

SSH

概要

Linuxへの遠隔ログインを行う上で、デファクトスタンダードとなってるSSHについて、説明する。
仮想マシンに対してSSHを行い、コマンド操作を行える環境を作成する。
また、SSH以前から使用され続けるTelnetについても併記する。

目次

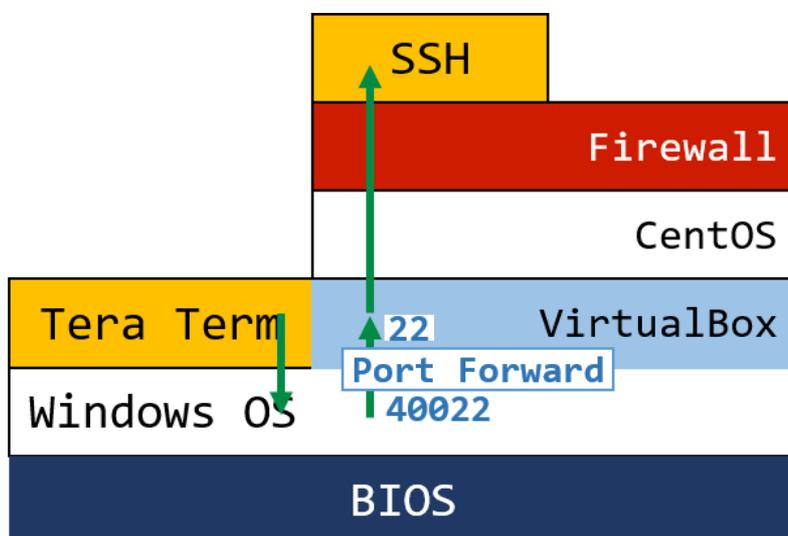
1. SSH
2. 使用方法
3. 注意点
4. Telnet

SSH

Linuxを始めとしたUnix系や近年ではWindowsにおいて、遠隔ログインに **SSH** (Secure SHell)が多く使われる。

遠隔サーバにログインでき、仮想端末を用いてコマンドを入力し、結果を受け取ることができる。
シェルスクリプトによる自動化を用いることで、サーバ間での処理の自動化ができる。

本演習では、別紙で作成した仮想マシン(仮想サーバ)に対し、下図のように遠隔ログインする。



SSHは、Telnetやrloginといった旧来のセキュリティに欠ける遠隔ログインのプロトコルを置き換える。
上記のプロトコルは、暗号化されておらず、パスワードやコマンドを含むデータを覗き見できるという問題点があった。

SSHは、通信を暗号化するため、これらの心配をなくす。

基本的に多くのUnix系にサーバプログラムが搭載されている。

使用時には、デーモンの起動やFirewallの許可が必要である。

また、Unix系に限らない多くのシステムにクライアントが搭載されている。

Windowsでも近年搭載されているが、長い期間の間搭載されていなかったため、サードパーティのクライアントである **Tera Term** を使うことが多い。

ユーザの認証方式には、パスワード認証と鍵認証の2つがある。

パスワード認証はユーザ名とパスワードで認証を行い、鍵認証は公開鍵と秘密鍵で認証を行う。

本資料では、パスワード認証を用いる。

SSHを応用することでファイル転送を行う、**SCP** や **SFTP** がある。

これらは、遠隔サーバとのファイル転送や取得によく使われる。

本演習で作成した仮想マシン上のファイルも、**WinSCP** などを使うことで、ホストマシンと相互に転送できる。

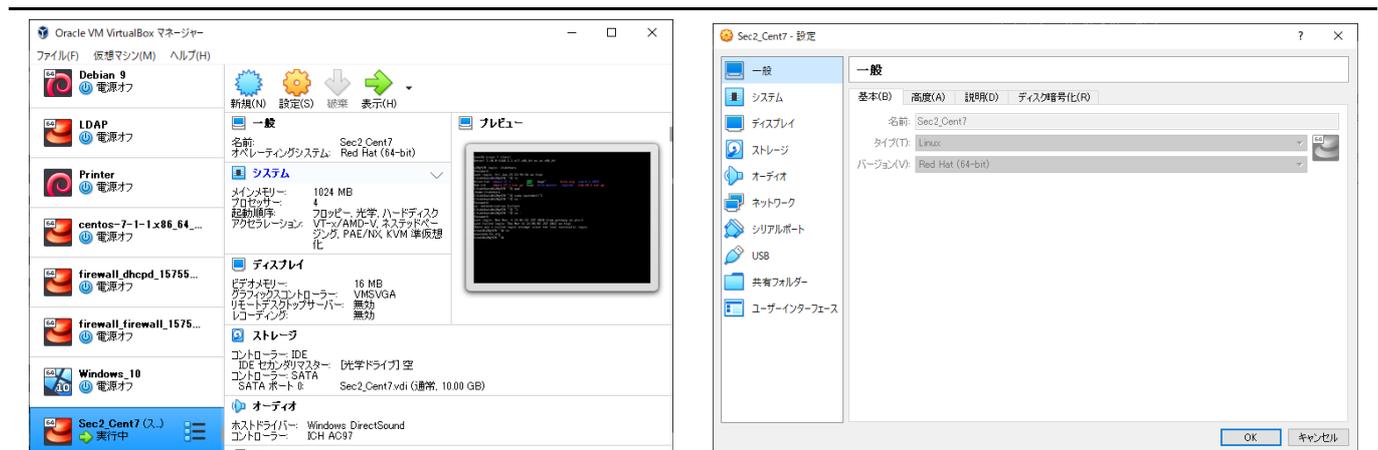
また、SSHのポートフォワード機能を用いることで、SSHを介してVPNのように様々な通信を転送できる。例えば、外部にSSHの鍵認証のみを許可しているSSHサーバを中継し、WindowsやLinuxのリモートデスクトップや、Sambaファイルサーバへのファイル転送ができる。

このようにして、リモートワーク体制を整えている研究室もある。

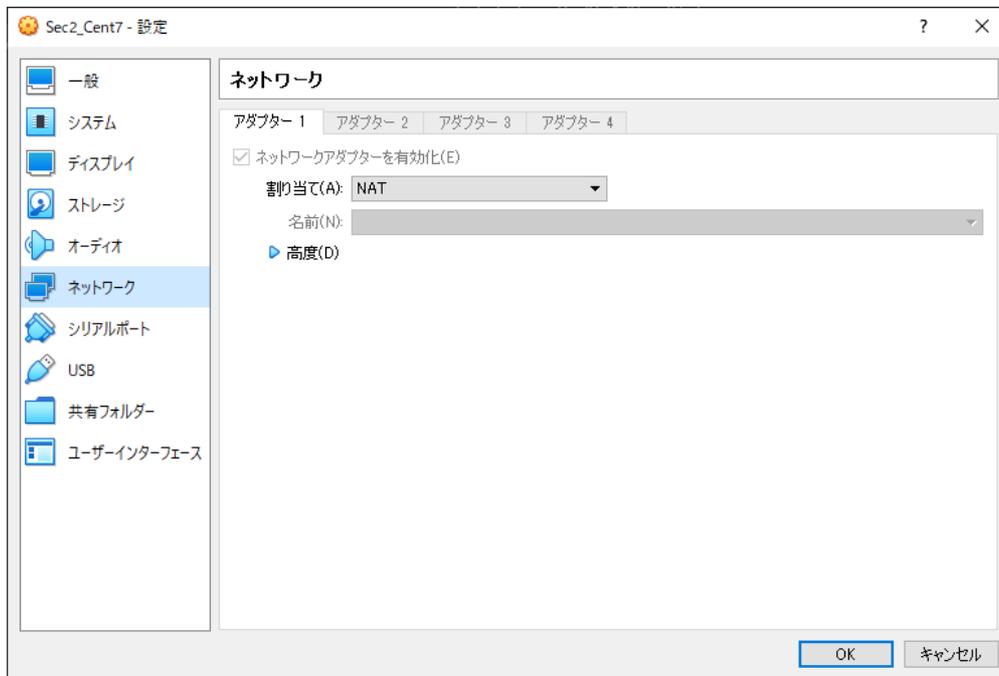
使用方法

1. VirtualBoxのポートフォワード設定を行う。

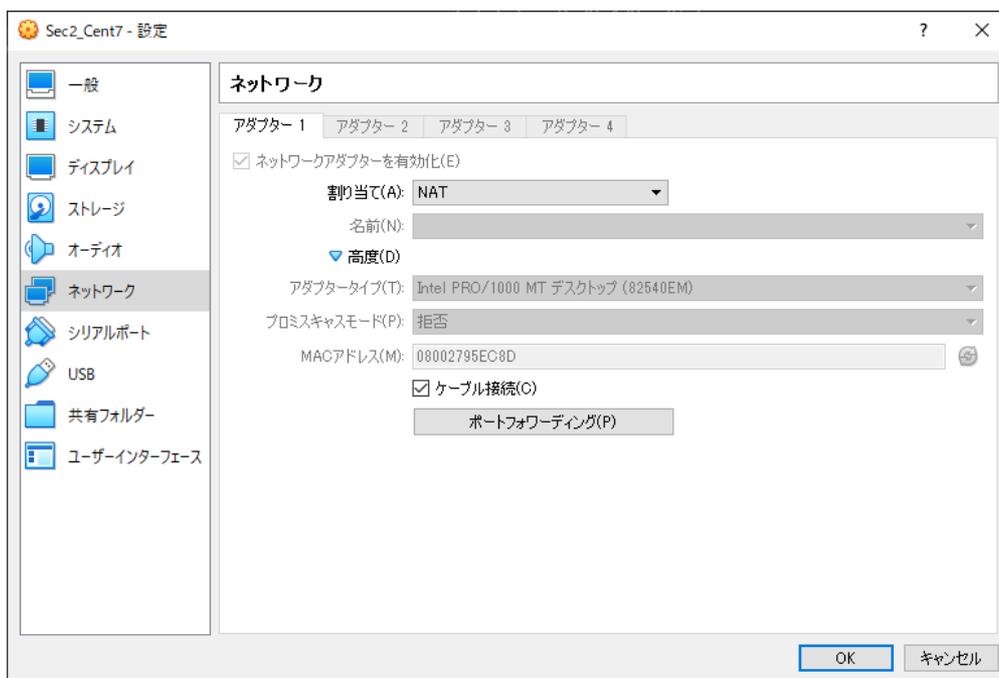
VirtualBoxの画面から仮想マシンを選択して、**設定** を開く。



設定の大項目の **ネットワーク** を選択する。

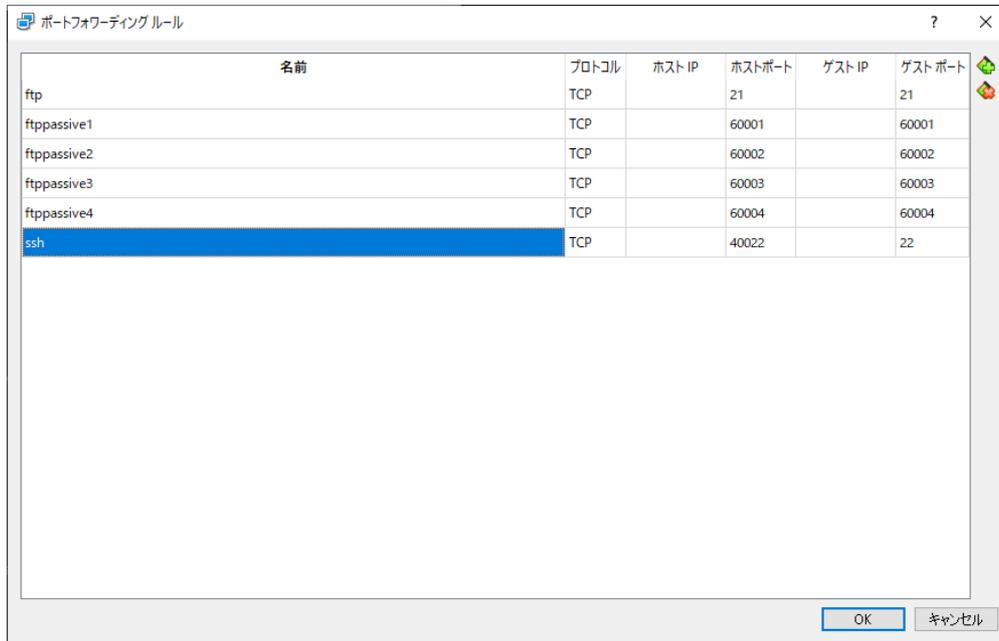


高度 から ポートフォワーディング を開く.



以下の最終行のように設定する.

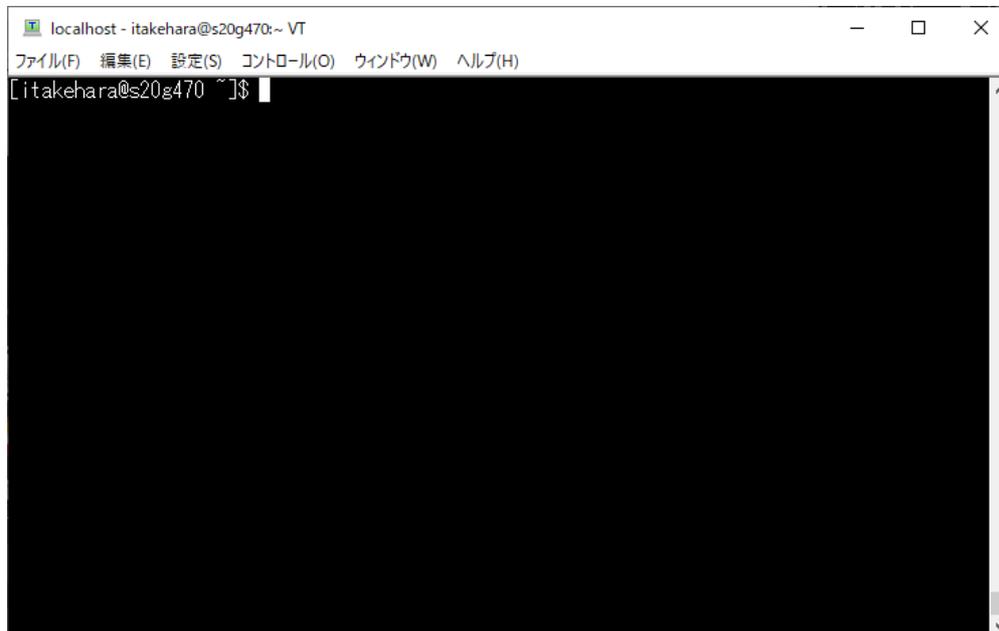
- 名前: ssh
- プロトコル: TCP
- ホストポート: 40022
- ゲストポート: 22



2. Tera TermなどのSSHクライアントを用いて接続する.

- ホスト: localhost
- TCPポート: 40022
- サービス: SSH
- ユーザ: itakehara
- パスワード: ユーザに対応するパスワード

3. ログインできれば、このような画面が表示される.



注意点

一般的にサーバがインターネットからの遠隔ログインを受け付けるには、セキュリティが重要である。ここでは、セキュリティを高める上で必須である、ログインの認証方法について述べる。

パスワード認証は、ユーザ名とパスワードが一致すると、ログインできるため、総当たり攻撃の対象になりやすい。

特に、ユーザ名はシステムユーザや多く使われる用語である程度絞られる。

古くから存在する遠隔ログインのプロトコルである。

通信を暗号化しないため、ユーザ名、パスワード、コマンドとその結果が、全て平文でネットワークに流れる。

その結果、悪意のあるものがパケットを盗み見ることができた。

近年では、上記のSSHが遠隔ログインには使われるが、多くのシステムに内蔵している点や、暗号化をしない故に高速な点で、サービスの通信の確認に使われることが多い。

Tera Termでは、Telnetもサポートしている。

例えば、hoge.eng.kagawa-u.ac.jpにHTTPポート(80番)に、接続すると、以下の結果が帰ってくる。

```
$ telnet hoge.eng.kagawa-u.ac.jp 80
Trying 192.168.1.2...
Connected to hoge.eng.kagawa-u.ac.jp.
Escape character is '^]'.
```

ここで、以下のリクエストを入力する。

```
GET /index.html HTTP/1.1
Host: hoge.eng.kagawa-u.ac.jp
(空行)
```

このようにヘッダを含む、応答が表示される。

```
HTTP/1.1 200 OK
Date: Wed, 18 Nov 2020 23:15:12 GMT
Server: Apache
Last-Modified: Sat, 01 Feb 2020 04:54:19 GMT
ETag: "4f-59d7c7ba47f55"
Accept-Ranges: bytes
Content-Length: 79
Content-Type: text/html

<html>
<body>
HTTPによるアクセステストです。(gin)
</body>
</html>
```

また、SSHポート(22番)に接続を試みると、以下のように帰ってくる。

```
Trying 192.168.1.2...
Connected to hoge.eng.kagawa-u.ac.jp.
Escape character is '^]'.
SSH-2.0-OpenSSH_7.4
```

このようにTelnetを用いることで、そのポートに対する通信の可否を判別することができる。

奥付

Name 竹原 一駿 (Ichitoshi TAKEHARA), 後藤 祥仁 (Yoshihito GOTO)
所属 香川大学大学院 工学研究科 信頼性情報システム工学専攻 最所研究室 M1
メールアドレス itakehara@fw.ipsj.or.jp

2020/12/03 初版

2021/04/10 2版

2021/05/18 3版
