

OTTの保護



はじめに

動画の著作権侵害は、今に始まった問題ではありません。プロの映画製作の黎明期から、「著作権侵害の形で私有財産を悪用」することで、手っ取り早くお金を儲けようとする人々はいました。無声映画の時代には、「バイサイクリング」というやり方（劇場での映画上映の延長）が流行し、当時、ハリウッドはその対策として、悪徳行為を行う映画館主を捕まえるために「チェッカー」と呼ばれる調査員を送り込みました。しかし、インターネットを通じた「共有」により、デジタル配信は、何千もの海賊版動画を数百万の視聴者に即時配信するための最も簡単かつ効果的な手段となりました。

昨今、著作権侵害者は、さまざまな攻撃ベクトルを利用してコンテンツの取得や配布を行っています。一般的な手法には、Credential Stuffing（視聴者の詳細を把握し、正当なアカウントをハイジャックする攻撃）やテレビと見分けのつかない体験を提供するリニアチャネルの再ストリーミングなどがあります。海賊版ビジネスでは、使いやすいユーザー体験、カスタマーサービス、柔軟で多様なビジネスモデルも提供されています。

このような背景を念頭に、Akamai は著作権侵害の課題を探り、戦略的フレームワークによる対抗策を考察していきます。

E.U. 諸国では 1,370 万人が違法な海賊版サービスに定期的にアクセスしていると推定されています（EUIPO 2019 より）。国別に見ると、違法アクセス人口が最も多いのは、英国（240 万人）とフランス（230 万人）です。E.U. では海賊版による年間収益が推定 10 億ユーロに上ります（EUIPO 2019）。米国では、1,250 万を超える世帯が海賊版動画にアクセスしていると推定されています（Parks Associates 2019）が、アジア太平洋地域ではさらに海賊版がまん延している可能性があります。たとえば、2019 年の AVIA 調査によると、香港では消費者の 24% がインターネット・ストリーミング・デバイスを使用して海賊版チャンネルにアクセスしていることがわかりました。消費者全体に占めるその割合は、フィリピンでは 28%、台湾では 34%、タイでは 45% にのびります。つまり、業界全体の取り組みにも関わらず、動画の著作権侵害は、依然として世界的に深刻な問題であると考えられます。影響は業界全体に及び、経済的な損失や失業が発生すると考えられ、実際にライセンスへの影響の兆しも確認されつつあります。

対象が複雑であるため、確実な数値を示すことは困難ですが、全米商工会議所が委託したレポートによると、経済的損失は、映画業界では 400 億ドルから 971 億ドル、テレビ業界では 393 億ドルから 954 億ドルと推定されています（NERA Consulting 2019）。これにより、政府の税収も減少します。

テレビや映画業界はセットデザイナー、メイクアップアーティスト、ミュージシャンからプロデューサーやディレクターまで、数多くの仕事をサポートしていますが、著作権侵害はこうした仕事をも脅かしています。デジタルの著作権侵害が米国経済に与える影響に関する 2019 年のレポートで、著者である Blackburn、Eisenach、Harrison の各氏は、海賊行為の直接的な結果として、2019 年に米国では 23 万から 56 万の雇用が失われたと推定しています。

OTT の保護

**400 億ドル～
971 億ドル**

海賊版動画による映画
業界の推定損失額

**393 億ドル～
954 億ドル**

海賊版動画によるテレ
ビ業界の推定損失額

さらに、クリエイティブ業界の生命線であるライセンスにも海賊版の影響が及びつつあり、その兆候が見え始めています。間違いなく、海賊版は大きな損害をもたらす戦略的問題です。簡単に言えば、海賊版サイトを通じてコンテンツが無料ですぐに見つかるのに、配信企業はなぜ著作権に多額を支払わなければならないのか、ということです。スポーツ関連の著作権を購入している世界有数の企業、beIN の最高経営責任者である Yousef Al-Obaidly 氏は、「世界の海賊版によってスポーツ著作権のバブルは崩壊しつつあり、今後ビジネスモデルの見直しが必要になるでしょう」と述べています。また同氏は、自らの組織にとって、著作権の価値は独占権のレベルに基づくことも示唆しています。オスカーにノミネートされ、エミー賞を受賞したプロデューサー、Jason Blum 氏も、海賊版は、革新的でリスクの高い映画の制作に投じられる資金に直接打撃を与えていると述べています。また、近い将来のある時点で、今の売上を持続することは不可能になり、映画スタジオは撮影シーンを削らざるを得ないだろうと示唆しています。

著作権侵害産業の仕組み

どのような闘いにおいても、敵を理解することは重要です。そうすることで、敵の動機、戦術、長所、短所を明らかにすることができます。当然のことながら、知見を手に入れるのは簡単なことではありませんが、犯罪者集団には上位グループと下位グループの複雑な序列があり、動機も巧妙さもそれぞれ異なります。以下ではこうしたグループについて説明します。



リリースグループ

多くの場合、犯罪者集団のメンバーは、自分たちのことを大企業に挑む革命家だと思っています。アップロードサイトの会員になれるのは、それに値する信頼できる人のみです。さまざまなグループや個人が特定のジャンルを専門とし、新しい素材を取得するために競い合い、それが評価されることで報酬を得ています。FACT は、この構造について、「複雑で巧妙かつ、十分に組織化されたハッカースタイルのグループが、その他のサイバー犯罪にも関与している疑いがある」と述べています。



サイトの運営者

Pirate Bay のような動画共有サイトまたは TeaTV のようなストリーミングスタイルのサイトなどの海賊版動画サイトを管理します。リリースグループとサイト運営者が同一の個人であるかどうかは不明ですが、多くの調査結果から、この 2 つの間には重なりが多いことがわかっています。サイト運営者は、他のプロセスでも確実に収益を得ており、多くの場合、複数の「ミラー」サイトを運営しているため、いずれかのサイトが当局によって閉鎖されたとしても、別のサイトはそのまま維持されるので、収入が途絶えることはありません。



インターネット・ストリーミング・デバイスの卸売業者

このようなデバイス、特に Kodi の普及は、日和見的な犯罪者に、予測可能かつ比較的安定した収益源をもたらしています。卸売業者は、完全に合法的な手段または犯罪者ネットワークを通じて、Kodi ボックスを輸入します。その後、違法なソフトウェアを使ってそれらを改ざんし、オンラインで販売できるようにします。



ソーシャルメディアの著作権侵害者

このグループの人々は、著作権侵害が違法であるという認識が低いか曖昧で、特定ジャンルのコンテンツの利用料またはサブスクリプション疲れが侵害行為の要因となっています。

著作権侵害者によるコンテンツの入手方法

バリューチェーンにはさまざまな弱点があり、著作権侵害者がそれを悪用してコンテンツを盗む方法はたくさんあります。最もよく利用される方法をユースケース別にまとめました。



テレビ番組とライブイベントの同時放送

著作権侵害で最も急増している形態は、テレビ番組やライブイベントの録画と再配信です。これには次のような手段が利用されています。

- 動画再生ソフトウェアや Android OS で改ざんする
- モバイルデバイスを使用して再生中の画面を録画する
- セットトップボックスに接続された HDCP ストリッパーを使用して、復号化された動画を傍受する
- Credential Stuffing 攻撃で正当な視聴者の詳細情報にアクセスして悪用する
- VPN を使用して特定の市場から動画を転送する



オンデマンドのコンテンツ

リリースグループは公開前のテレビ番組や映画を重視します。メディア業界の構造上、制作プロセスにはさまざまな組織や個人が関わるため、取得する機会も多様です。動画を獲得する一般的な手段としては次のようなものがあります。

- データセンターに不正にアクセスしてユーザーの認証情報や動画コンテンツを盗む
- ユーザー ID を盗み、さまざまな制作システムを通じて動画コンテンツへのアクセスを可能にする
- 共有や再配信を目的として物理的なアセットを録画する（現在はあまり利用されていない）
- さまざまな制作システムをハッキングして、動画に直接アクセスする
- iTunes などの正当な配信元からコンテンツをリッピングする
- 映画館で上映中の作品を盗撮する
- 中間者攻撃で直接盗む

OTT の保護

著作権侵害者によるコンテンツの配信方法

著作権侵害者はコンテンツを配信するために、次のようなあらゆるチャンネルや最新技術を使用します。

- 事前にプログラムされているテレビ番組のストリーミングにアクセスするカスタムビルドの IP セットトップボックス
- ストリーミングデバイスや PC で稼働し、海賊版の配信を可能にするソフトウェア（Kodi など）
- 市販のストリーミングデバイスにサイドロードされたアプリ
- YouTube など、ユーザーが制作したコンテンツをホストする Web サイトやソーシャル・メディア・サービス
- 検索やソーシャルメディアで見つかったリンクを通じて海賊版コンテンツをストリーミングする Web サイト
- 常に存在するダウンロードサイト、ファイル・ホスティング・サイト、サイバーロッカーサイト、動画共有サイト

著作権侵害者にはさまざまなタイプがあり、その配信戦略についてはあまり解明が進んでいないものの、リリースグループは、どこからでも利用できる利他的なサイバーロッカーや動画共有サイトなどのアセット共有モデルを好む傾向にあることがわかっています。これとは対照的に、金銭を目的とするサイト運営者は、合法的なサービスを模倣する ISD ノストリーミング戦略や複数の収益モデルを促す機能を好む傾向があります。

需要

人々はさまざまな理由で海賊版サイトを探します。経済的な理由や広範に影響が及ぶことを知らなかった、また基本的に時間的な制約なしにコンテンツにアクセスできるなど、その理由は多岐にわたります。VFT Solutions Inc. は、同社の 2019 年のレポートで、海賊版の視聴者にはさまざまなタイプがあることを指摘しました。これらを以下にまとめます。

- **「コンテンツアナーキスト」**：オンラインコンテンツは地域社会で共有され、自由にアクセスできると信じています。コンテンツに対して料金を請求すべきではなく、海賊版が不道德とも違法とも思っていません。
- **「コンテンツ・ロビン・フッド」**：考え方はそれほど過激ではありませんが、代替案を検討してもよいと考えています。このタイプの人はライブストリーミングサービスのユーザーではなく、共有動画ファイルの拡散に関係しています。
- **「功利主義者」**：コンテンツに価値があるのはつかの間のことなので、コンテンツが広く消費されても、権利者にとっては損失でも有害でもない主張することで、自分の行為を正当化します。
- **「怠惰な著作権侵害者」**：多くの場合、海賊版は違法であるという事実を知らないか、または知らないふりをしています。このタイプの人は、費用の節約や広範な入手可能性、さらにアクセスしやすさなどの影響を受けます。

VFT は、「怠惰な著作権侵害者」と「功利主義者」のタイプがコミュニティ全体の最大 70% を占めると推定し、これらのグループを啓発し、改心を促し、また違法行為については罰金を科すことで、著作権侵害の状況を大きく変えることができるとしています。

OTT の保護

著作権侵害は阻止できるか？

一言で答えると、残念ながら「完全には阻止できない」です。歴史を見ても、利他的な動機であろうと、営利目的であろうと、コンテンツを悪用しようとする海賊版はなくなりません。ただし、打つ手がないわけではありません。バリューチェーン全体で戦略的に問題に対処すれば、最小限に抑えることができます。実際問題としては、以下に示すような戦略領域について、業界全体の協力を強化することで、効果が持続します。

データ

明確な要件の 1 つは、世界の海賊版の拡がりと影響を測定する標準手法を確立することです。手法やテクニックが異なると、継続的な分析もコンテキスト分析もできず、アクティビティの優先順位を判断したり、海賊版対策の成果を理解する際に混乱が生じます。この状況は、Alliance for Creativity and Entertainment (ACE) のような業界団体がデータ収集を主導することで改善される可能性があります。

教育

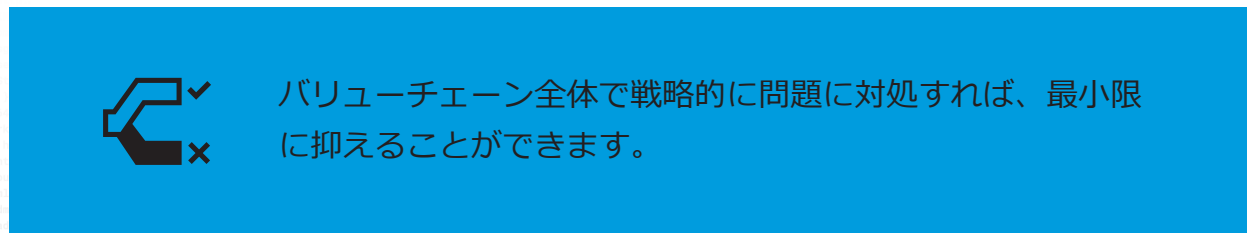
海賊版がまん延し、「誰でも」しているとみなされると、そのふるまいが普通となり違法行為には見えなくなります。人々を啓発する取り組みを継続することで、海賊版は犯罪であり生活に実際に影響するというのを継続的に思い出させる必要があります。

法律と規制

さまざまな業界団体の取り組みや、イタリアの FAPAV などの政府の取り組みのなかには、動画の著作権侵害者を訴追し、世界中の法の抜け穴を埋める優れたものもいくつかあります。このような取り組みには、調整や関連データへのアクセスが必要です。

技術と運用

コンテンツを保護せずに済む時代はもはや遠い昔です。では現実的にどうすべきかですが、運用を戦略的に見直し、制作から配信までの技術的なバリューチェーンにおける脆弱なリンクを特定し、適切な対策を適用することが必要です。これを全方位型の対策と言います。



全方位型の対策

私たちは、著作権侵害者の集団が動画の入手や配信に使う手段を再調査し、3つの基本原理に基づくフレームワークを構築しました。その3つとは、保護、検知、措置です。このフレームワークを使用すれば、業界での役割に基づいて脅威の状況を戦略的に見直し、運用および技術に関する適切な取り組みを実施することで、影響を最小限に抑えることができます。

保護

Credential Stuffing からの保護

前述のとおり、Credential Stuffing は著作権侵害者が視聴者の詳細情報を入手するためによく使う攻撃ベクトルです。通常、この攻撃には自動ボットが利用されます。以下は、その主な推奨事項です。

- OWASP によるログインページ／API のコード化。OWASP ベストプラクティスに従ってセキュアなコードを記述し、ログインエンドポイントでペネトレーション（侵入）テストを実施します。
- DDoS 防御対策の使用。大量のボットネットがインフラに到達して、アセットを制圧するのを防ぐことができます。
- Akamai の Bot Manager Premier などのボット管理ソリューションの利用。ユーザーのふるまいとデバイスステレメトリーの検証は、巧妙な Credential Abuse 攻撃を阻止するために役立ちます。

システムからの窃盗に対する保護

組織内の制作システム、デジタルストレージ、またはパブリッククラウドからの窃盗は、海賊版コンテンツの重要なソースです。大まかに言って、動画アセットの窃盗には以下のような形態が見られます。

- 著作権侵害者による直接的なハッキングや中間者攻撃
- パスワードなどの一意のシステム ID の入手
- 従業員やフリーランサーによる窃盗

こうしたリスクを最小限に抑えるために、企業はいくつかのテクノロジーを利用できます。それらは基本的に、企業がテクノロジーへのアクセスを変革する際に使用するフレームワークであるゼロトラストの考え方を中心としたものです。このフレームワークの主な構成要素は、場所やホスティングモデルに関係なくあらゆるリソースへの安全なアクセスを確保すること、最小権限に基づくアクセス制御戦略を実現すること、疑わしい活動を検知するためにすべてのトラフィックを調査して記録することなどです。このフレームワークでは、認証済みのユーザーとデバイスのみがアプリケーションやデータにアクセスできます。また、インターネット上の高度な脅威からアプリケーションとユーザーを保護することもできます。

OTT の保護

企業がゼロトラスト・フレームワークの実装に使用できる構成要素はいくつかありますが、制作やストレージのコアシステムに対する従業員／フリーランサーのアクセスにおいてセキュリティを確保することは非常に重要です。一時的な人員を抱えるメディア企業は、システムへのアクセス権の実装と取り消し（場合によっては毎日のように発生します）という独特の課題に直面しています。Akamai の Enterprise Application Access などのサービスを使用すれば、ユーザーおよびデバイスのアイデンティティとセキュリティ状況に基づいて、特定のアプリケーションに対する許可を即座に付与できます。そのため、動画の窃盗が生じる可能性のある社内ネットワーク全体へのアクセス権をユーザーに与えずに済みます。

ゼロトラストのもう 1 つのコアな側面は、著作権侵害者が中間者攻撃のツールとして使用するマルウェア、ランサムウェア、フィッシングなどの標的型脅威を事前に特定してブロックするシステムの実装です。たとえば、Akamai の Enterprise Threat Protector はセキュア Web ゲートウェイであり、リアルタイム・セキュリティ・インテリジェンスを使用して、マルウェア、ランサムウェア、フィッシング、DNS ベースのデータ流出などの標的型脅威を事前に特定してブロックします。

地理および IP ベースの権限侵害からの保護。著作権侵害者は多くの場合、VPN テクノロジーを使用して攻撃元の国や IP アドレスを隠し、正当な加入者の詳細情報を取得して、コンテンツの再ストリームに成功します。Akamai の Enhanced Proxy Detection のようなプロキシ検知テクノロジーは、匿名プロキシや VPN サービスに関連したリクエストをエッジでインテリジェントにブロックすることで、このようなユースケースを防ぎます。

再生侵害からの保護。これは、最もよく利用されている著作権侵害対策です。さまざまな方法で実現できますが、中でも最も普及している手法はデジタル著作権管理（DRM）です。DRM は、著作権で保護されたコンテンツを制限して、不正な配信を防ぐために使用されるツール、基準、およびシステムです。それ自体で 1 つのテクノロジーを意味するわけではありません。

保護対象のアセットの重要度にもよりますが、シンプルな暗号化（コンテンツをコード化し、キーを使ってコードを解除しないと、デバイスやソフトウェアで読み込みができないようにする方法）で十分だと考える配信業者もいます。この方法でも、解除用のキーが必要になるため、大ざっぱではあるもの無頓着な著作権侵害は防御できます。ただし、キーは一般に HTTP サーバーによって配信され、コピーや共有もできるため、多くの場合、これだけでは高価値コンテンツの保護には不十分です。

暗号化を補強するため、より高度な DRM テクノロジーでは、コンテンツ復号モジュールを介し、チャレンジ／レスポンス認証システムを使用してキーの伝達を処理します。キーの伝達は暗号化されるため、復号キーはハッキングされても解読することはできません。また、高度な DRM テクノロジーでは、ロケーションや時間ベースのルールなど、さまざまなデバイスでいつどのようにキーを使用できるかを定めたビジネスルールも設定できます。

パッケージ化のプロセスで DRM を実装したいと考える配信業者には、DRM の複雑さに対応できるクラウドプロバイダーと契約することをお勧めします。Akamai もそうしたプロバイダーとして、オンデマンドコンテンツのオリジンストレージを Bitmovin や Encoding.com などの複数のプロバイダーの処理機能と統合しているので、暗号化をほぼリアルタイムで実装できます。



一時的な人員を抱えるメディア企業は、システムへのアクセス権の実装と取り消し（場合によっては毎日のように発生します）という独特の課題に直面しています。

検知

形態を問わず窃盗はみな同様ですが、保護対策は成功するとは限らないため、侵害の検知はきわめて重要です。著作権侵害行為をほぼリアルタイムで検知するには、次のようないくつかの手法があります。



フィンガープリント

この手法には、元のメディアに手を加えることなく、動画コンテンツを特定する機能があります。ツールを使用して、動画ファイルの特定と抽出を行い、その属性を明らかにすることで、ファイル共有ネットワークなどに残された固有の「フィンガープリント」によって動画を特定できます。元のメディアに何も変更を加える必要がないのは長所ですが、フィンガープリントでは同じ作品の複数のコピーを区別することはできません。そのため、最初にどのコピーが漏えいしたのかはわかりません。



ウォーターマーク

著作権侵害を阻止することはできませんが、サービスプロバイダーが著作権侵害を検知し、当事者を特定し、何らかの対策を講じるのに役立ちます。動画のウォーターマークでは、判別できない消去不能な「ビット」パターンを動画ファイルに追加します。このデータを視聴者のアイデンティティに結び付けることで、復号されたコンテンツをコピーして、違法に再配信している著作権侵害者を追跡できます。現在使用されている動画ウォーターマークには、主に次の3種類の手法があります。

- **ビットストリームの変更。**動画品質を維持しながら映像の一部を変更しておくことで、視聴者とセッションを特定できるようにします。これは堅牢な手法ですが、コンピューティングのオーバーヘッドが大きく、システムにレイテンシーが加わるため、ライブコンテンツには適していません。
- **クライアント側のウォーターマーク。**ウォーターマークを迅速に抽出できるうえ、セットトップボックスのようなレガシープラットフォームにも展開できます。クライアントデバイスの動画ストリームにグラフィカルオーバーレイが合成されます。これは表示することも非表示にすることもできます。ウォーターマークは、クライアントデバイスに到達するまで適用されないため、動画ストリームにはさらに保護を追加する必要があります。クライアント側のテクノロジーには SDK のデプロイも必要となるため、OTT 環境が複雑になる場合があります。
- **A/B バリエーションウォーターマーク。**OTT セクターを対象とした手法です。同一の動画ストリーミングを2つ作成し、それらにウォーターマークを埋め込んでから、クライアント側、または CDN エッジ処理を通じてその2つをステッチまたはインターレースでつなぎ、一意の識別子を提供します。この手法は堅牢でコスト効率にも優れていますが、シーケンスの特定に時間がかかるため、ウォーターマークをすぐに抽出する必要があるケースでは好まれません。

どのウォーターマーク戦略にも重要なのは、監視を十分に行い、著作権侵害者に対して適切な措置を適用できるようにすることです。マネージド監視サービスを利用できることもあれば、社内で機能を開発するために助言を求めることもできます。Akamai は主要なウォーターマークプロバイダーと協力することで、実用的なソリューションを開発し、動画の著作権侵害に関する戦略全体に統合できるようにしています。

ストリーミングのログ ID

もう 1 つの検知手法として、配信ログのリアルタイム検査があります。この場合、ログを詳しく調べることで、認証済みの IP アドレスと不正な IP アドレスに基づいて、侵害アクティビティの全体像をリアルタイムで把握できます。Akamai の Stream Protector のようなソリューションのメリットは、状況に応じて機能のオンオフを切り替えられることです。これは、スポーツのように時間的な制約のある権利の保護には最適です。

措置

著作権侵害アクティビティが検知された場合、次に重要なのは適切な方法で対処することです。戦略によっては、多数のさまざまな手段を講じることになります。

- **アクセスの取り消し。**スポーツイベントのように、時間的制約のある動画アセットの場合は、違法ストリーミングの発信元へのアクセスを即座に取り消すことができます。アクセスを取り消す方法はいろいろあります。一般的な方法は、配信サービスプロバイダーと協力して、詳細な情報を交換し、違法な IP アドレスからのストリーミングアクティビティを停止します。ただし、この処理には時間がかかります。Akamai は、人の介入を必要とせずに、ストリーミングをリアルタイムで取り消すことができるサービスを提供しています。このサービスは、ウォーターマークまたはストリーミングのログ ID のいずれかを使用して、著作権侵害の監視を行っている場合は、特に効果的です。
- **ストリーミングの変更。**時間的制約が少ない場合、配信業者は海賊版ストリーミングを代替コンテンツ（Big Buck Bunny がよく使われます）に置き換えるか、ストリーミングの品質を低下させることで、海賊版ストリーミングに修正を加えることができます。このアプローチには、著作権侵害者が検知に気付かないため、別のストリーミングソースへの切り替えを阻止できるというメリットがあります。
- **リアルタイムのメッセージング。**著作権侵害者のタイプに関するセクションで説明しましたが、「怠惰な著作権侵害者」はインターネットの匿名性によって安全だと感じています。VFT のような組織は、ソーシャル・メディア・プラットフォームで海賊版ストリーミングの視聴者を特定し、権利侵害者に直接メッセージを送ることができます。この形態の措置では、配信業者は正規ストリーミングへのアクセスを提供し、それでも侵害が続く場合は法定通知を行うなど、措置を変更することができます。

結論

IP を利用した動画の著作権侵害は複雑で繊細な問題ですが、メディア業界の長期的な存続を脅かす可能性があることは衆知の事実です。著作権侵害が重大な経済的損害をもたらす証拠はたくさんありますが、さらに重要なのは、著作権侵害がグローバル・ライセンス・モデルを根本からむしばみ、大きな影響を与える可能性があるという点です。

しかし、これまで、業界からの反応はあまり聞かれませんでした。あるアナリストは、「今はまだ初期導入の段階であり、これからやるべきことが山積み状態です」と述べています。配信業者の多くが脅威を認識するようになり、「最大手（Tier1）」の動画制作会社や運営会社でも著作権侵害の理解を深めるための専門チームを設立して、自社の状況を評価し、著作権侵害対策戦略を実装しています。

本書では、差し迫った要件がいくつか特定されましたが、それらは業界が闘いに勝つために必要です。具体的には、著作権侵害の一貫したデータポイント、一般の人々に対する継続的な啓発とその改善、業界全体の協力の強化、そして、あらゆるジャンルの権利所有者のリーダーシップによって、権利の処理と配布において業界全体でユビキタス性を促進することが必要です。

うれしいことに、その多くは動き始めています。この問題に関する調査が検討され、より厳しい法律も制定されるようになりました。また、ベンダーは対策の効果を最大化するため、さまざまな機能を組み合わせています。たとえば、Akamai も、サイバーセキュリティの専門知識を活かすことに加え、主要なすべてのウォーターマーク企業と協力することで、著作権侵害者が検知された場合に、そのアクティビティを直ちに停止できるようにしています。さらに、著作権所有者が技術ワークフロー全体で、コンテンツ保護の最低基準を強く要求する兆しも見えています。今のところ、これらは個別の事例や「提案」(MPAA など) ですが、これからは、ビジネスの必須機能になっていくと思われます。

これらのような取り組みが実施されることで、問題は最小限に抑えられ、財政的な損失は減少し、雇用機会は守られ、ライセンス供与はグローバル市場で繁栄し続けることができます。

参考文献

- Asia Video Industry Association 『The Asia Video Industry Report』（アジアビデオ業界レポート）（2019 年）
- Bevir 『Cost of online piracy to hit \$52bn』（オンラインの著作権侵害による被害は 520 億ドルに到達）（2017 年）出典：<https://www.ibt.com/publish/cost-of-online-piracy-to-hit-52bn/2509.article>
- Blackburn 他 『Impacts of Digital Video Piracy on the U.S. Economy』（デジタル動画の著作権侵害による米国経済への影響）（2019 年）
- Coberly 「Streaming services are 'killing' piracy」（ストリーミングサービスは著作権侵害の「格好」の餌食）出典：<https://www.techspot.com/news/78977-streaming-services-killing-piracy-new-zealand-study-claims.html>
- CustosTech 『The Economics of Digital Piracy』（デジタル著作権侵害の経済学）（2014 年）
- Daly 『The pirates of the multiplex』（著作権侵害の倍増）出典：<https://www.vanityfair.com/news/2007/03/piratebay200703>
- Decary, Morselli, Langlois 『A Study of Social Organisation and Recognition Among Warez Hackers』（ウェアーズハッカーの社会組織と認知度に関する調査）（2012 年）
- Digital Citizens Alliance 『Fishing in the piracy stream』（海賊版ストリーミングによる不正行為）出典：https://www.digitalcitizensalliance.org/clientuploads/directory/Reports/DCA_Fishing_in_the_Piracy_Stream_v6.pdf
- EnigmaX 『Interview with a Warez Scene Releaser』（ウェアーズシーンのリリース担当者へのインタビュー）（2007 年）出典：<https://torrentfreak.com/interview-with-a-warez-scene-releaser/>
- 欧州委員会 『Estimating displacement rates of copyrighted content in the EU』（EU における著作権保護されたコンテンツの置き換え率の推定）（2015 年 5 月）
- 欧州連合知的財産庁 『Trends in Digital Copyright Infringement in the European Union』（EU におけるデジタル著作権侵害の傾向）（2018 年）
- 欧州連合知的財産庁 『Illegal IPTV in the European Union』（EU における違法 IPTV）（2019 年）
- FACT 『Cracking down on digital piracy』（デジタル著作権侵害の撲滅）（2017 年）
- Feldman 『Almost 5 million Britons use pirated TV streaming services』（ほぼ 500 万人の英国人が海賊版のテレビストリーミングサービスを使用）（2017 年）出典：<https://yougov.co.uk/topics/politics/articles-reports/2017/04/20/almost-five-million-britons-use-illegal-tv-streami>

FriendsMTS『Comparing subscriber watermarking technologies for premium pay TV content』（プレミアム有料テレビコンテンツ向けウォーターマークテクノロジーの比較）（2019 年）

Frontier Economics『The economic impacts of counterfeiting and piracy』（偽造と著作権侵害による経済的影響）BASCAP および INTA 用に準備された報告書（2017 年）

Granados『Report: Millions Illegally Live-Streamed El Clasico』（レポート:数百万人がエル・クラシコの違法ライブストリーミングを視聴）（2015 年）出典：<https://www.forbes.com/sites/nelsongranados/2016/12/05/sports-industry-alert-millions-illegally-live-streamed-biggest-spanish-soccer-rivalry/#3544c3f37147>

Greenburg『Economics of video piracy』（動画の著作権侵害の経済学）（2015 年）<https://pitjournal.unc.edu/article/economics-video-piracy>

Ibosiola D., Steery B., Garcia-Recueroy A., Stringhiniz G., Uhligy S., Tysony G.『Movie Pirates of the Caribbean: Exploring Illegal Streaming Cyberlockers』（映画『パイレーツ・オブ・カリビアン』:違法ストリーミングサイバーロッカーに関する考察）（2018 年）

英国知的財産庁『Online Copyright Infringement Tracker』（オンライン著作権侵害トラッカー）（2018 年）

Jarnikov 他『A Watermarking System for Adaptive Streaming』（アダプティブストリーミングのウォーターマークシステム）（2014 年）

Jones, Foo『Analyzing the Modern OTT Piracy Video Ecosystem』（最新の OTT 海賊版動画エコシステムの分析）SCTE・ISBE（2018 年）

Joost Poort 他『Global Online Piracy Study』（グローバルオンライン著作権侵害の調査）、University of Amsterdam Institute for Information Law（2018 年 7 月）

Kan『Pirating 'Game of Thrones'? That file is probably malware』（「ゲーム・オブ・スローンズ」の海賊版ファイルはマルウェアの確率が高い）（2019 年）出典：<https://mashable.com/article/pirating-game-of-thrones-malware/?europe>

Lee, T.『Texas-size sophistry』（テキサス規模の理屈）（2006 年）出典：<http://techliberation.com/2006/10/01/texas-size-sophistry/>

Liebowitz S.『The impact of internet piracy on sales and revenues of copyright owners』（インターネット著作権侵害が著作権所有者の売上と収益に与える影響）（Ruth Towse/Christian Handke 共同編集『Handbook on the Digital Creative Economy（デジタル制作経済に関するハンドブック）』に掲載の Edward Elgar『Internet piracy: the estimated impact on sales（インターネット著作権侵害：推定される売上への影響）』の縮約版）（2013 年）

Mick, J.『Nearly half of Americans pirate casually, but pirates purchase more legal content』（アメリカ人のほぼ半数が何気なく海賊版を利用しているが、著作権侵害者はそれより多くの正規コンテンツを合法的に購入している）（2013 年 1 月 21 日）出典：<http://www.dailytech.com/Nearly+Half+of+Americans+Pirate+Casually+But+Pirates+Purchase+More+Legal+Content/article29702.htm>

アメリカ映画協会『The Economic Contribution of the Motion Picture & Television Industry to the United States』（映画・テレビ産業による米国への経済的貢献）（2018 年 11 月）

『MPA Content Security Program - Content Security Best Practices Common Guidelines』（MPA コンテンツ・セキュリティ・プログラム - コンテンツセキュリティのベストプラクティス共通ガイドライン）Motion Picture Association（2019 年）

MUSO『Measuring ROI in content protection』（コンテンツ保護における ROI の測定）（2020 年）

Nordic Content Protection Group『Annual Report, 2020』（年間レポート、2020 年）

Parks Associates『Video Piracy: Ecosystem, Risks, and Impact』（動画の著作権侵害：エコシステム、リスク、影響）（2019 年）

Tassi, P.（2014 年 4 月 15 日）『“Game of Thrones” sets piracy world record, but does HBO care?』（「ゲーム・オブ・スローンズ」は著作権侵害の世界記録を樹立したが、HBO は気にしているのだろうか？）出典：<http://www.forbes.com/sites/insertcoin/2014/04/15/game-of-thrones-sets-piracy-world-record-but-does-hbo-care>

Sanchez, J.（2012 年 1 月 3 日）『How copyright industries con congress』（著作権業界は議会にいかにかに反論するか）出典：<http://www.cato.org/blog/how-copyright-industries-con-congress>

Sandvine『Video and Television Piracy』（動画とテレビの著作権侵害）（2019 年）

Schonfeld『Pirate Bay makes \$4m a year』（Pirate Bay は年間 400 万ドルの利益をあげている）（2008 年）出典：<https://techcrunch.com/2008/01/31/the-pirate-bay-makes-4-million-a-year-on-illegal-p2p-file-sharing-says-prosecutor/>

Sulleyman『Pirate Treasure: How Criminals Make Millions From Illegal Streaming』（海賊の宝物：犯罪者はいかにして違法ストリーミングから多額の金を稼ぐのか）（2017 年）出典：<https://www.independent.co.uk/life-style/gadgets-and-tech/news/piracy-streaming-illegal-feeds-how-criminals-make-money-a7954026.html>



Akamai は世界中の企業に安全で快適なデジタル体験を提供しています。Akamai のインテリジェントなエッジプラットフォームは、企業のデータセンターからクラウドプロバイダーのデータセンターまで広範に網羅し、企業とそのビジネスを高速、スマート、そしてセキュアなものにします。マルチクラウドアーキテクチャの力を拡大させる、俊敏性に優れたソリューションを活用して競争優位を確立するため、世界中のトップブランドが Akamai を利用しています。Akamai は、意思決定、アプリケーション、体験を、ユーザーの最も近くで提供すると同時に、攻撃や脅威は遠ざけます。また、エッジセキュリティ、Web / モバイルパフォーマンス、エンタープライズアクセス、ビデオデリバリーによって構成される Akamai のソリューションポートフォリオは、比類のないカスタマーサービスと分析、365 日 / 24 時間体制のモニタリングによって支えられています。世界中のトップブランドが Akamai を信頼する理由について、www.akamai.com、blogs.akamai.com、および Twitter の [@Akamai](https://twitter.com/Akamai) でご紹介しています。全事業者の連絡先情報は、www.akamai.com/locations をご覧ください。公開日：2020 年 7 月。