# IC カードを利用した P2P による コミュニケーションプラットフォームの提案

小宅宏明† 宮地玲奈†
菅原陽子† 岡田謙一†

近年，常時接続環境の普及にともない，どこででも利用可能で安全なコミュニケーションプラットフォームの需要が高まってきている．その一方で，任意の端末を使用することで，セキュリティの確保や，コミュニケーションに必要な情報の携帯手段が課題となっていた．本論文ではピア・ツー・ピア型のネットワークを用いて協調作業のためのグループを構築し，またグループ構築に必要な情報を IC カードによって携帯することによって，ユーザの移動に対応した安全なコミュニケーションプラットフォームを実現する方法を提案した．

# A Proposal for P2P-based Communication Platform Using IC Card

Hiroaki Ohya,† Reina Miyaji,† Yoko Sugawara† and Ken-ichi Okada†

Recently, the demand of a communication platform that it can use anywhere and safe has been increasing with the spread of regular connection environment. The pocket means of reservation of security and information required for communication had become a subject by on the other hand using arbitrary terminals. In this paper, the method of realizing the safe communication platform that can deal with movement of a user was proposed by building the group for cooperation work using a peer to peer type network, and carrying information required for group construction by the IC card.

## 1. はじめに

近年，異なる組織の人間同士が組織の壁を越えて一時的なチームを作りコラボレーションを行う機会が増えつつある．しかし組織の異なるグループのメンバ全員が同じ場所に集まって作業を行うのは時間的，空間的な調整が難しく頻繁に行えるとはいいがたい．そのような中で，ネットワークを介し，PC などの端末を利用して他のメンバと「いつでも」「すぐに」協調作業を行えるようなシステムが求められている．

また，ユーザが利用する端末を考えると同一のユーザが自宅，職場，モバイル端末，出先にある端末を一時的に借りるなど複数の端末を使用している．このように同じユーザでも使用する端末は毎回同じであるとは限らない．将来的には，ユーザは端末を持ち運んで利用するのではなく，自分の PC 環境のみを持ち運んで端末自体はその場にあるものを利用する，という形態も考えられる．そうなると使用する端末は毎回のように異なると考えられる．

そして端末が同じでない場合，当然端末が属する環境も異なる．ここで述べている環境とは IP アドレスやドメイン名，ファイアーウォールの有無などである．

協調作業のためのシステムにおいて，上述の点を考慮し，ユーザが異なる環境下のどの端末を使用しても同じようなシステムであるということが望ましい．

以上のことから，同期分散型のコミュニケーションプラットフォームに求められる条件は以下のようになる．

- アドホックにグループを構築し，コミュニケーションがとれること
- 端末および端末の属している環境に依存せず，相互運用が可能であること
- 通信が安全であることを保証していること

既存の同期分散型コミュニケーションプラットフォームとしてはロータスノーツのようなクライアント/サーバ型のものや NetMeeting のようなピュア P2P 型のものなど，様々なものが提供されている．しかしクライアント/サーバ型システムではサーバの導入・管理に

† 慶應義塾大学大学院理工学研究科
Faculty of Science and Technology, Keio University

大きなコストがかかる，機能の拡張がサーバに依存するといった欠点があり，またピュア P2P 型ではファイアーウォールによる利用の制限がある，プライベート IP アドレスを割り振られている端末どうしだとピュア P2P による通信を行えないなどの欠点があった．

そこで本論文ではハイブリッド型 P2P のネットワーク上で IC カードを利用した同期分散型コミュニケーションプラットフォームを提案する．本提案ではハイブリッド P2P 型ネットワークを使用することでアドホックなグループ構築を可能にし，Rendezvous Point というサーバ的役割をなす特殊なピアを設け，それをグループメンバの「待ち合わせ場所」とすることで，プライベート IP アドレスを持ち，ファイアーウォール下にある端末どうしの通信を可能にする．また，Rendezvous Point の情報とメンバ同士の認証，通信の暗号化に使用する暗号鍵を IC カードに格納し，ユーザがそれを携帯することにより，移動先での様々な端末および端末の属する環境を意識せずに安全に協調作業グループを構築し，作業を行うことが可能となる．

2 章では同期分散型協調作業を行うためのアーキテクチャについて，3 章では本提案である IC カードを利用した安全な P2P コミュニケーションプラットフォームについて述べ，4 章では関連技術，5 章では実装したシステムについて，6 章で評価実験と考察について述べ，最後に 7 章でまとめについて述べる．

## 2. 同期分散型コミュニケーションアーキテクチャ

ネットワーク環境に依存せずアドホックにグループ構築を行う同期分散型の協調作業を行うためのアーキテクチャとしては，ICQ や IRC などのクライアント/サーバ型，各々の端末が完全に対等な役割を果たすピュア P2P 型，サーバを併用して効率化やセキュリティの強化を図るハイブリッド P2P 型があげられる．

クライアント/サーバ型のシステムでは同一のサーバを利用できない環境では協調作業を行うことができない場合が多く，また前もってサーバにアカウントなどを用意する必要があるためアドホックな作業を行うには困難である．また，サーバの導入や管理，カスタマイズをするのには大きなコストが必要であるため，ある一定の期間のみグループを組んで作業を行うには適していない．

また，ピュア P2P 型のシステムでは，通信相手のネットワーク的な位置情報を管理するサーバがないため，どちらか一方が他方の位置情報を認知する必要がある．本論文では協調作業を行うのに使用する端末は不特定であるものとするため，ネットワーク上の位置を識別することができない場合協調作業を行うことができない．たとえば NAPT（Network Address and Port Translation）によってプライベート IP アドレスを割り振られた異なるネットワーク上に存在する端末どうしは，互いのネットワーク上の位置を知ることができないため，ピュア P2P による通信を行うことができない．したがってピュア P2P 型のシステムはアドホックなグループ構築には適していない．

また，協調作業を開始する際に，使用する端末が不特定である場合毎回ユーザの探索をする必要がある．P2P システムではノードごとに分散しているリソースを検索する仕組みを用意されている場合が多い．P2P システムにおいてユーザを探索する方法としてはリソース検索の仕組みを用いる方法が考えられる．

ピュア P2P 型のシステムでは次のようにリソース検索を行う．各ノードが他のノードに検索コマンドを発行し，検索コマンドを受け取ったノードはさらに他のノードに検索コマンドを転送する．そして自分のノードにリソースがあればそのことを検索コマンドを発行したノードに通知する．現在，この分野では FastTrack[4]や Jxta Search[6),14)]など，役割の異なるノードを階層的に組み合わせたり，FreeNet[5)]のようにピアにコンテンツキャッシュを持たせるなどのアプローチによって検索効率を高める研究が行われている．どちらの方式を用いてもある一定時間内に検索を終了できることを保証できない．捜しているユーザが検索した範囲内にいる場合のみ発見可能であるが，協調作業を行う場合通信相手を必ず発見しなければ作業が行えないため適切でない．また，本論文では 2〜10 人規模のグループでの協調作業を想定しているため，上記の方法を利用して相手を探す場合，仮に全員が発見できると仮定しても捜索時間が長くなると考えられる．

よって同期分散型協調作業をアドホックに行う場合においてはノードの発見とリソースのディレクトリサービスをサーバが行い，環境ごとに異なるサーバを設置する必要がないという点でハイブリッド P2P 型のアーキテクチャを使用するのが適しているといえる．

しかしハイブリッド P2P 型のアーキテクチャを用いても次のような問題点が発生する．ピア間での認証や通信においてのセキュリティ面での問題である．

ハイブリッド P2P 型では端末–サーバ間の認証は行われるが，ピアどうしが互いを客観的に認証する手段を持たないため，真正性を保証するのが困難である．特定の端末を利用する場合において，ピア間で安全な通信を開始する手順は文献 3) で初めて通信を行うピ

アどうし，過去に安全な通信を行ったことのあるピアどうしの認証について述べられている．しかし本論文においてはユーザが利用する端末は特定のものではないと想定しているため，文献 3) における方法を使用することができない．なぜならば端末はユーザが初めて使用するものであるため，認証を必要としている端末どうしは過去に安全な通信を行ったことはなく，また双方の端末にとって信用できる第三者のピアも存在しないからである．よってこの場合別の何らかの形で認証を実現する手段が必要となる．

また，ピアどうしの通信ではその内容が無関係のピアを経由してルーティングされる．よって盗聴と改ざんの危険性がある．これらの解決方法としては公開鍵暗号または秘密鍵暗号による通信内容の暗号化といったものがあげられるが，利用する端末が特定のものでない場合，鍵を直接端末に入れることはできない．よって端末が変わっても暗号化が可能な手段が必要となる．

## 3. IC カードを利用した安全な P2P コミュニケーションプラットフォーム

本論文における同期分散型のコミュニケーションプラットフォームで想定している協調作業の形態は以下のとおりである．

### 3.1 想定形態

- 本提案を利用するユーザは，広域なネットワークに数百人〜数千人規模で分散して存在しているものとする．そしてその中で，同じ目的を持った 2〜10 人程度が協調作業グループを構築し，作業を行う．
- 本提案を利用するユーザの端末の環境はそれぞれ毎回異なる．よってグローバルアドレスを持つ端末，ファイアーウォールの中にあって外のネットワークからは見えない端末などが対象である．
- 同期分散型の協調作業なので，作業への途中参加，離脱もありうる．

以上の点を考慮し，本提案では同期分散型コミュニケーションプラットフォームとして適切なハイブリッド P2P 型ネットワーク上において，IC カードを利用することにより利用する端末のおかれた環境に依存せず，かつ安全なコミュニケーションを可能にするシステムを提案する．

本論文が想定している同期分散型の協調作業では端末の環境が毎回異なる．このためには使用している環境に依存せずに通信相手を確実に発見し，ピアどうしで認証を行い，通信の安全性を保証するものでなければならない．また，グループを構築する際，ユーザが煩わしい作業を行うことなく，協調作業を即座に開始することができるよう設計すべきである．これによりユーザは本来の目的である協調作業のみに集中することができると考えられる．上述のような点を考慮すると以下のような技術用件が整理できる．

### 3.2 情報の携帯

任意の端末で協調作業を行うためには，グループ構築と通信に必要な情報をつねに取得できる手段が必要である．本提案では情報を取得する方法として IC カードによる情報の携帯を採用する．IC カードはカードとカード内にある情報を読み取る IC カードリーダライタで構成される．カードに必要な情報を入れ，携帯することによってユーザは任意の端末から協調作業を行うことが可能となる．

IC カードはユーザの利便性と耐タンパ性（不正なデータ解析に対する耐久能力）をあわせ持つデバイスであるため，認証情報のような秘密にする必要のある情報を持ち運ぶのに適している．

### 3.3 ユーザの探索

協調作業を行うためには，同じグループのメンバを確実に発見する必要がある．そこで 2 章であげたようなリソース探索法を利用したユーザの探索ではなく，本提案では Rendezvous Point という特殊なピアを用いることによりグループのメンバを探索する．Rendezvous Point とは一種の「待ち合わせ場所」であり，ユーザ 1 人またはグループ 1 つにつき 1 つの Rendezvous Point が存在する．たとえばユーザ A がユーザ B を探す場合にはユーザ A はユーザ B の Rendezvous Point に対してユーザ B を探索する検索コマンドを発行する．この方法はハイブリッド P2P 型のサーバを 1 つに限定することによって検索効率を高めると同時に検索範囲を限定して，必ずユーザを発見できるようにする方法であると考えることができる．

一方でユーザ Rendezvous Point を発見するために，Rendezvous Point はつねに一意に識別できる必要がある．このため，Rendez Point となるピアはファイアーウォールの内部にあってはならず，またつねに同じ IP アドレスを持っている必要がある．これらの条件を満たす Rendezvous Point を利用することでコミュニケーションをとりたいユーザの端末の IP アドレスを知らなくても，そのユーザを検索することが可能となる．

### 3.4 協調作業グループの構築

ユーザは IC カードを携帯し，移動先でその場にある端末を用いて次のような手順でシステムを利用し，

他のユーザとグループを構築する．

ユーザはICカードを端末のICカードリーダライタにセットすると，アクセス可能なユーザの一覧，およびグループの一覧が表示される．一覧の中からユーザはコミュニケーションを行いたい相手，グループを選択する．本システムが通信相手のRendezvous Pointへ接続し，選択されたユーザをネットワーク上で検索する．発見されれば相手に接続要求を出す．相手によって接続要求が許可されると，相手側のシステムと相互認証を行う．認証が成功すればグループが構築され，グループ内で協調作業が可能になる．

### 3.5 認　　証

本提案では認証アルゴリズムとして公開鍵暗号と共通鍵暗号を使う2種類のモデルを用いる．両者はなるべく違いが少なくなるように考慮されており，どちらの方法を用いても安全に同期分散型の協調作業を行うことができる．両者は排他的なものではなく，協調作業を行う相手に応じて同一のシステム上で併用することが可能である．たとえば，日頃公開鍵サーバを利用している相手には公開鍵暗号による方法を利用し，そうでない相手には共通鍵暗号による方法を利用する，といった使い分けが考えられる．

#### 3.5.1 共通鍵を用いる場合

共通鍵を用いる場合には公開鍵を用いる場合と比べて，より簡単にシステムの構築を行うことができるが，共通鍵を安全に共有するための仕組みが必要になる．最も安全な方法としては，鍵を共有するユーザが物理的に集まって同一の端末から鍵を供給する方法が考えられる．本提案では以下のような方法を用いる．

**認証**　チャレンジ・レスポンス方式[16)]

$Response = h(Challange||SecretKey)$

チャレンジ・レスポンス方式を用いることにより，共通鍵をカードから端末に読み込むことなく認証を行うことができる．なお，$h()$ はハッシュ関数，$||$ は連結を意味する．

**機密性**　共通鍵暗号を用いてセッションキーを共有し，セッションキーを用いてエンドツーエンドで共通鍵暗号による暗号化を行う．セッションキーの生成はカード内で行い，通信内容の暗号化はカード内で生成されたセッションキーを用いて端末上で行う．

**データの完全性**　メッセージをMAC（Message Authentication Code）に付加する．

$MAC = h(Message||SecretKey)$

#### 3.5.2 公開鍵を用いる場合

公開鍵を用いる場合，鍵の管理を公開鍵サーバで一元的に行うことが可能となるほか，ユーザが他のユーザ（またはそのメッセージ）を認証するための秘密情報を持たなくて済むという利点がある反面，公開鍵サーバを設けなければならないため，システムの構築にコストがかかるという欠点がある．認証や暗号化のプロトコルは，共通鍵を用いる場合となるべく近い方法を用いる．こちらの場合では，次のような方法を用いる．

**認証**　チャレンジ・レスポンス方式

$Response = Challange||UserID + $電子署名

$+$ は電子署名を付加することを意味する．

**機密性**　公開鍵暗号を用いてセッションキーを共有し，セッションキーを用いてエンドツーエンドで秘密鍵暗号による暗号化を行う．なお，$+$ は電子署名を付加することを表す．

**データの完全性**　メッセージに電子署名（メッセージのハッシュ値を秘密鍵で暗号化したもの）を付加する．

### 3.6 通信内容の暗号化

認証が成功すると，ユーザが利用する端末どうしの間でセッション鍵が配布され，通信内容はセッション鍵を用いて暗号化される．セッション鍵は協調作業に参加するすべてのユーザで同一の鍵を使用する．協調作業においては，すべてのユーザに同一の情報を送信することが多いと考えられるので，すべてのユーザで1つのセッション鍵を用いることにより，ユーザの人数分だけ暗号化を行ったり，ユーザによって鍵を使い分けたりする繁雑さを避けることができる．他のユーザが新たに作業に加わったり，途中であるユーザが作業から抜けたりする場合には，セッション鍵を更新する．新たなセッション鍵は，それまで用いていたセッション鍵を用いて暗号化されて各ユーザに渡る．途中から参加したユーザには，セッション鍵は認証で用いられた鍵で暗号化して送信される．

## 4. 関 連 技 術

本章では本研究に関連した技術について述べる．

### 4.1 JXTA

JXTA[12)]はSun Microsystemsが2001年に提唱したP2Pアプリケーションを実現するためのプロトコルである．従来のP2Pアプリケーションではアプリケーションごとにプロトコルが異なるため，互換性がなかった．そのような問題を解決するためのプラットフォームがJXTAである．JXTAアーキテクチャにはP2Pを構成するための重要な要素がいくつか存在する．

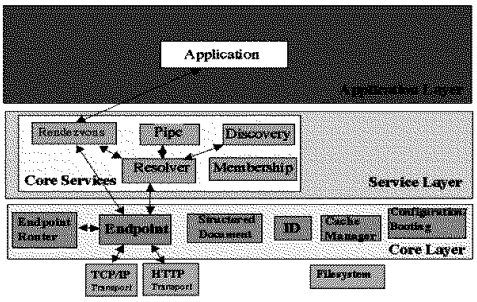


**図 1** JXTA 階層
Fig. 1 Hierarchy chart.

- 告知（Advertisement）
  JXTA では P2P の仮想空間にあるピアやピアグループ，サービスなど，利用できる資源に名前を付け，公開することで情報交換を円滑にする．ユーザはこの告知情報を検索し目的のサービスにアクセスする．
- HTTP プロトコルの使用
  JXTA では TCP/IP による通信のほかに，HTTP プロトコルによる通信をサポートしている．ファイアーウォールの内部にあるピアとの通信を可能にするためである．
- XML 形式のメッセージ
  告知によって公開される情報やピアどうしが交換しあうメッセージの形式はすべて XML である．これによりシステム形態にとらわれることなくプラットフォームに依存しないメッセージ交換を実現する．
- パイプ
  JXTA ではすべてのメッセージの交換をパイプと呼ばれる仮想的な通信路を通して行われる．ピアどうしが通信を行おうとする際，パイプを生成してから通信が始まる．
- Rendezvous Point
  JXTA では Rendezvous Point と呼ばれる，上述の告知のキャッシュを持ち，ピアがリソースを発見するのを支援するサーバ的役割を果たす特殊なピアが存在する．Rendezvous Point にはキャッシュを保持する機能だけでなく検索条件を別の Rendezvous Point に転送する機能もあわせ持つ．

#### 4.1.1 JXTA 階層

JXTA ではアーキテクチャを実現するために P2P システムを 3 つに階層化している（**図 1**）．

- JXTA Core
  ピア通信のモニタリング，パイプ（通信を行うための仮想的な通信路）管理などを行う．
- JXTA Service
  ファイルのインデックス化，共有，検索など P2P アプリケーションが直接利用できるサービスを提供する．
- JXTA Application
  JXTA Service 層の上位に位置し，Service 層が提供する機能を利用する．

上述より実装で JXTA を使用することで，本提案の目指す環境に依存しないコミュニケーションシステムのベース部分が実現可能になると考えられる．

### 4.2 Java Card

Java Card とは，Sun Microsystems の提供する，Java の実行環境を実装した IC カードであり，以下のような特徴がある．

- 異なるメーカのカード間でもアプリケーションの互換性が保たれる．
- 必要に応じてアプリケーションの追加，削除ができる．
- アプリケーションを複数搭載できる．
- 通常の Java 開発環境を利用できる．

Java Card 上で実行されるアプリケーションはアプレットと呼ばれ，プログラムとして機能するだけでなく，データを内部に格納することができる．また，内部にあるアプレットどうしは完全に独立しているためセキュリティを確保できる．

上述より，他のリムーバブル・メディアや従来の IC カードとは異なり，Java Card は汎用性が高く，高度なセキュリティを機能を持つ IC カードであるため，実装で使用するにあたって適しているといえる．

## 5. 実　　装

### 5.1 システム構成

本システムは次の 3 つの部分から構成される（**図 2** 参照）．

**ベース部分** P2P による通信を行う．

**サービス部分** 他のユーザの発見と認証，通信の暗号化を行う．

**アプリケーション部分** ユーザが協調作業を行うアプリケーション．

アプリケーション部分はサービス部分，およびベース部分とは独立して機能する．たとえばユーザが利用するアプリケーションはグループ構築の方法とは無関係に動作する．

OS に依存せずに動作するプラットフォームにするため，提案したシステムを Java 言語を用いて実装した．また，本提案で使用する P2P プロトコルとして

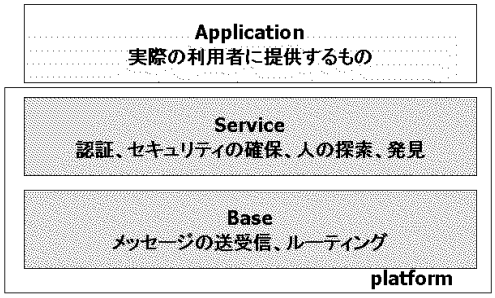


**図 2** システム構成
Fig. 2 System structure.

4.1 節で述べた JXTA [12]を採用した．本システムは 4.1.1 項における JXTA Service Layer に位置する．

また，本提案においてユーザ同士の待ち合わせ場所に使用した Rendezvous Point は JXTA によってグローバルネットワーク上で公開され，異なるグローバルアドレスを持つ 4 カ所の Rendezvous Point を使用した．

Java Card としてカードリーダには Gemplus 社の GCR401 を利用し，カードリーダにアクセスする手段として OCF（OpenCard Frameworks）を用いた．またカードは同じく Gemplus 社の Java Card である GemXpressoRad211IS を用いた．セキュリティに関しては，暗号化のアルゴリズムとして RC4 を用い，一方向性ハッシュ関数として SHA-1 を用いた．

### 5.2 カード内アプレット

JavaCard 上には Self アプレット，List アプレット，Group アプレットの 3 つのアプレットを実装した．それぞれのアプレットには以下の情報と機能を格納した．

- Self アプレット
  カードの持ち主の情報を格納する．情報としては持ち主の peerID（本システムでユーザを一意に識別するためのもの），持ち主の Rendezvous Point の IP アドレスである．
- List アプレット
  他のピアの情報を格納する．ピアの名前，peerID，Rendezvous Point の IP アドレス，ピアどうしの認証とその後の通信で使用するセッションキー生成のための秘密鍵である．また，認証と通信で使用する暗号化の機能をカード内に用意した．
- Group アプレット
  グループの情報を格納する．グループ名，GroupID，グループの Rendezvous Point の IP アドレス，認証とセッションキー生成のためのグループメンバ共通の秘密鍵である．また，認証，通信で使用する暗号化の機能を用意した．

### 5.3 JXTA サービス

JXTA を用いて協調作業を行うために，JXTA の Service Layer 上に JCGroup Service，JavaCardMembership，JCService の 3 つのサービスをそれぞれ実装した．これらは以下のようなサービスを提供する．

- JCGroup Service
  JCGroup とは本システムにおいて設定した認証成立後に協調作業を行うためのグループである．JCGroup に信頼できるピアだけが入るような仕組みを実装し，そのための基本となるサービスを実装した．以下の 2 つのサービスも JCGroupService から生成，呼び出されるものであり，本システムにおいて安全な通信を実現するための基本サービスである．
- JavaCardMembership
  認証要求を出すためのサービス
- JCService
  認証要求側のメッセージを受信し，認証を受ける側のサービス

上述のサービスを用いたグループ生成までの流れを以下に述べる．

(1) カードから情報を取得する．
カードから取得する情報は，ユーザ自身の peerID，グループの RendezvousPoint，GroupID である．読み出した情報から，システムが自動的にグループの Rendezvous Point に接続する．Rendezvous Point へのルーティングは JXTA 上の Endpoint Routing Protocol を用いて行われる．

(2) 告知（Advertisement）の生成
カードから取得した情報を元にグループ専用の告知を自動的に生成し，ネットワーク内に公開する．

(3) メンバの検索
同じグループ ID を持つ告知が公開されているかどうかを検索する．検索には JXTA 上にある Peer Discovery Protocol を使用する．告知が存在するか否かで以下の 2 通りに分かれる．
  - 告知を発見できた場合
    告知の中に含まれている親ピアの情報を読み取って，パイプを生成し親との認証を行う．
  - 告知を発見できなかった場合
    グループの告知を発見できなかった場合，他のメンバはまだ本システム上にいないと

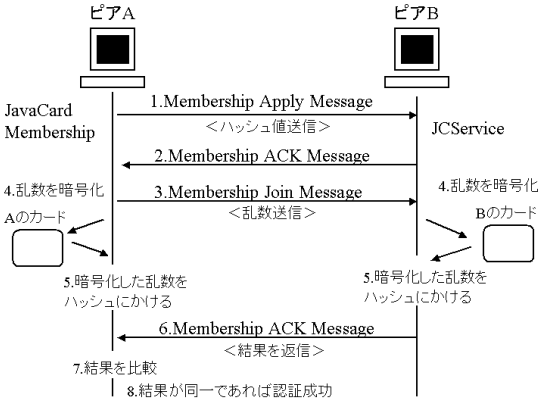


**図 3** ピア間の認証
Fig. 3 Authentication.

いうこととなり，このピアがグループの親になる．この場合，その後の認証に使用するためのパイプ情報を付加した告知を公開し，2 番目以降にネットワークに入ってきたグループのメンバに対して認証を行う．

(4) ピア間の認証
ピア間の認証は上述の JavaCardMembership と JCService を利用して以下の手順で行われる（**図 3**）．

(a) ピア A がピア B にパイプを通して XML 形式の認証要求メッセージ（MembershipApplyMessage）を送信する．このメッセージは JavaCardMembership で生成される．

(b) ピア B は認証要求メッセージを受け取るとその応答として認証許可メッセージ（MembershipACKMessage）を A に返す．

(c) ピア A がピア B に対し乱数を含んだメッセージ（MembershipJoinMessage）を送信する．ピア B は乱数を取り出し JavaCard 内で暗号化し，さらにハッシュにかけた結果をピア A に対し送信する．

(d) ピア A は同じ作業を同じ乱数を用いて行い，ピア B から送信された結果を比較する．

上述の作業を双方向で行い，両者とも認証に成功すればグループに加入できる．

(5) アプリケーション
本システムは JXTA の Service Layer 上に位置するため，JXTA 上で動作するアプリケーションはすべて使用することができる．今回の提案ではアプリケーション例としてネットオークションとチャットアプリケーションを実装した．

## 6. 評価実験および考察

### 6.1 評 価 実 験

本システムの有用性を示すために，評価実験を行った．

我々が想定している協調作業の形態（3.1 節）を満たすためには，作業をともに行うメンバがいかなる環境下の端末を利用していても確実に発見し，接続できることが最も重要である．よって 2 台の端末を用意し，

- 一方がファイアーウォール内にあり，一方がファイアーウォール外にあり，ファイアーウォール内の端末からファイアーウォール外の端末は見えるがその逆は見えない場合
- お互いが別のネットワークに存在し，両者ともファイアーウォール内にあるため直接はお互いが見えない場合

の 2 通りにおいて，一方のユーザから他方のユーザの検索を行った．

それぞれの場合において Rendezvous Point の選び方を変えて，ユーザを発見できた回数と，発見できた場合に要した時間を調べた．

Rendezvous Point への接続方法は次の 3 通りの方法を試した．

**評価 1** 2 つの端末から各々異なる Rendezvous Point に接続する．

**評価 2** 実験を行った時点において JXTA で用意されていた，それぞれ異なるグローバル IP アドレスを持つ 4 つの Rendezvous Point に順番に接続する．

**評価 3** 同一の Rendezvous Point に接続する．

また，検索には 10 分間の制限時間を設け，制限時間以内にユーザを発見できなかった場合には目的のピアを発見できなかったものとした．検索は各々10 回ずつ行った．実験結果は以下のとおりである（**表 1**，**表 2**）．

今回実施した 2 通りの評価実験で，どちらにおいても評価 3 においてのみ，つねに目的のピアを発見することができた．

### 6.2 考 察

ユーザが必ず発見できなければコミュニケーションプラットフォームとしては信頼性に欠ける．

JXTA で用意されている Rendezvous Point は，自分に接続しているピアの中に目的のものを見付けられなかった場合，他の Rendezvous Point にリクエストを出し，捜索範囲を広げる機能を持っている．よって

**表 1** ファイヤーウォール内のピアから
ファイヤーウォール外のピアを検索した場合
Table 1 Peer besides firewall is searched from the inside of firewall.

| | 発見できた回数 | 平均発見時間 |
|---|---|---|
| 評価 1 | 0 回 | — |
| 評価 2 | 6 回 | 4 分 36 秒 |
| 評価 3 | 10 回 | 32 秒 |

**表 2** ファイヤーウォール内のピアから
別のファイヤーウォール内のピアを検索した場合
Table 2 Peer inside of firewall is searched from the outside of firewall.

| | 発見できた回数 | 平均発見時間 |
|---|---|---|
| 評価 1 | 0 回 | — |
| 評価 2 | 4 回 | 4 分 58 秒 |
| 評価 3 | 10 回 | 24 秒 |

2 台の端末が異なる Rendezvous Point に接続している評価 1 の場合，10 分という制限時間を設けなければいずれ相手を見つける可能性も考えられなくはないが，本提案では P2P 上で協調作業を行うことが最終目的であるため接続時間に 10 分以上かかるのは即座に作業を開始できないため適当ではない．よって接続する Rendezvous Point が 2 台の端末間で同一である評価 2，3 方式での Rendezvous Point への接続が有効であると考えられる．

評価 3 の場合，接続する Rendezvous Point は 1 台のみと決まっているため，評価実験の結果からも 100 パーセントの確率で相手を発見できる．本提案ではこの評価 3 方式を採用しユーザ 1 人あるいはグループ 1 つにつき 1 台の Rendezvous Point を用意したため，スムーズに作業を開始することができた．

しかし，1 台の Rendezvous Point が機能しない場合もあることを考えた場合，予備の Rendezvous Point も数台準備しておくことが望ましい．これは評価 2 方式にあたる．今回の評価実験ではピア発見率が 40〜60 パーセントであり，しかも発見までにかかる時間が長かったため評価 2 方式をそのまま本提案に適用するのは得策ではない．

評価 2 方式を本提案に適用させるためには，JXTA 上でデフォルトで実装されている Rendezvous Point 間でのリクエスト転送プロトコルの上に，グループに関する Rendezvous Point のみにリクエストを転送する仕組みを作ることで発見率をあげることと，通常の告知の検索プロトコルの上に，本システムに関係のある告知情報のみを検索する機能を新たに持たせ，検索対象を減らすことで発見時間を短縮する，といった方法が考えられる．

## 7. ま と め

近年，異なる組織間のコラボレーションの増加や常時接続環境の普及にともない，どこでも利用可能で安全なコミュニケーションプラットフォームの需要が高まってきている．その一方で，任意の端末を使用することで，セキュリティの確保や，コミュニケーションに必要な情報の携帯手段が課題となっていた．

本論文では P2P 型のネットワークを用いて協調作業のためのグループを構築し，またグループ構築に必要な情報を IC カードによって携帯することによって，モバイル環境に適した安全なコミュニケーションプラットフォームを実現する方法を提案した．この提案によって，ユーザはその場にある PC 端末を利用して他のユーザを検索し，アドホックにグループを構築できるようになった．

今回実装したシステムはプロトタイプであり，また多くの課題があげられるが，本システムは次世代のコミュニケーションプラットフォームの 1 つとして発展して考えることが可能である．

**謝辞** この研究は，応用セキュリティフォーラムの支援を受けて行われた．

## 参 考 文 献

1) 小宅宏明，菅原陽子，宮地玲奈，岡田謙一：IC カードを利用したピア・ツー・ピアによるコミュニケーションプラットフォームの提案，情報処理学会研究報告 2002-GN-42，pp.13–18 (2002).
2) http://www.microsoft.com/japan/windows/netmeeting/default.htm (25, Nov. 2001).
3) http://www-6.ibm.com/jp/developerworks/java/011214/j_j-p2ptrust.html (25, Nov.2001).
4) http://www.fasttrack.nu/
5) http://www.freenetproject.org/
6) JXTA Search: Distributed Search for Distributed Networks, Sun Microsystems, Inc. (2001).
7) 山崎重一郎，岩尾忠重，塩内正利，和田祐二，岡田 誠，荒木啓次郎：P2P 型エージェントプラットフォームにおける信用ドメインの構築について，マルチメディア，分散，協調とモバイル 2001, pp.681–686 (2001).
8) 小柳恵一，星合隆成，梅田英和：P2P ネットワーキング技術の提案と紹介，電子情報通信学会論文誌，Vol.J85-B, No.3, pp.319–332 (2002).
9) 川原圭博，松本延孝，森川博之，青山友紀：ピアツーピアネットワーク型仮想環境における更新情報共有手法，信学総大，B-7-54 (Mar. 2002).

10) 松本延孝，川原圭博，森川博之，青山友紀：ピアツーピアネットワーク型仮想環境のためのピア発見機構，信学総大，B-7-51 (Mar. 2002).
11) Parameswaran, M., Susarla, A. and Whinston, A.B.: P2P Networking: An Information-Sharing Alternative, *IEEE Computing Practistics*, pp.31–38 (July 2001).
12) http://www.jxta.org/ (25, Nov. 2001).
13) Gong, L. and Sun Microsystems Inc.: JXTA: A Network Programming Environment, *IEEE Internet Computing*, pp.88–95 (May 2001).
14) Waterhouse, S., Doolin, D.M., Kan, G. and Faybishenko, Y.: Distributed Search in P2P Networks, *IEEE Internet Computing*, pp.68–72 (Jan. 2002).
15) http://www.java.sun.com/products/javacard/index.html (25, Nov. 2001).
16) 佐々木良一，吉浦 裕，手塚 悟，三島久典：インターネット時代の情報セキュリティ，共立出版株式会社

(平成 14 年 11 月 29 日受付)
(平成 15 年 6 月 3 日採録)

**小宅 宏明**（学生会員）

2001 年慶應義塾大学理工学部情報工学科卒業．2003 年同大学大学院理工学研究科開放環境科学専攻修了．グループウェアの研究に従事．

**宮地 玲奈**（学生会員）

2002 年慶應義塾大学理工学部情報工学科卒業．現在，同大学大学院理工学研究科開放環境科学専攻情報通信メディア工学専修修士課程に在学中．グループウェアの研究に従事．

**菅原 陽子**（学生会員）

2002 年慶應義塾大学大学院理工学研究科開放環境科学専攻修了．グループウェアの研究に従事．

**岡田 謙一**（正会員）

慶應義塾大学理工学部情報工学科教授，工学博士．専門は，グループウェア，コンピュータ・ヒューマン・インタラクション．「コラボレーションとコミュニケーション」（共立出版）をはじめ著書多数．GN 研究会運営委員，MBL 研究会運営委員，日本 VR 学会仮想都市研究会幹事．情報処理学会論文誌編集主査，電子情報通信学会論文誌編集委員．ECSCW2001 プログラム委員，INTERACT2001 財務委員長．IEEE，ACM，電子情報通信学会，人工知能学会会員．1995 年度情報処理学会論文賞，情報処理学会 40 周年記念論文賞，2000 年度情報処理学会論文賞受賞．