インターネットにおけるクレジット決済システム 2. 仮想商店システム

5M－4

工藤 道治、川副 博、中山 恭與
日本アイ・ビー・エム(株) 東京基礎研究所

1. はじめに

インターネットでのクレジットカード払いによる買い物システムを開発した[1]。インターネット上で複数者による処理を行う場合、次に示す情報セキュリティ上の問題を考慮する必要がある。

1. 改ざん防止
2. 否認防止
3. 相手認証
4. 機密保持

特にインターネットで商品の提供を行う場合、消費者の不正などにより仮想商店(インターネット上の商店)が一方的な不利益を被らないことを保証しなければならない。本稿では、主に仮想商店と消費者とのやりとりにおいて発生する可能性のある問題点を上げ、本システムにおいて上記のセキュリティが満たされていることを述べる。

2. 仮想商店と消費者とのセキュリティ

2.1 改ざん防止

消費者による商品決定プロセスは、仮想商店の提供する WEB のホームページにアクセスすることで実現している。一方で、クレジットカード支払プロトコル(iKP)[2]は、商品決定プロセスとは独立に設計されている。従って、仮想商店システムは、WEB と iKP プロトコルを連携したときに、消費者側で発生する可能性のある不正行為を検出できるように構成しなければならない。例えば、WEB のホームページで仮想商店から示された購入総額 10 万円の商品を消費者が改ざんして 1 万円に変更するような場合である。

商品決定と iKP プロトコルとの連携方法を図1に示す。消費者が WEB ブラウザを使って購入商品を決定したら、その注文内容は仮想商店の WEB サーバプログラムに送られる(①)。WEB サーバ側では、CGI プログラムを実行し注文内容を注文データベースに登録し注文番号を発行する。注文番号を受け取った消費者側プログラムは、iKP プロトコルを起動する(②)。このときに注文内容を引数として渡す。消費者 iKP プロトコルは注文内容のハッシュ値を仮想商店に送信する(③)。仮想商店は、消費者 iKP プロトコルが送信した注文内容のハッシュ値と、注文データベースに登録されている注文内容から計算されるハッシュ値とが同一の値になることを確認する。

消費者により注文内容等が改ざんされた場合、消費者 iKP プロトコルが生成する注文内容のハッシュ値が、仮想商店側の注文データベースの内容に基づいて計算されるハッシュ値と異なるので仮想商店側での検出が可能である。また、消費者が WEB を使った商品選択プロセスを実行せずに消費者 iKP プロトコルを不正に実行した場合、注文データベースに該当する注文が存在しないというエラーにより検出が可能である。また、正しく処理された買い物データを再度使って消費者 iKP プロトコルを不正に実行しようとした場合も、仮想商店側で複数回使用のエラーとして検出が可能である。

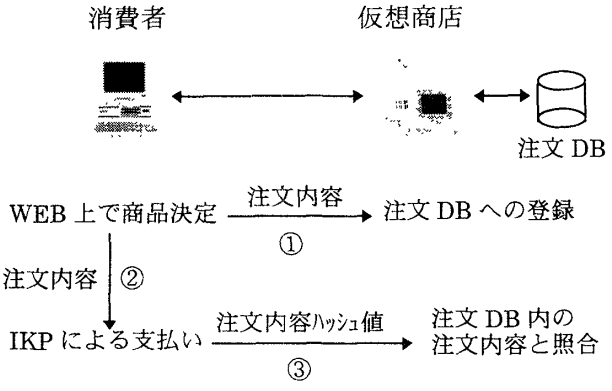

図1: 商品決定と iKP の連携

Payment by Credit Card on The Internet: 2. A System for Merchants, Michiharu KUDO, Hiroshi KAWAZOE, Yasutomo NAKAYAMA, Tokyo Research Laboratory, IBM Japan, 1623-14 Shimotsuruma, Yamato, Kanagawa 242, Japan

2.2 否認防止

消費者が実際には注文したのにも関わらず、注文していないと嘘をつくような場合を想定して、商店では消費者からの購入意志の証拠を保持しなければならない。また、クレジットカード会社が消費者の商品購入に際して与信 OK を判断したのにも関わらず、あとでそれを勝手に変更することができないように、商店ではクレジットカード会社の与信 OK の証拠を保持しなければならない。本システムでは、消費者の秘密鍵による注文内容に対するデジタル署名、およびクレジットカード会社の秘密鍵による与信結果に対するデジタル署名をデータベースに保持し、紛争時の証拠として利用できるようにした。

2.3 相手認証

消費者、仮想商店、クレジットカード会社は、証明書認証局が発行した証明書を前もって取得している。仮想商店は、消費者の認証に際して消費者が生成したデジタル署名を消費者の証明書を使って検証することによって相手を認証する。消費者の証明書は、iKP プロトコル実行時に消費者から送られる。同様の方法によりクレジットカード会社の認証も行う。

2.4 機密保持

消費者のクレジットカード番号は、本来商店側では知ってはいけない情報だが、店頭販売等においては知ることができてしまうのが現状である。iKP を使うと、消費者のクレジットカード番号はクレジットカード会社の暗号用公開鍵によって暗号化されるので、仮想商店では知ることができない。一方、注文内容は、本来クレジットカード会社が知る必要のない情報である。iKP プロトコルを使うと注文内容はクレジットカード会社に送られない。iKP プロトコルは注文内容の平文は送らず、ハッシュ値のみを仮想商店に送信するので通信途中での盗聴に対して安全である。図 2 に情報の機密保持について示す。なお、WEB を使った注文内容の送信における機密保持は、 WEB ブラウザの SSL などのセキュリティ機能を使うことで守ることとしている。

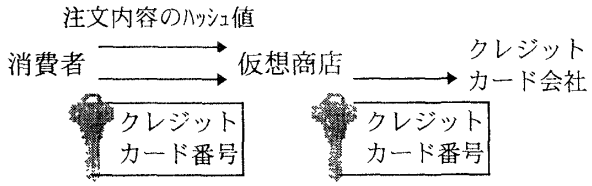

図 2: 情報の機密保持

3. 発注システムとの連携

インターネットでの商品購入が確定した場合、その注文を発注システムと連携させ発注処理に結び付ける必要がある。本システムでは、iKP プロトコルにおいてクレジットカード会社の与信 OK が得られた注文は全てログデータベースに出力される。発注システムとの連携プログラムは、任意のタイミングでログデータベースの未処理エントリにアクセスし、発注処理プログラムに注文データを渡すことができる。

4. 今後の課題

通信エラーが多発するような時に、全ての処理をインターネット上で行うことが困難な場合がある。例えば、仮想商店からクレジットカード会社に与信照会をしても、通信エラー等により与信結果を受信できない場合である。現状では人間系で対処せざるを得ないが、今後は、別の通信手段(例えば、電話や FAX)に自動的に切り替わるようなプロトコルを設計する必要があると考えられる。

5. おわりに

インターネット上で安全にクレジットカードによる買い物ができるシステムを開発した。セキュリティ上の問題点とその解決方法について述べた。

参考文献

[1] 中山他、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、情報処理学会、第 55 回全国大会, 1997

[2] M. Bellare, J. A. Garay, R. Hauser, A. Herzberg, H. Krawczyk, M. Steiner, G. Tsudik, and M. Waidner, "iKP - A Family of Secure Electronic Payment Protocols," Workshop on Electronic Commerce, pp.1-21, USENIX, 1995