情報処理学会論文誌　Vol. 51　No. 3　716–727 (Mar. 2010)

UGC市場のための微小課金方式

寺田雅之[†1]　野秋浩三[†1]　青野博[†1]
関野公彦[†1]　本郷節之[†1]

一般ユーザにより作成された映像・音楽コンテンツであるUGC（user-generated content）は，ネットワークのブロードバンド化にともない配布と利用がさかんに行われつつある．現在，ほとんどのUGCは無料で提供されているが，今後UGCがメディアとして健全に発展していくためにはコンテンツの作成者に対して適切な収益分配を行えるようにすることが望ましい．しかし，コンテンツの質に関して玉石混淆であるUGCを従来のコンテンツ販売方法で売買することは，購入したコンテンツの質に関して購入者に大きなリスクを負わせ，「レモン市場化」と呼ばれる現象により商品であるコンテンツの質のさらなる劣化と市場全体の衰退を招く恐れがある．本稿では，上記のUGC流通における購入者のリスクを低減させる手段として，コンテンツの逐次微小課金に着目し，ICカードを用いた安全かつ実用的な実現方式を提案するとともに，その安全性と実現性について議論する．

A Micro-billing System for User-generated Content Market

Masayuki Terada,[†1] Kozo Noaki,[†1] Hiroshi Aono,[†1]
Kimihiko Sekino[†1] and Sadayuki Hongo[†1]

UGC (user-generated content), also known as CGM (consumer-generated media) or UCC (user-created content), has been rapidly diffusing among the internet users and mobile phone users along with the recent spread of wired or wireless broadband internet access. Most of them are distributed free mainly because of the lack of the adequate billing scheme; the currently deployed billing schemes for content are inadequate for UGC, of which creator and quality are much more diverce than content created by professional creators, and accordingly the users have the risk to pay too much for crude or useless content. This risk may lead the UGC market to a *lemon market*, where most merchandises (i.e. UGC) in the market becomes inferior in quality. This paper discusses measures to address this problem and proposes a solution introducing a smartcard-based micro-billing scheme for UGC, by which a user pays for content according to how much she or he plays it, and thus the risk of the quality of content is mitigated. This paper also shows that the proposed scheme can be implemented securely and feasibly by using current smartcards.

1. はじめに

現在インターネット上において，YouTubeやニコニコ動画に代表されるような動画共有サイトなどを介し，一般ユーザにより作成されたコンテンツであるUGC（user-generated content）[⋆1]の配布および利用がさかんに行われつつある．OECDによれば，2006年時点において，米国のインターネット利用者の26%が自作の“artwork, photos, stories or videos”をオンラインで公表したことがあるとされ[15),16)]，eMarketerによる調べでは，2008年時点の米国において約8,250万人（インターネット利用者の約43%）がUGC（ブログなどを含む）を提供したことがあり，2013年にはこの数は1億1,450万人に増加すると予想している[3),14)]．さらに，インターネットだけでなく，特に若年層を中心として，携帯電話からのUGC利用も広まりつつあるとされる[18),19)]．

また，英国BBCがYouTubeを介して（二次利用が許諾された）クリエイティブ・コモンズライセンスでUGC作成用にコンテンツを提供したり，角川書店が一部の二次創作UGCに対して「公式」の認定を与えたりするなど，一般ユーザだけでなく大手のコンテンツ所有者もまたUGCのメディアとしての利便性および影響力に注目しつつある．

その一方で，これらのUGCのほとんどは無料で配布されており，大部分のコンテンツ作成者に対して収益を提供しない．このようにUGCが無料で提供されている現状は，UGCの利用者（消費者）の裾野を広げる役割を果たす一方，UGCの作成者がコストをかけて良質なコンテンツを作成することへの阻害要因となる．これは，中長期的にはUGCのメディアとしての健全な発展を損ない，さらには労働市場に悪影響をもたらすことも懸念されている[4),7)]．

この問題を解決するためには，コンテンツの作成者に対して適切な収益分配を行うための

†1 株式会社NTTドコモ
NTT DOCOMO, Inc.

⋆1 一般に「UGC」という言葉は，ブログ記事や掲示板への投稿など，一般ユーザにより作成されたテキストコンテンツも含んだ概念として扱われることも多いが，本稿では映像や音楽などのメディアコンテンツを主な議論の対象とする．

基盤の整備が必要である．そのための手段として，1)（UGC 配信サイトなどにおける広告収入や物販収入など）UGC の流通にともなう副次収入のコンテンツ作成者への一部還元，2)（コンテンツの有償化など）UGC の利用者からの対価の受領，があげられる[15),16)]．しかし，広告モデルを採用する多くの UGC 配信サイトが十分な収益をあげているとはいい難い現状に鑑みると，副次収入の一部還元だけでコンテンツ作成者に対して十分な収益を分配することは困難をともなうと考えられる．また，UGC の有償化に関しては，利用者リスクの増大が課題となる．すなわち，コンテンツの質に関して玉石混淆である UGC を有償で売買することは，購入したコンテンツの質が購入者の期待を満たすかどうかに関して購入者にリスクを負わせることになる．

このような購入者にとって商品の質に関するリスクが高い市場は，いわゆる「レモン市場化」をひきおこし，商品の質のさらなる劣化と市場全体の衰退を招くことが知られている[1),17),21)]．したがって，UGC を売買する流通市場を健全かつ持続的に運用するためには，コンテンツ販売における購入者のリスクを十分に下げるための対策が必要となる．

本稿では，上記の UGC 流通における購入者のリスクを低減させる手段としてコンテンツの逐次少額課金に着目し，IC カードを用いた安全かつ実用的な実現方式を提案する．本方式は，あるコンテンツの利用に関し，そのコンテンツをどの程度利用したかに応じた利用者への課金と作成者の収益分配を実現することにより，利用者にとって低リスクでのコンテンツの有償利用を可能とするとともに，質が高いコンテンツ作成者に対して多くの収益を分配し，質が高いコンテンツ提供へのインセンティブを与える．

以下，2 章において，従来の有償コンテンツ流通方式を UGC に適用する際の課題について議論し，3 章において課題への対処方針と設計目標を示す．また，4 章で提案方式の構成と手順を示し，5 章において，提案方式の安全性と実装のフィージビリティについて考察するとともに，関連方式に対する位置付けを示す．

2. 従 来 方 式

本章では，従来のネットを介した有償コンテンツ流通における課金方式を示し，それらを UGC に適用する際の課題について議論する．

コンテンツ流通において，コンテンツの利用者から提供者に対して対価を提供するための課金方式については，これまでに多くの検討がなされており，その一部は広く実用に供されている．それらの有料で提供されるコンテンツに対する課金モデルは，課金の対象や課金を実施するタイミングにより以下の方式に大別される．

配布時課金方式　ダウンロード課金とも呼ばれる．CD や DVD の販売と同じように，コンテンツを利用者が取得する際に課金を実施する．

利用時課金方式　ペイパービュー（Pay Per View，PPV）課金とも呼ばれる．コンテンツを利用者が視聴するごとに課金を実施する．

期間課金方式　サブスクリプション課金とも呼ばれる．ある一定の契約期間（1 カ月など）に対して課金を行い，その契約期間内であれば利用者は任意のコンテンツを利用できる．

これらの課金方式は，対象コンテンツや利用環境によって使いわけられている．たとえば，PC や携帯音楽機器，携帯電話へのコンテンツ配信においては，Apple Store や着うたにみられるように，配布時課金が採用されることが多い．有料衛星放送やケーブルテレビなど，放送型のコンテンツ配信システムにおいては，期間課金によりコンテンツの対価を徴収することが一般的である（コンテンツの種類によっては利用時課金が併用されることもある）．

2.1 UGC への適用における課題

以下，それぞれの課金方式について UGC への適用における課題を議論する．

2.1.1 配布時課金

1 章で触れたように，UGC の配布時課金は利用者にとってのコンテンツの質に対するリスクが課題となる．レコード会社や配給事業者がコンテンツの質の確保に関与する従来のプロコンテンツと異なり，UGC では基本的にコンテンツの質の良し悪しはほぼすべてコンテンツ提供者のスキルや作業品質によって左右され，かつプロフェッショナルの製作者からセミプロ，単なる素人まで幅広い作成者によってコンテンツが提供される．これは，今までにない「尖った」革新的なコンテンツが生み出される可能性に寄与する一方で，利用者にとっては，趣味に合わない，もしくは単に質が低いコンテンツに対して対価を支払う懸念が高くなることにつながる．

このような，「買ってみなければ分からない」商品（この場合ではコンテンツ）が多い市場は，消費者の逆選択（adverse selection）に基づくレモン市場（lemon market もしくは market for lemons）化を引き起こすとされる．すなわち，商品の質にばらつきが大きく，かつ商品の質に関して十分な情報を持たない消費者（コンテンツ利用者）は，リスク回避の観点から質が悪い商品を高額で「つかまされる」ことを恐れるようになり，質の良否にかかわらず安価な商品を選択・購入することになる（消費者による逆選択）．すると，質が高い商品を提供する販売者（コンテンツ提供者）は収支の悪化により市場から撤退することを迫られ，市場には安価だが質が悪い商品が蔓延する（レモン市場化）[1)]．そのため，良質なコンテンツの継続的な確保による UGC のメディアとしての持続的な発展，という目標とは逆の

結果をもたらすことになる．

2.1.2　利用時課金

利用時課金においても配布時課金と同様の問題が生ずる．利用時課金において，あるコンテンツに対する理論上の課金額は，配布時課金の課金額を，そのコンテンツに対して期待される課金回数で除したものとなる．利用者は，コンテンツの質に不満をおぼえたならばそれ以降の利用を中止すればよいため，理論的にはその分だけ利用者のリスクは小さくなる．

しかし，実際問題として，映像や音楽などの UGC は，（無料であっても）1 人の利用者が同一のコンテンツを何度も繰り返し視聴することは稀である．そのため，期待される課金回数が実際には十分に大きくならず，配布時課金と比較して利用者リスクが有意に小さくなることは期待しにくい．したがって，単に利用時課金を採用してもレモン市場化を防ぐことは困難と考えられる．

2.1.3　期 間 課 金

期間課金については，コンテンツ提供者への適切な収益の分配が課題となる．このモデルにおいては，一定の使用料を支払えば，その使用料のもとに提供されているどのコンテンツを利用しても利用者にとって新たな対価の支払いは発生しない．そのため，配布時課金や利用時課金で課題となった，コンテンツ購入時におけるコンテンツの質に関するリスクは発生しない．ただし，使用料による収益をコンテンツ提供者に適切に分配するため，コンテンツの利用頻度などの統計情報を配信サーバなどで収集する必要が生ずる．

これは，オフライン環境でのコンテンツ利用を妨げるとともに，提供者への収益分配における「サクラ攻撃（shilling attack）」による不正リスクを生じさせる．すなわち，提供者自身や提供者と結託した利用者（サクラ）が，通常の利用者のふりをして意味もなく当該提供者のコンテンツを利用し続ける（もしくは利用する「ふり」をしたダミープログラムを動作させ続ける）ことにより，分配金額を不正に大きくする攻撃が成立しうる．

この攻撃は，配布時課金や利用時課金など利用（もしくは配布）に費用がかかる課金モデルでは成立せず，また，従来の有料コンテンツ配信のように，利用者数と提供者数の比が圧倒的に大きい（利用者数が提供者数より多い）状況では攻撃の費用対効果が小さくなるため問題となりにくいが，多数のコンテンツ提供者が存在しうる UGC に期間課金方式を適用する際には，この問題への対策が必要となる．

3. 設 計 目 標

2 章で述べたように，UGC を有償で流通させる市場を健全な形で成立させるためには，1) 販売時課金もしくは利用時課金方式において，コンテンツの質に関する利用者リスクを低減させることにより，利用者の逆選択とレモン市場化を防ぐこと，もしくは，2) 期間課金方式において，サクラ攻撃など収益分配の不正を防止すること，のいずれかの対策をとることが必要となる．

本稿では，1) の方針を採用し，コンテンツの利用時における逐次微小課金を利用者環境上で安全に実現することにより，有償での UGC 流通におけるコンテンツの質に関する利用者リスクを低減させる方式を提案する．

すなわち，ある UGC を微小ブロックに分割し，それぞれのブロックを利用するごとに課金を実施することにより，利用時課金における「繰返し」回数を十分に確保し，利用者が「質が低い」コンテンツに対して多額の対価を支払うリスクを抑制する．また，コンテンツ提供者にとっても，コンテンツの「質が低い」と判断されると利用が中断され，低い収益しか望めないことになるため，提供されるコンテンツの質が高くなることが期待される．これは，レモン市場化への対策の 1 つとしてあげられる「取引の繰返し化」を実現することに相当する．

このようなコンテンツ課金は，たとえば PayWord [11] などに代表されるマイクロペイメント（少額決済）システム[22] を微小ブロックの視聴に対する決済手段として用い，利用者からのマイクロペイメントによる決済のたびごとに，決済サーバが当該決済に対応する微小ブロックを利用者に配信する，などの配信環境を構築することにより実現することができる．

ただし，このような逐次微小課金をネットワークを介して実施しようとすると，ネットワーク接続手段がないオフライン環境（たとえば携帯機器を用いたコンテンツ利用環境など）ではまったく利用することができなくなる．また，接続手段があったとしても，ネットワークの一時的な遅延増大が発生した際にコンテンツの再生が停止するなど，コンテンツの再生品質の悪化が懸念される．一般に，ネットワーク遅延による再生の一時停止などの品質悪化を防止するためにはコンテンツの先読み（バッファリング）が対策として用いられることが多い．しかし，逐次微小課金と先読みを併用すると，先読みした分だけ（実際には視聴していないにもかかわらず）課金が発生することになる．そのため，コンテンツの先読みの適用による再生品質の維持も困難である．

したがって，上記の逐次微小課金処理はネットワークを介することなく利用者環境内で実施することが望ましい．しかし，その場合は，いかに利用者環境で安全な課金を実施するか，すなわち，利用者による不正がありうる環境下において，コンテンツの利用と課金の実

施を公平に実現することが課題となる．

以上の議論から，提案方式の設計目標を以下のとおりに設定する．

(1) コンテンツ利用者にとって公平な方式であること．すなわち，質が低い，もしくは利用できないコンテンツに対する支払いリスクが低いこと．

(2) コンテンツ提供者にとって公平な方式であること．すなわち，コンテンツ利用の対価を確実に受領できること．また，なりすましやコンテンツ改竄などの不正行為により，不当に評判を落とされることがないこと．

(3) 実装上，実用的な構成および性能で実現可能であること．

4. 提案方式

前章の設計目標を達成するため，本稿では，逐次微小課金の実現手段として IC カードを用い，課金処理を利用者環境内で安全に実施する方式を提案する．以降，提案方式の概要を示した後，コンテンツ提供者による配布コンテンツの作成，コンテンツ利用者によるコンテンツの利用と課金，コンテンツ利用者からコンテンツ提供者への利用の対価の還元，のそれぞれの処理手順について詳細を説明する．

4.1 全体の概要

以下，本方式においてコンテンツ作成者 H が配布コンテンツ c を作成し，コンテンツ利用者 U が c を利用した後に H がその対価を受け取るまでの主な流れを示す．ここで，コンテンツ作成者 H は配布コンテンツ生成装置 G_H と対価受領装置 R_H，コンテンツ利用者 U は課金装置 B_U と再生装置 P_U を，それぞれ保有しているとする．なお，各装置の実現形態は説明の中で示す．

コンテンツ作成者 H は配布コンテンツ生成装置 G_H を用いて，コンテンツ m から配布コンテンツ c を生成する．ここで，G_H は PC などの計算機上で実現されたソフトウェアであり，m は一般的なエンコード形式（MPEG4 など）で符号化された映像・音楽などのコンテンツ情報である．G_H により m から生成された配布コンテンツ c は n 個の暗号化された微小ブロック $\{c_1, c_2, \ldots, c_n\}$ と，ヘッダ情報 c_0 から構成される（$c = \{c_0, c_1, \ldots, c_n\}$）．ヘッダ情報 c_0 は各ブロックと m との対応関係を示す分割情報 d_c，各ブロックに対する課金額を計算する課金関数 f_c，各ブロックの復号鍵生成のための鍵生成子 k_c，改竄防止のための認証子 a_c，および H の公開鍵 Pk_H から構成される（$c_0 = \{d_c, f_c, k_c, a_c, Pk_H\}$）．生成された配布コンテンツ c は，配布サーバないし P2P ネットワークなどを介してネットワーク上に公開される．ここで，通常のコンテンツ販売方式と異なり，対価の徴収はコンテンツの配布時ではなく，コンテンツの利用時に利用者環境内に閉じて行われるため，c の配布手段は任意の手段でかまわない（特にストリーミング配信機能や DRM 機能を備える必要はない）．

コンテンツ利用者 U は，課金装置 B_U と再生装置 P_U を用いて，H により公開された配布コンテンツ c を利用する．ここで，課金装置 B_U は電子マネー機能を備えた耐タンパデバイス（IC カードや IC カードを備えた携帯電話など）であり，c の利用において，再生装置 P_U からのブロック番号 i の指示に従い対応する微小ブロック c_i を復号するとともに，課金関数 f_c により計算された額の課金（電子マネーの減算）を行う（課金額は，後述するコンテンツ作成者への対価の還元のために記録される）．再生装置 P_U は，利用者 U コンテンツ m の再生機能を備えたコンテンツ再生機器ないし PC 上の（難読化措置が施された）コンテンツ再生ソフトウェアであり，利用者 U からの指示に基づいて課金装置 B_U に再生対象となるブロック番号 i を指示して c_i の復号結果を受け取り，その再生を行う．

コンテンツの再生終了後，もしくは一定期間（1 日や 1 カ月など）ごとに，課金装置 B_U に記録された課金額に基づいて B_U から対価受領装置 R_H へ対価の還元を行う．R_H は，ネットワーク上に設置された電子マネー口座や電子マネー機能を備えた携帯電話などであり，公平交換プロトコルを用いて B_U からの対価の受領（電子マネーの加算）を行う．対価を正しく受領するため，R_H の電子マネー機能は B_U と同一の電子マネーを扱えるものとする．

4.2 詳細な説明

以下において，本方式における各処理の手順を示す．ここで，Pk_H および Sk_H は，それぞれコンテンツ作成者 H の公開鍵および秘密鍵の鍵ペアであり，いずれもコンテンツ生成装置 G_H および対価受領装置 R_H により保持される．なお，Sk_H は G_H および R_H 内で安全に管理されており，（H 自身の不正を除いて）漏洩しないものとする．Pk_B および Sk_B は課金装置の公開鍵ペアであり，Sk_B はあらかじめすべての課金装置で安全に共有され，適切に更新されているとする．また，H は Pk_B をあらかじめ保持するか，安全に入手できるとする．なお，課金装置 B_U は IC カードなどの耐タンパ装置であり，利用者自身の不正によって，その振舞いが変更されたり，内部情報が漏洩もしくは改竄されることはないとする．

4.2.1 配布コンテンツの作成

コンテンツ作成者 H は，配布したいコンテンツ m を作成するとともに，どのようにコンテンツを分割するか，および各分割された微小ブロックに対していくらの額を利用者に対

して課金するかを決定し，配布コンテンツ生成装置 G_H に与える．G_H は，以下の処理手順により m に対応する配布コンテンツ c を生成する．

(1) コンテンツ作成者 H により与えられた指示に基づき，分割情報 d_c，課金関数 f_c を生成する．ここで，分割情報 d_c は n 個のコンテンツ位置情報 d_i から構成され（$d_c = \{d_1, d_2, \ldots, d_n\}$），コンテンツ m の $d_{i-1}+1$ バイト目から d_i バイト目まで（以降，これを m_i とする）が，微小ブロック c_i に対応することを表す．ただし，$d_0 = 0$，$d_n = |m|$ とする．また，課金関数 f_c は，ブロック番号 i と再生履歴 l_c（次節で説明する）を入力として，課金額 b_{i,l_c} と更新後の再生履歴 l'_c を出力する関数である（$f_c(i, l_c) \to \{b_{i,l_c}, l'_c\}$）．たとえば最も単純な場合として，今までの当該コンテンツの再生状況にかかわらず，すべての微小ブロックに対して同じ額 b を課金するならば，f_c は任意の入力に対して定数 b と空集合を出力する定数関数となる（$f_c(\cdot,\cdot) \to \{b, \phi\}$）．

(2) 乱数を用いて鍵長 kl のコンテンツ鍵 k_0 を生成し（$k_0 \leftarrow \{0,1\}^{kl}$），$k_0$ を課金装置の公開鍵 Pk_B を用いて暗号化することにより鍵生成子 k_c を生成する（$k_c = Pk_B(k_0)$）．

(3) コンテンツ鍵 k_0 とブロック番号 i（$1 \le i \le n$）を用いて m_i をそれぞれ暗号化し，微小ブロック c_i を生成する．ここで，c_i は以下の手順により暗号化される．

(a) 共通鍵暗号を用い k_0 を鍵として i を暗号化することにより，ブロック鍵 k_i を生成する（$k_i = k_0(i)$）．

(b) 伸長関数 $e : \{0,1\}^{kl} \to \{0,1\}^{|m_i|}$ を用いて，ブロック鍵 k_i から伸長鍵 e_i を生成する（$e_i = e(k_i)$）．ここで伸長関数 e は，疑似乱数系列を生成する一方向性関数である．

(c) m_i と e_i の排他的論理和をとることにより c_i を生成する（$c_i = m_i \oplus e_i$）．

ここで，c_i の生成にあたり，単に CTR モードで m を暗号化するのではなく，上記の手順を用いる理由は，後述の配布コンテンツの利用処理において，実装上 I/O 速度が遅いことが想定される課金装置との入出力量を抑えるためである．

(4) コンテンツ作成者の秘密鍵 Sk_H を署名鍵として用い，d_c，f_c，k_c およびすべての微小ブロックの連接に対するハッシュ値 $h(c_{1,n} = c_1|c_2|\ldots|c_n)$ を署名対象とする電子署名を生成し，認証子 a_c とする（$a_c = \mathrm{Sign}_{Sk_H}(d_c|f_c|k_c|h(c_{1,n}))$）．なお，ここで $h : \{0,1\}^* \to \{0,1\}^{hl}$（$hl$ はハッシュ長）は SHA-256 などの安全な一方向ハッシュ関数である．

(5) $c_0 = \{d_c, f_c, k_c, a_c, Pk_H\}$ とし，微小ブロック $\{c_1, c_2, \ldots, c_n\}$ とあわせ，配布コンテンツ $c = \{c_0, c_1, \ldots, c_n\}$ を生成する．

4.2.2　配布コンテンツの利用

コンテンツ利用者 U は，課金装置 B_U と再生装置 P_U を用い，以下の処理手順で配布コンテンツ c を利用する．配布コンテンツの利用処理は，初期化処理と再生処理から構成される．初期化処理は，配布コンテンツの再生を開始するごとに実施され，再生処理はそれぞれの微小ブロックを利用するごとに実施される．

初期化手順

初期化手順は，課金装置 B_U のみを用いて以下の手順で行われる．

(1) コンテンツ利用者 U は，利用対象とする配布コンテンツ c から課金関数 f_c を抽出し，コンテンツ利用にともなう課金額の総計および遷移が U にとって妥当かどうかを判断する．課金総額が高すぎたり，もしくは総額が妥当であっても f_c がコンテンツの最初の部分で高額な課金額を設定していたり，U にとって不当な課金処理が行われると判断される場合，U は以降の処理を中断する（c の利用を中止する）．

(2) U はハッシュ関数 h を用い，c に含まれるすべての微小ブロックの連接に対するハッシュ値 $h_c = h(c_{1,n})$ を計算する．

(3) U は c からヘッダ情報 c_0 を抽出し，h_c とともに課金装置 B_U に与える（$U \to B_U : \{c_0, h_c\}$）．

(4) B_U は，c_0 から d_c，f_c，k_c，a_c，Pk_H を抽出し，h_c とあわせて署名検証を行う（$\mathrm{Verify}_{Pk_H}(d_c|f_c|k_c|h_c, a_c) \stackrel{?}{=} \mathsf{success}$）．署名検証に失敗したら，$c$ に改竄があったとして U にその旨を通知し，以降の処理を中断する．

(5) B_U は，（Pk_H に対応づけられた）H に対する（未還元の）還元額 b_H を参照する．b_H がある定められた値 $b_{\max}$ を超過していたならば，U に対して H への還元処理を促す通知を行い，以降の処理を中断する．

(6) B_U は課金装置の秘密鍵 Sk_B を用い，k_c から k_0 を復号し，コンテンツ利用者 U に対して再生準備が完了した旨を通知する．

再 生 手 順

再生手順は，上記の初期化手順の実施後，課金装置 B_U と再生装置 P_U を用いて以下の手順で行われる．

(1) 再生装置 P_U は，d_i を用いて再生対象とする微小ブロックのブロック番号 i を特定し，課金装置 B_U に与える（$P_U \to B_U : i$）．

(2) B_U は，以下の手順により微小ブロック c_i の利用に対する課金を実施する．なお，課

金にともない，c の再生履歴を保持する情報である再生履歴情報 l_c を更新する．

(a)　再生履歴情報 l_c とブロック番号 i を課金関数 f_c に与え，課金額 b_{i,l_c} と更新後の再生履歴情報 l'_c を求める（$\{b_{i,l_c}, l'_c\} \leftarrow f_c(i, l_c)$）．ここで，$l_c$ は B_U が配布コンテンツごとに記録する情報であり，初期状態は空である．

(b)　保有する電子マネーの残高から b_{i,l_c} を減算する．残高不足などにより減算に失敗したら，その旨を通知して以降の処理を中断する．減算に成功したら，H への還元額 b_H に b_{i,l_c} を加算する．b_H は B_U がコンテンツ作成者ごとに記録する情報であり，コンテンツ作成者の公開鍵 PkH に対応づけられて管理されている．なお，b_H の初期値は 0 である．

(c)　再生履歴情報 l_c を l'_c へと更新する（$l_c \leftarrow l'_c$）．

(3)　B_U は，i を（初期化手順で抽出された）k_0 を鍵として暗号化することによりブロック鍵 $k_i = k_0(i)$ を生成し，P_U に与える（$B_U \rightarrow P_U : k_i$）．

(4)　P_U は，伸長関数 e を用い，k_i から伸長鍵 $e_i = e(k_i)$ を生成する．

(5)　P_U は，e_i と c_i との排他的論理和をとることにより m_i を生成（$m_i = e_i \oplus c_i$）し，再生を実施する．

4.2.3　対価の還元

コンテンツ利用者 U からコンテンツ提供者 H へのコンテンツ利用の対価の還元は，B_U と R_H とを用いて以下の手順で行われる．

(1)　B_U は，H の対価受領装置 R_H との間で，H への還元額 b_H を送付し，b_H を B_U から削除する許可を表す受領確認トークン d_{b_H} を受領する（B_U と R_H との間で b_H と d_{b_H} とを交換する）公平交換（fair exchange）プロトコル[9),12)] を実行する．ここで，受領確認トークン d_{b_H} が正しくコンテンツ作成者 H によって生成されたものであることを確認するため，d_{b_H} は Sk_H による電子署名を含む．たとえば具体的には，$d_{b_H} = \mathrm{Sign}_{Sk_H}(n_{b_H})$（ただし n_{b_H} は b_H と d_{b_H} との交換セッションに対応づけられた任意の一意な値とする）として d_{b_H} を構成し，公平交換プロトコルにおける受領物の確認フェーズにおいて，B_U は d_{b_H} に対して Pk_H を用いて署名検証を行う．署名検証に失敗したなら，交換を中止する（このとき，公平交換プロトコルの性質から b_H は R_H に還元されない）．

(2)　B_U は，上記プロトコルの実行の正常終了により d_{b_H} を受け取ったならば[⋆1]，b_H を消去する（$b_H = 0$ とする）．

なお，手順 (1) において（単なる電子マネーの移送プロトコルではなく）公平交換プロトコルを用いる理由は，利用者 U が正しく対価を H に還元しているにもかかわらず，（H の不正もしくは通信路の異常により）b_H が消去されずに B_U に残り続け，初期化手順の手順 (5) における未還元額の検証により以降のコンテンツ利用ができなくなる障害を防ぐためである．

5. 考　　察

本章では，前章で提案した方式の安全性と実装のフィージビリティについてそれぞれ示し，関連方式に対する本方式の位置付けについて議論する．

5.1 安　全　性

以下，本方式の安全性について，コンテンツ利用者の立場およびコンテンツ提供者の立場からそれぞれ議論する．

5.1.1　コンテンツ利用者の安全性

本方式において，コンテンツ利用者にとっての不利益とは，質が低い，もしくは利用できないコンテンツに対価を支払わされることである．その原因は，1) そもそも何の攻撃も発生していないが，利用したコンテンツ自体の質が（その利用者にとって）満足しないものであった，2) コンテンツ提供者が悪意を持って質が低い（もしくは利用できない）コンテンツを提供した（コンテンツ提供者による攻撃），3) 第三者が配布コンテンツを改竄した（第三者による攻撃），のいずれかに分類される．

1) に対しては，3 章で示したとおり，本方式はコンテンツ利用における微小課金を実現することにより従来の配布時課金によるコンテンツ販売に対して利用者のリスクを抑える．すなわち，n 個の微小ブロックから構成される配布コンテンツを m ブロック目まで利用して，コンテンツの質に不満を覚え利用を中断した場合，課金される対価は $\Sigma_{i=1}^{m} b_i$ [⋆2]となる．ここで，コンテンツの質が低いほど（利用中断の判断が早くつくことから）m は小さくなる．これに対し，通常の配布時課金における対価は全微小ブロックの課金額の総和 $\Sigma_{i=1}^{n} b_i$ 以上に相当するため，利用者のリスクはこれらの比，$\Sigma_{i=1}^{m} b_i / \Sigma_{i=1}^{n} b_i$ 以下に軽減される．

ただし，課金関数 f_c がコンテンツの最初の部分で高額な課金額を設定するなど（たとえば $i = 1$ のとき，つまり最初の微小ブロックの利用時に全額を課金するなど）極端な構成

⋆1 公平交換プロトコルの性質から，R_H が b_H を受領したならば，（U 自身が妨害しない限り）B_U は必ず d_{b_H} を受け取ることができる[2),12)]．

⋆2 本方式において，各ブロックの課金額は再生履歴に依存する値（b_{i,l_c}）であるが，簡単のため初回利用時の i ブロック目の課金額を b_i と表記する．

をとっている場合，上記の比は十分に小さいものとならない．しかし，利用者は初期化手順の冒頭で課金関数の確認を行う機会があるため，そのようなコンテンツについては最初から「利用しない」と判断することができる．

2) の場合は，1) と区別をつけることは本質的に難しい（たとえば提供者の「手抜き」により質が低くなった場合，どちらとも区別しがたい）．したがって，この場合のリスクも 1) の場合と同じ議論となる．

3) に対しては，認証子 a_c の電子署名によって配布コンテンツは改竄から保護されているため，この攻撃は成立しない．すなわち，配布コンテンツ c に含まれる情報のうち，d_c，f_c，k_c はいずれも a_c の署名対象であり，初期化手順における手順 (4) の署名検証により（利用する電子署名方式が安全である限り）改竄は検出される．微小ブロック $c_1, c_2, \ldots, c_n$ 自体は署名対象に含まれない[⋆1]が，それらの連接に対するハッシュ値 $h(c_{1,n})$ が署名対象として含まれているため，ハッシュ関数 h が安全であり，かつ利用者 U が初期化手順の手順 (3) において正しいハッシュ値 h_c を与えるなら，微小ブロックに対する改竄も同手順 (4) の署名検証により検出される．ここで，（利用者 U に対する攻撃を議論しているため）U 自身による攻撃は考慮する必要がないことから，第三者の配布コンテンツ改竄による利用者への攻撃に対する安全性は，利用する署名・検証方式 Sign/Verify およびハッシュ関数 h の安全性に帰着される．

5.1.2　コンテンツ提供者の安全性

次に，コンテンツ利用者にとっての安全性を議論する．本方式においてコンテンツ提供者にとっての不利益は，1) コンテンツ利用に対して課金が正しくなされないこと，2)（課金はされても）課金された対価が正しく還元されないこと，および，3) 配布コンテンツの改竄により評判を失うことである．

このうち，2) については，還元処理を実行するか否かにかかわらず，コンテンツ利用に対する課金はすでに再生処理の時点でなされているため，利用者にこの不正を行うインセンティブは存在しない（利用者が攻撃者となる動機が小さい）．さらに，初期化手順 (5) において未還元の課金額の検証を行うことにより，H の未収額の上限は，課金装置 1 つあたり $b_{max} + \Sigma_{i=1}^{n} b_i$（最後に利用するコンテンツの課金額の総和）となる．したがって，たとえば B_U に対して定期的に還元処理の実行を指示するよう利用者環境を実装するなど，簡単な実装上の対処によりこのリスクを十分に軽減することは可能と考えられる．また，3) については前節 3) で示したように認証子 a_c により保護される．そのため，以下では 1) の課金の不正に対するリスクについて重点的に議論する．

1) の攻撃は，配布コンテンツ c に含まれる課金関数 f_c の改竄により課金額を不正に操作するか，再生手順の手順 (2) における課金処理を行うことなく，復号されたコンテンツ m の部分情報を取得することにより達成される．ここで，前者の f_c の改竄については前述したとおり a_c の検証により検出される．このとき，課金装置 B_U は以降の処理を中断するため，（B_U の耐タンパ性を破らない限り）この攻撃は成立しない．

後者の課金処理の不正回避は，攻撃者 $\mathcal{A}$ がブロック番号 i を B_U に問い合わせることなく（i を入力とした再生手順を実行することなく）c_i から m_i を復号する攻撃を成功させることにより成立する．以下，この攻撃に関し，$\mathcal{A}$ が過去に正しく c_i を再生したことがあるか否かによって，2 種類のセッティングに分けて議論する．すなわち，まったく i を問い合わせることなく m_i を入手しようとする（c_i に対する課金はまったく行われない）場合と，過去に i を問い合わせた際の出力を再利用（replay attack）する（c_i に対する課金は 1 度だけ行われる）場合である．

まず，$\mathcal{A}$ がまったく i の問合せを行わず，c_i の利用に対する課金を完全に回避しようとする場合について議論する．このセッティングでは，$\mathcal{A}$ は，m_i，e_i，k_i，k_0，Sk_B に関する情報以外の任意の情報を知っており，ブロック番号 j（$j \neq i$）の問合せによる k_j の入手は許される．以下，本方式が用いる暗号プリミティブが安全であるならば，$\mathcal{A}$ が攻撃に成功しないことの証明を簡単に示す．

まず，c_i は $c_i = m_i \oplus e_i$ により生成された OTP（one time pad）であり，e_i が未知の乱数であるならば，長さ $|c_i|$ の乱数と区別することができない．ここで，e_i は k_i を初期値とした疑似乱数生成器 e の出力であり，c_i の生成にのみ用いられる使い捨ての値である．したがって，$\mathcal{A}$ が攻撃に成功する条件は，e の出力系列が乱数と区別可能か，もしくは k_i の部分情報を得られることに帰着される．$k_i = k_0(i)$ は共通鍵暗号によりブロック番号 i を k_0 を鍵として暗号化したものであり，$\mathcal{A}$ が k_i の部分情報が得られるならば，k_0 の部分情報が得られるか，$k_0(j)$（$j \neq i$）から k_0 の部分情報を得られる（共通鍵暗号として安全ではない）ことになる．ここで，k_0 は配布コンテンツ c を作成するごとに配布コンテンツ生成装置 G_H が生成する乱数であり，$k_1, k_2, \ldots, k_n$ 以外に k_0 から導出される情報は $k_c = Pk_B(k_0)$ のみである．そのため，$\mathcal{A}$ が k_0 の部分情報を得るためには，G_H が k_0 の生成に用いる乱数発生器の出力が乱数と区別可能か，k_c から k_0 が導出可能（$Pk_B()$ は公

⋆1 なお，これらを署名対象に直接含めると，課金装置に対してすべての微小ブロックを与える必要が生じる．これは，IC カードの入出力性能の制約から，実装上あまり現実的ではない．

開鍵暗号として安全ではない）か，ないし Sk_B を入手するか，のいずれかの条件を満たさなければならない．ここで，仮定により $\mathcal{A}$ は Sk_B に関する情報を知りえない．そのため，本方式が用いる暗号プリミティブについて，以下の条件が満たされるならば，$\mathcal{A}$ は攻撃に成功しない．

(1)　e の出力が乱数と区別できない．
(2)　k_i の生成に用いる共通鍵暗号が安全である．
(3)　k_0 の生成に用いる乱数発生器の出力が乱数と区別できない．
(4)　k_c の生成に用いる公開鍵暗号が安全である．

□

次に，$\mathcal{A}$ が，過去の B_U に対する i の問合せに関する出力を再利用する場合について議論する．この場合，再生手順における B_U に対する i の問合せ時に再生装置 P_U を corrupt する，もしくは B_U–P_U 間の通信路を盗聴することにより，明らかに $\mathcal{A}$ は k_i，e_i，m_i のいずれかを得ることができる．したがって，この場合の安全性は，P_U および B_U–P_U 間の通信路の攻撃者 $\mathcal{A}$（典型的には利用者 U 本人）に対する安全性に帰着される．B_U–P_U 間の通信路の安全性は，（P_U が攻撃者によって支配されないのであれば）P_U に対する認証を含む鍵交換プロトコルを用いて容易に確保することができるが，P_U 自体の安全性は P_U の実装形態に依存する．P_U の実装上の安全性については，次節において改めて議論する．

5.2　実装のフィージビリティ

本節では，本方式を構成する各装置 G_H，B_U，P_U の実装フィージビリティについて，実装可能性と実行性能の観点から議論する[⋆1]．なお，以下の議論において各暗号の鍵長は定数として扱う．

5.2.1　配布コンテンツ作成装置 G_H

本方式において，G_H は共通鍵暗号や公開鍵暗号，ハッシュ関数，疑似乱数生成器など，広く実用化されている一般的な構成要素のみから構成され，また，耐タンパ性などの安全性も求められないことから通常の PC などの計算機を用いて実現可能である．また，G_H の配布コンテンツの作成処理の実行性能について，入出力データ量および計算量のオーダはいずれも $O(|m|)$ である．特に計算量について，実際に $O(|m|)$ の演算を必要とするのは XOR 演算とハッシュ値の計算のみであり，一般的な PC を用いて明らかに十分な性能で実装可能と考えられる．

5.2.2　課金装置 B_U

次に，B_U の実装について議論する．B_U は，課金処理を安全に行うために耐タンパ性を備える必要がある．また，B_U はそれぞれの利用者が保有するため，現時点では事実上 IC カードを用いた実装に実装形態が限られる．IC カードでの実装を前提とする場合，IC カードの処理性能の特性（暗号プリミティブの実行などの演算処理は高速であるが，入出力スループットは数 k〜数百 kbps と低速である）[10),13)] から，特に入出力のデータ量が実用上十分に低く抑えられることが必要とされる．ここで，B_U が関わる各処理，すなわち配布コンテンツの利用における初期化手順と再生手順，およびコンテンツ利用の対価の還元処理手順のそれぞれについて，実装可能性と実行性能を議論する．

まず，初期化手順における B_U の処理内容は，署名検証と還元額の検証のみであり，入力データ長は $|c_0|+hl$ である．また，出力は処理の成功および失敗の通知のみである．ここで，$|c_0|=|d_c|+|f_c|+|k_c|+|a_c|+|Pk_B|$ であるが，このうち $|k_c|$，$|a_c|$，$|Pk_B|$ は利用する共通鍵暗号および公開鍵暗号によって定まる数百ビットの定数であり，IC カードで扱ううえでも特に問題となるデータ量ではない．$|d_c|$ は，扱うコンテンツの最大データ長を $|m_{max}|$，微小ブロックの最小分割単位を u とすると $|d_c|=n\cdot\log_2(|m_{max}|/u)$ ビットとなる．具体的には，最大 2^{32}（$=4\,\mathrm{G}$）バイトのコンテンツを扱い，微小ブロックの最小分割単位を 1 バイトとしたとき，ビットレート 1 Mbps で 10 分の動画コンテンツ（600 M ビット $=75\,\mathrm{M}$ バイト）を 10 秒ごとの微小ブロックに分割（60 分割）した際の $|d_c|$ は，$|d_c|=60\log_2(2^{32+8}|/8)=1{,}920$ ビット（240 バイト）となる．また，$|f_c|$ は課金の複雑さに依存するが，典型的な課金パターンをあらかじめコード化しておく（たとえば，各微小ブロックを同一額で課金する場合は「1」など）ならば，$|f_c|$ は課金パターンの数やパラメータの柔軟性に応じて数バイトから数十バイトの範囲とすることができる．したがって，$|c_0|$ は数百バイト程度となり，実効入出力スループットが 100 kbps 程度の IC カードを利用しても十分に実用的な性能で初期化手順は実現可能と考えられる．

再生手順においては，B_U の入力データ量は $|i|$，出力データ量は $|k_i|$ であり，明らかに入出力はボトルネックとならない．また，処理内容も再生履歴情報 l_c の参照と更新，電子マネー残高の参照と更新，還元額の更新，および f_c の実行と共通鍵暗号処理 $k_0(i)$ の実行のみである．ここで，f_c の実行以外は明らかに実用上ほぼ無視できる処理である．したがって，再生手順の処理性能に関する実用性は f_c の計算時間に依存するが，典型的には f_c は暗号処理と比較して，より単純な演算処理のみによって構成されるため，実用上ほぼ無視で

⋆1 提案方式において R_H に求められる機能は，B_U との間での公平交換プロトコルの実行だけであるため，その実装の詳細については本稿では議論しない．なお，IC カードを用いた公平交換プロトコルの実現可能性に関しては，後述のとおり文献 13) により示されている．

きる計算時間になると考えられる．

還元処理は，R_H との公平交換プロトコルの実行と b_H の削除から構成される．したがって，還元処理の実装可能性は IC カードを用いた公平交換プロトコルの実装可能性に帰着される．これに関しては，文献 13) により市販の IC カードを用いて楽観的な公平交換プロトコルが実用的な性能で実装可能であることが示されている．

したがって，B_U はいずれの処理についても実用上十分な性能で安全に実装可能と考えられる．

5.2.3　再生装置 P_U

P_U は，再生手順において B_U に i を与えることによる k_i の取得，疑似乱数生成器による k_i から e_i の生成，e_i と c_i との XOR 演算による m_i の生成，および m_i の再生を行う．P_U を通常の計算機上でソフトウェアとして実現した場合，これらの処理は（m_i の再生負荷が問題とならないなら）明らかに性能上の問題なく実現できる．ただし，この場合は前節で示した再利用攻撃に対する脆弱性が発生し，いったん m_i を利用したあとの，再度の利用に対する課金を保証できない．

この問題への対策は，DRM システムにおける安全性の保証と同じ困難さをともなう．たとえば，P_U の実装への難読化の実施などはカジュアルな攻撃に対して有用と考えられるが，MAC（mandatory access control）が保証できないシステムにおいて，ソフトウェア的な手段のみで完全な対策を行うことは難しい．したがって，現行の DRM システムと同様に，ある程度の不正リスクを前提としてシステムを実現するか，もしくは携帯電話やハードウェア再生機器など，利用者が容易に改竄もしくは内部情報を参照できない機器を用いて P_U を実装することが必要となる．

5.3　関 連 方 式

本稿では，UGC の提供者に対価を提供する原資として，利用者のコンテンツ利用に対する課金を前提としたが，それ以外にも原資を確保する手段は存在する．OECD の報告書[15),16)]によれば，UGC[⋆1]から収益をあげる（monetise）ための手段は以下に分類できるとされる．

(1)　自発的な寄付（voluntary donations）
(2)　視聴者への課金（charging viewers for services）
　(a)　コンテンツごとの課金（pay-per-item model）
　(b)　利用契約による課金（subscription model）
(3)　広告モデル（advertising-based models）
(4)　第三者へのライセンス提供（licensing of content and technology to third parties）
(5)　物販・サービス販売（selling goods and services to community）

上記の分類において，2 章で議論した配布時課金および利用課金方式，および提案方式はいずれも (2a) のコンテンツごとの課金に相当し，期間課金方式は (2b) の利用契約による課金に相当する．

(1) の自発的な寄付と (2) の視聴者への課金を除くと，(3)〜(5) の各方式はいずれもコンテンツの直接の利用者以外から原資を確保する，間接的な収益確保方式である．これらの方式は利用者からコンテンツ利用の対価を求めることがないため，利用者にとってはリスクなく UGC を利用できるという利点があるが，その一方で，間接的な原資の確保だけでは，(特に動画など広帯域を必要とする配信システムにおいて）少なくとも現状はコンテンツ提供者への収益の分配以前に UGC を配信するための配信システムを運用するための費用を確保することも難しいとされる．また，利用者にとってコンテンツ利用のリスクがないことから，2 章で述べた期間課金方式における課題と同様に，収益分配における不正を防ぐことが課題となる．

本方式は，これらの間接的な収益確保の手段と矛盾することなく併用することができる．さらに，本方式の併用により，上記の収益分配における不正を抑制する効果が期待される．たとえば，本方式における利用者からの対価に対し，間接収益を比例配分などにより上乗せしてコンテンツ提供者に分配することを考える．このとき，少額ながらもコンテンツ利用に対して利用者に課金がなされることになるため，不正な利用者によるサクラ行為による攻撃のインセンティブを抑える効果を期待できる．

また，3 章で議論したように，提案方式はレモン市場化への対策として「取引の繰返し化」の方針を採用している．レモン市場化への対策としては，その他にブランドの強化や利用者に対する商品に関する情報提供の積極化などが知られている[1)]．特に，Yamagishi ら[17)]によれば，評判管理システム（reputation management system）を用いた提供者に関する評判情報の提供が，消費者間の取引市場におけるレモン市場化の抑止に効果があるとされており，このアプローチを UGC 市場に適用し，そのレモン市場化を防止する方式が野秋ら[21)]により提案されている．評判情報の提供は本稿の提案方式と矛盾なく併用することができる．ただし，文献 21) では，評判情報を正しく与えるインセンティブとして，評判情報の提供者にも収益を分配するこれらの方針を提示している．この場合は，本稿で示した還元処理に修正を加える必要がある．

⋆1 文献 15), 16) では UCC（user-created content）と呼ばれている．

なお，4 章において提案した UGC の逐次微小課金の実現方式は，超流通（superdistribution）[6] の特徴としてあげられている，1) ソフトウェア製品（software product，提案方式における UGC に相当）それ自体は無償で制限なく配布され，利用者は製品を保有ないし取得することに対して課金されず，2) 製品提供者は製品の利用条件や利用料金を必要に応じて設定可能であり，3) 左記の利用条件を満たし利用料金を支払うならば，適切な利用環境を持つ利用者は誰でも製品を利用でき，4) 耐タンパ性を備えた利用環境が左記の製品の利用可否に関するエンフォースメントを行う，などの条件を満たす．したがって，4 章の提案方式は超流通モデルを実現する方式の 1 つとして位置付けることができる．

上記の条件を満たす超流通の実現方式として，文献 23) のほか，UDAC-MB [20] や OMA DRM [8]，Windows Media Rights Manager [5] などの各種のライセンス分離型 DRM 方式（もしくはライセンス分離に対応した DRM 方式）など，数々の方式が提案されている．

ただし，2 章および 3 章で議論したように，UGC への適用に対しては，さらに 5)（レモン市場化を防止するために）擬似的な取引の繰返し化（= 逐次微小課金）を実現すること，6) 逐次微小課金および対価の還元の手段の提供にあたっては，（それぞれ不特定多数である）コンテンツの利用者もしくは提供者に対して不公平にならない[⋆1]こと（3 章設計目標 (1)，(2)），7) 左記 5)，6) を実用的な構成および性能で実現可能であること（同設計目標 (3)），などの要件に対応することが求められる．従来の超流通実現方式との対比という観点では，提案方式はこれら 5)〜7) の要件をあわせて実現していることが特徴となる．

また，文献 24) は，コンテンツから内容に着目した「部品（コンテンツ中の特定人物など）」を分割して抜き出し，個々の部品に対して個別に電子透かしを埋め込んだうえで，それぞれ異なる鍵で暗号化して配布する（超流通モデルに適用可能な）コンテンツ配信モデルを提案している[⋆2]．このモデルは，部品に埋め込んだ電子透かしの組合せにより，（正当に支払いがなされた）復号コンテンツに対して，支払い者ごとに一意な識別情報を与えることを可能とする．つまり，復号コンテンツの不正な二次流通に対し，不正者を追跡する手段を提供する．

この技術自体は逐次微小課金の手段を提供せず，また，3 章で示した設計目標を満たさないが，提案方式と組み合わせることにより，（再生装置の出力などから取得された）コンテンツの不正な二次流通を抑止する効果を与えることが期待できる．すなわち，提案方式とは補完関係に位置する技術と考えられる．

ただし，上記技術により分割されたコンテンツ部品の合成は，計算量，データ量ともに提案方式と比較してコストが高い処理を必要とする．そのため，コンテンツ利用時における課金のエンフォースメントを実現する手段として提案方式のように IC カードを用いることは，少なくとも現状では困難と考えられる．したがって，上記技術の併用による二次流通の抑止手段の提供にあたっては，安全かつ実用的なエンフォースメント手段をいかに実現するかが課題となる．

なお，現状の UGC における課題としては，本稿で議論の対象としたコンテンツ提供者への適切な収益の分配のほかに，著作権法違反コンテンツや不適切コンテンツなど，法的もしくは社会的に不正とされるコンテンツへの対処があげられる．利用者による自発的な利用停止以外に，提案方式はこの問題への有効な対策を提供しない．そのため，この問題に対しては，不適切コンテンツの通報やコンテンツの類似度判定によるオリジナリティの検証など，別途の対策手段が必要となる．

6. おわりに

本稿では，UGC の有償流通に対して従来のコンテンツ販売方法を適用する際の課題分析を通じ，コンテンツの質に関する利用者リスクの観点からレモン市場化の懸念があることを示すとともに，その対策として IC カードを用いたコンテンツ利用の逐次微小課金方式を提案した．提案方式は，コンテンツの利用における逐次的な微小課金の繰返しを安全かつ効率的に実現することにより，レモン市場化への対策の 1 つとしてあげられる「取引の繰返し化」を UGC 市場において実現する．また，提案方式の安全性について，コンテンツ提供者とコンテンツ利用者のそれぞれの観点から考察し，実用性について現行の IC カードを用いて実用的な性能で実装可能なことを示した．

提案方式は，OECD の分類における UGC からの収益手段の 1 つである「視聴者への課金」を実現する手段に相当し，それ以外の間接的な収益手段とも効果的に組み合わせることが可能である．ただし，法的・社会的に不正なコンテンツへの有効な対策を本方式自体は提供しないため，実用にあたってはこれらに対処する手段を併用する必要があると考えられる．

⋆1 不特定多数の提供者によりコンテンツが提供されるという UGC の特徴から，不特定多数のコンテンツ提供者に対して適切に対価を還元可能であることが UGC の課金および対価還元における特徴的な要求の 1 つとなる．
⋆2 文献 24) は静止画を対象として議論しているが，原理的には動画像にも同様のモデルが適用可能である．

参 考 文 献

1) Akerlof, G.A.: The Market for 'Lemons': Quality Uncertainty and the Market Mechanism, *Quarterly Journal of Economics*, Vol.84, No.3, pp.488–500 (1970).
2) Asokan, N.: Fairness in Electronic Commerce, Ph.D. Thesis, University of Waterloo (1998).
3) eMarketer: Can User-Generated Content Generate Revenue? (2008).
4) Kleemann, F., Voß, G.G. and Rieder, K.: Un(der)paid Innovators: The Commercial Utilization of Consumer Work through Crowdsourcing, *Science, Technology & Innovation Studies*, Vol.4, No.1, pp.5–26 (2008).
5) Microsoft Corp.: *Taking Advantage of Super Distribution* (2007). Windows Media Rights Manager 10.1.2 SDK Programming Guide.
6) Mori, R. and Kawahara, M.: Superdistribution: The Concept and the Architecture', *Trans. IEICE*, Vol.E73, No.7, pp.1133–1146 (1990).
7) Morphy, E.: The Dark Side of Crowdsourcing, LinuxInsider (2009).
8) Open Mobile Alliance: DRM Specification V2.0 (2005).
9) Pagnia, H., Vogt, H. and Gärtner, F.C.: Fair Exchange, *The Computer Journal*, Vol.46, No.1, pp.55–75 (2003).
10) Rankl, W. and Effing, W.: *Smart Card Handbook*, 2nd edition, John Wiley & Sons (2001).
11) Rivest, R.L. and Shamir, A.: PayWord and MicroMint–Two Simple Micropayment Schemes, *Proc. 1996 Intl. Workshop on Security Protocols*, LNCS, No.1189, pp.69–87, Springer (1996).
12) Terada, M., Iguchi, M., Hanadate, M. and Fujimura, K.: An Optimistic Fair Exchange Protocol for Trading Electronic Rights, *Proc. 6th Smart Card Research and Advanced Application IFIP Conference* (*CARDIS2004*), IFIP, Vol.153, pp.255–270, Kluwer (2004).
13) Terada, M., Mori, K., Ishii, K., Hongo, S., Usaka, T., Koshizuka, N. and Sakamura, K.: A Framework for Distributed Inter-smartcard Communication, *J. Information Processing Society, Japan*, Vol.47, No.2, pp.534–546 (2006).
14) Verna, P.: User-Generated Content: More Popular than Profitable, eMarketer Reports (2009).
15) Vickery, G. and Wunsch-Vincent, S.: *Participative Web and User-Created Content: Web 2.0, Wikis and Social Networking*, OECD Publications (2007).
16) Wunsch-Vincent, S. and Vickery, G.: Participative Web: User-Created Content, Technical Report DSTI/ICCP/IE(2006)7/FINAL, Committee for Information, Computer and Communications Policy, OECD (2007).
17) Yamagishi, T. and Matsuda, M.: Improving the lemons market with a reputation system: An experimental study of internet auctioning, Hokkaido University (2002).
18) アイシェア：携帯電話の動画共有サービス利用とその著作権に関する意識調査 (2008).
19) ネットエイジアリサーチ：ケータイの動画コンテンツ視聴に関する調査 (2008).
20) 穴澤健明，武村浩司，常広隆司，長谷部高行，畠山卓久：コンテンツ保護の柔軟化を実現した開放型超流通基盤，情報処理学会研究報告 EIP-118，pp.31–42 (2001).
21) 野秋浩三，寺田雅之，関野公彦：なぜ UGM 市場は生まれないか？，コンピュータセキュリティシンポジウム 2008 予稿集，情報処理学会 (2008).
22) 服部　昇，菅野政孝：マイクロペイメント：デジタルコンテンツ流通のキーを握る決済手段（情報処理最前線），情報処理，Vol.39, No.1, pp.1–5 (1998).
23) 早川　豊：コンテンツ情報記録装置，課金システム及び課金方法，特開 2003-115017 (2003).
24) 高橋由泰，青木輝勝，安田　浩：階層化コンテンツ超流通システム，情報処理学会研究報告 EIP-85，pp.25–32 (2001).

(平成 21 年 5 月 25 日受付)
(平成 21 年 12 月 17 日採録)

寺田　雅之（正会員）

1995 年神戸大学大学院工学研究科修士課程修了．同年日本電信電話（株）入社，電子権利システムの研究開発に従事．2003 年（株）NTT ドコモへ転籍．以後，電子商取引における公平性保証方式，統計開示におけるプライバシ保護方式等，情報セキュリティ技術の研究開発に従事．博士（工学）．電子情報通信学会，IEEE 各会員．

野秋　浩三

2005 年東京大学大学院新領域創成科学研究科修士課程修了．同年（株）NTT ドコモ入社．以来，情報技術セキュリティ評価基準の研究開発を経て，現在，次世代モバイルサービスの研究開発に従事．

青野　　博（正会員）

1989 年日本電信電話公社入社．オブジェクト指向設計法の研究，それを利用したネットワークマネジメントシステムの研究開発，セキュリティの研究開発等に従事．電子情報通信学会会員．

関野　公彦

1988 年東京大学理学部情報科学科卒業．同年日本電信電話（株）入社．以来，リアルタイムオペレーティングシステム，情報セキュリティ技術の研究開発に従事．（株）NTT ドコモにて，モバイル公開鍵基盤の開発を経て，現在，次世代モバイルサービスの研究開発に従事．

本郷　節之（正会員）

1984 年岩手大学大学院工学研究科修士課程修了．同年日本電信電話公社入社．以後，ATR 視聴覚機構研究所，NTT ヒューマンインタフェース研究所にて視覚情報処理モデルの研究に従事．1999 年（株）NTT ドコモへ転籍．マルチメディア研究所セキュリティ方式研究室長着任後，モバイルセキュリティ技術の研究開発に従事．博士（工学）．電子情報通信学会会員．