

# パケットトレーサで学ぶNW構築 (基礎編)

⑤

総合実習  
(解説編)



# 本資料の位置付け

本資料はパケットレーサで学ぶNW構築(基礎編)の総合実習における構成及び設定及び機能確認の一例を提示するものです

- 1 構成図
- 2 構成条件
- 3 構成後の機能確認
  - (提供サービスの機能確認)
  - (監視条件)
  - (回線条件)
- 4 参考資料
  - (1) インタフェースモジュールの追加例
  - (2) VLANの作成及びIPアドレスの付与要領
  - (3) Netflowによるトラヒックの確認
  - (4) ルータへのSSH設定及び確認

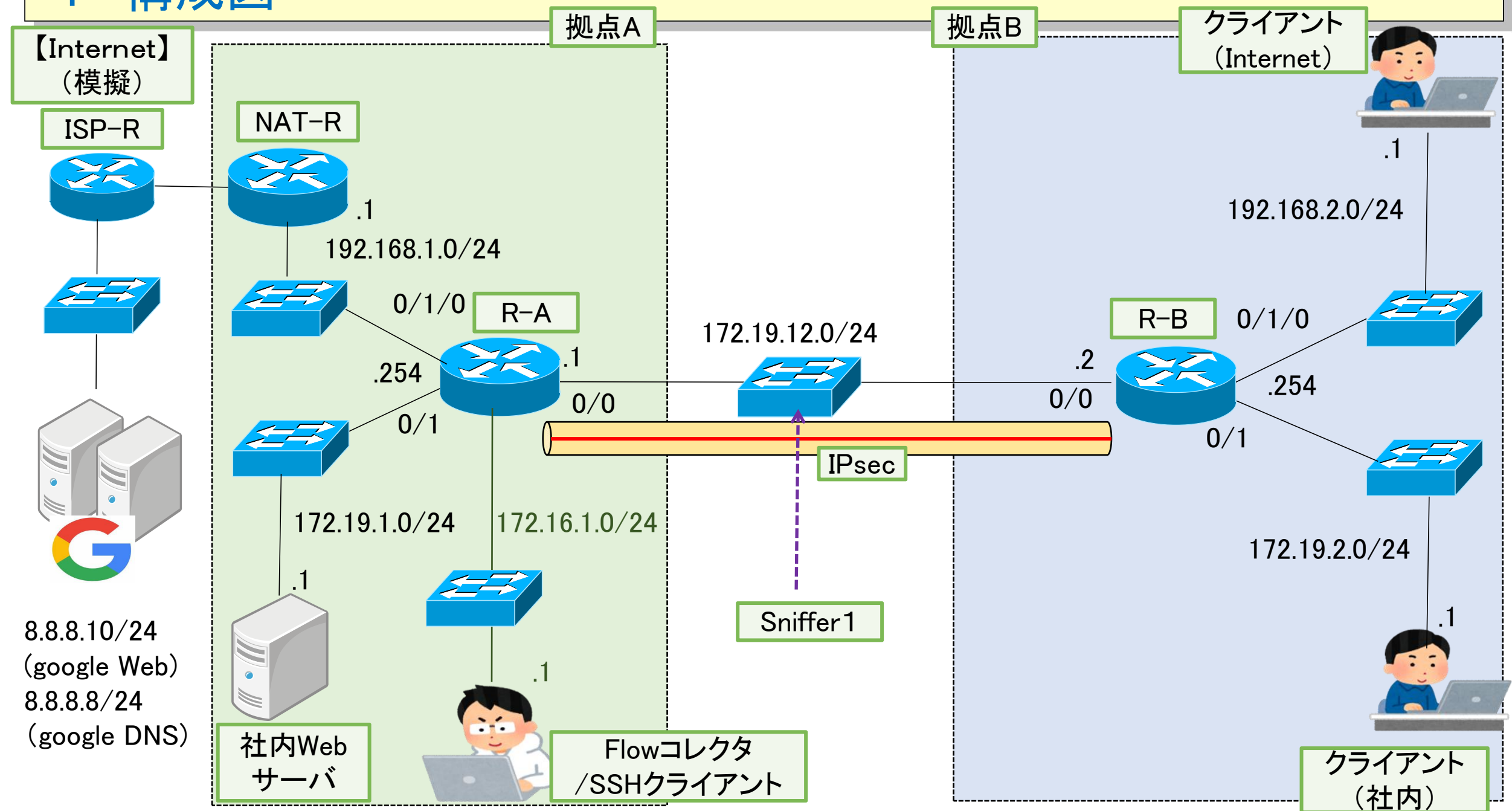
前回の資料からの追加分は紫色で示している項目になります！

サンプルpktファイルについては "sougou-1-mihon.pkt"になります

1

構成図

# 1 構成図



## 2 構成条件

## 2 構成条件

### (提供サービス)

拠点A～拠点B間において以下のサービスを提供する

- ① 拠点Bクライアント→拠点Aサーバに対するWebアクセス
- ② 拠点Bクライアント→拠点AのNAT-R経由によるインターネットアクセス

### (監視条件)

拠点Aの保守端末は以下の機能を具備します。

各NW機器に対するSSHアクセス

Netflowによるトラフィック確認

### (回線条件)

拠点A～拠点BにおいてはVPNルータにより秘匿(IPSEC)を実施

＜秘匿対象は全サービスとする＞

### (構成及び使用アドレス)

- 1 構成図のとおり

### 3 構成後の確認

### 3 構成後の機能確認

(提供サービスの機能確認)

拠点A～拠点B間において以下のサービスが提供できるかを確認してください

- ① 拠点Bクライアント→拠点Aサーバに対するWebアクセス
- ② 拠点Bクライアント→拠点AのNAT-R経由によるインターネットアクセス

(監視条件の機能確認)

拠点Aの保守端末から以下の動作が可能かを確認してください。

各NW機器に対するSSHアクセス

Netflowによるトラフィック確認

(回線条件の機能確認)

拠点間VPNルータにより秘匿(IPSEC)できているかを以下の方法で確認してください

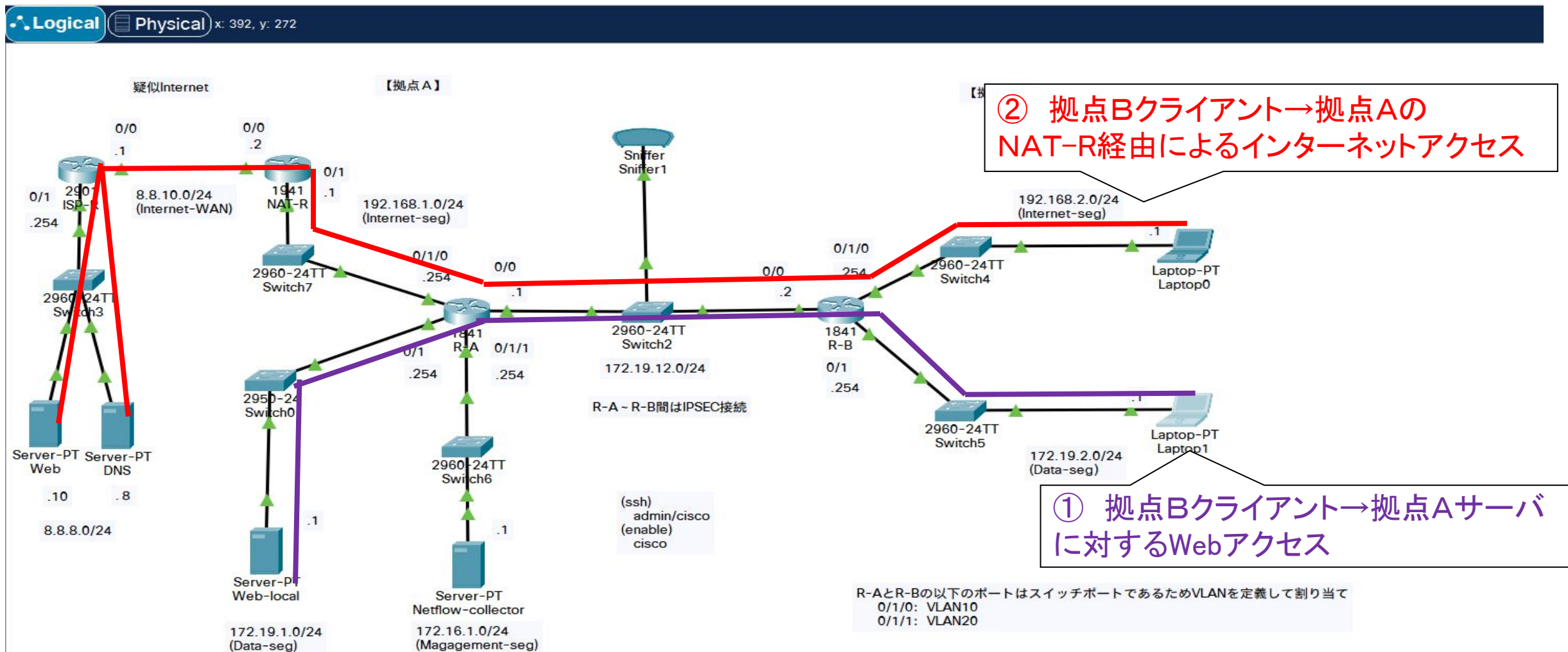
- ・ルータのIPSEC関連コマンドおよびアクセスリスト(カウンタ)での確認
- ・Snifer0による各提供サービスのトラフィックが秘匿(ESP)されているか？



# 3 構成後の確認

(提供サービスの機能確認)

拠点A～拠点B間において以下のサービスが提供できるかを確認してください



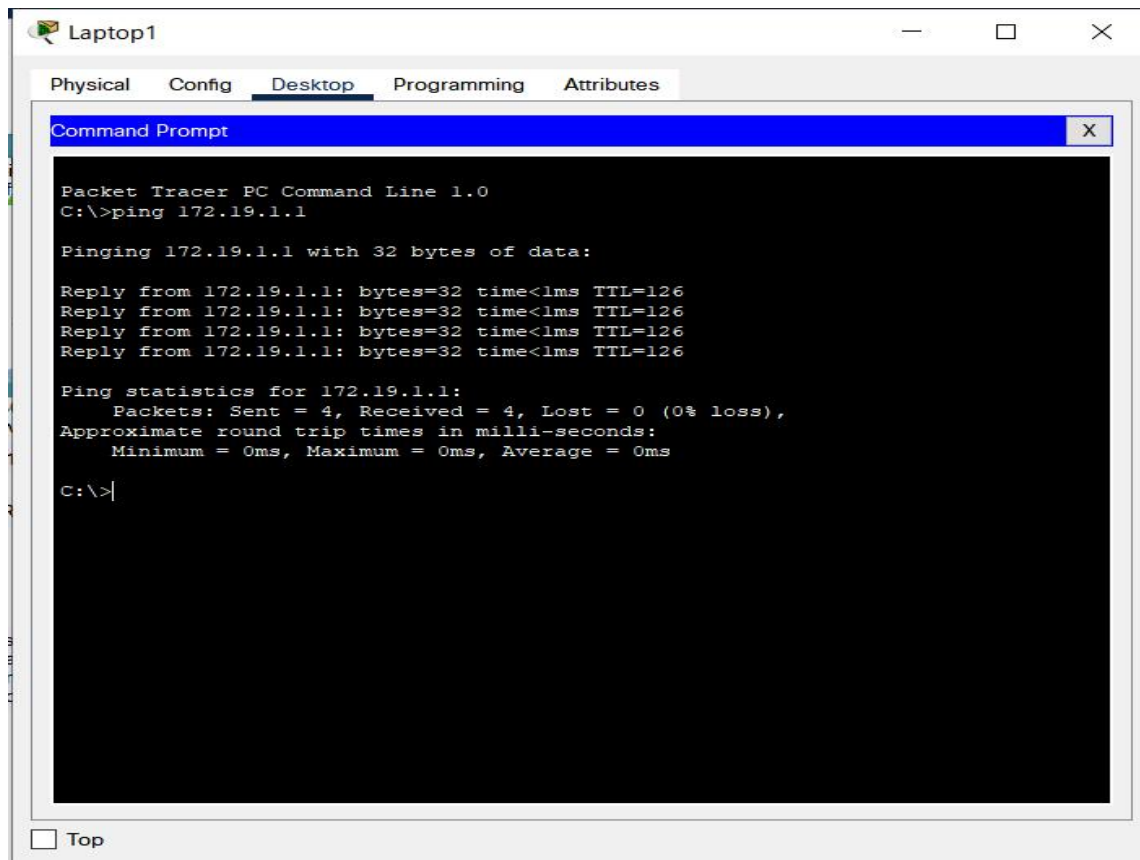
### 3 構成後の機能確認

(提供サービスの機能確認)

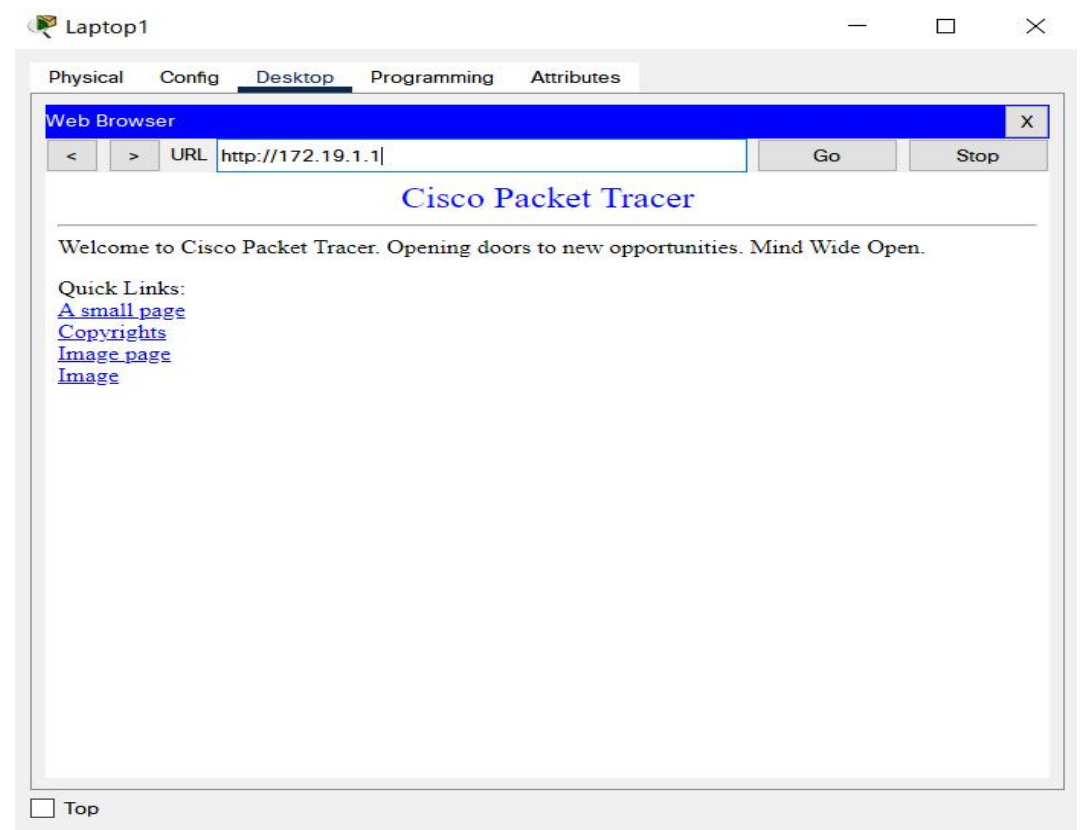
① 拠点Bクライアント→拠点Aサーバに対するWebアクセス

クライアント  
(社内)

【クライアントからWebサーバへのPING】



【クライアントからWebサーバにWebアクセス】



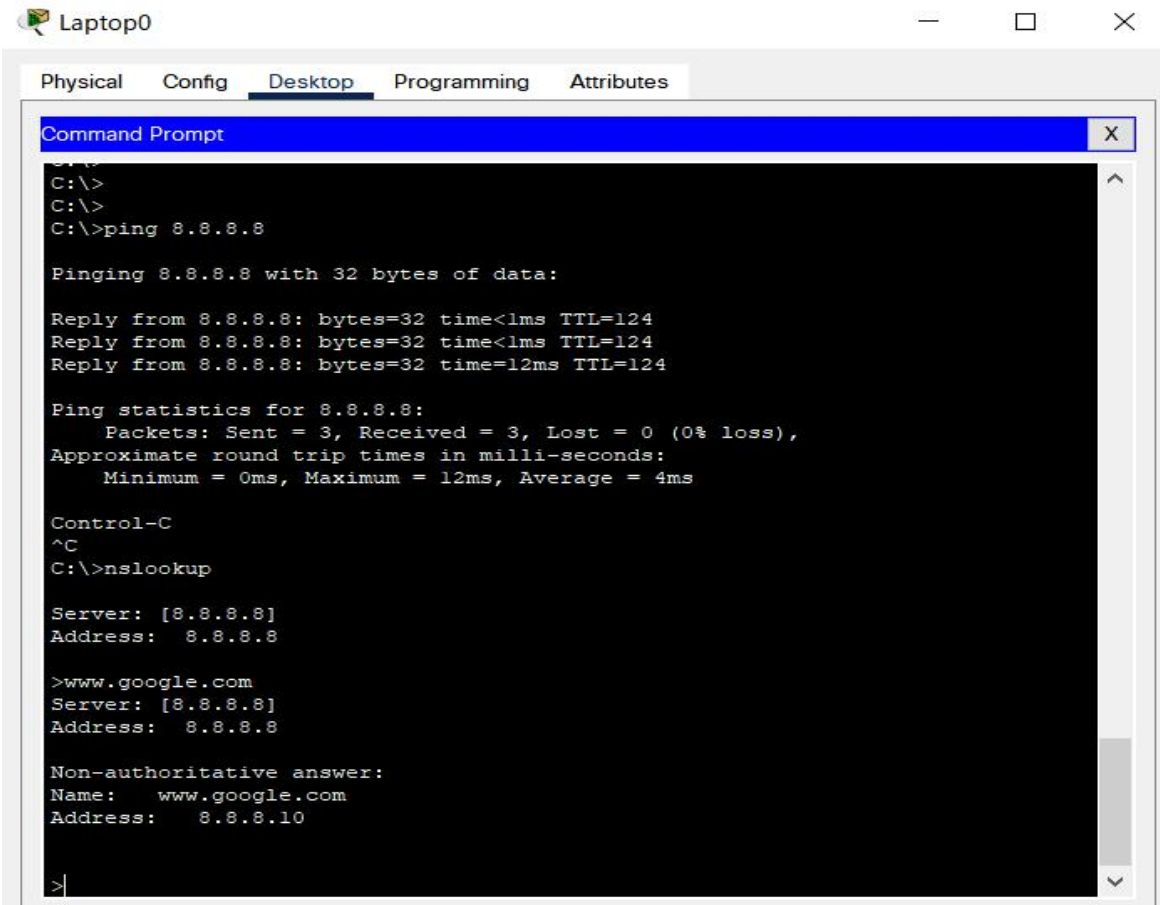
### 3 構成後の機能確認

(提供サービスの機能確認)

② 拠点Bクライアント→拠点AのNAT-R経由によるインターネットアクセス

拠点Bクライアント  
(Internet)

【DNSサーバへのPING及び名前解決】



```
Laptop0
Physical Config Desktop Programming Attributes
Command Prompt
C:\>
C:\>
C:\>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:

Reply from 8.8.8.8: bytes=32 time<1ms TTL=124
Reply from 8.8.8.8: bytes=32 time<1ms TTL=124
Reply from 8.8.8.8: bytes=32 time=12ms TTL=124

Ping statistics for 8.8.8.8:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 12ms, Average = 4ms

Control-C
^C
C:\>nslookup

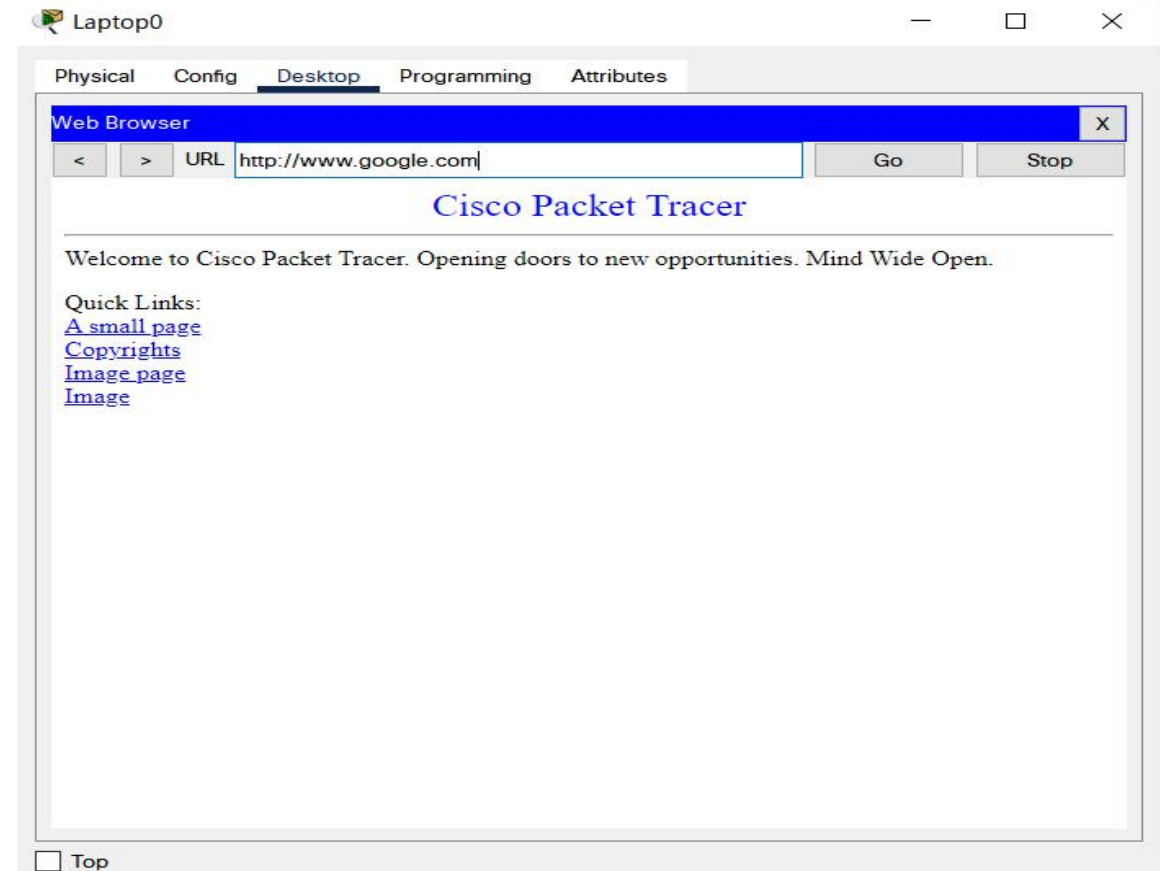
Server: [8.8.8.8]
Address: 8.8.8.8

>www.google.com
Server: [8.8.8.8]
Address: 8.8.8.8

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

>
```

【クライアントからWebアクセス】



### 3 構成後の機能確認

(提供サービスの機能確認)

#### ② 拠点Bクライアント→拠点AのNAT-R経由によるインターネットアクセス

【NAT-Rによるアドレス変換状況の確認】

“show ip nat translations” による確認

NAT-R

Physical Config CLI Attributes

IOS Command Line Interface

```
Processor board ID FTX152400KS
2 Gigabit Ethernet interfaces
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
249856K bytes of ATA System CompactFlash 0 (Read/Write)

Press RETURN to get started!

%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/1, changed
state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/0, changed
state to up

NAT-R>en
Password:
Password:
NAT-R#show ip nat tra
NAT-R#show ip nat translations
NAT-R#show ip nat translations
Pro  Inside global      Inside local      Outside local     Outside global
udp  8.8.10.2:1027        192.168.2.1:1027  8.8.8.8:53        8.8.8.8:53
udp  8.8.10.2:1028        192.168.2.1:1028  8.8.8.8:53        8.8.8.8:53
udp  8.8.10.2:1029        192.168.2.1:1029  8.8.8.8:53        8.8.8.8:53
udp  8.8.10.2:1030        192.168.2.1:1030  8.8.8.8:53        8.8.8.8:53
tcp  8.8.10.2:1025        192.168.2.1:1025  8.8.8.10:80       8.8.8.10:80

NAT-R#
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

# 3 構成後の確認

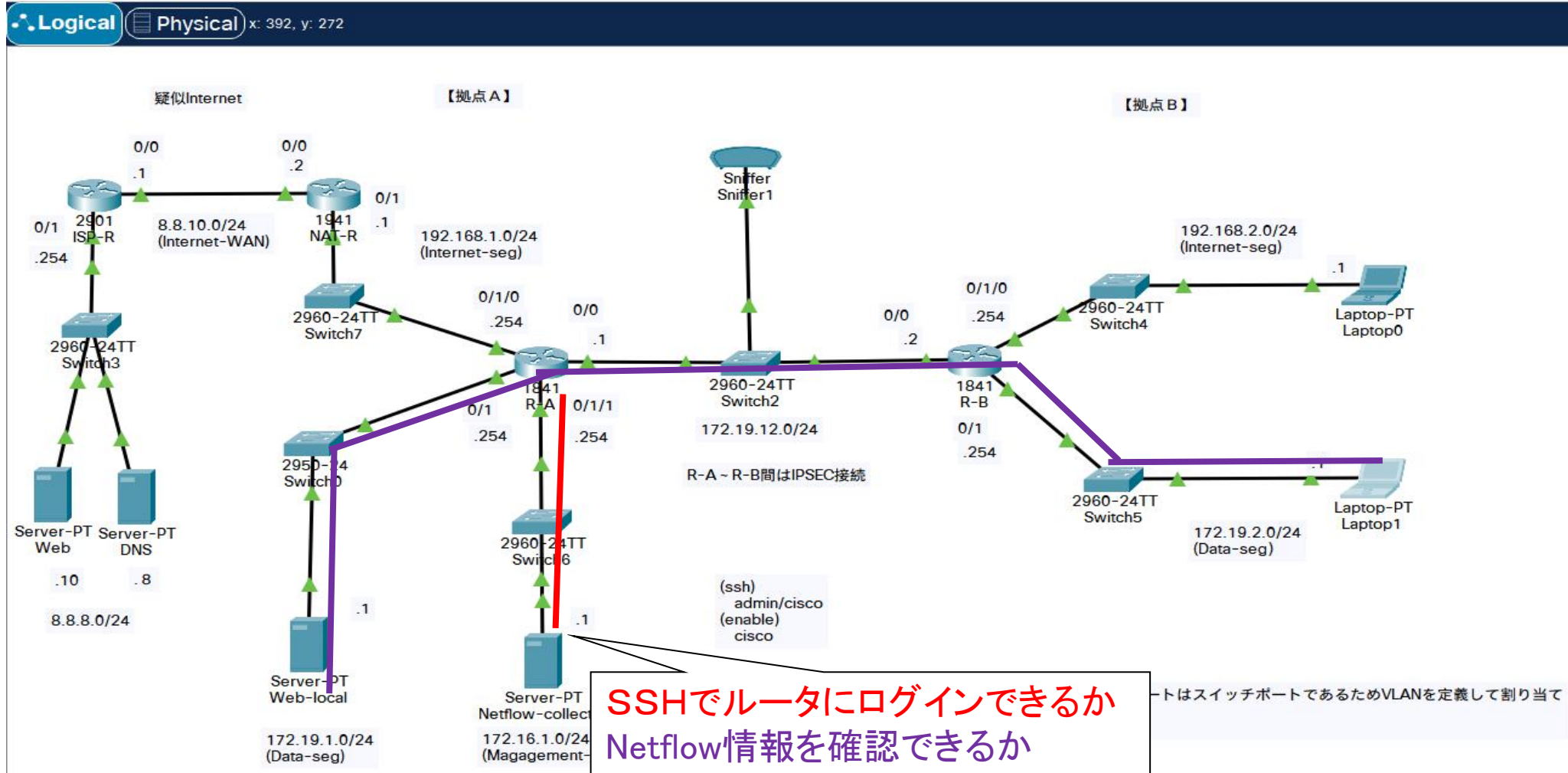
(監視条件の機能確認)



### 3 構成後の機能確認

(監視条件の機能確認)

拠点Aの保守端末から以下の動作が可能かを確認してください。

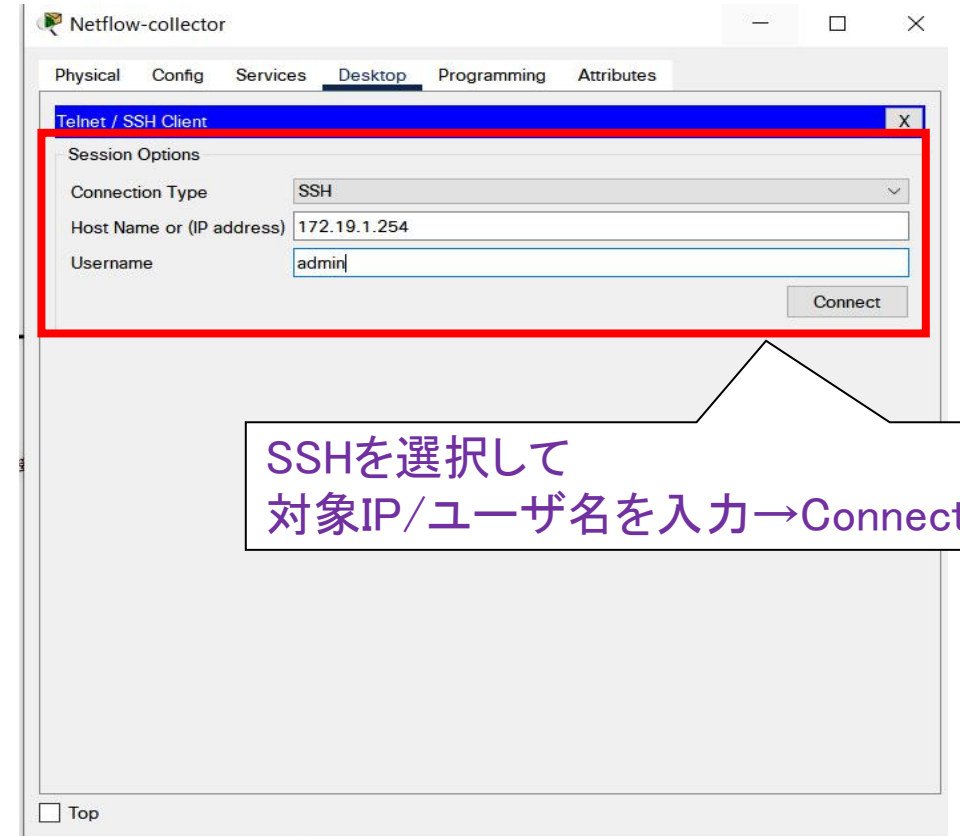
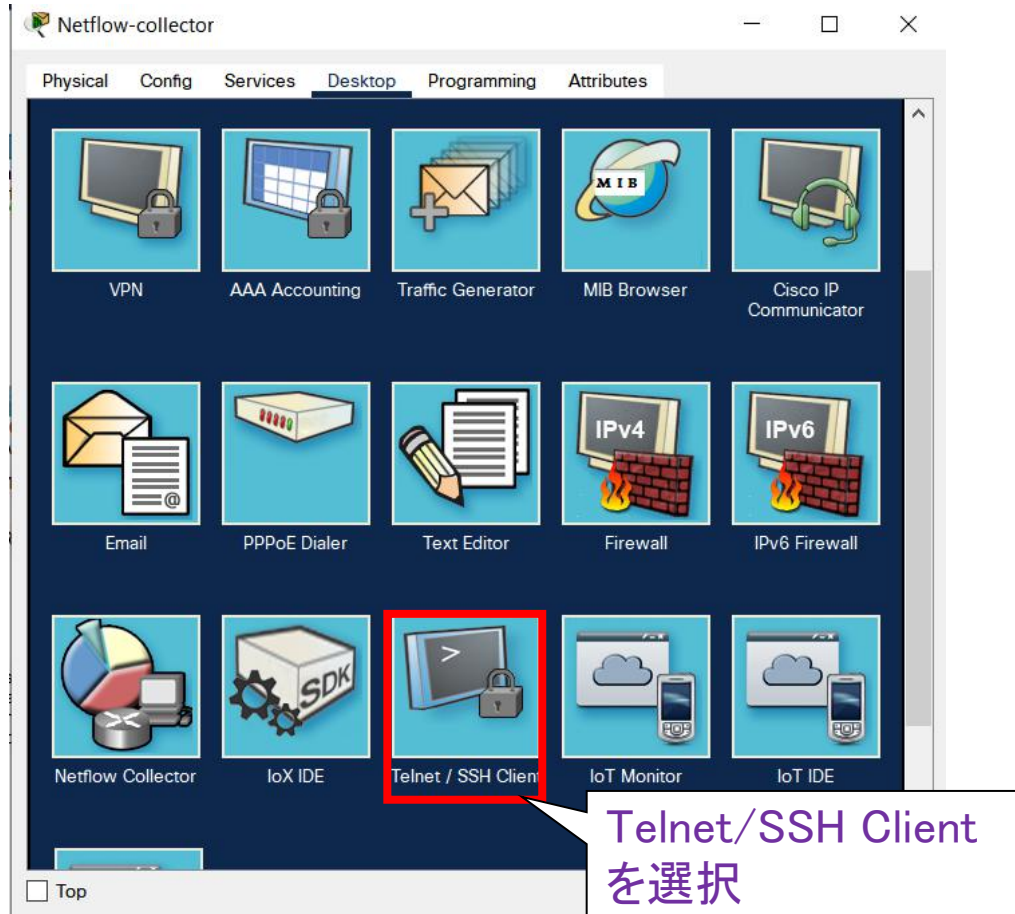


### 3 構成後の機能確認

(監視条件の機能確認)

拠点Aの保守端末から以下の動作が可能かを確認してください。  
各NW機器に対するSSHアクセス

【拠点A保守端末からのSSHクライアント起動及びログイン】



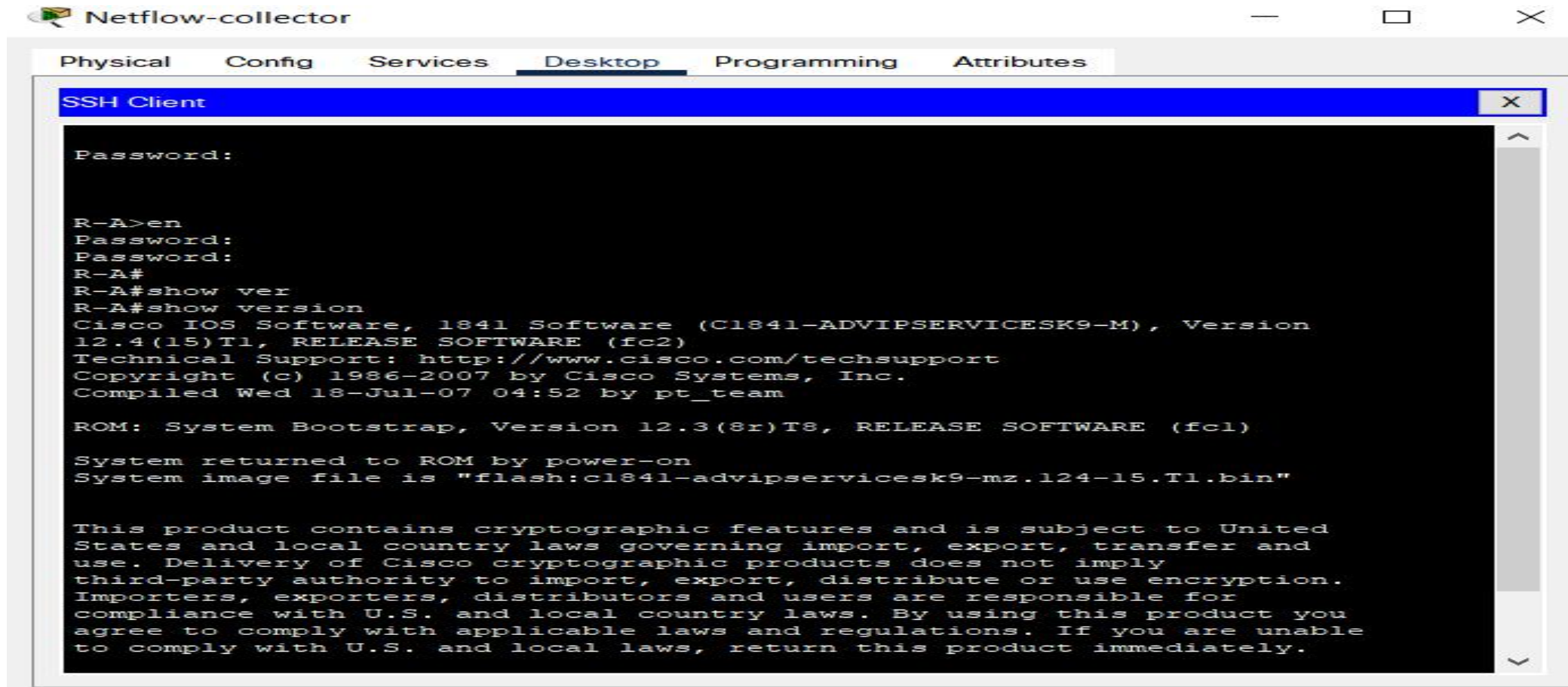


### 3 構成後の機能確認

(監視条件の機能確認)

拠点Aの保守端末から以下の動作が可能かを確認してください。  
各NW機器に対するSSHアクセス

【拠点A保守端末からのSSHクライアント起動及びログイン】



The screenshot shows a window titled "Netflow-collector" with several tabs: Physical, Config, Services, Desktop (selected), Programming, and Attributes. Inside the window is a terminal window titled "SSH Client". The terminal displays the following text:

```
Password:

R-A>en
Password:
Password:
R-A#
R-A#show ver
R-A#show version
Cisco IOS Software, 1841 Software (C1841-ADVIPSERVICESK9-M), Version
12.4(15)T1, RELEASE SOFTWARE (fc2)
Technical Support: http://www.cisco.com/techsupport
Copyright (c) 1986-2007 by Cisco Systems, Inc.
Compiled Wed 18-Jul-07 04:52 by pt_team

ROM: System Bootstrap, Version 12.3(8r)T8, RELEASE SOFTWARE (fc1)

System returned to ROM by power-on
System image file is "flash:c1841-advipservicesk9-mz.124-15.T1.bin"

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you
agree to comply with applicable laws and regulations. If you are unable
to comply with U.S. and local laws, return this product immediately.
```

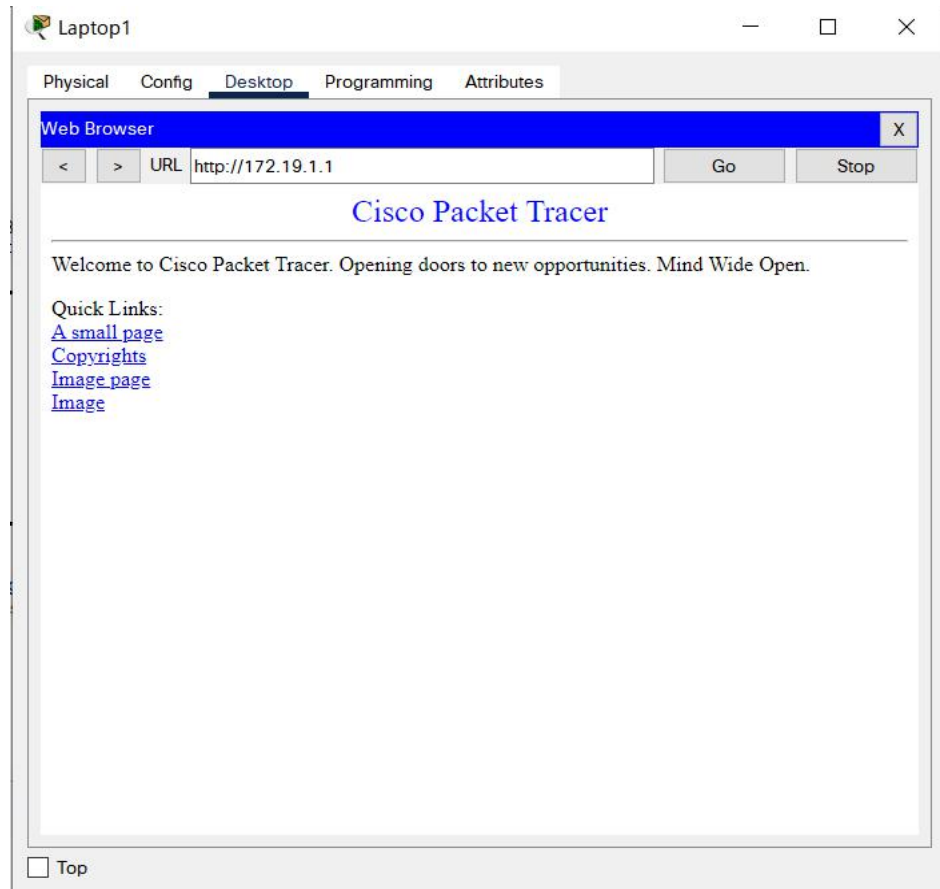
### 3 構成後の機能確認

(監視条件の機能確認)

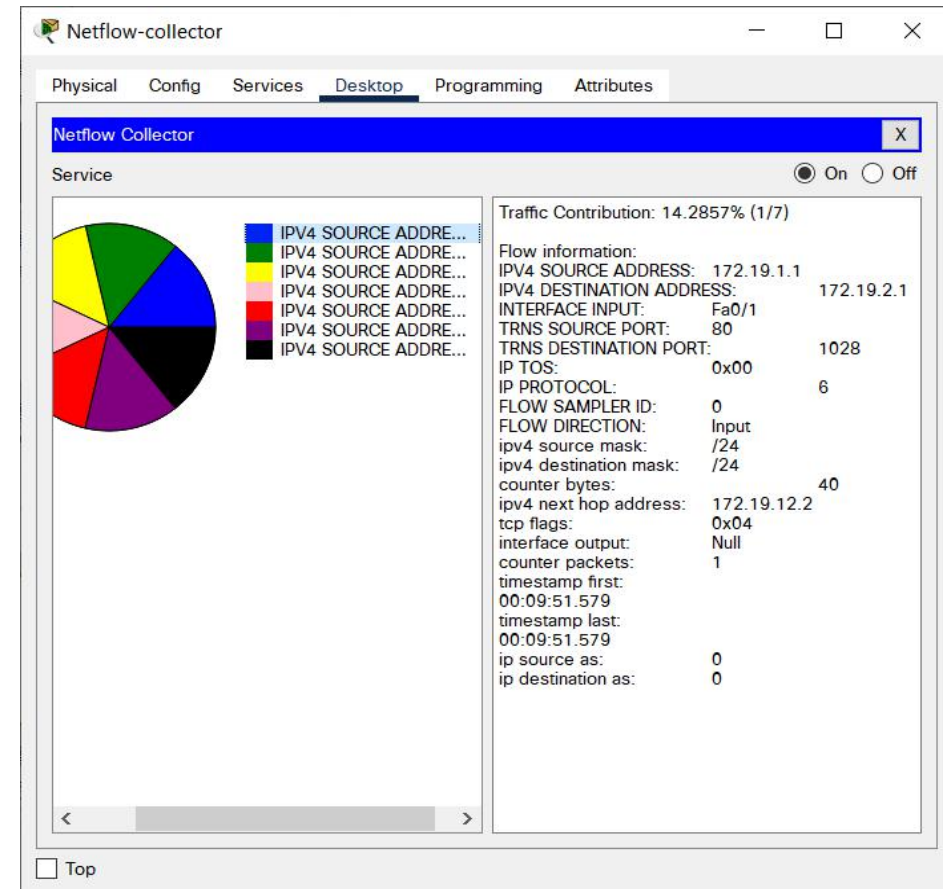
拠点Aの保守端末から以下の動作が可能かを確認してください。

Netflowによるトラフィック確認

#### 【拠点BクライアントからのWebアクセス】



#### 【NetflowコレクターによるFlow確認】



### 3 構成後の機能確認

(監視条件の機能確認)

拠点Aの保守端末から以下の動作が可能かを確認してください。

Netflowによるトラフィック確認

【NetflowExporter(R-A)によるFlow確認】

“show ip cache flow” による確認

R-A#show ip ch  
R-A#show ip ca  
R-A#show ip cache flow

IP packet size distribution (31 total packets):

Packet Size	Count
1-32	64
32-64	96
64-128	128
128-160	160
160-192	192
192-224	224
224-256	256
256-288	288
288-320	320
320-352	352
352-384	384
384-416	416
416-448	448
448-480	480
480-512	512
512-544	544
544-576	576
576-1024	1024
1024-1536	1536
1536-2048	2048
2048-2560	2560
2560-3072	3072
3072-3584	3584
3584-4096	4096
4096-4608	4608
4608-5120	5120

IP Flow Switching Cache, 278544 bytes  
0 active, 4096 inactive, 12 added  
0 ager polls, 0 flow alloc failures  
Active flows timeout in 30 minutes  
Inactive flows timeout in 15 seconds

IP Sub Flow Cache, 34056 bytes  
0 active, 1024 inactive, 0 added, 0 added to flow  
0 alloc failures, 0 force free  
1 chunk, 1 chunk added  
last clearing of statistics never

Protocol	Total	Flows	Packets	Bytes	Packets	Active (Sec)
Idle (Sec)						
TCP-HTTP	6	0.0	3	40	0.0	0.2
TCP-other	6	0.0	2	41	0.0	0.0
Total:	12	0.0	2	40	0.0	0.1

SrcIf SrcIPAddress DstIf DstIPAddress Pr SrcP DstP

R-A#

Ctrl+F6 to exit CLI focus

Copy Paste

Top

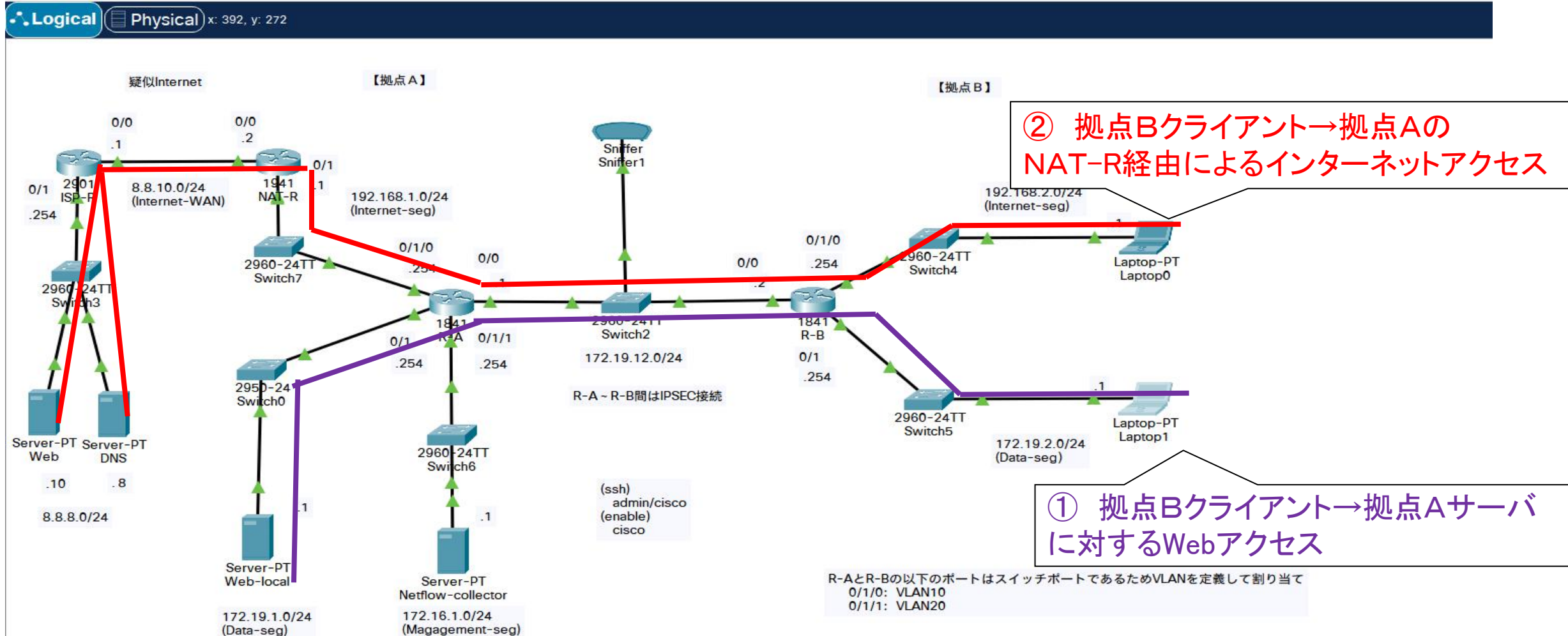
# 3 構成後の確認

(回線条件の機能確認)

### 3 構成後の機能確認

(回線条件の機能確認)

拠点間VPNルータにより秘匿 (IPSEC) できているかを以下の方法で確認してください





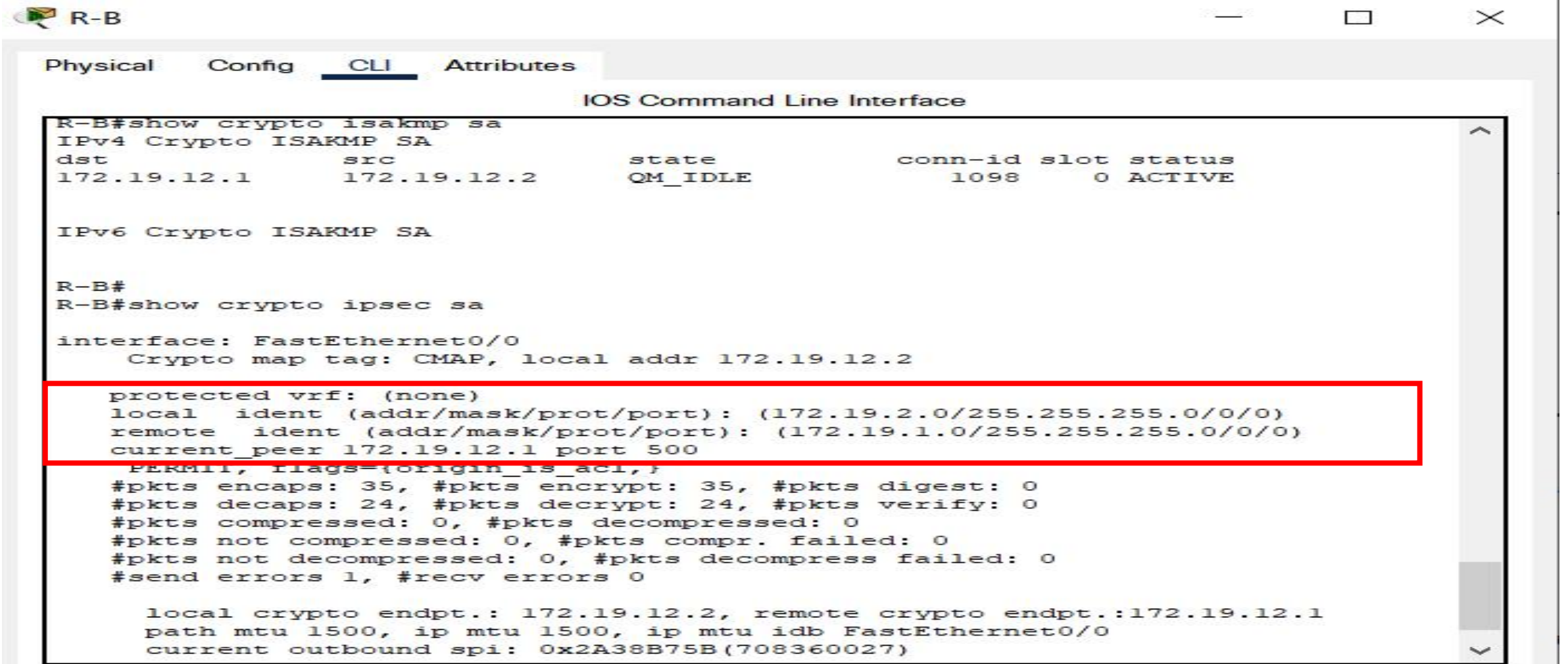
### 3 構成後の機能確認

(回線条件の機能確認)

拠点間VPNルータにより秘匿(IPSEC)できているかを以下の方法で確認してください

① 拠点Bクライアント→拠点Aサーバに対するWebアクセス

“show crypto ipsec sa” による確認



The screenshot shows the CLI of a router labeled R-B. The 'CLI' tab is selected. The command 'show crypto ipsec sa' has been executed on the 'FastEthernet0/0' interface. The output shows an active IPSEC SA for the local address 172.19.12.2 and remote address 172.19.1.1. A red box highlights the 'protected vrf: (none)', 'local ident', 'remote ident', and 'current\_peer' lines. Below this, statistics for packets are shown, and the local and remote crypto endpoints are listed at the bottom.

```
R-B#show crypto ipsec sa
IPv4 Crypto ISAKMP SA
dst          src          state          conn-id slot status
172.19.12.1  172.19.12.2  QM_IDLE        1098      0  ACTIVE

IPv6 Crypto ISAKMP SA

R-B#
R-B#show crypto ipsec sa
interface: FastEthernet0/0
Crypto map tag: CMAP, local addr 172.19.12.2

protected vrf: (none)
local  ident (addr/mask/prot/port): (172.19.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (172.19.1.0/255.255.255.0/0/0)
current_peer 172.19.12.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 35, #pkts encrypt: 35, #pkts digest: 0
#pkts decaps: 24, #pkts decrypt: 24, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 172.19.12.2, remote crypto endpt.: 172.19.12.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x2A38B75B(708360027)
```

### 3 構成後の機能確認

(回線条件の機能確認)

拠点間VPNルータにより秘匿(IPSEC)できているかを以下の方法で確認してください

② 拠点Bクライアント→拠点AのNAT-R経由によるインターネットアクセス

“show crypto ipsec sa” による確認

```
R-B
Physical Config CLI Attributes
IOS Command Line Interface

inbound pcp sas:
outbound esp sas:
outbound ah sas:
outbound pcp sas:

local ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (0.0.0.0/0.0.0.0/0/0)
current_peer 172.19.12.1 port 500
PERMIT, flags={origin_is_acl,}
#pkts encaps: 13, #pkts encrypt: 13, #pkts digest: 0
#pkts decaps: 0, #pkts decrypt: 0, #pkts verify: 0
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 1, #recv errors 0

local crypto endpt.: 172.19.12.2, remote crypto endpt.: 172.19.12.1
path mtu 1500, ip mtu 1500, ip mtu idb FastEthernet0/0
current outbound spi: 0x4669EB28(1181346600)

inbound esp sas:
spi: 0x9FFD663E(2684184126)
transform: esp-aes esp-sha-hmac ,
in use settings ={Tunnel,}
conn id: 2000, flow_id: FPGA:1, crypto map: CMAP
sa timing: remaining key lifetime (k/sec): (4525504/3590)
IV size: 16 bytes
 replay detection support: N

Ctrl+F6 to exit CLI focus
Copy Paste
Top
```

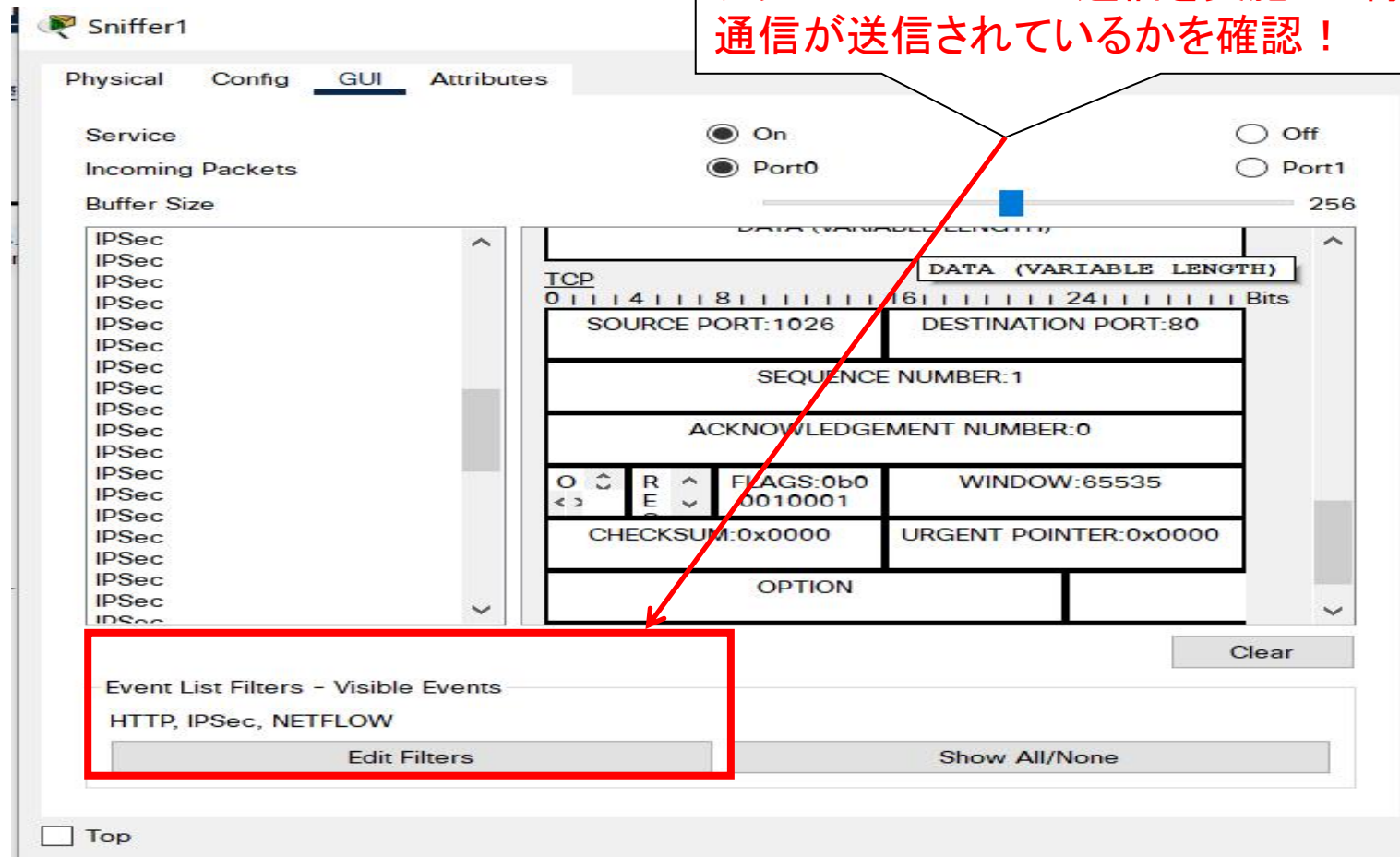
### 3 構成後の機能確認

(回線条件の機能確認)

拠点間VPNルータにより秘匿 (IPSEC) できているかを以下の方法で確認してください

【Snifferによるプロトコル確認】

HTTP、IPSEC等でモニターを実施  
クライアントでHTTP通信を実施した際にIPSECで  
通信が送信されているかを確認！





### 3 構成後の機能確認

参考:IPSEC不具合時の確認POINT！！

- ・以下3つのパターンについて紹介します

#### ◇ Pattern 1

```
Cisco#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                               src                               state                               conn-id status
```

#### ◇ Pattern 2 (失敗)

```
Cisco#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                               src                               state                               conn-id status
11.11.111.111                    22.22.222.222                    MM_NO_STATE                        0 ACTIVE
```

#### ◇ Pattern 3 (成功)

```
Cisco#show crypto isakmp sa
IPv4 Crypto ISAKMP SA
dst                               src                               state                               conn-id status
11.11.111.111                    22.22.222.222                    QM_IDLE                           1001 ACTIVE
```

(出典) ネットワークエンジニアのメモ IPsec-VPN:MM\_NO\_STATEとQM\_IDLEの原因と解決策

<https://www.infraeye.com/2018/04/04/network035/>

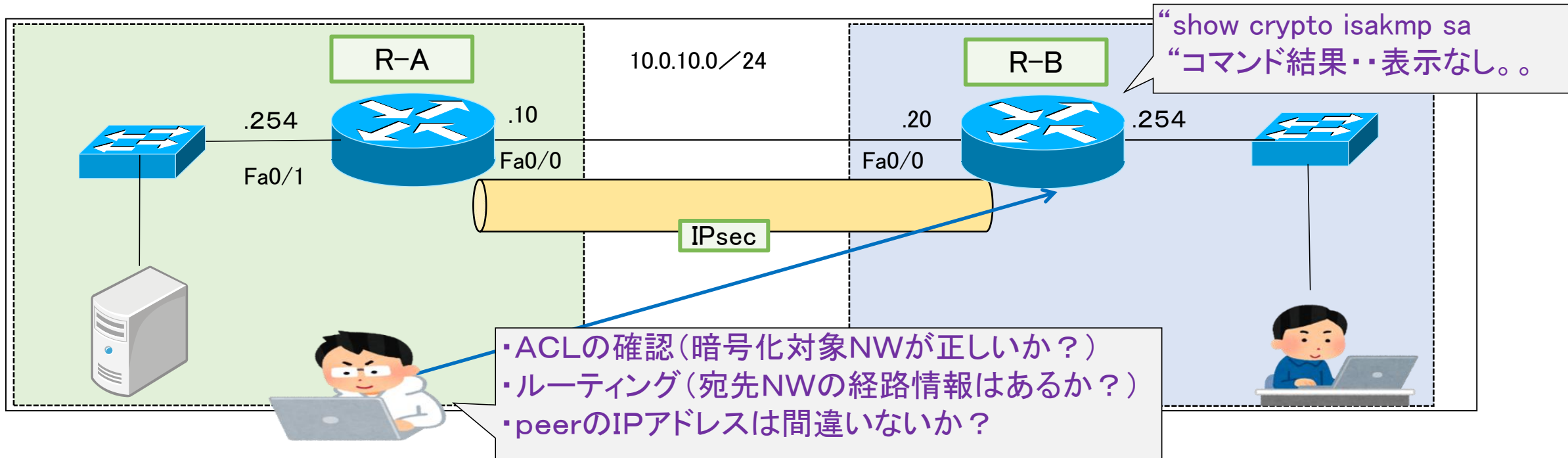
### 3 構成後の機能確認

参考:IPSEC不具合時の確認POINT！！

(パターン1)

**ステータスに何も表示されないケース。**このステータスはIPsec通信が行われていない状態を意味します。つまり、end-to-endで通信が行われていない状態であるためPCから対向拠点のPCに対してPINGなどで通信を行ってみましょう。  
それでも、何も表示されていない場合にはIPsec対象のACL設定ミス、ルーティング設定ミスである可能性が高いです。

【あと isakmp peerのアドレス(IPSEC終端ルータ)が間違っているなど。。】



### 3 構成後の機能確認

参考:IPSEC不具合時の確認POINT！！

(パターン2)

**ステータスにMM\_NO\_STATEと表示されるケース**。このステータスはIKEフェーズ1の失敗を意味します。IPsec-VPN接続を行う両方のルータでIKEフェーズ1の設定に間違いがないかどうかを確認しましょう。例えば、**Pre-shared Key (crypto isakmp key)** の設定が両端のルータで同じ値なのかを確認してみましょう。また、ACLの設定が原因である可能性もあるので障害切り分けのために、**ACLを外したり、一時的に緩いACLに変更して問題を切りわけましょう**。

この問題はルータの再起動によって解決する事例も報告されており、MM\_NO\_STATE (失敗)ステータスから、QM\_IDLE (成功)ステータスに遷移してくれる場合もあります。

(パターン3)

**ステータスにQM\_IDLEと表示されるケース**。このステータスは、IKEフェーズ1の成功を意味します。従って、現状のIKEフェーズ1の設定は正しいことを意味するので、**IPsec-VPN接続の通信が正常に行えない場合は、IKEフェーズ1ではなくて、IKEフェーズ2の設定に問題があることを意味します**

### 3 構成後の機能確認

参考:IPSEC不具合時の確認POINT！！

ルータ間のVPN(IPSEC)が確立される前はPINGが成功しません～

```
Packet Tracer PC Command Line 1.0  
C:\>ping 192.168.2.1
```

```
Pinging 192.168.2.1 with 32 bytes of data:
```

```
Request timed out.
```

```
Request timed out.
```

```
Reply from 192.168.2.1: bytes=32 time<1ms TTL=126
```

```
Reply from 192.168.2.1: bytes=32 time<1ms TTL=126
```

```
Ping statistics for 192.168.2.1:
```

```
    Packets: Sent = 4, Received = 2, Lost = 2 (50% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

```
C:\>
```

IPSec未確立の場合は  
PINGに失敗します・・

ルータ間のVPN(IPSEC)が確立された場合ははPINGが全て成功します！

## 4 参 考

### (1) インタフェースモジュールの追加例

## 4 参考資料

### (1) インタフェースモジュールの追加例

今回のルータはインターフェースが足りない。。ので以下の要領で追加しました！

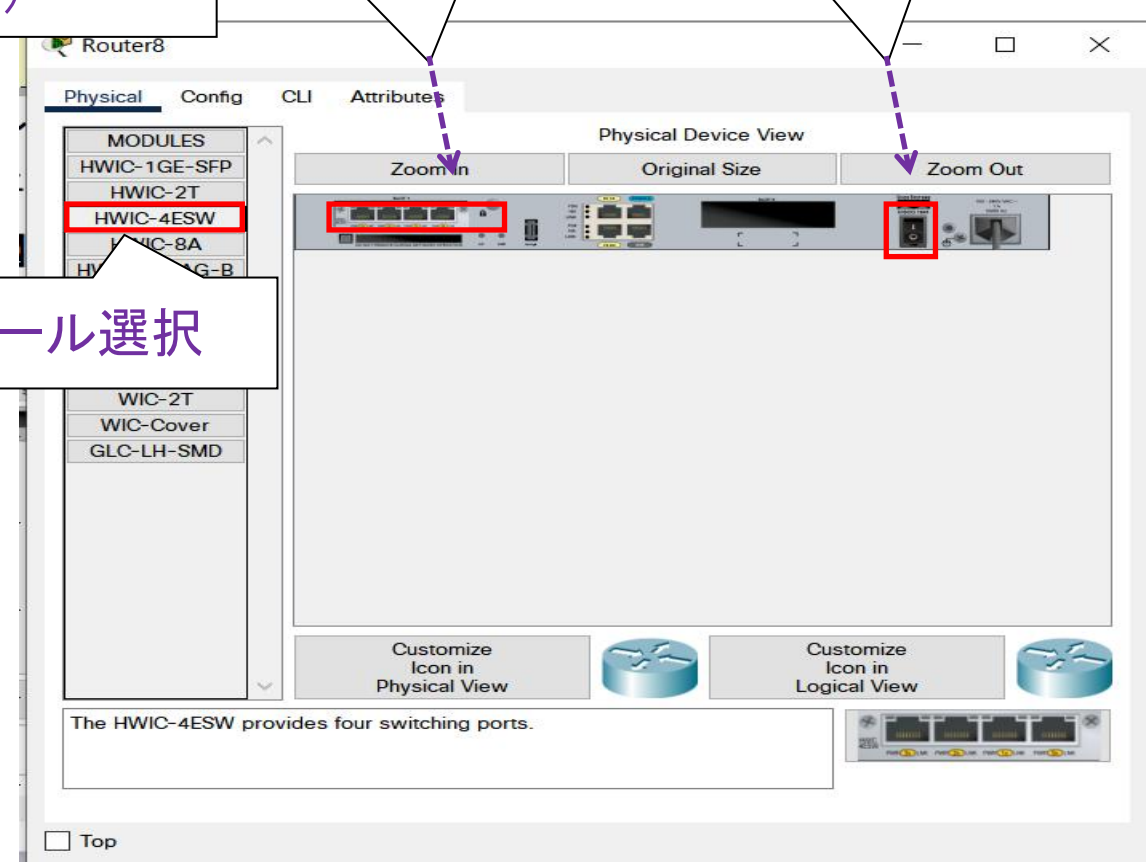
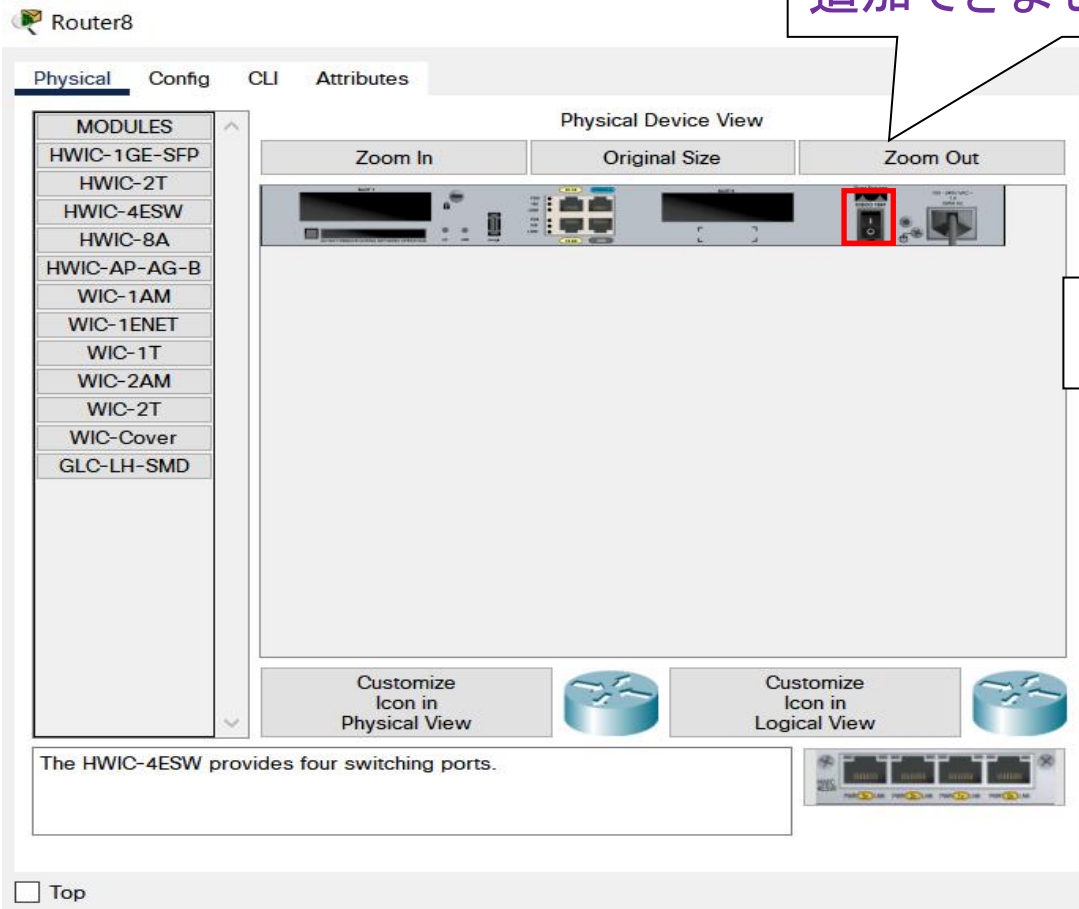
【ルータをクリック→Physical】

電源はOFF  
(OFFにしないとモジュール  
追加できません。。)

ドラック&ドロップ！

電源をON！！

モジュール選択





## 4 参考資料

### (1) インタフェースモジュールの追加例

モジュール追加後、インタフェースが認識しているかを確認！

(追加前)

```
Router#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	unassigned	YES	unset	administratively down	down
Vlan1	unassigned	YES	unset	administratively down	down

(追加後)

```
Router#show ip int brief
```

Interface	IP-Address	OK?	Method	Status	Protocol
FastEthernet0/0	unassigned	YES	unset	administratively down	down
FastEthernet0/1	unassigned	YES	unset	administratively down	down
FastEthernet0/1/0	unassigned	YES	unset	up	down
FastEthernet0/1/1	unassigned	YES	unset	up	down
FastEthernet0/1/2	unassigned	YES	unset	up	down
FastEthernet0/1/3	unassigned	YES	unset	up	down
Vlan1	unassigned	YES	unset	administratively down	down

```
Router#
```

## 4 参 考

### (2) VLAN設定及びIPアドレスの付与要領



## 4 参考資料

### (2) VLAN設定及びIPアドレスの付与要領

今回増設したインターフェースについてはスイッチポート(いわゆるL2ポート)であるため、IPアドレスを付与する場合は以下の要領で実施します。

- ① VLANの追加  
Vlan Databaseコマンドにより  
VLANコンフィギュレーションモードに移行  
→ VLAN "VLAN ID" を付与
- ② VLAN IDに対してIPアドレスを付与  
int VLAN "VLAN ID" コンフィギュレーションモードに移行  
→ IPアドレスを付与
- ③ 物理ポートに対してVLAN IDを付与  
IPアドレスを付与したい物理ポートに対して  
物理ポートコンフィギュレーションモードに移行  
→ switchport mode vlan "vlan id"

## 4 参考資料

### (2) VLAN設定及びIPアドレスの付与要領

#### ① VLANの追加

Vlan Databaseコマンドにより

VLAN設定モードに移行 → VLAN "VLAN ID" を付与

```
R-B#vlan database
% Warning: It is recommended to configure VLAN from config mode,
as VLAN database mode is being deprecated. Please consult user
documentation for configuring VTP/VLAN in config mode.

R-B(vlan)#vlan 10
VLAN 10 modified:
R-B(vlan)#exit
APPLY completed.
Exiting....
R-B#show vlan
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1/1, Fa0/1/2, Fa0/1/3
10	VLAN0010	active	Fa0/1/0
1002	fddi-default	active	
1003	token-ring-default	active	
1004	fddinet-default	active	
1005	trnet-default	active	

VLAN	Type	SAID	MTU	Parent	RingNo	BridgeNo	Stp	BrdgMode	Transl
1	enet	100001	1500	-	-	-	-	-	0
10	enet	100010	1500	-	-	-	-	-	0
1002	fddi	101002	1500	-	-	-	-	-	0

## 4 参考資料

### (2) VLAN設定及びIPアドレスの付与要領

- ② VLAN IDに対してIPアドレスを付与
- ③ 物理ポートに対してVLAN IDを付与



## 4 参 考

(3) Netfowの設定および確認

## 4 参考資料

### (3) Netflowの設定および確認

○ Netflowとは??

ネットワーク上で流れるトラフィックフローを受動的にモニタできる機能のことです。

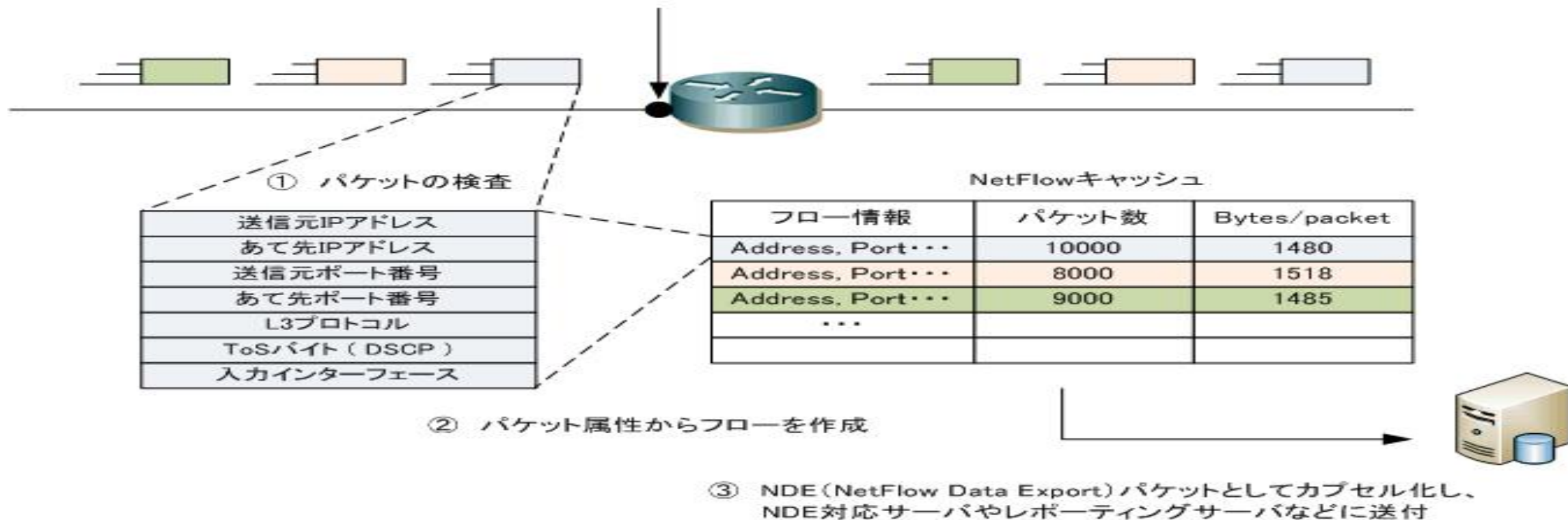
NetFlowはIOSの機能の1つであり、1996年にCiscoが開発しました。

NetFlow version 5 - アーキテクチャ

出典: ネットワークエンジニアとして

<https://www.infraexpert.com/study/netflow1.html>

NetFlowを有効化したI/F



## 4 参考資料

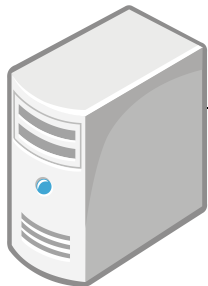
### (3) Netflowの設定および確認

#### ○ Netflow設定及び確認イメージ

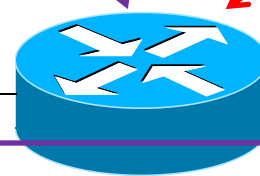
##### ① エクスポート(NW機器)に設定を投入

```
ip flow-export destination 192.168.110.1 9996
ip flow-export version 9
int fa0/0
ip flow ingress      /受信トラフィックを対象
ip flow egress       /送信トラフィックを対象
```

サーバ



fa0/1

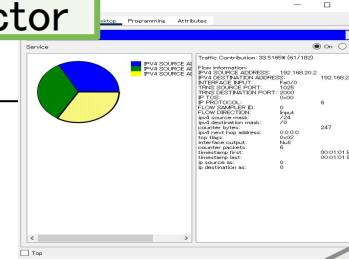


fa0/0

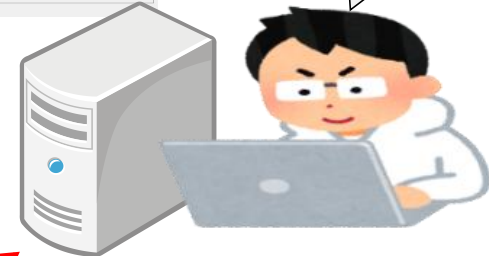
Netflow  
エクスポート

② トラフィックが通過

Netflow  
Collector



④ コレクター  
により確認



IP : 192. 168. 110. 1

③ コレクター  
にFlowを送信

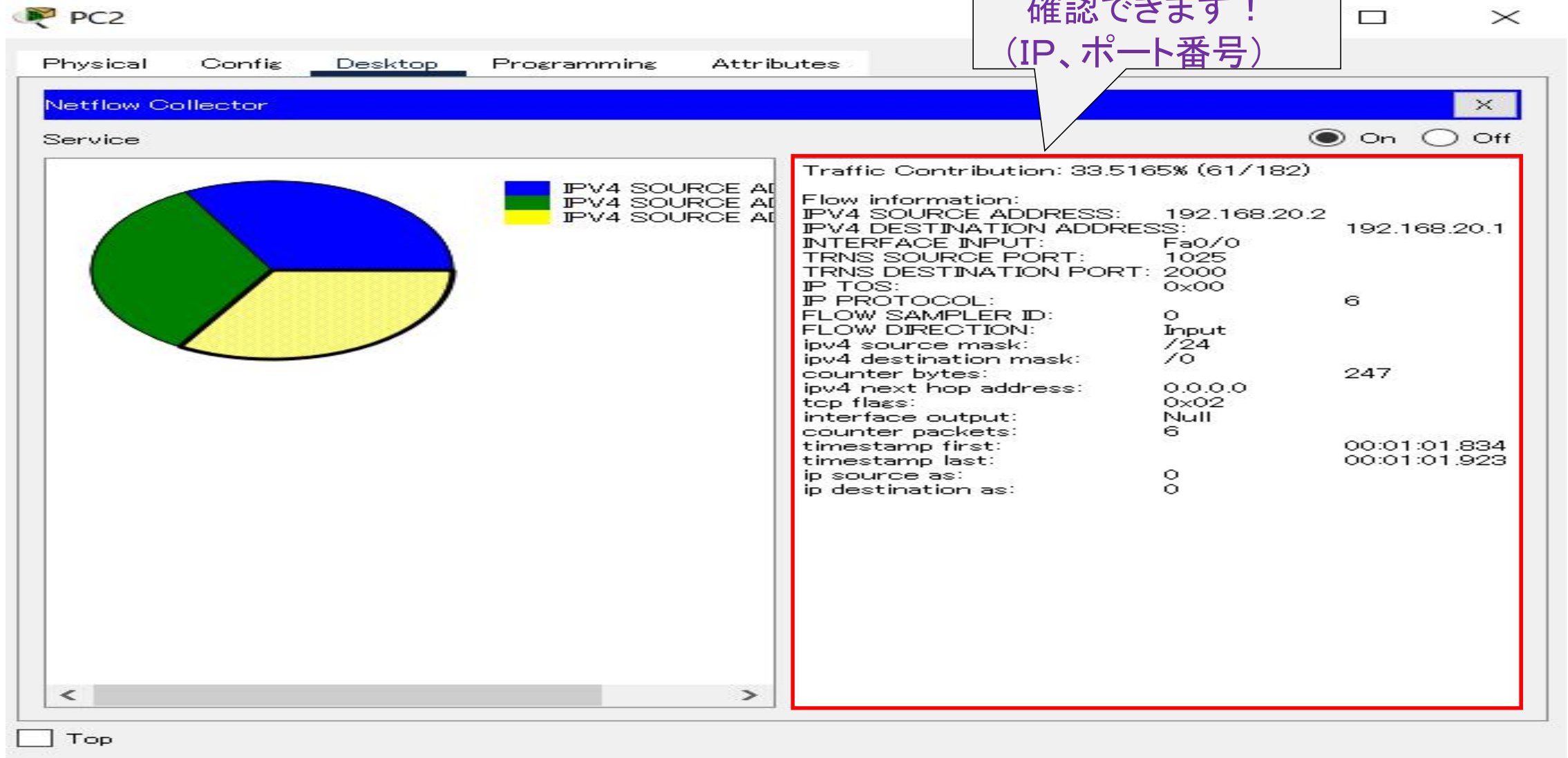
クライアント



## 4 参考資料

### (3) Netflowの設定および確認

#### ○ Netflowコレクターの出力例





## 4 参考資料

### (3) Netflowの設定および確認

#### ○ Netflowエクスポートでの確認(例)

#show ip cache flow コマンドで確認できます！

```
R-2#show ip cache flow
IP packet size distribution (261 total packets):
 1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
 .939 .023 .038 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000

 512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
```

```
IP Flow Switching Cache, 278544 bytes
 2 active, 4094 inactive, 118 added
 1 aged polls, 0 flow alloc failures
 Active flows timeout in 30 minutes
 Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 34056 bytes
 0 active, 1024 inactive, 0 added, 0 added to flow
 0 alloc failures, 0 force free
 1 chunk, 1 chunk added
last clearing of statistics never
```

この例では  
H323:VOIPの呼制御プロトコル  
その他プロトコルが確認できる！！

Protocol	Total Flows	Flows /Sec	Packets /Flow	Bytes /Pkt	Packets /Sec	Active (Sec) /Flow	Idle (Sec) /Flow
TCP-H323	1	0.0	6	41	0.0	3.0	15.0
UDP-DHCP	2	0.0	5	77	0.0	0.5	15.0
UDP-other	113	0.0	2	28	0.011250534.9		15.0
Total:	116	0.0	2	30	0.010959572.9		15.0

SrcIf	SrcIPAddress	DstIf	DstIPAddress	Pr	SrcP	DstP	Pkts
Fa	192.168.20.1	Local	192.168.110.1	11	0000	270c	2
Fa	192.168.20.1	Local	192.168.120.1	11	0401	0401	1

R-2#



## 4 参 考

### (4) ルータのSSH設定及び確認

```
R-B(config)#username admin password cisco /SSHログイン時のユーザ名/パスワード)
R-B(config)#ip domain-name cisco
R-B(config)#crypto key generate rsa
The name for the keys will be: R-B.cisco
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

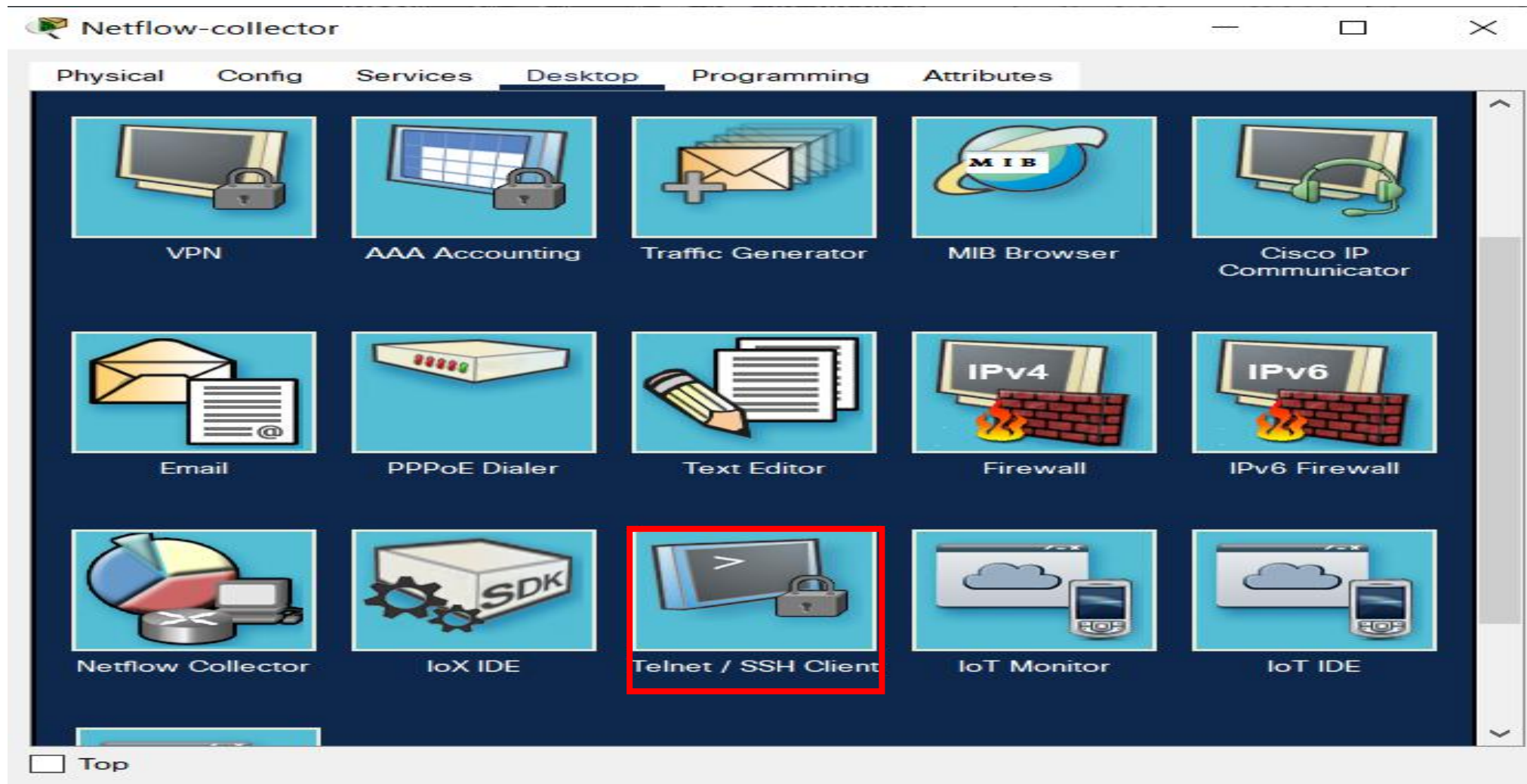
How many bits in the modulus [512]: 1024 / RSAキーは1024
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

*Mar 1 2:19:31.282: %SSH-5-ENABLED: SSH 1.99 has been enabled
R-B(config)#ip ssh version 2
R-B(config)#line vty 0 4 /ルータへのリモート接続
R-B(config-line)#login local /ローカルユーザを使用
R-B(config-line)#transport input ssh /SSH接続を許可
R-B(config-line)#exit
R-B(config)#
R-B(config)#enable secret cisco /enable Secret設定(Cisco)
R-B(config)#
```

## 4 参考資料

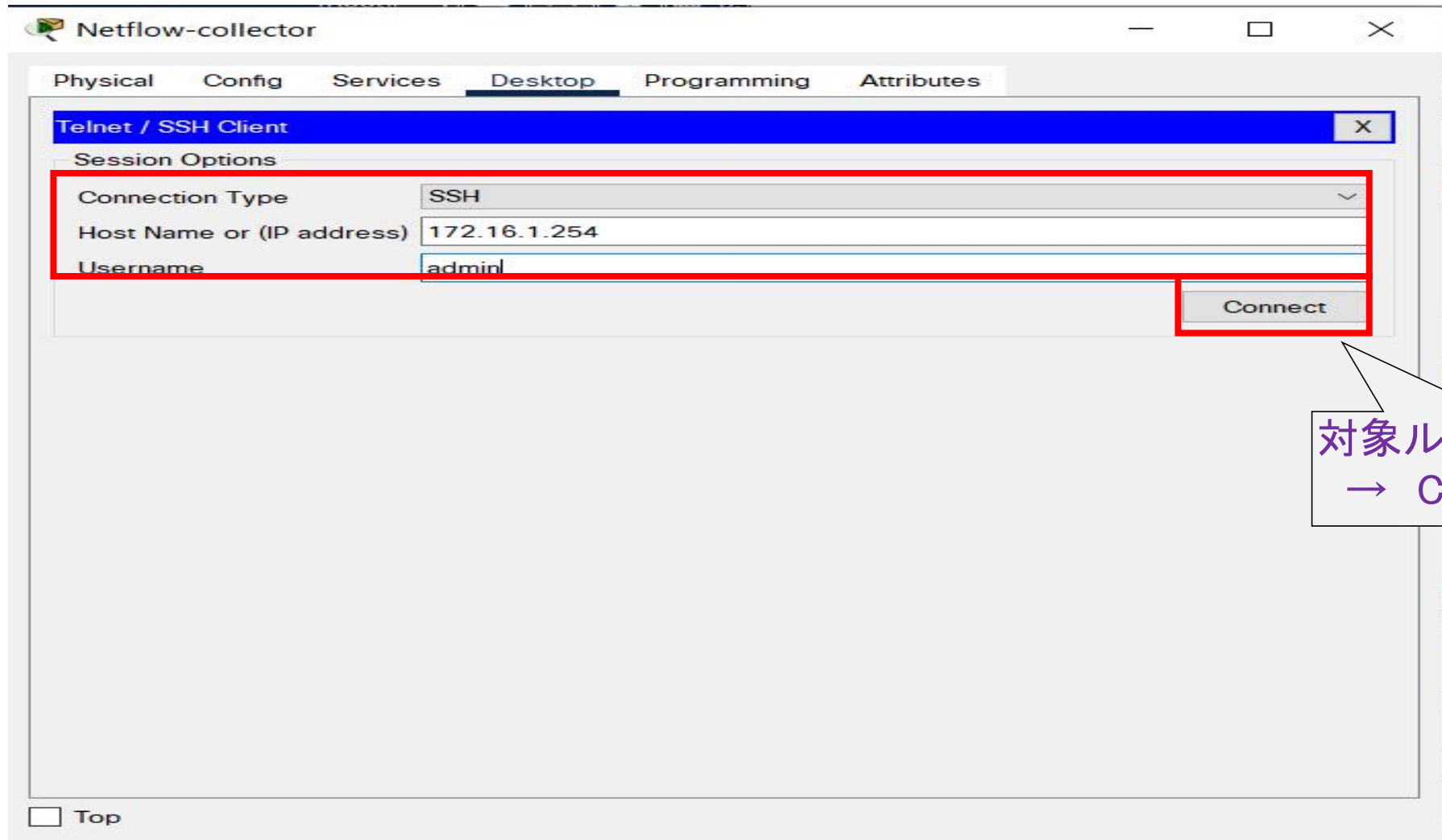
### (4) ルータのSSH設定及び確認

#### SSHクライアント使用方法



## 4 参考資料

### (4) ルータのSSH設定及び確認 SSHクライアント使用方法



## 4 参考資料

### (4) ルータのSSH設定及び確認

#### SSHクライアント使用方法

