chroot環境を構築したい

【きっかけ】

データ同期の際、rsync+SSHを利用。自動化を行う為に公開鍵認証方式(パスフレーズなし)で行っているが、
セキュリティ的に心配。万一の場合でも実行可能コマンドが制限されている、chroot環境を構築してみよう。

【手順】

chroot環境を作るのは、意外と手間な作業の為、ネット上で紹介されていたスクリプトを改修して、簡易化を行った。

(0) chroot環境構築スクリプトの入手

https://www.chovits.jp/git/?p=chrootmk.git;a=summary

「shortlog」 一番上(最新)の[snapshot]をクリックするか、
https://www.chovits.jp/git/?p=chrootmk.git;a=tree
から、chroot.sh、useradd.sh を入手。

[スクリプト作成環境]
RockyLinux8 X8684
おそらく、同系統のOS(RHEL8やCentOS8)でも動作すると思う。

(1) SSHログイン(chroot環境で利用する)アカウントを作成。(例：user001)

```
# useradd -u xxxx -g xxxx user001
```

(2) 公開鍵を配置

※ 公開鍵/秘密鍵はログイン元の端末で作成済
```
# su - user001
$ mkdir .ssh
$ chmod 700 .ssh
$ cd .ssh
$ vi authorizedkeys
  (公開鍵をコピペ)
```

(3) chroot構築スクリプト実行

```
# cd ~
# /root/chroot.sh
```
(デフォは、/chrootに出来る)

(4) /chroot配下(chroot環境)にアカウント情報を反映するスクリプト実行

```
# cd ~
# /root/useradd.sh user001
```

(5) sshdconfigを修正する

```
cd /etc/ssh
# cp -pi sshdconfig /sshdconfig.bkup.YYYYMMDD
# vi sshdconfig

Match User user001
ChrootDirectory /chroot/home/user001
```

(6) sshdをプロセス再起動

© 2026 netstaff <netstaff@chovits.net> ¦ 2026-11-22 23:13
URL: https://www.chovits.jp/phpmyfaq/content/0cat=1/25/ja/chroot環境を構築したい.html

systemctl restart sshd

(7) SSHログイン可能か確認

chroot環境にログインしているか確認
※ chroot環境内で必要なコマンドは、chroot.shを修正。
　既にchroot環境を構築済みでも、必要コマンド追記後に再実行OK。
　必要コマンドを除外した場合は、chroot環境から削除されないので手動で削除すること。

【最後に】

chroot環境が必要となる機会はあまり無いと思う。

sftpだけであれば、sshdconfig 「ChrootDirectory /home/user001」を設定すれば、
/bin/bash などのshellが/home/user001配下に存在しなくても、ファイル転送できるらしい。

(参考サイト)

ChrootDirectoryを使ってsshでchroot環境の作成
https://lab.sonicmoov.com/development/server/chrootdirectory-ssh-chroot/

添付ファイル::

一意的なソリューション ID: #1024
製作者: n/a
最終更新: 2022-10-24 08:58

© 2026 netstaff <netstaff@chovits.net> | 2026-11-22 23:13
URL: https://www.chovits.jp/phpmyfaq/content/0cat=1/25/ja/chroot環境を構築したい.html