

コンピュータ科学実験 1

ソフトウェア実験第一回レポート

名古屋大学情報学部コンピュータ科学科3年
101730196 竹安稜真

目次

1	概要	1
2	はじめに	1
2.1	本実験の目的	1
2.2	実験対象の説明	1
3	各実験	2
3.1	[課題 1] 初期環境の確認	2
3.2	[課題 2] ネットワーク設定	10
3.3	[課題 3] DHCP サービスの設定	21
3.4	[課題 4] ファイアウォールの設定	26
3.5	[課題 5] WWW サービスの設定	38
4	まとめ	44
	参考文献	44

1 概要

2 はじめに

2.1 本実験の目的

本実験での目的は TCP/IP ネットワークにおける各種サービスの提供・利用のために必要な基本的知識を学習することである。今回はローカルネットワーク・DMZ ネットワークを備えるサブネットワークを構築し、Linux におけるネットワーク構成方法、ファイアウォール設置方法を学習することを通じて現代の様々な計算機利用において必要不可欠になっている情報通信ネットワークに対する知見を深める。

2.2 実験対象の説明

2.2.1 TCP/IP ネットワークについて

ネットワーク越しに何かを送るときに必要なプロトコル（通信規約）の代表例、TCP「Transmission Control Protocol」と IP「Internet Protocol」を組み合わせたものである。TCP は信頼性に富み、IP は通信速度に富んでいる。本実験では TCP,IP の他に HTTP,DHCP,SSH,DNS, などのプロトコルが登場する。

（文献 [1], 文献 [2] を参考。）

2.2.2 ローカルネットワークについて

通称 LAN。限られた範囲内にあるコンピュータや通信機器、情報機器などをケーブルや無線電波などで接続し、相互にデータ通信できるようにしたネットワークのことである。概ね室内あるいは建物内程度の広さで構築されるものを指す。今回の実験では、machine1,2,3 で構成されたネットワークがこれにあたる。

（文献 [3] を参考）

2.2.3 DMZ ネットワークについて

DMZ は「DeMilitarized Zone」を略したものであり、非武装地帯を意味する。企業・組織が内部ネットワークに存在する機密情報を守りつつ、インターネットなどの外部ネットワークへアクセスを行う際、使用される緩衝地帯のことである。ファイアウォールと外部ネットワーク間に設けられており、DMZ セグメントと正式に呼ばれる。

（文献 [4] を参考）

3 各実験

3.1 [課題 1] 初期環境の確認

3.1.1 目的・概要

ルーター (machine1),WWW サーバー (machine2),PC(machine3) を PC 切替器を介して接続し、ネットワークを構成した。本課題ではその machine1 と machine2 の初期環境の確認や設定を行い、それぞれの特性を掴んだり、今後の課題を行いやすくすることを目的としている。

3.1.2 実験方法

machine1,machine2 より、Linux のコマンドで確認や設定作業を行う。script コマンドで保存したログとともに実験結果を記す。

3.1.3 実験結果

1. Linux カーネルリリース番号の確認 (machine1)

```
[root@localhost ~]# uname -r  
3.10.0-862.el7.x86_64
```

これより、CentOS ver.7.5-1804 であることがわかる
(文献 [5] を参考。)

2. ファイルシステムの確認 (machine1)

(a) ファイルシステムのマウントポイントを記述した設定ファイル

```
[root@localhost ~]# cat /etc/fstab  
  
#  
# /etc/fstab  
# Created by anaconda on Fri Mar 22 12:04:29 2019  
#  
# Accessible filesystems, by reference, are maintained under '/dev/disk'  
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info  
#  
/dev/mapper/centos-root / xfs defaults 0 0  
UUID=aee50255-ddf9-4231-babe-4df05beb2989 /boot xfs defaults 0 0  
/dev/mapper/centos-home /home xfs defaults 0 0  
/dev/mapper/centos-swap swap swap defaults 0 0
```

(b) ディスクパーティションとマウントされているファイルシステムを確認

```
[root@localhost ~]# fdisk -l

Disk /dev/sda: 250.1 GB, 250059350016 bytes, 488397168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x00016021

      Device Boot      Start        End      Blocks   Id  System
/dev/sda1  *        2048    2099199     1048576   83  Linux
/dev/sda2          2099200  488396799    243148800   8e  Linux LVM

Disk /dev/mapper/centos-root: 53.7 GB, 53687091200 bytes, 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/centos-swap: 8321 MB, 8321499136 bytes, 16252928 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/centos-home: 187.0 GB, 186969489408 bytes, 365174784 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[root@localhost ~]# df
Filesystem           1K-blocks   Used Available Use% Mounted on
/dev/mapper/centos-root 52403200 1006784 51396416  2% /
devtmpfs              3936440     0 3936440  0% /dev
tmpfs                 3949112     0 3949112  0% /dev/shm
tmpfs                 3949112   8872 3940240  1% /run
tmpfs                 3949112     0 3949112  0% /sys/fs/cgroup
/dev/sda1              1038336 145900 892436 15% /boot
/dev/mapper/centos-home 182498240 32944 182465296  1% /home
tmpfs                  789824     0 789824  0% /run/user/0
```

これにて各種情報を得ることが出来た。

(c) 論理ボリュームの内容を確認

```
[root@localhost ~]# lvdisplay
--- Logical volume ---
LV Path          /dev/centos/swap
LV Name          swap
VG Name          centos
LV UUID          558Xtv-0Z7e-3krn-HqEs-8xHA-CYFl-BfapS4
LV Write Access  read/write
LV Creation host, time localhost, 2019-03-22 12:04:24 +0900
LV Status        available
# open           2
LV Size          7.75 GiB
Current LE       1984
Segments         1
Allocation       inherit
Read ahead sectors auto
- currently set to 256
Block device    253:1

--- Logical volume ---
LV Path          /dev/centos/home
LV Name          home
VG Name          centos
LV UUID          vanhId-NRrd-icZs-ugHk-PTLw-F5zJ-XgnuQb
LV Write Access  read/write
LV Creation host, time localhost, 2019-03-22 12:04:25 +0900
LV Status        available
# open           1
LV Size          <174.13 GiB
Current LE       44577
Segments         1
Allocation       inherit
Read ahead sectors auto
- currently set to 256
Block device    253:2

--- Logical volume ---
LV Path          /dev/centos/root
LV Name          root
VG Name          centos
LV UUID          zNAd06-xqs9-t9PR-iKrf-C855-jD6d-Lv017q
LV Write Access  read/write
LV Creation host, time localhost, 2019-03-22 12:04:26 +0900
LV Status        available
# open           1
LV Size          50.00 GiB
Current LE       12800
Segments         1
Allocation       inherit
Read ahead sectors auto
- currently set to 256
Block device    253:0
```

3. ホスト名の設定 (machine1)

- (a) hostname コマンドでホスト名を設定し、設定結果を確認

```
[root@localhost ~]# hostname icesc17.ice.nuie.nagoya-u.ac.jp
```

ホスト名を正しく設定できた。

- (b) ホスト名の恒久的変更のために、設定ファイル/etc/hostname の内容を vi エディタで変更

```
[root@localhost ~]# vi /etc/hostname  
127.0.0.1 icesc17.ice.nuie.nagoya-u.ac.jp localhost.localdomain localhost
```

上記のように変更した。再起動してもホスト名は変わらなかった。

4. SELinux の状態確認と無効化 (machine1)

- (a) 現在の設定状況の確認

```
[root@icesc17 ~]# cat /etc/sysconfig/selinux  
  
# This file controls the state of SELinux on the system.  
# SELINUX= can take one of these three values:  
#       enforcing - SELinux security policy is enforced.  
#       permissive - SELinux prints warnings instead of enforcing.  
#       disabled - No SELinux policy is loaded.  
SELINUX=enforcing  
# SELINUXTYPE= can take one of three two values:  
#       targeted - Targeted processes are protected,  
#       minimum - Modification of targeted policy. Only selected processes are protected.  
#       mls - Multi Level Security protection.  
SELINUXTYPE=targeted
```

```
[root@icesc17 ~]# getenforce  
Enforcing
```

確認できた。

- (b) SELinux の設定を permissive モードに変更

```
[root@icesc17 ~]# setenforce 0  
[root@icesc17 ~]#
```

vi エディタを用い、以下のテキストから

```
[root@icesc17 ~]# vi /etc/sysconfig/selinux
"/etc/sysconfig/selinux" 14L, This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=enforcing
# SELINUXTYPE= can take one of three two values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

以下のテキストに変更した。

```
[root@icesc17 ~]# vi /etc/sysconfig/selinux
"/etc/sysconfig/selinux" 14L, This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

1. Linux カーネルリリース番号の確認 (machine2)

```
[root@localhost ~]# uname -r
3.10.0-862.el7.x86_64
```

上記より、CentOS ver.7.5-1804 と確認できた。

(文献 [5] を参考。)

2. ファイルシステムの確認 (machine2)

(a) ファイルシステムのマウントポイントを記述した設定ファイル /etc/fstab の内容を確認

```
[root@localhost ~]# cat /etc/fstab
#
# /etc/fstab
# Created by anaconda on Sat Apr  6 00:42:18 2019
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
/dev/mapper/centos-root /          xfs    defaults        0 0
UUID=5eb200c5-354e-419c-9306-bdcc507c72c5 /boot      xfs    defaults        0 0
/dev/mapper/centos-home /home      xfs    defaults        0 0
/dev/mapper/centos-swap swap      swap   defaults        0 0
```

```
[root@localhost ~]# fdisk -l

Disk /dev/sda: 250.1 GB, 250059350016 bytes, 488397168 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disk label type: dos
Disk identifier: 0x0002caf3

      Device Boot   Start     End   Blocks Id System
/dev/sda1  *       2048 2099199 1048576  83 Linux
/dev/sda2        2099200 488396799 243148800  8e Linux LVM

Disk /dev/mapper/centos-root: 53.7 GB, 53687091200 bytes, 104857600 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/centos-swap: 8321 MB, 8321499136 bytes, 16252928 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

Disk /dev/mapper/centos-home: 187.0 GB, 186969489408 bytes, 365174784 sectors
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes

[root@localhost ~]# df

Filesystem      1K-blocks    Used Available Use% Mounted on
/dev/mapper/centos-root 52403200 1007064 51396136  2% /
devtmpfs          3913240      0 3913240  0% /dev
tmpfs            3925936      0 3925936  0% /dev/shm
tmpfs            3925936    9052 3916884  1% /run
tmpfs            3925936      0 3925936  0% /sys/fs/cgroup
/dev/sda1         1038336 146056 892280 15% /boot
/dev/mapper/centos-home 182498240 32944 182465296  1% /home
tmpfs            785188      0 785188  0% /run/user/0
```

確認できた。

(c) 論理ボリュームの内容を確認

```
[root@localhost ~]# lvdisplay
--- Logical volume ---
LV Path          /dev/centos/swap
LV Name          swap
VG Name          centos
LV UUID          PohTZH-fMlu-Lf0h-Mdhh-Z2xs-I2QH-ZM8ush
LV Write Access  read/write
LV Creation host, time localhost, 2019-04-06 00:42:14 +0900
LV Status        available
# open           2
LV Size          7.75 GiB
Current LE       1984
Segments         1
Allocation       inherit
Read ahead sectors auto
- currently set to 256
Block device    253:1

--- Logical volume ---
LV Path          /dev/centos/home
LV Name          home
VG Name          centos
LV UUID          XYwPiS-jXOD-IKEh-Jzzo-NDvs-qfED-uV8ABr
LV Write Access  read/write
LV Creation host, time localhost, 2019-04-06 00:42:14 +0900
LV Status        available
# open           1
LV Size          <174.13 GiB
Current LE       44577
Segments         1
Allocation       inherit
Read ahead sectors auto
- currently set to 256
Block device    253:2

--- Logical volume ---
LV Path          /dev/centos/root
LV Name          root
VG Name          centos
LV UUID          0z554A-DomL-0GcW-B3u7-yAir-UU6R-Fa3bE1
LV Write Access  read/write
LV Creation host, time localhost, 2019-04-06 00:42:16 +0900
LV Status        available
# open           1
LV Size          50.00 GiB
Current LE       12800
Segments         1
Allocation       inherit
Read ahead sectors auto
- currently set to 256
Block device    253:0
```

各種情報を確認できた。

3. ホスト名の設定 (machine2)

- (a) hostname コマンドでホスト名を設定し、設定結果を確認

```
[root@localhost ~]# hostname www7.ice.nuie.nagoya-u.ac.jp
```

結果を確認できた。

- (b) ホスト名の恒久的変更のために、設定ファイル /etc/hostname の内容を vi エディタで変更

```
[root@localhost ~]# vi /etc/hostname  
127.0.0.1 www7.ice.nuie.nagoya-u.ac.jp localhost.localdomain localhost
```

vi エディタで上記のように変更した。再起動してもホスト名は変更されたままである。

4. SELinux の状態確認と無効化 (machine2)

- (a) 現在の設定状況の確認

```
[root@www7 ~]# cat /etc/sysconfig/selinux  
  
# This file controls the state of SELinux on the system.  
# SELINUX= can take one of these three values:  
#       enforcing - SELinux security policy is enforced.  
#       permissive - SELinux prints warnings instead of enforcing.  
#       disabled - No SELinux policy is loaded.  
SELINUX=enforcing  
# SELINUXTYPE= can take one of three two values:  
#       targeted - Targeted processes are protected,  
#       minimum - Modification of targeted policy. Only selected processes are protected.  
#       mls - Multi Level Security protection.  
SELINUXTYPE=targeted
```

```
[root@www7 ~]# getenforce  
Enforcing
```

確認できた。

- (b) SELinux の設定を permissive モードに変更

```
[root@www7 ~]# setenforce 0
```

```
[root@www7 ~]# vi /etc/sysconfig/selinux

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#       enforcing - SELinux security policy is enforced.
#       permissive - SELinux prints warnings instead of enforcing.
#       disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#       targeted - Targeted processes are protected,
#       minimum - Modification of targeted policy. Only selected processes are protected.
#       mls - Multi Level Security protection.
SELINUXTYPE=targeted
```

machine1 でやったように、vi エディタで編集することで恒久的変更を施した。

3.1.4 考察

Linux 端末からの確認により、ルーターや WWW サーバーでも正常に Linux がインストールされ、ファイルシステムや論理ボリュームを確認することが出来た。また、ホスト名を恒久的に変更する過程で、今回の実験では

vi /etc/hostname コマンドから,
vi エディタを編集することでそれを実現したが、他にも
hostnamectl set-hostname ホスト名
nmcli general hostname ホスト名
というコマンドでも恒久的な変更が行えることが分かった。
一時的なホスト名の変更と今後使い分けていきたい所存である。
(参考文献 [6] を参考。)

3.2 [課題 2] ネットワーク設定

3.2.1 目的・概要

本課題では、ネットワークの接続を試みることで、今後の課題の一歩とする。さらに各種情報を確認し、ネットワークが接続しているかの是非を確認する。

3.2.2 実験方法

machine1, machine2 について nmcli コマンドを利用してネットワークインターフェイスの接続設定を行う。(IPv6 は利用しない)

3.2.3 実験結果

1. 現在の状況の確認 (machine1)
 - (a) ネットワークデバイスの確認

```
[root@icesc17 ~]# nmcli device status
DEVICE  TYPE      STATE      CONNECTION
enp1s0   ethernet  disconnected  --
enp2s0   ethernet  disconnected  --
enp3s0   ethernet  disconnected  --
enp4s0   ethernet  unavailable  --
lo      loopback  unmanaged    --

[root@icesc17 ~]# nmcli device show
GENERAL.DEVICE:                         enp1s0
GENERAL.TYPE:                            ethernet
GENERAL.HWADDR:                          00:E0:67:12:2D:D4
GENERAL.MTU:                             1500
GENERAL.STATE:                           30 (disconnected)
GENERAL.CONNECTION:                      --
GENERAL.CON-PATH:                        --
WIRED-PROPERTIES.CARRIER:                on

GENERAL.DEVICE:                         enp2s0
GENERAL.TYPE:                            ethernet
GENERAL.HWADDR:                          00:E0:67:12:2D:D5
GENERAL.MTU:                             1500
GENERAL.STATE:                           30 (disconnected)
GENERAL.CONNECTION:                      --
GENERAL.CON-PATH:                        --
WIRED-PROPERTIES.CARRIER:                on

GENERAL.DEVICE:                         enp3s0
GENERAL.TYPE:                            ethernet
GENERAL.HWADDR:                          00:E0:67:12:2D:D6
GENERAL.MTU:                             1500
GENERAL.STATE:                           30 (disconnected)
GENERAL.CONNECTION:                      --
GENERAL.CON-PATH:                        --
WIRED-PROPERTIES.CARRIER:                on
```

```

GENERAL.DEVICE:                      enp4s0
GENERAL.TYPE:                        ethernet
GENERAL.HWADDR:                     00:E0:67:12:2D:D7
GENERAL.MTU:                         1500
GENERAL.STATE:                       20 (unavailable)
GENERAL.CONNECTION:                  --
GENERAL.CON-PATH:                   --
WIRED-PROPERTIES.CARRIER:           off

GENERAL.DEVICE:                      lo
GENERAL.TYPE:                        loopback
GENERAL.HWADDR:                     00:00:00:00:00:00
GENERAL.MTU:                          65536
GENERAL.STATE:                       10 (unmanaged)
GENERAL.CONNECTION:                  --
GENERAL.CON-PATH:                   --
IP4.ADDRESS[1]:                     127.0.0.1/8
IP4.GATEWAY:                        --
IP6.ADDRESS[1]:                     ::1/128
IP6.GATEWAY:                        --

```

確認できた。

(b) ネットワーク接続の確認

```

[root@icesc17 ~]# nmcli connection show --active
NAME  UUID      TYPE   DEVICE

```

確認できた。

2. 接続設定 (machine1)
3. ネットワーク接続の有効化 (machine1) ログへ書き込みていなかったが、ネットワーク接続を有効化できた。
4. 各種情報の確認 (machine1)

```
[root@icesc17 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp1s0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:e0:67:12:2d:d4 brd ff:ff:ff:ff:ff:ff
        inet 192.168.100.17/32 brd 192.168.100.17 scope global noprefixroute enp1s0
            valid_lft forever preferred_lft forever
        inet6 fe80::1c6d:12ae:203a:ba0/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: enp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:e0:67:12:2d:d5 brd ff:ff:ff:ff:ff:ff
        inet 192.168.150.1/32 brd 192.168.150.1 scope global noprefixroute enp2s0
            valid_lft forever preferred_lft forever
        inet6 fe80::c646:46f4:ddc1:96aa/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
4: enp3s0: <NO-CARRIER,BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:e0:67:12:2d:d6 brd ff:ff:ff:ff:ff:ff
        inet 192.168.200.1/32 brd 192.168.200.1 scope global noprefixroute enp3s0
            valid_lft forever preferred_lft forever
        inet6 fe80::b464:85d2:7f31:8c47/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
5: enp4s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc pfifo_fast state DOWN group default qlen 1000
    link/ether 00:e0:67:12:2d:d7 brd ff:ff:ff:ff:ff:ff
```

```
[root@icesc17 ~]# ip addr show route
default via 192.168.100.1 dev enp1s0 proto static metric 103
192.168.100.1 dev enp1s0 proto static scope link metric 103
192.168.100.17 dev enp1s0 proto kernel scope link src 192.168.100.17 metric 103
192.168.150.1 dev enp2s0 proto kernel scope link src 192.168.150.1 metric 104
192.168.200.1 dev enp3s0 proto kernel scope link src 192.168.200.1 metric 105
```

[root@icesc17 ~]# ip neighbour
 [root@icesc17 ~]# ip neighbour
 192.168.200.100 dev enp3s0 lladdr 94:c6:91:a9:cf:5b STALE
 [root@icesc17 ~]#

```
[root@icesc17 ~]# 
[root@icesc17 ~]# 
[root@icesc17 ~]# 
[root@icesc17 ~]# l
-bash: l: command not found
[root@icesc17 ~]# ip neighbour
Object "neighbour" is unknown, try "ip help".
[root@icesc17 ~]# ip neigbour
Object "neigbour" is unknown, try "ip help".
[root@icesc17 ~]# ip neighbour
192.168.200.100 dev enp3s0 lladdr 94:c6:91:a9:cf:5b STALE
[root@icesc17 ~]# _
```

確認できた。

1. 現在の状況の確認 (machine2)

(a) ネットワークデバイスの確認

```
[root@www7 ~]# nmcli device status
DEVICE      TYPE      STATE      CONNECTION
enp3s0    ethernet  disconnected  --
lo        loopback  unmanaged   --
wlp2s0    wifi      unmanaged   --
```

```
[root@www7 ~]# nmcli d show
GENERAL.DEVICE:                         enp3s0
GENERAL.TYPE:                            ethernet
GENERAL.HWADDR:                          94:C6:91:A9:07:2C
GENERAL.MTU:                             1500
GENERAL.STATE:                           30 (disconnected)
GENERAL.CONNECTION:                      --
GENERAL.CON-PATH:                        --
WIRED-PROPERTIES.CARRIER:                on
□ [m
GENERAL.DEVICE:                         lo
GENERAL.TYPE:                            loopback
GENERAL.HWADDR:                          00:00:00:00:00:00
GENERAL.MTU:                             65536
GENERAL.STATE:                           10 (unmanaged)
GENERAL.CONNECTION:                      --
GENERAL.CON-PATH:                        --
IP4.ADDRESS[1]:                          127.0.0.1/8
IP4.GATEWAY:                            --
IP6.ADDRESS[1]:                          ::1/128
IP6.GATEWAY:                            --
□ [m
GENERAL.DEVICE:                         wlp2s0
GENERAL.TYPE:                            wifi
GENERAL.HWADDR:                          18:1D:EA:F7:7A:BA
GENERAL.MTU:                             1500
GENERAL.STATE:                           10 (unmanaged)
GENERAL.CONNECTION:                      --
GENERAL.CON-PATH:                        --
IP4.GATEWAY:                            --
IP6.GATEWAY:                            --
```

確認できた。

- (b) ネットワーク接続の確認

```
[root@www7 ~]# nmcli c show --active
NAME  UUID    TYPE   DEVICE
```

確認できた。

2. 接続設定 (machine2)

```
[root@www7 ~]# nmcli c m add type ethernet ifname enp3s0 con-name enp3s0
Warning: There is another connection with the name 'enp3s0'. Reference the connection by its uuid '3d4ebb8c-5ded-4772-9ca9-8b325f6e538a'
Connection 'enp3s0' (3d4ebb8c-5ded-4772-9ca9-8b325f6e538a) successfully added.
```

```
[root@www7 ~]# nmcli c m enp3s0 connection.autoconnect yes
```

適切に接続し、OS 起動時の自動接続を指定。

3. ネットワーク接続の有効化 (machine2)

```
[root@www7 ~]# nmcli c down enp3s0
Connection 'enp3s0' successfully deactivated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/58)
[root@www7 ~]# nmcli c up enp3s0
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/59)
```

有効化できた。

4. 各種情報の確認 (machine2)

```
[root@www7 ~]# ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
        inet 127.0.0.1/8 scope host lo
            valid_lft forever preferred_lft forever
        inet6 ::1/128 scope host
            valid_lft forever preferred_lft forever
2: enp3s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 94:c6:91:a9:07:2c brd ff:ff:ff:ff:ff:ff
        inet 192.168.150.2/24 brd 192.168.150.255 scope global noprefixroute dynamic enp3s0
            valid_lft 3552sec preferred_lft 3552sec
        inet6 fe80::cd87:d270:a12c:6e52/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
3: wlp2s0: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN group default qlen 1000
    link/ether 18:1d:ea:f7:7a:ba brd ff:ff:ff:ff:ff:ff
[root@www7 ~]# ip route
default via 192.168.150.1 dev enp3s0 proto dhcp metric 100
192.168.150.0/24 dev enp3s0 proto kernel scope link src 192.168.150.2 metric 100
[root@www7 ~]# ip neighbour
```

3. Run the command with the repository temporarily disabled
yum --disablerepo=<repoid> ...
 4. Disable the repository permanently, so yum won't use it b
will then just ignore the repository until you permanentl
again or use --enablerepo for temporary usage:
- yum-config-manager --disable <repoid>
or subscription-manager repos --disable=<repoid>
5. Configure the failing repository to be skipped, if it is
Note that yum will try to contact the repo. when it runs
so will have to try and fail each time (and thus, yum wi
slower). If it is a very temporary problem though, this
compromise:

```
yum-config-manager --save --setopt=<repoid>.skip_if  
cannot find a valid baseurl for repo: base/7/x86_64  
root@www7 ~]#  
root@www7 ~]# ip neighbour  
192.168.150.1 dev enp3s0 lladdr 00:e0:67:12:2d:d5 STALE  
[root@www7 ~]# -
```

各種情報を確認できた。

3.2.4 考察

machine2についてip neighbourコマンドを入力したとき、何も表示されなかった。接続もちゃんとされているはずだがなぜかと考えた結果、実験中にネットマスクが関係しているのではということをちらっと耳にし

たため、調べることにした。ネットマスクはサブネットマスクともいう。サブネットマスクは上位何ビットがネットワークアドレスかを表す値で、サブネット毎に規定されている。例えば、サブネットマスクが2進数で「11111111 11111111 11111111 00000000」ならば、上位24ビットがネットワークアドレス、下位8ビットがホストアドレスとなる。これをネットワークアドレスと共に「198.51.100.0/24」のように、あるいは単に「/24」のように表記することもある（CIDR表記）。

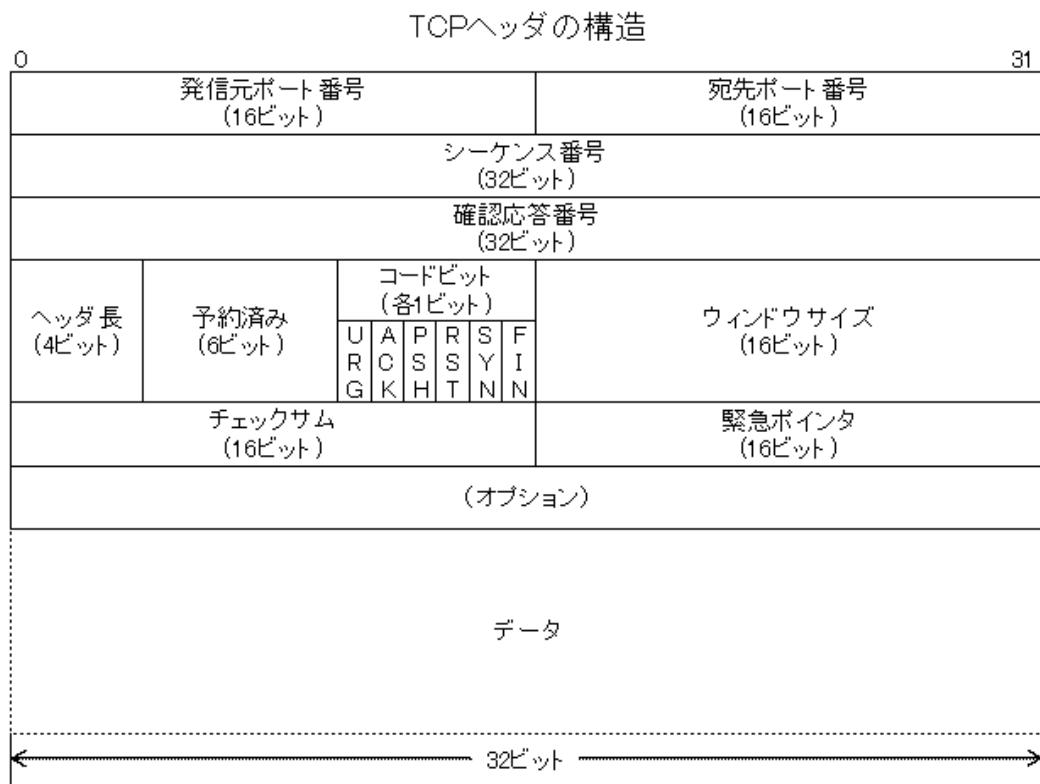
（文献[7]を参考。）

これだけの情報だと正直原因の究明には至らなかったが、IPアドレスに対して影響を与えていたのは確かであった。

3.2.5 調査課題

(1) TCPの構成は以下のようにになっている。

それぞれのフィールドの意味は以下の通りである。



- ・送信元ポート番号：16ビット送信元ノードのアプリケーションが使用しているポート番号がセットされる。
- ・宛先ポート番号：16ビット宛先アプリケーションが使用するポート番号がセットされる。
- ・シーケンス番号：32ビット送信するデータには、順序を付けるための「シーケンス番号」が付与される。このシーケンス番号で、この”データはデータ全体の中のどの位置のデータなのか”が分かるようになる。シーケンス番号は送信元ノードで管理され、データを送信するたびにデータ1バイトごとにシーケンス番号が加算されていく。
- ・確認応答番号：32ビットこのフィールドは、受信したデータに対してどの位置まで受信したか

を表すためのフィールドで、次に受信するデータのシーケンス番号は付与される。確認応答番号は受信側ノードが、送信元ノードへの応答パケットに付与して送信される。

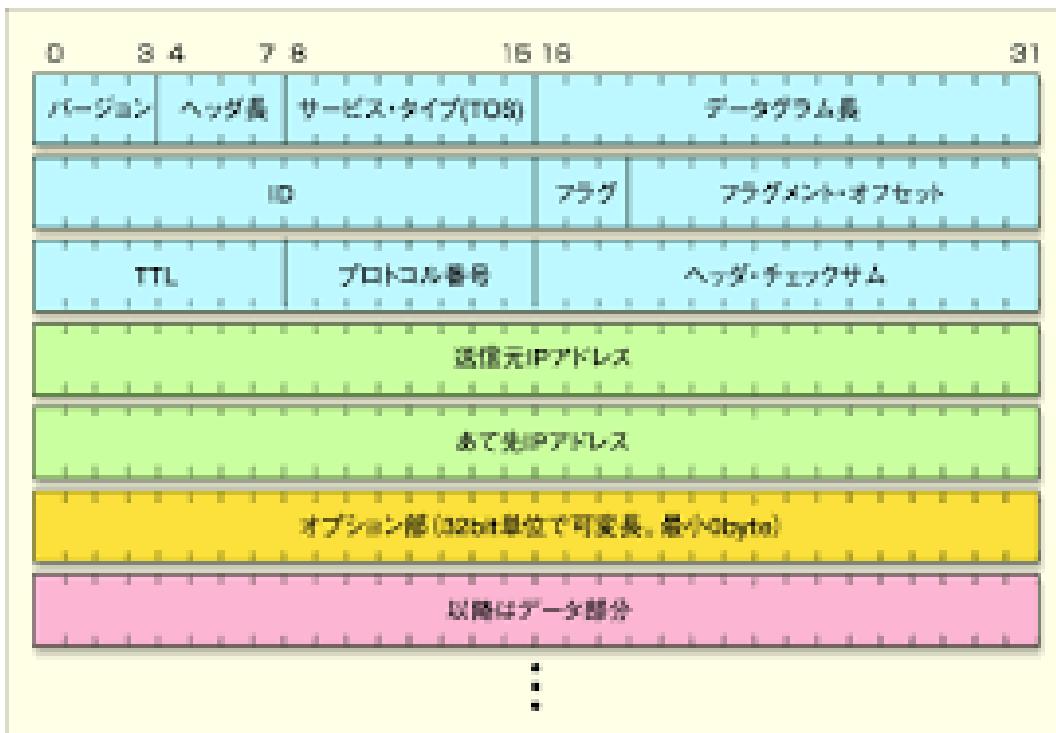
- ・データオフセット：4 ビット TCP データのヘッダ超が格納されるフィールドである。TCP ヘッダの長さはオプションがない場合、20 バイトとなるため、このフィールドには 5 (2 進数だと 0101) がセットされる。
- ・予約：6 ビットこのフィールドは将来の拡張のために用意されていて、通常はすべて「0」がセットされる。
- ・コードビット：6 ビットコードビットは 1 ビットずつに役割があり、フラグとして使用される。初期値はすべて「0」ですが、値が「1」の場合にそれぞれのフラグが有効となる。
- ・ウインドウサイズ：16 ビット受信側の受信可能なデータサイズを送信側に通知するために使用される。送信側では、このフィールドにセットされたウインドウサイズを見て、送信可能な最大データサイズを判断する。
- ・チェックサム：16 ビット UDP のチェックサムと同じで通信中にエラーが発生していないかどうかをチェックする数式がセットされる。
- ・緊急ポインタ：16 ビットコードビットフィールドの URG フラグが有効になっているときに使用するフィールドである。このフィールドには、緊急に処理しなければいけない、データの場所を示す値がセットされる。
- ・オプション TCP 通信で機能を付加する場合に使用されるフィールドである。

(文献 [4], 文献 [5] を参考。)

IP ヘッダについて

IP ヘッダの構成は以下のようになっている。

それぞれのフィールドの意味は以下の通りである。



○ Version (4 ビット)

IP のバージョンを表す。IPv4 であれば「4」が入りますし、IPv6 であれば「6」が入る。

○ IHL (4 ビット)

IHL (Internet Header Length : インターネットヘッダ長)。IP ヘッダーの長さを表しています。IHL でどこまでが IP ヘッダでどこからがデータなのかが分かります。

○ TOS (8 ビット)

TOS (Type of Service) ビットには、IP パケットの優先度などパケットの品質を決める情報が入ります。

○ Total Length (16 ビット)

IP ヘッダとデータを含めたパケット全体の長さを表します。

○ Identification (16 ビット)

大きなデータを運ぶときは、複数の IP パケットに分けてデータを送信します。その時に、分割したデータなのか、全く別のデータのパケットなのかを識別するために使用できます。

○ Flags (3 ビット)

IP パケットの分割を制御する時に使用します。各値の意味は以下の通りです。

ビット 0 : 予約 (未使用)	ビット 1 : 分割を許可するかしないかを表す値	値が 0 だと分割可
値が 1 だと分割不可	ビット 2 : フラグメントが最後かどうかを表す値	値が 0 だ
と最後のフラグメント	値が 1 だと後続のパケットが存在する	

○ Fragment Offset (13 ビット)

分割されたパケットが、元のデータのどこに位置しているかを表します。単位は 8 オクテットで最大 $8 \times 8192 = 65536$ オクテット。

○ TTL (8 ビット)

Time to Live (TTL)。パケットが通過可能なルータの数を表します。ルータを経由するたびに 1 づつ減っていき。0 になった時点でこのパケットは破棄されます。

○ Protocol (8 ビット)

IP の上位プロトコルを表します。主要なプロトコルは以下があります。

1 : ICMP (Internet Control Message Protocol) 6 : TCP (Transmission Control Protocol) 17 : UDP (User Datagram Protocol)

○ Header Checksum (16 ビット)

IP ヘッダのチェックサム。IP パケットの传送エラーがないかチェックするためにあります。IP ヘッダ内の TTL 値はルータを経由するたびに変わるために、各ルータでは転送する前にヘッダチェックサムの再計算を行っています。

○ Source Address (32 ビット)

宛先の IP アドレスがセットされています。

○ Options (可変)

IP パケットに付加するオプションを設定しています。

○ Padding (可変)

オプションを使用した場合、長さを 32 ビットにするために使用されます。(文献 [6] から引用)]

- (2) ブロードキャストは同報通信とも訳され、ネットワーク上の複数のコンピュータに対して、一斉にデータを送信する役割を担う。また、ブロードキャストアドレスは IP アドレス全てが “1” の IP アドレス、つまり、255.255.255.255のことである。正式には「リミテッド・ブロードキャストアドレス」といわれる。

リミテッド・ブロードキャストアドレスは同一ネットワーク上のすべてのホストに対して通信を行う場合に宛先アドレスとして使用される。ただし、コンピュータなどのホストに対して設定することは出来ない。ルータを越えることは出来ない、1 つのネットワーク内でのみ完結する通信である。

(文献 [10] を参考。)

- (3) 正直何を言っているかよくわかりません。

3.3 [課題 3] DHCP サービスの設定

3.3.1 目的・概要

DHCP サーバを起動させること

3.3.2 実験方法

machine1 から設定を行い、サービス起動後に machine2,machine3 で確認作業を行う。

3.3.3 実験結果

1. nano エディタのインストール必要ないと判断し、見送った。また、nano エディタは GNU プロジェクトの 1 つであり、GUI なしのターミナル環境で使える軽量エディタであり、特徴としては「ファイルの保存」や「エディタの終了」などに際して、コマンドを入力する必要がなく、常時表示されているメニューから選ぶだけでそれらを行うことが出来るため、初心者にも優しいことが挙げられる。

(文献 [3] を参考。)

2.稼働中のサービスの確認

```
[root@icesc17 ~]# systemctl list-units --type=service
UNIT                                     LOAD ACTIVE SUB   DESCRIPTION
auditd.service                           loaded active running Security Auditing Service
crond.service                            loaded active running Command Scheduler
dbus.service                             loaded active running D-Bus System Message Bus
firewalld.service                        loaded active running firewalld - dynamic firewall daemon
getty@tty1.service                       loaded active running Getty on tty1
irqbalance.service                      loaded active running irqbalance daemon
kdump.service                            loaded active exited Crash recovery kernel arming
kmod-static-nodes.service                loaded active exited Create list of required static device nodes for the current kernel
lvm2-lvmetad.service                    loaded active running LVM2 metadata daemon
lvm2-monitor.service                    loaded active exited Monitoring of LVM2 mirrors, snapshots etc. using dmeventd or progress polling
lvm2-pvscan@8:2.service                loaded active exited LVM2 PV scan on device 8:2
network.service                          loaded active exited LSB: Bring up/down networking
NetworkManager-wait-online.service     loaded active exited Network Manager Wait Online
NetworkManager.service                  loaded active running Network Manager
polkit.service                           loaded active running Authorization Manager
postfix.service                          loaded active running Postfix Mail Transport Agent
rhel-dmsg.service                       loaded active exited Dump dmsg to /var/log/dmsg
rhel-domainname.service                 loaded active exited Read and set NIS domainname from /etc/sysconfig/network
rhel-import-state.service               loaded active exited Import network configuration from initramfs
rhe-readyonly.service                  loaded active exited Configure read-only root support
rsyslog.service                         loaded active running System Logging Service
sshd.service                            loaded active running OpenSSH server daemon
systemd-backlight@backlight:acpi_video0.service loaded active exited Load/Save Screen Backlight Brightness of backlight:acpi_video0
systemd-journal-flush.service          loaded active exited Flush Journal to Persistent Storage
systemd-journal.service               loaded active running Journal Service
systemd-logind.service                loaded active running Login Service
systemd-random-seed.service           loaded active exited Load/Save Random Seed
systemd-readahead-collect.service     loaded active exited Collect Read-Ahead Data
systemd-readahead-delay.service       loaded active exited Replay Read-Ahead Data
systemd-remount-fs.service             loaded active exited Remount Root and Kernel File Systems
systemd-sysctl.service                loaded active exited Apply Kernel Variables
systemd-tmpfiles-setup-dev.service    loaded active exited Create Static Device Nodes in /dev
systemd-tmpfiles-setup.service        loaded active exited Create Volatile Files and Directories
systemd-udev-trigger.service         loaded active exited udev Coldplug all Devices
systemd-udevd.service                loaded active running udev Kernel Device Manager

systemd-update-utmp.service           loaded active exited Update UTMP about System Boot/Shutdown
systemd-user-sessions.service        loaded active exited Permit User Sessions
systemd-vconsole-setup.service       loaded active exited Setup Virtual Console
tuned.service                           loaded active running Dynamic System Tuning Daemon

LOAD  = Reflects whether the unit definition was properly loaded.
ACTIVE = The high-level unit activation state, i.e. generalization of SUB.
SUB   = The low-level unit activation state, values depend on unit type.

39 loaded units listed. Pass --all to see loaded but inactive units, too.
To show all installed unit files use 'systemctl list-unit-files'.
```

以上のように確認できた。

3. firewall の停止

```
[root@icesc17 ~]# systemctl stop firewalld
[root@icesc17 ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
  Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
  Active: inactive (dead) since Thu 2019-04-11 17:16:07 JST; 21s ago
    Docs: man:firewalld(1)
   Process: 700 ExecStart=/usr/sbin/firewalld --nofork --nopid $FIREWALLD_ARGS (code=exited, status=0/SUCCESS)
  Main PID: 700 (code=exited, status=0/SUCCESS)

Apr 11 17:16:05 icesc17.ice.nuie.nagoya-u.ac.jp systemd[1]: Stopping firewalld - dynamic firewall daemon...
Apr 11 17:16:07 icesc17.ice.nuie.nagoya-u.ac.jp systemd[1]: Stopped firewalld - dynamic firewall daemon.
Warning: Journal has been rotated since unit was started. Log output is incomplete or unavailable.
```

以上のように停止できた。

4. DHCP サーバのインストールと設定

(a) DHCP サーバのインストールと設定

```
[root@icesc17 ~]# yum list dhcp.*  
Loaded plugins: fastestmirror  
Determining fastest mirror...  
* base: mirrors.cat.net  
* extras: mirrors.cat.net  
* updates: mirrors.cat.net  
base  
extras  
updates  
(1/4): base/7/x86_64/group_db 3.6 kB 00:00:00  
(2/4): extras/7/x86_64-primary_db 3.4 kB 00:00:00  
(3/4): updates/7/x86_64-primary_db 3.4 kB 00:00:00  
(4/4): updates/7/x86_64-primary_db 166 kB 00:00:00  
[ 0.0 B/s | 2.8 MB --::-- ETA (4/4): updates/7/x86_64-primary_db  
| 187 kB 00:00:00  
| 3.4 kB 00:00:01  
Installed Packages  
dhcp-common.x86_64 12:4.2.5-68.el7.centos @anaconda  
dhcp-libs.x86_64 12:4.2.5-68.el7.centos @anaconda  
Available Packages  
dhcp.x86_64 12:4.2.5-68.el7.centos.1 base  
dhcp-common.x86_64 12:4.2.5-68.el7.centos.1 base  
dhcp-devel.i686 12:4.2.5-68.el7.centos.1 base  
dhcp-devel.x86_64 12:4.2.5-68.el7.centos.1 base  
dhcp-libs.i686 12:4.2.5-68.el7.centos.1 base  
dhcp-libs.x86_64 12:4.2.5-68.el7.centos.1 base  
  
[root@icesc17 ~]# yum info dhcp  
Loaded plugins: fastestmirror  
Loading mirror speeds from cached hostfile  
* base: mirrors.cat.net  
* extras: mirrors.cat.net  
* updates: mirrors.cat.net  
Available Packages  
Name : dhcp  
Arch : x86_64  
Epoch : 12  
Version : 4.2.5  
Release : 68.el7.centos.1  
Size : 513 k  
Repo : base/7/x86_64  
Summary : Dynamic host configuration protocol software  
URL : http://isc.org/products/DHCP/  
License : ISC  
Description : DHCP (Dynamic Host Configuration Protocol) is a protocol which allows individual devices on an IP network to get their own network configuration information (IP address, subnetmask, broadcast address, etc.) from a DHCP server. The overall purpose of DHCP is to make it easier to administer a large network.  
:  
: To use DHCP on your network, install a DHCP service (or relay agent), and on clients run a DHCP client daemon. The dhcp package provides the ISC DHCP service and relay agent.
```

```
[root@icesc17 ~]# yum install dhcp
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.cat.net
 * extras: mirrors.cat.net
 * updates: mirrors.cat.net
Resolving Dependencies
--> Running transaction check
--> Package dhcp.x86_64 12:4.2.5-68.el7.centos.1 will be installed
--> Processing Dependency: dhcp-libs(x86-64) = 12:4.2.5-68.el7.centos.1 for package: 12:dhcp-4.2.5-68.el7.centos.1.x86_64
--> Processing Dependency: dhcp-common = 12:4.2.5-68.el7.centos.1 for package: 12:dhcp-4.2.5-68.el7.centos.1.x86_64
--> Running transaction check
--> Package dhcp-common.x86_64 12:4.2.5-68.el7.centos will be updated
--> Processing Dependency: dhcp-common = 12:4.2.5-68.el7.centos for package: 12:dhclient-4.2.5-68.el7.centos.x86_64
--> Package dhcp-common.x86_64 12:4.2.5-68.el7.centos.1 will be an update
--> Package dhcp-libs.x86_64 12:4.2.5-68.el7.centos will be updated
--> Package dhcp-libs.x86_64 12:4.2.5-68.el7.centos.1 will be an update
--> Running transaction check
--> Package dhclient.x86_64 12:4.2.5-68.el7.centos will be updated
--> Package dhclient.x86_64 12:4.2.5-68.el7.centos.1 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package           Arch      Version            Repository  Size
=====
Installing:
dhcp           x86_64   12:4.2.5-68.el7.centos.1    base       513 k
Updating for dependencies:
dhclient        x86_64   12:4.2.5-68.el7.centos.1    base       284 k
dhcp-common    x86_64   12:4.2.5-68.el7.centos.1    base       175 k
dhcp-libs       x86_64   12:4.2.5-68.el7.centos.1    base       131 k

Transaction Summary
=====
Install 1 Package
Upgrade ( 3 Dependent packages)
```

手順通りインストールと設定を行えた。

(b) 設定ファイルの修正

ファイルを編集して、以下のように訂正した。

```
Welcome Guide dhcpd.conf

default-lease-time 3600;
max-lease-time 86400;
option domain-name-servers 10.10.1.2;
option subnet-mask 255.255.255.0;

subnet 192.168.150.0 netmask 255.255.255.0 {
    option routers 192.168.150.1;
    range 192.168.150.100 192.168.150.250;
    host ns {
        max-lease-time 2592000;
        hardware ethernet 94:C6:91:A9:07:2C;
        fixed-address 192.168.150.2;
    }
}

subnet 192.168.200.0 netmask 255.255.255.0 {
    option routers 192.168.200.1;
    range 192.168.200.100 192.168.200.250;
}
```

(c) DHCP サーバを起動し、クライアント機で動作確認

動作を確認できた。

(d) DHCP サーバのブート時自動起動を指定

```

Cleanup   : 12:dhclient-4.2.5-68.el7.centos.x86_64          5/7
Cleanup   : 12:dhcp-common-4.2.5-68.el7.centos.x86_64       6/7
Cleanup   : 12:dhcp-libs-4.2.5-68.el7.centos.x86_64         7/7
Verifying : 12:dhclient-4.2.5-68.el7.centos.1.x86_64        1/7
Verifying : 12:dhcp-common-4.2.5-68.el7.centos.1.x86_64      2/7
Verifying : 12:dhclient-4.2.5-68.el7.centos.1.x86_64        3/7
Verifying : 12:dhcp-libs-4.2.5-68.el7.centos.1.x86_64        4/7
Verifying : 12:dhclient-4.2.5-68.el7.centos.x86_64          5/7
Verifying : 12:dhcp-libs-4.2.5-68.el7.centos.x86_64          6/7
Verifying : 12:dhcp-libs-4.2.5-68.el7.centos.x86_64          7/7

Installed:
  dhcp.x86_64 12:4.2.5-68.el7.centos.1

Dependency Updated:
  dhclient.x86_64 12:4.2.5-68.el7.centos.1           dhcp-common.x86_64 12:4.2.5-68.el7.centos.1           dhcp-libs.x86_64 12:4.2.5-68.el7.centos.1

Complete!

```

自動起動を設定し、確認できた。

- (e) 結果提出 ICE のアカウントより、/pub1/jikken/cs-net/students/group7b のディレクトリに提出了した。

3.3.4 考察

ここではこの章で特に苦しめられた script コマンドで作成したログの文字化けについて考察したいと考える。調べてみると、いくつかの対処法が見つかった。1 つ目> col -bx | 変換前.log & 変換後.log

col コマンドは、改行コードなどのエスケープシーケンスを変換・削除するコマンド。b オプションは、バックスペースの出力を行わない x オプションは、タブの代わりに複数の半角スペースを出力(文献 [11] を参考)これでは文字化けが最大限に解消されなかった。

2 つ目 script コマンドで記録したログを less の-r や-R オプションで開く-r または -raw-control-chars 「そのままの」制御文字を表示させるようにする。デフォルトでは、制御文字をキャレット表記を使って表示する。例えば、control-A (8 進数 001) は ”^A” と表示される。警告: -r オプションが指定されると、less は(制御文字のタイプにどのように画面が反応するかに依存しているために)画面の実際の状況の経過を追うことができない。よって多くの場合、長い行が誤った位置で分割されてしまうといった問題が生じる。-R または -RAW-CONTROL-CHARS -r と似ているが、可能な場合には画面表示を正しく維持しようとする。このオプションが有効なのは、入力が通常のテキストの場合である。入力には ANSI の「カラー」エスケープシーケンスが含まれていてもよい。このシーケンスは ESC [...] m のような形式で、”...” は ”m” 以外の 0 個以上の文字である。画面の状況を保つため、全ての制御文字と ANSI カラーシーケンスは カーソルを移動させないと仮定している。less に ”m” 以外の文字を ANSI カラーエスケープシーケンスの終了文字として認識させることもできる。そのためには、認識させたい終了文字のリストを 環境変数 LESSANSIENDCHARS に設定すればよい。(文献 [12]) この方法で試してみたところなんとか上手くいった。

Linux が生んだ文字化けの対策を Linux でできるとはさすがオープンソースなソフトウェアといったところだ。

3.4 [課題 4] ファイアウォールの設定

3.4.1 目的・概要

ネットワークのセキュリティのために、ファイアウォールの設定を行い、外部からの不正アクセスを防ぐ。

3.4.2 実験方法

machine1,2 でファイアウォール設定を行い、設定後は内部・外部端末から仕様の確認を行う。

3.4.3 実験結果

1. machine1 のファイアウォール設定

- (a) パケット転送の有効化以下の様に設定ファイルを作成し、編集した。

```
[root@icesc17 ~]# vi /etc/sysctl.d/10-ipv4.conf
net.ipv4.ip_forward = 1
```

そして以下のコマンドを用い、再起動して有効化できた。

```
[root@icesc17 ~]# sysctl --sysctl
* Applying /usr/lib/sysctl.d/00-system.conf ...
* Applying /usr/lib/sysctl.d/10-default-yama-scope.conf ...
kernel.yama.ptrace_scope = 0
* Applying /etc/sysctl.d/10-ipv4.conf ...
net.ipv4.ip_forward = 1
* Applying /usr/lib/sysctl.d/50-default.conf ...
kernel.sysrq = 16
kernel.core_uses_pid = 1
net.ipv4.conf.default.rp_filter = 1
net.ipv4.conf.all.rp_filter = 1
net.ipv4.conf.default.accept_source_route = 0
net.ipv4.conf.all.accept_source_route = 0
net.ipv4.conf.default.promote_secondaries = 1
net.ipv4.conf.all.promote_secondaries = 1
fs.protected_hardlinks = 1
fs.protected_symlinks = 1
* Applying /etc/sysctl.d/99-sysctl.conf ...
* Applying /etc/sysctl.conf ...
[root@icesc17 ~]# reboot
```

- (b) firewalld から iptables-services への変更


```
[root@icesc17 ~]# systemctl status iptables
Created symlink from /etc/systemd/system/basic.target.wants/iptables.service to /usr/lib/systemd/system/iptables.service.
```

手順通りに行うことが出来た。

(c) サンプルの実行

```
[root@icesc17 ~]# scp uk6057965@ssh.ice.nuie.nagoya-u.ac.jp:/pub1/jikken/cs-net/iptables-sample.sh ~
The authenticity of host 'ssh.ice.nuie.nagoya-u.ac.jp (10.11.1.12)' can't be established.
RSA key fingerprint is SHA256:+TozKde2CBNkFKMvOG26EQtYfSz1kT3i4uIx2hIxSY.
RSA key fingerprint is MD5:71:49:d0:01:1b:11:5c:2e:06:81:3d:92:65:01:3fa3.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'ssh.ice.nuie.nagoya-u.ac.jp,10.11.1.12' (RSA) to the list of known hosts.
uk6057965@ssh.ice.nuie.nagoya-u.ac.jp's password:
iptables-sample.sh
```

```
[root@icesc17 ~]# sh iptables-sample.sh
```

実行できた。

(d) iptables の設定状況を確認

```
[root@icesc17 ~]# iptables -L -n
Chain INPUT (policy DROP)
target     prot opt source          destination
ACCEPT    all  --  0.0.0.0/0        0.0.0.0/0
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0          state NEW tcp dpt:22
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0          state NEW tcp dpt:22
ACCEPT    udp  --  0.0.0.0/0        0.0.0.0/0          state NEW udp dpt:67
ACCEPT    icmp --  0.0.0.0/0        0.0.0.0/0
ACCEPT    udp  --  0.0.0.0/0        0.0.0.0/0          state NEW udp dpt:67
ACCEPT    icmp --  0.0.0.0/0        0.0.0.0/0
ACCEPT    all  --  0.0.0.0/0        0.0.0.0/0          state RELATED,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source          destination
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0          state NEW,ESTABLISHED tcp dpt:22
ACCEPT    icmp --  0.0.0.0/0        0.0.0.0/0
ACCEPT    all  --  0.0.0.0/0        0.0.0.0/0          state RELATED,ESTABLISHED

Chain OUTPUT (policy DROP)
target     prot opt source          destination
ACCEPT    all  --  0.0.0.0/0        0.0.0.0/0
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0          state NEW tcp dpt:22
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0          state NEW tcp dpt:80
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0          state NEW tcp dpt:443
ACCEPT    udp  --  0.0.0.0/0        0.0.0.0/0          state NEW udp dpt:53
ACCEPT    icmp --  0.0.0.0/0        0.0.0.0/0
ACCEPT    icmp --  0.0.0.0/0        0.0.0.0/0
ACCEPT    tcp  --  0.0.0.0/0        0.0.0.0/0          state NEW tcp dpt:22
ACCEPT    all  --  0.0.0.0/0        0.0.0.0/0          state RELATED,ESTABLISHED
```

確認し、現在のルールを表示した。

(e) 設定スクリプトの修正

```
[root@icesc17 ~]# iptables-save
# Generated by iptables-save v1.4.21 on Thu Apr 18 14:14:07 2019
*nat
:PREROUTING ACCEPT [0:0]
:INPUT ACCEPT [0:0]
:OUTPUT ACCEPT [0:0]
:POSTROUTING ACCEPT [0:0]
-A POSTROUTING -s 192.168.200.0/24 -o enp1s0 -j SNAT --to-source 192.168.100.17
COMMIT
# Completed on Thu Apr 18 14:14:07 2019
# Generated by iptables-save v1.4.21 on Thu Apr 18 14:14:07 2019
*filter
:INPUT DROP [0:0]
:FORWARD DROP [0:0]
:OUTPUT DROP [0:0]
-A INPUT -i lo -j ACCEPT
-A INPUT -i enp1s0 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -i enp3s0 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A INPUT -i enp3s0 -p udp -m state --state NEW -m udp --dport 67 -j ACCEPT
-A INPUT -i enp3s0 -p icmp -j ACCEPT
-A INPUT -i enp2s0 -p udp -m state --state NEW -m udp --dport 67 -j ACCEPT
-A INPUT -i enp2s0 -p icmp -j ACCEPT
-A INPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
-A FORWARD -i enp3s0 -o enp1s0 -p tcp -m state --state NEW,ESTABLISHED -m tcp --dport 22 -j ACCEPT
-A FORWARD -i enp3s0 -o enp1s0 -p icmp -j ACCEPT
-A FORWARD -i enp1s0 -o enp3s0 -m state --state RELATED,ESTABLISHED -j ACCEPT
-A OUTPUT -o lo -j ACCEPT
-A OUTPUT -o enp1s0 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A OUTPUT -o enp1s0 -p tcp -m state --state NEW -m tcp --dport 80 -j ACCEPT
-A OUTPUT -o enp1s0 -p tcp -m state --state NEW -m tcp --dport 443 -j ACCEPT
-A OUTPUT -o enp1s0 -p udp -m state --state NEW -m udp --dport 53 -j ACCEPT
-A OUTPUT -o enp1s0 -p icmp -j ACCEPT
-A OUTPUT -o enp3s0 -p icmp -j ACCEPT
-A OUTPUT -o enp2s0 -p tcp -m state --state NEW -m tcp --dport 22 -j ACCEPT
-A OUTPUT -m state --state RELATED,ESTABLISHED -j ACCEPT
COMMIT
# Completed on Thu Apr 18 14:14:07 2019
```

(f) 確認用ソフトウェアのインストール

```
[root@icesc17 ~]# yum info lynx
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.cat.net
 * extras: mirrors.cat.net
 * updates: mirrors.cat.net
Available Packages
Name        : lynx
Arch       : x86_64
Version    : 2.8.8
Release   : 0.3.dev15.el7
Size       : 1.4 M
Repo      : base/7/x86_64
Summary   : A text-based Web browser
URL       : http://lynx.isc.org/
License    : GPLv2
Description: Lynx is a text-based Web browser. Lynx does not display any images,
            : but it does support frames, tables, and most other HTML tags. One
            : advantage Lynx has over graphical browsers is speed; Lynx starts and
            : exits quickly and swiftly displays web pages.
```



```
[root@icesc17 ~]# yum info bind-utils
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: mirrors.cat.net
* extras: mirrors.cat.net
* updates: mirrors.cat.net
Available Packages
Name        : bind-utils
Arch       : x86_64
Epoch      : 32
Version    : 9.9.4
Release    : 73.el7_6
Size       : 206 k
Repo       : updates/7/x86_64
Summary    : Utilities for querying DNS name servers
URL        : http://www.isc.org/products/BIND/
License    : ISC
Description: Bind-utils contains a collection of utilities for querying DNS (Domain
             : Name System) name servers to find out information about Internet
             : hosts. These tools will provide you with the IP addresses for given
             : host names, as well as other information about registered domains and
             : network addresses.
:
             : You should install bind-utils if you need to get information from DNS name
             : servers.

[root@icesc17 ~]# yum install bind-utils
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: mirrors.cat.net
* extras: mirrors.cat.net
* updates: mirrors.cat.net
Resolving Dependencies
--> Running transaction check
--> Package bind-utils.x86_64 32:9.9.4-73.el7_6 will be installed
--> Processing Dependency: bind-libs = 32:9.9.4-73.el7_6 for package: 32:bind-utils-9.9.4-73.el7_6.x86_64
--> Processing Dependency: liblwres.so.90()(64bit) for package: 32:bind-utils-9.9.4-73.el7_6.x86_64
--> Processing Dependency: libiscfg.so.90()(64bit) for package: 32:bind-utils-9.9.4-73.el7_6.x86_64
--> Processing Dependency: libisccfg.so.90()(64bit) for package: 32:bind-utils-9.9.4-73.el7_6.x86_64
--> Processing Dependency: libisc.so.95()(64bit) for package: 32:bind-utils-9.9.4-73.el7_6.x86_64
--> Processing Dependency: libdns.so.100()(64bit) for package: 32:bind-utils-9.9.4-73.el7_6.x86_64
--> Processing Dependency: libbind9.so.90()(64bit) for package: 32:bind-utils-9.9.4-73.el7_6.x86_64
--> Running transaction check
--> Package bind-libs.x86_64 32:9.9.4-73.el7_6 will be installed
--> Processing Dependency: bind-license = 32:9.9.4-73.el7_6 for package: 32:bind-libs-9.9.4-73.el7_6.x86_64
--> Running transaction check
--> Package bind-license.noarch 32:9.9.4-61.el7 will be updated
--> Processing Dependency: bind-license = 32:9.9.4-61.el7 for package: 32:bind-libs-lite-9.9.4-61.el7.x86_64
--> Package bind-license.noarch 32:9.9.4-73.el7_6 will be an update
--> Running transaction check
--> Package bind-libs-lite.x86_64 32:9.9.4-61.el7 will be updated
--> Package bind-libs-lite.x86_64 32:9.9.4-73.el7_6 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package          Arch      Version           Repository      Size
=====
Installing:
bind-utils      x86_64   32:9.9.4-73.el7_6      updates         296 k
Installing for dependencies:
bind-libs        x86_64   32:9.9.4-73.el7_6      updates         1.0 M
Updating for dependencies:
bind-libs-lite   x86_64   32:9.9.4-73.el7_6      updates         741 k
bind-license     noarch   32:9.9.4-73.el7_6      updates         87 k

Transaction Summary
=====
Install 1 Package (+1 Dependent package)
Upgrade  ( 2 Dependent packages)
```

正しくインストールできた

(g) ファイアウォールの動作状況の最終確認

```
[root@ccs17 ~]# lynx https://www.google.co.jp
Getting https://www.google.co.jp Looking up www.google.co.jp Making HTTPS connection to www.google.co.jp[subj=*google.co.jp]
Certificate issued by :[C=US]O=Google Trust Services/[CN=Google Internet Authority G3][0;10m][39;40m][31m][40m][0;10m][33m][44m]Secure 128-bit TLSv1/SSLv3
(ECDSA-ECDSS-AES128-GCM-SHA256) HTTP connection mding HTTP request. HTTP request sent; waiting for response from www.google.co.jp cookie: JAR=2019-04-18-06 Allow? (Y/N/Always/never)
Allowing this cookie:www.google.co.jp cookie: N=181g-c57x1giUk0H7nrlRgflV7vs06xwvSeFgjyC=0d0hYzHze6brh0X3V9PKU67l2JutR1D2h3xbs0Dvh0nzi2lQ3yRRe Allow? (Y/N/Always/never) Allowing this cookie.
Read 637 bytes of data, 34 bytes/sec. Data transfer complete Google 検索 画像 マップ Play YouTube ニュース 40mGmail ドライブ もっと見る
ヨリ 帰る 編集 改定 ログイン
Google
```

```

[root@icesc17 ~]# lynx http://www.mlit.go.jp
Getting http://www.mlit.go.jp Making HTTP connection to www.mlit.go.jp Sending HTTP request. HTTP request sent; waiting for response. 国土交通省 (p1 of 2) 災害・防災情報
報道・広報
動画チャンネル

□[33m□[40mトピックス

RSS
■ 言語

トピックス 國土交通省の活動

【4月15日】 石井大臣の中韓訪問
【4月15日】 石井大臣の中韓訪問
【4月15日】 バハマ共和国キハーノ運河府長官による阿達政務官へ...
【4月15日】 バハマ共和国キハーノ運河府長官による阿達政務官へ...
【4月12日】 中華人民共和国 程永華 駐日大使による石井大臣へ...
【4月12日】 中華人民共和国 程永華 駐日大使による石井大臣へ...
【4月4日】 I C A O (国際民間航空機関) リウ・ファン事務局長に...
【4月4日】 I C A O (国際民間航空機関) リウ・ファン事務局長に...
【4月1日】 敦賀/博多 新規航路開設歡迎式に阿達政務官が出席
敦賀/博多 新規航路開設歡迎式に阿達政務官が出席
一覧へ
【4月15日】 石井大臣の中韓訪問
【4月15日】 バハマ共和国キハーノ運河府長官による阿達政務官への表敬訪問
【4月12日】 中華人民共和国 程永華 駐日大使による石井大臣の表敬訪問
【4月4日】 I C A O (国際民間航空機関) リウ・ファン事務局長による阿達政務官への表敬訪問
【4月1日】 敦賀/博多 新規航路開設歡迎式に阿達政務官が出席
(3月31日) 「米姉自動車道 大阪IC」開通式典に阿達政務官が出席

新着情報

消費税率10%への引上げ後の住宅取得にメリットが出る支援策を用意!地図で確認、先人が伝える災害の教訓【国土地理院】
; <>> DIG 9.9.4-RedHat-9.9.4-73.el7_6 <>> google.co.jp
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 13356
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 9

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;google.co.jp. IN A

;; ANSWER SECTION:
google.co.jp. 300 IN A 172.217.161.195

;; AUTHORITY SECTION:
google.co.jp. 82177 IN NS ns2.google.com.
google.co.jp. 82177 IN NS ns3.google.com.
google.co.jp. 82177 IN NS ns4.google.com.
google.co.jp. 82177 IN NS ns1.google.com.

;; ADDITIONAL SECTION:
ns2.google.com. 147509 IN A 216.239.34.10
ns2.google.com. 80858 IN AAAA 2001:4860:4802:34::a
ns3.google.com. 147509 IN A 216.239.36.10
ns3.google.com. 80858 IN AAAA 2001:4860:4802:36::a
ns4.google.com. 147509 IN A 216.239.38.10
ns4.google.com. 80858 IN AAAA 2001:4860:4802:38::a
ns1.google.com. 147509 IN A 216.239.32.10
ns1.google.com. 80858 IN AAAA 2001:4860:4802:32::a

;; Query time: 38 msec
;; SERVER: 10.10.1.2#53(10.10.1.2)
;; WHEN: Thu Apr 18 15:53:34 JST 2019
;; MSG SIZE rcvd: 315

```

```
[root@icesc17 ~]# ping yahoo.com
PING yahoo.com (98.137.246.7) 56(84) bytes of data.
64 bytes from media-router-fp1.prod1.media.vip.gql.yahoo.com (98.137.246.7): icmp_seq=1 ttl=46 time=98.6 ms
64 bytes from media-router-fp1.prod1.media.vip.gql.yahoo.com (98.137.246.7): icmp_seq=2 ttl=46 time=98.1 ms
64 bytes from media-router-fp1.prod1.media.vip.gql.yahoo.com (98.137.246.7): icmp_seq=3 ttl=46 time=97.7 ms
64 bytes from media-router-fp1.prod1.media.vip.gql.yahoo.com (98.137.246.7): icmp_seq=4 ttl=46 time=97.9 ms
64 bytes from media-router-fp1.prod1.media.vip.gql.yahoo.com (98.137.246.7): icmp_seq=5 ttl=46 time=97.6 ms
64 bytes from media-router-fp1.prod1.media.vip.gql.yahoo.com (98.137.246.7): icmp_seq=6 ttl=46 time=97.7 ms
^C
--- yahoo.com ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5005ms
rtt min/avg/max/mdev = 97.690/97.991/98.683/0.498 ms
```

正しく繋ぐことが出来た。machine2,machine3 からの接続については、ログの長さより割愛した。

(h) 最終状態を保存

```
[root@icesc17 ~]# iptables-save > /etc/sysconfig/iptables
[root@icesc17 ~]# iptables-save > /etc/sysconfig/iptables.sh
iptables.sh rm iptables-all.sh iptables-save -L -n sh iptables.sh logout reboot script -a log1-4
vi sysctl --system reboot sysctl --system vi /etc/sysctl.d/10-ipv4.conf script log1-4 ip neighbour
cat /etc/resolv.conf ip route addr show systemctl restart network ip addr show route cat /etc/resolv.conf ip neighbour
script log1-4 vi /etc/sysctl.d/10-ipv4.conf sysctl --system reboot sysctl --system ls vi log1-4 script -a
reboot logout sh iptables.sh iptables L -n -save rm iptables-all.sh Psh iptables-save > /etc/sysconfig/iptables
```

保存できた

(i) 結果の提出提出できた。

2. machine2 のファイアウォール設定

(a) firewalld の動作状態を確認

```
[root@www7 ~]# 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 Thu 2019-04-18 16:19:10 JST; 2h 6min ago
     Docs: man:firewalld(1)
 Main PID: 755 (firewalld)
    CGroup: /system.slice/firewalld.service
           └─755 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Apr 18 16:19:09 www7.ice.nuie.nagoya-u.ac.jp systemd[1]: Starting firewalld - dynamic firewall daemon...
Apr 18 16:19:10 www7.ice.nuie.nagoya-u.ac.jp systemd[1]: Started firewalld - dynamic firewall daemon.
```

確認できた。

(b) 現在のゾーンの許可状態を確認確認できた。

(c) 必要なサービス許可設定の追加

```
[root@www7 ~]# firewall-cmd --add-service=dhcpv6-client
Warning: ALREADY_ENABLED: 'dhcpv6-client' already in 'public'
success

[root@www7 ~]# firewall-cmd --add-service=dhcpv6-client=http
success

[root@www7 ~]# firewall-cmd --add-service=https
success

[root@www7 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp3s0
  sources:
  services: ssh dhcpv6-client http https
  ports:
  protocols:
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:
```

追加できた。

(d) 動作確認

(e),(f) 各設定の永続化, firewall の再起動

```
[root@www7 ~]# firewall-cmd --add-service=dhcpv6-client
Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled; vendor preset: enabled)
Active: active (running) since Thu 2019-04-18 16:19:10 JST; 2h 15min ago
  Docs: man:firewalld(1)
Main PID: 755 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─755 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Apr 18 16:19:09 www7.ice.nuie.nagoya-u.ac.jp systemd[1]: Starting firewalld - dynamic firewall daemon...
Apr 18 16:19:10 www7.ice.nuie.nagoya-u.ac.jp systemd[1]: Started firewalld - dynamic firewall daemon.
Apr 18 18:32:50 www7.ice.nuie.nagoya-u.ac.jp firewalld[755]: WARNING: ALREADY_ENABLED: 'dhcpv6-client' already in 'public'
[root@www7 ~]# systemctl status firewalld
Warning: ALREADY_ENABLED: dhcpv6-client[00m
success
[root@www7 ~]# firewall-cmd --permanent --add-service=http
success
[root@www7 ~]# firewall-cmd --permanent --add-service=https
success
[root@www7 ~]# firewall-cmd --reload
success
```

永続化し、再起動した。

3.4.4 考察

ファイアウォールを設定する際、戻りがよくわからなかつたので、調べることにした。

DNS 行きのパケットを考える。ファイアウォールは、通過しようとするパケットに対して、事前に設定したルールに照らし合わせてチェックを行う。行きのパケットを通過させるには、単純に、宛先ポート番号が 53 のパケットを通過許可としてルールを設定すればよい。問題は、DNS サーバーからの戻りパケットのルールである。送信元ポート番号が 53 の通信を許可してしまうと、送信元ポートが 53 で通信するように作成したアプリケーションからの通信は、悪意のあるものも含めてすべてファイアウォールを通過し、社内 LAN に達してしまう。あて先ポート番号でフィルタリングしようと思っても、1024 以上のポート番号の通信をすべて

許可する必要があり、大きく口を開けることになってしまう。

そこでステートフル・インスペクションが登場する。この機能を使えば、通過するパケットの状態を監視し、行きのパケットの通過を許可した時点で、戻りのルール（行きパケットに対する戻りパケット用）を動的に設定、許可することができる。なお、この戻りパケット用のルールは一定時間で無効となる。（※ ステートフルインスペクションとは、ファイアウォールを通過するパケットの中身を見て、動的にポートを開放したり、閉鎖したりする機能のこと。このステートフルインスペクションでは LAN 側から送信したデータをセッションログとして一時的に保存しておき、WAN（インターネット）側から到着したパケットがセッションログと整合性が合うかどうかを確認して、整合性があう場合は開放、矛盾する場合は閉鎖する。）

（文献 [13]、文献 [14] を参考。）

3.4.5 調査課題

- (4) 1. UNIX または Linux システムのユーザーデータベースに対してユーザーを認証し、ユーザープロファイルを決定するために、UNIX システム認証がサポートする方法は次のとおりである。

・ローカルリポジトリ内で Unix ユーザー ID を検索する SGD のログイン画面で、ユーザーは、共通名（たとえば Indigo Jones）、ユーザー名（たとえば indigo）、電子メールアドレス（たとえば indigo@indigo-insurance.com）のいずれか、およびパスワードを入力する。SGD は、ユーザーの入力した内容と一致する「名前」属性を持つユーザープロファイルを、ローカルリポジトリ内で検索する。一致する人物オブジェクトがない場合、「ログイン名」属性を対象に、最後に「電子メールアドレス」属性を対象に検索を繰り返します。ユーザープロファイルが見つからない場合、次のログイン認証機構が試される。ユーザープロファイルが見つかると、そのオブジェクトの「ログイン名」属性が UNIX または Linux システムユーザー名として使用されます。このユーザー名およびユーザーの入力したパスワードが、UNIX または Linux システムユーザーデータベースと照合されます。認証が失敗した場合は、次の認証機構が試されるローカルリポジトリ内で Unix グループ ID を検索するデフォルトのユーザープロファイルを使用する。認証が成功しても、ユーザープロファイルの「ログイン」属性が有効になっていない場合、ユーザーはログインできず、ほかの認証機構が試されることはない。認証が成功して、ユーザープロファイルの「ログイン」属性が有効になっている場合に、ユーザーはログインできる。

・ローカルリポジトリ内で Unix グループ ID を検索する SGD は、ユーザーがログイン画面で入力したユーザー名およびパスワードを、UNIX または Linux システムユーザーデータベースと照合する。認証が失敗した場合は、次の認証機構が試される。

認証に成功すると、SGD はユーザープロファイルを検索する。（次のセクションを参照）。ユーザープロファイルの「ログイン」属性が有効になっていない場合、ユーザーはログインすることができず、ほかの認証機構が試されることはない。ユーザープロファイルの「ログイン」属性が有効な場合、ユーザーはログインできることになる。

・デフォルトのユーザープロファイルを使用する SGD は、ユーザーがログイン画面で入力したユーザー名およびパスワードを、UNIX または Linux システムユーザーデータベースと照合する。認証が失敗した場合は、次の認証機構が試される。認証に成功した場合、そのユーザーはログイン

できる。

(文献 [15] を参考)

2. DNS

DNS(ドメインネームシステム)とは、mynavi.jpなどのドメイン名から対象となるIPアドレスを教えてくれるシステムである。インターネットやメールなどのネットワークではIPアドレスを利用して通信を実現していますが、IPアドレスは人にとって分かり辛い数字の羅列で構成されている。

2016年10月26日には、NetflixやTwitter、Spotifyといった名だたるWebサービスやWall Street Journalなどの有名サイトがアクセス不能になった。このトラブルは、IoT(Internet of Things)機器を標的にしたマルウェアの「Mirai」が引き起こした。世界中の有名サイトにDNSのサービスを提供する米Dynを標的に、大規模なDDoS攻撃を行ったのだ。これ以降セキュリティの強化を着々と行っている。

(文献 [16] を参考)

3. メール配信システム

内部からの情報流出リスクを最低限に抑えるために、オペレータ毎に操作できる内容を細かく設定することができる。たとえば、利用できるデータベースの制限、メールコンテンツ作成、配信スケジュール設定、配信後のログデータダウンロード、分析など、メール配信にかかる各種機能毎の利用制限を、オペレータ毎に柔軟に設定することが可能である。また、「個人情報」と指定した項目について、オペレータ毎にデータ内容をマスクする/しないを選択することができます。(文面プレビューや配信ログ、管理機能での検索時などに適用される)他にも承認フローで内部統制強化したり、操作をSSL通信で暗号化したりして、セキュリティを強化できる。

(文献 [17] を参考)

3.5 [課題5] WWWサービスの設定

3.5.1 目的・概要

machine2でWWWサーバを動作させる

3.5.2 実験方法

machine2で設定を行い、サービス起動後にmachine3とICE端末で確認作業を行う。

3.5.3 実験結果

1. firewallの停止

```
[root@www7 ~]# yum info httpd
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: mirrors.cat.net
* extras: mirrors.cat.net
* updates: mirrors.cat.net
Available Packages
Name        : httpd
Arch        : x86_64
Version     : 2.4.6
Release     : 88.el7.centos
Size        : 2.7 M
Repo        : base/7/x86_64
Summary     : Apache HTTP Server
URL         : http://httpd.apache.org/
License     : ASL 2.0
Description  : The Apache HTTP Server is a powerful, efficient, and extensible
              : web server.

[root@www7 ~]# yum info mod_ssl
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: ftp.jaist.ac.jp
* extras: ftp.jaist.ac.jp
* updates: ftp.jaist.ac.jp
Available Packages
Name        : mod_ssl
Arch        : x86_64
Epoch       : 1
Version     : 2.4.6
Release     : 88.el7.centos
Size        : 112 k
Repo        : base/7/x86_64
Summary     : SSL/TLS module for the Apache HTTP Server
URL         : http://httpd.apache.org/
License     : ASL 2.0
Description  : The mod_ssl module provides strong cryptography for the Apache Web
              : server via the Secure Sockets Layer (SSL) and Transport Layer
              : Security (TLS) protocols.
```

停止できた。

2. WWW サーバのインストール


```

Verifying : httpd-2.4.6-88.el7.centos.x86_64 4/5
Verifying : apr-util-1.5.2-6.el7.x86_64 5/5

Installed:
httpd.x86_64 0:2.4.6-88.el7.centos

Dependency Installed:
apr.x86_64 0:1.4.8-3.el7_4.1      apr-util.x86_64 0:1.5.2-6.el7      httpd-tools.x86_64 0:2.4.6-88.el7.centos      mailcap.noarch 0:2.1.41-2.el7

Complete!
[root@www7 ~]# yum install mod_ssl[0:2.4.6-88.el7]
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirrors.cat.net
 * extras: mirrors.cat.net
 * updates: mirrors.cat.net
Resolving Dependencies
--> Running transaction check
--> Package mod_ssl.x86_64 1:2.4.6-88.el7.centos will be installed
--> Finished Dependency Resolution

Dependencies Resolved

=====
Package          Arch        Version           Repository      Size
=====
Installing:
mod_ssl         x86_64     1:2.4.6-88.el7.centos      base           112 k

Transaction Summary
=====
Install 1 Package

Total download size: 112 k
Installed size: 224 k
Is this ok [y/d/N]: y
Downloading packages:
mod_ssl-2.4.6-88.el7.centos.x86_64.rpm | 112 kB  00:00:00
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Installing : 1:mod_ssl-2.4.6-88.el7.centos.x86_64 [1/1]   ] 1/1  Installing : 1:mod_ssl-2.4.6-88.el7.centos
                                                               ] 1/1  Installing : 1:mod_ssl-2.4.6-88.el7.centos
                                                               1/1
Verifying : 1:mod_ssl-2.4.6-88.el7.centos.x86_64               1/1

```

正常にインストールできた。

3. SSL/TLS 事故署名証明書の作成

(a) 密鍵鍵の作成

```

[root@www7 ~]# openssl genrsa -aes128 1024 > server.key
Generating RSA private key, 1024 bit long modulus
+++++
e is 65537 (0x10001)
Enter pass phrase:
Verifying - Enter pass phrase:

```

適当な文字列を入力した。

(b) パスフレーズの除去

```

[root@www7 ~]# openssl rsa -in server.key -out server.key
Enter pass phrase for 'server.key':
writing RSA key

```

正常に除去できた。

(c) CSR の作成

```

[root@www7 ~]# openssl req -utf8 -new -key server.key -out server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
if you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:JP
State or Province Name (full name) []:Aichi
Locality Name (eg, city) [Default City]:Nagoya
Organization Name (eg, company) [Default Company Ltd]:Nagoya University
Organizational Unit Name (eg, section) []:Computer Science
Common Name (eg, your name or your server's hostname) []:example.ice.nuie.nagoya-u.ac.jp
Email Address []:yamada.yuya@mbox.nagoya-u.ac.jp

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:1234
An optional company name []:group7

```

指導書を参考に CSR を作成した。

(d) 有効期間 1 年のサーバ証明書の作成

```

[root@www7 ~]# openssl x509 -in server.csr -out server.crt -days 365 -req -signkey server.key
Signature ok
subject=/C=JP/ST=Aichi/L=Nagoya University/OU=Computer Science/CN=example.ice.nuie.nagoya-u.ac.jp/emailAddress=yamada.yuya@mbox.nagoya-u.ac.jp
Getting Private key

```

手順を踏んで作成できた。

4. WWW サーバの主設定ファイルを修正

```
[root@www7 ~]# vi /etc/httpd/conf.d/ssl.conf
# When we also provide SSL we have to listen to the
# the HTTPS port in addition.
#
Listen 443 https

##
## SSL Global Context
##
## All SSL configuration in this context applies both to
## the main server and all SSL-enabled virtual hosts.
##

#
# Pass Phrase Dialog:
# Configure the pass phrase gathering process.
# The filtering dialog program ('builtin' is a internal
# terminal dialog) has to provide the pass phrase on stdout.
SSLPassPhraseDialog exec:/usr/libexec/httpd-ssl-pass-dialog

#
# Inter-Process Session Cache:
# Configure the SSL Session Cache: First the mechanism
# to use and second the expiring timeout (in seconds).
SSLSessionCache [9CshmcB:/run/httpd/sslcache(512000)
SSLSessionCacheTimeout 300

#
# Pseudo Random Number Generator (PRNG):
# Configure one or more sources to seed the PRNG of the
# SSL library. The seed data should be of good random quality.
# WARNING! On some platforms /dev/random blocks if not enough entropy
# is available. This means you then cannot use the /dev/random device
# because it would lead to very long connection times (as long as
# it requires to make more entropy available). But usually those
# platforms additionally provide a /dev/urandom device which doesn't
# block. So, if available, use this one instead. Read the mod_ssl User
# Manual for more details.
SSLRandomSeed startup file:/dev/urandom 256
SSLRandomSeed connect builtin
#SSLRandomSeed startup file:/dev/random 512
#SSLRandomSeed connect file:/dev/random 512
#SSLRandomSeed connect file:/dev/urandom 512

#
# Use "SSLCryptoDevice" to enable any supported hardware
# accelerators. Use "openssl engine -v" to list supported
# engine names. NOTE: If you enable an accelerator and the
```

修正した。

5 WWW サーバの起動

しっかり起動できた。

6. machine3 と外部テスト端末から http, https 両方の動作を確認

木曜日 18:06

アプリケーション 場所 Firefox Web ブラウザ

国土交通省 - Mozilla Firefox

国土交通省 www.mlit.go.jp

YouTube 検索 English

標準 大音声読み上げルビ振り Google カスタム検索 検索 検索方法 サイトマップ

ホーム 国土交通省について 報道・広報 政策・法令・予算 オープンデータ お問い合わせ・申請

トピックス 国土交通省の活動 RSS 一覧

【4月15日】 石井大臣の中国訪問

【4月15日】 パナマ共和国キハーノ運河局長官による同達政務官への表敬訪問

【4月12日】 中華人民共和国 程永華 軍事大臣による石井大臣への表敬訪問

【4月4日】 ICAO（国際民間航空機関）リク・ファン事務局長による同達政務官への表敬訪問

【4月1日】 敦賀/博多 新規航路開設歡迎式に同達政務官が出席

【3月31日】 「常磐自動車道 大槻IC」開通式典に同達政務官が出席

新着情報 消費税率10%への引上げ後の住民所得にメリットが出る支援策を用意

重要なお知らせ 政策情報

改元に伴う元号による年表示の取扱い及び情報システム改進等への対応について 国土交通省生産性革命プロジェクト 政策クローズアップ

www.mlit.go.jp/page/kanbo01_hy_006867_re.html 提出済み

ice@icesc00~ 国土交通省 - Mozilla Firefox ホーム 1 / 4

木曜日 17:58

アプリケーション 場所 Firefox Web ブラウザ Google - Mozilla Firefox

Google https://www.google.com 検索 Gmail 画像 ログイン

Google

日本

広告 ビジネス Googleについて プライバシー 規約 設定

ice@icesc00~ Google - Mozilla Firefox 1 / 4

画像の通り、接続できた。

7. WWW サーバのブート時自動起動を指定自動起動を指定し、再起動後も接続ができた。

3.5.4 考察

machine3 で https に接続する時、例外的な接続という操作を挟んだので、それについて調べることにした。

安全な接続を行う間、ユーザーの接続先が意図した相手であり接続が暗号化されていることを確かにするために、ウェブサイトは信頼された 認証局 (Certificate Authority) により発行された証明書を提示しなくてはなりません。「警告：潜在的なセキュリティリスクあり」というエラーページで エラー内容 のボタンをクリックし、エラーコードに SEC_ERROR_UNKNOWN_ISSUER または ”OZILLA_PKIX_ERROR_MITM_DETECTED と表示された場合、これは、Firefox が知らない認証局により発行された証明書が提示されており、そのページは信頼できないことを意味します。

(文献 [19] より引用)

このように firefox で出所が不明な証明書を提示するときにエラーが出るというものだ。証明書に対するセキュリティはしっかりとしているんだと感じた。

3.5.5 調査課題

(5) メールの SMTP や POP,IMAP プロトコルと組み合わせた「SMTP over SSL/TLS」「POP over SSL/TLS」「IMAP over SSL/TLS」などが該当する。(文献 [18] を参考)

4 まとめ

本実験を通して、プロトコルの基礎であったり通信やファイアウォールについての知識を深めることができた。分量が多くすべてを理解することはできなかったが、様々な初めて見る単語たちが少しづつ意味が分かっていく感じがして楽しかった。

参考文献

- [1] エンジニアの入り口 - TCP/IP とは？, <https://eng-entrance.com/network-tcpip> (4/19 参照)
- [2] IT lab, <https://infotechlabo.com/2018/07/20/tcp-ip/> (4/19 参照)
- [3] IT 用語辞典, <http://e-words.jp/w/LAN.html>(4/25 参照)
- [4] DMZ（非武装地帯）とは, <https://boxil.jp/mag/a3157/>(4/25 参照)
- [5] CentOS, <https://ja.wikipedia.org/wiki/CentOS>(4/25 参照)
- [6] CentOS 7 で恒久的に hostname を変更する,
<http://pcmaster.hatenablog.com/entry/2016/02/20/150034>(4/25 参照)
- [7] @IT, https://www.atmarkit.co.jp/ait/articles/0212/06/news002_3.html(4/25 参照)
- [8] TCP/IP - TCP とは, <https://www.infraexpert.com/study/tcpip8.html>(4/25 参照)
- [9] IP ヘッダ内の各情報, <https://www.itbook.info/study/p89.html>(4/25 参照)
- [10]

- [11] 情報系の学生の備忘録, <http://dripping.blog53.fc2.com/blog-entry-53.html>(4/25 参照)
- [12] Qiita, <https://qiita.com/networkelements/items/aa4aec5417306b4c7e71l>(4/25 参照)
- [13] 日経 XTECH, <https://tech.nikkeibp.co.jp/it/members/NOS/ITBASIC/20020405/1/>(4/25 参照)
- [14] ステートフルインスペクションとステートフルフェールオーバーとは,
<https://www.infraexpert.com/study/security25.html>(4/25 参照)
- [15] Oracle Docs, https://docs.oracle.com/cd/E19728-01/820-2820/unix_auth.html(4/25 参照)
- [16] ビジネス +IT, <https://www.sbbi.jp/article/cont1/35800>(4/25 参照)
- [17] WEBCAS, <https://webcas.azia.jp/email/manage/>(4/25 参照)
- [18] ITmedia, <https://www.atmarkit.co.jp/ait/articles/1704/12/news035.html>(4/25 参照)
- [19] mozilla, <https://support.mozilla.org/ja/kb/error-codes-secure-websites>(4/25 参照)