BGP Flowspec(RFC5575)

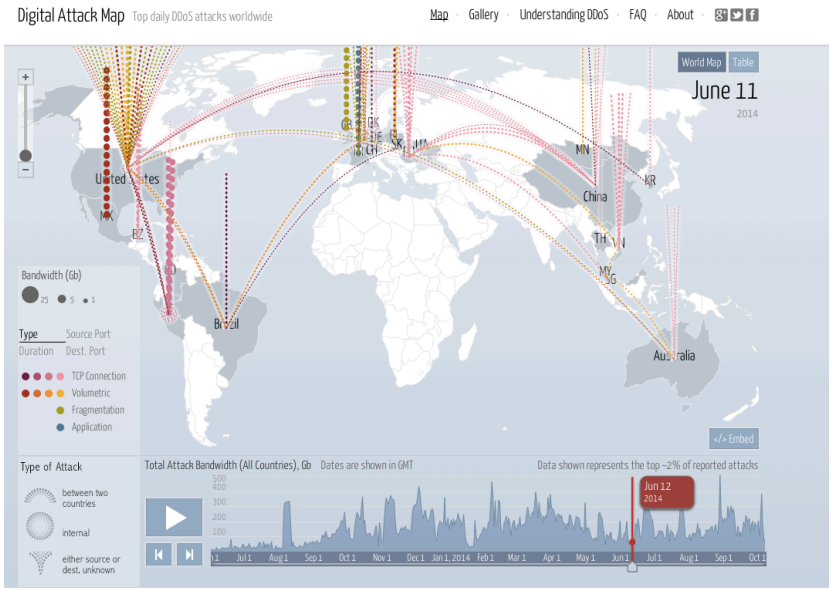
Shishio Tsuchiya

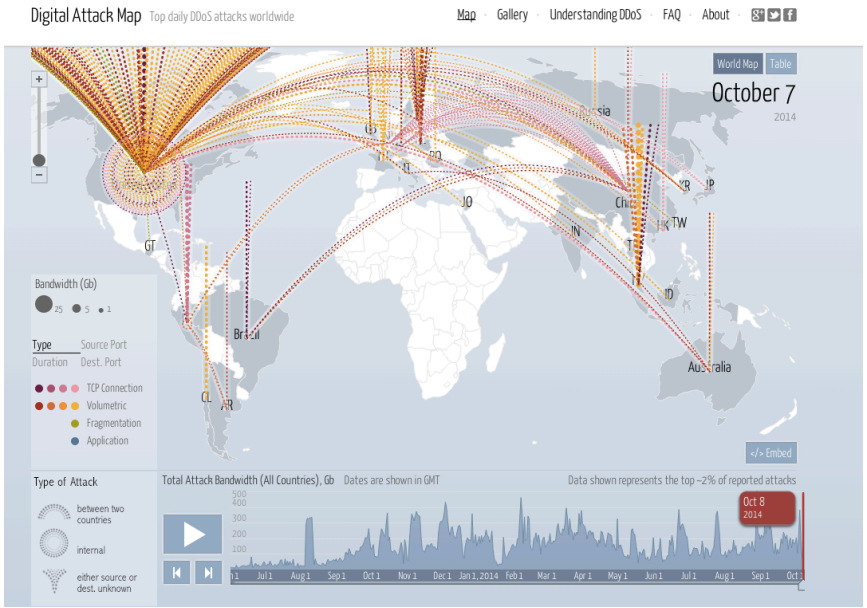
shtsuchi@cisco.com

本日の登壇者

- 土屋 師子生 (シスコシステムズ合同会社)
- 平澤 庄次郎 (ビッグローブ株式会社)
- 我妻 敏 (株式会社東陽テクニカ)

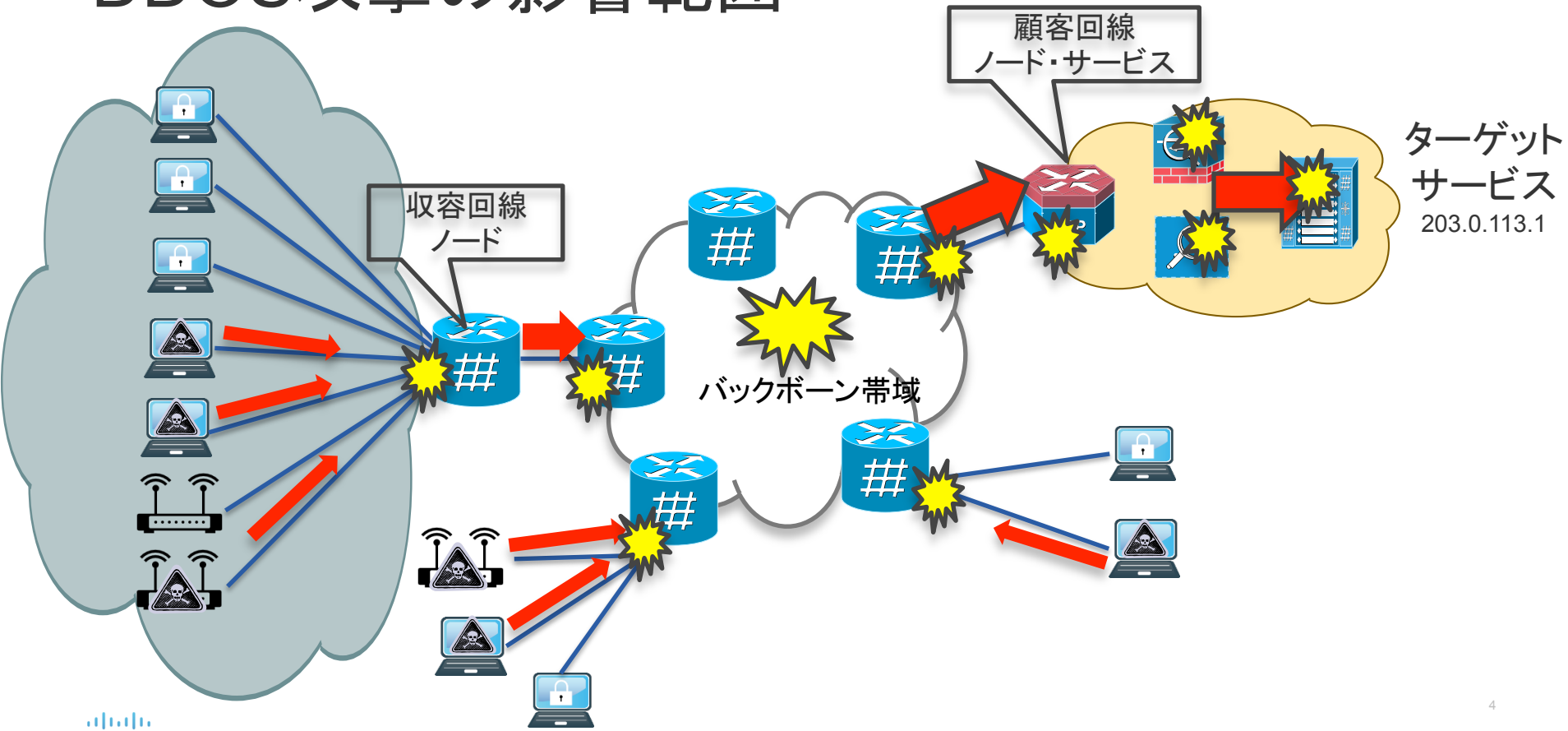
DDOSトラフィックは絶えず変化していく



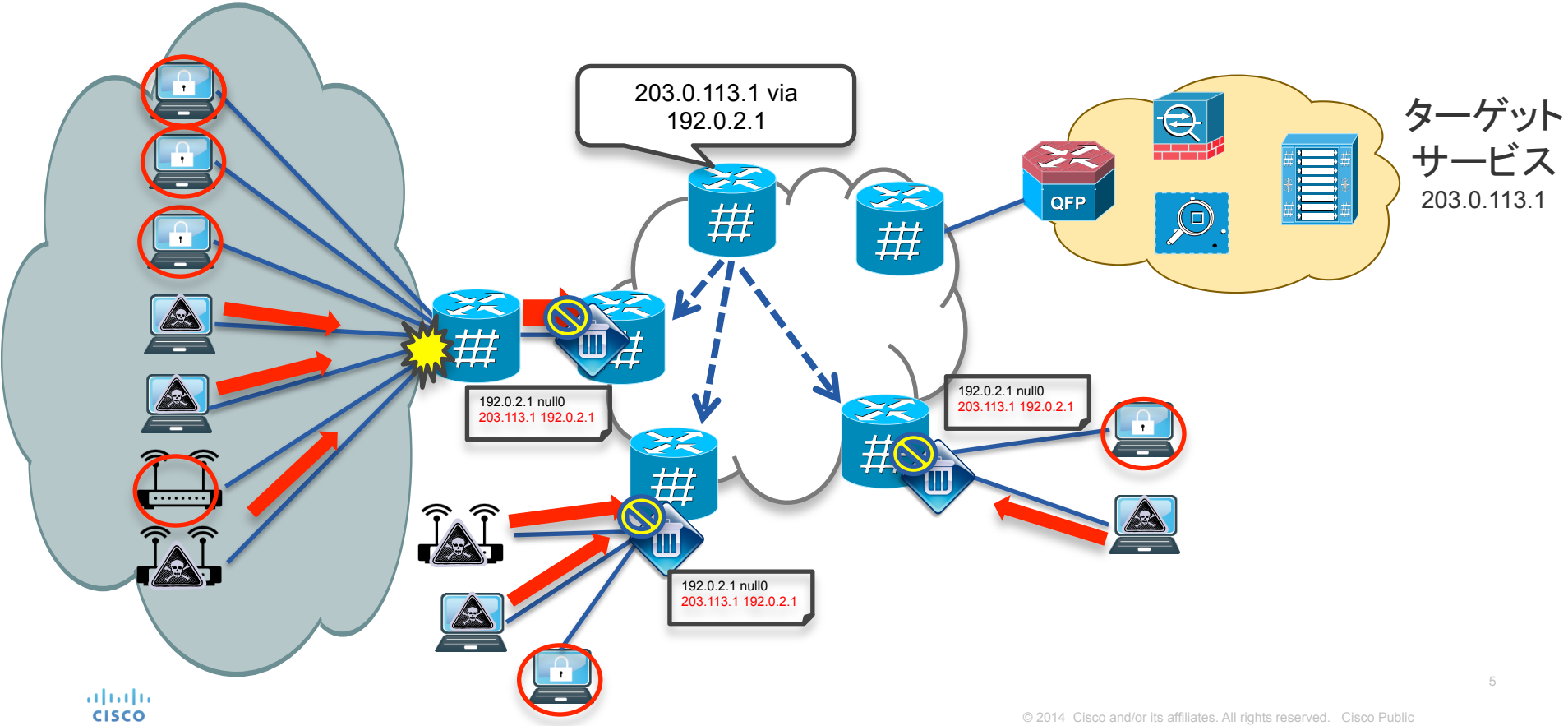


http://www.digitalattackmap.com/

DDOS攻撃の影響範囲

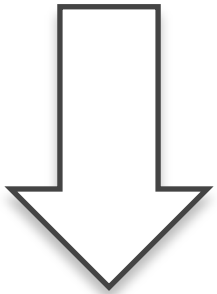


RTBH(Remote Triggered Black Hole Filtering)



BGP Flowspecの登場

- RTBHでは悪意の無いユーザのトラフィックも止まってしまう
- また急遽増えた攻撃に対しての検出/アクションの適用が難しい



Netflow+BGP Attribute

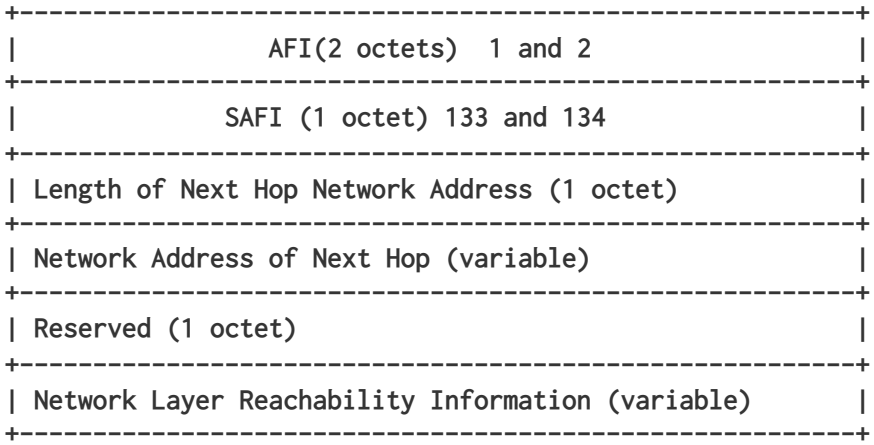
BGP Flowspec(RFC5575)+draft-ietf-idr-flow-spec-v6

- Dst IP
- Src IP
- protocol
- port
- Dst port
- Src Port
- ICMP Type
- ICMP Code
- TCP Flags
- Packet Length
- DSCP
- Fragment

Flow Type

- traffic-rate
- traffic-action
- redirect
- traffic-marking

Action Rule

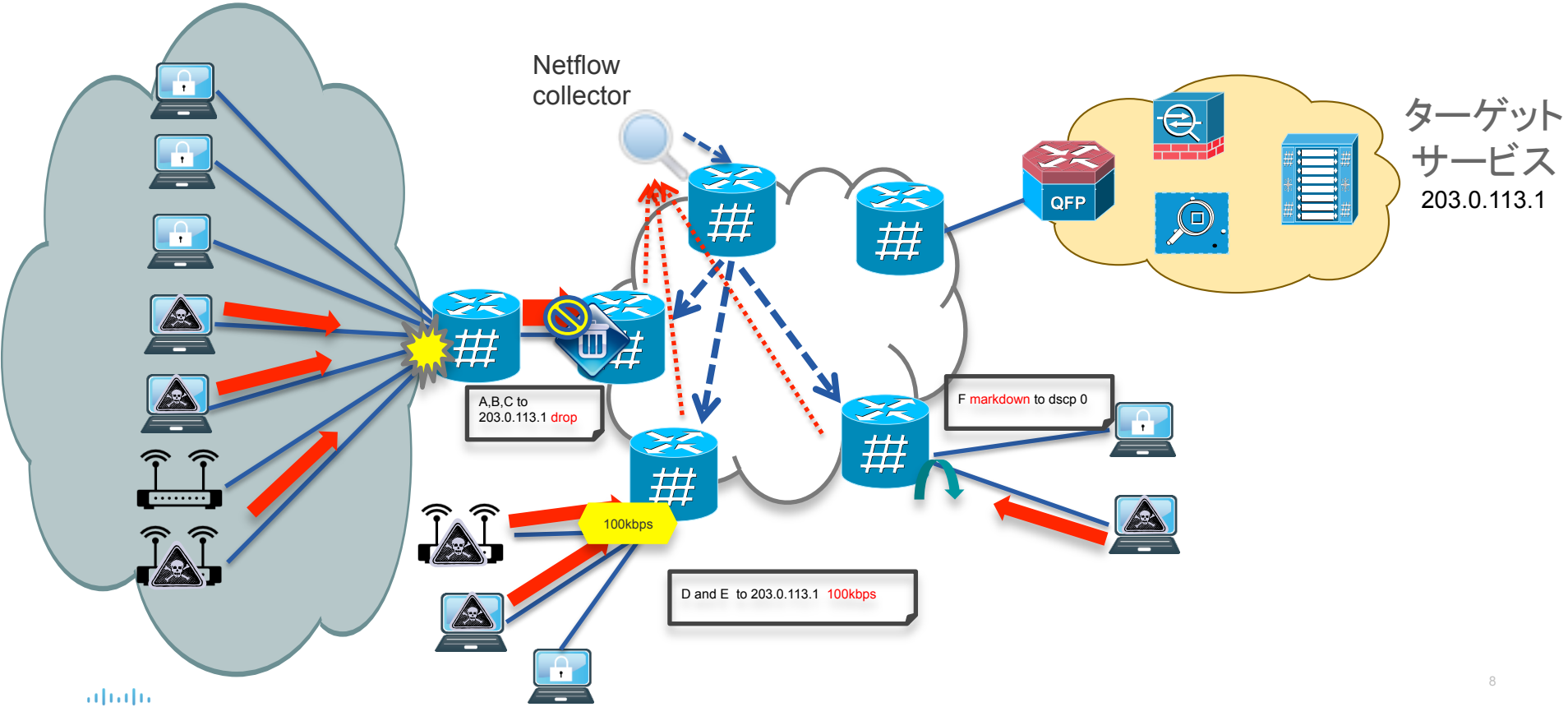


SAFI

133 Dissemination of flow specification rules

134 L3VPN dissemination of flow specification rules

BGP Flowspec(RFC5575)



Agenda

- イントロ　土屋
- World WideのDDOSトレンド 我妻さん
- ISPの現在のDDOSの状況と対策およびBGP Flowspecへの期待　　平澤さん
- 打ち合わせで出た疑問
- 会場との議論

Agenda

- イントロ　土屋
- World WideのDDOSトレンド 我妻さん
- ISPの現在のDDOSの状況と対策およびBGP Flowspecへの期待　　平澤さん
- 打ち合わせで出た疑問
- 会場との議論

疑問1　平澤さんから

BGP Flowspecってそもそもどこまで出来るの？

もう少し細かくFlow typeとRule Action

Flow Type

operator codeがあり、lt,gt,eqの指定が可能

Type	IPv4 (RFC5575)	IPv6 (flow-spec-v6)
1	Destination Prefix	Destination IPv6 Prefix
2	Source Prefix	Source IPv6 Prefix
3	IP Protocol	Next Header
4	Port	Port
5	Destination port	Destination port
6	Source port	Source Port
7	ICMP type	ICMP type
8	ICMP code	ICMP type
9	TCP flags	TCP flags
10	Packet length	Packet length
11	DSCP	DSCP
12	Fragment	Fragment
13	N/A	Flow Label

あ、IPv6アドレス指定が出来ない…

type	extended community	実際のアクション	RFC/draft
0x8006	traffic-rate	Policeレートを指定 0：drop	RFC5575
0x8007	traffic-action	特定のアクションを指定 Terminal bit:(0なら終了) Sample bit:(1ならlogging/sampling)	RFC5575
0x8008 0x8208 0x800b	redirect AS-2byte redirect AS-4byte redirect IPv6 specific AS	指定したVRFにredirect	flowspec-redirect-rt-bis flowspec-redirect-rt-bis flow-spec-v6
0x8108	redirect IPv4 address	指定したアドレスにredirect	flowspec-redirect-rt-bis
0x8009	traffic-marking	DSCPの値をマーキング	lowspec-redirect-rt-bis flow-spec-v6

実装状況

- Cisco
  IOS-XR:5.2.0-
  IOS-XE3.14 -
  IOS 15.5(1)S-
- Juniper
  JUNOS 7.3-
- Alcatel-Lucent
  SR-OS 9.0R1-
- Arbor Networks
  PeakFlow 6.0-
- Genie Networks
  5.5.1-

疑問2　馬渡さんから

そもそもフローで良いんだろうか？

疑問3 土屋・平澤さんから

DDOSの検証のイケてる方法って？

議論したい所

- IPv4アドレスが共有されている時代、フローベースでのフィルタが必要か？
  モバイル・CGNのDDOS状況はどうですか？
- BGP Flowspec for IPv6対応状況
  欲しいですか？
- 運用者から見た美味しい所、厳しい所
- 運用実績や状況など

TOMORROW starts here.