EXA Value Forum 2013
セッション B-4

# クラウド内のサーバーを ハッキングから守る方法
## ～低費用で実現～

2013年7月10日

株式会社 エクサ
開発推進本部 技術推進室
ITプロフェッショナル
谷　文秀

# 目次

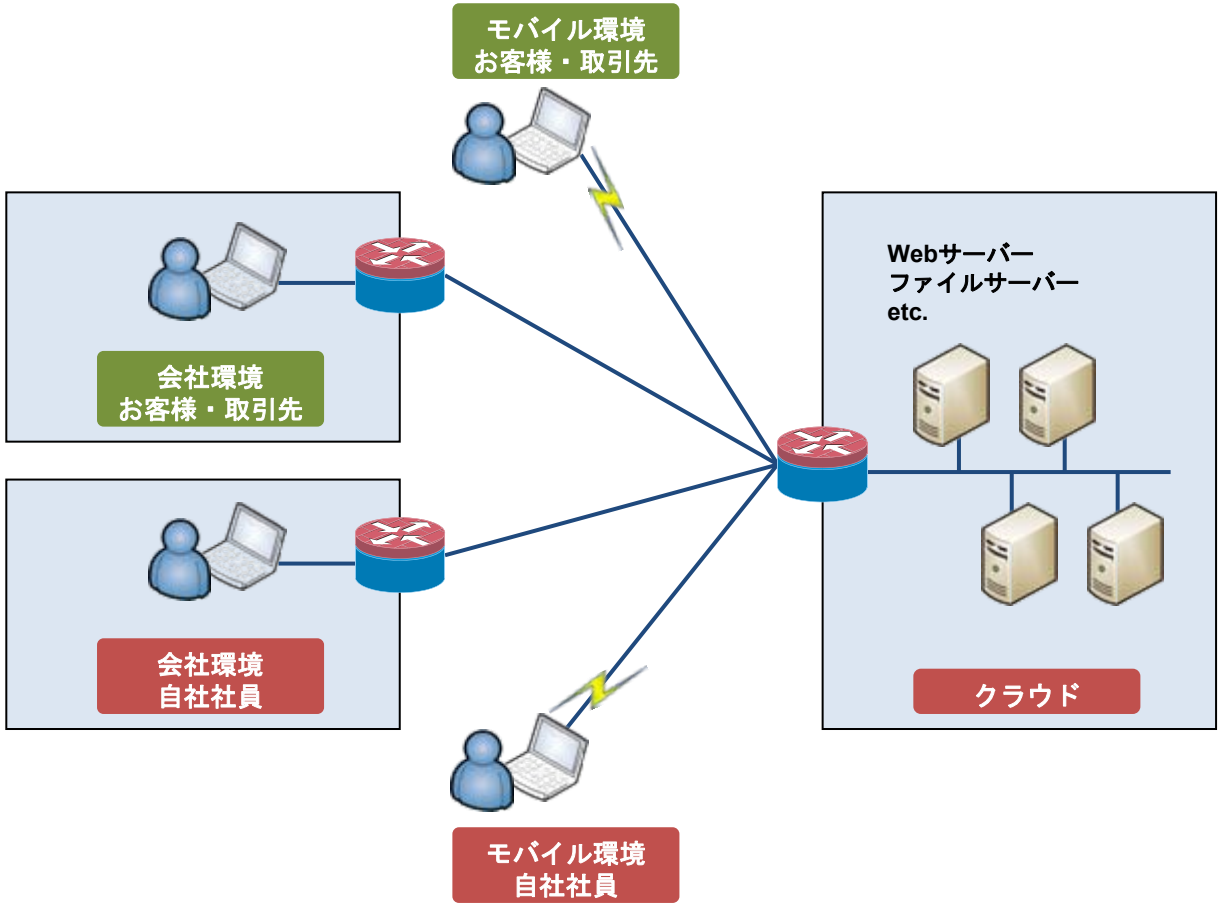
# 1. はじめに

- 昨今、自社にサーバーを置かず、クラウドサービスを利用しようとする企業が増えています。
- 自社のデータセンターをクラウド化するのであれば、従来のように、自社とクラウド間を専用線やVPNで接続するのが普通だと思います。
- しかし、専用線やVPNといった回線を用意するにはかなりの時間や費用がかかり、維持費用もかかります。
- システム規模が小さくて回線に費用をかけられない、クラウドを使ってサービスを早急に立ち上げる必要があるといった場合は、クラウド標準のインターネット接続でサーバーを利用、保守しなければなりません。
- いっぽうで、インターネット接続のクラウドは、ハッカーによる不正アクセスの格好の対象となっているのが実態です。
- 本講演では、こういった不正アクセスに対し、費用をかけずに実施できるセキュリティ対策を紹介します。

# ２．クラウドの利用形態と接続方法

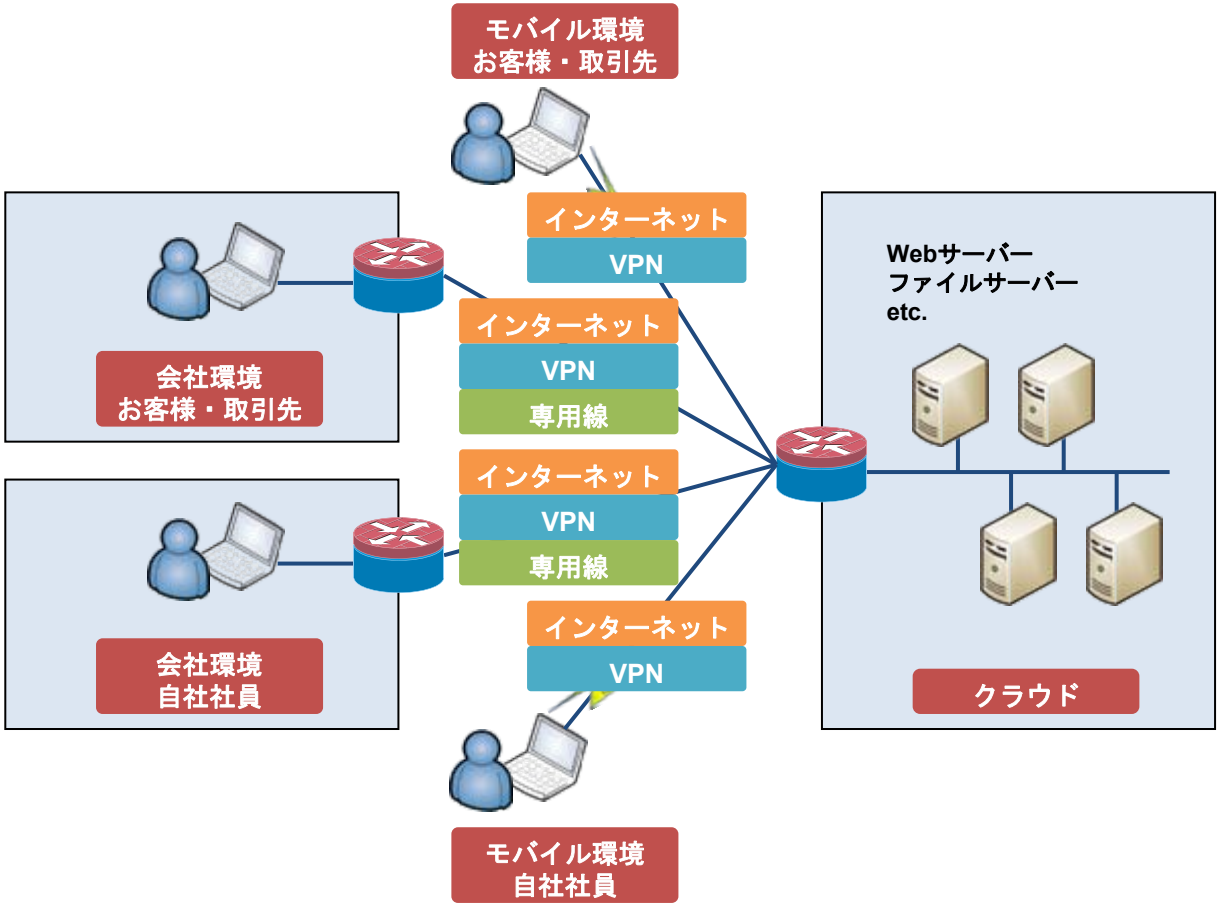
# 2. クラウドの利用形態と接続方法
## 2.1. サーバーの利用形態

- 自社専用のサーバー
- お客様や取引先向けのサーバー（公開サーバー）
- 取引先と自社を連携させた業務用のサーバー（限定公開サーバー）



# 2. クラウドの利用形態と接続方法
## 2.2. サーバーへの接続方法

- インターネット
- インターネットVPN　※以降、VPNと略します
- 専用線（広域イーサネット網/IP-VPN網）



# 2. クラウドの利用形態と接続方法
## 2.3. クラウドベンダーが提供する接続方法

- インターネット　※どのベンダーも基本はこれです。
- VPN　※ベンダーによって方式が異なります。

| クラウドベンダー | VPN接続 | 専用線接続 |
|---|---|---|
| Amazon EC2 | IPSec VPN（オプション、Amazon VPC） | AWS Direct Connect（オプション） |
| Nifty Cloud | IPSec VPN（オプション、VPNルーターが必要） | 専用線･閉域網接続サービス（オプション） |
| IDCフロンティア<br>パブリッククラウド セルフタイプ | L2TP/IPSec VPN 事前共有かぎ方式（標準） | プライベートコネクト（オプション） |
| NTTコミュニケーションズ Cloud$^{n}$ | L2TP/IPSecVPN（標準） | ー |
| GMO クラウド Public | OpenVPNの設定方法を公開（標準） | ー |
| BIGLOBE クラウドホスティング | SSL VPN（オプション）<br>IPSec VPN（オプション、VPNルーターが必要） | 専用線接続サービス（オプション） |

# 2. クラウドの利用形態と接続方法
## 2.3. クラウドベンダーが提供する接続方法

- インターネット　※どのベンダーも基本はこれです。
- VPN　※ベンダーによって方式が異なります。
- 専用線

| クラウドベンダー | VPN接続 | 専用線接続 |
|---|---|---|
| Amazon EC2 | IPSec VPN（オプション、Amazon VPC） | AWS Direct Connect（オプション） |
| Nifty Cloud | IPSec VPN（オプション、VPNルーターが必要） | 専用線･閉域網接続サービス（オプション） |
| IDCフロンティア<br>パブリッククラウド セルフタイプ | L2TP/IPSec VPN 事前共有かぎ方式（標準） | プライベートコネクト（オプション） |
| NTTコミュニケーションズ Cloud$^{n}$ | L2TP/IPSecVPN（標準） | ー |
| GMO クラウド Public | OpenVPNの設定方法を公開（標準） | ー |
| BIGLOBE クラウドホスティング | SSL VPN（オプション）<br>IPSec VPN（オプション、VPNルーターが必要） | 専用線接続サービス（オプション） |

- 専用線、VPNは、セキュアな通信が行えますが、利用開始まで時間がかかり、費用もかなりかかります。（特に専用線）

| 比較項目 | 専用線 | VPN | インターネット |
|---|---|---|---|
| 回線は安定しているか | ○ | △ | △ |
| セキュアな通信手段か | ○ | ○ | × |
| 費用は安いか | × | △～× | ○ |
| すぐに使えるか | × | △～× | ○ |

## 2.4. 接続方法と課題

- 専用線、VPNは、セキュアな通信が行えますが、利用開始まで時間がかかり、費用もかなりかかります。（特に専用線）
- インターネットは、すぐに使えて費用も安いです。しかし、セキュリティ面で不安があります。

| 比較項目 | 専用線 | VPN | インターネット |
|---|---|---|---|
| 回線は安定しているか | ○ | △ | △ |
| セキュアな通信手段か | ○ | ○ | × |
| 費用は安いか | × | △～× | ○ |
| すぐに使えるか | × | △～× | ○ |

# 3. インターネットを使ったアクセスと課題

## ファイアウォールの設定

外部インターネットから、お客様に付与されたグローバルIPアドレスに対する通信を制限するファイアウォールの設定をします。

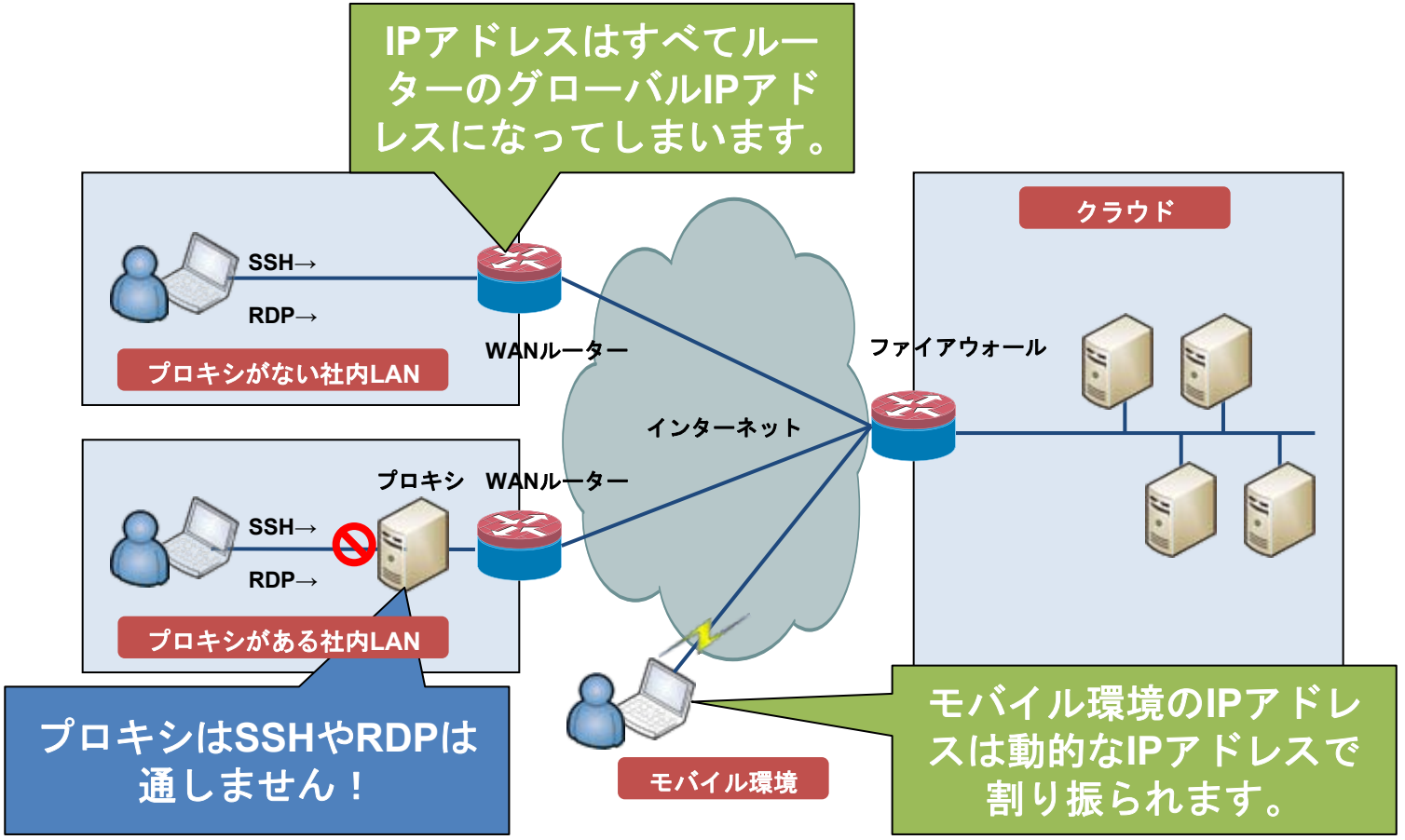
–Linuxサーバーの場合はSSH接続を許可します。
–Windowsサーバーの場合はリモートデスクトップ接続を許可します。
–Webサーバーを公開する場合はHTTP接続、HTTPS接続を許可します。

| プロトコル | ポート番号 | 用途 |
|---|---|---|
| HTTP | 80 | Webアクセス |
| HTTPS（SSL） | 443 | Webアクセス（暗号化通信） |
| SSH | 22 | ターミナルエミュレーター接続 |
| RDP | 3389 | リモートデスクトップ接続 |

SSH接続、リモートデスクトップ接続に関しては、お客様クライアントのソースアドレスが特定可能な場合は、アクセス制限することをおすすめします。

# 3. インターネットを使ったアクセスと課題
## 3.2. 社内LANからの接続とアクセス制限

- プロキシを使っている社内LANからは、プロキシに遮られてSSH接続やリモートデスクトップ接続ができません。
- クラウドにアクセスするクライアントのIPアドレスでアクセス制限をかけることは実際には困難です。

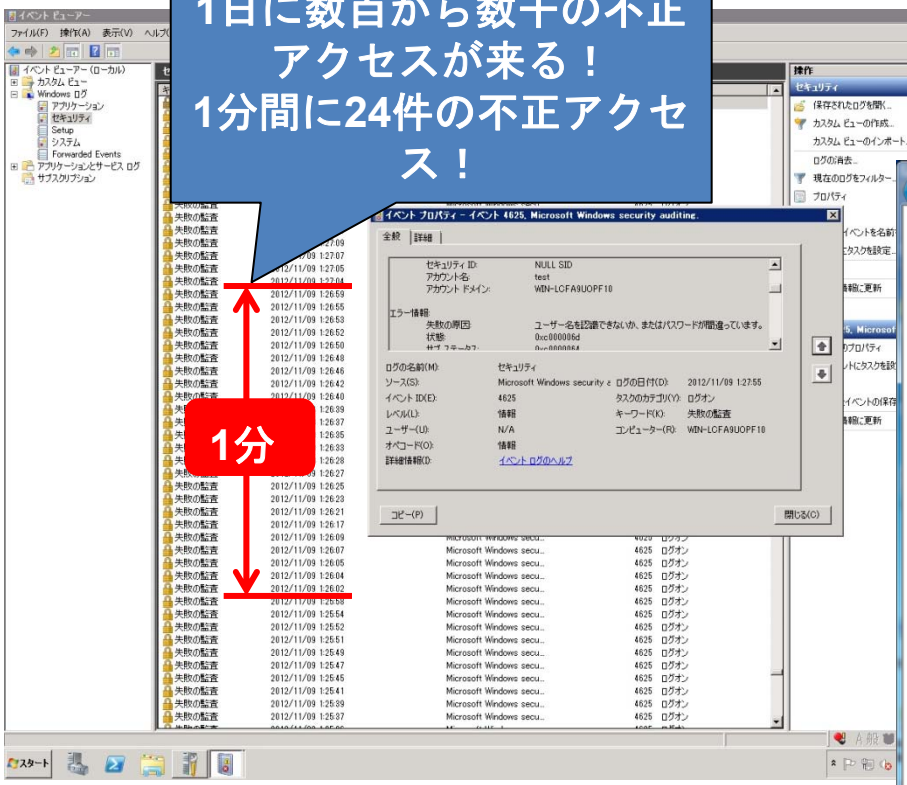


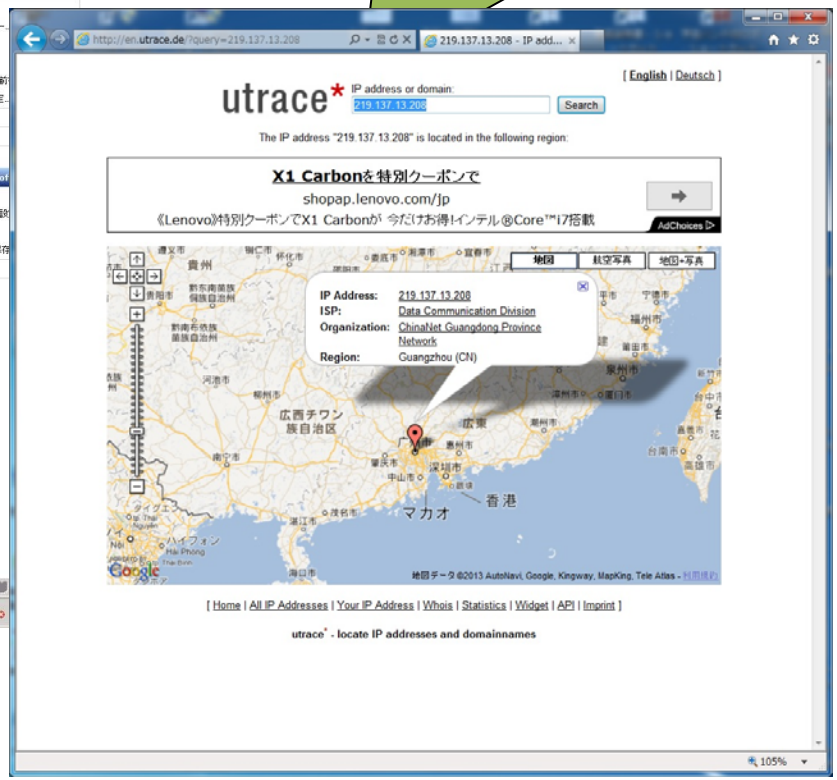
# 3. インターネットを使ったアクセスと課題
## 3.3. 不正アクセス

- パブリッククラウドは、SSH接続やリモートデスクトップ接続のポートに対するインターネットからの不正アクセスが非常に多く、ユーザー認証を突破されるとサーバーを乗っ取られてしまいます。

1日に数百から数千の不正アクセスが来る！
1分間に24件の不正アクセス！

通信元のIPアドレスを調べてみると・・・
中国・米国・欧州・他



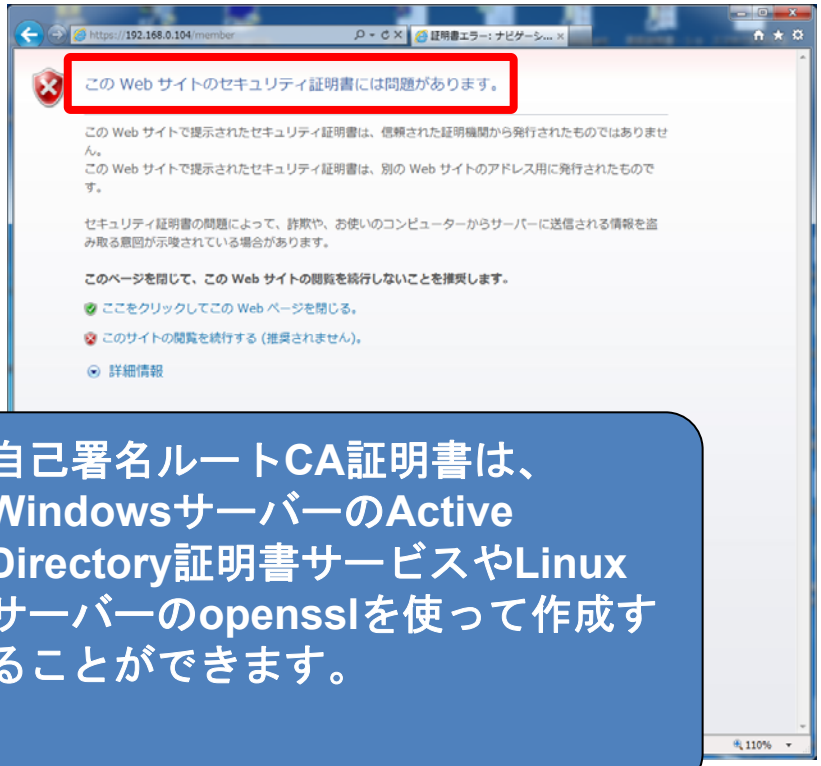
# 4. Webサーバーを立てる際のセキュリティ対策

- 自社の社員が使うシステム
- 特定の取引先･協力会社の社員が使うシステム

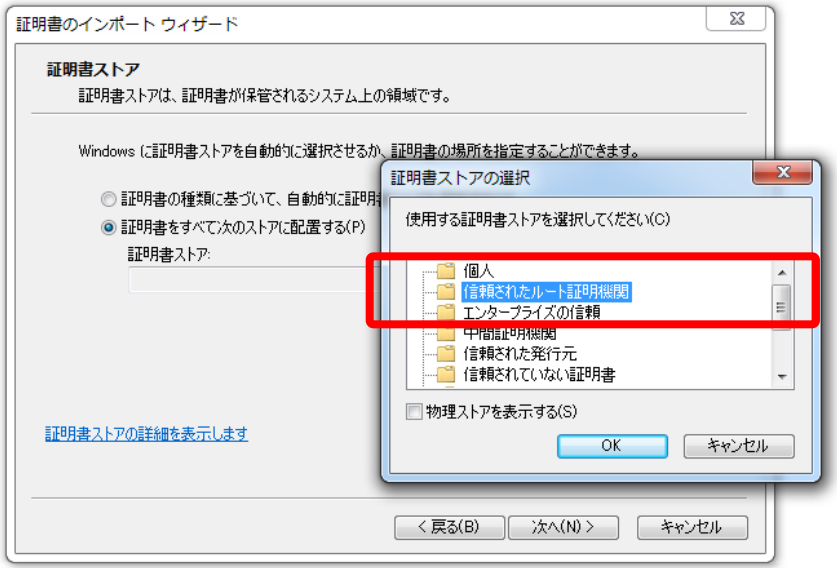
# 4. Webサーバーを立てる場合のセキュリティ対策
## 4.1. 通信の暗号化と自己署名SSLサーバー証明書

- ログイン認証を行うアプリの場合はSSLで通信を暗号化する。
- 自己署名のSSLサーバー証明書を作成し、Webサーバーに組み込む。
- ブラウザの警告を消すには、端末に自己署名ルートCA証明書を「信頼された認証機関」にインポートする。

ポイント



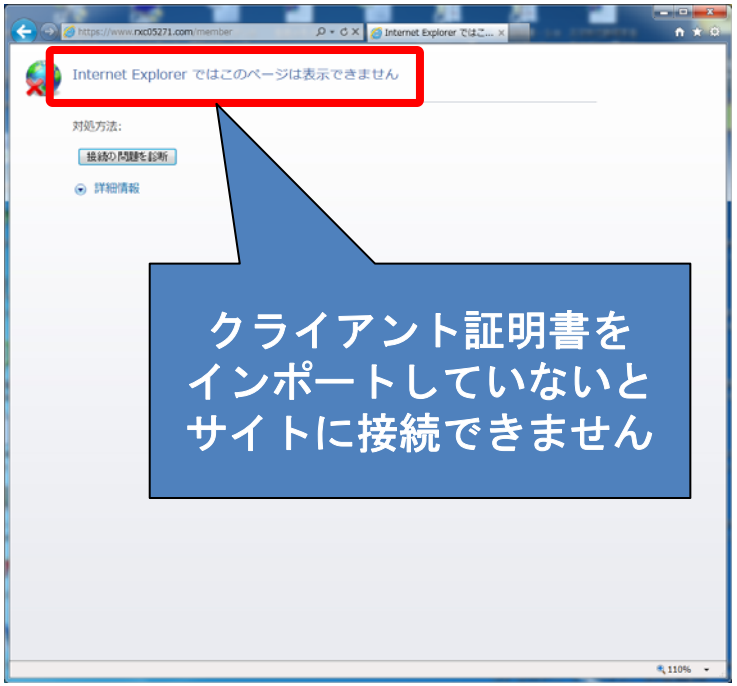

自己署名ルートCA証明書は、WindowsサーバーのActive Directory証明書サービスやLinuxサーバーのopensslを使って作成することができます。

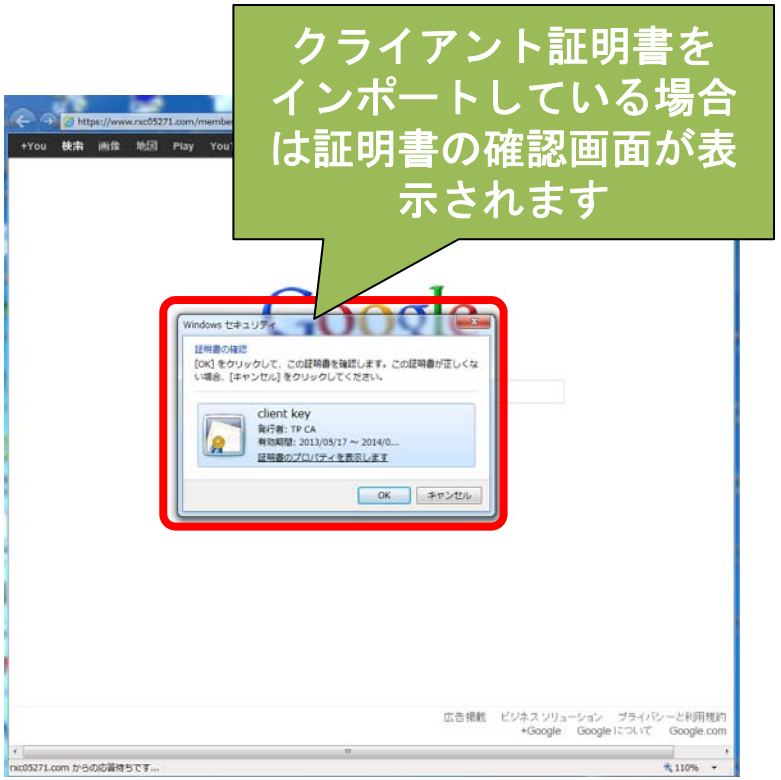


# 4. Webサーバーを立てる場合のセキュリティ対策
## 4.2. アクセス可能なクライアントを制限する

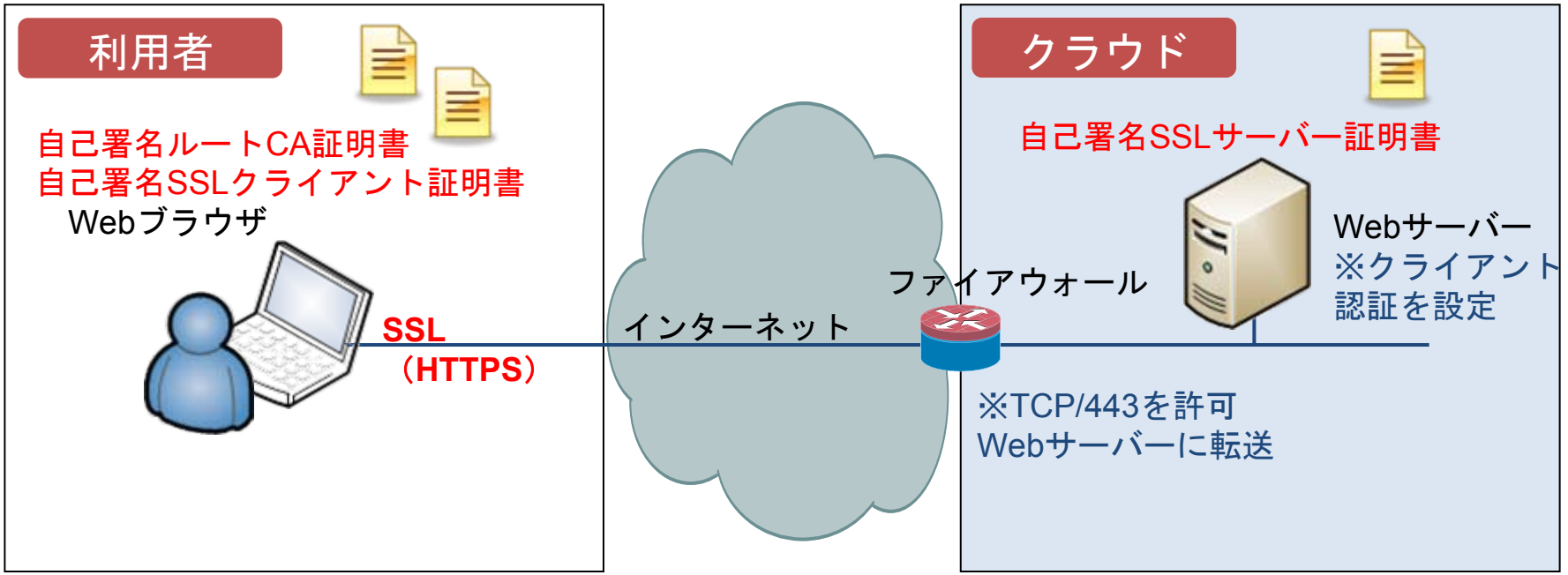
ポイント

- Webサーバー（IISやApache）のSSLクライアント認証機能を使用する。
- 自己署名クライアント証明書を作成し、クライアントにインポートする。
  ※クライアント証明書はActive Directory証明書サービスやopensslを使って作成することができます。



# 4. Webサーバーを立てる場合のセキュリティ対策
## 4.3. SSLクライアント認証概要図

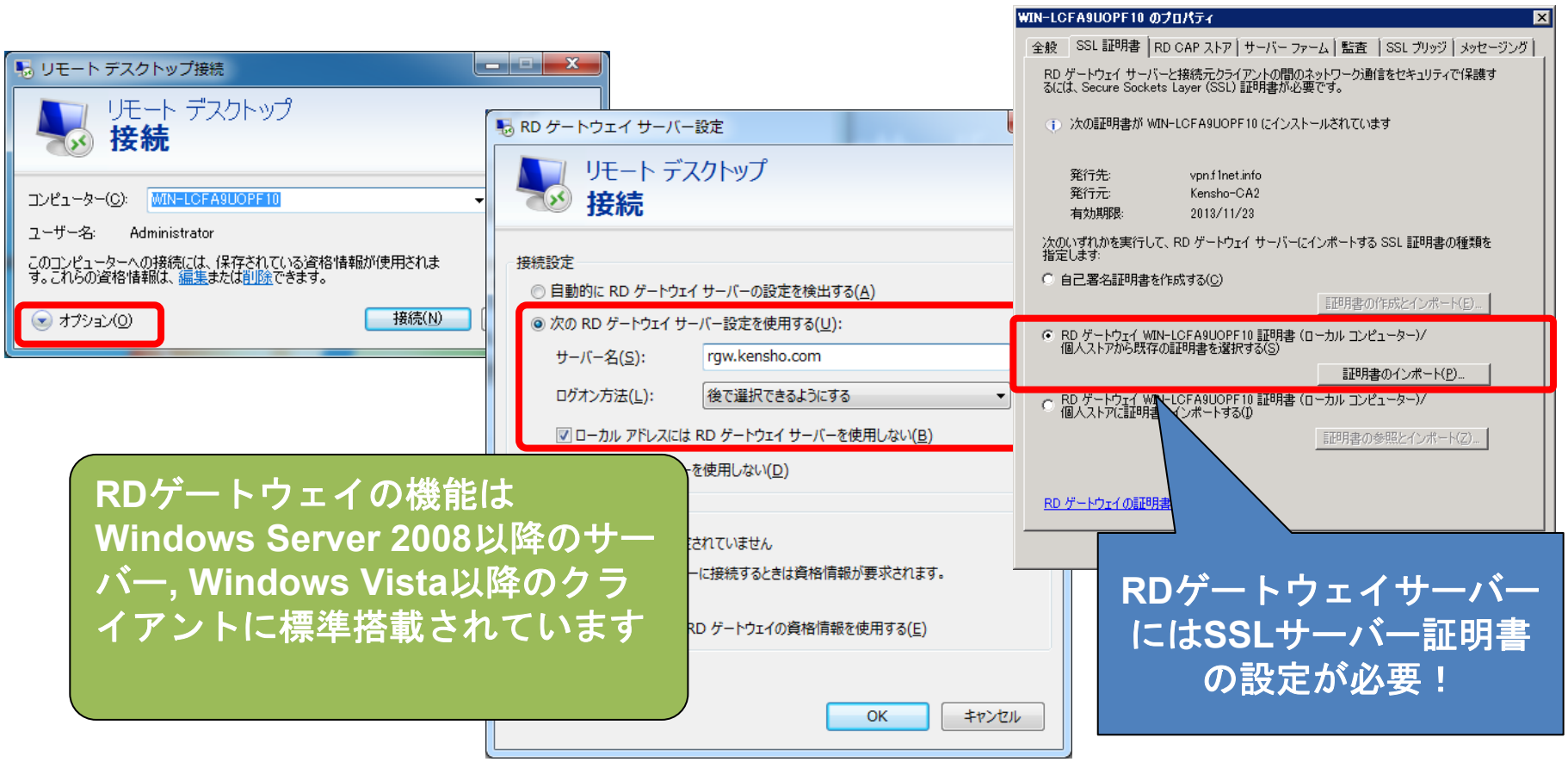


# 5. リモート保守における セキュリティ対策

# 5. リモート保守におけるセキュリティ対策
## 5.1. プロキシ越えでアクセスする（Windows）

ポイント

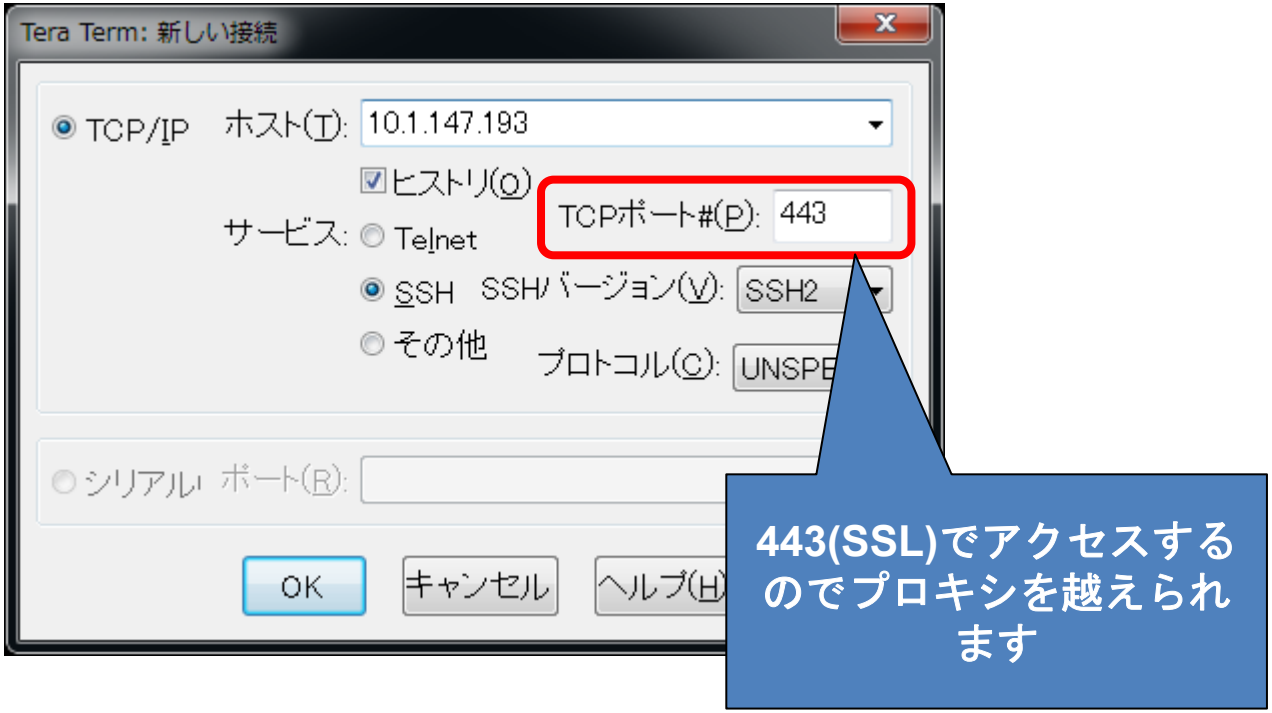
- WindowsサーバーのRDゲートウェイ機能を使う。
- RDゲートウェイ機能を使うときは、リモートデスクトップ接続のオプションで接続先のRDゲートウェイサーバーを指定する。
  ※RDゲートウェイはSSLで通信するので、プロキシを越えられます。



# 5. リモート保守におけるセキュリティ対策
## 5.2. プロキシ越えでアクセスする（Linux）

ポイント

- SSHサーバーを立て、リッスンポートに443を追加する。
- SSHクライアント（Tera Term, WinSCPなど）からポート443を指定してサーバーにアクセスする。
  ※SSL(443)で通信するので、プロキシを越えられます。

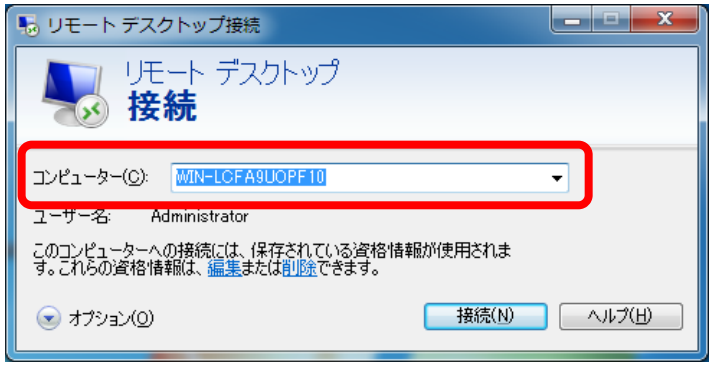


# 5. リモート保守におけるセキュリティ対策
## 5.3. アクセス可能なクライアントを制限する（Windows）

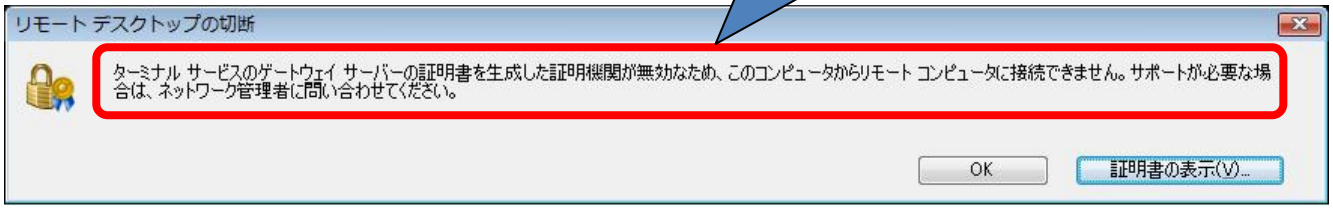
- 自己署名ルートCA証明書を作成し、クライアントの「信頼された証明機関」にインポートする。

ポイント

- リモートデスクトップ接続のオプションで接続先のRDゲートウェイサーバーを指定する。



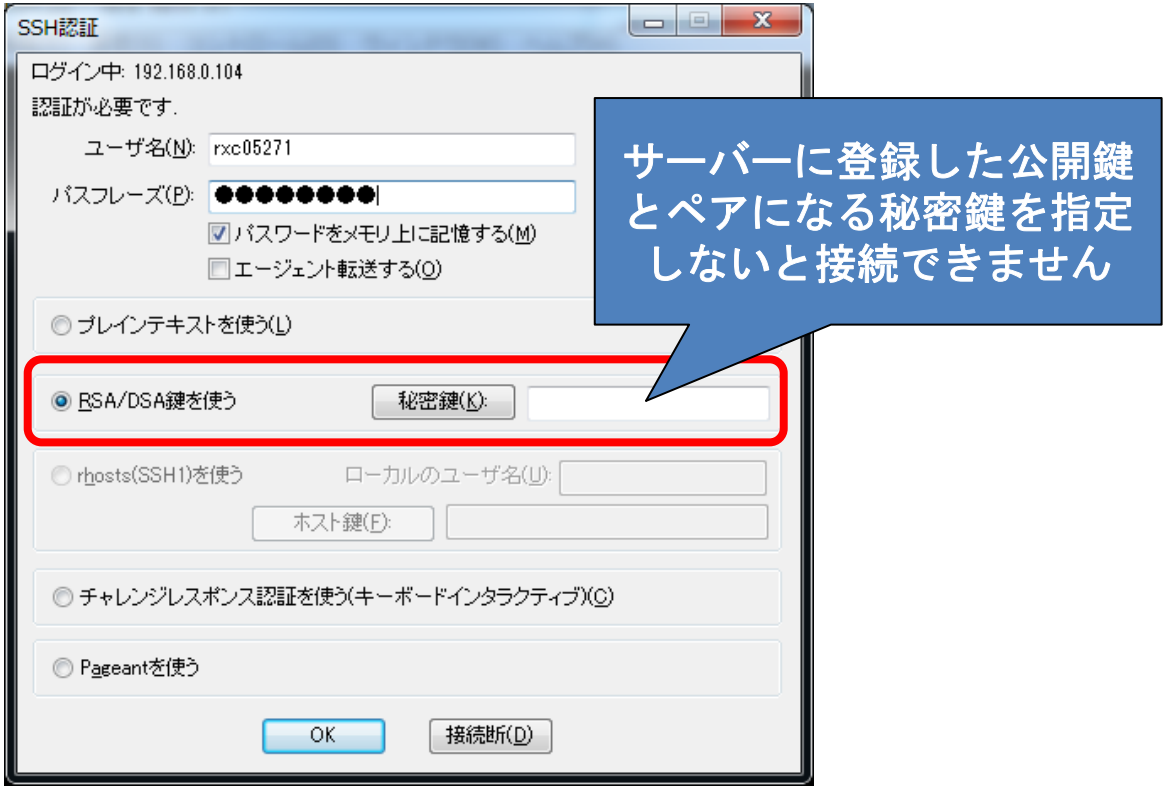

ルートCA証明書をインポートしていないとリモートデスクトップ接続が切断されます



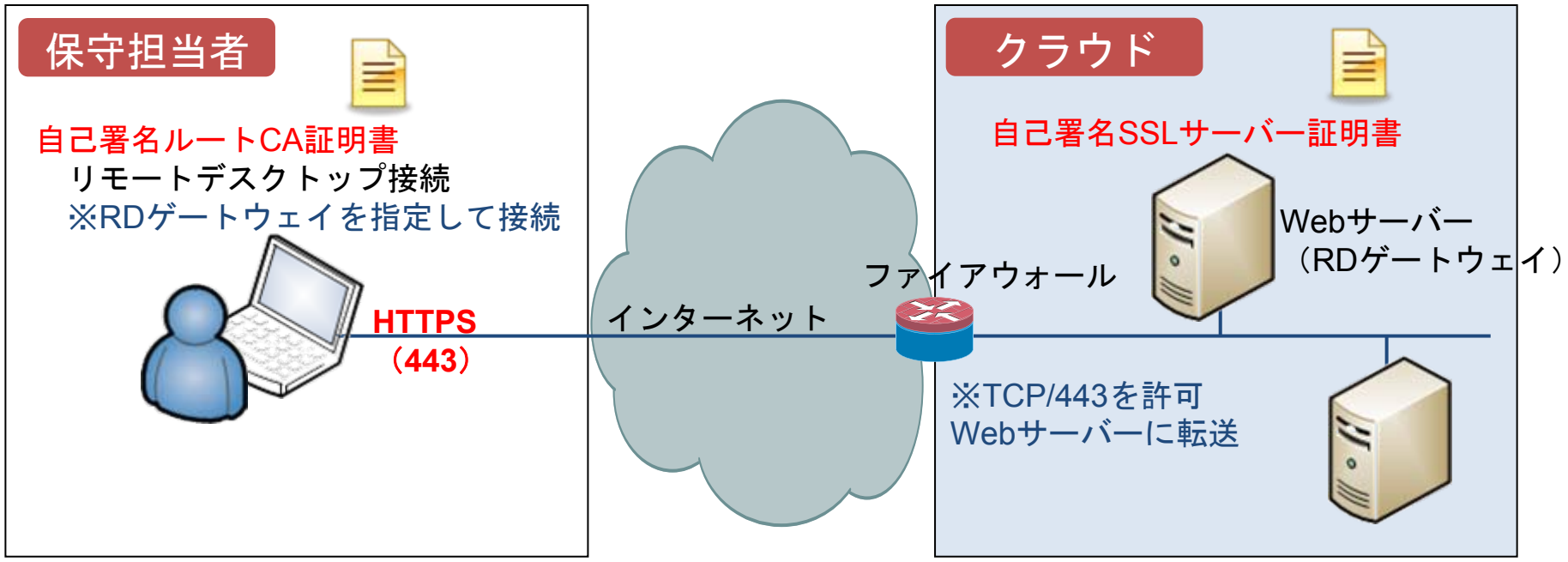
# 5. リモート保守におけるセキュリティ対策
## 5.4. アクセス可能なクライアントを制限する（Linux）

- SSHの公開鍵認証機能を使用する。 ポイント

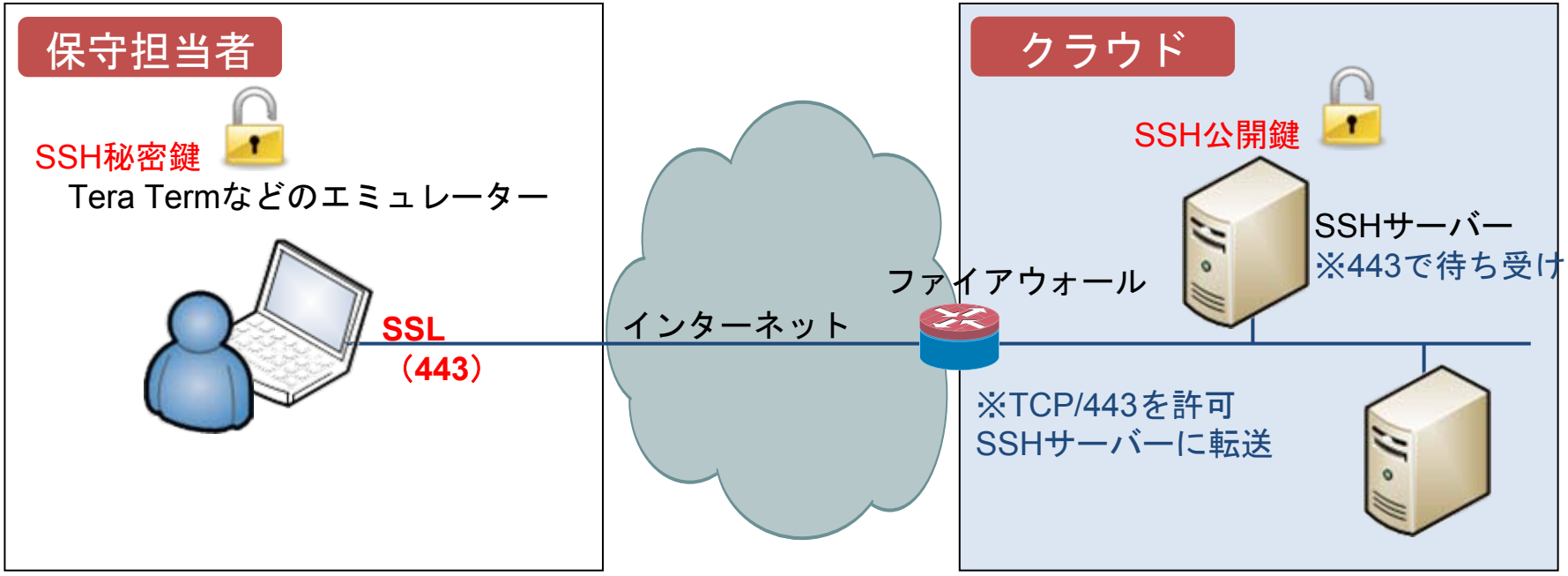
- クライアント上のTera Term等を使って公開鍵と秘密鍵を作成し、公開鍵をSSHサーバーに登録する。



# 5. リモート保守におけるセキュリティ対策
## 5.5. RDゲートウェイ概要図（Windows）



# 5. リモート保守におけるセキュリティ対策
## 5.6. SSHクライアント認証概要図（Linux）



# 6. VPNや専用線を使う場合との比較

- VPNや専用線は利用開始までにかなり時間がかかり、利用開始後も割高な接続サービス料金が発生します。

| | VPN、専用線 | インターネット＋今回紹介した方法 |
|---|---|---|
| コスト | [初期コスト]<br>・回線引き込み工事費用<br>・ルーターなどの装置費用/設置費用<br>・接続サービス加入料金（クラウド）<br>・LAN工事費用（社内）<br>・保守用スペース（部屋）の設置費用<br>[ランニングコスト]<br>・回線費用（月額）<br>・接続サービス利用料金（月額）<br>・保守用スペース（部屋）のフロア費用 | [初期コスト]<br>・RDゲートウェイやSSHの設定費用<br>・証明書の作成&導入費用<br><br>○ネットワーク工事が不要<br>○社内LANがそのまま使える<br>○保守用スペースが不要<br><br>[ランニングコスト]<br>・回線費用（月額） |
| 必要スキル | ・ネットワーク技術者 | ・WindowsやLinuxサーバーの管理者 |
| 利用開始までの期間 | ・おおよそ1~2か月 | ・おおよそ1週間 |

# 6. VPNや専用線を使う場合との比較

- VPNや専用線は利用開始までにかなり時間がかかり、利用開始後も割高な接続サービス料金が発生します。

- インターネットを利用する場合は、RDゲートウェイやSSHの設定の手間、証明書の作成と配置の手間だけで、あとは費用が発生しません。

| | VPN、専用線 | インターネット＋今回紹介した方法 |
|---|---|---|
| コスト | [初期コスト]<br>・回線引き込み工事費用<br>・ルーターなどの装置費用/設置費用<br>・接続サービス加入料金（クラウド）<br>・LAN工事費用（社内）<br>・保守用スペース（部屋）の設置費用<br>[ランニングコスト]<br>・回線費用（月額）<br>・接続サービス利用料金（月額）<br>・保守用スペース（部屋）のフロア費用 | [初期コスト]<br>・RDゲートウェイやSSHの設定費用<br>・証明書の作成&導入費用<br><br>○ネットワーク工事が不要<br>○社内LANがそのまま使える<br>○保守用スペースが不要<br><br>[ランニングコスト]<br>・回線費用（月額） |
| 必要スキル | ・ネットワーク技術者 | ・WindowsやLinuxサーバーの管理者 |
| 利用開始までの期間 | ・おおよそ1~2か月 | ・おおよそ1週間 |

# 7. いくつかの注意点

- 証明書ファイルや鍵ファイルの管理がかなり重要です。 ポイント
  - 証明書や鍵ファイルを盗まれないように、配布のしかたや保管のしかたに注意する必要があります。
  - 証明書の有効期限を短くして定期的に証明書を入れ替える、鍵ファイルを定期的に作り直すといったことが推奨されます。

- 1台のWindowsサーバー上で、SSL通信を行うWebサーバー（IIS）とSSL通信を行うRDゲートウェイは同居できます。

- 1台のLinuxサーバー上で、SSL通信を行うWebサーバー（Apacheなど）とSSL通信を行うSSHサーバーは同居できません。
  - 別のLinuxサーバーでSSHサーバーを動かす必要があります。

# 8. クラウドにおけるサーバー監視

# 8. クラウドにおけるサーバー監視
## 8.1. 各クラウドベンダーの対応状況

- ベンダーによってかなり異なります。可能なのはサーバーの死活監視、リソース使用率の監視ぐらいです。
- サービスやログの監視は自分でツールを用意する必要があります。
  （ログの監視機能は不正アクセスを検知するのに役立ちます）
- クラウドに置くサーバーの規模が小さい場合は、JP1やTivoliなどの高価な運用監視ツールを導入するのは避けたいところです。

ポイント

| クラウドベンダー | 標準サービスに含まれる監視機能<br>（メール通知が可能なもの） |
|---|---|
| Nifty Cloud | [基本監視]<br>Ping結果／サーバーステータス（停止）／CPU使用率／メモリー使用率／ディスク使用率 |
| IDCフロンティア<br>パブリッククラウド セルフタイプ | [セルフモニタリング]<br>ロードアベレージ/メモリ/Disk使用率、Disk Read/Write、ネットワークIn/Out、Web/Ping/DNS/ポート/SSL証明書有効期限チェック |
| NTTコミュニケーションズ Cloud$^{n}$ | なし |
| GMO クラウド Public | なし |
| BIGLOBE クラウドホスティング | [Ping監視] |

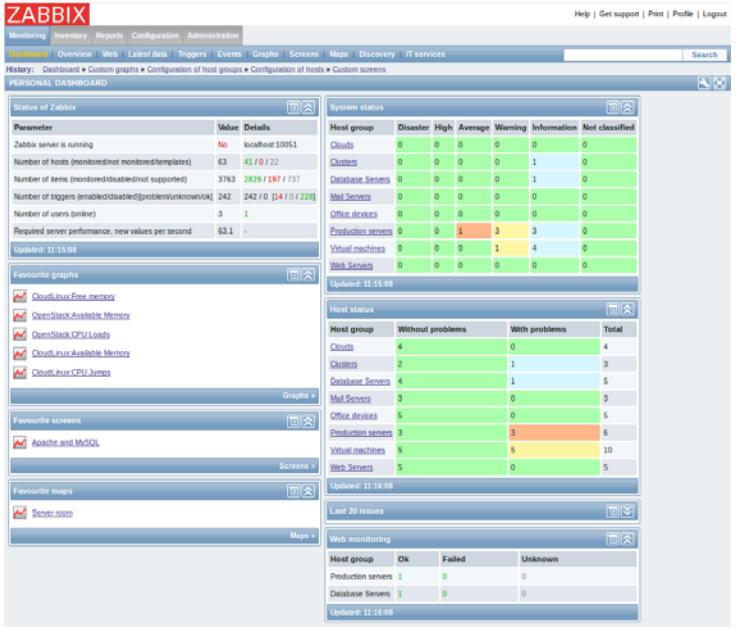
# 8. クラウドにおけるサーバー監視
## 8.2. 無償の運用監視ツールを使う

- Zoho ManageEngine OpManager
  無料版
  動作環境: Windows Server

サーバー10台まで無料。
英語での技術サポートあり。

無料版は画面に広告が入ります。

- Zabbix, Nagios
  オープンソース
  動作環境: Linux




※画面はZabbix

データセンターなどで豊富な実績

# 9. おわりに

- パブリッククラウドはクレジットカードで利用を申し込んでから30分も経たないうちにサーバーが使えるようになります。必要がなくなったらすぐに解約することができます。しかも課金は使った時間だけ。この利便性と費用の安さがパブリッククラウドの最大の特徴です。

- パブリッククラウドは不正アクセスが非常に多い環境です。自己署名の証明書や鍵ファイルを使ってアクセスできるクライアントを制限すれば、インターネット接続でも通信のセキュリティは十分に確保できます。不正アクセスからサーバーを守る手段として、来場者の皆さまがクラウドを活用する際の参考になれば幸いです。

# ご清聴ありがとうございました！