超流通における課金機構の開発

長谷部 高行　　木島 裕二　　鳥居 直哉
株式会社富士通研究所

概要

本稿では、ソフトウェアの超流通における課金機構の開発に関して報告する。開発した課金機構では、課金モジュールと呼ぶ専用ハードウェアをPCに搭載することにより、ローカルに課金が行える機構を開発した。

開発したシステムは、課金モジュールを搭載したユーザPCとセンタWSがTCP/IPで接続されており。課金の形態としては、買取り、回数課金、期間課金を実現している。

A prototype implementation of charging mechanism for super-distribution

Takayuki HASEBE　　Yuji KIJIMA　　Naoya TORII

ABSTRACT. A prototype implementation of charging mechanism for super-distribution is reported. Super-distribution is the concept that software should be charged on the pay per use basis. We have implemented the super-distribution system for PC software distribution.

The prototype system is consisted of user-PC, center-WS, TCP/IP network, and a special hardware for charging per use, which is equipped in every user-PC. This system enables three types of charging; pay per use, pay per period, and purchase.

1．背景

1983 年に筑波大学の森らにより情報化社会での電子情報の健全な流通をめざした*超流通システム*が提案された[1][2]。提案された超流通システムは、従来のコンテンツ（プログラム・データ等の電子情報）流通とは異なり、コンテンツのコピーを禁止するのではなく、むしろ、コピーを含めてユーザがいつでも・どこでもコンテンツの入手を可能とし、ユーザの利用時にはユーザの利用量に対する課金(従量課金)を行うことにより、情報提供者の利益(確実な料金徴収)とユーザの利便性(入手の容易さ、利用量に応じた課金)を提供するものである。

2．目的

本開発テーマは、超流通の仕組みを提供することを目的としており、具体的には、コンテンツの従量課金を可能にするための、ユーザ側、コンテンツ提供側の仕組みを実現することである

超流通システムを実現するためには、

（1）コンテンツに適した課金手段の提供

（2）コンテンツの不正利用防止
（料金を払わずにコンテンツを利用する）

（3）課金情報の不正書き換えの防止

等の課題を克服する必要がある。

本開発では、これらの課題を解決するような課金機構を、暗号化、署名等の技術を用いて開発した。

3．開発システム

開発した課金機構の概念を図１に示す。課金機構はコンテンツを利用するユーザＰＣ、及び、その利用を許可するセンタにより構成されており、両者間はネットワークで接続されている。センタはコンテンツ提供者からコンテンツの提供を受け、コンテンツ提供者への利用料金の分配を行う。更に、特徴的なこととして、ユーザＰＣには課金モジュールと呼ぶ課金情報を保護するためのハードウェアが接続されている。この課金モジュールは、各家庭に存在

する電気やガス、水道の利用量を計るためのメータに相当するものである。ユーザがコンテンツを利用する場合には、先ず、コンテンツを入手（ＣＤ－ＲＯＭ等の媒体経由でも、ネットワーク経由でも構わない）している必要がある。コンテンツは、課金モジュールがないと利用出来ないような処理（鍵かけ処理）がセンタにて施されており、これを超流通コンテンツ（超流通プログラム、超流通データ）と呼ぶ。これらは、無料または安価に入手することができる。

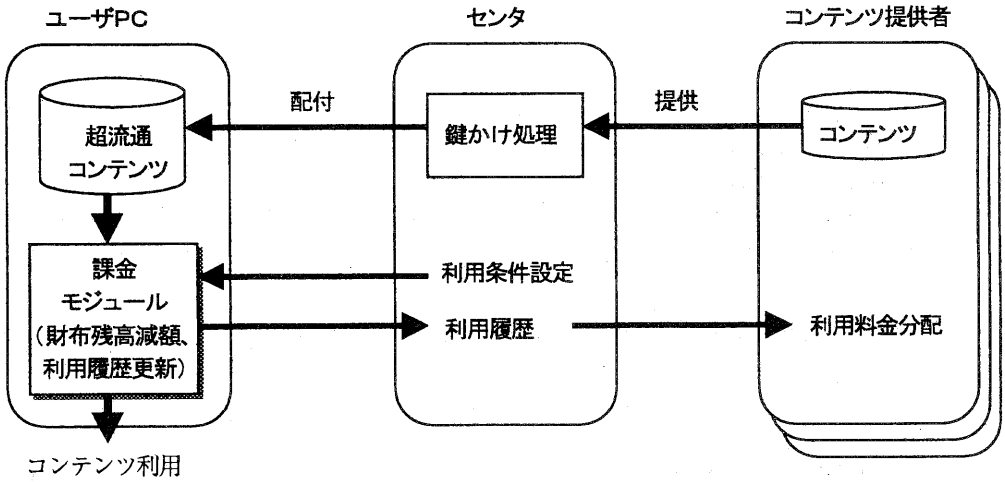

図１　課金機構の概念

超流通コンテンツを利用する場合には、課金モジュールに利用条件が設定されている必要がある。利用条件とは、超流通コンテンツを利用するための鍵、及び、利用可能な金額情報（財布の残高）である。

利用時には、超流通コンテンツは課金モジュールを経由することにより、利用が可能となる。この時に、課金モジュールの中では、財布の残高が減額されるとともに、コンテンツの利用履歴が更新される。

超流通コンテンツの利用価格が、課金モジュール内の財布の残高を上回る場合には、超流通コンテンツは利用できない。これを利用する為には、センタから利用条件の再設定を行ない、財布の残高を増やしてもらう必要がある。この時に、課金モジュールの中でカウントされていた利用履歴がセンタに送られる。

センタでは、利用履歴の情報に基づいて、各々のコンテンツ提供者に利用料金の分配を行う。

こうすることにより、利用の度にセンタに接続することなく、従量課金が可能となる（ローカル課金）。

３．１　課金の単位

超流通コンテンツを利用するための課金単位としては、以下の３種類を実装した。

・回数課金
・期間課金
・買取り

また、

・満期販売

もサポートした。

更に、支払いの方式として、

・一括財布方式
・個別財布方式

をサポートした。

（１）回数課金

超流通コンテンツを１回利用する度に、課金を行う。回数課金の場合には、課金モジュールに利用条件として、回数課金を示す情報、利用単価、及び、コンテンツを利用するための鍵が設定される。

（２）期間課金

超流通コンテンツを一定の期間単位で課金を行う。期間課金の場合には、課金モジュールに利用条件として、期間課金を示す情報、利用期間、利用価格、及び、コンテンツを利用するための鍵が設定される。

期間課金での利用を開始した時に、課金処理が行なわれ、課金モジュール内の時計の現在時刻と利用

期間により、利用期限情報が設定される。これ以降、期限内であればコンテンツ利用に対して課金を行わない。

又、期間が長いような場合には、後述の買取りと同様に、センタ課金でセンタから利用期限の設定をすることも可能である。

（3）買取り

超流通コンテンツを、一回の支払いにより無制限に利用が可能とする。買取りの場合には、課金モジュールに利用条件として買取りを示す情報とコンテンツを利用するための鍵が設定される。

買取りの場合には、課金モジュールの財布は利用せず、センタに直接支払いを行う（センタ課金）。

（4）満期販売

コンテンツの課金単位として従量課金(回数課金、期間課金）を選択している場合に、利用金額が所定の金額を超えた場合には、無償で買取りに変更する機能である。どの時点で満期販売にするかは、センタにより任意に設定が可能である。

（5）一括財布方式

通常は、ローカル課金でコンテンツを利用する場合には一括財布から利用料金が引き落とされ、利用履歴が更新される。

（6）個別財布方式

一部のコンテンツに対して、コンテンツ毎に専用の財布を用意する。

個別財布方式では、残高の補充を行った時点でコンテンツ提供者に利用料金の分配を行う為、利用履歴はとらない。

個別財布は優先的に用いられ、個別財布の残高が無くなった場合には、自動的に一括財布に切り替えられる。

3．2　超流通コンテンツの不正利用防止

超流通コンテンツには超流通プログラムと超流通データの２種類が存在する。

不正利用防止の為の方法は、超流通プログラムと超流通データでは異なっており、各々次のように動作する様に鍵かけ処理が施されている。

（1）超流通プログラム

超流通プログラムが起動されると、先ず認証ルーチンが動作し、課金モジュールとの間で認証処理を行う。認証処理には challenge & Response の暗号化を用いた認証を用いる。超流通プログラム内部で生成した乱数(challenge code)を課金モジュールにてコンテンツ鍵で暗号化し、response code を生成する。課金モジュールは、課金を行った後 response code を送り返す。超流通プログラムは、受け取った response code を確認し、正しい場合にのみ実行にうつる。（図２）

（2）超流通データ

超流通データを利用する場合には、超流通データビューアが必要となる。超流通データ自体は、鍵かけ処理としてコンテンツ鍵で暗号化されている。超流通データを利用する時には、超流通データビューアが、課金モジュールに超流通データを送る。課金モジュールでは課金を行ない、超流通データを復号する。課金モジュールから、復号された平文データを超流通データビューアが受け取ることによりデータが利用可能となる。（図３）

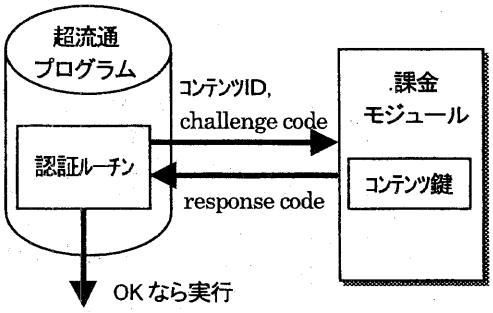

図２　超流通プログラムの構成

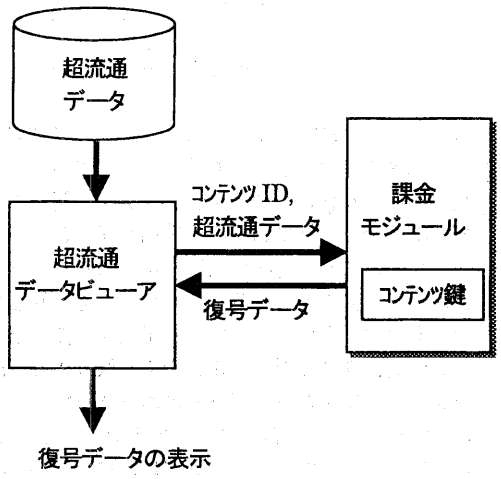

図３ 超流通データの仕組み

3．3　課金情報の不正書き換えの防止

3．3．1　課金モジュール

課金情報は、課金モジュールと呼ぶ専用のハードウェア内部に格納されている。

課金モジュールのハードウェア構成を図4に示す。

課金モジュールは、8ビットのマイクロコントローラ、プログラムROM、DES－LSI、時計（リアルタイムクロック）、課金情報等を格納するための内部メモリ（EEPROM）、及び、インタフェース用のバッファメモリ、レジスタ等で構成されている。それぞれはローカルバスで接続されており、ISAバスとのインタフェースは、バッファメモリ及びインタフェースレジスタを介して行っている。

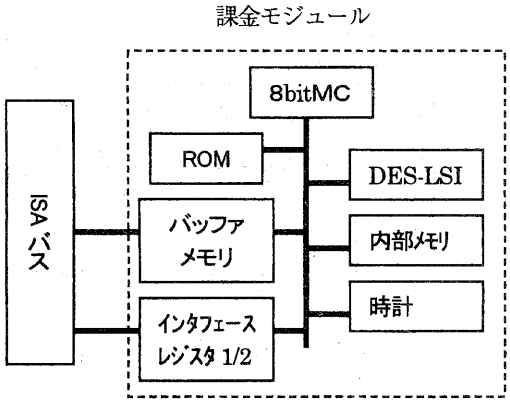

図4　課金モジュールの構成

3．3．2　内部メモリへの不正アクセスの防止

内部メモリが外部から直接アクセス可能ならば、利用条件の不正書き換えや、コンテンツ鍵、モジュール鍵といった鍵情報の不正読出しができる。

これらにより、財布の残高を増やしたり、課金モジュールを介さずに超流通コンテンツを復号したり、センタコマンドの偽造といった不正が可能となる。

この為、課金モジュールとのやり取りには、課金モジュールコマンド／応答の専用フォーマットを用い、内部メモリを直接アクセスできないようにした。ここで、センタからのコマンド以外は、残高を増やすことが出来ないようなアクセス制御を行っている。また、コンテンツ鍵、モジュール鍵といった鍵情報は、センタコマンドでも外部に出さない制御を行っている。

これにより、ファームウェアを改ざんしない限り、重要な鍵情報や利用条件等に外部からアクセスできなくなる。

3．3．3　センタコマンドに対する攻撃の防止

センタから課金モジュールに情報を設定する場合には、ネットワーク経由となる為、設定情報のモニタリングは容易である。センタからの設定情報の解析が可能となれば、課金モジュールへの利用条件等の不正設定やコンテンツ鍵の入手が可能となる。

又、センタからの設定情報の再利用が可能であれば、課金モジュールの財布の残高を増やすなどが可能となる。

この為、本開発システムでは、課金モジュール毎に異なるモジュール鍵を設け、秘密にしたい情報（例えば、コンテンツ鍵）はモジュール鍵で暗号化する。又、センター課金モジュール間の通信で再利用されては困る情報にはモジュール鍵で連番付き署名を付加する。

センタが発行する買取の場合の課金モジュールコマンドの概念的な説明を図5に示す。課金モジュールでは、コマンドを受け取ると、連番と署名の確認を行ない、暗号化コンテンツ鍵を復号し、買取の設定を行った後、連番の値をインクリメントする。

3．3．4　時計の改ざん防止

期間課金を実現する時には信頼できる時計の存在が必要である。

ｺﾏﾝﾄﾞ ID	ｺﾝﾃﾝﾂ ID	利用条件 (買取り)	暗号化 ｺﾝﾃﾝﾂ鍵	連番	署名

暗号化コンテンツ鍵：モジュール鍵で暗号化
署名:ｺﾏﾝﾄﾞ IDから連番までを、DES-MACを用いて署名作成

図5　課金モジュールコマンドの概念説明
（コンテンツ買取りの場合）

パソコンに搭載されている時計を用いて期間課金を実現した場合には、時計を遅らせることにより、期間が過ぎていても利用可能とすることができる。

本開発システムでは、ユーザが変更不可能な時計を確保する為に、課金モジュール内に時計（リアルタイムクロックーＬＳＩ）を実装した。

この時計の校正はセンタから行う。

4．まとめ

超流通におけるコンテンツ流通のための課金機構を開発した。開発した課金機構は、課金モジュールと呼ぶハードウェアを信頼点とした課金機構であり、
回数をベースとした従量課金、期間をベースとした従量課金を実現している。

本開発システムでは、ローカル課金を行うため、お金に係わる情報のセキュリティが問題である。開発した課金機構では以下の対策を行った。

○課金モジュールは専用のコマンドのみを受け付ける構成とし、内部情報の不正読出しや書き換へを出来なくした。

○センタから課金モジュールに送るコマンドに含まれる情報の内、秘匿したいもの（コンテンツの鍵）や再利用されては困るもの（財布の補充情報等の）は、モジュール鍵を用いた暗号化や連番付き署名により保護した。

[謝辞]

本開発は、情報処理振興事業協会(IPA)殿の創造的ソフトウェア育成事業の一環として開発を行なった成果です。

[参考文献]

[1]森,田代, "ソフトウェア・サービス・システム(SSS)　の提案", 電子通信学会論文誌, Vol.J70-D, No.1, pp.70-81 (1987).

[2](社)日本電子業振興協会"マイクロコンピュータに関する調査報告書[III]ソフトウェア技術", 91-パ-3 (平成3/3).