本資料について

- 本資料は下記文献を基にして作成されたものです．文書の内容の正確さは保障できないため，正確な知識を求める方は原文を参照してください．

- 著者：三代沢　正　厚井　裕司　岡崎　直宣　中谷　直司　亀山　渉
- 文献名：中継サーバを設けたセキュアな遠隔支援システムの開発と展開
- 出展：情報処理学会論文誌 Vol. 48 No. 2 pp.743-754
- Feb. 2007

中継サーバを用いたセキュアな遠隔支援システム

名城大学　理工学部

若原　宏太

はじめに

- 近年，広帯域のアクセス回線が普及
  - 企業，家庭でのインターネットに常時接続する環境
- ユーザの多くはPCやそのソフトウェアを購入したものの，なかなかその活用ができない
- ウイルスやDoS攻撃等のインターネット上での安全に対するさまざまな脅威

適切な安全対策が強く求められる

- しかし，安全対策は初期ユーザにとっては有効な対策がたてられていない

はじめに

- 初期ユーザでもPCを利用して各種ソフトウェアの操作やトラブルの解決，保守等の支援を低コストで手軽に安心して受けられる

  →リモートアクセス技術　遠隔操作機能

- 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ユーザ支援
  - VNC（Virtual Network Computing）
    - しかし，現在のVNCはネットワークの設定や画面の制御が複雑
    - 初心者にはレジストリ操作によるパラメータ設定が困難
    - ユーザ管理機能が実装されていない
      - 大規模なシステムを構築しにくい

既存リモートアクセス機能の比較

- 既存の主要なリモートアクセスソフトウェア
  - WindowsXPリモートデスクトップ
  - WinVNC

- リモートアクセス機能の要件

(1)ユーザ/支援者の同時操作

ユーザと支援者が画面を共有して，同時に作業を進められる．

(2)簡単操作

ユーザにはソフトウェアのインストールからリモートアクセス機能の利用まで極力単純な操作しか受け入れられない．NAT,FW,プロキシサーバに関連したネットワークの設定等は苦手．

(3)支援時の安全性

不正アクセス対策として登録されたユーザ/支援者以外の接続を拒否，通信内容を暗号化する対策を行う必要．ユーザは，支援者がリモートアクセスする機能レベルを選択可能

比較項目	リモート デスクトップ	WinVNC
(1)同時操作	×	○
(2)簡単操作	×	×
(3)支援時の安全性	×	×

モデル構築

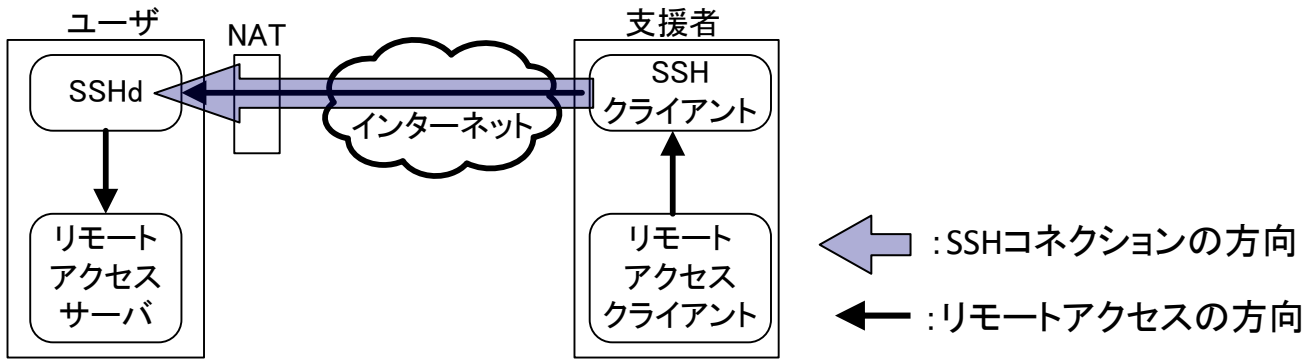
- ユーザ側のPCがNAT，FW，プロキシサーバを経由してインターネットに接続された場合，インターネットを利用している支援者はこれらのネットワーク機器を越えてユーザのPCにリモートアクセスする必要.
- ユーザにとってこれらの存在をなるべく意識することなく，困ったときにすぐに支援を得られることが望ましい.

- リモートアクセスソフトウェアとしてVNC等を使い，アプリケーションによるトンネリングにより，ネットワーク機器の乗り超えをするモデルを構築する.

モデル1

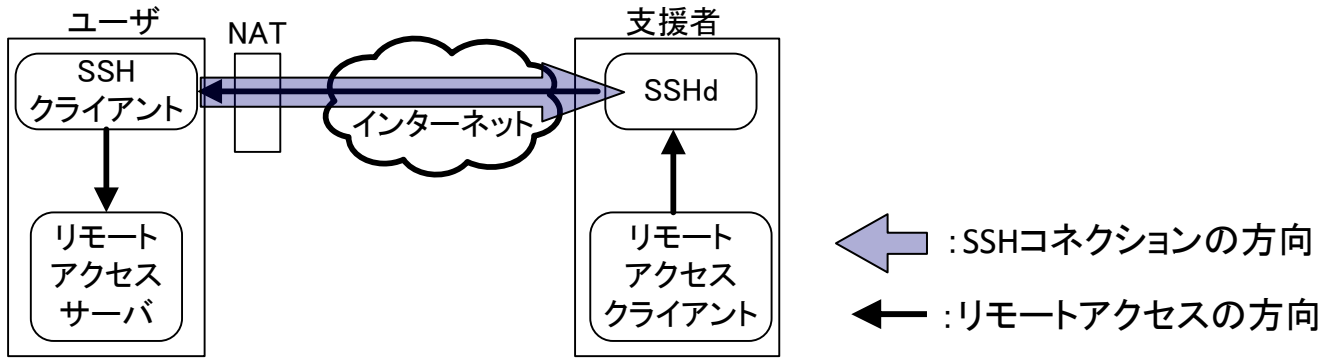
- SSHにはポート転送と呼ばれるほかのアプリケーションの通信を暗号化して安全に通信を行うためのトンネリング機能がある.
- リモートアクセスソフトウェアのサーバ側にSSHサーバ（SSHd）を設置するモデル

- しかし，このモデルをそのままユーザ支援に利用すると，ユーザ側にSSHサーバを設置する必要
- SSHサーバのIPアドレスが変わるたびに支援者に伝える必要
- ユーザのPCがNAT，FWの内側にある場合，外部からSSHによるコネクションが確立できない



モデル2

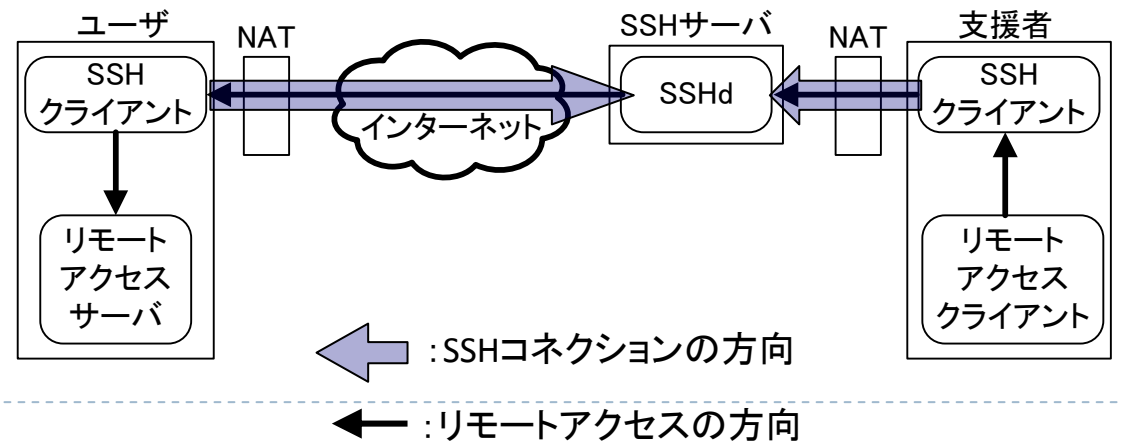
- モデル1に対して，逆方向のSSHポート転送を用いるモデル
- リモートアクセスクライアントソフトウェア側にSSHサーバ（SSHd）を設置
- リモートソフトウェアのサーバへの接続はNATの内側から一度SSHのコネクションを確立した後に通信を行うため，ユーザのPCがNATやFWの内側にある場合でも問題なく接続



モデル3

- SSHサーバをNATやFWの内側に設置すると，ユーザまたは支援者がリモートアクセスが行えない
- IPアドレスが変更されるたびに，SSHクライアントの接続先の設定を変える必要がある

- SSHサーバをユーザ，支援者とは別の場所に分散配置し，これを“リレイ”として用いるモデル



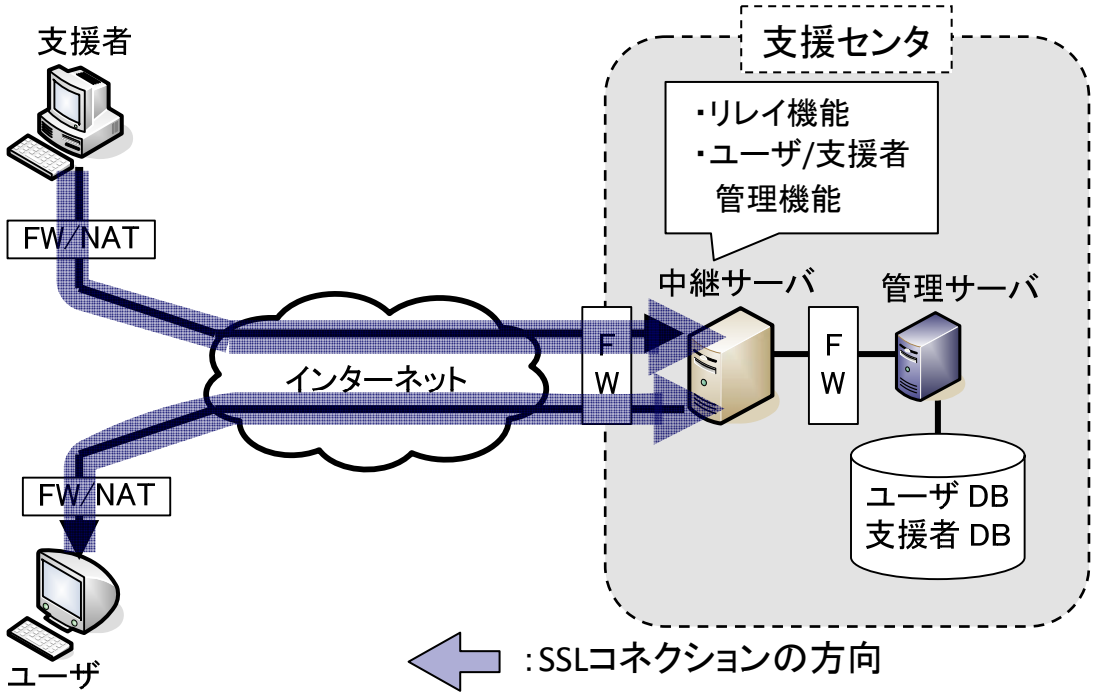
モデル4

- 企業などの組織内部から外部への通信
  - プロキシサーバがよく用いられる
    - 対象プロトコル→ほとんどの組織ではHTTPやHTTPSが一般的

- このような環境の組織内に所属するユーザ，支援者がリモートアクセス機能を利用
  - モデル3を前提に，ユーザ，支援者のクライアントソフトウェアをHTTPSに対応
    - プロキシサーバを乗り越える

遠隔支援システムの提案

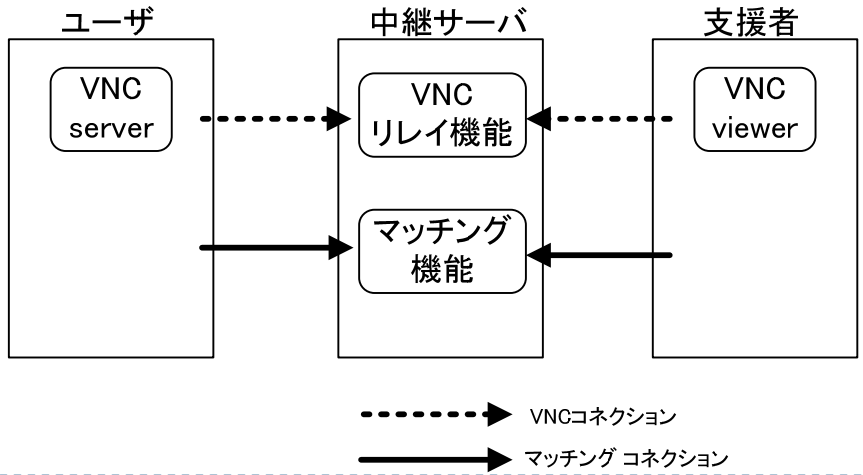
- モデル4をベースに中継サーバを“リレイ”として使い通信路はSSL（Secure Socket Layer）で暗号化
  - プロキシサーバの乗り越え
  - アプリケーションにより暗号化が容易



遠隔支援システム

- 支援者の選択
  - ユーザは問題解決に適した支援者を選択可能

- ユーザは中継サーバのマッチング機能にマッチングコネクションを張る
  - 支援者リストが表示され適した支援者を選択
- 支援者と中継サーバのマッチング機能間にコネクションが張られる
- 支援者がユーザからの依頼を受け付けるとVNCコネクションが支援者とユーザに対応したVNC ViewerとVNC Server間に接続



遠隔支援システム

- NAT,FW,プロキシサーバの乗り越え
  - 中継サーバにマッチング機能とVNCリレイ機能を配置
  - 全てのコネクションの向きをユーザまたは支援者から中継サーバへ接続する
    - 中継サーバは接続先がユーザ/支援者か，コネクションがマッチングコネクション/VNCコネクションにかかわらず，同一の接続処理

たとえば，

- マッチングコネクション　　:443番ポート
- VNCコネクション　　:80番ポート

} 各々のプロトコルをSSLで暗号化したHTTPSに対応付け

遠隔支援システム

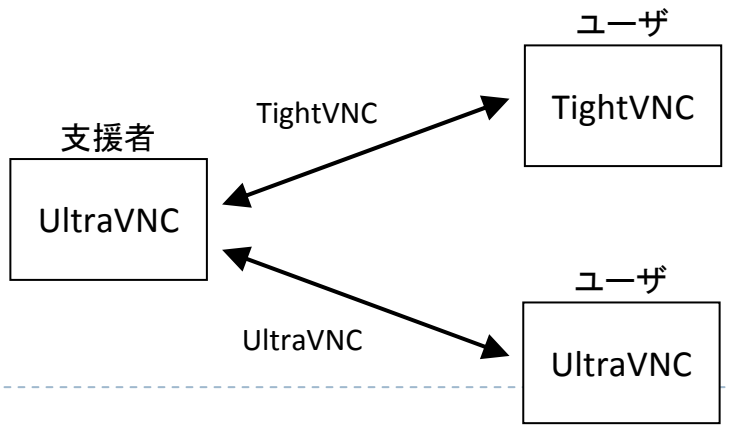
- 遠隔操作支援者の操作レベルの設定
  - 通常モード
    - どんな制限もなく，支援者はマウスとキーボードで遠隔操作可能
  - 見るだけモード
    - 支援者の全ての遠隔操作を無効
    - 支援者はユーザの画面を見るだけ

従来のVNCから，これらのモード選択はレジストリの変更で可能であったが，
ユーザに簡単にできるようにダイアログを設ける

遠隔支援システム

- 2種類のVNCソフトウェアの提供
  - VNCの種類
    - オリジナル：RealVNC
    - 転送速度向上：TightVNC
    - TightVNCにファイル転送機能等を追加：UltraVNC
- 支援者側　　：UltraVNC
- ユーザ　　：TightVNC　or　UltraVNC

※TightVNCとUltraVNCの相互通信はTightVNC相互の機能的範囲で可能



まとめ

- NATやプロキシサーバを，セキュリティを確保しながら　乗り越える遠隔支援システムを開発した
  - SSHのポート転送機能，SSHリモートポート転送を中継サーバに向けて行うモデルを構築
    - NATを乗り越え
  - ユーザ，支援者のクライアントソフトウェアをHTTPSに対応
    - ユーザと支援者間のコミュニケーションをSSLで暗号化
    - プロキシサーバに対応
- VNCには大規模なユーザ管理機能が実装されていないため，ユーザ管理機能の追加実装を行った