Windows Terminal Serviceの安全な使わせ方？

宮本 久仁男 a.k.a wakatono
wakatono@todo.gr.jp

Content.

- Windows Termina Serviceの概要
- WTSを安全に使ってみよう
- おまけ：Desktop VPN使ってみたよ

Windows Terminal Service概要

- Windows Terminal Service(WTS)とは何か
  - 画面転送型のリモートクライアント接続形態の1つ
  - TCP3389番を使う
  - Windows NT Server 4.0 Terminal Server Edition以降で提供
    - Windows Server系OSでは、Windows 2000 Server以降で標準機能となる

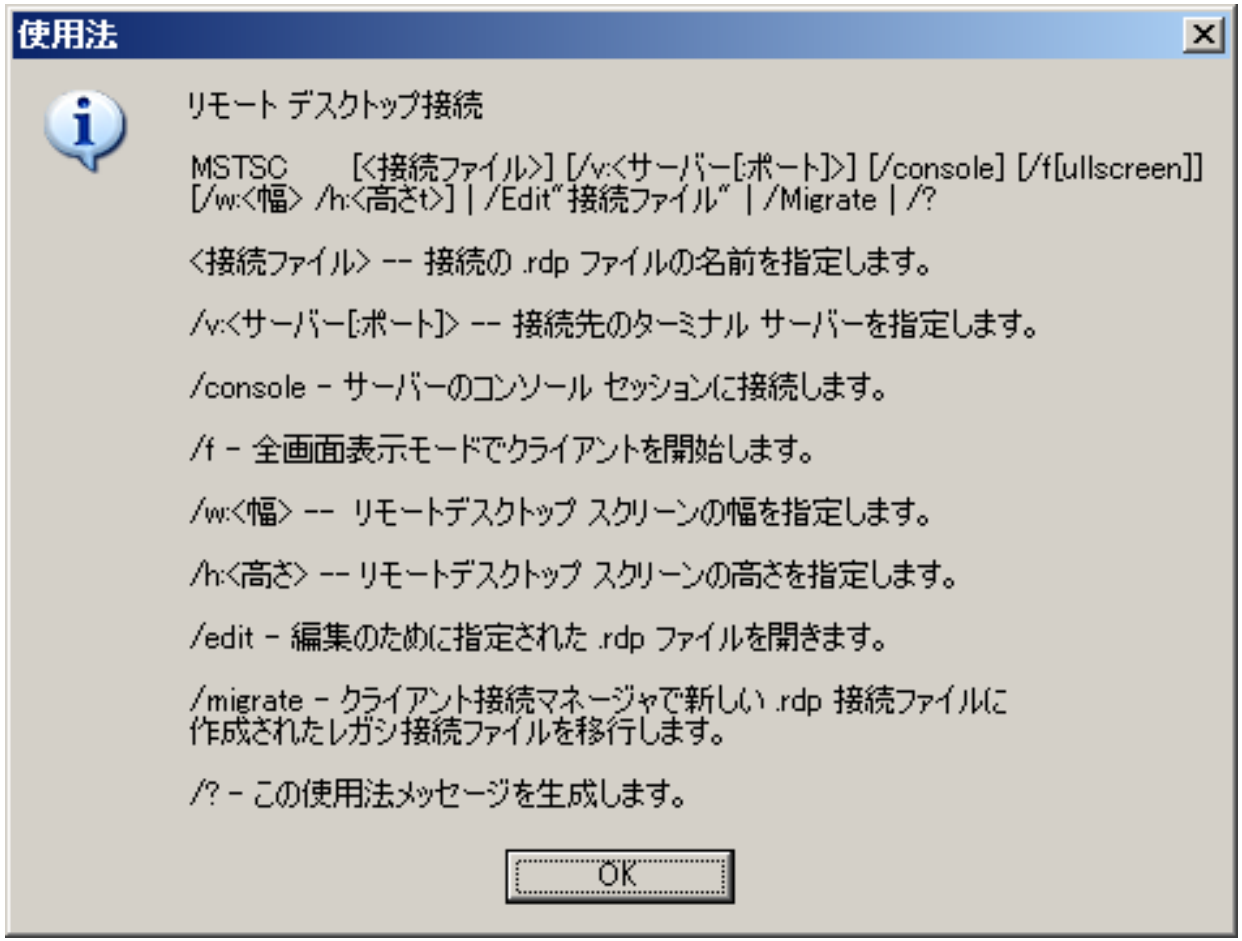
WTSクライアント

- mstsc.exe
  - Windows標準のWTSクライアント
- rdesktop
  - UNIX系OSのためのWTSクライアント
    - オープンソース
- SRC(Sun Remote Connector)
  - SunRay ServerからWTSサービスに接続するためのプログラム
    - 商用

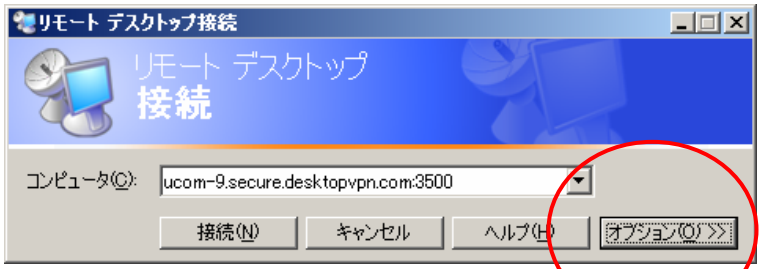
mstsc.exeで使える機能

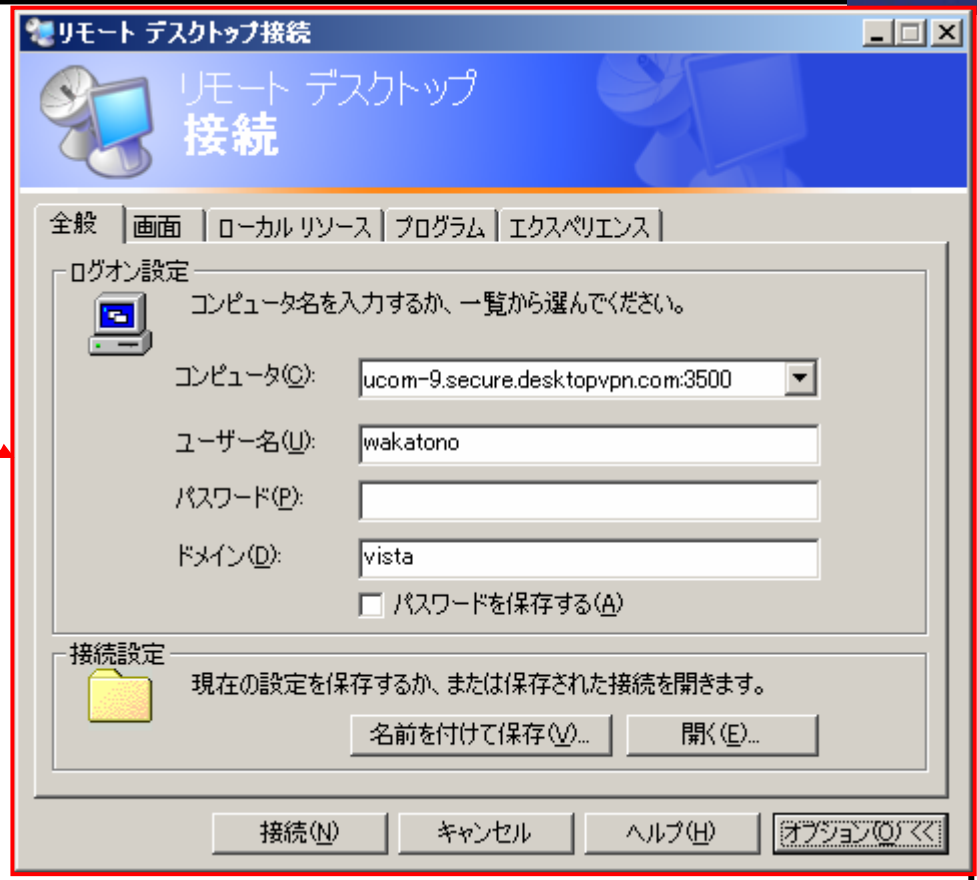
- 設定ファイルの作成／編集
- 接続先サーバ&ポート番号の指定
- 画面サイズの指定
- etc…

mstsc.exe /? を実行すると？



一応接続時のUIを再掲すると





- いろいろ設定は可能
- サーバ名＋ポート番号で、任意のポート番号での待ち受けに対応
  - さらなる設定項目はないのか？

RDP設定ファイルの一部

```
screen mode id:i:1
desktopwidth:i:1024
desktopheight:i:768
session bpp:i:16
winposstr:s:0,1,30,-8,1003,716
full address:s:ucom-9.secure.desktopvpn.com:3500
compression:i:1
keyboardhook:i:2
audiomode:i:0
redirectdrives:i:0
redirectprinters:i:1
redirectcomports:i:0
redirectsmartcards:i:1
displayconnectionbar:i:1
autoreconnection enabled:i:1
username:s:wakatono
domain:s:vista
```

- ポート番号などはサーバ名(FQDN)指定に含める

WTSで準備している認証手段

- パスワード認証
  - セットアップ後フツーに使える
- スマートカード認証
  - スマートカードを用いた認証（まんま）

- カジュアルに使うには、パスワード認証を使うしかないが…

Windows Serverを…

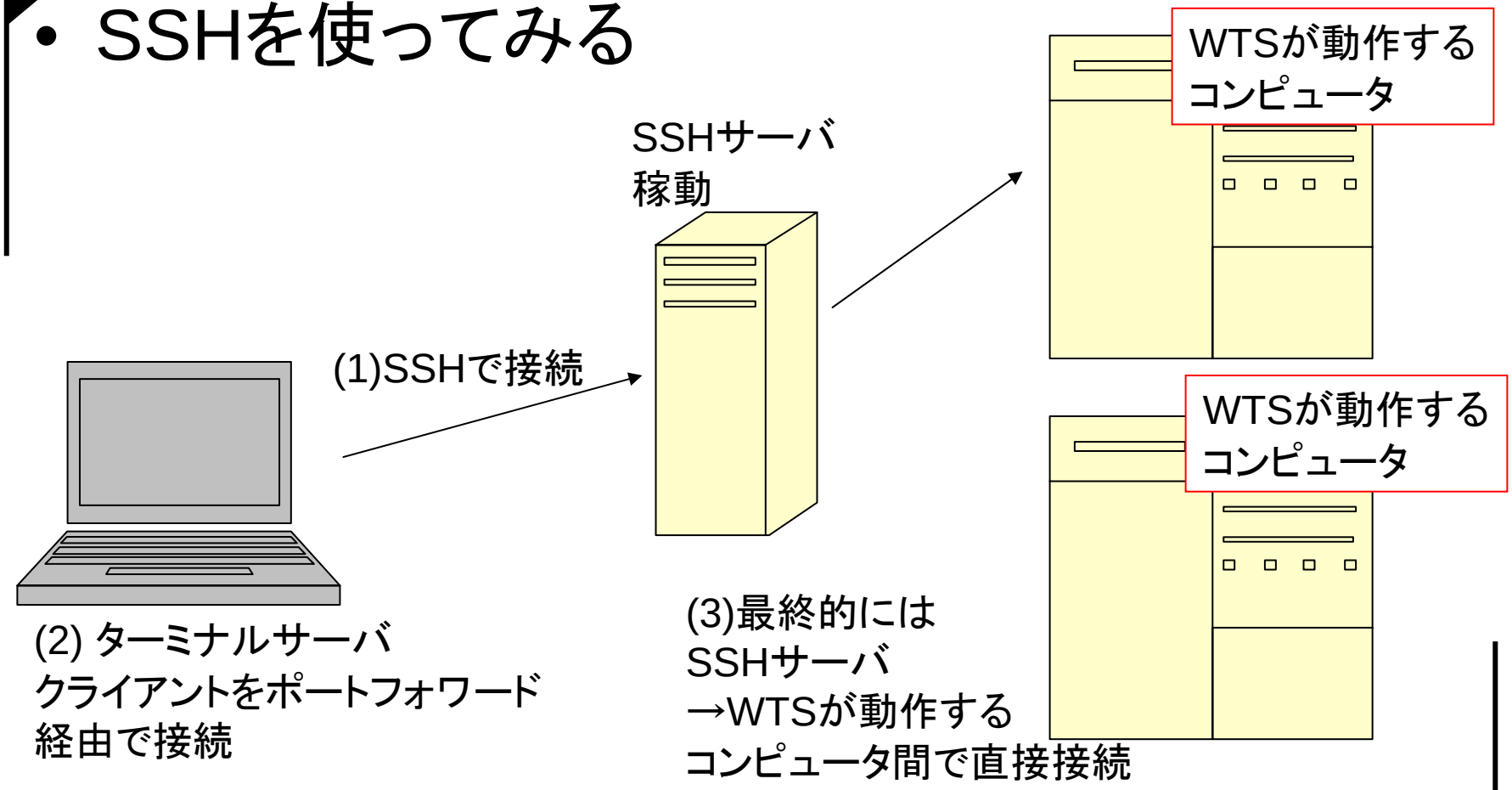
- インターネットに晒すのに抵抗がある人？
- グローバルアドレスを消費したくない人？
- あまりポートを開けたくない人？

- そんな人のための解決方法w

WTSを安全に使ってみよう

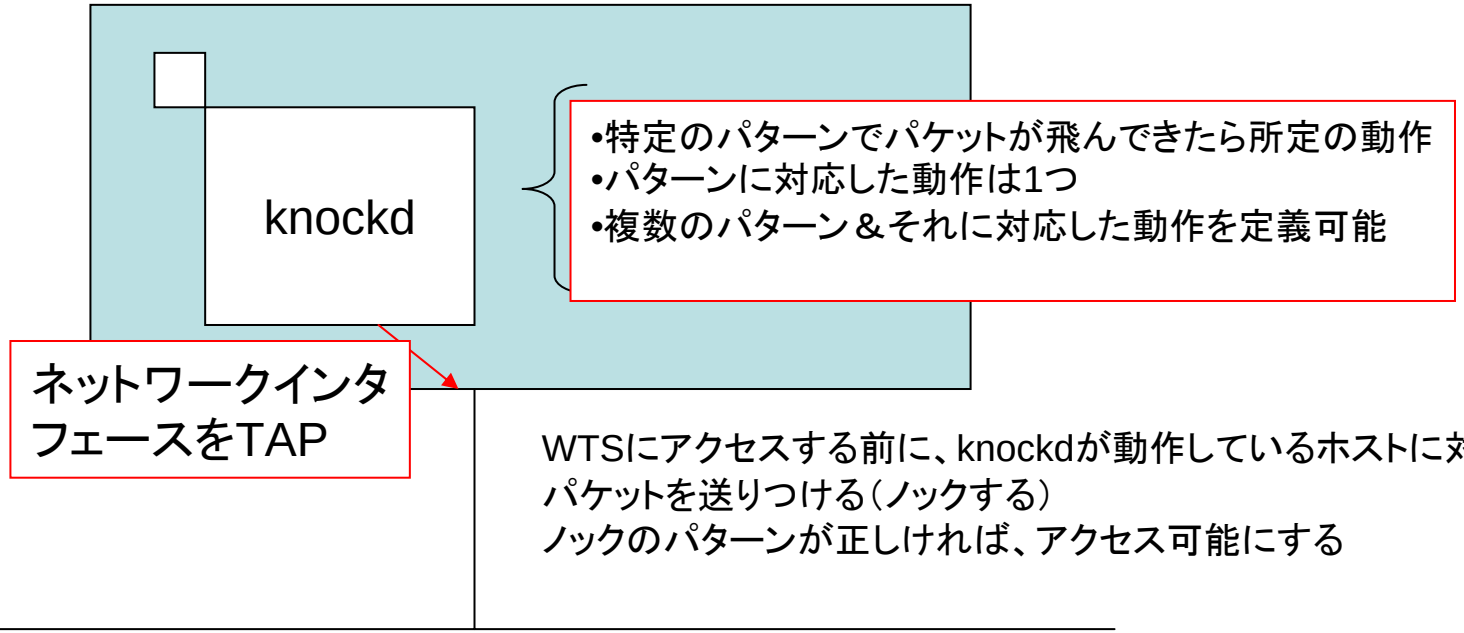
1. Gatewayを使う(1)

- SSHを使ってみる

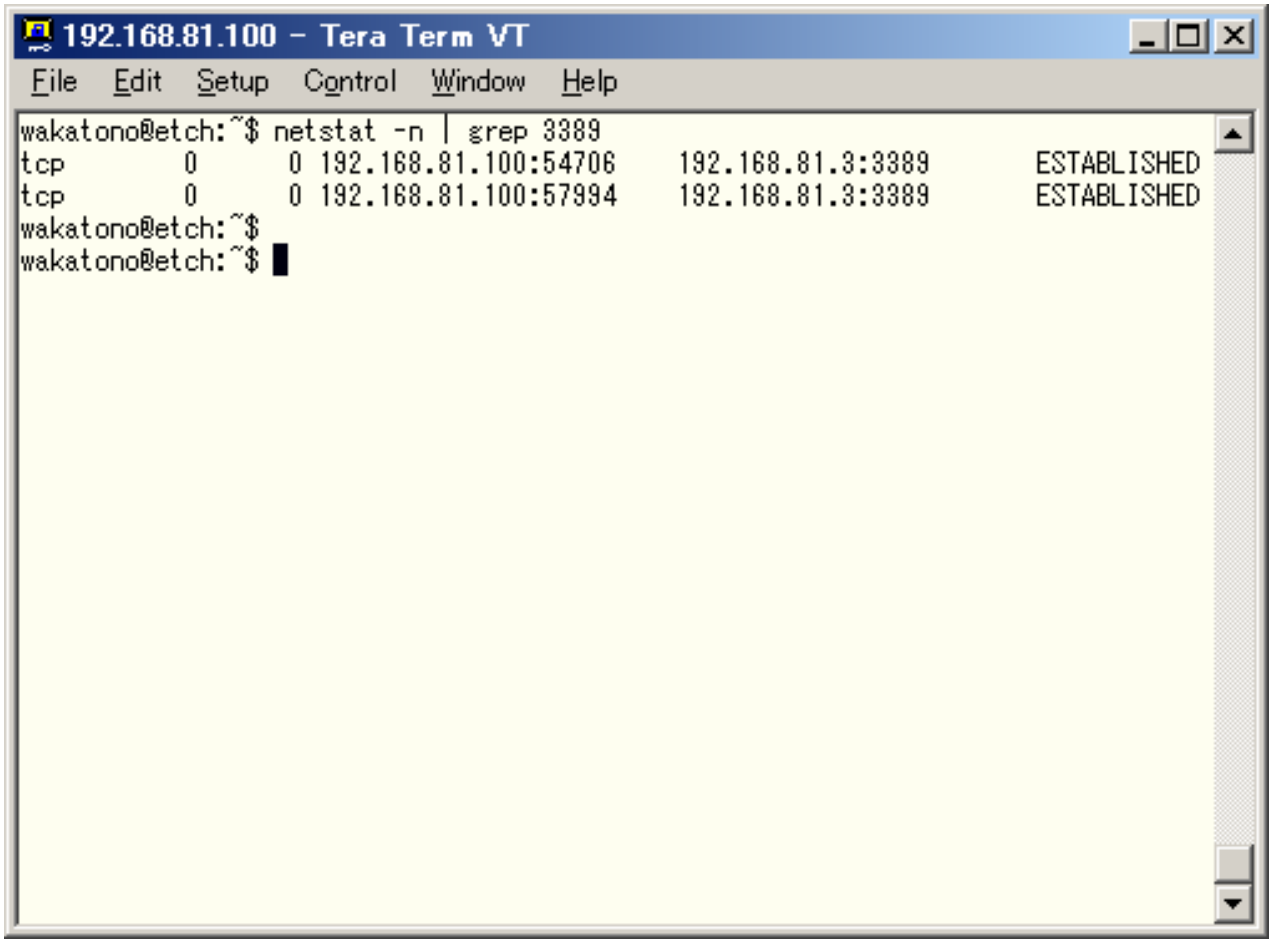


2. Gateway を使う(2)

- knockdを使ってみる



Gateway上の様子



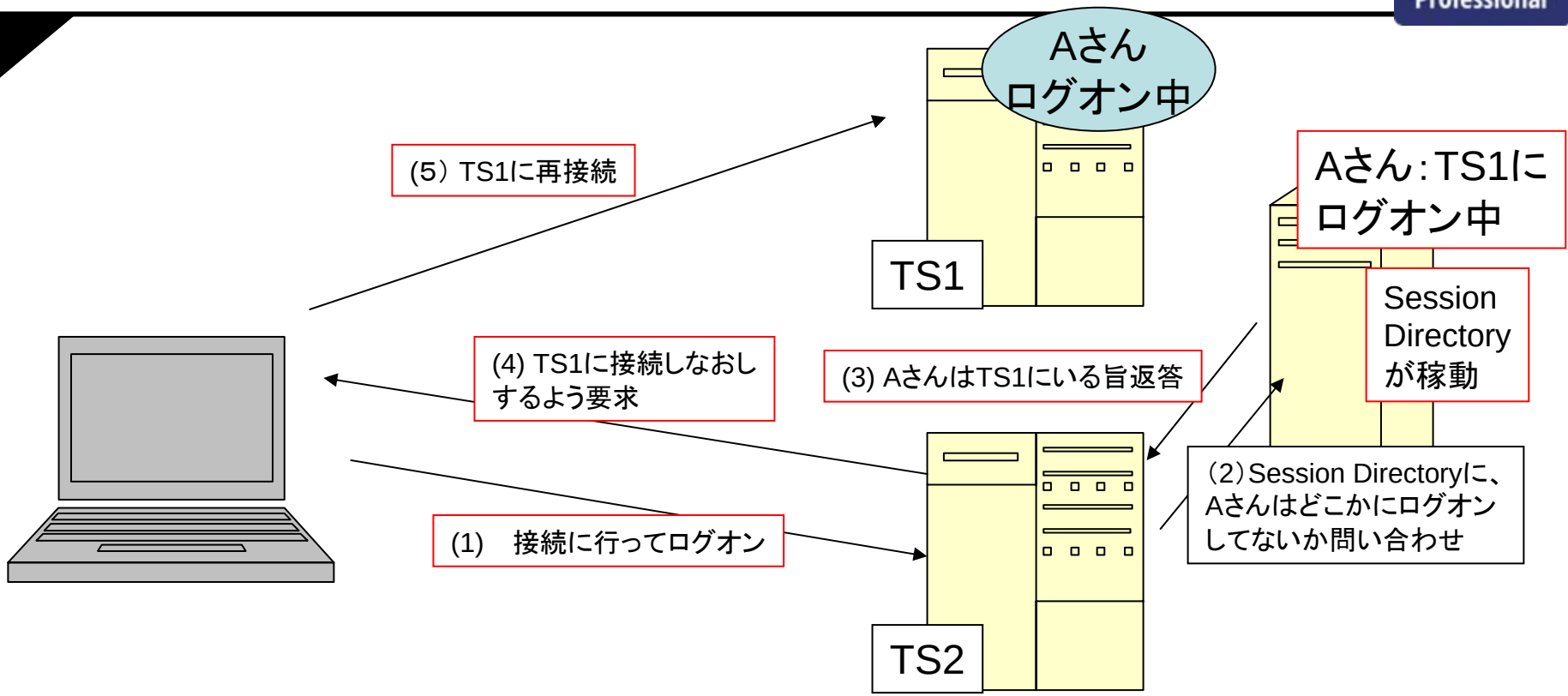
Gatewayを使うことの利点

- 複数のServerに対するクチを絞ることが可能
  - 必要に応じてバックエンドのサーバを増やすことが可能
  - VIPに対する接続をなんとかすれば、NLBとかも併用可能なはず（未検証）
- Windowsの脆弱性にSensitiveにならずに済む
  - 外界からは隔絶されている
- Windows ServerとGatewayのメンテナンスを独立に出来る
  - Gatewayのメンテナンスがあっても、WTS上の処理内容が消えるわけではない

欠点

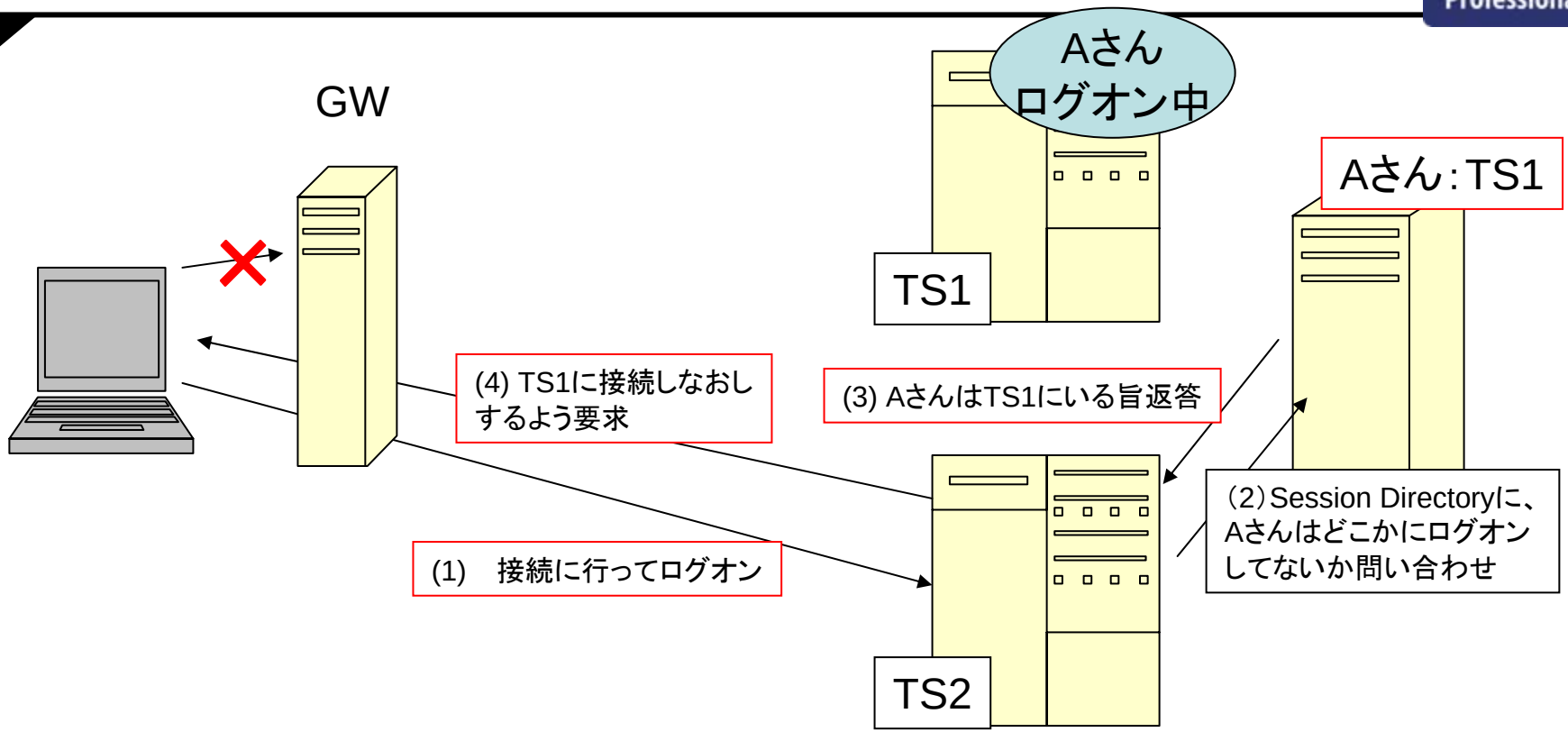
- Gatewayの脆弱性を気にする必要がある
- メンテナンス対象が増える
- 接続手続きが冗長になる
- Session Directoryが使えない
  - 新たな接続先を指定されても、直接接続は出来ない
  - Session Directorを使う場合には、VPNを使えるようにする必要がある

What is Session Directory?



- ユーザがログオンしてるマシンのデータベース
  - (1)で認証完了すると、(2)～(5)は自動で行われる
  - ドメイン構成は必須

何がまずい？



- (4)で通知した接続先につなげない
  - GW経由でつなぐので…

3. Windows Server単体で(1)

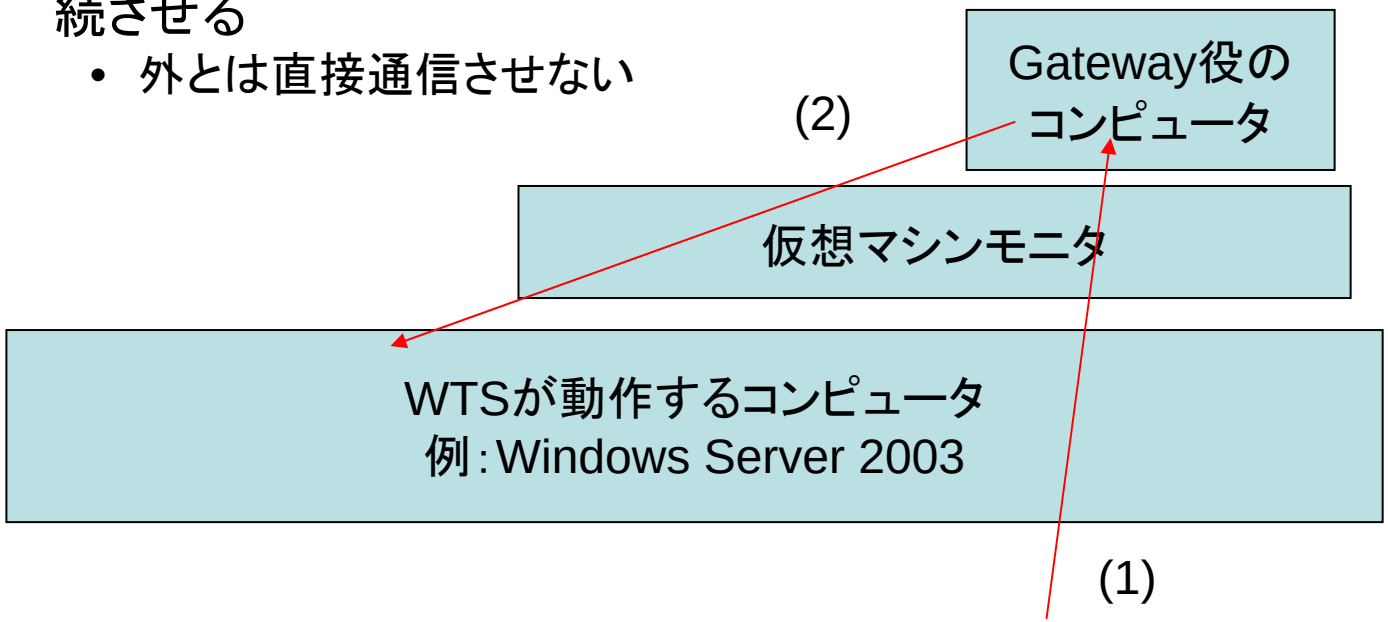
- 必要ないポートは全部「外からは」閉じる
- GatewayをWindows Server上のサービスとして構成する
  - あまりお勧めはしません
  - 派生系は後述

4. Windows Server単体で(2)

- IPsec+L2TPを使う
  - IPプロトコル番号50番、UDP4500番、UDP500番を解放
  - ISPによってはMTU問題が出てくる可能性あり
- PPTPを使う
  - 当たり前すぎるのでパスw
- 注意：IPsec「だけ」に頼ってはならない
  - IPsecはあくまで「端末認証」にのみ使用可能
    - ユーザの正当性はIPsecだけでは保証できない

5. Windows Server単体で(3)

- 1や2の構成を、VM上で実現する
  - KnockdやSSHサーバが動作するコンピュータをVMにホストし、外部との通信を行う
  - WTSが動作するコンピュータへは、Gateway役のコンピュータから接続させる
    - 外とは直接通信させない



結論

- どこでラクをしたいか見極めることが必要
  - Windowsそのもののメンテナンスを考慮
    - Windowsマシンのダウンタイムがどこまで許されるか
  - Gatewayのメンテナンスを考慮
    - Gatewayのダウンタイムがどこまで許されるか
- ゲートウェイは悪くない選択肢
  - WTSへの接続はポート1つだけで完了するため、SSHのポートフォワードなどとは相性がよい
    - SSHは公開鍵認証必須
  - 接続手順は若干わずらわしくなる
    - ツールを適切に選ぶことで、ほとんど気にはならなくなる

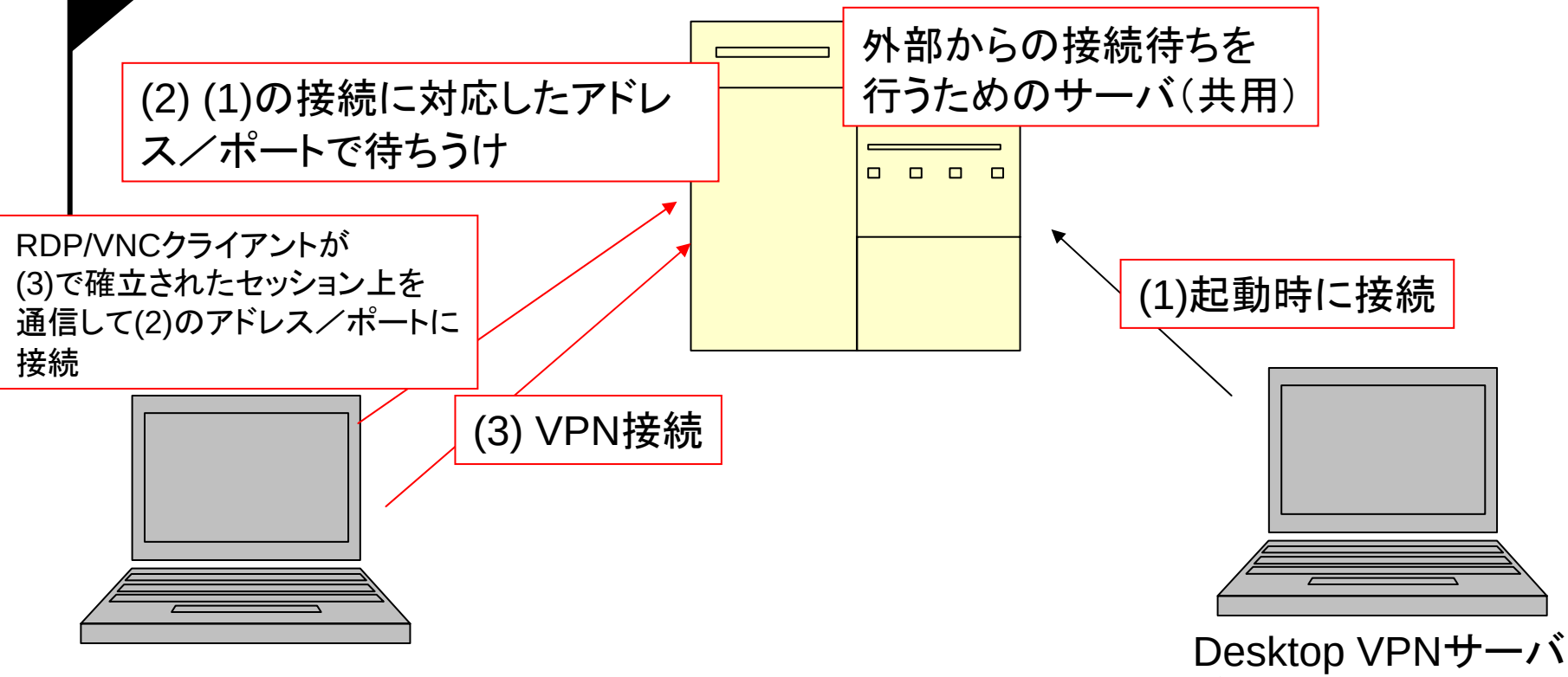
おまけ：Desktop VPN 使ってみたよ

具体的にはどんなのだろ？

Desktop VPNって何？

- ソフトイーサ社が開発中の、RDP/VNCベースの（安全に）リモートデスクトップを用いるためのシステム
- 現在beta1を配布中
- RDPではなくVNCを使うことで、Windows 98などの（古い）Windows系OSにも対応

実態は？



- RDP/VNC + ASP型のVPNサービス

現状でDesktop VPNを使うための条件

- Desktop VPNサーバから外部に接続できること
  - Proxy経由でもOK
- クライアントから外部に接続できること
  - Proxy経由でもOK
- Desktop VPNサーバとクライアントが接続に行くサーバへのアクセス制限がかかっていないこと

懸念事項

- いわゆるイントラネットに存在するPCでDesktop VPNサーバを動かして、外部から接続を許してしまう可能性
  - 管理されない接続が発生する懸念
- その他、コンピュータの（Desktop VPNで使う）IDが推測される懸念
  - 容易に推測可能な文字列＋数字なので…

通信を止めるためには？

- Desktop VPNサーバから外部のサーバへの通信を止める
  - アドレスを調べてフィルタリングを行うなど
- そもそも好きにソフトウェアをインストールさせない
  - 動作しているプロセスも監視
- 個人にPCクライアントを使わせない
  - やっぱThin Client？