マルチメディア通信と分散処理 91－24
（1999. 1. 22）

不正コピー防止を考慮した情報販売方式

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

概要

デジタルコンテンツは完全なコピーが可能なため、その流通販売では不正コピーを防止する必要がある。しかしながらこのために正当な購入者の利便性を犠牲にすることは避けなければならない。本提案では私的利用に限ったコピーのみを許可し、購入者の利便性とも共存する「不正コピー防止を考慮した情報販売方式」を提案する。本方式では、利用権を２つの情報で暗号化し、コンテンツ利用時にこれら使い分けることによって不正コピーを防止した。さらに本方式を既存の Infoket に PDF 販売システムとして実装し、評価を行った。また実際のサービス適用に向けての改良を行った。

An information marketing system with illegal copy protection

Shoko IHORI　Makoto TAMAI　Nobuhisa MIYAKE　Terunao SONEOKA
NTT Software Laboratories

Abstract

Digital contents can be copied without any loss of data, so the marketing system of them should have a mechanism to prevent illegal copies. However, the system should not decrease convenience of legal buyers. In this paper, the information marketing system with illegal copy protection is proposed; it only allows copies for private use, while keeping convenience of legal purchaser. The system prevents illegal copy, by encrypting rights for use with two informations and decrypting with either one when the contents will be used. The system has been applied to a PDF marketing system of the "Infoket". We have evaluated and improved the system to adapt to the actual services.

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デジタルコンテンツの情報販売が注目を集めている。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。このことは「デジタルコンテンツ流通に関するアンケート（ECN 主催 97/12/1-98/1/18 実施）[1]」でデジタルコンテンツ流通の利用経験の質問に対して 27.3％の人が経験ありと回答しているところからも覗える。またそのうちの 63.7％の人が今後も利用したいと答えており、これからの市場として期待できる。

デジタルコンテンツをインターネットを介して販売することは販売者側・購入者側双方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配慮した「不正コピー防止を考慮した情報販売方式」について提案し、評価を行う。また、この方式に基づいて情報販売システムを実装し、さらに実際のサービスとして適用する際に問題となるような不正利用について検討し、改良する。

2.情報販売方式の現状

現在、インターネット上ではいくつかの方式の情報販売が行われている。たとえば、Pay Per View[2]や Pay Per Copy などの方式がある。

Pay per View 方式とは、閲覧する権利を売買する情報販売方式である。この方式では、閲覧する権利のみをやり取りするため、デジタルコンテンツを購入端末に保存しないことから不正コピーの防止をを実現している。しかしながら、複数回利用するデジタルコンテンツの場合、利用するたび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。

Pay Per Copy 方式とは、デジタルコンテンツ

の所有権を売買する情報販売方式である。この方式では、デジタルコンテンツそのものをやり取りするため購入したデジタルコンテンツを購入端末に保存することが可能である。これにより、購入後のデジタルコンテンツは、購入者であるなしにかかわらず、また購入端末であるなしにかかわらず、コピーできることが問題である。その一方で、利用者は一度購入処理を行えば購入端末かどうかを意識せずに、簡単にデジタルコンテンツを利用できるという利点がある。

以下に、これら2つの方式の購入者の利便性と不正コピー防止対策について表1でまとめる。

	購入者の利便性			不正ｺﾋﾟｰ対策
	購入端末への保存	購入端末以外への保存	利用時の認証処理	購入者以外の不正ｺﾋﾟｰ防止
Pay per View	×	×	毎回必要	○
Pay per Copy	○	○	必要なし	×

表1：不正ｺﾋﾟｰ防止対策と利用者の利便性の比較

このように、これらの方式では購入者の利便性と不正コピー対策が両立していない。これは、これからのデジタルコンテンツの流通販売において大きな問題である。

この問題を解決するために、過去にもいくつかの方式が考えられている。たとえば、Pay Per Copy 方式では不正コピーを考慮して電子透かしを併用するという手法などが行われている。電子透かしとは購入者 ID などの情報を見た目にはわからない形で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するものである。しかしながら、最終的にコピーされるか否かは利用者のモラル次第であり、防止効果がないことが問題は依然解決されていない。

このように、現在の情報販売方式では購入者の利便性と不正コピー防止を両立できていないことが問題である。

3.不正コピー防止を考慮した情報販売方式

2 章で述べた問題を解決するために購入者の利便性と両立するような「不正コピー防止を考慮した情報販売方式」を提案する [3]。本提案では、以下の点を考慮する。

・購入者の利便性
　・購入端末にデジタルコンテンツを保存可能
　・購入端末以外へコピーが可能
　・入力項目の減少
・他者による不正コピーの防止
　・購入者以外のコピー防止
　・購入者の私的コピーの許可

本提案の方式では、売買するデジタルコンテンツを暗号化しその復号鍵を利用権とする。さらにこの利用権を 2 つの情報に基づいて暗号化して保存する。用途によって利用権の復号に使用する情報を使い分けることによってこれらを実現する。

次に提案する情報販売方式の概要について述べる。本提案の情報販売方式では、暗号化コンテンツとその利用権を格納したコンテンツサーバと購入端末が通信し、暗号化コンテンツ等の取得および決済を行う。コンテンツサーバと購入端末がやり取りする情報は、暗号化コンテンツとその利用権および決済情報の3つである。

以下に本方式におけるデジタルコンテンツの販売と利用について詳細に説明する。さらに本方式の評価を行う。

3.1 コンテンツの販売について

図1に本方式を用いてデジタルコンテンツを売買する際のフローを示す。

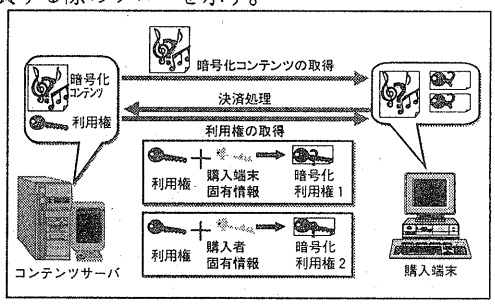

図1：デジタルコンテンツの売買

販売者は、コンテンツサーバに販売するデジタルコンテンツを登録する。この際、デジタルコンテンツを暗号化することによって暗号化コンテンツと利用権を生成し、これらをそれぞれコンテンツサーバに登録する。

購入者は、はじめに暗号化コンテンツを取得する。取得方法は CD－ROM や WWW を介したり、あるいはマルチキャスト衛星通信を利用するなどさまざまな方法が考えられる。取得した暗号化コンテンツはそのまま購入端末に保存する。また購入者は決済処理を行うことによって利用権を購入する。購入した利用権は、購入者固有情報と購入端末固有情報のそれぞれに基づいて暗号化して購入端末に保存する。

購入者固有情報には例として購入者ＩＤとパスワードの組み合わせ、クレジットカード番号、公開鍵暗号方式の秘密鍵などが挙げられる。また購入端末固有情報の例としては、ＯＳ製品番号や起

動ディスクパーティションのシリアルＩＤなどの組み合わせが挙げられる。

3.2 コンテンツの利用について

次に購入したデジタルコンテンツの利用について詳細に説明する。利用時のフローはデジタルコンテンツを購入時の端末で利用する場合と、他の端末にコピーして利用する場合で異なるため、それぞれの場合について説明する。

購入端末でデジタルコンテンツを利用する場合のフローを図２に示す。

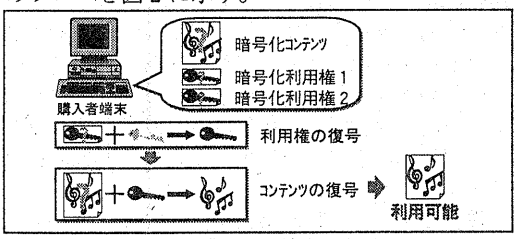

図２：購入時の端末で利用

購入端末でデジタルコンテンツを利用する場合は、購入端末固有情報を用いて利用権を復号する。そしてその利用権を基に暗号化コンテンツを利用可能にする。購入端末固有情報を基に利用権を復号するため、購入者の作業を伴うことなく、デジタルコンテンツを利用することが可能である。

購入端末以外へデジタルコンテンツをコピーして利用する場合のフローについて図３に示す。

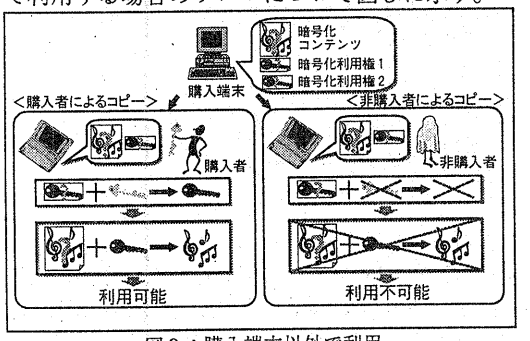

図３：購入端末以外で利用

購入端末以外の端末でデジタルコンテンツを利用する場合は、暗号化コンテンツとその利用権を目的の端末にコピーしなければならない。利用権は購入者固有情報で暗号化されたものをコピーする。そして初回利用時は、購入者固有情報を入力することによって利用権を復号し、さらに暗号化コンテンツを利用可能する。

一度、購入者固有情報を入力して利用権を復号すると、その利用権をコピーした端末の端末固有情報を基に暗号化する。よって次回にコンテンツを利用する際には、購入者固有情報を入力しなくても端末から自動的に端末固有情報を利用することによって利用権を復号することが可能になり、暗号化コンテンツを利用することが可能になる。

このように、購入者固有情報と購入端末固有情報という２つの情報を使い分けて利用権を暗号化および復号化することによって、正当な購入者の利便性を保持すると同時に他者による不正コピーの防止を実現する。

なお暗号化コンテンツおよび暗号化利用権は電子署名を付加し改竄や偽造を防ぐ必要がある。

3.3 評価

本方式と従来の方式との比較を表２に示す。

	購入者の利便性			不正ｺﾋﾟｰ対策
	購入端末への保存	購入端末以外への保存	利用時の認証処理	購入者以外の不正ｺﾋﾟｰ防止
Pay per View	×	×	毎回必要	○
Pay per Copy	○	○	必要なし	×
提案方式	○	○	必要なし	○

表２：提案方式と従来の方式の比較

本方式は、デジタルコンテンツを暗号化コンテンツと２つの暗号化利用権として端末に保存することにより、購入者の利便性を保ちつつ、不正コピー対策を行い、購入者以外の不正コピーを防止することを可能にした。購入者固有情報で暗号化した利用権を利用することにより、購入者であれば購入端末以外の端末へコピーし、保存することを可能にした。これと同時に購入者以外は購入者固有情報を持たないため、購入者以外による不正コピーの防止を可能とした。また、購入端末固有情報で暗号化した利用権を利用することにより、利用時に認証情報を入力しなくてもデジタルコンテンツを利用することを可能にした。

本方式のセキュリティ強度に関する評価については後述の６章にまとめる。

4.情報販売システムの実装

本提案に基づいた情報販売システムを Infoket [4]をプラットフォームとしてＰＤＦ形式のコンテンツの販売を行うシステムとして実装した[5]。以下に Infoket について説明し、Infoket と本提案システムの結合について考察した後、ＰDF 形式を利用した本システムの実装について述べる。

4.1 情報販売プラットフォーム Infoket

Infoket とは、購入者が先に暗号化されたデジ

タルコンテンツを取得し、その後決済を行うと同時に復号鍵を入手する鍵配送型情報販売方式のプラットフォームである。現在は、WWW を基盤としてさまざまな情報の販売を行っている [6]。Infoket での情報販売フローを図 4 に示す。

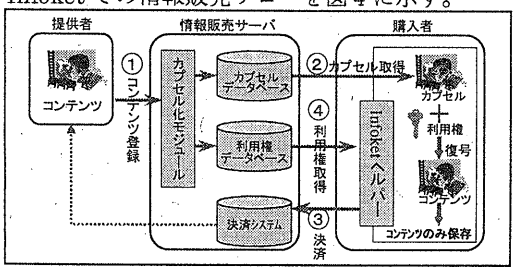

図 4 :Infoket 構成図

Infoket はデジタルコンテンツの販売者（販売端末）、情報販売サーバ（カプセルデータベース、利用権データベース、決済システム）、購入者（購入端末）から成り立つ。

販売者は、販売するデジタルコンテンツを情報販売サーバに登録する。登録されたコンテンツはカプセル化モジュールによって電子署名や利用権サーバのアドレス等の情報を付加して暗号化し、カプセル化される。そしてカプセル化したコンテンツはカプセルデータベースへ、カプセル化時に利用した暗号鍵を利用権として利用権サーバにそれぞれ保存する。

購入者はカプセル化コンテンツをインターネットや CD-ROM 等を経由して入手し購入端末に保存する。さらに決済処理を行って利用権を利用権サーバから入手する。そしてこの利用権と先に入手したカプセル化コンテンツを Infoket ヘルパーを用いて復号し、復号したデジタルコンテンツのみを購入端末に保存して利用する。

4.2 PDF 形式の情報販売システムの実装

4.1 節で紹介した Infoket システムを基盤として、PDF 形式のコンテンツの情報販売システムを実装した。PDF 形式のコンテンツのための情報販売システムを実装した理由は、PDF 形式のコンテンツにはコンテンツ内部にデジタル署名情報や利用権サーバアドレスなどを埋め込む領域が確保できるため Infoket を基盤とした情報販売システムに実装するのに適していたためである。PDF 形式のコンテンツを操作するためのアプリケーションとして Acrobat Exchange と Acrobat Reader を洗濯し、本システムはこれらのプラグインとして実現した。実装システムの構成図を図 5 に示す。

本システムではカプセル化モジュールで処理を

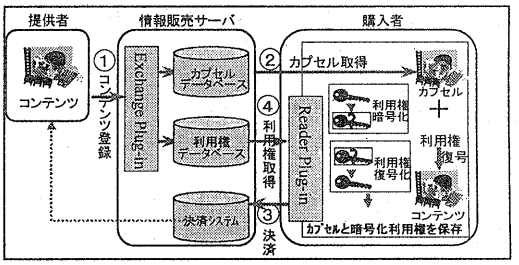

図 5 ：実装システム構成図

行っていたコンテンツ登録時のカプセル化処理を Accrobat Exchange Plug-in として実現し、デジタル署名情報や利用権サーバアドレスなどをＰＤＦファイルに埋め込んで暗号化するように実装した。このモジュールは Infoket のコンテンツ登録系と連動させ、販売者は登録時に暗号化形式として「暗号化ＰＤＦ」を選択するだけで自動的に処理がなされるようにした。

購入者側は、この暗号化ＰＤＦを Acrobat Reader で普通のＰＤＦファイルと同様に閲覧可能にするために Acrobat Reader のプラグインを利用して利用権の復号やＰＤＦファイルを利用可能にする操作を実装した。

4.3 購入者側の実装イメージ

以下に購入者側の実装イメージを示す。

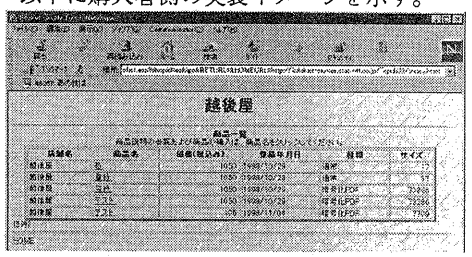

図 6 ：商品一覧

図 6 は情報販売サーバに登録された暗号化 PDF を WWW を経由して閲覧した場合の画面である。従来の Infoket での表示と同様の構成で商品名、価格、商品のサイズ等が表記されている。購入者はここから購入する PDF ファイルを選択することができる。

ここで購入者が暗号化 PDF のファイルを選択すると Acrobat Reader プラグインを通じて端末にその暗号化 PDF ファイルの利用権がないかを検索し、以前に購入したことのあるファイルかどうかのチェックを行う。もし利用権が存在しなければ図 7 のようなメッセージを表示し、鍵の購入を促す。これは WWW 上ではなく、デスクトップ上などの暗号化 PDF ファイルをダブルクリッ

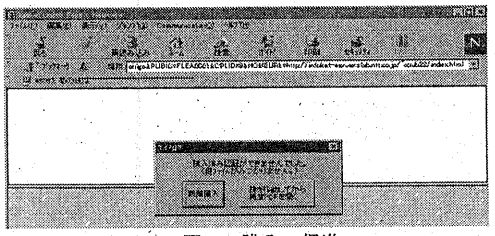

図7：購入の促進

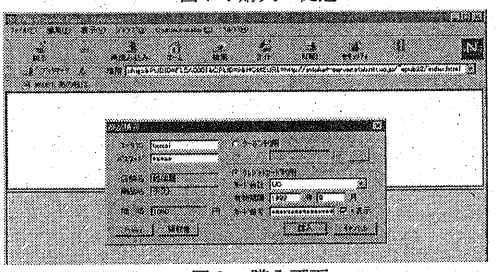

図8：購入画面

クしても同様の処理を行う。

新規購入のボタンを選択して購入処理を開始すると図8のような購入画面が現れる。購入者の情報と決済情報（クレジットカード情報あるいはクーポン情報）を入力することによって決済が開始される。決済の通信については Infoket を利用する。決済と同時に利用権を取得し、購入者固有情報と端末固有情報でそれぞれ暗号化する。利用権を取得すると図9のように PDF ファイルを閲覧

図9：PDF ファイルの閲覧

することが可能になる。それぞれの情報で暗号化した利用権はそのまま購入端末に保存する。この暗号化 PDF ファイルを他端末にコピーして開こうとした場合は、購入端末と異なる端末で利用しようとしている旨を警告するメッセージを表示する。さらにコピー先の端末に暗号化利用権がないか検索する。もし暗号化利用権が検知できなかった場合は暗号化利用権を目的の端末にコピーすることを指示する警告メッセージを表示する。暗号化利用権を検知したら購入者固有情報の入力を促す画面を表示する。ここで購入者固有情報が入力できるかどうかで購入者かどうかの判断を行う。これにより非購入者による不正コピーを防止している。さらにコピー先の端末で端末固有情報で利用権を再暗号化するかどうかを購入者が選択できるように実装した。これにより購入者が再暗号化を選択すると購入者認証情報の入力が必要なくなるため、購入者の利便性を確保することが可能である。また、再暗号化を行わず利用するたびに購入者認証を必要とする方式を選択した場合は、他端末へコピーしても購入者以外の利用を防ぐことが可能になり、より強い防止効果が必要な場合に用いることができる。

5.情報販売システムのセキュリティ分析

本提案の情報販売方式では、購入時や購入後に端末間でコピーする際に不正コピーを防止することを可能にした。しかしながら、実際のサービスとして運営する際には、購入時や端末間コピー以外にも図 10 に表すような 5 つの段階における不正利用を考慮し、それらを防御しなければならない。それぞれの段階の不正利用の攻撃について表2にまとめる。また本実装でそれぞれの項目においてどの程度の防御を可能にして実装したかについてもあわせて記述する。

図 10：不正利用の攻撃方法

攻撃対象	攻撃方法	防止効果
ｶﾌﾟｾﾙと利用権ﾌｧｲﾙ	ｺﾝﾃﾝﾂの改竄	○
	ｺﾝﾃﾝﾂの不正ｺﾋﾟｰ	○
	利用権の改竄	○
	利用権の不正ｺﾋﾟｰ	○
閲覧ソフト	ﾘﾊﾞｰｽｴﾝｼﾞﾆｱﾘﾝｸﾞによる閲覧ｿﾌﾄからの利用権盗聴	×
閲覧状態	画面からのｶｯﾄ&ｺﾋﾟｰ	○
	画面からのﾊｰﾄﾞｺﾋﾟｰ	△
印刷状態	ﾌﾟﾘﾝﾄﾒﾆｭｰからのﾌｧｲﾙ出力	○
	ﾌﾟﾘﾝﾀｻｰﾊﾞ等へ通信中のﾃﾞｰﾀ盗聴	△
印刷物	印刷物のﾊｰﾄﾞｺﾋﾟｰ	×

表2：不正利用に対する防御

以下にそれぞれの場合についての攻撃方法に対する対策と、本実装で取り扱った部分について述べる。

5.1 カプセルと利用権ファイルでの攻撃

カプセル（カプセル化コンテンツ）と利用権ファイルに対する不正利用の方法は4つ挙げられる。カプセルと利用権ファイルそれぞれの改竄および不正コピーである。改竄防止については本実装ではそれぞれのファイルに電子書名をつけて暗号化することによって実現した。また不正コピー防止については本提案方式により解決し実装している。また不正コピーについてはカプセルと利用権ともに暗号化することによってコピー先での利用を防ぐことで実現している。また購入者自身によるコピーについては私的利用の範囲内と判断して許容するが、その際は購入者固有情報の入力で購入者かどうかの判断を行っている。

5.2 閲覧ソフトでの攻撃

閲覧ソフトでは、閲覧ソフトから利用権を盗聴するなどの不正利用が考えられる。本システムではAcrobat Reader に対してリバースエンジニアリングをすることが挙げられるが、今回はこれに対応する対策を行っていない。しかしながら、Acrobat Reader およびその Plug-in に対するリバースエンジニアリングはかなり高度な技術を要すると考えられる。

5.3 閲覧状態での攻撃

閲覧状態では、画面からのカット＆ペーストによるコピーや、画面からのハードコピーなどの不正利用が考えられる。前者の方法に対してはAcrobat Reader のプラグインを用いて画面からのカット＆コピーを不可能にすることによって対応した。また後者の方法に対して派具体的な実装は行なっていないが、画面のハードコピーはPDFファイルではなく、bmp 形式等のファイルになってしまうことから PDF ファイルを生成できない。よって完全なコピーを行えないことから、ある程度の不正コピーは防止していると考えられる。

5.4 印刷状態での攻撃

印刷状態では、プリントメニュー等からファイル出力を選択してポストスクリプト形式でコンテンツをファイルに出力し保存する方法やプリンタサーバへの転送データを盗聴するという方法などの不正利用が考えられる。前者の方法に対しては、Plug-in を用いて PDF のメニューからファイルへの出力の項目を選択不可にするという対策を行った。後者の方法に対しては、購入者の ID 情報をプリントストリームに埋め込んで抑止し、また情報提供者によって印刷禁止の指定を可能にすることによって対応した。

5.5 印刷物での攻撃

印刷物でのコピーは、本システムでは可能になっている。今回の実装では対象外としたが、今後の予定としては、電子透かしを併用し、印刷物からも購入者 ID 情報等を取得可能にするなどの改善を行う予定である。

6.おわりに

本論文では、利用者の利便性を保ちつつ不正コピーを考慮した情報販売方式を提案し、そのシステムを Infoket 上で PDF コンテンツに関して実装した。これにより、購入者の複製を可能とし、かつ非購入者の複製を防止した PDF ファイルの時販売を Infoket システム上で行うことを可能にした。

今後の展開としては、本システムを現行のサービスに 1999 年 1 月中旬より適用する。そしてそこでの情報提供者や購入者からのフィードバックをもとにして改善を行っていく予定である。

また今回の実装はソフトウェアのみで行い、制約が非常に多かった。今後は OS での対応や専用端末（ハードウェア）まで含んだ実装についても検討していく。

参考文献

[1]http://www.commerce.or.jp/minfo/enq/report11/index.html デジタルコンテンツ流通に関する調査結果

[2]明石,森保,寺内: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,Vol146, No.2, 1997

[3]玉井,三宅,曽根岡: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, 1998.3

[4]庵,玉井,三宅,曽根岡:情報販売における不正コピー防止方式の提案, 情報処理学会第 57 回全国大会, 1998.10

[5]http://www.comket.co.jp

[6]玉井,庵,三宅,曽根岡: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, 1998.10