

アドホックネットワークにおけるユーザ認証と コンテンツ提供サービス実現の一検討

小口正人，中塚賀子[†]，富沢千帆[‡]

お茶の水女子大学 理学部情報科学科

A Study of User Authentication and a Content Distribution on an Ad-hoc Network

Masato Oguchi, Yoshiko Nakatsuka[†], and Chiho Tomizawa[‡]

Department of Information Sciences, Ochanomizu University

1 はじめに

携帯端末が普及し性能が向上するに従い，モバイル環境においてユーザに対し大容量のデータや情報の配信を行うコンテンツ提供サービスが望まれるようになってきた．このようなサービス実現に際し，ネットワークとして携帯電話網を用いるだけでは帯域やコストの面で十分と言えず，ホットスポットにおける広帯域無線 LAN 接続がこれを補うものとして期待されている．しかし固定的なホットスポットの場合には，エリアを面でカバーすることが難しい．そこで特定のアクセスポイントに依存せず，ユーザ同士が広帯域無線 LAN により P2P（ピア・ツー・ピア）で直接接続しデータのやり取りを行うアドホックネットワークの活用が考えられる．P2P は既存の計算機資源を有効に活用する手法として，今後の発展が期待されている [1]．

モバイル環境のアドホックネットワークは，各ノードが移動先で近隣のノードと一時的なネットワークを構成する形態であり，一般にサーバ等の管理システムは存在しない．そのためインフラネットワークに接続する場合と比較して，ユーザが利用することのできるサービスは限定される．しかしアドホックネットワークは携帯電話網等に比べ広帯域の通信を行うことが可能であるため，このネットワークを介し，ユーザ同士が直接データのやり取りを行う仕組みを，コンテンツ提供サービスの枠組みに取り入れることは，有効であると考えられる．アドホックネットワークをコンテンツ提供サービスに利用する場合，まずユーザ認証の仕組みが必要となる．すなわちインフラネットワークに接続されていない状態において，各ユーザがどのサービスをどの程度利用出来るか判断するための基本的な枠組みを用意しなければならない．不正なユーザや機器からシステムを保護するためにも，認証処理が不可欠である．

そこで本研究では，アドホックネットワークにおいて，コンテンツ提供サービスの実現に際し基本となるユーザ認証の枠組みを提案した．これはユーザ認証に段階を付け，段階ごとに認証グループを設けることにより，ユーザの信頼度に応じてレベ

ルの異なる処理が行える枠組みを提供するものである．またアドホックネットワークにおける高機能なクライアントを利用したコンテンツ提供サービスの実現手法を検討した．提案モデルの実装を汎用 P2P プラットフォームである JXTA を利用して行い，提案手法の動作を確認することができた．

2 アドホックネットワークにおけるユーザ認証機構の提案と実装

2.1 階層構造を持つユーザ認証機構

アドホックネットワークにおいては，各端末が常時インフラネットワークに接続できる状況ではないため，ユーザ認証を行った際にも特定のサーバに接続しての認証処理を期待できない．従ってアドホックネットワークにおいては，通常のネットワーク接続の場合にサーバのデータベースに照会するような，完全に信頼できるユーザ認証の実現は難しい．しかしアドホックネットワークにおいても，すべてのユーザを等しく「未認証」の扱いとするのではなく，各々の状況においてユーザの信頼度が異なっている方が一般的である．例えば同じアドホックネットワーク上の他のユーザに接する場合には，全く見知らぬ人と近くに居る友人とでは異なる対応を行える環境の方が望ましい．またユーザに対するサービス提供という視点から見た場合にも，例えばサービスを受ける権利を持ったユーザと持たないユーザについて，アドホックネットワーク上における対応が異なる形で実現されると有益である．

そこで本研究では，アドホックネットワークにおけるユーザ認証機構に，階層構造を導入することを提案する．これはアドホックネットワーク上に，ユーザの認証レベルに基づくグループを設け，認証レベルが上がるごとに上のグループへと所属が上がるというモデルである．すなわちある認証グループの中に一段高いレベルの認証グループが存在し，その中にはさらに高いレベルの認証グループが存在するといった階層構造を構成するものである．提案モデルの概念図を図 1 に示す．

アドホックネットワークは多くの場合開かれたネットワーク

[†]現在，日本ユニシス（株）

Currently with Nihon Unisys, Ltd.

[‡]現在，日本電気（株）

Currently with NEC Corporation

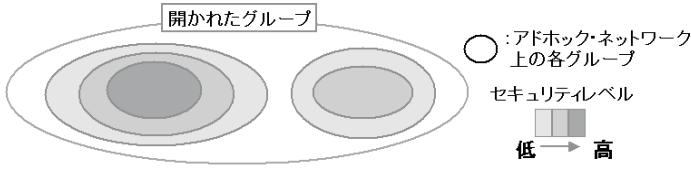


図 1: 階層構造を持つ認証グループ

であり、ユーザはネットワークに対し自由に参加及び離脱を行う。ユーザが最初にネットワークへ参加した段階においては、認証の全く行われていない開かれたグループへ所属する。このグループの中では限定されたサービスしか利用することが出来ない。その後、何らかの処理や手続きを経て、そのネットワークにおけるユーザの信頼度が上がったら、認証レベル（セキュリティレベル）が高いグループへと所属が移り、利用できるサービスの範囲も広がる。

アドホックネットワーク上でどのような処理を行いユーザの認証レベルを変化させるかという手法の検討は本論文の対象外とするが、例えばユーザが何らかの ID 情報を所持していたら認証レベルを高くする、或いはノードがインフラネットワークに接続しサーバにおける認証が行われたらその時点で認証レベルを高くするなどの例が考えられる。認証されたレベルはユーザがそのアドホックネットワーク内に所属している間のみ有効なものであり、それぞれのグループにおいて所属するメンバにどのような資格やサービスを提供するか定義することができる。

2.2 JXTA

提案手法を実装して実験を行うために、JXTA を用いた [2][3]。JXTA は言語独立でプラットフォーム非依存な P2P フレームワークであり、米国サン・マイクロシステムズ社により提供されている。JXTA は P2P アプリケーションを構築するための一連のプロトコル群からなる。プロトコル群には PDP (Peer Discovery Protocol)、PRP (Peer Resolve Protocol)、PIP (Peer Information Protocol) などが定義されている。これらのプロトコルを用いて JXTA のリソースを探査したり、クエリのフォーマットを規定したり、互いの情報をやり取りする仕組みが実現可能であり、P2P アプリケーションを動作させるための基本機能が提供されている。

プログラマは、JXTA を利用することにより P2P の細かい仕様を意識せずに P2P アプリケーションの構築を行うことができる。P2P ソリューションの基本処理単位となる、P2P ネットワーク上のノードはピアと呼ばれる。すべてのピアがすべてのプロトコルを実装する必要はなく、各ピアが実装するプロトコルの種類はピアの能力に利用目的に応じて選択が可能である。ピアは互いに独立で非同期的な動きをするが、いくつかのピアが自発的に共通の関心に基づいてグループを形成することができ、これはピアグループと呼ばれる。ピアもしくはピアグループはサービスを提供することができる。

2.3 JXTA のメンバシップサービス

JXTA はメッセージ等の記述に XML を用いた言語中立なフレームワークであるが、プログラミング言語 Java で開発さ

れた JXTA の参照実装である JXTA Java バインディングを利用することができる。JXTA Java バインディングにおいては、JXTA が規定するプロトコルに従い、基本的なサービスが定義され、またその実装が提供されている。定義された Java インタフェースはパッケージ net.jxta に含まれ、インターフェースの実装クラスはパッケージ net.jxta.impl に含まれている。

JXTA Java バインディングでは、ピアグループへのピアの参加を制御するメンバシップサービスが提供されている。ピアグループにどのピアを参加させるかは、メンバシップポリシーとして規定される。メンバシップサービスの参照実装としては、認証を行わずピアの要求に応じて身元を割り当てるだけの NullMembershipService と、ログイン ID 及び暗号化パスワードに基づいて簡単な認証を行う PasswdMembershipService が提供されている。しかしこの MembershipService 実装は認証機構としては不十分であり、実用的な認証を行うためには MembershipService の実装を定義し、認証アカウント情報の作成と検証を行う必要がある。そこで本研究では、PasswdMembershipService 実装を反映した階層的な認証機構を持つピアグループの作成を行った。

2.4 提案した認証機構の実装

JXTA を用いて、提案した階層構造を持つ認証機構をアドホックネットワーク上で実装した。実験環境としては、図 2 で示すように Linux2.4 を OS として用いたノート PC2 台に JXTA version1.0 をインストールし、これらを IEEE802.11b 無線 LAN で接続したアドホックネットワーク環境を用いた。

ピアグループを作成するためには、ピアグループアドバタイズメントが必要である。アドバタイズメントとは、ピアやピアグループといった JXTA ネットワークリソースを XML ドキュメントを使って表現したものであり、ピアグループアドバタイズメントにはピアグループの名前や ID、説明、仕様などが記述されている。全てのピアは、Net Peer Group と呼ばれるピアグループに所属しており、この Net Peer Group を元にしてグループを作成する。

本研究では、次のメソッドを定義した。

CreateGroup()

Net Peer Group のモジュール仕様の実装に関する情報を提供するモジュール実装アドバタイズメントをコピーし、新しいピアグループのアドバタイズメントを作成、パブリッシュする。パブリッシュされたピアグループアドバタイズメントをもとにピアグループを生成する。

CreatePeerGroup()

セキュアなピアグループの生成には、標準の NullMembershipService の代わりに、PasswdMembershipService を使用



図 2: 実験環境

```

JXTA>groups -r .....①
group discovery message sent
JXTA>groups .....②
group0: name = OrangePeerGroup
group1: name = PubTest
group2: name = Ocha
group3: name = SatellaGroup
JXTA>join -d group0 .....③
Stopping rdv
Enter the identity you want to use when joining this peergroup (nobody)
1Identity : yoshiko
JXTA>join .....④
Joined Group : worldgroup
Joined Group : netgroup
Joined Group : OrangePeerGroup (current)
JXTA>groups -r .....⑤
group discovery message sent
JXTA>groups .....⑥
group0: name = BluePeerGroup
JXTA>join -d group0 .....⑦
Stopping rdv
Enter the identity you want to use when joining this peergroup (nobody)
2Identity : SecurePeerGroups
2_Password : RULE
JXTA>join .....⑧
Joined Group : worldgroup
Joined Group : netgroup
Joined Group : BluePeerGroup (current)
Joined Group : OrangePeerGroup
JXTA>

```

図 3: JXTA Shell による認証グループへのジョイン

する。まず、`PasswdMembershipService`を反映したモジュール実装アドバタイズメントを作成し、パブリッシュする。次に、ピアグループアドバタイズメントの中に、新しく作成したメンバシップサービスの実装を反映するモジュール実装アドバタイズメント、ピアグループ名、ログイン名、パスワードを設定し、ログイン名とパスワードを用いて認証を実装している新しいピアグループを生成する。

階層的なピアグループの作成では、はじめに `CreateGroup()` メソッドを呼び出し、誰でも参加自由なグループ（これを `OrangePeerGroup` とする）を生成する。次に、`CreatePeerGroup()` メソッドを呼び出し、先ほど生成した `OrangePeerGroup` を親ピアグループとして用いることにより、ピアグループの中にセキュアなピアグループである `BluePeerGroup` を生成する。さらに、この `BluePeerGroup` を親ピアグループとしてセキュアな `GreenPeerGroup` を生成するというように、階層的な認証機能を持つピアグループの生成を実現した。他のピアは、JXTA アプリケーションである JXTA Shell を使って、作成したピアグループにジョインすることが可能である。この実行を図 3 に示す。

JXTA Shell を立ち上げて、`groups -r` コマンドでピアグループ発見要求メッセージを送り [①]、`groups` コマンドを実行するとグループのリストが表示される [②]。発見されたピアグループの中で `OrangePeerGroup` というピアグループにジョインするため、`join -d group0` というコマンドを打つ [③]。`OrangePeerGroup` はオープンなピアグループであるため、グループ内で使用したい ID を入力するだけでピアグループに参加でき、`join` コマンドで参加出来ていることが確認出来る [④]。次に先程と同じように `groups -r`、`groups` コマンドで `OrangePeerGroup` 内に存在するピアグループを発見し [⑤][⑥]、`join -d group0` コマンドを実行する [⑦]。参加しようとしている `BluePeerGroup` は認証を必要とするセキュアなピアグループであるため、設定したログインとパスワードが必要で正しい入力が行われた時のみ、ピアグループへの参加が可能となった。以上により、提案した階層構造を持つセキュアなピアグループの作成が確認出来た。

3 P2P 接続を利用したコンテンツ提供サービス

3.1 高機能クライアントの利用

前節で提案したユーザ認証機能が基盤の仕組みとして存在するものとし、P2P 環境におけるコンテンツ提供サービスの実現を検討した。モバイルネットワーク環境においては、クライアント端末にはブラウザなどの表示機能のみを持たせ、ネットワーク上のサーバで主要な処理を実行する形式が一般的である。しかしクライアントとして、大量のデータを蓄積したり処理したりできる能力のある端末が利用可能となってきている。例えばオンライン時にデータをダウンロードしキャッシュしておけば、オフライン時にもユーザがコンテンツを利用することが可能となる。さらには P2P 接続を用い、クライアント間でコンテンツの再配布を行うことにより、モバイルネットワーク環境におけるサービスの利用範囲が拡大する。本研究では、アドホックネットワークにおいてそのように高機能なクライアントモデルを利用したコンテンツ提供サービスの実現を提案する。概念図を図 4 に示す。

クライアントにおいてはコンテンツプロバイダとの直接接続だけでなく、他クライアントとの P2P 接続によるアドホックネットワークの広帯域通信を利用した効率的なコンテンツ配信が期待できる。また、クライアントが独自に生成したコンテンツを端末間で提供しあうことも可能になる。アドホックネットワークにおけるコンテンツの複製配置の研究も行われている [4][5]。本研究では、上図におけるアドホックネットワーク環境を構築し、その上で P2P 接続によるクライアント・サーバ型コンテンツ配信を実装した。

3.2 JXTA におけるパイプサービス

JXTA の基本プロトコルの 1 つに PBP (Pipe Binding Protocol) が存在し、このプロトコルをベースに実現されたサービスがパイプサービスである。パイプとはエンドポイント間の接続を抽象的に定義したもので、1 つの送信側エンドポイントから 1 つまたは複数の受信側エンドポイント間に接続を確立することができる。パイプの種類には、1 つのパイプと結ぶユニキャストパイプ、複数のパイプをバインドするプロパゲートパイプがあり、パイプアドバタイズメントを作成する際に指定する。本

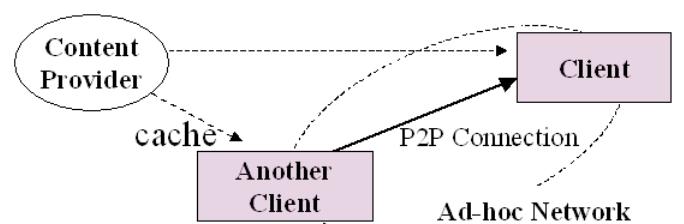


図 4: アドホックネットワークにおけるコンテンツ提供サービス

研究ではこのパイプサービスを利用し、アドホックネットワーク上におけるコンテンツ提供サービスのメカニズムを実現した。

3.3 コンテンツ提供サービスの実装

まず前述の環境において、JXTA のコアサービスを利用し、ピアが特定のピアにメッセージを送信するプログラムを作成した。このプログラムでは、サーバ側がサービスを提供するための新しいグループを作成してリモートにパブリッシュし、クライアント側がそれを発見する。クライアント側は、発見したサービスアドバタイズメントからサーバ側が作成したパイプの情報を抽出し、それを基に自身のパイプを作成して接続する。メッセージは共通のメッセージタグを通して配達される。送信側はメッセージをタグに String としてセットし、受信側はそこから抽出して受け取り表示する。これにより JXTA 環境において通信路を確立できた。このプログラムを用いることにより、サーバが所持する提供可能なコンテンツリストをクライアント側に提示でき、クライアント側はそれに基づき欲しいコンテンツを要求することが可能となる。

次にこのプログラムを、テキストデータのみでなくコンテンツデータも配信できるように拡張した。本研究ではコンテンツを画像や音声、実行可能形式プログラムなどのバイナリデータと定義する。バイナリファイルは文字コードの範囲などを考慮せずに構成されているため、メッセージの様に String としては扱えない。そのため、サーバ側はファイルのデータを一定のサイズごとに byte 型の配列としてタグにセットして送信し、これをファイルの終わりまで繰り返す。クライアント側は同様に byte 型の配列としてタグから抽出し、ファイルへ書き出す。

コンテンツ配信の際の実行結果を以下に示す。プログラムを実行すると、まずサーバとクライアント両方にそれぞれユーザインターフェースが表示される。サーバ側 [図 5] には "Send Message" "Send Content" "Quit" の三つのボタンを、クライアント側 [図 6] には "Send Message" "Quit" の二つのボタンを用意した。ユーザインターフェース上の枠にメッセージを入力し "Send Message" ボタンを押すと、相手のユーザインターフェース上にそのメッセージが表示される。サーバはクライアントからコンテンツの要求が来た場合、"Send Content" ボタンを押し、標準入力でファイル名を指定する。クライアントは要求以外の動作を何もせず、自動的にファイルをローカルディスクに受け取れる。図の例では、サーバが持っている実行可能ファイル "Server.class" を送っており、クライアント側は確かにそれを受け取り実行することに成功した。

4 まとめ

モバイル環境において、近隣の端末と一時的にネットワークを構築するアドホックネットワークは、大容量のコンテンツなどを扱うシステムやサービスの基盤として期待されている。そのようなシステムやサービスを実現するためには、ユーザ認証が不可欠であるため、本研究ではアドホックネットワークに適した階層構造を持つユーザ認証の枠組みを提案し、P2P フレームワークである JXTA を用いてその実装を行った。またアドホックネットワークにおいて、高機能なクライアントを利用してコンテンツ提供サービスのコンテンツ再配信を行うモデルを検討

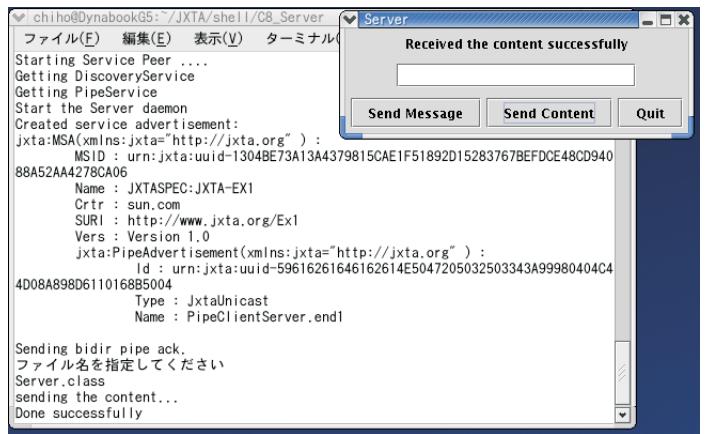


図 5: 実行結果（サーバ側）

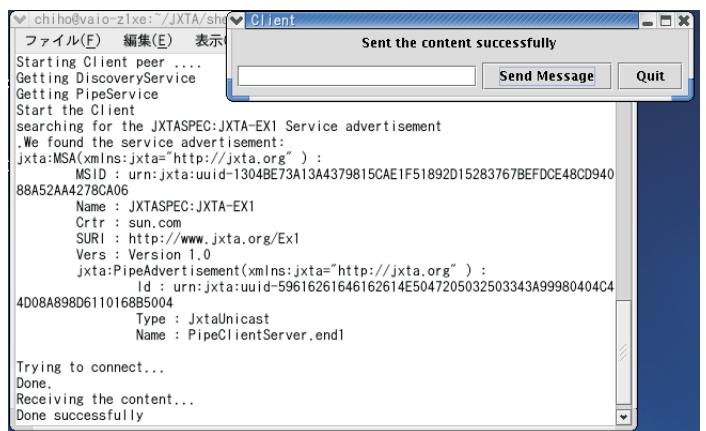


図 6: 実行結果（クライアント側）

し、JXTA を用いて実装した。今後の課題としては、アドホックネットワークにおいて、ユーザの認証を具体的にどのように行い認証レベルをどのような場合に変化させるか等の問題を検討ていきたい。

参考文献

- [1] Alfred W. Loo , "The Future of Peer-to-Peer Computing" Communications of the ACM , Vol.46 , No.9 , pp.56-61 , September 2003 .
- [2] Project JXTA , <http://www.jxta.org/>
- [3] Brendon J. Wilson , JXTA のすべて , 日経 BP 社 .
- [4] 原隆浩 , "アドホックネットワークにおけるデータ利用性向上のための複製配置" 電子情報通信学会論文誌 B , Vol.J84-B , No.3 , pp.632-642 , 2001 年 3 月 .
- [5] 沖野智幸他 , "無線アドホックネットワークにおける位置依存情報複製配布方式の評価" 情報処理学会研究報告 , Vol.24 , No.21 , pp.187-194 , 2004 年 3 月 .