2003－CSEC－21 (8)
2003／5／15

コンテンツ再生と不可分な課金演算処理によるクライアント上での課金方式の実装

青野博[†] 星野玲子[†] 本郷節之[†] 鈴木雅貴[‡] 赤井健一郎[‡] 松本 勉[‡]

あらまし：近年のモバイル E コマースにおいて多くのコンテンツダウンロードサービスが行なわれている．しかし，コンテンツダウンロードサービスには，不正コピーの問題がある．そのため，それを解決する手段として，ダウンロードした端末からコンテンツを取出せないようにするなど，ユーザの利便性を損なうようなシステムとなっていることが多い．本稿では，コンテンツの再配布を可能にしつつ，そのコンテンツの使用に対する課金も可能にするために，コンテンツ再生と課金処理が同時に行なわれるような方式を提案し，その実装について報告する．

An Implementation of the Charging system on the client by inseparable processing of content replay and charging

Hiroshi Aono[†] Reiko Hoshino[†] Sadayuki Hongo[†]
Masataka Suzuki[‡] Kenichiro Akai[‡] Tsutomu Matsumoto[‡]

Abstract: Recently, the contents downloading service is one of the major services of mobile E-commerce. But this service has the problem of the illegal copy substantially so that most of the systems that implement this service in order not to take out contents data from terminal. This implementation will spoil the user convenience. It is necessary that the system enables the user to transfer contents data freely and enables the contents provider to charge the user for using the contents. In this paper we propose the charging system on the client by inseparable processing of content replay and charging, and describe an implementation of it.

1. はじめに

近年のモバイル E コマースの利用状況は[2]にあるように，有料情報や音楽ダウンロードサービスが主流となっており，また今後の期待も大きい．しかし，音楽に限らずコンテンツのダウンロードサービスには不正コピーの問題があるため，その実装においては，複製防止機能などを実装したシステムが主になっている．これにより，端末間でコンテンツの移動に手間がかかるなど，ユーザは不利益を受ける場合がある．しかし，自由なコンテンツの流通を可能にすると，コンテンツプロバイダ(以下 CP)が，コンテンツ利用の対価を徴収しにくくなる．筆者らは[1]において，コンテンツの再配布を可能にしつつ，コンテンツ利用の対価を回収するために，コンテンツ再生と不可分な課金演算処理を行うことによりクラインと上で課金を行なう方式について提案を行なった．本稿では，その課金方式の実装について報告する．

2. コンテンツ流通方法と課金方法

従来のコンテンツに対する流通方式，課金方式は様々である．しかし，それらは CP 側で管理されていて，エンドユーザは CP ごとに契約し，CP ごとに料金を支払わなければならなかった．

[†] 株式会社 NTT ドコモ マルチメディア研究所
NTT DoCoMo, Inc. Multimedia Laboratories
[‡] 横浜国立大学 大学院 環境情報学府/環境情報研究院
Graduate School of Environment and Information Sciences, Yokohama National University

また，コンテンツの流通方式としては，主に以下の３種類の手法が知られている．①コピー自体許されていないコピープロテクト型[3]，②コピーにコピー回数，端末に制限があるコピー制限型[4]，そして③超流通型[5]である．また，それ以外に④ソフト電池と呼ばれる方式[6][7]がある．①，②については，端末固有の情報を利用して使用を制限しているために自由なコンテンツ流通が不可能である．③については，使用記録には必ず個人を特定する情報が必要なため，プライバシの侵害になる可能性がある．④については，ソフトウェアの使用時にクライアント上で課金することが可能である．具体的には，ソフトウェアを利用するたびに，ソフト電池マネージャがソフト電池と呼ばれるプリペイドマネーの購入金額のようなバリューを減算し，それが 0 になるまで利用でき，0 になった場合は再チャージが可能である．また，ソフト電池は可搬性があり他の端末でも利用することができるが，インターネット上に接続してソフト電池管理サーバを介する必要がある．

これら従来の方式では，CP ごとの課金方式にあわせてコンテンツ利用の対価を支払う必要性，自由なコンテンツの流通が困難といった問題があった．コンテンツと同時に課金方法を流通させ，クライアント上でコンテンツ利用の対価を課金することができれば，自由にコンテンツを流通しても CP はその対価を徴収することができる．また，ある枠組みにしたがって，課金方式をコンテンツに組込むことでエンドユーザは，各 CP の課金方法を意識する必要がない．この場合コンテンツ再生ソフトウェアの耐タンパー性が重要になってくるが，従来の耐タンパーソフトウェア技術だけでは，十分とはいえない．そこで，本研究では，コンテンツ再生と不可分に課金処理を行う方式を提案した[1]．本稿では，その実現性の確認と評価のために，音楽コンテンツの流通を題材にした実装について述べる．

3. コンテンツ再生と不可分な演算処理のよるクライアント上での課金方式

3.1. サービス要件

クライアント上でコンテンツ再生と課金処理を同時に行うことにより，CP はコンテンツの対価を徴収することができ，エンドユーザは CP ごとに支払を行い利用するわずらわしさが無くなり，また自由にそのコンテンツを流通することができる．

このようなサービスが成り立つためのサービス要件は大きく分けて CP とエンドユーザの側面からの要件がある．以下にそれぞれの側面からの要件を示す．

(1)CP 側の要件

- コンテンツを再生するならば，課金処理を実行する必要がある
- 課金の設定はコンテンツ単位で変更可能である
- コンテンツが利用された分の料金が徴収できる

(2)エンドユーザ側の要件

- 課金処理を実行するならば，コンテンツを再生する必要がある
- コンテンツはコピーすることにより，どのエンドユーザのどの端末でも利用できる
- 再生時の CP 等との通信処理は不要

3.2. システムの基本構成

本課金方式は，CP，料金代行徴収者，エンドユーザからなる．CP は，コンテンツデータ(M)の作成を行いそれに対する対価を徴収するための課金ロジック(P)と M を暗号化した M′と組み合わせて専用コンテンツデータ(data)とする．エンドユーザのクライアントソフトウェアでは，ダウンロードされ data に対する再生と使用料金の計算が同時に行なわれ，料金代行徴収者に M の使用料金を支払う．料金代行徴収者は，エンドユーザからの M に対する視聴情報を収集しそれを基に，各 CP にその売り上げを配分する．

支払方法としては，利用時に CP や料金代行徴収者との通信を行なわないために，使用料はプリペイドまたはポストペイで支払うことが考えられる．ポストペイの場合は，確実に支払を行なわせる方法についての検討が必要であるため，本実装においては，プリペイド方式で検討を行なった．プリペイドマネーおよび視聴情報は，data がどの端末でも利用可能にするという要件からオフライン状態での可搬性を持たせるためおよび，それらの不正利用を防ぐために耐タンパー装置である IC カードに蓄積することとした．

以上を踏まえたシステムの基本構成を図１に示す．以下の章で図１の(a)から(d)の詳細に

ついての検討について述べる.

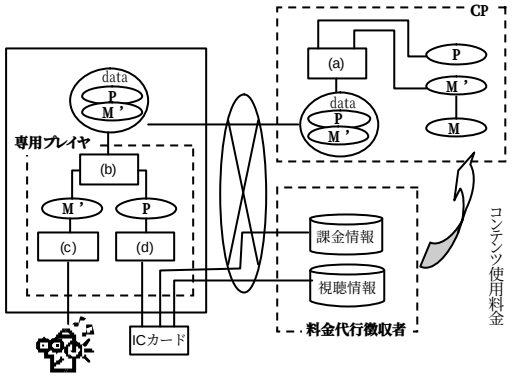

図１．システムの基本構成

3.3. 攻撃シナリオ

図１に示す基本構成に対しての攻撃のシナリオについて検討する. 攻撃者が持つ能力を以下とする.

- 専用プレイヤのモジュール間のデータ入出力を見ることができる
- 専用プレイヤのモジュール間のデータ入出力を改変することができる
- 専用プレイヤのモジュール内のデータを見ることができる
- 専用プレイヤのモジュール内のデータを改変することができる
- 専用プレイヤのモジュール内の内部処理を改変することができる
- IC カードに直接アクセスすることができる

攻撃者がこれらの能力を持っているとき, 前節で述べたサービス要件を脅かす場合を以下に示す.

⑴ 正しく課金を行なわないように P を書き換える.
⑵ M'を M に復号する鍵を盗聴, 記録することにより再生を行なう(data から M の抜き出し).
⑶ M を再生したアナログデータを蓄積し，コンテンツの再配布を行なう.
⑷ data を実行しないで，IC カードを直接操作し，プリペイドマネーまたは課金情報を改竄する.
⑸ data を実行するが，IC カードに正しい結果を出力しない.
⑹ IC カード内で課金処理を行わずに，IC カードの出力を IC カードと専用プレイヤ間で改変し，再生を行なう.
⑺ IC カードと課金代行徴収者間のインタラクションの傍受・偽造する.

3.4. 本システムの構成

本節では, 前節で示した脅威に対して対策を行なったシステムの構成について述べる. 本稿においては, 専用プレイヤは耐タンパーソフトウェアとして構成し，IC カードは耐タンパーハードウェアであることを前提とした. また, 出力されたアナログデータを保存される攻撃については，今回は考慮しない.

図２が要件を満たし, 攻撃に耐性のあるプレイヤ構成図である. 構成要素は以下のようになっている.

A) 専用コンテンツデータ(data)：M の取り出しを防止するため, M を暗号化した M'と P が不可分で一体化となったもの.
B) 署名検証モジュール(Verifier)：data が正しいサーバから配信されたものか，改竄されていないかの検証を行なう. M'や P が改ざんされることを防ぐための必要な機能である.
C) 分割モジュール(Splitter) ：data を M'と P に分割する.
D) IC カード：ここで P が実行され, 課金処理と M'を復号するための鍵(k)を生成する. 課金処理と鍵生成を IC カード内で行なうことにより, コンテンツ再生に IC カード内での計算結果が必要となり, IC カードの出力の偽造を防止する.
E) コンテンツ再生モジュール(Decoder) ：k で M'を復号する Decrypt 部と，M を再生する Decode 部からなる.
F) 制御モジュール(Manager) ：P を IC カードに送り，IC カードから得られた k を Decoder に渡す. IC カード上で P が正しく実行されているかを監視，そうでないときには再生を中止，また M'の復号が正しく行われない場合は課金を行わない制御を行う.

エンドユーザは data を利用する前に，専用プレイヤをダウンロードし, 個人情報とプリペイドマネーの情報を格納する IC カードを用意する．この IC カードを移動することで，端末を変えても同じプリペイドマネーを使うことが可能である．また，エンドユーザは data を CP サーバからダウンロード，または他のエンドユーザからコピーすることにより入手する．エンドユーザが M の再生を専用プレイヤに指

示すると，専用プレイヤは M を再生すると同時に P が実行し，IC カードに格納されているプリペイドマネーから M を再生した分の使用料を差し引く．これによって課金が行われる．また，視聴情報の送信は，プリペイドマネーチャージ時等任意のタイミングで行なわれるものとする．このとき，課金サーバでは視聴情報と個人情報を対応させる必要は無く，どの data がどのぐらい再生されたかを収集することにより，CP に対する料金の分配を行なう．

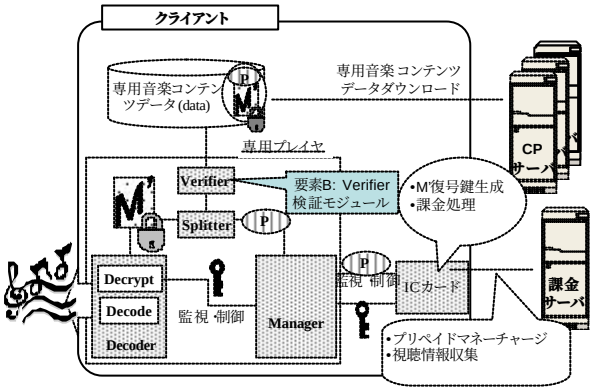

図２プレイヤ構成

3.5. data の構成

コンテンツデータは CP サーバにおいて専用コンテンツデータ(data)に変換し，専用プレイヤで再生される．本方式における専用コンテンツデータの構造を図 3 に示す．

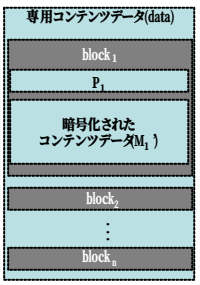

図 3 data の構成

専用コンテンツデータは n 個の block に分かれている（専用コンテンツデータ={$block_1$, $block_2$, … , $block_n$}）．それぞれの $block_i$(i=1, …, n)は課金の最小単位に相当し，その単位の課金情報を示す課金ロジック(P)と課金単位分のコンテンツのデータである M_i'からなる（$block_i$={P_i,M_i'}）．

専用プレイヤで専用コンテンツデータを再生するとき，プレイヤでは data の課金単位の $block_i$ 毎に処理される．

3.6. 専用プレイヤでの再生手順

専用プレイヤでの再生手順は図 4 のようになっている．

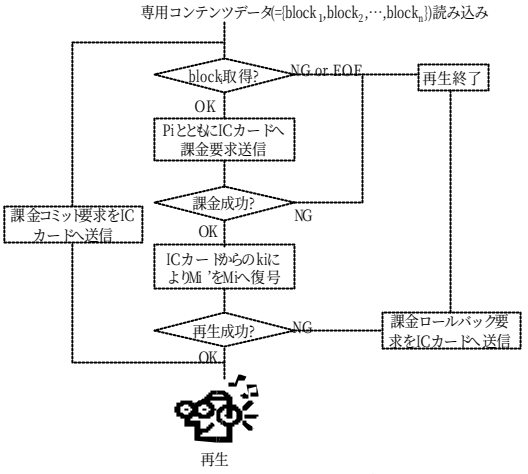

図 4 再生手順

まず，data を読み込み，課金単位の i 番目の $block_i$ を取得する．取得できなければ（EOF 含む），再生を終了する．$block_i$ を取得後，P_i と M_i'に分割し P_i と伴に課金要求を IC カードに送信し，IC カードで課金処理を実行する．IC カード内では，課金処理が実行できない場合(プリペイドマネー不足)，課金処理を行わずに NG を専用プレイヤに返す．課金可能な場合は M_i'の復号のための鍵 k_i を生成し，専用プレイヤに返す．k_i を受取った専用プレイヤは k_i を Decoder に送り，M_i'を復号しデコード処理を行う．正しく再生できない場合は，課金処理ロールバックを IC カードに送信し再生を終了し，正しく再生でき場合は課金コミットを IC カードに送信し再生を行なう．これを EOF まで繰り返す．

4. 実装と評価

前章で述べた課金方式の実装について述べる．今回の実装では，対象とするコンテンツデータを MP3 形式の音楽データとし，既存の MP3 プレイヤ(Zinf[8])に手を入れることで実装を行なった．以下に具体的な再生手順およびデータの構成について述べる．

4.1. データ構成詳細

専用の MP3 形式のデータを構成するに当たり以下の条件の下に検討を行なった

- data は MP3 ファイルと同様の形式である

こと.
- 一般のMP3プレイヤで再生しても正しい音楽が再生されないこと
- 音楽コンテンツデータは暗号化されていること.
- コンテンツごとに，電子署名を付し，正当なコンテンツサーバのコンテンツであることが検証できること.
- 課金単位のコンテンツデータごとに，課金ロジックの設定ができ，課金額のフレームが正しく復号できたことが検証できること.

これらの条件を満たすために，data を以下のような手順で作成する.

(I) 課金単位分の MP3 フレームデータを暗号化したデータ(M_i')とそれに対する課金ロジックと暗号化前のデータ(M_i)に対する MAC(MAC_i)を合わせて 1 つの block のデータ($block_i$)とする.

(II) 上記データは MP3 形式のオーディオデータのメインデータ部に分割して格納する

(III)ヘッダ部(ID3v2 タグ)に，CP が付し電子署名を格納するタグを追加.

(IV)コンテンツには，専用プレイヤの公開鍵で暗号化した CP と IC カード間で共有する秘密情報を含む

4.2. 再生手順

専用プレイヤと IC カード間の具体的な再生手順を図 5 に示す.

(i) IC カードは PIN によるユーザ認証を行い，専用プレイヤと IC カード間のセッション鍵(k)の交換を行なう.

(ii) 課金要求として，P_i および一つ前の課金単位の復号鍵(k_{i-1})と復号後のコンテンツデータのハッシュ値($hash_{i-1}$)を k で暗号化し IC カードに送る.

(iii) IC カードでは，課金処理および復号鍵の生成が行われ，復号鍵を k で暗号化して専用プレイヤに送る．ここで，復号鍵 k_i の生成は，k_{i-1} および $hash_{i-1}$ を利用して鍵生成を行なう.

(iv) コンテンツデータを復号し，$block_i$ のデータに含まれる MAC_i を検証し，正しければ IC カードに課金コミット要求を送信し，音楽を再生する．検証失敗の場合には，IC カードに課金ロールバックの要求を送信し，再生を中断する.

(v) IC カードでは，課金コミットを受取れば，実際にプリペイドマネーから再生した分の使用料を差し引く.

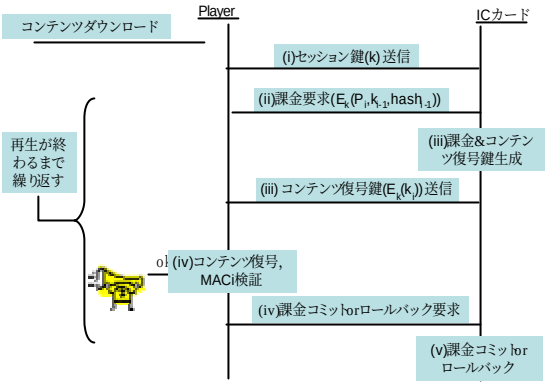

図 5 具体的再生手順

4.3. 実装結果

実装環境を表 1 に示す.

表 1 実装環境

(1)CP サーバ，課金サーバ

CPU	Pentium4 2.8G
Memory	2GB
OS	RedHat Linux 7.3
その他環境	Openssl0.9.6b-28, postgreSQL7.2.1-5, Apache1.3.23-14, tomcat3.3.3.1-4

(2)クライアント

CPU	Pentium3 866MHz
Memory	512MB
OS	WindowsXP,2000
専用プレイヤ	Zinf を変更
IC カード	SchlumbergerSema 社 CyberFlexAccess (JavaCard 2.1

実装を行なった結果，音飛び等の問題無く再生し，課金処理も行われていることが確認できた．3 秒毎の課金までは音飛びすることなく再生および課金処理することができる．また，5 秒毎に課金をすることで，約 1 割程度データサイズが大きくなった.

4.4. 攻撃シナリオに対す評価

今回の実装に関して，3.3 節で述べた攻撃シナリオに対する対策についての分析を行なう.

(1) 正しく課金を行なわないように P を書き換える.
→構成要素 A に CP の署名が含まれており，構成要素 B でそれを検証することにより，

data 内の P が改ざんされることを防いでいる.

(2) M'を M に復号する鍵を盗聴，記録することにより再生を行なう(data から M の抜き出し).
→専用プレイヤと IC カード間の通信をセッション鍵で暗号化することにより鍵の漏洩を防ぐ.

(3) M を再生したアナログデータを蓄積しコンテンツの再配布を行なう
→アナログデータに対する攻撃は対象外とする.

(4) data を実行しないで，IC カードを直接操作し，プリペイドマネーまたは課金情報を改竄する.
→構成要素 F における再生手順により，音楽データが正しく復号されない限りは，課金処理は完了しない．また，IC カードの耐タンパー性は信頼しており，IC カード内のデータを書き換えることはできないものとする.

(5) data を実行するが，IC カードに正しい結果を出力しない
→構成要素 A により課金ロジックが改ざんされることを防いでいる．また，コンテンツの再生をおこなうときには，IC カードへのアクセスのためにエンドユーザは PIN コードを入力する必要があり，正規のユーザ以外が IC カードにアクセスすることはできない.

(6) IC カード内で課金処理を行わずに，IC カードの出力の偽造を行い，再生を行なう.
→IC カード内の処理を課金のみにせずに，k_i の生成を IC カード内で行なうことにより，IC カードの出力が改変された場合には，復号が正しく行なわれないため，本攻撃に耐性がある.

(7) IC カードと課金サーバ間のインタラクションの傍受・偽造
→SSL サーバ認証を行なうことで対処.
プリペイドマネーチャージ時には，エンドユーザの ID，パスワードの認証を行なう.
課金サーバと IC カード間の end-to-end の認証は行なえていない.

5. まとめ

本稿では，CP ごとの課金方法に合わせて支払いを行なうのではなく，クライアント上で課金処理することにより，コンテンツを自由に再配布可能にするために，コンテンツ再生と不可分な形で課金演算処理を行う課金方式について実装について報告した．本実装により，コンテンツ再生と課金演算処理を不可分な形で実行し，正しく再生および課金ができることが確認できた.

今回は，専用プレイヤは耐タンパーソフトウェアであることを前提に実装を行なった．今後は，専用プレイヤ単体の耐タンパー性を前提とするのではなく，IC カードや専用プレイヤやサーバなどが連携することによりシステム全体として耐タンパー性を持たせる方式について検討を行なっていく.

文　献

[1] 星野他:"クライアント上での安全な課金方式とその応用"，情報処理学会第 65 回全国大会 pp. 4-323

[2] "モバイルインターネットの利用実体と今後の利用意向"，H13 ECOM モバイル EC-WG 報告書

[3] マイクロソフト　プロダクトアクティベーション
http://www.microsoft.com/japan/windowsxp/pro/techinfo/productactivation.asp

[4] 稲村勝樹，田中俊昭，中尾康二，"デジタルコンテンツにおける不正コピー防止方式の提案，"暗号と情報セキュリティシンポジウム，Jan.26-29.2003.

[5] 森亮一，河原正治，大瀧保弘，"超流通：知的財産権処理のための電子技術，"情報処理，Vol.37, No.2， pp.155-161， Feb.1996.

[6] 菅野和裕：稼動管理システム及び稼動管理方法，特許平成 10-83298 (日本)，(1998)

[7] 高田秀典：情報管理装置，情報管理システム，及び情報管理ソフトウェアを記憶した媒体，特許 2001-249730 (日本)，(2001)

[8] Zinf:http://www.zinf.org