課題１　ｇ０４０２１７　理一10組　加藤進介

１.

＊プロトコル

ネットワークを介してコンピュータ同士が通信を行なう上で、相互に決められた約束事の集合。通信手順、通信規約などと呼ばれることもある。英語しか使えない人と日本語しか使えない人では会話ができないように、対応しているプロトコルが異なると通信することができない。人間同士が意思疎通を行なう場合に、どの言語を使うか(日本語か英語か)、どんな媒体を使って伝達するか(電話か手紙か)、というように 2 つの階層に分けて考えることができるが、コンピュータ通信においても、プロトコルの役割を複数の階層に分けて考える。階層化することによって、上位のプロトコル(を実装したソフトウェア)は自分のすぐ下のプロトコルの使い方(インターフェース)さえ知っていれば、それより下で何が起きているかをまったく気にすることなく通信を行なうことができる。電話機の操作法さえ知っていれば、電話会社の交換局で何が起きているか知らなくても電話が使えるのと同じである。プロトコルの階層化のモデルは国際標準化機構(ISO)や国際電気通信連合(ITU)などによって 7 階層の OSI 参照モデルとして標準化されており、これに従ってプロトコルを分類することができる。現在インターネットで標準となっている IP は第 3 層(ネットワーク層)の、TCP や UDP は第 4 層(トランスポート層)のプロトコルであり、HTTP や FTP、SMTP、POP などは第 5 層(セッション層)以上のプロトコルである。

＊パケット

コンピュータ通信において、送信先のアドレスなどの制御情報を付加されたデータの小さなまとまりのこと。データをパケットに分割して送受信する通信方式をパケット通信と呼ぶ。データを多数のパケットに分割して送受信することにより、ある 2 地点間の通信に途中の回線が占有されることがなくなり、通信回線を効率良く利用することができる。また、柔軟に経路選択が行なえるため、一部に障害が出ても他の回線で代替できるという利点もある。

＊回線交換とパケット交換の違い

回線交換は通信する両者間に仮想的な回線を確保する方式で、接続中は専用回線を使う場合とおなじように通信でき、一定の通信速度が保証されるので、音声や動画などに適しているが、回線が確保できないと全く通信ができないことと、通信するデータがない場合でも回線を占有するため回線の利用効率が低くなることが欠点。一方、パケット交換はデータをパケットとよばれるある大きさの塊に小分けしてそれぞれに宛先をつけて配送する方式。1 パケットの送信時間以上は回線を占有しないため、回線上にさまざまな通信のパケットが混在できる。そのため回線の使用効率はよくインターネットではこちらが主流だが、遅延があり、通信速度が保証されにくいことが欠点。

＊ルーター

ネットワーク上を流れるデータを他のネットワークに中継する機器。OSI 参照モデルでいうネットワーク層(第 3 層)やトランスポート層(第 4 層)の一部のプロトコルを解析して転送を行なう。ネットワーク層のアドレスを見て、どの経路を通して転送すべきかを判断する経路選択機能を持つ。また、自分の対応しているプロトコル以外のデータはすべて破棄する。複数のプロトコルに対応したルーターをマルチプロトコルルーターと呼ぶ。

＊LAN と WAN

LAN は、より対線や同軸ケーブル、光ファイバーなどを使って、同じ建物の中にあるコンピュータやプリンタなどを接続し、データをやり取りするネットワーク。接続形態によってスター型 LAN、リング型 LAN、バス型 LAN などの種類があり、また通信制御方式によって Ethernet、FDDI、Token Ring などいくつかの種類がある。最も普及しているのは Ethernet 規格で、中でも、ツイストペアケーブルを使ったスター型 LAN である 10BASE-T や 100BASE-TX が主流。一方 WAN は、「広域通信網」の略。電話回線や専用線を使って、本社－支社間など地理的に離れた地点にあるコンピュータ同士を接続し、データをやり取りすることを言う。

＊IP アドレス

インターネットやイントラネットなどの IP ネットワークに接続されたコンピュータや通信機器 1 台 1 台に割り振られた識別番号。インターネット上ではこの数値に重複があってはならないため、IP アドレスの割り当てなどの管理は各国の NIC(ネットワークインフォメーションセンター)が行なっている。インターネットなどのネットワークは機器間の通信に IP(Internet Protocol)というプロトコル(通信規約)が用いられる。IP アドレスはこの IP で運用されるネットワークにおける個々の通信機器やコンピュータの住所のようなもの。現在広く普及している「IPv4」(Internet Protocol version 4)では、IP アドレスに 8 ビットずつ 4 つに区切られた 32 ビットの数値が使われ、「211.9.36.148」といったように、0 から 255 までの 10 進数の数字を 4 つ並べて表現する。単なる数値の羅列である IP アドレスはこのままでは人間にとっては覚えにくいため、コンピュータやネットワークに名前(ドメイン名やホスト名)がつけられている場合が多く、「DNS」(Domain Name System)というシステムによって IP アドレスとの相互変換が行なわれる。このため、普段インターネットを利用する時に IP アドレスそのものを目にしたり、意識するような場面はあまり多くない。現在の IPv4 では、32 ビットの数値で識別できる上限である約 42 億台(2 の 32 乗)までしか一つのネットワークに接続することができず(実際の運用ではこれより少なくなる)、インターネットで利用する IP アドレスが足りなくなることが懸念されている。このため、企業など多くの機器を利用するところでは、組織内ネットワークでは自由にいくらでも使えるプライベートアドレスを使い、インターネットとの境界にグローバルアドレスとのアドレス変換を行なう機器を設置するといった運用方法が普及している。また、次世代の IPv6 では 128 ビットの IP アドレスが使われ、単純計算で 2 の 128 乗、約 340 澗(かん)、約 3.40×10^{38} 個の IP アドレスが利用可能になるため、IPv6 に移行すれば当分のあいだ IP アドレスが足りなくなる心配はなくなると言われている。

＊ネットマスク、ネットワーク番号とホスト番号

ネットマスクはインターネットのような巨大な TCP/IP ネットワークは、複数の小さなネットワーク(サブネット)に分割されて管理されるが、ネットワーク内の住所にあたる IP アドレスのうち、何ビットをネットワークを識別するためのネットワークアドレスに使用するかを定義する 32 ビットの数値。ネットワークアドレス以外の部分が、ネットワーク内の個々のコンピュータを識別するホストアドレスである。サブネットマスク値から IP アドレスとビットの論理積を計算することによって、IP アドレスのネットワークアドレス部を取得できる。例えば、サブネットマスクが 2 進数で 11111111 11111111 11111111 00000000 ならば、IP アドレスのうち上位 24 ビットがネットワークアドレス、下位 8 ビットがホストアドレスである。111.18.10.2 という IP アドレスを 255.255.240.0 というサブネットマスク値を使って分割すると、この IP アドレスは、111.18.0 というネットワーク上の、ホストアドレス 10.2 のホストという意味になる。

ネットワーク番号は､IPアドレスの前半部分で記される,ネットワークのアドレスを意味する部分。プレフィクス(prefix)と呼ばれることもある。ある IPv4 アドレスのネットワーク番号は，そこに設定されているサブネット・マスクを照らすことで判断できる。例えば，IPv4 アドレスが「192.168.2.10」，サブネット・マスクが「255.255.255.0」のとき，ネットワーク番号は「192.168.2.0」となる。なお，ネットワーク番号の表記としては，ネットワーク番号のビット数をアドレスの末尾に「/」（スラッシュ）に続けて記す方法が一般的である。先ほどの例では，「192.168.2.0/24」となる。IPv6 では，前半 64 ビットがネットワーク番号に相当する。ホスト番号は、あるネットワークの中で個々のコンピュータに割り当てた番号。IP アドレスはネットワーク番号とホスト番号をつなげた構成になっている。IPv4 の場合は，IP アドレスとサブネット･マスクを照らすことで,32 ビットのうちどこからがホスト番号なのかを知ることができる。IPv6 の場合は後半 64 ビットがホスト番号となり，一般にインタフェース ID と呼ばれている。

＊ポート番号

インターネット上の通信において、複数の相手と同時に接続を行なうために IP アドレスの下に設けられたサブ(補助)アドレス。単にポートと略されることもある。TCP/IP で通信を行なうコンピュータはネットワーク内での住所にあたる IP アドレスを持っているが、複数のコンピュータと同時に通信するために、補助アドレスとして 0 から 65535 のポート番号を用いる。IP アドレスとポート番号を組み合わせたネットワークアドレスを「ソケット」と呼び、実際にはデータの送受信はソケット単位で行われる。実世界の住所で例えれば､マンションの所在地(「○○市××町 4-2-1 コーポ△△」)が IP アドレスにあたり、部屋番号(「305 号室」)がポート番号に対応する。

＊Mac アドレス

各イーサネットカードに固有の ID 番号。全世界のイーサネットカードには 1 枚 1 枚固有の番号が割り当てられており、これを元にカード間のデータの送受信が行われる。IEEE が管理・割り当てをしている各メーカーごとに固有な番号と、メーカーが独自に各カードに割り当てる番号の組み合わせによって表される。

＊共通鍵暗号と公開鍵暗号

共通鍵暗号は、暗号化と復号に共通の鍵を使う方式である。そのため、暗号文を盗聴している人が共通鍵を知っていると、平文に復号され、秘密は漏れてしまう。共通鍵として、DES や AES などがある。

公開鍵暗号は暗号文を作るときと復号するときの鍵が別である。自分用の鍵の組を作り、片方を公開して、他方を自分しか知らない秘密鍵として保つ。こうして、自分宛てに暗号化された文は自分だけが解読できるようになっている。

＊ディジタル署名とその利用方法

デジタル文書の正当性を保証するために付けられる、暗号化された署名情報。また、そのような署名を行なうための技術および一連の手順。公開鍵暗号を応用したもので、文書の送信者を証明し、かつその文書が改竄されていないことを保証する。送信者は、メッセージの原文から一定の計算手順で割り出した短いデータを文書に添付して送信する。受信者は受け取った署名データを一定の手順でこれを検証することにより、文書に署名を行なったのが送信者本人であることや、文書が通信途上で改ざんされていないことなどを確認することができる。デジタル署名は電子署名を実現するための方式の一つであり、電子署名とは紙に署名する行為を電子的に代替する技術の一般的な総称のことを指す。

＊ハッシュ関数

与えられた原文から固定長の疑似乱数を生成する演算手法。生成した値は「ハッシュ値」と呼ばれる。「要約関数」「メッセージダイジェスト」とも呼ばれる。通信回線を通じてデータを送受信する際に、経路の両端でデータのハッシュ値を求めて両者を比較すれば、データが通信途中で改ざんされていないか調べることができる。不可逆な一方向関数を含むため、ハッシュ値から原文を再現することはできず、また同じハッシュ値を持つ異なるデータを作成することは極めて困難である。通信の暗号化の補助や、ユーザ認証やデジタル署名などに応用されている。

＊イーサーネット

Xerox 社と DEC 社(現在は Hewlett Packard 社の一部門)が考案した LAN 規格。イーサネットは IEEE 802.3 委員会によって標準化された。アクセス制御には CSMA/CD を採用している。現在、特殊な用途を除いて、ほとんどの LAN はイーサネットである。イーサネットの接続形態には、1 本の回線を複数の機器で共有するバス型と、集線装置(ハブ)を介して各機器を接続するスター型の 2 種類がある。また、最大伝送距離や通信速度などによってもいくつかの種類に分かれる。10BASE-2 はケーブルに細い同軸ケーブル(Thin coax)を利用した、通信速度 10Mbps、最大伝送距離 185m、最大接続機器数 30 台のバス型 LAN。10BASE-5 は太い同軸ケーブル(Thick coax)を利用した、通信速度 10Mbps、最大伝送距離 500m、最大接続機器数 100 台のバス型 LAN。最も広く利用されている 10BASE-T は、より対線(UTP)を利用した通信速度 10Mbps、最大伝送距離 100m までのスター型 LAN。ハブの多段接続は 3 段階までである。最近では 100BASE-TX などの通信速度 100Mbps の Fast Ethernet の普及が進んでおり、1Gbps の通信を可能にする Gigabit Ethernet についても、100BASE-TX と物理層の互換性が高い 1000BASE-T を中心に普及が始まっている。なお、「イーサネット」という表現は元々10Mbps タイプの LAN 規格の名称だったが、現在は Fast Ethernet/Gigabit Ethernet を含んだ総称としての意味合いが強まっている。

＊DNS

インターネット上のホスト名と IP アドレスを対応させるシステム。全世界の DNS サーバが協調して動作する分散型データベースである。IP アドレスをもとにホスト名を求めたり、その逆を求めたりすることができる。各 DNS サーバは自分の管理するドメインについての情報を持っており、世界で約 10 台運用されているルートサーバにドメイン名と自分のアドレスを登録しておく。リゾルバと呼ばれるクライアントプログラムは、調べたいドメイン名(または IP アドレス)をまずルートサーバに照会し、そのドメインを管理する DNS サーバを調べ、その DNS サーバに情報を聞き出すことで変換を行なう。インターネット上で運用されている DNS サーバのほとんどは、カリフォルニア大学バークリー校(UCB)で開発された BIND である。

＊URL

インターネット上に存在する情報資源(文書や画像など)の場所を指し示す記述方式。インターネットにおける情報の「住所」にあたる。情報の種類やサーバ名、ポート番号、フォルダ名、ファイル名などで構成される。

＊SMTP,POP,IMAP

SMTP は、インターネットやイントラネットで電子メールを送信するためのプロトコル。サーバ間でメールのやり取りをしたり、クライアントがサーバにメールを送信する際に用いられる。
POP はインターネットやイントラネット上で、電子メールを保存しているサーバからメールを受信するためのプロトコル。現在最も広く普及している。電子メールの送信に使われる SMTP とセットで利用される。ユーザがタイトルや発信者を確認する前に、クライアントが全メールを受信してしまうため、発信者やタイトルの一覧を見てから受信するかどうか決められる IMAP を POP の代わりに利用する場合もある。POP を使うとパスワードがネットワーク上をそのまま流れるため、通信途中で盗まれるかもしれないという危険性がある。この弱点を改善し、パスワードのやり取りを暗号化したものを APOP という。
IMAP は、インターネットやイントラネット上で、電子メールを保存しているサーバからメールを受信するためのプロトコル。最初のバージョンは RFC 1730 として、改良版の IMAP4rev1 は RFC 2060 として規定されている。POP と違って、メールはサーバ上のメールボックスで管理され、タイトルや発信者を見て受信するかどうかを決めることができる。モバイル環境で特に便利な方式である。

＊HTML
Web ページを記述するためのマークアップ言語。W3C が作成している規格で、最新版は HTML 4.01。HTML は文書の論理構造や見栄えなどを記述するために使用される。また、文書の中に画像や音声、動画、他の文書へのハイパーリンクなどを埋め込むこともできる。HTML で記述された文書を閲覧するには通常 Web ブラウザを使用する。しかし、HTML 文書はテキスト文書の一種であるため、テキストエディタで HTML 文書を開き、タグごとテキスト文書として読み書きすることも可能である。HTML はもともと SGML の部分集合として策定されたが、現在は SGML の目的とはかなり異なる、独自の進化を遂げるに至っている。HTML は本来文章の論理構造を記述する言語であったが、主に Web ブラウザメーカーによる度重なる拡張の結果、単なる見栄えを記述するタグが大量に取り込まれた。しかし、HTML 4.0 では文書の論理構造を記述するという本来の目的に立ち返り、見栄えの記述は CSS を使って行なうように改められた。現在は、HTML を XML に準拠した仕様になるよう改良した XHTML が W3C 勧告として公開されている(最新版は XHTML 1.1)。W3C の仕様策定の主軸は既に XHTML に移行しており、今後は XHTML が HTML に代わり、Web ページ記述言語として徐々に浸透していくものと考えられている。

＊HTTP と HTTPS
HTTP は、Web サーバとクライアント(Web ブラウザなど)がデータを送受信するのに使われるプロトコル。HTML 文書や、文書に関連付けられている画像、音声、動画などのファイルを、表現形式などの情報を含めてやり取りできる。IETF によって、HTTP/1.0 は RFC 1945 として、HTTP/1.1 は RFC 2616 として規格化されている。
HTTPS は、Web サーバとクライアント(Web ブラウザなど)がデータを送受信するのに使われるプロトコルである HTTP に、SSL によるデータの暗号化機能を付加したプロトコル。サーバとブラウザの間の通信を暗号化し、プライバシーに関わる情報やクレジットカード番号などを安全にやり取りすることができる。Netscape Navigator や Internet Explorer など主要な Web ブラウザが対応していることから、WWW における暗号化の事実上の標準となっている。SSL は Netscape Communications 社が提唱した暗号化プロトコルで、HTTP 以外に FTP や Telnet などのプロトコルの暗号化にも使われる。

２.

＊CPU

コンピュータを構成する部品の一つで、各装置の制御やデータの計算・加工を行なう装置。メモリに記憶されたプログラムを実行する装置で、入力装置や記憶装置からデータを受け取り、演算・加工した上で、出力装置や記憶装置に出力する。1 回の命令で同時に処理できるデータの量によって 8 ビット、16 ビット、32 ビットなどの種類があり、値が大きいものほど性能が高い。また、同じビット数でも、1 秒間に実行できる命令の回数(「Hz」であらわされる)や、バスと呼ばれる周辺装置とのデータ伝走路が一度に運べるデータの量(「ビット」であらわされる)、バスが 1 秒間に行える転送の回数(「Hz」であらわされる)などに違いがあり、これらの値が大きいものほど性能が高い。厳密には、1 命令を行なうのにかかるクロック数や同時に実行できる命令数などの違いにも影響される。パソコンでは CPU の機能を一つのチップに集積されたマイクロプロセッサ(MPU)が利用され、Intel 社の x86 シリーズと各社の互換プロセッサが市場のほとんどを占めている。

＊レジスタ

マイクロプロセッサ内部にある、演算や実行状態の保持に用いる記憶素子。動作が極めて高速だが容量が小さい。一つのレジスタが記憶できる情報量(レジスタ長)が 32 ビットであるプロセッサ(CPU)を 32 ビットプロセッサ(32 ビット CPU)という。レジスタは役割によって、アキュムレータ、スタックレジスタ、プログラムカウンタ、割り込みレジスタ、フラグレジスタなどの種類があり、機能が限定されているものがある。機能が限定されていないレジスタを汎用レジスタという。

＊主記憶装置

コンピュータ内でデータやプログラムを記憶する装置。「主記憶装置」とも呼ばれる。半導体素子を利用して電気的に記録を行なうため、動作が高速で、CPU(中央処理装置)から直接読み書きすることができるが、単位容量あたりの価格が高いため大量には使用できない。また、電源を切ると内容が失われてしまうという欠点がある。このため、コンピュータにはメインメモリのほかに、ハードディスクやフロッピーディスクなどの外部記憶装置(補助記憶装置)が装備されており、利用者がプログラムを起動してデータの加工を行なう際には必要なものだけメインメモリに呼び出して使い、長期的な保存には外部記憶装置が利用される。

情報教科書及び IT 用語辞典より一部引用