自分の著作権を守るために　－　技術的視点から
To protect Copyrights　－　From Technical Points of View　－

佐野　睦夫
Mutsuo Sano
大阪工業大学　情報科学部，枚方市　北山　1-79-1
Osaka Institute of Technology, Hirakata Kitayama 1-79-1

あらまし：コンテンツの著作権を守り，インターネットの世界に安心して流通させるには，法律的視点からの取り組みとともに，コンテンツ流通のインフラをどのように設計し運用していく技術面からの取り組みが不可欠である．本報告では，著作権保護・管理技術の今までの取り組みを概観し技術的限界も示す．同時に，今後の著作権保護・管理技術の方向性について言及する．

Summary: In order to protect content copyrights and safely distribute content through internet, it is necessary not only to cope with its legal problems, but also to challenge technical problems to design an infrastructure of content distribution. This paper makes a survey of some significant technical challenges to protect copyrights and manage digital rights, and also show technical limitations to do them. Finally, we refer to the direction of copyrights protection techniques and digital rights management technology.

キーワード：著作権保護，著作権管理，コンテンツ流通，電子透かし，暗号化
Keywords: copyrights protection, digital rights management, content distribution, digital watermark, encryption

1．まえがき

近年，コンテンツのディジタル化とインターネットを介した流通が徐々に進展してきている．たとえば，インターネットによる音楽や映画のストリーミング配信，漫画やアイドル写真などのダウンロード販売などが挙げられる．また，2003年12月から限定地域で開始される地上波ディジタル放送など，インターネット分野だけでなく，放送分野においてもディジタルコンテンツの流通が進んできている．

ディジタルコンテンツの利点は，アナログと比較して，1）原理的には流通経路に関わりなく同じ品質で利用者に送ることができる，2）再編集がコンピュータを使えることで容易になり，繰り返し用いても劣化なく編集ができる，3）番組の再利用もアーカイブしておくことで簡単に行うことができることなどが挙げられる．一方，欠点は，ディジタルである性質から，品質の劣化なく何回でもコピー可能となり，不正利用の温床となる危険性があることである．実際，気に入った画像や映像を購入し，自分のホームページに勝手に掲載したり，購入したコンテンツをNapster，Gnutellaのように無料で相互利用を行うこともできる（現在は，Napsterは有料化されている）．このような制作者の著作権を無視した違法が横行することにより，コンテンツ制作者への対価の回収できなくなり，ひいては品質の悪いコンテンツしか生み出せない悪循環に陥る可能性がある．

ここで，この不正コピーを防ぎ，著作権を守るためには，法的な処置は不可欠であるが，技術的な仕組みの提供も不可欠である．本論文では，第2章で技術的な立場から，不正コピーを未然に防ぐコピー制御方式について論じる．第3章では，ハッキングにあった場合の事後処理として不正コピーの拡大を抑止し，不正利用コンテンツを検出する方式について述べる．不正利用コンテンツが検出できれば，法的手段を活用することも可能となり，全体として不正利用抑止効果が生まれる．

最後に，第4章では，著作権を総合的に守るための

システム構成法について議論し，コンテンツ流通を活性化させながら著作権を守る仕組みの重要性について言及する．

2．コピー制御技術

品質の劣化なく無限にコピーされる心配のあるディジタルコンテンツに関するコピー制御としては，コンテンツのヘッダに付与されたコピー制御フラグを用いる方法が一般的である．フラグは2bitで構成され，「00」はマスタ媒体作成に用いられるもので無限回コピーが可能，「10」として出荷しておけば，CDからMDへの変換などの正当なデータの複製を親コンテンツから1回だけ認め，1回コピーが実行されると，「11」となる．このような複製制御情報を録音機器側に送付し，「11」の状態，すなわち子のコンテンツから再度コピーしようとすると，録音機側でコピーできなくなるようにハードウェア制御を行う．この方式に基づく音楽コンテンツ版（CD や MD，DAT 等）が SCMS（Serial Copy Management System），ビデオ映像版（DV 等）が CGMS（Copy Generation Management System）である．しかし，コピー制御フラグ方式は，機器にバインドしたコピー制御方式であり，不正コピーの攻撃手法の進化に対しては機器自体をかえる必要があり，柔軟性はない．

一方，コンテンツ自体を暗号化し，再生機器は復号鍵を持っていなければ再生できないコンテンツ暗号化方式がある．コピー制御情報としては何度までコピー可能かという細かい情報がコンテンツにバインドでき，世代管理を柔軟に行うことが可能である．攻撃に対しては，

(1) コンテンツ固有の鍵とデバイス固有の鍵などの複数の鍵を組合せる

(2) 暗号方式自体を改良する

ことにより，全体の暗号化強度を高めることができる．また，機器のハードウェアに依存した方式ではないので，コピー制御技術の開発を機器の開発と分離して行えるという利点がある．

具体的には，DVD ビデオに採用されている CSS（Content Scramble System）方式，音楽の DVD 再生に用いられている CPPM（Content Protection for Prerecorded Media）方式，PC 家電の記録可能な DVD のメディアに用いられている CPRM（Content Protection for Recordable Media）方式などがある．

しかしながら，これらの方式は，

(1) 一度ハッキングにあってしまうと無力である

(2) 多少の劣化はあるものの，再生されたアナログコンテンツの不正コピーには対処の仕様がない

という問題点を有している．

3．不正コピー抑止技術

ハッキングによって流出したコンテンツに対して，それ以上流出が広がらせないための不正コピー抑止技術について述べる．不正コピーを抑止するには，少なくとも1つの不正コピーが検出される必要がある．次に，不正コンテンツをどのように効率的に探索するかという方式検討が必要である．

3．1　不正コピー検出方式

不正コピーを検出する方法は下記の2つに大別される．

・検出すべき著作権情報をあらかじめコンテンツに埋め込み，埋め込まれた著作権情報を検出する．

・コンテンツ固有の特徴情報を登録しておき，特徴情報を検出する．

前者の方式は，ＤＣＤ（Distributed Content Descriptor）方式および電子透かし（Digital Watermark）方式であり，後者の方式はフィンガープリント（fingerprint）よる方式である。以下，この3方式の比較検討を行う．

（1）　DCDに基づく検出

ＤＣＤは，コンテンツ ID フォーラム[1]で規定している流通コンテンツ記述子であり，図1のように，コンテンツにユニークな ID（コンテンツ ID）と，代表的な著作権情報および，コンテンツ本体と DCD との組み合わせを保証する，すなわちコンテンツがオリジナルであることを証明するためのコンテンツ本体のハッシュ値，コンテンツ本体または DCD が改ざんされた場合に検出するためのディジタル署名から構成されている．DCD は，コンテンツの各種フォーマットに適した埋め込み場所が設定されており，コンテンツとバインドされたものとして流通する．不正検出は，ディジタルコンテンツの著作権を含めたすべての情報を格納した知的財産権データベース（以後，IPR-DB と称する）を参照することにより，不正利用検出および改ざん検出が可能となる．

（2）　電子透かしに基づく検出

電子透かしとは，「人間の知覚特性を利用して，人間に知覚できないように埋め込む，コンテンツ自体とは別の情報」であり，著作権に関する情報がしばしば埋め込まれる．著作権保護の観点から電子透かしに求

コンテンツID
コンテンツ属性
権利属性
権利運用属性
流通属性・分配属性
コンテンツのハッシュ方式 コンテンツのハッシュ値
ディジタル署名方式 ディジタル署名値
自由領域

図1　DCDの構成

Fig.1 Structure of DCD

められる要件としては,

(a) コンテンツ全体に埋め込み，コンテンツと一体化していること

(b) コンテンツ自体を劣化させないこと

(c) コンテンツの一部切り出し，拡大縮小，輪郭強調などの編集・加工やJPEGのような非可逆圧縮に対しても残りつづけること

(d) 電子透かしアルゴリズムのリバースエンジニアリングや，複数のユーザがコンテンツを比較し 電子透かしの埋め込み位置を特定する結託攻撃のような，改ざんや消去などを行う悪意のある攻撃に対して耐性があること

(e) 多様なメディアに共通すること

(f) 埋め込みおよび読み出しの両面で高速処理が可能であること

(g) できるだけ多くの情報を埋め込む能力を有していること

が挙げられる[2]，[3]．

電子透かしを実現する方式としては，大きく以下の2つがある．

・原信号に直接埋め込む方式

透かし情報を，透かし鍵に基づいて擬似雑音を発生させランダムパターンを発生させ，これを原信号に加えることにより，透かし入りコンテンツを生成する．読み出しはその逆で，原信号が利用できる場合は，引き算することにより，透かし入りコンテンツから，ランダムパターンを取り出すことにより実現する。画像であれば輝度信号に，音声であれば振幅やパワーに埋め込む．

・周波数変換を利用する方式[4]，[5]

画像を例にとり説明する．画像をブロックに分割し，それぞれのブロックをFFTやDCT，Wavelet変換などにより周波数変換し，その周波数係数に対して操作を加える．どの係数を変更するかが透かし鍵となる．読み出しは，透かし入り画像をブロック分割し周波数変換して，透かし鍵に基づいた係数の値が領域に入っていれば1，入っていなければ0とし，それらの系列値を算出することにより，透かし情報の読み出しが可能となる．

次に，電子透かし技術を用いるときの留意点について考察する．電子透かしに求められる要件(a)～(c)および(f)は，電子透かし技術に対する必須条件であるので，必ず実現させなければならない．以下，それ以外の要件に対して，現状の技術レベルとその適用方針について述べる．

(e)の多様なメディアに対し適応可能という要求条件は，画像や音声，動画それぞれに独自のアルゴリズムになっているのが現状であり，各メディアに対してそれぞれ実装していくことが必要となる．

(g)の埋め込む情報量については，埋め込む量が大きいとトレードオフで，(b)の品質と(c)の耐性を悪化させる．現状の技術レベルでは，耐性と品質を維持しながら埋め込める情報量は，数10から150ビット程度と考えられている[2]．

(d)については，攻撃をするたびにコンテンツを劣化させる方式や，埋め込みと読み出しに異なる鍵を利用するなど鍵管理方式などが検討されている．また，結託攻撃を防ぐために結託耐性符号法も研究されている．このような対策を打っても，新しい意図的な攻撃が次々と生まれてくる可能性があり，より頑健な電子透かしアルゴリズムの開発を期待したい．しかしながら，この問題は，秘密鍵の暗号化技術と共通の問題でもあり，電子透かし技術のアルゴリズムは公開せず，攻撃の機会をできるかぎり与えない対策が，商用の電子透かし技術として一般にとられている．

(3)　フィンガープリントに基づく検出

コンテンツの信号データの特徴量を登録しておき，比較する検出法で，いわゆるパターン検出法[6]に相

当する方式である．パターン検出法としては，超高速性が要求される．

3方式の性能比較

電子透かしおよびフィンガープリントは，アナログコンテンツに対しても検出が可能である．耐タンパー性から言えば，フィンガープリントはコンテンツそのものなので分離させることはできなく，フィンガープリント＞電子透かし＞＞DCD である．ただし，フィンガープリントで，微妙なコンテンツの違いを検出するのは，かなりのコストを要し現実的ではない．電子透かしは，埋め込んだ情報を検出するだけなので，検出コストの面からは優っている．また，実装もフィンガープリントよりも簡単である．一方， DCD は，どちらかと言えば，著作権情報の簡易的な問い合わせに適していると言える．

暗号化・DCD・電子透かし・コンテンツ ID の統合

図2に，DCD の利点と電子透かしの利点，および暗号化を組み合わせたコンテンツの著作権保護の構成を示す．ここでは，コンテンツ ID フォーラムで提案されているコンテンツ ID をコンテンツにユニークな ID として利用し構成している．電子透かしに埋め込む著作権情報を 64bit のコンテンツ ID コードとし，埋め込みデータのコンパクト化を図っている．このコード長程度であれば画質には影響ないことが実証されている。この4つの要素技術の統合により，コンテンツの不正利用防止，万が一ハッキングされたときのコンテンツ不正利用検出，改ざん検出，および簡易問い合わせが可能となる[7]．

3．2　コンテンツ不正利用探索方式

不正コンテンツを効率的に探索する方式についていくつか提案されている[7]，[8]．

まず，探索ロボット型の方式は，一般的な検索エンジンのクローラを利用し，網をかける探索キーワードを設定することにより，その関連ページを収集する．各ページ内で一定ホップ数の深さのページに掲載されているコンテンツから，前節の検出法により著作権情報を検出し，IPR-DB と著作権照合を行い，違法サイトを検出する．違法サイト検出の具体方法としては，IPR-DB には，コンテンツが合法的に存在するURLリスとが格納されており，検出したURL と比較し，合致するかどうかを判断する．この方式では，キーワードの選定と検出ホップ数のしきい値の設定が検出率のポイントとなる．

次に，ノード監視型の方式は，メールサーバやプロキスサーバーなどのネットワークの中継ノードを通過するコンテンツをすべてチェックし，著作権情報を検出し，著作権照合する．違法サイトの範囲を絞ることができれば，取りこぼしがないので有効な方法である．

最後に，利用者協力型の場合は，協力してもらえるユーザから自動的に，閲覧したコンテンツに関する著作権情報のレポートをもらうもとにより，著作権照合をし，違法サイトを検出する。協力者はレポート送付を意識せずに通常のコンテンツ視聴を楽しむことができる．この方式の利点は，検索サイトに掲載されていないコンテンツもアクセスができ，協力者が利用したコンテンツはすべて著作権情報が検出可能である．いかに，協力者の範囲を広げていくかがポイントである．

これら3方式を組み合わせて，どのように効率化するかは今後の課題である．

4．著作権を総合的に守るためのシステム構成法

図3に，典型的な著作権管理（DRM：Digital Rights Management）システムの構成例を示す[7]．この例では，電子透かしを用いたソリューションは説明を簡単化するため除いている．コンテンツ配信元で，コンテンツを暗号化し，配信サーバに準備しておく．同時に，ライセンス発行サーバに，コンテンツの利用条件と，暗号化した鍵が格納されている．ここで，ユーザがコンテンツサイトのページを見て，サムネイルやコンテンツの PR 情報から，暗号化されたコンテンツをダウンロードしたとする．再生しようとしても暗号化されていて再生できないので，ユーザ端末から，再生要求をかけると，ライセンス発行サーバとつながり，利用許諾条件を了解し，所定の課金処理が済むと，復号化するための鍵を利用許諾条件とともに，ユーザ端末に送付し，復号化を行い，再生して視聴することができる．

ここで，利用者のコピーを最初から制限してしまうことは，コンテンツ流通の活性化にとってマイナスに働く可能性を含んでいる．森は，2次利用を促進する枠組みとして超流通（SuperDistribution）[9]，[10]を提案した．この枠組みでは，コンテンツを課金なしに事前配布する。コンテンツを利用するたびに使用記録が管理され，それを回収することによって料金を徴収し収入を再配分する．この枠組みは，コピーは自由で，いいコンテンツはどんどん使用されるので対価が大きくなり，悪いコンテンツは誰も利用しなくなり最終的には自然淘汰される．

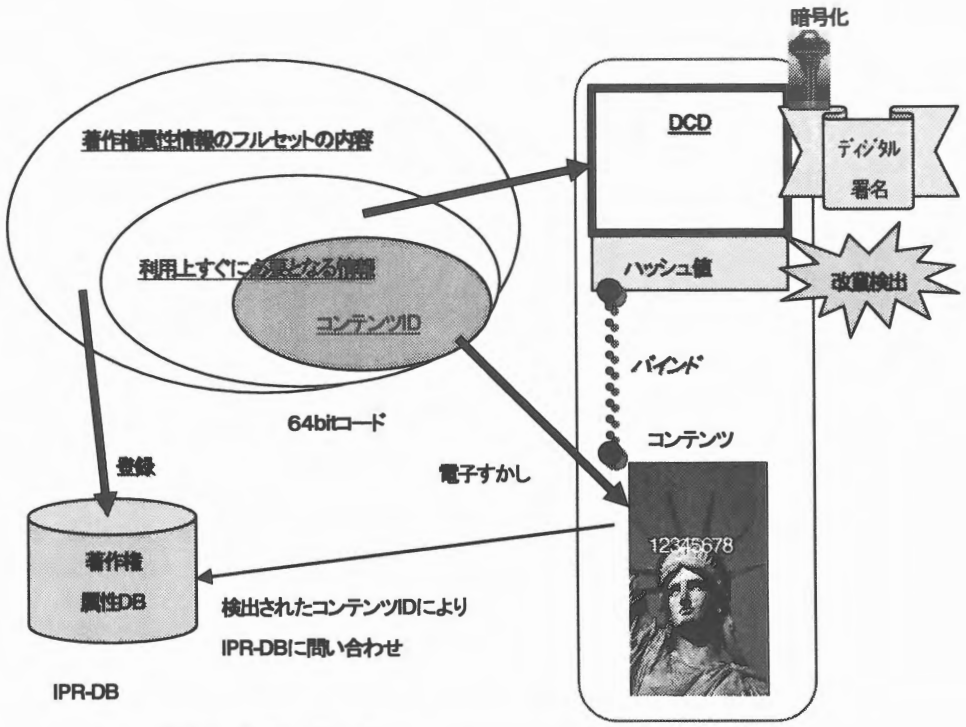

図2　暗号化・DCD・電子透かし・コンテンツ ID を統合した著作権保護

Fig. 2　Copyrights Protection with integrating encryption, DCD, digital watermark, and content ID

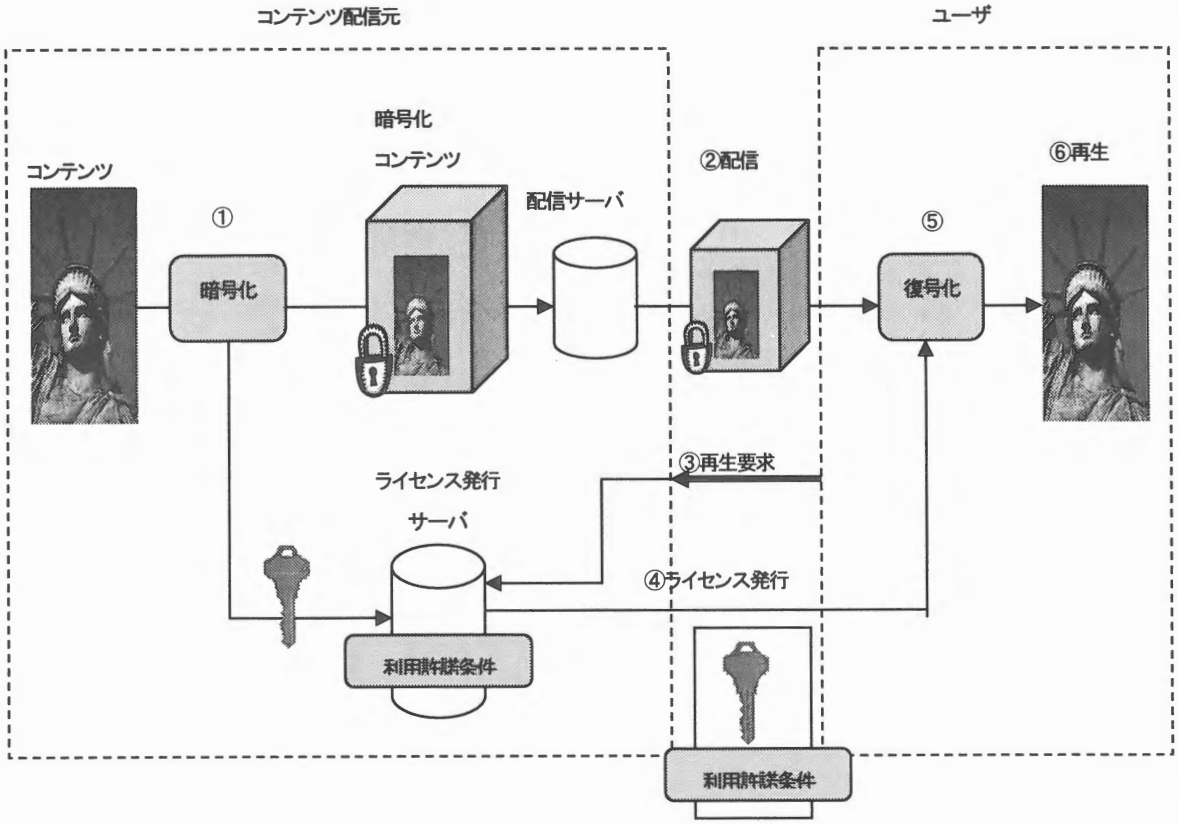

図3　典型的な DRM

Fig.3　A　typical example of DRM

一方で，コピー回数を売り手と買い手のマッチングにより決定し，回数自体は制限するという契約の概念を取り入れた仕組みとして，コピーマート（COPYMART）[11]がある．コピーマート方式は，著作権の集中管理方式であり，制度的にも運用しやすく，システム構築も容易である．現在のほとんどの著作権管理システムは，著作権情報やその契約情報を格納したデータベースサーバを核とした，この集中管理方式を採用している．ただし，コピーマートのように2次利用を前提とした体系化された契約形態に基づいたライセンス発行はしていない．

流通を活性化させるために，2次利用，さらに超流通のフレームワークの中で，著作者が安心できる著作権管理システムは，まだこれからである．最新映画のディジタル配信は，コンテンツを端末に残さないストリーミングしか，コンテンツホルダは許可していない．ハッキング対策との戦いであるが，BtoB, BtoC, BtoBtoC, PtoPのシームレスな流通フレームワークの中で，ユーザにも著作者にも受け入れられるシステムとして進化に期待する．

5．むすび

自分の著作権を守るために必要な技術について，現状の技術を整理し，現在の技術レベルや社会的評価を交えて論じたが，まだまだ解決すべきところが多いというのが実感である．筆者自身も，著作権管理システムを開発してきたが，BtoC，BtoBtoCをベースとしたものであった．今後の課題としては，インターネットの普及により個人がコンテンツを自ら作成し，自由に発信できるようになった現在，個人が所有する著作権を簡単にネゴシエートでき，今，ためらって利用できないコンテンツをどんどん利用できるようなシステムを作成していきたい．今，教育に携わっているが，教育コンテンツを再利用できるフレームワークは急務である．今後，著作権の垣根を越えてコンテンツ作成の生産性がどんどん上がり，それにつれて，産業もどんどん活性化する世界を期待している．

参考文献

[1] http://www.cidf.org

[2] 安田浩，安原隆一監修："ポイント図解式　コンテンツ流通教科書，"アスキー(2003)

[3] 松井甲子雄："電子透かしの基礎ーマルチメディアのニュープロテクト技術，"森北出版(1998)

[4] 中村高雄，小川宏，高嶋洋一："ディジタル画像の著作権保護のための周波数領域における電子透かし方式，"1997年暗号と情報セキュリティシンポジウム SCIS97-26A,JAN.（1997）

[5] 小川宏，中村高雄，高嶋洋一："DCTを用いたディジタル動画像における著作権情報埋め込み方法，"1997年暗号と情報セキュリティシンポジウム SCIS97-31G,JAN.（1997）

[6] 柏野 邦夫，黒住 隆行，村瀬 洋，同じ音や映像を高速に探す技術ー学習アクティブ探索法 NTT R&D, Vol.52, No.2, pp.115-121（2003）

[7] 佐野睦夫，茂木一男,，松浦由美子，堀岡力，千葉常之，稲垣博人，竹野浩，大森信行："情報流通プラットフォームが拓く21世紀のネットワーク化社会　その2ー　著作権管理 NTT技術ジャーナル　11月号 pp.26～30（2000）

[8] 岡田和比古監修："未来ねっと技術シリーズ　サイバーインタフェースのデザイン１２，"pp.130-133 電気通信協会（2001）

[9] 森亮一，河原正治，大瀧保広："超流通：知的財産権処理のための電子技術，"　情報処理，Vol.37，No.2，pp.155-161（1996）

[10] 森亮一，田代秀一："ソフトウェア・サービス・システム（SSS）の提案，"信学論　Vol.J70-D, No.1,pp.70-81(1987)

[11] 北川善太郎："電子著作権管理システムとコピーマート，"情報処理，Vol.38，No.8，pp.663-668（1997）