2019年度　IT基盤基礎技術勉強会　資料

SCSK

ネットワーク基礎
「Web通信がつながるまでをネットワーク技術（レイヤ2～7）を通じて基礎を理解する」

2019年 12月 3日

PFS事業部門　事業推進G
ネットワーク技術部
加藤　俊二

SCSK株式会社

アジェンダ

コース名	ネットワーク基礎	概要	Web通信がつながるまでをネットワーク技術（レイヤ2～7）を通じて基礎を理解する
学習目標	• IPネットワークの基礎理論、および技術を体系的に習得することができる。		
学習内容	1.OSI参照モデル 2.TCP/IP • TCP/IPの階層 • 各層でのアドレス • IP通信のフロー • ポート番号 • アドレス変換 3.HTTP • リクエストとレスポンス • ステータスコード • まとめ		4.ネットワーク機器 • ハブ • スイッチ • ルータ • ファイヤーウォール • ロードバランサー

タイムテーブル

開始時刻	終了時刻	所要時間	タイトル	備考
13:00	13:10	10分	OSI参照モデルについて	
13:10	13:50	40分	TCP/IPについて	
13:50	14:00	10分	休憩	
14:00	14:10	10分	HTTPについて	
14:10	14:40	30分	ネットワーク機器について	
14:40	14:50	10分	質疑応答	

1.OSI参照モデル

OSI参照モデル

通信プロトコル

ネットワーク上での通信に関する規約、約束事。

プロトコルを機能別に分類し、体系化したものをネットワークアーキテクチャ、プロトコルスタック、プロトコルスイートなどと呼びます。

OSI参照モデル

ISO(国際標準化機構)によって策定された
マルチベンダアーキテクチャ。

TCP/IPの普及に伴い、現在ではあまり
使用されていません。

データ送信は上位層から下位層へ、
受信時は下位層から上位層へ、
それぞれの層で処理が行われます。

第7層	アプリケーション層	Application Layer
第6層	プレゼンテーション層	Presentation Layer
第5層	セッション層	Session Layer
第4層	トランスポート層	Transport Layer
第3層	ネットワーク層	Network Layer
第2層	データリンク層	Data-Link Layer
第1層	物理層	Physical Layer

OSI参照モデル

第7層　アプリケーション層

ユーザの業務に応じた機能の提供

第6層　プレゼンテーション層

データ表現形式をプラットフォームに依存しない形式に変換

第5層　セッション層

セッション(アプリケーション間の通信、対話)を管理

第4層　トランスポート層

通信の確実性を保証

第3層　ネットワーク層

複数のネットワーク間の通信をする機能を提供

第2層　データリンク層

隣接した機器とのデータ転送方法を定義

第1層　物理層

電気信号を伝送するための定義

第7層	アプリケーション層
第6層	プレゼンテーション層
第5層	セッション層
第4層	トランスポート層
第3層	ネットワーク層
第2層	データリンク層
第1層	物理層

2.TCP/IP

TCP/IP

インターネットプロトコルスイート

インターネットで利用されるTransmission Control Protocol (TCP) とInternet Protocol (IP)にちなんで、TCP/IPプロトコルスイートとも呼ばれます。

図のように4階層で階層化され、OSI参照モデルとは一致しない部分があります。

トランスポート層ではTCP・UDPをネットワーク層ではIPを利用します。

したがってTCP・UDPとIPに対応していればどのようなアプリケーションでも利用できるという柔軟性があります。

第7層	アプリケーション層
第6層	プレゼンテーション層
第5層	セッション層
第4層	トランスポート層
第3層	ネットワーク層
第2層	データリンク層
第1層	物理層

OSI参照モデル

アプリケーション層	HTTP FTP DNS など
トランスポート層	TCP・UDP
インターネット層	IP
ネットワークインターフェイス層	

インターネットプロトコルスイート

TCP/IPモデルの各層とプロトコル一例

アプリケーション層

アプリケーション固有の通信規約を定義

DHCP　DNS　HTTP　など

トランスポート層

アプリケーションプロセス間の通信を提供するとともに、伝送品質を確保

信頼性のある双方向通信を実現するTCPやデータを一方的に転送するUDPなど

TCP　UDP

インターネット層

ホスト間の通信を提供

通信提供にはIPアドレスとMACアドレスが必要

IP(IPv4　IPv6)　ICMP　ARP

ネットワークインターフェイス層

パケットからフレームを生成し、信号に変換して伝送

イーサネットなどを利用

インターネット層　4つのアドレス

インターネット層はOSI参照モデルのネットワーク層に該当するプロトコルであり、End-to-Endの通信のための機能を持っています。

この層の中心となるプロトコルはIP(Internet Protocol)。

IPは異なるネットワーク間でデータを交換するための機能を持ちます。

またIPを補助するためのプロトコルとして、ARPやICMPなどが定義されています。

実際にデータ転送をする際には、**宛先IPアドレス**、**宛先MACアドレス**、**送信元IPアドレス**、**送信元MACアドレス**の4つのアドレスが必要となり、

どの機器かを識別するため、4つのアドレスはそれぞれユニークである必要があります。

MACアドレス

MACアドレス(自身のMACアドレス)はNIC(Network Interface Card)に製造時に付与されている。

NICはPCなどの端末に内蔵されています。

MACアドレスは48ビットの数値で一般的には8ビットずつ、6つに区切って16進数表記されており、物理アドレスともよばれます。

前半24ビットはベンダー(メーカー)毎に決まっており、ベンダーコードと呼びます。

後半24ビットはベンダ割当コードとなり、各ベンダーがそれぞれ任意で付与します。

MACアドレスを見ることで、**「どのベンダーが作った何番のNIC(PC)」**かということがわかります。

例：AA-BB-CC-DD-EE-FF

「どのPCか」が分かるので、LANのような狭いネットワークではMACアドレスのみでデータ転送が可能です。

しかし、MACアドレスでは対象のPCが「誰」かは分かるが、「どこ(のネットワーク)」がわからないため、インターネットなどの別のLANに対するデータ転送では、IPアドレス情報が必要となります。

IPv4アドレス(IPアドレス)

ネットワークインターフェイスに割り当てられる32ビットの数値です。

基本的にマシン同士は2進数でやり取りしますが、通常は人間に分かりやすいように、8ビットずつドット(.)で区切り、区切った8ビットを10進数で表記します。

2進数表記	**11000000**	**10101000**	**00001010**	**00000001**
10進数表記	**192**	**168**	**10**	**1**
	ネットワーク部			**ホスト部**

IPアドレスは以下の2つの部分から構成されています。

■ネットワーク部：ホストが接続されたネットワークを識別

■ホスト部：ネットワーク内のホストを識別

IPアドレスによって、ネットワークインターフェイスが、

「どのネットワークに所属する、何番のホストなのか」を識別することができます。

プライベートIPアドレス

インターネットと直接接続しない内部ネットワークで利用できるIPアドレスです。
内部ネットワークであれば基本的に管理者の任意でアドレスを設定可能ですが、
以下表のように内部ネットワークで利用できるIPアドレスにも規定があります。
よく見る192.168.X.XというIPアドレスはこの規定によります。

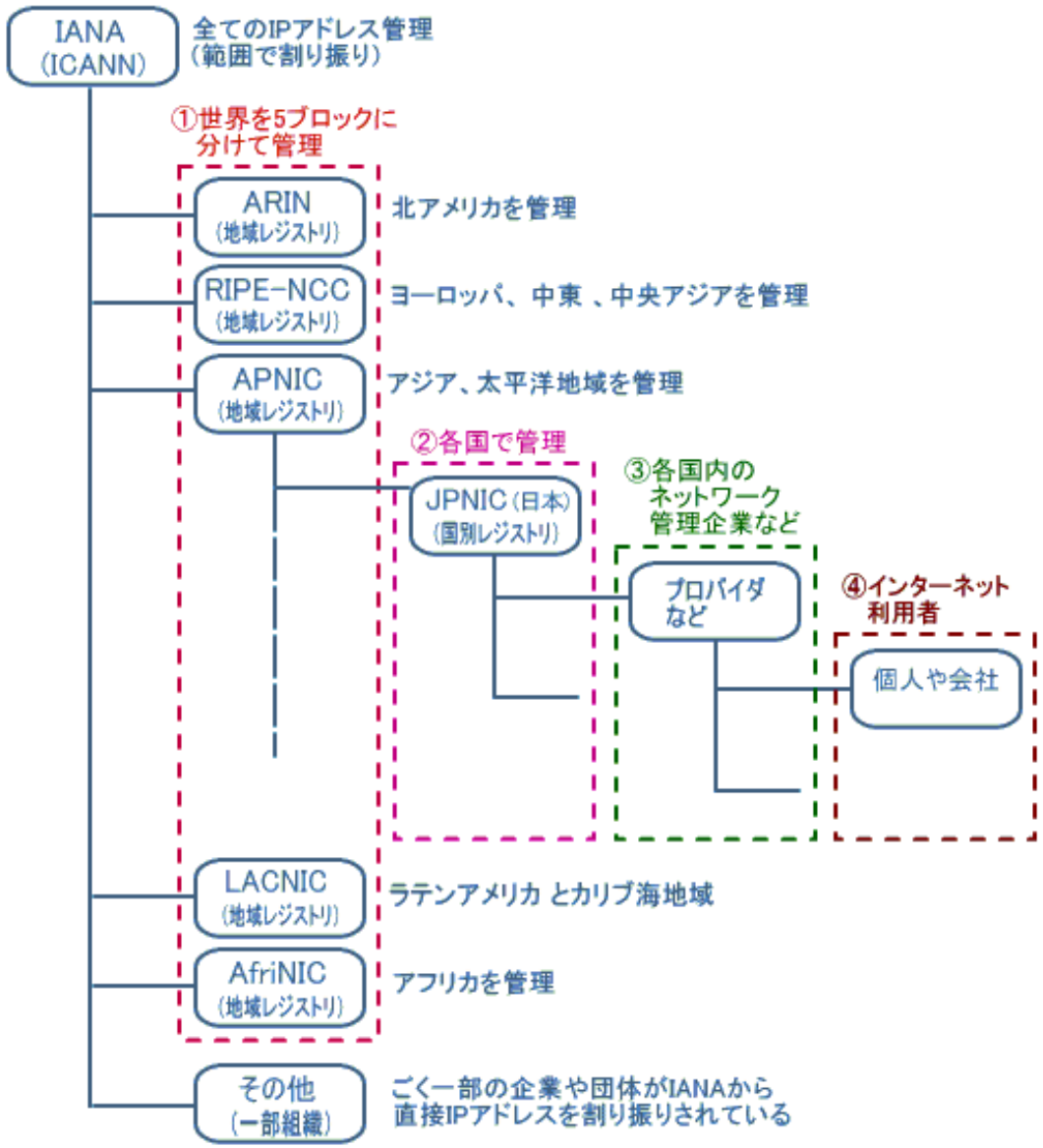
第1オクテット	第2オクテット	第3オクテット	第4オクテット
10	ホスト番号		
172	16～31	ホスト番号	
192	168	0～255	ホスト番号

グローバルIPアドレス

インターネットに接続するために必須となるIPアドレスとなります。
グローバルアドレスはIANAという組織で管理され、各地域で
利用するアドレスを割り当てます。
IANAのIPアドレスの払い出し状況は下記ページで確認できます。

https://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xhtml

TCP/IP



ARP

宛先MACアドレスを知る方法としてARPというプロトコルがあります。

ARPは宛先IPのみ知っている状態の時、

「IP：XXX.XXX.XXX.XXXのホスト、あなたのMACアドレスを教えて」

という通信を行い、教えてもらうことで宛先のMACアドレスを知ります。

この宛先IPアドレスと宛先MACアドレスの対応表(ARPテーブル)は、各ホストが持っており、

ARPで判明した組み合わせが追加されていきます。

コマンドプロンプトで「arp –a」と入力すると、PCのARPテーブルが参照できます。

ルーティング

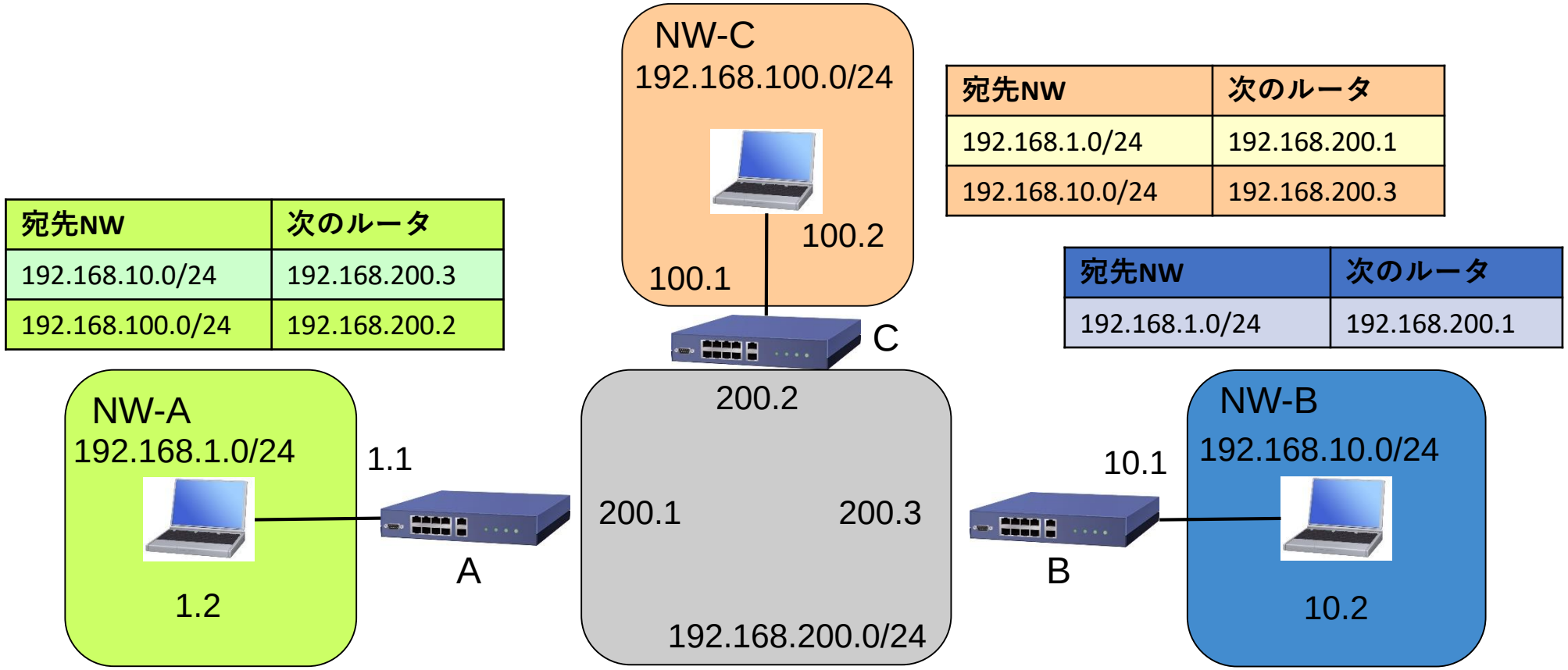
インターネットワークでは実際に通信する上で、「どの経路を通って通信をするか」、
という経路選択をする必要があります。
この経路選択、経路決定は一般的にルーターが行います。
ルートを決定するのでルーティング、ルーティングをするのでルーターということです。
自分と異なるネットワークに対しては、経路選択が必要となるため、ルーターがいないと通信はできません。
ルーターは自身が直接接続されているネットワークのIPアドレスと、
経路情報を記載したデータベース(ルーティングテーブル)を持ちます。
ルーティングテーブルには宛先のネットワークアドレス、
宛先のネットワークに到達するために通信を渡す先のアドレス、などが記載されています。
異なるネットワークとの接点、出入り口となる機器はデフォルトゲートウェイと呼ばれ、
一般的にルーターがデフォルトゲートウェイとなり、PCがインターネットなどと通信する際の出入り口となります。

TCP/IP

ルーティング例

下のネットワークでは、NW-AはNW-B、NW-Cと通信が可能です。

NW-BはNW-Cに対するルーティングテーブルがないため、通信できません。

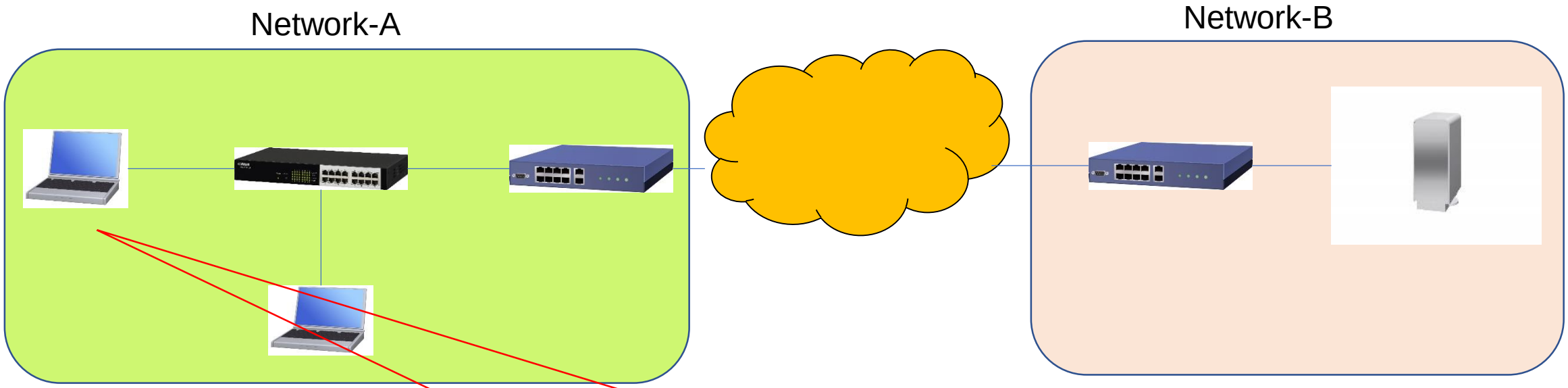


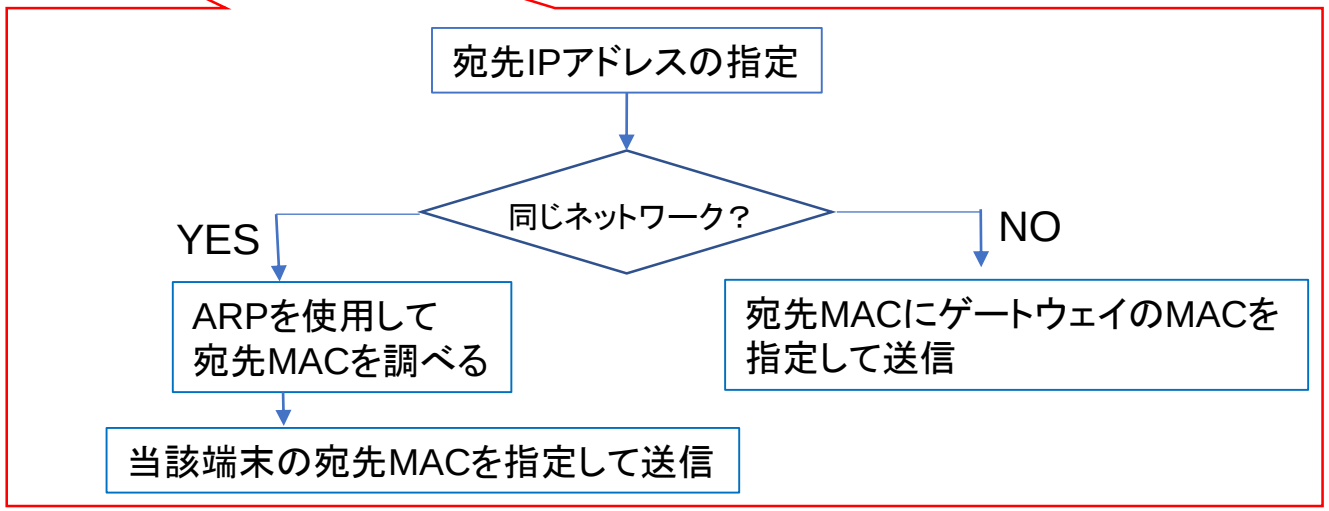
宛先NW	次のルータ
192.168.10.0/24	192.168.200.3
192.168.100.0/24	192.168.200.2

宛先NW	次のルータ
192.168.1.0/24	192.168.200.1
192.168.10.0/24	192.168.200.3

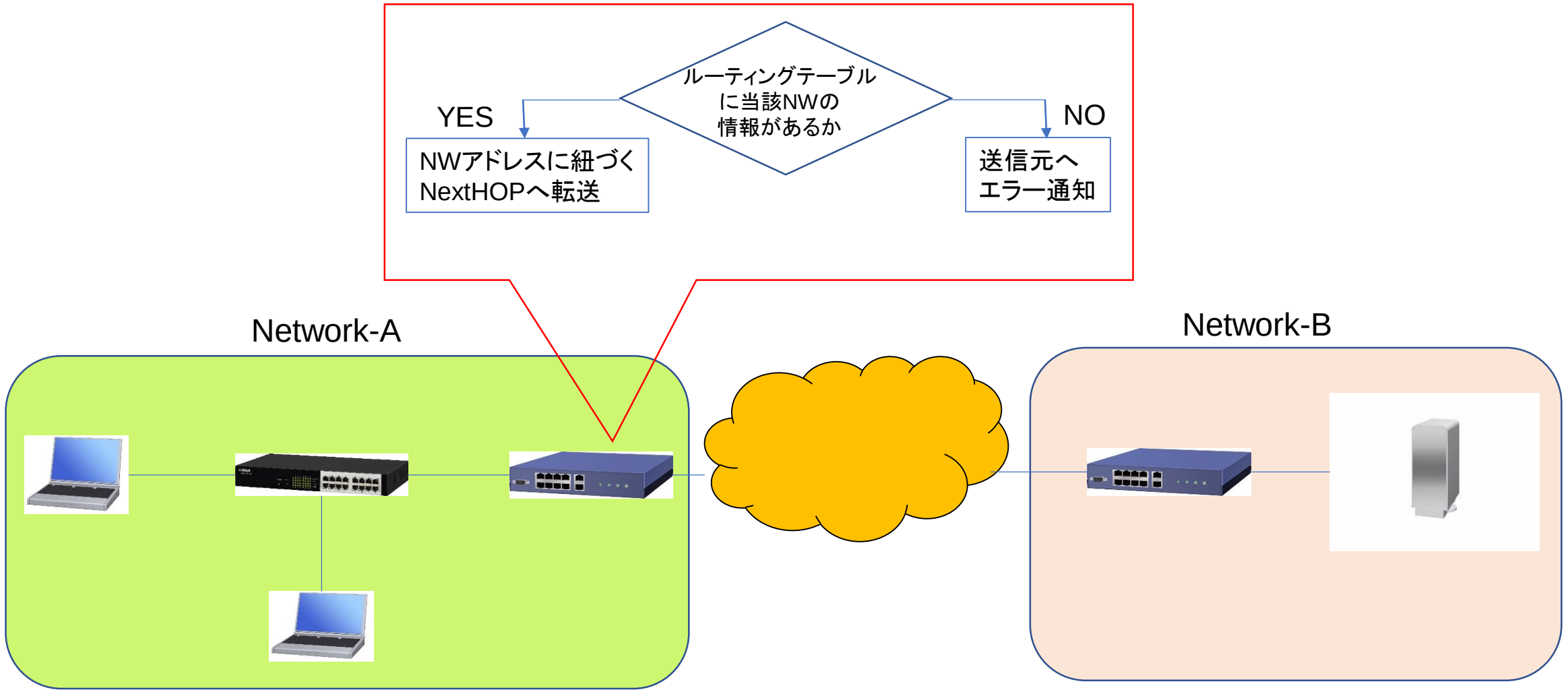
宛先NW	次のルータ
192.168.1.0/24	192.168.200.1

IP通信のフロー

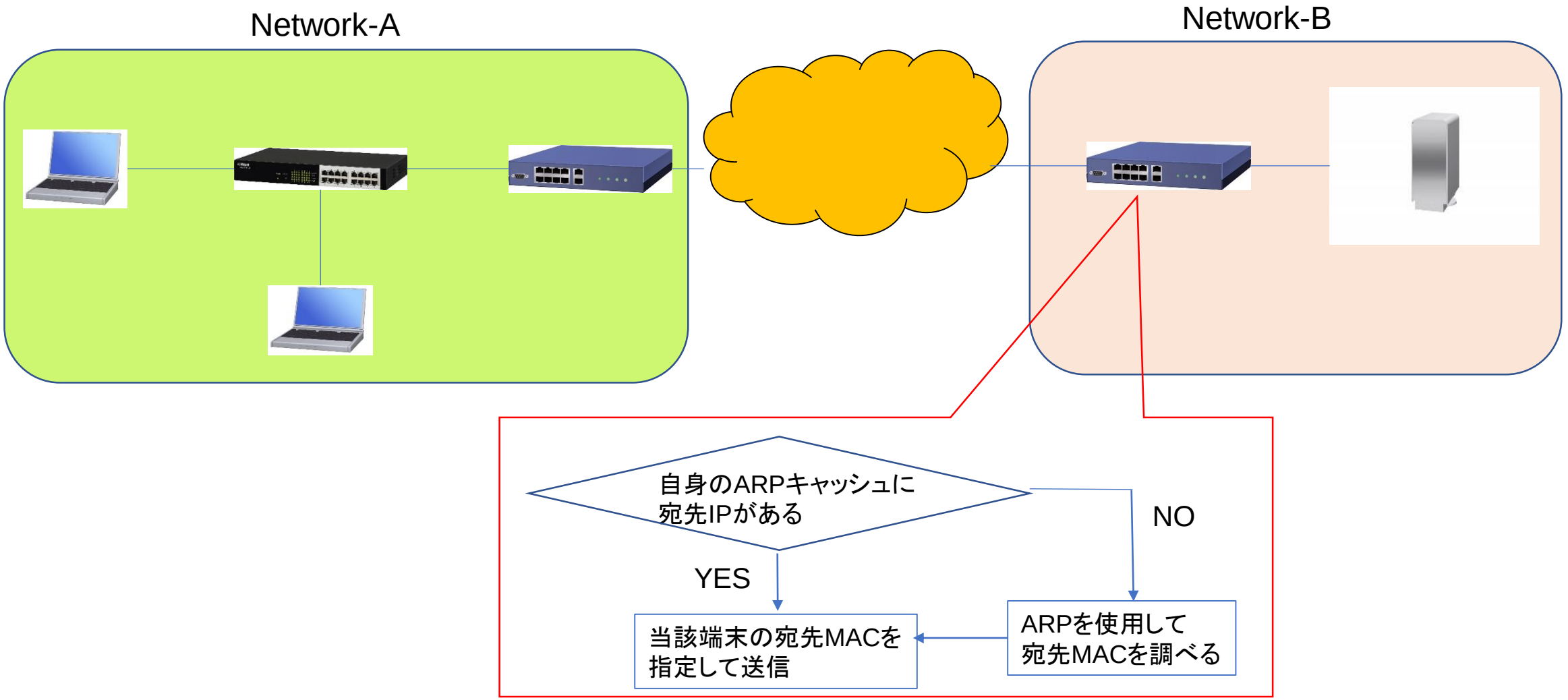




IP通信のフロー



IP通信のフロー



DNS(Domain Name System)

前述のように通信はあくまでもIPアドレス(数字)に対して行いますが、数字では覚えづらいのでドメイン名、ホスト名のように名前が使われます。

そしてIPアドレスと名前を対応づける必要があります。そのシステムがDNSです。

DNSサーバーは各組織に存在し、名前とIPアドレスの対応づけを行います。

DNSサーバーはクライアントから、「www.scsk.jpに通信したい」という要求を受け、

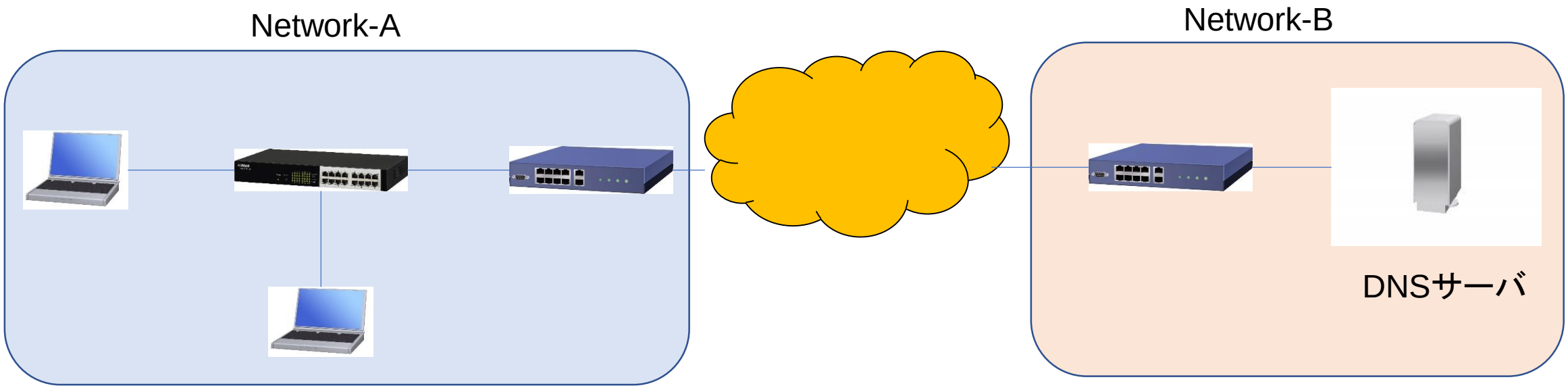
自分が持つIPアドレスと名前の対応表を探し、表にあればクライアントにIPアドレスを教えます。

自身が持つ対応表になかった場合、別の組織のDNSサーバーに問い合わせ、

その結果をクライアントに教えます。これらの動作をDNS名前解決と呼びます。

コマンドプロンプトで「nslookup FQDN」と入力すると、紐づけられたIPアドレスを調べることができます。

TCP/IP



www.scsk.jpのIPアドレスは？
(DNSクエリ)

203.179.35.68です
(DNSレスポンス)

ポート番号

送信元と宛先のアドレスで誰が誰と通信するかが決定されました。

しかし、宛先にパケットが到達しても、何のアプリケーションを利用するか分からなければ、

実際にサービスは利用することはできません。

例えばwebサーバーに対してメールソフトでアクセスしても、web閲覧はできません。

そこでポート番号というパラメーターを利用して通信を行います。

ポート番号は16ビット(65,536)あり、そのうちの1024番までがウェルノウンポートとして決められています。

代表的なウェルノウンポートは下記のものがあります。

例えば203.179.35.68のweb(80番)サーバーにアクセスする場合、 203.179.35.68 :80宛に通信を行います。

TCP:20,21	FTP
TCP:22	SSH
TCP:23	Telnet
UDP:53	DNS

UDP:67,68	DHCP
TCP:80	HTTP
TCP:110	POP3
TCP:443	HTTPS

TCP

TCPは通信品質を保証するコネクションを生成します。

TCPは通信相手との間に、制御ビットを用いたスリーウェイハンドシェイクを行い、コネクションを確立します。

制御ビットはTCPヘッダの中にあり、SYN(要求)、ACK(確認)、FIN(終了)があります。

コネクション開始側はSYNを送り(接続要求)、受け取った側はSYN+ACK(要求確認＋こちらからも要求)を返し、それを受け取った側はACK(確認)を返してコネクションが確立され、双方向の通信路が確保されます。

SYN→SYN+ACK→ACKの3回データ転送を行うので、スリーウェイハンドシェイクと呼びます。

通信終了時はFINを使って双方が切断できる状態になってからコネクションを終了します。

UDP

TCP/IPのトランスポート層において、TCPとともに中心になるプロトコル。

TCPには制御ビット(SYN、ACK、FIN)や、

大きなデータを分割して転送した際に順番通りに送るための番号(シーケンス番号)、

データ転送量を決める目安(ウィンドウサイズ)などのパラメーターがあります。

しかし、UDPのパラメーターはポート番号のみです。したがって転送するデータを小さくすることができ、TCPと比較して高速な通信が可能です。

そのため音声や映像のデータを転送することに適しています。

別の利点として、制御や通信の保証は行わずに(コネクションレス)送信しっぱなしなので、

ブロードキャスト通信に向いています。

特にDHCPは、DHCPが動作する時点ではIPが不明のためコネクションの確立ができません。

そのためUDPを利用します。

ネットワークアドレス変換(NAT)

IPアドレスはネットワーク内でユニークである必要があります。

従ってグローバルな空間(インターネット)ではプライベートアドレスを利用できません。

そこでNAT(Network Address Translation)という技術を利用し、

インターネット空間に送出される通信の送信元プライベートアドレスを、

グローバルアドレスに変換する必要があります。

NAT変換は通常インターネットゲートウェイ(ルーター等)で行われます。

NATは1:1の変換を行い、アドレス変換の情報はNATテーブルに記録されます。

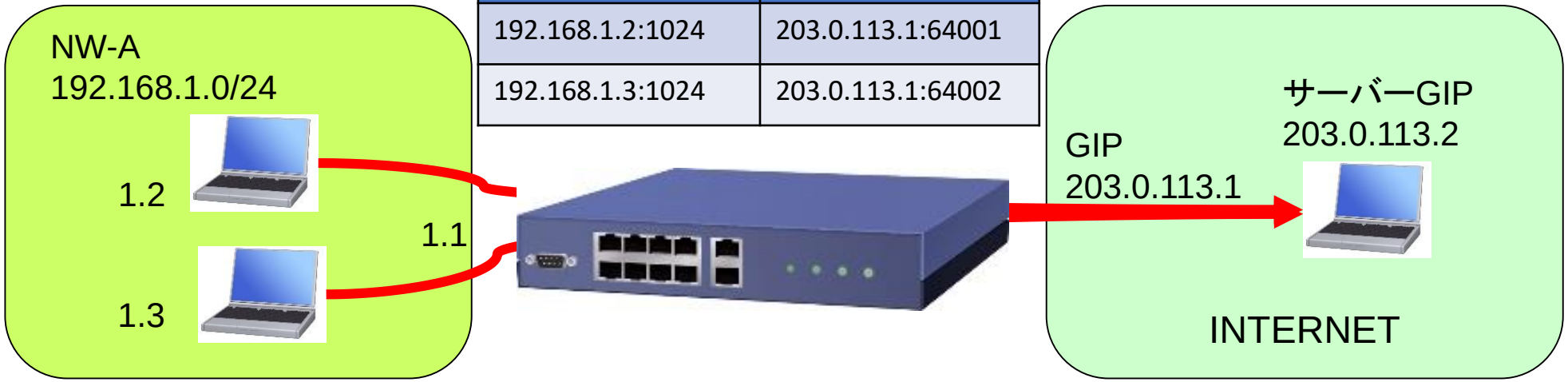
NAPT、IPマスカレード

NATでは1:1の変換が行われるため、インターネットに接続したいホストの台数分グローバルアドレスが必要になります。しかしインターネットに接続できる端末が一台のみでは、ネットワークに端末が複数台あった場合、対応できません。

そこでNAPT(IPマスカレード)を利用し、ポート番号ごと変換することで複数台でもインターネットに接続できるようにします。

NATテーブルには変換表が動的に記録されます。

NAPT前	NAPT後
192.168.1.2:1024	203.0.113.1:64001
192.168.1.3:1024	203.0.113.1:64002



3.HTTP

HTTP

HTTPはTCP上で動作するアプリケーション層のプロトコルです。

Webサーバーから情報を取り出したり、逆に、Webサーバーへ情報を送ったりするために使用されます。

HTTPでの通信には、通常、「クライアント」と「サーバー」という2種類のコンピューターが登場します。

クライアントとサーバーは、クライアントからサーバーに「リクエスト（要請）」を送り、サーバーが必要な処理を行って、サーバーからクライアントに「レスポンス（返答）」を返す、という流れで通信の処理を進めます。

HTTP通信の流れ

クライアント

Webサーバ

①ブラウザでURLを入力

②接続処理（TCP）

③リクエストを送る

④レスポンスを送る

⑤必要に応じて③- ④を繰り返す

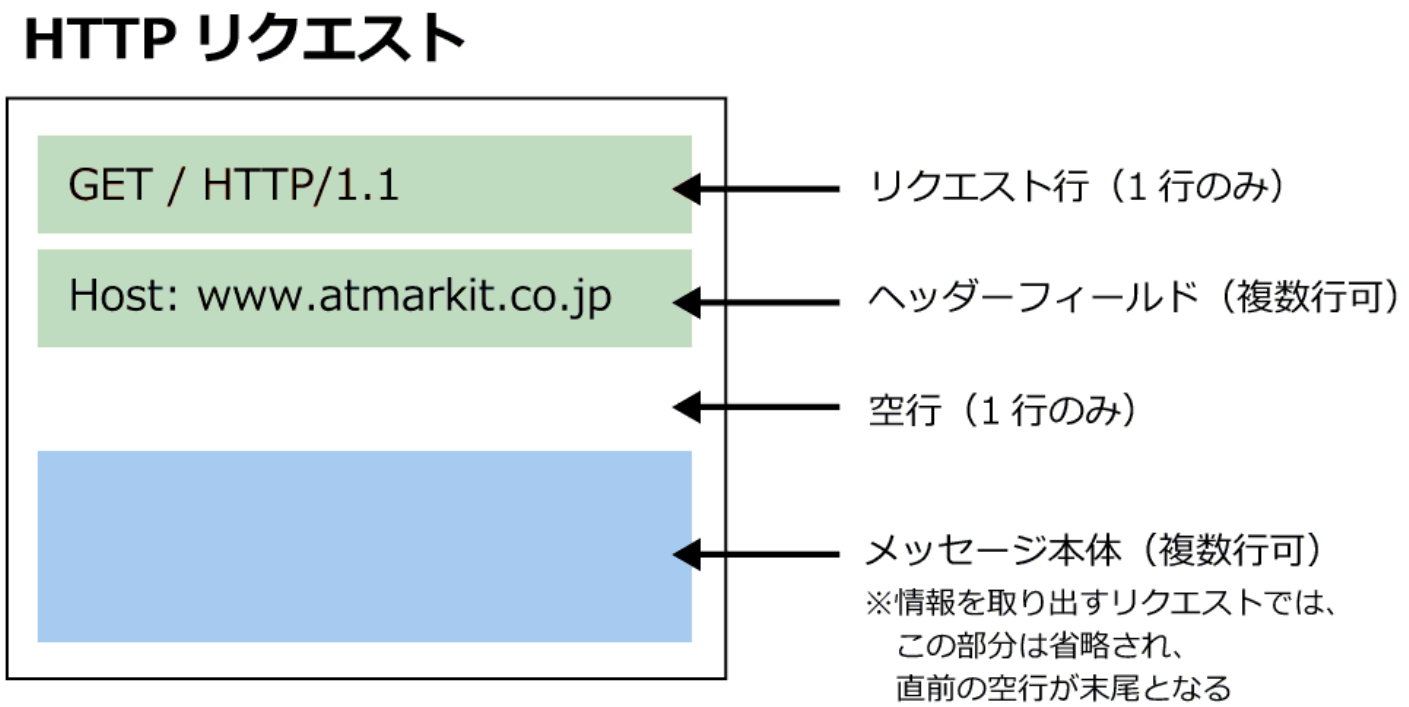
⑥切断処理（TCP）

⑦得られた情報をもとに
結果を表示する

＊HTTP 1.1の場合

リクエストとレスポンス

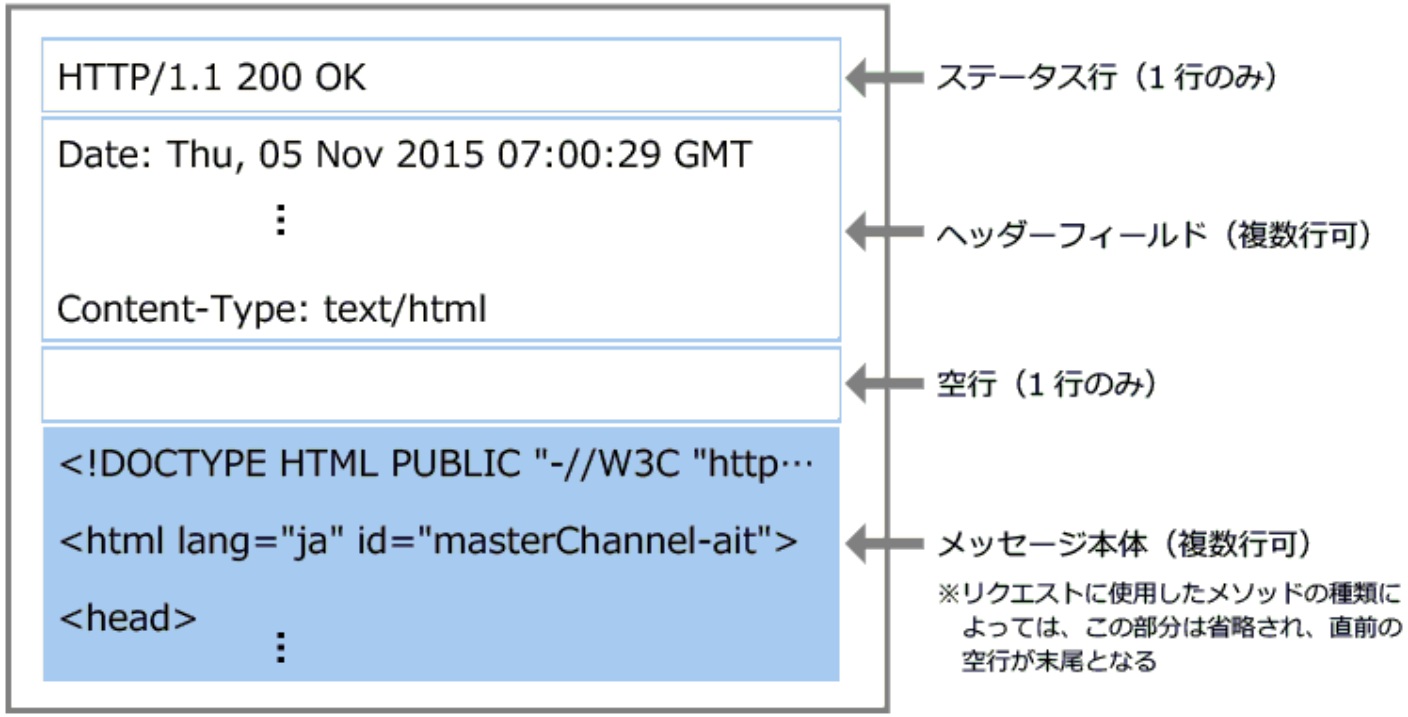
リクエストは大きく三つの部分に分類でき、それぞれ、「リクエスト行」「ヘッダーフィールド」「メッセージ本体」と呼ばれます。



リクエストとレスポンス

Webサーバーは受け取ったリクエストを処理して、その結果を「レスポンス」として返します。例えば、「HTMLファイル『sample.html』を取得せよ」という内容のリクエストであれば、指定された「sample.html」の中身がレスポンスとしてブラウザーに送り返されてきます。

HTTP レスポンス

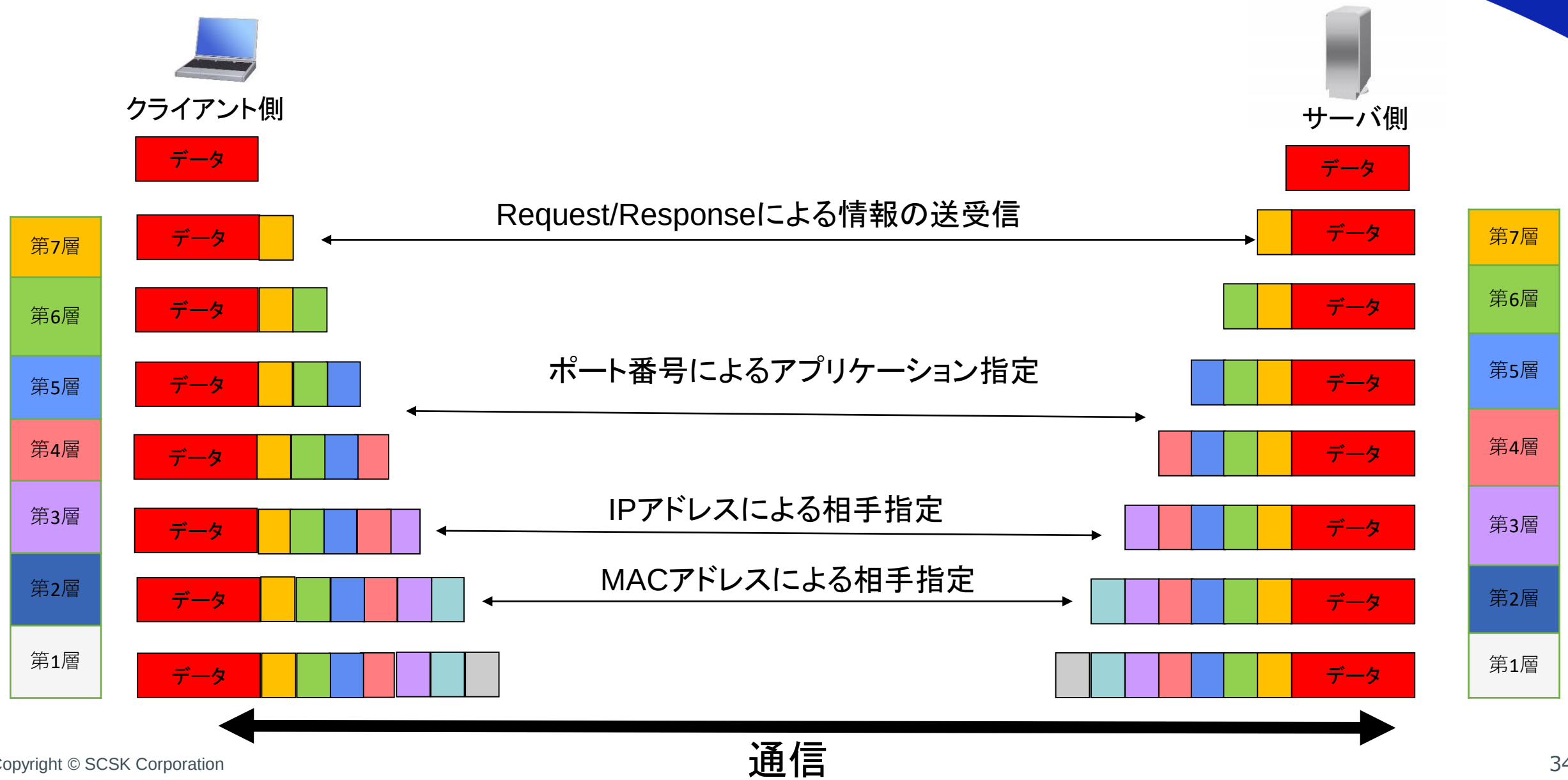


ステータスコード

レスポンスの1行目のステータス行の3桁の数字はサーバーがリクエストの処理を試みた結果を示します。多くの場合、レスポンスに含まれる情報の中で、このコードが最も重要な意味を持つことになります。ステータスコードは、先頭の1桁によって、その意味が大きく五つに分類されます

コード	分類	意味
1xx	情報系	リクエストを受信して、その処理を継続中
2xx	成功系	リクエストの処理に成功
3xx	リダイレクト系	リクエストを終えるには、さらに動作が必要
4xx	クライアントエラー系	リクエストの構文に問題がある。または実行できない
5xx	サーバーエラー系	リクエストの構文は正常だが、サーバーが実行に失敗

まとめ　–Web通信ができるまで



4.ネットワーク機器

ネットワーク機器

主なネットワーク機器

前章まではWeb通信ができるまでの大まかな流れの説明をしました。

この章ではWeb通信を行うにあたってどういったネットワーク機器を通っているかという

ことを大まかに見ていきたいと思います。

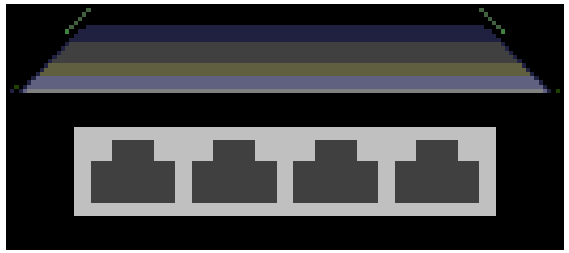
ネットワーク機器

ハブ（リピーター）

複数の端末を終端する集線装置としての役割を果たします。

信号の増幅、整理を行うのがメイン。

OSI参照モデルでは第1層（物理層）で働く機器となります。



ネットワーク機器

L2スイッチ（ブリッジ）

複数の端末を終端する集線装置としての役割を果たすのはハブと同じですが、

MACアドレステーブルにより、端末のMACアドレスと送り先ポートの対応付けを学習することができ、学習されたMACアドレス宛の Ethernetフレームであれば、対応付けされたポートのみからイーサフレームを転送します。

OSI参照モデルでは第2層（データリンク層）で働く機器となります。

ネットワーク機器

L2スイッチ（ブリッジ）

L2スイッチの中でも更に細分化され、搭載される機能で呼び分けされています。

・スマートスイッチ

スイッチングハブ機能に加え、VLANと呼ばれる機能により、ブロードキャストドメインを分割でき、また、IEEE802.1q等のタグVLAN 等の機能を利用できます。 機器本体にMACアドレスやIPアドレスを持ち、それゆえsnmpやsyslog、ntp等を使うことができ、また、telnetやssh、http(s)で管理コンソールにログインすることもできます。

・インテリジェンススイッチ

スマートスイッチの機能に加え、WEB認証/MACアドレス認証/IEEE802.1x認証のユーザ認証機能等のセキュリティや管理を強化したスイッチ。

冗長化機能を備えたものも。

ネットワーク機器

ブロードキャストドメイン

ブロードキャストフレームが届く範囲がブロードキャストドメインと呼ばれます。

ブロードキャストはネットワークの特定範囲の全機器に向けた通信のことで、一斉同報、または同報通信とも呼ばれます。(例：DHCP、ARP)

すべての機器に対して送信するため、ブロードキャストフレームの宛先MACアドレスは[FF-FF-FF-FF-FF-FF]となります。

L2スイッチにおいてもブロードキャストフレームを受け取ると全ポートに転送します。

ルーターは宛先IPアドレスで送信先を決定するため、ブロードキャストフレームの転送は行わずに、遮断します。

つまり一般的にブロードキャストドメインは同一のLAN内といえます。

L2スイッチはリピータハブと違い、通信効率が良いため、比較的ホストの数を増やすことが可能です。従い一般的に言ってL2スイッチを導入すると、ブロードキャストドメインが広がります。

ブロードキャストドメインが広がると、ブロードキャスト通信も増えるので、各ホストの負荷が上昇し、通信の遅延が発生する可能性があります。

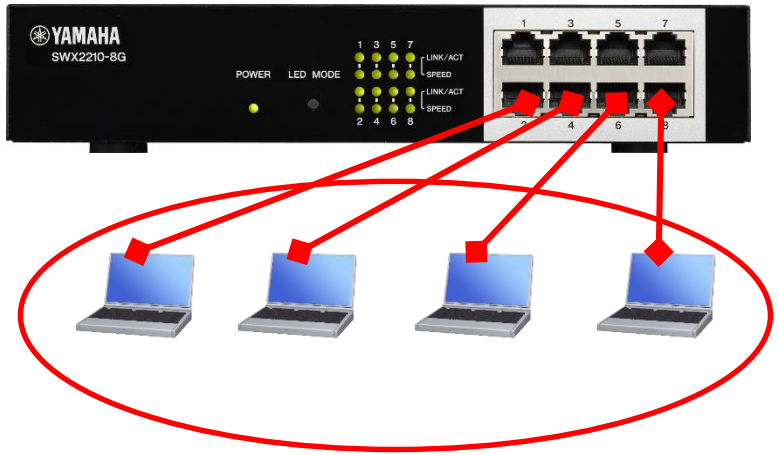
ネットワーク機器

ブロードキャストドメインとVLAN

広がってしまったブロードキャストドメインを分割する機能として、VLAN(Virtual LAN)があります。

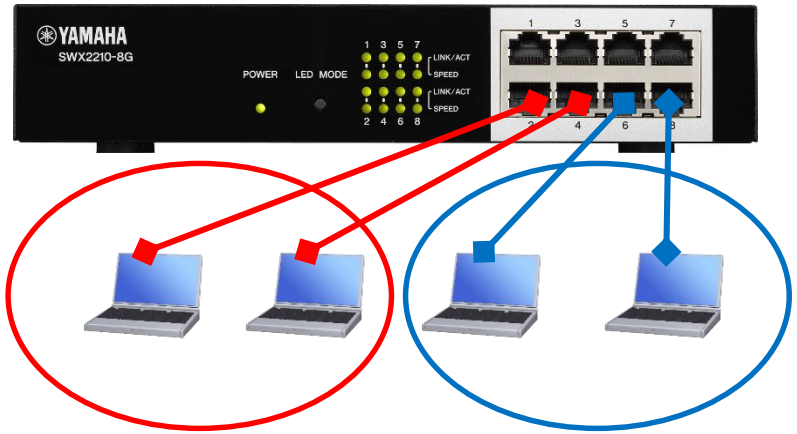
VLANはVLAN番号ごとにグループを作り、同じVLANに属したポートにブロードキャストフレームを送出することでブロードキャストドメインを分割します。

VLAN設定がない場合



192.168.1.0/24

VLAN設定がある場合



VLAN10
192.168.10.0/24

VLAN20
192.168.20.0/24

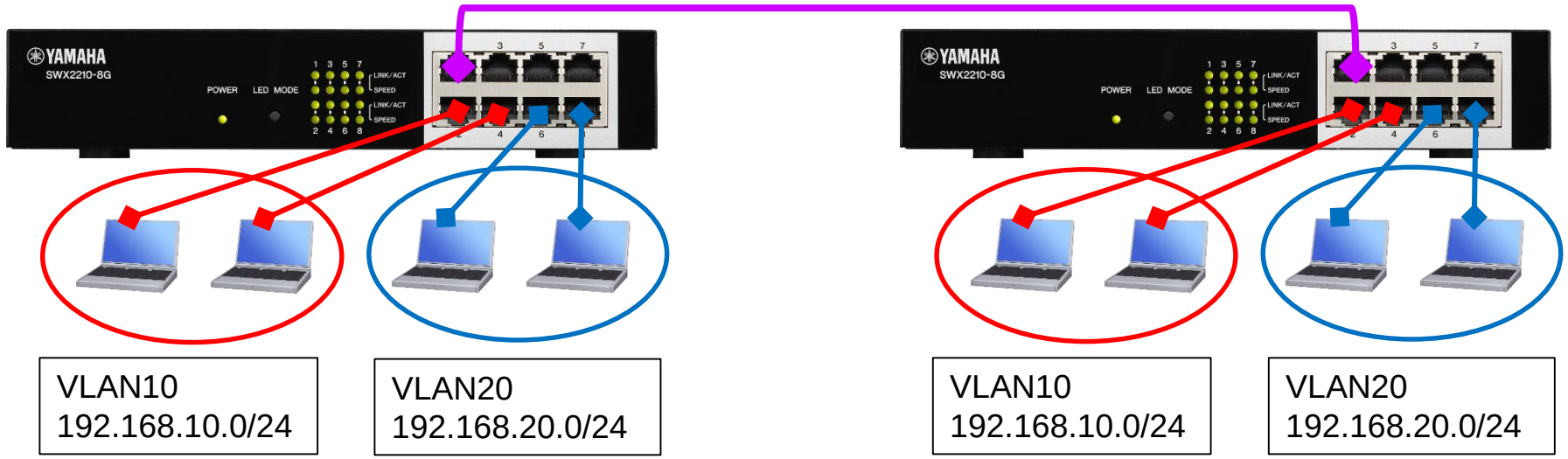
ネットワーク機器

タグVLAN

VLANの利点として、ブロードキャストドメインの分割以外では、物理配線に影響を受けにくいという点です。

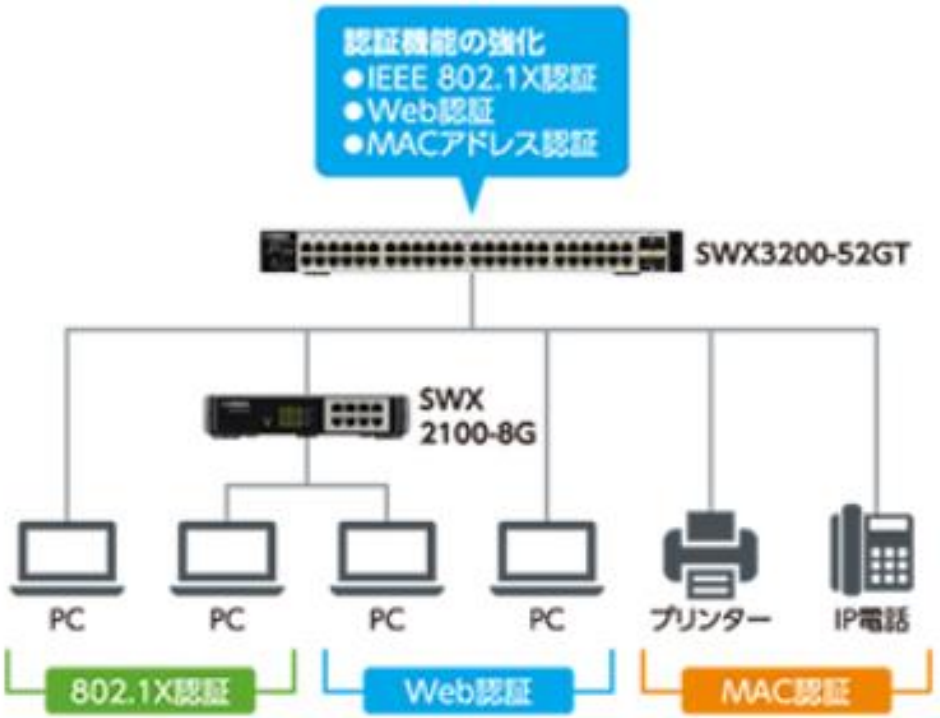
以下のようにスイッチの設置場所が離れていても、複数のVLAN番号を設定したポートでスイッチ同士を接続すれば、LANを拡張することが可能です。

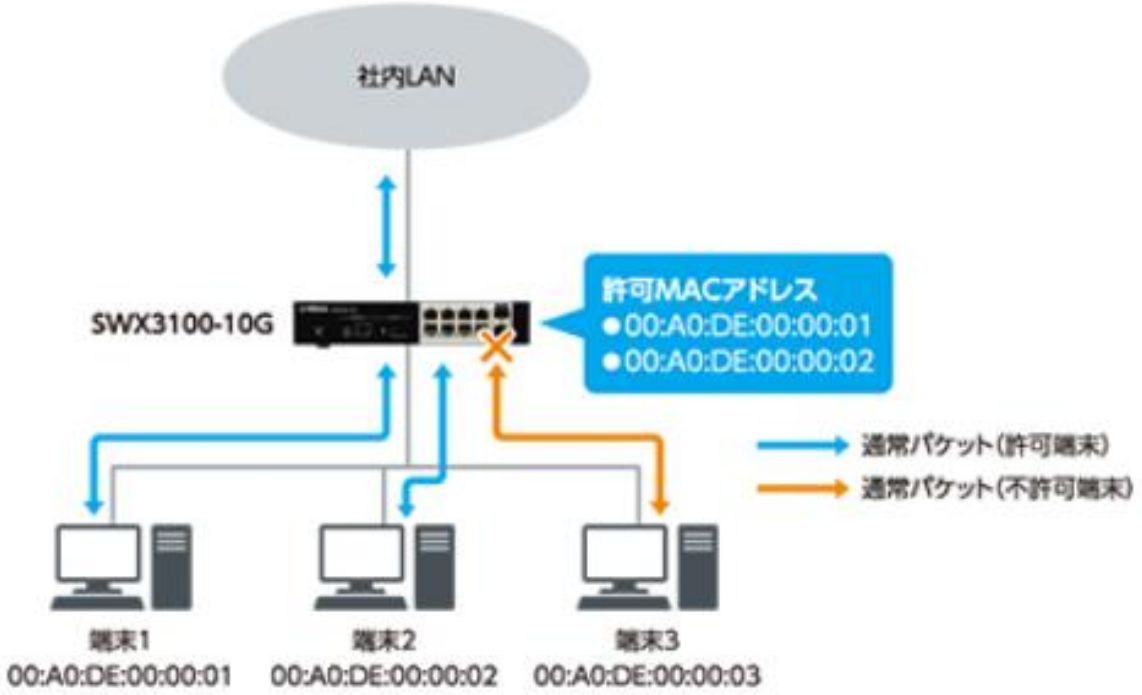
下図のポート1のように複数のVLANに属すポートをトランクポートと呼び、1つのVLANにしか属さないポートをアクセスポートと呼びます。トランクを流れるパケットにはどのVLANからのパケットかを示す情報としてタグが付加されます。



ネットワーク機器

認証機能





ネットワーク機器

無線アクセスポイント

端末間を無線接続するための電波を発信・受信する機器。

機器によって、ブリッジモード（無線-有線間のフレームの転送のみ）、

ルータモード（ルーティング機能も併せ持つ）の製品が存在する。

OSI参照モデルでは第2層（データリンク層）もしくは第3層（ネットワーク層）で

働く機器となります。

ネットワーク機器

ルーター、L3スイッチ

異なるネットワークに対し、経路情報を参照して適切な機器にパケットを転送するのがルーターの主な役割です。

OSI参照モデルでの第3層（ネットワーク層）で主に働きます。

ルーティング以外にもNATやアクセス制御（フィルタ、ACL）といった機能やWAN回線を経由して拠点間の専用経路を作成するためのVPN機能を併せ持つものがほとんどです。

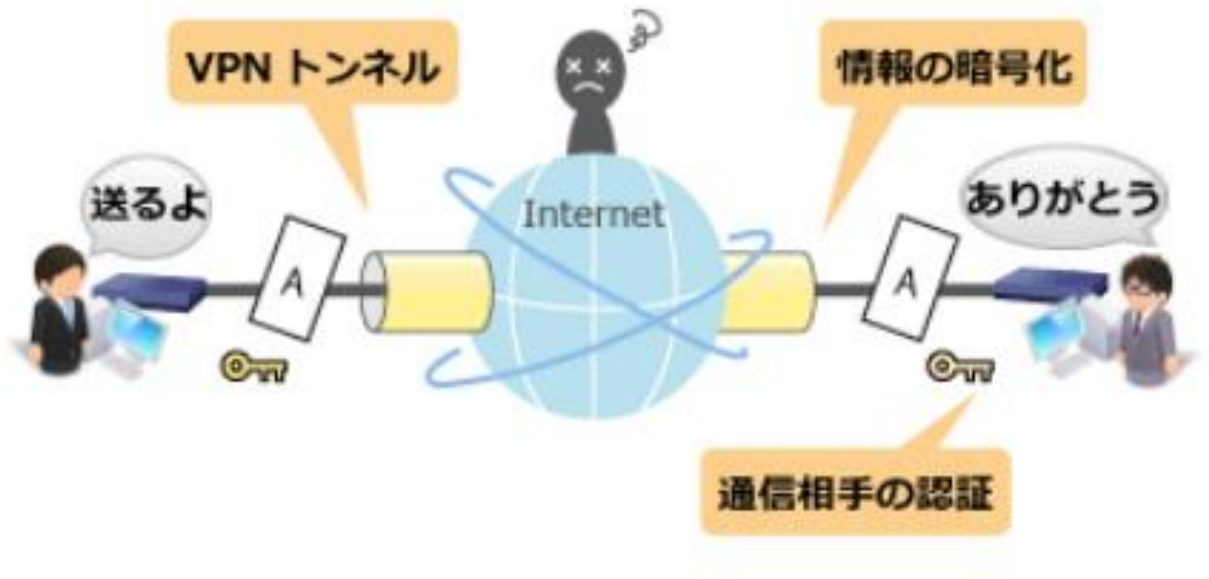
L3スイッチもルータ同様の動作を行うものとなります。

外部（WAN）との接続の境界にはルーター、内部のネットワークの集積用途としてL3スイッチを利用する、というのが主な使い分けになります。

ネットワーク機器

VPN（Virtual Private Network）

インターネットや他のネットワークの中に、機器間で専用の論理インターフェイスを
立てることで安全なプライベートネットワークをバーチャル（仮想）状態で構築します。
仮想状態のプライベートネットワークを構築する事によって、
外部から干渉を受けないようにネットワークを守る事ができます。



ネットワーク機器

ファイヤーウォール

外部のネットワークからの不正アクセスやサイバー攻撃を防ぐことが
主な役割となります。
ファイヤーウォールは自社ネットワークの内側と外側を中継する位置に設置され、
不正とみなした通信をシャットアウトすることでPC内への不正なアクセスを
防ぐことができます。
メインの機能面で考えると、OSI参照モデルでの第4層（トランスポート層）で働くものとなりますが、ルーターと同等の機能を持つものがほとんどのため、
第3層以上で働くものという考え方もできます。

ネットワーク機器

UTM、NGFW

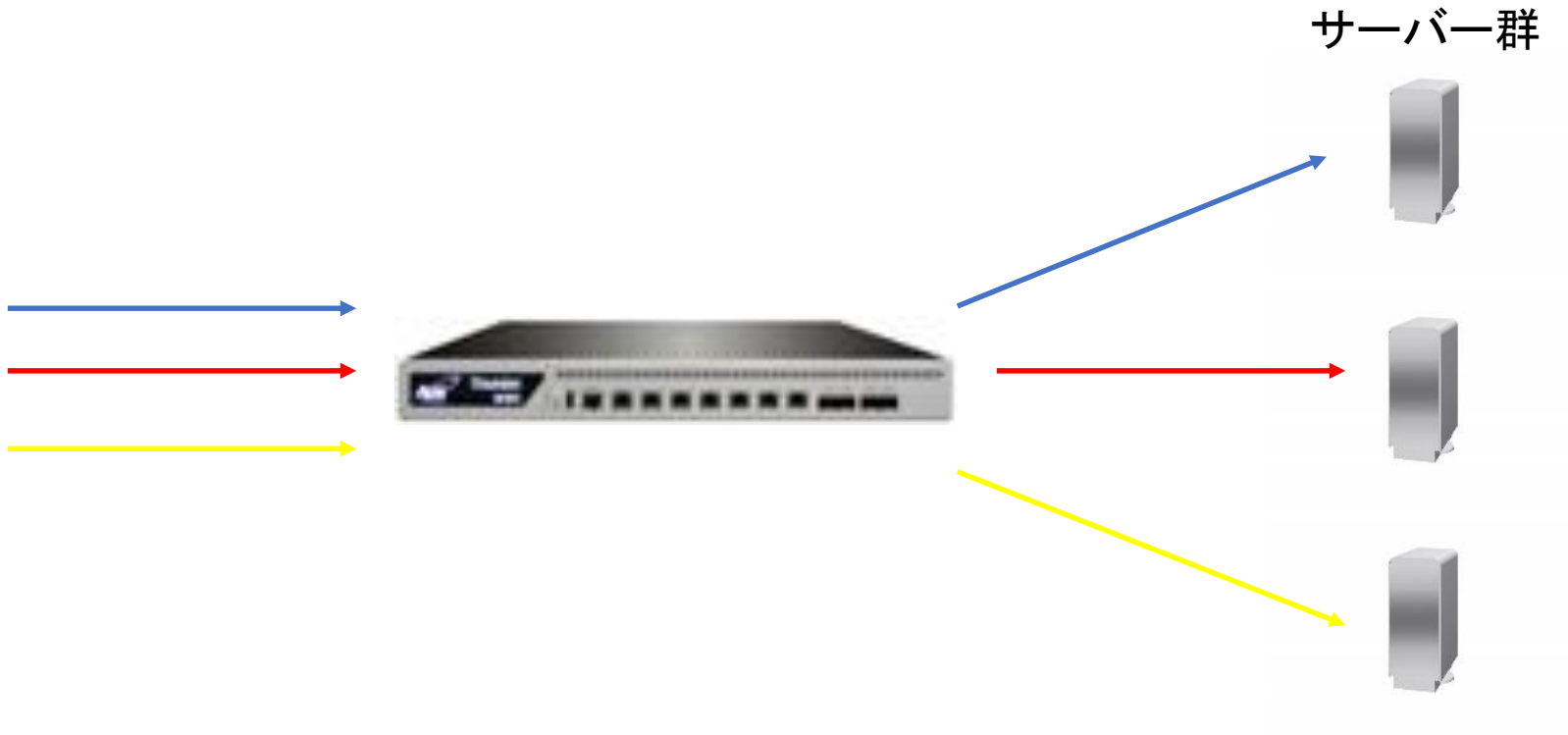
ファイヤーウォールの機能に加え、複数のセキュリティ機能を加えた
より強固なセキュリティ対策を行うことのできる装置となります。
共通して持っている主なセキュリティ機能として以下のものがあります。

・ウィルスチェック（AntiVirus）
・侵入検知、防御（IDS、IPS）
・ウェブサイトチェック（Web filtering）
・アプリケーション制御（Application control）

ネットワーク機器

ロードバランサー

サーバーにかかる負荷を、平等に振り分けるための装置のことを指します。これによって1つのサーバーにかかる負担を軽減する効果がのぞめます。



ネットワーク機器　– 構成例