コンテンツの私的コピーを考慮した著作権保護方式

6R - 07

藤井治彦　武井英明　三宅延久　桑名栄二
NTT 情報流通プラットフォーム研究所

1　はじめに

ネットワークの広帯域化、MP3 の蔓延により、音楽・映像等のコンテンツ配信ビジネスにおける著作権保護方式の重要性は高まっている。しかし、現行の方式は、不正コピーを防止するため、ユーザによる私的コピーに著しく制限を課しており、ユーザビリティー低下の原因となっている。私的コピーは、コンテンツのバックアップや再生機器間共有等に関する重要かつ使用頻度の高い機能であり、この点の改良は大きな課題の一つになっている[1]。

本稿では、現行方式により生じる私的コピーに関する問題点を改良した新しい著作権保護方式を提案する。

2　現行方式の問題点

音楽コンテンツ配信分野における主な著作権保護方式は、大きく分けて以下の 2 種類に分類可能であり、それぞれの特徴と問題点を記す。

[固有ＩＤ付きメディアを用いた暗号化方式]

（特徴） コンテンツを暗号化し、その復号鍵を、ユーザの所有メディアの固有ＩＤを用いて暗号化することにより、そのメディア上でなければ、コンテンツの再生を不可能にした方式[2]。

（問題） ①他のメディアにコンテンツをコピーすると、コンテンツが使用できなくなることから、例えば、バックアップさせたとしても、メディアを紛失・買い替えをすると視聴できなくなる。なお、メディアの固有ＩＤの代わりに携帯端末・ＰＣの固有ＩＤを用いる方式もあるが、この方式も、同様の理由で、携帯端末・ＰＣを、紛失もしくは買い換えると再生できなくなる。

[CPU 付きメディアを用いたアクセス制限方式]

（特徴） 特殊なアプリケーション以外からはアクセス不可能な記憶領域を持つＣＰＵ付きメディアを用いる方式。コンテンツを暗号化し、その復号鍵を前記のアクセス制限された記憶領域に格納する等してコンテンツ保護を行う方式。本方式は、チェックイン・チェックアウト作業を行うことによりコンテンツのコピーが可能である。ただし大量コピーを防ぐために回数制限が設けられている[2]。

（問題） ②ＣＰＵ付きメディアを扱えるプラットフォーム上でしか実現できない。すなわち、ＨＤＤなどＣＰＵを内蔵しない一般的な大容量メディアを用いたプラットフォーム上では適用できない。③コピー毎に回数制限に関する専用の操作・手段が必要であり、また、ユーザは制限回数を意識しながら使用せねばならないためユーザビリティーが低い。

3　提案方式の概要

本稿では、上記①～③の問題点を解決する著作権保護方式を提案する。本方式では再生機もしくはメディアをユーザ登録し、コンテンツも、そのユーザ情報を用いて暗号化・復号化することにより不正使用を防止する。以下に本方式の概要と特徴を示す。

[再生機登録]

ユーザは再生機を購入した時等に、登録サーバにネットを介して接続し、ユーザの所有する再生機の固有ＩＤとユーザ自身の個人ＩＤを送信する。登録サーバは固有ＩＤを用いて、個人ＩＤを暗号化してユーザに返す。ユーザは、サーバから暗号化された個人ＩＤを受け取り、再生機に記録する（図１参照）。

なお、本方式において、ユーザと登録サーバ間で、個人ＩＤを送信する際には、十分なりすまし防止・盗聴防止がされているものとする。

また、登録サーバ側で、ユーザの使用できる再生機数を記録・制御することも可能である。

The copyright protection method which admits a personal copy of contents

Haruhiko FUJII, Hideaki TAKEI, Nobuhisa MIYAKE, Eiji KUWANA
NTT Information Sharing Platform Laboratories

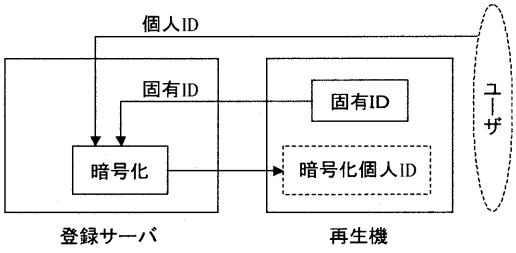

図1 再生機登録方法

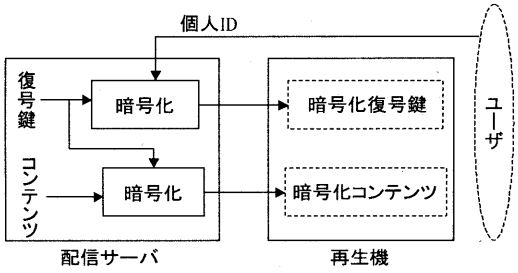

図2 コンテンツダウンロード方法

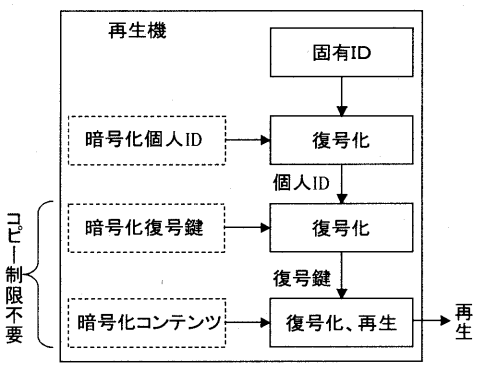

図3 再生方法

[コンテンツダウンロード]

配信サーバでは、あらかじめコンテンツは暗号化されており、ユーザからのダウンロード要求があると、ユーザから個人ＩＤを受け付け、これを用いて復号鍵を暗号化し、暗号化された復号鍵と、暗号化されたコンテンツをユーザに配信する（図２参照）。

サイズの大きなコンテンツは予めＤＶＤ等でパッケージ配送しておき、復号鍵のみをダウンロードする配信形態にも対応できる。

[再生]

再生時には、再生機は、固有ＩＤと暗号化個人ＩＤから、個人ＩＤを復号化し、これと暗号化復号鍵から、復号鍵を復号化し、これと暗号化コンテンツからコンテンツを復号化し再生する（図３参照）。

なお上記処理は、処理中に出てくる個人ＩＤや復号鍵を解読されないために、耐タンパーソフトウェアもしくは耐タンパーハードウェアを用いて行う必要がある。

配信サーバからダウンロードした、暗号化復号鍵と暗号化コンテンツは、通常のファイル同様、無制限にコピー可能であるが、復号化には正当な個人ＩＤが必要なため、コンテンツを再生できるのは、正当な個人ＩＤが埋め込まれた再生機のみである。

本方式が、現行の方式の問題点を解決していることを示す。複数の再生機・メディアに対して同一の個人ＩＤを埋め込むことが可能であり、それらで同じコンテンツを再生できるから問題点①は解決され、また、例えば固有ＩＤを持たないＨＤＤ等を使用する場合でも、再生機の固有ＩＤとしてＰＣのＭＡＣアドレスを用いることができるので、大部分の一般的なプラットフォーム上で実現可能なので問題点②も解決する。また、コピー回数制限が無いのでチェックイン・チェックアウト作業が不要であり、簡便な私的コピーが実現できるため問題点③も解決する。

さらに本方式では、再生機に登録されたユーザでないとコンテンツを再生できない特徴を持つ。このため、コンテンツのダウンロード時にネット上を流れる個人ＩＤが、ハッカーにより盗聴されて使用されたとしても、ハッカーはコンテンツを再生することが出来ないという長所を持つ。

4 終わりに

本稿では、私的コピーを考慮した著作権保護方式の基本方式を考案した。今後は、方式の詳細化を行い実用化を目指す。

参考文献

[1]平山,電子音楽配信の業界動向と商用運用の課題,映像情報メディア学会誌,Vol.54,No.6,pp.785~790.2000

[2]上野,庵,三宅,武井:”不正コピー防止を考慮したコンテンツ販売システム”,電子知的財産･社会基盤研究会,2000