情報Ⅰ　No.20
情報通信セキュリティ

年	2	組		番		名前	

第４章情報通信ネットワークとデータの活用　１節　情報通信ネットワークの仕組み
３・４．プロトコル～プロトコルとＩＰ・データ転送のしくみ　（教 P172－P175）

☞インターネットではどのように通信しているか理解しよう。

【TRY】自分の IP アドレス（インターネット上の住所）を右のサイトで調べよう。

自分の IP アドレス	

【知識の整理】

1　コンピュータネットワークでの通信の約束事

・（　　）＝送信側と受信側の間の通信手順やデータの形式の取り決めのこと

→（　　）＝インターネットでデータの送受信で主に使われるプロトコル

2　インターネットにおける通信のルール（TCP/IP の役割）

・送信時に、通信するデータを（　　）に分割する。

各階層で宛先やパケットの順番を示す（ヘッダ）とよばれる管理情報をデータに付加する。

元のデータ　→　データをパケットに分割　→　パケットに各階層にヘッダを付加して送る

＋順番 1/3＋宛先

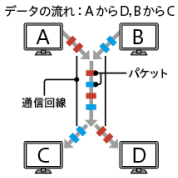
＋順番 2/3＋宛先

＋順番 3/3＋宛先

・パケットで通信すること（パケット交換方式）のメリット

→一つの通信回線を複数の人が利用することができる

⇔電話（回線交換方式）は一つの回線を独占的に使用



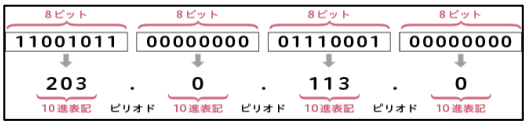
3　通信は４階層で分担して通信する

郵便で言えば・・	通信では	主なプロトコルと役割
①手紙を書く	（　　）層 ＝データを作る	・（ HTTP ）＝Web ページのやり取り ・（ SMTP ）＝メールの送信 ・（ POP ）＝メールの受信
②郵便ルールに従い準備 （例）封筒、切手、宛先	（　　）層 ＝通信の準備をする	・（　　）＝通信の信頼性を確保する ・（ UDP ）＝確実性よりリアルタイム優先 →メールは TCP、動画は UDP を使用
③宛先に届くよう投函 （例）郵便局に届ける	（　　）層 ＝宛先に届ける	・（　　）＝データを相手に届ける
④郵便局が相手に運ぶ （例）車、鉄道など	（　　）層 ＝物理的方法を選択	・（IEEE 802.11）＝無線 LAN の通信規格 ・（Ethernet）＝有線 LAN の通信規格

4　IP アドレスと枯渇問題

現在の IP アドレス：（ IPv4 ）＝2 進法 32bit で表す→2^{32} 個＝約 43 億個の割当てが可能

→8bit ずつ 10 進法で表記する



今は IP アドレス不足：（ IPv6 ）＝2 進法 128bit で表す→2^{128} 個＝約 340 澗（10^{36}）個の割当可能

→16bit ずつ 16 進法で表記　（例）ABCD:EF01:2345:6789:ABCD:EF01:2345:6789

5　ドメイン名と DNS　☞確認課題(2)

・（　　）＝IP アドレスと対応した識別するための名前
　→通信の際には（　DNS　）を利用してドメイン名を IP アドレスに変換する

組織名：ac 大学　ed 小中高校　co 企業
　　go 政府　ne ネットワークサービス
国　名：jp 日本　fr フランス　ph フィリピン
　　ca カナダ　us アメリカ　cn 中国

５．情報セキュリティ　６．７．暗号化　（教 P176―P181）

☞情報セキュリティの意味と、第三者に情報を読み取られないようにする暗号化のしくみを知ろう

【TRY】インターネット上のサービスで ID とパスワードが必要なものをあげよう。

【知識の整理】

1　情報セキュリティに求められる 3 つの要素

・（　　）＝権限がある人だけがアクセスできること→不正アクセスや情報漏洩の防止
・（　　）＝情報が正確で完全であることを確保する→情報の改ざんを阻止
・（　　）＝必要な時に情報にアクセスできる状態を確保する→システム障害の防止

2　情報セキュリティを確保する技術

・（　　）＝パスワードなどの知識情報、身分証明書などの所持情報、指紋などの（生体情報）で本人確認する技術、→これらを複数組み合わせた（　　）も多い
・（　　）＝外部ネットワークからの不正侵入を防ぐ
　→（　パケットフィルタリング　）＝不正に侵入しようとするパケットを検出し遮断する
・OS やアプリケーションソフトウェアの更新（アップデート）
　＝ソフトウェアの設計ミスなどによるセキュリティの欠陥（セキュリティホール）を修復する
・（　ウィルス対策ソフトウェア　）の導入＝マルウェアによる検知・駆除・隔離することができる

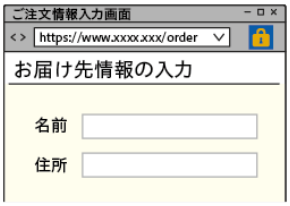
3　暗号化のしくみ

・暗号化＝第三者に情報を見られてもわからないようにする技術　☞確認課題(3)(4)

暗号化のしくみ	暗号化するとき	元に戻す（復号）するとき
（　共通鍵暗号方式　）	自分と相手しか知らない共通の鍵（秘密鍵）で暗号・復号化	
（　公開鍵暗号方式　）	受信者の（公開鍵）で暗号化	受信者の（秘密鍵）で復号化
（　電子署名・デジタル署名　）	送信者の（秘密鍵）で暗号化	送信者の（公開鍵）で復号化

4　暗号化と暗号化技術

・Web ブラウザにおける暗号技術（　SSL/TLS　）
　＝暗号技術を使って情報漏洩対策や個人情報保護を行う技術
　→https で始まる URL と錠前マークが表示される



【確認課題】**調べよう・考えよう！**

（1）次の Web ページの IP アドレスを右の IP 検索サイトを使って調べよう。

Yahoo （https://www.yahoo.co.jp）	
Google （https://www.google.com）	
学校 (https://www.assumption.ed.jp)	

（2）ドメインは個人でも申請できる。自分の Web を持つとしたらつけたい名前を考え、
ドメイン登録が可能かどうか調べよう。また 1 年間維持するのに必要な費用も調べよう。

考えたドメイン	
使用可能かの可否	
1 年間の登録費用	

☞初期サービス（〇か月無料は除いて、実際にかかる金額を調べよう）

（3）カエサル暗号（アルファベットで文字をずらして暗号化する）で自分の名前を暗号化しよう

自分の名前 ローマ字で	
暗号化 3 文字後ろにずらす	

（4）自分で暗号化の方法を考え、食べ物の名前を暗号化し、誰かに解読させてみよう。

元のデータ （ここは隠す）	
暗号化のルール （ここも隠す）	

⇩

暗号化したデータ	
解読を依頼した人 解読結果（成功？失敗？）	

【振り返り】No.20 の実習・学習で学んだこと、気づいたこと、考えたことを 3 行以上書きましょう。
