インターネット電話の世界規模での管理運用モデルの設計と実験

新美 誠
慶應義塾大学 SFC研究所

直江 宏一
慶應義塾大学 環境情報学部

渡邊 晴美
慶應義塾大学 環境情報学部

塚田晃司
(株) 日立製作所システム開発研究所

概要

現在、インターネット電話サービスが商業サービスとして多数立ち上がっている。
しかし、現状では、いくつかの問題点があり、不必要な「電話とインターネットのゲートウェイ」の乱立や、汎用性の低い「特化されたサービス」の乱立を招き、インターネットの重要な要素である分散協調性を低下させ、「多様なメディアが流れるバックボーンとしてのインターネット」におけるメディア間相互透過性を損ねている。
そこで、本論文では、これら問題点を解消すべく、まず、インターネット上でのインターネット電話管理運用モデルを作成し、3点に分類した。
さらに、この3つのモデルについて、認証方法、課金方法、相手先指定方法 (名前空間)、ユーザ情報などの管理方法の4点について考察、検討し、実際のインターネット上において、実験を行った。
特に、この3つのモデルの内、「ワールドワイド」モデルでは、公開鍵暗号 [1] を使用した「通行証」の概念を新たに考案した。
また、これらのモデルをインターネット電話だけでなく、インターネット FAX への応用についても考察をおこなった。

Design and experiment of a global management model for Internet telephone

Makoto Niimi
KEIO Research Institute at SFC, Keio University

Hirokazu Naoe
Faculty of Environmental Information, Keio University

Harumi Watanabe
Faculty of Environmental Information, Keio University

Tsukada Koji
Systems Development Lab., Hitachi, Ltd.

Abstruct

In these days, Internet telephone service has become popular as commercial service.
But such service causes some problems in the Internet environment. There are too many gateways between telephone and the Internet and specially customized systems that have low generality. That weakens distributed cooperativrity of the Internet, one of the most important factor, and disturbs transparency between several kinds of media in the Internet environment as a backbone.
This peper prepared three models of practical management for Internet telephone on the net. Each model has four point as followings; How to certify, How to charge, How to point(Name Space), How to maint user information.
Experiment on these models especially focused on "World wide" one. That model invented new concept 'safe-conduct pass' using public key cryptography.
The study examined not only problems of system for Internet telephone but practical use of Internet fax.

1 はじめに

1997 年 9 月 1 日に国際公専公接続が、インターネット電話サービスだけに対して認められた。これは、通常音声のサービスなどを差し置いての先行解禁である。この先行解禁に伴い、インターネット電話サービスが商業サービスとして多数立ち上がった。

しかし、これら商業サービスには、以下のような問題点がある。

1. サービス会社ごとの独立したサービスで、相互乗り入れを考慮していない。
2. そのサービスのほとんどが、通常電話から発信し、インターネットを経由し、通常電話へ着信することだけを想定したサービスで、インターネット上のコンピュータから通常電話への発信やその逆などは考慮されていない。

これら問題点は、不必要な「電話とインターネットのゲートウェイ」の乱立や、汎用性の低い「特化されたサービス」の乱立を招き、インターネットの重要な要素である分散協調性を低下させ、「多様なメディアが流れるバックボーンとしてのインターネット [2]」におけるメディア間相互透過性を損ねている。

そこで、本論文では、これら問題点を解消すべく、まず、インターネット上でのインターネット電話管理運用モデルを作成し、以下の 3 点に分類した。

1. 社内モデル
2. プロバイダモデル
3. ワールドワイドモデル

さらに、この 3 つのモデルについて、以下の 4 点について考察、検討し、実際のインターネット上において、実験を行った。

1. 認証方法
2. 課金方法
3. 相手先指定方法 (名前空間)
4. ユーザ情報などの管理方法

特に、この 3 つのモデルの内、「ワールドワイド」モデルでは、公開鍵暗号を使用した「通行証」の概念を新たに考案し、現在では行われていない、複数のサービス会社に跨ったインターネット電話サービスを可能とし、その際、ユーザやゲートウェイマシンの認証、サービス会社を跨いだ課金も可能にしたので、詳しく述べた。

なお、本論文ではインターネット電話とは、図 1で示す 3 つの形態全てをあらわす。

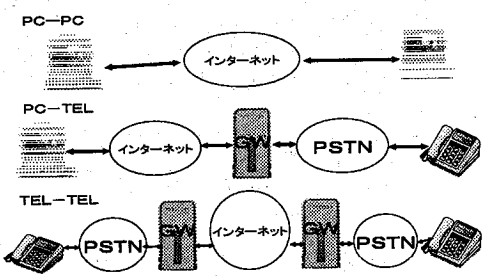

図 1: インターネット電話の 3 形態

このように、通常の電話から、パソコンで動作するインターネット電話への接続も考慮しているため、その相互透過性を保つために、相手の指定方法は全て数字で表すこととし、これをインターネット電話番号と呼ぶ。詳細は 3.1節で述べる。

2 インターネット電話管理運用モデル

インターネット電話管理運用のモデルをその規模に応じて以下の 3 つに分類した。

2.1 社内モデル

このモデルは、小規模な閉鎖されたネットワークでのモデルであり、企業内の内線の代わりに

インターネット電話を使うといった場合を想定している (図 2)。

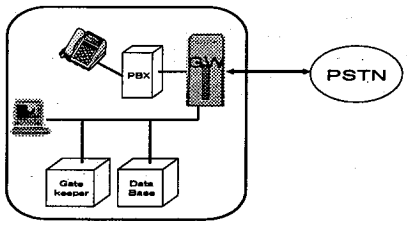

図 2: 社内モデル

社内に GateKeeper[3] やデータベースを持つ。データベースでは内線番号 (インターネット電話番号) と IP アドレスの変換テーブルを管理する。規模が小さいので、データベースの分散化は不要である。通話相手の指定方法は、以下の 3 種類が想定される。

1. 数桁の内線番号のみで指定
   地理的な場所の違いに関係無く、数桁の内線番号のみで管理する。ただし、規模が大きくなると不向き。

2. 代表呼び出し+内線番号で指定
   代表者番号に電話をかけ、応答メッセージの後に DTMF[1]で内線番号を入力する (ダイアルイン)。ISDN のようなデジタル電話ではサブアドレスの使用も考えられる。

3. 下数桁が内線番号となっているインターネット電話体系の採用
   会社毎 (ゲートウェイ [3] 毎) に会社番号を振るインターネット電話番号体系を作り、「会社番号」+「内線番号」という番号体系にする。

後述のモデルとの関係を考慮すると 3. を採用するのが望ましい。

[1]プッシュフォンのダイアルトーン。ピポパ音

課金については、このモデルではあまり必要が無いと思われる。ただ、ログを残すシステムは必要である。

2.2 プロバイダモデル

このモデルは、1 社のみのインターネットサービスプロバイダ会社[2]だけで運用する事を想定したモデルである (図 3)。

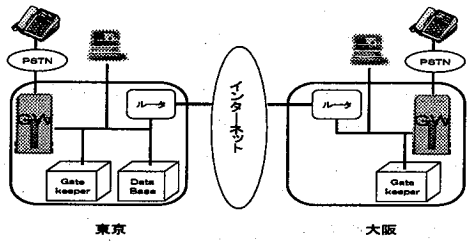

図 3: プロバイダモデル

このモデルでは、以下の事項を前提条件とする。

- 発信者は、そのプロバイダの契約者のみとする。
- 通話先がインターネットの場合は、通話相手はそのプロバイダ契約者のみ
- 通話先が公衆交換回線網[3]の電話の場合は、通話相手は特に限定しない。
- 使用するゲートウェイは、そのプロバイダ所有の物のみとする。
- インターネット電話番号から IP アドレスへの変換テーブルを持ったデータベースはそのプロバイダが管理する。

インターネット電話番号体系については、後述のワールドワイドモデルを考慮して、各プロバ

[2]以下プロバイダと省略
[3]通常の電話網。以下 PSTN とする

イダに特有の番号を上数桁に割り当て、各ユーザに下数桁に割り当てる。

PSTN 電話に発信する場合は、電話番号に特定の prefix をつけて指定し、IP アドレス変換データベースは使用しない。これは、内線電話から外線発信する場合には、0 や 9 といった prefix を付けて発信することが多いので、インターネット電話でも同様に扱った。

課金については、顧客情報管理のデータベースで一元管理する。

2.3 ワールドワイドモデル

このモデルは先のプロバイダモデルを拡張し、複数のプロバイダが分散協調を行いつつ運用するモデルである。このモデルでは、利用者が契約していないプロバイダのゲートウェイから PSTN へ発信する事も可能である (図 4)。

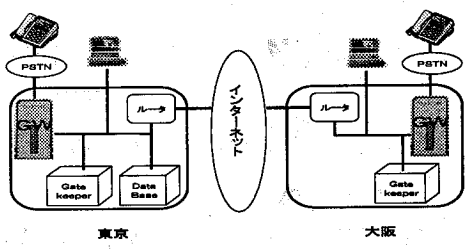

図 4: ワールドワイドモデル

インターネット電話番号から IP アドレスへの変換テーブルについては、全世界的なデータベースを集中管理することは困難であり、分散管理が必要である。このインターネット電話番号をサービス主体 (ここではプロバイダ) と無関係に割り当てると、番号→IP アドレスのデータベースを管理するのが複雑になる。そこで、上位数桁をプロバイダ番号とし、回数桁をユーザ番号とし、Domain Name System[4, 5] のように階層的に管理する。

PSTN 電話に発信する場合は、プロバイダモデルと同様に、電話番号に特定の prefix をつけて指定する。

課金については、利用者が契約しているプロバイダに課金情報が集まる必要があり、プロバイダ間での課金情報のやり取りを定める必要がある。本論文では、この課金のための仕組みを「通行証モデル」として提案し、4節で詳細を述べる。

3 インターネット電話番号とデータベース

本節では、インターネット電話番号とそれを管理するデータベースについて述べる。

3.1 インターネット電話番号

前述のように、通常の電話電話から、パソコンなどで動作するインターネット電話への接続も考慮するために、インターネット電話の名前指定方法には全て数字で表すこととし、本論文では、これをインターネット電話番号と呼ぶ。

このインターネット電話番号は「ワールドワイドモデル」の実現を考慮すると、インターネット電話番号→IP アドレスの変換テーブルが階層的に分散管理できるような体系にする必要がある。

そこで、既存の電話番号体系と同様に、

国番号 [6] + プロバイダ番号 + ユーザ識別番号

とする。

ユーザ識別番号は、利用者がプロバイダとサービス契約を結んだ時点で、プロバイダが発行する。

このような階層構造にすれば、各プロバイダは自社の契約者分についての変換テーブル・データベースを管理すれば良く、また、他のプロバイダ契約者にインターネット電話をかける際も検索が容易になる。

3.2 データベース

インターネット電話番号を管理するデータベースは、前述のように各プロバイダ毎に自社契

約者のインターネット電話番号と IP アドレスの対応を管理する。実際には、Domain Name System[4, 5] を、利用し TPC.INT[7, 8] と同様の仕組みを用いれば、容易に分散管理が可能である。

さらに、ダイアルアップ型接続や DHCP[9] などを利用すると、インターネット電話の IP アドレスが動的に変化する場合があるが、これは、Domain Name System Dynamic Update[10, 11] を利用することで対応が可能であり、このことは、分散データベースに Domain Name System を利用する利点の一つでもある。

4 通行証モデル

「ワールドワイドモデル」で使用する、通行証モデルを、図 5を元に説明する。

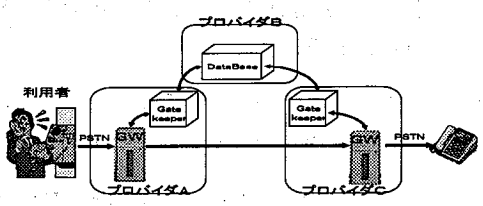

図 5: 通行証モデル

まず、条件として、プロバイダ A,B,C は提携関係にあり、利用者はプロバイダ B とのみ契約しているとする。

また、利用者の近くには契約してるプロバイダ B のゲートウェイがなく、また通信先の近くにもプロバイダ B のゲートウェイがないという場合を想定する。

最初に、利用者は身近なプロバイダ A のゲートウェイに電話をかけ、数字で構成された ID と PIN[4]を入力する。ID と PIN は、公開鍵暗号などを使った安全な通路を通り、プロバイダ B のデータベースに到着する。プロバイダ B のデータベースで認証を行い、正しく認証された場合に、プロバイダ B は自分の秘密鍵を用いて電子署名をした通行証を発行する。この通行証はプロバイダ B の公開鍵のみで開くことが可能である。つまり、通行証がプロバイダ B の公開鍵で開けた場合は、これを持った通信は、無条件で PSTN へ発信してよいことを保証する、つまり、PSTN への発信にかかったコストは電子署名をしたプロバイダ B が支払を保証することをあらわす。なお、この通行証は盗聴などによるリプレイアタックを防ぐために、時刻による有効期限が設定する。

そして、プロバイダ B が発行した通行証はプロバイダ A に渡り、実際に PSTN へ発信するプロバイダ C に渡る。プロバイダ C は、通行証があるので、発信者が不明でも、料金はプロバイダ B に請求すれば良いので、PSTN に向かって電話をかけ、通話を開始する。

通話が終了したら、その通信ログを課金情報としてプロバイダ B に送る。このようにすることで、プロバイダ C のゲートウェイには ID や PIN を渡さずに全てが処理でき、セキュリティーレベルの低下を防ぎつつ、かつ利用者が直接契約していないプロバイダを利用することができる。

この場合、各プロバイダのゲートウェイ、データベースなどのなりすましなどを防ぐためには、それぞれのマシン毎に秘密鍵と公開鍵を用意し、公開鍵暗号による認証を行う必要がある。

5 実験について

これらのモデルの検証として、実際のインターネット上で (株) 日立製作所のインターネット電話システムである、日立パーソナルマルチメディアコミュニケーションシステム Talkware[12] の改造機を用いて、WIDE Internet 内の国内 3 箇所、米国内 1 箇所の計 4 点にゲートウェイを設置し、現在実験をすすめている。

[4]Presonal Identification Number。数字だけのパスワード。

6 インターネット FAX への応用

今回は、インターネット電話でのモデリングと通行証モデルを提唱したが、これらはインターネット FAX でも同様に取り扱うことが出来る。

現在、インターネット FAX は IETF で国際標準化がすすめられている [13] が、このインターネット FAX システムは配送に電子メールを利用している。この電子メールに S/MIME などの公開鍵暗号方式を組み合わせれば、インターネット電話での場合と同様な実現が可能である。

7 おわりに

今後は、これらのモデルに基づいた実験をすすめ、スケーラビリティなどについて考察をすすめる必要がある。また、インターネット FAX に応用した実証実験も行い、IETF への提案等も考慮していきたい。

謝辞

本研究のきっかけをくださり、実験環境を提供してくださり、また、議論にお付き合いいただいた慶應義塾大学 徳田・村井・楠本・中村研究室の media-fusion group、(株) 日立製作所、WIDE プロジェクトと同プロジェクトの wt ワーキンググループ、の皆さんに感謝いたします。

参考文献

[1] Radia Perlman Charlie Kaufman and Mike Speciner. *NETWORK SECURITY*. Prentice Hall, 1995.

[2] 新美 誠. メディアバックボーンとしてのインターネット機構の研究. 慶應義塾大学大学院政策・メディア研究科 修士論文, January 1997.

[3] International Telecommunication Union. List Of ITU-T Recommendation H.323, Line Transmission of Non-Telephone Signals. May 1996.

[4] P. Mockapetris. Domain names - concepts and facilities, RFC1034. November 1987.

[5] P. Mockapetris. Domain names - implementation and specification, RFC1035. November 1987.

[6] International Telecommunication Union. List Of ITU-T Recommendation E.164, Assigned Country Codes. 1996.

[7] C. Malamud and M. Rose. Principles of Operation for the TPC.INT Subdomain: Remote Printing – Technical Procedures, RFC1528. October 1993.

[8] C. Malamud and M. Rose. Principles of Operation for the TPC.INT Subdomain: General Principles and Policy, RFC1530. October 1993.

[9] R. Droms. Dynamic Host Configuration Protocol, RFC2131. April 1997.

[10] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound. Dynamic Updates in the Domain Name System (DNS UPDATE), RFC2136. April 1997.

[11] D. Eastlake. Secure Domain Name System Dynamic Update, RFC2137. April 1997.

[12] (株) 日立製作所. 日立パーソナルマルチメディアコミュニケーションシステム Talkware. In *http://www.hitachi.co.jp/Prod/comp/network/talkware.htm.* (株) 日立製作所, 1996.

[13] J. Murai, H. Ohno, K. Toyoda, and D. Wing. A simple mode of facsimile using internet mail. *IETF Internet Draft,draft-ietf-fax-service-03.txt*, January 1998.