http://ja.528p.com/linux/centos/SE006-chroot-login.html
http://ja.528p.com/linux/centos/SE005-chrootssh.html
http://www.sssg.org/blogs/hiro345/archives/9147.html

sftp で chroot

chroot 先のディレクトリ作成

所有者が root で、755 のディレクトリを作成

/etc/ssh/sshd_config 編集

例 1
sftponly というグループを作成して
Match Group sftponly

```
ForceCommand internal-sftp
ChrootDirectory /home/%u
```

例 2
ユーザを指定
Match user centos

```
ForceCommand internal-sftp
ChrootDirectory /home/%u
```

ssh ログインで chroot

OpenSSH 4.7 以上で対応された

```
ChrootDirectory
```

を使う。

必要なコマンドだけを使う場合

■ chroot 先を作成して、必要なディレクトリを作成する

```
mkdir /opt/chroot_SSH
mkdir /opt/chroot_SSH/bin
mkdir /opt/chroot_SSH/home
mkdir /opt/chroot_SSH/lib
mkdir /opt/chroot_SSH/lib64
```

■コマンドに必要なライブラリとコマンドをコピー

コマンドに必要なライブラリを ldd コマンドで調べて、ライブラリを /opt/chroot_SSH/ 以下にコピーする

例：ls コマンド

```
ldd /bin/ls
```

```
        linux-vdso.so.1 =>  (0x00007fff53b03000)
 libselinux.so.1 => /lib64/libselinux.so.1 (0x00000038e8c00000)
 librt.so.1 => /lib64/librt.so.1 (0x00007f7c057d1000)
 libcap.so.2 => /lib64/libcap.so.2 (0x00000038eb000000)
 libacl.so.1 => /lib64/libacl.so.1 (0x00000038f1c00000)
 libc.so.6 => /lib64/libc.so.6 (0x00007f7c0543d000)
 libdl.so.2 => /lib64/libdl.so.2 (0x00007f7c05238000)
 /lib64/ld-linux-x86-64.so.2 (0x00007f7c059eb000)
 libpthread.so.0 => /lib64/libpthread.so.0 (0x00007f7c0501b000)
 libattr.so.1 => /lib64/libattr.so.1 (0x00000038f7c00000)
cp  /lib64/libselinux.so.1 /opt/chroot_SSH/lib64
cp /lib64/librt.so.1 /opt/chroot_SSH/lib64
....（以下続く）

cp /bin/ls /opt/chroot_SSH/bin
```

手っ取り早く使いたい場合

mount --bind を使って、ひと通りの機能を開放する。
chroot の意味を考えつつ、慎重にやったほうが良い。

■ chroot 先を作成して、必要なディレクトリを作成する

```
mkdir /opt/chroot_SSH
mkdir /opt/chroot_SSH/bin
mkdir /opt/chroot_SSH/home
mkdir /opt/chroot_SSH/lib
mkdir /opt/chroot_SSH/lib64
mkdir /opt/chroot_SSH/usr
```

あとは状況に応じて、 etc、var とか。

■マウントする

シンボリックリンクだと chroot 後はリンクできないが、mount --bind なら問題ない。

```
mount --bind /bin /opt/chroot_SSH/bin
mount --bind /home /opt/chroot_SSH/home
mount --bind /lib /opt/chroot_SSH/lib
mount --bind /lib64 /opt/chroot_SSH/lib64
mount --bind /usr /opt/chroot_SSH/usr
```

■再起動後に自動的にマウントする場合

fstab にマウント情報を書く

```
/bin                    /opt/chroot_SSH/bin     none    bind            0 0
/home                   /opt/chroot_SSH/home    none    bind            0 0
/lib                    /opt/chroot_SSH/lib     none    bind            0 0
/lib64                  /opt/chroot_SSH/lib64   none    bind            0 0
/usr                    /opt/chroot_SSH/usr     none    bind            0 0
```