東京ITスクール
TOKYO IT SCHOOL

# ネットワーク入門

目次

# 1. はじめに

## 1.1. はじめに

IT エンジニアとして業務を行う上で、プログラミング等のシステム開発の知識に加えて身に着けておくと役に立つのが、ネットワークの知識です。

普段私たちが利用しているメールや Web サイト、SNS、オンラインゲームなどのサービスは、全てネットワークの利用が前提となっており、IT に携わる方はもちろん、そうでない方にとっても切っても切り離せないものになっています。本資料では、そのようなネットワークの基礎知識を初学者向けに説明しています。

また、ネットワークに興味を持った方は、CCNA という資格に挑戦してみるのもいいでしょう。CCNA とは、世界最大手のネットワーク関連機器メーカーであるシスコシステムズ社が実施する、ネットワークエンジニアの技能を認定する試験です。

## 1.2. 各研修とのつながり

### 1.2.1 Java 研修

Java 研修では、最終的に Web アプリケーションを作成します。Web アプリケーションを作成するためのプログラミング言語はもちろん重要ですが、その Web アプリケーションが動作するのはネットワークがあるからです。ネットワークを学ぶことで、より深く Web アプリケーションを理解することができます。

### 1.2.2 組込み研修

組込みシステムに関連の深い技術として、IoT（Internet of Things）があります。IoT はモノがインターネット経由で通信することを意味します。IoT では、デバイスをインターネットに繋いだり、パソコンやスマートフォンを経由させたりするシーンが多くあるため、ネットワークの知識が重要になってきます。

### 1.2.3 インフラ研修

インフラ研修ではネットワークやサーバ、クラウドについて学習します。本資料よりも深いレベルのネットワークの知識を学ぶため、本資料でネットワークの基礎をしっかりと理解しておきましょう。

# 2. ネットワークの基礎知識

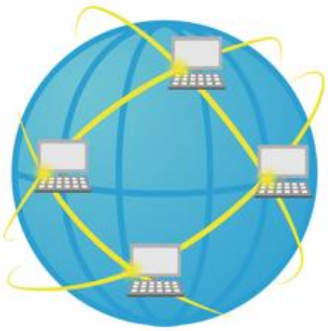
## 2.1. コンピュータとネットワーク

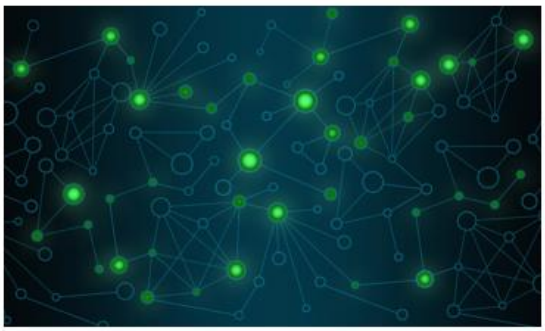
現代ではインターネットが普及し、様々なところでコンピュータが利用されるようになりました。私たちが普段コンピュータで行うメールの送受信やウェブでの検索などは、他のコンピュータと通信を行うことで成り立っています。この通信の仕組みを作り出しているのが、ネットワークです。

ネットワークという言葉は人と人のつながりを表現する場合にも利用されます。人と人のネットワークでは、会話や電話、文通をしたりすることで互いに情報のやり取りを行います。

コンピュータの世界のネットワークも、人のネットワークと同じようにコンピュータ同士を接続して互いに情報のやり取りを行います。

図 2-1　ネットワークのイメージ





### 2.1.1　ネットワークの役割

私たちが会社や家族、地域といったネットワークの中で互いに助け合って生活しているように、コンピュータも単体ではなく、他のコンピュータと相互に通信を行うことで力を発揮します。ここでは、コンピュータ同士をネットワークで接続することによって、どのようなことができるようになるのか紹介します。

■データの共有

現代ではほとんどの家庭や企業にコンピュータが導入され、様々なデータが保存・活用されています。皆さんの参加名簿や勤務情報等のデータもその 1 つです。それらのデータは、1 台のコンピュータで保存されているよりも、他の人と適切に共有されることで大きな価値を生み出します。

コンピュータ同士がネットワークに接続することで、多くの人と瞬時に情報を共有することができるようになります。皆さんのデータの場合は、研修の受講状況等を把握してもらうために、企業担当者の方に共有しています。

■リソース（資源）の共有

コンピュータ以外にもプリンターやスキャナーといったオフィス機器の利用にもネットワークは欠かせません。もしプリンターやスキャナーがネットワークに接続されていないと、毎回プリンターやスキャナーをコンピュータと接続するといった手間が発生してしまいます。

オフィスの中にネットワークを構築することで、そのネットワーク内でプリンター等の機器を共有することができるようになります。

■情報の送受信

ネットワークを利用することで、電子メールやリアルタイムチャット、個人ブログのように、情報の送受信が可能になります。

### 2.1.2　ネットワークの標準化

今ではネットワークを通じて情報のやり取りを行うことが当たり前になっていますが、ネットワークが普及し始めた当初は、ある問題が発生していました。

それは、異なるメーカーの機器同士が通信できないという問題です。機器同士の通信方法を各メーカーが独自で決めていたため、通信方法の異なる他社メーカーの機器には通信ができなかったのです。

この問題を解決するために、国際的に規格を標準化する動きが強まりました。機器等のハードウェアに関しては IEEE（Institute of Electrical and Electronics Engineers）という団体が、ネットワーク上で使用する技術に関しては IETF（Internet Engineering Task Force）という団体が標準化を行いました。

## 2.2. ネットワークの分類

コンピュータ同士を接続して互いに情報のやり取りを行う仕組みがネットワークです。そして、ネットワークはその規模によって LAN（Local Area Network）、WAN（Wide Area Network）、インターネットに分類されます。ここでは、それぞれの違いについて説明していきます。

### 2.2.1 LAN

LAN は、建物または敷地内で構築された構内通信網のことを指します。1 つの建物の中でパソコンとプリンターを接続するようなネットワークや、会社のオフィス内で何百台のコンピュータを接続するようなネットワークが LAN です。LAN はユーザが自分でネットワーク機器を配置して構築する必要があり、ネットワークの管理もユーザ自身で行わなければいけません。

### 2.2.2 WAN

WAN は、LAN 同士を接続したネットワークのことを指します。WAN を構築する場合、電気通信事業者が提供する回線を使用してネットワークを構築します。

例えばテレワークで家庭と会社間で通信を行いたい場合、家庭の LAN と会社の LAN を何らかの方法で接続しなければいけません。家庭と会社の間に自力でケーブルを伸ばして接続すればいいのですが、現実的ではありません。この場合、電気通信事業者が提供しているサービスを利用して、LAN 同士を繋ぐ WAN を構築します。

実際に WAN を構築する場合には、複数の WAN サービスからユーザの利用目的に合ったものを選択して契約する必要があります。WAN サービスの種類は様々で、専用線、広域イーサネット、IP-VPN、インターネット VPN などのサービスが存在しています。

### 2.2.3 インターネット

インターネットは、全世界の LAN や WAN などのネットワークを接続した、世界規模のネットワークのことを指します。どちらも広い範囲のネットワークのため、WAN と混同されることが多いですが、WAN はその範囲内のユーザのみしか利用できないのに対し、ネットワークは誰でも利用できるという違いがあります。

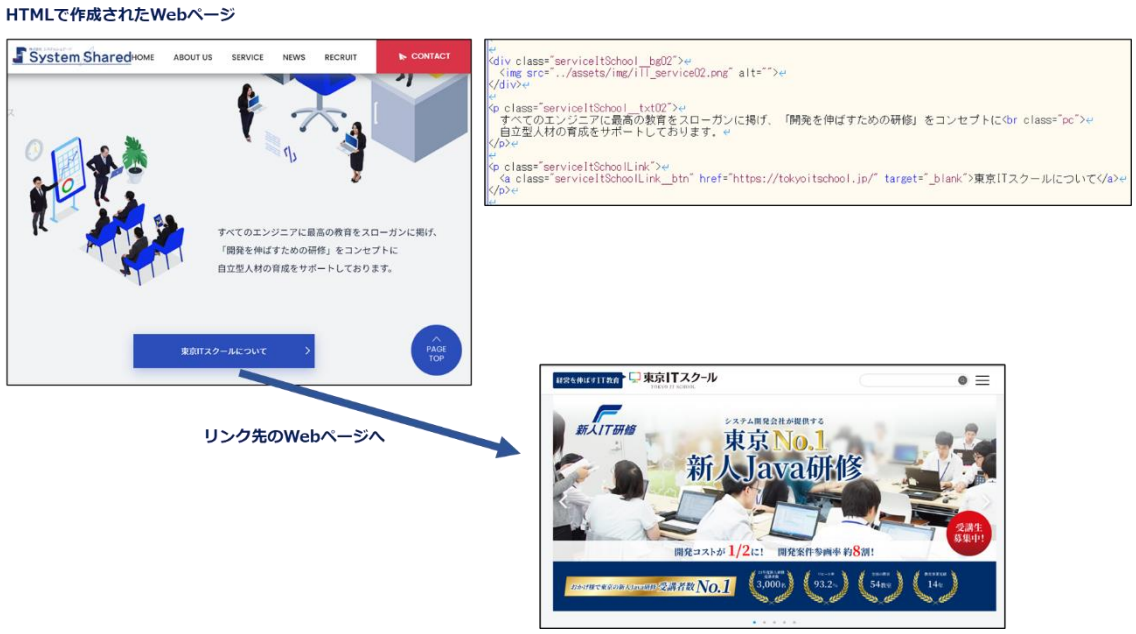
## 2.3. WWW

インターネットを利用することで、電子メールの送受信やファイルの転送、Web ページ（ブラウザに表示される 1 ページ分の情報のこと）の閲覧など様々なサービスを利用することができます。中でも Web ページの閲覧に使用する技術を「WWW（World Wide Web）」と呼びます。

WWW とは、インターネット上に公開されている Web ページ同士を結びつける仕組みのことです。

Web ページは HTML（HyperText Markup Language）という技術で作成され、画像や音声、動画など文字以外のデータも埋め込むことができます。また、Web ページには他の Web ページへのリンク（ハイパーリンク）を埋め込むこともでき、これを辿ることで、ハイパーリンクで繋がった Web ページを閲覧することができるようになります。

図 2-2　HTML で作成された Web ページ



## 2.4. ネットワーク機器

ネットワークを構築する際には、回線以外にもネットワーク機器が必要になります。ここでは、ネットワーク機器の中からルーター、モデム、ハブについて紹介します。

### 2.4.1 ルーター

ルーターは、コンピュータやプリンターといった複数の機器をインターネットに接続するための機器です。ルーターを使用することで、１つの回線で複数の機器をインターネットに接続することが可能になります。ルーターと一口に言っても、有線 LAN ルーター、無線 LAN ルーター、モバイルルーターなどの種類があります。

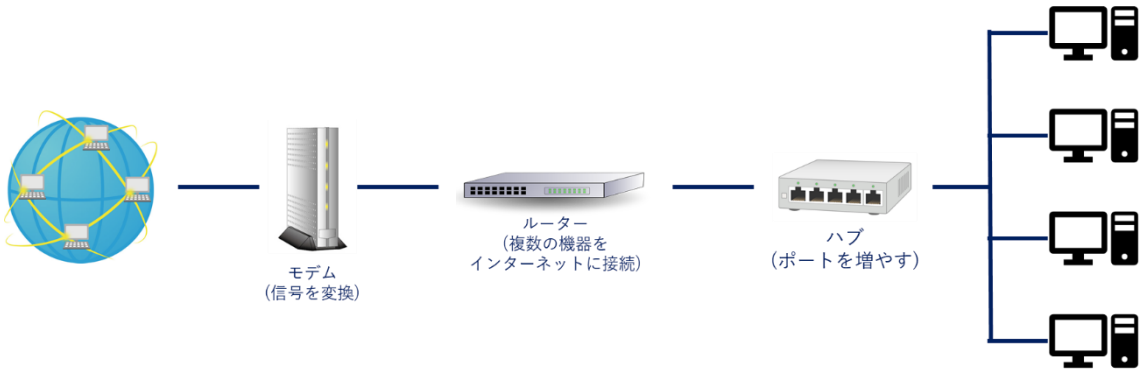
### 2.4.2 モデム

モデムは、アナログ信号をデジタル信号に、デジタル信号をアナログ信号に変換する機器です。コンピュータと回線では、使用する信号の種類が異なります。コンピュータではデジタル信号を、回線ではアナログ信号を使用します。信号の種類が異なったままだと通信をすることができないため、モデムを使用して信号の変換を行います。

### 2.4.3 ハブ

ハブは、複数の機器をインターネットへ接続したい場合に、ポート（差し込み口）を増やすための機器です。ルーターに備わっているポートは数が少ないため、接続できる機器が限られます。そのような際にハブを使用することで、ポートを増やすことができます。

図 2-3 ルーター、モデム、ハブの関係



# 3. 通信の仕組み

## 3.1. プロトコル

人と人が会話を行うときには、国や地域ごとの言葉のルールに合わせて会話を行います。当然ですが、英語がわからない方に英語で話しかけても会話は成立しません。

コンピュータも同様です。コンピュータ同士で通信をするためには、正しい手順が必要になります。その手順をルールとして定めることで、通信が可能になります。このルールのことを「プロトコル」あるいは「通信プロトコル」といいます。

プロトコルにはいくつか種類があり、以下で代表的なプロトコルを紹介します。

表 3-1　代表的なプロトコル

| プロトコル | プロトコルの概要 |
|---|---|
| IP(Internet Protocol) | データを送信先のコンピュータまで送り届ける際のプロトコル |
| TCP(Transmission Control Protocol) | 信頼性の高い通信を行う際のプロトコル |
| SMPT(Simple Mail Transfer Protocol) | インターネット上で電子メールを送信する際のプロトコル |
| POP3(Post Office Protocol version3) | インターネット上で電子メールを受信する際のプロトコル |
| FTP(File Transfer Protocol) | ファイルを送受信する際のプロトコル |
| HTTP(Hyper Text Transfer Protocol) | HTML で作成された Web ページをインターネット上でやり取りする際のプロトコル |
| HTTPS (Hyper Text Transfer Protocol Secure) | 通信内容を暗号化した HTTP |

電子メールを送信する際には電子メール送信用のプロトコル、ファイルを送受信する際にはファイル送受信用のプロトコルというように、通信の内容に応じて数多のプロトコルの中から適切なプロトコルを使用して通信を行います。

## 3.2. TCP/IP

### 3.2.1 TCP/IP とは

通信を行うには、ルール（プロトコル）に沿って通信を行う必要があります。そして、実際に通信を行う際は、1 つのプロトコルだけではなく、複数のプロトコルを使用して通信を行います。このような複数のプロトコルのセットのことを「プロトコルスイート」といいます。

プロトコルスイートにはいくつか種類があるのですが、現在広く利用されているのは「TCP/IP」というプロトコルスイートです。TCP と IP という 2 つのプロトコルが中心的な役割を果たしているため、TCP/IP と呼びます。

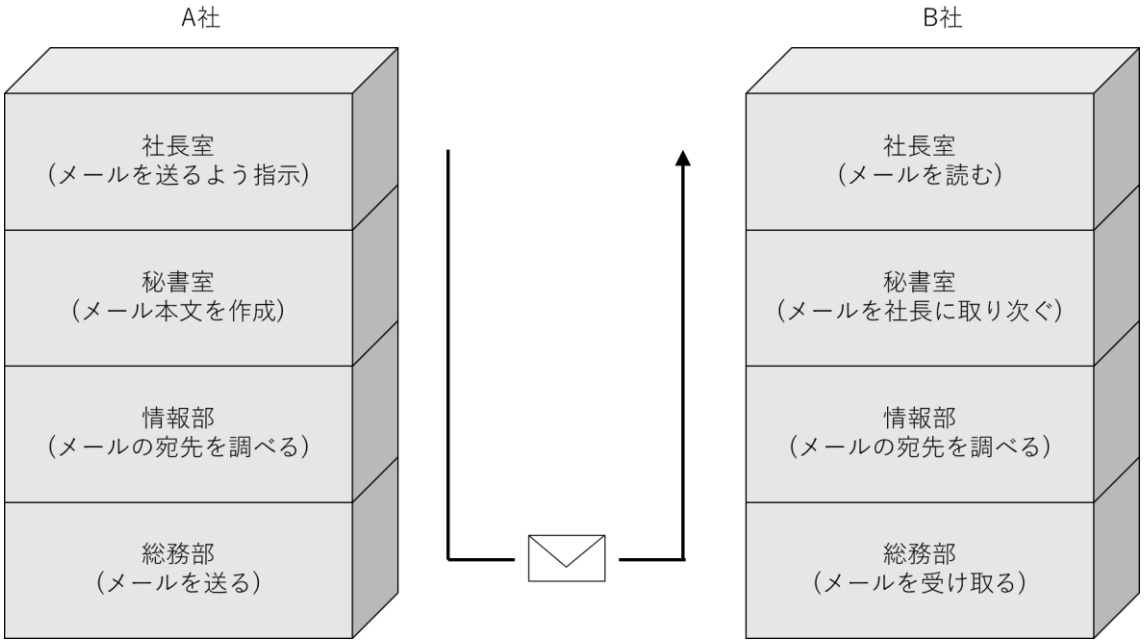
### 3.2.2 通信の階層化

TCP/IP では、通信の処理を 4 つの階層に分けて行っています。この階層のことを「レイヤー」といいます。

では、なぜレイヤーを分けて通信をするのでしょうか。レイヤー分けをすることにより、「通信の処理を単純化できる」「各レイヤーの変更が他のレイヤーに影響を及ぼさない」といったメリットがあります。

イメージしやすいように、通信を会社に置き換えて考えてみましょう。

図 3-1 通信の階層化のイメージ



この図は、A から B への通信を、A 社から B 社へのメール送信に置き換えたものです。

TCP/IP の 4 階層モデルが会社、各レイヤーが各部署だと思ってください。データを送信する際は上のレイヤーから下のレイヤー、データを受信する際は下のレイヤーから上のレイヤーを通るため、メール送信の流れも同じようになっています。

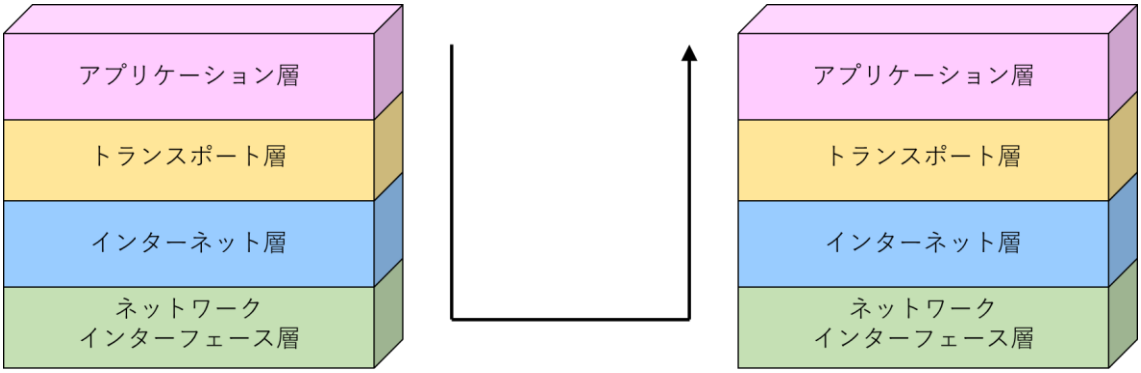
例えば、A社の総務部の担当者が退職したとしましょう。この場合、新しい総務部の担当者を雇う必要があるのですが、新しく雇われた担当者はメール送信という作業全体を把握する必要はありません。メールの送り方だけを把握すればいいのです。

このように部署毎で分けることによって、各部署で行う処理が単純化され、また、各部署の変更が他の部署へ影響することもありません。これが通信をレイヤー分けする理由です。

### 3.2.3　TCP/IP の 4 階層モデル

通信をレイヤー分けする理由について説明したところで、次は TCP/IP のレイヤーについて説明していきます。

図 3-2　TCP/IP の 4 階層モデルのイメージ




この図は、TCP/IP をレイヤー分けしたものになります。レイヤー毎にルール（プロトコル）が定められており、各レイヤーのルールに従って処理をすることで、正しく通信が行われます。

■アプリケーション層

アプリケーション層は、アプリケーションが通信を行う際のルールが定められています。

通信の種類によって使用するプロトコルが異なり、例えば Web ページへのアクセスに関する通信は HTTP/HTTPS、メールの送受信に関する通信は SMTP/POP3、ファイルの転送に関する通信は FTP を使用します。

■トランスポート層

トランスポート層は、信頼性の高い通信を行うためのルールが定められています。

通信をする際、必ずデータの送信に成功するとは限りません。また、送信に成功してもデータが欠けてしまうことも考えられます。そこで、データの送信に失敗した場合や、データが欠けてしまった場合を考慮し、通信の信頼性について定めています。

■インターネット層

インターネット層は、データを送信先のコンピュータまで送り届けるためのルールが定められています。

■ネットワークインターフェース層

ネットワークインターフェース層は、同じネットワーク上のコンピュータやその他機器との通信に関するルールが定められています。

ここまでの内容をまとめると、以下の表のようになります。

表 3-2　TCP/IP の 4 階層モデルの役割

| レイヤー | 役割 | 主な使用プロトコル |
|---|---|---|
| アプリケーション層 | アプリケーションが通信を行う際のルールを定める | HTTP 、 HTTPS 、SMTP、POP3、FTP |
| トランスポート層 | 信頼性の高い通信を行うためのルールを定める | TCP、UDP |
| インターネット層 | データを送信先のコンピュータまで送り届けるためのルールを定める | IP、ICMP |
| ネットワークインターフェース層 | 同じネットワーク上のコンピュータやその他機器との通信に関するルールを定める | イーサネット、Wi-Fi |

## 3.3. IP アドレス

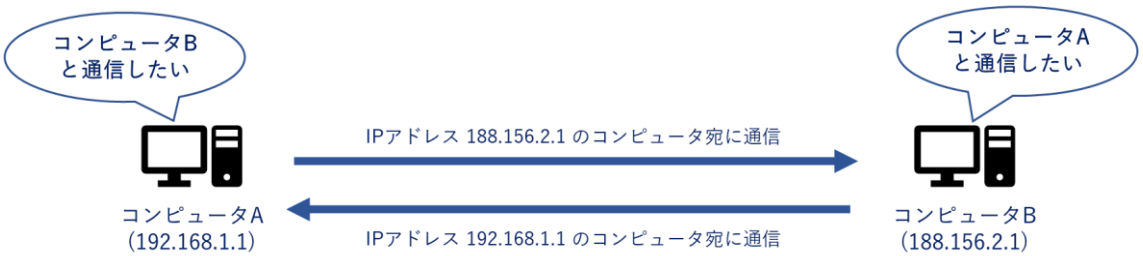
先ほどは、通信を行う際の主流のプロトコルである TCP/IP について説明しました。ここからは、通信の仕組みをより理解するための知識を紹介していきます。

### 3.3.1 IP アドレスとは

TCP/IP の 4 階層モデルのインターネット層では、データを送信先のコンピュータまで送り届けるためのルールを定めています。具体的には「IP」というプロトコルを使用します。IP は、送信先を特定するために「IP アドレス」という値を使用します。

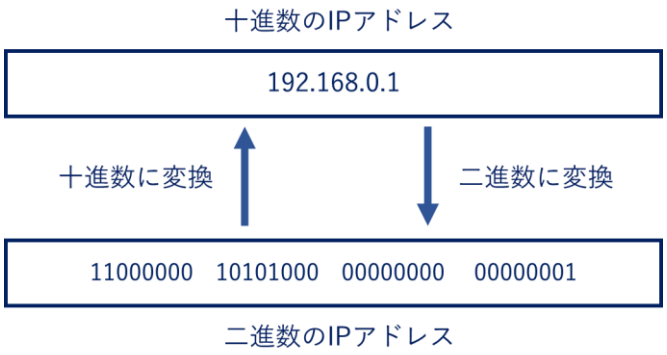
現実の世界で誰かに荷物を送る際には、宛先となる住所が必要です。IP アドレスはコンピュータの世界の住所の役割を果たしています。各コンピュータにはそれぞれ異なる IP アドレスが割り振られ、その IP アドレスを利用して送信先のコンピュータを特定します。

図 3-3　IP アドレスのイメージ




IP アドレスは 32 ビットの二進数で構成されていますが、それだと 0 や 1 ばかりで分かりにくいので、十進数に変換して表記します。変換する際には 32 ビットの数値を 8 ビット毎に 4 つに区切り、区切られた部分を十進数の 0～255 に変換します。そして、各値をピリオドで繋ぎます。この際、ピリオドで区切られた 8 ビット毎の単位を「オクテット」と呼びます。

図 3-4　IP アドレスの変換



**【コラム】自分のパソコンの IP アドレスを確認してみましょう**

Windows を利用している場合は、コマンドプロンプトを起動して「ipconfig」と打ち込むと、IP アドレスを確認することができます。「IPv4 アドレス」と書かれているアドレスが、あなたのパソコンの IP アドレスです。

### 3.3.2 IPv4 アドレスと IPv6 アドレス

現在利用されている IP アドレスは、「IPv4 アドレス」と「IPv6 アドレス」の 2 種類が存在しています。通常、IP アドレスといった場合は IPv4 アドレスのことを指します。

IPv4 アドレスは、理論上約 43 億の機器を識別することが可能ですが、インターネットに接続する機器の増加によって、利用できる IP アドレスの数が枯渇しそうな状況になっています。

そこで考案されたのが、IPv6 アドレスです。IPv6 アドレスは IPv4 アドレスと異なり、128 ビットを使用して IP アドレスを表現します。それにより、約 340 澗の機器を識別することができます。また、IPv6 アドレスは 16 進数を使用する点も大きな特徴です。

図 3-5　IPv6 アドレス


### 3.3.3 グローバル IP アドレスとプライベート IP アドレス

IP アドレスは、「グローバル IP アドレス」と「プライベート IP アドレス」に分類することができます。

グローバル IP アドレスは、インターネットに直接接続しているコンピュータ等の機器に割り振られる IP アドレスで、インターネット上の機器を識別するために重複しないようになっています。

プライベート IP アドレスは、インターネットに直接接続していないコンピュータ等の機器に割り振られる IP アドレスで、家庭や企業等の内部ネットワークで使用されます。グローバル IP アドレスとは異なり、ネットワークが別であれば重複しても問題ありません。

## 3.4. ポート

### 3.4.1 ポートとは

ポート番号とは、通信の際にデータがインターネットとコンピュータ等の機器を行き来する際に通るドアのようなものです。TCP/IP の 4 層モデルの中のトランスポート層において、通信を行うアプリケーションを識別するために利用します。

通信の際、IP アドレスを使用することで、通信相手のコンピュータを識別することができます。ただ、そのコンピュータ内のどのアプリケーションと通信を行うかは IP アドレスでは判断できません。そこでポート番号を使用することで、相手のコンピュータのどのアプリケーションと通信するべきなのか判断しています。

ポートには港という意味があります。船が出入りする港が数多くあるように、ポート番号も 6 万以上存在します。ポート番号は IP アドレスと異なり単純な数字で表現されていて、その範囲は 0～65535 となっています。

**【コラム】自分のパソコンが利用しているポート番号を確認してみましょう**

Windows の場合、コマンドプロントを起動して「netstat –n」と入力することで他のコンピュータとの接続状態を確認することができます。コマンドを実行すると、通信に利用しているプロトコルや自分と相手の IP アドレス、自分と相手のポート、接続状態が表示されます。

図 3-6　netstat コマンドの実行例

### 3.4.2　ウェルノウンポートと登録済みポート

0～65535 まであるポートのうち、0～1023 までのポート番号は「ウェルノウンポート」と呼ばれ、著名なサービスが使用するためのポート番号です。サービス毎に使用するポート番号が決められています。(下表参照)

1024～49151 は「登録済みポート」と呼ばれ、こちらも利便性の観点から利用するサービスとポート番号が決まっています。

そして、残りの 49152～65535 は使用するサービスが決められていないポートで、目的を問わずに自由に利用することができます。

表 3-3　代表的なウェルノウンポート

| ポート番号 | プロトコル | 用途 |
|---|---|---|
| 80 | HTTP | Web へのアクセス |
| 110 | POP3 | メールボックスの読み出し |
| 143 | IMAP4 | メールボックスへのアクセス |
| 25 | SMTP | サーバ間のメール転送 |
| 587 | SMTP Submission | PC からメールサーバーへのメール送信 |
| 443 | HTTPS | 暗号化した Web へのアクセス |
| 22 | SSH | 暗号化されたコンピュータへのアクセス |

どのサービスがどのポート番号を利用するかは IANA（Internet Assigned Numbers Authority）という組織によって管理がされていて、ポート番号のルールについても IANA が定めています（下記 URL 参照)。

IANA が定めるルールを無視してポートを利用することもできますが、多くのプログラムはこの割り当てに則って通信をする想定で作られています。不具合を起こさないためにも、何か特別な理由がない限りはこのルールに従うようにポートを利用するのが良いでしょう。

Service Name and Transport Protocol Port Number Registry（IANA）

https://www.iana.org/assignments/service-names-port-numbers/service-names-port-numbers.xhtml

## 3.5. ドメイン名と DNS

### 3.5.1 ドメイン名とは

通信の際、IP アドレスを使用して送信先のコンピュータを特定します。しかし、数字で表す IP アドレスは人間には扱いにくく、打ち間違いや他の IP アドレスと区別するのが難しいという問題があります。

そこで登場したのが「ドメイン名」です。ドメイン名は IP アドレスを人間にもわかりやすく文字で表したものです。「www.amazon.co.jp」や「www.google.co.jp」がドメイン名です。

ドメイン名は世界中で同じものが存在しないように専門の組織によって管理されています。また、ドメイン名はピリオドで区切られており、一番右側からトップレベルドメイン、セカンドレベルドメイン、サードレベルドメイン、フォースレベルドメインという構成になっています。

図 3-7　ドメイン名の構成


表 3-4　各レベルのドメインの説明

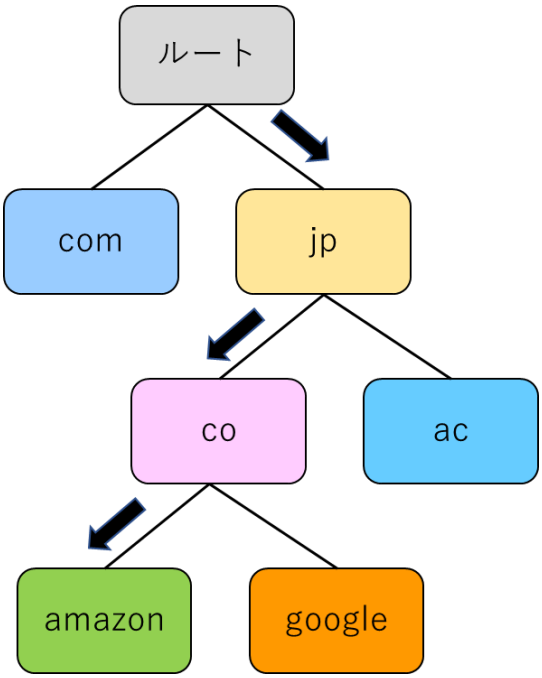
| ドメインレベル | 説明 | ドメイン名の例 |
|---|---|---|
| トップレベル<br>ドメイン | 国別や地域、商用であることを表す | jp (日本)、us (アメリカ)、com (商用) |
| セカンドレベル<br>ドメイン | 組織の種類を表す | co (一般企業)、ac (教育機関) |
| サードレベル<br>ドメイン | 具体的な企業名や組織を表す | amazon(アマゾン)、google(グーグル) |
| フォースレベル<br>ドメイン | コンピュータ(サーバ)を表す | www(Web サーバ) |

### 3.5.2　DNS の仕組み

数字で表す IP アドレスは人間にはわかりにくいため、わかりやすいドメイン名を使用してコンピュータを特定すると説明しました。ただ、ドメイン名を使用することで IP アドレスが不要になったわけではありません。ドメイン名からコンピュータを特定する際、ドメイン名を IP アドレスに変換してコンピュータを特定します。この変換の仕組みのことを「DNS（Domain Name System）」といい、IP アドレスとドメイン名を変換する処理のことを「名前解決」といいます。

ドメイン名はレベル毎に階層構造で管理されており、トップレベルドメイン、セカンドレベルドメイン、サードレベルドメインと辿ることで目的のドメイン名を探し出し、名前解決を行います。

図 3-8　DNS の仕組み（amazon.co.jp の場合）




**【コラム】ドメイン名に対応する IP アドレスを調べてみましょう**

Windows の場合、コマンドプロントを起動して「nslookup 3sss.co.jp」のように nslookup の後にドメイン名を指定することで、ドメイン名に対応する IP アドレスを調べることができます。

## 3.6. NAT

### 3.6.1 アドレス変換技術

IP アドレスを割り振る際、インターネット上の機器にはグローバル IP アドレスを割り振り、家庭や企業等の内部ネットワークにはプライベート IP アドレスを割り振ります。

プライベート IP アドレスはインターネット上で通信することができないため、内部ネットワーク内の機器からインターネットへ通信する場合は、プライベート IP アドレスをグローバル IP アドレスへ変換する必要があります。

アドレス変換には、「NAT（Network Address Translation）」という仕組みを利用します。通常はインターネットとの境界点となるルーターがこの変換を行います。NAT 専用の機器を使用する場合もありますが、NAT 機能が備わったルーターを使用するのが一般的です。

図 3-9　アドレス変換のイメージ


### 3.6.2 NAT の仕組み

NAT は、いくつかのグローバル IP アドレスをルーターで保持しておき、内部ネットワーク内の機器がインターネットへ通信する際に、保持しておいたグローバル IP アドレスを割り当てることでアドレス変換を行います。インターネットから内部ネットワーク内の機器へ通信を行う場合も同様の変換を行います。

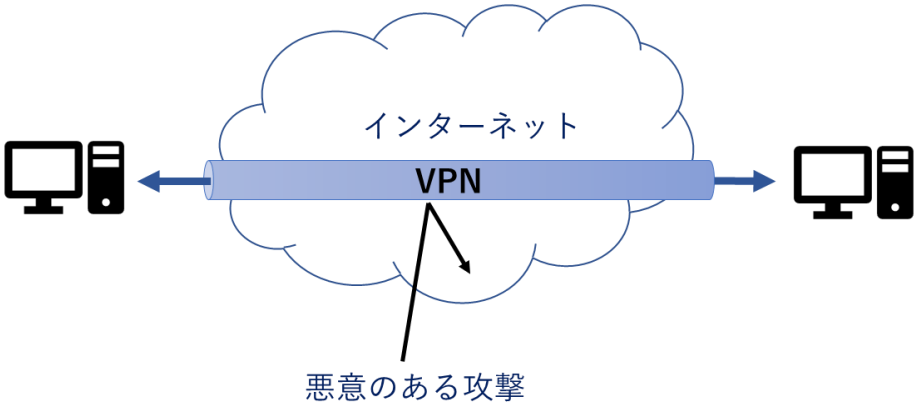
同時に通信する機器の数だけグローバル IP アドレスが必要になるため、もし利用できるグローバル IP アドレスが 1 つしかなければ、同時にインターネットを利用できる機器は 1 台だけということになります。

## 3.7. VPN

VPN（Virtual Private Network）は、異なるネットワークの間に特定の人のみが利用できる仮想的な通信回線を作成する技術です。

例えば機密性の高いデータを送信するとします。データはインターネットを通って送信されますが、インターネットは公共の道路のようなもので、第三者にデータを見られるリスクが伴います。そこで、第三者にデータを見られないようにするために、特定の人のみが利用できる通信回線を利用することで、安全にデータの送信が行えます。

図 3-10　VPN のイメージ




VPN が普及する前は、安全に通信を行うために通信事業者が提供する専用の通信回線（専用線）を利用していました。ただ、企業や拠点毎に専用線を敷設する必要があったため、費用が高くなってしまうというデメリットがありました。

そこで注目されたのが、インターネットです。世界中に張り巡らされているインターネットを使用することで、専用線を敷設する費用を抑えられるようになりました。インターネット上に専用線を用意し、そこを通る通信を暗号化することで、費用を抑えつつ安全に通信することが可能になります。

ただし、メリットばかりではありません。VPN を利用すると、普通にインターネットを利用する場合に比べて費用がかかってしまうのと、僅かに通信速度が低下してしまうというデメリットがあります。また、専用線を敷設する場合に比べると、安全性も劣ってしまいます。