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

2004－MBL－28　(26)
2004／3／5

エニキャストを用いた位置依存グループウェアの実装

朝長　康介[†]　　太田　昌孝[‡]
†九州大学大学院システム情報科学府　‡東京工業大学情報理工学研究科

あらまし　インターネットに接続された移動体端末の増加にともない、端末の位置に応じてデータ配信を行う位置依存サービスが有意義となった。しかし、端末の位置情報は提出者のプライバシ情報であるため、この公開は本人の承諾なしに行われてはならない。ところで、本稿では、エニキャストを用いた位置依存サービスとしてグループウェアの実装を行った。これは、利用者が互いの位置情報や個人情報を公開し合い、これにより連絡を取り合うというアプリケーションである。この実装にあたり、プライバシ情報の公開を利用者ごとで行う設計を採用し、実装に対する考察を行った。考察の結果、お互いのプライバシ情報を適切に公開する実装であることが示される。

Implementing Location-dependent Groupware Application Using Anycast

Kosuke Tomonaga[†]　　Masataka Ohta[‡]
†Graduate School of Information Science and Electrical Engineering, Kyushu University
‡Graduate School of Information Science and Engineering, Tokyo Institute of Technology

Abstract This paper describes implementation details of a groupware application that provides group communication service based on users' purpose and location. This groupware application works with location-dependent services using anycast. In this implementation, we especially focus on mechanisms for anonymity of users, because it is very dangerous if this groupware application reveals private information like users' location.

1. はじめに

インターネットに接続された移動体端末の増加にともない、サーバ側で端末の位置情報を取得し、その位置に応じたデータ配信を行うことが有意義となった。これを本稿では位置依存サービスと呼ぶ。この位置依存サービスを用いれば、自分の位置が分からない利用者に周辺案内を提供することや、利用者の関心を惹く情報を地域限定して公開することが可能となる。また、利用者がお互いの位置情報と連絡先を知らせ合うことで、近くの者と連絡を取り合うことが可能になる。これは、例えば旅行先で近くにいる者とネットワーク経由で情報を交換することや、スポーツ観戦で近くにいる者と情報交換をしつつ、場合によっては集うことを可能にする。

インターネットにおいてはPDAやノートパソコンなどの移動体端末が普及し、また802.11bなど無線LAN への接続を提供するプロバイダも増加した。位置依存サービスとしてはWEBを用いたサービスが既に行われている。

WEBを用いた位置依存サービスの方式としては、筆者らが提案したエニキャストを用いた位置依存サービス[1]がある。この方式では、同一のIPアドレスを持つ複数の位置情報サーバを無線基地局ごとに配置し、その電波が届く範囲にある端末は、その同一のアドレスにより最寄りのサーバから位置情報を受信する。この同一のアドレスはエニキャストアドレスと呼ばれ、本稿では、同一のアドレスをもつサーバをエニキャストサーバと呼ぶ。一般にインターネットにおける無線基地局の電波到達距離は数十メートルから数百メートルと短い。このため、この方式における移動体端末は、たかだか数十から数百メートル離れた地点の位置情報を得ることができる。また、位置情報とともにその提出先サーバのアドレスが配信されていれば、端末は位

置情報に基づくサービスを要求することが可能となる。この配信方法としては、例えばURLに位置情報とその提出先WEBサーバのホストポートを埋め込み、これをHTTP応答で返す方式がある。この方式には、位置情報の提出方法に標準が不要であるという利点がある。この理由は、エニキャストサーバにおけるURLへの埋め込み方法がWEBサーバごとに設定可能だからである。

また、別の方式としては、端末が独自にGPSで位置情報を取得し、これをHTTPでWEBサーバに提出する方式がある。この方式では、位置情報の提出方法に標準が必要であるが、現状はアプリケーションごとに異なっており統一されていない[2][3]。

ところで、位置依存サービスには、移動体端末の位置情報が本人の承諾なしに公開されない仕組みが必要である。これは端末の位置情報が本人に関わるプライバシ情報だからである。上記の両方式は端末が位置情報をWEB サーバに提出しないことが可能であり、この仕組みを備えている。また、位置依存サービスによっては連絡先などがプライバシ情報にあたり、これについても同じく公開を防ぐことが可能な仕組みが必要である。例えば、連絡先を公開する位置依存サービスでは、サービス専用の連絡先を用意し、利用者が日常的に用いる連絡先の公開は利用者ごとの判断に委ねられる必要がある。

本研究では、エニキャストを用いた位置依存サービスの応用として、目的と位置情報に基づくコミュニケーショングループウェア[4]を実装した。このグループウェアを本稿では[縁]と名付ける。このグループウェアは、利用者間の出会いを提供するアプリケーションである。日本の茶道では一期一会という言葉もあり、「出会い」は近年汚されているごとく淫靡な目的に限られた概念ではない。[縁]を用いれば、先に挙げた旅行やスポーツ観戦の例が実現可能となる。これを実現する動作としては、個人情報と位置情報を提出した利用者にたいして、付近で同じ目的を持つ利用者の個人情報を提供する。個人情報としては現在の目的情報や他の利用者に呼びかけるコメント、連絡先などがある。連絡手段は専用のメールアドレスと電話番号を用意し、利用者はこれを用いて匿名性を維持しつつ連絡を取り合うことが可能である。このため、日常的な連絡先を公開する必要はない。また、目的情報はグループウェア側で選択肢を

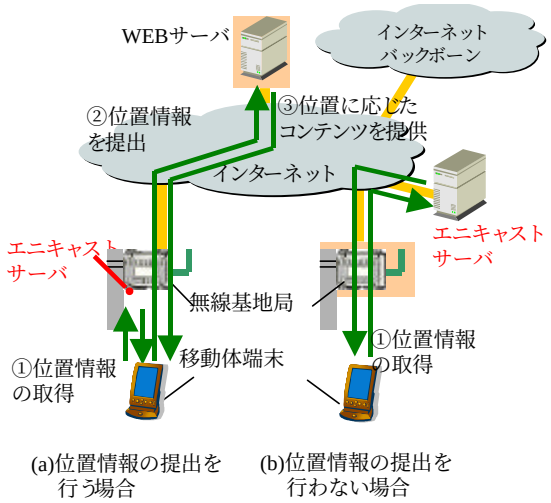


図１エニキャストを用いた位置依存サービス

提供することで、これに属さない目的での利用を困難にしている。さらに、アカウント管理と認証の徹底により、不正な目的の利用者にはグループウェアの使用を禁止する。

2. エニキャストを用いた位置依存サービス

エニキャストは、インターネット各地に同一のIPアドレスをもつサーバを複数配置し、この同一のIPアドレスにおいて、クライアントがネットワーク的に最寄りのサーバへパケットを送信する通信方式である。この同一のアドレスはエニキャストアドレスと呼ばれ、本稿ではこのアドレスを持つサーバをエニキャストサーバと呼ぶ。エニキャストにおける問題としては、インターネットバックボーンのルータが持つ経路表エントリが、エニキャストアドレス１つごとに1個消費されることが挙げられる。そのため、野放図にエニキャストを用いれば、バックボーンにおける経路表爆発が引き起こされる。

エニキャストを用いた位置依存サービスは、無線基地局上あるいはその周辺にエニキャストサーバを設置し、このサーバにおいて無線基地局の位置情報をHTTP で配信する方式である。一般に無線基地局の電波は数十メートルから数百メートル届くため、この範囲にいる移動体端末はたかだか数十から数百メートル離れた地点の位置情報を得ることができる。この際、バックボーンにおける経路表爆発問題は、エニキャストのルーティングを無線基地局の周辺で行うために起きない。この動作を、図1に示す。

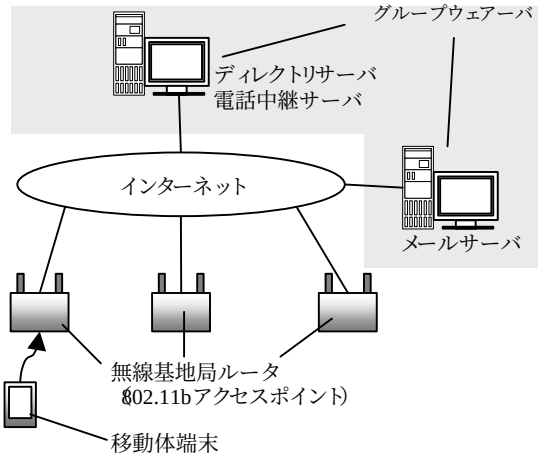


図 2 グループウェアの構成

位置情報の配信に際しては、エニキャストサーバが位置情報の提出先となるWEBサーバのURLに位置情報を埋め込み、このURLへのリダイレクト応答を用いる。移動体端末はエニキャストアドレスにHTTP 要求を送信することで、最寄りのエニキャストサーバからリダイレクトを促すHTTP 応答を受信する。そして、応答に含まれるWEBサーバのURLを検証し、この応答に従うならばURLが示すWEB サーバに位置情報を提出する。これは位置情報が埋め込まれたURLをGETするHTTP要求で行われる。このHTTP 要求を受信したWEBサーバは、要求されたURLの位置情報などに応じてコンテンツを返す。

3. 目的と位置情報に基づくコミュニケーショングループウェア

本稿ではエニキャストを用いた位置依存サービスの応用として、グループウェア[縁]を実装し、この詳細について述べる。このグループウェアは利用者間の出会いを提供するアプリケーションであり、この名前は袖振り合うも他生の縁という諺に由来する。

「出会い」という概念は、日本の茶道では一期一会という言葉もあり、近年汚されているごとく淫靡な目的に限られたものではない。旅先で近くにいる者とネットワーク越しに情報交換することや、道を教え合うことは、袖振り合うも他生の縁という諺もあるように古来より行われてきたことである。一方、現在は少子高齢化対策として、自治体が電子的な出会いの場を提供しようという動きもある。したがって、出会いを支えるグループウェアは社会的に有意義であると言える。

ところが、出会いによっては犯罪に巻き込まれたり嫌がらせを受けたりする恐れもある。そのため、出会う前に相手を十分に知り、慎重に考えた後に出会うことが重要となる。また、集団で会うことや、人気のない所で会わないことも重要である。これを支援する仕組みとしては、事前に連絡を取り合えるよう匿名の通信手段を提供することや、サービス提供エリアを制限することなどが考えられる。このような仕組みは出会いを提供するグループウェアに備えられるべきものである。

本章では、エニキャストを用いた位置依存サービスに即した形で、位置と目的情報に基づくコミュニケーショングループウェアの設計を紹介するとともに、実装の詳細について述べる。

3.1 グループウェアの構成

今回開発したグループウェア[縁]を構成するサーバを図 2 に示す。また、説明のために移動体端末、無線基地局ルータも同図に示す。

3.2 グループウェアの管理

アカウント管理

グループウェア[縁]では、個人情報を個別に管理するためのアカウントを発行する。これを用いれば、悪質な利用者に印しを付けることや利用を停止させることが可能である。

本稿の実装では、サーバごとのアカウントを統一的に管理するため、メールアカウントの形式に即したアカウントを発行する。つまり、アカウント名はメールアドレスに一致させ、パスワードは APOP で用いるものに一致させる。現段階においては、パスワードファイルは統一されておらず、アカウントの設定はサーバごとに手作業で行う。また、電話中継サーバに関するアカウント管理は後述する。

エリア管理

グループウェア[縁]においては、近い端末間で互いの個人情報を公開し合うための近さに定義が必要となる。本稿のグループウェアでは平面地図上で、二点を結ぶ直線を対角線とする矩形をエリアとして定義し、同じエリアにいる者同士を近いと定義する。

エリアを定義する二地点の地理的座標は、相対的あるいは絶対的に定義される。つまり、相対的な場合は、中心となる利用者を定めてその位置をエリアの中心とする。一方、絶対的な場合は、ある地理的座標をエリアの中心とする。

3.3 グループウェアの操作

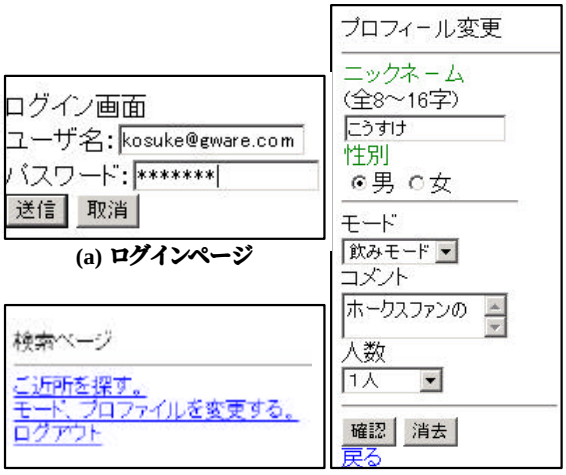
グループウェア[縁]に対する利用者からの操作は、ディレクトリサーバに対してのみ行う。これは、インターフェースを統一するためである。ディレクトリサーバの実体は WEB サーバの CGI で起動されるアプリケーションである。これは Perl で記述され、操作画面を WEB ページの形で提供する。この操作は、利用者が移動体端末上の WEB ブラウザから行う。操作としてはログイン、個人情報の設定、検索、表示がある。また電話中継サーバの設定もある。各操作は HTTP 要求の URL に埋め込まれた操作命令に基づき実行される。以降、各操作の詳細について記述する。

ログイン

ディレクトリサーバは、命令を与えない、もしくは認証に失敗した端末に対してログインページを提供する。このページを図 3(a)に示す。このページに関わる通信は、アカウント情報の傍受を阻止するため、SSL を用いて行われる。このページにおいて、利用者は事前に発行されたそれぞれのアカウントを用いてログインを試みる。ディレクトリサーバは、ログインの認証に失敗した利用者に対しては操作を認めずに再度ログインを促す。一方、成功した者に対しては個人情報の入力ページを提供する。

時限パスワードによる認証

アカウント情報の確認は操作ごとに行う必要がある。しかし、同じ情報を重複して入力するのは操作上好ましくないと考え、アカウント情報の入力を一定時間にわたり省く時限パスワードを用いる。時限パスワードは、アカウントのパスワードと発行時間をハッシュ化したものであり、これは発行時のアカウント名や発行時間とともに用いられる。本稿では、時限パスワード、発行時間、アカウント名をまとめて時限パスワードによる認証情報あるいは単に認証情報と呼ぶ。時限パスワードによる認証情報は、ログインに成功した以降のページに埋め込まれる。この方法については各操作の詳細で述べるが、ページごとに提出される情報とともにディレクトリサーバに提出されるよう工夫されている。



(a) ログインページ

(c)検索ページ

(b)個人情報の設定ページ

図 3 グループウェアの画面(1)

表 1. 個人情報

項目	例
ニックネーム	こうすけ
性別	男
目的	スポーツ観戦
コメント	ホークスファンで語り合いましょう。
人数	3 人
公開用メールアドレス	tomonaga@groupware.com

ディレクトリサーバは各ページの操作を実行する前に、まず認証を行う。そのため、ディレクトリサーバのパスワードファイルからアカウント名に対応するパスワードを取り出し、提出された情報から発行時と同じ手順で時限パスワードを生成する。生成された時限パスワードが提出されたものと同じものであれば認証成功であり、異なっていれば失敗となる。成功した端末に対しては提出された情報から操作を実行し、失敗した端末には再度ログイン画面を返す。この一連の認証を、本稿では時限パスワードによる認証と呼ぶ。

個人情報の設定

ログイン認証に成功した端末に対して、ディレクトリサーバは個人情報の設定ページを返す。このページを図 3(b)に示す。また、個人情報の設定命令を含む URL の要求に対しては、時限パスワードによる認証を行い、成功すれ設定ページを返す。設定命令を含む URL は、次に示す命

令とパラメータからなる。

- ディレクトリサーバのホストポート部
- 個人情報の設定命令 (command=change-profile)
- 時限パスワードによる認証情報
- 個人情報

URL の例を次に一部示す。

http://www.example.com:80/groupware.pl?command=change-profile&of=kosuke@gware.com&password=9fb994f97b6baa2c23a1f90f8cfcb320&time=1076111271&nickname=...

設定ページにはフォームによる入力欄があり、その<INPUT>タグに hidden 属性として時限パスワード情報が埋め込まれる。そのため、利用者がフォームに個人情報を入力して送信を行えば、ともに認証情報も送られる。

ディレクトリサーバは、まず時限パスワードによる認証を行う。認証に成功すれば、個人情報を検査し、空白の項目がなければ個人情報ファイルに格納して検索画面を返す。個人情報ファイルのエントリは各行に 1 つであり、アカウント名と個人情報からなる。ここでのアカウント名は、後にエントリの読み取りに利用される。また、アカウント名が公開されることはない。

もし個人情報に空白の項目があれば、再び個人情報の入力ページを返す。個人情報は表 1 にまとめた項目からなる。表中の項目は全て公開情報であり、各項目は次の意味を持つ。

- ニックネームは各利用者の呼び名である。
- 性別は男女の 2 値でどちらかである。
- 目的はグループウェアが用意した選択肢から 1 つを選択する。
- コメントは、テキストで 60 文字以内である。
- 人数は、グループの人数である。
- 公開用メールアドレスについては後述する。

目的の記入を制限した理由は、グループウェアの運用者が望まない利用を入力させないためである。

個人情報の検索

個人情報の設定が成功した後、ディレクトリサーバは検索ページを送信する。このページを図 3(c)に示す。この実装は、他人の個人情報を検索する際は、まず自らの個人情報を提出すべきだという考えに基づく。

検索ページは検索実行ページへのリンクを含む。このリンクの<A>タグには、次に示す検索実行の命令とそのパラメータが埋め込まれている。

- エニキャストサーバのホストポート部
- 検索実行命令(command=find)
- 時限パスワードによる認証情報

この URL の例を次に一部示す。

http://anycast.example.com/groupware.pl?command=find&of=kosuke@gware.com&&time=...

この URL のホストポート部はエニキャストアドレスのドメイン名である。

位置情報の提出

移動体端末上の WEB ブラウザは、検索実行リンクを処理することで位置情報の提出を開始する。まず、検索実行リンクが含む URL のホストポート部に基づき、エニキャストサーバと TCP コネクション確立を試みる。このコネクションは IP 層のルーティングにより最寄りのエニキャストサーバと確立され、WEB ブラウザの HTTP 要求は最寄りのエニキャストサーバに送信される。これを受信したエニキャストサーバは、要求された URL のホストポート部をディレクトリサーバのもので書き替え、さらに無線局の位置情報を'&'文字で繋げて新たなに URL を生成する。そうした後、この URL へのリダイレクトを促す HTTP 応答が生成され、この応答が WEB ブラウザに返される。この URL の例を次に示す。

http://www.example.com/groupware.pl?command=search&of=kosuke@gware.com&...&?el=139/44/49.493&nl=35/41/58.683...

WEB ブラウザが応答に従えば、検索実行リンクの URL に含まれていた情報に加え、位置情報がディレクトリサーバに送信される。ただしホストポート部はエニキャストサーバのものではなく、ディレクトリサーバのものである。

検索の実行

ディレクトリサーバは、次に示す命令とパラメータからなる URL を受信し、認証に成功すれば検索の実行を試みる。

- ディレクトリサーバのホストポート部
- 検索実行命令
- 時限パスワードによる認証情報
- 位置情報

この URL は、エニキャストサーバから返されたものと同じである。

検索の実行に際して、ディレクトリサーバは提出された位置情報の登録を行う。これは目的情報ごとに分けられた位置情報ファイルに対し

て行われる。このファイルのエントリは各行ごとに 1 つであり、位置情報を提出した利用者のアカウント名、提出時間、位置情報からなる。また、エントリは登録ごとに追記される。

次に、ディレクトリサーバは、目的情報に応じた位置情報ファイルを特定し、このファイルから一定時間分の位置情報エントリを取り出す。このため、アカウント名を時限パスワードによる認証情報から抜き出し、これを用いて個人情報ファイルを引くことで目的情報を先に得る。

さらに、位置情報エントリから検索者に近い利用者を見つけるため、エントリとエリア定義の照合を行う。これは、まず、検索者がいるエリアを提出された位置情報から確定し、このエリアに含まれる位置情報を持つエントリを確定する。次に、確定されたエントリからアカウント名のリストが作成され、このアカウントの個人情報が WEB ブラウザに返される。このページを図 4(a)に示す。このとき、個人情報のコメントは個人情報の表示ページへのリンクとなっており、その<A>タグの href 属性には、個人情報の表示命令とパラメータが含まれた URL が埋め込まれる。この命令とパラメータは次の項目からなる。

- ディレクトリサーバのホストポート部
- 個人情報の表示命令(command=show)
- 時限パスワードによる認証情報
- 公開用メールアドレス(target)

この URL の例を次に示す。

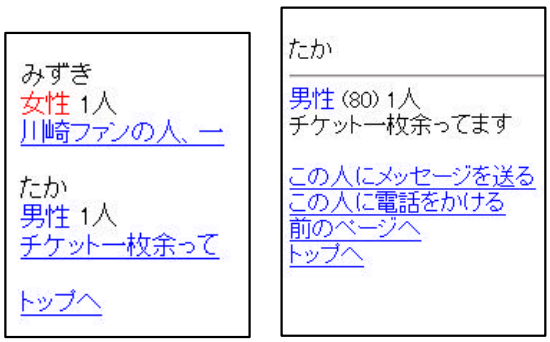
http://www.example.com/groupware.pl?command=show&target=tomonaga@gware.com&of=kosuke@gware.com&time=1076113078&password...

個人情報の表示

個人情報の表示命令とパラメータを受信したディレクトリサーバは、時限パスワードの認証を行い、成功すれば個人情報の表示する。このページを図 4(b)に示す。表示に際しては、提出されたパラメータのうち公開用メールアドレスから個人情報を特定する。この個人情報の表示ページでは電話の設定操作のリンクを含むが、これはについては後述する。

3.4 端末間通信の実現

プライバシ情報を公開せずとも連絡が取り合えるよう、メールサーバや電話中継サーバをグループウェアとして用いる。これにより、日常的に用いるメールアドレスや電話番号の公開は各利用者が決定可能となる。



(a)検索結果ページ　(b)個人情報の表示ページ

図 4　グループウェアの画面(2)

メールによる通信

公開用メールアドレスは変更を繰り返せることが重要である。なぜなら、この変更により他の利用者に対する匿名性が維持されるからである。しかし一方で、メールアドレスと利用者の対応は、管理する必要がある。これは、メールアドレスを不正に利用した者に対して使用を停止するためである。

メールアドレスの変更は、メールアカウントの変更あるいはそのエイリアスの変更で可能である。前者の変更は、パスワードや配送先など、その他の情報までも再設定が必要だという欠点がある。また、メールアカウントと利用者の対応付けに、別の管理が必要になるという欠点がある。これに対して後者の変更では、それだけで連絡先メールアドレスを変更できる利点がある。よって、本稿の実装では運用者がエイリアスを各アカウントに設定し、このエイリアスを連絡先メールアドレスとして各利用者に割り当てる。

電話による通信

インターネットにおける電話プロトコルは各種あり、本稿では NOTASIP(Nothing Other than A Simple Internet Phone)を用いて電話中継サーバを実装した。

NOTASIP では UDP を用いた音声データストリームで端末間の呼を確立する。まず、発呼側端末はプライベートポート P0 から、受呼側端末のウェルノウンポート P1 に音声を送信する。呼び出しを受けた受呼側端末では、予め用意してある呼出音を鳴らし、さらにプライベートポート P2 か発呼側端末のポート P0 に対して呼出音を送信する。これに対して、発呼側端末は、

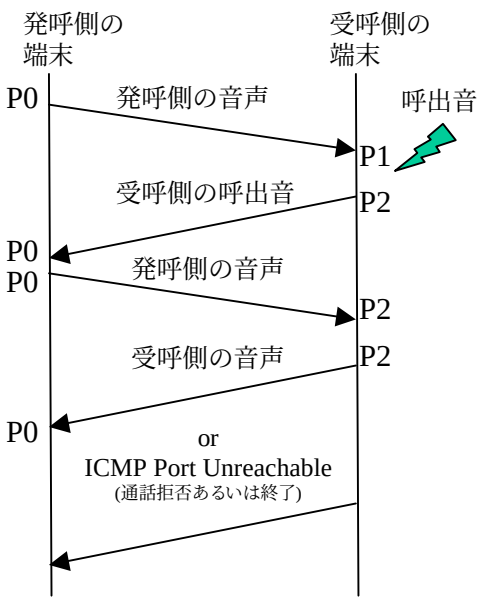


図 5 NOTASIP 端末間のパケットフロー

ポート P0 からの音声データストリームを受呼側端末のポート P2 へ切替える。もし、受呼側端末が受話器をとれば呼出音が音声へと代わり通話が成立し、また、どちらかの端末がポート P1 か P0 を閉じれば通話は拒否あるいは終了される。このとき、音声を送信し続けている相手には ICMP Port Unreachable が返される。 以上の動作を図 5 に示す。このようなプロトコルにおける電話番号は、IP アドレスもしくはドメイン名、UDP ポート、音声データ形式の組で表される。

NOTASIP で IP アドレスの公開を防ぐには、通話する端末間に電話中継サーバを設置し、これで UDP パケットを転送する方式をとる。この方式では、利用者間で公開し合う IP アドレスとウェルノウンポートは電話中継サーバのものを用いる。また、パケットの送受信のため、電話中継サーバは各利用者の連絡先 URL を保持する。

本稿の実装では、各利用者の連絡先は電話中継サーバのアカウント情報として管理する。これは、サーバを不正利用した者に対して運用者が使用を停止させるためである。このため、運用者は、利用者の連絡先 URL を電話番号ファイルに登録する。このファイルのエントリは各行ごとに 1 つであり、アカウント名と連絡先 URL を組にしたものである。

メールアドレスと同じく匿名性を維持するため、連絡先 URL のポート番号は変更可能である必要がある。この要求を満たすにあたってはポート番号の割り当てを単純化するため、通話ごとに動的に割り当てる方式を採用した。

電話中継サーバは、次のパラメータをとる UDP パケット転送サーバである。

- 転送元の IP アドレスとポート番号
- 転送先の IP アドレスとポート番号

このパラメータはプロセスの起動時に、次のように与えられる。

```
$ udpf 192.168.0.10 9999 192.168.0.20 10000
```

また、電話中継サーバの転送時のパケットフローについて図 6 に示す。

電話中継サーバの設定は、ディレクトリサーバの操作として行われる。これは個人情報の表示ページにある電話中継の設定ページへのリンクを用いることで可能である。このリンクの URL は、次の命令とパラメータを含む。

- ディレクトリサーバのホストポート部
- 電話中継の設定命令(command=call)
- 時限パスワードによる認証情報
- 公開用メールアドレス(target)

この URL の例を次に一部示す。

```
http://www.example.com/groupware.pl?command=call&target=tomonaga@gware.com&of=kosuke@gware.com&time=1076113078&password=...&time=...
```

この URL で HTTP 要求を受信したディレクトリサーバは、時限パスワードによる認証を行い、成功すれば電話中継サーバに与えるパラメータを特定する。転送先の IP アドレスは、公開メールアドレスから特定したアカウント名から電話番号ファイルを引いて特定する。このとき得られるのは連絡先 URL であるが、これから IP アドレスとポートと通信方式を特定する。転送元の IP アドレスは、認証情報のアカウント名を用いて転送先 IP アドレスと同様に連絡先 URL から特定する。また、ポート番号はローカルポートからランダムに選択する。全てのパラメータを特定した後、ディレクトリサーバは電話中継サーバのプロセスをパラメータとともに起動し、WEB ブラウザに連絡先 URL を表示するページを返す。この URL は、電話中継サーバの IP アドレス、送信元のポート番号、通信方式からなる。利用者は、この連絡先を NOTASIP 電話に

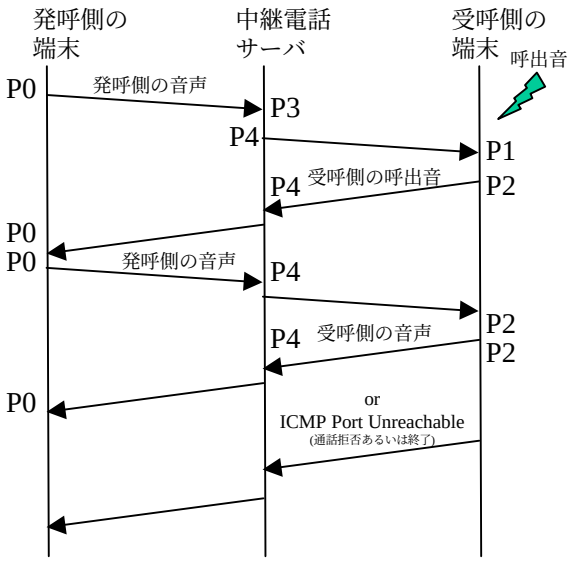


図 5 NOTASIP 端末間のパケットフロー

直に入力することで番号非通知の電話をかけることが可能である。

4. 考察

利用者の位置情報は、本人特定の有力な情報となり得る。そのため、利用者数が少ない場所では位置情報の提出を行わないなどの仕組みが必要となる。本稿の実装では、エニキャストを用いた位置依存サービスをもとにこれを実現した。利用者はエニキャストサーバからのリダイレクトに従わないことで、位置情報の提出を阻止できる。また、本稿では実装していないが、ディレクトリサーバ側で端末の位置に応じて注意を促したり、サービスの提供を停止したりすることが可能である。

また、利用者間が連絡を取り合うグループウェアにおける問題の一つは、望まない利用者との連絡が絶てないことである。本稿の実装では、グループウェア専用の変更可能な連絡先を提供することで、この問題を解決している。しかし、この専用の手段において日常的な手段を公開することも可能であるため、これを慎重に行うことが利用者に求められる。この匿名による連絡を用いれば、事前に相手をよく確認することが可能となる。

また、運用者が望まない利用により犯罪などの問題が起こる懸念もある。今回の実装では目的情報の選択肢をグループウェア側で提供し、さらにアカウントの個別管理とそれに基づく認証機構を提供している。これにより、不正にグループウェアを使用した者を利用停止にすることが可能である。また、メールサーバや電話中継サーバなどの不正利用は、その事実をサーバ側で記録することも容易に可能である。

5. まとめ

本研究では、エニキャストを用いた位置依存サービスの応用として、目的と位置情報に基づくコミュニケーショングループウェア[縁]を実装し、この安全性について検討した。このグループウェアは利用者間の出会いを提供するアプリケーションであり、近くにいる利用者の個人情報や連絡先などを提供する。提供に際しては、目的情報を運用側が提供し、適切なアカウント管理と認証機構において不正な利用を停止することが可能である。また、位置情報の公開は移動体端末が行うため、利用者の承諾なしに公開されることはない。さらに、連絡手段についても変更可能なものを専用に提供するため、望まない相手との連絡を絶つことが容易に可能である

文　献

[1]朝長康介,“エニキャストを用いた位置依存サービス”,情報処理学会研究会報告,
2001-MBL-20,March, 2001

[2] インクリメント・ピー株式会社,“iMapFan link 技術概要”,
http://www.mapfan.com/imflink/gaiyou.htm

[3]Joshua Schachter, ”Geo URL ICBM Address Server”,
http://geoURL.org/

[4]朝長康介,太田昌孝,“位置と目的情報に基づくコミュニケーショングループウェアの設計”,
2003-MBL-25,July, 2003