5M－3

インターネットにおけるクレジット決済システム
１．消費者用システム

中山恭與、工藤道治、川副博

日本アイ・ビー・エム株式会社　東京基礎研究所

1. はじめに

近年コンピュータネットワークを利用した電子商取引が非常に注目されている。中でもインターネットを利用したものは、その広域性の面から見て特に汎用性が高いといえる。しかしインターネットはオープン型のネットワークであるため、他方でセキュリティーの面で考慮すべき問題も数多い。

筆者らのグループでは、インターネットを利用したクレジット決済のシステムを開発した。このシステムの実証実験は平成８年４月より開始され、そこでは一般から募集したモニタユーザ（消費者）、商店およびクレジットカード会社の間で実際の取引が行われている。本稿ではこのうちの、消費者のためのシステムの仕組みやそれを使って実際の取引を行う際の操作などについて述べる。

2. 決済システム全体の概要

本システムは消費者、商店、クレジットカード会社の三者から構成される。この三者はそれぞれインターネットに接続されいる。消費者はWWWブラウザと専用の決済用プログラムを使って商店の作る「仮想商店」にアクセスする。商店側ではＷｅｂのホームページで商品を陳列するためのＷｅｂサーバプログラム（ＨＴＴＰＤ）と決済用のサーバが稼働している。クレジットカード会社ではカードの与信検査のシステムと接続された決済用のサーバが稼働している。この三者間でｉＫＰと呼ばれるプロトコル[1]を用いて通信を行いクレジットの決済を行う。このプロトコルではメッセージの暗号化や電子署名を使って取引の安全を図っている。

また、消費者のクレジットカードにはＩＣカードを使用しており、電子署名のための秘密鍵や証明書などはこの中に保存される。このため、カードの所有者本人しかクレジット決済による買い物ができない仕組みになっている。

3. WWWによる商品選択

実証実験のために公募したモニタユーザは、ＰＣを使ってインターネットにアクセスできることが募集の条件となっている。ユーザには決済用プログラム、マニュアル、ＩＣカード（クレジットカード）およびＩＣカードリーダが配布される。決済用プログラムをＰＣに導入すると、プログラムはユーザが使用しているWWWブラウザのヘルパアプリケーションとして自動的に登録される。

買い物を行う際、消費者はまず各商店のWWWのホームページ（仮想商店）にアクセスする。このホームページの内容や様式には特に規定がなく、各商店では自由にデザインする事ができる。一般的には、商品の選択や支払い方法の指定を行い、配達先や連絡先などを入力してから「申し込み」ボタンを押して商店のＨＴＴＰＤに必要な情報を送る。ＨＴＴＰＤではこれをシステムで規定されているフォーマットに変換し、規定されているＭＩＭＥタイプでWWWブラウザに返送する。WWWブラウザは決済用プログラムを起動し、受け取った情報（購入情報）をプログラムに引き渡す。購入情報には受け付けの日時、購入内容、金額などが含まれており、プログラムは起動の際にその内容のチェックを行う。

4. ＩＣカードによる鍵の保管

クレジットカード決済による取引を行う際には、購入情報の他にクレジットカードに関する

Payment by Credit Card on The Internet:
1. A System for Buyers

Yasutomo NAKAYAMA, Michiharu KUDO, Hiroshi KAWAZOE
Tokyo Research Laboratory, IBM Japan
1623-14 Shimotsuruma, Yamato, Kanagawa 242, Japan

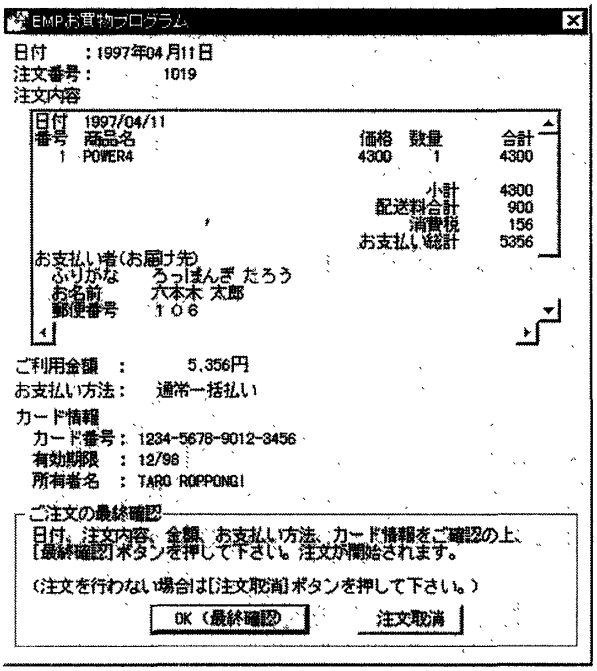

図１　最終確認画面

情報と電子署名のための鍵や証明書が必要になる。本システムではこれらの情報はＩＣカード内に保存されている。この情報はＰＣのシリアルポートに接続されたＩＣカードリーダを介してＩＣカードからプログラム内にロードされる。なお、ＩＣカードから情報を読み取るためには、４桁の暗証番号をカードリーダ上のパッドから入力する必要がある。

取引に必要な情報がすべてプログラムにロードされると、それらを表示するパネル（最終確認画面、図１参照）が現れ消費者に確認を促す。ここで「最終確認」ボタンを押すと決済用プロトコルが開始される。このボタンの押下は、通常のクレジットカードを使った買い物の際に行う署名に相当する。決済プロトコルの中では消費者、商店、クレジットカード会社の三者はそれぞれこのパネルに表示された情報に対して電子署名を行うので、消費者はボタンを押す前に表示内容をよく確認しなければならない。

5.　ｉＫＰプロトコルによる通信

決済プロトコルが開始されると、進行状況がパネルに表示される。消費者側からは、このプロトコルは商店側の決済用プログラムとの間でメッセージが２往復するように見える。２回目の往信の後、商店側の決済プログラムはクレジットカード会社に与信依頼を行いその結果を復信で返す。

通信およびそれに付随する処理全体にかかる時間は十数秒から数十秒程度である。決済用プロトコル中では注文内容そのものは送信されず、そのハッシュ値や注文番号で商店側との確認を行っている。このため各メッセージの長さはどの取引でもそれぞれほぼ一定で、長いものでも数百バイト程度のものである。従って通信そのものにかかる時間はほぼ一定となっている。処理時間の格差は主に消費者のＰＣのＣＰＵの処理速度によるもので、そのほとんどを暗証番号などの暗号化処理が占める。なお暗号方式は楕円エルガマル暗号を使用している。

プロトコル終了後、最終的な取引の結果（取引成立／拒否）が表示されて決済プログラムは終了する。最終画面に表示された内容やプロトコル中にやりとりされたメッセージの内容はログとしてファイルに保存される。

6.　ログビューア

決済プロトコルが終了して取引が成立した後の処理（配送など）は従来の電話や郵便による取引と全く同じに行われる。キャンセルやクレームも電話などで直接商店と連絡を取って行う。このような時には、ログビューアプログラムを使ってファイルに保存されたログを検索して、取引の内容を表示したり印刷する事ができる。

7.　おわりに

消費者用システムではプログラム本体のみならず、その導入方法や機器の接続法などにも簡便さや使いやすさが要求される。今回の開発にあたってはユーザインターフェイスにおいてそれらを考慮するとともに、マニュアルの記述などにも配慮した。

参考文献

(1)M. Bellare, J.A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Sterner, G. Tsudik, and M. Waidner, "iKP - a family of secure electronic payment protocols," Workshop on Electronic Commerce, pp. 1-21, USENIX, 1995