5N-10

再生攻撃を防止したデジタルコンテンツの再生回数制御

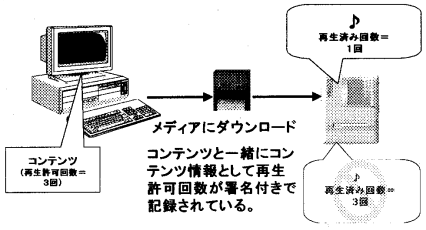
中里加奈　　大友健治

ＮＴＴ情報流通プラットフォーム研究所

1　はじめに

オンライン上の販売サイトでは既に音楽や画像等のデジタルコンテンツ販売が行われている[1][2][3]が、デジタルコンテンツであるという特性上、改ざんや不正利用を防ぐためにコンテンツの供給者がユーザのメディアに対して暗号化されたデジタルコンテンツ（以下コンテンツは全て暗号化されていると仮定する）に対し、コンテンツ供給者が予め再生可能な回数を決定し、その回数だけユーザに再生を許可するように設定しても、コンテンツのバックアップを取り、決められた回数の再生を終了した後でメディアにこのコンテンツをコピーすることによりコンテンツの不正な再生が可能になる（これを再生攻撃と呼ぶ)。本論文ではこの再生攻撃を防止しかつコンテンツに再生制御を加える技術の概要を報告する。

2　再生回数制御とは



メディアに書き込まれた再生済み回数が再生許可回数を過ぎていたらそれ以上の再生を禁止する。

図１　再生回数制御

コンテンツに再生を許可された回数情報が予め付加していて、その回数以上のコンテンツの再生は不可能にすると言った制御である。

3　再生回数制御の実現

コンテンツを再生する際にデバイス(プレイヤー)がコンテンツに付加された再生回数情報を読みとりそれに従って再生を許可する。予め決められた再生回数を超えるような再生は許可しない。

3.1　再生回数制御実現の問題

図２のように、ダウンロードしたコンテンツをユーザ端末や他のメディアにバックアップを取っておき、決められた回数の再生が終了したメディアにコピーすると、もう一度その再生回数分だけの再生が出来てしまう。これを繰り返すことによってほぼ無限回数の再生が可能になり、再生回数制御を無効にしてしまう。これを再生攻撃と呼ぶ。

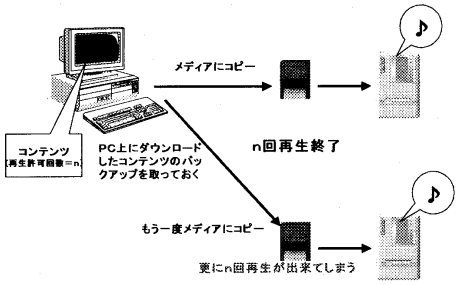


図２　再生攻撃

現状提案されている再生回数制御の方式[4]は乱数を発生させコンテンツに ID をつけそれを変化させる様な仕組みのもので、複雑な構成のメディアが必須になる。これに比べ後述する本方式は現在使用されている様なメディアを利用して実現可能である。

A Protection Methods of Replay Attack Using Usage Control of Digital Contents for Limiting Playback to A Certain Number of Times

Kana Nakasato

NTT Information Sharing Platform Laboratory

3-9-11,Midoricho,Musashino-city,180-8585 Tokyo,Japan

3．2 再生攻撃を防止する再生回数制御の実装

解決策として図 3 のようにユーザに書き換え不能な領域、または Write at Once 領域と通常のストレージエリアである書き換え可能領域の2つに分かれた領域を持つメディアを想定する。書き換え不能な領域、または Write at Once 領域にはコンテンツの ID とその ID を持つコンテンツの状態(存在の有無・利用の可不可)が書き込まれている。書き換え可能領域にはコンテンツ情報(データ、再生可能回数、コンテンツ ID)が書き込まれていてそれらの情報は改ざんを検知するために署名がついている。

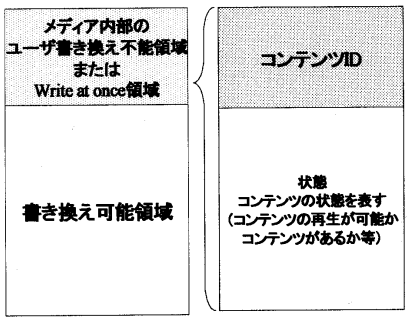


図 3 メディア内部構造

図 4 のようにコンテンツにコンテンツ ID をつけ、再生の度にこの ID を変更し変更前の ID を持つコンテンツは再生不可にする。これとは別にコンテンツの再生許可回数も再生ごとに減らしてゆく。

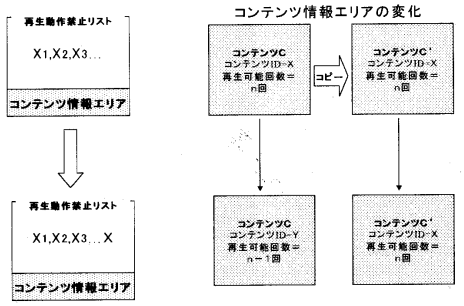


図 4 再生攻撃の防止策

このように一回再生をするとコピーを取ったコンテンツの ID は図 5 のように再生不可になるので再生攻撃を防止することが出来る。

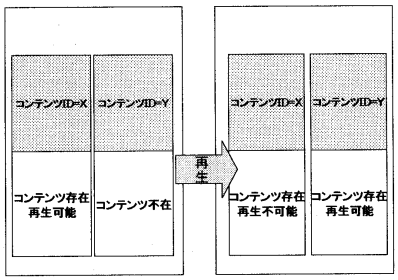


図 5 ID チェックエリアの変化

コンテンツファイルからIDを読み出し、IDチェックエリアからそのコンテンツIDに対応するコンテンツの状態(コンテンツがメディア内に存在するか、それは使用可能か)をチェックする。使用不可ならプログラムを終了する。

次にコンテンツファイルから再生可能残り回数を読み出し、残りが0回でなければ再生する。再生後はIDチェックエリアの中の今再生したコンテンツのIDを使用不可に変更する。コンテンツファイル内の再生可能残り回数を1回減らし、残りが0回でなければそのコンテンツに新しいIDを与える。

4 おわりに

本提案で、再生攻撃を防止したデジタルコンテンツの再生回数制御の実現可能性を確認した。今後は本方式を用いたプロモーションやレンタル業務等の新規ビジネスの展開を提案してゆく予定である。

［参考文献］

[1]OnlineShopBaySideTopPage, http://marine.bayside.ne.jp/~music/index.html

[2]musicBit!DOWNLOAD, http://www.maxell.co.jp/musicbit/download/index.html

[3]hithit.com, http://www.arche.ntt.ocn.ne.jp/nack5/nack5town/solid.html

[4]Michael A.Epstein, Michael S.Pasieka, Martin Rosner, J.P.Linnartz, Toine Staring, Digital Music Open Protection System Philips Research Response to the Call for Proposals 1999