JANOG35 Meeting
DAY3 - Flowspec (RFC5575)

ATLAS Q3 2014 Update – Japan

我妻　敏
agatsuma@toyo.co.jp

株式会社 東陽テクニカ

DDOS の WORLD WIDE の状況

株式会社 東陽テクニカ
ARBOR NETWORKS

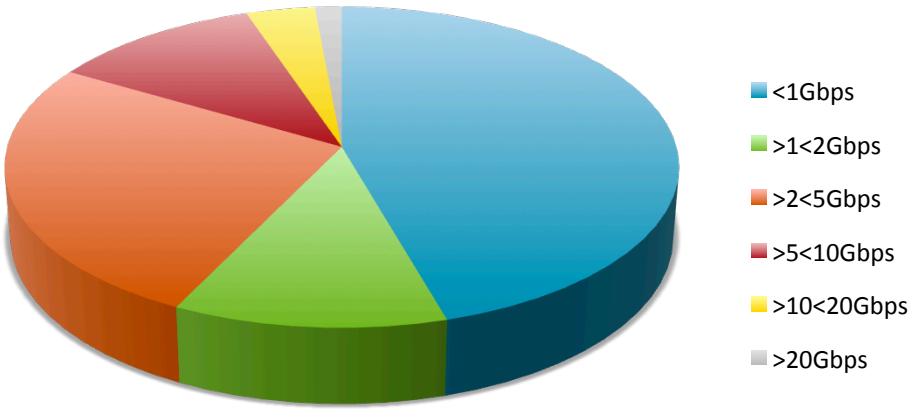
The Arbor ATLAS Initiative: Internet Trends

- 290以上のISPとのリアルタイムのデータ共有 - > ATLAS Internet Trends
  - 毎時XMLファイルを Arbor Server (HTTPS) に送出
  - ファイルは匿名化されており、ユーザー情報は次のものに限定
    - ユーザーの定義した地域　例：Europe
    - プロバイダー種別（自己申告）例：Tier 1
- データは、Flow/BGP/SNMP から統合化
  - Arbor Peakflow SP 製品は
    - サンプリングされた Flow と BGP をリアルタイムに関連付け
    - 分散システム
    - Network / Router / Interface の情報　例：Traffic レポート
    - 脅威の検出 (DDoS / 感染した内部システム)
    - 複数の検知機構
- 現在、ATLASは協力者からえられる IPv4 トラフィックをモニタしており、その対象はおよそ90Tbps
    - インターネット トラフィックのかなりの割合に及ぶ

株式会社 東陽テクニカ
ARBOR NETWORKS

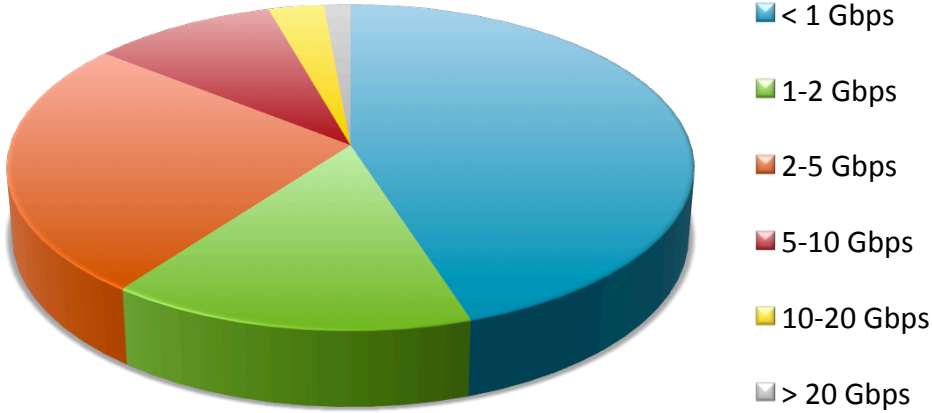
DDoS攻撃の規模

World 2013



- 2012年と比べ、2013年では20Gbpsを超える攻撃の数が8.6倍に
- 2012年と比べ、2−10Gbpsの攻撃規模は37.6%の増加
- 最も深刻な増加は10Gbps以上の攻撃で, 2012年から125% の増加

Asia 2013

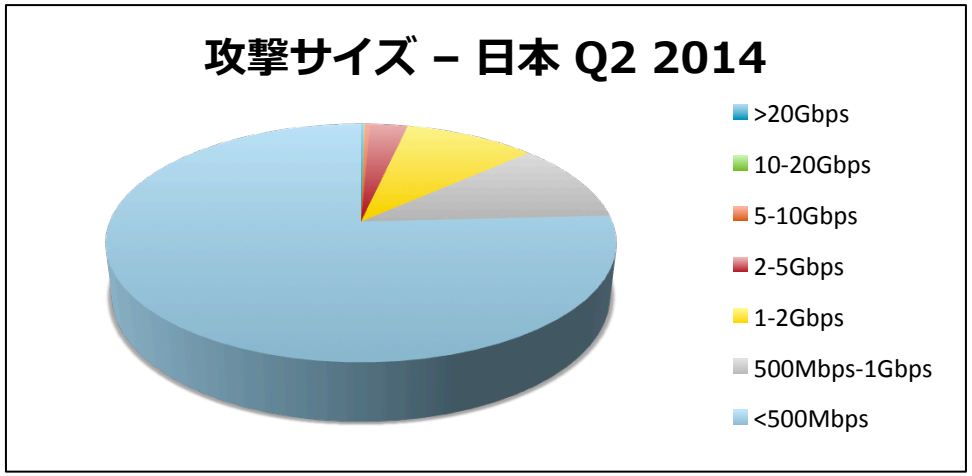


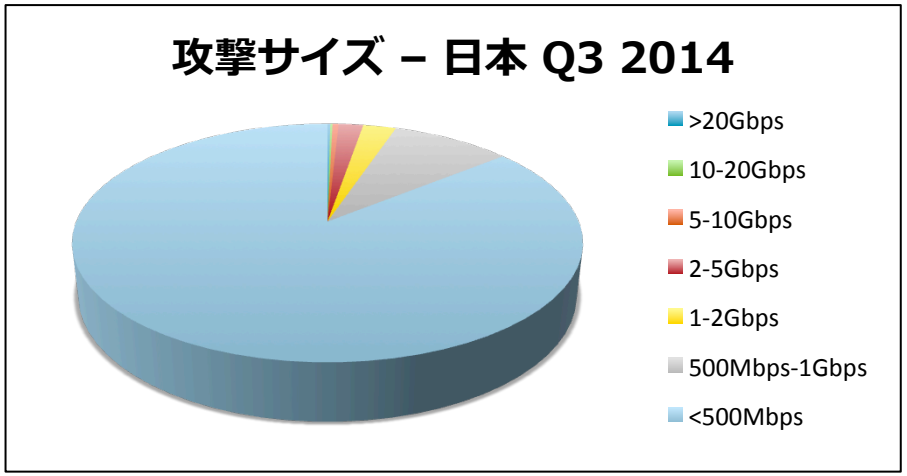
- アジアにおける攻撃規模の比率はワールドワイドと酷似

株式会社 東陽テクニカ ARBOR NETWORKS

2014 ATLASによる攻撃データ観測　攻撃サイズ

- 日本、アジア、ワールドワイドでの比較データ
  - 日本での1Gbps以下の攻撃は、APAC及びグローバルに対して若干多い状況
    - Q2 JP 88% / APAC 89% / 85% WW
    - Q3 JP 95% / APAC 88.1% / 83.1% WW

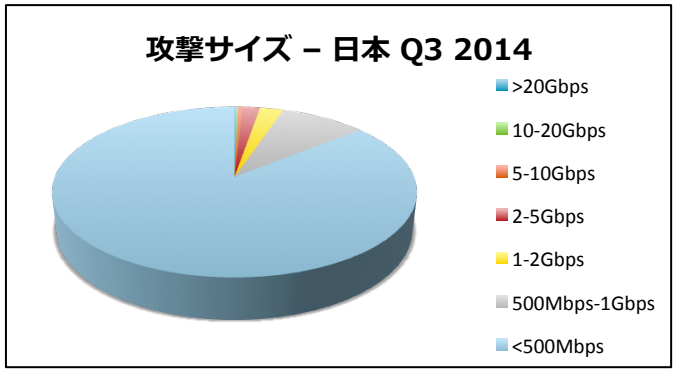


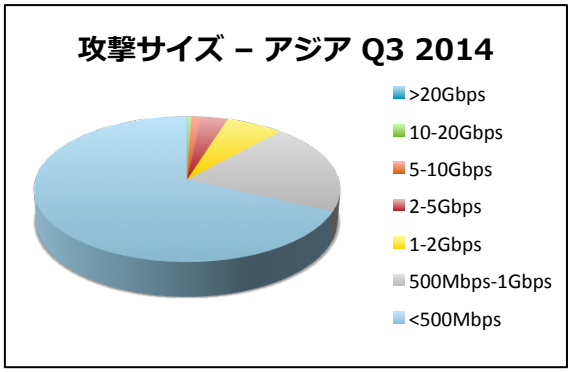


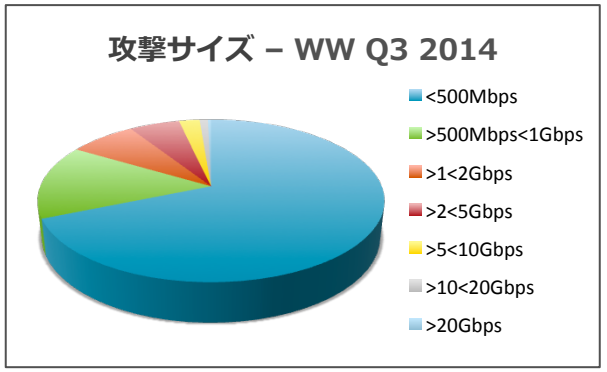
	日本平均	アジア平均	世界平均
Q2	491.63Mbps/118.54Kpps	530.5Mbps/ 119.84Kpps	759.83Mbps/199.85Kpps
Q3	365.8Mbps/202.61Kpps	588.74Mbps/170.38Kpps	858.98Mbps/238.35Kpps

2014 ATLASによる攻撃データ観測　最大攻撃サイズ

- 2014年Q3における日本、アジア、ワールドワイドでの比較







- 最大の攻撃は未だNTPアンプによるものが多く観測されている

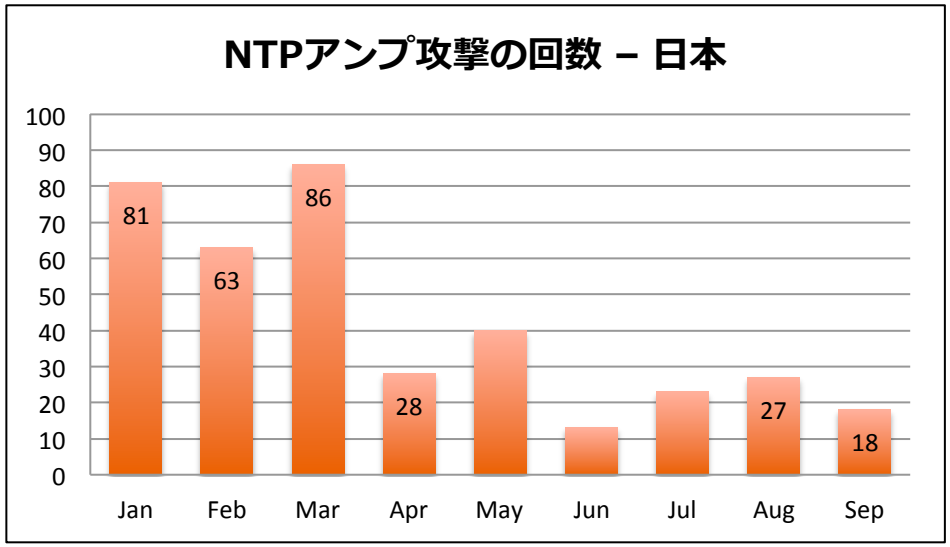
	日本最大	アジア最大	世界最大
Q2	63.06Gbps / 16.85Mpps Port80に対する NTPアンプでの攻撃で 攻撃時間は21分32秒	127.16Gbps / 34Mpps マレーシアで発生した Port52606に対するNTPアンプ 攻撃で 攻撃時間は29分	154.69Gbps / 41.34Mpps スペインで発生したPort80に対 するNTPアンプ攻撃で、攻撃時 間は24分
Q3	38.57Gbps / 6.04Mpps UDP Port80に対する UDPフラッディングの攻撃で、 攻撃時間は13分19秒	98.89Gbps / 26.44Mpps インドで発生した Port80に対するNTPアンプ攻撃 で、攻撃時間は31分	264.61Gbps / 98.93Mpps, 不 特定のPortに対するUDPフラッ ディング攻撃で、攻撃時間は1 時間4分

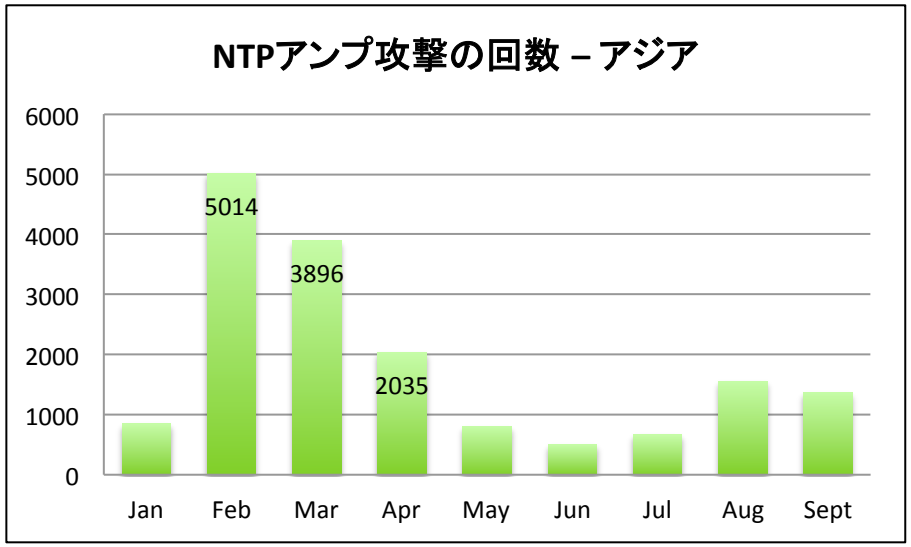
2014 ATLAS NTPアンプ攻撃の傾向

JP & APAC NTP trend

- 全世界におけるNTP攻撃は減少傾向にあります
- 日本におけるNTPアンプ攻撃は4ヶ月ほど前から減少傾向にあります

	日本平均	アジア平均
Q2	3.22Gbps 854.8Kpps	2.57Gbps 680.32Kpps
Q3	281.76Mbps 71.47Kpps	2.70Gbps 703.02Kpps





他のプロトコルでのアンプ攻撃

- NTPアンプ攻撃により大きなトラフィックを与えられる事が知られた事から、他のプロトコルでも同じことができるものについて注目が集まっています
- アンプ攻撃の為にどのソースポートを使ったかを調査します
- DNSはここ数年攻撃者に使われています
- ソースポート1900（SSDP)による攻撃が著しくしく増加しています
  - Q2　3回(最大1.18Gbps)
  - Q3　2457回

サービス	UDP ソースポート	Q3 攻撃の割合	Q3 最大攻撃サイズ	Q3 平均攻撃サイズ
SNMP	161	0.01%	3.75Gbps	769.1Mbps
Chargen	19	1.09%	21.26Gbps	1.12Gbps
DNS	53	3.79%	43.45Gbps	1.31Gbps
SSDP	1900	0.76%	51Gbps	5.11Gbps

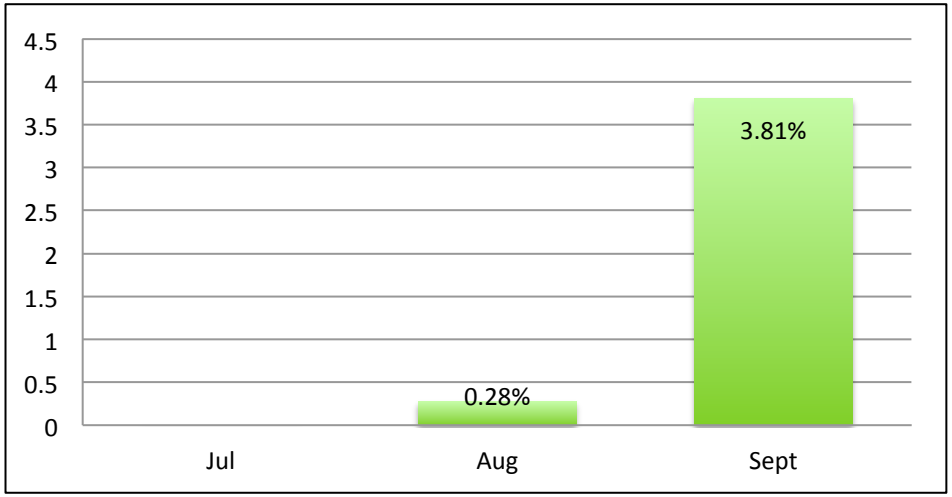
株式会社 東陽テクニカ　ARBOR NETWORKS

2014 ATLASによる攻撃データ観測　SSDP攻撃 – 日本

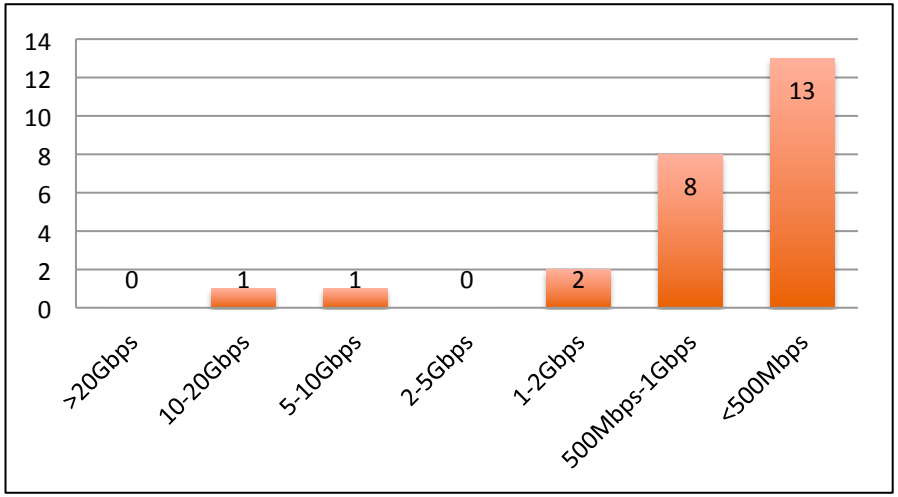
SSDP アンプ攻撃

- ソースポート1900（SSDP)による攻撃が増加している事が現れています
  - Q2にはゼロだったものがQ3では25回観測されています
- トップの攻撃元の国は:
  - ロシア：8%
  - 中国：8%
  - アメリカ：8%

- これまで見られたSSDPによる最大の攻撃は19.16Gbpsでポート80に対して行われました
- 攻撃先となっているポートは:
  - 80 ：96%
  - 53：4%



Number of SSDP events



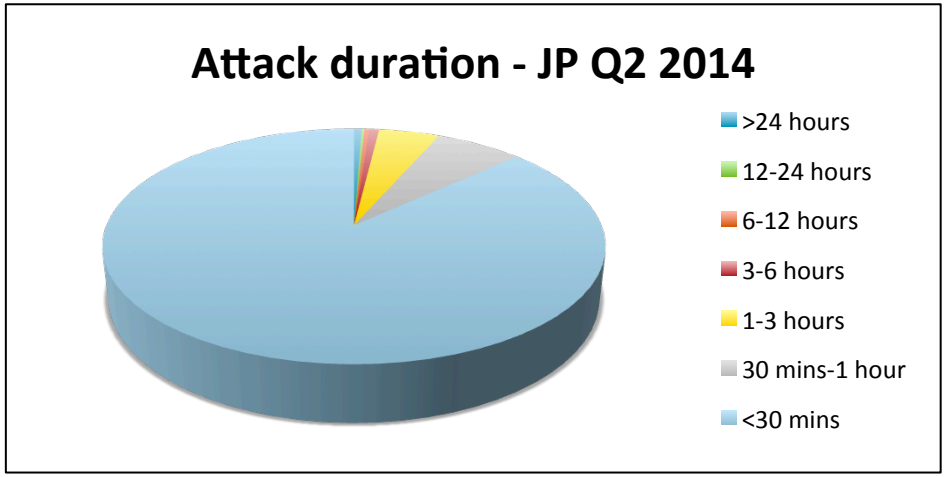
2014 ATLASによる攻撃データ観測　攻撃時間

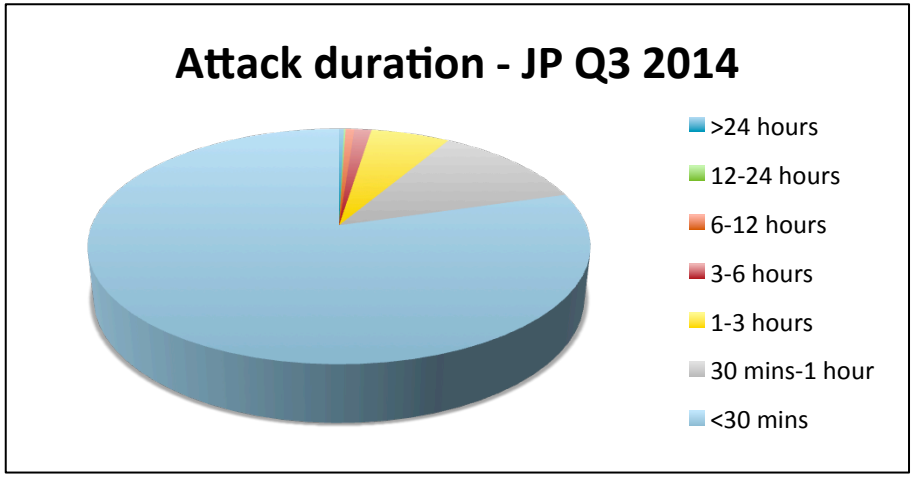
攻撃時間分布 Q2

- 多くの攻撃は短時間で、約94%の攻撃が1時間以内に終了してます。（世界平均は90.6%)
- 平均攻撃時間は2時間20分で、世界平均と比べると68分長くなっています
- 12時間以上の攻撃は1%で、世界平均は1.38%となっています

攻撃時間分布 Q3

- 多くの攻撃は短時間で、約92%の攻撃が1時間以内に終了してます。（世界平均は91.2%)
- 平均攻撃時間は3時間21分で、世界平均と比べると135分長くなっています
- 12時間以上の攻撃は0.5%で、世界平均は1.23%となっています

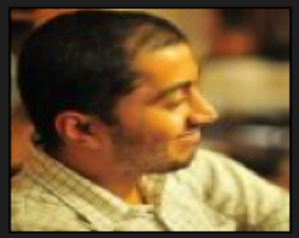




短い攻撃時間の背景 - DDoS攻撃代行サービスの利用

JunaidNoor

Junior Member



Join Date:	Jun 2008
Posts:	8

Professional DDoS Service! free test!

Hello all. i present to you professional DDoS service!

free test 5 minutes, only for serious clients!

i use private ddos bot - dirt jumper v5 (special edition for me).

supported methods of attack:
- TCP SYN Flood
- HTTP GET Flood
- HTTP POST Flood
- HTTP Downloading Flood
- HTTP Synchronous Flood

prices for attack:
- 4$ / hour
- 35$ / day
- 200$ / week

* prices may change, if target have Anti-DDoS protection!

payment:
- WMZ
- Liberty reserve

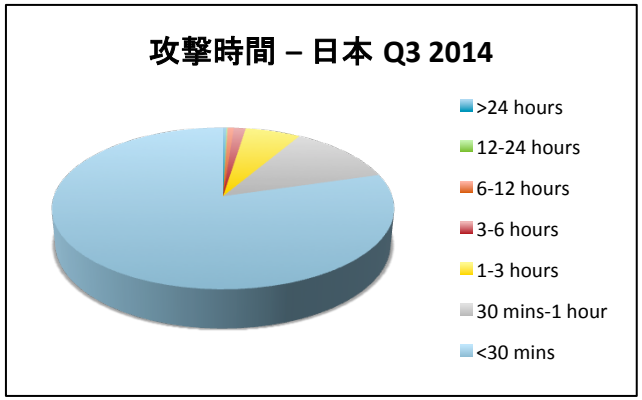
株式会社 東陽テクニカ

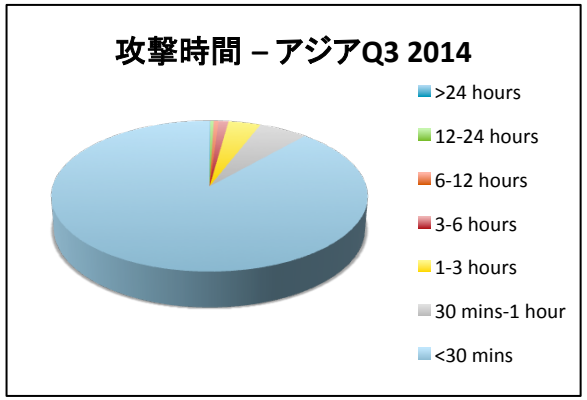
ARBOR NETWORKS

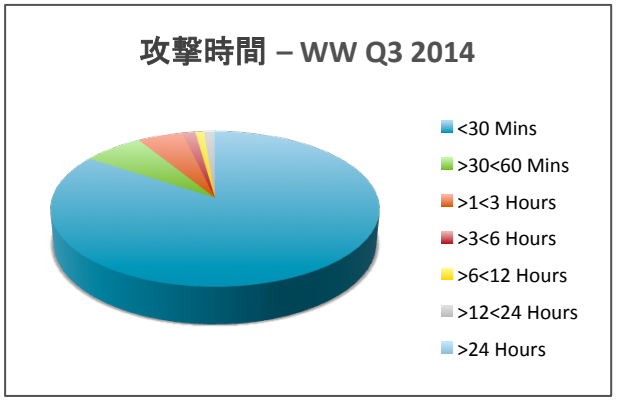
2014 ATLASによる攻撃データ観測　攻撃時間 日本、アジア、WW

攻撃時間分布 (Q3)

	日本平均	アジア平均	世界平均
平均攻撃時間	3時間21分	31分	66分
12時間以上	0.5%	0.49%	1.23%
1時間以下	92%	94.1%	91.2%







株式会社 東陽テクニカ　ARBOR NETWORKS

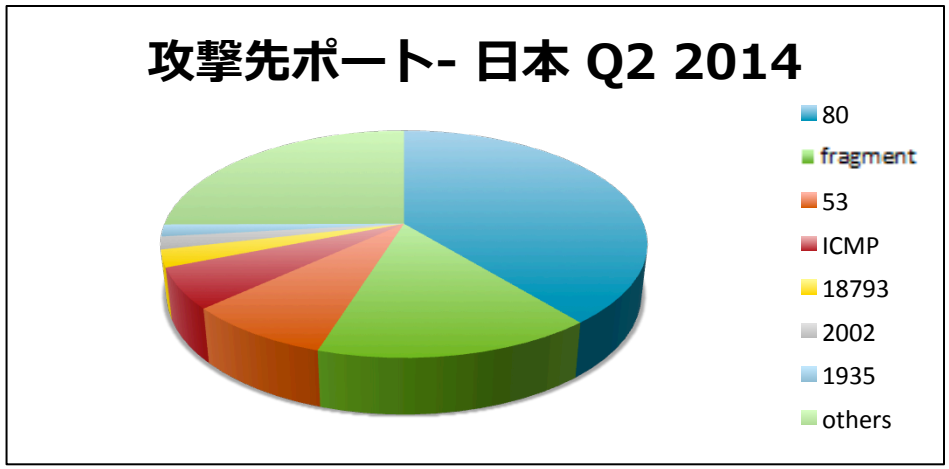
2014 ATLASによる攻撃データ観測　攻撃先ポート

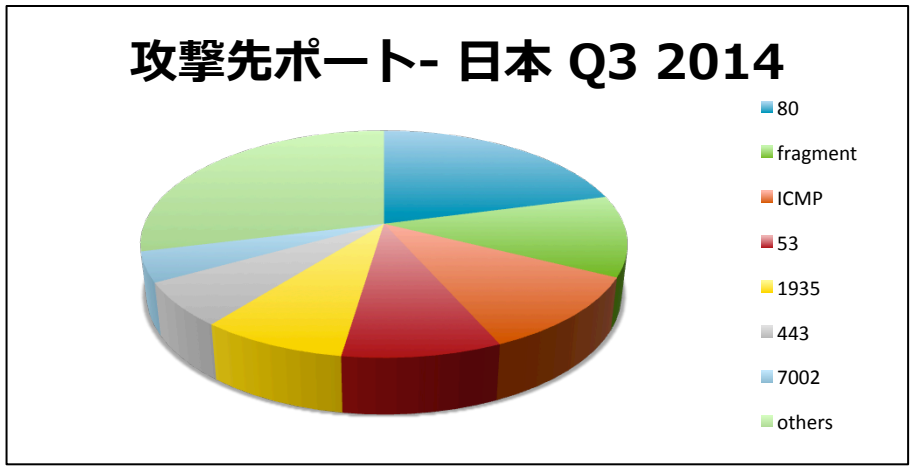
攻撃先ポート別分布 Q2

- 最も多いのはポート80で全体の39%になります
  - 全世界では16%となります
- 2番目はフラグメント攻撃で全体の16%となります
  - 全世界では24%となります
- 3番目はポート53で全体の8%になります
  - 全世界では13%となります

攻撃先ポート別分布 Q3

- 最も多いのはポート80で全体の21%になります
  - 全世界では19%となります
- 2番目はフラグメント攻撃で全体の12%となります
  - 全世界では26%となります
- 3番目はICMPで全体の11%になります
  - 全世界ではトップ3にはいっていません

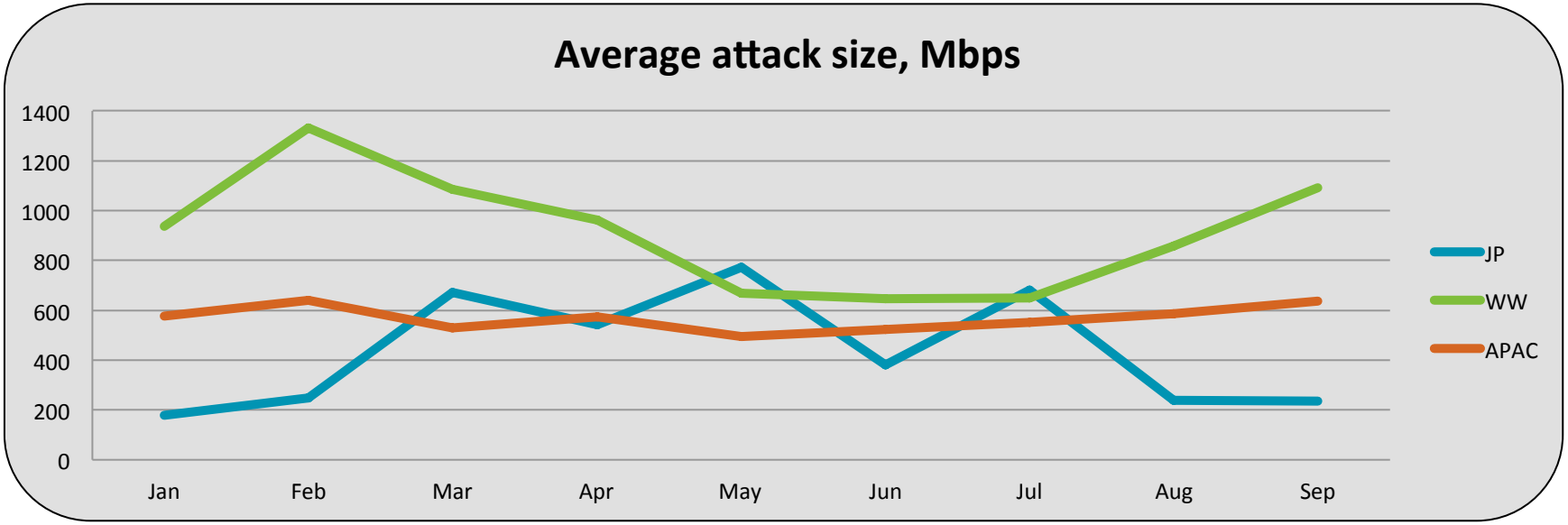




2014 ATLAS Initiative : Anonymous Stats, JP, APAC & WW

平均攻撃サイズの月次の推移　2014

- APAC において、平均攻撃サイズは、550Mbps - 650Mbps
- JPにおいて、3月から7月の平均攻撃サイズは、APACのそれと類似している

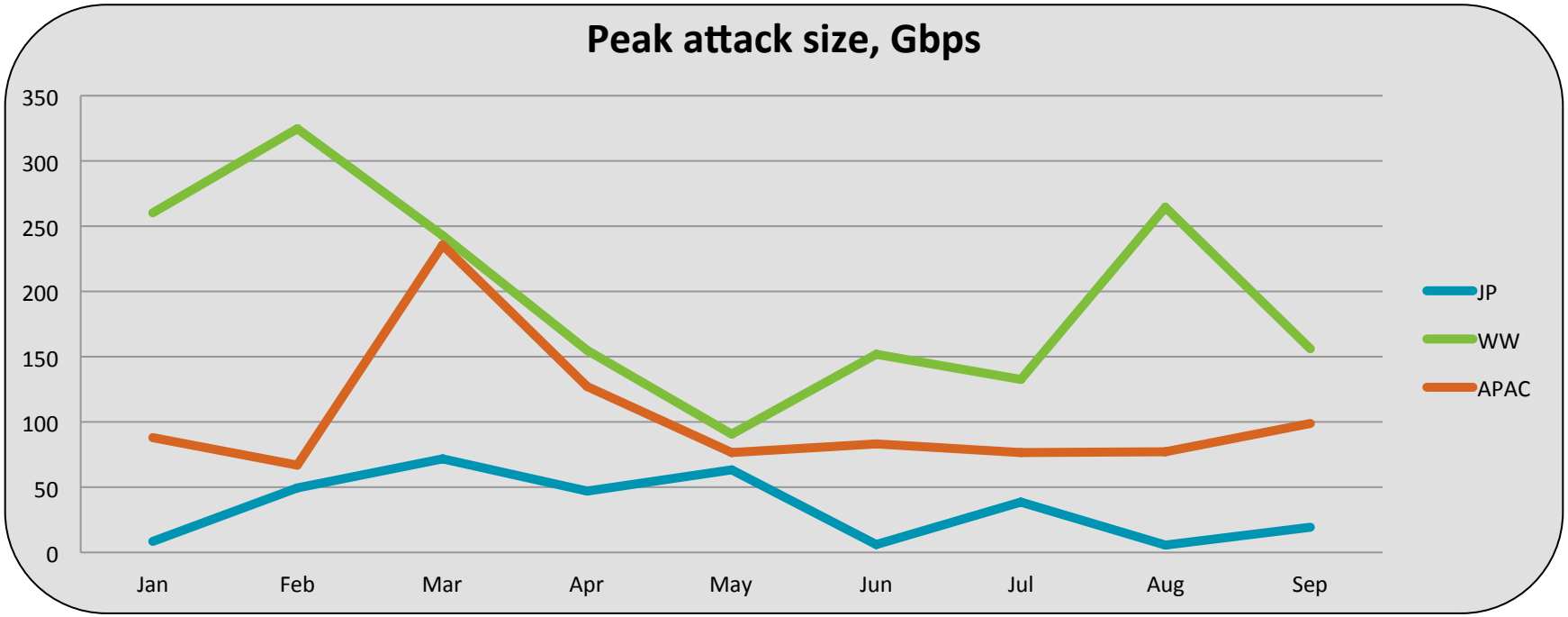


株式会社 東陽テクニカ　ARBOR NETWORKS

2014 ATLAS Initiative : Anonymous Stats, JP, APAC & WW

最大攻撃サイズの月次の推移　2014

- APAC において、3月、4月を除き、最大攻撃サイズは100Gbpsを下回っている
- JP において、最大攻撃サイズはほぼ50Gbpsを下回っている

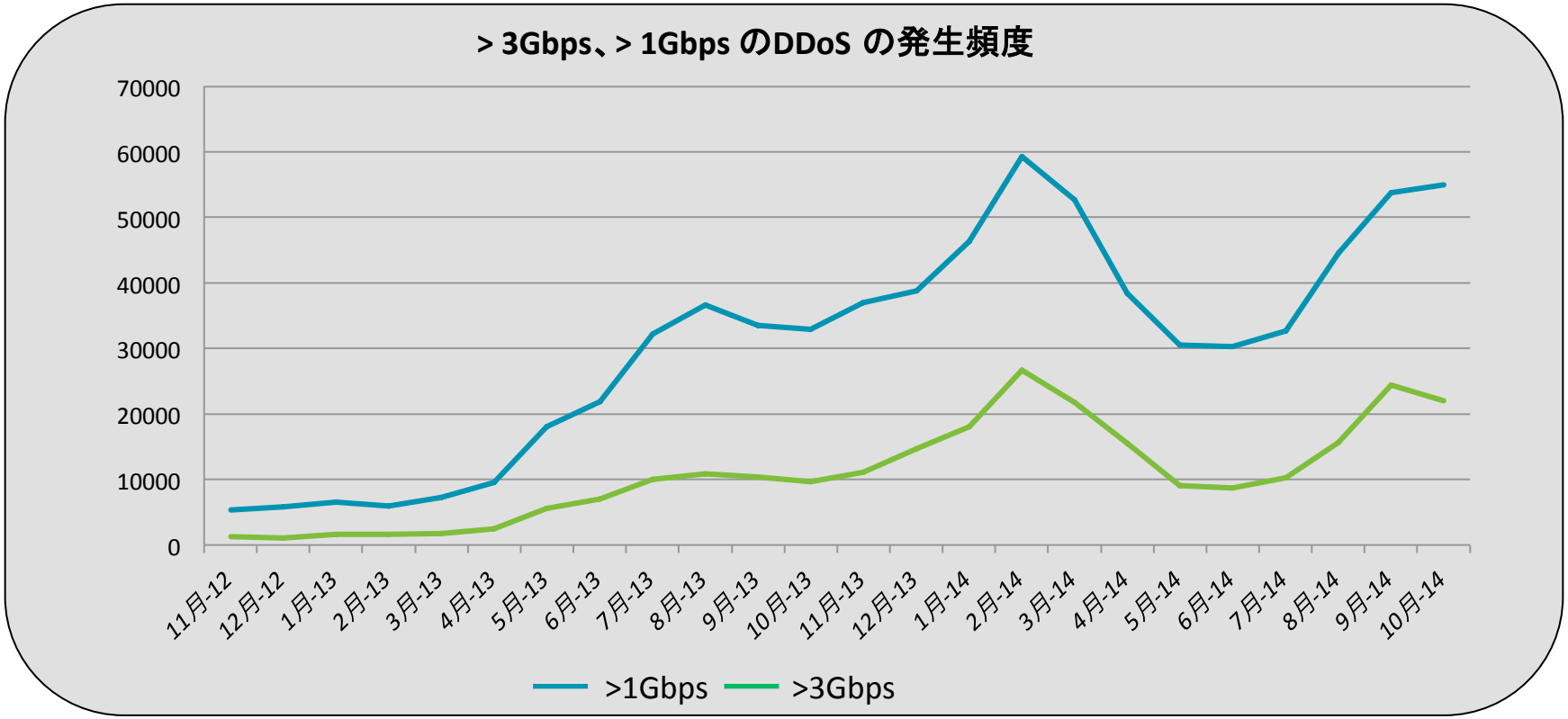


株式会社 東陽テクニカ　ARBOR NETWORKS

2014 ATLAS Initiative : Anonymous Stats, WW

最大攻撃サイズの月次の推移　2013/2014

- World Wide での、最大攻撃サイズ1Gbps以上、3Gbps以上のDDoS発生件数の推移



DDOS 検知と緩和

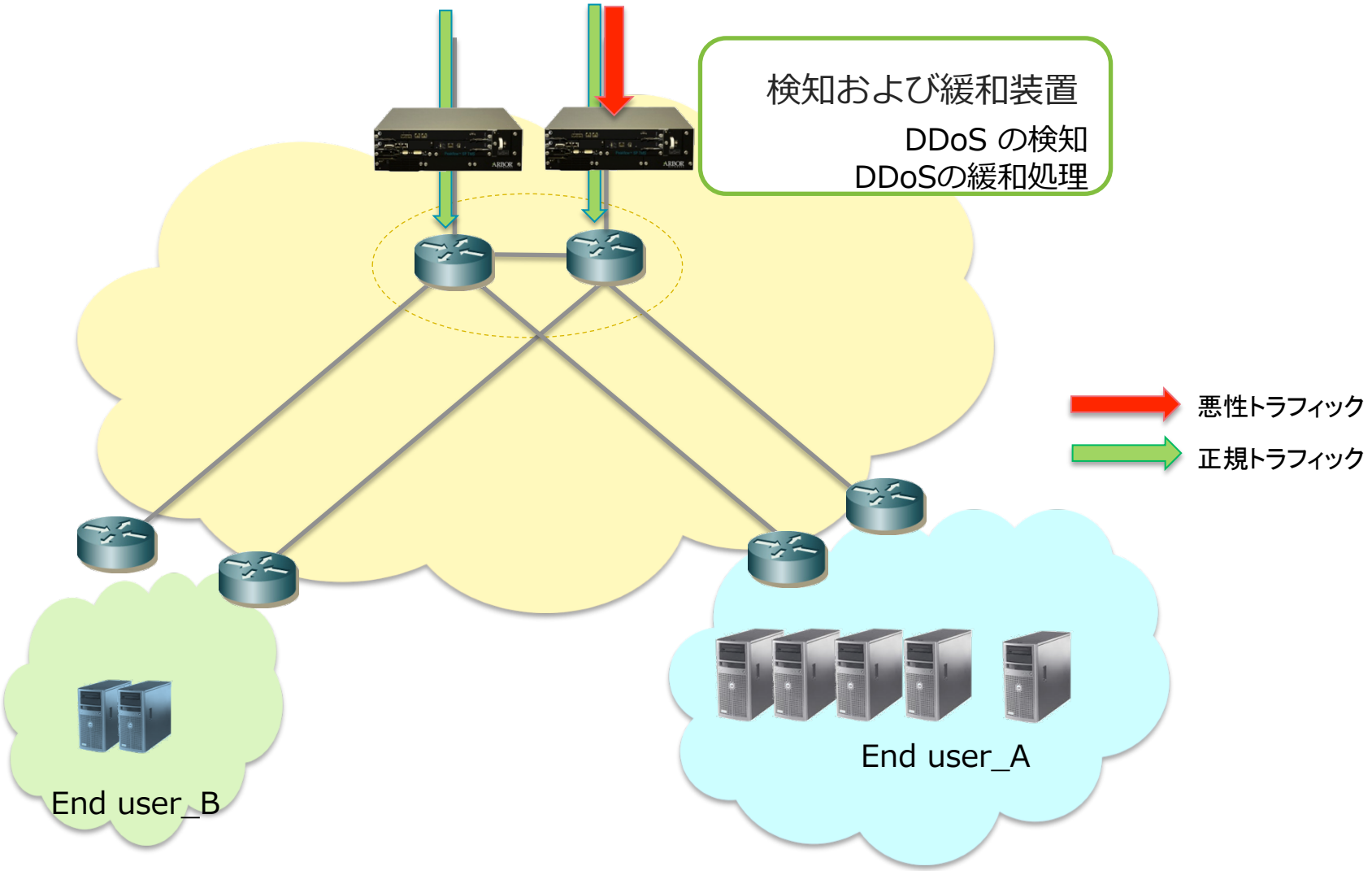
株式会社 東陽テクニカ
ARBOR NETWORKS

DDoS対策の目標

- DDoS の目的をくじく
  - とにかくサービスを落とさせない
    - 邪魔をする、嫌がらせをする、耳目をあつめるのが目的であれば、何としてもそれを阻止する

株式会社 東陽テクニカ
ARBOR NETWORKS

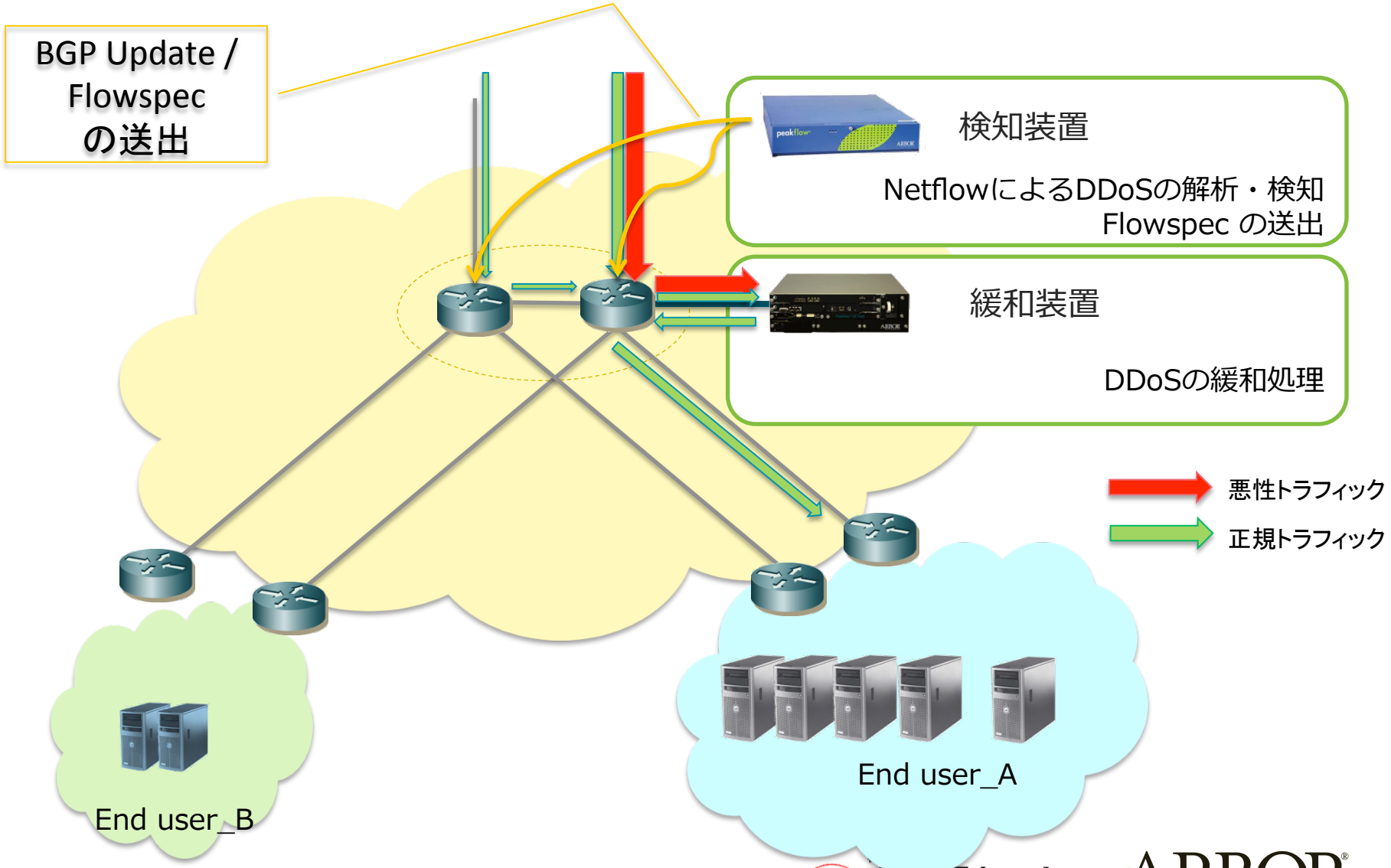
DDoS 対策機器の実装 - インライン型



株式会社 東陽テクニカ

ARBOR NETWORKS

DDoS 対策機器の実装 - Offramp 型



DDoS 検知、防御の実際

- 異常検知（Anomaly Detection)による検知
  - 閾値
  - Network Behavior Analysis（NBA / 振る舞い検知）
  - Deep Packet Inspection (DPI / プロトコル解析) まで行うと、大量のトラフィックに対応しきれない
    - 機器自身が気絶することがある
  - xFlow 技術を利用
    - 大量のトラフィックの検知を行うため、サンプリングされた xFlow 情報でよい
- 異常検知と不正検知（Misuse Detection）による緩和
  - 規約に違反したトラフィック
  - 閾値による制限

株式会社 東陽テクニカ ARBOR NETWORKS

検知と緩和 – インテリジェンスはどちらに置く？

検出装置 - Flowspec のイニシエーター	緩和装置 - DDoS 通信の排除
検知装置のインテリジェンスが十分高い - 検知精度が高く、攻撃性トラフィックのみを選択的に検知できる - 検知装置の負荷は高くなる - H/W の要求仕様も高くなり、価格も高くなるだろう	シンプルなフィルタリング機構でよい - 正規通信は回ってこないことを期待している - 機器に要求されるレベルもそれほど高くなくとも良い
検知装置は、DDoS が疑わしいトラフィックを検知する - 検知装置は、相対的に負荷が低くなる - 検知されたトラフィックには、正規通信が混じっている可能性がある	可能な限り、正規通信と攻撃性通信を判別する必要がある - 攻撃性が疑われるトラフィックを受信する - 正規通信を峻別し、それらを落とさない - 緩和装置の負荷は高くなる - H/W の要求仕様も高くなり、価格も高くなるだろう

株式会社 東陽テクニカ ARBOR NETWORKS

DDoS 緩和装置導入形態まとめ

インライン型	Offramp 型
回線の数分必要となる	共有資源となる
DDoSを含め、全部のトラフィックを観察し、処理しなくてはならない	攻撃性が高いと判定されたトラフィックのみを受信する
	Flowspec が生きる
耐障害性 - 障害発生時、機器をバイパスする機構が必要	耐障害性 - Flowspec の送出を停止し、通常のルーティングを行う

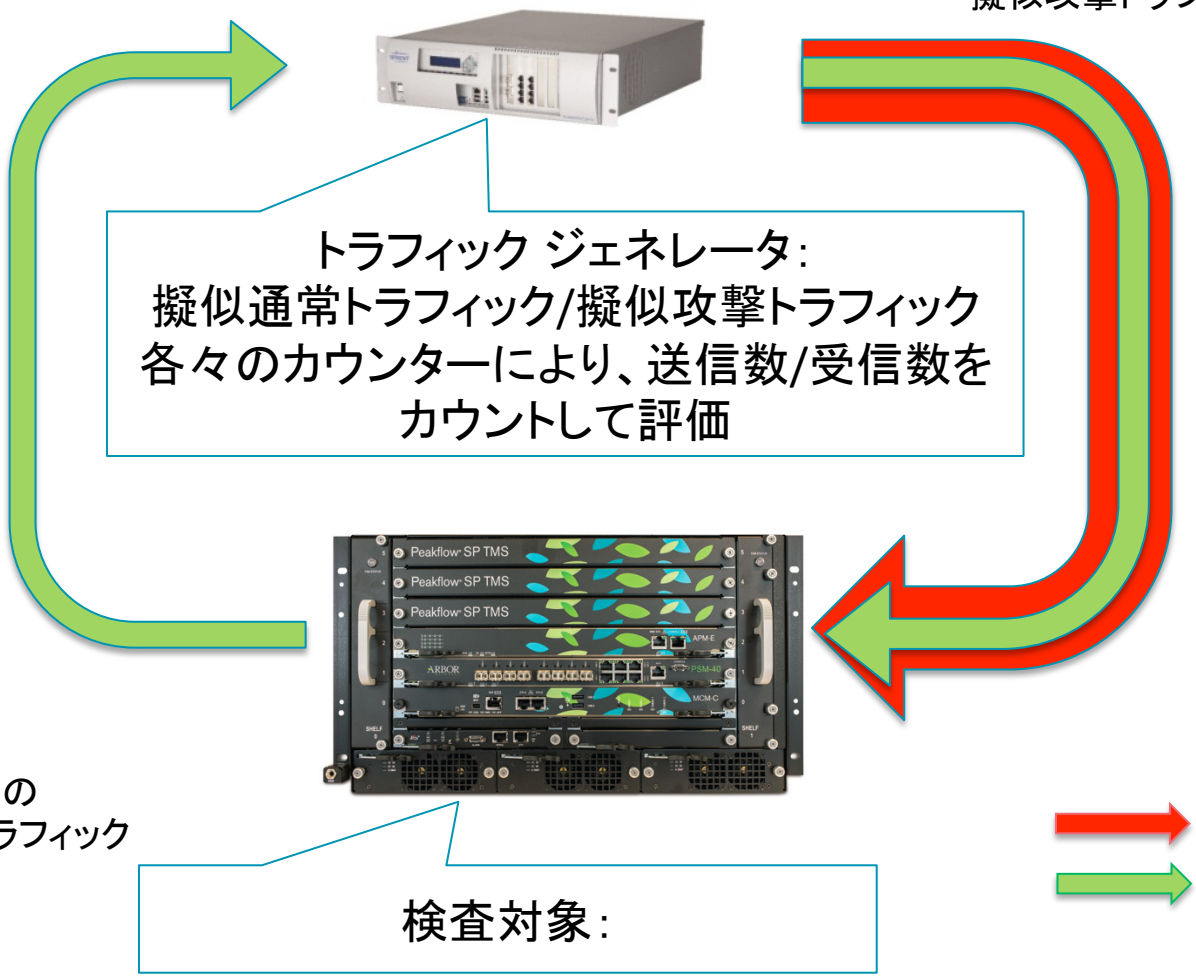
株式会社 東陽テクニカ ARBOR NETWORKS

DDoS 軽減装置試験の仕方

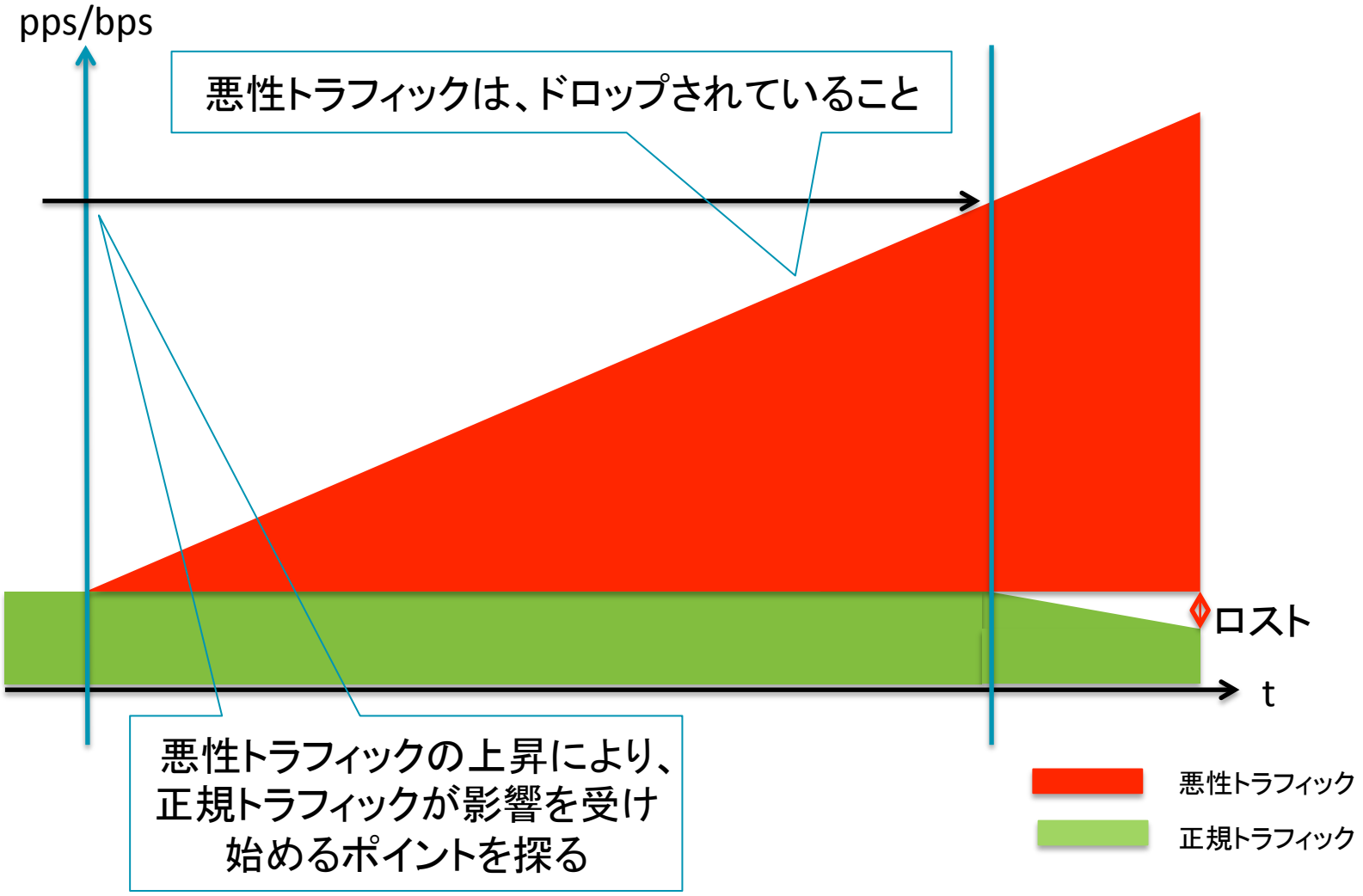
- 擬似通常トラフィックと擬似攻撃トラフィックを印加
- 擬似攻撃トラフィックは、トラフィック ジェネレーターの機能により定義する
  - 単一の攻撃対象IPアドレス、多数の攻撃元IPアドレス
  - DNS/NTP アンプ攻撃など、流行している手法を模擬
  - 様々なIPデータグラム長
  - Internet Mix
- 擬似通常トラフィックがドロップせずに、一定以上確保される通信帯域を確認する
  - 実際は多段にフィルタを適用するため、試験は、個々のフィルタリング機能ごとに評価する
  - チャレンジに対する応答をみる防御機構もあるため、実環境により変化する機能もある

株式会社 東陽テクニカ
ARBOR NETWORKS

試験環境


擬似通常トラフィックと
擬似攻撃トラフィック
トラフィック ジェネレータ:
擬似通常トラフィック/擬似攻撃トラフィック
各々のカウンターにより、送信数/受信数を
カウントして評価
Peakflow SP TMS
Peakflow SP TMS
Peakflow SP TMS
ARBOR
APM-E
PSM-10
MCM-C
緩和処理後の
擬似通常トラフィック
検査対象:
悪性トラフィック
正規トラフィック

DDoS 緩和機器対応可能帯域の決定



株式会社 東陽テクニカ

ARBOR NETWORKS