FTP サーバ設定(暗号化：Vsftpd Over SSL/TLS)

Vsftpd で SSL/TLS で利用できるように設定（課題 No.03 あり）

(1) 証明書の作成(https：NT43 Linux 資料 11 Web サーバ その 2 と同じ)

[hal@motobe certs]$**cd /etc/pki/tls/certs/**

[hal@motobe certs]$**sudo openssl req -x509 -nodes -newkey rsa:2048 -keyout vsftpd.pem -out vsftpd.pem -days 3650** ←注意！これで 1 行分です。一度メモ帳に張った方が良いかも

Generating a 2048 bit RSA private key
.....+++
.+++
writing new private key to 'vsftpd.pem'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.

Country Name (2 letter code) [XX]:**JP**
State or Province Name (full name) []:**Osaka**
Locality Name (eg, city) [Default City]:**Osaka**
Organization Name (eg, company) [Default Company Ltd]:**www.motobe.com**
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:**www.motobe.com**
Email Address []:**root@motobe.com**
[root@motobe certs]# ls
Makefile ca-bundle.crt localhost.crt renew-dummy-cert server.key
Makefile.old ca-bundle.trust.crt make-dummy-cert server.crt **vsftpd.pem**
[root@motobe certs]#

※証明書 vsftpd.pem を作成
※青字は各自の設定に合わしてください

[hal@motobe certs]$ **sudo chmod 600 vsftpd.pem**

(2)vsFTPD の設定ファイル変更

[hal@motobe ~]$ **sudo　vi　/etc/vsftpd/vsftpd.conf**

★最終行へ追記

・SSL 機能を有効化するための項目と、SSL 通信で利用するサーバー証明書ファイルのパスを設定します。

rsa_cert_file=/etc/pki/tls/certs/vsftpd.pem
ssl_enable=YES
#ssl_ciphers=HIGH
#ssl_tlsv1=YES

・POODLE の件もあるので明示的に NO。POODLE（Padding Oracle On Downgraded Legacy Encryption）攻撃は、SSL 3.0 プロトコルの脆弱性を突く攻撃のことです。2014 年に報告されました。SSL 3.0 による暗号通信の内容を解読されるおそれがあります。

ssl_sslv2=NO
ssl_sslv3=NO

・ノンセキュアな FTP は使用させず、SSL を強制

force_local_data_ssl=YES
force_local_logins_ssl=YES

・パッシブ FTP が利用できるように、データコネクション用のポートを固定します。パッシブモードではデータコネクションはポート番号 20 ではなく、ランダムなポート番号が割り当てられ、その情報が FTP クライアントにその情報が伝えられます。

　firewall が設定されていない場合はパッシブモードは不要ですが、授業では firewall が設定されているため、必要な設定になります。全てのポートをオープンすることはセキュリティ上、好ましくないため、今回は 60001 ～ 60010 ポートに FTP データコネクション用ポートを割り当てます。

pasv_enable=YES
pasv_min_port=60000
pasv_max_port=60100

※上書き保存

(3)vsFTPD の再起動

[hal@motobe ~]$ **sudo　systemctl　restart　vsftpd**
※エラーの出た方は設定をもう一度確認！「スペース」や「綴り」が間違っていませんか？

(4) Firewall 設定

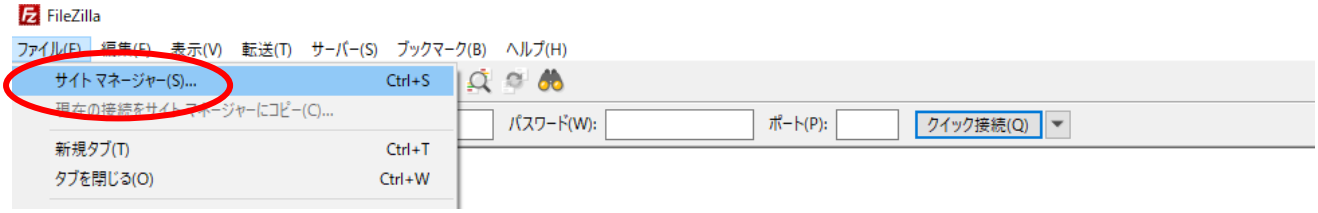
[hal@motobe ~]$**sudo firewall-cmd --add-port=60001-60010/tcp --zone=public --permanent**
success
※vsFTPD の設定ファイルに設定したポート(60001~60010)を開放

[hal@motobe ~]$**sudo firewall-cmd --reload**
success

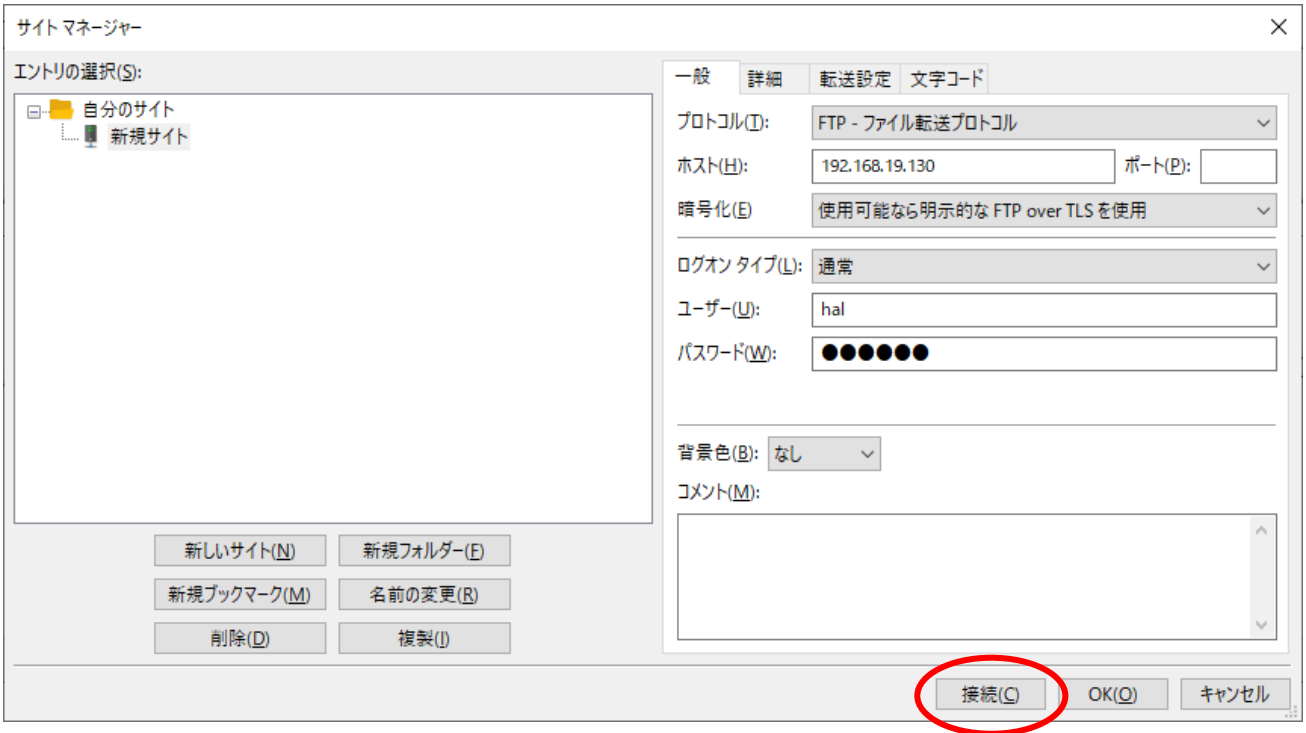
[hal@motobe ~]$**sudo firewall-cmd --list-port --zone=public**
60001-60010/tcp
※登録確認

(5)vsFTPD の動作確認(PASV モード)　　←GUI ベース

クライアント機より接続する(代表的な Windows や MAC の FTP ツールの FileZilla を使用)

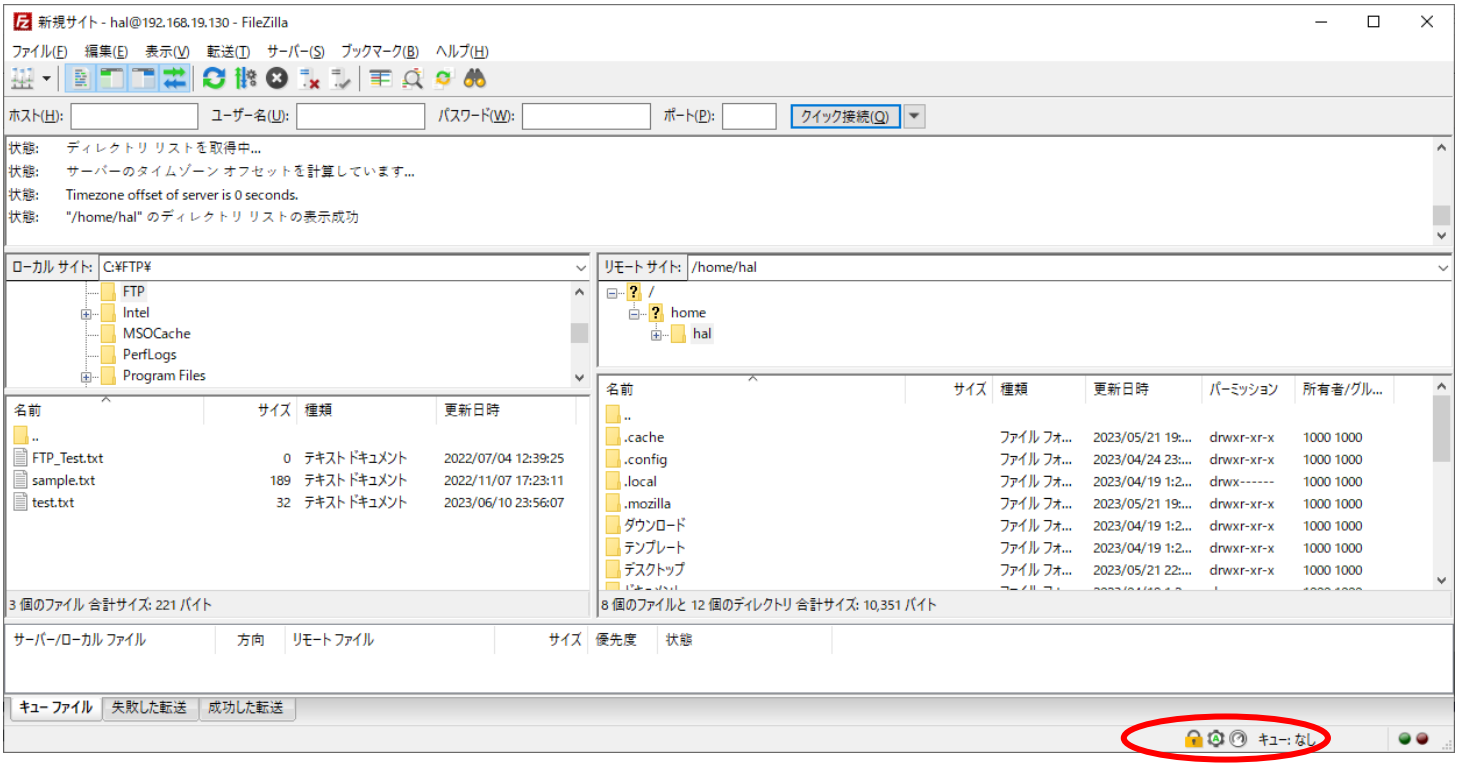


[ファイル]　→　[サイトマネージャー]　→　[新しいサイト]



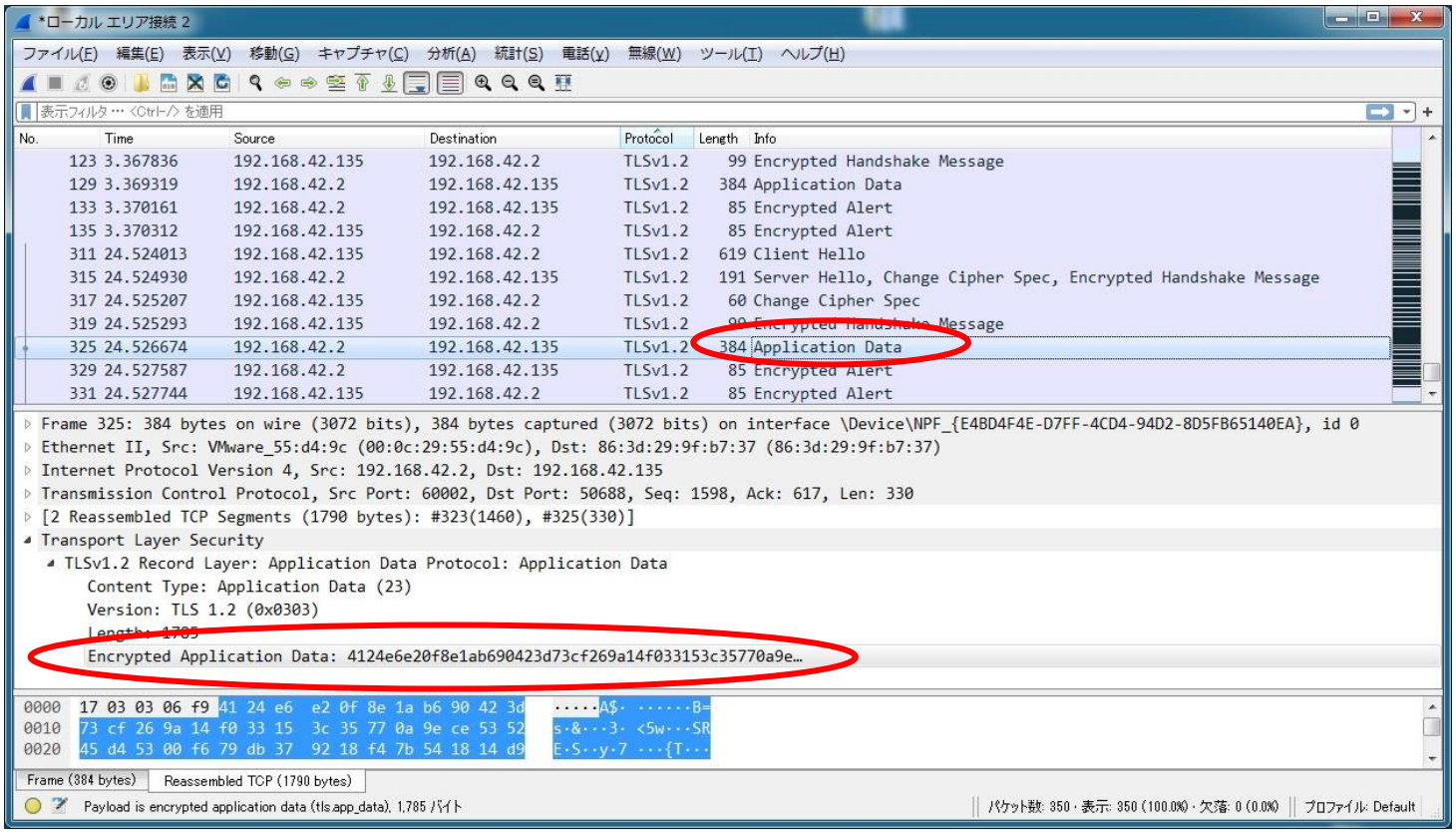
ホスト：Linux の IP アドレス　　暗号化：使用可能なら明示的~
ログオンタイプ：通常　　ユーザ：hal　　パスワード：halhal
[接続]

※先ほど作成した証明書が表示　→　[今後は常にこの証明書を使用する]を選択



※接続完了！　特に下に金色の鍵のマーク(暗号化の印)に注目！

(6)Wireshark で通信内容を確認



[Protocol 別に並び替え] → [TLSv1.2]を選択 → [ApplicationData]選択

上記のように **Encrypted ApplicationData があれば暗号化されています！(これは SSH でも見ましたね)**

★課題はこの Wireshark の暗号化の画面を見せて下さい！

※FileZilla の金色のカギのマークでも可

御苦労さま！

FTP もボリュームたっぷりでしたね♪

以上！

＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊＊

●課題No.03

科目：NT43　　主題：「FTPサーバ」

日付：6 月 19 日　　教員：元部 重和