*Masaru Kitajima*

# インターネットって何？Part 1

Open Door Chapel

# なぜインターネット？

- インターネットは、現在はインフラの一つとなっていて、無自覚なまま利用している事も多いです
- インターネットには様々なリスクがあります
- ガラケーだから安全と言う認識は間違いです
  - docomo.ne.jp・ezweb.ne.jp・softbank.ne.jpのメールアドレスを使う時はインターネットを利用しています

- ODCはFacebookと言うサービスでページを持っていて、皆さんにもフォローして欲しい
- 皆さんがFacebookに参加してくだされば、グループを作って、そこで会話する事ができます
- YouTubeと言う動画共有サイトで、メッセージ等のビデオを配信しているので、聖書の学びを深める復習教材として活用して欲しい
  - 等の理由で、インターネットを知って頂きたいと思っています

# 何を学んでいくか...

- およそ3回くらいで
  - ネットワークって何？
  - インターネットって何？
  - WEBって何？
  - E-mailって何？
- 等について、少し深く見てみます

# 実は2つあるインターネット

- 「インターネット」とカタカナで表記すると、同じ名詞になってしまいますが、「インターネット」には**広義のインターネット**と**狭義のインターネット**の二つがあります
- 両者の違いを見ていきたいと思います

# 広義のインターネット

- 2つ以上のコンピュータネットワークを相互に接続する技術の事です
- 英語ではinternetと表記して、「〜の間」を意味する”inter”と「ネットワーク(network)」の略語である”net”から作られた造語です

# コンピュータネットワーク

- コンピュータネットワークとは、複数のコンピュータを同一の物理的（ハードウェア）規格と論理的（ソフトウェア）規格で接続して、それぞれのコンピュータが通信できるようにしたものです
- ハードウェア規格とは接続する手段の事で、有線か無線か、どんなケーブルを使うか、コネクターの形状、無線の周波数、速度などです
- これが統一されていないと、物理的に接続できません

- ソフトウェア規格の事をプロトコルと呼びます
  - プロトコルとは元来は外交儀礼の事で、どの様な手順で外国の要人を迎えるかと言う事を定めています
- ソフトウェア規格としてのプロトコルも、どの様な手順で通信をするかを定めています
  - 手順の異なるもの同士では話が成立しません

# 現在主流のネットワーク

- ネットワークの起源は1950年代まで遡れます
- ネットワークが考案された当初は様々な方式が提唱され、実験されてきました
- その後、色々と変遷を繰り返して、現在は有線通信と無線通信の二種類があります

- 有線ネットワークのハードウェア規格はイーサネット（Ethernet）で、正式にはIEEE802.3と呼ばれます
  - イーサネットにも細かい規格があります
  - 考案当初より技術が進歩したので、より細いケーブルで、より速く通信できる様に改善を繰り返しています

- 無線ネットワークのハードウェア規格は正式にはIEEE 802.11と呼ばれますが、通称Wi-Fiです
  - Wi-FiはWi-Fi Allianceの登録商標です
  - Wi-Fiにも細かい規格があります
  - 考案当初より技術が進歩したので、より効率的に速く通信できる様に改善を繰り返しています

- 有線も無線も細かい規格がありますが、新しく作られた規格は以前の規格とも通信できる様にしていますので互換性があります
- ただし、Wi-Fiの最新規格であるIEEE 802.11acは、それまでのIEEE 802.11シリーズが周波数2.4GHzを利用していたのに対して5GHzを利用してる為、互換性がありません
- これはハブやルーターを介して解決します

- 有線通信も無線通信も、通信プロトコルとしてはTCP/IPかTCP/UDPの双方を使います
- この二つのプロトコルは「インターネット・プロトコル・スイート」と呼ばれるプロトコル群の一部です
  - TCP/IPはデータの欠落が許されない通信に使われます
  - TCP/UDPは動画再生の様に、多少データが欠落しても良い通信に使われます

- TCP/IPとTCP/UDPと書きましたが、これは二つのプロトコルの複合プロトコルです
  - TCPとIPまたはUDPです
  - ですが、IPもUDPもTCPが無ければ機能しません
  - 同様にIPやUDPが無ければTCPは無用の存在です
  - その為、TCP/IPやTCP/UDPと、セットで使われるのが一般的です

# 範囲による区分

- ナノネットワーク
- 近距離無線通信(NFC)
- ボディエリア(BAN)
- パーソナルエリア(PAN)
- ニアミー(NAN)
- ローカルエリア(LAN)
  - 家庭内(HAN)
  - 保存領域(SAN)
  - 無線(WLAN)
- キャンパス(CAN)
- バックボーン
- メトロポリタン(MAN)
- ワイドエリア(WAN)
- クラウド(IN)
- インターネット(IAN)
- 惑星間インターネット

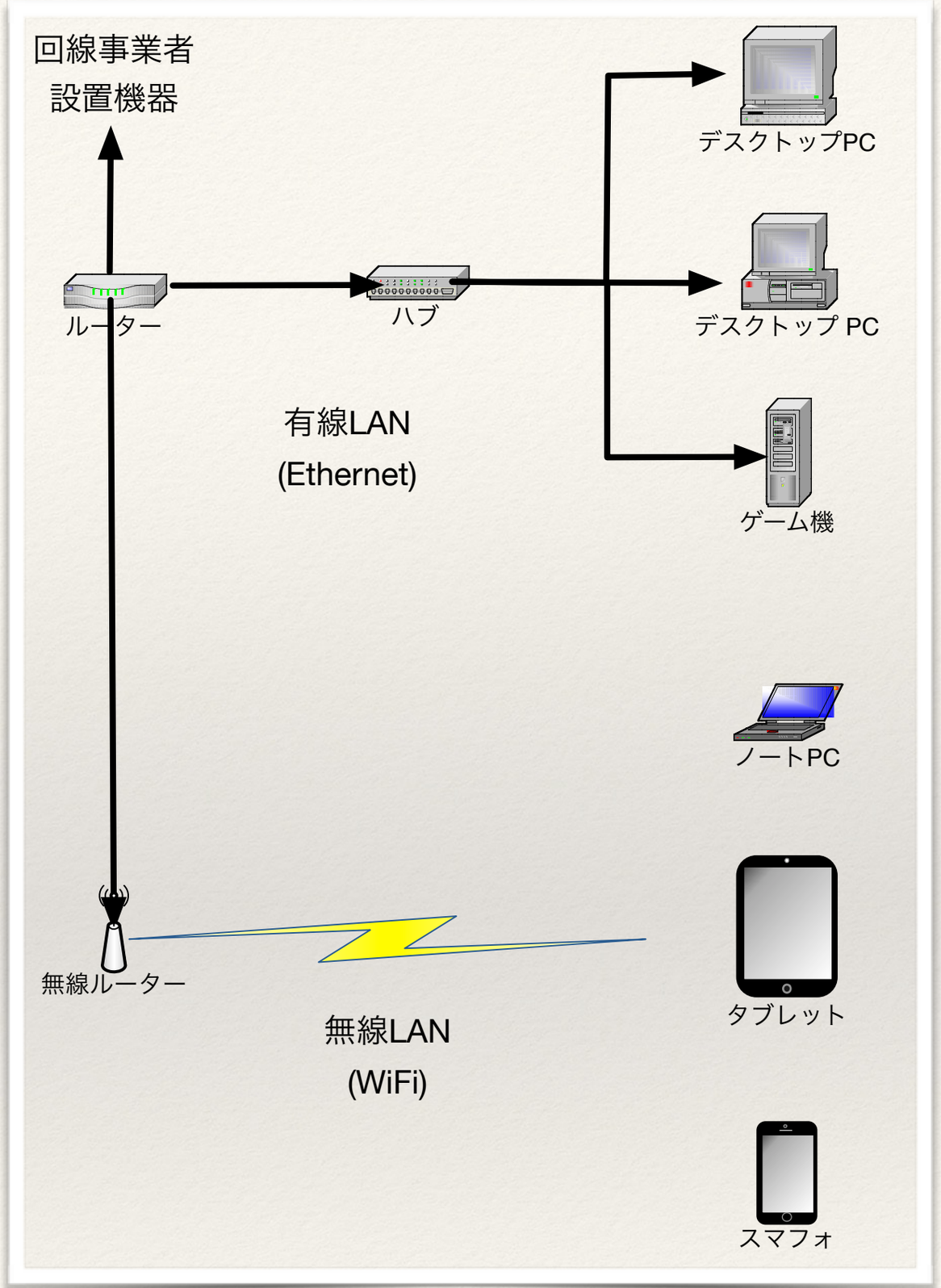
- 規約上は、様々な規模が想定されていますが、実際に使われているのは以下の三つがほとんどです
  - 局所的ネットワークであるLAN（Local Area Network）（含むWLAN）
  - LAN同士を接続した広域ネットワークであるWAN（Wide Area Network）
  - インターネット(IAN)
- ただし、iPhoneとApple Watchの様な関係はBANに当たります

- これは他の規模のネットワークが使われている事を否定しません
  - 惑星間インターネットは別ですが（笑）
- しかし一般の人が目にする機会が多いのはLAN・WAN・インターネットです

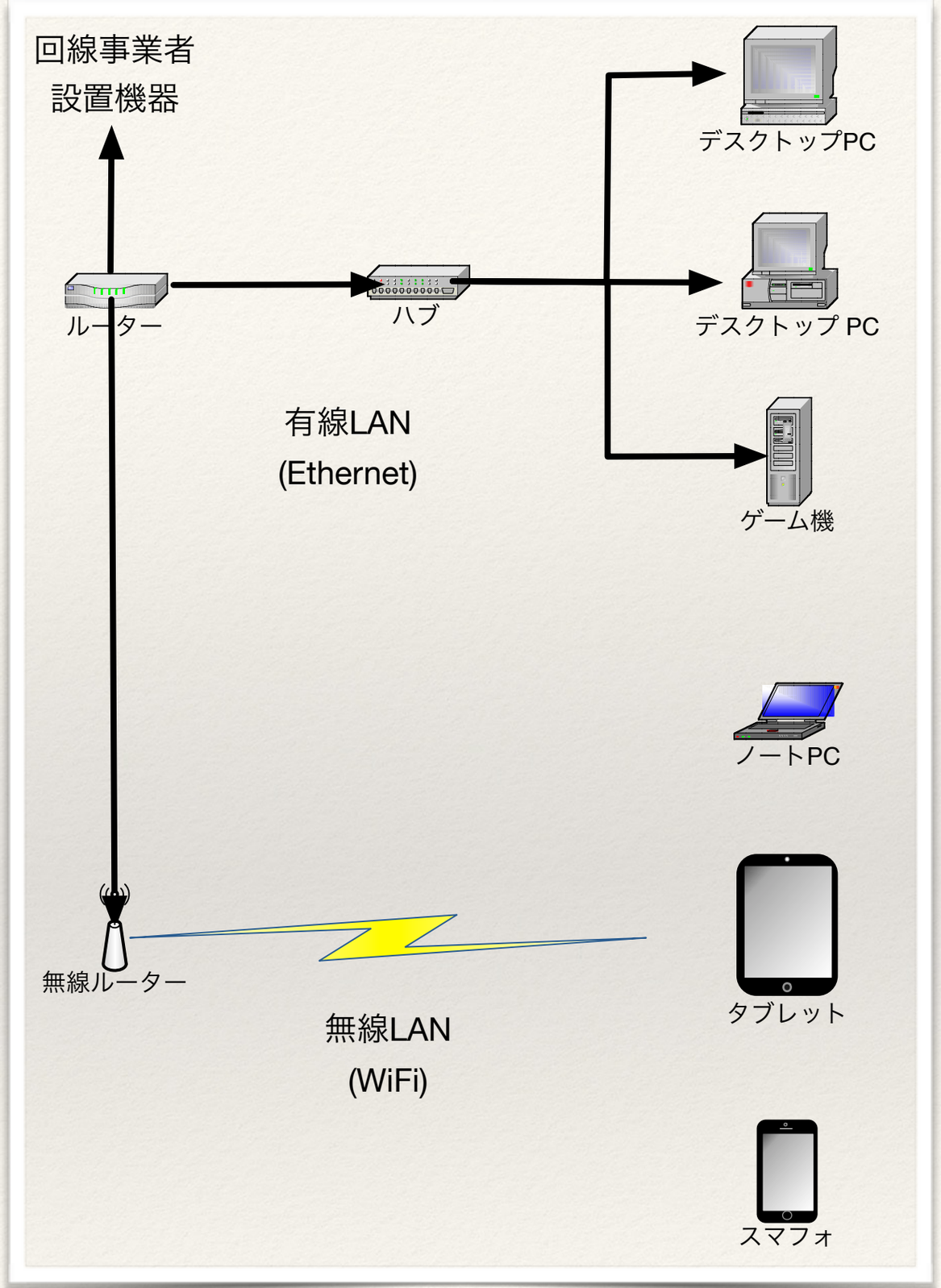
- LANとはLocalが示す通り、局所的なネットワークです
- ここで言う局所的とは、物理的・論理的に接続可能な範囲にある、と言う意味です
  - 家庭内
  - 小規模会社内
  - 小規模公共施設内
  - などです

# LANの構成

- 回線事業者設置機器とルータを接続します
- 回線事業者設置機器は外部に公開されています
- ルーターはLAN内の機器の通信を管理します
- ルーターは有線LANと無線LANと言う二つの方式を相互変換して通信可能にさせます



- 内部機器は基本的にルーターで接続されている機器同士でのみ通信できます
- ハブとは、ルーターの接続口の数を超える機器を接続したい時に、ルーターに接続して接続口の数を増やす機器です
- この状態を「閉じたネットワーク」と呼びます
- 内部機器はルーター経由でのみ外部と通信できます

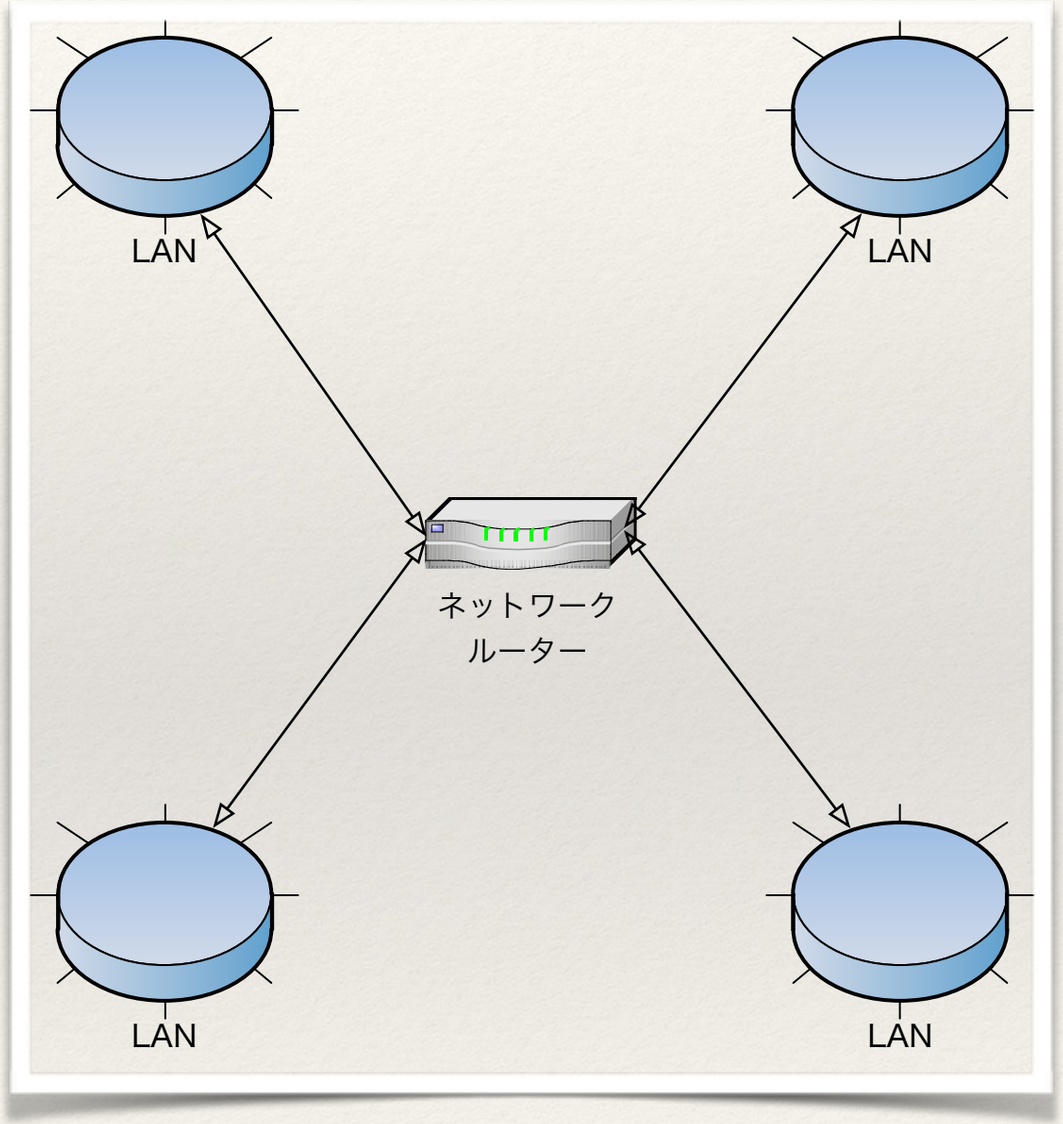


- これがLANの一般的な形態です
- 普通の家庭でインターネットを使っている方は、この構成になっています（無線があるかどうかは別です）
- 会社等の大きな組織でもこの構成が一般的です
- しかし、LANのLocalは「局所的」ですから、会社では
  - 部署を跨がない（論理的）
  - 別の階と接続していない（物理的）
- 事が前提になります

- 先の会社の例を考えると...
  - 他の部署
  - 他の階にある部署
- と接続するには、それぞれのLANを接続する必要があります
- つまり、WANを使います
  - この時、LANとLANを繋ぐ訳ですからinternetの技術を使います

# WANの概略

- この様に、それぞれのLANを束ねるネットワークルーターを介して相互に接続します
- ネットワークルーターはLANのルーターの大規模なものです
- ネットワークルーターから見ると、それぞれのLANはそのルーターしか存在が判りませんので、LANにおける内部機器と同じになります
- この様な形態のネットワークをスター型と呼びます



- WANを構成する場合、各LANのルーターの接続先は回線事業者設置機器ではなくて、ネットワークルーターになります
- つまり、WANはLANから見ると「外部」ネットワークになります
- WANを通じて、それぞれのLANの間でLANのルーターを経由して通信ができます
- 各LANの内部機器は自分のLANのルーターを利用してWANに接続して、ネットワークルーターを経由してのみ他のLANと通信できます

- また、会社を考えた時に本社と支社をネットワークで接続しています
- この場合は、LANやWANとは異なる通信方式を採用しているケースが大多数です
- 具体的には、NTTやKDDIが提供する本社と支社だけを結び、他とは接続しない専用回線を利用します

# コンピュータの住所

- ネットワークに接続したコンピュータ等の機器は、個別に識別されなければなりません
- Aさんが動画を見ようとした時に、Bさんの画面で再生されたら困りますよね
- そこで、各機器に住所を割り当てて、正しい相手と通信できる様にしました
- 住所は一定の規格で定められます

- 住所を決める規格は少々ややこしいので、次回解説します
  - ちょっとだけ数学の覚悟をしてください（笑）
- 住所は基本的には数字です

- この住所はネットワークの規模によって異なる5つの体系で割り当てられます
  - 複数のWANで構成される巨大WANで個別のWANに割り当てる数字は、それぞれのWANを個別に把握する必要がある為に重複が許されません
  - この数字は、巨大なWANの管理者によってWANで使える数字が割り当てられます

- LANにおいても、その内部機器を個別に把握する必要があります
- LAN内ではルーターの管理者が各機器に住所を割り当てます
- LANに新しい機器を導入する都度、手動で住所の割り当てをするのは煩雑ですし、住所の重複ミスを誘発します
- そこで、一般的にはLANではルーターが自動的に機器に住所を割り当てる仕組みを使っています
  - 賢い事に、ルーターは住所を持つ機器が取り外されたら、その住所を解放して、他の機器に使い回します。

- 住所はネットワーク内で機器を特定する為に使われます
- WANであれ、LANであれ、そのネットワーク内では住所の重複は許されません
- しかし、別なWANやLANは相互に関係性がありません
- ですから、WANやLANの中で使う住所は異なるネットワーク内の住所とは重複しても問題になりません

# 狭義のインターネット

- 私たちがWEBを見たり、電子メールを送ったりしている時に利用しているものです
- 日本語でインターネットと言う場合は通常はこちらの意味です
- 英語では”the Internet”と記述して明確に区別しています
- the Internetは「コンピュータ通信の世界規模のインフラ」と言えます

- インターネットは、インターネット・プロトコル・スイートを使用して、複数のWANやLANを相互接続した、グローバルなネットワークでIAN（Internet Area Network）です
- インターネットに接続するには、必ずIAN側の住所が必要になります
- 接続しているWANやLANの規模は、個人から公共機関・商用組織・教育期間・政府等の様に大小様々です

# IAN側の住所

- 家庭内LANであれば、ルーターがIAN側の住所を持ちます
- 会社等であればネットワークルーターがIAN側の住所を持ちます
- WAN同士を接続した巨大WANのある会社等であれば、中心となるネットワークルーターがIAN側の住所を持ちます

# 管理者不在の原則

- インターネット(the Internet)には、先ほど述べた様な色々なコンピュータネットワークが接続していますが、全てのコンピュータネットワークは原則的に対等な関係と言う原則があります
- そして、インターネットに接続している全てのコンピュータネットワーク全体を管理している上位組織は存在しません

- 各コンピュータネットワークの管理主体は、それぞれの組織によって異なります
- インターネットは、それらの組織の管理者が許容した情報の種類に類応じて、**善意で解放**したものが自分の管理するコンピュータネットワークの内、IAN側の住所を持っているルーターやコンピューターを通過させます
- これは善意、即ちボランティアベースですので、私の通信が数百のサーバーを経由したとしても、それらの管理者から費用を請求される事はありません

- ここで重要なのは、IANアドレスを所有してインターネットに公開されている機器は同時に内部ネットワークに接続されていると言う事です
  - そうでなければ、そのネットワーク内からインターネットに接続できませんよね？
- その為に、これらの機器は一般に非武装地帯(DMZ)に置かれます

- DMZは内部ネットワークと外部ネットワークからの接続を許容します
- 一方DMZからは外部ネットワークだけに接続を許容します
  - **DMZに置かれた機器から内部ネットワークには接続できません**
- つまりDMZにある機器の設定やメンテナンスは内部ネットワークからは行えず、管理者自らDMZに行ってDMZ内で作業をする必要があります。

- こうする事で、外部ネットワークはDMZには接続できるけれども、その先に何があるかを知る事はできませんので、外部ネットワークから内部ネットワークへの侵入を防いでいます
  - DMZにある機器は乗っ取られる危険があります
- DMZにも色々な手法がありますが、総じてファイアウォール（防火壁）と呼ばれます
- 家庭においてはルーターがDMZの役割を果たしています

- 例えば、私が今ここからGoogleの検索サイトに接続しようとした時に
  - 「Googleに接続したい！」と要求します
  - この時、直接Googleに接続される事は、ほぼあり得ません（アメリカにありますし...）
  - 先に述べた**善意で解放**されているIANに接続している機器を複数経由して、Googleに接続されます

- この時、どの様な機器の経路を通るかを決定する仕組みがルーター毎に備わっています（経路制御）
- つまり、その瞬間に最適と思われる経路を通ります
- 例えば、一つのWEBページを見ていても、それぞれのデータ（文章や画像など）は別な経路で送られて来ている可能性があります
- 経路によって速度が違う為にデータが正しい順番で届かない事もありますが、そこはプロトコルが解決してくれます

- これは、一見無駄な事をしている様に見えます
- しかし通信中に経路として利用していたネットワークが障害によって通過が不可能になる事はあります
- またはそのネットワークに接続が集中して、速度低下になる事もあります
- その時にはルーターの経路制御機構はそれを把握して代替の経路を探してくれます
- このお陰でインターネットの接続性が保たれている、非常に重要な機能です

- つまり、インターネットは各ネットワーク管理者が善意で解放している機器を経由して相互通信を可能にしているインフラと言えます
- 逆説的ですが、インターネットはこのような善意のネットワークと、大手の通信会社等が設置する負荷分散装置や海底ケーブル・衛星通信などを利用して成り立っていますが、それぞれ管理主体が異なります
- よってインターネット全体を**管理している主体は存在しません**