# 情報ネットワーク論（第6回）
# DHCP，NAT，DNS

H15，5，21

ファイル保存位置

\\172.17.40.249\www\情報ネットワーク論

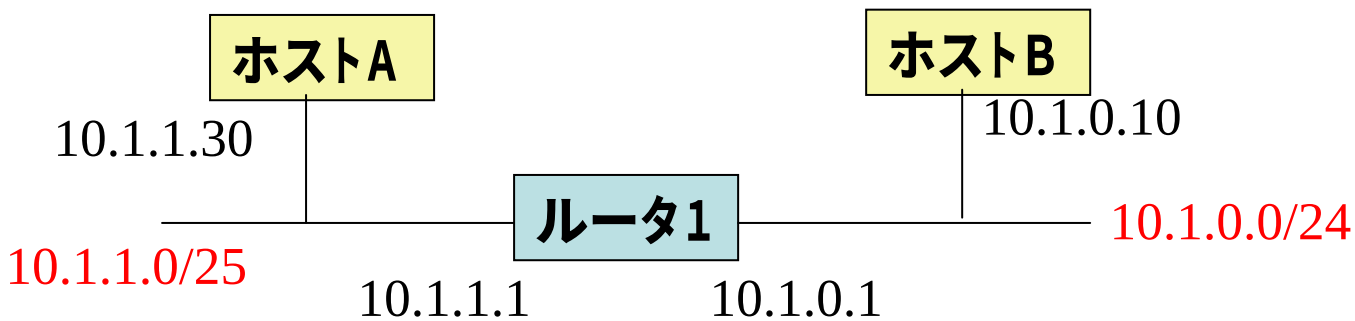


lsm-srv

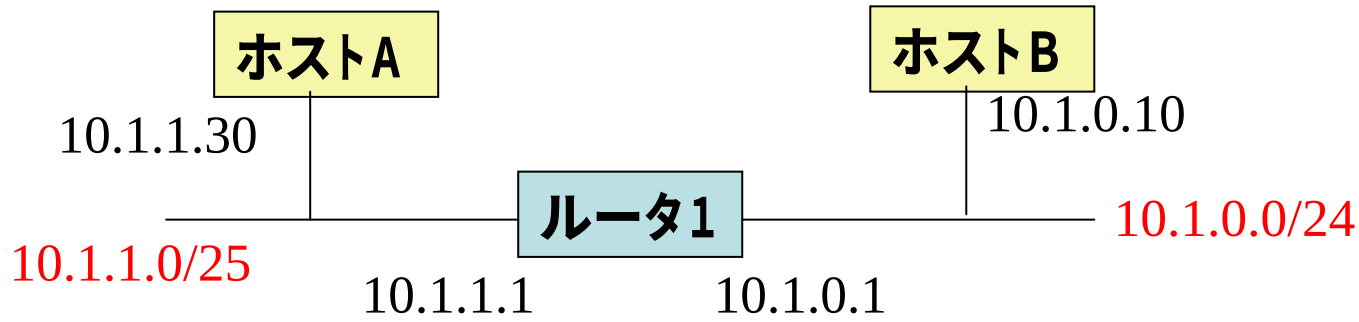
# 第5回の演習

①下図のネットワークにおいて、ホストA、ホストB、ルータ1が保持する経路制御表を示せ。

②ホストA→ホストBの転送を行うためにホストA、ルータ1、ホストBはどのような動作をするか。ＡＲＰの動作を含めて、経路制御表を用いて説明せよ。



# ホストの経路制御表




| ネットワークアドレス | 次のルータ |
|---|---|
| ﾃﾞﾌｫﾙﾄｹﾞｰﾄｳｪｲ | 最寄のﾙｰﾀ |
| 自分のﾈｯﾄﾜｰｸｱﾄﾞﾚｽ | 自分のｱﾄﾞﾚｽ |

経路制御表で解決できないパケットを送付する場所

宛先がＬＡＮに直結していることを示す

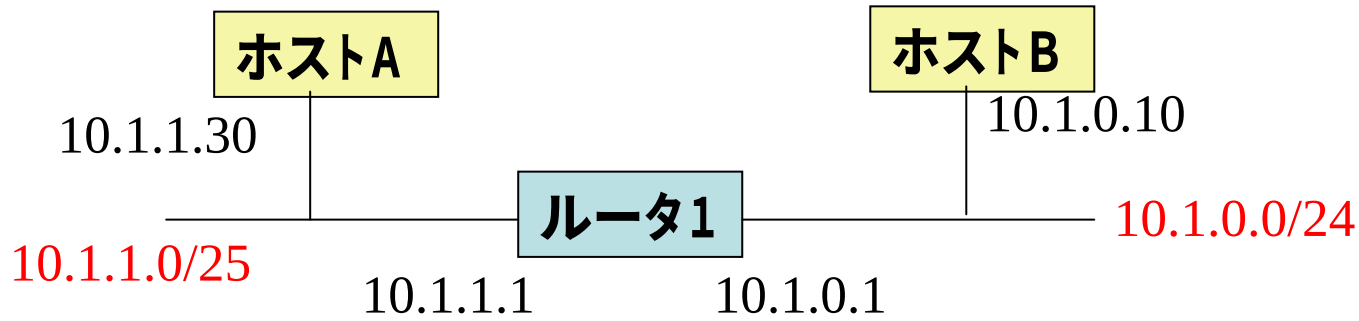
ホストA

| ネットワークアドレス | 次のルータ |
|---|---|
| 0.0.0.0/0 | 10.1.1.1 |
| 10.1.1.0/25 | 10.1.1.30 |

ホストB

| ネットワークアドレス | 次のルータ |
|---|---|
| 0.0.0.0/0 | 10.1.0.1 |
| 10.1.0.0/24 | 10.1.1.30 |

# ルータの経路制御表

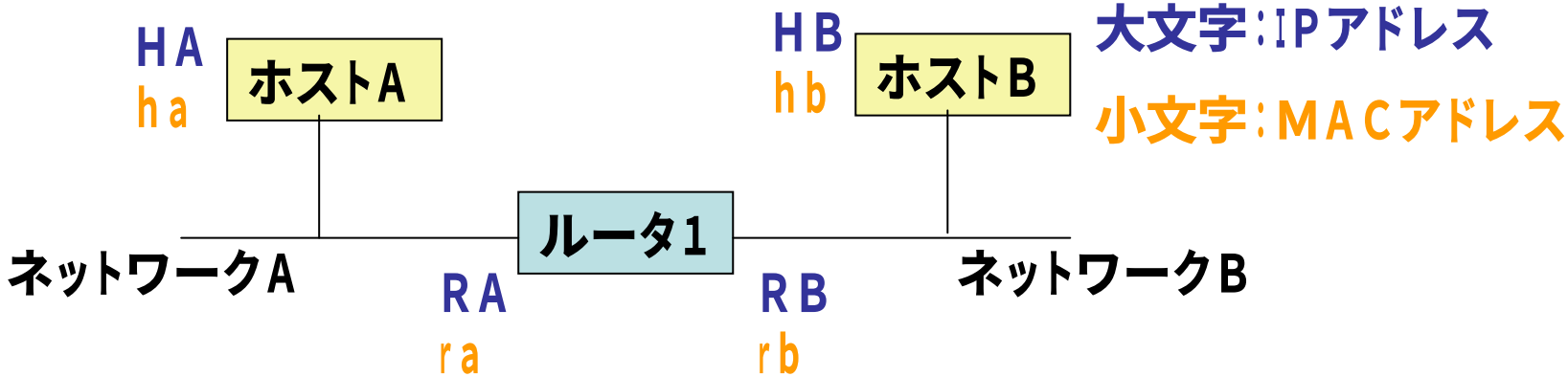



| ネットワークアドレス | 次のルータ |
|---|---|
| 遠方のネットワーク | 次のﾙｰﾀｱﾄﾞﾚｽ |
| 遠方のネットワーク | 次のﾙｰﾀｱﾄﾞﾚｽ |
| ⋮ | |
| 直結のネットワーク | 自分のｱﾄﾞﾚｽ |
| 直結のネットワーク | 自分のｱﾄﾞﾚｽ |

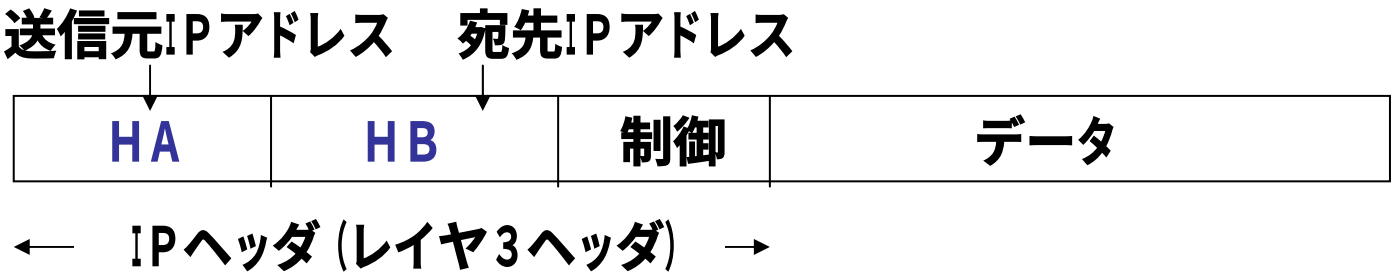
宛先がＬＡＮに直結していることを示す

ルータ1

| ネットワークアドレス | 次のルータ |
|---|---|
| 10.1.1.0/25 | 10.1.1.1 |
| 10.1.0.0/24 | 10.1.0.1 |




送り届けたいIPパケット



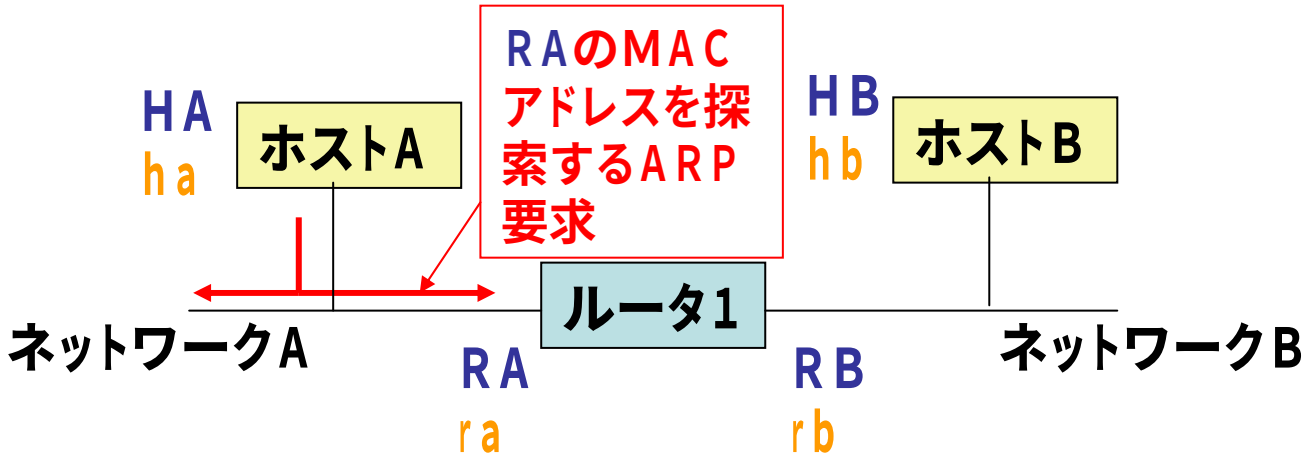

ホストAの経路制御表

| ネットワークアドレス | 次のルータ |
|---|---|
| ﾃﾞﾌｫﾙﾄｹﾞｰﾄｳｪｲ | RA |
| ネットワークA | HA |

ホストAの動作

経路制御表より、宛先HBは自ネットワークではない。

→デフォルトゲートウェイであるRAに送付する。




## ARP要求パケットの内容

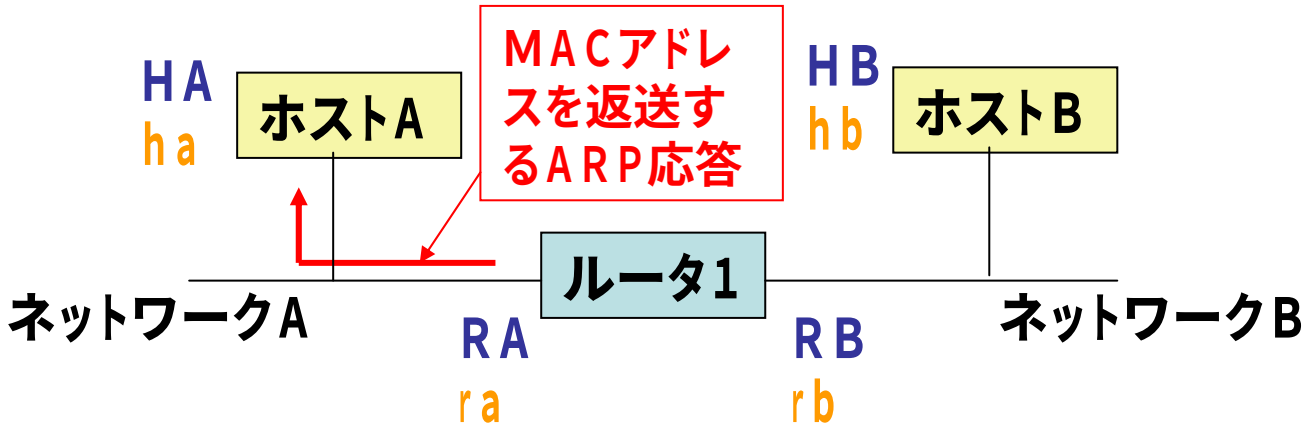
探索先のMACアドレスは不明なのでブランク

宛先MACアドレスはブロードキャスト

| all1 | ha | ホストA・MAC：ha | ホストA・IP：HA | 探索MAC：ブランク | 探索IP：RA |
|---|---|---|---|---|---|

送信元MACアドレス

レイヤ2ヘッダ




## ARP応答パケットの内容

宛先MACアドレス

送信元MACアドレス

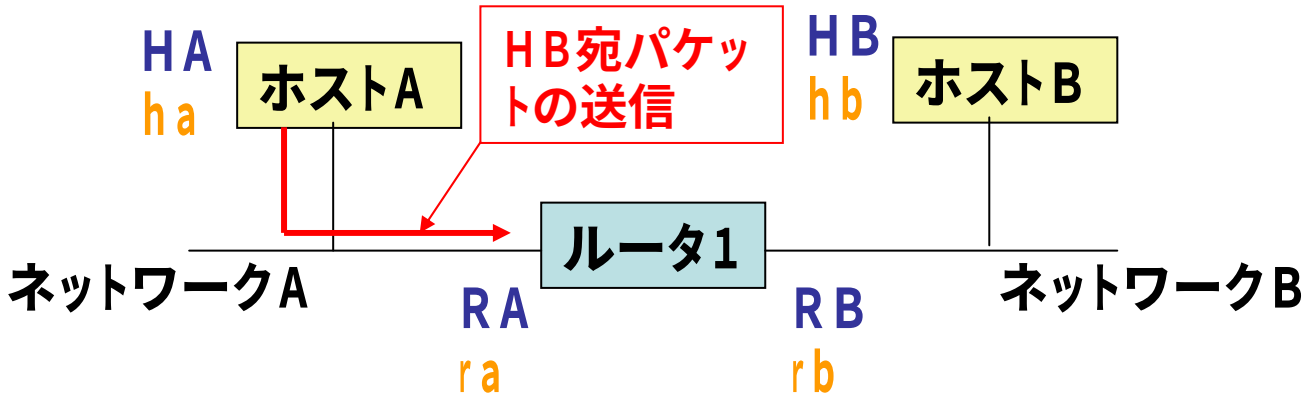
ルータ1のMACアドレスが埋められる

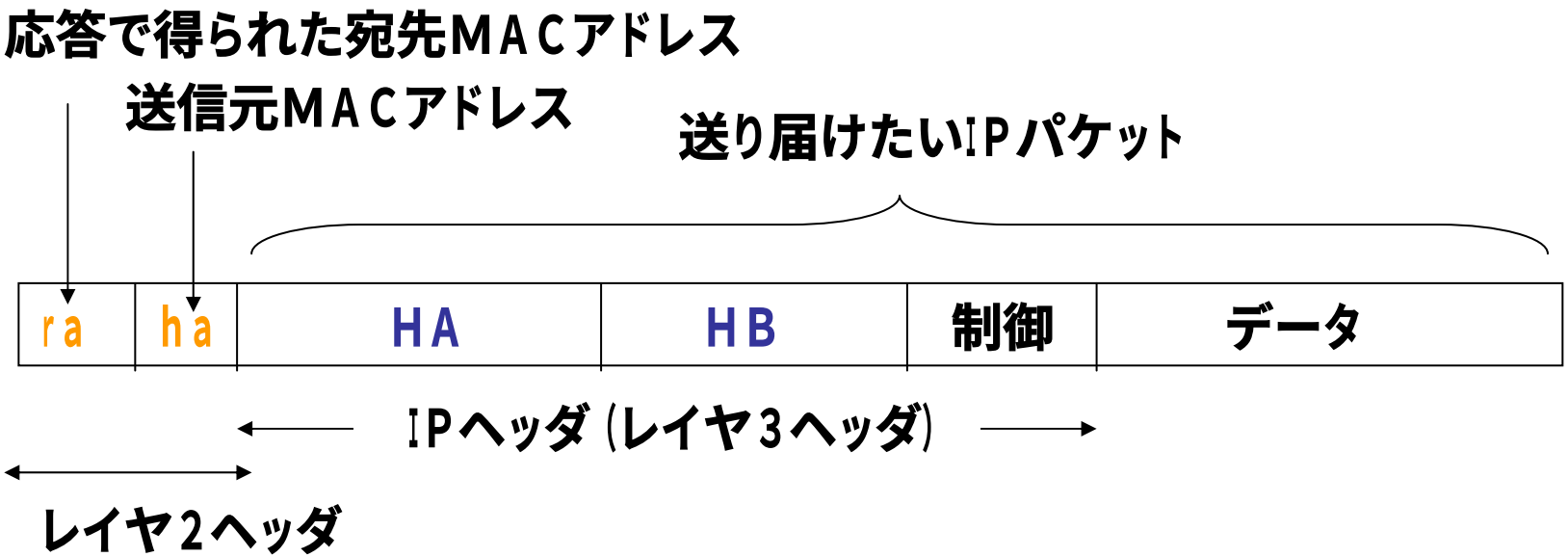
| ha | ra | ホストA・MAC：ha | ホストA・IP：HA | ルータ1・MAC：ra | ルータ1・IP：RA |
|---|---|---|---|---|---|

レイヤ2ヘッダ

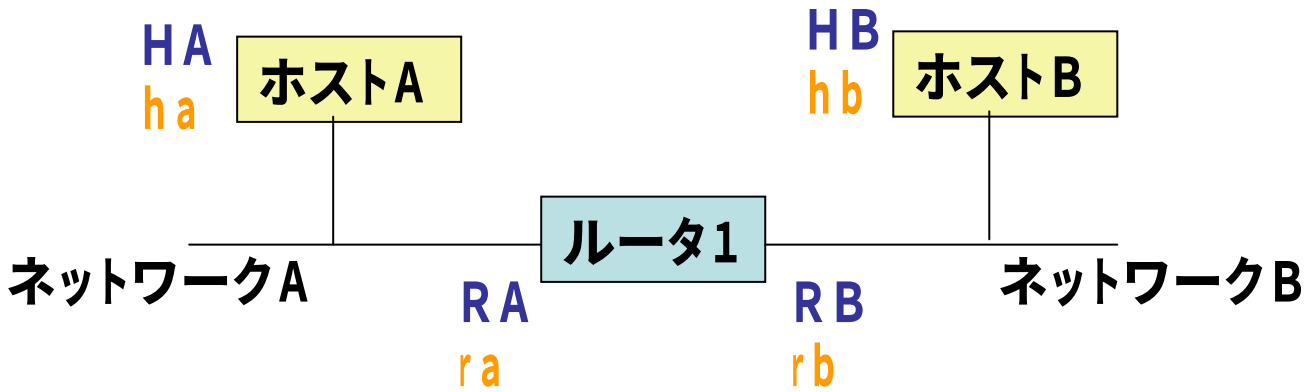
ARP要求と同じフォーマット

ホストAとルータ1の両方にARPキャッシュテーブルが作成される

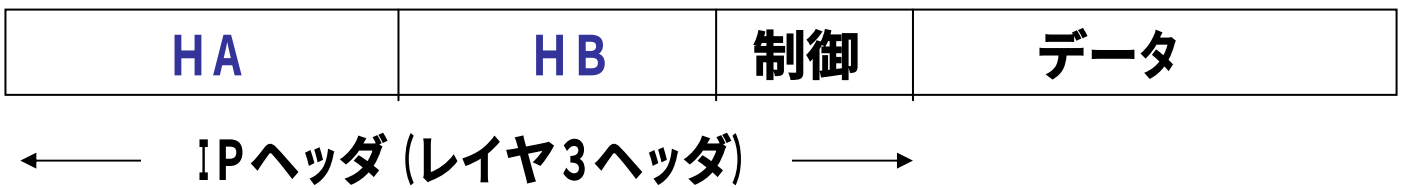



宛先、送信元の順はレイヤ2ヘッダとレイヤ3ヘッダで異なるので注意




受信したパケットを処理する（レイヤ2ヘッダは除去される）



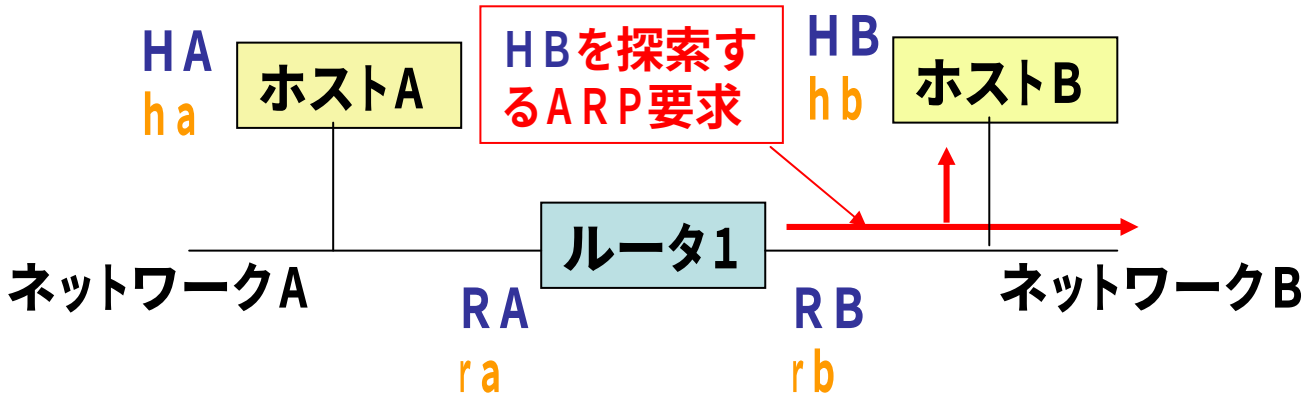

ルータ1の経路制御表

| ネットワークアドレス | 次のルータ |
|---|---|
| ネットワークA | RA |
| ネットワークB | RB |

ルータ1の動作

経路制御表より、宛先HBはネットワークBにあり、RB側に直結している。

→HBに直接送信する。



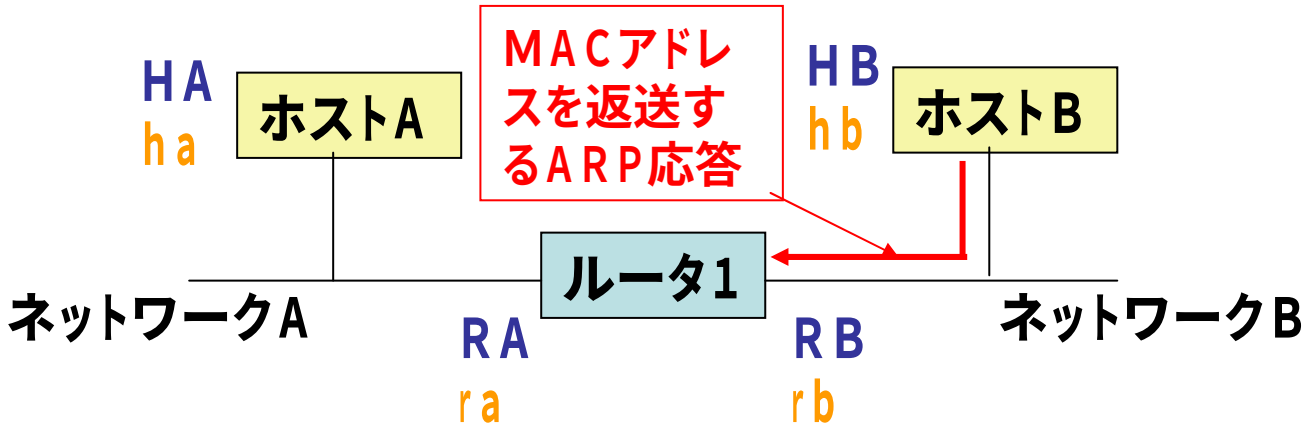

## ARP要求パケットの内容

探索先のMACアドレスは不明なのでブランク

宛先MACアドレスはブロードキャスト

| all1 | rb | ルータ1・MAC：rb | ルータ1・IP：RB | 探索MAC：ブランク | 探索IP：HB |
|---|---|---|---|---|---|

レイヤ2ヘッダ

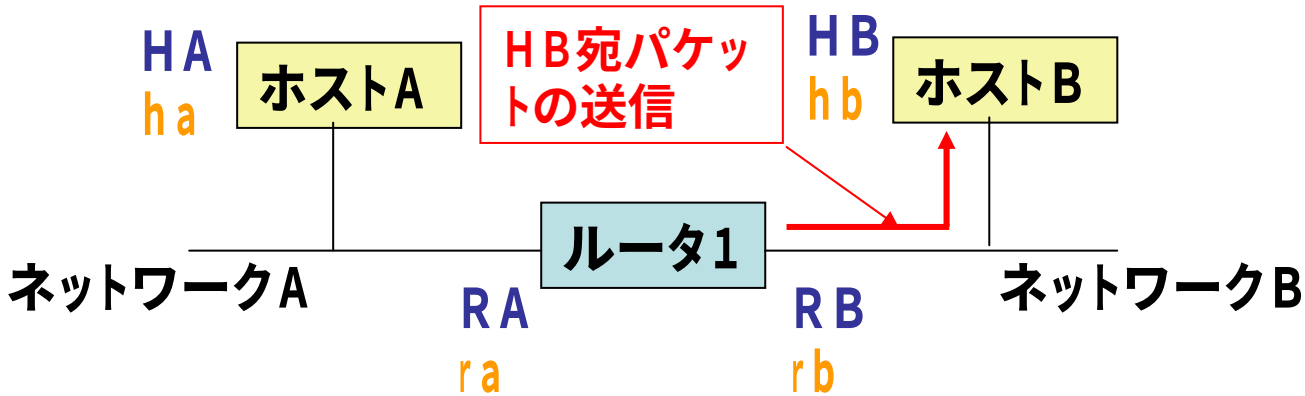



## ARP応答パケットの内容

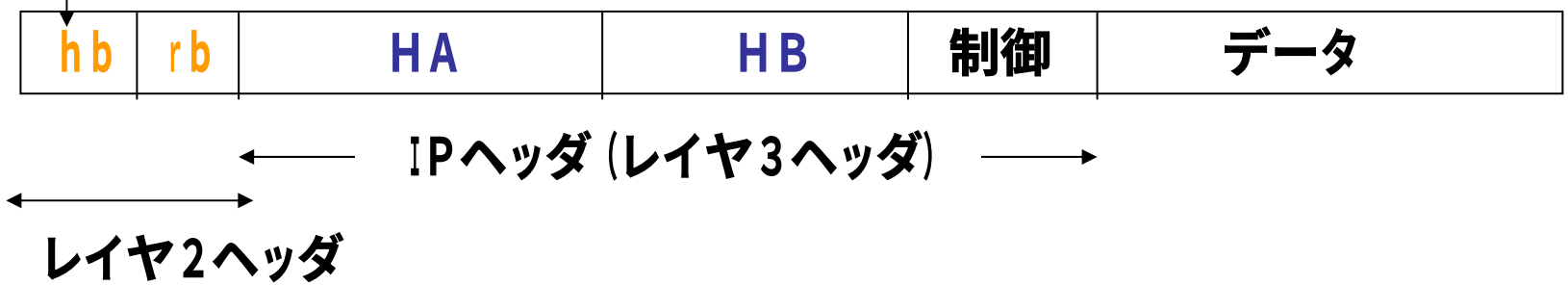
ホストBのMACアドレスが埋められる


レイヤ2ヘッダ

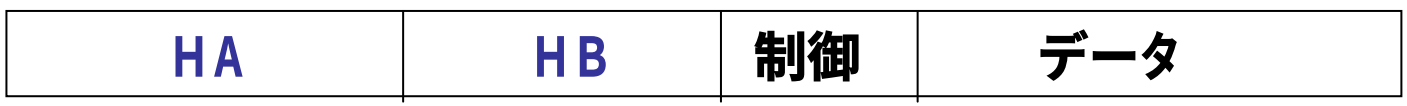
ARP要求と同じフォーマット



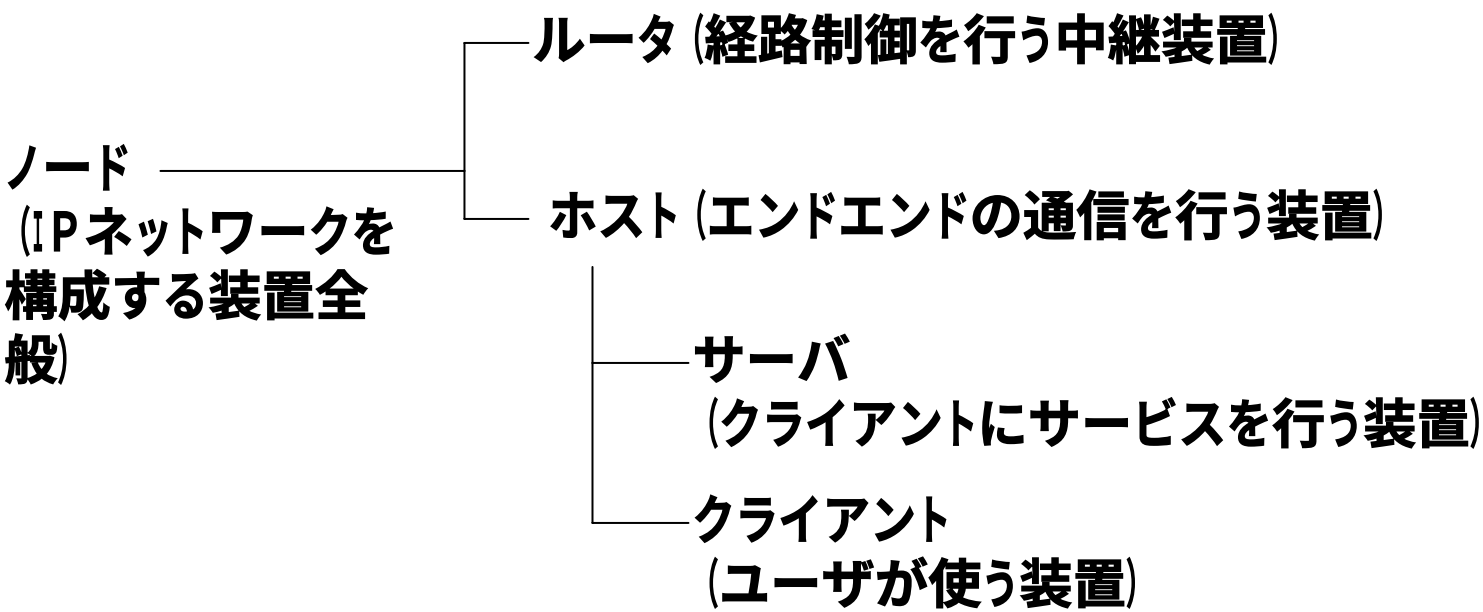

ARP応答で得られた宛先MACアドレス




届けられたIPパケット

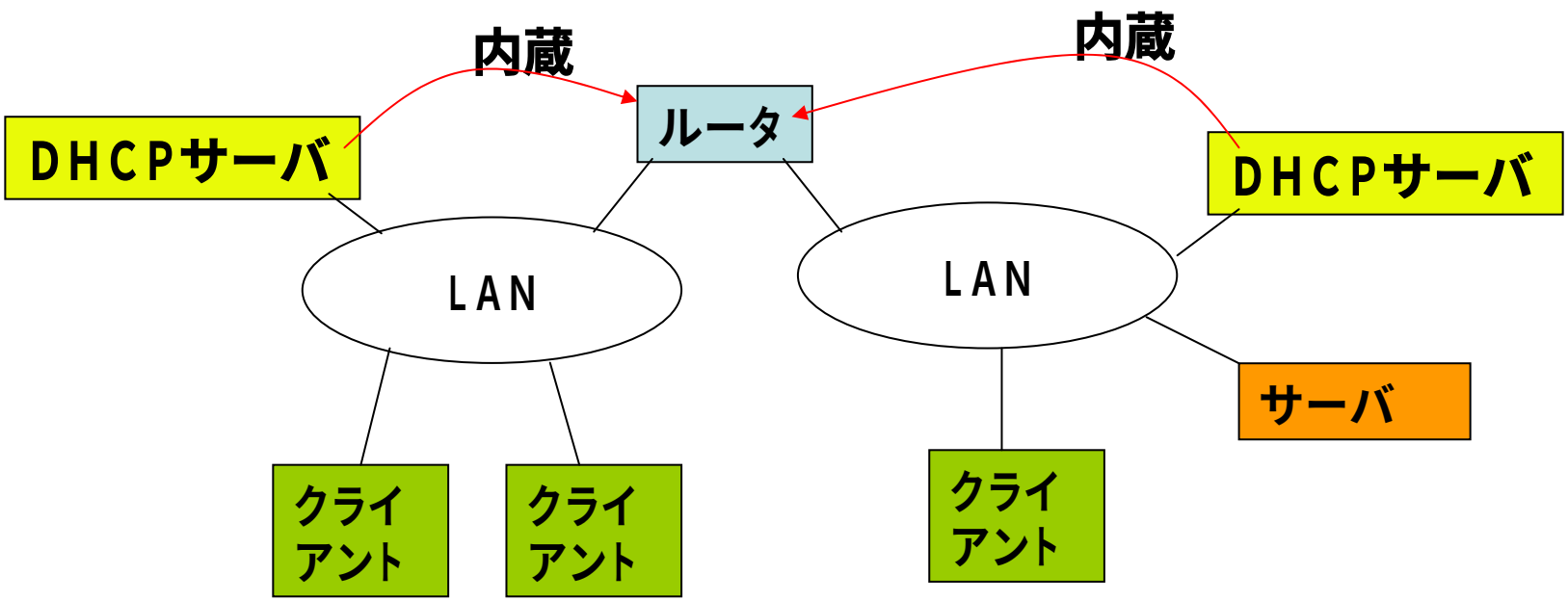


# 授業における用語の定義

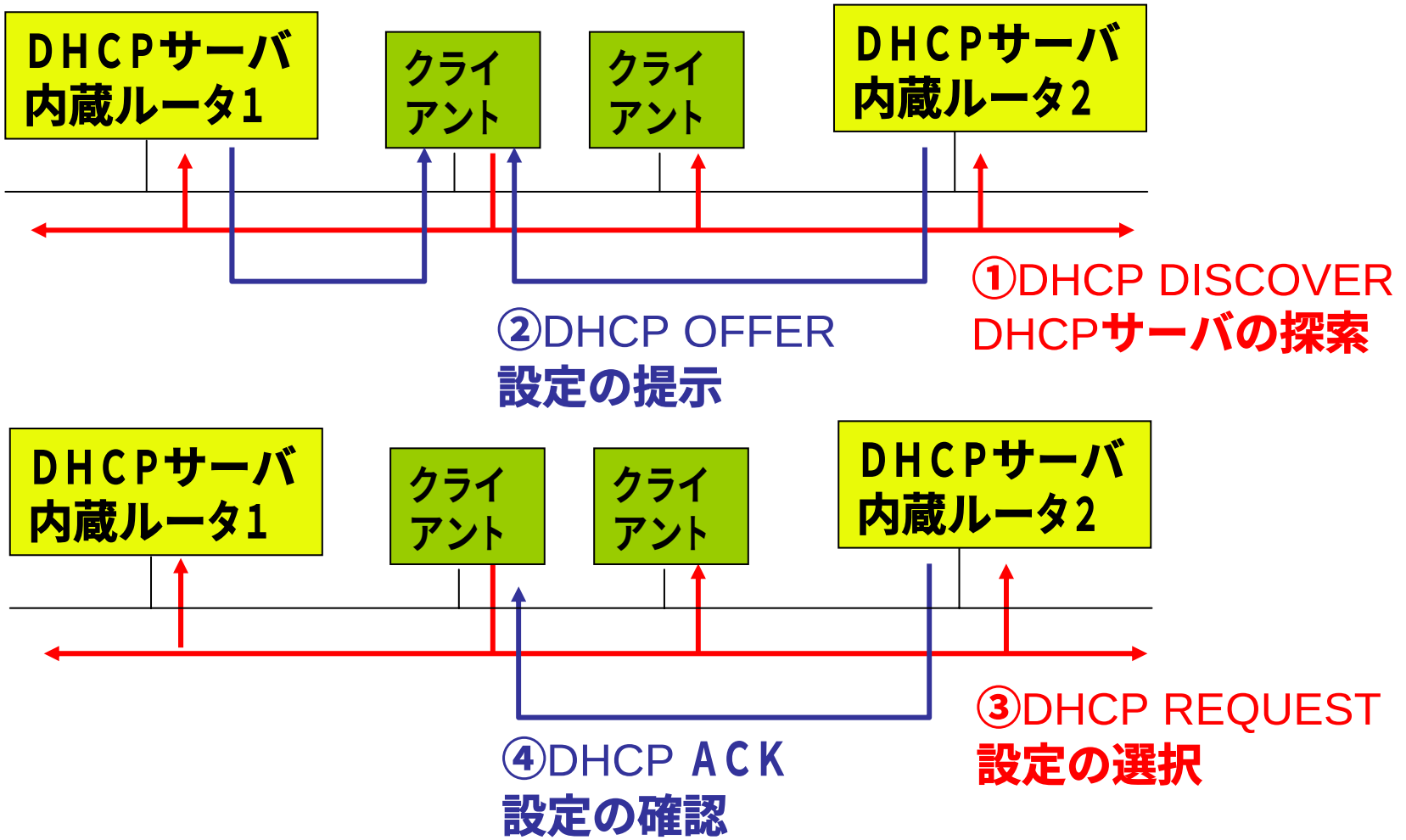


# DHCP (Dynamic Host Configuration Protocol)

- クライアントの設定を自動化する仕組み (プラグアンドプレイの実現)
- DHCPサーバをブロードキャストドメインごとに設置
- クライアントのIPアドレス、サブネットマスク、デフォルトゲートウェイアドレス、DNSサーバアドレスをDHCPサーバから自動配布。
- DHCPサーバ機能をルータが内蔵する場合が多い。
- サーバは一般にDHCPを使わない (IPアドレスが変わると困るため)。



# DHCPの仕組み




DHCPサーバは2重化が推奨されている

DHCPサーバはICMPエコーで2重アドレスのチェックを行う

クライアントはARP要求で2重アドレスのチェックを行う

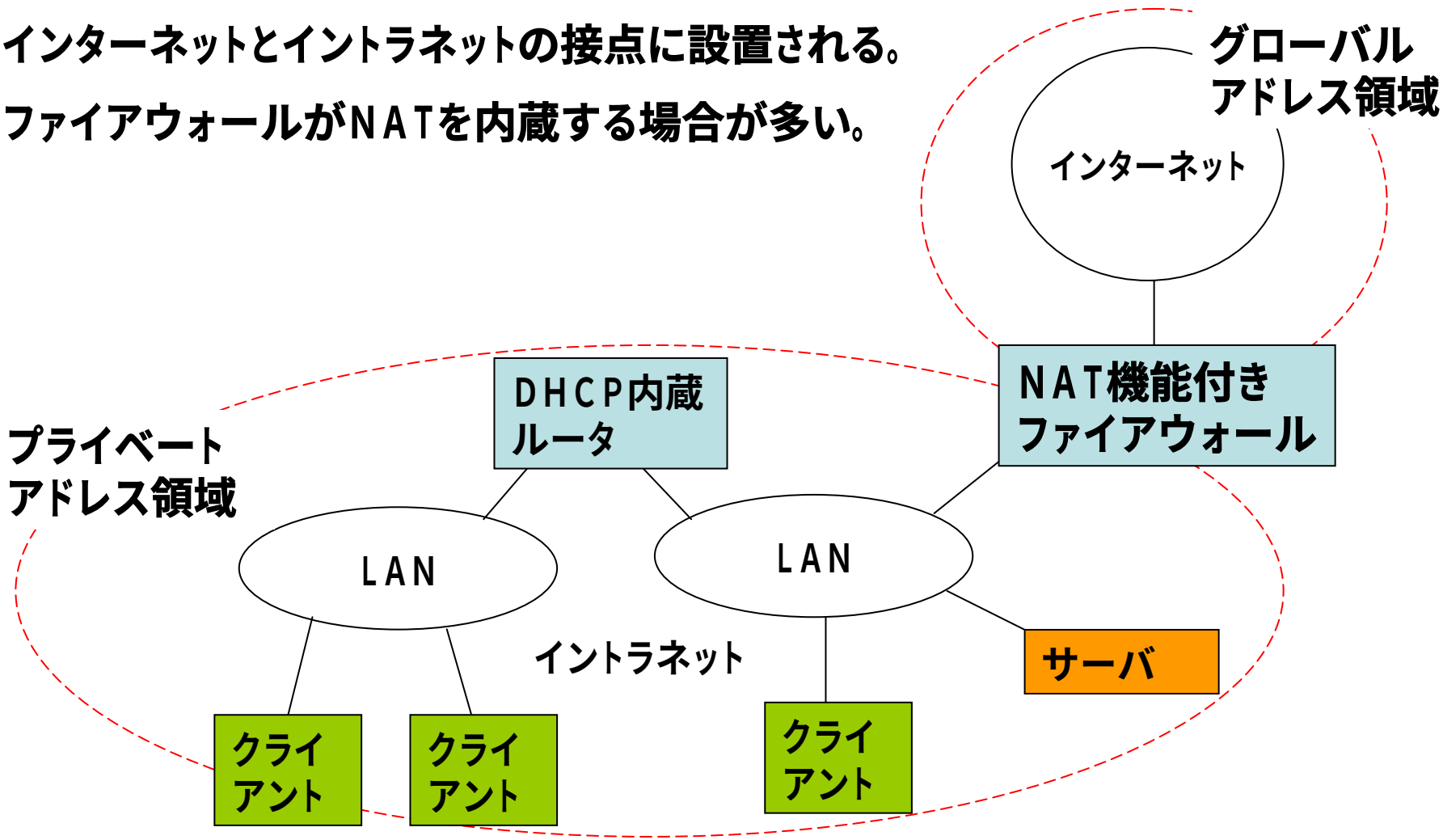
NAT (Network Address Translator)　ナットと呼ぶ

NAPT(Network Address Ports Translator)　ナプトと呼ぶ

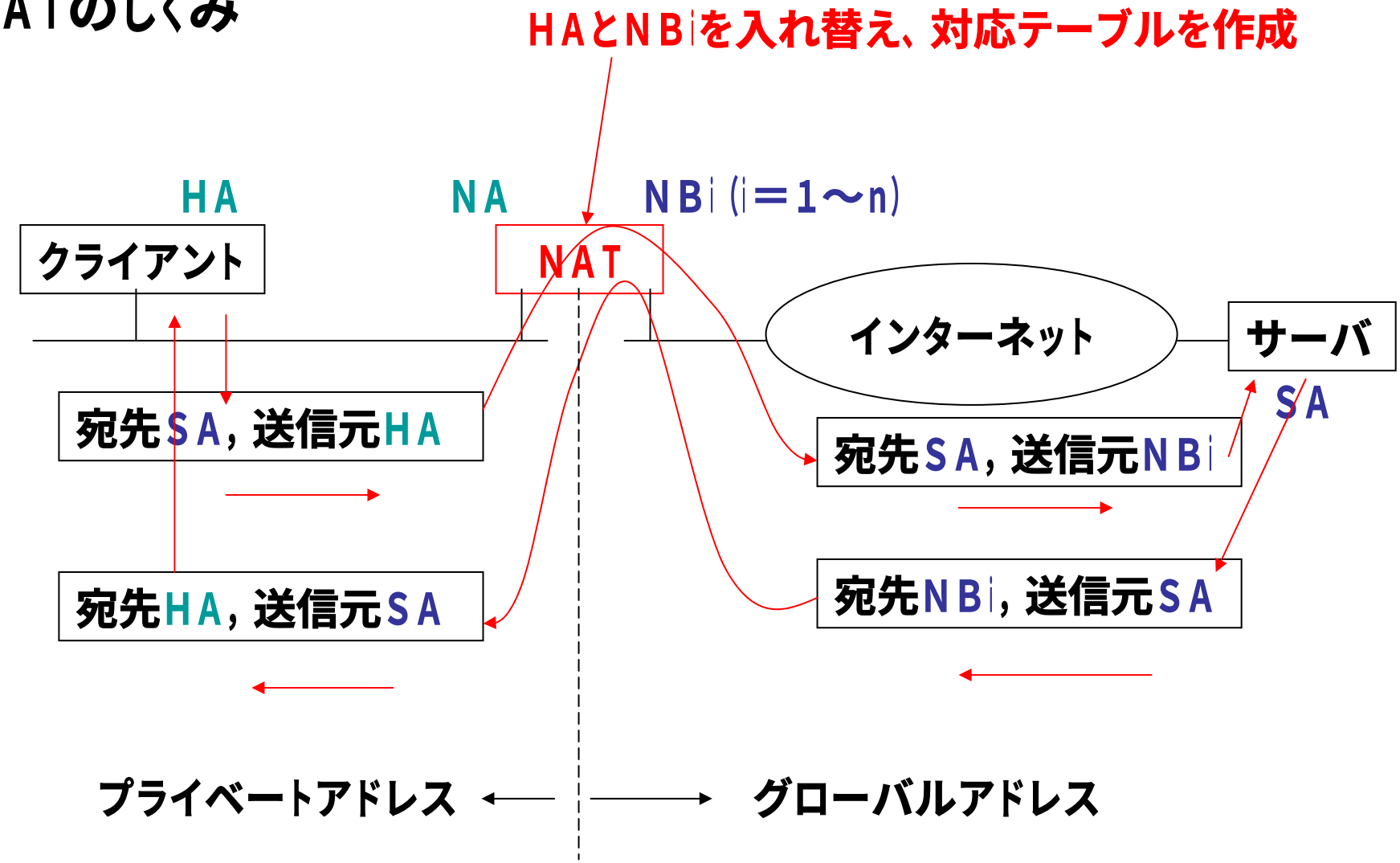
・プライベートアドレスとグローバルアドレスの変換を行う装置。

・インターネットとイントラネットの接点に設置される。

・ファイアウォールがNATを内蔵する場合が多い。



# NATのしくみ



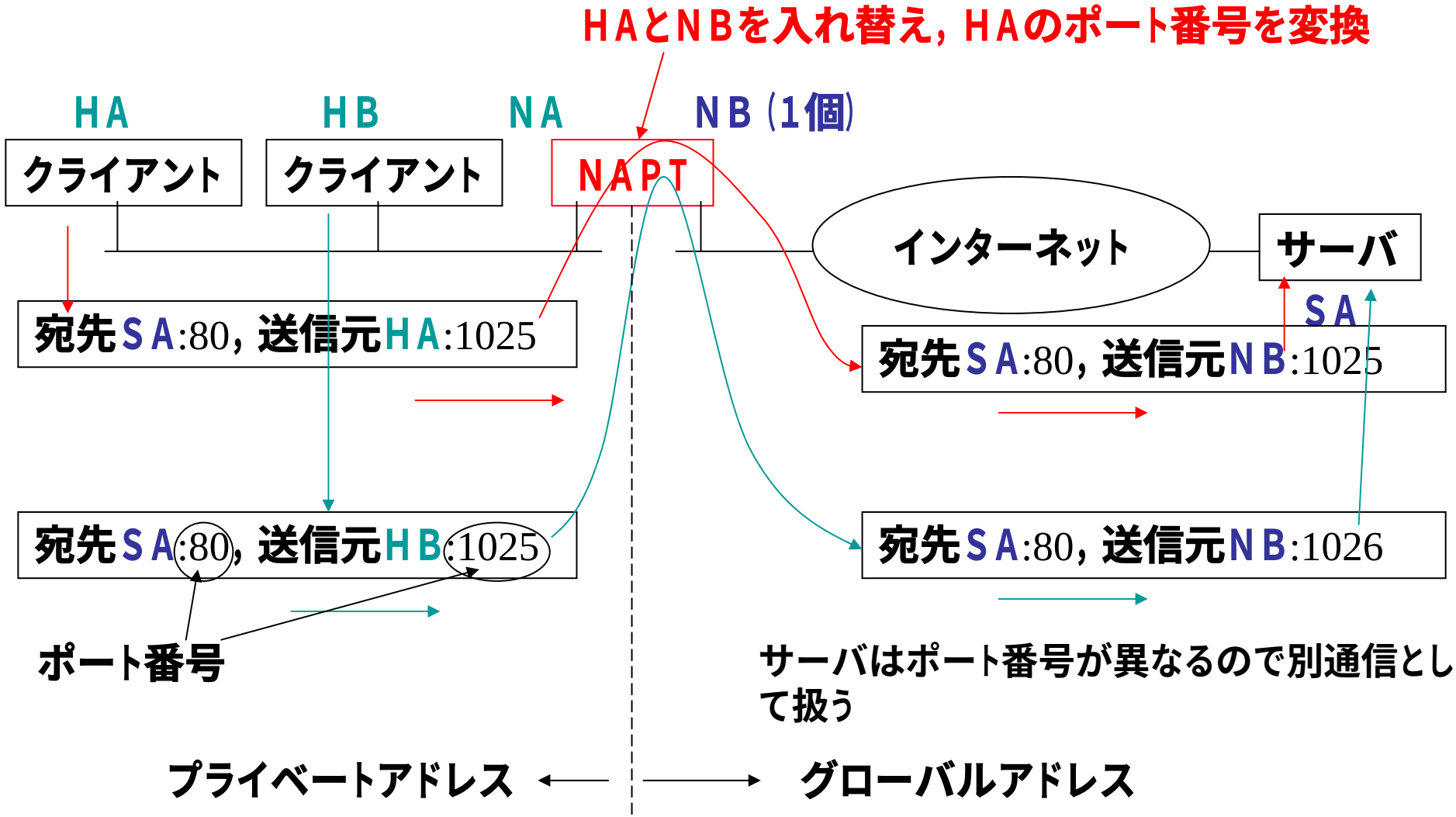

NATはn個のグローバルアドレスをプールしている

グローバルアドレス宛パケットはインターネット側へルーティングされる

# NAPTのしくみ

グローバルアドレスは1つだけ確保すればよい

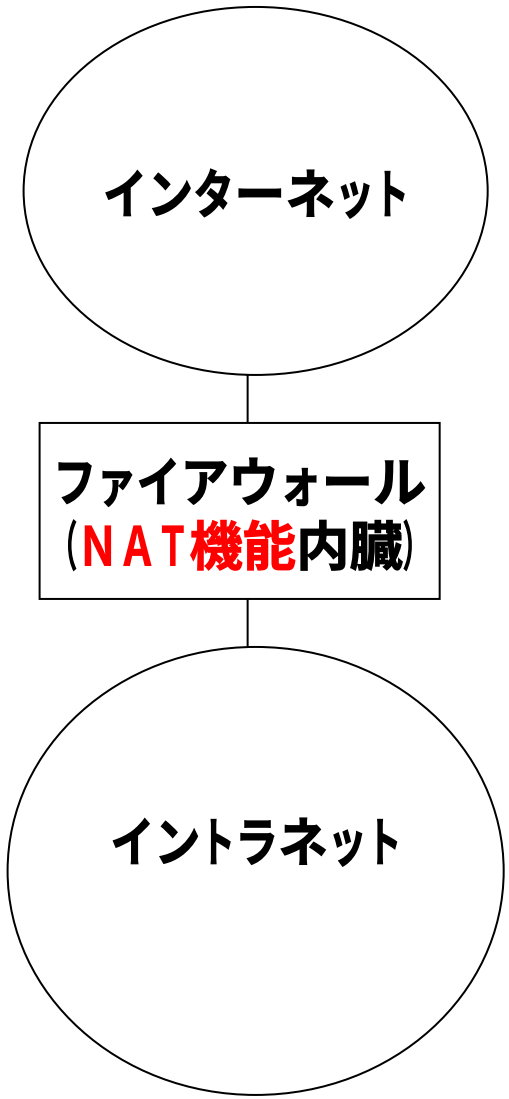
(TCP／UDPのポート番号を使う)



# ファイアウォール

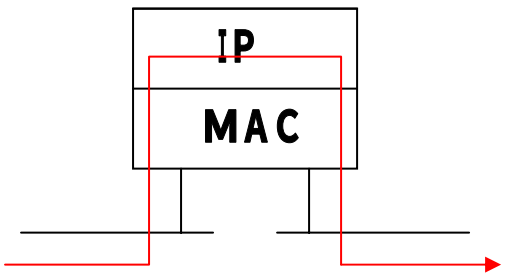
・組織内のネットワークを外部の脅威から守るための機器および技術の総称。

・ファイアウォールを設置する理由
  ・情報流出入経路の限定。
  ・内部ネットワークを統一的に保護。
  ・内部ネットワークの隠蔽。 ⟶NATのこと
  ・情報の取捨選択。
  ・入出力ログの作成、アクセスの記録。



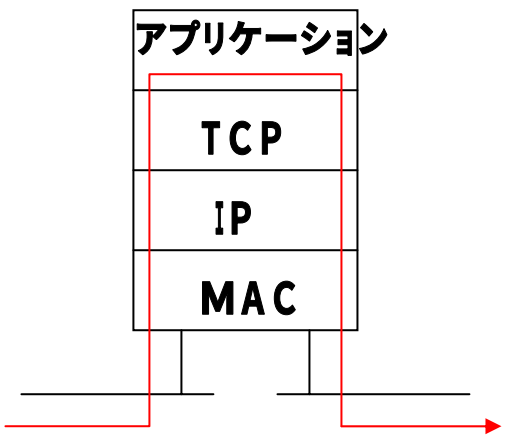
# ファイアウォールの制御方式

## パケットフィルタリング方式



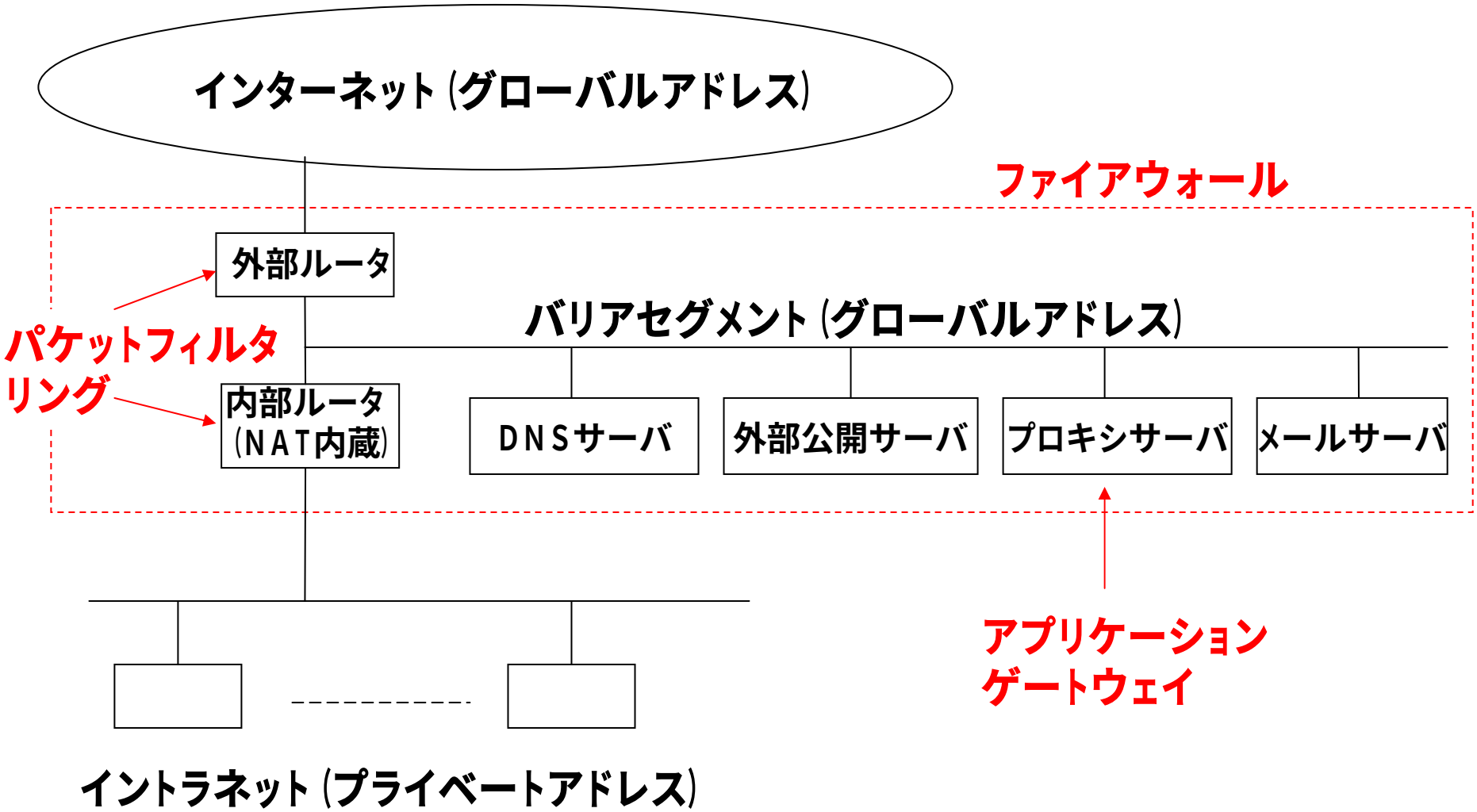

パケットごとにヘッダ部を精査する．
・IPアドレス，プロトコル番号（IPヘッダ）
・ポート番号，コネクションの方向（TCPヘッダ）
高速処理が可能
木目細かい制御は困難

## アプリケーションゲートウェイ方式




アプリケーションでデータの動きを監視
アプリケーション対応の制御
利用者認証が可能
代表はプロキシサーバ
セキュリティ強度が高い
アプリケーションごとにソフトウェアが必要
処理負荷大、性能低下

# ファイアウォールの具体的な構成（大規模組織の例）



# ホスト名

・ホストにはホスト名をつける。

・通信はホスト名を指定して行うのが一般（特にサーバに対して）。

例　rj43411.meijo-u.ac.jp　　個人のホスト名

www.meijo-u.ac.jp　　名城大学のWWWサーバ名

ドメイン名

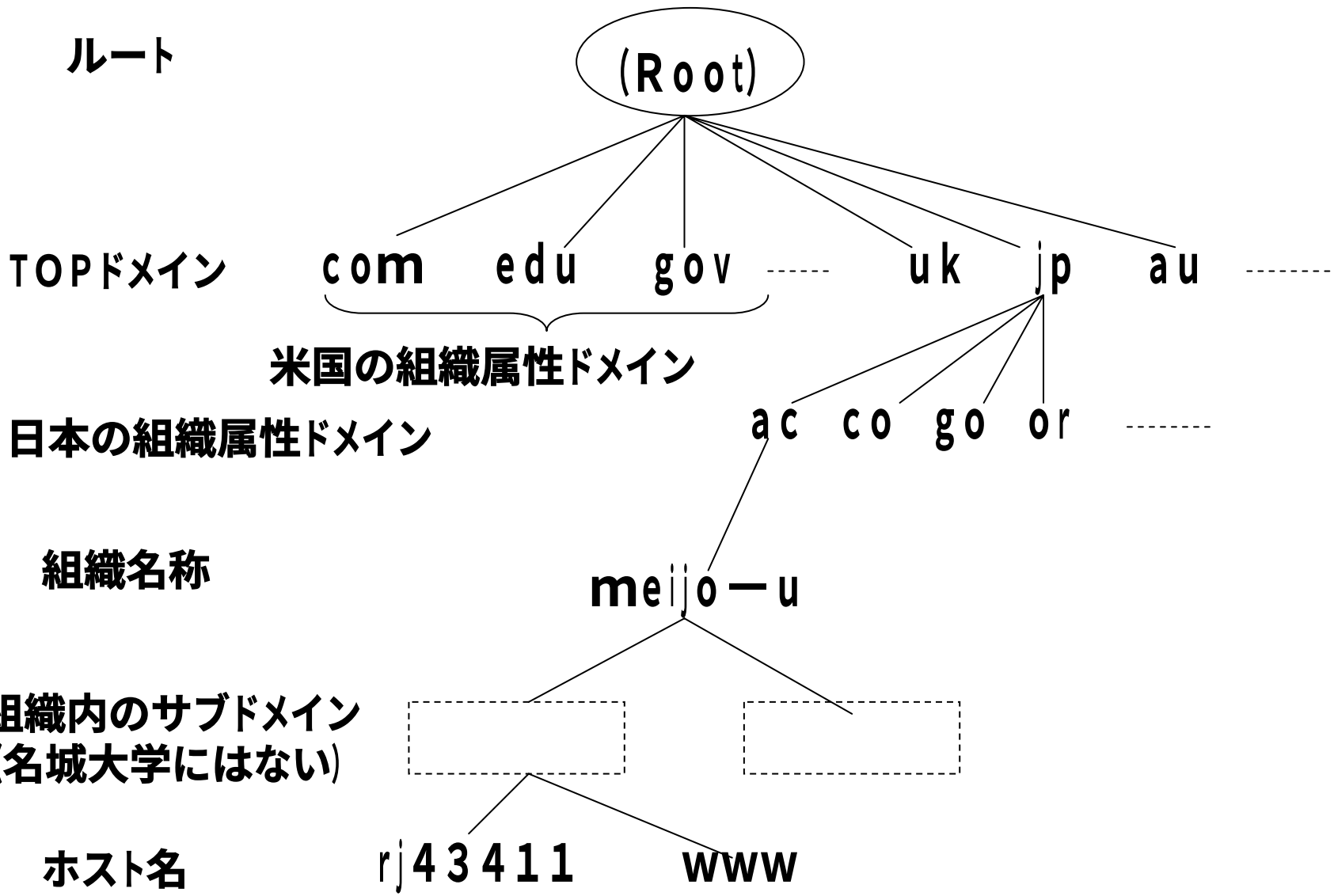
・組織名称のドメイン名はJPNICに申請するか、プロバイダ経由で申請する。

・組織内のサブドメイン名は、組織が管理する。

・ドメイン名の階層とIPアドレスの割り当ては基本的に無関係。

・ドメイン名は組織図に近い形で決めることができる。

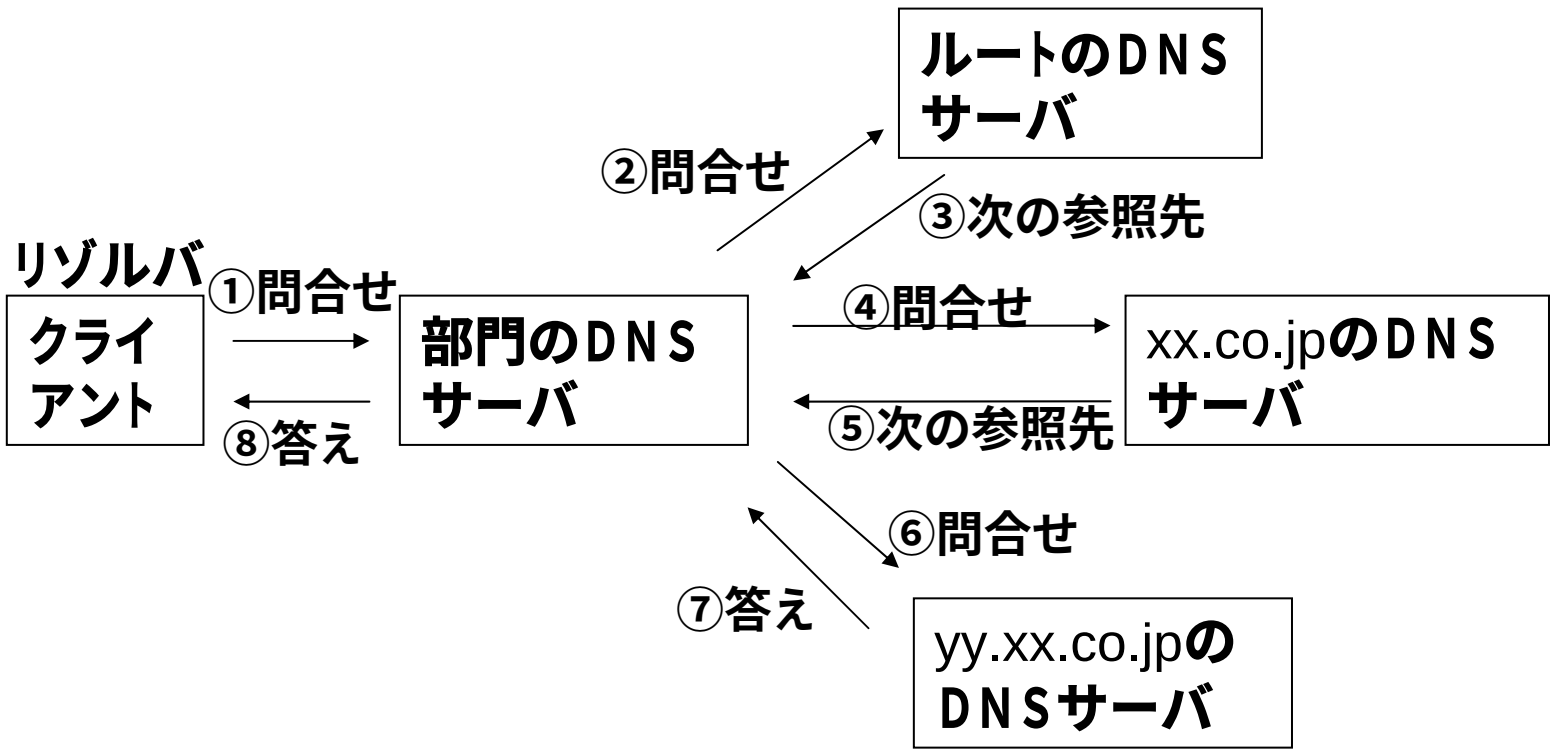
# ドメイン名


ルート
(Root)
TOPドメイン
com
edu
gov
uk
jp
au
米国の組織属性ドメイン
日本の組織属性ドメイン
ac
co
go
or
組織名称
meijo－u
組織内のサブドメイン
(名城大学にはない)
ホスト名
rj43411
www

# ＤＮＳ(Domain Name System)

・ホスト名とIPアドレスの関係を管理する分散データベースシステム

・リゾルバからのホスト名の問合せに対し、該当するIPアドレスを応える。




・ＤＮＳサーバはドメインごとに設置する。

・部門のＤＮＳサーバのIPアドレスはリゾルバに登録しておく必要がある。

登録情報：IPアドレス，アドレスマスク，デフォルトゲートウェイ，ＤＮＳサーバアドレス

# 演習

・ＮＡＴが必要となる理由と、その動作原理を示せ。

・ＤＮＳが必要となる理由と、その動作原理を示せ。