vsftpd

概要

旧来より広く使われる，FTPサーバを構築する．
また，Telnetによる通信の確認方法も習得する．

目次

FTPとは

FTP (File Transfer Protocol)ファイル転送を目的としたサービスである．
ファイル転送のみを目的としたプロトコルとしてよく使われたが，近年はHTTP(S)によるWebサービスを用いてファイル転送することが多い．

通常のFTPでは，ユーザ名やパスワードが平文で交換されてしまう．
そこで，SSL/TLSにてログイン認証部を暗号化して用いることが多い．
一方，SSHによる暗号化した通信上でファイルを交換する，SFTP (SSH File Transfer Protocol) に切り替えるところもある．

TCPを使ったプロトコルの1つであるが，制御用(21番ポート)と転送用の2つのポートを用いる．

アクティブ(Active)モードとパッシブ(Passive)モードの2つがある．

アクティブモードは，以下の流れで接続する．
以下，クライアントの動作は`[C]`，サーバの動作は`[S]`で示す．

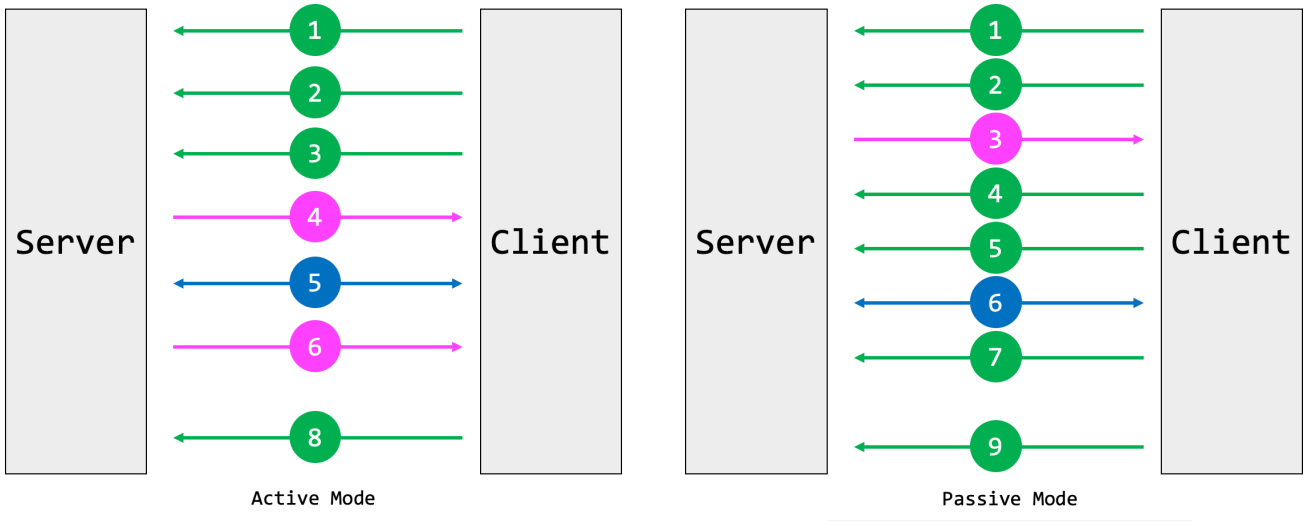
1. `[C]` サーバの21番ポートにアクセスし，制御用のコネクションを張る．
2. `[C]` 転送用コネクションのN番ポートを用意し，サーバに伝える．
3. `[C]` クライアントは，サーバにファイルの転送を要求する．
4. `[S]` N番ポートにアクセスし，転送用のコネクションを張る．サーバ側は20番ポートである．
5. `[S-C]` ファイルがサーバとクライアント間で転送される．
6. `[S]` `4.` が切断される．
7. 他のファイルを転送する場合は，`3.` ~ `6.` を繰り返す．
8. `[C]` `1.` が切断される．

つまり，クライアントが接続ポート(N番)を与え，それに対してサーバがコネクションを張る．
旧来のような，サーバとクライアントが直接接続するような環境であると，この方法で十分である．
しかし，NAPTの環境のような，IPアドレスとポートが同時に書き換わるような環境であると，クライアントからのN番ポートが，サーバに到達する前に書き変わり，うまく動作しなくなる．

そこで，クライアントからコネクションを張る，パッシブモードが用意されている．

1. [C] サーバの21番ポートにアクセスし，制御用のコネクションを張る．
2. [C] 転送用コネクションのためのポート番号をサーバに要求する．
3. [S] M番ポートをクライアントに通知する．
4. [C] サーバにファイルの転送を要求する．
5. [C] サーバM番ポートに転送用のコネクションを張る．
6. [S-C] ファイルがサーバとクライアント間で転送される．
7. [C] 5. が切断される．
8. 他のファイルを転送する場合は，3. ~ 7. を繰り返す．
9. [C] 1. が切断される．

つまり，サーバが接続ポート(M番)を与え，それに対してクライアントがコネクションを張る．
これならば，ポート番号が書き換わることがなく，間にNAPTがあったとしても動作する．



本演習では，FTPサーバを提供するアプリケーションの1つである， vsftpd を導入する．

応用1

どのような方法ならばセキュアにファイルをやり取りできるだろうか．

応用2

アクティブモード，パッシブモードを説明せよ．

SELinuxの無効化

CentOSは，Secure OSというセキュリティが強固なOSの1つであり， **SELinux** が導入されている．
本来は，有効化したまま運用することが望ましい．
また，有効化したまま一部のセキュリティのみを無効化することもできる．
しかし，本演習では，時間的束縛や基礎的知識の優先のため，無効化する．
動作モードには以下の3つがある．

1. Enforcing ... SELinuxの有効化する．
2. Permissive ... 警告モードである．セキュリティ違反があれば監査ログを残すのみである．
3. Disabled ... SELinuxの無効化する．

==========

演習1

`/etc/selinux/config` ファイルにて，SELinuxをpermissiveモードにせよ．
変更後は，適応のためシステムの再起動をすること．

==========

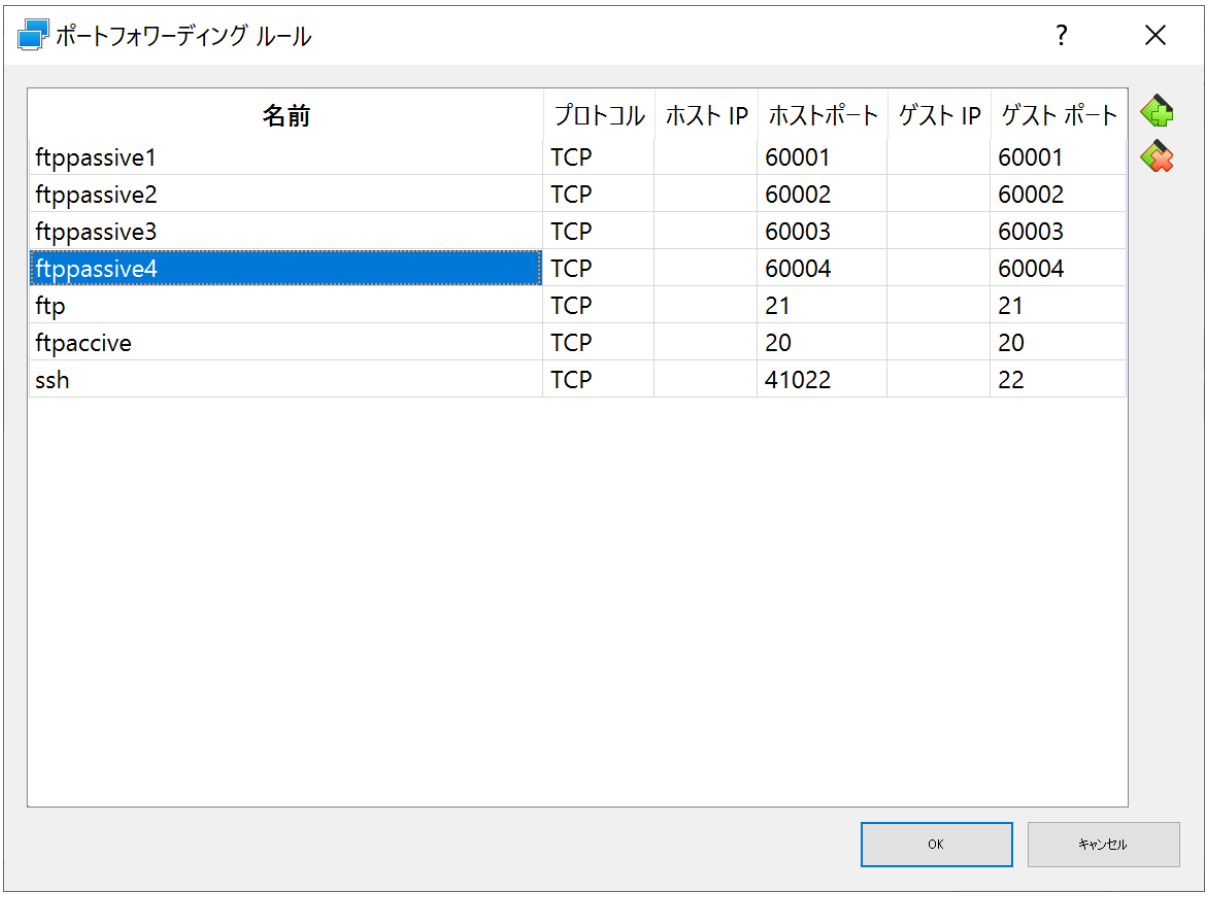
導入と確認

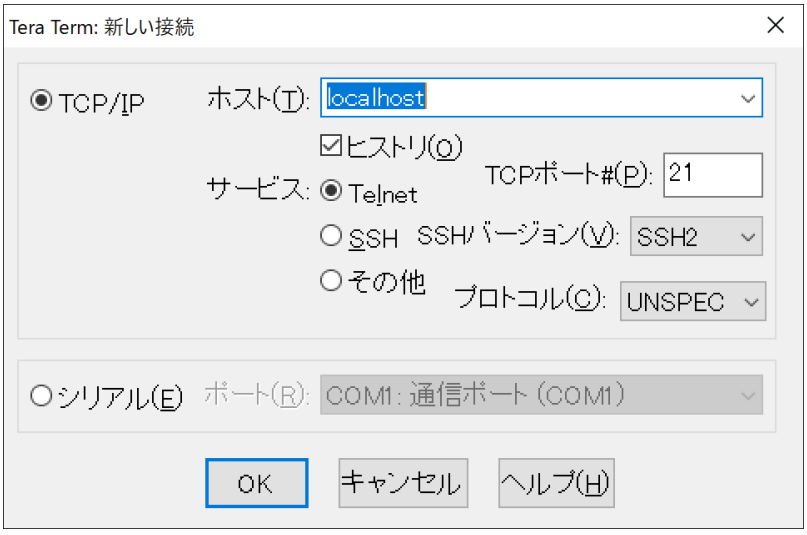
1. `yum` コマンドを用いてアップデートを行え．
2. Apacheなどと同様に， `vsftpd` をインストールせよ．
3. `firewall-cmd` を用いて， `ftp` サービスと `60001/tcp` ， `60002/tcp` の通信を許可せよ．
4. VirtualBoxのポートフォーワードを設定せよ．
    - 21番ポートをフォーワードする．(制御用)
    - 60001番と60002番ポートをフォーワードする．(転送用)
5. `systemctl` コマンドを用いてサービスを起動せよ．
6. Telnetによる通信で，接続を確認せよ． `Tera Term` により，以下の文字が表示されれば接続できている．

```
220 (vsFTPd 3.0.2)
```

==========

Tips!





==========

==========

余談だが，IPによるネットワーク間通信のTCPとUDPの違いを述べる．
TCPは，コネクションという仮想回線を送信元と送信先に確立することで，通信の信頼性を担保する．
コネクションさえ張ってしまえば，確実な通信が行える．
しかし，コネクション毎にリソースをある程度使用する．
UDPは，コネクションを確立せず，パケットを投げつける．
信頼性は低いが，低いリソースで使用できる．

つまり，TCPは，HTTPやSMTPなどの高い信頼性が必要で，リアルタイム性の求められない処理に向いている．
UDPは，DNS，DHCP，動画配信など，パケットレベルでの正確性が求められないものに使われる．

==========

設定

以下に本システムに導入するFTPサーバの要件を示す．

1. 匿名ログインを許可しない．FTPサーバにアクセスできるのは，存在するユーザのみである．
2. ローカルユーザのログインを許可する．
3. 全てのFTPコマンドを許可する．ファイルシステムを変更するようなものも含める．
4. アップロードとダウンロードの詳細がログファイルに記録されるようにする．
5. 外から来る接続はアクセス制御を適用しない．
6. スタンドアロンモードを有効化する．
7. IPv6を待ち受けない．
8. PASVをデータ接続の開始において許可する．パッシブモードを使用する．
9. PASV コマンドへの応答において，vsftpd が伝える IP アドレスに `127.0.0.1` を指定せよ．
10. PASV でのデータ接続に割り当てるポートの最小値を `60001` にする．
11. PASV でのデータ接続に割り当てるポートの最大値を `60002` にする．
12. wu-ftpd で使われているような標準的な xferlog フォーマットで転送ログファイルを作成する．

参考文献として，以下を参照すると良い．

- Man page of VSFTPD.CONF https://linuxjm.osdn.jp/html/vsftpd/man5/vsftpd.conf.5.html

==========
演習2
----
configファイルを見つけ出し，上記の要件に従って，設定せよ．
なお，大体のconfigファイルは， `/etc` 配下やサブディレクトリ内に存在する．
`find` や `grep` コマンド， `|` (パイプ)を利用すること．
==========

応用3

なぜ，以下のような設定を行うのか思考せよ．
応用2と関連付けると良い．

```
PASV コマンドへの応答において，vsftpd が伝える IP アドレスに `127.0.0.1` を指定せよ．
```

ファイルのアップロードとダウンロード

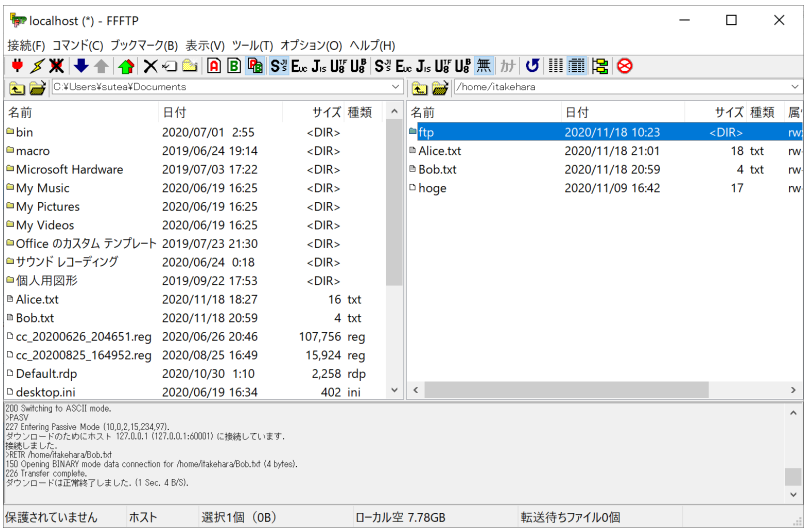
`[W]` で始まるのは，ホストOS(Windows)の操作である．
`[C]` で始まるのは，仮想マシン(CentOS)の操作である．

FTPクライアントは， `FFFTP` が推奨であるが，他のクライアントを使用しても構わない．
ただし，応用3の理由で，他のクライアントでの動作は難しいと考えられる(未検証)．

1. `[W] FFFTP` (FTPクライアント) をダウンロード，インストールする．
    - 「FFFTP」定番FTPクライアントソフト - 窓の杜
      https://forest.watch.impress.co.jp/library/software/ffftp/
2. `[W] FFFTP` の新規ホストを登録する．

    - ホストは，`127.0.0.1`
    - ユーザ名とパスワードは，`itakehara`とそのパスワード
    - 「拡張」タブより，「PASVモードを使う」にチェック
        - 必要ならばポートを変更
    - 「特殊機能」タブより，「PASVで返されるアドレスを無視」にチェック
3. `[W]` ホストに接続する．

接続できると，以下のように，WindowsとCentOSのファイル一覧が表示される．



4. `[W]` `Alice.txt` を作成する．
5. `[W]` FTPクライアントを用いて，CentOSに `Alice.txt` を転送する．
6. `[C]` `Bob.txt` を作成する．
7. `[W]` FTPクライアントを用いて，`Bob.txt` を取得する．

==========

演習3

CentOSとWindowsの両方に， `Alice.txt` と `Bob.txt` があることを示せ．

==========

==========

演習4

ファイルをやり取りしたログを `/var/log/xferlog` にて確認せよ．

==========

参考文献

- 斎藤. "CentOS7で作るネットワーク・サーバ構築ガイド", 株式会社秀和システム, 2015/04/01 第1版.
- TCPとUDPの違いと使い分け（第18回） | 日経クロステック（xTECH） https://xtech.nikkei.com/it/pc/article/NPC/20070130/260041/ , 2020/11/29.

奥付

```
Name     竹原 一駿 ( Ichitoshi TAKEHARA )
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
2021/05/25 2版
--------------------------------------------------------------------------------
```