平成27年度産業経済研究委託事業
コンテンツ保護の技術的手段に係る法制度
及び技術動向等に関する調査研究

報　告　書

平成２８年３月

一般財団法人デジタルコンテンツ協会

はじめに

１　調査の目的

近年、スマートフォンなどの高度通信機器の普及及び AV 機器の高度化・多様化が急速に進むに伴い、コンテンツ提供のあり方も大きく変化しつつある。コンテンツとメディアが 1 対 1 対応していた時代から、コンテンツがデジタルビット化されメディアを選ばない時代となり、映画やアニメなどの映像系コンテンツはインターネットを利用した動画サイトを通じて提供され、音楽系コンテンツは音楽ダウンロードサイトを通じて提供されるようになった。加えて、様々なスマートフォンアプリなどの従来普及していなかったモバイルコンテンツの社会浸透も著しい。

アメリカの Anime Expo、フランスの Japan Expo など、日本映画やアニメなど我が国のコンテンツは「クールジャパン」として世界でも高く評価されており、我が国におけるコンテンツ産業の市場規模も約 12 兆円に上る。このような中、行政府・立法府としても、コンテンツ振興の重要を認識しており、平成 16 年には「コンテンツ振興法（コンテンツの創造、保護及び活用の促進に関する法律)」が成立し、平成 25 年に策定された「知的財産政策ビジョン」においても「コンテンツを中心としたソフトパワーの強化」が政策の 4 本柱の一つとして盛り込まれているところである。

不正競争防止法等においては、コンテンツの不正複製・視聴等を防ぐためにコンテンツ提供事業者や著作権者が用いている技術的手段について、それを不正に回避・無効化する機器等の譲渡を規制すること等により、その保護を図っている。

しかし、上記のようなコンテンツ提供の態様の多様化・高度化が著しい状況を踏まえると、現在の不正競争防止法等による法的保護が実態に即したものとなっているか否かを即応的に確認していく必要がある。

上記に鑑み、本調査研究では、現在のコンテンツ提供における技術的手段の技術態様を把握するとともに、我が国における技術的手段に関連する法規制の状況、技術的手段に関する紛争における争点、不正競争防止法と著作権法による規制の状況比較、諸外国における技術的手段法制の実体法のあり方、その規制運用の状況等についての調査を行った。

２　調査方法

音楽、映像（放送を含む。)、ゲームソフト、電子出版、ビジネスソフトの各コンテンツ分野の企業及び関係団体等へのヒアリングを通じて情報収集、問題の所在の整理、現行規制に係る意見集約を行った。

また、我が国研究者へのヒアリング、調査対象国・地域（アメリカ、イギリス、ドイツ、フランス、EU）の研究者からの情報収集により、文献や判例を収集した。

３　本報告書における用語の定義

◇　**コンテンツ**

様々なメディア上で流通する映像・音楽・ゲーム・図書など、動画・静止画・音声・文字・プログラムなどの表現要素によって構成される情報の中身を言う。

（本報告書において用いる際は、当該情報が著作権保護対象であるか否かを問わない。）

◇　**コンテンツの利用**

複製、視聴、送信その他あらゆる態様により、コンテンツを享受することを言う。

◇　**コンテンツへのアクセス**

コンテンツの利用を可能とするために、コンテンツに接触することを言う。

◇　**コピー等利用制限技術**

コンテンツの利用を、電子的方法、磁気的方法その他の方法によって制限する技術を言う。

◇　**アクセス制限技術**

コンテンツへのアクセスを、電子的方法、磁気的方法その他の方法によって制限する技術を言う。

◇　**認証技術**

パスワード、ID 又は指紋・虹彩・音声等の識別符号を用いて、コンテンツにアクセスし、利用しようとする者が当該コンテンツに係る権原を有するか否かの確認を行うための技術を言う。

◇　**コピーコントロール技術**

日本著作権法において定められている著作物を利用する権利の対象となる行為を、電子的方法、磁気的方法その他の方法によって制限する技術を言う。

本報告書においては、もっぱら日本著作権法に関わる文脈においてのみ本用語を用いる。

◇　**アクセスコントロール技術**

日本著作権法において定められている著作物を利用する権利の対象外の行為を、電子的方法、磁気的方法その他の方法によって制限する技術を言う。

本報告書においては、もっぱら日本著作権法に関わる文脈においてのみ本用語を用いる。

◇　**技術的制限手段**

不正競争防止法第 2 条第 7 項によるものとする。

◇　**技術的保護手段**

著作権法第 2 条第 1 項第 20 号によるものとする。

◇　**技術的手段**

コピー等利用制限技術、アクセス制限技術及び認証技術の総称を言い、不正競争防止法及び著作権法における評価を勘案しないものとする。

◇　**DRM（Digital Rights Management）**

コピー等利用制限技術、アクセス制限技術、認証技術及びコンテンツに関わる権利の侵害を抑止するために用いられる電子透かし等の技術の総称を言い、不正競争防止法及び著作権法における評価を勘案しないものとする。

４　技術的手段の技術内容による分類

（１）非暗号型

①フラグ型

暗号化されていないコンテンツに利用制御信号（フラグ）を付加し、機器側がその信号（フラグ）を検出、反応して複製等を制御する技術的手段を言う。MD（Mini Disc）等に用いられる SCMS（Serial Copy Management System）、DVD 等に用いられる CGMS(Copy Generation Management System)、デジタル録画機器での擬似シンクパルス方式（マクロビジョン）がこれに該当する。

②エラー惹起型

暗号化されていないコンテンツに、エラー信号を付加し、当該信号によって機器の既存機能を一方的に誤作動させて、複製等を制御する技術的手段を言う。CCCD(Copy-Controlled Compact Disc)、アナログ録画機器での擬似シンクパルス方式（マクロビジョン）がこれに該当する。

（２）暗号型

コンテンツ自体を暗号化することにより、非正規機器による複製等を制限する技術的手段を言う。DVD 等に用いられる CSS（Content Scramble System）、SD カード等に用いられる CPRM（Content Protection for Recordable Media）、Blu-ray 等に用いられる AACS（Advanced Access Content System）、機器間伝送路用に用いられる DTCP（Digital Transmission Content Protection）・HDCP（High-bandwidth Digital Content Protection）、放送用に用いられる B-CAS（BS-Conditional Access Systmes）方式がこれに該当する。

５　主な技術的手段

略称	概要	分類
AACS	Advanced Access Content System。AACS LA が策定した映像コンテンツの保護規格。Blu-ray Disc に採用。機器メーカに対し、再生機器が規格に従うこと及び鍵情報の秘匿を義務付ける。規格に準拠した Blu-ray Disc の映像コンテンツは暗号化されており、復号鍵を持っている再生機器でしか再生することができない。コンテンツにコピー制御信号を付加することで、他の媒体への複製を制限する。	暗号型のアクセス制限及びフラグ型のコピー等利用制限
B-CAS	Broadcast Conditional Access System。B-CAS 社が管理運営する放送限定受信システム。B-CAS 社がカードの ID 番号とマスター鍵をカードベンダに発行、カードベンダがカード ID 番号とマスター鍵を書きこんだ B-CAS カードを製造し、受信機メーカに支給、受信機メーカが電波産業会(ARIB)の規格に準拠した受信機器に B-CAS カードを同梱して出荷。受信機を購入したユーザーがスロットに装着。放送は暗号化され、B-CAS カードのマスター鍵で復号化される。	暗号型のアクセス制限
C-CAS	Cable-Conditional Access System。日本 CATV 技術協会が策定したケーブルテレビ用限定受信システム。C-CAS カードが使用されるが、仕組みは B-CAS システムとほぼ同じ。	暗号型のアクセス制限
CCCD	Copy Controlled CD。音楽 CD に埋め込まれた誤り訂正符号を意図的に壊しておき、パソコンによるデータの読み取りを阻止する。midbartech 社の「CDS-200」「CDS-300」、First 4 Internet 社の「XCP」、ソニーミュージックの「レーベルゲート CD」などの製品がある。	エラー惹起型のコピー等利用制限
CGMS	Copy Generation Management System。映像コンテンツのコピーの可否、回数を制御するため、映像データに、コピー不可、コピー１世代可、コピー無制限を設定する制御信号を付加し、対応するレコーダーに相応の動作をさせる。	フラグ型のコピー等利用制限
Cinavia	電子音声透かしを利用したコピー等利用制限技術。不正な Blu-ray ディスクが再生されると、再生機器が、音声に埋め込まれた電子透かしに格納された情報から不正利用であることを検知し、映像コンテンツの再生を停止したり、音声をミュートする。	非暗号型・フラグ型のコピー等利用制限
CPRM	Content Protection for Recordable Media。録画された放送番組を DVD-R 等の記録媒体に１世代のみコピー可とする。CPRM 準拠の記録媒体には、媒体一枚ごとのメディア ID と記録媒体メーカごとの固有のデータである Media Key Block(MKB)が埋め込まれており、メディア ID と MKB によって暗号化鍵が作られ、中の映像が暗号化される。暗号化された映像は CPRM 対応の機器でなければ復号、再生することができない。また、他の記録媒体にコピーした場合、メディア ID と MKB はコピーできないため、復号できない。	暗号型のアクセス制限

略称	概要	分類
CSS	Content Scramble System。暗号技術を用いた DVD の技術的手段。DVD CSS が機器メーカに対し、再生機器が規格に従うことと鍵情報の秘匿を義務付ける。DVD の映像コンテンツは暗号化されており、復号鍵を持っている再生機器でしか復号、再生できない。	暗号型のアクセス制限
DTCP	Digital Transmission Content Protection。ホームネットワーク（家庭内 LAN）向けの暗号化方式。コンテンツを暗号化して IP ネットワーク上に送信することで、パケットの盗聴によるコンテンツの不正なコピー、及び、コンテンツの家庭内 LAN からインターネットなどの外部ネットワークへの流出を防ぐ。	暗号型のアクセス制限
FairPlay	マルティメディア技術 QuickTime をベースとする Apple 社のコンテンツ保護システム。ユーザーは、パソコンに iTunes をインストールし、iTunesStore にアクセスしてコンテンツの配信を受け、再生視聴等する。その際、配信サーバからダウンロードされるコンテンツはマスター鍵で暗号化されユーザーに送信される。また、マスター鍵がユーザー鍵で暗号化されて、Apple のサーバに DB 登録されるとともに、ユーザーに送信されユーザーのパソコンに登録される。iTunes は鍵 DB 登録されたユーザー鍵でマスター鍵を復号化した後、コンテンツを復号されたマスター鍵で復号化してユーザーに視聴可能にする。	暗号型のアクセス制限
HDCP	High-bandwidth Digital Content Protection system。映像コンテンツのコピー防止を目的として、映像再生機器とディスプレイ等の表示装置との間のデジタル信号の送受信経路を暗号化する。コンテンツを送出する再生機器が受信するディスプレイを認証し、公開鍵暗号によってコンテンツの暗号に使う鍵を共有する。鍵を用いて送出される映像データを暗号化し、伝送中に盗聴されたり改ざんされるのを防止する。暗号化されたコンテンツは、HDCP 非対応ディスプレイには表示されない。	暗号型のアクセス制限及びコピー等利用制限
HLS	HTTP Live Streaming。Apple 社が音声や動画のストリーミングを最適化するために開発した HTTP ベースのストリーミング・プロトコル。ストリーミングされるファイルを暗号化し、暗号化されたファイルをインターネットで送信して再生時に復号する暗号化の仕組みも規定されている。	暗号型のアクセス制限機能を有する通信プロトコル
Marlin	Marlin Developer Community（MDC）が策定した IPTV（インターネット接続テレビ）向け DRM 規格。ユーザー側のセットトップボックス（STB）がサーバ側に視聴を要求。要求メッセージには STB の識別情報（DRM-ID）が含まれている。サーバは DRM-ID でユーザーが登録済みの正規ユーザーであるかどうかを確認し、正規ユーザーに対してはデジタル証明書を発行。この証明書には暗号化された映像データを復号するための復号鍵が含まれている。続いて配信サーバは、暗号化された映像データを STB に配信する。暗号化された映像データは、正規ユーザーに配布した復号鍵だけでしか復号することができない。	暗号型のアクセス制限

略称	概要	分類
OpenMG	ソニーが開発した音楽コンテンツの DRM 規格。音楽コンテンツをPCに取り込む又はネットワークからダウンロードする際、音楽を暗号化した上でパソコンのハードディスク等の記憶媒体に記録。パソコンから視聴機器への転送（コピー）には専用のソフトウェアが必要で、1 世代に制限される。	暗号型アクセス制限及びコピー等利用制限
PlayReady	Microsoft 社が開発した配信システム。コンテンツ配信事業者は、Microsoft 社のライセンスを受けて、配信するコンテンツを暗号化した映像ファイルに変換した上でネットワーク伝送。デバイスのメーカは、Microsoft 社のライセンスを受けて規格に従ってクライアント・ソフトを開発し、デバイスに埋め込む。デバイスの利用者が暗号化された映像ファイルをダウンロードすると、認証情報をもとに復号が行われ、視聴が可能になる。復号による視聴のほか、その後の再生の期間制限やコピー制限等を合わせて規定することが可能。	暗号型のアクセス制限機能を有する配信システム コピー等利用制限機能の付加も可
RTMP	Real Time Messaging Protocol。Adobe 社が開発した Adobe Flash プレイヤーとサーバ間のストリーミング・プロトコル。映像コンテンツをストリーミングする配信事業者は、Adobe 社が提供するソフトで映像コンテンツを Flash VIdeo 形式に変換した後、Adobe 社独自の通信プロトコルである RTMP を暗号化した RTMPE で配信する。ユーザーは、Adobe 社の正規クライアント・ソフトでのみストリーミング視聴することができる。	暗号化することで暗号型のアクセス制限機能を有するストリーミング・プロトコル
SCMS	Serial Copy Management System。音楽 CD のコピーの可否、回数を制御するため、音楽 CD のデータに、コピー不可、コピー1 世代可、コピー無制限を設定する制御信号を付加し、対応する複製機器に相応の動作をさせる。	フラグ型のコピー等利用制限
Widevine	Google 社の暗号化技術。2010 年に Google 社が Widevine 社を買収したことで所有。Widevine 技術で暗号化された映像コンテンツを再生する際、プレイヤーの一部である Widevine クライアントが、ライセンス・プロキシー・ サーバを呼び出す。サーバは、コンテンツのライセンスの付与を判断した後、クライアントに提供される。クライアントは、ライセンスを使用して映像コンテンツを復号化する。	暗号型のアクセス制限
WMRM	Windows Media Rights Manager。Microsoft 社のダウンロード及びストリーミングにおける暗号化技術。Windows Media ファイルを暗号化したファイル形式（使用と配信に関するルールをヘッダーに追加した後、暗号化）に変換。鍵はライセンス内に格納され、ライセンスを要求したユーザーをライセンスサーバで認証した後、認証を経たユーザーに配布。ユーザーが復号化して再生。再生回数、転送可能なデバイスの制限、有効期限などを設定することが可能。	暗号型のアクセス制限 コピー等利用制限機能の付加も可

第Ⅰ章　コンテンツ保護の技術的手段の動向

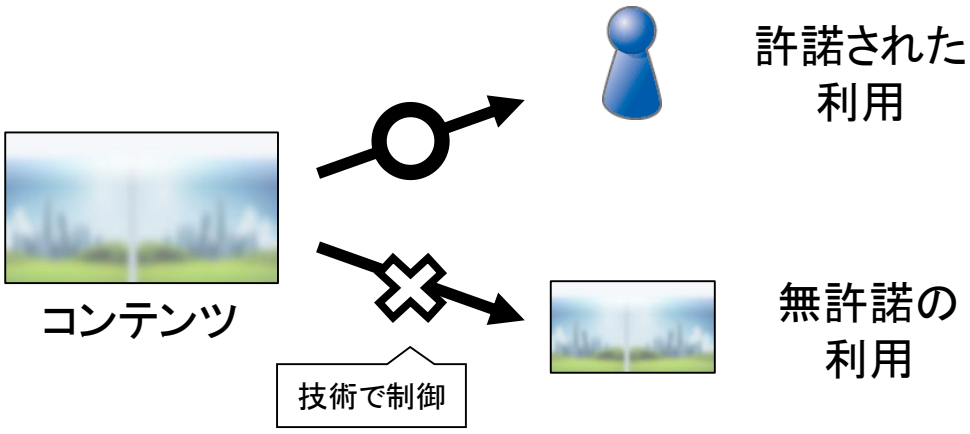
１　技術の概要

コンテンツ提供に係る技術的手段の概要として、コンテンツ保護の考え方、保護を実現するための技術、及び、その利用例について述べる。

１．１　コンテンツ保護の考え方

コンテンツの保護の考え方は、コンテンツのコピー等の利用をコントロールする「コピー等利用制限」と、コンテンツに対するアクセスそのものをコントロールする「アクセス制限」に大別し得る。以下に双方を図示する。

（１）コピー等利用制限



コピー等利用制限の例

コピー等利用制限は、ユーザーに許諾された利用は制限せず、許諾されていない利用を制限する。例えば、音楽や映像の視聴は許諾されているが、それ以外の利用が許諾されていないとき、無許諾の利用だけを制限する。具体的には、CD や DVD 等に用いられている複製制限、また複製の回数制限等がこれにあたる。

コンテンツ

○ or ×

技術で制御

許諾された
利用

アクセス制限の例

アクセス制限は、コンテンツを利用しようとするユーザーによるコンテンツに対する接触自体を制限する。

１．２　コンテンツ保護を実現するための技術

技術的制限を実現する技術は、コンテンツを暗号化して保護する暗号型とコンテンツ自体は暗号化せずに付加情報で保護する非暗号型の２種類に大別される。非暗号型は、さらに、コンテンツを利用する機器が信号を解釈して保護を実現する「フラグ型」と、コンテンツを利用する機器を誤動作させて保護を実現する「エラー惹起型」に分類される。

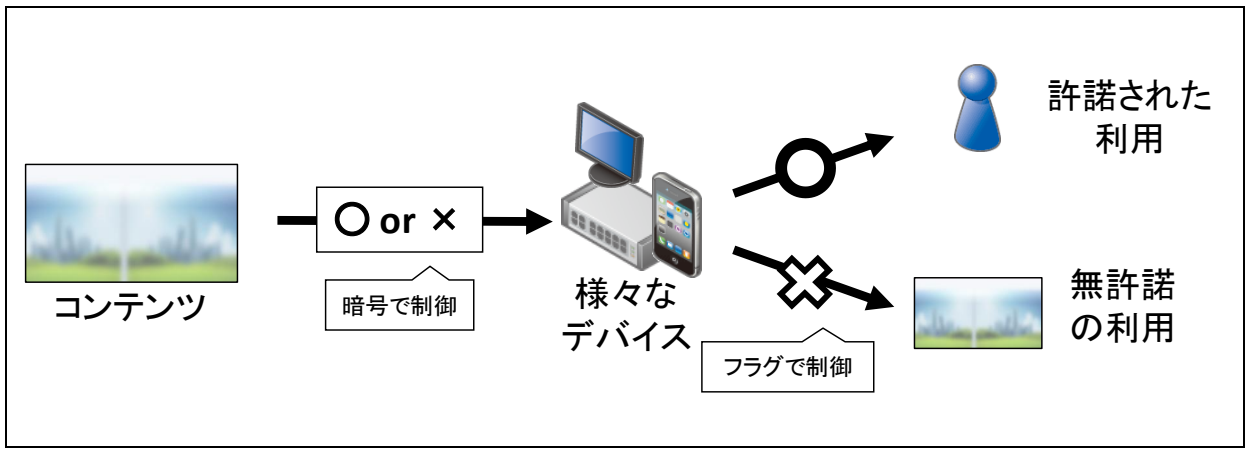
分類		対象例	保護されるものの例	具体的な技術例
暗号型		記録媒体用	DVD、Blu-ray	CSS CPRM AACS
		機器間伝送路用	ホームネットワーク （家庭内LAN）	DTCP HDCP
		放送用	有料放送	B-CAS方式 C-CAS方式
			地上波限定	ソフトウエアキャス
		インターネット配信	ダウンロード ストリーミング	WindowsMedhiaDRM Playready Fairplay Widevina Marlin
非暗号型	フラグ型	記録媒体用	DVD、VHS、CD、MD	CGMS
			DCC、DAT	SCMS
	エラー惹起型	記録媒体用	CD	CCCD

また、ビジネスソフト等の特定のコンテンツの提供においては、コンテンツを利用しようとする者が当該コンテンツに係る利用権原を有する者か否かの確認をする認証技術も用いられている。認証技術は、ID・パスワード、シリアルキー等の識別符号等の入力や照合等を要求することによって、利用しようとする者や利用するデバイスが当該コンテンツの利用権原を有しているか否かの認証を行い、利用権原を有することが確認されれば、制限の解除を行う。

１．３　コンテンツ保護の最近の傾向

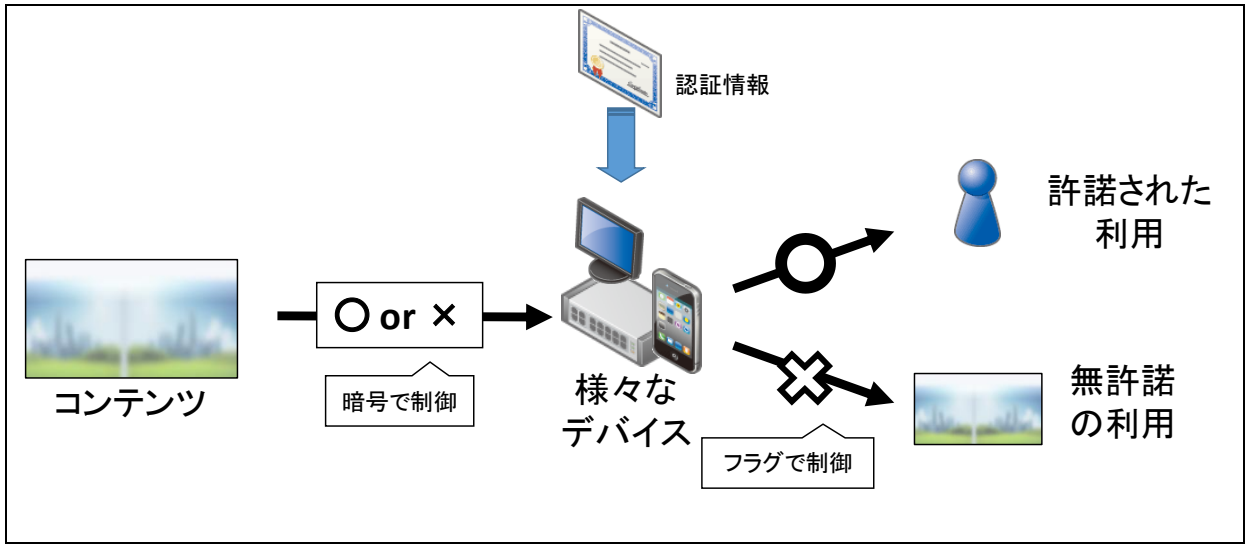
最近の傾向として、コピー等利用制限やアクセス制限といった手法や、暗号型や非暗号型といった技術は、いずれか一方を利用することは少なく、二つの手法と技術を組み合わせて利用している。

①暗号型技術によるアクセス制限と非暗号型技術によるコピー等利用制限を組合せた例



①の例では、コンテンツは暗号技術を用いてアクセス制限の手法で保護されデバイスに読み込まれており、アクセス制限の解除ができることをきっかけとして、非暗号型の技術であるフラグを用いてコピー等利用制限が行われ、初めて視聴等の利用ができるようになる。

②アクセス制限とコピー等利用制限に、さらに認証技術を組合せた例



さらに、最近のネットワーク経由のコンテンツ提供においては、上図のように、認証情報を組み合わせる場合がある。

認証技術の利用により、コンテンツを利用しようとする者が正規の購入者であるか否かの認証、当該利用者が有する利用権原の内容（利用可能な期間、利用可能な機能、利用可能なデバイス及びその台数等）を認証することができる。

２　コンテンツ分野別及び流通形態別の技術的手段

コンテンツの分野ごとに、現在、利用されている主な保護技術とその状況について以下にまとめる。

分野 流通手段	音楽	映像	ゲーム	電子書籍	ビジネスソフト
パッケージ(CD、DVD、Blu-Ray、ニンテンドーDS カードなど)	無し（2002 年から 2004 年までは CCCD を利用)	CSS AACS	ハードウェアによるメーカ独自の技術的手段	無し	認証によるメーカ独自の技術的手段
放送	-	B-CAS C-CAS CPRM	-	-	-
ダウンロード	・フィーチャーフォン[1]向けにはフラグ型のキャリア独自の技術的手段 ・PC、スマートフォン向けは保護無し（2012 頃までは FairPlay 等の技術的手段を利用）	FairPlay、PlayReady、Widevine 等（DECE[2]対応の技術的手段）	認証によるメーカ独自の技術的手段	各電子書店の独自の技術的手段	認証によるメーカ独自の技術的手段
ストリーミング	・HLS での通信経路の暗号化 ・FairPlay ・サービス独自の技術的手段など	・RTMPE による通信経路の暗号化 ・PlayReady や Widevin などの DECE 対応技術的手段	-	-	（クラウド型提供の場合）認証を用いたメーカ独自の技術的手段

1 携帯電話の端末の中で通話以外の機能を有する端末。スマートフォンほど高機能ではないものを指すことが多いことから、本報告書においてもスマートフォンを除く用語として使用する。

2 Digital Entertainment Content Ecosystem.。ハリウッドのスタジオ、家電メーカ、IT 企業、通信機器メーカの 60 社が参加して、2008 年に発足した米国の法人。インターネットによる動画配信に利用するファイル形式の標準仕様を策定し、2011 年よりライセンスしている。

３　音楽コンテンツに係る技術的手段

音楽コンテンツにおいては、2002 年から 2004 年にかけて CD にエラー惹起型のコピー等利用制限技術を施した CCCD（Copy Controlled Compact Disc）を販売したが、現在、CD には技術的手段を施していない。また、ダウンロードについても、フィーチャーフォン向けダウンロードサービスにおいてはキャリア（携帯電話会社）[3]独自仕様の技術的手段が施されているが、PC やスマートフォン向けダウンロードサービスにおいては一般に技術的手段を利用していない。ユーザーの利便性を妨げないことを理由として、技術的手段は施さない方向に進んでいる。

ただし、サブスクリプション型[4]ストリーミングサービスにおいては、契約期間や利用条件ごとにコピー等利用制限やアクセス制限が必要であるため、Apple の FairPlay や HLS と端末での暗号化を組み合わせた技術的制限が施されている。

３．１　パッケージ

３．１．１　主な技術的手段

現状、国内の音楽パッケージ流通の形態は CD が主流であるが、CD には技術的手段はかけられていない。

３．１．２　回避・無効化の実態

CD は技術的手段がかけられていないため、回避・無効化も行われていない。

３．１．３　経過、現状及び課題

2002 年から、音楽 CD から PC へのリッピング[5]を防止するため、CCCD が発売された。CCCD には、一般の CD 再生機器で再生する通常の音声データと、PC 上で再生する音声データ及びその専用再生ソフトウェアが記録され、このうち通常の音声データは、PC 上では再生できない仕組みであった。ところが、特定の CD 再生機器で CCCD を再生することができない事態が生じたりするなど、専用再生ソフトウェアが不具合を起こしたりした。また、発売当初から、一定の技術知識があるユーザーであれば当該技術的手段を回避・無効化してリッピングすることができてしまっていた。このため、レコード製作者は 2004 年以降、次々に CCCD の新規発売を取りやめることとなった。その後、CD に対して技術的手段は施されていない状況である。

---

[3] NTT ドコモ、KDDI グループ、ソフトバンクグループがあり、独自にコンテンツを提供している。

[4] 利用するコンテンツの数に応じた料金ではなく、一定期間ごとに定額料金を支払う方式のサービスをいう。

[5] 音楽 CD や映像 DVD 等の記録媒体から、データを抜き取ること。

３．２　ダウンロード

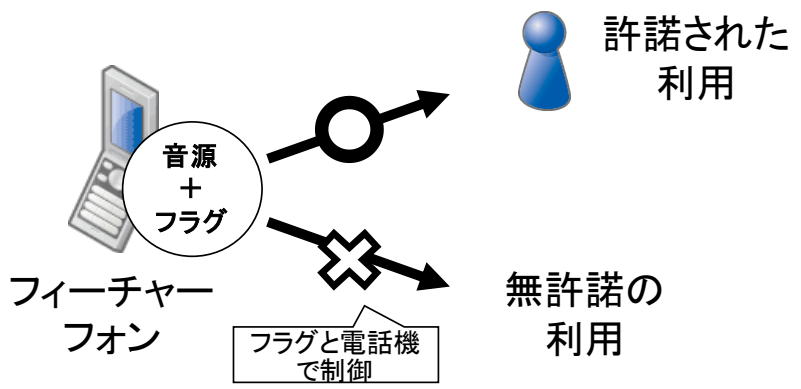
３．２．１　主な技術的手段

現在、音楽のダウンロード販売には、以下のような形態が存在する。

①フィーチャーフォン向けのダウンロード販売（着メロ、着うた等）

②スマートフォン、PC 向けのダウンロード販売（iTunes、Mora など）

このうち、①「フィーチャーフォン向けのダウンロード販売（着メロ、着うた等）」については、音声ファイルの一部にコピー制限の情報を持たせておき、電話機側でその情報を読みこんで再生期限や転送の制限を実現している。これらはフィーチャーフォン向けの音声ファイルの規格によるもので、通信キャリアとフィーチャーフォンメーカーの独自の仕様である。以下に利用の形態を図示する。



フィーチャーフォンにおいて用いられる技術的手段の概要

このように、フィーチャーフォンの例では音源ファイルに付着したフラグによってコピー等利用制限をしており、「非暗号型のフラグ型技術による利用制限」が実装されている状況である。

これに対して、現在主流の利用形態である「スマートフォンや PC 向けのダウンロード販売（iTunes、Mora など）」では、ダウンロードまでの仕組みには認証技術が利用されているが、正規にダウンロードされた後のコンテンツには、現状、技術的手段はかけられていない。

例えば、Apple の iTunes におけるダウンロードまでの仕組みは、ユーザーが PC に iTunes をインストールし、iTunesStore にアクセスしてコンテンツの配信を受け、再生視聴するというものである。ここでは最初にユーザーが音楽コンテンツ購入のため配信サーバにアクセスすると、配信サーバがユーザーのソフトが iTunes であるかを認証する。有料ダウンロードに関しては、購入申し出の段階でクレジットカード等での課金が行われる。課金後に配信サーバからダウンロードされる音楽コンテンツは、マスター鍵で暗号化されユーザーに送信されてくる。また、マスター鍵はユーザー鍵で暗号化されて、Apple の配信サーバのデータベースに登録されるとともに、ユー

ザーに送信され、ユーザーの PC に登録される。iTunes は鍵データベースに登録されたユーザー鍵で最初にマスター鍵を復号化した後、次に復号されたマスター鍵を使って音楽コンテンツを復号化してユーザーが視聴可能な状態にする。

３．２．２　回避・無効化の実態

ヒアリングではフィーチャーフォン向けで用いられている制限を回避・無効化されたことはないとの見解が聞かれたが、ネット上ではバイナリエディタ[6]を用いた制限の回避・無効化の方法を紹介するサイトが存在することから、回避・無効化が行われているおそれはある。

スマートフォン、PC 向けのダウンロードサービスにおいては、技術的手段が施されていないため、回避・無効化の実態もない。

３．２．３　経過、現状及び課題

フィーチャーフォン向けダウンロードサービスの技術的手段は、着メロ、着うたの開始時から一貫してキャリアの独自仕様で行われている。なお、現状、着メロ・着うたの利用が減少傾向にあるため、技術的手段の回避・無効化は大きな問題になっていない。

スマートフォンや PC 向けのダウンロードサービスでは、iTunes では Apple の FairPlayDRM、Mora では SONY の OpenMG[7]による暗号化を利用した ATRAC[8]音声データ等の技術的手段を用いていたが、2012 年頃からこうした技術的手段はかけないようになっている。背景には、ユーザーが正規に購入したコンテンツを自分の複数の機器間で自由に視聴することができないことに関する議論のほか、技術的手段の実装にかかるコストの問題があり、配信事業者と著作権者との合意の下で技術的手段を外していく動きになっていった。

前提として、音楽は放送やパッケージ販売をした時点で音源をファイル化され、それらがインターネット上で無許諾アップロード、共有されてしまっている実態がある。この海賊版による被害の方が正規購入されたファイルの複製より圧倒的に被害や影響が大きく、こちらの方が音楽業界としては悩みが大きいとの意見があった。

---

6 ファイルのフォーマットに関わりなく、ファイルの生データを表示・編集することを可能とするプログラム。

7 パソコンに音声データを取り込む又はネットワーク上から音声データをダウンロードする際、音声データを暗号化した上でハードディスク等の記憶媒体に記録する技術。ソニーが開発。

8 Adaptive TRansform Acoustic Coding の略。ソニーが開発した音声データ圧縮技術。

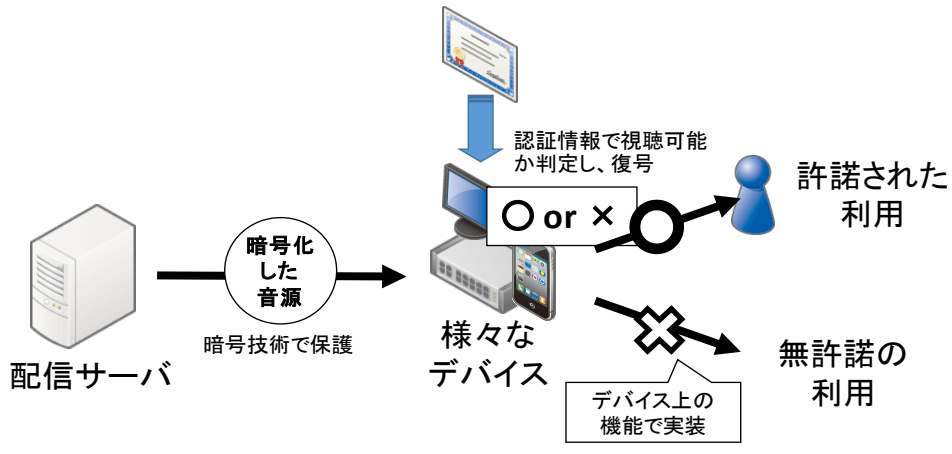
３．３　ストリーミング

３．３．１　主な技術的手段

音楽のストリーミングサービスでは、認証されたユーザーアカウントごとに一定期間楽曲をどれだけストリーミングしても定額という、サブスクリプション型のサービスが一般的である。あるストリーミングサービス事業者は、HLS（HTTP Live Streaming）[9]を用いてインターネット上を流れるコンテンツデータを暗号化した上で通信し、ユーザー側の端末上では別の仕組みでキャッシュが行われると同時に、オフライン再生用のコンテンツファイルの暗号化と期間制限を実装し、アカウントごとのアクセス制限（期間制限等）と複製の制限を実現している。

著名なサブスクリプションサービスである AppleMusic は FairPlay DRM をかけており、暗号化とアカウントに紐づいたアクセス制限（期間制限等）とオフライン再生用データの複製制限[10]が実現されている。日本では開始されていないが、最大手のサブスクリプションサービスである Spotify にも、オフライン再生機能[11]がある。この機能を利用するためには 30 日に 1 度はインターネットに接続する必要があり、接続の際に会員資格が失効していると、ダウンロードしたデータの再生が制限されるという仕組みであると考えられる。会員資格が失効していなければ、技術的手段が施されたオフラインデータがダウンロードされる（技術の詳細は公表されていない）。

このように、ストリーミングサービスの場合はストリーミング自体を保護する目的ではなく、サブスクリプションというアカウントに紐づけて利用期間を制限する必要があるため、技術的手段を用いることが一般的となっていると考えられる。以下に利用の形態を図示する。



ストリーミングサービスにおいて用いられる技術的手段の概要

9　音声や動画のストリーミングを最適化するために Apple によって開発された HTTP ベースのストリーミング・プロトコル。ストリーミングされるファイルを暗号化し、暗号化されたファイルをインターネットで送信して再生時に復号する暗号化の仕組みも規定されている。

10　AppleMusic の期間制限(https://support.apple.com/ja-jp/HT204962)

11　Spotify オフライン再生について(https://support.spotify.com/is/learn-more/guides/#!/article/Listen-offline)

サブスクリプションでのストリーミングサービスの例では、音源を暗号化した上でネットワーク上で伝送し、認証情報をもとに復号が行われ、視聴が可能になる。復号後もオフライン再生の期間制限やコピー制限などが実装されているため、「暗号型技術に認証技術を加えたアクセス制限、及び、端末でのアクセス制限の解除をきっかけとしたコピー等利用制限」が実装されている状況である。

３．３．２　回避・無効化の実態

ストリーミングサービス事業者へのヒアリングでは、HLS による暗号化と端末側の制限に対する回避・無効化の実例は報告されなかった。ただし、一部サービスについては、技術的手段の解除方法、ツールがネット上に確認される。

３．３．３　経過、現状及び課題

日本国内では、サブスクリプション型の音楽ストリーミングサービスが本格的に開始されてからまだ 1 年程度であるが、現時点において、技術的手段の回避・無効化の実態は確認されていない。また、ストリーミングサービス事業者は、セキュリティよりユーザーの使い勝手を重視しており、技術的手段を強化する状況にはなっていない。

海外で提供されている一部のストリーミングサービスの状況を調査したところ、技術的手段を回避・無効化して楽曲を PC に保存するという複数の事例があった[12]が、あまり活発に回避・無効化が行われている状況ではないようである。

音楽については前述の海賊版の問題が大きく、技術的手段を回避・無効化してまで楽曲を得る必要がないことが理由として考えられる。無料音楽聞き放題の違法な海賊版サイトに対する規制や、如何に利便性を高くした有償サービスを提供するか[13]、という点が課題である。

４　映像コンテンツに係る技術的手段

映像コンテンツにおいては、パッケージには CSS、AACS 等の記録媒体用の暗号技術が、機器間の伝送路には DTCP や HDCP 等の暗号技術がそれぞれ施されている。また、放送には、B-CAS、C-CAS 方式の暗号化によるアクセス制限と機器によるコピー等利用制限がかかっている。

パッケージ、放送ともに技術的手段を回避・無効化する手段が存在し、実際に回避・無効化された事例も散見される。

12　PANDA chomps through Spotify's DRM(http://www.theregister.co.uk/2014/07/04/spotify_drm_broken/)

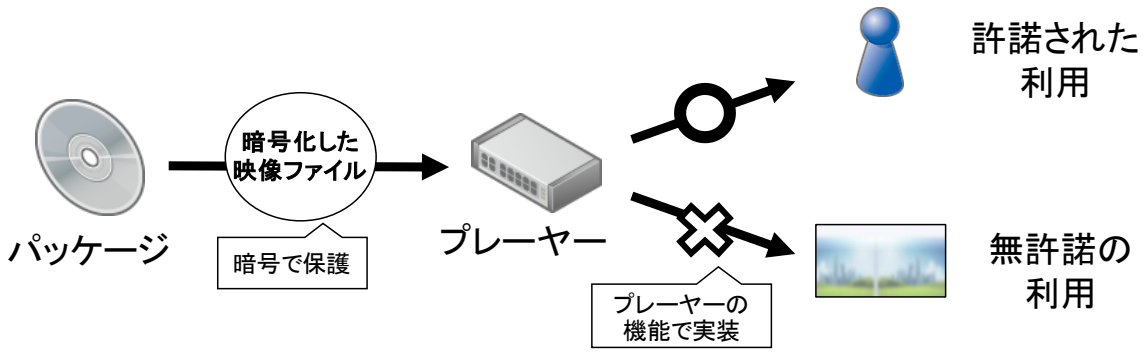
13　Spotify は違法ダウンロードよりも便利(http://www.musicman-net.com/SPPJ01/06.html)

ダウンロードとストリーミングにおいては、コンテンツによって PlayReady や Widevine など DECE 対応の技術的手段がかかっているものから、Adobe 社の RTMPE などによる通信経路中の暗号化[14]のみをかけているものなどがある。これらの保護については技術的な興味や功名のために技術的手段を回避・無効化する試みはみられるものの、一次流通元である放送や、二次流通であるパッケージの技術的手段を回避・無効化する方が簡便であるためか、あまり積極的には行われてはいない。

４．１　パッケージ

４．１．１　主な技術的手段

現状、日本国内の映像コンテンツのパッケージ流通の主体は DVD と Blu-ray ディスクである。現在、DVD については CSS という規格に基づいて暗号化による保護が行われている。Blu-ray については AACS という規格に基づいて暗号化による保護が行われている。CSS と AACS についてはそれぞれの技術のライセンサーである DVD CCA と AACS LA が規格を定め、規格に準拠した形で出力やコピーを制御したハードウェア機器のベンダーがライセンスを取得して復号し、コピー等利用制限をかけて再生されることを意図した技術である。また、一部の Blu-ray ディスクは AACS に加え、別途 Cinavia という電子透かし技術を利用した保護も施されている場合がある。Cinavia は、不正にコピーされた Blu-ray ディスクを再生すると、再生機器が、音声に埋め込まれた電子透かしに格納された情報から不正利用であることを検知し、再生を停止したり音声をミュートしたりすることができる技術で、非暗号型・フラグ型のコピー等利用制限技術である。以下に利用の形態を図示する。



CSS、AACS において用いられる技術的手段の概要

14 Real Time Messaging Protocol。Adobe 社が開発した Adobe Flash プレイヤーとサーバ間のストリーミング・プロトコル。映像コンテンツをストリーミングする配信事業者は、Adobe 社が提供するソフトで映像コンテンツを Flash VIdeo 形式に変換した後、Adobe 社独自の通信プロトコルである RTMP を暗号化した RTMPE で配信する。ユーザーは、Adobe 社の正規クライアント・ソフトでのみストリーミング視聴することができる。

このように、映像のパッケージの例では、映像は暗号化されており、暗号を解くことができるライセンスを受けたプレイヤーによって復号が行われて、視聴が可能になる。暗号を解くことができるライセンスを得るには、復号後のコピー等制限を実装する必要がある。「暗号型技術によるアクセス制限及び、アクセス制限の解除をきっかけとしたコピー等利用制限」が実装されている。さらに、上述の通り、一部の Blu-ray ディスクには、Cinavia による「非暗号型・フラグ型によるコピー等利用制限」も施されている。

４．１．２　回避・無効化の実態

CSS と AACS については、PC 上で動作する多くの技術的手段の回避・無効化ソフト（リッピング・ソフトウェア）が存在し、パッケージ上のデータに施された暗号を復号した上で、コピー等利用制限がかかっていない映像データとして保存することができる状況である。また、回避・無効化ソフトを用いて作成された映像データが、海賊版として多く出回っていると考えられる。

４．１．３　経過、現状及び課題

CSS は 1996 年に商用利用が開始された。しかし、1999 年に CSS のライセンスを受けていない LinuxOS 上で DVD を閲覧するためのソフトウェアとして、CSS の暗号による保護を回避・無効化する DeCSS が発表された。DeCSS はその後、CSS を回避・無効化する技術として様々なソフトウェアに搭載されたため、CSS の管理団体である DVD CCA が、これらのソフトウェアの作者を提訴するに至った[15]。

AACS は、CSS での復号鍵の漏えいを踏まえ、鍵の期限設定と更新の機能を実装した。しかし、更新される鍵を、リッピング・ソフトウェア側が追随するという、いたちごっこが続いている状況である。

日本国内においては 2012 年の著作権法改正により、第 2 条第 1 項第 20 号において、技術的保護手段の対象に、「著作物等の利用に用いられる機器が特定の変換を必要とするよう著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像を変換して記録媒体に記録し、又は送信する方式（暗号方式）」を加えることとされた。

また、第 30 条第 1 項第 2 号において、技術的保護手段の回避に係る定義に、「特定の変換を必要するよう変換された著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像の復元」を加えることされた。

このことにより、私的使用目的であっても、暗号方式による技術的保護手段の回避により可能となった複製を、その事実を知りながら行う場合には、民事上違法となることとされた。

なお、暗号方式による技術的保護手段には、具体的には、現在 DVD に用いられている CSS や

---

15 なお、訴訟は取り下げられた。『「DeCSS」公開を巡る訴訟が取り下げ』(http://japan.cnet.com/news/media/20063867/)

Blu-ray に用いられている AACS が該当する。

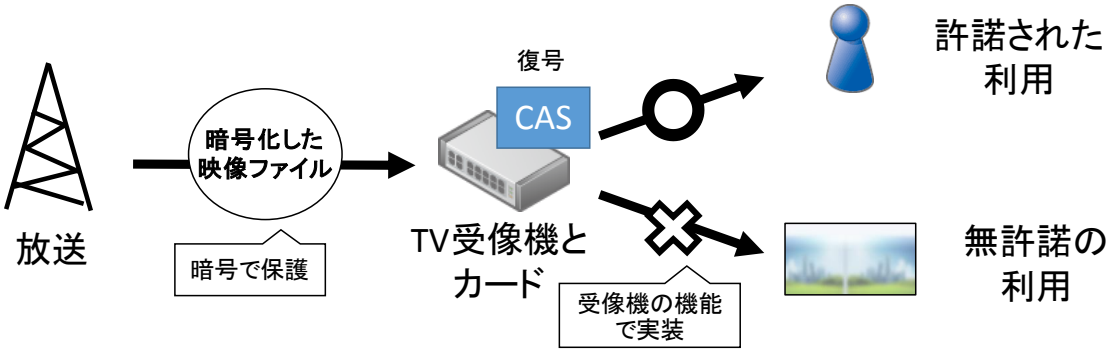
４．２　放送

４．２．１　主な技術的手段

現在の地上波デジタル放送には、B-CAS という暗号技術による保護がかかっている。B-CAS は B-CAS 社が規格を定め、一般社団法人電波産業会（ARIB）が定めたデジタル放送運用規定を順守した受像機メーカにライセンスする技術である。受像機にカードを差し込み、該当カードに記載されたユーザー識別情報に対して復号鍵を放送波に載せて配信し、カード側に記録することで復号を行う。B-CAS カードには複数の放送事業者の復号鍵と著作権管理情報を保存することができるため、地上波デジタル放送に加え、BS 放送、CS 放送、ケーブルテレビでも利用されており、日本国内の放送における保護技術としては事実上の標準規格となっている。

放送番組の録画については、録画機器ごとの形式で放送コンテンツの暗号化が行われ、コピー等利用制限を実装している。そのため、データ自体を複製し、他の録画機器に転送したとしても、転送先の機器では再生ができない（メーカごとに技術が異なり、その方式は公開されていない）。

以下に利用の形態を図示する。



放送番組において用いられる技術的手段の概要

このように、放送の例では、映像は暗号化されており、暗号を解くことができるライセンスを受けた TV 受像機と B-CAS や C-CAS のカードによって復号が行われて視聴が可能になる。

また、録画された放送番組が無制限に DVD-R 等の記録媒体にコピーされるのを防ぐため、CPRM という方式に準拠した記録媒体に 1 世代しかコピーできないようにしている。また、その再生にあたっては CPRM 対応の機器が必要になる。CPRM 準拠の記録媒体には、媒体一枚ごとのメディア ID と記録媒体メーカごとの固有のデータである Media Key Block(MKB)が埋め込まれており、メディア ID と MKB によって暗号化鍵が作られ、中の映像が暗号化される。CPRM 対応の機器でなければ、復号することができない。また、他の記録媒体にコピーしたとしても、メディ

ア ID と MKB がコピーできないため、復号することができない。

４．２．２　回避・無効化の実態

B-CAS によるアクセス制限を回避・無効化する方法は複数存在する。

一つは市販のカードライターを用いて B-CAS カードに書き込まれた情報を改ざん[16]し、有効期限などの制限を変更する方法である。カード内部の情報を改ざんすると、通常の受像機で有料放送を契約無く無料で視聴することが可能となる。改ざんカードを販売する事業者も存在する。保護された放送データを保護の無いファイルに保存する方法としては、また、通称 TS 抜きと呼ばれる方法がある。この方法は、保護規定に準拠していないチューナーと正規の B-CAS カードを用いて、伝送されてきた暗号化された放送データ（MPEG2-TS 形式）を復号し、PC 等に保護のかかっていないファイルとして保存してしまう方法である。

また、録画された放送番組の記録媒体へのコピーを防止する CPRM についても、解除ソフトウェアが存在する状況である。

４．２．３　経過、現状及び課題

B-CAS は、復号鍵情報を更新することによって、不正に改造された B-CAS カードを無効化することが可能である。このため、過去に何度か鍵情報の更新が行われているようである（正式に公開された情報は無い）。しかし、更新の度に、鍵情報の探索と解読を行う者があらわれ、更新と解読のいたちごっこの状況である。

不正 B-CAS カードの販売者については、刑事罰が言い渡された事案が幾つか存在する。

2013 年 3 月には全国の地上テレビ放送局でコンテンツ権利保護専用方式[17]が開始された。コンテンツ権利保護専用方式は、地上デジタル放送のコンテンツ保護専用の方式で、ARIB 標準規格（STD-B25 第 3 部）を方式のベースとしている。この方式では、放送局が、放送波にコピー制御の信号を付加して放送コンテンツを暗号化することは、B-CAS 方式と同様であるが、コピー制御の機能を備える受像機メーカに対して、鍵データの発行と技術情報の開示を行うため、B-CAS 方式のような物理的なカードが不要となっており、多様なデジタル受像機ニーズへの対応が容易になることによる視聴者の選択肢拡大と利便性向上を目的としている（地上波デジタル放送を行う放送局は、B-CAS 方式の情報に加えて、コンテンツ権利保護専用方式の情報を放送波に多重して伝送し、受像機メーカでは、商品の企画や形態等に応じて、どちらかの仕組みを選択することが可能となっている）。

16 不正改ざんカードについて(https://www.b-cas.co.jp/support/faq/#category07)

17 コンテンツ権利保護方式(https://www.trmp.or.jp/new_method/)

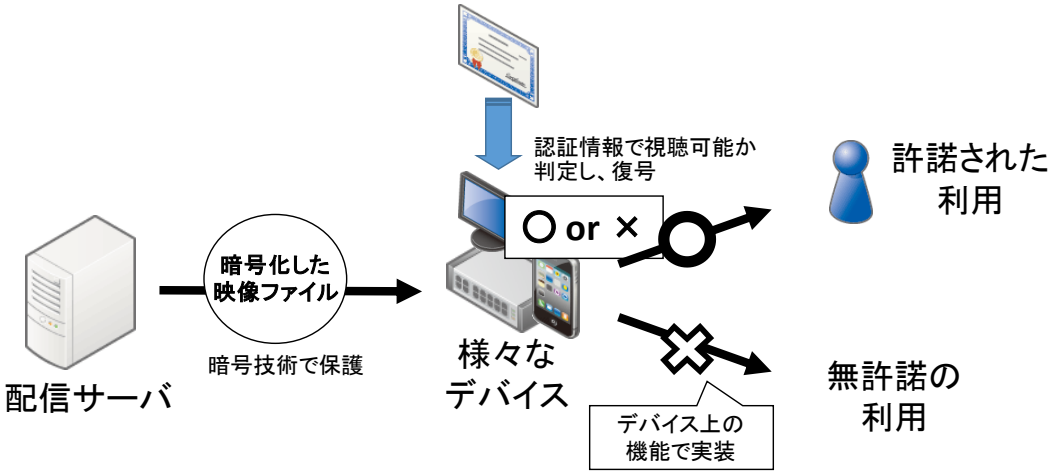
なお、B-CAS 方式のように、地上デジタル放送のみに対応した仕組みであるため、衛星放送などについては、これまで通り B-CAS 方式が利用される。

４．３　ダウンロード

４．３．１　主な技術的手段

Apple の iTunes は、独自の技術的手段である FairPlay を使っている。他の映像配信事業者は、Microsoft の PlayReady などアメリカの映画業界が定めた DECE（Digital Entertainment Content Ecosystem）に準拠した標準的な技術的手段を使っている。

配信事業者は、多様なデバイスに対応するため、及び、コンテンツホルダーの要請にこたえるため、業界標準の技術的手段をかける必要があるとの話がヒアリングでは聞かれた。以下に利用の形態を示す。



映像コンテンツのダウンロード販売において用いられる技術的手段の概要

例えば PlayReady を利用する配信事業者は、Microsoft 社のライセンスを受けて、配信するコンテンツを暗号化した映像ファイルに変換した上でネットワーク伝送する。デバイスのメーカは、Microsoft 社のライセンスを受けて規格に従ってクライアント・ソフトを開発し、デバイスに埋め込ませる。デバイスの利用者が暗号化された映像ファイルをダウンロードすると、認証情報をもとに復号が行われて、視聴が可能になる。なお、PlayReady は、復号による視聴のほか、その後の再生の期間制限やコピー制限なども規定することができる。

したがって、「暗号型技術に認証技術を加えたアクセス制限、及び、アクセス制限の解除をきっかけとしたコピー等利用制限」が実装されているということができる。

４．３．２　回避・無効化の実態

ダウンロードサービスでは、DECE 基準に対応している技術的手段では回避・無効化の実態はなかったが、ネット上の情報では一部の技術的手段については回避・無効化がされている状況が見られる。

４．３．３　経過、現状及び課題

ダウンロード販売で利用されている技術的手段について、公開されている情報を調査したところ、以前は WindowsMedia RightsManagement（WMRM）[18]を用いたサービスが多かったが、解除されたため、現在は WMRM を使っているサービスは少ない。

現在は、PlayReady、FairPlay が多く使われている。

４．４　ストリーミング

４．４．１　主な技術的手段

現状、映像配信のストリーミングサービスには、PPV（Pay per view）型、サブスクリプション型、無料配信型がある。一部のサブスクリプションサービスは技術的手段で保護されたファイルをダウンロードし、一定期間内は視聴できるオフライン再生と呼ばれる視聴形態も提供している。

これらのうち、ハリウッド作品を扱うサービスの場合、DECE 対応の PlayReady、Marlin と Adobe Primetime といった技術的手段が用いられている。IPTV[19]と呼ばれるテレビデバイス向けの配信には国内で開発された Marlin という規格が使われているが、国内テレビ局のインターネット向けオンデマンドサービスは伝送路中の暗号化のみを行う RTMPE を使い、暗号技術によるアクセス制限のみを行っているところが多い[20]。多くのサービスでは各種のデバイスに対応するために複数の技術を併用しているようである。

利用の形態としては映像ダウンロードサービスとほぼ同じであり、「暗号型技術に認証技術を加えたアクセス制限及び、アクセス制限の解除をきっかけとしたコピー等利用制限」が実装されている。

---

18 Windows Media Rights Manager。Windows Media ファイルを暗号化したファイル形式に変換することで、音楽や映像コンテンツのダウンロードやストリーミングの安全を図る。

19 IPTV フォーラムが定めた技術規格に従って、LAN ケーブルなどを使って IP 方式で提供されるサービス（アンテナケーブルを使って RF（電波）方式で提供されるサービスは含まない）

20 各サービスの利用技術(http://www.slideshare.net/otachan/140123-html5j-tvbudrm P.5)、

アクトビラの DRM (http://av.watch.impress.co.jp/docs/news/20150715_711856.html)

４．４．２　回避・無効化の実態

現在ストリーミングサービスで配信されるコンテンツは過去に放送されたものの二次利用のものが多く、すでに高画質の海賊版が出回っている場合がある。このため、ストリーミングから技術的手段を外すモチベーションが少ないためか、回避・無効化の実態はないようである。今後ストリーミングが一次公開となる映像作品が増えれば、回避・無効化が問題になると考えられる。

４．４．３　経過、現状及び課題

ダウンロードと同様に以前の WMRM は回避・無効化されていた。アナログキャプチャや違法コピーの問題があるため、ある程度までしか対応できないという反応があった。

多くの配信事業者はコンテンツホルダーの要望に応じて、暗号化や商用の DECE 基準の技術的手段を導入している。独自仕様の暗号技術ではコンテンツホルダーの許諾が得られにくいようである。

現状は Microsoft 社の PlayReady が大きなシェアを持っている。ただし、配信事業者は Windows だけでなく Android や STB[21]など多様なデバイスのセキュリティを確保するために複数のプラットフォームで動作できる技術に対応する必要がある。これにより用意するファイルの種類が増えてコストが増える可能性もあるが、昨今では技術的手段にかかる費用が廉価になっている例もある。Widevine や FairPlay は無償や低コストで提供されるようであり、今後 iOS は FairPlay、アンドロイドでは Widevine の利用が増えていく流れがある。

５　ゲームソフトに係る技術的手段

ゲームソフトは、インターネットを介さずにプレイする従前からのコンピュータゲーム（以下、「コンピュータゲーム（オンラインゲームを除く）」）と、インターネットを介してプレイするオンラインゲーム（以下、「オンラインゲーム」）とに大別される。

コンピュータゲーム（オンラインゲームを除く）においては、ソフトはパッケージの店頭販売・通信販売、及び、オンラインでのダウンロードによって提供され、データはユーザーの端末に置かれる。

オンラインゲームにおいては、ソフトはオンラインでのダウンロード提供、ブラウザ提供（WEB アプリ）[22]、ストリーミング提供（クラウドゲーム）[23]され、データは、運営サーバとユーザーの

---

21 Set-Top Box。テレビ受像機に接続して使用する電子機器の一つで、衛星放送やケーブルテレビ放送などの放送信号を受信して、一般のテレビで視聴可能な信号に変換する装置

22 ソフトがユーザーの端末にインストールされることはなく、インターネットに接続してゲームの内容をブラウザ上に表示して動作させる。データは、ゲーム運営サーバとユーザーの端末に置かれる。なお、現時点において、スマートフォンでは、ダウンロード（ネイティブアプリ）形式と、ブラウザ（WEB アプリ）形式の両者が共存している

23 ソフトはユーザーの端末にインストールすることなく、ゲーム運営者のサーバに置かれる。。

端末の両方に置かれる場合と、運営サーバのみに置かれる場合とがある。

（1）コンピュータゲーム（オンラインゲームを除く）における技術的手段

利用端末は、専用ゲーム機[24]、パソコン、モバイル[25]に分かれており、各々における技術的手段は概略以下の通りである。

専用ゲーム機の場合、同機に実装されている技術的手段により不正行為を防止する。

パソコンの場合は、ゲームソフト側に動的解析及び静的解析[26]を防ぐ仕組みを実装する場合や、１ユーザーあたりの利用可能台数を制限する技術を利用する場合がある。

モバイルのうちフィーチャーフォンを端末とする場合は、携帯電話通信サービス会社（キャリア）指定の技術的手段を施す。スマートフォンを端末とする場合は、ゲームソフト提供者が上述パソコンを端末とする場合と同様、動的及び静的解析対策の仕組みを実装する場合がある[27]。

（2）オンラインゲームにおける技術的手段

オンラインゲームでは、サーバへの不正なアクセスを制限するため、ID・パスワード等による認証を行う。

また、ユーザーによるデータの書き換えを防ぐため、ユーザーの端末にあるデータの動的及び静的解析を防ぐ仕組みを実装しているものや、運営サーバとユーザー端末との間の通信を暗号化しているものがある。

また、認証を経てアクセスしたプレイヤーの振る舞いは、目視等により監視する。

５．１　コンピュータゲーム（オンラインゲームを除く）

５．１．１　主な技術的手段

（1）専用ゲーム機を利用端末とする場合

技術的手段はハードウェア側の機能で実現しており、ソフトウェア側からはかけていない。技術はハードウェアごとに異なると言われているが、ゲーム機メーカがその仕様を公表していないため、詳細は不明である。以下に、利用の形態を示す。

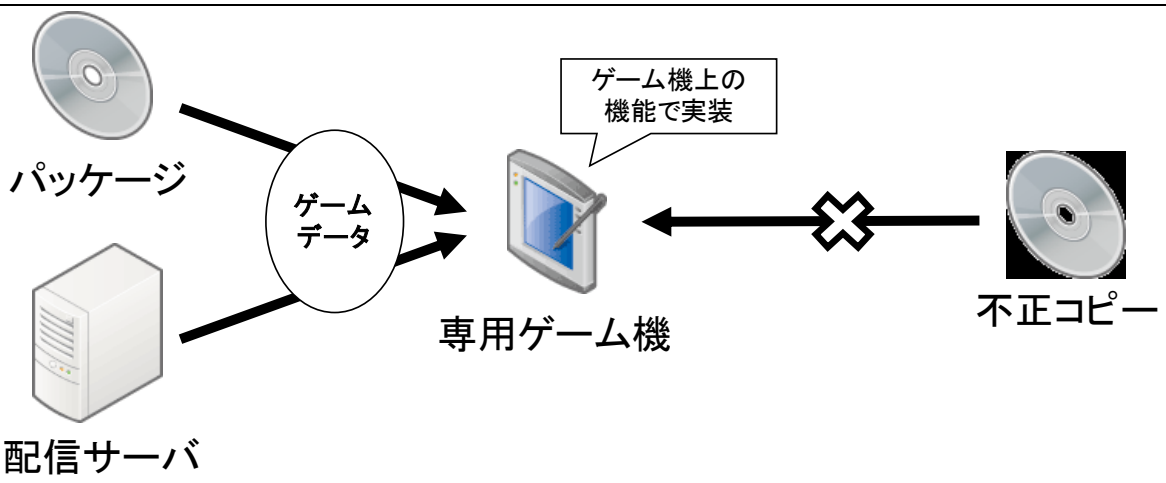
---

24 PlayStation、Wii、Xbox 等の据置型、及び、PlayStationPortable、ニンテンドー3D 等の携帯型がある。

25 フィーチャーフォン（携帯電話）、及び、スマートフォンがある。

26 コンピュータ・プログラムの解析手法の一種。プログラムを実行することなく解析を行うことを静的解析、プログラムを実行して解析を行うことを動的解析と呼ぶ。静的解析は一般にソースコードに対して行われることが多い。

27 『Android アプリ DRM ガイドライン』（一般社団法人モバイル・コンテンツ・フォーラム、2012 年）を参照。
https://www.mcf.or.jp/temp/mcf_drm_gl.pdf



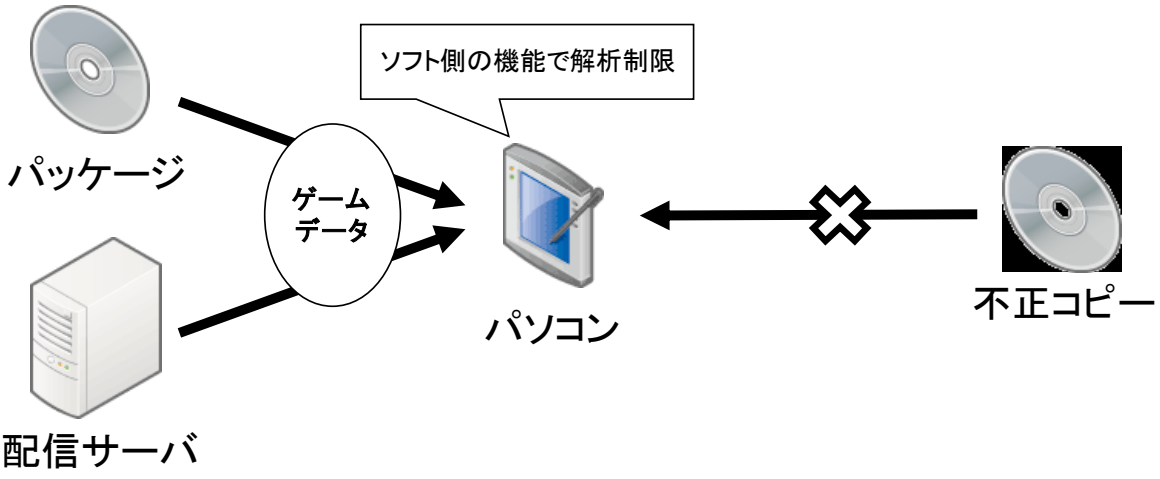
専用ゲーム機を利用端末とする場合の技術的手段の概要

専用ゲーム機上の機能でゲームデータの情報と組み合わせて保護を実現しているようであり、「非暗号型・フラグ型の利用制限」が実装されているようである。

（2）パソコンを利用端末とする場合

ゲームソフト側に動的解析や静的解析を防ぐ機能をもたせている例がある。例えば、ゲームソフトを解析してデータを改ざんしたり、秘匿してある情報を閲覧するなどの動作を検知した場合にゲームの動作を止めるといった機能である。しかし、動的であるか静的であるかを問わず、ユーザーの手元で行われる解析行為を防ぐことは現実的には困難である。

また、ソフトをオンラインで頒布する際に、ライセンス認証によって１ユーザーあたりの利用可能パソコン台数を制限する技術の導入事例がある[28]。



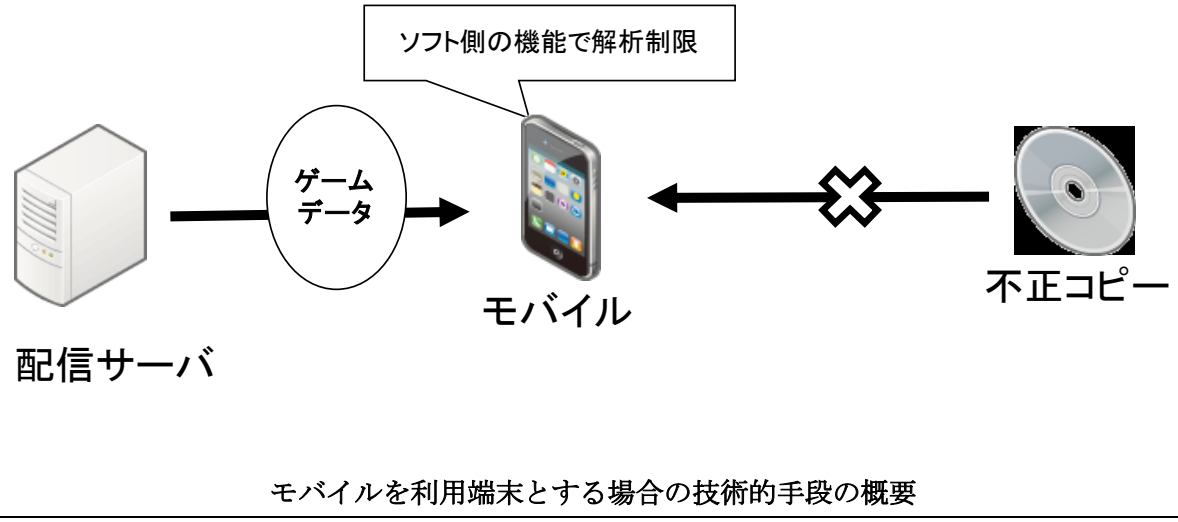
パソコンを利用端末とする場合の技術的手段の概要概要

28 サーファーテックの WEB ページ(http://www.cyphertec.co.jp/entertainment/entertainment09.html)

（3）モバイルを利用端末とする場合

フィーチャーフォンでは、キャリア指定の技術的手段を施す。

スマートフォンでは、ゲームソフト提供者が技術的手段を施すか否か、また、そのレベル等を、自らの意思で決定する。以下の通り、パソコンを端末とするゲームソフト同様、ソフト側に静的及び動的解析を防ぐ機能を持たせている場合がある。



モバイルを利用端末とする場合の技術的手段の概要

５．１．２　回避・無効化の実態

（1）専用ゲーム機を利用端末とする場合

専用ゲーム機であるニンテンドーDS は、不正に抽出されたゲームデータを読み込ませることでゲームがプレイできるようになる、いわゆる「マジコン」によって、技術的手段が回避・無効化されている実態がある。ゲームデータの抽出自体は比較的難易度が高いが、不正に抽出されたゲームデータはインターネット上の数々のサイトからダウンロードすることができる状況であり、回避・無効化する技術力のない者であっても、「マジコン」を購入すれば、比較的容易に不正ゲームデータを入手し、不正ゲームデータをプレイすることが可能となる。

同じく専用ゲーム機の PlayStationPortable(PSP)の場合は、マジコンのような追加のハードウェアは不要で、ファームウェア[29]を改変することで不正コピーしたゲームソフトを動作させるといった回避・無効化が行われている。

現在でも PlayStation3(PS3)、Xbox360、Wii などの一世代前の専用機で利用できる不正なゲームデータの流通がある。PS3 は現在も新作ソフトが発売されているが、PS3 は不正改造されたファームウェアで不正にコピーされたソフトが動作してしまう。アジアの一部の国・地域では、一世

29 ゲーム機に内蔵される基本ソフトウェア。ゲームの起動や本体の設定などを行う。

代前の専用機である PS3、Wii、Xbox360 用の不正コピーソフトの入ったディスクが売られている状況である。

なお、現行機種の PlayStation4、Xbox One、WiiU、PlayStationVita は、現時点において、解析や不正改造がなされておらず、不正コピーされたゲームソフトが出回る状況にはなっていない。

（2）パソコンを利用端末とする場合

パソコンを利用端末とするゲームに関して、静的及び動的解析対策の回避・無効化等の実態は明らかでない。

（3）モバイルを利用端末とする場合

モバイルのうちスマートフォンを利用端末とするゲームに関して、静的及び動的解析機能の回避・無効化等の実態は明らかでない。

５．１．３　経過、現状及び課題

（1）専用ゲーム機を利用端末とする場合

ニンテンドーDS のマジコンについては、関税法に基づく水際差止めの手続きが行われているため、中国サイト等からの個人輸入で税関をすりぬけるケースがあるものの、同マジコンの日本国内の業者による流通はあまり見られなくなっているようである。しかし、東アジア諸国では、いまなお流通がなされており、将来的な課題となっている。

専用ゲーム機に対するハッキングは後を絶たず、PS3、Xbox360、Wii などの一世代前までの専用機の技術的手段は既に回避・無効化されている。しかし、前記したように、現行機種の PlayStation4、Xbox One、WiiU、PlayStationVita に係る技術的手段は、現時点において回避・無効化されていない。

（2）パソコンを利用端末とする場合

パソコンを利用端末とするゲームソフトについて、ゲームソフトメーカーは、ゲームソフト側に静的又は動的解析を防ぐ機能をもたせている。

なお、現在、パソコンを利用端末とするゲームは、オンラインゲーム（WEB アプリ、及び、クラウドゲーム）の比率が増しており、当該ビジネス領域において新たな対策は講じられていない[30]。

（3）モバイルを利用端末とする場合

フィーチャーフォンを利用端末とするゲームソフトは、キャリアから提供される技術的手段を

30 ビジネスの主軸が移行したため、技術的手段の開発又は導入コストをかけないという判断に至ったものと考え得る。

施している。

スマートフォンを利用端末とするゲームソフトは、ゲームソフト提供者が、技術的手段を施すか否か、そのレベルを自ら判断し、またその導入維持費用も自ら負担する。現在、上述のパソコン同様、ゲームソフトメーカーは、ゲームソフト側に静的又は動的解析を防ぐ機能もたせている。なお、スマートフォンを端末とするゲームは、オンラインゲーム（WEB アプリ等）の比率が増しており、上述したパソコンを利用端末とする場合と同様、当該ビジネス領域において新たな対策は講じられていない。

５．２　オンラインゲーム

５．２．１　主な技術的手段

（１）利用時の認証

オンラインゲームのビジネスは、ソフト自体の売上（ユーザーがゲームソフトを購入する際に発生する初期費用による売上）と、運営サービス売上（月額課金、アイテム販売等の売上）からなる。その内訳は 2014 年の統計で、ソフト自体の売上が 10 億 8,100 万円、運営サービス売上 859 億 2,100 万円であり、およそ 99%を運営サービス売上が占める[31]。このため、オンラインゲーム運営者の関心は、運営サービスの健全な運営に向いており、利用時における ID・パスワード等による認証[32]は必須である。

（２）ユーザーによるデータ書き換え防止

ユーザーが自分の端末にあるデータを書き換えたり、自己の端末と運営サーバとの間の通信の内容を閲覧等してデータを書き換えることがある。例えば、レースゲームにおいて、自分のレーシングカーのスタート直後にゴールを置くといったデータの書き換えや、戦闘ゲームにおいて購入していない武器を幾つも所有している状態にするなどのデータ改ざんを自らの手元の端末で行う。データ改ざんによって無類の強さのプレイヤーや、アイテムと課金のバランス等が一致しないプレイヤーが出現すると、健全なユーザーが場を去ってしまうなどオンラインゲーム運営ビジネスに甚大な影響を及ぼす。

このため、運営者が、ユーザーが端末のメモリにあるデータを書き換えることを防ぐための静的及び動的解析対策ソフト[33]を導入する場合がある。

また、ゲーム運営サーバとユーザーの端末との間の通信の内容を改ざんしてデータの書き換え

---

31 前掲『2015CESA ゲーム白書』156 頁

32 ネットワーク接続時に当該ユーザーが利用権原を有するか否かを確認する。

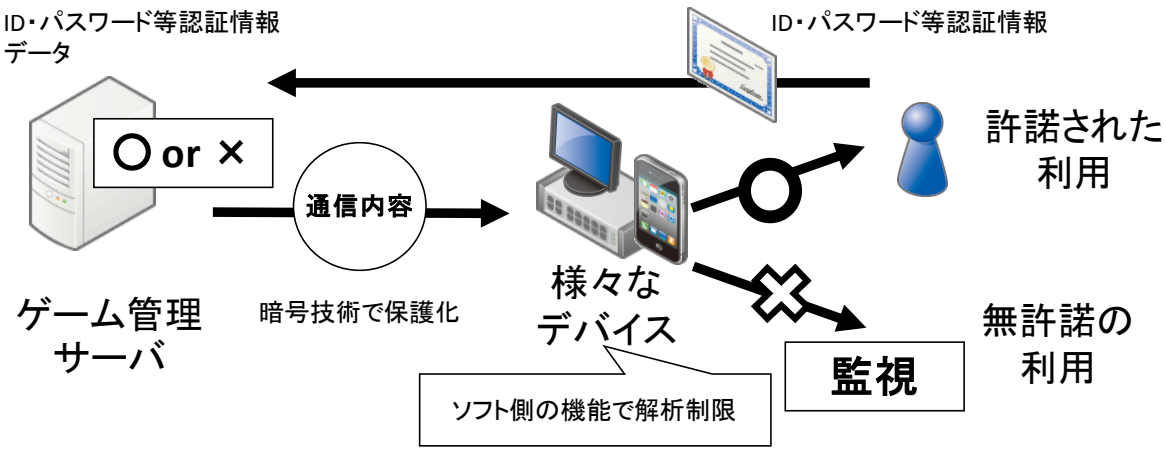
33 あるソフトウェアは、静的解析対策として、ＡＥＳ暗号化、逆アセンブル対策、改ざんチェック、動的解析対策として、デバッガ対策、メモリアクセス対策、コード挿入対策、エミュレータ対策に係る機能を有する。また、ゲームビジネスに特化したソフトウェアには、ボット対策、不正プログラム対策、デバッガ対策、エミュレータ対策、プロセスステルス、サーバクライアント認証、通信パケット暗号化、スピードハック検出、不正動作通知などの機能を具備しているものがある。

が行われる危険を減らすため、通信内容を暗号化する措置を講じる場合がある[34]。

なお、オンラインゲームの設計は一様ではなく、必ずしも静的及び動的解析対策ソフトや通信暗号化技術を導入する必要がないものもある。例えば、そもそもユーザーに一定の自由度が与えられている設計もある。また、ユーザーが更新したデータがサーバに送られてきた時点で厳重にチェックするという設計もある。

（３）プレイヤーの監視

認証を経てサーバにアクセスしたプレイヤーの振る舞いについては、目視等による監視が行われる。その結果、例えばあるプレイヤーが、これまでのプレイ時間やステータスとは異なる状態でゲームしていることを発見することがある。こうした場合、データの書き換えが行われた可能性が高い。利用規約に違反する行為であることが明らかになった場合、運営者が、当該プレイヤーに対しアカウント停止等の措置をとることもある。



オンラインゲームにおける技術的手段等の概要

このように、オンラインゲームでは、「認証により実現するアクセス制限、ユーザーによる解析対策、通信の暗号化、及び、プレイヤーによる不正行為の監視」、が行われている。

５．２．２　回避・無効化の実態

（１）利用時の認証

オンラインゲームでは利用時の認証が行われるが、他人の ID・パスワードを使用してゲーム運営サーバに不正にアクセスする者が後を絶たないというのが実情である。

34 サイファー・テックＷＥＢページ参照。(https://www.cyphertec.co.jp/cypher_guard/apptrusty.html)

（2）ユーザーによるデータ書き換え防止

ユーザーによるデータの書き換えを容易化するチート・ツールと呼ばれるプログラムが出回っており、これを利用したデータの書き換えが行われている実態がある[35]。

なお、現在出回っているチート・ツールが、どのような技術的手段を回避・無効化するものでわるかは、ヒアリングでは明らかにされていない。

５．２．３　経過、現状及び課題

運営サーバへの不正なアクセスが後を絶たない状況にあり、不正アクセス禁止法違反での対応が続いている[36]。

チート・ツールの譲渡等に対し、2015 年 7 月以降、著作権法、不正競争防止法、私電磁的記録不正作出・供用罪の適用事例が徐々に蓄積されつつある[37]。

６　その他

電子書籍は、各電子書店ごとの技術的手段と認証を組み合わせた保護が行われており、ユーザーに対するアクセス制限と電子書籍の複製制限や閲覧できるデバイス台数の制限等が実施されている。独自の技術的手段が採用されているため、異なる電子書店で購入した電子書籍を一元管理できず、相互運用性が問題となっている。

ビジネスソフトは、ユーザーが汎用コンピュータにインストールして繰り返し使用するものであるため、プログラム自体には技術的制限手段を講じないのが一般的であり、ライセンス認証システム[38]によってビジネスを保護している。ライセンス認証を実現する手段としては、ドングル[39]やシリアルキーの文字列を使った認証、オンラインでのユーザー認証を用いている例が多い。このため、シリアルキーなどの認証文字列だけを流通させる行為が問題となっている。

６．１　電子書籍の保護

６．１．１　主な技術的手段

現状多くの電子書店は epub 形式のフォーマットに対して書店ごとで様々な形式の技術的手段

35 本報告書第Ⅲ章４．２参照。

36 本報告書第Ⅲ章２．３参照

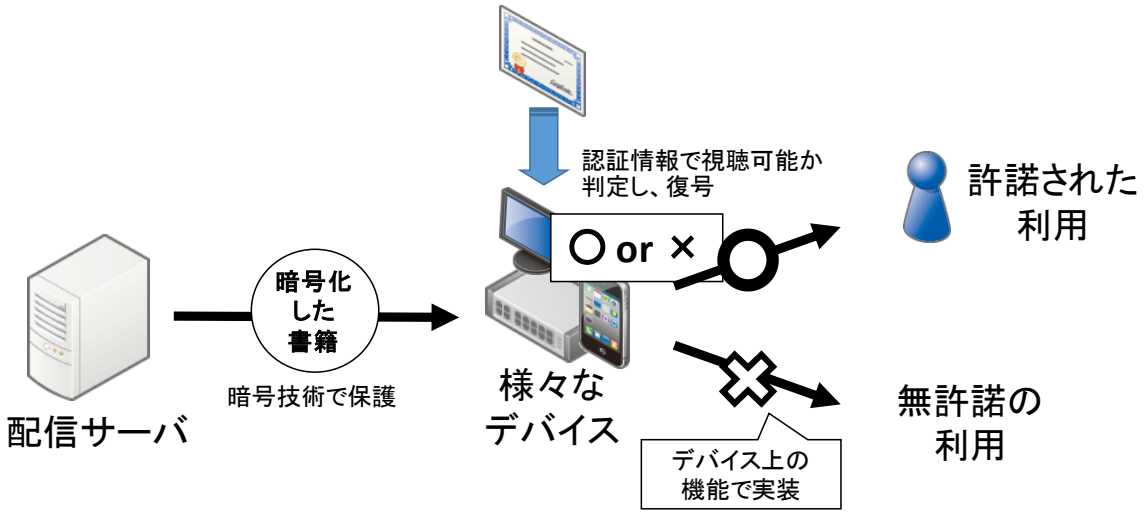
37 本報告書第Ⅲ章４．２参照。

38 プログラムの実行可能化条件として、メーカが送付する認証済みメッセージの受信とユーザ・コンピュータへの記録を求める仕組み。

39 コンピュータに接続する装置を言い、現在は USB を指すことが多い。ビジネスソフトの認証の場面では、コンピュータの起動時や実行中にドングルが装着されていることをチェックし、装着されていることを検出できない場合、ソフトウェアは起動しないか、または使用できる時間や機能などを制限する。

をかけている。独自の技術的手段を用いている電子書店もあれば、外部ベンダーが提供している汎用的な epub 用の技術的手段を用いている電子書店もある。技術的手段をかける目的は、伝送路中のコンテンツの暗号化、コピーの制限と利用端末の台数制限である。１アカウントあたりのデバイスを 5 台に制限する例が多いようである。

PC におけるキャプチャの制御を実施している電子書店もあったが、タブレットとスマホは OS 上の制約で制御の実現が困難であることから、書籍の権利者と協議のうえキャプチャ防止は入れないことにしている電子書店が多い。また、ブラウザでの閲覧については、技術的手段を使わず、Javascript による難読化（通信経路を監視し、通信途中の画像データを通信経路上から複製しても、スクランブルがかかったようにバラバラになるもの）をしている例があった。



電子書店において用いられるコピー等の利用制限

このように、電子書籍においては書籍を暗号化した上でネットワーク伝送させ、認証情報をもとに復号が行われて読むことが可能になる。復号後もオフライン閲覧の期間制限やコピー制限、キャプチャの防止機能などが実装されているため、「暗号型技術に認証技術を加えたアクセス制限及び、アクセス制限の解除をきっかけとしたコピー等利用制限」が実装されている状況である。

６．１．２　回避・無効化の実態

電子書店へのヒアリングでは、電子書籍に施した技術的手段の回避・無効化は認識していないという回答であった。他方、現状、海外の電子書籍サービスの技術的手段が回避・無効化されたという情報は存在する。

また、ヒアリングでは、書籍の場合は、アナログの紙のスキャンや電子版の画面キャプチャによって“有効な”海賊版が簡単にできてしまうため、電子書籍に施された技術的制限手段を一定の技術力をもって回避・無効化するまでもないのではないかとの見解も寄せられた。

６．１．３　経過、現状及び課題

2000 年前後から PC への配信には技術的手段がかけられており、KeyringPDF[40]という技術を用いていたようである。2005～2006 年頃のフィーチャーフォンでは CELSYS 社の Booksurfin[41]という技術で、コミックサーフィンという製品を多くの会社が使っていた。

現在は epub 形式に対応したの技術的手段が多く使われているが、一部の書店では電子書籍のフォーマットを epub 形式に統一せず、技術的手段は電子書籍のフォーマットがどのような形式であったとしても使えるように、汎用性を持たせているケースもあった。

電子書籍は、映像やゲームと異なり、ビューア（アプリ）が電子書店によって異なるため、技術的手段は出版社と電子書店との契約事項に基づいてそれぞれの電子書店が独自でかけることになる。また、スマートフォンや PC など閲覧するデバイスの OS など、プラットフォームのアップデートにも追随しなければならない。このため、技術的手段にかけるコストが高くつく。

技術的手段をかけることで書棚を別にしなければならなかったり、本来は汎用性の高い epub 形式のデータであるにもかかわらず特定のデバイスでなければ読めなくなるという問題も生じる。この点について Apple の iBooks が家族間でのデータ共有を可能とするなど、利用制限を緩くする流れもある。

なお、ヒアリングにおいては、技術的手段を回避・無効化することの最大の目的は、ハッカーが自らの技術力を誇示することにあるのではないか、このためもっぱら米国の大手電子書籍サイトである Amazon の技術的手段がターゲットとされているのではないか、との見解も示された。日本の電子書籍は、基本的には国内でしか購入できないこともあり、現状ではターゲットになることは少ないようである。

６．２　ビジネスソフトの保護

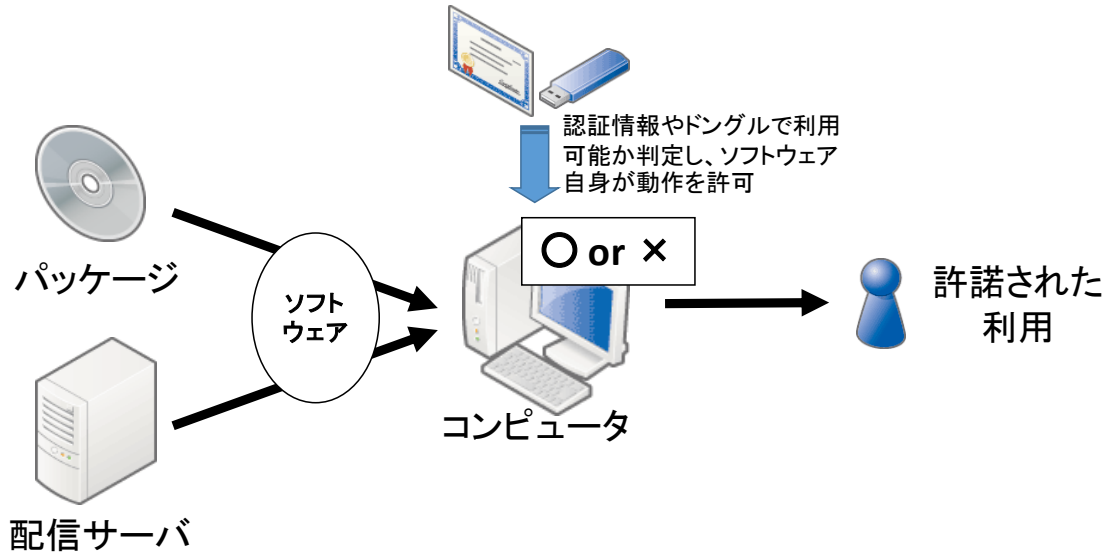
６．２．１　主な技術的手段

ビジネスソフト分野では、ライセンス認証によってビジネスを保護している。仕組みは、ネットワーク越しの認証情報の付与(アクティベーション)、もしくは期間内の利用許諾であるサブスクリプションが多いようである。特定のツールに関してはドングルを使っているものがあるが、これは主に映像処理ソフトや画像処理ソフト等の高額なソフトウェアのライセンスで使用されている。以下に利用の形態を図示する。

---

40 Keyring PDF (https://www.keyring.net/)

41 CELSYS (http://www.celsys.co.jp/)



ビジネスソフトにおいて用いられる技術的手段の概要

ビジネスソフトの例では、パッケージで提供されるソフトウェア、及び、サーバからダウンロード形式でコンピュータにインストールされるソフトウェア自体は保護されておらず、ソフトをインストールしようする者が利用権原を有しているかどうかを認証することで不正利用を防いでいる。一般には、ネットワーク越しの認証情報やハードウェアドングルと組み合わせて認証を実現している。

６．２．２　回避・無効化の実態

現在多く確認される回避・無効化の形態は、ビジネスソフトの期間限定の体験版に対して、不正シリアル番号などの認証情報を使って期間制限を解除する形である。体験版のソフトは正規のダウンロード方法で入手されており、認証情報だけが別に流通している。現在、しばしば見られる回避・無効化の形態は以下の通りである。

１．体験版のダウンロードを行ったユーザーに対し、不正なシリアル番号やレスポンスコード（オフライン認証したい場合に使う）を入力すれば期間制限を解除することのできるクラック・ツールと呼ばれるソフトウェアの提供

２．不正なシリアル番号やレスポンスコードを不正に作り出すキージェネレーターと呼ばれるソフトウェアの提供

３．ホストファイルや認証に関わるコードを改変する動作を行い、永続版として利用することができるソフトウェアの提供

６．２．３　経過、現状及び課題

ソフトウェアの利用及び提供形態が急速に変化している。従前は、ソフトウェアを CD-ROM 等の媒体に格納してユーザーに提供していた。しかし、インターネットの普及に伴い、徐々に、ソフトウェアをオンラインでダウンロードさせる提供形態が多くなってきた。さらに、現在、クラウド・コンピューティングの進展とともに、ソフトウェアをサーバ上で利用させる形態が増えつつある。

CD-ROM 等の媒体に格納して販売される場合、ユーザーは購入したビジネスソフトをインストールする際、CD-COM に同梱されている書類に書かれたシリアル番号の入力を求められ、この入力によって正規の購入者であることを認証する。しかし、インストールを終えたユーザーの中には、番号をネットオークションで売る者がいる。

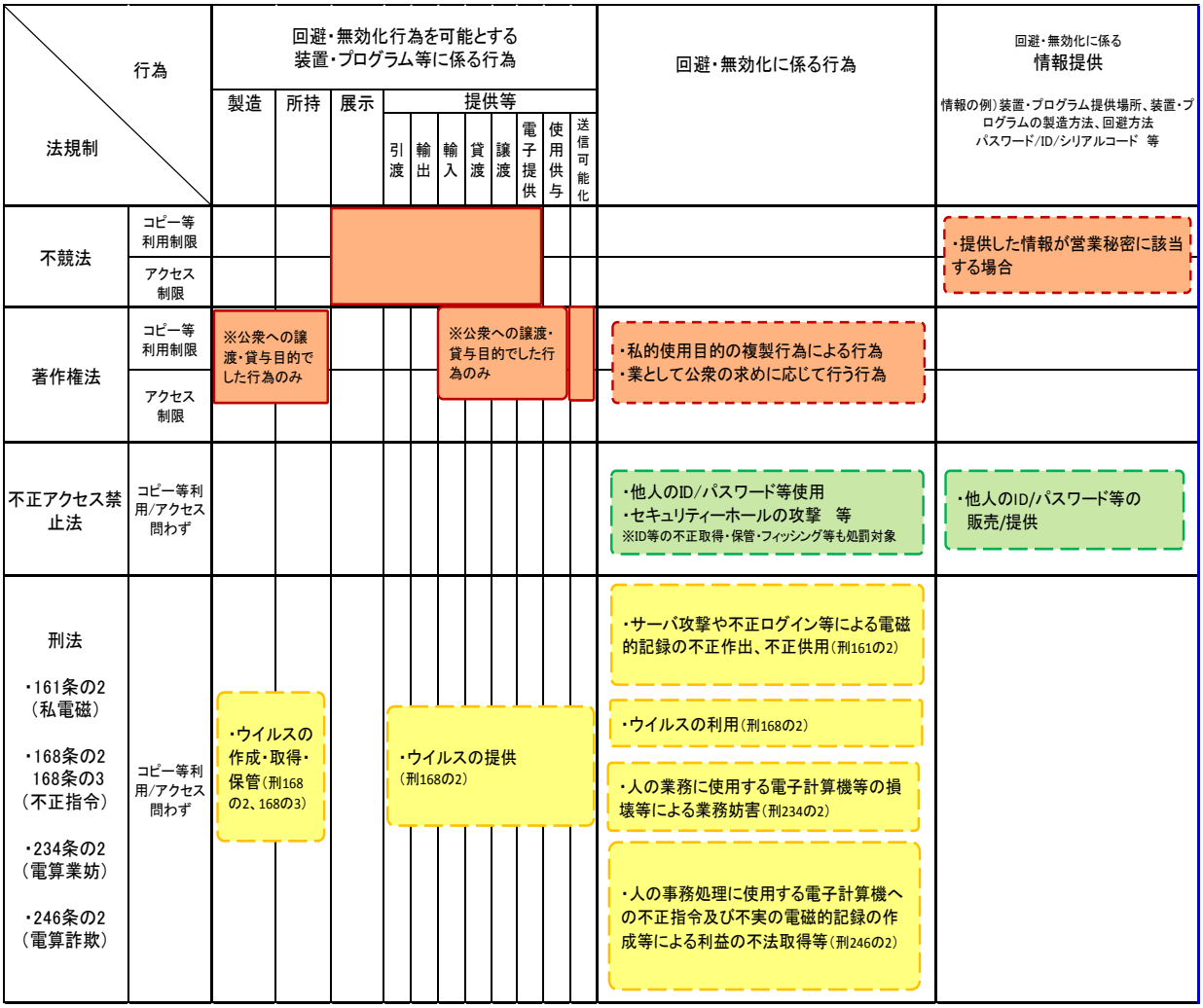
ダウンロード形式で提供される場合、ユーザーがソフトメーカーのウェブサイトからソフトをダウンロードすると、当該ソフトウェア用のシリアル番号が送られてくる。これを決まった方式で入力すれば、認証がなされ、決められた条件での使用が可能になる。無料で提供される体験版や試用版の場合は、ユーザーがソフトウェアをダウンロードすると、ユーザーの PC に未認証のシリアル番号等が記憶され、ここで使用期間や機能にロックがかかる。しかし、この認証を回避・無効化し、使用期間や機能の制限のない製品版プログラムの実行を可能化する信号である不正なシリアル番号等をユーザーの PC 内に偽造・偽装するプログラム（クラック・ツール）の提供が行われている。また、不正なシリアル番号や認証コードはネットオークション等で購入し、別途、クラック・ツールは蔵置されているウェブページからダウンロードする場合もある。

ソフトウェアをサーバ上で利用させる、いわゆるクラウドサービスにおいて、クラウドをハッキングしてソフトウェアを不正利用するようなケースは、現時点において起きていない。

第Ⅱ章　我が国における法規制の現状

1　法規制の全体像

技術的手段の回避・無効化に関する行為への法の適用関係を俯瞰する。



※ ┌ ┐で囲まれた部分は、条文上の一定の条件を満たした場合規制対象となるものであり、その横幅の広狭が、規制対象行為の広狭を示すものではない。
（例：著作権法の ┌業として公衆の求めに応じて行う行為┐ は、回避・無効化に係る行為の欄の横幅と同程度の幅で記載されているが、全ての回避・無効化行為を規制することを表すものではなく、回避・無効化行為のうち、業として公衆の求めに応じて行う行為のみを規制対象とすることを表す。）

（1）回避・無効化行為を可能とする装置・プログラム等に係る行為

技術的手段を回避・無効化することを可能とする装置・プログラム等に係る行為は、主に不正競争防止法及び著作権法による規制の対象となっている。

具体的に規制対象となる行為としては、両法の適用範囲が重なるものも多いが、そのうち片方の法律のみが適用される行為も存在する（「第Ⅱ章 1. 1 不正競争防止法及び著作権法による規制の概要を参照」）。

また、不正競争防止法において保護対象となる技術的手段は、原則、コピー等利用制限技術・アクセス制限技術の別を問わないのに対して、著作権法において保護対象となる技術的手段は、コピーコントロール技術（コピー等利用制限技術に含まれる）と、コピーコントロール技術を有効に機能させるためのアクセスコントロール技術（アクセス制限技術に含まれる）に限定されている（後述）。

なお、回避・無効化プログラムが、コンピュータ・ウィルスのような「不正指令電磁的記録」に該当する場合には、刑法上の不正指令電磁記録の作成・取得・保管・提供に関する罪が適用される可能性があるものと考えられる。

（2）回避・無効化に係る行為

技術的手段を回避・無効化する行為自体については、全ての行為態様が規制対象となるわけではないが、以下のような規制がなされている。

著作権法においては、技術的保護手段を回避して行う複製行為について、私的使用目的であったとしても規制対象（民事のみ）とされている。また、業として公衆の求めに応じて行う回避行為（回避サービス）についても規制の対象（刑事のみ）となっている。

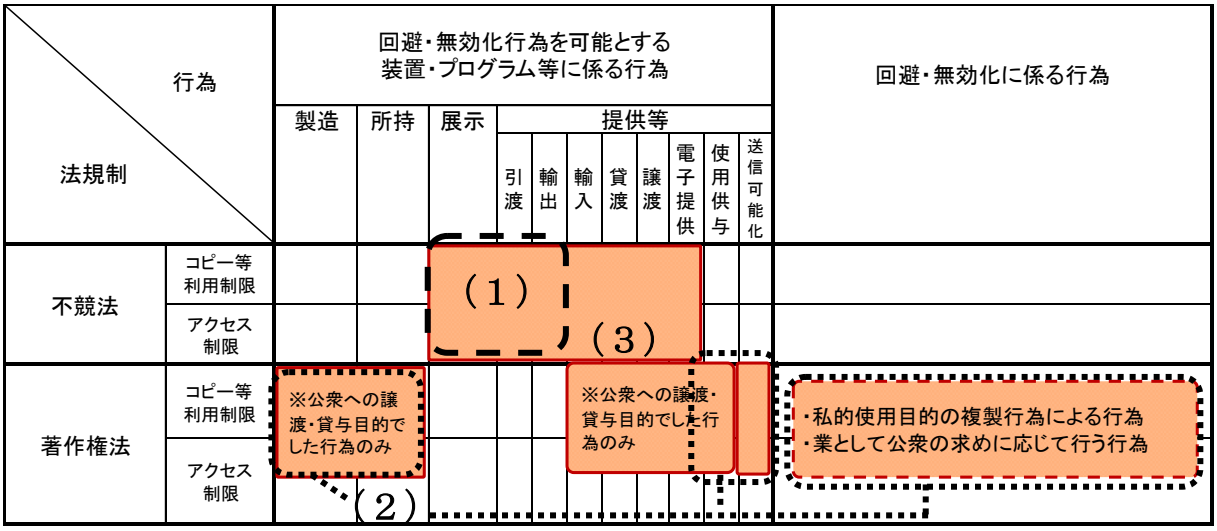
また、回避・無効化行為の態様が、他人の ID・パスワードの使用や、セキュリティ・ホール攻撃などの不正アクセス行為に該当する場合は、不正アクセス禁止法による規制がなされる可能性がある。その他、コンピュータ・ウィルスのような「不正指令電磁的記録」を回避・無効化行為に供した場合や、回避・無効化に当たって事業者の事務処理用の電磁的記録を書き換える等した場合、事業者が使用するコンピュータを損壊する等して業務妨害に至った場合などについては、それぞれ刑法上の罪が適用される可能性がある。

（3）回避・無効化に係る情報提供

回避・無効化に係る情報提供（「第Ⅳ章 2. 2 技術的手段の回避・無効化に係る「情報提供」の規制）参照）について、基本的に規制対象となる場合は限定的であるものと考えられる。例えば、提供される情報が事業者の営業秘密に該当する場合（技術的手段に用いられるプログラムコード等）には不正競争防止法（営業秘密不正開示罪）が、他人の ID・パスワード等に該当する場合には不正アクセス禁止法が適用される可能性があるものと考えられる。

１．１　不正競争防止法及び著作権法による規制の概要[42]

不正競争防止法及び著作権法による規制の異同及び重畳適用関係は以下の通り。なお、かかる規制の異同及び重畳適用関係をみる前提として、両法の射程が異なることに注意が必要である[43]。



（１）不正競争防止法のみの規制

・回避／無効化装置・プログラム等の引渡（貸与は著作権法と重畳規制）、譲渡・引渡目的の展示、輸出

（２）著作権法のみの規制

・回避／無効化装置・プログラム等の譲渡・貸与目的の製造および所持、使用供与、プログラムの送信可能化

・業として公衆の求めに応じて行う回避行為（刑事のみ）、回避によって可能になる私的使用のための複製（民事のみ）

（３）両法による重畳規制

・回避／無効化装置・プログラム等の譲渡、輸入（著作権法は譲渡・貸与目的の輸入）、電気通信回線提供（著作権法上は送信）、貸与（不正競争防止法上は引渡に含まれる。）

（４）留意点

・不正競争防止法は、回避／無効化行為等に及ばない。他方、著作権法は、業として行う回避行為に及ぶ。

・また、著作権法では、回避により可能となった複製は、私的使用のためであっても、民事上違法である。

・アクセス制限技術に関して、著作権法は、コピーコントロール技術を有効に機能させるた

42　詳細な分析は、本報告書第Ⅱ章２．３を参照。

43　不正競争防止法は、原則、コンテンツ提供者を保護対象者とし、コンテンツ（著作権保護対象であるか否かを問わない。）を保護対象物とするのに対し、著作権法は、著作者等を保護対象者とし、著作権保護対象の著作物を保護対象物とする。

めに用いられているアクセスコントロール技術を対象とし、アクセス制限技術全般には及ばない。

・不正競争防止法は、特定少数の者への譲渡等であっても規制対象となり得るのに対し、著作権法は「公衆への譲渡等」が規制の要件となっている。

１．２　技術的手段の回避･無効化に対する民事上及び刑事上の措置の概要

技術的手段の回避・無効化に関する行為に対し、我が国における法制度において規定される民事上及び刑事上の措置は、以下の通りである。

	対象	規制される行為	民事上の措置	刑事上の措置
不正競争防止法	回避･無効化装置（※装置には、容易に組み立てられる部品一式を含む）	譲渡、引渡（貸与を含む）、譲渡･引渡目的の展示、輸出、輸入	差止請求権(3 条) 損害賠償請求権(4 条)	5年以下の懲役または 500 万円以下の罰金（併科も可）（※不正の利益を得る目的、または営業上技術的手段を用いている者に損害を加える目的）21 条 2 項 2 項
	回避･無効化プログラムを記録した記録媒体			
	回避･無効化プログラムを記憶した機器			
	回避･無効化プログラム	電気通信回路を通じた提供		
著作権法	回避装置	公衆への譲渡、公衆への貸与、公衆への譲渡･貸与目的の製造、公衆への譲渡･貸与目的の輸入、公衆への譲渡･貸与目的の所持、公衆の使用供与	特に定めなし。	3年以下の懲役または 300 万円以下の罰金（併科も可）120 条の 2、1 号と 2 号
	回避プログラム			
	回避プログラム	公衆送信、送信可能化		
	回避行為	業として公衆の求めに応じて行う回避行為		
	私的使用目的の複製	技術的保護手段の回避により可能になった私的使用目的の複製	差止請求（112 条） 損害賠償請求権（民法 709 条）	なし
不正アクセス禁止法	アクセス管理者によって管理されたアクセス制御機能を有するコンピュータ	他人の識別符号（ID、パスワード等）を使って不正にアクセス（2 条 4 項 1 号）	－	3年以下の懲役または１００万円以下の罰金（11 条）
		セキュリティ･ホールを攻撃して不正にアクセス（2 条 4 項 2 号･3 号）	―	
	他人の識別符号	不正アクセス目的で取得（4 条）	―	1年以下の懲役または５０万円以下の罰金（12 条）
		無断で第三者に提供（5 条）	―	３０万円以下の罰金（13 条）
		不正アクセスする目的がある者に、そのことを知りながら提供（5 条）	―	1年以下の懲役または５０万円以下の罰金（12 条）
		不正アクセス目的で保管（6 条）	―	
		不正に入力を要求する行為（フィッシングサイト公開やフィッシング行為）（7 条）	―	

刑法161の2	権利・義務や事実証明に関する電磁的記録	・人の事務処理を誤らせる目的で不正に作出(1項) ・人の事務処理を誤らせる目的で不正に作成された電磁的記録を供用(3項)	—	5年以下の懲役 または 50万円以下の罰金
刑法168の2	不正な指令を与える電磁的記録その他の記録	正当な理由なく人の電子計算機の実行の用に供する目的でする －作成又は提供(1項)、 －実行(2項)	—	3年以下の懲役 または 50万円以下の罰金
刑法168の3	不正な指令を与える電磁的記録その他の記録	正当な理由なく人の電子計算機の実行の用に供する目的での取得又は保管	—	2年以下の懲役 または 30万円以下の罰金
刑法234の2	人の業務に使用する電子計算機 (損壊の場合は上記以外に、電計算機の用に供する電磁的記録も含む)	次のいずれかにより、電子計算機に使用目的に沿うべき動作させず又は使用目的に反する動作をさせて、人の業務を妨害した者 －損壊 －虚偽情報・不正指令を与え －その他の方法	—	5年以下の懲役 または 100万円以下の罰金
刑法246の2	人の事務処理に使用する電子計算機	虚偽又は不実の電磁的記録の作出、供用により財産上不法の利益を得、又は他人にこれを得させた者	—	10年以下の懲役

２　技術的手段の回避・無効化に対する法規制

２．１　不正競争防止法における規制

不正競争防止法は、第 2 条第 7 項に技術的制限手段の定義を、第 2 条第 1 項第 11 号及び第 12 号に技術的制限手段に対する不正行為の定義を規定する[44]。また、適用除外を第 19 条第 1 項第 8 号に、関連する民事上の措置を第 3 条、第 4 条、第 14 条に、関連する刑事上の措置を第 21 条第 2 項第 4 号にそれぞれ定める。

（１）技術的制限手段の定義

（定義）
第二条　この法律において「不正競争」とは、次に掲げるものをいう。
７　この法律において、「技術的制限手段」とは、電磁的方法（電子的方法、磁気的方法その他の人の知覚によって認識することができない方法をいう。）により影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を制限する手段であって、視聴等機器（影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録のために用いられる機器をいう。以下同じ。）が特定の反応をする信号を影像、音若しくはプログラムとともに記録媒体に記録し、若しくは送信する方式又は視聴等機器が特定の変換を必要とするよう影像、音若しくはプログラムを変換して記録媒体に記録し、若しくは送信する方式によるものをいう。

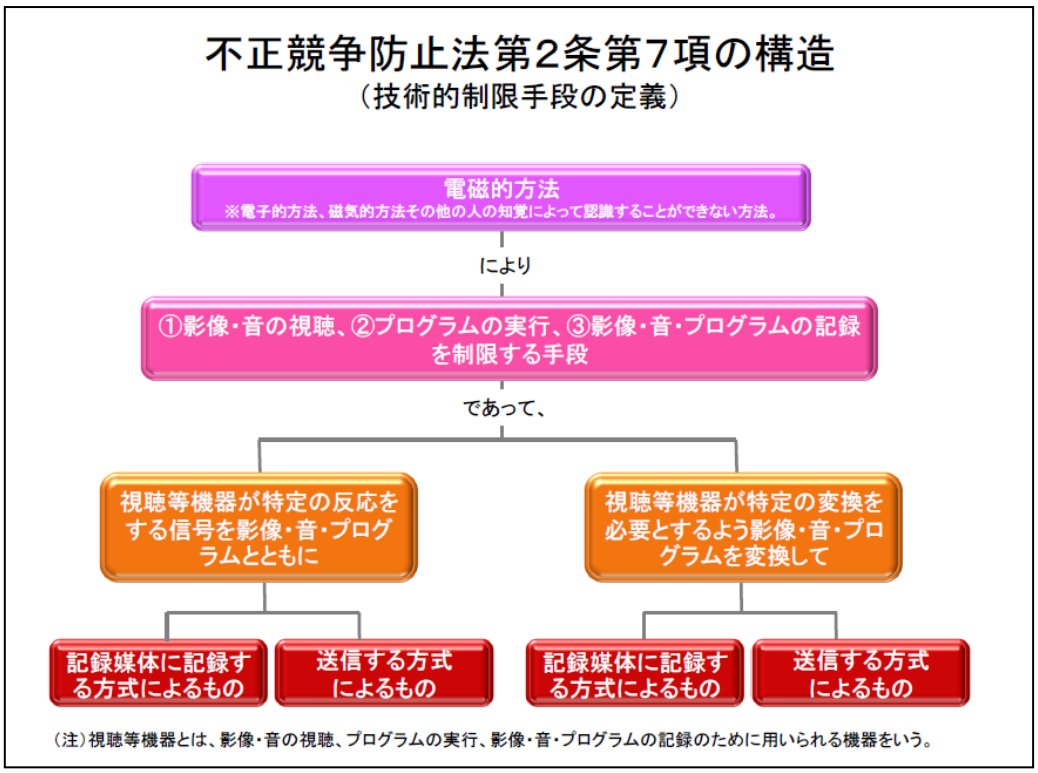
1999 年（平成１１年）の本規制導入時の逐条解説の一部を以下に摘記する[45]。（導入時は第２条第５項。）

・「電磁的方法」とは、人間の五感によっては感知できない方法を言う。また、「その他の・・・方法」の例としては、光学的方法がある。
・「制限する」とは、影像、音又はプログラムの提供者が、影像又は音の視聴、プログラムの実行、影像、音又はプログラムの記録に対して制約を課す管理を施すことを指す。有料衛星放送において、所定の料金を支払う特定の者に対してのみ番組の視聴を可能とすることも、「制限する」に含まれる。電力の配送技術、通信プロトコル技術、計算機のインターフェイス等は、影像又は音の視聴、プログラムの実行、映像、音又はプログラムの記録に対して制約を課す管理ではないので、本法上の無効化装置又はプロ

[44] 不正競争防止法における技術的制限手段に係る不正行為の定義は、2011 年（平成２３年）改正時には第２条第１項第１０号と同第１１号におかれていたが、2015 年（平成２７年）の別規制の改正により第１０号が新設されたため、それぞれ第１１号及び第１２号に変更された。本項においては、特に断りのない場合、2016 年（平成２８年）３月１日現在の条番号とする。
[45] 文化庁長官官房内著作権法令研究会・通商産業省知的財産研究会編『著作権法 不正競争防止法 改正解説 デジタル・コンテンツの法的保護』（有斐閣・1999 年）247 頁～251 頁。

グラムではない。

- 「影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を制限する手段」のうち、本法の対象は、「影像、音若しくはプログラムとともに記録媒体に記録し、若しくは送信する方式」と、「視聴等機器が特定の変換を必要とするよう影像、音若しくはプログラムを変換して記録媒体に記録し、若しくは送信する方式」に限定する[46] 。
- 「特定の反応をする信号」とは、影像若しくは音の視聴又はプログラムの実行を制限する手段を実施するために、影像、音又はプログラムの記録のために使用される機器に対して与えられる信号を言う。
- 「送信する」とは、影像、音又はプログラムを無線又は有線の手段により提供することを言う。無線としては放送、有線としては有線放送、インターネットが考えられる。
- 「特定の変換を必要とするよう影像、音若しくはプログラムを変換して」とは、有料放送のスクランブルのように、提供対象の影像、音若しくはプログラムを、規定のルールに従ってデータ変換させることを指す。



出典：経済産業省知的財産政策室編「不正競争防止法 2015」[47]

46 「視聴等機器特定の反応をする信号を影像、音若しくはプログラムとともに記録媒体に記録し、若しくは送信する方式」は非暗号型、「視聴等機器が特定の変換を必要とするよう影像、音若しくはプログラムを変換して記録媒体に記録し、若しくは送信する方式」は暗号型の技術的手段を念頭においているものと解され得る。

47 経済産業省ＷＥＢページ『不正競争防止法の概要（平成２７年度版）※平成２７年１２月更新』（http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/2015unfaircompetition-gaiyou_r.pdf）

＜「技術的制限手段」（不正競争防止法 2 条 7 項）の該当性が問題となった事件＞

2011 年（平成 23 年）改正前の事案であるが、第 2 条第 7 項の技術的制限手段該当性が問題となった事件として、東京地裁平成 21 年 2 月 27 日判決（特許ニュース 12503 号マジコン事件）がある[48]。

本件では、「ニンテンドーDS」等の本体および「DS カード」に用いられる仕組みが、技術的制限手段に該当し、いわゆる「マジコン」と称する装置が技術的制限手段を無効化する機能を有するか否かが問題となった。DS 本体は、DS カードを挿入するスロットを有し、DS カードを挿入すると、DS カードに記録されている特定信号を受信した場合のみ、それぞれの信号ごとに特定の反応をして、DS カードのプログラムを実行するものであるが、DS カードに格納されているゲームソフトを複製しても、特定信号は複製できるが、特定信号の機能は再現できず、プログラムの複製物は、DS 本体において使用することはできない。このように、DS 本体と DS カードは、組となって、特定信号を使用してプログラムの実行を制限し、視聴等機器が特定の反応をする信号をプログラム等とともに記録媒体に記録する方式のうち、その信号を検知した場合にプログラム等の実行を可能とする方式（検知→可能方式）によって、プログラムの実行を制限している。この検知→可能方式のほか、その信号を検知した場合にプログラム等の実行を制限する方式（検知→制限方式）もあり、本件では、技術的保護手段には検知→可能方式も含まれるかが問題となった。

本裁判例は、「不正競争防止法第 2 条第 1 項第 10 号（当時）の立法趣旨と、無効化機器の 1 つである MOD チップを規制の対象としたという立法経緯に照らすと、不正競争防止法第 2 条第 7 項の『技術的制限手段』とは、コンテンツ提供事業者が、コンテンツの保護のために、コンテンツの無断複製や無断視聴等を防止するために視聴等機器が特定の反応を示す信号等をコンテンツとともに記録媒体に記録等することにより、コンテンツの無断複製や無断視聴等を制限する電磁的方法を意味するものと考えられ、検知→制限方式のものだけでなく、検知→可能方式のものも含む」と判断し、DS 本体と DS カードに用いられる仕組みは技術的制限手段に該当すると結論づけた。マジコンは、DS カードに格納されているプログラムの複製物を DS 本体で実行できるようにするために、DS カードを普通に複製しても再現できない特定信号の機能を補うものであるが、裁判所は、このように使用されるマジコンは、不正競争防止法第 2 条第 1 項第 11 号（当時）の技術的制限手段を妨げる機能を有する装置に該当すると判断し、同号に基づく差止請求を認容した。

[48] 東京地方裁判所平成２１年２月２７日　平成 20 年（ワ）第 20886、35745 号。なお、本裁判例の解説は、『不正競争防止の法実務（改訂版）』（三協法規出版・2013 年）272 頁～273 頁に掲載された論文を執筆者井奈波朋子氏の許諾を得て掲載したものである。

（2）技術的制限手段に対する不正行為の定義

（定義）

第二条　この法律において「不正競争」とは、次に掲げるものをいう。

十一　営業上用いられている技術的制限手段（他人が特定の者以外の者に映像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために用いているものを除く。）により制限されている影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録（以下この号において「影像の視聴等」という。）を当該技術的制限手段の効果を妨げることにより可能とする機能を有する装置（当該装置を組み込んだ機器及び当該装置の部品一式であって容易に組み立てることができるものを含む。）若しくは当該機能を有するプログラム（当該プログラムが他のプログラムと組み合わされたものを含む。）を記録した記録媒体若しくは記憶した機器を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該機能を有するプログラムを電気通信回線を通じて提供する行為（当該装置又は当該プログラムが当該機能以外の機能を併せて有する場合にあっては、影像の視聴等を当該技術的制限手段の効果を妨げることにより可能とする用途に供するために行うものに限る。）

十二　他人が特定の者以外の者に映像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために営業上用いている技術的制限手段により制限されている影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録（以下この号において「影像の視聴等」という。）を当該技術的制限手段の効果を妨げることにより可能とする機能を有する装置（当該装置を組み込んだ機器及び当該装置の部品一式であって容易に組み立てることができるものを含む。）若しくは当該機能を有するプログラム（当該プログラムが他のプログラムと組み合わされたものを含む。）を記録した記録媒体若しくは記憶した機器を当該特定の者以外の者に譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該機能を有するプログラムを電気通信回線を通じて提供する行為（当該装置又は当該プログラムが当該機能以外の機能を併せて有する場合にあっては、影像の視聴等を当該技術的制限手段の効果を妨げることにより可能とする用途に供するために行うものに限る。）

第 2 条第 1 項第 11 号及び第 12 号について、2011 年（平成 23 年）及び 2012 年（平成 24 年）改正時の逐条解説の一部を以下に摘記する[49]（改正時はそれぞれ第 2 条第 1 項第 10 号及び第 11 号におかれていた。条文は同じである。）。

[49] 経済産業省知的財産政策室編著『逐条解説 不正競争防止法 平成 23・24 年改正版』（有斐閣・2012 年）79 頁～90 頁。

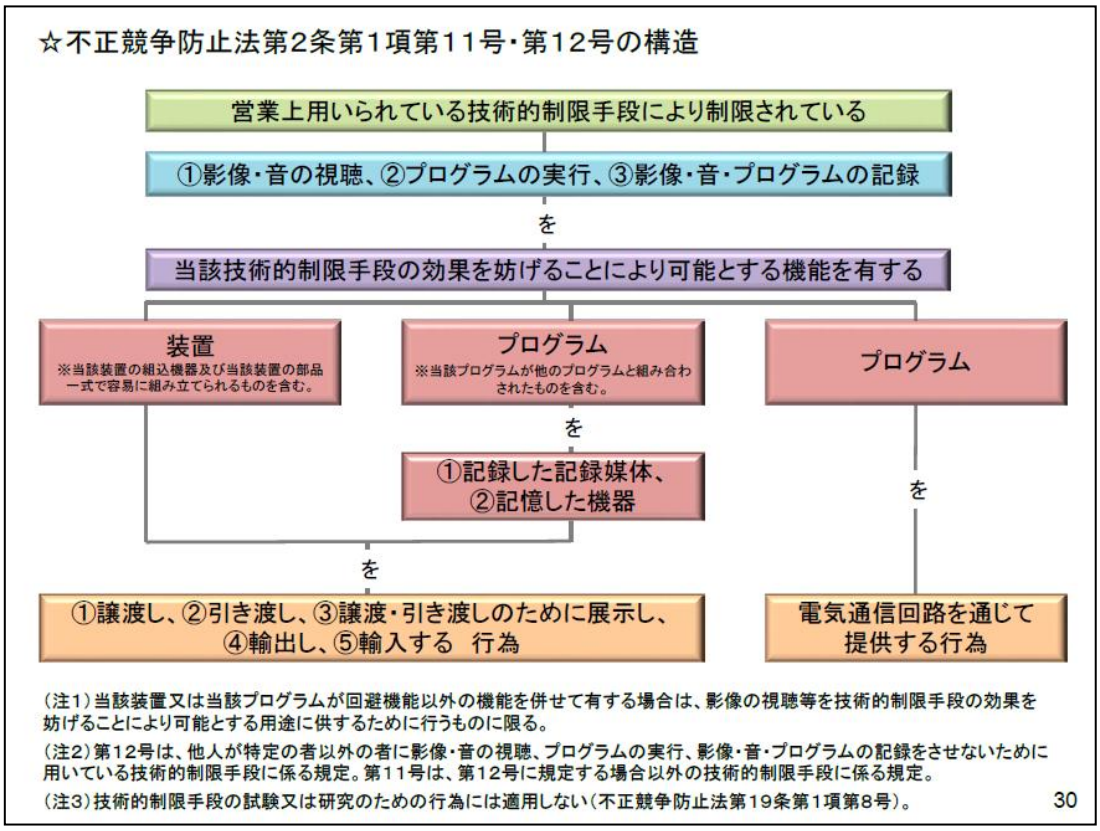
・「営業上用いられている」とは、「技術的制限手段」をある営業活動のために用いていることを示しているに過ぎず、例えばプライバシー保護の目的あるいは防衛上の目的で用いられている暗号化等は含まれない。
・「影像若しくは音の視聴」とは、映像、文字、図形等の視覚による感知又は音楽、音響等の聴覚による感知による情報の取得及び認識を言う。
・「プログラムの実行」とは、技術的制限手段は施される対象のうち、プログラムについて制限がなされる行為を示す。
・「影像、音若しくはプログラムの記録」とは、影像、音若しくはプログラムを、記録媒体に固定させることを言う。
・「当該技術的制限手段の効果を妨げることにより可能とする機能」とは、営業上用いられている技術的制限手段によって制限されている影像、音の視聴、プログラムの実行、影像、音、プログラムの記録を可能とする機能を言う。
・「装置」とは、一定の機能を有する機器の内蔵品という意味に解される
・「機器」とは、機械と器具を包括した概念であり、本法においては、影像の視聴を制限するために記録媒体に付された信号を解除する機能を有するチップを内蔵する箱体の機器を指す。
・「当該装置を組み込んだ機器・・・を含む。」とは、本来規制の対象とされている回避機能を有する装置だけの提供と認められる行為であれば、こうした装置を組み込んだ機器についても規制の対象となるという意味である。
・「当該装置の部品一式であって容易に組み立てることができるもの」とは、所謂「組み立てキット」であり、本法においては、技術的制限手段の回避装置の提供行為と同様に、当該装置の組み立てキットの提供も公正な競争を阻害する効果を有するものであるとして規制した。
・「当該プログラムが他のプログラムと組み合わされたもの」とは、技術的制限手段の効果を妨げる機能を有するプログラムと、別の機能を有するプログラムが組み合わされたものを言う。本体他の機能を有するプログラムとして作成されたのに、たまたま「技術的制限手段の効果を妨げる機能を有するプログラム」が外見上形式的に含まれている場合は、「当該プログラムが他のプログラムと組み合わされたもの」には含まれない。
・「当該装置又は当該プログラムが当該機能以外の機能を併せて有する場合にあっては、影像の視聴等を当該技術的制限手段の効果を妨げることにより可能とする用途に供するために行うものに限る。」とは、回避機能とそれ以外の機能を併せて有する装置等について、当該装置等を回避の用途に供するために提供する行為に限る意味で、これを不正競争として規制するものである。

1999 年（平成 11 年）の当該規制導入時には、規制の対象となる行為の範囲を、回避・無効化機能のみを有する装置等の提供行為としていた（いわゆる「のみ要件」）。しかし、その後、技術的制限手段を回避・無効化する機能に他の機能を追加的に付した装置が出回り、これらの装置は付加の機能があることによって「のみ要件」を充足せず、その提供行為は不正競争行為に該当しないと主張されることで、コンテンツ事業者に甚大な被害およぼすことなった。

こうした状況を踏まえ、2011 年（平成 23 年）改正において「のみ要件」を緩和するに至ったが、その際、規制対象となる装置や行為の範囲が過度に広汎にならないよう、「当該技術的制限手段の効果を妨げることにより可能とする用途に供するために行うものに限る。」との文言が挿入された。

また、いわゆる「無反応機器」と呼ばれるコンテンツに付された技術的制限手段を検知しない機器については、これを規制すると、記録や視聴等を制限するあらゆる信号に対応する措置を施すよう強制することになるとして、不正競争の対象としないことが適当とされた[50]。

本法において規制される行為は、技術的制限手段の効果を妨げることにより可能とする機能を有する装置若しくは当該機能を有するプログラムを記録した記録媒体若しくは機器の「譲渡」、「引き渡し」、「譲渡若しくは引き渡しの目的をもった展示」、「輸出」、「輸入」、「当該機能を有するプログラムの電気通信回線を通じた提供」である。



出展：経済産業省知的財産政策室編「不正競争防止法 2015」[51]

[50] 前掲・経済産業省知的財産政策室編著『逐条解説 不正競争防止法 平成 23・24 年改正版』87 頁。

[51] 前掲・経済産業省『不正競争防止法の概要』

第 11 号は、視聴機器や媒体等を所持する全ての者に対して一律に制限を課すために技術的制限手段を営業上用いている場合（ＤＶＤに組み込まれている録画制限機能等）についての不正行為である。これに対して、第 12 号は、契約等により特定された者以外の者に対してコンテンツの視聴等を制限するために技術的制限手段を営業上用いている場合（有料放送のように契約者以外の者は解除できないように施されている暗号等）についての不正行為である。

（３）適用除外

（適用除外等）

第十九条　第三条から第十五条まで、第二十一条（第二項第七号に係る部分を除く。）及び第二十二条の規定は、次の各号に掲げる不正競争の区分に応じて当該各号に定める行為については、適用しない。

八　第二条第一項第十一号及び第十二号に掲げる不正競争　技術的制限手段の試験又は研究のために用いられる同項第十一号及び第十二号に規定する装置若しくはこれらの号に規定するプログラムを記録した記録媒体若しくは記憶した機器を譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該プログラムを電気通信回線を通じて提供する行為

技術的制限手段の試験又は研究のため用いられる回避・無効化装置等の譲渡等には法の適用が除外される。コンテンツ提供事業者が、自ら使用する技術的制限手段や他人の技術的制限手段のレベル等について試験・研究する場合に回避・無効化装置等の譲渡を受けることを想定したものである[52]。

（４）民事上の措置

①差止請求権

（差止請求権）

第三条　不正競争によって営業上の利益を侵害され、又は侵害されるおそれがある者は、その営業上の利益を侵害する者又は侵害するおそれがある者に対し、その侵害の停止又は予防を請求することができる。

２　不正競争によって営業上の利益を侵害され、又は侵害されるおそれがある者は、前項の規定による請求をするに際し、侵害の行為を組成した物（侵害の行為により生じた物を含む。第五条第一項において同じ。）の廃棄、侵害の行為に供した設備の除却その他の侵害の停止又は予防に必要な行為を請求することができる。

[52] 前掲・経済産業省知的財産政策室編著 174 頁。

②損害賠償請求

（損害賠償）
第四条　故意又は過失により不正競争を行って他人の営業上の利益を侵害した者は、これによって生じた損害を賠償する責めに任ずる。ただし、第十五条の規定により同条に規定する権利が消滅した後にその営業秘密を使用する行為によって生じた損害については、この限りでない。

③信用回復措置請求

（信用回復の措置）
第十四条　故意又は過失により不正競争を行って他人の営業上の信用を害した者に対しては、裁判所は、その営業上の信用を害された者の請求により、損害の賠償に代え、又は損害の賠償とともに、その者の営業上の信用を回復するのに必要な措置を命ずることができる。

（５）刑事上の措置

（罰則）
第二十一条　（1 項略）
２　次の各号のいずれかに該当する者は、五年以下の懲役若しくは五百万円以下の罰金に処し、又はこれを併科する。
四　不正の利益を得る目的で、又は営業上技術的制限手段を用いている者に損害を加える目的で、第二条第一項第十一号又は第十二号に掲げる不正競争を行った者

不正の利益を得る目的で、又は、営業上技術的制限手段を用いている者に損害を加える目的で、技術的制限手段に係る不正行為を行った者に対する刑事処罰を可能とした[53]。2011 年（平成 23 年）改正により新設された。

２．２　著作権法における規制

著作権法は、第 2 条第 1 項第 20 号に技術的保護手段の定義、第 30 条第 1 項第 2 号に技術的保護手段を回避して行う私的使用のための複製について、第 112 条に差止請求権、第 113 条にみなし侵害、第 120 条の 2 第 1 号に技術的保護手段の回避装置・プログラム等の提供等に関する刑事罰、第 120 条の 2 第 2 号に業として公衆の求めに応じて技術的保護手段の回避行為を行った者に対する刑事罰を、それぞれ定める。

[53] 前掲・経済産業省知的財産政策室編著 198 頁。

（１） 技術的保護手段の定義

（定義）
第二条　この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
二十　技術的保護手段　電子的方法、磁気的方法その他の人の知覚によつて認識することができない方法（次号において「電磁的方法」という。）により、第十七条第一項に規定する著作者人格権若しくは著作権又は第八十九条第一項に規定する実演家人格権若しくは同条第六項に規定する著作隣接権（以下この号、第三十条第一項第二号及び第百二十条の二第一号において「著作権等」という。）を侵害する行為の防止又は抑止（著作権等を侵害する行為の結果に著しい障害を生じさせることによる当該行為の抑止をいう。第三十条第一項第二号において同じ。）をする手段（著作権等を有する者の意思に基づくことなく用いられているものを除く。）であつて、著作物、実演、レコード、放送又は有線放送（次号において「著作物等」という。）の利用（著作者又は実演家の同意を得ないで行つたとしたならば著作者人格権又は実演家人格権の侵害となるべき行為を含む。）に際し、これに用いられる機器が特定の反応をする信号を著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録し、若しくは送信する方式又は当該機器が特定の変換を必要とするよう著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像を変換して記録媒体に記録し、若しくは送信する方式によるものをいう。

技術的保護手段は、①電磁的方法により著作権等の侵害行為を防止又は抑止するものであること、②著作権者等の意思に基づいて用いられているものであること、③機器が特定の反応をする信号を著作物等とともに記録・送信する方式によるか、又は、機器が特定の変換を必要とするよう著作物等を変換して記録・送信する方式によるものであることを要件とする。

③のうち前者は、著作物のコピーを制限する SCMS や CGMS 等のコピーコントロール技術[54]に該当し、技術的保護手段の回避に関する規制が導入された 1999 年（平成 11 年）改正からの規制である。後者は、CSS や B-CAS 等のアクセスコントロール技術[55]に主に用いられる暗号化方式の技術で、2012 年（平成 24 年）改正によって保護の対象とした。

1999 年（平成 11 年）改正法により技術的保護手段に関する規定が設けられた当初、暗号型の技術的手段は、アクセスコントロール技術と捉えられ、著作権法で規制される技術的保護手段は、非暗号型の技術的手段のみを規制対象としていた。しかし、規制対象を非暗号型の技術的手段に限定すると、DVD や Blu-ray に用いられている暗号型の技術的手段は規制対象とならないため、著作権保護の実効性が確保できないとの問題が指摘されていた。

このため、2012 年（平成 24 年）著作権法改正では、規制対象となる技術的保護手段の範囲を

[54] 用語の定義は、本報告書「はじめに　３　報告書における用語の定義」の通り。
[55] 前脚注の通り。

拡大し、従来から規制対象となっていた非暗号型の技術的保護手段に加え、新たに暗号型の技術的手段も技術的保護手段の対象に加えた。

これは、アクセスコントロール技術であってもコピーコントロール技術を有効に機能させるための技術として用いられているものがあり、このような技術はコピーコントロール技術機能とアクセスコントロール技術機能を併せ有するものと評価できるので、著作権法上の技術的保護手段と位置づけるべきであると考えられたことによる。

著作権法第 2 条第 1 項第 20 号は、規制対象となる技術的保護手段について、「著作権等を有する者の意思に基づくことなく用いられているものを除く」と規定する。これは、技術的保護手段に関する規定が、著作権保護を確保するためのものであることによる。

（2）技術的保護手段を回避して行う私的使用目的の複製

（私的使用のための複製）

第三十条　著作権の目的となつている著作物（以下この款において単に「著作物」という。）は、個人的に又は家庭内その他これに準ずる限られた範囲内において使用すること（以下「私的使用」という。）を目的とするときは、次に掲げる場合を除き、その使用する者が複製することができる。

二　技術的保護手段の回避（第二条第一項第二十号に規定する信号の除去若しくは改変（記録又は送信の方式の変換に伴う技術的な制約による除去又は改変を除く。）を行うこと又は同号に規定する特定の変換を必要とするよう変換された著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像の復元（著作権等を有する者の意思に基づいて行われるものを除く。）を行うことにより、当該技術的保護手段によつて防止される行為を可能とし、又は当該技術的保護手段によつて抑止される行為の結果に障害を生じないようにすることをいう。第百二十条の二第一号及び第二号において同じ。）により可能となり、又はその結果に障害が生じないようになつた複製を、その事実を知りながら行う場合　。

前記の通り、1999 年（平成 11 年）改正は、本条の適用対象を信号方式のコピーコントロール技術に限定していたが、2012 年（平成 24 年）改正によって、複製権を保護するために用いられると認識し得る暗号化技術も適用対象とされた[56]。

これら二度の法整備により、私的使用目的であっても、技術的保護手段の回避によって可能となった複製、あるいは技術的保護手段の回避によって複製結果に障害が生じないようになった複製については、その事実を知りながら行う場合、私的使用のための複製から除外され、民事上違法とされた。

[56] 中山信弘『著作権法（第 2 版）』（有斐閣・2014 年）290 頁～298 頁

（3）差止請求権、侵害とみなす行為

①差止請求権

（差止請求権）

第百十二条　著作者、著作権者、出版権者、実演家又は著作隣接権者は、その著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する者又は侵害するおそれがある者に対し、その侵害の停止又は予防を請求することができる。

2　著作者、著作権者、出版権者、実演家又は著作隣接権者は、前項の規定による請求をするに際し、侵害の行為を組成した物、侵害の行為によつて作成された物又は専ら侵害の行為に供された機械若しくは器具の廃棄その他の侵害の停止又は予防に必要な措置を請求することができる。

②侵害とみなす行為

（侵害とみなす行為）

第百十三条　次に掲げる行為は、当該著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する行為とみなす。

一　国内において頒布する目的をもつて、輸入の時において国内で作成したとしたならば著作者人格権、著作権、出版権、実演家人格権又は著作隣接権の侵害となるべき行為によつて作成された物を輸入する行為

二　著作者人格権、著作権、出版権、実演家人格権又は著作隣接権を侵害する行為によつて作成された物（前号の輸入に係る物を含む。）を、情を知つて、頒布し、頒布の目的をもつて所持し、若しくは頒布する旨の申出をし、又は業として輸出し、若しくは業としての輸出の目的をもつて所持する行為

2　プログラムの著作物の著作権を侵害する行為によつて作成された複製物（当該複製物の所有者によつて第四十七条の三第一項の規定により作成された複製物並びに前項第一号の輸入に係るプログラムの著作物の複製物及び当該複製物の所有者によつて同条第一項の規定により作成された複製物を含む。）を業務上電子計算機において使用する行為は、これらの複製物を使用する権原を取得した時に情を知つていた場合に限り、当該著作権を侵害する行為とみなす。

3　次に掲げる行為は、当該権利管理情報に係る著作者人格権、著作権、実演家人格権又は著作隣接権を侵害する行為とみなす。

一　権利管理情報として虚偽の情報を故意に付加する行為

二　権利管理情報を故意に除去し、又は改変する行為（記録又は送信の方式の変換に伴う技術的な制約による場合その他の著作物又は実演等の利用の目的及び態様に照らしやむを得ないと認められる場合を除く。）

三　前二号の行為が行われた著作物若しくは実演等の複製物を、情を知つて、頒布し、若しくは頒布の目的をもつて輸入し、若しくは所持し、又は当該著作物若しくは実演等を情を知つて公衆送信し、若しくは送信可能化する行為

4　第九十四条の二、第九十五条の三第三項若しくは第九十七条の三第三項に規定する報酬又は第九十五条第一項若しくは第九十七条第一項に規定する二次使用料を受ける権利は、前項の規定の適用については、著作隣接権とみなす。この場合において、前条中「著作隣接権者」とあるのは「著作隣接権者（次条第四項の規定により著作隣接権とみなされる権利を有する者を含む。）」と、同条第一項中「著作隣接権」とあるのは「著作隣接権（同項の規定により著作隣接権とみなされる権利を含む。）」とする。

5　国内において頒布することを目的とする商業用レコード（以下この項において「国内頒布目的商業用レコード」という。）を自ら発行し、又は他の者に発行させている著作権者又は著作隣接権者が、当該国内頒布目的商業用レコードと同一の商業用レコードであつて、専ら国外において頒布することを目的とするもの（以下この項において「国外頒布目的商業用レコード」という。）を国外において自ら発行し、又は他の者に発行させている場合において、情を知つて、当該国外頒布目的商業用レコードを国内において頒布する目的をもつて輸入する行為又は当該国外頒布目的商業用レコードを国内において頒布し、若しくは国内において頒布する目的をもつて所持する行為は、当該国外頒布目的商業用レコードが国内で頒布されることにより当該国内頒布目的商業用レコードの発行により当該著作権者又は著作隣接権者の得ることが見込まれる利益が不当に害されることとなる場合に限り、それらの著作権又は著作隣接権を侵害する行為とみなす。ただし、国内において最初に発行された日から起算して七年を超えない範囲内において政令で定める期間を経過した国内頒布目的商業用レコードと同一の国外頒布目的商業用レコードを輸入する行為又は当該国外頒布目的商業用レコードを国内において頒布し、若しくは国内において頒布する目的をもつて所持する行為については、この限りでない。

6　著作者の名誉又は声望を害する方法によりその著作物を利用する行為は、その著作者人格権を侵害する行為とみなす。

著作権法上の権利侵害とは、第 18 条から第 28 条に規定される行為が無断で行われ、かつ、第 30 条から第 50 条までの権利制限規定が及ばない場合を言う。しかし、このように直接的な侵害行為でなくても、著作権侵害物品の輸入・販売のように、権利者の利益を害する行為があり、著作権法は、侵害とみなす行為と規定している。侵害とみなされた行為は、侵害行為と同様に取り扱われ、権利者は差止め及び損害賠償を請求することができる。また、行為者には刑事罰が科される。実質的にみた場合、侵害に関して権利範囲を拡張したものと言うことができる[57]。

[57] 前掲・中山 646 頁～659 頁。島並良・上野達弘・横山久芳『著作権入門』（有斐閣・2009）259 頁。

侵害とみなす行為の具体的な内容は、以下の通りである。なお、下表最下欄の「著作者の名誉・声望を害する利用」は、著作者人格権を侵害する行為とみなされる行為である。

侵害とみなす行為	内容
侵害物の輸入 （第 113 条第 1 項第 1 号）	国内において頒布する目的をもつて、輸入の時において国内で作成したとしたならば権利侵害となるべき行為によつて作成された物を輸入する行為 [例：海外で作られた海賊版 CD・DVD 等の輸入]
侵害物の知情頒布 （第 113 条第 1 項第 2 号前段）	権利侵害行為によつて作成された物を、情を知つて、頒布し、頒布の目的をもつて所持し、若しくは頒布する旨の申出をする行為 [例：海賊版 CD・DVD 等の販売等]
侵害物の頒布目的の輸出等 （第 113 条第 1 項第 2 号後段）	権利侵害行為によつて作成された物を、情を知つて、業として輸出し、若しくは業としての輸出の目的をもつて所持する行為 [例：海賊版 CD・DVD 等の輸出等]
違法作成プログラムの知情による業務上の使用 （第 113 条第 2 項）	プログラムの著作物の著作権を侵害する行為によつて作成された複製物を業務上電子計算機において使用する行為。ただし、その複製物の使用権原を取得した時に情を知つていた場合に限る。 [例：海賊版ビジネスソフト等の業務上使用等]
権利管理情報の故意による付加・除去・改変 （第 113 条第 3 項第 1 号・2 号）	権利管理情報として虚偽の情報を故意に付加する行為、および、権利管理情報を故意に除去又は改変する行為 [例：偽の権利管理情報の付加、権利管理情報の削除・改変]
権利管理情報の知情頒布等 （第 113 条第 3 項第 3 号）	権利管理情報の故意による付加・除去・改変が行われた複製物を、情を知つて、頒布し、若しくは頒布の目的をもつて輸入し、若しくは所持し、又は公衆送信・送信可能化する行為 [例：偽の権利管理情報の付加、権利管理情報の削除・改変が行われた複製物の輸入等]
国外頒布商業用レコードの輸入 （第 113 条第 5 項）	専ら国外頒布目的の商業用レコードを、国内頒布目的で輸入、国内で頒布、国内頒布目的で所持する行為。ただし、以下の 4 条件を満たす場合。 ①国内で先に又は同時に発行されている ②情を知っていること ③国外頒布目的レコードの頒布によって国内頒布目的レコードで見込まれる利益が不当に害される場合であること ④最初に国内で発行された日から 4 年が経過していないこと [例：国外販売用音楽レコードの輸入等]
著作者の名誉・声望を害する利用 （第 113 条第 6 項）	著作者の名誉又は声望を害する方法によりその著作物を利用する行為 （著作者人格権を侵害する行為とみなされる。） [例：荘厳な宗教曲を卑猥なショーの BGM として利用等]

（4）刑事上の措置

（罰則）

第百二十条の二　次の各号のいずれかに該当する者は、三年以下の懲役若しくは三百万円以下の罰金に処し、又はこれを併科する。

一　技術的保護手段の回避を行うことをその機能とする装置（当該装置の部品一式であつて容易に組み立てることができるものを含む。）若しくは技術的保護手段の回避を行うことをその機能とするプログラムの複製物を公衆に譲渡し、若しくは貸与し、公衆への譲渡若しくは貸与の目的をもつて製造し、輸入し、若しくは所持し、若しくは公衆の使用に供し、又は当該プログラムを公衆送信し、若しくは送信可能化する行為（当該装置又は当該プログラムが当該機能以外の機能を併せて有する場合にあつては、著作権等を侵害する行為を技術的保護手段の回避により可能とする用途に供するために行うものに限る。）をした者

二　業として公衆からの求めに応じて技術的保護手段の回避を行つた者

・・・・以下略・・・

第 120 条の 2 第 1 号は、技術的保護手段の回避装置や回避プログラムを公衆に譲渡・貸与した者、公衆への譲渡・貸与の目的で製造・輸入・所持した者、公衆の使用に供した者、回避プログラムを公衆送信・送信可能化した者に対して刑事罰を科すもので、3 年以下の懲役若しくは 300 万円以下の罰金、又はこれらの併科を内容とする[58]。

第 120 条の 2 第 2 号は、業として公衆の求めに応じて技術的保護手段の回避行為を行った者に対して刑事罰を科すもので、前号と同じく、3 年以下の懲役若しくは 300 万円以下の罰金、又はこれらの併科を内容とする。

（5）ＴＰＰ協定に伴う制度整備に関する議論

2015 年 10 月 5 日の環太平洋パートナーシップ協定（以下、ＴＰＰ協定と言う。）の大筋合意を受け、文化審議会著作権分科会法制・基本問題小委員会において、我が国著作権法の改正の要否及びその内容に関する検討が行われた後、3 月 8 日、政府が TPP 承認案及び他分野の関連法案とともに著作権法改正案を閣議決定し、国会提出するに至った。経過は以下の通り。

[58] 本条と第３０条第１項第２号との関係を DVD の例で整理すると、2012 年（平成 24 年）改正法が施行した同年１０月１日からは、私的使用目的であっても、DVD にかけられた技術的保護手段を回避して、DVD のデータを自分のパソコンに取り込むことは、民事上違法になる。また、DVDDに施された技術的保護手段の回避装置や回避プログラムを公衆に譲渡・貸与、公衆への譲渡・貸与の目的で製造・輸入・所持、公衆の使用に供し、回避プログラムを公衆送信・送信可能化した場合には、刑罰として「３年以下の懲役または 300 万円以下の罰金、又はそれらの両方（併科）」が科せられる。なお、現在、一般的に音楽 CD には技術的保護手段が施されていないが、このように技術的保護手段が施されていない音楽 CD、私的使用目的で自分のパソコンや携帯音楽プレイヤーに取り込むことそれ自体は民事上違法にはならない

◆　2015 年 11 月 4 日、文化審議会著作権分科会法制・基本問題小委員会（第 6 回）[59]

ＴＰＰ大筋合意を受けて我が国として検討すべき事項として、次の 5 項目が提示された。

①著作物等の保護期間の延長

②著作権侵害罪の一部非親告罪化

③著作物等の利用を管理する効果的な技術的手段（アクセスコントロール等）に関する制度整備

④配信音源の二次使用に対する使用料請求権の付与

⑤法定の損害賠償又は追加的な損害賠償に係る制度整備

③の技術的手段に関しては、現行著作権法においてコピーコントロール技術を有効に機能させるための技術として用いられているアクセスコントロール技術のみを規制しているところ、アクセスコントロール技術全体に関する検討を行うこととしたものである。

◆　2015 年 11 月 11 日、文化審議会著作権分科会法制・基本問題小委員会（第 7 回）[60]

技術的手段に関する基本的な考え方として、「著作物等の利用を管理する効果的な技術的手段（アクセスコントロール）に関する制度整備については、研究開発など一定の公正な目的で行われる権利者に不当な不利益を及ぼさないものが制度の対象外となるよう、適切な例外規定を定めること。」が示された。

◆　2016 年 2 月 10 日、文化審議会著作権分科会法制・基本問題小委員会（第 8 回）[61]

「環太平洋パートナーシップ（ＴＰＰ）協定に伴う制度整備の在り方等について（案)」が提示され、これに対する審議が行われた。技術的手段は、同案第 4 節「著作物等の利用を管理する効果的な技術的手段（アクセスコントロール）に関する制度整備」に述べられ、その主な内容は以下の通り。

①制度整備の方向性については、「アクセスコントロールにより確保される著作権者等の利益は基本的に著作権法による保護の対象とすべきものと評価し、当該手段の回避行為及び回避機器の流通等に一定の救済を認めることが適切である」として法整備の必要性を示した。

②保護対象とする技術的手段の技術方式については、「・・・技術方式を特段限定せず、広く著作物のアクセスを制限する手段全般を対象とすると、自由な情報アクセスを過度に制約するおそれがある。このため、保護対象とする技術的手段の範囲は、現時点で想定される著作権者等の利益の保護と密接な関係を有しているものに限定することが適切である。その際には、同様の趣旨から対象となる技術方式を「信号付加型」及び「暗号型」 の 2 つ

[59] 文化庁 WEB ページ(http://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/hoki/h27_06/)
[60] 文化庁 WEB ページ(http://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/hoki/h27_07/)
[61] 文化庁 WEB ページ(http://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/hoki/h27_08/)

の類型で規定している、現行の不正競争防止法第 2 条第 7 項の例を踏まえることが適当である。」とした。

③保護の内容・方法に関しては、「・・・権利者の利益を保護するため、（アクセスコントロール）回避行為に対して民事上の権利行使が可能となるよう、これを保護の対象とすることが適当である。その方法としては、例えばみなし侵害（第 113 条）の形で保護することが考えられる。」とした。また、アクセスコントロールの回避に使用される装置等を流通させる行為や公衆の求めに応じて反復継続してこれを回避する行為については刑事罰の対象とすることが適切とする一方で、回避行為そのものに対して刑事罰を科すことには慎重であるべきとした。

④例外規定に関しては、「・・・著作権者等の利益の保護及び国民の情報アクセスの自由との均衡を図る必要があることに鑑み、権利者に不当な不利益を及ぼさない形で行われる回避行為が広く例外規定の対象となり得るような制度設計とすることが適当である。」とした。

⑤保護の対象とする権利者の範囲について、「ＴＰＰ協定上規定されていない視聴覚的実演に関する権利や放送事業者の権利についても同様に措置を講ずるのが適当」であるとした。

◆ 2016 年 2 月 24 日、文化審議会著作権分科会法制・基本問題小委員会（第 9 回）[62]

前回までの検討を踏まえ、前回のとりまとめに対し以下の追記を盛り込んだ「報告書（案）」が示された。

②保護対象とする技術的手段の技術方式について、「アクセスコントロールに係る技術的手段の保護の範囲の在り方については、アクセスコントロールを巡る技術動向及び権利者の利益に及ぼす影響、国内外の関連する制度に係る動向等を踏まえ、情報アクセスの自由等とのバランスに留意しつつ、引き続き検討を行うことが適当である。」との認識が追加された。

④回避行為に関する例外規定について、権利者に不当な不利益を及ぼさない形で行われる回避行為を広く例外規定の対象とする場合を前提として、「そのような制度設計をした場合において、不当な不利益を及ぼすか否かの判断に当たっては、今回の制度整備の趣旨及び支分権について既に整備されている各権利制限規定の趣旨を勘案して、適切な結論が導かれることが期待される。」との認識が付記された。

◆ 2016 年 2 月 29 日、文化審議会著作権分科会（第 43 回）[63]

前記した第 9 回文化審議会著作権分科会法制・基本問題小委員会における議論を経た「環太平洋パートナーシップ（ＴＰＰ）協定に伴う制度整備の在り方等に関する報告書」が承認された。

62 文化庁 WEB ページ（http://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/hoki/h27_09/pdf/shiryo_1.pdf）

63 文化庁 WEB ページ（http://www.bunka.go.jp/seisaku/bunkashingikai/chosakuken/bunkakai/43/pdf/shiryo3_2.pdf）

なお、同報告書において、脚注ではあるが、アプリケーション・ソフトウェアのライセンス認証システムの回避ツールの提供について不正競争防止法違反を理由として有罪判決が下された裁判例があるとの記述がなされた。

◆ 2016 年 3 月 8 日、著作権法改正案を国会提出[64]
提出された法律案における関連条文案は次の通り。

第 2 条第 1 項第 20 号「技術的保護手段」の後に、同第 21 号「技術的利用制限手段」を加える。

（定義）
第二条　この法律において、次の各号に掲げる用語の意義は、当該各号に定めるところによる。
・・・・・
二十一　技術的利用制限手段電磁的方法により、著作物等の視聴（プログラムの著作物にあつては、当該著作物を電子計算機において利用する行為を含む。以下この号及び第百十三条第三項において同じ。）を制限する手段（著作権者、出版権者又は著作隣接権者（以下「著作権者等」という。）の意思に基づくことなく用いられているものを除く。）であつて、著作物等の視聴に際し、これに用いられる機器が特定の反応をする信号を著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録し、若しくは送信する方式又は当該機器が特定の変換を必要とするよう著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像を変換して記録媒体に記録し、若しくは送信する方式によるものをいう。

第 113 条のみなし侵害規定に、新たな第 3 項として、以下を加える。

（侵害とみなす行為）
第百十三条
・・・・・
3　技術的利用制限手段の回避（技術的利用制限手段により制限されている著作物等の視聴を当該技術的利用制限手段の効果を妨げることにより可能とすること（著作権者等の意思に基づいて行われる場合を除く。）をいう。第百二十条の二第一号及び第二号において同じ。）を行う行為は、技術的利用制限手段に係る研究又は技術の開発の目的上正当な範囲内で行われる場合その他著作権者等の利益を不当に害しない場合を除き、当該技術的利用制限手段に係る著作権、出版権又は著作隣接権を侵害する行為とみなす。

64 内閣官房 WEB ページ『環太平洋パートナーシップ協定の締結に伴う関係法律の整備に関する法律案』（http://www.cas.go.jp/jp/houan/160308/siryou3.pdf）

第 120 条の 2 を、次の通り改める（改正は下線部）。

（罰則）

第百二十条の二　次の各号のいずれかに該当する者は、三年以下の懲役若しくは三百万円以下の罰金に処し、又はこれを併科する。

一　技術的保護手段の回避若しくは技術的利用制限手段の回避を行うことをその機能とする装置（当該装置の部品一式であつて容易に組み立てることができるものを含む。）若しくは技術的保護手段の回避若しくは技術的利用制限手段の回避を行うことをその機能とするプログラムの複製物を公衆に譲渡し、若しくは貸与し、公衆への譲渡若しくは貸与の目的をもつて製造し、輸入し、若しくは所持し、若しくは公衆の使用に供し、又は当該プログラムを公衆送信し、若しくは送信可能化する行為（当該装置又は当該プログラムが当該機能以外の機能を併せて有する場合にあつては、著作権等を侵害する行為を技術的保護手段の回避により可能とし、又は第百十三条第三項の規定により著作権、出版権若しくは著作隣接権を侵害する行為とみなされる行為を技術的利用制限手段の回避により可能とする用途に供するために行うものに限る。）をした者

二　業として公衆からの求めに応じて技術的保護手段の回避又は技術的利用制限手段の回避を行つた者

三　営利を目的として、第百十三条第四項の規定により著作者人格権、著作権、実演家人格権又は著作隣接権を侵害する行為とみなされる行為を行つた者

四　営利を目的として、第百十三条第六項の規定により著作権又は著作隣接権を侵害する行為とみなされる行為を行つた者。

２．３　不正競争防止法と著作権法による規制の対比（補論）[65]

不正競争防止法 2 条 1 項第 11 号及び第 12 号は、技術的制限手段に係る不正行為を規制する。同第 11 号及び第 12 号は、1999 年（平成 11 年）改正法により新設され、同年 10 月 1 日から施行された。2011 年（平成 23 年）改正法（平成 23 年 12 月 1 施行）では、規制対象装置等の範囲が拡大されるとともに、技術的制限手段回避・無効化措置等の提供行為に対し刑事罰（第 21 条第 2 項第 4 号、第 22 条）が導入され、技術的制限手段に係る規制が強化された。

他方、著作権法においても、1999 年（平成 11 年）改正法により、技術的保護手段の回避行為に関する規定が設けられた後、2012 年（平成 24 年）改正法により技術的保護手段の範囲が広げられ、規制が強化された。

不正競争防止法の技術的制限手段に関する規制と著作権法の技術的保護手段に関する規制とは、目的においてどのように異なるのか。また、両者間にはどのような異同があり、それぞれいかなる行為を規制しているのかを、以下に比較する。

（１）規制の目的

①不正競争防止法における技術的制限手段

不正競争防止法第 2 条第 1 項第 11 号および第 12 号は、コンテンツ提供事業者間の競争秩序を維持するため、管理技術の無効化機能を有する機器やプログラムの提供を不正競争行為として規制する。すなわち、コンテンツ提供事業者は、コンテンツを保護するためコピー管理技術やアクセス管理技術を導入しているが、それを無効化する機器やプログラムが提供されれば、コンテンツ事業者はこれに対処するために、さらなる労力・資金を投入せざるを得ない。このような事態を回避・無効化し、コンテンツ提供事業者の存立を確保し、事業者間の競争秩序を維持することが、不正競争防止法による技術的制限手段の規制の目的である。

②著作権法における技術的保護手段

著作権法は著作権者等の保護を目的とし、著作権者等でないコンテンツ提供事業者を保護するものではない。すなわち、技術的保護手段は、著作権者等の利益を著しく害する複製を未然に防ぐ効果的な手段であるが、この場合に、技術的保護手段の回避行為を放置すれば、著作権保護の実効性が損なわれ、著作権者等は著作物等の供給を躊躇する結果となる。そこで、著作権法は、著作権保護の実効性を確保するため、著作権の例外となる私的複製から技術的保護手段の回避を知りながら行う私的複製を除外し、技術的保護手段の回避装置またはプログラムの複製物の譲渡行為等に対して刑事罰を科す。

---

[65] 本項は、『不正競争防止の法実務（改訂版）』（三協法規出版・2013 年）269 頁～276 頁に掲載された井奈波朋子『不正競争防止法２条１項１０号及び１１号所定の「技術的手段に対する不正競争」（著作権法との対比）』からの転載を基礎として、井奈波氏本人に加筆修正いただいた。

（２）規制対象（技術的制限手段と技術的保護手段）

不正競争防止法第２条第７項に定義される技術的制限手段と、著作権法第２条第１項第２０号に定義される技術的保護手段との異同は、以下の表に示すとおりである。

<table>
<tr><th colspan="4">技術的制限手段</th><th colspan="4">技術的保護手段</th></tr>
<tr><td colspan="4">電磁的方法により、</td><td colspan="4">電磁的方法により、</td></tr>
<tr><td colspan="4">①影像・音の視聴、②プログラムの実行、③影像・音・プログラムの記録を制限する手段であって、</td><td colspan="4">著作者人格権・著作権・実演家人格権・著作隣接権を侵害する行為の防止又は抑止をする手段であって</td></tr>
<tr><td colspan="2" rowspan="2">視聴等機器が特定の反応をする信号を影像・音・プログラムとともに</td><td colspan="2" rowspan="2">視聴等機器が特定の変換を必要とするよう影像・音・プログラムを変換して、</td><td colspan="4">著作物・実演・レコード・放送・有線放送の利用に際し、</td></tr>
<tr><td colspan="2">機器が特定の反応をする信号を著作物・実演・レコード・放送・有線放送に係る音・影像とともに</td><td colspan="2">機器が特定の変換を必要とするよう著作物・実演・レコード・放送・有線放送に係る音・影像を変換して</td></tr>
<tr><td>記録媒体に記録する方式によるもの</td><td>送信する方式によるもの</td><td>記録媒体に記録する方式によるもの</td><td>送信する方式によるもの</td><td>記録媒体に記録する方式によるもの</td><td>送信する方式によるもの</td><td>記録媒体に記録する方式によるもの</td><td>送信する方式によるもの</td></tr>
<tr><td colspan="2">非暗号型</td><td colspan="2">暗号型</td><td colspan="2">非暗号型</td><td colspan="2">暗号型</td></tr>
</table>

※網掛け部分は、2012 年（平成２４年）著作権法改正による追加。

①技術的制限手段

不正競争防止法は、コンテンツ提供事業者間の公正な競争を確保することを目的としているので、技術的制限手段は、影像・音の視聴、プログラムの実行、影像・音・プログラムの記録を制限する手段と定められ、コピー等利用制限技術だけでなく、アクセス制限技術をも対象とする。

②技術的保護手段

著作権法の技術的保護手段は、①電磁的方法により著作権等の侵害行為を防止又は抑止するものであること、②著作権者等の意思に基づいて用いられているものであること、③機器が特定の反応をする信号を著作物等とともに記録・送信する方式によるか、又は、機器が特定の変換を必要とするよう著作物等を変換して記録・送信する方式によるものであることを要件とし、コピーコントロール技術（コピー等利用制限技術に含まれる）と、コピーコントロール技術を有効に機能させるためのアクセスコントロール技術（アクセス制限技術に含まれる）を対象とする。

（３）規制される行為

①不正競争防止法により規制される行為

不正競争防止法は、技術的制限手段回避・無効化装置またはプログラムの提供行為を規制対象とするものであり、個々の技術的制限手段の無効化行為を規制対象とするものではない。

2011 年（平成 23 年）改正により、技術的制限手段の回避・無効化措置等に係る規制が強化された。改正前は、技術的制限手段の効果を妨げることにより無断コピーや無断視聴を可能とする機能「のみ」を有する装置または当該機能「のみ」を有するプログラムが対象となっていたが、改正により「のみ」要件は削除された。

また、これら機能を有する装置には、当該装置を組み込んだ機器のほか、当該装置の部品一式であって容易に組み立てることができるものを含む。このうち、部品一式で容易に組み立てることができるものが規制対象となることは、2011 年（平成 23 年）改正により追加された。

さらに、2011 年（平成 23 年）改正前は、回避・無効化機能のみを有する装置またはプログラムが規制対象であったため、回避・無効化機能とその他の機能を併せて有する装置等は規制対象外であった。2011 年（平成 23 年）改正法により、「当該装置または当該プログラムが、当該機能以外の機能を併せて有する場合」であっても、「映像の視聴等を当該技術的制限手段の効果を妨げることにより可能とする用途に供するために行うもの」が、規制対象とされた。

ただし、いわゆる無反応機器と呼ばれるコンテンツに付された技術的制限手段を検知しない機器については、これを規制すると、記録や視聴等を制限するあらゆる信号に対応する措置を施すよう強制することになるとして、不正競争の対象としないことが適当とされた。

第 11 号及び第 12 号に該当する行為によって、営業上の利益を侵害されまたは侵害されるおそれがある者は、民事上の差止請求を行うことができ（第 3 条）、故意または過失によりこれらの行為により営業上の利益を侵害した者に対して損害賠償請求ができる（第 4 条）。

さらに、2011 年（平成 23 年）改正法は、不正の利益を得る目的で、又は営業上技術的制限手段を用いている者に損害を加える目的で、第 2 条第 1 項第 11 号又は第 12 号に掲げる不正競争を行った者に対する刑事処罰を導入し、技術的制限手段に対する規制を強化した（第 21 条第 2 項第 4 号、第 22 条）。

不正競争防止法には適用除外があり、技術的制限手段の試験又は研究のために用いられる不正競争防止法 2 条 1 項第 11 号及び第 12 号に規定する装置若しくはこれらの号に規定するプログラムを記録した記録媒体若しくは記憶した機器を、譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、または当該プログラムを電気通信回線を通じて提供する行為については、民事上または刑事上の制裁の対象にならない（不正競争防止法 19 条第 1 項第 7 号）。

また、2011 年（平成 23 年）の関税法改正により、技術的制限手段回避・無効化措置は輸出入禁止品に追加された(関税法第 69 条の 2 第 1 項第 4 号)。

②著作権法により規制される行為

私的使用目的で行われる複製は著作権の権利制限の対象となるが、技術的保護手段の回避行為により可能となりまたはその結果に障害が生じないようになった複製を、その事実を知りながら行う場合、その適用除外となる（著作権法第 30 条第 1 項第 2 号)。したがって、不正競争防止法においては、個々の技術的制限手段の無効化行為は規制対象とならないのに対し、著作権法においては、技術的保護手段を回避して行う個々の複製行為は、複製権侵害として民事上違法となる。ただし、刑事罰の対象にはならない。

2012 年（平成 24 年）改正法においては、第 2 条第 1 項第 20 号に規定する特定の変換を必要とするよう変換された著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像の復元（著作権等を有する者の意思に基づいて行われるものを除く）を行うことにより可能となりまたはその結果に障害を生じないようになった複製を、その事実を知りながら行う場合も、規制対象とした(第 30 条第 1 項第 2 号)。つまり、私的使用目的で、暗号方式による技術的保護手段の回避により可能となった複製を、その事実を知りながら行う場合も、民事上違法となる。

さらに、著作権法は、技術的保護手段回避装置・回避プログラムの複製物の公衆への譲渡等を行った者（著作権法 120 条の 2 第 1 号)、業として公衆からの求めに応じて技術的保護手段の回避を行った者（同第 2 号）に対して刑事罰を科す。第 1 号にいう回避装置には、当該装置の部品一式であって容易に組み立てることができるものを含む。また、当該装置または当該プログラムが当該機能以外の機能を併せて有する場合にあっては、著作権等を侵害する行為を技術的保護手段の回避により可能とする用途に供するために行うものに限る。なお、著作権法においても無反応機器は規制対象とならない。

また、著作権法には、不正競争防止法第 19 条第 1 項第 7 号のような適用除外規定はない[66]。むしろ、第 30 条第 1 項第 2 号により、技術的保護手段を回避することで可能となった複製を、その事実を知りながら行った場合、たとえ私的使用目的であっても複製権は制限されずに、民事的に違法と評価される。これは、技術的保護手段を施した著作権者の期待（無断複製されて流通しないことを前提とするビジネスモデル）を守る趣旨であり、WIPO 著作権条約第 11 条、WIPO 実演・レコード条約第 18 条に対応したものである[67]。

他方、TPP 大筋合意を受けた文化審議会著作権分科会が 2016 年（平成 28 年）2 月 29 日、「・・・著作権者等の利益の保護及び国民の情報アクセスの自由との均衡を図る必要があることに鑑み、権利者に不当な不利益を及ぼさない形で行われる回避行為が広く例外規定の対象となり得るような制度設計とすることが適当である。」とする報告をとりまとめたことから、技術的保護手段の回避に係る例外規定の立法の方向性は固まったと言うことができる。

---

[66] 技術開発の円滑化のための規定として第３０条の４が設けられているが、本条は、例えば新しいテレビの開発段階における色調開発で他人の公表された著作物（映画やテレビ放送番組等）を利用することを合法としたものであり、新たな技術的保護手段を開発するために既存の技術的保護手段を回避して他人の著作物を利用することを射程とはしていないと考えられる。また、本条に言う技術は、著作物の利用に関する技術（録音、録画、送信、通信、上映、視聴、再生、翻訳、翻案等の支分権に規定された行為に関する技術）であり、技術的保護手段が本条に言う著作物利用技術に該当するか否かという別の問題も生じ得る。

[67] 前掲・中山 291 頁～292 頁。

③民事上の措置

不正競争防止法においては、以下の行為に対し、差止請求権（第３条）、損害賠償請求権（第４条）が及ぶ。

<table>
<tr><td colspan="2">不正競争防止法第２条第１項</td></tr>
<tr><td>第１１号</td><td>第１２号</td></tr>
<tr><td>営業上用いられている技術的制限手段により制限されている影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を当該技術的制限手段の効果を妨げることにより可能とする機能を有する装置若しくは当該機能を有するプログラムを記録した記録媒体若しくは記憶した機器を</td><td>他人が特定の者以外の者に影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録をさせないために営業上用いている技術的制限手段により制限されている影像若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を当該技術的制限手段の効果を妨げることにより可能とする機能を有する装置若しくは当該機能を有するプログラムを記録した記録媒体若しくは記憶した機器を、当該特定の者以外の者に</td></tr>
<tr><td colspan="2">譲渡し、引き渡し、譲渡若しくは引渡しのために展示し、輸出し、若しくは輸入し、又は当該機能を有するプログラムを、電気通信回線を通じて提供する行為</td></tr>
</table>

著作権法においては、以下の行為に対し、差止請求権（第１１２条）が及ぶ。また、かかる侵害については、民法第７０９条による損害賠償請求が可能である。

<table>
<tr><td>著作権法第３０条第１項第２号</td></tr>
<tr><td>技術的保護手段の回避により可能となり、又はその結果に障害が生じないようになつた複製を、その事実を知りながら行う場合</td></tr>
</table>

④刑事上の措置

不正競争防止法及び著作権法において、刑事責任を負う者、及び、その内容は以下の通り。

<table>
<tr><td>不正競争防止法第２１条第２項第４号</td><td>著作権法第１２０条の２</td></tr>
<tr><td rowspan="2">不正の利益を得る目的で、又は営業上技術的制限手段を用いている者に損害を加える目的で、第２条第１項第１１号または第１２号に掲げる不正競争を行った者</td><td>技術的保護手段の回避を行うことをその機能とする装置若しくは技術的保護手段の回避を行うことをその機能とするプログラムの複製物を公衆に譲渡し、若しくは貸与し、公衆への譲渡若しくは貸与の目的をもつて製造し、輸入し、若しくは所持し、若しくは公衆の使用に供し、又は当該プログラムを公衆送信し、若しくは送信可能化する行為をした者（第１号）</td></tr>
<tr><td>業として公衆からの求めに応じて技術的保護手段の回避を行った者（第２号）</td></tr>
<tr><td>5 年以下の懲役若しくは 500 万円以下の罰金に処し、又はこれを併科する</td><td>3 年以下の懲役もしくは 300 万円以下の罰金、またはこれを併科する</td></tr>
</table>

２．４　不正アクセス禁止法における規制

不正アクセス禁止法は、第 2 条第 4 項及び第 3 条によって、他人の識別符号を無断で使ってアクセス制御されているサーバ等に不正にアクセスする行為及びセキュリティ･ホール[68]を攻撃してシステムやプログラムを不正利用する行為を禁止する。また、第 4 条によって、他人の識別符号を不正に取得する行為を、第 5 条によって不正アクセス行為を助長する行為を、第 6 条によって他人の識別符号を不正に保管する行為を、第 7 条によって識別符号の入力を不正に要求する行為(いわゆるフィッシング行為)を、それぞれ禁止する。

（１）識別記号、アクセス制御機能及び不正アクセス行為の定義

①識別記号

（定義）
第二条　（１項略）
２　この法律において「識別符号」とは、特定電子計算機の特定利用をすることについて当該特定利用に係るアクセス管理者の許諾を得た者（以下「利用権者」という。）及び当該アクセス管理者（以下この項において「利用権者等」という。）に、当該アクセス管理者において当該利用権者等を他の利用権者等と区別して識別することができるように付される符号であって、次のいずれかに該当するもの又は次のいずれかに該当する符号とその他の符号を組み合わせたものをいう。
一　当該アクセス管理者によってその内容をみだりに第三者に知らせてはならないものとされている符号
二　当該利用権者等の身体の全部若しくは一部の影像又は音声を用いて当該アクセス管理者が定める方法により作成される符号
三　当該利用権者等の署名を用いて当該アクセス管理者が定める方法により作成される符号

第 1 号の符号はパスワードを、第 2 号の符号は指紋・虹彩・音声等を、また、その他の符号は ID を指す。

[68] アクセス制御機能のプログラムの瑕疵、アクセス管理者の設定上のミス等のコンピュータ・システムにおける安全対策上の不備を言う。警察庁『不正アクセス行為の禁止等に関する法律の解説』を参照。
(https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf)

②アクセス制御機能

（定義）

第２条

３　この法律において「アクセス制御機能」とは、特定電子計算機の特定利用を自動的に制御するために当該特定利用に係るアクセス管理者によって当該特定電子計算機又は当該特定電子計算機に電気通信回線を介して接続された他の特定電子計算機に付加されている機能であって、当該特定利用をしようとする者により当該機能を有する特定電子計算機に入力された符号が当該特定利用に係る識別符号（識別符号を用いて当該アクセス管理者の定める方法により作成される符号と当該識別符号の一部を組み合わせた符号を含む。次項第一号及び第二号において同じ。）であることを確認して、当該特定利用の制限の全部又は一部を解除するものをいう。

③不正アクセス行為

（定義）

第２条

４　この法律において「不正アクセス行為」とは、次の各号のいずれかに該当する行為をいう。

一　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号を入力して当該特定電子計算機を作動させ、当該アクセス制御機能により制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者又は当該識別符号に係る利用権者の承諾を得てするものを除く。）

二　アクセス制御機能を有する特定電子計算機に電気通信回線を通じて当該アクセス制御機能による特定利用の制限を免れることができる情報（識別符号であるものを除く。）又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為（当該アクセス制御機能を付加したアクセス管理者がするもの及び当該アクセス管理者の承諾を得てするものを除く。次号において同じ。）

三　電気通信回線を介して接続された他の特定電子計算機が有するアクセス制御機能によりその特定利用を制限されている特定電子計算機に電気通信回線を通じてその制限を免れることができる情報又は指令を入力して当該特定電子計算機を作動させ、その制限されている特定利用をし得る状態にさせる行為

④不正アクセス行為の禁止

第３条　何人も、不正アクセス行為をしてはならない。

⑤その他の禁止行為

（他人の識別符号を不正に取得する行為の禁止）

第４条　何人も、不正アクセス行為（第二条第四項第一号に該当するものに限る。第六条及び第十二条第二号において同じ。）の用に供する目的で、アクセス制御機能に係る他人の識別符号を取得してはならない。

（不正アクセス行為を助長する行為の禁止）

第５条　何人も、業務その他正当な理由による場合を除いては、アクセス制御機能に係る他人の識別符号を、当該アクセス制御機能に係るアクセス管理者及び当該識別符号に係る利用権者以外の者に提供してはならない。

（他人の識別符号を不正に保管する行為の禁止）

第６条　何人も、不正アクセス行為の用に供する目的で、不正に取得されたアクセス制御機能に係る他人の識別符号を保管してはならない。

（識別符号の入力を不正に要求する行為の禁止）

第７条　何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。

一　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為

二　当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為

第 1 号は、他人の識別符号を無断で使って不正にアクセスする行為を言う。第 2 号及び第 3 号は、セキュリティ・ホールを攻撃して不正にアクセスする行為を言う。

（2）禁止行為及び対応する刑事上の措置

第 2 条第 4 項から第 7 条までの禁止される行為ト罰則との対応関係は以下の通り。

禁止される行為	内容	罰則
第２条第４項及び第３条 不正アクセス行為	他人の識別符号を無断で使って不正にアクセスする行為（第２条第４項第１号）	３年以下の懲役又は 100 万円以下の罰金
	セキュリティ・ホールを攻撃して不正にアクセスする行為（同項第２号、第３号）	
第４条 他人の識別符号を不正に取得する行為の禁止	不正アクセス行為をする目的で、他人の識別符号を取得する行為	１年以下の懲役又は 50 万円以下の罰金
第５条 不正アクセス行為を助長する行為	他人の識別符号を無断で第三者に販売・提供等をする行為	30 万円以下の罰金
	不正アクセス行為をする目的がある者に、そのことを知りながら、他人の識別符号を販売・提供等をする行為	１年以下の懲役又は 50 万円以下の罰金
第６条 他人の識別符号を不正に保管する行為	不正アクセス行為をする目的で、他人の識別符号を保管する行為	１年以下の懲役又は 50 万円以下の罰金
第７条 識別符号の入力を不正に要求する行為の禁止	フィッシングサイトを公開することや、電子メールによって識別符号を騙し取るフィッシング行為	１年以下の懲役又は 50 万円以下の罰金

不正アクセス禁止法における禁止行為と罰則[69]

第 3 条は、第 2 条第 4 項で規定する①他人の識別符号を悪用することにより、本来アクセスする権限のないコンピュータを利用する行為（すなわち、正規の利用権者等である他人の識別符号を無断で入力することによってコピー等利用制限を解除し、特定利用ができる状態にする行為）、②いわゆるセキュリティ・ホール（アクセス制御機能のプログラムの瑕疵、アクセス管理者の設定上のミス等のコンピュータ・システムにおける安全対策上の不備)を攻撃する行為を禁止する。

なお、セキュリティ・ホール攻撃による不正アクセスとは、特殊な情報（データ）又は指令（コマンド）を入力して行った場合のことを言い、他人の ID・パスワード等の識別符号は特殊な情報又は指令には当たらない[70]。このことから、例えば、ハッカーが他人のパスワードを高速自動生成したような場合などにおいて、その識別符号で不正アクセスした場合、セキュリティ・ホール攻撃による不正アクセスには該当しない。なお、そのような識別符号を用いて不正なアクセスが実現した時点で、当該識別符号は「他人の識別符号」に該当し、当該アクセスは第２条第４項第 1 号の不正アクセスと評価されるものと考え得る。

第 4 条は、他人の識別符号を不正アクセス行為の用に供する目的で取得（取得者自身に他人の識別符号を用いて不正アクセス行為を行う意図があって取得する場合のほか、不正アクセス行為

[69] 埼玉県警察サイバー犯罪対策課の WEB 掲載資料を参考に作成。
（http://www.police.pref.saitama.lg.jp/c0070/kurashi/cyber-fusei-ho.html）
[70] 前掲注・警察庁『不正アクセス行為の禁止等に関する法律の解説』。

を行う意図がある第三者に提供する意図を持って取得する場合も含む）を禁止する[71]。

第 5 条は、他人の識別符号を無断で第三者に販売・提供等をする行為、不正アクセス行為をする目的がある者に、そのことを知りながら、他人の識別符号を販売・提供等をする行為を禁止する。

第 6 条は、不正アクセス行為をする目的で、不正に取得された他人の識別符号を保管する行為を禁止するもので、不正アクセス行為を禁止することの実効性を確保するため、準備行為である保管が行われた時点で違法とする規定である。USB、使用する端末機器はもとより、紙媒体への記録保存も、故意であれば、「保管」に該当する[72]。

第 7 条は、サイト構築型フィッシング行為、及び、電子メール送信型フィッシング行為を禁止する。サイト構築型フィッシング行為とは、「正規のアクセス管理者が公開したウェブサイトであると誤認させ」かつ「ＩＤ・パスワードを入力することを求める旨の情報がある」ウェブサイトをネットワーク上に公開して公衆が見ることができる状態に置く行為を言う。電子メール送信型フィッシング行為とは、「正規のアクセス管理者が送信した電子メールであると誤認させ」かつ「ＩＤ・パスワードを入力することを求める旨の情報がある」電子メールを、利用権者に送信する行為を言う。いずれも、実際に他人の識別符号を取得することは要件ではない[73]。

コンテンツビジネス関連では、オンラインゲームの運営者のサーバに他人の ID やパスワードを使用してアクセスしたとして逮捕等されるケースが見受けられる[74]。他人の ID やパスワードを使用していることから、第 2 条 4 項第 1 号に該当する類型であると考えられる。

刑事処分に至った事案としては、オンラインゲーム「リネージュ 2」のアイテムを転売する目的で、マンガ喫茶に置かれたパソコンから他人の ID を不正に入手して、ゲーム運営サーバに不正にアクセスした会社員男性が、2010 年（平成 22 年）12 月 14 日、川崎簡易裁判所から罰金 30 万円の略式命令を受けた事例がある。

---

71 例えば、インターネット上での検索中にたまたま他人の識別符号が表示された場合や、他人の識別符号が電子メールで勝手に送りつけられてきたような場合には、不正アクセス行為をする目的で取得することの認識がないことから、本条に違反しない。（不正アクセス対策法研究会編著「逐条 不正アクセス行為の禁止等に関する法律（第２版）」不正アクセス対策法研究会編著 83８３頁）

72 なお、本条に言う「不正に取得された」識別符号とは、第４条該当行為により取得された識別符号や第５条該当行為により提供された識別符号が該当するが、これらに限定されない。例えば、不正アクセス行為の用に供する目的以外の別の目的で他人の識別符号を正当な権限なく取得した場合、第４条の禁止対象とはならないが、当該識別符号を不正アクセス行為の用に供する目的で保管した場合には本条に該当することとなる。（前掲・「逐条 不正アクセス行為の禁止等に関する法律（第２版）」不正アクセス対策法研究会編著９４頁）

73 ただし、利用権者を誤認させようとする意図を持っていない場合は、本条に違反しない。警察庁『不正アクセス行為の禁止等に関する法律の解説』(https://www.npa.go.jp/cyber/legislation/pdf/1_kaisetsu.pdf)

74 本報告書第Ⅲ章２．３を参照。

２．５　刑法１６１条の２　私電磁的記録不正作出及び供用罪

技術的手段の回避・無効化に適用され得る私電磁的記録不正作出及び供用罪の規定は以下のとおり。

（電磁的記録不正作出及び供用）

第百六十一条の二　人の事務処理を誤らせる目的で、その事務処理の用に供する権利、義務又は事実証明に関する電磁的記録を不正に作った者は、５年以下の懲役又は５０万円以下の罰金に処する。

２　前項の罪が公務所又は公務員により作られるべき電磁的記録に係るときは、１０年以下の懲役又は１００万円以下の罰金に処する。

３　不正に作られた権利、義務又は事実証明に関する電磁的記録を、第１項の目的で、人の事務処理の用に供した者は、その電磁的記録を不正に作った者と同一の刑に処する。

４　前項の罪の未遂は、罰する。

人の事務処理を誤らせる目的で、権利・義務に関する電磁的記録（銀行の元帳ファイル、自動改札定期券の残高記録等）や事実証明に関する電磁的記録（ホストコンピュータ内の顧客データベースファイル等）を、不正に作った者（第１項）及び利用に供した者（第３項）を罰する。

コンテンツビジネスとの関係では、放送分野におけるアクセス制限技術である B-CAS カードの改造事案への適用、及び不正改造された B-CAS カードの使用事案への適用事例がある。また、オンラインゲーム関係で、チート・ツールを使用してアイテム等を不正に取得等したとして本条が適用された事案がある[75]。さらに、オンラインゲーム関係では、他人の ID・パスワードを不正使用した行為について、不正アクセス禁止法に加えて本条が適用された事例が散見される[76]。

[75] ゲーム運営者は、チート・ツールの提供及びゲーム内アイテムの不正取得で、不正競争防止法違反、私電磁的記録不正作出罪に問われ有罪判決が言い渡された事例を明らかにし、注意を呼び掛けている。
（https://ava.pmang.jp/new_notices/1433?kind_index=6）

[76] 本報告書第Ⅲ章２．４を参照。

２．６　刑法第１６８条の２・同３　不正指令電磁的記録作成・提供・取得保管罪

（不正指令電磁的記録作成等）
第百六十八条の二　正当な理由がないのに、人の電子計算機における実行の用に供する目的で、次に掲げる電磁的記録その他の記録を作成し、又は提供した者は、３年以下の懲役又は 50 万円以下の罰金に処する。
一　人が電子計算機を使用するに際してその意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録
二　前号に掲げるもののほか、同号の不正な指令を記述した電磁的記録その他の記録
２　正当な理由がないのに、前項第１号に掲げる電磁的記録を人の電子計算機における実行の用に供した者も、同項と同様とする。
３　前項の罪の未遂は、罰する。

（不正指令電磁的記録取得等）
第百六十八条の三　正当な理由がないのに、前条第１項の目的で、同項各号に掲げる電磁的記録その他の記録を取得し、又は保管した者は、２年以下の懲役又は 30 万円以下の罰金に処する。

人が電子計算機（コンピュータ）を使用するに際して、その意図に沿うべき動作をさせず、又はその意図に反する動作をさせるべき不正な指令を与える電磁的記録等を作成・提供、取得・保管した場合の罰則を規定する。不正指令電磁的記録とは、コンピュータ・ウィルス等が想定されているため、本罪は「ウィルス作成罪」ともよばれる。

第 168 条の 2 は作成・提供罪、第 168 条の 3 は取得・保管罪をそれぞれ規定する。

コンテンツビジネスとの関係では、オンラインゲームの他人のＩＤやパスワードを不正に入手するためのコンピュータ・ウィルスを作成したとして、不正アクセス禁止法とともに本条が適用された事案がある[77]。「作成」が問われたことから、第 168 条の 2 作成罪が適用されたと考えられる。

[77] 本報告書第Ⅲ章２．５を参照。

２．７　刑法第２３４条の２　電子計算機損壊等業務妨害罪

（電子計算機損壊等業務妨害）
第二百三十四条の二　人の業務に使用する電子計算機若しくはその用に供する電磁的記録を損壊し、若しくは人の業務に使用する電子計算機に虚偽の情報若しくは不正な指令を与え、又はその他の方法により、電子計算機に使用目的に沿うべき動作をさせず、又は使用目的に反する動作をさせて、人の業務を妨害した者は、五年以下の懲役又は百万円以下の罰金に処する。
２　前項の罪の未遂は、罰する。

人の業務に使用する電子計算機（コンピュータ）に対する加害行為による業務妨害行為を処罰の対象とするものである。コンテンツビジネスとの関係では、オンライン対戦型ゲームで、チート・ツールの使用によってサーバコンピュータに対し意図しない不正な指令を与えて、オンラインゲーム事業者の運営業務に支障を生じさせたとして、本条が適用されたケースがある[78]。

２．８　刑法第２４６条の２　電子計算機使用詐欺罪

（電子計算機使用詐欺）
第二百四十六条の二　前条に規定するもののほか、人の事務処理に使用する電子計算機に虚偽の情報若しくは不正な指令を与えて財産権の得喪若しくは変更に係る不実の電磁的記録を作り、又は財産権の得喪若しくは変更に係る虚偽の電磁的記録を人の事務処理の用に供して、財産上不法の利益を得、又は他人にこれを得させた者は、十年以下の懲役に処する

人の事務処理に使用する電子計算機（コンピュータ）に虚偽の情報若しくは不正な指令を与えて財産権の得喪・変更に係る不実の電磁的記録を作る行為（不実の電磁的記録の作出）と、財産権の得喪・変更に係る虚偽の電磁的記録を人の事務処理の用に供する行為（電磁的記録の供用）の、二つの行為によって、財産上の利得を得ること等を処罰の対象とするものである。

「虚偽の情報」とは、コンピュータを使用する事務処理システムで予定されている事務処理の目的に照らしてその内容が真実に反する情報を指す。また、「不正な指令」とは、コンピュータを使用する事務処理の場面において与えられるべきでない情報を言う。

本規定は、コンピュータを使用する事務処理システムで用いられる電磁的記録を改変することによって財産上の利得を得ることを罰するもので、例えば、銀行のオンラインシステムに虚偽の振込送金情報を与える、プログラムを改変して預金を引き出しても残金が減少しないようにする、預金残高を増額するなどの行為が、本条に言う財産上不法の利益を得る行為に該当する。電子マ

[78] 本報告書第Ⅲ章２．６を参照。

ネーの利用権不正取得に本罪の成立が認められた裁判例もある[79]。

コンテンツビジネスとの関係では、ネットワークに不正アクセスしたとして不正アクセス禁止法に問われるとともに、映像パッケージの不正購入、オンラインゲームの仮想通貨の不正取得を行ったとして本条が適用された例が報道されているが、報道からはその具体的な態様を読み取ることはできない[80]。

３　関税法

（１） 輸出してはならない貨物

（輸出してはならない貨物）

第六十九条の二　次に掲げる貨物は、輸出してはならない。

三　特許権、実用新案権、意匠権、商標権、著作権、著作隣接権又は育成者権を侵害する物品

四　不正競争防止法　（平成五年法律第四十七号）第二条第一項第一号から第三号まで、第十一号又は第十二号（定義）に掲げる行為（これらの号に掲げる不正競争の区分に応じて同法第十九条第一項第一号から第五号まで又は第八号　（適用除外等）に定める行為を除く。）を組成する物品

（２） 輸入してはならない貨物

（輸入してはならない貨物）

第六十九条の十一　次に掲げる貨物は、輸入してはならない。

九　特許権、実用新案権、意匠権、商標権、著作権、著作隣接権、回路配置利用権又は育成者権を侵害する物品

十　不正競争防止法第二条第一項第一号から第三号まで、第十一号又は第十二号（定義）に掲げる行為（これらの号に掲げる不正競争の区分に応じて同法第十九条第一項第一号から第五号まで又は第八号（適用除外等）に定める行為を除く。）を組成する物品

[79] 大山弘『電子マネー利用権の不正取得と電子計算機使用詐欺罪の成否－最一小決平 18・2・14 刑集 60 巻 2 号 165（肯定）－』（2006 年 12 月・神戸学院法学第 36 巻第 2 号）

[80] 本報告書第Ⅲ章２．７を参照。

（3）技術的制限手段回避・無効化装置等について関税法上適用され得る罰則

名称	内容	法定刑	備考
輸出入してはならない貨物の密輸出入犯	関税法第 69 条の 2 第 1 項第 2 号、第 3 号及び第 4 号、第 69 条の 11 第 1 項第 7 号から第 10 号までの貨物	10 年以下の懲役若しくは 1,000 万円以下の罰金又は併科	未遂も同罪（予備は 5 年・500 万円）
輸入の目的以外の目的で本邦に到着した貨物の蔵置及び運搬犯	関税法第 69 条の 11 第 1 項第 8 号から第 10 号までの貨物（回路配置利用権のみを侵害するものを除く。）	10 年以下の懲役若しくは 700 万円以下の罰金又は併科	未遂も同罪（予備は 5 年・300 万円）

第Ⅲ章　我が国における事案

１　技術的手段回避･無効化事犯に係る検挙件数

2011 年（平成 23 年）12 月 1 日の不正競争防止法における刑事罰の導入及び 2012 年（平成 24 年）10 月 1 日の著作権法改正における保護範囲の拡大から、2016 年（平成 28 年）1 月 14 日までの技術的手段回避・無効化事犯に係る検挙件数は以下のとおり。

不正競争防止法事犯が、著作権法事犯に比して多い。また、著作権法事犯は第 120 条の 2 第 1 号違反（回避装置・プログラムの譲渡等）のみであり、同第 2 号違反（業として公衆の求めに応じて行う回避行為）の検挙例はない。

	不正競争防止法（法第21条第2項第4項）（法第2条第1項第11号・第12号）		著作権法（法第120条の2第1号）		著作権法（法第120条の2第2号）	
	件数	人員	件数	人員	件数	人員
平成２３年度	０	０	０	０	０	０
平成２４年度	５７	２０	１	１	０	０
平成２５年度	６６	３０	４	２	０	０
平成２６年度	３９	２８	４	１	０	０
平成２７年度	４７	２９	５	６	０	０

技術的制限手段回避・無効化事犯検挙件数（平成 28 年 1 月 14 日現在）[81]

※検挙人員は、刑法犯において警察などが検挙した事件の被疑者の数を言う。
検挙件数は、刑法犯において警察などで事件を検察官に送致・送付又は微罪処分（犯罪が軽微であるため、検察に送致することなく刑事手続を終了させる処分）にした件数を言う。

２　事件の記録

2010 年（平成 22 年）1 月 1 日から 2016 年（平成 28 年）1 月 31 日までの 6 年余の間に我が国で起きたコンテンツ提供に係る技術的手段の回避・無効化の関連事件を、関係団体等[82]より提供を受けた資料及び報道記事等により収集した情報の範囲で整理する。したがって、以降の記載は全ての関連事件を網羅しているものではないこと、また、記載した事件の内容や結果は、基本的に

[81] 警察庁より本調査のために提供いただいた。
[82] 情報収集にあたり、一般社団法人コンピュータソフトウェア著作権協会、ザ・ソフトウェア・アライアンス（BSA）、株式会社 ビーエス・コンディショナルアクセスシステムズ（B-CAS）に、多大なご協力をいただいた。

報道記事等から得られた情報に基づいて記載したものであり、必ずしも十分な正確性を有するものではないことに留意されたい。

複数の法令が関わる場合は、いずれにも掲載することとし、図表の日付欄にカッコ書きで記すこととした。その際、便宜上、法令名は、次の表記とした。

・不正競争防止法：　不競法
・著作権法：　著作権法
・不正アクセス禁止法：　不正アク
・私電磁的記録作出及び供用：　私電磁
・不正指令電磁的記録作成・取得保管：　不正指令
・電子計算機損壊等業務妨害：　電算業妨
・電子計算機使用詐欺：　電算詐欺

２．１　不正競争防止法

（1）刑事事件

32 件の事案を確認した。内訳は、B-CAS カード関連が 14 件、ゲーム機改造及びマジコン関連が 8 件、ビジネスソフトの認証クラック関連が 5 件、映像パッケージのリッピングが 2 件。放送関係で、電波妨害機器が 1 件、正規チューナー販売後の回避・無効化プログラム提供が 1 件、オンラインゲームのチート行為が 1 件であった。

＜報道記事・団体からの情報提供等により確認された事件一覧＞

2012 年 2 月 2 日 （著作権法にも掲載）	ゲームソフト	オークションを通じて権利者に無断で海賊版ゲームソフトを販売するとともに、海賊版ソフトを動作させるためゲーム機 Wii の改造を請け負ったとして、福岡県北九州市の無職男性（41）が、著作権法違反ならびに不正競争防止法違反の疑いで逮捕され、福岡地検に送致された。Wii の改造では、依頼者に送付させた Wii と SD カードに技術的制限手段回避機能を有するプログラムを記録して返送した。	福岡県生活経済課サイバー犯罪対策室、筑紫野署、福岡地検	罰金 80 万円の略式命令
2012 年 5 月 30 日	ゲームソフト	任天堂の携帯用家庭ゲーム機に内蔵されている不正コピー版ゲームソフト使用制限プログラムを無効化する装置を、インターネットを通じて販売した埼玉県三郷市の自営業の男性（39）が、不正競争防止法違反（技術的制限手段回避装置譲渡）の疑いで逮捕された。マジコン販売事案への初適用。	愛知県警サイバー犯罪対策課、千種署	罰金 100 万円

2012 年 6 月 19 日	放送番組	有料放送を無料で視聴できるように改造した B-CAS カードを販売したとして、不正競争防止法違反の疑いで西東京市の男性（43）が逮捕された。	京都府警サイバー犯罪対策課	逮捕。 処分不明
2012 年 7 月 3 日	ゲームソフト	任天堂の家庭用ゲーム機「Wii」の海賊版ソフトを起動可能にする不正プログラムをインターネット上で提供したとして、不正競争防止法違反の疑いで京都府向日市の私立大学2年の男性（19）が逮捕、送検された。	埼玉県警サイバー犯罪対策課，所沢署	逮捕。 処分不明
2012 年 7 月 16 日	ゲームソフト	ニンテンドーDS に内蔵されている不正コピー版ゲームソフト使用制限プログラムを回避してコピーゲームの起動を可能にするマジコンを販売した大阪市の電子部品販売店経営の男性（35）が不正競争防止法違反（技術的制限手段回避装置提供行為）の疑いで逮捕された。	大阪府浪速署、住吉署	罰金 100 万円の略式命令
2012 年 7 月 17 日	映像ソフト	DVDのコピーを防止する技術的制限手段を無効化するソフト入りのCD―ROMを雑誌の付録にして販売したとして、不正競争防止法違反で、出版社の社員4人が逮捕された。	警視庁サイバー犯罪対策課	逮捕。 処分不明
2012 年 8 月 14 日	ゲームソフト	PSPで違法ソフトが使えるよう改造したメモリーを販売したとして、不正競争防止法違反などに問われた栃木県足利市の無職の男性（29）に対し、懲役2年、執行猶予4年、罰金200万円が言い渡された。2011 年 12 月同種装置の譲渡を禁じる不正競争防止法改正法施行後、初の判決言い渡し。	宇都宮地裁栃木支部	懲役 2 年、執行猶予 4 年、 罰金 200 万円
2012 年 9 月 6 日	放送番組	有料放送を無料視聴できるようにした不正な B-CAS カードを輸入等したとして、不正競争防止法違反容疑などで大阪市平野区の会社員の男性（33）が書類送検された。	大阪府警	書類送検。 処分不明
2012 年 9 月 27 日	放送番組	有料放送を無料で見られるように不正に書き換えたB-CASカードをインターネットのオークションサイトに出品したとして、不正競争防止法違反容疑で横浜市の男性（53）が逮捕された。	群馬県警	逮捕。 処分不明
2013 年 2 月 13 日	放送番組	不正競争防止法違反の疑いで、違法有害情報販売サイト「激裏情報」の運営者の男性（41）を逮捕した。12 年 5 月下旬に、「B-CAS カードを改竄する方法」とうたって、有料放送を無料で見られるように「B-CAS カード」を書き換える不正プログラムをネット上で販売した疑い。	京都府警サイバー犯罪対策課	懲役 2 年 6 月、 執行猶予 5 年 （求刑懲役 2 年 6 月）
2013 年 3 月 5 日	映像ソフト	Blu-ray/DVDビデオのリッピングソフトをCD-Rに収録してネットオークションで販売していた男が、不正競争防止法違反で摘発された。	北海道警察本部生活安全部生活経済課サイバー犯罪対策室、留萌警察署	摘発。 処分不明
2013 年 4 月 21 日	放送番組	不正な B-CAS カードを、インターネットの販売サイト（既に閉鎖）に「暗号解読版 B-CAS カード」として出品し、販売したとして、男性2人が逮捕された。両容疑者の自宅からは不正カード計約700枚が押収された。米国のサーバを使用しており、捜査を免れようとしたとみられている。	兵庫県警サイバー犯罪対策課	逮捕。 処分不明

2013 年 5 月 15 日	放送番組	有料の衛星放送「スカパー！」を不正に視聴できる機器を製造、販売したとして、不正競争防止法違反（技術的制限手段回避装置譲渡）の疑いで、兵庫洲本市の男性（41）が逮捕された。衛星放送を解約すると、専用の受信機に番組を視聴できないようにする電波が送られるが、この電波を妨害する装置を受信機に取り付け、解約後も見られるようにしていた。	兵庫県警	逮捕。 処分不明
2013 年 5 月 21 日	放送番組	有料衛星放送を無料で視聴できるように不正改造された B-CAS カードを譲り渡したとして、4人が逮捕された。	宮城県警仙台中央署	逮捕。処分不明
2013 年 5 月 30 日 （私電磁にも掲載）	放送番組	有料テレビ放送を無料で見られるように B-CAS カードを書き換える不正プログラムをネット上で販売したほか自らも使用したとして、不正競争防止法違反と私電磁的記録不正作出・供用罪に問われた情報販売サイト「激裏情報」の運営者に対し、懲役2年6月、執行猶予5年が言い渡された。	京都地裁	懲役 2 年 6 月、 執行猶予 5 年
2013 年 6 月 21 日	放送番組	有料デジタル放送を無料で視聴できるように不正に書き換えた改造 B-CAS カードをネットで広告し販売したとして、さいたま市の2人が商標法違反と不正競争防止法違反の疑いで逮捕された。	栃木、北海道、富山、宮崎など9道県警の合同捜査本部	逮捕。 処分不明
2013 年 7 月 19 日	放送番組	有料テレビ放送を無料で視聴できるように B-CAS カードを改ざんし、販売したとして、さいたま市の会社役員（34）ら男4人が、不正競争防止法違反（技術的制限手段回避装置譲渡）容疑で逮捕された。	警視庁サイバー犯罪対策課	逮捕。 処分不明
2013 年 7 月 23 日	放送番組	テレビの有料放送を無料で視聴できるよう B-CAS を改ざんし、職場の同僚に譲り渡した男性2人が逮捕された。	山梨県警サイバー犯罪対策室と笛吹署	逮捕。 処分不明
2013 年 8 月 2 日	放送番組	デジタル放送を視聴するのに必要な B-CAS カード約 2,000 枚を改ざんされることを知りながら不正に転売したとして、東京都品川区の電子機器製造販売会社社長（56）が、不正競争防止法違反幇助容疑で逮捕された。	警視庁サイバー犯罪対策課	逮捕。 処分不明
2013 年 8 月 30 日	ゲームソフト	携帯ゲーム機PSPを不正なゲームソフトがプレイできるように改造しネットオークションで販売した男性（33）が逮捕された。	兵庫県警三田署	逮捕。 処分不明
2013 年 9 月 20 日	ゲームソフト	携帯ゲーム機 PSP を不正に改造し、インターネットオークションで販売したとして、不正競争防止法違反や商標法違反などの疑いで、千葉県の定時制高校4年の男子生徒（18）が書類送検された。	茨城県警古河署、水戸地検	書類送検。 処分不明
2013 年 12 月 5 日	放送番組	不正に入手した改ざん前の B-CAS カード数千枚を、既に逮捕された密売グループに転売したとして、東京都豊島区の中国籍の電子部品販売店経営者(47)が、不正競争防止法違反幇助の疑いで逮捕された。	千葉県警（サイバー犯罪対策課、浦安署）、警視庁	逮捕。 処分不明
2014 年 2 月 1 日	放送番組	有料テレビ放送を無料で見られるように改造した B-CAS カードを台湾から輸入したとして、奈良県大和郡山市の自営業の男性（29）が、不正競争防止法違反（技術的制限手段回避装置の輸入）の容疑で逮捕された。	大阪府警サイバー犯罪対策課、門司海上保安部	逮捕。 処分不明

2014 年 2 月 24 日	放送番組	有料衛星放送を無料で見られるように不正改造した B-CAS カードを100人程度に販売したとして、不正競争防止法違反の疑いで東京都新宿区の男性（30）が逮捕された。	宮城県警	逮捕。 処分不明
2014 年 5 月 16 日	ゲームソフト	携帯型家庭用ゲーム機に内蔵されている不正コピー版ゲームソフト使用制限プログラムを無効化する装置(マジコン）を、中国から発送して、インターネットを通じて販売したとして、国外在住の会社員の男性（43）が、不正競争防止法違反（技術的制限手段回避装置譲渡）の疑いで逮捕された。	千葉県警サイバー犯罪対策課、船橋署	逮捕。 処分不明
2014 年 10 月 15 日	ビジネスソフト	試用版である「Office2013ProfessionalPlus」のライセンス認証を回避して、不正なプロダクト ID をユーザパソコン内に偽造・偽装することで、使用期間や機能制限のない製品版プログラムとしての実行を可能にするクラックプログラムを提供した行為が不正競争防止法違反にあたるとして、福井県内の男性に対し、罰金 50 万円を科す略式命令が言い渡された。	福井簡易裁判所	50 万円の罰金刑を科す略式命令
2014 年 12 月 5 日	ビジネスソフト	試用版である「Office2013ProfessionalPlus」のライセンス認証システムを回避するクラックプログラムを販売したネットショップ経営者の男性に対し、不正競争防止法違反を認め、懲役 1 年 6 月（執行猶予 3 年）、罰金 50 万円の併科が科された。	宇都宮地方裁判所	懲役 1 年 6 月（執行猶予 3 年）、 罰金 50 万円の併科
2015 年 3 月 10 日	放送番組	VISIONPRO と呼ばれるチューナーをネット通販等で販売した後、購入者に対し有料放送に施された技術的制限手段を回避・無効化するプログラムのダウンロード先をメールで教えていた男女4人が不正競争防止法違反の疑いで逮捕された。チューナー販売と、回避・無効化プログラムの URL 提示を分けて行っていた。	埼玉県サイバー犯罪課、東入間署	（有罪判決との情報あり）
2015 年 6 月 24 日 （著作権法にも掲載	ビジネスソフト	マイクロソフトコーポレーションの「Office 2013 Professional」体験版及びアドビ システムズ インコーポレイテッドの「Adobe Photoshop CC」のライセンス認証システムを回避することを可能にするクラック・ツールを、自ら開設した会員制ウェブサイト上で販売していたとして、大阪府和泉市内の男性が、不正競争防止法違反及び著作権法違反の疑いで逮捕された	宮崎県警生活環境課、延岡署	逮捕。 処分不明
2015 年 7 月 29 日 （私電磁にも掲載）	オンラインゲーム	オンラインゲームのキャラクターに通常ではあり得ない動きをさせたり、武器や道具を無限に増やしたりするチート・ツールを販売したとして、不正競争防止法違反（技術的制限手段回避プログラム電気通信回線提供）、私電磁的記録不正・作出罪で逮捕起訴された兵庫県姫路市の無職(30)に、懲役 2 年（執行猶予 4 年）の有罪判決が言い渡された。	東京地裁	懲役 2 年 （執行猶予 4 年）
2015 年 9 月 8 日	ビジネスソフト	マイクロソフトの試用版製品を正規の認証作業を行わずに製品版として使用可能にするクラックプログラムを、インターネットオークションを通じて販売した男性に対し、神戸地方裁判所は、不正競争防止法を適用して、懲役 2 年（執行猶予 5 年）、罰金 200 万円併科の有罪判決を言い渡した。	神戸地方裁判所	懲役 2 年 （執行猶予 5 年）、 罰金 200 万円併科の有罪判決

2016 年 1 月 12 日	ビジネスソフト	「Adobe Creative Suite 6 Master Collection」をインターネットオークションサイトに出品し、落札者に対して、アドビ システムズより体験版として提供されていたプログラムを製品版として使用可能にするクラックプログラムとその使用方法を記載したマニュアルが保管されているストレージサイトのアドレスを教え、落札者にダウンロードさせる形で提供していた東京都目黒区の男性に、不正競争防止法違反で、懲役 2 年（執行猶予 4 年）、罰金 100 万円を併科する有罪判決が下された。	長崎地裁	懲役 2 年（執行猶予 4 年）、罰金 100 万円の併科

（2）民事事件

B-CAS カード関連事件が 2 件あったほか、マジコン輸入業者事件が最高裁で確定した。

2013 年 7 月 31 日	放送番組	有料テレビ放送等に用いられる技術的制限手段を妨げる不正なプログラムをファイル共有ソフトで提供、及び、改ざんした B-CAS カードを譲渡するなどしたとして有罪が確定した東京都の男性(37)に対する損害賠請求訴訟で、不正競争防止法第 4 条に基づき、約 240 万円の損害賠償が命ぜられた。	東京地裁	約 240 万円の損害賠償
2014 年 5 月 29 日	放送番組	スカパーJSAT、スター・チャンネル、WOWOW の 3 社が、不正改ざんした B-CAS カードを第三者に販売した 3 人を相手取って、東京地方裁判所に提起していた民事訴訟において、3 億 2590 万 9127 円の損害請求の全額支払いが言い渡された。	東京地裁	3 億 2590 万 9127 円の損害賠償
2013 年 7 月 9 日	ゲームソフト	任天堂とソフトメーカーがマジコンの輸入業者に対して起こしていた差止等請求訴訟について、2013 年 7 月 9 日東京地裁は、被告にマジコン輸入販売の差し止めと総額 9562 万 5000 円の損害賠償金の支払いを命じる判決を下した。	東京地裁	販売差止め、9562 万 5000 円の損害賠償
2014 年 6 月 12 日		東京地裁判決を不服として一部マジコン輸入業者が控訴したが、2014 年 6 月 12 日知財高裁は、これを棄却した	知財高裁	
2016 年 1 月 12 日		知財高裁決定を不服として一部マジコン輸入業者が上告したが、2016 年 1 月 12 日最高裁は不受理とした。 これにより、販売差止めと 9562 万 5000 円の損害賠償金の支払いが確定した。	最高裁	

２．２　著作権法

ゲーム機改造 2 件、オンラインゲームのチート行為 2 件、ビジネスソフトの認証クラック関連が 2 件、影像パッケージのリッピングが 1 件、ビジネスソフトのプロダクトキー販売が 1 件の、計 8 事案を確認した。

2010 年 5 月 24 日	ゲームソフト	海賊版ソフトを稼働できるように改造した PSP 本体とゲームソフトを無断複製したメモリースティックを、インターネットオークションでセット販売した広島市の無職の男性(45)が逮捕された。	兵庫県生活経済課、尼崎南署	逮捕。 処分不明
2012 年 2 月 2 日 (不競法にも掲載)	ゲームソフト	オークションを通じて権利者に無断で海賊版ゲームソフトを販売するとともに、海賊版ソフトを動作させるためゲーム機 Wii の改造を請け負ったとして、福岡県北九州市の無職男性(41)が、著作権法違反ならびに不正競争防止法違反の疑いで逮捕され、福岡地検に送致された。Wii の改造では、依頼者に送付させた Wii と SD カードに技術的制限手段回避機能を有するプログラムを記録して返送した。	福岡県生活経済課サイバー犯罪対策室、筑紫野署、福岡地検	罰金 80 万円の略式命令
2013 年 6 月 12 日	ビジネスソフト	権利者に無断で複製したコンピュータソフトウェアを搭載した中古パソコンをライセンス認証(アクティベーション)回避のためのクラック・ツールと共に販売したとして、福岡市のパソコン販売業の男性(52)が著作権法違反の疑いで逮捕 された。	福岡県警察本部サイバー犯罪対策課、東警察署	逮捕。 処分不明
2015 年 7 月 10 日	オンラインゲーム	「パズル＆ドラゴンズ」を有利に進めるためのチート・ツールを販売したとして、さいたま市の会社経営の男性(39)が、著作権法違反(技術的保護手段回避プログラムの複製物譲渡)の罪で、略式起訴された。	横浜区検	罰金 50 万円
2015 年 8 月 19 日	映像ソフト	DVD ビデオの CSS 暗号化を回避して複製するリッピングソフト「DVD Shrink 日本語版」を、ウェブサイトにアップロードしていた者を著作権法違反で検挙した。リッピングソフトの提供行為は、これまで不正競争防止法違反で検挙されることはあったが、2012 年に改正著作権法違反では初検挙。	神奈川県警察本部サイバー犯罪対策課、戸部警察署	検挙。 処分不明
2015 年 11 月 22 日	オンラインゲーム	「モンスターストライク」のデータを改ざんしてゲームを有利に進めるためのチート・ツールをインストールしたスマホを、インターネットオークションに出品して譲り渡したとして、大阪府内の私立高校3年の男子生徒(17)が、著作権法違反(技術的保護手段回避プログラム譲渡)容疑で逮捕された。	奈良県警	逮捕。 処分不明
2015 年 12 月 15 日	ビジネスソフト	「Office Standard 2010」の海賊版をネットオークションで販売するとともに、「MICROSOFT OFFICE」と類似する商標を掲載して「Microsoft Office Professional Plus 2010」のプロダクトキー販売に関する広告を大手通信事業者が管理するサーバに記録して利用者に閲覧させた福岡県の男女に対し、著作権法違反(公衆送信権侵害)と商標法違反を認め、男性に対しては懲役 2 年 4 か月(執行猶予 4 年)と罰金 60 万円、女性に対しては懲役 1 年 6 か月(執行猶予 3 年)と罰金 30 万円をそれぞれ併科する有罪判決を下した。	福岡地裁	男性被告: 懲役 2 年 4 か月(執行猶予 4 年)、 罰金 60 万円、 女性被告: 懲役 1 年 6 か月(執行猶予 3 年)、 罰金 30 万円
2015 年 6 月 24 日 (不競法にも掲載)	ビジネスソフト	マイクロソフトコーポレーションの「Office 2013 Professional」体験版及びアドビ システムズ インコーポレイテッドの「Adobe Photoshop CC」のライセンス認証システムを回避することを可能にするクラック・ツールを、自ら開設した会員制ウェブサイト上で販売していたとして、大阪府和泉市内の男性が、不正競争防止法違反及び著作権法違反の疑いで逮捕された	宮崎県警生活環境課、延岡署	逮捕。 処分不明

２．３　不正アクセス禁止法

オンラインゲーム関連で 38 件、映像コンテンツ関連で 1 件を確認し、以下に整理した。

前者では、小学児童を含む未成年者による犯罪事例が顕著である。

処分まで確認できた事案では、オンラインゲームのアイテムを転売する目的で他人の ID を不正に入手したとして男女 2 人が逮捕されうち 1 名は罰金 30 万円の略式命令を受けた事件、オンラインゲームのサーバにある約 130 万人のゲームデータを改ざんしたとして元システム担当に懲役 2 年 6 月・執行猶予 4 年の有罪判決が下された事件がある。

2010 年 2 月 18 日	オンラインゲーム	「ハンゲーム」に他人の ID などを使用して不正にアクセスし、ゲームをしたとして、徳島東署は、和歌山県の小学6年の女子児童(12)を不正アクセス禁止法違反の疑いで補導し、徳島県中央児童相談所に通告した。	徳島東署、徳島県中央児童相談所	補導、通告
2010 年 2 月 23 日	オンラインゲーム	オンラインゲーム運営会社のサイトに他人の ID とパスワードを使って接続したとして、不正アクセス禁止法違反の疑いで、東京都府中市の派遣社員(22)が逮捕された。	長崎県警江迎署	逮捕。 処分不明
2010 年 7 月 14 日	オンラインゲーム	他人のパスワードを使ってオンラインゲーム上のキャラクター「アバター」を乗っ取ったとして、埼玉県狭山市の無職男性(29)が不正アクセス禁止法違反の疑いで逮捕された。	高知県警、高知南署	逮捕。 処分不明
2010 年 7 月 15 日	オンラインゲーム	他人のIDとパスワードを使用してオンラインゲームに不正にアクセスしたとして、不正アクセス禁止法違反の疑いで、新潟県上越市の高校1年の男子生徒(15)が書類送検された。	茨城県警生活環境課、鉾田署	書類送検。 処分不明
2010 年 9 月 24 日	オンラインゲーム	他人のIDやパスワードを使用してオンラインゲームに不正アクセスしたなどとして、不正アクセス禁止法違反容疑などで仙台市青葉区の無職の男性(29)が書類送検された。	愛知県警	書類送検。 量刑不明
2010 年 9 月 27 日	オンラインゲーム	オンラインゲームに他人の ID とパスワードで不正にアクセスし、ゲーム内の仮想通貨やアイテムなどを盗んだとして、埼玉県内の無職少年(18)と東京都内の無職男性(24)が不正アクセス禁止法違反容疑で逮捕された。	愛知県警	逮捕。 処分不明
2010 年 10 月 1 日	オンラインゲーム	オンラインゲームのアイテムを盗む目的で他人の ID とパスワードを不正に使用したとして、不正アクセス禁止法違反容疑で、福岡市博多区の会社員(23)が書類送検された。アイテムを盗む目的でパスワードで不正にアクセスし、盗んだアイテムを転売し約 60 万円の利益を得ていたという。	愛知県警	書類送検。 処分不明
2010 年 10 月 12 日	オンラインゲーム	他人の ID でオンラインゲームのサーバに不正アクセスしたとして、愛知県の高校 1 年の男子生徒(16)、埼玉県の内装作業員(16)、横浜市の会社員(34)が書類送検された。	愛知、宮城、福島各県警の合同捜査本部	書類送検。 処分不明
2010 年 11 月 10 日 (私電磁にも掲載)	オンラインゲーム	オンラインゲームで他人のパスワードなどを使用してキャラクターを横取りしたとして、不正アクセス禁止法違反と私電磁的記録不正作出・同供用の疑いで、三重県熊野市の中学生(15)が長野地方検察庁上田支部に書類送検された。	長野地方検察庁 上田支部、県警生活環境課	書類送検。 処分不明

2010 年 12 月 14 日	オンラインゲーム	オンラインゲーム「リネージュ 2」のアイテムを転売する目的で他人の ID を不正に入手したとして男女 2 人が逮捕された事件で、川崎市の会社員（29）が不正アクセス禁止法違反の罪で略式起訴され、川崎簡易裁判所から罰金 30 万円の略式命令を受けた。	川崎簡易裁判所	略式起訴、罰金 30 万円の略式命令
2011 年 6 月 22 日	オンラインゲーム	他人のIDとパスワードを使ってオンラインゲームに不正にアクセスしたとして、不正アクセス禁止法違反の疑いで、愛媛県の高校 1 年の女子生徒（15）と神奈川県藤沢市の高校 2 年の男子生徒（17）が書類送検された。	愛知県警愛知署	書類送検。処分不明
2011 年 10 月 24 日	オンラインゲーム	着せ替えゲーム「コーデマニア」のサーバに仕組んだ不正プログラムを利用して、約 130 万人のゲームデータを改ざんしたとして、東京都豊島区の派遣社員（31）が不正アクセス禁止法違反容疑などで逮捕された事件で、懲役 2 年 6 月、執行猶予 4 年が言い渡された。	東京地裁	懲役 2 年 6 月（執行猶予 4 年）
2012 年 2 月 2 日	オンラインゲーム	他人のIDとパスワードを使ってアメーバピグに不正にアクセスしたとして、不正アクセス禁止法違反の非行事実で奈良県に住む小学 4 年の女子児童（10）が補導された。	福井県警生活環境課と福井署	補導
2012 年 2 月 10 日 （電算詐欺にも掲載）	映像ソフト	プレイステーションネットワーク上で、他人の ID などを使って映画コンテンツを不正に購入したとして、富山県射水市に住むフィリピン国籍の無職（22）が、電子計算機使用詐欺や不正アクセス禁止法違反などの疑いで逮捕された。	警視庁	逮捕。処分不明
2012 年 3 月 14 日	オンラインゲーム	他人の会員情報などを使用してアメーバピグのオンラインゲームにアクセスしたとして、不正アクセス禁止法違反容疑で、兵庫県の中学 2 年の男子生徒（14）が補導され、児童相談所に通告された。	福井県警	補導、児童相談所に通告
2012 年 5 月 24 日	オンラインゲーム	「アメーバピグ」に他人の会員情報を使って不正なアクセスをしたとして、岐阜県の中学 3 年の男子生徒（14）が不正アクセス禁止法違反容疑で甲府地検に書類送検された。	山梨県韮崎署、甲府地検	書類送検。処分不明
2012 年 6 月 12 日	オンラインゲーム	「アメーバピグ」に他人の会員情報を使って不正なアクセスをしたとして、不正アクセス禁止法違反の疑いで、大阪府の小学 6 年の女児（11）が補導され、児童相談所に通告された。	山梨県警富士吉田署	補導、児童相談所に通告
2012 年 6 月 13 日	オンラインゲーム	個人運営のオンラインゲームの利用者 ID とパスワードを第三者が閲覧可能なインターネット上の掲示板に公開したとして、和歌山市の無職少年（16）が不正アクセス禁止法違反容疑で逮捕された。	京都府警サイバー犯罪対策課	逮捕。処分不明
2012 年 9 月 27 日 （不正電磁にも掲載）	オンラインゲーム	オンラインゲームの ID やパスワードを不正に取得するコンピュータ・ウィルスを作成したとして、佐賀県の県立高校 1 年の男子生徒（15）が、不正指令電磁的記録作成、及び、不正アクセス禁止法違反の疑いで逮捕された。	京都府警	逮捕。処分不明
2012 年 11 月 16 日	オンラインゲーム	オンラインゲームに他人の IDとパスワードを使ってアクセスしたとして、神奈川県に住む男子高校生(18)2 人が、不正アクセス禁止法違反の疑いで書類送検された。	静岡県警	書類送検。処分不明

2012 年 11 月 21 日 （私電磁にも掲載）	オンライン ゲーム	オンラインゲームのアイテムを盗むため、他人の ID とパスワードを推測して特定した後、入力して不正にアクセスしたとして、福岡市の無職少年（17）が、不正アクセス禁止法違反及び私電磁的記録不正作出・同供用などの疑いで福島地検に書類送検された。	二本松署、福島県警本部生活環境課サイバー犯罪対策室、福島地検	書類送検。 処分不明
2012 年 12 月 1 日 （私電磁にも掲載）	オンライン ゲーム	オンラインゲームに他人の ID とパスワードを使って不正にアクセスしたとして、北海道に住む 14～15 歳の中学生の男子生徒 3 人が、不正アクセス禁止法違反、私電磁的記録不正作出・供用罪の疑いで書類送検された。他人の ID とパスワードは、ゲーム内の会話機能のコメントから推測して特定した。	北海道警	書類送検。 処分不明
2012 年 12 月 11 日 （不正指令にも掲載）	オンライン ゲーム	コンピュータ・ウィルスを使い、オンラインゲームなどの ID とパスワードを不正に取得したとして、大阪府の高校生（17）と愛知県の専門学校生（17）が、不正アクセス禁止法違反（識別符号の不正取得）、及び、不正指令電磁的記録作成・供用などの容疑で、秋田地検横手支部に書類送検された。	秋田県警	書類送検。 処分不明
2013 年 2 月 7 日	オンライン ゲーム	「アメーバピグ」に他人のアカウントを利用して不正にアクセスしたとして、大阪府阪南市の無職少年（16）が、不正アクセス禁止法違反容疑で書類送検された。	福井県警生活環境課	書類送検。 処分不明
2013 年 3 月 19 日 （電算詐欺にも掲載）	オンライン ゲーム	オンラインゲームの他人のアカウントに不正アクセスし、仮想通貨などをだまし取ったとして、愛知県愛西市の市立中学 2 年の男子生徒（14）が、電子計算機使用詐欺及び不正アクセス禁止法違反容疑で書類送検された。	愛知県警	書類送検。 処分不明
2013 年 4 月 3 日 （私電磁にも掲載）	オンライン ゲーム	オンラインゲームに他人の ID とパスワードを使って不正にログインしたとして、福岡県北九州市の高校 1 年の男子生徒(15)が、不正アクセス禁止法違反と私電磁的記録不正作出・同供用の疑いで書類送検された。ウェブサイト内の掲示板に「サイト内の通貨を増やしてやる」と書き込み、その書き込みに応じた者から直接 ID とパスワードを聞き出していた。	高岡署、県警サイバー犯罪対策室	書類送検。 処分不明
2013 年 6 月 21 日 （私電磁にも掲載）	オンライン ゲーム	「アメーバピグ」に不正にアクセスし他人のパスワードを変更したなどとして、神奈川県に住む中学生の少年（14）が、不正アクセス禁止法違反、及び、私電磁的記録不正作出・同供用の疑いで宇都宮地検足利支部に書類送検された。	宇都宮地検足利支部	書類送検。 処分不明
2013 年 7 月 30 日 （電算詐欺にも掲載）	オンライン ゲーム	携帯電話販売店に展示されていた宣伝用デモ機のパスワードを推測で入力してオンラインゲームサイトに不正にアクセスし、仮想通貨を不正に取得したとして、不正アクセス禁止法違反及び電子計算機使用詐欺などの疑いで、横浜市の廃品回収業の男性（36）が逮捕された。	愛知、三重両県警	逮捕。 処分不明
2013 年 11 月 13 日 （不正指令にも掲載）	オンライン ゲーム	「ハンゲーム」の ID やパスワードを不正に入手できるコンピュータ・ウィルスを作成したとして、岡山市南区の高校 1 年の男子生徒（16）が不正指令電磁的記録作成などの疑いで、同市の高校 1 年の男子生徒（15）と岐阜県美濃加茂市の専門学校 1 年の男子生徒（19）が不正アクセス禁止法違反などの疑いで、それぞれ書類送検された。	宮城、岐阜両県警	書類送検。 処分不明

2013年11月20日 （不正指令にも掲載）	オンラインゲーム	オンラインゲームの他人のIDなどを不正に取得するウィルスを作成するなどしたとして、不正指令電磁的記録作成及び不正アクセス禁止法違反の容疑で北海道の高校1年(16)と千葉県の高校3年(18)が、不正アクセス禁止法違反で神奈川県の高校1年(16)と石川県のパート従業員(17)の計4人が、書類送検された。	栃木県今市署と県警生活環境課	書類送検。 処分不明
2014年2月3日	オンラインゲーム	スマホ用ゲーム「パズル＆ドラゴンズ」に他人のアカウントを利用して不正なアクセスを行ったとして、神奈川、沖縄に住む男子高校生2人が、不正アクセス禁止法違反容疑で書類送検された	大阪府警四條畷署	書類送検。 処分不明
2014年2月27日	オンラインゲーム	携帯電話店の販売員(27)が、機種変更手続き中の顧客の携帯電話の暗証番号などを盗み見して、スマホを無断で操作して、ソーシャルサイト「グリー」の仮想通貨「GREE コイン」を顧客の携帯代金引き落としで購入したとして、不正アクセス禁止法違反などの容疑で逮捕された。	千葉県警サイバー犯罪対策課、同県松戸市日暮、	逮捕。 処分不明
2014年3月12日 （私電磁にも掲載）	オンラインゲーム	他人のアカウントを不正に取得・改変して、ソーシャルゲーム「暴走列伝単車の虎」に不正なアクセスを行ったとして、茨城県小美玉市の会社員(24)が、不正アクセス禁止法違反と私電磁的記録不正作出・同供用容疑で逮捕された。勝手に変更したアカウントを利用して不正ログインし、ゲーム内アイテム12種類を入手した。	神奈川県警サイバー犯罪対策課	逮捕。 処分不明
2014年5月23日	オンラインゲーム	スマホ用ゲーム「パズル＆ドラゴンズ」に他人のアカウントを利用して不正にアクセスしたとして、沖縄市の大学生(18)が、不正アクセス禁止法違反容疑で書類送検された。	長野県警松本署	書類送検。 処分不明
2014年6月20日	オンラインゲーム	他人に売り渡した自分のゲームアカウントを再び自分のものとするために、オンラインゲームの認証サーバに接続し、パスワード情報を改ざんするなどの不正アクセス行為をしたとして、愛知県の無職の男性(29)が、不正アクセス禁止法違反の疑いで書類送検された。	足利署、栃木県警生活環境課	書類送検。 処分不明
2014年9月30日	オンラインゲーム	「パズル＆ドラゴンズ」のサーバに別の男性のIDとパスワードで接続したとして、埼玉県川口市の男子中学生(14)が、不正アクセス禁止法違反などの疑いで書類送検された。	佐賀県警生活環境課、武雄署、佐賀地検	書類送検。 処分不明
2014年10月20日	オンラインゲーム	オンラインゲームに他人のIDを使って不正にアクセスしたとして、不正アクセス禁止法違反などの疑いで、徳島市の男子大学生(19)と男子専門学校生(18)が、福岡地検飯塚支部に書類送検された。	福岡県警飯塚署サイバー犯罪対策課、福岡地検飯塚支部	書類送検。 処分不明
2014年11月5日	オンラインゲーム	「ドラゴンクエスト X」に他人のアカウントを使ってアクセスしたとして、不正アクセス禁止法違反などの疑いで、北九州市の中学3年の男子生徒(15)が書類送検された。	警視庁少年事件課	書類送検。 処分不明
2014年11月19日	オンラインゲーム	オンラインゲームに他人のパスワードでアクセスしたとして、不正アクセス禁止法違反の疑いで、秋田県三種町の男性(32)が逮捕された。	埼玉県警	逮捕。 処分不明

２．４　刑法第１６１条の２　私電磁的記録不正作出及び供用

B-CAS カード関連事件を 8 件、オンラインゲーム関連事件を 8 件、確認した。

B-CAS カード関連事件には、京都地方裁判所で懲役 2 年 6 月・執行猶予 5 年が言い渡された「激裏情報」運営者事件、大阪高等裁判所による控訴棄却によって京都地方裁判所の懲役 1 年 6 月・執行猶予 3 年が維持された「平成の龍馬」事件が含まれる。

オンラインゲーム関連事件 8 件のうち 2 件はチートプログラムに関係し、うち 1 件は不正競争防止法違反にも問われた事案である。残る 6 件は他人の ID・パスワードの不正な作成等に関わるもので、不正アクセス禁止法違反にも問われている。

2010 年 11 月 10 日 （不正アクにも掲載）	オンラインゲーム	オンラインゲームで他人のパスワードなどを使用してキャラクターを横取りしたとして、不正アクセス禁止法違反と私電磁的記録不正作出・同供用の疑いで、三重県熊野市の中学生（15）が長野地方検察庁上田支部に書類送検された。	長野地方検察庁　上田支部、県警生活環境課	書類送検。 処分不明
2012 年 6 月 19 日	放送番組	有料放送を無料で視聴できるように B-CAS カードを改造して自宅 PC で使用したとして、電磁的記録不正作出・同供用の疑いで、京都府の男性が逮捕された。男性は、「平成の龍馬」というブログで B-CAS カードを書き換える方法を紹介したことでも問題になった。	京都府警サイバー犯罪対策課	逮捕。 処分不明
2012 年 11 月 21 日 （不正アクにも掲載）	オンラインゲーム	オンラインゲームのアイテムを盗むため、他人の ID とパスワードを推測して特定した後、入力して不正にアクセスしたとして、福岡市の無職少年（17）が、不正アクセス禁止法違反及び私電磁的記録不正作出・同供用などの疑いで福島地検に書類送検された。	二本松署、福島県警本部生活環境課サイバー犯罪対策室、福島地検	書類送検。 処分不明
2012 年 12 月 1 日 （不正アクにも掲載）	オンラインゲーム	オンラインゲームに他人の ID とパスワードを使って不正にアクセスしたとして、北海道に住む 14～15 歳の中学生の男子生徒 3 人が、不正アクセス禁止法違反、私電磁的記録不正作出・供用罪の疑いで書類送検された。他人の ID とパスワードは、ゲーム内の会話機能のコメントから推測して特定した。	北海道警	書類送検。 処分不明
2013 年 2 月 12 日	放送番組	有料デジタル放送を無料で見られるように不正改造された B-CAS カードを使用したとして、暴力団工藤会（本部・北九州市）の幹部ら2人が、私電磁的記不正作出・同供用容疑で逮捕された。	福岡県察	逮捕。 処分不明
2013 年 4 月 3 日 （不正アクにも掲載）	オンラインゲーム	オンラインゲームに他人の ID とパスワードを使って不正にログインしたとして、福岡県北九州市の高校 1 年の男子生徒(15)が、不正アクセス禁止法違反と私電磁的記録不正作出・同供用の疑いで書類送検された。ウェブサイト内の掲示板に「サイト内の通貨を増やしてやる」と書き込み、その書き込みに応じた者から直接 ID とパスワードを聞き出していた。	高岡署、県警サイバー犯罪対策室	書類送検。 処分不明

2013 年 5 月 30 日 （不競法にも掲載）	放送番組	有料テレビ放送を無料で見られるように B-CAS カードを書き換える不正プログラムをネット上で販売したほか自らも使用したとして、不正競争防止法違反と私電磁的記録不正作出・供用罪に問われた情報販売サイト「激裏情報」の運営者に対し、懲役2年6月、執行猶予5年が言い渡された。	京都地裁	懲役 2 年 6 月 執行猶予 5 年
2013 年 6 月 21 日 （不正アクにも掲載）	オンラインゲーム	「アメーバピグ」に不正にアクセスし他人のパスワードを変更したなどとして、神奈川県に住む中学生の少年（14）が、不正アクセス禁止法違反、及び、私電磁的記録不正作出・同供用の疑いで宇都宮地検足利支部に書類送検された。	宇都宮地検足利支部	書類送検。 処分不明
2013 年 7 月 23 日	放送番組	テレビの有料放送を無料で視聴できるよう B-CAS を改ざんし、職場の同僚に譲り渡した男性2人が逮捕された。	山梨県警サイバー犯罪対策室と笛吹署	逮捕。 処分不明
2013 年 11 月 26 日	放送番組	有料テレビ放送を無料で見られるように、不正に改ざんされた B-CAS カードを使ったとして、20～60 代の男女計 27 人が、私電磁的記録不正供用容疑で東京地検に書類送検された。	警視庁サイバー犯罪対策課、東京地検	書類送検。 処分不明
2014 年 3 月 12 日 （不正アクにも掲載）	オンラインゲーム	他人のアカウントを不正に取得・改変して、ソーシャルゲーム「暴走列伝単車の虎」に不正なアクセスを行ったとして、茨城県小美玉市の会社員（24）が、不正アクセス禁止法違反と私電磁的記録不正作出・同供用容疑で逮捕された。勝手に変更したアカウントを利用して不正ログインし、ゲーム内アイテム 12 種類を入手した。	神奈川県警サイバー犯罪対策課	逮捕。 処分不明
2014 年 5 月 22 日	放送番組	有料テレビ放送を見るのに必要な B-CAS カードを改ざんし無料で視聴したとして、元京都大職員(31)が私電磁的記録不正作出・同供用罪容疑で逮捕され（いわゆる「平成の龍馬事件」）、2013 年 12 月 3 日の京都地裁が懲役1年6月、執行猶予3年を言い渡していた事件の控訴審で、大阪高裁は控訴を棄却した。	大阪高裁（原審京都地裁）	控訴棄却 原審京都地裁: 懲役1年6月 執行猶予3年
2015 年 1 月 20 日	放送番組	有料テレビ放送を無料で見られるように B-CAS カードを不正に改造したとして、受信機器製造大手マスプロ電工の社員2人が、私電磁的記録不正作出などの疑いで逮捕された。	愛知、群馬警察	逮捕。 処分不明
2015 年 7 月 15 日	放送番組	B-CAS カードの偽造品を使って、有料テレビ放送を不正に視聴できるようにしたとして、私電磁的記録不正作出・供用の疑いで、51 歳の男性が逮捕された。	宮城県警察本部サイバー犯罪対策室、白石警察署	再逮捕。 処分不明
2015 年 7 月 29 日 （不競法にも掲載）	オンラインゲーム	オンラインゲームのキャラクターに通常ではあり得ない動きをさせたり、武器や道具を無限に増やしたりするチート・ツールを販売したとして、不正競争防止法違反（技術的制限手段回避プログラム電気通信回線提供）、私電磁的記録不正・作出罪で逮捕起訴された兵庫県姫路市の無職(30)に、懲役 2 年（執行猶予 4 年）の有罪判決が言い渡された。	東京地裁	懲役 2 年 （執行猶予 4 年）
2016 年 2 月 29 日	オンラインゲーム	スマホ向けオンラインゲームのデータを改ざんすることができるチートプログラムを使い、レアキャラクターを入手して販売したとして、私電磁的記録不正作出・同供用容疑で、大阪府豊中市の男性（33）が逮捕された。	兵庫県警サイバー対策課等	逮捕 処分不明

２．５　刑法第１６８条の２・同３　不正指令電磁的記録作成提供・取得保管

オンラインゲーム関連で４件を確認した。いずれも不正アクセス禁止法違反にも問われている。

2012 年 9 月 27 日 （不正アクにも掲載）	オンラインゲーム	オンラインゲームの ID やパスワードを不正に取得するコンピュータ・ウィルスを作成したとして、佐賀県の県立高校 1 年の男子生徒(15)が、不正指令電磁的記録作成、及び、不正アクセス禁止法違反の疑いで逮捕された。	京都府警	逮捕。 処分不明
2012 年 12 月 11 日 （不正アクにも掲載）	オンラインゲーム	コンピュータ・ウィルスを使い、オンラインゲームなどの ID とパスワードを不正に取得したとして、大阪府の高校生(17)と愛知県の専門学校生(17)が、不正アクセス禁止法違反（識別符号の不正取得）、及び、不正指令電磁的記録作成・供用などの容疑で、秋田地検横手支部に書類送検された。	秋田県警	書類送検。 処分不明
2013 年 11 月 13 日 （不正アクにも掲載）	オンラインゲーム	「ハンゲーム」の ID やパスワードを不正に入手できるコンピュータ・ウィルスを作成したとして、岡山市南区の高校 1 年の男子生徒(16)が不正指令電磁的記録作成などの疑いで、同市の高校 1 年の男子生徒(15)と岐阜県美濃加茂市の専門学校 1 年の男子生徒(19)が不正アクセス禁止法違反などの疑いで、それぞれ書類送検された。	宮城、岐阜両県警	書類送検。 処分不明
2013 年 11 月 20 日 （不正アクにも掲載）	オンラインゲーム	オンラインゲームの他人の ID などを不正に取得するウィルスを作成するなどしたとして、不正指令電磁的記録作成及び不正アクセス禁止法違反の容疑で北海道の高校 1 年(16)と千葉県の高校 3 年(18)が、不正アクセス禁止法違反で神奈川県の高校 1 年(16)と石川県のパート従業員(17)の計 4 人が、書類送検された。	栃木県今市署と県警生活環境課	書類送検。 処分不明

２．６　刑法第２３４条の２　電子計算機損壊等業務妨害

オンラインゲーム関連の２件を確認した。うち１件はチート・ツールを作動させたと報じられている。

2014 年 6 月 25 日	オンラインゲーム	ネクソンの「サドンアタック」において共謀してチート・ツールを作動させ、運営者の意図しない動作を繰り返し行い、運営業務に支障を生じさせ業務を妨害したとして、福島県会津若松市の大学 1 年生(18)、奈良県五條市の高校 3 年生(17)、徳島県徳島市の専門学校生(17)が、電子計算機損壊等業務妨害容疑で書類送検された。	神奈川県警、横浜地検川崎支部に	書類送検。 処分不明
2014 年 9 月 18 日	オンラインゲーム	アカウントを凍結されたことに対する不満から、オンラインゲーム運営会社ゲームオンが運営する「アライアンス・オブ・ヴァリアント・アームズ(AVA)」に対する DDoS 攻撃を海外業者に委託し運営会社の業務を妨害したとして、電子計算機損壊等業務妨害容疑で、熊本市の高校 1 年の男子生徒(16)が書類送検された。	警視庁サイバー犯罪対策課	書類送検。 処分不明

２．７　刑法第２４６条の２　電子計算機使用詐欺

ネットワークへの不正アクセス行為を行った上で本罪に至った事案を 3 件確認した。仮想通貨の不正取得が 2 件、ネット上のコンテンツ不正購入が 1 件（影像コンテンツ）であった。

2012 年 2 月 10 日 （不正アクにも掲載）	映像ソフト	プレイステーションネットワーク上で、他人の ID などを使って映画コンテンツを不正に購入したとして、富山県射水市に住むフィリピン国籍の無職(22)が、電子計算機使用詐欺や不正アクセス禁止法違反などの疑いで逮捕された。	警視庁	逮捕。 処分不明
2013 年 3 月 19 日 （不正アクにも掲載）	オンラインゲーム	オンラインゲームの他人のアカウントに不正アクセスし、仮想通貨などをだまし取ったとして、愛知県愛西市の市立中学 2 年の男子生徒(14)が、電子計算機使用詐欺及び不正アクセス禁止法違反容疑で書類送検された。	愛知県警	書類送検。 処分不明
2013 年 7 月 30 日 （不正アクにも掲載）	オンラインゲーム	携帯電話販売店に展示されていた宣伝用デモ機のパスワードを推測で入力してオンラインゲームサイトに不正にアクセスし、仮想通貨を不正に取得したとして、不正アクセス禁止法違反及び電子計算機使用詐欺などの疑いで、横浜市の廃品回収業の男性(36)が逮捕された。	愛知、三重両県警	逮捕。 処分不明

２．８　関税法による技術的制限手段回避・無効化装置の輸入差止申立受理

2011 年（平成 23 年）12 月 1 日より、不正競争防止法第 2 条第 1 項第 11 号及び第 12 号に掲げる行為を組成する物品（技術的制限手段回避・無効化装置等）を、輸出及び輸入してはならない貨物に追加する法整備がなされた。

2012 年（平成 24 年）11 月 21 日には、経済産業大臣が意見書を交付したニンテンドーDS の技術的制限手段を回避・無効化する装置（いわゆるマジコン）に関して、任天堂株式会社からの輸入差止申立てが税関において受理され、全国の税関で差止め対象に追加された。技術的制限手段回避・無効化装置等に対する輸入差止申立ての受理は本件が初であった[83]。

2015 年（平成 27 年）9 月までの申立（件数）、差止実績（件数）、及び、差止実績（点数）は以下の通り。2015 年度（平成 27 年度）の申立（件数）は未集計である。

	平成 23 年	平成 24 年	平成 25 年	平成 26 年	平成 27 年 (1 月-9 月)
申立（件数）	0	1	2	5	－
輸入差止実績（件数）	0	0	16	86	11
輸入差止実績（点数）	0	0	60	112	17

技術的制限手段回避・無効化装置の輸入差止実績[84]

※「輸入差止実績（件数）」は、税関が差し止めた知的財産侵害物品が含まれていた輸入申告又は郵便物の数。「輸入差止実績（点数）」は、税関が差し止めた知的財産侵害物品の数。したがって、例えば、1 件の輸入申告又は郵便物に、20 点の知的財産侵害物品が含まれていた場合は、「1 件 20 点」として計上。

[83] 経済産業省プレスリリース資料（http://www.meti.go.jp/press/2012/11/20121122004/20121122004-1.pdf）
[84] 税関ホームページ「知的財産侵害物品の取締り」に基づき作成。
（http://www.customs.go.jp/mizugiwa/chiteki/pages/jisseki.htm）

３　具体的な裁判例

過去５年間における裁判例のうち、判決書を入手することができた裁判例の内容を摘記する。

３．１　刑事事件

（１）B-CAS カードに係る私電磁的記録不正作出・同供用事件

事件番号	平成２６年（う）第１２１号
裁判年月日	平成２６年５月２２日
裁判所名	大阪高等裁判所第３刑事部
結果	懲役１年６月（執行猶予３年）　※控訴棄却により原審確定
原審	京都地方裁判所平成２４年（わ）第８８５号　（平成２５年１２月３日判決）
裁判要旨	B-CAS カードに記録された電磁的記録は、刑法１６１条の２第１項、３項所定の人の事務処理の用に供する権利、義務に関する電磁的記録に該当し、被告人がこれを改変する行為は、同条１項所定の、人の事務処理を誤らせる目的で人の事務処理の用に供する権利、義務に関する電磁的記録を不正に作ったこと（不正作出）に該当するほか、被告人が改変した上記電磁的記録を記録した B-CAS カードをテレビに接続された衛星放送受信可能なチューナー内蔵レコーダーに挿入する行為は、同条３項所定の、人の事務処理を誤らせる目的で不正に作られた権利、義務に関する電磁的記録を人の事務処理の用に供したこと（供用）に該当すると認められる。

（２）試用版ビジネスソフト認証回避プログラム販売不正競争防止法違反宇都宮事件

事件番号	―
裁判年月日	平成２６年１２月５日
裁判所名	宇都宮地方裁判所
結果	懲役１年６月（執行猶予３年）、罰金５０万円
原審	―
裁判要旨	マイクロソフト社が著作権を有する試用版プログラム「Office 2013 Professional Plus」のライセンス認証システムの効果を回避するプログラム（クラックツール）の販売は、営業上用いられている技術的制限手段により制限されているプログラムの実行を、当該技術的制限手段の効果を妨げることにより可能とする機能を有するプログラムを記録した電磁的記録媒体を譲渡するものであり、不正競争にあたる。

（3）オンラインゲーム内アイテム不正入手目的私電磁的記録不正作出・供用事件、及び、
オンラインゲーム技術的手段回避プログラム電気通信回線提供不正競争防止法違反事件

事件番号	平成２７年刑（わ）第 1054 号、特（わ）第 1132 号、特（わ）第 1286 号第
裁判年月日	平成２７年７月２９日
裁判所名	東京地方裁判所刑事第 18 部
結果	懲役２年（執行猶予４年）
裁判要旨	【私電磁的記録不正作出・供用事件】 オンラインゲームのアイテムを不正に入手しようと企て、運営事業者の事務処理を誤らせる目的で・・・オンラインゲームのシステムを構築するサーバコンピュータに接続し、不正な指令を送信して購入処理をさせ、・・・購入アイテムの受領操作を行い、・・・所有アイテムとなった旨の虚偽の情報を送信しこれらを前記サーバコンピュータに記憶蔵置させ、もって人の事務処理の用に供する事実証明に関する電磁的記録を不正に作り、同社の事務処理のように供した。 【不正競争防止法違反事件】 電気通信回線を通じてオンラインゲームの運営事業者が・・・同ゲームの正規利用者以外の者がゲームプログラムを実行できないようにするために営業上用いている技術的制限手段の効果を妨げることにより、上記ゲームプログラムの実行を可能とする機能を有するプログラムを・・・送信して提供し、もって不正競争を行った。

（4）試用版ビジネスソフト認証回避プログラム販売不正競争防止法違反神戸事件

事件番号	平成２７年（わ）第１６１号、第２１８号、第４６７号
裁判年月日	平成２７年９月８日
裁判所名	神戸地方裁判所第１刑事部
結果	懲役２年（執行猶予５年)、罰金２００万円
原審	―
裁判要旨	マイクロソフト社が著作権を有する試用版プログラム「Office 2013 Professional Plus」のライセンス認証システムの効果を回避するプログラム（クラックツール）を、インターネットオークション運営者のサーバコンピュータに記憶・蔵置した上、当該クラック・ツールの蔵置先ＵＲＬを、オークション落札者に提供した行為は、営業上用いられている技術的制限手段により制限されているプログラムの実行を、当該技術的制限手段の効果を妨げることにより可能とする機能を有するプログラムを電気通信回線を通じて提供するものであり、不正競争にあたる。

（5）ビジネスソフト認証回避プログラムのインターネットオークション販売不正競争防止法違反事件

事件番号	―
裁判年月日	平成２８年１月１２日
裁判所名	長崎地方裁判所刑事部
結果	懲役２年（執行猶予４年)、罰金１００万円
原審	―
裁判要旨	アドビ社の「Adobe Creative Suite 6 Master Collection」のライセンス認証システムの効果を回避するプログラム（クラックツール）を、インターネットオークション運営者のサーバコンピュータに記憶・蔵置した上、当該クラック・ツールの蔵置先ＵＲＬを、オークション落札者に通知して落札者がダウンロードできる状態にして提供したことは、営業上用いられている技術的制限手段により制限されているプログラムの実行を当該技術的制限手段の効果を妨げることにより可能とする機能を有するプログラムを電気通信回線を通じて提供するものであり、不正競争にあたる。

３．２　民事事件

（1）ニンテンドーDS 用マジコンに対する不正競争行為差止・損害賠償等請求事件

事件番号	平成２６年（オ）第１３１４号
裁判年月日	平成２８年１月１２日
裁判所名	最高裁判所
結果	不受理
控訴審	平成２６年６月１２日知的財産高等裁判所（平成２５年（ネ）第１００６７号）控訴棄却
第１審	平成２５年７月９日東京地方裁判所（平成 21 年（ワ）第 40515 号、同平成 22 年（ワ）第 12105 号、同第 17265 号）
裁判要旨	＜確定した原審要旨＞ ニンテンドーDS 本体では営業上用いられている技術的制限手段によりプログラムの実行が制限されていると認められる、また、本件 DS 用マジコンは当該技術的制限手段の効果を妨げることにより可能とする機能のみを有するプログラムを記録した記録媒体に当たると認められる。 本件 DS 用マジコンの輸入により、原告は相当額の損害を被っており、マジコンの輸入行為の差止、及び、総額９，５６２万円余の損害賠償金の支払いを命ずる。

（2）B-CAS カード電磁的記録改変等に対する損害賠償請求事件

事件番号	平成２５年（ワ）第１１８２６号
裁判年月日	平成２５年７月３１日
裁判所名	東京地方裁判所
結果	損害賠償金２４０万円余
原審	―
裁判要旨	B-CAS 方式は、電磁的方法により影像若しくは音の視聴を制限する手段であって、視聴等機器が特定の変換を必要とするよう影像、音を変換して送信する方式によるものであり、不競法第２条第７項が定める「技術的制限手段」に該当する。営業上用いている技術的制限手段を妨げることにより、放送の視聴を可能とするプログラムは、技術的制限手段回避プログラムに該当し、これを不正に作出し譲渡した行為は不正競争行為に該当する。 被告の不正行為により被った損害合計２４０万円余の賠償を命ずる。

４　技術的手段の回避・無効化に係る事案のまとめ

コンテンツ事業者は、コンテンツ提供にあたって、コンテンツのコピー等利用制限、コンテンツに対するアクセス制限、及び、コンテンツにアクセスする者が当該コンテンツに係る利用権原を有するか否かを確認する認証を用いることで、ビジネスを保護している。ここまで見てきたように、これらに係る技術は技術的手段と評価され、その回避・無効化に対しては、不正競争防止法、著作権法、さらには、回避・無効化を可能とする電磁的記録の不正作出・供用があった場合につき刑法第 161 条の 2（私電磁的記録不正作出・供用罪）が適用されてきた実態が明らかとなった。

また、コンテンツ事業者は、インターネットにおいてコンテンツ提供サービスを行う場合、ID・パスワード等による認証によって当該サービスへの不正なアクセスからサービスを保護している。係る認証関連技術が技術的手段と評価された事案はない。しかし、ここまで見てきたように、コンテンツ提供サービスのサーバに対する不正アクセスがなされた場合には不正アクセス禁止法が適用されてきた。また、不正アクセスに用いる他人の ID・パスワード等の不正作出・供用につき刑法第 161 条の 2（私電磁的記録不正作出・供用罪）、不正アクセスに用いる他人の ID・パスワード等を不正に入手するためのウィルス作成につき刑法第 168 条の 2 及び 3（不正指令電磁的記録作成提供・取得保管罪）、事業者のサーバに意図しない不正な指令を与える加害行為があったときは刑法第 234 条の 2（電子計算機損壊等業務妨害罪）、事業者のコンピュータに虚偽の情報等を与えて不正な決済等をしたときは刑法第 246 条の 2（電子計算機使用詐欺罪）が適用されてきた。

以下では、2010 年（平成 22 年）1 月 1 日から 2016 年（平成 28 年）2 月 29 日にかけて、技術的手段の回避・無効化のための装置等の譲渡等に適用される不正競争防止法・著作権法及び当該装置等に係る電磁的記録の作出・供用行為に適用されることが多い私電磁的記録不正作出・供用罪が適用された 47 件の事例を整理する。

行為	適用法令			適用数（事件数）
	不競法	著作権法	私電磁	
製造・作出等			８	８
譲渡等	２９	６		３６
使用・供用			７	７
輸入	３			３
電気通信回線提供	３			３
				５６（４７）

４．１　映像コンテンツ分野

４．１．１　パッケージ

（1）事案

年月日	対象	行為	法令
2012 年 7 月 17 日	リッピングソフト	譲渡	不正競争防止法
2013 年 3 月 5 日	リッピングソフト	譲渡	不正競争防止法
2015 年 8 月 19 日	リッピングソフト	譲渡（注１）	著作権法

（注１）報道では、送信可能化をとらえたものか送信をとらえたものかが不明であること、さらに、実際にはアップロードしていたのではなくリッピングソフト蔵置サイトにリンクをはっていたとの報もある。送信可能化、送信、ほう助のいいずれかが確認できない。本項では、譲渡に適用されたものと見なし、下記では「譲渡等」に整理した。

（2）法の適用

分野	対象	行為	適用法令			適用数（事件数）
			不競法	著作権法	私電磁	
映像	リッピングソフト	製造・作出等				
		譲渡等	2	1		3（3）
		使用・供用				
						3（3）

上記の 3 事案のうち 2 件について不正競争防止法が適用された。いずれも「譲渡等」に対するものである。1 件については著作権法が適用された。なお、著作権法事件は、（注 1）の通り、譲渡に適用されたものと見なし、「譲渡等」に整理した。

４．１．２　放送（B-CAS 等）

（1）事案

年月日	対象	行為	法令
2012 年 6 月 19 日	不正 B-CAS カード	作出　供用	私電磁的記録不正作出・供用
2012 年 6 月 19 日	不正 B-CAS カード	譲渡	不正競争防止法
2012 年 9 月 6 日	不正 B-CAS カード	輸入	不正競争防止法
2012 年 9 月 27 日	不正 B-CAS カード	譲渡	不正競争防止法
2013 年 2 月 12 日	不正 B-CAS カード	供用	私電磁的記録不正作出・供用
2013 年 2 月 13 日	不正 B-CAS カード	譲渡	不正競争防止法
2013 年 4 月 21 日	不正 B-CAS カード	譲渡	不正競争防止法
2013 年 5 月 21 日	不正 B-CAS カード	譲渡	不正競争防止法
2013 年 5 月 30 日	不正 B-CAS カード	譲渡 供用	不正競争防止法 私電磁的記録不正作出・供用
2013 年 6 月 21 日	不正 B-CAS カード	譲渡	不正競争防止法 （商標法）
2013 年 7 月 19 日	不正 B-CAS カード	譲渡	不正競争防止法
2013 年 7 月 23 日	不正 B-CAS カード	作出 譲渡	不正競争防止法 私電磁的記録不正作出・供用
2013 年 7 月 31 日	不正 B-CAS カード	譲渡	不正競争防止法
2013 年 8 月 2 日	不正 B-CAS カード	譲渡	不正競争防止法
2013 年 11 月 26 日	不正 B-CAS カード	供用	私電磁的記録不正作出・供用
2013 年 12 月 5 日	不正 B-CAS カード	譲渡	不正競争防止法
2014 年 2 月 1 日	不正 B-CAS カード	輸入	不正競争防止法
2014 年 2 月 24 日	不正 B-CAS カード	譲渡	不正競争防止法
2014 年 5 月 22 日	不正 B-CAS カード	作出　供用	私電磁的記録不正作出・供用
2014 年 5 月 29 日	不正 B-CAS カード	譲渡（民事判決）	不正競争防止法
2015 年 1 月 20 日	不正 B-CAS カード	作出	私電磁的記録不正作出・供用
2015 年 7 月 15 日	不正 B-CAS カード	作出　供用	私電磁的記録不正作出・供用
2013 年 5 月 15 日	ＴＶ電波妨害機器	製造　販売	不正競争防止法
2015 年 3 月 10 日	TV チューナーと回避・無効化プログラム	TV チューナー譲渡及び URL 情報提供（注２）	不正競争防止法

（注２）報道では、回避・無効化プログラムのダウンロード先をメールで教えていたとされており、蔵置 URL 情報の提供と見做し得る可能があるが、判決書を入手しての確認ができていない。下記では「譲渡等」に整理した。

（２）法の適用

① B-CAS

分野	対象	行為	適用法令			適用数（事件数）
			不競法	著作権法	私電磁	
放送	B-CAS	製造・作出等			５	５
		譲渡等	１５			１５
		供用・供用			６	６
		輸入	２			２
						２８（２３）

23 事件のうち、18 件に対し不正競争防止法が、8 件に対し私電磁的記録不正作出・供用罪がそれぞれ適用された。2 件には、両法が重畳適用された。

不正競争防止法の 17 件のうちの 15 件は譲渡（1 件は民事判決）、2 件は輸入に対するものであった。また、（注 2）を踏まえ、「譲渡等」に整理した事件が 1 件ある。

私電磁的記録不正作出・供用罪が適用された 8 件のうち 5 件は作出罪が、6 件は供用罪が適用され、3 件は両罪が重複適用された。

② 電波妨害機器

分野	対象	行為	適用法令			適用数（事件数）
			不競法	著作権法	私電磁	
放送	電波妨害機器	製造・作出等	1			1
		譲渡等	1			1
						２（1）

有料放送を解約後も不正に視聴する電波妨害機器の製造及び販売に対し、不正競争防止法が適用されたとの報道から、「製造・作出等」1 件、「譲渡等」 1 件とした。

４．２　ゲームソフト分野

４．２．１　改造ゲーム

（１）事案

年月日	対象	行為	法令
2010 年 5 月 24 日	改造ゲーム機	譲渡	著作権法
2012 年 2 月 2 日	改造ゲーム機	譲渡 （著・海賊版）	不正競争防止法 （著作権法）
年月日	対象	行為	法令
2012 年 7 月 3 日	改造ゲーム機	譲渡	不正競争防止法
2012 年 8 月 14 日	改造ゲーム機	譲渡	不正競争防止法
2013 年 8 月 30 日	改造ゲーム機	譲渡	不正競争防止法
2013 年 9 月 20 日	改造ゲーム機	譲渡	不正競争防止法 （商標法）

（２）法の適用

分野	対象	行為	適用法令			適用数（事件数）
			不競法	著作権法	私電磁	
ゲーム	改造ゲーム機	製造・作出等				
		譲渡等	5	1		6（8）
		供用・供用				
		輸入				
						6（6）

上記の６事案のうち、５件について不正競争防止法が、１件について著作権法が、いずれも譲渡に対し適用された。

４．２．２　マジコン

（１）事案

年月日	対象	行為	法令
2012 年 5 月 30 日	マジコン	譲渡	不正競争防止法
2012 年 7 月 16 日	マジコン	譲渡	不正競争防止法
2014 年 5 月 16 日	マジコン	譲渡	不正競争防止法
2016 年 1 月 12 日	マジコン	輸入（民事判決）	不正競争防止法

（2）法の適用

分野	対象	行為	適用法令			適用数（事件数）
			不競法	著作権法	私電磁	
ゲーム	改造ゲーム機	製造・作出等				
		譲渡等	3			3（3）
		供用・供用				
		輸入	1			1（1）
						4（4）

4 件いずれも不正競争防止法事件である。うち 3 件は譲渡等に対するもの。1 件は、輸入差し止め及び損害賠償をめぐって争われ、2016 年（平成 28 年）1 月 12 日の最高裁の不受理によって約 9,562 万円の損害賠償が確定した民事事件である。

４．２．３　チート・ツール

（1）事案（注３）

年月日	対象	行為	法令
2015 年 7 月 10 日	チート・ツール	譲渡	著作権法
2015 年 7 月 29 日	チート・ツール	電気通信回線提供 作出　供用	不正競争防止法 私電磁的記録不正作出
2015 年 11 月 22 日	チート・ツール	譲渡	著作権法
2016 年 2 月 29 日	チート・ツール	作出　供用	私電磁的記録不正作出・供用

（注３）これら 4 事案について、運営者がどのような技術的手段を施していたのか、また、当該チート・ツールが当該技術的手段を回避・無効化する振る舞いをするプログラムであるのか否かについての詳細は明らかにされていない。しかし、2015 年 7 月 29 日東京地方裁判所の判決は、「…ゲームの正規利用者以外の者がゲームプログラムを実行できないようにするために営業上用いている技術的手段の効果を妨げることにより、上記ゲームプログラムの実行を可能とする機能を有するプログラム…」としており、少なくとも本事案においては、裁判所が、オンラインゲーム運営者が施す技術的手段を不正競争防止法上の技術的制限手段と評価し、当該技術的制限手段を回避・無効化するプログラムの提供を不正競争と認定したことは明らかになっている。

（2）法の適用

分野	対象	行為	適用法令			適用数（事件数）
			不競法	著作権法	私電磁	
オンライン G	チート・ツール	製造・作出等			2	2
		譲渡等		2		2
		供用・供用			2	1
		電気通信回線提供	1			1
						6（4）

著作権法の譲渡が適用された事件が 2 件、不正競争防止法の電気通信回線提供と私電磁的記録不正作出・供用罪が適用された事件が 1 件、私電磁的記録不正作出罪及び供用罪が適用された事件が 1 件ある。なお、前述（注 3）の通り、本主題についての評価は慎重である必要がある。

4．3　ビジネスソフト分野

（1） 事案

年月日	対象	行為	法令
2013 年 6 月 12 日	クラック・ツール	譲渡	著作権法
2014 年 10 月 15 日	クラック・ツール	譲渡	不正競争防止法
2014 年 12 月 5 日	クラック・ツール	譲渡	不正競争防止法
2015 年 6 月 24 日	クラック・ツール	譲渡 譲渡	不正競争防止法 著作権法
2015 年 9 月 8 日	クラック・ツール	電気通信回線提供(注 4)	不正競争防止法
2016 年 1 月 12 日	クラック・ツール	電気通信回線提供(同上)	不正競争防止法

（注 4）判例は「・・・回避するプログラム（クラックツール）を、インターネットオークション運営者のサーバコンピュータに記憶・蔵置した上、当該クラック・ツールの蔵置先ＵＲＬを、オークション落札者に提供した行為は、営業上用いられている技術的制限手段により制限されているプログラムの実行を、当該技術的制限手段の効果を妨げることにより可能とする機能を有するプログラムを電気通信回線を通じて提供するものであり、不正競争にあたる。」としている。

（2）法の適用

分野	対象	行為	適用法令			適用数（事件数）
			不競法	著作権法	私電磁	
ビジネスS	クラック・ツール	製造・作出等				
		譲渡等	3	2		5
		供用・供用				
		電気通信回線提供	2			2
						7（6）

6件のうち、著作権法で譲渡が適用された事件、不正競争防止法で譲渡が適用された事件2件、不正競争防止法と著作権法で譲渡が一度に適用された事件1件、不正競争防止法の電気通信回線提供が適用された事件2件を確認することができた。

第Ⅳ章　我が国における関連法制の適用に関して生じ得る争点

１　コンテンツ分野ごとのヒアリング調査結果

１．１　全体像

映像（放送）分野、ゲームソフト分野及びビジネスソフト分野でのヒアリングにおいて、技術的手段の回避・無効化について、何らかの法律上の対応に係る検討の必要性があるのではないか、との意見が寄せられた。

		技術的手段			技術的手段の回避・無効化以外の問題、及び、対策案
		利用の現状	回避・無効化の実態	何らかの法律上の対応に係る検討の必要性	
音楽	パッケージ	なし（過去CCCD等利用）	なし（技術的手段の利用がない）	なし	・従来型海賊版対策 ・違法なプロバイダに対する国際的に統一された規制 ・違法な海外サーバへの国内からのアクセス遮断 ・無料音楽聞き放題の違法アプリ規制 ・ビジネスモデルの再構築
	ダウンロード　フィーチャーフォン	利用（キャリア毎の独自技術）	あり	なし	
	ダウンロード　スマホ PC	2012 年以前利用 2012 年以降なし	2012 年以前:あり 2012 年以降:なし	なし	
	ストリーミング	利用（FairPlay、HLS 等）	あり（ネット上に回避・無効化ツール散見）	なし	
映像	パッケージ	利用（CSS、AACS 等）	あり	なし	・従来型海賊版対策 ・違法アップロードコンテンツの削除 ・ネットと動画共有サイトの連動 ・放送法における不正無料視聴に対する罰則規定 ・アクセスコントロールに対する著作権法整備 ・違法サイト紹介メール対策 ・不正 B-CAS カードのネットオークションにおける販売
	放送	利用（B-CAS、C-CAS）	あり	あり	
	ダウンロード	利用（FairPlay、Playready 等）	あり（ネット上に回避・無効化ツール散見）	なし	
	ストリーミング	利用（Playready 、Primetime 等）	なし	なし	
ゲームソフト	スタンドアロン	利用（主として非暗号型(フラグ型)）	前機種:あり 現機種:なし	あり	・著作権法における「送信」の定義 ・技術的手段のコスト問題 ・訴訟における技術内容の開示 ・国外で行われる不正行為に対する実効性ある対策
	オンライン	利用（認証技術）	あり	あり	
電子出版		利用	あり	なし	・スキャニング、画面キャプチャ ・技術的保護手段回避ツール流通 ・版面権立法 ・海外の海賊版サイト対策 ・その他
ビジネスソフト		利用（認証技術）	あり	あり	・プロバイダ責任制限法ガイドラインの位置づけ

１．２．１　放送

○「装置」と「プログラム」の別の者による分離提供について

【ヒアリングにおいていただいた意見】

・　B-CAS カードの改ざんカードは、不正競争防止法第 2 条第 1 項 11 号に言う「技術的制限手段を妨げる装置」に、また、改ざんプログラムは、同「当該機能を有するプログラム」に各々該当する。

・　2013 年（平成 25 年）に起きた VISIONPRO 事件は、単体では通常の性能のみを有する機器である VISIONPRO と呼ばれるチューナーをネット通販等で販売した後、有料放送に施された技術的制限手段を回避・無効化するプログラムのダウンロード先をメールで教えていた。その際、「装置」（チューナー）と「プログラム」の提供は、別の者によって行われた。

・　VISIONPRO 事件では、「装置」と「プログラム」の提供者の共謀が立証され不正競争防止法違反の有罪判決が言い渡されたが、両者の共謀が立証できないケースが起こり得る。

・　第 2 条第 1 項 11 号は、「技術的制限手段の効果を妨げることにより可能とする機能を有する装置」及び「「当該機能を有するプログラム」を規制対象としているが、これに、「組み合わせることで技術的制限手段の効果を妨げる機能を有する装置またはプログラム」を付加する法整備が必要ではないか。

１．２．２　ゲームソフト

○改造ゲーム機の製造行為について

【ヒアリングにおいていただいた意見】

・　技術的手段を回避・無効化するようにゲーム機を改造する「回避・無効化装置製造行為」が行われている実態がある。また、回避・無効化装置製造行為の方法や必要な道具等の情報を提供するウェブサイトも散見される。

・　このような製造行為は、不正コピーされたゲームソフトで遊ぶことを目的としていると考えられることから、回避・無効化装置の製造行為それ自体を規制対象に付加する法整備が必要ではないか。

○オンラインゲームにおけるチート行為等について

【ヒアリングにおいていただいた意見】

・　オンラインゲームのビジネスは、ゲーム自体は無料で提供し、そこで使われる道具や武器やキャラクター等のアイテムに対する課金（有料販売）で成り立っている。

・　現在のオンラインゲーム運営において、看過し得ない悪質なユーザーの行為としては以下のようなものがある。

①他人のＩＤ・パスワードを使ってゲーム運営者のサーバに不正アクセスし、他人のアイテム等を不正に取得する。

②チート・ツールを使って自分のアイテム等や、不正アクセスで不正に取得した他人のアイテム等のデータを書き換えた後、データが書き換えられたアイテム等を供用して、ゲームを有利に運ぶ。

③データが書き換えられたアイテム等を他人に販売する。

④チート・ツールを他人に販売する。

・　このうち、②の「アイテム等の不正な書き換え・供用」をチート行為と呼ぶことが多い。

・　チート行為が行われ、考えられない強さのゲーム参加者が出現すると、健全なユーザーが遠のいてしまうといった運営上のマイナスが生じる。また、運営サーバに意図しない動作が生じる場合もある。

・　運営者は、どのアイテムを誰がいくらで購入したかをサーバで管理しており、例えば、1個しか売れていないアイテムが 10 人に使われていれば、9 人は不正に入手したということが分かる。このような場合、運営者は、利用権原のないユーザーに対し、利用規約に基づき、注意喚起・警告し、場合によってはアカウント停止等の措置をとっている。

・　チート行為は、ゲームプログラムを書き換えるものではなく、ゲーム内のアイテム等に係るデータを書き換えるものであるので、どの法令違反で訴えることが可能なのか難しい面がある。

・　従って、現状では利用規約違反が一番多い対処策ということになる。

・　セーブデータを書き換えるチート・ツールを販売する者がいる。これだけでも止めたいが、対策がとれない。セーブデータを書き換えることによって、別のキャラクターが登場したり、敵のキャラクターを味方に変えたりというような、意図しない現象が起きてしまう場合もある。

・　著作権法の同一性保持権侵害で訴える場合、そのツールを買って使っているのはユーザーなので、ユーザーを直接侵害者として訴え、チート・ツール販売者は幇助で訴えるしかないと考える。

・　また、同一性保持権侵害を主張するには、「ありえない改変」がキーワードになるため、普通に遊んでいて到達できる可能性があれば主張できない。

・　キャラクターを自動で動かすチート・ツールもある。四六時中ずっと自動で動かして経験値を上げてから転売する。
・　②及び③について、データを書き換えたことをとらえて、私電磁的記録不正作出・供用罪が適用された事案がある。また、運営サーバに意図しない動作を起こしたとして、電子計算機損壊等業務妨害が適用されたケースがある。
・　①については不正アクセス禁止法が適用されたケースがある。
・　④については著作権法（技術的保護手段回避プログラム譲渡）、不正競争防止法（技術的制限手段回避プログラム電子通信回線提供）の適用事例がある。

１．２．３　ビジネスソフト

○ライセンス認証システムについて

【ヒアリングにおいていただいた意見】
・ ビジネスソフトは汎用コンピュータで繰り返し供用されるものであるため、プログラム自体には技術的制限手段を講じないのが一般的。ライセンス認証システム（プログラムの実行可能化条件として、メーカが送付する認証済みメッセージの受信とユーザーの PC への記録を求める仕組み）でビジネスを保護している。
・　CD-ROM 販売されたビジネスソフトをインストールする際、ユーザーは、CD-COM に同梱されている書類に書かれたシリアル番号の入力を求められる。インストールが終わった後、番号をネットオークションで売る者がいる。
・　供用期間や機能が制限される体験版や試用版などをメーカのウェブサイトからダウンロードする場合は、ダウンロードすると体験版用のシリアル番号が送られてくる。これを入力すれば、決められた期間や機能での供用が可能になる。このときユーザーの PC には未認証のシリアル番号等が記憶され、供用期間や機能にロックがかかる。しかし、この認証を回避・無効化し、供用期間や機能の制限のない製品版プログラムの実行を可能化する信号である不正なシリアル番号等をユーザーの PC 内に偽造・偽装するプログラム（クラック・ツール）の提供が行われている。
・　クラック・ツールは「技術的制限手段により制限されているプログラムの実行を当該技術的手段の効果を妨げることによる可能とする機能を有する」ものであるとして、提供した者に刑事罰を科す判決が幾つか出ている。
・　しかし、不正なシリアル番号や認証コードは依然としてネットオークションで出回っている。また、落札者にクラック・ツールを直接渡すのではなく、クラック・ツールが蔵置されている、あるいは、クラックの仕組みの解説を掲載するウェブページの URL を教えるといったやり方で言い逃れしようとしている。
・　認証技術は影像・音・プログラムと「ともに」記録されているものではないので、不正競

争防止法の対象外とする見解がある。経済産業省の準則にも、直ちに該当しないとの解釈が書かれている[85]。

- 現行不正競争防止法における技術的制限手段の定義は、現在広く採用されているライセンス認証システムを考慮したものではない。
- 技術は進歩しており、認証システムを技術的制限手段ととらえた上で、これを偽装して回避・無効化することを規制する不正競争防止法の整備が必要ではないか。
- また、現行準則におけるソフトウェア制限解除に関する上記記述はライセンス認証システムの存在を前提としておらず、現在の技術動向と齟齬がある。最新判例に鑑み、改定又は全面的に削除されるべきであり、また、改訂サダムする場合、現在の記述における結論の適用場面を限定・明確化することを要望する。

２　考察

２．１　単体では完全な回避・無効化機能を果たさない装置等の取扱い

放送分野の事業者からは、VISIONPRO 事件（本報告書 101 頁参照）を引き合いに、装置等単体では技術的制限手段を回避・無効化する機能はないが、特定のプログラムを合わせること等により回避・無効化が実現する場合の法的規制についての問題提起があった。

本論点に関し、経済産業省における平成 23 年不正競争防止法改正に係る議論[86]では、次の考え方を示している。

④単体では完全な回避機能を果たさない装置等の取扱い

昨今、装置等単体では技術的制限手段回避の機能を有しないものの、装置等単体に、特定のプログラム等を合わせることによって、初めて技術的制限手段の回避が実現されるような技術的制限手段回避装置等の提供形態が出現しているが、「のみ」要件の見直し後における当該装置等単体の提供行為に係る「不正競争」行為該当性については、以下のとおりと考えられる。

ある装置等単体について、それ単体では完全には回避効果を果たさないが、それと特定のプログラム等を合わせた装置等全体として、利用者の利用実態、販売者の販売態様などの事情を総合的に考慮しつつ判断した結果、明確に技術的制限手段を妨げる機能をその中核的機能とする装置等に該当すると考えられる場合であって、当該装置等単体の購入者が、購入後に技術的制限手段の回避を実現するためプログラム等を合わせることが確実である場合にお

85 経済産業省『電子商取引及び情報財取引等に関する準則』（2015 年）ⅲ.77。

86 産業構造審議会知的財産政策部会・技術的制限手段に係る規制の在り方に関する小委員会『技術的制限手段に係る不正競争防止法の見直しの方向性について（案）』4 頁～9 頁。
(http://www.meti.go.jp/committee/sankoushin/chitekizaisan/gijutsutekiseigen/004_03_00.pdf)

いては、当該装置等単体の提供行為についても、不正競争防止法第 2 条第 1 項第 10 号及び第 11 号に規定する回避装置等の提供行為を構成する蓋然性の高い行為と考えられることから、「のみ」要件が見直された場合においてもなお、これらの号の規制対象とし得ると考えられる。

VISIONPRO 事件では、報道によれば、チューナー販売事業者による単体では回避・無効化機能を有しないチューナーの販売後に、この販売事業者と共謀した別の事業者が当該チューナーにダウンロードすることで当該チューナーに回避・無効化機能を備えさせることができるプログラムのダウンロード先を、購入者に電子メールで通知していた事実が認められるようである。また、同事件については有罪判決がなされたとの報道もあるが、そのような共謀の事実や購入者へのダウンロードの働きかけ等の事実が、「・・・当該装置等単体の購入者が、購入後に技術的制限手段の回避を実現するためプログラム等を合わせることが確実」との認定のために積極的に評価されたものと考えられる。

本論点については、このように現行法下においても、法律の解釈・運用により、一定の場合に規制がなされている例があるが、一方で、ヒアリングにおいては、「組み合わせることで技術的制限手段の効果を妨げる機能を有する装置またはプログラム」を付加する法整備が必要ではないかとの意見もあった。

この点について、そのような規制を求めるニーズは理解できるものではあるが、そのような法規制は、場合によっては適法行為の組み合わせを違法行為とすることにもつながり得るため、適法な行為への不当な萎縮効果の有無や、適法・違法行為の境界を明確なものとするための適切な法律要件の定立困難性などを十分に踏まえなければならない。個別具体的な事情に応じて、事案ごとに妥当な結論を導くことが可能となる利点も存在することも考え合わせると、本論点については、現行法の解釈による対応状況を見定めつつ、慎重に検討を進めていくべきものであると考えられる。

２．２　技術的手段の回避・無効化に係る「情報提供」の規制

一般的に、情報提供それ自体は、不正競争防止法第 2 条第 1 項第 11 号及び第 12 号の定義上、不正競争行為と評価することは困難であるが、ヒアリング等においては、以下のような技術的手段の回避・無効化に係る情報提供について問題意識が示された。

提供される情報の分類	提供される情報例とその提供のされ方
（１）回避・無効化装置・プログラムの製造・改造等に係る情報	・正規ゲーム機で不正ゲームデータが作動するように改造する方法に関する情報（改造コードや改造手順等）をインターネットで公開 ・他人がインターネットに掲載した上記の情報について、その URL を自らの HP に転載、又は電子メール等で送信
（２）回避・無効化装置・プログラムの入手行為や回避・無効化行為を容易化する情報	・回避・無効化装置・プログラムの入手場所や入手方法（その販売店や購入方法）について自身のホームページで紹介 ・他人がアップロードした回避・無効化プログラムの URL をインターネット掲示板サイトに書込み、又は電子メール等で送信 ・回避・無効化装置・プログラムの供用方法（操作方法や PC でのセッティング方法等）を自身のブログで紹介 ・オンラインゲームのチートのためのゲームデータ改ざん方法を SNS を通じて発信
（３）認証情報	・ビジネスソフト等のアクティベート認証に用いられるシリアルキーに関して、キージェネレーターにより偽造したシリアルキーをインターネットオークションサイトにおいて販売 ・不正に入手した他人の ID・パスワードや、偽造した ID・パスワードをメール等で送信

（１）回避・無効化装置・プログラムの製造・改造等に係る情報

技術的手段の回避・無効化装置・プログラムの提供行為自体は、現行不正競争防止法及び著作権法の規制対象となり得るが、当該装置・プログラムを作り出すための製造・改造方法に関する情報を提供する行為は、基本的に法規制の対象とはなっていない。

当該情報提供行為の規制の是非については、それが直ちに回避・無効化装置等の製造等につながるとは必ずしも言えないことに加えて、表現に関する自由度は最大限確保すべきであること[87]や、その製造・改造行為自体は不正競争防止法による規制対象となっていない[88]（著作権法においては一部規制対象）こととの均衡などを踏まえた検討が必要になるものと考えられる。

87 不正競争防止法に技術的制限手段に係る規定が盛り込まれた平成 11 年改正当時においても、無効化手段としての情報提供行為に対する規制の検討に関し、「情報提供については最大限の自由度を確保すべきことなどを考慮すれば、相当に慎重な検討が必要」とされた。著作権法令研究会・通商産業省知的財産政策室編『著作権法 不正競争防止法改正解説』218 頁。

88 技術開発や情報利用への悪影響が出ないよう、当該装置等の製造は規制せず、その提供を規制する。前掲・産業構造審議会・17 頁～18 頁。

（２）回避・無効化装置・プログラムの入手行為や回避・無効化行為を容易化する情報

回避・無効化装置・プログラムの入手場所、入手方法、供用方法、アップロードされた回避・無効化プログラムの URL 情報、データ改ざん方法などの提供行為についても、基本的には法規制の対象とはなっていない。

しかし、当該情報提供行為の規制の是非についても、（１）同様の観点や、回避・無効化装置・プログラムの単純所持や供用自体は不正競争防止法による規制対象となっていない（著作権法においては一部規制対象）こととの均衡なども踏まえた慎重な検討が必要になるものと悪考えられる。

（３）認証情報

認証技術において、その認証の方法として ID・パスワードやシリアルキー等の認証情報を用いる場合に、その認証技術を回避・無効化する手段として、不正な ID・パスワードやシリアルキーが利用される場合がある。そのような不正な認証情報を作出するプログラム（キージェネレーター等）の譲渡等については、不正競争防止法等の適用の余地はあると言えるものの、その不正な認証情報自体のやり取りについては、少なくとも不正競争防止法の規制の対象ではない。

この点、不正な認証情報の提供自体に何らかの規制がなければ、その作出のためのプログラム（キージェネレーター等）の譲渡等を規制する意義が薄れてしまうおそれがあることや、特にビジネスソフトの分野において実際に不正なシリアルキーの売買が行われていることなどを踏まえると、不正な認証情報に対する規制については検討に値するものとも考えられる。

ただし、無断で他人の ID・パスワードを譲渡等する行為は不正アクセス禁止法による規制対象となり得るなど、不正な認証情報の中には、その提供等が刑法等の他法令による規制対象となるものも存在することが思料されることから、当該情報提供行為の規制の検討の前提として、刑法等の他法令の適用可能性について精査する必要があるものと考えられる。

なお、米国裁判例の中には、他人の認証情報（ID・パスワード等）が不正な手段・動機で入手され利用された場合に、DMCA 上のアクセスコントロールを回避するものと主張した原告の請求を棄却する裁判例が少なくとも二つ存在する（第Ⅵ章 1. 2（13）と（25）の各裁判例）。規範的に見れば権利者の意図しないコンテンツへのアクセスではあるが、裁判所は、各被告が技術的手段を物理的・技術的に迂回・回避することも、機能を無効化することもなく、コンテンツにアクセスしているため、DMCA 違反は認められないとしている。広義の意味ではアクセスコントロールの手段とも位置づけられる認証技術の不正（取得後）利用行為は、アクセスコントロールを正面から規制している米国でさえ、アクセスコントロールを回避するものと評価されていない。

（4）まとめ

上述のとおり、技術的手段の回避・無効化に係る「情報提供」といっても、その情報提供が実際に回避・無効化につながる蓋然性の高さや、通常、犯罪に当たる行為の方法を提供したとしても、その情報提供行為自体は不可罰であることが多いこととの均衡といった点において、様々な性質の「情報提供」が存在するものと考えられる。

ただし、その中には、ビジネスソフトのライセンス認証に用いられる不正なシリアルキーの提供のように、不正なシリアルキーを作出するプログラム（キージェネレーター）等の提供が不正競争防止法における規制対象となっていることとの均衡などから、一定程度の当罰性があるともいえる行為が存在するが、不正競争防止法ではなく、刑法等の他の法令による規制対象となることについて、なお精査の余地があるものと思われる。

よって、本論点については、「情報提供」のうち、真に当罰性があると考えられる行為を見極め、その行為が現行の他法令において規制される可能性などを検討した上で、新たな法律上の対応の必要性について慎重に検討すべきものと考えられる。

２．３　「チート」に対する規制

特定のユーザーによるチート行為に対し、オンラインゲーム運営者が講じ得る法的規制手段としては、利用規約違反を根拠とする制裁、不正競争防止法、著作権法、私電磁的記録不正作出・供用罪、不正アクセス禁止法、不正指令電磁的記録作成罪又はそれらの組み合わせが考えられる。

運営者として最も容易な規制は、利用規約におけるチート行為の禁止及び規約違反に基づく制裁としてアカウント停止等の措置をとるものであるが、法的な罰則があるわけでなく、一般予防の見地から抑止力には限界がある。

一方で、本調査により、チート行為に関連して、

- 不正アクセス禁止法（チート行為をするために他人のID・パスワードを用いて事業者のサーバに不正に侵入した事件等）。
- 不正指令電磁的記録作成罪（かかる不正アクセスを可能とするために他人のＩＤ・パスワード等を得るためのウィルスを作成・提供した事件等）、
- 電子計算機損壊等業務妨害罪（チート・ツールを作動させ、運営者の意図しない動作を繰り返し、運営業務に支障を生じさせ業務を妨害した事件等）、
- 電子計算機供用詐欺罪（不正アクセスにより、オンラインゲーム上の仮想通貨を騙取した事件等）、
- 私電磁的記録不正作出・供用罪（オンラインゲームのキャラクターに通常ではあり得ない動きをさせたり、武器や道具を無限に増やしたりするチート・ツールを販売した事件等）

の適用事例が確認されたところである（第Ⅲ章参照）。

不正競争防止法に関しては、「チート」を制限する技術が、同法第２条第７項に規定する「影像

若しくは音の視聴若しくはプログラムの実行又は影像、音若しくはプログラムの記録を制限する手段」に該当するか否かが不明確ではあるものの、そもそも不正競争防止法により規制すべき行為か否か、上記のとおり刑法等の他法令による適用事例が確認される中で法無規制の射程外となっている「チート行為」がどの程度存在するのか、といった点については精査の余地があるものと考えられる。

よって、本論点については、そのような点についての精査を前提に議論を進めるべきものと考えられる。

２．４　「認証技術」の回避・無効化

ビジネスソフト分野において用いられるライセンス認証などの認証技術が、不正競争防止法の保護を受けるためには、そのような認証技術が、同法第 2 条第 7 項に規定する「技術的制限手段」の定義を満たす必要があるが、「第 1 章 6．3．3　経過、現状及び課題」で述べたとおり、特にビジネスソフトのアクティベーションに係る認証技術等については、その定義を充足するとの解釈には至っていないという現状もある[89]。

一方で、近時、Microsoft 社が著作権を有する試用版プログラム「Office 2013 Professional Plus」を、不正なシリアルキーをユーザパソコン内に偽造・偽装することで、同社のライセンス認証システムによる認証を回避・無効化させ、体験版・制限版のプログラムを供用期間や機能制限のない製品版プログラムとしての実行を可能にするクラック・ツールの提供が不正競争行為であると判断する下級審裁判例が続いているという現状もある。

したがって、アクティベーションを含む認証技術について、一律に不正競争防止法第 2 条第 7 項に規定する「技術的制限手段」に該当しないという解釈・運用は適当とは言えず、その技術の内容・態様に応じて、同法の技術的制限手段と評価できるかを個別具体的に判断されるべきものと考えられる。そして、そのような解釈・運用がなされるべきことについて、様々な機会を捉まえて明確化を図っていくことが望まれる。

89 経済産業省『電子商取引及び情報財取引等に関する準則』（2015 年）ⅲ.77。準則は、「しかしながら、一般に、制限版における制限方法は、特定の反応をする信号がプログラムとともに記録されていたり、プログラム自体が特定の変換を必要としたりするようなものではなく、技術的制限手段に該当しない。」と述べる。

３　技術的手段の回避・無効化以外の問題に関する意見

本調査の一部として実施したヒアリング調査においては、技術的手段の回避・無効化以外の問題や問題解決策案についての意見が寄せられた。

３．１　音楽分野

【従来型海賊版対策】

○ 無料聞き放題と銘打ったサイトやアジアの一部の国・地域のサイトに、日本の権利者の許諾を得ていない不正な音楽コンテンツが多数アップされている。正規版の発売と同日に、歌詞まで付けてアップされることもある。

○ 違法サイトには、正規サービスと遜色のない豊富な品ぞろえを有するサイトもある。

○ 中高生を含む若年層の中には、正規サービスを無料提供期間だけ利用し、この期間が終了すると違法サイトに移行する者がいる。

○ 現時点において、CD、ダウンロードでは技術的保護手段を施していない。施しているのは、ストリーミングだけである。違法なサイトにアップされているのは、CD やダウンロードのデータをリッピングしたものと考えられる。このような状況において、わざわざ、ストリーミングのデータに施された技術的制限手段を回避・無効化する者はいないと考えられる。

【違法なプロバイダに対する国際的に統一された規制】

○ 海外の違法サイトが野放しになっているのは問題である。プロバイダの責任に関して、国際的に統一したルールを作ることが必要ではないか。

【海外の違法サイトへの国内からのアクセス遮断】

○ 海外の違法なサイトに対する国内からのアクセスを遮断することはできないか。

【無料音楽聞き放題の違法アプリ規制】

○ 無料音楽聞き放題と銘打った違法なサービスに対する規制が必要である。現状、このような違法なサービスのアプリ開発提供者には利益が入るが、権利者には何も入らないという事態も生じている。

【ビジネスモデルの再構築】

○ 逆に、法律でこれ以上縛りをかけても効果があるかどうかわからない。むしろ、自由にコピーが出来る技術環境の中でのビジネスモデルの組み立てを再構築する必要があるのではないか。

３．２　映像分野

３．２．１　映像配信

【従来型海賊版対策】

○パッケージや配信で用いられている技術的手段を破らなくても、画面をキャプチャしたり、4K ビデオで盗撮すれば複製物はできてしまう。このようにしてユーザーの手元で作成された複製物が動画共有サイト等のネットにアップされると、配信事業者のビジネスを脅かすことになる。

○オンデマンド放送の動画のキャプチャソフトが存在しており、画面に表示される動画をファイルにすることができる。視聴期間が設定されている動画も、保存して後から再生することができる。機能としてはキャプチャするだけなので、ユーザーの手元にある限り違法とは言えない。

○ネットにアップされた場合、配信から抜かれたものであれば、予め透かしに埋め込んでいたウォーターマークをもとに追跡することができる。どのデバイスからかということが分かる場合もある。しかし、画面キャプチャや盗撮ではそれもできない。

【違法アップロードコンテンツの削除】

○日本で動画共有サイトサービスをしている海外法人や、海外のサイトに対して現状は何もできない。

○無料の動画サイトが存在していることが問題。ユーザーが無料に慣れてしまうと、課金の文化がなくなり、ビジネスが成り立たなくなる。

○TVer はこの問題の対策として作られた認識している。見逃し配信が 1 日遅れれば違法コンテンツがネット上にアップロードされてしまう。正規の無料配信を行うことで違法コンテンツのアップロードを抑える苦肉の策である。TVer はじめ正規の無料配信を行うことで違法コンテンツのアップロードを抑えることが必要である。

○動画共有サイト等にアップされた違法コンテンツの削除要請を、プロバイダ責任制限法に基づき徹底的に行う。

【ネットと動画共有サイトとの連動】

○他方、ネットとの連動も考えていくべき。例えば、現在、ゲームの実況が動画共有サイトで行われている。以前、ゲーム動画は削除の対象だったが、現在は上手く連動してゲームのプロモーションにしている。また、テレビでサッカーの試合をやっているとき、サッカーをテレビで観ている視聴者が試合について議論をしているところを動画共有サイトで“生放送”して盛り上がった事例もある。

３．２．２　放送

【放送法における不正無料視聴に対する罰則規定】

○放送法第 157 条には、有料放送事業者との契約なしに有料放送を受信してはならないと規定しているが、実際に不正視聴した者に対する罰則規定がない。不正視聴者に対する罰則が必要と考えている。

【アクセスコントロールに対する著作権法整備】

○放送のスクランブル解除などのアクセスコントロール回避・無効化は、現時点において、不正競争防止法と著作権法による規制の対象である。しかし、著作権法による規制はコピーコントロールを有効に機能させるためのアクセスコントロールの回避・無効化に限定されており、全面的な規制ではない。

【海外違法サイト紹介メール問題】

○現在、日本の有料テレビ放送を見ることができる違法サイトを紹介してアクセスさせるランダムメールが問題になっている。違法サイトは海外にある。メールの発信元も海外のようだが、メールがサーバを転々としており、発信元を特定しにくい。

【不正 B-CAS カードのネットオークションにおける販売】

○不正改造した B-CAS カードや B-CAS カードを書き換える不正プログラムに関する情報が検索エンジンで上位に来る。また、これらがインターネットオークションで販売されている。最近は、商品の紹介の仕方が巧妙になり、画面上からは不正と判断しにくく、プロバイダに削除要請をしても対応してもらえないケースがある。

３．３　ゲームソフト分野

【著作権法における「送信」の定義】

○著作権第 2 条第 1 項第 20 号の定義に「記録・送信する方式」と書かれているが、「送信」の定義がない。遠距離に信号を送る場合を想定しているとすると、ゲームソフトの場合のように、カートリッジからゲーム機本体に送信する場合はどうなのか。カートリッジとゲーム機本体の間の部分が含まれないとすると、この部分の暗号化は保護対象外ということになる。カートリッジとゲーム機本体の間で行う送信も著作権法に言う「送信」に該当するということを明文化することが必要である。

【技術的手段のコスト問題】

○法制度ではないが、技術的保護手段を利用する場合、技術供用料が高い。ペンタゴンが使っている優れたセキュリティ技術があるが、供用料も超一流の額で、相当な売り上げを見込むことのできるメジャーなタイトルでないと使えない。強固な技術を安価に使うことができるようになるとありがたい。

【訴訟における技術内容の開示】

○セキュリティ技術に関する訴訟では、技術内容やそれがどのように回避・無効化されたかを裁判所で公にする必要が出てくる。国によって異なるが、一般に、かなりのレベルまでオープンにする必要がある。閲覧制限はかけられるが、一番みせたくないとされる相手方に示さないといけない。例えば、特定の業者しか実現できていない回避・無効化方法があった場合、その業者を訴えると当該回避・無効化方法を説明しなければならず、この方法が他の業者に伝わって被害が拡大するおそれがある。

【国外で行われる不正行為に対する実効性ある対策】

○マジコンは、現時点でほぼすべてが中国で作られ、中国から発送されるので、取り締まりは税関が頼りである。根本を断とうとすれば、中国の店舗や工場の取り締まり、送金に関与している人物への対策を取る必要がある。日本人がかかわっているものがあり、刑事事件で逮捕してもらったが、証拠不十分になったことがある。送金に使われている銀行口座を止めようとしたが、生活にも使われている口座だとして凍結ができなかった。実効性のある対策は日本だけではできないのではないか。

３．４　電子書籍分野

【スキャニング、画面キャプチャ】

○インターネットオークションで裁断本が売られている状況がある。また、ネットショップの中古本のなかに裁断書籍が並んでいる。これらは、明らかに自炊行為を誘発するものであると思うが、ただちに違法にはあたらない。

○紙のスキャンや電子版の画面キャプチャで、“有効な”海賊版が簡単にできてしまう。海賊版をつくるのが目的であれば、わざわざ電子書籍に施された難しい技術的制限手段を回避・無効化する必要はない。紙の本を裁断して PDF 化すれば済む。

○業界としては紙のスキャンによる海賊版に対する意識が高く、電子書籍の技術的制限手段の回避がクローズアップされることはない。技術的制限手段が破られても被害は軽微だが、海賊版の被害は非常に大きい。

○なお、画面キャプチャの場合、マンガ・コミックスは電子書籍版とほぼ同じクオリティのものができるが、文章作品は、キャプチャするとリフロー（文字サイズを変更すると画面の大きさに合わせて 1 行の文字数が自動的に変更される表示方法）しない版になるので、利便性は下がる。

【技術的保護手段を破るツール流通】

○技術的保護手段を破るオープンソースのツールが出回っている。このようなオープンソースのツールの開発者は愉快犯的な者が多く、戦うのは大変。アップローダと戦うのはあり得ると思うが、彼らの多くは海外にいる。

取り締まりをすればするほど、取り締まられる側は僻地へいく傾向がある。

【版面権立法】

○作家の先生が非独占で許諾を出していた場合、版面権がないと侵害対策ができない。版面権を立法してほしい。

【海外の海賊版サイト対策】

○発売前の雑誌をスキャンしたものがアップロードされる。英語と中国語に翻訳され、その後、さらに様々な言語に翻訳される。

日本では海賊版の読者は多くないが、海外は海賊版サイトがライセンシーの事業を圧迫している。その原因は紙をスキャンして作られた海賊版。海賊版配信サイトはアドネットワークで儲けている。Notice&Takedown に基づく削除要請が行っているが、外国のサーバは手が出せない。国レベルで動いてほしい。

【その他】

○プラットフォームの手数料が高いのでブラウザベースで配信しているところも少なくない。外資大手の手数料は 30%であり、他の会社もそれに追随している。これまでのキャリア決済は 10～15%、クレジット決済はもっと低かった。手数料を考えると、今後は配信会社がストリーミングのサービスを行うこともあり得る。

○著作権法を強化し過ぎるとマイナスの場合があり得る。例えば、電子書籍は、アナログ本と異なり家族や友達に貸すなどの行為ができないが、家族で一緒に読むサービスがあってもよいのかも知れない。ゆるくして広がるサービスもある。

技術的制限手段についても同じで、制限手段をかけると不正が減って売上があがり、かけないと不正が横行して売上が減るのかどうかわからない。

３．５　ビジネスソフト分野

【プロバイダ責任制限法ガイドラインの位置づけ】

○掲示板については、プロバイダ責任制限法ガイドラインの基づき削除要請ができているが、ガイドラインのままでいいのか、法的なレベルまで高めるべきかという問題がある。権利者としては法的レベルまで上げてもらう方がよい。

第Ⅴ章　国際議論

１　ＷＩＰＯ条約 [90]

（１）経緯

インターネット時代の到来により、エンターテインメント・コンテンツ産業のビジネスがネットワーク上の配信モデルへと移行するようになり、オンライン上での利用許諾の必要が高まるなど、契約の重要性が高まる一方、著作権者等自身が自らの権利を守るために技術的な手段（暗号化、パスワード、ログイン手順、電子透かしなど）を用いることが増えるようになった。しかし、そのような手段を講じたとしても、それを回避・無効化する者、そしてそれを業とする者が現れるため、当該手段を法的に保護する必要が生じた。それが国際的なレベルで認識された結果が 1996 年の WIPO 条約に盛り込まれた技術的手段の保護である。

なお、後述するとおり、WIPO 条約における技術的手段の保護の内容が、「技術的手段に対する十分な法的保護と効果的な法的救済」の付与を義務づけるという極めて抽象的な内容にとどまったため[91]、加盟国において一定の裁量が付与され、地域ごとに対応の差が生じることとなった。その時間的経緯を俯瞰すると以下の表のとおりとなる。

	国際条約 EU(指令･CJEU)	各国法整備	各国主要動向
1990			
1991	EU プログラム保護（ソフトウェア）指令		EU･EU 評議会の暗号化されたテレビサービスの法的保護に関する推奨･視聴覚録音物のパイラシー（盗用）への対抗策についての推奨
1992		米･家庭内録音法	
1993			
1994			
1995			米･ホワイトペーパーで技術的手段の保護を課題として明記。
1996	WIPO(WCT ・ WPPT)条約採択		

[90] Paul Goldstein＝Burnt Hugenhotz, International Copyright (2010, Oxford Univ. Press) §9.1.6

[91] 米国は、クリントン政権が 1995 年に出しているホワイトペーパーにおいて技術的手段の強力な保護を求めており、これを国際条約レベルで実現することを企図していたが、アフリカ諸国の強い反対によってそれを明確にはできなかった。Paul Goldstein, Copyright Highway(2003), at 174-175

	国際条約 EU(指令･CJEU)	各国法整備	各国主要動向
1997			
1998	EU 条件付アクセス指令	米･デジタルミレニアム著作権法(DMCA)	
1999		日･不競法改正 日･著作権法改正	
2000			米･第1回 DMCA 規則制定手続(適用除外の公表)
2001	EU 情報社会指令		
2002	WIPO(WCT ・ WPPT)条約発効		
2003		独・著作権法改正 英・著作権法改正	米・第 2 回 DMCA 規則制定手続（適用除外の公表）
2004			米・Chamberlain 事件
2005			
2006		仏・著作権法改正	米・第 3 回 DMCA 規則制定手続（適用除外の公表）
2007			
2008			英・Higgs 事件
2009	EU プログラム保護指令改正 EU、WIPO 条約批准		日・DS 該当性事件
2010			英・DS 事件. 米・MDY 事件 米・第 4 回 DMCA 規則制定手続（適用除外の公表）
2011		日・不競法改正	仏・DS 事件
2012		日・著作権法改正	米・DMCA 適用除外
2013			日・DS 差止等事件(地)

	国際条約 EU(指令･CJEU)	各国法整備	各国主要動向
2014	CJEU DS 事件先決裁定（Milano Tribunal からの付託に基づく）		日・DS 差止等事件(高)
2015	TPP 協定大筋合意		米・第 5 回 DMCA 規則制定手続（適用除外の公表） イタリア･(CJEU 裁定後) DS 差止事件（Milano Tribunal)
2016	TPP 協定署名式		日・DS 差止等事件(最)

（2）内容

WIPO 条約の第 11 条は、次のように定めている[92] [93]。

第 11 条　技術的手段に関する義務 締約国は、著作者によって許諾されておらず、かつ、法令で許容されていない行為がその著作物について実行されることを抑制するための効果的な技術的手段であって、この条約又はベルヌ条約に基づく権利の行使に関連して当該著作者が用いるものに関し、そのような技術的手段の回避を防ぐための適当な法的保護及び効果的な法的救済について定める。

上記条文の文言から明らかなとおり、技術的手段の保護について詳細を定めないオープンエンドな規定であり、加盟国における国内法制化において、かなりの裁量が与えられている。後述のとおり、米国及び EU がそれぞれ細部で異なる技術的手段の保護法制をとるに至った要因は、このオープンエンドな条文の故である。なお、同条約は、技術的手段の保護について著作権の枠組の中で実現することを要求はしていないが、多くの国では著作権法の中で規制している[94]。

---

[92] 公益社団法人著作権情報センター（以下「CRIC」という。）の翻訳による。
http://www.cric.or.jp/db/treaty/wch_index.html#11

[93] WIPO 条約は著作権に関する国際条約であるが、実演家・レコード製作者の権利を保護するために用いられている技術的な手段についても、WIPO 実演・レコード条約（WPPT）18 条で同様の技術的手段の保護が定められている。

「第十八条　技術的手段に関する義務
締約国は、実演家又はレコード製作者によって許諾されておらず、かつ、法令で許容されていない行為がその実演又はレコードについて実行されることを抑制するための効果的な技術的手段であって、この条約に基づく権利の行使に関連して当該実演家又はレコード製作者が用いるものに関し、そのような技術的手段の回避を防ぐための適当な法的保護及び効果的な法的救済について定める。」（CRIC の翻訳による）

[94] 前掲 Paul Goldstein＝Burnt Hugenhotz,,　335 頁

日本では、著作権法 2 条 1 項 20 号、同 30 条 1 項 2 号、同 120 条の 2 第 1 号及び不正競争防止法 2 条 1 項 11 号、12 号、同 3 条）において履行されている。著作権法においていわゆるコピー等利用制限技術（著作権侵害行為を防止するための技術的措置）の回避・無効化が、不正競争防止法においては、コピー等利用制限技術に加えて、アクセス制限技術（著作物性を問わず、対象へのアクセスを規制する技術的措置）の回避・無効化が、それぞれ一定の要件の下で禁止され、法的救済措置が定められている。

２　ＥＵ 指令

２．１　情報社会指令第 6 条

情報社会指令（E.C. Copyright in the Information Society Directive of 2001）第 6 条は、技術的手段の保護について、次のように定めている。情報社会指令第 6 条は、EU 領域内において WIPO 条約の定める技術的手段の定めを履行するものである。ただし、WIPO 条約 11 条及び WIPO 実演家・レコード条約 18 条の定める内容があいまい・抽象的だったため、指令において定める内容について加盟国その他利害関係人間で様々な議論を生み、一定の合意をするために妥協の産物の形となったと評価されている[95]。

第 6 条[96]

技術的手段に関する義務

1. 加盟国は、効果的な技術的手段の目的を知って、又は合理的に知るべくして、利害関係者がそれを回避することに対して十分な法的な保護を提供するものとする。

2. 加盟国は、(a)効果的な技術手段の回避を目的として広告宣伝、販売活動、営業活動がなされる、(b)効果的な技術手段を回避すること以外に商業的に重要な目的又は利用方法が限られている、若しくは(c)効果的な技術手段を可能又は促進させる目的を第一次的なものとして、設計、生産又は改良又は実施される、装置、商品、部品の製造・輸入・頒布・販売・貸与・販売又は貸与のための広告・営利目的での所持若しくはサービスの提供に対する十分な法的保護を提供するものとする。

3. 本指令において、「技術的手段」との表現は、その通常の動作において、法律に規定された著作権又は著作隣接権（関連権）若しくは Directive 96/9/EC の第 3 章に規定された特別法 (suigeneris) 上の権利者によって許諾されていない著作物その他の権利の対象に関する

95 Prof. mr. M.M.M. van Eechoud , Mr. dr. L. Guibault , Prof. dr. N. Helberger , Prof. mr. P.B. Hugenholtz , G. Westkamp & T. Rieber-Mohn," Study on the Implementation and Effect in Member States' Laws of Directive 2001/29/EC on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society" （以下「IVIR Study」という。）, at 73.

96 指令中の「acceess control」、「copy control」は、便宜上、報告書における定義の例外として、カタカタ表記の訳語を当てた。

行為を阻止又は制限することを意図するあらゆる技術、装置又は部品を意味する。技術的手段は、アクセスコントロール若しくは、暗号化、スクランブル、その他著作物又は他の権利の対象物の変容もしくは保護目的を達成するコピーコントロールの仕組といった保護プロセスの提供を通じ、著作物又はその他の権利の対象がコントロールされる場合に、「効果的」なものとみなされるものとする。

4. 第 1 項に定められる法的保護に関わらず、権利者と利害関係者との間の契約など、権利者によってとられている任意の手段がない場合、加盟国は、5 条(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) 又は (3)(e)に従って国内法で規定された権利の例外又は制限の受益者に対し、当該受益者が例外又は制限からの利益を享受するに必要な範囲で、かつ、当該受益者が保護された著作物又はその他の権利の対象に対する適法なアクセスを有している場合、当該例外又は制限による利益を享受する手段を権利者が提供するように適切な措置を講じるものとする。

加盟国は、また 5 条(2)(b)に従って規定された例外又は制限の受益者に関し、このような措置を講じることができる。ただし、5 条(2)(b) and (5)に従った複製の数に関して十分な手段をとることを妨げることなく、これらの規定に従って例外又は制限から利益を得るために必要な範囲での私的複製が許容されていない場合に限る。

権利者によって任意にとられた技術的手段（任意の契約の履行の際にとられた手段も含む）及び加盟国によってとられた手段の履行の際にとられた技術的手段は、第 1 項の法的保護を享受するものとする。

第 1 及び第 2 パラグラフは、公衆が選択する場所から、又は公衆が選択する時間に応じてアクセスできる形態で合意された契約条件に基づき提供されている著作物及びその他の権利の対象物には適用されないものとする。指令 92/100/EEC and 96/9/EC に本条文が適用される場合には、本項も同様に適用される[97]。

[97] Article 6 の原文は以下のとおりである。
Article 6 (Obligations as to technological measures)
1. Member States shall provide adequate legal protection against the circumvention of any effective technological measures, which the person concerned carries out in the knowledge, or with reasonable grounds to know, that he or she is pursuing that objective.
2. Member States shall provide adequate legal protection against the manufacture, import, distribution, sale, rental, advertisement for sale or rental, or possession for commercial purposes of devices, products or components or the provision of services which:
(a) are promoted, advertised or marketed for the purpose of circumvention of, or
(b) have only a limited commercially significant purpose or use other than to circumvent, or
(c) are primarily designed, produced, adapted or performed for the purpose of enabling or facilitating the circumvention of any effective technological measures.
3. For the purposes of this Directive, the expression "technological measures" means any technology, device or component that, in the normal course of its operation, is designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder of any copyright or any right related to copyright as provided for by law or the sui generis right provided for in Chapter III of Directive 96/9/EC. Technological measures shall be deemed "effective" where the use of a protected work or other subject-matter is controlled by the rightholders through application of an access control or protection process, such as encryption, scrambling or other transformation of the work or other subject-matter or a copy control mechanism, which achieves the protection objective.
4. Notwithstanding the legal protection provided for in paragraph 1, in the absence of voluntary measures taken by rightholders, including agreements between rightholders and other parties concerned, Member States shall take appropriate

なお、EU においては、情報社会指令に先立ち、技術的手段の規制を定める 2 つの指令が存在する。その結果、EU においては、技術的手段の保護に関連する指令が 3 つ共存するため、その相互関係を意識する必要がある。その点については、以下に、情報社会指令に先立つ 2 つの指令を紹介した後に述べる。

２．２　コンピュータ・プログラム保護指令（1991 年、2009 年[98]）

情報社会指令が出される以前に、1991 年にコンピュータ・プログラムの法的保護に関して定められた指令である。欧州委員会は、WIPO 条約の締結前から技術的手段の保護の必要性について検討しており、1988 年のグリーンペーパーにおいて、デジタル録音機の製造者に技術的手段の保護機能をビルトインすることを義務づけることも提案されたが、そこまでの合意には達せず、一定の要件の下でコンピュータ・プログラムに付された技術的手段の法的保護を義務づけることに合意したのが、ソフトウェア指令とも言われるコンピュータ・プログラム指令である。[99]

同指令 7 条(c) は次のように定め、コンピュータ・プログラムについてなされた技術的手段について特に保護することを要求している。なお、本指令における「コンピュータ・プログラム」とは、ベルヌ条約に定められた意味で「言語著作物」として保護されるものである旨が同指令の第 1 条 1 項に定められており、著作物性のあるコンピュータ・プログラムが前提とされている。

第 7 条　特別な保護手段[100]
1. 第 4 項、5 項、6 項の規定の効力を損なうことなく、加盟国は、国内法に基づき、下記(a), (b), (c)に列挙された行為を行う者に対し、適切な救済措置を講じるものとする。:
(a)　違法複製されたコンピュータ・プログラムであると知って、又は知るだけの合理的理由

measures to ensure that rightholders make available to the beneficiary of an exception or limitation provided for in national law in accordance with Article 5(2)(a), (2)(c), (2)(d), (2)(e), (3)(a), (3)(b) or (3)(e) the means of benefiting from that exception or limitation, to the extent necessary to benefit from that exception or limitation and where that beneficiary has legal access to the protected work or subject-matter concerned.

98 2009 年は、1991 年の指令のわずかの修正(minor amendments)のためのもので、実質的な内容に変更はない。特にコンピュータ・プログラムに施される技術的手段に関する Article 7 は全く同じ内容である。

99 IVIR Study, at 69-70

100 Article 7 の原文は以下のとおりである。
Article 7 (Special measures of protection)
1. Without prejudice to the provisions of Articles 4, 5 and 6, Member States shall provide, in accordance with their national legislation, appropriate remedies against a person committing any of the acts listed in subparagraphs (a), (b) and (c) below:
(a) any act of putting into circulation a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;
(b) the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy;
(c) any act of putting into circulation, or the possession for commercial purposes of, any means the sole intended purpose of which is to facilitate the unauthorized removal or circumvention of any technical device which may have been applied to protect a computer program.

があって、当該違法複製物を頒布する行為
(b)　違法複製されたコンピュータ・プログラムであると知って、又は知るだけの合理的理由があって、当該違法複製物を営利目的で所持する行為
(c) コンピュータ・プログラムを保護するために付されている技術的手段を許諾なく除去又は回避することを促すことを唯一の目的とする手段を頒布するか、又は営利目的で所持する行為
2. コンピュータ・プログラムの違法複製は関係加盟国の国内法に従って差押する責任を負う。

3. 加盟国は、上記 1(c)で言及した手段の差押を提供することができる。

２．３　条件付きアクセス指令（1998 年）[101]

テレビやラジオ放送等、サービス事業者の許諾なくサービスを受信するための装置の製造・販売・貸与・営利目的所持等を規制する指令である。

WIPO 条約に先立つ 1991 年、すでに EU 評議会（the Council of Europe）が条件付のアクセスシステム・装置の法的保護の必要性を訴えていた。同評議会は、暗号化されたテレビサービスの法的保護に関する推奨 [No. R(91)14] （これはその後、視聴覚録音物の不正利用（piracy）への対抗策についての推奨［No. R(95)1]として結実するもの）を各加盟国に対して発行した。その後、1996 年、欧州委員会は、EU 内市場における暗号化されたサービスに関する不正利用(piracy)問題に取り組み､条件付アクセスシステムを用いた有料サービスの保護法制について EU 内での統一（harmonization）の必要を説いた。その結果採択されたのが、条件付アクセスに基づき又は条件付アクセスによって構成されるサービスの法的保護に関する、条件付アクセス指令である｡要するに､有料 TV サービスを不正利用から保護することを主眼とする指令である[102]。

この指令は、コンテンツを配信する際に付される技術的手段の保護と重複するように思われるため、その両者の関係も問題となる。欧州委員会は、条件付アクセス指令は情報社会指令 6 条の技術的手段の保護を補充する規定であると認識し、条件付アクセス指令で保護されるのは条件が付されたサービスであって、それに著作物が含まれるか否かを問わないという点、そしてそれ故に、その保護対象は著作権者ではなくサービスの提供者であるという点が情報社会指令とは異なると考えていた[103]。この点は、後に補足するが（第Ⅳ章 2.1)、例えば、英国では、各指令に対応する国内法の規定が明確に設けられ、それぞれが事案に応じて適用されるものと

[101] Directive 98/84/EC of the European Parliament and of the Council of 20 November 1998 on the legal protection of services based on, or consisting of, conditional access.

[102] Thomas Heide, Access Control and Innovation under the Emerging EU Electronic Commerce Framework, 15 Berkeley Tech. L.J. 993 (2000). Available at: http://scholarship.law.berkeley.edu/btlj/vol15/iss3/3

[103] Id. at 1018

解されている（理論上は重畳適用もあり得る）。
同指令第 2 条は、次のように保護されるサービス等を定義する。

本指令の解釈上、
(a)「保護されるサービス」とは、条件付きアクセスに基づき有料で提供される、以下のサービスをいずれかを意味するものとする。
－指令 89/552/EEC 第 1 条 a で定義されるテレビ放送
－公衆に受信されることを目的とするラジオ番組の、有線または、衛星を含む無線での送信を意味するラジオ放送。
－技術水準と技術規制と情報社会サービスに関する規則の分野の情報提供のための手続を定める 1998 年 6 月 22 日の欧州議会及び評議会の指令 98/34/EC 第 1 条(2)の意味に含まれる情報社会サービスまたは、サービスとしての、上記のサービスに対する条件付きアクセスの提供。
(b)「条件付アクセス」とは、明瞭な形態で保護されるサービスへのアクセスが事前に個々の承認を要件とするための技術的手段及び/又は取り決めを意味するものとする。
(c)「条件付アクセス装置」とは、明瞭な形態で保護されるサービスへのアクセスを可能にするように設計又は調整された装置またはソフトウェアを意味するものとする。
(d)「関連サービス」とは、条件付アクセス装置の設置、保守又は交換、及び、保護されるサービス又はそれらに関係する営業目的のコミュニケーションサービスの提供を意味するものとする。
(e)「違法装置」とは、明瞭な形態で保護されるサービスへの、サービス提供者による許諾がないアクセスを可能とするように設計又は調整された装置またはソフトウェアを意味するものとする。
(f)「この指令によって調整される分野」とは、第 4 条で特定された違法行為に関係する何らかの規定を意味する。

さらに、同 4 条は、違法行為として、次の 3 つの行為を定め、同 5 条は、そうした違法行為に対する適切な法的救済（損害賠償・差止・廃棄）を付与することを義務づける。

加盟国は、その領土内で、以下のすべての活動を禁止するものとする。
(a) 違法装置を営利目的で製造、輸入、頒布、販売、貸与又は所有する行為
(b) 違法装置を営利目的で設置、保守又は交換する行為
(c) 違法装置の広告宣伝のために営利目的の通信を利用する行為

２．４　欧州司法裁判所（Court of Justice European Union, “CJEU”）の判断

２．４．１　欧州司法裁判所の先決裁定

EU 加盟国は、自国において EU の法令・政策を実施する責任を負う。そして、その EU 法を定めるのが欧州議会または欧州理事会である[104]。EU 運営条約 288 条[105]は、その法行為として、規則、指令、決定、勧告、意見を挙げる。この点、「指令」は、「達成されるべき結果について、名宛人である構成国を拘束するが、方式及び手段の選択は構成国の機関に委ねられている」（EU 運営条約 288 条）ものである。

そのため、指令と各加盟国が選択した方式・選択に相違が生じる事態が想定されるところ、そのような場合に、EU 加盟国が EU 法（指令）を遵守しているか否かの判断を行う最終的な権限を有するのが欧州司法裁判所である。

EU 運営法 267 条は[106]、欧州司法裁判所は、①EU 条約及び EU 運営条約の解釈、②EU の諸機関または諸組織の行為の効力及び解釈に関係する先決裁定を下す管轄権を有すると定めている。指令は、EU の諸機関の一つである欧州委員会の行為として、その効力及び解釈が欧州司法裁判所の判断の対象となる。

そのため、EU 指令の内容と各国著作権法との齟齬が生じた場合、EU 加盟国国内裁判所は、自らの判決に先立ち、当該国内法の EU 法の適合性について欧州司法裁判所に判断を求める（付託する）ことができると同時に、その判断（先決判決：preliminary rulings）に EU 各国内裁判所は法的に拘束される（違反に対して欧州委員会は当該国に制裁金を課すことを提案でき、制裁

---

104 EU 運営条約（Treaty of the Functioning of the European Union, TFEU）192 条 1 項:

Article 192 の原文は以下のとおり。

1. The European Parliament and the Council, acting in accordance with the ordinary legislative procedure and after consulting the Economic and Social Committee and the Committee of the Regions, shall decide what action is to be taken by the Union in order to achieve the objectives referred to in Article 191.

105 Article 288 の原文は以下のとおり。

(ex Article 249 TEC)

To exercise the Union's competences, the institutions shall adopt regulations, directives, decisions, recommendations and opinions.

A regulation shall have general application. It shall be binding in its entirety and directly applicable in all Member States.

A directive shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.

A decision shall be binding in its entirety. A decision which specifies those to whom it is addressed shall be binding only on them.

Recommendations and opinions shall have no binding force.

106 中西優美子　「EU 法」（新世社 2012）239 頁以下参照。267 条の訳は同書 242 頁の訳による。

金についても裁判所が判断する)。

前述のとおり技術的手段の法的保護を定めた情報社会指令のほか、関連する指令が存在し、加盟国はそれを国内法化する。各加盟国の国内法の争点が EU 指令の解釈に関連する場合、担当裁判所が欧州司法裁判所に論点を命じて付託するケースが増えている[107]。前述のとおり欧州司法裁判所の判断は EU 法（本報告書の文脈では EU 指令）との適合性の判断であり、他の加盟国の国内裁判所も同様の論点について法的に拘束されることから、CJEU の判断を通じて、EU の法規範が形成される傾向が高まっている。その結果、CJEU が存在する場合、その判決内容は EU 全域に適用される法規範と理解することになる。

２．４・２　技術的手段の法的保護に関する先決判決

技術的手段の法的保護に関する欧州司法裁判所の先決判決が一件存在するので[108]、以下、同事件について紹介する。

（１）事案の概要

任天堂 DS と Wii（ゲームとコンソール）を製造・販売する株式会社任天堂、Nintendo USA 、Nintendo Europe （以下、総称して「任天堂」という。）が、DS や Wii のコンソールに挿入することで、任天堂の正規のゲーム以外を利用可能にする装置をオンライン上で販売した PC Box と PC Box のウェブサイトのホスティングサービス提供事業者に対し、装置の製造・販売の差止の仮処分を求めた事案である。

本件で任天堂は、コンソール（コンソールとはゲームを操作する機器のことである）上に認識システムと著作物たるゲームが組み込まれているハウジングシステム（著作物たるコンピュータ・プログラムが格納されている部分のことである。日本の事例に即していえば、ゲームカートリッジ内を意味する）に暗号化コードを施していた。その結果、ユーザーがコンソール上でゲームを実行するためには、適法に販売されたゲームソフトに付されている暗号コードをゲーム機であるコンソールが認識しなければならないため、ユーザーは違法複製されたゲームソフトをコンソール上で実行することができなかった。任天堂はこのようにして、適法なゲームソフトの流通を確保していた。

被告の PC Box は、任天堂のコンソールと共に任天堂以外の者が制作したソフトウェアを販売していたが、そのソフトウェアを任天堂のコンソール上で利用するためには、任天堂が付した技術的手段を解除する PC Box 機器(mod chip)の事前インストールを必要とするものであった。

---

107 その付託は国内裁判所はどの裁判所も行うことが許される（EU 運営条約 267 条 2 項、同書 247 頁)。

108 ドイツでの任天堂 DS を巡る事件も欧州裁判所に付託されたが（Andreas Grund acting as administrator in the insolvency proceedings concerning the assets of SR-Tronic GmbH, Jurgen Reiser and Dirk Seidler v. Nintendo Co Ltd. and Nintendo of America Inc (C-458/13)、本判決後に、論点（ビデオゲームについては、情報社会指令が適用されるのか、コンピュータプログラム指令が適用されるのか）が同じである旨の回答が CJEU から出され、ドイツ最高裁が回付を撤回している(2014 年 5 月)。

PC Box は、任天堂の真の目的は、コンソール上で任天堂製品以外の MP3 ファイル、映画、ビデオを実行するソフトウェア（違法な複製物ではない）を利用させないことであるとして、そのような任天堂のアクセス制限技術は、情報社会指令 6 条を国内法化したイタリア著作権法 102quator によって保護される「技術的手段」ではないと争った。

この事案はミラノの裁判所（Milano Tribunal）に係属したが、裁判所が国内手続を止め、以下の２点について、欧州司法裁判所へ回付し、判断を仰いだ。

（２）争点（判決文 18 項）

①保護される技術的手段の「対象」

情報社会指令 6 条の定める「法律に規定された著作権又は著作隣接権（関連権）…（略）…の権利者によって許諾されていない著作物その他の権利の対象に関する行為を阻止又は制限することを意図するあらゆる技術、装置又は部品」に対する保護が、同じ者によって製造・販売され、当該著作物が含まれる別の収納媒体上に付された認証コードを認識することができるハードウェア機器（その認証コードを欠けばゲームが作動せず、また、同認証コードを欠くため任天堂以外の付随的な機器又は製品と互換性を有しない機器である）にまで及ぶか。つまり、著作物に直接施されていない技術的手段も、著作物の保護に向けられているということで保護される「技術的手段」と評価され得るか。

②技術的手段を回避・無効化することが許容される基準

技術的手段を回避・無効化することを目的とする製品又は部品の利用が、その他の商業上重要な目的又は利用を上回るものかどうかを検討する必要があると仮定した場合、情報社会指令 6 条に基づき、国内の裁判所がその点を評価する際、著作権者が保護されるコンテンツを含んだ製品に対して特に意図していた利用を重視する基準か、若しくはそれに代えて又は加えて、回避・無効化技術の利用形態を他の利用形態と比較する量的基準ないし、回避・無効化による利用行為それ自体の性質や重要性という質的基準のいずれを採用すべきなのか。

（３） 判決の概要

①争点 1 に対する判断

EU 情報社会指令 6 条(3)に定義される「効果的な技術的手段」は幅広く定義づけられており、アクセス制限技術や、暗号化・スクランブル・著作物の変容・利用制限技術を含むものであること、そして、そのような広い定義は、知的創造物に不可欠な著作者に優位なハイレベルの法的保護を提供するという情報社会指令の目的と合致することから、任天堂の DS や Wii のように一部がゲームプログラムに、一部が分離されたコンソールに技術的手段が施され、その両者で相互にやりとりがなされる形態も、情報社会指令 6 条(3)「効果的な技術的手段」に含まれると判断した（判決文 27 項、28 項）。

②争点２に対する判断

情報社会指令 6 条(2)における「技術的手段」を回避することを禁止する法的範囲を判断する際には比例（proportionality）原則が妥当し、技術手段を回避すること以外に商業上重要な目的と利用態様を持っている装置や活動を禁止することは許されない（判決文 30）。

法的保護が与えられる技術的手段は、著作物に関して、著作権者から許諾されていない行為を阻害又は除去することを目的とする手段に限られ、その目的を達成するのに必要な範囲を超えて保護されない（判決文 31）。

よって、対象となる技術以外の技術が、権利者の保護に相当の保護を図りながら、権利者の許諾を必要としない第三者の行為をより制限しない手段といえるかどうか、さまざまなタイプの技術的手段が権利者の利益保護にどのように効果的かを検証することが必要となる（判決文 32、33）。特に、技術的手段の回避・無効化すること以外に商業上重要な目的又は利用を有する技術的手段か、回避・無効化を可能又は促進することを主として目的とした技術的手段か、を評価することが重要である。その際、装置等の目的を判断するためには、具体的に当該事件と同様の事情の下で、第三者の実際の利用状況に関する証拠が特に必要である（判決 36）。

本件では、PC Box の装置が実際に任天堂の違法複製物を任天堂のコンソール上で利用するために用いられているのか、また、PC Box の装置が任天堂の著作権を侵害しない態様で利用されているのかを特に検証する必要がある（判決文 36、37、38）。

（４）判決の影響 [109]

本判決は、情報社会指令 6 条(3)における「効果的な技術的手段」の範囲について CJEU がその解釈を明らかにした事例である。ゲームプログラムに対する技術的手段と、コンソール側に付された技術的手段という分離した形態のものであっても、「効果的な技術的手段」の範囲に含まれるとした。さらに、保護技術がその目的に照らし必要以上の規制をして、第三者の権利を侵害してはならないことを明らかにし、本件では特に任天堂以外の製品ができず、それらの製品を排除するシステムとなっているかどうかを国内裁判所が検証すべきことを明らかにした[110]。

３　ＴＰＰ協定第 18 章 68 「技術的保護手段」

2015 年 10 月に暫定合意に至った環太平洋経済協力 (Trans Pacific Partnership) 協定（いわゆる TPP）の知的財産条項に「技術的保護手段」の章が設けられた。その内容は、以下のとおりである[111] 。なお、文化庁において TPP 協定に基づく著作権改正案が検討され[112]、2016 年 3 月 8

[109] Petroula Vantsiouri, “A Legislation in Bits and Pieces: The Overlapping Anti-Cercumvention Provisions of the Information Society Directive, the Software Directive and the Conditional Access Directive, and their implementation in the United Kingdom” at 587, [2012] E.I.P.R., Issue 9

[110] 2015 年 11 月 16 日、Milano Tribunal（知的財産部）は、任天堂が採用している技術的手段はその目的に照らして過度に制限的に過ぎるものではないとして、任天堂の用いた技術的手段の法的保護を認め、PC Box の機器の製造・販売の差止を認めた。判決文は公開されておらず、具体的な技術の評価や当事者が提出した証拠等は不明である。任天堂のプレスリリース https://ap.nintendo.com/_pdf/news/283613675.pdf を参照。

[111] 平成 28 年 2 月 2 日時点での仮訳による。http://www.cas.go.jp/jp/tpp/naiyou/tpp_text_kariyaku.html

日、環太平洋パートナーシップ協定の締結に伴う関係法律の整備に関する法律案が閣議決定を経て国会に提出された[113]。提出された法律案は、本書「第ｖ章 2.2」の通り。

1　各締約国は、著作者、実演家及びレコード製作者が自己の権利の行使に関連して用い、並びにその著作物、実演及びレコードについて許諾されていない行為を抑制する効果的な技術的手段に適当な法的保護を与え、及び当該技術的手段の回避に対する効果的かつ法的な救済措置を講ずるため、次のいずれかの行為を行う者が第 18・74 条（民事上及び行政上の手続及び救済措置）に規定する救済措置について責任を負い、及び当該救済措置に従うことを定める。

(a) 保護の対象となる著作物、実演又はレコードの利用を管理する効果的な技術的手段を権限なく回避する行為であって、そのような行為であることを知りながら又は知ることができる合理的な理由を有しながら（注 1）行うもの（注 2）

（注 1）この(a)の規定の適用上、締約国は、申し立てられた不法行為に係る事実及び状況を考慮して、知ることができる合理的な理由を合理的な証拠により立証することができることを定めることができる。

（注 2）いずれの締約国も、保護の対象となる著作物、実演又はレコードの著作権又は関連する権利を構成する排他的権利を保護する効果的な技術的手段であって、当該著作物、実演又はレコードの利用を管理するものでないものを回避する者について、この規定に基づき民事上の責任を負わせ、又は刑事上の責任を課することを要求されない。

(b) 次の要件を満たす装置、製品若しくは部品を製造し、輸入し、若しくは頒布し、若しくは公衆にこれらの販売若しくは貸与を申し出、若しくは他の方法によりこれらを提供する行為又は次の要件を満たすサービスの提供を公衆に申し出、若しくは当該サービスを提供する行為

（注）締約国は、製造、輸入及び頒布についてこの(b)に定める義務が、それらの行為が販売若しくは貸与のために行われる場合又は著作権若しくは関連する権利を保有する者の利益を害する場合にのみ、適用されることを定めることができる。

(i) 効果的な技術的手段を回避することを目的として、この(b)に規定する行為を行う者が販売を促進し、宣伝し、又は販売すること。

（注）締約国は、この(i)の規定が、この(b)に規定する行為を行う者が第三者のサービスを通じて販売を促進し、宣伝し、又は販売する場合についても適用されることを了解する。

(ii) 効果的な技術的手段を回避すること以外の商業上意味のある目的又は用途が限られてい

112　上野達弘「TPP 協定と著作権法」（ジュリスト 1488 号、61 頁以下）

113　内閣官房 WEB ページ『環太平洋パートナーシップ協定の締結に伴う関係法律の整備に関する法律案』（http://www.cas.go.jp/jp/houan/160308/siryou3.pdf）

ること
（注） 締約国は、この(b)に規定する行為が効果的な技術的手段を回避すること以外の商業上意味のある目的又は用途を有しない場合には、この 1 の規定を遵守することができる。
(iii) 効果的な技術的手段を回避するために主として設計され、生産され、又は提供されていること。

各締約国は、いずれかの者が故意に及び商業上の利益又は金銭上の利得のために(a)及び(b)に掲げるいずれかの行為に従事したことが判明した場合について適用する刑事上の手続及び刑罰を定める。
（注 1）この条及び次条（権利管理情報）の規定の適用上、故意には、認識の要素が含まれる。
（注 2）締約国は、一の締約国が、この条、次条（権利管理情報）及び第 18・77 条（刑事上の手続及び刑罰）1 の規定の適用上、「金銭上の利得」を「商業上の目的」として取り扱うことができることを了解する。
（注 3）いずれの締約国も、自国又は自国の許可若しくは同意を得て行動する第三者による行為について、この条及び次条（権利管理情報）の規定に基づく責任を負わせることを要求されない。締約国は、当該刑事上の手続及び刑罰が非営利の図書館、博物館、記録保管所若しくは教育機関又は公共の非商業的な放送機関については適用されないことを定めることができる。また、締約国は、これらの機関のいずれについても、(a)及び(b)に掲げる行為が禁じられていることを知らずに善意で当該行為を行う場合には、第 18・74 条（民事上及び行政上の手続及び救済措置）に規定する救済措置が適用されないことを定めることができる。

2 いずれの締約国も、1 の規定を実施するに当たり、家庭用電化製品、電気通信機器若しくはコンピュータ製品の設計又はこれらの製品の部品及び構成品の設計及び選択が特定の技術的手段に対応することを要求することを義務付けられない。ただし、これらの製品が 1 の規定を実施する措置に違反しない場合に限る。

3 各締約国は、この条の規定を実施する措置の違反が、著作権及び関連する権利に関する自国の法令に基づいて起こり得る侵害から独立していることを定める。
（注）締約国は、1(a)に規定する回避についての犯罪行為について他の方法により刑事上の処罰を行う場合には、当該犯罪行為を独立した違法行為として取り扱うことを要求されない。
4 1 の規定を実施する措置に関し、
(a) 締約国は、知的財産権を侵害しない供用を可能とするため、1(a)及び(b)の規定を実施する措置が当該知的財産権を侵害しない供用について現実に悪影響を及ぼす場合又は悪影響を及ぼす可能性がある場合には、自国の法令に基づく立法上、規制上又は行政上の手続によって、及び当該手続によって証拠が提出されるときは当該証拠に十分な考慮（当該締約国の法令に

基づく著作権及び関連する権利の制限及び例外を受益者が享受することができるようにするために権利者がとった措置が適当かつ効果的であるかどうかに関するものを含む。）を払いつつ、当該措置の制限及び例外を定めることができる。

（注）この(a)の規定は、締約国に対し、次のいずれかの要件を満たす効果的な技術的手段の法的保護の制限及び例外について、この(a)規定する立法上、規制上又は行政上の手続を通じて新たな決定を行うことを要求するものではない。ただし、当該制限(a)及び例外がその他の点においてこの 4 の規定に適合していることを条件とする。

(i) 二以上の締約国間で効力を有する貿易協定に従って既に定められたものであること。

(ii) 締約国が既に実施していること。

(b) 1(b)の規定を実施する措置の制限又は例外は、意図された受益者がこの条の規定に基づいて許容される制限又は例外を正当に利用することができるようにするためにのみ許される。当該措置の制限又は例外は、当該意図された受益者を超えて装置、製品、部品又はサービスを利用可能なものとすることを許可するものではない。

（注 1）締約国は、1(b)の規定に対する例外に対応する 1(a)の規定に対する例外を定めることなく、当該 1(b)の規定に対する例外を定めることができる。ただし、当該 1(b)の規定に対する例外が、この(b)の規定に基づく 1(a)の規定に対する制限又は例外の範囲内における正当な利用を可能とするものに限定されることを条件とする。

（注 2）1(a)の規定は、この(b)の規定の解釈のためにのみ、5 に定義する全ての効果的な技術的手段について準用されるものと解釈されるべきである。

締約国は、この章の規定に従い、(a)及び(b)の規定に基づく制限及び例外を定めることにより、著作者、実演家若しくはレコード製作者が自己の権利の行使に関連して用い、又はその著作物、実演若しくはレコードについて許諾されていない行為を抑制する効果的な技術的手段を保護するための自国の法制の妥当性又はこのような効果的な技術的手段の回避に対する法的な救済措置の効果を損なわせてはならない。

5「効果的な技術的手段」とは、効果的な技術、装置又は構成品であって、その通常の機能において、保護の対象となる著作物、実演若しくはレコードの利用を管理するもの又は著作物、実演若しくはレコードに関連する著作権若しくは関連する権利を保護するものをいう。

（注）通常の場合において、偶発的に回避される技術的手段は、「効果的な」技術的手段ではない。

第Ⅵ章　諸外国の法制度等

１　アメリカ

米国では、1992 年のオーディオ家庭内録音法に、著作物のコピー制御装置の回避を目的とする輸入・製造・頒布の禁止という限定的な形で技術的手段の保護に乗り出した。その後、広汎な技術的手段の保護が国内でも議論されたことを背景に、WIPO において米国自らが強力な技術的手段の保護を提案し、WIPO 条約において技術的手段の保護を明記することに貢献した。そして、WIPO 条約の合意内容を国内法に履行したのが、デジタルミレニアム著作権法 1201 条の定めである。明文規定上は、1201 条(a)(1)がアクセス制限技術の回避を禁止し（日本における不正競争防止法の規制及び平成 24 年著作権法の改正により含まれた暗号型の技術的手段の規制に概ね対応する）、同条(b)(1)が利用制限技術の回避を禁止する（日本における不正競争防止法及び著作権法上の平成 24 年改正前からの技術的手段の規制に概ね対応する）ものと読むのが自然（後述 1.2（23）の MDY 事件の裁判例がこの立場）だと思われるが、下級審裁判例の中には、1201 条(a)(1)で保護されるアクセス制限技術の要件として、著作権侵害の回避との関連性を求め、純粋に著作物へのアクセスのみの規制する技術を保護の対象外とするものもあり（後述 1.2（8）の Chamberlain 事件の裁判例など）、連邦最高裁の解釈が示されていないため、その解釈はいまだ一定していない。

なお、米国では、1201 条が広く技術的手段の回避の禁止を原則とする一方、3 年に一度、技術的手段の回避を法的に許容する例外を議会図書館が著作権局の推奨に基づき定めることになっており（1201 条(a)(1)(C), (D)）、欧州とは異なり、この手続きが活発に利用されている点に特徴がある。

１．１　法制度

（１）現行法

①1992 年オーディオ家庭内録音法

1992 年オーディオ家庭内録音法（Audio Home Recording Rights Act of 1992,「AHRA」）は、米国において著作物のコピー制御装置の回避を目的とする装置の輸入・製造・頒布の禁止をはじめて規定した。

1002 条(a)項は、「連続コピー制御システム、連続コピー制御システムと同一の機能を有するもの、商務長官が無断の連続コピーを禁止されたシステムであると証明するものに適合しないデジタル音声記録装置またはデジタル音声インターフェイス装置」の、「輸入、製造、頒布」を禁止した。また、同上(c)項は、(a)項に定めるシステムの回避を禁じた。

条文は以下の通りである。

第 1002 条　コピー制御装置の組み込み

(a) 輸入、製造および頒布の禁止－何人も、以下に適合しないデジタル音声録音装置またはデジタル音声インターフェイス装置を輸入し、製造しまたは頒布してはならない。

(1) 連続コピー制御システム。

(2) 連続コピー制御システムと同一の機能的特徴を有し、かつ、当該方式の連続コピー制御を供用する装置と連続コピー制御システムを供用する装置との間で、著作権および世代の状況に関する情報を正確に送信し、受信しかつ作用することを要するもの。

(3) その他、商務長官が無断の連続コピーを禁止されたシステムであると証明するもの。

(b) 認証手続の設定－商務長官は、利害関係者の申立によりシステムが第(a)項(2)に定める基準に合致することを認証する手続を設定しなければならない。

(c) システム回避の禁止－何人も、第(a)項に定めるシステムの全部または一部を実行するプログラムまたは回路を忌避し、迂回し、除去し、無効にしその他回避することを主たる目的または主たる効果とする装置を輸入し、製造しまたは頒布し、またはかかる目的または効果を有するサービスを提供しもしくはその提供申出を行ってはならない。

(d) デジタル音楽録音物における情報の暗号化－

(1) 不正確な情報の暗号化の禁止－何人も、録音物の原典の分類コード、著作権状況または世代状況に関連する不正確な情報を含む録音物のデジタル音楽録音物を暗号化してはならない。

(2) 著作権状況の暗号化不要－本章のいかなる規定も、デジタル音楽録音物の輸入または製造に従事する者に対し、著作権状況についてデジタル音楽録音物を暗号化することを要求するものではない。

(e) デジタル方式の送信に伴う情報－録音物をデジタル方式にて公に送信しその他伝達する者は、本章において録音物の著作権状況に関連する情報を送信しその他伝達することを要求されない。上記の者で上記著作権状況にかかる情報を送信しその他伝達する者は、上記の情報を正確に送信しまたは伝達しなければならない。

以上のとおり、AHRA は、はじめて「回避」という用語を用いて規制した連邦法であり、次に紹介するデジタルミレニアム著作権法の技術的手段回避の立法過程で上院・下院のいずれのレポートにおいても回避禁止措置の先例として引用されている。

ただし、SCMS という特定の技術に対応する法律であるため、柔軟性と範囲に限界がある。また、利用者自身の回避については何も規制していない[114]。

[114] June M. Besek, Anti-Circumvention Laws and Copyright: A Report from the Kernochan Center for Law, Media and the Arts 27 Columb. J.L. & Arts 385, 437

②デジタルミレニアム著作権法

1998 年、WIPO 著作権条約を受けて、米国商法典に第 17 章を追加し、技術的手段の保護を定める 1201 条を追加した（デジタルミレニアム著作権法)。その特徴は、WIPO 条約上は明確には要求されていない（前述のとおり、主にアフリカ諸国からの強い反対により明示的には含まれなかった）アクセス制限技術についても、コピー等利用制限技術とともに保護対象に含めている点である。

すなわち、1201 条は、(a)著作物に対する不正アクセスを制御する技術的手段と(b)著作権によって与えられる権利の不正な行為（違法複製など）を制御する技術的手段を区別して規定している。そして、1203 条と 1204 条において、1201 条違反の場合の民事上の救済と刑事罰を定めている。

第 1201 条　著作権保護システムの回避

(a)　技術的手段の回避にかかる違反－

(1) (A) 何人も、本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避してはならない。第 1 文に掲げる禁止は、本章の制定日から 2 年間の終了時に発効する。

(B) 著作権のある特定の種類の著作物の供用者が、本編に基づき第(C)号に定める特定の種類の著作物を権利侵害なく供用するにつき第(A)号に含まれる禁止により不利益を受け、または続く 3 年間に不利益を受ける可能性がある場合、当該禁止は当該供用者には適用されない。

(C) 第(A)号に掲げる 2 年間および続く 3 年間毎に、連邦議会図書館長は、著作権局長が商務省通信情報担当長官補と協議しその見解について報告説明した上で行う勧告に基づき、第(B)号に関して、続く 3 年間に、本編に基づき著作権で保護された特定の種類の著作物を権利侵害なく供用するにつき第(A)号に基づく禁止により不利益を受けまたは受ける可能性がある供用者であるか否かを、規則制定手続において決定しなければならない。当該規則制定手続にあたり、連邦議会図書館長は以下を審査しなければならない。

(i)　著作権のある著作物の利用可能性。

(ii)　非営利的な資料保管、保存および教育目的での著作物の利用可能性。

(iii)　著作権のある著作物に供用される技術的手段の回避に対する禁止が、批判、解説、ニュース報道、学習指導、学術または研究に及ぼす影響。

(iv)　技術的手段の回避が著作権のある著作物の市場または価値に及ぼす効果。

(v)　連邦議会図書館長が適切と考えるその他の要素。

(D) 連邦議会図書館長は、著作権のある著作物の種類のうち、連邦議会図書館長が第(C)号に基づき行う規則制定手続において、著作権のある著作物の供用者が侵害なくこれを利用するにつき不利益を受けまたは受ける可能性があり、第

(A)号に含まれる禁止が当該供用者に対して当該種類の著作物については続く3年間は適用されるべきでないと決定したものを、公表しなければならない。

(E) 第(A)号に含まれる禁止の適用に関する第(B)号に基づく例外および第(C)号に基づき行われる規則制定手続においてなされた判断は、本節を除く本編の規定を行使する訴訟において抗弁とすることができない。

(2) 何人も、以下のいずれかに該当するいかなる技術、製品、サービス、装置、部品またはそれらの一部分を製造し、輸入し、公衆に提供し、供給しまたはその他流通させてはならない。

(A) 主として、本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避することを目的として設計されまたは製造されるもの。

(B) 本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避する以外には、商業的に限られた目的または用法しか有しないもの。

(C) 本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避するために供用することを知っている者またはこれに協力する者によって販売されるもの。

(b) 補足的違反行為－

(1) 何人も、以下のいずれかに該当するいかなる技術、製品、サービス、装置、部品またはそれらの一部を製造し、輸入し、公衆に提供し、供給しまたはその他流通させてはならない。

(A) 主として、著作物またはその一部分に対する本編に基づく著作権者の権利を効果的に保護する技術的手段により施される保護を回避することを目的として設計されまたは製造されるもの。

(B) 著作物またはその一部に対する本編に基づく著作権者の権利を効果的に保護する技術的手段により施される保護を回避する以外には、商業的に限られた目的または用法しか有しないもの。

(C) 著作物またはその一部に対する本編に基づく著作権者の権利を効果的に保護する技術的手段により施される保護を回避するために供用することを知っている者またはこれに協力する者によって販売されるもの。

（２）回避行為

1201(a)(1)は、「何人も、本編に基づき保護される著作物へのアクセスを効果的にコントロールする技術的手段を回避してはならない。第 1 文に掲げる禁止は、本章の制定日から 2 年間の終了時に発効する」と定め、個人・法人等の主体や営利・非営利等の目的を問わず、アクセス制限技術を回避することを禁止している。他方、1201(b)では 1201(a)(1)に対応する条文がなく、回避そのものは規制していない。

（３）回避装置等の取引行為

1201 条(a)(2)と同条(b)(1)が同様の内容を定めており、一定の条件を満たす回避装置等を製造、輸入、公衆に提供し、供給しまたはその他流通させてはならない」と広範に規制している。

（４）制限・例外

- 1201(d)：非営利目的の図書館、博物館又は教育機関がある作品を入手するかどうかを判断するためだけに、アクセス制限技術を回避することを認める。
- 1201(e)：特定の法執行行為について回避禁止の例外を認める。
- 1201(f)：リバースエンジニアリングの目的でのアクセス制限技術・コピー等利用制限技術の回避禁止の例外を認める。
- 1201(g)と(h)：暗号化とセュリティテストのためのアクセス制限技術回避禁止の例外

１．２　主要判例（事案の概要・争点・裁判所の判断）[115]

1201 条をめぐる主な裁判例を概観する。

（１）　Real Networks, Inc. v. Streambox, Inc.[116]

Real Networks は、「secret handshake」という RealPlayer のファイルの認証装置と「copy switch」という提供する音楽･映像コンテンツをダウンロードされることを防止するセキュリティ装置（ユーザーのコンピュータからデータが消去される）を施し、RealMedia フォーマットで音楽・映像のストリーミングサービスを提供していた。Streambox は、secret handshake の疑似認証手続を踏んだ後、copy switch を無視し、ユーザーの手元でコンテンツのダウンロードを可能にする装置（VCR）と RealMedia から別のフォーマットにファイル変換を行う装置（Ripper)等[117]を製造・販売していたため、Real Networks が、1201 条(b)違反などを根拠に差止請求をした事案。

裁判所は、(i)secret handshake の疑似認証手続を踏んだ後、copyswitch を無視（無効化）し、

115　山本隆司「コンテンツ・セキュリティと法」（商事法務・2015）164 頁以下は、参考になる裁判例を網羅的に検討している。同書で言及されている裁判例に基本的に準拠している。

116　2000 U.S. Dist. LEXIS 1889 (W.D. Wash. 2000)

117　デフォルトになっている RealMedia の検索エンジンを StreamBox の検索エンジンに変更する装置（Ferret）の提供について、検索インターフェイスに対する著作権侵害に対する寄与侵害も主張され、認められている。

ユーザーの手元でコンテンツのダウンロード（複製）を可能にすることを、1201(b)違反と認めた。

（２） Universal City Studios, Inc. v. Corley[118]

本件は、ノルウェーの青年 Jon Johansen が開発した DeCSS という CSS（Content Scramble System：DVD に収めるコンテンツを暗号化し、コンテンツを視聴するためにはその暗号を解除するキーを必要とする技術であり、DVD Copy Control Association がそのキーをライセンスしている。）を解除するプログラムを開発した。1999 年、被告の Eric Corley は、DeCSS のソースコードとオブジェクトコードを運営するウェブサイトに掲載し、ダウンロード可能な状態に置くとともに、DeCSS を入手できる他のリンク先の情報を表示した。Eric 自身は開発者ではなく、また、自ら暗号化を解除して回避したものではないが、Universal City Studios, Inc.が回避装置の取引を禁止する 1201(a)(2)に違反するとして、仮差止めを求めた事案である。
裁判所は、DeCSS がアクセス制限技術を回避する装置であることは明白であるとして、ソースコード等の掲載を差し止めるとともに、それが入手できるウェブサイトへのリンクの掲載についても差止めを認めた。

なお、被告は、DeCSS は本来 DVD プレイヤーの Linux との互換性を達成することを目的としたもので、不正利用目的でないことを強調したが、裁判所は、「Linux DVD プレイヤーの開発が DeCSS の開発の動機であったかどうかは、被告が…DMCA 上の回避装置取引の禁止に違反したかどうかの問いにとって重要なことではない。」と指摘した。被告は、DVD に CSS を搭載することで合法利用を阻害するリスクも指摘したが、裁判所は、議会はそうしたリスクも検討したうえで、装置の回避を上回る利益と判断し、立法したものだとした[119]。

（３） United States v. Elcom Ltd.[120]

被告の Elcomsoft は、Adobe Acrobat e-Book Reader の電子書籍に出版社が施した技術的手段を回避し、電子書籍から PDF へ転換する e-Book Processor を製造・販売したため、1201(a)、(b)に違反するものとして、刑事責任を追及された事案である。被告は、DMCA の規定が明確性の原則に反するとして憲法違反を主張したが、裁判所はその主張をすべて排斥した。ただし、陪審は、故意とは言えないとして、被告人に対して無罪評決をした。

---

118 273 F.3d 429 (2d Cir. 2001)

119 裁判所はそのような弊害も理解しつつ、議会が、法律上の例外規定と３年に一度の例外に関する認証手続によってアクセスコントロールと利用のバランスをとったと評価し、フェアユースとして回避が許容されるとの被告の主張を退けている。

120 203 F. Supp.2d 1111 (N.D. Cal. 2002)

（４） Pearl Investments, LLC v. Standard I/O, Inc.[121]

Pearl Investments, LLC（「Pearl」）は、自動株式取引システム（ATS）を開発するためのソフトウェア開発業務を Standard I/O, Inc（「Standard」）に委託した。ATS 開発完了後、Standard の開発担当者の一人である Chunn（人物）は自分自身の実験的自動取引システムを開発し、Pearl の ATS システムと同じサービスプロバイダーによって管理されるサーバ上に置いていた。Pearl のシステムは、特別なアクセス制限を施した VPN を施していたが、サービスプロバイダーのミスで、Pearl の ATS のルーターに Chunn のシステムをプラグインさせてしまった。そのため、Chunn は、Pearl のパスワードで守られた VPN を回避して、ATS システムのアクセスを得た。Pearl は Standard と Chunn に対して、1201(a)(1)(A)違反として訴訟を提起した。

裁判所は、Standard については、Chunn の行為は Standard の従業員としての行為ではないとして責任を認めず、事実審理省略判決をした。他方、Chunn については、Chunn の事実審理省略判決申立てを却下した。裁判所は、Pearl の VPN は「鍵付のドアの電子版」であるとして、法律上のアクセス制限技術であると認めた。また、Chunn は、自ら開発したもので、バックアップコピーも有しているから、Chunn に対しては「効果的な技術的手段」とはいえないとも指摘したが、裁判所は、通常の操作において有効か否かを判断すれば足りるとして、その主張を排斥した。VPN へのトンネルを構成したのがサービスプロバイダーの従業員だけなのか、Chunn の行為もあるのかという事実に争いがあるとした。陪審は、その後、Chunn に有利な判断をした。

（５）321 Studios v. Metro-Goldwyn-Mayer Studios, Inc.[122]

DVD Copy Plus という、DeCSS を用いて暗号を解除し、DVD の複製を可能にするソフトウェアを製造・販売していた。321 Studios は自身の販売するソフトウェアが 1201 条に違反するものではないことの確認判決を求めたが、裁判所はその請求を斥け、321 Studios のソフトウェア取引が 1201 条に違反するものであるとした。

1201(a)(2)について、321 Studios は、DVD の購入者は著作権者から CSS を迂回して DVD をプレイすることについて許諾を得ているから、真正に購入した DVD 上でのみ動作する本件ソフトウェアは 1201 に違反しないと主張した。しかし、裁判所は、DVD の購入によって CSS を解除することが許諾されるのではなく、むしろ、当該 DVD でコンテンツを視聴することが認められるに過ぎないと判断した。

他方、1201(b)(1)について、321 Studios は、CSS は、コンテンツの複製をコントロールも阻害もしないからコピー等利用制限技術ではないと主張したが、裁判所は、技術上は 321 Studios の指摘は正しいが、暗号化が解除された DVD はアクセスされない限り複製できないので、なお、コピー等利用制限技術であるとした。さらに、321 Studios は、DVD Copy Plus の主たる目的は、CSS へのアクセスに関係しない、又はパブリックドメインにある著作物の複製やフェ

[121] 257 F. Supp.2d 326 (D. Me. 2003)
[122] 307 F. Supp.2d 1085 (N.D. Cal. 2004)

アユースに基づく複製に関係したりするなど様々な目的に利用することであるとも主張したが、裁判所は、ユーザーによる実際の合法的な利用は、ソフトウェアの開発者の 1201(b)(1)違反に対する抗弁にはならない、と判断した。

321 Studios は、1201(a)(2)、(b)(1)の双方について、DVD Copy Plus の機能は DVD の複製がその基本であって、CSS の解除はその一部にすぎない。よって、技術的手段を回避するために設計・制作された装置ではないと反論したが、裁判所は、321 Studios のソフトウェアの一部は、CSS の回避のみを目的とするものであることは争いがないとし、DMCA に違反すると判断した。

（６） I.M.S. Inquiry Management Systems, Ltd. v. Berkshire Information Systems, Inc.[123]

原告は、ウェブ上でクライアントに対して、クライアントの広告追跡情報を提供するサービスを行っており、クライアントは、パスワードによって、当該情報へアクセスすることができる。被告は、第三者に発行されたユーザーID とパスワードを得て、それによって、原告のウェブサイトにアクセスし、レポートの約 85 パーセントを複製し、自社サービスに利用した。裁判所は、被告が回避したのは技術的手段ではなく、原告による技術的手段を通じることについて許諾を得なかったことであり、技術的手段を浸食していないとして、DMCA 違反を認めなかった。

（７）Comcast of Illinois X, LLC v. Hightech Electronics, Inc.[124]

被告 Hightech は、違法通信ケーブル装置を販売する 30 を超えるウェブサイトへのリンクを含んだウェブサイト（1-satellite-dish.com）を運営していた。Comcast は、被告と被告のドメインネームサーバー管理者（Net Results）に対して、1201(a)(2)、(b)(1)違反の主張を行った。

裁判所は、プログラムにスクランブルをかけることによりアクセス制限技術を行っており、それにより著作権者の利益を保護しているとして、DMCA 違反を認めた。(2)事件と同様、回避装置を販売している他のウェブサイトへのリンクも違反の対象とした。

（８） Chamberlain Group, Inc. v. Skylink Technologies, Inc.[125]

原告 Chamberlain は、ガレージドアの開閉システム（Garage Door Opener、「GDO」）の製造業者である。GDO システムは、泥棒対策のローリングコードとコード受信機で構成される。コード化されたラジオ波（radio frequency）信号を送信装置から GDO に送信し、ドアを開閉する。しかし、この信号がキャッチされ、その後、泥棒がドアを開閉するために利用する危険がある。そこで、Chamberlain 製品のローリングコードは、GDO が動作する度に変更され、その危険を回避している。Chamberlain 製品のこの機能は、ローリングコードの送信装置と受信装

123 307 F. Supp.2d 521 (S.D. N.Y. 2004)
124 2004 WL 1718522 (N.D. Ill. 2004)
125 381 F.3d 1178 (Fed Cir. 2004)

置それぞれに含まれているコンピュータ・プログラムによって実現されていた。

これに対し、被告 Skylink Technologies は、Chamberlain 製の GDO を開閉することができる汎用性のある送信装置を製造・販売した。被告製品から Chamberlain 製の GDO に送信されるものはローリングコードではなかったが、被告のドア開閉機は Chamberlain 製のローリングコードを回避していた。Skylink Technologies の装置が、Chamberlain の施した技術的手段を回避する装置の製造・販売となり、1201(a)(2)に違反するとして、Chamberlain が訴訟を提起した。連邦巡回控訴裁判所は、作品へのアクセスを得るためのあらゆる形態の回避に対し 1201 条(a)が適用されるものではなく、「著作権法が著作権者に付与した保護と合理的な関係のある形態のアクセスを実現する回避にのみ適用される」ことを明らかにした。つまり、「著作権侵害を促進する形の回避装置の製造・販売者でなければ、1201 条の責任を負わない」とした。

連邦巡回控訴裁判所がこのように判断したのは、大きく次の３つの理由に基づくものである。第一に、1201 条の文言は、アクセスが常に「保護」と結びついていること、第二に、判例法上、常に著作権法上保護された権利とアクセスが関連性を有していること、第三に、Chamberlain が主張のようにアクセスを広義に解釈し、あらゆるアクセスを保護すると、競争に対して潜在的な害悪を与えることである。

同裁判所は、上記の立場から、1201(a)(2)違反を主張するための要件を①有効な著作権の存在、②効果的な技術的手段が回避されている事実、③第三者が現在アクセスできる事実、④権利者から許諾がないこと、⑤著作権法によって保護されている権利を侵害する又は侵害を促進する態様であること、⑥被告の製品が(i)回避することを主に目的として設計又は制作されていること、(ii) 回避以外に商業上の価値が限られているにも関わらず市場にあること又は (iii) コントロールするための技術的手段の回避に用いるために販売されていること、とした上で、本件では④と⑤の要件を欠くとした。特に要件⑤について、Chamberlain が回避による著作権侵害の主張もどのように被告製品が Chamberlain の有する著作権を侵害するかを説明していないと断じた。事実、被告の送信装置は、ユーザーが GDO のプログラムを利用できるようにするだけで著作権を侵害する行為に結びつくものではなかった。

なお、④について、Chamberlain は、GDO の販売時に、ユーザーは Chamberlain が許諾する以外の送信装置を供用してはならないという制限を付していないと認定し、契約によって明示的に禁じていないとした。

本件は、1201 条(a)(2)が著作権侵害と合理的な関係を有するアクセス制限技術に限り保護することを明らかにしたことで非常に重要な判例である。

（９） Lexmark International, Inc. v. Static Control Components, Inc.[126]

Lexmark は、2 種類のレーザープリンター用トナーカートリッジを販売していた。「レギュラーカートリッジ」は、第三者の製品により再充填をすることができるタイプで、「プリベー

[126] 387 F.3d 522 (6th Cir. 2004)

ト（prebate)カートリッジ」の供用後は、Lexmark に対して変換されることがライセンスで合意されていた。Lexmark のレーザープリンターは 2 種類のコンピュータ・プログラム（Printer Engine Program は、用紙の動き等をコントロールするプログラム、Toner Loading Program は、トナーカートリッジに付着するマイクロチップの中にあり、Lexmark プリンターがカートリッジの残量をおおよそ把握することを可能にしていた）を含んでいた。Lexmark はこれを保護するため、認証シークエンス（Sequence)を利用し、カートリッジがプリンター上で動作するために、カートリッジのマイクロチップで計算される Message Authentication Code (MAC)がプリンター側に送信され、プリンター側で計算される MAC と一致することが要求される。一致すれば、Printer Engine Program がプリントを実行させ、Toner Loading Program が正規品のカートリッジの残量をモニターする。

被告 Static Control は、「SMARTEK」という Lexmark のトナーカートリッジ内のマイクロチップと互換性を有するマイクロチップを販売していた。SMARTEK は、Toner Loading Program のデッドコピーを含み、Lexmark の認証シークエンスを回避することを可能にしていたため、Lexmark 正規品でないカートリッジではないにもかかわらず、Lexmark のレーザープリンターで利用することができた。そのため、Lexmark が DMCA 違反と著作権侵害でその販売仮差止めを求めた事案である。

原審は、1201(a)(2)違反の主張を認容した。原審は、SMARTEK マイクロチップは、著作物に対するアクセスを有効にコントロールする技術的手段を回避することを主たる目的とするものであると判断した。裁判所は、「アクセス」の意義を辞書的な意味合いの「入る」、「取得する」、「利用する」ことであると解釈した。そのため、本件では、認証シークエンスが、Lexmark の著作物である Toner Loading Program と Printer Engine Program に対する有効なアクセス制限技術であると判断し、それを回避する SMARTEK チップの製造・頒布・販売を 1201(a)(2)違反とした。

また、Static Control は、互換性を達成するためのアクセス制限技術の回避であり、独立して創作されたプログラムとの互換性を達成することを目的としたリバースエンジニアリングのための回避を例外と定める 1201(f)が適用されると主張したが、前述のとおり、SMARTEK チップが Toner Loading Program のデッドコピーが含まれており、独立して創作されたプログラムとは言えないことや、SMARTEK の目的は Lexmark の認証目次列によるコントロール回避のみであるとして、その主張を退けた。

これに対し、第 6 巡回控訴裁判所は、地裁の判断を取消し、差し戻した。控訴審は、Lexmark の認証シークエンスは、プリンターのメモリーから誰でも Printer Engine Program の文字コードを見ることができるから、1201 条の適用が認められるほどには Printer Engine Program に対するアクセスをコントロールしていないと判断した。プリンターを作動させないという形で同プログラムへの一つのアクセスをコントロールしているが、同プログラムの複製または文字コードの利用に対するアクセスはコントロールしていない、とした。

さらに、Toner Loading Program に関しては、被告のチップは、同プログラムへの「アクセス」

を提供するものではなく（だからアクセス制限技術の回避にはならない）、Toner Loading Program の置き換えを行うものであるとし、さらに、DMCA の規定が適用される「著作権法上保護される作品」にも該当しないとした。

なお、原審が、互換性の抗弁（1201(f)）の適用を認めなかったことに対し、Toner Loading Program が複製されていることだけで独立プログラムが創作されていないとは言えないとして、互換性の抗弁を認める余地を残した。

（１０） DirecTV, Inc. v. Borow, 2005 WL 43261, 17 ILR (P&F) 304 (N.D. Ill. 2005)

被告の Randy Borow が、視聴料の支払いをせずに DirecTV のプログラムを見るために、エミュレーターを用いて、必要とされるアクセスカードを供用せず、DirecTV の暗号化されたシグナルを回避したことについて、1201(a)(1)違反を認めた。

（１１） Davidson & Associates v. Internet Gateway[127]

Davidson & Associates は Blizzard Entertainment（「Blizzard」）としてビジネスを行っており、いつくかのコンピュータゲームについて著作権を有していた。Blizzard は、複数のプレイヤーがオンライン（Battle.net）で戦うことができ、対戦記録を残すこともできる仕様になっていた。Battle.net にログオンするためには、認証シークエンス（ゲームのパッケージに記載されている）である CD キーが必要であった。当該キーを Battle.net へ送ると、その有効性と他に同じキーでゲームをするものがいないか確認され、ゲームが利用されていなければ、ゲームを開始することができる仕様になっており、違法複製されたゲームでは Battle.net に参加できないようになっていた。被告は、bnetd server として知られるサーバを開発した。同サーバは、Battle.net サービスをエミュレートし、bnetd server 上で Blizzard のゲームの対戦ができるように作られたものである。被告は、このサーバの開発の際、プロトコルを知るため Blizzard のゲームをリバースエンジニアリングし、コンピュータファイルに含まれている Battle.net のインターネットアドレスを変更し、bnetd server に接続されるようファイルの修正を施した。そして、Blizzard ゲームの CD キーを bnetd server が受領しても、bnetd server はその有効性や他の者によって現在利用されているかを確認しない。その結果、被告 bnetd server のサーバ上では、違法複製物ゲームでも対戦に参加することができるものであった。

Blizzard は、被告に対し、①リバースエンジニアリングし、Battle.net へのアクセスを得る際に技術的手段（CD キー）を回避した点について 1201(a)(1)(A)違反を主張し、②bnetd ソフトウェアの製造・販売について、CD キーを回避することを唯一の目的とするものだとして、1201(a)(2)違反を主張した。

①について、被告は、リバースエンジニアリングとして例外的に許容されるとの抗弁を主張

[127] 334 F.Supp. 2d 1164, 1168 (E.D. Mo. 2004).

した（1201(f)(1)）[128]。すなわち、本件で被告は、適法に Blizzard のソフトウェアを購入し、Battle.net にアクセスしており、その目的は互換性の達成であると主張した。

この点、地方裁判所は、被告が独自にプログラムを創作しておらず、被告の行為は、著作権侵害の領域に踏み入るものだとし、さらに、被告のサーバが CD キーの有効性を確認せず、違法複製物によるゲームの利用を可能にしてしまう点をとらえ、互換性の達成以上のことを可能にならしめているとして、リバースエンジニアリングの抗弁を認めなかった。

②について、被告は 1201(f)(2)(3)の抗弁を主張したが、裁判所は被告の目的は互換性の達成に限られるものではなく、むしろ、Battle.net に対するアクセス制限を回避することにあるとして、「互換性を達成するために」という要件を満たさないと判断した[129]。

（１２）Storage Technology Corp. v. Custom Hardware Engineering & Consulting, Inc.[130]

Storage Technology は、大量のコンピュータデータを保存・検索するためのシステムを販売していた。そして、その付随サービスとして、システムの不具合・問題個所の特定のための診断ソフトウェア（Maintenance Code）を提供していた。Storage Technology は、そのサービス市場を守る目的から、Maintenance Code へのアクセスを GetKey というコードで制限していた。あるシステムに Maintenance Code を利用する場合、技術者は Storage Technology の技術サポート・スタッフにコンタクトして当該システムのシリアルナンバーを提供し、Maintenance Code のレベルを指定する。それによって技術者は GetKey を得て、保守レベルをリセットすることができる。

被告は、Storage Technology のシステムに対する保守サービスで競合し、GetKey を回避し、Maintenance Code へアクセスし、メンテナンスレベルをリセットするためのアルゴリズムを取

128 リバースエンジニアリング
(f)
(1)第(a)項(1)(A)の規定にかかわらず、コンピュータ・プログラムのコピーを使用する権利を適法に取得した者は、独自に創作したコンピュータ・プログラムとその他のプログラムとの互換性を達成するために必要なプログラムの要素であって、回避を行う者にとってそれまで容易に入手することができなかったプログラムの要素を特定し解析する目的のみのために、かかる特定および解析の行為が本編に基づく侵害を構成しない範囲において、当該プログラムの特定の部分へのアクセスを効果的にコントロールする技術的手段を回避することができる。
(2)第(a)項(2)および第(b)項の規定にかかわらず、互換性の達成のために必要である場合は、第(1)節に基づく特定および解析を可能にするために、または、独自に創作されたコンピュータ・プログラムとその他のプログラムとの互換性を達成するために、本編に基づく侵害を構成しない範囲において、技術的手段を回避する技術的手段、または技術的手段により施される保護を回避する技術的手段を、開発し使用することができる。
(3)第(1)節に基づき許容される行為によって得られた情報および第(2)節に基づき許容される手段は、第(1)節または第(2)節にそれぞれ掲げる者が当該情報または手段を、独自に創作されたコンピュータ・プログラムとその他のプログラムとの互換性を達成するためのみに提供する場合には、本編に基づく侵害を構成せず、また本条以外の適用法に違反しない範囲において他者に提供することができる。
(4)本項において、「互換性」とは、コンピュータ・プログラムが情報を交換し、交換された情報を相互に使用できる機能をいう。

129 Davidson & Associates v. Jung, 422 F.3d 630 (8th Cir. 2005)　控訴審もこの判断を支持した。

130 421 F.3d 1307 (FedCir. 2005)

得した。メンテナンスレベルをリセットする過程で、RAM 上に Maintenance Code のコードが複製される。そのため、Storage Technology が著作権侵害と DMCA 違反で仮差止めを求めた事案である。

地裁は、GetKey がアクセスをコントロールするものであり、被告がこれを回避していることは明白だとした。被告は 1201(f)リバースエンジニアリングの抗弁を主張したが、裁判所は、GetKey を回避後に RAM コピーが作られ著作権侵害があるため、「本編に基づく侵害を構成しない範囲において」とする要件を充足しないとしてその主張を退けた。

しかし、連邦巡回控訴裁判所はこれを破棄し、原告の主張を退けた。まず、控訴裁判所は、RAM 上への複製について、117(c)で修理に伴う複製として権利侵害を否定した。そして、1201(a)違反の点について、Lexmark、RealNetwork v. Streambox を引用し、裁判所は、「一般的に裁判所は、問題とされるアクセスについて著作権法上保護される権利と結びつきのある場合のみ DMCA の違反を認めてきた…Storage Technology の著作権法上の権利にリスクがない以上、DMCA の適用はない。」

（１３） Egilman v. Keller & Heckman, LLP[131]

原告の Egilman は医者で、裁判所において専門家証人として証言した。裁判所が証言内容の秘匿命令を出し、発言内容を公開しないことが命じられていた。しかし、Egilman はウェブサイト上に名誉棄損的な発言内容を公開したため、罰せられた。Egilman は、被告の法律事務所が彼のウェブサイトにログインするユーザーネームとパスワードを不正に入手し、他の法律事務所に提供。それによって Egilman のウェブサイトでの発言内容が入手されたとして、DMCA に違反するとして法律事務所を相手に提訴した。

裁判所は、有効なユーザーネームとパスワードを利用することは、仮にその利用について許諾がないとしても、DMCA 上の「回避」に該当しないと判断した。Egilman により使われた「技術的手段」は「回避」されたのではなく、実行されただけであるとした。

（１４）Macrovision v. Sima Products Corp.[132]

Macrovision は著作物を含んだ DVD に Analog Copy Protection（ACP）を埋め込んでいた。ACP システムによって複製物を視聴できないほどに解像度のクオリティが低下させられる。被告 Sima の装置は、アナログ信号からこの ACP を除去し、解像度の落ちない複製物を作成することを可能にするものであり、1201 条におけるコピー等利用制限技術であることは明白なものであった。

Sima は、その装置の主たる目的は、DVD コレクションのためのバックアップコピーを作るフェアユースを認めることであると主張したが、裁判所は、1201(a)(2)(B)において一定のユーザーのフェアユースを認めるが、その例外は、1201(a)(2)によって禁止される装置の製造・販

131 401 F. Supp.2d 105 (D. DC 2005)

132 2006 WL 1063284, 20 ILR (P&F) 87 (S.D. N.Y. 2006)

売には適用されないとした。

（１５） Auto Inspection Services, Inc. v. Flint Auto Auction, Inc.[133]

Auto Inspection は、リース期間が終了した後の自動車の統一的な検査法を提供する自動車検査プログラムの保有者である。そのプログラムの一部としてクオリティコントロールが含まれており、プログラムを利用して集めた情報を監視することができる。この仕組みにより、Auto Inspection は無許諾利用から同プログラムを守っていた。

被告 Flint Auto Auction は、上記プログラムについてかつてライセンスを受けていたが、その後、自ら自動車検査プログラムを制作した。Auto Inspection は、被告がそのプログラムの著作権を侵害するとともに、前述のクオリティコントロールがアクセス制限技術であるから、DMCA 違反であるとも主張した。

裁判所は、クオリティコントロールのユーザー検知機能は、ソースコードへのアクセスを規制しておらず、誰がプログラムを利用しているのかについて Auto Inspection に対して警告する機能をするに過ぎないことから、DMCA 違反は認められないとした。

（１６）Sony Computer Entertainment America, Inc. v. Divineo, Inc.[134]

ソニーはプレーステーション上で違法ソフトが実行されないよう、正規品であることを認証されたソフトのみを実行するシステムを採用していた。被告は、①HDLoader:プレーステーションと両立するゲームの複製を可能にするもの、②Mod Chips:プレーステーションコンソールに接続されると、認証システムを回避し、違法ソフトウェアを実行することを可能にするもの、③認証システムのためのソフトウェア・ハードウェアを起動させず、プレーステーションを動作させる装置を販売した。

被告 Divineo は、著作権侵害にならない態様があることや、ソフトウェア開発者にとって高価なソニーコンソールの代替装置としてプレーステーション向け自作ゲームを試すために用いることができるなど、回避すること自体以外の目的を指摘するとともに、独自創作のコンピュータ・プログラムをプレーステーションと互換性を持たせていることから 1201(f)のリバースエンジニアリングであると主張した。

裁判所は、被告主張の抗弁をすべて排斥した。すなわち、被告装置は、プレーステーションが採用する認証システムを回避することを第一の目的として設計されていると判断した。そして、回避後のフェアユースや合法利用の存在は、そのような回避装置の取引に対する責任を免除しないと述べた。

また、リバースエンジニアリングの抗弁について、仮にユーザーが互換性の達成のために技術的手段を回避することが許容されると主張できるとしても、装置の第一次的な目的が技術的手段の回避である以上、その装置の製造業者や販売業者はそのような抗弁を主張できないと判

133 2006 WL 3500868 (E.D. Mich. 2006)
134 457 F. Supp.2d 957 (N.D. Cal. 2006)

断した。

（１７） Healthcare Advocates Inc. v. Harding, Earley, Follmer & Frailey[135]

Healthcare Advocates が商標・著作権・営業秘密の侵害を理由とした訴訟を提起した被告の代理人法律事務所を提訴したものである。法律事務所の職員は、裁判における反論の準備のために、Healthcare Advocates の過去のウェブサイトの情報を収集するために、Internet Archive が提供する Wayback Machine システムを利用した。Wayback Machine は、ウェブ上の情報をすべてアーカイブしていくものであるが、ウェブサイトオーナーの意思を尊重し、a robots.txt file がサイトを保存しない旨を記している場合には保存しない仕組みとなっている。

本件では、その機能に不具合があった際に、当該法律事務所の職員が、Healthcare Advocates がサイト上保存をしないことを明記していたにもかかわらず、その対象を閲覧することが偶々できた。

Healthcare Advocates は、a robots.txt file という技術手段を無効化してアーカイブの閲覧をしたとして、DMCA 違反を主張した。

本件では、1201 条(a)(3)(b)の「『著作物へのアクセスを効果的にコントロールする』とは、当該技術的手段がその動作の通常の過程において著作物へのアクセスを行うには、著作権者の許諾を得て情報を入力しまたは手続もしくは処理を行うことを必要とする場合をいう。」との定義に照らし、a robots.txt file の Indication が技術的手段と言えるのかが論点となった。
裁判所は、本件事案の下では、Wayback Machine が正常に動作していれば、a robots.txt file を置くことで、アーカイブ化されたスクリーンショットへのアクセスはきちんとブロックされると認定し、「技術的手段を効果的にコントロール」していると判断した。
ただし、本件でスクリーンショットを法律事務所の職員が見ることができたのは、偶然の不具合　によるもので、故意に回避した結果ではないため、1201(a)(1)の違反には当たらないと判断した。

（１８）Ticketmaster L.L.C. v. RMG Technologies, Inc.[136]

本件は、被告 RMG が提供したツールが、チケット大量購入を目論むユーザー（チケットブローカーなど）が Ticketmaster の CAPTCHA システム（チケット販売システムにアクセスするためには、利用者がスクリーンに表示される文字と数字をシステムに挿入しなければならない）を回避し、チケットの機械的な大量購入を可能にするものであったため、これに対し Ticketmaster が DMCA 違反で仮差止めを求めた事案である。

被告は、当該システムは、チケット販売をコントロールしているが、著作物へのアクセスをコントロールするものではないとして 1201 条が適用されないと主張した。裁判所は、DMCA 上、「技術的手段」となっており、システムやプログラムと限定されていないこと、実際に自

135 497 F.Supp.2d 957 (E.D. Pa. 2007)
136 507 F. Supp.2d1096 (C.D. Cal. 2007)

動化機器のほとんどは、著作物たるチケット販売ページへのアクセスを得るための文字や数字を認識、打ちこむことができないことなどから「効果的な技術的手段」と判断した（1201(a)(2)違反）。

さらに、同技術は、チケット販売ウェブページへのアクセスを制限することで、当該ページの複製を阻害するので、コピー等利用制限技術を回避するものと判断し（1201(b)(1)）、仮差止命令を出した。

（１９）CoxCom, Inc. v. Chaffee[137]

CoxCom は、ケーブルボックスのリースを行い、申込者は、送信されてくるシグナルの暗号を視聴のために解除することができ、逆に、有料番組の購入に関する情報（請求に係る利用状況を示す情報など）をユーザーから CoxCom に対して送信するシステムを用いていた。

被告は、低周波信号を除外するデジタルケーブルフィルターを販売していた。同フィルターは、FM ラジオやその他家庭内機器からの周波数障害を除去するという違法ではない利用方法もあったが、被告は、有料番組の請求情報の送信を除外し、請求を免れることができるとして販売促進活動をしていた。第 1 巡回区控訴裁判所は、本件では、有料放送の利用状況の送信とそれに基づく請求システムが「技術的手段」であり、被告はそれを回避しているとして、原告勝訴の原審を支持した。

（２０）Realnetworks, Inc. v. DVD Copy Control Association, Inc.[138]

DVD Copy Control Association（「DVDCCA」）は、コンテンツコントロールシステム（CSS）技術のライセンスを行っており、DVD コンテンツを守るために認証プロセスと暗号化レイヤーを DVD に含んでいた。認証プロセスを経て、暗号解除を経なければ、DVD コンテンツを視聴することができない。

Realnetworks 製品 Real DVD は、DVD のコピープロテクションを施されたコンテンツをハードディスクに複製し、DVD ドライブ上に DVD がなくとも、その後の視聴をすることを可能にする装置を製造・販売した。そのため DVDCCA は、Realnetworks に対して仮差止めを求めて提訴した。

裁判所は、認証プロセスがアクセス制限技術、暗号がコピー等利用制限技術であるとして、その両者を回避する Realnetworks の装置の販売は、1201(a)(1)(A)と 1201(b)に違反すると判断した。Realnetworks は、DVDCCA の保護技術が広く破られている事実を示し、「効果的な技術的手段」ではないと主張したが、裁判所は、保護技術の強弱は法文上問われておらず、消費者のレベルで簡単に複製物を作ることができなければ十分であるとして、その主張を退けた。

また、Realnetworks は、その装置がユーザーが私的にフェアユースをすることを支援するものであるから、当該装置の製造・販売もフェアユースとして許容されると主張した。裁判所は、

137 536 F.3d 101 (1st Cir. 2008)
138 641 F.Supp.2d 913 (N.D. Cal. 2009)

DMCA は限定的にユーザーに対してフェアユースの例外を提供するかもしれないが、ユーザーがそのような行為を行うことを手助けする装置を製造･販売することまでも許容するものではないとして、かかる主張も退けた。

（２１） MGE UPS Systems Inc. v. GE Consumer and Industrial Inc.[139]

MGE UPS Systems は、無停電電源装置（UPS）を販売していた。UPS の利用には、MGE UPS Systems が権利を有するソフトウェアプログラムを必要とした。その利用時には、セキュリティのためのドングル（特定の PC でのみソフトウェアが作動するようにするもの）がラップトップのシリアル番号と結びつくことが必要であった。

しかし､ソフトウェアのハッカーがこのドングルのセキュリティを破るための情報をネット上に公開し､それによってハックされたソフトウェアは無制限で利用可能なものとなった｡被告従業員は、そのセキュリティを破られたソフトウェアを利用した。MGE UPS Systems が 1201(a)(1)違反を主張したが、連邦巡回控訴裁判所は、1201(a)(1)は、技術的手段を回避することを規制するもので､回避後の複製行為を規制するものではないとし､被告の従業員による回避が認定できないとした。

（２２） MDY Industries, LLC v. Blizzard Entertainment, Inc.[140]

MDY Industries（｢MDY｣）は、Blizzard Entertainment（｢Blizzard｣）が提供するオンラインゲーム World of Warcraft（｢WoW｣､プレイヤーが Blizzard の提供するサーバにアクセスしてゲームを楽しむ）において、プレイヤー自身がゲームを行わず、不在のままでもプレイを続け、その結果、ゲームを前へ進めることを可能にするソフトウェア Glider を制作・販売した。Glider 自体は、WoW プログラム自体を複製し、改変するものではなかったが、Blizzard は、プレイヤー間の公平等からオンライン上の対戦ゲームの魅力を減退させることを懸念し､Glider のようなロボットの利用を規約上禁止するとともに､Glider 等のロボットを検知し、検知した場合にはゲームを行うことができないようにする技術（Warden）を施した。

Warden は、２つのソフトウェアから構成されている。１つは、ユーザーが Blizzard サーバにアクセスした際に、ユーザーが Glider 等を利用していないことを確認し、利用が確認されればアクセスを拒否する scan.dII というソフトウェア｡もう１つは､ユーザーがプレイ中に bot プログラム利用していることを検知した場合、その時点でゲームへのアクセスを遮断する resident というソフトウェアである。

第９巡回区控訴裁判所は、1201(a)(2)と 1201(b)の法文上の相違[141]から、1201(a)(2)の適用については、1201(b)とは異なり、著作権侵害との合理的な関連性を要求するものではなく、端的

139 modified en banc, 622 F.3d 361 (5th Cir. 2010)

140 629 F.3d 928 (9th Cir. 2010)

141 1201 条(a)では、｢本章で保護されている作品｣（work protected under this title）とされているのに対して、1201 条(b)では、｢著作権者の権利｣（a right of a copyright owner）である。

に、著作物に対するアクセスを保護するもの（著作物の保護のために権利を拡張するもの）との見解を示した。法文上の相違点として、1201(b)は、回避装置の取引行為を禁止しているものの、回避行為そのものを禁止していない点に着眼し、その理由が、そのような行為がすでに著作権侵害行為として捕捉されているという点にあることから、1201(a)(1)で回避行為そのものを違法にするのは、著作権侵害行為とは関係のない、新たな回避禁止権（a new anti-circumvention right）を付与するものと解釈した。

1201 条(a)が例として挙げているスクランブルや暗号化の解除が必ずしも著作権侵害やそれを助長するものではないという点も指摘している。

そのような 1201 条の理解を前提としたうえで、WoW のソースコード部分と個別の非言語的部分（モンスターの視覚的イメージ等 400,000 の構成要素）に対するアクセスは、プレイヤーのハードドライブからアクセスすることが可能で、Blizzard サーバを通じずにアクセスできた。よって、WoW に対するアクセス制限技術は「効果的な」ものではないとして、その部分へのアクセスについて 1201 条違反ではないと判断した。

他方、ダイナミックな非言語的部分と判決が呼ぶ部分（リアルタイムで別世界を旅する経験、サーバ上での戦いのシーンの構成、そこに現れる住人・モンスター・他のプレイヤーなど）に対するアクセスについて、前述のとおりサーバにアクセスすることが不可避であることから、Warden は効果的にアクセスをコントロールしていると判断し、それを回避する装置の製造・販売を行う MDY について 1201(a)(2)違反を認めた。

しかし、1201(b)(1)については、次のような理由から違反を認めなかった。すなわち、エンドユーザーライセンス上、WoW のプレイヤーが RAM にソフトウェアコードを複製することは認められている。したがって、複製行為それ自体は著作権侵害ではなく、Glider を利用したプレイについてラインセンス違反があるとしても、それは著作権侵害を構成するものではなく、Warden は効果的に利用制限をするものではないから、1201(b)(1)を充足しないとした。

本判決は、1201(a)(1)(2) を新たな拡張的な権利としてのアクセス権を著作権者に付与するということを立法経緯や法律文言に照らして明らかにし、(8)、(9)の他の巡回区控訴裁判所が採用した 1201(a)(1)(2)のアクセス制限技術に関する制限的な解釈（著作権侵害との合理的な関連性を要求する立場）を明確に批判し、それとは異なる立場を採用している点に意義がある。

（２３）Murphy v. Millennium Radio Group LLC[142]

原告 Murphy は写真家であり、ある写真の著作権を保有している。被告の従業員が雑誌から Murphy の写真をスキャンし、著作権管理情報を削除したうえ、被告のウェブサイト等にアップした。Murphy が DMCA 1202 条違反として差止めを認めた。

原審は、写真のクレジットは、自動的な著作権保護又は管理システムの一部になっていないため、DMCA 下の著作権管理情報（CMI）と言えないと判断した。

142 650 F.3d 295 (2011)

しかし、第 3 巡回区控訴裁判所は、条文上明確に CMI が自動的な著作権保護又は管理システムの一部であることを要求していないとして、1201 条と 1202 条とは独立して設けられており、両者を結びつけ、1201 条の技術的手段との関連性の中で 1202 条が解釈されなければならないとの被告の主張を退けた。

本件は、1201 条の解釈ではなく、CMI の定義の解釈に関するものである。

（２４）Dish Network LLC v. World Cable Inc.[143]

Dish Network は、衛星テレビ放送事業者として、番組を暗号化しており、サービス利用者は専用受信機によって当該放送を受信し、暗号化を解除して視聴する。本件で、World Cable は、Dish Network と契約を締結して、当該放送を受信したうえ、暗号化を解除して、他の第三者へ再送信していた。

Dish Network は、World Cable が受信契約において、視聴目的で利用することを合意しており、転送目的を秘した欺もう的な受信契約の締結が、1201(a)(1)のアクセス制限技術の回避だと主張した（(19) Dish Network は CoxCom 判決をその主張の拠り所とした）。

これに対して裁判所は、受信契約の締結が欺もう的行為によるものだとしても、 World Cable は、回避技術の手順に従っているだけで、技術的手段を「回避」していないとして、その主張を退けた。

ID・パスワードを不正に入手して、それを利用した結果、技術的手段による遮断を受けない場合が、技術的手段の「回避」にならないとする（13）と同種の判断である。

１．３　議会図書館長による規則制定の歴史

1201 条 (a) (1) は、前述のとおりアクセス制限技術を規制する条項であるが、その中に、著作権局の推奨に基づき、議会図書館長が、1201 条 (a) (1) 第(A)号に基づく回避の禁止規定の例外となる著作物 3 年に一度定める（期間は 3 年間とされ、その次の規則制定見直し時に、更新されるか、その時点で例外的取扱いが終了するのかが定められる）ことができる旨を規定し、アクセス制限技術の規制と円滑な著作物の利用のバランスを図ろうとしている。

（１） 2000 年の例外[144]

2000 年 10 月 27 日、米著作権局は、議会図書館長が認める 1201(a)(1)の回避禁止規定の例外となる著作物を明らかにした（施行日は 2003 年 10 月 28 日までの間）。

①フィルタリングソフトウェア･アプリケーションによってブロックされているウェブサイトのリストから構成される編集物

②アクセス制限技術によってアクセスを制限される言語著作物（コンピュータ・プログラム、

143 893 F.Supp.2d 452 (E.D. N.Y. 2012)

144 65Fed. Reg. 64556(Oct.27, 2000)

データベースを含む）のうち、誤作動・故障・劣化のためにアクセスできなくなっているもの

（２）2003 年の例外（2003 年 10 月 27 日米著作権局の推奨。2006 年 10 月 27 日まで有効）[145]

①ドメインやウェブサイトへのアクセスを制限する目的をもった市販ソフトウェアアプリケーションによってブロックされているインターネットロケーション（ドメイン・URL・IP アドレス等）のリストで構成された編集物（ただし、コンピュータを保護する目的のみでブロックするもの、ファイヤーウォールや対ウイルスソフトウェアなどは除く）。

②誤作動・故障によるアクセスがドングル（dongle：特定の機器でのみソフトウェアを利用できるようにするソフトウェア）によって制限されるコンピュータ・プログラムのうち、劣化しているもの。

③時代遅れ[146]となったフォーマットで配布されているコンピュータ・プログラムとビデオゲームで、アクセスのために元の媒体又はハードウェアを必要とするもの。

（３） 2006 年の例外（2006 年 11 月 27 日。2009 年 10 月 27 日まで有効）

①大学の映像メディア研究部門に属する図書館に納められている視聴覚著作物（ただし、回避が同研究部門の教授による教材に利用するために編集物を制作する目的によるものに限る）。

②時代遅れとなったフォーマットで配布されているコンピュータ・プログラムとビデオゲームで、アクセスのために元の媒体又はハードウェアを必要とするもの（ただし、回避が図書館や博物館が発行済のデジタル著作物を保存する目的によるものに限る）。

③誤作動・故障によるアクセスがドングル（dongle：特定の機器でのみソフトウェアを利用できるようにするソフトウェア）によって制限されるコンピュータ・プログラムのうち、劣化しているもの（これは、2003 年時の②と同様）。

④電子書籍フォーマットで配布された言語著作物（ただし、その全てが電子書籍バージョンがアクセス制限技術を有し、書籍の音読機能やテキストを特殊なフォーマットへ変更するスクリーンリーダーの利用を妨害している場合に限る）。

⑤ワイヤレス携帯のワイヤレスネットワークへのアクセスを可能にするファームウェア形態のコンピュータ・プログラム（ただし、回避がワイヤレスネットワークへアクセスする正当な目的がある場合に限る）。

⑥コンパクトディスクの形態で頒布され、かつ、技術的手段によって保護されている録音物と録音物に伴う聴覚著作物（ただし、当該手段が適法に購入された場合に限る。）

---

145 この時に主張された例外の中に、Static Control によって提出された Lexmark International 社のプリンターにて Lexmark International 社製以外のカートリッジを利用できるように、同社の認証シークエンスを回避することを認めるように求めた。米著作権局は、これは裁判例において解決しているとして、明示的な例外として認めなかった。68 Fed. Reg. at 62017

146 この点は、著作物を認識するために必要とされる装置が製造されていないか、もはや合理的な手段では市場で入手できない場合に充足するものとされる。

（４）2010 年の例外（2010 年 7 月 27 日。2012 年 10 月 27 日まで有効）[147]

①適法に制作され入手された DVD で、CSS（コンテンツスクランブルシステム）で保護されている映画（ただし、批判又は批評といった新たな作品に映画の一部を取り込むことのみを目的とする回避であって、行為者がそのような回避が利用目的の達成のために必要であると信じる又は信じるだけの合理的な理由がある場合に限る：教育目的利用、ドキュメンタリー制作、非商業目的利用）。

②ワイヤレス携帯電話がソフトウェアアプリケーションの実行を可能にするコンピュータ・プログラム（ただし、回避が、適法に取得されたアプリケーションの互換性を実現する目的の場合に限る）。

③中古のワイヤレス携帯電話をワイヤレスネットワークにコネクトすることを可能にするファームウェア又はソフトウェアの携帯のコンピュータ・プログラム（ただし、回避が、コンピュータ・プログラムの所有者によって行われ、ワイヤレス通信ネットワークに接続し、ネットワークのオペレーターからそのアクセスが許容されている場合に限る）。

④個人の PC 上でアクセスできるビデオゲームで、適法に取得された著作物へのアクセスをコントロールする技術的手段で保護されているもの（ただし、回避が、セキュリティ上の欠陥、脆弱性をテスト、調査、訂正を行う善意の目的による場合に限る）。

⑤誤作動・故障によるアクセスがドングル（dongle：特定の機器でのみソフトウェアを利用できるようにするソフトウェア）によって制限されるコンピュータ・プログラムのうち、劣化しているもの（これは、2006 年時の③と同様）。

⑥電子書籍フォーマットで配布された言語著作物（ただし、その全ての電子書籍バージョンがアクセス制限技術を有し、書籍の音読機能やテキストを特殊なフォーマットへ変更するスクリーンリーダーの利用を妨害している場合に限る）（これは、2006 年時の④と同様）。

（５）2012 年の例外（2012 年 10 月 26 日）[148]

①電子書籍フォーマットで配布された言語著作物（ただし、その全ての電子書籍バージョンがアクセス制限技術を有し、書籍の音読機能やテキストを特殊なフォーマットへ変更するスクリーンリーダーの利用、その他の支援技術を妨害している場合に限る）

②携帯電話が適法に取得されたソフトウェアアプリケーションの実行を可能にするコンピュータプログラム（ただし、その回避がアプリケーションの互換性を達成するために行われているものに限る）

③本例外が認められてから 90 日以降にワイヤレス通信ネットワークのオペレーターから入手した携帯電話を異なるネットワーク通信に接続することを可能にするファームウェア又はソフトウェア形態のコンピュータ・プログラム（ただし、当該携帯がロックされている通信ネットワークのロックを解除するよう所有者より要求がなされた後、合理的な期間に

147 77 Fed. Reg. 43825(July 27,2010)

148 77 Fed. Reg. at 43849

解除しない場合に限る)。

④適法に制作され入手された DVD に収められ、CSS（コンテンツスクランブルシステム）で保護されている、17 章 101 条で定義されている映画（ただし、回避を行う者が、その映画の批判又は批評を達成するために必要とされる高画質を他の合理的に取り得る手段（非回避的方法又はスクリーンキャプチャーといった例外としてすでに認められている技術）では実現できないと信じる又は信じるだけの合理的な理由がある場合であり、かつ、そうした回避が次の一定の場合の批判又は批評目的で短い時間の映像を利用するためだけに行われる場合：教育目的利用、ドキュメンタリー制作、非商業目的利用)。

⑤適法に制作されオンライン配信サービスを通じて入手された、様々な技術的手段で保護されている、17 章 101 条で定義されている映画（ただし、回避を行う者が、その映画の批判又は批評を達成するために必要とされる高画質を他の合理的に取り得る手段（非回避的方法又はスクリーンキャプチャーといった例外としてすでに認められている技術）では実現できないと信じる又は信じるだけの合理的な理由がある場合であり、かつ、そうした回避が次の一定の場合の批判又は批評目的で短い時間の映像を利用するためだけに行われる場合：映画研究などの教育目的利用、ドキュメンタリー制作、非商業的ビデオ、映像分析を提供するマルティメディアのノンフィクション電子書籍)。

⑥適法に制作され入手された DVD に収められ、CSS（コンテンツスクランブルシステム）で保護されている、17 章 101 条で定義されている映画（ただし、その回避が適法な暗号解除後に映画コンテンツの複製を可能にするものと明示され、かつ、一般に提供されたスクリーンキャプチャー技術を用いてなされ、回避を行う者が当該回避が望ましい批判又は批評を行うために必要であると信じる又は信じるだけの合理的な理由がある場合であり、かつ、そうした回避が次の一定の場合の批判又は批評目的で短い時間の映像を利用するためだけに行われる場合に限る：映画研究等の大学教育から初等中等教育のためなどの教育目的利用、ドキュメンタリー制作、非商業的ビデオ、映像分析を提供するマルティメディアのノンフィクション電子書籍)。

⑦適法に制作されオンライン配信サービスを通じて入手された、様々な技術的手段で保護されている、17 章 101 条で定義されている映画（ただし、その回避がスクリーンキャプチャー技術を用いてなされ、回避を行う者が当該回避が望ましい批判又は批評を行うために必要であると信じる又は信じるだけの合理的な理由がある場合であり、かつ、そうした回避が次の一定の場合の批判又は批評目的で短い時間の映像を利用するためだけに行われる場合に限る：映画研究等の大学教育から初等中等教育のためなど教育目的利用、ドキュメンタリー制作、非商業的ビデオ、映像分析を提供するマルティメディアのノンフィクション電子書籍)。

⑧適法に制作され入手された DVD に収められ、CSS（コンテンツスクランブルシステム）で保護されている、又は、オンラインサービスによって配信され、作品へのアクセスをコントロールする技術的手段によって保護される DVD に収められた映画及び視聴覚著作物(た

だし、その回避が、当該作品の複製物に埋め込まれたプレーヘッド及び・又は関連タイムコード情報にアクセスするためだけに達成されるもので、かつ、その目的が互換性を有するプレイヤーを制作するためのものである場合に限る)。

（６） 2015 年の例外[149]（2015 年 10 月 28 日）

①映画の著作物（テレビ番組、ビデオを含む）（更新）：映画の著作物を批判・論評目的でわずかの部分を利用するための回避措置

②電子的に配信された言語著作物（音読機能を阻止し、スクリーンリーダーその他の補助技術を妨害する技術的手段によって保護されたもの）（更新）

③コンピュータ・プログラム（ワイヤレスネットワークに接続することを可能にするためのもの）（更新）

④コンピュータ・プログラム（スマートフォンその他の移動式コンピューティング装置のアプリケーションの互換性を達成するためのもの）（更新）

⑤コンピュータ・プログラム（スマート TV 上でアプリケーションの互換性を達成するためのもの）（新設）

⑥自動車の機能をコントロールするコンピュータ・プログラム（診断・修理・適法な修正のため）（新設）

⑦適法に取得された装置又は機械のコンピュータ・プログラム（安全性のテストのためになされる回避）（新設）

⑧ビデオゲーム（認証のためにサーバとのコミュニケーションが必要となる場合）（新設）

⑨３D プリンターの原材料を制限するソフトウェア（新設）

⑩埋め込まれたネットワークデバイスから取得される患者のデータ（新設）

１．４　最新動向

技術的手段のアクセス制限技術の回避について、アクセス制限技術と著作権侵害との間の関連性が要求されるかという論点について、下級審の判断が巡回区で異なっているが（前期(8)(9)と(23)の対照的な判断)、最高裁の判断は示されてはいない。しかし、ここ 3 年ほどこの論点に関する新たな裁判例や注目すべき論文等は確認できず、議論は沈静化している様子である。

なお、2015 年 10 月に新たな回避禁止の例外（1.3 に記載のとおり）が発表されたばかりであるが、2015 年に世界を震撼させた VW（フォルクスワーゲン）の不正が、NGO による VW 車のプログラムへの（コントロールを回避した、法的には「違法な」）アクセスによって発覚した経緯から、米国では、厳格なアクセス制限技術の回避禁止への疑義が高まり、技術的手段の法

[149] U.S. Copyright Office, 37 CFR Part 201［Docket No. 2014-7］, “Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies”) 2015, at 71

的保護については再び関心が集まっている[150]。

米著作権局長自ら、2013 年に、過去 15 年を振り返り、暫定的な例外を 3 年に一度認める規則制定手続及びその結論について再評価する必要を訴え、2015 年 12 月には実際に現行制度の問題点について検討を開始した（Section 1201 Study）[151]。今後のリフォームの動向では、議会が再評価を行う否定できない[152]。

[150] 例えば、http://boingboing.net/2015/09/19/vws-car-drm-let-it-get-away.html は、VW 社は、DMCA の規制により長年不正の発覚を免れた面があるものの、一般にその回避を自由にすれば、ソフトウェアの排ガス規制に関する数値変更を自由に行うことができてしまう弊害にも言及する。

[151] http://copyright.gov/policy/1201/

[152] Maria Pallante 「次世代の偉大な著作権法」（知的財産法政策学研究 45 号、2014）55 - 57 頁

２　イギリス

イギリス法の技術的手段の規制は、前述した EU における各指令（コンピュータ・プログラム指令、条件付アクセス指令、情報社会指令）にそれぞれ対応する規定を著作権法の中に明確に有していることに特徴がある。

判例上、技術的手段と評価するためには、著作権によってコントロールされる権利を保護するものであることを要求しているものがあるが、近時の任天堂事件では、コンソール上での一時的複製を防止する暗号化認証システムについてコピー等利用制限技術との判断が示されており、コピー等利用制限技術の概念が拡大している様子が伺える。また、純粋なアクセス制限技術に規制が及ぶことが明確なのは、有料 TV サービス等の不正受信を違法とする規定のみである。

また、規制の例外については、許諾行為（permitted acts）を設け、その正当な回避を妨害される者に異議申し立てを認める法制度を設けているが、具体的な事例は見られない。

２．１　法制度

（１）　情報社会指令情報社会指令に対応する法規制

英国では、著作権・意匠・特許 1988 年法（「Copyright, Design and Patents Act 1988」、以下「CDPA」という）の 296ZA 以下で情報社会指令を国内法制化するために技術的手段の新たな規定を定めたが、その立法形式の特徴は、コンピュータ著作物か否かで適用条文に相違があることに起因する。これは、立法がそれぞれ異なる情報社会指令情報社会指令に対応する立法となっているためである。

すなわち、2001 年の情報指令を国内法化する以前に、すでにコンピュータ・プログラム保護指令にもとづき、技術的手段を回避してなされるプログラムの商取引行為については、これを著作権侵害とする規定を有していたため（CDPA296：著作権保護を回避することを意図した装置）、2003 年の改正時に挿入された条項は、コンピュータ・プログラム著作物を除く著作物についてのみ適用されるものとされた。

また、条件付アクセス指令に対応する法規制として、297 条以下が設けられた。以下、この３つの規制について概観する。

（２）コンピュータ・プログラムに対する規制

296(1)は、次のように定める。

(1)本条は、次の場合に適用される。(a)技術的装置（device）がコンピュータ・プログラムに付されており、かつ、(b)ある者(A)が、違法な複製物を作るためと知りながら、又は知るべき合理

的な理由がありながら、(i)技術的装置を無許諾で除去又は回避することのみを目的とする手段(means)を販売又は貸与目的で製造・輸入・頒布・販売若しくは、貸与先を探す、販売又は貸与目的で提供・販売又は貸与目的で広告、営利目的で所持する場合、(ii)技術的装置を除去又は回避することを可能に又は容易にさせる意図をもって情報を公開する場合

そして、かかる「技術的装置」の定義を前提として、296(2)は、(a)こうした技術的装置が付されたコンピュータ・プログラムの複製物を公衆に提供する者又は公衆送信する者、(b)(a)に該当しない場合には、著作権者又は独占的利用被許諾者、(c)コンピュータ・プログラムに付された技術装置の知的財産権の権利者又は独占的利用被許諾者が、前記の技術的装置の除去又は回避行為に対して、著作権侵害に対して著作権者が有する権利と同様の権利を有する旨を定める[153]。

（３）コンピュータ・プログラム以外の著作物に対する規制

①技術的手段の回避行為規制

コンピュータ･プログラム以外の著作物については CDPA294ZA から ZF に定められている。296ZE(2)において、著作物に対して技術的手段が講じられている場合に、許諾された行為(permitted acts)を行うことができない場合、その者又は、そうした者のクラス（団体）の代表者は、Secretary of State（国務大臣）に対して不服申立てすることができるとする。

つまり、技術的手段を回避することを一般的に禁止したうえで、技術的手段のためにできない行為の一部を「許諾された行為」(permitted acts)として特定し、そうした行為を行おうとする者に講じられた技術的手段に対する異議申立てをみとめるスキームを採用している。

「許諾された行為」については、296ZE(1)で、「著作権の存続にかかわらず、別表 5A の Part1 に掲載された本法律の条文に基づき著作物に関連してなされる行為」と定義されている。

不服申立てを受けた Secretary of State は、著作権者又は独占的利用被許諾者に対し、そうした許諾された行為について、任意的な措置又は合意が存在するかどうかを確認するため、適当な指示を著作権者等に与えることができる(296ZE(3))。任意の措置や合意が存在しない場合には、申立人が許諾された行為を行うによって当該行為の利益を享受できる範囲で許諾行為を行うことができるようにするよう必要な指示を与える。

また、Secretary of State は、上記不服申立ての形式・方式、自発的措置や合意についての証拠の形式・方式、そして、不服申し立ての手続について定めることになっており(296ZE(4))、Secretary of State による指示は書面によりなされ(296ZE(6))、その後の指示で修正や撤回がなされることもある(296ZE(5))。

[153] 本条文では効果についての特別な記載はないが、著作権侵害に対応して著作権者に与えられる救済手段（差止・損害賠償・違法複製物等の廃棄）が与えられる（CDPA96 以下）。この仕組みは、コンピュータ著作物以外の著作物の規定においても踏襲されている。

②技術的手段の回避装置等の取引行為規制

上述したのは、技術的手段を「回避すること」それ自体についての規制だが、情報社会指令は回避それ自体に留まらず、回避を可能にする装置の販売・貸与・輸入・頒布・販売若しくは、貸与先を探す、販売又貸与目的で提供・販売又は貸与目的で広告又は営利目的で所持する場合をも規制しており、それに対応して、英国法もその旨の規定を用意している(296ZB-ZD)。

296ZB(1)及び(2)は次のように犯罪(offense)が成立する旨を定める。

296ZB (1) 第一次的に、効果的な技術的手段の回避を可能又は促進する目的で設計・生産・採用されている装置・製品・部品を(a) 製造又は貸与する者、(b) 私的利用以外の目的で輸入する者、(c) 取引の過程において(i) 販売又は貸与、(ii) 販売又は貸与のため申し出や提供をする者、(iii) 販売又は貸与のために広告宣伝する者、(iv) 所持する者、(v) 頒布する者又は(d) 取引外で頒布し、当該頒布が著作権者に悪影響を与えている者は、有罪とする。

296ZB(2) その目的が効果的な技術的手段の回避を可能又は促進することにあるサービスを、(i) 取引上、又は(ii) 取引外だが、著作権者に悪影響を与えながら、広告宣伝、販促活動を行う者は、有罪である。

さらに 296ZD は、民事上の責任について、次のように定めている。

本条は次の場合に適用される。(a) 効果的な技術的手段がコンピュータ・プログラム以外の著作物に付されており、かつ、(b)ある者(c)が、 (i)当該手段の回避を目的として広告宣伝、販売活動または営業がされている、 (ii)当該手段を回避すること以外に商業上重要な目的ないし利用方法がない、又は (iii)当該手段を回避することを可能にする又は促進する目的を第一として設計・制作・変形・実施されている 装置・製品・部品・サービスを販売又は貸与目的で製造・輸入・頒布・販売し、若しくは貸与先の募集、販売又は貸与目的での提供・広告、営利目的所持の各場合、(a) こうした効果的技術的手段が付された著作物を公衆に提供する者又は公衆送信する者、(b)(a)に該当しない場合には、著作権者又は独占的利用被許諾者、(c) 効果的保護手段の知的財産権の権利者又は独占的利用被許諾者が、前記の効果的技術的手段の除去又は回避行為に対して、 著作権侵害に対して著作権者が有する権利と同様の権利を有する

（4）不適切な送信信号の受信

1998 年の条件付アクセス指令を国内法制化するために創設された 297 条は、英国内から発信される放送サービスに含まれるプログラムをその支払いを逃れる目的で欺罔的に受信する行為を犯罪とし、罰金を科すとともに、297A は、許諾のない暗号化解除装置の製造・販売等

について犯罪として、罰金・懲役刑（6 か月を超えない）を科す。また、298 で民事上の救済手段として著作権侵害に対するのと同じ救済措置が認められている。

以下、関係条文は以下のとおりである。

297 条（1）（番組を不正受信する罪）

連合王国内にある場所から提供される放送サービスに含まれる番組を、その番組の受信に適用される料金の支払いを回避する意図をもって不正に受信する者は罪となり、簡易な有罪認定手続により、標準等級のレベル 5 を超えない罰金に処せられる。

297 条 A

(1) 何人も、次に掲げる行為を行う場合には、罪となる。

(a) 無許諾の解読装置を製作し、輸入し、頒布し、販売し、貸与し若しくは販売又は貸与のために提供又は陳列すること。

(b) 無許諾の解読装置を営利目的で所持すること。

(c) 無許諾の解読装置を営利目的で設置、保守又は交換すること。

(d) 無許諾の解読装置を販売又は貸与のために広告し、若しくはその他無許諾の解読装置を営利目的の通信を用いて販売促進すること。

(2) 第 1 項で有罪とされる者は、次に掲げるいずれかの刑に処せられる。

(a) 簡易な有罪判決手続により、6 か月を超えない禁固又は法定の最高限度を超えない罰金若しくはその併科

(b) 起訴による有罪判決により、10 年を超えない期間の禁固又は罰金若しくはその併科

(3) 解読装置が無許諾の解読装置であることを被告が知らず、又は無許諾のものであると考える合理的な根拠を有しなかったことを被告が立証することは、本条に基づく罪についての訴追に対して抗弁となる。

298 条

(1) 次に掲げる者は、以下に定める権利を有し、救済を求めることができる。

(a)連合王国又はいずれかの加盟国から提供される放送に含まれる番組の受信について課金する者

(b)連合王国又はいずれかの加盟国から他の種類の暗号化送信を送る者

(c)連合王国又はいずれかの加盟国内から条件付きアクセスサービスを提供する者

(2) 前項（1）の者は、次に掲げることを行う者に対して、著作権者が著作権侵害に対して有するものと同一の権利を有し、同一の救済を求めることができる。

(a)資格を有しない者が番組その他の送信にアクセスすること、又は番組その他の送信に関係する条件付きアクセス技術を回避することを可能とし、若しくは補助することを意図し、又は適応している機器について、次に掲げることを行う者

(i) 作成し、輸入し、頒布し、販売し、賃与し、販売又は賃与のために提供し、陳列し、若しくは販売又は賃与のために広告すること。

(ii) 営利目的で所持すること。

(iii)営利目的で取り付け、維持し、又は交換すること。

(b)資格を有しない者が番組その他の送信にアクセスすること、又は番組その他の送信に関係する条件付きアクセス技術を回避することを可能とし、若しくは補助することを意図されるいずれかの情報を公表し、又はその他営利目的の通信を用いて販売促進すること。

(3) さらに、その者は、第 99 条又は第 100 条（ある種の物品の引渡し又は押収）に基づいて、そのような機器に対して、著作権者が侵害複製物に関して有する権利と同一の権利を有する。

このように指令に対応して複雑な規制をしており、例えば、著作物を含んだ有料 TV プログラムを不正に受信する装置の製造・販売などのように、当該回避装置が主に回避のみを目的とするものであった場合には、298（2）（a）（iii）とともに 297ZD（1）（b）（iii）にも違反し、重畳適用されると解されている[154]。

２．２　主要判例

調査の結果、技術的手段の条項を巡る裁判例は非常に限られており、また、現在、技術的手段の法的保護は過去の議論と認識されているとのコメント(Paul Torremans, Nottingham University)が得られた。

技術的手段を規制する条項(CDPA296ZB)の解釈に関し参考になるものとしては、以下の裁判

[154] Lionel Bently& Brad Sherman, Intellectual Property Law (fourth edition), at 357-366

例が挙げられるが、近時目立った動きはなく、法的には安定した状況にあると言える。

（１） R v. Higgs (Neil Stanley) [2009] 1 WLR 73, [2008] FSR 34(CA)

【事案の概要】

本件は、Higgs 氏が、コンソールにセットすることで、適法な CD-ROM に埋め込まれたコードを有しない違法複製の CD-ROM をコンソール上で作動させる Modchips を販売していたため、CDPA296ZB に反するとして刑事処分に問われた事案である。

【裁判所の判断（概要）】

原審は、Modchips が技術的手段を回避するものであるとして刑事罰を肯定したが、最高裁は、同条項における「技術的手段」は著作権侵害を一般的に抑制ないし妨害する性格のものでは足りず、著作権侵害を物理的に妨害する手段である必要があると判断し、無罪としたものである。

検察官側は、「技術的手段」を著作権侵害を回避するための手段と「制限的に」解釈したオーストラリア判決が英国法をオーストラリアよりも広範な規制をするものと指摘していた部分を引き、法律上の文言の差（下記）を強調し、オーストラリアとは異なる解釈を主張したが、最高裁はこれを実質的な差異と捉えなかった。

Australian: "to prevent or inhibit the infringement of copyright"

UK: "prevention or restriction of acts that are not authorised by the copyright owner of that work and are restricted by copyright."

また、検察官は、EU 情報社会指令第 6 条の文言と比べ、英国法において「and are restricted by copyright」が付加されている（著作権侵害行為を回避する手段と解釈することを強く支える）点について、EU 情報社会指令を尊重し、これを無視すべきだと主張した（下線付加）。

Directive: "designed to prevent or restrict acts, in respect of works or other subject-matter, which are not authorised by the rightholder"

UK Act: "prevention or restriction of acts that are not authorised by the copyright owner of that work and are restricted by copyright."

しかし、最高裁は、この追加文言が特別に何かの意味を付加しているものではなく、指令の「which are not authorized by the rightholder」との文言からも、本来は法律上権利者から許諾(authorization)を得なければならない行為を規制する趣旨であることは暗黙の前提であり、英国の立法はそれを明確化したものにすぎないとして退けた。

その結果、最高裁は、Modchips がコンソール上での著作権侵害行為を回避ないし抑止するものではない（すでに違法複製された CD-ROM を稼働させるだけである）ことから、法文上の「技術的手段」に該当しないと結論づけた。

（２） Nintendo Company Ltd & Anor v Playables Ltd & Anor [2010] EWHC 1932 (Ch) (28 July 2010)

①事案の概要

正規の任天堂ロゴデータファイル(NLDF)が検知されないゲームをコンソール上で作動することを可能にし、任天堂 DS の違法複製ゲームを（このコピー自体にはこの装置は関係がない）をコンソール上で利用できるようにする装置を販売する業者の行為が、296ZD（コンピュータ･プログラム以外の著作物に対する効果的な技術的手段回避に対する民事上の責任）及び 296（コンピュータ・プログラムについての技術的装置回避に対する民事上の責任）に関して、技術的手段を回避する行為と評価できるか、が問われた事案。

②裁判所の判断

裁判所は、正確な NLDF が存在しなければ、ゲームがコンソール上に複製されないようになっていること、またコミュニケーション時にデータを暗号化、スクランブルしてやりとりするキーデータも、それが存在しなければ、ゲームの通信が阻害されるという点で、コピーコントロールであるとして、技術的手段の回避行為であると認めた。

この判決は、コンソール上への一時的な複製行為としてとらえ、コピーコントロールとして位置づけたところが特徴的であり、アクセス制限技術に一部含まれる態様の技術についても法的保護を及ぼすものと評価できるように思われる。

２．３　最新動向

上記裁判例のほか、近時特に目立った動きはなく、DRM をめぐる新たな議論は生じていない。また、米国に比べ、圧倒的に DRM を巡る裁判例の数が少ないという点に特徴がある。この点については、著作権法等の法律による DRM の規制はさて置き、例えば、全てを禁止するのではなく複製の数を規制するといった著作権者による柔軟な対応が見られ（技術、契約、ビジネスモデルによる著作権法のオーバーライド）、これに対してユーザーがある程度満足している（著作権法上許される以上の複製をする必要がなく、契約で許容される範囲で十分である）といった事情を指摘する見解がある[155]。

[155] Séverine Dusollier, “The protection of technological measures: Much ado about nothing or silent remodeling of copyright?” , Intellectual Property at the Edge: the Contested Contours of IP (Edited by Rochelle Cooper Dreyfuss & Jane C. Ginsburg) at 266-268　ただし、この点は、英国に限ったことではなく、ＥＵ全域において一般的に妥当するものとして指摘されている。

３　ドイツ

ドイツは情報社会指令 6 条を著作権法 95 条 a から 95 条 d において国内法化した。ただし、コンピュータ・プログラムについてはこの対象から外れ、69 条 f（2）は、権利者は、技術的なプログラム保護の仕組みの違法な除去又は回避を容易にすることのみに向けられた手段に対して廃棄を求めることができるとされている。これは、同条がコンピュータ・プログラム指令の国内法化に対応する条文であるためである。

ドイツ法は、日本法と異なり、技術的手段の回避を全面的に禁止し、そのうえで、95 条 b で幅広く禁止の例外を定めている。すなわち、技術的手段の回避のみではなく、それに利用される機器の製造・販売などその前段階にある行為についても広範に規制を及ぼす一方、著作権の制限規定の利益を享受する者がその利益を受けるために必要な措置を講じることを権利者に義務づけている点が特徴的である[156]。

なお、条件付アクセス指令については、既存の刑法と不正競争防止法により対応された。刑法（StGB）202 条は、特定のセキュリティシステムによって保護されるデータの不正利用を処罰し、条件付アクセスサービスの権利侵害は不正競争[157]とされている。

３．１　法制度

（1）現行法

ドイツは情報社会指令 6 条（技術的手段の法的保護）を、以下のとおり、95 条 a、95b で導入した。95 条 a(1)は、技術的手段を回避する行為を一般的に禁止し、95b は、その例外（回避が認められる場合）を定める[158] [159]。

> 第 95a 条　技術的手段の保護[160]
> (1) この法律に基づき保護を受ける著作物その他この法律に基づき保護を受ける保護対象[161]の保護のために[162]有効な技術的手段は、それを回避する行為が当該著作物若しくは保護対象へのアクセス又はそれらの供用を可能にすることを目的として行われることを、その行為者が知り、又は諸般の事情に照らし知るべきものと認められるときは、権利保有者の同意を得ることなく回避してはならない。

156　小橋馨「技術的保護手段と著作物の自由利用」中山信弘先生古稀記念論文集（弘文堂 2015）638 頁

157　§§1, 3, 4 Nr. 11 Unlauteren Wettbewerb gesetz)

158　なお、ドイツ法 95 条 d は、技術的手段を付していることを製品について十分にはっきりと表示する義務を著作権者に課している。

159　前掲注 61、627 頁以下で、現行法の日独比較をされている。

160　翻訳は CRIC による。

161　つまり、著作物に対して付されていなければならず、非著作物には適用がない。この点は、わが国の不正競争防止法とは異なる。

162　コンピュータ・プログラムには適用がない。69 条(a)－(g)の特別規定によってコンピュータ・プログラムが保護されることになっている。

(2) この法律の意味における技術的手段とは、技術、装置及び部品であって、通常の操作において、保護を受ける著作物その他この法律に基づき保護を受ける保護対象に関する行為のうち権利保有者によって許されていないものを禁止し、又は制限するよう特定されているものをいう。技術的手段が有効である[163]とは、当該技術的手段により、アクセス制御、暗号化、歪み、加工その他の変更のような保護機構、又は複製行為の制御のための機構で保護の目的の達成を確かなものとするものを通じて、保護を受ける著作物又はその他この法律に基づき保護を受ける保護対象の供用が、権利保有者の管理のもとに置かれるものと認められる場合をいう。

(3) 装置、製品又は部品の製造、輸入、頒布、販売、賃貸、販売又は賃貸に関する広告、及び業を目的とする所持、並びに役務の提供で次の各号のいずれかに掲げるものは、禁止される。

1. 有効な技術的手段の回避を目的とする販売促進、広告又は商品化の対象であるもの
2. 有効な技術的手段の回避を除いて、限定された経済的な目的又は有用性を有するにすぎないもの
3. 有効な技術的手段の回避を可能にし、又は容易にすることを主要な目的として、立案され、製造され、調整され、又は提供されるもの

(4) 公共の安全の保護又は刑事司法を目的とする官公署が有する任務及び権限は、第 1 項及び第 3 項に係る禁止によって妨げられることはない。

第 95b 条　制限規定の貫徹

(1) 権利保有者が、技術的手段をこの法律の定めるところに従い用いるものと認められる場合において、次の各号に定めるいずれかの規定による受益者が、著作物又は保護対象に合法的にアクセスするものと認められるときは、権利保有者は、その者に対して、当該規定を必要と認められる限度において行使し得るために不可欠な手段を、処分に供する義務を負う。

1. 第 45 条（司法及び公共の安全）
2. 第 45a 条（障害者）
3. 第 46 条（教会、学校又は授業の用に供するための編集物）
4. 第 47 条（学校放送）
5. 第 52a 条（授業及び研究のための公衆提供）
6. 第 53 条（私的及びその他の自己の供用のための複製）

[163] この点は、技術的に特に優れた者でなく、一般人の見地から有効性が評価される。

a） 第 1 項　複製が、任意の写真製版の方法その他類似の効果を有する方法を用いて、紙又は類似の支持物に行われるものと認められるとき。

b） 第 2 項第 2 文第 1 号

c） 第 2 項の第 2 文第 1 号又は第 3 号と併せ、同項第 1 文第 2 号

d） 第 2 項の第 2 文第 1 号及び第 3 文とそれぞれ併せ、同項第 1 文第 3 号及び第号

e） 第 3 項

7. 第 55 条（放送事業者による複製）

第 1 文に基づく義務の排除を目的とする合意は、無効とする。

(2) 前項の求めに従わない者に対して、同項に定めるいずれかの規定の受益者は、それぞれの権限を実現するために必要とされる手段を処分に供するよう、請求することができる。提供された手段が、権利者の団体と制限規定による受益者との間における合意に適合するときは、その手段は十分であるものと推定する。

(3) 前二項は、著作物及びその他の保護対象が、契約上の合意に基づき、公衆の構成員がその選択に係る場所及び時においてそれらを供用できる方法で公衆に提供されるものと認められるときは、適用しない。

(4) 第 1 項から生ずる義務を履行するために用いられる技術的手段は、任意になされた合意を実施するために用いられる手段を含め、前条に基づく保護を受ける。

なお、技術的手段の保護は、著作隣接権とは異なる、著作権に付随する権利であり、そのような保護が正当化されるのは、回避後の著作権侵害を防止する点に求められる。

（２）回避行為

95(a)(1) は、効果的な技術的手段の回避それ自体を一般的に禁止している。「回避」には、技術手的手段を操作して回避する態様だけでなく、当該手段を無効化するものも含まれると解されている[164]。回避行為が当該著作物若しくは保護対象へのアクセス又はそれらの供用を可能にすることを目的として行われることを、その行為者が知り、又は諸般の事情に照らし知るべきものと認められれば、当該回避は違法なものと評価される。

なお、回避の禁止の法的意義について、ドイツ国内では、独立した権利ではなく、あくまでも著作権に付随する権利との理解が多数であると指摘されている。したがって、リージョンコードによるコピー等利用制限を回避して、DVD を視聴する行為については、禁止の対象から外れると解釈される余地もあるが、学説上、回避それ自体を不法行為（tort）と捉える見解もあり、そのような立場からは、著作物に対して（アクセスをコントロールする）技術的手段が付されていればそれで要件を充足し、著作物の視聴（著作権侵害行為ではない行為）のために回避することも違法と評価される。

164 Westcamp Guido, “The Implementation of Directive 2001/29/EC in the Member States”(2007) at 233

（３）回避装置等の取引

95(a)(2)は、情報社会指令に準拠し、技術的手段に利用される「装置、製品又は部品の製造、輸入、頒布、販売、賃貸、販売又は賃貸に関する広告、及び業を目的とする所持、並びに役務の提供」を禁止している。

（４）制限・例外規定

95 条 (b)は、情報社会指令 6 条（4）に準拠し、権利制限・例外の場合に対応する利用に関して、回避禁止の例外を定めている。

３．２　主要判例

技術的手段に関する８件の裁判例（ただし、CJEU へ回付された件も含む。）がある。

（１） IFPI v.　HeiseOnline [165]

技術的手段を回避するツールの説明文書と当該ソフトウェアへのリンクを張ったオンラインマガジン提供事業者の行為が 95 条(a)違反として認められた事案。本件で被告 HeiseOnline は、オンライン上でリージョンコードを破るソフトウェアの解説をし、そのソフトウェアの置かれた場所の URL を付したが、当該ソフトウェアを販売する目的で行ったものではなかった。しかし裁判所は、これをアクセスコントールの回避を妨害するものと評価した[166]。

（２）Alles Brenner Software [167]

CD バーニングのためのコンピュータ・プログラムを個人が非営利目的でオンラインプラットフォーム上で転売する行為が、95 条(a)（3）違反として認められた事案。本件では、営利目的を有していない販売広告も 95 条（a）（3）は禁止していると判断した。

（３）BGH, 27.11.2014 - I ZR 124/11, GRUR 2015, 672 - Nintendo II

任天堂が製造･販売する DS のコンソールの技術的手段が 95(a)の効果的な技術的手段といえるのかが争点となった。ドイツ連邦裁判所は、「コンピュータ・プログラムおよび他の著作物で保護された著作物から構成されるビデオゲームを保護するための有効な技術的手段は、著作権法 95 条(a)に基づいて保護される」「著作権法 95 条 2 項にいう、ビデオゲームを保護するための有効な技術的措置は、ビデオゲームが保存されたカードとビデオゲームが再生されるゲー

[165] LG Munchen I, 7 March 2005, 21 O 3220/05; 2005 年 7 月にミュンヘン最高裁判所によって支持された。 ZUM 2005/12, pp.896-901

[166] 前掲注 74 Westcamp, at 237-238 は、95 条 a(2)が（創設的な）法定責任ではなく、ドイツ法上の不法行為と理解され、ドイツ法上不法行為に適用される disturbance liability（妨害責任：不法行為の幇助責任に類したものと思われる）法理によって、出版社が回避プログラムの存在を報じるためにそのソフトウェアが置かれた URL を付しただけの行為に責任が認められており、この判示を前提とすると、95 条 a(2)の明文規定の内容を超え、周辺に位置する活動が規制の対象となる余地を指摘する。

[167] LG Koln, Urteil v. 23.11.2005 - Az: 28 S 6/05(2006)

ム機とがその寸法で互いに調整され、そのカードに保存されたビデオゲームだけをそのゲーム機で再生することができ、資格のない多様なビデオゲームをそのゲーム機で再生することが阻止されるということで成立し得る（鍵・鍵穴の原理）」、「著作権法 95 条(a)第 2 項にいう効果的な技術的手段は、著作権法 95 条(a)に基づき、その供用が比例原則を維持し、合法的供用機会が過度に制限されない場合にのみ保護される」、「著作権法 95 条(a)第 3 項 3 号にいう仕掛けが、『主に』その有効な技術的措置を可能にするという目的のために設計又は製作されたかを判断する際、実際の供用において示される客観的な目的の確定が重要になる」等と判示した。
その内容は、第Ⅳ章２．４．２で紹介した CJEU 判決の内容に沿ったものである。

３．３　最新動向

上記裁判例のほか、近時特に目立った動きはなく、DRM をめぐる議論は、現在ではホットな論点ではなくなっている。

４　フランス

フランス法は、情報社会指令 6 条を 331 条-5 条以下で国内法に導入している。ソフトウェアをその対象から外しているのは、英独と同様である。技術的手段の保護範囲としては、回避行為そのものを禁止する点は英独と同様であるが、私人の自由を確保する種子から、刑罰が科される対象を装置等を利用しない場合という極めて例外的な場合（一般人は、流通する回避装置を利用するのが通常である）に限定している点は特筆すべき点である。

また、回避禁止の例外については、技術的手段規制機関を設けて、技術的手段が過度に又は広汎にわたり、他の利益を害していないかを当該機関が監視する義務があるという点や、互換性の達成について合理的を認め、当該機関への申し出を条件に互換性達成に必要な情報が取得できる旨を定めている点は他国にない特徴である。

なお、フランスは、英国と異なり、条件付アクセス指令の国内法化を著作権法の中に取り込まず、視聴覚法（Audiovisual Law of 1986）を改正する形で導入した[168]。この法律は刑法として分類され、禁止行為（例えば、欺もう的な手段で有料放送を受信するための装置・機器の製造、輸入・販売・保管・設置等）を定め、禁止違反に対し 30,490 ユーロ以下及び 2 年以下の懲役が科されるものとされる。

４．１　法制度

（1） 現行法

情報社会指令 6 条を著作権法(CPI) 331 - 5 条ないし 331 - 10 条で国内法に導入している[169]。

> 第 331 の 5 条　著作物（ソフトウェアを除く。）の著作権者又は実演、レコード、ビデオグラム若しくは番組の著作隣接権者が許諾していない供用を防止すること、又は制限することに当てられる有効な技術的手段は、この章に規定する条件に従って保護される[170]。
>
> 2　第 1 項に規定する技術的手段とは、機能の働きの通常の範囲内においてこの項に規定する機能を遂行するいずれの科学技術、装置及び構成部品をもいう。これらの技術的手段は、アクセス・コードの適用、暗号化、受信妨害その他保護対象のいずれの変換のような保護の方式の適用、又はこの保護の目的を達成する複製物の管理の仕組みの適用のおかげで、同項にいう供用が権利者によって管理される場合には、有効であるとみなされる。
>
> 3　プロトコル、フォーマット又は暗号化、受信妨害若しくは変換の方式は、それ自体としては、この条に規定する技術的手段を構成しない。

168 Article 268 Law No. 92-1336 of 16 December 1992
169 日本語翻訳については、CRIC の翻訳による。
170 342 -3 は、データベースの権利に関する技術的手段の保護を規定する。

4　技術的手段は、著作権の尊重のために、相互運用の有効な活用を妨げる効果を持ってはならない。技術的手段の提供者は、第 331 の 6 条及び第 331 の 7 条に定める条件に従って、相互運用に不可欠な情報へのアクセスを許す。

5　この節の規定は、伝達の自由に関する 1986 年 9 月 30 日の法律第８６-１０６７号第７９の１条から第７９の６条まで及び第９５条に起因する法的保護を再び問題にしない。

6　技術的手段は、この法典に規定する権利及び権利の保持者が与える権利の限度内における著作物又は保護対象の自由供用を妨げることはできない。

7　この条の規定は、この法典第１２２の６の１条の規定を害することなく、適用される。

第 331 の 6 条　第 331 の 17 条にいう技術的手段規制機関は、第 331 の 5 条にいう技術的手段が、それらの相互の互換性がないこと又はそれらの相互運用ができないことを理由として、著作物（ソフトウェアを除く。）の著作権者又は実演、レコード、ビデオグラム若しくは番組の隣接権者によって明示的に決定される制限の補足的及び独立的制限を著作物の供用に持ち込むという結果をもたらさないように監視する。

第 331 の 7 条　ソフトウェアのいずれの出版者、技術システムのいずれの製造者及び役務のいずれの利用者も、相互運用に不可欠な情報へのアクセスが拒否される場合には、技術的手段規制機関に対して、当事者の権利を尊重しつつ、現存のシステム及び役務の相互運用を保証すること、並びにこの相互運用に不可欠な情報を技術的手段の権利者から入手することを、要求することができる。この申立てから起算して 2 か月の期間を利用して、同機関は、その決定を行う。

2　相互運用に不可欠な情報とは、初めに定義された著作物又は保護対象の供用条件を尊重しつつ、技術的手段によって著作物又は保護対象にアクセスすること（数値経済に対する信頼に関する 2004 年 6 月 21 日の法律第 2004-575 号第 4 条に規定する開かれた基準における場合を含む。）、及び結合した電子形式の情報にアクセスすることを、技術装置に可能とさせるために必要な技術的ドキュメンテーション及びプログラミングのインターフェイスをいう。

3　技術的手段の権利者は、その独立した、かつ相互運用するソフトウェアのソースコード及び技術的ドキュメンテーションの公表が、前記の技術的手段の安全及び効率に重大な損害を与える結果になるという証拠を提出しない限り、その公表を中止することを受益者に強制することはできない。

4　同機関は、当事者が提案する約束であって、相互運用に反する慣行を終らせることができる性質のものを受諾することができる。当事者間に合意がない場合には、同機関は、利害関係者がその意見を述べることができるようにした後に、請求の却下の理由を付した決定を行い、又は請求者が相互運用に不可欠な情報にアクセスすることができる条件、技術的手段の効率及び同一性を保証するために請求者が尊重しなければならない約束、並びにアクセス及び保護内容の供用の条件を、必要の場合には科料を課すことを条件として、指示する差止命令を発する。同機関が言い渡した科料は、同機関によって確定される。

5　同機関は、その差止命令の不履行の場合又は同機関が受諾した約束の不尊重の場合に適用される金銭的制裁を科する権限を有する。各金銭的制裁は、利害関係者に与えた損害の大きさ、制裁された団体又は企業の事情、及び相互運用に反する慣行のありうる反復に対応する。各制裁は、個別に、かつ理由を付して決定される。その最高額は、企業の場合には相互運用に反する慣行が実施されていた会計年度の前年度以来閉鎖されている会計年度中に取得した最高の税外世界売上げの額の5%とし、その他の場合には1万5,000ユーロとする。

6　同機関の決定は、法律によって保護される秘密を尊重しつつ、公表される。それらの決定は、当事者に通告される。当事者は、パリ控訴院に上訴を提起することができる。上訴は、執行停止の効力を有する。

7　技術的手段規制機関総裁は、支配的立場の濫用について、及び競争の自由行使を妨害する慣行であって、技術的手段の分野において知ることができるものについての審議を競合審議会に付託する。この審議付託は、緊急の手続の範囲内において、商事法典第464の1条に規定する条件に従って提出することができる。同機関総裁は、また、その権限に属するいずれの問題をも、意見を求めるために、同審議会に付託することができる。競合審議会は、競合の管轄範囲に入るいずれの審議付託をも同機関に伝達し、及びこの法典第331の5条にいう技術的手段の分野において審議付託された慣行についての意見を収集する。

第331の8条　私的複製のための例外及びこの条にいう例外の特権は、この条及び第331の9条から第331の16条までの規定によって保証される。

2　第331の17条にいう技術的手段規制機関は、保護の技術的手段の活用が、次の各号に定める例外を受益者から奪う結果とならないよう監視する。

(1)第 122 の 5 条第 2 号及び第 3 号(e)（2007 年 1 月 1 日以後）並びに同条第 7 号及び第 8 号

(2)第 211 の 3 条第 2 号及び第 3 号最終段（2009 年 1 月 1 日以後）並びに同条第 6 号及び第 7 号

(3)第 342 の 3 条第 3 号及び第 4 号（2009 年 1 月 1 日以後）

3　第 331 の 9 条から第 331 の 16 条までに従うことを条件として、同機関は、前記の例外の行使の条件を決定し、及び特に私的複製のための例外の範囲内で許される複製の最小限の数量を、著作物又は保護対象の種類、公衆への伝達の各種の方法、及び利用できる保護技術によって提供される可能性に応じて、決定する。

第 331 の 9 条　第 331 の 5 条に定める保護の技術的手段に頼る権利者は、複製物の部数を制限する目的のためにそれらの手段を当てることができる。ただし、それらの者は、それらの手段の活用が、第 331 の 8 条にいう例外の受益者からそれらの手段の有効な行使を奪わないために、有用な措置をとる。それらの者は、消費者の公認団体その他の関係当事者との協議でそれらの手段を定めるよう努力する。

2　この条の規定は、技術がそれを可能とする限度において、それらの例外の有効な特権を著作物又はレコード、ビデオグラム若しくは番組への適法なアクセスに従わせることができ、かつ、通常の利用を害し、又は著作物若しくは保護対象の権利者の正当な利益に不当な損害を与えるような効果を持たないように監視することができる。

第 331 の 10 条　著作物又は隣接権による他の保護対象が、当事者間で締結される契約条項に従って、各人が選択する場所から、及び各人が選択する時にアクセスすることができるように公衆の利用に供される場合には、権利者は、第 331 の 9 条の規定を採用する義務を負わない。

（2）回避行為 (335－3－I)

第３３５の３の１条　I　コード解読、暗号解読、その他保護若しくは管理の仕組みを迂回し、無効にし、又は除去することを目的とするいずれかの個人的介入によって著作物の保護を改悪させるために、第３３１の５条に定めるような有効な技術的手段に対して、研究以外の目的で、承知の上で損害を与える行為は、この損害が、II にいう技術の応用、装置又は現存の構成部品の供用以外の手段によって実現される場合には、３，７５０ユーロの罰金に処せられる。

ここで重要なのは、回避が違法として罰せられる（3750 ユーロの罰金）のが、回避のための装置を利用せず実行している場合に限られ、回避それ自体が違法になるケースが非常に絞られていることである。この点は情報社会指令 6 条 1 項の文言と比較すると、特徴的である。これ

は、（多くは回避装置を利用しなければ回避できない）私人を規制の対象からはずし、専門業者のみを規制する趣旨である。

（３）回避装置等の取引行為（335-3-II）

３３５条の３ II　第３３１の５条に定めるような有効な技術的手段に対して、次の各号に掲げる方式の一によって損害を与えるために考えられ、又は特別に適応された手段を、承知の上で直接的又は間接的に他人に得させ、又は提案する行為は、６か月の禁錮及び３万ユーロの罰金に処せられる。 直接的又は間接的に他人に得させ、又は提案する行為は、６か月の禁錮及び３万ユーロの罰金に処せられる。 (1) 技術の応用、装置又は構成部品を、研究以外の目的で、製造し、又は輸入すること。 (2) 販売、貸与若しくは賃貸のために保持し、それらと同一の目的のために提供し、又は技術の応用、装置若しくは構成部品をなんらかの形式で公衆の利用に供すること。 (3) この目的のために役務を提供すること。 (4) 前記（１）から（３）までに掲げる方式の一の供用を扇動し、又はそのための宣伝を指揮し、構想し、組織し、複製し、頒布し、又は普及させること。

有効な技術的手段を損なうために設計又は特別に改造された回避装置等を第三者に対し、有効な技術的手段を(i) 研究以外の目的で製造又は輸入する、(ii) 販売または貸与の目的で所持、提供、又は公衆に提供する、(iii) 回避する目的でサービスを提供する、(iv) 回避装置等の利用を促し、広告宣伝をする、ことにより、効果的な技術的手段を損なう目的で設計された手段を直接的または間接的に第三者に故意に提供する行為を規制する。これらの取引行為を行った者は、6 か月以内の懲役及び 30,000 ユーロの罰金に処せられる。ただし、コンピュータセキュリティ上の理由からそのような取引を行った者には適用が除外される（335-3-3）。上記のとおり、対象となる回避装置が情報社会指令 6 条 2 項よりも制限的になっている。

（４）制限・例外規定

331 条の 5 第 6 号は、「技術的手段は、この法典に規定する権利及び権利の保持者が与える権利の限度内における著作物又は保護対象の自由供用を妨げることはできない」として権利制限の範囲内での例外を明確にしている。技術的手段規制機関（Authority of Regulation of Technological Measures）が創設され、回避禁止の例外該当性について判断する権限が与えられる。ただし、この機関により例外の回避が判断された事例は現在確認されていない。

４．２　主要判例

（１）Nintendo v. Divineo[171]

任天堂が、Modchips に類似する（偽造ゲームを任天堂のコンソール上で実行可能にする）ツール（日本の事件で言う「マジコン」）の販売の差止を求めた事案において、第一審裁判所は、第 331 の 7 条「ソフトウェアのいずれの出版者、技術システムのいずれの製造者及び役務のいずれの利用者も、相互運用に不可欠な情報へのアクセスが拒否される場合には、技術的手段規制機関に対して、当事者の権利を尊重しつつ、現存のシステム及び役務の相互運用を保証すること、並びにこの相互運用に不可欠な情報を技術的手段の権利者から入手することを要求することができる。この申立てから起算して 2 か月の期間を利用して、同機関は、その決定を行う。」との規定を、技術的手段が互換性を妨害してはならないことを示唆するものと解し、任天堂のコンソール上で他のゲームを行えるようにして互換性を実現する（任天堂が施した技術的手段を回避する）チップは著作権法によって禁止されていないとし、任天堂の請求を退けた。

（２）Nintendo c. Absolute Games & Divineo[172]

331 条の 7 が互換性のための回避を許容しているという上記（1）判決の判断を覆し、以下のように判示した。

「知的財産権法典 L. 331-5 条が以下のとおり定めている点を考慮する。著作権を尊重するために、技術的手段は、相互運用の有効活用を妨げる効果を有してはならない。技術的手段の提供者は、第 331-6 条および第 331-7 条に定める条件に従って、相互運用に不可欠な情報へのアクセスを許可する。さらに、これら 2 つの条項（2009 年 10 月 28 日の法律により、それぞれ L. 331-31 条および L. 331-32 条となった。）の趣旨において、上記の行為に適用される記述を考慮する。

『技術的手段の規制機関は、L. 331-5 条にいう技術的手段に互換性または相互運用性がないことを根拠として、ソフトウェアを除く著作物の著作権者または実演、レコード、ビデオグラムもしくは番組の隣接権者によって明示的に決定される制限の補足的制限が著作物の供用に課せられるという結果にならないように留意する。』

ソフトウェアの製作販売者、技術システムの製造者およびサービスの利用者は、相互運用に不可欠な情報へのアクセスを拒否された場合には、当事者の権利を尊重しつつ現存のシステムとサービスの相互運用を保証すべき旨および相互運用に不可欠な情報を技術的手段の権利者か

171 TGI Paris, December 3, 2009, Nintendo v. Divineo, available at http://juriscom.net/2009/12/tgi-paris-3-decembre-2009-nintendo-c-sarl-divineo-et-autres/.

172 CA Paris, September 26, 2011 Nintendo c. Absolute Games & Divineo, available at www.legalis.net/spip.php?page=jurisprudence-decision&id_article=3238.

ら入手すべき旨を、高等機関に対して請求することができる。請求を受けた高等機関は、その日から起算して 2 カ月以内に、当該請求に応じるか否かを決定する。これらの本文に基づき、『Hadopi（インターネットにおける著作普及および権利保護のための高等機関）』（「AMRT」を前身とする唯一の担当独立行政機関）は、ソフトウェアの製作販売者、技術システムの製造者またはサービスの利用者の請求に応じ、技術的手段の権利者から当該請求者にシステムの相互運用を保証しうる情報を伝達させるべきか否かを決定する。

本事案においては、いずれの被告も Hadopi において手続をしたことを証明しておらず、したがって、いずれの被告も自己の防禦を目的としてシステムの相互運用の除外を援用することができないという点を考慮する。」

331 条の 7 は、あくまでも技術的手段規制機関に対する申立てその他の要件を充足する限りにおいて互換性の実現が保護されるに過ぎないとし、かかる手続を経ない被告の技術的手段の回避は、被告の製品は、任天堂が施した技術的手段を回避することだけを意図した Modchips であるとした。

４．３　最新動向

上記裁判例のほか、近時特に目立った動きはなく、DRM をめぐる議論についてアップデートすべきものはないように思われる。

第Ⅶ章　各国規制の比較

１　各国における技術的手段

国	保護される技術	著作権侵害との明示的な関連性	回避・無効化行為	回避･無効化のための装置等
米国	アクセス制限技術	なし※1	禁止 (§1201 (a) (1))	禁止 (§1201 (a) (2))
	コピー等利用制限技術	あり	禁止されない	禁止 (§1201 (b))
日本	アクセス制限技術	なし※2	一部禁止 （著作権法 30 条 2 号、120 条の 2 第 2 号）	禁止 (不競法、著作権法 120 条の 2 第 1 号)
	コピー等利用制限技術	なし※2	一部禁止 （著作権法 30 条 2 号、120 条の 2 第 2 号）	禁止 (不競法、著作権法 120 条の 2 第 1 号)
EU	アクセス制限技術	なし	禁止 (情報社会指令 6 条 (1))	禁止 (情報社会指令 6 条(2))
	コピー等利用制限技術	あり	禁止(情報社会指令 6 条 (1))	禁止 (情報社会指令 66 条(2))

※1　米国では、条文の文言上は著作権侵害との関連性は求められていないが、裁判例でその解釈が分かれる。

※2　日本では、不正競争防止法では著作権侵害との関連性は問わないが、一方、著作権法では、保護対象となる技術的手段は、著作権等の侵害行為を防止又は抑止するものに限られる。

上記表は、WIPO 条約等で求められる「技術的手段に対する保護」について、米国、日本、EU における法規制態様の相違を一覧表にまとめたものである。

米国では、デジタルミレニアム著作権法（1201 条）に基づき、著作物に対するアクセス制限技術（1201(a)）と著作物に対する著作権法上の権利侵害を防止するコピー等利用制限技術）1201(b)）の規定を設けている。著作権に対する規制として規定されているため、ともに著作物を対象とするものである。

米国内で解釈上争いがあるのは、1201(a)のアクセス制限技術としての保護は、当該技術的手段が著作権侵害と一定の関連性を有することが必要か（第Ⅵ章 1.2（8)裁判例など)、又は、単に著作物へのアクセスに条件を付してコントロールするだけか（同（23）裁判例）とい

う点である。控訴審レベルで解釈が分かれたままとなっている。

他方、第Ⅳ章 1・3 で言及した 3 年ごとに著作権局の推奨に基づきコントロールの例外を認める規定に基づく規則制定手続には、通常、利害関係人から例外を認める要請が数多く出され、非常に積極的に利用されている。規則制定手続開始後、認められる例外は前記のとおり増え、例えば、2014 年の規則制定手続では、44 件の新たな例外を要望する申立て（petition）がなされ、その後、著作権局による暫定提案に対する 40,000 件のコメント、2015 年に 2 度の公開ヒアリング（ロサンゼルスとワシントンで合計 7 日間）が実施されるなど、新たな例外について一般に関心が高く、多くの利害関係人の意見が反映されて著作権局の推奨が行われている[173]。

また、前述のとおり、2015 年 12 月 29 日、米著作権局は 1201 条の技術的手段の保護規制についてパブリックコメントを求め、その問題点の検討（Section 1201 Study）に着手しており[174]、ヨーロッパとは様相が異なっている。

日本は、WIPO 条約に対応して平成 11（1999）年に著作権法を改正し、技術的手段の回避に係る規制を新設した。これにより、技術的手段を回避した上での私的複製を違法とするとともに（民事措置のみ）、専ら技術的手段を回避することを機能とする装置等の製造・譲渡・貸与等に対して刑事罰を規定した。しかし、平成 11 年改正においては、著作権法上で保護対象とする技術的手段は、いわゆる非暗号型技術によるもののみであった[175]。これは、改正当時、音楽やビデオソフト等のコンテンツに用いられていた技術的手段は、無断複製の防止を目的とした技術が多く、SCMS や CGMS 等の非暗号型技術により主に実現されていたためであると考えられる[176] [177]。

他方、主にアクセス制限を目的として用いられる、いわゆる暗号型技術による技術的手段については、平成 11（1999）年の不正競争防止法改正により、技術的制限手段を回避・無効化する装置等の提供行為を不正競争行為と位置づけることで対応した。不正競争行為を規制するものであることから、条文上も対象を著作物に限定していない。コピー等制限技術として主に用いられる非暗号型技術については著作権法と不正競争防止法のいずれにおいても規制対象

---

173 前掲注 60、at 9-11

174 2016 年 3 月 4 日で一次のコメント募集が打ち切られたが、オンライン上では少なくとも 68 件の利害関係者からのコメントが確認できる。http://www.regulations.gov/#!docketDetail;D=COLC-2015-0012

175 平成 11 年改正当時の「技術的保護手段」の定義

「二十　技術的保護手段　電子的方法、磁気的方法その他の人の知覚によって認識することができない方法（次号において「電磁的方法」という。）により、第十七条第一項に規定する著作者人格権若しくは著作権又は第八十九条第六項に規定する著作隣接権（以下この号において「著作権等」という。）を侵害する行為の防止又は抑止（著作権等を侵害する行為の結果に著しい障害を生じさせることによる当該行為の抑止をいう。第三十条第一項第二号において同じ。）をする手段（著作権等を有する者の意思に基づくことなく用いられているものを除く。）であつて、著作物、実演、レコード、放送又は有線放送（次号において「著作物等」という。）の利用（著作者の同意を得ないで行ったとしたならば著作者人格権の侵害となるべき行為を含む。）に際しこれに用いられる機器が特定の反応をする信号を著作物、実演、レコード又は放送若しくは有線放送に係る音若しくは影像とともに記録媒体に記録し、又は送信する方式によるものをいう。」

176 著作権法令研究会・通商産業省知的財産政策室著「著作権法不正競争防止法改正解説（デジタル・コンテンツの法的保護）」（1999 年 12 月発行　有斐閣）

177その後、平成 24 年改正において「送信する方式又は当該機器が特定の変換を必要とするよう著作物、実演、レコード若しくは放送若しくは有線放送に係る音若しくは影像を変換して記録媒体に記録し、若しくは送信する方式」が追加され、暗号型の保護技術を対象に加えた。暗号型の保護技術について、「アクセスコントロール機能とコピーコントロール機能が一体化したもの」（平成 23 年 1 月文化審議会著作権分科会報告書）との評価によるものである。

とし、著作権法で担保されない暗号型技術については不正競争防止法で規制するという枠組を採用した[178]。

EU では、前述のとおり、各国の利害調整の難しさを原因として、情報社会指令 6 条が定める技術的手段の保護が抽象的に定められた結果、アクセス制限技術とコピー等利用制限技術双方について法的な保護を与えることが定められ、かつ、条文の文言上は、著作権侵害回避との関連性が求められていない。そのため、純粋なアクセス制限技術を保護するか否かは各国の裁量に委ねられ、前章でみたような裁判例が生じている。

[178] 平成 24 年著作権法改正で暗号型の保護技術が対象に加えられ、一定のアクセスコントロールが著作権法上の技術的保護手段として保護の対象に加えられたが、著作権保護と一切関係のないアクセスコントロールは依然として保護の対象外と認識されている。

2　各国における個別行為の規制状況

上述の法の枠組を前提として、規制対象行為の細部を各国の法律上の文言及び裁判例に基づき整理したのが以下の表である。

	日本	アメリカ	イギリス	ドイツ	フランス
私人の回避・無効化行為	△（回避により可能となる私的供用目的の複製に限る）	△（ただし、アクセス制限技術に限る）	○（コンピュータ・プログラムを除く）	○（コンピュータ・プログラムを除く）	△（回避装置を利用しない場合のみ罰金の対象とする[335 条3の1]）（コンピュータ・プログラムを除く）
業（サービス）として行う回避行為	○著作権法	△（ただし、アクセス制限技術に限る）	○（コンピュータ・プログラムを除く）	○（コンピュータ・プログラムを除く）	△ 同上
回避装置・プログラムの提供行為（引渡・展示・輸出・譲渡・輸入）　**（※1）**	○不競法	○	○	○	○
回避プログラムの送信	○不競法 ○著作権法	○	○	○	○
回避プログラムの送信可能化	○著作権法	○	○	○	○
回避装置・プログラムの貸与	○不競法 ○著作権法	○	○	○	○
回避装置・プログラムの譲渡貸与目的の製造	○著作権法	○	○	○	○
回避装置・プログラムの譲渡貸与目的所時	○著作権法	○	○	○	○
回避装置・プログラムの供用供与	○著作権法	○	○	○	○
回避プログラムが置かれたURLの提供	× **（※2）**	○（第VI章 1.2（2）裁判例）	○（コンピュータ・プログラムに限る。[回避プログラムが置かれている場所を明示するものなので、296 条 1 項「技術的措置を除去又は回避することを可能に又は容易にさせる意図を持って情報を公開する場合」に該当すると考えられる）	○（第 VI 章 3.2（1）裁判例）	○（335 条の3 II の（3）、回避装置の供用を「宣伝を指揮し、構想し、組織し、複製し、頒布し、又は普及すること」に該当する余地があると考えられる。）

	日本	アメリカ	イギリス	ドイツ	フランス
回避装置・プログラムの製造方法に関する情報提供	×	×	△（コンピュータ・プログラムに限り、○となる可能性がある。［情報の正確性・確実性等、その内容次第では、296 条 1 項「技術的措置を除去又は回避することを可能に又は容易にさせる意図を持って情報を公開する場合」に該当する余地がある］）	△（販売又は貸与のための広告として○となる可能性がある）	△（335 条の 2（3）（4）において、「役務」「宣伝」と解釈される可能性がある）
認証キー（プロダクトキー等）のみの譲渡等	△（ID・パスワードの場合は不正アクセス禁止法により○となる可能性がある）	×	×	×	×
回避システムに入力されるデータのみの譲渡等	×	×	△（コンピュータ・プログラムに限り、○となる可能性がある。［296 条 1 項「技術的措置を除去又は回避することを可能に又は容易にさせる意図を持って情報を公開する場合」に該当する余地がある］）	×	△（335 条の 2（3）（4）において、「役務」「宣伝」と解釈される可能性がある）
回避により可能となる私的供用目的の複製	○著作権法	×	○（私的複製が許容されていない）	×（95b(1)6)）ただし、デジタル複製には権利制限が及ばない	○

（※1）日本以外は、「輸出」を規制対象として明記していないが、特段、各国が「輸出」を規制対象から除外する趣旨は確認できない。「その他流通させる行為」（米）、「販売、頒布行為」（英、独）、「販売、提供行為」（仏）として規制されると考えられる。

（※２）たとえば、平成 27 年 9 月 8 日神戸地裁判決（平成 27 年（わ）第 161 号、第 218 号、第 467 号）は、被告人行為は URL の情報提供にすぎないという弁護人の主張に対して、「URL の提供行為に留まらず、自ら認証回避プログラムを自分が供用する登録名に割り当てられ

た記憶領域に記憶・蔵置させ、これを他のインターネット利用者が閲覧、取得できるように設定している」と指摘し、これらを「一連の行為」と評価し、情報ないしノウハウの提供にとどまらず、プログラムの「提供」に該当すると判示している。同判決（その他の類似裁判例）は、URL の提供のみでは不正競争防止法上の「提供」には当たらないと解釈するものと理解できる。