エニキャストを用いた位置依存グループウェアの設計と実装

朝長, 康介
九州大学大学院システム情報科学府情報工学専攻 : 博士後期課程

太田, 昌孝
東京工業大学情報理工研究科

荒木, 啓二郎
九州大学大学院システム情報科学研究院情報工学部門

https://doi.org/10.15017/1516214

出版情報：九州大学大学院システム情報科学紀要. 10 (2), pp.103-108, 2005-09-26. 九州大学大学院システム情報科学研究院
バージョン：
権利関係：

九州大学大学院
システム情報科学紀要
第10巻　第2号　平成17年9月

Research Reports on Information Science and
Electrical Engineering of Kyushu University
Vol.10, No.2, September 2005

エニキャストを用いた位置依存グループウェアの設計と実装

朝長康介*・太田昌孝**・荒木啓二郎***

Design and Implementation of Location-dependent Groupware Application Using Anycast

Kosuke TOMONAGA, Masataka OHTA and Keijiro ARAKI

(Received June 13, 2005)

Abstract: This paper describes design and 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.

Keywords: Location-dependent service, Social software, Anycast, Routing, Internet

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，移動体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サーバ側で行うことが有意義となった．このようなサービスを本稿では位置依存サービスと呼ぶ．位置依存サービスを用いることで，迷子の利用者に周辺情報を提供することや，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，お互いの位置情報と連絡先を知らせ合うことで，近くの者が互いに連絡を取り合うサービスが可能となる．例えば，これは旅先やスポーツ観戦での情報交換に有用である．

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．しかし，無線LAN向けの位置依存サービスは未だ存在しない．

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[2]は，無線LANを含めた低電力無線技術向けのWebサービスである．エニキャスト・アドレスと呼ばれる同一のIPアドレスを持つ無線LAN基地局を位置依存サービス・エリアに配置し，各基地局ではセル特有のコンテンツを配信する．そうすることにより，無線LAN端末では，セル間の移動に関係なく同一のエニキャスト・アドレスを用いることで，接続する基地局特有のコンテンツの受信が可能となる．

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．なぜなら，端末の位置情報は本人に関わるプライバシ情報だからである．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適切に行う仕組みが必要である．

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］を設計，実装した．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，先に挙げた旅行やスポーツ観戦での情報交換を匿名で実現する．具体的には利用者の目的情報や位置情報などの公開個人情報がディレクトリ・サービスにおいて提供され，別の利用者は付近で同じ目的を持つ利用者についての公開個人情報の閲覧が行える．また，公開個人情報に含まれる連絡先情報を用いれば，互いに匿名性を維持しつつメールやIP電話の通信も行える．

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[2]は，インターネット各所に同一のIPアドレスを付されたサーバを複数配置し，この同一のIPアドレス宛のパケットを，クライアントからネットワーク的に最寄りのサーバに配信する経路制御方式である．ここで，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有する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・バックボーンに接続されるルータの経路表エントリが，エニキャスト・アドレス1つごとに1つ消費されることがある．そのため，野放図にエニキャストを用いれば，バックボーンにおいて経路表爆発が生じる．

エニキャストを用いた位置依存サービス[1]では，無線

平成17年6月13日受付
＊　情報工学専攻博士後期課程
＊＊　東京工業大学情報理工研究科
＊＊＊情報工学部門

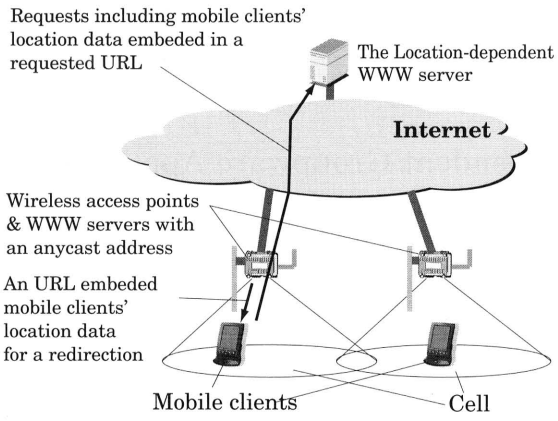


Fig. 1 Location-dependent Service Using Anycast.

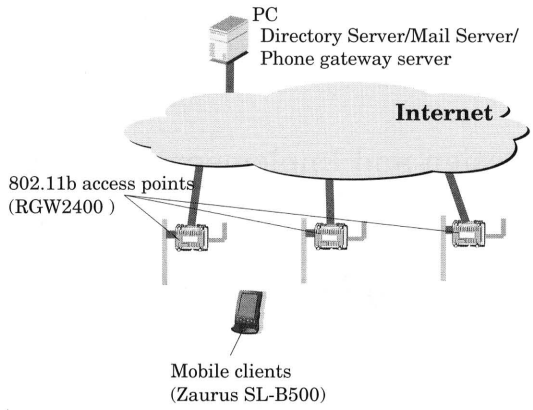


Fig. 2 Network Configuration of EN.

LAN 基地局上にエニキャスト・サーバを搭載し，無線 LAN 基地局特有の位置依存コンテンツを基地局ごとに HTTP [3] で配信可能な方式である．動作原理を **Fig. 1** を用いて説明する．一般に，無線 LAN 基地局の電波は数十メートルから数百メートルまで到達するため，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基地局からセル特有のコンテンツを取得することが可能となる．この際，バックボーンにおける経路表爆発は，エニキャストのための経路制御が無線 LAN 基地局周辺のみで行われるために生じない．ここで，位置依存コンテンツとしては，位置情報の提出先となる WEB サーバの URL に，無線 LAN 基地局の位置情報が埋め込まれたものがリダイレクトを促す HTTP 応答で配信される．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，最寄りの基地局上にあるエニキャスト・サーバからリダイレクト応答を受信する．もし，移動体端末がリダイレクト応答に従うならば，位置情報が URL に示される WEB サーバに提出され，WEB サーバ上に集約された位置依存コンテンツが返される．また，応答に従わない場合には，WEB サーバに位置情報が提出されることはなく，移動体端末のプライバシ情報は漏洩しない．

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［縁］

本章では，エニキャストを用いた位置依存サービスを応用したグループウェア［縁］の設計，実装を紹介する．

［縁］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，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古来より行われてきたことである．しかし，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こともあった．そのため，出会う前に相手を十分に知り，慎重に考えた後に素性を明かすことが重要である．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．これらの自衛策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．

3.1 グループウェアの構成

［縁］のネットワーク構成を**Fig. 2**に示す．グループウェア・サーバは，ディレクトリ・サーバ，電話中継サーバ，メール・サーバからなり，それぞれインターネットに接続される．今回の実装では，ディレクトリ・サーバと電話中継サーバを開発し，メール・サーバは sendmail [4] を利用した．ここで，ディレクトリ・サーバは Web サーバの CGI アプリケーションであり，Perl で開発された．また，電話中継サーバは UDP パケット転送デーモンであり，C 言語で開発された．**Fig. 2** では全てのグループウェア・サーバが一台の PC 上にインストールされ，インターネットに接続されている．一方，移動体端末は，無線 LAN 基地局を介してインターネットに接続され，WEB ブラウジングが行えるものである．実装では PDA の Zaurus SLB-500[5] を用いたが，グループウェアのために特別に開発したソフトウェアはなかった．また，無線 LAN 基地局には 802.11b のアクセスを提供する RGW2400[7] を用いたが，エニキャスト・サーバは文献１）で開発したものを利用した．

3.2 グループウェアの管理

3.2.1 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，利用者に対して一意になるよう発行する．よって，悪質な利用者に印を付け，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・アカウントを統一的アカウントとして発行する．つまり，アカウントは

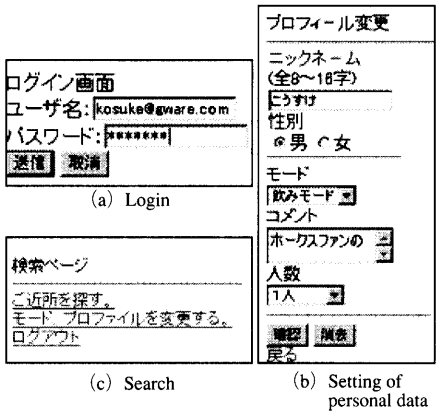


Fig. 3 Interface of EN(1).

メール・アドレスに一致し，パスワードはAPOPで用いるものに一致する．

3.2.2 エリア管理

最寄りの端末間で互いの個人情報を公開し合うためには近さの定義が必要となる．本稿では，平面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

利用者からの操作は全てディレクトリ・サーバに対して行うよう設計されている．これは，インターフェースが複数のサーバに散在する煩わしさを感じさせないためである．他のサーバに対しては，ディレクトリ・サーバが起動ないしは設定変更を行う．具体的な操作については，ディレクトリ・サーバ上のWEBページを，移動体端末のWEBブラウザで取得して行う．操作の種類としてはログイン，個人情報の設定，検索，表示，電話中継サーバの設定がある．各操作はURLに埋め込まれ，HTTP要求としてディレクトリ・サーバに送信される．以降，各操作の詳細について記述する．

3.3.1 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・ページを配信する．ログイン・ページを**Fig. 3**(a) に示す．ログインに関わる通信には，アカウント情報の第三者による傍受を阻止するためにSSLが用いられる．さて，ログイン・ページにおいて，利用者は事前に発行された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他の操作を認めず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設定ページを提供する．

3.3.2 時限パスワードによる認証

WEBを用いるため，アカウント情報の確認は個別の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工夫として時限パスワードを用いた．時限パスワードとは，アカウントのパスワードと発行時間とをハッシュ化したものである．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．詳細については各操作の説明において述べられる．

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・サーバにはパスワード・ファイルが置かれる．パスワード・ファイルはメール・アカウントとパスワードからなるエントリが利用者ごとに一行ずつ納められたものである．認証を行うディレクトリ・サーバは，まず利用者から時限パスワード，アカウント名，発行時間を受信する．次に提出されたアカウント名に対応するパスワードをパスワード・ファイルから取り出し，提出されたアカウント名，発行時間とともに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であれば認証成功であり，異なっていれば認証失敗となる．成功した端末に対しては提出された操作命令を実行した結果画面を，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．

3.3.3 個人情報の設定と個人情報ファイル

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．この例を**Fig. 3**(b) に示す．個人情報の設定ページには，次のような設定命令とパラメータを含むURLが含まれる．

- 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
- 公開個人情報

URLの例を次に示す．

http://www.example.com:80/groupware.pl?
command=change-prof ile&of=kosuke@gware.
com&password=9f b994f 97b6baa2c23a1f 90f8c
fcb320&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すれば，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．

Table 1 An example of personal data.

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	ソフトバンク・ホークスについて語りましょう
人数	3人
公開用メール・アドレス	tomonaga@groupware.com

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，後に個人情報ファイルの検索鍵となる．また，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が返される．さて，個人情報は**Table 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．
- 目的は用意された選択肢の1つである．
- 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．

目的の選択肢はグループウェア・サーバの管理者が用意する．これにより，グループウェアの運用者が望まない利用目的が制限される．

3.3.4 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返す．検索ページの例を**Fig.3**（c）に示す．ここで，検索前に必ず個人情報の設定が必要となるのは，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設計が基づくからである．検索ページは検索実行ページへのリンクを含み，リンクのAタグには次に示すような検索実行命令と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

検索実行命令が埋め込まれたURLの例を次に示す．

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

ここで，ホストポート部はエニキャスト・アドレスに対応するドメイン名であり，リンクへの要求はまず無線LAN基地局上のエニキャスト・サーバへと提出される．

3.3.5 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・サーバとのTCPコネクションの確立が試みられる．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・サーバとの間に確立され，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・サーバのものに書き替え，さらに無線LAN基地局の位置情報を‘&’文字で繋げた新たなURLを生成する．その後，生成したURLにリダイレクトを促すHTTP応答が生成され，WEBブラウザに返される．生成された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に含まれていた命令などの情報とともに，位置情報がディレクトリ・サーバに送信される．

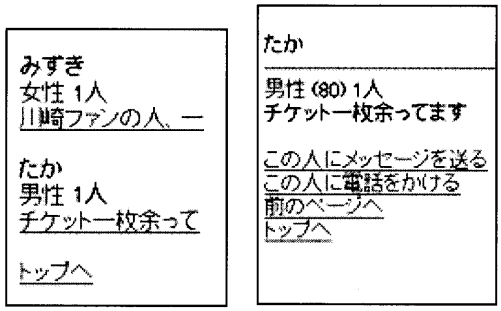
3.3.6 検索の実行と位置情報ファイル

ディレクトリ・サーバは，検索命令とパラメータを含む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

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を位置情報ファイルへと登録する．位置情報ファイルは目的情報ごとに個別に用意され，位置情報ファイルのエントリは各行で1つである．エントリは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，検索実行命令とともに提出された時限パスワードによる認証情報からアカウント名を抜き出し，個人情報ファイルを引くことで目的情報を得る．さらに目的情報から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エントリを取り出す．ここでの一定時間とは過去5分間，10分間などといったグループウェアの既定値であり，運用者が更新スピードに応じて起動時に定めることが可能である．短いほど検索条件は厳しくなるが，検索結果に古い情報が含まれなくなる．さて，位置情報ファイルから抜き出したエントリから検索者に近い利用者を見つけるため，ディレクトリ・サーバは，取り出したエントリに含まれる位置情報とエリアの照合を行う．照合は，まず，提出された位置情報から検索者がいるエリアを定め，検索者と同一エリアにいる利用者のエントリを定めることで行われる．照合の結果，得られたエントリからはアカウント名のリストが作成され，アカウント名ごとに個人情報ファイルが引かれつつ検索結果がWEBブラウザに返される．このページを**Fig. 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



(a) Example of search result　(b) Example of interface for a personal data

Fig. 4 Interface of EN (2).

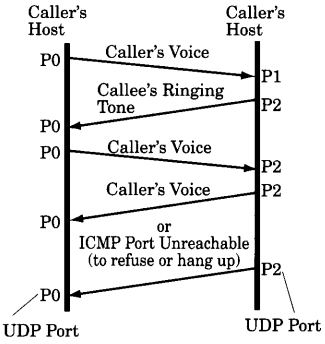


Fig. 5 Packet flow of NOTASIP.

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．表示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）

表示命令が埋め込まれた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=107611 3078&password…

3.3.7 公開個人情報の表示

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，成功すれば公開個人情報を表示する．個人情報の表示ページを**Fig. 4** (a) 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ファイルのエントリを特定する．なお，個人情報の表示ページにおいては電話の設定操作のリンクが含まれる．

3.4 匿名通信の実現

プライバシ情報を公開せずとも連絡が取り合えるよう，グループウェア専用のメール・サーバや電話中継サーバを匿名通信に用いる．これにより，日常的に用いるメール・アドレスや電話番号とは別に，利用者はグループウェア用の連絡先を持つことが可能となる．

3.4.1 メールによる匿名通信

公開用メール・アドレスは変更の容易さが重要である．なぜなら，メール・アドレス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・アドレスと利用者と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エイリアスの変更で可能である．前者は，パスワードやメール配送先ディレクトリまでも再設定する必要がある．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．これに対し，後者は，連絡先メール・アドレスのみの変更が行える利点がある．よって，本稿の実装では運用者がエイリアスをアカウントごとに設定し，エイリアスを匿名通信用メール・アドレスとして各利用者に割り当てる．

3.4.2 電話による匿名通信

インターネット電話の通信プロトコルのうち，本稿ではNOTASIP (Nothing Other than A Simple Internet Phone) [8] を用いた．NOTASIPのパケット・フローを**Fig. 5**に示す．呼はUDPを用いた音声データ・ストリームを用いて確立される．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，発呼側端末はポートP0からの音声送信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，音声送信を中止しない相手にはICMP Port Unreachableが返され続ける．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，UDPパケットを転送すれば良い．

本節の設計では，利用者のエイリアス・アカウントを用いて通話先を指定する．これは，もしサーバの不正利用が発覚した場合は，利用停止を可能とするためである．実装としては，まずサーバの管理者が，利用者端末のIP電話番号を電話番号ファイルに登録する．ここで，IP電話番号はIPアドレス，ウェルノウン・ポート番号の組であり，電話番号ファイルの各エントリはアカウントとIP電話番号を組にしたものである．メール・アドレスと同様の匿名性を維持するため，IP電話番号のポート番号は通話ごとに動的に割り当てられる．さて，電話中継サーバは，発呼側，

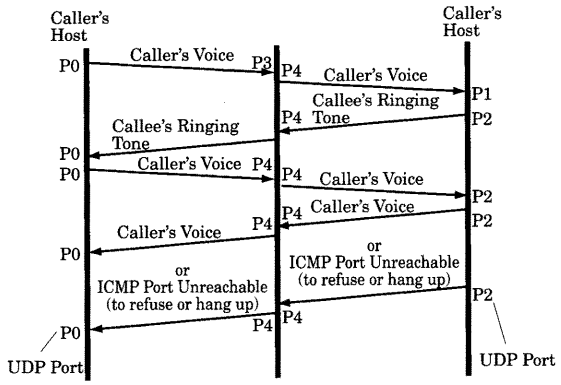


Fig. 6　Packet flow of NOTASIP with EN.

受呼側端末のIPアドレスとポート番号をパラメータとして取るUDPパケット転送サーバである．起動時のパラメータは次のように与えられ，転送時のパケット・フローは**Fig.6**のようになる．

$ udpf 192.168.0.10 9999 192.168.0.20 10000

電話中継サーバの起動は，利用者から起動命令を受け付けたディレクトリ・サーバが行う．起動命令には次のパラメータを含むURLが用いられる．

- ディレクトリサーバのホストポート部
- 電話中継サーバの起動命令（command = call）
- 時限パスワードによる認証情報
- 通話相手のエイリアス・アカウント（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=107611
3078&password=…&time=…

起動命令を含むHTTP要求を受信することにより，ディレクトリ・サーバは通話相手のアカウント名から電話番号ファイルを引くことによりIP電話番号を得る．また，通話を開始する利用者向けに電話中継サーバのIP電話番号をWEBページとして返信する．ここでも時限パスワードによる認証は行われ，認証失敗の場合は起動も行われず，認証失敗を意味するWEBページが返信される．

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の機能を用いて，位置情報の提出を利用者が決定する方式を実現した．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，ディレクトリ・サーバ側では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，利用者が連絡を取り合うグループウェアにおいては，望まない利用者との連絡が絶てないことが問題となる．そこで，本稿の実装では，匿名通信手段を提供することで問題を解決した．しかし，匿名通信で日常的な連絡先を公開することも可能であるため，連絡先の公開には慎重さが求められる．

また，グループウェアの管理者が望んでいない利用により，犯罪や事件などが発生する懸念もある．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，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］を設計，実装した．これ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公開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．

参 考 文 献

1) Tomonaga, K., Ohta, M., and Araki, K., Privacy-aware Location Dependent Services over Wireless Internet with Anycast, Proc. of HSI2005, pp.311-321, LNCS2713 (2005).
2) Partridge, C., Mendez, T., and Milliken, W.: Host Anycasting Service. RFC1546 (1993).
3) Fielding, R., Getty, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and Berners-Lee, T.: Hypertext transfer Protocol-HTTP/1.1. RFC2616 (1999).
4) The Sendmail Consortium.: http://www.sendmail.org/.
5) Sharp Corporation.: http://www.sharp.co.jp/ products/slb500/.
6) IEEE.: Wireless LAN Medium Access Control (MAC) and Physical Layer(PHY) Specifica-tions: High-Speed Physical Layer Extention in the 2.4 GHz Band. IEEE802.11b (1999).
7) ROOT INC.:http://www.root-hq.com/e/ products/RGW2400.html.
8) Ohta, M., Fujikawa, K., Kitagawa, T., Sola, M., and Satoh, K., The Simple Internet Phone, Proc. of INET2000, http://www.isoc.org/inet2000/cdproceedings/4a/4a_3.htm, July 2000.