マルチメディア通信と分散処理 79－16
（1996. 11. 15）

情報流通システムにおける鍵配送通信の実装

森保 健治　　明石 修　　寺内 敦

NTT ソフトウェア研究所

概要

近年，インターネットの普及により，EC (Electronic Commerce)，つまりネットワークを利用した電子商取引が一般的になりつつある．今後，ネットワーク上の情報販売に対する市場が拡大すると予想される中で，我々は，情報販売のためのプラットフォームとして，情報流通システム Infoket を提案してきている．Infoket は，ディジタル情報の特徴を生かしつつ，情報提供者の利益を守ることを目的としたシステムである．本稿では，インターネットを利用した情報販売について，Infoket を実現するための KEY となる技術，鍵配送機能について，実装し評価を行なったので報告する．

A Communication Architecture of Key Delivery Protocol for Information Market System

Kenji MORIYASU　　Osamu AKASHI　　Atsushi TERAUCHI

NTT Software Laboratories

abstract

Recently, the internet is spreadging around the globe and EC (Electronic Commerce) becomes prevailing for us. In the near future, the market on the internet for information business will enlarge more and more, then we propose an informatin distribution system Infoket as a platform of information business.

The aim of Infoket is to make the best of the features of digital information and to preserve the information provider's profit. This paper describes the result that a key delivery protocol which is the KEY technology of Infoket is developed and estimated.

1 はじめに

近年，インターネットの普及により，EC (Electronic Commerce)，つまりネットワークを利用した電子商取引が一般的になりつつある．ネットワーク上で扱われる商品には，有形である場合と無形である場合に大きく分けることができ，それぞれ物品販売，情報販売に対応づけることができる．現在は，電話，FAX 等での注文，商品カタログの配布をインターネットに置き代えるだけで，導入が比較的容易な物品販売が主流であるが，今後は情報販売が大きく飛躍するものと考えられる．なぜなら，マルチメディア情報などで代表されるデジタル情報は，コピー，伝送，在庫管理が容易という，ネットワークで扱うのに優れた特徴を持つことと，パソコンの普及，オーサリングツールの発達により，有料のデジタル情報に対する市場はこれから爆発的に拡大することが予想されるからである．

我々は，ネットワークを利用した情報販売のためのプラットフォームとして，情報流通システム Infoket [1] を提案している．本稿では，特にインターネット上で Infoket を実現するための **KEY** となる技術である鍵配送機能について，実装し評価を行なったので報告する．

2 情報販売の方式

情報販売を実現する上で最も重要なポイントは，情報提供者 (以下，IP) の利益を守ることである (もちろん，購入者のプライバシ保護は，情報販売に限らず EC 全体のレベルで重要である)．デジタル情報は，コピー，伝送，在庫管理が容易という，ネットワークで扱うのに優れた特徴を持つが，その特徴故に，不正利用により IP が不利益を被る場合が少なくない．

インターネットを経由して情報を販売する手法には，以下の二つの方式が考えられる．いずれの方式であっても，悪意のある第三者に対して購入者のプライバシを保護するため，購入していない第三者に対して無料で商品 (デジタル情報) を渡さないために，秘密通信技術の利用は不可欠である．

(方式 1) 商品配布時に課金
SSL などの秘密通信プロトコルを利用して，購入情報と交換に商品を download する．

(方式 2) 使用権の付与時に課金
商品はそのままでは利用できないような形で事前に配布し，秘密通信プロトコルを使って，購入情報と交換に，商品が利用できる function を利用者に与える．

我々は，(方式 2) の手法を取った情報流通システム Infoket[1] を提案している．Infoket は，商品の利用時に必ず代金が徴収されるようにすることによって，前述のデジタル情報の特徴を生かしつつ，IP の利益を守る，つまり著作権の保護を目的としている．

Infoket では，予め商品は暗号化して配布される (以下，暗号化商品)．この時，暗号化商品はそのままでは使用することができないので，無料で配布することができ，WWW サーバや anonymous FTP サーバなどで商品展示することが可能である (ただし，利用者が download したファイルの正当性をチェックするための機能は必要である)．暗号化商品を手にした利用者が商品を購入する際には，暗号を解くための復号鍵を管理する “鍵センタ” に接続し，クレジット番号等の購入情報と復号鍵を交換する．この購入処理中，利用者端末では，受信した復号鍵を使って暗号化商品が自動的に復号化され，商品として利用できる形となる．と同時に，鍵センタでは購入情報を元に課金処理を行ない，IP への収益が確保される (図 1)．

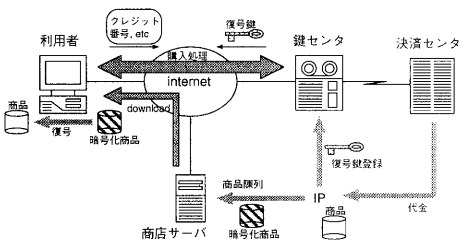

図 1: Infoket の概要

(方式 1) と (方式 2) の特徴を表 1に示す．

表 1: 情報販売手法

	(方式 1)	(方式 2)
商品の事前配布	ない	暗号化した商品を自由に配布
販売形態	商品そのものを販売	復号鍵を販売
対象商品	刻々と更新される情報	静的情報，大容量情報
商品展示	WWW サーバ等を利用	
IP の作業	暗号化の必要なし	暗号化および復号鍵の登録

株式現況，DBの集計情報といったリアルタイムな情報は，いちいち暗号化して，暗号化商品が流通してからでないと使えないととなると，情報としての価値が下ってしまうので，(方式1)が適していると思われる．一方，市販ソフトウェアや動画像データような比較的静的，大容量な情報は，購入処理中の回線トラブル等を考慮すると，任意のタイミングで暗号化商品をdownloadでき，購入に要する時間が短い(方式2)が適していると言える．つまり，両者の方式は，どちらか一方のみがあれば完全という訳ではなく，商品の性質によって，互いに補完し合う方式であるといえる．

さて，Infoketを実現する上で必要最小限の機能は以下の通りである．(*印は，(方式1)と(方式2)で共通)

(機能1) 暗号化商品の安全な配布機能 [2]

(機能2) 安全な購入処理機能 [3]

(機能3) 鍵センタや商店における課金機能 (*)

(機能4) 鍵センタへの復号鍵の登録機能

(機能5) 商店サーバでの(暗号化)商品の陳列機能 (*)

本報告では，(機能2)について実装し評価を行なったので報告する．

3 鍵の配送機能

(機能2)は，利用者端末で入力されたクレジット番号，商品ID等の購入情報と商品IDに対応する復号鍵を安全に交換する機能，および利用者端末にて受信した復号鍵を使って暗号化商品を復号する機能から構成される．(機能2)に対する要求条件は以下の通りである(詳細は文献[3])．

(条件1) 購入情報を第三者から保護

(条件2) 復号鍵は第三者からのみでなく，利用者からも保護

前者は，EC全体のレベルで必要な条件であるが，後者は，(方式2)を取るInfoket特有の条件である．復号鍵を利用者に渡してしまうと，利用時の代金徴収機能が働かなくなってしまうばかりか，他の利用者が無料で商品を手に入れることも可能となるからである．

今回インターネット上の鍵配送機能を実装する上で，さらに以下の点を配慮した．

(ポイント1) 複数の鍵センタに，鍵センタ用，端末用各プログラムを配布することを考慮する．

(ポイント2) 利用者端末にて，端末プログラムがHelperやPlug-inなどで実現できるような汎用的なAPIとする．

(ポイント3) 鍵センタ側では，他の機能(例えば，DB構成，運用機能など)に依存しないAPIとする．

(ポイント4) 複数の決済手段を利用できるようにする．

4 実装

4.1 (ポイント1)の実装

前章の(条件1)(条件2)を満足する機能を得るだけであれば，SSL等の汎用的な秘密通信プロトコルを利用し，そのAPI上に復号鍵を利用者に見せないような復号鍵管理層を作成すればよい[3]．しかし，誰でも入手可能な既知の秘密通信プロトコルを利用することにより，新たに以下の攻撃が生じうる．

(攻撃1) 秘密通信プロトコルのAPIの返値を監視し，受信した復号鍵を得る攻撃
既知の秘密通信プロトコルのAPIの返値は，既に復号化された通信メッセージであるため，それを監視することにより，その中に含まれる復号鍵を見付けることが容易になる．つまり，端末プログラムに対する監視ポイントが限定されてしまい，復号鍵を見付けるための手掛りを与えてしまうことになる．

(攻撃2) 自作の復号鍵管理層を作成し，鍵センタへ接続し復号鍵を獲得する攻撃
正規の端末プログラム中の復号鍵管理層の代りに，復号鍵を表示するような復号鍵表示プログラムを組込んだ端末プログラムを使って鍵センタへ接続し，復号鍵を得ることが，既知の秘密通信プログラムを利用した場合，困難でなくなる．

(攻撃1)(攻撃2)を防ぐために，復号鍵をさらに暗号化して復号鍵管理層で復号するという方式が考えられるが，それでは何のために秘密通信プロトコルを利用したのか分らなくなってしまう．

さらに，互いに関係のない複数の鍵センタ，およびそれぞれの鍵センタに対応する複数種類の端末プログラムが存在する場合，ある鍵センタの運営者(端

末プログラムを作成する) が, (攻撃 2) によって, 他の鍵センタの鍵取得プログラムを作成することになれば, (ポイント 1) を満足することはできない.

したがって, 今回の実装では, 秘密通信機能および復号鍵管理機能を一つにまとめた鍵配送機能を専用に設計した. 具体的には, 文献 [4] で挙げた電話網経由の鍵配送機能をインターネット向けにセキュリティ強化する方向で検討した.

4.2 (ポイント 2)(ポイント 3)(ポイント 4) の実装

(ポイント 2) や (ポイント 3) を実現するには, 購入処理のために必要な機能に対して過不足ない API を定める必要がある.

特に鍵センタには, 商品 DB(復号鍵を含む), 売上 DB などによる各種情報管理機能, 決済システム (例えば, クレジットカードの場合は, CAFIS センタなど) との接続機能, 運用状態監視機能などがあり, これらの機能に対する API が必要となる. 具体的には, 以下を考慮した.

- 利用者の認証機構 (会員 DB とのインタフェース)
- 復号鍵の取出し機構 (商品 DB とのインタフェース)
- ロギング機構 (売上 DB および各種ログ機能とのインタフェース)
- 課金機構 (決済システムとのインタフェース)

一方, 端末側は, 購入情報を鍵センタに送るための API があればよい.

また, (ポイント 4) のために, 以下を考慮した.

- 購入手段を選択できること
- 将来, 新しい購入手段が増えても API の変更とならないこと

以上のことを考慮して, 以下の API を用意した (利用者が端末に打込むための GUI に関するものを含まない).

- 端末側 API

  (API1) 商品の購入
  購入手段, 購入手段に応じた購入情報, 商品 ID, 商品展開ディレクトリなどを引数とし, 復号鍵の受信, 商品の復号化および指定ディレクトリへの展開, 復号鍵の破棄を一度に行なう API である.

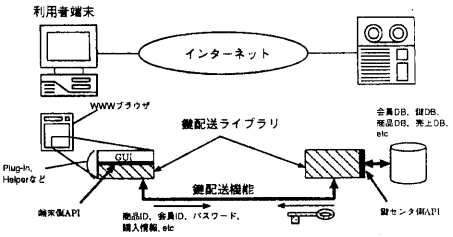

図 2: 鍵配送機能の API

(API2) 商品情報の確認
本機能は, 2 章の (機能 1) に関するもので, 暗号化商品の内容を読み出す API である. 詳細は文献 [2] に譲るが, 前述のように暗号化商品は, WWW サーバや anonymous FTP サーバにて自由に配布できるようにするために, 流通途中で改ざんされず, かつそれ自体単独で流通できる必要がある. 具体的には, 暗号化商品には, 鍵センタに関する情報 (アドレスなど), 商品に関する情報 (価格, 有効期限など) を, 暗号化された商品本体とともにたたみこんで格納されており, summary を付けて 1 つのファイルにカプセル化してある. 本 API は, 端末プログラムがそれらの内容を読み出すために利用する.

これらの API の上に GUI などを AP として作成することにより, Helper や Plug-in などの端末プログラムを実現することができる. 端末側 API の基本的な利用法は以下の通りである.

1. (API2) を実行し, 指定された暗号化商品の価格等を確認, 表示する.
2. クレジット番号等の購入情報の入力を受付ける.
3. (API1) を実行し, (API2) で読み出した情報 (商品 ID など) と, 入力された情報を鍵センタへ送り, 購入処理を行なう.

- 鍵センタ側 API

  (API3) 会員情報のチェック依頼
  利用者の鍵センタに対する会員 ID, パスワードを引数とし, そのチェックを依頼する API である.

  (API4) 復号鍵の獲得
  商品 ID を引数として, 復号鍵が登録され

ている商品 DB(復号鍵 DB) から復号鍵を取得するための API である.

(API5) 購入手段に応じた課金処理依頼
購入手段および購入情報を引数とし，購入手段に応じた適当な課金処理を依頼する API である.

(API6) 売上情報の登録
鍵センタで売上情報をタンキングするために，会員 ID，商品 ID，価格，購入結果などを引数として，売上 DB 等へ登録することを依頼する API である.

これらの API は，鍵センタ側の鍵配布機能を実行する常駐プログラム (daemon) から call されるものである．各 API は上記の順序で呼ばれるため，それに対応するプログラム (特に各種 DB とのインタフェース部分) を作成することによって，鍵センタを構築することができる.

5 評価

5.1 攻撃に対する防御強度

文献 [4] では，プラットフォームとなるネットワークとして電話網を利用している．インターネットでは，電話網に比べ，中継ノードでのメッセージのタンキングが容易であることに起因する攻撃，例えば，メッセージの改ざん，利用者の認証後の成りすましがありうる．したがって，各メッセージに対する summary による改ざんチェック機能，メッセージ間に関連を持たせた成りすまし防御機能などを，新たに導入した．表 2に実装した鍵配送機能の対処および効果を示す.

表 2: 鍵配送機能の防御法

攻撃	対処
盗聴	利用者端末，鍵センタ間の全てのメッセージは暗号化されている．暗号鍵は接続するたびに異なるため，メッセージの再利用はできない.
改ざん	各メッセージの summary を取ってメッセージに添付している．改ざんされた場合は，その summary を調べることでチェックすることができる.
成りすまし	公開鍵方式を利用しており，互いに認証をすることができる．さらに，各メッセージ間での矛盾チェックを行なっているため，通信途中から成りすますことはできない.

5.2 API の十分性

5.2.1 端末側 API

文献 [3] では，商品の購入 API として，復号鍵の受信，商品の復号化，復号鍵の破棄に対してそれぞれ独立の API を設けることを提案している．これは，利用者端末の HD 上に商品を復号，展開しない Pay per View 型の販売方式 (利用時毎に課金する販売方式) を実現する上で，復号鍵が必要になるタイミングが多岐に渡るであろうという予測から，復号鍵の保存期間を制御可能とすることを目的としている.

しかし，前述のように複数の鍵センタで利用できるように，鍵配布機能を (ライブラリなどにして) 配布することを考えると，復号鍵の保存を自由に制御できることからくる復号鍵露見のリスクを回避することと，Pay per View 実現の自由度を拡大することをトレードオフと考えて，今回は前者を優先することとした.

また，(ポイント 2) を満たすように Windows3.1, Windows95 で動作可能なライブラリとして実現したため，本ライブラリ上にユーザからの入力 GUI プログラムを作成することにより，Helper や Plug-in として端末プログラムを実現することが可能となった．これにより，現在広く行なわれている，WWW を利用したショッピング用プログラムとして違和感のないユーザインタフェースを実現することができた．図 3に鍵配布機能を Helper として実現した購入画面例を示す.

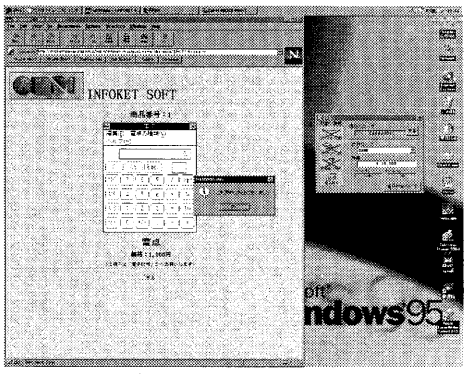

図 3: Infoket による購入画面例

5.2.2 鍵センタ側 API

文献 [4] で実現されている鍵センタ機能を，本 API を利用しても十分実現できることを確認した．さらに，(ポイント 3) を満たす汎用的な API とすることができたため，たとえ既存の DB があるホストマシンに対しても，DB とのインタフェースプログラムを作成するだけで，容易に鍵センタを構築できるようになった．

さらに，課金手段を選択できるようにし，課金手段に応じた購入情報を扱えるようにしたため，(ポイント 4) も実現することができた．

5.3 サイズ

鍵配布機能を実現したプログラムサイズを表 3に示す (暗号化ルーチンを除く)．

表 3: 鍵配送プログラムの規模

	規模 (Kline)
端末側プログラム	2.7
鍵センタ側プログラム	2.2

本プログラムを利用して，実際に情報流通システムを構築するには，前述のように，ユーザとの GUI 部分および鍵センタ側の各種 DB とのインタフェース部分を作成する必要がある．これらの部分は，Visual Basic などによる画面入出力や SQL を call するプログラムである．本プログラムは，それらの外部プログラムとリンクしても，性能上問題ない規模で実現できたと言える．

6 おわりに

本稿では，情報流通システム Infoket をインターネット上で実現するための要素技術である鍵配送機能について，実装し評価を行なったので報告した．

本機能は，ネットワーク上の商取引に必要な条件である，購入者のプライバシの保護だけでなく，暗号化商品を予め配布する Infoket のコンセプトにおいて必要な，復号鍵の露見の防御を目的としており，Infoket 実現の KEY となる機能であると言える．

今回，鍵配送機能を，インターネット上での第三者および利用者からの攻撃への防御，および汎用的な API 構成を考慮して実装したが，ほぼ目標通り実現できたと思われる．

今後は，以下を検討していく予定である．

- 現在の Infoket は，基本的に会員制を前提としているため，会員情報を各鍵センタが管理する構成になっている．今後，CA が普及して会員情報が CA で扱われる場合への対応を行なう．
- 情報販売の場合，購入単位として個数 (市販ソフト 1 本，2 本…，) が一般的であるが，物品販売の場合必ずしもそうではない場合が多い (D ○m × W △m × H □m など)．このような場合，画一的な購入画面では，対処できないことになり，予め Helper などで作っておくことはできない．したがって，(既存の WWW の改造なしに) 購入画面を柔軟に作成，表示する機構を検討する．
- いろいろな暗号化方式で暗号化された商品や，複数のファイルで構成された商品が扱えるようにする．

参考文献

[1] 金井，三宅，明石，生沼，“マルチメディア情報流通システム (InfoKet)”，情処技法 DPS70-6(1995, 5)

[2] 明石，森保，寺内，“FleaMarket 方式による情報流通”，DPS ワークショップ 95，pp243-250，(1995.10)

[3] 森保，明石，寺内，三宅，“情報流通システムにおける鍵配送通信の構成法”，DPS ワークショップ 95，pp.259-265，(1995.10)

[4] 三宅，明石，奥山，寺内，森保，“CD-ROM 情報流通サービス実現方式”，NTT R&D，vol. 44, pp.881-886，(1995.10)