マルチメディア通信と分散処理 70－6
（１９９５．５．２５）

マルチメディア情報流通システム（InfoKet）

金井　敦、三宅　延久、明石　修、生沼　守英

NTTソフトウェア研究所

武蔵野市緑町3-9-11

あらまし

CD-ROMを媒体として、各種情報を廉価に小売強く流通させるためのシステムの基本的考え方および構成について述べる。本システムでは、流通させたい情報を暗号化して　CD-ROMに格納して流通させ、利用者が望む時にサーバと通信をして代金を支払うと同時に利用権を得るシステムである。本システムは、CD-ROMのオーサリング、端末、サーバのサブシステムから構成されるプラットホームである。本稿では、このようなシステムに要求される条件や機能を明確にし、具体的なシステムの構成について述べる。

和文キーワード

マルチメディア　情報流通　CD-ROM　オーサリングツール　鍵配送

Multimedia Information Market System (InfoKet)

Atsushi Kanai, Nobuhisa Miyake, Osamu Akashi, Morihide Oinuma

NTT Software Laboratories

9-11 Midori-Cho 3-Chome, Musasho-Shi, Tokyo 180 Japan

The basic concept and system architecture to distribute many kinds of information using CD-ROM are presented in this paper. On this system, the information distributed to end users is encrypted, and stored in a CD-ROM, when an end user want to use the information, the user pays a fee of the information and get the right to use the information. The platform consists of CD-ROM authoring sub-system, terminal sub-system and server sub-system. In this paper, conditions and functions are clarified and an actual system construction is discussed.

英文キーワード

Multimedia , information distribution, CD-ROM, authoring tool, key distribution

1 はじめに

情報はそもそもコピーしたり運んだりするのにかかるコストは非常に小さいという性質がある．しかし，現在の情報の流通はパッケージにして販売したり，コピーガードをかけたりして，物としての性質をむりやり持たせることにより，既存の物流機構や販売制度に乗せて流通させている．これでは，情報の持っている本来の素晴らしい性質を殺していることになる．そこで，自由にコピーや入手が可能でなおかつ情報の提供者に権利侵害のない形で相応の対価を返す事ができるようになれば情報の流通は飛躍的に増加することになると思われる．この様な発想で，超流通などが従来から提案されている [1]．また，情報の提供に対して旧来の物流にのせるような場合の様にイニシャルコストがかからなくなるため，一般の人がだれでも思いついた時に情報発信をすることができるようにもなる．この様な環境へ至る第一歩として，大量情報を廉価に蓄積できる CD-ROM を用いて新しい情報流通の仕組みが試みられている．これは，流通させたい情報を暗号化することにより使用できないようにしておき安価な CD-ROM を媒体として非常に安くエンドユーザの手元に届ける．エンドユーザはその情報を利用したくなった時に，その使用権を得ることによりすぐに利用できる．すでに，我国でも幾つかサービスが開始されているが，米国では２０種類近くのこのような CD-ROM がすでに流通している [2]．既存のこのようなシステムは，人間の音声により鍵を授受する仕組みである．これに対して我々は，この様な情報の流通を実現する方式として，鍵を蓄積管理しているサーバと端末がオンラインで接続し，鍵の配送と課金処理を全自動かつ安全に行なうシステム（InfoKet システム）を構築した．上記の既存のサービスでは，情報の売り切りサービス（チャージパーコピー（CPC））のみしか実現できないが，こののシステムを利用することにより，CPC 以外の以下のような質の異なるより柔軟なサービスを実現することができる．

1. CPC のみでなく，利用に応じた課金（チャージパーユース（CPU））が可能となる．
2. アンケートや通販の申し込を自動化でき，同時に支払も自動化できる．
3. オンライン情報と融合した柔軟な情報提供が可能となる．
4. 24 時間のサービスが低コストに実現できる．

以下，第２章では，新しい情報流通のサービスコンセプトを述べる．第３章ではそのコンセプトを実現するプラットホームである InfoKet の要求条件とそのシステムの概要を示す．

2 新しい情報流通サービス

2.1 基本的考え方

情報はトラックなどの大がかりな物理的輸送手段を使用しなくても必要なところへ届けることができる．通常は無線通信，有線通信，CD－ ROM などの媒体を通して必要なところへ情報が伝達される．しかし，情報の伝達コストが低く押えられるにも関わらず例えば，ネットワークを通じたソフトウェアの流通はパッケージ販売に比較すると良く使われているとは言いがたい．さらに，手元にあるソフトウェアについても，コピープロテクトをしたりハードキーをつけたりとむしろ情報の優れた特徴であるコピーコストが低いという性質を殺すような施策がとられている．このように，現状では情報のスムーズな流通が阻害されていると言っても過言ではない．このような一見不可思議な現象は状況は，以下の原因で生み出されていると考えられる．

1. 社会制度が物流に最適化されているため，さしあたりの情報の流通のためには現状の物流に情報を載せるのがてっとり早い．
2. コピーコストや伝達コストそのものは非常に低くできるが，その結果生じる著作権侵害などの問題に対処できていない．
3. ネットワークを使った流通の場合などは，情報の販売代金を回収する適切な方法が少ない．

１の問題は社会的問題であるため，少しづつインパクトの少ないやり方で改善して行く必要がある．２の問題は技術的に解決できると思われる．３の問題は技術的問題というよりは，金融制度などの制度面の制約が大きいが，クレジットカードなどのオンライン決裁機能や

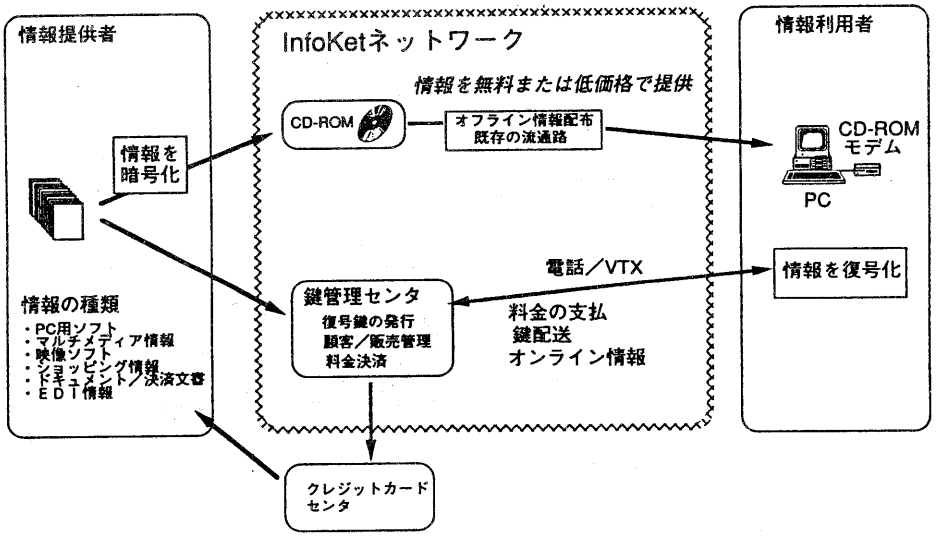

図1： 情報流通サービスイメージ

網の代行徴収機能などを巨く使用することによりかなり解決できる．本稿では，まずCD− ROMを媒体として情報を流通させる場合に，上記の問題を解決する手段としてInfoKetプラットホームを構築した．InfoKetで構築できる情報流通サービスのイメージを図 | に示す．図 | に示すように，大量の情報を暗号化しCD− ROMに格納する．情報が暗号化されているためCD-ROMの生のデータを入手してもそれを利用することはできないため，暗号化される前は多量で高価な情報であってもCD−ROMの原価程度でも流通させる事ができる．ユーザはその情報を使いたい時に，使用権（復号化鍵）を管理しているセンタにアクセスして代金を支払い，鍵をもらって情報を使用する．こうすることにより，大量の情報やソフトウェアを手元に置くことができ使いたい時に何時でも手に入れられるようになる．さらに，暗号化された情報は原理的にコピー自由であり（現InfoKetシステムでは運用上できない）どのような流通経路であろうが何の制限もなく自由に取り扱う事ができる．究極的にはすべてのコンピュータ環境にInfoKetシステムが埋め込まれれば，情報が暗号化されているということを意識せずに，CD− ROMや通信を介して自由に手に入れた情報を何時でも利用することができるようになる．もちろんその際には，必要な課金処理などが自動的に行なわれていることになる．

2.2 システム上の要求条件

ここでは，これまで述べてきたサービスを構成する上で要求される機能について概観する．

2.2.1 システムトータルとしての要求機能

課金処理（決裁機能） 情報を流通させる場合に，その場で課金をする機能である．

使用権配布 料金支払などある条件を満たさないとエンドユーザ側でユーザが目的とする情報を使用することができないようにする機能である．この機能を実現する具体的方式として，暗号技術を利用している．そのために，使用権の授受は鍵の授受として取り扱われる．

使用権管理 使用権（具体的には鍵）はサーバ側で一元的に管理される．鍵とCD-ROMタイトル，CD-ROM内の個々の情報と鍵とのリンク情報あるいは情報に関する販売者の情報などを管理する．

表 1: 防御方法

攻撃対象	想定される攻撃	防御方法
情報そのもの	暗号解読	情報の暗号化（秘密鍵方式）
アクセスプログラム	プログラム解析	鍵はアクセスプログラム中にのみ存在
通信電文	電文解析	各種暗号方式を組み合わせた方式
端末	なりすまし	乱数生成による過去電文の再利用防止
サーバ	なりすまし	乱数生成による過去電文の再利用防止

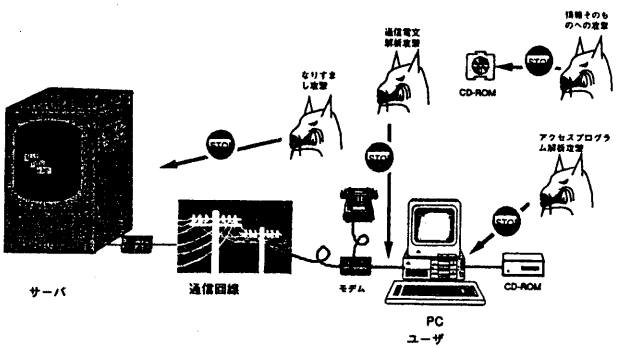

図 2: エンドユーザから見た攻撃対象

利用状況把握　情報流通は物流と異なり，何もしないと販売料などは何も把握できない．そこで，使用権の販売状況などを把握する必要がある．

復号化，暗号化　暗号化はオーサリングシステムで行ない，復号化はエンドユーザ端末で実行される．暗号化と復号化はその使い方によりペアで取り扱われる必要がある．例えば，ソフトウェア販売の場合 (CPC) は，あるファイル（あるいはディレクトリ）が暗号化され，そのファイルが端末側でまるごと復元される．また，チャージバース（CPU）の場合は，アプリケーションがそれを意識してチャージの方法をコントロールする必要があるため，暗号化する部分やその方法などはかなりアプリケーション依存となる．

2.2.2　セキュリティ

本システムでは流通させる情報の使用をコントロールする必要がある．そのため，情報の使用をコントロールするための機構が悪意を持った者にやぶられないようにしなければならない．一般にオンラインシステムではエンドユーザの視点から見た場合図 2に示すような攻撃ポイントがある．

本システムでは，それぞれの攻撃に対して表1 に示すような対策をこうじている．

3　InfoKet プラットホーム

InfoKet プラットホームはこれまで述べてきたコンセプトを実現するためのプラットホームであり，このプラットホーム上にアプリケーションを構築することにより，様々なサービスが実現できる．本章では，このプラットホームの構成について述べる．

3.1　全体構成

本プラットホームは 図 3に示すように，オーサリングシステム，エンドユーザ端末，サーバの大きく三つのサブシステムから構成される．オーサリングシステムで作られた CD-ROM は，流通機構に乗せられエンドユーザの手元に届く．エンドユーザはその CD-ROM を使用する時に鍵の受けとりと料金支払をする（端末側で自動的に行なう）．その際，エンドユーザ端末はサーバと通信する．サーバ側では鍵を送ると同時に課金処理などを行なう．

3.2 オーサリング系

オーサリング系のプラットホームは，情報を効率良く暗号化し，端末アプリケーションのデバグを含めた開発作業を効率良く行なうためのプラットホームである．以下の機能を持つ [3].

1. 鍵生成
2. 情報の暗号化
3. APをデバグするためのスタブ
4. 鍵サーバで必要な各種の情報生成

3.3 端末系

端末系のプラットホームでは，以下の機能を持つ．

1. 通信機能
   電話網およびビデオテックス (VTX) 網を用いた下位レイヤのプロトコル処理を行なう．
2. 鍵配送／課金機能
   InfoKetプロトコルを使用して，サーバと接続し安全に鍵を受けとる．課金のためのクレジットカード番号なども，安全にサーバに送ることができる．
3. 情報の復号化
   サーバから受けとった鍵により，暗号化情報を復号化し暗号化前の完全な情報を生成する．この機能は主に，チャージパーユース (CPC) の時に使用する．この機能を使用した場合の流れを図4に示す．図に示すような方法をとることにより，ビジネス上重要な以下の特徴がある．
   (a) 復号化するAPのインストーラの改造が極小
   (b) 鍵をローカルに保存しない（セキュリティが高い）
   (c) 責任範囲が明確
4. 基本機能の提供 チャージパーユース (CPU) を実現するための基本機能を提供する．

3.4 サーバ系

サーバ系のプラットホームでは以下の機能を持つ．

1. 鍵配送／課金機能
   InfoKetプロトコルを使用して，端末からの要求に応じて鍵を配送する．配送する際に，会員ID・パスワードのチェック，各種有効期限や条件などをチェックする機能，クレジットカード課金やビデオテックス網の課金を行なう機能を持つ．
2. 鍵の管理機能
   鍵に対応する情報の属性 (情報の名前，定価，販売価格，有効期限，情報の発行元，等) などを管理する．
3. 鍵配送記録、検索機能
   鍵を配送した際の記録を保持し，伝票や明細を管理・出力する機能を持つ．また，後の問い合わせに答えるために必要となる情報蓄積・検索の機能を持つ．

3.5 InfoKetプロトコル

InfoKetプロトコルとは，サーバとエンドユーザを繋ぐプロトコルであり，主に以下に示す機能を持つ．

1. 安全な鍵配送
2. 認証
3. クレジット課金機能
4. ビデオテックス課金機能
5. 秘密通信機能

上記の機能は，各種の暗号方式を組み合わせ、暗号鍵をトランザクション中に複数回変更する方式を用いて実現している．プロトコルは下位層より、データ転送および課金処理レイヤ、鍵配送レイヤとしている。更に端末側では鍵配送グルーを上位層として定義する（図5参照）。

データ転送および課金処理レイヤは、メッセージ伝達のための基本機能を提供するが、課金処理部分に関してメッセージの扱いが網により異なるため、課金処理も同じ層として扱う構成となっている。課金は現在クレジッ

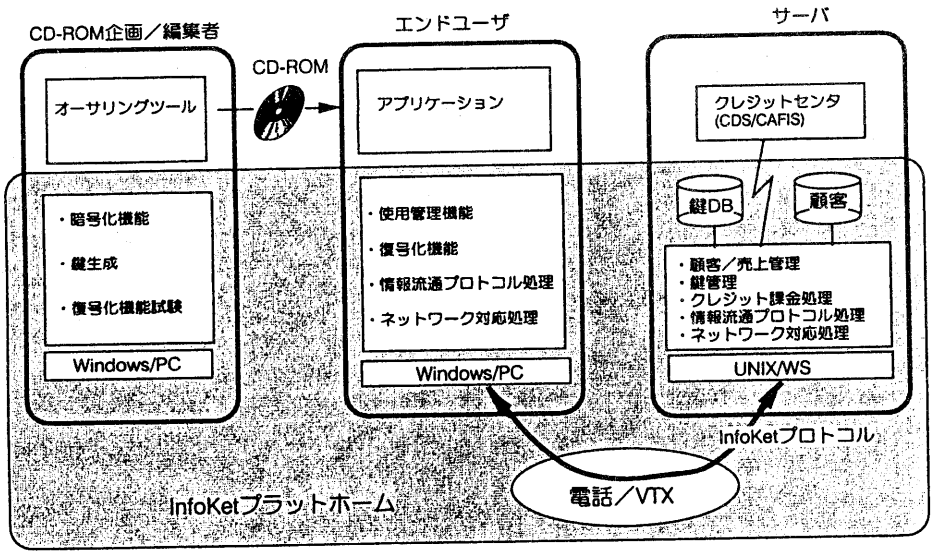

図3： InfoKetプラットホーム全体構成

ト課金、VTX 網課金が定義されている。鍵配送レイヤはサービスの実現部分であり、パスワードによる認証、配付制限、鍵の配送機能を提供する。下位層で網の性質の違いは吸収してあるので、鍵配送レイヤは網の性質や課金種別に依存しない。なお鍵配送トランザクション中に鍵以外の情報を同時に暗号化し送ることも可能である。鍵配送グルーは、さまざまなアプリケーションインタフェースを提供するための層であり、機能としては独立している。しかしながらセキュリティの観点から、鍵配送プロトコル実現部と同じモジュールとして実現する。

4 おわりに

情報を流通させるための新しい手段としてのInfoKetプラットホームの構成について述べた。この様な流通サービスは今までにない新しい試みであるが，パッケージ流通の置き換えであるチャージバーコピー（CPC）方式については，先行するサービスの状況などから既存の流通業者の反発などがあり得る．しかし，チャージバーユース（CPU）については，新マーケットを創造する可能性を秘めており，今後InfoKetプラットホームを用いて多くのCPUサービスの実現が期待される．

謝辞

本研究の機会と有益な御助言を頂いたNTTソフトウェア研究所，細谷所長，中村プロジェクトリーダ，NTTサービス生産本部，市川部長並びに関係者皆様に深謝致します．

参考文献

[1] 森 亮一，超流通の構造，防御，人々の利益，電子情報通信学会，信学技報 ISEC94-13,pp1-8(1994).

[2] CD-ROM WORLD,:Attention, Keystroke Shoppers!,pp47-51(1994).

[3] 三宅，奥山，寺内，金井,:CD-ROM 情報流通システムにおける情報オーサリングに関する一考察，信学会総合大会，(1995).

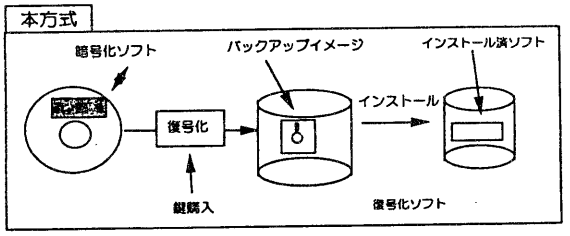

図 4: 端末での CPC 実現方式

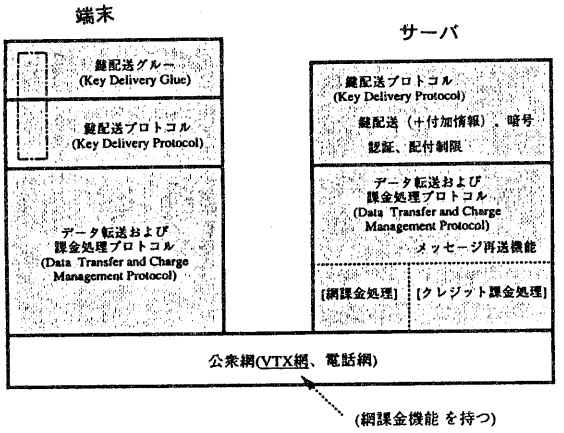

図 5: InfoKet プロトコルレイヤ構成