クライアント上での安全な課金方式とその応用

星野　玲子† 青野　博† 本郷　節之†
鈴木　雅貴‡ 赤井　健一郎‡ 松本　勉‡
NTT ドコモ　マルチメディア研究所†
横浜国立大学　大学院　環境情報学府/環境情報研究院‡

1. はじめに

本研究は，サービスプロバイダ(xSP)ごとに異なる課金方法（課金額，単位など）に対して各々に支払うのではなく，それぞれの xSP の課金方法に従ってクライアント上で安全に課金処理を行うことを目的とする．この安全とは，xSP と利用者の双方にとって課金が正しく実行されるということである．

本稿では，クライアントでの安全な課金方式として課金額，単位などを示す課金ロジックとサービス提供 AP が不可分でかつ同時進行性を持つ方式を提案する．

その実現性を確認するため，筆者らは提案方式を音楽コンテンツ流通へ応用し，課金ロジックと音楽コンテンツデータ(M)が不可分な状態で配信され，M を利用した時には必ず課金処理が同時に実行されるシステムを構築した．本報告ではこのシステムの設計方針について述べる．

2. 従来の課金方式の課題

従来のサービスに対する課金方式は固定課金，従量課金など様々である．しかし，それらはxSP側で管理されていて，利用者はxSPごとに契約し，xSPごとに料金を支払わなければならなかった．

また，サービスのためのAPや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コピーに制限があるコピープロテクト型[1]，②コピー自体許されていないコピープロテクト型[2]，そして③超流通型[3]である．

課金方式としては，①，②のように入手時に課金するもの，③のように使用前後に課金するものがある．従来方式では，利用と課金は同時には行われていない．このため，利用者は利用しないかもしれないのに支払わなければならない場合や，xSPは料金を取り損なう恐れがある場合があった．

3. クライアントによる安全な課金方式

従来方式における課題を解決するため，本方式では xSP ごとに異なる課金方法に対して各々に支払うのではなく，それぞれの xSP の課金方法に従ってクライアント上で課金処理を行う．

図１は本方法の概念図である．まず，xSP サーバでサービス提供 AP と課金ロジック(P)が一体で不可分なものに変換する．クライアント側で，サービス提供 AP と P は同時に実行され，課金処理は IC カードのような耐タンパーハードウェア上で行う．

今回，サービスの一例として音楽コンテンツ流通に対応した提案を行う．

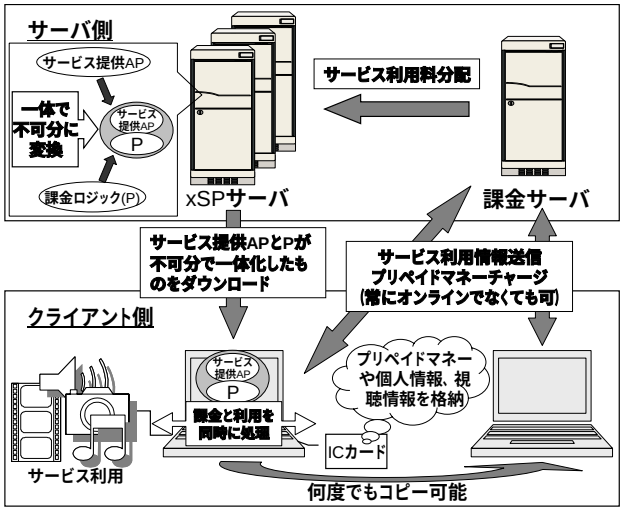

図 1 本方式概念図

4. 音楽コンテンツ流通への応用

本方式では，利用者は P と M が一体で不可分となった専用音楽コンテンツデータ(data)をコンテンツプロバイダ(CP)サーバからダウンロードすることや利用者間の直接配布によって入手できる．また，課金処理を行うモジュールをプレイヤとは独立に持ち回ることで，複数のプレイヤでコンテンツ利用可能である．M を再生するには，同時に P を実行し生成される鍵を必要とする．このため，M の再生には P を実行する必要があるため，安全な課金が可能となる．

5. 本方式を実現するための要件と提案モデル

5.1. 本方式を実現するための要件

要件は CP 側からのものと利用者の側からのものの２つに大きく分けられる．以下の要件を満たすことにより，安全な課金方式が実現できる．

5.1.1. CP 側の要件

CP からの要件は以下のようになる．

① M を再生するならば，P を実行する必要がある
② P の設定はコンテンツ単位で変更可能である

The secure charging model on the client, and its application
Reiko Hoshino† ,Hiroshi Aono† ,Sadayuki Hongo†
Masataka Suzuki‡ ,Kenichiro Akai‡ , Tsutomu Matsumoto‡
† Multimedia Laboratories, NTT DoCoMo, Inc.
‡Graduate School of Environment and Information Sciences, Yokohama National University

③ 以下の処理を正しく行う
- プリペイドマネーチャージ
- 課金情報と視聴情報収集

5.1.2. 利用者側の要件

利用者からの要件は以下のようになる.

① P を実行するならば，M を再生する必要がある
② data はコピーにより，どの利用者のどの端末でも利用できる
③ 再生時の CP サーバとの通信処理は不要

5.2. 提案モデル

仮定している環境としては，専用プレイヤは耐タンパーソフトウェアであり，IC カードは耐タンパーハードウェアである．よって，それらは解析できないものとし，したがって改ざんできない．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．CP の不正については，data に対する署名によって CP を特定できるため抑止できる.

利用者は 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が格納された IC カードを用意する.

図２のように，利用者は CP サーバからダウンロード，または他の利用者からコピーにより data を入手する．利用者が M を再生すると同時に P が実行され，IC カードに格納されたプリペイドマネーから M を再生した分だけ使用料を払うことによって課金が行われる．また，課金情報や視聴情報の送信は，プリペイドマネーチャージ時に行われる.

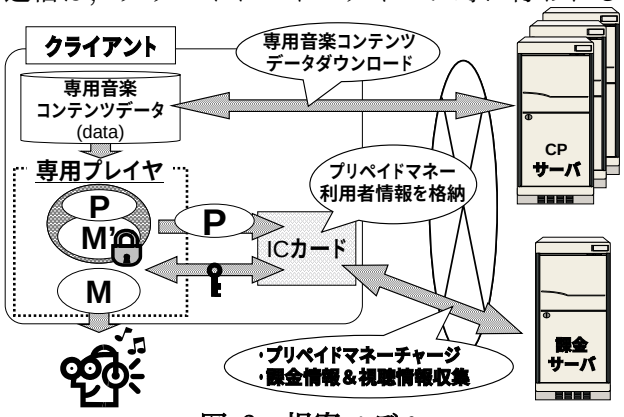

図 2　提案モデル

6. 要件を満たすプレイヤ構成

図３が要件を満たす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) data：モジュール間またはモジュール内の M の取り出しを防止するため暗号化された音楽コンテンツ(M')と P が不可分で一体化したもの
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検証する
C) 分割モジュール(Splitter) ：data を M'と P に分割する
D) IC カード：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
E) コンテンツ再生モジュール(Decoder) ：k で M'を復号し，M を再生する
F) 制御モジュール(Manager) ：P を IC カードに，また 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

要件	要件を満たすためのメカニズム
CP①	構成要素 A～F によって実現している
CP②	構成要素 A，F によって実現している
CP③	構成要素 D により情報改ざんから守られており，通信には SSL を行い，ユーザ認証を行うことによって実現している
利用者①	構成要素 A～F によって実現している
利用者②	構成要素 A によって実現している
利用者③	構成要素 D，F によって実現している

表 1　要件とそれを満たすためのメカニズムの対応

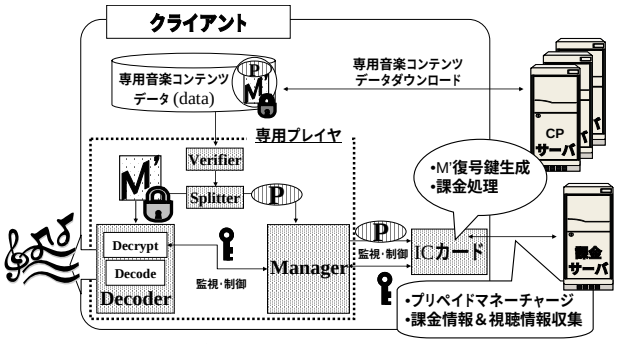

図 3　要件を満たすプレイヤ構成図

7. まとめと今後の課題

今回は，クライアントでの安全な課金方式として，課金ロジックとサービス提供 AP が不可分でかつ同時進行性を持つ新しい方式を提案した.

また，その実現性を確認するため，音楽コンテンツ流通へ応用し，課金ロジックと音楽コンテンツデータが不可分な状態で配信され，その専用音楽コンテンツデータを利用した時には必ず同時に課金処理が実行されるシステムの設計方針について報告した.

今後は，今回提案したシステムの実行性について検証を行う．また，音楽コンテンツ流通以外のサービス AP に対応するシステムについても検討する.

参考文献

[1] 稲村勝樹,田中俊昭,中尾康二,清本晋作，“ユーザ端末を限定しない著作権保護方式の提案，” 電子情報通信学会情報セキュリティ研究会，Sep.2002.
[2] 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
[3] 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.