情 報 メ デ ィ ア 36－3
電子化知的財産・社会基盤 7－3
（2000．1．29）

不正コピー防止を考慮したコンテンツ販売システム

上野 正巳 庵 祥子 三宅 延久 武井 英明
NTT情報流通プラットフォーム研究所

概要

電子情報は容易に複製可能という特徴を持っており近年のインターネットの発展と音楽情報圧縮技術の発展は音楽コンテンツの違法コピーという問題を生み出している。本稿ではこのような問題に対処し、利用者の利便性を低下せずに不正コピーを防止するためにはどのような手法が必要か検討し、不正コピーを防止したコンテンツ販売システムである InfoBind の基本的な考え方を述べる。そしてネットワークオーディオ SolidAudio[1]のために実装する際に考慮した点について述べ、最後に本方式の評価を行う。

Prevention of illegal copying in a digital-contents distribution system

Masami UENO Shoko IHORI Nobuhisa MIYAKE Hideaki TAKEI
NTT Information Sharing Platform Laboratories

Abstract

Electronic information is easily reproduced and the development of the Internet and the development digital music compression technology has led to the problem of illegal copying of music. In this paper, we describe a technique that prevents an illegal copying without decreasing the benefit and convenience of this medium to the user. We explain the basic idea of this technique, called InfoBind, and how it is used in a contents sales system to prevent illegal copying. We also evaluate this technique when implemented for SolidAudio[1], a networking audio system.

1. はじめに

デジタルコンテンツには複製が容易に作成できるという特徴があるが、近年のインターネットの普及によりデジタルコンテンツが権利者の承諾無しに複製され、ネット上で公開され問題となっている。また、特に音楽コンテンツにおいては、MP3(MPEG-1/audio layer 3)等の音楽情報圧縮技術が登場したことにより音楽コンテンツの品質をそれほど落さずにデータサイズを小さくすることが可能になったため、権利者に無断で音楽コンテンツを圧縮エンコードしネット上で公開するということが頻繁に行われるようになり、大きな問題となっている。

このような問題があるためコンテンツホルダーは警戒し、ネット上で音楽コンテンツが流通しにくいという現状を作り出している。

本稿ではまず２章でデジタルコンテンツの権利保護に関する問題と方式の検討を行う。次いで３章でネットワークオーディオ SolidAudio 上

[1] SolidAudio は日本電信電話(株)の登録商標です

に実装した著作権保護技術 InfoBind で、上記のような問題をどのように解決しているのか具体的に述べる。４章では InfoBind の評価を行っている。

2. 権利保護方式

ここではネットワークを利用してコンテンツを販売する場合に、著作権者およびユーザの利便性をどのようにバランスさせ確保するかという点に関して、特に音楽コンテンツにターゲットを絞り考察を行う。

2.1. 著作者の権利と著作権の制限

[4]によると著作者の権利は図 1のように著作者人格権と狭義の著作権に分類され、著作者人格権は手放す事が出来ないが、狭義の著作権は財産的なものであり譲渡や相続が可能である。また、著作権には制限が有り、他者が自由に著作物を利用できる範囲が定められている。このため利用者の私的利用や正当な引用に対して権利者は権利を主張する事はできない。現在物理的に流通している著作物を考えた場合でも、上記の条件を満たすようにシステムが形成されている。このことからも、ネット上での音楽コンテンツの流通を考えた場合、これらの著作権、および利用者の権利（図中の点線で囲んだ部分）を両立させたものにする必要がある。

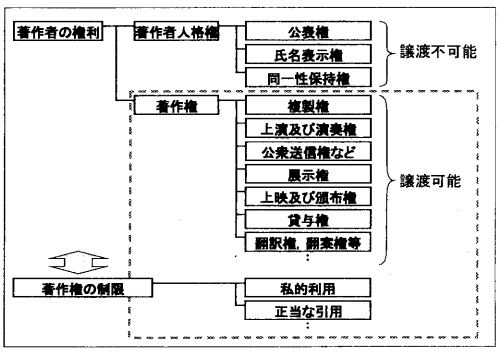

図 1 著作権の分類

2.2. 不正コピーによる権利の侵害

近年のインターネットの爆発的な普及と音声圧縮技術の発展は不正にコピーされた音楽コンテンツの氾濫を招き、従来物理的な媒体での音楽販売を行ってきた業界や著作権者の権利を侵害している。

著作権者から見た場合の、このような問題の原因は次の３点に集約できる。

- 一度デジタル化したコンテンツは容易に複製可能
- 音声圧縮技術により、ネット上での送受信が容易になった
- MP3 等の一般的なファイルフォーマットと対応するアプリケーションの普及

翻って考えた場合、これらは、電子情報流通の利点でもあり、電子情報流通を促進するためには、著作者の権利を保護した上で上記のような特徴を持った電子情報流通を実現する仕組みを早急に整える必要がある。

2.3. 権利保護方式

ネット上での音楽コンテンツ販売において、著作権者の権利を守る方法として従来以下の様な方法が提示されてきた。

- 透かしによる複製の抑止
- ストリーミングによるダウンロード防止
- 暗号化アクセス制御

これらの特徴をまとめると表 1のようになる。

表 1 権利保護方式の比較

方式	不正利用防止	コンテンツの保存
透かし	△ 抑止のみ	○
ストリーミング	○	×
暗号化アクセス制御	○	○

まず、「**透かしによる複製の抑止**」であるが、これは購入時に購入者の情報などをコンテンツ

に透かし込み、複製されたコンテンツがネット上に置かれた場合にそのコンテンツの複製元を判別する事が出来るというものである。この方法はあくまでユーザのモラルに依存した抑止効果しか持っておらず、直接的にコンテンツの複製を防ぐ事はできない。

次に、「**ストリーミングによるダウンロード防止**」である。これはコンテンツを利用する際に、ネットに接続し、プロトコルと音楽再生のためのクライアントプログラムを制限する事により、ユーザにコンテンツを保存させないようにしたものである。この方法を用いた場合、複製は防止できるが、コンテンツを保存できないためコンテンツ利用時に常にネットワークに接続している必要が有り利便性に欠けている。

最後に「**暗号化アクセス制御**」であるが、これはコンテンツを暗号化して配布し、その暗号を解くための鍵を購入したユーザしか利用できないようにする方法である。この方法は暗号化したコンテンツを複製しても鍵を購入しないと利用できないため不正利用を防ぐことは出来るが、鍵情報と暗号化コンテンツの両方を複製されてしまった場合に不正利用されてしまうという問題がある。我々は[3]において PC 上でのコンテンツ利用を前提とした場合の解決方法を提示している。図 2にその方式の概要を示す。

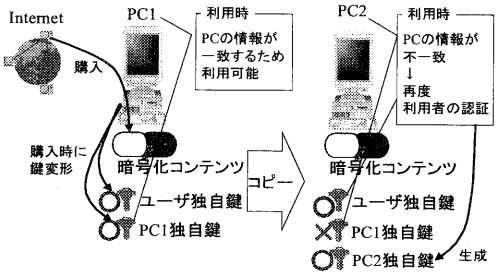

図 2 PC 上での暗号化アクセス制御例

これは、購入者の独自情報すなわち購入者のパスワードと購入者端末(PC)の独自情報を利用して鍵情報を暗号化した上で保存を行い、ユーザが同じ端末(PC)でコンテンツを利用する分には認証不要で、また、別の端末に複製した場合でも購入者のパスワードを入力する事により暗号化コンテンツは利用可能となり、ユーザの利便性と権利保護の両立を図ったものである。SolidAudio で利用した InfoBind は、この方法を発展させ携帯型音楽プレーヤーでの暗号化コンテンツ利用に最適化させたものである。

なお、安全な音楽流通の規格である SDMI[1]においても、音楽コンテンツの保護方法はこの暗号化アクセス制御方式が主流を占めている。

2.4. バインド種別

暗号化アクセス制御方式で、PC 上で暗号化コンテンツの鍵を保存する際に利用者の独自情報を用いて暗号化することにより暗号化コンテンツの複製を防ぐ手法を前項で述べた。このようにコンテンツをある特定条件を満たすものにしか利用できないようにしてしまう方法を、情報をその特定条件にに縛り付けてしまうという意味で、本稿では「バインド」と呼ぶ。携帯型音楽プレーヤー（以下携帯端末と略す）を利用するシーンに登場するものを考えた場合、次の３つのバインド先が考えられる。

- 利用者
- 音楽を再生する携帯端末
- 音楽を記録するメモリメディア

各バインド先によって比較すると表 2のようにまとめることができる。

表 2 バインド種別の比較

方式	コンテンツ保護	使用透過性	コンテンツの移動・可搬性
利用者バインド	○	×認証データの入力が必要	○
端末バインド	○	○ CDと同じ使用感	×端末間での移動性なし
メディアバインド	○	○ CDと同じ使用感	○ CDと同じ可搬性

まず情報を特定の利用者にバインドする「**利用者バインド**」である。利用者バインドを行う場合、鍵は利用者しか知り得ない独自情報を用いてバインドする必要がある。この場合、コンテンツを利用する際に毎回その利用者が正しいのか認証をする必要が有るため、パスワードを入力するなどの作業が発生し、利用者の利便性を著しく低下させる事になる。また、このパスワードなどの利用者独自の情報が、他の利用者に不正使用されないように注意する必要も有る。

次に考えられるのは、携帯端末にそれぞれ固有情報を持たせ、それを利用して鍵を暗号化する「**端末バインド**」である。この場合、鍵の購入処理の際に、携帯端末固有の情報が必要になるため、携帯端末自体がオンラインになりネットワークに接続する必要がある。このため、端末バインドを行う際には通信の為のインターフェイスが必要になり、端末の製造コストが高くなる。また、端末バインドの場合、携帯端末毎にコンテンツを購入する必要があり、携帯端末を買い換えた場合に過去に購入したコンテンツが利用できなくなるなどの問題もある。

そこで、携帯端末に音楽コンテンツの情報を記録するための記憶媒体として小型のメモリメディアを考える。メモリメディアに固有情報を持たせる事により「**メディアバインド**」を実現する事が出来る。この場合、コンテンツ購入時にはメモリの固有情報を読み出すためにそのメディアをネットワーク端末に接続するだけで済み、装置は既存のＰＣとメディアドライブを用いることで安価に提供できる。また、メディアを移し替えるだけでコンテンツを他の携帯端末でも利用できるため、従来からある音楽ＣＤ等と同様の使用感と可搬性を持つことが出来る。更に、購入したコンテンツを他の人にプレゼントする場合でも、コンテンツを記録したメディアのみを渡すだけで済み、購入者、利用者の利便性も音楽ＣＤ等と同等に保たれている。このようにメディアバインド方式を取る事により、ユーザの利便性をできるだけ下げずにコンテンツの保護を行うことが出来る。

音楽コンテンツの利用を想定した SolidAudio では上記の理由から、メディアバインド方式を取ったが、コンテンツの種類や利用方法によってバインドする対象は様々であり、各々のバインド方式の利点を組み合わせて利用することにより、コンテンツの利用形態に合わせた著作権保護を行うことが出来る。

2.5. 記憶メディアの種別

ここで、記憶メディアの種別に関して考察してみる。前述のメディアバインド方式を用いて著作権保護を実現するため、記憶メディア周辺の機能としては

図 3に示すような記憶領域および機能が必要になる。

- データ記憶領域
  暗号化したコンテンツを記憶する領域
- メディア固有ＩＤ記憶領域
  利用者が変更できないメディア固有のＩＤを記録した領域
- 秘匿データ記憶領域
  複号鍵情報やコンテンツの管理に用いる認証されたプログラム等からしか見えない記憶領域

• 認証機能

固有ＩＤや秘匿領域にアクセスする外部のソフトウェアや装置を認証する機能

• 暗号／複号機能

鍵情報を用いてコンテンツを暗号化して格納したり、格納された暗号化コンテンツを復号する処理

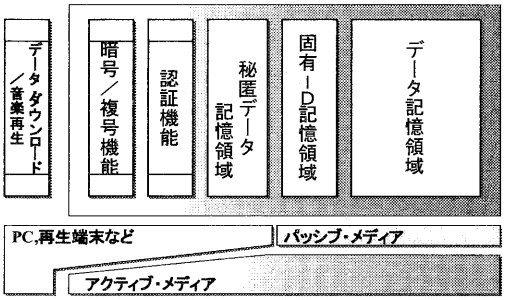

図 3 著作権保護に必要な機能とメディア種別

これらのうち、どこまでを記憶媒体に持たせるのかにより記憶媒体は下記の２種類に区別することが出来る。

- アクティブ・メディア
- パッシブ・メディア

「**アクティブ・メディア**」とは、単純な記憶領域以外にコントロールチップを内蔵しており認証機能や暗号化機能、秘匿領域アクセス機能等を持ったものである。現在発表されているものにメモリースティック[2],SD メモリーカード, セキュア・マルチメディアカード などがある。これはメディア内蔵の認証機能を使用して、認証されたプログラムやハードウェアだけが秘匿領域に鍵情報を書き込むなどの方法で、暗号化コンテンツを保護する事ができる。アクティブ・メディアはメディア自体にこのような機能が盛り込まれているため、比較的容易にコンテンツの複製防止策を実現できる一方で、メディアにコントロールチップを載せているためコスト面で割高になる。

次に「**パッシブ・メディア**」であるが、これは上記アクティブメディアのような認証や暗号化の機能を持つコントロールチップを持たず、単純な記憶領域のみを持つメディアである。但し、本稿で述べているメディアバインド方式のようなコンテンツ保護を行うためにはメディア毎に異なる何らかの固有情報が必要になり、その固有情報は利用者によって書き換えられないものでなくてはならない。SolidAudio で用いた InfoBind 方式では、メディア毎に異なる ID を持った ID 付きスマートメディア[3]にメディアバインド方式を適用してコンテンツの保護を行っている。パッシブ・メディアは、コントロールチップ等を内蔵していないため、アクティブ・メディアに比べてコンテンツを保護するための機能がＰＣや音楽再生端末側に必要になり方式が複雑になる傾向がある。一方コスト面ではアクティブ・メディアに比べて割安になり利用者の負担を軽減できることになる。

3. 実装方法

ここまで述べてきた著作権保護方式に暗号化コンテンツの作成や登録、鍵データの配送までを含めたトータルソリューションとして従来から開発してきた Infoket[2] を拡張する形で InfoBind 方式を開発した。この InfoBind 方式を実際に SolidAudio に適用する際に問題となった点や実装に当たっての考慮点などに関して述べる。

[2] メモリースティックはソニー（株）の商標です

[3] スマートメディア は（株）東芝の登録商標です

3.1. InfoBind の基本方式

まず InfoBind 方式の基本的なデータの流れについて述べる。

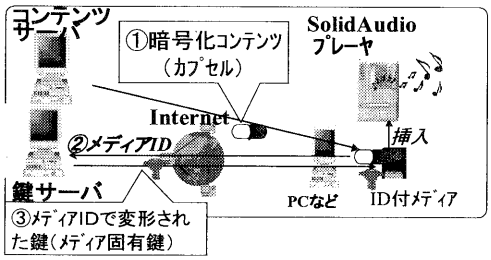

図 4 InfoBind の基本的な配送

図 4のように利用者は暗号化したコンテンツを WWW や CD-ROM などを用いて手もとに入手する。このコンテンツの暗号を解くための鍵は利用者が使用するメディアのＩＤを用いて変形されるため、メディアをＰＣなどに挿入しそのＩＤを鍵サーバに送信する。メディアのＩＤを受け取った鍵サーバはＩＤを利用して、暗号化コンテンツを復号するための鍵を変形して利用者のＰＣに送信し、ＰＣでは暗号化コンテンツと変形されたコンテンツ鍵をまとめてメディアに記録する。

InfoBind では基本的に暗号化の仕組みをＰＣに持たせていない。また、ＰＣ上で再生する手段も現在提供していない。このため、利用者による暗号方式の解析による攻撃が困難になっている。

また、暗号化コンテンツと暗号化された鍵情報をひとつにして記録メディア内に保存している。このデータを復号するにはそのメディアのＩＤが必要であり、複号機能は現在、携帯端末にしか持たせてない。このためコンテンツデータを他のメディアにコピーしてもメディアのＩＤが異なるために再生は不可能である。このために鍵情報をコンテンツと分離することなく一体化して保存していても安全性が確保できている。

3.2. 保護の強度と必要処理能力

小型の携帯型音楽端末で再生する音楽コンテンツはまず音楽情報圧縮のためのエンコードが施され、更にこれをそのまま利用できないように暗号化されたコンテンツが格納されている。音楽再生時にはまず 1)コンテンツの暗号化を復号する処理を行いつつ、2)圧縮された音楽情報を復元する必要がある。これを形態端末内のプロセッサで処理しなければならない。プロセッサで複雑な演算を多く行えばそれだけ多くの電力を消費する必要がある。すなわち音楽圧縮や暗号化コンテンツを復号するための計算量が増えるほど電力の消費が増えることになる。

小型の携帯音楽端末での音楽再生を考えた場合、装置はバッテリーで駆動され、その電源容量には限りがある。プロセッサが行う処理が多ければ多いほど電力の消費が大きくなり、それに反して連続使用可能時間が短くなる。連続使用可能時間は利用者の利便性に関わってくるために、できるだけ長くすることが望ましい。SolidAudio で用いている InfoBind 方式ではコンテンツデータは暗号化と比較的処理量の少ないスクランブルの組み合わせでデータの保護を行っている。実際の携帯端末への実装に際しては、ここで述べたようなバランスを考慮しつつ暗号強度とスクランブル処理のバランスを設定した。

また、InfoBind 方式ではコンテンツの暗号化方式は可変になっており将来バッテリーの電源容量ややプロセッサの処理能力が増した場合に、より強力な暗号を用いることができ、暗号化方式が万一破られたでも別の暗号化方式に変更することで、鍵配送などを含めたシステム全体が破綻するのを防いでいる。

3.3. 保護のレベル

電子情報流通が活発になると複数の利用者や業者が配信に関わることになり、悪意を持った

攻撃が行われる可能性も高まる。InfoBind 方式では鍵情報や暗号化方式の解析や漏洩による多様な攻撃に備えるために複数の保護レベルを設けて、万一鍵情報などが漏れた場合でもコンテンツホルダーが受ける被害を最小限に抑えることが出来るようになっている。InfoBind 方式で設けた二つの保護レベルについて述べる。

3.3.1. 配信業者別の鍵による保護

複数の配信業者が本システムを利用した場合、本方式では鍵データの配送時に鍵サーバ側で利用者のメディアに合わせた鍵データの暗号化が行われるため、鍵データのソフトウェアを逆行分析され、暗号化の方式を解析されて悪用されてしまうという脅威がある。この脅威に備えて、InfoBind システムでは配信業者毎にＩＤを発行すると共に、暗号化のための鍵データを発行するようになっている。配信業者毎に鍵が異なるために、ある配信業者が鍵を解析し悪用しようとしても、同じ鍵は他の配信業者の暗号化には適用できないため、他の配信業者のコンテンツに被害を与えることはできないようになっている。また、配信業者以外によって解析が行われた場合でもその被害の範囲を特定配信業者だけに抑えることが出来る。

3.3.2. 配信メディア別の鍵による保護

2.1でも述べたように、著作物は私的利用が認められており、従来からもＣＤをカセットテープに録音し私的に聴くな行為は私的利用の範囲内として認められていた。SolidAudio でも利用者の利便性を考慮し、私的録音を実現するために利用者が購入したＣＤから SolidAudio で再生できるデータを作成できるが、このような私的録音の場合でもメディアバインドを行うようになっている。このため、InfoBind の鍵暗号化のシステムがエンコードを行うＰＣ上にも存在し、利用者に提供されている鍵の暗号化方式がソフトウェアの逆行分析などにより解析されてしまう脅威がある。

万一ＰＣ上での鍵の暗号化方式が解析された場合でもネットワーク上で販売されているコンテンツが影響を受けないように、私的録音の際にコンテンツ鍵を暗号化するための鍵を、ネットワーク配信で用いる鍵とは別のものにしている。

これにより、万一私的録音の鍵情報が解析された場合でもネットワーク販売されているコンテンツには影響を及ぼさないようになっている。

この鍵種別は私的録音を含む配信メディア別の鍵種別として位置付けられ、現在本方式を用いた音楽情報販売はインターネットを通じて販売する方式のみが実際に提供されているが、将来他のメディアによる音楽販売が行われた場合でも同様に別の鍵を用いることができるため、特定のメディアでの販売に用いる鍵が暴かれた場合でも、他のメディアでの販売に及ぼす影響を最小限に抑えることができる。

3.4. 鍵配送方式

コンテンツを復号する鍵をネットワーク配送する場合、ユーザ側ＰＣの成りすましや、鍵サーバの成りすましによって鍵を盗聴される攻撃にも備える必要がある。

InfoBind では鍵の配送に際してセキュアな通信路を確保するために http 上に公開鍵ベースの独自のプロトコルを設けている。これにより鍵の配送途中の攻撃にや盗聴を防ぐと共に、http ベースのプロトコル採用により広い環境での利用が可能になっている。

3.5. 運用系とセキュリティの確保

トータルなシステムとして音楽情報販売を考えた場合、販売のシステムのみではなく決済系とのインターフェイスや、暗号化コンテンツの作成からサーバへの登録までの機能を持つ必要

がある。InfoBind では決済系との連携のためのインターフェイスを持たせるとともに、暗号化コンテンツの作成やサーバへのコンテンツや鍵の登録を複数のＰＣから行うことが出来る。複数のＰＣで暗号化コンテンツの作成が可能になるため、音楽圧縮エンコードやコンテンツの暗号化処理の負荷を分散させることが出来る。

鍵の登録に際しては認証に加えて公開鍵方式ベースのセキュアな通信を用いるため、情報提供者側においてもコンテンツの改竄や盗聴を防いでいる。

4. 評価

不正コピー防止を考慮したコンテンツ販売システムとしてInfoBind 方式の開発を行った。本方式は図 5のような攻撃を想定し対処している。

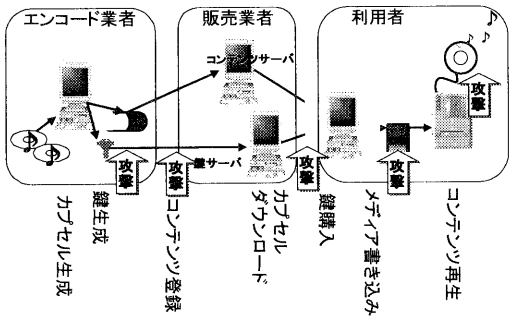

図 5 攻撃方法

それぞれに対する本方式での防御の有無を表3に示す。本方式ではPC 上で再生を行った場合に安全にコンテンツを守る手法が確立していないという考えに基づき、現状では PC 上での再生を実装していない。また、アナログ出力による盗聴は音楽の圧縮に非可逆圧縮方式を用いていることもあり、オリジナルよりも少しずつ劣化していく点、デジタルではないため更にコピー行為によって品質が劣化していく点などを考慮し、特別な防止対策は打っていない。

表 3 攻撃に対する防御

攻撃対象	攻撃方法	防止効果
カプセルと鍵データ暗号化方式	カプセル改竄	○
	カプセル不正コピー	○
	鍵データ改竄	○
	鍵データ不正コピー	○
	暗号化方式解析	△
登録処理	鍵サーバ成りすまし	○
鍵データ購入	鍵サーバ成りすまし	○
記録メディア上のコンテンツ	コンテンツ改竄	○
	カプセル改竄	○
PC上での再生	復号方式の解析による盗聴	−
プレーヤー	アナログ出力の盗聴	×

5. おわりに

不正コピー防止を考慮したコンテンツ販売システムとしてInfoBind方式を開発しSolidAudio用の音楽コンテンツ販売に適用した。今後は音楽以外のメディアやストリーミング等の配布形態にも対応を行ってゆく予定である。

参考文献

[1] SDMI: SDMI Portable Device Specification Ver1.0,1999.7

[2] 明石,森保,寺内:FleaMarket 方式による情報流通システム, 情報処理学会論文誌 Vol 39 No.2(1998.2)

[3] 庵,玉井,三宅,曽根岡:不正コピー防止を考慮したコンテンツ販売方式,マルチメディア通信と分散処理研究会,1999.1

[4] 社団法人 著作権情報センター Web ページ http://www.cric.or.jp/