情報販売における不正コピー防止方式の実装

2K－3

玉井 誠　庵 祥子　三宅 延久　曽根岡 昭直
ＮＴＴソフトウエア研究所 ソフトウエア技術研究部

1．はじめに

現在，インターネット，CD-ROM，DVD，衛星など様々なメディアを介したデジタルコンテンツの流通販売方式が注目されている．しかしながら，際限なくコピー可能で，時間が経っても劣化しないというデジタルコンテンツの特性は，現在の著作権の枠組みの中では，ビジネスとしてのコンテンツ流通の発展を阻害させる原因となっている．現状のデジタルコンテンツ流通方式の多くがコンテンツ著作者の著作権を守るために，コピープロテクトなどの方法で制約を加えることが多く，この場合，利用者の利便性や快適さが犠牲になりやすい．

本論文では，利用者の利便性を考慮し，購入したデジタルコンテンツの私的な利用による複製を考慮しつつ，不正な二次流通を防ぐことのできるシステムの具体的な実装について説明する．なお，不正コピー防止方式については[1]を参照されたい．

2．Infoket

Infoket とは，ＮＴＴソフトウエア研究所で開発された鍵配送型情報販売方式の情報流通プラットフォームである[2]．鍵配送型情報販売方式とは，情報(デジタルコンテンツ)を暗号化して自由に配布し，ユーザが必要になった際に，その使用権に相当する復号鍵をインターネットを介して鍵センタから利用者に送り，同時に課金を行うことにより情報を販売する方式である．図 2.1 に，Infoket での情報購入の基本的な流れを示す．これを実現するために，単に情報を暗号化するだけではなく，改竄防止のためデジタル署名や，復号鍵取得(決済)時に必要となる鍵サーバのアドレスなどを暗号化された情報以外に埋め込んだカプセルという形式でインターネットや様々なメディアを通じてユーザに配布を行っている．また，ネットワーク上での盗聴・改竄だけではなく，悪意のあるユーザからの攻撃に対しても安全な鍵配送プロトコルを実現している．

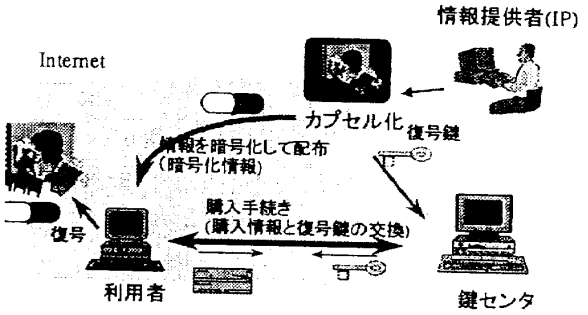

図２．１ Infoketの流れ

3．復号鍵の暗号化による不正コピー防止

本論文で提案するシステムは Infoket 上で実装している．実装方法として，(1) 暗号化したファイルを配送する時にカプセルを使用するか否か，(2) 端末に鍵を保存する時に，暗号化ファイル(またはカプセル)に埋め込むのか否かの４種類について考慮した(表 3.1)．カプセルを使用しない方式は，コンテンツに電子署名や鍵サーバアドレスを埋め込む必要があるために，扱えるコンテンツのフォーマット形式に制約が生じる．しかしその一方で，利用者にとってはカプセルが，普段使用しているコンテンツと同一の形式となるために，従来そのコンテンツを閲覧しているのと同一の操作で，閲覧できる利点がある．次に鍵ファイルの保存方法についてであるが，暗号化ファイルに埋め込んだ場合には，正当な利用者がファイルを他の端末に複製する時に，鍵の存在を意識せずに，(暗号化されている)コンテンツだけを複製すれば良いために，ユーザの利便性が高い．しかし，コンテンツ自体に鍵情報が埋め込むことが不可能な場合や，容量の大きいデジタルコンテンツ（動画，音楽）をＣＤ－ＲＯＭやＤＶＤなどのメディアに蓄積して配布したい，鍵情報ファイルのみをＦＤやＩＣカードに保存し持ち歩きたい，などの要求に対しては後者の方法が有効にある．表 3.1 に示

Implementation methods of illegal copy protection for Information distribution.
Makoto Tamai　Shoko Iori　Nobuhisa Miyake　Terunao Soneoka
Software Engineering Laboratory NTT Software Laboratory
9-11,Midori-Cho 3-Chome,Musashino-Shi,Tokyo 180 Japan

すような分類のなかで，“カプセル使用，鍵ファイルコンテンツ付加”の例として，音楽コンテンツ（TwinVQ）の販売システムと，“カプセル未使用，鍵ファイル分離型“の例としてＰＤＦファイルの販売システムのプロトタイプを開発したので，説明を行う．

表３．１ 実装方法の組み合わせ

	カプセル使用	カプセル未使用
鍵ファイル一体	（例）TwinVQ	
鍵ファイル分離		（例）PDF

３．音楽コンテンツの不正コピー防止

本システムでは，従来の Infoket を用いた音楽コンテンツ販売システム[4]の機能を拡張し，購入したコンテンツの不正コピーを防ぎつつ，正当な購入者であれば，任意の端末への複製・再生を可能とした音楽コンテンツ Pay Per Copy 販売システムである． Infoket で購入した復号鍵をユーザ端末固有の値，ユーザ固有の値（コンテンツ購入に用いるユーザＩＤとパスワード）をそれぞれ暗号鍵として暗号化し，暗号化されたコンテンツのカプセルに付加することによってこの機能を実現する[1]．複製したい音楽コンテンツの正当な購入者であれば，Infoket のユーザＩＤおよびパスワードを入力することにより，購入した音楽を任意の端末上で聴くことができる（図 3.1）．

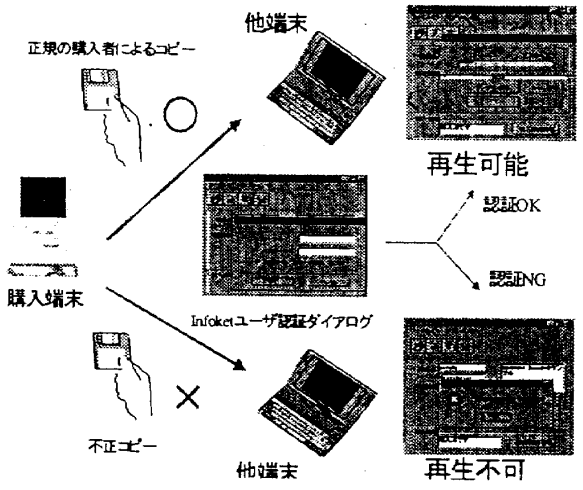

図 3.1 音楽コンテンツの不正コピー対策

４．ＰＤＦファイルの不正コピー防止

４．１ システムの概要

Adobe Systems(http://www.adobe.com)社の開発したＰＤＦ自体が持っているセキュリティ機能のパスワード設定を行うことにより他人によるＰＤＦの閲覧を禁止できる．本システムでは，このＰＤＦのセキュリティ機能に用いるパスワードを Infoket を用いて販売する．購入したパスワードは，鍵情報ファイルとして，ユーザ端末固有の値，ユーザ固有の値（コンテンツ購入に用いるユーザＩＤとパスワード）をそれぞれ暗号鍵として暗号化し保存する[1]．正規の購入者はＰＤＦファイルと対応した鍵情報ファイルを任意の端末に複製し，閲覧できる．

４．２ システムの実現

本システムはカプセルを使用しないために，従来のカプセル化処理を行う部分を，ＰＤＦファイルのパスワード設定(従来の暗号化処理に相当)と，デジタル署名情報，鍵サーバアドレス情報などの埋め込みをする処理を，Acrobat Exchange プラグインで実現した．このモジュールは Infoket の登録系と連動しており，利用者は登録する時に，暗号化形式として，「PDF 暗号化」を選択するだけで自動的に処理がなされる．また，利用者側も，カプセルを使用していないため，PDF の Reader である Acrobat Reader プラグインにより実現した．

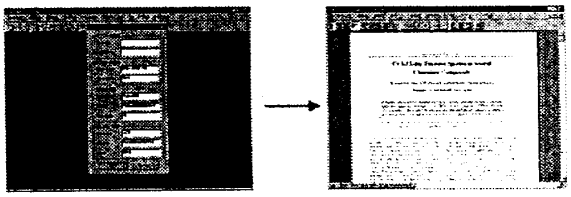

図 4.1 Reader プラグインによるパスワード購入の流れ

５．まとめ

本論文では，ユーザの利便性を損なうことなく，デジタルコンテンツの不正コピーを防止し流通させるシステムの実装例を音楽コンテンツとＰＤＦコンテンツについて紹介した．今後，前者はＮＴＴで開発中のポータブル TwinVQ プレイヤーへ，後者は平成 10 年秋に Infoket 電子出版サービス(http://www.infoket.or.jp)へ適用予定である．

文献

[1]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”，本論文集掲載
[2]明石,森保,寺内，“インターネットを用いた情報流通プラットフォーム:Infoket-I”, NTT R&D Vol.46 No.2 1997
[3] N.Iwakami,T.Moriya and S.Miki:"High-Quality Audio-Coding ar Less Than 64 kbit/s by Using Tranfrom-Domai WeightedInterLeaveVector Quantization(TwinVQ)".Proc.IEEE ICASSP'95,pp.3095-3098,1995.
[4]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”,電子情報通信学会，1998年全国大会論文集