シームレス環境のための耐タンパー課金技術

モバイルEコマースで提供されている音楽ダウンロードサービスでは，不正コピーを防止するため，ダウンロードした端末からコンテンツを取り出せないようにするなど，ユーザの利便性を損なった実装となっていることが多い．

この問題を打破するべく，音楽など，コンテンツの自由な再配布および，それらのコンテンツに対する課金を可能にするシステムを開発した．

青野 博（あおの ひろし）　星野 玲子（ほしの れいこ）　本郷 節之（ほんごう さだゆき）

1. まえがき

近年，ADSL（Asymmetric Digital Subscriber Line）をはじめとする，ブロードバンドインターネットの環境下で提供されていたディジタルコンテンツが，携帯電話でも流通しはじめている．これは，携帯電話によるインターネット接続が高速化したことにほかならない．その一方で，ディジタルコンテンツのダウンロードサービスにおける不正コピーが大きな問題となってきている．主な対応策として，複製防止または複製制限機能などのシステムを実装している．しかし，この方法では利用できる端末に制限があるなど，ユーザは不利益を受ける場合がある．反対に，自由なディジタルコンテンツの流通を可能にすると，コンテンツ提供事業者（CP：Contents Provider）が，利用料を回収しにくくなるといった問題が浮上する．

従来の不正コピー防止策として，コピーをまったく許さない方式[1]や，1次コピーのみを許す方式[2][3]などが提案されていた．これらの方式は，メディアや機器側に固有のIDを持たせた不正コピー防止技術として採用され，SDメモリカードやDVD-R/RWやCPRM（Content Protection for Recordable Media），MagicGate*1メモリースティック，Blue-ray Diskなどに実装されている．しかし，これらの技術は端末固有の情報を利用して使用を制限しているため，自由なディジタルコンテンツ流通を困難にする可能性をはらんでいる．

＊1　MagicGate：ソニーが開発したマルチメディアデータの著作権保護技術．著作権が保護された音楽などのデータは暗号化され，認証により正統と認められた機器もしくは機器間のみで，データの再生や送受ができる．

また，ディジタルコンテンツを自由に配布し，クライアント上で課金するという観点では，超流通モデル[4]，ソフト電池[5][6]というものがある．超流通モデルでは，暗号化されたディジタルコンテンツを自由配布し，セキュア・マルチメディアカードと呼ばれる耐タンパーハードウェア内の秘密鍵を用いて，コンテンツの復号鍵などのライセンス情報を配信，移動することができる．超流通モデルに基づくサービスである“ケータイ de ミュージック[7]”では，ディジタルコンテンツの自由な配布が可能である．ソフト電池は，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，バリュー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．一方，ドコモは横浜国立大学の松本勉教授らと共同で，ディジタルコンテンツの再配布を可能にしつつ，その利用の対価を回収するために，ディジタル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ト上で課金を行う方式について提案を行っている[8]～[10]．この方式によれば，自由にコンテンツを流通しても CP はその使用料金を回収することができる．また，本提案の枠組みに従った課金方式をコンテンツに組み込むことでエンドユーザは，各 CP の課金方法ごとにクライアントのソフトウェアや装置を変える必要がない．クライアント上で課金をするという考え方は，超流通モデルやソフト電池と同様である．本方式の特長は，エンドユーザの利便性を確保しながらも，ディジタルコンテンツの再生と課金処理が不可分でかつ同時進行することで，不正に再生または課金のみを単独で実行することを防止できる点が挙げられる．

本稿では，本サービスでの前提条件と要件，攻撃シナリオを明確にした上で，提案モデルとデータ形式，プレイヤについて概説する．次に，提案方式を実装し，安全性および性能に関する評価について報告する．

2. コンテンツ再生と不可分な演算処理によるクライアント上での課金方式

2.1 システムの基本構成

本システムの基本構成を図1に示す．

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（以下，M と表す）の作成を行い，それに対する使用料金を回収するための料金のルールが書かれた課金ロジック（以下，P と表す）を構築する data 生成機能により，P と M を暗号化したコンテンツデー

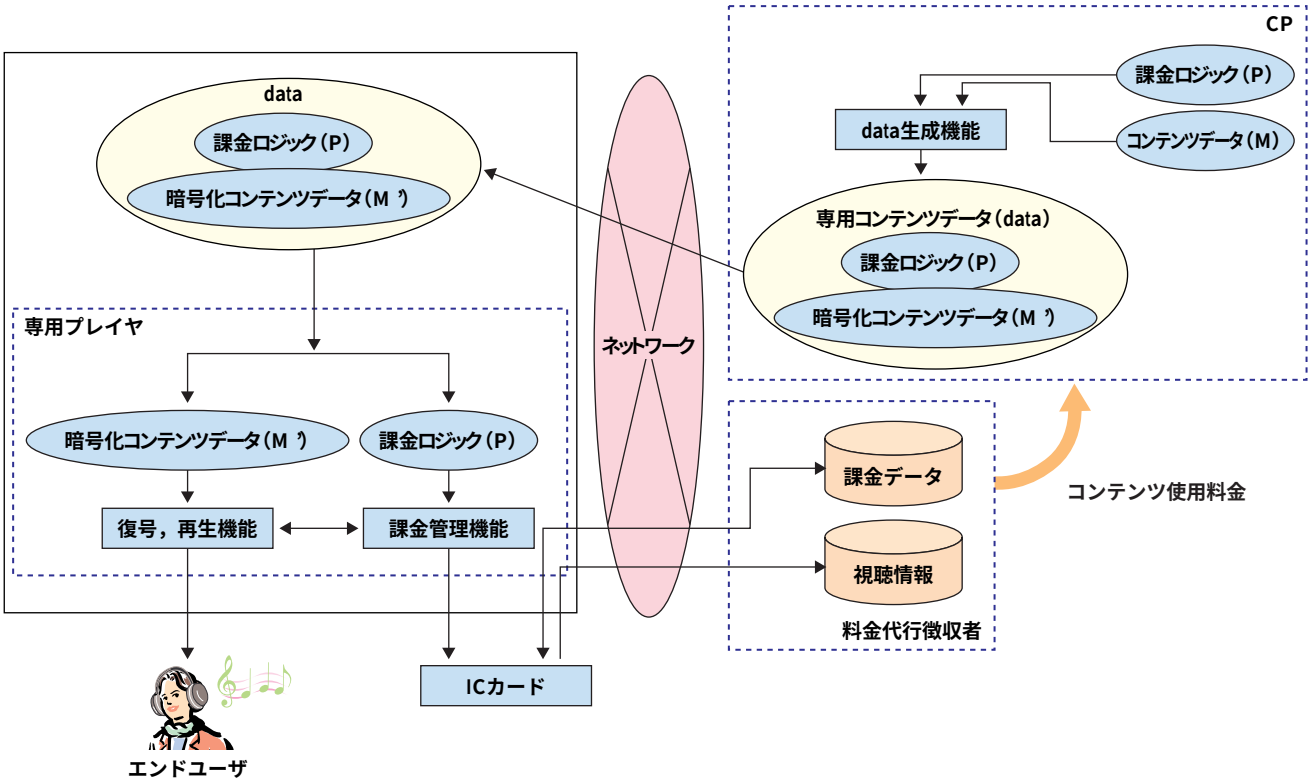

図1　本システムの基本構成

タ（以下，Mと表す）と組み合わせて専用コンテンツデータ（以下，dataと表す）を形成する．エンドユーザの専用プレイヤでは，ネットワーク経由でダウンロードされたdataに対する再生と使用料金の計算が同時に行われ，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に売上げを配分する．

使用料の支払方法は，利用時にCPや料金代行徴収者との通信を行わないために，プリペイドまたはポストペイが考えられる．ポストペイの場合は，確実に支払を行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，また，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カードに蓄積する方式とした．

2.2 サービス要件

コンテンツ再生処理と課金処理が独立に行われると使用料金を払わずに視聴したり，コンテンツの再生を行わずに使用料金を徴収するなどの不正が行われる可能性が高い．そこで，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はコンテンツの使用料金を回収することができ，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る．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を成り立たせるためのサービス要件はCP例とエンドユーザ側に大別できる．以下に，それぞれの要件を示す．

①CP側の要件
- コンテンツを再生と同時に，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できる
- コンテンツが利用された分の使用料金が回収できる

②エンドユーザ側の要件
- 課金処理を実行した場合には，コンテンツを再生できる
- 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などとの通信処理は不要である

2.3 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した．この検討では，攻撃者が持つ能力を以下のように想定した．

- 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想定したとき，前節で述べたサービス要件を脅かす可能性を以下に示す．

①正しく課金を行わないようにPを書き換える．
②MをMに復号する鍵を盗聴，記録することにより再生を行う（dataからMの抜き出し）．
③M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う．
④data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ざんする．
⑤dataを実行するが，ICカードに正しい結果を出力しない．
⑥IC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，再生を行う．
⑦ICカードと課金代行徴収者間のインタラクションを傍受・偽造する．

2.4 提案モデル

本節では，2.1節の基本構成からサービス要件および攻撃に対する対策を行った提案モデルについて述べる．本提案モデルでは，以下の条件を前提に設計を行う．

- ICカードの耐タンパー性は信頼する
- 認証局は信頼する
- 専用プレイヤは耐タンパー性を持ち，ICカード内部の秘密情報は静的な解析においては漏洩しない
- 2.3節の攻撃シナリオ③については，検討対象外とする

本提案モデルにおける構成要素は，基本構成と同様であり，専用プレイヤの構成方法によって，サービス要件および攻撃に対する対策を行う．専用プレイヤの構成要素は専用コンテンツデータ（data），署名検証モジュール（Verifier），分割モジュール（Splitter），コンテンツ再生モジュール（Decoder），制御モジュール（Manager），ICカー

ドからなる（図2）．dataは，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である．署名検証モジュール（Verifier）は，dataが正しいサーバから配信されたものか，改ざんされていないかの検証を行うものであり，MやPが改ざんされることを防ぐために必要な機能である．分割モジュール（Splitter）は，dataをMとPに分割する．ICカードは，Pを実行し，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，課金処理のみ実行による不正課金や鍵生成のみ実行によるコンテンツの不正利用を防ぐことができる．コンテンツ再生モジュール（Decoder）は，kでMを復号するDecrypt部と，Mを再生するDecode部からなる．制御モジュール（Manager）は，PをICカードに送り，ICカードから得られたkをDecoderに渡し，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する，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（詳細は，2.6節のコンテンツ再生手順を参照）．

2.5 専用コンテンツデータ（data）構成

MはCPにおいてdataに変換し，専用プレイヤで再生される．本方式におけるdataの構造を図3に示す．

dataは課金単位ごとにn個のblockに分かれている（$data = \{block_1, block_2, \cdots, block_n\}$）．それぞれの$block_i$（$i = 1, \cdots, n$）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_i）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（$block_i = \{P_i, M_i'\}$）．例えば，課金ロジック（P_i）には，10秒間の視聴に5円課金し，そのコンテンツの課金額が300円を超えると5割引，700円を超えるとそれ以上課金しないような内容が専用のフォーマットで書かれている．

今回の実装においては，MP3（Moving Picture Experts Group-1 Audio Layer-3）形式の音楽データを対象とした．専用のMP3形式のデータを構成するにあたり，以下を条件に検討した．

- dataはMP3ファイルと同様の形式であること
- 一般のMP3プレイヤでは正しく音楽を再生できないこと
- 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CP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．

①課金単位分のMP3フレームデータを鍵k_iで暗号化したデータ（M_i'）とそれに対する課金ロジック（P_i）と暗号化前のデータ（M_i）に対するメッセージ認証子（MAC：Message Authentication Code,（MAC_i））を合わせて，1つのblockのデータ（$block_i$）とする．

②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．

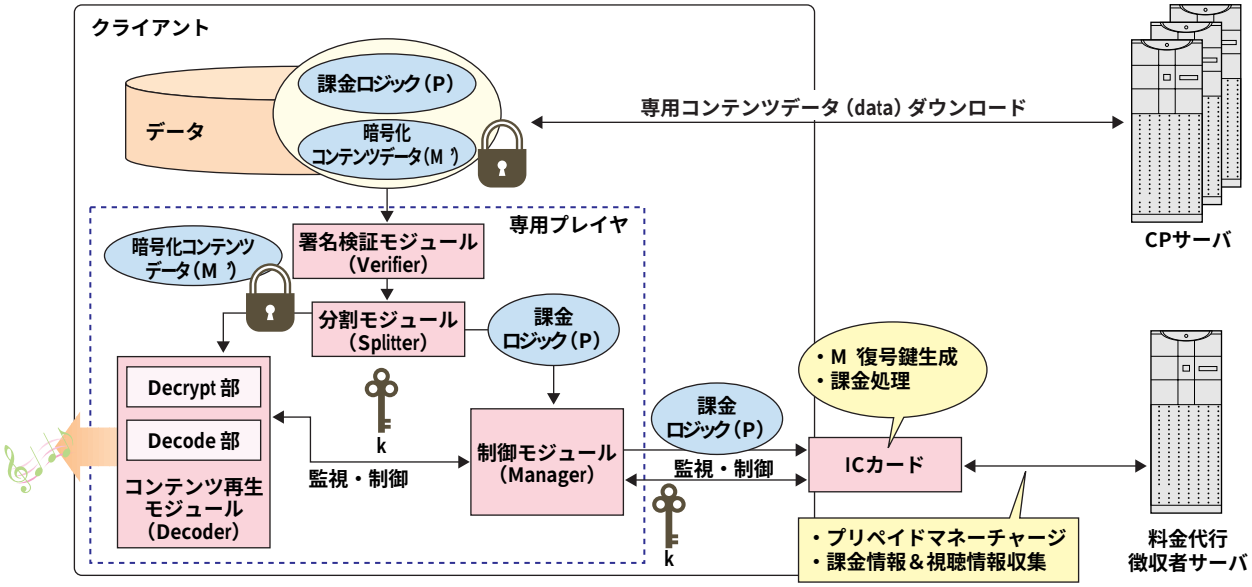

図2　専用プレイヤの詳細構成

③ヘッダ部（ID3v2タグ）に，CPが付した電子署名を格納する．

④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．

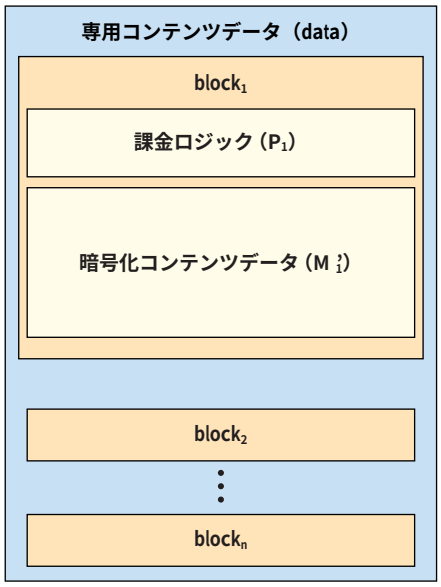

図3　専用コンテンツデータの構成

2.6 専用プレイヤでの再生手順

専用プレイヤとICカード間の具体的な再生手順を図4に示す．

①ICカードはPIN（Personal Identification Number）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)の交換を行う．

②課金要求として，P_iおよび1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*2（$hash_{i-1}$）をkで暗号化しICカードに送る．

③IC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う．

④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

*2　ハッシュ値：任意の長さの入力に対して，固定長の出力値を生成する一方向性関数であるハッシュ関数の出力のこと．通信の途中でデータが改ざんされていないかを調べることができる．

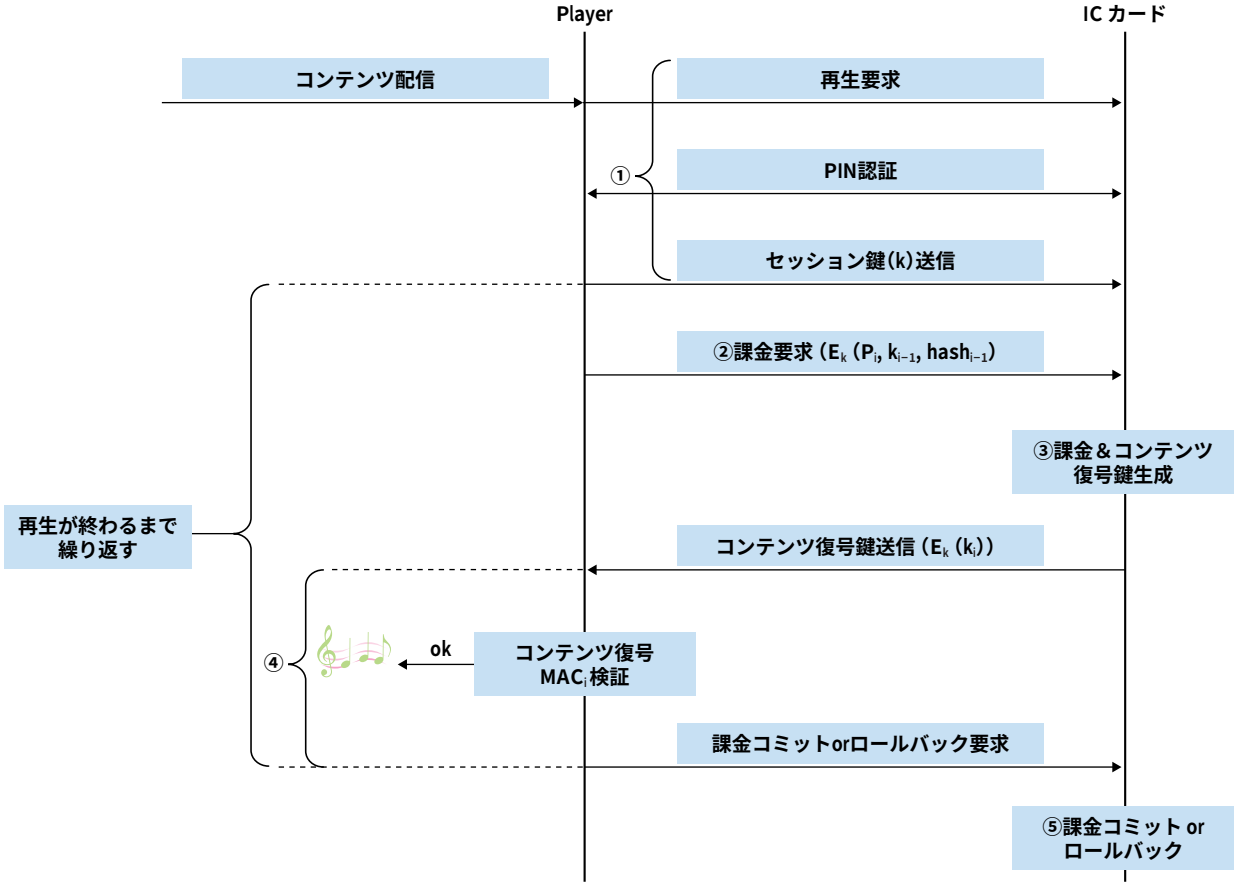

図4　専用プレイヤでの再生手順

生を中断する．

⑤ICカードでは，課金コミットを受け取ると，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き，課金ロールバックを受け取ると使用料の差引きを中止し終了する．

3. 実装と評価

前章で述べた課金方式を検証するプロトタイプ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[11]）に手を入れることで実装を行った．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．

3.1 実装結果

実装環境を表1および図5に示す．ネットワーク経由でダウンロードした専用コンテンツをクライアントPC上での再生時の性能について実測し評価を行った．

通常の演奏と比べてICカードとの通信およびICカード内の処理分がオーバヘッドとなるため，音飛びなく再生するためには，この時間を考慮に入れて課金単位時間を決める必要がある．ICカードとの通信，ICカード内の課金および鍵生成にかかる時間は約2秒である．この結果から，課金単位時間を2秒以上にすることで音飛び無く再生できることが分かり，2秒間隔での課金において正常に再生できることが確認できた．

データサイズに関しては，表2に示すように課金単位時間を短くすればするほど専用コンテンツのデータサイズは増加する．これは，課金ロジックPおよびMACが課金単位の数n分加えられるためである．例えば，5分の曲の場合は，150個のPおよびMACのサイズ（約64Byte×150）が増加することになる．

本提案モデルでは，必ずしもネットワークからコンテンツをダウンロードする必要が無いため，データサイズの増加は大きな問題にならないが，端末のメモリや記録メディア（例えばSDカード，メモリースティックなど）を占めるデータサイズを考慮するとデータサイズは少ないほうが良いというユーザからの要求がでる可能性も考えられる．その場合は，安全性も考慮にいれ，課金単位時間を決定する必要がある．

3.2 攻撃シナリオへの対策

今回の実装に関して，2.3節で述べた攻撃シナリオへの対策についての分析を行う．

(1)正しく課金を行わないようにPを書き換える．dataにはCPの署名が含まれており，署名検証モジュール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う（dataからMの抜出し）．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．

表1　実装環境（条件）

（a）CPサーバ，料金代行徴収者サーバ

CPU	Pentium®4　2.8GHz
Memory	2GB
OS	RedHat®Linux® 7.3
その他環境	Openssl0.9.6b－28, postgreSQL7.2.1－5, Apache™1.3.23－14, tomcat3.3.1－4

（b）クライアント

CPU	Pentium®3　866MHz
Memory	512MB
OS	Windows®XP, 2000
専用プレイヤ	Zinfを変更
ICカード	SchlumbergerSema社 CyberFlex™ Access（JavaCard™ 2.1）
ICカードR/W	SchlumbergerSema社 Reflex20（PCカード）

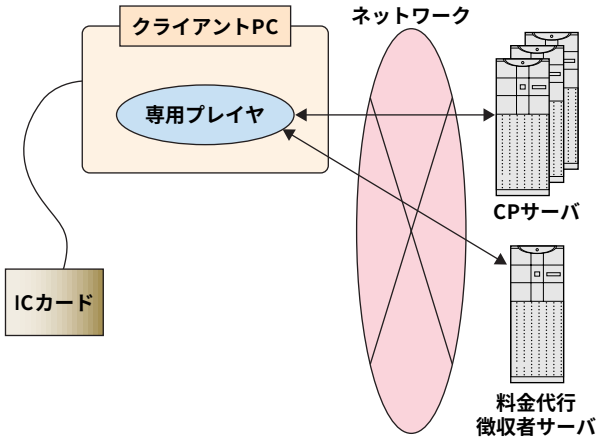

図5　実装環境構成

表2　課金単位時間とdataのサイズの増加（結果）

課金単位の時間（秒）	dataのサイズの増加率（%）
1	17.70
2	13.79
3	12.92
4	12.75
5	12.31
6	11.96
7	11.73
8	11.80
9	11.66
10	11.52

(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う．アナログデータに対する攻撃は対象外としている．

(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ざんする．制御モジュール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行うときには，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困難である．

(6)ICカード内で課金処理を行わずに，ICカードの出力を偽造して，再生を行う．ICカード内の処理を課金のみにせず，k_iの生成もICカード内で行う．これにより，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・偽造は，SSL（Secure Sockets Layer）サーバ認証を行うことで対処．プリペイドマネーのチャージ時には，エンドユーザのID，パスワードの認証を行う．

4. あとがき

本稿では，CPごとの課金方法に合わせてその都度支払いを行うのではなく，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の提案とその方式を検証するためのプロトタイプの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ったが，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っていく．

文　献

[1] 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

[2] 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，2003.

[3] 稲村勝樹，田中俊昭：“デジタルコンテンツにおける不正コピー防止方式の実装と評価，”CSEC-22，Jul.7.2003.

[4] 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.2，1996.

[5] 菅野和裕：“稼動管理システムおよび稼動管理方法，”特許平成10-83298（日本），1998.

[6] 高田秀典：“情報管理装置，情報管理システム，およ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

[7] ケータイdeミュージック・コンソーシアム，http://www.keitaide-music.org/index_j.html

[8] 星野，ほか：“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2003.

[9] 青野，ほか：“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，”第21回CSEC研究会，2003.

[10] 青野，ほか：“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システムの評価，”CSS2003，2003.

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

用 語 一 覧

ADSL：Asymmetric Digital Subscriber Line
CP：Contents Provider（コンテンツ提供事業者）
CPRM：Content Protection for Recordable Media
CPU：Central Processing Unit
MAC：Message Authentication Code（メッセージ認証子）
MP3：Moving Picture Experts Group-1 Audio Layer-3
PIN：Personal Identification Number
SSL：Secure Sockets Layer