リモートアクセスによる初心者ユーザ支援の安全性に関する検討

岡崎　直宣[1)]・油田　健太郎[2)]

Security issues of the beginner PC user support system using remote access

Naonobu Okazaki, Kentaro Aburada

Abstract

Remote access attracts attention as a technique for supporting the beginner PC users in remoteness. However, when remote PC is connected to the internet via a router which has function of the Network Address Translator, remote access to such the PC from the outside is difficult. In this paper, we will report an examination of the method for realize a secure remote access in such network architecture. We will also describe our prototype-system.

Key Words:
Remote access, Network address translator, User supporting system

1. はじめに

近年，ADSL や光ケーブルなどのブロードバンドが普及し，インターネットに常時接続する環境が整ってきた．そのような中で，PC の操作に慣れたユーザのみならず，多くの初心者ユーザがインターネットに接続するようになった．ところが，初心者ユーザの多くは PC 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．また近年，インターネット上での安全に対するさまざまな脅威が広がり，インター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る．したがって，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．

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として E-Learning などの新しい手法が注目されている．本研究では特に，リモートアクセス技術とよばれる PC の遠隔操作機能に着目し，初心者ユーザが PC の操作やトラブルの解決，保守などの支援を低コストで手軽に安心して受けられる方法について検討する．

リモートアクセス技術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，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遠隔教育支援システムの例[2)]などがある．ここでは，支援者が遠隔から PC の画面を直接操作する事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．これによって時間と場所の制約を緩和する事により利用者の利便性の向上やコストの削減を図る事ができる．

以下では，２．でリモートアクセスによる初心者ユーザ支援のモデルを示し，リモートアクセスに求められる機能について整理する．そして，その実現のための課題として，安全性の確保の実現と，ネットワークアドレス変換(NAT : Network Address Translator[3)])機能を持ったルータを越えて支援する方法の実現がある

1) 情報システム工学科助教授
2) 情報システム工学科学部生

事を示す．3．では，これらの課題を解決する方法としてアプリケーションレベルでの暗号によるトンネリングを用いる方法について提案する．また，プロトタイプシステムの構築について述べる．4．はまとめである．

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ー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は，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必要がある．

2.2 リモートアクセスソフトウェアの機能と性能の比較

初心者ユーザを遠隔から支援する環境を実現するために以下のような点を考慮する必要がある．

(1) 支援者と初心者ユーザが同時に操作できる機能が必要である．この機能により，支援者がリモートアクセスしている画面を初心者ユーザも見る事ができる．これにより，支援者が遠隔にいる初心者ユーザをあたかも後ろに支援者がいるような感じで教える事ができる．また，初心者ユーザからリモートアクセスしている画面を見る事ができるため，支援者が遠隔支援に関係のない操作を行わないように抑制する事ができる．

(2) リモートアクセスの際には，操作する PC の管理者権限が必要な場合がある．支援者は状況によ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管理者権限で操作できる必要がある．

(3) 初心者側の PC が NAT を介して外部へ接続されている場合，NAT を越えて支援を行う必要がある．

(4) 不正アクセス対策として登録された IP アドレス以外の接続を拒否する，通信内容を暗号化するなどの対策を行い，不正アクセスやデータの盗聴などを防ぐべきである．

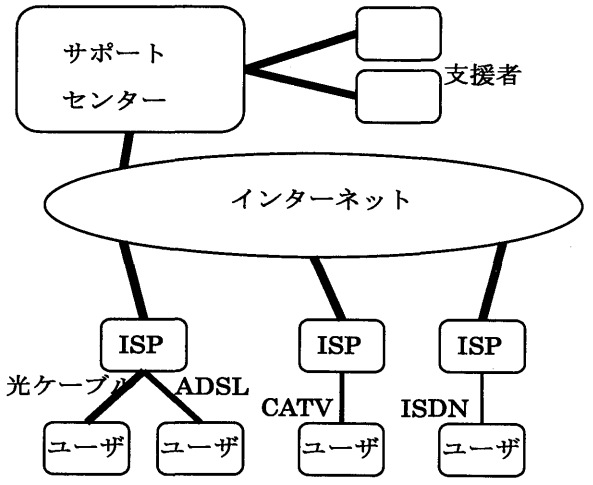

図 1　リモートアクセスのモデル

以上のような機能を満たしているかを，既存の主要なリモート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]について検証した(表 1)．

その結果，(1)(2)の項目の機能については問題がないが，(3)(4)の項目の機能については不十分である事が分かった．以下ではこれらの課題の解決法について検討する．

2.3 リモートアクセスの課題とその解決法の比較

インターネットを介してリモートアクセスを行う際には，悪意を持った他のユーザからデータの盗聴，データの改ざんなどをされる恐れがある．特にリモートアクセスでは全ての操作を許してしまう危険がある．そのため，通信内容を保護する仕組みが必要である．

また，支援する初心者ユーザの PC が NAT 機能を持つルータを介してインターネットに接続されている場合には，外部から内部のネットワークを参照する事ができないため，通常はリモートアクセスにより支援する事はできない．これに対して，ルータの設定で特定のポートをフォワーディングする，又は DMZ：DeMilitarized Zone(非武装地帯)に設定する方法も考えられるが，前者の場合，特定のポートをターゲットに不正アクセスされる恐れがあり，また後者の場合，全てのパケットを通過させてしまうためセキュリティ上大変問題が大きい．

NAT を介したリモートアクセスを安全に行う方法と

表1　リモートアクセスソフトウェアの機能の比較

	リモートアクセスソフトウェア	
項目	WindowsXP リモートデスクトップ	WinVNC 3.3.3J
(1)支援者/初心者ユーザによる同時操作	不可	可
(2)リモートユーザが得られる権限	初心者ユーザ側でログインしている権限と同じになる.	
(3)NAT の内側にある PC へのアクセスの可否	不可	不可
(4)不正アクセス対策	不可	不可

して以下の(1)～(3)が考えられる.
ただし，これらは以下の前提条件を満たしているものと考える.

- ルータや初心者ユーザの PC には事前に支援者の IP アドレスが設定されている.
- 支援者は初心者ユーザの PC に設定したリモートアクセスのためのパスワードを知っている.

(1)ルータの機能を拡張する方法

初心者ユーザ側のルータに以下の機能を拡張する事によりセキュリティを高める方法である(図 2).

- ルータはリモートアクセスを行うために，必要な時だけポートを開き，通信が終わり次第ポートを閉じる.
  (ポート動的制御機能)
- 特定のクライアント以外の接続をルータで遮断する.
  (フィルタリング機能)
- セキュリティ向上のために通信に使うポートを動的に変更する.
  (動的ポート変換機能)

これらの機能により，不正アクセスを行いにくくする事によってある程度セキュリティを高める事ができるが，通信内容を保護する事ができないため，データの盗聴，改ざんの恐れがある.

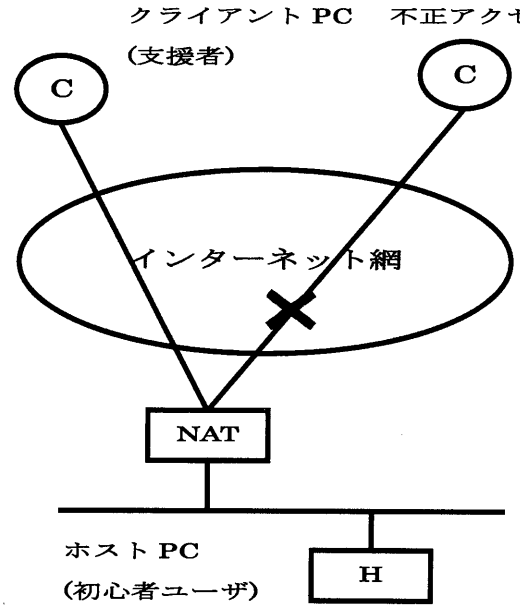

図2　ルータの機能を拡張する方法

(2) VPN(Virtual Private Network)を使う方法

仮想プライベートネットワーク(VPN)とは，ユーザの回線の両端に専用の VPN 装置を設置し，公衆ネットワークをあたかも専用線のように利用できるサービスの事である [6]. VPN を使用する事によってリモートアクセスをする際にデータの盗聴や改ざんの心配がなくなる(図 3). しかしこの方法は，初心者ユーザ宅にも VPN 装置を設置する必要があるため，コストの点から実用的ではない.

また，VPN を実現する手段として IPsec[7]を用いる方法もある. IPsec は，共通鍵暗号と公開鍵暗号の技術を採用した標準的な手法として通信データを暗号化するには大変有効な手段であるが，NAT を介している場合は，アドレス変換機能により IP ヘッダの送信アドレスが書き換えられてしまうため，IPsec の認証機能が働きパケットが改ざんされたものとみなされてしまう. また，NAPT においては送信先のポート番号の書き換えが行われるが，IPsec が適用されたパケットのトランスポート層のヘッダは，認証の対象，または暗号化されているため NAPT では使用できない. したがって，このような場合には利用する事ができない.

(3) アプリケーションによるトンネリングを行う方法

SSH(Secure SHell)などのアプリケーションを使ってトンネリングを行い VPN と同等な環境を構築する事ができる. この場合には，専用の VPN 装置のような高

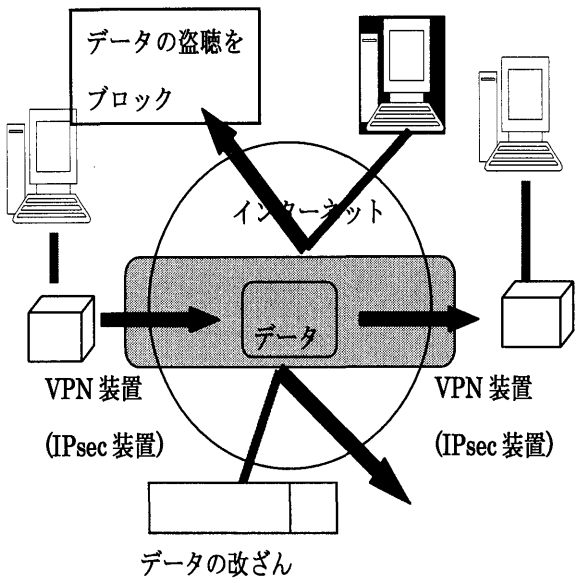

図3 VPNによるリモートアクセス通信の保護

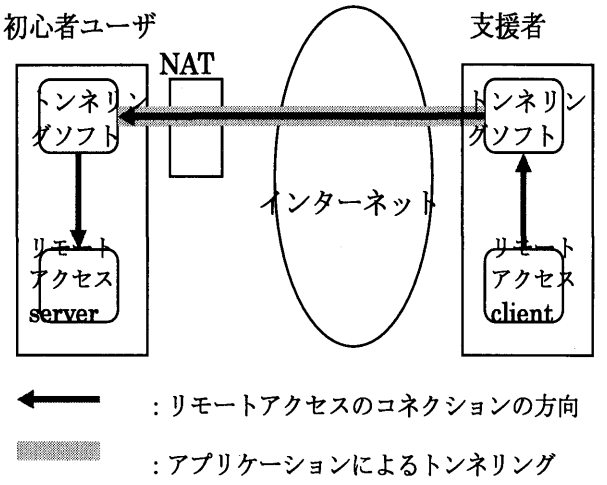

図4 アプリケーションによるトンネリング

価な装置は必要なく，トンネリングによりデータの盗聴や改ざんも防ぐ事ができる[8]．また，一度トンネリングによるコネクションを張る事ができれば，NATを越えてデータ通信を行う事ができる(図4)．

(1)～(3)までの方法を比較した結果，本研究では，安価に通信データを保護できる点，またトンネリングによりNATを越えてデータ通信を行える点から，アプリケーションによるトンネリングを行う事により通信内容を保護する方法について検討する．

3. 提案する解決方法

3.1 提案するシステム

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SSHを用いた方法について検討する．SSHとは，通信路を暗号化する事により安全性を高めたリモートシェルの事を指す．SSHが提供する暗号化した通信経路を利用する事によりデータの盗聴等を防ぐ事ができる．

SSHには以下のような利点がある．

- データを暗号化して送るため，データの盗聴を防ぐ事が可能である．
- SSHにログインする際のパスワードも暗号化されるため，パスワード盗聴が困難になり，不正ユーザの成りすましを防ぐ事が可能である．
- データの暗号化の際にデータの圧縮を行うため通信時のトラフィックを軽減する事が可能である．
- POP3，FTP，X-Windowなど，通信時にデータが暗号化されないプロトコルでもSSHを使用する事により暗号化する事が可能である．

また，SSHには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機能がある．SSHでトンネルリングを行い，その中にリモートアクセスソフトウェアのセッションを張る事により暗号化された安全なリモートアクセスを行う事ができる．

SSH port forwardingによるリモートアクセスとしては通常，表2のような方法が一般的である．この方法は，出張先から会社のPCへリモートアクセスする場合などに用いられる．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．さらにSSHサーバのIPアドレスが固定でない場合はクライアント側からSSHサーバにアクセスするためにはIPアドレスが変わる度に支援者に伝える必要がある．また安全なリモートアクセスを行うために各種設定をしなければならない．これらの事は，初心者ユーザには荷が重いと考えられる．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ウ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張る事ができない．

これに対して本研究では，表3で示すようなこれとは逆方向のSSH port forwardingの考え方を用いる．

表 2　一般的なリモートアクセス

	支援者側 PC	初心者ユーザ側 PC
リモートアクセスソフトウェア	client	server
トンネリング	SSH client	SSH server

表 3　提案するリモートアクセス

	支援者側 PC	初心者ユーザ側 PC
リモートアクセスソフトウェア	client	server
トンネリング	SSH server	SSH client

以下，これを逆方向 SSH port forwarding と呼ぶ(図 5).

逆方向 SSH port forwarding を利用する事により初心者ユーザ側に SSH サーバを立てる必要がなくなる．また，リモートソフトウェアの server 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．

さらに，図 5 の逆方向 SSH port forwarding において，支援者の PC が NAT やファイアウォールの内側にある場合を考える．この場合には，図 5 の構成では初心者ユーザ側の SSH client からの接続ができない．また，支援ユーザの IP アドレスが変わるごとに SSH client の接続先の設定を変更しなければならない．上記に加えこれらの問題を解決するために，SSH サーバを別の場所に置きこれをリレーに使う方法を提案する(図 6).

これにより複数の初心者ユーザを一つの SSH サーバを用いて支援する事ができるようになる．また，支援者は常にサポートセンター側にいる必要はなくインターネット上のどこにいても初心者ユーザを支援することができる(図 7).

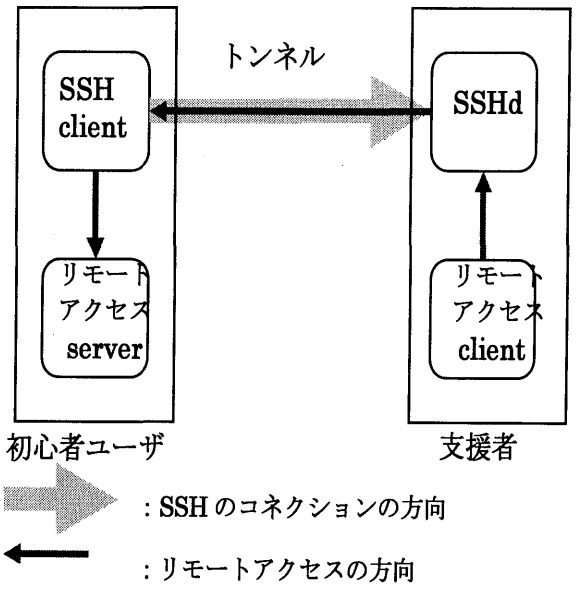

図 5　逆方向 SSH port forwarding

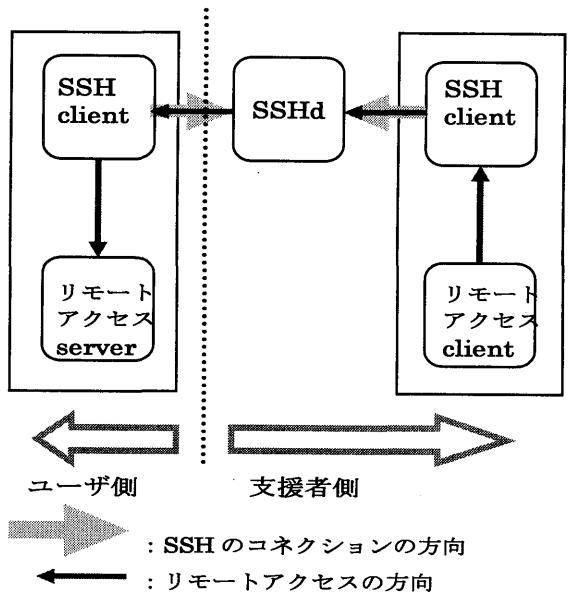

図 6　SSH サーバをリレーに使う手法

3.2 プロトタイプシステムの構築

図 7 の環境を実現するためには以下の条件が必要である．

・ 初心者ユーザ側は，SSH client，リモートソフトウェアの設定をしなければならないため，一度支援者

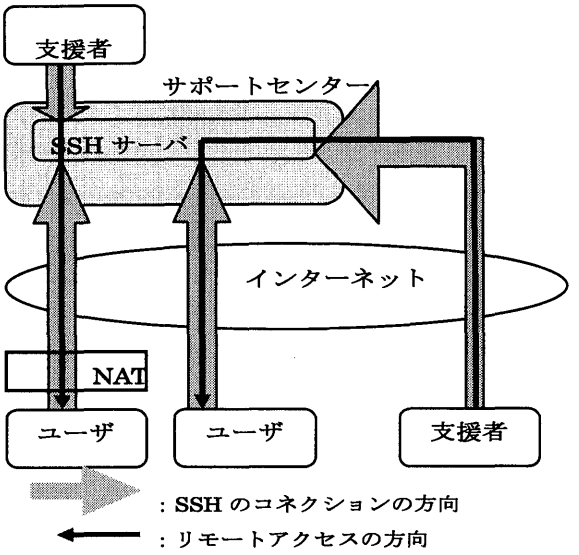

図 7 複数のユーザを同時に支援するモデル

が初心者ユーザ宅に行くなどして設定を行う必要がある.

- リモートアクセスを行うために, 初心者ユーザ側のIP アドレスが固定でない場合は, 接続の際の IP アドレスを支援者に伝える必要がある.
- SSH はシェルを提供するため, SSH client から SSH サーバ(SSHd)にログインする際に root の権限でログインされると設定を変更されてしまう恐れがあるため, 権限を制限したアカウントを作成する.

これらの点に考慮して, 初心者ユーザに使い易いリモートアクセスの環境を提供するためのシステムを以下のように提案する.

- SSH client を使って SSHd に接続する又はリモートアクセスソフトウェアを起動する事が困難である初心者ユーザのために「ヘルプボタン」を押すだけで, 自動で VNC server を立ち上げ, SSH client が SSHd に接続し, 支援者に IP アドレスを送るようなインターフェイスを開発し実装する.
- ユーザの IP アドレスを知る方法については, 支援者側に DynamicDNS[9]サーバを設ける事により接続の度に IP アドレスを支援ユーザ側に伝える.

ここでは実際に逆方向 SSH port forwarding を利用し, 図 6 で示した SSH サーバをリレーに使う方法によるプロトタイプシステムを構築した(表 4).

なお実装には, 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[10], トンネリングソフトには OpenSSH[11]を使用した. また, VNC のクライアント・サーバに Windows XP Professional, SSH サーバには Red Hat Linux 8.0 を使用した. 構築した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ー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事を確認できた. また, 初心者ユーザ側に NAT を介している場合でも問題なく通信を行う事ができた. さらに, 支援者が複数いる場合の同時接続(図 7)もできる事を確認した.

表 4 実装に用いた構成

	ユーザ側 PC	支援者側 PC	SSH サーバ
OS	WindowsXP Professional		RedHat Linux 8.0
SSH	Tera Term Pro 2.3 + ttssh 1.54		OpenSSH[7] 3.4p1-2
リモートアクセスソフトウェア	TightVNC 1.26		--

操作感, 使用感については, SSH を使用している事を意識しなくても 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事ができた. 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. また今回行った実装では 2 人までの同時セッションについて確認したが何人まで同時に使用できるか確認する必要がある.

4. おわりに

本論文では, 初心者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事を目的とし, NAT を介したリモートアクセスを SSH を使用して安全に行う方法を提案した. 通信が暗号化される事によってパスワードの盗聴などを防ぐ事ができ非常に効果的である事が分かった.

今後の課題としては以下のようなものがある. まず,

提案するシステムにおいては初心者ユーザの PC においてリモートアクセスに使用するポートをあらかじめ常に開いておく必要がある．通信が終わってもそのポートが開いたままの状態になるのでセキュリティ上の問題が残る．すなわちポートスキャンなどをされた場合に不正アクセス，又は攻撃の対象となる恐れがある．そのため通信が始まる直前に必要なポートを開き通信が終わったら閉じるような仕組みが必要となる．また，複数のユーザで通信を行う際に，一つの SSH サーバに最大同時に幾つまで通信を行う事ができるかなどの規模の拡張性に関する検討も必要である．

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)Remote Desktop, http://www.microsoft.com/windowsxp/pro/using/howto/gomobile/remotedesktop/.
5)VNC, http://www.uk.research.att.com/vnc/.
6)金城 俊哉, "よくわかる最新 IP-VPN の基本と仕組み", 秀和システム, 2002.
7)S. Kent, R. Atkinson, "Security Architecture for the Internet Protocol", RFC 2401, 1998.
8)中國 真教, "セキュアなネットワーク環境の構築",宮崎大学情報処理センター広報, Vol. 12, pp. 38-46, 2002.
9)ASH Multimedia Lab., "BIND", SOFT BANK Publishing, 2002.
10)TightVNC, http://www.tightvnc.com/.
11)OpenSSH, http://www.openssh.com/.
12)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).