IP マネジメントレビュー13 号 4 頁（2014.6）

特別寄稿

# 著作権法によるコンテンツ・セキュリティの保護
## ～「複製利用モデル」から「アクセス利用モデル」へ～

インフォテック法律事務所 弁護士・ニューヨーク州弁護士
山本 隆司

## １．はじめに

クラウド・ビジネスの成功には、著作権による適切な保護が不可欠です。

著作権法は、著作物の創作活動に直接従事する創作者（「著作者」）に、著作物利用に対する独占的権利（「著作権」）を与えて、著作物の創作活動を促進する制度です。

著作権は、著作物の利用行為（鑑賞行為）に対する独占権であり、著作権者はこれに課金することによって著作物創作の対価回収・利益収得を行います。しかし、かつては、著作物の利用行為（鑑賞行為）それ自体に権利を及ぼしても、それを外部から認識する技術（コントロールを及ぼす技術）がありませんでした。その結果、著作物の利用行為（鑑賞行為）の前段階において、著作物の利用行為（鑑賞行為）のために必要とされる複製物の作成（有形複製）や見せ聞かせる行為（無形複製）に権利を及ぼしていました（「複製利用モデル」）。

ところが、いまではデジタル化の進歩により、著作物の利用行為（鑑賞行為）＝再生行為・視聴行為に対して直接コントロールを及ぼすことが技術的に可能になりました。また、複製を伴わない著作物の利用行為（鑑賞行為）が登場しています。したがって、デジタル環境においては、著作物の利用行為（鑑賞行為）それ自体にまで著作権を及ぼす必要が生じています（「アクセス利用モデル」）。そして、これを技術的に可能にするコンテンツ・セキュリティ技術に対する著作権の保護が、現在、課題となっています。

本稿では、コンテンツ・セキュリティ技術の態様とこれに対する著作権保護の国際動向をご紹介したいと思います。

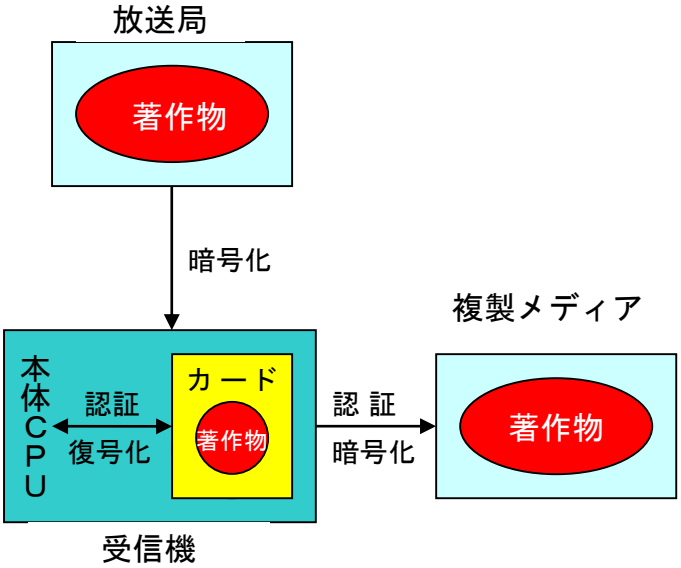
## ２．放送コンテンツのセキュリティ技術

放送におけるコンテンツ・セキュリティには、地デジ放送で用いられる地上 RMP 方式、衛星放送で用いられる B-CAS 方式、ケーブル放送で用いられる C-CAS 方式があります。

たとえば、B-CAS 方式においては、コンテンツを暗号化して放送し、B-CAS カードに暗号解読情報を持たせます。B-CAS カードは、CPU を組み込んでおり、それ自体が一つのコンピュータです。受信機に装着された B-CAS カードは、装

©2014 Takashi B. Yamamoto

着された受信機が規格（ARIB の STD-B25 や TR-B15 など）に準拠する受信機か否かを判別し、非準拠の受信機との接続を拒否します。放送コンテンツを受信し再生する機器を製造販売しようとするメーカーは、また、規格に準拠することで、B-CAS 社からライセンスを受け、B-CAS カードの提供を受けることができます。当該規格は、受信機器に対する、複製制御と外部出力制限を義務づけています。



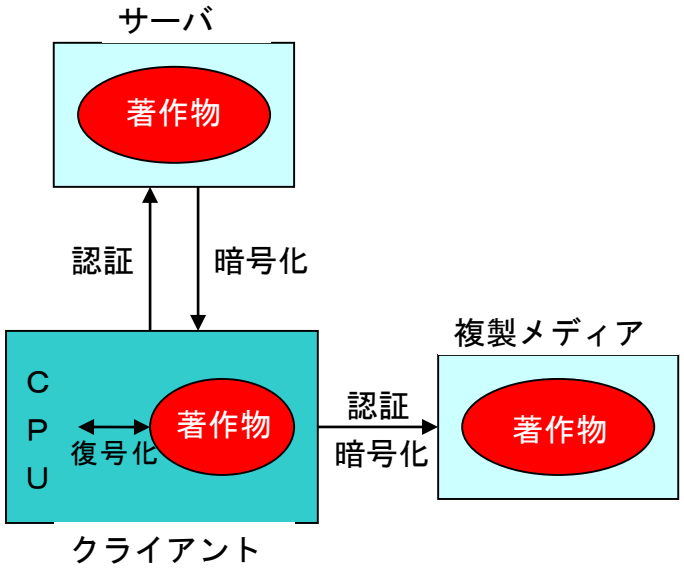

その結果、規格準拠の受信機器は、B-CAS カードと相互認証（アクセス・コントロール）して復号情報を取り込み、暗号化された放送コンテンツを復号化（アクセス・コントロール）して再生します。また、ダビング１０などのコピー制御信号に従って規格準拠の複製メディアに複製することが可能です（コピー・コントロール）。他方、規格に準拠しない受信機器は、複製制御や出力制限の義務づけを受けませんが、B-CAS カードを利用できないので暗号化された放送コンテンツを復号化することができません。

ここで用いられるコンテンツ・セキュリティは、認証と暗号化と複製制御信号です。現行著作権法は、従来より保護していた複製制御信号に加えて、2012 年の改正で暗号化をも保護するようになりましたが、未だに認証を保護していません。

## ３．ダウンロード・コンテンツのセキュリティ技術

ダウンロード・コンテンツのセキュリティ技術の代表例は、FairPlay です。FairPlay は、アップルが iTunes Store で音楽配信に利用するシステムです。利用者は、パソコンにインストールした音楽プレーヤ iTunes で、音楽ファイルを購

入し、これをパソコンで再生し、また iPod などに複製して視聴できます。




利用者は、まず、そのパソコンにクライアント・ソフトである iTunes をインストールすることが必要です。iTunes で利用者が登録されると、アップルのサーバは利用者ごとにユーザ鍵を作成し、これを当該利用者に送ります。当該利用者の iTunes は、その作成する鍵データベースにユーザ鍵を登録します。

コンテンツのダウンロードを求めて、利用者が配信サーバにアクセスすると、配信サーバは、利用者のソフトが iTunes であるかを認証し（アクセス・コントロール）、配信サーバはコンテンツのダウンロードを許します。配信サーバは、ダウンロードされるコンテンツをマスタ鍵で暗号化し（アクセス・コントロール）、またマスタ鍵をユーザ鍵で暗号化して、利用者に送信します。利用者の iTunes は、まず保有するユーザ鍵でマスタ鍵を復号化し、さらにその復号化したマスタ鍵でコンテンツを復号化するという二段階の手順（アクセス・コントロール）を踏んで、コンテンツを視聴できる状態にします。

また、iTunes は、所定の許容された複製以外の複製を禁止する機能を持っていて、所定の許容された複製以外の複製を許しません（コピー・コントロール）。

ここで用いられるコンテンツ・セキュリティは、認証と暗号化と複製制御信号です。現行著作権法は、複製制御信号と暗号化を保護しますが、認証を保護しません。

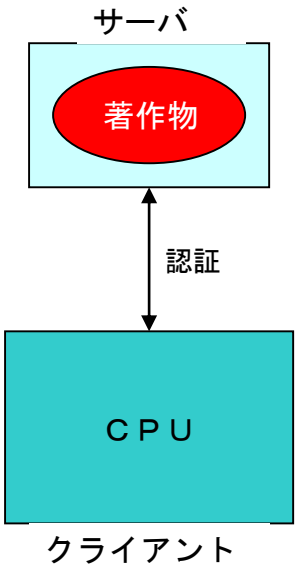
## ４．アクセス利用コンテンツのセキュリティ技術

クラウド・サービスの本質的特徴は、利用者が従来パソコンに持たせていた機能（データ処理とデータ蓄積）のすべてをインターネット上のサーバに移し、利

用者の利用機器は操作端末の機能さえあれば足りる、という情報処理環境にあります。これを利用したコンテンツ提供のクラウド・サービスのなかでもその最たるものが、ここで紹介するアクセス利用型サーバ・コンテンツの提供サービスです。

たとえば、オンライン会計処理サービスにおいては、利用者は、料金を払い、インターネット経由で業者のサーバに接続して、サーバ上の会計処理プログラムを利用します。

アクセス利用型サーバ・コンテンツの提供サービスにおいては、通常、サーバ・ソフトとクライアント・ソフトの 2 種類のプログラムが利用されます。サーバ・ソフトが会計処理プログラムです。他方、クライアント・ソフトは、データ入力と出力表示のユーザ・インタフェースを提供し、利用者のパソコンを入力端末として機能させます。利用者が自己のパソコンにクライアント・ソフトをインストールし、サーバ・ソフトにアクセスすると、サーバ・ソフトはクライアント・ソフトを認証し、また利用者の利用権限を認証します（アクセス・コントロール）。




利用者は、パソコンからサーバ・ソフトに対する操作指示とサーバ・ソフトに処理させるデータを入力します。サーバ・ソフトは、当該操作指示に従ってデータを処理し、処理後のデータをパソコンに出力します。クライアント・ソフトは、サーバ・ソフトから出力されたデータをそのユーザ・インタフェースに出力表示します。

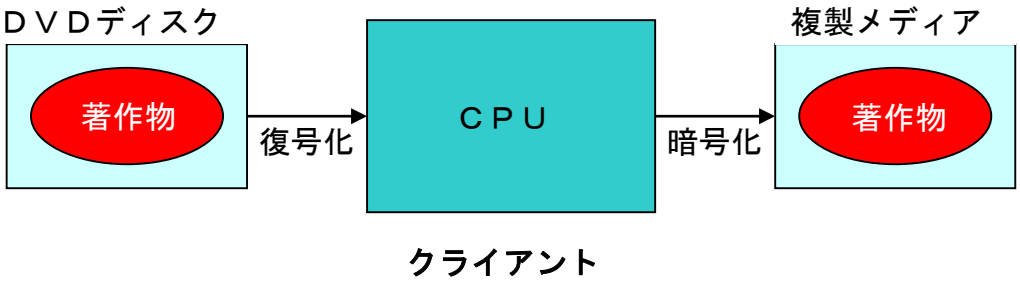
以上の処理においては、コンテンツはサーバに置かれたままであり、利用者のパソコンにダウンロードされることはありません。

©2014 Takashi B. Yamamoto

ここで用いられるコンテンツ・セキュリティは、認証のみです。しかし、現行著作権法は、認証を保護しません。

５．パッケージ・コンテンツのセキュリティ技術

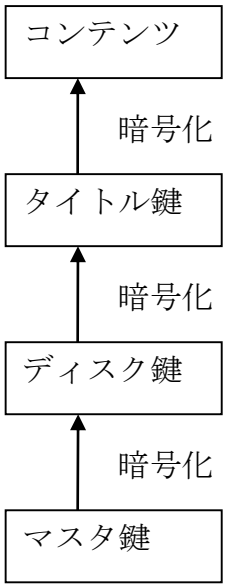
パッケージ･コンテンツのセキュリティ技術の代表例は､CSS（Content Scramble System）です。CSS は、DVD で使用されている権利管理システムです。CSS においては、DVD コンテンツを暗号化します（アクセス・コントロール）。規格準拠の再生機器のみが､暗号化されたコンテンツの復号鍵を与えられており､暗号化された映画コンテンツを復号し、視聴する状態にできます。他方、規格準拠の再生機器は、暗号化のほか、複製制御（コピー・コントロール）や出力制限など（リージョンコードの設定､マクロビジョンへの対応等）を義務づけられます。




DVD CCA（The DVD Copy Control Association）が配給会社や機器メーカーなどにその規格をライセンスしています。

DVD コンテンツは、コンテンツごとに設定されるタイトル鍵で暗号化されます（アクセス・コントロール）。タイトル鍵は、ディスクごとに設定されるディスク鍵で暗号化され､ディスク上のセクタヘッダ領域に記録されます。さらに、ディスク鍵は､マスタ鍵（規格準拠の再生機器を製造する機器メーカーごとに設定されるものです）で暗号化され､再生機器が通常､読むことのないディスク上のリードイン領域に記録されます。

規格準拠の再生機器は、機器内に秘密に保管されたマスタ鍵を使って、DVD ディスク上の暗号化されたディスク鍵を復号化します。つぎに､復号化されたディスク鍵を使って､暗号化されたタイトル鍵を復号化します。最後に､復号化されたタイトル鍵を使って､暗号化されたコンテンツを復号化し､コンテンツを視聴可能な状態にします。




規格に準拠しない再生機器は、複製制御や出力制限などの義務づけを受けていませんが、復号化に必要なマスタ鍵を与えられないので、暗号化された DVD の映画コンテンツを復号化することができません。

ここで用いられるコンテンツ・セキュリティは、暗号化と複製制御信号です。現行著作権法は、複製制御信号と暗号化を保護しています。

## ６．システム・コンテンツのセキュリティ技術

システム・コンテンツのセキュリティ技術には、たとえば、お試しソフトがあります。利用者は、お試しソフトを自己のパソコンにインストールし、一定期間これを無料で利用することができます。当該期間を越えて利用するには、すでにソフトウエア自体は PC に複製されていますが、コンテンツ・プロバイダから認証コードを購入して、これを利用してソフトの認証を受けることが必要になります。

ここで用いられるコンテンツ・セキュリティは、認証です。現行著作権法は、認証を保護していません。

## ７．コンテンツ・セキュリティに対する法的保護

コンテンツ・セキュリティは、著作権法においては「技術的保護手段」や「技術的手段」といわれています。日本の著作権法は、技術的保護手段を暗号化と複製制御信号に限って保護しています。しかも、暗号化は複製防止のために利用さ

れるものに限って保護しています（著作権法 2 条 1 項 20 号）ので、あくまでも複製利用モデルに踏みとどまっています。

なお、不正アクセス禁止法は、ネットワークで用いられる認証を保護しています。しかし、著作物の創作促進を目的とする制度ではなく、著作権法の代わりにはなりません。

他方、米国は、1998 年制定の DMCA によって著作権法を改正し、技術の種類を制限することなく、広くアクセス・コントロールとコピー・コントロールを保護しています（1201 条）。すなわち、アクセス・コントロールについては、回避行為自体を禁止するほか、回避装置等の製造販売等も禁止しています。また、コピー・コントロールについては、回避装置等の製造販売等を禁止しています（その回避行為自体は複製権などで規制されるので特段の禁止規定を置いていません）。したがって、暗号化も認証もアクセス・コントロールとして保護しています。また、欧州連合は、2001 年の情報社会指令において、加盟各国に対して、技術の種類を制限することなく、広くアクセス・コントロールとコピー・コントロールを保護することを義務づけています（6 条）。

以上のとおり、欧米では、認証を含めたアクセス・コントロールに対する法的保護（アクセス利用モデル）を定めており、クラウド・サービスで利用される著作物への保護体制を確立しています。

実は、著作物に対する技術的手段の保護は、1996 年締結の WIPO 著作権条約で各国に義務づけられたものです。この条約 11 条は、「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【技術的手段】」について、保護義務を課しています。WIPO 著作権条約の 8 条は、「公衆のそれぞれが選択する場所からかつ選択する時期における（from a place and at a time individually chosen by them）著作物へのアクセス」に公衆伝達権を及ぼしています。この中には、アクセス利用コンテンツの形態も含まれます。したがって、日本も、アクセス利用モデルに基づいて技術的手段を保護する条約上の義務を負うと考えられます。ところで、日本では、上記規定部分を「公衆のそれぞれが選択する場所及び時期において著作物の使用」と誤訳しているため、その中には、利用者の PC にコンテンツが送られてくるダウンロード利用コンテンツの形態しか公衆伝達権に含まれないと解釈しているのです。

## ８．おわりに

クラウド・ビジネスの成功には、著作権による適切な保護が不可欠です。しかし、以上のとおり、日本の著作権法は、この点で遅れています。すなわち、アクセス利用モデルに基づいて技術的手段を保護せず、複製利用モデルの枠を出ていないことと、技術の種類を限定している点において、クラウド・ビジネスで利

用される著作物への保護に欠けています。国際的なミニマムスタンダードを定めるだけの条約の水準にさえ達していません。

日本では、立法関係者は、この立ち後れに気がついていないようです。日本では一般的に法律家が技術に疎いことに、その原因があるのでしょうか。

著作権の発展を見ていると、メモリーへの一時的蓄積への対応、輸入権の創設、間接侵害に対する対応、そして、このコンテンツ・セキュリティの保護への対応についてはと、日本は世界をリードする国ではなく、先進国グループの一員でさえないように思えます。コンテンツ・セキュリティに対する適切な保護を怠ると、日本のクラウド・ビジネスは、現在のレコード・ビジネスのように、シュリンクしてしまうのではないか、と懸念されるところです。

以上

©2014 Takashi B. Yamamoto