pay per view　暗号化技術　コンテンツ流通拡大

Technology Reports

コンテンツの自由な配布と確実な課金を両立するコンテンツ流通技術

コンテンツビジネスのさらなる発展を促すために，新しいコンテンツ課金の仕組みを考案し，コンテンツ流通技術を試作した．本技術を用いることにより，再配布された場合も含めコンテンツ再生時に料金を請求すること，コンテンツのコマーシャル部分などに対してマイナス課金（キャッシュバック）を行うことなどの柔軟な課金が可能となる．

石原　武　伊東 秀昭
寺田 雅之　本郷 節之

1. まえがき

現在，コンテンツに対する課金は，配信時に課金すれば課金管理がしやすいなどの理由のため，サーバからの配信時に行うことが一般的である．しかし，ダウンロードしたコンテンツをユーザがつまらないと感じた場合には，途中までしか再生されないにもかかわらず視聴しない部分に対しても課金されてしまうという問題があった．本コンテンツ流通技術では，ダウンロード時には課金せずに移動端末などのクライアント側で再生時に実際に視聴する分だけの課金処理を確実に行う方式とすることで，この問題を解決する．クライアント側で課金することから，以下，このコンテンツ流通技術をクライアント課金技術と呼ぶ．

クライアント課金技術は圏外での課金，従量課金，コンテンツ提供側として視聴してほしいコンテンツ，例えばコマーシャル（CM）などの部分に対してマイナス課金（キャッシュバック）ができるため，柔軟な課金が行える．また，細かな視聴情報の取得やコンテンツの流通を自由に行うことも可能である．クライアント課金技術を用いることによって，「いつでも」，「どこでも」pay per viewが実現できることからユーザの利便性を向上させることができる．例えば，ダウンロードしたコンテンツを途中までしか視聴していない場合に全額払うことなく，視聴した部分だけの支払いで済ませることが可能となる．また，ユーザはたとえ圏外であっても雑誌の付録などで入手したり友人からもらったりしたコンテンツデータを視聴することも可能となる．

ドコモでは，コンテンツ市場のさらなる開拓を目的として，クライアント課金技術を用いた動画配信の実現可能性について検討を行ってきた．実現方式としては，ノートパソコン（PC）で動画再生を行い移動端末で課金を行う方式と移動端末単独で行う方式が存在するが，はじめに前者を検討し，コンテンツの暗号化方法を工夫することによってクライアント課金が実現可能であることを確認した．

本稿では，クライアント課金技術の概要説明，実現性が確認できたシステムの構成および他技術との比較について述べる．

2. クライアント課金技術の特徴

クライアント課金技術の5つの特徴を以下に説明する．

①圏外であっても課金が可能

クライアント側で課金処理を自律的に実行するため，圏外であってもコンテンツの再生・課金が実行できる．

②コンテンツを自由に配布可能

本方式では，コンテンツが暗号化されていて再生する際には必ず復号・課金されることから，コピ

ー自体を防ぐ必要がなく，利用者間で自由にコンテンツを流通させることができる．

③コンテンツに対して逐次課金（1分10円など）が可能

コンテンツをいくつものブロックに分け（例えば1分ごと），それぞれのブロックを再生するたびに課金処理を行うことが可能である．また，ブロックごとに課金額を変えることもできる．

④マイナス課金（キャッシュバック）が可能

ブロックに対する課金額としてマイナスの値を与えることによりマイナス課金，つまりキャッシュバックを視聴者へ行うことができる．これにより，例えばCM付コンテンツに対して通常コンテンツ部分は課金し，CM部分はキャッシュバックするといったことができる．

⑤ユーザがどの部分を視聴したかという細かな視聴情報が取得可能

課金されたブロックは視聴されたブロックとしてみなすことができる．これにより，それぞれのユーザごとにコンテンツのどの部分を再生したかという，きめ細かな視聴履歴が把握できる．

これらの特徴のうち，③～⑤に相当するクライアント課金技術における課金方法の具体的な例を**図1**に示す．

3. クライアント課金における暗号化技術

3.1 全体概要

クライアント課金技術では，移動端末で課金を行いつつ移動端末と視聴機器が頻繁に通信を行うにもかかわらず，動画再生品質に影響を与えないような軽快に動作する暗号化・復号方式を用いることにより，移動端末と視聴機器のCPU負荷が少ない処理を可能としている．

クライアント課金技術の全体構成を**図2**に示す．サーバが生成したICカード鍵は，安全な方法で移動端末内にコピー，格納されている．サーバはコンテンツを暗号化し，専用コンテンツを生成する．専用コンテンツは暗号化されたコンテンツ，暗号化されたコンテンツ鍵（初期鍵），課金表，メッセージ認証子（MAC：Message Authentication Code）[*1]で構成される．専用コンテンツは自由にコピー可能なため，不当にコンテンツが視聴されないようにする必要があり，コンテンツを，例えば1分ごと，数秒ごとなどのブロック単位で暗号化している．同様の理由により，コンテンツの復号に必要なコンテンツ鍵も暗号化している．また，初期鍵や課金表が改ざんされると，課金が不正に行われたり，課金されても再生が正しく行われなかったりすることになる．そのため，初期鍵と課金表から計算した値をMACとして付与し，専用コンテンツ生成時に計算された値と一致するかを再生前に確認することによりこれらの改ざんを検知し，誤課金を防いでいる．

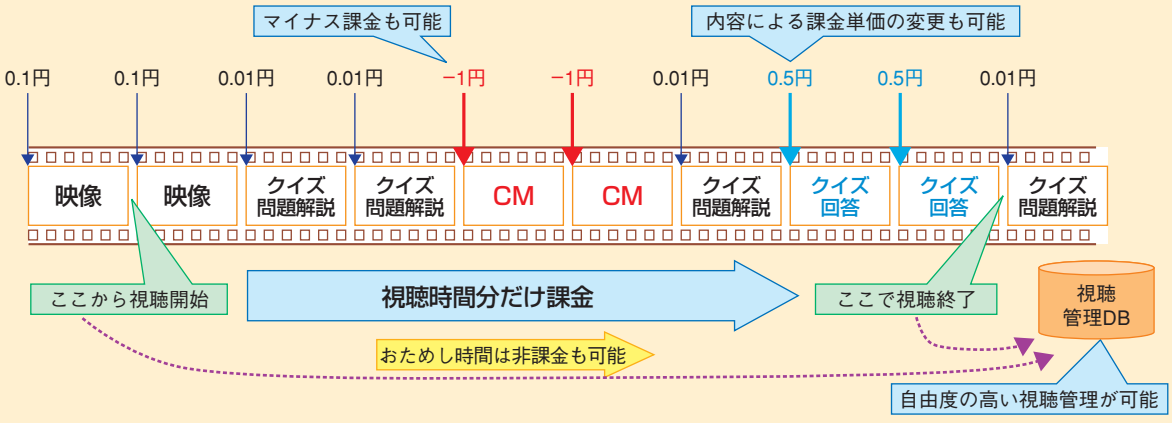

図1　本技術の課金方法

＊1　**メッセージ認証子（MAC）**：データが改ざんされていないかを確認するために用いられるコード．

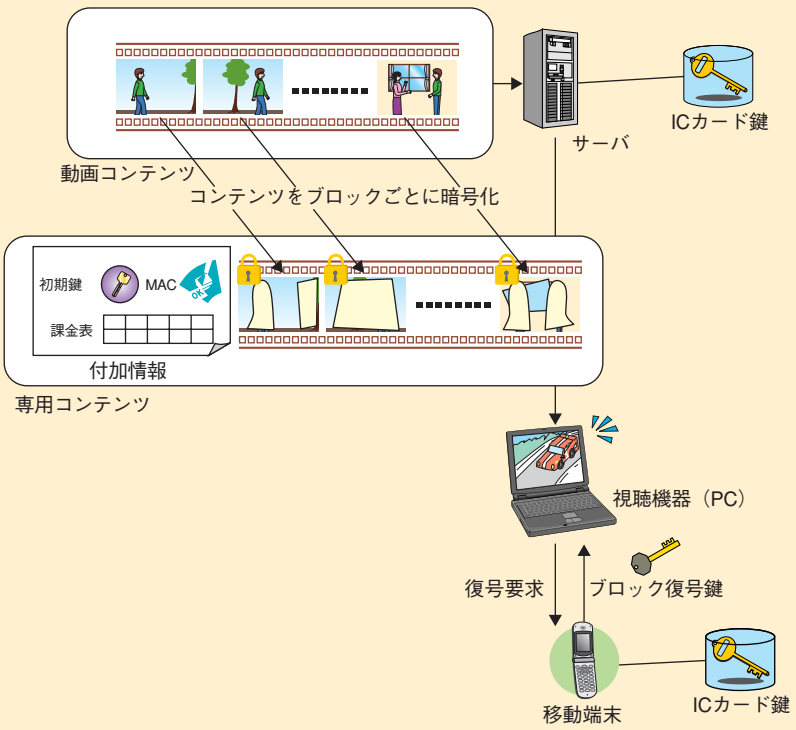

図2　クライアント課金技術の全体構成

視聴機器はクライアント課金技術の専用コンテンツを，コンテンツが暗号化された状態でサーバからダウンロードする．視聴機器（PC）は再生する際に，移動端末に復号要求を行う．すると，移動端末は暗号化されたコンテンツを復号するブロック復号鍵を作成し，併せて課金処理を行う．PC側では，ブロック復号鍵を受け取り，コンテンツを復号し再生を行う．

3.2 暗号化の方法

コンテンツを暗号化する手順（**図3**）を以下に示す．

暗号化するコンテンツに対応するコンテンツ鍵をランダムに決定する（図3①）．課金表，コンテンツ鍵，ICカード鍵を用いてコンテンツ鍵を

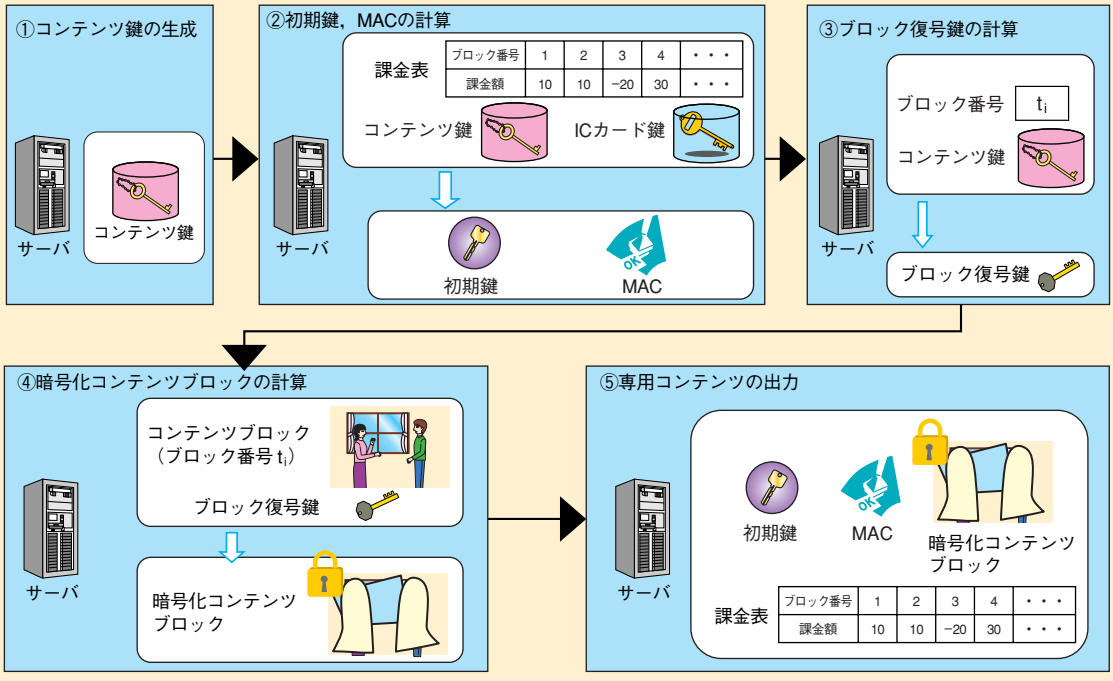

図3　暗号化の手順

暗号化した初期鍵，そしてMACを計算する（図3②）．次にコンテンツ鍵，ブロック番号を基にブロック復号鍵を計算する（図3③）．各コンテンツブロックを各ブロックに対応するブロック復号鍵を用いて共通鍵暗号方式[*2]で暗号化し，暗号化されたコンテンツブロック（暗号化コンテンツブロック）を生成する（図3④）．すべての暗号化コンテンツブロック，初期鍵，課金表，MACをまとめて専用コンテンツとして出力する（図3⑤）．

3.3 復号の方法

専用コンテンツを復号し，再生する手順（**図4**）を以下に示す．

まず，移動端末は，初期処理として個々の専用コンテンツに含まれる固有の初期鍵を基に，あらかじめ移動端末内に保存されたICカード鍵を用いてコンテンツ鍵を導出する（図4①）．MACを用いて初期鍵，課金表，コンテンツ鍵に改ざんがないことを確認する（もし改ざんがあった場合には処理を終了する．）（図4②）．次に，移動端末は，視聴機器からのブロック番号を伴ったブロック復号鍵送信要求に基づき，コンテンツ鍵とブロック番号を用いて該当するブロック復号鍵を導出すると同時に，該当箇所に対応する金額を課金表より確認し，移動端末上で課金を行う．導出されたブロック復号鍵は視聴機器へ送信される（図4③）．視聴機器は，ブロック復号鍵を更新し，暗号化コンテンツブロックをブロック復号鍵を用いて共通鍵暗号方式で復号したうえで，復号されたコンテンツブロックを再生する（図4④）．復号されたデータを再生し終える，あるいは再生可能な復号されたデータが少なくなると視聴機器はふたたび，移動端末へブロック復号鍵送信要求を行い再生する工程を，再生終了まで繰り返す（図4⑤）．

以上の手順により，本技術ではコンテンツ再生時に確実に課金ができることから，専用コンテンツをサーバからのダウンロードやmicroSDやDVDなどの外部記憶媒体からの入手，さらには別のユーザの視聴機器から受信するといった流通手段にとらわれずに配布することが可能となっている．

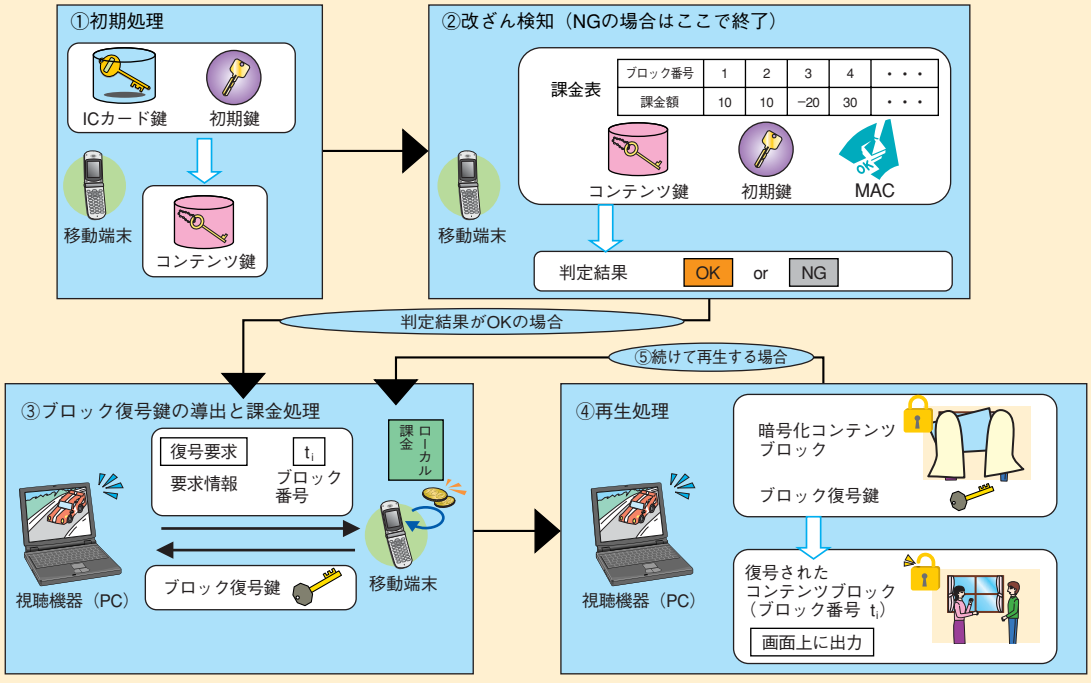

図4　復号・再生の手順

＊2 **共通鍵暗号方式**：暗号のための鍵と復号のための鍵が同一である暗号方式．双方の鍵が異なる暗号方式に比べて演算量が少なくて済むというメリットがある反面，事前に鍵を復号する相手に渡しておく必要がある．

4. システム構成

クライアント課金技術では，動画再生品質に影響を与えないような，軽快に動作する暗号化・復号方式が必要であった．考案した方式が実際に要件を満たしていることを実証するためにシステムを構築し検証を行った．このシステムの構成を**図5**に示す．

システムは，コンテンツを暗号化する機能と，変換された専用コンテンツを保存・配信する機能とをもつコンテンツサーバ，エンドユーザの移動端末と視聴機器（PCなど），そして管理サーバからなる．移動端末はP903iを用いて実現し，視聴機器に用いたのはクロック周波数1.66GHzのPCである．約1.2MBを1ブロックとして扱い，暗号化・復号を行った．

コンテンツは，コンテンツサーバによって暗号化される．暗号化された専用コンテンツはエンドユーザの視聴機器にダウンロードされる．専用コンテンツを再生する際には，視聴機器が専用コンテンツの復号したいブロック番号を移動端末に送信する．移動端末ではそのブロックを復号するためのブロック復号鍵を視聴機器へ送信するとともに，移動端末内部で課金処理を行う．課金処理は，例えばプリペイドマネーの減額によって行うことができる．視聴時には視聴機器，移動端末共にネットワークにつながっている必要はない．移動端末がネットワークにつながった際，視聴ログと，移動端末内で行われた課金処理に関する情報を視聴料回収事業者の管理サーバに送信する．

検証のためのシステムでは，プリペイドマネーの減額によって課金処理を行うとして，コンテンツサイズ720×480pixelの動画を問題なく課金・再生できることを確認した．

なお，ここでは視聴機器と移動端末の通信は赤外線を用いて行う方式の実現性を確認したが，原理的にはFeliCa®＊3やBluetooth®＊4を用いることも可能である．

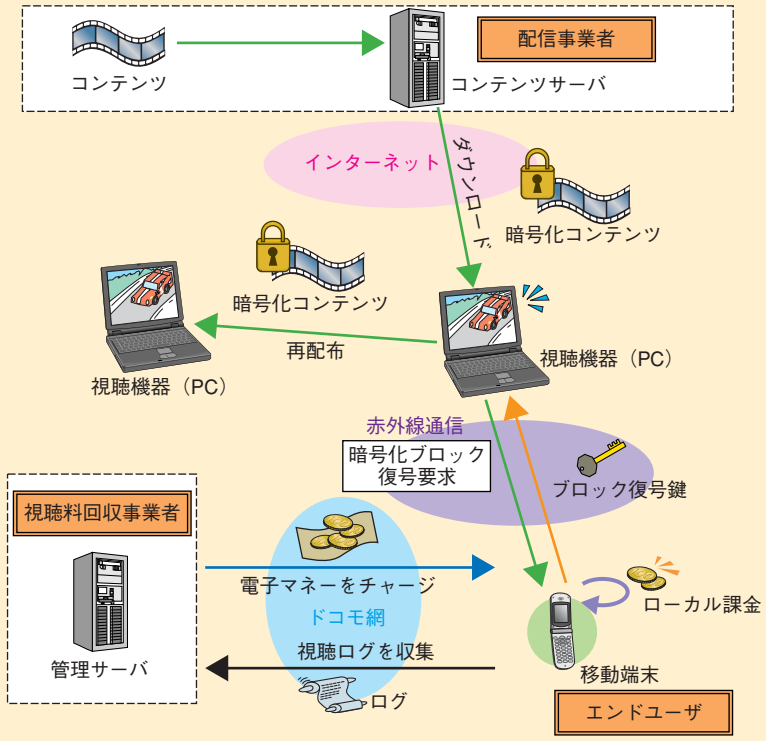

図5　実現性が確認できたシステム構成

5. 他技術との比較

従来技術との差異を**表1**に示す．ここではiTunes®＊5，LISMO®＊6などで用いられている一般的なデジタル著作権管理（DRM：Digital Rights Management）＊7技術と，4th MEDIA®＊8などで用いられているオンライン配信技術，そしてクライアント課金技術の比較を行う．

(1)視聴時の課金可否

コンテンツ再生時の課金可否を示す．一般的なDRM技術では，課金後にダウンロード可能となるために，視聴時に課金することはできない．一方，オンライン配信技術では，視聴時にコンテンツもしくは視聴権をダウンロードし，その際に課金されるため，視聴時の課金が可能となる．クライアント課金技術については，コンテンツの視聴時に初め

＊3 **FeliCa®**：ソニー(株)が開発した非接触型ICカードの技術方式で，同社の登録商標．
＊4 **Bluetooth®**：移動端末，ノートパソコン，PDAなどの携帯端末向け短距離無線通信規格．
米国Bluetooth SIG Inc.の登録商標．
＊5 **iTunes®**：米国Apple Computer, Inc.の登録商標．
＊6 **LISMO®**：KDDI(株)の登録商標．
＊7 **デジタル著作権管理（DRM）**：デジタルコンテンツの著作権を保護するために，再配布制限や不正コピー防止などの管理を行う機能の総称．
＊8 **4th MEDIA®**：(株)ぷららネットワークスの登録商標．

表1　類似・対抗する従来技術との差異

	DRM技術	オンライン配信技術	クライアント課金技術（本技術）
視聴時の課金可否	×	○	○
課金の柔軟性	× 曲単位で売り切り	○ 視聴状況や再生箇所に応じて課金可能	○ 視聴状況や再生箇所に応じて課金可能
エンドユーザによるコンテンツ再配布（クチコミ流通）	△ 一部の技術は可能	×	○
オフライン視聴可否	○	×	○
視聴時の通信要否	○ 通信不要	×	○ 通信不要
取得可能な視聴情報（マーケティング情報）	△ 販売情報のみ	○ 実際の視聴状況を取得可能	○ 実際の視聴状況を取得可能

○：可能　△：一部条件付きで可能　×：不可能

て課金されるため，視聴時の課金が可能となる．

⑵課金の柔軟性

課金がどの程度柔軟に行えるかを示す．一般的なDRM技術ではコンテンツ単位での売り切りとなってしまっており，柔軟性は低い．一方，一部のオンライン配信技術では，視聴状況に応じた課金が可能となっている．クライアント課金技術では，コンテンツの各ブロックに対して課金できるなど，柔軟性は非常に高い．

⑶エンドユーザによるコンテンツ再配布（クチコミ流通）

ダウンロードしたコンテンツファイルの再配布可否を示す．再配布は，一部のDRM技術で可能となっている．クライアント課金技術では再生時に課金するために自由に再配布が可能である．

⑷オフライン視聴可否

コンテンツのオフラインでの視聴可否を示す．一般的なDRM技術やクライアント課金技術では可能であるが，オンライン配信技術では，オンラインでなければコンテンツの視聴ができないために不可能である．

⑸視聴時の通信要否

視聴時に通信を行う必要があるかどうかを示す．一般的なDRM技術ではダウンロード後の視聴時に通信を行う必要はない．しかし，オンライン配信技術では，オンライン状態で初めて視聴ができる．この際，コンテンツもしくは視聴権をダウンロードしなければコンテンツ視聴ができないため，通信を行う必要がある．視聴権のダウンロードだけであれば通信量は少ないが，通信自体は必須である．一方，クライアント課金技術ではコンテンツ視聴時に通信する必要はない．視聴後，通信路が確保されたときに通信を行えば十分である．

⑹取得可能な視聴情報（マーケティング情報）

サービス提供者が利用者の視聴情報をどの程度得られるかを示す．一般的なDRM技術ではコンテンツごとの販売情報しか得られないが，オンライン配信技術やクライアント課金技術については，細かな視聴記録を得ることができる．

なお，一般的なDRM技術では使われ方によって安全性に問題がある場合もあるが，クライアント課金技術についてはICカードなどの耐タンパ装置[*9]を用いることによって，さらに安全性を向上させることが可能であることも特徴の1つである．

6. あとがき

本稿ではクライアント課金技術の特徴およびその技術を用いて実現したシステム構成に関して説明した．

今後の課題としては，課金処理のみならず視聴まで含めて移動端末のみで可能となることも確認すること，動画コンテンツ以外のコンテンツに対しても実現することを確認することである．前者によって視聴機会の増大，後者によって適用範囲の拡大を目指していく予定である．

文　献

[1] 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.

[2] 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. 2003.

＊9　**耐タンパ装置**：コンテンツの内部解析や改変に対する対策を施した装置のこと．回路の中身，内部の動作や処理手順が外部に漏れたり，変更されると一般にはセキュリティが確保できなくなってしまう．

[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, 1996.
[4] 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.
[5] 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.
[6] 星野 玲子，青野 博，本郷 節之，鈴木 雅貴，赤井 健一郎，松本 勉：“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.
[7] 青野 博，星野 玲子，本郷 節之，鈴木 雅貴，赤井 健一郎，松本 勉：“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.
[8] 青野 博，星野 玲子，本郷 節之，鈴木 雅貴，赤井 健一郎，松本 勉：“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.