

# クラウドのための ネットワーク知識

ネットワーク技術

---

# 自己紹介

- 佐伯幸郎(さいきさちお)
- 神戸大学システム情報学研究科
- クラウド・AI・ビッグデータの教育プロジェクトに従事

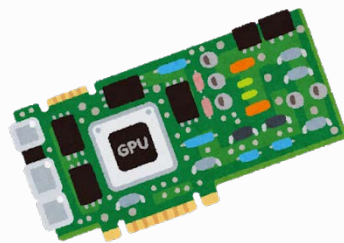
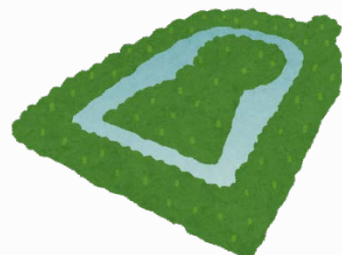


enpit

Cloud Spiral

AiBiC Spiral

- カープと古墳とビデオカードが好き



# 今日の内容

- 前回学んだクラウドを実際に利用するにあたり、必要となるネットワークの基礎を身に付ける。
  - 細かい仕様、技術は知らなくても良いが、最低限必要な概念や知識を身に付けることで、どのようなサービスをどう使っていくか、考えることが可能になる。
- 2コマで網羅することは無理・・・
  - 概念の理解に努める
  - 分かりやすさを重視 → 厳密性はある程度犠牲に



**注意**

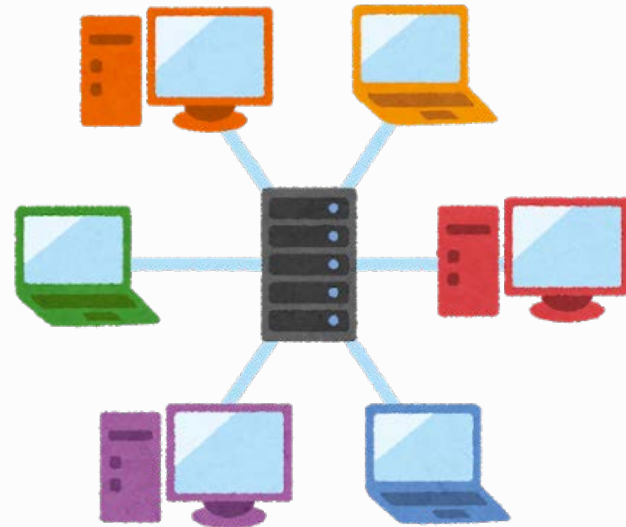
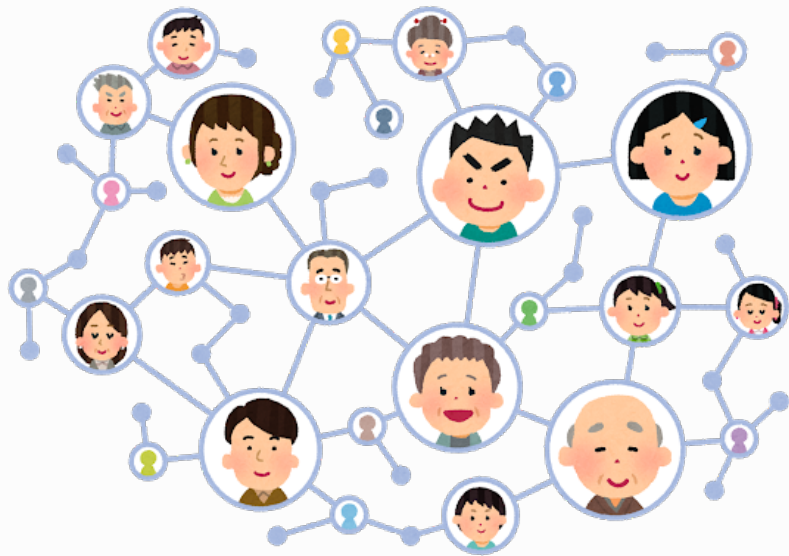
# ネットワーク入門

情報伝達をしよう

---

# ネットワーク？

- Net(網) + Work(作られたもの)
  - 人やものごとを網状につなげた系、システム (wikipedia)
  - つながっているもの: ノード
  - ノード同士のつながり: リンク



# 様々なネットワーク

- \*\*\*ネットワークという言葉
  - ネットワークが何をつないでいるのか (対象)
    - 人的ネットワーク、コンピュータネットワーク、放送局ネットワーク
  - ネットワークを利用して何をするのか (目的)
    - 通信ネットワーク、交通ネットワーク
  - ネットワーク内を移動する中身 (内容)
    - 情報ネットワーク、人材ネットワーク
  - ネットワークの決まり事 (手順)
    - TCP/IPネットワーク、

# ネットワーク通信

- 情報ネットワーク内のノード間で行う情報伝達



# 情報伝達の手順

- 通信はお互いがルールを守らないと成立しない



日本語で  
口頭で話をする  
相手が話しているときは黙っておく



町内会で決められた順番で  
紙に情報が書いてある  
受け取ったら2日以内に次の人に回す  
読んだらサインをする



決められたお金を払い  
相手の郵便番号と住所を記載  
ポスト・郵便局で投函  
配達員が指定場所に届ける



# 伝達先の指定方法



やすし君のお母さん

ネットワーク内で一意に決まる必要

- ・大域的に一意
- ・局所的に一意



隣の家のきよし君ち



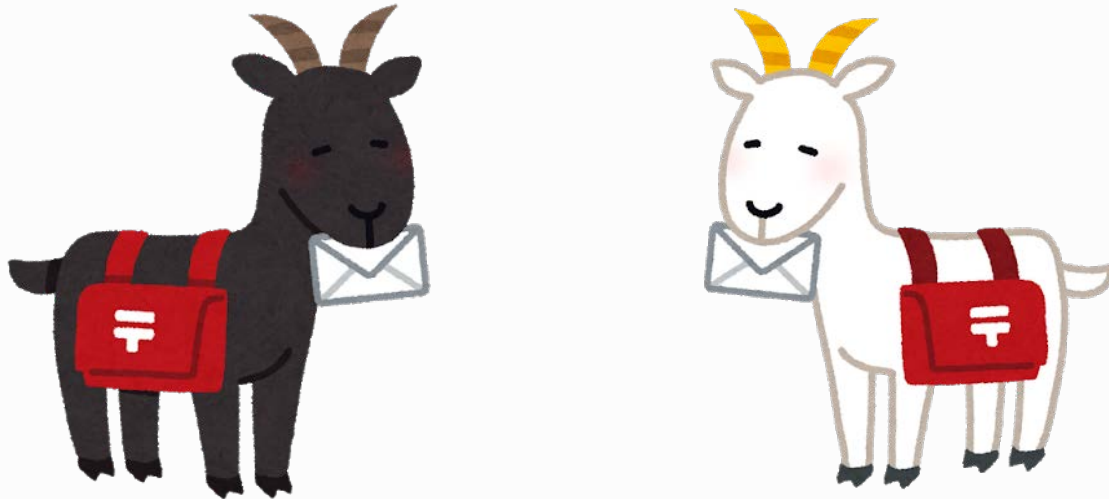
〒652-8510 兵庫県神戸市兵庫区御所通1丁目2-28

# 情報伝達を成立させるために

- 通信の手順
- 相手の指定の仕方

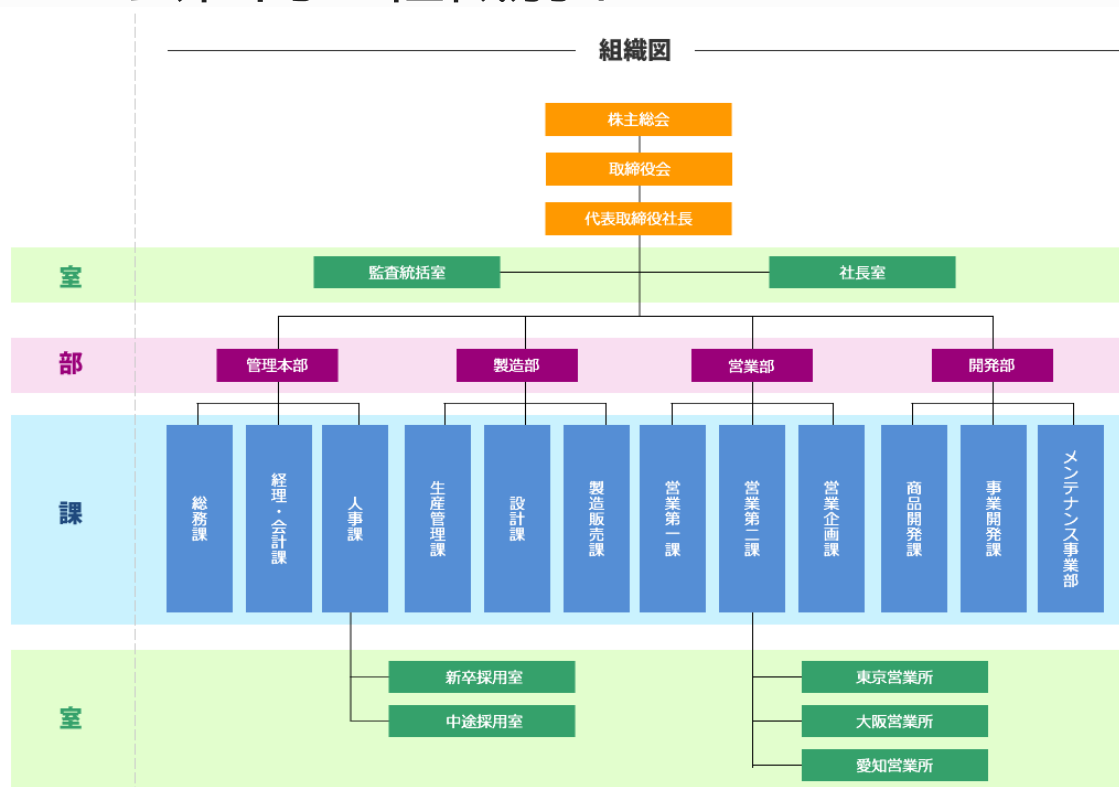


- などを決めておく必要がある



# ネットワークの構造

- 複数あるネットワークがリンクを持つ場合もある
  - とよりの町内会とお互い情報交換
  - 会社内の組織別ネットワーク



ネットワークは階層構造で考える  
(と効率が良い)

情報伝達の範囲を指定しやすい

# まとめ

- ネットワークとは人・ものなどを網の上につなげたもの
    - 対象・目的・内容で \*\*\*ネットワークと呼ぶ
  - ネットワーク通信はネットワーク上でつながったノード同士が行う情報伝達
  - 情報伝達を行うにはルールを決める必要がある
  - ネットワークは階層構造で考えよう
-

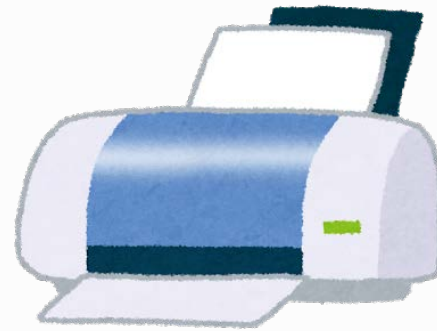
# コンピュータネットワーク通信

TCP/IPとインターネット

---

# コンピュータの世界での通信

- ノード: コンピュータなどの情報機器



- ルール: **プロトコル**で決まっている
  - どんな接続方法で(有線? 無線? 光ファイバー?)
  - 通信速度
  - データの構造
  - 通信手順 …… などなど

# 標準的に使われるプロトコル

- TCP/IP(プロトコルスイート・スタック)
  - 事実上今日のコンピュータネットワークの標準となっている
    - TCP(Transmission Control Protocol)
    - IP(Internet Protocol) を中心とした構成
  - 通信をパケット飛ばれる単位で送受信する
  
- DARPA(Defense Advanced Research Projects Agency、アメリカ国防高等研究計画局)がARPANETの次世代プロトコルのために策定

# (参考)OSI7層モデル

- いろいろな機器をつなぐ通信機器に必要なとなる通信機能を階層化して世界標準とした規格
- TCP/IPの方が先に確立していたため(4層モデル), 正確にはOSI7層モデルには準拠していない。対応づけは可能

OSI参照モデル		TCP/IPプロトコルスタック	プロトコル
第7層 (レイヤ7)	アプリケーション層	アプリケーション層	FTP,TFTP,SMTP,POP,TELNET,SSH HTTP,SNMPなど
第6層 (レイヤ6)	プレゼンテーション層		
第5層 (レイヤ5)	セッション層		
第4層 (レイヤ4)	トランスポート層	トランスポート層	TCP,UDP
第3層 (レイヤ3)	ネットワーク層	インターネット層	IP、ARP、ICMPなど
第2層 (レイヤ2)	データリンク層	ネットワークアクセス層	Ethernet,FDDI,ATM,フレームリレー HDLC,PPP
第1層 (レイヤ1)	物理層		



# TCP/IPに使われる通信網

- ネットワークアクセス層で定義
  - 小規模
    - Ethernet (LANケーブル: UTP・STP)
    - IEEE802.11(WiFi)
  - 大規模
    - FDDI (大昔)
    - ATM (昔)
    - Ethernet (光ファイバ)



TCP/IPプロトコルスタック	プロトコル
アプリケーション層	FTP,TFTP,SMTP,POP,TELNET,SSH HTTP,SNMPなど
トランスポート層	TCP,UDP
インターネット層	IP、ARP、ICMPなど
ネットワークアクセス層	Ethernet,FDDI,ATM,フレームリレー HDLC,PPP

# TCP/IPに使われる通信の種類

## • TCP

- パケット送信ごとに毎回相手と確認を送る。信頼性が高い
  - (A)今から送るよ→(B)了解。こっちも返事送るよ→(A)了解
  - 3-way ハンドシェイク
  - (ABA)3-wayハンドシェイク→(A)送信→(B)受信しました
- 通信のオーバーヘッドが大きい

## • UDP

- いきなり送り付ける。受信保証も無い。
- 映像のストリーミングなどで使う

# IPアドレス

- TCP/IPにおけるノードの指定方法。宛先。
  - 32bitの数字（2進数32桁）
    - 11000000101010000000000000000001
  - 8bitごとに10進数に変換して表記(ドットつき十進表記)
    - 192.168.0.1
  - 約43億のアドレスを識別できる
    - 0.0.0.0～255.255.255.255
- ネットワークアドレスとホストアドレスに分割される
  - サブネットマスクによる表現
  - CIDRによる表現



# ネットワークアドレス

- TCP/IPではネットワークアドレスが同じノード同士が直接通信可能(リンク内にいる)
  - サブネットマスク
    - IPアドレスのネットワークアドレスかを示す
    - 32bitのマスクでIPアドレスと論理積(AND)を算出
    - 例)サブネットマスク 255.255.255.0
      - 11000000101010000000000000000001 (IPアドレス)
      - 111111111111111111111111111100000000 (サブネットマスク)
      - 11000000101010000000000000000000 (ネットワークアドレス)
  - CIDR
    - IPアドレスの上位何ビットがネットワークアドレスかを示す
    - /24 でネットワークアドレスのビット数を表記
    - 192.168.0.0/24 → **192.168.0.** がネットワークアドレス
      - **11000000101010000000000000000000** (ネットワークアドレス)



# ホストアドレス

- IPアドレスのネットワークアドレス以外の下位ビット
  - 192.168.0.1/24 の場合
    - 11000000101010000000000000000000**00000001** (下位8ビット)
  - サブネットマスクに応じて存在できるホストの数が決まる
    - 8ビットの場合、00000000～11111111の256台
    - ただし、以下の特別なアドレスは使用できないため、254台になる
      - ホストアドレスが全て0 → ネットワークそのものを指す
      - ホストアドレスが全て1 → ブロードキャスト(全体へ送る)
    - ネットワークアドレス: 192.168.0.0
    - ホストアドレス: 192.168.0.1～192.168.0.254
    - ブロードキャストアドレス: 192.168.0.255

# ネットワークの大きさ

## • LAN

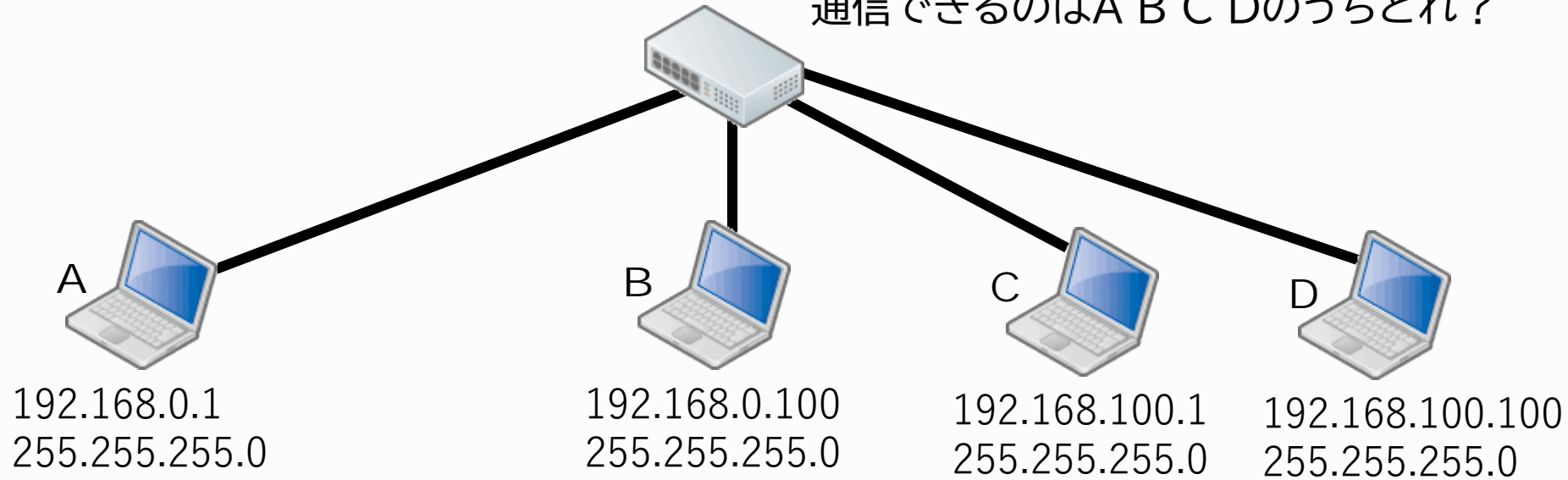
- Local Area Network。部屋や建物といった比較的小さな範囲で運用されるネットワークのこと
- 家庭内LAN(家の中の機器をつなぐネットワーク), 社内LAN(会社内の機器をつなぐネットワーク)など

## • WAN

- LANに対して地理的空間を隔てた場所同士をつなぐネットワーク。日本語では広域情報通信網という
- 会社の支社間をつなぐ, 大学のキャンパスをつなぐなど。

# 通信の可否を考えよう

通信できるのはA B C Dのうちどれ？

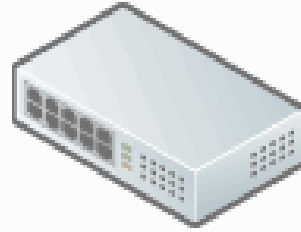


Aのネットワークアドレス: 192.168.0.0  
 Bのネットワークアドレス: 192.168.0.0  
 Cのネットワークアドレス: 192.168.100.0  
 Dのネットワークアドレス: 192.168.100.0

A⇔B OK  
 A⇔C NG  
 A⇔D NG  
 B⇔C NG  
 B⇔D NG  
 C⇔D OK

# ネットワーク機器

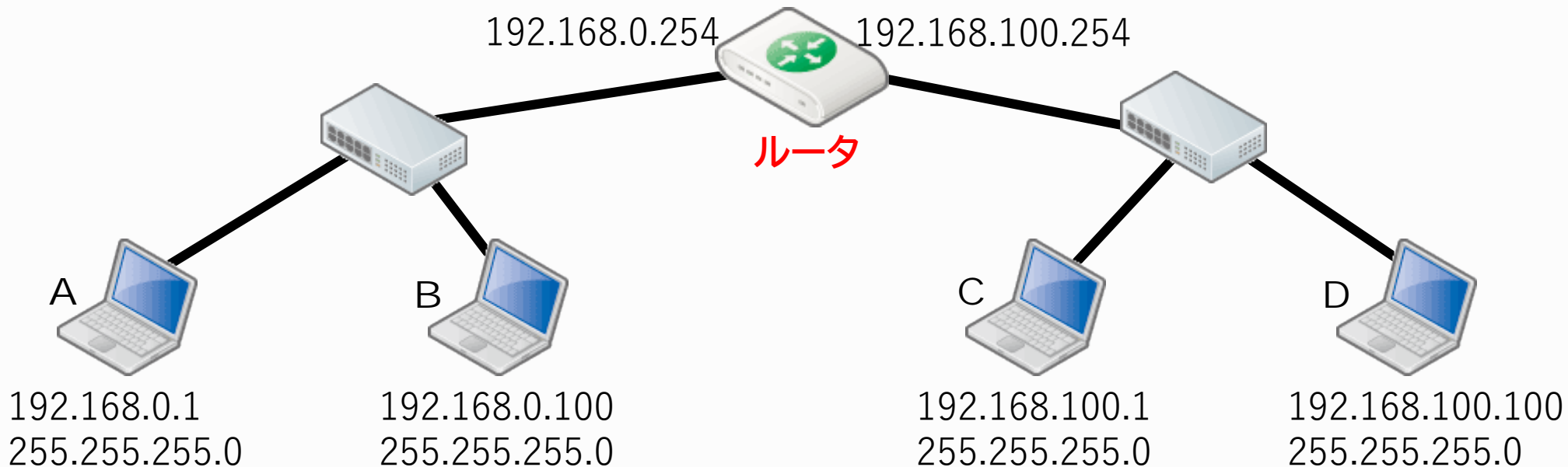
- ハブ(Hub)
  - 複数のノードを接続するための機器
- スイッチ
  - 少し賢いハブのこと。正式名称はスイッチングハブ
- ルータ
  - ルーティングを行うTCP/IPには欠かせない機器。口述





# ネットワークを超えた通信

- 違うネットワーク(ネットワークアドレスが異なる)との通信
  - ルータによるルーティングを行う(後述)



# Inter – Net / The Internet

- Inter \*\*\*
    - インターカレッジ, インターナショナル, インターチェンジ
    - ~間の, ~をまたいだ
  - Inter – Net
    - 複数のネットワークをルーティングによって接続したネットワーク
    - ネットワークの管理は各ネットワークごとに行われる
  - The Internet
    - 世界中のネットワークをルーティングによって接続し, 世界で一つのネットワークを構築
-

# Local IP / Global IP

## • Local IP

- Privateなネットワークで利用するIPアドレス
- LAN
- ネットワーク内で唯一であればよい
  - 違うネットワーク内では同一IPは使われている
- 接続された先のことは知らない

## • Global IP

- インターネットの世界で利用するIPアドレス
- 世界で唯一である (IANAが管理)
- 接続されたネットワークに同じIPがいることはない



# 素朴な疑問

- 家のパソコンでもスマホでもSwitchでもなんでもかんでもインターネットにつながっていますが、みんなグローバルIPが割り当てられているんですか？
  - 多くの場合、一つはISPからグローバルIPを割り当てられている
  - NATという技術を使い、家庭内LANのローカルIPとグローバルIPをうまく接続しています

# (おまけ)インターネット誕生の歴史

- アメリカの研究所や大学のコンピュータを相互に利用できるよう作られた研究用ネットワーク: ARPANET
  - 1969/10 運用開始
  - 1972 ARPA → DARPAに改称
  - 1973/9 TCP/IPの最初の規格文章
  - 1983/1 ARPANETでTCP/IPの運用開始
  - 世界中で色々なネットワーク(主に学術)が相互に接続される
  - 1988/8 初めて日米間でTCP/IP通信が太平洋を渡る
  - **1989/3 HTMLの原型ができる**
  - 1990/2 ARPANET終了
  - 1992/11 日本初の商用ISP(AT&T Jense株式会社)

# よくある質問

- インターネットは米国が核攻撃に合っても大丈夫なように作られたものって本当ですか？
  - 公式に否定。結果としてはもちろんそういう運用にも向いた。
- インターネットとはWorld Wide Webですよね？
  - HTMLはインターネットの仕組みが出来たあと、初めて生まれた
- インターネットっていつからできたんですか？
  - 気が付いたらなっていました。
- なんでこんなに急速に普及したんですか？
  - Windows95がISPへのダイヤルアップ・TCP/IPスタック・ブラウザを標準的に持っていたから



**注意**

# まとめ

- コンピュータネットワーク通信は現在はTCP/IPによって行われている。
- TCP/IPは通信を4つのレイヤに分けて管理する
- IPアドレスはネットワーク/ホストアドレスに分けられる
- ネットワークアドレスが異なる場合、ルータを経由して通信する
- インターネットはもともとは色々な学術・研究機関のネットワークを相互につないで計算機を利用するものだった
- グローバルIPで構成されたTCP/IPネットワークが今のインターネットである

# ネットワーク上のサービス

TCP/IPネットワーク上で利用されるサービス

---



# 用語の定義

- サーバ
  - サービスを提供するコンピュータやそのアプリケーション
- クライアント
  - サービスを利用するコンピュータやそのアプリケーション
- 端末/ホスト
  - ネットワークにつながっているコンピュータのノード
- 通信はサーバ・クライアントモデルをとる

**注意**

# DNS

- TCP/IPでは通信先はIPアドレスで指定する
- ブラウザなどではFQDNと呼ばれるホスト名+ドメイン名



- サーバのIPアドレスが変わると分からなくなる
- そもそも数字だと意味がよくわからない



- IPアドレスとドメイン名を管理するシステム
  - [www.denso-ten.com](https://www.denso-ten.com) → 104.120.14.74
  - FQDNからIPを検索することを正引き。逆を逆引き

# ドメイン名

- ネットワーク上の住所表記(のようなもの)
- 階層構造で管理され、世界で唯一となる
  - 住所表記と座標表記のような関係
    - 兵庫県神戸市兵庫区御所通1丁目2-28
    - 緯度: 34.660357 経度: 135.164474
- FQDNでは階層ごとに . で区切られ、ホスト名が付く

www.denso-ten.com

ホスト名

ドメイン名

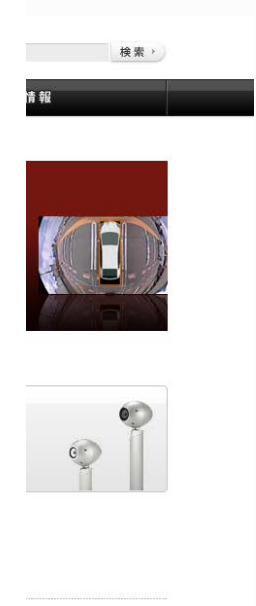
# Web (World Wide Web)

- インター
- HTMLの参
- 互に

システム  
URLへ  
同士を相

```

<!DOCTYPE html>
<!--[if lt IE 7 ]> <html class="ie8" lang="ja" prefix="og: http://ogp.me/ns# fb: http://www.facebook.com/2008/fbml" > <![endif]-->
<!--[if IE 7 ]> <html class="ie7" lang="ja" prefix="og: http://ogp.me/ns# fb: http://www.facebook.com/2008/fbml" > <![endif]-->
<!--[if IE 8 ]> <html class="ie8" lang="ja" prefix="og: http://ogp.me/ns# fb: http://www.facebook.com/2008/fbml" > <![endif]-->
<!--[if IE 9 ]> <html class="ie9" lang="ja" prefix="og: http://ogp.me/ns# fb: http://www.facebook.com/2008/fbml" > <![endif]-->
<!--[if (gt IE 9)!!(IE)]><!--> <html lang="ja" prefix="og: http://ogp.me/ns# fb: http://www.facebook.com/2008/fbml" > <!--><![endif]-->
<head>
<meta charset="UTF-8">
<title>デンソーテン - DENSO TEN Japan -</title>
<meta name="description" content="カーエレクトロニクスメーカー、株式会社デンソーテンの公式サイトです。インフォテインメント機器、電子制御機器、衝突安全<
<meta name="keywords" content="デンソーテン,Vehicle-ICT,ICT,車載情報機器,カーナビ,カーナビゲーション,株式会社デンソーテン,DENSO TEN,ECLIPSE,イクリパ<
<meta name="viewport" content="width=device-width, initial-scale=1">
<meta name="format-detection" content="telephone=no">
<meta http-equiv="X-UA-Compatible" content="IE=edge,chrome=1">
<meta property="og:title" content="デンソーテン - DENSO TEN Japan -">
<meta property="og:type" content="website">
<meta property="og:image" content="https://www.denso-ten.com/jp/_resource/img/common/icon_ogp.png">
<meta property="og:url" content="https://www.denso-ten.com/jp/">
<link rel="apple-touch-icon-precomposed" href="/_resource/img/common/icon_precompose.png">
<link rel="index" href="/_resource/img/common/icon_precompose.png">
<link rel="start" href="/_resource/img/common/icon_precompose.png">
<link rel="canonical" href="https://www.denso-ten.com/jp/"><!-- only index page -->
<link rel="stylesheet" href="/_resource/css/style.css">
<!--▼▼▼編集エリア▼▼▼-->
<style>
body.top .top_content .personal_box {
border-top: none;
}
.bnr_cg {
text-align: center;
width: auto;
padding: 0 0 30px;
margin: 0 0 25px;
border-bottom: 1px solid #e5e5e5;
}
body.top .top_content .personal_box .bnr_cg a {
display: inline-block;
}
body.top .top_content .personal_box>:first-child {
width: auto;
}
</style>
<!--▲▲▲編集エリア▲▲▲-->
<script src="/_resource/js/jquery/2.2.0/jquery.min.js"></script>
<script>window.jQuery || document.write('<script src="/_resource/js/jquery-2.2.0.min.js"></script>')</script>
<script src="/_resource/js/useful.js"></script>
<script src="/_resource/js/jqueryAutoHeight.js"></script>
<script src="/_resource/js/common.js"></script>
<!--[if lt IE 9]>
<script src="/_resource/js/html5shiv-printshiv.js"></script>
<script src="/_resource/js/selectivizr-min.js"></script>
<![endif]-->
<script src="/_resource/js/top.js"></script>
</head>
<body class="top">
<!-- Google Tag Manager -->
<noscript><iframe src="//www.googletagmanager.com/ns.html?id=GTM-QLCP"
height="0" width="0" style="display:none;visibility:hidden"></iframe></noscript>
<script>(function(w,d,s,l,i){w[l]=w[l]||[];w[l].push({'gtm.start':
new Date().getTime(),event:'gtm.js'});var f=d.getElementsByTagName('script')[0],
  
```



# WWW

- HTMLを公開する、Webサーバ
  - HTMLを転送するために策定されているプロトコル: HTTP
  - HTTPサーバとも言う
- サーバにアクセスし、HTMLを表示するWebブラウザ




# HTTPS (HTTP Secure)

- HTTPはリンク上の通信はすべて平文(もとのまま)で送る
  - 経路上の通信は簡単に盗聴可能
  - パスワードなどが丸見えになる
  
- クライアント-サーバ間通信を暗号化する
  - SSLを用いる
  
- 暗号化すれば安全というわけではないが
  - SSL証明書により相手の認証も行う



# URI/URL/URN

- URI: Uniform Resource Identifiers
  - Web上に存在するあらゆるリソースの場所を示したもの
  - URL + URN = URI
- URL: Uniform Resource Locator 
  - scheme + authority + path
- URN: Uniform Resource Name
  - 永続化されたWeb上のファイルの名前

## URI

### URL

<http://www.denso-ten.com/index.html>

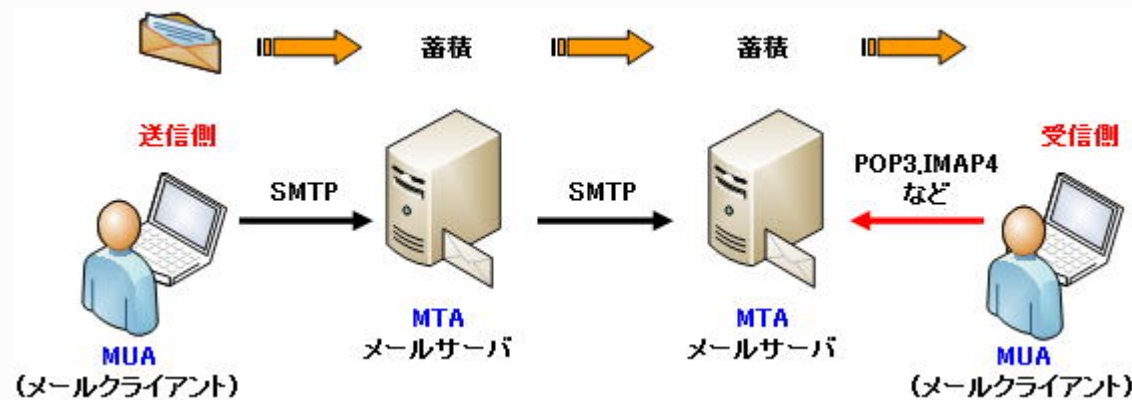
### URN

urn:densoten:-:W3C:DTD+HTML+4.01:JP



# メール

- メール送受信アプリケーション(MUA)
  - Thunderbird、Outlook、gmail
- 実際にメールを送信、相手のサーバに届ける(MTA)
- メールの送信には SMTP、受信にはPOP3などを利用





# FTP

- ネットワーク上でファイルをやり取りするサービス
  - FTPプロトコルを利用
- ファイル送受信を行うFTPクライアント



# SSH

- ネットワークに接続されたコンピュータなどを(安全に)遠隔操作するためのプロトコル
    - rsh(Remote Shell)のセキュア版
    - (リモートデスクトップのコマンドラインのようなもの)
  - 公開鍵認証、パスワード認証でサーバ・ユーザの正当性を確認
  - 通信内容も暗号化
-

# 最近のWebアプリケーション

- Webサーバ上で動くアプリケーションや、RESTと呼ばれる機能を使い、ブラウザとHTTP通信を介し、様々な機能を提供。
  - ハイパーテキストの転送だけに留まらない
  - クラウド時代のアプリケーションの形



# ポート番号

- TCP/IPでは通信時にポートと呼ばれる通信の出入り口を利用する

- IPアドレス:ポート番号
- 104.120.14.74:80

192.168.0.1:12345



- ポート番号は 1~65535まで利用可能
- サービスごとにサーバ側ポートが決められているものもある
  - Well-known Port

# Well-Known Port

- サービス提供にサーバが利用するポート
  - 20/21 FTP
  - 22 SSH
  - 25 SMTP
  - 53 DNS
  - 80 HTTP
  - 110 POP3 などなど...

# まとめ

- サーバ
    - ネットワーク上でサービスを提供する端末やソフトウェア
  - クライアント
    - サーバで提供されているサービスを利用する端末やソフトウェア
  - IPアドレスはDNSによってFQDNと紐づけられる
  - www FTP Mail SSH などのサービス
  - Webアプリケーションの仕組み
  - TCP/IPの通信には送受信にポートが必要
-

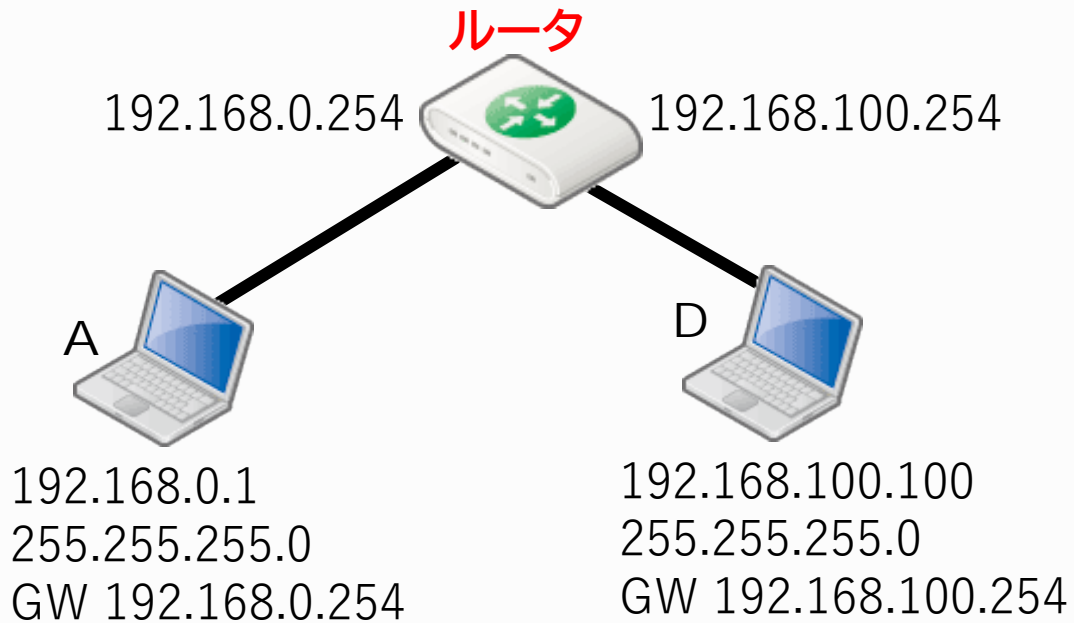
# ネットワークはなぜつながるのか

ルーティング・NAT・

---

# ルーティング

- TCP/IPでは、通信相手が自分のネットワークアドレスと異なる場合、デフォルトゲートウェイに通信を転送する



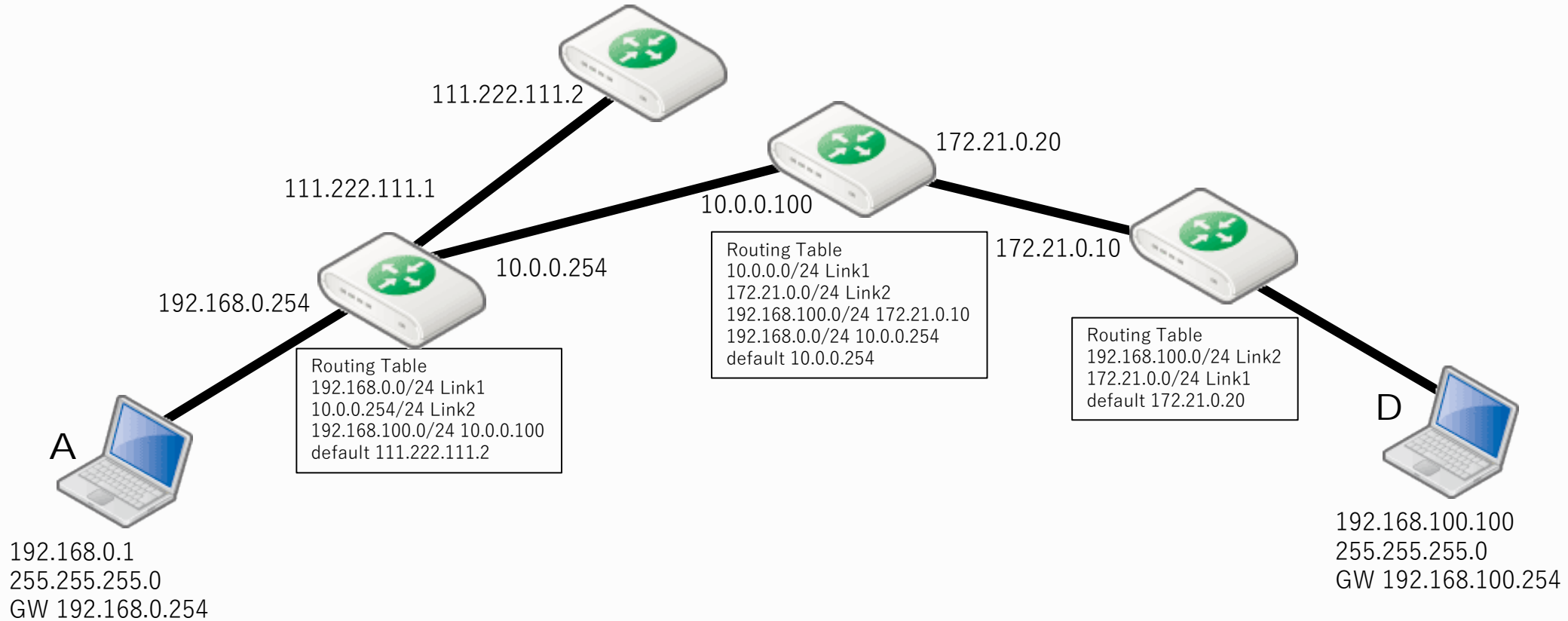
A が D と通信する場合

1. D のアドレスは A 自身のネットワークアドレスと異なる
2. A のデフォルトゲートウェイとして記述されているルータに転送
3. ルータは D のネットワークアドレスも持っているため D と直接通信
4. D に A からの通信が転送される
5. 通信に対する応答も逆向きに同様となる



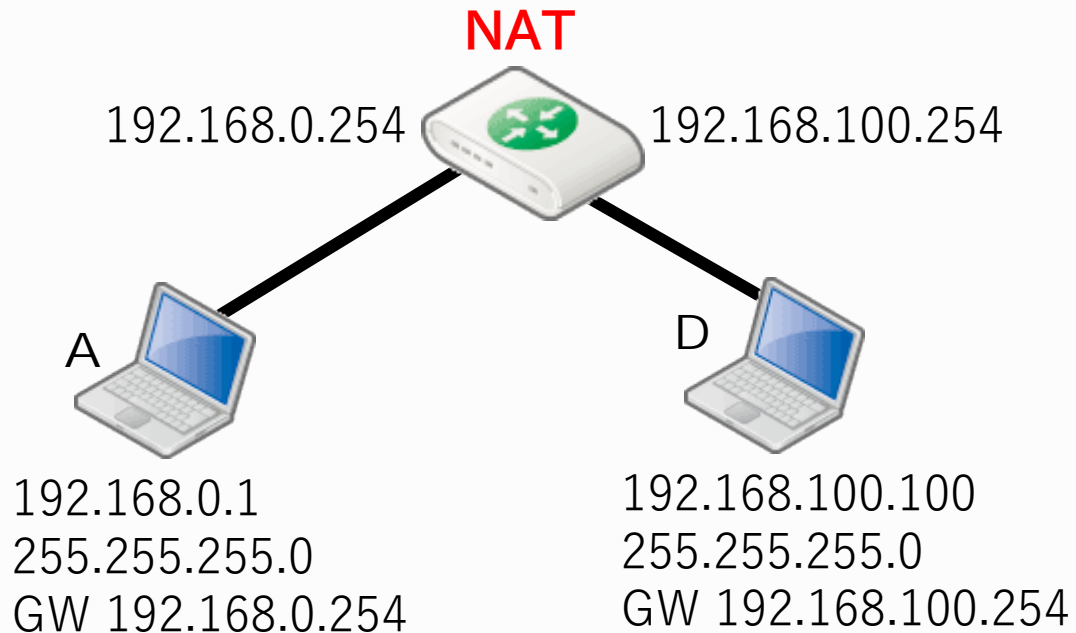
# 大規模なネットワーク

- 複数のネットワークを経由するような場合でも基本は同じ
  - ルータに転送 → **ルーティングテーブル**によって転送先を制御



# NAT (Network Address Translation)

- ネットワークをまたいだ通信を行う
- ルーティングではなくIPアドレスをNATルータが変換する



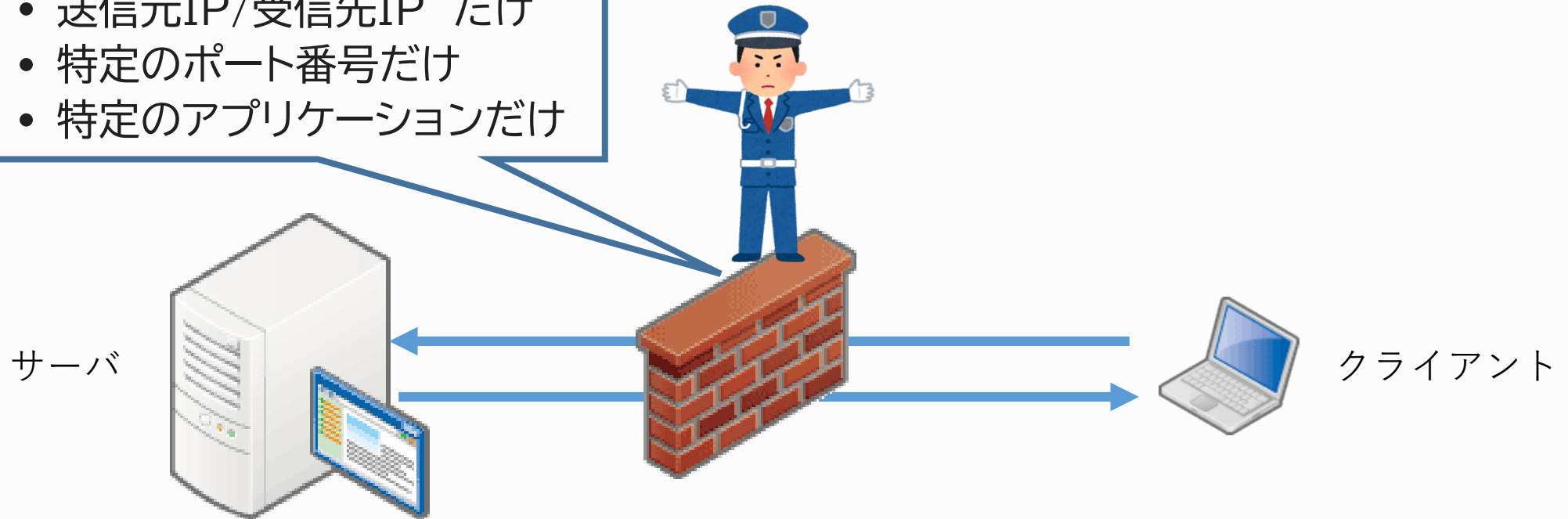
A が Dと通信する場合

1. DのアドレスはA自身のネットワークアドレスと異なる
2. Aのデフォルトゲートウェイとして記述されているルータに転送
3. ルータはAから受け取ったパケットの送信元を自分自身のD側IPアドレスに書き換える
4. 送信元を書き換えたパケットをNATがDに送信する
5. DはNATから送信された(と書きかえられた)通信にNATを宛先として返事をする
6. NATはDから受け取った本来はA宛てのパケットの宛先をAに書き換えてAに送信する

# ネットワーク通信のセキュリティ

## • Firewall(防火壁)

- 必要な通信だけ通す
- InBound / OutBound
  - 送信元IP/受信先IP だけ
  - 特定のポート番号だけ
  - 特定のアプリケーションだけ



# まとめ

- TCP/IPのネットワークはルーティングによりネットワークをまたいだ通信が可能
  - NATにより異なるネットワークアドレスに変換し通信を行うことも可能
  - 通信はFirewallによって、通信の許可・拒否を行う
-

# 全体のまとめ

- 「ネットワーク」とは何か理解
- 「ネットワーク通信」の概念
- 「コンピュータネットワーク」の理解
  - TCP/IP
  - The Internet
- ネットワークはなぜつながるのか

