M-3 携帯電話†を用いた匿名購入システム

An anonymous purchasing using authentication based on mobile phone serial number

藤井 治彦‡ 塩野入 理‡
Haruhiko Fujii Osamu Shionoiri

1．まえがき

ほとんどのネット上の商店では,住所,氏名,クレジットカードなどを入力してユーザ登録をし,ID,パスワードを発行してもらってから購入をすることになる.しかし,このような方式だと,様々な商店を回るたびに,個人情報流出の危険性が高くなる.また ID,パスワードも増えていき,どれがどのID,パスワードか分からなったり,忘れてしまったりする.

筆者らは,携帯電話を用いた認証方式[1]を提案してきた.本稿では,これを応用し,上記の問題点を解決する,高利便性かつ安全で普及性のある匿名購入システムの提案および,これに基づく実装について説明する.

2．要求条件

購入システムのうち,特に,認証と個人情報管理に関する要求条件には以下のものが挙げられる.

(1)利便性：使い勝手がよいこと.パスワード方式は,入力自体は簡単であるが,ほとんど利用しない商店でも，商店ごとに異なった ID,パスワードの組を記憶しておかなければならない.

(2)安全性：なりすましが困難であること.パスワードは数個の文字列なので簡単に解析してなりすましができる.

(3)普及性：ユーザ側の導入コストが低いこと.IC カードやバイオメトリクス方式では,ユーザ側に認証専用のハード・ソフトが必要となり,現時点での急激な普及は見込めない.

(4)匿名性：個人情報の流出を防げること.ほとんどの商店では,品物は宅配かつクレジットカード決済などになるため,商店側に氏名,住所,クレジットカード番号などの情報と,どのユーザが何を買ったかという情報が必ず残る.

3．提案方式

本方式の構成要素は,以下のものがある.

- **認証サーバ**：各ユーザのユーザ ID と住所,カード番号,携帯電話の固体識別情報，メールアドレスなどの情報を予めもつ(表 1).SessionID は,現在進行中の取引を識別する情報であり随時入れ替わる.NULL は現在取引が行われていないことを示す.
- **携帯電話**：ユーザの所有物であるとする.
- **端末**：専用ハード・ソフトが不要なので任意の端末が可.
- **商店サーバ**：商品 DB（商品 ID と金額など）を持ち,オンラインショッピングのページを端末に表示する.
- **課金サーバ**：ユーザに対して課金を行う.
- **配送会社サーバ**：配送会社にあり配送伝票の受信を行う.

また,端末と商店サーバ間の通信とメールの送受信以外の通信は全て SSL で行われるものとする.

表 1：認証サーバ内 DB

ユーザ ID	birdman	orange	･･
氏名	小泉次郎	山田太郎	･･
住所	大阪府****	神奈川県****	･･
カード番号	8918444****	3098576****	･･
固体識別番号	SN7126****	PR8563****	･･
ﾒｰﾙｱﾄﾞﾚｽ	koi@docomo***	yam@docomo***	･･
SessionID	12841	NULL	･･
ﾜﾝﾀｲﾑURL	https://***.com/9iweoi8ryfh.html	NULL	･･

図 1 を元に,提案方式の説明を行う.

S1：ユーザは端末から商店サーバにアクセスする.商店サーバは認証サーバに SessionID の発行を要求し,SessionID を含ませたオンラインショッピング画面を表示する(図 2).

S2:ユーザは商品を選択しユーザ ID と商品 ID を送信する.

S3:商店サーバは,商品 ID に対応する金額と,ユーザ ID を認証サーバに送信すると同時に,端末に対して,リロードタグを入れたページを表示して,端末をﾘﾛｰﾄﾞ状態とする(図 3)

S4：認証サーバは,ワンタイム URL を生成し,ユーザ ID に対応する携帯電話のメールアドレスに対して,以下のようなメールを送信する(図 4).

FROM：(認証サーバのアドレス)
TO：(携帯電話のアドレス)
SUBJECT：購入確認メール
本文：購入の場合は,セッションID を確認の上,
リンクをクリックしてください.
ユーザID：foma-beta
購入金額：9800 円
セッションID：12841
*https://***.com/9iweoi8ryfh.html*

S5:ユーザは,メールを受け取ると,メールと端末の各々に表示されている SessionID が同じであることを確認してから,メールの中のワンタイム URL をクリックする.

S6:携帯電話に表示されたページには下に示すタグ[2]が含まれており,「購入」ボタンを押すと固体識別番号と SessionID が認証サーバに送信される.

```
<form method="***" action="***.cgi" utn>
<input type="hidden" name="SessionID" value="12841">
<input type="submit" value="購入">
```

S7:認証サーバは,受信したら送信元の IP アドレスをチェックした後,受信した固体識別番号と SessionID および FORM データの送信元ページの URL の組み合わせ等をチェックし,問題が無ければ,課金サーバに課金情報を送信する.その後,ワンタイム URL の HTML ファイルを消去する.

S8：認証サーバは商店サーバに対して購入終了のメッセージを送信し,商店サーバはリロード状態を解除して,購入操作が正常終了した旨のメッセージを端末に表示する.

S9：認証サーバは,配送会社サーバに対して図 5 に示す内容の伝票(氏名,住所,SessionID,商店名などを含む)を送信し,配

† 本稿では携帯電話として固体識別情報送信機能つきブラウザフォン(i モード 503i 以降や FOMA など)を想定する.

‡ 日本電信電話株式会社 NTT 情報流通ﾌﾟﾗｯﾄﾌｫｰﾑ研究所

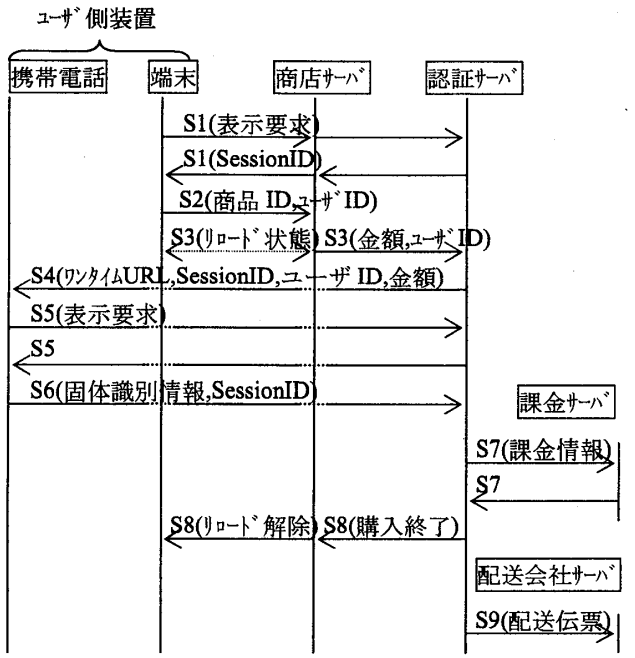

図 1：構成要素間の通信の概要

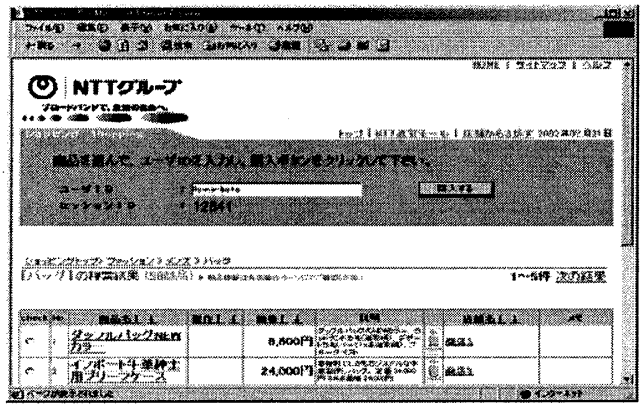

図 2：オンラインショッピング画面

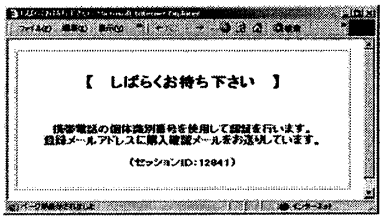

図 3：リロード状態の画面

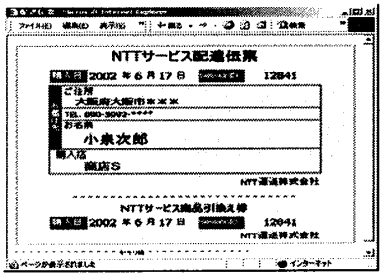

図 5：配送伝票

図 4：携帯電話の画面

送会社は,この伝票に記載されている商店に行き,SessionID に対応する商品を受け取り,ユーザに商品を配送する.ただし商品は包装されており中に何が入っているかは配送会社には分からないものとする.

4．考察

(1)利便性：ユーザは,購入に際してユーザ ID を入れる以外は,全て,クリックのみであり,また,ユーザ ID は各商店で共通に使用できる.更にメールの形で購入歴が残るのでレシート代わりになり利便性は非常によい.

(2)安全性：S2 で他人がユーザ ID を使用しても,S4 で確認メールを受け取ることができないので不正購入はできない.更に確認メールを盗聴もしくは,総当り攻撃などをしてワンタイム URL が分かったとしても,S6 をなりすますのは困難である.なぜならば,携帯電話の固体識別情報は書き換えることが不可能であり,更に固体識別情報は SSL 通信で必ず電話会社のサーバを介して送信されるため,S7 のチェックをすり抜けることは困難である.

(3)普及性：本方式では携帯電話を認証用ハードウェアとして使用するが,これは IC カードのように認証のみに使用するハードウェアではない.固体識別番号送信機能付き携帯電話の普及率は高く,今後更に普及が予想される.オンラインショッピングをする人は IT リテラシが比較的高いので,このような携帯電話を持つ確率は高いといえる.よって本方式の普及性は十分にあるといえる.

表 2：代表的な認証方式と提案方式(認証部分)との比較

方式名	利便性	安全性	普及性
パスワード方式	×	×	○
IC カード方式	○	○	×
バイオメトリクス方式	○	○	×
提案方式(認証部分)	○	○	○

(4)匿名性：表 3 に,各構成要素がもつ情報を示す.表からも分かるように,商店サーバは何が売れたかはわかるが,誰が買ったかが分からず,認証サーバ,課金サーバは誰が幾ら使ったかは分かるが,何を買ったかが分からない.また,配送会社サーバは誰がどこで買ったかは分かるが,何を買ったのかが分からない.よって,匿名性は非常に高い.また,逆にユーザが購入を否認したとしても SessionID を元に各サーバに問い合わせれば購入の事実を証明できる.

表 3：各構成要素が持つ情報

構成要素	金額	氏名住所	商店名	商品名
商店サーバ	○	×	○	○
認証サーバ	○	○	○	×
課金サーバ	○	○	×	×
配送会社サーバ	×	○	○	×

5．むすび

本稿では携帯電話と端末を併用する新しいタイプの購入システムの提案と実装物の紹介を行った.認証サーバと課金サーバを電話会社がすると非常に安全性が高くなるので,今後実用化に向けて検討していきたい.

[1] 藤井治彦, "携帯電話を用いた認証方式, "情報処理学会第 64 回全国大会, Vol.3, pp.429-430,March 2002.
[2] i モード対応 HTML Version3.0 タグ,http://www.nttdocomo.co.jp/mc-user/i/tag/utn.html