SSH サーバ設定(パスワード認証)

Telnet の学習をした事を覚えていると思います。その時にも話をしましたが Telnet は通信の暗号化をしない為、使用を控えたほうが良いと言いました(WireShark で盗聴もしましたね)。現在のネットワークの世界では暗号化通信を行う SSH が主流となっています。

SSH サーバ自体は特に何もしない限りはデフォルトで OpenSSH がインストールされており、新たに何かインストールする必要はありません。

(1) インストールの確認

[hal@motobe ~]$ **rpm -q openssh-server**
openssh-server-8.7p1-28.el9.x86_64

[hal@motobe ~]$ **rpm -q openssh-clients**
openssh-clients-8.7p1-28.el9.x86_64
※もし無かったら yum でインストールして下さい

(2) ログイン設定

SSH サーバーは CentOS9 最小構成インストールでも、デフォルトで OpenSSH がインストールされ、自動起動設定になっているため、パスワード認証方式でのログインは可能となっています。セキュリティを強化するならば、以下のように root アカウントの直接ログインの禁止設定を実施しておくとよいでしょう。

① 設定ファイル編集

[hal@motobe ~]$ **sudo cp /etc/ssh/sshd_config /etc/ssh/sshd_config.old**
※先ずは設定ファイルのバックアップ！
※設定ファイルは「sshd_config」です！紛らわしい「ssh_config」が有りますが間違わないで下さい！

[hal@motobe ~]$ **sudo vi /etc/ssh/sshd_config**
#40 行目
PermitRootLogin no ←先頭の#を削除して no に変更(root(管理者)でのログインを禁止)

#66 行目
PermitEmptyPasswords no ←先頭の#を削除(空パスワードの禁止)

② SSH の再起動

[hal@motobe ~]$ **sudo systemctl restart sshd**
※SSH は最初から起動しているため再起動

③Firewall

firewalld を有効にしている場合は、SSH サービスの許可が必要です。なお、SSH は 22/TCP を使用します。
CentOS9 はデフォルトで SSH が許可されているので、**以下のコマンドは必要ありません。**

[hal@motobe ~]$ **sudo firewall-cmd --add-service=ssh --zone=public --permanent**
Warning: ALREADY_ENABLED: ssh
success
※already：既に
[hal@motobe ~]$ **sudo firewall-cmd --reload**
success
[hal@motobe ~]$ **sudo firewall-cmd --zone=public --list-services**
cockpit dhcpv6-client http **ssh** telnet

(3) アクセス確認

[hal@motobe ~]$ **ssh hal@192.168.221.128** **←@の後は Linux の IP アドレス**
The authenticity of host '192.168.221.128 (192.168.221.128)' can't be established.
ED25519 key fingerprint is SHA256:q0DPsIoXDrJu0/oLBA0CTK8vrXrngGEqd90WGmEMM5w.
This host key is known by the following other names/addresses:
~/.ssh/known_hosts:1: localhost
Are you sure you want to continue connecting (yes/no/[fingerprint])? **yes**
Warning: Permanently added '192.168.221.128' (ED25519) to the list of known hosts.
hal@192.168.221.128's password:
Activate the web console with: systemctl enable --now cockpit.socket

Last login: Mon May 15 00:16:59 2023 from ::1
[hal@motobe ~]$ **pwd**
/home/hal

●現在 Linux にログインしているユーザの確認
[hal@motobe ~]$ **who**
hal seat0 2023-05-14 21:28 (login screen)
hal tty2 2023-05-14 21:28 (tty2)
hal pts/1 2023-05-14 23:03 (localhost)
hal pts/2 2023-05-15 00:19 (192.168.221.128)
※hal にログインできた

●Windows から接続確認

(1)コマンドプロンプトを利用

Windows10 や 11 はデフォルトで SSH クライアントが入っていますのでコマンドプロンプトからアクセス出来ます。

C:¥Users¥moto>ssh　hal@192.168.221.128

The authenticity of host '192.168.221.128 (192.168.221.128)' can't be established.

ECDSA key fingerprint is SHA256:WiHPWjhi7b3EtxIbXFxe/uyby+WDcf0zODqdKp5TV4s.

Are you sure you want to continue connecting (yes/no/[fingerprint])? **yes**

Warning: Permanently added '192.168.221.128' (ECDSA) to the list of known hosts.

hal@192.168.221.128's password:　　←Linux 上のユーザ hal のパスワード(halhal)

Activate the web console with: systemctl enable --now cockpit.socket

Last login: Sun May 14 23:16:42 2023 from ::ffff:192.168.221.1

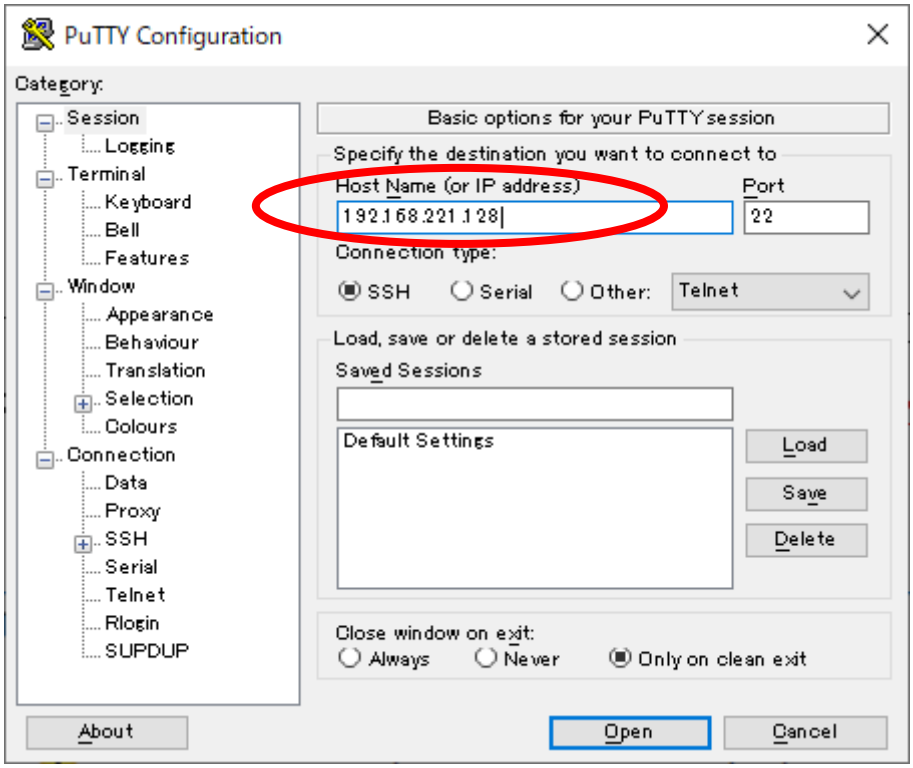
[hal@motobe ~]$ **pwd**

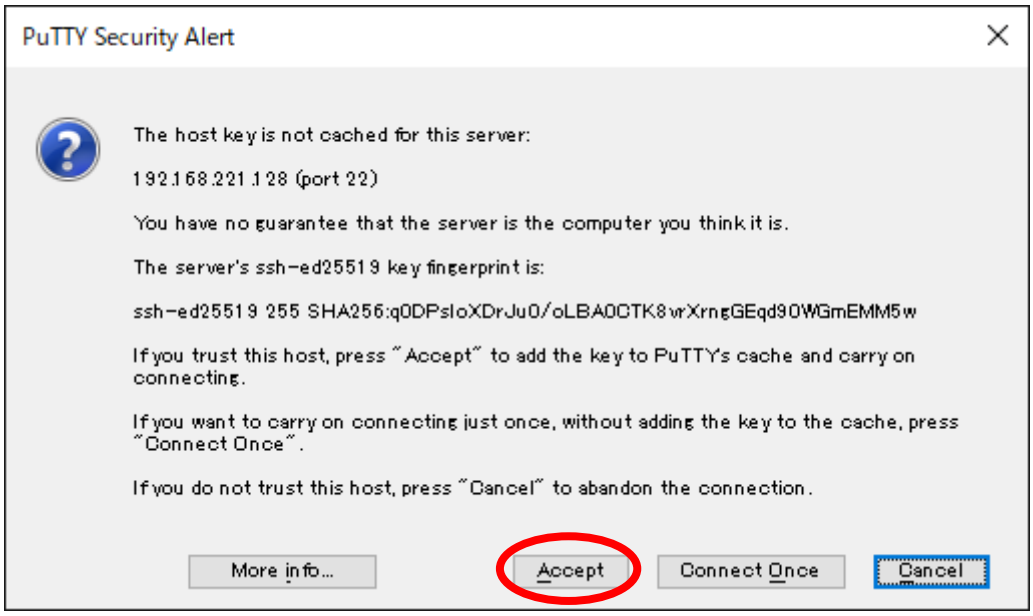
/home/hal

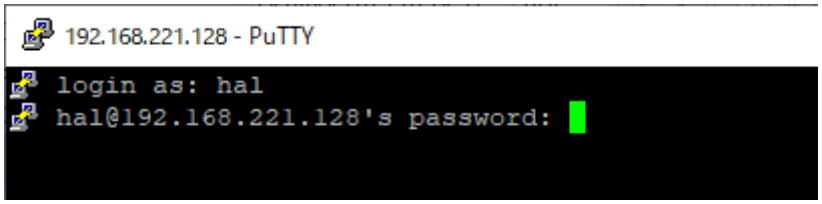
(2)SSH 接続アプリを利用

クライアント側で SSH 接続できるソフトウェアを用意します。一般的には、 TeraTerm Pro や Putty 等が有名で、ここでは Putty を使用します。　←素材フォルダ「配布プログラム」の中の「**putty-64bit-0.78-installer.msi**」

起動したら、以下のような画面がでるので、ホスト名のところにサーバー(Liunx)の IP アドレスを入力し、「open」をクリックして接続します。

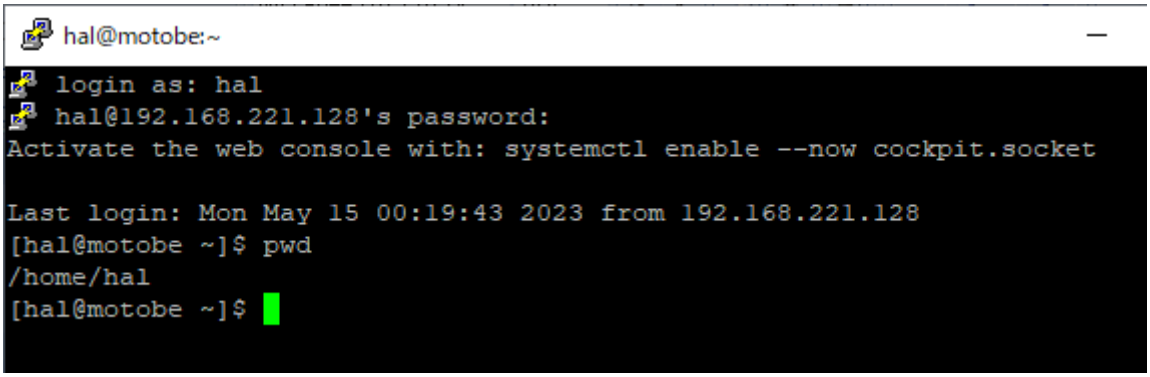






※Linux のユーザ ID とパスワードを入力

ユーザ：hal　　パスワード：halhal



ログイン出来ました！

●MAC から接続確認

基本的には Windows と同じ様にすれば OK。MAC の Terminal 上で

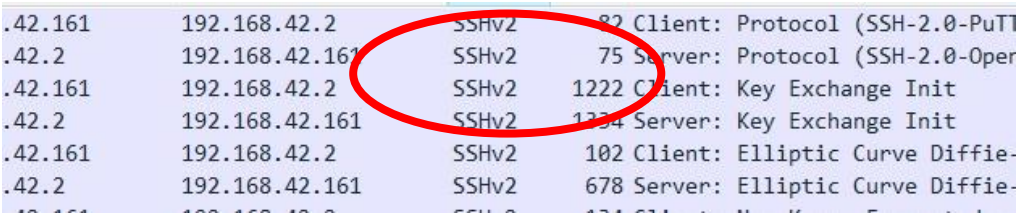
motobe@moto Desktop % **ssh hal@192.168.64.6**
The authenticity of host '192.168.64.6 (192.168.64.6)' can't be established.
ECDSA key fingerprint is SHA256:WiHPWjhi7b3EtxIbXFxe/uyby+WDcf0zODqdKp5TV4s.
Are you sure you want to continue connecting (yes/no/[fingerprint])? **yes**
Warning: Permanently added '192.168.64.6' (ECDSA) to the list of known hosts.
hal@192.168.64.6's password: **←Linux 上のユーザ hal のパスワード(halhal)**
Activate the web console with: systemctl enable --now cockpit.socket
Last login: Sun May 14 23:16:42 2023 from ::ffff: 192.168.64.1
[hal@motobe ~]$ **pwd**
/home/hal

でアクセス出来ます。
※Terminal は、「アプリケーションフォルダ」内の「ユーティリティフォルダ」にインストールされています。

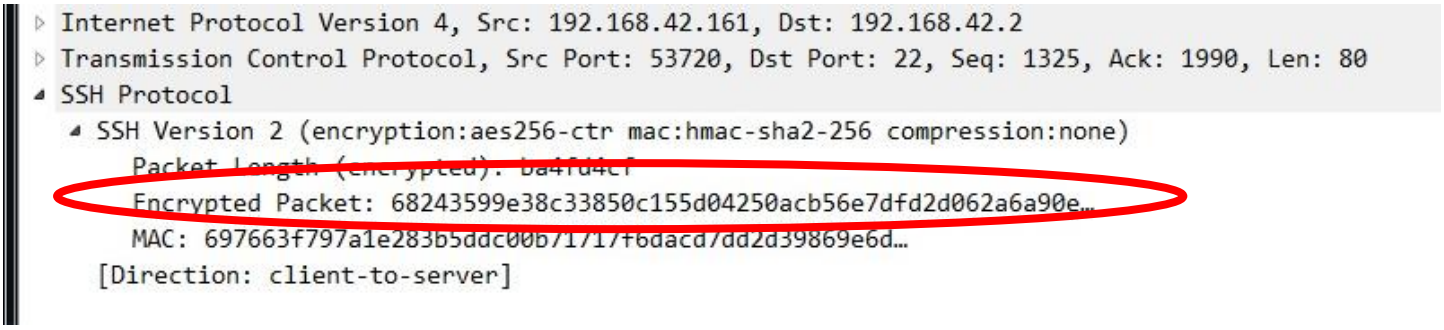
(4) 暗号化確認 ←重要！

WireShark を起動して、通信が暗号化されている事を確認して下さい。
何回か使用していますので大丈夫と思いますが・・・

①もう一度、Putty で SSH 接続を行う



・[Protocol]をクリックして並び替え
・[SSHv2]を選択
・パケットの中身の確認
　どれか適当に[Encrypted]のパケットを選択 → 真ん中の画面の一番下[SSH Protocol]を開く
　→[SSH version2 ～]をひらくと **Encrypted Packet**(←暗号化という意味)と表示されている。



これで安全な通信が確保されました！

※上手く自分の Linux に入れない方は先生の Linux や友人の Linux に入って確認しても良いです。

実務では必ずリモートアクセスは Telnet ではなくて SSH を利用するようにして下さい！

(5)　SSH(SCP)を用いたファイル転送　　←UTM と VirtualBox の方は重要！

①Windows や MAC 上に Linux へ転送したいファイル「例：test.txt や 001.pdf」をデスクトップに用意

②Windows の方

C:¥Users¥moto>cd　Desktop

C:¥Users¥moto¥Desktop>dir

2023/05/15　00:39　　3 test.txt　　←Linux に転送したいファイル

●scp を用いて Windows から Linux へファイル転送

C:¥Users¥moto¥Desktop>scp　test.txt　hal@192.168.221.128:/home/hal

hal@192.168.221.128's password:　　←hal のパスワード

test.txt　　100%　3　0.9KB/s　00:00

※ファイル(test.txt)が転送出来た！

C:¥Users¥moto¥Desktop>ssh　hal@192.168.221.128

hal@192.168.221.128's password:

Activate the web console with: systemctl enable --now cockpit.socket

[hal@motobe ~]$ ls

test.txt　ダウンロード　テンプレート　デスクトップ　ドキュメント　ビデオ　音楽　画像　公開

※転送出来ている事を確認出来ました！

●scp を用いて Linux から Windows へファイル転送

C:¥Users¥moto¥Desktop>scp　hal@192.168.221.128:/home/hal/abc.txt　.

※「．」を忘れないように

③MAC の方

●UTM を使用

・文字のコピペは可能

・データのコピペが出来ないので SCP を用いてファイル転送をしましょう！

●VirtualBox を使用

・ツールキットをインストールしていれば文字もデータもコピペ可能

・ツールキットをインストールしていない時は、SCP を用いて MAC から授業 pdf を Linux へ転送すると、長いコマンド他を入力しなくて済みます。

●scp を用いて MAC から Linux へファイル転送

※転送するファイルのファイル名は日本語が無い単純な名前に変えた(例：001.pdf など)方が良いです。

※以下の作業は全て「MAC のターミナル上」で実行して下さい ←Linux 上では無い！

motobe@moto ~ % **pwd**

/Users/motobe ←MAC 上のカレントディレクトリ確認

motobe@moto ~ % **cd Desktop** ←転送したいデータがデスクトップ上にあるので移動

motobe@moto Desktop % **ls**

001.pdf ←これを Linux に転送したい(単純な名前に変更済み)

CentOS-Stream-9(aarch64).iso

(省略)

motobe@moto Desktop % **scp 001.pdf hal@192.168.64.6:/home/hal**

hal@192.168.64.6's password:

001.pdf 100% 153KB 29.0MB/s 00:00

※Linux へコピーできました！

●scp を用いて Linux から MAC へファイル転送

motobe@moto Desktop % **scp hal@192.168.64.6:/home/hal/libXaw-1.0.13-19.el9.aarch64.rpm .**

※「 . 」を忘れないように

hal@192.168.64.6's password:

libXaw-1.0.13-19.el9.aarch64.rpm 100% 193KB 47.5MB/s 00:00

motobe@moto Desktop % **ls**

001.pdf

CentOS-Stream-9(aarch64).iso

(省略)

libXaw-1.0.13-19.el9.aarch64.rpm

※Linux から MAC へコピー出来ました！

以上