7章 ネットワークの基礎

7.1 インターネットプロトコルの基礎

- コンピュータなどの端末がネットワーク通信を行う場合、共通のルールが必要
- 現在の通信プロトコルの標準は「TCP/IP」である。

7.1.1 TCP/IPの通信フロー

- 4つの層に分けて管理をする
    - アプリケーション層
    - トランスポート層（ヘッダ -> ポート番号）
    - インターネット層（ヘッダ -> IPアドレス）
    - ネットワークインターフェイス層（ヘッダ -> MACアドレス）
- データを送信するときは「ヘッダ（＝パケット）＋データ」を送信する
- それぞれの層で利用されるプロトコルは異なる

レイヤー	**通信プロトコル**
アプリケーション層	FTP SSH Telnet SMTP DNS HTTP POP3 IMAP4 NTP HTTPS
トランスポート層	TCP UDP
インターネット層	IP ICMP ARP
ネットワークインターフェイス層(通信規格*TCP/IPとは別)	Ethernet IEEE802 PPP

- アプリケーション層
    - 各種ネットワークアプリケーションの制御を行う層
    - Webデータの閲覧、メールの送信など
- トランスポート層
    - データの転送制御を行う層
    - TCP：コネクションを確立し、エラー発生時は再送するなどのサポートをする信頼性の高い通信
    - UDP：コネクションは確立せず、エラー発生時も再送はしない
    - アプリケーション層でどの通信プロトコルを扱ったのかを指定するため、**ポート番号**を記録
        - ポート番号：１～１０２３＝ウェルノウンポート（特権ポート）

ポート番号	**アプリケーション**
20	FTP（データ利用）
21	FTP (制御)

ポート番号	アプリケーション
22	**SSH**
23	Telnet
25	**SMTP**
53	**DNS**
80	**HTTP**
110	POP3
123	**NTP**
139	NBT Session
143	IMAP
161	SNMP
162	SNMP Trap
389	LDAP
443	**HTTPS**
465	SMTPS
514	syslog
636	LDAPS
993	IMAPS
995	POP3S

- ネットワーク層
    - 宛先や伝送経路の制御
    - IPアドレスという宛先情報を利用
    - pingなどはこの層のプロトコルの**ICMP**を利用する
- ネットワークインターフェイス層
    - 様々な種類の回線への接続を管理
    - 同一ネットワークにおける宛先端末の管理
    - 宛先情報としてMACアドレスを扱う

7.1.2 IPv4アドレスとネットワーク構成

- 宛先情報としてIPアドレスを使用（IPv4 / IPv6）
- IPv4アドレスは32ビットで構成されており、8ビットずつ10進数に置き換えて、**IPアドレス**と**サブネットマスク**で次のように構成。
    - IPアドレス：192.168.56.11
    - サブネットマスク：255.255.255.0 (＝　/24)

- サブネットマスクが「1」になっている範囲を**ネットワークアドレス部**
- それ以降は、**ホストアドレス部**
- 各ネットワークで先約のあるアドレス
    - 各ネットワークの先頭：**ネットワークアドレス**
        - ネットワーク自体を表す
    - 末尾のアドレス：**ブロードキャストアドレス
        - 同じネットワーク内の全端末に送信が可能なアドレス

```
                    ネットワークアドレス          192.168.56.0
192.168.56.0/24     ホストアドレス                  192.168.56.1 ～ 254
                    ブロードキャストアドレス      192.168.56.255
```

- 同じネットワーク範囲のホストはARPでMACアドレスを検出し、直接通信する
    - MACアドレスはNICに対して物理的に割り当てられているアドレス
    - ブロードキャストでネットワーク内の全端末へ
- 異なるネットワーク範囲に接続する場合はルーターを使用する
    - ルーターのアドレスについては、**デフォルトゲートウェイ**アドレスを割り当てる

```
・各端末には、IPアドレスとサブネットマスクが必要
・各ネットワークには、ネットワークアドレスとブロードキャストアドレスが存在する
・異なるネットワークに接続するときは、デフォルトゲートウェイが必要
```

7.1.3 IPアドレスクラスとサブネット分割

クラス	第一オクテット（2進数での先頭部分）	デフォルトマスク
A	0 ～ 127 (0 ～)	255.0.0.0 (/8)
B	128 ～ 191 (10 ～)	255.255.0.0 (/16)
C	192 ～223 (110 ～)	255.255.255.0 (/24)

- デフォルトのマスク値が決まっているため、増やすのはかまわないが減らすのはできない

```
172.16.10.5/8  ･･･「×」 クラスBなので、/8にはできない
172.16.10.5/16 ･･･「〇」 クラスBのデフォルトのマスク値
172.16.10.5/14 ･･･「〇」 増やすのはOK
```

- 本来ホストアドレス部だった部分をネットワークアドレス部として利用する方法を**サブネット分割**という
- ネットワーク分割実行時のネットワーク数とホスト数

マスク値	分割後のネットワーク数	各ネットワークの最大ホスト数
/25	2	126(128-2)

マスク値	分割後のネットワーク数	各ネットワークの最大ホスト数
/26	4	62(64-2)
/27	8	30(32-2)
/28	16	14(16-2)
/29	32	6(8-2)
/30	64	2(4-2)

- IPv4 には
  - プライベートアドレス
  - グローバルアドレス（＝＞　ICANNによって管理される一意のアドレス）

IPアドレスクラスごとのプライベートアドレス範囲

クラス	プライベートアドレス範囲	デフォルトマスク
A	10.0.0.0 ～ 10.255.255.255	/8
B	172.16.0.0 ～ 172.31.255.255	/16
C	192.168.0.0 ～ 192.168.255.255	/24

特殊な用途で使用されるアドレス範囲

アドレス範囲	用途
127.0.0.0/8	ループバックアドレス（ホスト自身を表すアドレス、一般的には127.0.0.1を利用）
169.154.0.0/16	APIPA（DHCPサーバーからアドレスを取得できなかった場合に自動構成されるIPアドレス）

7.1.4 IPv6アドレス

- IPv6アドレスは、128ビットで構成され、これを8ビットずつ16進数に置き換える

```
2001:0dgt:dead:beef:0000:0000:1234/64
```

- 先頭に0がある場合は、表記を省略できる
- 0しか書かれていない数値列(0000)(ゼロフィールド)は省略できる
- ネットワークアドレス部(＝プレフィックス)とホストアドレス部(＝インターフェイス識別子)で構成
- IPv6には**アドレスのスコープ**という概念がある
- IPv6ではループバックアドレスは「::1」

スコープの種類	アドレス	用途
グローバル	2000::/3	インターネットで一意に利用。IPv4でのグローバルアドレスに相当

スコープの種類	アドレス	用途
ユニークローカル	fc00::/7	組織内のネットワークで一意に利用。IPv4でのプライベートアドレスに相当
リンクローカル	fe80::/10	同一ネットワークで一意に利用。IPv4でのリンクローカルアドレスに相当(APIPA)

インターフェイス

- enp0s3：仮想マシン同士の接続で利用するインターフェイス
- enp0s8：インターネットなど外部ネットワークへの接続で利用するインターフェイス

7.2 基本的なネットワーク構成

7.2.1 ホスト名の設定

```
cat /etc/hostname
```

```
# ホスト名の確認・設定
hostname [ホスト名]
```

7.2.2 TCP/IPの基本的な設定

nmcli

- NetworkManagerサービスを利用することで異なる環境でも同様にネットワークの設定ができる
- nmcli

```
# 再起動後も設定が残る
nmcli オブジェクト [サブコマンド] [引数]

    オブジェクト
        connection      接続情報の管理。インターフェイスの設定など。
        general         NetworkManagerサービスの管理
        device          デバイスの管理

    サブコマンド
        show            設定を参照
        modify          設定を変更
        up              接続の有効化
```

- show

```
nmcli connection show

NAME        UUID                                  TYPE      DEVICE
enp0s3      de428841-c5bc-4767-bcef-1a62963dd676  ethernet  enp0s3
有線接続 1  d8592de7-e07a-3393-b9ed-cfff1aed6161  ethernet  enp0s8nmcli connection
```

```
nmcli connection show enp0s3
```

- modify

```
nmcli connection modify enp0s3 connection.autoconnect "yes"

nmcli connection modify enp0s8 ipv4.address "10.0.0.1/24"
```

ip

- IPアドレスの確認

```
# インターフェイスやルーティング設定を確認・設定
ip [オプション] サブコマンド

    サブコマンド
        addr    IPアドレスに関する情報を表示・設定。サブコマンドで処理を実行
                show [インターフェイス名]   #設定情報を表示
                add IPアドレス/マスク dev インターフェイス名 #IPアドレスを設定
                del IPアドレス/マスク dev インターフェイス名 #IPアドレスを削除

        route   ルーティングテーブルに関する情報を表示・設定。(アドレス部にdefauletでデフォゲの設定)
                add IPアドレスまたはネットワークアドレス/マスク via 転送先 #ルート情報を追加
                del IPアドレスまたはネットワークアドレス/マスク via 転送先 #ルート情報を削除
```

```
ip a
ip addr
```

- nmcliコマンドで設定した内容を読み込ませる

```
systemctl restart network
```

- ipコマンドでIPアドレスを設定する
    - networkサービスが起動している間、有効

```
# loインターフェイスにIPアドレスを追加
ip addr add 127.0.0.2/8 dev lo

ip addr show lo
```

ifconfig

```
ifconfig [オプション] [インターフェイス名] [IPアドレス [netmask サブネットマスク]] [up/down]

    -a   無効になっているインターフェイスも表示する
```

- インターフェイスの有効化、無効化は以下でもできる
  - ifup インターフェイス名
  - ifdowm インターフェイス名

	iprouteパッケージ	**net-toolsパッケージ**
インターフェイス/IPアドレスの参照・設定	ifconfig、ifup、ifdown	ip
ルーティングテーブルの参照・設定	ip route	route
ネットワーク接続情報	ss	netstat

7.2.3 ルート情報の設定

ルーティングテーブル

- ルータに記録される経路情報で、ルーティング処理を行う際に参照する。作成方法には、スタティックルーティングとダイナミックルーティングの2種類がある。
- あるネットワークの端末Aから別のネットワークの端末Bへデータを転送するとき、中継するルータは端末Bが所属するネットワークへ届けるための経路、つまりルートをルーティングテーブルから参照して転送する。
- スタティックルーティングとは、あらかじめネットワーク管理者が接続するネットワークのアドレスを設定する方法だ。一方のダイナミックルーティングとは、ルータ同士が経路情報をルーティングプロトコルによって交換し、自動でルーティングテーブルに設定する方法である。

```
ip route

default via 10.0.2.2 dev enp0s3 proto dhcp metric 100
10.0.2.0/24 dev enp0s3 proto kernel scope link src 10.0.2.15 metric 100
192.168.21.0/24 dev enp0s8 proto kernel scope link src 192.168.21.3 metric 101
```

```
route (表示)
route add -net ターゲット netmask マスク gw ゲートウェイ /
```

```
                                        default gw ゲートウェイ (追加)
route del -net ターゲット / default (削除)

    -n  ルート情報を名前解決せずに表示
```

7.3 基本的なネットワークの問題解決

ping

```
ping [オプション] 宛先

    -c 回数 :  指定した回数、ぱけっとを  送信
```

- pingによる疎通確認
  - ICMPパケットを送信して確認する
  - ICMPはインターネット層のプロトコルだが、IPヘッダとともにICMPメッセージが付与される

```
Ethernetヘッダ  +  IPヘッダ  +  ICMPヘッダ  +  データ
                    __  | |__
                  __|       |__
                 |              |
メッセージタイプ  +  メッセージコード  +  チェックサム  +  各タイプのヘッダ
```

- 主なICMPメッセージタイプ

メッセージタイプ	意味
0：エコー応答	pingパケットを受信したホストが返す応答メッセージ
3：宛先到達不能	途中経路などで設定ミスなどにより、目的のホストにメッセージを送るのが不可
8：エコー要求	pingを実行したときに贈られるエコー応答を要求するメッセージ
11：時間経過	経由したルーターが多すぎるなど、目的のホストにメッセージを送ることができない場合に帰ってくる

traceroute

```
# 宛先に到達するまでの経路を出力できる
traceroute [オプション] 宛先

    -I  :  ICMPエコー要求による経路を確認(既定ではUDP)
```

tracepath

```
# 宛先に到達するまでの経路をMTUとともに出力
tracepath [オプション] 宛先
```

Ipv6に対して

- ping6
- traceroute6
- taracepath6

7.3.2 TCP/IP通信の状態を確認

ss

```
# TCP/IP通信の状態を表示
ss [オプション]

    -a  :   待機ポートも含むすべての状態の通信を表示(-lを指定しなければ、確立した通信のみを表示)
    -l  :   待機(LISTEN)ポートを表示
    -n  :   名前解決せずに表示
    -t  :   TCP通信を表示
    -u  :   UDP通信を表示
    -p  :   対応するプロセスのPIDを表示
```

```
#  すべてのTCP/IP通信を表示
ss -atu
```

netstat

```
# TCP/IP通信の状態を表示
netstat [オプション]

    オプションはssと同じ
```

7.3.3 指定したポートへの接続

nc

```
# 指定したポートへの接続、もしくは指定したポートを待ち受け

    -l  :   指定したポートを待ち受ける
```

7.4 クライアント側のDNS設定

7.4.1 名前解決の設定

- 端末上に存在するetc/hostsファイルの情報を参照し、名前解決
- /etc/resolve.confファイルに指定されたNSサーバーに問い合わせて名前解決

この処理順は、/etc/nsswitch.confファイルに定義されている

```
# grep ^host /etc/nsswitch.conf
hosts:      files dns myhostname
```

```
# /etc/nsswitch.confの書式
システムデータベース：  サービス [サービス]
```

```
# /etc/hostsファイルの書式
IPアドレス ホスト名 [ホスト名]
```

DNSのはなし

- DNSサーバによる名前解決
  - FQDN(完全修飾ドメイン=ドメイン名のついたホスト名)とIPアドレスｗｐ解決
  - FQDNからIPアドレスを問い合わせる名前解決を**正引き**
  - IPアドレスからFQDNを問い合わせることを**逆引き**
- DNSサーバへの問い合わせの流れ
  - ISPや社内のDNSサーバに問い合わせ
  - example.comの権威NSサーバ(ゾーンを管理しているサーバ)に問い合わせ
  - 権威サーバが保持するゾーン情報からホスト名を検索
  - ローカルDNSサーバに対し応答
  - クライアントに応答
- 主なDNSレコード

レコードの種類	**内容**
SOA	ゾーンの権威情報
NS	DNSサーバー
MX	メールサーバー
A	ホスト名に対応するIPv4アドレス。ホスト名を指定した名前解決(正引き)の際に利用
PTR	IPアドレスに対応するホスト名。IPアドレスを指定した名前解決(逆引き)の際に利用
CNAME	ホストの別名

- 参照するDNSサーバは、/etc/resolve.confに記述する

```
# /etc/resolve.confファイルの書式
設定項目 値

    設定項目              意味
    search | domain      ドメイン名として補完
    nameserver           DNSサーバーアドレス(複数行設定可能)
```

7.4.2 名前解決の検証

- host

```
# 名前解決を検証し、簡易的な情報を出力
host [オプション] 名前 [DNSサーバー]

    -t レコード      :    問い合わせるレコードの種類を指定
```

- dig

```
# 名前解決を検証し、詳細な情報を出力
dig [オプション] [@サーバー] 名前 [レコード]

    -x       :    逆引きの問い合わせ(PTRレコードの問い合わせ)を実行
```

- nslookup

```
# 名前解決を検証し、簡易的な情報を出力
nslookup [オプション] 名前 [DNSサーバー]

    -type=レコード   :    問い合わせるレコードの種類を指定
```

最強Web問題集から

> ipコマンドを使って、以下の条件でルーティングテーブルに新しい経路を追加したい。正しいコマンドはどれか
> 宛先ネットワークアドレス：192.168.3.0
> サブネットマスク：255.255.255.0
> ゲートウェイ：192.168.1.1

```
ip route add 192.168.3.0/24 via 192.168.1.1
```

- RHEL7やCentOS7以降はnet-toolsがインストールされず、新しいiproute2が採用されている

	net-tools	**iproute2**	**iproute2（省略形）**
アドレスの表示	ifconfig	ip addr	ip a
リンク状態の表示	ifconfig	ip link	ip l
ルーティングテーブルの表示	route	ip route	ip r
ソケットの表示	netstat	ss	ss
ソケットの表示（プログラム名付き）	netstat -tulpn	ss -tulpn	ss -tulpn
インターフェイスの統計情報表示	netstat -i	ip -statistics link	ip -s l
ARP テーブルの表示	arp	ip n	ip neighbor
ARP テーブルのモニタ	-	ip monitor	ip mo

- ルーティングテーブルに新しい経路を追加する