社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2003－ EIP－21 (6)
2003／11／29

超流通型P2Pによる画像共有・配信における認証と課金システム

細谷博子† 華表清香† 大村 梢† 佐藤浩史† 河原正治††
† お茶の水女子大学 理学部 〒112-8610 文京区 大塚 2-1-1
†† 筑波技術短期大学 〒305-0821 つくば市 春日 4-12-7
blueques@act.is.ocha.ac.jp sayaka.t@act.is.ocha.ac.jp kozue1220@act.is.ocha.ac.jp
sato@is.ocha.ac.jp masaji@k.tsukuba-tech.ac.jp

あらまし 従来型のサーバ・クライアントシステムが抱える問題の解決法として注目されているのが，Peer-to-Peer(P2P) 型システムである．このシステムを実用化するためには，著作権処理や個人認証などの課題があり，それらを解決する必要がある．将来的には，携帯端末が身分証明の機能や，日常生活の様々な決済機能を担うことが期待されている．将来の携帯端末が持つべき機能を明確にするために，本研究では一つの例として，携帯電話に課金機能を組み込んだシステムを構築した．このシステムを既存のP2P型の画像共有システムに適用させた結果について報告する．

キーワード 超流通，P2P，DRM，ユーザ認証，携帯端末

Authentication and Billing in Sharing and Sending Images by P2P Based on Superdistribution

HOSOYA Hiroko † TORII Sayaka † OHMURA Kozue†
SATO Hiroshi † KAWAHARA Masaji ††

†Faculty of Science, Ochanomizu University Otsuka 2-1-1, Bunkyo-ku, Tokyo 112–8610, Japan
††Tsukuba College of Technology Kasuga 4-12-7, Tsukuba-shi, Ibaraki 305–0821, Japan

blueques@act.is.ocha.ac.jp sayaka.t@act.is.ocha.ac.jp kozue1220@act.is.ocha.ac.jp
sato@is.ocha.ac.jp masaji@k.tsukuba-tech.ac.jp

Abstract The Peer-to-Peer (P2P) type systems attracts a great deal of attention, since this system can solve the various problems existing in the current server-client systems. In order to put the system to practical use,however, it is necessary to settle the problems such as regulation of the Copyright Act and the individual-authentication. In future, it is expected that "mobile device"will be used as a means of personal identification and of the various settlement of accounts in daily life. In this research, as an example to make clear the function of future mobile device, we have constructed a kind of superdistribution system, that is, we have implemented the function of the billing to a cellular phone. Fuether more, we have combined the system and the existing P2P type system of sharing images. In this paper, we report the result of this combined system.

Keywords Superdistribution, P2P, DRM, User Authentication, Personal Digital Assistant (PDA)

1. はじめに

NapsterやGnutellaで話題になったPeer-to-Peer(P2P)システムは，当初のファイル交換用途だけでなく，オンラインゲームや情報家電ネットワークなど様々な展開を見せ，今後も発展すると考えられている．このようなP2Pシステムは，サーバ・クライアントシステムと違い，集中的に処理を行うサーバが不要であり，すべてのコンピュータが対等な関係になるという特徴を持つ．すなわち，P2Pシステムを利用すれば，それぞれのコンピュータが，情報を提供するサーバにも，情報を要求するクライアントにもなれ，ユーザ同士で簡単な操作で情報を交換することができる．

このようなP2P型システムは，従来のサーバ・クライアントシステムが抱える問題を解決するとして注目されているが，一方でその本格的実用化には，著作権処理やユーザ認証などに関する課題を解決する必要がある．我々は，携帯電話を主とする携帯型端末に認証や課金機能を実装し，P2Pネットワークに組み込むことにより上記問題の解決を目指している．

携帯電話の高機能化は急速に進んでおり，指紋照合を使った認証，自動販売機などでの料金支払い実験などが行われている．本研究では，携帯端末によってユーザを特定し，それを用いて課金を行うことで，安全な認証と簡単な操作での課金を実現できるシステム構築を目的としている．

本稿では，P2P型の画像配信システムを例にとり，携帯端末で個人認証と課金を行うシステムについて報告する．以下では，P2Pの簡単な説明と課題，および超流通の概要について述べた後，携帯端末技術の現状と今後の展望について説明する．次に，携帯端末を用いた画像配信における認証と課金のプロトタイプシステムについて報告する．

2. P2Pについて

2.1 P2Pの概要

P2Pシステムは，計算機同士が対等な関係を持った形で，資源やサービスを共有する技術である．P2Pシステムは，管理用サーバを必要とせず各ピアがメッセージを転送してサービスを提供するPure型P2Pと管理用サーバを必要とするHybrid型P2Pに分類できる．

Pure型P2Pシステムは，このネットワークは完全にピアのみで構成され，中心となる管理用サーバを必要としない．データは隣接するピアが次々と中継する方式で目的のコンピュータまで届けられる．このようなシステムは，

- ネットワーク的に離れたところにあるデータへのアクセス効率が悪い
- 中心がないためセキュリティ的には弱いが一部が使用不能になってもシステムは機能する

といった特徴がある．

Hybrid型P2Pシステムはピアと管理用の中央サーバで構成されるが，一般のサーバ・クライアント型と異なり，サーバの役割は認証やデータのインデックス管理のみで，実際のデータ転送はインデックス情報に基づき直接ピアが一対一で行う．

従来のクライアント・サーバシステムは局所的なトラフィックの増大を起こす危険性があり，さらにサーバの障害に対して脆弱であるという欠点をもつ．これに対してP2P型ネットワークでは，各ピアがP2Pアプリケーションを「ピア単位」で独立して実装する点が特徴である．特に，Pure型P2Pシステムの場合，従来のように情報を一括管理するサーバを持つ必要が一切なく，同じネットワークに接続している対等なピアの計算機資源を利用したシステムが実現されている．つまり，災害などによっていくつかのピアに物理的トラブルが発生しても，システムの運用への影響を小さくすることができる．

2.2 P2Pの課題

P2Pには以上のような利点がある反面，ネットワークを構築する各ピアの端末に高度な処理性能が求められる点，ネットワーク全体に高めの負荷がかかるため拡張性に弱いなどの問題点もある．さらに，現在大きな問題となっているのは利用者認証と著作権処理である．

Napsterは音楽著作物の自由な交換をインターネットを使って世界規模で可能にした．このような方式を使えば著作権侵害は無制限に拡大すると同時に，不正な取引を捕捉することが極めて困難となる．

クライアント・サーバシステムにおいて違法な情報の交換・共有などが発生した場合には，サーバ管理者がユーザのアクセス情報，通信履歴，Web サーバの情報などをもとに違法行為を調査することが可能であった．

ところが P2P システムでは，Web サーバなどの特定の計算機にデータを置く必要がなく，すべてのデータはユーザのハードディスクで管理される．また，データの所在を示すインデックス情報についても，Gnutella で示されたように，中央のサーバにおいて管理する必要がなくなりつつある．

このような動きが加速されれば，適切な規制は不可能になる．

著作権およびユーザ認証に関する問題に対応するためには，P2P システムにおいて，ピア間の相互認証に加えてシステム利用者の個人認証機能を整備することが必要である．これによって安全性の高いコンテンツ共有環境が実現する．さらに利用者のプライバシーに配慮することも重要である．

また，Napster や Gnutella の最大の課題は著作権侵害に対する有効な対策がなかったことである．コンテンツをダウンロードし利用した者からコンテンツ提供者に対して，何らかの対価を支払うという構造が不可欠である．

このような課題は，P2P に超流通技術を組み合わせると解決できる．次節では超流通および超流通型 P2P について説明する．

3. 超流通と超流通型 P2P

超流通は，ディジタルコンテンツの利用に応じた課金を安全に行うことによって，コンテンツ権利者の利益を保証しながら，利用者に低価格と利便を提供する．超流通では，従来の流通経路に加えて「利用者による複製および再配布」もコンテンツ流通の正当な手段となり，以下の二点が両立される [1, 2].

1. Napster や Gnutella などと同様に，見ず知らずの利用者間で自由にやりとりする方式でコンテンツを入手できること．
2. コンテンツ利用料を適切に分配し，権利者が正当な報酬を得ること．

典型的な超流通システムでは，利用者の手元でコンテンツ利用料の課金を管理するための SdLR(Superdistribution Label Reader) が必要である．SdLR は，ハードウェアとしてもソフトウェアとしても実装可能である．

P2P ネットワーク上の各デバイスがこのような SdLR を実装すれば，P2P における著作権処理や認証に関する課題が解決できる [3].

本研究では、超流通型 P2P システムの例として，P2P 型画像共有システムである PicShare に以下のような機能を追加したものを利用する．

1. 暗号化・復号機能
2. 携帯端末との課金に関する通信機能
3. ユーザ認証機能

超流通型の PicShare では，暗号化した画像を多数のユーザが自由に共有できる．画像を表示する際には，課金を行う携帯端末と，画像が保存されている PC または携帯端末を接続し，ユーザ認証と課金を行った後，画像が復号・表示されることになる．このように携帯端末を媒介として，コンテンツ提供者の権利を保護しながら自由に画像を共有することが可能となる．

4. DRM

上で述べたような超流通モデルを目指して，ディジタルコンテンツに関わる権利を保護する技術として様々な DRM(Digital Rights Management) が提案されている．ここでは，代表的な DRM について概説する．

4.1 UDAC-MB

UDAC-MB(Universal Distribution with Access Control–Media Base) は，汎用コンテンツ保護技術で，超流通モデルに基づく DRM 技術である [4]．暗号化コンテンツをユーザ間で自由に交換でき，コンテンツ再生のための復号鍵を取得したユーザのみが再生を行えるようになっている．鍵が不正にコピーされるのを防ぐために，コンテンツとライセンスキーを分離して管理する．暗号化コンテンツは通常のフラッシュメモリ領域に格納するのに対し，ライセンスキーは耐タンパ性モジュールと呼ばれる内部解析や改竄を防ぐ領域に格納される．また，再生する時も耐タンパ性モジュール領域でアナログ信号に変換する．

4.2 OMA DRM

Warner Music と Bertelsmann は 2003 年 10 月，携帯電話で楽曲をダウンロードして，その楽曲を友人と共有できるようにする技術を発表した [5]．この新しいデジタル権利管理（DRM）技術は OMA DRM サーバと呼ばれる．この新技術のコンセプトは，マルチメディアメッセージング（MMS）機能つきの携帯電話を持つユーザで構成される非公開の P2P ネットワークを作るというもので，ユーザはネットワーク内で他の携帯ユーザと画像や楽曲クリップを互いに送受信できる．OMA DRM を使うと，レコード会社は中央サーバからダウンロードされた楽曲とユーザ間で交換された楽曲の代金を徴収できる．

以上の他に，Microsoft 社による，Windows Media Rights Manager や，SONY による Open Magic Gate，Real Networks による Helix DRM などがある．また，携帯電話に最適化した DRM としては，NEC の RightShell(MRS) がある [6]．

5. 携帯端末技術

5.1 ケータイ de ミュージック

「ケータイ de ミュージック」は携帯端末への音楽配信サービスで，上述の UDAC-MB を利用している [7]．

楽曲のデータは制作時に暗号化されており，ライセンスキーを取得することで復号し，再生する．再生のためにライセンスキーを取得した時点で課金が行われることにより，コンテンツの著作権を守っている．ユーザはダウンロードした暗号化コンテンツを，自由に複製をとったり他人に譲渡を行ったりできる．また，ブロードバンド通信を使用して大容量の暗号化コンテンツをダウンロードし，ライセンスキーだけを携帯電話で購入することもできる．この場合，料金は電話代と一緒に電話会社からの請求となる．

今後は暗号化コンテンツを接続した LAN や P2P を利用して各端末へと送り，あらかじめ共有しておくことや，一回の利用料，購入後の三日間は何回聞いても定額といったように，コンテンツ利用の方式を変えてのサービスも考えられる．

5.2 マルチメディアメッセージング

マルチメディアメッセージング (MMS) は，携帯電話で P2P システムを実現する技術である．特徴は，複数のメディア・ソース（文字，音声，画像，動画など）を統合し，これらを同期化したメッセージを送受信できることである．たとえば，MMS を使うと，テキストおよび動画像付きのディジタル・ポスト・カードなどを送受信することが可能になる．

5.3 電子チケット，電子マネー

携帯電話を使った電子チケットは，携帯電話の赤外線通信を利用する形で提供されている．携帯電話は赤外線通信でパソコンなどと通信することで，チケットを確認できるようになっている．チケット販売サイトにアクセスし，電子チケットを購入できる．購入したユーザの情報をチケット販売事業者が正確に把握できることや，ネットワークを介して個人間でチケットのやりとりができることが利点である．

また，携帯電話を使った電子マネーとしては，日本コカコーラなどによる「Cmode」サービスが代表例として挙げられる．Cmodo 対応の自動販売機が認証データを Cmode サイトに送信しユーザを特定する仕組みになっている．ユーザが現金を投入すると，自動販売機 Cmode サイトの現金の残高を増す機能も提供されている．

様々な既存のサービスに対して，携帯電話が仲介することによる利便が広がっていくと考えられている [8]．

6. 超流通型画像共有アプリケーション

上で述べたような動向を考慮すると，近い将来には，携帯電話を主とする携帯端末が身分証明の機能，日常生活の様々な決済機能を担うと考えられる．

本研究では，将来の携帯端末が持つべき機能を明確にするために，携帯電話に課金機能を組み込んだシステムを構築し，このシステムを既存の P2P 型の画像共有システムに適用させた．本節では，このシステムについて詳述する．

6.1 PicShare

PicShare は，JxtaCast プロジェクトにより提供される P2P 型画像共有アプリケーションであ

り，P2P プロトコルとして JAXA を利用している [9, 10, 11]．それぞれのピアには，ピクチャーフレームが表示されており，そこに画像を表示させると同じピアグループに属する他のメンバーすべてに画像の配信が行われ，グループ内の他のすべてのピアのピクチャーフレームにその画像が表示される．画像と共に文字によるメッセージの送受信も可能で，さらに受信した画像はファイルとして保存することができる（図 1 参照）．

図 1: PicShare の初期画面

6.2 画像の共有

上述の PicShare を用いて，暗号化した画像をパーソナルコンピュータ (PC) と携帯端末間で次の手順で共有することができる．携帯端末は，JXME(JAXA for J2ME) プロトコルを利用した通信を行う．

1. PC においてリレーピアを起動.
2. 携帯端末の画像共有アプリケーションを起動し，携帯端末をリレーピアに接続する.
3. PC において PicShare を起動.
4. 携帯端末側で PicShare と同じ P2P による画像共有のピアグループに参加する.
5. PicShare の画面のピクチャーフレームの中へ共有したい画像をドラッグ & ドロップする.

以上の手順で，画像は同じピアグループに属する端末へと配信され共有される（図 2 参照）．

図 2: スクランブル画像を共有した例

それぞれの画像はユニークな固有の画像識別 ID(以下画像 ID) を持ち，以下の議論では，携帯端末も同様に個々の識別 ID（以下個人 ID) が定められていることを前提とする．また，将来的には PicShare を起動することなく，バックグラウンドでコンピュータの空き時間を利用し，画像共有を自動で行うことも可能である．このとき共有される画像は暗号化されたコンテンツであるため，復号鍵を入手していない限り正しく表示されない．この復号鍵をコンテンツキーと呼ぶ．

6.3 ユーザ認証

上で述べたように，画像を表示する時は，コンテンツキーを取得することになる．将来的には他人の所持している画像を買いたいときに，その人と通信をして画像 ID をもらい，それを用いて画像買い取りが行えるようになる．これは赤外線通信または有線で行われるものとし，これら ID は外へ漏れることがなく，安全性が確保されているものとする．携帯端末がサーバに ID を送ると，ここで携帯・サーバ間の認証が行われる．今回は認証に以下に述べるような暗号鍵方式を用いた（図 3 参照）．

1. 携帯端末は表示したい画像 ID と自分の個人 ID をサーバに送る.

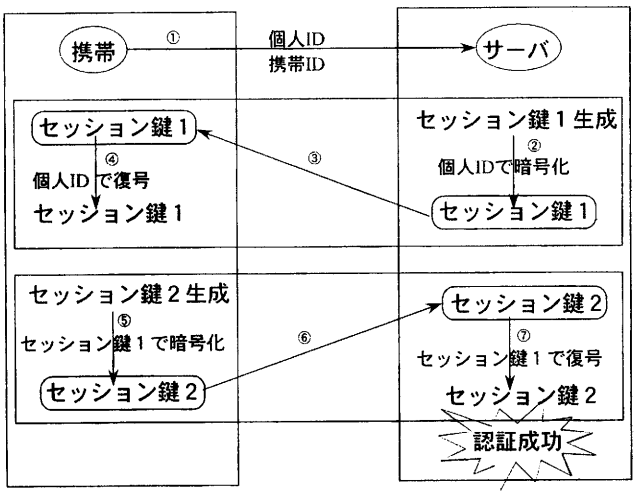

図 3: 画像共有における認証手順

2. サーバは携帯端末から個人 ID を受け取ると,乱数によってセッション鍵 1 を生成する.
3. 作られたセッション鍵 1 は個人 ID で暗号化して携帯端末へ送られる.
4. 携帯端末は受け取ったデータを自分の個人 ID で復号し，セッション鍵 1 を取り出す.
5. 乱数によってセッション鍵 2 を生成し，それを先ほど取り出したセッション鍵 1 で暗号化しサーバに送る.
6. サーバは送られてきたデータをセッション鍵 1 で復号し,セッション鍵 2 を取り出す.

これが成功すると，サーバ・携帯端末間の認証が成功したことになる．暗号化と復号は，端末内で行うことが望ましい．今回は携帯端末用のサーブレットを用意して，送られてきたデータをサーブレットで処理する方法を採用した.

6.4 課金システム

認証が終了すると，画像データベースの検索が行われる．画像データベースには，いくつかのテーブルがあり，画像 ID や料金などの画像情報，クライアントがその画像を参照した回数，ユーザ情報が入っている．この課金システムでは，料金を払って画像を参照するたびに，データベース内で画像参照回数が増えていく．それが画像ごとに定められた一定回数に達すると買い取りとみなされ，次回からは課金されることなく画像表示を行えるようになっている．また，画像を参照する際に「一回参照」と「一括購入」を選択でき,「一括購入」を選べば一度で買い取りをすることも可能である．一回参照と一括購入はそれぞれ料金が決まっており，データベースに収められている.

1. サーバは携帯端末から送られた画像 ID と個人 ID を受け取る,
2. 画像 ID から画像の料金を検索する,
3. 画像 ID と個人 ID から，クライアントがその画像を何回参照しているかを調べる,
4. 携帯端末に検索結果が送られ，画像の料金と「一回参照」,「買い取り」,「やめる」の選択肢が表示される（図 4 参照）.
   ここで参照している回数が，画像の買い取り回数を満たしていたら，一回参照の料金で買い取れる,
5. 「一回参照」または「買い取り」を選択すると，完了したというメッセージが現れる（図 5 参照）.
6. サーバは携帯端末事業者の課金データベースに料金データと個人 ID を送信し，課金がなされる．この料金は携帯端末の使用料金と共に，一括請求されることになる.

図 4: 画像表示料金の選択画面

図 5: 画像購入後の画面

6.5 コンテンツキー

買い取りが終了するとサーバは画像 ID に対応したコンテンツキーを検索する.

1. 個人 ID とセッション鍵 2 で二重に暗号化し，携帯端末に送る.
2. 送られてきたコンテンツキーは，携帯端末内に格納される. 本来は耐タンパ性モジュールに格納するが，今回は代わりとして RecordStore を用いた. RecordStore とは，MIDP で定義されている，端末側にデータを保存できる機能である.
3. 画像表示をするために携帯端末は，コンテンツキーを復号して取り出す.
4. コンテンツキーを用いて画像の復号を行い，画像は正常に表示されることになる.
5. 「一回参照」だった場合は，ここでコンテンツキーを破棄する.「買い取り」の場合には，このまま安全な格納場所に保管することになる.

コンテンツキーをこの携帯で使用せずに，自分の PC や他者に譲渡することもできるが，今回は，自分の携帯上での表示のみを実装した.

7. 今後の計画

本稿で報告したシステムは，携帯端末の所有者と画像を表示する媒体の所有者が同一であることを前提とした. 実際には，他人にコンテンツをプレゼントすることも考えられ，自分が購入したコンテンツキーを他人に譲渡できるようなシステムを検討中である. 料金は自分が支払い，コンテンツの利用権を他人に贈ることが可能となる. この機能が実現されれば，ユーザ同士の情報交換が活発になり，コンテンツ販売数の上昇にもつながる.

また，ユーザ認証においても，コンテンツの不法コピーを防ぐためには，より高いセキュリティを持つ認証技術が必要とされる.

このような観点から，携帯端末を媒体とする超流通型 P2P の実用性を確保するために，以下のようなシステムの検討を行っている.

パソコンと携帯端末間の通信 今回はパソコン内の仮想携帯端末を用いてプログラムを開発したが，実際の場面ではパソコンから画像 ID を送信する際に，パソコンと携帯端末を接続する必要がある. 赤外線や Bluetooth などの無線通信の利用を検討している.

コンテンツの他人への譲渡 コンテンツの受け取り人と料金支払人とを別に認証することにより，他者へのコンテンツ譲渡を可能にする. そのためには，携帯端末同士で相互に認証を行う機能が必要となる.

指紋認証などによる個人認証 指紋認証などの

認証システムを組み込むことによって，使い勝手がよく確実な個人認証機能を組み込む．

音楽・動画コンテンツへの対応 本稿で報告したシステムは静止画像のみを対象としている．今後は音楽や動画像などの様々なコンテンツへの対応を進めたい．

8. むすび

本研究では，超流通型P2Pモデルの画像配信システムを例にとり，携帯端末を媒体とした認証と課金システムの実装について報告した．

本稿で述べたような超流通型P2Pでのコンテンツの共有が一般的となれば，コンテンツの利用と利用料の支払いが簡単な手数で行えるようになる．また，P2Pの実用化の課題のひとつである個人認証についても，指紋認証などを用いた携帯端末を媒体とすることで確実に行えるようになる．

今後は，上で述べたような実用的な超流通型P2Pアプリケーションの構築を目指して，研究を進める予定である．

参考文献

[1] Mori,R., Kawahara,M.: "Superdistribution : The Concept and the Architecture", The Trans. of IEICE, Vol.E73, No.7, pp.1133–1146 (1990)

[2] Mori, R., Kawahara, M. : "Superdistribution: An Electronic Infrastracture for the Economy of the Future", Trans. IPS. Japan, Vol.38, No.7, pp.1465–1472 (2000).

[3] 荒牧久美子，箕浦美智子，麓真祈子，佐藤浩史，河原正治: "超流通型P2Pアプリケーションにおける認証について"，情報処理学会研究報告，Vol.2002, No.117(EIP–18), pp.29–36 (2002).

[4] 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靭化を実現した開放型超流通基盤"，情報処理学会研究報告，Vol.2001, (2001–EIP–14), pp.31–42 (2001)

[5] http://www.beepscience.com/

[6] 仁野裕一，中村暢達，田口大悟，谷幹也: "携帯電話向けJava実行環境を用いた著作権管理システム"，情報処理学会研究報告，Vol.2003, No.17(EIP–19), pp.33–40 (2003)

[7] http://www.keitaide-music.org/

[8] "携帯電話は万能ツールの夢を見るか"，NIKKEI BYTE, pp.55–73 (2003).

[9] Brookshier, D., Govoni, D., Krishnan, N, Soto, J.: "JXTA : Java P2P Programming", p.413, Macmillan Computer Pub. (2002).

[10] http://www.jxta.org/

[11] 石原晋也，武本充治，田中健一郎："ワイヤレスP2Pがやってきた！"，JAVA PRESS, Vol.28, pp.102–146 (2003).