DRM 機能を持つ決済システムについて

「天野　光司」1*　　「塚本　克治」2
「工学院大学情報学専攻修士２年」1　　「工学院大学教授、　LINCS 所長」2

1. はじめに

近年、一般家庭へのインターネットが急速に普及し、決済システムでは、代金引換からクレジットカード決済や、電子マネー決済へと広がりを見せ、決済がインターネット上で行われる事が多くなって来ている。また、商品もパッケージ流通から情報コンテンツ流通へと変化し始めている。このような社会背景に対し今回試作するシステムでは、ユーザがセキュリティを特に意識する事なく利用でき、システム側では様々な認証を用い、安全性を確保できるようなセキュリティ設計を試みた。

DRM に配慮した電子決済システムにおける一部試作を紹介しながら考察していく。

2. 現状の整理

コンテンツの流通には様々な社会的要因も関係するのため、システムの説明の前に社会的背景の把握、問題の洗い出しを行う事にする。

(1) e コマースの背景

e コマースはどのような問題を抱えるのであろうか。インターネット犯罪を示す資料や統計はあまり存在していない。それは、資料が直接システムや、セキュリティに反映されるため、なかなか公に出ない状況があるためだろう。また、e コマースでは、決済方法として決済代行機関（カード会社等）が使用される事が多い。そこで今回は、

末藤高義『クレジットカード犯罪トラブル対処法』民事法研究会
を参考して問題点をまとめた。

e コマースの普及に伴い、クレジットカード番号の入力を求められたる事が多くなってきた。そのカード業界では出資法上限金利の引き下げ、金融再編成、IT の発展の影響を受けると共に、消費者金融との連携、コンビニや自動車会社などの参入、アウトソーシング、IC カードへの移行、ハウスカードの増加、インターネットや携帯電話への対応、収益構造の見直等により、今後の進むべき道を模索している。

インターネット決済方式を表１に示す。

表1インターネットショッピングの決済方法

銀行振込、郵便振替	指定口座に代金振込み、確認後商品発送
代金引換	宅配業者に品物引き換えに現金を渡す（クレジットカードで払うことが出来る場合もある
クレジットカード	カード情報をネット上の HP に入力
コンビニ決済	売り手が通知する番号により、買い手がコンビニから商品を受け取り、代金を払う
プリペイド方式	コンビニで事前にカードを購入。このカード情報を入力して代金を支払う
ネットバンキング	インターネットバンキングの応用
ネットデビット	同上。普通預金口座開設者に ID を与え、買い物をした際、この ID を入力すると、口座から代金が引き落とされる
プロバイダー料金に上乗せ	プロバイダーに毎月支払う利用料に、商品購入代金をオンしてクレジットカードで支払う。

出典：アクセンチュア（株）調べ

表１におけるクレジット決済の比率は日々増している。しかし、不正行為と犯罪も、増加の一途をたどっている。日本で、２００１年の１年間に発生したクレジットカード不正使用による被害額は、276 億円（うち、偽造カードによる被害額は 146 億円）に達している（日本クレジット産業協会調べ）。

カード情報に関する危険性については、

1:スキミング
2:偽造カード使用
3:ATM が関係する犯罪
4:虚偽申請

などが問題とされ、カード決済における犯罪については、

1:ユーザのなりすまし。
2:他人 ID・パスワードの覗き見、盗用。
3:詐欺・代金を受けて商品を送らない。
4:不法商品売買、他人名義の銀行口座使用。
5:カード情報、クレジットマスター、

クレジットウィザードの悪用。
6:身に覚えの無い請求。
7:不正アクセス
8:データ消去、改竄
9:個人情報漏洩、プライバシー保護
10:脅迫・恐喝
11:二重請求
12:伝票横流し
13:不良加盟店（POC 等）
14:チャージバック
など、システム設計やセキュリティシステム設計において念頭に置く必要性がある問題は多い。

これらの問題に対し、ガード会社はどのようなシステムを提供するのか。それについての記事を以下に示す。

{VISA、国内メンバーカード会社 7 社とインターネット向け本人認証サービス開始

従来のインターネットにおけるクレジットカード決済は、カード番号と有効期限、氏名を入力することで購入手続きが済んでしまう E コマースサイトが多く、カード番号(と期限)が盗まれた際に“なりすまし”による不正利用の可能性があったという。

VISA 認証サービスでは、Visa が開発したインターネット向けセキュリティープロトコル“3-D セキュア”を利用して、カード番号と有効期限、本人専用パスワードを、エンドユーザーとカード発行会社の間でやりとりし、カード発行会社が直接本人認証を行なう。パスワードの入力は、E コマースサイトのウインドーと別のウインドーで行なうため、E コマースサイト側にもパスワードは見えない。これによって、単純ななりすましだけでなく E コマースサイトぐるみの不正も防げる仕組み。

なお、3-D セキュアにおけるデータ通信は SSL(Secure Socket Layer)によってすべて暗号化されている。エンドユーザーは基本的に SSL 対応のウェブブラウザーを用意すればよく、パソコン以外の PDA や携帯電話での決済にも対応できる。ただし、本人認証の方法はカード発行会社が決定できるもので、パスワード以外に、IC カードや、指紋などのバイオメトリクスなどが考えられ、そうした場合は特別なハードウェアやソフトウェアが必要になる。

ビザ・インターナショナル・アジア太平洋地域の e-Visa 担当シニアバイスプレジデント、マーク・バービッジ(Mark Burbidge)氏は

「実際にクレジットカード番号を盗んだりするためには、インターネットから盗むよりもずっと単純で簡単な方法があるにもかかわらず、消費者の 8 割がインターネットでのクレジットカード決済に不安を持っているという調査結果がある。実際にハッキングを受ける可能性は非常に小さいものだが、消費者が不安に思うことが問題だ。」

と述べてた。}

(ASCII24_2002 年 7 月 22 日)

カード番号、有効期限、氏名、本人専用パスワードの情報が第三者に漏れた場合、既存のカード決済のセキュリティ問題と同様の問題が生じる。もし、その問題の解決を図るとしたら、記事における「本人認証の方法はカード発行会社が決定できるもので、パスワードパスワード以外に、IC カードや、指紋などのバイオメトリクスなどが考えられる」と言う部分である。ここで、どんな認証システムを採用するかによってシステムが大きく変化する。指紋などのバイオメトリック認証を適応するならばオーソリ請求を必要とし、逆に IC カードによってスタンドアロン認証を行えば、オーソリ請求 1 回に掛かる 10 円～30 円の料金を節約する事が出来る。このため、認証システムは任意ではあるが、慎重に選ぶ必要性があると考えられる。

(2)　著作権関係の背景

アメリカでは Apple Computer がオンライン音楽サービス「iTunes」を開始し、システムは現在大成功を納めている。これに続き多くの企業が音楽ダウンロードサービスの提供の準備を進めている。今後、音楽を情報コンテンツと一般化し、様々なサービスが誕生することは必然的なことである。

{上院の常設捜査小委員会議長を務めるノーム・コールマン議員は 7 月 31 日、RIAA に宛てて、一連の召喚状について批判し、発表文で「この業界が著作権侵害について懸念するのは当然のことだ。しかし業界が採用している無差別的なアプローチは、無実な相手までも傷つけてしまう恐れがある」と述べている。 }

(ZDNet2003 年 8 月 2 日)

{ダウンロード購入した音楽の転売は“アリ”か？

iTunes Music Store で購入された音楽ファイルがオークションに出されている。「オンライン音楽サービスをめぐる問題提起」という目的が愛好家の共感を呼び、99 セントの楽曲に 1 万 5000 ドル以上の値が付いている。

ミシガン州アナーバー在住の Web 開発者ジョージ・ホテリング氏は、違法コピーを防止するためのデジタル権利管理（DRM）技術をはじめとする、商用オンライン音楽サービスをめぐるいくつかの難題を検証することが狙いという。そうした考えから、同氏は落札価格が購入時の価格を上回った分については電子フロンティア財団（EFF）に寄付すると明言している。

EFF のローマン氏は、転売に関する問題は、商用オンライン音楽サービスをめぐって表面化しつつある、ほかの未解決の法的問題を提起することにもなるだろうと指摘している。例えばユーザーがオンラインでダウンロードした楽曲を貸し出したり寄贈したりする権利なども、そうした問題の 1 つという。

1 ドル足らずで購入できる楽曲に何百ドルも支払うというのはあまり理にかなっていない。だが、少なくとも入札者の 1 人は「音楽業界がデジタル販売に力を注ぐ中、自分の入札によって重要な問題の提起に貢献したい」といった内容のメールを送ってきている。

カナダのバンクーバー在住の IT 管理者ジェフ・グラント氏は、「自分は本気で入札した。ただし、その狙いは楽曲を購入するためではなく、音楽業界がわれわれ消費者の権利をないがしろにしているという事実について問題提起することにある」とメールに記している。

かつてレコード会社やミュージシャンと仕事をしたこともあるという同氏は、さらに次のように続けている。「問題は多数ある。今回のオークションは、ダウンロードした楽曲については、果たして自分が所有していることになるのか、ライセンスはどうなっているのかといった問題を提起している。音楽業界は、購入後の楽曲を消費者がどのように扱うかを完全に管理しようとしているように思われる」 }
(ZDNet2003 年 9 月 4 日)

{ダウンロード音楽のオークションが中止に

eBay は 9 月 4 日、Apple Computer のオンライン音楽サービス「iTunes Music Store」で購入した音楽ファイルの転売を試みたオークションを、同社の出品規約に違反するとの理由で中止した。

Apple が iTunes サービスを 4 月に立ち上げた際（4 月 30 日の記事参照）、スティーブ・ジョブズ CEO（最高経営責任者）は、消費者は音楽をレンタルするのではなく、所有したいのだと宣言した。だが、もし転売に関する規制が適用されれば、「所有モデル」というよりもむしろ「レンタルモデル」に近いものになる。}
(ZDNet2003 年 9 月 5 日)

これらの記事はアメリカにおけるユーザと著作権保護に関係する機関、政府の動きを浮き彫りにしている。最後に提示した記事の拡張として、息子がひとり暮らしをする時デジタルコンテンツを家に置いて行ったり、持って行ったりすることが出来るのか？また、娘が嫁ぐ時デジタルコンテンツを花嫁道具に含める事が出来るのかについても考える必要性が出てくるであろう。

日本においても著作権について動きがあった。これまで著作権管理団体は仲介業務として国の許可を受けた著作権管理団体が行っていた。それが、2001 年 10 月の改正により、「著作権管理事業法」が施行され、法人であれば誰でも著作権管理事業に参入が可能になり、事業者は文化庁長官に必要事項を届け出れば、著作権管理ビジネスに参入することが出来る事となった。既に３０以上の管理機関の誕生している。

管理事業者が取り扱う著作物の種類についても、「楽曲、楽曲を伴う場合の歌詞、小説、脚本」に限られていたが、新制度では、「著作物の種類を問わない」となった。これにより、デジタルコンテンツからプログラムまで様々な著作物が対象となるばかりでなく、著作物のライセンス情報自体もまた、著作物として著作権管理が可能となる。これにより超流通システムも円滑に稼動出来るようになる。

日本のコンテンツ配信についての状況を新聞や報道では「米国に比べて、かなり遅れている。」「キラーコンテンツ次第」と伝えているが、以下の記事に注目したい。

「日本製アニメ、米で 5200 億円市場・・・ジェトロ調査

米国における２００２ 年の日本製アニメの市場規模が推定で４３ 億６０１１ 万ドル（５２３２ 億円）に達したことが、日本貿易振興会（ジェトロ）の調査で分かった。米国が同年に日本から輸入した鉄鋼製品額の約３ ・２ 倍に相当する規模に当たる。」
(msn ニュース 2003 年 8 月 14 日)

日本には既に世界に誇れるキラーコンテンツが存在している。「キラーコンテンツ次第」という話は過去の見解と言えるだろう。今、必要なのはそのコンテンツを配信、使用するインフラの設計及び整備である。また、コンテンツを提供する相手は誰かという問題も同時に考える必要性がある。コンテンツを提供する相手は、無味乾燥なコンピュータではない。また、指紋や虹彩、耳によって厳重に管理された人間 1 人のみでもない事に留意しなければならない。

様々な企業と意見交換を行ってきたところによると、日本の場合、著作権保護に対する考え方は極めて弾力的で、コンテンツ対価が正当に支払われるならば、その配信システム及び管理システムについては、それほど厳格に縛る必要はないと考えている事が分った。しかしながら大胆なシステムを会社として発表する事に対しては極めて慎重である事も同時に伺い知る事が出来た。

ユーザが何を求めるのかも重要である。ユーザの関心は世界的に見てストリーミング型からダウンロード（所有）型へ変化しつつある。さらに、前記の米国の記事のように、同一コンテンツでありながら、パッケージ購入とネット購入で使用できる範囲が違う事はユーザが困惑する 1 つの要因である。また、使用権が１アカウント、もしくは 1 台のマシンに固定されていた場合、親（支払い能力のあるユーザ）が購入したコンテンツを子（支払能力が無いユーザ）が使えない。子供はどのようにして、インターネット決済を経てコンテンツの使用権利を得れば良いのであろうか。

コンテンツには使用誓約書が付いているが、それを完全に理解し、同意ボタンを押せる未成年者がどれほどいるのかも考慮する必要性がある。権利や、誓約を理解しない世代にいきなり警告文が送られてきて、「盗用の念を否めない」や、「法的手段も辞さない」などの文面を見たときの衝撃は想像を絶するものがあるだろう。このような情報化社会が日本が目指す e ジャパンなのかも考える必要性がある。

3. システム全体のフレームワーク

今回、決済システムが導入される市場を、著作権保護が必要なデジタルコンテンツ配信市場と設定した。その中で、著作権問題と決済を組み合わせた新しいタイプの情報コンテンツ流通、課金決済システムを考えていく。その骨格となるものが、下記のフレームワークである。

「端末装置から配信を要求されたコンテンツ等の著作権保護情報を暗号化する場合において、課金の徴収を行う先を単位とし、暗号化及び、復号化を行う鍵を作成する。

同じ徴収先として登録された端末装置において、前記機能で暗号化された情報を復号化し使用できるようにする。」[特願 2001-292542]

これにより、お金を払う事によって、使用権利が得られる。「家庭での鑑賞を許可する」という権利範囲を言葉だけでは無く、システマティックに定義、管理する事が可能となる。また、エンタープライズにおける部署等のグループユーザに適応する事も可能となる。

決済システムにおいては、自作電子決済システム「ぽけマネー」システム、「Login 認証」「赤外線認証」「Mozichi」「ダブルライセンス」「Trust_Back」など様々なアイデアを盛り込んでシステムの設計、構築を行っていく。

４． e コマースにおけるアプローチ

今回のシステムの 2 本柱のうちの 1 本は e コマースにおける決済システムである。決済システムに必要な最低限の機能は、
・デジタルコンテンツの課金を行う機能、
・コンテンツを購入する客のダブルライセンス情報の取得機能、（ダブルライセンスについては、著作権におけるアプローチを参照）
・コンテンツに応じたライセンスを発行、送信する機能である。

今回はユビキタス決済システムの一例として、携帯電話を利用した自作電子決済システム「ぽけ

マネー」システムを導入する。

(1) e コマース事例

ここでは、e コマース事例として主にコンテンツの決済を行うシステムを取り上げる。

図 1 にシステム当事者を示す。

図 1　ぽけマネーシステムの当事者

左の携帯は「ぽけマネー」システムのクライアント側 i アプリである。右 1 番目の「PokeMoney」は、ぽけマネーのサーバセンターである。右 2 番目の「AccessBank」はユーザ取引銀行である。右 3 番目の「スペースソフトウェア」はインストール型ソフトウェアと、Web 上でのアプリケーションサービスを行っている会社である。右 4 番目の「Media_online」は楽曲、映画、写真等のストリーミング及び、ダウンロード型コンテンツを配信している企業という設定になっている。

今回以下の 3 つを例に挙げて、決済とライセンス管理について考察する。

事例 1:　ネットからのコンテンツの購入

事例 2:　ネットアクセスライセンスの購入

事例 3:　POS レジでのコンテンツ購入

(2)「ぽけマネー」システムの機能

「ぽけマネー」はインターネットショッピングにおける支払いに対応している。パッケージ商品の支払いばかりでなく、著作権付き情報コンテンツの決済システムにも対応してい点が最大の特徴である。

ぽけマネーの機能を以下に記す。認証に必要な機能として

・パーソナルデータの書面からの登録

・パーソナルデータのダウンロード

・パーソナルデータの保持

・端末 Login ユーザ認証機能

・Internet パスワード認証機能

・ライセンス引用型 Internet パスワード認証

・端末認証機能

・サーバ認証機能

・赤外線認証機能

支払い機能として

・ユビキタス銀行取引（Master ユーザのみ）

・赤外線によるユビキタス支払い

・ネットショッピングでのユビキタス支払い

・請求書に対するユビキタス支払い

・ユーザ-ユーザ送金機能(Internet)

・ユーザ-加盟店送金機能(Internet)

・ユーザ-銀行送金機能(Internet)

ユーザサービスについての機能として

・Login 画像の設定（著作権付き無料/有料コンテンツ）

・ニュース/レシート/ライセンス情報の保持（ライセンスはネットアクセス/コンテンツ/コンテンツダウンロードの 3 種類）

・ニュース/レシート/ライセンス情報のダウンロード（ダウンロード手段はサイト/メール/赤外線）

・ニュース/レシート/ライセンス情報の赤外線送信（ライセンス転送はライセンス情報により転送可否が決まる）

・情報削除機能

ダブルライセンス関係の機能とその他の機能

・ライセンス情報の暗号化

・ぽけマネーファミリー機能

・ぽけマネーファミリー情報の保持

・ぽけマネーファミリーID 引用機能

・ぽけマネーヘルスチェック機能

・カスタマーセンターコール機能

今回はデジタル著作権保護機能を有しているため、前記のフレームワークに従い、コンテンツ使用において同一ファミリーとなるユーザは同一課金徴収先を指定する形になる。今回は「AccessBank」を同一課金徴収先として指定している。親の口座資金が幾ら豊富でもそれを勝手に子供が使用する事は望ましくない。そこで、今回は親からの送金という手続きにより、Family ユーザの「ぽけマネー」システムにデポジットするシステムを適応した。

(3)事例 1:　ネットからのコンテンツの購入

今回は、「ぽけマネー」システムの Login 画面に「Media_online」の有料コンテンツを設定するシステムを例に取る。

図 2 に一連の作業で表示される「ぽけマネー」画面を示す。

図 2　「ぽけマネー」画面

上段左：Login 画面、

上段右：main 画面

中段左：Info_Box[ ]の中身、

中段右：License_Box[ ]の中身

下段左：License 表示画面

下段右：有料 Login 画像の登録完了画面

以下に決済手順を示す。

1:ユーザはブラウザ機能を使い、購入したい写真、イラストを選択する。

2:決済ボタンを押し、「ぽけマネー」での決済に移る。

3:「ぽけマネー」i アプリはブラウザより LaunchUp される。

4:Login 画面によりユーザ認証(スタンドアロン認証）を行う。

5:決済の確認画面より「Yes」を選択し決済に移る

6:サーバとの通信が始まり、サーバ認証、端末認証（Mozichi 認証）を行う。

7:認証が終了したら決済に入る。

8: ダブルライセンスを「ぽけマネー」クライアントに発行する。

9:電子レシートを発行

10:コンテンツがダウンロードされ、Login 画面に設定される。

11:再起動をかける。

コンテンツダウンロードと保存でエラーが生じた場合でもライセンスのダウンロードが完了していれば、不要な料金を支払う事無くユーザは直接コンテンツをダウンロードする事が出来る。

(4)事例 2:　ネットアクセスライセンスの購入

「スペースソフトウェア」の Web サービスのライセンス購入の場合、流れは以下のようになる。

1:から 7:までは上記と同じである。

8: ライセンス情報として、Internet における ID とパスワードを発行する。

9:電子レシートを発行

10:ユーザはライセンス一覧表の中から目的のライセンスを選びネット接続ボタンを押す事で、煩雑な入力作業を行う事無くサービスを受ける事が出来る。

(5) 事例 3:　POS レジでのコンテンツ購入

リアルショップにおける POS レジでの支払いは以下のようになる。

1:パッケージを持ってレジへ行く

2:赤外線でレジから商品情報を受け取る

3:支払いを了承する。

（この時ダブルライセンス情報を送信する）

4:ライセンス発行を行う。

5:レシート発行を行う。

6:コンテンツのインストールを行う。

7:シリアルナンバー入力の代わりに赤外線で携帯電話内のライセンス情報を転送する。

5.　各機能の設計ポイント

ここでは、今回自作した機能の根拠と役割を記す。

(1) 入会審査

入会審査は主に違法な他人名義銀行口座使用防止のために行われる。入会審査においては、平成 15 年 1 月より施行された「金融機関等による顧客等の本人確認に関する法律（本人確認法）」に従

って、運転免許証、パスポート、健康保険証、住民票の写しのいずれかの確認により行っている。登録は必ず書面で行い 3 箇所ないし 4 箇所の捺印を必要としている。ファミリーメンバーへの登録も書面で行われるがファミリーメンバーがシステムを利用できるようにするためには、赤外線認証を別途必要としている。赤外線認証については後で記す。
図 3 に入会申請書例を示す。

図 3 入会申請書例（三井住友 VISA）

(2)Login 認証

Login 認証は主にユーザ認証のために行う。ぽけマネーシステムのユーザが自分の「ぽけマネー」を第三者に使用されたり、ニュースやレシートライセンス情報を見られたくないという要望を満たす事を目的としている。

既存のカード規約には「暗証番号は他人に知られないよう、厳重に保管してください。暗証番号を必要とする取引において、第三者による不正利用が行われた場合の損害は、全て会員のご負担となります。」とあるにも関わらず、たった 4 桁の暗証番号しか設定出来ないのは問題があると感じたため、今回の認証はスタンドアロン環境で行われ、ユーザは自分の覚えやすい PIN を設定出来るようにした。このとき「ぽけマネー」センターには Login 認証用の暗証番号は通知されない。

(3)インターネット認証

インターネット認証は既存 PIN を使った認証であるが、今回は PIN の使用頻度は少ない。インターネット認証は主にユーザ認証のために行うが、こちらは Login 認証と違い、「ぽけマネー」センターが PIN を管理している。「ぽけマネー」センターからのパーソナルデータのダウンロードや、認証システムが認証不可状態になった場合等に使用されるだけなので、使用頻度は極めて少ない。

カード犯罪見逃せない問題となっているオーバーザショルダー（肩越しに ID と PIN を覗き見される問題）は PIN 入力による成りすましを引き起こす。PIN の入力頻度が高ければ高いほどなりすましを引き起こす可能性が高くなるため、上記の 2 つの場合のようにここぞと言うとき以外は使用しない PIN としている。これは「ぽけマネー」センターからのパーソナルデータのダウンロードや、認証システムが認証不可状態になった場合の認証はセキュリティレベルを Login 認証以上にする必要性があると判断したためである。

(4)赤外線認証

赤外線認証も今回のチャレンジポイントの 1 つである。これはファミリーメンバーが正規のメンバーであるかどうかファミリーマスターが認証するスタンドアロン認証である。

入会審査は登録する事項に虚偽がない事を確認する事が重視されている。しかしながら、誰が記入し、印鑑を押したかを問う事はない。そのため、今日のように本人が知らない間に会員登録がなされてしまう問題が発生している。そこで、ダウンロードしたパーソナルデータに対し、ファミリーマスターが認証するシステムを搭載した。
図 4 に赤外線認証概略図を示す。

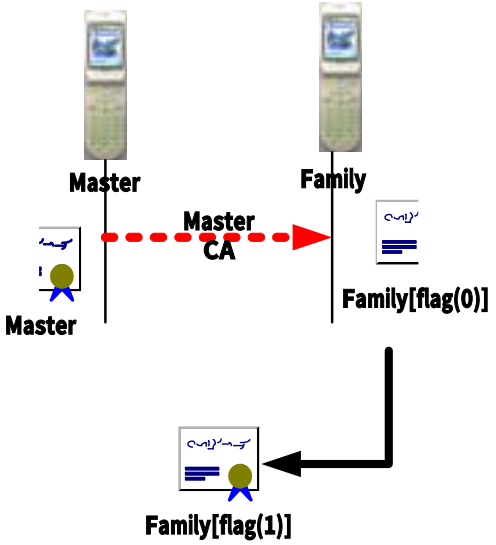

図 4　赤外線認証概略図

これにより、書面でのユーザ環境の整備とマスター本人からの認証によって、優良家族会員にサービスを提供出来るようになる。

ファミリーマスターは赤外線認証を必要としないが、パーソナルデータのダウンロードにおいてなりすましが起こる事は殆ど無いと考えてよいだろう。なぜなら入会審査は書面で行われ、インターネット認証で使用される PIN も書面で受け取る。

受け取った PIN 自体も、「ぽけマネー」システムが正常稼動し、ユーザが機種変更する事が無ければ、使用されるのはこれが最初で最後となるからである。

(5)サーバ認証・端末認証（Mozichi）

サーバ認証・端末認証も今回の電子決済システムのチャレンジポイントである。認証において使用するデータを生成するシステム「経験値蓄積型連続的認証システム」を試す事にした。

以下「Mozichi」と呼ぶ事にする。

既存のインターネット認証で使用する PIN を常用せず、連続的に正規サーバ、正規端末を認証していくシステムである。これは、携帯電話のように電波状況による認証切断、オーバーザショルダーから生じる他端末からのなりすまし、チャージバック問題に効力を発揮するシステムである。

Mozichi はある固定長（今回は 256bit）のデータを生成する。生成の元になるトークンは最大 n 回の経験値である。n の数はセキュリティポリシーにより変更可能であるが、今回 n<=5 とした。n は認証を経て、サービスが提供され、手続きが完了したものとなる。従って、正規端末が正規サーバと常にやり取りし、毎回エラー無く取引が完了していれば、Mozichi トークン数は最大値の 5 となる。図 5 に「Mozichi」認証概略図を示す。

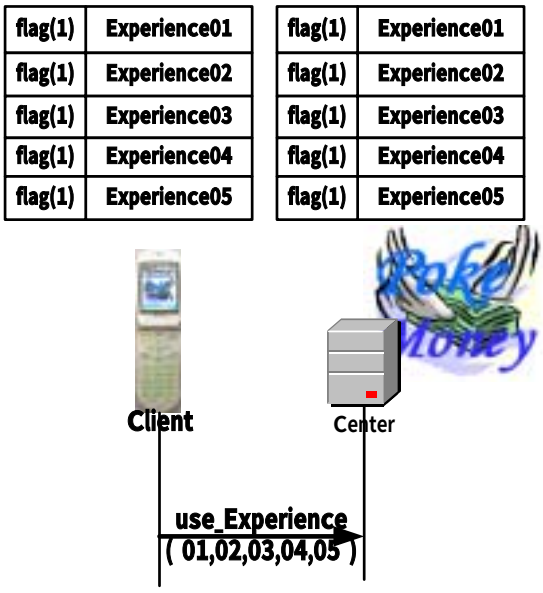

図 5 正常稼動時の「Mozichi」認証概略図

今回は、認証途中で圏外となったり、認証が失敗した場合のものはトークンとして使用及び経験値蓄積をしないセキュリティポリシーを設定している。

図 6 に「Mozichi」データ作成の概略図を示す。

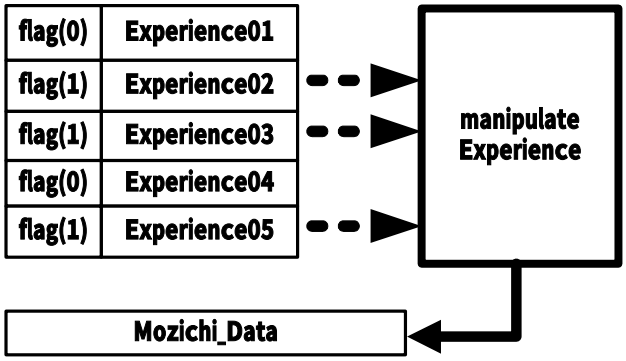

図 6「Mozichi」データ作成の概略図

これにより、インターネット認証用 PIN を使用せずに端末、サーバの認証を行っている。注意すべき点は毎回認証データが変化する事である。経験値を有するため、1 回データが読み取られても経験値全てが揃わないと意味を成さない事が特徴である。

Mozichi 認証では、最初に使用するトークンを通知する。これにより、例え flag 設定直前で回線エラーが起こった場合でも認証が可能となる。

図 7 に取引が不完全状態で終了した経験を持つ時の認証概念図を示す。

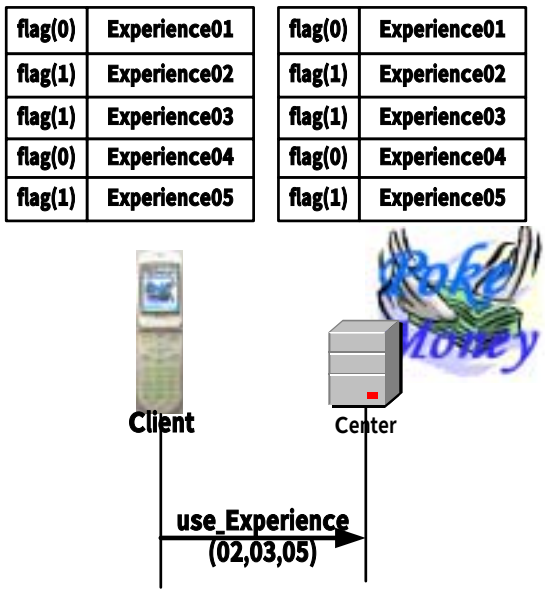

図 7　取引が不完全状態で終了した経験を持つ時の認証概念図

さらに、認証時使用するトークンの数は、例えflag 設定直前で回線エラーが起こった場合でも以下の関係が成り立つようプロトコルを設計してある。

「ぽけマネー」クライアントが使用を宣言するトークン数:　n

「ぽけマネー」センターが flag の状況から経験値の使用を試みるトークン数:　n'

$$n \geq n'$$

これにより、仮に数回の経験値を手に入れ、なりすましをしようと考えた場合、「ぽけマネー」クライアントは使用する経験値番号通知において、「ぽけマネー」センターに保存されている flag(1)の経験値番号か、それを含むそれ以上のトークンを提示しなければ認証が開始されない。

図 8 に n ≥ n' 時の概略図を示す

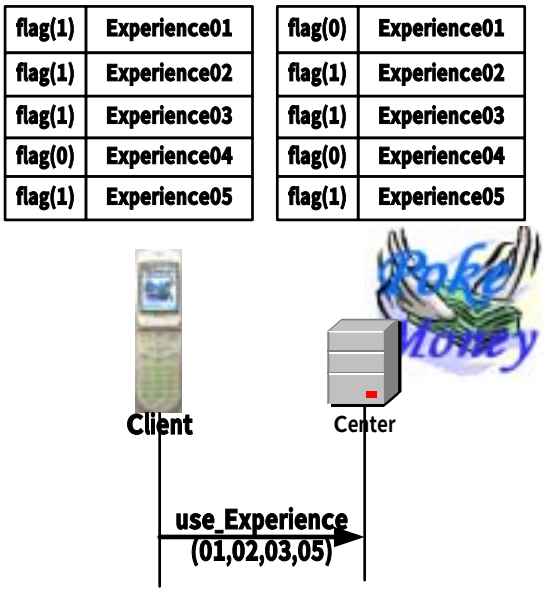

図 8　n ≥ n'時の概略図

図 9 には Experience(01,02,04)と記してあるが、なりすましを試みようとする不良ユーザは入手した Experience が何番目のトークンであるか分らないため、図における use_Experience メッセージを正確に送る事が出来ない。そのため、戦略的に認証に入る事が出来ない、use_Experience において全てのトークンを使用するよう通知すれば、認証に入れるが入手した断片的な Experience は意味をなさない事になる。

しかしながら、セキュリティレベルが 256bit の PIN セキュリティシステムを越える事は無い。

認証が根本的に成立しなかった場合はなりすましがあったものとし、警戒を強めるか、サービスを停止する。認証が成立しなかったにも関わらず、「ぽけマネー」サーバに対する次のアクセスで認証が成立した場合は、なりすましを試みた端末が存在した事を検知する事が出来る。

正規ユーザでありながら認証が成立しなくなった場合は、有人「ぽけマネーセンター」の場合、センターに連絡し、Mozichi トークンのリセットを PIN によってかける。無人の場合はメールによって発行されたワンタイム PIN とユーザ PIN を併用して Mozichi トークンのリセットを行う。

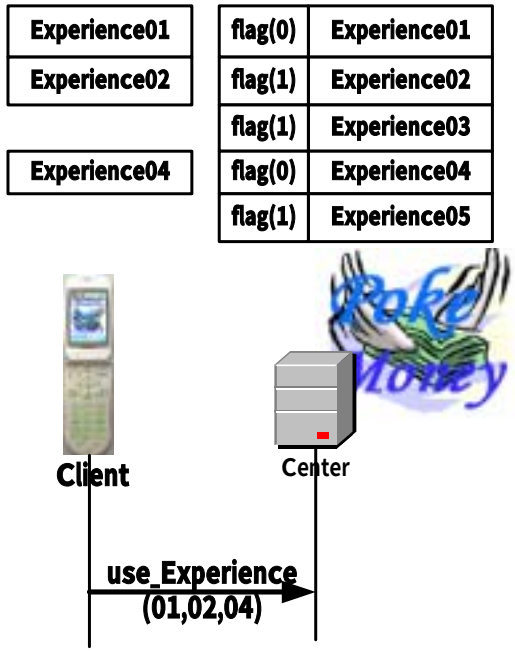

図 9　なりすまし時の Experience 概略図

(6)電子公証と Mozichi

Mozichi は認証機能のみではなく、電子公証やチャージバック問題にも効力を発揮する。例えばカードを利用した覚えのない取引を例に挙げる。会員による「覚えのない取引」申し立ての類型を下記に記す。

1 本人に起因する場合
　案件を忘れる。気付かないうちにホテルの備品等を壊したなど。
2 本人が知らない場合
　家族が（本人に無断）でカードを使った場合
3 第三者の不正行為による場合
　盗難、紛失、なりすまし等。
4 不良加盟店による場合
　二重請求、伝票横流し、POC
5 関与しているが知らぬ存ぜぬと白を切る場合
　不良ユーザ、最も悪質。

の 5 つが例として挙げられる。1、2 の場合は解決は比較的容易である。3 の場合は携帯端末が直接盗まれ、Login 認証後のものを入手しなければ、「Mozichi」の通常機能により認証をはじく事が出来る。4 の場合はインターネット「ぽけマネー」決済を利用する事で悪質な加盟店が認証、決済に手を加える事を防いでいる。
5 の場合が「Mozichi」が他の方法よりも効力を発揮する時である。「経験値蓄積型連続的認証システム」は過去の取引の正当性と共に、自らの取引の安全性を確保し、未来の安全性確立の補助を行う。従って、過去、現在、未来を通じ、取引の正当性を証明し、不法ユーザのチャージバックを防ぐ事を可能としているためである。

ユーザが不当にチャージバックを求める場合、その前後の取引もチャージバックを行う必要性があり、連続的に行われた全ての取引がチャージバック対象であることを証明する必要性がある。これは極めて困難である。そこで、上記システムを使用し、カード犯罪で問題となっているチャージバック問題の解決を図る。

身に覚えのない請求、二重請求に対しては、「ぽけマネーセンターで公証（Trust_Back）を行う。

(7)証拠

トラブル解決には、物的証拠が必要である。口頭の主張はまず認められない。そのためにも、日頃の取引書類等の整理・保管が必要である。それに対し、今回のシステムでは電子レシートの発行を行っている。

(8)Trust_Back とあぶり出し

不良加盟店、不良ユーザのあぶり出しは安全な e コマースを確立する上で重要である。不良加盟店のあぶり出しは、一定期間中のある加盟店のチャージバック、不正システムによる取引、不正な売り上げ伝票デポジット、伝票の横流しなどの事故取引件数・金額を分母とし、総売上件数・金額を分母として、その割合が一定の比率を越える加盟店弾き出す事によって行われる。

取引は「ぽけマネー」センターへの売り上げ伝票デポジットとユーザからの支払い要求を相殺する形で決済が行われる。これを「**Trust_Back**」と呼ぶ事にする。この 2 つのデータに相違が生じた場合、エラー以外であれば、何らかの目的で伝票が書き換えられた事になる。この「**Trust_Back**」は不正加盟店の伝票の不正操作（伝票分割、複数伝票、端末操作）の問題を解決する事が可能である。伝票を分割した場合、分割した伝票情報の全てについてユーザからの支払要求が必要となる。購入日の後日、白紙伝票を使って架空の売り上げを立てる問題に対しても、レジ端末操作において、架空の取引データを入力する問題も阻止する事が出来る。

今回はオン・アスシステムを前提に設計されているので、問題のある加盟店が発見されると当該店の監視や教育の強化が行われる。次いで加盟店名をセキュリティ関係警告書に掲載し、公表する措置が取られる。この加盟店が関与した不正行為に対しては、無条件でチャージバックが認められ、加盟店はこれに対抗できないものと定めた。

不良ユーザのあぶり出しも同様にして行われる。ユーザが支払い確認データに手を加えれば、加盟店から上がってくる売り上げ伝票デポジットと値が合わなくなるため、不正操作を検知する事が出来る。この結果はユーザのスコアリングに即座に反映させることが可能となる。

本来ならば加盟店から「ぽけマネー」センターへの売り上げ伝票デポジットのみで良いのだが、あえて意味の無い改竄チャンスを与えている。

認証中断回数等もユーザのスコアリングに含めるのが妥当だが、今回は携帯端末を利用しているため、正規ユーザであっても認証が不確実な状態で終了する場合がある。そのため、今回はカウントせず、「Mozichi」認証において、通信障害以外で認証が成立しなかった回数をカウントしている。スコアリングがある一定の値を越えた場合、該当する会員の取引停止、会員権の回収が行われる。

オーソリ請求（信用照会請求）の場合、ユーザから受け取ったデータ（カードでは磁気テープのデータ）を全て無修正で「ぽけマネー」センターに伝送することを加盟店へ義務付ける。違反すれば、無条件チャージバックの対象とする。これは、加盟店が自分に不利なデータの伝送を故意に行わない、などの行為を抑止するためである。

6.e コマースのまとめ

今回の「ぽけマネー」システムの決済関係のキーワードは『家族』である。「ぽけマネー」マスターユーザはクレジット、携帯電話料金に上乗せ、ネットデビットなど様々な決済システムを同一課金徴収先として設定出来、「ぽけマネー」ファミ

リーユーザはマスターユーザが指定した同一課金徴収先を指定し、登録する事によって、お得なサービスを受ける事が可能となるばかりでなく、デジタルコンテンツ購入に対して安全で経済的な環境を得る事が可能となる。

同一課金徴収先を設定するシステムの実現性はどれほどのものなのだろうか。それを分りやすく図 10 に示した。

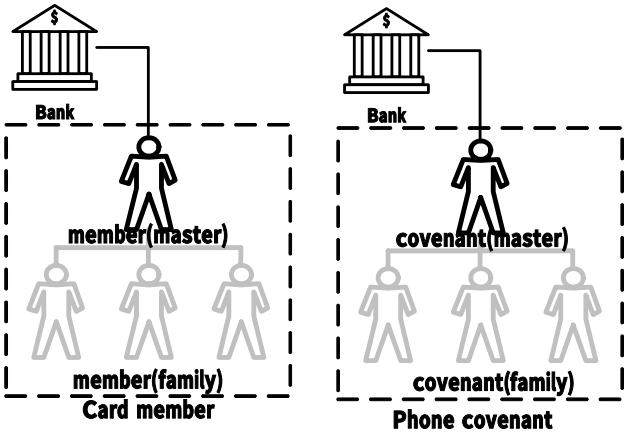

図 10 同一課金徴収先の実現性

左側がカード会社の家族会員におけるシステム図で、右側が携帯電話家族割引におけるシステム図である。この図より、同一課金徴収先を指定するシステムは構造的には比較的、導入が容易である事が推察され、さらには日本の社会の中に浸透しつつある事が分る。従って、フレームワークを元に DRM 機能を持った決済システムは技術的には早期実現が可能である事が推察される。

今回はシステムを自作するために、携帯電話を端末とし、「ぽけマネー」i アプリを作成したが、フレームワークの実現のみを考慮すると、携帯電話の代わりに IC カード、PDA 等を利用することも可能である。

7..著作権問題解決へのアプローチ

著作権問題解決へのアプローチは全て前記のフレームワークを元に行われる。その中でも著作権管理法は今回の情報コンテンツ流通システムを支える 2 つ目の柱と言える。著作権問題解決におけるキーワードもまた『家族』である。

(1)著作物使用可能ユーザの種類

購入したコンテンツを使用できるユーザの種類を図 11 のように 3 種類設定した。

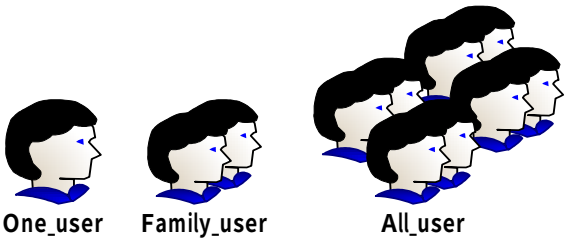

図 11　ユーザの種類

「One」は購入したユーザのみ使用が許されているコンテンツの使用権利を示す。

「Family」は購入したユーザとその家族のみ使用が許されているコンテンツの使用権利を示す。

「All」は購入したユーザに関わらず、誰でも使用が許されているコンテンツの使用権利を示す。（主に体験版の配布や宣伝に使用される事が見込まれる。）

これらにより、コンテンツを利用できるユーザの管理が可能になる。著作権関係の背景にて問題提起した、購入コンテンツと親子ユーザの問題も解決する。親が購入したコンテンツでも、Family 権限のコンテンツであれば、子供も楽しめる事になる。逆に、子供が購入したコンテンツでも親も使用することも可能となる。

このユーザの種類区分は至極当たり前のように思えるが、これまでは実現が難しい問題であった。

(2)著作物使用可能端末の設定

これまでの著作権保護システムは使用端末を中心に行われてた。しかし、これではユーザが複数端末使用していた場合の利便性が保てない。かと言ってユーザ認証のみでは、端末数が制限できないため、上記の著作物使用ユーザの管理と共に端末の管理も行う。

ユーザが使用する機器の管理法を図 12 に示す。図 12 はユーザ 1 人対して 3 台の端末で使用できる許可を与えた場合の図である。コンテンツの使用権利種目を「One」とする事で、既存の著作権保護システムを確立する事が出来る。既存のシステムとは異なった環境を作り出すのが、コンテンツの使用権利種目が「Family」の場合である。ユーザは各々3 台までのコンテンツ使用端末を指定する事が出来る事になる。例として、ユーザ使用端末最大値を 3 台としても、5 人家族では 15 台の端末でコンテンツを使用する事が可能となる。これだけあれば、殆どの家庭で著作権を細かく意識する事無く、居間のパソコンを使用しても、自分の

部屋のパソコンを利用しても、自分のノート型パソコンを利用しても「Family」コンテンツを使用することが出来る。「All」コンテンツは文字通りどの端末でも使用する事が可能となる。
図 12 は超流通システムを想定して作成されている。この場合、コンテンツはどこから入手してもよく、端末からはライセンスを購入している。

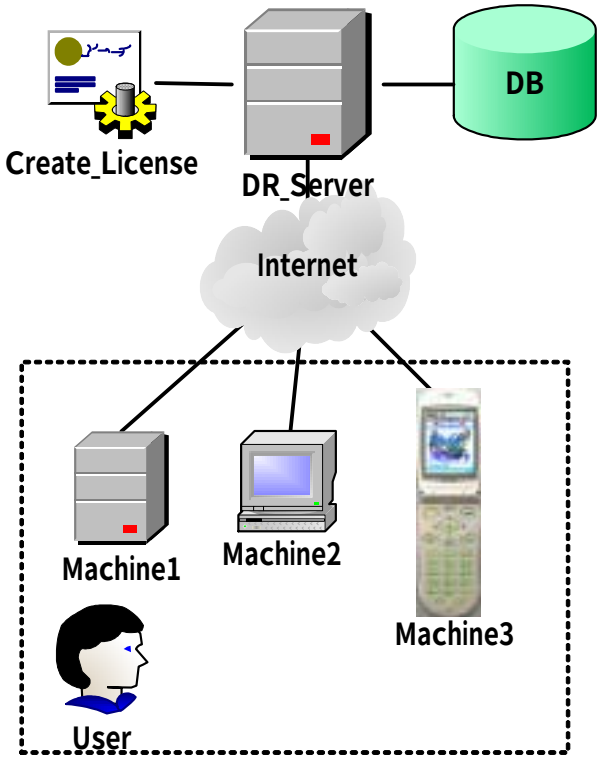

図 12　ライセンス管理概略図

(3)暗号化技術、ライセンス制度との関係

今回の著作権保護システム暗号化技術に依存しない。また、ライセンス制度による売り上げ配当システムにも依存しない。
暗号化復号化に必要な技術は図 13 に示すとおりである。

暗号化システムは平文と暗号化キーを入力すると出力として暗号文を出力する機能を持ち、復号化システムは暗号文と復号化キーを入力すると出力として平文を出力する機能を持っていれば良い。従って、使用端末のスペックやコンテンツホルダーの要求によって自由に暗号化復号化アルゴリズムを変更する事が可能である。

コンテンツ対価における著作権料の制度はコンテンツの価格に大きく影響するが、今回の著作権管理システムには影響しない。ユーザは唯、提示されたコンテンツの対価を払う事によってコンテンツ利用権を得る事が出来る。コンテンツ利用ユーザの範囲及びユーザ端末の制限は権利保有者が決め、著作権管理機関に登録する事によって適応される。

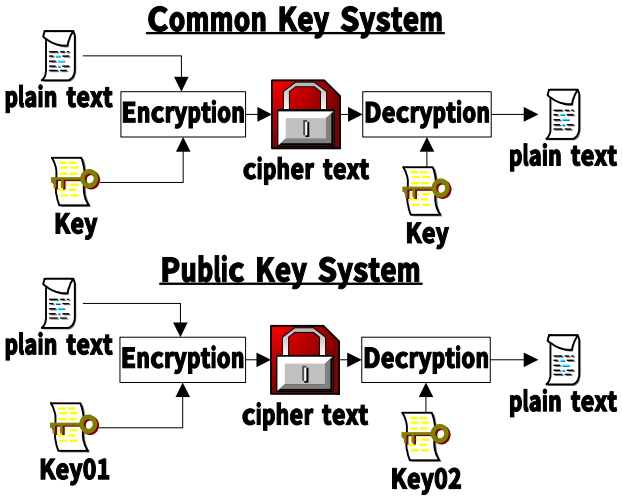

図 13　暗号化復号化技術

(4)家族の定義

コンテンツ使用可能ユーザとして定義した、「Family」とは何か。研究社「リーダーズ英和辞典」によると『Family:　所帯（夫婦とその子供、召使も含む）、家族（夫婦とその子供）』と解説している。
「所帯」「家族」とは何か。広辞苑によると『所帯: 一戸を構えて独立の生計を営むこと。住居および生計をともにする者の集団』『家族: 夫婦の配偶関係や親子・兄弟などの血縁関係によって結ばれた親族関係を基礎にして成立する小集団』とある。「Family」コンテンツはこの「所帯」と「家族」2 つの要素を併せ持つフィールドにおいて使用が許される必要性がある。

これまでパッケージコンテンツ（映画等）ではこのフィールドを冒頭の青画面に言葉で表示する事により使用制限をかけていた。しかし、それ自体に効力はなく、早送りされてしまう事が殆どであった。

それを今回はシステマティックに「同一課金徴収先」により「所帯」「家族」というフィールドを定義する。

図 14 に同一課金徴収先の概念図を示す。

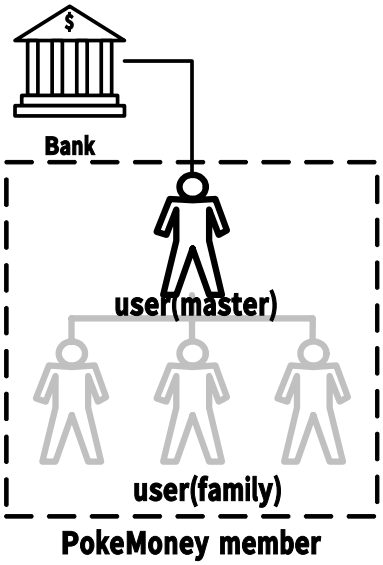

図 14　同一課金徴収先概念図

(5)Family ライセンス（ダブルライセンス）

家族で使用するため、ライセンス項目も新しいものを設計する必要がある。今回は新しく、ユーザフィールドを 2 つにする方法を試みた。ここではダブルライセンスと呼ぶ事にする。

図 15　にダブルライセンスの概念図を示す。

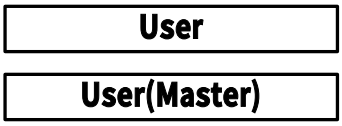

図 15　ダブルライセンス構成図

前に示したユビキタス電子財布システム『ぽけマネー』に対応させるため、ライセンス名を「User」と「User(Master)」とした。

「User」は実際にコンテンツが欲しいと思い、コンテンツを購入したユーザを示す。

「User(Master)」は家族の長また､所帯主である。フレームワークによれば、今回は同一課金徴収先の持ち主となる。

この 2 つのユーザ項目により家族というフィールドを制限する。例を以下に示す。

AMANO_KOJI（ユーザ番号:　00000001, ユーザタイプ:　Master）がコンテンツを購入したとき

「User:　　00000001」

「User(Master):　00000001」

となる。

子供 AMANO_SON（ユーザ番号:　00000002, ユーザタイプ:　Family）

がコンテンツを購入した時は

「User:　　00000002」

「User(Master):　00000001」

となる。

このダブルライセンスシステムで前記のコンテンツが使用できるユーザ区分「One」を表すと図 16 のようになる。

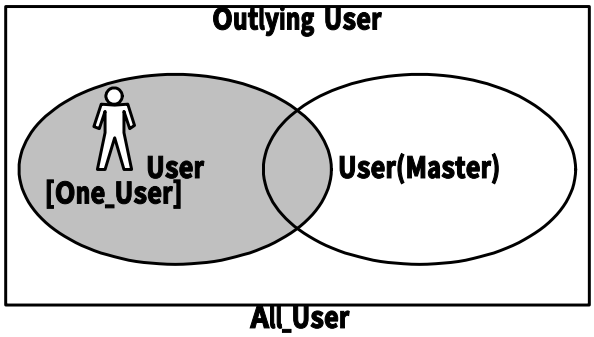

図 16　ユーザ区分「One」

「One」の場合購入したユーザのみが使用できる仕組みになっている。

次に「Family」を表すと図 17 のようになる。

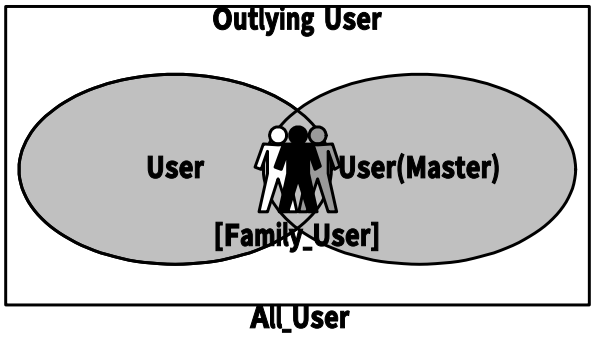

図 17　ユーザ区分「Family」

図 17 のようにコンテンツを購入したユーザでなくても、「User(Master)」が同一のユーザであれば、「Family」コンテンツを使用できる事が分る。

同じく、「All」を表すと図 18 のようになる。

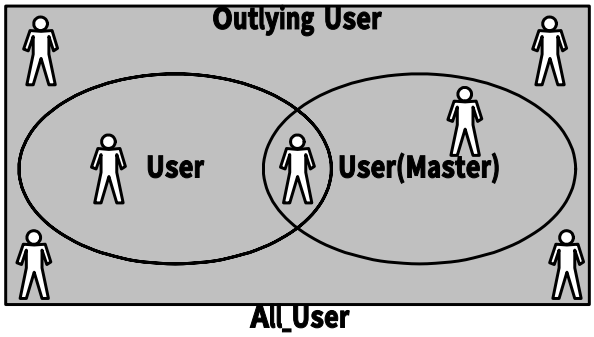

図 18　ユーザ区分「All」

All の場合、たとえ「User」「User(Master)」が違うユーザであっても、コンテンツを使用する事が可能となる。
四角の枠はユーザダブルライセンスシステムに登録してある全てのユーザの枠である。内部の楕円はダブルライセンスにおける「User」「User(Master)」を表し、コンテンツが使用可能なユーザをグレーにする事で表してある。

(6) 使用範囲の変更

お店の前で「買って！買って！」と駄々をこねる子供が居るのはいつの時代でも、またどこの国でも同じである。しかし、親に「買って攻撃」が出来る年頃を過ぎ、買ってもらえなくなったら子供は何と言うのか？結果は「じゃあ良いよ、自分で買うから」である。

この年頃から子供は、自分だけコンテンツを使えるようにしたいと考える場合も出てくる。これは一種のセキュリティとも言えよう。デジタルコンテンツをベットの下に隠す事をイメージして頂ければ良いと思う。この場合、購入時に「Family」コンテンツを「One」コンテンツに変更する事も可能である。使用範囲をユーザが狭める事に文句を言うコンテンツホルダーは居ないことは既存のシステムを見ても周知の事である。

(7) ファミリーユーザが独立する場合

子供が独立したらどうなるのか。先ほど「Family」の定義をしたが、子供に支払い能力が生じ独立して行った場合、今までの「家族」の定義には入っても、「所帯」としては別となる。

今回のシステムでは、支払い能力が生じ、「所帯主」になったら親に頼らず自分で買うと言う事になっている。これもまた、いたって当たり前の事であるが、デジタル著作権管理保護システムの中では実現が困難な問題であった。

図 19 にシステムにおける所帯の切り離し、及びコンテンツ使用権の切り離しを示す。分りやすいようにフィールドには名前を入れているが、実際は ID となる。
これは AMANO_SON が自立する前と後に購入したコンテンツのダブルライセンスのユーザフィールドである。「User(Master)」が自分自身のものになった事が一人前になった証である。

これにより、AMANO_SON はかつてのファミリーコンテンツに対して、図 20 のような位置づけになる。

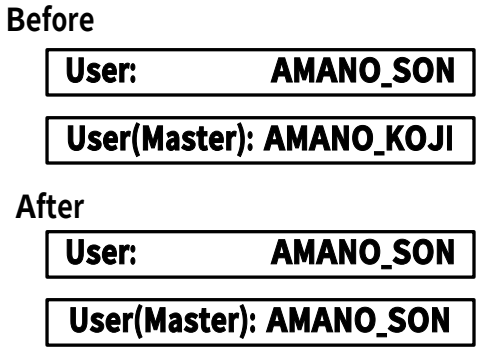

図 19　ユーザが独立する場合のライセンス変移

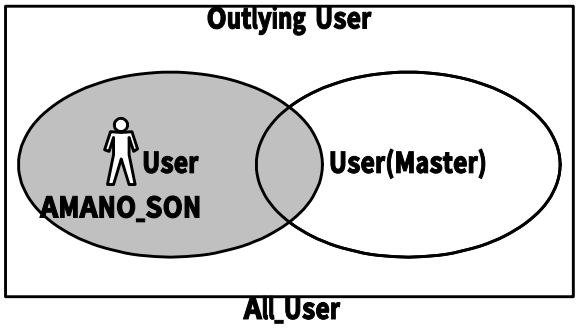

図 20　独立ユーザのコンテンツ使用範囲

かつて、自分自身が購入したコンテンツは使用出来るが、他の家族が購入したコンテンツは「User(Master)」が違うため、使用できない。これが自立した場合の辛さである。しかしながら、自立とはそういうものだと理解できる年頃になっている事は間違いない。

過去のコンテンツに対して、さらに使用権を狭める事も可能で、「User(Master)」が違った場合使用できないようにすれば、AMANO_SON は過去に自らが購入した「Family」コンテンツに対して図 21 のようになる

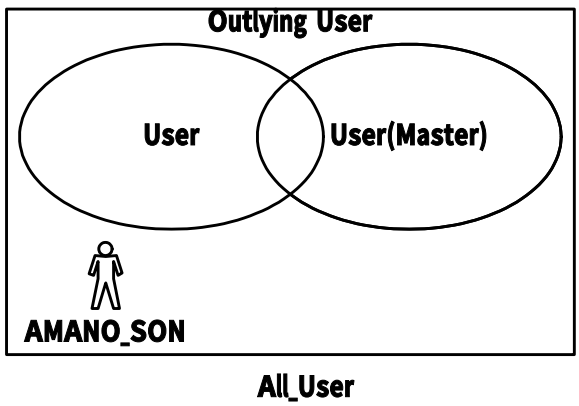

図 21　完全独立ユーザのコンテンツ使用範囲

図 21 を見ていただければ分るが、AMANO_SON はあかの他人同然となる。「所帯」「家族」とも別のユーザとなんら変わりない扱いとなる訳である。

しかし、今回我々が目指し提案するデジタル著作権保護システムはユーザマインドに立脚したシステムである。そこで、AMANO_SON はこれまでのコンテンツを家に置いて行くのか、それとも持って行くのか決定する事が出来る。これは引越しのときの部屋整理をイメージして頂ければ、分りやすい。

このシステムは主に、Player を必要とするコンテンツや、OS レベルで著作権管理した場合のソフトウェアソフトウェアコンテンツへの適用が期待出来る。

(8) 他のファミリーのメンバーなる場合

娘さんが「お嫁に行きます。」と言い出した場合はどうなるのであろう。デジタルコンテンツを花嫁道具に含める事は可能であろうか？

今回のシステム（フレームワーク及びダブルライセンスシステム）ではこの問題を解決する事が出来る。

図 22 に他の「Family」に属する場合の例を示す。

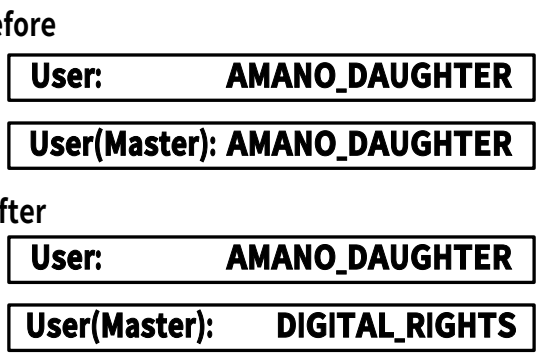

図 22　ファミリー変更時のダブルライセンス

AMANO_DAUGHTER と DIGITAL_RIGHTS が結婚し、同一課金徴収先に DIGITAL_RIGHTS 氏の課金徴収先を指定した場合を示している。これにより、AMANO_DAUGHTER はこれまでに自分が購入したデジタルコンテンツを使用できると共に、DIGITAL_RIGHTS 氏の「家族」「所帯」として彼の購入した「Family」コンテンツを使用できるようになる。

5. 著作権問題解決へのアプローチのまとめ

ユーザの種類として我々が提示したものは、企業がコンテンツを作成するにあたって、ターゲットとするグループであり、かつ著作権保護システムを適応したいグループである事は理解して頂けたと思う。

既存の著作権保護システムには、

・「端末単位ライセンス」（端末を主体としコンテンツ使用許可を与えるライセンス法）

・「アカウントライセンス」（アカウント単位でライセンスを与える法）、

・「ユーザライセンス」（単一ユーザにライセンスを与える法）

などがあるが、今回のシステムではこれらでは表現できない『家族』という単位を前面に押し出したシステムとなっている事が分る。また、『家族』というユーザを限定するために、今回我々が提案するフレームワークが有効である事も理解して頂けたと思う。

家族は正当なライセンスの元、家族の一人が購入してきたコンテンツを安心して使用する事ができる。さらには、デジタルコンテンツ使用権利の切り離しという難題も解決出来ている。

人生門出には何らかの決断の時が来る。デジタル著作権保護システムにもそれが当てはまる。いままで家族にお世話になり使用していたコンテンツを手放す時が来るのである。また、自分が購入したコンテンツを家族に託すのか、それとも自分が持って家を出るのか。この葛藤は子供が大人になるうえで重要な経験であると考えている。

子供の成長に合わせて、課金義務や著作権というものを理解してもらい、そして自立するときには決心をしてもらった上で、自分が「世帯主」となり「Family」を構成してもらう。これこそ今後のデジタル社会に生きる子供達に対する親心であり、e ジャパンが目指さなければならないシステムであると考えている。

8. まとめ

電子決済システムは着実に社会に浸透している。食事での支払い等では比較的簡単に電子決済システムを導入する事が可能で、着実にインフラ整備が進んでいる。しかし、モノの決済に対する電子決済システムは簡単ではなく、通販での問題と同様の問題が生ずるが、今回はカード犯罪における

犯罪手口類型を元に、なりすまし、不良加盟店、不良ユーザ等の問題の解決を図るシステムの一例を提示する事が出来た。

「Mozichi」は現在利用されている乱数発生システムの代わりに導入する事も可能で、既存システムとの親和性については今後さらに検討する価値がある事が推察される。

「Trust_Back」はシステムの構成自体の変更を伴うため、実装は新規システム設計において検討する事が妥当であると考えている。

さらにモノがパッケージのような物体ではなく情報であった場合、決済が終った後になっても決済完了の証明をする必要性がある事が叫ばれている。今回は決済とデジタル著作権管理を組み合わせる事で、コンテンツのライセンスにおいて決済が完了していることを証明する事が出来た。

また、ライセンスとコンテンツを分離した事で、超流通システムにも対応出来るようになった。

使用範囲の設計では、フレームワークを元にダブルライセンスと言う方式を提唱する事で、ファミリーの使用環境をベン図で示す事が可能となった。これにより、ベン図をプログラムの判断文に適応する事で、そのままシステムがコンピュータ上で稼動する事を示す事が出来た。

ダブルライセンスを適応する事で、家系図全体が第３者に流れる事を防ぐ事が出来た。

スタンドアロンシステムにおけるライセンス管理や、コンテンツの暗号化方式、プレイヤーの作成、などは今後の課題ではあるが、何れもライフスタイルに即したデジタルコンテンツ使用環境の構築が出来る見通しが付いたと判断している。

9. 参考文献

1. 末藤高義『クレジットカード犯罪トラブル対処法』民事法研究会
2. ASCII24 ニュース
3. msn ニュース
4. ZDNet ニュース
5. Edy Card 入会申込書
6. 三井住友 VISA カード入会申込書

抜粋記事の全文

「VISA、国内メンバーカード会社 7 社とインターネット向け本人認証サービス開始」
http://ascii24.com/news/i/serv/article/2002/07/22/637408-000.html

「RIAA の個人追及を有力議員が批判」
http://www.zdnet.co.jp/news/0308/02/nebt_04.html

「ダウンロード購入した音楽の転売は“ アリ ”か？」
http://www.zdnet.co.jp/news/0309/04/ne00_itunesauction.html

「ダウンロード音楽のオークションが中止に」
http://www.zdnet.co.jp/news/0309/05/ne00_ebay.html

10. 付録　用語の説明

今回はカード会社における用語を使用してシステムの紹介をしているため、ポイントとなる用語を下記に示す。

(1) スキミング

クレジットカードを偽造するための手法の一つ。特殊な電気機器によりカードの磁気テープに入力された全てのデータを盗み取ること。

(2) チャージバック

「クレーム申し立て」、「意義申し立て」の意味を含み、「請求をつき返す」あるいは「取られた代金を取り戻す」行為である。国際的な平均値で見ると、クレジットの場合、1 万回利用されると、15～20 件のトラブルが発生すると言われている（国内では２～３件）具体的には、カード会員がカード利用明細書を見て、クレームを申し立て、イシュアーがこのクレームに理ありと認めた場合、一定のルールに従って、アクワイアラーに対してこの請求を不当とし、先取りされた代金を取り戻す行為

図 a に会員登録からチャージバックまでの流れを示す

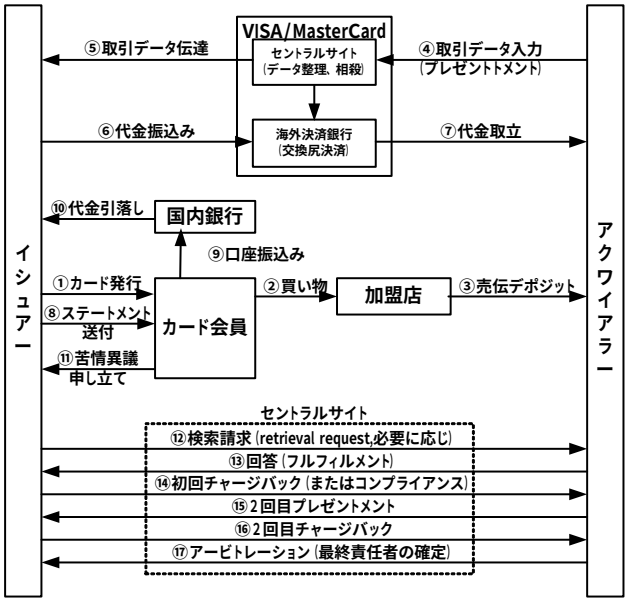

図 a チャージバックの流れ

(3) POC

Point of Compromise カード情報を横流しする不良加盟店

(4) イシュアー

「issuer」クレジットカードを発行する機関（カード会社）

(5) アクワイアラー

「acquirer」加盟店を開拓し、加盟店契約を締結し、加盟店を管理するクレジット会社

(6) オーソリゼーション

加盟店は、カード会員が一定の金額を越える買い物をしようとする場合には、これに応じてよいかどうか（与信の可否について）、カード会社の認証を求めなければならない。これを「オーソリゼーション」（信用照会、オーソリ請求＝AR＝authorization request）という。

(7) オン・アス取引

イシュアーとアクワイアラーが同一の場合の取引形態である。

図 b にオン･アス取引の概念図を示す。

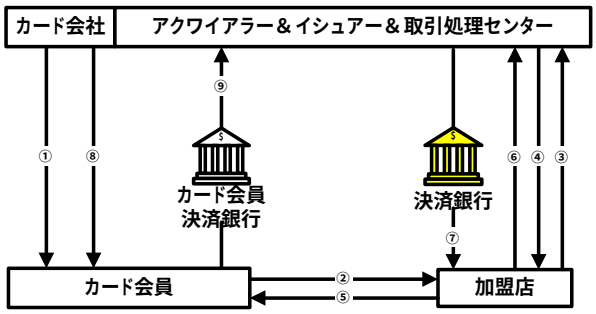

図 b オン･アス取引概念図

①カード発行　②商品・サービス購入（カード提示）
③オーソリ請求　④オーソリ承認　⑤商品・サービス提供（信用販売）⑥売上代金請求　⑦売上代金立替払い
⑧代金請求　⑨代金支払い

(8) ノン・オン・アス取引

イシュアーとアクワイアラーが別の場合の取引形態である。

図 c にノン・オン・アス取引の概念図を示す。

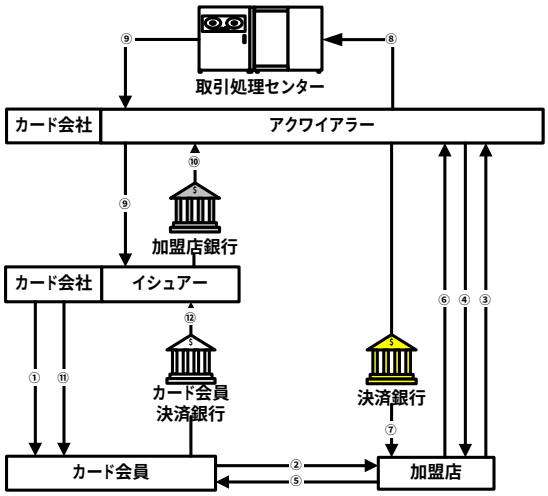

図 c ノン・オン・アス取引概念図

①カード発行　②商品・サービス購入（カード提示）
③オーソリ請求　④オーソリ承認　⑤商品・サービス提供（信用販売）⑥売上代金請求　⑦売上代金立替払い
⑧取引データ送付⑨取引処理センターより加工済み取引データをアクワイアラー・イシュアーに送付　⑩アクワイアラー・イシュアー間の決済　⑪代金請求　⑨代金支払い

(9) 「DEM」付きオン・アス取引

「DRM」機能付ぽけマネーがクレジット機能を持った場合の例を図 d に示す。

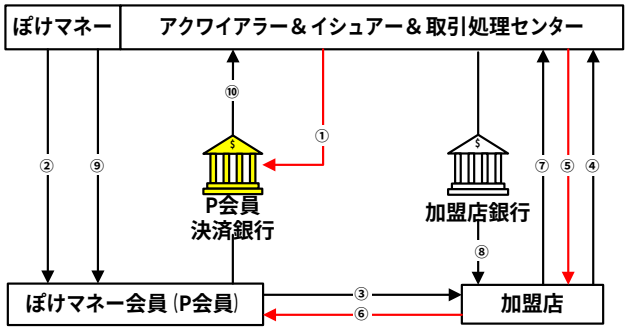

図 d「DRM」ぽけマネー例

①同一課金徴収先設定　②ぽけマネーサービス開始
③商品・サービス購入　④オーソリ請求　⑤オーソリ承認。同一課金徴収先情報またはコンテンツ暗号鍵または、鍵生成用トークン受信　⑥暗号化ライセンス情報もしくは暗号化情報コンテンツ送信　⑦売上代金請求　⑧売上代金立替払い　⑨代金請求　⑩代金支払い

(10)スコアリングシステム

入会審査等において会員の情報をスコアリングテーブルによって点数化し、保険数理や統計学に裏打ちされた、コンピュータ処理システムによって与信の可否を判定するシステム。このシステムはトップシークレット扱いになっており、外部から内容を窺い知る事は出来ない。

(11)ダブルライセンス

自作ライセンス管理方式「Family」を例とする、ある一定のグループにコンテンツの使用権を与えるシステムにおけるグループ化方式

(12)Mozichi

自作認証システム「経験値蓄積型連続的認証システム」過去、現在、未来を通して連続的に認証を行う、端末・サーバ認証および、不正利用検知システム。

(13)Trust_Back

自作信用照会及び、電子公証システム。加盟店またはアクワイアラーから、「ぽけマネー」センターに売上デポジットを送信すると共に、ユーザに対しも支払い確認として同一情報を送信する。支払い要求としてユーザから戻ってきた情報と売上デポジットを比較して、信頼の確認を行う。

本来ならば売上デポジットのみでも稼動するが、不良加盟店、不良ユーザによる改竄を確認し、安全な決済を促進するために使用する。

改竄が見られた場合、早期にスコアリングに反映させ不良加盟店、不当ユーザの洗い出しを行う事を可能としている。

(14)不正利用検知システム

カード決済における認証では、オーソリゼーションリクエスト(AR)と併せて、不正利用検知システムが稼動している。代表例として、「FALCON」や「PRISM」がある。「FALCON」はニューラルネットを使用している事が特徴的であるが、両者とも、スコアリング方式により、あるカード取引をカード会員の一般的な購入パターンと比較して、不正利用の確立を算出、警告を出す機能を持つ。これにより、偽造したカードを使用して換金性の高い高額商品を短時間で限度額ギリギリまで購入する行為を検知し、警告を出している。