2H-05　情報中継サービス業者によるプライバシーの保護方式の提案

梶原 清彦†，鷲見 卓哉‡
NTT 東日本 研究開発センタ†
NTT 西日本 研究開発センタ‡

1.はじめに

音楽配信などの各種のコンテンツがインターネットを介して販売されるようになってきている。これにより、顧客は早く簡単にコンテンツが購入できるが、販売元に自分の身元（氏名、年齢、住所などの個人情報）が知られてしまうことになる。すなわち、店頭販売で守られていた個人情報がネットワーク販売では破られてしまうことを意味する。

本稿では仲介業者が販売元と購入者の間に入ることで、購入者のプライバシーを保護する方式を提案する。

2.目標と課題

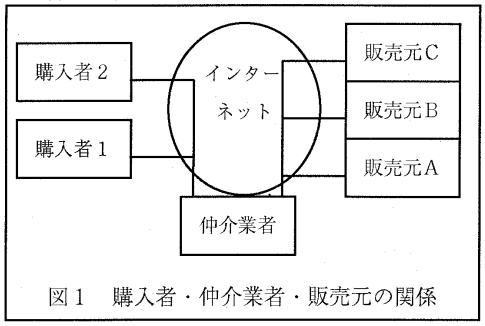

図１　購入者・仲介業者・販売元の関係

本稿では図１に示すネットワークにおいて、以下の状況を想定する。

・購入者はインターネットを利用して仲介業者にアクセスし、電子メディア商品の申込み、商品受取、代金支払いを行う。
. 仲介業者は販売元に対して、代金を購入者に代わり販売元に支払う。

前記の想定において、以下の目標を達成できれば、実用的なプライバシー保護（購入者の個人情報を数社の信頼がおける企業に限定すること）が可能となる。

(1) 購入者の個人情報を販売元から保護すること
(2) 購入者からの購入に関する問合せに対応するための情報が残ること

このために、以下の３つの課題を解決できる方式を考案しなければならない。

(a) 個人情報の保護
購入者の個人情報は仲介業者のみが知り、販売元にはしられないようにする方法の確立。
(b) 購入情報の保護
仲介業者に購入者が何を購入したかを知られずに購入できる方法の確立。
(c) 購入確認
購入者，仲介業者，販売元の間で購入に関する情報を確認できる方法の確立。

3. 解決方法

提案する方式は、購入決定と支払いは購入者と仲介業者の間で行い、商品購入は購入者と販売元で行うという購入プロセスの分割により、個人情報と購入情報を分離することでプライバシーを守る。

購入決定と商品購入を単純に分割してしまうと、購入確認のための情報を突合せることができなくなるため、以下のようにして突合せ可能にする。

・仲介業者が発行する利用者 ID と販売元が発行する販売 ID を、毎回新しい番号になるように生成する（これは WWW サーバへの匿名アクセスで一般的に用いられている方法[1]と同様である）。仲介業者は利用者 ID で支払いを識別し、販売元は販売 ID で商品購入を識別できるようにする。

A proposal of how to protect privacy from resellers with a mediator

†Kiyohiko Kajihara，‡Takuya Sumi
†NTT East Corp. Reserch and Development Center
‡NTT West Corp. Reserch and Development Center

・仲介業者は利用者ではなく、利用者 ID を販売元に提供することで個人情報を保護する。販売元は商品購入の際に得られる利用者 ID、販売 ID、商品を対応付けることで購入情報を管理できる。

3.1 プライバシー保護方式

購入者の個人情報を販売元に伝えず、仲介業者には購入情報がわからないようにできる方法を図 2 に示す。具体的な動作にともなう利用者 ID・販売 ID の授受は以下の通りである。

(1) 利用者 ID を埋め込んだ、商品を参照する HTML ファイルを作成する。

(2) 購入商品の選択により、販売元の WWW サーバにアクセスする。その際、利用者 ID が渡される。

(3) 商品を FTP 等により購入者に渡す。さらに、販売 ID を埋め込んだ商品受取確認のための HTML ファイルを作成し、購入者に確認してもらう。

(4) 受領確認を行うと、仲介業者に購入 ID が渡される。

(5) 販売元は利用者 ID と販売 ID と請求額を仲介業者に通知する。

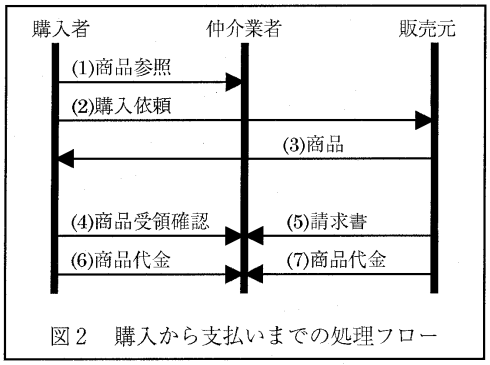

図 2　購入から支払いまでの処理フロー

(6) 購入者は販売 ID と商品代金を仲介業者に支払う。

(7) 仲介業者は利用者 ID と販売 ID と商品代金を販売元に支払う。

3.2 目標達成の確認

購入者、仲介業者、販売元に残るデータは以下のとおりである。

購入者　：商品、利用者 ID、購入 ID
仲介業者：利用者 ID、購入 ID、個人情報
販売元　：利用者 ID、購入 ID、購入情報

目標は以下の通り、達成できている。

(1) 購入者の個人情報の販売元からの保護
販売元は、自社では個人情報に結びつけることができない利用者 ID しか持たないため、購入者の個人情報を知ることはできない。

(2) 購入に関する問合せへの対応
購入者は利用者 ID・購入 ID により、仲介業者にも販売元にも問合せが可能である。仲介業者と販売元も利用者 ID・購入 ID により、相互に確認ができる。

4.考察

本方式と WWW サーバへの匿名アクセス機構である LPWP[2]と比較したものを表 1 に示す。表 1 からわかる通り、本方式は匿名性において、既存方式より優れている。

表 1　本方式と LPWP の比較

特性項目	通信 匿名性	情報 匿名性	個人 適用性
本方式	販売元へのアクセスは部分的な保護	購入情報と個人情報の保護	低い
LPWP[2]	部分的な保護	個人情報の保護	高い

5.おわりに

本稿では仲介業者の介在により、電子メディア商品の購入におけるプライバシー保護方式を提案した。仲介業者の存在は、電子メディア商品の信用保証や購入代金の支払いの簡便化という点でも購入者にメリットがある。さらに TRUSTe[3]のようなプライバシー保護基準の監査機関の認定を受けた仲介業者も増えてきている。そのような業者での本方式の利用を進めたい。

参考文献

[1] M.K.Reiter and A.D.Rubin, Anonymous Web Transaction with Crowds, CACM Vol.47, No.12 (1999)

[2] E.Gabber, P.B.Gibbons, D.M.Kristol, Y. Matias and A.Mayer:Consistent, Yet Anonymous, Web Access with LPWP, CACM Vol.47, No.12, pp.42-47 (1999)

[3] TRUSTe, http://www.truste.org/