ユビキタス社会における情報アクセシビリティー
「インターネットを活用した『どこでも情報保障』の提案」

パソコン要約筆記サークル「ラルゴ」　矢野 佳子、栗田 茂明
愛媛大学大学院医学系研究科　木村 映善
愛媛大学総合情報メディアセンター　村田 健史

まえがき

パソコン要約筆記サークル「ラルゴ」では、約１年間、「在宅入力情報保障」について研究してきました。その結果を是非多くの方にご報告させていただき、情報保障における諸問題の解決の一助に寄与したいと考えています。なお、本稿の内容は、2006 年 6 月 10 日～11 日に札幌市において開かれた、第 24 回全国要約筆記問題研究集会第３分科会（情報アクセス権）で発表させていただいた内容に加え、時間の都合上やむを得ず割愛した部分をまとめたものです。発表およびデモンストレーションの機会を与えてくださった NPO 法人全国要約筆記問題研究会、並びに第３分科会のスタッフの皆様に、この場をお借りしてお礼を申し上げます。

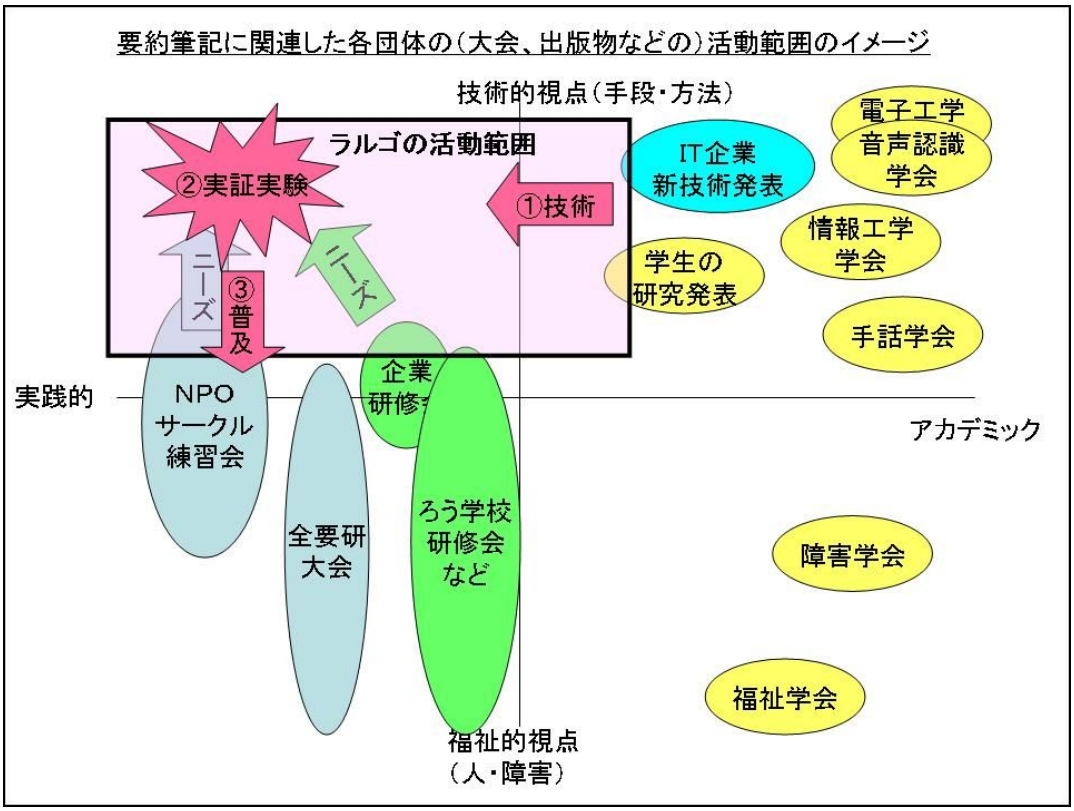
第１章　ラルゴについて

ラルゴは、インターネット上で活動する研究サークルです。例会、連絡などはインターネットを使って行うため日本のどこにいても参加でき、コミュニケーションは文字（メイル、チャット）であるため、健聴、難聴は関係ありません。（難聴の方も参加しています。）2006 年６月現在、北は北海道から南は鹿児島まで、全国から 19 名の会員が活動しています（**図－１**）。

図－１　ラルゴ会員マップ

ラルゴの研究目的は、サークルが単独で導入するには難しい技術を実践的な観点から検証し、分かりやすい方法に置き換え、要約筆記者に広めることです（**図－２**）。本発表のテーマ「在宅入力情報保障」についても、愛媛大学の研究者と協力して実証実験などを行い、全国のサークルが日常的な活動に採用できる方法を見つけたいと考えます。

（ラルゴのホームページ：http://iptalk.hp.infoseek.co.jp/largo/largo_top.htm）



図－２　ラルゴの活動領域イメージ

第２章　研究の背景

（１）パソコン要約筆記におけるユビキタス

パソコン要約筆記はこの８年間で情報保障としての市民権を得、入力の方法も一応完成し、全国各地で行われるようになりました。ネットワーク、パソコンの利用技術としても実用的なレベルに達し、本格的な普及の時期に入りつつあると考えます。

総務省は「いつでも、どこでも、何でも、誰でも」ネットワークに繋がることのできる「ユビキタスネット社会」を 2010 年に実現しようと「u-Japan 政策」を展開しています[2]。ICT（近年 IT は「コミュニケーション」を加え ICT と言われます）を活用するパソコン要約筆記もユビキタスネット社会への対応が期待されます。しかし、パソコン要約筆記者には要約筆記の技術（日本語力、要約力など）に加え、パソコン(Windows 操作、日本語入力、ネットワークなど)の技術とパソコン要約筆記特有の技術（連係入力）に関する技術などが必要であるため、手書きに比べて養成が進みにくく、慢性的に入力者が不足しています。

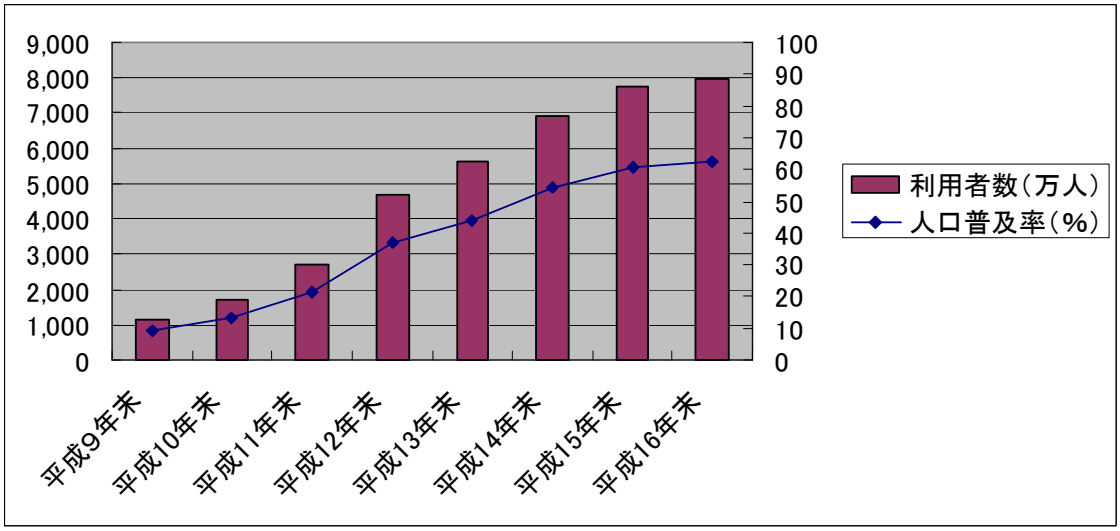
また、入力者は都市部に集中して在住しています。全国的にももちろんですが、都道府県レベルでも地域的偏在があります。障害者自立支援法の施行により、県内広域派遣について各地域で問題になったことは記憶に新しいところです。この「入力者の不足」と「入力者の地域的偏在」は特に「どこでも」に密接に関係し、パソコン要約筆記のユビキタスネット社会への対応を妨げていると感じます。

タイトルには「どこでも情報保障」という表現をさせていただいています。これは利用者だけでなく、入力者にとっても実現が望まれるところです。利用者が通信によって情報保障を利用する場合、利用者の情報源は文字のみ、データの送受信は片方向ですが、入力者の場合は、情報源は文字＋音声（＋映像）、データの送受信は双方向のため、入力者のユビキタスの実現はより難しいと言えます。

しかし、もしこれが実現されれば、入力者の移動を伴わず、移動に伴う経費を削減し、拘束時間を削減し、全体のコストダウンを図ることで、依頼者（主催者）側にも「どこでも」のメリットが適用されるかもしれません。入力者として新たな資源（町村部在住者、育児中の主婦層、外出が困難な下肢障害者など）の掘り起こしも可能になるかもしれません。また、それによって、情報保障の依頼が増加し、「何でも」を始め、他のスローガンの実現への良循環に繋がる可能性が期待されます。

近年、「u-Japan 政策」の前身「e-Japan 政策」の成果で、インターネット、ブロードバンドが家庭レベルで浸透してきました。インターネットによって、日本に限らず、世界中のコミュニケーションの地理的、時間的、費用的制約が解消されつつあります。インターネットの普及によって「ユビキタスネットワーク社会」の実現が現実的になってきたと言えるでしょう。前述のように、パソコン要約筆記による情報保障ついてもユビキタスを実現するためには、一般的なコミュニケーション同様、これらの制約を解決する必要があり、インターネット、ブロードバンドは、その有力な手段となり得ると考えられます。

総務省の調査[3]によれば、平成 16 年末現在、日本におけるインターネットの利用状況は**図－３**の通りです。



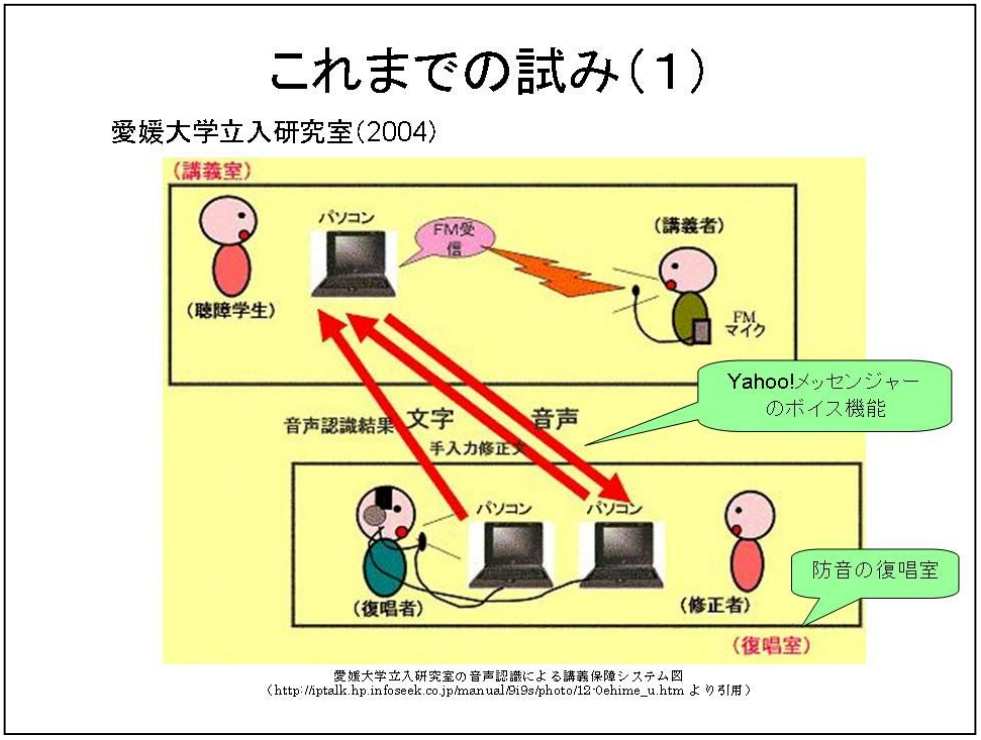
図－３　総務省「通信利用動向調査」より

このように、家庭へのインターネットの普及が進んでいます。（平成 16 年末現在、インターネット利用者 7,948 万人、人口普及率 62.3%）これに伴い、「入力者の不足」の解決方法の一つとして、「インターネットを使い在宅で入力する」（在宅入力情報保障）という方法を従来から多くの方が提案しています。

（２）これまでの試み

① 愛媛大学立入研究室の講義保障システム（2004 年）

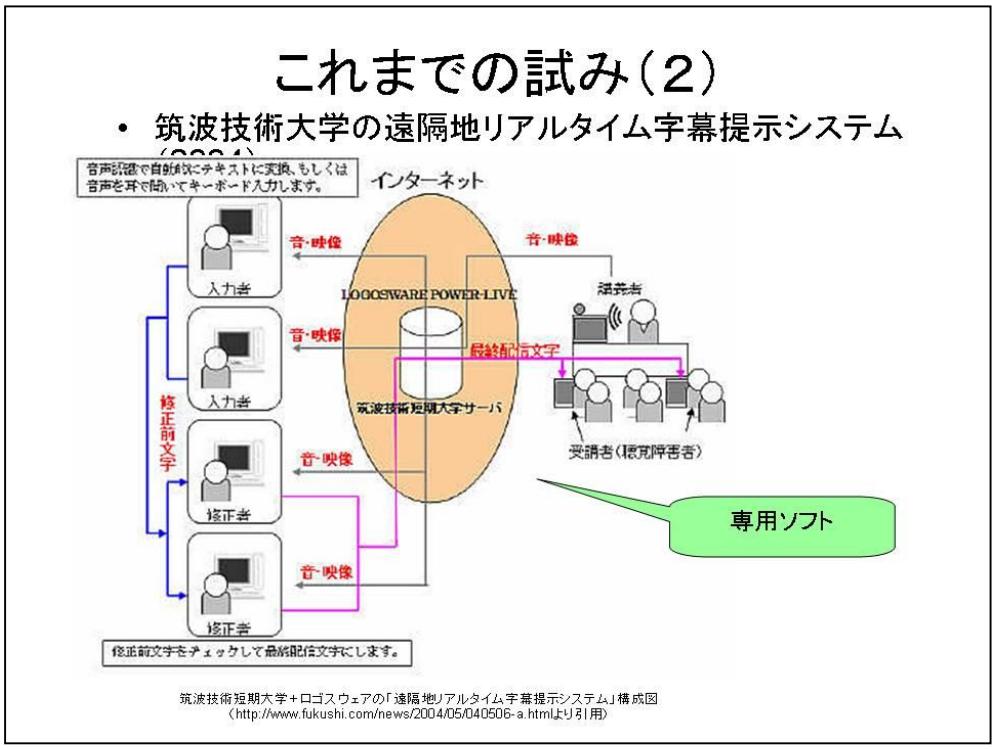
講義室から離れた場所（学内）にある復唱室から講義室への情報保障が行われました。音声の通信はインターネット（Yahoo!メッセンジャーのボイスチャット機能）を用い、音声認識システムで作成された文字情報は学内 LAN を介して利用者のパソコンに送られました。（**図－４**）



図－４　愛媛大学立入研究室の音声認識による講義保障システム[4]

② 筑波技術短期大学（現筑波技術大学）の遠隔地リアルタイム字幕提示システム（2004 年）

専用ソフトウェアによる情報保障を行っています。専用ソフトウェアは VPN の機能を持ち、ファイアーウォールの問題（p.8）の解決が図られています[5]。同大学では、このシステムを利用した情報保障支援や技術的支援も行っています。（**図－５**）

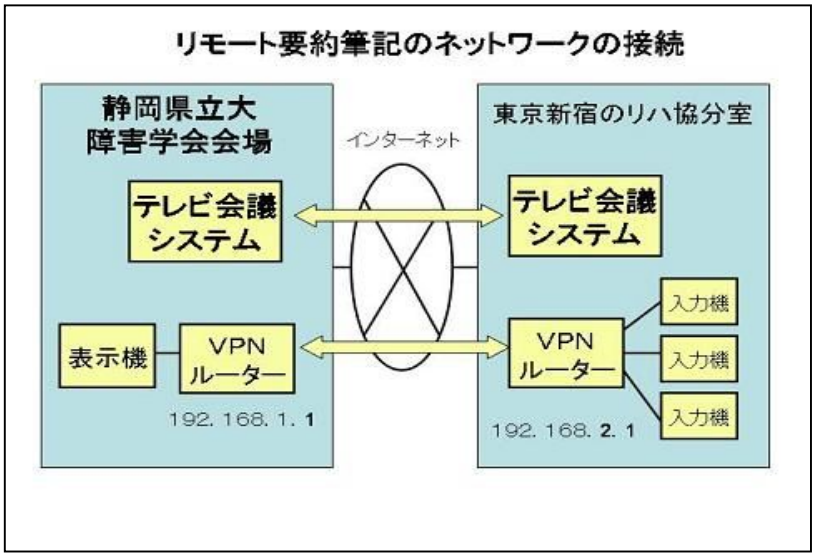


図－５　筑波技術大学とロゴスウェアの「遠隔地リアルータイム字幕提示システム」[6]

③ 障害学会第一回大会のリモート要約筆記（2004 年）

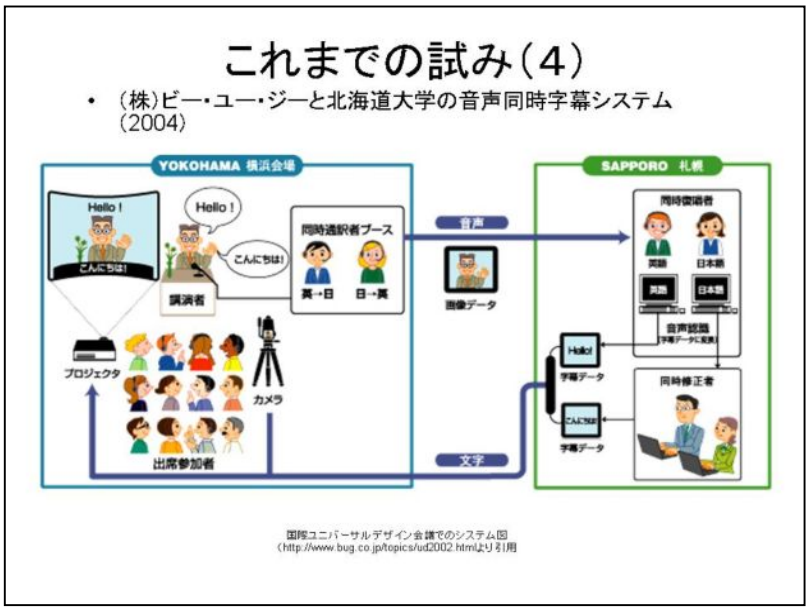
図－６　障害学会で使用された機器
（左：テレビ会議システム、右：VPN ルータ）[4]

2004 年 6 月 12 日～13 日に静岡県立大学において開かれた同大会で行われた、遠隔からの情報保障です。入力は全国要約筆記問題研究会が協力し[7]、VPN ルータ（図－６）を用いて静岡の会場と東京の入力室をビデオ会議システム（図－６）とインターネットで接続し、情報保障を行いました。（図－７）



図－７　障害学会リモート要約筆記システム図[4]

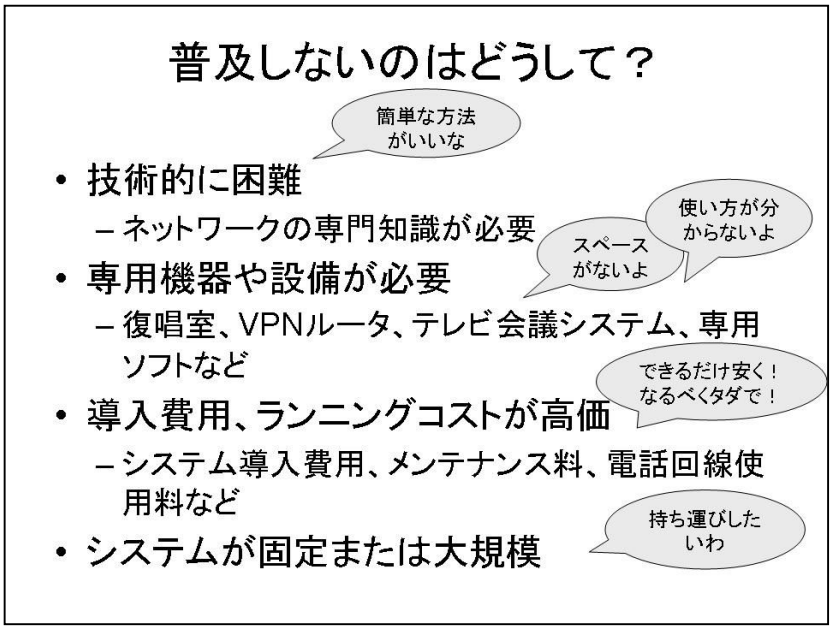
④（株）ビー・ユー・ジー（BUG）＋北海道大学の音声同時字幕システム（2002 年）



図－８　国際ユニバーサルデザイン会議でのシステム[8]

2002 年、札幌で行われた世界 DPI 会議、横浜で行われた国際ユニバーサルデザイン会議において使用されたシステムです。音声は電話回線、文字情報はインターネットを介して送信されました。（図－８）

（２）普及しないのはどうして？



図－９　普及しないのはどうして？

①～④のいずれもインターネットを活用しますが、運用にはネットワークの知識と特殊な機器（復唱者用防音室、VPN ルータなど）や費用（システム導入費用や保守料、電話回線および通話料）が必要なため、一般のサークルでの導入は難しいと思われます。（図－９）

また、セッティングについても「どこでも」を実現するためには、利用者が単独で短時間にできる簡便性と機動力が求められますが、いずれのシステムでもまだ実現されていません。

第３章　在宅入力情報保障実験計画

（１）問題点の確認

入力者の大多数を占める一般のボランティアサークルが情報保障としてこれまでの方法を取るには至っていません。これには、次のような理由があると考えています。

① 要約筆記用ソフトウェア（IPtalk)がインターネットでは使いにくい（機能的に不充分である）
② ルータの設定やパソコンの設定など、機器類の取り扱いの情報が少ない
③ 利用者と離れて在宅で入力する情報保障の運用方法（依頼の受け方、入力者の手配、トラブルの対応方法）などが確立していない
④ 実施している一般のボランティアサークルが無い

また、これまでの試みは、主に利用者側が「どこでも情報保障が受けられる」ことを目指すものでしたが、入力者側が「どこでも情報保障に参加できる」ことを検討した試みを私たちは知りません。そこで、今回私たち「パソコン要約筆記 ラルゴ」の活動テーマとして、主に入力者側の視点から「どこでも情報保障」を実現するための方法の１つとしてインターネットを活用した「在宅入力情報保障」の検討と実証実験を行いました。

本稿では、①と②について報告します。

（２）実験の概要

前述の問題点を踏まえ、ラルゴでは、専用の機器類を用いた方法から無料でできる方法までいろいろな方法を試し、一般のサークルに最適な方法を見つけたいと考えました。また、評価についても、従来のフィーリングによる定性的な評価ばかりではなく、愛媛大学村田研究室の協力を得て、入力やネットワーク環境などの定量的な評価も行っています。

実験は**図－10** の要領で行いました。

STEP 1	インターネットで IPtalk を使う方法の検討
STEP 2	インターネットを使って動画や音声を送受信する方法の検討
STEP 3	インターネットを通して配信される動画や音声（大学の講義ビデオ）で在宅入力する実験
STEP 4	模擬講義をインターネットで情報保障する実証実験
STEP 5	講義をインターネットで情報保障する運用実験

図－10　在宅入力情報保障実験の概要

実施日程は**図－11** のとおりです。

図－11　実験日程

第４章　実験

1　STEP　1　インターネットで IPtalk を使う方法の検討

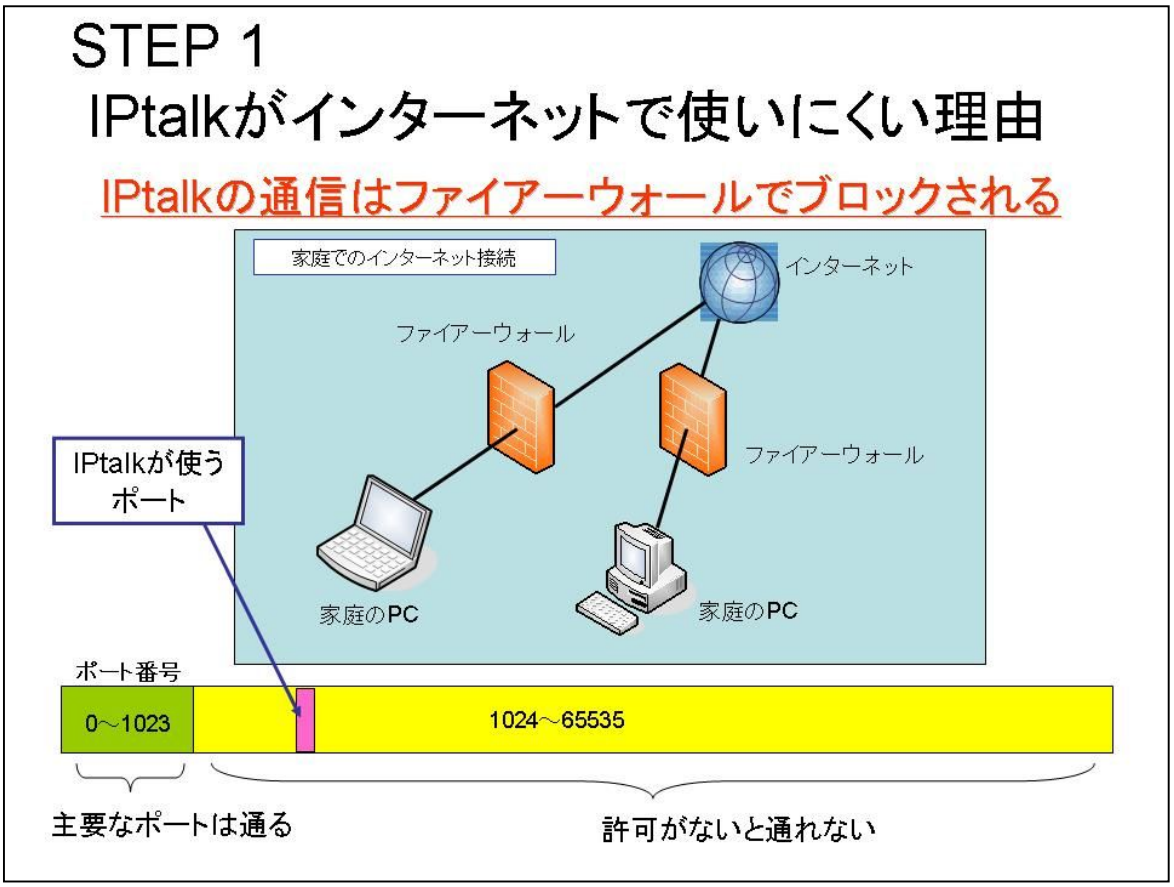
（１）　IPtalk がインターネットで使いにくい理由

IPtalk には、インターネットでも利用できる機能「インターネットウィンド」が実装されています。しかし、その機能を使っても通信ができない（相手がパートナーページに現れない、入力した文字がお互いにモニタできない、など）ことがあります。その主な理由は、ファイアーウォールと考えられます。

ファイアーウォールにはいろいろありますが、一般には決まったポート番号のみを通す機能を備えています。インターネットで使用するポートにはメール送信用、受信用、ホームページ閲覧用など、あらかじめ用途が決まっており頻繁に使用されるもの(well-known port ウェルノウンポート= 0～1023 番)と、独自に開発したアプリケーションで自由に使えるもの(Ephemeral port エフェメラルポート= 1024～65535 番)があります。

ファイアーウォールでは、前者の主要ポートは開放されていますが、後者は外部からの攻撃を防ぐため、許可なしでは使えない仕組みになっており、ADSL や光ケーブルなど、インターネット常時接続の状態でもセキュリティが確保されます。

IPtalk では後者のポートを利用して通信を行ってるため、LAN では問題なく通信できますが、インターネットで通信する場合は、ファイアーウォールによって通信がブロックされます。（**図－12**）



図－12　IPtalk がインターネットで使いにくい理由

1）　ファイアーウォールの分類と IPtalk

家庭におけるファイアーウォールとして、①ルータ、②Windows ファイアーウォール、③ウィルス対策ソフトウェアが挙げられます。

① ルータ

家庭においてインターネットを利用する場合、インターネットと家庭内 LAN を接続する、ブロードバンドルータが用いられることがあります。

また、複数台のパソコンやプリンタ等を LAN 接続する家庭では、家庭内 LAN を構築するためにローカルルータが用いられることがあります。

これらは前述の通り主要なポートのみの通信を通すため、IPtalk の通信はブロックされます。

② Windows ファイアーウォール

ラルゴで収集した情報によれば、Windows ファイアーウォールは、「有効」のままでも IPtalk の通信は通すため、特に問題ないと考えられます。

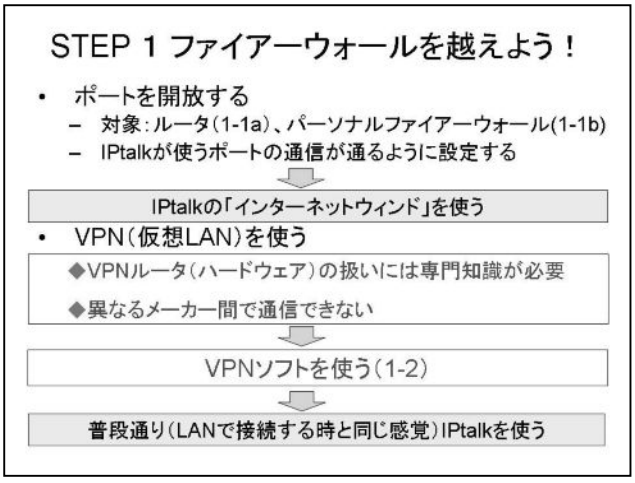
Windows XP の場合、各バージョンの初回起動時に「ブロックを解除する」を選択すれば、以後はインターネットでの通信も通します。

③ ウィルス対策ソフトウェア

近年、ウィルス被害の拡大により、パソコンにセキュリティ対策のため、ウィルス対策ソフトウェアをインストールすることが推奨されています。主なアプリケーションには、「ウィルスバスター」「ノートン・インターネットセキュリティ」「マカフィー・パーソナルファイアーウォールプラス」などがあります。ウィルス対策ソフトウェアは、インターネットを介しての通信を監視したりブロックしたりしています。IPtalk の通信は前述の通りあまり使われないポートを経由するため、ウィルス対策ソフトウェアによっても通信がブロックされているケースがあります。特に何も設定しなくても IPtalk の通信を通していると思われるソフトウェアもありますが、通信の安定性に疑問があります。

2）　ファイアーウォールを越えよう！

ファイアーウォール越えるためには、（1）IPtalk で使用するポートを開放する（穴を開ける）設定をする方法と、（2）VPN（仮想 LAN）を使う方法が考えられます（**図－13**）。そのため、具体的に IPtalk をインターネットで使うには、大きく分けて以下の２つの方法があると言えます。



図－13　ファイアーウォールを越えよう！

① 「ポート開放」し、IPtalk の「インターネットウィンド」を使う

② VPN ソフトウェアを使う

それぞれについて、以下で概要と実験結果を説明します。

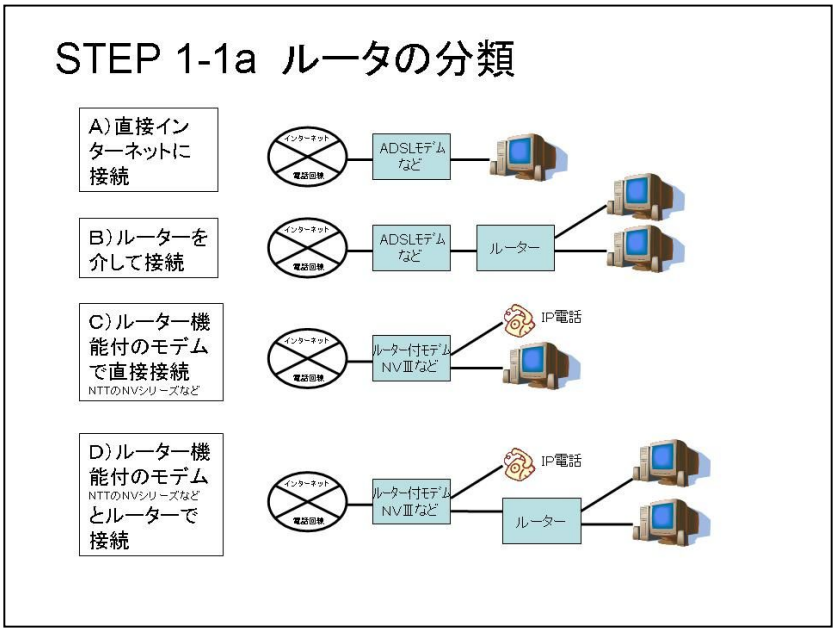
なお、VPN はこれまでにも試みられていますが、ハードウェア（機器）で構築されていたため、ネットワークの専門知識が必要であり、また異なるメーカー間で通信できないことが導入しにくい理由と考えられます。そこで、ラルゴでは、ハードウェアではなくソフトウェアを用いて VPN を構築する方法を試みました。

（１）ポート開放

１）　ルータのポート開放

ルータのポート開放（穴あけ）の設定方法は機種によって様々です。設定の際に使われる用語も統一されていないため、情報共有が困難です。ラルゴでは、会員の各家庭にあるルータについて設定方法などの情報収集と公開の準備を進めています。

インターネットを介して在宅入力をする場合、各家庭の通信環境は**図－14** のように分類できます。



図－14　ルータの分類

図－14 の分類のうち、B)、C)、D）の環境の家庭から在宅入力を行う場合、ルータは IPtalk の通信をブロックします。これらに該当する家庭は総務省の調査からも多数を占め[3]、今後も増加が見込まれるため、これらの家庭への対策は不可欠です。

１．ポート開放の方法

ルータのポート開放は、**図－15** の手順で行います。設定の詳細はルータの機種により異なるため、ラルゴでは会員の使用するルータについて設定情報を収集しています。ポート開放の機能には、次のような名前が使用されています。

「アドレス変換」「バーチャルサーバ」「静的マスカレード」「ポートマッピング」「NAT アドレス変換」「スタティック IP マスカレード」「ローカルサーバ」

使っているルータに、IPtalk で使用している以下のポート番号を開放するよう設定します。

ポート番号（ＵＤＰ）
6711,6712,6713,6718,6719,6721,6722,8723,6724,6727,6731
（6711-6731 のように、まとめても可）

STEP 1-1a ポート開放の方法

1. 自分のPCのIPアドレスを固定する
   - ■ DNSサーバアドレスを控えておく(プロバイダ毎に違う)
   - ■ 家庭内LANに接続する機器の台数より多い数の番号を割り当てるのがコツ
2. ルータのポート開放をする
   - ■ 機能の名称はメーカーや機種によって違う

     アドレス変換、バーチャルサーバ、静的マスカレード、ポートマッピング、NATアドレス変換、スタティックIPマスカレード、ローカルサーバ、…など
   - ■ IPtalkで使用するポートを、1. で割り当てた自分のPCのIPアドレスに送るよう設定する(機種によって方法は異なる)

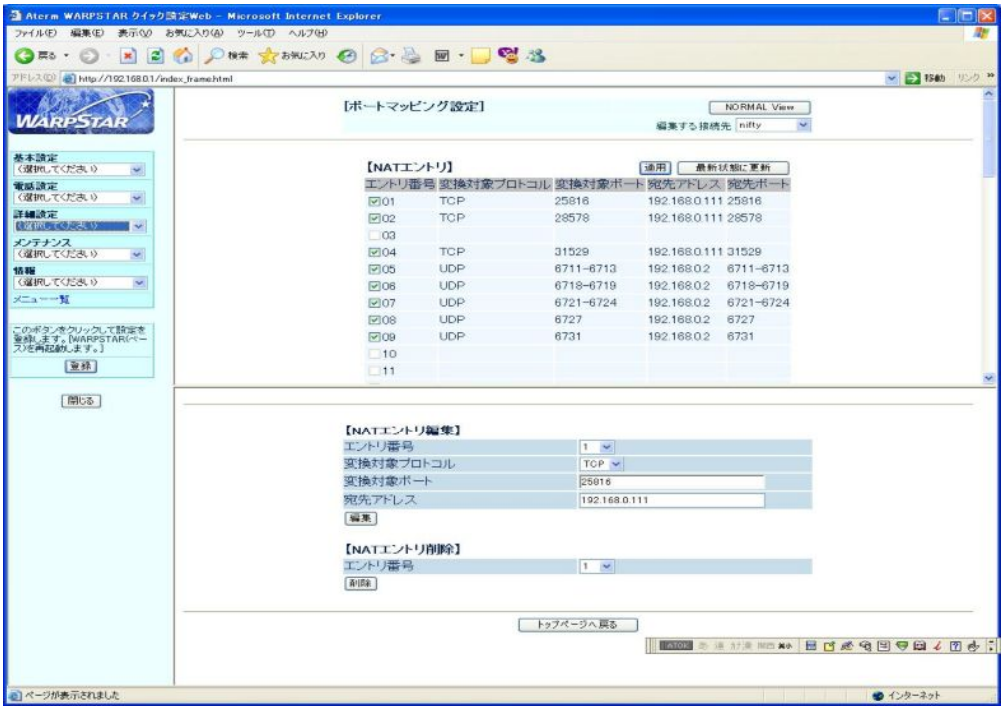
IPtalkが使用するポート(全てUDP)	6711, 6712, 6713, 6718, 6721, 6722, 6723, 6724, 6731 (6711-6731 のように、まとめて設定しても良い)

図－15　ポート開放の方法

２．ポート開放の例

図－16 のルータ機能付き ADSL モデム（NEC WARPSTAR Aterm WD605CV）の場合、ポート開放の設定をする機能は「ポートマッピング」と呼ばれます。IPtalk で使用するポートは UDP 6711～6731 ですが、**図－16** ではより細かく設定をしています。

家族が別々のパソコンを使う家庭が増えています。パソコン以外にも、プリンタや DVD プレイヤーなど、家庭内 LAN に接続される機器が増えています。そこで、特定のポート宛に届いた情報を特定のパソコン宛に送るよう設定するため、パソコンの家庭内 LAN 用 IP アドレス（プライベートアドレス）を固定します。この例では「192.168.0.2」が IPtalk の通信用に使うパソコンの IP アドレスです。この設定で、IPtalk で使うポートに届いた通信が、「192.168.0.2」のパソコンだけに送られるようになります。



図－16　ポート開放の例（１）

図－17 のルータ（corega BAR SD）では、同じ機能が「バーチャルサーバー」と呼ばれます。

図－17　ポート開放の例（２）

３．IPtalk の「インターネットウィンド」

IPtalk9i の「インターネットウィンド」を使う方法です。手順は以下のとおりです。

① ルータのポート開放（穴を開け）をします。

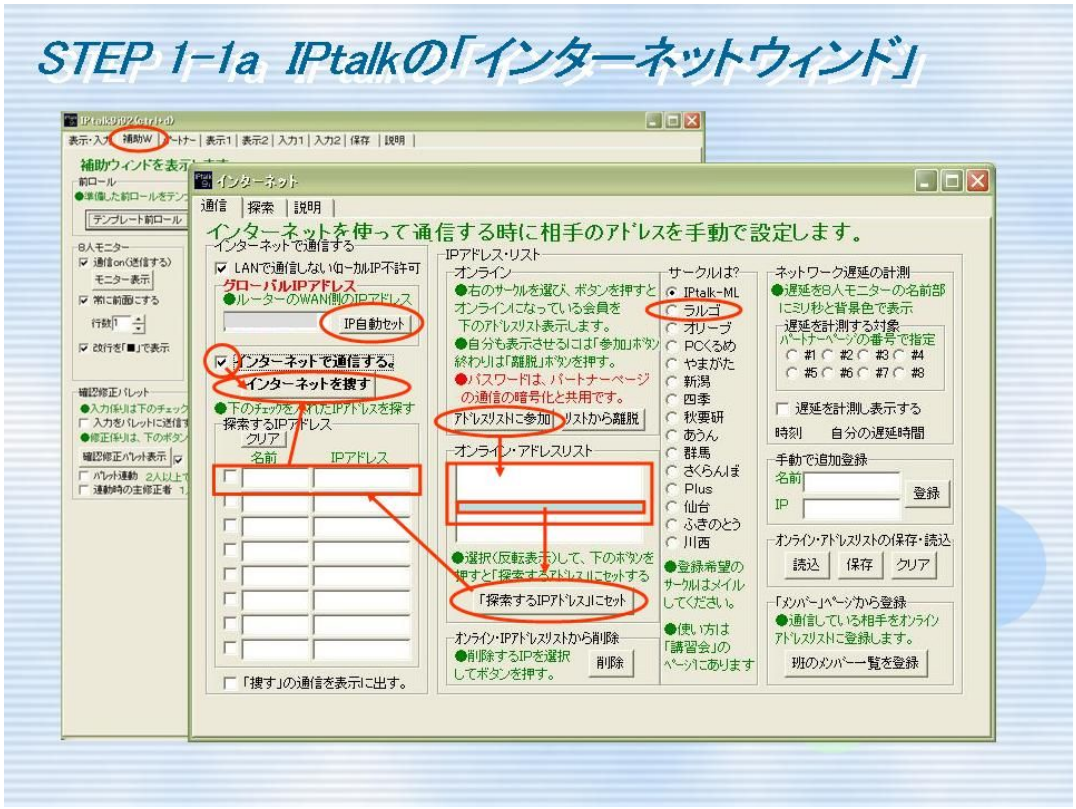
② 「通信」ページの「グローバル IP アドレス」に「IP 自動セット」ボタンを押して、ルータのグローバル IP アドレスを入力します。

③ 「通信」ページの「インターネットで通信する。」のチェックを入れ、「探索する IP アドレス」の「IP アドレス」の枠に相手の IP アドレスを入力し、チェックを入れます。

＊ サークルが登録してあれば、「サークルは？」のラジオボタンをいれ、「オンライン」の「アドレスリストに参加」ボタンを押すと、インターネットに接続している IPtalk の IP アドレス一覧が出ます。

④ 「インターネットを捜す」ボタンを押すと、後は通常通り通信できます。

図－18 にインターネットウィンドの操作画面を示します。



図－18　IPtalk の「インターネットウィンド」

４．ポート開放実験手順

「ポート開放」が完了している人が、「被験者」の通信を以下の手順でチェックします。

Ａ０）被験者は、IPtalk を立ち上げます。

Ａ０－１）「パートナー」ページの「通信を暗号化する」のチェックを入れ、「→パスワード」の横の枠にパスワードを入力します。

Ａ０－２）「補助W」ページの「インターネットを探索」の「インターネット」ボタンを押します。

Ａ０－３）「インターネット」ウィンドの「ＩＰ自動セット」ボタンを押します。→出ない時は、もう一度押してください。

Ａ０－４）「インターネットで通信する」のチェックを入れます。（インターネットを捜すのボタンが現れます。）

Ａ０－５）「サークルは？」のラジオボタンを入れます。

Ａ０－６）「アドレスリストに参加」のボタンを押します。（下の「オンラインアドレスリスト」に自分の名前が現れます。）

Ａ０－７）ファイアーウォールを無効にする必要のある人は無効にしてあるかチェックしてください。

この時に「インターネットで捜す」のボタンは押さずに待ちます。

Yahoo! メッセンジャーで、チェックする人に準備完了と伝えます。

Ａ１）この状態で、チェックする人から「インターネットで捜す」をしてもらい、

Ａ１－１）チェックする人のメンバー一覧に現れる。

Ａ１－２）被験者のメンバー一覧に現れる。

Ａ２）チェックする人が「なってよ！」ボタンを押した時、

Ａ２－１）チェックする人でパートナーボタンが動く。

Ａ２－２）被験者でパートナーボタンが動く。

Ａ３）チェックする人が何か入力した時に

Ａ３－１）被験者の表示部に表示される。

Ａ３－２）被験者のモニター部に表示される。

Ａ３－３）被験者の８人モニターに表示される。

Ａ４）被験者が入力部で何か入力した時に

Ａ４－１）チェックする人の表示部に表示される。

Ａ４－２）チェックする人のモニター部に表示される。

Ａ４－３）チェックする人の８人モニターに表示される。

－－－－－－－－－－－－－－－－－－－－

テストＢ

テストＡの後に試します。次は、被験者が操作します。

まず、チェックする人が、テストＡで出た一覧を元にもどします。

・チェックする人が「パートナー」ページの「お休み」ボタンを押します。

・チェックする人が「パートナー固定」のチェックを外します。（これを忘れると通信できません。）

・被験者の一覧からチェックする人が消えるはずですが、たまに消えないこともありますが、そのままテストＢ１を行います。

Ｂ０）被験者が次の準備をします。

Ｂ０－１）「オンラインアドレスリスト」からチェックする人の名前をクリックして反転表示させます。

Ｂ０－２）「探索するＩＰアドレスにセット」ボタンを押します。（左の「探索するＩＰアドレス」にチェックする人の名前とＩＰが表示されます。）

Ｂ１）次に、被験者が、「インターネットで捜す」のボタンを押します。
　　Ｂ１－１）チェックする人のメンバー一覧に現れる。
　　Ｂ１－２）被験者のメンバー一覧に現れる。
Ｂ２）被験者が、「なってよ！」ボタンを押した時、
　　Ｂ２－１）チェックする人でパートナーボタンが動く。
　　Ｂ２－２）被験者でパートナーボタンが動く。
Ｂ３）被験者が、何か入力した時に
　　Ｂ３－１）チェックする人の表示部に表示される。
　　Ｂ３－２）チェックする人のモニター部に表示される。
　　Ｂ３－３）チェックする人の８人モニターに表示される。
Ｂ４）チェックする人が入力部で何か入力した時に
　　Ｂ４－１）被験者の表示部に表示される。
　　Ｂ４－２）被験者のモニター部に表示される。
　　Ｂ４－３）被験者の８人モニターに表示される。

５．ルータのポート開放実験結果

ポート開放が行えた例と行えなかった例がありました。

「接続方法」と「ポート開放の可否」については、以下のように言えると思います。

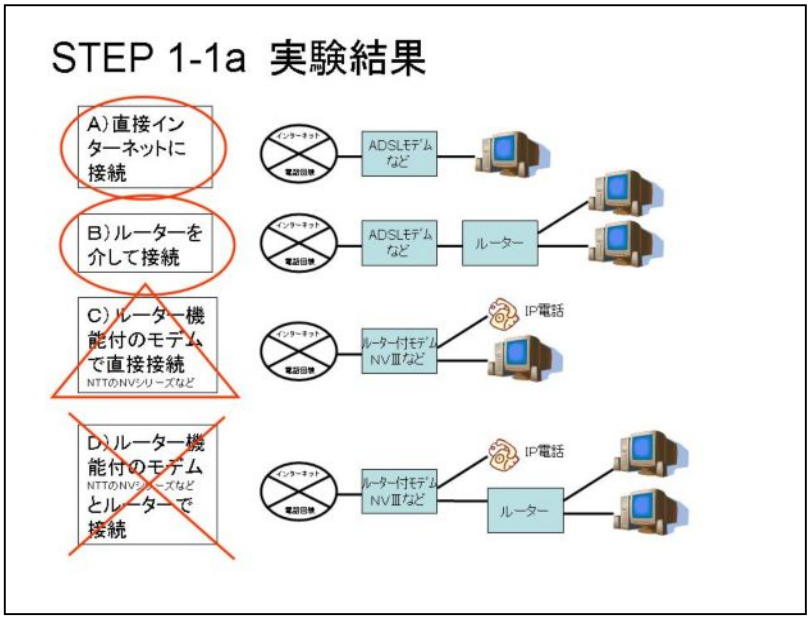
「ＯＫ」となった人のルータ接続種類は、圧倒的に「Ａ」「Ｂ」が多く、「Ｃ」は２件、「Ｄ」はありませんでした。（**図－19**）

「Ａ」は何もしなくても穴が開いている。

「Ｂ」の人が使った設定は、「バーチャルサーバー」「アドレス変換」である。

「Ｃ」の人が使った設定は、「NAT エントリ」と「DMZ ホスト」で、後者は正しいルータの使い方とは言えない。（通常、DMZ は外部に対して公開する必要のあるサーバを置くための機能）

また、「Ｃ」の中には、不完全に開放された例がありました。ラルゴの収集した範囲内では、機種に依存する問題と考えられます。これについては、次ページの考察の中で詳しく述べます。



図－19　ルータのポート開放実験結果

６．ルータのポート開放についての考察

ア） 集合住宅の共用ルータ

各家庭のネットワーク環境は多様化しています。最近はインターネット付きマンションが増えていますが、光ファイバーや有線放送、CATV などのインターネット回線を使用している場合は、マンション全体で１台のルータを共用している場合があり、個人の権限ではポート開放ができません。また、その場合には、マンション全体で１回線の通信帯域を分け合うため帯域の確保が流動的になり、通信が不安定になる可能性も考えられます。

イ）二重ルータ

家庭内の複数のパソコンで同時にインターネット接続をする家庭が増えています。各家庭に接続されているインターネット回線は、通常１回線なので、それを複数で分け合うために、家庭内 LAN を構築する家庭が増加していますが、中にはローカルルータを使用して構築するケースがあります。ローカルルータには有線 LAN 用、無線 LAN 用があります。

家庭に ADSL または光ファイバーなどのブロードバンドルータがある場合、家庭内 LAN 用のローカルルータを使用すると、ルータが二重になります。

ポート開放を行う場合には、両方のルータにポート開放の設定を行う必要がありますが、ローカルルータのポート開放の設定が複雑になります。ローカルルータに「アクセスポイントモード」等と呼ばれるブリッジ接続機能がない場合は、二重ルータの解決にはやや専門的な知識が必要なようです。

ウ）機種に依存する問題

プロバイダは、ルータ付きモデムをレンタルする場合があります。**図－19** ルータの分類Ｃ）において、NTT が貸与している一部のルータ（SV シリーズ、NV シリーズ）では、ポート開放の設定をしていても、外側からのアクセスはブロックし続け、内側から通信を通すことで初めて双方からの通信が可能になります。

この動作は不具合ではないのですが、情報保障場面においては、入力者の場合、パートナーが IPtalk で送信してくれるまでは、パートナーの入力がモニターできないという問題があります。利用者の場合は、自分から何かを送信しない限り、入力された文字列が届きません。そのため、各自が自分のルータの状況を把握したり、お互いに通知し合う仕組みやルールが必要になると思われます。

エ）プロバイダに依存する問題

Yahoo!BB の無線 LAN パックでは、グローバル IP アドレスを知ることができないため、IPtalk のインターネットウィンドの設定ができません。ラルゴ会員の例では、無線 LAN を使わず、有線 LAN を使用すると解決できました。理由は不明です。

オ）セキュリティの問題

ポート開放をする場合、IPtalk の通信だけを通すよう設定できるわけではありません。IPtalk と同じポートから入る情報は、全て通してしまいます。もしそこに外部から悪意のあるアクセスがあったとしても、自分のパソコンは無防備になります。不特定多数に対しポート開放を行うことは、セキュリティ上は好ましくないと言えるでしょう。

ルータの中には、ポート開放をする相手先 IP アドレスを指定する機能を備え、セキュリティを確保した状態でポート開放を行えるものもあります。しかし、実際に IPtalk での通信を行う場合には、家庭で固定のグローバル IP アドレスを所有している例は少ないため、ポート開放の相手を指定する方法は手続きが煩雑になり、現実的ではないでしょう。

2）　パーソナルファイアーウォール

ウィルス対策ソフトウェアにこの機能があり、ルータのポート開放ができていても、ここでブロックされることがあります。設定は各パソコンごとにできるため、共用による問題はありません。この機能を「無効」にすると IPtalk の通信は通りますが、同時にソフトウェアによる監視が全ての通信に対して「無効」になるため、セキュリティ上好ましい方法とは言えません。できれば、IPtalk の使うポートの通信だけを通せるよう設定できることが望ましいと考えられます。

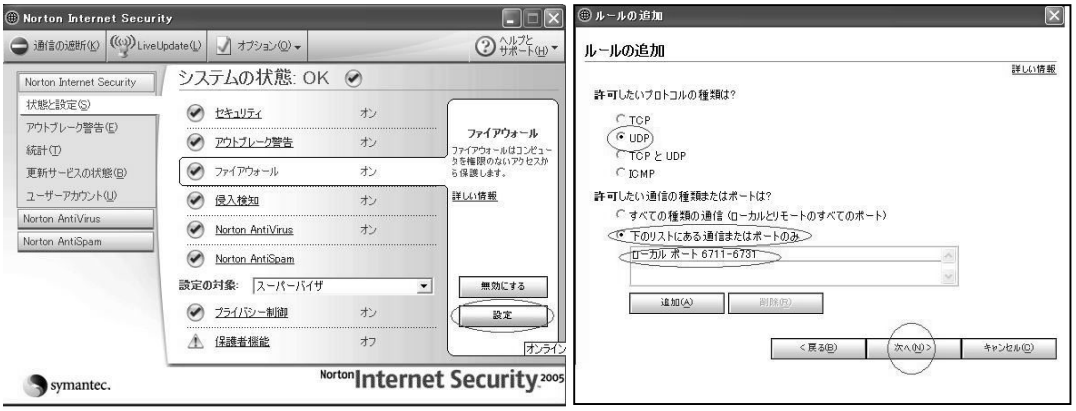
1．ソフトウェアの種類別設定例

ウィルス対策ソフトウェアのパーソナルファイアーウォールにおけるポート開放の例を**図－20～23**に示します。詳細は、それぞれのソフトウェアのマニュアルやヘルプを参照してください。

＜トレンドマイクロ社　ウィルスバスター＞

図－20　ウィルスバスター設定例

＜シマンテック社　ノートン・インターネットセキュリティ＞

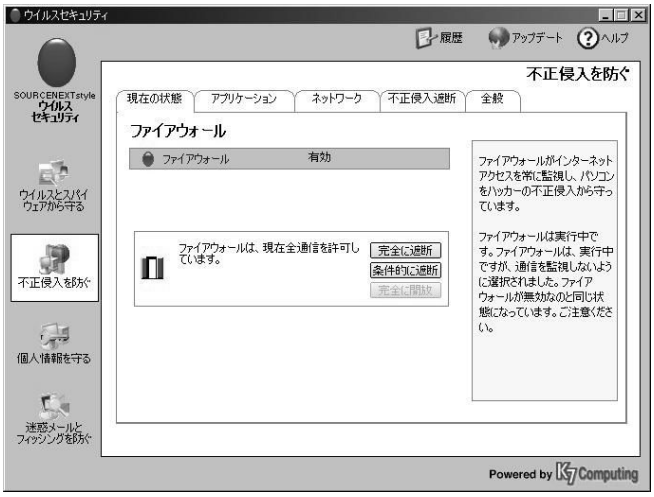


図－21　ノートン・インターネットセキュリティ設定例

＜マカフィー社　パーソナルファイアーウォールプラス＞

図－22　マカフィー・パーソナルファイアーウォールプラスの設定例

＜ソースネクスト社　ウィルスセキュリティ＞



図－23　ウィルスセキュリティの設定画面

２．パーソナルファイアーウォール実験結果

ポート開放が行えた例と、行えなかった例がありました。（**図－24**）

ア）通信チェックがＯＫになった場合

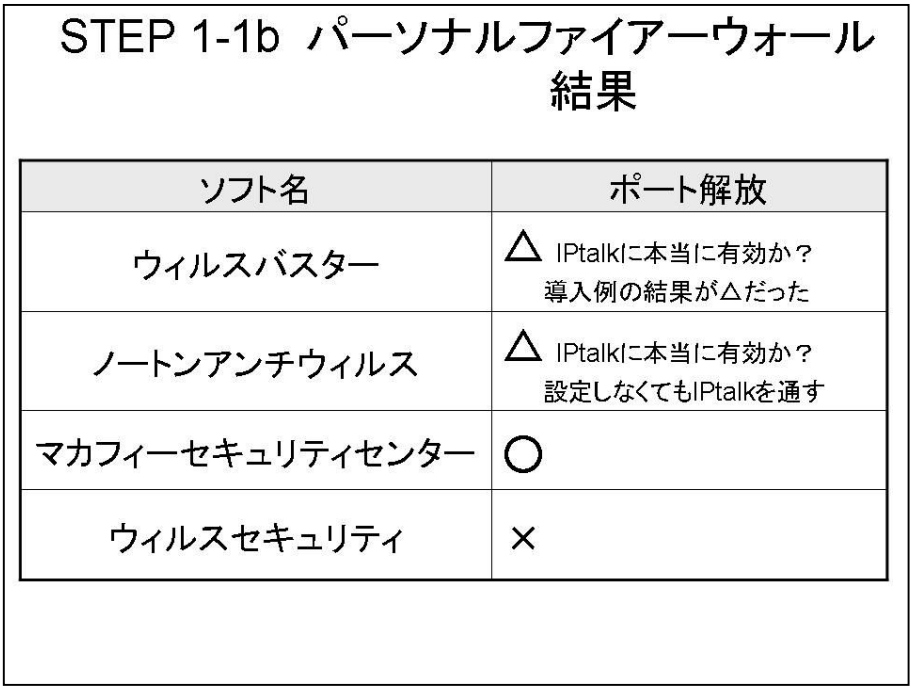
ラルゴ会員の例では、「無効」「完全に開放」としている例が多いです。

マカフィーは、UDP ポート指定で 6711-6731 を開けることが可能です。

ノートンは、ポート開放未設定で有効のままでも、IPtalk を通します。（注１：ただし、これは疑問も残ります）

イ）通信チェックがＯＫではない場合

ルータでのポート開放実験で部分的ＯＫとなった例（ルータ分類Ｃ））で、ウィルスバスターとノートンにはポート開放が設定されていましたが、IPtalk に有効かどうかは確認できていません。



図－24　パーソナルファイアーウォールポート開放実験結果

３．パーソナルファイアーウォールのポート開放についての考察

ウィルス対策ソフトウェアのパーソナルファイアーウォールにも、ポート開放や、ソフトウェアによっては無効にするなどの設定を行う必要がありますが、これはルータと同様に、自らセキュリティホールを開けることです。その危険性を充分に認識し、対策について事前に検討した上で行う必要があります。

３）　ポート開放実験の結論

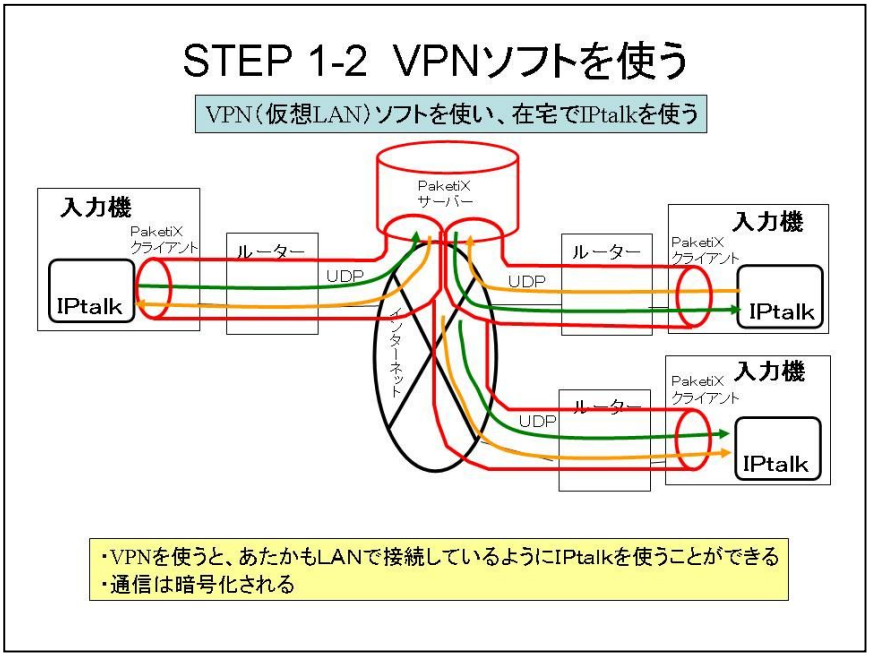
ポート開放を行う方法は、「ルータ」と「ウィルス対策ソフトウェアのパーソナルファイアーウォール」の両方とも開放を完了させる必要があります。開放の手順は、①ルータ、②パーソナルファイアーウォールの順が推奨されます。

一般のサークルで採用する場合、通信環境によりメンバーを限定すれば費用がかからず比較的簡単に実現できる方法と言えるでしょう。

（３）VPN ソフトウェア

VPN（Virtual Private Network）とは、共有ネットワーク上に仮想的なトンネルを造り、プライベートネットワークを構築することやその技術を言います。VPN を構築することで、本来ならインターネットを経由できないプライベートアドレスでの通信や IPtalk で使用するポートでの通信が行えます（**図－25**）。また自動的に暗号化を行うため、盗聴などによる情報漏洩を予防できます。

従来は VPN ルータという機器が用いられてきましたが、扱いにはネットワークの知識が必要であり、異なるメーカー間での通信ができないという問題がありました。そこでラルゴでは、従来ハードウェアで構築されてきた VPN での運用上の問題点と、ルータのポート開放に伴う問題点を、VPN ソフトウェアを用いることで解決しようと試みています。



図－25　VPN ソフトによる IPtalk の通信

1）　VPN ソフトウェアの種類

STEP 2 VPNソフトの種類

	日本語版	FW越え	無償
PacketiX	○	○	△ 一部無償
TinyVPN	○	△ 制約あり	○
OpenVPN	× 英語版	○	○
Hamachi	× 英語版	○	○

図－26　VPN ソフトウェアの種類

現在、VPN ソフトウェアとして代表的なものには、

1）PacketiX（パケティックス）、
2）TinyVPN（タイニーＶＰＮ）、
3）OpenVPN（オープンＶＰＮ）
4）Hamachi（ハマチ）

なとがあります。

調査の結果、3）と 4）は英語版のみの提供、2）はファイアーウォール越えが完全ではないなど一部の機能制約があります。そこで、ラルゴでは 1）の PacketiX を採用しました。（**図－26**）

2）　PacketiX の概要と使い方

PacketiX の概要は、以下の通りです。

・サーバ用ソフトウェアとクライアント用ソフトウェアで構成される
・入力者、利用者が使うのは「クライアント用」
・サーバ用はどこかに 1 つあれば良い
・入力者、利用者は、PacketiX サーバ内の「仮想 HUB」に接続する。

なお、インストール方法は以下の通りです。

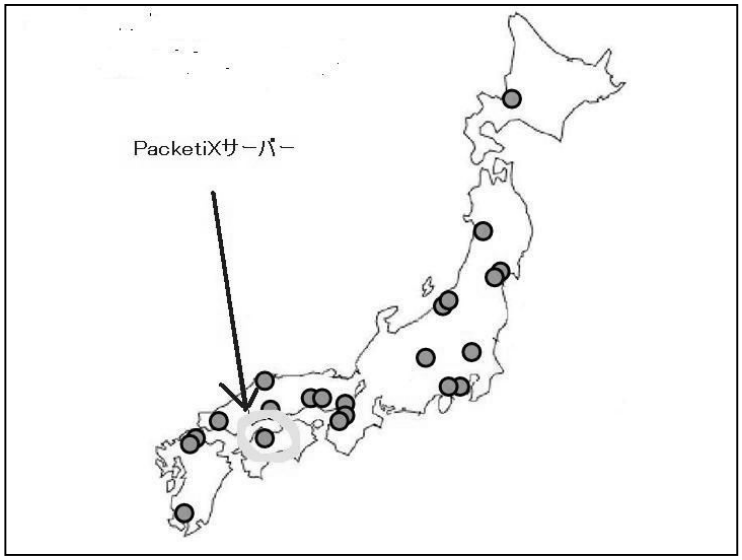
1．ソフトイーサ（株）の Web （http://www.softether.com/jp/download/vpn/）から「PacketiX VPN Client 2.0」をダウンロード

2．インストールする

3．「仮想 HUB」の接続情報を登録する

サーバ用ソフトウェアは多様な OS に対応しており、Windows 2000 Professional や、Windows XP Home Edition などにも対応しているため、サーバ専用機がなくてもシステムを構築できます。

ラルゴでは、現在は、愛媛大学総合情報メディアセンター村田研究室に設置された PacketiX サーバを利用して実験を行っています。（**図－27**）



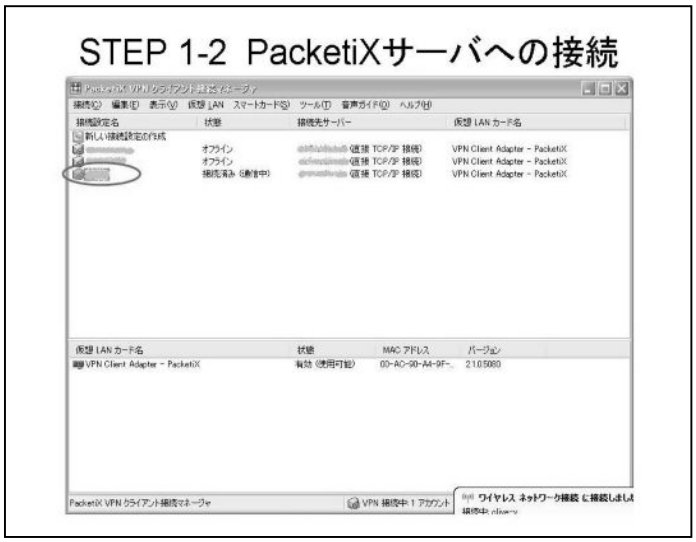
図－27　愛媛大学の PacketiX サーバ

3）　VPN ソフトウェア実験手順

図－28 は、PacketiX などの VPN ソフトウェアを使ってサーバに接続する方法です。

サーバ側にある仮想 HUB は、ソフトウェア上に存在し目に見えないためにこう呼ばれます。機能的には HUB と同じ役割をします。

クライアント側は、接続したい仮想 HUB（名前は自由に設定できます）のグローバルアドレスや ID、パスワードなどの情報を登録し、ダブルクリックすれば、「オフライン」から「接続済み（通信中）」となり、VPN 接続は完了です。



図－28　PacketiX サーバに接続する方法

次に IPtalk を起動すると、IP アドレスを２つ検出したという警告ウィンドウが開きます。これは、実際のネットワークと、VPN と、両方の IP アドレスが検出されるためです。警告ウィンドウを「ＯＫ」して閉じ、パートナーページで赤く光っている IP アドレスの欄で、VPN の IP アドレスを選択します。「パートナーページ」にメンバーが見えれば、通信は成功です。

ラルゴでは、接続テストを試みた８人全員が愛媛大学の PacketiX サーバに接続できました。

４） VPN ソフトウェアを使う方法の結論

PacketiX を用いれば、インターネット接続形態によらず、簡単にインターネットで IPtalk を使うことができます。クライアント側から見れば手軽な方法です。

しかし、サーバ用ソフトウェアの扱いにはネットワークの専門知識が必要であり、技術的ハードルはやや高くなります。また、サーバ用パソコンには固定グローバル IP アドレスが必要なため、管理にもやや費用がかかります。そのため、一般のサークルでの導入や管理は困難と思われます。

＊ PacketiX の有料化について

実験開始当時は個人向けに無償配布されていた PacketiX ですが、2006 年 4 月より販売形態が変わり、サーバ用ソフトウェアは有償になりました。利用者と入力者が使用するクライアント用ソフトウェアは現在も無償で提供されていますが、PacketiX はサーバとクライアントによって構成されているため、クライアント用だけでは使えません。サーバ用ソフトウェアの価格はアクセス数や仮想 HUB 数によって変動します。実際の通訳現場でもよくある入力者４名＋表示機１台＝５クライアントの構成で試算すると、86,000 円です。サークルで練習会などをするために同時アクセス数を増やそうとすると、たとえば 6～10 アクセスの場合は 114,000 円、11～50 アクセスでは 330,000 円です。

PacketiX のライセンスには研究機関向けの無償版（Academic Edition）があり、愛媛大学村田研究室はそれを使用しています。ラルゴは村田研究室と共同研究を行っているため、村田研究室の PacketiX サーバを利用させていただいています。

他のサークルについても、大学等の研究機関と共同研究をするか、または多少の不便さをクリアして無償の VPN ソフトウェアを使うか、どちらかの方法で VPN の導入は可能と考えます。

（４）STEP １「インターネットで IPtalk を使う方法の検討」の結論

インターネットで IPtalk を使う方法について、ポート開放と VPN ソフトウェアの PacketiX を試しました。

費用的な面では、「ポート開放」がよく、サークルでも導入しやすいと思います。しかし、家庭のインターネット環境によってはポート開放ができない場合もあると思います。汎用性では「PacketiX」が優れていますが、技術的にハードルが高くなります。一長一短で、どちらが良いとは言い切れません。

2 STEP 2 「インターネットを使って動画や音声を送受信する方法の検討」

通訳の情報源としてインターネットを介して遠隔地で音声や動画像を視聴する際の必要な要件としては、以下が挙げられると考えます。

ア）充分な音質・画質
イ）複数に同時に配信（タイムラグがない）
ウ）守秘義務への対応（暗号化、盗聴予防）
エ）特殊な機材を必要としない

ラルゴでは、（１）「音声のみ」を送る方法と（２）「音声と動画」を送る方法について検討しました。

（１）音声のみ送る方法の検討

図－29 は音声送信の代表的な無料ソフトウェアを比較した表です。

ソフト名	ルータの設定	音質	暗号化
ネットミーティング	必要な場合もあり	△	×
Windows メッセンジャー	必要な場合もあり	△	×
Yahoo! メッセンジャー	なし	△	×
Skype	なし	◎	○

図－29　音声チャットサービス比較[10]

通訳を行うために充分な音質と、著作権、守秘義務等の観点から、暗号化によるセキュリティを重視し、ラルゴでは、「Skype」（**図－30, 31**）を採用することとしました。

他のソフトウェアは音声がぶつぶつ途切れて聞き取りにくく、音質も不明瞭で、片方向の会話しかできませんでした。Skype は双方向の会話で５人までの会議通話機能があり、複数同時配信の要件も満たしています。

なお、話者の音声を送信用パソコンまで送る方法は、携帯性や汎用性を重視し、会場などの設備とは別に情報保障用のマイクを用意することとしました。話者から送信用パソコンまでの現実的な距離や電波法による連続通話制限などを考慮し、ワイヤレスガイドシステム（ワイヤレス PA システム）とピンマイクを採用しています。費用は、一式で約８万円です。

図－30　Skype 操作手順[11]

図－31 Skype

（２）音声と動画を送る方法の検討

情報保障現場においては、入力者にとっては音声情報が主です。しかし、PowerPoint のスライド、板書、講師の動き、参加者や受講者（フロア）からの発言など、時に補助的に視覚情報が必要な場合があります。現場での入力中に視線をパソコンのディスプレイから外してでも音源を見るという経験は誰にもあることでしょう。在宅入力による情報保障でも、音声だけでなく、視覚情報も得られることが望ましい状況があると考えられます。

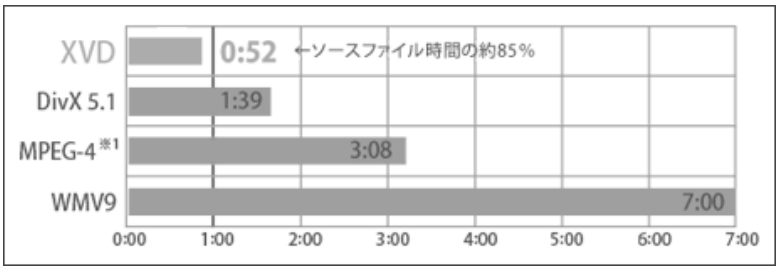
インターネットで動画を送信する方法としては、近年 Web カメラの普及が著しい状況です。Web カメラは画質も向上し、パソコンに USB で接続して手軽に使えます。価格も 2,000 円を切るものもあり、身近になっています。上述の音声送信ソフトウェアを併用すれば、音声との同時送信も可能ですし、音

声と動画が統合化されたものもあります。複数の人と簡易テレビ会議ができるものもあります。

しかし、Web カメラは元々個人の通信用で、パソコンの前の人の映像の送信に特化してあり、視界も狭く、ズーム機能もありません。そのため、主に入力者への視覚情報提供用として用いるには不充分と考えられます。また、テレビ会議システム（**図－6**）は高画質の撮影と動画像配信ができますが、数十万円と高価なため、サークルでの導入には適さないと考えられます。そこで、ラルゴでは、画質や機能で優れている家庭用ビデオカメラで動画撮影をしています。

動画像配信の方法には、他にストリーミングがあります。インターネットで映像を見る場合などに用いられる技術で、企業ホームページでの商品ＣM映像配信やアーティストのコンサートのインターネットライブ中継など、ブロードバンドの普及を背景に様々な分野に拡大しています。

ストリーミング技術は、ストリーミング対応のデータを作成（エンコード）するエンコーダ、配信を行なう配信サーバ、受信し再生を行なうプレイヤーの 3 点で構成されます。エンコードしたデータを一度ファイルに保存してから配信サーバで配信する方法を「オンデマンド配信」、エンコードと配信を並列して行ないリアルタイムの配信を行なう方法を「ライブ配信」と呼びます。情報保障では「ライブ配信」を活用します。Web でのライブ配信も増加しており身近な技術になってきました。Windows Media エンコーダなど、無償のエンコーダもありますが、情報保障で活用する際にはエンコードの速度が最優先事項と考えます。



図－32　エンコード速度比較（ビットレート 1000Kbps）[12]

XVD 方式は、1Mpbs という大容量のデータでも 1 秒以内にエンコードが完了します（**図－32**）。情報保障現場では１秒の遅延も惜しまれますが、他の方式に比較すると最も高速です。また、圧縮率が高いので低ビットレートで高画質の配信ができ、低速回線の利用者も充分な画質を得られやすくなります。他の方式と異なり、再生のための専用プレイヤーソフトを必要とせず、Web ブラウザ（Internet Explorer）上で見ることができます。

ストリーミングには企業のレンタルサーバサービスを利用する方法もありますが、月または週単位で課金され、１ヶ月あたり約 7 万円～10 万円、１年あたり約 84 万円～120 万円必要になり、サークルでの導入は困難です（**図－33**）。XVD 方式の専用機器 CamCast SX(同時４アクセスまで可)はエンコーダとサーバを兼ねています。価格は約 16 万円ですが、ランニングコストは不要なため、サークルでの導入も不可能ではない価格と思われます。また、123×79×26mm、210g と小型で携帯性に優れています。（**図－34, 35**）

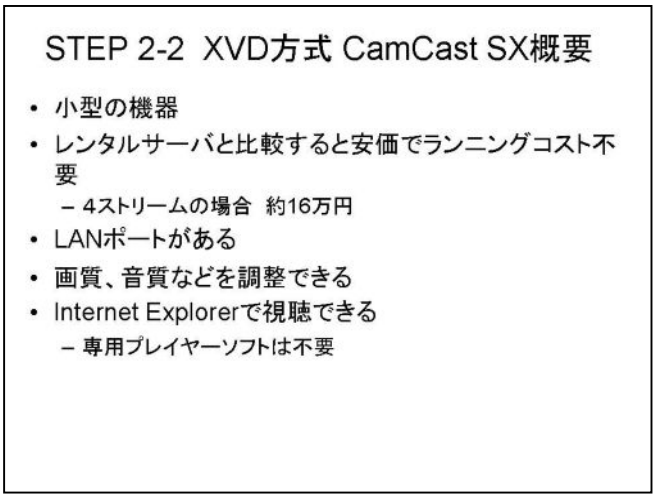
	単位	価　格(円)	備　考
So-net	回	200,000	ライブエンコード料、サーバ利用料。撮影費別
DIGITAL STUDIO	月	105,000	
HALSC.com	週	15,750	

図－33　レンタルサーバ使用料の例

ストリーミングの利点として、ユーザーのパソコンに動画像ファイルが保存できないという点が挙げられます。遠隔地からの入力であっても守秘義務を伴う通訳であることに変わりはありません。通訳現場の映像や音声が機能的に残らない（残せない）ことは重要な要件と考えられます。

以上の点から、ラルゴでは、音声と動画を送る方法として、XVD 方式の CamCast を選択しました。

図－34　CamCast SX



図－35　CamCast SX の概要

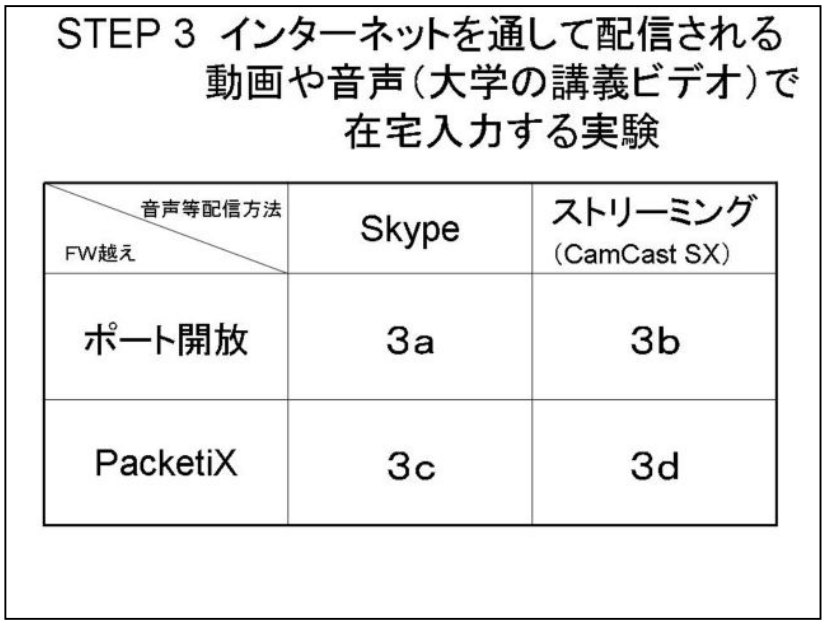
（３）STEP 2 の結論

音声のみ送信する場合は Skype、音声と動画を送信する場合はストリーミングが適していると考えられます。ストリーミングでは、エンコード速度が速く、小型で比較的安価な CamCast が優れています。

3　STEP 3　インターネットを通して配信される動画や音声（大学の講義ビデオ）で在宅入力する実験

（１）実験概要

愛媛大に設置した CamCast に、DVD の映像を流し、全国のメンバーが視聴して、評点をつけました。



図－36　STEP 3 実験方法

また、一部の実験では、入力中に愛媛大から各入力者端末に ping を継続的に送り、愛媛大から各端末との間の通信的距離を計測し、入力文字数との関連を解析しました。

実験の方法としては、STEP 1 の結果と STEP 2 の結果を組み合わせた４通りが考えられます。（**図－36**）

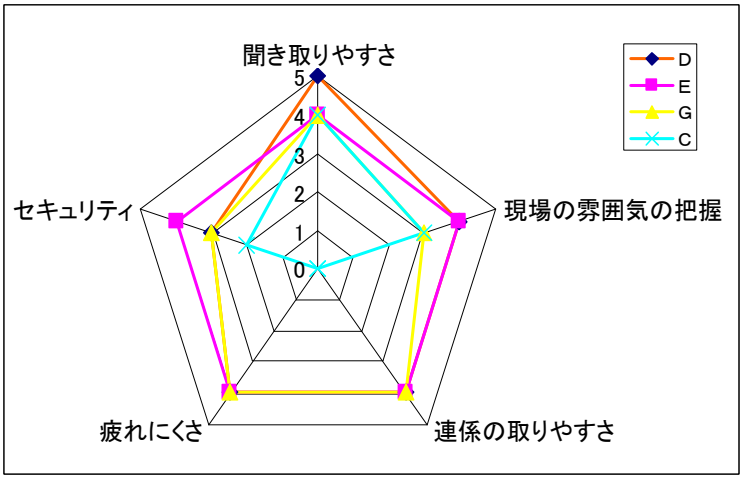
なお、2006 年 6 月 11 日に全要研集会第３分科会で行ったデモンストレーションは、方法ｄ（**図－36** の「3d」）です。

（ａ）ポート開放＋Skype 実験

【ルータのポート開放による入力テスト報告（2006/5/27）】

日　時：2006 年 5 月 27 日(土) 21 時～22 時 50 分
参加者：４名
場　所：Yahoo!メッセンジャーのカンファレンスおよび Skype の会議通話
内　容：
・ルータのポート開放による IPtalk での入力
・１名が仮想話者となり、Skype 会議通話上で話す音声の入力
・ポート開放での接続テストが確認できた、２名で連係入力

以下の現象が報告されたが入力には影響は少なかった。
・音声が波打つように聞こえることあり。
・入力者２名に同時に波打つ現象が起きる。
・音声が途切れることもあった。これも２名同時。



図－37　ポート開放＋Skype 入力者評点

＜入力者評価＞

- 音質はとてもクリア
- 音声が波打って聞こえることがあった
- 波打ち現象はパートナーに同時に起きる
- 細かく音飛びすることがある
- 話し声のみよく通るので、かえって周りの雰囲気が分かりにくい
- 周りの音までいろいろ拾う
- エコーバックが起きることもある

＜ポート開放＋Skype 実験結論＞

この方法は情報保障に実用可能と評価できる。（**図－37**）

（註：レーダーチャートの水色（入力者Ｃ）は入力しなかったため一部評価無しの項目があります。）

（ｂ）ポート開放＋ストリーミング

CamCast に固定のグローバルアドレスが必要になるため、実験は行えていません。

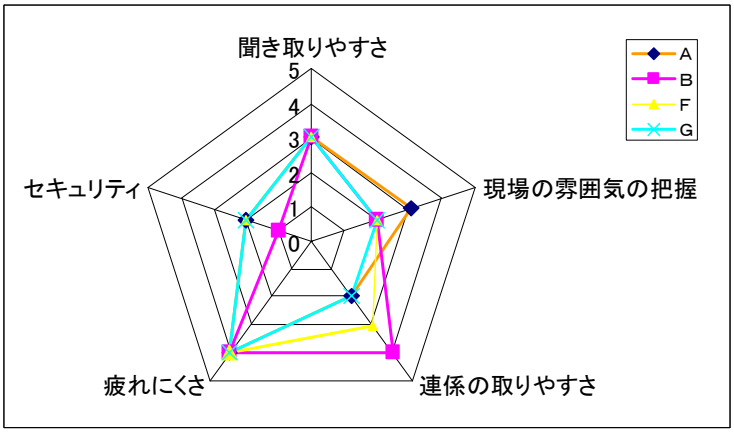
（ｃ）PacketiX＋Skype 実験

＜実験手順＞（以下は、実験参加者に伝えた手順です。）

Skype は ver.2 の正式版がリリースされています。
http://www.skype.com/intl/ja/
１．スカイプ名の連絡
皆さんのスカイプ名を交換して、コンタクトリストに登録しておきます。
当日の話し合いや打合せもスカイプの文字チャット機能でできます。
２．ヘッドセットの準備
入力者は必ず用意をします。事前に通信テストを行うため、マイク付きのヘッドセットが望ましいです。
（入力中はマイクは不要なので、プラグを抜くか、マイクスイッチを切ります）
３．入力準備
Skype の同時通話は５人までです。
２人入力を行うためには、ペアずつに分けて、途中ペアの交代を行いながら入力します。
４．時計合わせ
５．PacketiX の「接続」
仮想 HUB「○○○」を使用しますので「接続」します。
６．IPtalk
A 班に入って待機してください。
テストの際には、A 班、B 班を使用します。
見学は可能ですが、入力班以外の方は入力をお控えください。
実験後、IPtalk の各データを保存します。

＜実験結果＞

4/15 Skype での入力テストの報告です。
【参加者】
５名
【内　容】
Skype の会議通話を使い、愛媛大学からの DVD（模擬講義）音声（映像なし）で
２人入力を２セット（5 分ずつ）行った。
連絡、打合せ等は、Skype のグループチャットで行った。



図－38　PacketiX＋Skype 入力者評点

＜入力者評価＞

- 音声がパートナーより遅れて入力しにくいことがあった
- 音声に強弱の波があることがある
- 映像がある方が現場の雰囲気が分かり、入力しやすい
- 簡単に IPtalk で接続できるのが良い

＜PacketiX＋Skype 実験の結論＞

この方法は情報保障に実用可能と評価できる。

（ｄ）PacketiX＋CamCast

この実験は、予備実験と本実験を各１回、以下の日程で行いました。

＜予備実験＞

【日 時】2006 年 2 月 4 日(土) 21:00～24:30
【内 容】21:00～21:30 PacketiX、ストリーミング、IPtalk の接続確認
21:30～22:00 愛媛大より実験についての説明
22:00～22:30 設定等の確認、ペア組調整等打合せ
22:40～22:50 １人打ち（講義ビデオ）
23:00～23:20 ２人打ち（講義ビデオ 続き）
23:20～24:30 インタビュー、ディスカッション
＜ラルゴ＞
愛媛大 CamCast のストリーミング受信による１人入力および２人入力
IP アドレス、IPtalk の「入力の記録」等のデータ保存
上記情報の愛媛大への提供
感想など、簡単なインタビュー（入力後）
＜愛媛大 村田研＞
実験目的、手順の説明
各在宅端末と愛媛大サーバ間の通信所要時間の計測
通信ログの取得、分析
【参加者】６名

【見学者】４名

【結 果】
大きな問題なく、在宅入力を行うことができた。

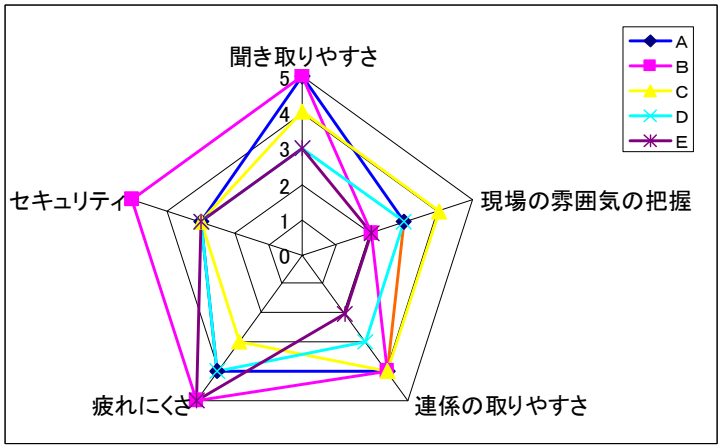
＜本実験＞

【日 時】2006 年 2 月 8 日(水) 21:00～24:30
【内 容】模擬講義ビデオを 5 分を１セットとし、１人打ち、２人打ちによる入力を 3 セットずつ行った。
21:00～21:45 準備、設定確認、ペア決め、手順説明
21:50～21:05 １人打ち １回目
22:01～22:06 １人打ち ２回目
22:10～22:15 １人打ち ３回目
22:24～22:29 ２人打ち １回目
22:45～22:50 ２人打ち ２回目
22:25～23:00 ２人打ち ３回目
23:05～23:10 ２人打ち １回目(Ｂペアのみ再入力)
23:10～23:30 インタビュー

23:30～24:30 ディスカッション

＜ラルゴ＞
愛媛大 CamCast のストリーミング受信による１人入力および２人入力
IP アドレス、IPtalk の「入力の記録」等のデータ保存
上記情報の愛媛大への提供
感想など、簡単なインタビュー（入力後）
＜愛媛大 村田研＞
実験目的、手順の説明
各在宅端末と愛媛大サーバ間の通信所要時間の計測
通信ログの取得、分析
【参加者】６名
【見学者】４名
＜愛媛大＞４名(１名は、毎日新聞記者)

＜本実験結果＞
・Ｂチームのみ再入力
見学者がストリーミングサーバに接続したため､B チームの入力者１名がストリーミング視聴不可(サーバーオーバーローデッド)になったため、終了後、そのパートの再入力を行いました。
・遅延、パケットロス
パートナー間で情報の受け取るタイミングが違うとの報告がありました。また、音声が止まるなどのパケットロスと思われる報告がありました。遅延は各自(各チーム)によりばらつきがあるようです。**(図－40, 41)**



図－39　PacketiX＋CamCast 入力者評点

＜入力者評価＞
- モニター窓の文字表示がゆっくり見えることがあった
- パートナーに情報が届くのが遅れることがある
- 音がぶつぶつ途切れる
- 自宅で入力できるのでリラックスできて疲れにくい
- 板書が見えて良かった
- アクセス数を超えると入力者が落ちてしまうので注意が必要

＜本実験考察＞
ア）引っかかり
　ストリーミングの引っかかり報告（パケットロスによりバッファリングがかかるため、3～5 秒映像が止まる現象）が全員から寄せられました。現象の起きるタイミングは全員ほぼ一致していると思われますが、頻度は個人差がありました。たとえば、ストリーミングで連係入力をしている際、自分は引っか

かっていて音が聞こえない時にも他のメンバーは入力ができているという現象の報告がありました。

実験に参加したメンバーは全てブロードバンドの利用者であり、実験時の実測速度は、2.1Mbps～8.5Mbps でした。ストリーミングの映像は 400kbps、音声は 64kbps で配信されており、全員充分な帯域があったと思われますが、引っかかりの起きた原因については、送信側、受信側のどちらに問題があったかも含めて不明です。ストーミングの映像、音声のパラメータを下げれば、引っかかりも減少するという相関関係はあるようです。

イ）IPtalk の引っかかり

モニタ部が入力途中で止まっているように見えていても、数秒後に一気に文字がたくさん(不自然な量)表れる現象が報告されました。通信が途切れた間に溜まっていた受信文が、一度に押し出されるように表示されているように見えます。これを「IPtalk の引っかかり」と仮に呼んでいます。

ストリーミングの引っかかりと同期して、この IPtalk の引っかかりも起こることがありました。ストリーミングのみ引っかかり、IPtalk が通る時もありましたが、逆パターンの報告はありません。パートナーや同じ班のメンバーが引っかかっているかどうかは、他のメンバーからは全く把握できません。

ウ）その他

Internet Explorer で、初めてストリーミングサーバの URL にアクセスする時、自動的に ActiveX コントロールがインストールされます。その他は何も設定の必要がなく、インターネット・エクスプローラ上で他のソフトウェアを併用することなくストリーミングを視聴できます。 この ActiveX コントロールが Internet Explorer のみの対応であるため、他のブラウザ（FireFox、Opera など）では CamCast によるストリーミングを利用できません。しかし、Windows PC の場合は Internet Explorer が標準添付されているため、利用者や入力者が制限されるような深刻な問題ではないと考えます。

また、入力者はディスプレイの狭い面積にストリーミングの画面と IPtalk の画面を配置しなければなりません。これについては、最適な配置を工夫することによって、より利用しやすい画面構成を提案できると考えます。（**図－45**）

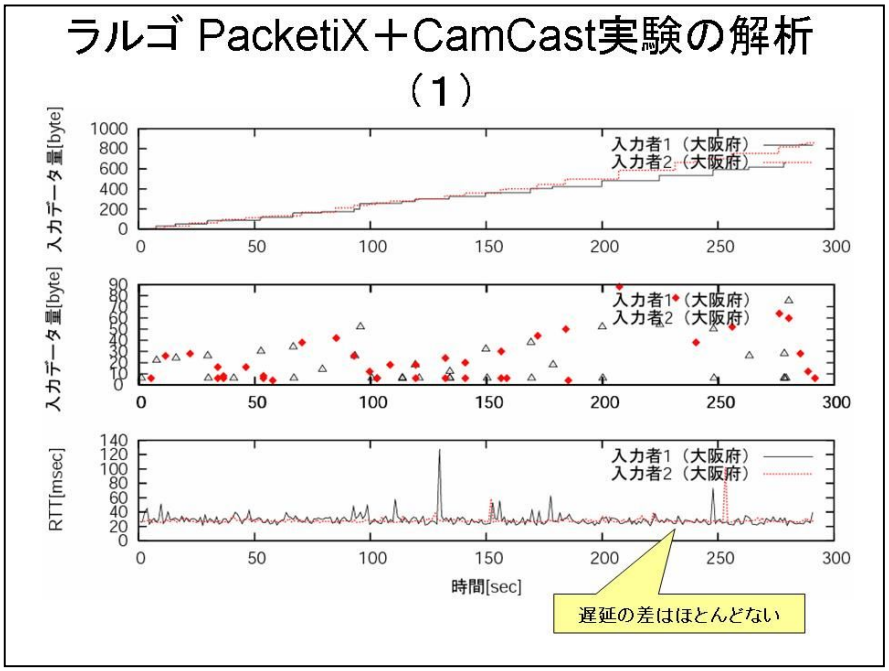
エ）IPtalk 遅延計測機能追加

IPtalk は、この結果から次の機能を追加しました。

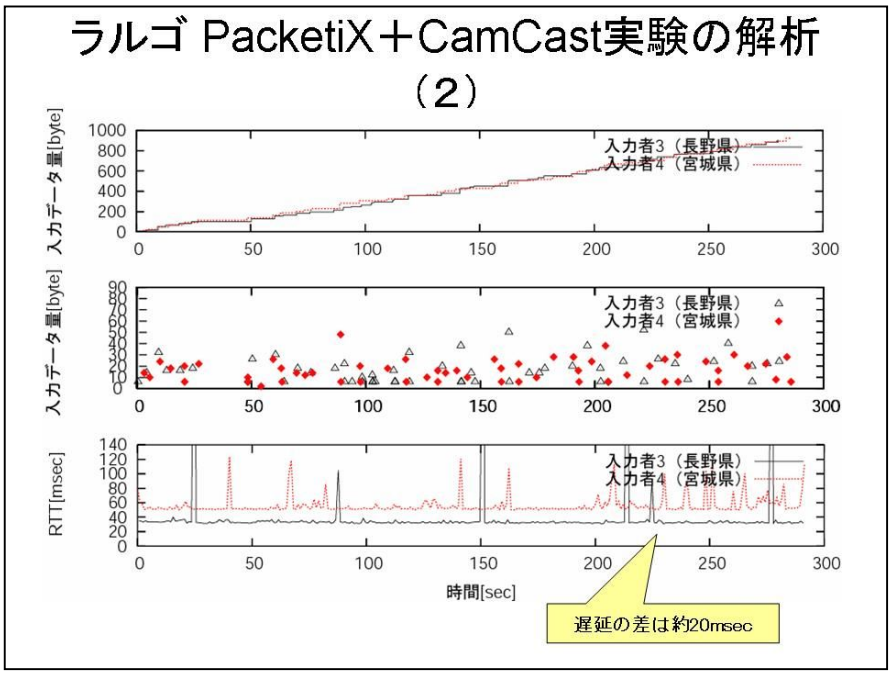
＜０６０２２６／ＩＰｔａｌｋ９ｉ９１＞
１）「インターネットウィンド」に「ネットワーク遅延の計測」を追加した。
「遅延を計測し表示する」のチェックを入れると５秒おきに、「遅延を計測する対象」との間の通信時間を計測し、入力班の全員の８人モニターに送信する。

オ）愛媛大学によるデータ解析結果[13][14]

ペアごとに遅延の差が計測され、第７章の基礎実験で述べる遅延の入力への影響が確認されました。



図－40　PacketiX＋CamCast 実験解析結果（１）



図－41　PacketiX＋CamCast 実験解析結果（２）

＜PacketiX＋CamCast 実験の結論＞

この方法は情報保障に実用可能と評価できる。（**図－46**）

（２）STEP３　考察

IPtalk の使用感では、ポート開放で「インターネットウィンド」を使う方法より PacketiX を使用する方法が簡単で違和感なく使えます。

情報源としては、Skype、CamCast とも品質は充分ですが、ネットワーク遅延の影響を受けることが

あります。特に CamCast では動画像と音声を配信するため広帯域を必要とするため遅延が起こりやすく、Skype より不安定と言えるでしょう。また、利用者や入力者同士のコミュニケーションをサポートできる双方向性において Skype は優れており、補助情報として動画像が得られることにおいては CamCast にアドバンテージがあると言えるでしょう。

4 STEP 4　模擬講義をインターネットで情報保障する実証実験

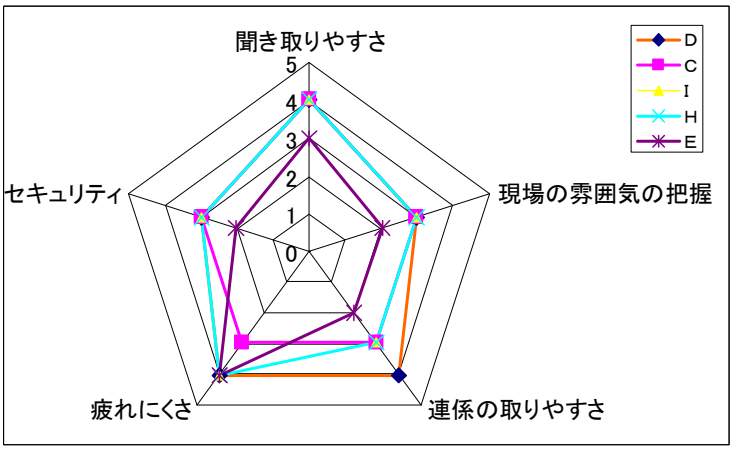
（1）実験内容

全要研集会第三分科会でのデモンストレーションと同じ機器を用いて本番に近い環境を作り、セッティング、入力、発表のリハーサルを兼ねて実験、検討を行いました。

IPtalk の接続は PacketiX、情報配信は CamCast によるストリーミング（方法ｄ）を用いました。

（2）実験結果

トラブルの際の連絡方法を事前に決める必要があることや、入力中にインターネットから落ちた時の連絡法、極端なネットワーク遅延が発生した時のリカバー法などの運用上の検討課題を確認しました（**図－47**）。今後も実験を継続し、事例を収集しなければ結論は得られないと考えます。



図－42　講義保障テスト　入力者評点

＜入力者評価＞

- 時々音がぶちぶち途切れた
- 雑音が入り聞きづらい時があった
- 映像が、後半ぼやけたように思う
- パートナーより遅れて情報が届くと、結果的に１人入力になる
- トラブルの際の連絡方法を事前に決める必要がある
  - ➢ インターネットから落ちたら連絡方法はどうするか

5 実験のまとめ

一連の実験の結果から、一般のサークルがインターネットを使った在宅入力情報保障を行うのに最適な方法は、以下のように言えます。

1）費用と性能の両方を同時に満たす方法は、今回、見つけることはできなかった。

2）費用的な面からは、「ポート開放」＋Skype が推奨できる。

3）性能的には、「PacketiX」＋「CamCast」が推奨できる。

4）導入の技術的な難易度の観点から見ると、一般のサークルには、「PacketiX」＋「CamCast」はハードルが高すぎると思われる。

したがって、現状で一般のサークルが導入する方法としては、「ポート開放」＋Skype となります。ただし、インターネット環境によっては、「ポート開放」ができない場合があります。
また、一般のサークルに技術的支援（設備も）をするＮＰＯなどの団体があれば、性能的に優位な「PacketiX」＋「CamCast」が、費用対性能からも推奨できるでしょう。

第５章　利用者の「どこでも」は？

本稿では、主に入力者の視点から実験・検証を行ってきました。利用者が情報保障を必要とする時は、自宅や職場など一定のネットワーク環境にいるとは限らないため、この結果は利用者が「どこでも」情報保障を利用する際にも適用できます。

利用者が「在宅入力による『どこでも情報保障』」を利用する場合、以下の環境であれば可能と言えます。

１）インターネットが利用できる施設 ⇒ PacketiX＋Skype
２）ネットワーク管理者の協力を得て、ポート開放できる ⇒ ポート開放＋Skype
３）携帯電話などの移動体通信によって、自分でインターネット接続する
　⇒ Skype（ポート開放不要）、PacketiX＋Skype

３）の場合は、144kbps の携帯電話や PHS では Skype の利用は帯域不足のため不可能です。最近は 2Mbps など携帯電話による通信が高速化しています。こうした高速タイプの携帯通信カードなどを利用すれば、音声送信にも充分利用可能です。

１）、２）については、施設の回線がブロードバンドであれば、CamCast による映像も配信可能です。

今回提案した方法では、入力者は現場に同席しないため、利用者が音声や動画を配信するためのセッティングを行います。従来にはなかった、入力者と利用者が共同作業により情報保障を行うシステムです。情報保障を利用する側だった聴覚障害者も、この方法で配信を担当することにより、自らの情報保障に積極的に参画できます。そのため、現場で単独で短時間にセッティングできるように、システムの簡素化、軽量化、手順の簡略化、マニュアル化が求められます。

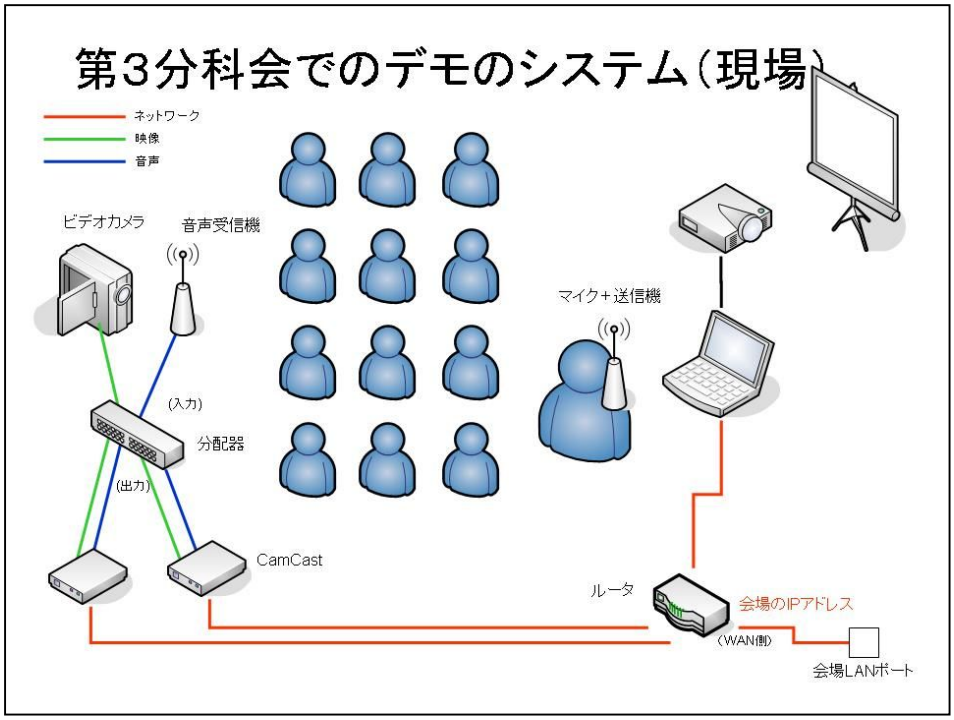
第６章
第 24 回全要研集会第三分科会でのデモンストレーションのシステム

分科会会場のシステム構成を**図－43** に示します。IPtalk の接続は PacketiX による VPN、音声と動画配信は CamCast によるストリーミング（方法ｄ）で行いました。入力は、宮城、新潟、長野、神奈川、大阪、兵庫在住のラルゴ会員が各自の自宅から行いました（**図－44**）。入力者のディスプレイの表示状態の例を**図－45** に示します。ストリーミングの映像はキャプチャできないため、表示領域を加筆し

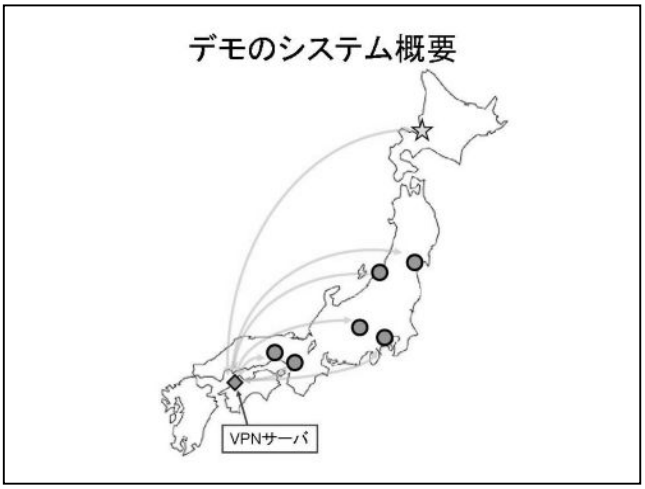
ています。このデモでは入力者が６名であったため、CamCast を２台用意しました。また、会場中央のデモ用スクリーンには、在宅入力による IPtalk の字幕と、ストリーミングの映像を投影しました。

一般的な、入力者４名で行われる情報保障現場に置き換えると、利用者側には映像は不要と思われるため、ストリーミングは入力者４名が見られれば良く、CamCast は１台のみで充分です。それに伴い、分配器とルータも不要となるため、さらにシンプルな構成になります。

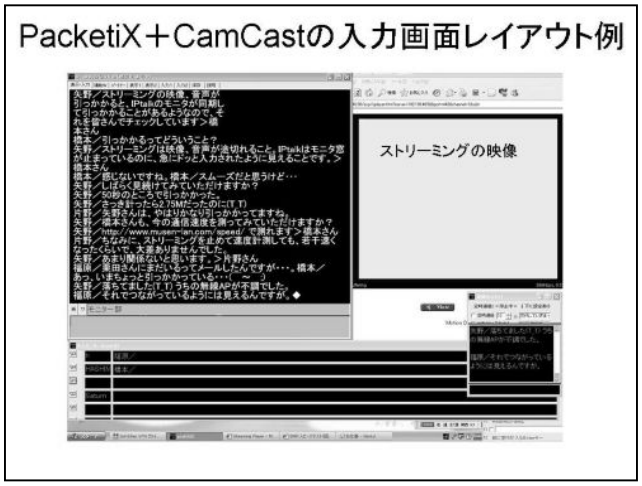
会場では最後部より撮影したため、ビデオカメラは 1.4mの三脚を使用して設置しましたが、利用者が前方の席で撮影を行う場合、30ｃｍ程度の小型三脚を用いれば、より省スペースでの設置が行えます。



図－43　全要研集会第３分科会でのデモンストレーションシステム構



図－44　デモのシステム概要



図－45　PacketiX＋CamCast の入力画面レイアウト例

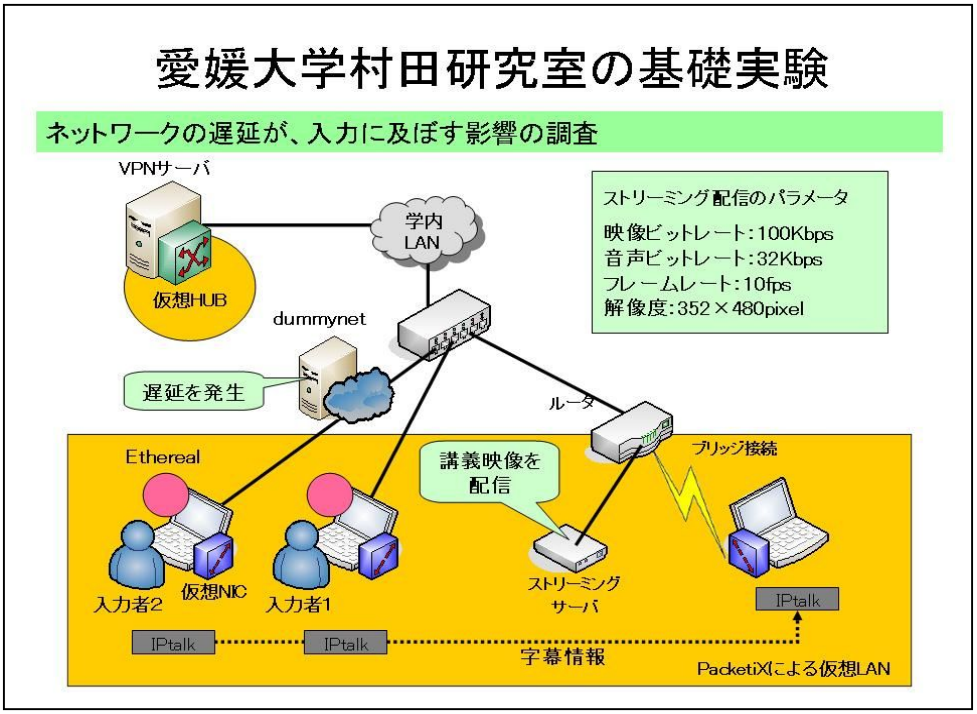
第７章　愛媛大学村田研究室の基礎実験

（１）実験概要

愛媛大学村田研究室では、インターネットによる遅延が入力に与える影響を調べるため、基礎実験を行いました。この研究の報告は、2006 年 1 月に電子情報通信学会福祉情報工学研究会[13]、2006 年 3 月に愛媛大学工学部情報工学科卒業論文[14]で発表されています。

インターネットでの通信は、ルーティング（通信経路）やトラフィック（混雑状態）により状態は一定ではありません。距離的に近くても、インターネットを介する場合はプロバイダによっては経由する中継点も異なり、数百ミリ秒単位の遅延が発生する可能性があります。

基礎実験では、LAN 内に機械的に遅延を発生させる「遅延ボックス」を用いた疑似インターネット環境を構築しました。室内に入力者２名が待機し、模擬講義を録画した DVD をストリーミング（動画配信）で視聴しながら入力をします。そのうち１名にのみ人為的にネットワーク遅延を与え、そのパラメータ（秒数）を変更することで遅延が入力に及ぼす影響を調べました。この実験のシステム構成図を**図－46** に示します。

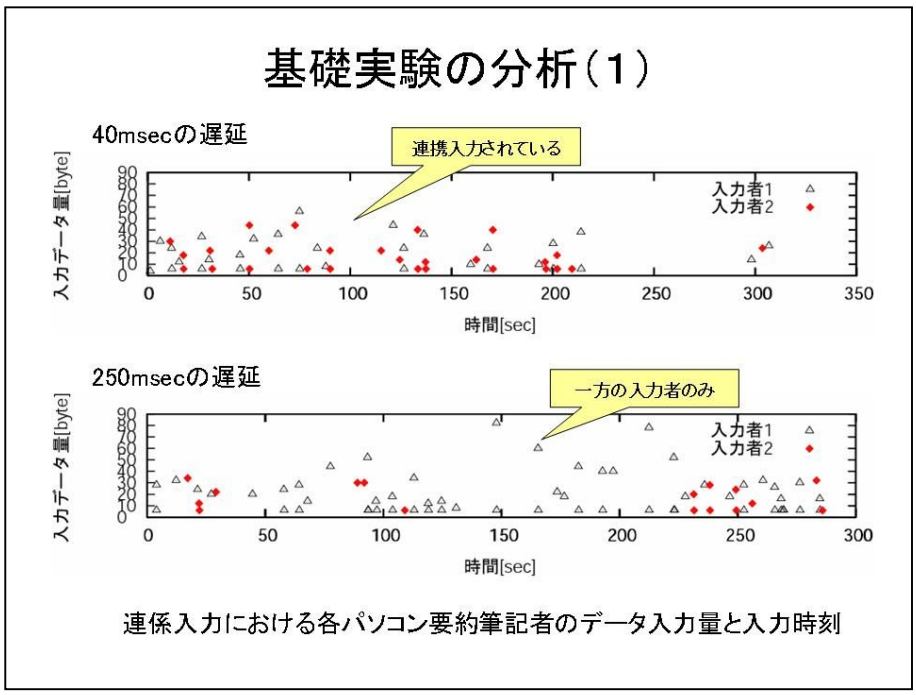


図－46　愛媛大学村田研による基礎実験システム構成図[13][14]

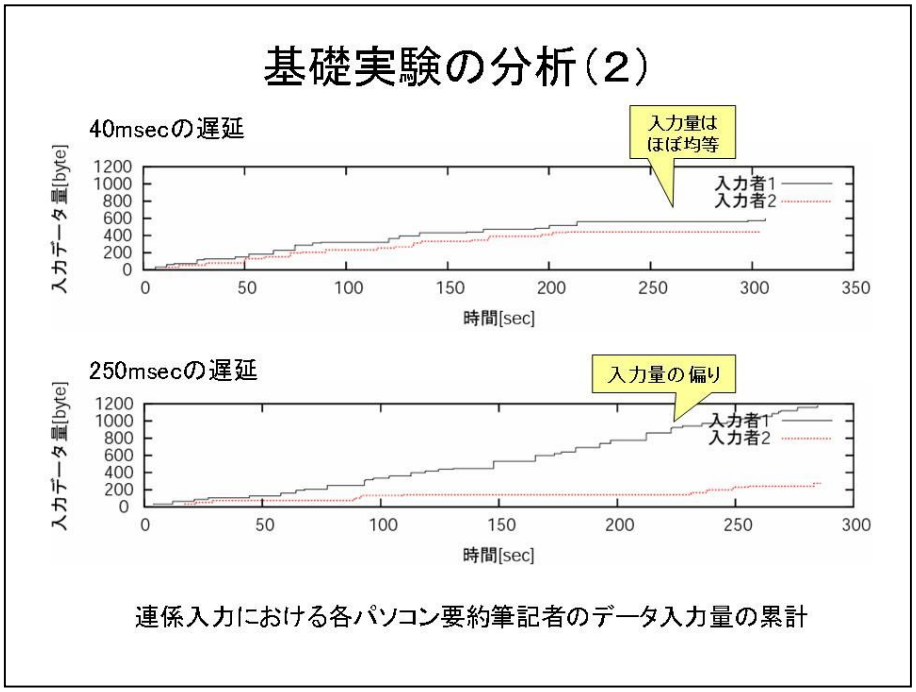
（２）実験結果

入力者２の遅延が 40msec（ミリ秒）の場合、入力者１との連係入力はスムーズに行われ、遅延の影響はほとんど見られませんでした。

入力者２の遅延が 250msec の場合は、入力者２の映像が頻繁に停止し、同時に音声と IPtalk の通信も中断します。入力者２の映像が再開して聞こえてくる音声は、既に入力者１が入力済みで表示部に表れています。入力者２が情報源となる音声と映像の情報を得るタイミングが入力者１より遅れるため、両者の情報取得の同期が取れなくなります。このため、連係入力を行うことが困難となり、遅延のない入力者１が、ほぼ１人入力する状態になりました。（**図－47, 48**）



図－47　基礎実験分析結果（１）



図－48　基礎実験分析結果（２）

（３）基礎実験の考察

インターネットを介して連係入力を行う場合、ネットワークの状態により遅延が起き、パートナーとの情報取得の同期が取れません。こうした状況が起きることを事前に知識としておくことで、在宅入力時の遅延にも冷静に対応できるでしょう。

また、現段階ではパートナー同士の遅延状況を把握することが困難です。お互いに遅延の状況を通知し合う方法や仕組みの開発が望まれます。

第８章　今後の課題

（１）入力者の技術的課題

入力者は、普段の現場では会場の一角に集まって入力を行っており、パートナーの顔が見えず声も聞こえないという状況での連係入力には不慣れです。連係入力は、パートナーが同時に情報を得られることを前提として発展してきた技術です。インターネットの遅延の状態は流動的であるため、パートナーと情報を得るタイミングについて同期の保証がありません。

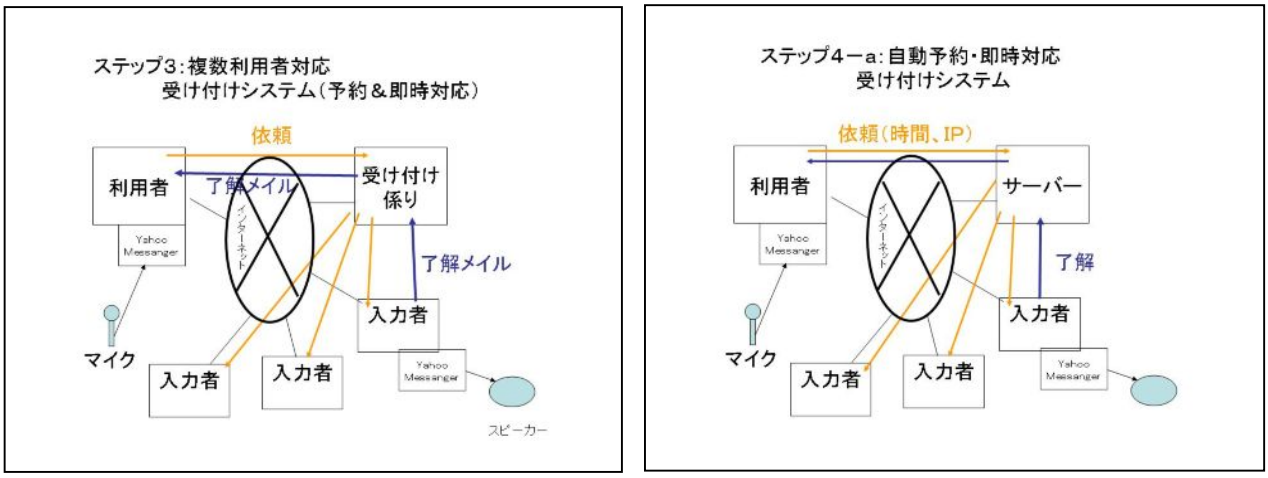
IPtalk に機能が追加され、互いの通信的な距離を把握することはできるようになりました。しかし、「どちらが遅れているのか」は一定ではないため、入力しながら判断しなければなりません。

パートナーに遅延が生じた時、連係入力の比率を変化させたり、急遽単独入力に切り替えたりする対応が必要になります。そのため、パートナー同士のより息の合ったコンビネーションや、要約率を自在に変化させる技術が必要になります。

（２）コーディネート方法の検討

在宅入力による遠隔通訳を運用する際には、メールや電話などによる直接の依頼に加え、Web による募集やエントリー、マッチングなど、インターネットを活用した方法が取り入れられることにより、時間的制約が解消でき、利用者と入力者、双方の利便性が向上することが期待されます。（**図－49**）

また、利用者、入力者、コーディネーターそれぞれが地理的に離れているため、トラブルへの対応が困難であったり、遅れたりすることが考えられます。実用化前に遠隔地からのトラブルシュートの方法を検討し、確立する必要があるでしょう。



図－49　Web による 24 時間自動受付システム（構想）

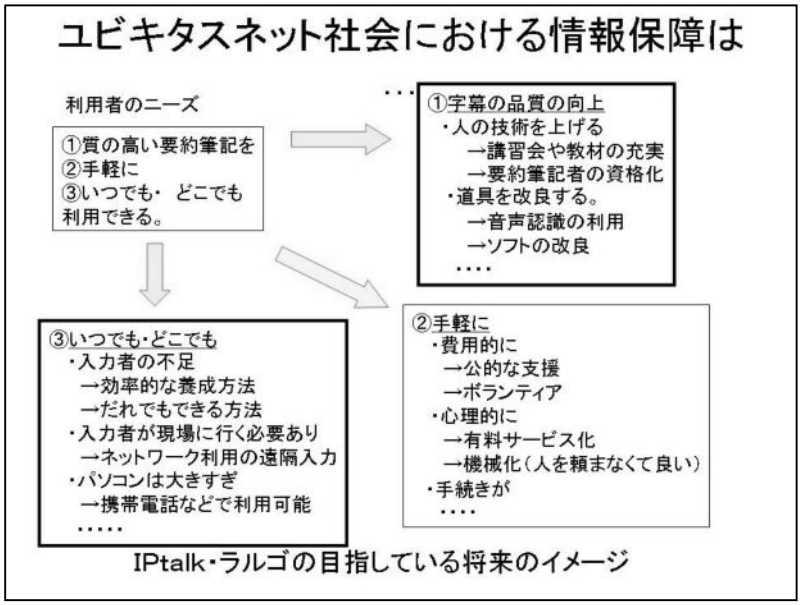
（３）システムの改善

在宅入力情報保障では、利用者が単独でセッティングを行うことを前提としています。そのため、システムの簡素化、軽量化、取り扱い手順の簡略化、マニュアル化を検討し、「誰でも」扱える手軽なシステムへと発展させる必要があると考えます。

第９章　ユビキタスネット社会における情報保障

u-Japan 政策の推進により、ネットワークを活用した技術は今後ますます発展し、身近になると思われます。それにより、インターネットを活用した在宅入力による情報保障も技術的な問題が解決されることが期待されます。しかし、技術的に可能になるだけでは、不充分です。

総務省の u-Japan 政策のホームページによれば、u-Japan の「u」には、ユビキタス(Ubiquitous)以外にも「Universal」「User-Oriented」「Unique」の「U」も含まれています[2]。「Universal」において「ICT で、高齢者も障害者も元気に社会参加」と謳われています。「いつでも、どこでも、何でも、誰でも」の理念が発展し、「いつでも、どこでも、誰でも、何でも、誰でも」情報にアクセスできる権利の保障や、環境の整備に繋がることに期待します。また、本稿のようなインターネットを介した新しい形態のサービスが公的制度として整備され、聴覚障害者の社会参加の拡大に繋がることを願います。(**図－50**)



図－50　要約筆記の将来イメージ

あとがき

本稿では、在宅入力情報保障に興味を持たれた方が取り組みやすいよう、マニュアルの要素も持たせたため長文になってしまいました。最後までお読みいただき、どうもありがとうございます。今後同様の試みを志す方々にとって、本稿が１つの足がかりになれば幸いです。

＜謝　辞＞

本稿を、一緒に実験、検討を進めてきたパソコン要約筆記サークル「ラルゴ」の仲間に感謝を込めて捧げます。全要研集会でのデモンストレーションで前例のないコーディネーターを努めながら入力も担当してくださった樋口智美さん、入力に参加してくださった鷲澤和歌子さん、片野雅義さん、杉本菊子さん、五十川咲子さん、槇山正二郎さん、機材の準備等でお世話になった脇坂みどりさん、会場でセッティングを担当してくださった愛媛大学大学院理工学研究科の加地正法さん、愛媛大学の PacketiX サーバ管理者としてトラブルシュートにも対応してくださった同大学大学院理工学研究科の岩元一徳さんに深く感謝します。本実験の実施、データ解析およびサーバ運用などの技術支援をしてくださった愛媛大学村田研究室の学生の皆さん、また、基礎実験に一緒に参加してくださった「愛媛要約筆記サークルオリーブの会」の清家ゆみ子さん、高田淳美さんに感謝します。

＜参考文献＞

[1] パソコン要約筆記サークル ラルゴ
http://iptalk.hp.infoseek.co.jp/largo/largo_top.htm

[2] 総務省 u-Japan 政策 http://www.soumu.go.jp/menu_02/ict/u-japan/

[3] 総務省情報通信データベース
http://www.johotsusintokei.soumu.go.jp/field/tsuushin01.html

[4] IPtalk http://iptalk.hp.infoseek.co.jp/

[5] ロゴスウェア株式会社 http://www.logosware.com/

[6] 筑波技術大学コミュニケーション支援研究グループ
http://www.fukushi.com/news/2004/05/040506-a.html

[7] 障害者情報ネットワーク ノーマネット
http://www.normanet.ne.jp/~rtcap/recap/040612.html

[8] 株式会社ビー・ユー・ジー http://www.bug.co.jp/topics/ud2002.html

[9] ソフトイーサ株式会社 http://www.softether.com/jp/

[10] 比較の穴 http://www.hikakuya.or.tv/ana/03.html

[11] Skype http://www.skype.com/intl/ja/helloagain.html

[12] 株式会社ＢＨＡ http://xvd.bha.co.jp/products/xcc_sx.html

[13] 小林　敏泰、村田　健史、木村　映善、遠隔パソコン要約筆記システムの開発、電子情報通信学会技術研究報告、vol.105, No.506, pp.55-60, 2006.

[14] 小林敏泰、VPN を用いた動画像ストリーミング配信による遠隔パソコン要約筆記の検討、愛媛大学工学部情報工学科卒業論文、2006.