電子化知的財産・社会基盤 18－6
（２００２．１２．７）

超流通型P2Pアプリケーションにおける認証について

荒牧久美子† 麓真祈子† 箕浦美智子† 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

kumiko@act.is.ocha.ac.jp makiko.f@act.is.ocha.ac.jp
mino@act.is.ocha.ac.jp sato@is.ocha.ac.jp
masaji@k.tsukuba-tech.ac.jp

あらまし Peer-to-Peer(P2P) 型システムは，従来型のクライアント・サーバ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のためには，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．現在我々は，P2P システムに超流通技術を組み込んだ超流通型P2P システムにおいて，上のような課題を解決する方法を検討している．本稿では，P2P 型のチャットプログラムを例にとり，ユーザ認証の問題について検討し，指紋認証機能を使った解決方法について報告する．

キーワード 超流通，P2P，電子的著作権管理，ユーザ認証，指紋認証

User Authentication for P2P Applications Based on Superdistribution

ARAMAKI Kumiko† FUMOTO Makiko† MINOURA Michiko† SATO Hiroshi†
KAWAHARA Masaji§

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

kumiko@act.is.ocha.ac.jp makiko.f@act.is.ocha.ac.jp
mino@act.is.ocha.ac.jp sato@is.ocha.ac.jp
masaji@k.tsukuba-tech.ac.jp

Abstract Peer-to-Peer (P2P) system attracts a great deal of attention, since this system can solve the various problems existing in the current client-server 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 user-authentication. We are investigating new systems to solve the above-mentioned problems on the P2P system by adopting "the superdistribution technique." In this paper, we take up, as an example, a chat-program and present a solution for the user-authentication by using a finger print sensor method.

Keywords Superdistribution, P2P, Electronic Copyright Management, User Authentication, Fingerprint Authentication

1. はじめに

ここ数年の間に，Napster，Gnutellaといった Peer-to-Peer(P2P) 型のファイル共有アプリケーションが次々に発表され，短期間に数千万人の利用者を獲得し話題になった．このようなP2P システムは，クライアント・サーバシステムと違い，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．すなわち，どのコンピュータも情報を提供するサーバであり，また，情報を要求するクライアントでもある．P2P システムを使えば，Web サーバのような特定のコンピュータに登録された情報だけではなく，ユーザ個人のコンピュータに保存されている情報まで簡単な操作で交換することができる．

このような P2P 型システムは，従来のクライアント・サーバ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．

現在我々は，P2P システムに超流通技術を組み込むことにより，上の課題を解決する方法を検討しているが，本稿では，P2P 型のチャットプログラムを例にとり，ユーザ認証の問題とその解決方法について報告する．

以下では，P2P の簡単な説明と課題について述べた後，超流通および超流通技術を組み込んだ P2P システム (超流通型 P2P) の概要を説明する．次に，P2P 型のチャットプログラムに指紋認証機能を付加したプロトタイプシステムについて解説する．

2. P2P の概要と課題

2.1 P2P とは

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．共有される資源やサービスには，情報の交換，CPU の処理時間，一時的な作業領域の提供，永続的な保存領域の提供などがある．

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 システムを利用した有名なファイル共有アプリケーションが Gnutella である．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 システムの代表例が Napster である．Napster 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．

Hybrid 型 P2P の問題点は以下の通りである．

- Pure 型 P2P システムと違い，管理サーバによるセキュリティ管理などは容易に実現できるが，サーバの障害がシステム全体に影響を及ぼすという欠点がある，
- サーバで管理されているインデックスを使って情報検索は効率よく行えるが，そのインデックス情報が常に最新のものとは限らないという問題点も持つ．

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

3.1 超流通

「超流通」は，個人の創作活動の産物であるディジタルコンテンツを，著作権を保護しながら，安全かつ公平に，しかも経済的，効率的に流通させる，次世代の流通システムの概念である．

超流通の基本的な考え方は以下の通りであり，1983 年に森亮一（当時，筑波大学教授）によって提唱された．

1. ディジタル情報すなわちコンテンツと，それに関する超流通ラベルとを暗号化して公開する．これは誰でも自由に複製・交換できる．
2. これらと正しい復号鍵との 3 者があるときのみコンテンツを利用できる．
3. ユーザの手元において，超流通ラベルにしたがってコンテンツの利用が管理され，必要に応じて記録される．

コンテンツを暗号化して正しい復号鍵を持つときのみ利用可能にする方式は現在では広く使われているが，ここでは超流通を特徴づける「超流通ラベル」,「超流通ラベルリーダ」について解説する．

超流通ラベル　超流通ラベル（SDL: Superdistribution Label）は，コンテンツのメタ情報であり，権利者に関する情報，権利者が望む利用の条件（典型的には対価の支払い），世界中で一意に識別するためのコンテンツ ID などが含まれる．利用の条件は，プログラムで記述できるものならば原理的には実現可能であり，ユーザに歓迎されるような条件を設定することによって競争原理が働く．コンテンツとその SDL とは論理的に不可分であり，暗号技術などを用いて改変・除去から保護される．

超流通ラベルリーダ　超流通ラベルリーダ（SDLR: Superdistribution Label Reader）は，SDL の記載条件に従ってコンテンツの利用を管理する．正しい鍵を持つ SDLR がなければコンテンツは利用できない．また，SDL の記述によって，利用を許可する SDLR を指定することもできる．

超流通では，ディジタル情報の所有に対して課金するのではなく，電気や電話などと同じように，利用者がどのくらいディジタル情報を利用したかを計測し，それに応じて課金する．

利用量に応じて課金することは，必ずしも料金が利用量に「比例」するということではない．例えば，累積利用量といった情報を利用することで，権利者が指定したある限度までは課金さ

れない「無料試用」や，ある一定料金を支払うことでそれ以上は課金されない「買い取り」といった課金方法もできる．

料金体系の別の側面として，利用量の軸をどのように選ぶかという問題がある．わかりやすいのは「時間」や「回数」であるが，コンピュータソフトウェアの場合には「処理内容」なども可能である．

原理的には，計算機で処理できる方法ならばどのような料金体系であっても実現可能なので，利用者に快適な様々な料金体系を設定することができる．

3.2 超流通型 P2P

上のような処理はSDLRが実行するため，暗号技術，アクセス制御技術，タンパーレジスタントモジュールの採用などによって，コンテンツ，使用記録，暗号化鍵などを保護すると同時に，SDLRに対する不正なアクセス，SDLRのなりすましなどを防ぐ必要がある．

暗号化・復号機能，アクセス制御技術などを備えたSDLRが各ピアに装備されたP2Pシステムを実現すれば，コンテンツの課金だけではなく様々な新しいサービスを展開することができる．例えば，CPU時間，ディスク領域などについてもユーザが利用料金を指定できるようになる．朗読やカウンセリングといった人的なサービスについても適切な料金設定と競争が実現されるだろう．

このように超流通型P2Pでは，著作権を保護すると同時に，多数のユーザをオンラインでサービス可能状態にすることができる．

3.3 SDLRと個人認証

上で述べたように，超流通型P2Pにおいて多様なサービスを展開するためには，SDLRが利用者の個人認証を的確に行う必要がある．

個人認証機能を装備することにより，

- コンテンツのより的確な利用者制限，
- 人的サービス課金の場合のなりすまし防止，

などが可能となる．

認証機能の中で今注目されているのが指紋や静脈に代表される生体的な特徴や行動上の特徴を使ったバイオメトリクス認証である．以下にいくつか例を示す．

指紋 指紋にある特徴的な情報を抽出し，その方向などから判別する特徴点抽出方式と，指紋を画像として取り込み画像同士を重ね合わせて照合を行うパターンマッチングに大別される．

顔 顔の形を読み取る方式．目や口などの部位を基点にした2次元位置データとして照合する方式や3次元計測による照合などがある．

網膜 眼底の毛細血管の模様を用いる．

虹彩 黒目の中（瞳孔の外）にある模様を用いる．

掌（手形，掌紋） 手の大きさや形を読み取る方式や，掌にある指紋と同じような紋様を用いる方式がある．

静脈 掌の甲の皮膚の下にある静脈血管のパターンを用いる．

声紋 声の波形に表れる特徴を抽出し，その個人差を識別する．

以上のように様々なバイオメトリクス認証が提案されているが，虹彩や声紋などを使う方式は技術的に未成熟で実用例が少ない．そこで，個人認証機能つきSDLRの有効性を示すために，実現が比較的簡単で実用性の高い指紋認証を採用することにした．

4. プロトタイプの構成

プロトタイプの主要な構成要素は以下の3つである．

- P2Pチャットプログラム
- SDLRエミュレータ
- 指紋認証モジュール

以下では，これらの構成要素について解説する．

4.1 P2Pチャットプログラム

P2PチャットプログラムはJava言語を使用したが，P2Pの通信プロトコルとしてJXTAを利用した．以下でJXTAについて簡単に説明する．なお，P2Pチャットプログラムの詳細については，5.節で述べる．

4.2 JXTA

NapsterやGnutellaなどでは，各ピア間でどのような手順でデータを検索・送受信するかなどのプロトコルはそれぞれ独自に開発されたものであった．P2Pを実装するための共通のプロトコルがあれば，開発コストを削減できると同

時に各アプリケーションを協調して動かすことも可能となる．このような発想をもとに，Sun Microsystems社が中心となってJXTAプロジェクトの活動が始められた．

JXTAはプロトコルのみを規定しており，言語やOSなどの動作環境，P2Pアプリケーションが動作するネットワークに依存しないことに特長がある．このため，TCP/IPのみではなく携帯電話網など多種多様なネットワークを使った実装も進められている．

また，JXTAはアプリケーションのサンプルコードなども含めて完全なオープンソースプロジェクトとして運営されており，JXTAを使って様々なサービスを比較的容易に実装することができる．

JXTAは，資源発見・通信機構と，資源の抽象化機構から構成される．JXTAにおける各ピアは，提供可能な資源が書かれたメッセージを，異なるピア間で交換する．JXTAの核となる部分では基本的な以下の6つのプロトコルが規定されている．

Peer Discovery Protocol 各ピアによる資源の告知と発見のためのプロトコル．

Peer Information Protocol ピアの状態を監視するためのプロトコル．

Peer Resolver Protocol 他のピアに問い合わせを送り，応答を受信するためのプロトコル．

Pipe Binding Protocol ピア間の通信を行うための仮想的な通信路（パイプと呼ばれる）を生成するためのプロトコル．

Peer Endpoint Protocol ピアへの経路を選択するためのプロトコル．

Peer Membership Protocol ピアの集まりが形成するピアグループへの参加要求，それに対する許可，参加取り消しなどを実現するプロトコル．

JXTAでは上の6つのプロトコルを組み合わせて，様々なP2Pアプリケーションから利用可能なファイル交換，分散検索，ストリーミングなどのサービスを提供することができるようになっている．

4.3 SDLRエミュレータ

SDLRは，コンテンツのメタ情報にしたがってコンテンツの利用を管理する．メタ情報にはコンテンツの利用料をはじめ利用者制限に関する情報などが記載されている．例えば，CPU時間やディスクの使用領域に応じた課金も可能である．したがって，典型的なSDLRは，

- 課金機能，
- 暗号化・復号機能，
- 実行制御機能

を持つ．

SDLRは，素子技術の急激な進歩に伴って，ハードウェアを使用したタンパーレジスタントモジュールによる実装が主流となる方向にある．

本研究では，上の3つに追加して個人認証機能の有効性を試すために，実装が容易なソフトウェアでSDLRを実現することにした．このSDLRは，C++言語を使ったダイナミックライブラリによってエミュレーションされており，下で述べる指紋認証ソフトウェアのライブラリと組み合わせて動作する．

4.4 指紋認証モジュール

認証には，顔・虹彩・静脈・声紋など様々な方法があるが，3.3で述べたように本研究では指紋認証を用いることにした．認証の方法はあくまで手段であり，指紋以外の認証方法でも問題はない．

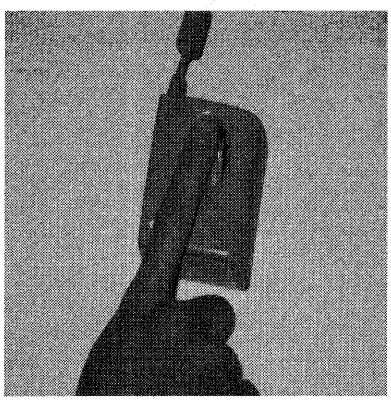

図 1: 指紋認証装置

指紋認証には，OMRON(株)のFPS-3000指紋照合システム・ソフトウェア開発キットVer.2.1

のCライブラリを使用した．このライブラリは，図1に示した指紋センサー部とともに動作する．

指紋照合システム・ソフトウェア開発キットは，5つのダイナミックライブラリ(DLL)と，4つのCライブラリから構成されている．まず指紋を管理するためのデータベース・ツールを，ダイアログ形式のデータベース管理ソフトとして作成した．機能としては，新規指紋データベースの作成，1個人が左右10本の指まで登録可能とし，登録データの削除，ユーザ一覧表示ができるごく標準的なものをツールとして用意した．

指紋データベース管理ツールで作成された指紋データベースは，認証用の指紋辞書として使用される．指紋データベースはCによるダイアログ形式のツールで作成されたものであり，指紋認証ライブラリは前述の指紋データベース管理ツールに対して認証の可否のみを与えればよい．

5. プロトタイプの動作

5.1 アプリケーションの初期化・開始

チャットアプリケーションを起動すると，JXTAプラットフォームの初期化を行う．起動後の画面を図2に示す．ここで，P2Pチャットのピアグループに参加するためのユーザ名とパスワードを登録する．

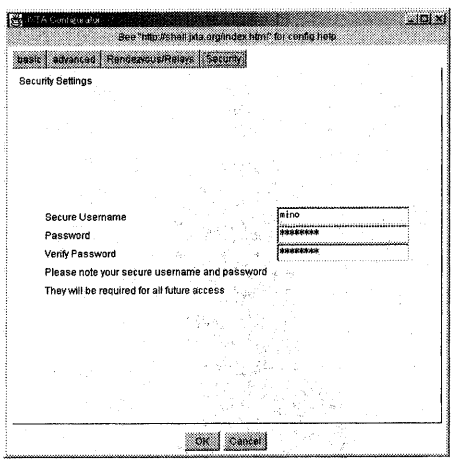

図 2: ピアの初期化画面

次に，チャット用告知の生成（create）または探索（find）を行う．告知が見つかった場合，チャットを行うかどうかのダイアログを表示させ，ユーザーは，“Yes”，“No”，“Cancel”のいずれかを選択する．“Yes”を選択すれば，チャットが行える環境となる（図3）．告知の生成・探索にはJXTAのPeer Discovery Protocolを用いる．

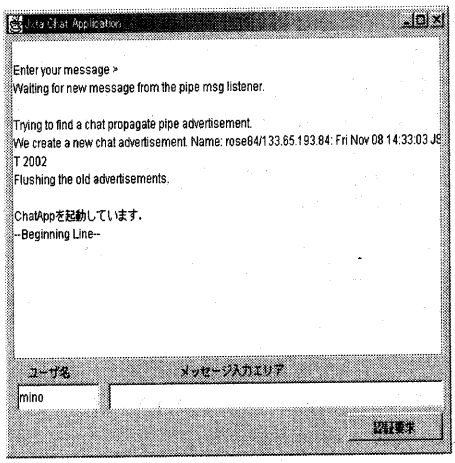

図 3: 告知公開画面

告知が見つからなかった場合，新しい告知を“create”するか，または再び告知を“find”するかのダイアログを表示させる．ここで“find”が選択されると告知が見つかるまで以上の動作を繰り返す．

5.2 チャットの開始

メッセージ入力エリアに文字を入力しエンターキーを押すことで相手に文字列が送信される．メッセージの送受信は，JXTAのPipe Binding Protocolを使い，ピア間に仮想的な通信路を形成することで可能となっている．

チャット中はいつでも認証要求ボタンを押すことができる．認証要求の動作については下で述べるが，この機能によって，相手がその場にいることをいつでも確認できるようになる．

5.3 認証要求

認証要求ボタンが押されると，チャットを行っている相手側の端末に「指紋認証要求がきました」というダイアログが表示される（図4）．この要求に対して“Yes”，“No”の選択ができる．

ここで，“Yes”を選択した場合は，指紋セン

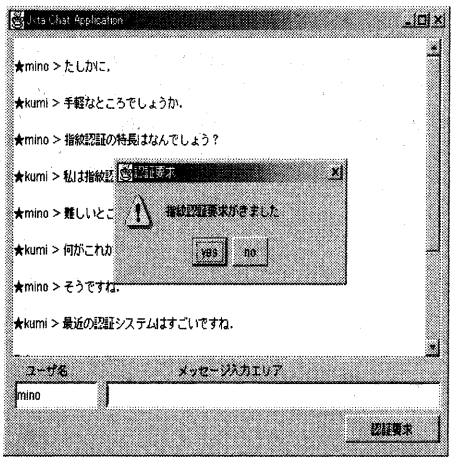

図 4: 認証要求画面

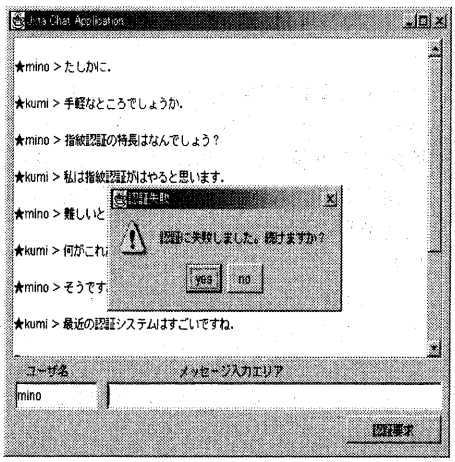

図 6: 認証失敗

サーを用いて認証を行う．図 5 に示した指紋認証画面が表示される．ここで，指紋センサーに指を置くことで指紋認証が行われる．

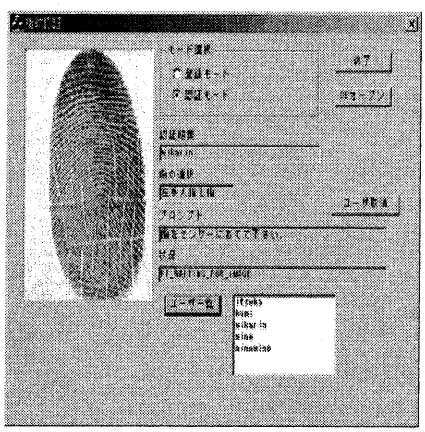

図 5: 認証画面

本人であることが確認されれば，認証要求をしたユーザーのところに,「認証に成功しました」というダイアログが表示される．本人であることが確認できない場合は認証要求をしたユーザーのところに「認証に失敗しました」というダイアログが表示され，それでもチャットを続けるかどうかを選択させるダイアログが表示される．

“Yes”を選択すれば，チャットはそのまま続行され，“No”を選択すればチャットは終了となる．

6. 今後の計画

ファイル交換ネットワークにおいて，情報の提供側も利用者も納得のいく形で著作権使用料を徴収できるならば問題はない．しかし実際にはNapsterやGnutellaなどで公開されたデータの多くは，個人が勝手にデジタルコピーした音楽であり，また交換される者たちが未知の他人同士であり著作権を侵害していた．

しかし，ファイル交換ネットワークという考え方は，短期間に数千万人のユーザを集めたことからもわかるように便利なシステムである．本格的な常時接続環境が整えば，膨大な金額を投じてシステムを構築する必要もなく，世界中が並列コンピュータをつなげた状態と巨大なデータベースを擁した状態が実現されることになる．

このように見ていくとファイル交換ネットワークそのものを禁止することは妥当な選択でない．問題なのは著作物の違法コピーが簡単に配布できるところにある．つまり，著作権者になんらかの利益還元ができる仕組の構築こそが不可欠である．

このような観点から，超流通型 P2P の実用性を確認するために以下のようなシステムの検討を行っている．

ファイル共有機能 P2P システム上で，上で報告したユーザ認証機能を付加したファイル

共有システムを開発し安全な共有を実現する．

音楽データの交換と課金 ファイル共有を発展させて音楽データの交換と課金を実現する．

携帯端末での実装 音楽配信においては，家の中に固定されたパソコンより，携帯電話などの携帯型の端末への配信が普及すると考えられる．また自宅のパソコンでダウンロードしたものを，携帯型の再生装置などに転送して持ち歩きたいというニーズも今後拡大していくだろう．そこで，以上のようなアプリケーションを携帯電話上で実現することにより，より実用性を高くしていきたい．

7. むすび

本研究では，超流通型 P2P アプリケーションの簡単な例として，P2P チャットを実現した．従来にはない，指紋による個人認証要求機能というオプションをつけることにより，利用者間の信頼できる通信を可能にした．指紋認証による本人確認の正否によってプログラムの動作を利用者が選択できるようにし，利用者は安心して通信プログラムを利用することができる．

P2P アプリケーションの実装にはオープンなプラットフォームである JXTA プロトコルを用いた．

今後は，上で述べたように本格的な超流通型 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] 河内 正夫, 小柳 恵一: “P2P インターネット新世紀”, p.153, 電気通信協会 (2002)

[2] Brookshier,D., Govoni,D., Krishnan,N., Soto,J.: “Jxta: Java P2P Programming”, p.413, Macmillan Computer Pub. (2002)

[3] Mori,R. and Kawahara,M.: “Superdistribution : An Electronic Infrastructure for the Economy of the Future”, Trans. IPS. Japan, Vol.38, No.7, pp.1465–1472 (1997)

[4] 大瀧保広, 河原正治: “超流通における使用記録の回収とプライバシー保護”, 情報処理学会論文誌, Vol.41, No.11, pp.2978–2984 (2000)

[5] “Project JXTA”, http://www.jxta.org/

[6] 菅知之編: “特集 ここまできたバイオメトリックスによる本人認証システム”, 情報処理, Vol.40, No.11, pp.1072–1103 (1999)

[7] オムロン（株）: “FPS-3000 指紋照合システムソフトウェアキット Ver.2.1”, p.141 (2001)