2003－MBL－25 (9)
2003／7／4

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

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

近年、携帯端末や無線機器の性能が向上したことにより、無線でインターネットに接続された携帯端末間で電話を行うことが可能となった。一方、インターネット接続端末向けの位置依存サービスも実現されており、これを用いることで携帯端末の位置情報に適したサービス提供が可能である。本論文では携帯インターネット電話端末の位置情報を活用し、近くにいる同じ目的を持つ者同士がコミュニケーションを行うためのグループウェアを設計した。このグループウェアの特徴は匿名でメール、電話、WEB掲示板を用いたコミュニケーションを行える点にある。これにより、グループウェアの利用者はコミュニケーションを行いつつ、そのプライバシを保護することが可能である。

Designing Groupware for Communication based on Location and Purpose

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

In this paper, we describe the designing of groupware which provide group communication service based on members' purposes and locations. The groupware users submit their location and porpose data to their groupware server, by using thier internet mobile phone. On the other hand, the groupware server executes matching operations of users' data, and forms users into groups so that the members in a group have a same purpose and staying in close to each other. The server also provides some methods such as anonymous BBS (Bulletin Board System), anonymous mail and anonymous internet phone service for communication within every group. The users will take advantage of this group to establish close relationship with other users, based on their location and purpose. In this designing, we especially focus on mechanisms for anonymity of users, because it is very dangerous if personal addresess or private infomation is revealed by using this groupware.

1 はじめに

近年、携帯端末や無線機器の性能向上に伴い、無線でインターネットに接続された携帯端末間で音声通信を行なうことが可能になった。そのような端末でインターネット電話プロトコルを用いれば、携帯端末によるインターネット電話の実現も可能である。

一方、携帯端末が持つ移動性という特徴を活かしたアプリケーションも出現している。携帯電話向けのアプリケーションであるナビゲッティ [1] は、飲み仲間や話し相手の募集など同一の目的を持つ利用者のうち、約 2.5 キロメートル以内にいる者と電子掲示板によるコミュニケーションを行うためのグループウェアである。このようなグループウェアを用いれば、同じ目的を有する近くの利用者に店舗や道などについて尋ねることが可能になる。袖振り合うも他生の縁という諺があるように、人は日常生活においても多くの人との出会い経験している。そうした出会いにおいては相手が信用できるとは限らないため、名前や電話番号など個人情報を相手に伝えるのは危険である。そのため、ナビゲッティに代表される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では、利用者のプライバシ情報の保護を技術的に実現せねばならない。そうしたプライバシの保護が実現されれば、日常に起こる多くの出会いにお

いて、利用者はコミュニケーショングループウェアを用いることが可能になる。

ところで、エニキャストを用いた位置依存サービス [2] を用いれば、インターネットに接続された携帯端末向けの位置依存サービスが実現可能となる。このサービスでは、携帯端末が HTTP 要求をエニキャストアドレスに対して送信し、その付近のエニキャストホストから位置情報を取得する。位置情報は HTTP リダイレクト応答の URL に埋め込まれて提供されるため、携帯端末は取得した位置情報を URL が示す WEB サーバに提出することが可能であり、一方、WEB サーバでは携帯端末の位置情報に応じた情報を配信することが可能である。

本論文では、インターネットに接続された携帯端末向けの位置依存サービスとして、ナビゲッティに代表される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を設計した。本グループウェアにおいては電子掲示版を用いたテキストベースのコミュニケーションだけでなく、メール、あるいはインターネット電話を用いた音声によるコミュニケーションも可能とした。音声通信の設計にあたっては、互いを信用しない利用者間でも通信可能であるよう匿名通話機能の設計を行った。

2 関連研究

2.1 NOTASIP

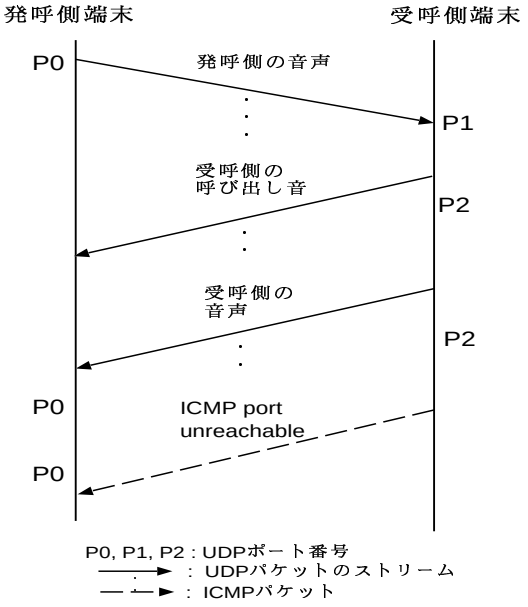

図 1: NOTASIP の動作概要

NOTASIP (Nothing Other than A Simple Internet Phone) [3] は、インターネットに接続された 2 台の端末が、双方向の音声通信ストリームを UDP [4] で確立するためのプロトコルである。Mobile IP [5] などと併用し移動により変化しない固定 IP アドレスを NOTASIP 対応の携帯端末に割り振ることで携帯インターネット電話端末が実現される。

NOTASIP の動作概要を説明する。まず発呼側の端末は通話に用いる UDP のポート (P0) を選択し、そのポートから受呼側端末の well-known ポート (P1) に音声通話データを送信し続ける。次に受呼側の端末は、通話に用いる UDP ポート (P2) を選択し、そのポートから発呼側端末のポート (P0) に呼出し音データを送信し続ける。もし受呼側端末が通話に応じない場合は ICMP port unreachable を返し、通話に応じる場合は既存の呼出しの音声データストリームの代わりに受呼側端末の音声データストリームを送信する。以上の動作概要を図 1 に示す。

NOTASIP では、受呼側が対応する音声データ形式や well-known ポートを発呼側が予め取得しておく必要がある。これらの情報は次のような URL で記述される。

```
iphone://<host>:<port>/<encoding-method>
```

例えば、RTP (Real-Time Protocol) [8] において 8KHz L16 モノラルエンコーディングと RTP ペイロードでダイナミックマップ 97 を用いる場合を次に示す。

```
iphone://mohta.person.titech.ac.jp:49230/&m=rtp:
49230:97:L16:8000
```

受呼側の URL を公開するディレクトサービスは WEB の検索エンジンとして提供される。この検索エンジンの動作概要を以下に示す。各行の頭にある C はその行がクライアントから検索エンジンへのデータであることを示し、S は検索エンジンからクライアントへのデータであることを示す。

```
C> HTTP /?tomonaga HTTP/1.1
C> Host:directory-serv.org
C>
S> HTTP1.1 200 OK
S> Content-Type:text/html
S>
S> iphone://192.168.0.1:10000/DVI4:8000
```

2.2 エニキャストを用いた位置依存サービス

エニキャストとは、複数のホストに共有される一つのエニキャストアドレス宛のパケットを、そのエニキャストアドレスを持つ複数のホストのうち、送信者からもっとものに到達させる技術である。

エニキャストを応用すれば、インターネットに接続した携帯端末向けの位置依存サービスが実現される。例えば無線 LAN 基地局ルータがその設置場所に応じた位置情報を HTTP で配信し、さらにエニキャストアドレスを持つとする。その基地局に接続する携帯端末がエニキャストアドレスに HTTP 要求を送信すれば、携帯端末は接続する無線 LAN 基地局ルータから位置情報を得ることが可能である。さらに HTTP/1.1 [9] のリダイレクトを応用すれば、携帯端末がリダイレクトに従うことで WEB サーバに位置情報を提出することが可能になる。この場合、無線 LAN 基地局ルータ上の HTTP サーバがエニキャストアドレスごとに位置情報を提出すべき WEB サーバを選択し、その WEB サーバの URL に位置情報を付加した次のような URL を HTTP リダイレクトで返信する。

```
www.example.com/?lat=e133.33.33&lon=n33.33.33
```

携帯端末はリダイレクトに従わないことで WEB サーバに位置情報を提出しないことが可能であるため、携帯端末の位置情報というプライバシは WEB サーバ単位で保護できる。

3 ナビゲッティの概要と利害得失

ナビゲッティは携帯電話向けのグループウェアであり、“めしモード” や “のみモード” など 7 種類の目的から 1 つを選択した利用者が、2.5 キロメートル以内に存在し、且つ同じ目的を持つ利用者とコニュニケーションを行うグループウェアである。ナビゲッティを用いて利用者は WEB 掲示板を介したテキストメッセージのやりとりを行う。また利用者の位置情報は携帯電話向け位置依存サービスである i エリア [6] や au の簡易位置情報 [7] を用いて特定される。

犯罪目的の利用を防止するため、利用者が選択可能な目的は安全なものに限定されている。また電子掲示版は暴力的あるいは不快な表現を書き込みの際に排除する機能を持つ。

ナビゲッティでは携帯電話向けでありながら匿名で音声通信を行えないという欠点を持つ。またメールも利用不可能である。

4 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の設計

4.1 匿名用識別子

電子掲示版、メール、電話を用いたコミュニケーションを匿名で行うため、グループウェアサーバはメールアドレス形式に適合した匿名用識別子を利用者に発行する。この識別子は匿名性維持のため常に変更が許されている。グループウェアサーバの FQDN が gware.org である時、ユーザに発行する匿名用識別子は例えば次のようになる。

```
alice@anonymous.gware.org
```

発行時にグループウェアサーバは、住所や氏名など利用者の身元を特定するに十分な情報、パスワード、グループウェアで使用する IP アドレス、そしてもし必要なら NOTASIP 用 URL の登録を求める。また登録情報の更新や抹消を行う手段を提供する。登録や更新に応じない利用者や、虚偽の情報を提出した利用者への識別子の発行は拒否される。また更新によって登録情報が不正なものになった場合、その利用者の匿名用識別子は剥奪される。これらの登録、更新、抹消は SSL など安全な通信路を用いて行なう。

一方、グループウェアと利用者は匿名用識別子を URL へ埋め込む形式について予め同意しておく必要がある。埋め込まれた URL は例えば次のようになる。

```
www.gware.com/?user=alice
```

4.2 目的情報と位置情報

グループウェアは利用者が選択可能な目的を定義し、それぞれの目的に URL で使用を許可された文字を用いて識別子 (目的識別子) を付ける。目的識別子は例えば次のような文字列となる。

```
nomi-mode
```

一方、グループウェアは URL において使用を許可された文字を用いて位置情報を表す形式を定義する。例えば北緯 33 度 33 分 33 秒、東経 133 度 33 分 33 秒の位置情報は形式に基づいて次のように表される。

```
lat=e133.33.33&lon=e33.33.33
```

また、目的情報と位置情報を URL に埋め込む形式は、予め利用者とグループウェア間で同意しておく必要がある。埋め込まれた URL は例えば次のようである。

```
www.gware.com/?lat=e133.33.33&lon=33.33.33
&p=nomi-mode
```

4.3 位置と目的情報の送信

利用者がグループウェアサーバに対して HTTP GET を送信する時、利用者は URL に匿名識別子、位置情報、目的情報を同意した形式で埋め込む。

URL への位置情報の埋め込みには、例えばエニキャストを用いた位置依存サービスを応用することが可能である。

4.4 WEB 掲示板による匿名通信

匿名識別子、位置情報、目的情報が埋め込まれた URL を含む HTTP GET を受信したグループウェアサーバは、それらの情報に応じた匿名通信用の電子掲示板を利用者に提供する。匿名用の電子掲示板を提供する場合、閲覧や書き込みの要求形式、あるいは要求とそれに必要な情報の URL への埋め込み形式は予め利用者とグループウェア間で同意しておく必要がある。これらが埋め込まれた URL は例えば次のようである。

書き込み:

```
www.gware.com/?board=write&msg=hello&lat=e133.33.33
&lon=e33.33.33&p=nomi-mode&user=alice
```

閲覧:

```
www.gware.com/?board=read&lat=e133.33.33
&lon=e33.33.33&p=nomi-mode&user=alice
```

グループウェアサーバは、URL に含まれる匿名識別子、位置情報、目的情報が予め同意した形式に適合しているかどうかを判定せねばならない。もし適合しない場合は HTTP GET を送信した利用者に対して HTTP 応答 “400 Bad Request” を送信する。適合していた場合は、さらに利用者が登録した IP アドレスから HTTP GET を送信しているかを判断する。もし登録された IP アドレスから送信されていない場合は、利用者に対して HTTP 応答 “403 Forbidden” を送信する。そうでなければ、目的情報や位置情報のほか書き込み用の情報を匿名識別子と組にして記憶し、提出された位置情報に近い利用者の匿名識別子とその利用者が書き込んだメッセージの一覧を HTTP 応

答 “200 OK” で返す。ここでどの利用者間が近いとするかはグループウェアサーバが任意に決定する。また個人情報に関するデータはここで一切表示しない。動作の一例を以下に示す。

```
C> HTTP (閲覧用 URL) HTTP/1.1
C>
S> HTTP1.1 200 OK
S> Content-Type:text/html
S>
S> Alice<alice@anonymous.gware.com><BR>
S> I never seen bars around here. Can you tell me where?<BR>
S>
```

4.5 メールによる匿名通信

グループウェアは利用者に対して匿名識別子を用いたメールサービスを提供することが可能である。このサービスを用いれば、グループウェアの掲示板から取得した匿名識別子の利用者とメールをやりとりすることが可能になる。

4.6 NOTASIPによる匿名通信

NOTASIPでは音声パケットを通話者間で直に送受信するため、パケットの送信元アドレスから通話相手が特定される。しかし、グループウェアが代理パケット転送を行えば、利用者はグループウェアサーバと通話を行うことで匿名通信を行うことが可能となる。以下、その動作原理を説明する。

匿名で発呼を望む利用者は受呼させたい他の利用者の匿名用識別子を何らかの方法で取得し、この識別子と自分の識別子を埋め込んだ URL をグループウェアに HTTP GET で送信する。この URL は例えば次のようである。

```
www.gware.com/?phone=notasip&from=alice&to=bob
```

次にグループウェアは HTTP GET を送信した IP アドレスが、発呼を望む利用者の IP アドレスに等しいか判定する。等しくない場合は発呼を望む利用者に “403 Frobiden” を送信して処理を終了する。そうでなければ登録情報から受呼者の固定識別子の検索を開始する。検索の結果、受呼者の固定識別子が発見されない場合はグループウェアサーバは発呼を望む利用者に”500 Internal Server Error”を送信して処理を終了する。発見された場合は、発呼側と受呼側の利用者の IP アドレスとポート番号を一組としたレコードを生成し、発呼を望む利用者に “200 OK” を送信する。ここでポート番号には未使用を意味する任意の負の整数を与える。レコードの 1 項目と 2 項目をそれぞれ発呼者と受呼者のアドレス、3 項目をポート番号とすれば、例えばレコードは次のようである。

```
(192.168.0.1, 192.169.0.2, -1)
```

また、“200 OK” を送信する際、そのボディ部を用いて、グループウェアサーバは発呼者に匿名通信先の NOTASIP の URL を伝える。この URL は受呼者の NOTASIP 用 URL の書き換えを行う。すなわちホスト名をグループウェアサーバのホスト名に、ポート番号をグループウェアサーバの受呼用ポート番号に置換する。この URL は例えば次のようである。

```
iphone://notasip.gware.com:10000/DVI4:8000
```

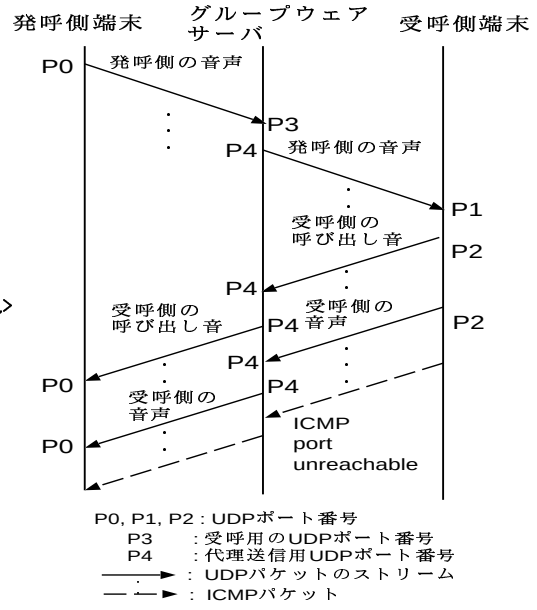

図 2: 匿名音声通信の動作例

4.7 代理転送の動作原理

グループウェアは NOTASIP の匿名通信に複数の UDP ポートを用いる。そのうち 1 つは受呼のために初期状態から用意され、残りは代理転送用のために未使用のポートが最大転送数分用意される。

受呼用ポートに UDP パケットが届くと、グループウェアはそのパケットの送信元 IP アドレスを調べ、そのアドレスが発呼側の利用者のアドレスに一致するレコードを検索する。レコードが発見されればそのポート番号の正負を調べ、負であれば未使用のポートから 1 つを選択し、それをレコードのポート番号に書き込む。このポートが代理転送ポートとなる。グループウェアは受信したパケットのアドレス部を書き換え、これを代理転送ポートから再送信する。ここで書き換えは送信元アドレスがグループウェアサーバのアドレス、送信先アドレスがレコードに含まれる受呼側の利用者のアドレスとなるよう行われる。もしレコードの発見に失敗あるいはポート部が正であればそのパケットは破棄される。

代理転送用ポートに UDP パケットが届くと、グループウェアはそのポート番号を調べ、同一のポート番号が含まれているレコードを検索する。レコードが発見されればパケットの送信元と送信先アドレスの両方がレコードに含まれているかを判定し、どちらも含まれる場合、グループウェアは受信したパケットのアドレス部を書き換えたパケットを生成し、これを元のパケットを受信した代理転送ポートから再送信する。ここでアドレス部の書き換えは、送信元アドレスがグループウェアサーバのアドレスに、送信先アドレスはパケットの送信元が発呼者のとき受呼者のアドレスに、受呼者のとき発呼者のアドレスになるよう行われる。もしレコードの発見に失敗あるいはアドレス部にいずれかが含まれていない場合はそのパケットは破棄される。

代理転送用ポートに ICMP port unreach が届くと、グループウェアサーバはそのパケットの送信元アドレスが発呼者あるいは受呼者の項目に含まれるレコードを検索する。レコードが

発見されればレコードに含まれるポート番号を負の任意の値に変え、そのポートを塞ぐ。塞がれたポートは NOTASIP と同様 286 秒間再使用しない。レコードが発見されない場合は受信した ICMP パケットを破棄する。

以上の原理に基づいた通話例を図 2 に示す。グループウェアサーバは発呼者と受呼者のパケット送信を模倣し、発呼者と受呼者からはグループウェアサーバと NOTASIP で通話しているように見える。

5 考察

本論文において設計したグループウェアは、その利用者が提出した位置と目的情報に基づき、近くにいる同じ目的を持つ利用者間のコミュニケーションを可能にする。そのコミュニケーションの手段としては、電子掲示板やメール、インターネット電話の利用が可能である。

IP アドレスなど利用者の個人情報を保護するため、設計したグループウェアはメールアドレス形式の匿名用識別子を発行し、利用者はこの識別子を用いて匿名メールの送受信やインターネット電話かけることが可能である。

6 終わりに

本研究では位置と目的情報に基づくグループウェアの設計を行った。今後は Zaurus SL-B500 への実装を行ない、評価を行う予定である。

参考文献

[1] いまだ系ここだ系ナビゲッティ.
http://www.navigety.tv/index.html

[2] 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

[3] Ohta M., Fujikawa K., Kitagawa T., Sola M.,
and Satoh K., “The Simple Internet Phone,” Proc. of
INET2000, July 2000

[4] J.Postel. User datagram protocol. RFC768, August 1980.

[5] C. Perkins, Ed.IP Mobility Support for IPv4. RFC3344,
August 2002.

[6] NTT DoCoMo,Inc. “オープン i エリア”,
http://www.nttdocomo.co.jp/mc-user/iarea_o.html

[7] KDDI 株式会社,“簡易位置情報”,
http://www.au.kddi.com/ezfactory/tecs/spec/eznavi.htm

[8] H.Schulzrinne, S.Canser, R.Frederick, V.Jacobson.
RTP:A Transport Protocol for Real-Time Applications.
RFC1889, January 1996.

[9] R.Fielding, J. Gettys, J.Mogul, H.Frystyk, L.Masinter,
P.Leach, T.Berners-Lee, RFC2616, June 1999.