3J－3

World Wide Web による情報販売方式[1]

清水 亮博　三宅 延久　鈴木 英明　平川 豊[2]

{akihiro, miyake, suzuki, hirakawa}@slab.ntt.jp

NTT ソフトウェア研究所[3]

1 はじめに

現在 Internet 上では World Wide Web(以下 WWW) による情報提供が盛んに行われるようになっているが、そのほとんどが無料の情報提供である。今後新聞社等のコンテンツ販売業者による情報販売を発展させるためには、WWW によって提供された情報の対価を徴収するシステムが必要である。本研究では、これまで筆者らのグループが手がけてきた Infoket モデルを WWW に適用することで、この問題を解決する。

2 要求条件

WWW による情報販売システムが満たすべき条件は、以下の通りである。

2.1 セキュリティの確保

本システムに対するセキュリティ上の脅威としては、商品の盗聴、改竄や購入者、情報提供者、購入処理サーバのなりすましがある。

2.2 商品と代金の確実な交換

商品と課金情報の交換が保証されていないと、サーバが商品を送信したにも関わらず課金されない事故や、課金されたにもかかわらずクライアントが商品を受け取れない事故が起りうる。

2.3 多様な課金方式の実現

例えば新聞や雑誌等の WWW による販売を想定すると、一部毎の販売の他に定期講読による割引や、記事毎の課金などが考えられる。また書籍の出版では、一部を無料で提供し、それ以外は課金する手法などが考えられる。

これらの様々な課金を、以下の 2 つの課金方式を組み合わせることで実現する。

従量課金 利用できる情報の量に対し、対価を支払う課金方法。

期間課金 情報を利用できる期間に対し、対価を支払う課金方法。

3 情報配送のアプローチ

情報配送方式に着目して、解決策を考える。

第一に購入処理時に購入した商品をすべて渡す手法が考えられるが、これは期間課金という概念を実現し得ない。

次にサーバでのアクセス制御によって各ユーザの購入した商品を管理する方法が考えられるが、これはユーザや商品の数が増えたときに、アクセス制御情報が増大するという問題がある。

最後に Infoket モデルを WWW に適用する手法が考えられる。Infoket モデルは、販売する情報を対称鍵暗号で暗号化した上で配布し、暗号鍵を販売することで情報販売を実現する (図 1)。このモデルに基づいた情報販売システムとしては、CD-ROM によって暗号化した情報を配布し、鍵を電話網を用いて販売する Infoket-C[4][5, 3, 1] と、暗号化した情報、鍵の配布を Internet 上で行う FleaMarket 方式 [4] がある。次節ではこの Infoket モデルを WWW に適用する手法を示し、要求条件を満たすことを示す。

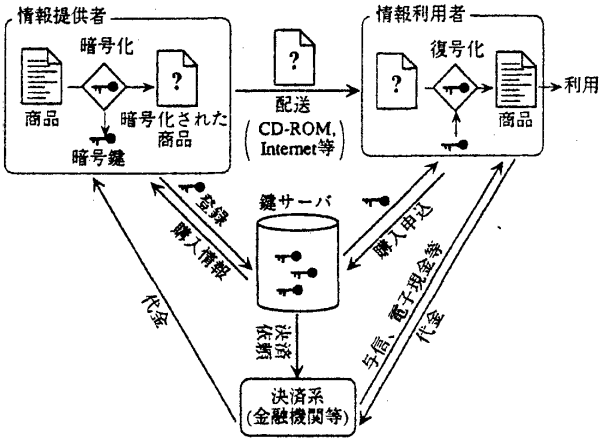

図 1: Infoket モデル

[1] An information selling method with World Wide Web

[2] Akihiro Shimizu, Nobuhisa Miyake, Hideaki Suzuki, Yutaka Hirakawa

[3] NTT Software Laboratories

[4] サービス名: miTaKaTTa

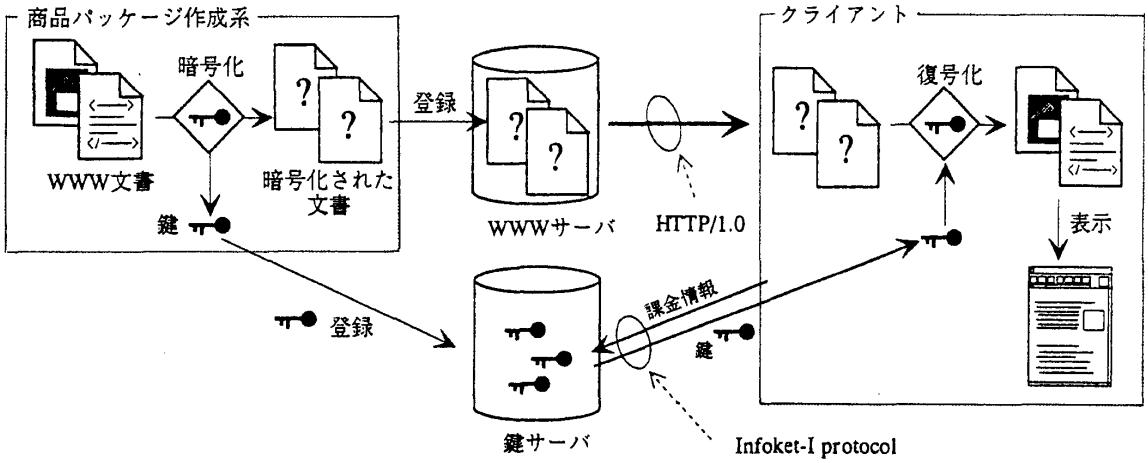

図 2: Infoket モデルによる情報販売システム

4 Infoket モデルの WWW への適用

4.1 システムの概略

図 2に、Infoket モデルを適用した WWW による情報販売システムの概略[5]を示す。

商品パッケージ作成系は WWW 文書の暗号化、WWW サーバへの登録、および暗号鍵の管理、鍵サーバへの登録を行う。

クライアントは暗号化された文書を通常の WWW と同様に HTTP/1.0 で受信[6]し、鍵サーバから購入した鍵を用いて復号化、表示する。このクライアントは、WWW クライアントに課金処理と復号化を行うモジュールを追加することで実現する。

4.2 要求条件による本方式の検証

以下では、2節で述べた要求条件を本方式が満たすことを示す。

セキュリティの確保 商品は暗号化されているので盗聴不可能である。商品の改竄、購入者、情報提供者、購入処理を行う鍵サーバのなりすましは電子署名によって防止する。

商品と代金の確実な交換 鍵と課金情報は FleaMarket 方式でも用いられている Infoket-I プロトコル [2] によって atomic に交換される。その後商品自体のダウンロードに失敗しても、再度ダウンロードを行えばすでに入手済の鍵によって復号化して利用できる。

多様な課金方式の実現 従量課金は、商品毎に暗号鍵を変えることで実現する。期間課金は期間毎に鍵を変える手法と、鍵に有効期限を記入しておき expire する手法で実現する。

4.3 本方式の課題

現在の課題は、保存した暗号鍵のコピー防止手法、WWW クライアントの拡張手法、商品パッケージ作成系の構成などがある。

5 今後の予定

今後は特定のクライアントに対する依存性、パフォーマンス等の点を考慮して設計を決定し、実装、実験運用を通してシステム全体を評価する。

[5]決済系については省略している。

[6]このため WWW サーバは無改造で使用可能で、proxy サーバのキャッシュ機能も利用可能である。

参考文献

[1] 三宅延久, 明石修, 奥山浩伸, 寺内敦, 森保健治. CD-ROM 情報流通サービス実現方式. *NTT R&D*, Vol. 44, No. 10, pp. 19–24, 10 1995.

[2] 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, October 1995.

[3] 生沼守英, 堀田博文, 金井敦, 大道泰信. CD-ROM 情報流通サービスの構成と評価. *NTT R&D*, Vol. 44, No. 10, pp. 11–18, 10 1995.

[4] 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, October 1995.

[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.