第4章 情報通信ネットワークとデータの活用

（4）「情報通信ネットワークとデータの活用」で学ぶこと

- 情報通信ネットワークの仕組みや構成要素、プロトコルの役割及び情報セキュリティを確保するための方法や技術について
- データを蓄積・管理・提供する方法、情報通信ネットワークを介して情報システムがサービスを提供する仕組みと特徴について
- データを表現・蓄積するための表し方と、データを収集・整理・分析する方法について

（4）「情報通信ネットワークとデータの活用」で学ぶこと

- 要するに

学習18, 19, 20,21

- インターネットの仕組み
- 暗号
- オープンデータ
- データベース（Access）
- 量的データの分析（Excel）
- 質的データの分析
- データの可視化

学習18 情報通信ネットワークの仕組み

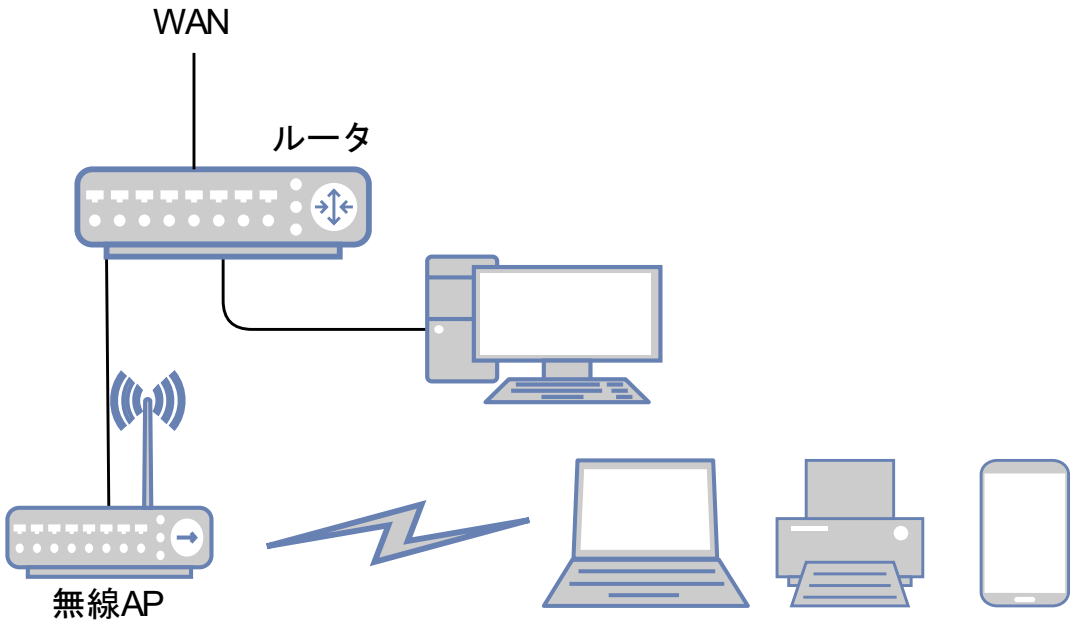
(1)身近なLAN について考えてみよう

(2)有線LAN と無線LAN の違い

(3)情報通信ネットワークのプロトコル

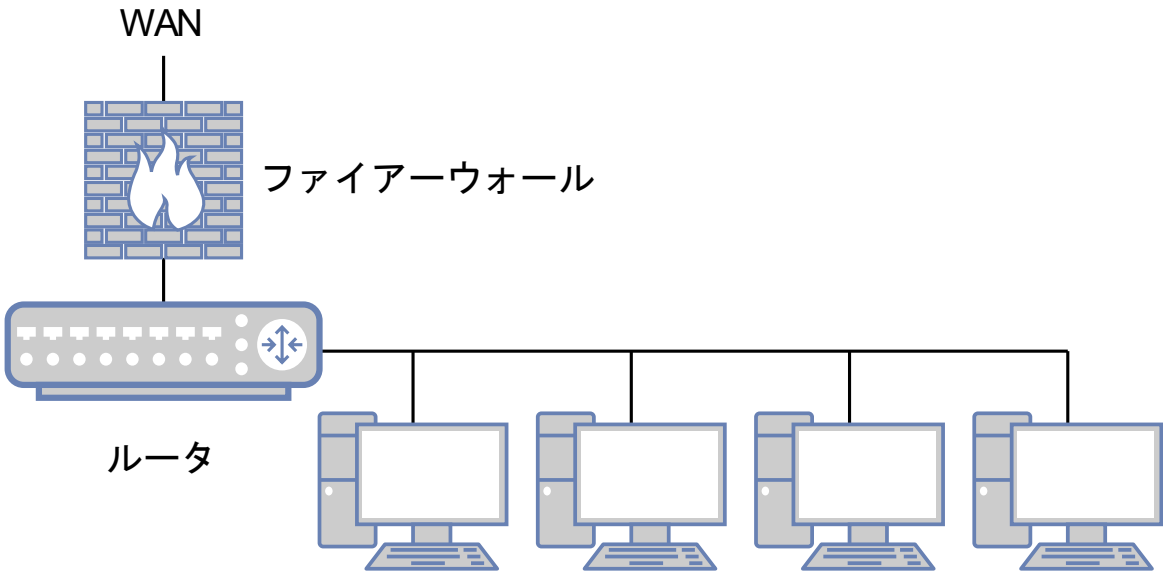
(1) 身近なLAN について考えてみよう

- LAN (Local Area Network) とは
  - パソコン・プリンタ・スマートフォンなどの情報機器や、テレビ・エアコン・照明などの家電を接続し、情報のやりとりを行うためのネットワーク
  - ルータ等によって外部との接続を持つ



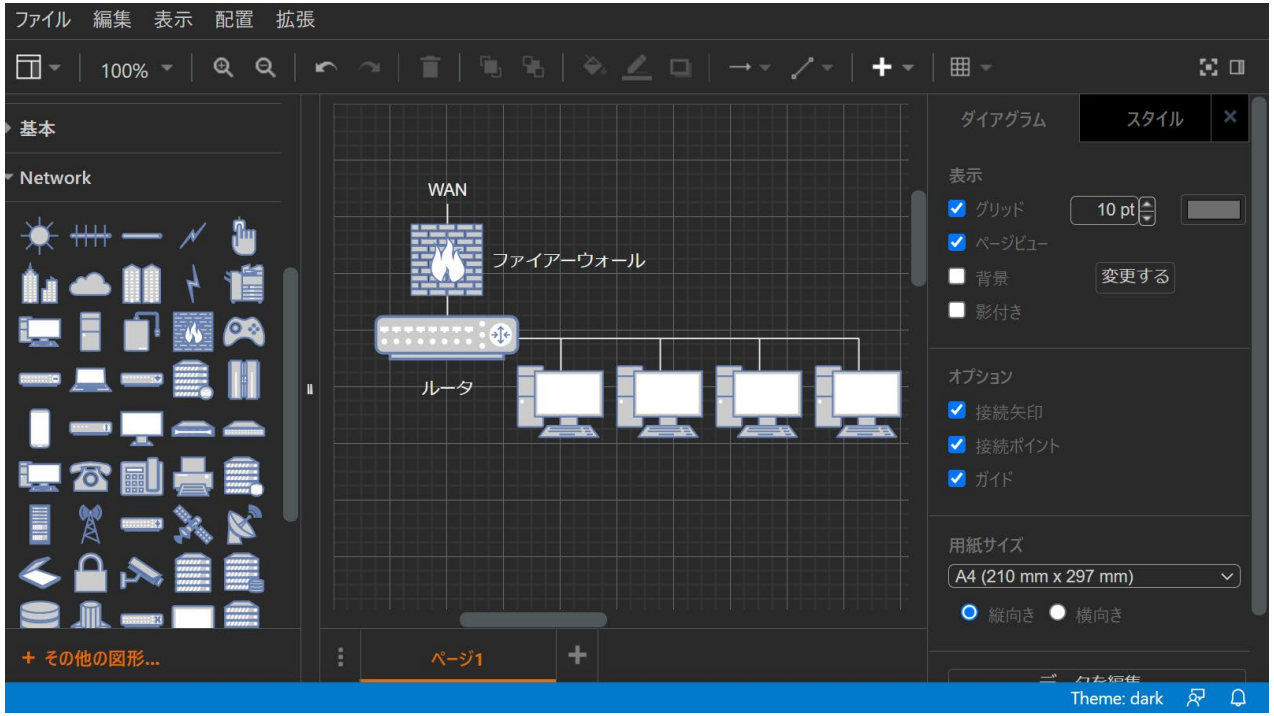
(1) 身近なLAN について考えてみよう

- LANの規模と構成
  - 家庭では、比較的小数の機器で小規模LANが構成され、IoT技術を用いて家電製品の操作などが行われることもある
  - 学校のコンピュータ室などは中規模LANが構成され、他のLANと切り離したり、ファイアウォールを設置する構成となることもある



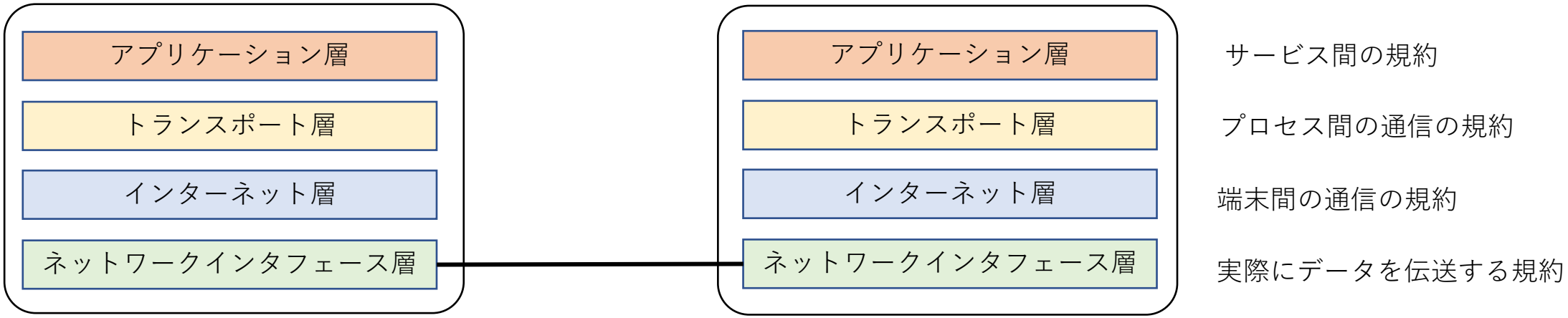
補足：描画ソフトdraw.io

- 特徴
  - 典型的な作図作業に用いる部品が豊富に準備されている
  - ブラウザやVSCodeの拡張機能で利用できる



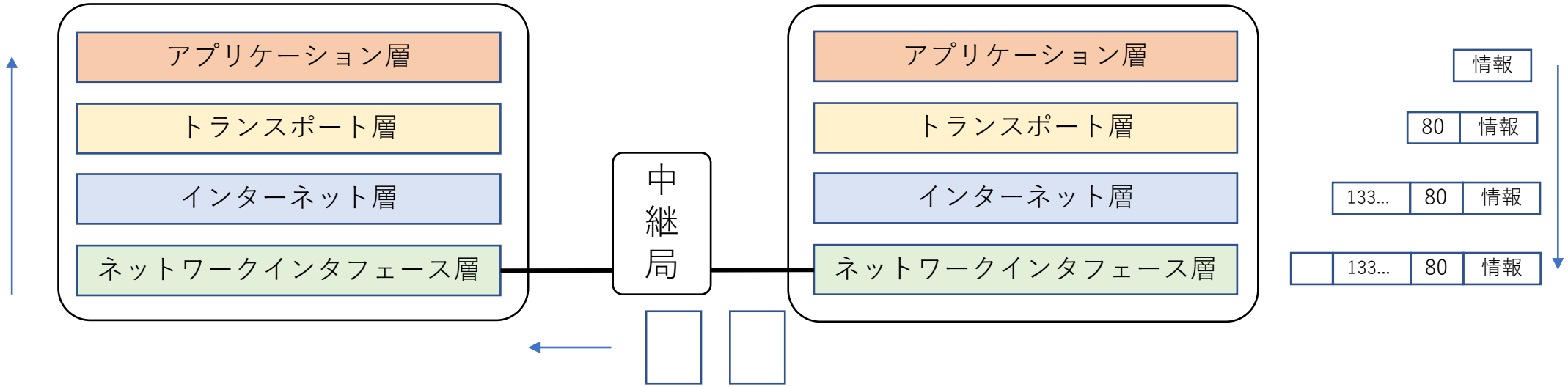
(2) 有線LANと無線LANの違い

- ネットワークの階層モデル
  - 標準的なTCP/IPを中心としたプロトコル群の4階層
    - アプリケーション層：HTTP, IMAP, DHCP
    - トランスポート層：TCP, UDP
    - インターネット層：IPv4, IPv6
    - ネットワークインタフェース層：イーサネット, Wi-Fi



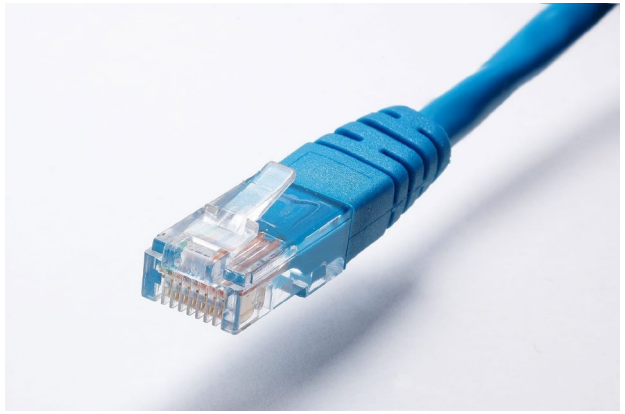
(2) 有線LAN と無線LAN の違い

- コンピュータネットワークの原理
  - パケット通信
    - 回線を独占せずに、情報を小さい単位に分割して送信し、受信側ではそれらを順序通りに組み立てる
    - 複数の機器が同じ回線を使える
    - 宛先が同じパケットが同じルートを通ってくるとは限らない



(2) 有線LAN と無線LAN の違い

- 有線／無線の違い
  - 有線LAN: イーサネット(IEEE802.3規格)ケーブルによる通信
  - 無線LAN: Wi-Fi (IEEE802.11規格) に基づく電波による通信

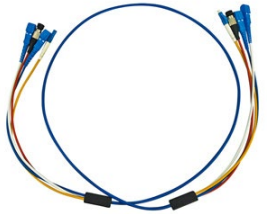


RJ45コネクタ

バッファロー社製 Wi-Fiルータ

(2) 有線LAN と無線LAN の違い

- 有線通信の手段
  - イーサネットケーブルの名称
    - （最大通信速度 Mbps）BASE- (ケーブルの種類)
  - よく使われるケーブル
    - 室内・建屋内：10GBASE-T カテゴリ6, 6A
      - ✓ ツイストペアケーブル（より線）：ノイズの影響を減らす
      - ✓ 最大長100m
    - 建屋間、広域：10GBASE-LR
      - ✓ 光ファイバー：信号減衰がほとんどない
      - ✓ 最大長10Km



サンワサプライ社製 光ファイバーケーブル

(2) 有線LANと無線LANの違い

- 無線通信の手段

分類	通信距離	技術名称
短距離無線	数m	RF-ID
無線PAN	10m前後	Bluetooth
無線LAN	100m前後	WiFi6 802.11ax: 9.6Gbps, 2.4GHz/5GHz WiFi5 802.11ac: 6.9GHz, 5GHz
無線WAN		3G, LTE, 4G, 5G

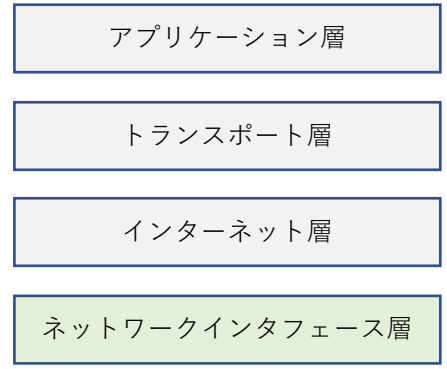
(2) 有線LAN と無線LAN の違い

- 無線LANの認証方式と暗号化アルゴリズム（p.158 図表7）
  - WEP: 暗号化方式もWEPとよばれる。古くから使われているが、簡単に暗号化キーが解読できてしまう
  - WPA-TKIP: 暗号化アルゴリズムにRC4を用い、WEPよりも解読が難しい。TKIPは一定時間毎に暗号鍵を変更する方法
  - WPA2-CCMP:暗号化アルゴリズムにAESを用い、WPAよりも解読が難しい。AESはデータの入れ替えなどを何段階か繰り返すことで暗号を複雑なものにする方法
  - WPA3: より安全な新しい暗号規格。総当たり攻撃の防御が可能

(3) 情報通信ネットワークのプロトコル

- プロトコルとは
  - もともとの意味は「外交儀礼」
  - 後にコンピュータ間の通信規約の意味を持つようになった
- プロトコルと階層性
  - アプリケーションごとに通信規約を決めていては互換性がなくなる
  - ひとつの通信規約ですべてをカバーすると、新しい技術に対応するごとに全体を見直さなければならない
  - 適切に階層を設定することで、上下の階層の実装とは独立に規約を考えることができる

(3) 情報通信ネットワークのプロトコル



- ネットワークインタフェース層
  - 原則としてお互いの通信が見えている範囲の通信
    - ひとつのハブ/無線APでつながっているLAN
  - MACアドレスで通信
    - 通信可能なハードウェアに割り当てられた全世界で唯一のアドレス

      例）04-A3-43-5F-43-23　(6オクテット=48bit=約280兆)
    - 上位3オクテットで機器の製造者がわかる
    - 最近のiOSやAndroidではランダム化されていることもある

(3) 情報通信ネットワークのプロトコル

アプリケーション層

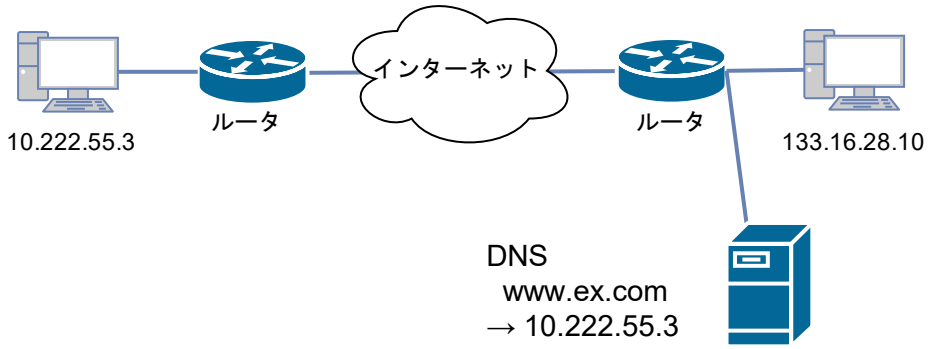
トランスポート層

インターネット層

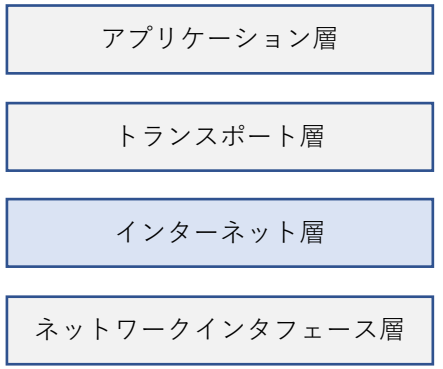
ネットワークインタフェース層

- インターネット層
  - インターネットでつながっている機器間の通信
    - 通信可能な機器はIPアドレスを持っている
      - ✓ IPアドレス
        - 通信可能な機器に割り当てられた全世界で唯一に見えるアドレス

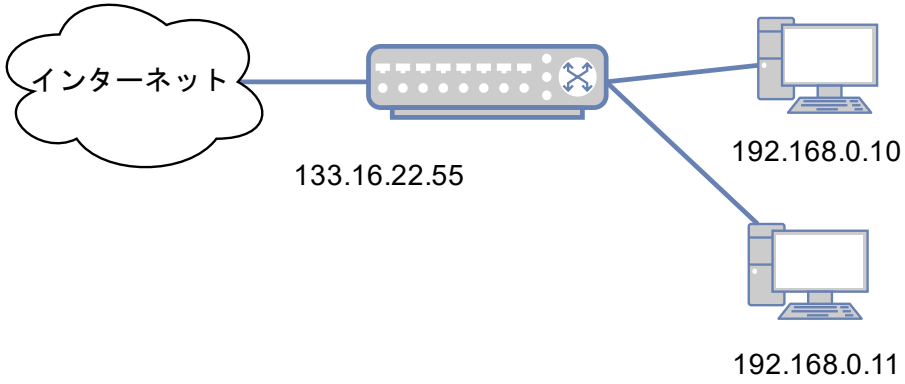
          例）133.16.28.10（32bit=約43億）
    - どのIPアドレスのデータをどのルータに渡すかという情報はルータ間で交換している



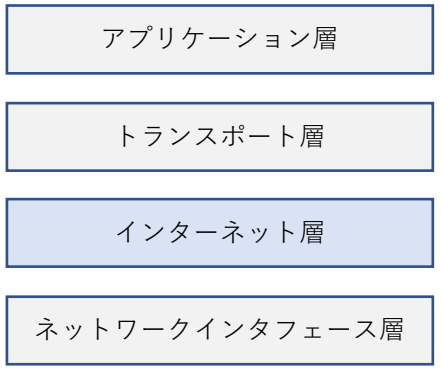
(3) 情報通信ネットワークのプロトコル



- IPアドレス
  - グローバルとプライベート
    - 組織ごとに上位ビット(クラスA:8, B:16, C:24)が割り当てられ、各組織では下位ビットを機器に割り当てる（グローバルアドレス）
      - ✓ 例）京都工芸繊維大学はクラスBの 133.16.X.X が割り当てられている
    - プライベートアドレス（192.168.X.X など）はLAN内で自由に割り当てられる
    - グローバルアドレスが割り当てられた組織内のスイッチでプライベートアドレスに変換することができる



(3) 情報通信ネットワークのプロトコル

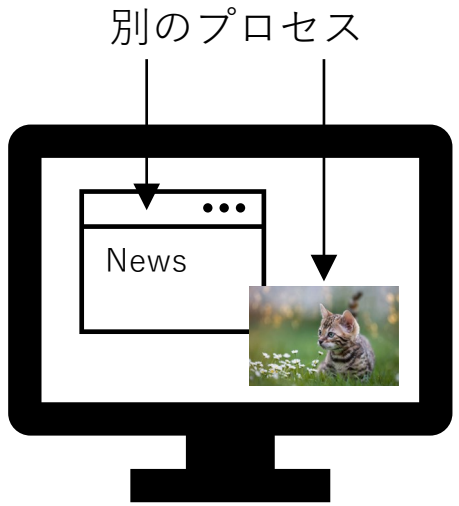


- IPアドレスとドメイン名
  - 人間がIPアドレスを記憶するのは大変
  - 組織毎に割り当てられたドメイン名とホスト名で通信機器を表す

    - FQDNとIPアドレスの対応を管理するものがDNS (Domain Name System)
  - ドメイン名
    - 指定事業者などに申請して取得する：com, jp, …　申請・継続に費用がかかる
    - 一部のドメインは使用者が限定される： go.jp: 政府機関等、ac.jp: 教育機関等

(3) 情報通信ネットワークのプロトコル

- トランスポート層
  - OSから見たプロセス間の通信
  - 正確に情報を送るために確認・再送を手順化したTCPと、リアルタイム性を重視して取りこぼしを認めるUDPがある
  - IPアドレスにポート番号を付けて送信
    - 例） 127.0.0.1:80
    - いくつかのポート番号はアプリケーション層で標準化されている
      - ✓ TCP/22 ssh，UDP/67 DHCP，TCP/443 HTTPS, …



(3) 情報通信ネットワークのプロトコル

- アプリケーション層
  - メールやwebなど、それぞれのアプリケーションで
    サーバとクライアント間などのやりとりが決められている
  - 例：HTTPステータスコード
    - 200 OK
    - 404 Not Found
    - 500 Internal Server Error

学習19 情報通信ネットワークの構築

(1)小規模なLAN の構築と情報機器

(2)情報機器をLAN に参加させる方法

(3)無線LAN の構築に関するセキュリティ

(4)ネットワークのトラブル対応

(1) 小規模なLAN の構築と情報機器

- 小規模LANの構築にあたっての検討事項
  - ルータとアクセスポイントやハブとの有線接続の環境を調べる
  - 電波状況を調べ、無線LAN アクセスポイントの機種や設置数を決める
  - 無線接続の情報機器がIEEE802.11のどの規格に対応しているのかを調べる
  - ルータの設定でセキュリティを高める場合、インターネット接続に関してどのようなプロトコルが必要なのかリストアップする
  - セキュリティを高めるためにはLANを分割する

(2) 情報機器をLANに参加させる方法

- 情報機器側の設定に必要な情報
  - SSIDの入力、暗号化キーの入力、暗号化方式の設定
- アクセスポイント/ルータの設定に必要な情報
  - SSIDの設定、暗号化キーの設定
  - DHCPによるIPアドレス配布を行うか
  - ポート番号によるフィルタリングを行うか
- 学校や企業内LANでの注意点
  - 参加の容易さとセキュリティのバランスをとる

(3) 無線LANの構築に関するセキュリティ

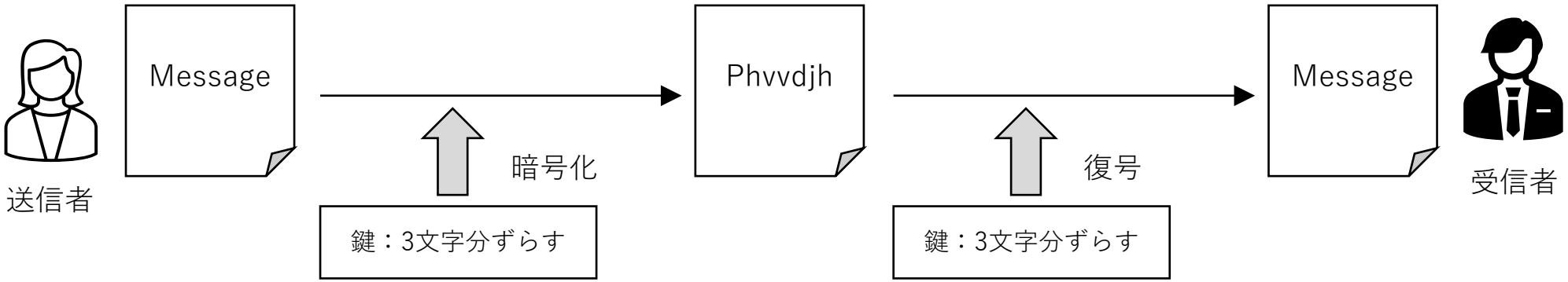
- 無線ルータや無線アクセスポイントの設定
  - 使用するIEEE802.11の規格、暗号化方式、SSID の設定、DHCPの設定、フィルタの設定などを把握しておく
  - WPSなどによる簡易接続を許可するか
  - SSIDや暗号化キーを複雑なものに変更し、場合によっては公開しないようにする
- 複数のLANを設定する場合
  - 業務用無線LANと来客用無線LANのそれぞれの設定を考えてみる

(4) ネットワークのトラブル対応

- トラブルへの対応
  - 点検を体系的に行い、それぞれの点検項目でどのようなトラブルが特定できるかを知っておく必要がある
    - 機器が正常に稼働しているか
    - 必要なネットワーク接続設定ができているか
    - 通信が可能か
    - アプリの設定が適切か

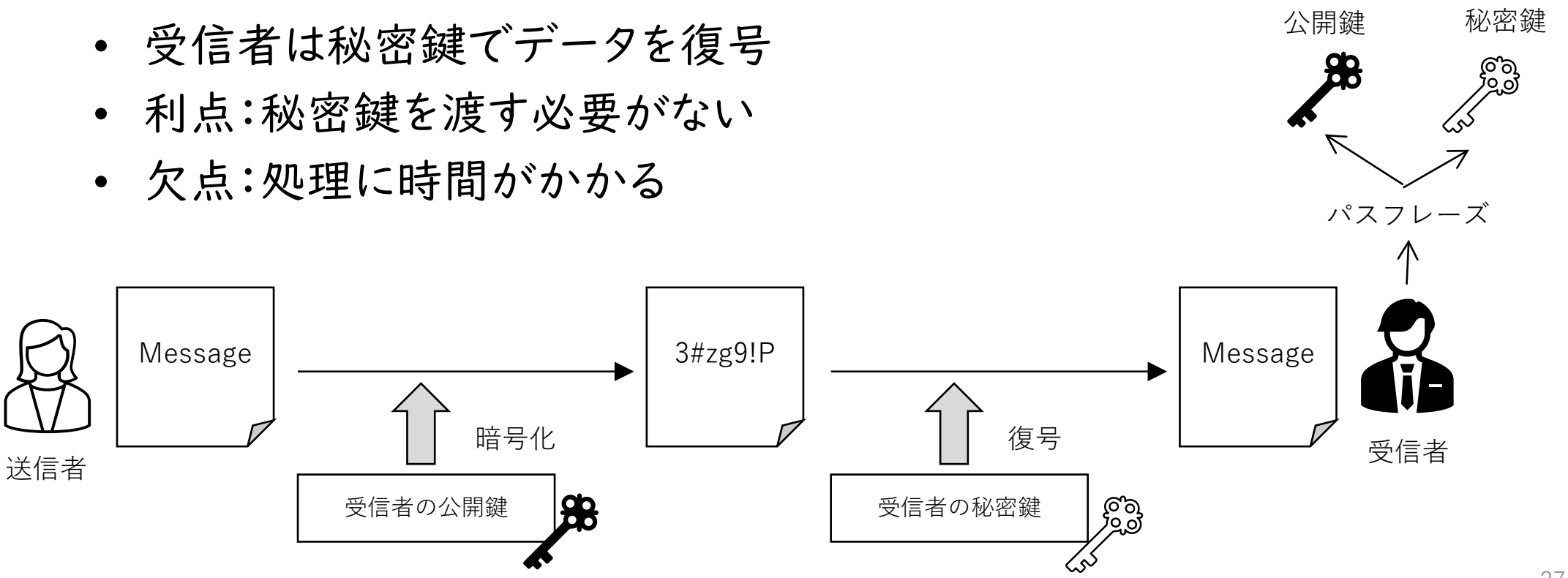
補足:暗号

- 暗号の方式
  - 共通鍵暗号
    - 1つの鍵でデータの暗号化と復号を行う
      - ✓ 例)鍵:文字コードを3文字分ずらす
        - Message → Phvvdjh
    - 利点:処理が高速
    - 欠点:鍵をどうやって渡すかが問題



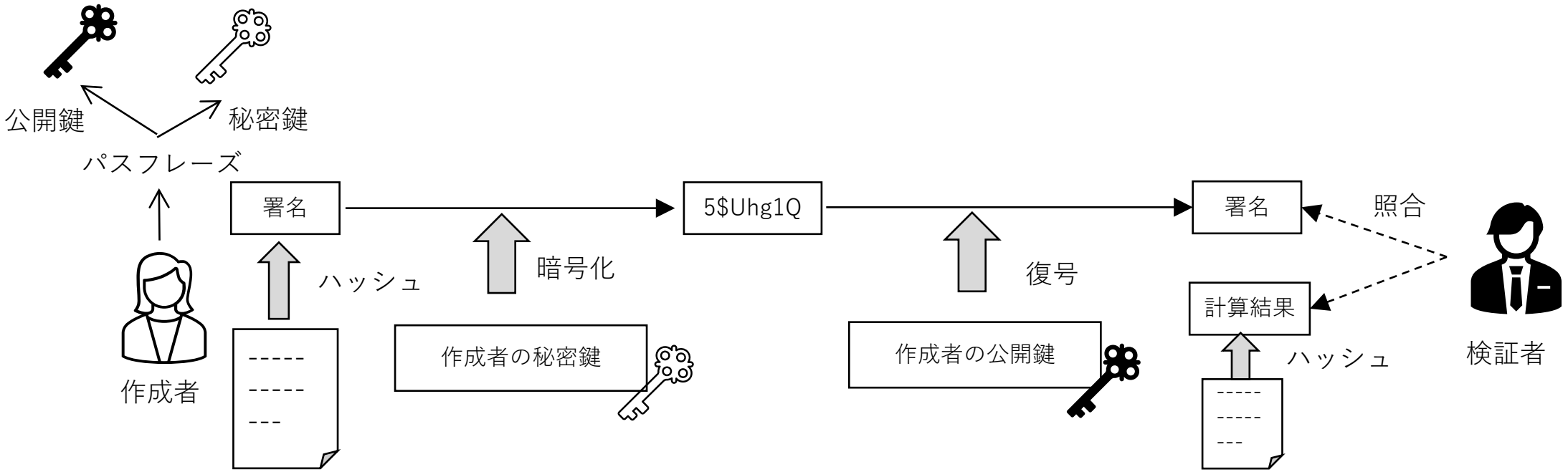
補足:暗号

- 暗号の方式
  - 公開鍵暗号
    - 受信者の公開鍵でデータを暗号化
    - 受信者は秘密鍵でデータを復号
    - 利点:秘密鍵を渡す必要がない
    - 欠点:処理に時間がかかる



補足:暗号

- デジタル署名
  - 文書作成者は文書からハッシュ関数を用いて署名を作成
    - ハッシュ関数の例:文書内の文字コードを合計したものの下4桁
  - 検証者は受け取った署名と文書から計算したものを照合



参考文献・資料

- ネットワーク
  - 井上他：マスタリングTCP/IP　入門編（第6版）、オーム社、2019.
- 暗号
  - 光成滋生：図解即戦力　暗号と認証のしくみと理論がこれ1冊でしっかりわかる教科書、技術評論社、2021.

学習20 情報システムが提供するサービス

(1)情報システムが提供するサービス

(2)オープンデータの重要性とその活用

(3)データを蓄積・管理・提供する方法

(4)国や地方公共団体が提供するオープンデータ

(5)GIS を用いたデータの可視化と問題発見

（1）情報システムが提供するサービス

- サービスの種類
  - 行政, 医療, 教育など
  - 情報通信ネットワークにより様々なデータが送受信されて運用されている
- 活用法
  - 個人情報を含むデータや企業活動の根幹にかかわるデータは情報セキュリティを確保して漏洩することがないようにする
  - 公共性が高いデータはオープンデータとして活用する

(2) オープンデータの重要性とその活用

- オープンデータの定義
  - 営利目的・非営利目的を問わず二次利用が可能
  - 機械判読可能
  - 無償で利用できる
- オープンデータ利用の効果
  - 国民参加による諸課題の解決
    - 参考：Code for Japan (https://www.code4japan.org/)
  - 行政の高度化・効率化
  - 透明性・信頼の向上

(3) データを蓄積・管理・提供する方法

- オープンデータとして公開されるデータのファイル形式
  - 統計情報など：CSVなどの表形式
    - セル結合や不用な空白の挿入などで可読性が失われている場合がある
    - 外見を整えるためにデータをゆがめたようなExcelファイルは「ネ申Excel」とよばれる
  - 報告書など：PDFなどの文書形式
    - 本来CSVで公開して欲しい情報がPDFになっており、機械処理が難しい場合がある
  - 地図情報：shpなどの地理空間情報形式

(4) 国や地方公共団体が提供するオープンデータ

- オープンデータの具体例 (https://www.data.go.jp/)
  - ◆ 国
    - 人口や世帯, 経済, 産業, 安全, 環境, 教育など省庁が調査したデータ
    - 気象庁が観測した気象データ
    - 国立環境研究所による大気汚染や騒音などの観測データ
  - ◆ 地方公共団体
    - 市町村の人口、町丁字ごとの人口や避難場所
    - AED の設置場所、フリースポットの場所、市内を走るバスに関するデータ
      - ✓ 参考：京都市オープンデータポータルサイト https://data.city.kyoto.lg.jp/appli

(5) GIS を用いたデータの可視化と問題発見

- 例題
  - 人口密度のデータとAED設置場所のデータを重ね合わせて表示することにより可視化し、設置台数が足りているかを考える
  - 手順
    - 地図で見る統計 jSTAT MAP のアカウントの作成
    - AED設置場所のデータを取得し、jSTAT MAP の形式に加工
    - 人口密度のデータを取得し、jSTAT MAP の形式に加工
    - 描画された地図から問題点を検討

学習21 さまざまな形式のデータとその表現形式

(1)リレーショナルデータベース

(2)データのさまざまな表現形式

(3)Web API によるデータの取得

(4)キー・バリュー形式のデータの処理・蓄積

(5)キー・バリュー形式のデータを用いた問題発見

(1) リレーショナルデータベース

- リレーショナルデータベースとは
  - テーブルとよばれる表形式でデータを表現
    - 正規化：データの重複をなくし、整合的にデータを取り扱えるようにテーブルを設計すること
  - テーブルの列はフィールドとよばれ、項目名を表す
  - テーブルの行はレコードとよばれ、1件分のデータを表す

書籍		
書籍ID	書籍名	作者ID
1	羅生門	1001
2	こころ	1002
3	坊ちゃん	1002
4	鼻	1001
5	舞姫	1003
6	吾輩は猫である	1002

作者	
作者ID	作者名
1001	芥川龍之介
1002	夏目漱石
1003	森鴎外

(1) リレーショナルデータベース

- リレーショナルデータベースにおける関係演算
  - 選択：テーブルから条件を満たすレコードを抽出
  - 射影：テーブルから一部のフィールドを取り出す
  - 結合：複数のテーブルを1つの表にする
  - これらの関係演算に加えてレコードの追加・削除などを行うにはSQLという言語が用いられる

補足：SQL

- SQLの文法
  - 抽出　SELECT文
  - 挿入　INSERT文
  - 更新　UPDATE文
  - 削除　DELETE文

補足：SQL

- データの抽出：SELECT文

  SELECT フィールド名 FROM テーブル名 WHERE 条件;
- 例
  - 特定のフィールドの抽出
    - SELECT 書籍名 FROM 書籍;
  - 条件で絞り込んだレコードの抽出
    - SELECT * FROM 書籍 WHERE 作者ID=1001;
  - 結合
    - SELECT * FROM 書籍 INNER JOIN 作者 ON 書籍.作者ID=作者.作者ID;

(2) データのさまざまな表現形式

- グラフ
  - 頂点と辺を用いてつながりや関係を表現したもの
  - 無向グラフ：辺の方向性を考えない
  - 有向グラフ：辺の方向性を考慮する
- グラフの表現
  - 隣接行列：行列を用いて結合を表現
  - 隣接リスト：頂点名をキー、接続している頂点のリストをバリューとしたもの

(3) Web APIによるデータの取得

- Web APIとは
  - プログラムで扱いやすい形式で、インターネット上のシステムからデータを提供する方法
  - XML形式やJSON形式でデータが提供される
  - XML形式ではタグ名がキー、内容がバリューになる
  - JSON形式ではコロンの前がキー、後がバリューになる

(4) キー・バリュー形式のデータの処理・蓄積

- キー・バリュー形式のデータの処理
  - Pythonでは辞書型で扱う
  - Redisなどのキー・バリュー形式のデータベースもあり、これらは総称して NoSQLとよばれる

(5) キー・バリュー形式のデータを用いた問題発見

- キー・バリュー形式のデータを用いた問題発見の例
  - 例）SNSで自分の友人に共通する友人で、自分とはつながっていないユーザを発見する

情報処理学会試作問題 第7問

- 解答
  - ア ② C のスイッチングハブ
  - イ ⓪ A のスイッチングハブ
    - ポイント:ルータの故障ではない理由は何か?
  - ウ ⓪ 192.168.1.11