マルチメディア通信と分散処理　90－21
コンピュータセキュリティ　2－21
（１９９８．９．１８）

コンテンツメータリングサーバを用いた課金システム

川副 博
（株）日本アイ・ビー・エム 東京基礎研究所

ＷＥＢのサーバを設置運営し、コンテンツを更新するためには費用が発生するので、インターネットのＷＥＢのコンテンツを販売したいという需要は多い。一コンテンツあたりの価格が安いので、複数コンテンツの購入をまとめて決済し、一コンテンツあたりの決済コストを下げなければならない。各消費者の未決済分の管理を行う必要がある。 この管理を消費者のシステム上で行うと、悪意のある消費者は改竄するであろう。同様に商店のシステム上で行うと悪意のある商店は改竄するであろう。消費者、商店以外の第三者が管理するのが一般的である。 本論文ではＨＴＴＰのトラフィック上で消費者と商店との間に入るサーバによって管理する方法について述べる。

Charging system for contents using metering server

Hiroshi KAWAZOE
Tokyo Research Lab. IBM Japan Ltd.,

There are strong demands for selling WEB contents. WEB contents are so low that multiple purchase should be cleared in once. The prices of purchases should be accumulated. Both malicious buyers and merchants will forge the accumulated value if buyers or merchants accumulate. Thus the third party accumulates. A system in which third server between buyer and merchant is described.

1 はじめに

SET[1]により、インターネットでの「お買い物」は身近なことになってきている[2,3]。WEBのサーバを設置運営し、コンテンツを更新するためには費用が発生するので、インターネットのWEB のコンテンツを販売したいという需要は多い。「物」の販売と「コンテンツ」の販売との違いは、「コンテンツ」の価格が「物」に比べて安いことにある。そのため、SET でのクレジットカード払いに適さない。コンテンツの販売のためには SET 以外の課金、決済の仕組みが必要である。一コンテンツの価格が安いので、一コンテンツあたりの決済コストを下げなければならない。このために、複数のコンテンツの代金をまとめて決済する方法がある。複数の代金をまとめて決済するには、未決済代金の管理を行う必要がある。この管理を消費者のシステム上で行うと、悪意のある消費者は改竄する。同様に商店のシステム上で行うと悪意のある商店は改竄する。従って、消費者、商店以外の第三者が管理しなければならない。

本論文では HTTP のトラフィック上で消費者と商店との間に入るサーバによって管理する方法について述べる。以下、2章で WEB コンテンツ課金の特徴を述べ、3章で課金システムへの要求をまとめ、4章で既存の WEB コンテンツ課金システムを比較する。5章で筆者らのシステムについて述べる。6章で今後の課題をまとめ、7章でまとめを述べる。

2 コンテンツ課金の特徴

2.1 コンテンツは安い

新聞を記事毎にインターネットで販売する場合を例として考える。駅の売店での新聞一紙の値段が１００円程度である。速報性などでの紙の新聞以上の付加価値がない限り、記事毎の価格は１００円以下となる。さもなければ、消費者は新聞を駅の売店で買う。このようにコンテンツは安価であることが多い。インターネットでの「お買い物」で使われる SET での決済は現行のクレジットカード払いである。クレジットカード払いでは、商店は一取り引き毎にクレジットカード会社に取り引き金額に応じて手数料を払っている。このクレジットカード会社へ払う手数料は最低金額が決められていることが多く、日本では７円程度である。 したがって、商店は価格が安いコンテンツをクレジットカード払いで売れない。銀行の口座振り替え、振り込みでも決済のコストは発生するので、クレジットカード決済が問題なのではない。安い金額のための決済方法がないことが問題である。 この問題の解決方法は、複数のコンテンツ代金をまとめ、決済コストに見合う金額にして、決済することである。

決済コストに見合う金額になるまで、未決済金額の蓄積を消費者、または、商店のシステムで行うと未決済金額を消費者、商店が改竄する可能性がある。 改竄を防ぐために、消費者、商店以外の第三者（以下では決済者と呼ぶ。）が蓄積を行う。さらに、商店または、消費者が蓄積をすると、最悪の場合、各消費者は全商店との未決済代金の管理をしなければならない。 同様に各商店は全消費者の未決済代金を管理しなければならない。決済は各消費者、商店の組み合わせ毎に行われるので決済コストは消費者数と商店数との積に比例する。決済者が各消費者の未決済代金、各商店の売上げを蓄積し、消費者はすべての商店の支払い分をまとめて決済者に払い、決済者が全消費者の支払いを商店毎に分配し、商店へ支払うようにすれば、決済者は消費者数と商店数とを合わせた残高記録を管理するだけとなる。 決済コストは消費者数と商店数との和に比例する。

2.2 HTTP と課金プロトコルの連携が必要

コンテンツを運ぶプロトコル HTTP は要求応答型である。消費者（の WEB ブラウザ）からの要求に対して、商店（の WEB サーバ）が応答として、要求されたコンテンツを送る。第三者が関

与しないので、 コンテンツ購入のプロトコルと未決済金額の情報を決済者に送るプロトコルとの連携が必要である。課金プロトコルでは、商店、消費者は自分の得になるように偽った情報を送る可能性があるので、決済者が消費者、商店が互いに了承した金額での購入であることを確認できなければならない。

3 課金システムへの要求

ここでは課金システムへの要求についてまとめる。

3.1 消費者と商店とを認証し、両者が合意した価格であることを確認でき、コンテンツの配送と課金とが不可分であること

悪意のある消費者は購入情報自体を決済者に送らないようにしたり、価格を減じたり、他人のふりをする。 悪意のある商店は実際に購入されていないのに購入されたようなふりをしたり、消費者に示した以上の価格を決済者に報告したり、課金だけを発生させコンテンツを消費者に届けなかったりする。 これらの不正行為を排除するために、決済者は消費者、または、商店から送られた購入情報が偽造されたものでないことを確認でき、消費者、商店を認証できなければならない。消費者、商店どちらか一方からだけ購入情報を得る方式では電子署名などを使って改竄防止を行う必要がある。

3.2 消費者、商店にとって簡単なシステムであること

先払いシステムでは退蔵金を少なくしたいので、消費者はなるだけ多くの商店で使える課金システムを望む。商店は潜在消費者数が多いシステムへ参加したほうが、販売の機会が多くなる。より多くの商店に課金システムが使われるためには、導入コスト、運営コストを低くしなければならない。導入コストは課金のためのサーバ設置や専用ソフトウェアなどにより発生する。 運営コストはコンテンツを更新する時に、コンテンツ更新以外の作業（例えば、決済者への登録など）により発生する。

消費者にとってはコンテンツ購入のための専用ソフトウェアの導入は心理的抵抗になる。 コンテンツ購入時の操作も少なければ少ないほどコンテンツ購入に対する抵抗が少ない。

3.3 ネットワーク障害に対処できること

消費者がコンテンツを受け取っている間にネットワーク障害が発生する可能性がある。この場合、消費者は不完全なコンテンツしか受け取らない。それにもかかわらず、通常通り課金するシステムは消費者に受け入れられない。コンテンツが完全に消費者に渡ったと確認できた場合だけ課金するシステムでは、悪意のある消費者は故意にネットワーク障害を発生させて、コンテンツを部分的にただで得ることができる。ネットワーク障害が実際に発生した場合は、消費者が不利にならないで、かつ、消費者が故意にネットワーク障害を発生させても消費者がコンテンツをただで部分的にも得ることができないようにしなければならない。解決策として、消費者が購入したコンテンツは一定時間は何回でも無料で得ることができるようにする方法がある。 商店、決済者はコンテンツを渡し始めた時点で課金する。実際にネットワーク障害が発生した場合は、消費者は規定時間内での再試行でコンテンツを得る。無料再試行の時間は商店の方針によって違い、同じ商店でもコンテンツの更新の頻度により変わる。よって、無料で再試行できる時間をコンテンツ毎にコンテンツの更新間隔より短い時間に設定するために、コンテンツ毎に無料時間を設定できた方が商店にとってはよい。 決済者、商店は消費者毎に無料で取れるコンテンツの一覧を記録しておかなければならない。 消費者が無料で取れるコンテンツの数に制限がないと記録容量予測が難しくなる。 消費者が「最後に」購入したコンテンツに関してだけ、一定時間は無料で得ることができるようにすると、

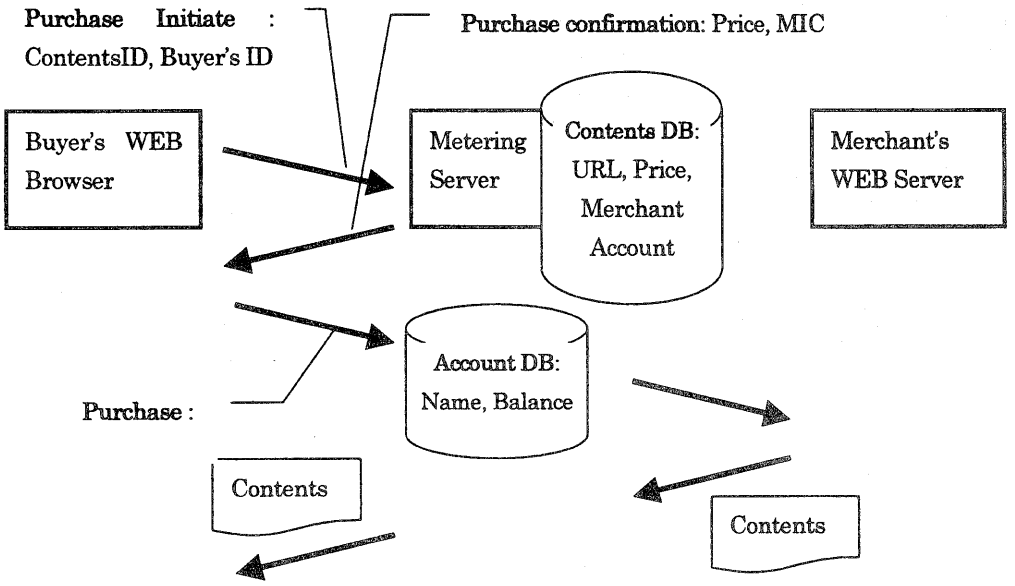

図 1 PayPerClick System

消費者毎に一コンテンツだけを記録するので、記録容量は消費者数から事前に予測できる。

4 既存のコンテンツ課金システム

コンテンツ課金システムには次のようなシステムがある。

BitCash[4]は決済者を使う先払いシステムである。 このシステムでは消費者が商店の WEB サーバで商品購入を選択すると、消費者の WEB ブラウザと決済者の WEB サーバが通信する。決済者が消費者を認証する。決済者は、消費者が価格の確認をすると商店に決済可能を示すデータが渡るような WEB の画面を消費者の WEB ブラウザに送る。消費者が価格の確認をすると、消費者の WEB ブラウザは決済者が作成した決済可能を示すデータを商店へ送る。 商店の WEB サーバでは、決済者が実行可能形式で商店に渡したプログラムが決済可能を示すデータの正当性を確認し、決済者に消費者からの購入要求が来たことを、決済者が作成した決済可能を示すデータとともに送る。決済者は消費者の残高から購入金額を減じ、商店に決済済みであることを通知する。決済済み通知を受け取った商店はコンテンツを消費者に送る。

アコシス[5]は決済者を使う後払いシステムである。このシステムでは消費者が商店の WEB サーバで商品購入をすると、WEB リクエストが商店のサーバ上の決済者が実行可能形式で提供しているプログラムに渡る。このプログラムが商店名、価格の改竄防止データを作り、この改竄防止データ付きの商店名、価格が決済者にわたるような WEB の画面を消費者の WEB ブラウザに返す。消費者が確認ボタンを押すと、改竄防止データ付き商店名、価格が決済者に送られる。 決済者は消費者の認証を行い、消費者の未決済残高を価格分増やす。決済者が与信（決済を行うことの保証）確認したことを示すデータが消費者から商店へ送られるようなＷＥＢの画面を決済者は消費者へ返す。消費者がこの画面の購入ボタンを押すと与信確認したことを示すデータが商店の決済者が提供しているプログラムに送られる。このプログラムが与信確認したことを示すデータの正当性を確認し、商店の WEB サーバにコンテンツを消費者に

送ってよいことを通知する。通知を受けたWEBサーバは消費者へコンテンツを送る。

どちらのシステムも消費者と商店とが納得した取り引きであることを決済者が確認するために、決済者は消費者、商店の両者と通信する。さらに、消費者の認証のために、決済者は消費者と通信する。これらの通信が終わった後に、コンテンツが商店から消費者まで送られるので、購入までのメッセージ数（HTTP 要求、HTTP 応答それぞれを1と数える）は 8 となる。また、商店は決済者が決済を承認したことを確認するための専用のソフトウェアが必要である。コンテンツは最後に商店から消費者へ送られるので悪意のある商店がコンテンツを送らなかった場合、決済者はこれを検知できない。

5 PayPerClick システム

筆者らが開発した PayPerClick システム[6]でのコンテンツの購入過程を図 1 に示す。商店は販売するコンテンツの URL(課金された場合と無料再試行の場合との2種類)と価格とをメータリングサーバに登録し、メータリングサーバよりコンテンツ ID を得る。消費者がそのコンテンツを購入すると、このコンテンツ ID がメータリングサーバへ消費者の WEB ブラウザから決済者へ送られるように商店の WEB のページを構成しておく。消費者が商店の WEB サーバで商品を購入をすると、HTTP 要求がメータリングサーバへ送られる。この HTTP 要求では消費者を識別するための ID、購入しようとしているコンテンツの ID を送る。メータリングサーバはコンテンツ ID をキーとして、コンテンツデータベースを検索し、価格と商店の ID,実際のコンテンツの URL とを得る。その後、消費者の WEB ブラウザに対して、価格を確認するための画面を提示する。この確認画面を消費者が確認すると消費者が購入した時点での登録価格が、決済者に渡るようにしてある。消費者が確認すると、確認したことがメータリングサーバに送られる。メータリングサーバは価格の確認が有効時間内に行われたことと、価格に変化がなかったこととを確認し、商店のサーバへ WEB のリクエストを送る。商店のサーバよりコンテンツを得たら、このコンテンツを消費者に価格確認の返答として送る。同時に消費者、商店の口座をそれぞれ更新する。

本システムでは、決済者が商店と消費者との間に位置するので、購入までのメッセージ数は 6 である。また、商店には決済者が決済を承認したことを確認するための専用ソフトウェアは不要である。決済者は課金と消費者へのコンテンツの受け渡しとを同時に行う。商店がコンテンツを送らなかった場合は消費者に対する課金は発生しない。

5.1 評価

ここでは、本システムが3章で述べた課金システムへの要求を満たしていることを確認する。

- **消費者、商店の認証**

コンテンツメータリングサーバは消費者、商店ともに直接 HTTP での通信を行う。消費者、商店の認証はこの通信で行える。消費者に対しては、SSL[7]でのクライアント認証、HTTP での基本認証で行える。商店に対しては、SSL でのサーバ認証で行える。

- **合意した価格であることの確認**

コンテンツの価格は、商店がメータリングサーバに登録する。消費者がコンテンツを購入するときに、メータリングサーバは消費者に価格を提示し、消費者の確認を得る。悪意のある商店が決済者に登録した価格より低い価格を消費者に提示している場合は、この確認画面で消費者は実際に課金される金額を確認できる。消費者への確認画面とその応答には、その画面を作成したときのコンテンツの価格を含むので、消費者が確認している間に、商店がメータリングサーバへの登録価格を変更したことをメータリングサーバは検出できる。この場合は、その取り引きを不成立とする。

- **課金とコンテンツの受け渡しが不可分である。**

コンテンツは消費者からメータリングサーバを経

由して消費者へ渡るので、メータリングサーバは消費者へコンテンツを送ったのと同時に課金することができる。

- **簡単なシステムであること**

商店はメータリングサーバからの課金する場合のURLに対するHTTP要求はメータリングサーバで課金されることがわかっているので、確認のためのプログラムは必要でない。 メータリングサーバからのHTTP要求であることはSSLクライアント認証で確認できる。

商店は課金された場合と無料再試行の場合で2種類のURLをメータリングサーバへ登録しなければならないが、実際に同じコンテンツを2個持たなくてもよい。WEBサーバが提供するURLのパス変換機能を使えば、実際には一つのコンテンツに対して2種類のURLを持たせられる。

- **ネットワーク障害に対処できること**

コンテンツをメータリングサーバから消費者に送るのと同時に課金するので、課金だけされることはない。 消費者がコンテンツを受け取っている間にネットワーク障害が起こった後、消費者が再試行を行ったことは、メータリングサーバが認識するので課金しない。

6 今後の課題

本システムではメータリングサーバはネットワーク上に一台しかないので、メッセージのボトルネックになる可能性がある。 これは他の既存システムでも同じであるが、本システムはメータリングサーバをコンテンツが流れるので、メータリングサーバ、メータリングサーバが接続しているネットワークの負荷が他システムに比べて高くなりやすいと予想される。 この点を解決するために、ネットワーク上に複数のメータリングサーバが存在するシステムに拡張が必要である。

7 おわりに

本論文ではコンテンツ課金を消費者と商店との中間に位置するメータリングサーバで行うシステムについて述べた。本システムで、コンテンツ課金のための要件を満たすことを示した。さらに、商店と消費者との中間にメータリングサーバが位置するので他のコンテンツ課金システムに比べコンテンツ購入までのメッセージ数が少ないことと課金とコンテンツの受け渡しが不可分であることを示した。今後は複数のメータリングサーバを使うシステムに拡張していきたい。

参考文献

[1] Secure Electronic Transaction, http://www.setco.org/set_specifications.html

[2] 電子商取引に関する意識調査集計結果, http://www.ecom.or.jp/seika/press/980707enquete/index.htm

[3] EMP実証実験レポート, http://www.emp.or.jp/report/index.html

[4] http://www.bitcash.co.jp/

[5] http://www.acosis.com/

[6] http://ppc2.fiesta.or.jp/

[7] A. Freier. P. Karlton, and P. Kocher, "The SSL Protocol Version 3.0", http://home.netscape.com/eng/ssl3/draft302.txt