rssh を試してみました

面 和毅

平成 15 年 1 月 14 日

rssh を試してみました

1　rssh の説明

rssh とは、「restricted secure shell」の略です。ログインをさせずに scp/sftp のみをさせたいユーザーのために使用します。

2　rssh の入手方法

rssh は、

`http://www.pizzashack.org/rssh/`

からダウンロードできます。

3　rssh のインストール

適当なディレクトリ (/tmp など) で展開して、

```
./configure
make
```

して、エラーが出ずにコンパイルできたら

```
su -（root になる）
make install
```

で、インストールするだけです。configure の時にオプションを指定しなければ、/usr/local/bin 配下にインストールされているはずです。

4　それぞれの制限されたシェルの説明

ユーザーにどの機能を使用させるかに依って、使用するシェルが変わります。

1. rssh ———- scp, sftp を使用できるが、ログインは出来ない
2. scpsh ———- scp を使用できるが、sftp, ログインは出来ない
3. sftpsh ———- sftp を使用できるが、scp, ログインは出来ない

となります。

5　rssh を使用するユーザーの設定

ユーザーアカウントを作成する時、又は/etc/passwd で/usr/local/bin/rssh などを指定するだけです。

1. test0 ——— scp, sftp の両方を使用できるユーザー
2. test1 ——— scp のみ使用できるユーザー
3. test2 ——— sftp のみ使用できるユーザー
4. testno ——— ログインできないユーザー (比較用)

/etc/passwd には、それぞれ下記のように設定しました。

```
test0:x:501:502::/home/test0:/usr/local/bin/rssh
test1:x:502:503::/home/test1:/usr/local/bin/scpsh
test2:x:503:504::/home/test2:/usr/local/bin/sftpsh
testno:x:504:505::/home/testno:/sbin/nologin
```

6.1 testno(nologin) の場合

比較のために、/sbin/nologin をシェルとしたアカウントでテストしてみます。普通に、ssh でログインしようとすると

```
omok@lucretia:~$ ssh -l testno 172.16.0.10
testno@172.16.0.10's password:
This account is currently not available.
Connection to 172.16.0.10 closed.
```

となり、ログインできません。次に、scp をテストします。

```
omok@lucretia:~$ scp ./testdata testno@172.16.0.10:/tmp
testno@172.16.0.10's password:
This account is currently not available.
```

となり、scp も出来ません。
最後に sftp をテストします。

```
omok@lucretia:~$ sftp testno@172.16.0.10
Connecting to 172.16.0.10...
testno@172.16.0.10's password:
Received message too long 1416128883
```

となり、sftp も出来ません。

6.2 test0(scp 可, sftp 可) の場合

普通に、ssh でログインしようとすると

```
omok@lucretia:~$ ssh -l test0 172.16.0.10
test0@172.16.0.10's password:

This account is restricted to scp or sftp only.  If you believe
 this is in error, please contact your system administrator.

Connection to 172.16.0.10 closed.
```

となります。次に、scp をテストします。

となり、scp は可能です。
　最後に sftp をテストします。

```
omok@lucretia:~$ sftp test0@172.16.0.10
Connecting to 172.16.0.10...
test0@172.16.0.10's password:
sftp> cd /tmp
sftp> mput testdata
Uploading testdata to /tmp/testdata
```

となり、sftp も出来ます。

6.3　test1(scp 可, sftp ダメ) の場合

　普通に、ssh でログインしようとすると

```
omok@lucretia:~$ ssh -l test1 172.16.0.10
test1@172.16.0.10's password:

This account is restricted to scp or sftp only.  If you believe
 this is in error, please contact your system administrator.

Connection to 172.16.0.10 closed.
```

となります。
次に、scp をテストします。

```
omok@lucretia:~$ scp ./testdata test1@172.16.0.10:/tmp
test1@172.16.0.10's password:
testdata              100% |*****************************|   100       00:00
```

となり、scp は可能です。
　最後に sftp をテストします。

```
omok@lucretia:~$ sftp test1@172.16.0.10
Connecting to 172.16.0.10...
test1@172.16.0.10's password:
Connection closed
```

となり、sftp は拒否されます。

6.4　test2(scp ダメ, sftp 可) の場合

　普通に、ssh でログインしようとすると

```
omok@lucretia:~$ ssh -l test2 172.16.0.10
test2@172.16.0.10's password:

This account is restricted to scp or sftp only.  If you believe
 this is in error, please contact your system administrator.

Connection to 172.16.0.10 closed.
```

```
test2@172.16.0.10's password:

This account is restricted to sftp only.  If you believe
 this is in error, please contact your system administrator.

lost connection
```

となり、scp は拒否されます。
　最後に sftp をテストします。

```
omok@lucretia:~$ sftp test2@172.16.0.10
Connecting to 172.16.0.10...
test2@172.16.0.10's password:
sftp> cd /tmp
sftp> mput testdata
Uploading testdata to /tmp/testdata
```

となり、sftp は可能です。