

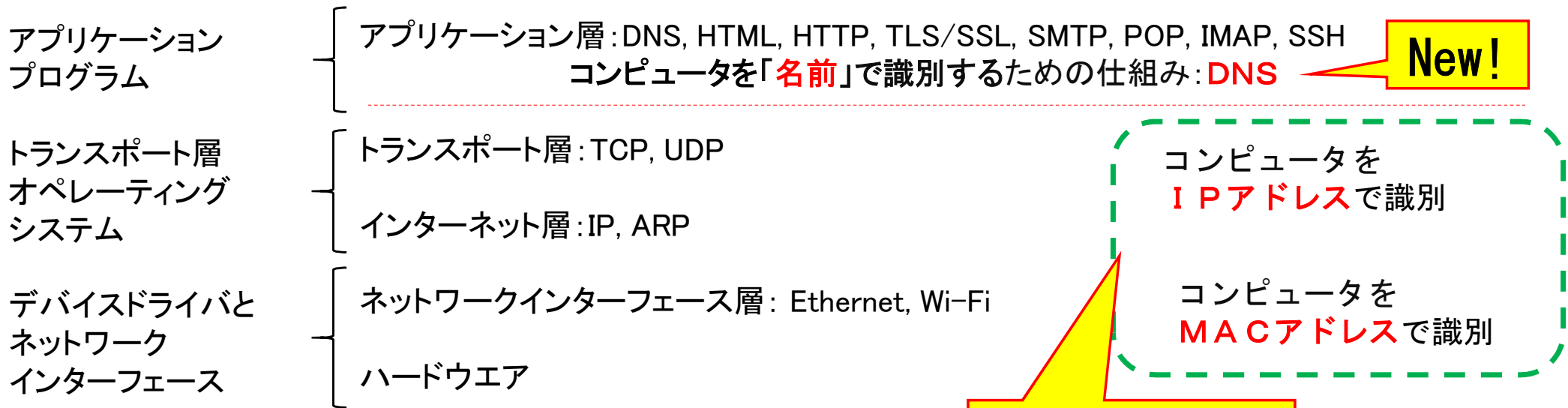
船舶海洋情報学

02. ネームサービス(DNS)／DHCP



九州大学
KYUSHU UNIVERSITY

TCP-IPプロトコルの階層



人間にとって
分かりにくく不便!

DNS (Domain Name System)

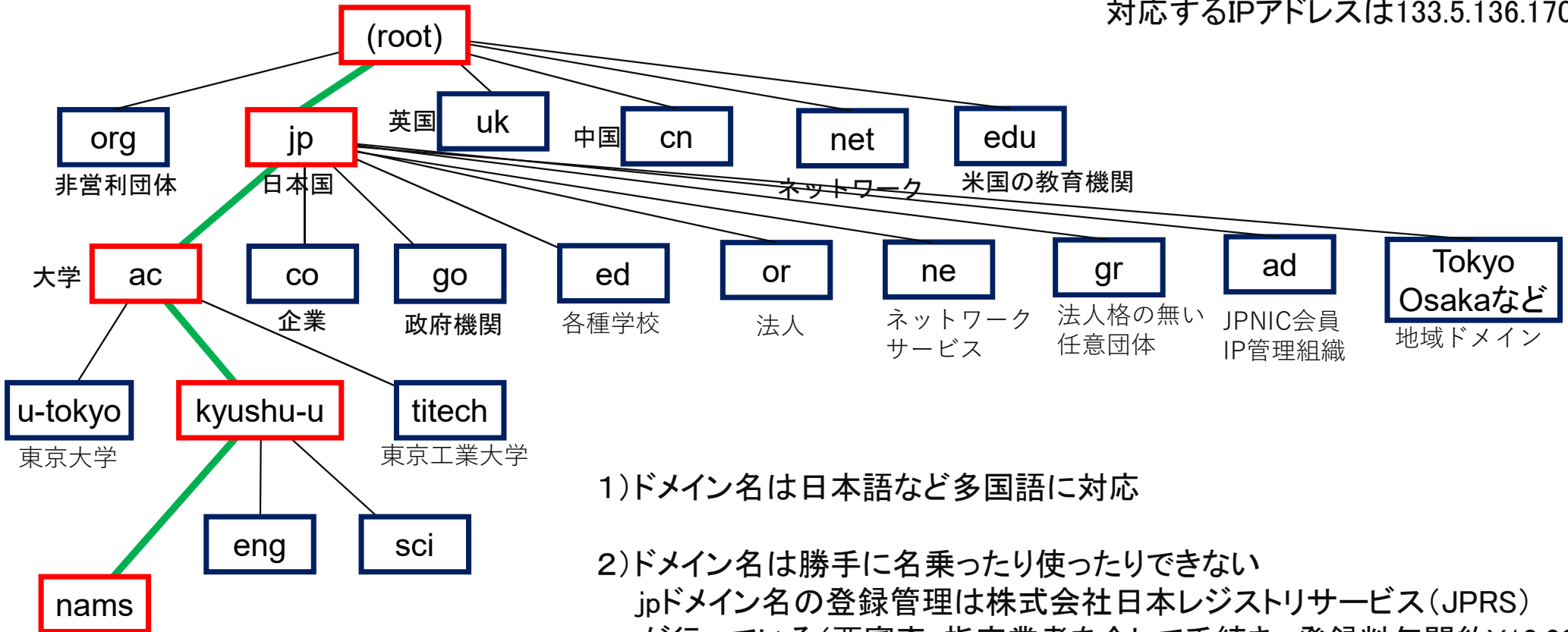
ローマ字やピリオドを使った名前からIPアドレスへの変換、およびその逆変換を行う仕組み

ドメイン名の構造

・ドメイン名: 「ホスト名」や「組織名」を識別するための階層的な名前

例) $\overbrace{\text{sysplan}}^{\text{ホスト名}}.\overbrace{\text{nams.kyushu-u.ac.jp}}^{\text{所属組織名(階層構造を持つ)}}$

対応するIPアドレスは133.5.136.170



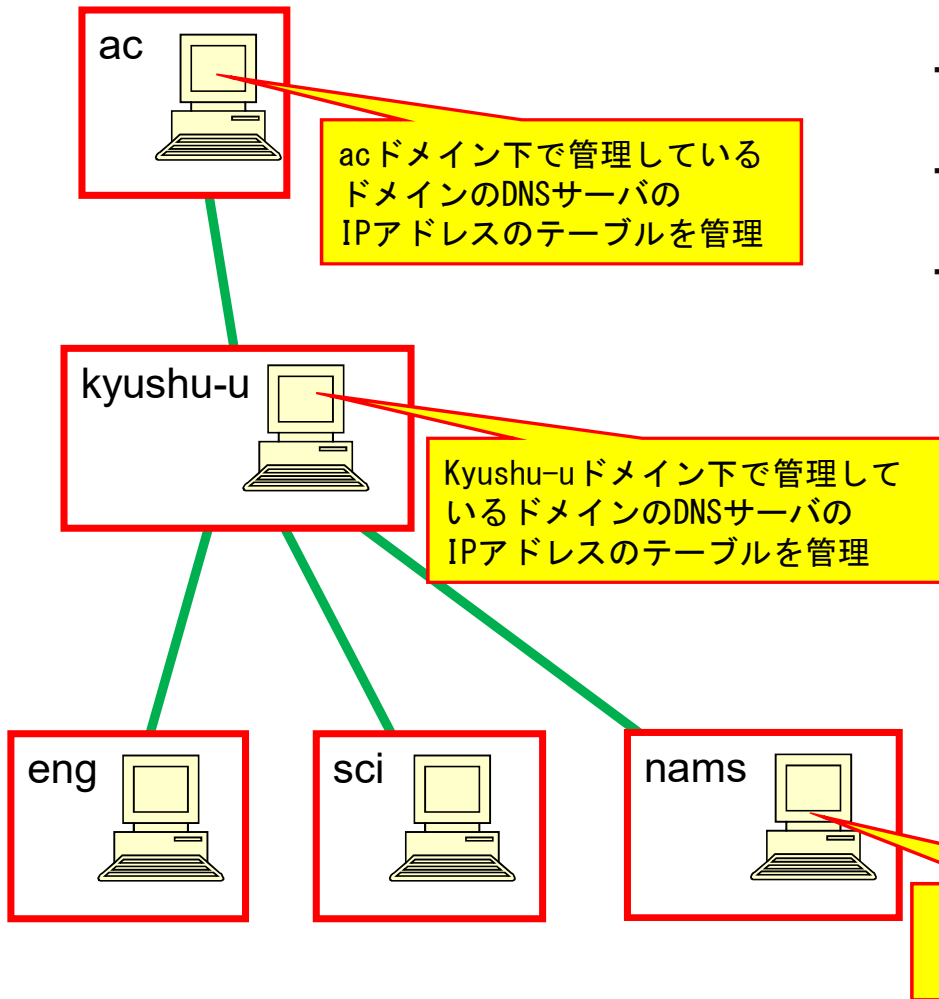
1)ドメイン名は日本語など多国語に対応

2)ドメイン名は勝手に名乗ったり使ったりできない

jpドメイン名の登録管理は株式会社日本レジストリサービス(JPRS)が行っている(要審査:指定業者を介して手続き、登録料年間約¥10,000)

ドメイン名は会社名などの「商標」に準じてビジネス上重要なため高額で取引される場合がある

ドメイン名を管理するホストやソフト: ネームサーバ(DNSサーバ)



- ・それぞれのドメインの階層毎にネームサーバが配置
- ・各ネームサーバは下階層のネームサーバの情報を管理
- ・全てのネームサーバはrootから木構造で結ばれる
- ・ルートから順番に辿ることで世界中のホストへ接続

- ・管理しているドメインより下の階層であればホスト名やサブドメインを自由に設定可能 (IPアドレスは割り当てられた範囲内に制限)

インターネット上の分散データベース

- ・各階層のDNSサーバは、障害発生に備え複数設置されることが多い:
プライマリサーバ=オリジナルデータ保持
セカンダリサーバ=プライマリから定期的にデータをコピー

ネームサーバ(DNSサーバ)の利用

・DNSの正引きレコードの例 (namsドメイン)

キャッシュ時間	43200	ネームサーバ	メールサーバ 優先度
nams.kyushu-u.ac.jp.	43200	IN NS	hosting3.nams.kyushu-u.ac.jp.
nams.kyushu-u.ac.jp.	43200	IN MX 10	vwall.nc.kyushu-u.ac.jp.
rie.nams.kyushu-u.ac.jp.	43200	IN MX 10	vwall.nc.kyushu-u.ac.jp.
vortex.nams.kyushu-u.ac.jp.	43200	IN MX 10	vwall.nc.kyushu-u.ac.jp.
rie.nams.kyushu-u.ac.jp.	43200	IN MX 30	rie.nams.kyushu-u.ac.jp.
vortex.nams.kyushu-u.ac.jp.	43200	IN MX 30	vortex.nams.kyushu-u.ac.jp.
mserver2.nams.kyushu-u.ac.jp.	43200	IN A	133.5.136.90
FDDI.nams.kyushu-u.ac.jp.	43200	IN A	133.5.136.254
rie.nams.kyushu-u.ac.jp.	43200	IN A	133.5.136.10

DNSに問い合わせを行うホストやソフト: **リゾルバ(resolver)**

IPアドレス (IPv4)

例) Windowsのコマンドプロンプトで以下を実行するとIPアドレスを得る(正引き/逆引き)

> **nslookup** system.nams.Kyushu-u.ac.jp

ドメイン名 → IPアドレス : 正引き

- ・インターネット層以下の階層で通信するために通信相手のIPアドレスは必須
- ・IPアドレスさえ分かれば接続はできる
- ・複数のドメイン名に同じIPアドレスが割り当てられている場合がある(**alias**)

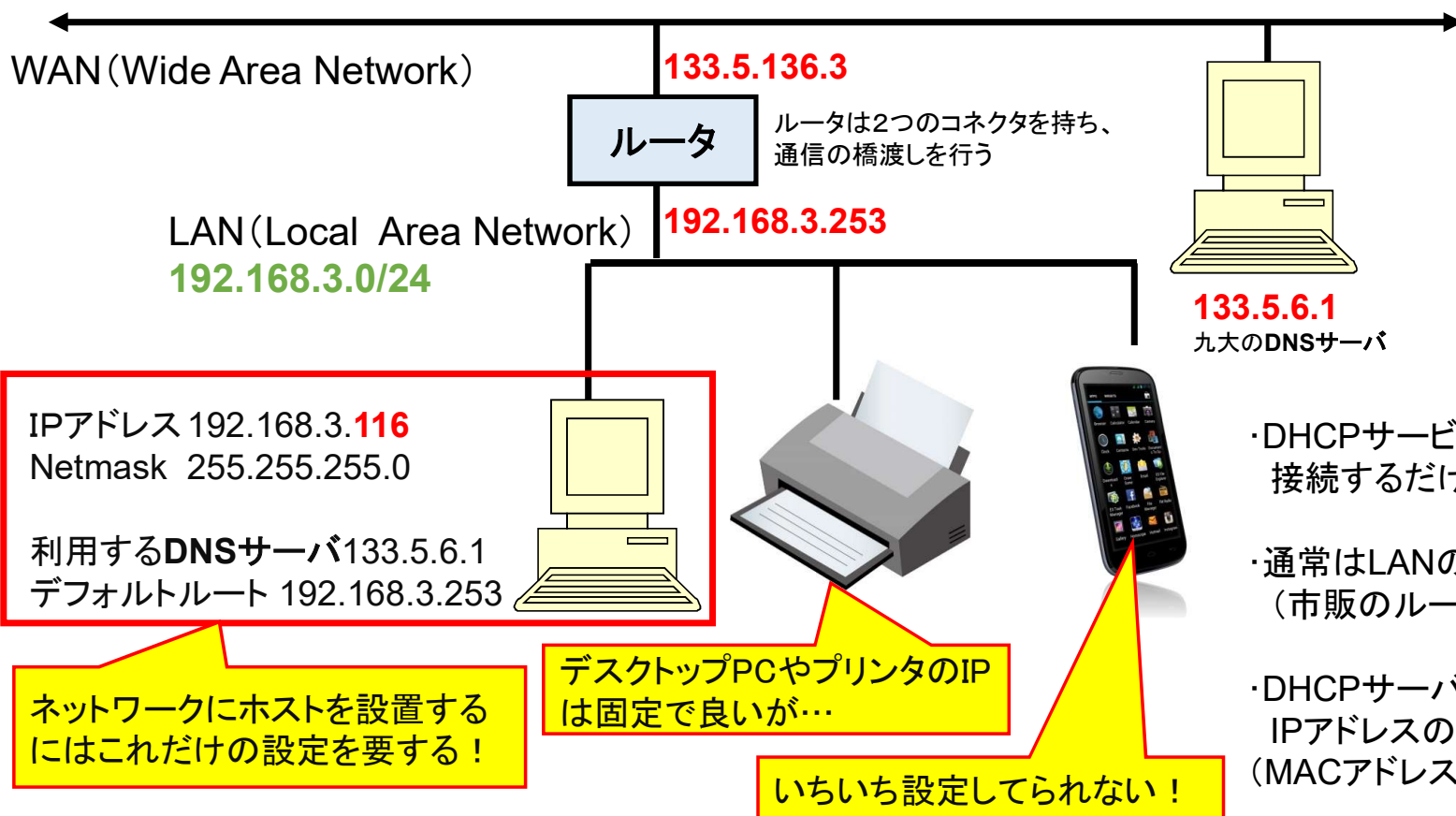
IPアドレス → ドメイン名 : 逆引き

- ・例えばインターネット上のサーバへ接続してくる不特定多数のホストは、そのIPアドレスのみをサーバへ開示している
接続してきたホストの所属(組織名など)を確認するためDNS逆引きを利用
- ・DNSの逆引きレコードに記載されていないIPアドレスは、身元不明で不正アクセスの可能性あり
セキュリティの厳しいサービスでは、DNS逆引きできないIPアドレスからの接続を拒否するが多い

-
- ・ドメイン名の取得・管理と、IPアドレスの取得は、一般に別々に行う
 - ・IPアドレスはインターネットプロバイダから割り当てられ、DNSの管理も基本的にプロバイダに依頼
 - ・DHCP(後述)を利用しているためIPアドレスが固定できない場合は**ダイナミックDNS**(DDNS)というネームサービスがある

DHCP (Dynamic Host Configuration Protocol)

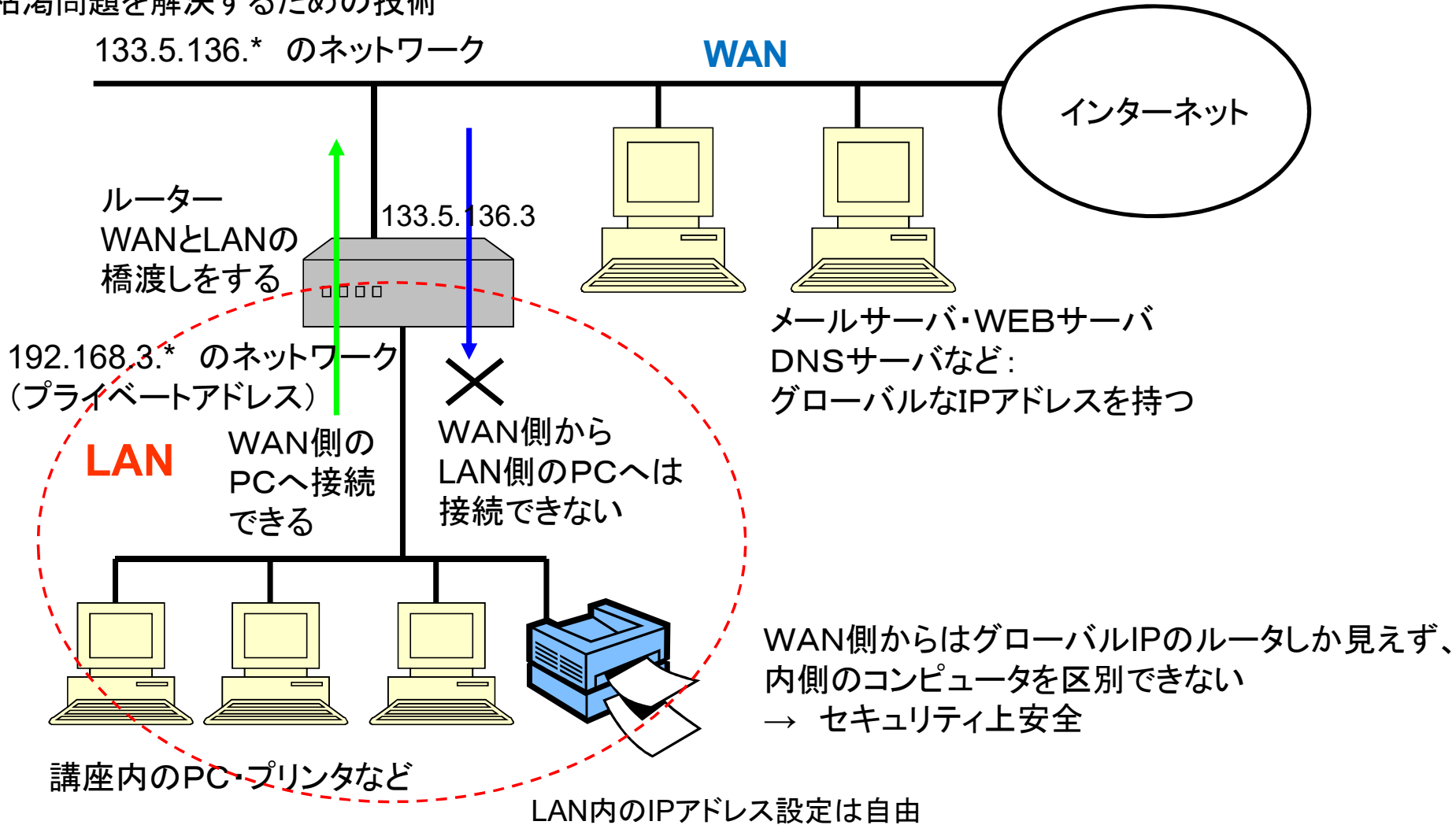
- ・いわゆる「自動ネットワーク接続」「プラグ & プレイ」の仕組み
- ・PCの設定で上記を選択するとDHCPサービスを利用したネットワーク設定になる



- ・DHCPサービスを利用すると、物理的にネットワークへ接続するだけで通信に必要な設定が自動的に行われる
- ・通常はLANの中にDHCPサーバを設置すべし (市販のルータの多くはこの機能を持っている)
- ・DHCPサーバは、リクエストに応じて予め設定したIPアドレスのリストから使っていないものを選んで割当 (MACアドレス毎に固定割当も可能)

NAT (Network Address Translator)

- ・LANの内側でプライベートIPを使い、インターネットへ接続するときグローバルIPアドレスへ変換する仕組み
- ・IPv4のアドレス枯渇問題を解決するための技術
- ・ルータの機能

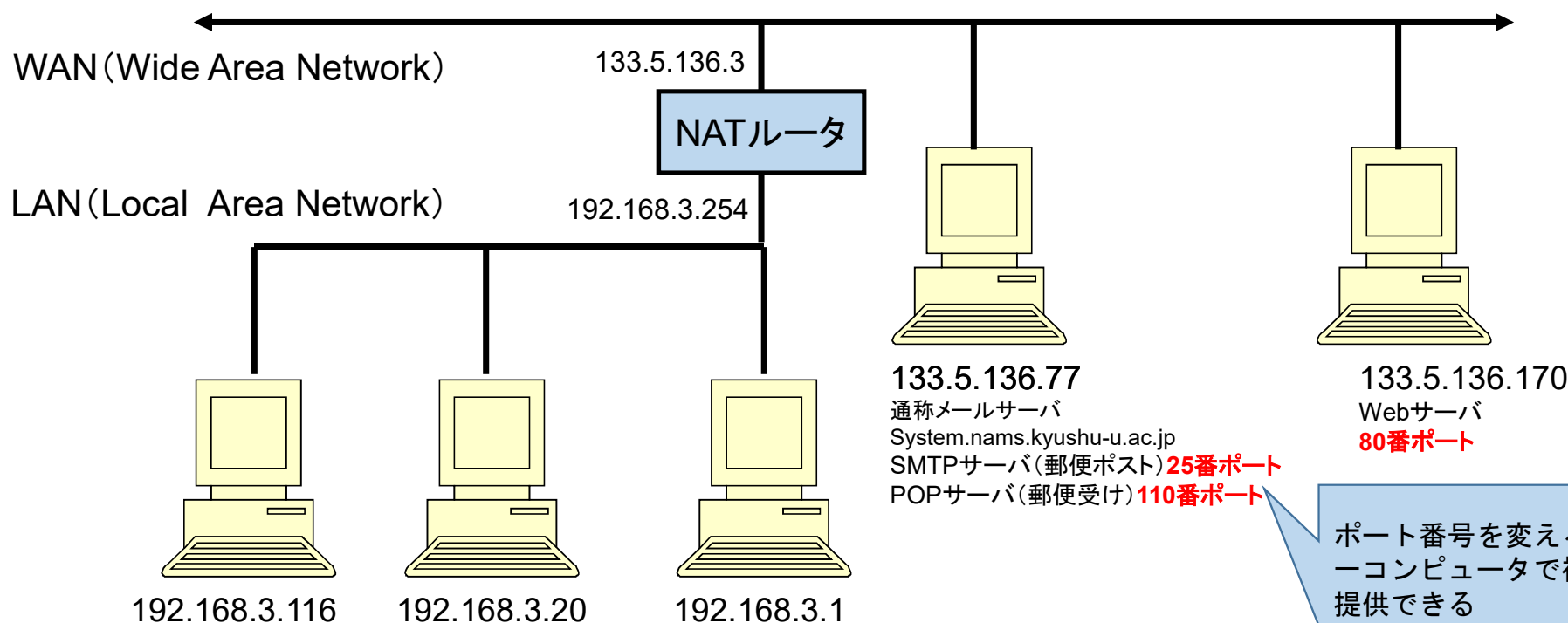


【復習】各IPアドレスのコンピュータにおけるサービスの区別

「IPアドレス」でコンピュータを区別

さらにサービスも区別せねばならぬ →

各コンピュータにサービス受付の「**ポート番号**」



LANの内側のホストは、通常WAN側から接続できない
(WAN側からはLAN内の全てのホストをNATルータのインターネット側のホスト1台として認識)

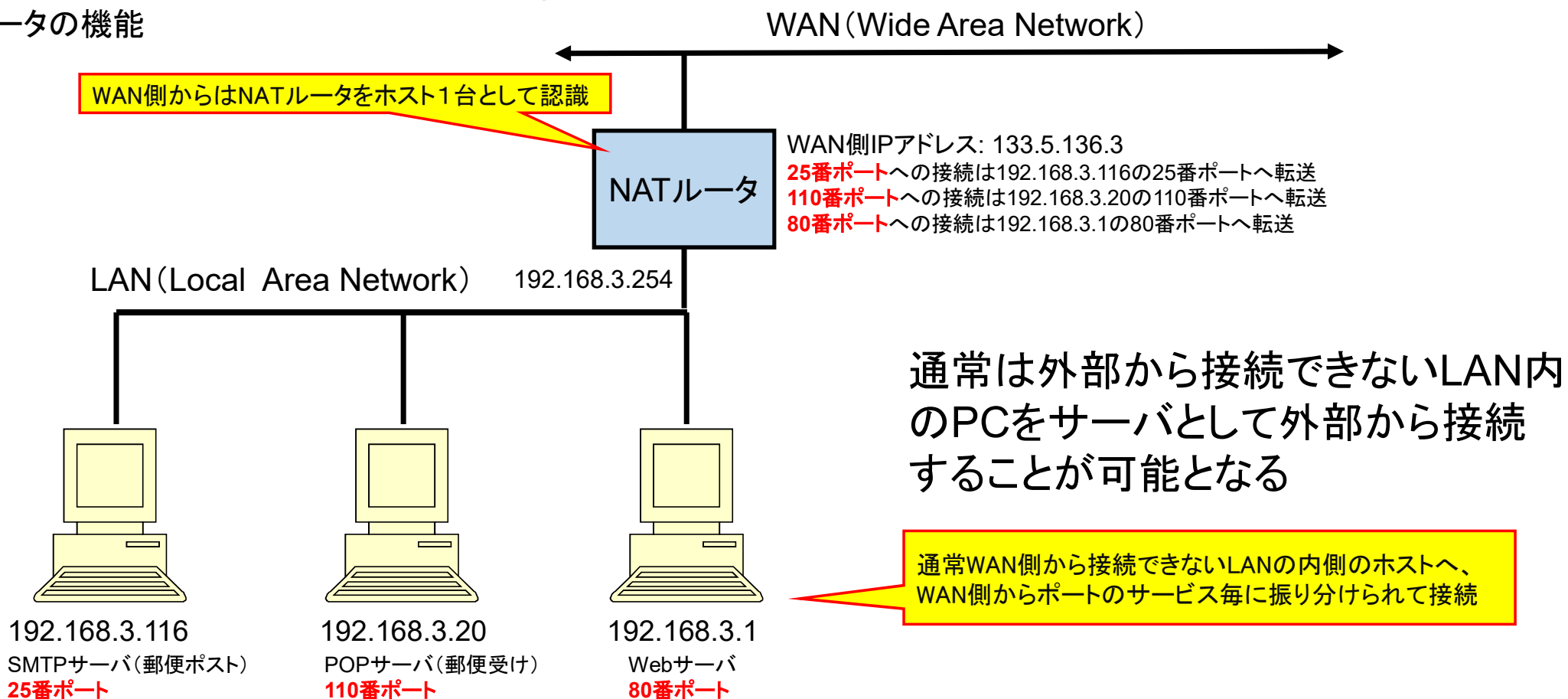
ポート番号を変えることにより、同一コンピュータで複数のサービスを提供できる

有名なプロトコルのポート番号はほぼ決められている

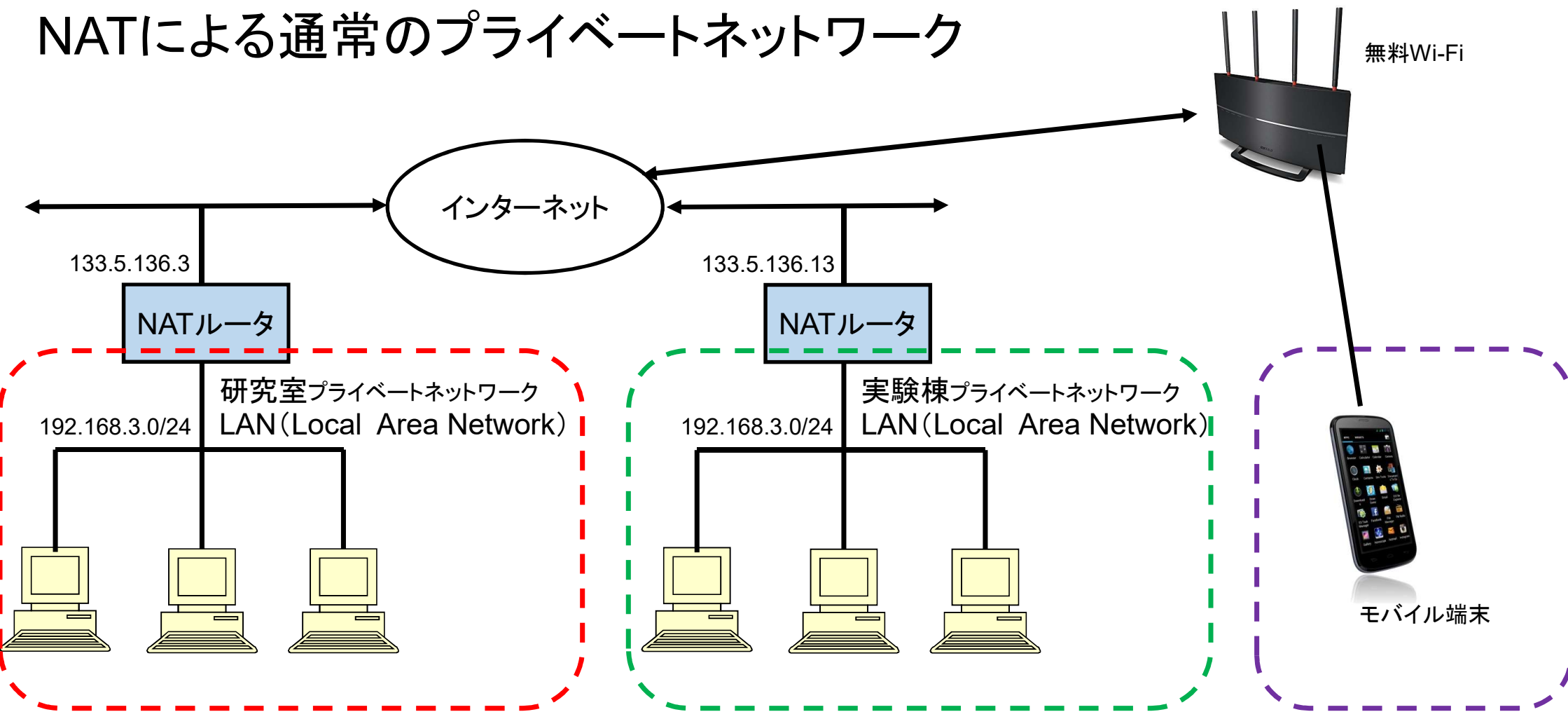
サービスを行うホストはWANへ接続

ポートフォワーディング (NAPT: Network Address Ports translator)

- LANの内側でプライベートIPを使い、インターネットへ接続するときにグローバルIPアドレスへ変換するNATの仕組みに加えて**ポート番号も付け替える**
- IPv4のアドレス枯渇問題を解決するための技術
- ルータの機能

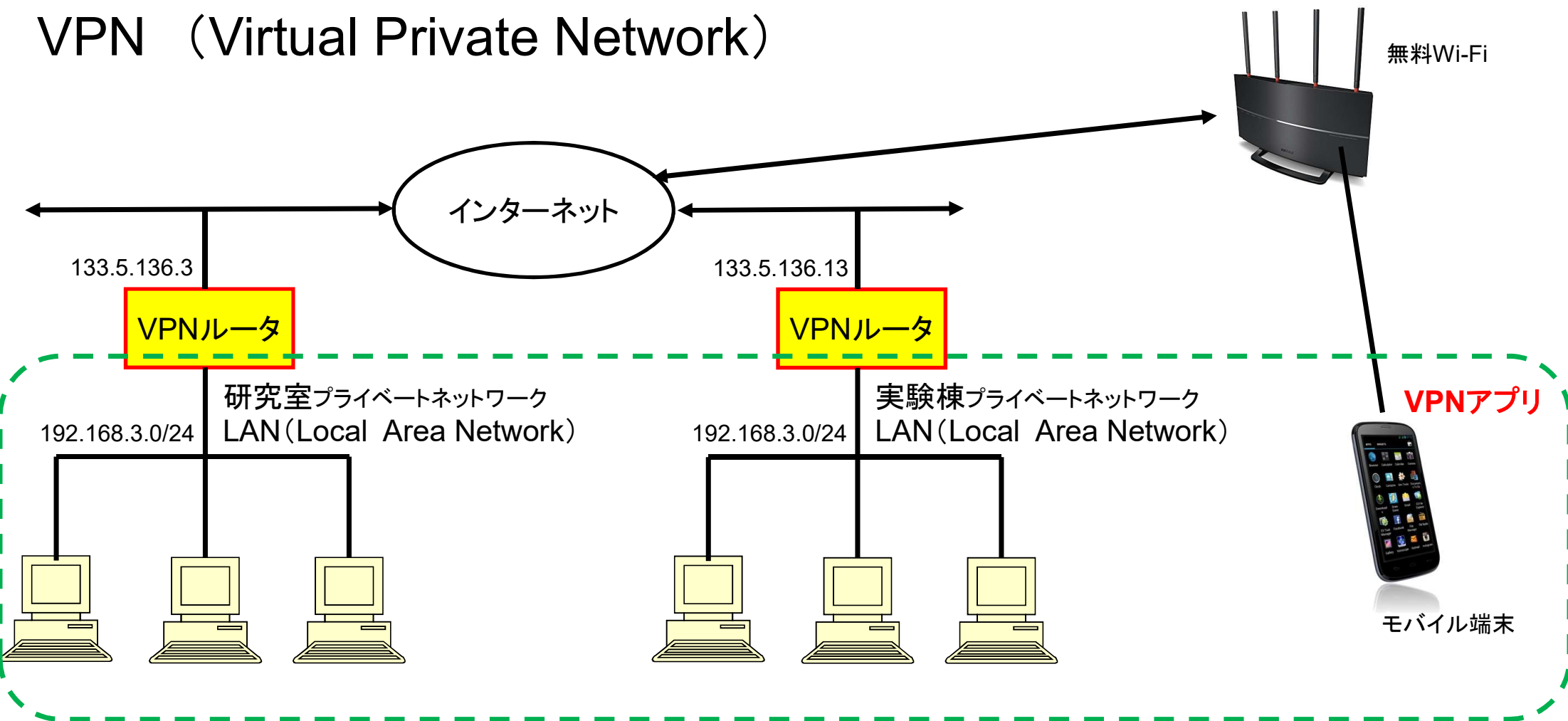


NATによる通常のプライベートネットワーク



通常は研究室内のLAN内のPCと実験棟内のLANのPC同士で直接通信したり
外部のモバイル機器からLAN内のPCと直接通信はできない

VPN (Virtual Private Network)



**VPNルーター同士のIPアドレスなどを互いに設定することにより、
同一のプライベートアドレスで接続され、互いのPC同士が自由に通信できる**

WindowsコマンドプロンプトからDNSやIPアドレス、TCP接続情報を取得する

- ホスト名からIPアドレスを調べる(正引き) IPアドレスからホスト名を調べる(逆引き)

> nslookup (ホスト名またはIPアドレス)

- 対象のWindowsPCのTCP-IPに関する情報を得る: netsh コマンド

> netsh interface ip show

使用できるコマンドは次のとおりです:

このコンテキストのコマンド:

show addresses - IP アドレスの構成を表示します。

show compartments - コンパートメント パラメーターを表示します。

show config - IP アドレスおよび追加情報を表示します。

show destinationcache - 宛先キャッシュ エントリを表示します。

show dnsservers - DNS サーバー アドレスを表示します。

show dynamicportrange - 動的ポート範囲の構成パラメーターを表示します。

show global - グローバル構成パラメーターを表示します。

show icmpstats - ICMP 統計情報を表示します。

show interfaces - インターフェイス パラメーターを表示します。

show ipaddresses - 現在の IP アドレスを表示します。

show ipnettoimedia - IP net-to-media のマッピングを表示します。

show ipstats - IP 統計情報を表示します。

show joins - 参加したマルチキャスト グループを表示します。

show neighbors - 近隣キャッシュ エントリを表示します。

show offload - offload 情報を表示します。

show route - ルート テーブル エントリを表示します。

show subinterfaces - サブインターフェイス パラメーターを表示します。

show tcpconnections - TCP 接続を表示します。

show tcpstats - TCP 統計情報を表示します。

show udpconnections - UDP 接続を表示します。

show udpstats - UDP 統計情報を表示します。

show winsservers - WINS サーバー アドレスを表示します。

> netsh interface ip show config を実行する

> netsh interface ip show dnsservers を実行する

> netsh interface ip show tcpconnections を実行する

```
C:\Users\kimura>netsh interface ip show tcpconnection
```

```
MIB-II TCP 接続エントリ
```

```
ローカル アドレス ローカル ポート リモート アドレス リモート ポート 状態
```

ローカル アドレス	ローカル ポート	リモート アドレス	リモート ポート	状態
0.0.0.0	135	0.0.0.0	0	リッスン
192.168.3.2	139	0.0.0.0	0	リッスン
0.0.0.0	554	0.0.0.0	0	リッスン
0.0.0.0	623	0.0.0.0	0	リッスン
127.0.0.1	5939	0.0.0.0	0	リッスン
127.0.0.1	6044	0.0.0.0	0	リッスン
0.0.0.0	9980	0.0.0.0	0	リッスン
0.0.0.0	16992	0.0.0.0	0	リッスン
127.0.0.1	18402	0.0.0.0	0	リッスン
127.0.0.1	18402	127.0.0.1	49155	確立済み
127.0.0.1	49161	127.0.0.1	18402	確立済み
0.0.0.0	49163	0.0.0.0	0	リッスン
127.0.0.1	49164	127.0.0.1	18402	確立済み
127.0.0.1	49175	127.0.0.1	18402	確立済み
127.0.0.1	49182	127.0.0.1	18402	確立済み
127.0.0.1	49254	0.0.0.0	0	リッスン
192.168.3.2	49786	23.41.22.130	443	終了を待機中
192.168.3.2	50729	133.5.8.126	443	終了を待機中
192.168.3.2	50732	133.5.8.126	443	終了を待機中
192.168.3.2	50901	133.5.8.126	443	終了を待機中
192.168.3.2	50923	133.5.8.126	443	終了を待機中
192.168.3.2	50924	133.5.8.126	443	終了を待機中
192.168.3.2	50933	133.5.8.126	443	終了を待機中
192.168.3.2	50988	133.5.8.126	5274	終了を待機中
192.168.3.2	51010	133.5.8.126	5274	終了を待機中
192.168.3.2	51012	133.5.8.126	5274	終了を待機中
192.168.3.2	51014	133.5.8.126	5274	終了を待機中
192.168.3.2	51017	133.5.8.126	5274	終了を待機中
192.168.3.2	51029	133.5.8.126	5274	終了を待機中
192.168.3.2	51043	133.5.8.126	5274	終了を待機中
192.168.3.2	51060	133.5.8.126	5274	終了を待機中
192.168.3.2	51085	133.5.8.126	5274	終了を待機中
192.168.3.2	51086	133.5.8.126	5274	終了を待機中
192.168.3.2	51093	133.5.8.126	5274	終了を待機中
192.168.3.2	51122	133.5.8.126	5274	終了を待機中
192.168.3.2	51128	130.211.17.117	443	確立済み
192.168.3.2	51129	130.211.17.117	443	確立済み
192.168.3.2	51130	130.211.17.117	443	確立済み
0.0.0.0	445	0.0.0.0	0	リッスン

Netshコマンドの実行結果

0.0.0.0は「IPアドレスを保有していない」または「システムにおけるすべてのインターフェースのすべてのIPアドレス」を意味する

127.0.0.1は自分自身(localhost)のIPアドレスを意味する(ループバック用IPv4アドレスと呼ばれる)

PCがどんなホストと何番ポートで通信しているの分かる

まとめ

(1) DNS (Domain Name System) ホスト名 \longleftrightarrow IPアドレスを変換する仕組み

ドメイン名とは？

ネームサーバ(DNSサーバ)

リゾルバとは？

(2) DHCP (Dynamic Host Configuration System) ネットワーク自動接続のための仕組み

DHCPサーバ

(3) NAT, ポートフォワーディング(NAPT), VPN

レポート課題：

(1) 以下のIPアドレスのホスト名を調べよ

133.5.12.36

131.112.125.45

(2) 以下のホストのIPアドレスを調べよ。また調べたIPアドレスから逆引きして別のドメイン名の有無を調べよ。

www.thingiverse.com

www.google.com

下記の課題提出用フォルダへ、課題の番号と提出者が分かるようにファイル名を以下のようにしてアップロードせよ
第2回2TE19xxxZ名前.pdf

<https://share.iii.kyushu-u.ac.jp/public/hROwAAqIPI5ATI4BUXJtIJeJbMLJzVszfitNI89GHcMK>

上記フォルダへのリンクは下記ホームページから

<http://sysplan.nams.kyushu-u.ac.jp/gen/edu/NavalInformationProcessing/2019/index.html>

