初心者ユーザ遠隔支援システムにおける ユーザ管理手法に関する検討

油田 健太郎[1)]・金澤 昌史[2)]・平塚 祥泰[2)]・岡崎 直宣[3)]

Examination about user management technique in the beginner PC user support system

Kentaro ABURADA, Masashi KANAZAWA, Yoshihiro HIRATSUKA, Naonobu OKAZAKI

Abstract

Remote access attracts attention as a technique for supporting the beginner PC users. However, when remote PC is connected to the internet via a fire-wall, remote access to the PC from the outside is difficult. In this paper, we will propose a method for realize a secure remote access in such cases. We will also describe our implementation of prototype system.

Key Words:
Remote access, Network Address Translator, User supporting system.

1．はじめに

近年，ADSL（Asymmetric Digital Subscriber Line）や光ケーブルなどの広帯域のアクセス回線が普及し，多くの初心者ユーザがインタネットに常時接続する環境が整ってきた。ところが，初心者ユーザの多くはPCを購入したもののその操作や保守の方法を習得するために時間とコストがかかり，なかなかその活用ができないでいるのが現状である。また，ウイルスやDoS（Denial of Service）攻撃などのインタネット上での安全に対するさまざまな脅威が広がり，インタネットに常時接続されたPCについてもその適切な安全対策が強く求められている。しかしながら，そのような安全対策は初心者ユーザにとっては大変荷が重く，そのためほとんど有効な対策がたてられていないのが実情であろう。従って，初心者ユーザでも適切な安全対策を施せるような方法が強く求められている。

1) 情報工学専攻大学院生
2) 情報システム工学科学部生
3) 情報システム工学科助教授

このような状況の中で，初心者ユーザを遠隔から支援する方法が注目されている。著者らは，初心者ユーザを遠隔から支援するための手段として，リモートアクセスと呼ばれる技術に着目した。リモートアクセスとは，遠隔からネットワークサービスを利用するための技術であり，特にここでは遠隔からPCを操作することのできる機能を含むものを考える。これまで，リモートアクセスを用いた遠隔操作に関しては出先あるいは自宅から企業や大学内のLANへのアクセスする際の安全性に関する検討の報告[1)]がある。また，遠隔教育支援システムとしてはチャットや共有黒板と呼ぶウィンドを用いたテキストベースのシステムの例[2)]などがある。しかしながら，遠隔からPCの画面を直接操作するリモートアクセス技術を用いた初心者ユーザ支援については，その安全性を含めた十分な検討がなされていない。

本論文では，支援者が遠隔からPCの画面を直接操作することによって，初心者ユーザの支援を行うシステムについて考察する。これによって初心者ユーザに対して直接的で分かりやすい支援を行うことができ，また時間的，場所的な制約を緩和することにより，利

用者の利便性の向上や運用管理コストの低減が期待できる。

2．リモートアクセスを用いた初心者ユーザの遠隔支援

2.1 リモートアクセスのモデル

図1に様々なアクセス回線で接続している初心者ユーザを支援者がインタネットを介して遠隔支援するためのネットワークモデルを示す。安全で使い易いリモートアクセスの環境を実現するために，リモートアクセスを実現するプラットフォーム（以下，リモートアクセスソフトウェア）に求められる機能を整理し，課題とその解決法を検討する。

2.2 リモートアクセスソフトウェアに必要な機能

初心者ユーザを遠隔から支援することのできる環境を実現するための機能として，以下を考える。

（1） 同時操作

支援者と初心者ユーザが画面を共有し，双方が同じ操作をすることができる機能が必要である。この機能により，初心者ユーザは遠隔にいる支援者があたかもその場にいるような感覚で教授されることができる。また，支援者が遠隔支援に無関係の操作を行わないようにする抑制効果があると考えられる。

（2） 管理者権限

支援者は状況にとっては初心者ユーザの PC のドライバの更新なども行う必要があるため，リモートアクセスの際には，初心者ユーザの許可の下で管理者権限でその PC を操作できる必要がある。

（3） NAT を越えたアクセス

初心者ユーザ側の PC がネットワークアドレス変換装置（NAT[3]：Network Address Translator）またはその機能を有したルータなどを介してインタネットへ接続されている場合，外部にいる支援者から NAT を越えてプライベートネットワーク内部の PC にリモートアクセスを行うことができる必要がある。

（4） 安全性

リモートアクセスソフトウェアは，遠隔から PC のほとんどすべての機能を操作し得る強力なツールであるため，不正なアクセスや盗聴を許してしまうとセキュリティ上の重大な脅威になる可能性がある。そのため，不正アクセスやデータの盗聴などを防ぐ必要がある。

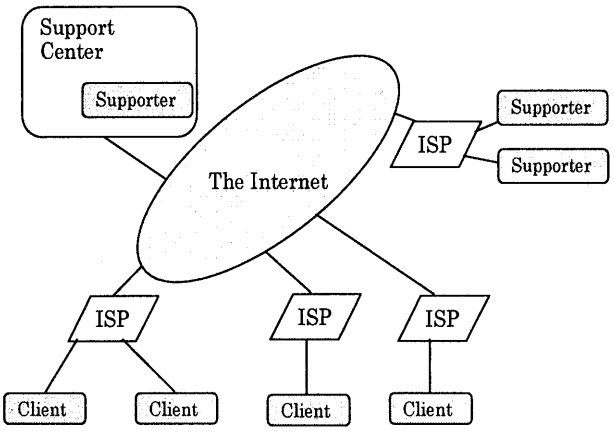

図1 リモートアクセスのモデル.

□

2.3 初心者ユーザ支援におけるリモートアクセスの課題と解決法

2.2で述べた観点から，既存の主要なリモートアクセスソフトウェアである Windows XP リモートデスクトップ[4]と WinVNC[5]について，遠隔支援システムとして必要な機能を有しているかどうかを調査した。その結果，（1）および（2）については既存のリモートアクセスソフトウェアにより対応可能であるものの，（3）（4）については不十分であることがわかった[9]。これらの課題の解決法としては，

(i) ポートを必要なときだけ開くようにしたり，ポートを動的に変更するなどにより不正アクセスを行いにくくする方法，

(ii) ユーザの回線の両端に専用の暗号化装置（VPN 装置）を設置することにより不正アクセスやデータの盗聴・改ざんを防ぐ方法，

(iii) 暗号化アプリケーションを使ってトンネリングを行い，不正アクセスやデータの盗聴・改ざんを防ぐ方法，

などが考えられる。

これらのうち，(i) は不正アクセスの可能性を排除することができないこと，(ii) は専用の装置が必要となりコストの面から実現性に問題があること，これらに対して，(iii) はフリーで提供されているソフトウェアを用いることができ，安全性や運用管理コストの面で優れていることなどを考慮し，本論文では（iii）の方法について検討する。

3．安全な初心者ユーザ遠隔支援システム

3.1 ユーザ支援の形態

ここでは以下のようなユーザ支援の形態を想定する。支援を受けたい初心者ユーザは，支援を請け負う事業者（支援業者）と支援に関する契約を結ぶ。その際，必要であれば支援業者は初心者ユーザの PC やアクセスルータなどに設定を行う。支援業者はまた，初心者ユーザを支援する者（支援者）と守秘義務を含む初心者ユーザに対する支援業務に関する契約を結ぶ。支援業者は初心者ユーザ及び支援者の状態を管理し，初心者ユーザからの要請に基づき，支援者に初心者ユーザの支援を依頼する。支援業者はサポートセンタを設置し，支援業者はサポートセンタ内だけでなく外部からの支援を可能とする形態にすることにより，支援者に対する場所的，時間的な制約が緩和され，より柔軟な支援を行うことができるようになる。また，初心者ユーザ及び支援者はサポートセンタに設置されるサーバに接続を行い，サーバを介して支援を行うようにする。このことにより，特に外部にいる支援者が直接初心者ユーザに接続して支援する場合に比べ，支援の状態の支援業者による管理が容易になり，また場合によっては支援の内容の監視を行うことも可能となるため，支援者による不正行為の抑止になると期待できる。

3.2 提案システム

ここでは，アプリケーションによるトンネリングを行う方法として，通信路を暗号化することにより安全性を高めたリモートシェルである SSH（Secure SHell）を用いた方法について検討する。SSH にはポート転送（port forwarding）と呼ばれる他のアプリケーションの通信を暗号化して安全に通信を行うためのトンネリング機能がある。

SSH のポート転送機能を用いたリモートアクセスとしては，リモートアクセスソフトウェアのサーバ側に SSH サーバ（SSHd）を設置するのが一般的である[5]。この方法は，出張先から職場の PC へリモートアクセスする場合などに用いられる。この形態のポート転送を「ローカルポート転送」と呼ぶ。しかし，この方法をそのまま初心者ユーザ支援に利用すると，初心者ユーザ側に SSH サーバを設置する必要がある（図２）。さらに SSH サーバの IP アドレスが固定でない場合は，SSH クライアントから SSH サーバにアクセスするた

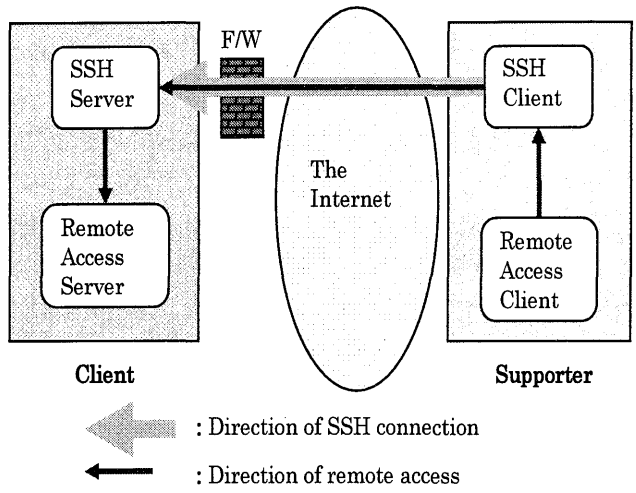

図２　ローカルポート転送によるリモートアクセス.

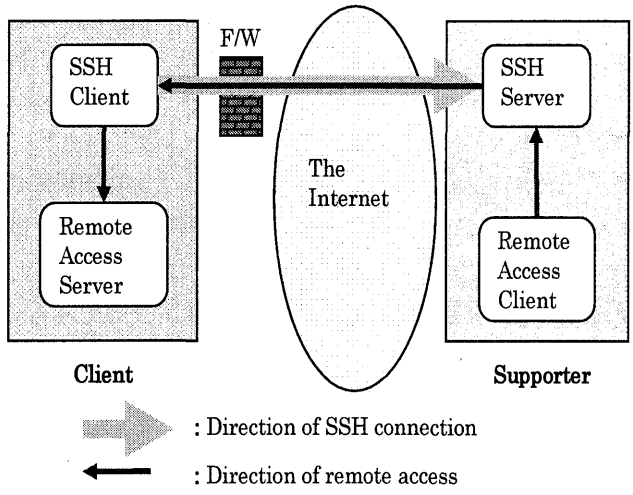

図３　リモートポート転送によるリモートアクセス.

めには IP アドレスが変わる度に支援者に伝える必要がある。これらのことより，この方法は実現が困難であると考えられる。さらに初心者ユーザの PC が NAT を介してネットワークに接続されている場合やファイアフォールの内側にある場合には，外部から SSH によるコネクションを確立することができないという課題もある。

これに対して，逆方向の SSH ポート転送を用いる方法が考えられる。すなわち，リモートアクセスソフトウェアのクライアント側に SSH サーバを設置する。この形態のポート転送を「リモートポート転送」と呼ぶ。この方法では，初心者ユーザ側に SSH サーバを設置する必要がなくなる（図３）。また，リモートアクセスソフトウェアのサーバへの接続は NAT の内側から一

度 SSH のコネクションを確立した後に通信を行うため，初心者ユーザの PC が NAT やファイアウォールの内側にある場合でも問題なく接続できる。

ここではさらに，3.1 で述べたユーザ支援の形態を実現するために，支援者がサポートセンタの外部から支援を行う場合を考える。このとき，初心者ユーザだけでなく，支援者の PC が NAT やファイアウォールの内側にある場合も考慮する必要がある。このような場合には，SSH サーバを NAT やファイアウォールの内側に設置すると，上記のリモートポート転送によるリモートアクセスを用いることができないという問題が生じる。また，支援者側に NAT やファイアウォールがない場合でも，アクセス回線の形態により支援者の IP アドレスが固定でない場合には，IP アドレスが変わるごとに SSH クライアントの接続先の設定を変更しなければならない。これらの問題を解決するために，ここでは SSH サーバを支援者とは別の場所（サポートセンタ）に設置し，これをリレーとして用いる方法を提案する（図４）。ここでは，ユーザからの SSH サーバへの接続および支援者からの SSH サーバへの接続には，それぞれリモートポート転送およびローカルポート転送を用いる。さらに，この方法を実現するために，以下のような機能を新たに開発する。

・ポート転送機能
　初心者ユーザおよび支援者からのそれぞれの SSH のポートを転送し，リモートアクセスのコネクションを接続する機能
・ユーザ／支援者管理機能
　初心者ユーザおよび支援者のそれぞれの登録やアクセス状況などを管理し，また支援の要請に基づき支援者を選択し，支援の開始要求を出す機能
・支援内容検証機能
　初心者ユーザへの適切な支援が行われたかどうかを検証する機能

3.3 ポート転送機能

ユーザ／支援者管理機能により割り当てられたポート番号同士をつなぐ処理を行う。また，支援終了の際にポート中継の終了を行う（本システムでは 2 つのポート同士をつなぐために relayTCP プログラムを作成した）。

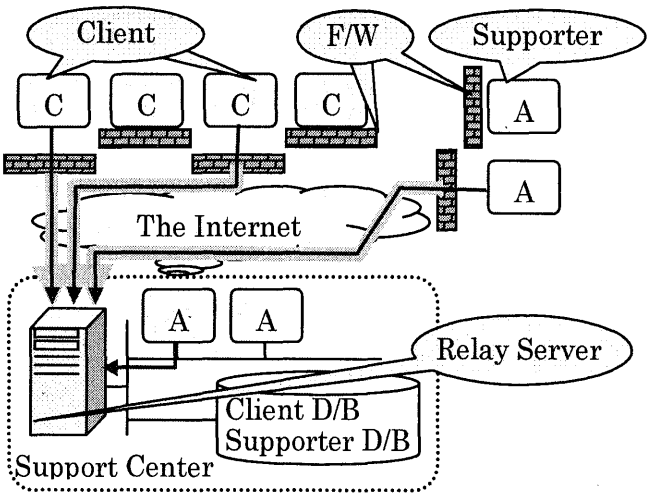

図４　提案するリモートアクセスシステムモデル.

3.4 ユーザ／支援者管理機能

本システムでは効率の良い支援を行うため，またユーザの状態を管理しやすくするためリレーショナルデータベースを用いる。データベースでは以下の４つの項目を管理する。

A)　ユーザ ID
ユーザを識別するための ID を示す。
B)　ポート番号
ユーザに割り当てたポート番号を示す。
C)　ユーザの支援内容
支援内容に応じて 1～3 までのランクを示す。
D)　ユーザの状態
支援中もしくは待機中などのユーザの状態を示す。

以下にデータベースの処理について述べる。

{データベース処理１}

(1)　新しい初心者ユーザからログインがあった場合にはその初心者ユーザのランクを参照する。
(2)　初心者ユーザと同じランクの支援者が存在するかデータベースを参照し調べる。
(3)　同じランクの支援者が存在した場合にはその支援者が他の初心者ユーザを支援中かどうか，データベースを参照する。同じランクの支援者が存在しない場合には初心者ユーザの状態を待ち状態にしてデータベースに追加する。
(4)　支援者が他の初心者ユーザを支援中でなければ，支援者，初心者ユーザにランダムなポート番号を割り当て支援を開始する。他の初心者ユーザを支援中であれば初心者ユーザの状態を待ち状態にしてデータベースに追加する。

{データベース処理2}

(5)　支援終了後にデータベースから支援の終了した初心者ユーザを削除し支援者の状態を待ち状態にする。その後データベースを参照し待ち状態の初心者ユーザが存在するかどうか確認する。

(6)　待ち状態の初心者ユーザが存在した場合には(2)の動作へ移る。存在しない場合には新しくログインがあるか，支援が終了するまで待機しておく。

3.5 支援内容検証機能

本システムでは支援終了後に初心者ユーザの PC に問題が起こった場合に支援内容を再現し，適切な支援が行われたかどうかを検証するために支援内容を動画として記録する機能を導入する。これにより，初心者ユーザへの適切な支援が行われたか検証できるようになる。

記録する情報としてまず，初心者ユーザの PC のデスクトップ画面と考える。さらに初心者ユーザの PC には現れない支援者の操作（例：telnet などによる操作）を記録することにより，その両方を比較し支援終了後に検証できるようにする。

システムの構成は，支援者のデスクトップも記録するため，支援者の PC にもリモートアクセスソフト(以下，RAS）サーバを設置する。また，記録・編集作業は PC に多大な負荷をかけるため，ポートを中継するサーバとは別にサポートセンタ内に記録を行うレコーディングサーバ（以下，レコサーバ）を設置する（図5）。

3.6 システムの詳細手順

以下にシステムの通信を行う際の手順を述べる（図6）。ap1〜ap3，op4〜op6 はそれぞれリレーサーバから割り当てられたポート番号，PC のローカルなポート番号をさす。

(1) 初心者ユーザがヘルプボタンを押すとRASサーバが起動する（RAS Server Start）。

(2) 初心者ユーザはSSHを用いてリレーサーバにログインを行う(SSH Connect)。

(3) データベース処理1を行い，初心者ユーザと支援者のポートをつなぐ処理を行う(Database process 1)。

(4) リレーサーバは初心者ユーザに支援時に使用するポート番号を渡し，SSHでの再ログインを要求する（Reconnect ap1)。

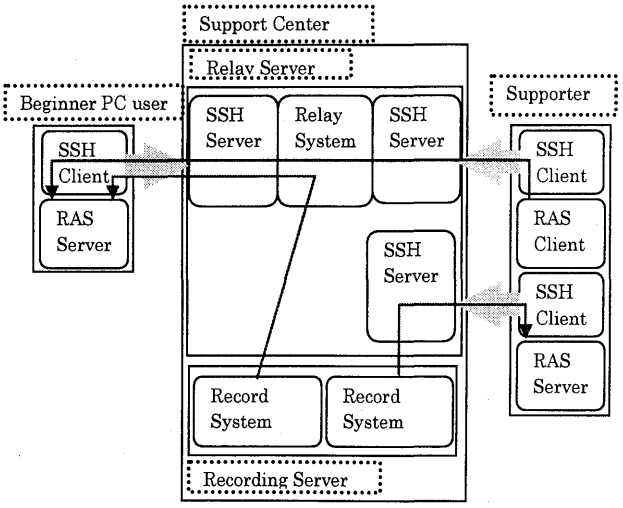

図5　支援内容検証機能のシステムの構成.

(5) リレーサーバは支援者に支援時に使用するポート番号ap2と記録時に使用するポート番号ap3を渡し，SSHでの再ログインを要求する（Reconnect ap2 , Connect ap3)。

(6) 支援者がRASサーバを起動させる（RAS Server Start）。

(7) 初心者ユーザは指定されたポート番号をもとにリモートポート転送の設定を行い，SSHを用いてリレーサーバにログインを行う（Remote port forward ap1 to op4)。

(8) 支援者は指定されたポート番号をもとにローカルポート転送の設定を行い，SSHを用いてリレーサーバにログインを行う（Local port forward op5 to ap2）。

(9) 支援者は記録用のリモートポート転送の設定を行い，SSHを用いてリレーサーバにログインを行う（Remote port forward ap3 to op6）。

(10) 初心者ユーザおよび支援者はSSHのポート転送を用い，記録サーバに接続を行う（Connect Reco Server)。

(11) 初心者ユーザ・支援者はそれぞれレコサーバに記録開始の指示を行う(Request Start Record）。

(12) レコサーバは記録開始の指示を受けて記録を開始する（Start Record)。

(13) 支援者がRASクライアントを起動させる（RAS Client Start）。

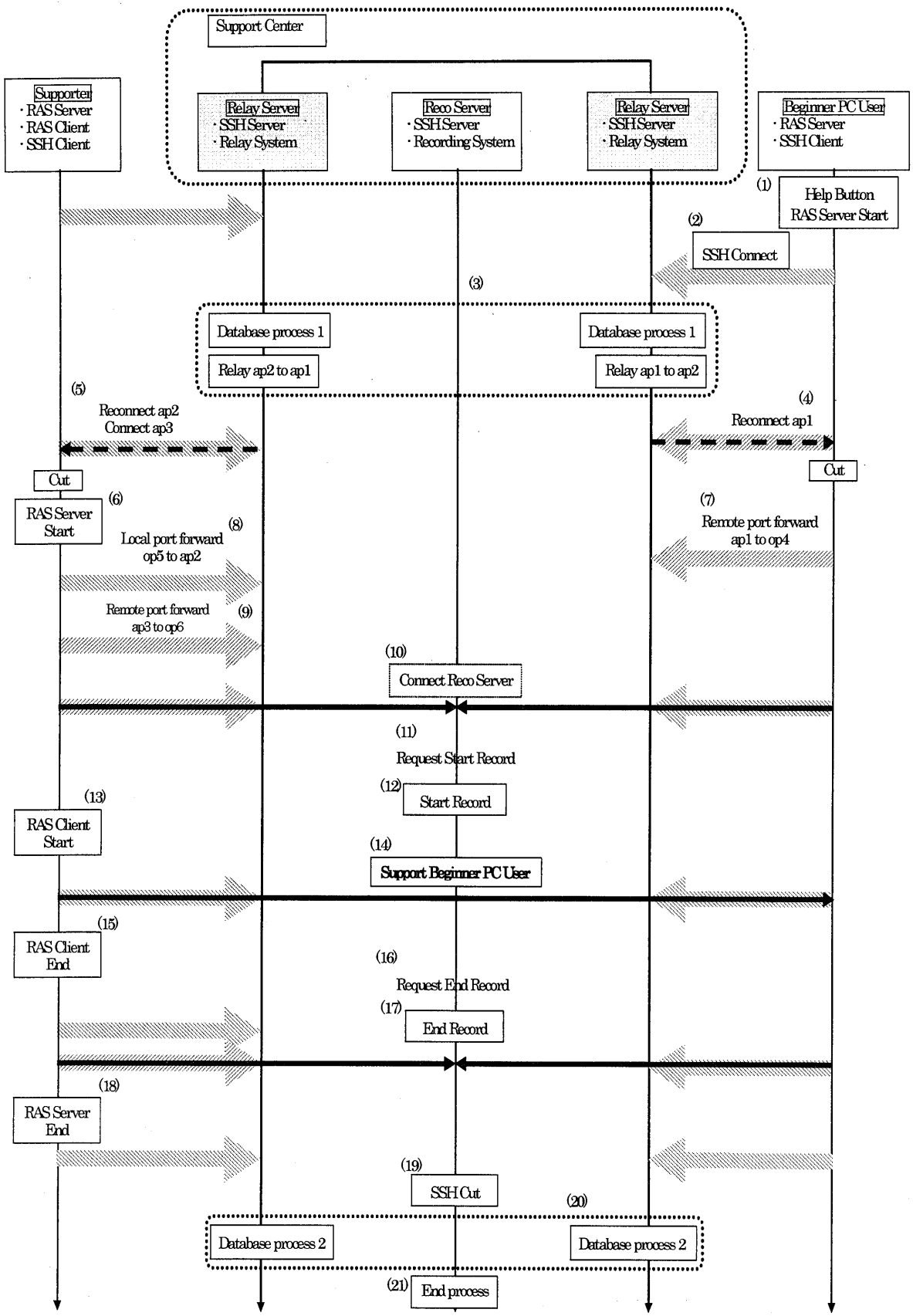

図6 システムの詳細手順.

(14) 支援者はSSHでトンネリングされた経路を用いリモートアクセスによる支援を開始する（Support Beginner User)。
(15) 支援者は支援が終了するとRASクライアントを終了させる（RAS Client End)。
(16) 初心者ユーザ・支援者はそれぞれレコサーバへ記録終了の支持を行う（Request End Record)。
(17) レコサーバは記録終了の指示を受けて記録を終了させる（End Record）。
(18) 支援者はRASサーバを終了させる（RAS Server End）。
(19) 初心者ユーザおよび支援者はSSHのコネクションを切断する(SSH Cut)。
(20) データベース処理２を行う（Database process 2)。
(21) 初心者ユーザのRASサーバの終了，ポートをつなぐ処理の終了などの終了処理を行う(End process)。

□

4．プロトタイプシステムの構築

３章で提案した方法に基づき，表１で示す構成で初心者ユーザの遠隔支援のためのプロトタイプシステムを構築した。ここではリモートアクセスソフトウェアとしてVNCの改良版であるTightVNC[6]を，トンネリングソフトウェアにOpenSSH[7]を使用した。また，VNCのクライアント／サーバにWindows XP Home，SSHサーバにはRed Hat Linux 9.0，記録システムにはvncrec[8]を使用した。なお，プロトタイプシステムは基本的な動作の確認を目的としたため，3.2で示した機能のうち，ユーザ／支援者管理機能としてはあらかじめ用意されたファイルに基づく簡易な管理機能のみ実装し，実験時は接続およびデータベースの操作はマニュアルで行った。新たに開発をした部分に関しては，C言語で実装を行った。

4.1 プロトタイプシステムの評価

まず，支援内容検証機能を使用しないシンプルな構成でシステムが正常に動作するかどうかの確認を行った。実験では，ネットワーク環境としてADSLによるアクセス回線を介して初心者ユーザがインタネットに接続している場合と，100BaseTXのLANでSSHサーバに接続している場合について動作を確認した。

構築したプロトタイプシステムにおいてパケット解析ツールを用いて通信データをキャプチャして解析を行った結果，通信の内容が暗号化されており安全にリモートアクセスが行われていることを確認できた。また，初心者ユーザ側及び支援者がそれぞれNATを介している場合でも問題なく通信を行うことができた。さらに，初心者ユーザ／支援者がそれぞれ複数いる場合の同時接続も可能であることを確認した。操作感については，SSHを使用していることを意識しなくてもSSHを使用していない場合と同じようにスムーズに操作することができた。しかしながら，これはアクセス回線の帯域やネットワークの混雑状況，PCの処理能力に大きく依存すると考えられる。また，ユーザ情報の管理部分にリレーショナルデータベースを用いることにより，情報の取得，参照，追加，削除，更新を簡易に行えるようになるとともに，初心者ユーザ及び支援者にランクという情報を持たせ初心者ユーザ支援の効率化を図ることもできるようになった。

次に支援内容検証機能を実装し，2組の初心者ユーザ・支援者の組を用意し，正常に支援が行えるか，また支援内容がレコサーバに記録できているか確認を行った(図７)。その結果，正常に支援を行うことができ，初心者ユーザ，支援者のそれぞれの支援内容を記録できていることが確認できた。さらに，「悪意を持った支援者が初心者ユーザのPCから不正に個人情報を奪取しようとしている」というケースを想定し，その様子を記録した。その結果，初心者側のデスクトップ画面の記録，支援者側のデスクトップ画面の記録の両方を比較することにより，初心者ユーザのPC上でのバック

表１ プロトタイプシステムの構成.

	User PC/ Support PC	SSH Server	Reco Server
OS	Windows XP Home	Red Hat Linux 9.0	Red Hat Linux 9.0
SSH	TeraTerm Pro 2.3 + ttssh 1.54	OpenSSH 3.4p1-2	OpenSSH 3.4p1-2
Remote Access Software	TightVNC 1.26	----	----
Record Software	----	----	vncrec 0.2

グラウンドで行われた不正な操作を発見する事ができた。また，3分ほどの実験を行い，支援者と初心者ユーザの記録データのファイルサイズを比較すると支援者側で6.8MB，初心者ユーザ側で1.9MBであった。支援者側のデータが初心者ユーザ側のデータに比べ約3.6倍になっている。これは支援者側のデータは支援者のデスクトップ情報と初心者ユーザのデスクトップ情報の2つの情報を持っているためであると思われる。なお，記録システムは支援の記録の圧縮等の加工は行っていない。

5．まとめ

本論文では初心者ユーザを遠隔から支援するための安全で使い易い環境を実現することを目的とし，必要な機能を整理しそれらを設計，また実装を行いその有効性を確かめた。通信が暗号化されることによってパスワードの盗聴などを防ぐことができ非常に効果的であることが分かった。また，ユーザ情報の管理にリレーショナルデータベースを用いることにより情報の管理が容易に行え，支援内容検証機能により支援者による不当な操作を発見することができた。

今後の課題としては，以下のようなものがある。今回はプロトタイプシステムとして基本的な機能を確認する目的であったため実装を行わなかった，ユーザからの支援を受けて自動的に支援者を割り当てる機能などについて拡張を行い，より実用的なシステムとする必要がある。また，複数のユーザで通信を行う際に，ひとつの SSH サーバに最大同時にいくつまで通信を行うことができるかなどの規模の拡張性に関する検討も必要と考える。さらに相互の表情，会話を通してより親しみやすいシステムにするための拡張，記録データの圧縮，インデックス付けなどが挙げられる。

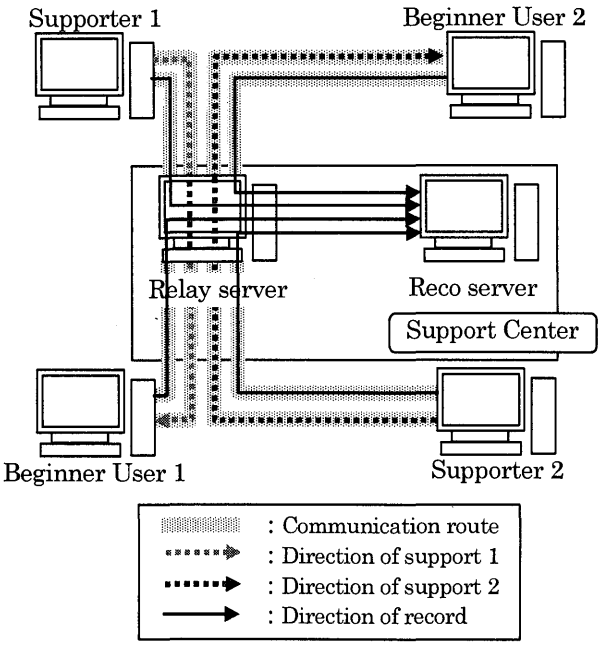

図７　実験環境.

参考文献

1)川瀬 徹也, 渡邊 晃, 笹瀬 巌, "暗号を用いたセキュアリモートアクセス方式の提案", 電子情報通信学会技術研究報告, IN, Vol. 97, No. 493, pp. 1-6, 1998.

2)篠崎 明, 佐藤 和寿, 澤村 浩, 伊与田 光宏, "リモートアクセスを利用した教育支援システム", 電子情報通信学会ソサイエティ大会講演論文集, D-414, p.418, 1994.

3)P. Srisuresh, K. Egevang,"Traditional IP Network Address Translator",RFC 3022, 2001.

4)Using Remote Desktop, http://www.microsoft.com/windowsxp/pro/using/howto/gomobile/remotedesktop/.

5)Virtual Network Computing, http://www.uk.research.att.com/vnc/.

6) TightVNC, http://www.tightvnc.com/.

7) OpenSSH, http://www.openssh.com/.

8) vncrec, http://www.sodan.org/~penny/vncrec/.

9)油田 健太郎, 田岡 智成, 岡崎 直宣, 中谷 直司, 厚井 裕司, 朴 美娘, " NAT を介した PC のリモートアクセスに関する一検討", 情報処理学会火の国情報シンポジウム 2003 予稿集, pp.161-167 2003.