情報販売システムの構成に関する研究*

4J－9

竹内 格　森保 健治　平川 豊 †
NTT ソフトウェア研究所‡

1　はじめに

我々はインターネット上で情報流通を行なうためのセキュアなモデルとしてInfoketを提案してきた[1]。Infoketアーキテクチャでは、予め利用者端末に配布された暗号化されたディジタル情報(暗号化商品)を復号化する鍵(情報鍵)を鍵センタから送る際に課金処理を行なう。これにより商品の著作権を守りつつ、ネットワーク上での情報販売が可能となる(図1)。本研究ではInfoketアーキテクチャを用いた情報販売システムの構成について検討する。

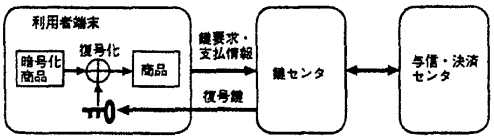

図1: Infoket アーキテクチャ

2　システム構成

オンラインショッピング等の情報販売におけるサーバシステムの構成要素としては以下がある(なお、本稿では商品とは市販ソフトウェアやマルチメディアコンテンツを指す)。

モール:	利用者に商品情報や暗号化商品を提供。
会員情報:	会員番号やパスワード等の会員利用者の情報を管理。ここではIPも会員とする。
商品情報:	商品名、商品コード、単価等の商品情報を管理。
決済系:	購入時の決済処理。
鍵管理:	商品の暗号化作業、暗号化商品の復号鍵の管理、購入時の鍵配送。

またここでは、条件としてモール管理、会員情報管理、商品情報管理は常にモール管理者が行なうものとする。考えられる構成は以下の通りである：

1. 集中型: モール管理、会員情報管理、商品情報管理、鍵管理、決済系を一括してモール管理者が行なう。

2. 鍵管理・決済系分離型: 鍵管理・決済系をモール管理者とは別の組織が管理を行なう。

3. 鍵管理分離型: モール管理者はモール管理、会員情報管理、商品情報管理、決済系の管理を行なう。鍵管理は別組織が行なう。

4. 決済系分離型: モール管理者はモール管理、会員情報管理、商品情報管理、鍵管理を行なう。決済系は別組織が管理を行なう。

本稿ではそれぞれの場合において、情報販売における主要なサービスフローにおいて必要となる機能について述べるが、ここでは特に1.と2.の構成について述べる。

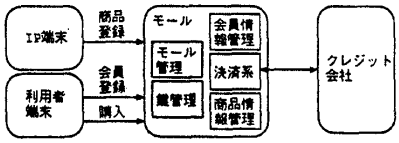

図2: 集中型

3　必要な機能について

3.1　集中型

図2に集中型の構成を示す。サービスを行なうサーバシステムを単にモールと呼ぶことにする。以下では主要なサービスフローとして会員登録、商品登録、購入のそれぞれにおいてモールが行なうべき動作と必要な機能を述べる。なお、以下で述べる、鍵配送以外の動作や機能は特に手動/自動の区別は与えていない。

- 会員登録
  1. 利用者→モール
     利用者の名前・住所・電話番号等をモールに送る。
  2. モール:
     会員番号と会員パスワードを割り当て、会員情報データベースに登録する。
  3. ユーザ←モール
     会員番号とパスワードを送る。

- 商品登録
  1. IP→モール
     IPはモールに、IPの登録番号・パスワードと、登録したい商品、商品名、単価、取り扱っているクレジット会社等の情報をセンタに送る。
  2. モール:
     IPの認証確認後、商品の暗号化作業を行ない、復号鍵を生成する。暗号化商品をモールに登録し、商品名や単価などの情報を商品情報データベースに登録する。

- 購入

*A Study of Constructing Information Distributing System
†Kaku TAKEUCHI, Kenji MORIYASU, Yutaka HIRAKAWA
‡NTT Software Laboratories

1. 利用者→モール
   利用者端末は会員番号、会員パスワード、商品番号、個数、クレジット番号等を送る。
2. モール:
   モールは会員認証、商品番号チェック、クレジット与信を行なう。
3. 利用者←モール
   暗号化商品の復号鍵を送る。利用者端末では暗号化商品の復号作業が行なわれる。

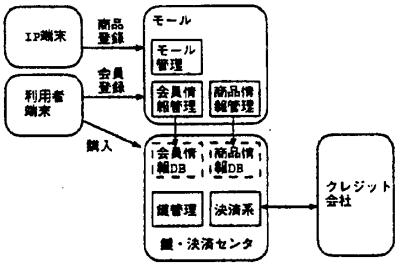

図 3: 鍵管理・決済系分離型

3.2 鍵管理・決済系分離型

鍵管理・決済系を処理するシステムを鍵・決済センタと呼ぶ。復号鍵配送時に利用者の認証作業を行なうため、鍵・決済センタにおいても会員番号やパスワード等の会員情報のデータベースが必要となる。また、購入時に利用者が指定してきた商品コードや販売価格をチェックするために商品情報のデータベースも必要となる。モールから鍵・決済センタにアクセスする際の認証の機構も必要である。

- 会員登録

  モールが会員登録を受け付けた際に、モールから鍵・決済センタへの新規会員の登録作業を行なう。この接続時に、鍵・決済センタはモールの認証確認を行なう。

- 商品登録

  モールが IP からの商品登録を受け付けた際に、モールから鍵・決済センタへ商品を送り、暗号化作業を依頼する。鍵・決済センタ側では、モールの認証確認の上で暗号化作業を行ない、暗号化商品はモールに送り、復号鍵を登録し商品情報データベースを更新する。モール側では鍵・決済センタからの暗号化商品をモールに登録し、商品情報データベースを更新する。

- 購入

  フロー自体は基本構成の場合とまったく同様だが、利用者はモールにではなく、鍵・決済センタに対して購入要求を出し、利用者側は鍵・決済センタから復号鍵を取得し、復号化作業を行なう。

この他、売り上げ情報等を鍵・決済センタからモールに送る機構が必要である。

3.3 その他の構成

鍵管理分離型: 鍵管理を行なうシステムを鍵センタと呼ぶことにする。鍵・決済系分離型の場合と同様に、鍵センタには会員情報や商品情報のデータベース、モールの認証機構が必要となる。購入処理はモール側で行なう場合と鍵センタ側で行なう場合が考えられる。

決済系分離型: 決済系を管理するシステムを決済センタと呼ぶことにする。決済センタに接続してくるモールの認証機構が必要である。

また、上のどちらにも鍵センタ (決済センタ) からモールへ課金情報や売り上げ情報を送る機構が必要である。

4 検討

鍵管理・決済系分離型、鍵管理分離型、決済系分離型のそれぞれの構成では、集中型よりも機能や運営方法が複雑となる。

- 鍵管理・決済系分離型

  会員登録をオンラインで行ない、利用者がすぐにサービスを使えるようにするには、モールからセンタへの会員登録処理をリアルタイムに行なう機構が必要である。またニュースなどのような即時性の必要とされる情報を販売するような場合にも、センタの商品登録データベースをリアルタイムに更新する機構が必要となる。他方、この構成ではセンタを複数のモールから共有して使えるようにすることが可能だが、会員情報・商品情報データベースのマージ方法を意識する必要がある。

- 鍵管理分離型

  この構成ではモール - 鍵センタ間での通信のやりとり多いため、特に購入時の即時性が低くなる恐れがある。これに対し、購入処理をモールで行なう場合に、復号鍵をモール側でキャッシュすることが可能だが、モールでの鍵管理が必要となる。

- 決済系分離型

  決済センタにクレジットの与信依頼がかかる際にクレジット会社と通信を行なうため、購入時の即時性が低くなる恐れがあり、またモール - 決済センタ間でセキュアな通信の機構を用意する必要がある。現実的にはモール - 決済センタ間は高速な専用線が使われると考えられる。

5 おわりに

Infoket を用いた情報販売システムの構成についていくつか検討を行なった。今後の方針として特に集中型および鍵管理・決済系分離型の構成において必要となる機能のさらなる比較・検討とコスト的な調査を行なっていく予定である。

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)