FleaMarket方式による情報流通 *

明石 修　　森保 健治　　寺内 敦†
NTT ソフトウェア研究所 ‡

概要

情報は非常に小さなコストで複製や移動が可能である点に特徴があり、本質的に従来の物理的な流通システムの制約を受けない。我々はこの性質に注目し、情報を暗号化して自由に配布し、必要な時に復号鍵を配布することにより情報を参照する情報流通方式を提案してきた。この方式をインターネットに適用するにあたって、FleaMarket方式による情報流通を提案する。

FleaMarket方式による情報流通では、大規模な特定組織のみでなく、一般ユーザがネットワーク上のFleaMarketにおいて簡易に情報を登録し、暗号化した後に付加情報と共にカプセル化して流通させ、最終的に情報を参照したユーザからその料金を回収することが可能である。このとき復号鍵取得手続きを計算機上で実現するため、鍵取得に関するマーケット情報管理をシステムに組込むことが可能であり、FleaMarketへのpaybackや、さまざまな形態での商品管理へ適用できる。本稿ではFleaMarket方式による情報流通のモデル、およびその実現法に関して述べる。

1　はじめに

情報の流通は、非常に小さなコストで複製や移動が可能であり、本質的に従来の物理的な流通システムの制約を受けないことに特徴がある。これは必要に応じて、電子的な手段により自由に情報にアクセスすることが可能であることを意味する。一方情報には著作権が存在し、場合によっては情報の使用者を特定し、料金を回収する必要がある。

我々はこのような情報の特質に注目し、CD-ROMを用いて多数の暗号化情報を配布し、ユーザが必要な時に公衆網を通じて情報の復号鍵を配布するサーバに接続し、有料情報の場合には料金決済を行なった後、その情報を参照することが可能な情報流通システム(Infoket-C[2])を実現した。しかしながらCD-ROM自体は物理的な媒体であり、情報の本質を生かすにはインターネットのような環境での情報流通を実現する必要がある。また情報の提供者は特定の大きな組織になりがちであり、情報の提供者とユーザは分離し一方向の情報の流れしか起こらないという問題がある。

一方特定サーバに情報を置いておき、そのサーバから情報を持っていく時に認証/決済を行ない、情報料金を回収するという方式[6, 4]がある。しかしながらローカルな計算機に情報を置いておき、実際に使う時に料金を払うというCharge Per Useというような方式への適用は難しい。また商品となる情報を陳列し、認証および決済処理を行ない、更に情報の転送も行なうとなると特定サーバやネットワークへの負荷は大きい。

我々はインターネットに情報流通モデルを適用するにあたって、FleaMarket方式による情報流通システムを提案する。FleaMarket方式による情報流通とは、大規模な特定組織のみでなく、一般ユーザが簡易に商品となる情報を登録し、付加情報と共に暗号化して自由にネットワーク上を流通させ、最終的に情報を使用したユーザからその料金を回収することが可能な情報流通方式である。情報の登録を行ない、情報を流通可能な形に整形

---

*Information Distribution by FleaMarket System

†Osamu Akashi, Kenji Moriyasu, Atsushi Terauchi
akashi@nuesun.ntt.jp, {moriyasu,terauchi}@slab.ntt.jp
‡NTT Software Laboratories

する場所をFleaMarketと呼ぶ。このとき復号鍵取得手続きを計算機上で実現するため、鍵取得に関するマーケット情報管理をシステムに組込むことが可能であり、FleaMarketへのpaybackや、さまざまな形態での商品管理へ適用できる。本稿ではFleaMarket方式の情報流通モデルに関して述べた後、システムの構成と実現法の詳細に関して述べる。

2 情報流通モデル

さまざまな組織やホストを相互接続するインターネットに情報流通モデルを適用するにあたって、一般ユーザがCD-ROMのような物理的な媒体を介さずに簡易に情報を配布できることが重要である。FleaMarket方式による情報流通モデルでは、情報提供者はFleaMarketと呼ぶ場所で情報をアップロードして登録し、復号化のための制御情報と共に暗号化して自由に配布する。この暗号化された1かたまりのデータをカプセルと呼ぶ。

情報使用者はあらかじめ配布されたカプセルアクセス関数を通じて、カプセルから情報を復号して取り出し、必要に応じて料金の支払いを行なう。すなわちネットワークにアクセス可能なユーザは、情報提供者にも、消費者にもなれるという特徴を持つ。図1にモデル概要を図示する。

このモデルでは、以下のサブシステムが定義されている。

- FleaMarket ··· 情報の登録、配布
- 鍵センタ ··· 復号鍵管理、決済
- NetBank ··· 決済処理を抽象化(課金システムの実現に関しては[5]参照)
- 端末アプリケーションプログラム ··· カプセルアクセス関数ライブラリとリンクされる
- anonymous FTP site

本モデルでは、FleaMarket、鍵センタ、NetBankは信用できる組織が運営していると仮定する。またカプセルアクセス関数ライブラリは信用できる組織がバイナリを配布することと仮定とする。サブシステムはそれぞれ複数存在可能であるが、説明の簡素化のためそれぞれ1つして説明する。

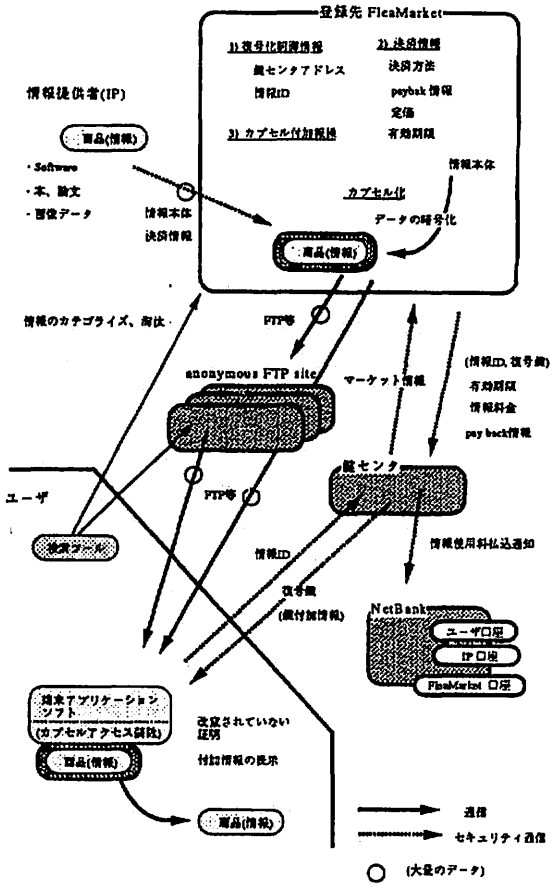

図 1: FleaMarket方式概要

FleaMarketは、情報提供者が情報(=商品)の登録を行なう場所である。登録とは、情報のアップロード、決済方法の取り決め、鍵配布による復号化のための制御情報の付加を指す(3.1節参照)。FleaMarketはこれらの情報をカプセルとしてまとめ、暗号化する。FleaMarketはカプセルを商品として展示し配布するが、このカプセル化された情報は公開鍵暗号によるディジタル署名とデータ暗号化機能により改竄を防止してあるため、anonymous FTPサイトに自由に配布することも可能である。カプセル化の具体的な仕組みに関しては、3.2節で述べる。

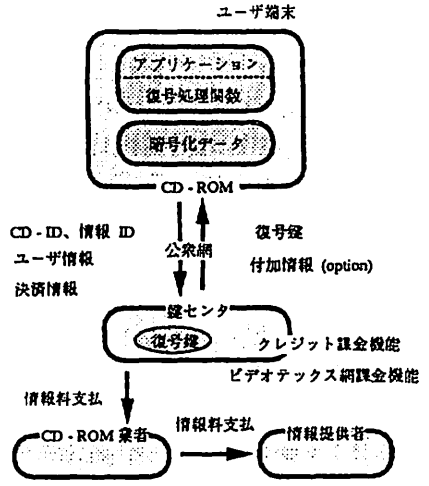

図 2: Infoket-C 概要

鍵センタは情報を復号するための鍵の管理を行なう。鍵センタは復号鍵のほかに、情報料金や情報有効期限に関する制御情報を持ち、情報使用者との間の決済も行なう。FleaMarket は情報のカプセル化後、鍵センタと通信し、復号に必要な情報を鍵センタに送る。逆に鍵センタは復号鍵へのアクセス等のマーケット情報を FleaMarket に定期的に送信し、その情報は FleaMarket での商品管理や、ユーザへの提示等に使われる。(5章参照)

ここで FleaMarket 方式による情報流通のモデルでは、情報提供者と情報使用者は FleaMarket との間で最終的な決済手段を持つことが条件となる。Infoket-C[2] では図 2に示すように、鍵センタがクレジットまたはビデオテックス網によりユーザとの間で決済を行ない、CD-ROM 業者を通じて情報提供者に料金が支払われる。

FleaMarket 方式では、決済に関しては FleaMarket が CD-ROM 業者に相当し、情報提供者に情報使用料を払い込む。しかしながら特定の決済方法を流通方式と切り離して扱うため、抽象的な決済方法として NetBank を導入する。モデル上は鍵センタの指示で NetBank 上の情報使用者の口座から FleaMarket の口座に使用料が振り込まれ、更に鍵センタの復号鍵アクセス情報に基づき FleaMarket の指示で FleaMarket の口座から情報提供者の口座に振り込みが行なわれる。

情報を参照するユーザは、FleaMarket あるいは anonymous FTP サイトにアクセスし、必要な情報を FTP 等の通常の転送プロトコルを用いダウンロードする。端末側ではあらかじめ配布された端末アプリケーションプログラムのカプセル化情報にアクセスする機能を用い、デモに必要な情報や復号に必要な情報等を取り出す。最終的にユーザが情報を復号する時は、端末アプリケーションプログラムを通じて、鍵センタに接続し、復号処理を行なう。

以上のような FleaMarket 方式による情報流通システムでは、一般ユーザが簡易に配布する情報を登録し、その料金を回収するすることが可能となる。また情報のカプセル化により第3者による改竄や偽の情報の混入を防止することにより、通常の anonymous FTP サーバへの配布が可能であり、情報の配布 / 転送、情報の保管、認証 / 決済、という機能をわけることが可能であり、計算機およびネットワークの負荷は分散できる。またローカルな計算機に情報を置いておき、実際に使う時に料金を払うという Charge Per Use 方式への適用が可能である。

なお FleaMarket で扱う情報は、ソフトウェア、文書、画像等の更新頻度のあまり高くない物を対象とする。なお Infoket-C で実現したように、鍵センタ - 端末間で復号鍵以外の鍵付加情報をやりとりすることも可能であるが、"予約システム" 等のように鍵センタから他のサーバに対してトランザクション処理を必要とする種類の物は除く。

3 システム構成と実現

FleaMarket の機能を以下のように分け、個々の機能を説明する。

1. 情報の登録
2. 情報のカプセル化と流通
3. 鍵センタとの情報交換
4. マーケット情報の管理

3.1 情報の登録処理

情報提供者は、ネットワークアドレスの公開されている FleaMarket に接続し、情報登録手続きを行なう。その際の手続きは以下の順番で行なわれる。

1. 情報提供者による流通や決済に関する情報の入力
   - ユーザの NetBank 口座番号 ··· 必要に応じて認証手続き
   - 販売価格 (上限 / 下限)
   - 有効期限 (上限 / 下限)
2. 決済日、 payback 率等の確認
3. 情報 (= 商品) の FleaMarket へのアップロード
4. 鍵配送時の鍵付加情報 (optional)
5. 情報のカプセル化 (3.2節参照)
6. 鍵センタへの復号制御情報の通知

登録された情報には情報 ID が付与され、その情報 ID により鍵センタは一意に復号鍵を対応付ける。鍵付加情報は復号鍵の配送時に、鍵に附随して同時に端末側に送付される情報で、情報提供者付加部分と、 FleaMarket 付加部分からなる。付加情報の中味は随時変更可能である。また情報提供者は情報の有効期限や販売価格を指定するが、これは上限 / 下限の形で設定し FleaMarket が情報有効期限や実販売価格 (= 情報料金) を変更することも可能とする。

FleaMarket はこのような新規登録手続きに加えて、以下よような関連した処理も行なう。これらの手続きを行なうためには、新規登録時に FleaMarket から情報提供者に発行される登録 ID とパスワードが必要である。

- 配布する情報本体の差し替え
- 情報提供者登録データの変更
  - 有効期限、鍵付加情報、 NetBank 口座変更

この処理により、ユーザが該当情報の配布停止や、ソフトウェアの version up 等の差し替え処理を行なうことが出来る。差し替えは、古い情報の復号鍵を有効期限切れとし復号不可とするのと同時に、新しい情報とその復号鍵を登録する。通常の有効期限切れと違う点は、差し替えのお知らせ等の鍵付加情報を登録しておき、古い復号鍵をアクセスした場合でも、ユーザの端末にその鍵付加情報を表示させることができる点である。

3.2 情報のカプセル化

FleaMarket では、ユーザの登録した情報を、流通に適した形に整形する。これを情報のカプセル化と呼ぶ。カプセル化の目的は、情報本体に加えて、復号等に必要な制御情報を 1 つの意味的な固まりとして、1 つのファイルとして扱えるようにするためである。その上で実現する機能として、以下の点があげられる。

- カプセル化したファイルの改竄を検知可能とする
- 特定関数のアクセスでのみ、意味のある情報を取り出せること
  - 情報の隠蔽、保護、統一インタフェースの提供

カプセルは自由な流通の観点から、バイナリデータの入った通常のファイルとして実現するが、意味のある情報を取り出すためには、特定のカプセルアクセス手続きを実行しなければならない。従って、端末側のプロトコル階層は図 3のようになる。

3.2.1 カプセルの構造

カプセルは、情報の復号、決済、証明書といったカプセル制御に関するデータを含むヘッダ部と、内容物である情報やオプショナルなカプセル付加情報を含むデータ部からなる。ヘッダ部は FleaMarket がディジタル署名を行ない、第 3 者による改竄を防ぐ。データ部は先頭にインデックスをおいて構造化し、ヘッダ部にある認証用データと認証関数により第 3 者による改竄が検知出来るようにする。図 4に概要を示す。

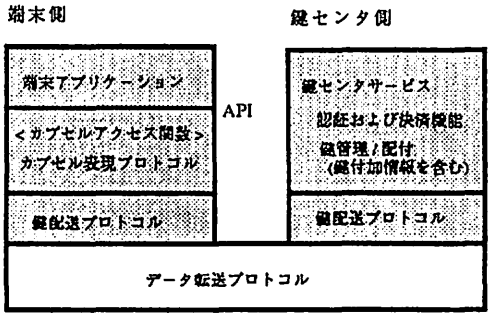

図 3: Infoket-I プロトコル概要

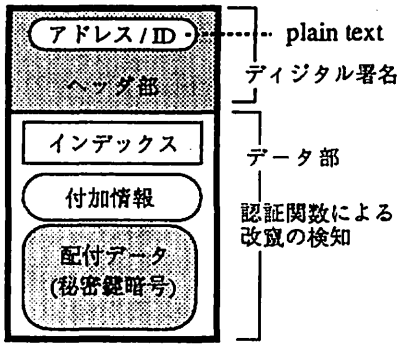

図 4: カプセルの構造

カプセルヘッダに組込まれる情報は以下の通りである。なお特に plain text と記していない部分はディジタル署名が行なわれる領域である。

- FleaMarket アドレス (plain text)
- ディジタル署名 ID (plain text)
- ヘッダ部認証子 ···FleaMarket アドレス、ディジタル署名 ID
- 復号化制御情報 ··· 情報 ID、鍵センタアドレス、有効期限
- 決済情報 ··· payback 用流通経路情報、決済方法一覧、定価
- データ部の正当性検査用データ
  - 認証子 (authenticator)
  - 認証子関数 IV(Initial Vector)

ヘッダ部の先頭の FleaMarket アドレス、ディジタル署名 ID は plain text であり、ディジタル署名されたヘッダ部の認証のための鍵を捜すインデックスとして用いる。ディジタル署名の暗号方式には、全てのメッセージに対して暗号と認証が可能であるように、RSA 暗号のような暗号化関数と復号化関数が全単射であるものを仮定する。

公開鍵暗号暗号方式 f_{pub} によるディジタル署名に用いる秘密鍵 K_{sec} と公開鍵 K_{pub} は FleaMarket ごとに何組か用意し、

$$K_{pub} = f_1(FleaMarket\text{アドレス}, \text{署名}ID)$$

は一意に求まるように (秘密鍵以外の) データを公開する。ヘッダ部は、K_{pub} と対になる秘密鍵 K_{sec} でディジタル署名する。ヘッダ部の復号は、上の関数と、ヘッダ部の先頭の値をパラメータとして適用して得る K_{pub} で行なう。

$$\text{署名文}(\text{ヘッダ部}) = f_{pub}(\text{ヘッダ情報}, K_{sec})$$
$$\text{ヘッダ情報} = f_{pub}(\text{署名文}, K_{pub})$$

この方式によりヘッダ部は読むことは可能であるが、ヘッダ部のデータを第 3 者が改竄すると意味のないデータとなる。これはヘッダ部認証子と plain text であるヘッダの先頭を比較すればよい。なお plain text の部分の改竄も同様に検知出来る。したがって、ヘッダ部に意味のあるメッセージを埋め込めるのは、復号鍵 K_{sec} を知っている FleaMarket のみとなる。

データ部は、データ部の構造化を定義するインデックス、カプセル付加情報、配布する情報本体を暗号化した配布データ部からなる。カプセル付加情報に入れる情報は、情報提供者が登録時等に設定した情報や、FleaMarket が設定する広告等からなり、暗号化は行なわず、情報料金回収の対象とならないデータである。

配布する情報本体の暗号化は秘密鍵暗号方式 $f_{sec}()$ を用いる。通常暗号鍵と復号鍵は等しく、K_i とすると、配布データ部 $= f_{sec}(\text{情報本体}, K_i)$ である。次にこの配布データ部に FleaMarket で一意に定まる情報識別子 ID_i を付与し、ID_i と K_i は 1 対 1 に対応付ける。この後 FleaMarket は、ID_i、K_i の対を鍵センタに送る。

3.2.2 データの改竄の検知と暗号化

データ部が改竄されていないことを検査するには、まず以下のような条件を満たす認証子生成関数 f_a が必要である。(認証子を計算する対象のデータを D とする。)

1. D の全ての bit に依存した値を生成
2. $f_a(D) = f_a(D')$ となる D' を見つけることが困難
3. 計算が高速に実行可能

データ部はヘッダ部に比べデータ量が多いことから、(3) の条件が必須である。そのためヘッダ部と異なり、計算量の多い公開鍵方式の暗号ではなく、秘密鍵方式の暗号を用いる。

本実現では、秘密鍵暗号方式の FEAL を段数 8 (=FEAL-8)、CBC(Cipher Block Chaining) モードで使用する。FEAL-8 は上の条件を満たす関数であり、FEAL-8 の初期値として IV を与え、データ部を 8byte のブロック単位で FEAL-8 の関数にフィードバックしながら計算し、最終ブロックの計算の出力結果を認証子関数の値とする。その値をヘッダ部に存在する認証子と比較し、等しければ改竄されていないとする。

データ部の暗号は、同様に計算量の観点から公開鍵暗号方式ではなく秘密鍵暗号方式を用いる。ただし既知平文攻撃等の可能性があるので、より暗号強度の高い段数 16 の FEAL-16 を CBC モードで用いる。なお認証子の計算はこの暗号化されたデータに対して行なわれる。

以下に Sun SparcStation2 上で例として RSA 暗号によるディジタル署名 / 検証、FEAL による認証子計算、データ部暗号化の時間測定結果を表 1に示す。

操作	設定	時間
ディジタル署名	作成 (64byte)	1.5[s]
	検証 (64byte)	0.12[s]
認証子計算	FEAL-8-CBC(100kbyte)	0.7 [s]
データ部復号	FEAL-16-CBC(100kbyte)	1.3 [s]

表 1: 暗号化関数時間測定結果

3.2.3 端末 API

カプセルアクセス手続きを実行し、アプリケーションインタフェースとなる関数として、以下がある。これはカプセルアクセス関数ライブラリとして提供される。いずれもカプセル化したファイルを引数にとり、内部表現を解釈し、アプリケーションにサービスを提供するカプセルアクセス関数である。

- `check_certificate(fname)`
- `get_payment_info(fname)`
- `decode_content(fname,user_info)`
- `get_optional_info(fname)`
- `demo(fname)`

またカプセルアクセス関数ではないが、前述の機能を実現するユーティリティ関数として以下がある。

- `get_pubkey(name, ID)`
- `set_user_info(user_info)`

`check_certificate()` は、`get_pubkey()` を用いて得た公開鍵によりディジタル署名を検証した後、ヘッダ部の認証子の値と認証子関数によりデータ部の非改竄を検証する。

`get_payment_info()` は、情報提供者の指定する決済方法のリストを取りだす。その中からユーザは決済方法を選択することが可能である。`set_user_info()` は、選択した決済情報やユーザ情報を `user_info` と呼ぶデータ構造体にセットする。`decode_content()` は `user_info` を引数に取り、カプセル中に存在する鍵センタアドレスに接続し、FleaMarket アドレスと情報 ID に対応する復号鍵を要求する。

`decode_content()` は戻り値として、復号処理結果と鍵付加情報へのポインタを返す。`get_optional_info()` は、カプセル中の付加情報エリアの中味を取り出す。`demo()` はこのカプセル付加情報エリアにデモ情報がセットされている時に、有効な関数である。

3.2.4 復号化の流れ

情報使用者はまず check_certificate() を呼び出し、そのカプセルが改竄されていないことを確かめ、同時にヘッダ情報を取り出す。購買時には、get_payment_info() を通じて決済可能な方法のリストを取りだし、決済方法を選択する。この後、会員情報等その他に必要な情報を set_user_info() を通じて user_info に設定し、復号化関数 decode_content() を実行する。鍵センタアドレス、情報 ID はヘッダ部にあるので、その鍵センタにアクセスし、情報 ID に対する復号鍵を要求する。

Infoket-C では会員制サービスとし、会員番号とパスワードをあらかじめ発行しておき、認証を行なった。その後クレジットカード決済の場合は、カード種別を選択後、カード番号、有効期限等を入力し、与信を行なった。Infoket-I では NetBank として実決済方法を抽象化して扱っているが、NetBank が会員による認証を要求する場合、鍵センタが対応する認証関数を実行する。この部分は、鍵センタと NetBank の契約となる。

復号処理実行後、復号化関数 decode_content() は終了する。

3.3 情報料の決済

復号鍵取得にともなって、その鍵に対応する料金が NetBank の FleaMarket の口座に振り込まれる。FleaMarket は鍵センタからの鍵取得情報に基づいて、情報提供者に情報料金を払い込む。情報提供者は料金を上限 / 下限の形で示してあり、実際の料金は FleaMarket が随時変更するため、明細書に実際の販売価格を明示する必要がある。その上で、FleaMarket の取り分 (=payback 率に基づいて計算) を差し引いた分を、情報提供者の口座に送金する。

4 鍵センタの機能

鍵センタは、復号鍵の管理と配布、NetBank で決済を行なうためのユーザ認証を含めた決済機能、NetBank の FleaMarket 口座に対する振り込み処理依頼といった基本サービスを行なう。また FleaMarket が情報料金を情報提供者に分配することが出来るように、情報 ID と料金の対を含む明細書を作成し、FleaMarket に渡す。

FleaMarket から鍵センタへは、随時データ登録や修正の依頼が届く。渡される情報は、新規登録、差し替え、ユーザデータの変更時で異なるが、データとしては以下の通りである。

- 情報 ID、復号鍵、販売価格
- 有効期限
- 鍵付加情報

修正時の販売価格や有効期限の変更は、鍵サーバ自身が FleaMarket に渡した復号鍵取得状況 (=マーケット情報) に基づき FleaMarket が決定したデータである。

本試作における鍵配送通信には、Infoket-C で用いられている公開鍵暗号と秘密鍵暗号を組み合わせた鍵配送プロトコル KDP(Key Delivery Protocol) の部分を流用し、Infoket-I プロトコル (図 3) として用いる。しかしながら、上位層におけるサービス実現部分は独立となるように設計し、将来的には SHTTP[4] 等の標準的な秘密通信プロトコルを下位レイヤとして組込み可能となるようにする ([3] 参照)。

5 マーケット情報の管理

FleaMarket は、その FleaMarket に展示している商品に関するアクセスログ、鍵センタから得た復号鍵取得ログといったマーケット情報を保持している。ただしカプセルを anonymous FTP サイト経由でユーザが情報を得た場合は、アクセスログは残らないので完全な情報ではない。またここで対象とする情報 ID は、その FleaMarket でカプセル化した情報に関してのみである。

- FleaMarket に展示した情報 ID ごとのアクセス総数
- 情報 ID 毎の購買総数

特に復号鍵取得に関しては、どの商品がどれだけ売れただけでなく、どのユーザがいつ復号鍵を

取得したかの時間情報も取得可能なので、例えば以下のような解析が可能である。しかしながらこれらの情報の取り扱いは、プライバシーの観点から、ユーザが誰であるか特定される情報は用いないように配慮する必要がある。

- 同一ユーザが、ある商品A、B、Cとも購入する傾向がある
- 商品Xを購入した後、商品Yを購入する傾向がある。

これらのマーケット情報は、以下の用途で使用されることを想定する。

- FleaMarketが商品を分類して展示販売する
- FleaMarketが売れ筋情報をピックアップし広告する
- セット販売によるディスカウント
- グルーピングされた復号鍵の鍵付加情報に、同じグループの商品の広告を入れる
- ユーザが関連商品を検索する
- 販売価格の変更
- 販売期間の変更

このFleaMarket方式による情報流通モデルで、これらのフィードバックによる操作が可能であるが、具体的なアルゴリズムや戦略は規定しない。むしろ本試作の試行サービス等のデータを集め、解析/適用していく過程で具体的戦略が定まってくると考えられるので、本稿ではマーケット情報の利用に関しては枠組みだけの紹介としておく。

6 おわりに

大規模な組織のみでなく、一般ユーザがネットワーク上において簡易に情報を登録して自由に配布し、最終的に情報の使用者から料金を回収するFleaMarket方式による情報流通システムを提案した。

現在本システムを試作中であるが、特にマーケット情報の利用に関しては、Infoket-C等の実システムのデータを集め解析し、適用することが必要と考えられる。またFleaMarketが提示するだけでなく、ユーザ側から逆にマーケット情報等を利用して検索するシステムや、複数の組織の運営するFleaMarketやanonymous FTPサイト全体を通して、情報を検索する方法が今後の課題である。

参考文献

[1] 池野信一, 小山謙二. 現代暗号理論. 電子情報通信学会, 1986.

[2] 金井敦, 三宅延久, 明石修, 生沼守英. マルチメディア情報流通システム(InfoKet). マルチメディア通信と分散処理研究会, May 1995.

[3] 森保健治, 明石修, 寺内敦, 三宅延久. 情報流通システムにおける鍵配送通信の構成法. マルチメディア通信と分散処理ワークショップ, Oct 1995.

[4] E. Rescorla and A. Schiffman. The Secure HyperText Transfer Protocol, 1995. INTERNET-DRAFT.

[5] 寺内敦, 森保健治, 明石修. 情報流通システムにおける課金方式. マルチメディア通信と分散処理ワークショップ, Oct 1995.

[6] William T. Wong. Secure NCSA Mosaic Reference Manual, 1995.