ネットワーク全般　基礎知識

2025年4月3日

改定履歴

版数	発行日	改訂内容
第1版	2025年4月3日	初版発行

資料の内容は2025/4/3 時点のものです。製品のアップデートにより変更となる場合がございます旨でご了承ください。

Agenda

1. 前提情報
    1. 前提条件
    2. 本書の目的とゴール

2. ネットワークの基本
    1. ネットワークとは
    2. ネットワークの種類
    3. ネットワーク機器の種類
    4. まとめ

3. IPアドレスと通信の基礎
    1. IPアドレスとは
    2. IPアドレスの構成
    3. グローバルIPとプライベートIP
    4. NATと通信の流れ
    5. IPv4 とIPv6について
    6. OSI参照モデル
    7. TCP/IP参照モデル
    8. TCP・UDPの違い
    9. まとめ

4. ネットワークプロトコル
    1. ネットワークプロトコルとは
    2. HTTP/HTTPSの仕組み
    3. 一般的なプロトコル
    4. まとめ

5. DNS
    1. DNS基本
    2. Azure DNS（クラウド環境でのDNS管理）
    3. まとめ

6. クラウドネットワーク
    1. オンプレとクラウドネットワークの違い
    2. ハイブリッドクラウド環境について
    3. まとめ

7. セキュリティ
    1. ファイアウォールとは
    2. ネットワークの通信を制御する仕組み
    3. ファイアウォールとポート制御
    4. インバウンド・アウトバウンドルール
    5. ポート開放とセキュリティリスク
    6. まとめ

1. 前提情報

1.1. 前提条件

・本書に記載するサービス仕様、サービス名称などの各情報については、2025年4時点でのサービス仕様に基づくものとしております。

・本書は、Windows Server 2022のキャプチャを利用しております。

・ドメイン参加済みの Windows Server 2022 を使用することをお勧めします。 Microsoft Entra Connect は Windows Server 2016 にデプロイできますが、Windows Server 2016 は延長サポートであるため、この構成に支援が必要な場合は有償サポート プログラムが必要になることがあります。

1.2. 本書の目的とゴール

目的

クラウド環境では、オンプレミスと異なるネットワークの概念や構成が求められるため、
基本的なネットワークの仕組みを理解することで、Azureの学習をスムーズに進めることができます。
本資料では、Azureを学ぶ前に必要となるネットワークの基礎となるIPアドレス、ネットワーク機器、プロトコル、セキュリティなどの基本概念を学び、習得することを目的としています。

ゴール

本資料を学ぶことで、以下の内容を理解し、Azureネットワークの概念にスムーズに移行できる状態を目指します。

1. **ネットワークの基本構造と種類**
2. **IPアドレスの仕組みや通信の基礎**
3. **主要なネットワークプロトコルの役割**
4. **DNSの仕組みとAzure DNSの活用**
5. **クラウドネットワークの特徴と設計の考え方**
6. **ファイアウォール、ポート制御、インバウンド・アウトバウンド通信の概念を理解する**

2. ネットワークの基本

2.1. ネットワークとは

■ネットワークとは

ネットワークとは、通常、コンピューター、スイッチ、ルーター、プリンター、サーバーで構成されるネットワーク対応デバイスの集合です。 ネットワークは私たちの日常生活に欠かせないものであり、自宅、職場、公共の領域に存在します。
ネットワークによって、あらゆる種類のネットワーク対応デバイスが通信できるようになります。

■ネットワークの役割

主な役割は以下の通りです。

- データの共有（ファイル共有、クラウドストレージ）
- 通信（メール、チャット、ビデオ通話）
- リソースの共有（プリンタ・サーバー・インターネット接続の共有）
- ビジネスの効率化（企業のシステム連携、クラウド活用）

現代のITシステムはネットワークなしでは成り立たないため、基本を理解することが重要です

2.1. ネットワークとは

■ネットワークの基礎を学ぶ必要性について

Azureには**「IaaS」「PaaS」「SaaS」**というサービスモデルがあり、その中で **「IaaS」**は仮想マシン（VM）や仮想ネットワーク(Vnet)などのインフラ部分をクラウド上で提供するサービスを指します。

右の図は Microsoft社が公開しているモデルで、責任共有モデルに基づく一般的な責任範囲を表しており、IaaS の **[ネットワーク制御]**は**利用者の責任**となっています。

Azureのサービスには仮想ネットワーク(Vnet)やネットワークセキュリティ(NSG)などのネットワーク設定が必須であり、何か問題が発生した際にも切り分け等の対応できるよう、クラウドの基盤となるネットワークの基礎的知識は必要不可欠です。

共同責任モデル（責任共有モデル）

		オンプレミス	IaaS	PaaS	SaaS
顧客の責任範囲	情報とデータ				
	デバイス				
	アカウントとID				
クラウドサービスの種類によって責任範囲が変わる	ID・ディレクトリの基盤				
	アプリケーション				
	ネットワーク制御				
	OS				
クラウドサービスプロバイダーの責任範囲	物理ホスト				
	物理ネットワーク				
	物理データセンター				

利用者責任　共同責任　サービス提供者責任

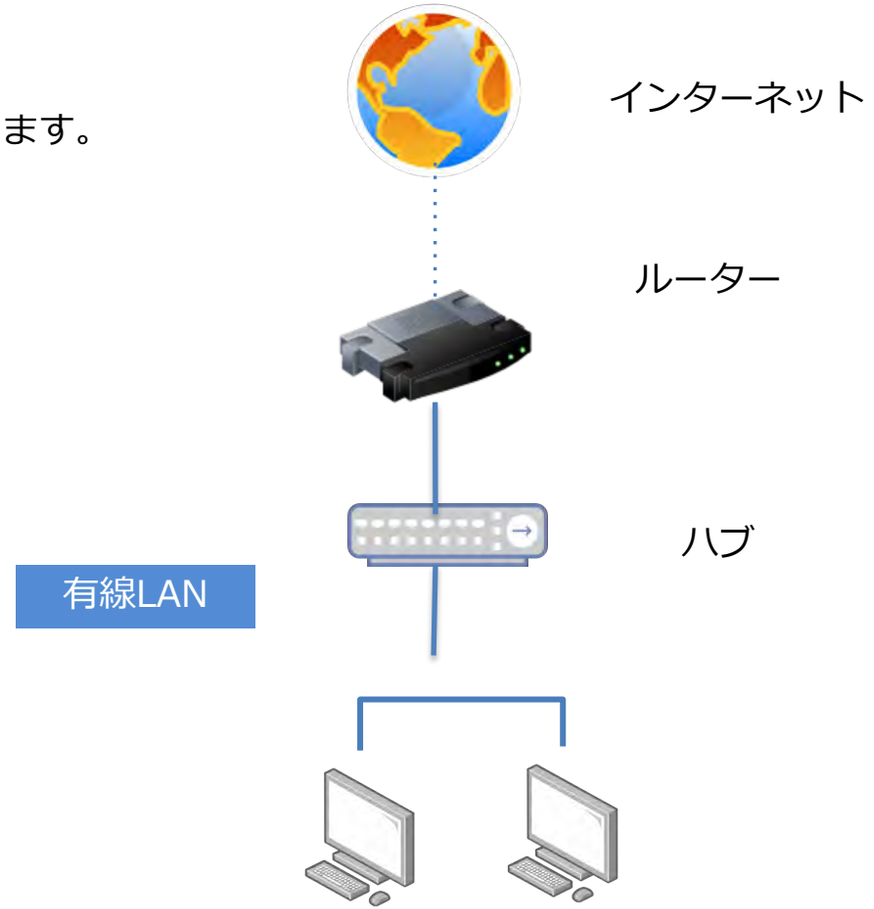
2.2. ネットワークの種類

ネットワークは「 **LAN** 」と「 **WAN** 」「**VPN**」と、大きくわけて3種類あります。

■LAN（Local Area Network)

LANは会社や学校、家庭などの狭い範囲で構成される小規模なネットワークのことです。
LANは、ルーターやスイッチを使って、パソコンやスマホ、プリンターなどをつないでいます。

<例>
家のWi-Fi ： 家の中のスマホやパソコンをつなぐ
会社の同じフロア内のパソコン ： パソコン同士がつながっている



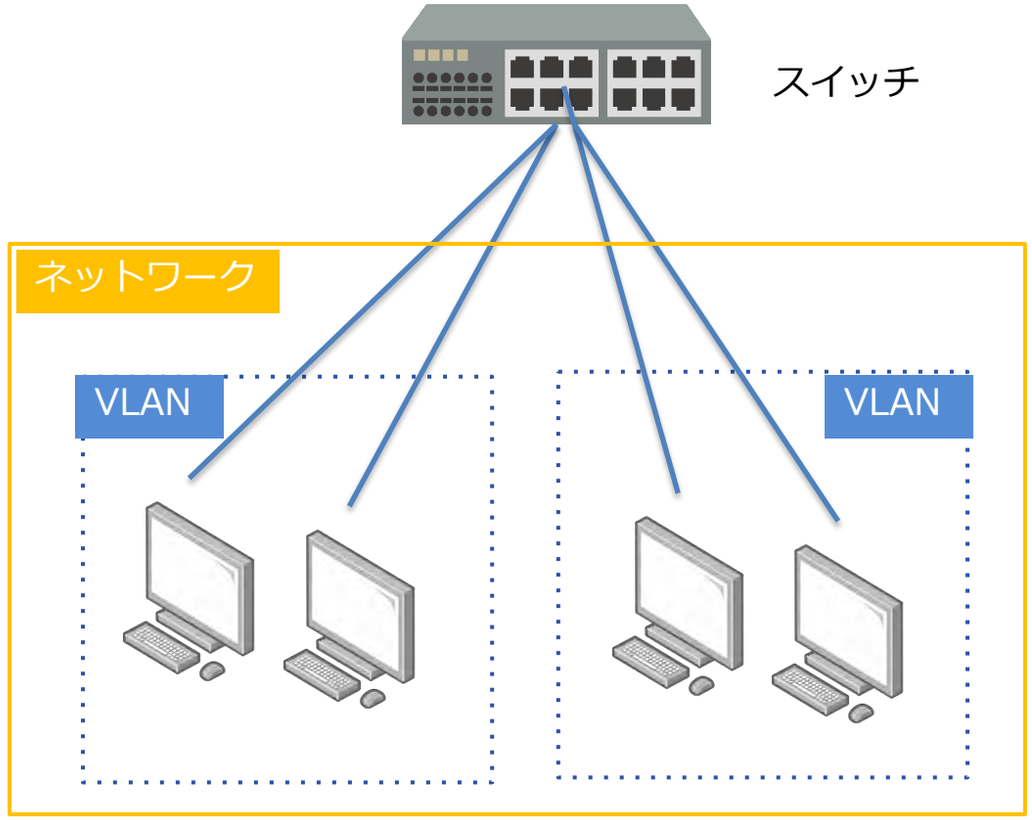
2.2. ネットワークの種類

■VLAN（Virtual Local Area Network)

LANの構成方法の一つとしてVLANという技術があります。
VLANは１つの物理的なネットワークを「複数の独立した仮想ネットワークに分ける技術」です。
異なる場所にあるデバイスを同じネットワークに属させたり、同じ場所にあるデバイスを異なるネットワークに割り当てたりすることができます。

物理的なLANで機器同士を接続していくと、ネットワークの数にあわせてルーターやスイッチなどの機器が必要になりますが、VLANを活用すれば、ひとつの物理的なネットワーク環境のうえにいくつもの仮想的なネットワーク環境を構築できるようになります。

１つのネットワークを複数の仮想ネットワークに分けることで、企業や組織はネットワークの柔軟性とセキュリティを大きく向上させることが可能になります。



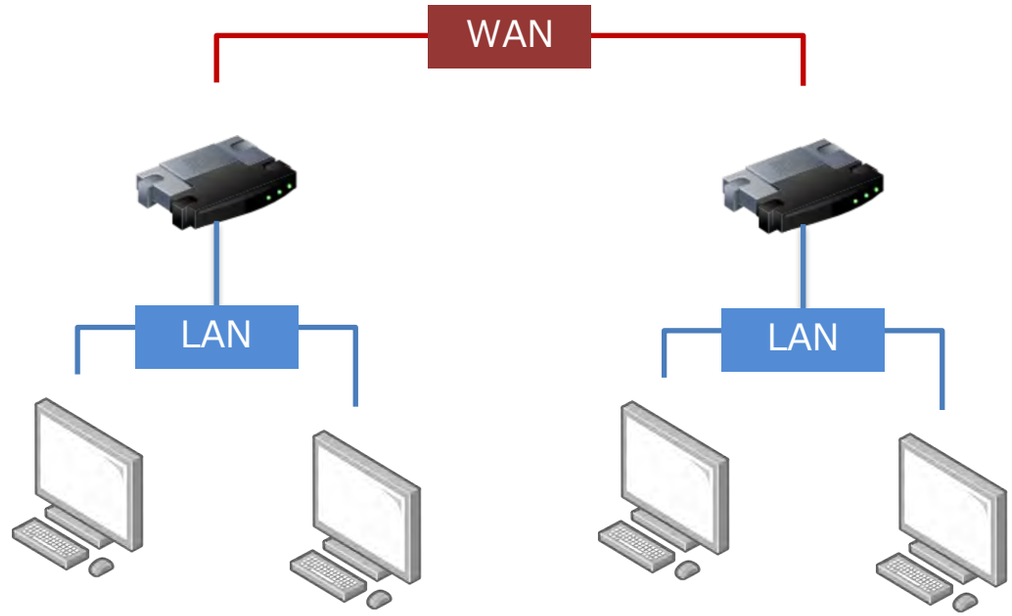
2.2. ネットワークの種類

■WAN（Wide Area Network）

WANとは広範囲にわたるネットワークのことで、細かくいうとLANとLAN同士を繋ぐ（離れた拠点同士を繋ぐ）大きなネットワークです。

LANは限定的なエリアのネットワークであった一方で、WANは遠く離れた場所と繋がっているネットワークであり、広い範囲で接続できる点が最大の特徴です。

そしてWANを世界規模で実現しているのが「インターネット」で、LAN同士が繋がりWANという大きなネットワークが構築されることで、世界中の人たちと自在にコミュニケーションが可能となっています。



2.2. ネットワークの種類

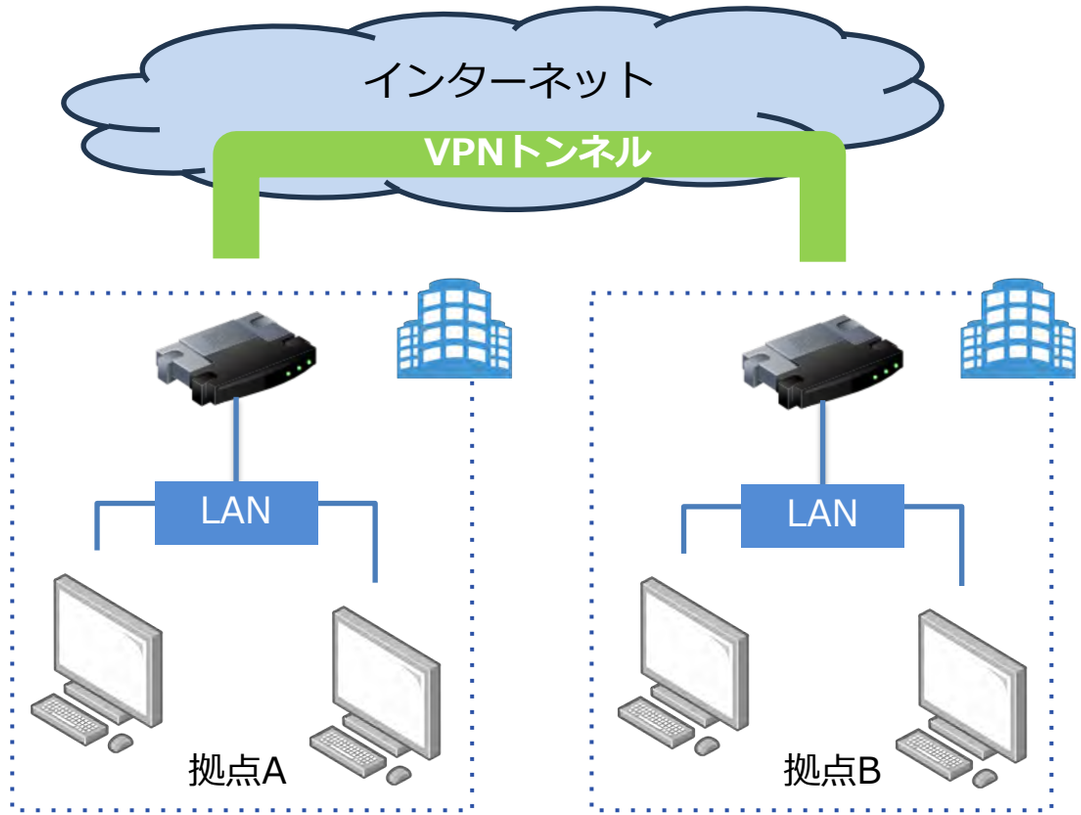
■VPN（Virtual Private Network）

VPNとはWANの一種で、LANとLANの間を**仮想的なプライベートネットワーク**で繋ぐ技術です。

不特定多数のユーザーが利用するインターネットの空間ですが、VPNは名前の通り、**送信側と受信側の間に仮想の専用線(トンネル)を設ける**ことで、通信の内容を保護し、不正アクセスなどのセキュリティ脅威から守ることができます。

LANはその建物内だけでアクセスできる閉じたネットワークのため、
同じ会社であっても、拠点Aから拠点BのLANにアクセスすることはできません。
そこでVPNによってWANを構築すれば、LAN同士が大きなネットワークで繋がることができ、異なる拠点のLANに接続できるようになります。

なおVPNを利用すれば、通信の「暗号化」などによりセキュリティを強化できるため、個人情報や機密情報といったデータのやりとりを行う際に利用されています。



2.2. ネットワークの種類

■VPNの種類

VPNの代表的な種類としては、主に**「インターネットVPN」**と**「エントリーVPN」**と**「IP-VPN」**と**「広域イーサネット」**の4つの種類に分類されています。それぞれ構築される仕組みが異なるほか、運用コストや通信品質、セキュリティやカスタマイズの自由度等にも違いがあります。

種類	説明	ユースケース（例）
IP-VPN	通信事業者の閉鎖型ネットワークで構築するVPN。セキュリティや通信品質の点で、より専用線に近い環境で利用できます。通信事業者との契約が必要となるためコストが高くなる可能性があります。	● 企業の本社・支社間のセキュアなデータ通信 ● 金融機関など、高いセキュリティと安定性が求められる業界など
インターネットVPN	インターネット上に仮想のネットワーク環境を構築する接続方式。比較的安価に構築できるが、自社で構築することはできるが、セキュリティの確保などが必要です。	● 小規模な拠点間通信（中小企業のオフィス間接続など） ● 在宅勤務・リモートワークでの社内ネットワーク接続
エントリーVPN	ADSLなどのインターネット回線を用いて閉域IP網を構築する接続方式。通信事業者の設置する閉域網を使用するため、、セキュリティの強度や信頼性は高いが、使用する回線自体はインターネット回線のため通信速度が遅くなる場合があります。	● 中規模模な拠点間通信
広域イーサネット	通信事業者の閉域ネットワークを利用して仮想のネットワークを構築するVPN。通信品質やLAN同士の繋げやすさが強みです。	● データセンターと本社間の高速データ転送 ● 大規模な拠点間ネットワーク構築（製造業・流通業など） ● 映像や大量のデータをやり取りする企業

2.2. ネットワークの種類

■ネットワークの特徴比較

「LAN」「WAN」「VPN」のそれぞれの特徴と違いは以下となります。

項目	LAN	WAN	VPN
範囲	限定的	広範囲	仮想的な専用ネットワーク
接続方法	有線/無線	インターネット/専用線	インターネット上の仮想専用線
セキュリティ	高い	中程度	非常に高い
利用目的	家庭やオフィス内の通信	遠隔地間の通信	安全な通信環境の構築

2.3. ネットワーク機器の種類

ネットワーク機器には、通信ネットワークを構成し、データを適切に転送するためのさまざまなデバイスがあります。
以下に、主要なネットワーク機器について説明します。

■ルーター（Router）
異なるネットワーク（例：LANとインターネット）を接続する機器
IPアドレスを基にパケットを転送する
主な機能
NAT（Network Address Translation）：プライベートIPアドレスをグローバルIPアドレスに変換
DHCP（Dynamic Host Configuration Protocol）：ネットワーク内のデバイスにIPアドレスを自動割り当て
ファイアウォール機能を備えることもある

■スイッチ（Switch）
LAN内のデバイス同士を接続し、データ転送を制御
主な種類
レイヤー2スイッチ：MACアドレスを基にデータ転送
レイヤー3スイッチ：IPアドレスを基にルーティング可能（ルーターの一部の機能を持つ）
ポート数が多く、複数のデバイスを同時に接続できる

2.3. ネットワーク機器の種類

■ファイアウォール（Fire Wall）

ネットワークのセキュリティを確保するために使用されるネットワーク機器またはソフトウェアのことです。外部（インターネットなど）と内部（企業ネットワークなど）の間に配置され、不正なアクセスを防ぎ、許可された通信のみを通過させる役割を持っています。

（ファイアウォールの詳細は第7章に記載しています。）

■ロードバランサー（Load Balancer）

外部からの通信（トラフィック）を複数のサーバーに負荷を分散する装置です。

主に使われるのはWebサーバーのロードバランサーです。外部からの通信（トラフィック）を複数のサーバーに分散するロードバランサーは、負荷分散装置とも呼ばれます。いったんサーバーへのアクセスを集約し、リソースに余裕があるサーバーを接続先として選択するといった機能により、サーバーを含むシステム全体の可用性向上させる特長があります。

2.4. まとめ

まとめ

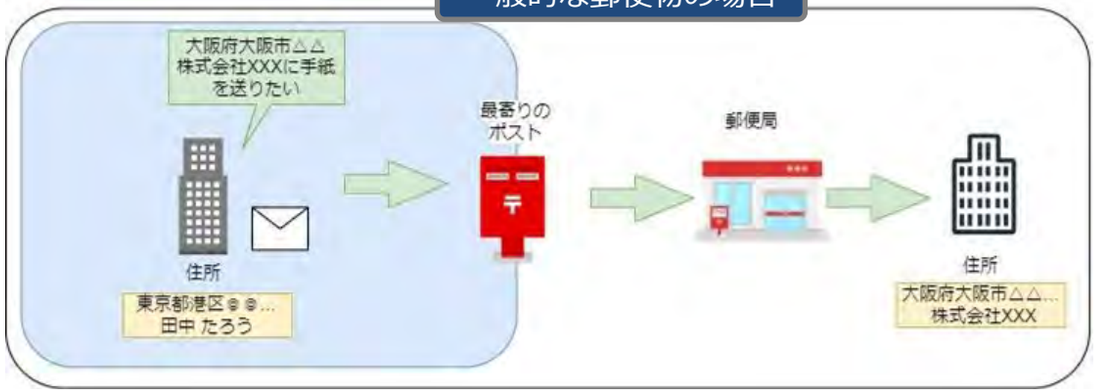
- ✓ ネットワークとは、複数のコンピュータやデバイスを相互に接続し、データをやりとりできる仕組み
- ✓ ネットワークの種類には大きく3つ(「LAN」「WAN」「VPN」)あり、それぞれ通信範囲や接続方法などが異なります。
- ✓ 「LAN」は家庭などの狭い範囲で構成される小規模なネットワークで、LAN内ではプライベートIPで通信します。VLANを使用することによって物理的に同じスイッチに接続されているデバイスを論理的に異なるネットワークに分離することができます。
- ✓ 「WAN」はLANとLAN同士を繋ぐ大きなネットワークで、グローバルIPで通信を行います。
- ✓ 「VPN」はWANの一種で、LANとLANの間を仮想的なプライベートネットワークで繋ぐ技術です。
- ✓ ネットワーク機器には、ルーターやスイッチなどの通信ネットワークを構成し、データを適切に転送するためのさまざまなデバイスがあります。

3. IPアドレスと通信の基礎

3.1. IPアドレスとは

IPアドレスとは、ネットワークに繋がっている機器（PCやスマートフォンなど）に割り振られた番号のことを言います。
IPアドレスは**「インターネット上の住所」**と言われており、端末同士でデータをやり取りする際に「送信先」や「発信先」を特定する役割を担っています。

一般的な郵便物の場合



現実世界で郵便物を送る場合は、宛先や自分の住所を記載します。
（*左上図）

ネットワーク上の通信の場合

一方、ネットワーク上の通信では、IPアドレスによって
「どこにあるどの機器に接続したいのか」「どこから発信するのか」を識別します。（*左下図）

例えば、「192.168.0.1」のように、0から255までの数字を4つ並べた形式で表現されます。
この数字の組み合わせによって、世界中のコンピュータを一意に識別することができます。

3.2. IPアドレスの構成

IPアドレスは、ネットワーク部とホスト部の2つの部分から成り立っており、サブネットマスクを使用して、
IPアドレスのどの部分がネットワーク部であり、どの部分がホスト部であるかを示します。

■ネッとワーク部・ホスト部

IPアドレス構成（例）

10進数表記

192.168.100.10 / 24

ネットワーク部　　ホスト部　　サブネットマスク

2進数表記

11000000.10101000.01100100.00001010

24ビット　　8ビット

ネットワーク部

IPアドレスのネットワーク部は、そのIPアドレスが属しているネットワークを識別するための部分を示します。
左の図だと、サブネットマスクが24ビットで示されている場合、
この数字はIPアドレスの２進数表記において、
左から数えて24番目のビットまでがネットワーク部に属することを意味します。

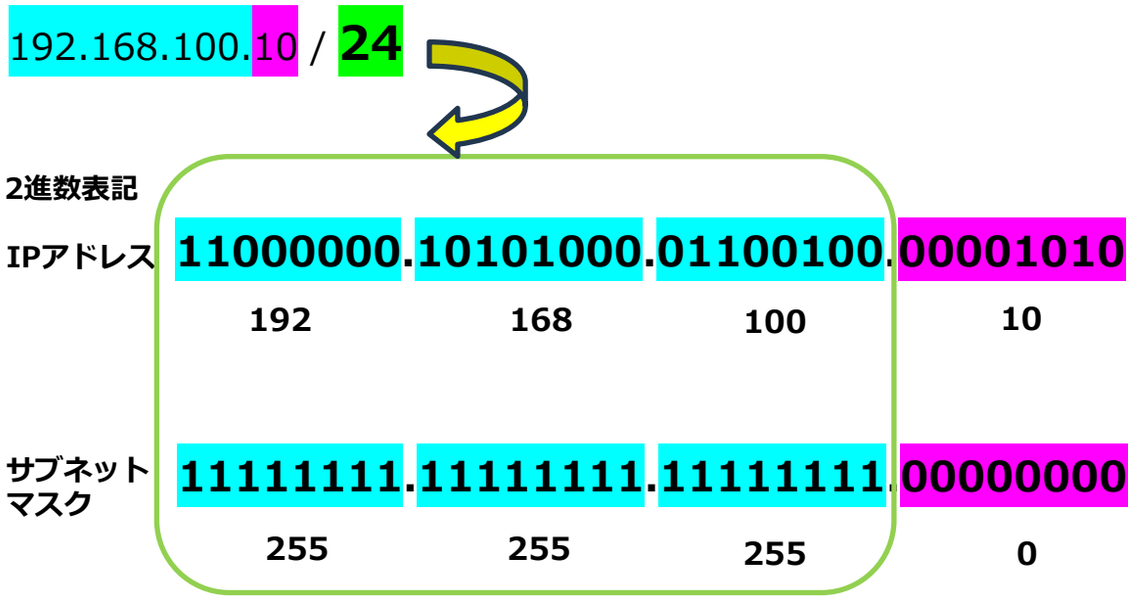
ホスト部

ホスト部は、ネットワーク内のコンピュータを識別するための部分です。
具体的には、そのIPアドレスがネットワーク内のどのコンピュータに割り当てられているかを特定します。
左の図の場合、ネットワーク部がサブネットマスクから24ビットまでとわかるので、残りの8ビットがホスト部になります。

3.2. IPアドレスの構成

■サブネットマスク

192.168.100.10 / 24



【例】
ネットワークアドレス：192.168.100.0
ブロードキャストアドレス：192.168.100.255
利用可能なホスト範囲：192.168.100.1～192.168.100.254
利用可能ホスト数：254台

サブネットマスク

IPアドレスをネットワーク部とホスト部を区別するために使用されます。
サブネットマスクを用意することで、IPアドレスのネットワーク部を自由に設定可能です。
例だと、サブネットマスクが24ビットと設定されているので、2進数表記のIPアドレスを左から順に数え、24ビットをネットワーク部、残り８ビットをホスト部と区別することができます。

計算方法

まず、サブネットマスクから「ネットワークアドレス」を求めます。

ネットワークアドレス

そのネットワーク全体を表すアドレスです。
例だと「192.168.100.0」がネットワークアドレスで「192.168.100.◎」に属する機器が同一ネットワーク内にいることを示します。

ブロードキャストアドレス

同じネットワーク内のすべての機器に一度にデータを送るための特別なアドレスです。例だと「192.168.100.255」です

ホスト数

ネットワークアドレス 「192.168.100.0」 ～ 「192.168.100.255」間のアドレスがホストに割り当て可能なアドレス数（254台）となります。

3.2. IPアドレスの構成

サブネットを分ける理由・メリット

① ネットワークの効率化・スケーラビリティ向上
大きなネットワークに多数のデバイスがあると、ブロードキャスト通信（LAN内の一斉送信）が増えて効率が落ちます。
サブネットで小分けにすることで、ブロードキャスト範囲を限定し、通信の効率を向上できます。

② セキュリティ向上
異なる部署やシステム（例：社内ネットワークとゲスト用ネットワークなど）をサブネットで分けることで、
アクセス制御（ファイアウォール等）を個別に設定することができます。

③ 管理のしやすさ
ネットワーク機器ごとにIPアドレス範囲を明確にでき、IPアドレスの管理が容易になります。
構造的にネットワークを分けることで、トラブル発生時の影響範囲が限定されるため、障害対応がしやすくなります。

※＜補足＞※
④ 仮想ネットワーク環境（例：AzureやAWS）での構成上の要件
クラウドでは、仮想ネットワーク（VNet）内でサブネットを分けて構成するのが基本です。
VMやPaaSサービスを異なるサブネットに分けることで、役割ごとのトラフィック制御やセキュリティポリシーの適用が可能です。

3.3. グローバルIPとプライベートIP

IPアドレスは、大きく分けて「グローバルIPアドレス」と「プライベートIPアドレス」の2種類に分類することができ、さらにその中でも、固定IPアドレスと動的IPアドレスの二つに分類することができます。

グローバルIPアドレス

インターネットに接続する機器に必ず利用されるIPアドレスです。
同じグローバルIPアドレスは、**世界中で重複することはなく、必ず１台の機器に対して、１つのIPアドレスが割り当てられます。**
例えるなら、「電話番号」や「住所」などと同じようなモノです。

一般的に、プロバイダーと契約することで、ルーターに、グローバルIPアドレスが割り振られます。
グローバルIPアドレスは、世界中を繋ぐインターネット上で使用されるものであり、世界中の機関によって管理されているため、自分で変更することができません。

プライベートIPアドレス

プライベートIPアドレスは、「ローカルIPアドレス」とも言われ、**自宅内や会社内のネットワークで使われるIPアドレスです。**
具体的には、一般家庭などでは、「192.168.1.1」や「192.168.0.11」など、「192」で始まるIPアドレスが、プライベートIPアドレスとして使われるケースが多いです。
なお組織内でのアドレスが重複しなければ自分で変更することも可能です。

3.3. グローバルIPとプライベートIP

IPアドレスの範囲は「0.0.0.0 ～255.255.255.255」ですが、ネットワークを効率よく分割し、管理・通信しやすくするため に範囲によって用途が定められています。

■プライベートIPアドレスの範囲

プライベートIPアドレスの範囲はRFC 1918という文書で規定されています。
以下の通りクラスA、B、Cの 3種類があります。クラスごとに設定できる範囲（数値）が既定されており、通常はその範囲内で設定をします。
クラスAは大規模ネットワーク向け、クラスBは中規模ネットワーク向け、そしてクラスCは小規模ネットワーク向けとなっています。

	プライベートIPアドレスの範囲
クラスA (大規模ネットワーク向け)	10.0.0.0～10.255.255.255 （10.0.0.0/8）
クラスB （中規模ネットワーク向け）	172.16.0.0～172.31.255.255（172.16.0.0/12）
クラスC （小規模ネットワーク向け）	192.168.0.0～192.168.255.255 （192.168.0.0/16）

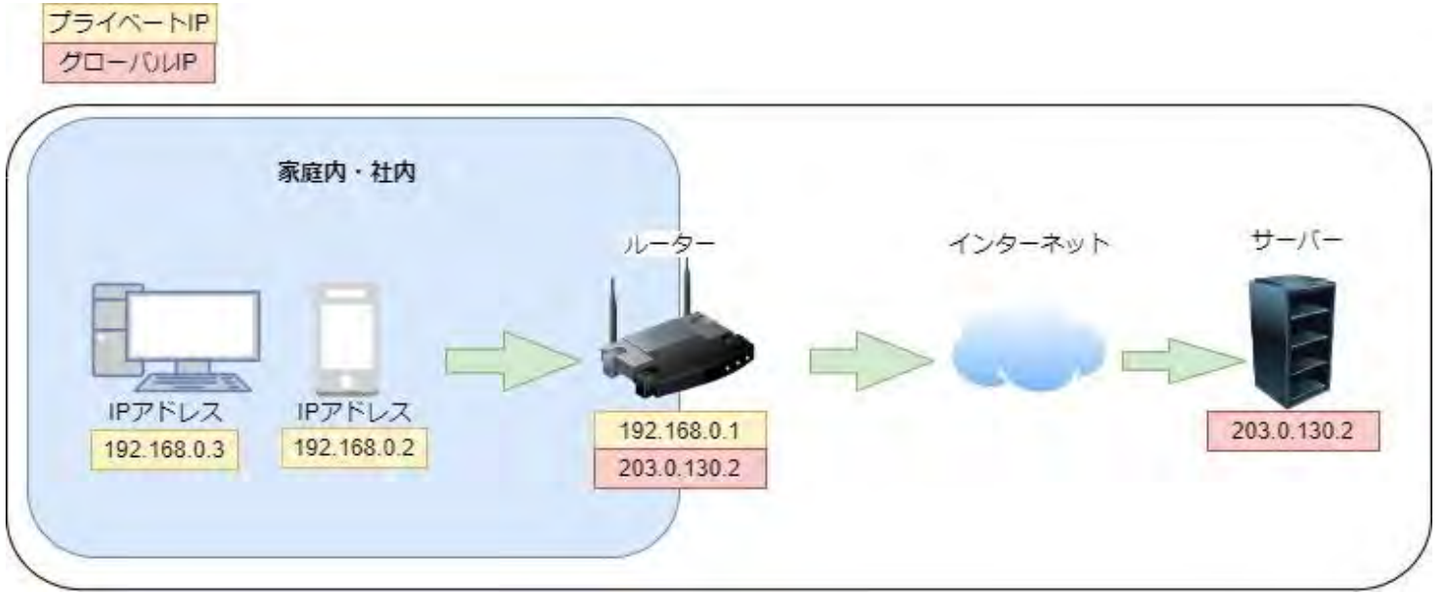
■グローバルIPアドレスの範囲

上記のプライベートIPアドレス範囲を除いた、[0.0.0.0 ～ 255.255.255.255] の中で一意にインターネット上で使用できるアドレスがグローバルIPとなります。

3.3. グローバルIPとプライベートIP

なぜ、プライベートIPアドレスが存在するのか？全部グローバルIPではだめなのか？

世界中にある全ての端末にグローバルIPアドレスを割り振ると、IPアドレスの数が足りなくなります。
その為、グローバルIPアドレスは、インターネット回線の自宅からの出口にあるルーターに１つ割り振ります。
そしてルーターの内側にあるパソコンやスマートフォン、タブレットなどの端末には、プライベートIPアドレスを割り振ります。
このようにすることで、IPアドレスの枯渇を防ぐことができます。

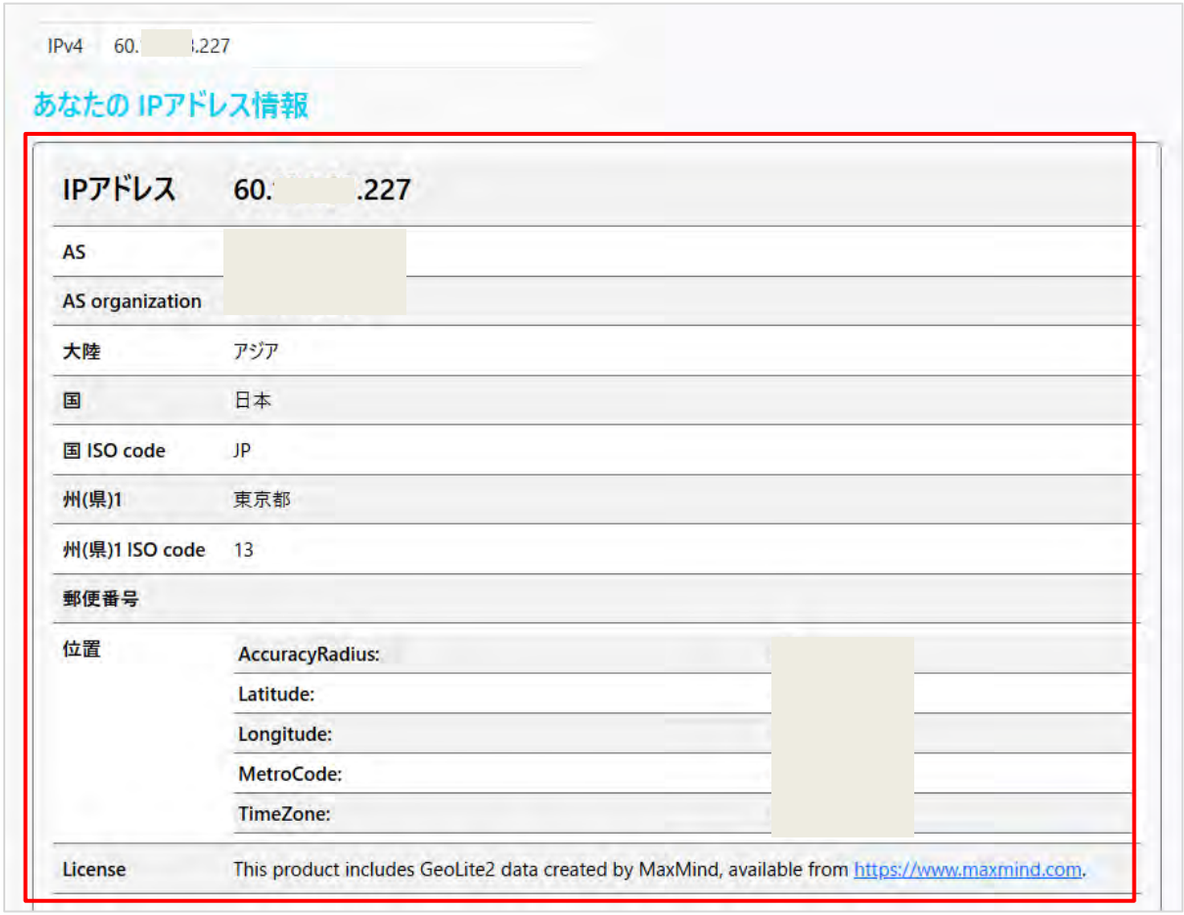


左図の場合、PC、スマートフォン、ルーターには家庭内・社内通信用にプライベートIPが割り当てられ、
ルーターにはISPから振り出された一意のグローバルIPが割り当てられ、インターネット上の通信を可能にしています。

3.3. グローバルIPとプライベートIP

グローバルIPとプライベートIPを確認する方法について記載しております。

■グローバルIP確認手順



1．グローバルIPを確認できるサイトを検索し、アクセスします。

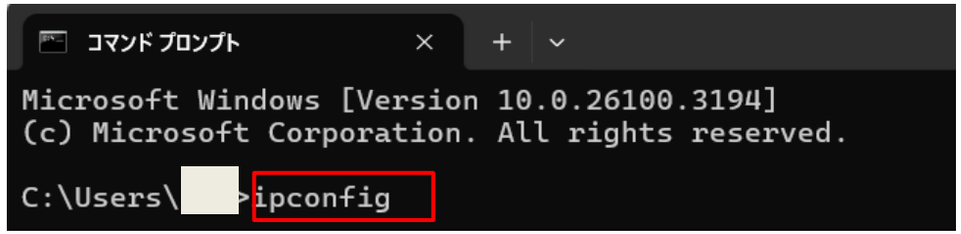
2．グローバルIPアドレスが表示されます

<補足> ■WebサイトでIPアドレスを返す仕組み

① ユーザーがサイトにアクセス
アクセスすると、ブラウザがそのWebサイトのサーバーにHTTPリクエストを送信します。
② サーバーがIPアドレスを取得
Webサイトのサーバーは、リクエストの送信元である クライアントのグローバルIPアドレス を読み取ります。
③ WebサイトがIPアドレスを表示
サーバーは取得したグローバルIPアドレスをページに表示したり、さらに詳細な情報（地域やISP）とともにユーザーに表表示します。

3.3. グローバルIPとプライベートIP

■プライベートIP確認手順

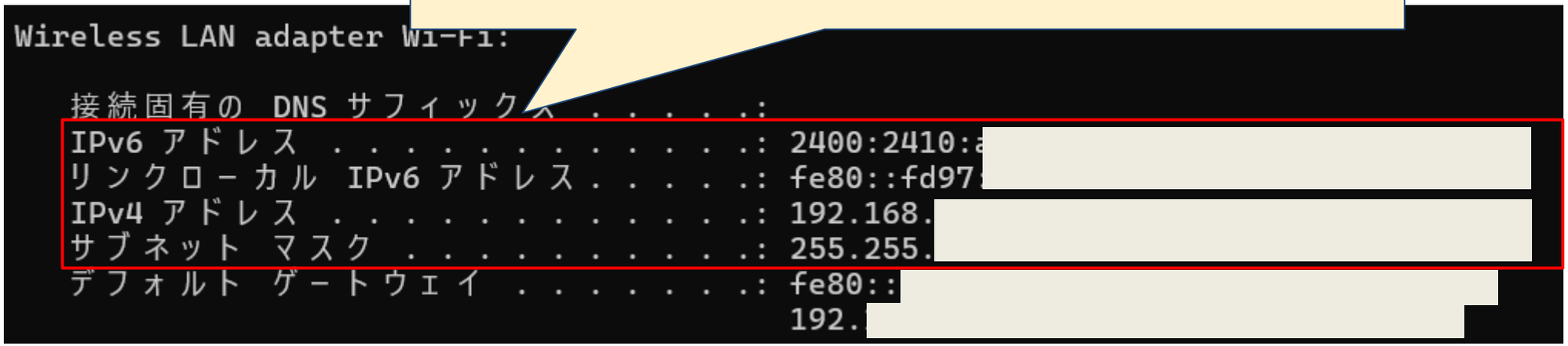


１．Windowsのスタートボタンから、「コマンドプロンプト」を立ち上げます。（もしくは、検索窓に「cmd」と入力し立ち上げます）

2. 「ipconfig」と入力し、[Enter]を押します

※ipconfig…Windowsにおいて、主にIPネットワークの設定情報を表示するコマンドとなります。

多くのネットワークでは 「デュアルスタック」 という方式を採用し、IPv4とIPv6の両方を使えるようになっています。そのため両方のアドレスが表示されています



3.4. NATと通信の流れ

■NAT

NATとは、プライベートIPアドレスとグローバルIPアドレスを相互に変換する技術 です。

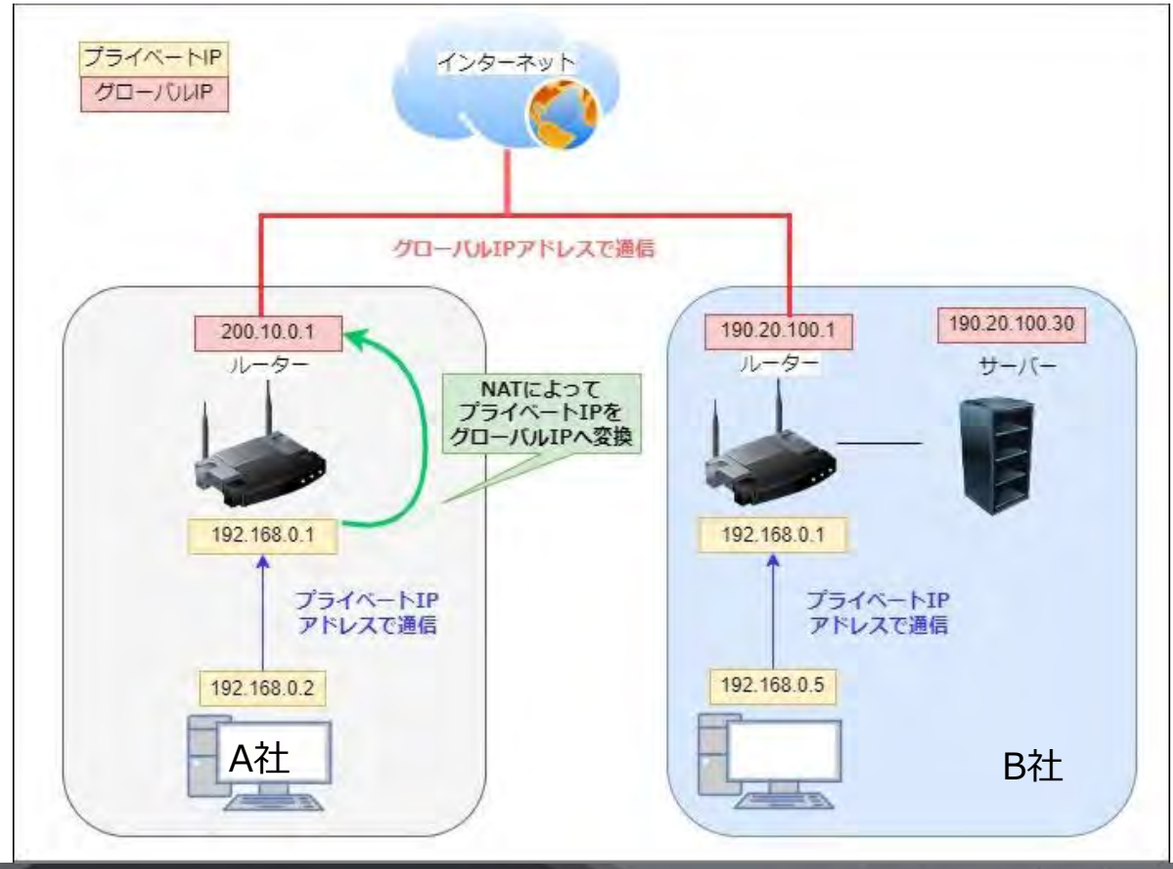
主に 「社内ネットワーク（LAN）からインターネットに出る際に使われる技術」 であり、限られたグローバルIPアドレスを効率的に利用するために利用されます。

企業ネットワークでは、プライベートIPアドレスを使用して構築されたネットワークなので、企業LANネットワークのクライアントPCがインターネット接続する場合、プライベートIPアドレスをグローバルIPアドレスに変換（NAT）をする必要があります。

■通信の流れ

実際の通信の流れについて右の図を例に説明します。

1. PC（プライベートIP:192.168.0.2）がB社のPC（192.168.0.5）に通信を開始
2. A社のルーターがNATを行い、グローバルIP(200.10.0.1)に変換
3. インターネットを経由してB社に到達
4. B社のルーターがNATを行い、B社のプライベートIP（192.168.0.5）に変換
5. B社のPCがA社のPCからの通信を受け取る



3.5. IPv4とIPv6

IPアドレスには「Ipv4」と「IPv6」と2つの形式があります。それぞれの特長について以下にまとめています。

IPv4

IPv4は、2進数の数字32ケタ（＝32ビット）から成り立つIPアドレスの形式です。8ビット（=1バイト）ずつ4つに区切られています。

2進数の32ケタを10進数の数字に置き換えたものが、私たちが普段目にしているIPアドレスです。
例えば「192.168.1.1」」のように表記され、その数は、
「4,294,967,296（約43億個）」が最大数です。

現在の世界では約70億人を超える人口がいるので、単純に１人が１個のIPアドレスを割り当てることができません。
この為、「IPv4」は、IPアドレスが足りなくなることが問題となっています。

192.168.1.1

2の32乗 = 43億個

IPv6

IPv6とは、枯渇しつつあるIPv4の問題を解消するために作られたIPアドレスの形式です。
16ビットずつ「:」（コロン）で区切られた8つの数値を、16進数で表記しています。
（例：「2000:11ab:123:1:2b:2bxf:fa6a:a8s8」）

16進法のIPv6を、2進法に変換すると128ビット（＝128ケタ）となります。そのため、2の128乗で約340澗個と、
実質的に無限とも言えるぐらいのIPアドレスを使うことができるようになります。

2000:11ab:123:1:2b:2bxf:fa6a:a8s8

2の128乗 = 340澗個

3.6. OSI参照モデル

OSI参照モデル（Open Systems Interconnection Reference Model）とは、コンピューターネットワークで様々な種類のデータ通信を行うために機器やソフトウェア・通信規約（プロトコル）などが持つべき機能や仕様を7つの階層（レイヤー）に分割・整理したモデルです。
ネットワークの全体像を把握し、問題解決や設計に活かすために、OSI参照モデルは重要とされています。

■OSI参照モデル

	階層	ネットワーク機器	主なプロトコル	説明
7	アプリケーション層	ファイアウォール、 ロードバランサー、ゲートウェイ	HTTP,FTP,SMTP	各アプリケーションに用意されたプロトコルを特定する
6	プレゼンテーション層	ファイアウォール、ゲートウェイ	文字コード	データ形式などを決定する
5	セッション層	ゲートウェイ	セッション	通信開始・維持・終了を決定する
4	トランスポート層	ロードバランサー、	TCP/UDP	ノード間の通信制御するための機能を決定する
3	ネットワーク層	ルータ、L3スイッチ、ファイアウォール（L3）	IPアドレス、ルーティング	複数のネットワークでエンドツーエンドの通信を可能にする機能を既定する
2	データリンク層	L2スイッチ、スイッチングハブ、ブリッジ	MACアドレス、VLAN	ちょくせつ接続されたノード間で通信可能にする機能を決定する
1	物理層	NIC、リピータ、ハブ	リンクアップ、Auto-Negotiation	コンピュータ上で使用するデータの電気信号への変換などを既定

3.6. OSI参照モデル

各階層の特徴は以下となります。

第1層： 物理層

ネットワークデータの物理的な送受信を担当します。これは電気信号、光信号、無線信号など、具体的な媒体を通じてデータを送信します。物理層は、データリンク層（第２層）からのデータを物理的な信号に変換し、ネットワークを通じて送信します。逆に、受信した信号をデジタルデータに変換し、それをデータリンク層に送信します。

第2層：データリンク層

データリンク層は物理的な接続を介してデータを転送します。エラーチェックとフレームの同期もこの層で行われます。ネットワーク層（第３層）からのデータパケットを物理的に伝送するために、物理層（第１層）に送信します。また、物理層から送られてきた信号を解析し、それをフレームに変換してネットワーク層に送信します

第3層：ネットワーク層

データパケットの送受信を管理し、データのルーティングと送信を行います。トランスポート層（第４層）からのデータをパケットに分割し、それらを最適な経路を通じて下位のデータリンク層（第３層）に送信します。また、データリンク層から送られてきたパケットを再構成し、それをトランスポート層に送信します。

3.6. OSI参照モデル

第4層：トランスポート層

トランスポート層はエンドツーエンドのデータ転送を提供し、必要に応じてデータの再送、フロー制御、エラー検出と修正を行います。セッション層（第5層）から送られてきたデータを分割し、各部分に番号を割り当てて、下位のネットワーク層（第３層）に送信します。一方で、ネットワーク層から送られてきたデータを再構成し、それをセッション層に送信します。

第5層：セッション層

セッション層は通信セッションの設定、維持、終了を管理します。これには、セッションの同期と通信の制御が含まれます。プレゼンテーション層（第6層）から送られてきたデータを、一定の間隔（セッション）で分割し、下位のトランスポート層（第４層）に送信します。また、トランスポート層から送られてきたデータを再構成し、それをプレゼンテーション層に送信します。

第6層：プレゼンテーション層

プレゼンテーション層はアプリケーション層（第　７層）からのデータを受け取り、ネットワークの他の部分で理解できる形式に変換します。
□□□□□□□□□□□□□□□□□□□□層 で行われます。この 層 は、上位のアプリケーション 層 から送られてきたデータの圧縮や暗号
□□□□□□□□□□□□□□□□□□□層□□□□□□□□□□□□□□□□□□□□□□□□層 が理解できる形に変換します。

3.6. OSI参照モデル

第7層：アプリケーション層

アプリケーション層は最上位の層で、ユーザーの目に直接触れます。この層の主な役割は、エンドユーザーがネットワークリソースと効率□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□層（第6層□□層から送られてきたデータをユーザーが理解できる形式に変換します。

3.7. TCP/IPモデル

■TCP/IPモデル

TCP/IPモデルは、インターネット上でデータをやり取りするための階層的なフレームワークを提供します。

このモデルは、データの送受信を円滑に行うために、4つの主要な階層から構成されています。

- **アプリケーション層**
  ・・・ユーザーが使うアプリのデータを処理
- **トランスポート層**
  ・・・データの分割・順序管理
- **インターネット層**
  ・・・IPアドレスを使ってデータを転送
- **ネットワークインターフェース層**
  ・・・物理的な通信（LANやWi-Fi）

OSI参照モデルと比較すると下図のように対応します。OSIの第1～2層がネットワークインタフェース層として、5～7層がTCP/IPのアプリケーション層としてまとめられ、OSIよりも実装面で効率的、かつ現実的な仕様となっています。
（OSI参照モデルは理論的モデル、TCP/IPは現実的に使用される動作しているモデル）

3.7. TCP/IPモデル

■TCP/IPの通信の流れ

TCP/IPの4階層モデルにおける各階層間の連絡手段として、「カプセル化」があります。
通信データを整理し、各階層で必要な情報をヘッダー情報として付加することで、ネットワーク通信で送られる情報を管理することができ、ネットワーク間のデータの輸送を効率的に、正確に実施することが可能になります。

アプリケーション層	AからBへデータを送信		
トランスポート層	TCPヘッダを付加 （ポート番号など）		
インターネット層	IPヘッダを付加 （IPアドレスを付加）		
ネットワークインターフェイス層	イーサネットヘッダ及びFCSを追加	電気信号に変換	ビット列に変換

カプセル化　　非カプセル化

3.8. TCP・UDPの違い

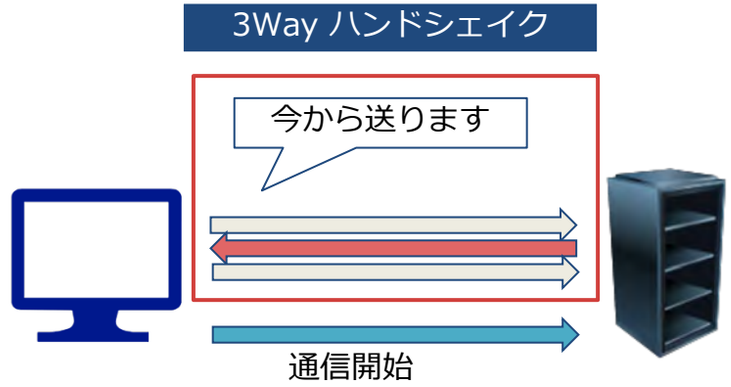
TCP（Transmission Control Protocol）と**UDP**（User Datagram Protocol）は、どちらもネットワーク通信に使われるトランスポート層（レイヤー4）のプロトコルです。
ネットワーク通信における**主要なプロトコル**であり、データを送受信する際の方式を決める役割を持っています。

TCP

TCPは、インターネット通信において、データの送受信を正確かつ信頼性の高い形で行うためのプロトコルです。
TCPは、通信を行う前に接続を確立し、その後データを送信します。このプロトコルにより、データが正しい順序で到達し、データが欠けることなく送られることが保証されます。

特徴

信頼性が高い データの損失やエラーが発生した場合、自動的に再送が行われ、完全なデータが送信されます。
データの順序が保証される 送信したデータは、受信側で正しい順序で復元されます。
接続を確立する データ送信前に**「3ウェイハンドシェイク」**と呼ばれる手順で通信を確立します。



・Webページの閲覧（HTTP/HTTPS） Webサイトをブラウジングする際、テキストや画像、動画などのデータは順序どおりに表示される必要があります。TCPはその信頼性の高さから、Web通信に最適です。
・ファイル転送（FTP） ファイルを正確に送受信するため、TCPはファイル転送プロトコル（FTP）でも利用されます。
・データの一部が欠けることなく送信されるため、大容量ファイルのやり取りも安心です。
・メール送信（SMTP、POP3、IMAP） メール通信でも、データが完全であることが要重です。

3.8. TCP・UDPの違い

UDP

UDP（User Datagram Protocol）は、TCPとは異なり、軽量で高速な通信を行うためのプロトコルです。UDPは、接続を確立せずにデータを送信し、送信の確認や再送の手続きが行われません。そのため、信頼性はTCPよりも劣りますが、通信のオーバーヘッドが少なく、リアルタイム性が求められる場面で利用されます。

特徴

コネクションレス 通信を行う前に接続を確立する手順が不要です。

速度が速い 確認や再送の手続きがないため、TCPに比べて通信速度が速く、リアルタイム性に優れています。

信頼性が低い データの順序保証や再送が行われないため、データが欠損したり、順序が乱れることがあります。

・動画ストリーミング（YouTube、Netflix） 動画視聴においては、多少のデータ欠損よりもスムーズな再生が求められます。

UDPはその高速性により、途切れのないストリーミング再生をサポートします。

・オンラインゲーム（リアルタイム性が重要） オンラインゲームでは、遅延が少ない通信が重要です。UDPは高速であるため、リアルタイムにゲーム内のアクションを反映させることが可能です。

・VoIP（音声通話）（Skype、Zoom） VoIPのようなリアルタイム音声通信では、少しのデータ欠損は会話に支障を与えません。UDPは遅延の少ない通話を実現するため、VoIPアプリで広く利用されています。

3.8. TCP・UDPの違い

■TCPとUDPの特徴の比較

TCPはデータの正確性が求められる用途に適し、UDPはリアルタイム性が重要な場面で使われます。

	TCP	UDP
接続方式	コネクション型 （ハンドシェイクあり）	コネクションレス型 （ハンドシェイクなし）
信頼性	高い （再送・誤り検出）	低い （再送無し）
データ送信確認	行う	行わない
通信速度	遅い （オーバーヘッド大）	早い （オーバーヘッド小）
主な用途	Web、ファイル転送、メール	ストリーミング、ゲーム、 DNS、音声通話

3.9. まとめ

まとめ

- ✓ IPアドレスとは、端末同士でやりとりする際に「送信先」や「発信先」として特定する住所録のような役割をもつ。
- ✓ IPアドレスには「ネットワーク部」「ホスト部」「サブネットマスク」があり、サブネットマスクからネットワークアドレスやブロードキャストアドレス、割り当て可能なアドレス数を算出することが可能です。
- ✓ IPアドレスは「グローバルIP」と「プライベートIP」の二種類があり、グローバルIPはインターネット上で使用、プライベートIPは自宅や社内のネットワークで使われるIPです。
- ✓ IPアドレスの枯渇防止のため、NATの変換技術を用いてプライベートIPからグローバルIP変換しインターネットを経由して接続します。
- ✓ OSI参照モデルは7つのレイヤーに分割したモデルでネットワーク全体像を把握するための理論として用いられます。
- ✓ TCP/IP参照モデルはインターネット上でデータ通信をやりとりするための理論となり、4つのレイヤーに分かれており、必要な情報をヘッダー情報として付加し通信を行います。
- ✓ TCP/UDPはインターネットで使用される主要なプロトコルです。TCPはデータの正確性が求められる用途に適し、UDPはリアルタイム性が重要な場面で使用されます。

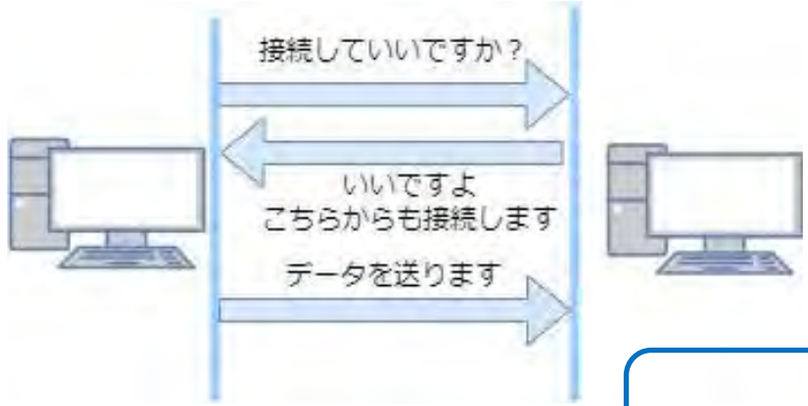
4. ネットワークプロトコル

4.1. ネットワークプロトコルとは

■プロトコル

ネットワークにおけるプロトコルとは、データのフォーマットと処理の一連のルールのことであり、通信を行うために取り決めた約束ごとを意味します。
ネットワーク内のコンピュータは、ソフトウェアやハードウェアが大きく異なっていても、プロトコルを使用することで、相互に通信することができます。

コンピュータネットワークでは、メールを送るためのプロトコル、受け取るためのプロトコル、ファイルを送るためのプロトコルなど、様々な通信ごとに決まり事を事前に決めた上で通信を行っています。これと同じように通信を行う場合にも手順が存在します。
コンピュータネットワークでは、前項のOSI参照モデルというアーキテクチャを推進しています。



接続の方法やデータの送り方、
届かなかったときにどうするかなどを決めています

4.2. 一般的なプロトコル

その他、よく使用される一般的なプロトコルについても紹介します。

プロトコル	説明
FTP	「File Transfer Protocol」のことであり、ファイルを転送するための通信規格です。クライアントとサーバ間で、ファイルのアップロードやダウンロードを行うときに使われるプロトコルです。
SMTP	「Simple Mail Transfer Protocol」の頭文字を取ったもので、電子メールの送受信に使用される通信プロトコルです。
HTTP	HTTP（HyperText Transfer Protocol）は、WebブラウザとWebサーバーが通信するためのプロトコル（通信規約） です。Webページのデータ（HTML、画像、動画など）を転送するために使用されます。
POP3	POP3（Post Office Protocol version 3）は、メールを受信するためのプロトコル です。メールサーバーからメールをダウンロードし、ローカルのPCやスマートフォンに保存する仕組みを提供します。
SSH	SSH（Secure Shell）は、ネットワーク上で安全にリモートコンピュータへ接続するためのプロトコル です。主にリモートサーバーの操作やファイル転送に利用されます。
RDP	RDP（Remote Desktop Protocol）は、Windowsのリモートデスクトップ接続を実現するためのプロトコル です。Microsoftが開発したプロトコルで、遠隔のPCをまるで直接操作しているかのように使うことができる 仕組みを提供します。
SMTP	SMTP（Simple Mail Transfer Protocol）は、メールを送信するためのプロトコル です。主にメールクライアント（Outlook、Thunderbirdなど）やメールサーバーが、メールを送信・転送するときに使用 します。
DHCP	DHCP（Dynamic Host Configuration Protocol）は、ネットワーク上のデバイスにIPアドレスやネットワーク設定を自動的に割り当てるプロトコル です。

4.3. まとめ

まとめ

- ✓ プロトコルとは、データのフォーマットと処理の一連のルールのことであり、通信を行うために取り決めた約束ごと
- ✓ ネットワーク内のコンピュータは、ソフトウェアやハードウェアが大きく異なっていても、プロトコルを使用することで、相互に通信することができます。

5. DNS

5.1. DNSの基本

DNSとは、「Domain Name System」の頭文字であり、ドメイン名を用いてインターネットが利用できるようにするためのシステムのことです。DNSは「ドメイン名」と「IPアドレス」を紐づけた情報が管理され、「ドメイン名」から自動的に「IPアドレス」が特定できるようになっています。

例えば、「https://www.test.com/」というサイトを見たいとき、実際にはそのサイトのサーバーには「200.10.0.1」のような数字のIPアドレスがあります。しかし、このよううな数字の羅列数字を覚えるのは大変です。

そこでDNSは、 「https://www.test.com/」を「 200.10.0.1 」 のように、人間が覚えやすいようコンピューターが理解できる数字（IPアドレス）に変換します。

具体的には **DNSサーバー**が、**DNSの仕組みを提供し、ドメイン名とIPアドレスを変換する役割を担います。**

5.1. DNSの基本

■DNSサーバーの種類

DNSサーバがIPアドレスと名前（ドメイン）の紐づけを電話帳のように管理していますが、このDNSサーバには大きく2つの役割に分かれています。

①権威サーバー

一般的にDNSサーバといえばこの権威サーバーを指します。IPアドレスとドメイン名の関連付け１行１行をレコードセットとして管理していて、他のサーバーに問い合わせることなく応答するサーバです。

管理しているドメイン名の情報をもとに、**「キャッシュDNSサーバー」からの問い合わせに応答する役割を**担っています。

権威サーバは自分が管理する範囲をルートを頂点に分担しており、範囲外の問い合わせがあれば委任先の権威サーバの情報を応答することで成り立っています。

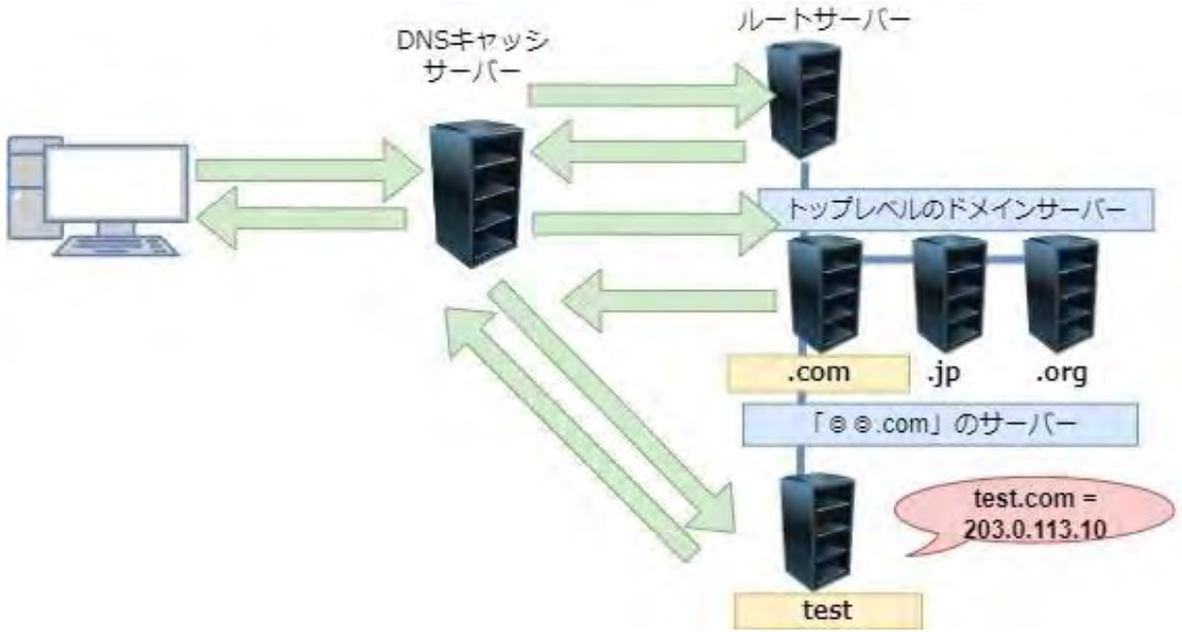
②DNSキャッシュサーバ

クライアント（ブラウザ）からの要求を受け取って、ドメイン名のIPアドレスを探しにいくサーバーです。権威DNSサーバーにアクセスして情報を引き出し、突き止めたIPアドレスをユーザーに返す役割があります。一度調べたIPアドレスは決められた時間だけ蓄積しておいて、同じドメイン名に対する権威サーバへの問い合わせを省略できるようになっています。

5.1. DNSの基本

■DNS　問い合わせの流れ

（該当ドメインに初めてアクセスする場合の例）



①PCからDNSサーバーに問い合わせ

「www.test.com」のIPアドレスを教えて”とDNSサーバーに問い合わせ

②DNSキャッシュサーバーへ問い合わせ

もしキャッシュを持っていたら、すぐにIPアドレスを返す

キャッシュがない場合は、さらに上位のDNSサーバーへ問い合わせを開始する

③キャッシュがない場合「ルートDNS → TLD(トップレベルドメインDNS) → 権威DNS」の順に問い合わせ

権威DNSから” IPアドレスは「203.0.113.10」です ” と返答がきます。

④DNSキャッシュサーバーが結果を保存（キャッシュ）

取得した 「203.0.113.10」 の情報を キャッシュ（一時保存） します。

次回以降、同じドメインの問い合わせが来たら、すぐにキャッシュから返答できます

⑤PCがIPアドレスを受け取り、Webサイトに接続します

5.2. AzureDNS（クラウド環境でのDNS管理）

■Azure DNS
Microsoft Azure が提供している DNS サービスで「クラウド上のDNSサービス」です。
一般的な DNS の仕組みと基本的には同じですが、Azure のクラウド環境に最適化された特長 があります。
Azure のインフラを使用してドメインを管理し、高い可用性・セキュリティを保ちながら高速な名前解決を行います。

種類

Azure には、「パブリック DNS」 と 「プライベート DNS」 の 2 種類があります。

①Azure Public DNS（パブリック DNS ゾーン）
Azure 上の グローバルなドメイン名（例: example.com）を管理します。
インターネット上の通常の DNS クエリに対応。
外部向け Web サイトや API の DNS レコードをホストするのに使用します。
例: www.example.com → 52.168.10.5（Azure VM のパブリック IP）

②**Azure Private DNS**（プライベート DNS ゾーン）
Azure 内の VNet内部でのみ使われる DNS サーバー。
仮想マシン（VM）や Azure サービス間の名前解決 に使用。
インターネットからはアクセス不可。
例: myvm.internal.azure → 10.0.0.4（プライベート IP）

特徴

- クラウドで管理
  物理的なDNSサーバーが不要で、Azureポータルから簡単に設定・管理ができる。
- 高速＆グローバル対応
  MicrosoftのDNSネットワークを活用し、高速で信頼性の高い名前解決が可能です。
- Azureサービスとシームレスに連携
  Azureの仮想マシン（VM）やロードバランサーと簡単に統合できる。
- 高可用性・耐障害性がある
  Azureの分散アーキテクチャで、DNSのダウンタイムを最小限に抑えることができる。

5.2. AzureDNS（クラウド環境でのDNS管理）

■一般的なDNSとAzure DNSの特徴と比較

項目	DNS（一般的なDNS）	Azure DNS
提供元	インターネット全体の標準技術	Microsoft Azureのクラウドサービス
役割	ドメイン名をIPアドレスに変換	クラウドベースのDNS管理と名前解決
ホスティング	ISPやドメインレジストラが管理	AzureのDNSゾーンとして管理
カスタムドメイン	GoDaddy、AWS Route 53 などの外部DNSでも管理可能	Azure上でカスタムドメインを管理
統合機能	なし（DNSサーバーごとに設定）	Azureリソースと統合（VM、App Serviceなど）
セキュリティ	DoS攻撃の影響を受ける可能性	DDoS対策済み（Azureのセキュリティ基盤
プライベートDNS	通常は外部向けの公開DNSが主	Azure Private DNSを利用可能
料金	無料または外部プロバイダーの料金	Azureの使用量に応じた課金提供元提供元

5.3. まとめ

まとめ

- ✓ DNSはインターネット上の「住所録」のようなもの。ドメイン名を、コンピューターが理解できるIPアドレスに変換する役割を担っています
- ✓ DNSには「DNSキャッシュサーバー」「権威サーバー」があり、以前に問い合わせがあったIPアドレスをキャッシュしておいたり、IPアドレスを返したりする役割があります。
- ✓ Azure DNSはMicrosoft社が提供しているクラウド上のDNSサービス。一般的なDNSよりも、管理が楽でAzureサービスと統合しやすいです

6. クラウドネットワーク

6.1. オンプレミス環境とクラウドネットワークの違い

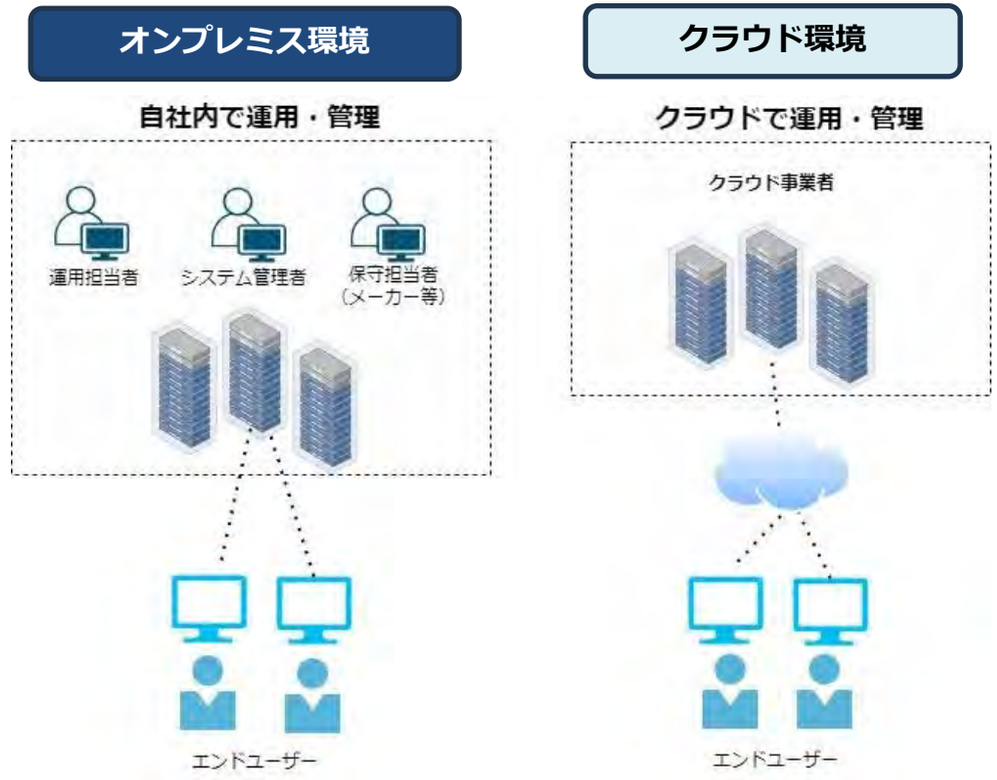
ネットワークの環境には**「オンプレミス環境」**と**「クラウドネットワーク環境」**があります。

■オンプレミスネットワーク環境

企業や組織が自社でサーバーやネットワーク機器を購入・管理し、システムを運用する形態のことを指します。
データセンターやオフィスのサーバールームに物理サーバーを設置し、
社内ネットワークを構築して運用します。

■クラウドネットワーク環境

インンターネットを経由して提供される仮想化されたITインフラやサービスを利用する環境のことです。
サーバー、ストレージ、ネットワークなどのリソースがクラウドプロバイダー（Azure、AWS、GCPなど）によって提供され、利用者は必要な分だけリソースを活用することができます。



6.1. オンプレミス環境とクラウドネットワークの違い

オンプレミス環境とクラウド環境のそれぞれの特徴は以下となります。

オンプレミス環境

・自社でインフラを管理
企業が自分たちでサーバー、ネットワーク、ストレージなどの機器を設置し、管理・運用を行います。

・初期投資が必要
ハードウェア（サーバー、ネットワーク機器）、ソフトウェア（ライセンス）、設置スペース、電力・冷却コストなどが発生します。
一度導入すれば長期間使用できるが、維持費がかかります。

・高いセキュリティとカスタマイズ性
インターネットを介さず社内ネットワークのみで運用可能なため、外部からの攻撃リスクを低減できます。

・スケールアップが難しい
追加のサーバーやストレージを増設する際に、機器購入や設置作業が必要となるため、すぐのスケールアップは難しいです。

クラウド環境

・クラウドプロバイダーがインフラを管理
物理サーバーやネットワーク機器はクラウドプロバイダーが所有・運用するため、ユーザーは仮想マシンやデータベースなどのサービスを設定するだけで利用できます。

・初期投資が不要
従量課金制なので、サーバーや機器を購入する必要がありません。
短期間のプロジェクトや急なリソース増減にも柔軟に対応可能です。

・スケーラビリティが高い
必要に応じてリソースを増減可能です。

・どこからでもアクセス可能
インターネットがあれば、世界中どこからでもクラウド環境にアクセスできます。

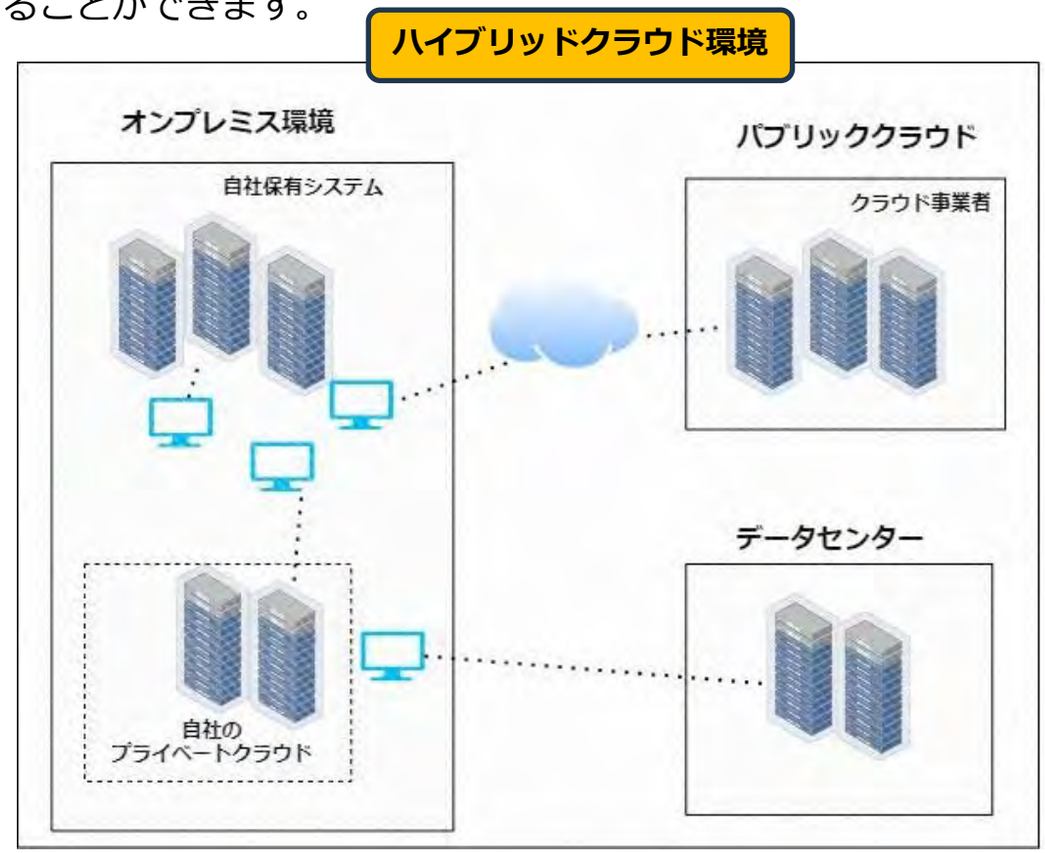
・高可用性と災害対策
分散しているため、障害時でもサービスを継続しやすいことが特徴です。
データのバックアップや復旧なども比較的容易です。

6.2. ハイブリッドクラウド環境について

ハイブリッドクラウドは、パブリッククラウド、プライベートクラウド、物理サーバーのような異なるサーバーを組み合わせて使うクラウドのことです。
セキュリティやコスト、柔軟性などの要件に応じて、最適なリソースを使い分けることができます。

パブリッククラウドは、ユーザーを問わずに提供されているクラウドサービスです。
一般的にはインターネット上で提供されており、Webサイトなどから申し込むことで即座に利用することが可能となっています。

プライベートクラウドは、特定のユーザーが占有して利用するクラウド環境を指します。
ユーザーが独自に構築したクラウド環境を利用する形態のほか、クラウドプロバイダーが提供する、ほかのユーザーからは隔離されたクラウド環境を利用する形態などが挙げられます。



＜構成例＞
オンプレミス＋パブリッククラウド　or データセンター
オンプレミス＋データセンター＋パブリッククラウド
パブリッククラウド＋プライベートクラウド　等

6.2. ハイブリッドクラウド環境について

ハイブリッドクラウド環境の特徴とユースケースは以下となります。

特徴

・コスト最適化

クラウドの従量課金を活用し、必要な分だけリソースを利用するなどが可能

24時間365日稼働する基幹システムはオンプレミスに維持し、一時的なデータ処理はクラウドに任せることで、全体のコストを抑えられます。

・柔軟なリソース活用

重要なデータやアプリケーションはオンプレミスに配置。

一時的な負荷が高い処理やデータ分析はクラウドで対応することが可能です

・セキュリティとコンプライアンス対応

企業の個人情報、機密データなどはオンプレミスに保管。

・既存システムとの連携

長年運用しているオンプレミスのシステムあり、すぐにクラウドへ移行できないケースが多いが、ハイブリッドクラウドなら、既存システムを残しつつ、新しいサービスをクラウド上に追加し、段階的にクラウドに移行することも可能となります。

ユースケース

・医療業界

機密性の高い、患者の診療記録や検査結果はオンプレミスないしはプライベートクラウドで管理。

予約システムのようなアクセス性の良さを求める患者データはパブリッククラウドに配置することで、患者データの管理方法がより効率的かつ安全になります。

・金融業界

秘匿性の高い金融取引に関するデータはオンプレミスないしはプライベートクラウドで管理し、効率的な処理にはパブリッククラウド上のトランザクション処理を導入することで、業務運用を総合的に改善させることができます。

6.3. まとめ

まとめ

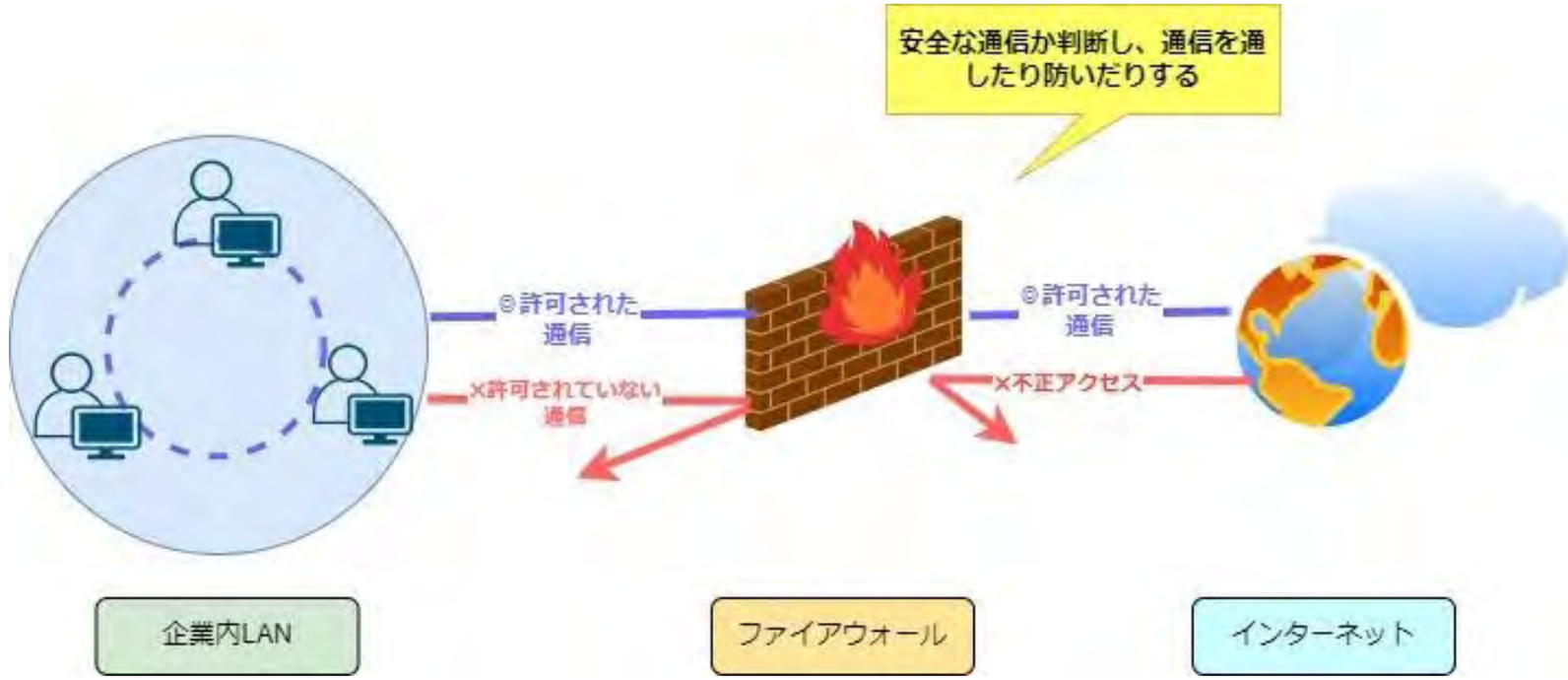
- ✓ **自社でサーバーやネットワーク機器を管理するオンプレミス環境とクラウドサービス提供者のインフラを利用するクラウド環境がある**
- ✓ **ハイブリッドクラウドとは異なるサーバーを組み合わせて使うクラウド環境のことを指します。（オンプレミス＋クラウド等）近年はハイブリッドクラウドの活用が増加しています。**

7. セキュリティ

7.1. ファイアウォールとは

ファイアウォール（Firewall）とは、**外部ネットワーク（インターネットなど）と内部ネットワーク（企業のLANなど）の間に設置され、不要な通信や不正アクセスを防ぐためのセキュリティシステム**です。

ネットワークの防火壁（Fire Wall）として、**許可された通信のみを通し、不正なアクセスや攻撃をブロック**する役割を持ちます。



7.2. ネットワークの通信を制御する仕組み

一般に、ファイアウォールは以下の3つの機能・役割を有しています。

①フィルタリング機能

通信のパケットをチェックし、通信の通過・遮断を判断する機能です。通過の許可条件を登録すると、そのルールに則って通信の可否を判断します。
登録する情報が多い場合は、類似の設定をまとめたり、「通過させる通信以外はすべて遮断」と設定したりできます。定期的に条件の見直しや更新も必要なため、目標とする防御の強度や範囲により、更新しやすいルールを設定する必要があります。

②アドレス変換機能

内部ネットワークで使用する「プライベートIPアドレス」と、インターネット上で使用する「グローバルIPアドレス」を変換する機能（NAT）です。

IPアドレスは、各ネットワーク機器の住所にあたる存在です。外部に知られると、攻撃の対象になりかねないため、各機器には内部ネットワーク専用のプライベートIPアドレスが付与され、外部へのアクセス時はNATが外部接続用のIPアドレスに変換。プライベートIPアドレスの漏洩を防ぎます。
また、NATを使用すれば、任意の通信を特定のコンピュータに誘導できます。これにより、部署や部門ごとにセキュリティレベルを分けることも可能です。

③監視機能

ログの監視・追跡機能です。各種サーバーとファイアーウォールが稼働しているときは、通信のログが残ります。これを分析すれば「いつ、どのように攻撃を受けたか」が分かり、対策立案のヒントになります。
また、ファイアーウォールは遠隔操作も可能です。万が一不正アクセスを許した場合も、システムがすぐ担当者に通報。担当者は遠隔地からでも、ログの取得や設定変更を行えます。

7.2. ネットワークの通信を制御する仕組み

■ファイアウォールの制御の種類

ファイアウォールは事前に定めたルール（ポリシー）に基づいて通信を許可または拒否します。
主な制御方法は以下の通りです。

種類	特徴
パケットフィルタリング型	パケットを監視（フィルタリング）して、決められたルールに従って通信を許可・拒否します。多くのファイアウォールはこのパケットフィルタリングに該当します。 パケットフィルタリング型はさらに以下の3種類に分類されます。 ・スタティックパケットフィルタリング ・ダイナミックパケットフィルタリング ・ステートフルパケットインスペクション
サーキットレベルゲートウェイ型	従来のパケットフィルタリング型の動作にポート指定や制御の機能を加えたものです。 TCPやUDPなどトランスポート層のレベルで任意のポートの通信を制御するため、パケットフィルタリング型では防げない送信元IPアドレスの偽装を防御できます。
アプリケーションゲートウェイ型	HTTPやFTPなどアプリケーションプロトコルごとに通信を制御するタイプです。 送受信されるデータの中身を詳細に監視するため、「なりすまし型」の不正アクセスにも効果を発揮します。

7.2. ネットワークの通信を制御する仕組み

■補足

ファイアウォールとルータはどちらも「通信を制御する」役割があるが、何が違うのか？

ファイアウォールはセキュリティ製品、ルーターは通信機器です。
ファイアウォールとルーターは、どちらも通信・アクセス制限ができる点は同じですが、セキュリティの観点で違いがあります。

ファイアウォールは、インターネットと企業内LANの間に設置します。事前に設定した規則に基づき、アクセスを遮断するか否かを見極め、不正アクセスやサイバー攻撃などからネットワークを保護する仕組みです。

ルーターはセキュリティ製品ではなく通信機器になります。**ルーターの機能はあくまでも異なるネットワーク同士を接続すること**です。セキュリティ対策を行うための製品ではないことに注意する必要があります。

	ファイアウォール	ルータ
目的	不正な通信を防ぐ	ネットワークをつなぐ
主な機能	通信の監視・制御・アクセス制御	ルーティング、NAT、DHCP
通信の扱い	通信を許可/拒否する	通信を転送する
セキュリティ	高度なセキュリティ機能あり	基本的な制御のみ

7.3. ファイアウォールとポート制御

ファイアウォールは **「どの通信を許可し、どの通信をブロックするか」** を決める機能を持っています。
通信を制御するために **ポート番号** を指定してアクセスを許可・拒否します。

■ポート

各アプリケーションは、特定のポート番号を使用して通信を行います。
ポートは、コンピュータが通信をする際に使う **「扉」** のようなものです。
IPアドレスは住所(家)であれば、ポートは外に出たり、外から入る「扉」と言われており、実際には「IPアドレス+ポート番号」で通信を行っています
IPアドレスだけでは通信相手の「どのサービス」か、「どのアプリケーション」にデータを送るべきなのか特定することはできません。
その特定を行うのがポート番号の役割です。

ファイアウォールは、指定されたポート番号をもとに、データパケットの通過を許可するかどうかを判断し、
ネットワークを不正アクセスから保護します。

■ファイアウォールの代表的なポート番号

ポート番号	プロトコル	説明
21	FTP	不正アクセスを避けるための有効なフィルタリング
22	SSH	リモートアクセスを制限し、特定のIPアドレスを許可
80	HTTP	外部からのアクセスを許可
443	HTTPS	セキュリティのために暗号化された通信を許可

7.4. インバウンド・アウトバウンドルール

ファイアウォールの **インバウンド（Inbound）ルール** と **アウトバウンド（Outbound）ルール** は、通信の方向を制御するための設定です。これらのルールを適切に設定することで、外部からの不要なアクセスを防ぎつつ、内部からの通信を適切に管理できます。

■インバウンドルール

インバウンドルール は、「外部から内部へ入ってくる通信（受信）」を制御します。

例：インターネット上の誰からでもWebサーバーにアクセスできるようにする

送信元	宛先	プロトコル	ポート	アクション
任意（0.0.0.0/0）	Webサーバー	TCP	80,443	許可

■アウトバウンドルール

アウトバウンドルール は、「内部から外部へ出ていく通信（送信）」を制御します。

例：社内PCからインターネットへのアクセスを制限し、
特定のサイト(192.158.100.50)のみ許可します

送信元	宛先	プロトコル	ポート	アクション
社内ネットワーク (192.168.1.0/24)	192.168.100.50	TCP	80.443	許可
社内ネットワーク (192.168.1.0/24)	任意（0.0.0.0/0）	TCP	80.443	拒否

7.5. ポート開放とセキュリティリスク

ポート開放とは、**特定の通信を許可し、外部から内部ネットワークの特定のデバイスへアクセスできるようにすること** です。
ポートを開放すると、外部からのアクセスが可能になりますが、それに伴い**セキュリティリスク**が発生します。

例 <セキュリティリスク>

- 不正アクセスのリスク
- マルウェア・ボットネット感染
- DDoS攻撃（分散型サービス拒否攻撃）
- 内部ネットワークへの侵入

ポート開放が必要な場合は、以下の対策を取ることでリスクを最小限にできます。

安全にポートを解放する方法

- 不要なポートは開放しない
  - 使用しないポートは必ず閉じる
- アクセス制限をかける
  - IPアドレスを制限する（信頼できるIPのみ許可する）
  - ファイアウォールで通信のルールを明確化する
- 暗号化通信を利用する
  - HTTPS、SSH、VPNを利用し、暗号化された通信を行う
- ログ監視とアラート設定
  - ファイアウォールのログを監視し、不審なアクセスがないかチェックを行う
  - 異常な通信が検出されたら通知を受け取る設定をする

7.6. まとめ

まとめ

- ✓ ファイアウォールとは、外部ネットワーク（インターネットなど）と内部ネットワーク（企業のLANなど）の間に設置され、不要な通信や不正アクセスを防ぐためのセキュリティシステムです
- ✓ 制御方法は3つあります（パケットフィルタリング型、サーキットレベルゲートウェイ型、アプリケーションゲートウェイ型）
- ✓ ファイアウォールは、指定されたポート番号をもとに、データパケットの通過を許可するかどうかを判断し、ネットワークを不正アクセスから保護します
- ✓ 特定の通信を許可し、外部から内部ネットワークの特定のデバイスへアクセスできるようにすることをポート開放と言います。ポートを解放することによりセキュリティリスクが生じるため、安全にポートを解放するための対策が必要です