Internet Week 2016

T1 知って納得！企業のDDoS対処戦略
～基礎から実践まで～

4.DDoS時代のIXとの付き合い方
～IXPからみた現状と展望～

2016/11/29

BBIX株式会社 矢萩茂樹

AGENDA

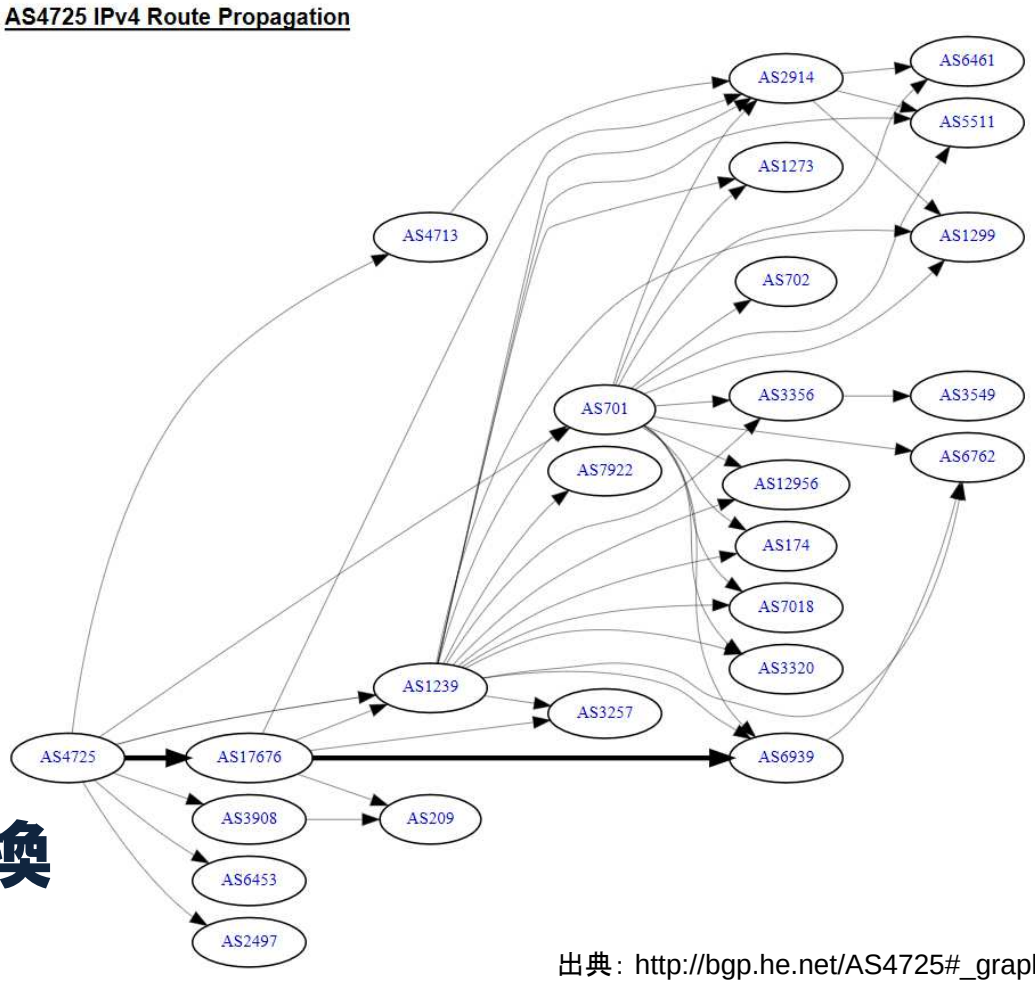
- Internetの構造とトラフィック分布とIX
- DDoSの傾向分析
- DDoSをIXとトランジットでどう防ぐか？

AGENDA

- Internetの構造とトラフィック分布とIX
  - Internetの構造とIX
  - インターネットトラフィック分布と流入傾向
- DDoSの傾向分析
- DDoSをIXとトランジットでどう防ぐか？

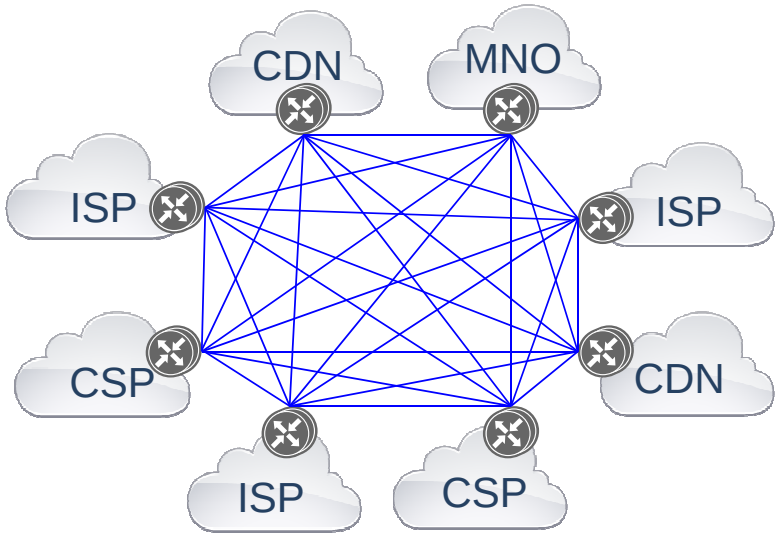
Internetの構造：ネットワーク組織=ASの集合体

- インターネットは独立したネットワーク組織の集合体
  - ネットワーク組織＝AS（Autonomous System）
- インターネット上位はAS間での接続となる
- AS間でBGP(Border Gateway Protocol)を利用して経路を交換

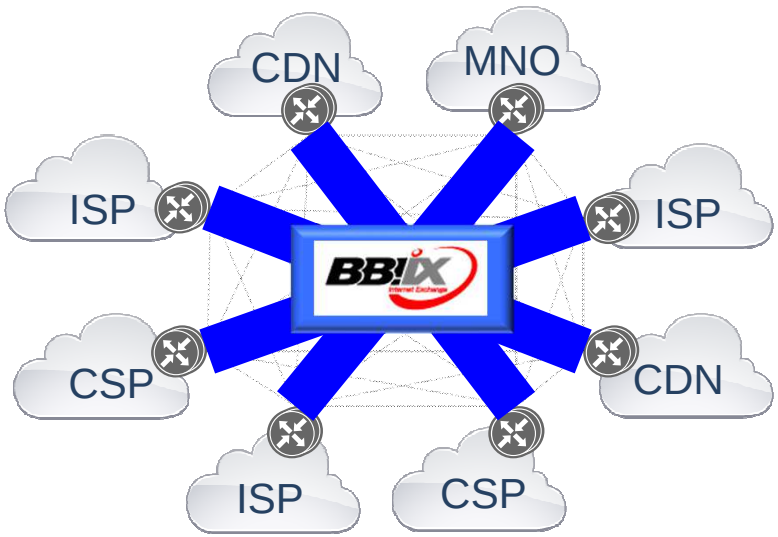


出典：http://bgp.he.net/AS4725#_graph4

Internet eXchange =
ネットワークを効率的に接続するためのトラフィック交換市場



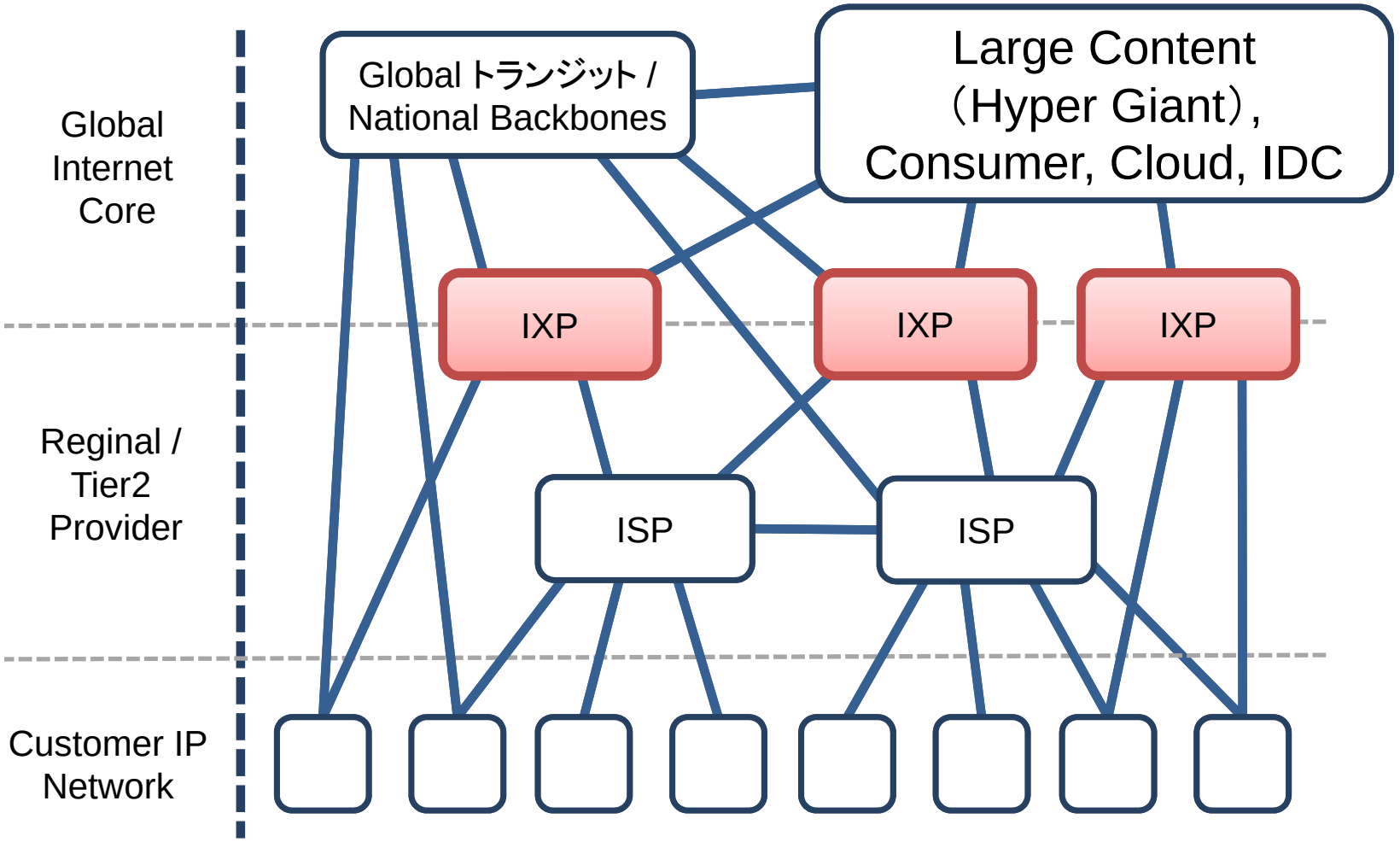
旧来の接続方式
複雑・細い帯域で非効率な構成



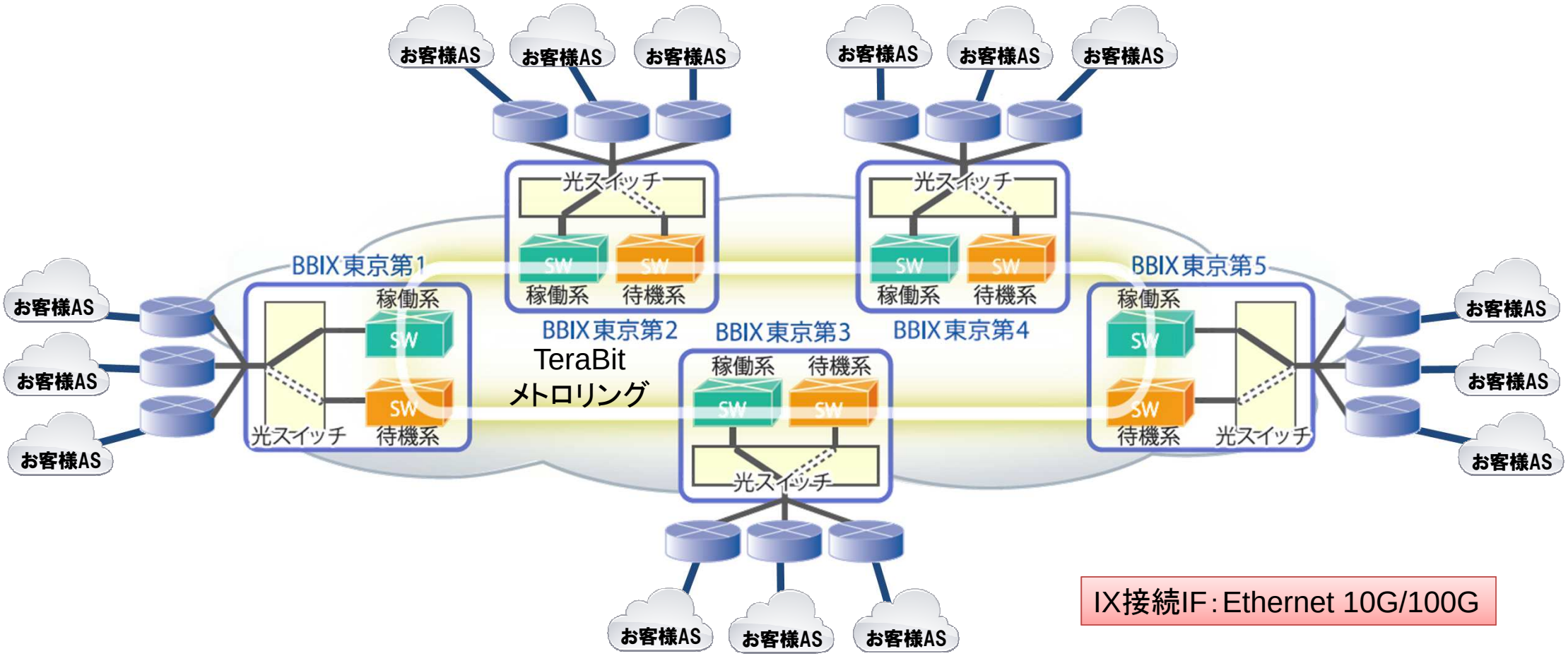
Internet eXchange
シンプルかつ広帯域回線で集約

- IX (Internet eXchange) =AS間の相互接続ポイント
- Internetに接続している組織が特定の場所 (IX) にあつまることで、相互接続を効率的に行えるトラフィック交換市場を提供
- 各AS参加者がL2接続し、BGPにより経路を交換することで相互接続する

IXのポジション（ Internetの構造 - 2009～ ）

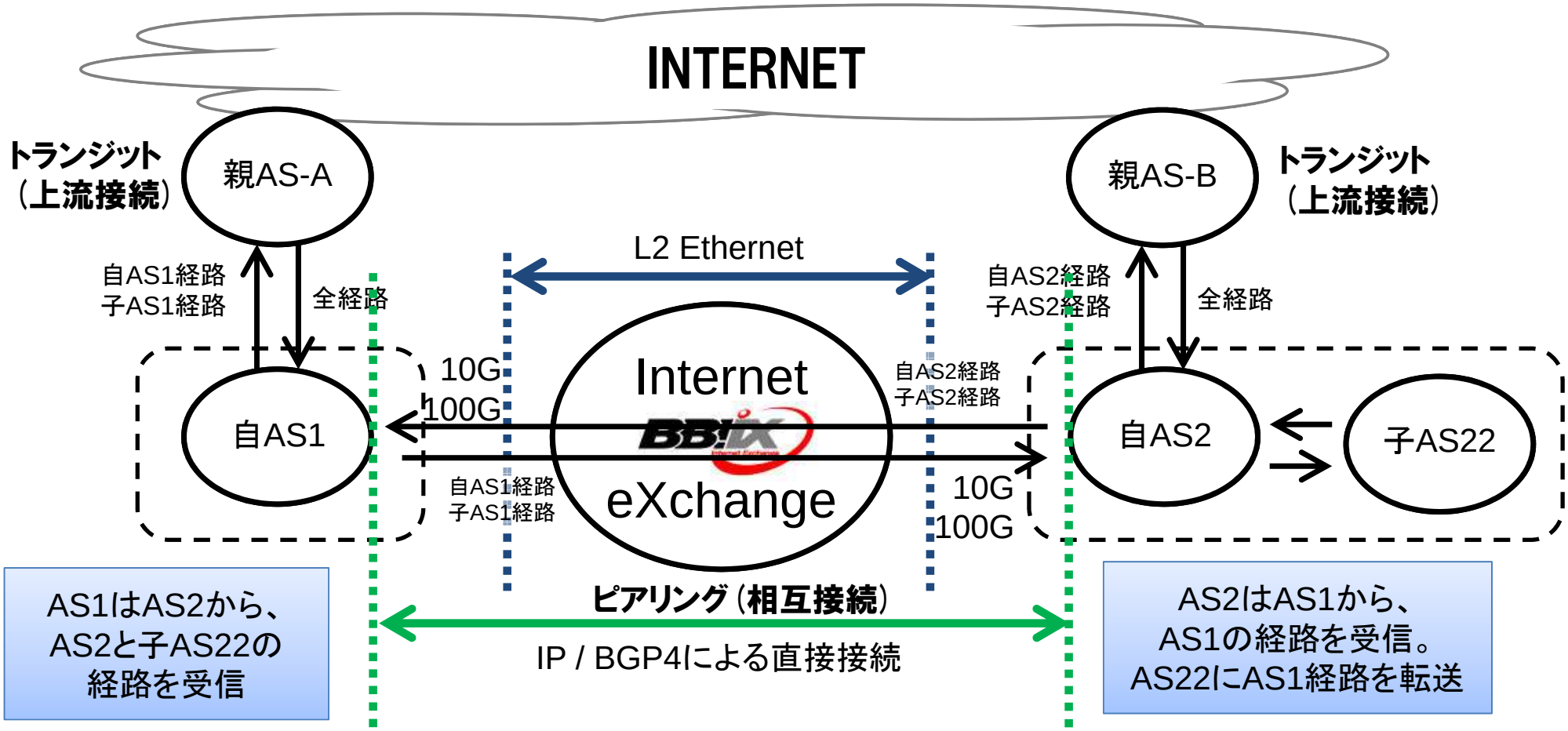


IXの構造（BBIX東京）



IX接続IF：Ethernet 10G/100G

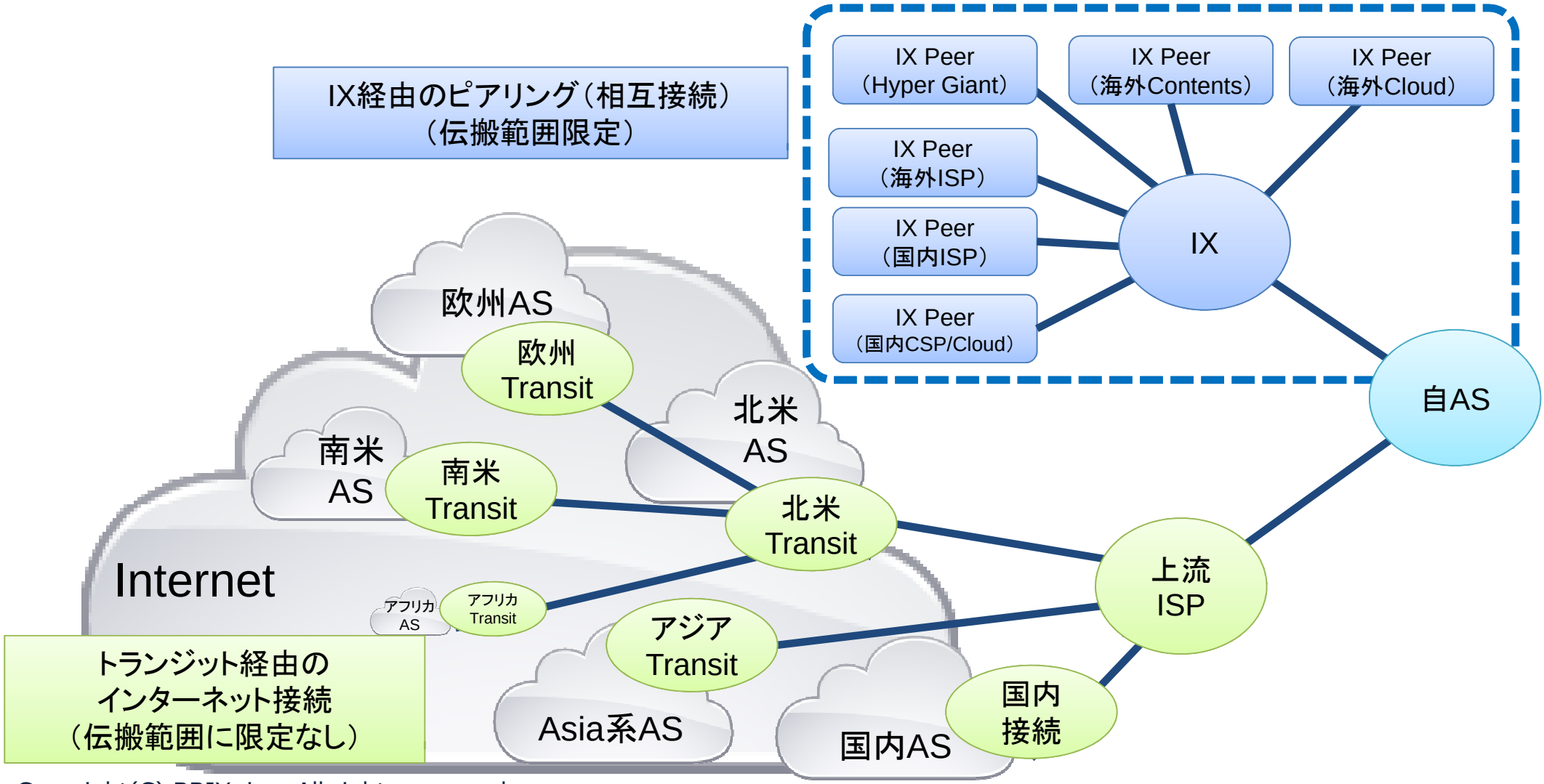
トランジットとピアリング（相互接続）



トランジットとピアリング（相互接続）

- トランジット（上流接続）→ ISPとの接続：トランジットだけAS接続：1～n
  - インターネット全ての経路・トラフィックを交換する
    - 上流ISPへは自ASと配下のASの経路を流す
    - 上流ISPからは全インターネットの経路をもらう
  - 上位プロバイダからサービスを有償購入
  - 売買契約が存在し、上流ISPには品質保持の義務が生じる
    → フィルタリングなどの対応依頼ができる
- ピアリング（相互接続）→ IXでの接続：ASの数だけBGP接続：数十～数百
  - 相互合意の下、お互いの配下の経路・トラフィックを交換する
    → 管理された自ASの経路を交換するため
  - 基本的には相互交換となるためほとんど場合、相互接続費用は発生しない
    - 大手とのピアリングについては最低トラフィック量クリアの条件が付く場合がある
  - 多くの場合、窓口交換の覚書による接続であり、相手のトラフィックやサービスレベルに保障や義務は生じない
    → BGPの経路制御は可能。人手のかかる作業依頼などは一般的に対応困難。

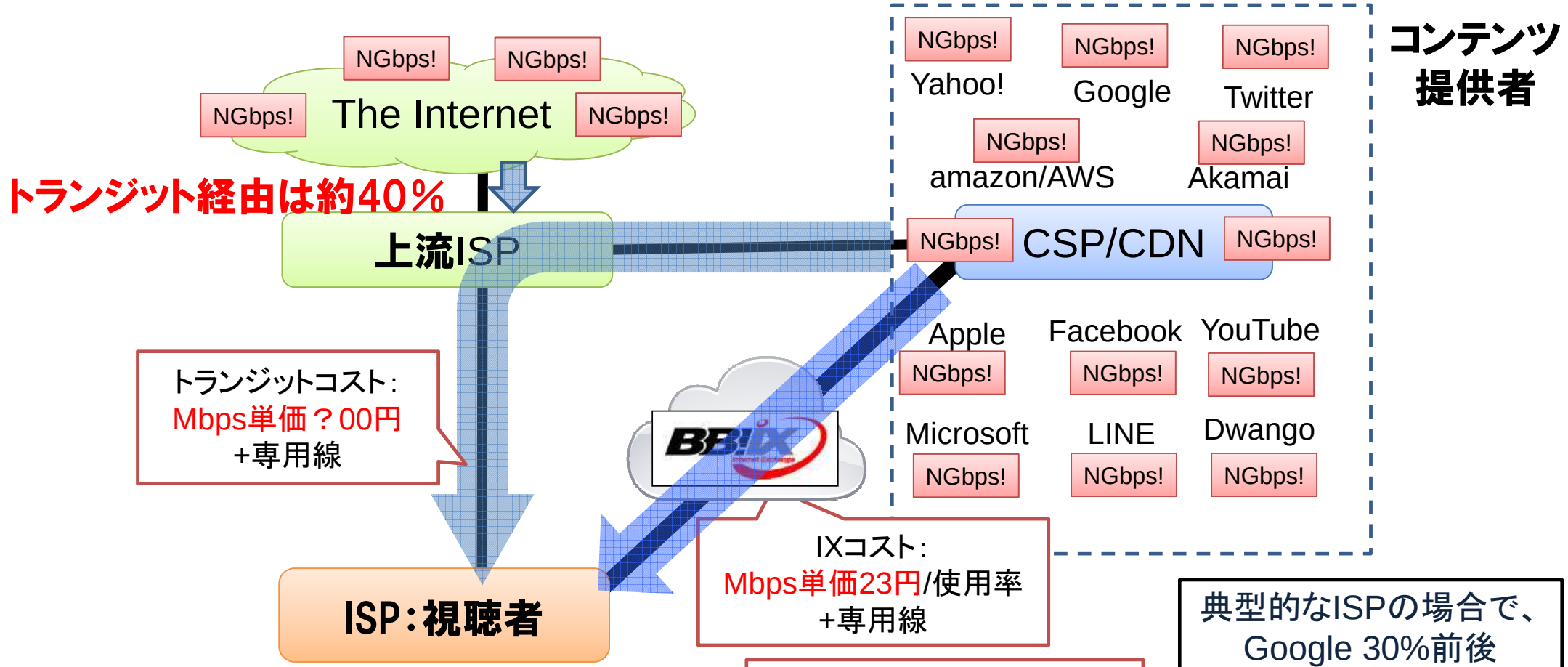
IXをとり入れたInternet接続構成



AGENDA

- Internetの構造とトラフィック分布とIX
  - Internetの構造とIX
  - インターネットトラフィック分布と流入傾向
- DDoSの傾向分析
- DDoSをIXとトランジットでどう防ぐか？

ISPからみたInternetのトラフィック分布

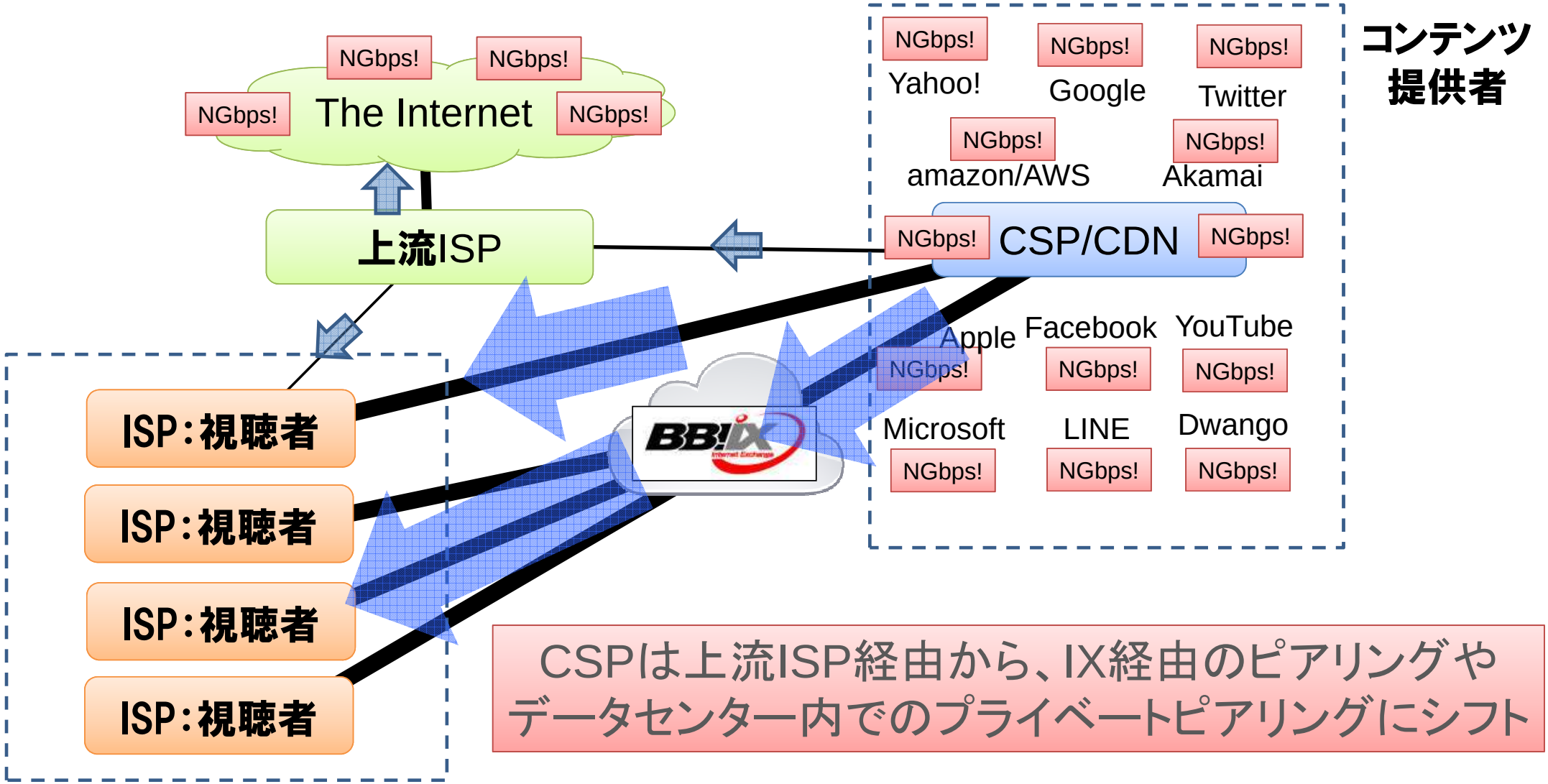


IXは視聴者とコンテンツ提供者を直接つなぐトラフィック交換市場

IX経由で交換できるトラフィック全体の60%

典型的なISPの場合で、
Google 30%前後
Akamai 15%前後
Top20AS 75%に集中

CSPからみたInternetのトラフィック交換経路



CSPは上流ISP経由から、IX経由のピアリングや
データセンター内でのプライベートピアリングにシフト

IXを介したトラフィックの流れ

2016/12現在（BBIX東京）

		Hyper Giant	国内	海外	総計
コンテンツ提供者	Contents	9	20	18	47
	Cloud	2	7	3	12
視聴者	ISP	---	41	10	51
	総計	11	68	31	110

Cloud 間通信

Japan Contens

コンテンツ提供者から視聴者へ

ISP加入者間通信

Internetの構造とトラフィック分布とIX：まとめ

- Internet接続形態はISPに完全依存していた構成から、ピアリング（相互接続）による直接接続構成が主流に
  - トラフィックはHyperGiant/大手CSP/大手ISPに8割以上集中
  - 大手間のトラフィック交換はIXやデータセンターでの相互接続が主流に

- IXはトラフィック交換市場：ISPとコンテンツ業者が集まる場
  - 各ASがIXに集まることでInternetの60%トラフィックをピアリングで交換可能

- トランジット（ISP経由の上流接続）とピアリング（IXでの相互接続）
  - トランジット接続には契約・SLAがあり、運用対処依頼が可能
  - IXでのピアリングは、各ネットワーク組織との相互接続となり、ピアリング相手との間にはサービスレベル保証や義務は生じない⇒運用対処依頼は困難

AGENDA

- Internetの構造とトラフィック分布とIX
- **DDoSの傾向分析**
- DDoSをIXとトランジットでどう防ぐか？

DDoS傾向分析：よくある仮説

- DDoSトラヒックは主に海外からやってくる?!
- 大規模なDDoSはほとんどない?!
- DDoSの多くは短時間で収まる?!

Akamai Report 2016-q2

Top 10 Source Countries for DDoS Attacks, Q2 2016

China	56.09%
US	17.38%
Taiwan	5.22%
Canada	3.77%
Vietnam	3.70%
Brazil	2.96%
Spain	2.94%
Singapore	2.90%
Italy	2.65%
UK	2.38%

Figure 2-6: China was the top source country for DDoS attacks, with a considerable increase in frequency compared with Q1 2016

- 1位：中国
- 2位：アメリカ
- 3位：台湾
- 4位：カナダ
- 5位：ベトナム
- 6位：ブラジル
- 7位：スペイン
- 8位：シンガポール
- 9位：イタリア
- 10位：イギリス

- ??位：日本????

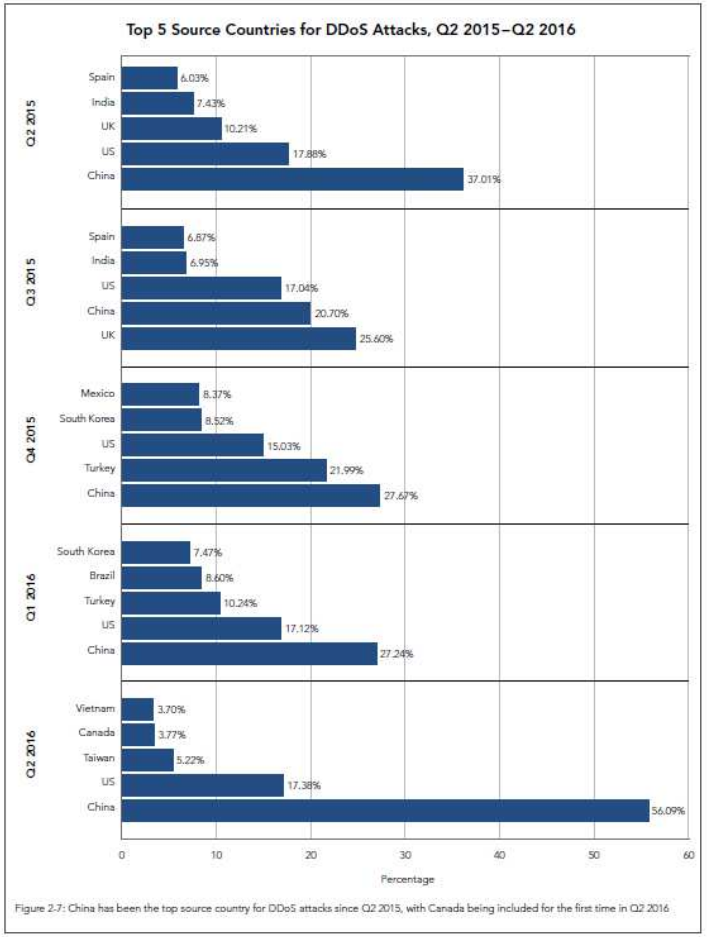
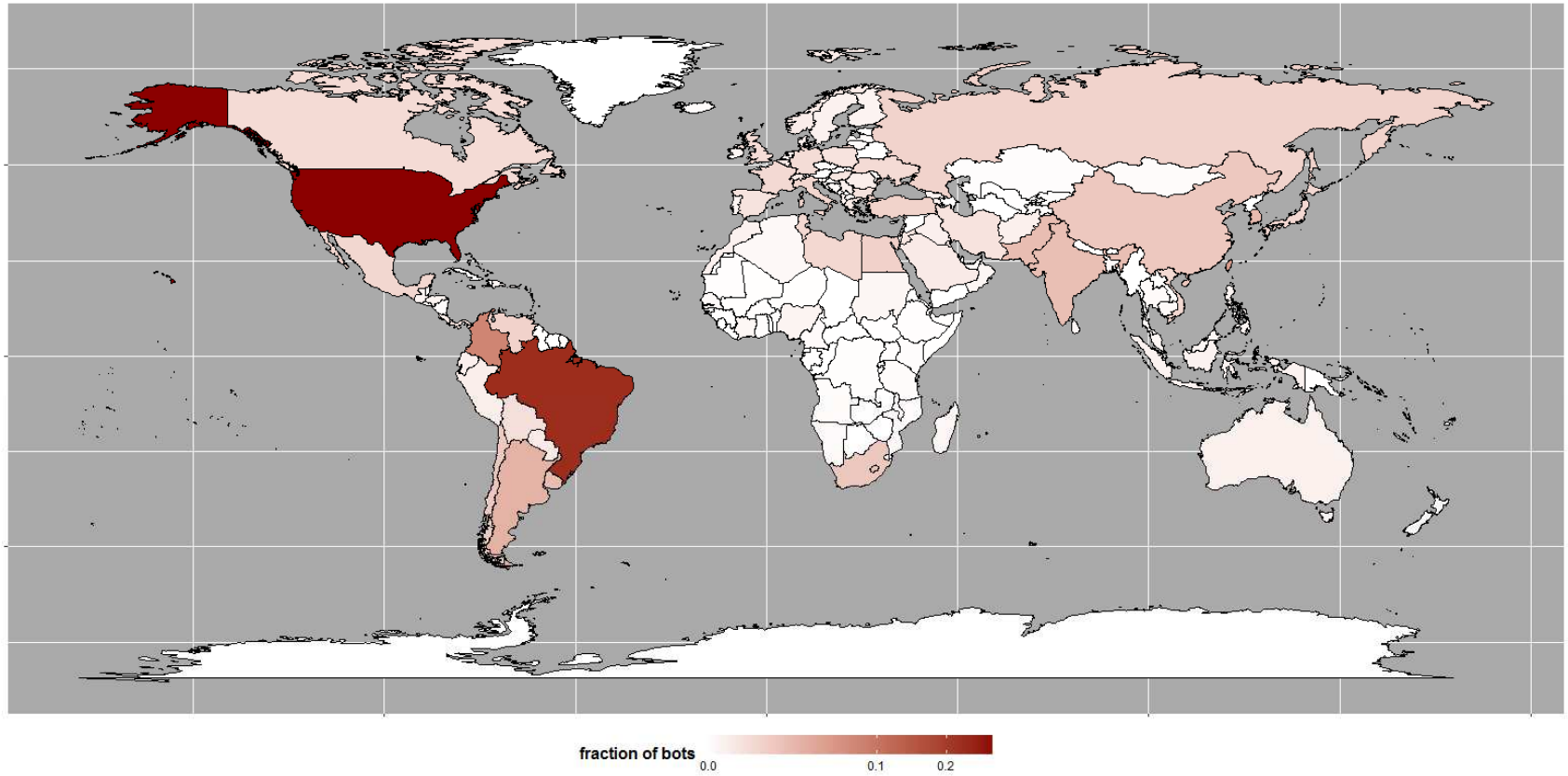


Figure 2-7: China has been the top source country for DDoS attacks since Q2 2015, with Canada being included for the first time in Q2 2016

出典：https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf

Fig4 Global Distributioin of Mirai bots



出典：http://blog.level3.com/security/grinch-stole-iot/

不正アクセス：port23/2323 国別上位20

- Internetに直接接続しているサーバにて計測
- ポート23/2323へのアクセス回数をFWログから解析
- 不正アクセスアドレスをAS情報に照らし合わせて、所属国を判定
- 解析期間：2016/11/2～9
- アクセスしてきたユニークIPアドレスとアクセス回数で集計
- ユニークIPアドレスでランキング

- ✓ 133か国からのアクセスを確認
- ✓ APNICエリアからのアクセスが非常に多い
- ✓ RIPE(東欧・ロシア)・LACNICからも多い
- ✓ Top10で66%。Top20で83%を占める
- ✓ 米国は規模に対して少ないが、1-IPあたりのアクセス回数頻度が多い
- ✓ 日本国内からのアクセスは非常に少ない

	gTLD	Registry	国名	アクセスIP数		アクセス回数		アクセス/IP	
1	VN	APNIC	ベトナム	1317	12.0%	2387	12.8%	1.8	
2	CN	APNIC	中華人民共和国	1271	11.6%	2486	13.3%	2.0	Top3
3	BR	LACNIC	ブラジル	961	8.8%	1510	8.1%	1.6	32%
4	TW	APNIC	台湾	805	7.3%	1766	9.4%	2.2	
5	RU	RIPE	ロシア	656	6.0%	951	5.1%	1.4	
6	TR	RIPE	トルコ	544	5.0%	813	4.3%	1.5	
7	IN	APNIC	インド	514	4.7%	625	3.3%	1.2	
8	UA	RIPE	ウクライナ	453	4.1%	594	3.2%	1.3	
9	KR	APNIC	大韓民国	386	3.5%	661	3.5%	1.7	Top10
10	RO	RIPE	ルーマニア	345	3.1%	631	3.4%	1.8	66%
11	US	ARIN	アメリカ合衆国	325	3.0%	986	5.3%	3.0	
12	MX	ARIN	メキシコ	275	2.5%	378	2.0%	1.4	
13	AR	LACNIC	アルゼンチン	214	2.0%	292	1.6%	1.4	
14	PL	RIPE	ポーランド	208	1.9%	365	2.0%	1.8	
15	IT	RIPE	イタリア	158	1.4%	175	0.9%	1.1	
16	CO	LACNIC	コロンビア	157	1.4%	239	1.3%	1.5	
17	FR	RIPE	フランス	148	1.3%	211	1.1%	1.4	
18	ID	APNIC	インドネシア	134	1.2%	157	0.8%	1.2	
19	CL	LACNIC	チリ	105	1.0%	134	0.7%	1.3	Top20
20	BG	RIPE	ブルガリア	89	0.8%	233	1.2%	2.6	83%
			その他	1898	17.3%	3036	16.2%	1.6	
			総数	10963		18704			
73	JP	APNIC	日本	12	0.1%	13	0.1%	1.1	

不正アクセス：port23/2323 AS Top20

- ✓ 1654ASからアクセス記録
- ✓ 上位は海外通信キャリア配下のアドレスからのもので占められる
- ✓ やはり、APNICエリアからが上位を占める
- ✓ 上位に米国のISP/Carrierはアクセスしてくるホストが少なく、このランキングからは見えない
- ✓ 日本からはアクセス数が非常に少ないが、やはり通信キャリア系からのアクセスが多い

	ASN	KIND	Network Name	gTLD	Registry	country	Unique IP		アクセス回数		アクセス/IP	
1	4134	Carrier	CHINANET-BACKBONE	CN	APNIC	中華人民共和国	753	6.9%	1614	8.6%	2.1	
2	3462	Carrier	HINET Data Communication Business	TW	APNIC	台湾	719	6.6%	1580	8.4%	2.2	Top3
3	45899	Carrier	VNPT(VietNam Post and Telecom)	VN	APNIC	ベトナム	551	5.0%	931	5.0%	1.7	18%
4	9121	Carrier	Turk Telekomunikasyon Anonim Sirketi	TR	RIPE	トルコ	424	3.9%	592	3.2%	1.4	
5	18403	Carrier	FPT Vietnum	VN	APNIC	ベトナム	350	3.2%	552	3.0%	1.6	
6	4837	Carrier	CNCGROUP China169 Backbone	CN	APNIC	中華人民共和国	277	2.5%	395	2.1%	1.4	
7	7552	Carrier	Viettel Corporation	VN	APNIC	ベトナム	270	2.5%	619	3.3%	2.3	
8	28573	Carrier	CLARO S.A.	BR	LACNIC	ブラジル	264	2.4%	397	2.1%	1.5	
9	18881	Carrier	Global Village Telecom	BR	LACNIC	ブラジル	224	2.0%	353	1.9%	1.6	Top10
10	4766	Carrier	Korea Telecom	KR	APNIC	大韓民国	201	1.8%	306	1.6%	1.5	37%
11	27699	Carrier	TELEFNICA	BR	LACNIC	ブラジル	155	1.4%	288	1.5%	1.9	
12	9829	Carrier	BSNL Broadband	IN	APNIC	インド	153	1.4%	170	0.9%	1.1	
13	15895	Carrier	Kyivstar PJSC	UA	RIPE	ウクライナ	150	1.4%	160	0.9%	1.1	
14	8708	Carrier	RCS-RDS RCS & RDS SA	RO	RIPE	ルーマニア	145	1.3%	246	1.3%	1.7	
15	17974	Carrier	PT Telekomunikasi Indonesia	ID	APNIC	インドネシア	126	1.1%	148	0.8%	1.2	
16	24086	Carrier	Viettel Corporation	VN	APNIC	ベトナム	124	1.1%	256	1.4%	2.1	
17	8151	Carrier	Aviso Uninet - Telmex	MX	ARIN	メキシコ	120	1.1%	218	1.2%	1.8	
18	12389	Carrier	PJSC Rostelecom	RU	RIPE	ロシア	105	1.0%	128	0.7%	1.2	
19	9050	Carrier	RTD TELEKOM ROMANIA	RO	RIPE	ルーマニア	101	0.9%	184	1.0%	1.8	Top20
20	24560	Carrier	Bharti Airtel Ltd. Telemedia Services	IN	APNIC	インド	96	0.9%	127	0.7%	1.3	48%
			その他				5655	51.6%	9434	50.4	1.7	
			総数				10963		18704			

	ASN	KIND	Network Name	gTLD	Registry	country	Unique IP		アクセス回数		アクセス/IP
208	4713	Carrier	OCN NTT Communications Corporation	JP	APNIC	日本	5	0.0%	5	0.0%	1.0
414	2519	ISP	VECTANT Ltd.	JP	APNIC	日本	2	0.0%	2	0.0%	1.0
664	2516	Carrier	KDDI CORPORATION	JP	APNIC	日本	1	0.0%	2	0.0%	2.0
664	2514	ISP	INFOSPHERE NTT PC Communications	JP	APNIC	日本	1	0.0%	1	0.0%	1.0
664	4765	ISP	World Net & Services Co. Ltd.	JP	APNIC	日本	1	0.0%	1	0.0%	1.0
664	7543	ISP	Pacific Internet (Australia) Pty Ltd	JP	APNIC	日本	1	0.0%	1	0.0%	1.0
664	17676	Carrier	Softbank Corp.	JP	APNIC	日本	1	0.0%	1	0.0%	1.0
			日本合計				12		13		1.1

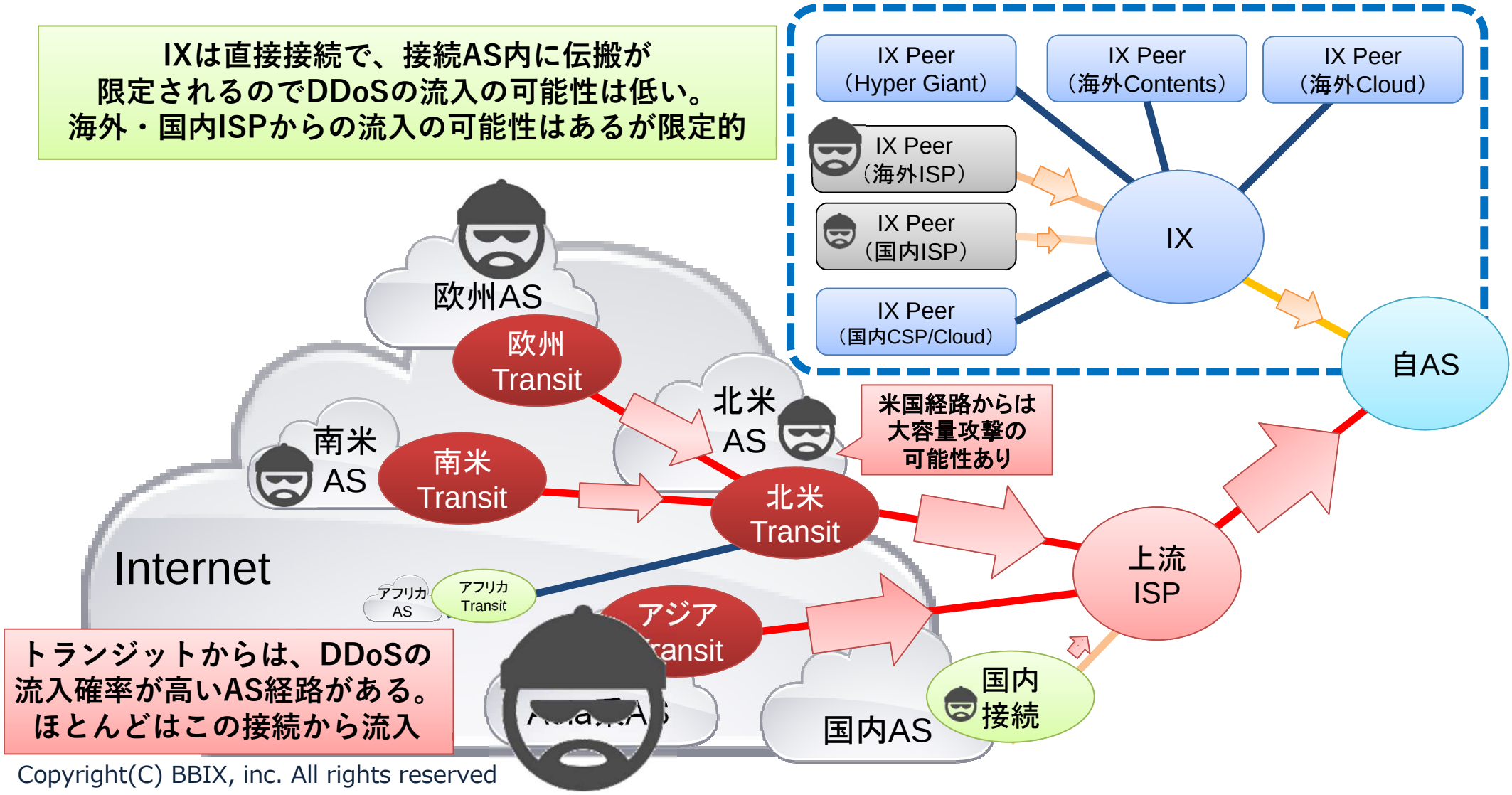
どこからDDoSはきそうか(IX)

		Hyper Giant	国内	海外	総計
コンテンツ提供者	Contents	9	20	18	47
	Cloud	2	7	3	12
視聴者	ISP	---	41	10	51
	総計	11	68	31	110

海外ISPからの攻撃の確率が高いが、
国内コンシューマーユーザからも流入の可能性はある

DDoSの流入経路は主に海外/コンシューマーから！

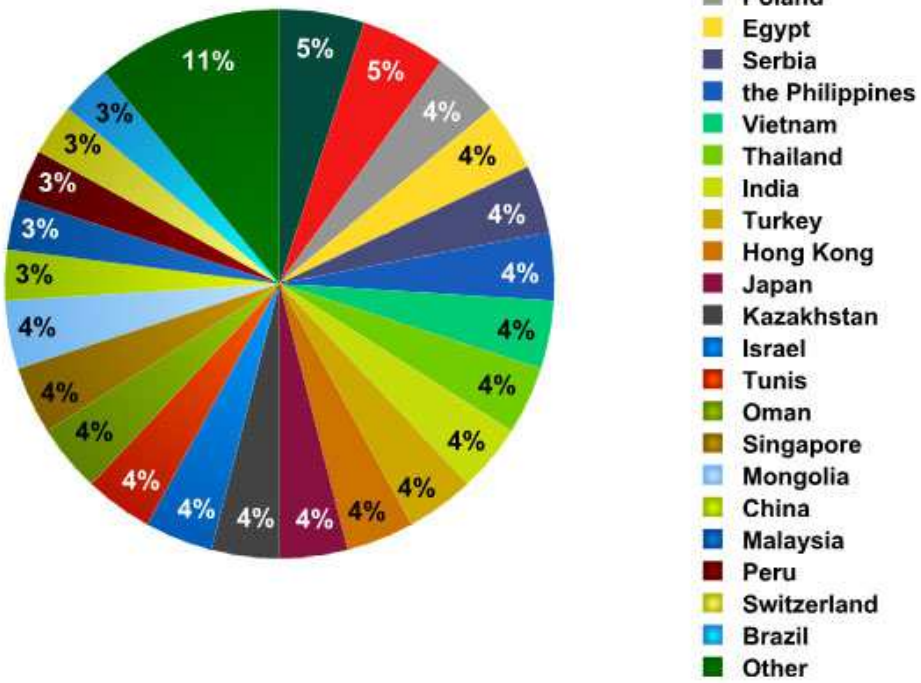
IXは直接接続で、接続AS内に伝搬が
限定されるのでDDoSの流入の可能性は低い。
海外・国内ISPからの流入の可能性はあるが限定的



トランジットからは、DDoSの
流入確率が高いAS経路がある。
ほとんどはこの接続から流入

ここで、DDoSのソースアドレス分布

- 実際のDDoS攻撃の
  ソースアドレス分布例
  - UDP/TCP SYN/ICMP Flooding
- 国が均等分布しているのは
  アドレス詐称されているため
- 発信源を追及するよりも、
  攻撃を受けているサイトの
  遮断・ミチゲーションを優先！



出典：**DDoS攻撃の無意味だけれど美しいグラフ from Fortinet**
http://www.fortinet.co.jp/security_blog/150703-beautiful-graphs-ddos.html

DDoS傾向分析：よくある仮説

✓ DDoSトラヒックは主に海外からやってくる?!

□ 大規模なDDoSはほとんどない?!

□ DDoSの多くは短時間で収まる?!

DDoSの観測事例

- ネットワーク種別：
- 測定期間：2016/8/1-10/26（87日間）
- 測定手段：
  - 測定データ：NetFlowデータ
  - Flowアナライザにより特定IP（/32）に閾値以上の通信がかかったケースを抽出
  - UDP Floodingイベントを抽出
  - 帯域：200M以上
  - 検知時間3分以上
- 分類種別：
  - 攻撃要素：攻撃帯域・攻撃経過時間・攻撃時間帯・攻撃曜日種別
  - IPアドレス種別：コンシューマー（ISPユーザ）・法人（専用線接続ユーザ）

DDoS：攻撃量と経過時間（コンシューマー）

ほとんどが
1Gbps以下(95%)

攻撃経過時間（分）

攻撃帯域	3-5分	6 -9分	10-19分	20-29分	30-44分	45-59分	60-120分	120分以上	総計
200Mbps～500Mbps	65.1%	13.1%	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	78.4%
500Mbps～1Gbps	10.9%	5.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	16.1%
1Gbps～5Gbps	2.1%	1.4%	1.0%	0.2%	0.1%	0.1%	0.1%	0.1%	4.9%
5Gbps～10Gbps	0.1%	0.2%	0.1%	0.1%	0.1%	0.1%	0.0%	0.0%	0.4%
10Gbps～20Gbps	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.1%
20Gbps以上	0.1%	0.1%	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%	0.1%
総計	78.3%	19.9%	1.2%	0.3%	0.1%	0.1%	0.1%	0.1%	100.0%

10分以内で
ほぼ終了(98%)

最大攻撃量　：31.6Gbps (4分)
最長攻撃時間：122分（1.8Gbps）

DDoS：攻撃量と経過時間（法人）

10分以内で56%
20分以内が80%

攻撃経過時間（分）

攻撃帯域	3-5分	6 -9分	10-19分	20-29分	30-44分	45-59分	60-120分	総計
200Mbps～500Mbps	8.6%	4.9%	0.0%	0.0%	0.0%	0.0%	0.0%	13.6%
500Mbps～1Gbps	2.5%	2.5%	0.0%	1.2%	0.0%	0.0%	0.0%	6.2%
1Gbps～5Gbps	17.3%	11.1%	16.0%	4.9%	2.5%	0.0%	0.0%	51.9%
5Gbps～10Gbps	1.2%	3.7%	3.7%	4.9%	0.0%	2.5%	1.2%	17.3%
10Gbps～20Gbps	0.0%	3.7%	4.9%	0.0%	0.0%	0.0%	2.5%	11.1%
総計	29.6%	25.9%	24.7%	11.1%	2.5%	2.5%	3.7%	100.0%

1G～10Gの
攻撃で69%

最大・最長攻撃：17.7Gbps (62分)
コンシューマーより大規模かつ長時間の攻撃となる

攻撃確率 時間統計(コンシューマー)

各曜日・時間帯ごとの攻撃回数を集計 単位:%

発生曜日	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	総計
月	0.6	1.0	0.8	0.7	0.7	0.6	0.7	0.4	0.5	0.5	0.4	0.7	0.5	0.7	0.5	0.7	0.5	0.8	0.5	0.7	0.5	0.3	0.3	0.4	14.2
火	0.5	0.7	0.4	0.8	0.5	0.9	0.4	0.4	0.5	0.6	0.6	0.6	0.6	1.1	0.7	0.8	0.7	0.4	0.8	0.9	0.8	0.4	0.3	0.3	14.8
水	0.9	0.8	0.4	0.4	0.7	0.3	0.5	0.5	0.7	0.3	0.8	0.4	0.4	0.4	0.4	0.5	0.5	0.6	0.4	0.7	0.4	0.5	0.5	0.4	12.4
木	0.4	0.7	0.9	0.5	0.2	0.7	0.6	0.5	0.7	0.4	0.4	0.8	0.5	0.5	0.5	0.5	0.5	0.7	0.4	0.4	0.7	0.4	0.4	0.5	13.0
金	0.3	0.8	0.3	1.0	0.8	0.6	0.5	0.2	0.2	0.7	0.4	0.2	0.5	0.7	0.7	0.5	0.4	0.8	0.5	0.4	0.5	0.5	0.3	0.3	12.0
土	0.3	0.9	0.7	0.5	0.5	0.7	0.5	0.8	0.5	1.0	0.7	0.5	0.6	0.8	1.4	0.9	0.7	0.8	0.8	1.1	0.5	0.5	0.2	0.5	16.6
日	0.5	0.5	0.7	0.8	0.8	0.7	0.5	0.4	0.6	0.5	1.0	0.7	0.4	0.9	0.9	0.9	0.8	1.0	1.2	0.6	0.5	0.6	0.7	0.7	17.1
総計	3.6	5.4	4.2	4.8	4.1	4.6	3.8	3.2	3.7	4.1	4.4	3.8	3.7	5.0	5.1	4.8	4.2	5.1	4.6	4.8	3.9	3.2	2.7	3.1	100

Fletsなどの固定接続ユーザ。土日の攻撃が多い。平日深夜も多い。

攻撃確率 時間統計(法人)

各曜日・時間帯ごとの攻撃回数を集計 単位:%

発生曜日	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	総計
月	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.2	2.5	0.0	1.2	1.2	0.0	1.2	2.5	1.2	1.2	2.5	0.0	0.0	14.8
火	0.0	0.0	0.0	0.0	0.0	1.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.5	1.2	0.0	0.0	0.0	0.0	0.0	1.2	0.0	0.0	0.0	6.2
水	2.5	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	2.5	2.5	0.0	1.2	0.0	0.0	1.2	0.0	1.2	1.2	1.2	0.0	13.6
木	0.0	0.0	0.0	7.4	4.9	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.2	0.0	0.0	0.0	0.0	3.7	0.0	2.5	2.5	0.0	1.2	23.5
金	1.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.2	2.5	3.7	0.0	0.0	0.0	1.2	1.2	0.0	1.2	0.0	12.3
土	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.2	1.2	0.0	0.0	0.0	1.2	0.0	0.0	0.0	2.5	0.0	0.0	3.7	1.2	0.0	0.0	0.0	11.1
日	0.0	1.2	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	1.2	1.2	0.0	2.5	0.0	0.0	1.2	1.2	0.0	0.0	6.2	0.0	3.7	18.5
総計	3.7	1.2	0.0	7.4	4.9	1.2	0.0	1.2	1.2	0.0	0.0	2.5	7.4	7.4	7.4	6.2	2.5	2.5	8.6	6.2	8.6	12.3	2.5	4.9	100

一般法人の固定接続部分。曜日関係なく11時～21時までが多い。

あるDDoS傾向分析結果

法人への攻撃は大容量・長時間化の傾向

	コンシューマー	法人
攻撃量	1Gbps以下が95%	1Gbps以下　20% 1G-10Gbps　69% 10Gbps以上　11%
攻撃時間	10分以内 98%	10分以内 56% 20分以内 80%
最大攻撃量	31.6Gbps(4分)	17.7Gbps(62分)
最長攻撃時間	122分(1.8Gbps)	62分(17.7Gbps)
発生傾向	土日・平日深夜が多い	曜日を問わず 11時から21時が多い

10Gbps以上の大規模攻撃は少ない

10分以内の短時間攻撃が多く、短時間で終息の傾向

とはいえ、大規模・長時間攻撃で狙い撃ちされた際の被害甚大➡備えは必要

仮説の答え合わせ

- ✓DDoSトラヒックは主に海外から ○ 正解!
- ✓大規模なDDoSはほとんどない ○ 正解!
- ✓DDoSの多くは短時間で収まる ○ 正解!

AGENDA

- Internetの構造とトラフィック分布とIX
- DDoSの傾向分析
- **DDoSをIXとトランジットでどう防ぐか？**
  - **IXでの対処法：RTBH on L2**
  - IXを含めたDDoSへの対処

IXでの対処法：RTBH on L2

- どんなパケットでも廃棄するブラックホールIPアドレス（Blackhole Next-hop：BN）をIXで準備
- DDoSうけて無効化したいIPが判明したら、ブラックホール指定（BN）で攻撃を受けているASから経路広報。当該IPへの通信はIXで廃棄
  - 本処理中、当該IPのIX経由通信は利用不可となる
- ブラックホールへの誘導方法
  - 方法1（RouteServer経由）：Blackhole Communityをつけて経路広報。
  - 方法2（直接Peering）：Next-hopをBlackhole IP（BN）にして経路広報
  - 無効化するIPは、IPv4で1IP（/32）単位、IPv6で1IP（/128）単位。廃棄対象を小さくすると被害が少ないが効果は限定的（後述）

IXブラックホール：アドレス・コミュニティ

◆ IXでのBlackhole Community

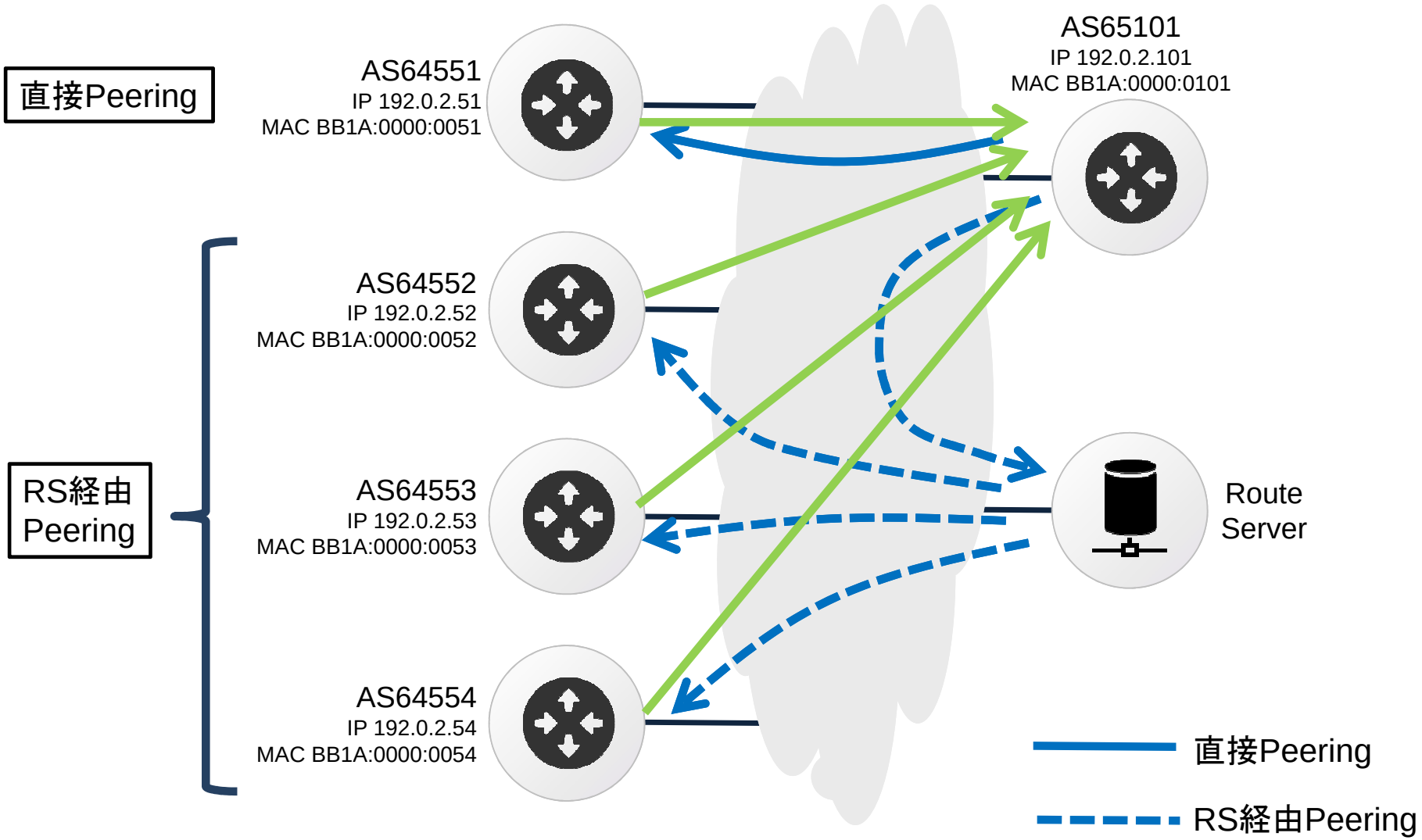
	RFC7999	DE-CIX	MSX-IX	Equinix	HKIX	BBIX
Blackhole Community	65535:666	65535:666	0:666	65535:666	4635:666	65535:666

◆ BBIX Blackhole Community / Address

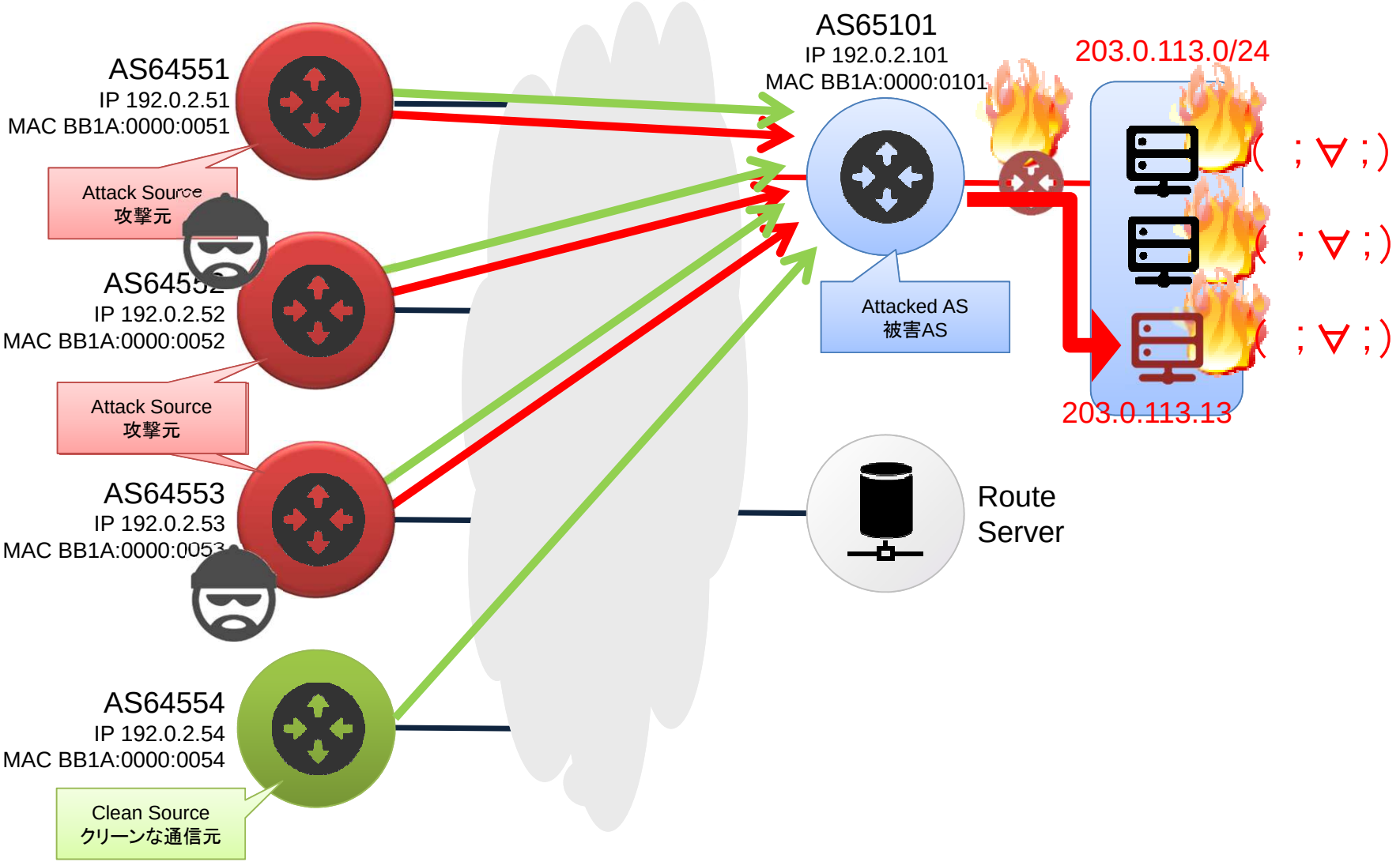
	IPv4 Blackhole	Blackhole MAC	Blackhole Community
Hong Kong	103.203.158.166	0200:dead:0103	65535:666
Singapore	103.231.152.166	0200:dead:0101	65535:666
Tokyo	218.100.6.166	0200:dead:0100	65535:666

※BBIX東京　Blackhole Communityは2017/3より提供予定

通常のトラフィックの流れ



AS65101防戦中

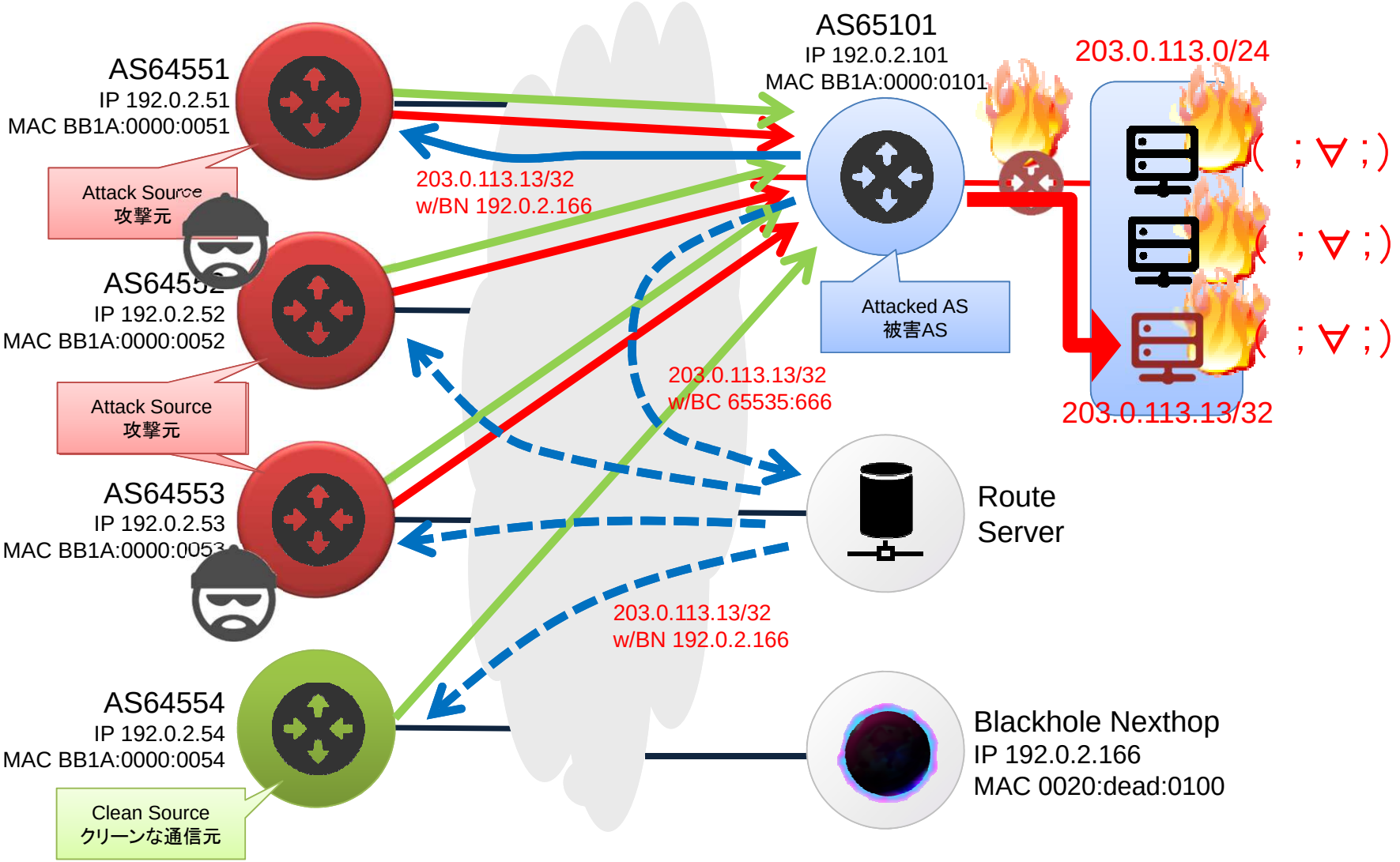


IX BlackholeによるDDoS攻撃の防御

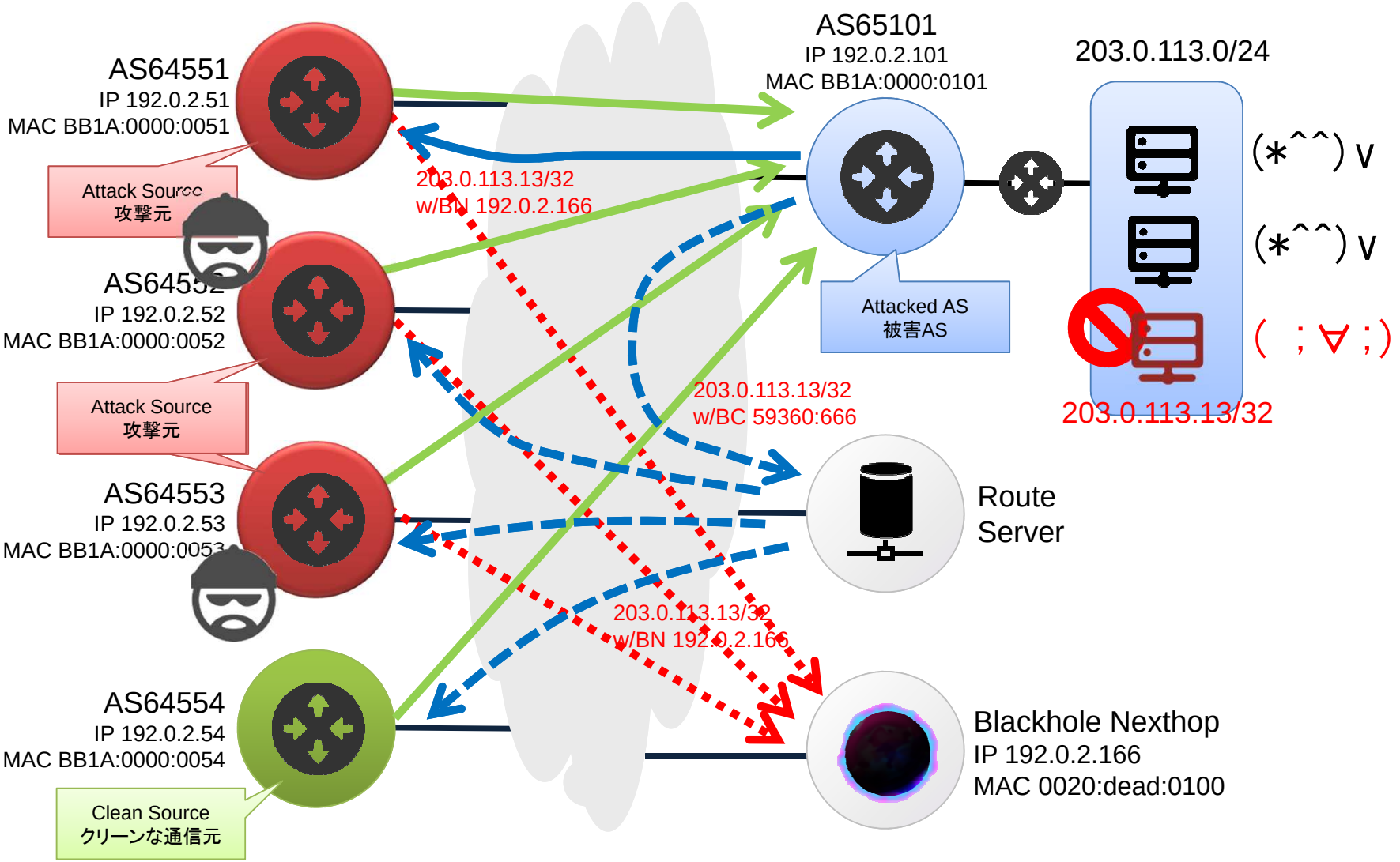
- AS65101はDDoSに対抗するために、攻撃を受けているPrefix (/32) に対しBlackhole Communityをつけてアナウンスを開始
- Route ServerはBlackhole Communityを受信することで、当該PrefixをBlackhole Nexthop (BN) に付替えて広報する
- 直接接続しているAS64501っは、当該PrefixにBNをつけてアナウンスすることで、Blackholeに誘導する
- PeeringしているASは/32経路を受信することで、アナウンスされた経路をベストパスとして認識。BN MACアドレスの解決はBBIX Proxy ARPサーバーにより行う
- BN MACのついたパケットはBBIXスイッチのACLにより入側(Ingress)にて廃棄される

- Blackholeに落とされるPrefixへの通信は遮断されることとなるが、他のPrefixへの通信は回復する。

IX RTBHによるDDoS攻撃防御：BNアナウンス



IX RTBHによるDDoS攻撃の防御：BNへ誘導



IXでのRTBHの課題

- IX Blackholeは対処を被害ホストに限定して、全Peerに対応できるメリットがあるが、課題も多い

- 課題１：相互接続での受け入れポリシー/32問題
  - 国内AS間接続では通常、/24より深いアナウンスは受けつけないのが一般的。
    現状では/32アナウンスの効果は参加者への効果は限定的。(/24なら効果あり)
  - とはいえ、一般ルール化され総括的に対応できる手順はIX RTBHしかないことから、
    IX参加者が/32受入れしてくれるコンセンサスの形成が課題

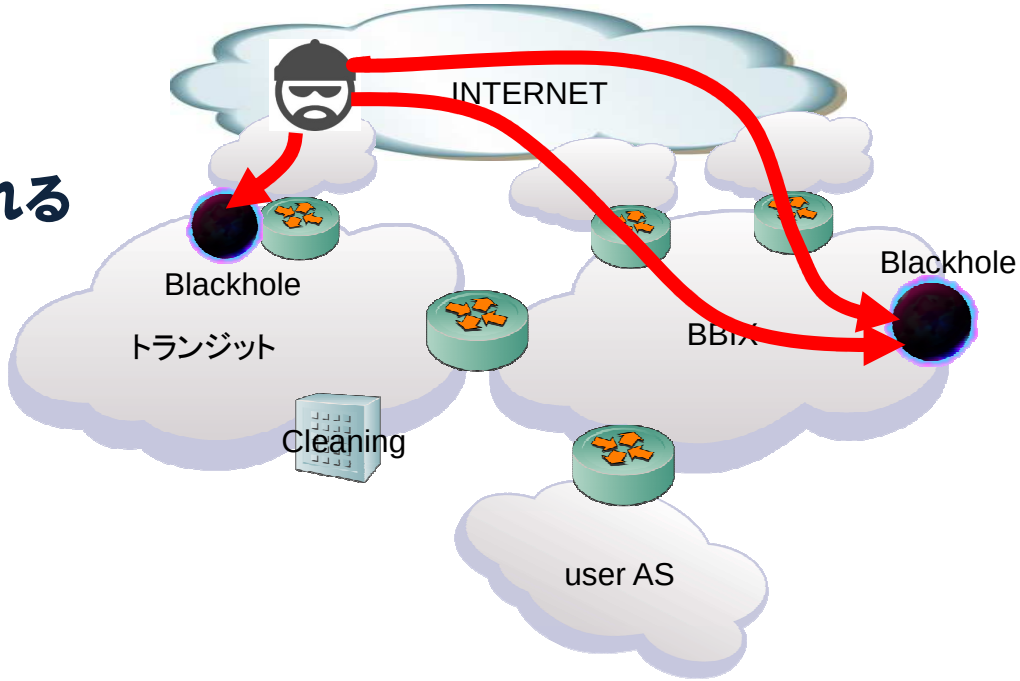
- 課題2：Blackholeコミュニティーの設定
  - IXでのBlackhole処理はIXが準備したBlackhole Nexthop：BNに誘導するCommunity設定が必要
  - IX提供のRoute Server：RSには実装されているが、RSを経由しない直接Peeringの場合、
    Communityが使えず、落としたいIPアドレスのNextHopをBN指定してのアナウンスが必要
    → この設定はtemplateなど下準備が結構必要
  - ルーターベンダーのRFC7999の実装に期待

AGENDA

- Internetの構造とトラフィック分布とIX
- DDoSの傾向分析
- **DDoSをIXとトランジットでどう防ぐか？**
  - IXでの対処法：RTBH on L2
  - **IXを含めたDDoSへの対処**

DDoS対策に必要なこと

- DDoSが来るのは海外からが多い。ほとんどはトランジット接続回線から流入
  - DDoSはIX Peerからもくる可能性があるが、IXだけからくることはほぼない
- トランジットへのフィルター依頼対応では、対処までには時間がかかり、
  短時間でのDDoSに対しては対応不能
- 対外接続をBGP化すると、自分の意思で
  制御することができ、対応速度の高速化される
- トランジット/IXと連携した対応策
  ① RTBH:Blackhole Routing
  ② 経路広報規制



対策：守るべきものは何か

- 対策にあたってはどこまでを守るかを明確化が必要
  - サービス　　：全サービス？優先サービス？必須サービス
  - 自分のNW　　：全ネットワーク？ 特定ホスト？サブネット？
  - アクセス　　：全Internetが必要？特定地域アクセスは遮断できる？
国内アクセスだけでも守ればどうか？

- 特定ホストを犠牲にすることで対処→RTBH：Blackhole対処
- 特定エリア（例えば日本国内）のみのアクセスを防御→流入経路規制

- 犠牲にできないものについては、DDoS緩和機構の保護検討に
  - Mitigation装置による保護
  - CDN/ISPのスクラビングサービスでの保護

総合的対策1:トランジットでの対策

① Blackhole対処

② 流入経路規制

規制方法	Community	制御内容
BLACKHOLE	4725:9999	広報した/32経路に関し、AS4725ですべてのトラフィックを廃棄する
流入経路規制	4725:10000	AS4725から米国向けに広報しない
流入経路規制	4725:600	AS4725からアジア向けに広報しない
流入経路規制	4725:500	AS4725から国内向けに広報しない

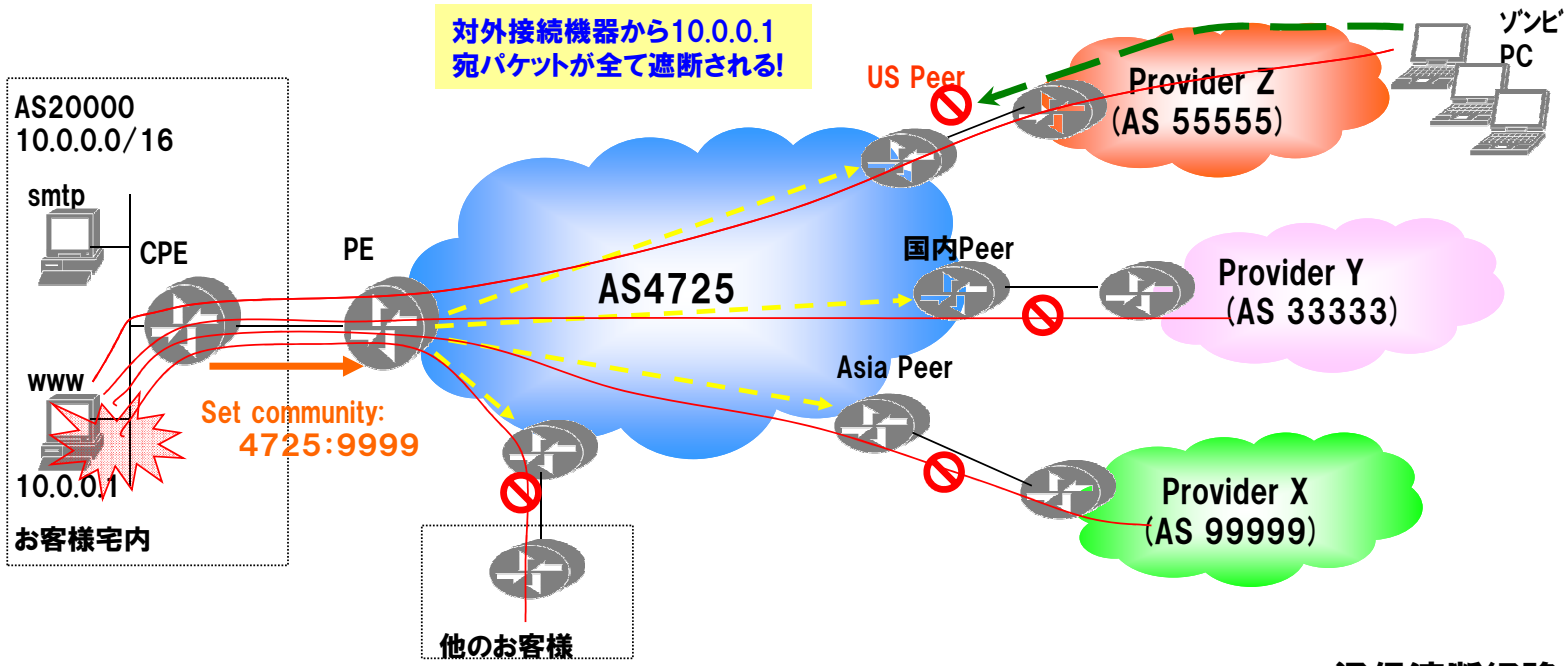
トランジットでのBlackhole制御例

◆ご要望

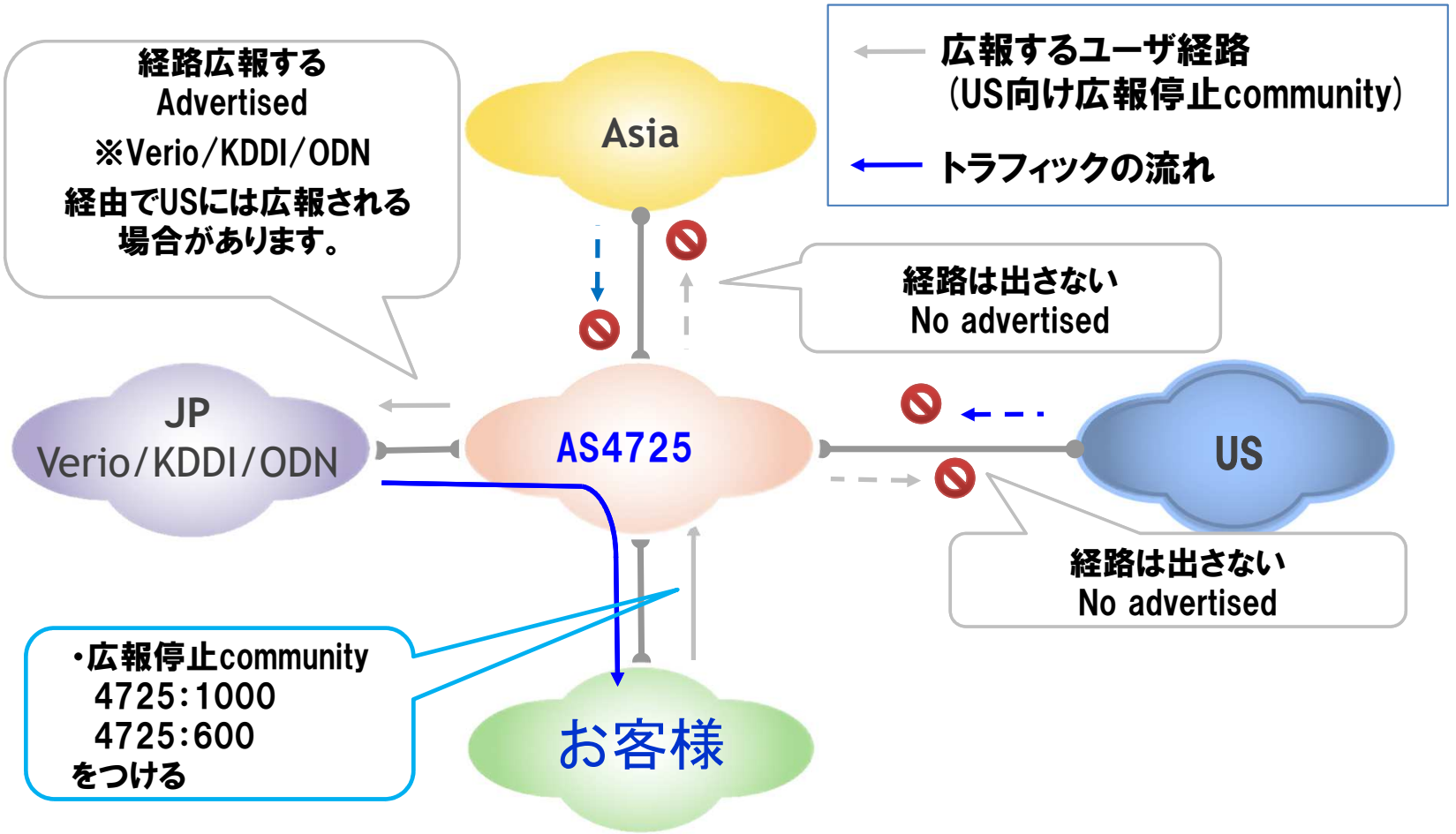
USのISP経由でお客様サイト内特定サーバ（WWW）がDDoS攻撃を受けており、他のSMTPサービスなどが回線の逼迫によりスムーズに運用できない被害を被っておりこれを防止したい。

◆対応方法

1. お客様 CPEにてwwwアドレス（10.0.0.1/32）に対しcommunity 4725:9999 を付与し広報する
2. PEでは受け取った /32 経路にLOCAL-AS を 付加し, Local Preferenceを強く4725網内に広報
3. 対外接続用ルータでは community 4725:9999がついている経路へのトラフィックを破棄する
4. US ISP軽油だけでなく、wwwアドレス（10.0.0.1/32）に対する全パケットを破棄する。



トランジットでの経路規制による対処例



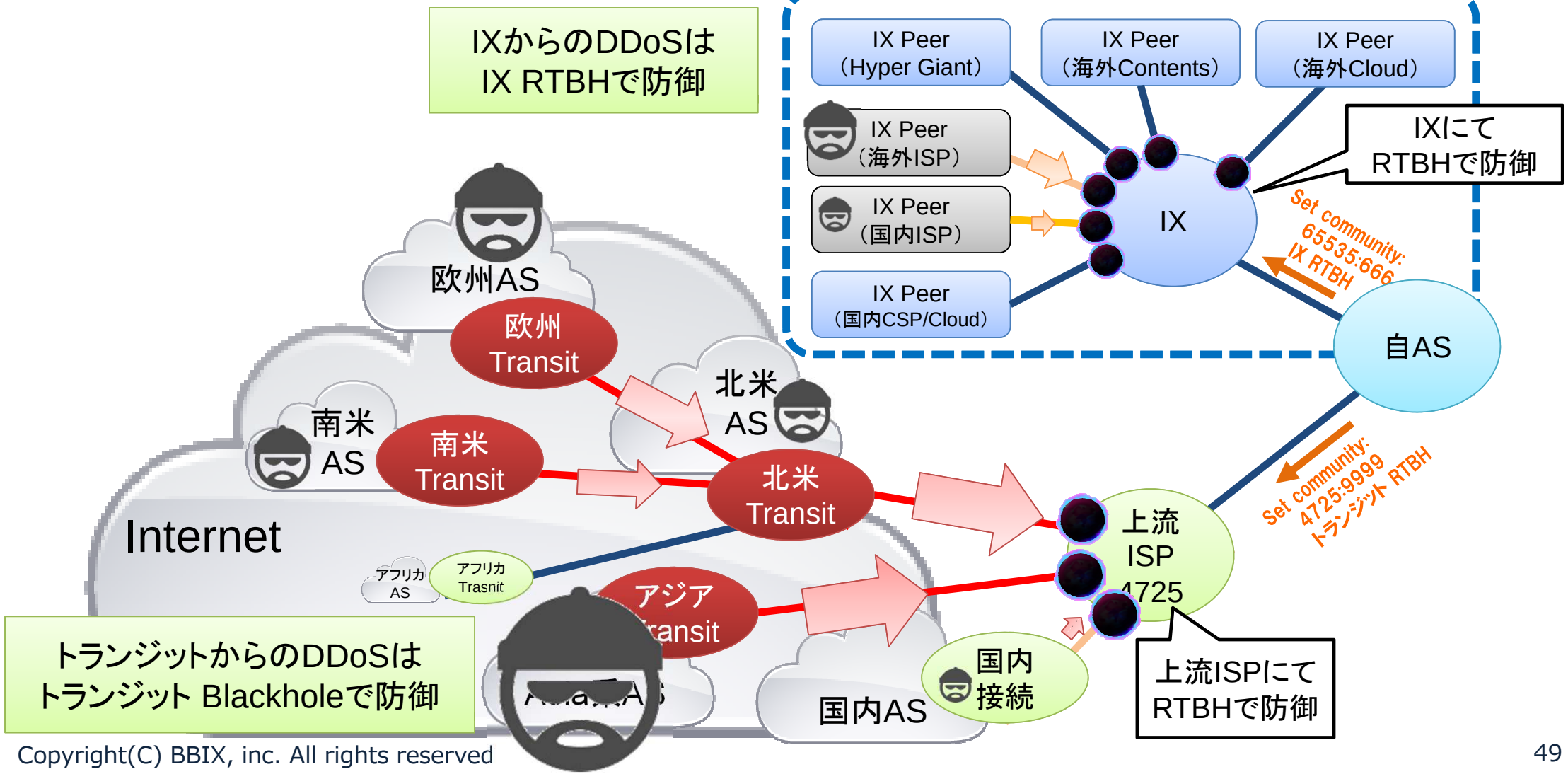
上記の場合、コミュニティ付与して広報したアドレスに対して、US・Asia向けへ広報するのを停止。
US・Asiaからみたお客様宛のパスは無くなるので、海外からのトラフィック流入を制限することが可能。
結果、国内のみに経路広報することが可能です。

総合的対策2：IXでの対応

- トランジットからのDDoS対処はしたがIXから止まっていない。どうする？
  - IXでの接続はピアリング（相互接続）では、フィルター追加など能動的な作業依頼できない

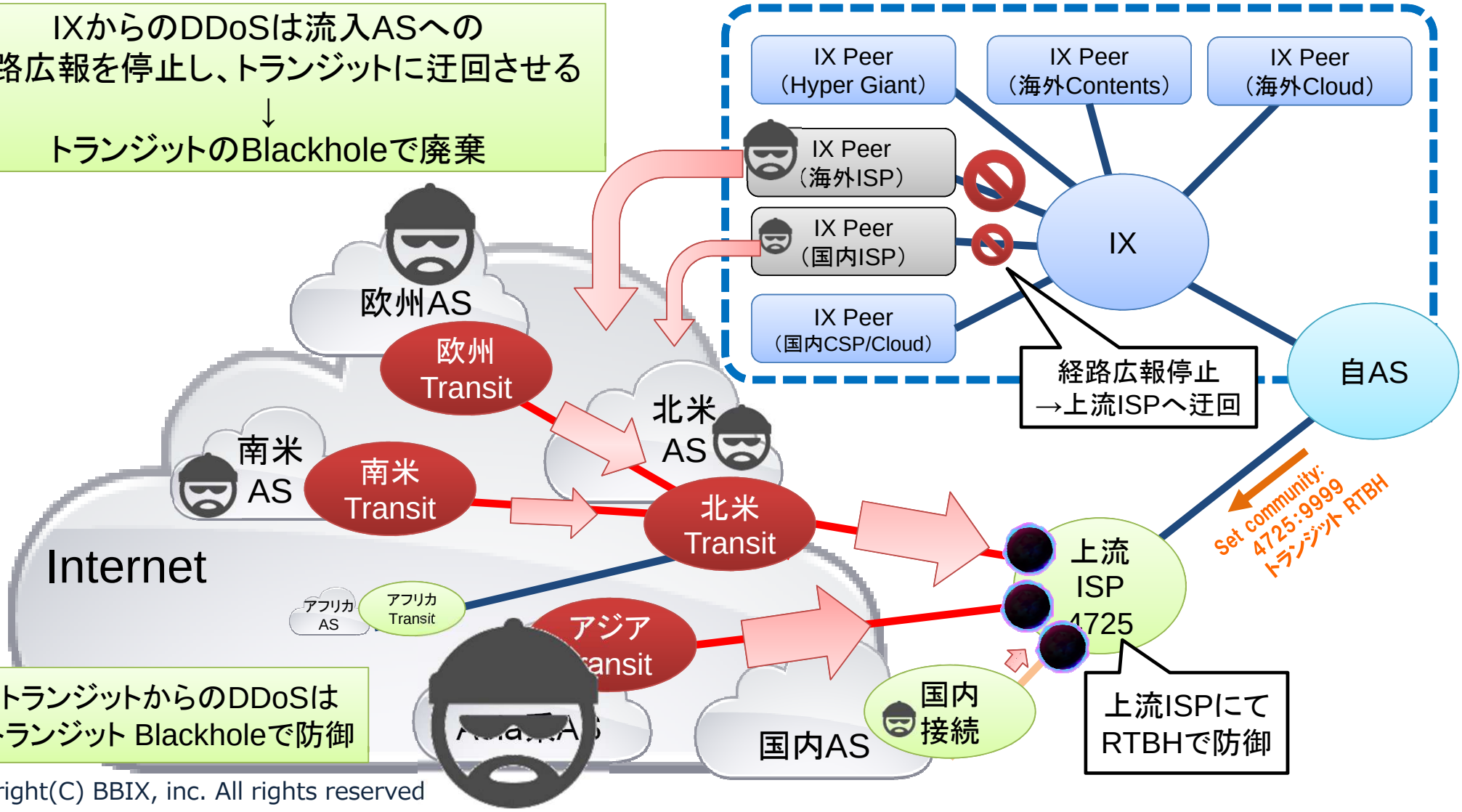
- IXのPeerが受け入れてくれるもの
  - ① 広報経路による制御：BGPのattribute制御でトランジットなど他経路を優先させる
    → 通常のトラフィック流量制限で利用。非常時は使えない！
  - ② IX RTBH：攻撃されているホスト経路にBlackhole指定でアナウンス → IXで廃棄
    - 利点：IXで接続している全ASに対して、廃棄するIP範囲を限定してDDoS対処可能。対象の判定不要！
    - 欠点：受付プリフィクス長制限があり、実際に効果があるのは/24単位でのRTBH（悪影響の懸念）
  - ③ 保守目的での経路広報停止 → トランジットに回してトランジットで廃棄
    - 利点：対象さえ把握できれば、簡単に実行可能
    - 欠点：トラフィックの異常超過Peerなどが把握できないとどのPeeringを規制したらいいかわからない。
      Peerへの対処をやりすぎるとトランジットに大量のトラフィックが流れ、品質低下・コスト増大となる
    - 対処：フロー解析による超過Peerの把握が必要。流入可能性の高い属性からの対処

DDoS対応1:トランジット RTBH + IX RTBH



DDoS対応2:トランジット RTBH + IXPeer規制

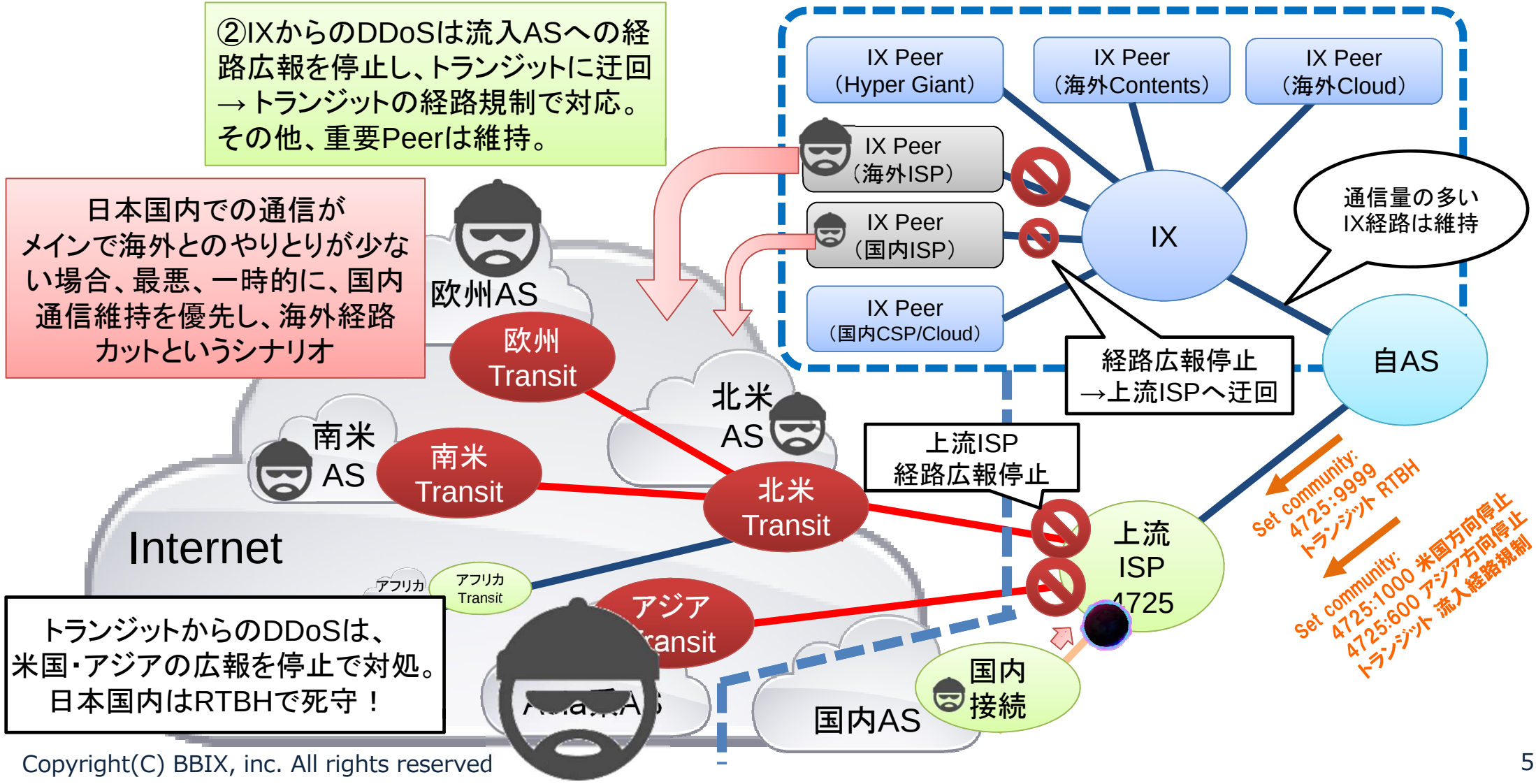
IXからのDDoSは流入ASへの
経路広報を停止し、トランジットに迂回させる
↓
トランジットのBlackholeで廃棄



DDoS対応3:トランジット流入経路規制 + IXPeer規制

②IXからのDDoSは流入ASへの経路広報を停止し、トランジットに迂回
→トランジットの経路規制で対応。
その他、重要Peerは維持。

日本国内での通信がメインで海外とのやりとりが少ない場合、最悪、一時的に、国内通信維持を優先し、海外経路カットというシナリオ



トランジットからのDDoSは、
米国・アジアの広報を停止で対処。
日本国内はRTBHで死守！

まとめ

- DDoSはいたるところから流入してくるが、入ってくる経路についてはある程度の予測は可能　→　事前に対策をたてることが可能
  - 海外キャリア・ISPからの流入の可能性が多い
- 現状においては10分以内での短時間での攻撃が主体
  - 短期ならそのままやり過ごすこともあり。でも把握はしたい。。。
  - 長期にわたる攻撃にはISP/IXと連携して対処
- 対応シナリオの策定と事前準備が重要
  - 優先防御リソースを想定した非常用対策手順
  - まずは検知体制の整備が必要

No Peering, No Internet!