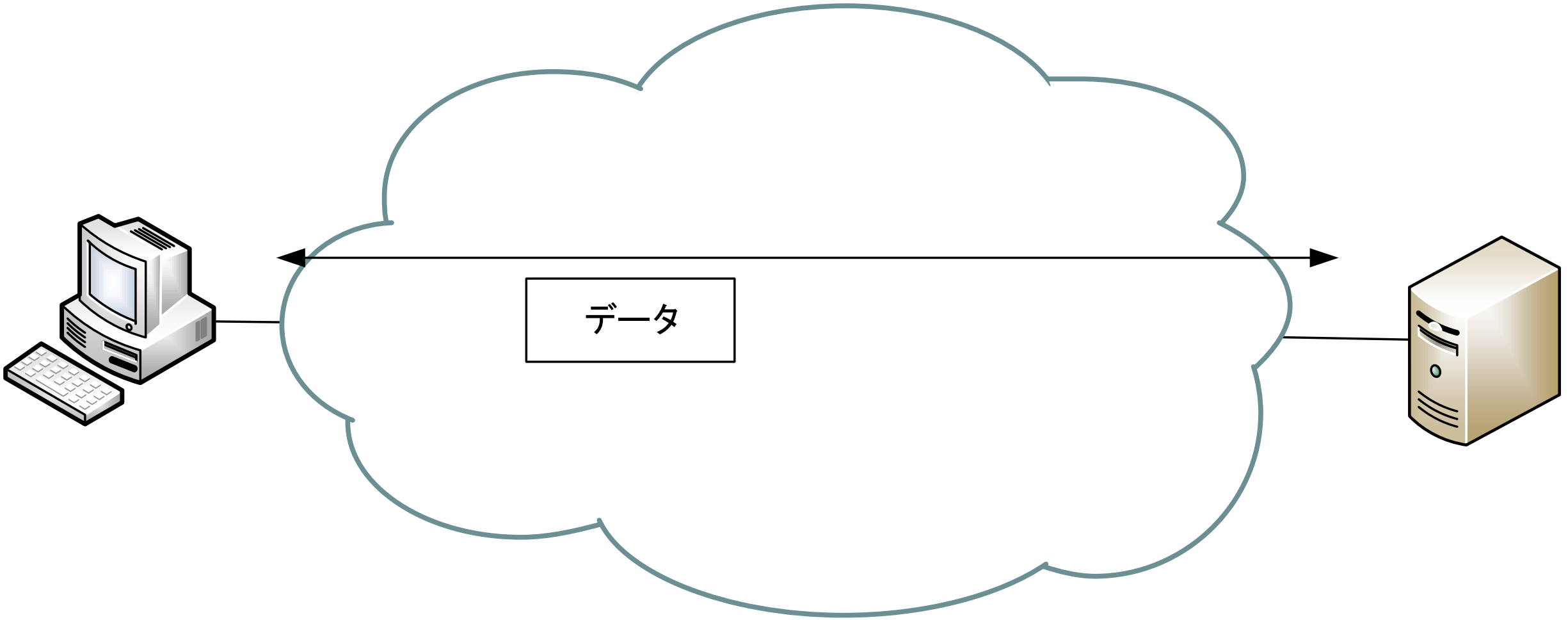
ネットワークの全体像を学ぼう

Office N-Study 土橋信浩(Gene)

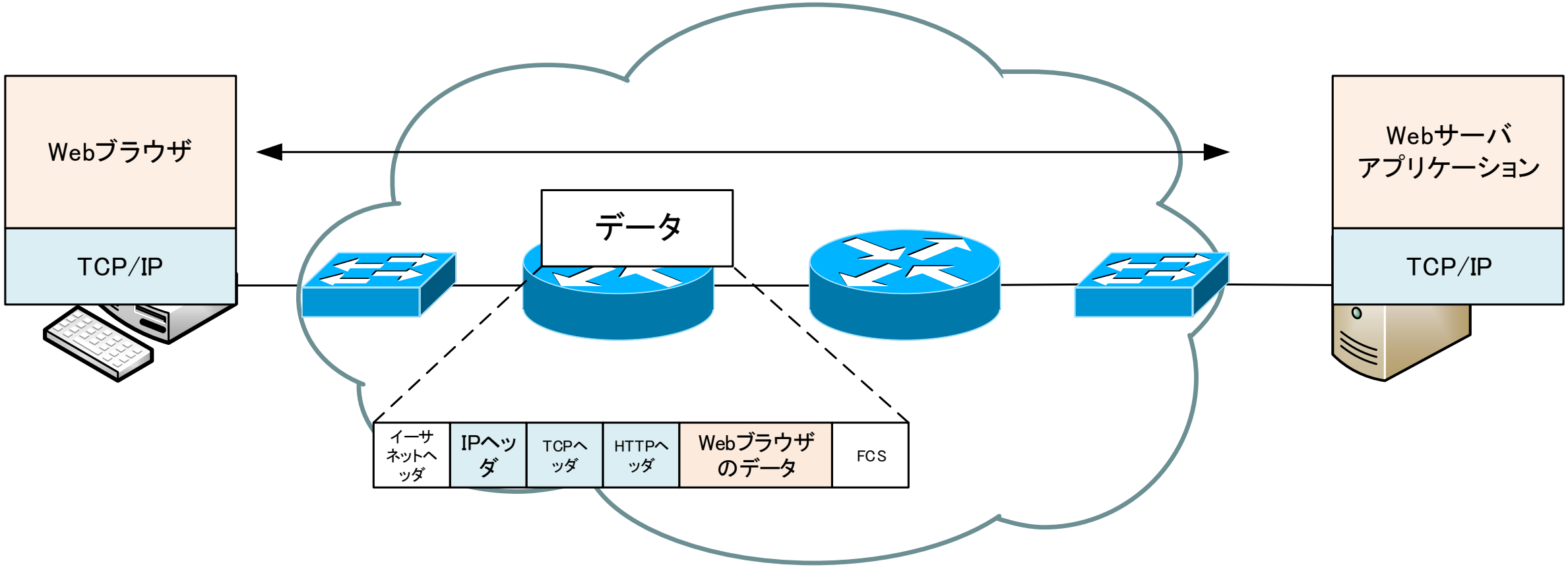
講座の目的

- ネットワーク上でのデータの転送の具体的な意味を知る
- 「誰が利用するネットワークなのか」というネットワークの分類を把握する
- ネットワークの具体的な構成を知る
- 代表的なネットワーク機器の概要を知る
- TCP/IPの概要を知る
- TCP/IPの設定の意味を知る

ネットワーク？？？



ネットワーク！！！


Webブラウザ
TCP/IP
データ
Webサーバ
アプリケーション
TCP/IP
イーサネットヘッダ
IPヘッダ
TCPヘッダ
HTTPヘッダ
Webブラウザのデータ
FCS

INDEX

担当講師 自己紹介

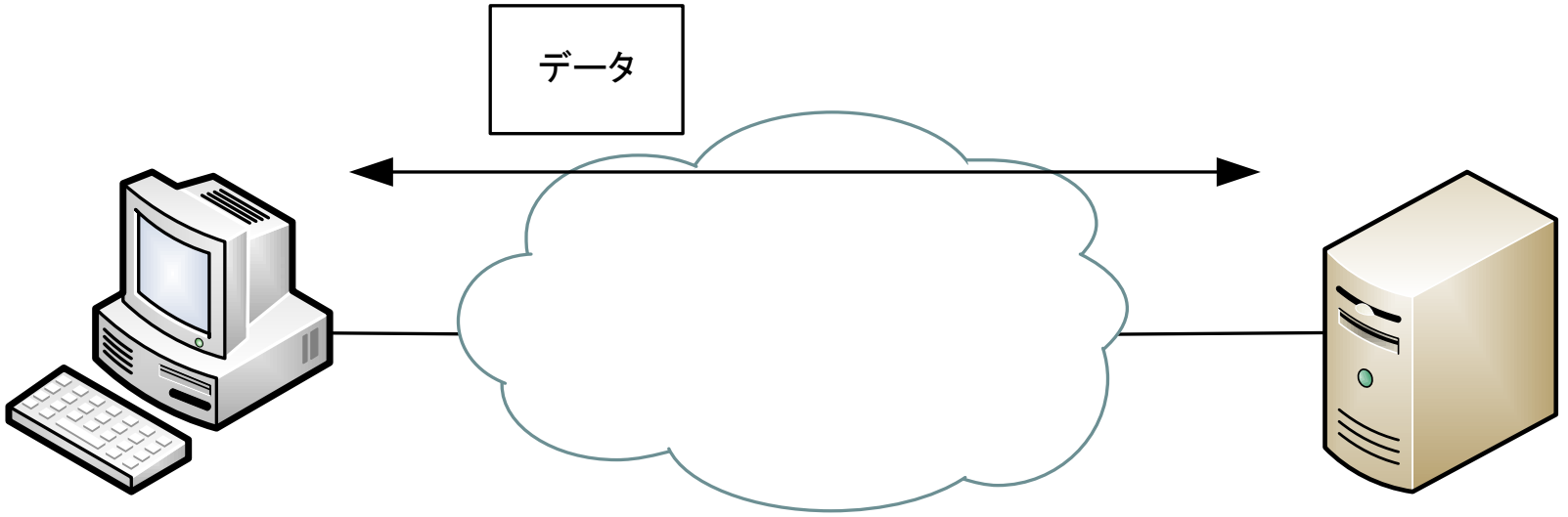
- 名前 : 土橋信浩(Gene)
- 経歴
  - 2000年よりネットワーク技術のインストラクタ
    - Cisco系の研修を主に担当
    - Webサイト/メールマガジン「ネットワークのおべんきょしませんか？」https://www.n-study.com を開始。ペンネーム「Gene」
    - ネットワーク技術系の著書多数
  - 2003年 CCIE Routing & Switching取得後、独立
    - 有限会社 オフィス・エヌ・スタディ
- 心がけていること
  - できるかぎりわかりやすく技術の仕組みを伝える
- 好きなこと
  - F1(フェラーリ)、B'z、ゲーム、ガンプラ、本を読むこと

そもそも「ネットワーク」とは？

ネットワークを利用していろんなメリットを享受する

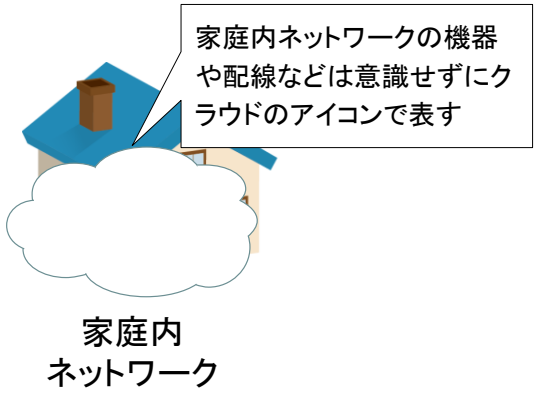
ネットワークの動作

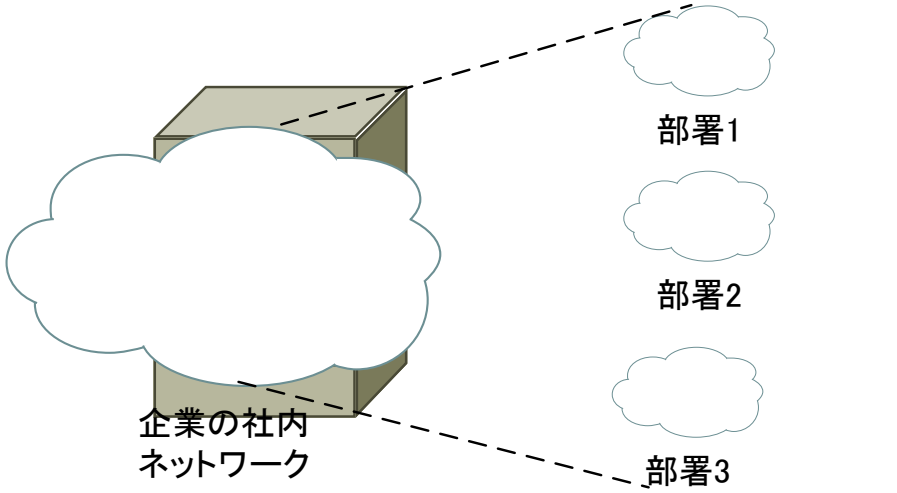
- ネットワークに接続しているサーバやPCなどの機器間でデータを転送



ネットワークの表現

- 雲(クラウド)のアイコンでネットワークを表現することが多い
  - 他には楕円のアイコンなど
  - ネットワークの具体的な構成を抽象化して表現している
- 前後の文脈によって、雲のアイコンが表現しているネットワークの規模は違うので注意
  - どこまで抽象化するかはケースバイケース
  - ひとつの雲で・・・
    - インターネット
    - 企業ネットワーク
    - 家庭内ネットワーク



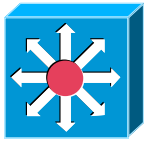


ネットワークの具体的な構成

- ネットワークは「ネットワーク機器」で構成する
  - ルータ
  - レイヤ2スイッチ
  - レイヤ3スイッチ
  - その他
    - 無線AP、無線LANコントローラ、ファイアウォール、IDS/IPS、VPNゲートウェイ、ロードバランサーなど

ルータ

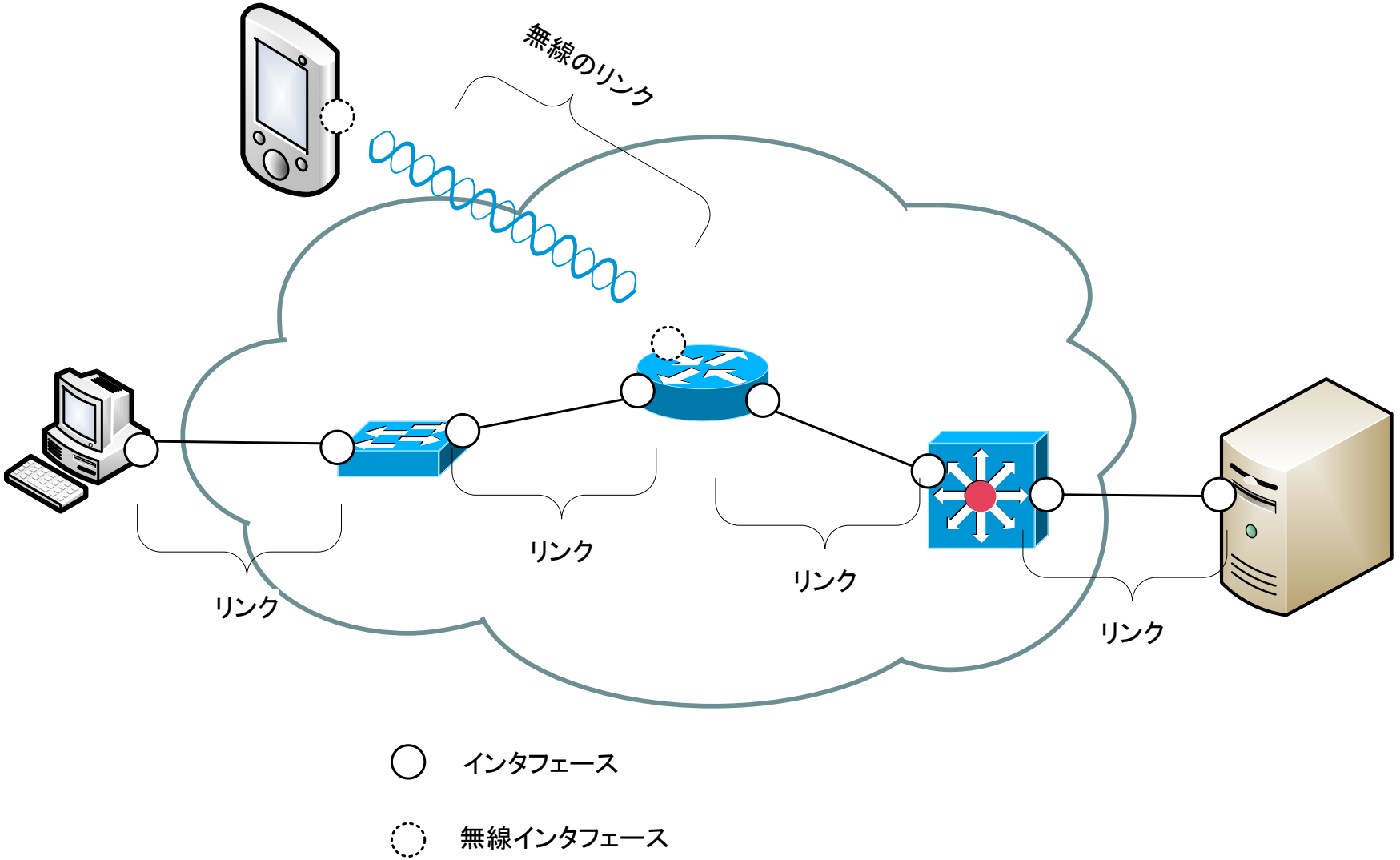
L2スイッチ



L3スイッチ

- ネットワーク機器やPC/サーバのネットワークインタフェース(ポート)同士を適切な伝送媒体(ケーブル)で接続してネットワークを構成する
  - インタフェース同士のつながり = リンク
    - 「セグメント」と表現することもたまにある

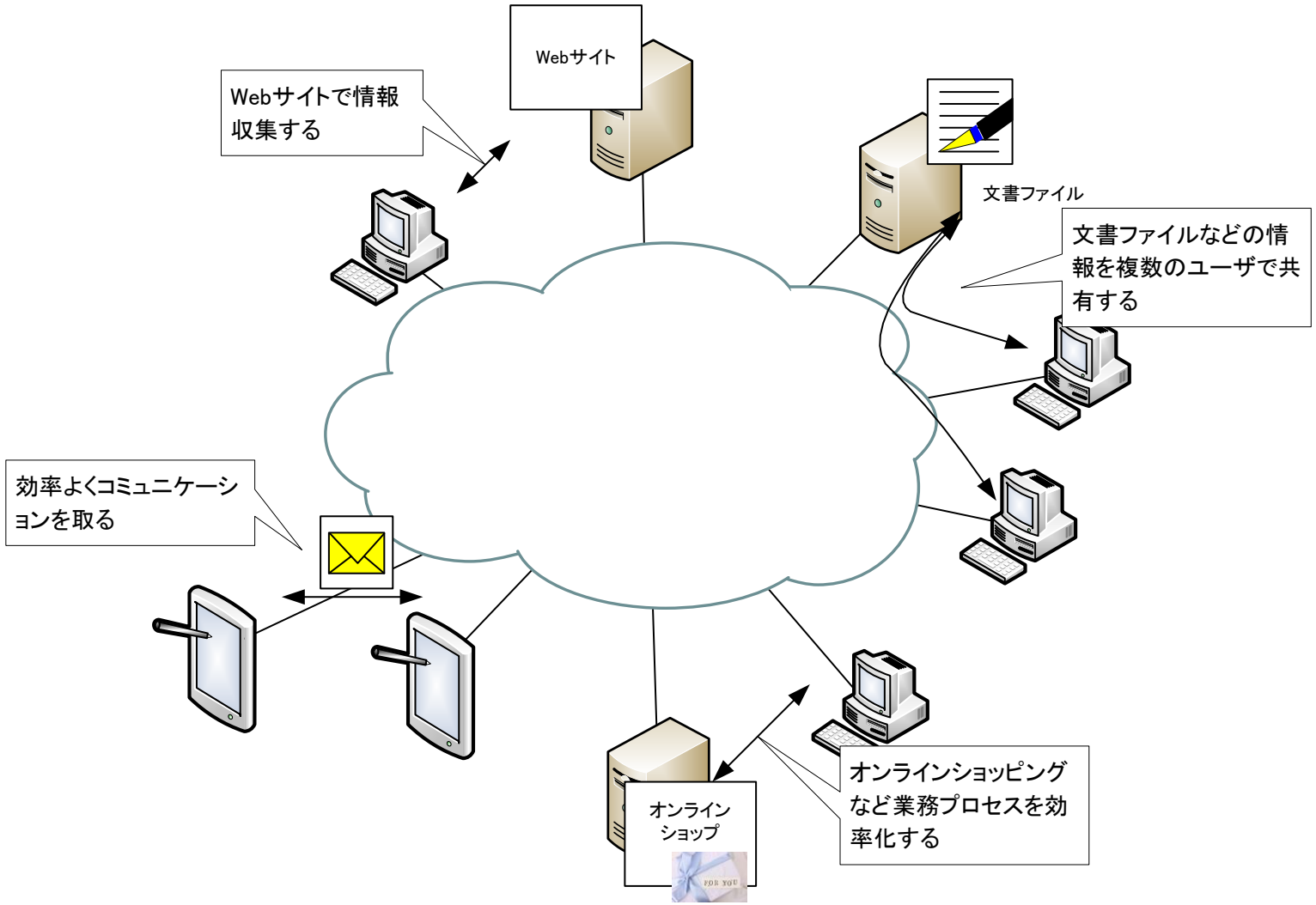
ネットワークの具体的な構成の例



ネットワークを利用する目的

- **データを転送することがネットワークを利用する目的ではない**
- ネットワークを利用する主な目的
  - いろんなメリットを享受するためにネットワークを介してデータを転送する
  - 情報収集
  - 情報共有
  - 効率的なコミュニケーション
  - 業務プロセスの効率化

ネットワークを利用する目的



アプリケーションが通信の主体

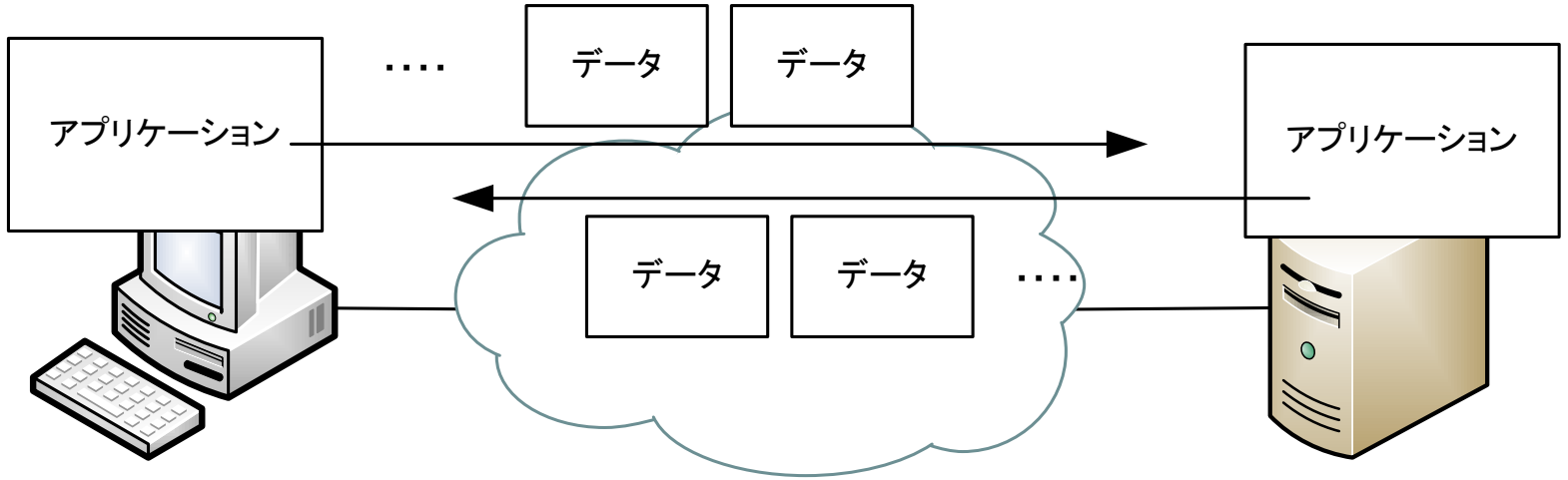
- ネットワークの目的のためにいろんなアプリケーションを利用している
  - 一番よく利用するアプリケーションがWebブラウザ
    - Google Chrome/Microsoft Edge/Apple Safariなど
- **データを送受信するのはアプリケーションがメイン**
  - **ネットワークに送り出すデータを作っているのはアプリケーション**

ネットワーク上の通信のポイント

- 通信の主体はアプリケーション
  - データは複数に分割して連続して転送される
  - アプリケーションの一連のデータのまとまり = フロー
- 通信は双方向
  - クライアントアプリケーションからサーバアプリケーションへリクエスト
  - サーバアプリケーションからクライアントアプリケーションへリプライ(レスポンス)

ネットワーク上の通信のポイント

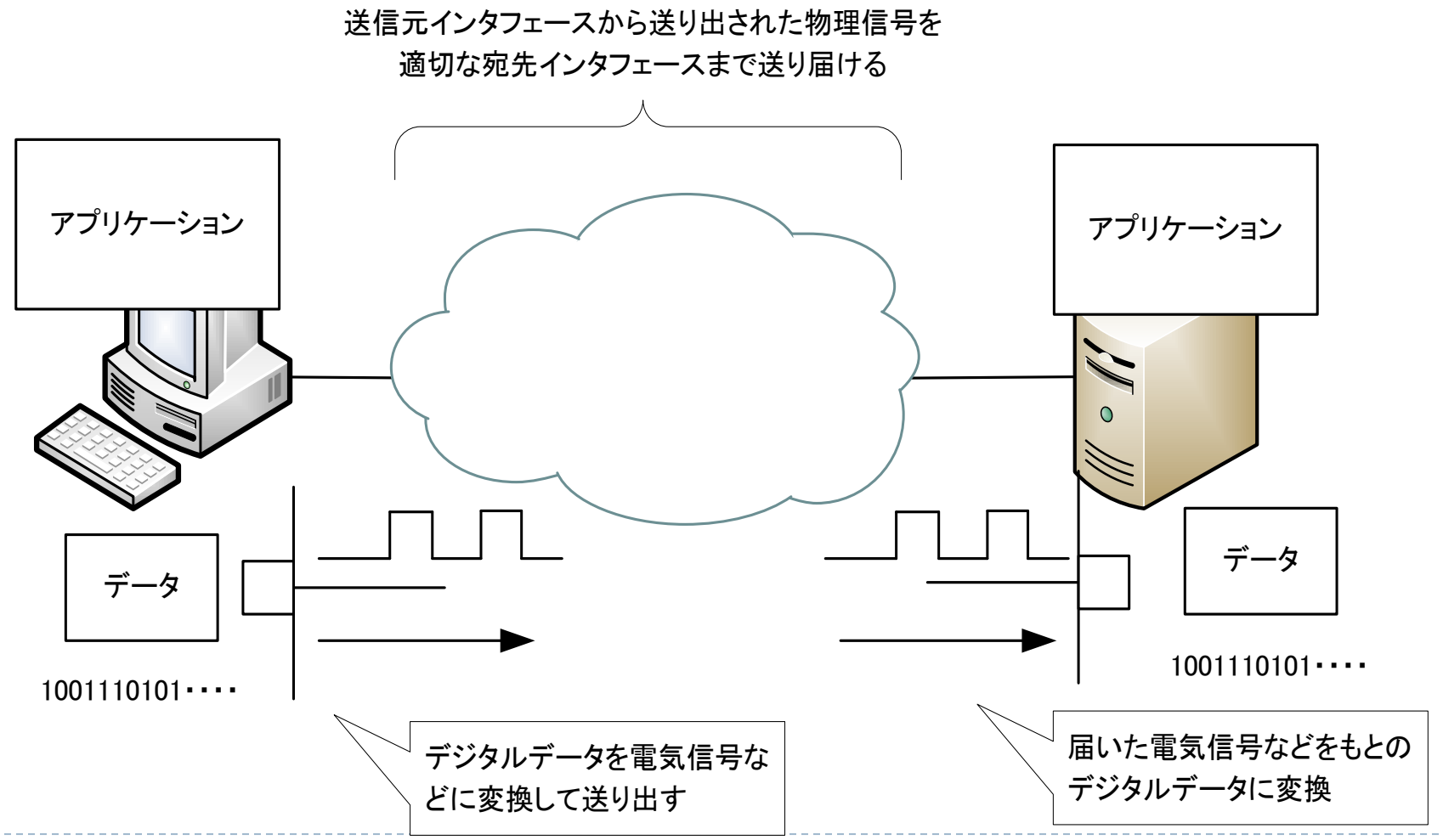
- データを送受信する主体はほとんどの場合、アプリケーション
- 通信は原則として双方向で行うので何かデータを送ったら、返事が返ってくる



ネットワーク上のデータの転送

- PC/サーバなどの内部でのデータは「0」「1」のデジタルデータ
- 送信元機器からデータを送り出すときに電気信号などの物理的な信号に変換
  - デジタルデータと物理信号の境界がインタフェース
- ネットワーク上のデータの転送
  - 送信元機器のインタフェースから送り出された物理信号を適切な宛先機器のインタフェースまで送り届ける
    - 私のPCのインタフェースから送り出された電気信号を他のどこでもないあなたのPCのインタフェースまで送り届ける
      - そのために、データにはいろんな制御情報(ヘッダ)を付加する
  - このようなネットワーク上のデータの転送そのものを実現する基盤
    - ネットワークインフラストラクチャ(ネットワークインフラ)

ネットワーク上のデータの転送



ネットワークインフラを構築するための技術

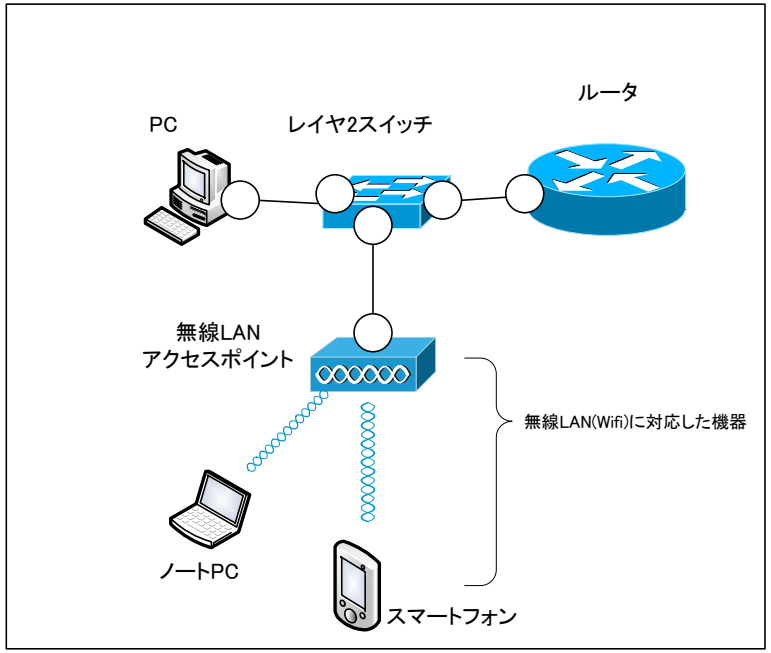
- 企業の社内ネットワークや家庭内ネットワークでよく利用する技術
  - イーサネット、無線LAN(Wi-Fi)
  - 社内ネットワークと家庭内ネットワークは規模が違うだけで、利用している技術は同じ
- ネットワークインフラを構築
  - イーサネットに対応している機器のインタフェース同士をイーサネットに対応しているケーブル(LANケーブル)で接続していく

ネットワークインフラの例

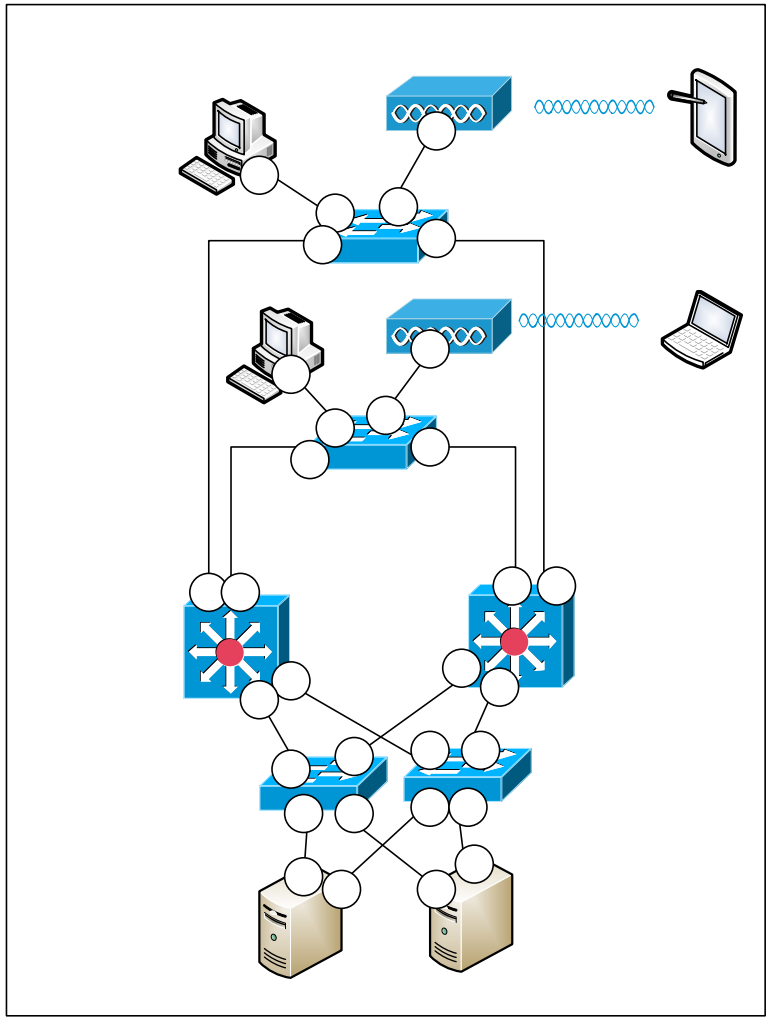
イーサネットに対応したケーブル(LANケーブル)

イーサネットに対応したインタフェース(LANポート)

家庭内のネットワークインフラストラクチャ



社内のネットワークインフラストラクチャ



家庭内でも企業の社内でもネットワークインフラストラクチャは、主にイーサネット、無線LANに対応した機器で構築する

ネットワークの分類

～誰に利用させるネットワーク？～

ネットワークの分類の観点

- いろんな観点でネットワークを分類できる
- **「誰に利用させるネットワークなのか」**
  - 一番重要なネットワークの分類の観点
  - プライベートネットワーク(クローズドネットワーク)
    - 限られたユーザにしか利用させないネットワーク
    - ユーザ数はあまり多くはならない
  - インターネット(オープンネットワーク)
    - 利用するユーザを限定できない = どんなユーザが利用しているかわからない
      - 悪意を持つクラッカーもインターネットを利用している
    - ユーザ数が膨大(2019年現在 約43.8億人)
      - https://wearesocial.com/global-digital-report-2019

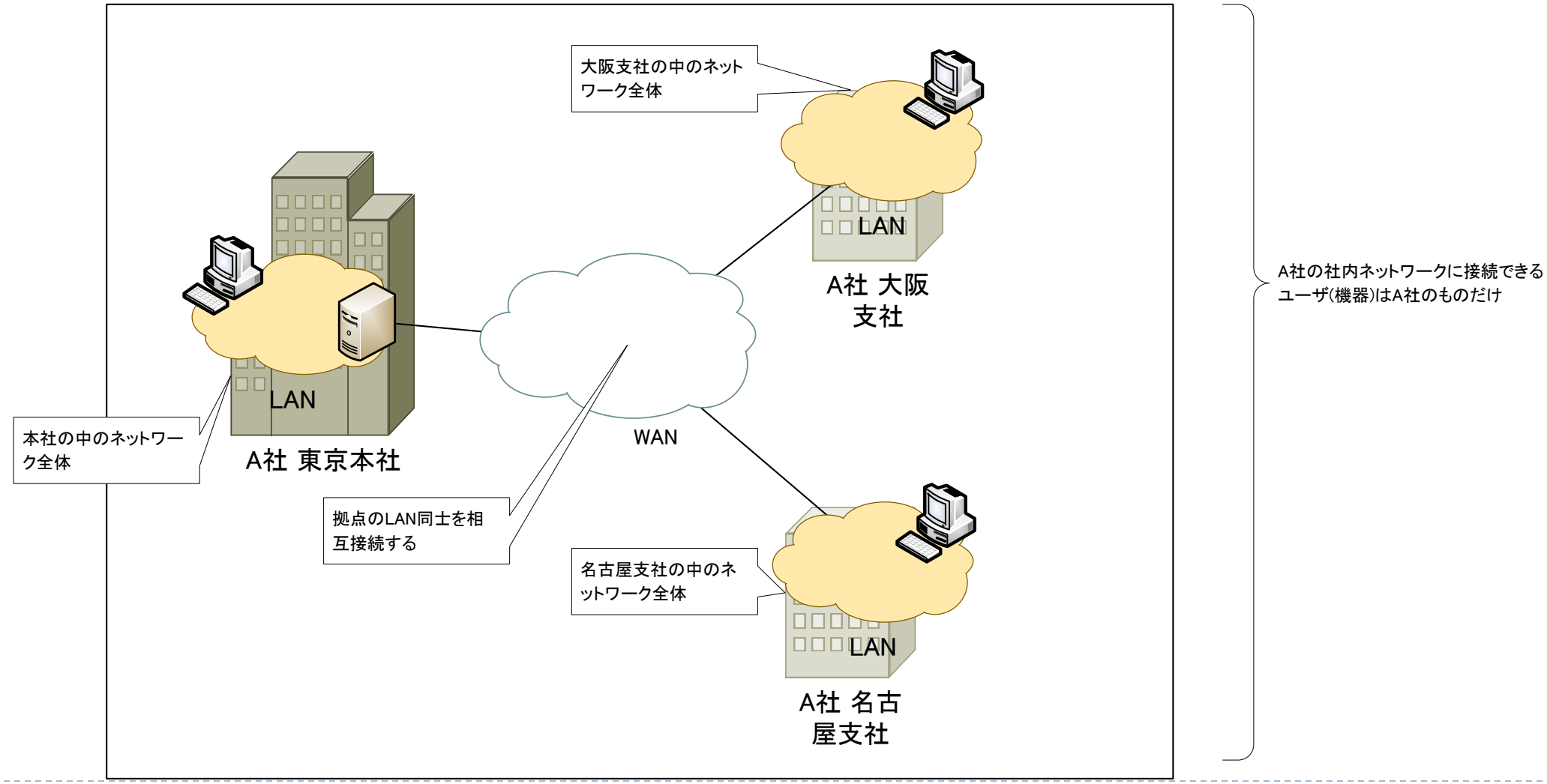
プライベートネットワーク

- 限られたユーザにしか利用させないネットワーク
  - 企業の社内ネットワーク
    - 企業の社員や一時的にオフィスに訪問するゲストのみが利用するネットワーク
  - 家庭内ネットワーク
    - 家族や一時的なゲストのみが利用するネットワーク
- プライベートネットワークのセキュリティ対策のポイント
  - 限られたユーザにしか利用させないような対策を行うことがまず第一歩
    - ネットワーク接続時の認証など

企業の社内ネットワーク

- LAN(Local Area Network)とWAN(Wide Area Network)で構成する
  - イントラネット(Intranet)とも呼ぶ
    - 20年ぐらい前によく使っていた言葉。最近はあんまり見かけない。
  - LAN:ある拠点内のネットワーク全体
    - 原則として、自前で構築・運用管理を行う
    - LAN内の通信には料金は発生しない
  - WAN:拠点同士のネットワークを接続する
    - WANは自前で構築・運用管理しない(できない)
      - 通信事業者(キャリア/サービスプロバイダ)のWANサービスを利用する
    - WANを経由する通信を行うには料金が発生する
      - 料金体系はWANサービスによってさまざま

企業の社内ネットワーク



プライベートネットワークだけでは…

- あまりネットワークの利便性がない
  - 同じ会社の社員間しかメールできない
  - 家族の間でしかファイル共有できない
- 「ネットワークの価値は利用するユーザが多くなればなるほど高まる」
- プライベートネットワークをインターネットに接続するとさらに便利に！！
  - ただ、その分、セキュリティリスクが増える

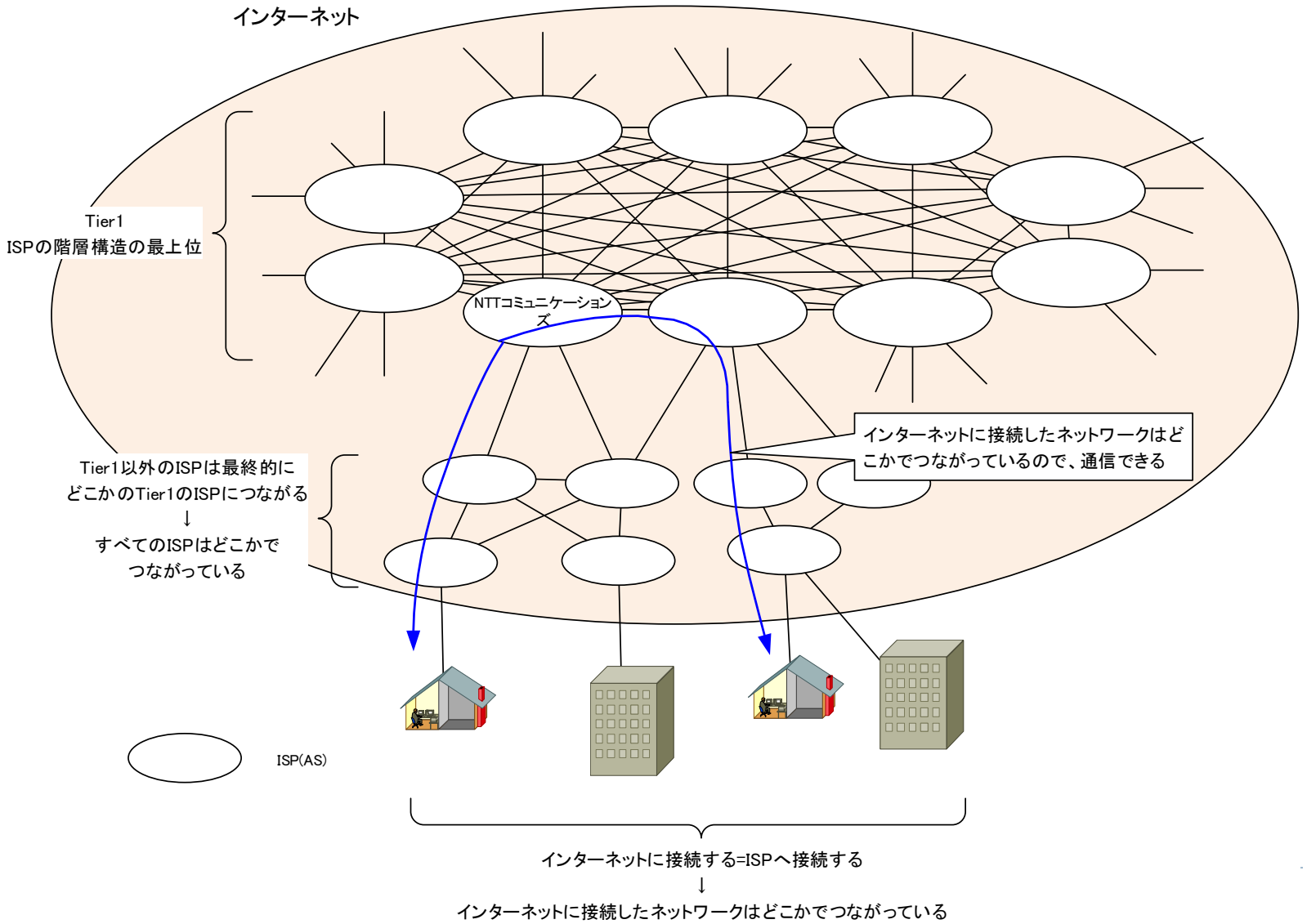
インターネット(オープンネットワーク)

- 世界中のいろんな組織のネットワークが相互接続しているネットワーク
- AS(Autonomous System : 自律システム)
  - インターネットを構成するさまざまな組織のネットワーク
    - それぞれの組織が独自のポリシーに基づいてネットワークを構築・運用管理
  - ASの例
    - ISP(Internet Service Provider)
      - インターネット接続サービスを提供する事業者
        - NTTコム/IIJ/So-net/BIGLOBEなど
      - 携帯キャリアもISP
        - NTTドコモ/au/ソフトバンクなど
    - インターネット上でサービスを提供する企業のネットワーク
      - Google/Amazon/Facebook/Apple/Microsoftなど

「インターネットに接続する」とは

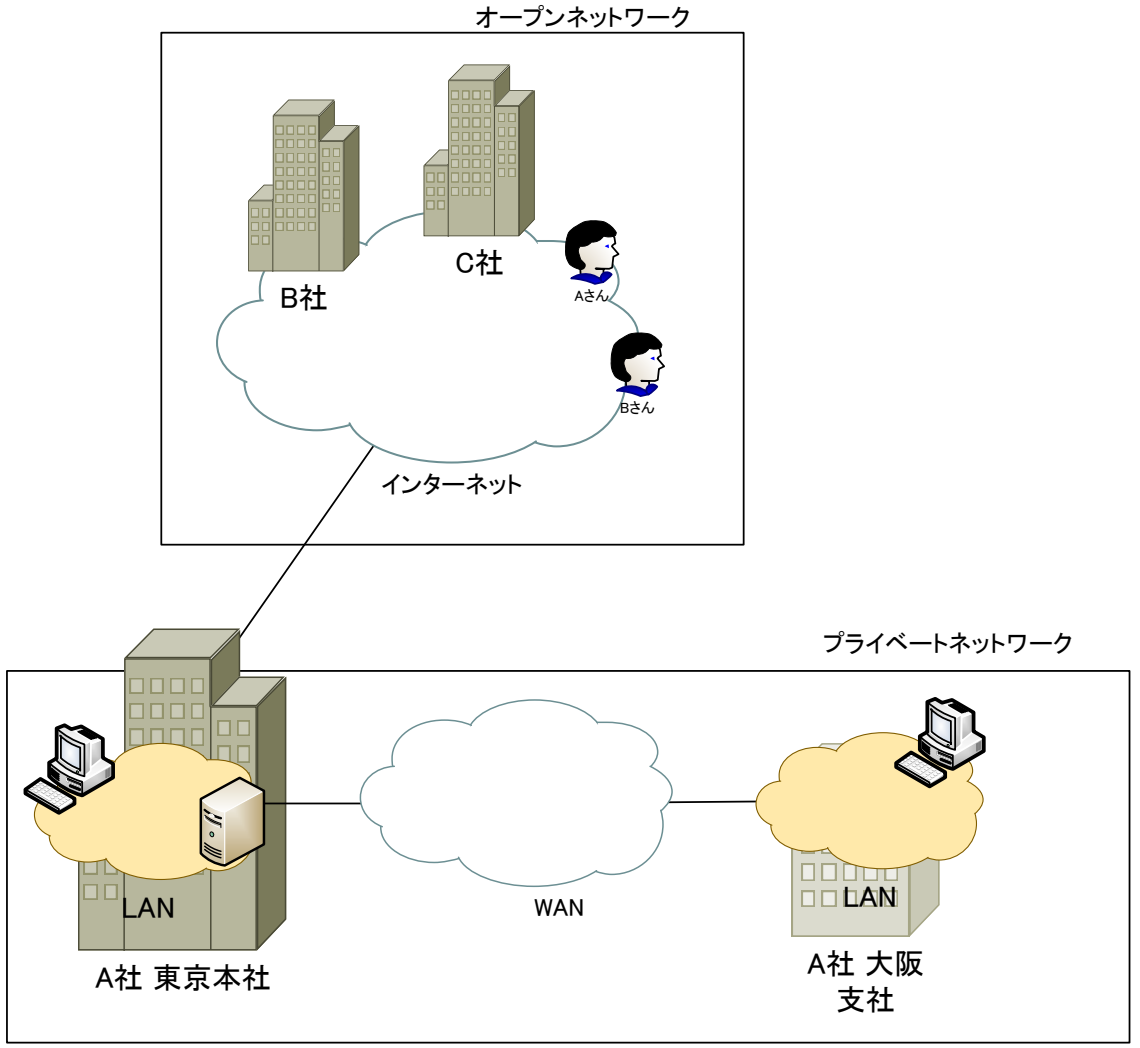
- ISPとインターネット接続サービスを契約して、ISPが運用するネットワークに所属する
  - 契約するISPはどこでもいい
    - 契約したISPは他のISPとどこかでつながっているので、契約したISPのユーザ以外とも通信可能
  - 個人やほとんどの企業のインターネット接続の形態
- すでにインターネット接続しているネットワークに相乗りする
  - 街なかのファストフード店やカフェ、コンビニ、ホテルなどでのインターネット接続
- 独立したASとして他のAS(ISP)と接続する
  - インターネット上でさまざまなサービスを提供するような企業のインターネット接続の形態

インターネットの構成


インターネット
Tier1
ISPの階層構造の最上位
NTTコミュニケーションズ
インターネットに接続したネットワークはどこかでつながっているので、通信できる
Tier1以外のISPは最終的にどこかのTier1のISPにつながる
↓
すべてのISPはどこかでつながっている
ISP(AS)
インターネットに接続する=ISPへ接続する
↓
インターネットに接続したネットワークはどこかでつながっている

インターネット ≠ WAN

- インターネットと企業の拠点間を接続するWANはまったく別物
  - WANの先に接続しているのは、自社の別拠点だけ
    - WANを通じて接続している拠点はあくまでもプライベートネットワーク
      - WANの部分は自社ではない
    - どんなユーザがいるか制御できるし、きちんとわかる
  - インターネットの先に接続しているのは、世界中のインターネットユーザ
    - どんなユーザがつながっているか制御できないし、わからない



用語のまとめ

用語	意味
ネットワーク機器	ルータ/レイヤ2スイッチ/レイヤ3スイッチなどネットワークを構成するための機器。複数のネットワークインタフェースを備えている
リンク	ネットワークのインタフェース同士のつながり
ネットワークインフラストラクチャ	データの転送を実現するための基盤。イーサネットや無線LAN(Wi-Fi)などの技術に対応したネットワーク機器によって作る
プライベートネットワーク	企業の社内ネットワークや個人の家庭内ネットワークなど利用するユーザを限定しているネットワーク。
LAN(Local Area Network)	ある拠点のネットワーク全体
WAN(Wide Area Network)	LAN同士を相互接続するためのネットワーク。通信事業者のWANサービスを利用する
インターネット	世界中のさまざまな組織のネットワークを相互接続して利用するユーザを限定していない(できない)ネットワーク。悪意を持つユーザが存在することを前提として考える

確認テスト Part1

- 以下のURLにここまでの内容を確認するテストを公開しています。
  - https://forms.gle/dDeT1bkAR8yuVYku6

ネットワーク上に送り出されるデータの形

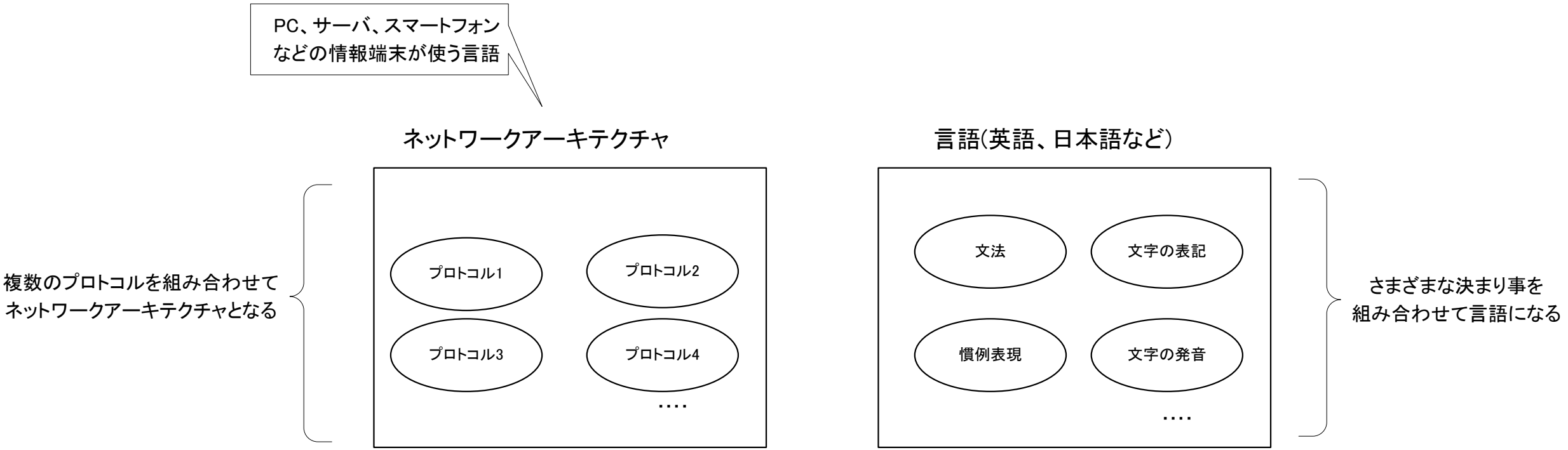
ネットワークアーキテクチャ

プロトコル、ネットワークアーキテクチャ

- ネットワークを介してアプリケーションのデータを送受信するためにはいろんなルールを決める。送信元と宛先で同じルールに基づいて、データを送受信する
- プロトコル
  - 通信するためのルール
- ネットワークアーキテクチャ
  - 複数のルールの組み合わせ
  - 人間が利用する「言語」に相当
  - 「プロトコルスタック」「プロトコルスイート」とも呼ぶ

プロトコル、ネットワークアーキテクチャ

- 現在、事実上の標準として利用しているネットワークアーキテクチャがTCP/IP



プロトコルの制御

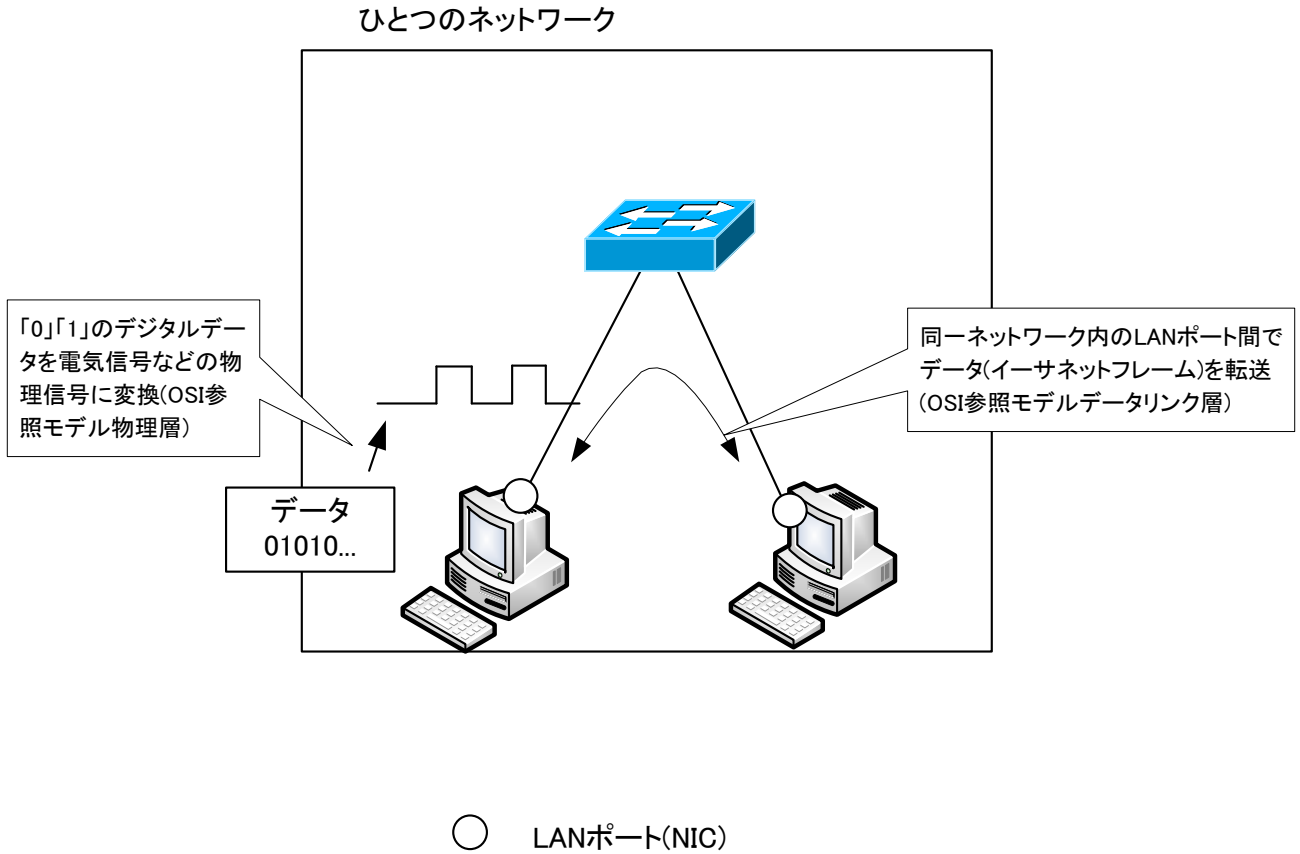
- アプリケーションのデータを正しく送り届けるためには、複数のプロトコルを組み合わせる
  - 各プロトコルで制御するための制御情報(ヘッダ)
  - データの送信側:アプリケーションのデータにいろんなヘッダを付加していく(カプセル化)
  - データの受信側:ヘッダを解釈して、ヘッダを外したあと他のプロトコルの処理を継続(逆カプセル化)

TCP/IPの階層

- ネットワークアーキテクチャは階層化して複数のプロトコルを組み合わせる
  - 階層ごとにデータを転送する上で必要な機能をわけて考える
- TCP/IP 4階層
  - アプリケーション層
  - トランスポート層
  - インターネット層
  - ネットワークインタフェース層

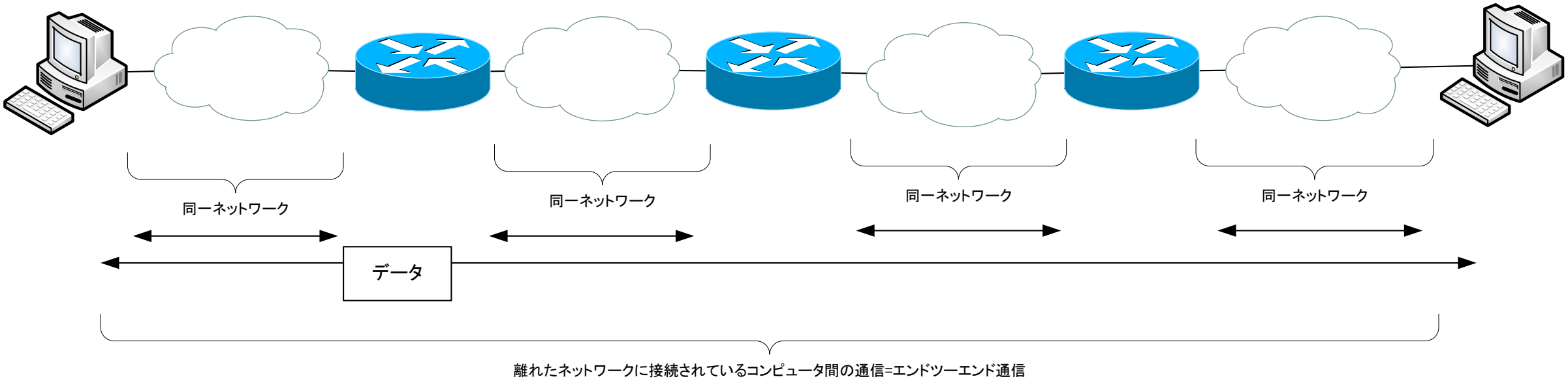
ネットワークインタフェース層

- データを物理的な信号に変換して伝える
- 同一ネットワーク内のデータの転送を行う



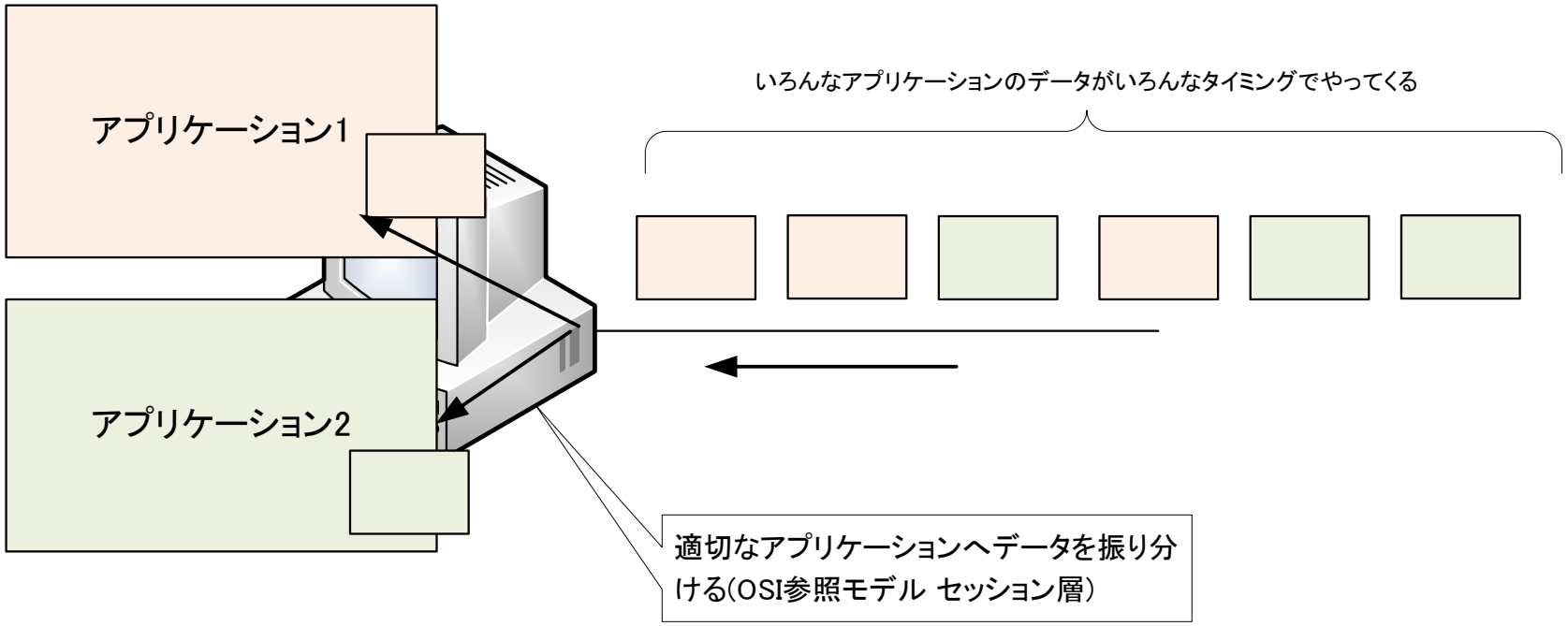
インターネット層

- 異なるネットワーク間のデータの転送を行う
  - エンドツーエンド通信



トランスポート層

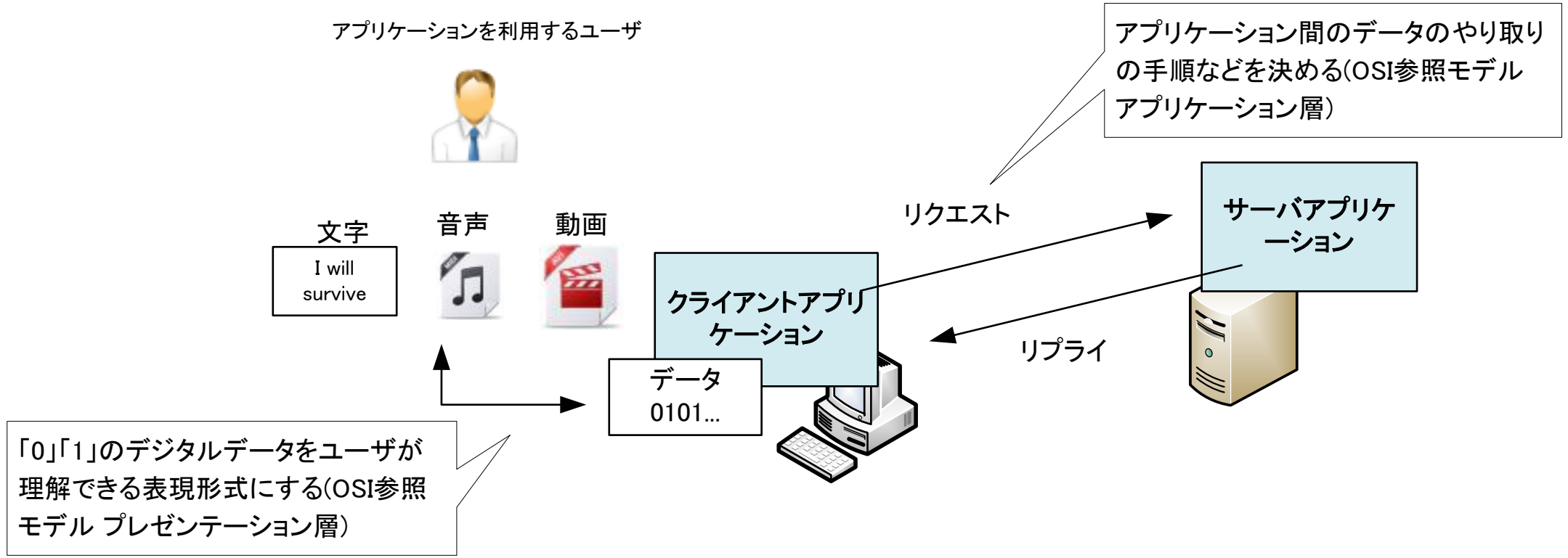
- エンドツーエンド通信の信頼性を確保する(TCP)
- アプリケーションへデータを振り分ける(TCP/UDP)



※ TCPの場合、データの分割と組み立て、データの再送制御、データの順序制御などの機能も利用できる(OSI参照モデル トランスポート層)

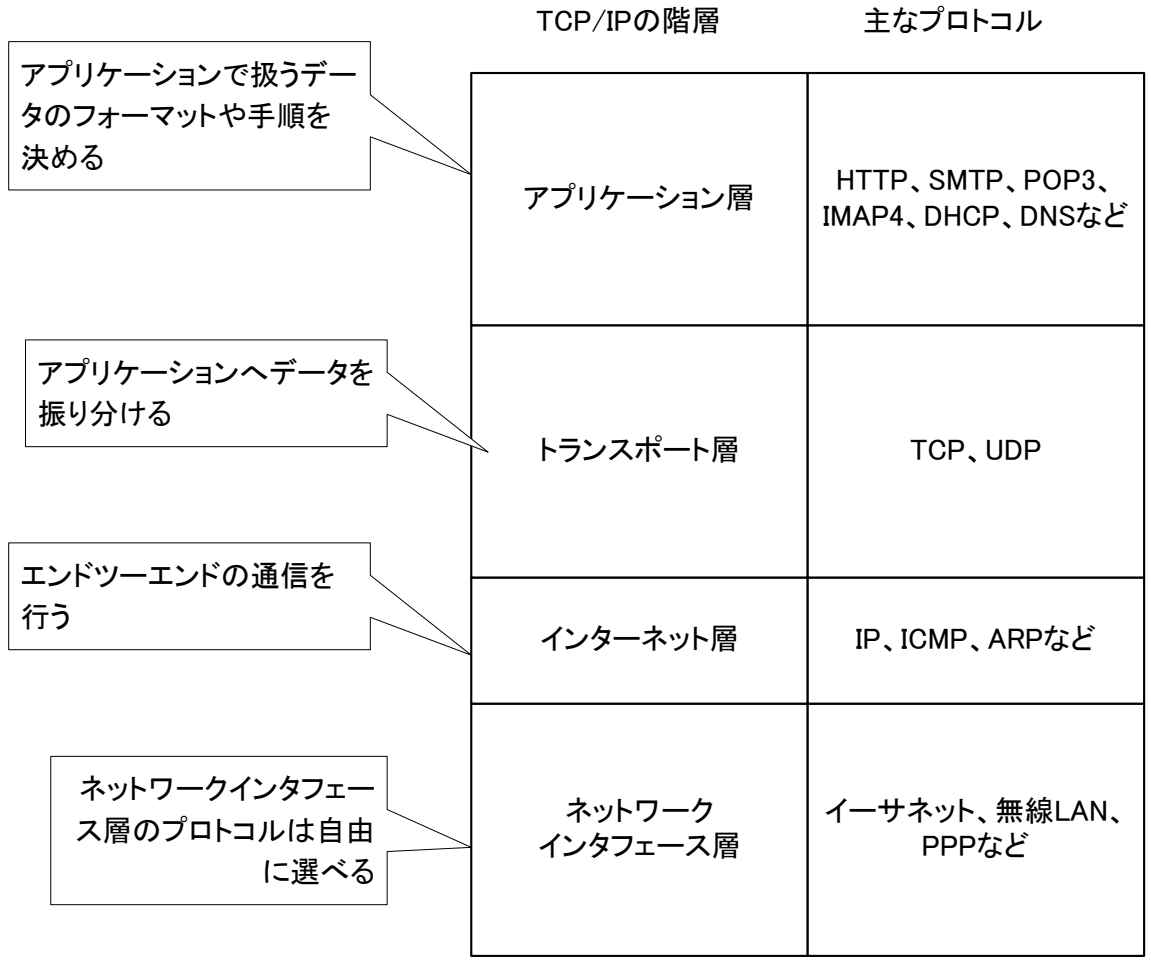
アプリケーション層

- データの表現形式を一致させる
- アプリケーション固有の機能を実現する

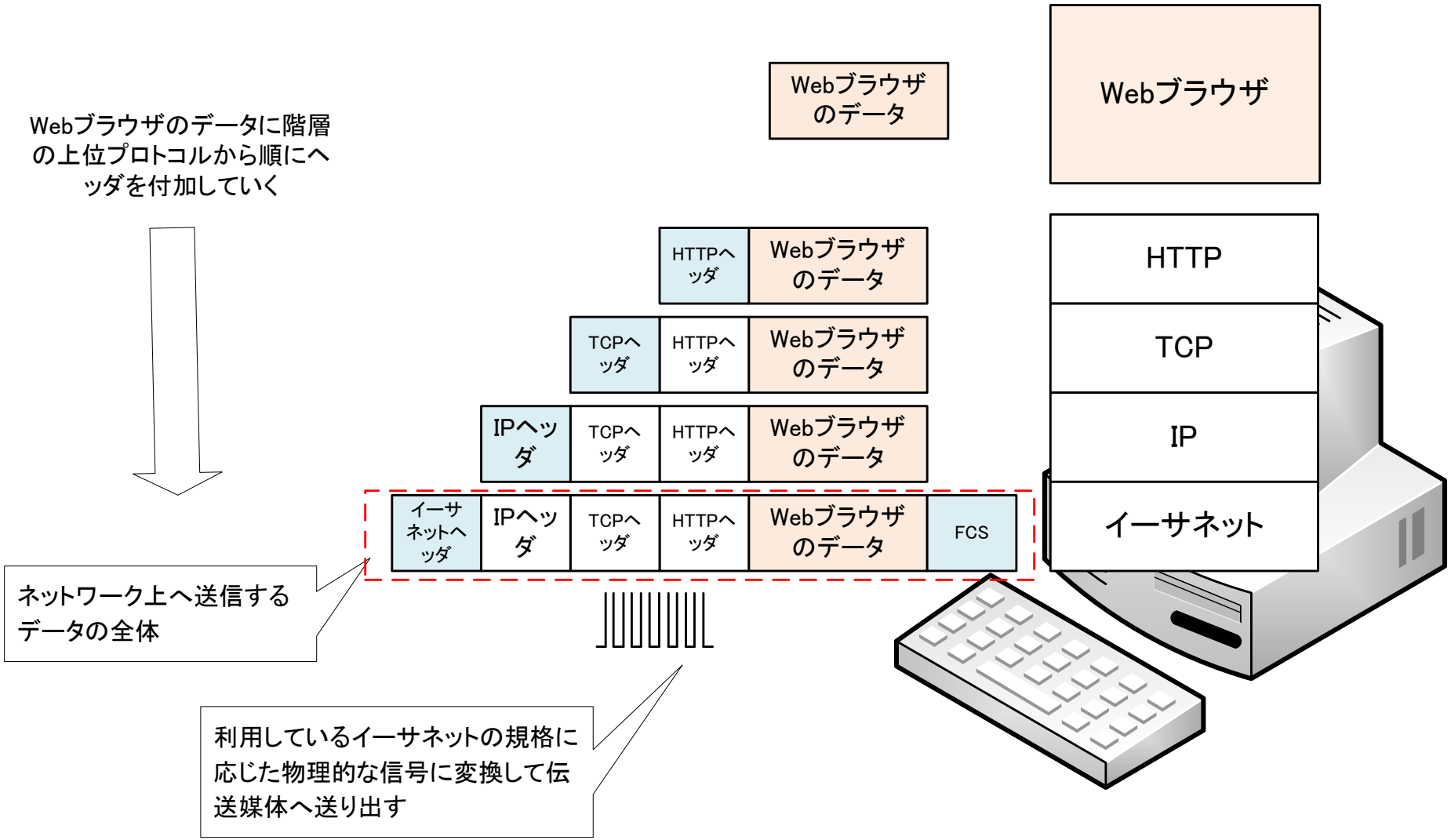


TCP/IPの階層

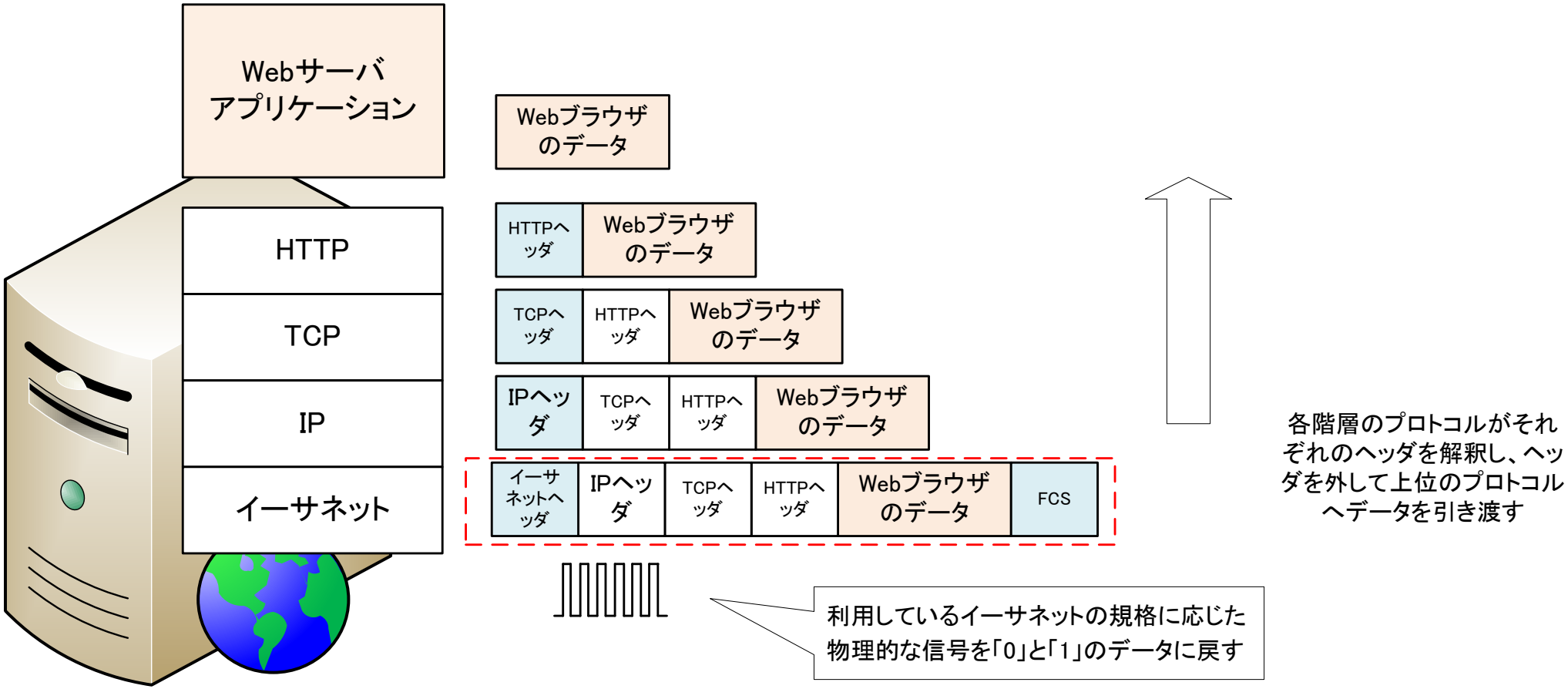
- ネットワークインタフェース層のプロトコルで、同じネットワーク内でデータを転送
  - 物理的な信号に変換して送り届ける
  - 何を使ってもいいけど、イーサネット、無線LANがメイン
  - MACアドレス
- アプリケーションのデータをIPで宛先まで送り届ける
  - IPアドレス
- 届いたアプリケーションのデータをTCP/UDPで適切なアプリケーションに振り分ける
  - ポート番号



Webアクセス(送信側)


Webブラウザのデータに階層の上位プロトコルから順にヘッダを付加していく
Webブラウザのデータ
Webブラウザ
HTTPヘッダ
Webブラウザのデータ
TCPヘッダ
HTTPヘッダ
Webブラウザのデータ
IPヘッダ
TCPヘッダ
HTTPヘッダ
Webブラウザのデータ
イーサネットヘッダ
IPヘッダ
TCPヘッダ
HTTPヘッダ
Webブラウザのデータ
FCS
HTTP
TCP
IP
イーサネット
ネットワーク上へ送信するデータの全体
利用しているイーサネットの規格に応じた物理的な信号に変換して伝送媒体へ送り出す

Webアクセス(受信側)

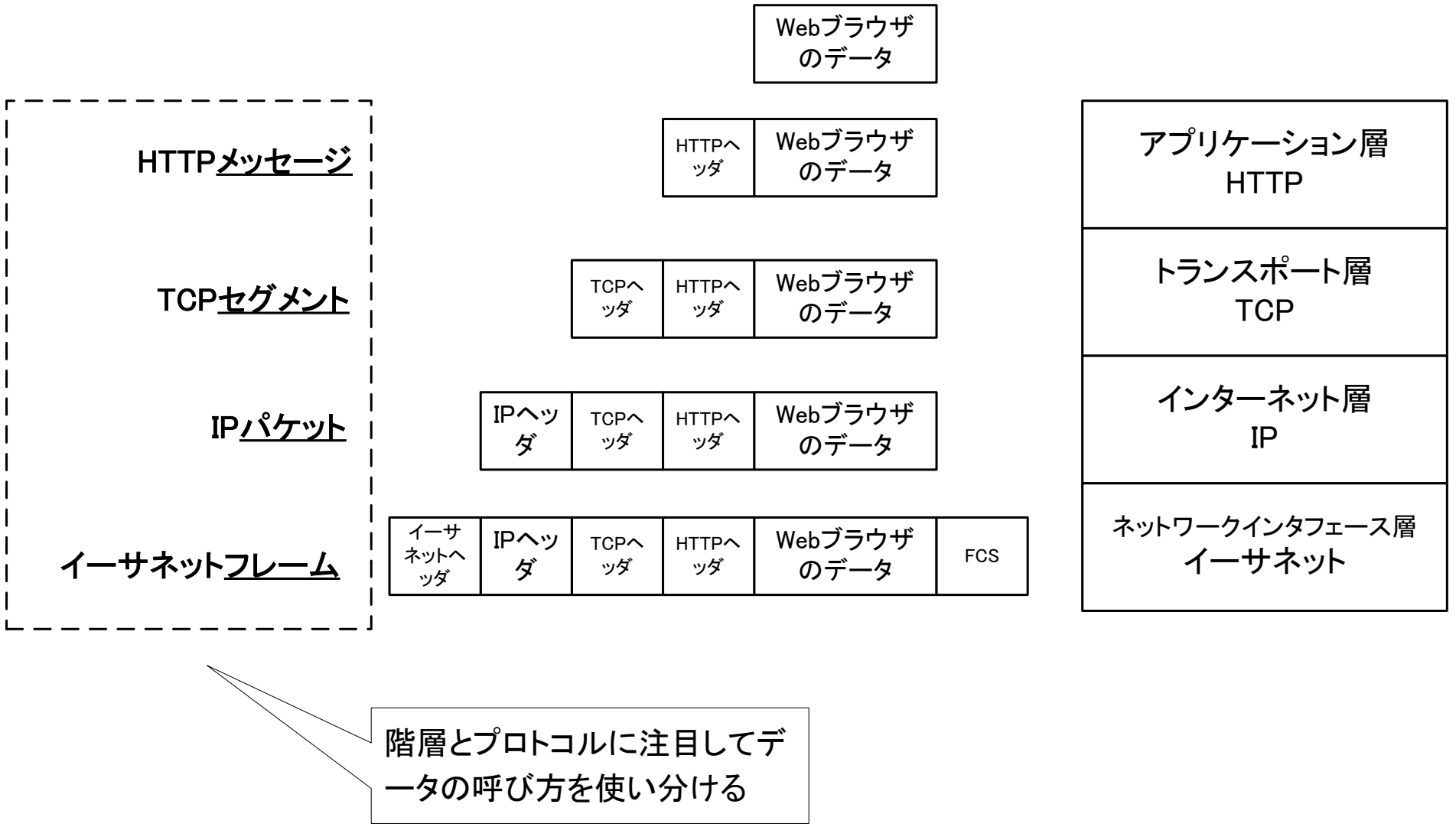

Webサーバ
アプリケーション
HTTP
TCP
IP
イーサネット
Webブラウザのデータ
HTTPヘッダ
Webブラウザのデータ
TCPヘッダ
HTTPヘッダ
Webブラウザのデータ
IPヘッダ
TCPヘッダ
HTTPヘッダ
Webブラウザのデータ
イーサネットヘッダ
IPヘッダ
TCPヘッダ
HTTPヘッダ
Webブラウザのデータ
FCS
各階層のプロトコルがそれぞれのヘッダを解釈し、ヘッダを外して上位のプロトコルへデータを引き渡す
利用しているイーサネットの規格に応じた物理的な信号を「0」と「1」のデータに戻す

データの呼び方

- どの階層に注目しているかによって、データの呼び方が変わることがある
  - アプリケーション層:メッセージ
  - トランスポート層:セグメントまたはデータグラム
  - インターネット層:パケットまたはデータグラム
  - ネットワークインタフェース層:フレーム

- でも、厳密にきちんと呼び方を使い分けているわけではない

データの呼び方


HTTPメッセージ
TCPセグメント
IPパケット
イーサネットフレーム
Webブラウザのデータ
HTTPヘッダ
TCPヘッダ
IPヘッダ
イーサネットヘッダ
FCS
アプリケーション層
HTTP
トランスポート層
TCP
インターネット層
IP
ネットワークインタフェース層
イーサネット
階層とプロトコルに注目してデータの呼び方を使い分ける

用語のまとめ

用語	意味
プロトコル	ネットワーク上で通信を行うための決まりごと。さまざまな役割を持つプロトコルが存在する
ネットワークアーキテクチャ	通信をするために必要なプロトコルをまとめているもの。人間が利用する言語に相当する
TCP/IP	現在主流のネットワークアーキテクチャ。ほぼすべての通信はTCP/IPに基づいて行われていて、いわば、ネットワークの共通言語。
ヘッダ	プロトコルの処理を行うための制御情報。ヘッダを付加することをカプセル化と呼ぶ
メッセージ/セグメント/パケット/フレーム	データの呼び方。どの階層に注目しているかによって、データの呼び方を使い分けることがある

確認テスト Part2

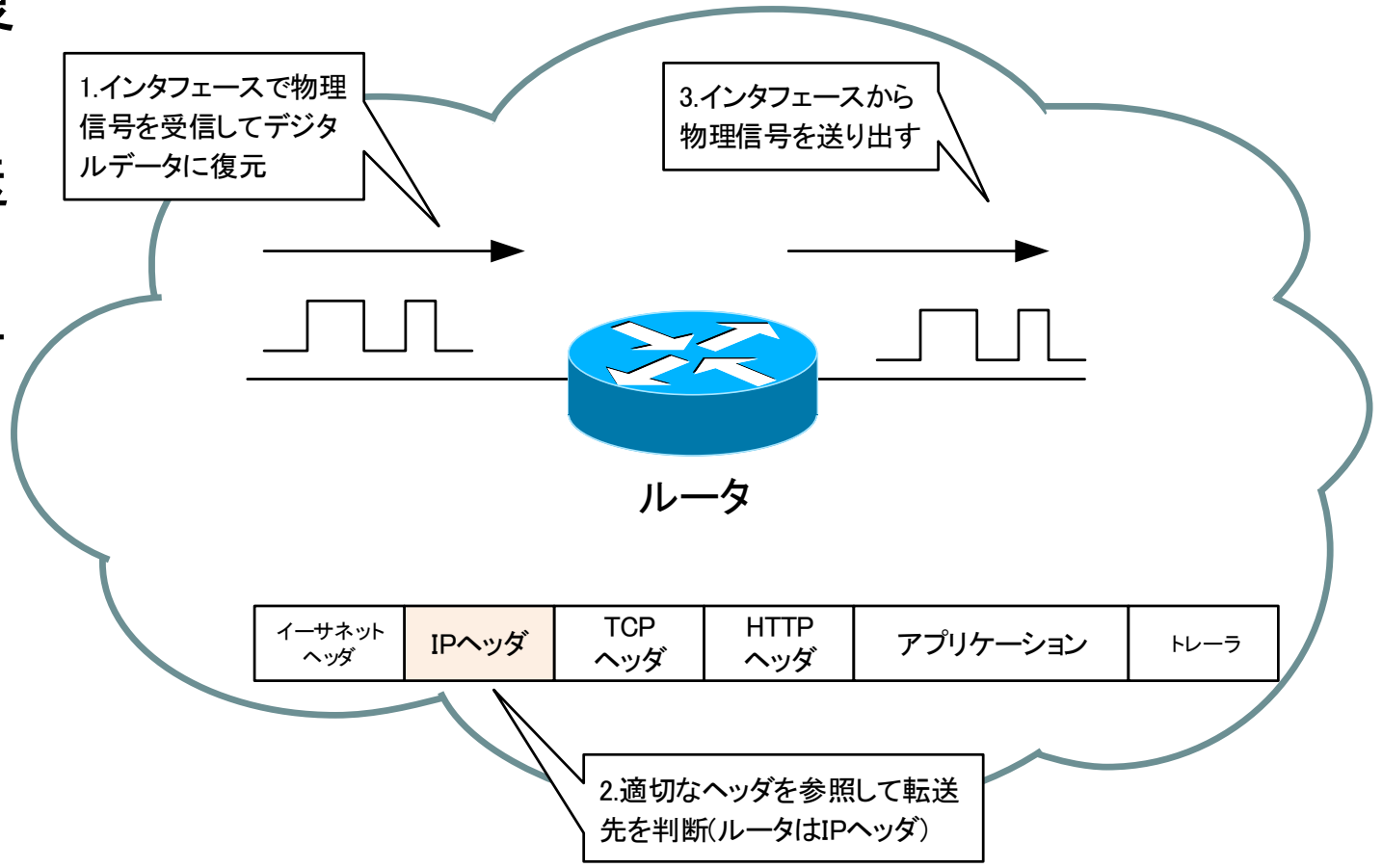
- 以下のURLにここまでの内容を確認するテストを公開しています。
  - https://forms.gle/6NTdXAPW4rsuw1f39

ネットワーク機器のポイント

レイヤ2スイッチ/ルータ/レイヤ3スイッチ

ネットワーク機器の動作

1. インタフェースで物理的な信号を受信してデジタルデータに復元
2. 適切なヘッダを参照して、転送先を判断
3. 出力インタフェースから物理信号を送り出す



ネットワークを構成する主なネットワーク機器

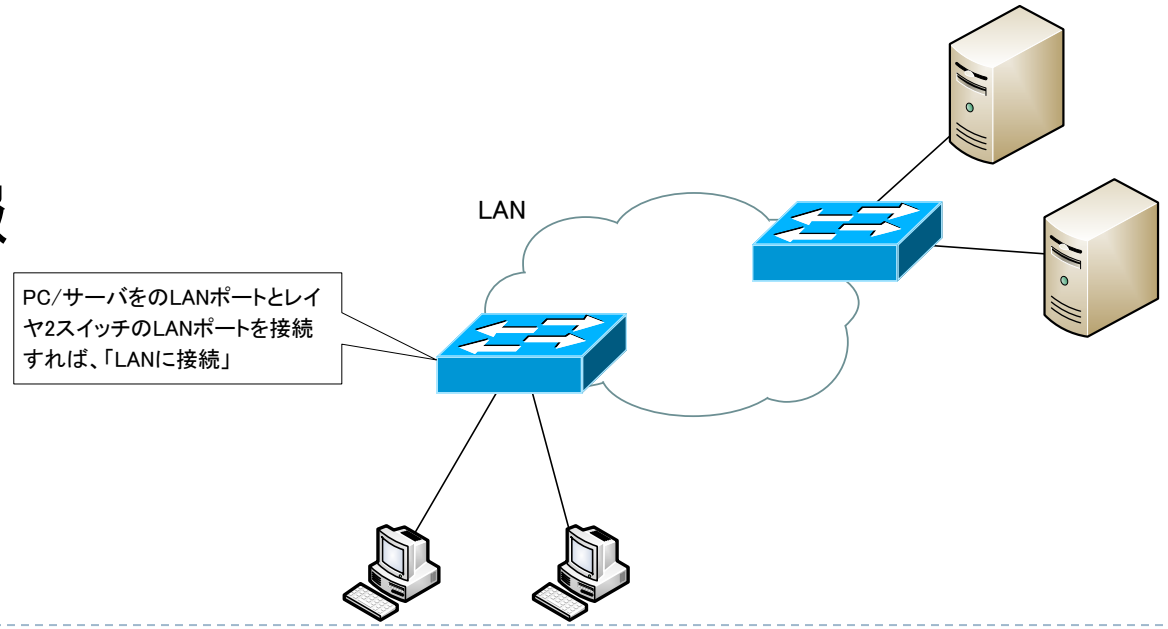
- 企業の社内ネットワーク、家庭内ネットワークを構築するための主なネットワーク機器
  - レイヤ2スイッチ
  - ルータ(ブロードバンドルータ)
  - レイヤ3スイッチ
- それぞれのネットワーク機器の役割や仕組みをしっかりと把握しておくことが重要
  - 役割
  - データの転送範囲
  - データの転送の判断に利用する情報

ネットワーク機器のポイント

種類	データの転送範囲	転送に利用する情報	役割
レイヤ2スイッチ	同じネットワーク内	MACアドレス MACアドレステーブル	「ひとつ」のネットワークを作る ネットワークの入口
ルータ	ネットワーク間	IPアドレス ルーティングテーブル	ネットワークの相互接続
レイヤ3スイッチ	同じネットワーク内 ネットワーク間	MACアドレス MACアドレステーブル IPアドレス ルーティングテーブル	レイヤ2スイッチとルータを兼ね備えた機器

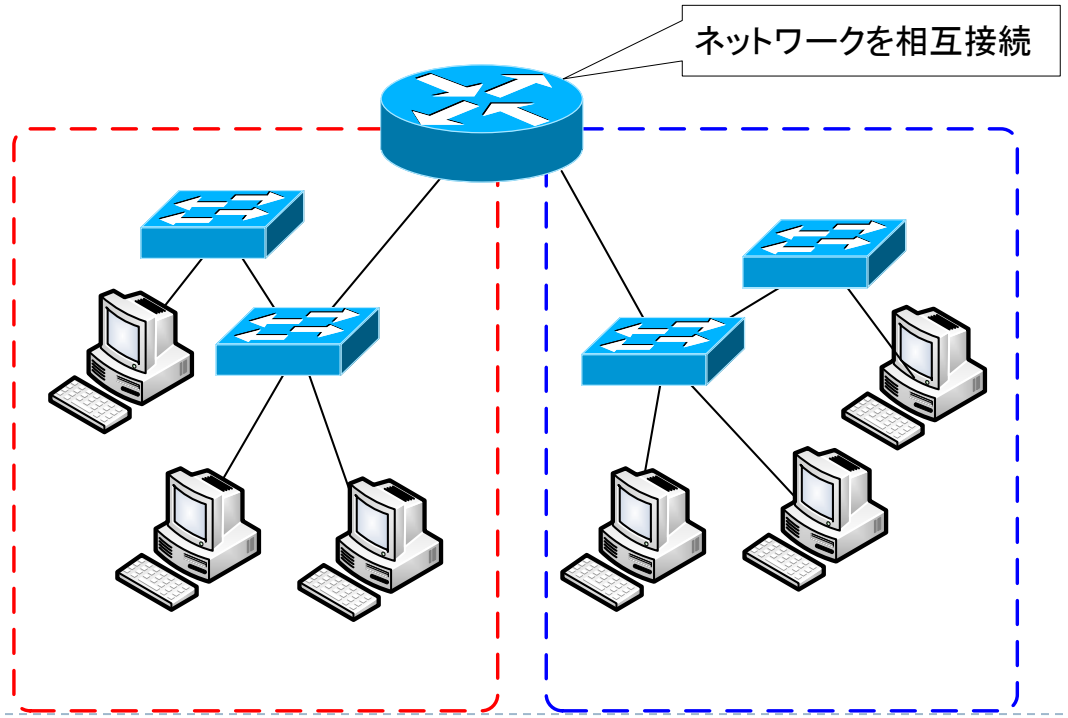
レイヤ2スイッチのポイント

- レイヤ2スイッチの主な役割
  - 「ひとつの」イーサネットのネットワークを構築する
  - ネットワークの入口
    - 社内ネットワークや家庭内ネットワークに接続する→PCなどをレイヤ2スイッチに接続
    - たくさんのイーサネットポートを持っている
- データの転送範囲
  - 同じネットワーク内
- データの転送の判断に利用する情報
  - MACアドレス
  - MACアドレステーブル



「ひとつのネットワーク」

- 技術的に「ひとつのネットワーク」とは？
  - レイヤ2スイッチで「ひとつのイーサネットネットワーク」を作る
    - レイヤ2スイッチを何台接続していても、全体として「ひとつのネットワーク」
  - ルータで区切られる範囲
  - ルータはネットワークの相互接続を行う



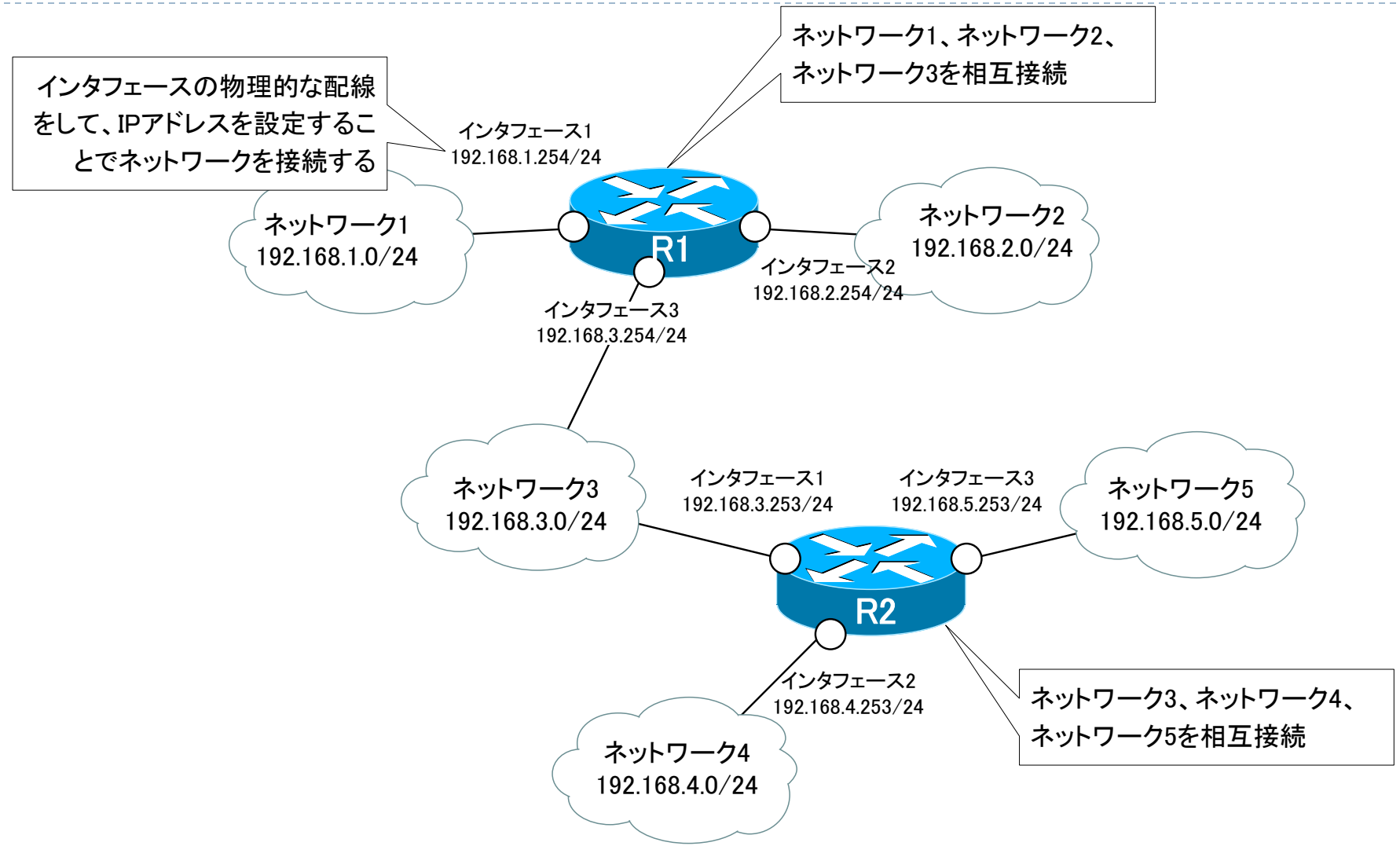
ルータのポイント

- ルータの主な役割
  - ネットワークの相互接続
    - さまざまなネットワークはルータによって相互接続されている
    - ルータがネットワークを分割する(区切る)といってもいい
- データの転送範囲
  - ネットワーク間
    - ルータが直接接続しているネットワークでなくてもいい
  - ルーティング
    - ルータによるネットワーク間のデータの転送
- データの転送の判断に利用する情報
  - IPアドレス
  - ルーティングテーブル

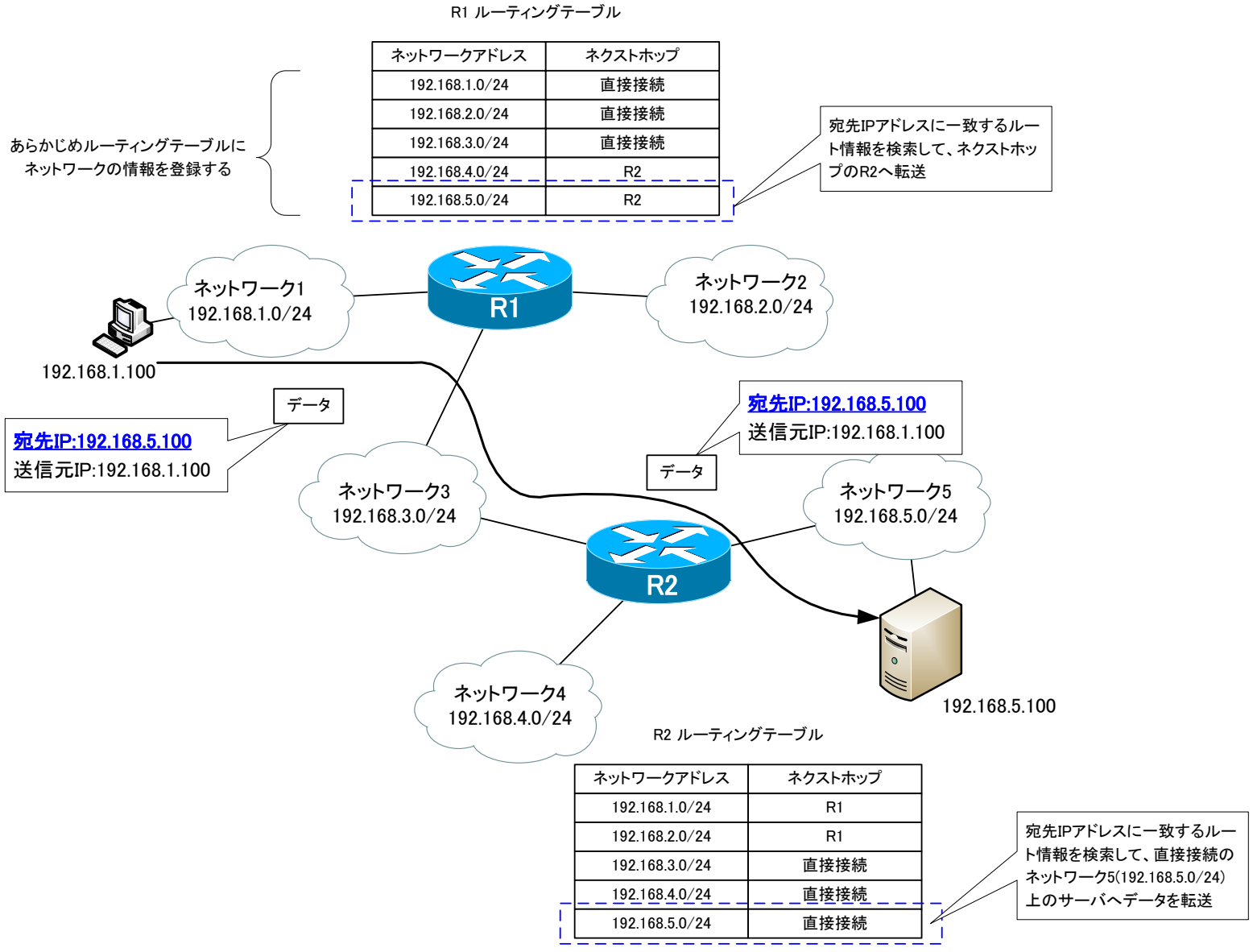
ネットワークに接続する

- 「ネットワークに接続する」とは？
  - 物理的な接続
    - 電気信号、光信号など物理的な信号をやりとりできるようにする
  - 論理的な接続
    - インタフェースにIPアドレスを設定する
- ルータは複数のインタフェースを備えるので、複数のネットワークに接続できる
  - 接続したネットワーク間のデータの転送が可能
  - PCはたいてい1つのインタフェースだけ
    - 複数インタフェースがある場合は、PCでも複数のネットワークに接続可能
    - ただし、ネットワーク間のデータの転送は通常はできない

ルータによるネットワークの相互接続



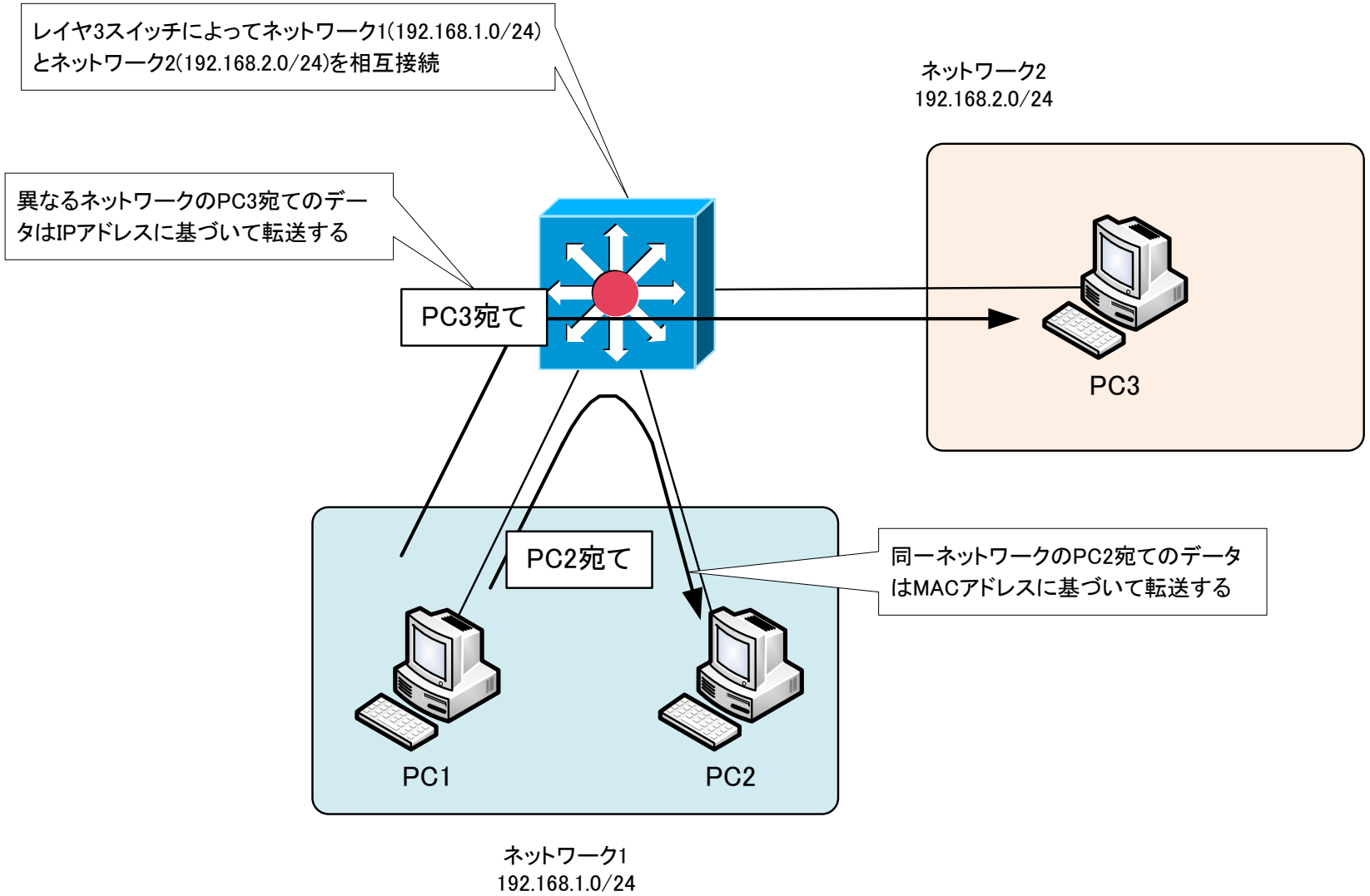
ルーティングの概要


R1 ルーティングテーブル
ネットワークアドレス
ネクストホップ
192.168.1.0/24
直接接続
192.168.2.0/24
直接接続
192.168.3.0/24
直接接続
192.168.4.0/24
R2
192.168.5.0/24
R2
あらかじめルーティングテーブルに
ネットワークの情報を登録する
宛先IPアドレスに一致するルート情報を検索して、ネクストホップのR2へ転送
ネットワーク1
192.168.1.0/24
R1
ネットワーク2
192.168.2.0/24
192.168.1.100
データ
宛先IP:192.168.5.100
送信元IP:192.168.1.100
宛先IP:192.168.5.100
送信元IP:192.168.1.100
データ
ネットワーク3
192.168.3.0/24
ネットワーク5
192.168.5.0/24
R2
192.168.5.100
ネットワーク4
192.168.4.0/24
R2 ルーティングテーブル
ネットワークアドレス
ネクストホップ
192.168.1.0/24
R1
192.168.2.0/24
R1
192.168.3.0/24
直接接続
192.168.4.0/24
直接接続
192.168.5.0/24
直接接続
宛先IPアドレスに一致するルート情報を検索して、直接接続のネットワーク5(192.168.5.0/24)上のサーバへデータを転送

レイヤ3スイッチのポイント

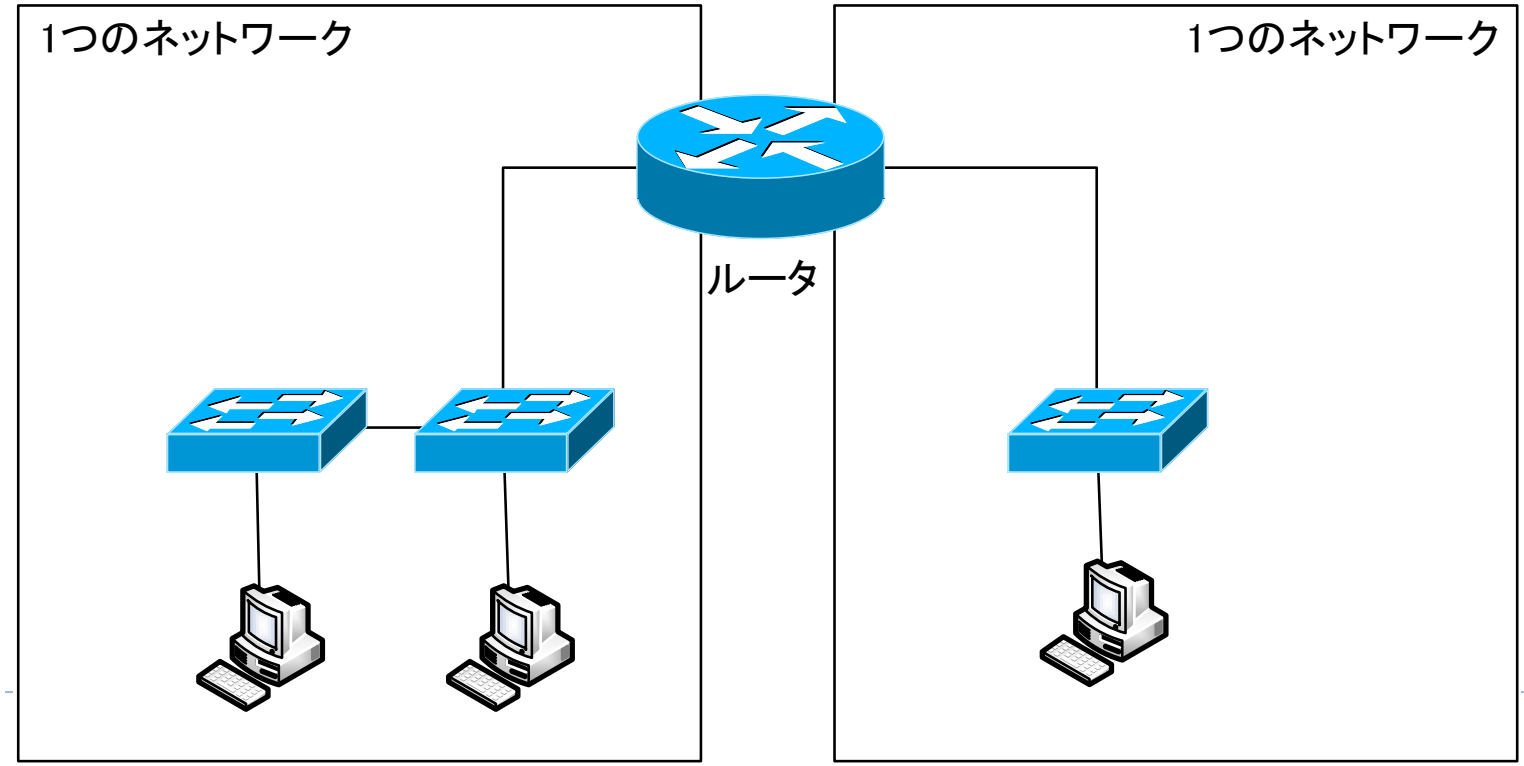
- レイヤ3スイッチの主な役割
  - ほとんどルータと同じように利用する
  - ネットワーク(VLAN)の相互接続
  - ネットワーク(VLAN)間の高速なデータの転送
- データの転送範囲
  - ネットワーク内
  - ネットワーク間
- データの転送の判断に利用する情報
  - MACアドレス
  - MACアドレステーブル
  - IPアドレス
  - ルーティングテーブル

レイヤ3スイッチのポイント



ルータ/レイヤ2スイッチのポイントまとめ

- レイヤ2スイッチは、「ひとつの」イーサネットのネットワークを作り、ネットワーク内のデータ転送を行う
- ルータは、ネットワークを相互接続して、ネットワーク間のデータ転送を行う



用語のまとめ

用語	意味
レイヤ2スイッチ	1つのネットワークを構成するためのネットワーク機器。同一ネットワーク内でのデータ転送を行う
ルータ	複数のネットワークを相互接続して、ネットワーク間のデータ転送を行うためのネットワーク機器。
レイヤ3スイッチ	レイヤ2スイッチにルータの機能を組み込んだネットワーク機器。多くの場合、ルータと同じように利用する

確認テスト Part3

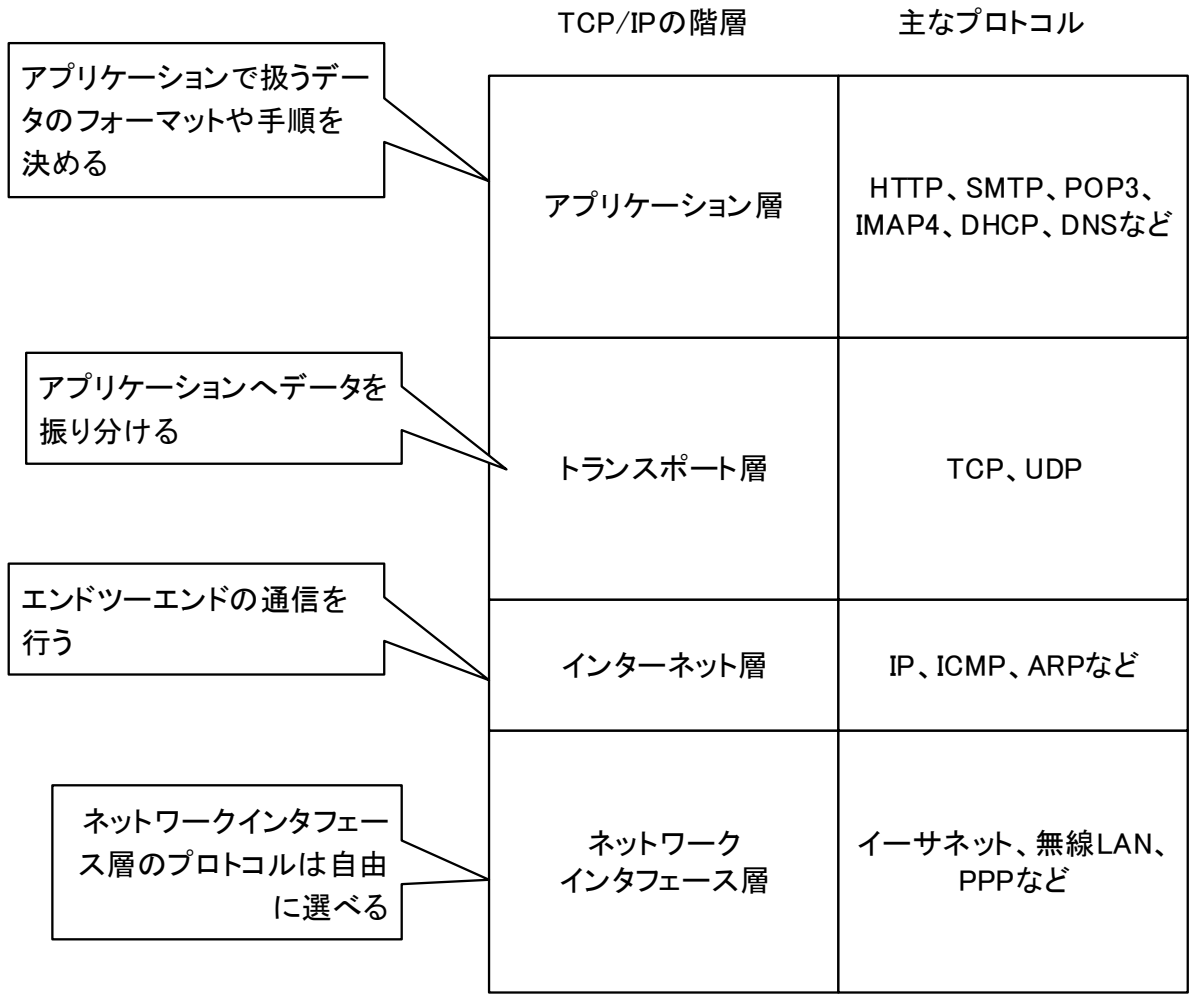
- 以下のURLにここまでの内容を確認するテストを公開しています。
  - https://forms.gle/uz1qv4uPvuJ9hDKb8

TCP/IPの概要

ネットワークの共通言語

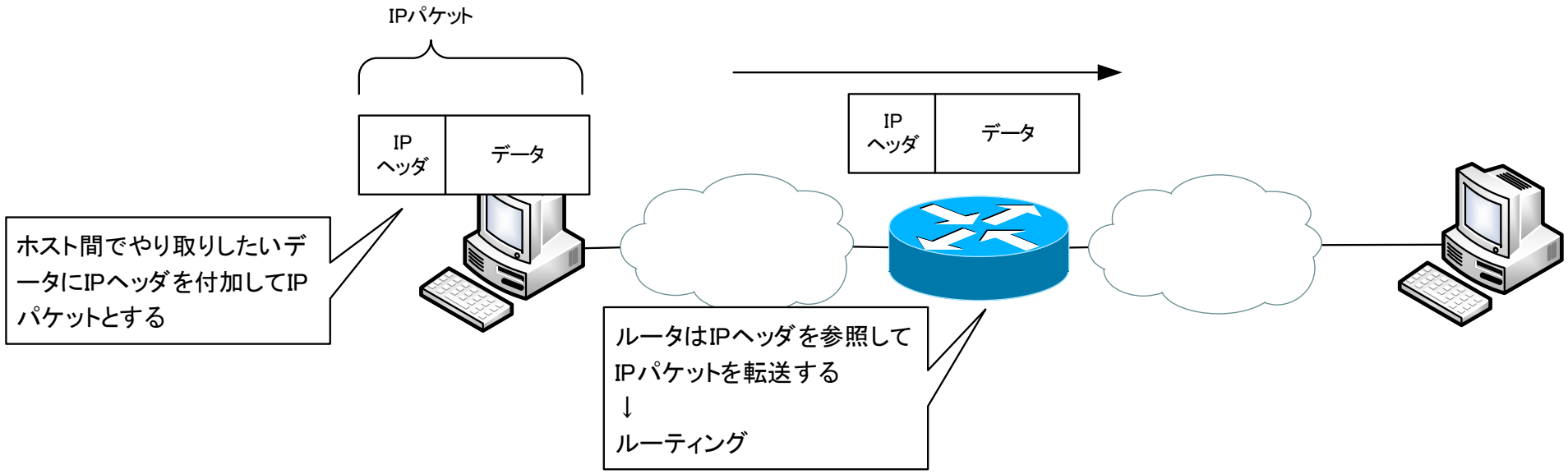
TCP/IPの階層と主なプロトコル

- TCP/IPのプロトコルはインターネット層より上の階層に位置するプロトコル
  - ネットワークインタフェース層は何を使ってもいい
    - 有線イーサネットでもWi-Fiでも、4G/5GでもOK
- 特に重要なプロトコル
  - IP
    - 宛先のホストまでデータを送る
  - TCP/UDP
    - データを適切なアプリケーションへ振り分ける
  - DNS
    - 宛先IPアドレスを求める
  - HTTP
    - Webブラウザで主に利用するプロトコル

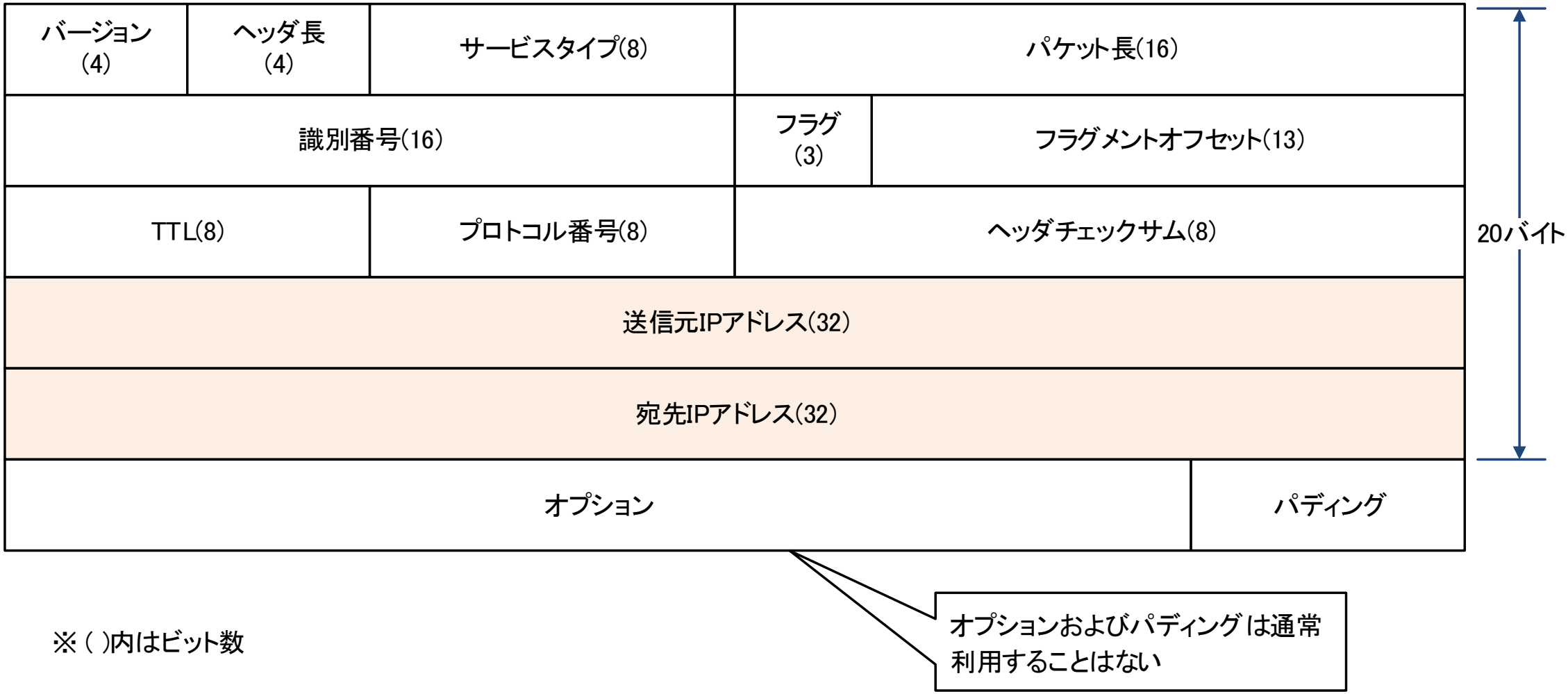


IP(Internet Protocol)

- TCP/IPの中でも特に重要なプロトコル
- あるホストから別のホストまでデータを転送するために利用するプロトコル
  - 転送するデータにIPヘッダを付加してIPパケットにする
  - IPパケットをネットワーク上に送り出すと経路上のルータが宛先まで転送してくれる



IPv4ヘッダフォーマット

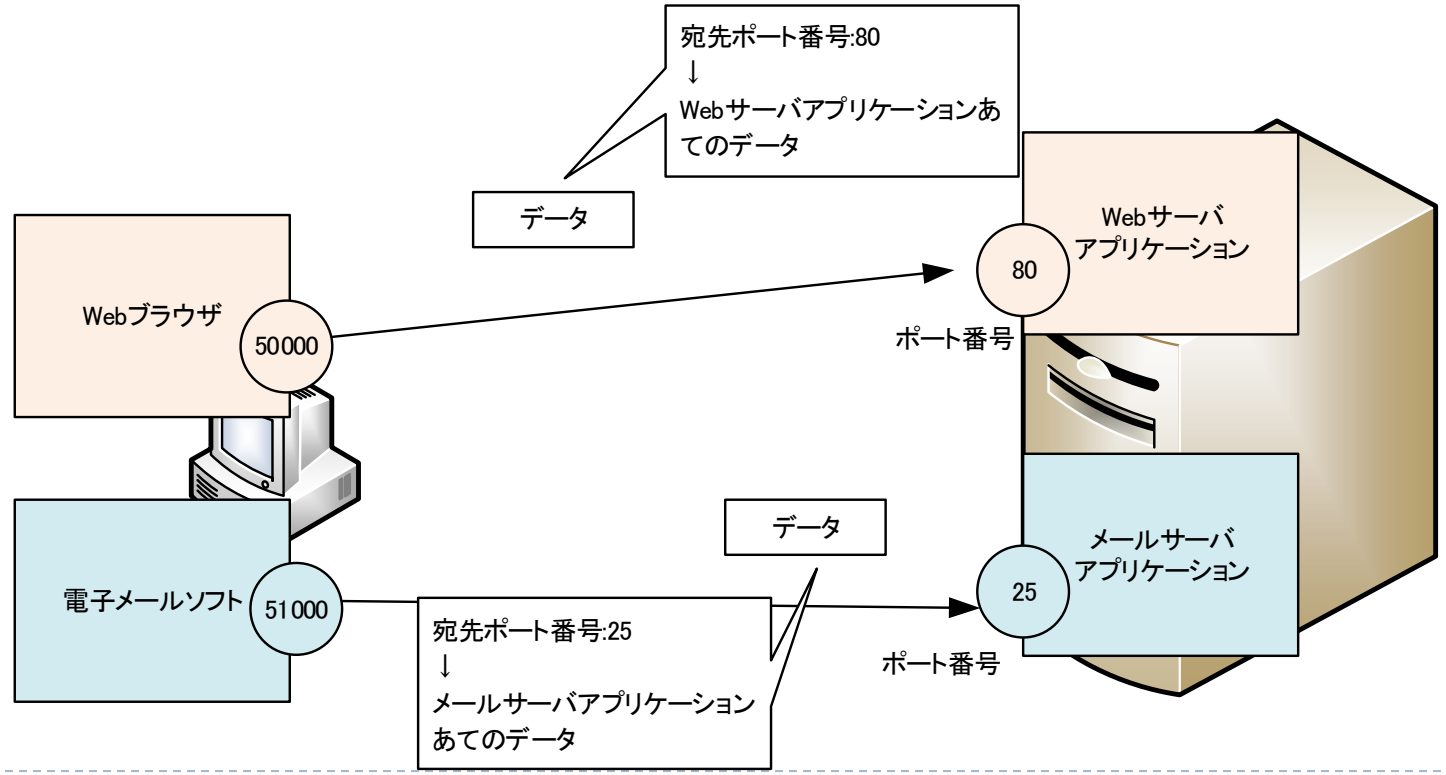


IPでのデータ転送に必要なこと

- **宛先IPアドレスを与えてあげなければいけない**
  - IPヘッダには宛先/送信元IPアドレスを指定しなければいけないので
  - 送信元IPアドレスは自分のアドレスなので簡単にわかる
- **IPアドレスは数字の羅列なのでわかりにくい**
  - 宛先IPアドレスを覚えていられない
  - 宛先IPアドレスを指定するときに間違えるかも・・・
- **一般のユーザには宛先IPアドレスを意識せずに自動的に求める仕組みがDNS**

ポート番号

- TCP/IPのアプリケーションプロトコルを識別するための番号
  - 16ビット(0～65535)
  - TCP/UDPヘッダに記述される
    - 宛先/送信元ポート番号



ポート番号の種類

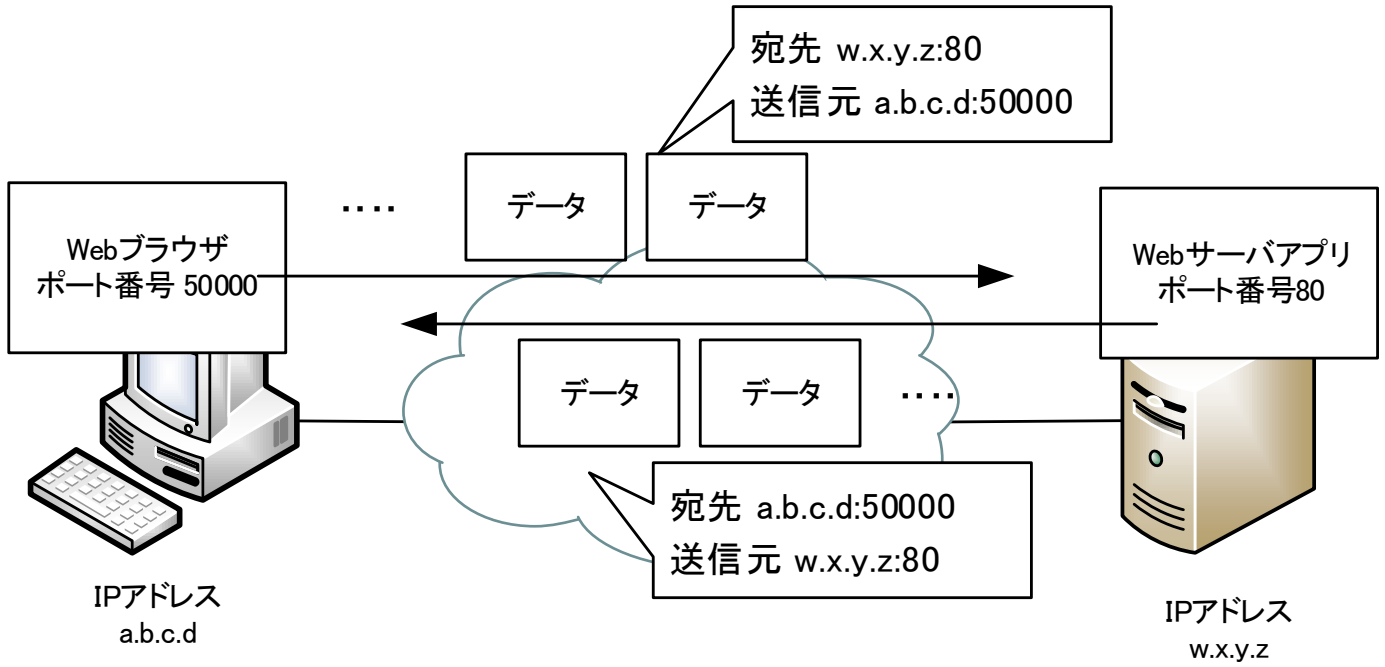
名称	ポート番号の範囲	意味
ウェルノウンポート	0～1023	サーバアプリケーション用に予約されているポート番号
登録済みポート	1024～49151	よく利用されるアプリケーションのサーバ側のポート番号
ダイナミック/プライベートポート	49152～65535	クライアントアプリケーション用のポート番号

主なウェルノウンポート

プロトコル	TCP	UDP
HTTP	80	-
HTTPS	443	-
SMTP	25	-
POP3	110	-
IMAP4	143	-
DNS	53	53
FTP	20/21	-
DHCP	-	67/68
Telnet	23	-

アプリケーション間の通信の識別

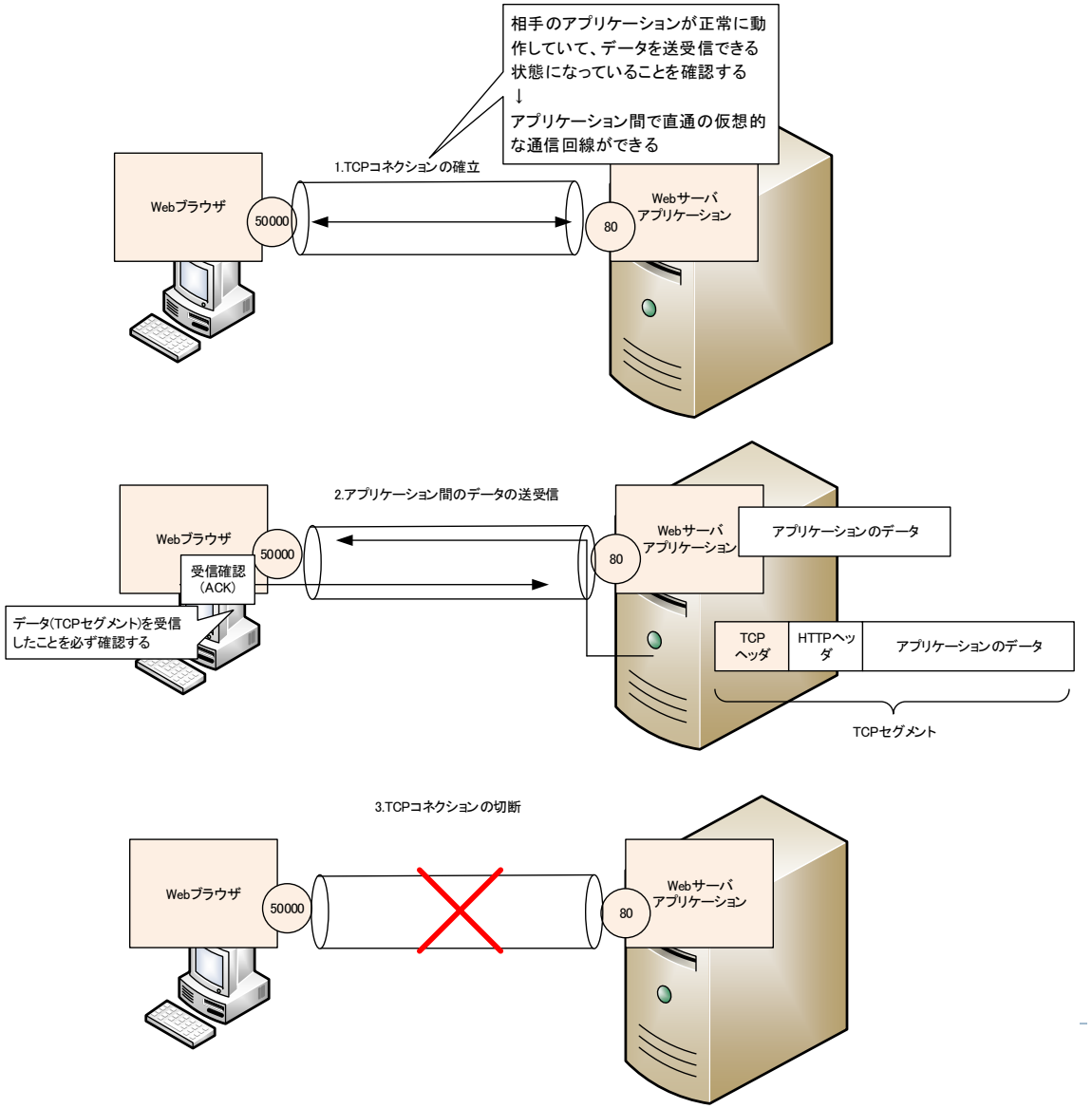
- 通信の主体はアプリケーション
- **TCP/IPのアプリケーション間の通信(フロー)はIPアドレスとポート番号の組み合わせで識別できる**
  - IPアドレス:ポート番号



TCPの特徴

- 信頼性のあるアプリケーション間のデータの転送を行う
  - データを送信する前にコネクションを確立する
    - 宛先のアプリケーションが正常にデータを受信できるかどうかを確認している
    - コネクション型転送プロトコル
  - データの適切なサイズに分割する
    - 分割する単位 MSS(Maximum Segment Size)
  - ポート番号によってデータをアプリケーションに振り分ける
  - データの受信確認を行う
  - ネットワークの混雑を検出すると、データの送信レートを下げる
    - データが失われてしまったら、ネットワークの混雑とみなす
  - データの転送が完了するとコネクションを開放する

TCPのデータ転送の概要

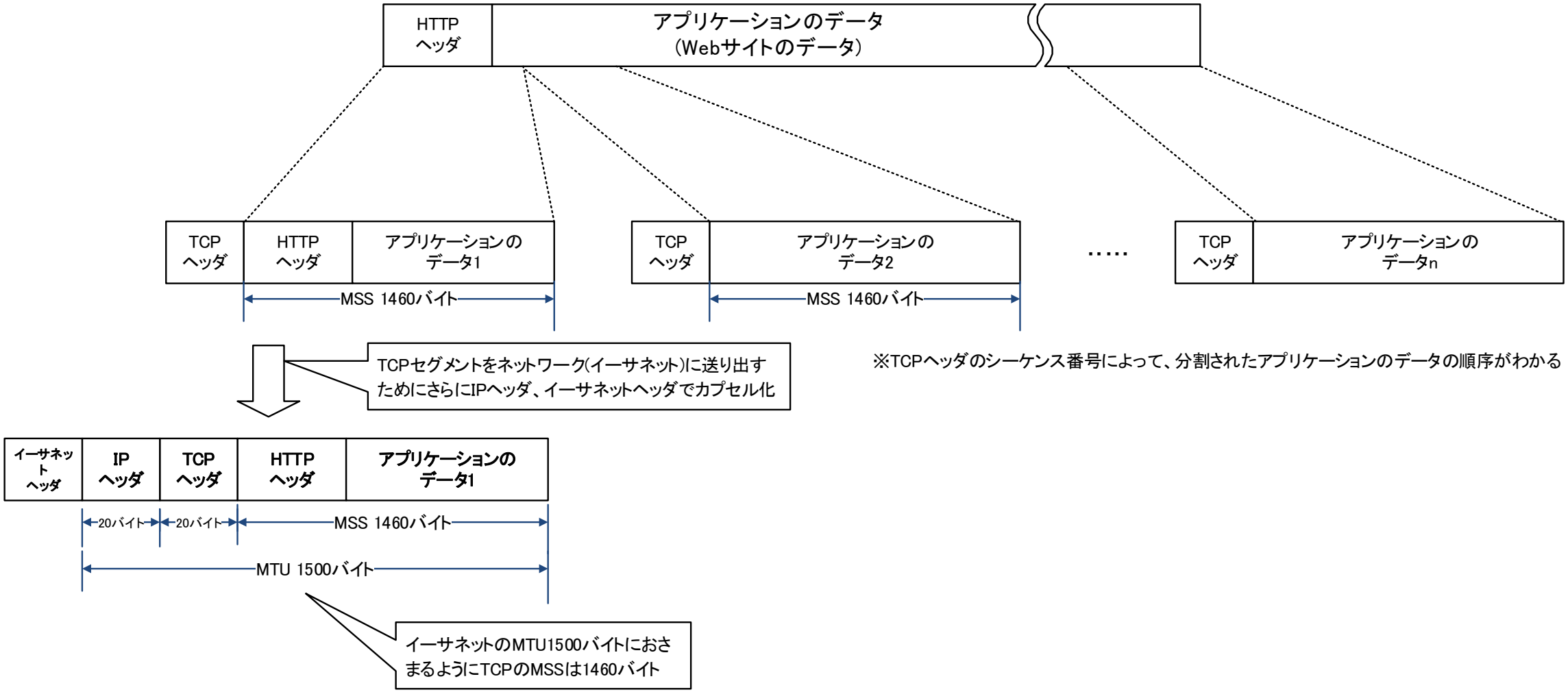


TCPヘッダフォーマット

<table>
<tr><td colspan="2">送信元ポート番号(16)</td><td colspan="2">宛先ポート番号(16)</td></tr>
<tr><td colspan="4">シーケンス番号(32)</td></tr>
<tr><td colspan="4">ACK番号(32)</td></tr>
<tr><td>データ
オフセット(4)</td><td>予約(6)</td><td>フラグ(6)</td><td>ウィンドウサイズ(16)</td></tr>
<tr><td colspan="2">チェックサム(16)</td><td colspan="2">アージェントポインタ(16)</td></tr>
</table>

※( )内はビット数

TCPでのデータの分割



UDPの特徴

- アプリケーション間のデータの転送を行う
  - UDPヘッダを付けて、アプリケーションの識別ができるようにして送り出すだけ
    - コネクションレス型転送プロトコル
  - 受信の確認やデータの分割などTCPに備わっている機能はない
    - 必要ならアプリケーションプロトコルで確認や分割を行うようにする
- UDPヘッダフォーマット
  - とてもシンプル

送信元ポート番号(16)	宛先ポート番号(16)
データグラム長(16)	チェックサム(16)

※( )内はビット数

TCP？UDP？

- TCPとUDPは特徴を踏まえて使い分ける

プロトコル	TCP	UDP
信頼性	高い	高くない
転送効率	よくない	よい
主な機能	アプリケーションへのデータの振り分け データの分割/組み立て 再送制御 フロー制御	アプリケーションへのデータの振り分け
用途	データのサイズが大きく信頼性が必要なアプリケーションのデータの転送	リアルタイムのデータの転送 ブロードキャスト、マルチキャスト データのサイズが小さいアプリケーションのデータ転送

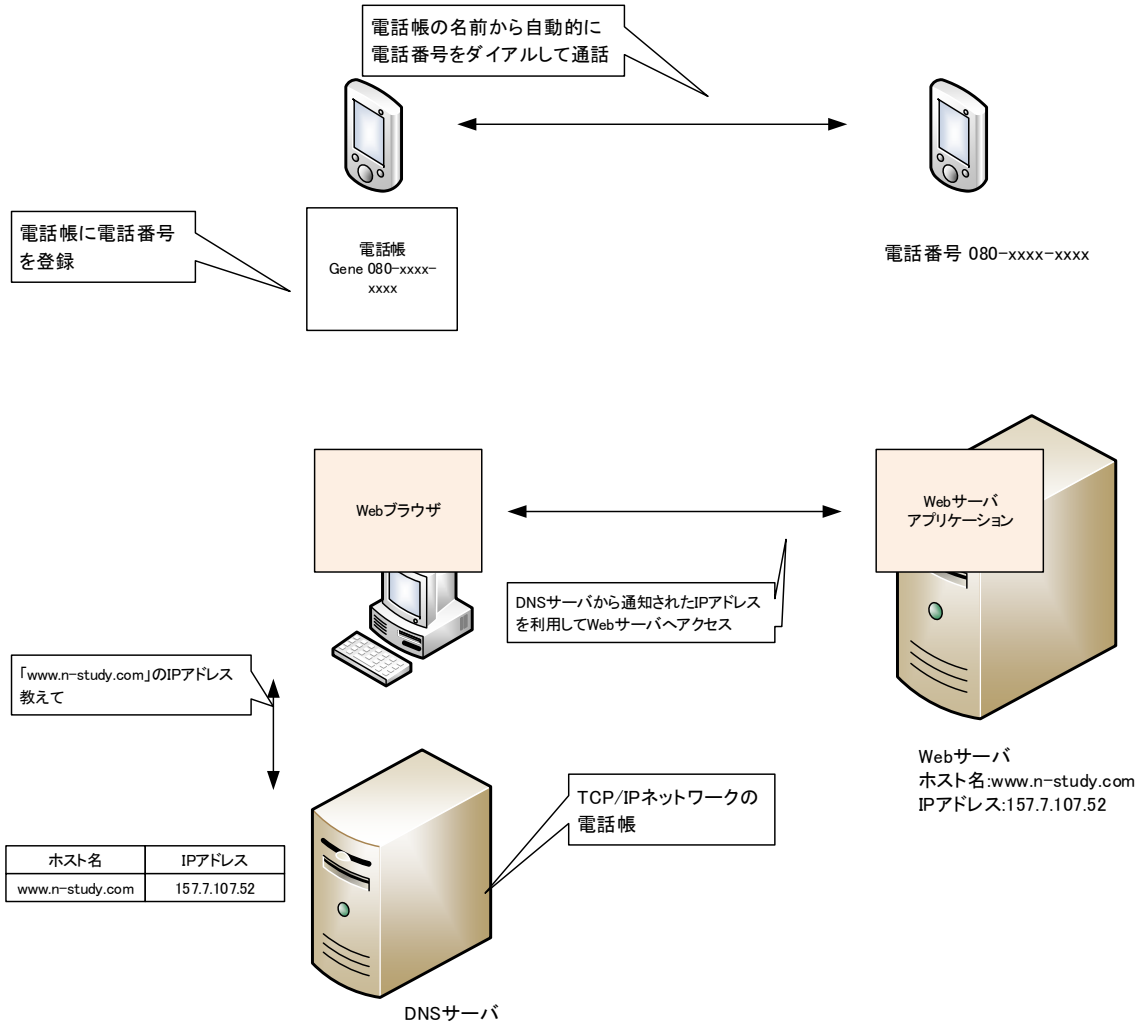
DNS(Domain Name System)

- DNSの目的
  - ホスト名からIPアドレスを求める名前解決を行う
  - ホスト名=PCやサーバなどTCP/IPで通信する機器につける名前
- TCP/IPでは必ずIPアドレスを指定しなければいけない
  - ユーザにはIPアドレスを意識させない
  - アプリケーションで利用するアドレスからDNSによってIPアドレスを自動的に求める
    - DNSリゾルバ:DNSでIPアドレスを求めるプログラム
    - アプリケーションのアドレスには、ホスト名そのものかホスト名を導き出す情報が含まれている
    - Webブラウザ　URL http://www.n-study.com/
    - 電子メール gene@n-study.com
- DNSは自動的に行われるので一般のユーザはあまり意識しないが、

TCP/IPの通信を支えるとても重要なシステム

ネットワークの電話帳

- DNSはネットワークの電話帳のイメージ
  - IPアドレスを明示的に指定しなくても、宛先のIPアドレスがわかる



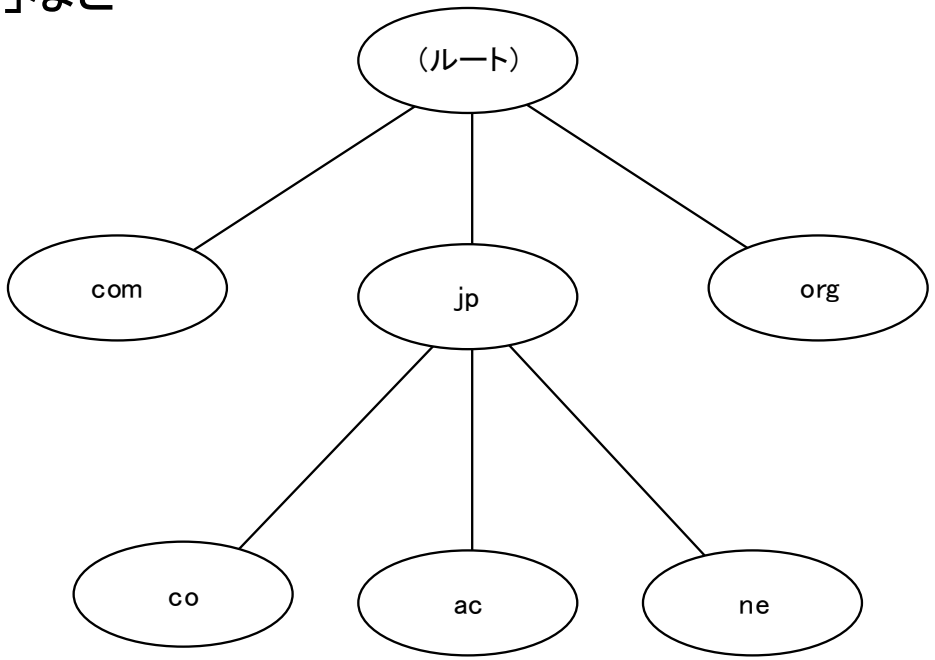
リソースレコード

- DNSサーバに登録する情報
  - DNSサーバに登録されているリソースレコードが正しいことがDNSによる名前解決の大前提

タイプ	意味
A	ホスト名に対応するIPアドレス
AAAA	ホスト名に対応するIPv6アドレス
CNAME	ホスト名に対応する別名
MX	ドメイン名に対応するメールサーバ
NS	ドメイン名を管理するDNSサーバ
PTR	IPアドレスに対応するホスト名

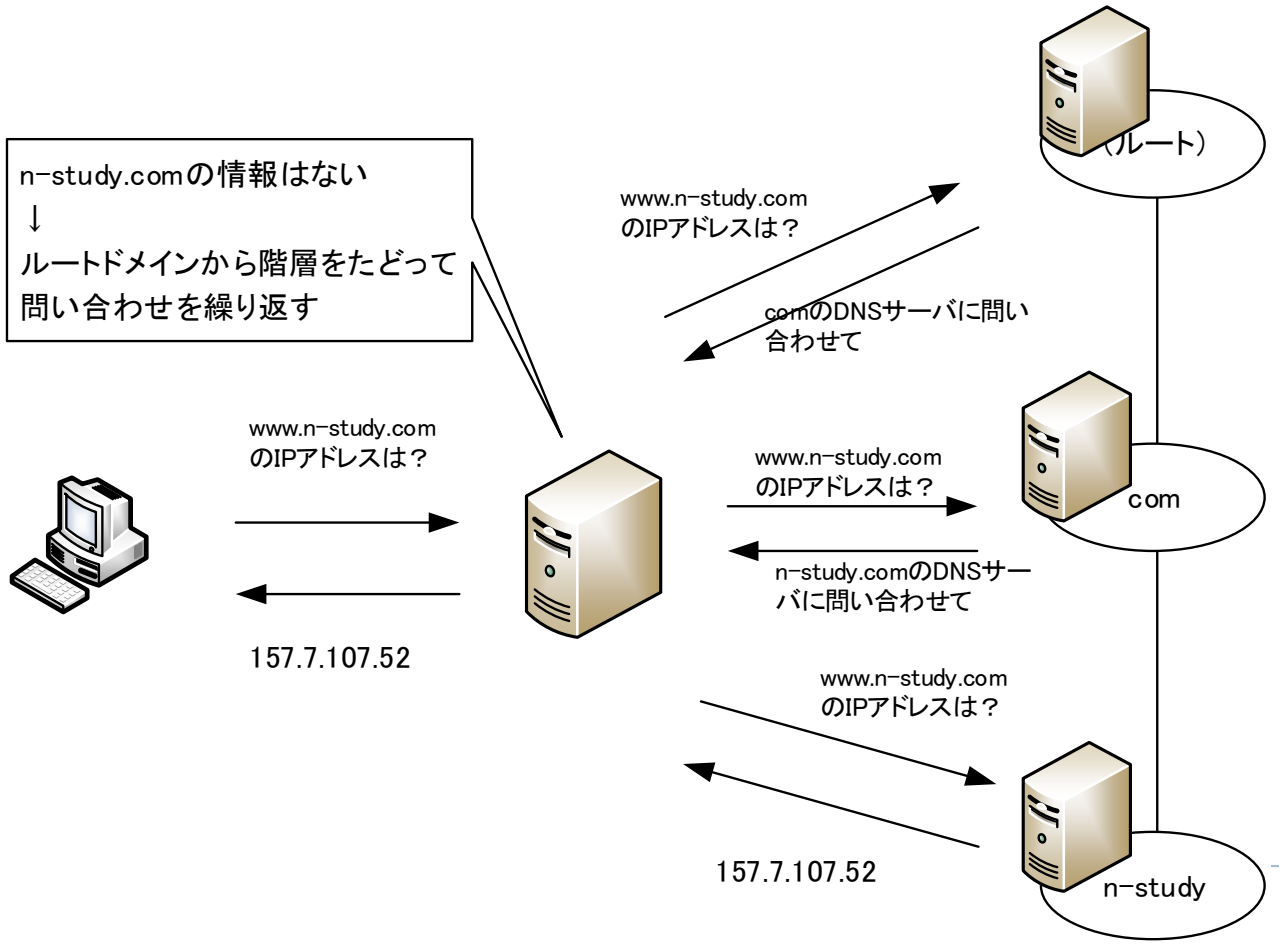
ドメイン名

- DNSのドメイン=ホスト名の集まり
  - 企業などの組織がドメインを管理する
  - ドメイン内のホストには共通のドメイン名を付ける
    - 「www.n-study.com」「file.n-study.com」「mail.n-study.com」など
  - FQDN(Fully Qualified Domain Name)
    - ホスト名とドメイン名を合わせたフルネーム
- ドメインの階層
  - インターネット上ではドメインは階層化されている
  - 頂点「.(ルートドメイン)」
  - TLD(Top Level Domain)
    - 「.com」「.jp」「.org」など



DNSによる名前解決の動作

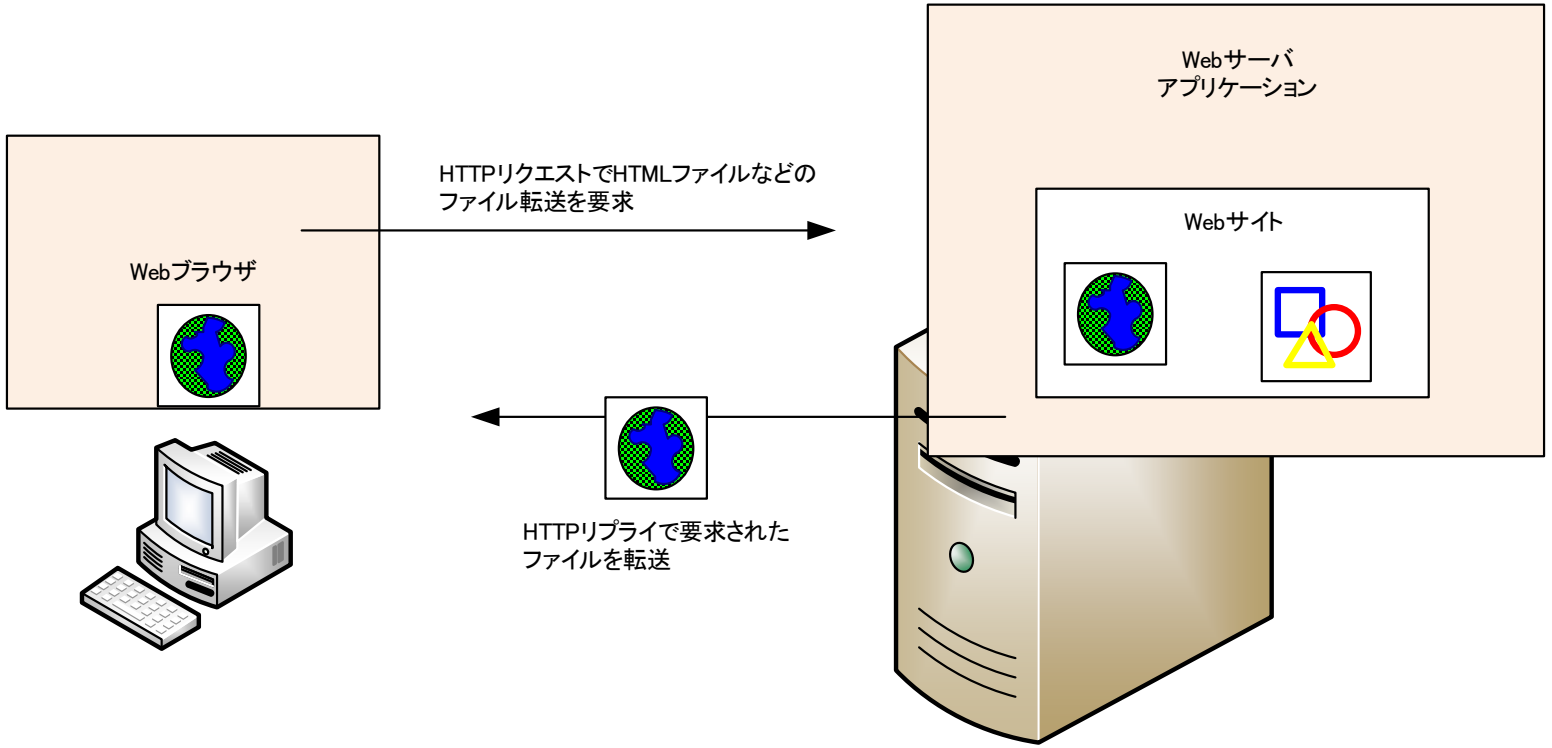
- PCに設定されているDNSサーバにまず問い合わせる(DNSネームクエリー)
- DNSサーバに登録されていなければ、ルートからたどっていく
  - DNS再帰検索



HTTPの概要

- ハイパーテキストを転送するためのプロトコル
  - ハイパーテキスト:通常のテキストファイルを越えた機能を持つ
    - リンクで任意のドキュメントに関連付ける
    - ドキュメントの構造を明示する
    - ハイパーテキストの例 :Webサイトを構成するHTMLファイル
  - 今ではハイパーテキストファイル以外にもさまざまなファイルを転送する汎用的なファイル転送プロトコルとして利用している

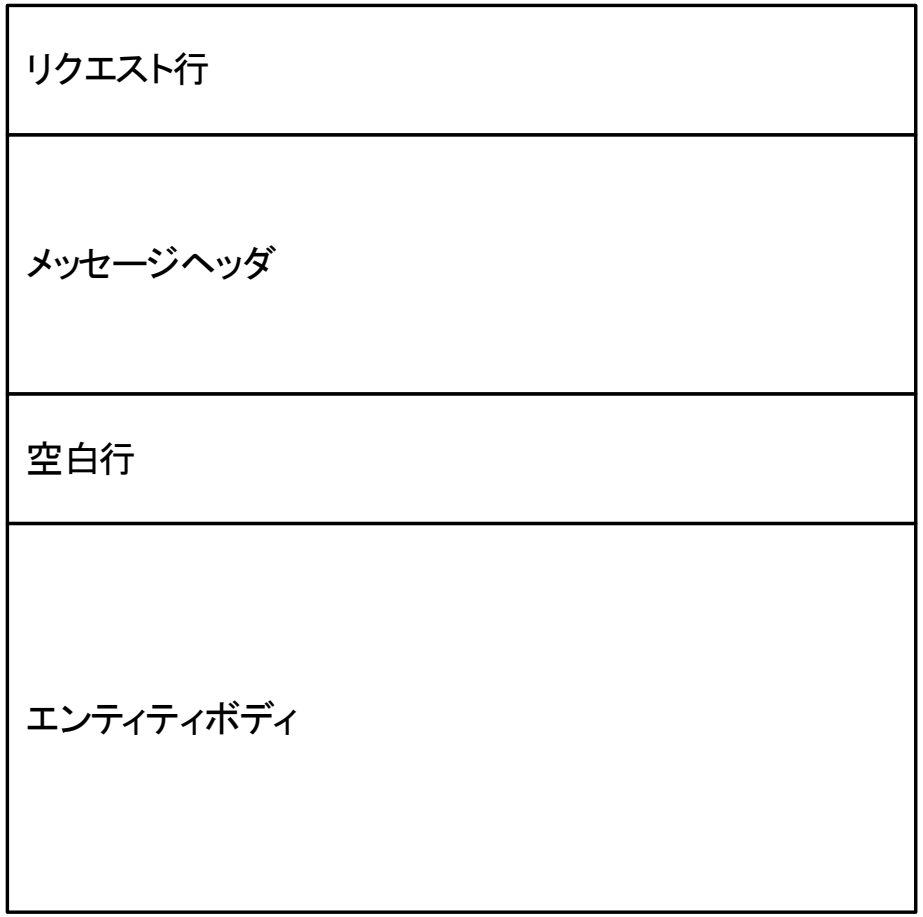
HTTPの概要



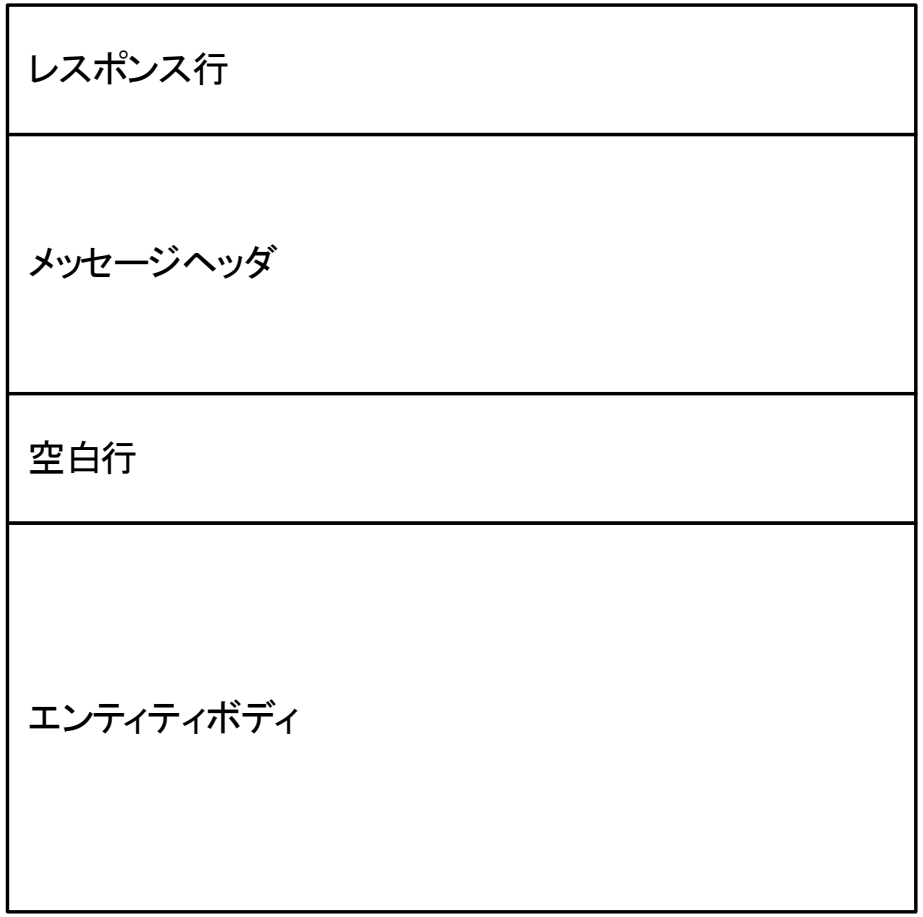
HTTP ウェルノウンポート80	アプリケーション層
TCP	トランスポート層
IP	インターネット層
イーサネットなど	ネットワークインタフェース層

HTTPリクエスト/レスポンス

HTTPリクエストのフォーマット

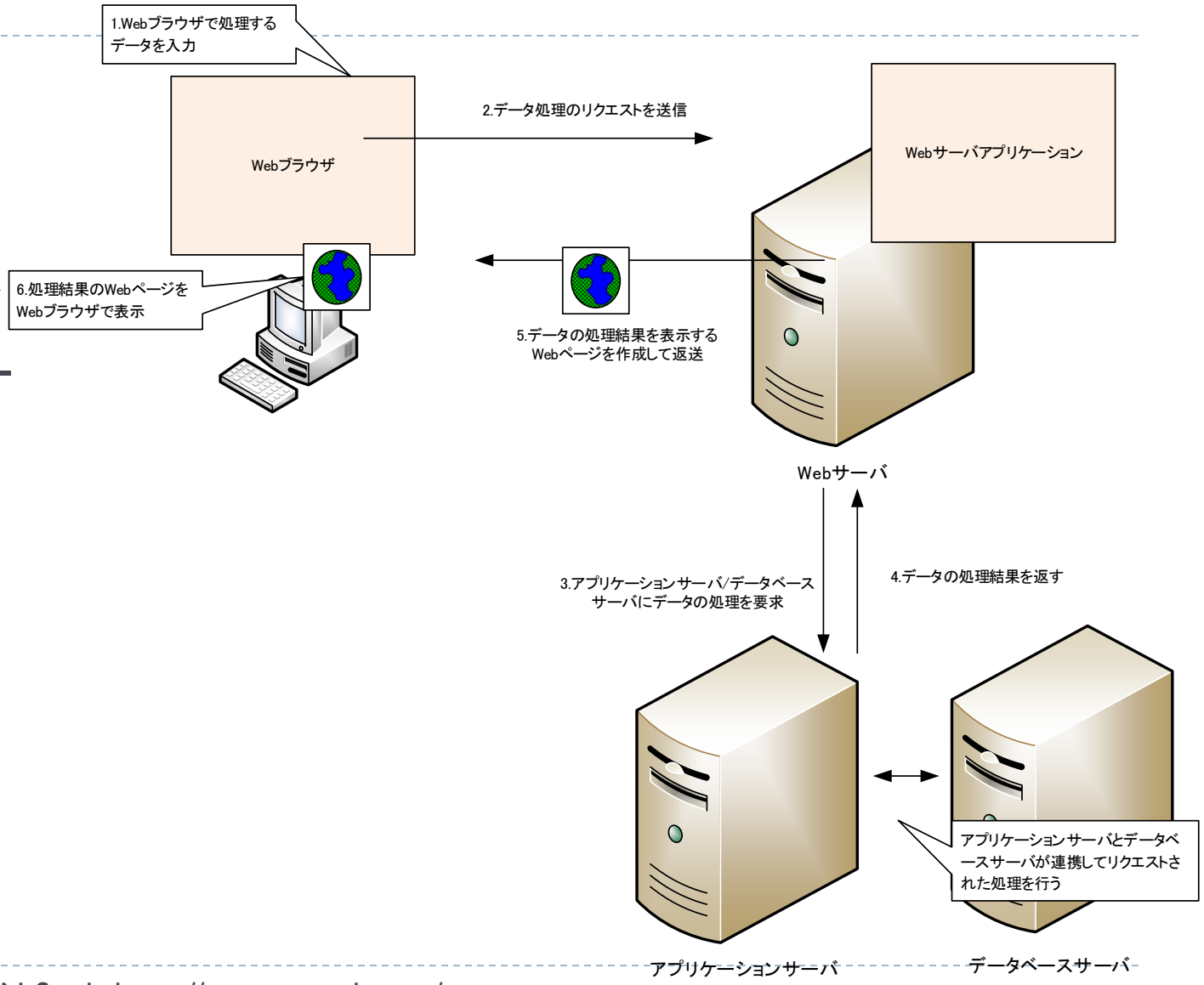


HTTPレスポンスのフォーマット



Webアプリケーション

- Webアプリケーション
  - Webブラウザをユーザインタフェースとするアプリケーション
  - ユーザのPCにはWebブラウザだけあればよい。専用のアプリケーションを追加でインストールする必要がない
  - 例
    - 証券会社のオンライントレード
    - 銀行のオンラインバンキング
    - Googleカレンダー



用語のまとめ

用語	意味
IP	データをあるホスト(機器)から別のホスト(機器)まで転送するために利用するプロトコル
IPアドレス	IPでデータを転送するときに宛先/送信元を識別するための識別情報
ポート番号	PC/サーバ内で動作しているアプリケーションを識別するための識別情報
TCP	PC/サーバに届いたデータを適切なアプリケーションに振り分けるために利用するプロトコル。エラー時の再送機能やデータの分割機能などがある
UDP	PC/サーバに届いたデータを適切なアプリケーションに振り分けるために利用するプロトコル。振り分けるだけで、その他の特別な機能はない。
DNS	アプリケーションで利用するアドレス情報からIPアドレスを求めるためのプロトコル
HTTP	Webページのデータ(HTMLファイル)を転送するために利用するプロトコル

確認テスト Part4

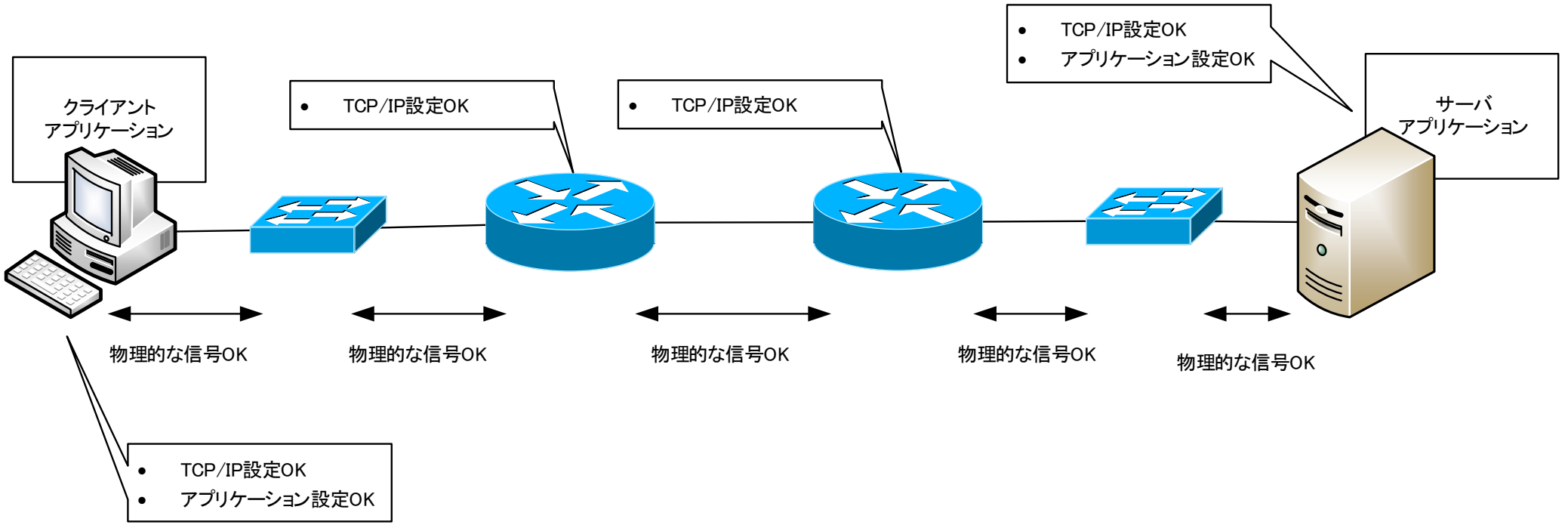
- 以下のURLにここまでの内容を確認するテストを公開しています。
  - https://forms.gle/m3vgUgsxSvAjAcwcA

TCP/IPの設定

正しいTCP/IP設定が大前提

TCP/IPでアプリケーションの通信を行う大前提

- 経路上の機器間で物理的な信号がきちんと送り届けられるようになっている
- 経路上のすべての機器のTCP/IP設定が正しく行われている
- 利用するアプリケーションの設定が正しい



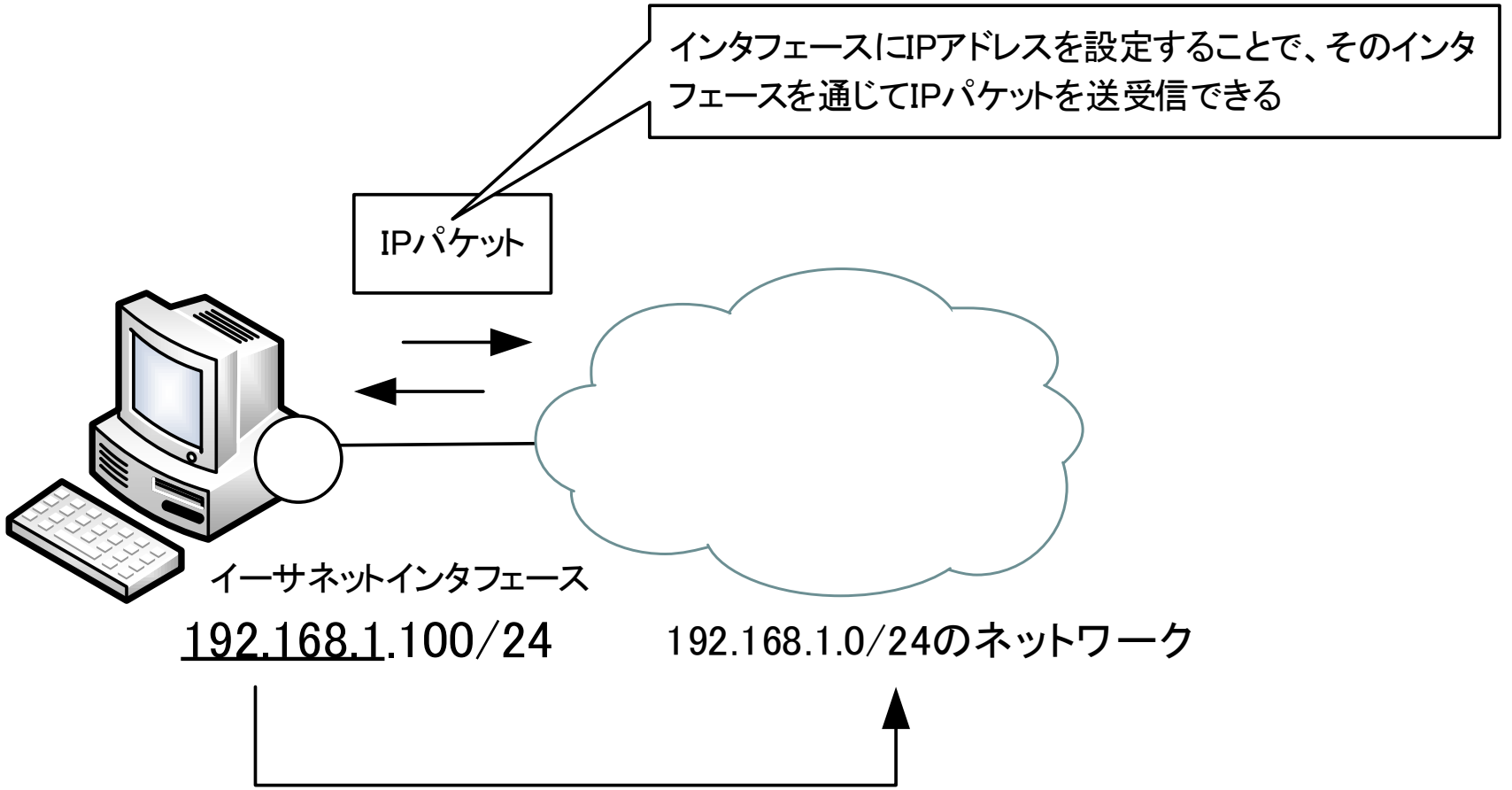
TCP/IPの設定

機器	主な設定内容
PC、サーバ	IPアドレス/サブネットマスク デフォルトゲートウェイのIPアドレス DNSサーバのIPアドレス
ルータ	IPアドレス/サブネットマスク ルーティング(ルーティングテーブル)
レイヤ2スイッチ	特になし

IPアドレス/サブネットマスク

- TCP/IPでは、IPアドレスによって通信相手(のインタフェース)を識別
  - IPアドレスを設定する = ネットワークに(論理的に)接続すること
    - IPパケットの送信/受信ができるようになる
    - 普通のユーザには、ほとんど意識させないようにしているが、技術者なら必ず意識しておく
- サブネットマスク
  - IPアドレスのうち、ネットワークアドレスがどこまでかを表す

IPアドレス/サブネットマスク

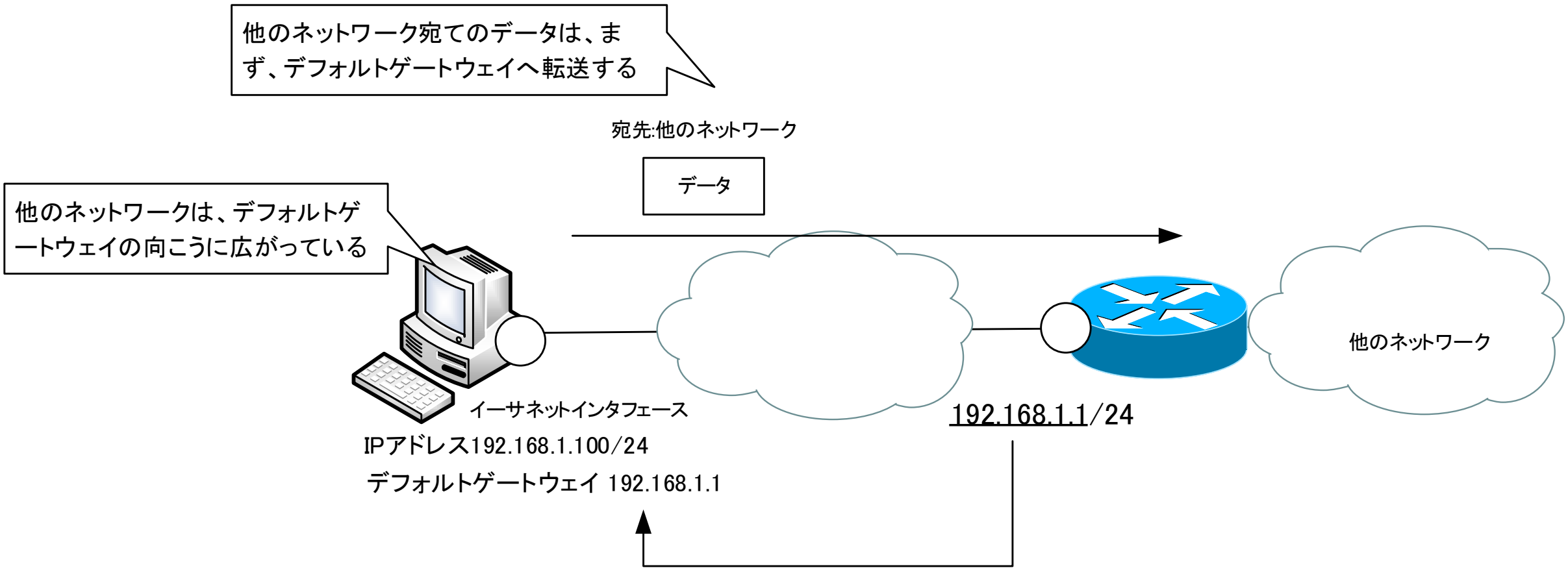


設定したIPアドレス/サブネットマスクからホストが接続しているネットワークアドレスがわかる

デフォルトゲートウェイのIPアドレス

- デフォルトゲートウェイ
  - 同じネットワーク上のルータ/レイヤ3スイッチ
  - 他のネットワークは、デフォルトゲートウェイの先にあるはず
    - ゲートウェイ(gateway) = 入り口
  - 他のネットワーク宛てのパケットはまずデフォルトゲートウェイに転送する
    - そのためには、デフォルトゲートウェイのIPアドレスがわかっていなければいけない
  - 単に「ゲートウェイ」と表現することもよくある
- デフォルトゲートウェイの設定が間違っている/デフォルトゲートウェイがダウンすると・・・
  - 他のネットワーク宛ての通信がいっさいできない
    - 同じネットワークなら大丈夫

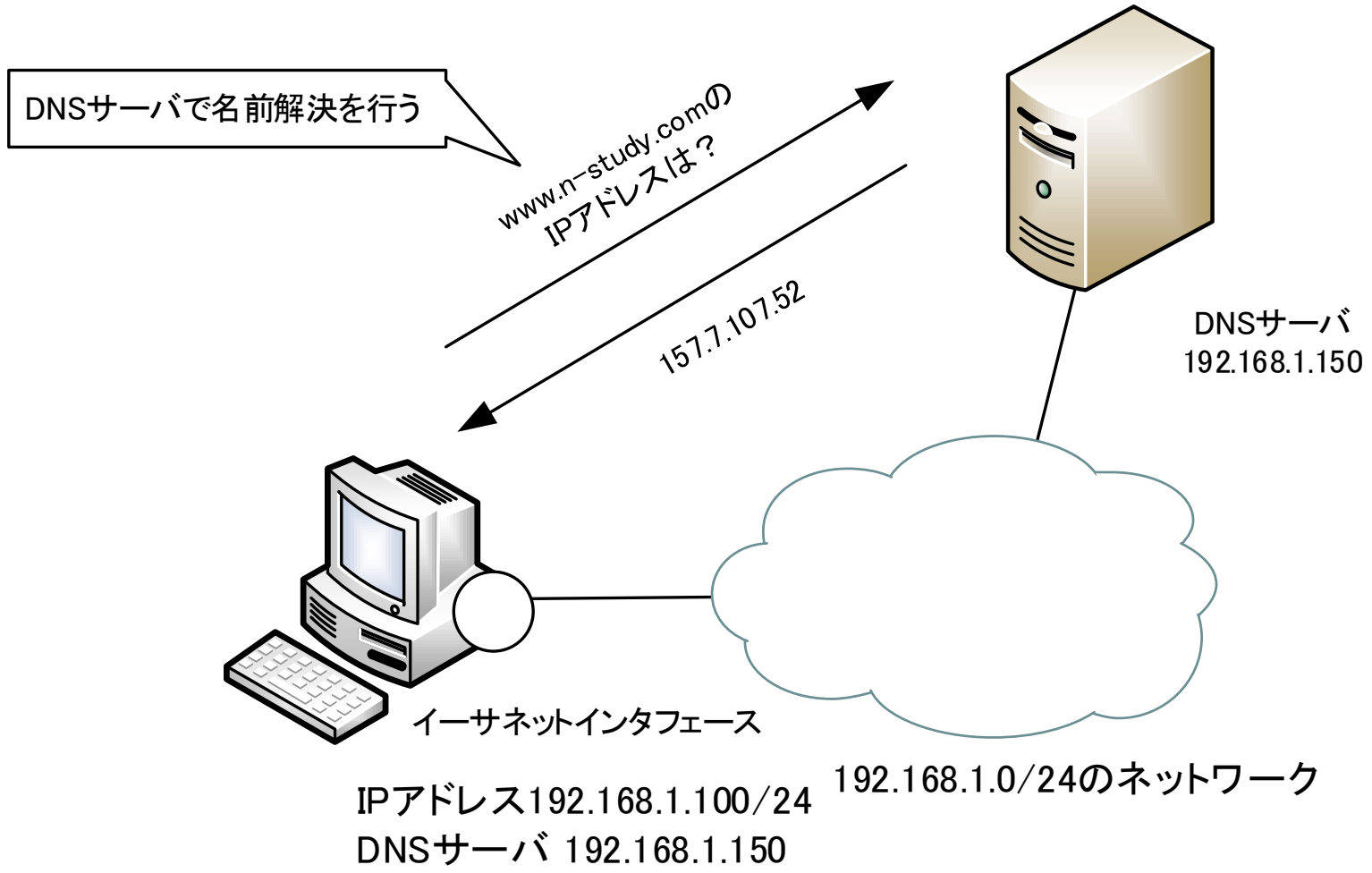
デフォルトゲートウェイのIPアドレス



DNSサーバのIPアドレス

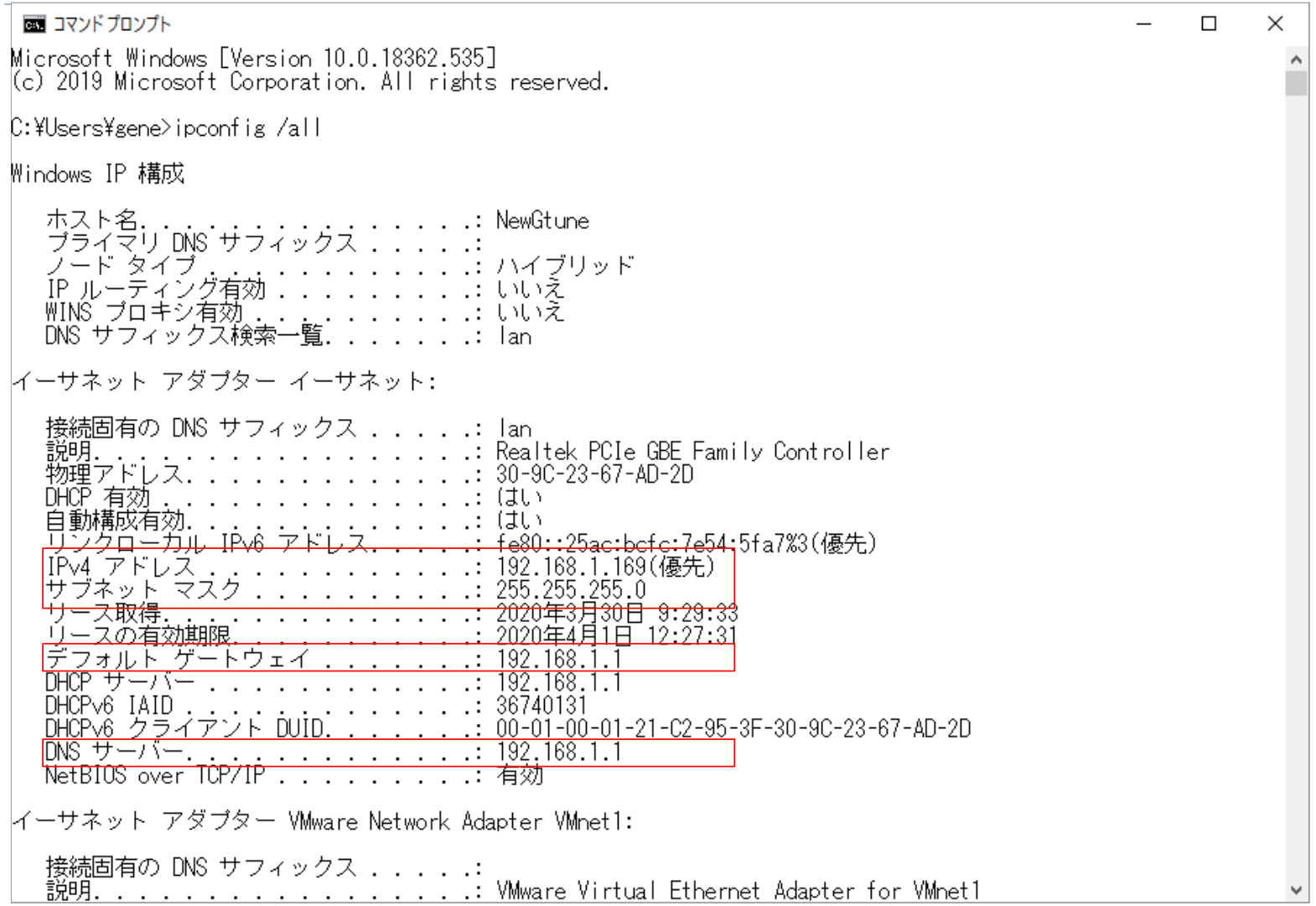
- 名前解決
  - DNSサーバに問い合わせて宛先IPアドレスを調べる
  - そのために、問い合わせ先のDNSサーバのIPアドレスがわかっていなければいけない
- DNSサーバのIPアドレスの設定が間違っている/DNSサーバがダウンすると・・・
  - 宛先IPアドレスがわからなくなるので、通信そのものができない

DNSサーバのIPアドレス



TCP/IP設定の確認

- Windows OS
  - コマンドプロンプトで「ipconfig /all」
  - ネットワークインタフェースごとにTCP/IPの設定内容が表示される



用語のまとめ

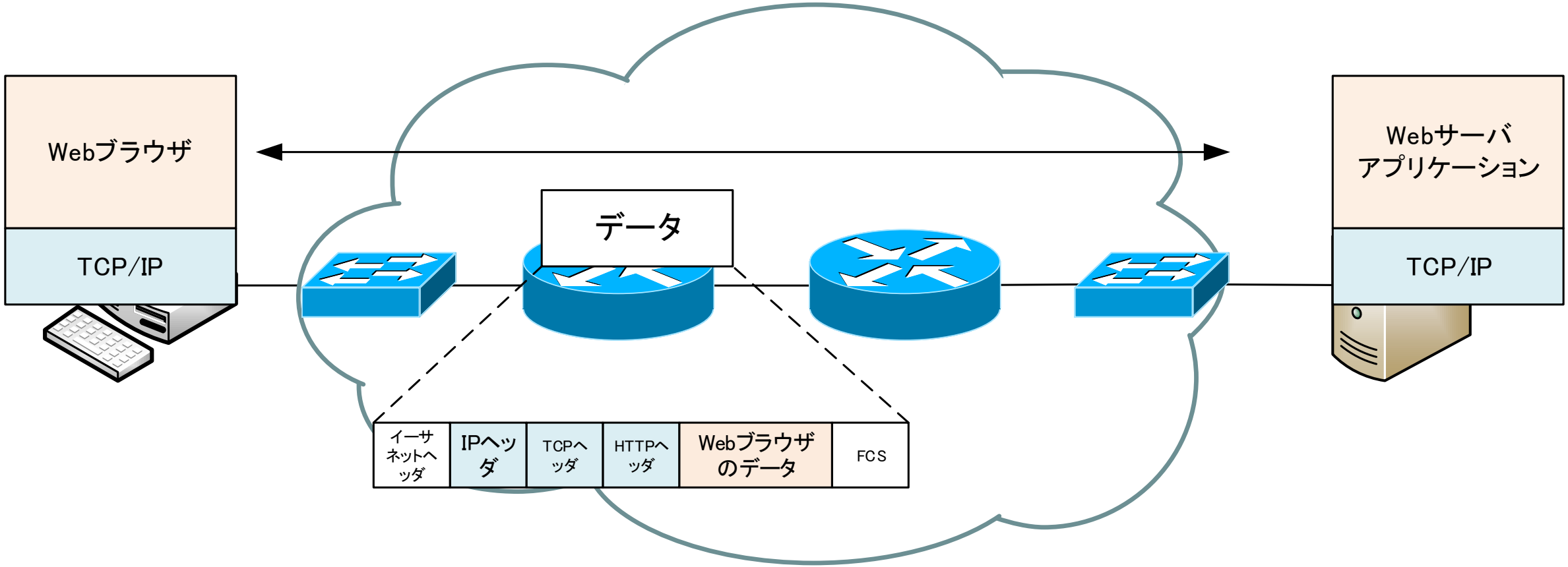
用語	意味
サブネットマスク	IPアドレスのうちどこまでがネットワークアドレスであるかを表す情報
デフォルトゲートウェイ	同じネットワーク上のルータまたはレイヤ3スイッチ。他のネットワークへデータを転送するときに、まず、デフォルトゲートウェイへ転送する
DNSサーバ	アプリケーションのデータを送信するときに宛先IPアドレスを問い合わせるサーバ

確認テスト Part5

- 以下のURLにここまでの内容を確認するテストを公開しています。
  - https://forms.gle/RTqc9FCgNjJjqNBs6

まとめ

ネットワーク！！！


Webブラウザ
TCP/IP
データ
Webサーバ
アプリケーション
TCP/IP
イーサネットヘッダ
IPヘッダ
TCPヘッダ
HTTPヘッダ
Webブラウザのデータ
FCS

まとめ

- ネットワークを利用する目的は、さまざまなアプリケーションを利用してそのメリットを享受すること
- 通信の主体はアプリケーションで、原則として通信は双方向
- ネットワークは、ルータ/レイヤ2スイッチ/レイヤ3スイッチなどのネットワーク機器で構成されている
  - ネットワーク機器のインタフェース同士を接続してリンクを構成していく
- ネットワークの分類として「誰が利用するネットワークなのか」を考える
  - プライベートネットワーク:限られたユーザのみが利用できる
  - インターネット:誰でも利用できる(ユーザを限定できない)
- データの転送は、送信元インタフェースから送り出された物理信号を適切な宛先インタフェースまで送り届ける
- ネットワーク機器は、適切なヘッダを参照して転送先を判断する

まとめ

- TCP/IPは事実上の標準のネットワークアーキテクチャで、いわば「ネットワークの共通言語」
- IPで宛先のホストまでデータを送り届ける
- DNSによって宛先IPアドレスを求める
- TCP/UDPで届いたデータを適切なアプリケーションへ振り分ける
- アプリケーションの通信を行うには、正しいTCP/IPの設定がされていることが大前提
  - IPアドレス/サブネットマスク
  - デフォルトゲートウェイのIPアドレス
  - DNSサーバのIPアドレス
- Windowsコマンドプロンプトで「ipconfig /all」コマンドを入力して、TCP/IP設定を確認する

もっと詳しく知りたい！！！

- TCP/IP
  - https://www.n-study.com/tcp-ip/
- イーサネット
  - https://www.n-study.com/ethernet/
- レイヤ2スイッチの仕組み
  - https://www.n-study.com/layer2switch/
- IPアドレス
  - https://www.n-study.com/ip-addressing/
- ルータ/ルーティング
  - https://www.n-study.com/iprouting/