SETを用いた情報流通プラットフォーム

2G－2

三浦 一善　森保 健治　生沼 守英
NTTソフトウェア研究所

1. はじめに

ソフトウェアやマルチメディアコンテンツなどのデジタル情報販売は在庫管理や物流のコストが不要であり、インターネットを利用することにより各地に店舗を設置する必要もないことなどから、今後の需要の伸びが期待される。

一方、1997年5月にVISAおよびMaster Cardの共同開発による、インターネット上でのクレジット決済プロトコル規格SET [1] (Secure Electronic Transaction) が規定され、将来的にはインターネット上での決済手段のデファクトスタンダードの地位を確立することが予測される。しかし、SETは「物」の販売に主眼を置いており、SETのみでデジタル情報の販売を扱うのは難しい。

このためデジタル情報販売においてもSETを利用することで、利用範囲をより広げることが可能になると考えられる。

本稿はSETを利用してインターネット上での情報販売を実現するための手法について、従来の検討結果[2]を元に実装における課題について報告する。

2. インターネット上における情報販売

インターネット上でデジタル情報を販売するために、我々は情報流通プラットフォームInfoket [3]を提案している。Infoketでは、まず暗号化されたデジタル商品をCD-ROMやインターネット経由で自由にダウンロードするなどして配布する。利用者はダウンロードが正常に完了したことを確認した後、復号鍵を安全確実に取得するためのInfoketプロトコルを実行することにより決済処理を行うことができる。

本方式は決済処理が商品のサイズとは無関係であるため、インターネットのような不安定なネットワークに向いている方式といえる。

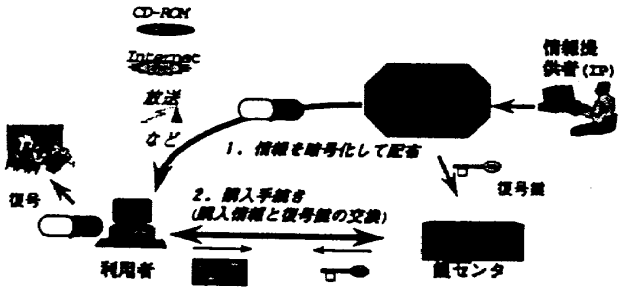

図1：Infoketによる情報販売

3. SET

従来、インターネット上でのクレジットカード番号の送信はSSL等の暗号化プロトコルを用いてきた。これにより、SET以前にも通信の秘密保持、改ざん防止について対処してきた。しかしこれらのプロトコルでは、クレジットカード番号の送り主の本人性確認ができない、商店において利用者のクレジットカード番号が見られるなどの問題もあった。

SETは、これらの問題を解決してクレジットカードでのインターネット経由の安全な支払いを実現するために開発された。

SETは以下の特徴を持つ。

- 利用者 (Cardholder)、販売店 (Merchant)、カード会社 (Acquirer) がそれぞれ正当なものであるかどうか、認証局 (CA) を使用して、全てデジタル証明書により認証される。
- 注文情報のうちカード番号等の個人情報は、販売店では読めず、カード会社にそのまま転送される。
- 異なるベンダーによるソフトウェアの相互運用性が確保される。

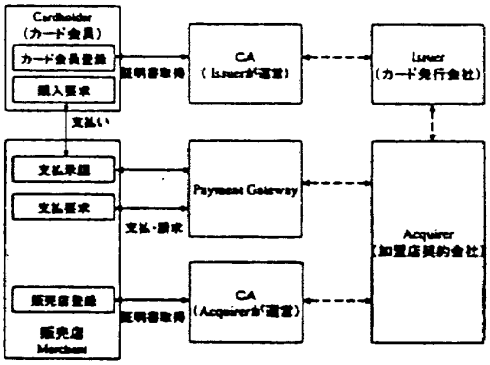

図2：SETの概要

4. SETとの結合

SETを利用してInfoketを実現するためには以下を考慮する必要がある。

- クレジットカード情報はSETプロトコルで送信する。
- SETプロトコルとInfoketプロトコルの同期をとり、与信結果と復号鍵配送結果の情報を共有する。
- ユーザビリティを重視する。
- 特定のWalletに依存させない。
- Merchant Server、Walletの改造は行わない。

5. SETとの同期

同一の端末からSETプロトコルとInfoketプロトコルが動作し、SETプロトコルによる決済が終了した端末に対してInfoketプロトコルで対応する復号鍵を配送する必要がある。このためには、2つのプロトコルの同期を図るためのキーとそのキーの共有方法、および同期のタイミングの検討が必要である。

5.1 同期をとるキー

Infoketと SETの間で同期をとるためには、それぞれのトランザクションから同一トランザクションを結び付ける必要がある。ここでトランザクションを識別するID（以下、決済

An Information Distribution Platform with SET
Kazuyoshi Miura, Kanji Moriyasu, Morihide Oinuma
NTT Software Laboratories

識別 ID）を設ける。決済識別 ID に対する要求条件は、同一販売店において一意な値であること、なりすましを防ぐため他の決済識別 ID を推定できないような暗号学的に安全な乱数を含むことがあげられる。

2 つのプロトコルで決済識別 ID を共有するためには Infoket の端末プログラム（Helper）と SET の Wallet が、決済識別 ID（あるいはそれと 1 対 1 の関係にある ID）を知る必要がある。前述の要求条件を満たし、販売店側で生成された決済識別 ID を端末側に通知する手段として、SET については Payment Initiation 中の必須項目である LID-M を利用することが考えられる。LID-M は、販売店がトランザクションを識別するためのラベルとして定義されている。また、Infoket については既存のプロトコルに決済識別 ID を付加することで容易に対処できる。

5.2　同期タイミング

Infoket は SET の与信結果を参照し、与信が成功であれば復号鍵を配送し、復号鍵の配送が成功した後に SET Server に請求処理を依頼する。また、復号鍵の配送が失敗した場合は SET Server に与信の取り消しを依頼する必要がある。

以下の 3 つの方式について評価検討してみた。

（方式 1）2 つのプロトコルを並行して実行

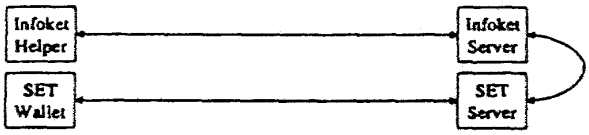

図 3：並行処理方式

- 2 つのプロトコルの同期を販売店側で行うため確実である。
- 双方のプロトコルが任意のタイミングで失敗することがあるため、そのリカバリ処理が複雑となる。
- 2 つのダイアログが利用者端末に現れるため、並列で入力が必要になる場合がある。

（方式 2）2 つのプロトコルを逐次実行

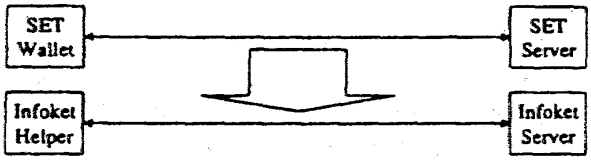

図 4：逐次処理方式

- 2 つのプロトコルは順に処理されるので異常状態の検出、リカバリ処理が容易に行える。
- 利用者が同時に入力するダイアログは一つになる。
- SET Wallet の与信結果を安全確実に Infoket Helper 側へ伝える必要がある。

（方式 3）Infoket プロトコルが SET プロトコルをトンネル

図 5：トンネル方式

- Infoket プロトコルが SET プロトコルを解釈する必要がある。
- デジタル情報購入時と物品の購入の場合とで Wallet の Proxy 設定を変更する必要がある。

（方式 3）については、決済手段に応じて Proxy の設定が必要となる。（方式 1）については複数の入力プロセスが同時に発生するため、ユーザビリティの点から（方式 2）を採用することとした。

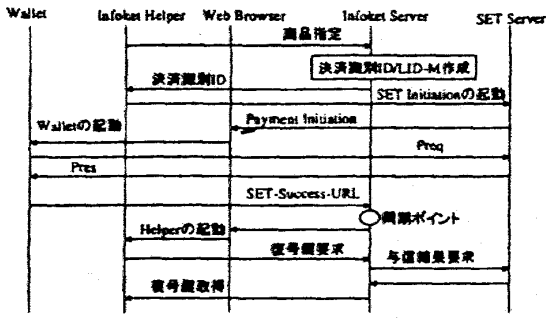

図 6：SET と Infoket の結合

（方式 2）を実装する際に問題となるのは、SET Wallet から Infoket Helper への同期時に攻撃される危険性である。SET Wallet から Infoket Helper へのトランザクションの引継ぎは Payment Initiation 内の LID-M を用いることを述べたが、Payment Initiation は特に暗号化などはされない仕様となっていて、LID-M を盗聴されてしまう。そこで、LID-M の中に直接決済識別 ID を入れるのではなく、Infoket Server にて決済識別 ID と LID-M を関連付け、決済識別 ID を隠すことによりセキュリティを強化する。

6.　おわりに

情報流通プラットフォーム Infoket を SET に対応させるため、2 つのプロトコルの同期について検討してきた。日本国内において SET を運用するには日本独自の決済方法の変革、Japanese Requirement などへの対応が必要となる。

SET の次期バージョンである V2.0 についても議論が開始されている。SET V2.0 については現在、追加機能要望のとりまとめが済み、VISA と Master Card で検討を進めている段階である。今後のスケジュールについては発表されていない。主な項目としては IC カード対応、暗証番号対応、新しい暗号方式などがあげられている。その中で、デジタル商品の電子配送についても検討項目としてあがっているので、今後の動向に注意が必要である。

参考文献

[1] VISA International and MasterCard International, Secure Eletronic Transaction (SET) Specification Book 1~3 Version 1.0, 1997.5.31 (http://www.visa.com/cgi-bin/vee/nt/ecomm/main.html, http://www.mastercard.com/set/)

[2] 森保:「SET を利用した情報販売手法」.電子情報通信学会 1996 年基礎・境界ソサイエティ大会,A-169

[3] 明石・森保・寺内:「インターネットを用いた情報流通プラットフォーム:Infoket-I」.NTT R&D,46,pp.107-114