中澤ゼミ

# デジタルコンテンツの利便性を考慮した著作権管理システム
## ～“柔らかなDRM”をめざして～

A1200409 栗城 晴菜

## 1 はじめに

近年，音楽や映像，テキストといったコンテンツのデジタル化が進み，加えてインターネットの普及やパソコンの高速・大容量化にともなって，著作者の許諾を得ない違法なコピー・交換などが増えている[1][2]．デジタル化されたコンテンツは何度コピーしても，どんなに遠距離を送受信しても品質は劣化しないため，不正コピーのまん延によって著作者は多大な不利益を被ってしまう．これらの不正行為を防止するため，現在，有料デジタルコンテンツの多くはDRM（Digital Rights Management；デジタル著作権管理）技術によってその著作権が保護されている[3]．

しかし，DRMによって著作権が強力に保護される反面，コンテンツの私的な使用のためのコピーさえ厳しく制限されてしまうなど，正当なユーザがデジタルコンテンツに不便さを感じる状況になってしまっているのも事実である．こうした権利強化の動きに対して，比較的緩い制限でコンテンツを使用できる環境を提供しようとする動きも始まっている[1][7]．

本研究では，現存のDRMシステムの利用状況やその技術について述べたうえで，適度な制限を持つ理想的な新システムについて考察する．具体的には，著作者の権利を確実に守りながらも，ユーザの利便性が考慮された適切な著作権管理システムを，“柔らかなDRM”として提案する．

## 2 DRMシステム

DRMシステムとは，流通するコンテンツの暗号化[1]，利用者の認証，専用の視聴用ソフトの使用，電子透かし[2]等の技術を組み合わせて，デジタルコンテンツの著作権を総合的に保護するシステムである[2][3]．デジタルコンテンツは，その流通手段としてCDやDVDなどのパッケージ販売やデジタル放送，ネットワーク配信といった形態があり，フォーマットも様々であるが，DRMシステムを使用することで，あらゆる流通の場面でコンテンツを保護することができる．

### 2.1 DRMの技術と現存のシステム

コンテンツの不正使用防止を実現している技術としては，大きく「コピー制御方式」と「アクセス制御方式」に分類される[3]．なお，コピー制御方式とアクセス制御方式は併用される場合もあることを，あらかじめ述べておく．

#### 2.1.1 コピー制御方式

コピー制御方式は，コンテンツをコピーしようと操作を加えた際に制限がかけられるもので，“コピーを全くさせない”か，または“一定回数までしかコピーを許さない”方法がとられる．前者の代表的な例に，ソニーやエイベックスが過去に発売したCCCD[3]（Copy Control CD）がある．このCDでは完全にコピーを防ぐために規格外の信号を埋め込んでいるため，正規の利用にも関わらず再生できない，音飛びしてしまう，などといった誤作動が起きるという問題があった[16]．

後者の“一定回数までしかコピーを許さない”方法に関しては，「コピー制御情報型」と「ネットワーク認証型」に分けられる．「コピー制御情報型」では，CCI（Copy Control Information）というコピー回数制限の情報を，コンテンツと一緒に記録しておく．そして，対応する記録端末は送られてきたCCIに従ってコピー制御を行う．例えば，“一回だけコピー可”といったCCIを記録しておくことで，そのコンテンツは2回目以降のコピーを不可能にすることができる．DVDのコピー制御に用いられるCPRM[4]やDTCP[5]，デジタル放送のCAS[6]などでこの技術が利用される[5]．

一方の「ネットワーク認証型」では，コンテンツや記録媒体，プレイヤーごとにそれぞれ固有のIDを付与しておく．このIDを用いてネットワーク上の認証サーバにコピー可/否の問い合わせをし，認証サーバから送られた可/否情報に基づいて，再生端末にてコピー制限を行う．ソニーのレーベルゲートCD[7]などがこの技術を用いている．

#### 2.1.2 アクセス制御方式

アクセス制御方式は，コピー操作には制限をかけないが，コンテンツを再生する際に視聴を不可能とさせるものである．基本的には暗号化技術をコンテンツに施してそのままでは視聴できない形で流通させ，アクセスを許されている人だけが入手できる鍵で暗号化を解除させる仕組みになっている．

---

[1] デジタルデータをやり取りする際に，通信途中で第三者に盗み見られたり改ざんされたりされないよう，決まった規則（アルゴリズム）と鍵の2つを使ってデータを変換すること．鍵を使って暗号文を元のデータに戻すことを復号化という．

[2] 画像や音声などのデジタルデータに人間が知覚できない程度の情報データを埋め込むことで，不正流通の流出元などを把握できる．

[3] パソコンのCD-ROMドライブでの読み取りを困難にした音楽CDだが，CDの規格を定めた「Red Book」仕様書に準拠していない．

[4] Content Protection Recordable Media．DVDレコーダやフラッシュ・メモリ・カードなど，書き込み可能なメディアのコンテンツを保護するもの．記録デバイス，記録メディア，再生デバイスすべてが4C Entityという組織からライセンスを受けないと，読み書きができないことを保証している．

[5] Digital Transmission Content Protection．家庭内でつながった機器間で，データを転送する際にそれを保護する．DTLA（Digital Transmission Licensing Administrator）という組織からライセンスを受けた機器のみがコンテンツを読み書きできる．

[6] Conditional access system．放送データにスクランブル信号をかけ，特定の視聴者だけが視聴できるようにした放送システム．

[7] ソニーが開発したCD規格でCCCDの一種．パソコンで再生するには，専用ソフトを起動し，インターネットで個別認証手続きをする必要がある．

そして鍵の流通の形態別に，「メディア型」「放送型」「ネットワーク型」と分類できる．既述のCPRMが「メディア型」，CASが「放送型」に対応している．

このようにコンテンツに応じて様々な管理情報が設定されており，機器側はこの情報に従ってコンテンツを扱う必要がある（図1）．また，配信から利用までに1ヶ所でも不正流出する経路があれば，DRMシステム全体の連携に影響を与えることとなってしまう[14]．つまり，コンテンツの正当な受け渡しルールが，記録機器（またはメディア）と再生機器間で設定されることが重要となる．

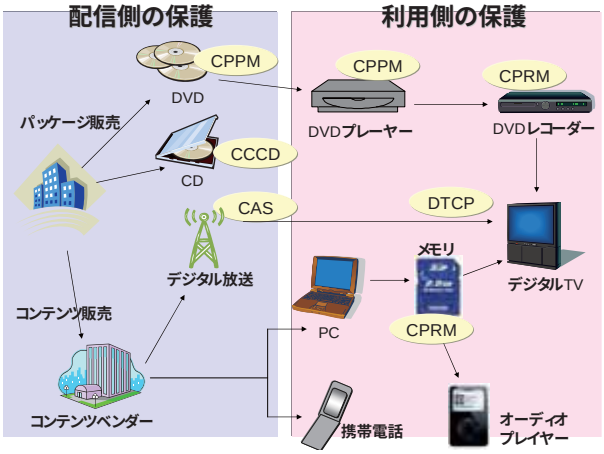


図1．DRMの連結による著作権保護

### 2.2 DRMの問題点

以上のように，現状ではDRMシステムを採用することで著作者の提示する権利を強力に保護することが可能となっている．しかし，不正コピーなどを意図しないユーザにとっては煩わしいだけでなく，今までは許されていたはずの私的な使用の範囲でのコピーも制限されてしまうなど，コンテンツの使用が敬遠される原因ともなってしまう．そこで，デジタルコンテンツの中でも生活に身近な音楽コンテンツとその著作権保護に注目し，適切な著作権保護のあり方を考察する．

## 3　音楽コンテンツにおける著作権保護の現状

まず音楽CDに関しては，現在販売されているほとんどに著作権保護が施されていないため，レンタルしたものからCD-Rを作成し，パソコンを使ってさらに複製を作るということが可能となってしまっている．また，音楽配信サービスでのダウンロード購入も普及し始めており，そのメリットとして一曲単位で購入できる，店に出向く必要がない，品切れすることがない，試聴可能などといった，手軽に音楽を楽しめる魅力がある．しかし，配信サービスが複数存在することで，各サービスに対応する専用のオーディオプレイヤーが必要である場合が多い．さらに，著作権保護のためにデータの形式が乱立することで，目的のコンテンツが入手できないなどといったこともあり，ユーザの混乱を招く要因となっている．

また，特別な例ではあるが，携帯電話の「着うた」市場も今や軽視できないほど大きくなっているといえる．ただし，完全に著作権を保護するために携帯電話本体から全くデータを移動させることができないという点で，極めて利便性が低くなっている．

以上のような音楽コンテンツの著作権保護方法に加え，近年注目されつつあるのが，SDメモリーカードやメモリースティック[8]といった，メモリーを利用したコンテンツ管理である．本研究では特にSDカードに着目し，以下，その概要と可能性を述べることとする．

## 4　SDカードの著作権保護システム

SDメモリーカード（以下，SDカードと呼ぶ）は1999年に松下電器，サンディスク，東芝によって共同開発された[13]．高度な著作権保護機能であるCPRMの仕組みを備えていることもあり，デジタルカメラや携帯端末で利用され，今や半導体メモリーカードのデファクトスタンダードとなっている[13]．DRMの一種であるCPRMに関しては2.1.1で少し触れたが，詳細をここで説明する．

SDカードで扱う音楽データの形式はSD-Audioと呼ばれる独自のものとなる．このSD-Audio形式に対応した機器とSDカードの間で，お互いが4C[9]から認証を受けた正当なものであるかを認証しあう．その後，データの書き込みや再生が行われることとなる．SDカードはコンテンツを格納する「通常領域」以外に，一般的なアプリケーションからはアクセスできない「認証領域」を持つ．また，「MKB（Media Key Block）」「メディアID」「メディアユニーク鍵」といったメディア固有の情報を持っており，これらの情報から，SDカードのコンテンツ保護メカニズムである「メディアバインド」，「無効化」，「相互認証」の3つを実現させている[15]．

まずメディアバインドとは，メディアIDと暗号技術を用いて，不正コピーによるコンテンツや鍵の利用が防止される技術である．図2を用いて，SDカードを利用した著作権保護処理の流れを説明する．ここでは対称暗号を用いていることから，コンテンツを暗号化するための鍵（Kコンテンツキー）は，復号鍵であるともいえる（①）．つまり，このコンテンツキーが正常に得られた機器に関してはコンテンツを再生できることとなる．共有秘密鍵（②）とは記録機器と再生機器が共有して持つ暗号鍵であり，この共有秘密鍵とメディアIDから算出された関数をGとする（③）．記録機器はこの値でコンテンツキーを暗号化し，「暗号化済コンテンツキー」としてSDカードの認証領域に格納する（④）．同時に，コンテンツキーで暗号化されたコンテンツも通常領域に格納する（⑤）．再生機器はメディアIDと共有秘密鍵からGの値を算出し（⑥），認証領域に格納されている暗号化済コンテンツキーを復号化することとなる（⑦）．

これにより，認証領域に格納された「暗号化済コンテンツ鍵」をコピーすることは不可能となる．また，もしこの鍵が何らかの方法で他のメディアに不正にコピーできたとしても，メ

[8] ソニーが提唱・製造している，フラッシュメモリタイプの記録メディア
[9] 4C Entity．IBM，Intel，松下，東芝によってコンテンツの保護規格をライセンスする目的で作られた組織．

ディアIDが異なるため，再生機器はコンテンツキーを正しく復号化することができない．つまり，結果的にコンテンツの不正使用防止が実現される．

次に無効化とは，例えばある特定の機器から鍵情報が漏洩し，コンテンツが不正利用された場合に，以降のコンテンツの利用を禁止させる技術である．SDカードの持つMKB[10]の情報を操作する（⑧）ことで実現される．

最後に相互認証とは，秘密情報を共有する機器間だけにできる方法でデータを交換することで相手を認証する技術である．この仕組みをAKE（Authentication and Key Exchange）という（⑨）．機器とSDカードのAKEによって，両者間のデータ転送が一時的な暗号化によって保護されるため，両者間の通信内容を第三者が傍受することができなくなる．

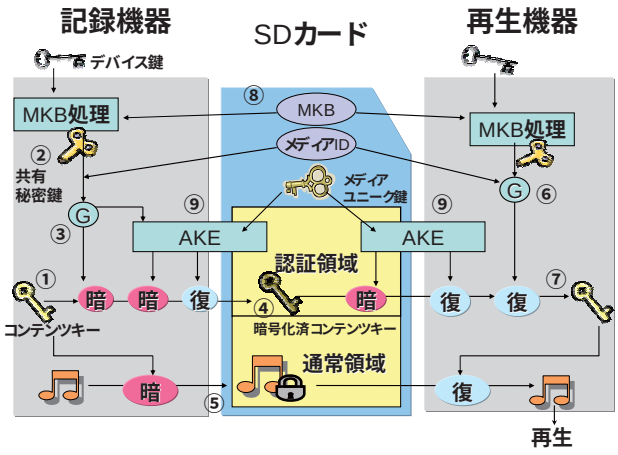


図2．SDカードの著作権保護

## 5　SDカードを利用した音楽配信サービス

### 5.1　MOOCSの概要

SDカードを活用した音楽配信サービスに，ニフティが提供する“MOOCS”（ムークス）がある．MOOCSを利用するには，ユーザはまず専用ソフトの「MOOCS PLAYER」を無料でダウンロードする．そして，CPRMが採用されたこのソフトで音楽の管理や転送を行うこととなる．音楽をSDカードに格納する方法としては，CDから取り込むか，MOOCSの音楽配信サイト（MOOCS MUSIC STORE）からダウンロード購入したコンテンツをSD-Audio形式で保存する方法がある．MOOCS PLAYERからSDカードに曲を転送するには，CPRMに対応したカードリーダ/ライタを使う必要があるが，一度SDカードに格納したデータはSD-Audio対応の機器ならどれでも再生可能となる．最大の利点は，携帯電話をミュージックプレイヤーとして利用できる点ではないだろうか．また，コンビニなどに設置されている専用端末から自分のSDカードにコンテンツを購入するスタイルも提供されており，ユーザの利便性を考慮した環境の提供がされつつある．

[10] Media Key Block．「デバイスキー行列」と「メディアキー」の二つの情報で構成される．特定の機器のデバイス鍵の行列と対応させ，無効データを潰すことで不正機器を排除する．

### 5.2　MOOCSの柔軟性

楽曲の使用の柔軟性に関して，使用制限はレーベルごととなっており，例えば東芝EMIのある楽曲なら“SDカードへの転送が3回，CD-Rへの書き込みは7回”とされている．また，SDカードへの転送はチェックイン・チェックアウトシステムが採用されている．MOOCS PLAYERからSDカードへデータを転送することを「チェックアウト」といい，SDカードに格納されたデータを再びMOOCS PLAYERに戻すことを「チェックイン」と呼ぶ．ムーブ（データの移動）とは異なり，移動元のデータは完全には消去されない．例えば「3回までチェックアウト可能」とされた楽曲があった場合，同時に3枚のSDカードにデータを格納することができる．しかし，SDカードから直接他のSDカードに移動させたり，購入したパソコン以外の機器にデータを移すことはできない．このため，別のSDカードに移し変えたい場合には，チェックインさせることで残りチェックアウトの回数を戻すことが可能となる．

このシステムの問題点は，ダウンロード購入したコンテンツのバックアップをとることが許されていないところである．そのため，パソコンのトラブルやSDカードの紛失などでデータを失った場合の保証はされない．

## 6　バックアップシステムの提案

そこでユーザの利便性向上のために，ダウンロード購入したコンテンツのバックアップを可能とすることで，一度入手したコンテンツが永続的に保障されるシステムを提案する．適切なバックアップの実現のためには，作業をユーザ自身に委ね，データが手元に残るようなシステムであってはならない．手元のデータを必要以上に復元させ，使用することができてしまうため，不正コピーの温床となる恐れがあるからである．そこで，バックアップのデータを有効とするには，現在使用しているコンテンツのデータを完全に使用できない状態とする（＝無効化する）ことが必要条件となる．バックアップシステムのイメージを図3に示した．

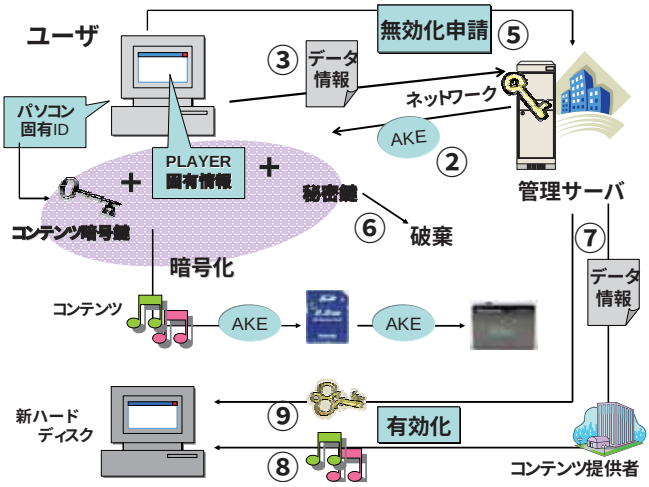


図3．バックアップシステムのイメージ

中澤ゼミ

まず，音楽配信サービスから入手したコンテンツはパソコンの固有ID，プレイヤーの固有情報に加え，管理サーバが提供する秘密鍵で暗号化し，保存することとする（①）．つまり，パソコンで再生させるには，その都度ネットワークを介して管理サーバより秘密鍵を入手することとなる．なお，管理サーバより送信される秘密鍵はユーザに解読されることがあってはならない．この時の鍵情報の保護に関しては，SDカードの著作権保護の一つであるAKEの仕組みを用いることとする．そして，現時点での楽曲データ利用状況（保存楽曲，チェックアウト回数など）の正確な情報をサーバに伝える必要がある（③）．これは，最終的に保有していた楽曲情報に基づいてデータをバックアップさせる際に，ユーザが本来保障されるべきデータ量分だけを正確に提供するためである．例えば，ある3回チェックアウトできる楽曲を2枚のSDカードに格納している状態にもかかわらず，バックアップデータとして再び「3回までチェックアウト可能」な状態で提供することはできない．そして新しいハードディスクにデータを移し変えることが必要となった場合に，データの無効化申請を行い（⑤），管理サーバに秘密鍵を破棄してもらうこととなる（⑥）．これにより，これまでのパソコンでのデータ再生は不可能となる．代わりに新たな保管先での使用を有効化してもらう．具体的には，管理サーバがユーザのデータ情報を楽曲提供者に転送し（⑦），これに基づいた，バックアップデータに相当する新しいコンテンツが提供されることとなる（⑧）．このデータは新たなハードディスクの固有IDとプレイヤーの固有情報，そして新規に生成・発行された秘密鍵によって暗号化され（⑨），管理されることとなる．

本システムでは，バックアップデータや秘密鍵の管理を管理サーバに委ねることで，ユーザの不正を防ぎながらも確実にデータを保障することを可能とした．ただし，再生のたびにネットワークを介さなければならないという点が課題である．さらに，楽曲データの情報を提供することでプライバシーの問題も出てくるであろう．そのため，このバックアップシステムを利用するか否かの判断はユーザに委ねる形とする．

また，ユーザごとのコンテンツ情報が膨大なものになり，管理サーバの負担が大きくなるという問題も予想される．

## 7　むすび

本研究では，ユーザの利便性に考慮したデジタルコンテンツの著作権保護をめざし，SDカードを利用した管理システムに注目した．現在，ある程度柔軟性が高いと思われるMOOCSのサービスにデータのバックアップ保障というシステムを加えることで，よりユーザの利便性を向上させることとした．デジタルコンテンツをSDカードで管理・使用することで，ユーザはあらゆる場面でコンテンツを利用でき，同時に，確実な著作権保護により違法コピーなどの不正は減少するだろう．このようなデジタルコンテンツの使用環境を実現するには，コンテンツの入手にすべてSDカードを利用し，コンビニなどの専用機器，インターネット上の音楽配信，携帯電話の専用サイトから購入する環境が望ましい．つまり，現在Redbookに準拠している，著作権保護が施されない“音楽CD”という規格は将来的には排除されるべきであると考える．今後ますますデジタルコンテンツの市場が拡大していく中で，より著作権保護に重点を置いたコンテンツ市場が形成されなければならない．レーベルの理解や対応機器の普及，および法的な部分での改正も必要となるであろう．しかし，SDカードの将来性からも，著作権に配慮された様々な形式のコンテンツを手軽に楽しむことが可能になると考える．

## 参考文献


[1] “ユーザを不幸にしないコピー・プロテクトかくあるべし，”NIKKEI BYTE，pp.38-55，2003年9月．

[2] http://e-words.jp/w/DRM.html，IT用語辞典e-Words

[3] ディジタル情報流通システム　コンテンツ・著作権・ビジネスモデル，画像電子学会，2005.1

[4] デジタルコンテンツ白書2005，財団法人デジタルコンテンツ協会，2005年8月

[5] http://www.jpo.go.jp/indexj.htm，AVネットワークのコンテンツ保護規格DTCP，特許庁

[6] http://www.houko.com/00/01/S45/048.HTM，著作権法，法庫

[7] 関亜紀子・亀山渉(早稲田大学)，柔軟なコンテンツ流通のためのシステム要件と研究課題，情報処理学会，2003．3

[8] http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h15/html/F1402500.html，情報通信統計データベース「日本発の新IT社会を目指して」，平成15年版　情報通信白書，総務省

[9] http://internet.watch.impress.co.jp/cda/event/2005/12/02/10077.html，安全なコンテンツ流通の鍵は個人認証 Network Security Forum 2005，Internet Watch

[10] http://www.toshiba.co.jp/about/press/2003_07/pr_j1702.htm，プレリリースSDカードを利用したデジタル著作権保護技術の開発について，東芝

[11] http://moocs.com/ NIFTY，MOOCS

[12] http://bb.watch.impress.co.jp/cda/special/11652.html，携帯電話で聴けるニフティの音楽配信「MOOCS」の実力を検証，Broadband Watch

[13] http://www.sdcard.com/japan/，SDメモリーカード総合サイト

[14] 山田尚志・石原淳・加藤拓，“マルチメディア時代のコピープロテクション”，電子情報通信学会論文誌，2004．6

[15] 上林達・下田乾二・坂本広幸，“SDカードのコンテンツ保護”，東芝レビューVol.58No.6，2003

[16] http://kk.rs2.on.tiki.ne.jp/Audio/cccdbase.htm，NO!CCCD