情報Ⅰ　No.20
情報通信のセキュリティ

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）

☞プロトコルの役割とＩＰについて理解しよう。

【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

・（　　）＝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

→インターネットでは（　　）が利用され（　４階層モデル　）で分担して通信を行う

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

3　４階層モデルによる通信の流れ　☞確認課題(2) (3)

４つの階層	使われるプロトコルと役割
（　アプリケーション　）層 ＝アプリケーション毎に固有の プロトコルを使う ↓送信時　　↑	（　HTTP　）＝Web ページのやり取りで使われるプロトコル →ブラウザからのリクエストに応じ情報を返すやり取り役割 （　SMTP　）＝メールをメールサーバに転送するプロトコル （　POP　）＝メールサーバからメールを転送するプロトコル
（　トランスポート　）層 ＝アプリケーションを識別し、 通信の信頼性を保障する ↓　　↑	（　　）＝通信の信頼性を確保するプロトコル →データ欠落を検知すると再送を要求し確実に届ける役割 （　UDP　）＝確実性よりリアルタイム性を優先するプロトコル →メールなどは TCP、動画のストリーミングは UDP を使う
（　インターネット　）層 ＝宛先のコンピュータに届ける ↓　　↑受信時	（　　）＝データを目的にコンピュータに届けるプロトコル →目的のコンピュータまでの（　ルーティング　）の担当 ・（　　）＝宛先を表す固有の番号
（　ネットワーク インターフェイス　）層 ＝物理的な通信手段を決める	（IEEE 802.11）＝無線 LAN の通信規格 （イーサネット・Ethernet）＝有線 LAN の通信規格

4　IP アドレスの枯渇問題

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

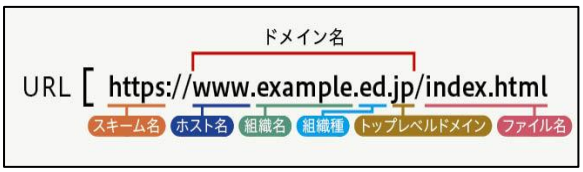
→8bi ずつ 10 進法で表記する

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

5　ドメイン名と DNS　☞確認課題(3)

・（　　）＝IP アドレスと対応した識別するための名前
　→（　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】自分が利用している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

・（　認証技術　）＝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(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(5)

【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）インターネット通信で使われるプロトコルをプリントを参考に整理しよう。

プロトコル	階層	役割
（　　）	インターネット層	データを宛先に届ける役割
（　　）	トランスポート層	IP の役割の上に、再送要求など信頼性を高める役割
（　　）	トランスポート層	IP の役割の上に、音声通話や動画な即時性を高める役割
（　　）	アプリケーション層	Web ブラウザと Web サーバ間で情報のやり取りを行う
（　　）	アプリケーション層	メールをメールサーバへ転送するプロトコル

（3）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	

（4）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	

（5）送受信するビット列に、確認用の符号としてビット列全体の「1」の数が偶数または奇数になるよう付加するビットを「パリティビット」という。このうち「1」の個数が偶数になるものを「偶数パリティ」という。例を参考に「偶数パリティ」となるように数値を加えてください。

（例）0110　→すでに 1 の数が偶数なので 0 を最後の桁に加える→　01100　＝1 が偶数個

①1000　→（　　）　②0101→（　　）　③1110→（　　）

【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。