マルチメディア通信と分散処理 76－18
（1996. 5. 16）

FleaMarket 方式による情報流通システムの実装

明石 修　森保 健治　三宅 延久　寺内 敦
akashi@nuesun.ntt.jp {moriyasu, miyake, terauchi}@slab.ntt.jp
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 FleaMarket 方式による情報流通方式を提案してきた。

FleaMarket 方式による情報流通では、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なモデルである。本稿では FleaMarket 方式による情報流通モデルをシステムとして実装するにあたっての問題点と解決方法を、情報のカプセル化と流通、鍵配送システム、決済システムとの連動、の点から述べる。

Structure of the FleaMarket Information Distribution System

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

abstract

The information distribution with copyright control has become a major topic in the electronic commerce. We have proposed the FleaMarket information distribution model which allows commercial information registered by a information provider to be freely distributed on the Internet with copyright control. The content is protected against falsification and access without authorization by utilizing encryption techniques. We describe problems and solutions when we construct the FleaMarket system, especially with these points: 1) encapsulation and distribution of commercial information, 2) the key delivery system, 3) incorporation with payment systems.

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質がある [5]。インタネット環境でこの特質を活用し、なおかつ著作権を保護する方法として、我々は FleaMarket 方式による情報流通モデルを提案してきた [1, 2]。

FleaMarket 方式では、一般ユーザによって提供された商品情報を暗号化することにより、そのままでは情報にアクセスできないようにし、インタネット上で自由に配布する。この配布する単位を“カプセル”と呼び、著作権管理を行なうための機能を持たせる。カプセル化した情報は、アクセス権を得たユーザがインタネット上で復号鍵を取得することにより、取り出すことが可能である。インタネット上で自由に配布されることから、カプセルは以下の機能を持つことが必要である。

- 正規の FleaMarket で作成されたことが証明可能
- カプセルが第三者により改竄されていないことが証明可能

また復号のための鍵は、Key Delivery Protocol(KDP) と呼ぶ鍵配送プロトコルを用いて配送するが、第三者による盗聴を防ぐと共に、鍵配送システムでは以下の機能を実装する必要がある [7]。

- 端末側アプリケーションに直接鍵を見せない
- メッセージの記録 / 再生による攻撃への対処
- サーバの成りすましに対する対処
- メッセージ改竄の検知

決済に関しては、FleaMarket モデル上では情報流通システムと決済系が独立して扱えるように必要最低限の機能の定義であり、やや抽象化して扱っていたが、本システムでは CD-ROM 情報流通システム Infoket-C[5] で実装したクレジット決済システムと、電子プリペイドカード決済システム [10] とのインタフェースを実装した。

本稿では、FleaMarket 方式による情報流通モデルの概要に関して述べた後、モデルを実システムに適用するにあたっての問題点とその解決方法を、情報のカプセル化と流通、復号鍵配送システム、決済システムとの連動、に分けて述べる。

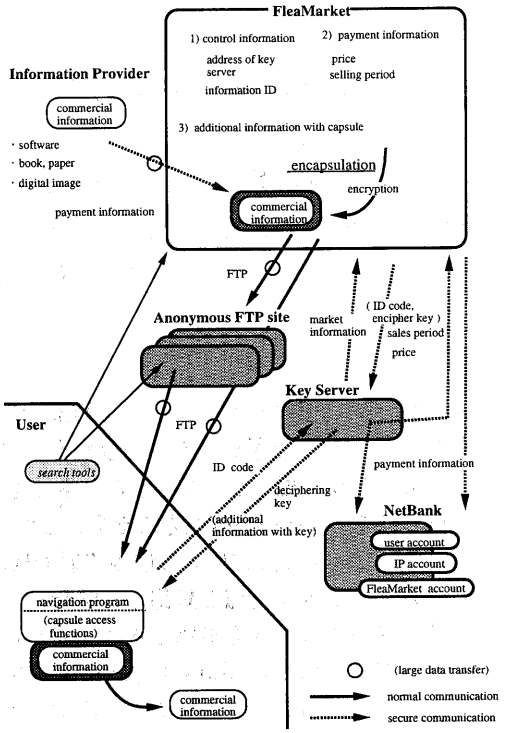

図 1: FleaMarket 方式概要

2 FleaMarket 情報流通モデルの概要

本章では、FleaMarket 方式による情報流通モデルの概要を説明する。(図 1)

FleaMarket は、情報提供者が商品情報の登録を行なう場所である。登録手続きは、情報提供者の認証、商品情報と付加情報のアップロード、決済方法等の販売情報の取り決めからなる。付加情報とは、カプセルに付加される README やデモ情報と、鍵配送時に送られる鍵付加情報からなり、改竄の検知以外は著作権管理を行なわない無料情報である。商品の価格変更、鍵付加情報は、後で変更可能である。カプセル化した商品情報の復号鍵や価格情報は、鍵サーバに送られる。

鍵サーバは情報復号鍵の管理を行なう。商品情報へのアクセス権付与手続きは、購買者の認証、復号鍵の KDP による配布からなる。鍵サーバは決済情報を定期的に NetBank と FleaMarket に送信する。

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。

3 FleaMarketシステムの実装

FleaMarketシステムの実装にあたって、機能を以下のように分け、個々にシステムの適用に当たっての問題点と解決方法を述べる。

1. 情報のカプセル化と流通
2. 鍵配送システム
3. 決済システムとの連係

以下、'⊕'は結合を表し、$\{A\}_{K_x}$はメッセージAをxの公開鍵K_xで暗号化したものを示す。$\{A\}_{K_{x,y}}$は、メッセージAをxとyで共有されている鍵$K_{x,y}$で暗号化したものを示す。なお前者は公開鍵暗号方式であり、後者は秘密鍵暗号方式を用いる。K_x^{-1}はK_xに対応する秘密鍵を示す。

3.1 情報のカプセル化と流通

商品情報には登録時に、FleaMarket内で一意性を保証する情報IDが付与され、FleaMarket IDと情報IDにより、システム全体で一意となるように管理する。この対をカプセルIDと呼ぶ。カプセルIDは、復号鍵と共に鍵サーバに送られる。一方カプセルIDはカプセルの内部情報として埋め込まれ、鍵要求時に鍵サーバに送られ、復号鍵を指定する。

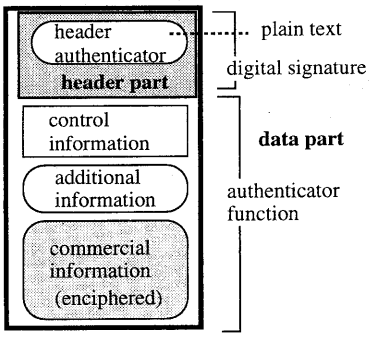

図2: カプセルの構造

なお登録時には、FleaMarketから情報登録証$\{$カプセルID、シリアル番号、情報提供者名$\}_{K_f^{-1}}$が情報提供者に発行される。情報提供者が鍵付加情報、販売価格、販売期間を後で変更する際には、この登録証を提示する必要がある。

カプセルは、情報の復号、カプセルの認証という基本機能を実現するための情報を持つカプセルヘッダ部と、その他のデータを含むデータ部からなる。データ部は、内容物である暗号化された商品情報や、デモや商品説明に関する暗号化されない付加的な情報、およびそれらの構造を定義するための制御情報と、定価、情報ID、商品のMIMEタイプ等の商品情報からなる。これらの情報を表すために用いられる整数型は、ネットワーク表現を用いることとする。(図2)

カプセルヘッダに組込まれる情報は以下の通りである。ヘッダ部はFleaMarketが公開鍵暗号[9]の秘密鍵K_f^{-1}(現在は64byte)を用いて、ディジタル署名を行なう。

- ヘッダ部認証子 $\cdots$ FleaMarket ID⊕ディジタル署名ID
- データ部認証子(MD5ダイジェスト)
- データ部の制御情報サイズ、タイプ

$$signature := \{header\_part\_data\}_{K_f^{-1}}$$
$$header := header\_autheticator \oplus signature$$

平文のヘッダ部認証子と、ディジタル署名中の認証子が等しいことにより、正規のFleaMarketで

作成されたカプセルであることが保証される。また制御部のデータは以下の通りである。

- 復号化制御情報 ···FleaMaket ID、情報 ID、鍵センタアドレス
- 商品情報 ··· 定価、有効期限、MIME タイプ、オフセット、サイズ、暗号化前のサイズ
- (付加情報オフセット、サイズ、MIME タイプ) のリスト

認証子関数は、改竄がされていない証明と共に、比較的対象とするデータ量が大きいため実行速度も問われる。初期の実装 [1] では、秘密鍵暗号方式の FEAL[6] を段数 8(=FEAL8)、CBC(Cipher Block Chaining) モードで使用したが、暗号強度的に十分であり、より高速に実行可能な MD5[8] を認証子関数として採用することにした。

3.2 鍵配送システム

FleaMarket モデルでは、FleaMarket、鍵サーバ、NetBank は信用できる組織により運営されていると仮定したので、このモジュール間の通信は主に第三者による盗聴対策を考えればよく、これは既存の Secure Socket Layer (SSL[3]) 等を流用可能である。しかしながら、鍵配送の場合は、ユーザは悪意を持って攻撃するかもかもしれない、と仮定してあるので、以下のような要求条件がある。

- アプリケーション層には直接復号鍵を見せない。端末側には鍵配送層の上に復号機能のみを提供する層を設け、そのインタフェースのみを AP に提供する。
- 以前に使用されたメッセージを記録し、再生したとしても、カプセルの中味は取り出せない。

またインターネットのような環境では、偽サーバによる成りすましという攻撃も考慮する必要がある。

3.2.1 プロトコル階層と端末 API

図 3は鍵配送プロトコル階層を示す。KDP は端末側、サーバ側双方で定義されるが、更に端末側ではカプセルの内部表現を解釈する層を規定する。

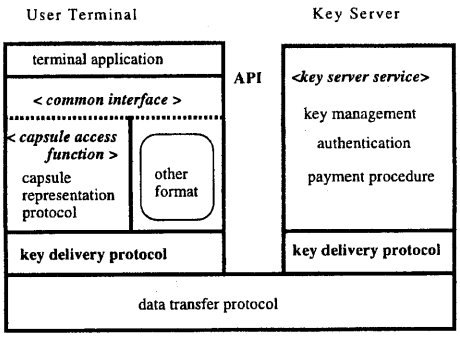

図 3: プロトコル階層

しかし直接アプリケーション層には鍵を見せないという制約から、特定のファイルを復号するという機能をアプリケーションに提供する層を規定する。

アプリケーション層に提供するインタフェースは、現在のところ、クレジットカードあるいは電子プリペイドカードで決済を行ない、暗号化情報を取得する関数と、ファイルの付加情報やデモ情報等の商品情報を取り出す関数が規定されている。このインタフェースはカプセル化ファイルだけでなく、Infoket-C 形式等の別形式のファイルでも共通とする。従って、内部には鍵取得を行なう機能と、特定のファイル形式に依存した処理を行なう機能が必要である。ここのモジュール間インタフェースは非公開とする。

すなわち公開するアプリケーションインタフェースに、ファイルの形式を引数として渡すことにより、対応したファイル形式に適した処理が呼ばれる方式とする。FleaMarket システムの場合には、鍵取得機能に加えて、以下のようなカプセルアクセス関数が存在する。

- `PurchaseCapsule()`··· カプセル形式のファイルから、商品情報を取り出す。引数は、カプセルファイルのファイルポインタ、決済方法、プリペイドカードまたはクレジット情報等。
- `GetCapsuleInfo()`··· カプセル形式のファイルから、特定の (暗号化されていない) 商品情報を取り出す。引数は、カプセルファイルのファイルポインタ、取り出す情報項目名等

3.2.2 鍵配送アルゴリズム

KDP は、鍵配送のために、6 つのメッセージで 1 つの鍵取得トランザクションを構成する。そのうち始め 4 つが鍵配送のコアの部分であり、残り 2 つが acknowledgment とトランザクションの終了処理のためのメッセージである。復号鍵を取得するトランザクションの特徴は以下の通りである。

1. 暗号化鍵をメッセージ毎に変える ⇐ 第三者による解読、録音再生攻撃に対する対策
   - 初期化には公開鍵暗号方式を用いるが、実行速度の点からその他は秘密鍵暗号方式 FEAL32 を用いる。
   - 暗号化鍵の生成に用いる乱数関数を複数用意し、それぞれ初期化の種を複数化する。
   - メッセージ生成に間する履歴を取り、乱数生成に対する不正な操作や、メッセージの繰り返し使用を検知する仕組みを付加する。
2. RPC のような 1 往復 (2 メッセージ) ではなく、4 メッセージ方式である。
   - RPC 方式ような 2 メッセージでは、悪意のあるユーザが 1 つめの鍵要求メッセージを録音し、そのまま鍵サーバに送ったとしても、鍵サーバではそのメッセージが元のユーザが送ったのかどうか、判断が不可能となるため。
3. メッセージのやりとりの中で、相手の送ったデータの一部を送り返すことにより、成りすましを検知する

これらの機能により、偽サーバによる成りすまし、記録 / 再生による攻撃に対処する。しかしながら、記録 / 再生に対する対処は、暗号アルゴリズム的には保証されてはいない。従って、履歴チェック、4 メッセージ方式により、システム的な防御を施し、直接的な解読を困難とする。

3.2.3 鍵配送メッセージ全体の改竄防止

KDP のメッセージはインタネットを経由して送られるため、鍵配送のアルゴリズム部分だけでなく、トランザクション制御の部分も含めて改竄を検知可能とする必要がある。

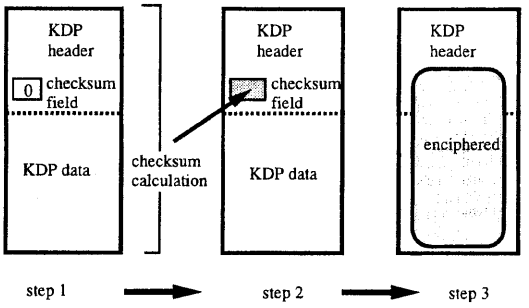

図 4: Checksum calculation

それぞれの KDP メッセージは、ヘッダ部とデータ部からなる。データ部には、前述した鍵配送のためのデータが入れられる。ヘッダ部は、6 メッセージからなるトランザクションを制御するための情報やチェックサムを持つ。チェックサム計算には MD5[8] を用いた。これは、ヘッダ部を含むメッセージ全体のチェックサムを計算し、メッセージの改竄を検知するためである。なおカプセルの表現と同様に、これらの情報を表すために用いられる整数型は、ネットワーク表現を用いることとする。(図 4)

MD5 ダイジェストは、暗号化前の KDP メッセージに対して計算されているため、KDP プロトコル中で用いられているメッセージ暗号鍵を知らない第 3 者が、チェックサム自体を再計算することは不可能である。従って、端末、鍵サーバ以外の第 3 者によるメッセージの改竄は検知可能である。

3.3 決済システムとの連動

FleaMarket モデル上は特別な決済系に依存しないように、口座とその振り込み機能がある NetBank を仮定した。一方 FleaMarket システムでは、現時点で Infoket-C システムと同様のクレジットカード決済システムと、電子プリペイドカードシステム [10] と連動させることとした。このため、鍵サーバの決済系に対するインタフェースは、特定の課金システムに依存しないような関数を設けて、課金データに関する解釈と処理はその関数内で定義することとした。

端末アプリケーションレベルでは、カプセルファイルの一覧を表示し、特定のファイルを選択し、個々の README やデモデータを取り出す。この

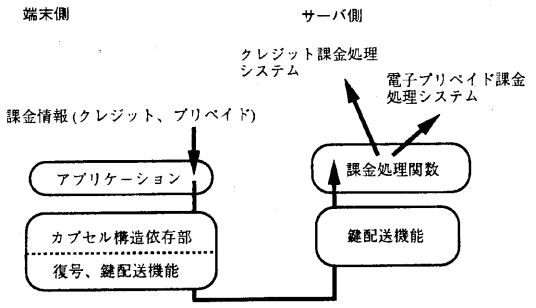

図 5: モジュール構造

場合は GetCapsuleInfo() を用いる。購入する場合には、決済方法を指定し、PurchaseCapsule() を用いる。この引数として、決済方法を渡すことにより、鍵配送プロトコル上の課金種別フィールドを設定する。会員認証に必要な会員 ID、パスワードは、クレジットカード購買でも電子プリペイドでも共通であり、アプリケーションレベルで設定する。その他、クレジット購買に必要なクレジットカード番号と有効期限、電子プリペイドカードであればプリペイドカードへのポインタは、それぞれ同様に端末アプリケーションで設定し、PurchaseCapsule() の引数として渡す。この中味は PurchaseCapsule() の中では解釈せずに、課金データとして鍵配送プロトコルに従って、鍵サーバにそのまま転送する。

鍵サーバでは、端末から送られてきた課金種別フィールドの値により、ユーザの決済情報 (クレジット情報または電子プリペイドカード) を識別する。しかしそのデータを鍵サーバは解釈せずに、課金処理関数を呼び出す。引数としては、課金種別モードに種類を設定し、鍵配送プロトコルで送られてきた課金情報をそのまま渡す。トランザクションの継続、アボートは課金処理関数の戻り値により決定する。(図 5)

このように、端末のアプリケーション以下の鍵配送モジュール、鍵サーバ共に特定のサービス、課金システムに依存しないように実装することが可能であり、更に FleaMarket 情報流通システムのみでなく、他の情報流通システムとの共存も可能である。

4 おわりに

インターネット環境に置いて、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著作権を保護した上で自由に配布し、最終的に利用者から料金を回収する FleaMarket 情報流通システムの実装に関して述べた。現在、鍵サーバおよび決済系は UNIX マシン上で作成し、端末プログラムは Windows95 上で動作する。このシステムは、鍵配送システム、FleaMarket 情報流通システム、決済システムとそれぞれ別モジュールとして実装され、他のサービスモデルとの結合も可能である。今後は、FleaMarket システムの適用によるフィードバックと機能拡張を行なう予定である。

参考文献

[1] 明石修, 森保健治, 寺内敦. FleaMarket 方式による情報流通. マルチメディア通信と分散処理ワークショップ, Oct 1995.

[2] Osamu Akashi, Kenji Moriyasu, and Atsushi Terauchi. Information Distribution by FleaMarket System. In *Proc. of the 3rd International Workshop on Services in Distributed and Networked Environments (to be appeared)*, June 1996.

[3] Kipp E.B. Hickman and T. Elgamal. The SSL Protocol, June 1995. Internet-Draft (IETF).

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

[5] 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.

[6] S. Miyaguti. The FEAL Cipher Family. In *Proc. of Crypto '90*, 1990.

[7] 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.

[8] R. Rivest. The MD5 Message-Digest Algorithm, Apr. 1992. RFC1321.

[9] R.L. Rivest, A. Shamir, and L. Adleman. A method of obtaining digital signature and public key cryptsystems. *CACM*, pp. 120–126, Feb. 1978.

[10] 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.