情報流通システムにおける課金方式*

寺内 敦、森保 健治、明石 修†
NTT ソフトウェア研究所‡
terauchi@slab.ntt.jp

概要

近年の Internet の普及はめざましく、非常に多くの人々が利用できるようになっている。そのため、これらの大量のユーザを対象として Internet 上で商取引をするシステムが多く提案されている。このような商取引システムにおいて重要なのは商品に対する料金を確実に徴収することのできる課金システムである。課金システムにおいては安全な取引ができることやユーザにとっての使い勝手のよさが重要な要求条件である。本稿では安全性だけでなく使い勝手にも考慮した課金プロトコルを提案する。

1　はじめに

近年の Internet の普及はめざましく、非常に多くの人々が利用できるようになっている。そのため、これらの大量のユーザを対象として Internet 上で商取引をするシステムが多く提案されている。これらのシステムでは Internet 上で直接流通させることのできるソフトウェアなどのデータの販売、あるいは購入申込を Internet で行い商品は後日送られてくる Internet 版通信販売などさまざまな形態のサービスが提供されているが、いずれの場合にも重要になってくるのが商品に対する料金を確実に支払、受領することのできる課金システムである。

Internet に限らずネットワーク上で課金手続きを行うとネットワーク上にはクレジットカード番号など個人の支払いに関する非常に重要な情報が流れる。例えばこのときネットワークを盗聴されると、このような重要な情報を無断でコピーされ後に悪用される可能性がある。この攻撃に対してはネットワーク上を流れるメッセージはすべて暗号化するという対処が必要である。このように、想定される攻撃に対してあらかじめ十分な対策を講じてセキュリティを確保できるということは課金システムに対する要求条件の中でももっとも重要なものである。

また、課金システム実現におけるもう1つの重要なポイントは支払方式である。現在、ネットワーク上の課金システムでは実装の容易さなどからクレジットカードによる支払がもっとも多く使われている。しかし、現実の世界ではクレジットカードだけではなくプリペイドカードなどサービスの種類によってさまざまな支払方式が存在してユーザの使い勝手が向上している。今後、ネットワーク上の商取引が発展してくるにつれてユーザの要求は多様化することが予想され、単にセキュリティが守れるだけではなくて現実世界と同様の使い勝手のよさが求められてくると考える。実際、日本国外で提案されているネットワーク上の商取引システムではクレジットカードだけでなく、さまざまな支払方式が提案されている。

そこで本稿では、過去に提案されている課金システムにおける支払方式の整理を行い、それらの長短について検討を行う。その上で、セキュリティを守

*Network Payment Protocol for Information Market System

†Atsushi TERAUCHI, Kenji MORIYASU, Osamu AKASHI
‡NTT Software Laboratories

れるだけでなく、より使い勝手を向上させたネットワーク上の課金プロトコルを提案する。

2 課金システムの支払方法

2.1 従来の方式

現在、提案されているネットワーク上の課金システムでサポートされている支払方法は大きく分けると次の3つである [1]。

2.1.1 電子キャッシュ方式

電子キャッシュと呼ばれるデータを現金代わりにしてネットワーク上で商品の売買を行う方式である。このカテゴリーには Digicash[2] や NetCash[3] システムが含まれる。この方式の特徴は、実際の現金による取引と同様に商取引における購入者の anonymity(匿名性) を保証できるという点である。つまり、誰が何を買ったかは本人以外のエンティティには知ることができない。この方式の欠点は同一キャッシュの二重使用を防ぐために大量のデータベースを管理しなければならないことである。また、本方式と後述の電子小切手方式では電子キャッシュ (小切手) を発行する機関の他に、発行された電子キャッシュ (小切手) の妥当性を保証するための機関 (銀行、クレジットカード会社など) が必要になる。

2.1.2 電子小切手方式

電子キャッシュのような無記名の貨幣ではなく、署名付きの電子小切手を用いて売買を行う方法である。NetBill [4] や NetCheque [1] といったシステムがこのカテゴリーに分類される。特徴は電子小切手に署名が付加されているため、トランザクションの正当性、取引相手の正当性などを検証するための枠組を組み入れることが容易なことである。反面、使用する電子小切手には使用者の署名を付加するので anonymity は保証されない。

2.1.3 オンラインクレジットカード方式

現状のクレジットカードを用いる方式である。現在、提案されているシステムの大半はこのカテゴリーに含まれると思われる。基本的にはクレジットカード番号を暗号化通信によってやりとりするだけである。長所としては、ユーザはクレジットカードだけがあればすぐにサービスが利用できる点である。しかし、この方法は、課金のコストが高いため少額の商品を多数購入するようなサービスには向かないなどクレジットカードの欠点をそのまま継承している。

2.2 提案する方式

近年では、Internet における商取引においてもプライバシー保護の観点から、anonymity を保証できるということが重要な要求条件の1つとされることが多くなっている。提案されている電子キャッシュ方式によるシステムでもその点をセールスポイントとしている。しかし、anonymity を保証することは犯罪の検出のし易さとトレードオフの関係にある。そのため、セキュリティのことを考えると anonymity の保護は課金システムにとって、必ずしも必須の要求条件とは言えない。そこで、本稿ではセキュリティを守る仕組みを組み入れやすい電子小切手方式に基づく課金システムを考える。

従来提案されている電子小切手方式 [1, 4] ではエンドユーザは (実際の小切手のように) 好きなときに小切手の発行を行って購入を行うことができるが、決済はその都度行われるわけではなく、後日まとめて決済される。このことはオンラインクレジットカード方式でも同様である。しかし、ユーザの使い勝手の点を考えると、決済はあらかじめ済ませておいた一定額の電子小切手を手元に持っておき、支払いの際に必要なだけ使うプリペイド (前払い) 課金の方が (1) あらかじめ決済が済んでいるので買う側、売る側双方にとって安心感がある、(2) 手元に電子小切手があるので、まとめ買い、時間による従量課金などにも適用可能、(3) 一定額だけ決裁しているのでユーザの知らない間に課金額が増加することがない、というメリットがあり使い勝手の点で優れる。そこで、本稿ではセキュリティの高い電子小切手とユーザにとってより使い勝手のよいプリペイド課金を併用した課金方式を提案する。

2.3 実現のポイント

この方式を実現するために克服すべきポイントは、「電子小切手を複製・改竄を防御しながら、どうやってユーザの端末に保存するか」ということである。電子小切手を単純にディスク上に保存してしまうと簡単に偽造、あるいは盗難(コピー)される恐れがある。

その問題点の解決策として考えられるのがタンパーフリーハードを用いる方法である。タンパーフリーハードとは、内部に保存された情報の盗難および改造を防御するために作られたハードウェアの総称で、メモリの入ったカードの蓋を開封するとメモリの内容がすべて消えてしまうなどさまざまな方法が提案されている。タンパーフリーハードを使うと原理的に完全な防御ができるため、ユーザの端末にタンパーフリーハードの存在を仮定すれば情報の安全性を保証することができる。しかし、タンパーフリーハードはまだ十分に普及しているとはいえず、その存在を仮定することは現実的ではない。つまり、現状ではソフトウェアだけで防御するしかないことになるが、そのような状況でどこまでセキュリティを保護できるかを知ることは重要である。そのため、本稿ではタンパーフリーハードを用いない観点からシステムを設計する。

そこで、提案するプロトコルでは上記の問題に対処するために、電子小切手に関する情報は基本的に信頼できる第三者が保存しておいてユーザは購入の開始時にその第三者から自分の情報をダウンロードして購入終了時に第三者に戻す、という方法を用いる。このため、ユーザが自分の端末に保存している間に電子小切手の偽造を行っても第三者に送り返した時点で第三者の保存する情報との喰い違いが生じるため偽造が検出できる。

3 提案する課金システム

3.1 モデル

本稿で想定する課金システムのモデルについて説明する(図1)。このモデルに含まれるエンティティは、以下に示すように「ユーザ」「商店」「センタ」と「銀行」の4つである。

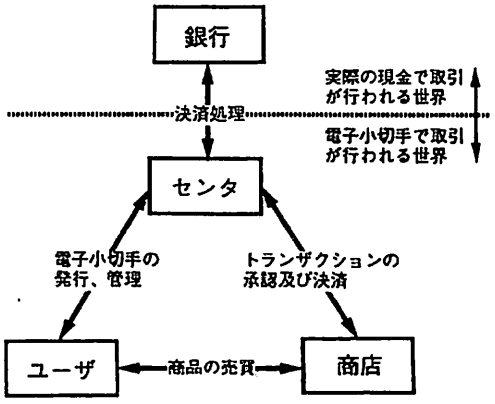

図1: 課金システム

4者の役割について説明する。

- ユーザ
  センタに電子小切手を申し込み、この電子小切手を用いて商店から商品を購入する。
- 商店
  電子小切手を持ったユーザに対して商品を売る。ユーザからの購入申込が来たらセンタに対して承認依頼を行う。取引が承認されれば商品をユーザに送る。またトランザクション終了後、センタに対して売上の決済を依頼する。
- センタ
  ユーザに対しては電子小切手を発行、管理し、商店に対しては取引の承認を行う。また「銀行」と通信して電子小切手による取引の決済を依頼する。
- 銀行
  センタからの決済要求を受けて決済を行う。銀行かクレジットカード会社がこのエンティティになり得る。

ネットワーク上の課金に関わるエンティティは「ユーザ」、「商店」、「センタ」の3者である。「セン

タ」と「銀行」の間では通常の決済処理が行われる。そのため、「センタ」と「銀行」間のやりとりについては安全な通信ができるもの、つまりその間で盗聴などの犯罪が行われることはないと仮定して以下では言及しない。また、「ユーザ」「商店」は(単独でも結託してでも)悪事を働く可能性があるが「センタ」は信頼できるものとする。

「センタ」は1つであるが「ユーザ」「商店」は各々複数あってもかまわない。しかし、簡単のため以下では「ユーザ」「商店」も1つであると仮定して議論を進める。

3.2 課金プロトコル

本稿で提案する課金プロトコルは大きく(1)電子小切手の申込、(2)商品の購入という二つのフェーズに分割できる。それぞれについて手順を説明する。説明においては以下のことを仮定する。

- メッセージの暗号化にはRSA暗号などの公開鍵暗号方式[5]を用いる
- 各エンティティは他のエンティティの公開鍵を知っている。
- ユーザおよび商店はあらかじめセンタに登録を行っており固有のIDおよびパスワードを持っている。
- メッセージ消失などのプロトコルエラーは生じない。

3.2.1 記法

- U, M, C: それぞれユーザ、商店、センタ
- $E_k\{M\}$: メッセージMを公開鍵kを用いて暗号化する関数
- $Sign_X(M)$:Mに対してなされたX(XはU, M, Cのいずれか)のディジタル署名
- e: 署名作成関数
- d: 署名検証関数
- U_{ID}, C_{ID}, M_{ID}: それぞれユーザID、電子小切手ID、商店ID
- $Cash(U_{ID}, C_{ID}, price)$: 電子小切手
- (KP_X, KS_X): 公開鍵暗号の公開鍵、秘密鍵の組(XはU, M, Cのいずれか)
- $h()$: 一方向ハッシュ関数

3.2.2 電子小切手の申込

1. ユーザはセンタに対して電子小切手の申込を行う。センタに送付すべき情報はU_{ID}およびユーザの銀行口座情報、申し込む電子小切手の金額である。このメッセージには、ユーザのディジタル署名を付加する。メッセージはセンタの公開鍵によって暗号化されている。そこで、送信されるメッセージは以下のように表現できる。

$$\begin{cases} E_{KP_C}\{Sign_U(h(M)), M\} \\ M = U_{ID}, \text{銀行口座情報}, \text{電子小切手の金額} \end{cases}$$

2. 申込を受け取ったセンタは、自分の秘密鍵によってメッセージを復号化して、送られてきたディジタル署名の正当性を以下のようにして検証する。ここで、

   $Sign_U(h(M)) = e_{KS_U}\{h(M)\}$

   であるから、KP_Uを用いて

   $d_{KP_U}\{Sign_U(h(M))\} = d_{KP_U}\{e_{KS_U}\{h(M)\}\} = h(M) \cdots (1)$

   である。ここで、e, dは$(e_{KP_X} \circ d_{KS_X})$が恒等変換となる性質を持つ。$h(M)$は$M$に依存した値であるから、送られてきた$M$から$h(M)$を計算して式(1)の値と一致すればメッセージの改竄がなかったことが分かる。

3. 改竄のなかったことが分かればセンタは銀行に対してユーザの口座から引き落としを要求した後、申込が完了した旨のメッセージをユーザに送付する。このメッセージにはセンタのディジタル署名を付加して、発行する電子小切手に付

加した一意な番号 C_{ID} を含める。センタではこの C_{ID} を U_{ID} と組にして管理する。これにより誰がどの電子キャッシュを所有しているかを知ることができて偽造などの犯罪行為が行われたときの追跡が容易になる。

4. ユーザは送られてきた申込完了メッセージの署名を確認する。また、C_{ID} は今後の購入に必要になるので保存しておく。

図2にプロトコルのシーケンス図を示す。

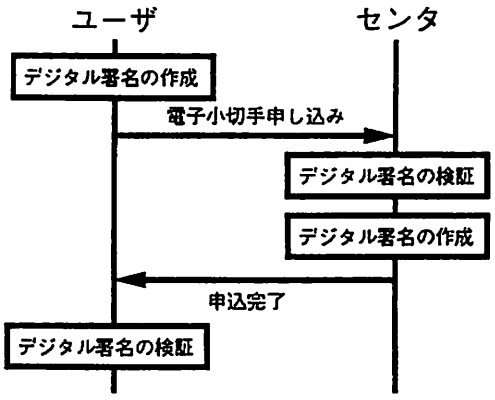

図 2: 電子小切手の申込

3.2.3 商品の購入

申込が完了すれば電子小切手を用いて商品の購入ができるようになる。ここでの「商品」とはソフトウェア、データなどネットワーク上を伝送可能なものとする。また、商品のソフトウェアあるいはデータはあらかじめ暗号化された状態でユーザの端末にダウンロードされており、復号鍵なしでは使用あるいは内容を見ることはできないものとする。商品の暗号、復号には実行速度を考慮して FEAL などの秘密鍵暗号方式 [5] を用いる。

1. 購入を始める前にユーザは自分の電子小切手をセンタからダウンロードする。このとき、センタに送る情報は U_{ID}、パスワードと C_{ID} である。センタは U_{ID} と C_{ID} より電子小切手を検索してユーザに送信する。

2. ユーザは商店に対して購入申込を送る。商店に送るべき情報は U_{ID} と商品 ID および電子小切手である。このメッセージは商店の公開鍵で暗号化しユーザのディジタル署名を付加する。

$$\begin{cases} E_{KP_M}\{Sign_U(h(M)), M\} \\ M = \text{商品}ID, Cash(U_{ID}, C_{ID}, price) \end{cases}$$

3. 商店は購入申込を受け取ったらセンタに転送する。

4. センタは転送された購入申込のディジタル署名を検証する。加えて、送られてきた電子小切手の残高が保存してある値と一致するか、U_{ID} と C_{ID} の組は一致するかを検証する。

5. 問題がなければセンタは商店にトランザクションを承認するメッセージを送る。

6. 商店は復号鍵および署名付きの領収書をユーザに送る。この中にはユーザの電子小切手の更新後の残高が含まれる。

7. ユーザは署名の検証を行い問題がなければ、自分の署名を付加した受領書を商店に送る。

8. 送られてきた復号鍵を用いて暗号化された商品の復号化を行う。復号化完了後、復号鍵は消去する。また、電子小切手の残高を更新する。

9. 商店は受領書をもらったら売上情報の更新を行いセンタに決済要求を送る。受領書はセンタによる決済が終わるまでは保存しておく。

10. 購入を終わらせるときはセンタに電子小切手をアップロードしてから終了する。アップロード後は端末上の電子小切手は消去する。ダウンロードとアップロードの間は電子小切手の残高がなくなるまで何回でも購入を行うことができる。

図3にプロトコルのシーケンス図を示す。

4 セキュリティに関する検討

ネットワークによる課金システムではハッカーによる攻撃や購入者・販売者間のトラブルなどが現金

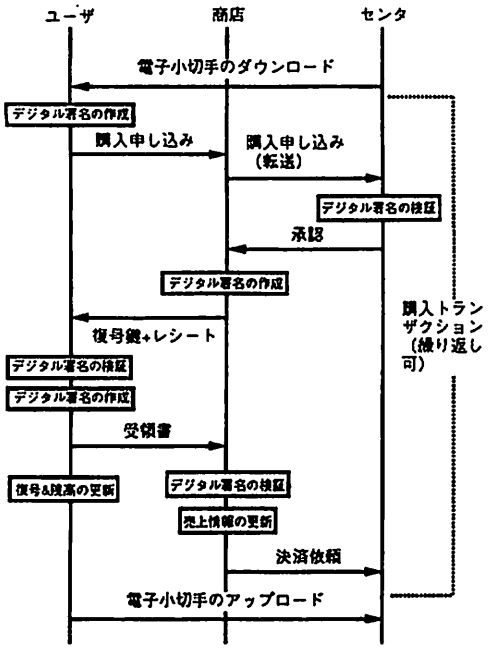

図 3: 商品の購入

による取引と比べて起こりやすいと考えられる。この章ではそのような攻撃、トラブルとしてどのようなものが考えられるかを列挙して、提案プロトコルにおける対処方法について述べる。

4.1 電子小切手および売上情報の偽造

提案するプロトコルでは電子小切手は基本的に信頼できるセンタが保存しておいて、購入トランザクションを起こしている間だけユーザの手元に置くという方法を採用している。商店についても、個々のトランザクションは必ず一旦センタに送って承認を受けなければならず、売上はセンタに報告して決済をしてもらわなければならない。この方式では以下のようにして情報の盗難や改竄を検出することが可能である。

1. 個々のユーザの電子小切手情報と商店の売上情報はすべてセンタに集まるのでセンタでは決済前に双方の情報の収支を計算する。偽造された情報が含まれると必ずこの二つの情報に喰い違いが生じるので、偽造があったことが分かる。

2. 偽造があったことが分かればセンタは商店に対して関連トランザクションのすべての受領書を提出させる。

3. 受領書にはユーザのディジタル署名を付加するので商店が捏造することはできない。そのため、受領書があれば商店が偽造を行い、なければユーザが偽造を行っていることが分かる。

4.2 通信路の傍受

前述のように通信路を流れるメッセージはすべてRSA などの公開鍵方式暗号によって暗号化する。これにより通信路のメッセージが盗聴されても中のデータは読めない。

しかし、たとえメッセージが暗号化されていてもメッセージに規則性[1]があればメッセージを録音することにより「なりすまし」攻撃が可能である。つまり、擬似センタを作って録音メッセージで端末とやりとりすれば復号鍵をコピーしたのと同じ効果が得られる。これを防ぐためには、メッセージの中に乱数を埋め込むなどしてメッセージの規則性をなくしてしまうことが必要である。今回、提案したプロトコルではその機能は含まれていないが、筆者らが過去に提案している Infoket プロトコル [6] などと組み合わせることによって可能である。

4.3 鍵の違法コピー

サービスの種類によっては復号鍵をすぐに消すことができず、一定期間端末に残さなければならない場合も考えられる。しかし、電子小切手と同様に復号鍵の偽造、盗難もやはりソフトウェアだけで完全に防御することは原理的に不可能である。本稿では端末に復号鍵を保存する方法については考慮していない。これに関してはアプリケーションと下位のプロトコルの間に暗号、復号を行うレイヤを設けて復号鍵がそのままの形でメモリ上に現れないようにする方法 [7] や復号鍵に個々のユーザやマシンに依存し

[1]同一人物が同一復号鍵を購入するとメッセージが同じになる

た情報を付加して他のマシンにコピーしても使用できないようにするなどの対処を考える必要がある。

5 実装

提案するプロトコルを実現する課金システムの簡単なプロトタイプをWWW(World Wide Web)を用いて試作した。実装方法は以下の通りである。ただし、今回の試作では公開鍵暗号やディジタル署名の部分など暗号に関わる部分は実装していない。

- センタ
  UNIXマシン(SPARC Station2)上でCGIスクリプトにより実現。
- 商店
  鍵配送部分はセンタと同様にCGIスクリプトによって実現。ただし、暗号化された商品のダウンロードはanonymous FTPを利用することにした。
- ユーザ
  WWWのクライアント。

その結果、提案プロトコルのベースとなる課金機能はWWWを用いると容易に実装できることが確認された。その反面、現状のWWWではユーザの動きを制御することが難しいため、セキュリティ保護の点からはやや不安があることも分かった。今後は専用のブラウザの開発なども検討していく予定である。

6 おわりに

本稿ではネットワーク上で課金を行うための課金プロトコルを提案した。提案プロトコルでは、従来の電子小切手方式にプリペイド課金を併用することにより、高い安全性を保ちながら、より使い勝手を向上させたことが特徴である。また、検討の結果、提案プロトコルでは、電子小切手の偽造など想定されるさまざまな攻撃に対して防御が可能であることが分かった。

今後の課題としては以下のようなことが挙げられる。

- feasibilityの評価
  暗号化を含む実装およびさまざまなサービスへの適用実験を行い、本プロトコルの有効性を評価する。
- 他のセキュリティ通信プロトコルとの融合
  今回提案したプロトコルでは暗号化など最小限のセキュリティ対策は講じてあるが、実際にはより多くの攻撃が考えられる。前述の「なりすまし」攻撃などはその1つである。すでに提案されているプロトコルとの融合を含めて、より安全なプロトコルを作成する予定である。

  また、Internet上でセキュリティ通信を行うプロトコルとしてはSSL [8], S-H'TTP [9]がほぼ標準と考えられ、これらをサポートしたWWWクライアントも米国では提供されている。これらの標準的なプロトコルと提案プロトコルとの共存方法についても検討する必要がある。
- プロトコルの途中中断
  本稿ではメッセージ消失などのプロトコルエラーは発生しないという仮定で議論した。しかし、課金システムは分散システムであるから予期せぬエラーによってプロトコルが途中中断するようなことが起こり得る。特に受領書の送受信が失敗することは偽造の検出にも影響を与えるため、重要な問題である。そのため、プロトコルエラー時の対処について十分なより検討を進めていくことが必要であると思われる。
- 銀行などとの接続
  本稿ではあくまで電子小切手の流通する範囲を対象にした。しかし、提案した課金システムが現実に稼働するためには「銀行」のような決済機関との接続はもっとも重要な課題の1つである。この問題について今後、検討を進めていく。

謝辞

本研究の機会と有益な御助言をいただいたNTTソフトウェア研究所第一プロジェクトチームのみなさまに深謝いたします。また、課金システムの試作

においては東京工業大学の元木光雄君に多大なご尽力をいただきました。重ねて深謝いたします。

参考文献

[1] B. Clifford and G. Medvinsky: "Requirement for Network Payment: The NetCheque Perspective", Technical report, University of Southern California, 1995, ftp: //prospero.isi.edu/ pub/ papers/ security/ netcheque-requirement-compcon95.ps.Z.

[2] David Chaum: "Achieving electoronic privacy", In *Scientific American*, pp. 96–101, 1992.

[3] G. Medvinsy and B. C. Newman: "NetCash: A Design for Practical Electronic Currency on the Internet", In *Proc. of 1st ACM Conf. on Comp. and Comm. Security*, 1993, ftp:// prospero.isi.edu/ pub/ papers/ security/ netcash-cccs93.ps.Z.

[4] Marvin Sirbu and J. D. Tygar: "NetBill: An Internet Commerce System Optimized for Network Delivered Services", In *Proc. of IEEE Compcon'95*, 1995, ftp:// www.ini.cmu.edu/ netbill/ CompCon.html.

[5] 岡本栄司, 「暗号理論入門」 共立出版, 1993.

[6] 金井他: "マルチメディア情報流通システム (InfoKet)", マルチメディア通信と分散処理研究会, Vol. 70-6, pp. 31–37, 1995.

[7] 森保他: "情報流通システムにおける鍵配送通信の構成法", マルチメディア通信と分散処理ワークショップ, 1995.

[8] K. E. B. Hickman: "Secure Socket Library.", *Netscape Communications Corp.*, 1995, http:// home.mcom.com/ newsref/ std/ SSL.html.

[9] C. Neuman and A. Schiffman: "The Secure HyperText Transfer Protocol.", *Enterprise Integration Technologies.*, 1994, http:// www.eit.com/ projects/ s-http/ draft-ietf-wts-shttp-00.txt.