電子化知的財産・社会基盤 11－9
（2001. 2. 24）

自由度の高い私的コピーを実現する著作権保護方式

藤井治彦 武井英明 中里加奈 庵祥子 三宅延久

NTT 情報流通プラットフォーム研究所

近年、音楽配信などインターネットを介したコンテンツ流通ビジネスの発展に伴い、著作権保護方式の重要性は増している。しかし、従来の著作権保護方式は、コピー制限など、ユーザの自由度を制限するものが多く利便性が低い。本稿では、再生装置とコンテンツに所有者証明情報を付加し、両者の所有者が等しい人物であると証明できた時のみ再生する方式を提案する。本方式を用いれば、従来のようにコンテンツに対するコピー制限などが不要となり、共有（複数の再生装置間でのコピー）、購入（配信サーバから再生装置などへのコピー）、再発行（コンテンツを誤削してしまった場合の再ダウンロード）といった操作の利便性を向上させることができる。

A New Method of Copyright Protection Enabling Less Restricted Personal Copy

Haruhiko FUJII Hideaki TAKEI
Kana NAKASATO Shoko IHORI Nobuhisa MIYAKE

NTT Information Sharing Platform Laboratories

The contents distribution business such as music distribution has recently expanded. But exiting copyright protection methods have many restrictions such as restricting the number of copies, so their usability is low.
This paper describes a new type of copyright protection method. In this method, the certificate issuer attaches owner information to the contents player at first, and the contents server also attaches owner information to the content. The user is permitted to view or listen to the content only when the two pieces of owner information show the same person. This method allows the user to purchase and copy contents among several players easily and allows the reissue of contents by the server easily.

1. はじめに

近年、インターネットのブロードバンド化につれて音楽配信などが急速に発展しており、著作権保護方式の重要性は増している。従来のパッケージ流通での著作権保護方式では、主にコピー禁止を実現すれば良かったが、現在のように、インターネットを介するノンパッケージ流通では、コピーに関する操作が必要になってくる。コピーに関する操作としては①共有（端末から携帯端末などへのコピー）、②購入（配信サーバから端末へのコピー）、③再発行（誤削除もしくは端末の故障時など、配信サーバから端末への再コピー）などが挙げられる。

これに対し、商用化されている主な著作権保護方式では、①共有に関しては、禁止もしくは煩雑な操作を介して回数制限を課した上でしか実現できていなかった。また②購入に関しては、購入用の専用ソフトがインストールされた端末からでしか購入できないであるとか、購入した端末上でしか再生できなかった。また③再発行に関しては、禁止されていたりするものが多い等の問題点があった[1]。

今日、一人の人間が会社や自宅のPC、携帯電話など様々な再生・購入端末を持つことや、コンテンツの誤削除、PCの故障や買い替え等を考慮すると、上記コピー関連操作の不備は、ユーザ側から見ると「買いにくく、使いにくく、いつかは視聴できなくなる。」となり、CDや不正MP3の方が良いということになる。

本稿では、このような課題を解決するために、図1のように再生装置購入時などに所有者証明情報を再生装置に記憶させ、さらに、コンテンツ購入時にも所有者証明情報をコンテンツに付加させ、再生時には、両情報をチェックして、両者が同一の人物の所有物であることを証明できれば再生を許可するという著作権保護方式を提案する。

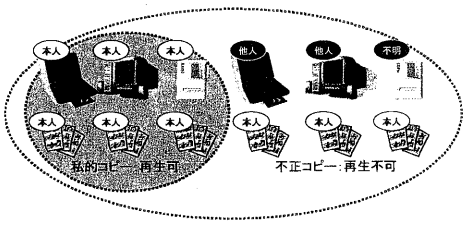


図1　提案モデル

本方式は、コンテンツのコピーを行っても不正使用が出来ないので共有・購入・再発行操作の自由度を上げ、利便性を高めることができる。また、従来方式のようにコンテンツのコピー制限機構などが必要ないので、比較的簡易な装置環境で実現可能となる。

以下、2章ではコピー操作が考慮された著作権保護方式についての関連研究を紹介し、3章では利便性の高い著作権保護方式のための要求条件を示す。4章では提案方式の説明を行い、5章では提案方式の実装について述べる。6章では要求条件についての検討・評価を行う。最後の7章では、まとめと今後の課題を述べる。

2. 関連研究

コンテンツの著作権保護方式は、これまで活発に議論が行われてきた[2,3,4,5]。音楽配信などのネットワーク配信型コンテンツに適し、コンテンツの私的コピーが可能な著作権保護方式の中で主なものとしてSDMI方式（SDMI準拠著作権保護方式）がある。

2．1. SDMI方式

米国レコード協会(RIAA)を中心とした団体であるSDMI(Secure Digital Music Initiative)[3]によって検討されている規格で、これに準拠した著作権保護方式としては、MagicGate/OpenMG ☆[4]などが有名である。

MagicGate/OpenMGでは、CPU付メディアを用いコピー回数制限を課す事によって著作権保護を実現しているため、コピーの度にチェックイン・チェックアウトなど煩雑な操作が必要である。また購入時使用した端末以外ではコンテンツの再生ができないので端末の買い替えを行うと全てのコンテンツが再生できなくなる。また、購入したコンテンツを誤削除した場合、コンテンツの再発行は原理的に困難であって実際サポートされていない。なぜならば、コンテンツを紛失していないのに、紛失したと嘘をついて再発行される可能性があり、ユーザはコンテンツを2個不正に保有することができ、コピー可能回数が2倍になり、コピー回数制限の意味が無くなってしまうからである。

☆MagicGate/OpenMG は,ソニー(株)の登録商標です.

3．要求条件

本章では、以上の問題点を踏まえ、音楽配信などのコンテンツ流通に適する著作権保護方式の要求条件を、以下のように定義する。ただし、以降、視聴権という言葉を用いるが、コンテンツを視聴する権利もしくは、それを証明するデータのことを指す。

(A1)不正使用防止

視聴権の偽造や譲渡が困難であること。これは、著作権保護方式の基本的な要求条である。例えば、シェアウェアのパスワードのように、視聴権を単純に特定の文字列のみにしてしまうと、①第三者が視聴権（パスワード）を何パターンも試すことにより比較的容易に偽造ができてしまう。また、②正当なユーザが視聴権（パスワード）を大量に不正コピーして再配布する可能性もある。特に音楽配信ビジネスでは②は起り易く必ず防止されなければならない。

(A2)共有

視聴権の私的コピーが可能であること。何台もの PC や小型端末を所有している人が多くなってきていることや、PC の買い替えを考慮すると共有は重要となる。

主な SDMI 方式では、煩雑な操作を介することにより、PC と CPU 付きメディア間での回数制限付きコピーを実現しているが、PC の買い替えを行うと、全てのコンテンツが視聴できなくなる。これは(A1)不正使用防止を強めた結果であるが、この点に不満を持つユーザは多い[1]。

(A3)購入

視聴権の購入がしやすいこと。現行の主な商用サイトは、購入端末に特別なソフトや装置がないと購入ができなかったり、購入時に用いた端末上でしか再生ができなかったりする。これは、購入時にコンテンツに対して(A1)不正使用防止の機能をつけるためであるが、コンテンツの販売形態を狭める原因となっている。

(A4)再発行

視聴権の再発行が可能であること。これはコンテンツが誤削除や PC の故障などにより完全に消えてしまった場合でも、無料で再ダウンロードが可能であることを言う。現行の主な商用サイトは、再発行を許可していない。これは前章でも述べたように再発行を許可すると、ここがボトルネックとなりシステム全体の著作権保護レベルを下げることになるからである。

4．提案方式

本稿で提案する所有者証明手法[5]による著作権保護方式の説明を、前提条件、構成要素、操作手順の順で説明を行う。

4．1．前提条件と各構成要素

本方式の4つの構成要素である、証明書発行局と、配信サーバと、再生装置と、任意の端末の特徴・役割を記す。

前提条件

- 証明局、配信サーバの内部処理は非公開とする
- 再生装置には耐タンパ性があるとする

証明書発行局(Certificate Issuer:CI)

再生装置(PL:後述)の所有者を証明する情報である所有者証明情報(C(sid,uid))を発行する。

ただし、uid は一意に個人を特定する情報である個人識別情報を表し、sid は一意に再生端末(PL)を識別する装置識別情報を表す。

配信サーバ(SHop:SH)

ユーザから個人識別情報(uid)を受付、それをもとに、次節で示す配信手順を用いて、暗号化されたコンテンツと復号鍵を含むデータであるカプセルコンテンツ(CCO(uid))の配信・課金を行う。ただし、本稿では、著作権保護方式の説明が主眼であるので、課金部分についての考察・実装は省略する。

再生装置(PLayer:PL)

ユーザの不正な操作ではアクセス不可能なアクセス制御領域を持ち、その中に装置識別情報(sid)を格納することができる。再生時に、装置識別情報(sid)と、所有者証明情報(C(sid,uid))と、カプセルコンテンツ(CCO(uid))を読み込める機能を持ち、次節で説明する再生手順を、耐タンパー機構内の処理にて行える機能を持つ。

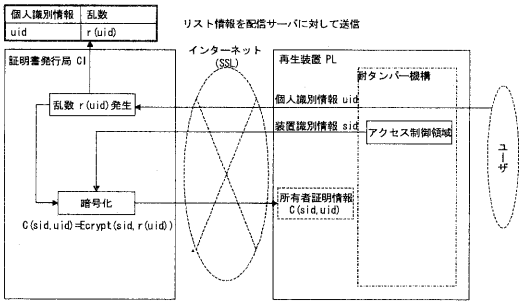


図3　再生装置の所有者証明情報発行

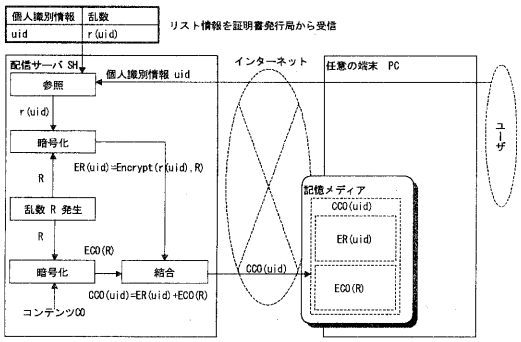


図4　コンテンツ購入

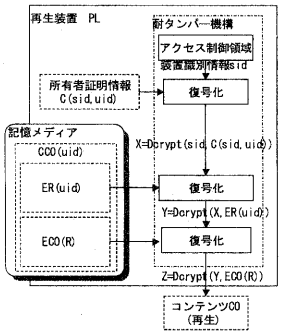


図5　コンテンツ再生

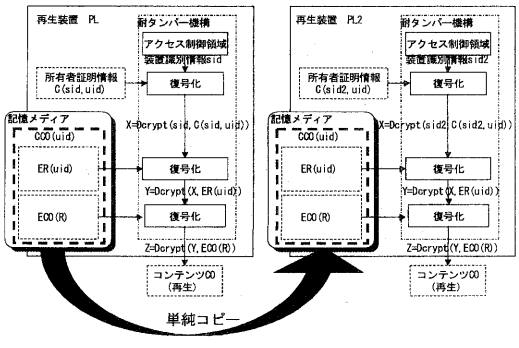


図6　私的コピー

任意の端末(Personal Computer:PC)

個人識別情報(uid)の入力をユーザから受け付けて配信サーバ(SH)に送信が可能であり、カプセルコンテンツ(CCO(uid))のダウンロードができる機能を持つ。

4．2．各種手順の詳細

本方式の 4 つの操作である、再生装置の所有者証明書発行手順と、コンテンツ購入手順と、再生手順と、私的コピー手順を示す。また、この説明図を図 3～6 に示す。
ただし、以下の定義を行う。

- Ecrypt(x,y)は鍵 x で平文 y を暗号化することを表す
- Dcrypt(x,y)は鍵 x で暗号文 y を復号化することを表す
- x+y はデータ x とデータ y の結合を表す

再生装置の所有者証明発行手順　(頻度：小)

本操作(図 3 参照)は、再生装置(PL)1 台に付き 1 回行えば十分である。例えば、再生装置(PL)を購入した時のみに行えばよい。ただし本手順における構成要素間通信は、盗聴不可能な秘密通信を用いる。

(B11)再生装置(PL)をインターネットに接続し、証明書発行局(CI)に接続する。

(B12)ユーザは、証明書発行局(CI)にログインしてから、再生装置(PL)の装置識別情報(sid)と、個人識別情報(uid)を送信する。
ただし、本操作は、セキュリティー性を高めるために装置識別情報(sid)の読み取りを、耐タンパー機構の内部処理にて行わせることができる。

(B13)証明書発行局(CI)は、個人識別情報(uid)を判定し、まだ一度も使用されていない個人識別情報(uid)ならば、第 1 乱数(r(uid))を発生させ、表 2 に示すリスト情報(L)を作成して、証明書発行局(CI)内部で保管すると共にリスト情報(L)を配信サーバ(SH)に送信する。個人識別情報(uid)が既に使用されているものならば、保管してあるリスト情報(L)を参照して対応する第 1 乱数(r(uid))を読み込む。図 3 には新規の個人識別情報(uid)が使用された場合のモデルを示す。

(B14)証明書発行局(CI)は、以下の計算により所有者証明情報(C(sid,uid)) を作成する。

C(sid,uid)＝Ecrypt(sid,r(uid)) (1)

(B15)証明書発行局(CI)は、再生装置(PL)に所有者証明情報(C(sid,uid))を送信し、再生装置(PL)は所有者証明情報(C(sid,uid))を記憶する。

表 2 リスト情報

個人識別情報	第 1 乱数
uid	r(uid)

コンテンツ購入手順 (頻度：中)

本操作は、コンテンツ購入毎に発生する。特定の端末からではなく任意の端末(PC)から購入でき、購入したカプセルコンテンツ(CCO(uid))は任意の記憶メディアに保存できる(図 4 参照)。

(B21)ユーザは、任意の端末(PC)から配信サーバ(SH)に接続しログインを行う。

(B22)購入するコンテンツを選択し、課金処理(本稿では、この部分の考察は省略する)後、個人識別情報(uid)を入力する。ただし、ログイン時の ID と個人識別情報(uid)が等しい場合は、個人識別情報(uid)の入力は省略できる。

(B23)配信サーバ(SH)は、事前に証明書発行局(CI)から送信されてきて内部で保管してあるリスト情報(L)を参照し、入力された個人識別情報(uid)に対する第 1 乱数(r(uid))を読み込む。

(B24)配信サーバ(SH)は、新たに第 2 乱数(R)を発生させ平文のコンテンツ(CO)を暗号化し暗号コンテンツ(ECO(R))と暗号化復号鍵(ER(uid))を生成する

ECO(R)=Ecrypt(R,CO) (2)

ER(uid)=Ecrypt(r(uid),R) (3)

(B25)配信サーバ(SH)は以下の計算を行い、カプセルコンテンツ(CCO(uid))を生成する

CCO(uid)=ER(uid)+ECO(R) (4)

(B26)配信サーバ(SH)は、端末(PC)にカプセルコンテンツ(CCO(uid))を送信する。

再生手順 (頻度：大)

事前に任意の端末(PC)から、カプセルコンテンツ(CCO(uid))を、再生装置(PL)にコピーしておく。本方式では、再生・コピーにおいて IC カードの挿入であるとか、パスワードの入力は不要である(図 5 参照)。

(B31)再生装置(PL)は、装置識別情報(sid)と、カプセルコンテンツ(CCO(uid))を読み込み、暗号コンテンツ(ECO(uid))と、暗号化復号鍵(ER(uid))を取り出す。

(B32)式(1)～(3)より以下の計算を行う

＃第 1 乱数(r(uid))の復元

X =Dcrypt(sid,C(sid,uid))

=Dcrypt(sid,Ecrypt(sid,r(uid)))

=r(uid) (5)

＃第 2 乱数(R)の復元

Y =Dcrypt(X,ER(uid))

=Dcrypt(r(uid),Ecrypt(r(uid),R))

=R (6)

#コンテンツ(CO)の復元

Z =Dcrypt(Y,ECO(R))

=Dcrypt(R,Ecrypt(R,CO))

=CO (7)

式(5)～(7)は、再生装置(PL)の所有者証明情報(C(sid,uid))が発行される時に使用された個人識別情報(uid)と、カプセルコンテンツ(CCO(uid))の購入時に使用された個人識別情報(uid)が等しい時のみ再生が可能であることを示している。

私的コピー手順 (頻度：中)

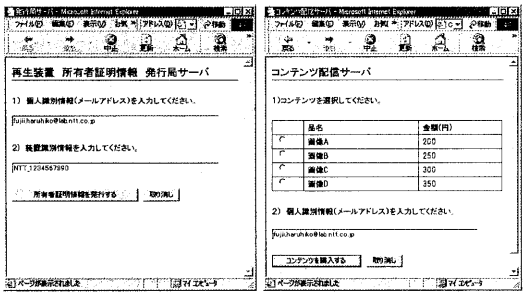
図 6 のように、予め装置識別情報(sid2)である再生装置(PL2)に対して同一の個人識別情報(uid)で所有者証明情報(C2(sid2,uid))は事前に発行されているものとする。また、上記再生手順で使用したカプセルコンテンツ(CCO(uid))を私的コピーするものとする。

再生手順でも説明したように、所有者証明情報(C2(sid2,uid))と、カプセルコンテンツ(CCO(uid))に使用されている個人識別情報(uid)は等しいから単純にコピーしただけで再生が可能であり、MagicGate/OpenMG のような特殊なコピー専用手段やコピー回数制限は不要である(図 6 参照)。

ここで、異なる個人識別情報(uid2)の所有者証明情報(C(sid2,uid2))を持つ再生装置(PL2)にコピーしても、式(5)において正しい第 2 乱数(R)が出てこないので再生は出来ない。

また、所有者証明情報(C(sid,uid))とカプセルコンテンツ(CCO(uid))をセットにして、他の再生装置(PL2)にコピーしても、式(4)において正しい第 1 乱数(r(uid))が復号されないから再生は出来ない。

つまり、第三者に譲渡するには、再生装置(PL)と所有者証明情報 C(sid,uid)とカプセルコンテンツ(CCO(uid))の 3 つをセットにする必要がある。



(a) (b)

図7 発行局サーバ(a)と、配信サーバ(b)

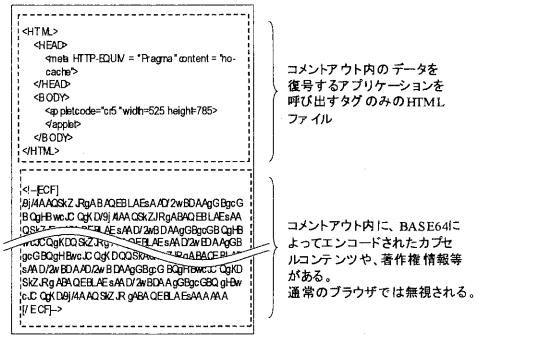


図8 カプセルコンテンツのフォーマット

図9 再生アプリケーション

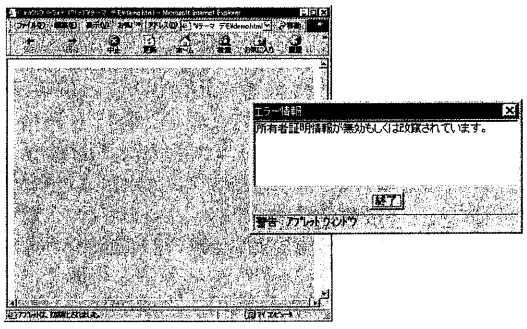


図10 不正使用時の動作画面

3. 実装

前章で述べた提案方式に基づきシステムの構築を行った(図 7～10 参照)。対象とするコンテンツの種類は画像とし、再生アプリケーションは、Internet Explore など WEB ブラウザをビューワーとして利用した。復号化部分は JAVA を利用し Windows98 上で実装を行った。また、所有者証明情報(C(sid,uid))の発行局サーバ(CI)と、コンテンツ配信サーバ(SH)は、WEB サーバをたて CGI として実装を行った。また、再生装置(PL)の装置識別情報(sid)は、「固有 ID ファイル」を置くことによりエミュレートを行った。

再生装置の所有者証明発行

WEB ブラウザで、発行局サーバ(CI)(図 7(a)参照)を開き、個人識別情報(uid)としてメールアドレスを入力し、装置識別情報(sid)を固有 ID ファイルから読み取り入力する。

入力を受け付けると、発行局サーバ(CI)は、第 1 乱数(r(uid))を発生させ、装置識別情報(sid)を鍵として、第 1 乱数(r(uid))を DES で暗号化する。出力されたデータは、さらに BASE64 でエンコードされ、指定されたメールアドレスに添付ファイルとして送付する。

また、発行局サーバ(CI)は、第 1 乱数(r(uid))とメールアドレスのリスト情報(L)を配信サーバ(SH)(図 7(b))に通知する。

コンテンツ購入

コンテンツの配信サーバ(SH)を開き、希望するコンテンツツ(CO)を選択後、メールアドレスを入力する。ただし、本実装では課金処理部分は省略した。本方式では、コンテンツ購入する端末(PC)は任意であるので、WEB ブラウザさえあればよく、コンテンツのダウンロード専用ヘルパーソフトウェアも必要ない。入力が終了すると、配信サーバ(SH)は前記配信手順に従いカプセルコンテンツ(CCO(uid))を生成する。ただし、暗号手法として DES を用い、生成されたカプセルコンテンツ(CCO(uid))は BASE64 にてエンコードされ、更に図 8 に示すようフォーマットに整形されて配送される。配送方式は 2 種類あり、ダウンロード配信オプションが選択されているとダウンロードになり、メール配信オプションが選択されているとカプセルコンテンツ(CCO(uid))がメールで添付ファイルとして配信される。

再生

カプセルコンテンツ(CCO(uid))は、HTML ファイルであるので、表示させるには、アイコンをダブルクリックをする等、通常の HTML ファイルと同様の操作を行って表示が可能である。表示時に、復号化アプリケーションが起動され、装置識別情報(sid)や所有者証明情報(C(sid,uid))のチェックを行い、これらを元に復号を行う。図 9 のように、表示される画像には、①視聴権情報(本実装では個人識別情報(uid)：メールアドレスとした)、②著作権情報、③コンテンツ ID、④装置識別情報(sid)が、元画像の上に表示され、画面のハードコピーによる現画像の不正コピーを抑止している。また、「画面詳細情報」ボタンを押すと、ウィンドウが開き、更なる詳細情報が表示される。

私的コピー・不正コピー

カプセルコンテンツ(CCO(uid))のコピーは、通常のファイルと同様、単なるコピーコマンドで実現できる。ただし、再生装置の所有者証明情報(C(sid,uid))は、他の再生装置(PLx)にコピーしても無効となる。よって、私的コピー(同一の個人識別情報を表す所有者情報がある再生装置間コピー)では、図 9 のように再生が可能であり、不正コピー(同一の個人識別情報を表す所有者証明情報を持たない再生装置間コピー)では、図 10 のように、再生アプリケーションは、エラー情報を表示する。

6．検討・評価

本方式を、先に示した要求条件の観点などから検討・評価を行う。

6．1．要求条件における検討

(A1) 不正使用防止

本方式では、視聴権をカプセルコンテンツ(CCO(uid))と、所有者証明情報(C(sid,uid))と、装置識別情報(sid)とに分散する。

カプセルコンテンツ(CCO(uid))の復号に用いられる第 1 乱数(r(uid))と第 2 乱数(R)は、個人識別情報(uid)と関連性が無い情報であり、また、配信サーバ(SH)内部の暗号化手法は非公開なので、カプセルコンテンツ(CCO(uid))を不正に復号化するのは困難といえる。

また、所有者証明情報(C(sid,uid))も、同様に個人識別情報(uid)と関連性の無い第 1 乱数(r(uid))を用いて装置識別情報(sid)を暗号化することと、証明書発行局(CI)内部の暗号化手法は非公開であることと、証明情報発行時は秘密通信を用いることを考慮すると所有者証明情報(C(sid,uid))の偽造も困難である。

また、再生装置(PL)は、耐タンパー性を前提条件としているので、装置識別情報(sid)もなりすまして使用することが困難となる(図 5 参照)。

また、カプセルコンテンツ(CCO(uid))には、何らコピー制限を課してはいない。よって、カプセルコンテンツ(CCO(uid))は、第三者に不正譲渡されることも想定している。もし不正譲渡が行われた場合、式(5)～(7)において、第三者の装置識別情報と個人識別情報をそれぞれ sid2,uid2 とすると

＃第 1 乱数(r(uid))の復元

$$X = Dcrypt(sid2,C(sid2,uid2)) = Dcrypt(sid2,Ecrypt(sid2,r(uid2))) = r(uid2) \quad (8)$$

＃第 2 乱数(R)の復元

$$Y = Dcrypt(X,ER(uid)) = Dcrypt(r(uid2),Ecrypt(r(uid),R)) \neq R \quad (9)$$

#コンテンツ(CO)の復元

$$Z = Dcrypt(R',ECO(R)) = Dcrypt(R',Ecrypt(R,CO)) \neq CO \quad (10)$$

となるため、カプセルコンテンツ(CCO(uid))の復号ができない。

また、所有者証明情報(C(sid,uid))とカプセルコンテンツ(CCO(uid))が両方第三者に渡ったとするとしても式(5)において

＃第 1 乱数(r(uid))の復元

$$X = Dcrypt(sid2,C(sid,uid)) = Dcrypt(sid2,Ecrypt(sid,r(uid))) \neq r(uid) \quad (11)$$

となり、これ以降のカプセルコンテンツ(CCO(uid))の復号化が出来ない。

つまり、不正譲渡を行うには、再生装置(PL)と所有者証明情報(C(sid,uid))とカプセルコンテンツ(CCO(uid))の 3 つをセットにして物理的に譲渡する必要がある。しかし、現在商用化されている主な音楽配信においても、再生装置や記憶メディアとコンテンツをセットすれば第三者に物理的に譲渡が可能であることから、この点に関しては、他の方式とほぼ同等レベルであると言える。

(A2)共有

本方式では、先述したように、カプセルコンテンツ(CCO(uid))に対してコピー制限は一切課していないため、共有(再生装置間でのコピー)は、MP3と同様に無制限かつ特殊なソフト不要で単純なコピーコマンドで行える。よって多くのユーザが不満を持っていた点である、コピー回数制限や、共有操作の煩雑性や、PCを買い換えると視聴できなくなるということは解消され、LANやネット上のサーバに音楽ファイルを置いて使用したり、CD-Rにコピーして保存したり、頻繁に携帯プレーヤに出し入れして視聴する等、MP3とほぼ同様の使い方ができる。

(A3)購入

本方式では再生装置の登録を厳重に行えば、コンテンツの購入は簡略化できる（ただし、本稿においては課金部分は考慮していない)。なぜならば、もし、購入者が不正に他人の個人識別情報(uid)を使用して購入したとしても、その個人識別情報(uid)のついている再生装置(PL)は入手できないので再生することが出来ない。同様に、カプセルコンテンツ(CCO(uid))をダウンロードしているときに盗聴されても不正使用できないので秘密通信をする必要さえない。

よってコンテンツの購入は任意の端末から行え、本実装のようにメール配送という形態をとることもできる。

また、再生装置の厳重認証の具体案としては、携帯電話のように、再生装置購入時に店頭にて免許証を提示して本人確認を行った上で登録を行うという手法が考えられる。

(A4)再発行性

前述したように従来方式では、視聴権の再発行を可能にすると、大量に不正再発行される危険性があった。

本方式では、視聴権(カプセルコンテンツ(CCO(uid)))の再発行は、(A2)共有と同様に無制限に行っても問題はない。また、再発行時の本人認証も(A3)購入と同様に、厳重なものでなくても不正使用は防止できる。

ただし、新しい再生装置(PLx)に対して所有者証明情報(C(sidx,uid))を再発行する場合は課題が残る。一人あたりの登録できる再生装置数の上限を決めておかないと、大量に再生装置(PLx)を登録して、大量のカプセルコンテンツ(CCO(uid))と共に不正に再販売するという犯罪が成立するからである。この点の対処は今後の課題とする。

6．2．関連研究との比較

表2に、①SDMI方式と、②MP3など(著作権保護機能がないもの)と、本稿で述べた③所有者証明手法について、上記要求条件(A1)～(A4)の観点から比較を行う。表に示す通り(A1)不正使用防止はSDMI方式と同レベルであり、(A2)共有、(A3)購入、(A4)再発行はMP3などと、ほぼ同レベルなっている。ただし、MP3などにおける購入は不正ダウンロードを意味し、再発行は再不正ダウンロードを意味するものとする。

表3　関連研究と本研究とMP3等との比較

	(A1)	(A2)	(A3)	(A4)
	不正使用防止	共有	購入	再発行
SDMI方式	○	△制限、煩雑	△特定端末	×困難
MP3など	×	○無制限	○任意端末	○無制限
所有者証明手法	○	○無制限	○任意端末	○無制限

7．おわりに

本稿では、音楽などのコンテンツ流通における利便性の高い著作権保護方式である所有者証明手法を提案し、実装を行い、検討・評価を行った。所有者証明手法により、共有・購入・再発行の操作の利便性が向上できる。

今後は、Napster[6]やGnutella[7]などファイル交換ソフトと共存できる著作権保護方式に発展させて行く予定である。

謝辞

本研究の遂行にあたって貴重なご意見をいただいたNTT情報流通プラットフォーム研究所の畠中優行氏、桑名栄二氏に深く感謝いたします。

参考文献

[1]OOPS！MusicCommunity,オンラインミュージックマガジンOOPS！,pp.90-92(2000)
[2]山中善義,中村高雄,小川宏,高嶋洋一,曽根原登:著作権保護技術の動向，情報処理,Vol41,No4,pp.382-387(2000)
[3]http://www.sdmi.org
[4]http://www.world.sony.com/JP/Electronics/memorystick/menu.html
[5]藤井,武井,三宅,桑名，コンテンツの私的コピーを考慮した著作権保護方式,情報処理学会第61回全国大会,Vol7,No3,(2000)
[6] http://www.napster.com
[7] http://gnutella.wego.com/