情報販売における不正コピー防止方式の提案

2K－2

庵 祥子　玉井 誠　三宅 延久　曽根岡 昭直
NTTソフトウェア研究所

1.はじめに

近年のインターネットの急速な広がりに伴い、インターネットを介した情報流通販売方式が注目を集めている。中でもデジタルコンテンツはその特性から、インターネット上で流通し、決済が行われることが多い。このような環境はユーザにとって便利であるが、著作権を守る機構の実現が必要とされる。

この実現のために最も単純な機構として不正コピーを防止する方法について検討がなされてきている。しかしながら、それらは抑止機能しかないものであったり、正当な購入者の利便性を損なうものであるなどの問題がある。

そこで本論文では購入者の利便性を考慮した情報販売における不正コピー防止方式について提案する。

なお、以下の議論では説明を簡単にするため、「鍵配送型情報販売方式[1]」に対する拡張として行う。

2.鍵配送型情報販売方式の現状

鍵配送型情報販売方式とは、商店側で販売するコンテンツを暗号化してあらかじめ配送し、決済と同時に復号鍵を配送する販売方法である。通常暗号化したコンテンツの配送(CD-ROM、衛星などのマルチキャスト等)と決済を分離するため、暗号化は購入者に依存しないコンテンツごとの鍵で行われることが多い。現在、Pay per View[2]や売り切り[1]などの販売方式が行われている。

Pay per View 方式は、購入した端末にコンテンツを保存させないことにより不正コピーの防止を実現している販売方式である。この方式の場合、複数回利用するコンテンツでは利用する度に購入処理を行う必要があり、利用者の利便性を損なっていることが問題である。

売り切り方式は、購入した端末にコンテンツを保存することが可能である。しかしながら、購入後は購入者であるなしに関わらず、また購入時の端末であるなしに関わらずコピーできるという問題がある。

このように既存の鍵配送型情報販売方式だけでは、不正コピーに対して有効な手段を有していないことが問題であった。

このため近年では電子透かし方式[3]が不正コピー抑止のために利用されてきている。この方式では購入者ＩＤなどの情報を見た目にはわからない形でデジタルコンテンツに埋め込み、追跡性をもたせることによって不正コピーの抑止効果を実現している。しかしながら、最終的にコピーされるか否かは購入者のモラル次第であり、防止効果がないことが問題である。

今までに述べた３つの方式それぞれの不正コピーに対する現状について表１でまとめる。

	購入者による購入端末への保存	購入者による他端末への保存	非購入者による他端末への保存防止	利用者ＩＤ入力などの認証
Pay per View	×	×	○	毎回必要
売り切り	○	○	×	必要なし
電子透かし	○	○	×	必要なし

表１：不正コピー防止への対応の比較

このように、既存の鍵配送型情報販売や電子透かしだけでは、購入者の利便性を保ちつつ、不正コピーを防止することが難しい。

3.復号鍵の暗号化による不正コピー防止方式の提案

２章で述べた現状を基に、本提案では以下の４点を考慮し、既存の鍵配送型情報販売方式に適した不正コピー防止方式を提案する。

- 購入者による購入端末への保存が可能
- 購入者であれば購入端末以外へのコピーが可能
- 購入者以外による不正コピーを防止
- 購入者の利便性を損なわない

本提案の方式では、鍵配送型情報販売で利用されるコンテンツの復号鍵を２つの鍵で暗号化し、用途によって利用する鍵を使い分けることによってこれらの課題を実現する。

以下に提案する方式について、主に購入時の流

An Illegal Copy Protection Method for the Information Distribution
Shoko IHORI　Makoto TAMAI　Nobuhisa MIYAKE　Terunao SONEOKA
NTT Software Laboratories

れと利用時の流れの２つに分けて述べる。

3.1 購入時の流れについて

購入時の流れを図１に示す。

購入者は商店サーバ（暗号化コンテンツと復号鍵を保存）から必要なコンテンツを暗号化されたままの状態で購入者端末にダウンロードして保存する。そして、決済と同時に商店サーバから復号鍵をダウンロードし、これを購入者認証情報とマシンＩＤの２つを鍵としてそれぞれ暗号化して購入者端末に保存する。購入者認証情報には、ユーザＩＤとパスワードの組み合わせを利用したり、公開鍵暗号方式を利用することが可能である。

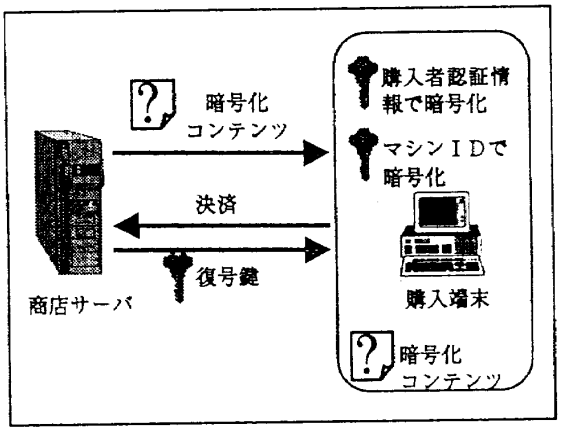

図１：購入時の流れ

3.2 利用時の流れについて

次に利用時の流れについて述べる。利用時の流れは図２のとおりである。

購入時の端末で利用する場合はコンテンツの復号鍵はマシンＩＤで自動的に復号される。このため購入者が復号を意識する必要がなく、購入者の利便性を保つことが可能である。

購入時の端末以外で利用する場合は、暗号化されたコンテンツと暗号化された復号鍵を目的の端末にコピーする。そして初回利用時に購入者が購入者認証情報を入力することによって復号鍵を復号し、コンテンツの復号を可能にする。これにより正当な購入者であれば購入端末以外の端末へのコピーが可能となる。

また、購入者認証情報の公開は購入者の損失(他人に自分の口座で決済されるなど)に結びつくために他人に公開されないことから購入者以外による不正コピーの利用を防止することが可能になる。また、コピーした端末で再びマシンＩＤを利用して復号鍵を暗号化し直すことによって、次回からはその端末でもマシンＩＤでの復号を可能にする。

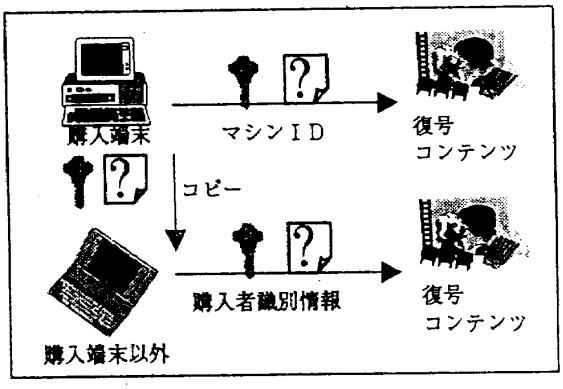

図２：利用時の流れ

4.おわりに

鍵配送型情報販売方式では、本提案の方式を採用することにより購入者が購入したコンテンツを購入端末へ保存し、必要があれば他の端末にコピーすることを可能にできることがわかった。また、購入者の利便性を損なわずに、購入者以外による不正コピーを防止できることがわかった。

今後の課題としては、より多くの情報販売方式に適用するために、WWWのアクセス制御等によりコンテンツをそのままダウンロードするような「非暗号型情報販売方式[4]」への適用が挙げられる。本提案は、購入端末で暗号化することによって非暗号型情報販売への適用が可能である。しかしながら、セキュリティやネットワークの負荷などの問題を考慮すると、本提案は鍵配送型情報販売方式により適していると考えられる。

現在、本方式を用いて音楽コンテンツやＰＤＦファイルを販売するための実装を鍵配送型情報販売方式である「Infoket」に基づいて行っている[5]。今後はこれらの実装をもとに現在行っている電子出版サービス等にこの方式を適用していく予定である。

参考文献

[1] 明石修,森保健治,寺内敦:インターネットを用いた情報プラットフォーム：Infoket-I, NTT R&D,Vol46,No.2, 1997

[2] 玉井誠,三宅延久,曽根岡昭直:情報流通プラットフォーム「Infoket」を用いた音楽コンテンツ販売システム,1998 年電子情報通信学会総合大会

[3] 特集「電子透かし」がマルチメディア時代を守る,日経エレクトロニクス,1997.2.24

[4] http://www.so-net.ne.jp/So-netSquare/

[5] 玉井誠,庵祥子,三宅延久,曽根岡昭: 情報販売における不正コピー防止方式の実装, 情報処理学会第 57 回全国大会