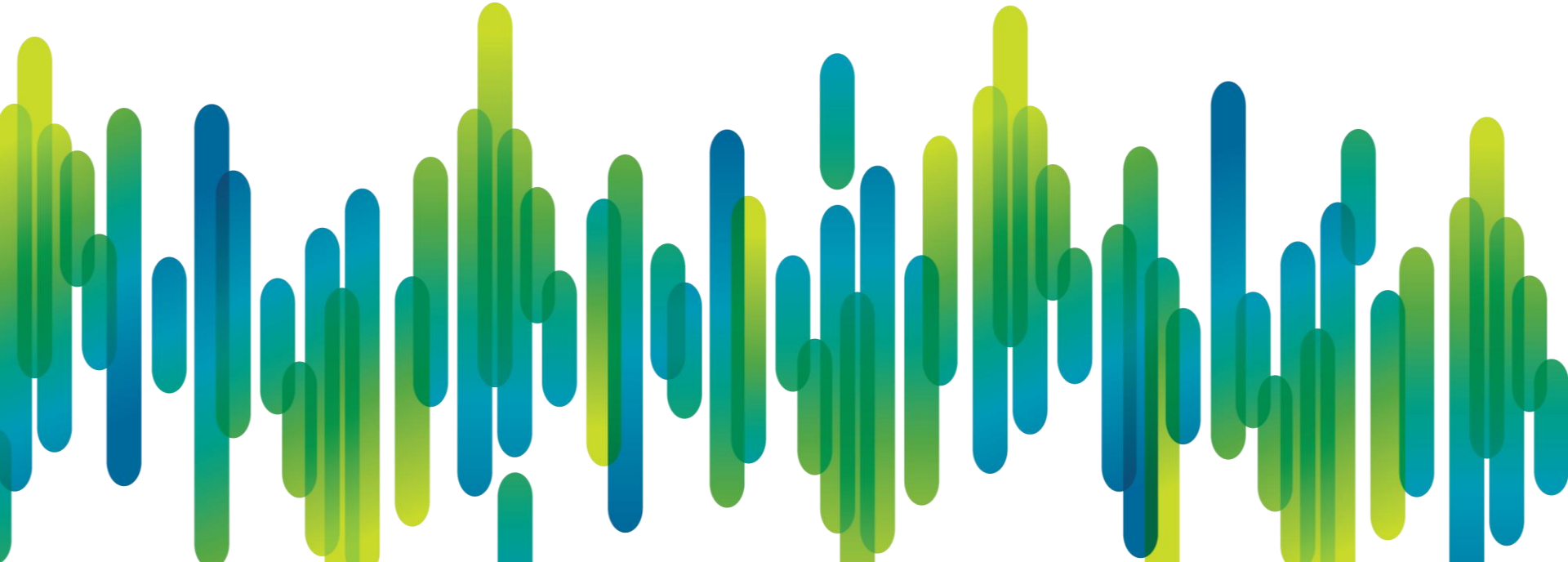
Cisco Firewall 製品のトラブルシューティング

～ASA/FWSM の NAT とパフォーマンス問題について～

秦　昭（シン ショウ）

テクニカルサポート部門　Firewall テクニカルリード



アジェンダ

- NAT（アドレス変換）
  - ASA バージョン 8.2 より以前の NAT
  - ASA バージョン 8.3 より以降の NAT
- パフォーマンス問題
  - ASA/FWSM のアーキテクチャ
  - インターフェイスにおけるドロップ
  - NP（ネットワークプロセッサ）の過負荷
  - CPU 使用率が高い

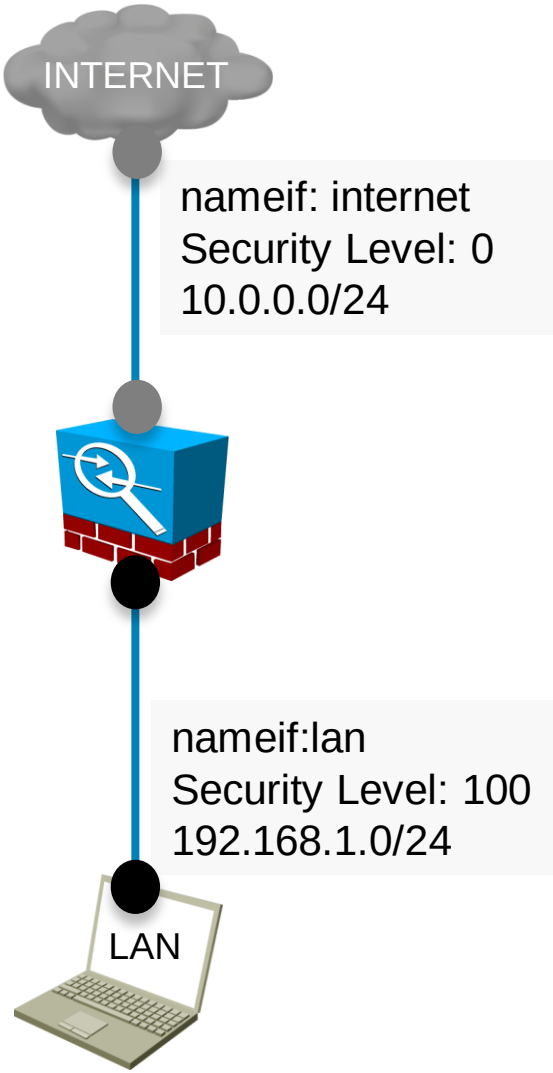
NAT （アドレス変換）

NATの目的と概要

- プライベートアドレスの変換
- グローバルIPアドレスの節約、有効利用
- 内部ネットワークの秘匿、保護
- オーバラップするサブネット間の通信

8.2 より以前の NAT ：

- **Dynamic NAT (PAT)**
- **Dynamic Policy NAT**
- **Dynamic Identity NAT**
- **Static NAT (PAT)**
- **Static Policy NAT**
- **Static Identity NAT**
- **NAT Exemption**
- **Dual NAT**
- **Outside NAT**

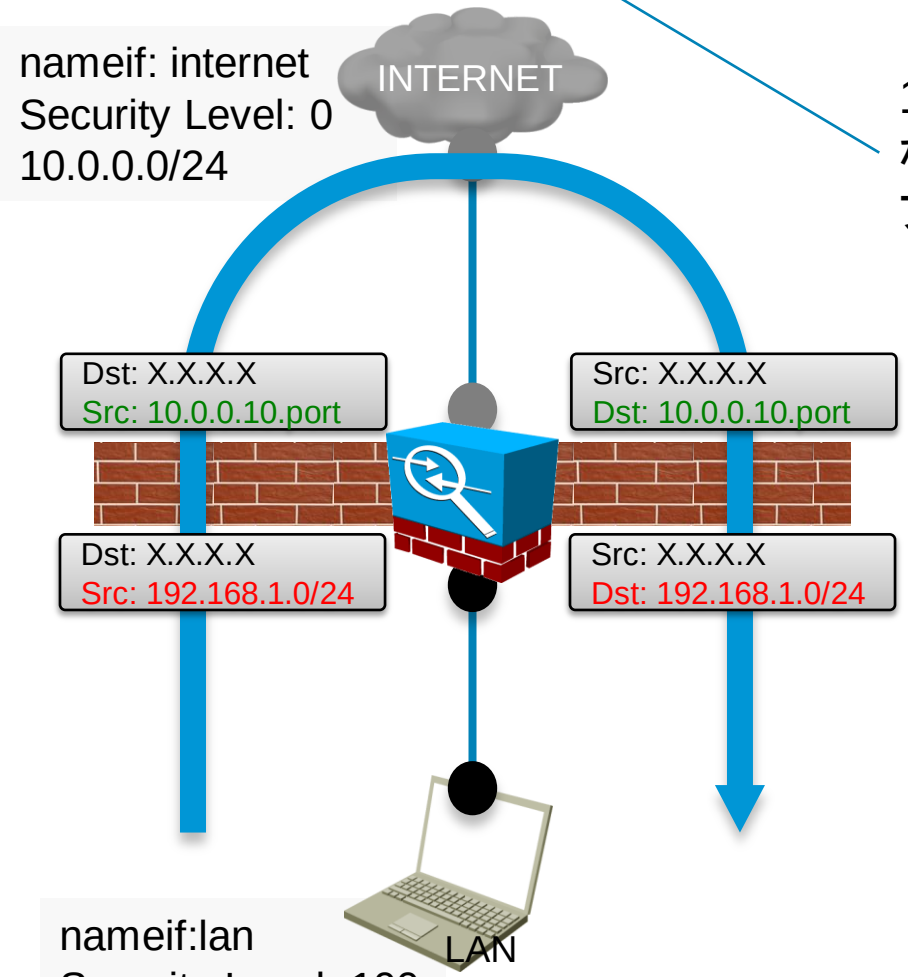


Dynamic NAT

```
global (internet) 1 10.0.0.10
nat (lan) 1 192.168.1.0 255.255.255.0
```

global コマンドで 10.0.0.10 を変換先アドレスとしてプール1 に入れる

192.168.1.0/24 が送信元アドレスとなる通信がインタネットに出る時、プール1 のアドレスに変換する



LAN 側のネットワークを隠しながら、INTERNET にアクセスする

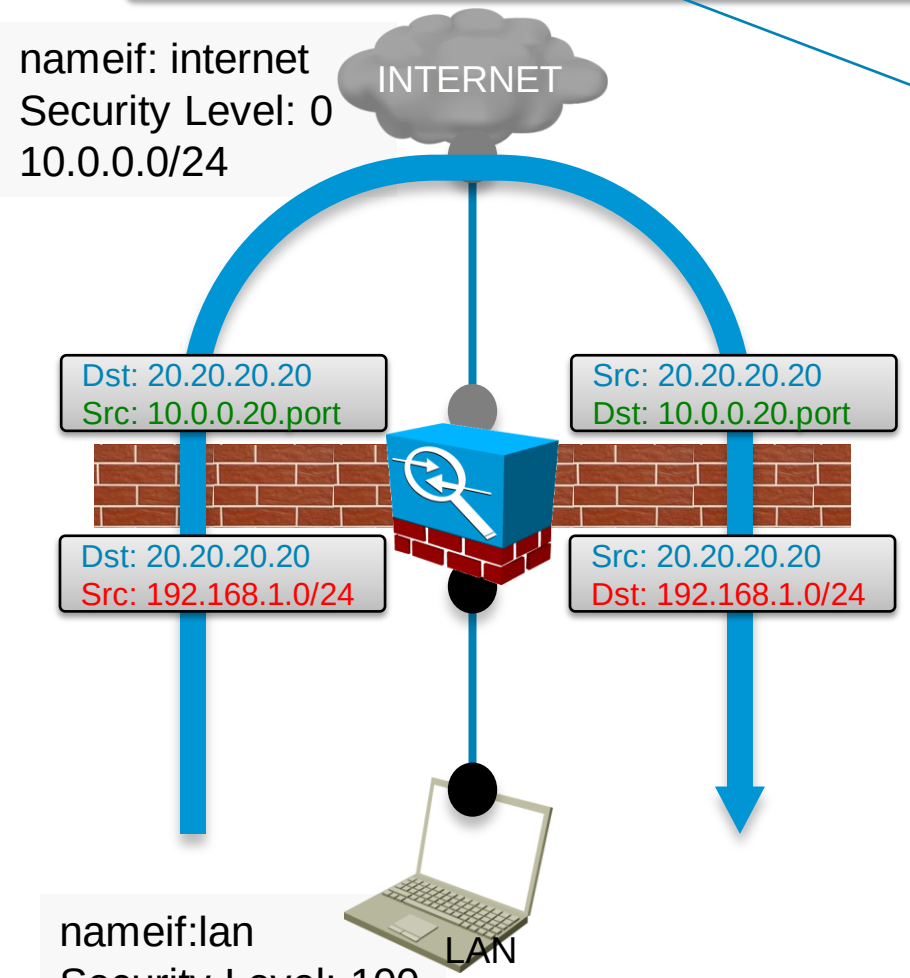
一方向のアクセス:
LAN から発生した通信の戻りパケットのみがインタネットから LAN に転送される。

Dynamic Policy NAT

```
access-list DynamicPolicyNAT permit ip 192.168.1.0 255.255.255.0 host 20.20.20.20
global (internet) 2 10.0.0.20
nat (lan) 2 access-list DynamicPolicyNAT
```

access-list で Src/Dst アドレスを指定する

nat コマンドで access-list と変換プールを紐付ける



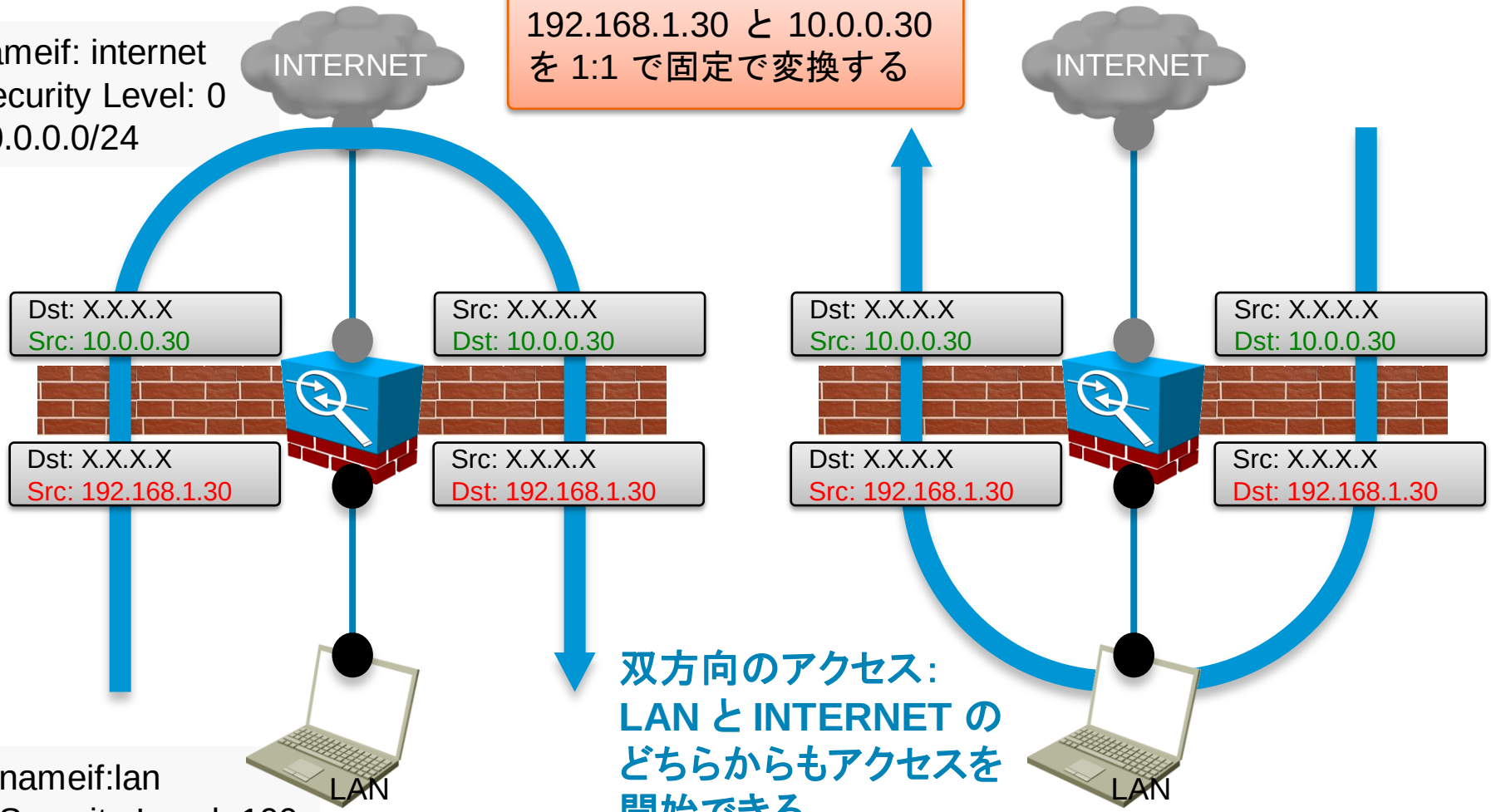
送信元と送信先アドレスを指定して、特定ホスト間の通信を特別に変換する

Static NAT

```
static (lan,internet) 10.0.0.30 192.168.1.30 netmask 255.255.255.255
```

192.168.1.30 と 10.0.0.30 を 1:1 で固定で変換する

nameif: internet
Security Level: 0
10.0.0.0/24



双方向のアクセス:
LAN と INTERNET のどちらからもアクセスを開始できる

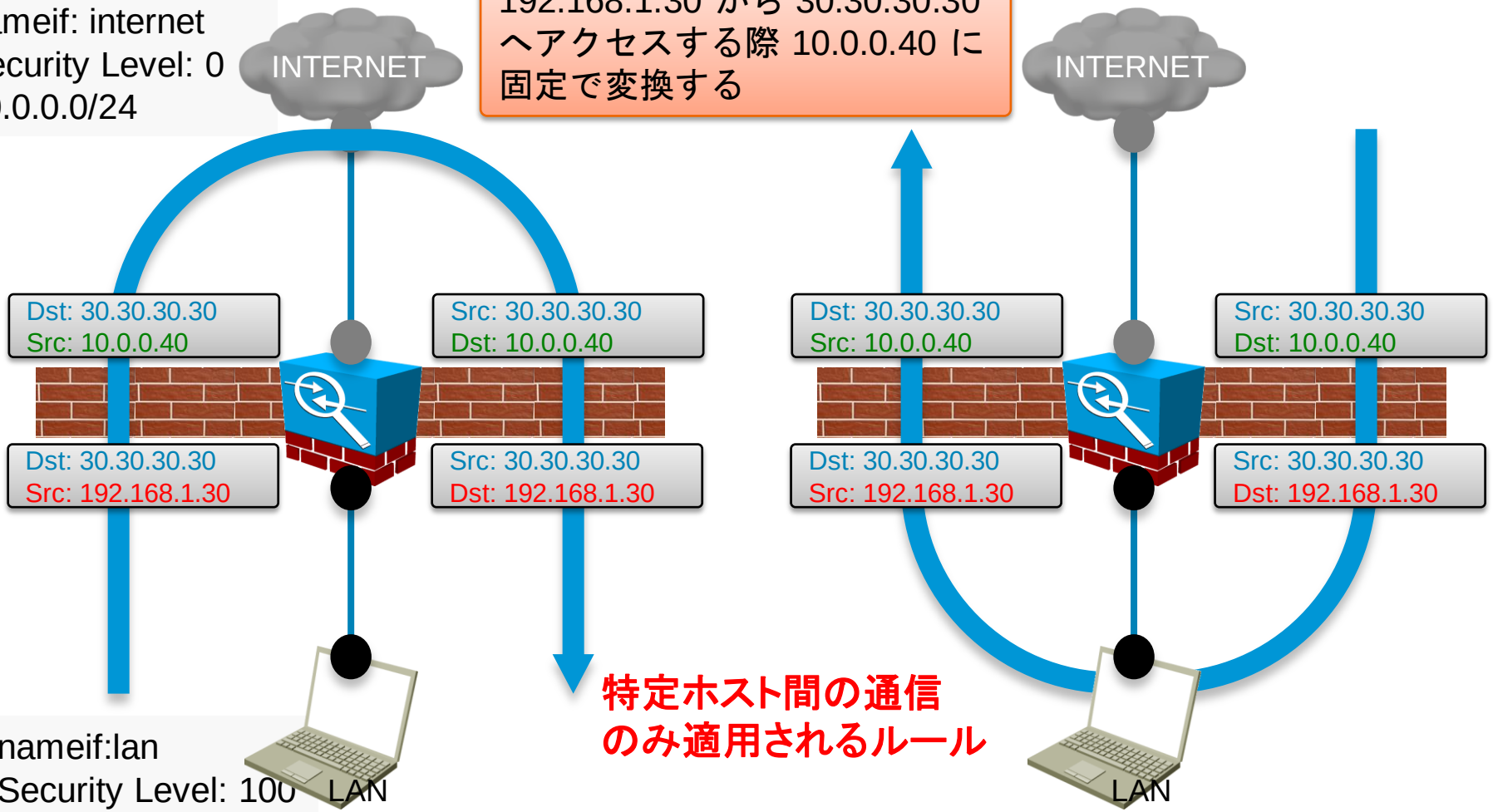
nameif:lan
Security Level: 100
192.168.1.0/24

Static Policy NAT

```
access-list StaticPolicyNAT permit ip host 192.168.1.30 host 30.30.30.30
static (lan,internet) 10.0.0.40 access-list StaticPolicyNAT
```

192.168.1.30 から 30.30.30.30 へアクセスする際 10.0.0.40 に固定で変換する

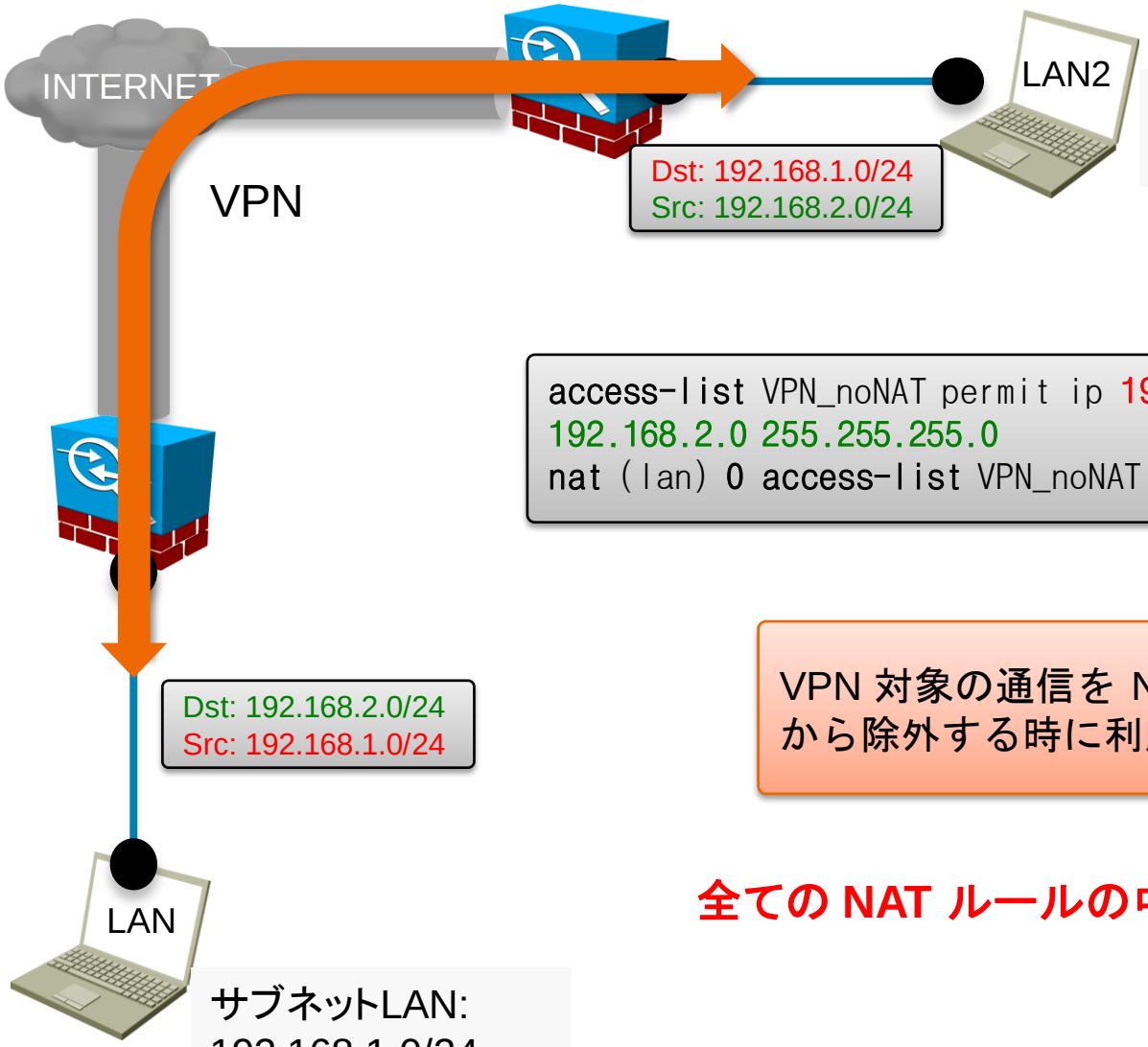
nameif: internet
Security Level: 0
10.0.0.0/24



特定ホスト間の通信のみ適用されるルール

nameif:lan
Security Level: 100
192.168.1.0/24

NAT Exemption

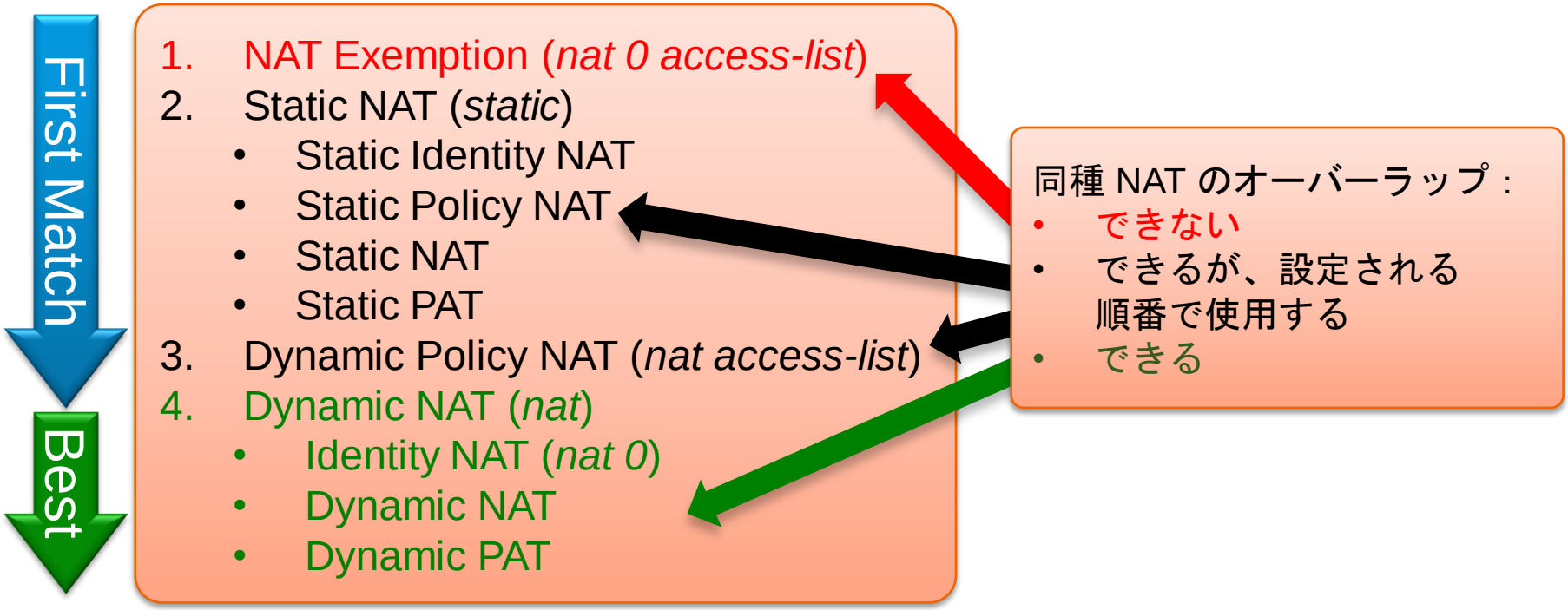



```
access-list VPN_noNAT permit ip 192.168.1.0 255.255.255.0
192.168.2.0 255.255.255.0
nat (lan) 0 access-list VPN_noNAT
```

VPN 対象の通信を NAT 処理から除外する時に利用する

全ての NAT ルールの中で最優先される

NAT の順序(ASAバージョン 8.2 以前)



オーバーラップとは、一つの通信フローが複数の NAT ルールにヒットすること、例えば、以下の設定で 192.168.1.0/25 からの通信の場合 :

global (internet) 1 10.0.0.10
nat (lan) 1 192.168.1.0 255.255.255.0
global (internet) 2 10.0.0.11
nat (lan) 2 192.168.1.0 255.255.255.128

新しい NAT (ASAバージョン 8.3 以降)

NAT ルールは二種類のみ：
- Network Object NAT (Auto NAT)
- Twice NAT (Manual NAT)

- object をベースとする考え方
- NAT 設定が nat 一つのコマンドで行う
- 順序は完全にカスタマイズできる
- アクセスリストを使用しない

First Match

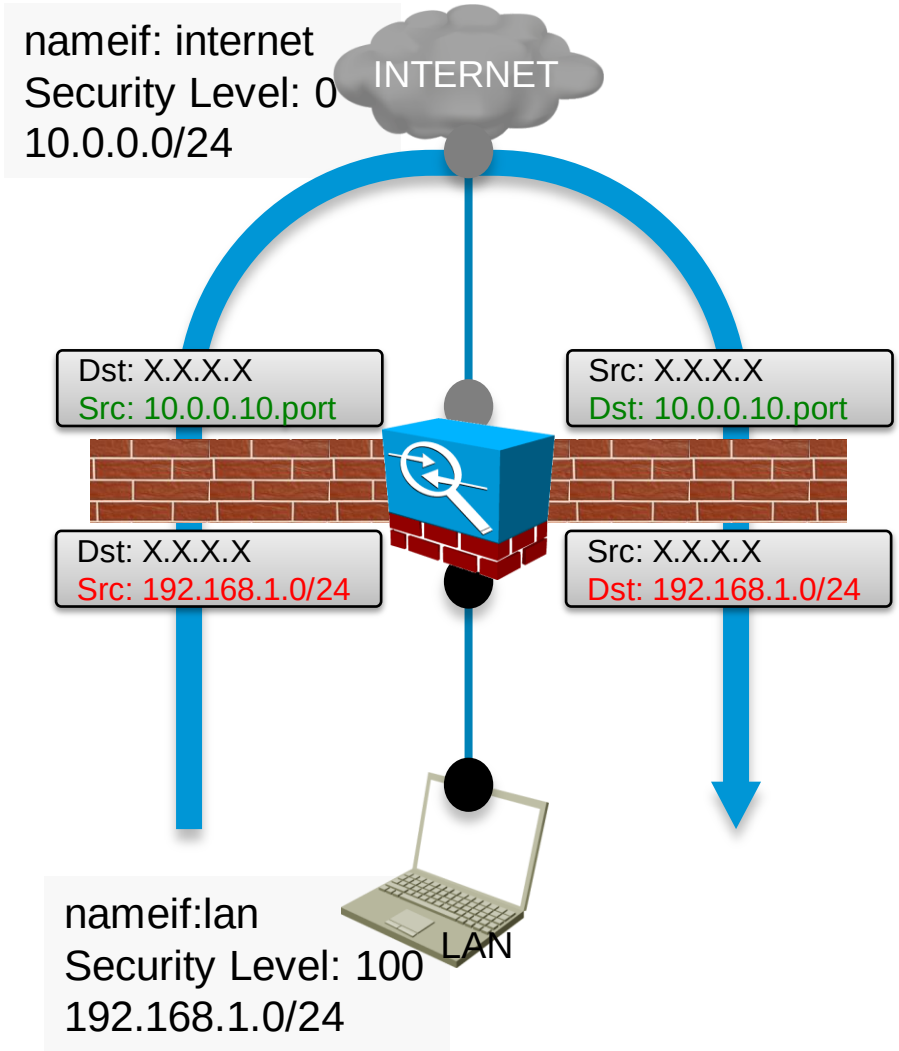
1. Twice NAT(Section 1)

2. Network Object NAT(Section 2)
   1. Static Rule (Best Match)
   2. Dynamic Rule (Best Match)

3. Twice NAT (*after-auto*) (Section 3)

```
ciscoasa# show nat
Manual NAT Policies (Section 1)
1 (inside) to (outside) source static SRC1 MAP1
    translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source static SRC2 MAP2
    translate_hits = 0, untranslate_hits = 0

Auto NAT Policies (Section 2)
1 (inside) to (any) source static IN OUT
    translate_hits = 0, untranslate_hits = 0
2 (inside) to (outside) source dynamic LAN interface
    translate_hits = 0, untranslate_hits = 0

Manual NAT Policies (Section 3)
1 (any) to (any) source static SRC20 MAP20
    translate_hits = 0, untranslate_hits = 0
```

Network Object NAT (Section 2)



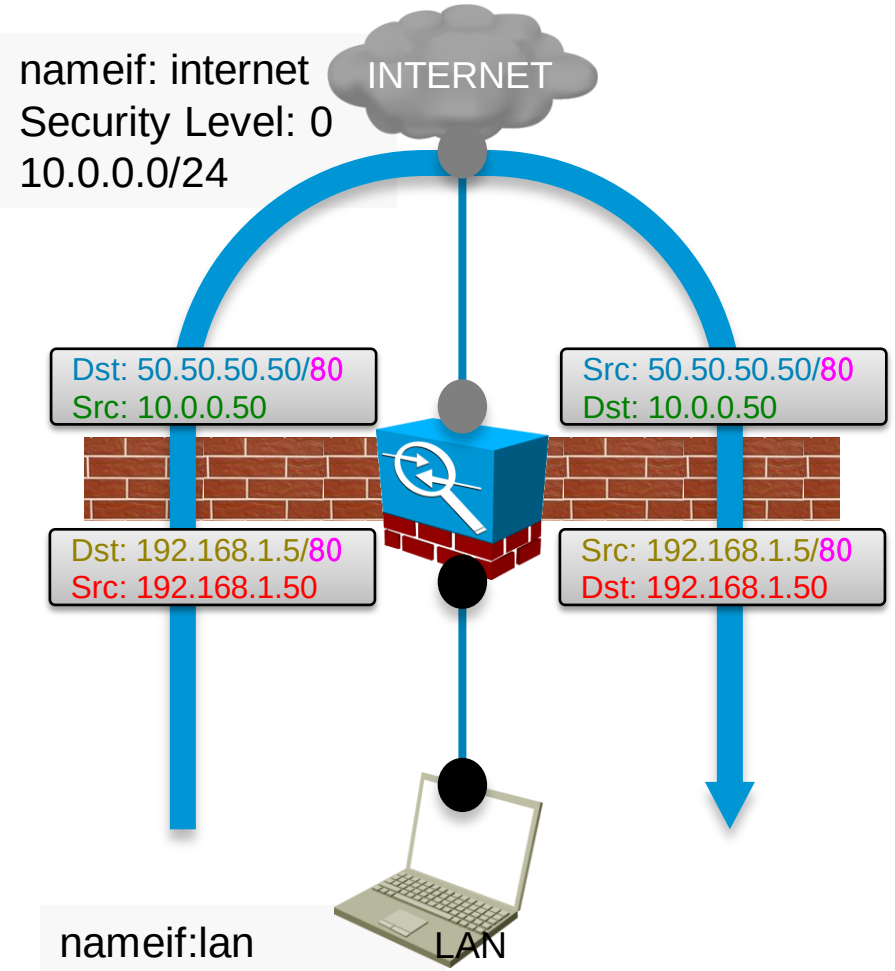

```
object network LAN
 subnet 192.168.1.0 255.255.255.0
object network POOL
 host 10.0.0.10
!
object network LAN
 nat (lan,internet) dynamic POOL
```

設定手順：

1. NAT したい送信元アドレスの object を作成
2. 変換先アドレスの object を作成
3. NAT したい object の中で、nat ルールを作成

Twice NAT (Section 1)

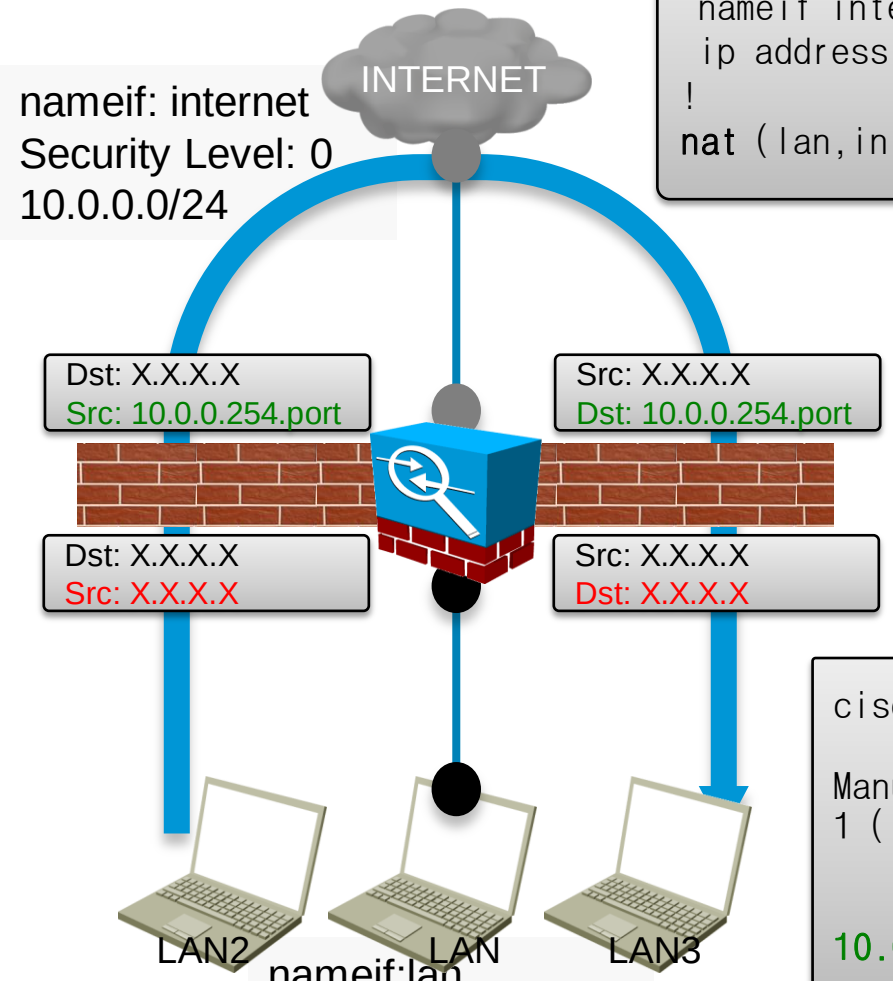
Src/Dst 両方のアドレスを同時変換する




```
object network CLIENT
 host 192.168.1.50
object network MAPPED_CLIENT
 host 10.0.0.50
object network MAPPED_SERVER
 host 192.168.1.5
object network SERVER
 host 50.50.50.50
object service WEB_ACCESS
 service tcp destination eq www
!
nat (lan,internet)
  source static CLIENT MAPPED_CLIENT
  destination static MAPPED_SERVER SERVER
  service WEB_ACCESS WEB_ACCESS
!
access-list INTERNET_IN extended permit
 tcp object SERVER eq www
     object CLIENT
access-group INTERNET_IN in interface internet
```

```
access-list INTERNET_IN extended permit
 tcp host 50.50.50.50 eq www
     host 192.168.1.50
```

Twice NAT (Section 3)




```
interface GigabitEthernet0/0
 nameif internet
 ip address 10.0.0.254 255.255.255.0
!
nat (lan,internet) after-auto 99 source dynamic any interface
```

```
ciscoasa# show nat detail

Manual NAT Policies (Section 3)
1 (lan) to (internet) source dynamic any interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 0.0.0.0/0, Translated:
10.0.0.254/24
```

二種類 NAT の使い分け

Network Object NAT

```
object network REAL
 host 192.168.1.60
object network MAPPED
 host 10.0.0.60
!
object network REAL
 nat (lan,internet) static MAPPED
```

=

Twice NAT

```
object network REAL
 host 192.168.1.60
object network MAPPED
 host 10.0.0.60
!
nat (lan,internet) source static REAL MAPPED
```

- nat が object のパラメータ
- 順序は自動生成
- src と dst を同時変換できない
- 設定と管理が簡単

- object が nat のパラメータ
- 順序は手動指定
- src と dst を同時変換できる
- 柔軟な設定が可能

NAT 関連の便利なコマンド

- packet-tracer
  通信がどの NAT ルールにヒットするかを確認する
- show xlate (debug)
  生成された Xlate を確認する
- show nat (detail)
  設定した NAT ルールの処理順序を確認する

packet-tracer で NAT 設定をテストする

```
ciscoasa# packet-tracer input lan tcp 192.168.1.100 1234
10.10.10.10 80
......
Phase: 3
Type: NAT
Subtype:
Result: ALLOW
Config:
object network LAN
 nat (lan,internet) dynamic POOL
Additional Information:
Dynamic translate 192.168.1.100/1234 to 10.0.0.10/55765
......
Action: allow



ciscoasa# show xlate
1 in use, 18 most used
TCP PAT from lan:192.168.1.100/1234 to
internet:10.0.0.10/55765 flags ri idle 0:00:04 timeout
0:00:30
```

調査したい通信を指定

意図しているNATルールにヒットするか

結果は allow か、deny か

作成した xlate を確認する

show nat (バージョン8.3以前)


```
ciscoasa# show nat
NAT policies on Interface lan:
  match ip lan 192.168.1.0 255.255.255.0 internet 192.168.2.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip lan 192.168.1.0 255.255.255.0 lan 192.168.2.0 255.255.255.0
    NAT exempt
    translate_hits = 0, untranslate_hits = 0
  match ip lan host 192.168.1.30 internet any
    static translation to 10.0.0.30
    translate_hits = 0, untranslate_hits = 0
  match ip lan host 192.168.1.30 internet host 30.30.30.30
    static translation to 10.0.0.40
    translate_hits = 0, untranslate_hits = 0
  match ip lan 192.168.1.0 255.255.255.0 internet host 20.20.20.20
    dynamic translation to pool 2 (10.0.0.20)
    translate_hits = 0, untranslate_hits = 0
  match ip lan 192.168.1.0 255.255.255.0 lan host 20.20.20.20
    dynamic translation to pool 2 (No matching global)
    translate_hits = 0, untranslate_hits = 0
  match ip lan 192.168.1.0 255.255.255.0 internet any
    dynamic translation to pool 1 (10.0.0.10)
    translate_hits = 0, untranslate_hits = 0
  match ip lan 192.168.1.0 255.255.255.0 lan any
    dynamic translation to pool 1 (No matching global)
    translate_hits = 0, untranslate_hits = 0
```

show nat detail (バージョン8.3以降)


```
ciscoasa# show nat detail

Manual NAT Policies (Section 1)
1 (lan) to (internet) source static CLIENT MAPPED_CLIENT   destination static
MAPPED_SERVER SERVER service WEB_ACCESS WEB_ACCESS
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.1.50/32, Translated: 10.0.0.50/32
    Destination - Origin: 192.168.1.5/32, Translated: 50.50.50.50/32
    Service - Origin: tcp destination eq www , Translated: tcp destination eq www

Auto NAT Policies (Section 2)
1 (lan) to (internet) source dynamic LAN POOL
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 192.168.1.0/24, Translated: 10.0.0.10/32

Manual NAT Policies (Section 3)
1 (lan) to (internet) source dynamic any interface
    translate_hits = 0, untranslate_hits = 0
    Source - Origin: 0.0.0.0/0, Translated: 10.0.0.254/24
```

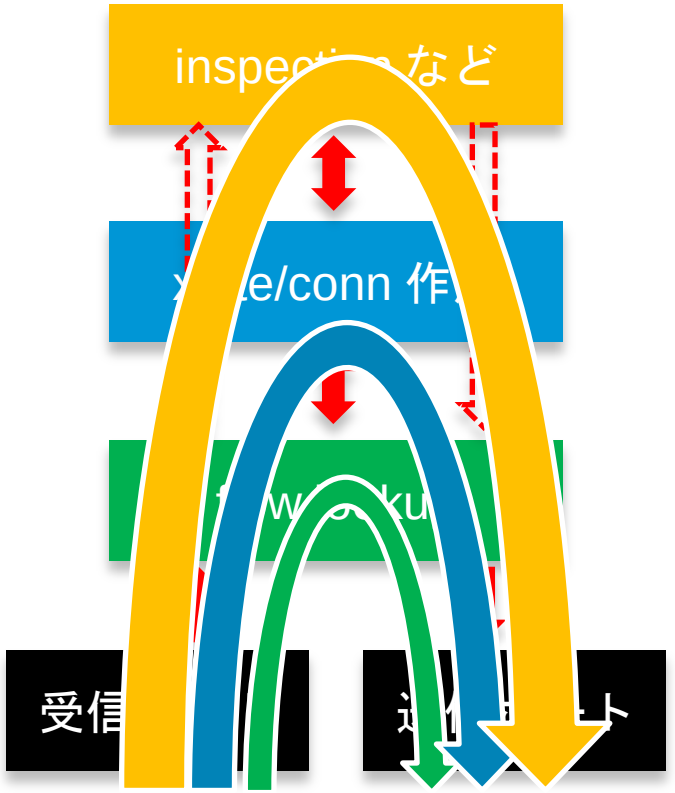
パフォーマンス問題

パフォーマンス問題の概要

- 期待通りのパフォーマンスが得られない
- 期待以上にリソースが消費されている

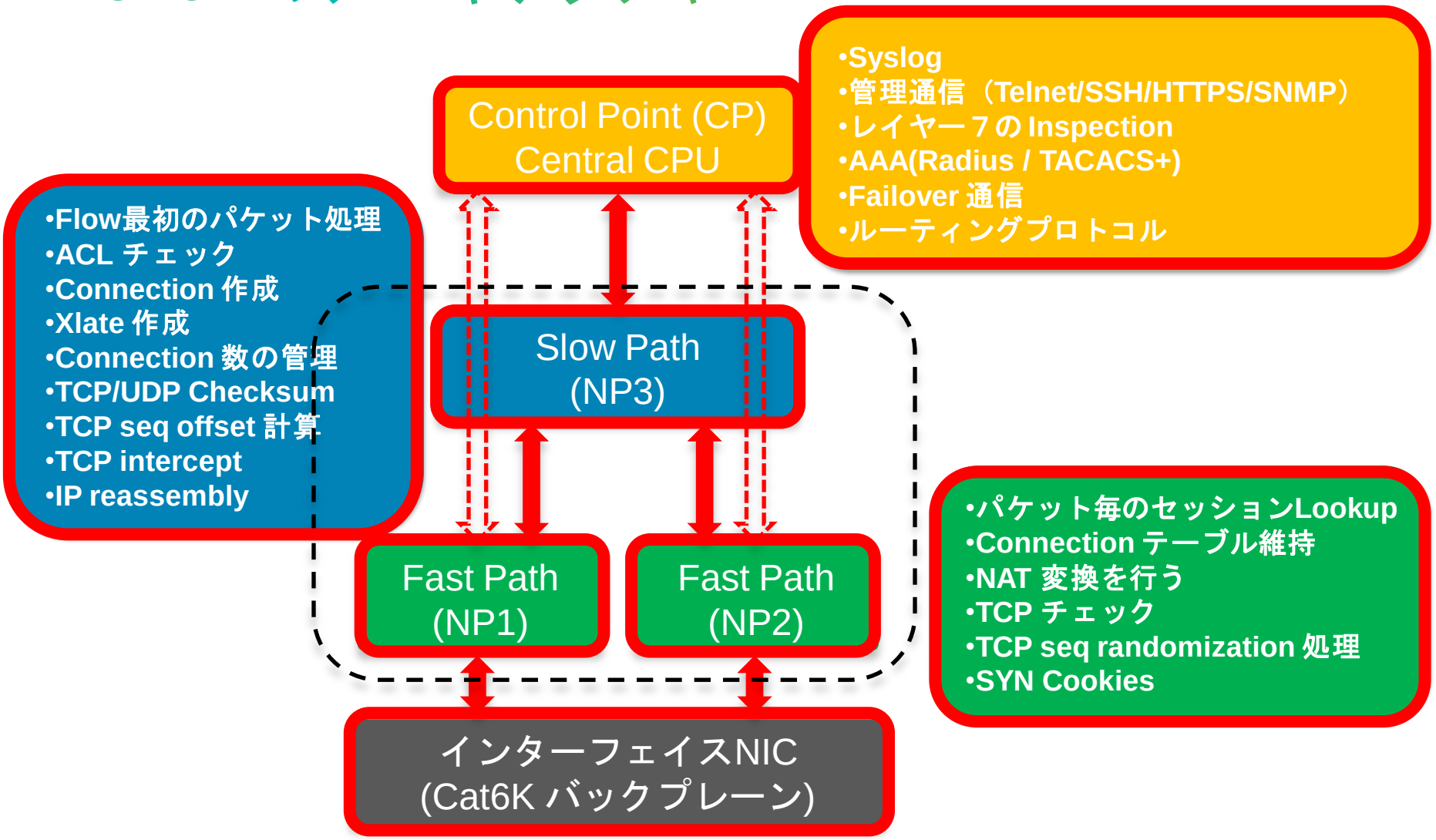
‖

どこかがボトルネックになっている？
- インターフェイス NIC のバッファー
- ネットワークプロセッサ (NP) のバッファー
- CPU 処理サイクル
- メモリの空き容量
- 予め決められた制限

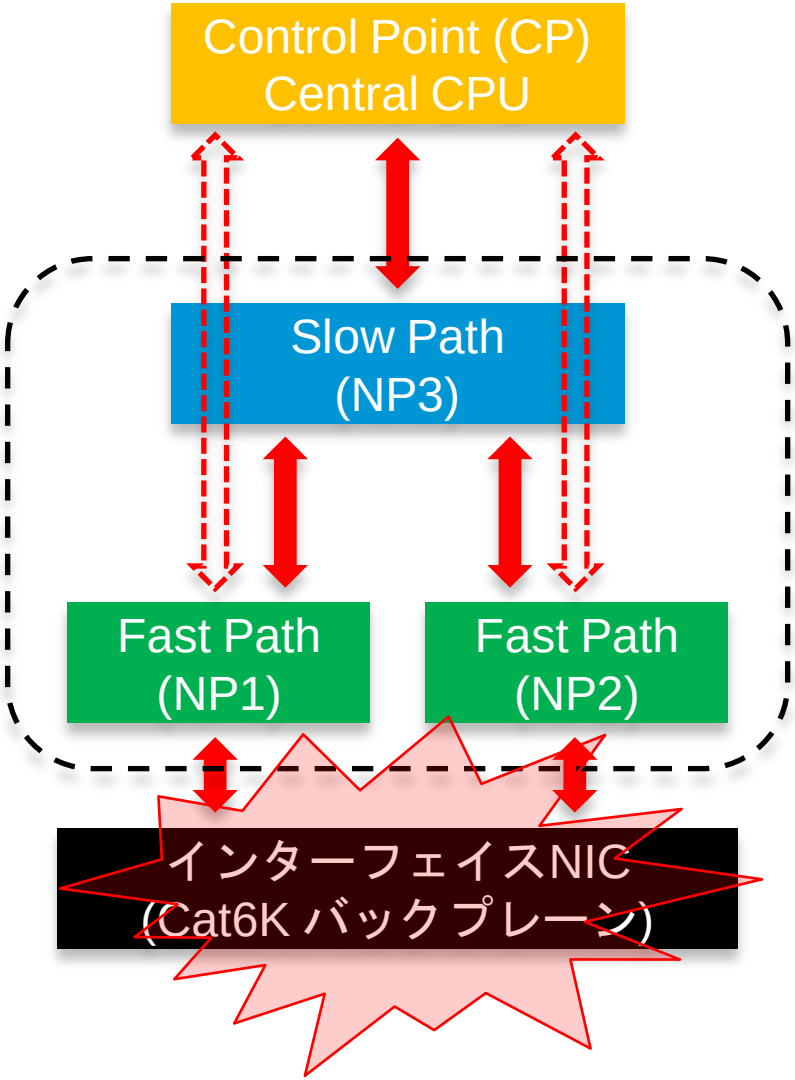


3つの事例:
- 事例①: (ASA) インターフェイスにおけるドロップ
- 事例②: (FWSM) NP(ネットワークプロセッサ) の過負荷
- 事例③: (ASA) CPU 使用率が高い

Firewall のアーキテクチャ



※ASA では ASP (Accelerated Security Procesor) として、
ソフトウェアで NP の機能を実現しています。



事例①:(ASA) インターフェイスにおけるドロップ

事象：MRTG データから見るトラフィックレートは 100Mbps 前後で安定しており、平均通信レートは ASA5520 のカタログ指標を超えていないのに、 パケットドロップが不定期に頻発する。

```
ciscoasa# show interface
Interface GigabitEthernet0/0 "inside", is up, line protocol is up
  Hardware is i82546GB rev03, BW 1000 Mbps, DLY 10 usec
            Full-Duplex(Full-duplex), 1000 Mbps(1000 Mbps)
...
            699873 input errors, 0 CRC, 0 frame, 699873 overrun, 0 ignored, 0 abort
            41241173102 packets output, 40173518257598 bytes, 25103507 underruns
...
      1 minute input rate 3816 pkts/sec,  967980 bytes/sec
      1 minute output rate 5520 pkts/sec,  5005321 bytes/sec
      1 minute drop rate, 0 pkts/sec
      5 minute input rate 3031 pkts/sec,  1297990 bytes/sec
      5 minute output rate 2578 pkts/sec,  1156442 bytes/sec
```

平均レートが低い ≠ ASA が完全処理できる

エラーカウンターの意味

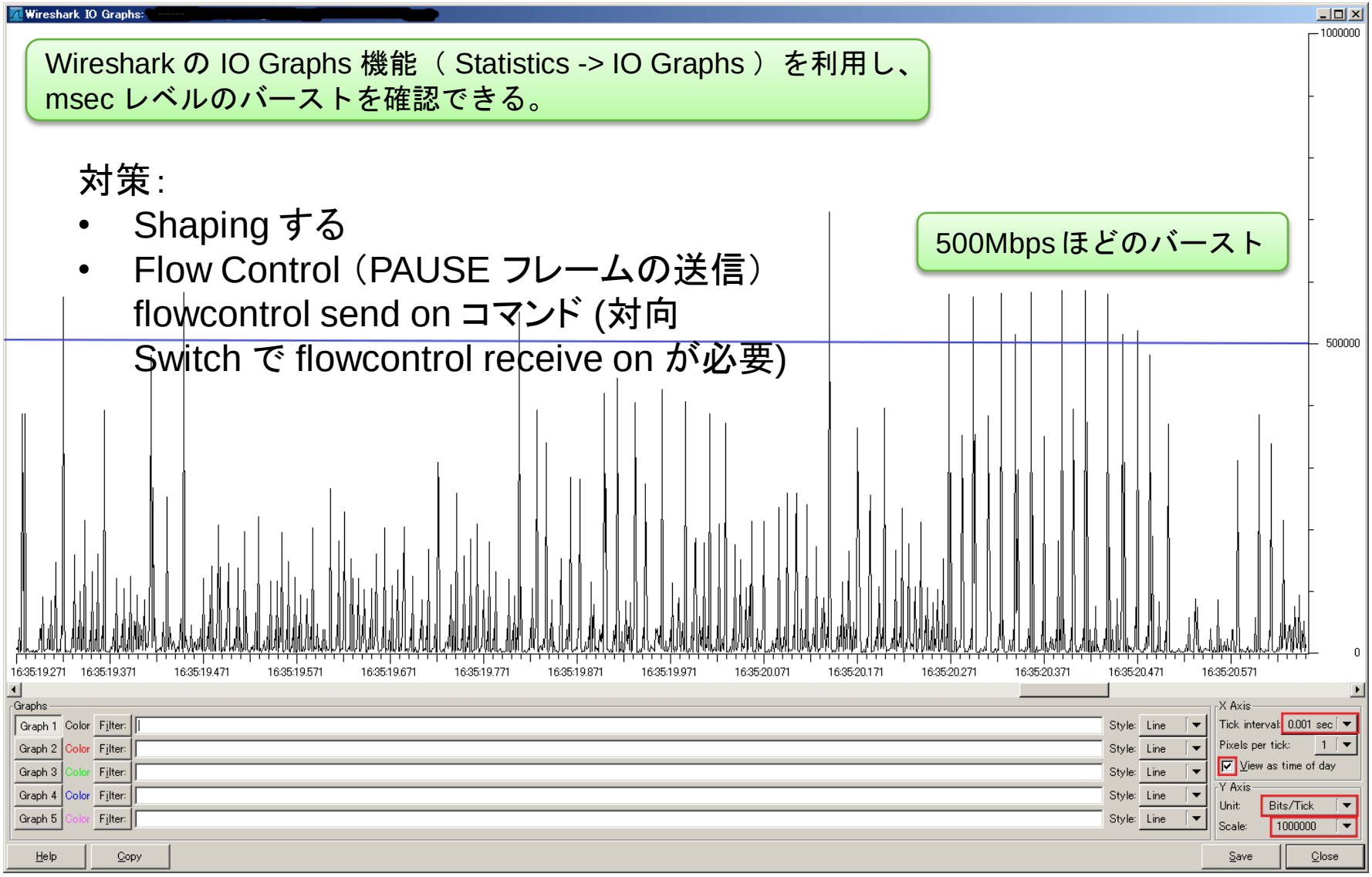
```
ciscoasa# show interface
Interface GigabitEthernet0/0 "internet", is up, line protocol is up
...
      789320 packets input, 307897342 bytes, 0 no buffer
      Received 0 broadcasts, 0 runts, 0 giants
      18 input errors, 0 CRC, 0 frame, 18 overrun, 0 ignored, 0 abort
      0 pause input, 0 resume input
      0 L2 decode drops
      3517869 packets output, 3024568394 bytes, 31 underruns
      0 pause output, 0 resume output
      0 output errors, 0 collisions, 2 interface resets
      0 late collisions, 0 deferred
      0 input reset drops, 0 output reset drops, 0 tx hangs
      input queue (blocks free curr/low): hardware (255/255)
      output queue (blocks free curr/low): hardware (255/254)
...
```

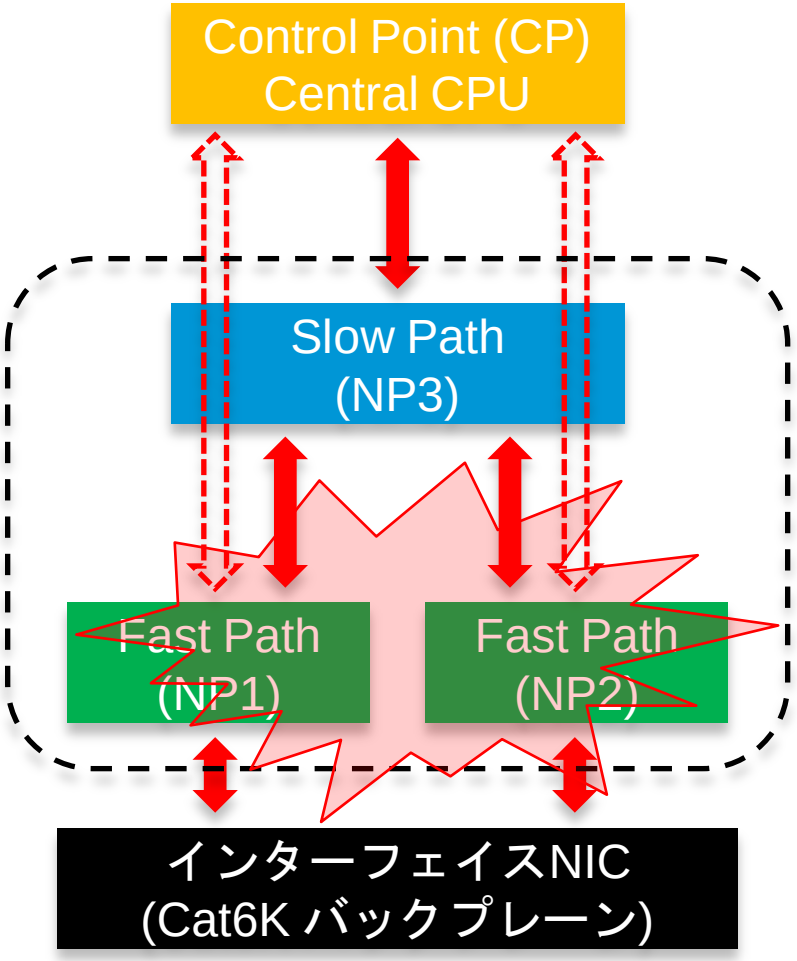
リソース不足で送受信処理できず、インターフェイスで破棄した際のカウンター

パケット破棄の主な理由

- **overrun**: Ethernet コントローラ・チップ内の受信バッファがフルのため、ワイヤーからパケットを受け取れない等
- **no buffer**: 受信したパケットを格納するバッファー（ASA のメインメモリ上のパケット・ブロック）が不足
- **underrun**: パケット・ブロックから Ethernet コントローラ・チップ上の送信バッファへ転送するためのキューがフルのため、送信が必要なパケットを NIC に転送できない

msec レベルのバースト





事例②: (FWSM) ネットワークプロセッサの過負荷

事象：Syslog サーバで Failover Interface test が開始したログが確認され、同時に一部の通信が不通になったが、しばらくすると自動復旧した。

%FWSM-1-105005: (Secondary) Lost Failover communications with mate on interface dmz
%FWSM-1-105008: (Secondary) Testing Interface dmz
%FWSM-1-105009: (Secondary) Testing on interface dmz Passed

Failover Hello パケットが
- 経路上ロスされ、受信できなかった
- 受信したが、リソース不足により処理できなかった

```
FWSM# show np blocks
                  MAX    FREE   THRESH_0   THRESH_1   THRESH_2
NP1 (ingress)   32768   19872        151    8945239   31260065
    (egress)   521206  521206          0          0          0
NP2 (ingress)   32768   32768          0          0          0
    (egress)   521206  521206          0          0          0
NP3 (ingress)   32768   32768          0        124        988
    (egress)   521206  521206          0          0          0
```

```
FWSM# show np all stats | include pause
PF_MNG: pause frames sent (x3)                    : 1238
PF_MNG: pause frames sent (x3)                    : 0
```

THRESH_x のカウンターは、NP 内パケット転送用のバッファーの量がその閾値以下まで減少した回数を示す

特に THRESH_0 が増加する場合、システム内部の制御用通信も破棄される

PAUSE フレームの送信は、NP1/2 バッファーの枯渇を示す

NP1 が過負荷

```
Cat6504E# show etherchannel summary | include Po
Group  Port-channel  Protocol    Ports
272    Po272(SU)         -      Gi3/1(P)    Gi3/2(P)    Gi3/3(P)

Cat6504E# show interfaces port-channel 272 counters etherchannel

Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Po272         58344382967      301711994              0        3840231
Gi3/1         55753226428      284455167              0              1
Gi3/2               172              1              0              1
Gi3/3         194046752           1001              0        2556838
Gi3/4               172              1              0              1
Gi3/5               172              1              0              1
Gi3/6         149622316         427132              0        1278426

Port           OutOctets   OutUcastPkts   OutMcastPkts   OutBcastPkts
Po272        128118829096      443011651       28065921       42947534
Gi3/1         57065955423      290209812        2566514              1
Gi3/2            97159788        1278417              0              1
Gi3/3                 240              2              0              1
Gi3/4              184028             29           2130             14
Gi3/5            23190248              1              0          32208
Gi3/6            92902905              1           2121          40037
```

NP1
NP2
NP1
NP2

FWSM と Cat6K 間の Port-Channel

FWSM → Cat6Kへの通信

通信が 偏っている

Cat6K → FWSMへの通信

- Port-channel 各ポートで通信量の偏りにより、特定の NP が過負荷になりうる
- IOS 側でポート間の負荷分散モードを調整できる（デフォルトは src-dst-ip）

通信が偏る原因を調べる

負荷分散モードは
src-dst-ip

通信が NP1 に偏っている

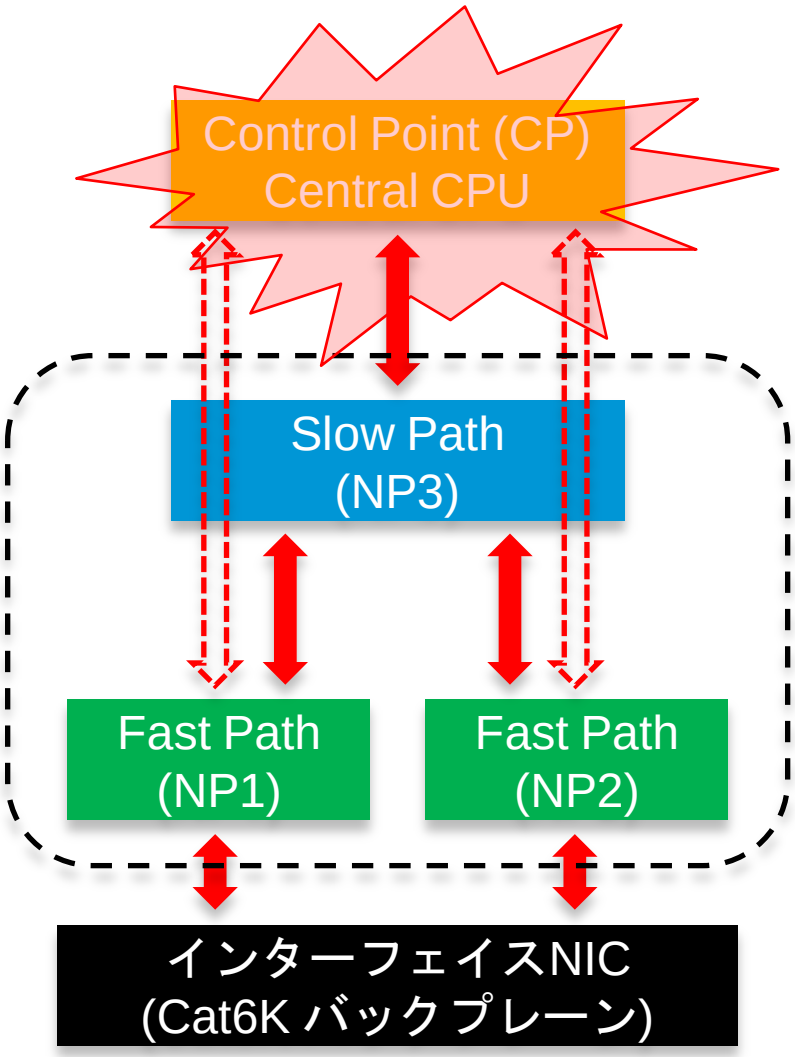
→ 特定 src/dst ip 間の通信が多発 → パケットキャプチャで ip を調べる → 二つの Malware に感染されたホストから不正の DNS 通信が大量に送信されていることを確認した

Catalyst 6500 側で SPAN を利用する

```
Cat6504E# show etherchannel summary | include Po
Group  Port-channel  Protocol    Ports
272    Po272(SU)         -      Gi3/1(P)    Gi3/2(P)    Gi3/3(P)

Cat6504E(config)# monitor session 1 source interface port-channel 272
Cat6504E(config)# monitor session  1 destination interface gigabitEthernet 1/1
```

FWSM 側で capture コマンドを利用する

```
FWSM(config)# access-list CAP permit ip any any

FWSM# capture CAP interface outside access-list CAP

FWSM# copy /pcap capture:CAP tftp:
```



事例③: (ASA) CPU 使用率が高い

事象：監視装置（SNMP Polling によるモニターリング）から、
ASA の CPU 使用率が時々 90% 以上に高騰することが観測される。

```
ciscoasa# show cpu
CPU utilization for 5 seconds = 86%; 1 minute: 82%; 5 minutes: 46%

ciscoasa# show processes cpu-usage sorted non-zero
PC         Thread       5Sec     1Min     5Min   Process
0x081ecc51   0x6ddc0f3c    85.4%    81.1%    45.0%   Dispatch Unit
0x08e1e785   0x6ddb7e1c     0.0%     0.1%     0.0%   ssh
```

Dispatch Unit
は原因のプロセス

```
Ciscoasa# show xlate count
113 in use, 1161 most used

ciscoasa# show conn count
189 in use, 2008 most used

ciscoasa# show interface | include err
0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
        84967728 packets output, 61743320357 bytes, 0 underruns
        0 output errors, 0 collisions, 0 interface resets
        0 late collisions, 0 deferred
...
```

しかし、xlate数、
conn数は多くない

Interface 上もエラー
がカウントされず

Dispatch Unit の仕事を増やしたものは？

- Dispatch Unit はASA 内の各機能モジュール間でパケットの搬送を行うプロセス
- CPU 使用率が高くなる場合、Dispatch Unit は直接の原因となるのは一般的
- ただ、根本原因は別にある可能性を考慮する必要がある

•Logging 設定は、logging trap informational のみで、問題なさそう

•Logger プロセスの CPU 使用率が低い

•監視機器の SNMP polling間隔は CPU 使用率が高くなる間隔と一致しない

•snmp / SNMP Notify Thread プロセスの CPU 使用率が低い

•Syslog
•管理通信（Telnet/SSH/HTTPS/SNMP）
•レイヤー７の Inspection
•AAA(Radius / TACACS+)
•Failover 通信
•ルーティングプロトコル

CP で処理されるパケット

```
ciscoasa# show service-policy

Global policy:
  Service-policy: global_policy
    Class-map: inspection_default
......
      Inspect: rtsp, packet 6321392, drop 0, reset-
drop 0
               tcp-proxy: bytes in buffer 0, bytes
dropped 0
......
```

RTSP 通信の大量発生が原因

RTSP は動画ストリーミングで利用するプロトコル

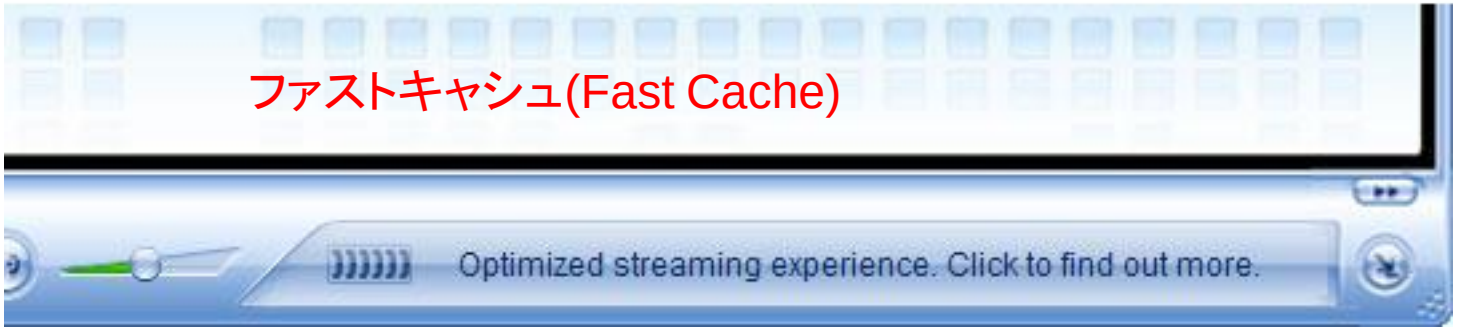
```
ciscoasa# show clock
12:16:44.585 JST Sun Nov 20 2011
Ciscoasa# show service-policy inspect rtsp | include packet
      Inspect: rtsp, packet 432464, drop 0, reset-drop 0
ciscoasa#
ciscoasa# show clock
12:16:47.625 JST Sun Nov 20 2011
Ciscoasa# show service-policy inspect rtsp | include packet
      Inspect: rtsp, packet 456696, drop 0, reset-drop 0
```

10個の動画再生セッションで 10000 packet/sec の RTSP パケットが観測される

再現環境では、10個の動画再生セッションでCPU使用率が一時 50% を超え、同時に、動画再生が途中で止まるなどの問題を観測した。

対策：
- ファストキャッシュ無効化
- inspect rtsp を無効化

RTSP パケットが大量発生する原因は：



トラブルシューティングの考え方

流れ:

1. 影響された通信を把握する (src/dst ip/port, protocol)
2. 通信経路を追跡する
3. 経路上の被疑機器を絞る
4. 被疑機器におけるパケットフローに基づき、被疑機能(モジュール)を絞る
5. 対策を検討する

ツール:

- Syslog
- show コマンドの出力
- パケットキャプチャ
- packet-tracer
- debug コマンドの出力

英語資料

- Cisco ASA 5500 Series Adaptive Security Appliances Configuration Guide
  http://www.cisco.com/en/US/products/ps6120/products_installation_and_configuration_guides_list.html
- Cisco ASA 5500 Series Adaptive Security Appliances Command References
  http://www.cisco.com/en/US/products/ps6120/prod_command_reference_list.html
- Cisco ASA 5500 Series Adaptive Security Appliances Error and System Messages
  http://www.cisco.com/en/US/products/ps6120/products_system_message_guides_list.html
- Cisco Catalyst 6500 Series Firewall Services Module Configuration Guide
  http://www.cisco.com/en/US/products/hw/modules/ps2706/products_installation_and_configuration_guides_list.html
- Cisco ASA 5500 Migration to Version 8.3 and Later
  http://www.cisco.com/en/US/docs/security/asa/asa83/upgrading/migrating.html
- PIX/ASA 7.x and FWSM: NAT and PAT Statements
  http://www.cisco.com/en/US/products/ps6120/products_configuration_example09186a008046f31a.shtml
- PIX/ASA: Monitor and Troubleshoot Performance Issues
  http://www.cisco.com/en/US/products/hw/vpndevc/ps2030/products_tech_note09186a008009491c.shtml
- Single TCP Flow Performance on Firewall Services Module (FWSM)
  https://supportforums.cisco.com/docs/DOC-12668

日本語資料

- Cisco ASA 5500 シリーズ マニュアル
  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/index_sec_asa.shtml
- Firewall Services Module マニュアル
  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/index_sw_cat6500.shtml
- Cisco ASA 5500 バージョン 8.3 用移行ガイド
  http://www.cisco.com/japanese/warp/public/3/jp/service/manual_j/sec/asa/mg83/OL-22176-01-J.pdf
- PIX/ASA 7.x および FWSM：NAT と PAT の設定例
  http://www.cisco.com/cisco/web/support/JP/102/1020/1020420_pix70-nat-pat-j.html
- PIX/ASA：パフォーマンスの問題の監視とトラブルシューティング
  http://www.cisco.com/cisco/web/support/JP/102/1021/1021301_pixperformance-j.html

次回予告

トピック:
Cisco Unified Computing System (UCS) に関する内容*

日程: 2012年3月27日

***内容の詳細は、決定次第サポートコミュニティ上でご案内いたします。**

ソーシャルメディアを使って
シスコサポートコミュニティと繋がろう

http://www.facebook.com/CiscoSupportCommunityJapan

https://twitter.com/cscjapan

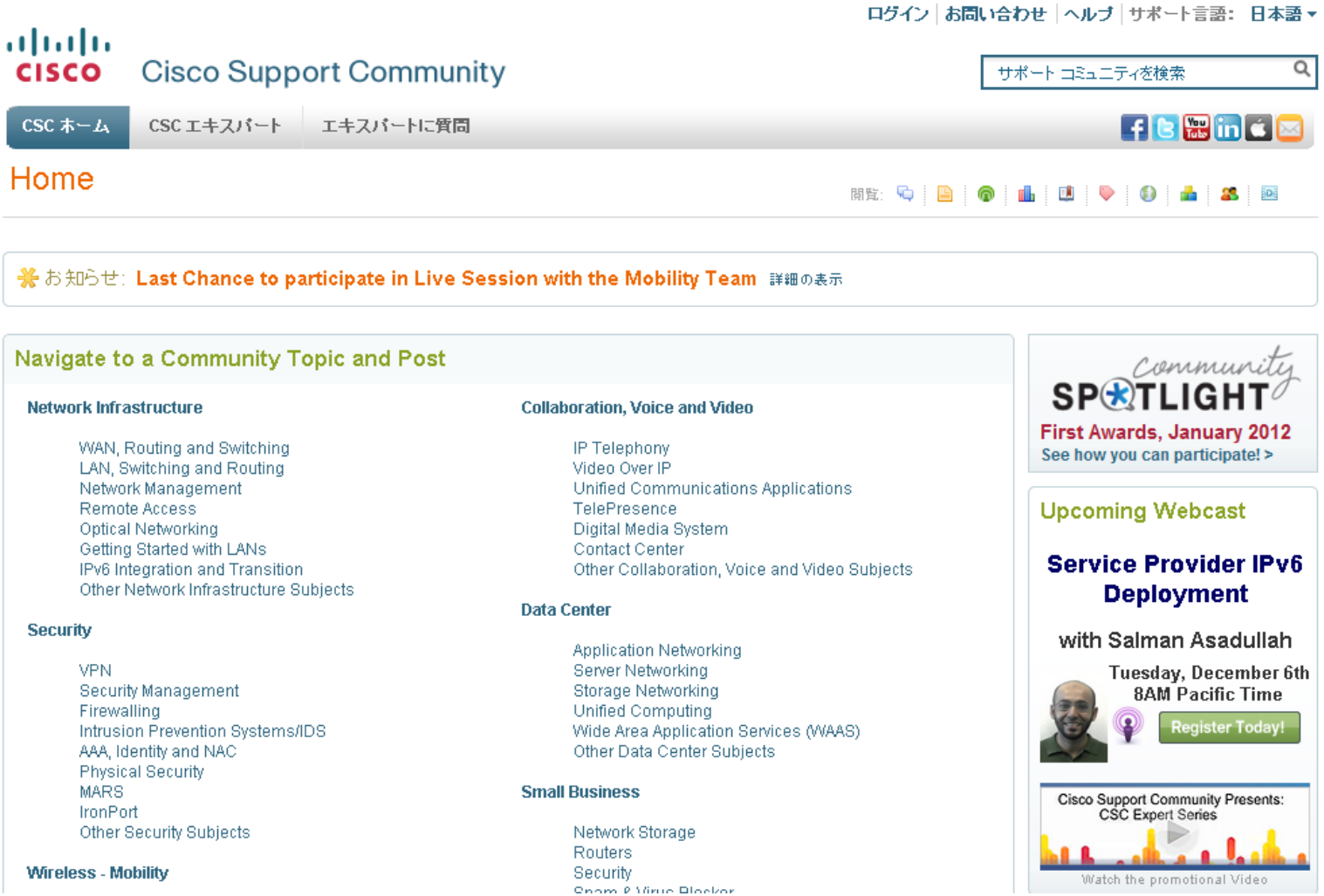
http://www.youtube.com/user/ciscosupportchannel

http://itunes.apple.com/us/app/cisco-technical-support/id398104252?mt=8

http://www.linkedin.com/groups/CSC-Cisco-Support-Community-3210019

英語版サポートコミュニティ

https://supportforums.cisco.com



シスコ認定ラーニングパートナー

スペシャリゼーション	ラーニングパートナー	リンク
データセンター	NGN-SF	http://ngn-sf.co.jp/
データセンター	ネットワンシステムズ	https://www.netone.co.jp/academy/index.html
コラボレーション	グローバルナレッジ	http://www.globalknowledge.co.jp/

- シスコ認定ラーニングパートナーでは皆様のソリューションを最適化するために、Ciscoの認定したカリキュラムを使ったトレーニングを提供しております。

- また、シスコ認定ラーニングパートナーの中でも、シスコスペシャライズドパートナーは特にその専門分野においてのスキルを認められたパートナーのみが授与される認定資格となっております。


CISCO