentation/Manual/AssetBundles-Integrity.html>

[55]:「Protecting Content」 Unity Technologies, Unity 5.4 マニュアル (アーカイブ) .

<https://docs.unity3d.com/540/Documentation/Manual/protectingcontent.html>

[56]:「Interface IDataConverter」 Unity Technologies, [Addressables.CN](https://docs.unity3d.com/Packages/com.unity.addressables.cn@1.18/api/UnityEngine.ResourceManagement.ResourceProviders.IDataConverter.html) 1.18.11 API.

<https://docs.unity3d.com/Packages/com.unity.addressables.cn@1.18/api/UnityEngine.ResourceManagement.ResourceProviders.IDataConverter.html>

[57]:「Project Section of the Unreal Engine Project Settings」 Epic Games.

<https://dev.epicgames.com/documentation/unreal-engine/project-section-of-the-unreal-engine-project-settings>

[58]:「Packaging Projects」 Epic Games, Unreal Engine 4.27.

https://dev.epicgames.com/documentation/unreal-engine/packaging-projects?application_version=4.27

[59]:「FPakInfo」 および「RegisterEncryptionKey」 Epic Games, Unreal Engine API Reference.

<https://dev.epicgames.com/documentation/unreal-engine/API/Runtime/PakFile/FPakInfo>

[60]:Anti-Tamper game security, Denuvo by Irdeto. <https://irdeto.com/denuvo/anti-tamper/>

[61]:「DRM 機能 (デジタル作品保護機能) はありますか?」 BOOTH (ピクシブ株式会社) .

<https://booth.pixiv.help/hc/ja/articles/231284508>

[62]:「BOOTH 3D モデルカテゴリ 取引白書 2026」 ピクシブ株式会社, 2026 年 2 月 6 日.

<https://www.pixiv.co.jp/2026/02/06/110000>

[63]:「映像データの保存形式」『タイムベースト・メディアを用いた美術作品の修復／保存のガイド』京都市立芸術大学芸術資源研究センター (文化庁事業) , 2017 年 2 月 16 日.

<https://www.kcua.ac.jp/arc/time-based-media/?p=787>

[64]:Stock Footage, Getty Images. (2026 年 8 月確認)

<https://www.gettyimages.com/creative-video/stock-videos>

[65]:HLS requirements, Akamai Technologies. (2026 年 8 月確認)

<https://techdocs.akamai.com/msl/docs/hls-requirements>

[66]:glTF 2.0 Specification, The Khronos Group. 第 5 章 (スキニングおよびアニメーション) .

<https://registry.khronos.org/glTF/specs/2.0/glTF-2.0.html>

[67]:WebGPU Explainer, GPU for the Web Community Group. <https://gpuweb.github.io/gpuweb/explainer/>

[68]:Minutes 2018-01-10, GPU for the Web Community Group.

<https://github.com/gpuweb/gpuweb/wiki/Minutes-2018-01-10>

[69]:Past Community Groups, W3C. <https://www.w3.org/community/groups/past/>

[70]:Asset protection for glTF, Khronos Community Forums, 2020 年 7 月 24 日.

<https://community.khronos.org/t/asset-protection-for-gltf/106080>

[71]:Digital Asset Management Domain Group, Metaverse Standards Forum.

<https://portal.metaverse-standards.org/>

[72]:ID3D12Device4::CreateProtectedResourceSession, Microsoft Learn.

<https://learn.microsoft.com/en-us/windows/win32/api/d3d12/nf-d3d12-id3d12device4-createprotectedresourcesession>

- [73]:WebGPU Explainer, GPU for the Web Community Group. <https://gpuweb.github.io/gpuweb/explainer/>
- [74]:Radium LCP Specifications, Radium Foundation. <https://readium.org/lcp-specs/>
- [75]:3MF Secure Content Extension 1.0.2, 3MF Consortium.
https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf
- [76]:Materialise Identify3D, Materialise.
<https://www.materialise.com/en/industrial/software/identify3d>
- [77]:IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE 1735-2023. <https://standards.ieee.org/ieee/1735/7237/>
- [78]:Content Credentials, Leica Camera. C2PA に準拠したカメラ実装の公式資料.
<https://leica-camera.com/en-US/photography/content-credentials>
- [79]:Content Credentials in Adobe Photoshop, Adobe. 編集ソフトにおける付与機能の公式資料.
<https://helpx.adobe.com/photoshop/desktop/save-and-export/metadata-content-credentials/use-content-credentials.html>
- [80]:Edit images in Google Photos by simply asking, Google, 2025 年 8 月 20 日. Google Photos における C2PA Content Credentials 対応の公式資料.
<https://blog.google/products-and-platforms/products/photos/ai-photo-editing-google-photos/>

本章の記述に関する注記

- 4-3-4 の記述について。映像分野において、コンテンツを供給する側が「保護要件を満たさなければ供給しない」と表明した契約、公式声明、議会証言は、本調査の範囲では確認できませんでした。本文の記述は、保護要件が仕様として策定・公表されていること、および要件に対応しなかった場合の市場上の帰結をプラットフォーム側が公式に説明していることの範囲に限定しています。
- 4-4-1 および 4-4-3 の電子透かしに関する記述について。方式によって耐性が異なることが確認されています。本書は「電子透かしは無効である」と述べていません。また、リギングや UV 展開の変更に対する耐性を扱った研究は確認できませんでした。「確認できなかった」ことは「耐性がない」ことを意味しません。
- 4-4-3 の glTF 2.1 に関する記述について。同版は 2026 年 8 月時点でプレビュー段階です。予約フィールドの存在は Khronos の公開情報で確認できますが、暗号化機能を定義した採択済み仕様ではありません。
- 4-5-2 で用いた文化庁の保存ガイドおよびストックフッテージ市場の記述は、映像にも制作原本の層が存在することを示すために引用したものです。映像分野の保護実務を評価する趣旨ではありません。
- ITU-T の「作られも使われもしなかった (never created or used)」という記述の対象は、JPSEC 規格そのものではなく、その第 7 条が定めていた「JPSEC registration authority」です。本書は、この区別を厳密に保っています。
- 特定非営利活動法人 IRI の現在の活動状況、および ISO による登録機関指定の現況については確認できていません。
- nizima の内部実装 (サーバー側での preview.zip の展開・変換・配信方式) は公開資料では確認できないため、本章では公式ガイドに記載された範囲のみを記述しています。同社が独自の暗号化や端末拘束を実施しているか否かについては、確認も否定もしていません。
- Live2D 社および nizima について、本章はセキュリティ上の過失を指摘するものではありません。むしろ、公開資料から確認できる範囲で先進的な多層防御の実践例として扱っています。
- Unity Addressables の暗号化 API については、特定バージョンでの存在を確認したのみであり、現行の一般向けパッケージにおける状況は確認できていません。

第5章 ケーススタディ ― Web プレビューの構造的ジレンマ

前章では、暗号化規格、GPU 保護機構、用途別の統合基盤が存在する一方、一般 Web・複数形式を横断して、標準 API、信頼された実行・描画境界、鍵・ライセンス運用、適合性ガバナンスを接続する共通層は確認できないことを示しました。

本章では、この構造がマーケットプレイスの現場でどのように現れるかを検討します。

はじめに、本章の方針を明示します。本章は、特定の事業者のセキュリティ上の過失を指摘するものではありません。むしろ逆に、公開資料から確認できる範囲で先進的な設計を行っている事業者においてすら、個社の努力では届かない領域が残ることを示すために、これらの事例を取り上げます。また、特定の流出事案について、一次資料で確認できない内容を事実として記載することもしません。

5-1 プレビューは、欠かすことのできない機能です

保護を論じる際、最も単純な解決策は「プレビューをやめること」です。原本に近いデータをクライアントへ送らなければ、その経路からの取得は生じません。

しかし、この解決策は採用できません。理由は経済的なものです。

インタラクティブなアセットにおいて、購入判断に必要な情報は静止画では伝わりません。Live2D モデルであれば、表情がどう変化するか、口の開閉が自然か、髪や衣服の物理演算が破綻しないか、目線の追従が滑らかかといった要素が価値を決めます。3D モデルであれば、ポリゴンの流れ、リグの品質、モーション適用時の挙動が問題になります。これらは、実際に動かしてみなければ判断できません。

購入者が事前に品質を確認できない市場では、購入者は品質の不確実性を織り込んで低い価格しか払えなくなり、結果として高品質な出品者が市場から退出していきます。プレビューは、この情報の非対称性を緩和する機能を担っています。

しかも、この市場は既に相当の規模に達しています。ピクシブが公表した資料によれば、BOOTH の 3D モデルカテゴリの 2025 年の取扱高は約 104 億円、注文件数は約 774 万件であり、2023 年の約 31 億円から 2 年で 3 倍以上に拡大しています[1]。

したがって、問題はこう定式化されます。

プレビューを提供しなければ購入判断に必要な情報が不足し、プレビューを提供すればレンダリングに必要なデータがクライアント環境に存在することになります。

これが本章で扱うジレンマです。そして重要なのは、これが誰かの設計ミスではなく、インタラクティブアセットをクライアント側で描画する Web プレビューに内在する構造だという点です。

5-2 先進事例 ― 目的別のデータ分離という設計

このジレンマに対して、実務がどのような設計で応答しているかを見ます。Live2D 社が運営するマーケットプレイス nizima の公式ガイドは、その一例を明快に示しています。

同ガイドによれば、Cubism Editor からの出力により、編集できないモデルデータである `export.zip`、編集可能なデータである `original.zip`、そして作品詳細ページで表示するプレビュー用の `preview.zip` という三種類のデータが生成されます[2]。

この三つのデータの分離は、単なるファイル形式の違いではありません。目的ごとに、渡すデータの範囲を変えろという設計思想の表れです。

- `original.zip` は編集可能な最も価値の高いデータであり、その権利を購入した者にのみ渡されます
- `export.zip` は組み込んで使えるが編集はできないデータであり、用途に応じた中間的な提供物です
- `preview.zip` は購入判断のための表示専用データです

さらに、プレビュー側には複数の縮退措置が公式に説明されています。プレビュー用のテクスチャは販売用データより小さくできること、そして公開用の `preview.zip` 自体はダウンロード提供の対象ではないことが明記されています[3]。出品者が購入検討者へダイレクトメッセージで確認用データを送る場合には、受信者がダウンロード可

能であるため、解像度を落とした確認用データを用いることが推奨されています[4]。

整理すると、次の四種類の対策が組み合わされています。

手段	具体例	分類
データ分離	原本・組み込み用・プレビュー用の三つのデータの分離	データ最小化
データ縮退	プレビュー用テクスチャの縮小、DM 時の低解像度化	価値の低減
アクセス制御	preview.zip はダウンロード提供の対象外	取得主体の限定
利用条件	規約による許諾範囲の明示	契約的強制

これは、現行の技術的前提のもとで採り得る設計として、高い水準にあると評価できます。第 6 章で個別の対策を比較検討しますが、そこで挙げる主要な手段のほとんどが、既にここで実装されています。

ただし、二点を正確に述べておく必要があります。

第一に、これらを総称して「DRM」と呼ぶことは技術的に不正確です。データ分離、縮退、アクセス制御は、いずれも利用条件をクライアント側で技術的に強制する仕組みではありません。第 3 章で定義した用語に従えば、これらはデータ最小化、価値低減、アクセス制御に分類されます。

第二に、プレビュー用データがダウンロード提供の対象でないことと、ブラウザヘレンダリング用データが渡らないこととは、同義ではありません。前者はサービス上のアクセス制御であり、後者は Web 版 SDK の動作原理に関わる問題です。前章で確認したとおり、Cubism SDK for Web はモデルデータをバイト列として読み込んでモデルを生成します[5]。表示と操作が成立している以上、その計算に十分なデータがクライアント環境に存在します。

なお、同社がサーバー側で独自の暗号化や配信制御を実施しているか否かは、公開資料からは確認できません。本書は、その有無について確認も否定もしません。

5-3 「DRM 機能はありません」という明示

もう一つの事例を見ます。BOOTH の公式ヘルプは、DRM 機能を提供していないことを明記しています[6]。これは注目に値する記述です。3D モデルカテゴリだけで年間 100 億円規模に達する取引を扱うプラットフォームが[1]、技術的強制ではなく、契約とアクセス制御によって運営されていることを、自ら明示しているのです。

これを同社の怠慢と評価することはできません。前章で確認したとおり、本調査で確認した公開一次資料の範囲では、一般 Web・複数形式を横断して利用できる共通保護層を確認できないためです。仮に一社が独自の DRM を実装しても、そのままでは当該プラットフォーム外の制作ツールや他社サービスと相互運用できません。第 3 章で見た CENC のように、単一の暗号化データを複数のシステムへ接続する共通仕様と運用基盤が必要です。

むしろ、DRM 機能がないことを利用者に対して明示する姿勢は、誠実な情報開示として評価されるべきです。同様の状況は国外でも確認できます。VRChat は 2022 年のセキュリティ更新において、改造クライアントが利用者に無断でアバターの不正抽出とアーカイブ化を行っている実態を公式に指摘し、対策としてアンチチート技術を導入しました[7]。しかしこれは、実行プロセスの正当性を監視するアクセス制御であり、アセットデータを暗号化して利用条件を強制する DRM ではありません。

少なくとも本章で確認した BOOTH と VRChat の公開資料では、対策の中心はアクセス制御、契約または実行環境の監視です。これを市場全体の状況へ一般化することはできませんが、一般 Web・複数形式横断の共通保護層が確認できないという前章の分析と整合します。

5-4 個社の努力が届かない領域

ここまでの事例を、第 3 章で整理した七つの条件に照らして評価します。

条件	個社の努力で到達できるか
① 共通暗号化フォーマット	自社形式は作成できるが、相互運用可能な共通形式には標準化団体と複数の実装者が必要
② 標準インターフェース	自社 API は作成できるが、一般 Web の標準 API には標準化団体とブラウザベンダーの協力が必要

③ 厳密な信頼境界	個別アプリでは構築できる場合があるが、一般 Web の共通境界には DRM、User Agent、OS、GPU 等の協調が必要
④ ハードウェア隔離	ネイティブ GPU 機構は利用できる場合があるが、一般 Web からの標準接続経路は確認できない
⑤ 経済的アンカー	自社サービス内には形成できるが、複数形式横断の実装要求には継続的な需要側連携が必要
⑥ 適合性ガバナンス	自社内の審査は可能だが、サービス間の相互運用には共通の認証・適合性制度が必要
⑦ 法的裏付け	事業者は契約を整備できるが、立法自体は政策主体の領域

個社は各条件の一部を自社サービス内で実装できます。しかし、一般 Web・複数形式を横断する相互運用可能な仕組みへ広げるには、標準化団体、ブラウザ・OS・GPU 事業者、権利者、実装事業者、政策主体の協調が必要です。本章で見た事例は、個社が到達可能な範囲を高い水準で埋めています。

この構造から、三つの帰結が生じます。

第一に、重複投資です。各社がそれぞれ独自にプレビュー方式、データ分離設計、ウォーターマーク、アクセス制御を設計しています。相互運用可能な共通仕様があれば共通化できる部分についても、各事業者が個別に実装・運用する必要があります。中小の事業者や個人クリエイターにとって、この負担は無視できません。

第二に、水準のばらつきです。共通の要件が確認できないため、事業者ごとに対策の水準が異なります。その結果、相対的に取得しやすい経路が選ばれる可能性があります。共通の適合性要件がなければ、一社の対策を他社の経路へ引き継ぐことはできません。

第三に、事後追跡の断絶です。ウォーターマークによる識別は、埋め込まれた識別子を照合できて初めて機能します。しかし照合の仕組みが事業者ごとに閉じている場合、自社サービス外へ流出したデータについては、識別子が埋め込まれていても実効的な追跡が困難になります。第 3 章で見た映像分野が、複数の DRM 事業者と権利者の間に契約と適合性審査の網を張ることで実効性を確保したのとは対照的です。

さらに、越境の問題があります。取得されたアセットが国外のプラットフォームへ再アップロードされた場合、対応は削除要請と法的手段に依存します。横断的な流通制御や照会制度がなければ、権利者は事後的な対処を、自らの費用と労力で、しばしば言語の壁を越えて行うことになります。これは個人クリエイターによる権利行使を困難にする要因となります。

5-5 本章の結論

本章で確認したことを整理します。

第一に、プレビューは市場の成立に必要な機能であり、廃止は解決策になりません。インタラクティブアセットの品質は動かさなければ判断できず、購入者が品質を確認できない市場は成立しないためです。

第二に、実務は既に多層防御を実践しています。本章で確認した目的別のデータ分離、データ縮退、アクセス制御、利用条件の組み合わせは、現行の技術的前提のもとで採り得る有力な設計です。

第三に、それでもなお、個社の努力だけでは一般 Web・複数形式横断の共通層へ到達できません。標準インターフェース、信頼された実行・描画境界、ネイティブ GPU 機構への Web 標準接続、鍵・ライセンス運用、適合性ガバナンスを一体として構築するには、複数主体の協調が必要です。

したがって、本章の結論は次のとおりです。

本章で取り上げた事業者は、公開資料から確認できる範囲で、利用可能な手段を組み合わせています。それでも残る課題は、事業者の努力不足に起因するものではありません。

本調査で確認した公開一次資料の範囲では、一般 Web・複数形式を横断する共通保護層と制度を確認できません。そのため各事業者が個別に設計する必要があり、重複投資、水準のばらつき、事後追跡の断絶が生じます。

これは、個別の企業努力だけで解決できる問題ではありません。

次章では、ここまでに言及した個別の技術的対策について、何を防げて何を防げないのかを横断的に比較します。「完全に防止できる手段」は存在しないという前提のもとで、それぞれの手段が実際に何を達成し、どこに限界を持つのかを整理します。

出典（第 5 章）

[1]:「BOOTH 3D モデルカテゴリ 取引白書 2026」ピクシブ株式会社, 2026 年 2 月 6 日.

<https://www.pixiv.co.jp/2026/02/06/110000>

[2]:「Live2D 作品の投稿」nizima (Live2D Inc.) . <https://docs.nizima.com/guide/item-upload/live2d/>

[3]:「nizima に投稿できる作品の種類」nizima (Live2D Inc.) . <https://docs.nizima.com/en/guide/item-upload/>

[4]:「ダイレクトメッセージの使い方」nizima (Live2D Inc.) . <https://docs.nizima.com/en/guide/direct-message/>

[5]:「モデルについて (Web)」Live2D Inc., Cubism SDK Manual.

<https://docs.live2d.com/4.2/en/cubism-sdk-manual/model-web/>

[6]:「DRM 機能 (デジタル作品保護機能) がありますか?」BOOTH (ピクシブ株式会社) .

<https://booth.pixiv.help/hc/ja/articles/231284508>

[7]:VRChat Security Update, VRChat Inc., 2022 年 7 月. <https://hello.vrchat.com/blog/vrchat-security-update>

本章の記述に関する注記

- 本章で取り上げた事業者について、セキュリティ上の過失を指摘する意図はありません。公開資料から確認できる範囲で、現行の技術的前提のもとでの先進的な実践例として扱っています。
- 各事業者の内部実装（サーバー側での変換処理、独自の暗号化、配信制御の詳細）は公開資料では確認できないため、本章では公式ガイド・公式ヘルプに記載された範囲のみを記述しています。実装されていない対策があると主張するものではありません。
- 特定の流出事案については、一次資料で確認できないため記載していません。
- 本章は、アセットの取得手法や、対策を回避する具体的な方法については一切記載していません。

第 6 章 既存対策の効果と限界

本章では、現在利用可能な技術的対策を横断的に比較します。

はじめに、本章の前提を明示します。

利用者の端末で表示・実行される情報について、取得を完全に防止する手段は存在しません。

これは技術の未熟さではなく、表示と実行という機能そのものに由来する制約です。第 3 章で確認したとおり、成熟した保護基盤を持つ映像分野においても、画面の撮影による取得までは防止できません。

したがって本章が問うのは「どれが完璧か」ではありません。それぞれの手段が何を達成し、どこに限界を持ち、どれだけの費用を要するかです。

6-1 六つの分類

対策を目的別に六つに分類します。この分類は、第 4 章で整理した層構造と対応しています。		
分類	考え方	第 4 章の層との対応
A 渡さない	価値の高いデータをそもそもクライアントへ送らない	層に依存しない 設計上の選択
B 価値を下げる	渡すデータから価値の源泉を削る	同上
C 取得主体を限定する	権限のない者による取得を防ぐ	アクセス制御 (DRM ではない)
D 実行環境を信頼する	復号後のデータを非信頼の環境から隔離する	②標準 API・③信頼境界 ・④ハードウェア隔離
E 事後に追跡する	流出時に出所を特定し、抑止力とする	⑥適合性ガバナンスに依存
F 異常を検知する	大量取得等の兆候を捉え、対処につなげる	運用の層

この分類の要点は、個社で実装できる範囲と、複数主体の協調が必要な範囲を分けることにあります。A・B・C・F は、個々の事業者が自社の判断で実装できます。E も自社サービス内では実装できますが、サービス外へ流出したデータを照合するには共通の識別・照会制度が必要です。D を一般 Web・複数形式横断の仕組みとして成立させるには、ブラウザ、OS、GPU、鍵・ライセンス運用、適合性審査等の接続が必要です。

6-2 各分類の検討

A 渡さない

プレビュー専用派生データは、原本とは別に、表示専用の派生物を生成して配信する方式です。原本の直接取得を回避でき、実装も比較的容易です。第 5 章で見た三つのデータの分離設計がこれにあたります。留意点は、派生データ自体が十分な価値を持つ場合、その取得は依然として損害となることです。

注目すべきは、この考え方が既に規格化されていたことです。第 4 章で述べたとおり、JPSEC は空間領域、解像度レベル、色成分、品質レイヤーの単位でセキュリティサービスを適用する設計を持ち[1]、JPEG 委員会は用途例として低解像度プレビューのみを許可し高解像度へのアクセスを制限する例を挙げていました[2]。現在の実務が到達している運用は、20 年前に国際規格として設計されていたものです。

サーバーサイドレンダリング／リモートレンダリングは、レンダリングをサーバー側で実行し、結果の映像のみをクライアントへ配信する方式です。原本データの直接配布を回避できるという点で、構造的に最も強力です。しかも配信物が映像である以上、第 3 章で見た映像分野の保護基盤を適用できる可能性があります。

ただし、三つの重い制約があります。

第一に、コストです。利用者ごとに GPU 処理と映像配信を継続するため、閲覧回数、解像度、フレームレート、セッション時間に応じて計算資源と帯域の費用が増加します。通常の静止画・動画プレビューよりも、容量設計と障害対応を含む運用負担が大きくなります。

第二に、同時接続の制約です。利用者ごとに独立した描画状態と入力処理が必要なため、多数の閲覧者を同時に扱うマーケットプレイスでは、GPU 資源の分割、セッション管理、待ち時間、地域ごとの配信容量が障壁となります。

第三に、商用サービスの安定性です。Microsoft の Azure Remote Rendering は 2025 年 9 月 30 日をもって廃止されました[6]。この分野の商用基盤が必ずしも長期に維持されないことを示す実例です。

加えて、保護上の限界も正確に述べる必要があります。多視点の画像から三次元形状や新規視点表現を再構成する技術は、査読研究として確立されています[7][8]。したがってこの方式は、原本データの直接取得を回避する手段ではあっても、表示内容から得られる情報の漏えいまで防ぐ手段ではありません。ただし、元のトポロジー、UV 展開、リグ、シェーダー構成、編集履歴まで同一に復元できることを示す研究は確認できていません。

現実的な運用は、静止画・動画を通常のプレビューとし、価値の高いアセットや購入意図の明確な利用者に限って短時間のインタラクティブセッションへ昇格させるハイブリッド構成です。

B 価値を下げる

解像度低下は、テクスチャや画像の解像度を落として配信する方式です。実装が容易で、閲覧用途を満たしつつ再利用価値を下げられます。第 5 章で見た nizima の公式ガイドにも、プレビュー用テクスチャの縮小と、確認用データの低解像度化が示されています[9]。限界は、低解像度でも十分な用途（SNS 表示等）には効果が薄いことです。

機能削減は、モーションの一部のみを提供する、ポリゴン数を削減する、リグを含めない、レイヤーを統合するといった方式です。原本と表示物の距離が大きいという第 4 章 4-5 の指摘は、裏返せば、価値の源泉を削った派生物を作りやすいということでもあります。イラストであればレイヤーを統合した平坦な画像、Live2D モデルであればモーションを限定した実行用データ、3D モデルであればリグを除いた形状データが、これにあたります。

可視ウォーターマークは、作品上に識別表示を重畳する方式です。そのままの再利用に対する抑止となりますが、除去や、重畳部分を避けた利用は防げません。

C 取得主体を限定する

この分類の手段は広く普及していますが、その位置づけを誤解しないことが重要です。

暗号化配信（TLS）は伝送路の秘匿であり、正規の受信者に届いた後のデータを保護しません。

Signed URL と短寿命トークンは、権限のない第三者による取得を防ぎます。しかし、これはコンテンツ保護ではありません。この区別は標準文書自体が明示しています。CDN 相互接続における URI 署名を規定する RFC 9246 は、URI 署名がコンテンツ保護スキームではなく、コンテンツ自体の保護には別の仕組みが必要である旨を述べています[10]。

セッション認証は、認証された利用者に配信を限定します。Device Binding は特定の端末に利用を紐づけますが、Web 環境では端末識別子の取得手段が限られ、プライバシー保護の観点からも制約があります。

Rate Limit、Bot Detection、Anti-Scraping は、大量の自動取得を抑制します。対象と実装が適合すれば、比較的導入しやすく、網羅的な収集の時間と費用を引き上げられます。限界は、正規利用者が自身の権限内で行う取得を対象としないことです。

D 実行環境を信頼する

この分類が、本書の中心的な論点です。

ライセンス管理、Key Rotation、Revocation は、利用条件を継続的に管理・更新・失効させる仕組みです。映像

分野では DRM 事業者と適合性審査によって支えられています。電子出版、積層造形、電子設計 IP 等には用途別の基盤が存在します[20][21][22]。一方、本調査で確認した公開一次資料の範囲では、一般 Web・複数形式を横断してこれを担う共通基盤は確認できませんでした。

WebCrypto はブラウザ標準の暗号 API です。鍵素材を取り出せない形で扱うことは可能ですが、アプリケーションが復号結果を利用する構成では、復号後のデータを JavaScript から隔離する保護描画経路を WebCrypto 自体は定義しません。第 3 章で見た DRM 固有 CDM、User Agent、TEE、secure media pipeline 等を接続した信頼境界とは役割が異なります。

WASM と難読化は、処理内容の解析コストを引き上げます。実装は比較的容易で、一定の抑止効果があります。しかし、十分な動機を持つ解析者に対する恒久的な保護ではありません。

Anti-Tamper は、実行ファイルの改変やデバッガの接続、コード注入を検知・妨害します[11]。ただし対象範囲の区別が必要です。これは実行ファイルの保護であって、レンダリング中にメモリ上へ展開されたアセットデータの秘密性を保証する機能ではありません。

TEE および Hardware-backed Protection は、この分類の中核です。第 4 章で確認したとおり、Vulkan の保護メモリ等の機構は仕様として存在しますが、対応はオプションまたは実装依存です[12]。Khronos の公開資料は、保護メモリへアクセスするパイプラインが少数であるとの設計前提を示しています[13]。本調査で確認した公開一次資料の範囲では、汎用 3D アセット保護としての広範な商用実装は確認できませんでしたが、これは市場全体で利用されていないことを意味しません。

2026 年 8 月 28 日時点の公開 WebGPU 仕様、WebGL 仕様および登録拡張には、ネイティブ GPU の保護資源を汎用アセット向けに利用する標準の保護セッション、保護キューまたは保護リソース API を確認できませんでした[3][4]。WebGPU Explainer は将来の候補として JavaScript から読み戻せない保護キューを挙げていますが、実装済み機能ではありません[5]。したがって不足しているのは GPU 能力そのものではなく、Web 標準 API、信頼境界、鍵・ライセンス運用、保護出力、適合性制度を結ぶ経路です。

ゲームエンジンの開発元自身が、この分類の限界を明示的に述べています。Unity の公式マニュアルは、クライアントがデータを受け取った後は、十分な動機を持つ第三者による取得を暗号化だけで防ぐことは困難であるという趣旨を記載しています[14]。Unreal Engine の公式ドキュメントは、Pak 暗号化の目的をデータ抽出や改変を妨げるものとして説明しており、不可能にするとは表現していません[15]。

要するに、用途別には複数の層を接続した基盤が成立していますが、一般 Web・複数形式横断の経路では、個別の部品が共通の運用基盤として接続されていません。

E 事後に追跡する

個体識別ウォーターマークは、配信のたびに購入者や閲覧者を識別する情報を埋め込む方式です。流出時に出所を特定でき、その事実自体が抑止力として働きます。取得を防ぐのではなく、取得後の行動を抑止するという点で、性質が異なります。

Forensic Fingerprinting も同様の目的を持ちます。3D メッシュへの電子透かしには研究の蓄積があり、相似変換やノイズ付加には高い耐性を示します。しかし、ポリゴン削減、再トポロジ、頂点順序の変更といった位相構造を破壊する操作に対しては抽出が困難になる場合が多く報告されています[16]。近年の深層学習を用いた手法では耐性の向上が報告されていますが[17]、リギングや UV 展開のやり直しに対する耐性を扱った研究は確認できませんでした。

静止画については、画素レベルに情報を埋め込む方式において、生成モデルを介した再構成で検出が損なわれ得ることが査読研究で示されています[18]。一方、生成過程そのものに情報を埋め込む方式では、同種の攻撃下でも検出が維持されたとする報告があります[19]。方式によって耐性が異なるため、「電子透かしは生成 AI によって無効化される」という一般化はできません。

そして最大の制約は、技術だけでなく制度にもあります。埋め込まれた識別子は、照合できて初めて機能します。

照合の仕組みが事業者ごとに閉じていれば、自社サービス外へ流出したデータの追跡は困難です。一般 Web・複数形式横断の識別・照会・適合性制度を確認できないという第 4 章の問題が、ここに直接現れます。

F 異常を検知する

Honey Asset は、実在しないアセットや識別用のデータを配置し、それが外部に現れた場合に不正取得の経路を推定する手法です。低コストで実装でき、検知の起点として有用です。

Audit Log は、アクセスと配信の記録を残す運用です。それ自体は何も防ぎませんが、異常の検知、事後の立証、対策の評価の基礎となります。個人情報の取扱いと保存期間の設計が必要である点に留意が必要です。

手段	主に防げるもの	防げないもの	実装 難易度	運用 コスト	Web	Native	標準化の余地
A 渡さない							
プレビュー専用派生データ	原本の直接取得	派生データ自体の取得	低	低	○	○	高(JPSEC に前例あり)
サーバーサイド リモートレンダリング	原本データの配布	表示内容の取得、多視点からの近似再構成	高	極めて高	○	○	中
B 価値を下げる							
解像度低下	高解像度用途での再利用	低解像度で足りる用途	低	低	○	○	中
機能削減	完全な再利用	提供部分の再利用	低	低	○	○	中
可視ウォーターマーク	そのままの商用利用	除去、回避した利用	低	低	○	○	中
C 取得主体を限定する							
暗号化配信 (TLS)	経路上の傍受	受信後のデータ利用	低	低	○	○	済 (標準)
Signed URL／短寿命トークン	権限外の取得、URL 共有	権限内の利用者による取得	低	低	○	○	済 (RFC 9246)
セッション認証	未認証者の取得	認証済み利用者の取得	低	低	○	○	済
Device Binding	他端末での利用	同一端末での取得	中	中	△	○	中
Rate Limit	大量・網羅的な自動取得	少量の手動取得	低	低	○	○	中
Bot Detection／Anti-Scraping	自動収集	人手による取得	中	中	○	○	中
D 実行環境を信頼する							
ライセンス管理	条件外の利用 (基盤がある場合)	共通基盤がなければサービス間で相互運用できない	高	高	△	○	高 (最重要)
Key Rotation／Revocation	漏えい鍵の継続利用	既に取得されたデータ	中	中	△	○	高
WebCrypto	保管・伝送時の秘匿	復号後のデータの露出	中	低	○	○	済
WASM／難読化	容易な解析	動機を持つ解析者	中	低	○	○	低
Anti-Tamper	実行ファイルの改変・解析	メモリ上のアセットの秘密性	高	高	×	○	低
TEE／Hardware-backed	復号後データの一般環境への露出	画面の撮影	極めて高	高	×	△	高
E 事後に追跡する							
個体識別ウォーターマーク	(抑止) 流出後の匿名性	取得そのもの	中	中	○	○	高
Forensic Fingerprinting	同上	大幅な改変、再生成	高	中	○	○	高
F 異常を検知する							
Honey Asset	(検知) 取得経路の推定	取得そのもの	低	低	○	○	低
Audit Log	(検知・立証)	取得そのもの	低	中	○	○	中

○=対応可能 △=用途・実装上の制約あり ×=一般 Web で利用できる標準的な仕組みを確認できない

6-4 本章の結論

三点を指摘します。

第一に、多くの場合に費用対効果が高いのは A・B・C の組み合わせです。プレビュー専用派生データ、解像度低下、機能削減、アクセス制御、Rate Limit の組み合わせは、原本の直接取得を避け、大量・網羅的な取得のコストを引き上げます。具体的な効果は対象と実装により異なりますが、第 5 章の事例は、実務がこれらを組み合わせていることを示します。したがって、本書は「事業者が対策を怠っている」とは主張しません。

第二に、D を一般 Web・複数形式横断の仕組みとして成立させることは、個社の努力だけでは困難です。ライセンス管理、TEE、Hardware-backed Protection を接続するには、ブラウザ、OS、GPU、鍵・ライセンス運用、保護出力、適合性審査が必要です。ただし、Radium LCP、3MF Secure Content、Identify3D、IEEE 1735 のように、対象分野と実装環境を限定した基盤は既に存在します[20][21][22]。課題は技術の全面的不在ではなく、一般 Web・複数形式横断の共通層が確認できないことです。

第三に、E のサービス外での実効性も制度に依存します。ウォーターマークの技術的耐性が向上しても、識別子を横断的に照合する仕組みがなければ、追跡は自社サービス内に閉じます。技術と制度は分離できません。

以上を踏まえ、対策の全体像を次のように整理できます。

現在の実務では、A・B・C・F を組み合わせることで、原本の直接配布を避け、大量・網羅的な取得のコストを引き上げることができます。

D は用途別には成立例がありますが、一般 Web・複数形式横断の共通層としては確認できません。E は個社で実装できるものの、サービス外での照合には共通制度が必要です。いずれも横断的な実効性を個々の事業者だけで構築することは困難です。

また、どの手段を組み合わせても、表示された情報の取得を完全に防ぐことはできません。目指すべきは完全防止ではなく、不正取得の技術的・経済的コストを引き上げ、流出時の追跡可能性を高め、不正利用の誘因を削ぐことです。

次章では、ここまでの検討を統合し、「技術的保護格差」を定義したうえで、コンテンツ類型別の比較と、格差が生じた要因の分析を行います。

出典（第 6 章）

[1]:Recommendation ITU-T T.807 (V2), Information technology — JPEG 2000 image coding system: Secure JPEG 2000, ITU-T, 2023 年 2 月 13 日承認.

<https://www.itu.int/epublications/publication/itu-t-t-807-v2-2023-02-information-technology-jpeg-2000-image-coding-system-secure-jpeg-2000>

[2]:Call for contributions to JPEG Privacy, JPEG Committee, 2013 年 1 月 21 日.

https://jpeg.org/items/20130121_4.html

[3]:WebGPU, W3C Candidate Recommendation Draft, 2026 年 8 月 20 日. <https://www.w3.org/TR/webgpu/>

[4]:WebGL 2.0 Specification, Khronos Group, Editor's Draft, 2026 年 6 月 30 日.

<https://registry.khronos.org/webgl/specs/latest/2.0/>

WebGL Extension Registry, Khronos Group. <https://registry.khronos.org/webgl/extensions/>

[5]:WebGPU Explainer, GPU for the Web Community Group. <https://gpuweb.github.io/gpuweb/explainer/>

[6]:Azure products retirement in September 2025, Microsoft. Azure Remote Rendering の 2025 年 9 月 30 日廃止を確認する公式一覧.

<https://learn.microsoft.com/en-us/lifecycle/announcements/azure-products-retirement-september-2025>

- [7]:Mildenhall, B. et al., NeRF: Representing Scenes as Neural Radiance Fields for View Synthesis, ECCV 2020.
<https://arxiv.org/abs/2003.08934>
- [8]:Kerbl, B. et al., 3D Gaussian Splatting for Real-Time Radiance Field Rendering, ACM SIGGRAPH 2023.
<https://arxiv.org/abs/2308.04079>
- [9]:「nizima に投稿できる作品の種類」 nizima (Live2D Inc.) . <https://docs.nizima.com/en/guide/item-upload/>
「ダイレクトメッセージの使い方」 nizima (Live2D Inc.) . <https://docs.nizima.com/en/guide/direct-message/>
- [10]:RFC 9246, URI Signing for Content Delivery Network Interconnection (CDNI), IETF, 2022 年.
<https://www.rfc-editor.org/rfc/rfc9246.html>
- [11]:Anti-Tamper game security, Denuvo by Irdeto. <https://irdeto.com/denuvo/anti-tamper/>
- [12]:Protected Memory, Vulkan Documentation Project, Khronos Group.
<https://docs.vulkan.org/guide/latest/protected.html>
- [13]:VK_EXT_pipeline_protected_access, Vulkan Documentation Project, Khronos Group.
https://docs.vulkan.org/features/latest/features/proposals/VK_EXT_pipeline_protected_access.html
- [14]:「Protecting Content」 Unity Technologies, Unity 5.4 マニュアル (アーカイブ) .
<https://docs.unity3d.com/540/Documentation/Manual/protectingcontent.html>
- [15]:「Packaging Projects」 Epic Games, Unreal Engine 4.27.
https://dev.epicgames.com/documentation/unreal-engine/packaging-projects?application_version=4.27
- [16]:Kai Wang et al., "A Comprehensive Survey on Three-Dimensional Mesh Watermarking," IEEE Transactions on Multimedia, 第 10 巻第 8 号, 2008 年 12 月. <https://ieeexplore.ieee.org/document/4694850/>
- [17]:Xingyu Zhu et al., "Rethinking Mesh Watermark: Towards Highly Robust and Adaptable Deep 3D Mesh Watermarking," AAAI 2024. <https://ojs.aaai.org/index.php/AAAI/article/view/28613>
- [18]:Xuandong Zhao et al., "Invisible Image Watermarks Are Provably Removable Using Generative AI," NeurIPS 2024.
https://proceedings.neurips.cc/paper_files/paper/2024/hash/10272bfd0371ef960ec557ed6c866058-Abstract-Conference.html
- [19]:Yuxin Wen et al., "Tree-Ring Watermarks: Fingerprints for Diffusion Images that are Invisible and Robust," NeurIPS 2023. <https://arxiv.org/abs/2305.20030>
- [20]:Radium LCP Specifications, Radium Foundation. <https://radium.org/lcp-specs/>
- [21]:3MF Secure Content Extension 1.0.2, 3MF Consortium.
https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf
- Materialise Identify3D, Materialise. <https://www.materialise.com/en/industrial/software/identify3d>
- [22]:IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE 1735-2023. <https://standards.ieee.org/ieee/1735/7237/>

本章の記述に関する注記

- 表 2 の実装難易度・運用コストの評価は、一般的な構成を前提とした相対的な目安です。実際の値は、事業規模、既存の技術構成、対象アセットの性質によって大きく変動します。
- サーバーサイドレンダリングの費用は、利用するクラウド、リージョン、GPU、解像度、フレームレート、同時実行数、CDN 構成等によって大きく変動するため、本章では具体的な単価試算を行っていません。
- 本章は、各対策を回避する具体的な手法については記載していません。

第7章 「技術的保護格差」の定義と分析

前章までに、映像分野の保護基盤の構造、非映像デジタルアセットに適用できる技術と用途別基盤、一般 Web・複数形式横断の経路で確認できない接続、現場での実装の到達点、そして個別対策の効果と限界を検討してきました。

本章では、これらを統合し、本書の中心概念である「技術的保護格差」を定義します。そのうえでコンテンツ類型別の比較を行い、格差が生じた要因を分析します。

7-1 定義

本書は、「技術的保護格差」を次のように定義します。

技術的保護格差とは、コンテンツの類型と利用環境によって、権利者が利用できる技術的保護、信頼された実行・描画経路、ライセンス運用、適合性制度の厚みに体系的な差がある状態をいいます。

本書が主に扱う格差は、一般 Web 環境において、複数形式の非映像デジタルアセットを横断する共通保護層が確認できないことと、映像配信では複数の保護層が相互運用可能な運用基盤として接続されていることとの差です。

この定義には、四つの含意があります。

第一に、「保護技術や統合基盤が存在しない」という主張ではありません。第4章で確認したとおり、暗号化規格、権利表現規格、ネイティブ GPU の保護機構に加え、電子出版、積層造形、電子設計 IP 等には用途別の統合基盤も存在します[9][10][11][12]。

第二に、「完全な保護が可能な類型」が存在するという主張でもありません。第3章で述べたとおり、映像分野においても画面の撮影による取得は防止できません。格差は「完全か不完全か」ではなく、利用可能な防御層の厚みの差です。

第三に、格差の所在は接続関係として特定できます。個別の形式や GPU 機構ではなく、一般 Web で複数形式を扱うための標準 API、信頼された実行・描画境界、鍵・ライセンス運用、保護出力、経済的アンカー、適合性ガバナンスを一体として接続する共通層を、本調査で確認した公開一次資料の範囲では確認できませんでした[13][14]。

第四に、個々の事業者やクリエイターは、自社内のデータ分離、価値低減、アクセス制御、監視等を実装できます。しかし、一般 Web・複数形式横断の共通層へ広げるには、標準化団体、プラットフォーム事業者、OS・GPU 事業者、権利者、実装事業者、政策主体の協調が必要です。

7-2 コンテンツ類型別の比較

表 1-A 保護層の充足状況

第 3 章で整理した七つの条件のうち、①から⑥について、一般 Web での利用を中心に類型別の状況を整理します。用途別・独自実装として成立する仕組みと、複数形式横断の共通層を区別します。

類型	①共通暗号化	②標準 API	③信頼境界	④HW 隔離	⑤経済的アンカー	⑥適合性ガバナンス
映像・音声配信	○ CENC	○ EME	○ DRM 固有 CDM、User Agent、OS 等の合 成	○ TEE、secure media pipeline、出 力保護	○ 権利者・配信事 業者	○ 堅牢性規則と適合性審査
一般 Web の静止画像	○ CENC のアイテム 対応、JPSEC、19566- 4	— 横断 API 未 確認	— 共通境界未確 認	△ ネイティブ機構 はあるが Web 接続 未確認	△ 関係主体は存 在	△ JPSEC に旧登録制度あり。 保存公開一覧に項目は表示さ れていないが、全期間の履歴は 不明
一般 Web の Live2D モデル	△ 汎用暗号の適用は 可能	— 横断 API 未 確認	— 共通境界未確 認	△ ネイティブ機構 はあるが Web 接続 未確認	△ サービス内に は存在	△ サービス内運用に限定
一般 Web の 3D モデル・アバター	△ 汎用暗号・用途別 3MF は存在。glTF／ VRM に標準暗号化な し	— 横断 API 未 確認	— 共通境界未確 認	△ Vulkan 等は存 在。Web 接続未確認	△ 用途別には存 在	△ 用途別には存在
ゲーム・制作アセット	△ エンジン独自の暗 号化	△ 独自・ネイ ティブ API	△ Anti-Tamper 等の個別実装	△ ネイティブ機構	○ パブリッシャ ー・エンジン事業 者	△ ベンダー・サービス内に限 定

○＝対象となる利用環境で運用基盤として成立 △＝用途別、独自実装または部分的 —＝本調査で確認した公開一次資料の範囲では、一般 Web・複数形式横断の仕組みを確認できず

この表は、単一技術の有無ではなく、各層の接続範囲に差があることを示します。静止画像には映像と共通する暗号化規格があり、3D・製造・出版等には用途別基盤もあります。しかし、一般 Web で画像、Live2D、汎用 3D モデル、アバター、テクスチャ、モーション、ゲームアセットを横断する共通層は確認できません。

格差は暗号技術だけの差ではありません。

表 1-B 保護の便益に関わる性質

技術的な充足状況とは別に、類型ごとに「保護を強化することの便益」が異なります。

類型	制作原本・構造データが利用者端末に必要な	端末に渡るデータの再利用可能性	配信経路の保護で守れる範囲
映像・音声配信	制作原本は不要。配信用に符号化されたデータを受信	主に視聴用。制作原本と同一ではない	配信用データと再生経路を広く覆える
静止画像・イラスト	プレビューでは派生画像で足りる。提供目的により高解像度原本も渡る	表示、再投稿、印刷、素材利用等。品質は配信データに依存	派生データの伝送は守れるが、表示後の取得は残る
Live2D モデル	クライアント描画には実行用モデル、テクスチャ、設定が必要	改変・再演・別環境での利用に転用され得る	伝送・保管は守れるが、復号後の構造データに共通境界が必要
3D モデル・アバター	クライアント描画にはメッシュ、テクスチャ、アニメーション等が必要	改変・再演・組み込み等に転用され得る	伝送・保管は守れるが、復号後の構造データに共通境界が必要
ゲーム・制作アセット	実行用データをクライアントが参照する場合がある	別作品への流用等に転用され得る	独自・ネイティブ対策は可能。一般 Web 横断の評価とは分ける必要

第 4 章 4-5 で論じた構造が、ここに現れています。一般的な映像配信では、制作原本を端末へ渡さずに視聴目的を達成できます。一方、クライアント側で操作するアセットでは、表示と操作の計算に実行用の構造データが必要です。ただし、実行用データが常に編集可能な制作原本と同一であるとは限りません。

この差は、配信経路の保護だけで対応できる範囲を左右します。映像配信では、媒体暗号化から保護再生・出力までが接続されています。インタラクティブアセットでは、伝送と保管を暗号化しても、正規利用時に復号された構造データをどの実行・描画境界で扱うかという問題が残ります。

表 1-B の評価は本書が構成した相対的な整理であり、定量的な計測に基づくものではありません。また、表示物の層については、類型を問わず、鑑賞用途に対する保護の便益は小さくなります。静止画像でスクリーンショットが実用上の代替になり得ることと、3D モデルでレンダリング動画が鑑賞用途を満たし得ることは、同じ性質の現象です。

この二つの表を重ねると、本書の問題意識が明確になります。

映像配信では、媒体暗号化、標準 API、DRM 固有実装、保護された媒体経路、ライセンス、認証・適合性制度が接続されています。一般 Web の非映像アセットには個別規格、ネイティブ GPU 部品、用途別基盤がありますが、汎用の Web 経路と横断的な運用基盤は確認できません。この接続範囲の差が、本書のいう技術的保護格差です。この関係を図 3 に示します。

本書は、いずれの類型も同格に扱います。静止画像は、共通暗号化に利用できる規格が整備されていても、それだけでは一般 Web の保護運用が成立しないことを示す重要な事例です。この点は 7-3-1 で改めて論じます。

図3 技術的保護格差

格差は暗号技術やGPU能力の有無ではなく、複数層が運用基盤として接続される範囲にある。

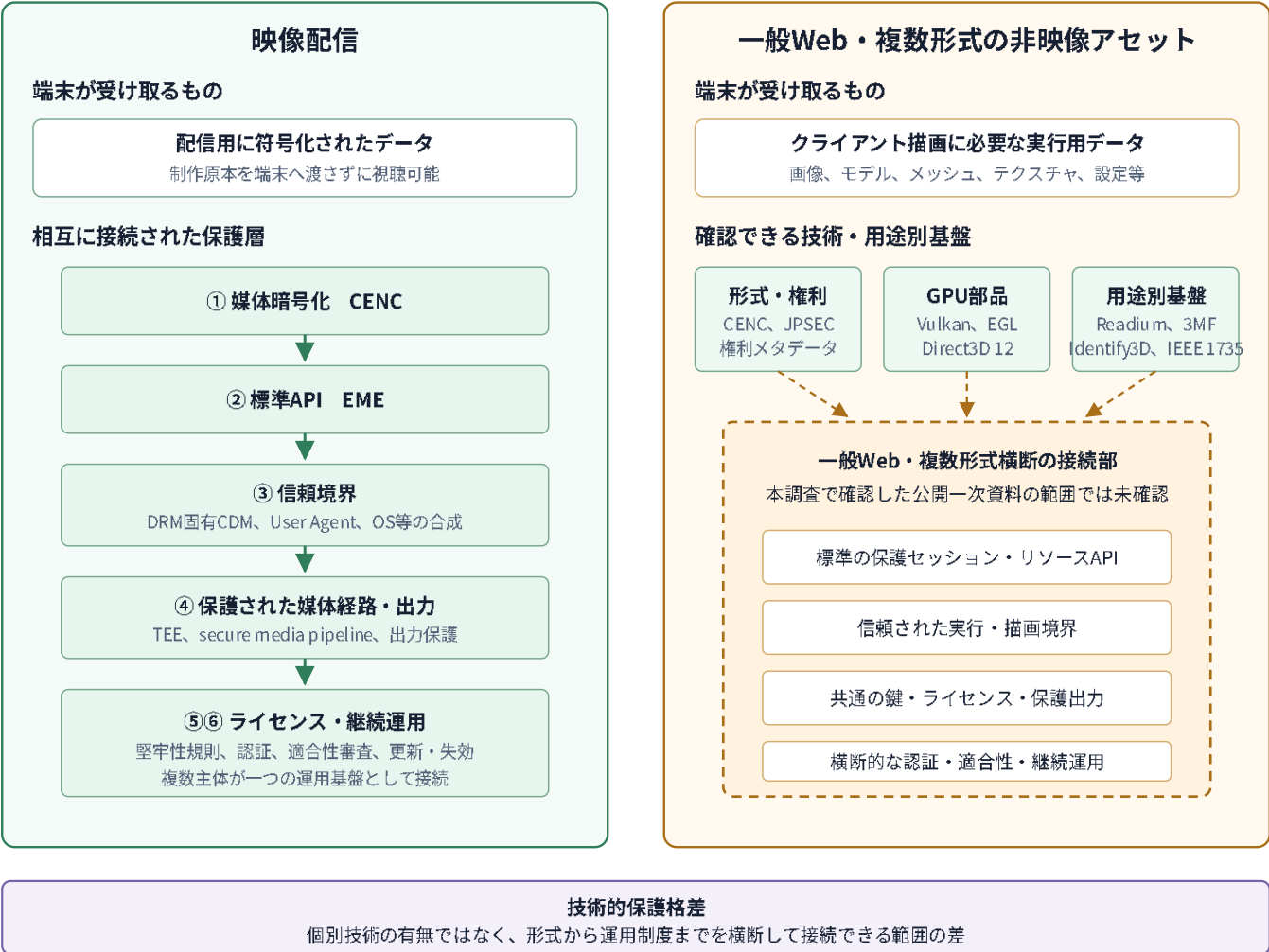


図 3 技術的保護格差

7-3 なぜ格差が生じたのか

7-3-1 技術的困難だけでは説明できません

格差の説明として、しばしば技術的困難が挙げられます。「3D データはレンダリングのためにアプリケーションが直接参照する必要があり、映像のような隔離は難しい」という説明です。

この説明には一定の妥当性があります。第 4 章で確認したとおり、映像の復号後データがデコーダからディスプレイへ方向に流れるのに対し、3D の頂点データはスキニング、物理演算、衝突判定によって繰り返し参照されます。保護メモリ上でこれを完結させるには、パイプライン全体の設計が必要になります。

しかし、この説明では格差の全体を説明できません。

重要な対照例は、静止画像です。静止画像には 3D のような頂点変形や物理演算はありません。CENC 第 4 版の公開要約はアイテムを対象に含め、JPSEC は条件付きアクセス等を規定しています[1][2]。ただし、本書は有料の CENC 規格本文にある個別ボックス及び適用条件を検証していません。したがって、3D 固有の計算上の困難だけでは、一般 Web・複数形式横断の格差全体を説明できません。

暗号化や条件付きアクセスの技術があっても、一般 Web の標準 API、信頼された実行・描画境界、ライセンス運

用、適合性制度まで接続されるとは限りません。

したがって、技術決定論では格差を説明できません。要因は別のところにあります。

7-3-2 要因1 需要側アンカーの有無

第3章3-6の条件⑤で述べたとおり、映像分野では、コンテンツを供給する側や DRM 事業者が保護要件を仕様・契約として策定し、端末・プラットフォーム側が対応を進めました。公開契約にも secure boot、鍵と平文経路の保護、出力保護等の堅牢性要件があります[15]。一方、保護レベルごとの全要件を体系的に示す公開公式資料は確認できておらず、供給条件との直接的な因果関係も本書では実証していません。

電子出版、積層造形、電子設計 IP、ゲーム等には、用途別の需要側主体や提供主体が存在します。一方、本調査で確認した公開一次資料の範囲では、一般 Web で複数の非映像形式を横断し、プラットフォームへ共通実装を継続的に求める主体は確認できませんでした。

OMA DRM には、通信事業者と端末ベンダーという実装主体が存在しました。ただし、その対象と運用体系は、本書が検討する一般 Web・複数形式横断の共通層とは異なります。

JPSEC、MPEG IPMP、ISO/IEC 19566-4 については、OS・ブラウザ・チップセット・アプリケーションの各ベンダーに一般 Web 向けの共通実装を継続的に求める横断的主体を、公開資料から確認することはできません。

本書が対象とするクリエイター向け市場では、権利者が個人クリエイター、小規模スタジオ、複数のマーケットプレイス等に分散しています。市場規模が大きくても、それだけでブラウザ、OS、GPU、制作ツールへ共通実装を求める継続的な交渉主体が形成されるとは限りません。横断的な要件形成と合意形成を支えることが、政策関与を検討する根拠の一つです。

7-3-3 要因2 利用環境の集中と分散

映像配信は、多様な端末を含みながらも、媒体形式、再生 API、DRM、保護出力等の役割分担が比較的標準化されています。共通の再生経路を実装する利益と主体が形成されました。

非映像デジタルアセットは、画像ビューア、3D エンジン、DCC ツール、ゲームエンジン、WebGL/WebGPU アプリケーション、OS のファイルビューア等、形式と利用目的が多様です。一般 Web の単一 API で対象範囲、権限、互換性、プライバシー、性能を調整する主体が形成されにくい構造があります。

7-3-4 要因3 標準化における設計選択

第4章で確認した二つの記録は、この要因を直接示しています。

MPEG-4 IPMP-X は、相互運用性の欠如を問題として認識しながら、機能インターフェースを定義するアプローチを採らなかったと記録しています。代わりに、メッセージルーターを介した通信方式を選択しました[3]。

MPEG-21 の IPMP Components と REL は、保護手段、鍵、鍵管理、信頼管理、暗号アルゴリズム、認証基盤を規定しません。汎用性を高める設計である一方、信頼されたクライアントと運用制度の構築は各実装に委ねられます[4]。

映像分野では、標準 API とは別に、ブラウザ、OS、チップセット、DRM 事業者、権利者の実装・契約・適合性制度が信頼境界を形成しました。用途別の非映像基盤でも統合主体は存在しますが、一般 Web・複数形式横断では同等の接続を確認できませんでした。

7-3-5 要因4 制度運用層を支える主体の有無

JPSEC 初版には、保護ツールの識別子を管理する登録機関制度がありました。2023 年版は旧第7条を削除し、旧登録機関の廃止を理由として登録機関を用いる仕組みを非推奨化しています[2][5]。2025 年2月9日付の保存公開一覧には登録項目が表示されていませんが、これは全期間の登録履歴又は制度変更の原因を証明するものではありません[16]。

一方、映像分野では、DRM 事業者が OEM に対し実装から適合性検証までを契約で求める継続的な運用があり

ます[6]。Readium LCP や IEEE 1735 等も、対象分野を限定して仕様、認証実装または信頼モデルを接続しています[9][12]。

この経過から JPSEC の利用実績や制度変更の原因を確定することはできないため、JPSEC 単独を運営主体又は制度設計の成否を示す因果的証拠には用いません。提言では一般原則として、仕様、実装、需要、費用、適合性、更新及び撤退時移行を別々に検証します。

7-3-6 要因 5 オープン性という設計思想との緊張

最後に、3D 分野に固有の要因を挙げます。これは、相互運用性、開放性、保護の強制をどの層で担うかという設計上の緊張です。

glTF は、ランタイム非依存性、拡張可能性、伝送効率を重視し、現行コア仕様と公式拡張には暗号化・利用条件の技術的強制を確認できません。VRM は、権利者の意思をファイルに明記するメタデータを規定しますが、その条件を技術的に強制する仕様ではありません[7]。OpenUSD 側の知的財産保護提案は、2026 年 8 月 28 日時点で Open かつ Draft であり、DRM、暗号方式、具体的なアクセス制御の実装をスコープ外としています[8]。

これらの事実は、現行の交換形式や提案だけで保護実行基盤まで完結しないことを示します。ただし、各標準化主体の動機や、将来の拡張可能性まで否定するものではありません。

本書は、開放性を誤りとして評価するものではありません。相互運用性を維持しながら、保護を形式、Web API、実行環境、ライセンス、制度のどの層に配置するかを検討する必要があります。その費用と便益を評価するための横断的な実態データは、本調査の範囲では確認できませんでした。この点は第 9 章で改めて論じます。

7-4 本章の結論

技術的保護格差の要因を整理すると、次のようになります。

要因	性質	個社で対処可能か
3D 等の双方向処理を保護境界内で扱う難しさ	技術	個社だけでは困難。研究開発と実装協調が必要
横断的な需要側アンカーを確認できないこと	経済・制度	個社だけでは困難
形式・利用環境・実装主体の分散	構造	個社だけでは困難
標準が実装詳細を各主体へ委ねること	制度・設計	標準化と複数実装者の協調が必要
継続的な認証・更新を担う主体の形成	制度	共通運用主体が必要
オープン性・相互運用性との調整	設計・政策	利害関係者の合意形成が必要

この六要因は、第 3 章 3-6 の七条件と、第 4 章から第 6 章までの事例を用いて構成した分析仮説です。技術上の難しさだけでなく、需要、標準化、利用環境、継続運用、相互運用性の調整が関係します。単一要因の因果効果を実証したものではなく、枠組みの外にある要因は検討範囲に入っていません。

したがって、本章の結論は次のとおりです。

技術的保護格差は、暗号技術や GPU 能力の有無だけでは説明できません。

用途別の保護基盤は存在しますが、本調査で確認した公開一次資料の範囲では、一般 Web において複数形式を横断し、形式、標準 API、信頼された実行・描画境界、鍵・ライセンス運用、保護出力、適合性ガバナンスを接続する共通層を確認できませんでした。映像配信では、これらに相当する複数層が運用基盤として接続されています。この接続範囲の差が、本書のいう技術的保護格差です。

解決の道筋には、技術開発だけでなく、需要の集約、標準化、相互運用、認証・適合性、継続運用の設計が必要です。本書は DRM の一律導入を求めるものではなく、利用目的とリスクに応じて参加・選択できる共通層を検討するものです。

次章では、この分析を踏まえ、次世代のデジタルアセット保護基盤がどのような設計原理を持つべきかを検討します。あわせて、DRM の義務化を提案するものではないことを明確にしたうえで、過去の失敗事例から得られる

教訓を整理します。

出典（第 7 章）

本章は第 3 章から第 6 章までの検討を統合したものであり、個別の事実に関する出典は各章に記載しています。本章で言及した主要な事実の出典は以下のとおりです。

[1]:ISO/IEC 23001-7:2023（第 4 版）, ISO. 公開要約は、共通暗号化がファイル、アイテム、トラック及びトラックフラグメントのメタデータを対象に含むことを示す。規格本文の個別ボックス及び適用条件は未確認。

<https://www.iso.org/standard/84637.html>

[2]:Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認. <https://www.itu.int/rec/T-REC-T.807>

[3]:MPEG-4 Intellectual Property Management and Protection Extension (IPMP-X), MPEG 文書 N7505, 2005 年 7 月. <https://mpeg.chiariglione.org/standards/mpeg-4/ipmp-extensions.html>

[4]:ISO/IEC 21000-4:2006 および ISO/IEC 21000-5:2004 の適用範囲に関する ISO 公式カタログの記述。

<https://www.iso.org/standard/41836.html> / <https://www.iso.org/standard/36095.html>

[5]:Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認. 2023 年版の本文及び旧登録機関制度の変更. <https://www.itu.int/rec/T-REC-T.807-202302-I/en>

[6]:Integrating PlayReady in Devices, Microsoft.

<https://learn.microsoft.com/en-us/playready/overview/integrating-in-devices>

[7]:VRM 1.0 仕様 VRMC_vrm.meta, VRM コンソーシアム.

https://github.com/vrm-c/vrm-specification/blob/master/specification/VRMC_vrm-1.0/meta.ja.md

[8]:Separation of Concerns for IP Protection in USD, PixarAnimationStudios/OpenUSD-proposals PR #107, 2026 年 5 月 14 日提出。2026 年 8 月 28 日時点で Open かつ Draft.

<https://github.com/PixarAnimationStudios/OpenUSD-proposals/pull/107>

[9]:Radium LCP Specifications, Radium Foundation. <https://readium.org/lcp-specs/>

[10]:3MF Secure Content Extension 1.0.2, 3MF Consortium.

https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf

[11]:Materialise Identify3D, Materialise. <https://www.materialise.com/en/industrial/software/identify3d>

[12]:IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE 1735-2023. <https://standards.ieee.org/ieee/1735/7237/>

[13]:WebGPU, W3C Candidate Recommendation Draft, 2026 年 8 月 20 日. <https://www.w3.org/TR/webgpu/>

[14]:WebGL 2.0 Specification および WebGL Extension Registry, Khronos Group.

<https://registry.khronos.org/webgl/specs/latest/2.0/> / <https://registry.khronos.org/webgl/extensions/>

[15]:Widevine License Agreement, Exhibit A, Google.

<https://developers.google.com/widevine/contact/widevine-mobile-license-use>

[16]:List of registered items, JPSEC RA, 2025 年 2 月 9 日保存版. 保存時点では登録項目が表示されていない。全期間の登録履歴を証明するものではない。

https://web.archive.org/web/20250209211023id_/https://www.jpsec-ra.jp/items/

本章の記述に関する注記

- 7-3 の要因分析は、第 3 章 3-6 で構成した七条件を分析枠組みとして用いたものです。本書は、この枠組みの外にある要因を検討していません。また、映像分野において七条件が成立した経緯そのものについては独自の実証を行っておらず、公開されている技術文書と各当事者の公式説明に依拠しています。したがって本章の要

因分析は、枠組みと整合する説明であって、因果関係を実証したものではありません。

- 表 1-B の「配信経路の保護で守れる範囲」は、本書が構成した相対的な整理です。定量的な計測に基づくものではありません。
- 7-3-2 について、映像分野において供給側が「保護要件を満たさなければ供給しない」と表明した契約、公式声明、議会証言は、本調査の範囲では確認できませんでした。第 3 章 3-6 の注記を参照してください。
- 表 1-A および表 1-B の評価は、本書の調査範囲において確認できた事実に基づく相対的な整理です。「一」は当該層を担う仕組みの絶対的な不存在ではなく、一般 Web・複数形式横断の仕組みを公開一次資料から確認できなかったことを意味します。
- 7-3-6 は、現行仕様と公開提案のスコープを比較したものです。標準化主体の動機、将来の仕様、開放性と保護の優劣を断定するものではありません。

第 8 章 次世代デジタルアセット保護基盤の構想

前章までの分析から、非映像デジタルアセットに保護技術が存在しないわけではないことが分かりました。電子出版の Radium LCP、積層造形の 3MF Secure Content と Materialise Identify3D、電子設計 IP の IEEE 1735 など、暗号化、ライセンス又は利用制御を接続した用途別基盤は既に存在します[17][18][19][20]。

一方、本書の調査で確認した公開一次資料の範囲では、一般 Web 環境において、静止画像、Live2D モデル、汎用 3D モデル、アバター、テクスチャ、モーション、ゲームアセットを横断し、共通暗号化形式、標準 API、信頼された実行・描画境界、ライセンス管理、適合性ガバナンスを一体として提供する共通層は確認できませんでした。

本章が構想するのは、用途別基盤を置き換える新しい一枚岩の DRM ではありません。既存技術と用途別基盤を相互運用可能な形で接続し、権利者が資産の性質、利用目的、脅威、費用に応じて必要な機能だけを選べる共通層です。

8-0 本章が提案しないこと

本書は、あらゆるデジタルアセットへの DRM の義務化を提案しません。この点を最初に明示する理由は三つあります。

教訓 1 CCCD の失敗

2000 年代前半、日本の音楽業界はコピーコントロール CD を導入しました。しかし、一部の再生機器で正常に再生できない、正規購入者の利便性を損なうといった問題が生じました。

文化審議会著作権分科会の私的録音録画小委員会が 2007 年 10 月にまとめた中間整理は、コピーコントロール CD が一部の OS で意図した効果を発揮せず、一部の CD プレーヤー等で正常に再生されない場合があったことなどを挙げ、同整理の作成時点で、これを発売しているレコード会社はない旨を記載しています[1]。

技術的保護は、正規利用の利便性や相互運用性を大きく損なえば、普及しません。本書は、この教訓を無視した提案を行いません。

教訓 2 EME 標準化への異論

第 3 章で述べたとおり、EME の標準化に際しては、オープンであるべき Web 標準に DRM との接続機構を組み込むことへの異論がありました。主な論点は、技術的保護手段の回避禁止規定が、セキュリティ研究や互換実装の開発を制約し得ることでした[2]。

同じ懸念は非映像デジタルアセットにも生じます。アーカイブ、研究、アクセシビリティ、修理、互換実装、権利者自身による長期保存を妨げない設計が必要です。

教訓 3 開放性がもたらしてきた便益

glTF や VRM は、異なる実装間での利用と交換を重視して発展してきました。VRM は、利用許諾に関するメタデータをファイルに記録する仕組みを備えています[3]。OpenUSD 側で 2026 年に提出された知的財産保護に関する提案も、本書の確認時点では Open かつ Draft であり、DRM、暗号方式、具体的なアクセス制御をスコープ外としています[4]。

これらは、相互運用性を維持しながら保護を加える難しさを示しています。保護のないアセットや非対応環境を排除する設計は避けるべきです。

したがって本章が目指すのは、保護を必要とする権利者が、必要な場面で、相互運用性を損なわずに利用できる選択肢が存在する状態です。

8-1 五つの設計原理

原理1 既存の層を分離して捉え、必要な接続だけを標準化する

映像分野の保護は、暗号化、標準 API、DRM 固有の実装、端末内の保護経路、ライセンス、出力保護、認証・適合性運用の接続によって成立しています。非映像分野にも暗号、メタデータ、GPU 保護資源、用途別ライセンス基盤などの部品は存在します。

したがって、すべてを新規に作り直すのではなく、各層の責任範囲を分け、相互運用に必要な境界と接続方法を定めるべきです。

原理2 任意参加と比例原則を採用する

保護を適用するか、どの水準を選ぶかは、権利者と提供者が資産の性質、利用目的、脅威、費用、正規利用への影響を踏まえて選べるようにします。保護を適用しないアセットは従来どおり流通でき、不参加を理由に不利益を受けない設計とします。

公開作品、共同編集用素材、販売用原本、期間限定プレビュー、機密設計データでは、必要な保護が異なります。すべてに同一の DRM を要求することは、費用対効果と比例原則の両面で適切ではありません。

原理3 相互運用性、可搬性、フォールバックを確保する

保護基盤の価値は、一事業者の製品内だけでなく、複数の形式、ツール、ブラウザ、OS、サービス間で必要な情報を引き継ぐときに生じます。

同時に、保護されていないアセットの流通、既存ツールの動作、正当な変換、長期保存を妨げてはなりません。保護機能に対応しない環境では、権利者が定めた範囲で低解像度表示、機能限定表示、代替形式、又は利用不可のいずれかを明示的に選べるフォールバックが必要です。

原理4 保護水準を段階化し、多層防御として組み合わせる

すべての利用にハードウェアによる信頼境界を要求する設計は、実装と参加の障壁を高くします。第6章で整理した既存対策には、原本を渡さない、価値を下げる、取得主体を限定する、実行環境を信頼する、事後に追跡する、異常を検知するという異なる役割があります。

保護基盤は、これらを単一の強度順に並べるのではなく、目的の異なるモジュールとして組み合わせられるようにします。各対策の限界を明示し、完全防止を約束しないことも設計要件です。

原理5 制度運用、透明性、プライバシーを技術と同時に設計する

技術仕様だけでは基盤は機能しません。JPSEC 初版には登録機関制度がありましたが、2023 年版は旧第7条を削除し、旧登録機関の廃止を理由として登録機関を用いる仕組みを非推奨化しています[5]。この経過だけから利用実績又は制度変更の原因を確定することはできません。したがって、仕様、実装、需要、費用、適合性、更新及び撤退時移行を別々に設計・検証する必要があります。

仕様の策定と同時に、次の事項を定める必要があります。

- 仕様の維持主体と意思決定手続
- 適合性審査の主体、基準、異議申立て
- 鍵、証明書、実装の失効と更新
- 障害時の復旧、撤退時の移行、長期保存
- 費用負担と小規模事業者への参加条件
- 収集する情報の最小化、利用目的、保存期間、第三者提供
- 利用者への表示、監査可能性、研究・アクセシビリティへの配慮

8-2 一般 Web・複数形式横断の共通層

構想する共通層は、用途別基盤を置き換えず、それらと一般 Web 環境を接続するための五つの機能層から成ります。

層 1 暗号化と安全なパッケージング

既存の部品として、CENC のアイテム対応[6]、JPSEC[7]、ISO/IEC 19566-4[8]、3MF Secure Content[17]、Radium LCP[18]、IEEE 1735[20]があります。これらは、静止画像、積層造形、電子出版、電子設計 IP など、それぞれの対象と運用条件に合わせて設計されています。

不足しているのは、Live2D モデル、汎用 3D モデル、アバター、テクスチャ、リグ、モーション等について、暗号化対象、鍵識別子、初期化情報、部分暗号化の単位を複数形式横断で扱う共通プロファイルです。glTF 2.1 の検討には将来の圧縮又は暗号化に利用し得る予約領域がありますが、glTF 2.1 自体が暗号化を定義しているわけではなく、版も本書の確認時点ではプレビュー段階です[9]。

層 2 識別子、権利・利用条件、来歴

既存の部品として、C2PA、JPEG Trust、IPTC 等のメタデータ、VRM の利用許諾メタデータ[3]、glTF の KHR_xmp_json_ld[10]、MPEG-21 REL[11]などがあります。

これらは、識別子、権利者、利用条件、来歴を記述するために利用できます。ただし、メタデータの記述は利用条件の技術的強制と同じではありません。また、形式やサービスを越えた相互変換、照合、訂正、更新の共通手続は未整備です。

層 3 Web 標準 API

EME は、HTMLMediaElement と Key System を接続する音声・映像向けの標準 API です。画像、3D メッシュ、汎用アセットを対象とする能力指定は定義されていません[12]。

2026 年 8 月 28 日時点の公開 WebGPU 仕様、WebGL 仕様及び登録拡張には、保護セッション、鍵システムの選択、保護リソースの生成、通常の JavaScript 環境への読み戻し制御を、汎用 3D アセット向けに接続する標準 API は確認できませんでした[21][22]。

この層は、一般 Web・複数形式横断の共通層における主要な未整備部分です。ブラウザ、OS、GPU、形式、鍵・ライセンス運用の責任境界を定める必要があります。

層 4 信頼された実行・描画と出力制御

Vulkan の保護メモリ[13][14]、EGL の保護コンテンツ拡張[23]、Direct3D 12 の Protected Resource Session[24]など、ネイティブ GPU 環境には利用可能な部品があります。ただし、対応はオプション又は実装依存であり、これらの仕様だけで DRM 要件やエンドツーエンドの保護が保証されるわけではありません。

不足しているのは、暗号化データを通常メモリへ露出させずに保護領域へ取り込み、保護された GPU 資源で処理し、読み戻しと出力を制御する経路を、層 3 の Web 標準 API、鍵・ライセンス、端末認証、適合性運用まで接続する横断的な実装基盤です。

層 5 ライセンス、適合性、失効、ガバナンス

Radium LCP、Identify3D、IEEE 1735 等の用途別基盤には、対象分野に応じたライセンス又は利用制御の運用があります[18][19][20]。したがって、この層の技術や制度が非映像分野全体で存在しないとは言えません。

一般 Web・複数形式横断の共通層として不足しているのは、利用条件の表現と強制の境界、実装の適合性審査、証明書・鍵・実装の失効と更新、障害時対応、費用負担、撤退時の移行を分野横断で扱う運用枠組みです。JPSEC 初版には登録機関制度がありました[5]。2025 年 2 月 9 日付の保存公開一覧には登録項目が表示されていませんが、

これは全期間の登録履歴又は制度変更の原因を証明するものではありません[15]。

8-3 段階的な実現の道筋

五つの層を同時に構築することは現実的ではありません。各段階が単独でも価値を持つよう、三段階に分けて進めます。以下の年数は確定的な工程表ではなく、検討の目安です。

第1段階 低介入の相互運用基盤

期間の目安：1年から3年

この段階では DRM を導入せず、次の作業を進めます。

1. 権利・ライセンス・来歴メタデータの対応表と変換規則を整備する
2. 作品・権利者・登録情報を事業者横断で照合するための識別子と問い合わせ手続を検討する
3. 不正取得、流出、削除対応、再発の測定方法を共通化する
4. 任意参加、情報最小化、訂正、異議申立て、監査、アクセシビリティの原則を先に定める
5. 小規模なクリエイター、事業者、利用者を含む公開のガバナンス体制を設計する

文化庁は 2026 年 2 月、分野横断権利情報検索システム及び個人クリエイター等権利情報登録システムの運用開始を公表しました[16]。この国内基盤との接続可能性を検討しつつ、ファイル内メタデータ、民間サービス、国際的な識別子との関係を整理する必要があります。

識別子照合と個体識別透かしは、利用者又は購入者に関する情報を扱い得ます。設計時には、参加の任意性、目的の限定、データ最小化、保存期間、第三者提供、開示・訂正、異議申立て、監査、追跡用途への転用禁止を要件とします。

第2段階 対象別プロファイルと実証

期間の目安：3年から7年

層1と層2について、対象形式ごとの暗号化単位、鍵識別子、権利表現、来歴情報のプロファイルを検討します。既存の 3MF、Radium LCP、IEEE 1735 等から、共通化できる要素と対象分野に残すべき要素を分けます。

層3と層4については、標準化を直ちに前提とせず、要件定義と実証を行います。保護セッション、保護リソース、鍵・ライセンス、信頼された実行・描画、出力制御、フォールバックをどの責任分界で接続できるかを検証します。実証には、正規利用の性能、互換性、アクセシビリティ、プライバシー、実装費用を含む評価が必要です。

第3段階 国際標準化と継続運用

期間の目安：7年以降

実証で有効性と必要性が確認された範囲について、W3C、Khronos、ISO/IEC 等の既存の場で国際標準化を検討します。日本単独の独自仕様を既成事実として広げるのではなく、相互運用性、競争中立性、研究可能性、アクセシビリティ、プライバシーを含む合意形成が必要です。

層5の制度設計は、第3段階まで待たず、第1段階から並行して進めます。技術仕様が完成しても、維持、適合性審査、失効、更新、費用負担、撤退時の移行が定まらなければ、継続運用できないためです。

各段階の開始、継続、拡張は、被害実態、導入効果、正規利用への影響、費用、プライバシーへの影響を公開評価し、見直せるようにします。

8-4 多層防御という考え方

保護基盤が整備されても、取得や再利用を完全に防止することはできません。成熟した映像分野でも、画面の撮影など保護経路の外側に残る取得方法があります。

したがって目指すべきは、単一の完全な障壁ではなく、資産と利用場面に応じて複数の対策を組み合わせ、不正取得の技術的・経済的コストを引き上げ、流出後の追跡と対応を可能にすることです。

図4は、第6章で整理した六つの対策を、既存の用途別基盤及び一般Web・複数形式横断の共通層と接続した構想を示します。

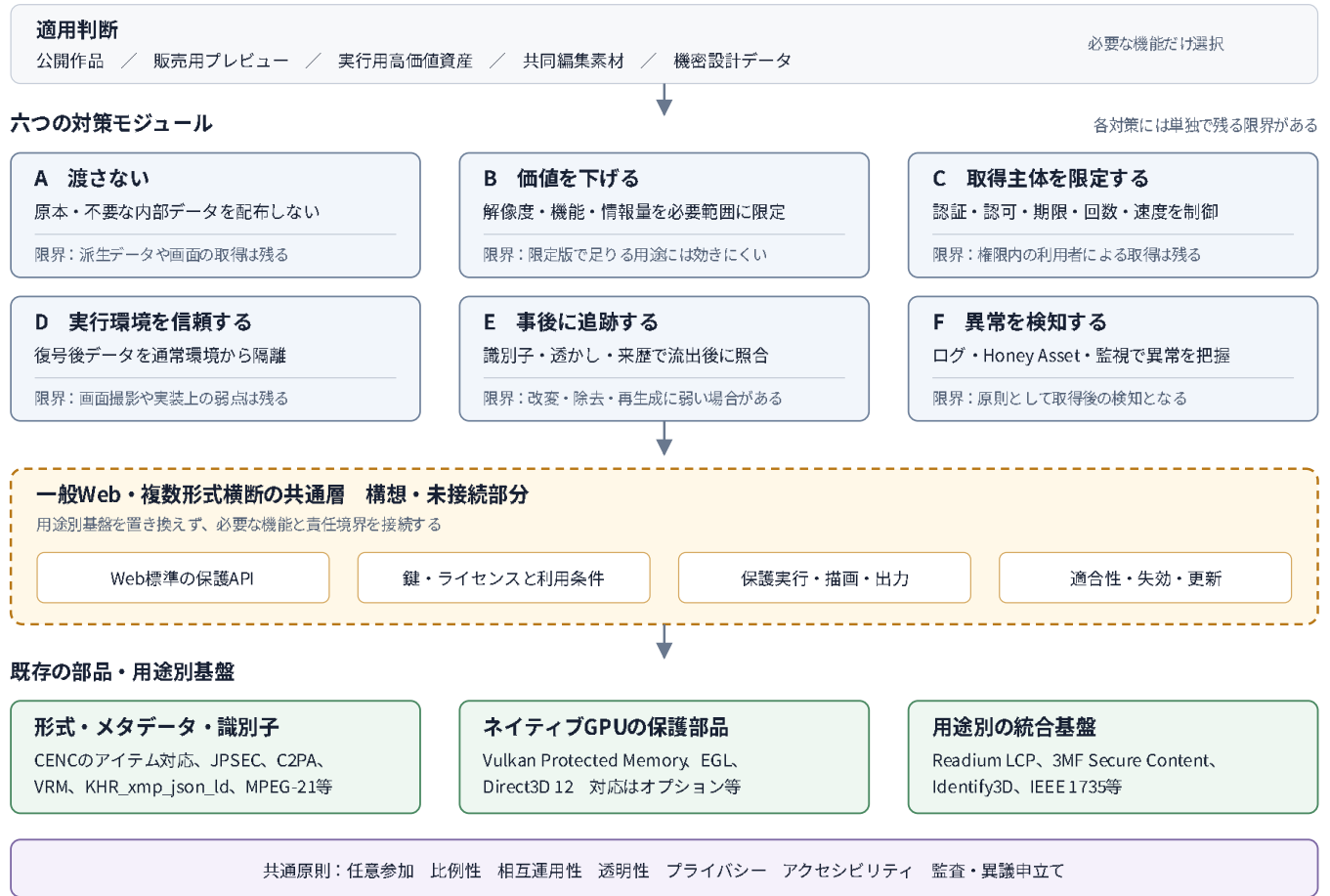
区分	主な役割	単独では残る限界
A 渡さない	原本や不要な内部データを配布しない	派生データや画面の取得は残る
B 価値を下げる	解像度、機能、情報量を必要範囲に限定する	限定版で足りる用途には効きにくい
C 取得主体を限定する	認証、認可、期限、回数、速度を制御する	権限を持つ利用者による取得は残る
D 実行環境を信頼する	復号後データを通常環境から隔離する	画面撮影や実装上の弱点は残る
E 事後に追跡する	識別子、透かし、 来歴により流出後の照合を助ける	改変、除去、再生成に弱い場合がある
F 異常を検知する	ログ、Honey Asset、 監視により異常を把握する	原則として取得後の検知となる

すべてのアセットに六区分を適用する必要はありません。公開作品では層2の権利・来歴情報だけを用い、販売用プレビューではA、B、Cを組み合わせ、高価値の実行用資産では条件が整った場合にDを追加し、流通後の対応が必要な場合にEとFを加えるなど、目的とリスクに応じて選択します。

Dについては、用途別基盤とネイティブGPUの部品が存在します。一方、一般Web・複数形式横断の利用では、Web標準API、鍵・ライセンス、保護された実行・描画、出力制御、適合性運用を接続する経路が、本書の確認した公開一次資料の範囲では確認できません。図4では、この未接続部分を既存部品と分けて示します。

図4 選択型の多層防御モデル

資産・利用目的・脅威・費用に応じて選択する。全アセットへの一律適用ではない。



注：破線枠は、本書が提案する一般Web・複数形式横断の接続層。既存部品や用途別基盤が存在しないことを示す図ではない。

8-5 構想が実現しない場合への備え

この領域では、過去の標準化の試みが継続しなかった例があります。また、一般 Web・複数形式横断の共通層は、多数の標準化団体、ブラウザ、OS、GPU、形式、サービス、権利者、利用者の合意を要します。構想全体が実現しない可能性も織り込む必要があります。

そのため、各段階を独立して利用できるようにします。

- 第 1 段階のメタデータ相互運用、識別子照合、被害指標、ガバナンス原則は、保護 Web API が実現しなくても利用できる
- 第 2 段階の対象別プロファイル、要件定義、実証結果は、個別形式や事業者の設計指針として利用できる
- 層 5 の運用設計は、対象を層 1 と層 2、又は特定の用途別基盤に限定しても利用できる
- 標準化を中止又は縮小する場合も、登録情報、鍵、証明書、アセットを移行又は保存する手順をあらかじめ定める

すべてが実現しなければ何も得られない構想にしないことが、継続可能性の条件です。

8-6 本章の結論

本書が構想するのは、DRM の義務化ではありません。用途別の先行基盤と既存技術を尊重しつつ、一般 Web・複数形式を横断して必要な機能を接続できる、任意参加の共通層です。

短期に着手できるのは、権利・来歴メタデータの相互運用、識別子照合、被害指標、ガバナンス原則です。保護 Web API と信頼された実行・描画の接続は、技術的にも制度的にも難しく、実証と国際的な合意形成を要します。

技術仕様と同時に、適合性、失効、更新、障害対応、費用負担、撤退時の移行、透明性、プライバシーを設計しなければなりません。各段階を公開評価し、必要性和比例性が認められた範囲だけを進めることが、本構想の前提です。

次章では、この構想を具体的な政策提言へ落とし込みます。

出典（第 8 章）

- [1]:文化審議会著作権分科会 私的録音録画小委員会「中間整理」文化庁, 2007 年 10 月 12 日. 第 49 頁および脚注 32. https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/h1910_rokuon_chukan.pdf
- [2]:Notice to the W3C of EFF's appeal of the Director's decision on EME, Electronic Frontier Foundation, 2017 年 7 月 12 日. <https://lists.w3.org/Archives/Public/public-html-media/2017Jul/0005.html>
- [3]:VRM 1.0 仕様 VRMC_vrm.meta, VRM コンソーシアム, https://github.com/vrm-c/vrm-specification/blob/master/specification/VRMC_vrm-1.0/meta.ja.md
- [4]:Separation of Concerns for IP Protection in USD, PixarAnimationStudios/OpenUSD-proposals PR #107, 2026 年 5 月 14 日. <https://github.com/PixarAnimationStudios/OpenUSD-proposals/pull/107>
- [5]:Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認. 2023 年版の本文及び旧登録機関制度の変更. <https://www.itu.int/rec/T-REC-T.807-202302-I/en>
- [6]:ISO/IEC 23001-7:2023 (第 4 版), ISO. 公開要約は、共通暗号化がファイル、アイテム、トラック及びトラックフラグメントのメタデータを対象に含むことを示す。規格本文の個別ボックス及び適用条件は未確認. <https://www.iso.org/standard/84637.html>
- [7]:Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認. <https://www.itu.int/rec/T-REC-T.807>

- [8]:ISO/IEC 19566-4:2020, Information technologies — JPEG systems — Part 4: Privacy and security, 2020 年 3 月発行. <https://www.iso.org/standard/73607.html>
- [9]:Introducing glTF 2.1 with Complex Scenes, Khronos Group, 2026 年.
<https://www.khronos.org/blog/introducing-gltf-2.1-with-complex-scenes>
; glTF Issue #2594. <https://github.com/KhronosGroup/glTF/issues/2594>
- [10]:KHR_xmp_json_ld 拡張仕様, Khronos Group.
https://github.com/KhronosGroup/glTF/blob/main/extensions/2.0/Khronos/KHR_xmp_json_ld/README.md
- [11]:ISO/IEC 21000-5:2004, Information technology — Multimedia framework (MPEG-21) — Part 5: Rights Expression Language, 2004 年 4 月発行. <https://www.iso.org/standard/36095.html>
- [12]:Encrypted Media Extensions 2, W3C Working Draft, 2026 年 7 月 7 日.
<https://www.w3.org/TR/encrypted-media-2/>
- [13]:Protected Memory, Vulkan Documentation Project, Khronos Group.
<https://docs.vulkan.org/guide/latest/protected.html>
- [14]:VK_EXT_pipeline_protected_access, Vulkan Documentation Project, Khronos Group.
https://registry.khronos.org/vulkan/specs/latest/man/html/VK_EXT_pipeline_protected_access.html
- [15]:List of registered items, JPSEC RA, 2025 年 2 月 9 日保存版. 保存時点では登録項目が表示されていない。全期間の登録履歴を証明するものではない。
https://web.archive.org/web/20250209211023id_/https://www.jpsec-ra.jp/items/
- [16]:「『分野横断権利情報検索システム』及び『個人クリエイター等権利情報登録システム』の運用開始について」文化庁, 2026 年 2 月 26 日. https://www.bunka.go.jp/koho_hodo_oshirase/hodohappyo/94333101.html
- [17]:3MF Secure Content Extension 1.0.2, 3MF Consortium.
https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf
- [18]:Radium LCP Specifications, Radium Foundation. <https://readium.org/lcp-specs/>
- [19]:Materialise Identify3D, Materialise. <https://www.materialise.com/en/industrial/software/identify3d>
- [20]:IEEE 1735-2023, IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE Standards Association. <https://standards.ieee.org/ieee/1735/7237/>
- [21]:WebGPU, W3C, 2026 年 8 月 20 日版. <https://www.w3.org/TR/webgpu/>
- [22]:WebGL Extension Registry, Khronos Group. <https://registry.khronos.org/webgl/extensions/>
- [23]:EGL_EXT_protected_content, Khronos Group.
https://registry.khronos.org/EGL/extensions/EXT/EGL_EXT_protected_content.txt
- [24]:CreateProtectedResourceSession, Microsoft Learn.
<https://learn.microsoft.com/en-us/windows/win32/api/d3d12/nf-d3d12-id3d12device4-createprotectedresourcesession>

本章の記述に関する注記

- 「確認できない」という記述は、2026 年 8 月 28 日までに公開されていた仕様、公式レジストリ、公式資料を対象とします。非公開システム、契約者限定機能、未索引資料まで含む不存在を意味しません。
- 8-3 で示した年数は、検討順序を示す目安であり、確定的な実施時期ではありません。
- 本章は保護基盤の構想を述べるものであり、特定の実装方式又は製品を推奨するものではありません。
- 権利表現、識別子、来歴、ライセンスの既存仕様は、本章で挙げたものに限りません。標準化の開始前に対象範囲を改めて調査する必要があります。

第9章 政策提言

前章までの分析を踏まえ、本章では具体的な政策提言を行います。

政策対象は、非映像デジタルアセット全般に新しい DRM を導入することではありません。電子出版、積層造形、電子設計 IP 等には用途別の保護基盤が既に存在します。本章が対象とするのは、一般 Web・複数形式を横断する相互運用、参加条件、実証、適合性、継続運用の枠組みです。

9-1 なぜ政策の関与が必要か

理由1 判断の基礎となるデータと共通指標が不足しています

非映像デジタルアセットの権利者は、個人クリエイター、小規模スタジオ、中小事業者に広く分散しています。不正取得、無断再配布、無断再販売、対策費用、削除要請の結果を共通の方法で集計する仕組みも整っていません。

被害と対策費用が把握できなければ、政策介入の必要性、優先順位、費用対効果を判断できません。実態調査と共通指標の整備は、特定の保護方式を採用する前に行うべき公共的な基礎作業です。

理由2 相互運用と制度運用は個社だけでは形成されにくい課題です

一事業者が自社サービス内で暗号化、アクセス制御、透かし、監視を実装することは可能です。しかし、形式間の権利情報の変換、事業者横断の識別子照合、適合性審査、失効、更新、撤退時の移行は、複数主体の合意を必要とします。

これらは、便益が業界全体に広がる一方、初期費用と運用責任が特定主体へ集中しやすい機能です。市場だけでは供給されにくいため、中立的な検討の場、公開仕様、参加条件、費用負担の設計を政策が支える意義があります。

理由3 Web 標準と国際標準は国内の個社だけでは成立しません

一般 Web 上で保護された資産を扱うには、形式、ブラウザ、OS、GPU、鍵・ライセンス、出力制御、適合性運用の責任境界を接続する必要があります。2026 年 8 月 28 日時点の公開 WebGPU 仕様、WebGL 仕様及び登録拡張には、汎用 3D アセット向けの標準的な保護セッション又は保護リソース API を確認できませんでした[15][16][17]。

この課題は W3C、Khronos Group、ISO/IEC 等にまかかります。国内で要件と実証結果を整理し、国際的な議論へ継続して参加する体制が必要です。

9-2 標準化と継続運用から得られる示唆

JPSEC 登録制度の変遷

JPEG 2000 のセキュリティ規格である JPSEC の初版には、保護ツールの識別子を管理する登録機関制度がありました[1][2]。2023 年版は旧第 7 条を削除し、旧登録機関の廃止を理由として登録機関を用いる仕組みを非推奨化しています[3]。

2025 年 2 月 9 日付の保存公開一覧には登録項目が表示されていませんが、これは全期間の登録履歴又は制度変更の原因を証明するものではありません[4]。

この経過から直接確認できるのは、初版に登録制度があり、後の版で旧第 7 条が削除され、登録方式が非推奨化されたことです。利用実績及び制度変更の原因は確定できないため、JPSEC 単独を運営主体又は制度設計の成否を示す因果的証拠には用いません。提言では一般原則として、仕様、実装、需要、費用、適合性、更新及び撤退時移行を別々に検証します。

ISO/IEC 24216-1:2026 の経験

2026 年、日本が原案開発を主導したアバターに関する国際規格 ISO/IEC 24216-1:2026 が発行されました。経済産業省の公表資料によれば、国内検討委員会での議論を経て、ISO/IEC JTC 1/SC 35 における国際規格化へ進みました[5]。

同規格は権利保護や技術的保護手段を対象としません。また、本書の対象は W3C、Khronos Group、ISO/IEC 等にまたがるため、同じ経路をそのまま適用できるものでもありません。

それでも、国内の継続的な検討体制を整え、国際標準化の場へ提案する実務的な経路が日本に存在することを示しています。

9-3 政策実施の原則と判断ゲート

五つの提言は、次の原則に従って実施します。

- 1. 保護技術への参加は任意とし、不参加を不利に扱わない
- 2. 用途別の既存基盤を優先して調査し、共通層がそれらを置き換えないようにする
- 3. 資産、用途、脅威、費用に応じて必要な機能だけを選ぶ
- 4. 相互運用性、可搬性、フォールバック、長期保存を確保する
- 5. プライバシー、アクセシビリティ、研究可能性、競争中立性を技術要件と同時に評価する
- 6. 仕様、評価結果、意思決定、異議申立ての手段を公開する
- 7. 完全防止を政策目標としない

実施段階には次の判断ゲートを設けます。

ゲート	判断事項	判断結果の扱い
1 実態	被害、対策費用、正規利用への影響が政策資源の投入に見合うか	見合わない場合は高介入の施策を拡大しない
2 既存基盤	用途別基盤又は既存規格の適用・拡張で対応できるか	対応できる範囲では新規仕様を作らない
3 実証	保護効果、性能、互換性、費用、アクセシビリティを両立できるか	要件を満たさない方式は標準化対象から外す
4 社会的影響	プライバシー、競争、研究、長期保存への影響が比例的か	公開評価と是正策なしに運用へ移さない

9-4 五つの提言

表 3 政策提言の全体像

#	提言	主な提言先	時間軸	介入の程度
1	不正取得・再利用と対策費用の実態調査	経済産業省、文化庁	短期	低
2	既存の保護基盤、技術的選択肢、限界の調査研究	文化庁、経済産業省	短期	低
3	権利・来歴メタデータの相互運用と識別子照合の整備支援	文化庁、経済産業省、知的財産戦略本部	短中期	低から中
4	一般 Web・複数形式横断の要件定義と実証支援	経済産業省、文部科学省	中期	中
5	国際標準化と継続運用への参画支援	経済産業省、	長期	中

提言 1 不正取得・再利用と対策費用の実態調査

経済産業省が公表した日本発コンテンツの海賊版被害額調査は、映像、出版、音楽、ゲーム等を対象としています[6]。静止画像素材、Live2D モデル、3D モデル、アバター、テクスチャ、モーション、単体で流通するゲームアセットについては、対象の性質に応じ、独立分類又は別建ての調査を検討すべきです。

調査項目には、少なくとも次を含めます。

- 不正取得、無断再配布、無断改変、無断再販売の類型と件数
- 権利者と事業者が負担する技術対策、監視、削除要請、法的対応の費用
- 越境事案における削除要請の結果と所要期間
- 原本、実行用データ、レビュー用派生データごとの被害
- 正規利用者に生じている性能、互換性、アクセシビリティ上の負担
- AI 学習用データセットへの取り込みについて、取得経路、許諾、アクセス制限の回避、権利者の認識

非映像デジタルアセットの被害は、視聴機会の逸失だけでなく、編集可能なデータの取得、改変、再販売として現れます。消費者アンケートだけに限定せず、制作者、出品者、マーケットプレイス、制作ツール、削除対応事業者等から証拠を収集する設計が必要です。

本提言は、個別の著作物利用が適法か違法かを一括して評価するものではありません。法的評価と、取得経路・対策費用の実態把握を分けます。

提言 2 既存の保護基盤、技術的選択肢、限界の調査研究

非映像分野に統合基盤が存在しないという前提で新規開発を始めてはなりません。電子出版の Readium LCP、積層造形の 3MF Secure Content と Materialise Identify3D、電子設計 IP の IEEE 1735 には、暗号化、ライセンス又は利用制御を組み合わせた用途別基盤があります[11][12][13][14]。

調査研究では、次を比較します。

- 用途別基盤が接続している機能、運用主体、参加条件、費用、適合性
- CENC のアイテム対応[21]、JPSEC、ISO/IEC 19566-4 等の適用範囲
- C2PA、JPEG Trust、VRM、KHR_xmp_json_ld、MPEG-21 等による識別子、権利、利用条件、来歴の表現
- データ最小化、アクセス制御、透かし、ログ、Honey Asset、サーバー側処理等が防げるものと防げないもの
- Vulkan、EGL、Direct3D 12 等のネイティブ GPU 保護部品の保証範囲と実装依存性[18]
- 正規利用への影響、実装費用、運用費用、プライバシー、アクセシビリティ

成果物は、単一の推奨技術ではなく、用途と脅威に応じた選択表、既存基盤の再利用方針、追加研究が必要な未接続部分とします。

文化庁の著作権施策に関する調査研究等、既存の公的調査枠組みとの接続を検討します[7]。対象、事業名、予算は実施時点で改めて確認します。

提言 3 権利・来歴メタデータの相互運用と識別子照合の整備支援

文化庁は 2026 年 2 月、分野横断権利情報検索システム及び個人クリエイター等権利情報登録システムの運用開始を公表しました[8]。本提言は、新たな中央データベースの創設を直ちに求めるものではありません。

まず、既存の公的基盤、民間サービス、ファイル内メタデータの関係を調査し、次を検討します。

1. 作品、権利者、登録情報を結び付ける識別子の取扱い
2. VRM の利用許諾メタデータ[9]、glTF の KHR_xmp_json_ld[10]、C2PA、JPEG Trust 等との対応関係
3. 形式間で権利・利用条件・来歴を変換又は照合する共通語彙
4. 事業者横断の識別子問い合わせ、訂正、異議申立て、監査
5. API 等の機械可読な接続が必要か、その場合の認証と公開範囲

公開資料から機能を確認できないことを、機能が存在しないことの証明として扱ってはなりません。関係機関と運用主体への確認を経て、必要な追加機能だけを決めます。

識別子照合と個体識別透かしは、利用者又は購入者に関する情報を扱い得ます。任意参加、目的限定、データ最小化、保存期間、第三者提供、開示・訂正、異議申立て、監査、追跡用途への転用禁止を要件とします。

この提言は DRM の導入を前提としません。権利者の意思を正確に伝え、流出後の照合を助ける低介入の施策として先行できます。

提言 4 一般 Web・複数形式横断の要件定義と実証支援

一般 Web・複数形式を横断する共通層について、標準策定の前に要件定義と概念実証を支援します。

実証対象には、次を含めます。

- 静止画像、Live2D モデル、汎用 3D モデル、アバター等の暗号化単位とパッケージング
- 保護セッション、鍵システム、保護リソースを扱う Web API の要件
- 暗号化データを通常メモリへ露出させず、信頼された実行・描画経路へ渡す責任分界
- 鍵・ライセンス、利用条件、端末認証、出力制御、失効、更新の接続
- データ最小化、低解像度表示、サーバー側処理等の代替手段
- 非対応環境でのフォールバック、長期保存、アクセシビリティ

ネイティブ GPU には Vulkan 等の保護部品がありますが、対応はオプション又は実装依存です[18]。Web 標準 API、鍵・ライセンス、保護された実行・描画、出力制御、適合性運用を接続した汎用経路として実証する必要があります。

評価項目には、保護効果だけでなく、性能、互換性、実装費用、運用費用、誤拒否、障害時の復旧、プライバシー、アクセシビリティを含めます。要件を満たさない方式は、標準化対象から外します。

提言 5 国際標準化と継続運用への参画支援

W3C、Khronos Group、ISO/IEC JTC 1 等における関連議論へ、日本から継続して参加・提案する体制を支援します。目的は、日本独自の仕様を先に固定することではなく、国内の実態調査と実証結果を国際的な要件形成へ反映することです。

OpenUSD の知的財産保護に関する PR #107 は、2026 年 8 月 28 日時点で Open かつ Draft であり、DRM、暗号方式、具体的アクセス制御をスコープ外としています[19]。このような既存の問題整理と責任分離の議論も把握し、重複を避けます。

支援には、次を含めます。

- クリエイター、事業者、利用者、研究者、標準化専門家、行政による国内検討体制
- 会合参加、仕様作成、翻訳、実証、適合性試験に必要な継続的資源
- 個人クリエイターと中小事業者の意見を国際議論へ反映する経路
- 複数団体にまたがる課題、責任分界、仕様依存関係の管理
- 仕様維持、適合性、失効、更新、障害対応、撤退時移行の運用計画

政府の国際標準戦略と基準認証政策には、戦略的な標準化活動を支援する枠組みがあります[20]。本提言を接続する場合は、技術の採択を成果とせず、公開要件、実証、国際合意、継続運用を評価します。

9-5 提言先別の役割

内閣・知的財産戦略本部

府省横断の方針、判断ゲート、国際標準戦略との接続を担います。特定技術の採用を先に決めるのではなく、実態調査、相互運用、参加条件、公開評価を政策文書に位置付けます。

経済産業省

コンテンツ産業の実態調査、研究開発、事業者間連携、国際標準化支援を担います。提言 1、2、3、4、5 を産業政策と標準化政策の間で調整します。

文化庁

著作権政策に関する調査研究、権利情報基盤との関係整理、技術的保護手段及び技術的利用制限手段の法的整理を担います。提言 1、2、3 を中心に、権利者と利用者の双方への影響を検討します。

文部科学省

セキュアレンダリング、電子透かし、暗号、ヒューマン・コンピュータ・インタラクション、アクセシビリティ等の基礎研究と人材育成を支援します。

総務省・デジタル庁等

情報通信政策、政府情報システム、データ連携、認証、プライバシー、国際連携に関係する範囲で協力します。行政組織名、部署名、事業名は変更され得るため、提出時点で担当を再確認します。

9-6 政策評価指標

完全防止を共通指標としてはなりません。各手段の目的に対応した指標と、正規利用への副作用を対にして評価します。

対象	効果の指標	副作用・運用の指標
権利・来歴メタデータ	付与率、検証可能性、形式間の変換成功率	誤記率、訂正時間、既存ツールとの互換性
識別子照合・透かし	照合成功率、誤検出率、対応サービス範囲	個人情報収集量、異議申立て処理時間
アクセス制御	無許可取得の遮断率、大量取得の抑制	正規利用の誤拒否率、運用費用
データ最小化	配布する原本情報の削減、 代替表示の利用率	表示品質、制作意図、 アクセシビリティへの影響
信頼された実行・描画	通常環境への読み戻し制御、攻撃コスト	性能、端末対応率、障害、長期保存
ガバナンス	適合性審査、失効、更新、復旧の処理時間	費用負担、参加主体の偏り、 意思決定の透明性

施策の継続又は拡張は、効果だけでなく、費用、誤拒否、競争、研究、プライバシー、アクセシビリティへの影響を公開して判断します。

9-7 想定される反論への応答

反論 1 CCCD の失敗を繰り返すのではないか

本書は DRM の義務化を求めません。提言 1 と 2 は調査、提言 3 はメタデータ相互運用と識別子照合、提言 4 は実証、提言 5 は国際議論への参加支援です。

任意参加、比例原則、非対応環境のフォールバック、正規利用への影響評価を導入条件とします。利便性と相互運用性を損なう方式は、判断ゲート 3 と 4 で運用対象から外します。

反論 2 保護機構は開放的な 3D エコシステムを損なうのではないか

その懸念は正当です。保護のないアセットと既存ツールを排除せず、既存形式へ付加できる選択制とする必要が

あります。

本書は開放性を制限することを前提とせず、開放性の便益、権利者の負担、正規利用への副作用を実態と実証に基づいて比較することを求めます。

反論 3 3D データの技術的保護は原理的に不可能ではないか

Vulkan、EGL、Direct3D 12 には、保護された GPU 資源を扱う部品があります。ただし、対応はオプション又は実装依存であり、それだけで一般 Web 向けのエンドツーエンド保護が成立するわけではありません[18]。

2026 年 8 月 28 日時点の公開 WebGPU 仕様、WebGL 仕様及び登録拡張には、これらを汎用 3D アセット向けに接続する標準 API を確認できませんでした[15][16][17]。したがって、原理的不可能でも、既に解決済みでもありません。部品と用途別基盤は存在するが、一般 Web・複数形式横断の接続が未整備というのが本書の整理です。

反論 4 政府が技術を選ぶべきではないのではないか

政府が特定製品又は暗号方式を選定することは、本提言の目的ではありません。政府の役割は、実態調査、中立的な比較、公開の要件形成、実証、国際参加、参加条件とガバナンスの整備です。

技術の採否は、公開された評価指標と判断ゲートに基づき、複数の実装可能性を残して判断します。

反論 5 法的救済と削除要請を優先すべきではないか

法的救済、削除要請、契約、技術的対策は代替関係ではありません。技術的対策だけで完全防止はできず、法的救済だけでは流出元の特定や大量事案への対応に限界があります。

提言 3 の識別子と来歴情報は、権利者の意思の伝達と、事後対応の証拠形成を助けます。技術と法制度を役割分担させます。

9-8 本章の結論

本章が求めるのは、非映像デジタルアセットへの DRM 義務化ではありません。

第一に、実態、対策費用、正規利用への影響を把握します。第二に、用途別の先行基盤と既存技術を調査し、再利用できるものと未接続部分を分けます。第三に、権利・来歴メタデータの相互運用と識別子照合を、低介入の施策として進めます。第四に、一般 Web・複数形式横断の共通層について要件定義と実証を行います。第五に、その結果を国際標準化の議論へ継続的に反映します。

すべての段階で、任意参加、比例原則、相互運用性、透明性、プライバシー、アクセシビリティを要件とします。被害と効果が政策費用に見合わない場合、又は副作用が比例的でない場合は、高介入の施策を拡大しません。

仕様の策定だけでなく、適合性、失効、更新、障害対応、費用負担、撤退時移行まで支える主体と手続を設計することが必要です。各段階では、仕様、実装、需要、費用、適合性、更新及び撤退時移行を別々に検証します。

出典（第9章）

[1]:ISO/IEC 15444-8:2023（第2版）, ISO. JPEG 2000 向けセキュリティ規格の現行版.

<https://www.iso.org/standard/82566.html>

[2]:Recommendation ITU-T T.807, ITU-T. 2023 年版を現行、2006 年版を旧版として示す一覧.

<https://www.itu.int/rec/T-REC-T.807>

[3]:Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認. 旧第 7 条の削除及び登録機関を用いる仕組みの変更. <https://www.itu.int/rec/T-REC-T.807-202302-I/en>

[4]:List of registered items, JPSEC RA, 2025 年 2 月 9 日保存版. 保存時点では登録項目が表示されていない。全期間の登録履歴を証明するものではない.

https://web.archive.org/web/20250209211023id_/https://www.jpsec-ra.jp/items/

[5]:「アバターに関する国際規格が発行されました」経済産業省, 2026 年 6 月 29 日.

<https://www.meti.go.jp/policy/economy/hyojun-kijun/is/20260629.html>

[6]:「日本発コンテンツの海賊版被害額調査」経済産業省, 2026 年 1 月 26 日公表.

<https://www.meti.go.jp/press/2025/01/20260126001/20260126001.html>

[7]:「令和 8 年度文化庁予算（案）の概要」文化庁.

https://www.bunka.go.jp/seisaku/bunka_gyosei/yosan/pdf/94306401_01.pdf

[8]:「『分野横断権利情報検索システム』及び『個人クリエイター等権利情報登録システム』の運用開始について」文化庁, 2026 年 2 月 26 日. https://www.bunka.go.jp/koho_hodo_oshirase/hodohappyo/94333101.html

[9]:VRM 1.0 仕様 VRMC_vrm.meta, VRM コンソーシアム.

https://github.com/vrm-c/vrm-specification/blob/master/specification/VRMC_vrm-1.0/meta.ja.md

[10]:KHR_xmp_json_ld 拡張仕様, Khronos Group.

https://github.com/KhronosGroup/glTF/blob/main/extensions/2.0/Khronos/KHR_xmp_json_ld/README.md

[11]:3MF Secure Content Extension 1.0.2, 3MF Consortium.

https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf

[12]:Radium LCP Specifications, Radium Foundation. <https://readium.org/lcp-specs/>

[13]:Materialise Identify3D, Materialise. <https://www.materialise.com/en/industrial/software/identify3d>

[14]:IEEE 1735-2023, IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE Standards Association. <https://standards.ieee.org/ieee/1735/7237/>

[15]:Encrypted Media Extensions 2, W3C Working Draft, 2026 年 7 月 7 日.

<https://www.w3.org/TR/encrypted-media-2/>

[16]:WebGPU, W3C, 2026 年 8 月 20 日版. <https://www.w3.org/TR/webgpu/>

[17]:WebGL Extension Registry, Khronos Group. <https://registry.khronos.org/webgl/extensions/>

[18]:Protected Memory, Vulkan Documentation Project, Khronos Group.

<https://docs.vulkan.org/guide/latest/protected.html>

[19]:Separation of Concerns for IP Protection in USD, OpenUSD-proposals PR #107.

<https://github.com/PixarAnimationStudios/OpenUSD-proposals/pull/107>

[20]:「新たな国際標準戦略」知的財産戦略本部, 2025 年 6 月 3 日決定.

<https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2025/pdf/kokusaisenryaku.pdf>

; 「新たな基準認証政策の展開」経済産業省, 2025 年 6 月 16 日.

<https://www.meti.go.jp/policy/economy/hyojun-kijun/jisho/pdf/20250616point.pdf>

[21]:ISO/IEC 23001-7:2023（第4版）, ISO. 公開要約は、共通暗号化がファイル、アイテム、トラック及びトラックフラグメントのメタデータを対象に含むことを示す。規格本文の個別ボックス及び適用条件は未確認。

本章の記述に関する注記

- 「確認できない」という記述は、2026 年 8 月 28 日までに公開されていた仕様、公式レジストリ、公式資料を対象とします。非公開システム、契約者限定機能、未索引資料まで含む不存在を意味しません。
- JPSEC の利用実績及び制度変更の原因は、公開資料から確定できません。本章は、運営主体又は制度設計の成否との因果関係を主張しません。
- 行政組織名、部署名、事業名、予算は変更され得るため、提出時点で再確認する必要があります。
- 本章の提言は、特定の技術方式、製品、事業者を推奨するものではありません。
- 提言 3 の公的システムに関する機能は、公開資料の記載だけで不存在を判断せず、運用主体への確認を経て検討します。

第 10 章 結論

10-1 本書が明らかにしたこと

本書は、日本のデジタルクリエイター産業における技術的保護格差を検証しました。検討の出発点にあった仮説は、調査の過程で修正されています。最終的な結論を五点に整理します。

1 非映像分野にも技術要素と用途別の統合基盤があります

静止画像には CENC のアイテム対応、JPSEC、ISO/IEC 19566-4 等があります。ネイティブ GPU 環境には Vulkan、EGL、Direct3D 12 の保護機構があります[1][2][3]。

さらに、電子出版の Readium LCP、積層造形の 3MF Secure Content と Materialise Identify3D、電子設計 IP の IEEE 1735 には、暗号化、ライセンス又は利用制御を組み合わせた用途別の保護基盤があります[4][5][6][7]。

したがって、「非映像デジタルアセットには統合的な保護基盤が存在しない」という広い命題は維持できません。保護技術も統合例も存在します。

2 空白は、一般 Web・複数形式を横断する共通保護層にあります

用途別基盤は、対象形式、業界、対応アプリケーション、ネイティブ環境又は特定の運用体系に合わせて成立しています。

一方、本書が 2026 年 8 月 28 日までに確認した公開一次資料の範囲では、一般 Web 環境において、静止画像、Live2D モデル、汎用 3D モデル、アバター、テクスチャ、モーション、ゲームアセットを横断し、共通暗号化形式、標準 API、信頼された実行・描画境界、鍵・ライセンス管理、出力制御、適合性ガバナンスを一体として提供する共通層は確認できませんでした。

EME は HTMLMediaElement と Key System を接続する音声・映像向けの標準 API です。画像、3D メッシュ、汎用アセットを対象とする能力指定は定義されていません[8]。公開 WebGPU 仕様、WebGL 仕様及び登録拡張にも、汎用 3D アセット向けの標準的な保護セッション又は保護リソース API は確認できませんでした[9][10]。

これは、暗号方式又は GPU 能力が存在しないという意味ではありません。不足しているのは、形式、Web 標準 API、信頼境界、鍵・ライセンス、保護出力、適合性運用を分野横断で接続する経路です。

3 技術的保護格差は、技術の有無ではなく接続と利用可能性の差です

映像分野では、暗号化形式、標準 API、DRM 固有の実装、端末内の保護経路、ライセンス、出力保護、認証・適合性運用が接続されています。ただし、その保証は単一規格によるものではなく、DRM、User Agent、OS、ハードウェア、契約上の堅牢性規則等の組合せに依存します。

一般 Web 上の非映像アセットでは、暗号、メタデータ、アクセス制御、透かし、GPU 保護資源等の部品があっても、それらを同じ責任分界と運用体系で利用できるとは限りません。

本書が技術的保護格差と呼ぶのは、個々の技術の保護強度の差ではなく、保護に必要な複数層がエンドツーエンドで接続され、権利者が現実利用できる状態にあるかどうかの差です。

4 格差の要因は、技術だけでは説明できません

ネイティブ GPU には保護機構があり、用途別には統合基盤も成立しています。それでも一般 Web・複数形式横断の共通層が形成されていないことから、純粋な技術的不可能性だけでは現状を説明できません。

本書は、需要側の交渉力、権利者の分散、標準化の調整費用、制度運用の担い手、費用負担、開放性との緊張、正規利用への副作用等を要因として整理しました。これらの相対的な寄与を数量的に実証したわけではなく、公開資料と比較分析に基づく説明仮説です。

映像分野では、コンテンツを供給する側が保護要件を示し、プラットフォームへ実装を促す構造がありました。非映像デジタルアセットの権利者は個人クリエイター、小規模スタジオ、中小事業者に分散しており、同じ交渉構造を形成しにくいと考えられます。

5 原本又は再利用可能な構造データが配信される領域では、別の設計が必要です

一般的な映像配信では、制作原本そのものを視聴者の端末へ渡さず、配信用に符号化されたデータを配信できます。

一方、Live2D モデル、汎用 3D モデル、アバター、モーション、テクスチャ、ゲームアセット等では、表示、操作、編集又は実行に構造データが必要です。取得されたデータは、改変、組込み、再演、再販売等に利用され得ます。

したがって、配信経路だけを保護する一律の設計では十分ではありません。原本を渡さない、価値を下げる、取得主体を限定する、実行環境を信頼する、事後に追跡する、異常を検知するという異なる対策を、用途とリスクに応じて組み合わせる必要があります。

10-2 放置した場合に残る課題

本書は、将来の被害を確定的に予測しません。市場が拡大していることと、保護上の課題が存在することは両立します。

現状のままでは、少なくとも次の課題が残ります。

第一に、政策判断の基礎となるデータが蓄積されません。非映像デジタルアセットの不正取得、再利用、対策費用、正規利用への副作用を共通の方法で把握できなければ、政策介入の必要性和費用対効果を判断できません。

第二に、対策費用が事業者と権利者ごとに重複します。用途別基盤が適用できない一般 Web・複数形式横断の場面では、各事業者が独自に対策を組み合わせる必要があります。この負担は、個人クリエイターと小規模事業者ほど重くなり得ます。

第三に、形式やサービスを越えた権利情報、識別子、失効、更新、異議申立ての相互運用が進みません。個社の対策が有効でも、サービス外へ流出した後の照合と対応には限界が残ります。

第四に、国際的な要件形成へ日本の利用実態が十分に反映されない可能性があります。アバター、Live2D モデル、同人流通等の利用実態を、国内で整理して国際的な議論へ継続的に提示する経路が必要です。

10-3 それぞれの立場で可能なこと

クリエイターと権利者

作品と利用場面に応じて、原本と実行用データの分離、プレビュー用派生データ、解像度又は機能の限定、アクセス制御、識別子、透かし、記録保存を選択します。すべての対策を適用する必要はありません。

被害、削除要請、対策費用、正規利用への影響を記録することは、実態調査と政策評価の基礎になります。

サービス事業者

提供する保護機能、守れる範囲、守れない範囲、収集する情報、保存期間、異議申立ての方法を利用者へ明示します。

権利・来歴メタデータの相互運用、識別子照合、共通指標は、DRM を導入せずに事業者間で先行検討できる領域です。

標準化団体と実装者

用途別基盤を置き換えず、共通化すべき機能と対象分野に残すべき機能を分けます。形式、Web API、信頼境界、鍵・ライセンス、出力、適合性の責任分界を明確にします。

保護のないアセット、既存ツール、長期保存、研究、アクセシビリティを排除しない任意参加の設計が必要です。

研究者

一般 Web・複数形式横断の共通層について、可能性だけでなく、性能、互換性、費用、誤拒否、プライバシー、アクセシビリティを含む実証を行います。

原理的に可能であること、標準化できること、社会的に採用すべきことを分けて評価します。

行政

第9章の五つの提言に従い、実態調査、既存基盤の比較、低介入の相互運用、要件定義と実証、国際参加を段階的に支援します。

特定技術の採用又は DRM の義務化を先に決めず、各段階で必要性、効果、費用、副作用、比例性を公開評価します。

10-4 本書が求めるもの

本書が求めるのは、コピーを完全に防ぐ技術ではありません。そのような保証は、成熟した映像分野にもありません。

求めるのは、用途別の先行基盤と既存技術を尊重しつつ、一般 Web・複数形式を横断して必要な機能を接続できる選択肢を増やすことです。

その第一歩は、被害と対策費用を把握し、既存基盤と技術的選択肢を比較し、権利・来歴メタデータの相互運用と識別子照合を進めることです。保護 Web API と信頼された実行・描画の接続は、実証と国際的な合意形成を経て、必要性和比例性が認められた範囲だけを進めます。

すべての参加は任意とし、相互運用性、透明性、プライバシー、アクセシビリティ、研究可能性、長期保存を同時に守らなければなりません。

また、仕様を定めるだけでは足りません。適合性、失効、更新、障害対応、費用負担、撤退時の移行を継続的に支える主体と手続が必要です。JPSEC 初版には、保護ツールの識別子を管理する登録機関制度がありました。2023 年版は旧第7条を削除し、旧登録機関の廃止を理由として登録機関を用いる仕組みを非推奨化しています[2][11]。2025 年 2 月 9 日付の保存公開一覧には登録項目が表示されていませんが、これは全期間の登録履歴又は制度変更の原因を証明するものではありません[13]。

この経過から JPSEC の利用実績及び制度変更の原因を確定することはできないため、JPSEC 単独を運営主体又は制度設計の成否を示す因果的証拠には用いません。提言では一般原則として、仕様、実装、需要、費用、適合性、更新及び撤退時移行を別々に検証します。

一方、日本には、国内の継続的な検討体制からアバターに関する国際規格を成立させた経験があります[12]。同じ経路をそのまま適用することはできませんが、国内の利用実態を整理し、国際的な要件形成へ反映する能力があることは示されています。

技術的保護格差を縮小するとは、すべての作品を閉じることではありません。保護を必要とする権利者が、必要な場面で、正規利用と開放性を損なわない範囲の選択肢を持てるようにすることです。

出典（第 10 章）

- [1]:ISO/IEC 23001-7:2023（第 4 版）, ISO. 公開要約は、共通暗号化がファイル、アイテム、トラック及びトラックフラグメントのメタデータを対象に含むことを示す。規格本文の個別ボックス及び適用条件は未確認。
<https://www.iso.org/standard/84637.html>
- [2]:Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認. <https://www.itu.int/rec/T-REC-T.807>
- [3]:Protected Memory, Vulkan Documentation Project, Khronos Group.
<https://docs.vulkan.org/guide/latest/protected.html>
- [4]:Radium LCP Specifications, Radium Foundation. <https://readium.org/lcp-specs/>
- [5]:3MF Secure Content Extension 1.0.2, 3MF Consortium.
https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf
- [6]:Materialise Identify3D, Materialise. <https://www.materialise.com/en/industrial/software/identify3d>
- [7]:IEEE 1735-2023, IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE Standards Association. <https://standards.ieee.org/ieee/1735/7237/>
- [8]:Encrypted Media Extensions 2, W3C Working Draft, 2026 年 7 月 7 日.
<https://www.w3.org/TR/encrypted-media-2/>
- [9]:WebGPU, W3C, 2026 年 8 月 20 日版. <https://www.w3.org/TR/webgpu/>
- [10]:WebGL Extension Registry, Khronos Group. <https://registry.khronos.org/webgl/extensions/>
- [11]:Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認. 旧第 7 条の削除及び登録機関を用いる仕組みの変更. <https://www.itu.int/rec/T-REC-T.807-202302-I/en>
- [12]:「アバターに関する国際規格が発行されました」経済産業省, 2026 年 6 月 29 日.
<https://www.meti.go.jp/policy/economy/hyojun-kijun/is/20260629.html>
- [13]:List of registered items, JPSEC RA, 2025 年 2 月 9 日保存版. 保存時点では登録項目が表示されていない。全期間の登録履歴を証明するものではない。
https://web.archive.org/web/20250209211023id_/https://www.jpsec-ra.jp/items/

本章の記述に関する注記

- 「確認できない」という記述は、2026 年 8 月 28 日までに公開されていた仕様、公式レジストリ、公式資料を対象とします。非公開システム、契約者限定機能、未索引資料まで含む不存在を意味しません。
- 要因分析は、公開資料と章間比較に基づく説明仮説であり、各要因の寄与を数量的に実証したものではありません。
- JPSEC の利用実績及び制度変更の原因は、公開資料から確定できません。本章は、運営主体又は制度設計の成否との因果関係を主張しません。
- 10-2 は現状から導かれる課題を述べたものであり、将来の被害又は市場動向を確定的に予測するものではありません。

第 11 章 用語集

本章は、本書で用いる主要な用語を整理したものです。個別の技術仕様、適用範囲、出典及び調査上の留保は、第 1 章から第 10 章までの該当箇所を参照してください。

11-1 目的の異なる技術

本書では、次の技術を目的と評価指標の異なるものとして区別します。

用語	本書における意味	主な目的	コピー防止との関係
DRM (Digital Rights Management)	鍵、ライセンス、クライアント実装、利用条件の適用等を組み合わせ、コンテンツへのアクセス又は利用を技術的に管理する仕組み	許可された条件で利用させる	暗号化だけを意味せず、完全防止を保証しない
暗号化	データを鍵なしでは解読しにくい形式へ変換する処理	伝送中又は保管中の秘匿	正規利用時の復号後データまで自動的に保護するものではない
アクセス制御	データ又は機能を利用できる主体を認証・認可によって限定する仕組み	無権限者による取得又は操作の抑制	正規権限を得た利用者による取得後の行為には別の対策が必要
電子透かし	識別情報等をコンテンツへ知覚可能又は知覚困難な形で付加する技術	流出後の識別、追跡、抑止	原則として取得そのものを防止しない
権利・来歴メタデータ	作成者、権利者、利用条件、生成・編集履歴等を機械可読に記録する情報	権利意思の伝達、真正性・来歴の確認	利用条件の記録と技術的な強制は別である
ライセンス管理	利用主体、対象、期間、権限、鍵等を発行・更新・失効させる運用	許諾条件と利用資格の管理	継続運用とクライアント側の適用機構が必要
異常検知・監査	アクセス、配信、認証、照合等の記録を分析する仕組み	大量取得や不審挙動の検知、事後検証	単独では取得を防止しない

来歴管理の成果を防止できたコピー数だけで測るなど、技術の目的と評価指標を取り違えないことが重要です。政策評価の考え方は第 9 章 9-6 に記載しています。

11-2 本書の中心概念

技術的保護格差

コンテンツの類型と利用環境によって、権利者が利用できる技術的保護、信頼された実行・描画経路、ライセンス運用、適合性制度の厚みに体系的な差がある状態をいいます。

個別の暗号技術や GPU 機能が存在するかどうかだけではなく、複数の層が接続され、権利者が費用と運用の面でも現実に利用できるかどうかを含む概念です。第 7 章 7-1 で定義しています。

一般 Web・複数形式横断

特定のネイティブアプリケーション、業界又は一種類のファイル形式だけに閉じず、一般的な Web ブラウザ環境で、静止画像、Live2D モデル、汎用 3D モデル、アバター、テキストチャ、モーション、ゲームアセット等を共通の考え方で扱う範囲を指します。

共通層

形式、標準 API、信頼された実行・描画境界、鍵・ライセンス運用、保護出力及び適合性ガバナンスを接続する横断的な仕組みを指します。本書は、用途別基盤を共通層で置き換えることを提案していません。

成立を支える七つの条件

第3章 3-6 で映像分野の比較枠組みとして整理した、共通暗号化形式、標準インターフェース、信頼境界、ハードウェア隔離、需要側主体、適合性ガバナンス及び法的裏付けを指します。歴史的な因果関係を実証した七条件ではなく、本書の比較分析に用いる枠組みです。

原本、実行用データ、プレビュー用派生データ、表示物

原本は制作・編集・販売の基礎となるデータ、実行用データは表示又は操作に必要な構造を含むデータ、プレビュー用派生データは目的に応じて情報量や機能を縮退したデータ、表示物は画面上のレンダリング結果を指します。

実行用データが常に編集可能な制作原本と同一であるとは限りません。本書の論点は、表示・操作に必要な再利用可能データがクライアント側の処理経路へ現れる場合があることです。

信頼境界

鍵、復号処理、平文データ、GPU 資源、出力等について、どの主体と実行領域を信頼し、どこからのアクセスを制限するかを定める境界です。API が存在することと、エンドツーエンドの信頼境界が成立することは同じではありません。

需要側アンカー

保護要件を集約し、実装主体へ継続的に対応を求め、費用と運用を支える需要側の主体又は構造を指す本書の分析用語です。一般 Web・複数形式横断の共通実装を求める主体を確認できないことは、形成要因に関する仮説の一つであり、単独の原因として実証したものではありません。

適合性ガバナンス

仕様への適合確認、認証、鍵・証明書・実装の失効、更新、監査、異議申立て、障害対応、費用負担及び撤退時移行を継続的に運用する仕組みを指します。

11-3 映像分野の保護技術

CENC (MPEG Common Encryption)

MPEG Common Encryption の略称です。ISO/IEC 23001-7 として標準化され、複数の DRM が同じ暗号化媒体を扱えるよう、暗号化と関連メタデータの共通形式を定めます。CENC 自体が DRM システム又はライセンス運用を定義するわけではありません。

2023 年発行の第4版について、ISO の公開要約は対象にファイル、アイテム、トラック及びトラックフラグメントのメタデータを含むことを示しています。本書は、有償の規格本文にある個別ボックス及び適用条件を検証していません。

EME (Encrypted Media Extensions)

Encrypted Media Extensions の略称です。Web アプリケーション、HTMLMediaElement 及び Key System を接続する W3C の標準 API です。EME 単体が特定の DRM、ハードウェア隔離又は復号後データの保護を一律に保証するものではありません。

CDM (Content Decryption Module)

Content Decryption Module の略称です。EME から利用される復号・鍵処理等の機能を提供する実装上の構成要

素です。具体的な信頼境界、実行環境及び保護強度は、Key System、ブラウザ、OS、ハードウェア等の実装に依存します。

Key System

EME が識別するコンテンツ保護機構の体系です。Web アプリケーションは Key System を指定し、能力情報、セッション及びライセンス交換を通じて暗号化媒体の再生へ接続します。

Clear Key

EME が共通の基準として定める Key System です。EME の相互運用確認には利用できますが、商用 DRM と同等の堅牢性、鍵の秘匿又はハードウェア保護を提供するものではありません。

TEE (Trusted Execution Environment)

Trusted Execution Environment の略称です。通常の OS 環境から隔離された実行領域で、鍵又は機密処理を扱うために利用されます。TEE の存在だけで媒体形式、Web API、出力保護及び適合性運用まで接続されるわけではありません。

Secure Media Path

復号後の媒体データを保護されたメモリ及び処理経路で扱い、一般アプリケーションからの読み出しを制限しながら出力へ渡す実装を指します。対応範囲と保証はプラットフォーム及び DRM 実装に依存します。

出力保護

外部ディスプレイ等への出力経路を保護する仕組みです。HDCP は代表例ですが、画面撮影等のアナログホールを防ぐものではありません。

Compliance and Robustness Rules

DRM 事業者等が実装者に求める適合性及び堅牢性の要件と、その検証・契約上の運用を指します。公開標準だけでは表現されない継続的な運用層の一例です。

アナログホール

画面の撮影や音声の再録音のように、正規出力後の情報を別の手段で取得できる性質を指します。成熟した映像保護でもコピーの完全防止が成立しない理由の一つです。

11-4 静止画像、権利情報及び来歴

JPSEC

Secure JPEG 2000 の通称です。ISO/IEC 15444-8 及び ITU-T T.807 として標準化され、JPEG 2000 に対する機密性、完全性、認証、条件付きアクセス等を扱います。2023 年版が現行の第 2 版です。

初版には保護ツールの識別子を扱う登録機関制度がありました。2023 年版では旧第 7 条が削除され、旧登録機関の廃止を理由として登録機関を用いる仕組みが非推奨化されています。公開資料から、全期間の登録実績又は制度変更の原因を確定することはできません。

ISO/IEC 19566-4

JPEG Systems の Privacy and security を扱う規格です。JPEG 系のボックス構造におけるプライバシー及びセキュリティ機能を扱います。規格の存在だけで、一般 Web 上の横断的な API、信頼境界又は運用制度が成立するわけではありません。

C2PA (Coalition for Content Provenance and Authenticity)

Coalition for Content Provenance and Authenticity が策定する、コンテンツの出所や編集履歴等を暗号的に検証可能な形で結び付ける仕様です。調査基準日時点の現行仕様は第 2.4 版です。C2PA は来歴と真正性の確認を主目的とし、コピー防止又は DRM そのものではありません。

Content Credentials

C2PA 仕様に基づいてコンテンツへ付与・関連付けられる来歴情報の実装・表示上の呼称です。カメラ、編集ソフト及びプラットフォームで実装例がありますが、付与された情報が常に残ること、表示主体が内容が無条件に信頼すること、又は利用を強制することを保証しません。

JPEG Trust

ISO/IEC 21617 シリーズです。真正性、来歴、帰属、知的財産権及び完全性等を含む、媒体への信頼情報の枠組みを扱います。Part 1 の現行版は ISO/IEC 21617-1:2026 です。

11-5 用途別及び形式非依存の保護基盤

OMA DRM

Open Mobile Alliance が策定した、媒体形式や実行環境から一定程度独立した DRM 体系です。ゲーム、写真、音楽等を対象例に含み、日本の携帯端末にも実装例がありました。本書が対象とする一般 Web・複数形式横断の共通層と同一ではありません。

MPEG-4 IPMP-X

ISO/IEC 14496-13:2004 として標準化された、MPEG-4 の知的財産管理保護拡張です。保護ツール間のメッセージ連携等を扱いますが、一般 Web 向けの共通信頼境界を成立させるものではありません。

MPEG-21 IPMP Components 及び REL

IPMP Components は ISO/IEC 21000-4、Rights Expression Language は ISO/IEC 21000-5 です。保護要素及び権利条件の表現を扱いますが、鍵管理、信頼管理、認証基盤又は権利条件の強制をすべて一体として定めるものではありません。

Readium LCP

電子出版向けの保護基盤です。出版物の暗号化、ライセンス文書、利用条件、署名、状態管理等を組み合わせます。電子出版という用途と対応アプリケーションの範囲で成立する先行例として扱います。

3MF Secure Content

積層造形向けの 3MF 拡張です。製造データの暗号化、利用権及び保護されたワークフローへの接続を扱います。

Materialise Identify3D

積層造形データの保護、認可、追跡等を提供する商用基盤です。用途別に技術と運用が接続された実装例として扱います。

IEEE 1735

電子設計 IP の暗号化及び管理を扱う IEEE 規格です。暗号化、利用権、ライセンス検証及び信頼モデルを対象分野内で接続する用途別基盤の例です。

11-6 Web、3D 及び GPU

glTF 及び GLB

Khronos Group が策定するランタイム向け 3D アセット形式です。glTF は JSON 等で構成され、GLB は関連データを単一のバイナリコンテナへ格納できます。開放性、拡張性及び相互運用性を重視します。現行コア仕様及び登録拡張に、一般 Web 向けの横断的な DRM 又は保護セッションを確認できないことは、将来の拡張可能性を否定するものではありません。

KHR_xmp_json_ld

glTF へ XMP に基づくメタデータを格納する Khronos 拡張です。帰属やライセンス等を表現できますが、その条件をレンダリング時に技術的に強制する仕様ではありません。

VRM

3D アバター向けのファイル形式です。VRMC_vrm.meta は、利用者、商用利用、改変等に関する権利者の意思を表現します。メタデータの表現と、その条件の技術的強制は別です。

OpenUSD

3D シーン記述のための技術体系です。知的財産保護に関する公開提案もありますが、調査基準日時点の当該提案は Open かつ Draft であり、DRM、暗号方式及び具体的なアクセス制御をスコープ外としています。

WebGL 及び WebGPU

Web ブラウザから GPU 機能を利用するための API です。本書が調査基準日までに確認した公開仕様及び登録拡張の範囲では、一般 Web・複数形式横断の保護セッション又は保護リソース API を確認できませんでした。これは非公開実装又は将来仕様を含む絶対的な不存在を意味しません。

Vulkan Protected Memory

保護属性を持つメモリ、バッファ、画像及びキューを扱う Vulkan の機構です。ネイティブ GPU 環境に保護部品が存在することを示しますが、対応はオプション又は実装依存であり、Web API、鍵・ライセンス及び適合性制度まで自動的に接続するものではありません。

Protected Resource Session 及び Protected Content

Direct3D 12 の Protected Resource Session と EGL_EXT_protected_content は、ネイティブ環境で保護された GPU 資源又は出力を扱う機構です。一般 Web 上で複数形式を横断する共通 API とは区別します。

11-7 Live2D 及び Web プレビュー

Cubism SDK

Live2D モデルをアプリケーション又は Web 環境で表示・操作するための SDK です。モデル、テクスチャ、モーション、物理演算等の実行用データを読み込んで描画します。

moc3、model3.json、motion3.json 及び physics3.json

moc3 はモデル本体、model3.json は関連ファイルを結び付ける設定、motion3.json はモーション、physics3.json は物理演算に関するデータです。ファイルごとの役割を区別し、制作原本、実行用データ及びプレビュー用データを一括して同一視しません。

MOC3 Consistency Checker

moc3 ファイルの整合性を確認し、不正な変更が疑われる状態の検出を助ける機能です。コピー防止又は DRM そのものではありません。

Web プレビュー

購入又は利用の判断に必要な外観・動作をブラウザ上で確認できる機能です。表示と操作に必要なデータをクライアント側で処理する必要と、再利用可能な構造データの価値を下げたい必要が衝突する場合があります。本書は、この関係を構造的ジレンマとして扱います。

11-8 個別の対策技術

データ最小化

利用目的に不要な原本情報を配布せず、プレビュー専用派生データ、低解像度データ又は機能を限定したデータを用いる考え方です。

Signed URL 及び短寿命トークン

期限、対象又は署名を含む URL 等により取得主体と期間を限定するアクセス制御です。URL の共有や正規取得後のデータ利用まで防ぐコンテンツ保護方式ではありません。

Rate Limit

主体、時間、IP アドレス、認証情報等に応じてリクエスト回数を制限する仕組みです。大量取得のコストを上げますが、低速な取得又は正規利用者による保存を完全には防ぎません。

WebCrypto

Web アプリケーションから暗号機能を利用する標準 API です。非抽出鍵を扱える場合がありますが、通常の JavaScript 処理へ復号結果を渡す設計では、復号後データの利用境界を単独では形成しません。

Device Binding

ライセンス又は利用資格を特定端末へ結び付ける仕組みです。端末識別、移行、故障、プライバシー及びアクセシビリティへの配慮が必要です。

Key Rotation 及び Revocation

鍵を定期的に更新すること、又は漏えいした鍵、証明書、端末若しくは実装を失効させることです。継続的な運用主体、復旧手続及び正規利用者への影響管理を必要とします。

Honey Asset

識別用又は囷となるアセットを配置し、外部での出現から不正取得経路を推定する手法です。取得の防止よりも検知と調査を目的とします。

Audit Log

アクセス、認証、配信、照合等の記録です。異常検知、事後の立証及び対策評価の基礎になりますが、記録対象、保存期間、アクセス権及びプライバシーを設計する必要があります。

サーバー側レンダリング及びピクセルストリーミング

レンダリングをサーバー側で行い、クライアントへ主として映像結果を送る方式です。構造データを直接配布しない利点がある一方、費用、遅延、同時接続、画質、アクセシビリティ及び事業継続性の制約があります。

Anti-Tamper

実行ファイルの改変、デバッグ、コード注入等を検知・妨害する技術です。実行ファイルの保護と、レンダリング中のアセットデータの秘密性は別の問題です。

11-9 政策及び標準化

技術的保護手段及び技術的利用制限手段

日本の著作権法上の概念です。本書で一般的に用いる技術的対策、DRM 又はアクセス制御と法的な定義が常に一致するわけではありません。具体的な法的評価は、対象行為と要件に即して別途行う必要があります。

任意参加

権利者、利用者、実装者又はサービスが保護機構への参加を選択でき、不参加を不当に不利に扱わない原則です。

比例原則

保護の必要性和効果に対して、費用、正規利用への制約、プライバシー、競争、研究、アクセシビリティ等への影響が過大でないことを求める考え方です。

相互運用性

複数の形式、実装、サービス又は主体の間で、データ、権利情報、識別子又は保護機能を一貫して扱える性質です。単一事業者への固定を意味しません。

PoC

Proof of Concept の略称です。標準化又は本格運用の前に、技術的可能性、性能、互換性、費用及び副作用を検証する概念実証を指します。

適合性評価

実装が公開仕様及び運用要件を満たすかを試験・確認する手続です。認証、監査、更新及び失効と組み合わせて継続運用される場合があります。

Working Draft、Candidate Recommendation 及び国際規格

Working Draft は検討中の草案、Candidate Recommendation は実装経験等を集める段階、国際規格は所定の標準化手続を経て発行された規格です。名称が似ていても確定度が異なるため、本書は調査基準日時点の状態を区別して記載します。

判断ゲート

第9章で提案する、施策を次段階へ進める前の判断点です。実態、既存基盤、実証及び社会的影響を評価し、要件を満たさない高介入の施策を拡大しないために設けます。

継続運用

仕様の策定後も、実装更新、適合性、鍵・証明書の失効、障害対応、異議申立て、費用負担、組織の撤退及び移行を支える活動を指します。

第 12 章 参考文献一覧

本章は、第 1 章から第 10 章までの章末出典を URL 単位で重複統合した索引です。調査基準日は 2026 年 8 月 28 日です。

各章の出典番号は章内で完結しているため、本章の整理番号とは対応しません。引用、検証又は再利用の際は、「本編参照」に示した章の章末出典を確認してください。複数の URL を一つの章内出典で示した資料は、本章では URL ごとに分けています。

規格の状態、製品仕様、行政資料及び URL は変更される場合があります。提出又は公開の時点で再確認してください。

12-1 政府・行政機関

R-001

「日本発コンテンツの海賊版被害額調査の結果を取りまとめました」経済産業省（委託：一般社団法人コンテンツ海外流通促進機構、再委託：PwC コンサルティング合同会社）、2026 年 1 月 26 日公表（2026 年 5 月 22 日更新）。
URL：<https://www.meti.go.jp/press/2025/01/20260126001/20260126001.html>

本編参照：第 1 章、第 2 章、第 9 章

R-002

「知的財産推進計画 2026」知的財産戦略本部、2026 年 6 月 12 日決定。

URL：https://www.cas.go.jp/jp/seisakukaigi/titeki2/260612/keikaku_all.pdf

本編参照：第 1 章、第 2 章

R-003

「アバターに関する国際規格が発行されました」経済産業省、2026 年 6 月 29 日。対象規格は ISO/IEC 24216-1:2026（ISO/IEC JTC 1/SC 35、2026 年 5 月発行）。

URL：<https://www.meti.go.jp/policy/economy/hyojun-kijun/is/20260629.html>

本編参照：第 1 章、第 2 章、第 9 章、第 10 章

R-004

「『分野横断権利情報検索システム』及び『個人クリエイター等権利情報登録システム』の運用開始について」文化庁、2026 年 2 月 26 日。

URL：https://www.bunka.go.jp/koho_hodo_oshirase/hodohappyo/94333101.html

本編参照：第 1 章、第 8 章、第 9 章

R-005

文化審議会著作権分科会 私的録音録画小委員会「中間整理」文化庁、2007 年 10 月 12 日。第 49 頁および脚注 32。

URL：https://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/pdf/h1910_rokuon_chukan.pdf

本編参照：第 1 章、第 8 章

R-006

「令和 8 年度文化庁予算（案）の概要」文化庁。

URL：https://www.bunka.go.jp/seisaku/bunka_gyosei/yosan/pdf/94306401_01.pdf

本編参照：第 9 章

R-007

新たな国際標準戦略, 知的財産戦略本部, 2025 年 6 月 3 日決定.

URL : <https://www.kantei.go.jp/jp/singi/titeki2/chitekizaisan2025/pdf/kokusaisenryaku.pdf>

本編参照：第 9 章

R-008

新たな基準認証政策の展開, 経済産業省, 2025 年 6 月 16 日.

URL : <https://www.meti.go.jp/policy/economy/hyojun-kijun/jisho/pdf/20250616point.pdf>

本編参照：第 9 章

R-009

北京インターネット法院公表事例（一番：（2024）京 0491 民初 4936 号、二審：（2025）京 73 民終 603 号）の専用ページ.

URL : https://english.bjinternetcourt.gov.cn/2025-10/29/c_819.htm

本編参照：第 2 章

12-2 国際規格・標準仕様・業界仕様

R-010

ISO/IEC 23001-7:2023（第 4 版）, 2023 年 8 月 8 日発行. 序文（画像アイテムを対象に含める旨）。規範的条項の本文は無償公開の対象外のため未確認.

URL : <https://www.iso.org/standard/84637.html>

本編参照：第 1 章、第 3 章、第 4 章、第 7 章、第 8 章、第 9 章、第 10 章

R-011

Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認.

URL : <https://www.itu.int/rec/T-REC-T.807>

本編参照：第 1 章、第 4 章、第 7 章、第 8 章、第 9 章、第 10 章

R-012

Protected Memory, Vulkan Documentation Project, Khronos Group.

URL : <https://docs.vulkan.org/guide/latest/protected.html>

本編参照：第 1 章、第 4 章、第 6 章、第 8 章、第 9 章、第 10 章

R-013

Encrypted Media Extensions 2, W3C Working Draft, 2026 年 7 月 7 日.

URL : <https://www.w3.org/TR/encrypted-media-2/>

本編参照：第 1 章、第 3 章、第 4 章、第 8 章、第 9 章、第 10 章

R-014

3MF Secure Content Extension 1.0.2, 3MF Consortium.

URL : https://3mf.io/wp-content/uploads/sites/55/2025/02/3MF_Secure_Content_v1_0_2.pdf

本編参照：第 1 章、第 2 章、第 4 章、第 6 章、第 7 章、第 8 章、第 9 章、第 10 章

R-015

Radium Licensed Content Protection 1.0.

URL : <https://readium.org/lcp-specs/releases/lcp/latest>

本編参照：第 1 章、第 2 章

R-016

IEEE Recommended Practice for Encryption and Management of Electronic Design Intellectual Property (IP), IEEE 1735-2023.

URL : <https://standards.ieee.org/ieee/1735/7237/>

本編参照：第 1 章、第 2 章、第 4 章、第 6 章、第 7 章、第 8 章、第 9 章、第 10 章

R-017

WebGL Extension Registry, Khronos Group.

URL : <https://registry.khronos.org/webgl/extensions/>

本編参照：第 1 章、第 4 章、第 6 章、第 7 章、第 8 章、第 9 章、第 10 章

R-018

glTF Extensions, Khronos Group.

URL : <https://github.com/KhronosGroup/glTF/tree/main/extensions>

本編参照：第 1 章

R-019

Past Community Groups, W3C.

URL : <https://www.w3.org/community/groups/past/>

本編参照：第 1 章、第 4 章

R-020

Separation of Concerns for IP Protection in USD, OpenUSD-proposals PR #107, 2026 年 5 月 14 日.

URL : <https://github.com/PixarAnimationStudios/OpenUSD-proposals/pull/107>

本編参照：第 1 章、第 4 章、第 7 章、第 8 章、第 9 章

R-021

MovieLabs Specification for Enhanced Content Protection, Version 1.4, MovieLabs.

URL : https://movielabs.com/ngvideo/MovieLabs_ECP_Spec_v1.4.pdf

本編参照：第 1 章、第 3 章

R-022

DASH-IF Interoperability Guidelines Part 6: Content Protection and Security, v5.0.0, DASH Industry Forum.

URL : <https://dashif.org/docs/IOP-Guidelines/DASH-IF-IOP-Part6-v5.0.0.pdf>

本編参照：第 3 章

R-023

CTA-5001-E, Web Application Video Ecosystem — Content Specification, Consumer Technology Association.

URL : <https://cdn.cta.tech/cta/media/media/resources/standards/pdfs/cta-5001-e-final.pdf>

本編参照：第 3 章

R-024

RFC 8216, HTTP Live Streaming, IETF, 2017 年 8 月.

URL : <https://www.rfc-editor.org/rfc/rfc8216.html>

本編参照：第 3 章

R-025

Encrypted Media Extensions, W3C Recommendation, 2017 年 9 月 18 日.

URL : <https://www.w3.org/TR/2017/REC-encrypted-media-20170918/>

本編参照：第 3 章

R-026

W3C Publishes Encrypted Media Extensions (EME) as a W3C Recommendation, W3C, 2017 年 9 月 18 日.

URL : <https://www.w3.org/press-releases/2017/eme-recommendation/>

本編参照：第 3 章

R-027

Notice to the W3C of EFF's appeal of the Director's decision on EME, Electronic Frontier Foundation, 2017 年 7 月 12 日.

URL : <https://lists.w3.org/Archives/Public/public-html-media/2017Jul/0005.html>

本編参照：第 3 章、第 8 章

R-028

MPTF Requirements for Content Protection, W3C Web and TV Interest Group, Media Pipeline Task Force, W3C Editor's Draft, 2012 年 8 月 16 日.

URL : <https://www.w3.org/2011/webtv/MPTF/cpreq.html>

本編参照：第 3 章

R-029

Encrypted Media Extensions, W3C First Public Working Draft, 2013 年 5 月 10 日.

URL : <https://www.w3.org/TR/2013/WD-encrypted-media-20130510>

本編参照：第 3 章

R-030

ISO/IEC 23001-7:2016, Information technology — MPEG systems technologies — Part 7: Common encryption in ISO base media file format files (第 3 版) .

URL : <https://www.iso.org/standard/68042.html>

本編参照：第 4 章

R-031

ISO/IEC 15444-8:2007, Information technology — JPEG 2000 image coding system: Secure JPEG 2000, 2007 年 4 月発行.

URL : <https://www.iso.org/standard/37382.html>

本編参照：第 4 章

R-032

ISO/IEC 15444-8:2023 (第 2 版) .

URL : <https://www.iso.org/standard/82566.html>

本編参照：第 4 章、第 9 章

R-033

Call for contributions to JPEG Privacy, JPEG Committee, 2013 年 1 月 21 日.

URL : https://jpeg.org/items/20130121_4.html

本編参照 : 第 4 章、第 6 章

R-034

ISO/IEC 19566-4:2020, Information technologies — JPEG systems — Part 4: Privacy and security, 2020 年 3 月発行.

URL : <https://www.iso.org/standard/73607.html>

本編参照 : 第 4 章、第 8 章

R-035

Draft Call for Proposals on JPEG Privacy & Security, ISO/IEC JTC 1/SC 29/WG 1 (JPEG), 文書番号 WG1N74015, 2017 年 1 月.

URL : https://jpeg.org/downloads/privacy_and_security/wg1n74015_Draft_CfP.pdf

本編参照 : 第 4 章

R-036

OMA DRM Architecture V2.1, Open Mobile Alliance, 文書番号 OMA-AD-DRM-V2_1-20070724-C, 2007 年 7 月 24 日.

URL : https://www.openmobilealliance.org/release/drm/V2_1-20070724-C/OMA-AD-DRM-V2_1-20070724-C.pdf

本編参照 : 第 4 章

R-037

ISO/IEC 14496-13:2004, Information technology — Coding of audio-visual objects — Part 13: Intellectual Property Management and Protection (IPMP) extensions, 2004 年 9 月発行.

URL : <https://www.iso.org/standard/39110.html>

本編参照 : 第 4 章

R-038

MPEG-4 Intellectual Property Management and Protection Extension (IPMP-X), MPEG 文書 N7505, 2005 年 7 月.

URL : <https://mpeg.chiariglione.org/standards/mpeg-4/ipmp-extensions.html>

本編参照 : 第 4 章、第 7 章

R-039

ISO/IEC 21000-4:2006, MPEG-21 IPMP Components.

URL : <https://www.iso.org/standard/41836.html>

本編参照 : 第 4 章、第 7 章

R-040

ISO/IEC 21000-5:2004, MPEG-21 Rights Expression Language.

URL : <https://www.iso.org/standard/36095.html>

本編参照 : 第 4 章、第 7 章、第 8 章

R-041

VK_EXT_pipeline_protected_access, Vulkan Documentation Project, Khronos Group.

URL : https://docs.vulkan.org/features/latest/features/proposals/VK_EXT_pipeline_protected_access.html

本編参照 : 第 4 章、第 6 章

R-042

WebGPU, W3C Candidate Recommendation Draft, 2026 年 8 月 20 日.

URL : <https://www.w3.org/TR/webgpu/>

本編参照：第 4 章、第 6 章、第 7 章、第 8 章、第 9 章、第 10 章

R-043

WebGL 2.0 Specification, Khronos Group.

URL : <https://registry.khronos.org/webgl/specs/latest/2.0/>

本編参照：第 4 章、第 6 章、第 7 章

R-044

EGL_EXT_protected_content, Khronos Group, Version 13, 2021 年 12 月 6 日.

URL : https://registry.khronos.org/EGL/extensions/EXT/EGL_EXT_protected_content.txt

本編参照：第 4 章、第 8 章

R-045

RFC 9246, URI Signing for Content Delivery Network Interconnection (CDNI), IETF, 2022 年.

URL : <https://www.rfc-editor.org/rfc/rfc9246.html>

本編参照：第 4 章、第 6 章

R-046

ISO/IEC 21617-2, JPEG Trust — Part 2.

URL : <https://www.iso.org/standard/89038.html>

本編参照：第 4 章

R-047

ISO/IEC 21617-3, JPEG Trust — Part 3.

URL : <https://www.iso.org/standard/90209.html>

本編参照：第 4 章

R-048

JPEG Trust Workplan, JPEG Committee.

URL : <https://jpeg.org/jpegtrust/workplan.html>

本編参照：第 4 章

R-049

Are Content Credentials a form of DRM?, C2PA FAQ. (仕様本文ではなく FAQ における記述です)

URL : <https://c2pa.org/faqs/>

本編参照：第 4 章

R-050

ISO/IEC 12113:2022, Information technology — Runtime 3D asset delivery format — Khronos glTF™ 2.0, 2022 年 7 月 26 日発行.

URL : <https://www.iso.org/standard/83990.html>

本編参照：第 4 章

R-051

KHR_xmp_json_ld 拡張仕様, Khronos Group.

URL

:

https://github.com/KhronosGroup/glTF/blob/main/extensions/2.0/Khronos/KHR_xmp_json_ld/README.md

本編参照：第 4 章、第 8 章、第 9 章

R-052

VRM 1.0 仕様 VRMC_vrm.meta, VRM コンソーシアム.

URL : https://github.com/vrm-c/vrm-specification/blob/master/specification/VRMC_vrm-1.0/meta.ja.md

本編参照：第 4 章、第 7 章、第 8 章、第 9 章

R-053

ISO/IEC 23090-14:2025 (第 2 版) , Information technology — Coded representation of immersive media — Part 14: Scene description, 2025 年 11 月発行.

URL : <https://www.iso.org/standard/90191.html>

本編参照：第 4 章

R-054

MPEG Extends and Integrates glTF 2.0 into MPEG-I Scene Description ISO/IEC 23090, Khronos Group, 2024 年 7 月 26 日.

URL : <https://www.khronos.org/blog/mpeg-extends-and-integrates-glTF-2.0-into-mpeg-i-scene-description-iso-iec-23090>

本編参照：第 4 章

R-055

glTF 2.1 64-bit upgrade to binary format, KhronosGroup/glTF Issue #2594.

URL : <https://github.com/KhronosGroup/glTF/issues/2594>

本編参照：第 4 章、第 8 章

R-056

glTF 2.0 Specification, The Khronos Group. 第 5 章 (スキニングおよびアニメーション) .

URL : <https://registry.khronos.org/glTF/specs/2.0/glTF-2.0.html>

本編参照：第 4 章

R-057

WebGPU Explainer, GPU for the Web Community Group.

URL : <https://gpuweb.github.io/gpuweb/explainer/>

本編参照：第 4 章、第 6 章

R-058

Minutes 2018-01-10, GPU for the Web Community Group.

URL : <https://github.com/gpuweb/gpuweb/wiki/Minutes-2018-01-10>

本編参照：第 4 章

R-059

Asset protection for glTF, Khronos Community Forums, 2020 年 7 月 24 日.

URL : <https://community.khronos.org/t/asset-protection-for-glTF/106080>

本編参照：第 4 章

R-060

Digital Asset Management Domain Group, Metaverse Standards Forum.

URL : <https://portal.metaverse-standards.org/>

本編参照：第 4 章

R-061

Readium LCP Specifications, Readium Foundation.

URL : <https://readium.org/lcp-specs/>

本編参照：第 4 章、第 6 章、第 7 章、第 8 章、第 9 章、第 10 章

R-062

Recommendation ITU-T T.807 (V2), Information technology — JPEG 2000 image coding system: Secure JPEG 2000, ITU-T, 2023 年 2 月 13 日承認.

URL : <https://www.itu.int/epublications/publication/itu-t-t-807-v2-2023-02-information-technology-jpeg-2000-image-coding-system-secure-jpeg-2000>

本編参照：第 6 章

R-063

Recommendation ITU-T T.807 (V2), ITU-T, 2023 年 2 月 13 日承認. 2023 年版の本文及び旧登録機関制度の変更.

URL : <https://www.itu.int/rec/T-REC-T.807-202302-I/en>

本編参照：第 7 章、第 8 章、第 9 章、第 10 章

R-064

Introducing glTF 2.1 with Complex Scenes, Khronos Group, 2026 年.

URL : <https://www.khronos.org/blog/introducing-gltf-2.1-with-complex-scenes>

本編参照：第 8 章

R-065

VK_EXT_pipeline_protected_access, Vulkan Documentation Project, Khronos Group.

URL : https://registry.khronos.org/vulkan/specs/latest/man/html/VK_EXT_pipeline_protected_access.html

本編参照：第 8 章

R-066

Content Credentials: C2PA Technical Specification, Version 2.4, Coalition for Content Provenance and Authenticity.

URL : https://spec.c2pa.org/specifications/specifications/2.4/specs/C2PA_Specification.html

本編参照：第 4 章

R-067

ISO/IEC 21617-1:2026, Information technology — JPEG Trust — Part 1: Core foundation.

URL : <https://www.iso.org/standard/91405.html>

本編参照：第 4 章

12-3 企業・サービス・実装資料

R-068

「BOOTH 3D モデルカテゴリ 取引白書 2026」ピクシブ株式会社, 2026 年 2 月 6 日.

URL : <https://www.pixiv.co.jp/2026/02/06/110000>

本編参照：第 1 章、第 2 章、第 4 章、第 5 章

R-069

Statement of IRI, JPSEC RA（特定非営利活動法人 Intellectual Resource Initiative）.

URL : <https://www.jpsec-ra.jp/statement-of-iri/>

本編参照：第 1 章、第 4 章

R-070

Materialise Identify3D, Materialise.

URL : <https://www.materialise.com/en/industrial/software/identify3d>

本編参照：第 1 章、第 2 章、第 4 章、第 6 章、第 7 章、第 8 章、第 9 章、第 10 章

R-071

「VTuber 市場に関する調査」株式会社矢野経済研究所, 2025 年 4 月 28 日（プレスリリース No.3806）.

URL : https://www.yano.co.jp/press-release/show/press_id/3806

本編参照：第 2 章

R-072

「Live2D 作品の投稿」nizima（Live2D Inc.）.

URL : <https://docs.nizima.com/guide/item-upload/live2d/>

本編参照：第 2 章、第 4 章、第 5 章

R-073

「モデルについて（Web）」Live2D Inc., Cubism SDK Manual.

URL : <https://docs.live2d.com/4.2/en/cubism-sdk-manual/model-web/>

本編参照：第 2 章、第 4 章、第 5 章

R-074

「クリエイター向けオーダーメイドガイド」nizima（Live2D Inc.）.

URL : <https://docs.nizima.com/guide/creator-ordering/>

本編参照：第 2 章

R-075

「DRM 機能（デジタル作品保護機能）はありますか？」BOOTH（ピクシブ株式会社）.

URL : <https://booth.pixiv.help/hc/ja/articles/231284508>

本編参照：第 2 章、第 4 章、第 5 章

R-076

VRChat Security Update, VRChat Inc., 2022 年 7 月.

URL : <https://hello.vrchat.com/blog/vrchat-security-update>

本編参照：第 2 章、第 4 章、第 5 章

R-077

Using content protection systems with HLS, Apple Inc.

URL : <https://developer.apple.com/documentation/http-live-streaming/using-content-protection-systems-with-hls>

本編参照：第 3 章

R-078

PlayReady Content Encryption, Microsoft.

URL : <https://learn.microsoft.com/en-us/playready/packaging/content-encryption>

本編参照：第 3 章

R-079

セキュリティ レベル (PlayReady) , Microsoft.

URL : <https://learn.microsoft.com/ja-jp/playready/overview/security-level>

本編参照：第 3 章

R-080

MediaDrm, Android Developers API Reference, Google.

URL : <https://developer.android.com/reference/android/media/MediaDrm>

本編参照：第 3 章

R-081

PlaybackMetrics, Android Developers API Reference, Google.

URL : <https://developer.android.com/reference/android/media/metrics/PlaybackMetrics>

本編参照：第 3 章

R-082

Integrating PlayReady in Devices, Microsoft (最終更新 2018 年 2 月 1 日) .

URL : <https://learn.microsoft.com/en-us/playready/overview/integrating-in-devices>

本編参照：第 3 章、第 4 章、第 7 章

R-083

Reconciling Mozilla's Mission and W3C EME, Mozilla, 2014 年 5 月 14 日.

URL : <https://hacks.mozilla.org/2014/05/reconciling-mozillas-mission-and-w3c-eme/>

本編参照：第 3 章

R-084

Moving to HTML5 Video, Google, 2016 年.

URL : <https://developers.google.com/media/pdf/2016-HTML5-Video-Whitepaper.pdf>

本編参照：第 3 章

R-085

Widevine Mobile License Agreement, Exhibit A, Google.

URL : <https://developers.google.com/widevine/contact/widevine-mobile-license-use>

本編参照：第 3 章、第 7 章

R-086

Vodafone 804N 取扱説明書 (英語版) , ソフトバンク公式アーカイブ.

URL : <https://www.softbank.jp/en/mobile/set/data/support/users-guide/shared/sb804n/804n-e-manual.pdf>

本編参照：第 4 章

R-087

What is JPSEC RA?, JPSEC RA (特定非営利活動法人 Intellectual Resource Initiative) .

URL : <https://www.jpsec-ra.jp/whatisra/>

本編参照：第 4 章

R-088

Duties of JPSEC RA, JPSEC RA.

URL : <https://www.jpsec-ra.jp/duties/>

本編参照：第 4 章

R-089

Contact information, JPSEC RA.

URL : <https://www.jpsec-ra.jp/contactinfomation/>

本編参照：第 4 章

R-090

「組み込み用データ」Live2D Inc., 最終更新 2025 年 8 月 26 日.

URL : <https://docs.live2d.com/cubism-editor-manual/export-moc3-motion3-files/>

本編参照：第 4 章

R-091

「モーションについて」Live2D Inc., 最終更新 2026 年 1 月 29 日.

URL : <https://docs.live2d.com/en/cubism-sdk-manual/motion/>

本編参照：第 4 章

R-092

nizima に投稿できる作品の種類, nizima (Live2D Inc.) .

URL : <https://docs.nizima.com/en/guide/item-upload/>

本編参照：第 4 章、第 5 章、第 6 章

R-093

「Live2D プレビュー操作ガイド」nizima (Live2D Inc.) .

URL : <https://docs.nizima.com/guide/preview-guide/>

本編参照：第 4 章

R-094

ダイレクトメッセージの使い方, nizima (Live2D Inc.) .

URL : <https://docs.nizima.com/en/guide/direct-message/>

本編参照：第 4 章、第 5 章、第 6 章

R-095

「MOC3 Consistency Checker」Live2D Inc., 最終更新 2025 年 8 月 26 日.

URL : <https://docs.live2d.com/en/cubism-editor-manual/moc3-consistency-checker/>

本編参照：第 4 章

R-096

「AssetBundle Download Integrity and Security」Unity Technologies.

URL : <https://docs.unity3d.com/2023.1/Documentation/Manual/AssetBundles-Integrity.html>

本編参照：第 4 章

R-097

「Protecting Content」 Unity Technologies, Unity 5.4 マニュアル（アーカイブ）.

URL : <https://docs.unity3d.com/540/Documentation/Manual/protectingcontent.html>

本編参照：第 4 章、第 6 章

R-098

「Interface IDataConverter」 Unity Technologies, Addressables.CN 1.18.11 API.

URL

<https://docs.unity3d.com/Packages/com.unity.addressables.cn@1.18/api/UnityEngine.ResourceManagement.ResourceProviders.IDataConverter.html>

本編参照：第 4 章

R-099

「Project Section of the Unreal Engine Project Settings」 Epic Games.

URL : <https://dev.epicgames.com/documentation/unreal-engine/project-section-of-the-unreal-engine-project-settings>

本編参照：第 4 章

R-100

「Packaging Projects」 Epic Games, Unreal Engine 4.27.

URL : https://dev.epicgames.com/documentation/unreal-engine/packaging-projects?application_version=4.27

本編参照：第 4 章、第 6 章

R-101

「FPakInfo」 および「RegisterEncryptionKey」 Epic Games, Unreal Engine API Reference.

URL : <https://dev.epicgames.com/documentation/unreal-engine/API/Runtime/PakFile/FPakInfo>

本編参照：第 4 章

R-102

Anti-Tamper game security, Denuvo by Irdeto.

URL : <https://irdeto.com/denuvo/anti-tamper/>

本編参照：第 4 章、第 6 章

R-103

「映像データの保存形式」『タイムベースト・メディアを用いた美術作品の修復／保存のガイド』京都市立芸術大学芸術資源研究センター（文化庁事業）, 2017 年 2 月 16 日.

URL : <https://www.kcua.ac.jp/arc/time-based-media/?p=787>

本編参照：第 4 章

R-104

Stock Footage, Getty Images. (2026 年 8 月確認)

URL : <https://www.gettyimages.com/creative-video/stock-videos>

本編参照：第 4 章

R-105

HLS requirements, Akamai Technologies. (2026 年 8 月確認)

URL : <https://techdocs.akamai.com/msl/docs/hls-requirements>

本編参照：第 4 章

R-106

ID3D12Device4::CreateProtectedResourceSession, Microsoft Learn.

URL : <https://learn.microsoft.com/en-us/windows/win32/api/d3d12/nf-d3d12-id3d12device4-createprotectedresourcesession>

本編参照：第 4 章、第 8 章

R-107

Azure products retirement in September 2025, Microsoft. Azure Remote Rendering の 2025 年 9 月 30 日廃止を確認する公式一覧.

URL : <https://learn.microsoft.com/en-us/lifecycle/announcements/azure-products-retirement-september-2025>

本編参照：第 6 章

R-108

BOOTH 3D モデルカテゴリ取引白書 2025, ピクシブ株式会社, 2025 年 2 月 19 日. 2023 年の取扱高に関する公式資料.

URL : <https://inside.pixiv.blog/2025/02/19/114500>

本編参照：第 1 章、第 2 章

R-109

Content Credentials, Leica Camera. C2PA に準拠したカメラ実装の公式資料.

URL : <https://leica-camera.com/en-US/photography/content-credentials>

本編参照：第 4 章

R-110

Content Credentials in Adobe Photoshop, Adobe. 編集ソフトにおける付与機能の公式資料.

URL : <https://helpx.adobe.com/photoshop/desktop/save-and-export/metadata-content-credentials/use-content-credentials.html>

本編参照：第 4 章

R-111

Edit images in Google Photos by simply asking, Google, 2025 年 8 月 20 日. Google Photos における C2PA Content Credentials 対応の公式資料.

URL : <https://blog.google/products-and-platforms/products/photos/ai-photo-editing-google-photos/>

本編参照：第 4 章

12-4 学術論文・研究資料

R-112

St  phanie Delaune, Joseph Lallemand, Gwendal Patat, Florian Roudot, Mohamed Sabt, Formal Security Analysis of Widevine through the W3C EME Standard, USENIX Security Symposium, 2024 年.

URL : <https://www.usenix.org/conference/usenixsecurity24/presentation/delaune>

本編参照：第 3 章

R-113

Your DRM Can Watch You Too: Exploring the Privacy Implications of Browsers (mis)Implementations of Widevine EME, Proceedings on Privacy Enhancing Technologies, 2023 年, Volume 2023, Issue 4, pp.306-321. DOI: 10.56553/popets-2023-0112

URL : <https://doi.org/10.56553/popets-2023-0112>

本編参照：第 3 章

R-114

Xuandong Zhao et al., "Invisible Image Watermarks Are Provably Removable Using Generative AI," NeurIPS 2024.

URL : https://proceedings.neurips.cc/paper_files/paper/2024/hash/10272bfd0371ef960ec557ed6c866058-Abstract-Conference.html

本編参照：第 4 章、第 6 章

R-115

Yuxin Wen et al., "Tree-Ring Watermarks: Fingerprints for Diffusion Images that are Invisible and Robust," NeurIPS 2023.

URL : <https://arxiv.org/abs/2305.20030>

本編参照：第 4 章、第 6 章

R-116

Kai Wang et al., "A Comprehensive Survey on Three-Dimensional Mesh Watermarking," IEEE Transactions on Multimedia, 第 10 巻第 8 号, 2008 年 12 月.

URL : <https://ieeexplore.ieee.org/document/4694850/>

本編参照：第 4 章、第 6 章

R-117

Xingyu Zhu et al., "Rethinking Mesh Watermark: Towards Highly Robust and Adaptable Deep 3D Mesh Watermarking," AAAI 2024.

URL : <https://ojs.aaai.org/index.php/AAAI/article/view/28613>

本編参照：第 4 章、第 6 章

R-118

Mildenhall, B. et al., NeRF: Representing Scenes as Neural Radiance Fields for View Synthesis, ECCV 2020.

URL : <https://arxiv.org/abs/2003.08934>

本編参照：第 6 章

R-119

Kerbl, B. et al., 3D Gaussian Splatting for Real-Time Radiance Field Rendering, ACM SIGGRAPH 2023.

URL : <https://arxiv.org/abs/2308.04079>

本編参照：第 6 章

12-5 保存資料・その他

R-120

List of registered items, JPSEC RA, 2025 年 2 月 9 日保存版. 保存時点では登録項目が表示されていない。全期間の登録履歴を証明するものではない。

URL : https://web.archive.org/web/20250209211023id_/https://www.jpsec-ra.jp/items/

本編参照：第4章、第7章、第8章、第9章、第10章

12-6 原典確認と参照上の留保

本書は、政府・行政機関、標準化機関、仕様策定主体、公式レジストリ、事業者の公式資料及び査読付き学術論文を優先しました。Wikipedia、出所不明の再配布資料、個人ブログ、まとめサイト又は一次資料で確認できない匿名投稿は、本文の事実根拠として採用していません。

有償規格については、公式カタログ、公開要約、目次又は発行機関が無償公開する部分だけを確認した箇所があります。特に CENC のアイテム対応は、ISO の公開要約から対象範囲を確認しており、有償の規格本文にある個別ボックス及び適用条件までは検証していません。

「確認できない」という記述は、公開一次資料の調査結果です。非公開システム、契約者限定機能、未索引資料又は将来仕様を含む絶対的な不存在の証明ではありません。

JPSEC について、保存公開一覧に登録項目が表示されていないことは、全期間の登録履歴を証明しません。また、制度変更の原因は公開資料から確定できません。

C2PA は来歴・真正性のための仕様であり、DRM 又はコピー防止そのものではありません。第 2.4 版、カメラ、編集ソフト及びプラットフォームの各公式資料を分けて掲載しています。

市場規模資料は、対象範囲と算定方法が異なるため単純に合算できません。市場規模の拡大は、被害額又は将来の被害増加を直接証明しません。

本章の収録 URL は重複除外後 120 件です。

第 13 章 図表一覧

本章は、第 1 章から第 10 章までに掲載する図、番号付きの表及び主な整理項目を一覧化したものです。図の内容は、対応する章の本文、出典及び「本章の記述に関する注記」と一体として参照してください。

13-1 図

番号	表題	ファイル	掲載箇所	内容
図 1	映像分野における保護の構造	図 1 映像分野における保護の構造.svg	第 3 章 3-6	映像分野で暗号化、API、信頼境界、ハードウェア、ライセンス及び適合性制度が接続される構造
図 2	非映像デジタルアセットにおける保護の構造	図 2 非映像デジタルアセットにおける保護の構造.svg	第 4 章 4-3-5	個別規格、GPU 部品及び用途別基盤が存在する一方、一般 Web・複数形式横断の接続を確認できない部分
図 3	技術的保護格差	図 3 技術的保護格差.svg	第 7 章 7-2	映像分野と一般 Web 上の非映像アセットにおける保護層の接続範囲の差
図 4	多層防御モデル	図 4 多層防御モデル.svg	第 8 章 8-4	既存対策と次世代共通層を用途とリスクに応じて組み合わせる構想

図 1 と図 2 は、対応する層を対照できる構成です。図 3 は、その接続範囲の差を本書の中心概念として示します。図 4 は、すべての対策を一律に適用する図ではなく、目的に応じて選択する多層防御の考え方を示します。

図中の「確認できない」又は「未接続」は、すべての技術、非公開実装又は将来仕様の不存在を意味しません。調査基準日までに確認した公開一次資料の範囲を示します。

13-2 番号付きの表

番号	表題	掲載箇所	内容
表 1-A	保護層の充足状況	第 7 章 7-2	類型ごとに、形式、API、信頼境界、ハードウェア、需要側主体及び適合性運用の成立範囲を比較
表 1-B	保護の便益に関わる性質	第 7 章 7-2	制作原本・構造データの必要性、端末へ渡るデータの再利用可能性及び配信経路で守れる範囲を比較
表 2	技術的対策の横断比較	第 6 章 6-3	六分類の対策について、守れる対象、限界、費用及び副作用を比較
表 3	政策提言の全体像	第 9 章 9-4	五つの提言、主な提言先、時間軸及び介入の度を整理

表中の評価記号は、本書の調査範囲に基づく相対的な整理です。対象となる仕組みの絶対的な不存在、すべての実装の性能又は将来の対応可能性を断定するものではありません。

13-3 本文中の主な整理項目

番号付きの表以外にも、議論の流れの中で次の表、一覧又は段階整理を掲載しています。

内容	掲載箇所
DRM、暗号化、アクセス制御、電子透かし、来歴管理及びライセンス管理の区別	第 3 章 3-1
映像分野の保護基盤を支える七つの条件	第 3 章 3-6

非映像分野に存在する規格及び技術要素の棚卸し	第 4 章 4-2-5
七条件に照らした一般 Web 上の接続状況	第 4 章 4-3-5
類型別の原本、実行用データ及び表示物	第 4 章 4-5
映像と非映像デジタルアセットの処理構造の対比	第 4 章 4-5-2
Web プレビューにおける目的別のデータ分離	第 5 章 5-2
七条件と個社が到達できる範囲	第 5 章 5-4
技術的対策の六分類	第 6 章 6-1
技術的保護格差の形成要因	第 7 章 7-4
次世代保護基盤の五つの機能層	第 8 章 8-2
段階的な実現経路	第 8 章 8-3
政策実施の判断ゲート	第 9 章 9-3
提言先別の役割	第 9 章 9-5
効果と副作用を分けた政策評価指標	第 9 章 9-6

13-4 図の利用上の注意

SVG は拡大しても劣化しないベクター形式です。Web 掲載、文書への挿入又は画像形式への変換を行う場合は、次を確認してください。

1. 縦横比、文字、矢印、凡例及び色の対応を維持する
2. 図の内容を説明する代替テキスト又は周辺本文を提供する
3. 色だけで意味を伝えず、ラベルと記号を残す
4. 対応章の留保より強い不存在又は完全防止の表現へ変更しない
5. 図だけを転載する場合も、書名、図番号、対応章及びライセンスを示す

13-5 表の利用上の注意

表を転載又は再構成する場合は、列見出し、評価記号の意味、調査範囲及び対応章を併記してください。表 1-A、表 1-B 及び形成要因の表は、本書が構成した比較・分析であり、定量的な実測値又は全実装の網羅調査ではありません。

第 14 章 奥付

14-1 利用条件

本書は、クリエイティブ・コモンズ 表示 4.0 国際 (CC BY 4.0) の条件で提供します。

ライセンス： <https://creativecommons.org/licenses/by/4.0/deed.ja>

出典を表示し、ライセンスへのリンクを示し、改変した場合はその旨を明示することで、複製、配布、改変及び営利目的での利用ができます。

出典表示例：

『技術的保護格差—非映像デジタルアセットの保護基盤に関する調査と政策提言—』

デジタルアセット保護基盤検討委員会 (Lycoris Studio)、2026 年、CC BY 4.0

本書が引用又は参照する各資料、規格、図表、商標、製品名等の権利は、それぞれの権利者に帰属します。CC BY 4.0 の対象は、デジタルアセット保護基盤検討委員会 (Lycoris Studio) が本書のために作成した文章、整理表及び図を基本とし、第三者の資料へ新たな利用許諾を与えるものではありません。

14-2 引用・紹介に関するお願い

次の事項は CC BY 4.0 の法的条件を追加又は制限するものではなく、本書の趣旨を正確に伝えるためのお願いです。

1. 本書を、非映像デジタルアセットには保護技術又は用途別基盤が一切存在しないとする資料として紹介しないでください
2. 本書を、コピーの完全防止が可能であるとする資料として紹介しないでください
3. 本書を、すべての作品への DRM 義務化又は開放的な形式の排除を求める資料として紹介しないでください
4. 個別事業者の過失又は脆弱性を断定する根拠として、事例部分だけを切り離して使用しないでください
5. 「確認できない」という記述を、非公開実装、未索引資料又は将来仕様まで含む絶対的な不存在へ置き換えないでください
6. 表又は図を改変した場合は、原図・原表と改変版を区別してください

14-3 免責及び調査上の限界

本書は、調査基準日までに公開されていた政府資料、公式仕様、標準化団体の資料、公式レジストリ、事業者の公式資料及び学術論文等に基づく調査と分析です。正確性の確保に努めていますが、次の限界があります。

1. 非公開システム、契約者限定機能、未索引資料及び将来の仕様を網羅していません
2. 有償規格には、公式カタログ、公開要約、目次又は無償公開部分だけを確認した箇所があります
3. 第 7 章の形成要因は、公開資料と章間比較に基づく説明仮説であり、各要因の寄与を数量的に実証したものではありません
4. 市場規模の拡大は、被害額又は将来の被害増加を直接証明しません
5. 行政組織名、部署名、事業名、予算、規格の状態、製品仕様及び URL は変更される場合があります
6. 本書は、個別事案に関する法律、セキュリティ、技術導入又は事業上の助言を提供するものではありません
提出、公開、引用又は施策化の時点で、更新性の高い情報を再確認してください。

14-4 訂正方針

事実誤認、出典との不一致、URL の変更、規格の更新又は表記上の誤りが判明した場合は、確認後に訂正版を公開します。意味に影響する訂正では、版番号、訂正日、対象箇所、訂正前後の内容及び理由を更新履歴へ記録します。

単なる誤字又は体裁修正であっても、公開済みファイルを差し替える場合は、少なくとも更新日を記録します。

14-5 お問い合わせ

本書に関する事実確認、訂正提案、専門的な意見又は利用に関する連絡は、次のお問い合わせフォームから受け付けます。

デジタルアセット保護基盤検討委員会（Lycoris Studio）お問い合わせフォーム：<https://dcapic.jp/contact/>

お問い合わせ時は、本書の書名、対象章、該当箇所、確認できる資料及び返信先を記載してください。

14-6 関連文書

本書には、用途の異なる次の関連文書があります。

文書	用途
行政提出用要約	行政機関及び政策担当者が中心命題、五つの提言、 判断ゲート及び評価指標を短時間で確認する
一般向け要約	技術的保護格差と政策提言を専門知識なしで理解する
要約と本編に差異がある場合は、本編第 1 章から第 14 章までを優先します。	

14-7 更新履歴

版	日付	内容
1.0	2026 年 09 月 01 日	初版公開

14-8 書誌情報

書名	技術的保護格差—非映像デジタルアセットの保護基盤に関する調査と政策提言—
種別	政策提言書
作成・著作権者	デジタルアセット保護基盤検討委員会（Lycoris Studio）
調査基準日	2026 年 8 月 28 日
版	1.0
公開日	2026 年 9 月 1 日
公開形態	オンライン文書
本文の正本	DOCX・PDF
図の正本	SVG