|  |
| --- |
| 情報Ⅰ　No.20情報通信のセキュリティ |

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 年 | ２ | 組 |  | 番 |  | 名前 |  |

2024©Assumption-Kokusai

|  |
| --- |
| 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→232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→2128個＝約340澗（1036）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。

|  |
| --- |
|  |