

パケットトレーサで学ぶNW構築 (基礎編)

③ NATを使用してインターネットに接続してみよう！



お 品 書 き

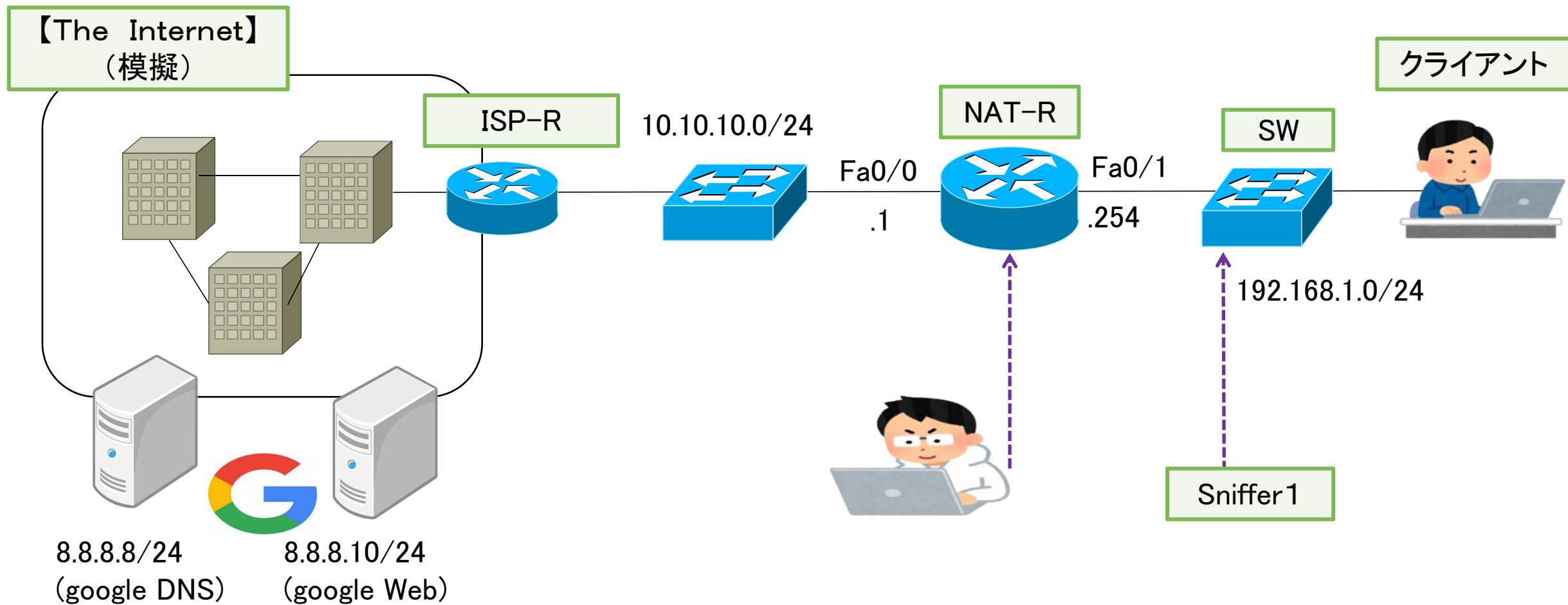
- 1 構成の確認
 - 2 (おさらい)ルータによるルーティングの基礎
 - 3 NAT(IPマスカレード)の概要
 - 4 NATを使用してインターネットに接続してみよう！
 - 5 参考:DNSサーバの設定
- 参考サイト ネットワークエンジニアとして (NAT/PATをはじめてから)
<https://www.infraexpert.com/study/study34.html>

使用する実習ファイルはNO.3.pktになります！

1 構成の確認

1 構成の確認

構成図



インターネットのアドレス
は架空のものです

2（おさらい）

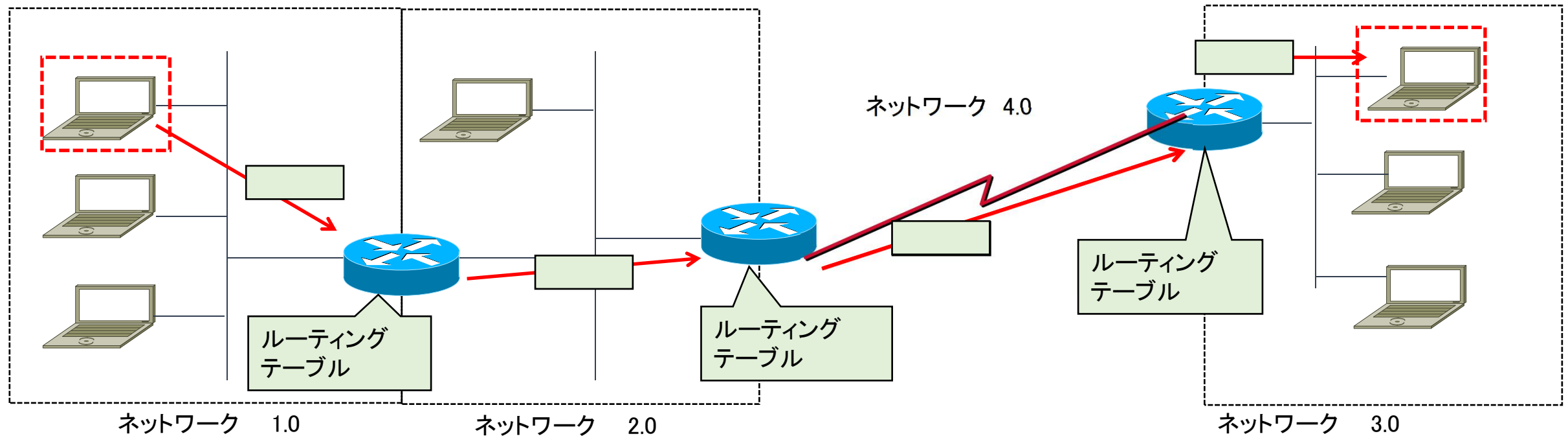
ルータによるルーティングの基礎

2 (おさらい) ルータによるルーティングの基礎

【ルータの役割】

- 異なるネットワークアドレスを持つネットワークの接続することが役割です
【接続されたネットワークアドレスの情報をルーティングテーブルとして作成管理】
- データの宛先プロトコルアドレスを使用してルーティングテーブルを用いてルーティングする

イメージ



- * ルータはブロードキャストドメインを分割
- * 異なるネットワークを結ぶにはルータが必要

2 (おさらい) ルータによるルーティングの基礎

【ルーティングテーブルとは？】

通信可能なネットワークへの経路情報を管理(ルータがデータ転送の際の判断基準)

(例 CISCORルータでの場合)

テーブル上にある宛て先ネットワークをどのような方法で取得したか

Router#show ip route

Codes: C – connected, S – static, R – RIP, M – mobile, B – BGP

D – EIGRP, EX – EIGRP external, O – OSPF, IA – OSPF inter area

N1 – OSPF NSSA external type 1, N2 – OSPF NSSA external type 2

E1 – OSPF external type 1, E2 – OSPF external type 2

i – IS-IS, su – IS-IS summary, L1 – IS-IS level-1, L2 – IS-IS level-2

ia – IS-IS inter area, * – candidate default, U – per-user static route

o – ODR, P – periodic downloaded static route

デフォルトルートの設定

※ Gateway of last resort is 0.0.0.0 to network 0.0.0.0

出カインタフェース

S 192.168.30.0/24 is directly connected, Serial0
[1/0] via 192.168.20.1

ネクストホップ

C 192.168.10.0/24 is directly connected, FastEthernet0

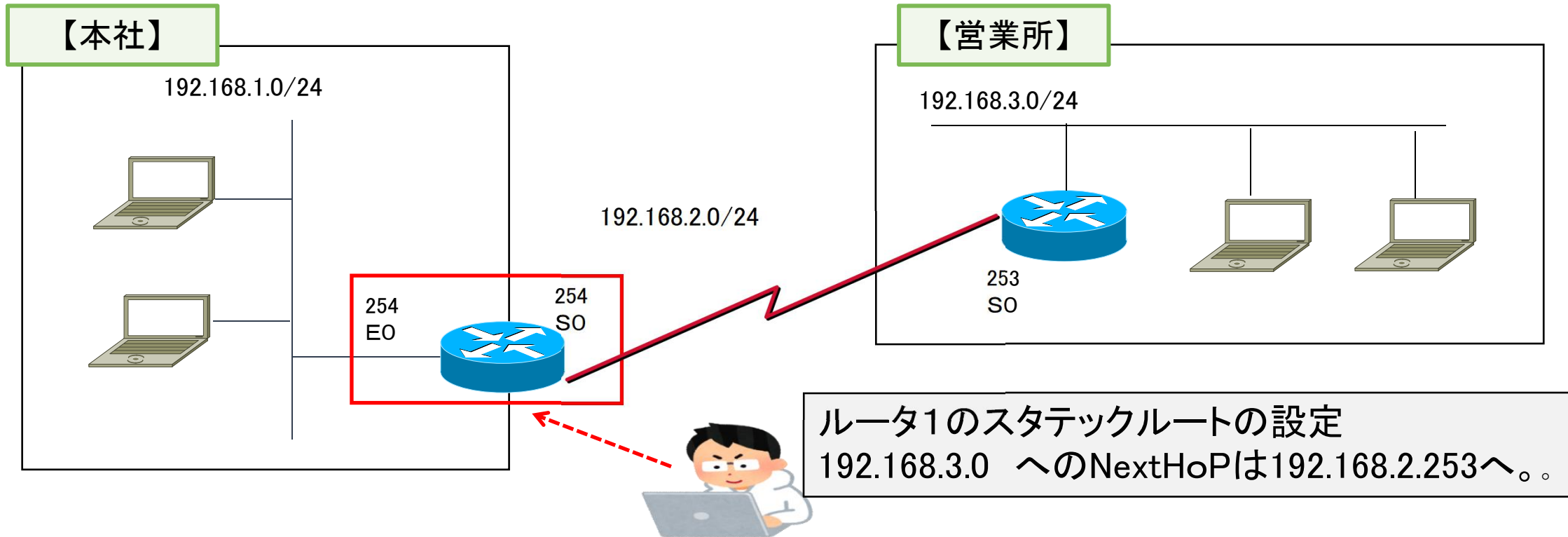
C 192.168.20.0/24 is directly connected, Serial0

S* 0.0.0.0/0 is directly connected, FastEthernet0

2 (おさらい) ルータによるルーティングの基礎

【スタテックルーティング】

○ルータの管理者が明示的にルーティングの情報を設定します！！



利点: 経路が固定されているため、管理者の意図した経路を選択可能

ルーティング情報の交換によるネットワーク上の帯域の使用がない

欠点: 通信させたいネットワークへの経路情報を全て登録する必要がある。

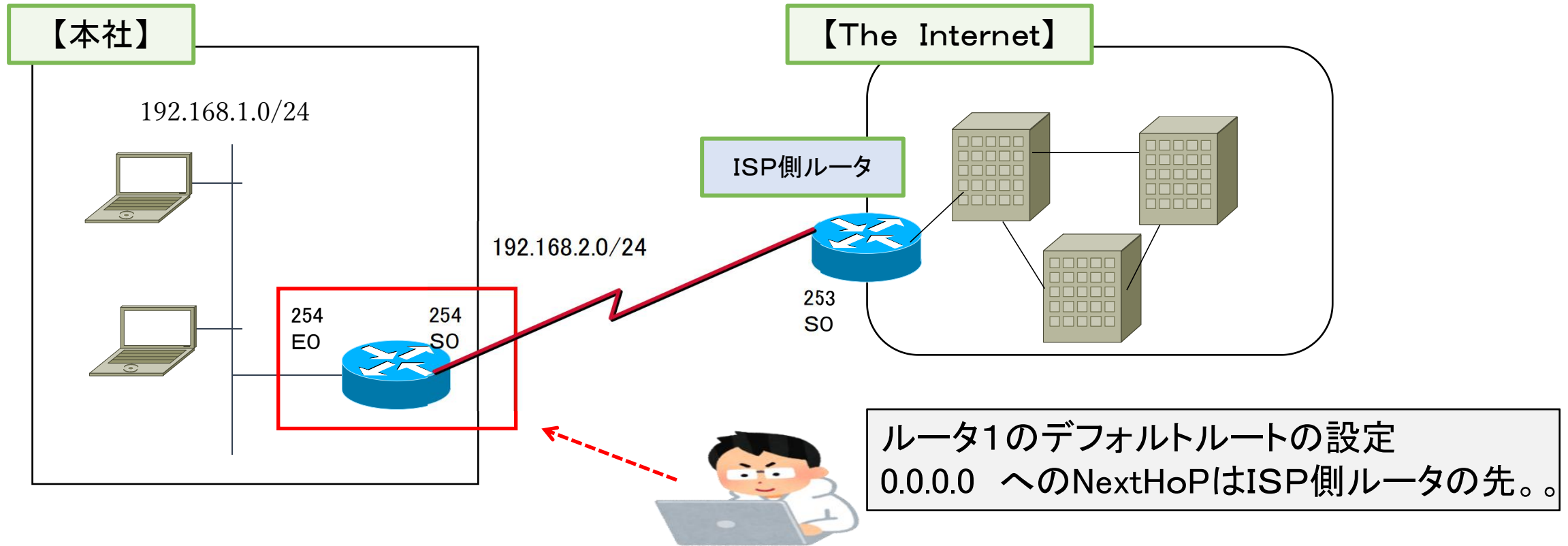
各ルータに整合性のある経路情報を設定する必要がある。

経路に障害が発生した場合に自動的に経路を変更したり、追加したりできない。。

2 (おさらい) ルータによるルーティングの基礎

【スタックルーティング: デフォルトルート】

- ・ルーティングテーブルにないネットワーク宛のデータを転送する経路
- ・一般に「0.0.0.0」に対する経路がデフォルトルートになります。



インターネットに接続される家庭用ルータなどでよく使用します！

(インターネットの経路は一杯あるので、全部全部設定していたら大変。。)

→ 1行で済むので楽ちん！！

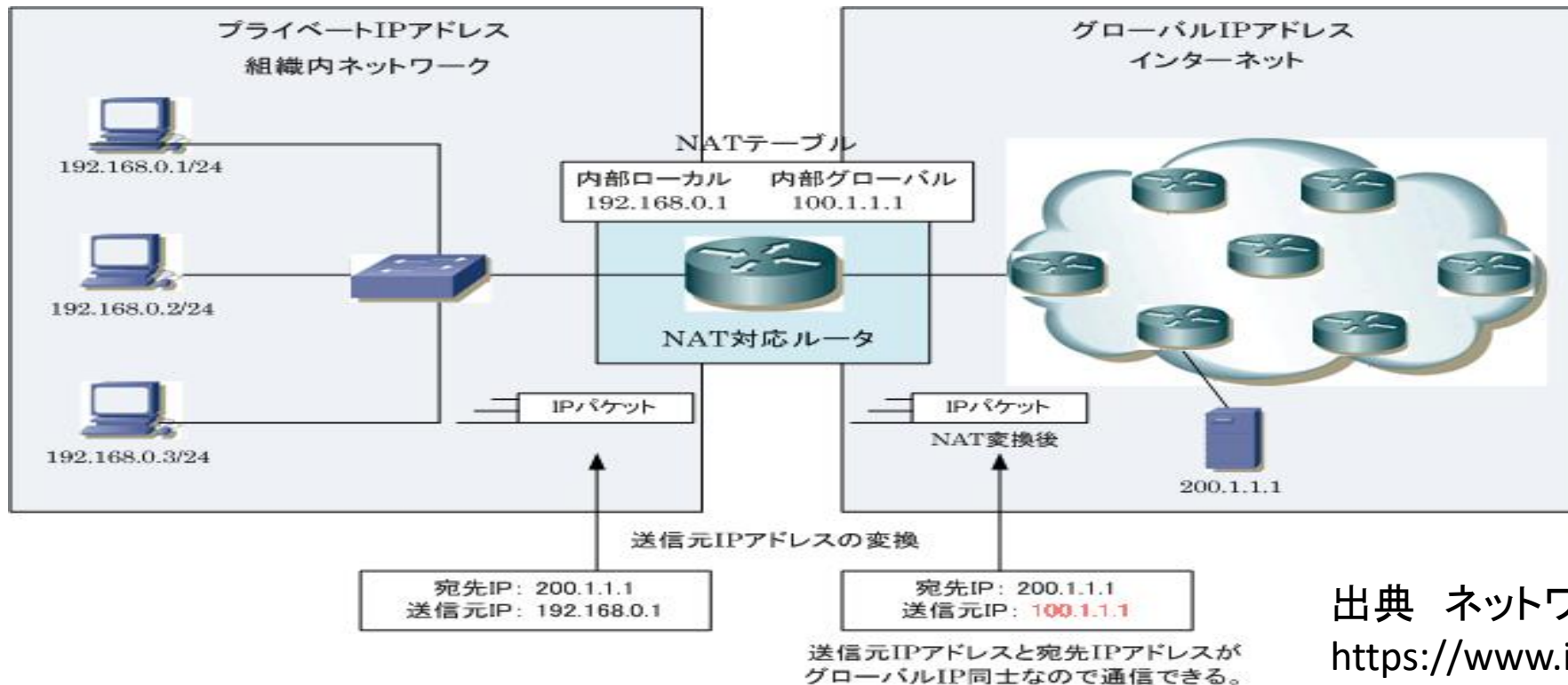
3 NAT(IPマスカレード)の基礎

3 NAT(IPマスカレード)の基礎

NAT(IPマスカレード)とは??

NAT(Network Address Translation)はIPアドレスを変換する技術です。

一般的には、プライベートIPアドレスをグローバルIPアドレスに変換する技術とされています。インターネットでは、グローバルIPアドレスを使用して構築したネットワークですが、企業ネットワークでは、プライベートIPアドレスを使用して構築されたネットワークなので、企業LANネットワークのクライアントPCがインターネット接続する場合、プライベートIPアドレスをグローバルIPアドレスに変換(NAT)をする必要があります。



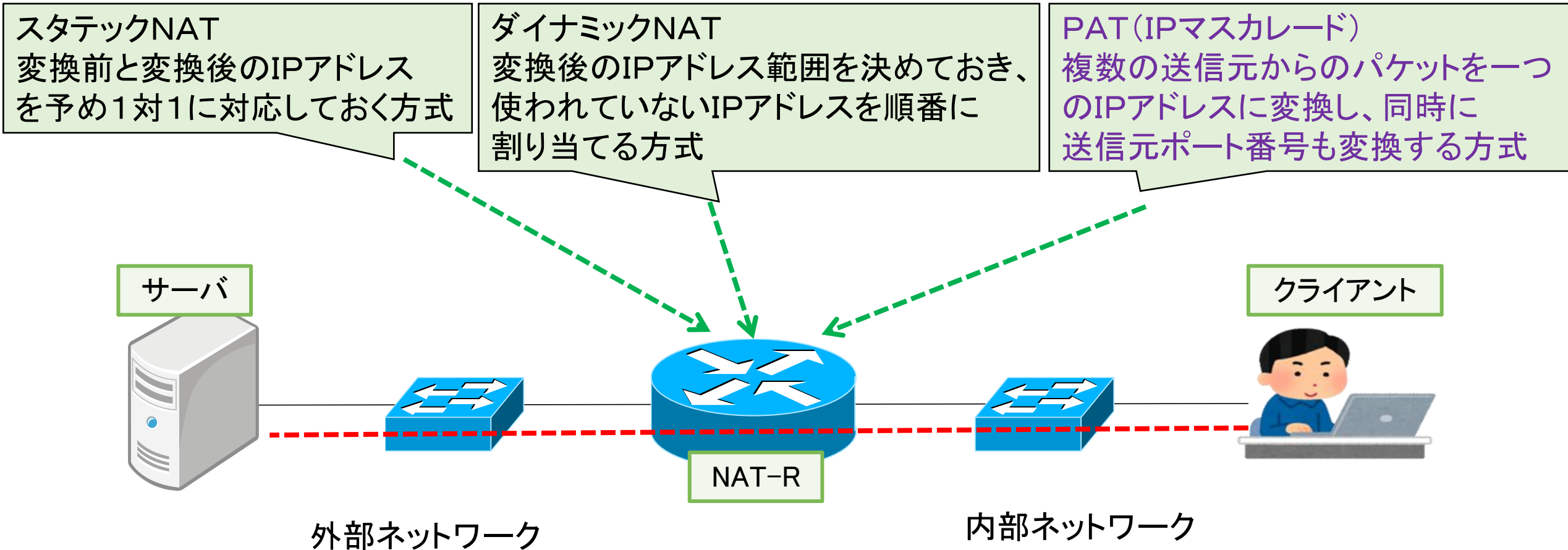
出典 ネットワークエンジニアとして

<https://www.infraexpert.com/study/ip10.html>

3 NAT(IPマスカレード)の基礎

NATの方式

NATには「スタテックNAT」、「ダイナミックNAT」、「PAT」の3つの方式があります。
パケットの送信元アドレスを変換するのはいずれも同じです！



今回はPAT(port address translation)を使用してインターネットに接続します！

3 NAT(IPマスカレード)の基礎

CISCOルータにおけるNATの設定手順

- ① ACLによるアドレス変換対象ネットワークの指定
変換対象のネットワークを正しく設定しましょう！
- ② NAT設定
今回はPAT(port address translation)を設定しています！
- ③ 該当のインタフェースにNAT設定を適用
WAN側とLAN側にそれぞれ適用しましょう！

それぞれの設定の意味
を理解しましょう！



3 NAT(IPマスカレード)の基礎

ACLとは??

ACLは指定した内容の packets を操作するための条件文のリストです。
インタフェースにACLを適用すると packets を通過させたり廃棄したりするフィルタとして利用できる。

条件文を1行目
から順番に参照

ACL: 100番

1行目: Telnetアクセスは拒否

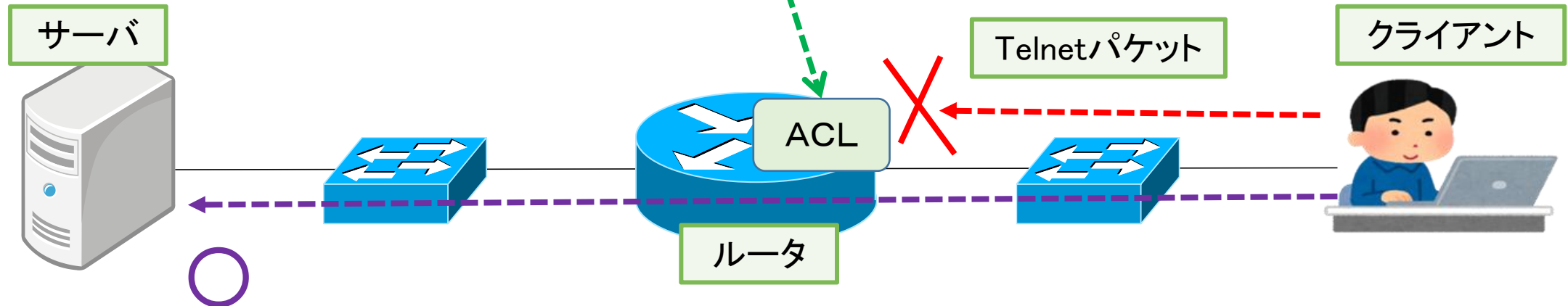
2行目: Webアクセスは許可

・
・
・

最終行: すべて拒否(暗黙の拒否)

パケットの内容と
条件文を比較

どの条件にも
合致しなかったら拒否
(自動的に挿入される)



3 NAT(IPマスカレード)の基礎

今回のACL使用イメージ

ACLで指定した条件を「パケットのフィルタリング」と「NATにおける変換対象の指定」に使用します！

ACL100番を「フィルタリングの条件指定」と「NATにおける変換対象の指定」の2つに使う

ACL: 100番

1行目: 10.100.100.0/24からのWebアクセスは許可

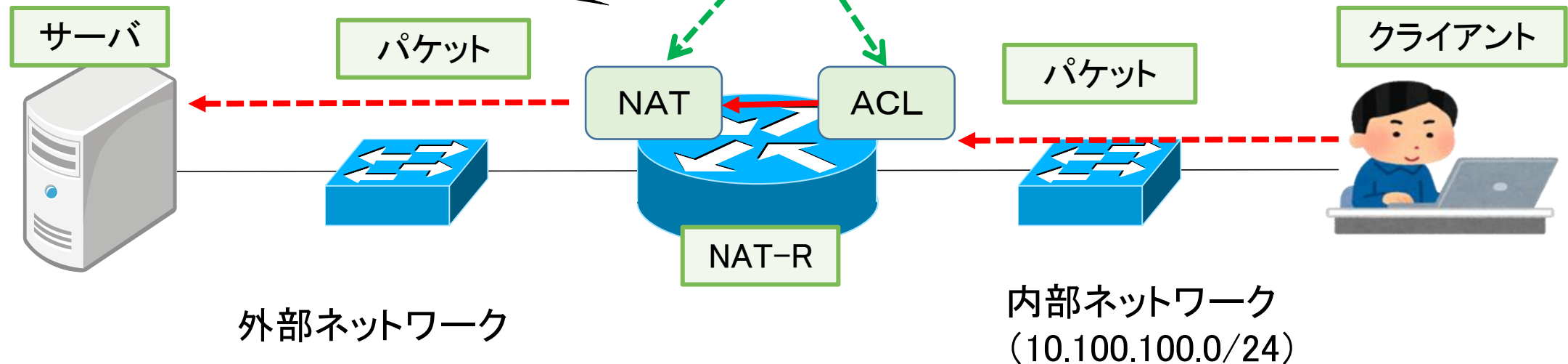
・

・

・

・

最終行: すべて拒否(暗黙の拒否)



3 NAT(IPマスカレード)の基礎

今回のNAT(PAT)ルータの設定例

```
!
interface FastEthernet0/0
  description WAN-segment
  ip address 10.10.10.1 255.255.255.0
```

NAT設定(外向け)

```
ip nat outside
```

```
duplex auto
speed auto
!
```

```
interface FastEthernet0/1
  description LAN-segment
  ip address 192.168.1.254 255.255.255.0
  ip access-group 100 in
```

NAT設定(内向け)

```
ip nat inside
```

```
duplex auto
speed auto
!
```

```
interface Vlan1
  no ip address
  shutdown
!
```

PAT設定
(ACL100をFa0/0向けに有効)

```
ip nat inside source list 100 interface FastEthernet0/0 overload
```

```
ip classless
```

```
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
```

デフォルトルート
設定

```
!
ip flow-export version 9
!
```

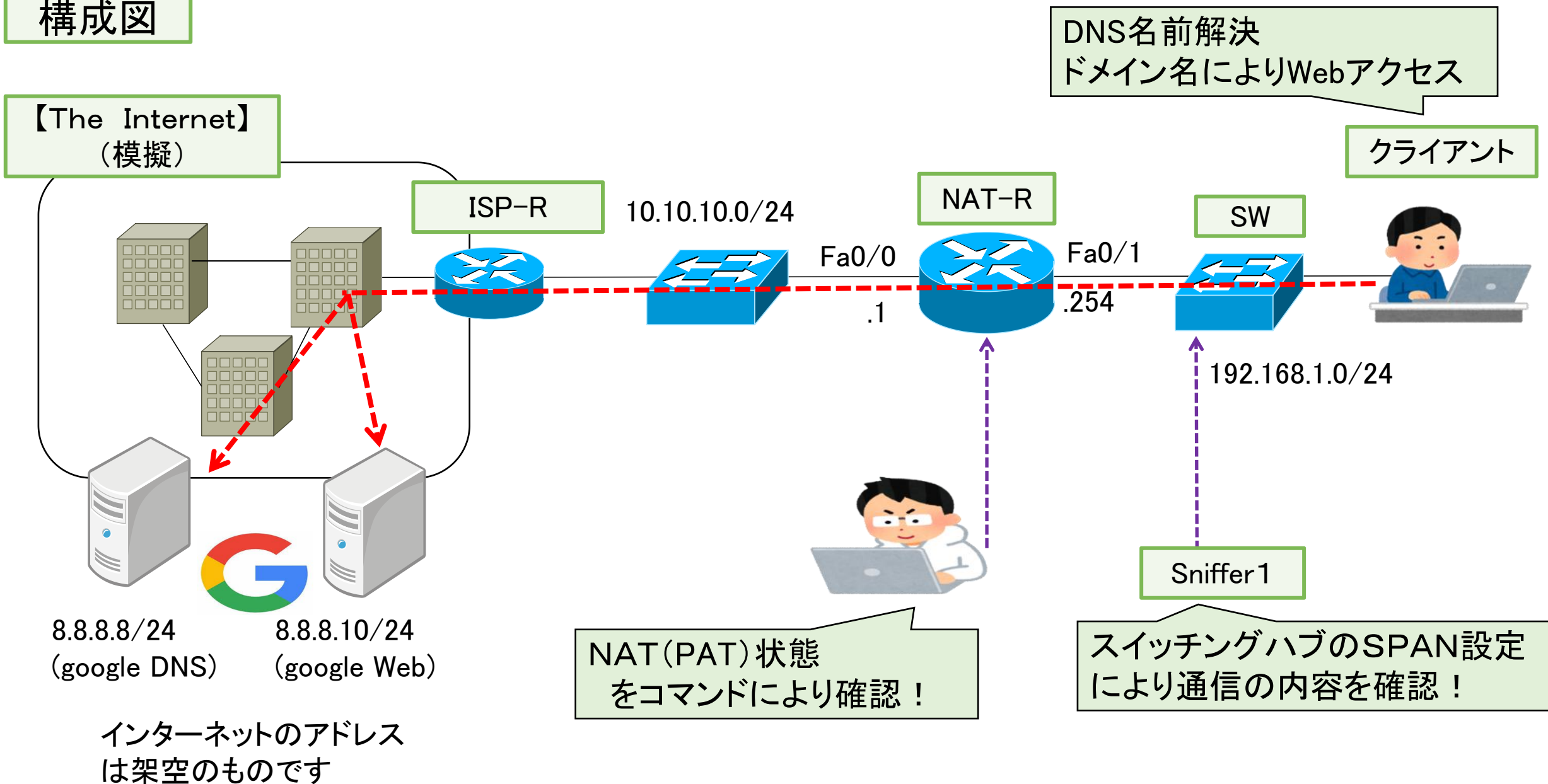
```
access-list 100 permit ip 192.168.1.0 0.0.0.255 any
!
```

ACL設定

4 NATを使用してインターネット に接続してみよう！

4 NATを使用してインターネットに接続してみよう！

構成図



4 NATを使用してインターネットに接続してみよう！

実施内容

事前準備

- ・NATルータにログインして以下のコマンドを実施しましょう！
”clear ip nat translation *” → アドレス変換テーブルをクリア
- ・NATルータにログインして以下のコマンドを実施しましょう！
”clear access-list counters” → アクセスリストカウンタをクリア

- ① クライアントからDNSサーバ及びWebサーバにpingを実施します。
- ② NATルータで ”show ip nat translation”を実施し、アドレス変換状況を確認します。
- ③ クライアントからWebサーバ(www.google.com)にWebアクセスを実施します。
- ④ NATルータで ”show ip nat translation”を実施し、アドレス変換状況を確認します。
- ⑤ NATルータで ”show access-list”を実施して、カウンタ増加を確認します

4 NATを使用してインターネットに接続してみよう！

- ④ NATルータで ”show ip nat translation” を実施し、アドレス変換状況を確認します。

”show ip nat translations” の結果

```
NAT-R#show ip nat translations
```

Pro	Inside global	Inside local
udp	10.10.10.1:1053	192.168.1.1:1053
udp	10.10.10.1:1054	192.168.1.1:1054
tcp	10.10.10.1:1067	192.168.1.1:1067

変換後のIPアドレス
(WAN)

変換前のIPアドレス
(クライアント)

宛先のIPアドレス
(DNS/Web)

Outside local	Outside global
8.8.8.8:53	8.8.8.8:53
8.8.8.8:53	8.8.8.8:53
8.8.8.10:80	8.8.8.10:80



名前解決後、Webサーバ
にアクセスしているな！！

4 NATを使用してインターネットに接続してみよう！

- ⑤ NATルータで ”show access-list”を実施して、カウンタ増加を確認します

”show access-lists” の結果

```
NAT-R#
```

```
NAT-R#show access-lists
```

```
Extended IP access list 100
```

```
10 permit ip 192.168.1.0 0.0.0.255 any (10 match(es))
```

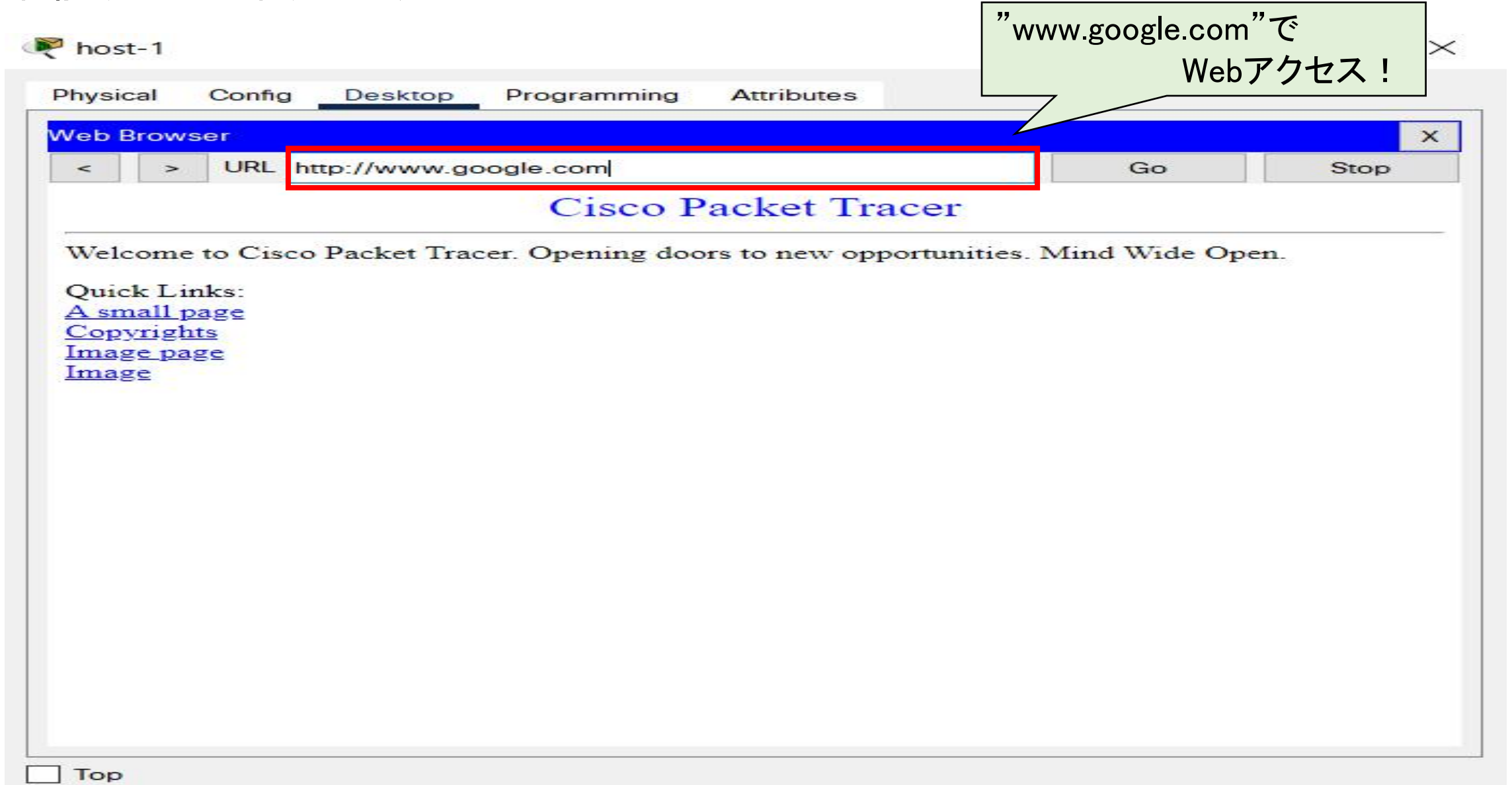
```
NAT-R#
```



該当のNWからパケットが
来ているな～

4 NATを使用してインターネットに接続してみよう！

- 名前(ドメイン名)によりWebサーバにアクセス



4 NATを使用してインターネットに接続してみよう！

- Nslookupコマンドによる名前解決の確認

```
C:\>nslookup
```

```
Server: [8.8.8.8]  
Address: 8.8.8.8
```

```
>www.google.com
```

問い合わせたいドメイン名

```
Server: [8.8.8.8]  
Address: 8.8.8.8
```

```
Non-authoritative answer:  
Name: www.google.com  
Address: 8.8.8.10
```

DNSサーバからの回答

```
>exit  
C:\>
```

5 (参考)DNSサーバの設定

5 (参考)DNSサーバの設定

- DNSサービスをONにしてAレコードに "www.google.com" を追加

The screenshot shows the 'DNSサーバ' (DNS Server) configuration window. The 'Services' tab is selected, and the 'DNS' service is highlighted in the left sidebar. In the main panel, the 'DNS Service' is set to 'On'. Below this, the 'Resource Records' section shows an 'A Record' for 'www.google.com' with the address '8.8.8.10'. A 'DNS Cache' button is visible at the bottom.

DNSサーバ

Physical Config **Services** Desktop

SERVICES

- HTTP
- DHCP
- DHCPv6
- TFTP
- DNS**
- SYSLOG
- AAA
- NTP
- EMAIL
- FTP
- IoT
- VM Management
- Radius EAP

DNS Service ☒ On ☐ Off

Resource Records

Name Type A Record

Address

Add Save Remove

No.	Name	Type	Detail
0	www.google.com	A Record	8.8.8.10

DNS Cache

☐ Top

DNSサービスをON

Aレコードを登録