コンピュータネットワーク入門

コンピュータネットワーク

我々の生活に欠かせない存在となったインターネットですが、その起源は意外にも古く1969年頃まで遡ることができます。当時のアメリカ国防総省高等研究計画局(ARPA、現在のDARPAの前身)が、戦争に耐えられる情報通信ネットワークの構築を目的に開発されたARPANETがインターネットの起源と言われています。ARPANETの開発に関連し電子メールやハイパーリンクの開発も行われてきました。

通信方式の種類

コネクション型とコネクションレス型

コンピュータ同士が互いに接続を確立したい状態で通信を行う方式をコネクション型、接続は確立せずに通信を行う方式をコネクションレス型と呼びます。TCPはコネクション型、UDPはコネクションレス型です。各プロトコルについては後述します。

ユニキャスト・マルチキャスト・ブロードキャスト

接続の仕方による分類のほか、通信単位による分類もできます。単一の送信相手にデータを送信することをユニキャスト、複数の端末にデータを送信することをマルチキャスト、すべての端末にデータを送信することをブロードキャストと呼びます。なお、ブロードキャストはIPv6では実装されていません。

OSI参照モデルとTCP/IPモデル

OSI参照モデル

ネットワークをきちんと階層化して定義したものに、OSI参照モデル（Open Systems Interconnection reference model）があります。これは、表に示すように7階層に定義されています。各階層は、次に示すような機能を規定しています。

表1. OSI参照モデルの各階層

レイヤー	名称	役割
7	アプリケーション層	アプリケーション間のやり取り
6	プレゼンテーション層	データの表現形式
5	セッション層	接続の手順
4	トランスポート層	データ通信の制御
3	ネットワーク層	インターネットワークでの通信
2	データリンク層	同一ネットワーク上での通信
1	物理層	ケーブルや電気信号やコネクタなど

- アプリケーション層

　　アプリケーションごとのデータの形式や処理の手順などを規定します。Web、電子メール、ファイル転送などのプロトコルは、この層で規定されます。

- プレゼンテーション層

　　データの表現形式、例えば文字コードの種類や暗号化などを扱います。双方の機器の間で文字コードが違う場合の変換、通信の暗号化と復号といった処理はこの層で行われます。

- セッション層

　　クライアントとサーバーなど、プログラム間の接続手順を規定します。この層により、2つのプログラムの間でデータ交換を行う論理的な通信チャネルが用意されます。

- トランスポート層

　　実際にデータのやり取りを行うプログラムの間でのデータ伝送を実現します。エラーの訂正、データのブロックサイズの違いの吸収（大きなデータを小さなパケットに分割するなど）などはこの層で行います。

- ネットワーク層

　　ネットワーク上の2台のコンピュータの接続を確立します。下位のデータリンク層と同じように見えますが、データリンク層が同じ方式を使った1つのネットワーク上の接続を確立するのに対して、ネットワーク層は相互に接続された複数のネットワークの接続を定めるものです。これらの複数のネットワークは、同じ形式のものであっても、異なるものであっても構いません。

- データリンク層

　　イーサネット、無線LANなど、ネットワークの方式に基づいたメディアアクセス制御（MAC、Media Access Control）や実際のデータ伝送について規定します。つまり、それぞれのネットワーク方式が、どのように通信メディアを使ってデータを伝送するのかを定めています。これにより、LAN上やWAN上の機器の間の通信が実現されます。

物理層

実際のネットワーク媒体（ケーブルなど）の上を流れる電気信号の形式やコネクタなど、個々のネットワーク方式ごとに、ハードウェアにもっとも近い部分を規定します。

TCP/IP モデル

インターネットで使われているTCP/IPプロトコルは、OSIモデルに沿っていません。OSIモデルが構築される以前から、実用的なネットワークとして稼働していたということもありますし、ネットワークの普及期に様々な機種・OS・ネットワーク方式・アプリケーションが登場したから、OSIモデルのような詳細な階層分けが必要になったとも考えられます。

表2. TCP/IPモデルの各階層

レイヤー	名称	役割
4	アプリケーション層	アプリケーション間のやり取り
3	トランスポート層	プログラム間の通信、通信の制御
2	インターネット層	インターネットでの通信
1	ネットワークインターフェイス層	同一ネットワーク上での通信、ハードウェア仕様など

アプリケーション層

OSIモデルのセッション層からアプリケーション層に相当します。個々のプログラムの間で、どのような形式や手順でデータをやり取りするかを定めます。文字コードや画像などの形式、暗号化など、データの表現形式などもこの層で扱います。Webや電子メールなどのアプリケーションプロトコルはこの層に属します。

トランスポート層

OSIモデルのトランスポート層に相当します。通信を行うプログラムの間でのデータ伝送を実現します。必要に応じて、エラーの検出と回復や、双方向の通信路の確立なども行います。単にデータを伝送するだけのUDP（User Datagram Protocol）、信頼性のある双方向の通信を実現するTCP（Transmission Control Protocol）はこの層のプロトコルです。

インターネット層

OSIモデルのネットワーク層に相当します。複数のネットワークを相互に接続した環境（インターネットワーク）で、機器間のデータ伝送を実現します。IP（Internet Protocol）はこの層のプロトコルです。

ネットワークインターフェイス層

OSIモデルの物理層とデータリンク層に相当します。実際のネットワークハードウェアが通信を実現するための層で、各種イーサネット、無線LANなどがこの層に属します。また、モデムや光回線などを使って特定の相手と接続し、TCP/IPで通信するためのPPP（Point To Point）プロトコルなども、この層のプロトコルとなります。

ネットワーク機器

OSI参照モデルとTCP/IPモデルを確認したところで、主要なネットワーク機器を確認します。

ハブ

リピーターハブ（ハブと略される）は、物理層（ネットワークインタフェース層）で動作するネットワーク機器です。リピータハブは、電気信号の増幅のみ行い、パケットのルーティングなどはできません。

スイッチ

スイッチングハブやスイッチは、データリンク層（ネットワークインタフェース層）で動作するネットワーク機器です。MACアドレスによるルーティングやARP・RARPといったプロトコルに対応します。

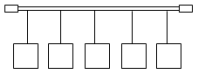
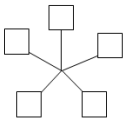
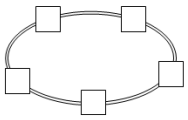
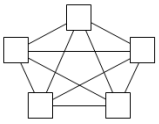
ルーターおよびL3スイッチ

ルータは、ネットワーク層（インターネット層）で動作するネットワーク機器です。ネットワーク層のプロトコルであるIPやOSPFなどのEGP(Exterior Gateway Protocol)、インターネット制御プロコトル(ICMP)やトンネリング(GRE)といった機能を提供します。

ネットワークトポロジー

ネットワークがどのように接続されているか、ということをネットワーク・トポロジーと呼びます。同軸ケーブルやトークンリングが普及していた頃はバス型やリング型といった接続形態が存在していましたが、現在ではLANではスター型、WANではメッシュ型の構造がほとんどです。表3に主要なネットワークトポロジーを記載します。

表3. 主要なネットワークトポロジー

名称	模式図	説明
バス型		一つの回線に複数のノードが接続される形 10Base-2や10Base-2同軸ケーブルに接続する場合に使われる。
スター型		中央の集線装置に全てのノードが接続される形 ノードの追加、削除が容易な形態で、現在のLANの主流形態 ツイストペアケーブルや光ファイバケーブル接続に使われる。
リング型		リング状にノードを配置した形LANトークンリング接続に使われた。
メッシュ型		多くのノードが相互接続する形態で、WAN、インターネットで使われる。一つの接続が切れても、迂回した接続があれば動作可能で、冗長性が高い。

インターネットの構造

インターネットの構造自体は単純で、語弊を恐れずに言うとメッシュ型ネットワークとスター型ネットワークの入れ子構造です。ルーターやL2スイッチを使ってLANを構成し、ルーターはISP(Internet Service Provider)が提供するWANへ接続されています。単一のISPが提供しているネットワークは、`自律システム(Autonomous System)`と呼ばれます。またISP内のネットワークは`IGP`と呼ばれるルーティングプロトコルで接続されています。ISP同士は異なるASを相互接続するプロトコルである`EGP(BGP)`で接続されています。概念図は次のとおりです。

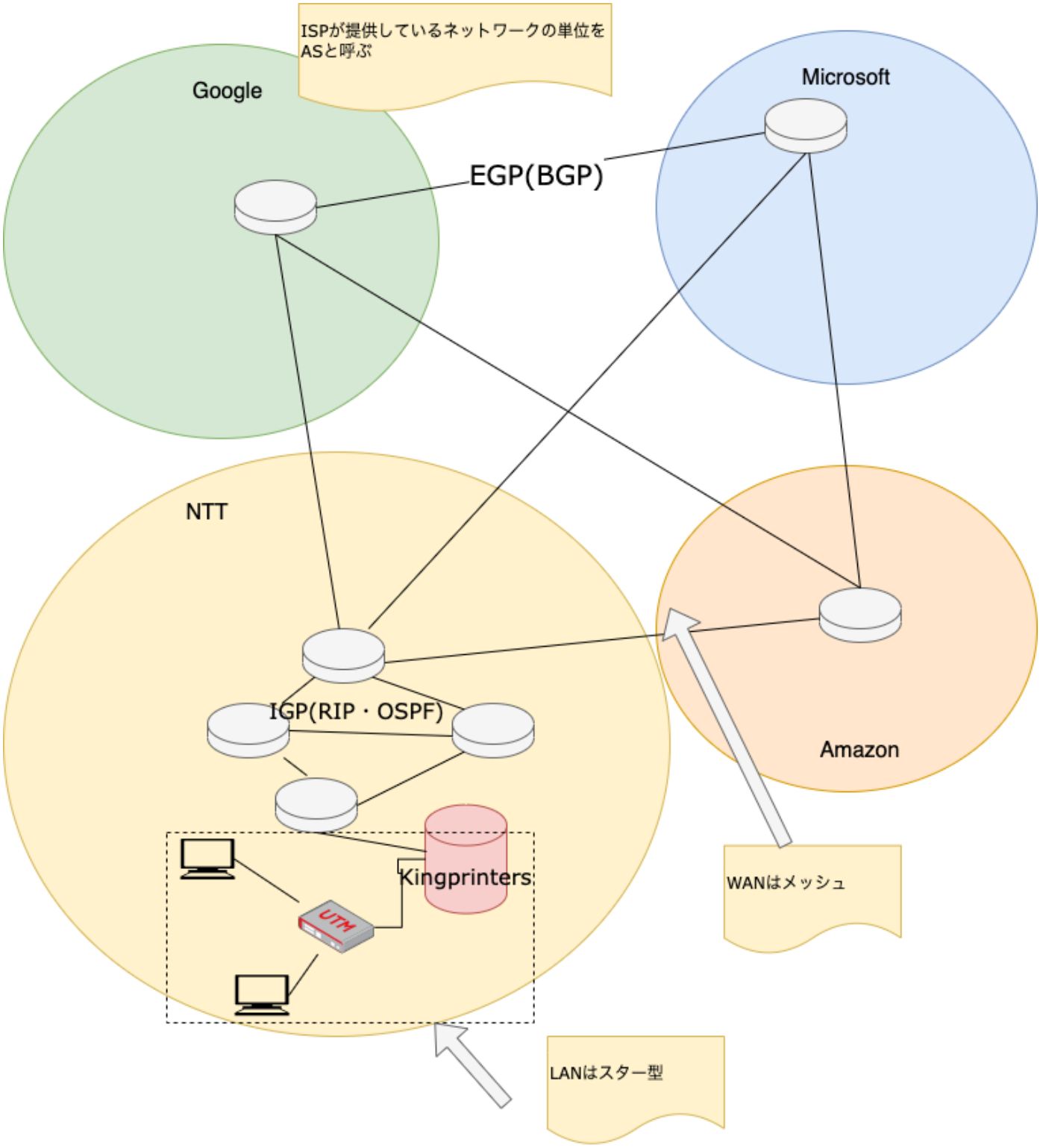


図1 インターネットの全体像

データリンク層

実際の通信においては、Ethernetに代表される物理媒体を使って行われます。データリンク層では、通信媒体で直接接続された機器同士で、データのやり取りをできるようにする役割を持ちます。

MACアドレス

Ethernetで接続された機器同士を識別するための情報を、`MAC(Media Access Control)`アドレスまたは、物理アドレスと呼びます。このアドレスは、L2スイッチなどデータリンク層で動作するネットワーク機器で利用され、Ethenetに流れる`データ（フレーム）`はかならず宛先MACと送信元MACが付与されます。そのため、Ethernetにおいて、MACアドレスのない機器は通信できません。MACアドレスは次のように48bitで構成されており、NICに焼き込まれています。このアドレスは全世界で重複することのないユニークなアドレスです。

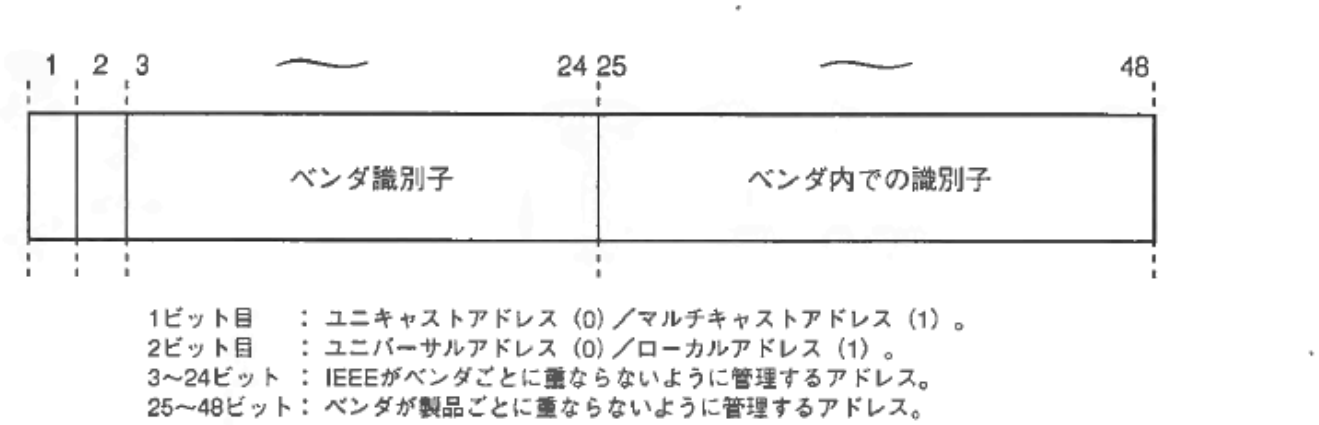


図2 MACアドレスのフォーマット [^tcp-ipより抜粋]

カプセル化

パケットがEthernetなどの物理媒体を流れるときには、次の図のような形式になります。ただし、この図はヘッダに含まれる情報などをかなり簡略化されています。

上位レイヤのデータは、下位のレイヤで宛先・送信先・ポート番号など各レイヤに関連する付加情報としてヘッダが付与されていき、データリンク層で最終的に物理媒体に流すためのフレームになります。このように上位レイヤの情報をかいレイヤの情報で包み込んでいくことを、カプセル化と呼びます。受信するときは逆の手順で下位レイヤのヘッダから順に外されていき最終的な受信データとなります。

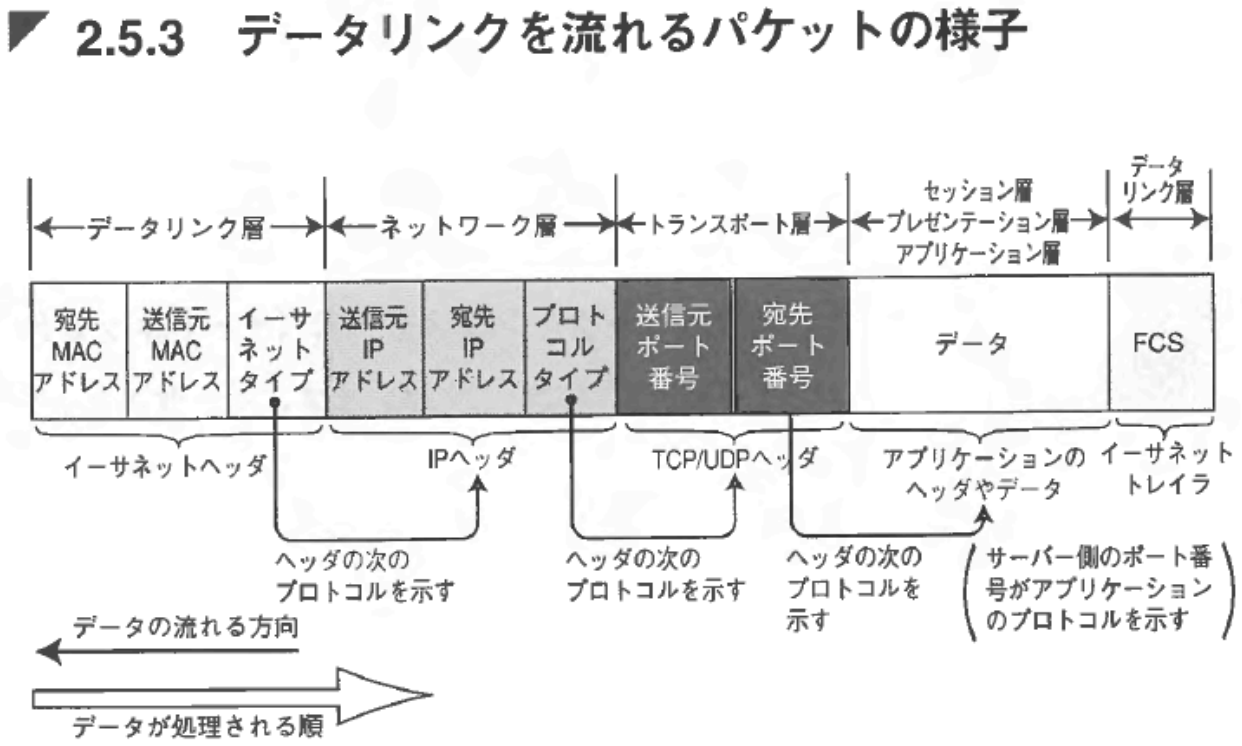


図3 パケットの流れ [^tcp-ipより抜粋]

IPプロトコル

IPはIPアドレスに基づいて、データの塊（パケット）を宛先ネットワークやホストに届けるプロトコルです。IPネットワークでは、IPアドレスをコンピュータやネットワーク機器に付与し、ルータがルートテーブルに従っての宛先に送り届けます。

IPアドレス

IPアドレスは、8bit(0~255)の数字を.区切りでつなげた4つの数字で表記され、ネットワークを表すネットワーク部と接続された機器を示すホスト部からなっています。

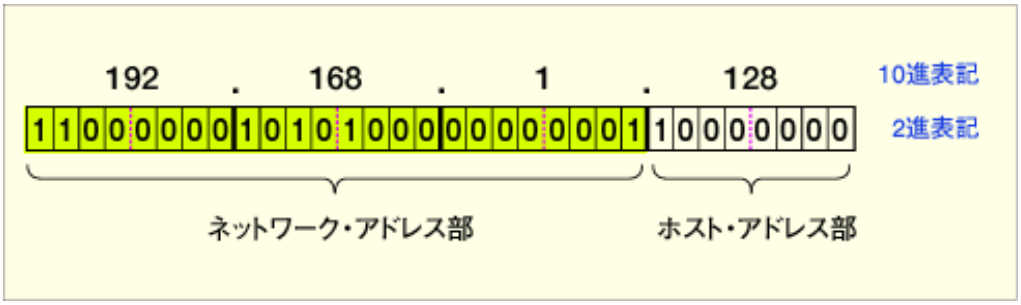


図3 IPアドレス [^ip-addrより抜粋]

アドレス方式

初期のIPv4アドレスの割り当てや運用で用いられていた方針で、アドレス空間全体をサイズの異なるクラスに分割し、組織の大きさなどに応じて発行する仕組みを `クラスフルアドレス方式` と呼びます。クラスフルアドレスでは、32ビットのIPv4アドレス全体をクラスAからクラスEまで5つのアドレスクラスに分割し、それぞれのクラス内で固定された数ごとに割り当てを行う。通常用いられるのはクラスA、B、Cの3種類で、クラスDとクラスEは実験用に予約された特殊な領域で一般的な用途での割り当てでは使われません。

上記のクラスフルアドレス方式は、割当の効率が悪いため現在ではブロック単位で割り当てができる `クラスレスアドレス方式` が使われています。

ネットワークアドレスとブロードキャストアドレス

クラスCのプライベートアドレスは、192.168.0.0~192.168.255.255 と決まっていますが、このなかで使用できうるのは、192.168.0.1~192.168.255.254の範囲のみです。192.168.0.0はネットワークアドレス（ホスト部がすべて0）、192.168.255.255（ホスト部はすべて1）で予約されているためです。

ネットワークアドレスは、ネットワークそのものを示すアドレスです。ブロードキャストアドレスは、ネットワークに所属するホスト全てと通信するためのアドレスです。

サブネット分割とCIDR

クラスCのプライベートアドレスは、192.168.0.0~192.168.255.255と決まっていますが、これだけでも65023台のホストが接続できます。小さな組織では、ホストは100台にも満たないでしょう。そのため、一つのネットワークを複数の小さなネットワークに分割することを `サブネット分割` と呼びます。分割するためのマスク情報を `サブネットマスク` と呼びます。例えば、192.168.0.0のネットワークを253台接続できるネットワークを考えます。253台つなげればいいので、8bit(=255)あれば足ります。

```
192.168.0.0
255.255.0.0
↓
192.168.0.0
255.255.255.0
```

そのためネットワーク部を255.255.0.0から255.255.255.0へ拡張することで、ホスト部を小さくしサブネットが作れるようになります。

また、この表記は

```
192.168.0.0
255.255.255.0
```

これを次のように簡略表記することができます。このような表記を `CIDR` と呼びます。

```
192.168.0.0/24
```

ルーティング[1]

ルーティングとは、`異なるネットワークにパケットを送信するときに最適な経路を求める`ことです。ルーティングは、ネットワーク層のネットワーク機器の役割です。これには、ルーターやL3スイッチなどが含まれます。これらの機器が宛先までのネットワーク間のガイドをしてくれることで宛先へパケットが到達します。

L3ネットワーク機器には、ルートテーブル（経路表）と呼ばれる、どこにパケットを送るかということが定義された情報を持っています。

ルートテーブルには、宛先ネットワーク・ゲートウェイ・インタフェース・種別・付加情報といった情報が定義されています。ルートテーブルに含まれる主な情報は次のとおりです。

情報	意味
宛先ネットワーク	パケットの宛先となるネットワーク
ゲートウェイ	パケットを次に転送する先
インタフェース	パケットを転送するルーター自身のインタフェース
種別	ルーティングの種類です。静的ルーティングの場合は static、動的ルーティングの場合は RIP、ルーター自身が管轄するネットワークの場合は implicit と表示
付加情報	ルーティングの種類ごとに使用する情報です。

ARPとRARP

ARP (Address Resolution Protocol）は、`IPv4アドレスからMACアドレス`を得られるプロトコルです

LANに接続されたコンピュータ間で通信するためには、IPパケットは下位のレイヤでL2ヘッダが付加された上で伝送されることからMACアドレスの情報が必要となります。しかしこれらのIPアドレスとMACアドレスは自動的な関連づけがないので、ARPでMACアドレスを得る必要があります

RARP (Reverse Address Resolution Protocol) とは、`MACアドレスからIPv4アドレス`を得ることのできるプロトコルです。ARPとは逆の動きのこのプロトコルは、現在ほぼ使用されていません。どのような場合に使用されるかというと、IPアドレスを持たないと通信できない機器であるにも関わらずIPアドレスの設定ができない（またはIPアドレスの設定が保存できない）機器がある場合に使用されます。

ICMP

ICMP（Internet Control Message Protocol）は、IP通信をサポートするプロトコルです。IP自体はベストエフォート型のプロトコルのため宛先に届くという保証はありません。ICMPは、IPパケットが宛先に正しく届いているかを確認したり、その結果を送信元に知らせたりする仕組みを提供し、TCP/IPが正常に通信できることを補助するためのプロトコルがICMPです。

ICMPを使用するコマンドには、`dig`、`ifconfig`、`traceroute`などがあります。変わり種としては、`tcptraceroute`などトランスポートレイヤで実装されるICMPコマンドもあります。

IP関連技術

DHCP 2

DHCP (Dynamic Host Configuration Protocol) は、`IPv4ネットワークにおいてIPアドレスの割当を動的`に行うためのプロトコルです。

IPv4での通信を行う際には、個々のホストにIPv4アドレス・サブネットマスク・デフォルトゲートウェイ・DNSサーバのアドレスを設定する必要があります。 このような設定は煩雑であるため設定ミスが起こりやすく、また台数が増えてくると手動での対応はできなくなります。 このような問題を解決するのがDHCPとなります。

DHCPを利用すると、個々のホストはDHCPサーバに問い合わせをすることで、 各種設定に必要な情報を入手して、自動的に設定してくれます。

DHCPでは、一定の範囲から自動的に割り当てたり、各ホストの識別子(MACアドレスなど)に対応した静的なアドレスを割り当てたりといった運用が可能です。

• NATとNAPT[3]

NAT（Network Address Translation）は、`ネットワークの内部と外部で通信する際、送信元や宛先のIPアドレス`を書き換える技術です。

通常イントラネット内のIPv4アドレスには、プライベートIPv4アドレスを使われていますが、インターネット上では、グローバルでユニークなIPアドレスで運用されています。そこで必要となるのがNATです。

ルーターのNAT機能は、ネットワーク内部の端末が外部ネットワーク（インターネット）のサーバーにアクセスするとき、送信元プライベートIPアドレスを、自身が保持しているグローバルIPアドレスに書き換えて送信します。

逆に外部ネットワークからルーターが保持するグローバルIPアドレスにアクセスがあった場合、ルーターはNATテーブルを参照し、宛先IPアドレスをネットワーク内部にある端末のプライベートIPアドレスに書き換えて送信します。

IPアドレスを1対1で変換する技術をNATと呼ぶのに対して、`IPアドレスと併せてポート番号も変換する技術`はNAPT（Network Address Port Translation）と呼ばます。

• VPNとトンネリング[4]

VPN接続は、トンネリングと暗号化によって実現されています。トンネリングを行えるプロトコルには　PPTP、L2F、L2TP、IPsec、GRE などがあります（プロトコルの詳細については割愛します）。一方、これらのうち暗号化を行えるプロトコルはIPsecだけとなります。従って、VPN接続のためにIPsecを使用すればこのプロトコルだけで暗号化とトンネリングを行うことができます。我々がリモートワーク中に使っているL2TP over IPsecは、L2TPでトンネリングしてIPsecで暗号化するタイプのVPN接続方式です。

TCP プロトコル

冒頭で述べたとおり、信頼性のあるコネクション型通信を実現するためのプロトコルが`TCP(Transmission Cntrol Protocol)`になります。SSHやFTPなど、通信の信頼性が要求されるプロトコルで利用されます。

TCPは、通信先とのコネクション確立のほか、通信フローの制御やウィンドウ制御といった通信にかかる細かな制御も行います。

TCPセッションの確立

IPアドレス＋ポート番号の組み合わせにより**「仮想経路（バーチャルサーキット）」**を確立し、論理的な伝送経路とする。 接続要求→受信側からの確認応答→送信側からの確認応答により最終的にコネクションを確立します。（**3ウェイハンドシェイク**）[5]

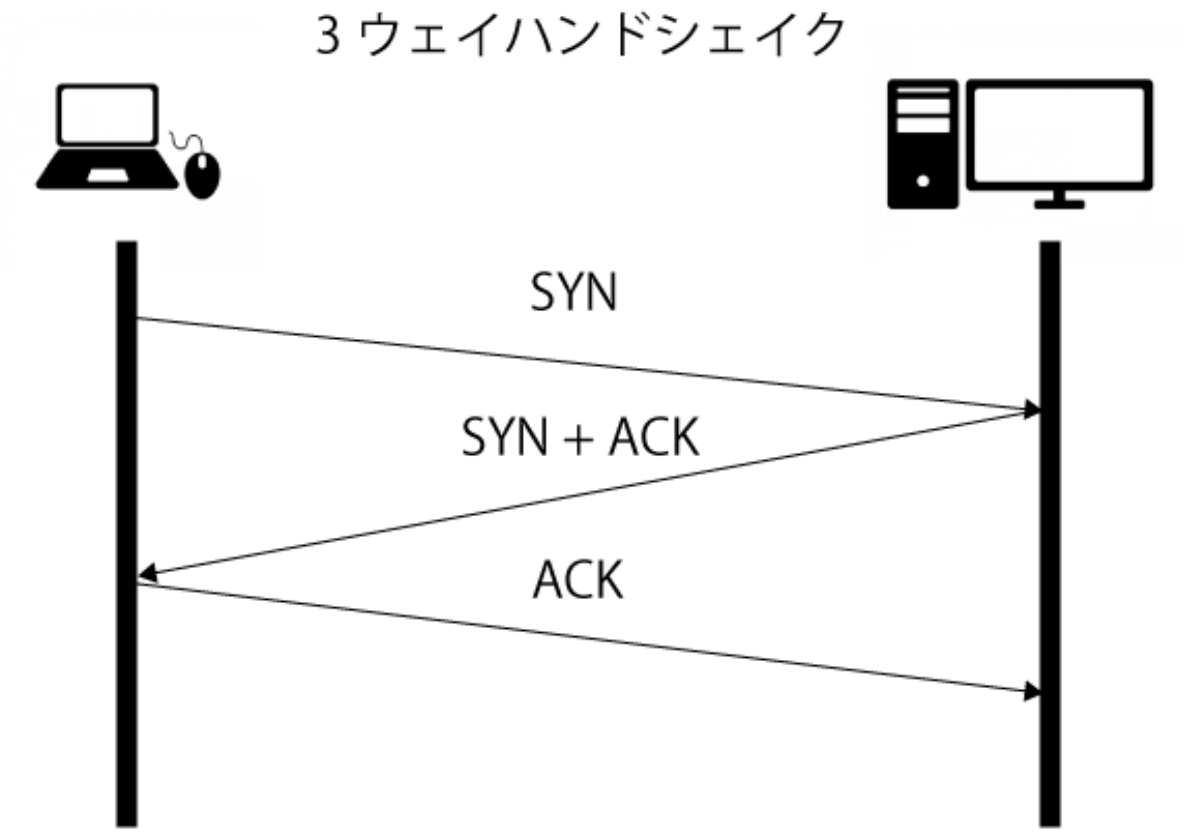


図4 3wayハンドシェイク

ポート

IPネットワークは、IPアドレスに従って宛先へ送信されると前述しましたが、使用するアプリケーション例えばメーラーとブラウザといったアプリケーションの違いを識別するにはポートと呼ばれる追加の情報使います。ポート番号のうち**0~1023のポートはウェルノウンポート(Welknown Port)**とよばれ、IANAによって管理されており用途が決められています。

TCP/UDP	ポート	プロトコル
TCP	20	FTP（データ）
TCP	21	FTP（制御）
TCP	22	SSH
TCP	23	Telnet
TCP	25(587)	SMTP
UDP	53	DNS
UDP	67	DHCP（サーバ）
UDP	68	DHCP（クライアント）
TCP	80	HTTP
TCP	110	POP3
TCP	123	NTP
TCP	443	HTTPS

1024〜49151まではユーザポート(User Port) と呼ばれ、アプリケーションによって登録済みのポート番号となります。**49152-65535まではエフェメラルポート(Ephemeral Port、あるいはローカルポート)と呼ばれ**、IP通信をするためにTCP/IPスタックから事前に定義されている範囲の値を自動で割り当てるためのポートです。

情報セキュリティの3要素

- 機密性(Confidentiality)
    - 正当な人のみがデータにアクセスできる
- 完全性(Integrity)
    - データの破壊・改ざんがされていないことを確実にしておくこと
- 可用性(Availability)
    - データが必要なときに取り出せること

情報セキュリティのレベルを考えるときには、機密性・完全性・可用性のバランスを考慮することが重要です。基本的に機密性と可用性はトレード・オフの関係にあるので、機密性を高めると可用性が悪くなり、可用性を高めると情報漏えいしやすくなります。

暗号化方式

共通鍵暗号方式

共通鍵暗号方式は、暗号化と復号化で`同じ鍵を使う方式`です。暗号化や復号が簡素なため高速に処理ができるメリットの一方、`共通鍵を相手と共有するための手間や通信相手が増えるについて鍵の管理が増える`というデメリットがあります。

共通鍵暗号方式は、固定長のブロック単位で行う`ブロック暗号`と、ビットストリーム単位で行う`ストリーム暗号`があります。

👉代表的な共通鍵暗号アルゴリズム

- DES・・・ブロック暗号（鍵長は56ビット）
- AES・・・ブロック暗号（鍵長は128/192/256ビットから選択）
- RC4・・・ストリーム暗号
- KCipher-2・・・ストリーム暗号

公開鍵暗号方式

公開鍵暗号は、`復号に使う鍵と暗号化に使う鍵をそれぞれ別にする方式`。暗号化や復号化の処理が複雑なため高速に処理はできませんが、`鍵の管理が共通鍵暗号に比べて簡易`であることが特徴。

👉代表的な公開鍵暗号アルゴリズム

- RSA・・・非常に大きな合成数の素因数分解の困難さを利用した暗号
- Elgamal・・・離散対数問題の難しさを利用した暗号
- DSA・・Elgamal暗号をもとにディジタル署名用途に開発された暗号
- 楕円曲線暗号・・・離散対数問題に楕円曲線を適用したもの

👉重要

公開鍵・秘密鍵は、`用途によって利用する鍵が異なる`ので注意する

- ディジタル署名

        - 秘密鍵で署名をし、公開鍵で本人確認・改ざん検出を行う
- 暗号化
        - 公開鍵で暗号化し、秘密鍵で復号する

ディジタル署名

ディジタル署名は、ハッシュ関数を利用することにより `メッセージの改ざん検出` と、 `本人認証` を可能にする技術です。ディジタル署名は、メッセージを送信したことを否認できなくする `否認防止` にも有効です。

ハッシュ関数

ハッシュ関数とは、次のような性質を持つ関数のことを指します。

- ハッシュ値の長さは固定長
- ハッシュから元のメッセージの復元は困難（原像回復困難性）
- 同じハッシュ値を生成する異なる2つのメッセージの探索は困難（衝突発見困難性）

👉代表的なハッシュ関数

- MD5
    - ハッシュ値は128ビット。
- SHA-1
    - ハッシュ値は160ビット。脆弱性が発見されているため**SHA-2へ以降を推奨**
- SHA-2
    - SHA-1に変わるハッシュ関数の規格。SHA-224、SHA-256、SHA-384、SHA-512などがある
- SHA-3
    - SHA-2に変わるハッシュ関数の規格。

ディジタル署名とPKI

ディジタル署名や公開鍵暗号を利用するときには、事前に相手の公開鍵を入手する必要があります。公開鍵の正当性は、認証局(Certification Authority, CA)によって保証されます。CAの役割は大きく分けて2つあり、1つは申請者を承認しディジタル証明書を作成し発行すること、もう1つはディジタル証明書の失効情報を管理・公開することです。

ディジタル証明書の構成

ディジタル証明書には、`ITU-Tが策定したX.509`があります。X.509の主な項目には次のような項目があります。

- バージョン番号
- 証明書シリアル番号
- 署名アルゴリズム識別子
- 発行者名（認証局名）
- 有効期限
- 所有者名
- 所有者の公開鍵

これらの項目をもとにハッシュ関数からハッシュ値を生成したものを秘密鍵で暗号化すると認証局のディジタル署名が得られます。

CRL（失効証明書リスト）

秘密鍵を漏洩するなどして何らかの理由で使えなくなったとき、この鍵ペアの効力がなくなったことを証明する証明書リストです。認証局が当該証明書を無効とし、署名書の失効情報をCRLに登録します。証明書の失効情報を関係者が確認する方法には、次の方法があります。

- OCSPモデル
    - ディジタル証明書の失効情報を保持したサーバーへ問い合わせる方法
- CRLモデル
    - 発行されたCRLをリポジトリに登録・公開し、利用者が確認する方法

PKI

公開鍵暗号を利用したセキュリティ基盤のことを`公開鍵基盤(Public Key Infrastructure)`と呼びます。PKIを利用するものには、SSLやTLS、S/MIMEがあります。

- SSL/TLS
- S/MIME

認証とアクセス制御

MFA(Multi Factor Authentication、多要素認証)

ユーザIDとパスワードによる認証に加えて、異なるデバイスに認証コードを送り認証コードを受信したデバイスで認証を許可することで認証の強度を上げる方法です

コールバック(Callback)

ユーザIDとパスワードによる認証に加え、公衆回線経由の各利用者に事前に電話番号を登録させその電話番号にかけ直して接続するという方法

ファイアウォール(Firewall)

ファイアウォールは内部ネットワークの防火壁として機能するセキュリティ機構です。ネットワークを、内部・外部・DMZに分割し、それぞれの境界で通信制御と監視を行います。

パケットフィルタリング型

パケットフィルタリングでは、パケットの送信元や相手先のIPアドレス、ポート番号などを検査し事前に決められたフィルタリングルールに基づいてパケットの通過・遮断をします。

WAF（Web Application Firewall）

WAFは、Webアプリケーションへの攻撃に特化したセキュリティ機構です。Webアプリケーションの脆弱性をついた攻撃などを検知してこれを防御します。

WAFで使われる検出パターンのリストには次の2つがあります。

- ブラックリスト方式
- ホワイトリスト方式

プロキシー(Proxy)

各パソコンからのインターネットのアクセス要求を代理して行うサーバのことを指します。これによりインターネットから隠蔽された環境で安全に外部との通信が可能になります。

侵入検知システム

侵入検知システムには、**IDS**と**IPS**がある。

- IDS(Intrusion Detection System)・・・不正アクセスを検知するのみ
- IPS(Intrusion Prevension System)・・・不正アクセスを検知し、遮断する

Webアプリケーションのセキュリティ対策

攻撃手法には様々な方法があります。代表的な攻撃手法を以下の表に記載します。

表3. 代表的な攻撃手法

名称	内容
SQLインジェクション	データベースと連携したWebアプリケーションで、データベースの不正操作を行う悪意のあるSQL文を埋め込んで情報を窃取する手法
セッションハイジャック	認証が終了し、セッションを開始しているWebブラザとWebサーバの通信においてCookieなどに埋め込まれているセッション情報を抜き出して、Webブラウザなどになりすます。
DNSキャッシュポイズニング	DNSサーバーのキャッシュ機能を悪用した攻撃。DNSキャッシュに偽のドメイン情報覚えさせることで利用者を偽装されたサイトに誘導する手法
DoS攻撃	インターネット上に公開されているサーバーに大量のデータや不正なパケットを送りつけて、コンピュータ資源やネットワーク資源を利用できない状況にする手法
リフレクション攻撃	DNSやNTPサーバーなどの「問い合わせに反射的な応答を返す」サーバーを踏み台にする攻撃
ポートスキャン	サーバーが公開されているポートを順に操作して侵入口となる脆弱なポートがないかどうかを調べる
バッファオーバーフロー	プログラムが確保した領域を超えるようなデータを与え、バッファを溢れさせる手法
パスワードクラック	パスワードを不正に探り当てること 辞書攻撃・類推・ブルートフォース
パスワードリスト攻撃	不正な手口で入手したパスワードのリストからWebサイトへのログインを試みる

マルウェア対策

マルウェアとは、コンピュータに有害なプログラムの総称です。

マルウェアの分類

アドウェア、ウイルス、トロイの木馬、ワーム

マルウェア対策

マルウェア対策として最も効果的なのは、ウイルス対策ソフトを利用することです。ただし、ウィルス対策ソフトも万全ではないので、OSやウィルス対策ソフトのバージョン常に最新にし、ウィルス対策ソフトのパターンファイルも最新の状態に維持することが重要です。

- **パターンファイルを最新の状態に保つ**
- **できるだけ最新のソフトウェアを使用する**
- **自動･リアルタイムスキャンをオンに設定しておく**
- **ウイルス対策ソフトは、全社共通のものを使用する**

1. https://network.yamaha.com/knowledge/routing ↩
2. https://www.nic.ad.jp/ja/basics/terms/dhcp.html ↩
3. https://www.infraexpert.com/study/ip10.html ↩
4. https://www.infraexpert.com/study/ipsec2.html ↩
5. http://software-engineering-lab.com/network/tcp.html ↩