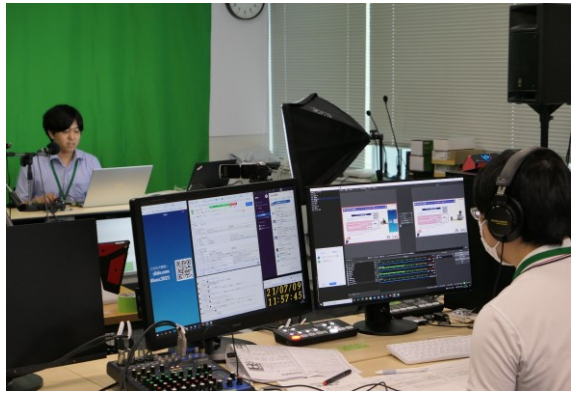
ROVで経路をCHANGE
~10分くらいで魅せるROVの効果 ~

JPNIC　塩沢啓

自己紹介

- **名前：塩沢　啓**
- **所属：JPNIC**
- **普段の業務：インターネット推進部・技術部**
  - DNS, BGP触ったり
  - セミナー/イベントの企画運営
    - 最近はオンライン化で配信なども

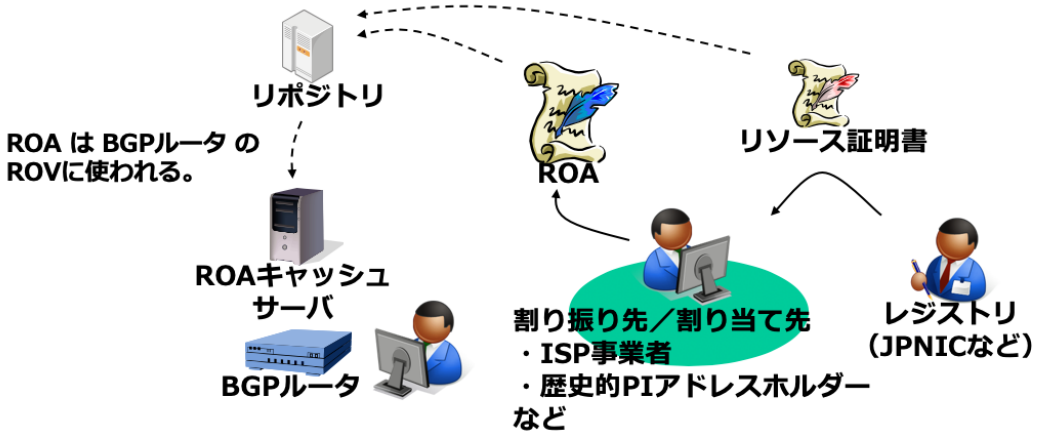


目次

- **RPKI、ROA、ROVとは**
- **模擬環境でROVを試してみます**
  - 今回、偽のWebサイトに誘導させるため、不正な経路を流してみます
  - ROVで不正な経路を検出して正しいWebサイトにアクセスできるようにしてみます
- **ROVの効果を体験**
  - SETP 1　通常の状態
  - STEP 2　不正な経路で偽のWebサイトに誘導
  - STEP 3　ROV (Route Origin Validation)の効果を体験

RPKI, ROA, ROV

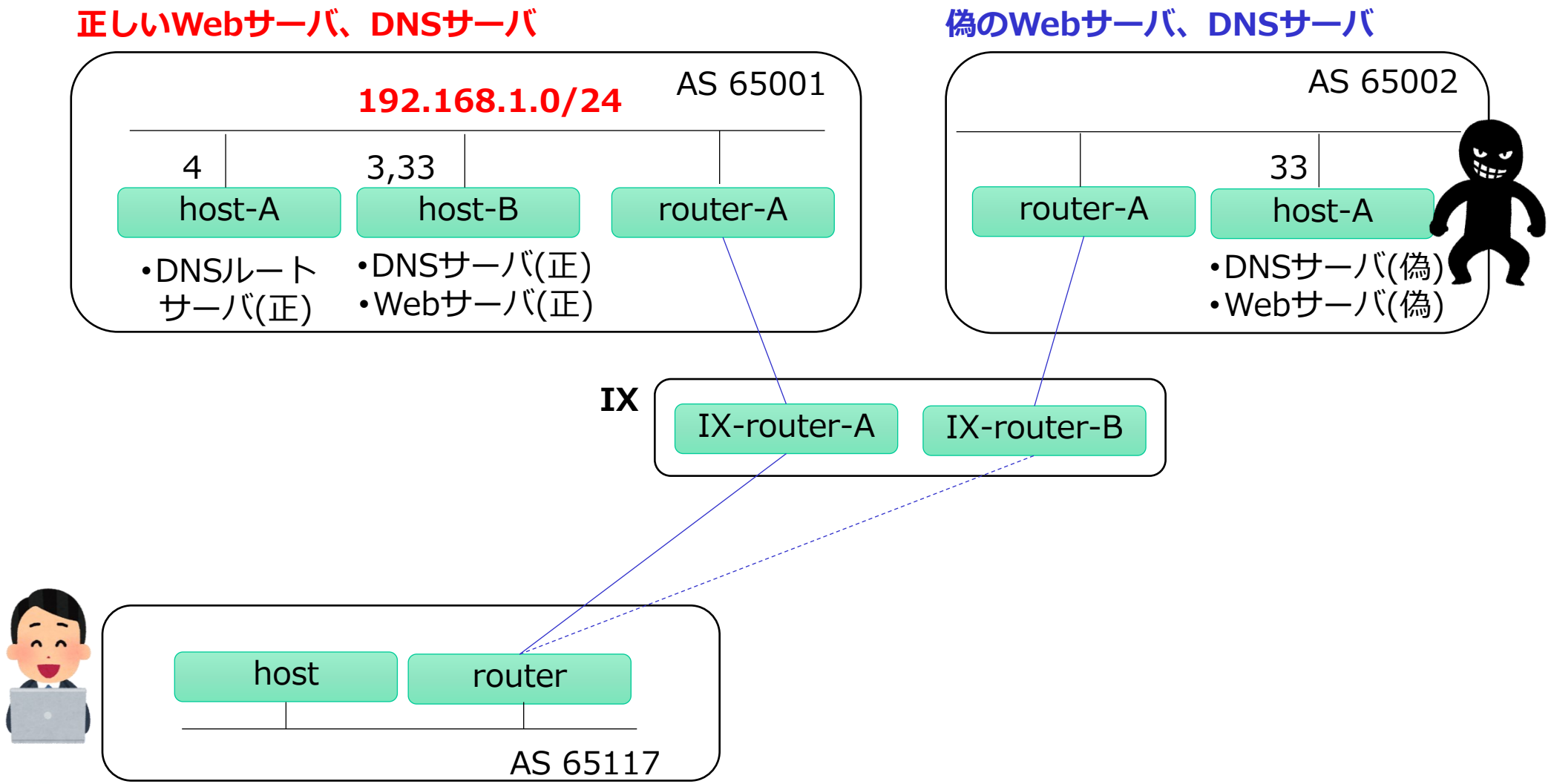
- **RPKI（Resource Public-Key Infrastructure）**
  - IPアドレスやAS番号といった番号資源の割り振り／割り当てを証明するPKI



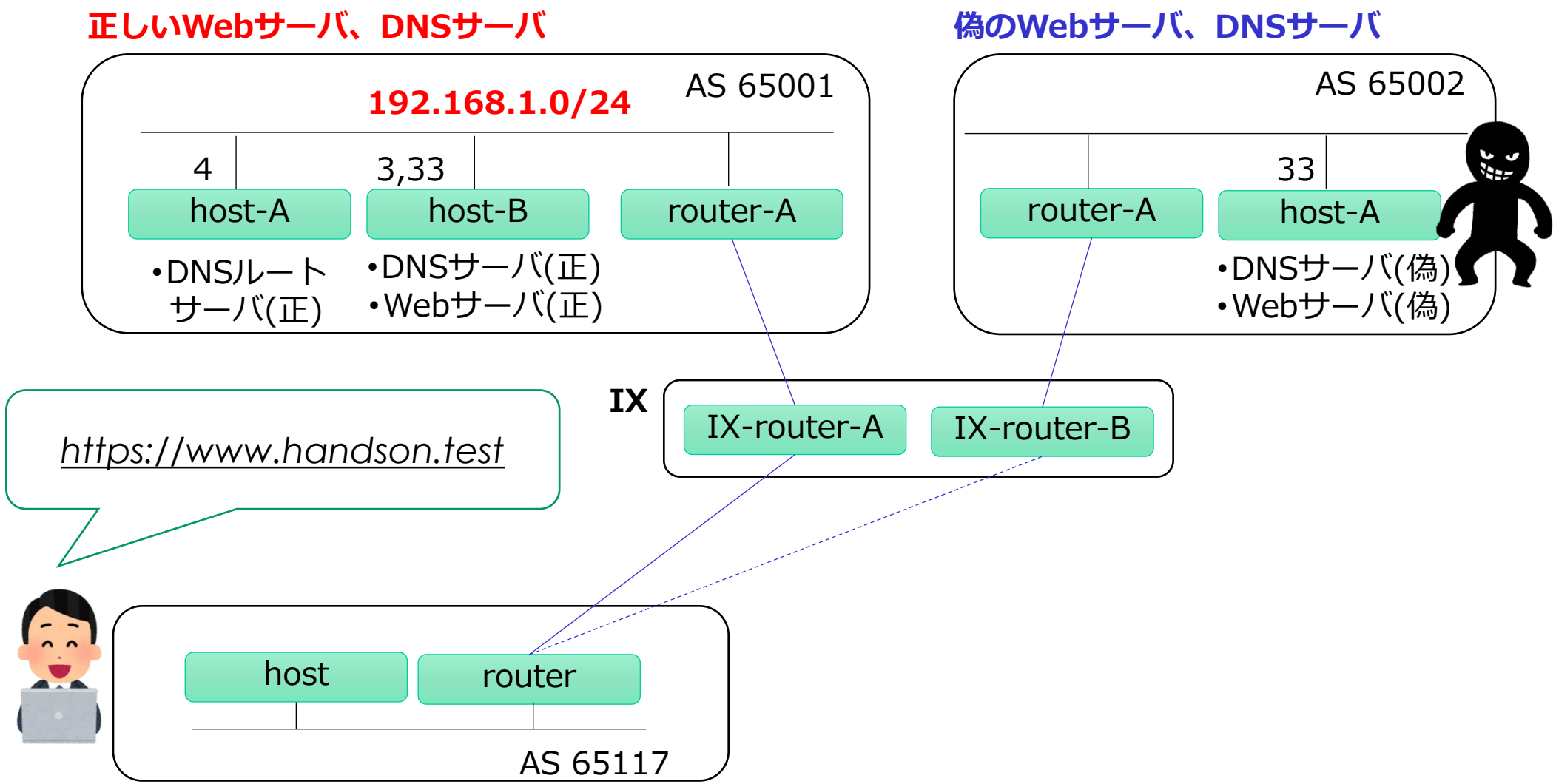
- **ROA (Route Origination Authorization)**
  - IPアドレスとそれを広報するAS番号の組み合わせに対して、 それが正しい組み合わせであることを示す電子署名が施されたデータ

- **ROV (Route Origin Validation)**
  - 経路情報中のIPアドレスとAS番号の組み合わせが正しいかどうかをROAに基づいてBGPルータで検証する仕組み

模擬環境



SETP 1　通常の状態

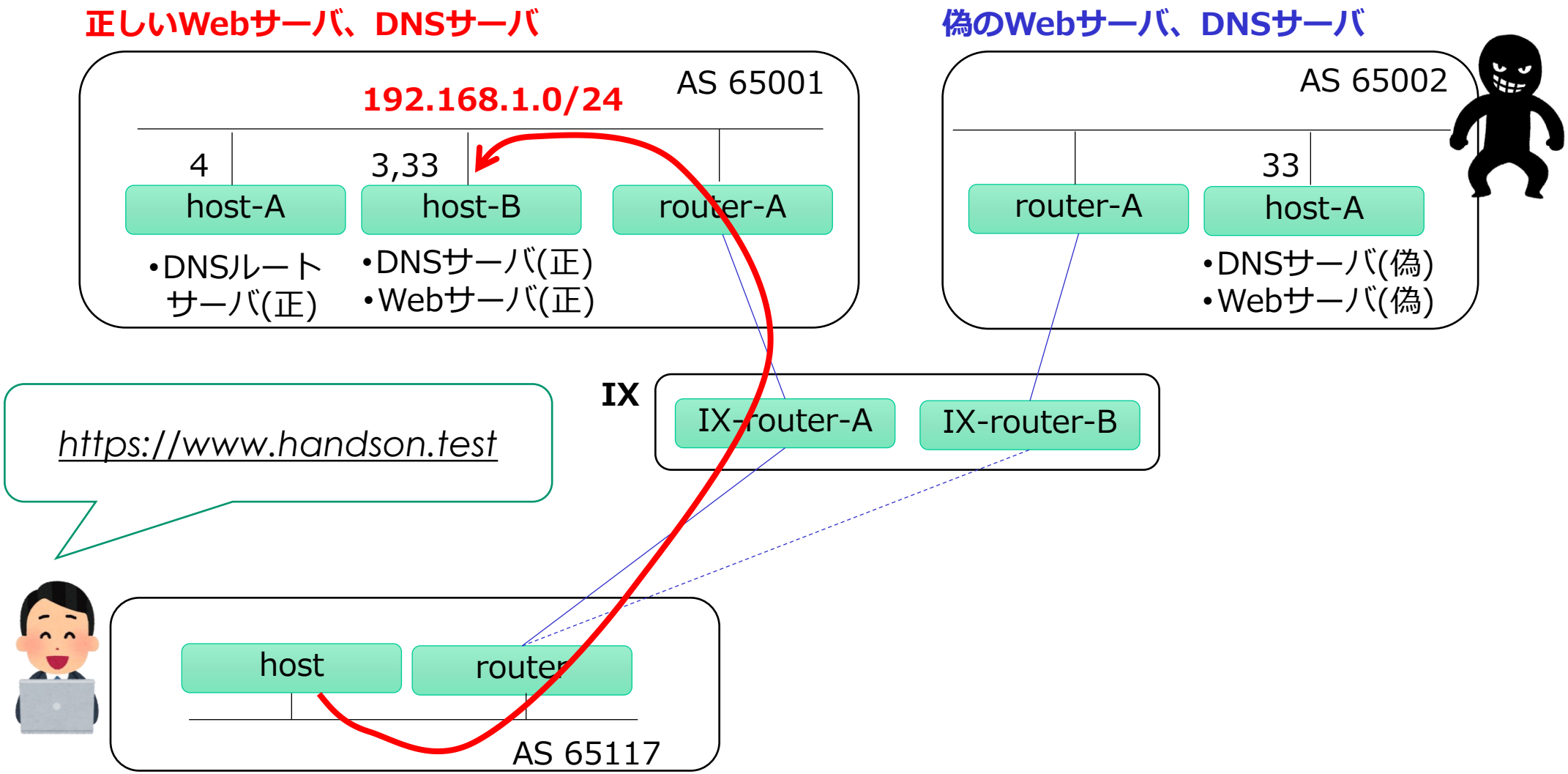


SETP 1　通常の状態

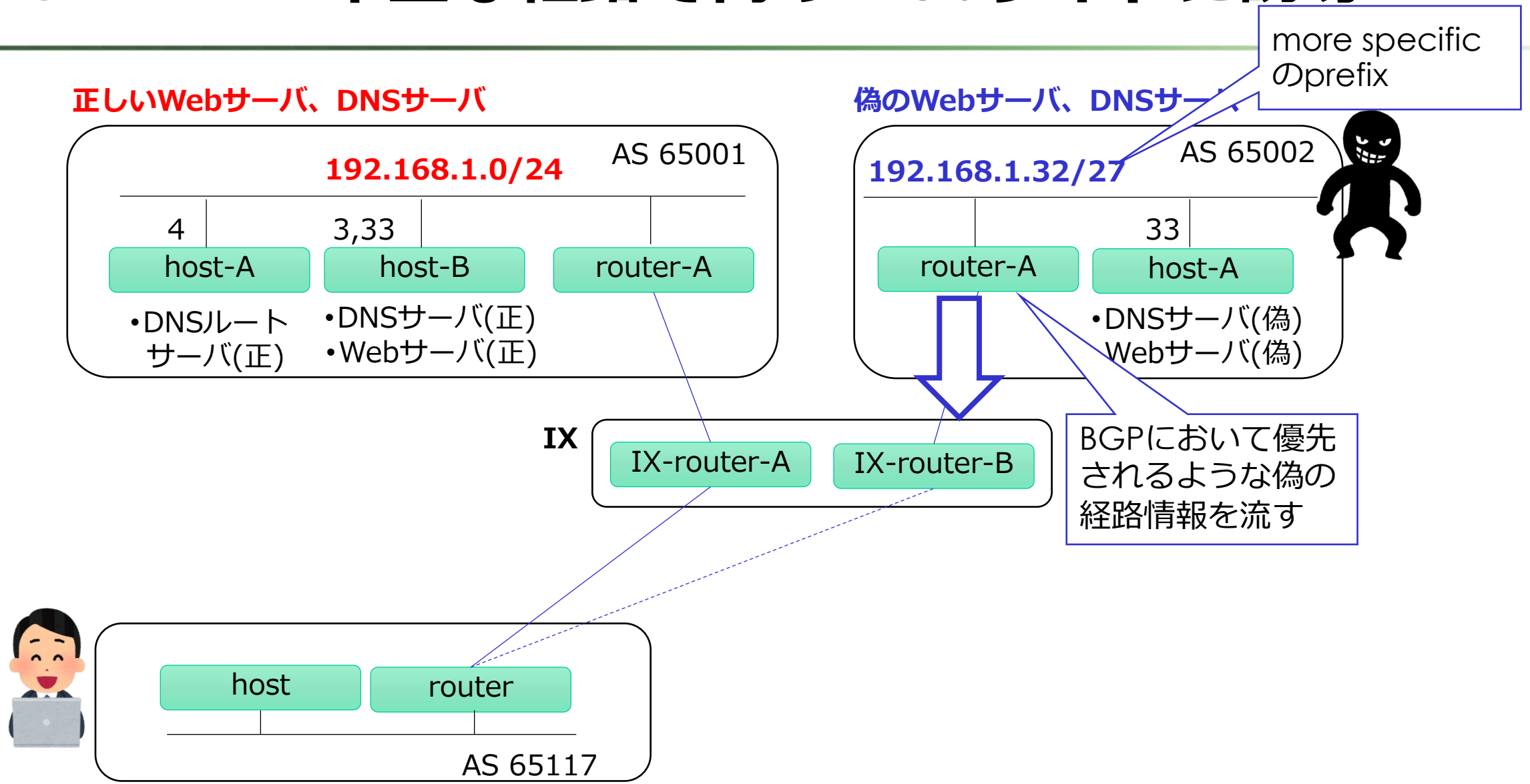
正しいWebサーバ、DNSサーバ

偽のWebサーバ、DNSサーバ

SETP 1　通常の状態



STEP 2　不正な経路で偽のWebサイトに誘導



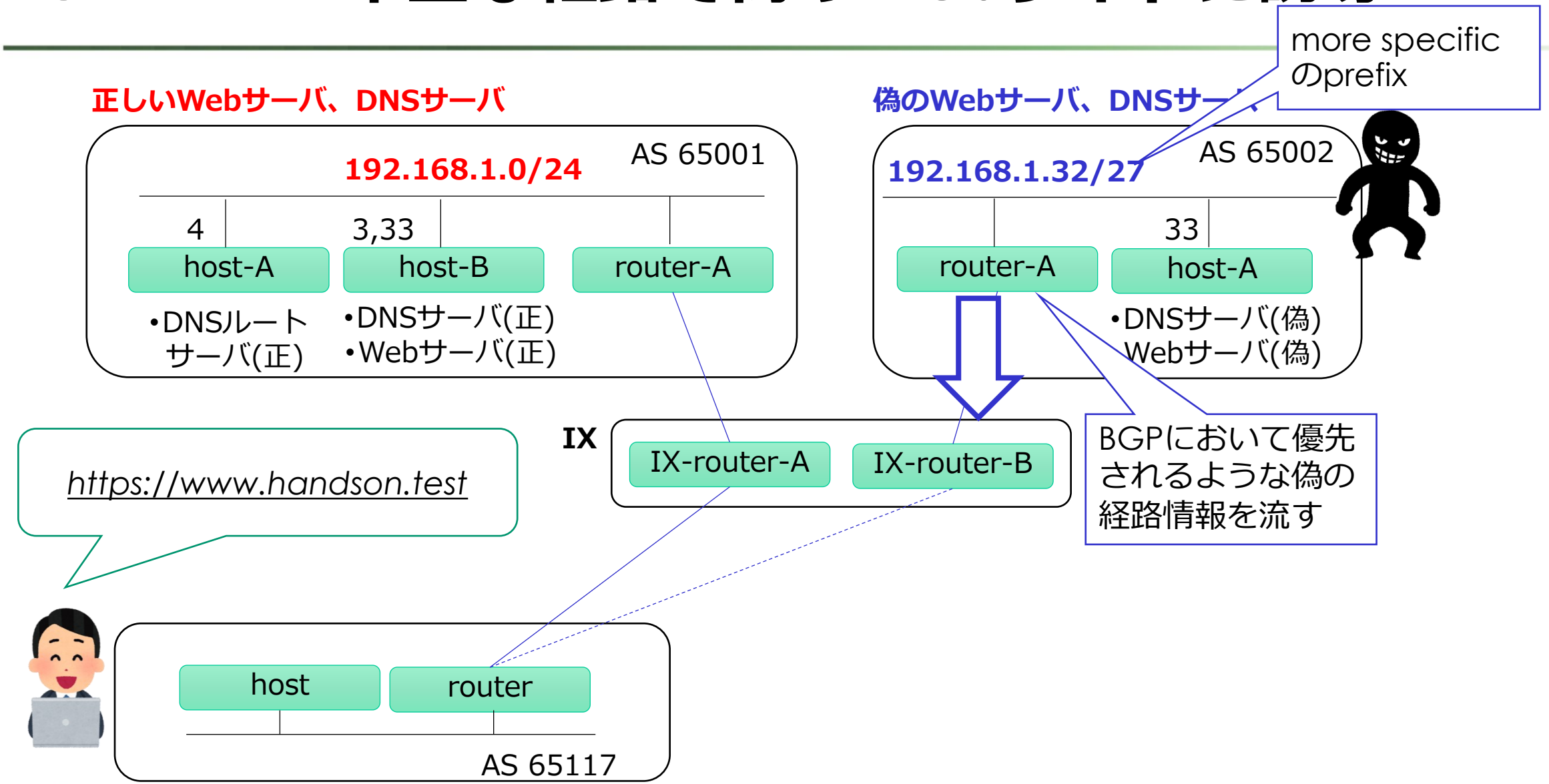
STEP 2　不正な経路で偽のWebサイトに誘導

more specific
fix

正

```
[hiromu@handson-island ~]$ ssh vyos@k2-router1
Welcome to VyOS
vyos@k2-router1's password:

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Jul 14 22:21:34 2022 from 172.16.11.1
vyos@k2-router1:~$
vyos@k2-router1:~$
vyos@k2-router1:~$ conf
[edit]
vyos@k2-router1#  set protocols bgp 65002 address-family ipv4-unicast network 192.168.1.32/27
[edit]
vyos@k2-router1#
```

STEP 2　不正な経路で偽のWebサイトに誘導



STEP 2　不正な経路で偽のWebサイトに誘導

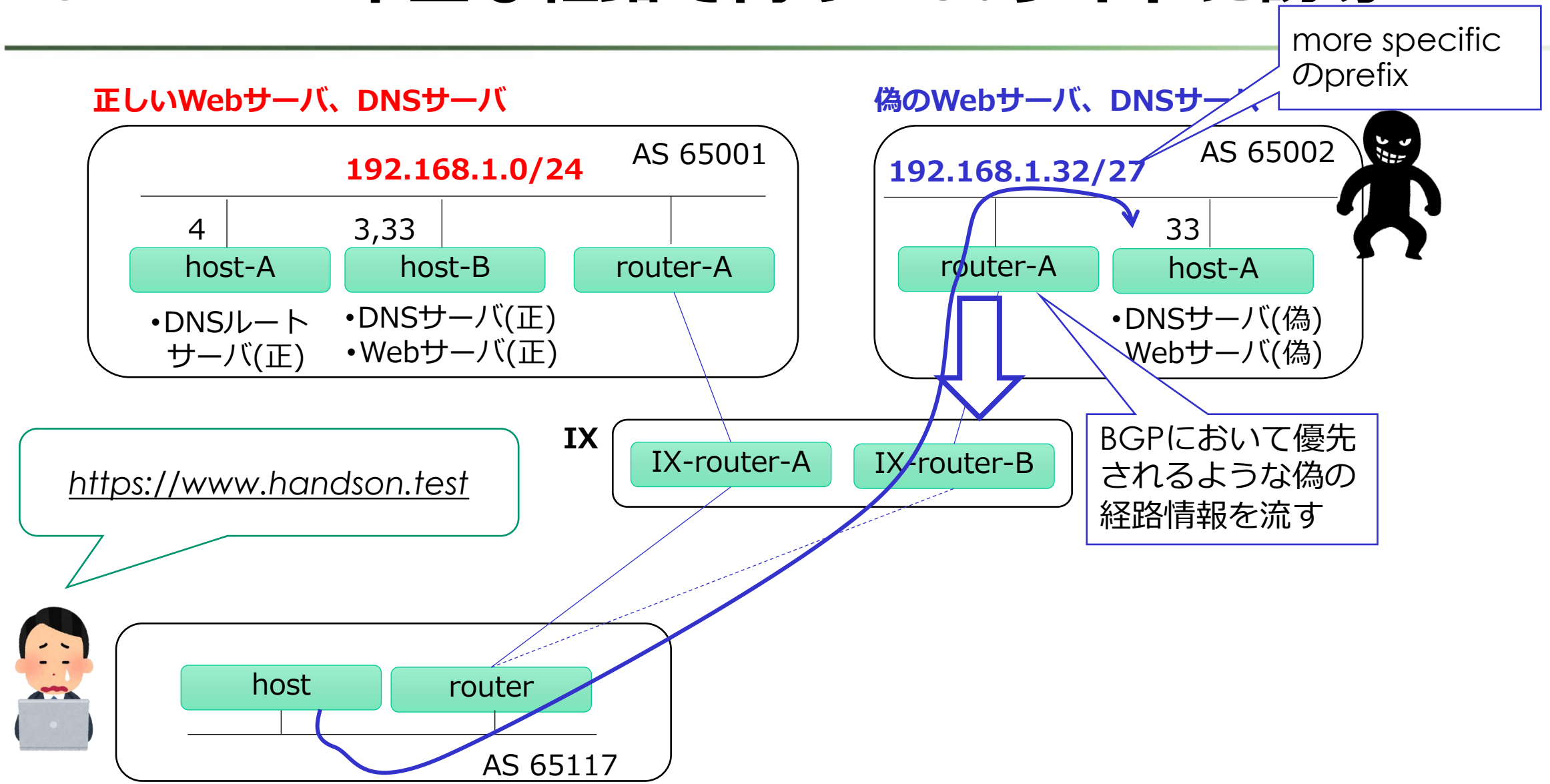
more specific
prefix

正しい

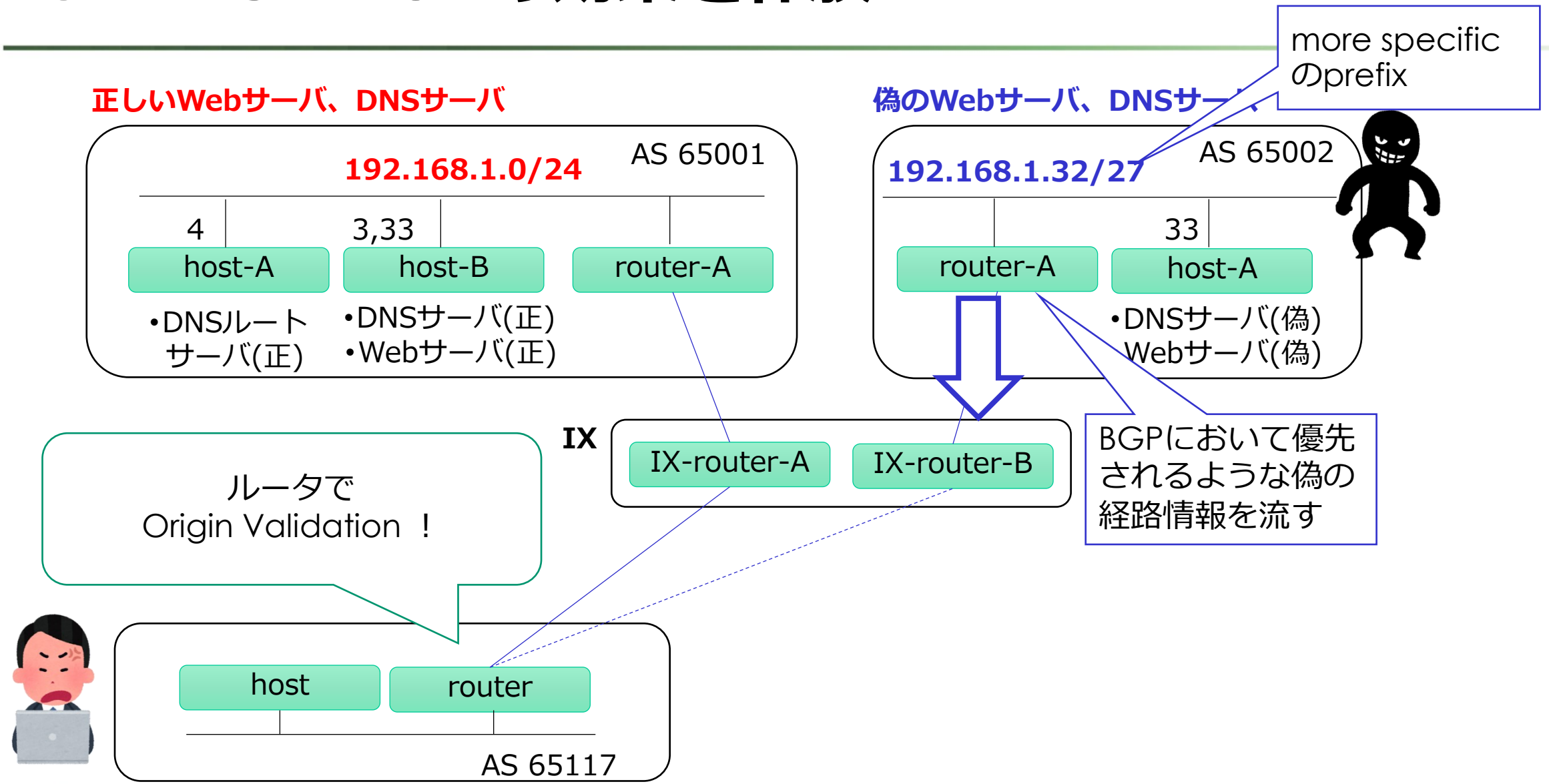
https:/

```
</html>

user-p@host117:~$  curl https://www.handson.test/
<!DOCTYPE html>
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <title>B4 fake</title>
</head>

<body> <pre>

 ######    ##    #    #  ######          ######    ##    #    #  ######
 #        #  #   #   #   #               #        #  #   #   #   #
 #####   #    #  ####    #####           #####   #    #  ####    #####
 #       ######  #  #    #               #       ######  #  #    #
 #       #    #  #   #   #               #       #    #  #   #   #
 #       #    #  #    #  ######          #       #    #  #    #  ######

</pre> </body>

</html>

user-p@host117:~$
```

STEP 2　不正な経路で偽のWebサイトに誘導



STEP 3　ROVの効果を体験

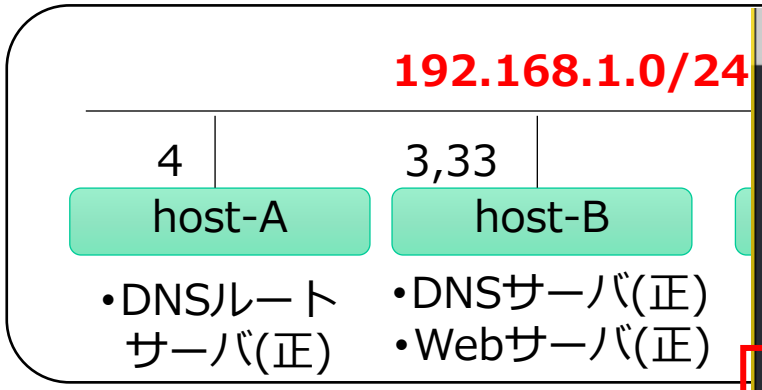


STEP 3　ROVの効果を体験

正しいWebサーバ、DNSサーバ

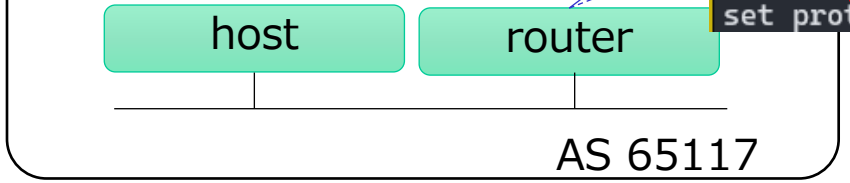
偽のWebサーバ、DNSサーバ

more specific のprefix



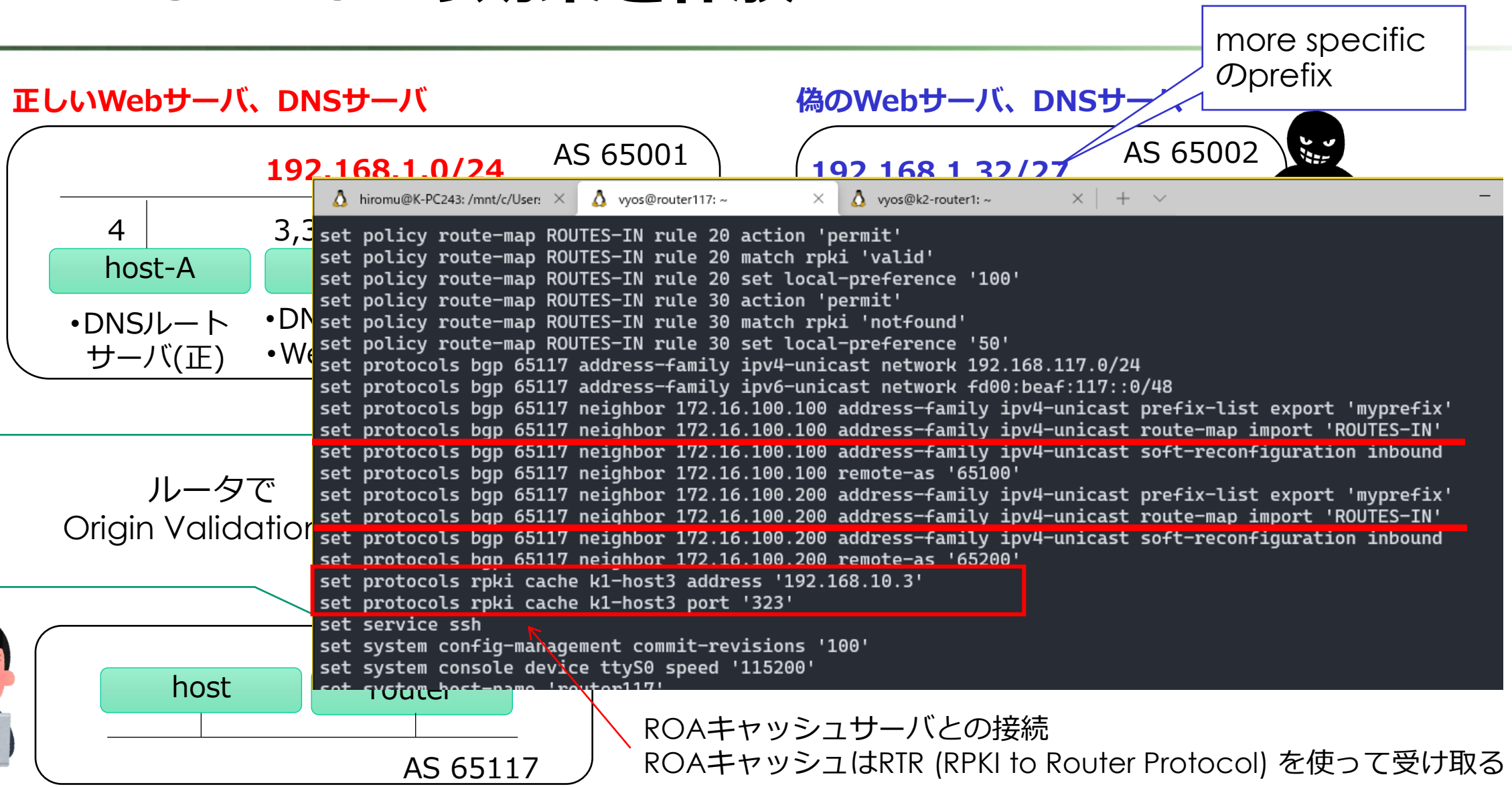

```
hiromu@K-PC243: /mnt/c/User:   vyos@router117: ~   vyos@k2-router1: ~
set interfaces ethernet eth0 hw-id '00:0c:29:42:e9:de'
set interfaces ethernet eth1 address '192.168.117.1/24'
set interfaces ethernet eth1 hw-id '00:0c:29:42:e9:e8'
set interfaces ethernet eth2 address '172.16.1.117/24'
set interfaces ethernet eth2 hw-id '00:0c:29:42:e9:f2'
set interfaces loopback lo
set policy prefix-list myprefix rule 10 action 'permit'
set policy prefix-list myprefix rule 10 prefix '192.168.117.0/24'
set policy route-map ROUTES-IN rule 10 action 'deny'
set policy route-map ROUTES-IN rule 10 match rpki 'invalid'
set policy route-map ROUTES-IN rule 20 action 'permit'
set policy route-map ROUTES-IN rule 20 match rpki 'valid'
set policy route-map ROUTES-IN rule 20 set local-preference '100'
set policy route-map ROUTES-IN rule 30 action 'permit'
set policy route-map ROUTES-IN rule 30 match rpki 'notfound'
set policy route-map ROUTES-IN rule 30 set local-preference '50'
set protocols bgp 65117 address-family ipv4-unicast network 192.168.117.0/24
set protocols bgp 65117 address-family ipv6-unicast network fd00:beaf:117::0/48
set protocols bgp 65117 neighbor 172.16.100.100 address-family ipv4-unicast prefix
set protocols bgp 65117 neighbor 172.16.100.100 address-family ipv4-unicast route-
set protocols bgp 65117 neighbor 172.16.100.100 address-family ipv4-unicast soft-r
set protocols bgp 65117 neighbor 172.16.100.100 remote-as '65100'
```

ルータで
Origin Validation ！

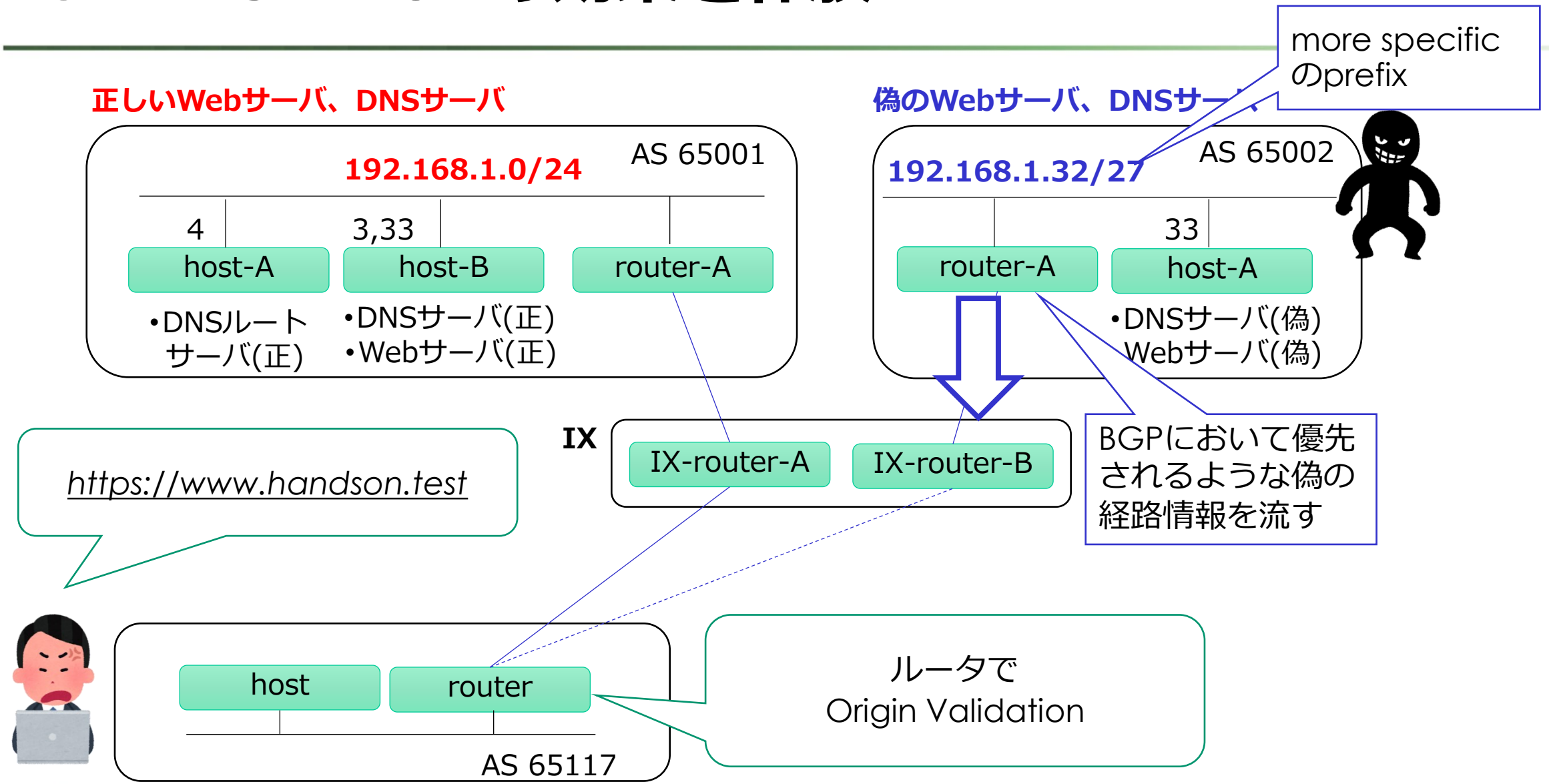


RPKIでinvalidになった経路＝Prefixが一致するROAが存在するがOriginASが異なる場合＝そのprefixが不当なASから経路広報されている場合は deny

STEP 3　ROVの効果を体験



STEP 3　ROVの効果を体験



STEP 3　不正な経路で偽のWebサイトに誘導

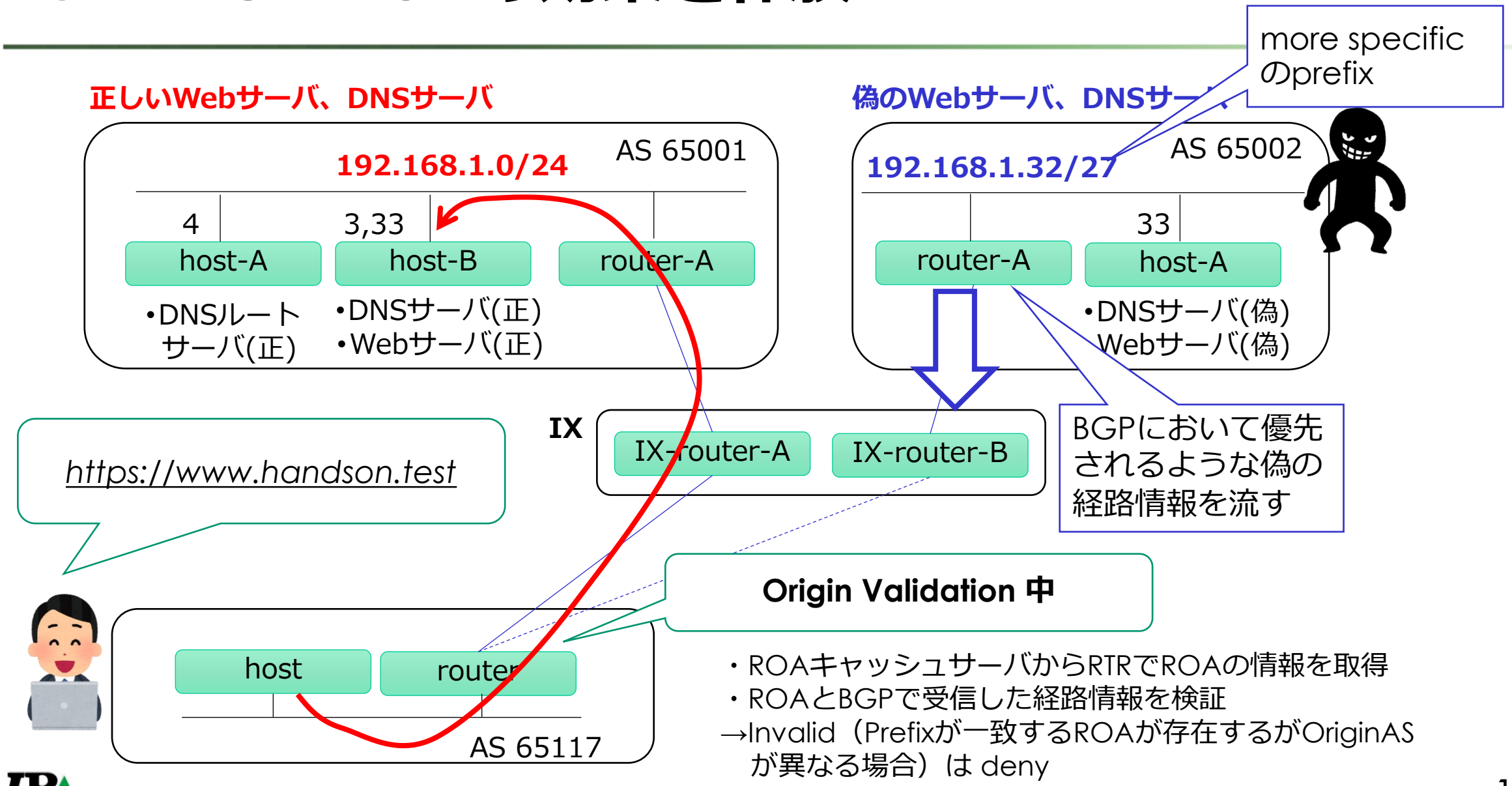
more specific
Prefix

正しいW

```
<head>
  <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
  <title>B4 real</title>
</head>

<body> <pre>

 #####   ######    ##    #                ####      #     #####  ######
 #    #  #        #  #   #               #          #       #    #
 #    #  #####   #    #  #                ####      #       #    #####
 #####   #       ######  #                    #     #       #    #
 #   #   #       #    #  #               #    #     #       #    #
 #    #  ######  #    #  ######           ####      #       #    ######

  /\_/\
 ( o.o )
  &gt; ^ &lt;

</pre> </body>

</html>

user-p@host117:~$
```

https://v

STEP 3　ROVの効果を体験



以上、簡単ですが、

ROVの効果～不正な経路をCHANGE～

でした