目次

SSHサーバの設定 3
設定 3
sshd の設定 3
sshd 設定の変更(パスワード認証の無効化) 10
sshd の再起動 12
パスワード認証無効の確認 13

SSHサーバの設定

MA-E3xx/4xx/MA-S1xx には、標準で SSH サーバ (OpenSSH) をインストール、起動するように設定してあります。
しかし、標準ファームウェアの初期設定は利便性重視の設定としているため、

- パスワード認証を有効にしてあるため、総当り攻撃に弱い
- Firewall の設定もしていないため、上の弱点が突かれやすい

という問題があり、インターネットに晒す場合、設定を変更することを強くお勧めします。

設定

sshd の設定

OpenSSH sshd の設定ファイルは /etc/ssh/sshd_config で、出荷時設定は下記の通りとなっています。

sshd_config

```
# Package generated configuration file
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will
bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
```

```
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for
RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues
with
# some PAM modules and threads)
ChallengeResponseAuthentication no

# Change to no to disable tunnelled clear text passwords
#PasswordAuthentication yes

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

# Allow client to pass locale environment variables
#AcceptEnv LANG LC_*
```

```
Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM yes

UseDNS no
```

1つめの弱点“パスワード認証”を無効にし、公開鍵暗号による認証のみでログインできるように設定してみます。

秘密鍵・公開鍵の作成

まず、作業を行う端末で、秘密鍵・公開鍵のペアを作成します。

Linux/MacOS X の場合

ssh-keygen コマンドにより作成します。

```
testuser@lubuntu-vpc:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/testuser/.ssh/id_rsa):
Created directory '/home/testuser/.ssh'.
Enter passphrase (empty for no passphrase):  <--- パスフレーズ入力
Enter same passphrase again:                 <--- パスフレーズ確認
Your identification has been saved in /home/testuser/.ssh/id_rsa.
Your public key has been saved in /home/testuser/.ssh/id_rsa.pub.
The key fingerprint is:
3d:c4:71:49:84:13:7e:5f:6c:c6:c2:59:2b:65:bd:1d testuser@plum
The key's randomart image is:
+--[ RSA 2048]----+
|          o=+. oo|
|         ooo..oEo|
|          +...+.X|
|         o . ..*.|
|        S o   .  |
|           .     |
```

```
|                  |
|                  |
|                  |
+------------------+
testuser@lubuntu-vpc:~$
```

より安全にする(秘密鍵が漏れた場合の保護)場合、パスフレーズを入力しておくほうがよいでしょう。
作成された秘密鍵・公開鍵のペアは、ユーザのホームディレクトリ直下の .ssh/ ディレクトリに配置されます。

```
testuser@lubuntu-vpc:~$ ls -l .ssh/
合計 8
-rw------- 1 testuser testuser 1679  6月 19 09:43 id_rsa     <--- 秘密鍵
-rw-r--r-- 1 testuser testuser  395  6月 19 09:43 id_rsa.pub <--- 公開鍵
testuser@lubuntu-vpc:~$
```

Windows の場合

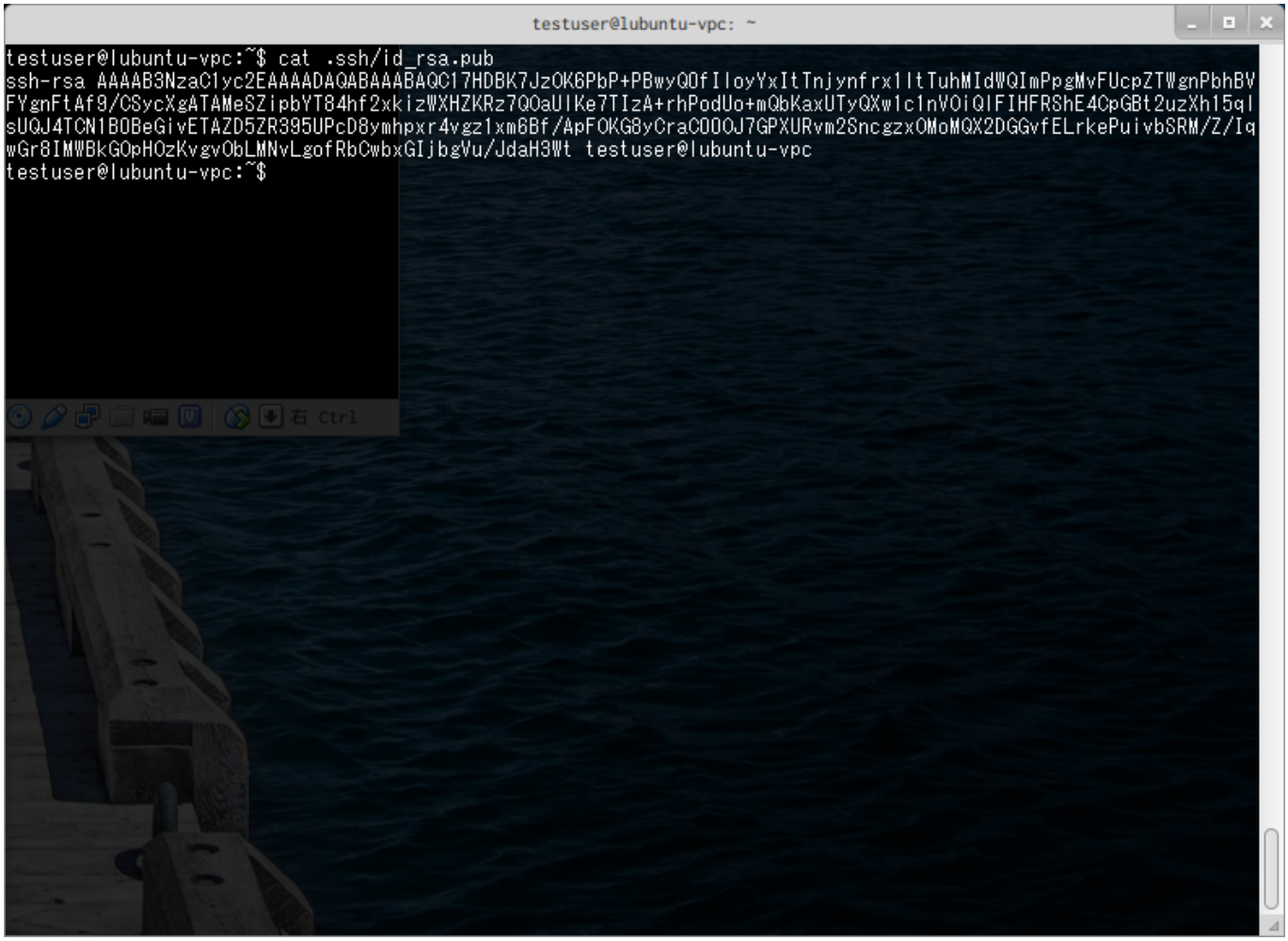
PuTTY[1] という Telnet/SSH Client ソフトがオススメです。
とても参考になるサイトを紹介しておきます。

- 安全な通信方式での接続方法(その1) -- PuTTY で SSH 接続 --
- PuTTY で鍵交換方式による SSH 接続

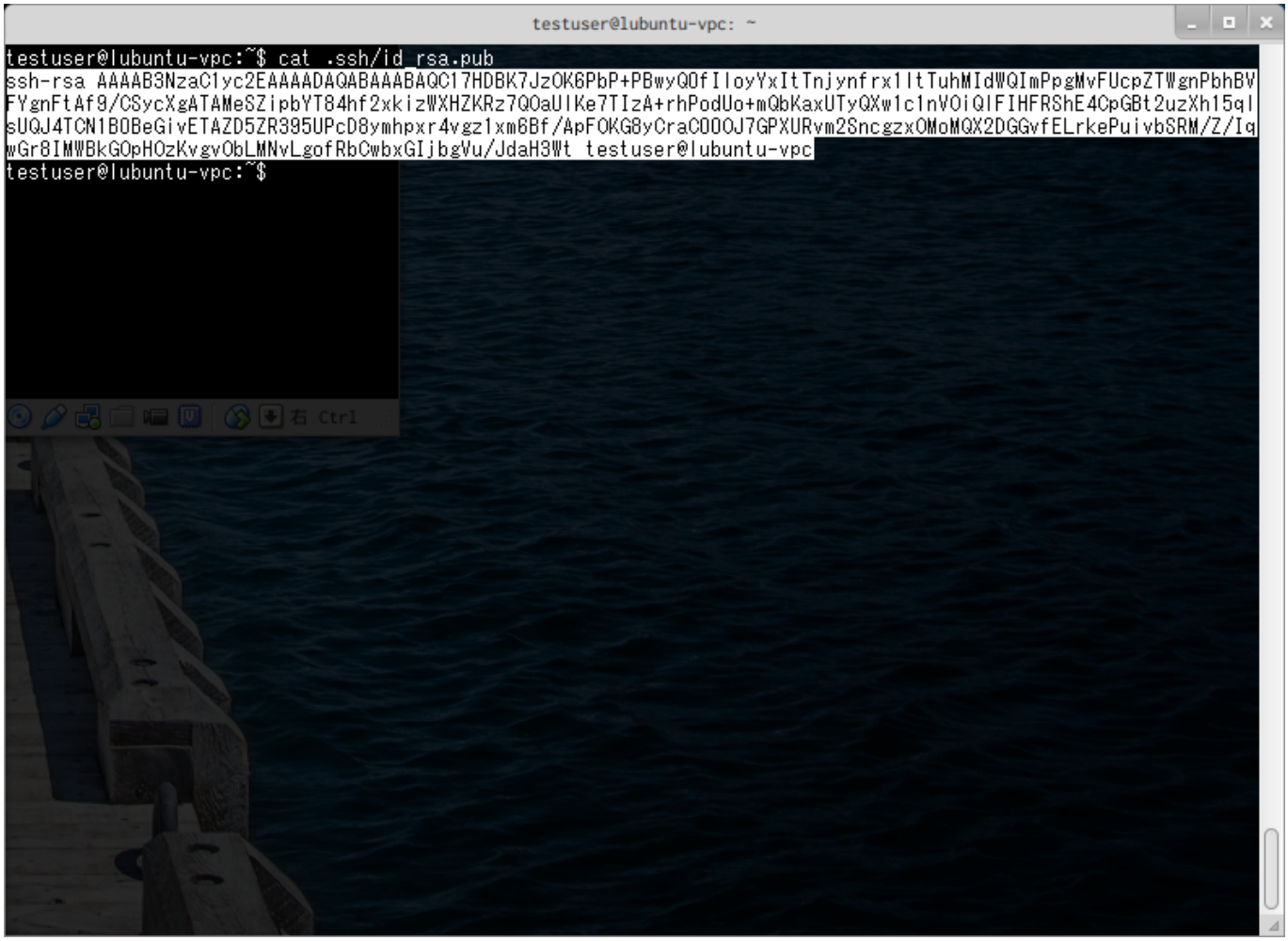
公開鍵の登録

MA-E3xx/4Xxx のログイン先ユーザに、作成した公開鍵を登録します。
2つの端末エミュレータで、公開鍵をコピーペーストする方法が簡単です。

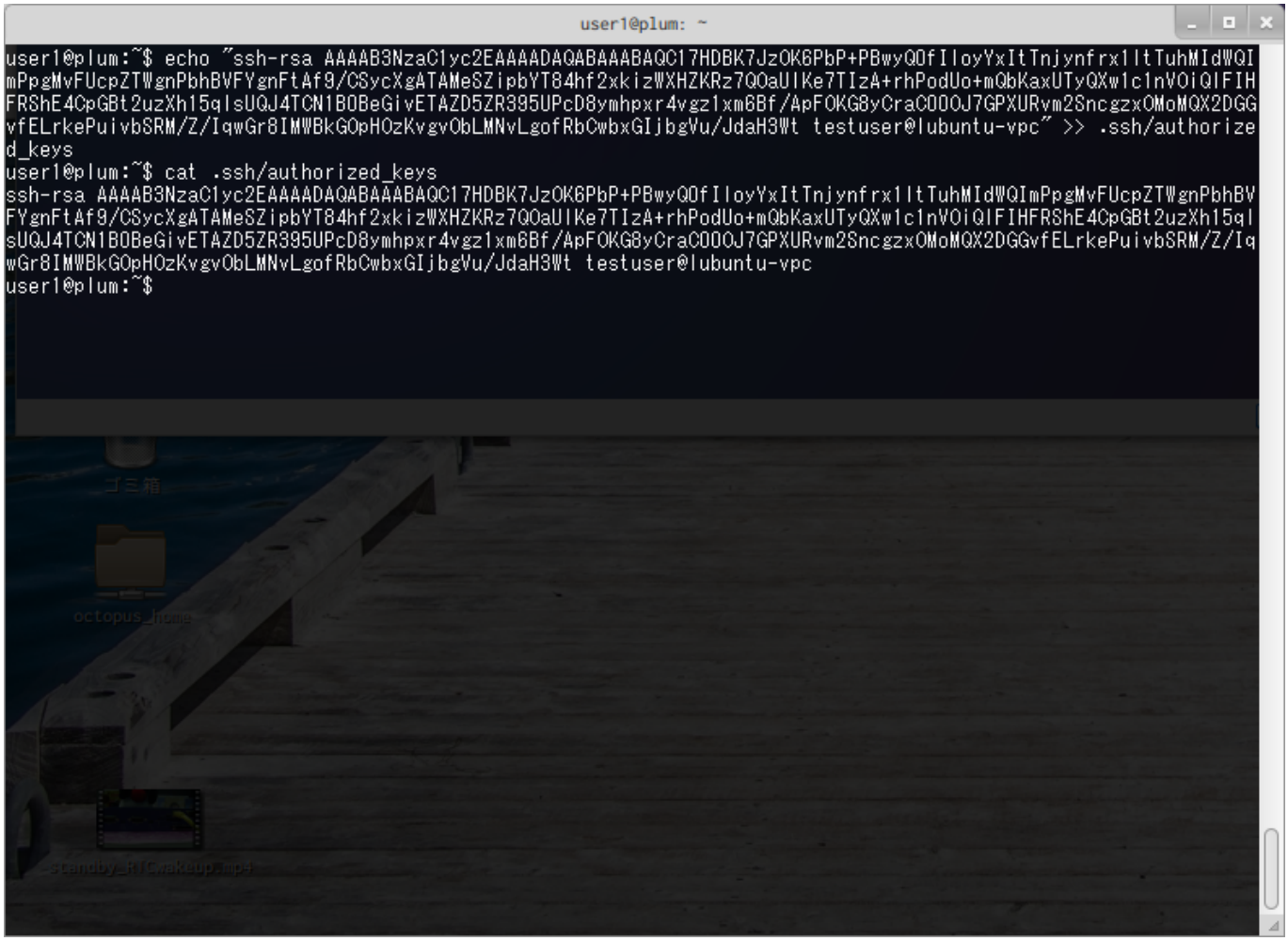
作成した公開鍵を、cat コマンドで表示します。



公開鍵の部分を選択・**コピーします**。

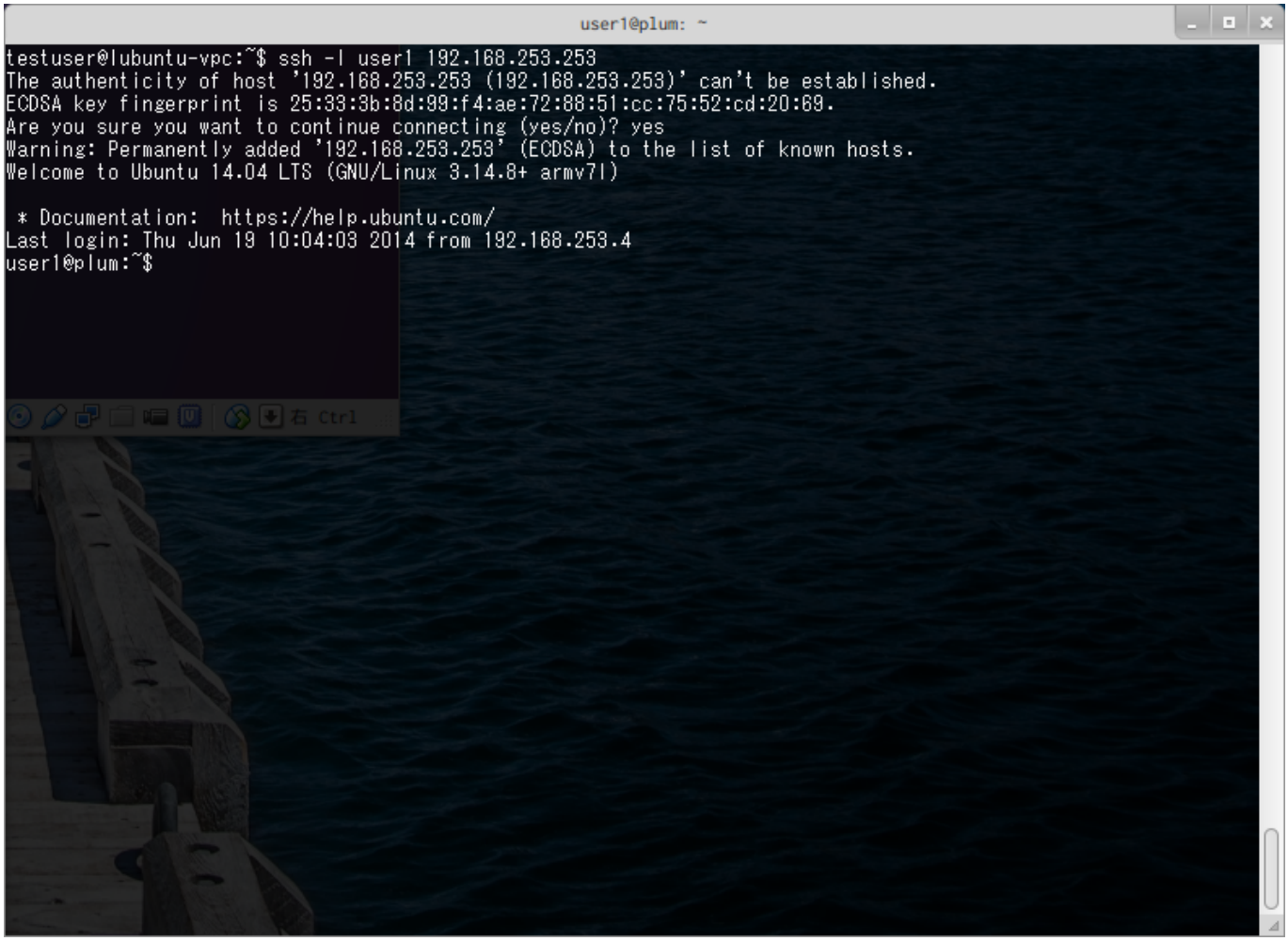


ログイン先の端末**で、**下**のようにペーストし、**echo **コマンドで** .ssh/authorized_keys **へ**追記**します。**



動作確認

パスワード認証を無効にしてしまう前に登録した公開鍵による認証が可能か確認しておきます。



このように、パスワード入力なしでログインができれば、公開鍵は正しく登録されています。

sshd 設定の変更(パスワード認証の無効化)

公開鍵認証によりログインできることが確認できましたので、パスワード認証を無効にします。
/etc/sshd/sshd_config の、下記項目を変更します。

項目名	初期値	設定値	備考
PasswordAuthentication	Yes	No	パスワード認証有効/無効
UsePAM	Yes	No	PAMを使用する/しない

エディタにより、ファイルを編集します。

```
user1@plum:~$ sudo nano -w /etc/ssh/sshd_config
```

編集後のファイルはこのようになります。

sshd_config

```
# Package generated configuration file
```

```
# See the sshd_config(5) manpage for details

# What ports, IPs and protocols we listen for
Port 22
# Use these options to restrict which interfaces/protocols sshd will
bind to
#ListenAddress ::
#ListenAddress 0.0.0.0
Protocol 2
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
#Privilege Separation is turned on for security
UsePrivilegeSeparation yes

# Lifetime and size of ephemeral version 1 server key
KeyRegenerationInterval 3600
ServerKeyBits 1024

# Logging
SyslogFacility AUTH
LogLevel INFO

# Authentication:
LoginGraceTime 120
PermitRootLogin no
StrictModes yes

RSAAuthentication yes
PubkeyAuthentication yes
#AuthorizedKeysFile %h/.ssh/authorized_keys

# Don't read the user's ~/.rhosts and ~/.shosts files
IgnoreRhosts yes
# For this to work you will also need host keys in /etc/ssh_known_hosts
RhostsRSAAuthentication no
# similar for protocol version 2
HostbasedAuthentication no
# Uncomment if you don't trust ~/.ssh/known_hosts for
RhostsRSAAuthentication
#IgnoreUserKnownHosts yes

# To enable empty passwords, change to yes (NOT RECOMMENDED)
PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues
with
# some PAM modules and threads)
ChallengeResponseAuthentication no
```

```
# Change to no to disable tunnelled clear text passwords
PasswordAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosGetAFSToken no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes

X11Forwarding yes
X11DisplayOffset 10
PrintMotd no
PrintLastLog yes
TCPKeepAlive yes
#UseLogin no

#MaxStartups 10:30:60
#Banner /etc/issue.net

# Allow client to pass locale environment variables
#AcceptEnv LANG LC_*

Subsystem sftp /usr/lib/openssh/sftp-server

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
UsePAM no

UseDNS no
```

sshd の再起動

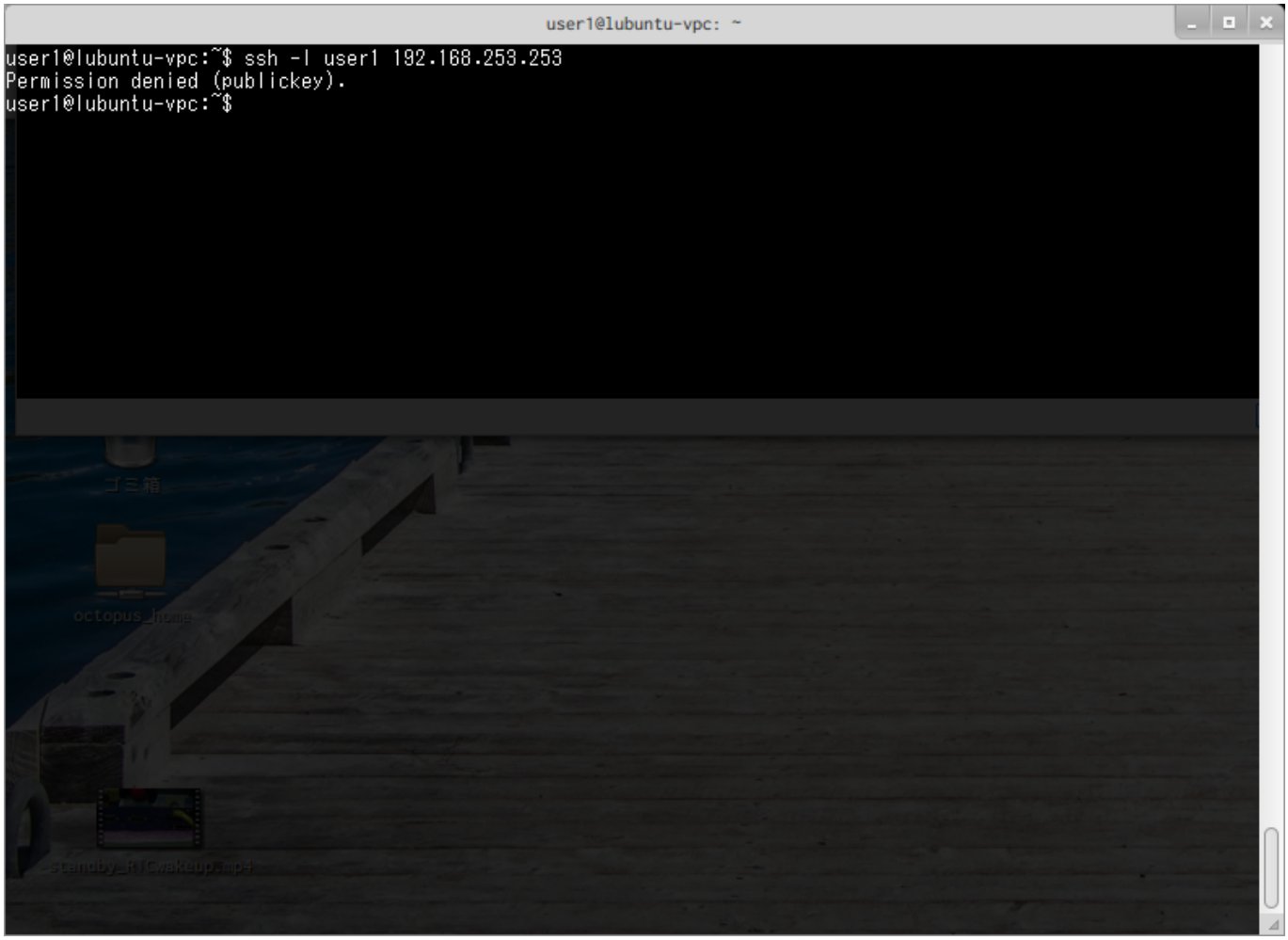
sshdを再起動させます。

```
user1@plum:~$ sudo service ssh restart
```

```
ssh stop/waiting
ssh start/running, process 2310
user1@plum:~$
```

パスワード認証無効の確認

公開鍵を登録していない端末から接続を試し、接続を拒否されることを確認しておきます。



“Permission denied (publickey).” と出力されており、ログインできないことが確認できました。
これで、秘密鍵が漏れない限り、インターネットに晒して使用することができます。

[1)]

http://www.chiark.greenend.org.uk/~sgtatham/putty/