LinuC

LinuC レベル1 技術解説セミナー
2022/1/15 開催

「セキュリティ管理」

主題	1.10：セキュリティ
副題	1.10.1 セキュリティ管理業務の実施 1.10.2 ホストのセキュリティ設定

三澤 康巨

LPI-JAPAN

本日の講師

三澤 康巨

- KDDI株式会社で、電話等のネットワークサービス設備のエンジニアリングをはじめ様々な業務を担当しました。
- 2017年10月から2年半、KDDIグループ内のサーバ研修講師を務めました。
- サーバ研修受講者の中から、200名を超える LinuC レベル1 合格者を出しました。
- 2020年3月、KDDIを定年退職しました。

- LinuCレベル1技術解説セミナーの講師を担当
  - 2020年7月18日「ブートプロセスとsystemd」
  - 2021年1月23日「ハードディスクのレイアウトとパーティション」
  - 2021年3月　6日「ファイルシステムの作成と管理、マウント」
  - 2021年6月26日「テキストデータ処理」
- その他
  - 2020年11月28日、オープンソースカンファレンス２０２０ オンライン/福岡「Linuxマシンを作ってみよう　～LinuC レベル１／レベル２ 学習環境構築ガイド～」の講師を担当

LinuCレベル１／レベル２ Version10.0とは

■LinuCとは

クラウド時代の即戦力エンジニアであることを証明するLinux技術者認定

✓現場で「今」求められている新しい技術要素に対応

- オンプレミス／仮想化・コンテナを問わず様々な環境下でのサーバー構築
- 他社とのコラボレーションの前提となるオープンソースへの理解
- システムの多様化に対応できるアーキテクチャへの知見

✓全面的に見直した「今」身につけておくべき技術範囲を網羅

今となっては使わない技術やコマンドの削除、アップデート、新領域の取り込み

✓Linuxの範疇だけにとどまらない領域までカバー

セキュリティや監視など、ITエンジニアであれば必須の領域もカバー

クラウドを活用できるITエンジニアに必須の技術がまとまっている

AWSなどのパブリッククラウドを活用するための技術

間が欠けている状態

オンプレミスのサーバーサイドLinux技術

【今まで／その他】

AWSなどのパブリッククラウドを活用するための技術

仮想マシン／コンテナ技術、クラウドセキュリティ、アーキテクチャ、ほか

オンプレミスのサーバーサイドLinux技術

LinuC Version10.0

セキュリティ管理

1.はじめに

2.システム管理者権限の利用と設定

3.ユーザ管理

4.セキュリティ調査と設定

1.はじめに

2.システム管理者権限の利用と設定

3.ユーザ管理

4.セキュリティ調査と設定

はじめに

■本セミナーでは、主題1.10の中から、「セキュリティ管理」について解説します。

■システム管理者はシステムを安全に運用する必要があります。本セミナーではセキュリティ管理の基本として、管理者権限、ユーザ管理、サービス管理等について学習します。

※暗号の利用（SSH、GnuPG）は今回の解説範囲に含まれません（副題1.10.3）。

■学習効果を高めるため、実行例の出てくる部分では、ご自分でも実行してみることをお勧めします。

■Linuxには多数のディストリビューションが存在しますが、本セミナーの実行例では、CentOS 7 を使用します。

- ビジネス用サーバーの多くで稼働している Red Hat Enterprise Linux 7 (RHEL7) と互換性があります。
- RHEL7は有料ですが、CentOS 7 は無料で利用できます。
- CentOSとRHELの最新バージョンは「8」ですが、本セミナーでは、普及が進んでいるバージョン「7」を使います。

はじめに

■CentOS 7 に基づく学習環境の構築方法を、LPI-Japanのサイトでご紹介しています。

LinuC レベル１／レベル２ Version 10.0 学習環境構築ガイド

https://linuc.org/docs/v10/guide_text.pdf

■学習環境構築ガイドでは、2種類の環境の構築方法を紹介しています。

【環境A】

- 用意したコンピュータの内蔵ストレージを上書きして、Linux専用コンピュータを構築します。
- WindowsやMacOS等の既存OSは使えなくなります。
- 不要になった古いPC等がある場合に、それを使ってください。

【環境B】

- WindowsやMacOS等の既存OSを壊すことなく、外付けSSDにLinuxをインストールします。
- これによって、既存OSとLinuxとの間を切り替えて利用することができます。
- 但し、既存OSとLinuxとを同時に利用することはできません。

1.はじめに

2.システム管理者権限の利用と設定

3.ユーザ管理

4.セキュリティ調査と設定

管理者権限とsuコマンド

■システム管理者権限を利用するには、スーパーユーザ（root）でログインするのが最も簡便ですが、作業ミスなどのリスクも高くなってしまいます。そこで、一般ユーザでログインし、必要な時だけスーパーユーザに切り替えて権限を利用することが一般的です。

■ユーザを切り換えるには、suコマンドを使用します。

su コマンド

su［オプション］［ユーザ名］　※ユーザ名を省略するとスーパーユーザに切り替え

オプション	説　明
-	ユーザ環境も切り替える（カレントディレクトリやシェル変数など）

管理者権限とsuコマンド

ユーザの切り替え

```
$ su -
パスワード:
最終ログイン: 2022/01/04 (火) 18:59:05 JST日時 pts/0
# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
# pwd
/root
# exit
ログアウト
$ id
uid=1000(user1) gid=1000(user1) groups=1000(user1)
context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
```

sudoコマンド

- 一般ユーザに管理作業を委託する場合には、 /etc/sudoers ファイルに設定を記述します。委託されたユーザは、sudoコマンドを利用します。
- この仕組みにより、スーパーユーザのパスワードを共有する必要がなく、必要なコマンドだけを許可することができます。
- /etc/sudoers ファイルを安全に編集するには、visudoコマンドを使用します。

/etc/sudoers ファイルの書式

```
ユーザ名 許可するホスト=(実行ユーザ) 許可するコマンド [,コマンド・・・]
```

sudo コマンド

```
sudo [オプション] 実行コマンド
```

オプション	説　明
-u ユーザ名	実行ユーザを指定（デフォルトはスーパーユーザ）

sudoコマンド

sudoの利用

```
$ su -
パスワード:
最終ログイン: 2022/01/04 (火) 19:09:45 JST日時 pts/0
# grep user1 /etc/sudoers
user1 ALL=(ALL)       /bin/cat /var/log/messages, /bin/cat /var/log/secure
# exit
ログアウト
$ cat /var/log/secure
cat: /var/log/secure: 許可がありません
$ sudo cat /var/log/secure
[sudo] user1 のパスワード:
Jun 21 13:14:44 SSD2-CentOS7 su: pam_unix(su-l:session): session opened for user root by
user1(uid=1000)
 . . .
Jan  4 19:16:43 SSD2-CentOS7 sudo:   user1 : TTY=pts/0 ; PWD=/home/user1 ; USER=root ;
COMMAND=/bin/cat /var/log/secure    ※sudo利用のログ
Jan  4 19:16:43 SSD2-CentOS7 sudo: pam_unix(sudo:session): session opened for user root
by user1(uid=0)
```

sudoコマンド

sudoの利用

```
$ sudo -l    ※自分に許可されているコマンドを調べる
既定値のエントリと照合中 (ユーザー名 user1) (ホスト名 SSD2-CentOS7):
    !visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin, env_reset,
env_keep="COLORS DISPLAY HOSTNAME
    HISTSIZE KDEDIR LS_COLORS", env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS
LC_CTYPE", env_keep+="LC_COLLATE
    LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES", env_keep+="LC_MONETARY LC_NAME
LC_NUMERIC LC_PAPER LC_TELEPHONE",
    env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
secure_path=/sbin¥:/bin¥:/usr/sbin¥:/usr/bin

ユーザー user1 は SSD2-CentOS7 上で コマンドを実行できます
    (ALL) /bin/cat /var/log/messages, /bin/cat /var/log/secure
```

1.はじめに

2.システム管理者権限の利用と設定

3.ユーザ管理

4.セキュリティ調査と設定

ユーザ管理情報

- ユーザを管理している情報は /etc/passwd ファイルと /etc/shadow ファイルに格納されています。（副題1.08.1の範囲）
- ユーザのパスワードは /etc/shadow ファイルに格納されています。同ファイルはパーミッションが “000” となっていて、パスワードを盗み見られないように保護されています。パスワードはハッシュ化（暗号化）された形で格納されているため、システム管理者であってもパスワード自体を知ることはできません。

/etc/shadow ファイルとパスワード

```
# ls -l /etc/shadow
----------. 1 root root 1292  5月  2  2021 /etc/shadow
# cat /etc/shadow
root:$6$N3e9dUea5sdhJnvl$IQITNQN8vLuT1wM8eyORwFk9JZNShjIMKOxaVfTx4cpEqXQ4Y6fLSdd.MaHAvoltSJAcesQwrCZxy3Ju7zupp0::0:99999:7:::
 . . .
user1:$6$WCsQolEAOugut5wQ$2dEIwTqoc/xRIUSHXNgsZ3j7YgfALijdxBN/C/lilCjiRG3l7O4Au.dbWLMoOVR2b3p40JIVlDqu2yOMY8X8c1::0:99999:7:::
 . . .
```

※ユーザ名:ハッシュ化されたパスワード:最終変更日:変更可能最短日数:有効期限:警告日:使用不可になるまでの日数:アカウント有効期限:予約フィールド

パスワードの設定・変更

■スーパーユーザはシステム内ユーザのパスワードを設定・変更することができます。

passwd コマンド

```
passwd [オプション] [ユーザ名]
```

パスワードの設定・変更

```
# useradd user9
# grep user9 /etc/shadow
user9:!!:18996:0:99999:7:::     ※パスワードが設定されていないので、まだアカウントを利用できない。
# passwd user9
ユーザー user9 のパスワードを変更。
新しいパスワード:
よくないパスワード: このパスワードは 7 未満の文字列です。
新しいパスワードを再入力してください:
passwd: すべての認証トークンが正しく更新できました。
# grep user9 /etc/shadow
user9:$6$Ws/GqxuJ$iYT0iKm2BKs7Eq/e3lwM7aBqVB7KQxe7CD9sHUSCDK3j/KycaH9ri8c/7C98YA3T01QoZSN
AHCQNv3/KmK4bW1:18996:0:99999:7:::
```

パスワードエージング情報の設定・変更

- /etc/shadowファイルに格納されたパスワードエージング情報を、システム管理者は適切に管理しなければなりません。passwdコマンド、usermodコマンド、chageコマンドを使用します。

passwd コマンド

```
passwd [オプション] [ユーザ名]
```

オプション	説　明
-x 日数	パスワードの有効期限を設定（chage -M と同じ：後出）
-e	パスワードを有効期限切れにする

パスワード有効期限の設定

```
# passwd -x 30 user9
ユーザー user9 のエージングデータを調節。
passwd: 成功
# grep user9 /etc/shadow
user9:$6$Ws/GqxuJ$iYT0iKm2BKs7Eq/e3lwM7aBqVB7KQxe7CD9sHUSCDK3j/KycaH9ri8c/7C98YA3T01QoZSN
AHCQNv3/KmK4bW1:18996:0:30:7:::
```

パスワードエージング情報の設定・変更

usermod コマンド

```
usermod [オプション] ユーザ名
```

オプション	説　明
-e 年-月-日	アカウントの有効期限を設定（chage -E と同じ：後出）

アカウント有効期限の設定

```
# usermod -e 2022-3-31 user9
# grep user9 /etc/shadow
user9:$6$Ws/GqxuJ$iYT0iKm2BKs7Eq/e3lwM7aBqVB7KQxe7CD9sHUSCDK3j/KycaH9ri8c/7C98YA3T01QoZSN
AHCQNv3/KmK4bW1:18996:0:30:7::19082:
```

パスワードエージング情報の設定・変更

- chageコマンドで様々なエージング（有効期限）情報を変更できます。変更結果は /etc/shadow ファイルに反映されます。

chage コマンド
chage [オプション] ユーザ名

オプション	説　明
-l	有効期限情報を表示
-m 日数	パスワードを変更できる最短日数を設定
-M 日数	パスワードの有効期限を設定（passwd -x と同じ）
-I 日数	パスワードの有効期限が切れてからアカウントを無効化するまでの日数を設定
-W 日数	パスワードの有効期限の警告を何日前から表示するかを設定
-E 年-月-日	アカウントの有効期限を設定（usermod -e と同じ）

パスワードエージング情報の設定・変更

様々なエージング情報の変更

```
# chage -l user9
最終パスワード変更日                                  :  1月 04, 2022
パスワード期限:                                       :  2月 03, 2022
パスワード無効化中                                    : なし
アカウント期限切れ                                    :  3月 31, 2022
パスワードが変更できるまでの最短日数                  : 0
パスワードを変更しなくてよい最長日数                  : 30
パスワード期限が切れる前に警告される日数              : 7
# chage -m 3 -M 60 -I 10 -W 5 -E 2022-10-31 user9
# chage -l user9
最終パスワード変更日                                  :  1月 04, 2022
パスワード期限:                                       :  3月 05, 2022
パスワード無効化中                                    :  3月 15, 2022
アカウント期限切れ                                    : 10月 31, 2022
パスワードが変更できるまでの最短日数                  : 3
パスワードを変更しなくてよい最長日数                  : 60
パスワード期限が切れる前に警告される日数              : 5
# grep user9 /etc/shadow
user9:$6$Ws/GqxuJ$iYT0iKm2BKs7Eq/e3lwM7aBqVB7KQxe7CD9sHUSCDK3j/KycaH9ri8c/7C98YA3T01QoZSN
AHCQNv3/KmK4bW1:18996:3:60:5:10:19296:
```

ログインの禁止

- passwdコマンドまたはusermodコマンドでパスワードをロックし、ユーザのログインを禁止することができます。特定ユーザのログインを一時的に禁止する場合に使用します。

passwd コマンド

```
passwd [オプション] ユーザ名
```

オプション	説　明
-l	パスワードをロック
-u	パスワードロックを解除

usermod コマンド

```
usermod [オプション] ユーザ名
```

オプション	説　明
-L	パスワードをロック
-U	パスワードロックを解除

ログインの禁止

パスワードロック

```
# passwd -l user9
ユーザー user9 用のパスワードをロック。
passwd: 成功
# grep user9 /etc/shadow
user9:!!$6$Ws/GqxuJ$iYT0iKm2BKs7Eq/e3lwM7aBqVB7KQxe7CD9sHUSCDK3j/KycaH9ri8c/7C98YA3T01QoZ
SNAHCQNv3/KmK4bW1:18996:3:60:5:10:19296:
# passwd -u user9
ユーザー user9 用のパスワードをロック解除。
passwd: 成功
# grep user9 /etc/shadow
user9:$6$Ws/GqxuJ$iYT0iKm2BKs7Eq/e3lwM7aBqVB7KQxe7CD9sHUSCDK3j/KycaH9ri8c/7C98YA3T01QoZSN
AHCQNv3/KmK4bW1:18996:3:60:5:10:19296:
# usermod -L user9
# grep user9 /etc/shadow
user9:!$6$Ws/GqxuJ$iYT0iKm2BKs7Eq/e3lwM7aBqVB7KQxe7CD9sHUSCDK3j/KycaH9ri8c/7C98YA3T01QoZS
NAHCQNv3/KmK4bW1:18996:3:60:5:10:19296:
# usermod -U user9
# grep user9 /etc/shadow
user9:$6$Ws/GqxuJ$iYT0iKm2BKs7Eq/e3lwM7aBqVB7KQxe7CD9sHUSCDK3j/KycaH9ri8c/7C98YA3T01QoZSN
AHCQNv3/KmK4bW1:18996:3:60:5:10:19296:
```

ログインの禁止

- ログインシェルを /bin/false または /sbin/nologin に変更することによっても、ログインを禁止できます。

ログインシェル変更によるログイン禁止

```
# usermod -s /bin/false user9
# grep user9 /etc/passwd
user9:x:1001:1001::/home/user9:/bin/false
# usermod -s /sbin/nologin user9
# grep user9 /etc/passwd
user9:x:1001:1001::/home/user9:/sbin/nologin
# usermod -s /bin/bash user9
# grep user9 /etc/passwd
user9:x:1001:1001::/home/user9:/bin/bash
# grep /sbin/nologin /etc/passwd
 . . .
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
 . . .
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
 . . .
apache:x:48:48:Apache:/usr/share/httpd:/sbin/nologin
```

ログインの禁止

- /etc/nologin ファイルを作成すると、全ての一般ユーザのログインを禁止できます。システム保守作業等の際に使用します。

ログインの全面禁止

```
# touch /etc/nologin

# rm /etc/nologin
rm: 通常の空ファイル `/etc/nologin' を削除しますか?
```

ユーザの利用状況監視

- システム管理者はユーザのシステム利用状況を監視して、不正利用や侵入などを防止します。
- whoコマンド、wコマンドで現在のログイン状況を確認できます。

who コマンド

```
who [オプション]
```

w コマンド

```
w [オプション]
```

ユーザの利用状況監視

ログイン状況の確認

```
# who
root     :0           2022-01-04 18:22 (:0)
user1    pts/0        2022-01-04 18:58 (:1)
user1    :1           2022-01-04 18:57 (:1)
# w
 21:45:24 up  3:24,  3 users,  load average: 0.00, 0.05, 0.10
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     :0       :0               18:22   ?xdm?   4:53   0.25s /usr/libexec/gnome-
session-binary --session gnome-classic
user1    pts/0    :1               18:58    4.00s  0.25s 15.28s /usr/libexec/gnome-
terminal-server
user1    :1       :1               18:57   ?xdm?   4:53   0.24s /usr/libexec/gnome-
session-binary --session gnome-classic
```

ユーザの利用状況監視

■lastコマンドでログインの履歴を確認できます。

last コマンド

```
last [オプション]
```

ログイン履歴の確認

```
# last
user1    pts/1        :1               Tue Jan  4 21:36 - 21:36  (00:00)
user1    pts/0        :1               Tue Jan  4 18:58   still logged in
user1    :1           :1               Tue Jan  4 18:57   still logged in
root     pts/0        :0               Tue Jan  4 18:26 - 18:56  (00:30)
root     :0           :0               Tue Jan  4 18:22   still logged in
. . .
```

リソース管理

■特定ユーザがシステムリソースを過剰に使用すると、システム全体に悪影響を与える場合があります。ulimitコマンドによって使用可能なリソースを制限できます。ユーザのシェル環境設定ファイルに含めておけば、当該ユーザに制限が適用されます。

ulimit コマンド

```
ulimit [オプション]
```

オプション	説　明
-a	制限値の一覧を表示
-c ブロック数	コアダンプファイルのサイズを制限
-n ファイル数	同時に開けるファイル数を制限

リソース管理

リソースの制限

```
$ ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
scheduling priority             (-e) 0
file size               (blocks, -f) unlimited
pending signals                 (-i) 30607
max locked memory       (kbytes, -l) 64
max memory size         (kbytes, -m) unlimited
open files                      (-n) 1024
 . . .
$ ulimit -n 64
$ ulimit -a
 . . .
open files                      (-n) 64
 . . .
```

自動ログアウト

■操作を長く中断しているユーザを自動的にログアウトさせるには、環境変数TMOUTを設定します。ユーザのシェル環境設定ファイルに含めておけば、当該ユーザに設定が適用されます。

自動ログアウトの設定

```
$ export TMOUT=300     ※5分間で自動ログアウト
$ echo $TMOUT
300
```

1.はじめに

2.システム管理者権限の利用と設定

3.ユーザ管理

4.セキュリティ調査と設定

実行ファイルの権限管理

- SUIDやSGIDビットが設定されている実行可能ファイルは、一般ユーザが実行しても高い権限で実行されます。（副題1.02.1の範囲）
- 必要のないファイルにまでSUID/SGIDが設定されていると、セキュリティホールになる恐れがあります。管理者はシステム内の状態を調査し、常に適正に維持しなければなりません。
- findコマンドの -permオプションを使って、 SUID/SGIDが設定されているファイルを検索することができます。

SUIDまたはSGIDが設定されているファイルを検索する

```
# find / -perm -4000 | xargs ls -l    ※SUIDは4000、SGIDは2000
 . . .
-rwsr-xr-x. 1 root root      27856  4月  1  2020 /usr/bin/passwd
 . . .
-rwsr-xr-x. 1 root root      32128  4月  1  2020 /usr/bin/su
---s--x--x. 1 root root     147336  4月  1  2020 /usr/bin/sudo
 . . .
```

ポートの管理

- 外部からの攻撃を防ぐためには、開いているポートを最小限に抑える必要があります。
- lsofコマンドでポートやファイルを開いているプロセスを調べることができます。

lsof コマンド

```
lsof [オプション] [ファイル名]
```

オプション	説　明
-i[:ポート番号]	指定したポートを開いているプロセスを表示

ポートを開いているプロセスの調査

```
# lsof -i
COMMAND    PID   USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
 . . .
sshd      1469   root    3u  IPv4  30133      0t0  TCP *:ssh (LISTEN)
sshd      1469   root    4u  IPv6  30135      0t0  TCP *:ssh (LISTEN)
 . . .
# lsof -i:22
COMMAND  PID USER   FD   TYPE DEVICE SIZE/OFF NODE NAME
sshd    1469 root    3u  IPv4  30133      0t0  TCP *:ssh (LISTEN)
sshd    1469 root    4u  IPv6  30135      0t0  TCP *:ssh (LISTEN)
```

ポートの管理

ファイルを開いているプロセスの調査

別の端末から

```
$ less /etc/passwd

# lsof /etc/passwd
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1000/gvfs
      Output information may be incomplete.
COMMAND   PID  USER   FD   TYPE DEVICE SIZE/OFF     NODE NAME
less    10247 user1    4r   REG  253,0     2419 35199543 /etc/passwd
```

ポートの管理

■fuserコマンドでも、ファイルを開いているプロセスを調べることができます。

fuser コマンド

```
fuser [オプション] [ファイル名]
```

オプション	説　明
-v	詳細情報を表示

ファイルを開いているプロセスの調査

```
# fuser -v /etc/passwd
                     USER        PID ACCESS COMMAND
/etc/passwd:         user1     10247 f.... less
```

ポートの管理

- netstatコマンドを使用してシステム内の開いているポートを調査できます。ssコマンドでも同様です。

netstat コマンド

netstat [オプション]

オプション	説　明
-n	名前解決しないで表示
-t	TCP通信を表示
-u	UDP通信を表示
-l	待機（listen）しているポートを表示
-p	プロセス情報を表示

ポートの管理

開いているポートの調査

```
# netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
PID/Program name
tcp        0      0 192.168.122.1:53        0.0.0.0:*               LISTEN
1937/dnsmasq
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1469/sshd
tcp        0      0 127.0.0.1:631           0.0.0.0:*               LISTEN
1473/cupsd
tcp        0      0 127.0.0.1:25            0.0.0.0:*               LISTEN
1883/master
tcp        0      0 0.0.0.0:111             0.0.0.0:*               LISTEN
838/rpcbind
tcp6       0      0 :::22                   :::*                    LISTEN      1469/sshd
tcp6       0      0 ::1:631                 :::*                    LISTEN
1473/cupsd
tcp6       0      0 ::1:25                  :::*                    LISTEN
1883/master
tcp6       0      0 :::111                  :::*                    LISTEN
838/rpcbind
```

ポートの管理

- nmapコマンドは、リモートホストの開いているポートを調査（ポートスキャン）できます。

nmap コマンド

```
nmap [オプション] ホスト
```

リモートホストの開いているポートの調査

```
# nmap 192.168.10.20

Starting Nmap 6.40 ( http://nmap.org ) at 2022-01-04 22:12 JST
Nmap scan report for 192.168.10.20
Host is up (0.000011s latency).
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
111/tcp open  rpcbind
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 1.63 seconds
```

ネットワークサービスの管理

■起動しているネットワークサービスを狙って、外部から攻撃される恐れがあります。必要のないサービスは停止し、自動起動設定も解除しておきます。

不要なサービスの停止

```
# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset:
disabled)
   Active: active (running) since 火 2022-01-04 22:15:11 JST; 11s ago
 . . .
# systemctl stop httpd    ※Webサービスが必要なければ、停止する。
# systemctl disable httpd    ※システム再起動時に自動起動しないように設定する
Removed symlink /etc/systemd/system/multi-user.target.wants/httpd.service.
# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset:
disabled)
   Active: inactive (dead)
```

ネットワークサービスの管理

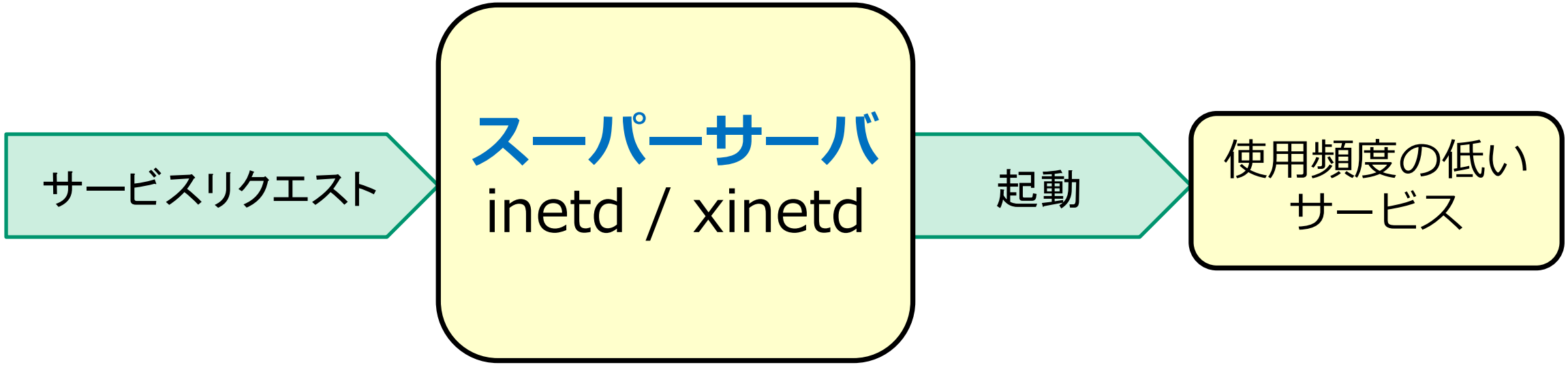
- 古いディストリビューション（RedHat系ならVer.6以前）では、systemdではなくinitプロセスがシステム全体を制御していました。serviceコマンドでサービスの状態確認と制御、chkconfigコマンドで自動起動の設定を行います。
- serviceコマンドは /etc/init.d/ ディレクトリに置いてあるスクリプトを実行します。そのスクリプトのパスを指定しても、実行することができます。

不要なサービスの停止

```
# service httpd status
httpd は起動しています
# service httpd stop    ※Webサービスが必要なければ、停止する。
httpd を停止中:
# chkconfig httpd off    ※システム再起動時に自動起動しないように設定する
# /etc/init.d/httpd status    ※service httpd status と同じ
httpd は停止しています
```

スーパーサーバ inetd, xinetd

- サービスの起動状態ではサーバプロセスがリクエストを待機（listen）しているので、使用頻度の低いサービスを起動していると、メモリの無駄遣いになります。この問題を解決する仕組みがスーパーサーバで、実装方式に inetd と xinetd があります。しかし、近年ではメモリが大型化しているため、使われることが少なくなっています。
- この方式では、スーパーサーバが設定されたサービスのリクエストを待機（listen）していて、リクエストを受付けた時に、要求されたサービスを起動します。



スーパーサーバ inetd, xinetd

- inetdの設定ファイルは /etc/inetd.conf です。必要のないサービスは、該当行をコメントアウトして、無効化します。

inetdの設定

```
# vi /etc/inetd.conf
 . . .
#telnet        stream  tcp     nowait  root    /usr/sbin/tcpd /usr/sbin/telnetd
 . . .
# service restart inetd
```

スーパーサーバ inetd, xinetd

- xinetdでは、/etc/xinetd.conf に全般的な設定を記述し、/etc/xinetd.d/ ディレクトリ下のファイルにサービス毎の設定を行います。

xinetdの設定

```
# cat /etc/xinetd.d/telnet
service telnet
{
        disable         = yes    ※yes：無効、no：有効
        . . .
}
```

Firewall

- 複数のLinuxカーネルモジュールから成る Netfilter は、テーブルとチェインの設定に従ってパケットを処理します。filterテーブルのチェインを設定することによって、Firewall機能を実現しています。

テーブル	説　明
filter	パケットフィルタリングの設定
nat	アドレス変換(NAT)の設定

チェイン	説　明
INPUT	自ホストへの入力パケットに適用するルール
OUTPUT	自ホストからの出力パケットに適用するルール
FORWARD	自ホストを経由する転送パケットに適用するルール
PREROUTING	ルーティング決定前に適用するルール
POSTROUTING	ルーティング決定後に適用するルール

Firewall

- Netfilterを設定するには、firewalld または iptables を使用します。いずれも、内部ではiptablesコマンドを実行しています。
- CentOS 7 の初期状態では、firewalldが有効に、iptablesが無効になっています。

Netfilter設定ユーティリティの確認

```
# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset:
enabled)
   Active: active (running) since 火 2022-01-04 18:21:29 JST; 4h 7min ago
 . . .
# systemctl list-units -a | grep iptables
● iptables.service
not-found inactive dead      iptables.service
```

Firewall

- firewalldにはゾーンと呼ぶテンプレートが用意されていて、簡単に設定できるようになっています。ゾーンをカスタマイズすることも可能です。

ゾーン	説　明
drop	外部からのパケットを全て破棄(drop)、ICMPリプライも返送しない。
public	パブリックエリア用　　※初期値
work	作業エリア用
home	家庭用
trusted	全てのパケットを許可

- firewalldを利用するには firewall-cmdコマンドまたはfirewall-config（GUIツール）を使います。

firewall-cmd コマンド

```
firewall-cmd [オプション]
```

Firewall

firewalldによるNetfilter設定

```
# firewall-cmd --get-active-zones
public
  interfaces: wlp7s0
# firewall-cmd --get-default-zone
public
# firewall-cmd --list-services --zone=public
dhcpv6-client ssh
# firewall-cmd --add-service=http --zone=public    ※許可サービスを追加
success
# firewall-cmd --list-services --zone=public
dhcpv6-client http ssh
# firewall-cmd --list-services --zone=public --permanent
dhcpv6-client ssh    ※httpは恒久化されていない
# firewall-cmd --add-service=http --zone=public --permanent    ※恒久的に追加
success
# firewall-cmd --list-services --zone=public --permanent
dhcpv6-client http ssh
```

Firewall

firewalldによるNetfilter設定

```
# cat /etc/firewalld/zones/public.xml    ※publicゾーンの設定ファイル
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Public</short>
  <description>For use in public areas. You do not trust the other computers on networks
to not harm your computer. Only selected incoming connections are accepted.</description>
  <service name="ssh"/>
  <service name="dhcpv6-client"/>
  <service name="http"/>
</zone>
```

本セミナーのまとめ

1. CentOS 7 に基づく学習環境を自分で構築してみましょう。

2. システム管理者権限を利用するには、suコマンドまたはsudoコマンドを使います。

3. システム管理者は、ユーザのパスワードや利用状況を適切に管理しなければなりません。

4. システム管理者は、ポート、ネットワークサービス、Firewall設定などを適切に管理しなければなりません。

ご清聴ありがとうございました