

デジタル著作権管理技術の現状と今後の展開

デジタル社会のガバナンス 技術と社会の調和を目指して

曾根原 登 岡田 仁志 渡辺 克也

国立情報学研究所 〒101-8430 東京都千代田区一ツ橋 2-1-2

E-mail: {sonehara, okada, charley}@nii.ac.jp

あらまし e-Japan 戦略はデジタル社会の到来を加速した。デジタル社会の理想は、自由、平等、安全の確保と経済発展にある。それを実現するには、デジタルの利便性、効率性、自由度の向上と、著作権や個人情報保護、情報の信憑性・信頼性などの安全性、との調和が必要である。それには技術と市場メカニズムの関係のみならず、社会・文化、法制度を有機的に連動させることが不可欠である。本文は、デジタル著作権管理技術について分析し、デジタル革新を経済発展の原動力とするための、技術と社会の分野と専門を超えた連携施策をデジタル社会のガバナンスとして提案する。

キーワード e-Japan, ICT(Information and Communications Technologies), デジタル著作権管理, デジタル権利表明, コピキタス, ブロードバンド, 公共政策, 電子商取引, 情報信頼性, 情報信憑性, ICT ガバナンス

Analysis and Future of Digital Rights Management Technology

Governance of Digital Society: Toward the Harmonization of Technology and Society

Noboru Sonehara, Hitoshi Okada and Katsuya Watanabe

National Institute of Informatics 2-1-2 Hitotsubashi Chiyoda-ku, Tokyo, 101-8430 Japan

E-mail: {sonehara, okada, charley}@nii.ac.jp

Abstract e-Japan strategy has accelerated up realization of a digital society. The digital society ideals revolve around the highest principles of society, economic development, freedom, equality, and safety. To realize these ideals and make full use of digital technology convenience and efficiency, it is necessary to balance credibility and reliability with increased freedom and at the same time ensures the copyrighting and protecting of individual information. In this respect, it is important that technologies, market mechanisms, social norms and legislative systems should be fully synchronized. Analyzing digital rights management technology from the technology and market perspectives, we propose the governance of digital society for the new digital rights management system as a new style of cooperation beyond the present fields or specialties.

Keyword e-Japan, u-Japan, ICT (Information and Communications Technologies), Digital rights management (DRM), Digital rights expression (DRE), Ubiquitous, Broadband, Public policy, e-commerce, Information reliability, Information trust, ICT governance

1. はじめに

近年、ネットワークのブロードバンド化と個人用端末の高性能化ともなって、デジタルコンテンツの流通は著しく活発化している。STB(Set Top Box)端末を対象としたビデオオンデマンド配信やPCあるいは携帯型端末を対象としたコンテンツ配信のマーケットは今後大きな市場になっていくものと考えられる。また、撮影機器のデジタル化および高画質化、録画機器の大容量化やデジタル映像の視聴が可能な携帯端末の普及なども、こうしたコンテンツ流通の活性化の一翼を担っている。

その一方で、コンテンツの不正利用がカジュアル化して

いるとも言われ、特にファイル交換ソフトを用いた映画や音楽などのコンテンツの不正交換が大きな問題となっており、セキュリティ技術の一層の向上が求められている。

本稿では、これらの情報セキュリティ技術の検討を踏まえた上で、デジタルコンテンツ流通に関わる著作権保護技術の現状と今後の展望する⁽¹⁾⁽²⁾⁽³⁾⁽⁴⁾⁽⁵⁾。

2. コンテンツの保護技術

コンテンツの不正コピー問題は、従来からコンテンツ流通の課題の一つであった⁽⁶⁾⁽⁷⁾。デジタルコンテンツは、その性質上、全く劣化のない複製を少ないコストで作成する

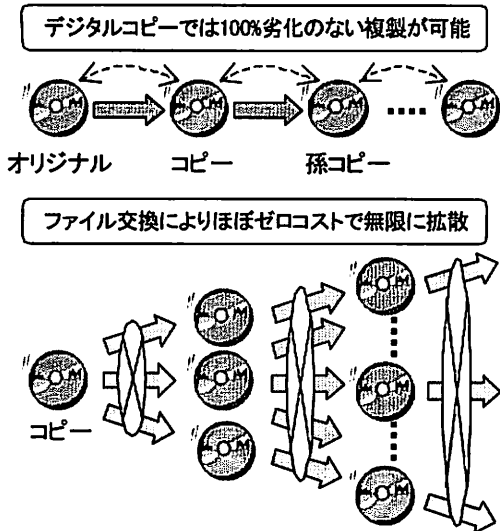


図1 コンテンツの不正コピーと不正交換 一度デジタル化された不正コピーコンテンツは、ネットワークを介したファイル交換により際限なく拡散し、根絶は困難である。

ことが可能である。したがって、オリジナルからのコピーだけでなく、コピーからのコピーといった、劣化のないコピーが繰り返し行われることにより、著作権者に対して本来支払われるべき対価なしに、コンテンツが不正に流通する恐れがある。不正コピー問題が深刻化したのは、ブロードバンド環境の普及による通信回線の高速化とファイル交換ソフトの蔓延によるところが大きい。

一度デジタル化した不正コピーコンテンツは、ネットワークを介したファイル交換によりほぼゼロコストで際限なく拡散するため、一度拡散してしまったコンテンツの根絶は困難である。

代表的なファイル交換ソフトとしては、WinMX と Winny などがあげられる。どちらも簡易なユーザインタフェース上での簡単な操作により、ファイルの共有・交換が可能となっている。これらのファイル交換ソフトを利用した違法コンテンツの交換状況は、映像ファイルで約 2.3 億ファイル、音楽ファイルで約 1.6 億ファイルとの調査結果⁽⁷⁾もあり、試算すれば 1000 億円以上の被害が出ている計算となる。最近になって、このような不正交換を行ったユーザに対し、訴訟にまで発展するケースが出てきたが、実態としては氷山の一角であり、不正コンテンツの交換に歯止めをかけることは難しい。

現在ファイル交換ソフトで交換されているコンテンツの多くが、著作権を侵害した違法コンテンツであると言われている。これらの違法コンテンツは、映画館などで上映中のコ

ンテンツをビデオカメラを使って撮影する CCAM 撮影や、DVD や CD などのコンテンツを PC を使ってデジタル化するリップキングを始めとして、テレビ、ビデオなどからのエンコーディング、スキャナーによる書籍や雑誌・コミックなどのスキャニング、ソフトウェアのバックアップやクラッキングなどの様々な手段によりデジタル化されたものである。今日では非常に多くのコンテンツがネットワークを介して交換され、対価の支払いなしに不正に視聴あるいは利用されている。こうしたコンテンツの不正利用を防止するには、コンテンツの違法なデジタル化すなわち不正コピーの防止と、ファイルを再生する端末における不正視聴の防止、そしてネットワークを介した不正交換の防止を目的とした技術が必要となる。

以下では、CD や DVD といった記録媒体により流通するメディアコンテンツの不正コピー防止技術、ネットワーク配信やデジタル放送により流通するネットワーク配信コンテンツの著作権管理技術、および不正コピーや違法ファイルの交換、不正利用を監視し、不正端末あるいは不正利用者を特定するトレイタートレーシング技術について紹介する。

2.1 メディアコンテンツの不正コピー防止技術

コンテンツの不正コピーへの対応策として、メディアに格納したコンテンツのコピーを禁止するコピープロテクションという考え方と、コピー先の媒体や機器、コピーの回数や世代数などを制限してコンテンツのコピーを許容するコピーコントロールという考え方の二通りがある。以下では、主要な映像流通メディアである DVD について、不正コピー防止技術を紹介する。

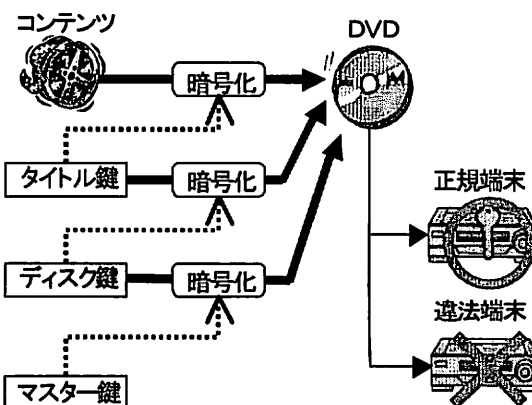


図2 CSSの暗号化手順 マスター鍵を保有しない違法端末ではディスク鍵・タイトル鍵を復元できず、暗号化されたコンテンツを再生することはできない。

(1). DVDメディアの保護技術

映像コンテンツをおさめたDVDメディアでは、幾つかの保護技術が規格化され、適用された⁽⁵⁾⁽⁶⁾。マクロビジョン(Macrovision)は、APS(Analog Protection System)ともいわれ、DVDからビデオなどへのアナログコピーを防止する技術である。ビデオのコピー防止技術として有名だが、同様の仕組みがDVDにも取り入れられている。ビデオなどの録画機器のAGC(Automatic Gain Control)に作用して誤作動を引き起こすAGC信号やカラーストライブ信号などをコンテンツに混入することにより、録画したコンテンツの色調などに異常を生じさせるものである。これによりビデオなどのアナログ録画機器を使った不正コピーが防止される。CGMS(Copy Generation Management System)は、CDメディアにおけるSCMSと同様に、複製制御情報CCIを用いて、DVHSやDVなどのデジタル録画機器へのデジタルコピーを制御する機構である。CGMSでは、CCIとして2ビットの信号を使用しており、コピー自由、コピーワンジェネレーション、コピー禁止、およびコピー済の4種類の制御信号により、録画機器の動作が制御される。

CSS(Content Scrambling System)はDVDビデオを再生可能な機器およびソフトウェアを制限するアクセスコントロール技術である。CSSでは、タイトル鍵、ディスク鍵、マスター鍵の3種類の、それぞれ40ビットの鍵を使用し、コンテンツを暗号化してメディアに記録する。まず、映像コンテンツはタイトル鍵で、タイトル鍵はディスク鍵で、ディスク鍵はマスター鍵で、それぞれ暗号化されて、暗号化コンテンツおよび暗号化タイトル鍵と暗号化ディスク鍵がDVDに記録される(図2)。マスター鍵を保有する正規端末では、暗号化ディスク鍵からディスク鍵を、暗号化タイトル鍵からタイトル鍵をそれぞれ復元し、タイトル鍵を使って暗号化コンテンツをデスクランブルすることで、コンテンツが再生可能となる。一方、マスター鍵を保有しない違法な端末ではスクランブルしたコンテンツを再生できないため、複製機能を有する違法な端末での不正コピーは防止される。

(2). DVD保護技術の高度化

CSSマスター鍵の漏洩という事態を受けて、鍵が漏洩しても頑健であるような新たな保護技術が必要となり、再生メディア用のCPPM(Copy Protection for Pre-recorded Media)と記録メディア用のCPRM(Copy Protection for Recordable Media)が規格化された。CPPMとCPRMでは鍵管理および暗号化技術が高度化され、56ビットの鍵による64ビットブロック暗号C2(Cryptomeria Cipher)がコンテンツおよび鍵の暗号化に

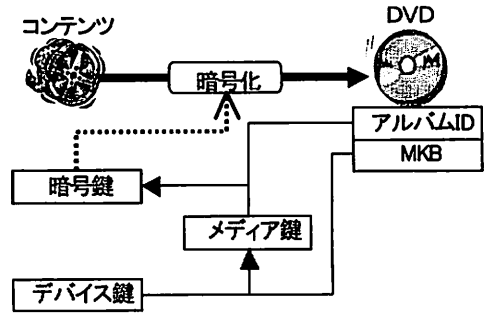


図3 CPPMの暗号化手順 アルバムIDとMKBは、メディア固有の情報として複製不可能な領域に記録されるため、コピーされたメディアからは正常な暗号鍵が復元できず、暗号化されたコンテンツを再生できない。

使用されている。

CPPMでは、デバイス鍵、MKB(Media Key Block)、アルバムIDの3種類の鍵により生成される。メディア鍵と暗号鍵を使用して、コンテンツの暗号化を行う(図3)。まず、デバイス鍵とMKBとからメディア鍵が生成される。デバイス鍵とは端末に与えられた固有の鍵、MKBは個々のデバイス鍵に対応する鍵の集合で、異なるデバイス鍵で暗号化処理を施しても結果として同じメディア鍵が得られる仕組みとなっている。このメディア鍵をアルバムIDで暗号化した結果がコンテンツの暗号化・復号に使用する暗号鍵となる。DVDには、暗号鍵で暗号化されたコンテンツと、アルバムIDおよびMKBが記録され、CSSと同様にデバイス鍵を保有する正規端末のみが暗号鍵を復元して、コンテンツをデスクランブルできる。

CPPMにより保護されたDVDメディアを不正にコピーした場合、メディア固有のアルバムIDが異なるため、正しい暗号鍵を復元することはできず、コンテンツが再生できない。これにより不正コピーが防止される。CPRMでは、さらに鍵の種類が増え、デバイス鍵、MKB、メディアID、タイトル鍵の4種類の鍵を使用する。コンテンツはタイトル鍵により暗号化され、デバイス鍵とMKBから生成されるメディア鍵を、メディアIDにより暗号化した結果でタイトル鍵を暗号化することで、メディアの個別化を図っている。CPPMと同様に、不正コピーしたメディアではメディアIDが異なるため、正しい暗号鍵を復元できず、コンテンツが再生できなくなる。

CPPMとCPRMはどちらも鍵の漏洩に対して頑健であるように設計されている。例えば、いずれかの端末がクラックされてデバイス鍵の一つが漏洩した場合でも、MKBの中に対応する情報を無効化することで、以降は漏洩したデ

バイス鍵からはメディア鍵を生成できなくすることが可能である。端末側にも同様の目的から、複数のデバイス鍵が付与されている。

このように、不正コピー防止技術は、コンテンツの暗号化における鍵の多様化と階層化による高度なコピーコントロールを行う方向に進みつつある。コンテンツとその記録メディア、および再生機器との間での鍵情報とコンテンツの制御を複雑化することで、セキュリティを向上させている。

2.2. ネットワーク配信コンテンツ著作権管理技術

メディアコンテンツの不正交換が問題視される一方で、オンラインコンテンツ配信が着実に活発化しつつある。iTunes に代表される音楽配信やビデオオンデマンドVOD (Video On Demand)による映像配信など、幾つかのコンテンツ配信ビジネスが立ち上がっている。これらの配信コンテンツには著作権を管理保護する技術が適用され、コンテンツの不正コピーや不正視聴を防いでいる。以下では、コンテンツ配信におけるDRM (Digital Rights Management) と、デジタル放送におけるCAS (Conditional Access System)を例として紹介する。

(1). デジタル権利管理

DRM(Digital Rights Management)

ネットワーク上のデジタル映像流通におけるコンテンツ保護技術として、現在最も広く利用されているのが、DRM (Digital Rights Management)⁽⁸⁾である。

DRMの基本的な考え方は、対象となるコンテンツを暗号化(カプセル化)して配送し、認証された個人あるいは端末に対してだけ復号を可能とすることにある。このような、

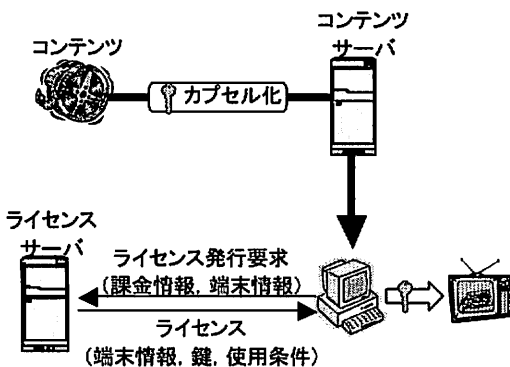


図4 DRMの基本概念 ライセンスに記述された端末情報および使用条件の下に復号鍵が導出でき、コンテンツが視聴可能となる。異なる端末ではライセンスの不一致によりコンテンツは再生できない。

コンテンツを視聴再生可能な個人や端末を制御する仕組みはアクセスコントロール(Access Control)と呼ばれる。

暗号化されたコンテンツを再生する際には、復号のための鍵情報とコンテンツの利用条件からなるライセンスが必要であり、利用者は取得したライセンスから鍵情報を得て初めてコンテンツの視聴が可能となる(図4)。したがって、コンテンツをコピーしてもライセンスを取得しない限りは再生できず、またライセンスは端末の固有情報を含むため、異なる端末では同様にコンテンツは再生できない。これにより許諾端末以外でのコンテンツの不正視聴が防止される。

主要なコンテンツ配信サービスでは、DRMを用いた著作権管理プラットフォームとして、Microsoft社のWM DRM (Windows Media Digital Rights Management)やRealNetworks社のHelix DRMなどが主に使われている。これらの製品の特徴は、XrML (eXtensible rights Markup Language)のような著作権記述言語により、視聴期間や視聴回数を限定したり、コピー可能な機器やメディアを制限したりといった、柔軟なライセンス管理が可能になる点にある。また、コンテンツの配信形態に合わせた複数フォーマットへの対応や、モバイル機器や家庭用電化製品などの多種多様な機器・メディア上でのコンテンツ保護が徐々に実現されてきている。

(2). 限定受信システム

CAS(Conditional Access System)

デジタル放送におけるCASは、コンテンツの視聴端末を限定するアクセスコントロール技術である⁽⁹⁾。CASでは、配信するコンテンツを数秒毎に異なるスクランブル鍵 K_s で暗号化し、このスクランブル鍵をワーク鍵 K_w で暗号化して、暗号化コンテンツと一緒にブロードキャスト配信する。ワーク鍵 K_w は一定の周期で更新され、個々の利用者

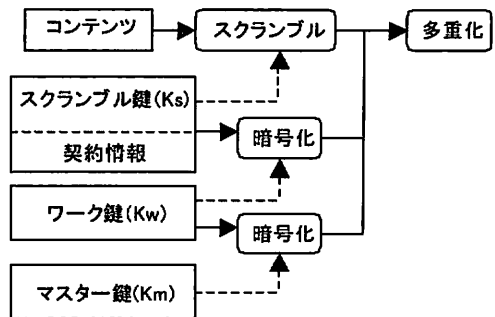


図5 CASの暗号化手順 ICカードに格納されたマスター鍵 K_m を有しない再生端末では、スクランブル鍵 K_s を取得するためのワーク鍵 K_w が導出できず、コンテンツのデスクランブル再生ができない。

の所有するマスター鍵 Km で暗号化された情報が、同様に配信される(図5)。

受信端末では、CASカードと呼ばれるICカードに格納されたユーザ個別のマスター鍵 Km を用いて受信情報からワーク鍵 Kw を導出し、これを使ってスクランブル鍵 Ks を逐次復元することで、コンテンツのデスクランブル再生が可能となる。

CASではマスター鍵 Km をCASカードの耐タンパーな領域に格納することで、鍵の漏洩を防いでいる。また、受信端末におけるコンテンツの録画やコピーなどはCCIやDTCPにより厳密に制御される。

さらに、放送コンテンツの蓄積と再生を可能とするサーバー型放送の実現に向けて、コンテンツの利用・課金方法の制御と、コンテンツおよびメタデータの不正利用や改竄の防止を実現する、高度なCASが提案されている⁽¹⁰⁾⁽¹⁴⁾。高度なCASでは、再生時に番組単位でコンテンツのアクセス制御を行えるように、新たにコンテンツ鍵を加えた四重鍵方式とし、暗号化した状態でコンテンツを蓄積し、視聴時にコンテンツを復号する方式となっている。また、コンテンツの利用制御情報であるRMPI(Rights Management & Protection Information)を併せて送出することで、蓄積コンテンツの利用を番組単位で制御可能としている。こうしたRMPIや、BML(Broadcast Markup Language)により記述された番組情報、電子番組ガイドEPG(Electronic Program Guide)などは放送コンテンツに関する一種のメタデータであり、不正な改竄が行われることは事業者および利用者双方にとって望ましくない。そこで、こうしたメタデータ改竄防止のためにデジタル署名技術が使われている。

2.3. トレイタートレーシング技術

これまでコンテンツの不正コピーを防止するための技術を中心に説明してきたが、これらの保護技術をすり抜けて不正流通するコンテンツも少なからず存在する。そこで、このような不正流通の状況を監視し、不正を行った端末あるいはその利用者を特定するトレイタートレーシング(Traitor Tracing)技術が必要となる。トレイタートレーシングは、幾つかの技術の組み合わせにより実現されるが、基本的には、コンテンツの識別技術とネットワークの監視技術とからなる場合が多い。そもそもネットワーク上で流通する不正コンテンツを特定することは難しいため、著作権管理されたコンテンツを識別する手段として、電子透かし技術などを用いたコンテンツへのID付与が提案されている。一方、ネットワークの監視技術としては、個々のノードとして参加して能動的な探索を行うロボット型と、受動的な

監視を行うゲートウェイ型があり、流通コンテンツのIDを読み出して著作権情報を調べることで不正コンテンツかどうかの判定を行う⁽¹¹⁾⁽¹²⁾。なお、コンテンツの識別手段として、コンテンツの特徴量を使ったフィンガープリンティングなども提案されている⁽¹³⁾。

このようなトレイタートレーシングは、前述のDRM技術のような積極的なコンテンツ保護技術ではないが、コンテンツの不正流通の監視や摘発時の有効な情報の一つとなる。しかしながら、トレイタートレーシングにかかるコストを誰が負担するかという運用上の問題が大きく、本格的な運用に至るケースは少ない。

3. コンテンツ保護技術の課題

コンテンツとメディア、コンテンツと端末機器をいかに結び付け、不正コピーを防止するかが、コンテンツセキュリティの課題となっている。その一方で、セキュリティコストの負担、利用者の利便性の向上とプライバシー保護のバランスなど新たな課題も出てきている。

(1). セキュリティコストとビジネスモデル

コンテンツ保護技術が高度化する一方で、技術の開発・運用にかかるセキュリティコストを誰が負担するか、という問題がある。こうしたコストは、一般にコンテンツ自体の価格に転嫁されることが多いが、コンテンツの価格は固定(または安価、または無償に)して、テレビと同じように広告収入を得ることでコストを賄うといった新たなビジネスモデルが検討されている。

また、音楽や映像の記録などを行う記録用メディアには、著作権の存在するコンテンツがコピーされることを前提に、あらかじめ補償金を課す私的録音・録画補償金制度という仕組みがあるが、最近では、こうした著作権管理料を携帯音楽プレーヤーなどに課すという動きがあり大きな議論を呼んでいる。

(2). プライバシー保護の問題

DRMやCASによる視聴管理はコンテンツを保護する観点からは極めて有効な技術であるが、その一方でプライバシー保護の問題を指摘する声もある。DRMやCASは、コンテンツの視聴再生に際して端末あるいは個人を認証することで、デジタルコンテンツの著作権を管理を実現している。この認証情報を利用すれば、誰が、いつ、どのようなコンテンツを視聴再生したかという詳細な視聴情報を取得することが可能となる。こうしたコンテンツに関する嗜好情報は一種の個人情報であり、適切な取得と管理の枠組みが必要とされている。

(3). 権利と制限のバランス

保護技術の過度な適用による、コンテンツの利用の制限も問題となっている。従来のコンテンツ保護技術では、こうした私的利用は強く制限され、時には利用者の利益を損なっている場合もある。

例えば、DRMでは購入したライセンスのバックアップを作成し、PCやデータの不慮の破損に備えることができる。しかし、PCの構成がライセンス購入時と異なるなどの理由で、バックアップしたライセンスではコンテンツの視聴ができなくなることもある。

デジタル放送におけるコピーワンスにも同様の問題があり、たとえばHDDレコーダーなどで録画したコンテンツを記録メディアにコピーする場合、本体から削除することで録画コンテンツが常に1つしか存在しないように制限する機能が備わっているが、停電などの不慮の中断や異常なコピーによりコンテンツが失われる場合がある。

さらに、教育目的での利用の範囲では、複製や上映が許されているが、たとえばWEBを使ったe-Learningによる教育を考えた場合に、アクセス範囲をどのように制限するか、また学生をいかに認証するかも課題となっている。

こうした家庭内や個人、教育機関での利用といった、著作権法で認められた一定の条件の下での許諾に対しては、権利と制限のバランスをいかに取るかが重要になる。これらの問題は物財とデジタル財の所有と利用、管理や保存方法の違いに根ざしており、デジタル革新に適合した仕組みを構築していかなければならぬ。

4. Web2.0時代の著作権管理技術

ブロードバンドの普及により、Web、Blog、SNSを使った個人や家庭、コミュニティからの情報発信が活発化している。また、近年、情報共有自由型(コモンズ)のパラダイムによるコモンズコンテンツの登場やメタデータ流通など⁽¹⁷⁾⁽¹⁸⁾新たなコンテンツビジネスモデルが立ち上がりつつある。それは、デジタル技術による大衆のコンテンツ創造と発信に基づくものであり、そのような個人、家庭、コミュニティからの情報発信というコンテキストで著作権管理の問題を考えていく必要がある。デジタル時代の著作権から、大衆からの発信時代の著作権へとパラダイムシフトが起こりつつある。

4.1. デジタル時代の著作権⁽²⁾⁽⁹⁾

デジタル時代に即応する権利流通モデルの代表例としては、法学研究者の北川善太郎氏(1997)の提唱する「コピーマート」がある⁽²⁰⁾。これは現行の法制度にそったものである。権利者とユーザは、著作権管理情報データベ

ースによって取引条件を確定し、著作物の売買とその決済をおこなう考え方である。

一方、情報システム研究者の森亮一氏(1996)の提案した「超流通システム」があり、これは技術主導型のシステムである⁽²¹⁾。複製物に関する流通追跡システムを社会のなかにインフラとして組み込み、その上で複製の流通を自由化する構想である。

また、法学者のローレンス・レッシグが始めたプロジェクトである「クリエイティブ・コモンズ(Creative Commons)」がある。自分の著作物について、自分でその利用方法を決めるというプロジェクトである⁽²²⁾⁽²³⁾⁽²⁴⁾。類似の提案としては、視覚障害者向けの「eye love eyeマーク」、文化庁の「自由利用マーク」及び林紘一郎氏(2004)の「dマーク」がある。

デジタルコンテンツのブロードバンド・ネットワーク流通を活性化するため、システム、サービスの共通概念としてNTT通信研究所から考案されたのが、コンテンツIDフォーラム(cIDf)である⁽¹⁴⁾。コンテンツごとにユニークなIDを与えるというコンテンツの固体化技術である。コンテンツIDは電子透かし技術などでコンテンツ自体に埋め込まれる識別子となっている。

4.2. Web・Blog・SNS時代の著作権管理

個人が情報、映像・音楽、ソフトウェアモジュール等のコンテンツを制作し、発信できる環境が整備された。日本型「YouTube」の動きも活発になっており、激しく市場が動き出す可能性がある。このような情報環境で、デジタルコンテンツの素材流通・登竜門、大衆創作コンテンツの流通市場を活性化するためには、創作者とコンテンツの認証・識別、複製・視聴・加工編集などの利用・再利用制御、課金・利益分配・契約などビジネスインフラが必要になる。一方で法制度の側面からは、検索エンジン、SNSサイトへの著作権訴訟が続いている。YouTubeが法的責任を負うことになるか否かは、著作権法の解釈にかかっている。判例としての「Betamaxスタンダード」が、デジタル時代になって初めて真価が問われる。

国際的にはCreative Commonsなどデジタルコンテンツ流通のプロジェクトが増加している。その中で、米マグナチューン、NTTのClipLife.jpが、Creative Commonsの導

このような課題を踏まえ、曾根原登(2006.3)は、Creative Commons を発展させ、技術、市場メカニズム、デジタル流通秩序の連携を目指したコンテンツのライフサイクル管理技術と実証的システム、権利流通サービスを開発した(25)(26)(27)。

コンテンツ流通の世界で独立していた概念であるコモンズ・ドメインと商用ドメイン間を、コンテンツ自身が自動的に遷移する流通モデルである。コンテンツのコモンズ・ドメインへの登録に際しては、創作者は、デジタル著作権表示(DRE)の考え方をベースに権利と利用条件を表明する。評判、購入度(ダウンロード数)が高まれば、その表明に従ったコンテンツの状態遷移を行い、商用ドメインに自動的に状態遷移する。逆に、評判、購入度が減少すると逆方向に自動的に遷移する。

コンピュータシステムを用いて、初期価格を投入するだけで、販売に関わる値付けを、そのコンテンツの需要に応じて価格を上げていくことができる。高すぎる価格付けで売れるものが売れなくなったり、低すぎる価格で制作者が本来得られる利益の機会を失ったりすることを回避することができる。こうして需要に応じた適正価格を自動的につけることでデジタルコンテンツ市場を正常に成長させることができる。また価格を徐々に上昇させるので、早く購入した利用者に損をさせることも避けことができ、早期購入リスクを軽減させることにもつながる(32)。

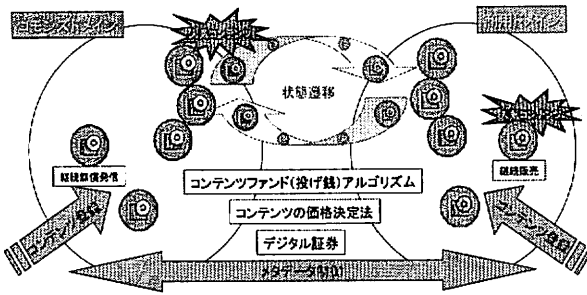
5. むすび

デジタル技術の浸透にともなって、流通形態の変化や、所有と利用の概念の分離、コモンズコンテンツの登場など、コンテンツ流通は大きく様変わりしつつある。

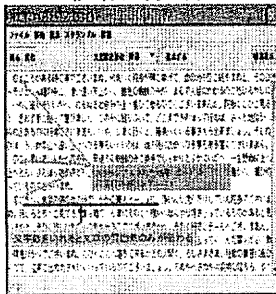
これまでのコンテンツ流通は、主に劇場映画や放送番組、メジャー音楽などのプレミアムコンテンツを流通させるという商用ドメインでの議論が多く、そのため、メディアの不正コピー防止技術やアクセスコントロール技術を中心に議論されてきた。しかし、デジタルからWeb, Blog, SNSなどを用いた情報発信時代の到来を迎え、商用コンテンツ以外の流通にも目を向ける必要が出てきた。

こうした流れの中、著作権保護技術も変革の時を迎えている。大衆からの情報発信を市場化していくような経済システムでは、情報発信を支えるコンテンツ制作技術、情報の価値や信頼性の評価技術、情報の所有と利用にかかわる情報資源管理技術など、新たな著作権保護や個人情報保護の考え方に基づいて可用性を高める技術が必要になっている(28)(29)(30)(31)。

自由・平等・安心というICT社会実現の目的の下で、自由度・利便性の向上や経済発展と、著作権保護、



例) 芥川龍之介「蜘蛛の糸」
(ライセンススクランブル)



利用度に応じた連続スクランブル生成方式

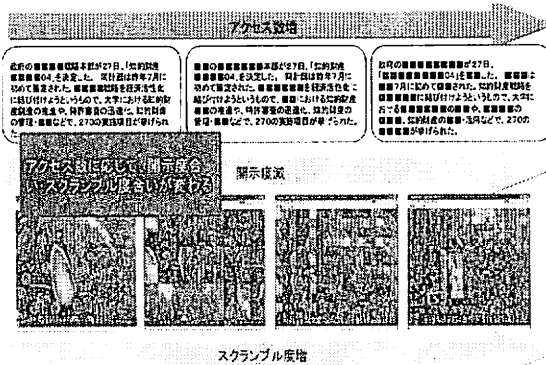
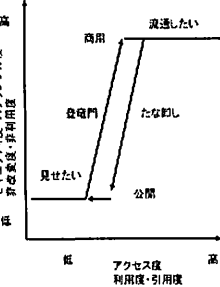


図6 デジタルコンテンツのライフサイクル管理
上)パブリックドメインと商用ドメインの状態遷移
中)テキストスクランブル、アクセス度と開示度の関係
下)テキスト伏字、画像スクランブルの開示度

入を打ち出している。オーストラリアでは、Registered Commons という登録するコンテンツを認証するサービスが始まっている。このようなデジタル著作権管理(DRM)から、権利表明指向のデジタル著作権表示(DRE)に対しての議論が急速に進み始めている。

4.3 コンテンツのライフサイクル管理技術

個人情報・プライバシー保護、情報セキュリティ技術などをバランス良く連携していく必要がある。

5-160. 森亮一, 河原正治, 大瀧保広
<http://sda.k.tsukuba-tech.ac.jp/SdA/reports/A-59/draft.html>

参考文献

- [1] 総務省, 「ブロードバンドサービス等の契約数(平成18年12月末)」, 報道発表資料, 2007/3/13
- [2] 林 紘一郎編著, 曾根原登ほか共著: 「著作権の法と経済学」, 勁草書房, 2004
- [3] 日本工学会アカデミー・日本学術会議編, 安田浩, 辻井重雄, 曾根原登ほか共著: 「2010年コンテンツ産業に必要な8つの要件 d-commerce宣言」, アスキー出版, 2004
- [4] 廣田啓一, 曾根原登, 「コンテンツ流通における不正利用防止技術」, 電子情報通信学会誌, 2005
- [5] 廣田啓一, 曾根原登, 「デジタル映像流通に関わる著作権保護の今後の展望」, 映像情報メディア学会誌, 2005
- [6] コンテンツ保護技術とその法的評価: デジタルコンテンツをめぐる法的課題に関する調査研究報告書, デジタルコンテンツ協会, 2003.
- [7] コンピュータソフトウェア著作権協会・日本レコード協会, ファイル交換ソフト利用実態調査, 2004.
- [8] D R M の アーキテクチャ, <http://www.microsoft.com/japan/windows/windowsmedia/wm7/DRM/architecture.aspx>
- [9] (社)電波産業会, デジタル放送におけるアクセス制御方式, ARIB STD-B25, 1999.
- [10] 西本友成・馬場秋継・栗岡辰弥・難波誠一, サーバー型放送のためのコンテンツのアクセス制御方式, 映情学会誌, Vol. 58, No. 7, pp. 1003-1008, 2004.
- [11] コンテンツIDフォーラム, cIDf仕様書第2.0版, <http://www.cIDf.org>, 2002.
- [12] 東條弘他, デジタルコンテンツ権利管理のためのコンテンツ不正掲載探索システムの検討, 信学技報, TM2001-30, pp. 45-50, 2001.
- [13] 長田礼子・安田浩他, 符号量圧縮ベクトル符号化技術を用いたデジタルコンテンツ著作権保護技術, ITX2001論文集, 情報処理振興事業協会, 2001.
- [14] 曾根原登, 新井紀子他共著, 「デジタルが変える放送と教育」, 丸善ライブラリー, 2005
- [15] 東倉洋一, 岡田仁志, 曾根原登, 他共著: 「情報セキュリティと法制度」, 丸善ライブラリー, 2005
- [16] 曾根原登 編著: 「デジタル情報流通システム」, 東京電機大学出版, 2005
- [17] 曾根原登編著: 「メタデータ技術とセマンティックウェブ」東京電機大学出版, 2006
- [18] 曾根原登, 他「メタデータ流通基盤」, 電子情報通信学会 IN 研究会, 2005.11
- [19] 名和小太郎, デジタル著作権, みすず書房, 2004.
- [20] 北川善太郎(1997)「電子著作権管理システムとコピーマート」情報処理, 38巻, 8号, pp663-668.
- [21] 森亮一(1996)「超流通: 知的財産権処理のための電子技術」情報処理, 37巻, 2号, pp15
- [22] <http://www.creativecommons.org/>
- [23] <http://www.creativecommons.jp/>
- [24] クリエイティブ・コモンズ・ジャパン編, ローレンス・レッシング・林紘一郎・相山敬士・若槻絵美・上村圭介・土屋大洋共著, クリエイティブ・コモンズ・デジタル時代の知的財産権, NTT出版, 2005.
- [25] 南憲一, 阿部剛仁, ローレンス・レッシング, 曾根原登, TEAM Digital Commons - ネットワーク・コンテンツ流通革命による市場活性化計画, NTT技術ジャーナル, 2004.
- [26] 曾根原登「デジタル権利ライフサイクル管理の提案」, NII 国際情報学シンポジウム, 「知的情報の流通と学術・文化の発展に向けて」, 2006.3.27
- [27] 曾根原登, 「ネットの文章・映像 / 国立情報学研がシステム / 人気出れば商品に格上げ」, 日本経済新聞, 2005.10.3
- [28] 渡辺克也, 「e-Japan 構想に見るユビキタスネットワーク社会」, 電子情報通信学会 / 第16回光通信システムシンポジウム, 2002.12.12
- [29] 渡辺克也, 「ユビキタスネットワーク」, 日本学術振興会 / 2002年度インターネット技術第163委員会シンポジウム 2003.3.11
- [30] 渡辺克也, 「ブロードバンド列島の近未来」, 日刊工業新聞社 / 情報戦略フォーラム 2002, 2002.12.6
- [31] 渡辺克也, 「ユビキタスネットワーク技術の将来展望と政策展開」, 2002.9.5, (電子情報技術産業協会 / デジタル家電フォーラム 2002)
- [32] 釜江, 曾根原, 他, 「デジタルコンテンツ販売のための開示度と料金の設定」, 電子情報通信学会, (To be appeared), 2007