情報流通システムにおける鍵配送通信の構成法*

森保 健治† 明石 修† 寺内 敦† 三宅 延久†

NTT ソフトウェア研究所‡
moriyasu@slab.ntt.jp

概要

マルチメディア情報などのディジタル情報をネットワーク上の商品として扱うため，暗号化した商品を入手した利用者が商品を使用する際に，復号化と代金徴収を同時に行なうシステム(情報流通システム)を提案してきた．ここで必要な技術は，商品の復号鍵を利用者の攻撃から守ることである．

本報告では，情報流通システムを支える技術して，商品の復号鍵を安全に扱うための，利用者端末プログラムのアーキテクチャを提案する．具体的には，復号鍵をハンドルする階層を設け，アプリケーション層に復号鍵が露見しない構造とする．この階層に対する必要な機能，APIの十分性，想定する攻撃に対する防御について整理する．

1 はじめに

近年，WWWサーバの普及などにより，インターネットが各種の情報交換手段として注目され発達してきた．それとともにインターネットは，研究者など一部の人だけでなく，業種を問わず多くの人々からも利用可能となってきた．このことより，ネットワーク上での商取引実現のための土壌が育ってきたといえる．特にマルチメディア情報などのディジタル情報は，コピー，在庫管理，伝送が容易という特徴を持ち，ネットワーク上で扱うのに適した商品である．

一方，上記の特徴ゆえに，従来の有形物をベースとした流通コンセプト，つまり所有に対して代金を徴収する方式では，ディジタル情報の商取引には対応できないことも明らかである．例えば，利用規則上でコピーを禁じたところで，利用者の計算機上でコピー操作を不可能にすることは困難である．したがって，ディジタル情報の流通においては，所有に対して課金するのではなく，利用に対して課金する方式の方が，その特徴を生かしているといえる．

我々は，上記ディジタル情報の特徴を踏まえて，情報流通システム[1]を提案してきた．情報流通システムでは，商品となる情報は予め暗号化して安価あるいは無料で配布され，利用者がその商品を必要とした時点で始めて商品が有効となり(復号鍵を獲得し，復号化される)，同時に代金が徴収される[1]．つまり，商品の利用に対して課金するコンセプト上に構築されたシステムである．

ここで必要な技術は，商品を復号化する復号鍵を

*Key Delivery Architecture for Information Market System

†Kenji MORIYASU, Osamu AKASHI, Atsushi TERAUCHI and Nobuhisa MIYAKE

‡NTT Software Laboratories

[1]文献[1]においては，暗号化された商品の配布にCD-ROM，復号鍵の獲得に電話網/VTX網を利用し，電話網の場合はクレジットカードによる課金方式を取った適用例を挙げている

利用者の攻撃から守ることである．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．

本報告では，情報流通システムを支える技術して，商品の復号鍵(以下では，一般的な秘密通信のための暗号鍵と区別するため，AP鍵と呼ぶ)が利用者に渡らないようにするための，利用者端末プログラムのアーキテクチャを提案する．具体的には，AP鍵をハンドルする階層を新たに設け，アプリケーション層にAP鍵が露見しない構造とする．この階層に対する必要な機能，APIの十分性，想定する攻撃に対する防御について整理する．

2 情報流通システムと攻撃

2.1 情報流通システムの概要

情報流通システムでは，商品を提供するIP(Information Provider)，商品を展示する商店[2]，AP鍵の管理および課金情報を管理する鍵センタ，情報流通システム上の金銭全体を管理するNetBankおよび利用者が，そのインフラであるネットワークで結ばれている．ネットワーク上では，商品そのもの以外に，AP鍵などの商品情報，NetBank口座番号/クレジットカード番号などの課金に関わる情報などが流れる．各種情報が情報流通システム上を流れるイメージを図1に示す．

IPは，(1)商品を価格などの商品情報と共に商店に登録する．商店では，商品を暗号化すると共に，(2)その復号鍵(AP鍵)および商品情報を鍵センタに登録する．さらに，(3)利用者へ配布ルート[3]を通じて，暗号化した商品の配布を行なう．インターネットにおける配布には，WWWサーバやanonymous

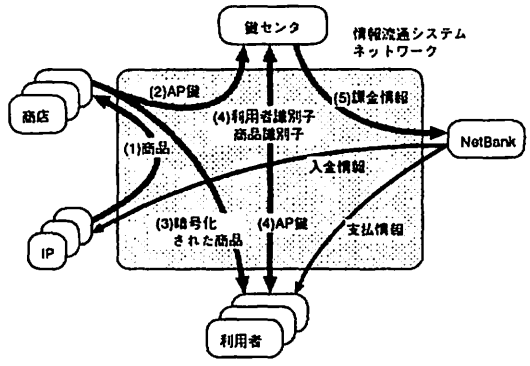

図1: 情報流通システムにおける情報の流れ

FTPサーバやなどの利用が考えられる．利用者は，商店から暗号化された商品を入手し，その商品が必要になった際に，(4)対応する復号鍵を鍵センタから獲得し復号化する．この時，(5)鍵センタは商品の価格に応じてNetBankにて料金を清算する．

2.2 情報流通システムへの攻撃

情報流通システムにおいて，商品，AP鍵，課金情報などの重要な情報は，第三者の攻撃から守る必要がある．攻撃対象および攻撃方法は，大きく分けて以下が考えられる．

暗号化された商品

(I) 暗号化してある商品を直接解析し，復号する攻撃

通信メッセージの内容

(II) 情報流通システムネットワーク上の通信メッセージを傍受/解析し，その中の情報を取得/改ざんする攻撃

端末

(III) 端末(利用者，IP，商店など)のプログラムあるいはメモリを解析し，その中の情報を取得/改ざんする攻撃

[2]文献[1]においてはCD-ROM企画/編集者，文献[2]においてはFreaMarketがこれに当る

[3]CD-ROM，パソコン通信などいろいろありうるが，ここでは特にインターネットに着目している．

成りすまし

(IV) 端末のプログラムを，必要な情報の取得/改ざんするように改造する攻撃

(V) 情報流通システムネットワーク上の通信メッセージを傍受/録音し，作成した擬似鍵センタあるいはNetBankを使って，他の端末/鍵センタとの通信を再現する攻撃

本報告では，特にAP鍵への攻撃に着目している．AP鍵を利用者に渡してしまうと，鍵センタへ接続の必要がなくなり，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，AP鍵を第三者に渡してしまうことにより，他の利用者も同様に無料で商品を利用するが可能となるからである．

上記の攻撃のうち，AP鍵に関係のある攻撃を以下に挙げる．

(II) より: 鍵センタと利用者端末間の通信メッセージを傍受/解析し，その中のAP鍵を探し出す攻撃 (攻撃1)

(III) より: 利用者端末のプログラムあるいはメモリを解析し，AP鍵を探しだす攻撃 (攻撃2)

(IV) より: AP鍵を取得するだけの利用者端末プログラムを作成して，鍵センタと接続することによってAP鍵を取得する攻撃 (攻撃3)

(V) より: 鍵センタと利用者端末間の通信メッセージを録音しておき，2回目以降は鍵センタと接続せずに，利用者端末と攻撃者が作成した擬似鍵センタ間でAP鍵のやりとりを再現し，課金を免れる攻撃 (攻撃4)

一般にSecure通信を支える技術として，通信メッセージそのものの暗号化技術，SSL[4]，SHTTP[5]あるいはInfoketプロトコル[1]といったSecureプロトコル，電子署名などが提案されている．これらの技術によって，(攻撃1) (攻撃4) といった攻撃を防御することができる．しかし，(攻撃2)(攻撃3) といった主に利用者が利用者端末プログラム (以下では，単に端末プログラムと呼ぶ) を攻撃し，AP鍵を取得する手法に対しては，従来の“通信メッセージの送信側と受信側は，正しい操作をしている”という仮定の上での技術では防御できない．これは，情報流通システム特有の攻撃であると言える．

これらの攻撃を完全に防御するには，タンパーフリーなハードウェア内に端末プログラムおよびAP鍵を内蔵し，利用者から遮断してしまうことが有効である．しかしながら，安価にシステムを普及させることを考えると，ソフトウェアのみでどこまで防御可能かを考えることは重要であり，本報告はこの観点から述べる．

3 AP鍵の保護法

3.1 情報流通システムにおける商品の販売形態

情報流通システムでは，以下の種類の販売形態が考えられる．

- Pay Per View(以下PPV)
  使用する毎に代金を支払うタイプの販売形態．ネットワーク上で扱うのに適している．以下のようなバリエーションがありうる．

  (PPV-1) 1回利用する毎に，商品の全機能が利用できる．その全機能は，端末プログラムを終了させるまで有効 (ex. 市販ソフトウェアなど)．

  (PPV-2) 商品の機能が複数に分割されていて，各機能毎に利用代金が必要となる．一度，他の機能を使うと，元の機能を利用する際には，再度課金される (ex. 辞書や電話帳の検索サービスなど)．

  (PPV-3) 商品の機能が複数に分割されていて，各機能毎に利用代金が必要となる．各機能

は一度代金を支払うと，端末プログラムを終了させるまで有効(ex. ページ毎に課金されるハイパーカード的な情報サービスなど).

- Pay Per Copy(以下PPC)
  最初に使用する際に，全代金を支払うタイプの販売形態．2回目以降は無料で利用できる(ex. 市販ソフトウェアなど).

- カタログ販売
  商品がディジタル情報ではなく，代金の支払いのみをネットワーク上で行なうタイプの販売形態.

AP鍵の保護という観点から見ると，これらのうちカタログ販売は必ずしもAP鍵を必要とせず，むしろ会員情報，課金情報といった情報の保護の方が重要であるためここでは言及しない.

さらに，PPVとPPCでは，以下の違いがある

- AP鍵の保護の違い
  PPCでは，最初に商品を復号化するため，AP鍵が必要な期間(つまりAP鍵を保護すべき期間)は短いが，PPVの場合は(PPV-3)のように，複数のAP鍵をある程度の期間，端末プログラム中にて保存する必要がある.

- 著作権保護の違い
  PPCでは，売り切りであるため(HDなどにインストールされる)，他への転用などに対する著作権保護についてはシステムの範囲を越えるが，PPVはその場限りの使用権を売る販売形態であるため，HDなどに蓄積することは，コピーなどの攻撃にあうおそれがある．他への転用を防止するためにも，PPVで販売される商品は蓄積なしに表示される必要がある.

2つ目の違いは，AP鍵の保護というより，ブラウザあるいドライバの機能の問題なので，ここでは触れないが，PPVを実現する上で重要な機能である.

以上より，PPC, PPVを実現するためのAP鍵保護機能に対して，以下の機能が要求される.

(PPV機能1) AP鍵の複数保存機能

(PPV機能2) AP鍵の継続保存機能

3.2 AP鍵配送層

一般に，通信システムでは，OSIの参照モデルに代表されるように，複数の階層から構成される．(攻撃3)のように利用者が擬似端末プログラムを構成してAP鍵を獲得しないようにするには，まずAP鍵が最上位のアプリケーション層に露見しないような構成とする必要がある．その為には，AP鍵を専用に扱う階層(AP鍵配送層)をアプリケーション層の下に設ける．AP鍵配送層に対する要求条件を以下に整理する.

まず，(攻撃2)(攻撃3)より，大前提として以下の要求条件がある.

(要求条件1) AP鍵がアプリケーション層に露見しない

(要求条件2) 解析によりAP鍵が露見しない

つぎに，(PPV機能1)(PPV機能2)より，以下も必要である.

(要求条件3) 複数のAP鍵を同時に保存，並行して操作できるAPIをアプリケーション層に提供できる.

(要求条件4) AP鍵の保存時間を制御できるAPIをアプリケーション層に提供できる

4 実現に向けて

情報流通システム特有の攻撃以外の攻撃に対しては一般の暗号化技術が利用できる.

例えば，電話網/VTX網上のSecureプロトコルであるInfoketプロトコルは，通信メッセージの秘密保持，端末/鍵センタの双方の成りすまし防止を保証しているため，(攻撃1)(攻撃4)を防御することができる[1].

また，インターネット上のSecureプロトコルの1つであるSSLは，インターネットでは標準的な通信プロトコルであるTCP/IP上にSSL(Secure Sockets Layer)と呼ばれる階層を置き，その上のアプリケーションに対して，通信メッセージの内容の秘密保持，偽称/改ざん防止，Reliableな通信が保証された通信チャネルを提供している[4]. したがって，(攻撃1)(攻撃4)に対する防御が可能である.

Secureプロトコルによって，通信路上の通信メッセージの内容の安全は保証されているため，AP鍵配送層はSecureプロトコル上に構築するのが効率的である. 本報告は，インフラとしてインターネットに着目しているため，Secureプロトコルとして SSLを使った場合の端末プログラムのアーキテクチャを図2に示す.

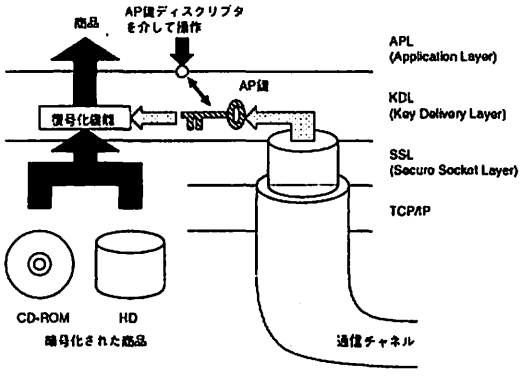

図 2: AP鍵配送層を持つ端末プログラムアーキテクチャ

図2に示すように，AP鍵配送層(KDL)は，SSL上に設ける. AP鍵配送層は，AP鍵の獲得/保護機能と商品の復号化機能を持つ.

AP鍵配送層への(要求条件1)については，AP鍵と1対1を成すディスクリプタ(以下では，AP鍵ディスクリプタと呼ぶ)を用意し，AP鍵への操作はこのディスクリプタを通して行なうことによって，AP鍵をアプリケーション層に露出せずにアプリケーションを作成することができる. ディクリプタを同時に複数持ち，それらを別々に使った操作ができれば，(要求条件3)も満たすことができる. また，AP鍵の破棄を行うまで，そのディスクリプタを有効とすれば，(要求条件4)を実現することもできる. ただし，アプリケーション終了時には，自動的にAP鍵を破棄する必要がある.

以上より，AP鍵配送層のAP鍵に関するAPIは，大きく分けて以下の関数を用意することで，(要求条件2)以外の各条件が満たされると思われる.

(API1) AP鍵ディスクリプタの獲得

(API2) 指定したAP鍵の破棄

(API3) AP鍵ディスクリプタを指定して商品の復号化

(API4) エラー処理，初期化，後処理

利用者が商品を利用する際は，基本的にアプリケーションが以下の手順を実行すれば，商品を購入することができる.

(手順1) 購入に必要な情報を入力させる.

(手順2) 鍵センタと通信をしてAP鍵を受信し，対応するAP鍵ディスクリプタを獲得する.

(手順3) AP鍵ディスクリプタを指定して，商品を復号化する.

(手順4) AP鍵ディスクリプタを指定して，AP鍵を破棄する.

(要求条件2)に関しては，一般論ではソフトウェアのみで完全に防御することは困難である. したがって，厳密には悪意の利用者の解析を困難にすること

程度しかできない．一般的な方針としては，以下が考えられる(プラットフォームに依存するような具体的な方法については，ここでは触れない)．

- 端末プログラム実行時
  なるべくオンメモリ上で実行できるように，実行オブジェクトの大きさに注意する．
  また，端末プログラムを認証する機能(ex. サイズ，チェックサムなどの確認)を組込む．
- 端末プログラム配布時
  AP鍵配送層をライブラリ化し，バイナリで配布する．
- 端末プログラムの構成
  AP鍵の格納場所を解析するためには，端末プログラムを解析する必要があるが，解析の糸口になる部分(ex. 乱数ライブラリ)は，汎用ライブラリを使用せずに自作する．
- 端末プログラム内のAP鍵の格納
  AP鍵の格納場所を分りにくくする(ex. 分割して格納，鍵センタから分割して受信)．

5 評価

提案するアーキテクチャを，(1)攻撃に対する防御，(2)APIの十分性の点から評価する．

5.1 攻撃に対する防御

2.2節に挙げた各攻撃に対する防御レベルについて述べる．まず，(攻撃1)(攻撃4)といった攻撃に対しては，Secureプロトコル(ここではSSL)が持つ，通信メッセージの内容の秘密保持，偽称/改ざん防止，Reliableな通信の保証，といった特性により防御可能と考える．

(攻撃2)(攻撃3)は，端末プログラムを解析/改造をする攻撃である．これらは，前章で述べたように，ソフトウェアのみで完全に実現することは困難である．ただし，提案するアーキテクチャでは，アプリケーション層にAP鍵が出ないため，攻撃からの防御の強度は，AP鍵配送層以下のプログラミング手法の強度と等しくなる．

このことは，情報流通システムを構成するために必要なプログラム(例えば，通信ライブラリや復号化ライブラリなど)を，IP/商店に配布した場合でも，悪意のあるIPあるいは商店が，AP鍵のみを獲得するアプリケーションを作成しにくくすることに有効である点で重要である．

5.2 APIの十分性

文献[1]で示した情報流通システムの試作において，端末プログラムで必要なAPIは大きく分けて以下の通りであった．

(API'1) AP鍵ディスクリプタの獲得

(API'2) 指定したAP鍵の破棄

(API'3) AP鍵ディスクリプタを指定して商品の復号化

(API'4) 商品識別情報の入出力

(API'5) 利用者識別用情報(ex. 会員情報，パスワード)の入出力

(API'6) クレジット課金情報情報の入出力

(API'7) エラー処理，初期化，後処理

上記APIを利用して，PPC, PPV，カタログ販売について適用実験をした所，API的に不足は特に見当たらなかった．

試作システムにおけるAPIは，4章で述べたAPIに比べて，商品を購入するのに必要な情報の入出力のAPI(API'4)(API'5)，および課金方式に依存したAPI(API'6)が増えている．これらは，AP鍵の保護には直接関係ないため，AP鍵保護層としてのAPIは，4章に挙げられたAPIで十分であるといえる．

ただし，インターネットにおける商取引においても，(API'4)～(API'6)のようなAPIは当然必要である．ただし，図1で示した情報流通システムのように，ネットワーク上のNetBankによる清算方式[3]を取れば，(API'6)のようにクレジット課金用のAPIではなく，NetBank口座番号などを指定するためのAPIとなろう．

また，(API'4)～(API'6)は，利用者が悪意を持って攻撃するという性質のものではないため[4]，第三者からの攻撃を防御するため，Secureプロトコルをそのまま利用することになる．

6 おわりに

本報告は，情報流通システムを支える技術として，商品の復号鍵を安全に扱うための，端末プログラムのアーキテクチャを提案した．特に，端末プログラムにおいて，復号鍵が利用者に渡らないようにするため，復号鍵を扱う階層をアプリケーション層とSecure通信プロトコル層の間に置く構成としている．

本アーキテクチャは，通信路あるいは商品そのものに対する攻撃には十分防御力がある．ただし，端末プログラムを解析/改造をする攻撃に対しては，ソフトウェアのみで完全に対処することは困難である．しかしながら，情報流通システムの普及を考えると，通信ライブラリや復号化ライブラリは標準的なものを用意/配布することが必須であり，本アーキテクチャは端末プログラムの効率的な開発，正しいアプリケーションの構築のためにも必要である．

また，仮に専用ハードウェアを利用した場合でも，アプリケーションはハードウェア上に必ずしも置くことができず，AP鍵の露見を防ぐための本アーキテクチャによる階層構造が有効になると思われる．

参考文献

[1] 金井他，"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] 明石他，"FleaMarket方式による情報流通"，本ワークショップ予稿

[3] 寺内他，"情報流通システムにおける課金方式"，本ワークショップ予稿

[4] "THE SSL PROTOCOL", Internet Draft, http://home.netscape.com/newsref/std/SSL.html

[5] "The Secure HyperText Transfer Protocol", Internet Draft, http://www.commerce.net/information/standards/drafts/shttp.txt

[4] 攻撃すると，自分自身が被害を被るため