NETSCOUT

C9 Flow技術まとめ ～基礎から最新動向・応用まで～

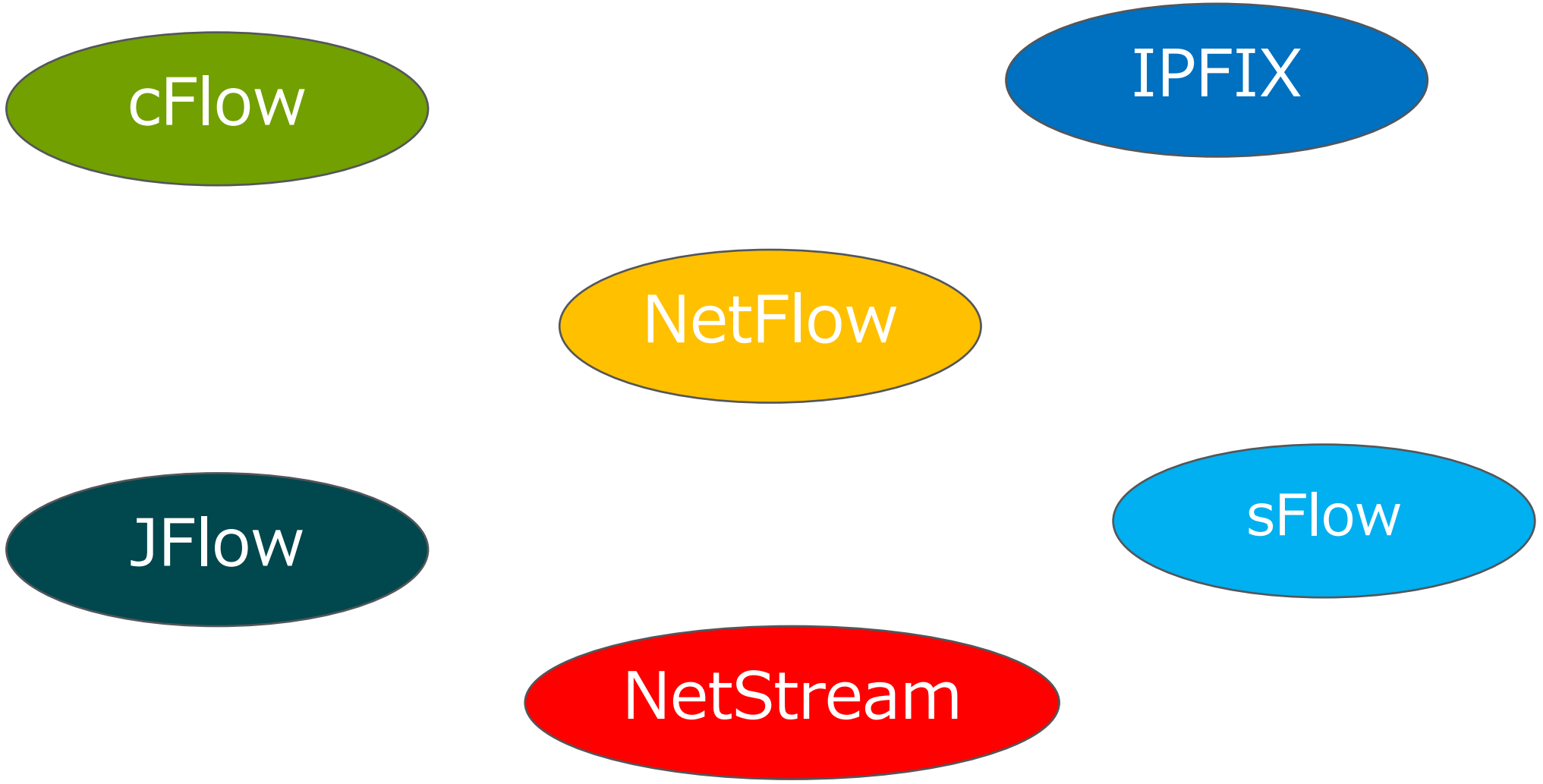
Flow技術入門

Internet week 2023

Takashi Sasaki

SE Director, Service Provider Sales, Japan

Flow技術とは



Flow技術とは

ルータやスイッチ等のデバイスが
トラフィックの統計情報を収集する技術

20年以上前から存在

一般的に利用されるようになったのは2010年（？）頃から

Flowの種類

NetFlow Version 5

NetFlow Version 9 (RFC 3954, 2004年)

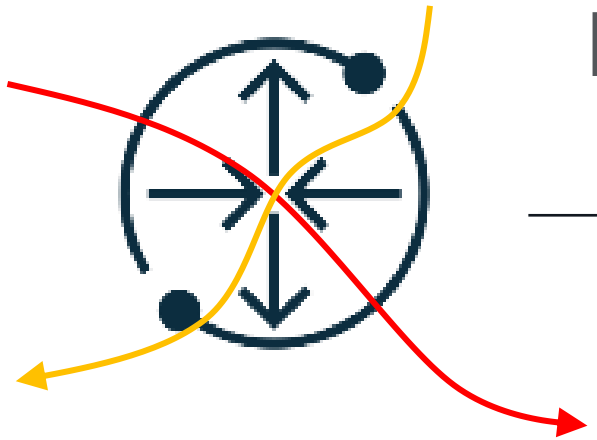
NetFlow Version 10 = IPFIX (RFC 5655, 2009年)

sFlow Version 4 (RFC 3176, 2001年)

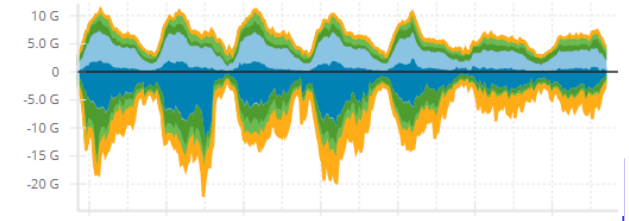
sFlow Version 5 （2004年）

Flow

通信の可視化



トラフィックの統計情報
（Flow）



可視化ツール
（フローコレクタ）

トラフィック

トラフィックモニタリングの手法

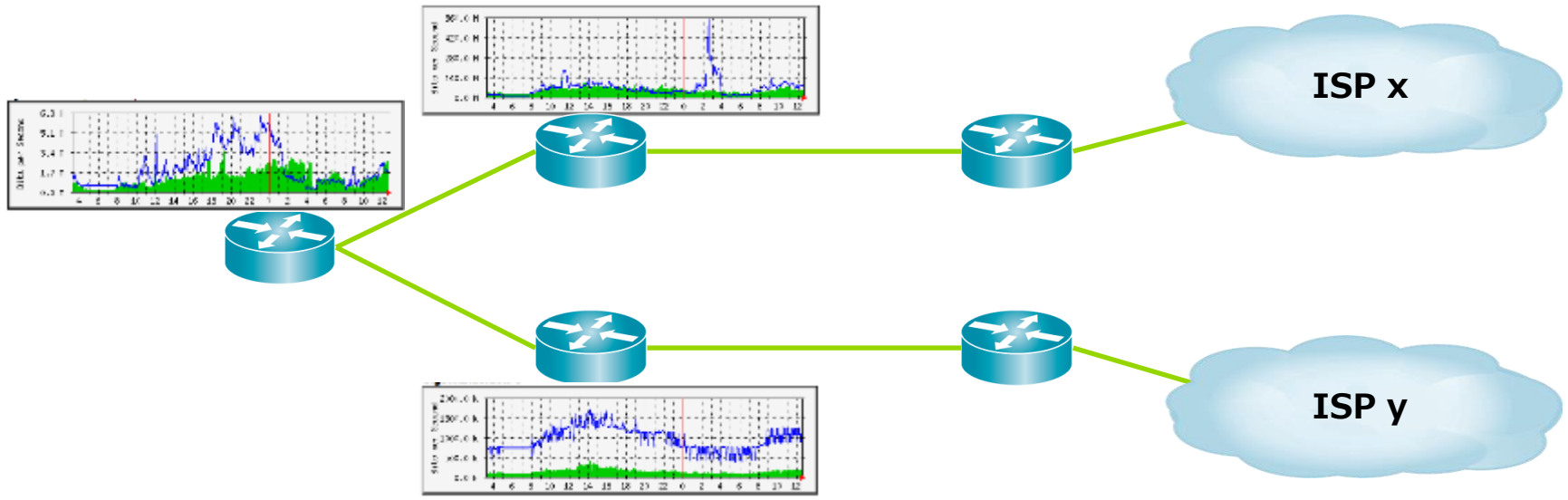
代表的なトラフィックモニタリング手法

- SNMP
- パケットキャプチャ
- NetFlow/sFlow

SNMPによるトラフィックのモニタリング

ルータ/スイッチからのSNMPによる統計情報
MRTG/Cactiによるグラフ化が一般的

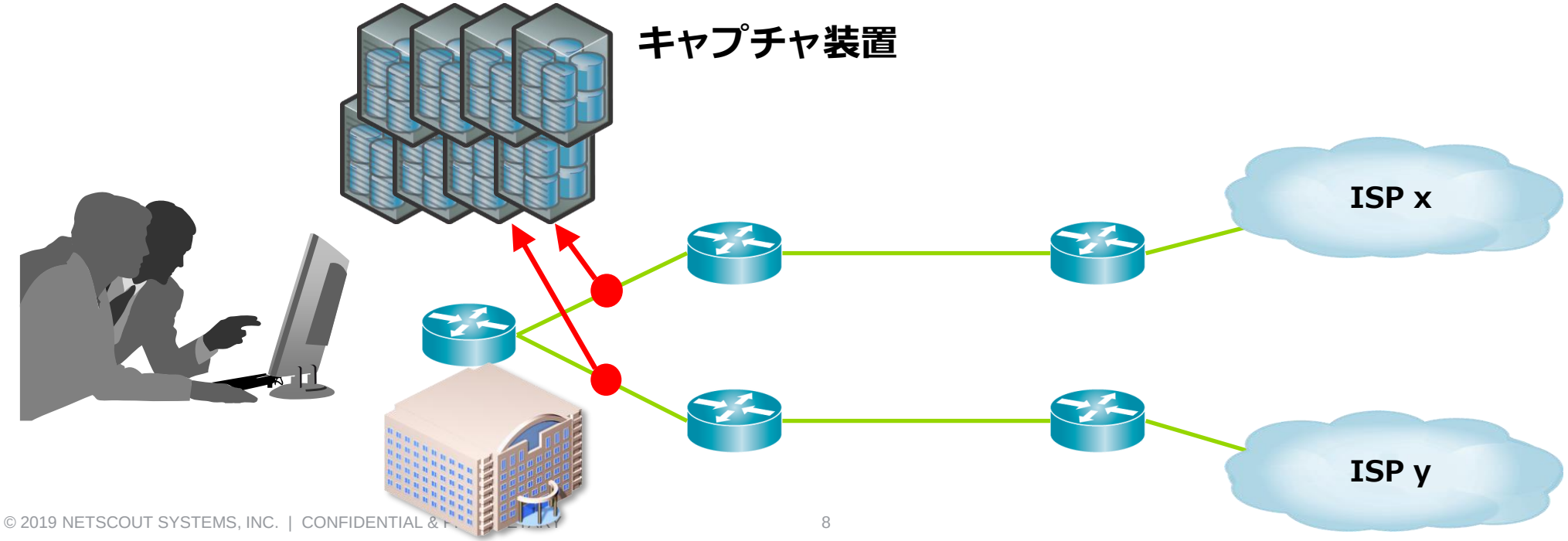
インターフェース単位での**流量の取得**
サービス、送信先・送信元等の情詳細報は得られない。



パケットキャプチャによるモニタリング

SPAN/TAPによりトラフィックをキャプチャ（若しくはインラインで）
ペイロードを含むすべての通信分析が可能

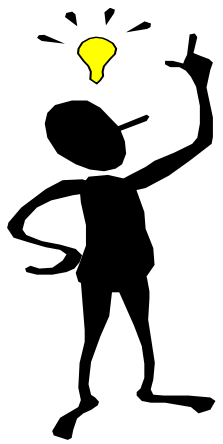
流量や保存容量による制限
まだまだ高価（？）



Flowによるモニタリング

少ない投資で**ネットワーク全体**を可視化、モニタリングすることに最適

- パケット長、プロトコル別、サービス別通信量
- トラフィックの地理的分布
- ルータ、インターフェイス単位での通信量
- トップトーカー
- ネットワークセキュリティ（DDoS攻撃等）監視　等々・・



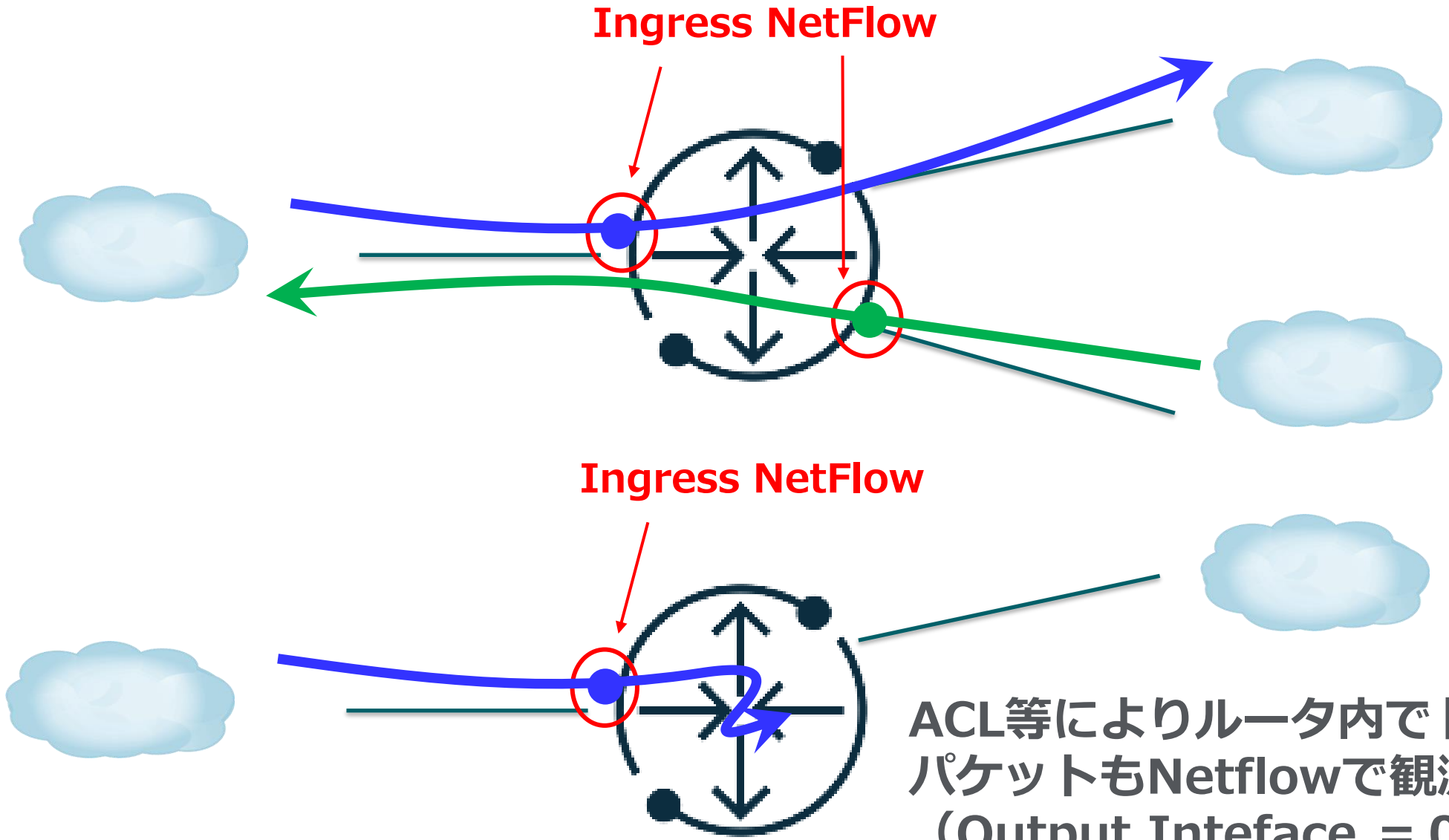
Flowレコードとは

- NetFlowレコードには以下が含まれます（一部抜粋）
  - ✓ Source/Destination IP
  - ✓ Source/Destination Port
  - ✓ L3 Protocol Type
  - ✓ ToS / TCP frag
  - ✓ In/Out Interface(ifIndex)
  - ✓ Packet数 / Byte数

NetFlowの有効化

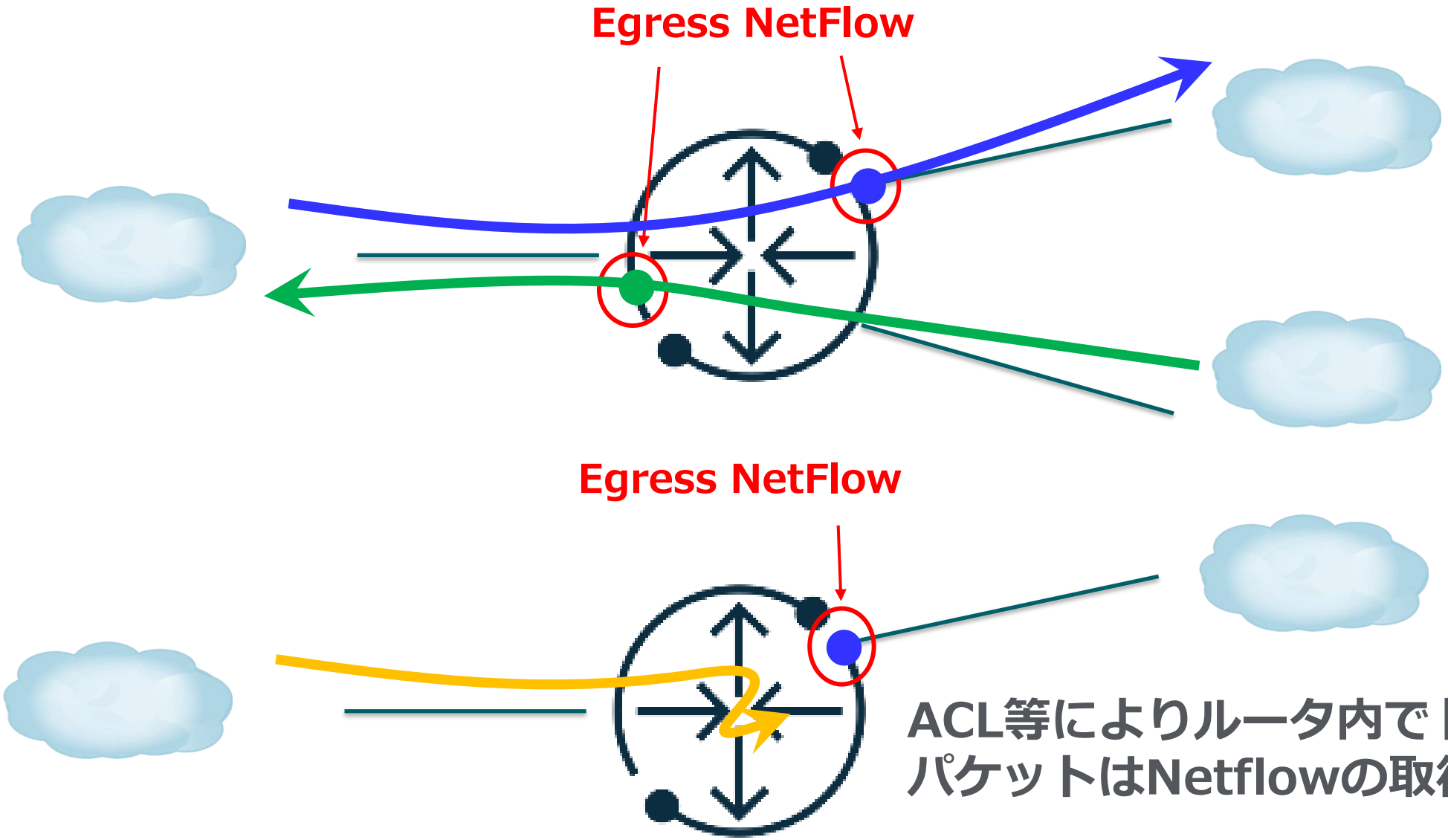
- NetFlowは各インターフェイス単位で有効化ができます
- Ingress/Egressで有効化オプションがあります
- Egress NetFlowを使った場合、ルータ内でDropされたパケットはカウントできなくなります
- Ingress/Egress両方をEnableにした場合は、コレクター側でダブルカウントされる可能性があります

NetFlowの有効化 (Ingress)



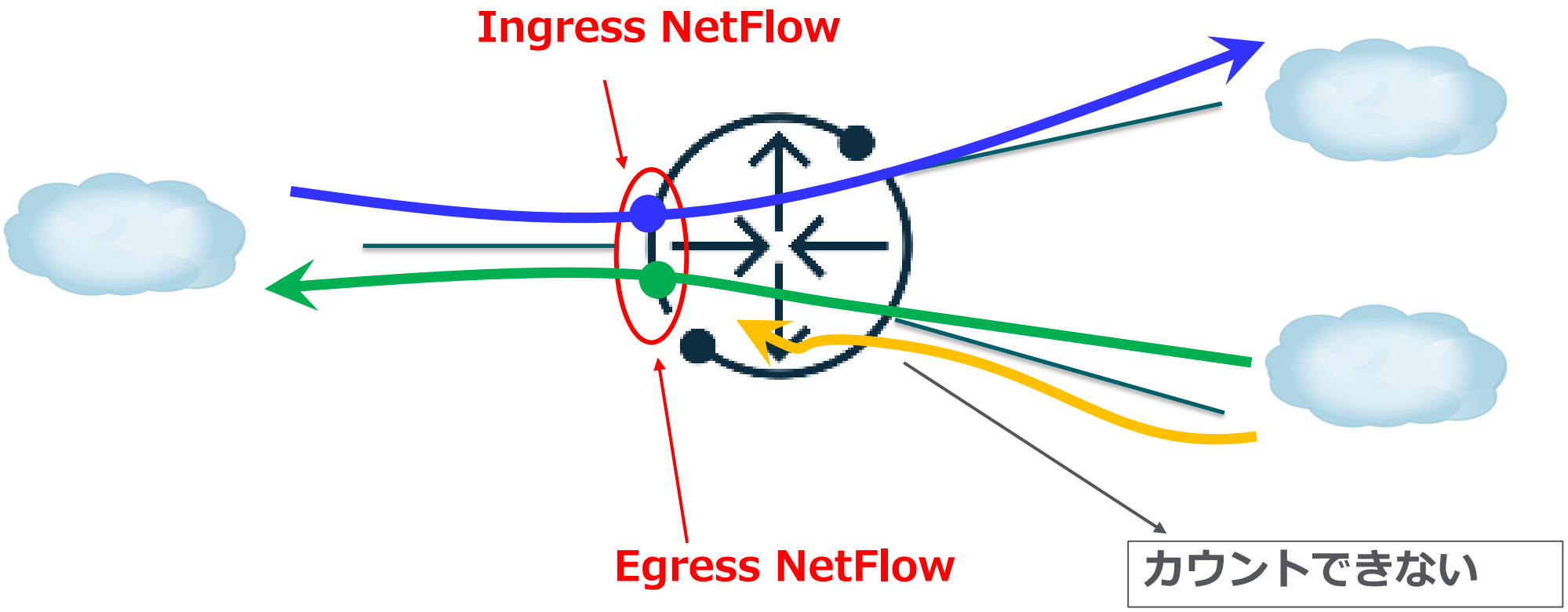
ACL等によりルータ内でドロップした
パケットもNetflowで観測が可能
（Output Inteface ＝0）

NetFlowの有効化 (Egress)



ACL等によりルータ内でドロップした
パケットはNetflowの取得が不可

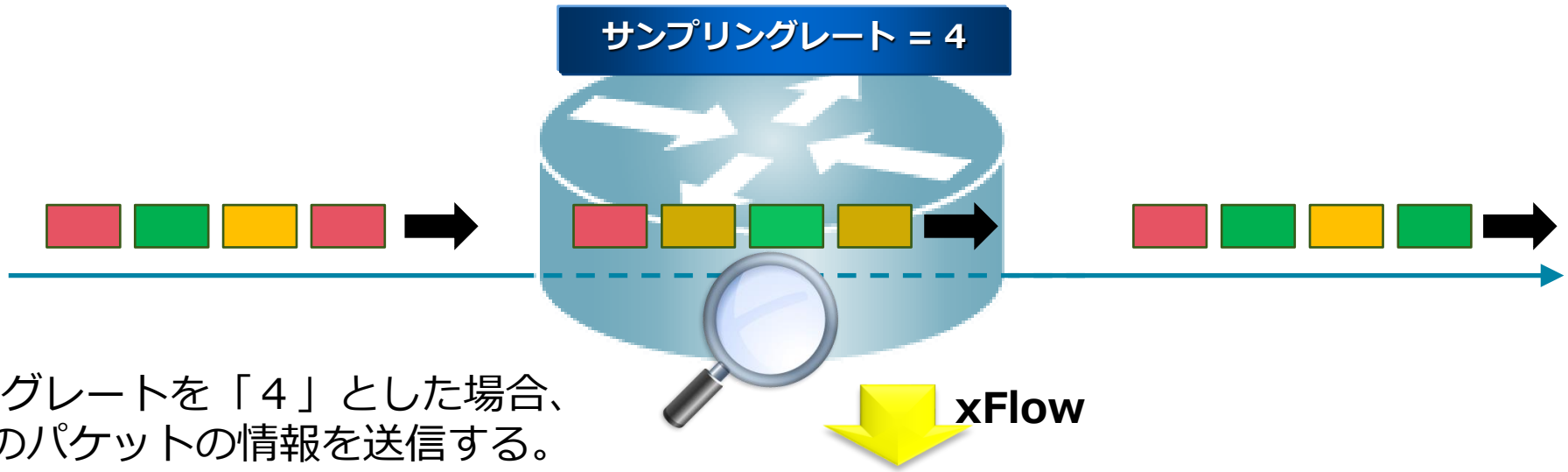
NetFlowの有効化 (Ingress + Egress)



特定インターフェイスのin/outだけを可視化する場合は有効

サンプリングについて

実際にネットワークのバックボーンでxflowを運用する際は、サンプリングによって統計情報を取得する。トラフィック量が多い場所では、数学的には実値と近似値となる。



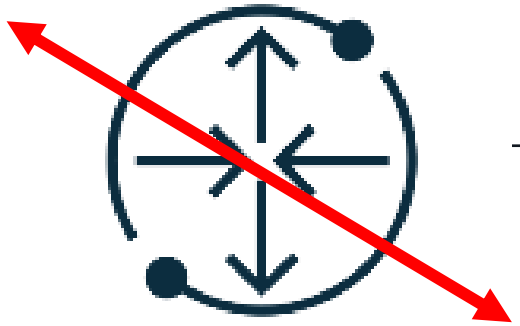
サンプリングレートを「４」とした場合、
4つに１つのパケットの情報を送信する。

サンプリングレート

- すべての通信を収集する（1/1)ことはルータ及びフローコレクタの能力的に問題があるため、実際の運用ではサンプリングを用いるケースが多い
- 一般的には1/1000 ～ 1/32000
- サンプリングレートを上げる ＝ ルータからのFlow送出が増える
- サンプリングレートを下げる ＝ルータからのFlow送出が減る

サンプリングレート

サンプリングレート　1/1000



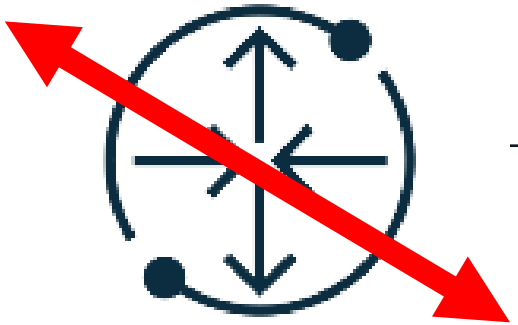
5000 FPS

10000 FPSまで

可視化ツール
（フローコレクタ）

サンプリングレート

サンプリングレート　1/1000



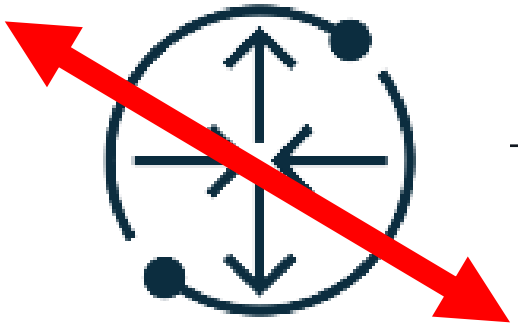
8000 FPS

10000 FPSまで

可視化ツール
（フローコレクタ）

サンプリングレート

サンプリングレート　1/2000



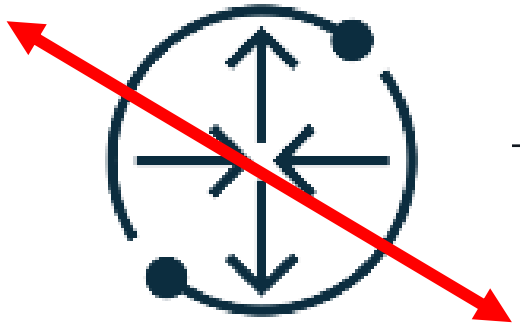
4000 FPS

10000 FPSまで

可視化ツール
（フローコレクタ）

サンプリングレート

サンプリングレート　1/1000



5000 FPS

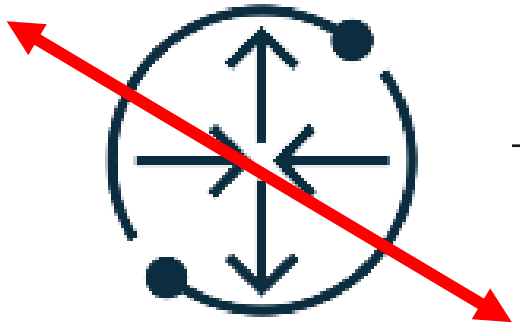
10000 FPSまで

可視化ツール
（フローコレクタ）

ルータ自身の制限　7000FPSまで（例）

サンプリングレート

サンプリングレート　1/2000



2500FPS

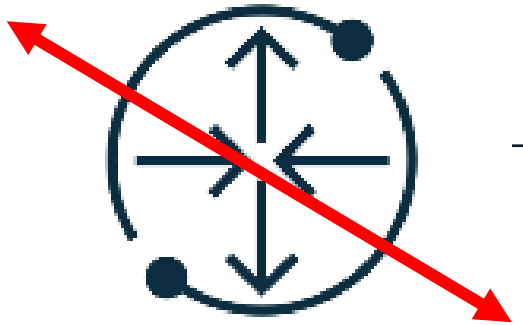
10000 FPSまで

可視化ツール
（フローコレクタ）

ルータ自身の制限　7000FPSまで（例）

サンプリングレート

サンプリングレート　1/2000



5000FPS

10000 FPSまで

可視化ツール
（フローコレクタ）

3000FPS

サンプリングレート　1/4000

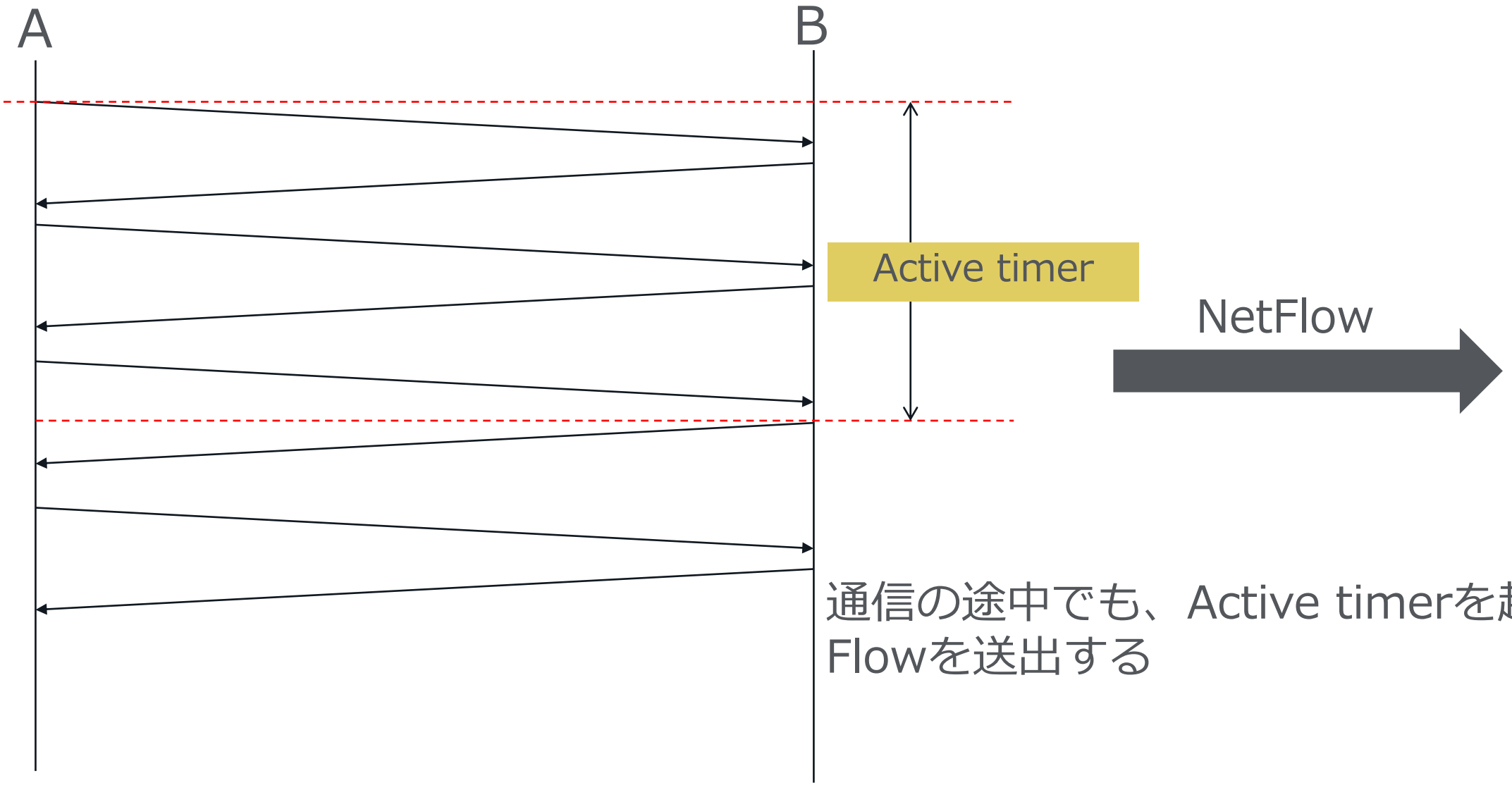
2000FPS

サンプリングレート　1/8000

NetFlowのタイマー

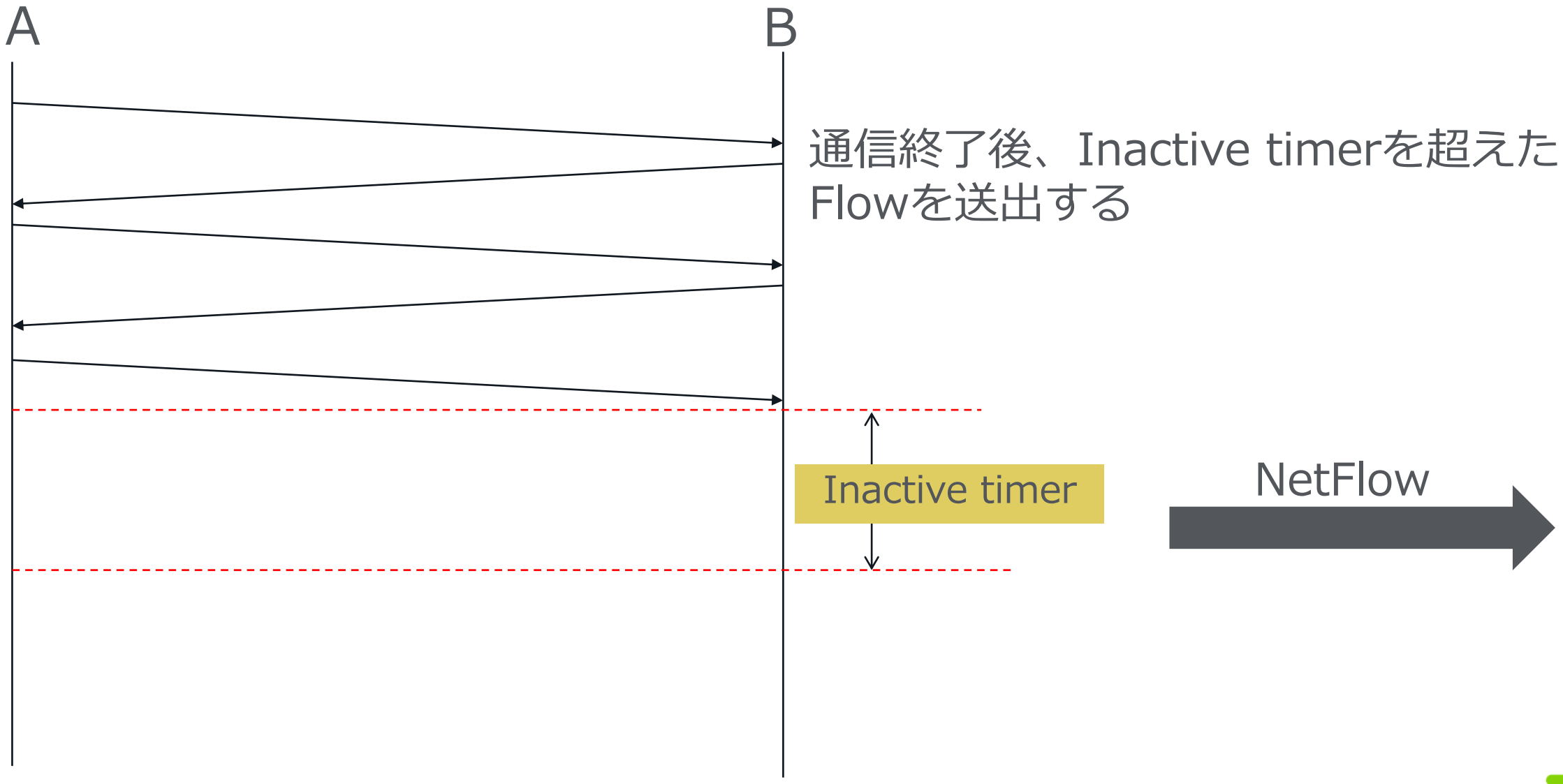
- NetFlowを送出するタイミングをタイマーで決定できます
- Active Timer => 通信が継続していてもTimerの時間が経過したらNetFlowを送出する
- Inactive Timer => 通信が停止してからTimerの時間が経過したらNetFlowを送出する

NetFlowのタイマー (Active Timer)



通信の途中でも、Active timerを超えたらFlowを送出する

NetFlowのタイマー (Inactive Timer)



フローコレクタの種類

- 商用版
  - 企業向け
  - 通信事業者向け
  - Flow以外の情報を組み合わせて、多角的に可視化
  - セキュリティ要素
- オープンソース
  - 無償でとりあえず試してみる
  - 導入・実装に困難な面も

Thank You.

www.netscout.com

NETSCOUT

C9 Flow技術まとめ ～基礎から最新動向・応用まで～

最新のFlow技術をキャッチアップ1

Internet week 2023

Takashi Sasaki

SE director, Service Provider Sales, Japan

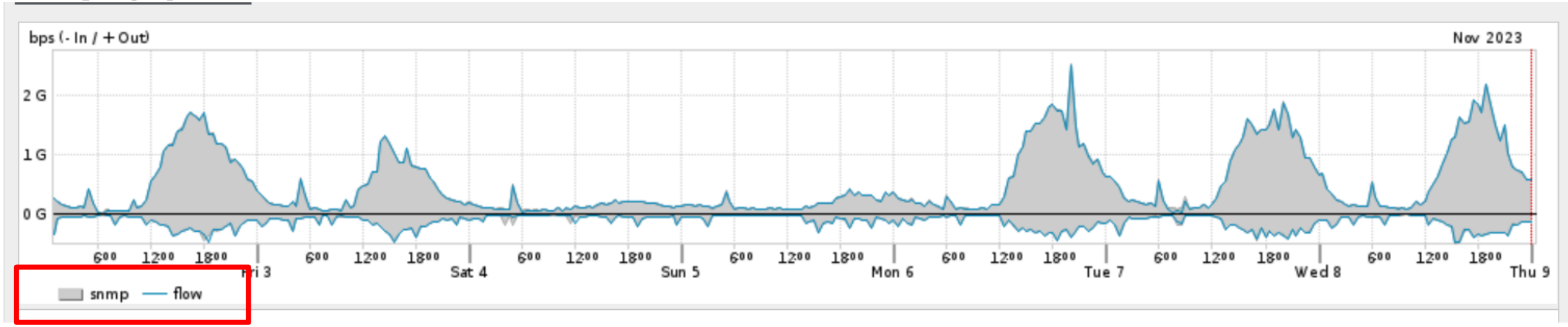
NetFlow送出の正当性の確認

ルータの能力や、設定ミス（例えばサンプリングレート）、Flowパケットのドロップ等によりNetFlowの正当性が疑われるケースがあります。

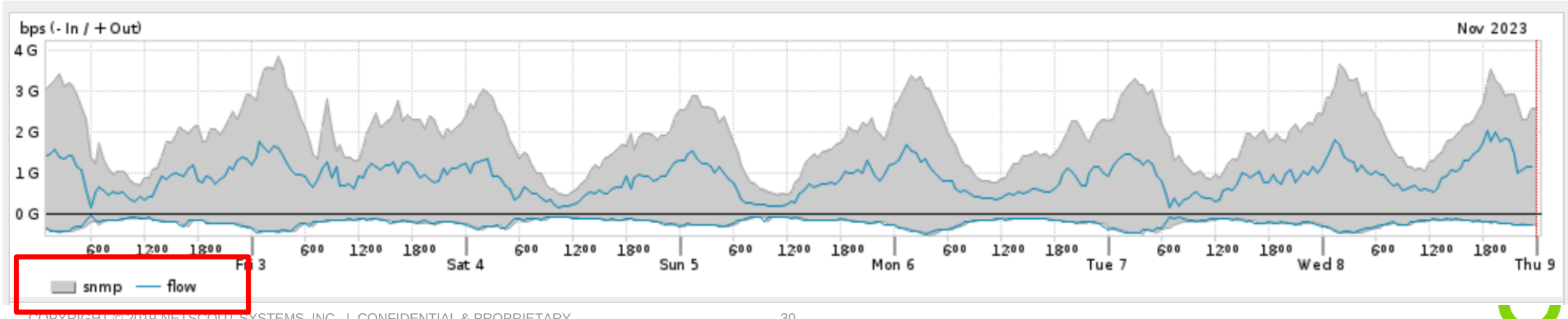
SNMPとFlowで取得したトラフィック量を比較する事で、Flowの正当性が確認できます

NetFlow送出の正当性の確認

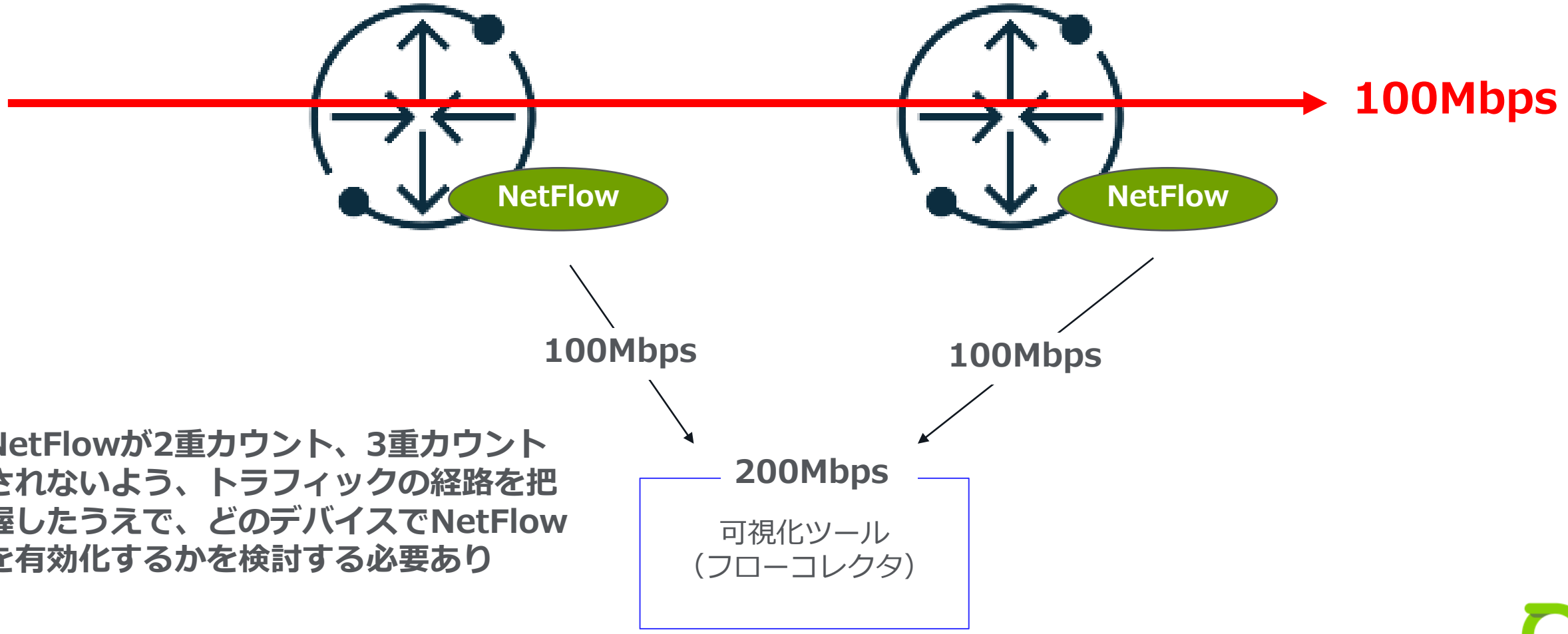
正常な状態



問題が発生している場合

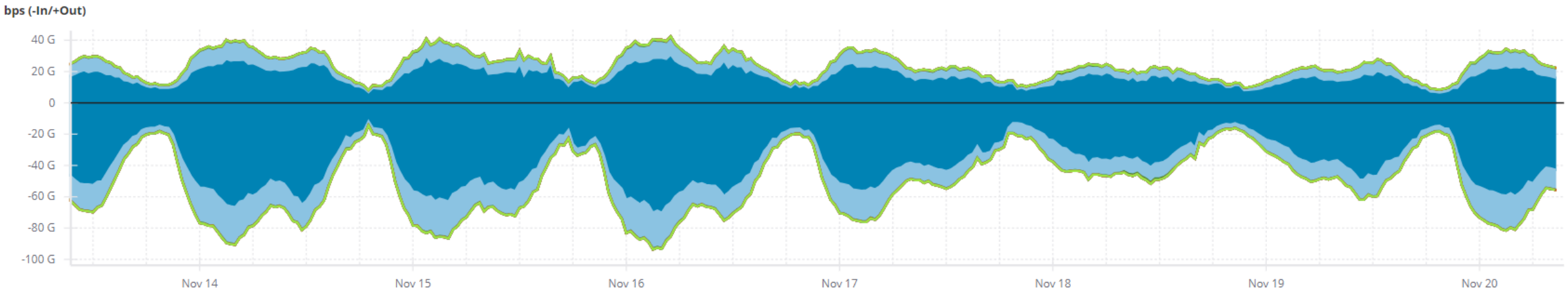


NetFlowのダブルカウント



NetFlowが2重カウント、3重カウントされないよう、トラフィックの経路を把握したうえで、どのデバイスでNetFlowを有効化するかを検討する必要あり

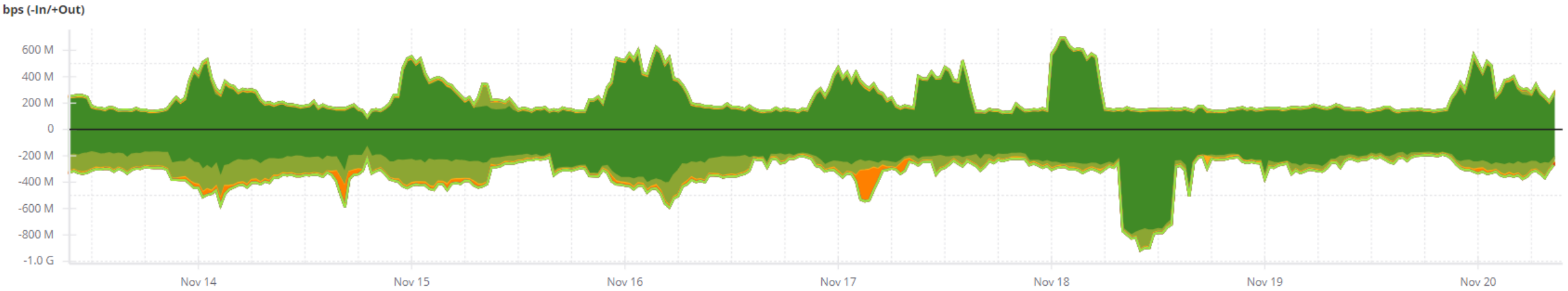
可視化レポート（プロトコル別）



Showing 25 items

Legend	Protocol	Number	Average (In)	Average (Out)	Average (In + Out)	% Total
A -	tcp	6	39.31 Gbps	17.48 Gbps	56.79 Gbps	75.38%
B -	udp	17	12.10 Gbps	5.861 Gbps	17.96 Gbps	23.84%
C -	esp	50	254.8 Mbps	239.5 Mbps	494.2 Mbps	0.66%
D -	gre	47	67.53 Mbps	3.516 Mbps	71.05 Mbps	0.09%
E -	icmp	1	8.142 Mbps	6.804 Mbps	14.95 Mbps	0.02%
F -	ah	51	8.491 Mbps	1.684 Mbps	10.17 Mbps	0.01%
G -	ipv6	41	12.37 Kbps	151.2 Kbps	163.5 Kbps	0.00%
H -	l2tp	115	36.67 Kbps	3.000 bps	36.67 Kbps	0.00%
I -	ipv6-icmp	58	40.00 bps	378.0 bps	418.0 bps	0.00%
J -	vrrp	112	0.000 bps	355.0 bps	355.0 bps	0.00%

可視化レポート（プロトコル別）

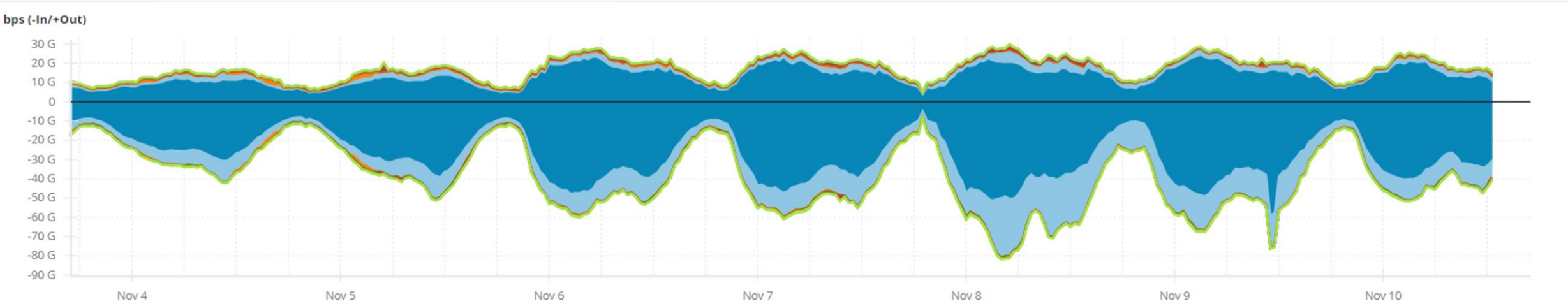


Showing 25 items

Legend	Protocol	Number	Average (In)	Average (Out)	Average (In + Out)	% Total
	tcp	6	39.31 Gbps	17.48 Gbps	56.79 Gbps	75.38%
	udp	17	12.10 Gbps	5.861 Gbps	17.96 Gbps	23.84%
C -	esp	50	254.8 Mbps	239.5 Mbps	494.2 Mbps	0.66%
D -	gre	47	67.53 Mbps	3.516 Mbps	71.05 Mbps	0.09%
E -	icmp	1	8.142 Mbps	6.804 Mbps	14.95 Mbps	0.02%
F -	ah	51	8.491 Mbps	1.684 Mbps	10.17 Mbps	0.01%
G -	ipv6	41	12.37 Kbps	151.2 Kbps	163.5 Kbps	0.00%
H -	l2tp	115	36.67 Kbps	3.000 bps	36.67 Kbps	0.00%
I -	ipv6-icmp	58	40.00 bps	378.0 bps	418.0 bps	0.00%
J -	vrrp	112	0.000 bps	355.0 bps	355.0 bps	0.00%

小容量通信に特化した可視化

可視化レポート（Port別）

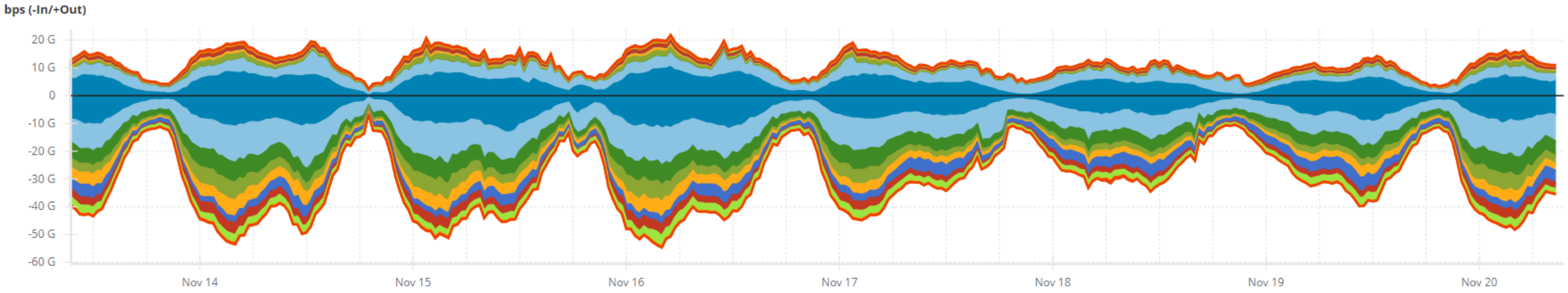


Showing 100 items

Legend	Application	Port	Average (In)	Average (Out)	Average (In + Out)	% Total
A -	https	443	27.95 Gbps	13.31 Gbps	41.26 Gbps	72.15%
B -	www-http	80	9.944 Gbps	2.197 Gbps	12.14 Gbps	21.23%
F -	ssh	22	154.1 Mbps	311.5 Mbps	465.6 Mbps	0.81%
G -	6180	6180	12.42 Mbps	368.0 Mbps	380.4 Mbps	0.67%
D -	targus-getdata1	5201	148.2 Mbps	173.6 Mbps	321.8 Mbps	0.56%
C -	rootd	1094	299.0 Mbps	19.93 Mbps	318.9 Mbps	0.56%
H -	synapse	2880	70.76 Mbps	231.5 Mbps	302.3 Mbps	0.53%
I -	http-alt	8080	82.08 Mbps	207.1 Mbps	289.2 Mbps	0.51%

さっくりとしたアプリケーション別の可視化

可視化レポート（パケットサイズ別）

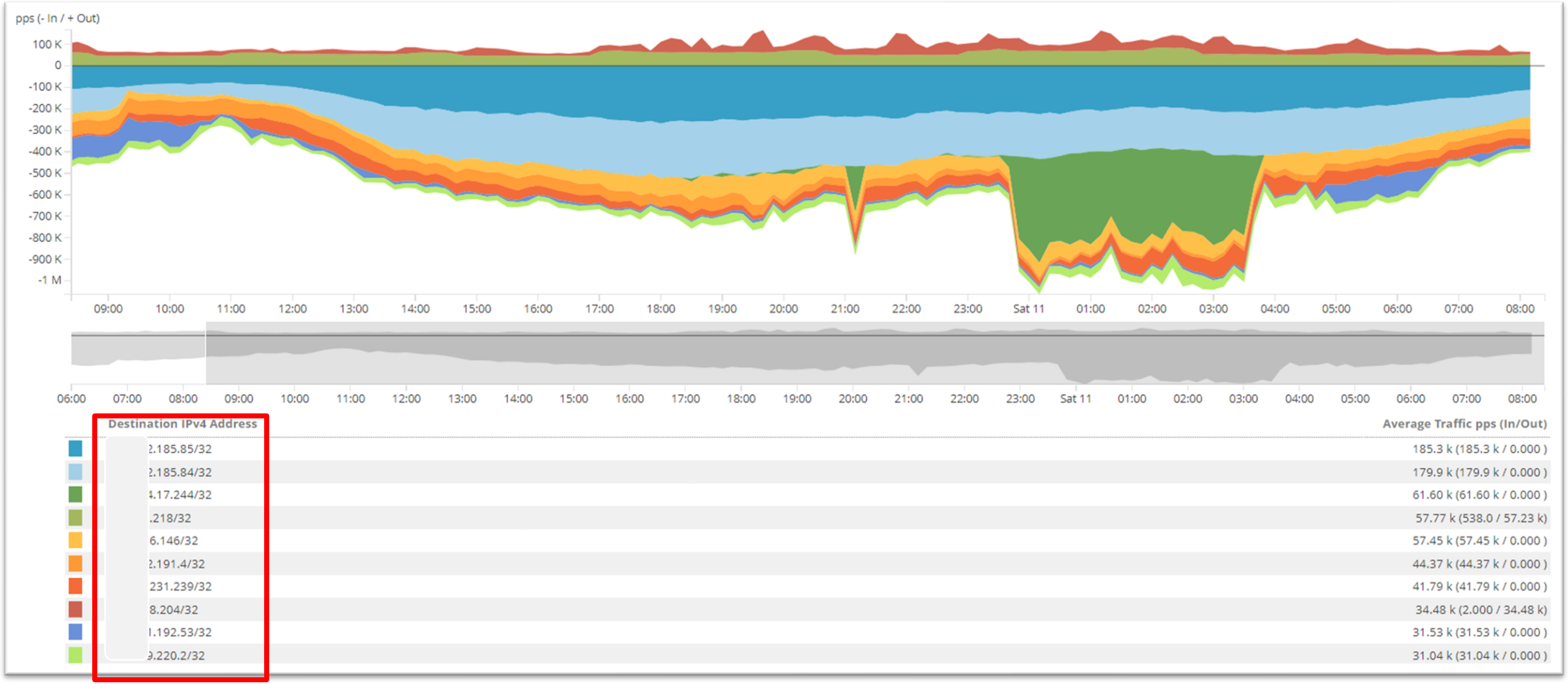


Showing 74 items

Legend	Packet Length	Average (In)	Average (Out)	Average (In + Out)	% Total
A -	1290	6.507 Gbps	5.469 Gbps	11.98 Gbps	19.76%
B -	1500	8.151 Gbps	3.636 Gbps	11.79 Gbps	19.45%
C -	1448	4.555 Gbps	38.29 Mbps	4.594 Gbps	7.58%
D -	1278	2.808 Gbps	890.6 Mbps	3.699 Gbps	6.10%
E -	1422	2.586 Gbps	374.3 Mbps	2.961 Gbps	4.89%
I -	1400	2.810 Gbps	103.1 Mbps	2.913 Gbps	4.81%
H -	1260	1.994 Gbps	752.4 Mbps	2.747 Gbps	4.53%
J -	1496	1.929 Gbps	97.45 Mbps	2.026 Gbps	3.34%

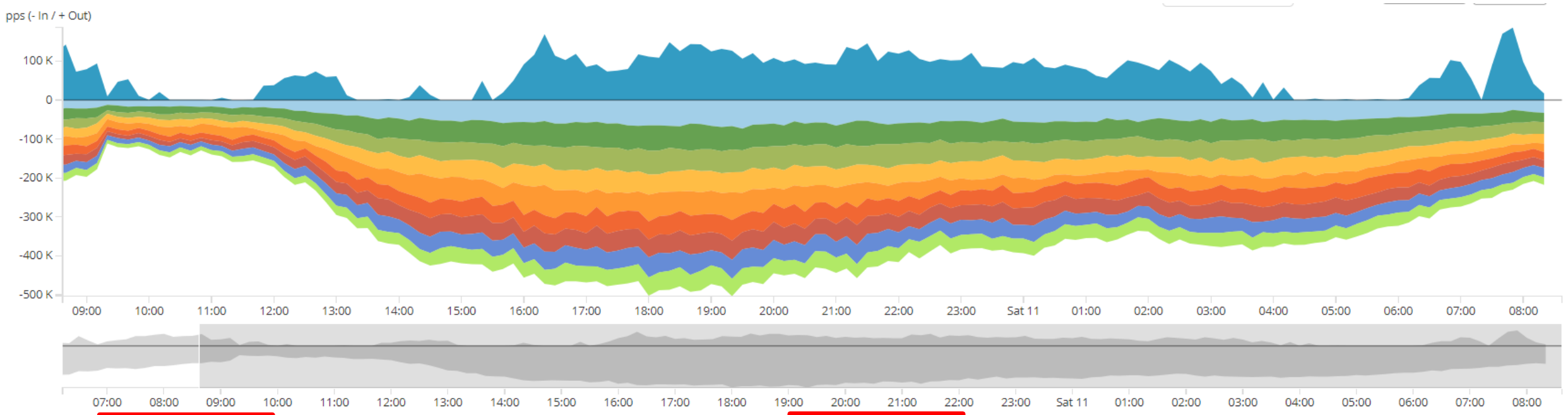
新しいデバイスを選択する際のパフォーマンスの参考値

可視化レポート（IPアドレス別）



トップトーカーの認識や、障害分析

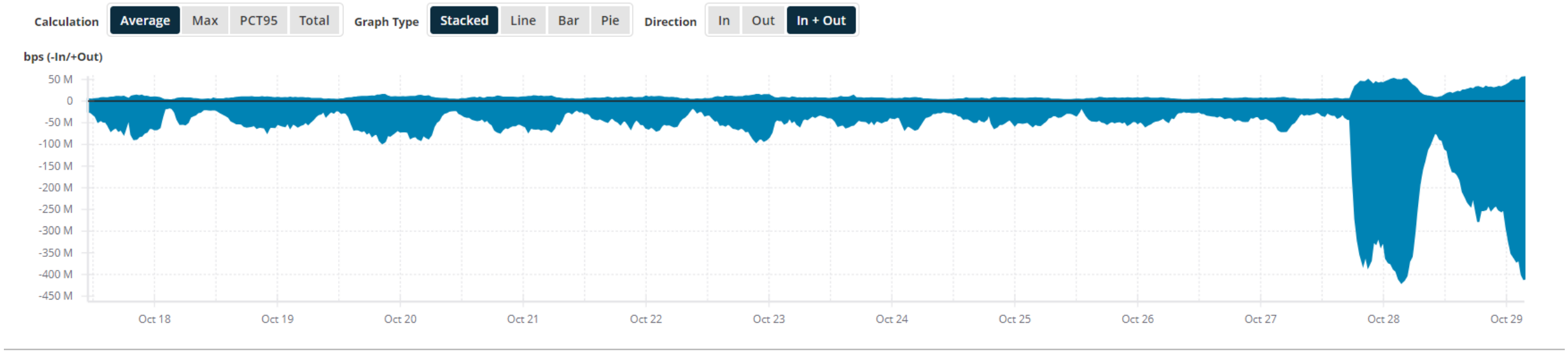
可視化レポート（サブネット別）



Destination IPv4 Address	Source IPv4 Address	Average Traffic pps (In/Out)
06.0/24	.10.0/24	67.37 k (0.000 / 67.37 k)
.185.0/24	4.133.0/24	45.43 k (45.43 k / 0.000)
.185.0/24	7.129.0/24	44.83 k (44.83 k / 0.000)
.185.0/24	.156.0/24	41.41 k (41.41 k / 0.000)
.185.0/24	.161.0/24	38.37 k (38.37 k / 0.000)
.186.0/24	.11.0/24	36.95 k (36.95 k / 0.000)
.185.0/24	4.55.0/24	34.74 k (34.74 k / 0.000)
.185.0/24	4.54.0/24	34.64 k (34.64 k / 0.000)
.185.0/24	.9.0/24	33.24 k (33.24 k / 0.000)
.185.0/24	.159.0/24	30.53 k (30.53 k / 0.000)

地域やサービス単位での可視化

特定アプリケーションの監視

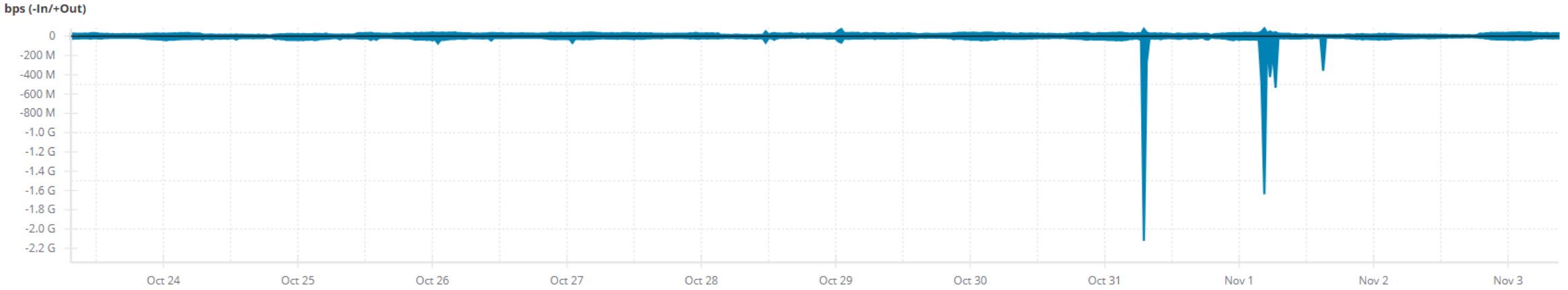


Showing 1 items

Legend	Application	Average (In)	Average (Out)	Average (In + Out)	% Total
A -	telnet	73.26 Mbps	9.367 Mbps	82.63 Mbps	100.00%
	Sum of selected items	**73.26 Mbps**	**9.367 Mbps**	**82.63 Mbps**	

telnetの通信量の変化　- ボットネット活動の疑い

特定アプリケーションの監視

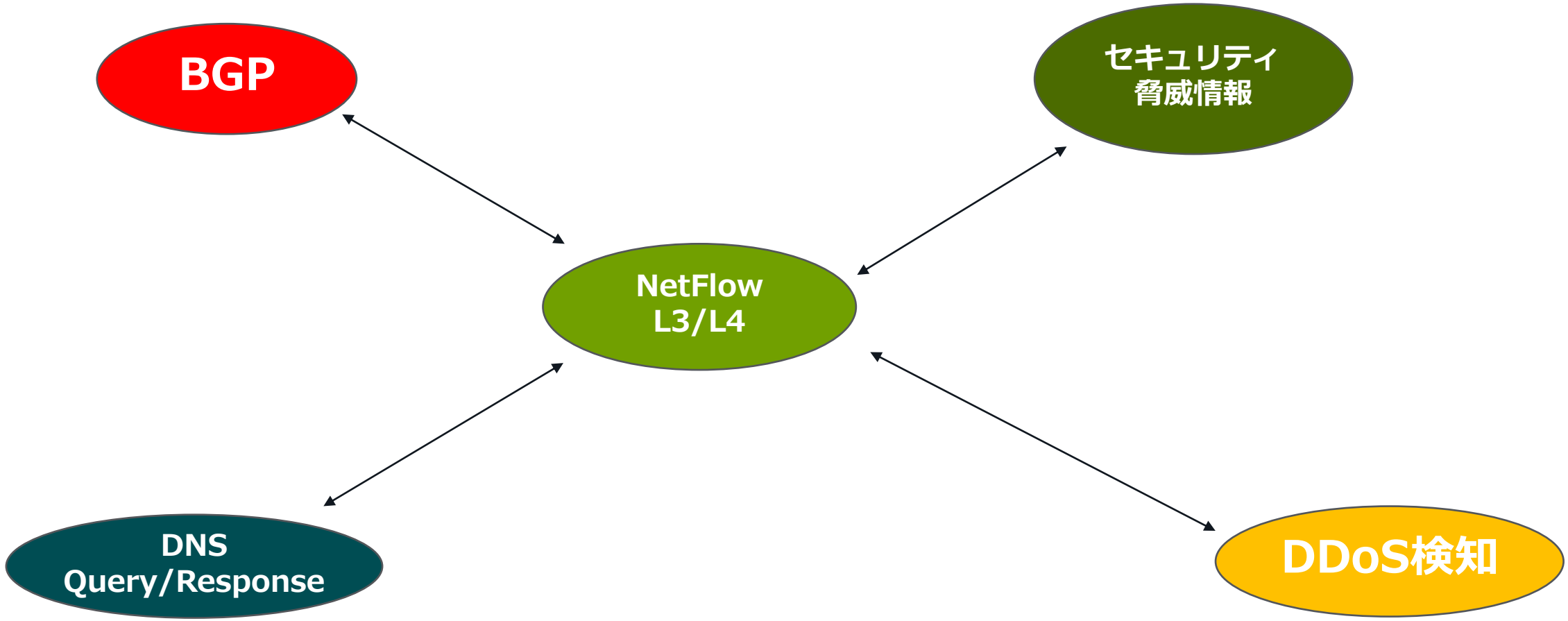


Showing 1 items

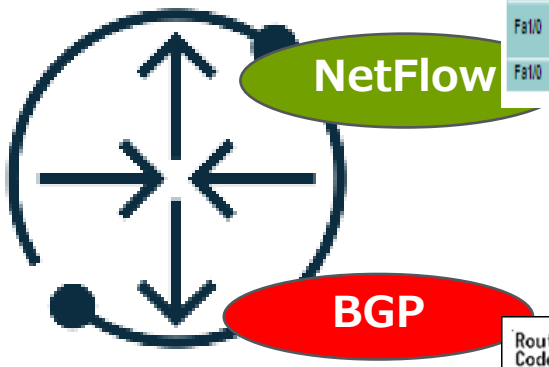
Legend	Application	Port	Average (In)	Average (Out)	Average (In + Out)	% Total
A -	domain	53	34.90 Mbps	26.10 Mbps	61.00 Mbps	100.00%
	Sum of selected items		**34.90 Mbps**	**26.10 Mbps**	**61.00 Mbps**	

DNS通信の変化 - DDoS攻撃の踏み台に使われた可能性

NetFlow x 何か =



NetFlow x BGP = ASN別通信量分析



SrcIf	SrcIPadd	DstIf	DstIPadd	Protocol	TOS	Flgs	Pkts	Src Port	Src Msk	Src AS	Dst Port	Dst Msk	Dst AS	NextHop	Bytes/ Pkt	Active	Idle
Fa1/0	173.100.21.2	Fa0/0	10.0.227.12	11	80	10	11000	00A2	/24	5	00A 2	/24	15	10.0.23.2	1528	1745	4
Fa1/0	173.100.3.2	Fa0/0	10.0.227.12	6	40	0	2491	15	/26	196	15	/24	15	10.0.23.2	740	41.5	1
Fa1/0	173.100.20.2	Fa0/0	10.0.227.12	11	80	10	10000	00A1	/24	180	00A 1	/24	15	10.0.23.2	1428	1145.5	3
Fa1/0	173.100.6.2	Fa0/0	10.0.227.12	6	40	0	2210	19	/30	180	19	/24	15	10.0.23.2	1040	24.5	14

L3/L4情報

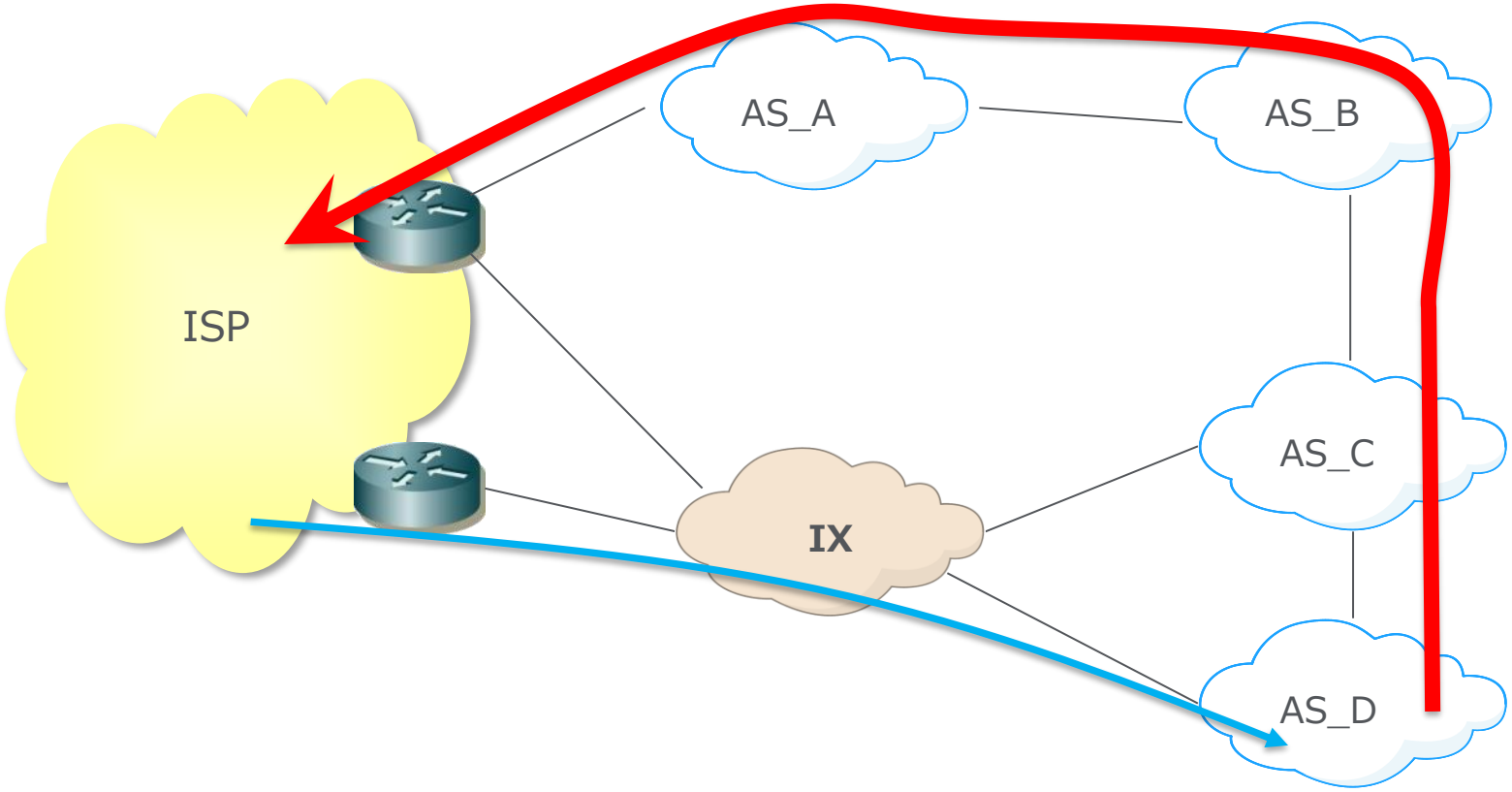
X

```
Router_2500#sh ip route
Codes: C - connected, S - static, I - IGRP, 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, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, * - candidate default
       U - per-user static route, o - ODR

  Gateway of last resort is 172.15.4.1 to network 0.0.0.0

       172.16.0.0/16 is variably subnetted, 6 subnets, 2 masks
  C       172.16.4.0/24 is directly connected, Serial0
  C       172.16.5.0/24 is directly connected, Serial1
  R       172.16.1.0/24 [120/3] via 172.16.4.1, 00:00:02, Serial0
  R       172.16.2.0/24 [120/2] via 172.16.4.1, 00:00:02, Serial0
  R       172.16.3.0/24 [120/1] via 172.16.4.1, 00:00:02, Serial0
  R    192.168.4.0/24 [120/2] via 172.16.4.1, 00:00:02, Serial0
  C    192.168.6.0/24 is directly connected, FastEthernet0
  R    192.168.7.0/24 [120/1] via 172.16.5.2, 00:00:15, Serial1
  R    192.168.1.0/24 [120/4] via 172.16.4.1, 00:00:03, Serial0
  R    192.168.2.0/24 [120/3] via 172.16.4.1, 00:00:03, Serial0
  R    192.168.3.0/24 [120/1] via 172.16.4.1, 00:00:03, Serial0
  S*   0.0.0.0/0 [1/0] via 172.16.4.1
```

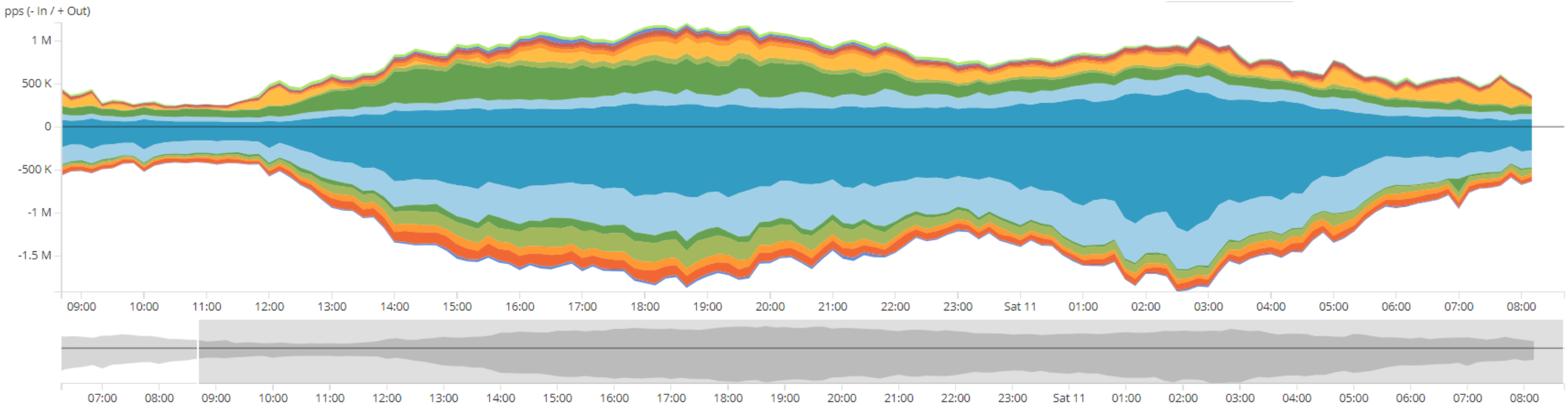
ASN 経路情報

トラフィックパスの分析

- 各ASからのトラフィック量を視点に、トラフィックパスの分析。



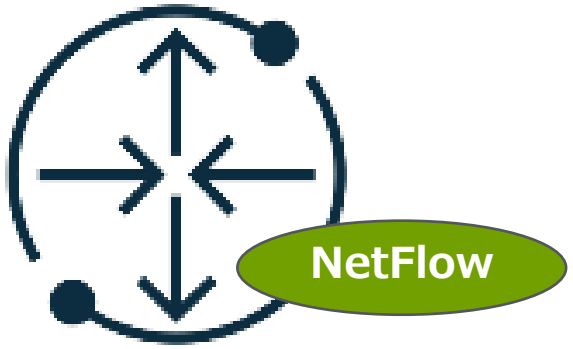
トラフィックパスの分析（AS別）



Interface	Origin ASN	Average Traffic pps (In/Out)
et-5/2/0.0 (router: sfld-cor-123net)	AKAMAI-ASN1 (20940)	767.0 k (572.1 k / 194.9 k)
et-5/2/0.0 (router: sfld-cor-123net)	FASTLY (54113)	458.8 k (343.9 k / 114.9 k)
et-5/2/0.0 (router: sfld-cor-123net)	MICROSOFT-CORP-MSN-AS-BLOCK (8075)	226.1 k (42.21 k / 183.9 k)
et-5/2/0.0 (router: sfld-cor-123net)	AKAMAI (16625)	135.2 k (103.8 k / 31.37 k)
et-5/2/0.0 (router: sfld-cor-123net)	BLUEARCHIVE-ZONE-1 (395717)	109.6 k (0.000 / 109.6 k)
et-5/2/0.0 (router: sfld-cor-123net)	CLOUDFLARENET (13335)	89.69 k (61.19 k / 28.50 k)
et-5/2/0.0 (router: sfld-cor-123net)	APPLE-AUSTIN (6185)	88.70 k (74.89 k / 13.81 k)
et-5/2/0.0 (router: sfld-cor-123net)	APPLE-ENGINEERING (714)	48.43 k (8.919 k / 39.51 k)
et-5/2/0.0 (router: sfld-cor-123net)	MICROSOFT-CORP-MSN-AS-BLOCK (8068)	27.13 k (13.04 k / 14.09 k)

特定のインターフェイスに対するオリジンASからの通信料

NetFlow x DNS



10.0.0.1 <=> 192.168.1.1　　L3/L4情報

X

192.168.1.1 =
abc.netscout.com

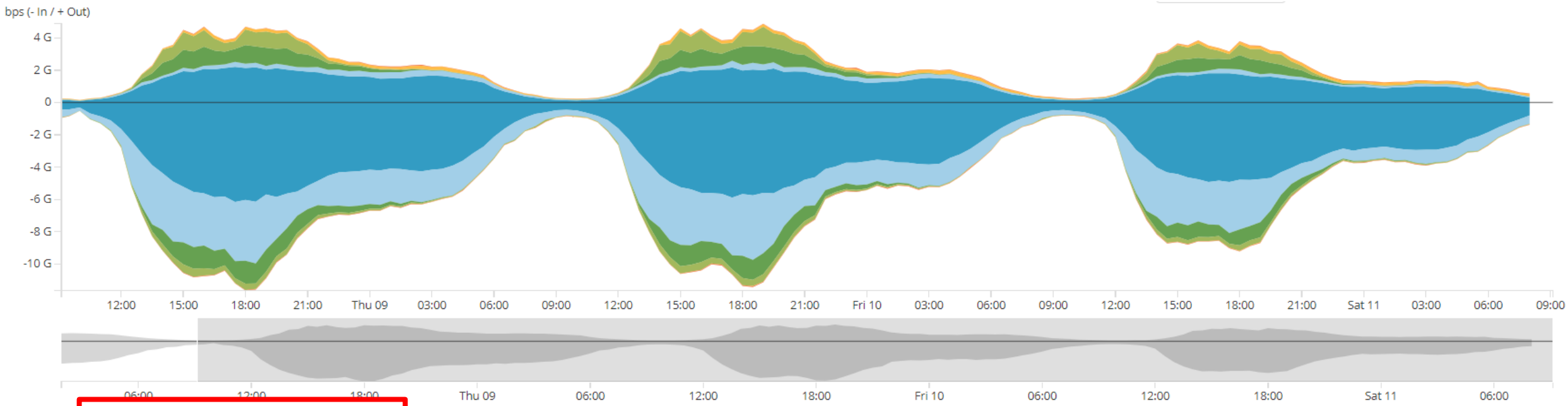
L3/Domain情報

NetFlow x DNS

NetFlow情報にDNSで解決されたドメインとA/AAAAレコードを付加することにより、ドメイン（サービス）別での可視化が可能になります

従来はDPIでしか可視化が難しかったアプリケーション識別の代替になります

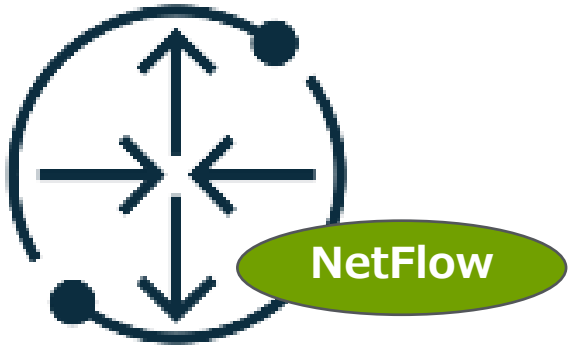
NetFlow x DNS



Profile	Average Traffic bps (In/Out)
Facebook (1)	4.460 G (3.266 G / 1.195 G)
YouTube	1.889 G (1.694 G / 194.6 M)
Zoom	650.6 M (354.2 M / 296.4 M)
Skype for Business Online and Microsoft Teams	405.1 M (145.1 M / 260.0 M)
Netflix OCA	112.2 M (4.114 M / 108.1 M)
ESPN	36.10 M (7.256 M / 28.85 M)
Telegram	28.00 M (17.59 M / 10.41 M)

アプリケーション（サービス）単位での可視化
網内CDNのヒット率の確認など

NetFlow によるDDoS検知

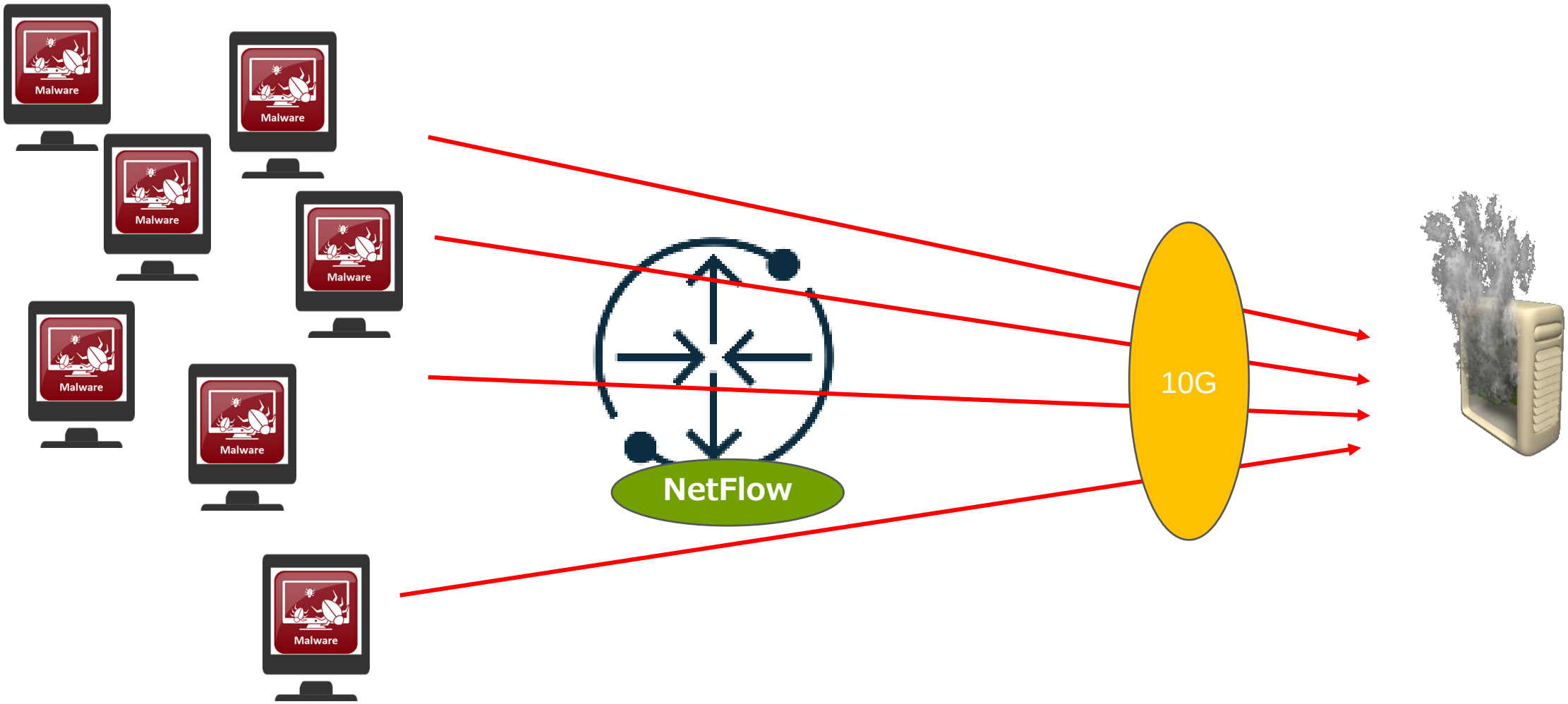


10Gbps > 192.168.1.1

特定の宛先に対する通信量が平常時の通信量を大きく超え、閾値以上になった場合は、何かしらのイベント（例えばDDoS攻撃）が発生しているとしてアラートを発生

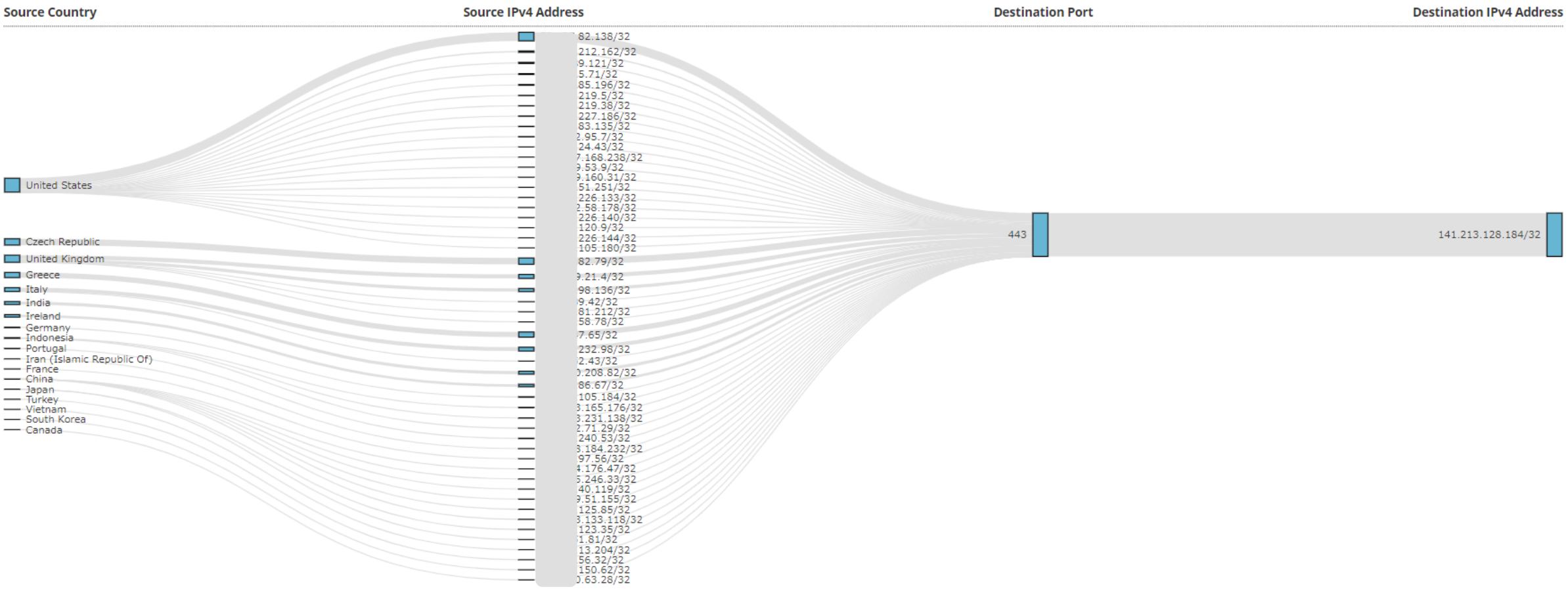
閾値

NetFlow によるDDoS検知



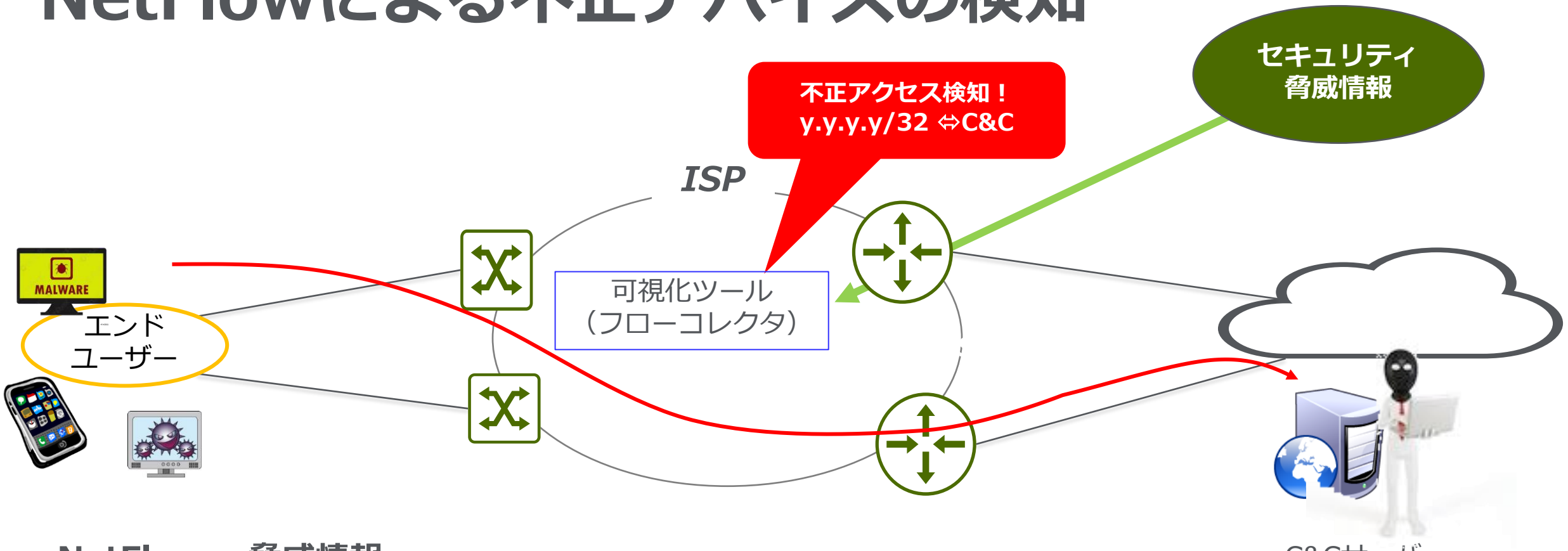
NetFlow によるDDoS検知

攻撃発信国　攻撃元IPアドレス　攻撃タイプ　攻撃先IPアドレス



DDoS攻撃の通信の流れを可視化

NetFlowによる不正デバイスの検知

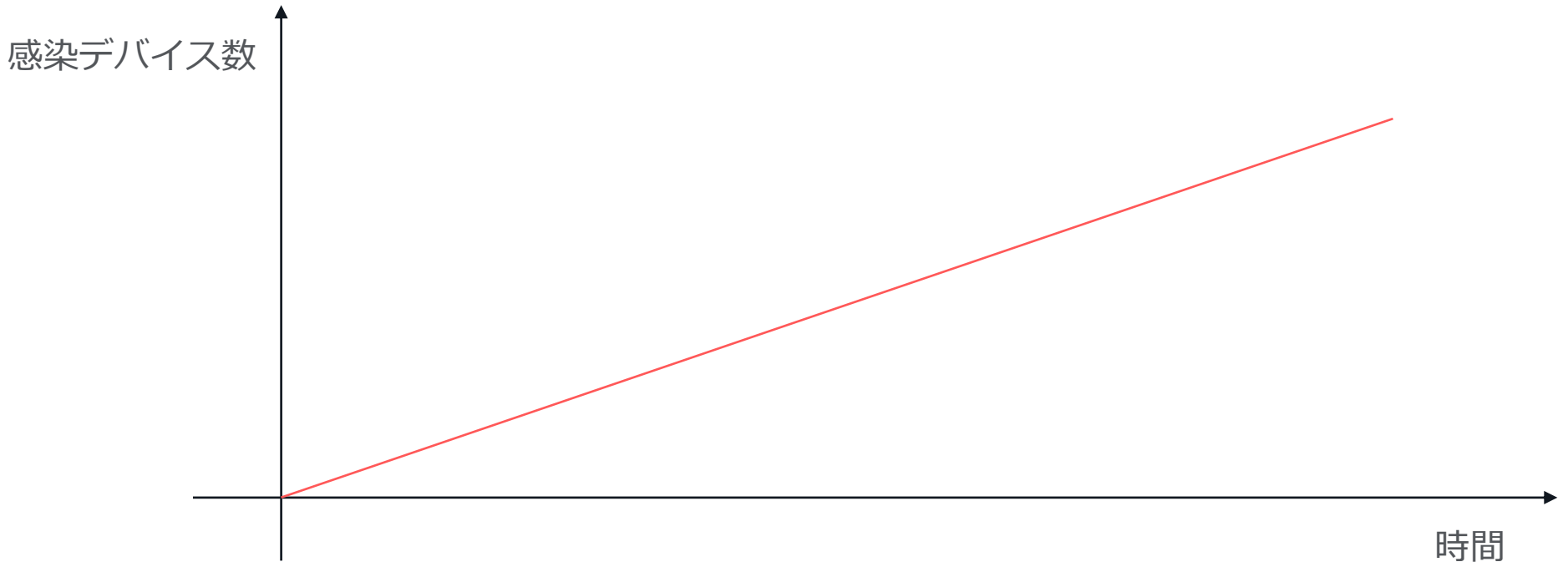


NetFlow x 脅威情報

マルウェアに感染しているデバイスを手間をかけることなく発見

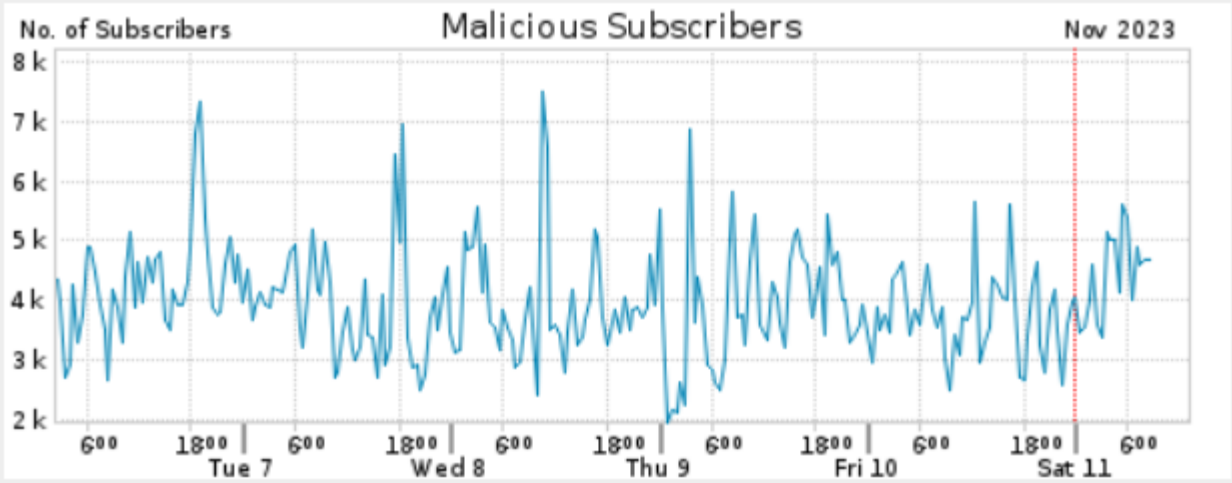
マルウェア感染デバイスの通信量を見ることが目的ではなく、その存在を見つける為の手法

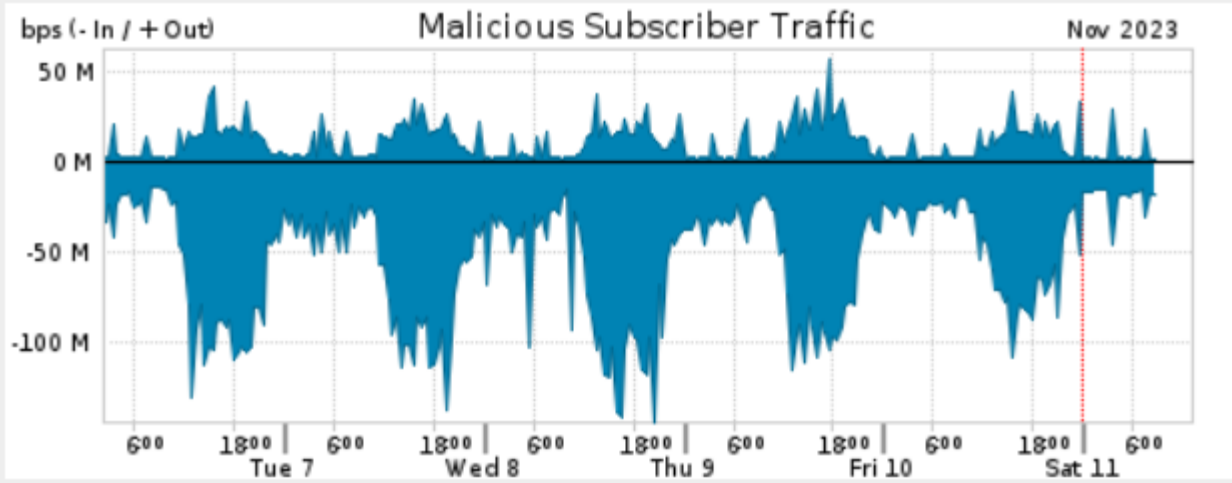
マルウェア感染デバイスの発見



時間経過と共に、サンプリングされたNetFlowでも徐々に感染デバイスを発見

マルウェア感染デバイスの発見





Avg. Malicious Subscribers	Avg. Malicious Share of All Subscriber Traffic	Avg. Malicious Traffic	Avg. Total Subscriber Traffic
3833	0.061%	63.04 Mbps / 28.66 Kpps	103.53 Gbps / 14.42 Mpps

マルウェア感染デバイスの台数や、不正通信のトラフィック量

まとめ

FlowにはL3/L4の情報が含まれます

Flowを利用する事で多くのコストをかけずに、ネットワークを全体の可視化が可能となります。

Flowにいくつかの要素を加える事により、多角的な可視化も実現できます

Flowによりネットワークセキュリティⅰの視点で利用する事も有用です

Thank You.

www.netscout.com