

4U-8

柔軟な条件設定を可能とする Pay per View 用 端末アーキテクチャ[†]

森保 健治[‡]NTT ソフトウェア研究所[§]

1 はじめに

今日の PC の急速な普及は、マルチメディアコンテンツを生み出すオーサリングツールの高度化やインターネットの発達に大きく起因するところであるが、これにより、今後は有料のデジタル情報を特にオンラインで扱う市場が拡大していくことが予想される。

市場が成長していく過程では、現実の世界をそのままに、各商店間での顧客獲得の競争が始まるため、他店との差別化を図ることが重要になってくる。差別化には、サービスのパーソナライズ化や支払手段の多様化などが考えられるが、個々のデジタル情報の課金方式そのものを多様化することも有効である。

デジタル情報の課金方式は大きく分けて2つあると考えられる。つまり、従来のカタログ販売の延長である売切り型 (Pay per Copy) と、回数、時間、機能などの単位の応じた利用権販売型 (Pay per View) である。Pay per View では、ユーザは選択した単位分のみの対価を支払えばいいことになるため、より安価に必要な商品を得ることができる。

本報告では、インターネットのような帯域の狭いオープンネットワーク上でのデジタル情報のオンライン販売に対して、後者の課金方式を実現するために、多様な条件 (利用単位等) を統一的に柔軟に設定できる端末アーキテクチャについての検討結果を示す。

2 Pay per View と実現に必要な機能

Pay per View とは、情報提供者により予め設定された条件下での、ユーザの利用に応じた代金を設定するタイプの課金方式である。実際の利用に対する代金徴収を遠隔で行なうため、ネットワークを用いることが最も有効に機能する課金方式といえる。Pay per View には、利用条件の設定法に以下のようなバリエーションが考えられる (組合せもありうる)。

- (1) 機能範囲制限型
商品の機能が複数に分割されていて、各機能毎に代金が設定されるタイプ
- (2) 回数制限型
商品の利用回数に対して、代金が設定されるタイプ
- (3) 時間制限型
商品の利用時間に対して、代金が設定されるタイプ

それぞれのタイプにおいて、以下の場合がありうる。

- (a) 既に代金を支払った部分が、商品を終了させるまで有効
- (b) 過去の利用履歴に関わらず、利用する度に支払いが必要

例えば、ページ毎に課金されるハイパーカードサービスなどは (1-a)、辞書サービスは (1-b)、ゲームやユーティリティソフトウェアなどは (2-b)、しばしば広帯域ネットワークが利用される VOD などは (3-a) のように分類される。以下、簡単のため、(3-a) の時間制限型について述べる。他のバリエーションについても、同様な手法で実現できる。

オンラインで代金を徴収する Pay per View を実現するために、ユーザ端末には、コンテンツを実際に再生、実行するビューアあるいはプレイヤー (以下統一的にプレイヤーと呼ぶ) 以外に、以下の機能が必要であると考えられる。

- (機能 1) ネットワークを利用した代金徴収機能
- (機能 2) 条件に応じたコンテンツの再生指示機能
- (機能 3) ユーザの利用状況の監視機能
- (機能 4) 悪意のある第三者あるいはユーザ自身による攻撃からの防御機能 [1]

本稿では、(機能 4) を考慮しつつ、(機能 1)(機能 2)(機能 3) を実現するための端末構成について述べる。以下では利用制限を規定する条件を“PPV 制限条件”と呼ぶ。

3 デジタル情報のオンライン販売方式

デジタル情報の販売方式には、以下の2つがある。

1. 決済とコンテンツ配送を同時に行なう手法
コンテンツを特定のサーバ (決済センタ) 上に格納しておき、購入時に SSL 等の秘密通信プロトコルを利用して購入情報 (クレジット番号等) と交換にコンテンツを配送する。
2. 決済とコンテンツ配送を別々に行なう手法 [2]
コンテンツはそのままでは利用できない処理 (暗号化等) をほどこして、ネットワークを含む任意の経路で事前に配布し、購入時に秘密通信プロトコルを利用して決済センタに接続し、購入情報と交換に、コンテンツを利用可能とする制御データ (復号鍵等) を配送する。

PPV で利用されるコンテンツは比較的容量の大きなものが多いことが予想される。インターネットのような帯域の狭いネットワークでは、ユーザが次の利用単位を利用するごとに、コンテンツを download する前者の方

[†]A Client Architecture for Pay per View Services with Flexible Restriction

[‡]Kenji MORIYASU

[§]NTT Software Laboratories

式よりも、制御データのみを交換する後者の方式の方が適していると思われる。本報告では、後者の方式を取った場合のアーキテクチャについて検討した。

4 PPV 制限条件

PPV 制限条件は、情報提供者が予め規定することができる条件で、コンテンツ個々に対して設定される。したがって、PPV 制限条件の設定データは、コンテンツとセットで配布することにする。

この配布の際、つまり情報提供者からユーザーに渡る経路上で、PPV 制限条件は、コンテンツそのものや金額、説明文等の付加情報と同様に、改ざんを防止する必要がある。以下では、暗号化されたコンテンツ、付加情報および PPV 制限条件に対して、まとめて改ざんチェック機能を施したファイル(配送する単位)を“カプセル”と呼ぶ。

PPV 制限条件には、前章での各種 PPV のタイプに応じた記述がされる。例えば、時間制限型では、以下のよう記述することができる。

```
[Time Constraint]
CONTENT_ID=1      ; コンテンツ ID
TIME_UNIT=HOURL  ; 課金時間単位(時間)
FEE_PER_UNIT=1000 ; 単位当りの金額(円)
CHARGE_METHOD=R.EDO ; 時間切れ時の課金処理を
                    ; 再度行なう
REPLAY=OK        ; 複数回再生が可能
```

多様な PPV 制限条件の記述に応じて、コンテンツを再生、実行する機能を実現することにより、柔軟な PPV を可能とする端末アーキテクチャとなる。

5 システム構成

ユーザーの端末上には、コンテンツのプレイヤーおよび課金用ソフトウェアが一体となった Pay per View 用端末プログラムを置く(図1)。両者を一体とする理由であるが、文献[1]にあるように、悪意のある第三者あるいはユーザー自身による攻撃に対処するためには、本来なら IC カード等のタンパーフリーなハードウェアを用意し、その中に処理プログラムを格納することが最善である。しかし、IC カードリーダの普及率などを考慮し、ある程度の危険とのトレードオフから、ソフトウェアのみで構成する場合、プレイヤーと課金用ソフトウェア間は、特に攻撃の対象となりやすいためである。

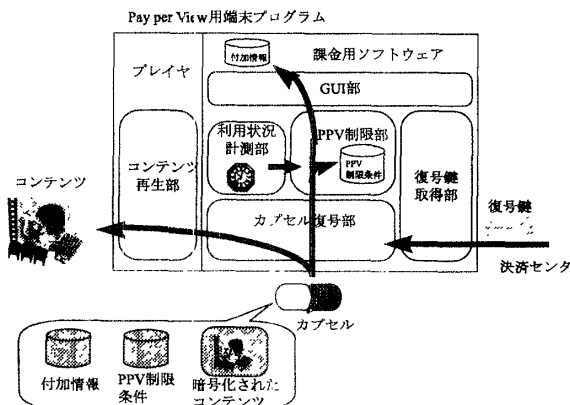


図1: Pay per View 用端末プログラムの構成

各モジュールの機能は、以下の通りである。

● 課金用ソフトウェア

- GUI部
コンテンツ付加情報の表示、購入情報の入力。
- PPV 制限部
カプセル内の PPV 制限条件と利用状況に応じて、コンテンツの再生を指示。
- 復号鍵取得部
決済センタ(復号鍵を管理)と接続し、購入情報と復号鍵を安全に交換。
- カプセル復号機能
カプセルから、付加情報、PPV 制限条件の獲得、コンテンツの復号。
- 利用状況計測部
ユーザーの利用状況の計測。

● プレイヤ

- コンテンツ再生部
課金用ソフトウェアの指示に従って、コンテンツを再生。

コンテンツの再生までの処理手順は以下の通り。

1. コンテンツの価格、説明文など、ユーザーが購入を決定するのに必要な付加情報を、カプセル復号部にて取りだし、提示する。
2. ユーザーが購入を決定し、購入情報が入力されると、復号鍵取得部にて、決済センタと接続し、その購入情報と復号鍵を交換する。(本交換処理は、必要に応じて随時行なわれる)
3. PPV 制限部は、カプセル復号部を通して、カプセルから PPV 制限条件を獲得する。
4. PPV 制限部は、PPV 制限条件と利用状況計測部からの測定結果から、カプセル復号部へ適切なタイミングでコンテンツの復号を指示する。
5. コンテンツ再生部は、PPV 制限部の指示に従って、復号されたコンテンツを再生する。

PPV 制限部が読込める PPV 制限条件を多様にすることで、柔軟な PPV の条件設定が可能となる。

6 おわりに

本報告では、柔軟に PPV 制限条件の設定を可能とする PPV 用端末アーキテクチャについて述べた。PPV を柔軟に実現するために、PPV 制限条件をコンテンツとともに配布し、購入時にそれを読みながら再生する構成を提案した。今後は、PPV 制限条件の記述法の十分性の検討と、実装を通して、実現可能な PPV のバリエーションを増して行く予定である。

参考文献

- [1] 森保, “Pay per View における攻撃と防御法に関する一考察”, 信学春全大 A-7-13, (97.3)
- [2] 明石, 森保, 寺内, “インターネットを用いた情報流通プラットフォーム: Infoket-I”, NTT R&D, vol.46, pp.107-114, (97.2)