Internet Week ショーケース

企業のDDoS対処戦略 Reloaded
～基礎から実践まで～

DDoS時代の対外接続
～BGP運用者、そしてIXPからみたベストプラクティス～

2017/6/2

BBIX株式会社 矢萩茂樹

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？

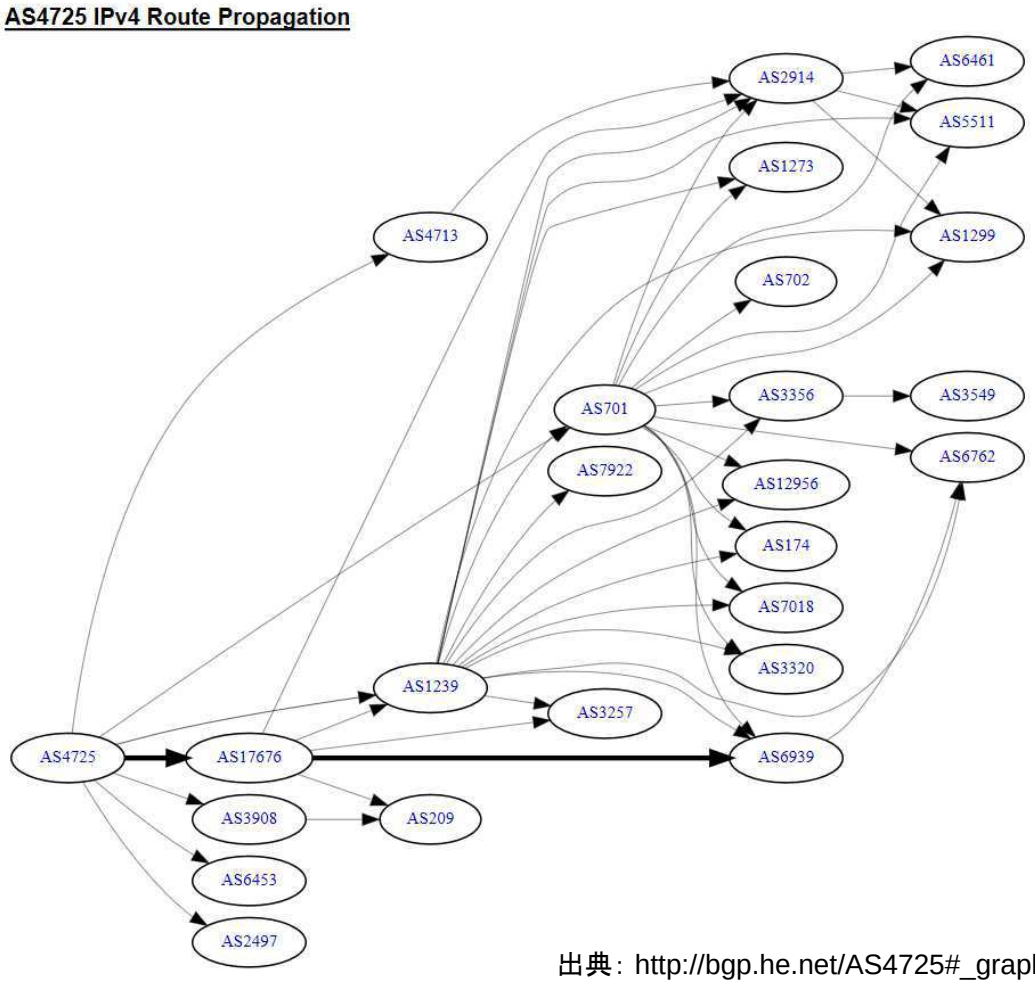
- Internetの構造を知り、上位ISPと連携した防御法をみてみよう

AGENDA

- Internetの構造とトラフィック分布とDDoSの流入経路
- DDoSをネットワーク構造でどう防ぐか？

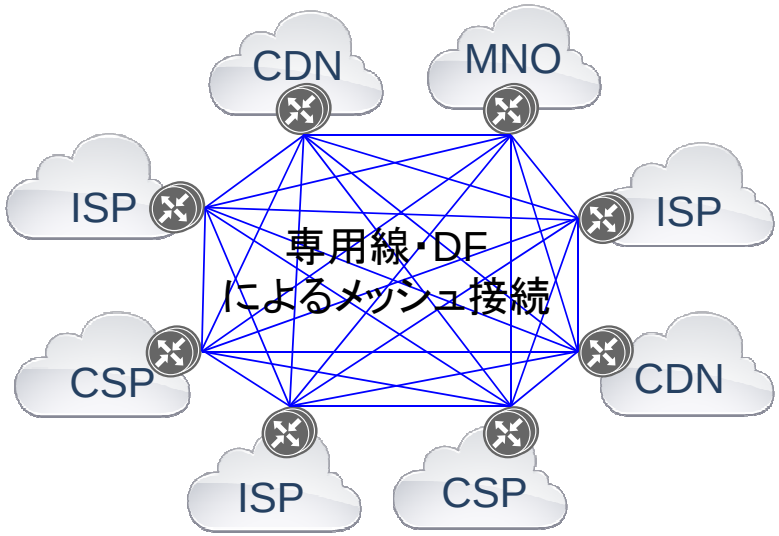
Internetの構造：ネットワーク組織の集合体

- 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階層接続はAS間での接続となる
- AS間でBGP(Border Gateway Protocol)により各々のNW情報（経路）を交換

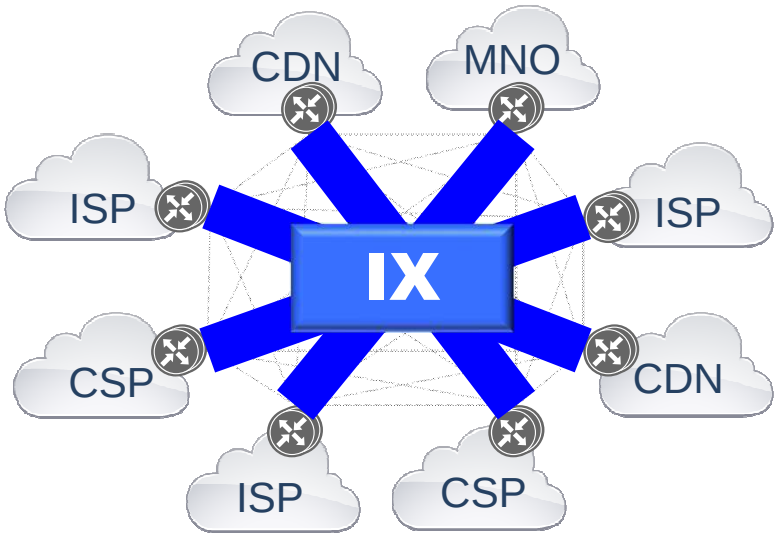


出典：http://bgp.he.net/AS4725#_graph4

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



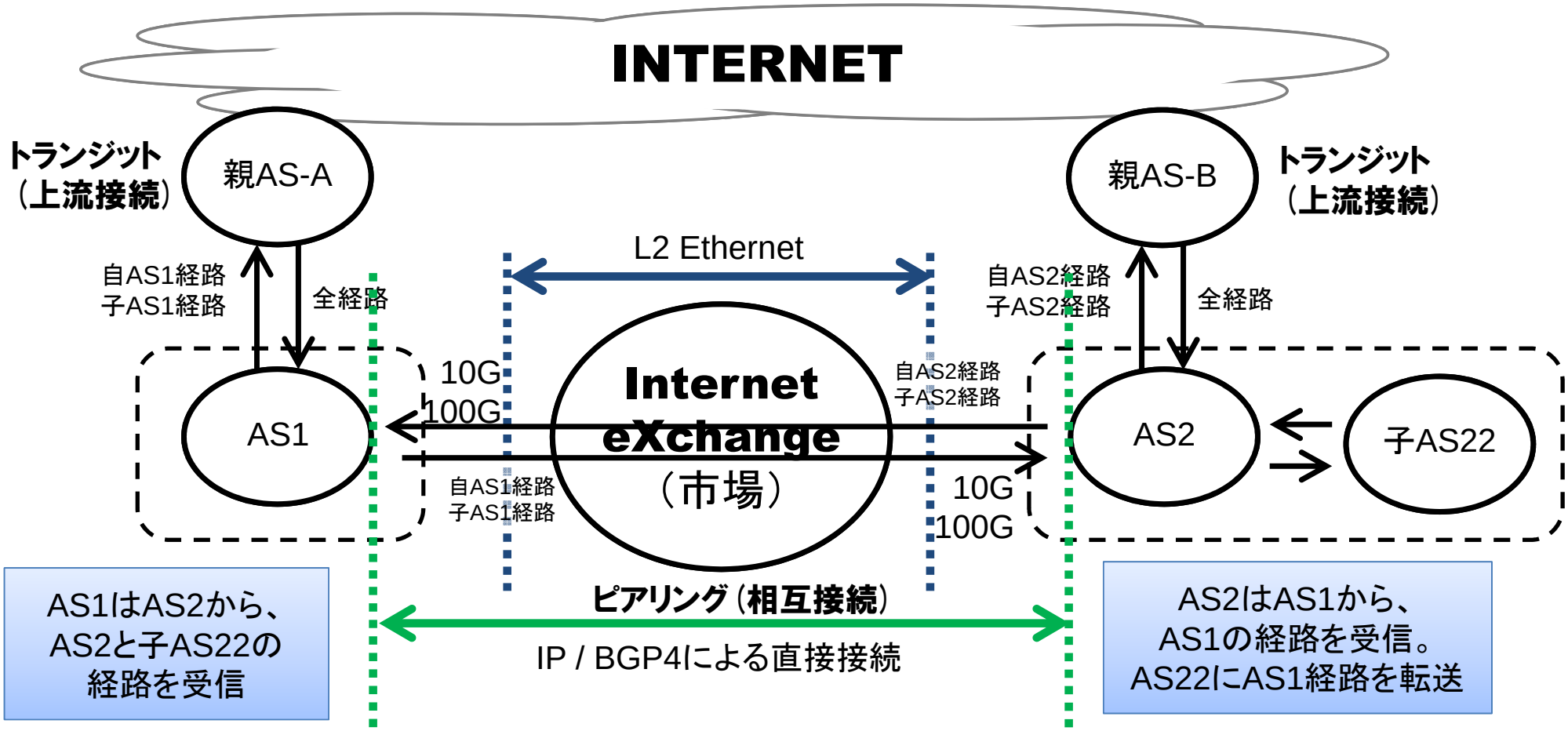
旧来の接続方式
複雑・細い帯域で非効率な構成



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でのピアリング（相互接続）とトランジット



トランジットとピアリング（相互接続）

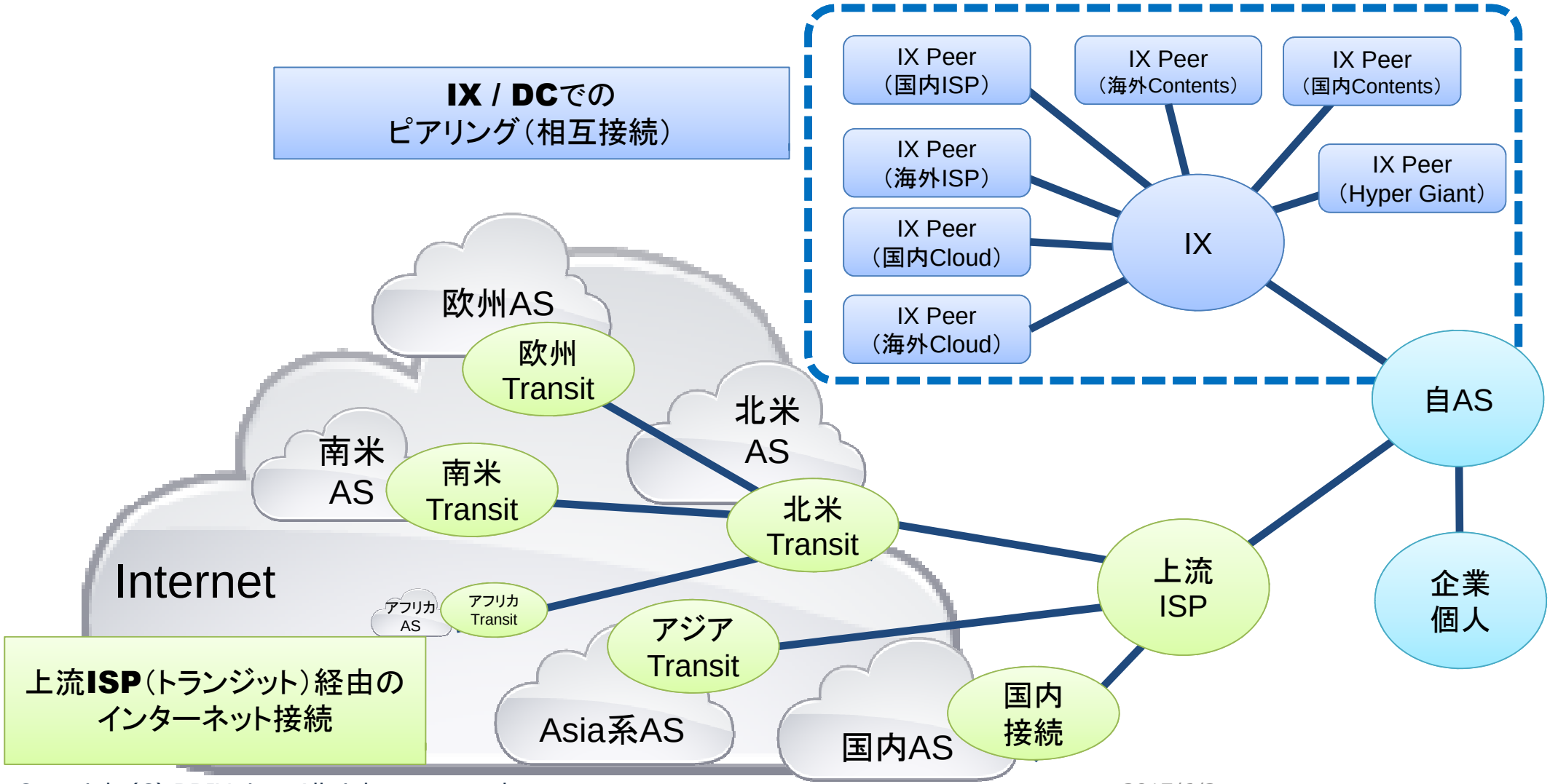
ISPでのインターネット接続 ➡トランジット(上流接続)

- 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

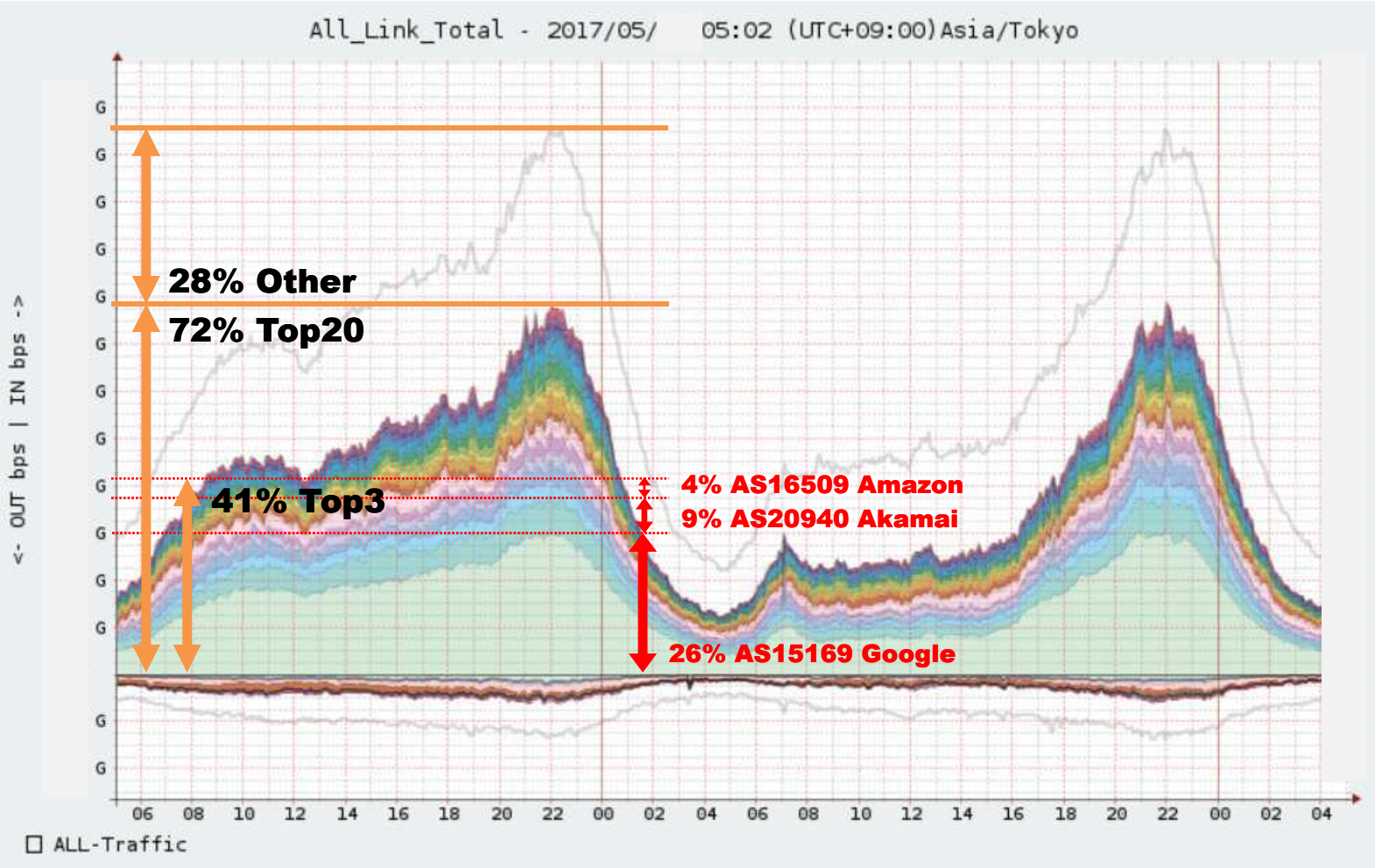
IX経由でのISP間相互接続 ➡ピアリング（相互接続）

- 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。

日本からみたインターネットの構造



ISPネットワーク傾向：全トラフィック

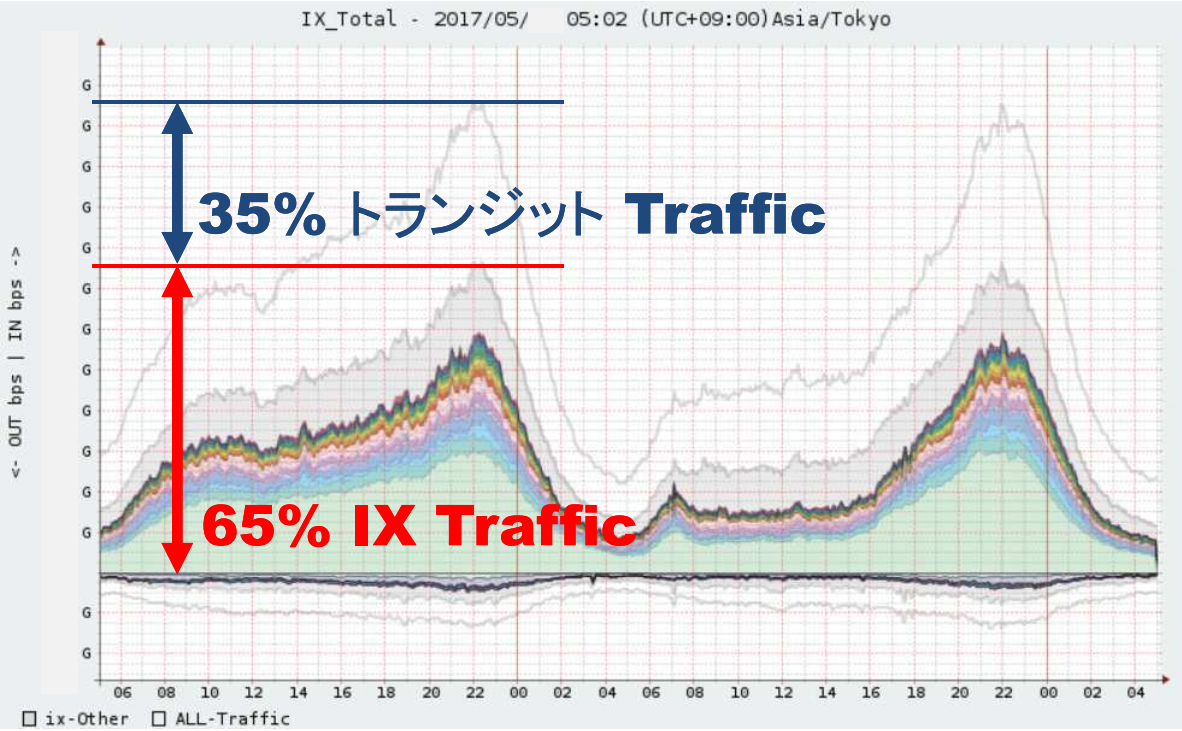


Top20 AS Ranking

	AS	
1	AS15169	Google Inc.,US
2	AS20940	Akamai International B.V.
3	AS16509	Amazon.com, Inc.,US
4	AS6185	Apple Inc.,US
5	AS22822	Limelight Networks, Inc.,
6	AS32934	Facebook, Inc.,US
7	AS2516	KDDI Co,JP
8	AS714	Apple Inc.,US
9	AS4713	NTT Communications Co.,JP
10	AS23816	Yahoo Japan Co.,JP
11	AS38634	DWANGO Co.,Ltd.,JP
12	AS8068	Microsoft Co.,US
13	AS2497	Internet Initiative Japan
14	AS15133	EdgeCast Networks, Inc.,U
15	AS13414	Twitter Inc.,US
16	AS24572	Yahoo Japan,JP
17	AS2906	Netflix Streaming Service
18	AS36408	CDNetworks Inc.,US
19	AS17676	Softbank BB Corp.,JP
20	AS16625	Akamai Technologies, Inc.

30%弱 Google
約10% Akamai
約70% Top20AS
に集中

ISPネットワーク傾向:トランジット vs IX



全traffic Top20 AS Ranking

	AS	
1	AS15169	Google Inc.,US
2	AS20940	Akamai International B.V.
3	AS16509	Amazon.com, Inc.,US
4	AS6185	Apple Inc.,US
5	AS22822	Limelight Networks, Inc.,
6	AS32934	Facebook, Inc.,US
7	AS2516	KDDI Co,JP
8	AS714	Apple Inc.,US
9	AS4713	NTT Communications Co.,JP
10	AS23816	Yahoo Japan Co.,JP
11	AS38634	DWANGO Co.,Ltd.,JP
12	AS8068	Microsoft Co.,US
13	AS2497	Internet Initiative Japan
14	AS15133	EdgeCast Networks, Inc.,U
15	AS13414	Twitter Inc.,US
16	AS24572	Yahoo Japan,JP
17	AS2906	Netflix Streaming Service
18	AS36408	CDNetworks Inc.,US
19	AS17676	Softbank BB Corp.,JP
20	AS16625	Akamai Technologies, Inc.

IX経由 Top20 AS Ranking

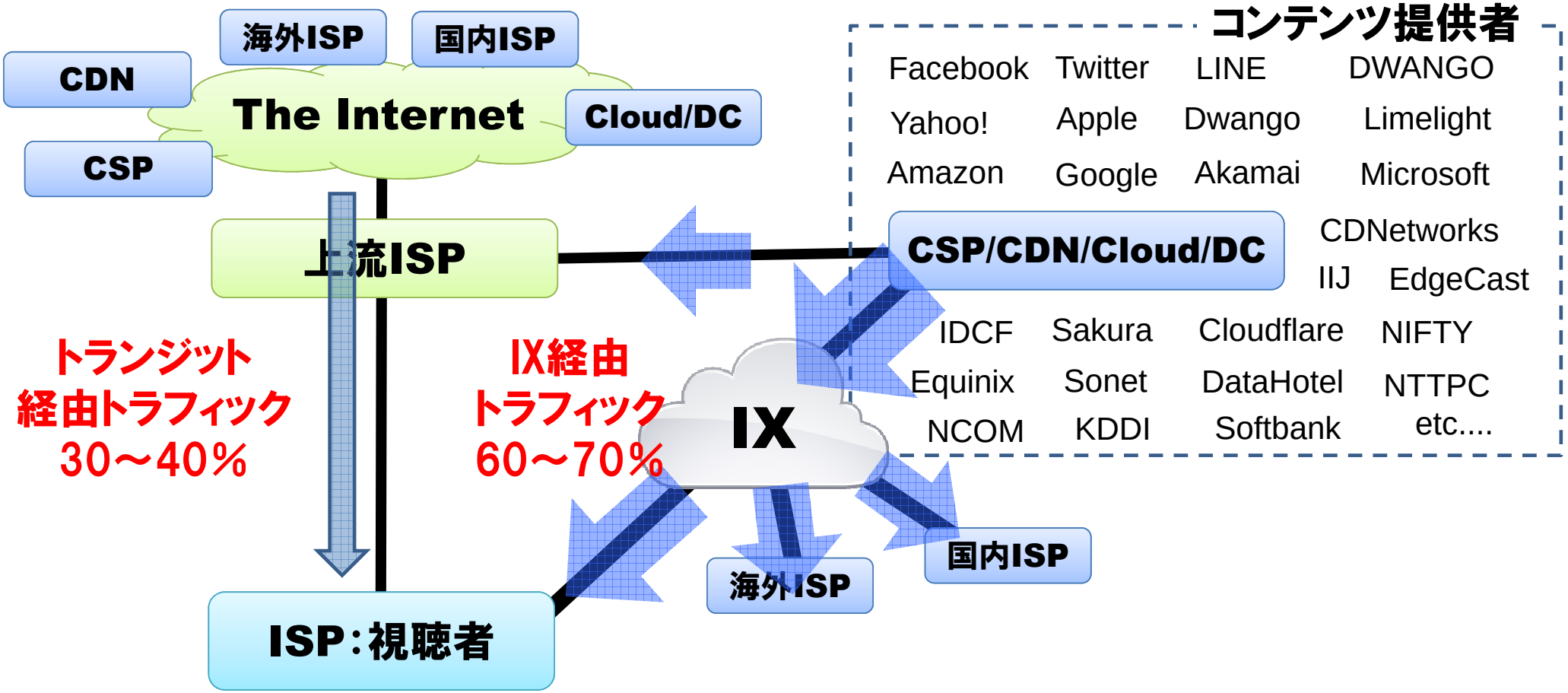
	AS	
1	AS15169	Google Inc.,US
2	AS16509	Amazon.com, Inc.,US
3	AS20940	Akamai International B.V.
4	AS6185	Apple Inc.,US
5	AS714	Apple Inc.,US
6	AS23816	Yahoo Japan Co.,JP
7	AS38634	DWANGO Co.,Ltd.,JP
8	AS8068	Microsoft Co.,US
9	AS32934	Facebook, Inc.,US
10	AS2906	Netflix Streaming Service
11	AS13414	Twitter Inc.,US
12	AS15133	EdgeCast Networks, Inc.,U
13	AS23620	DooGA Co., Ltd.,JP
14	AS16625	Akamai Technologies, Inc.
15	AS17676	Softbank BB Corp.,JP
16	AS4694	Yahoo Japan Co.,JP
17	AS24572	Yahoo Japan,JP
18	AS2527	So-net Entertainment Co.,
19	AS8075	Microsoft Co.,US
20	AS32590	Valve Co.,US

- このデータでIX経由でのトラフィックランキングのらないAS
  #あくまでも今回の測定での分類
- IXには接続しているがPeering条件があるAS

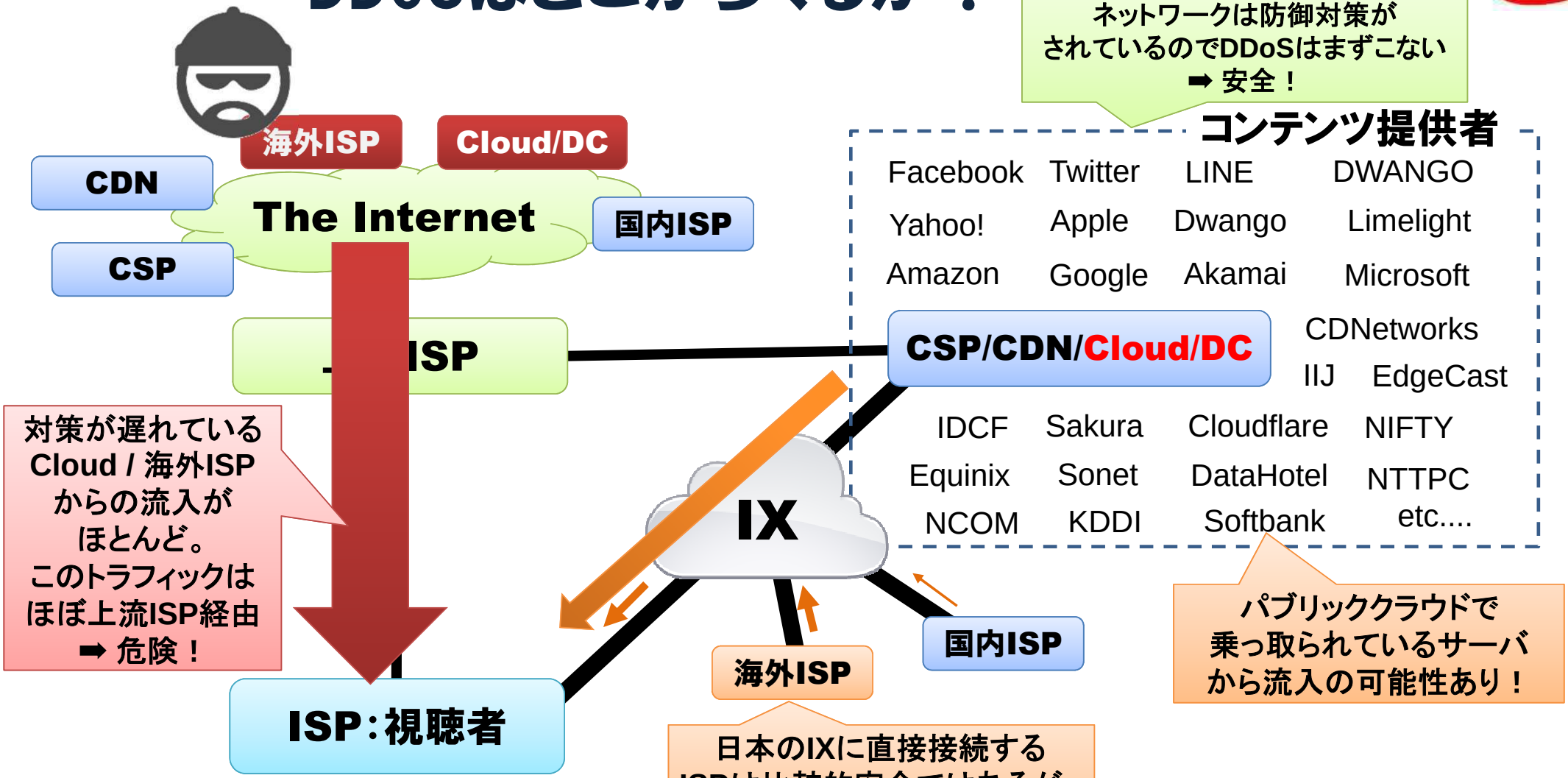
IX経由のトラフィックは全体の約70%

上位ASの多くはIX経由

ISPからみたInternetのトラフィック分布

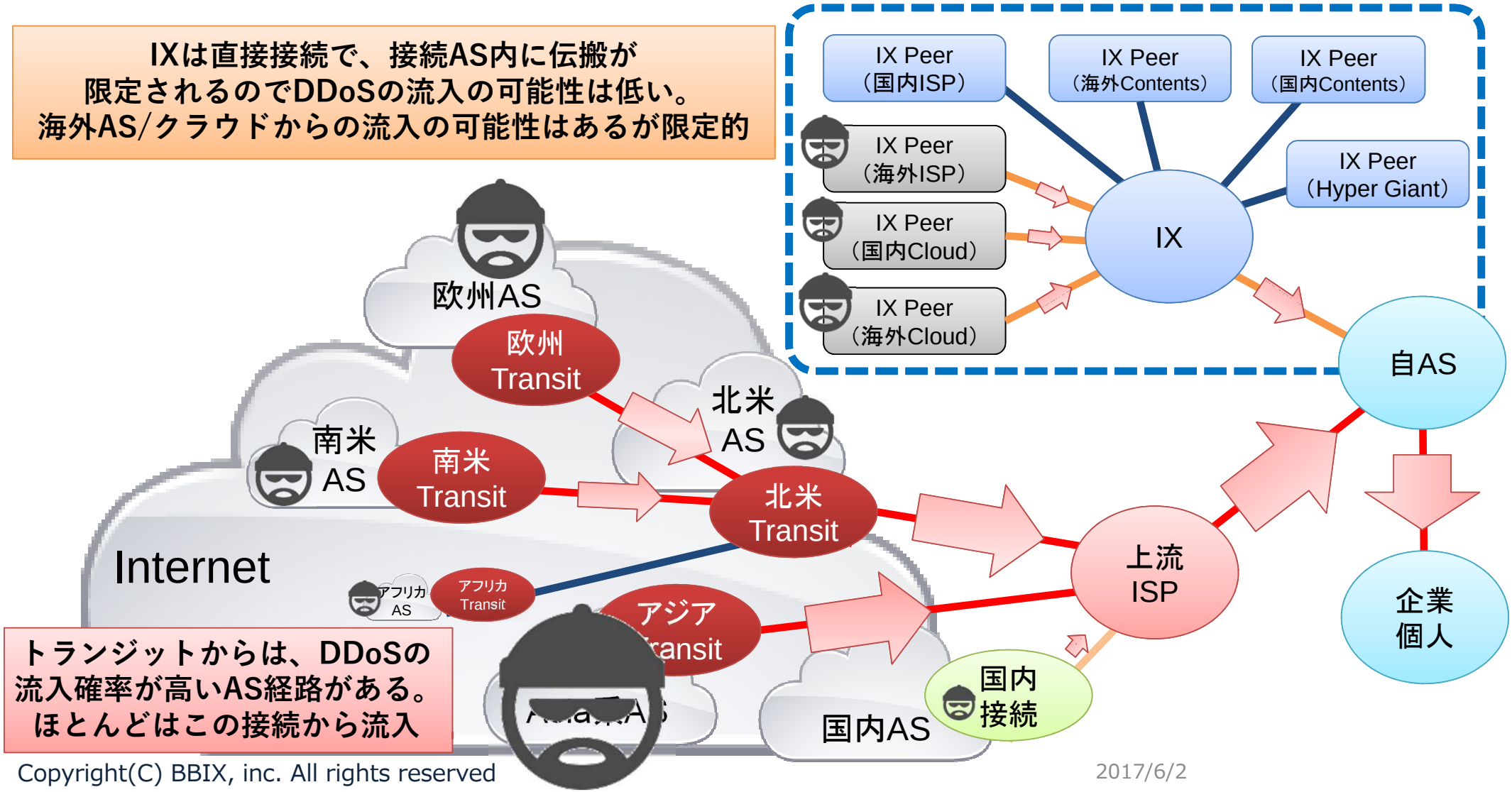


DDoSはどこからくるか？



DDoSの流入経路は主に海外/クラウドから！

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AS/クラウド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

AGENDA

- Internetの構造・トラフィック分布とDDoSの流入経路
- **DDoSをIXとトランジットでどう防ぐか？**

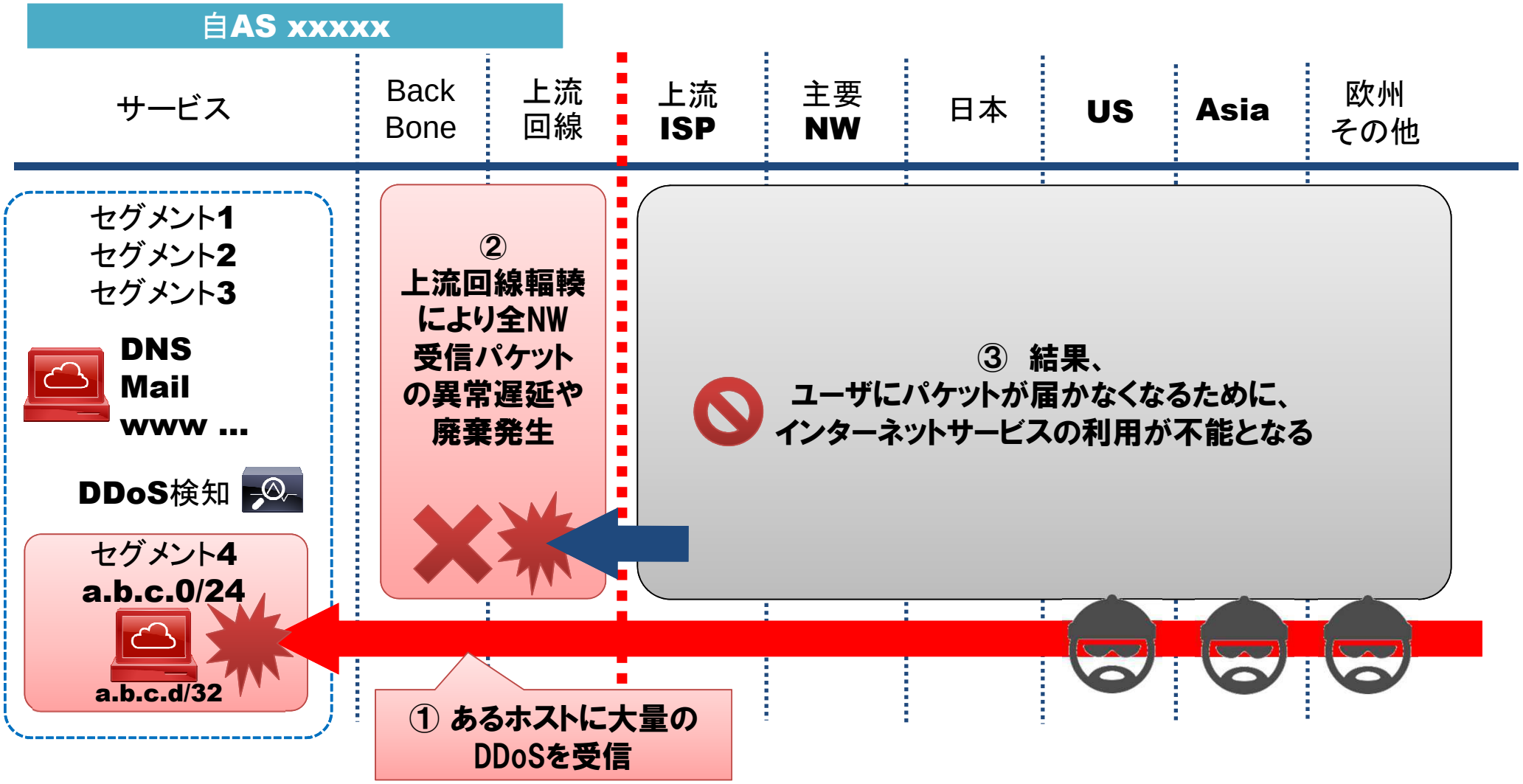
対策：守るべきものは何か

- 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？

- キャリア系ISPでは、BGP4ユーザ向けに上流ISP内でのポリシー変更をユーザが設定できる機能（BGP Community制御）を提供している。これが有効！
  ① 上位ISPでのBlackhole起動
  ② 上位ISPでの流入経路規制

- 対外接続のBGP化により、ユーザからのポリシー起動が可能となり、
  対応速度の高速化される！

DDoS影響の例



総合的対策:トランジット・IXでの対策

① Blackhole対処

◆ IXでのBlackhole Community

規制方法	**Community**	制御内容
BLACKHOLE	**17676:2089**	広報した**/32**経路に関し、**AS17676**ですべてのトラフィックを廃棄する
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

◆ 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

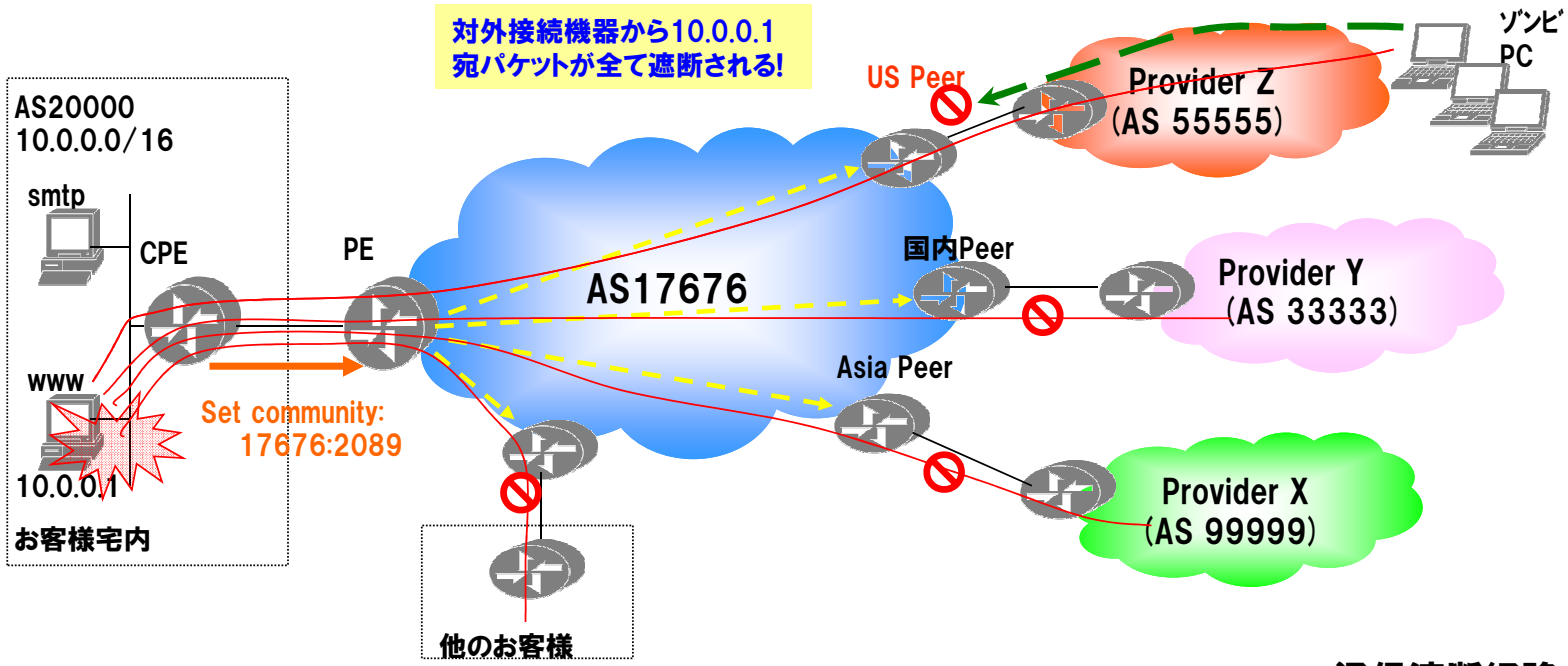
トランジットでのBlackhole制御

◆ご要望

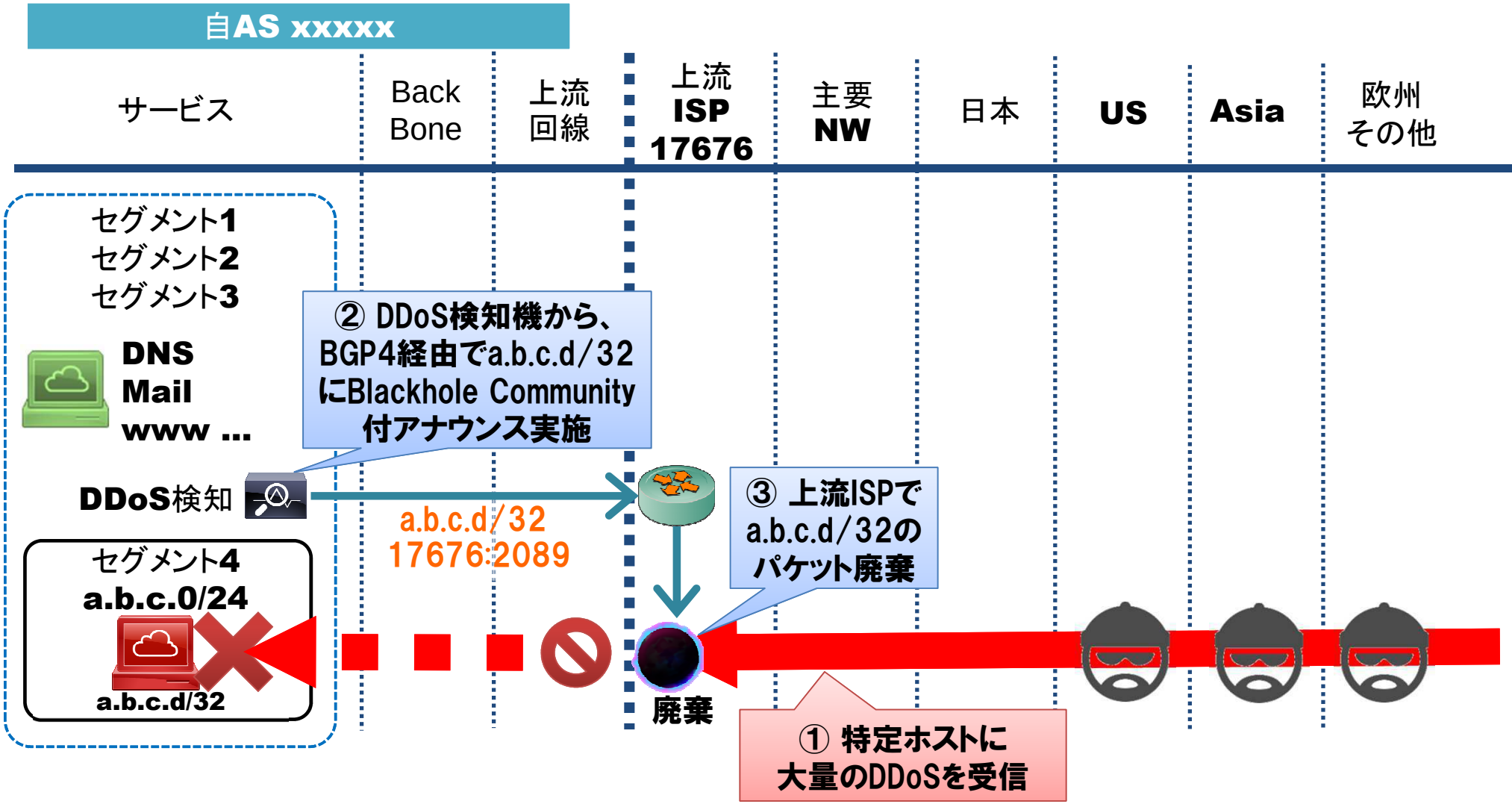
USのISP経由でお客様サイト内特定サーバ（WWW）がDDoS攻撃を受けており、他のSMTPサービスなどが回線の逼迫によりスムーズに運用できない被害を被っておりこれを防止したい。

◆対応方法

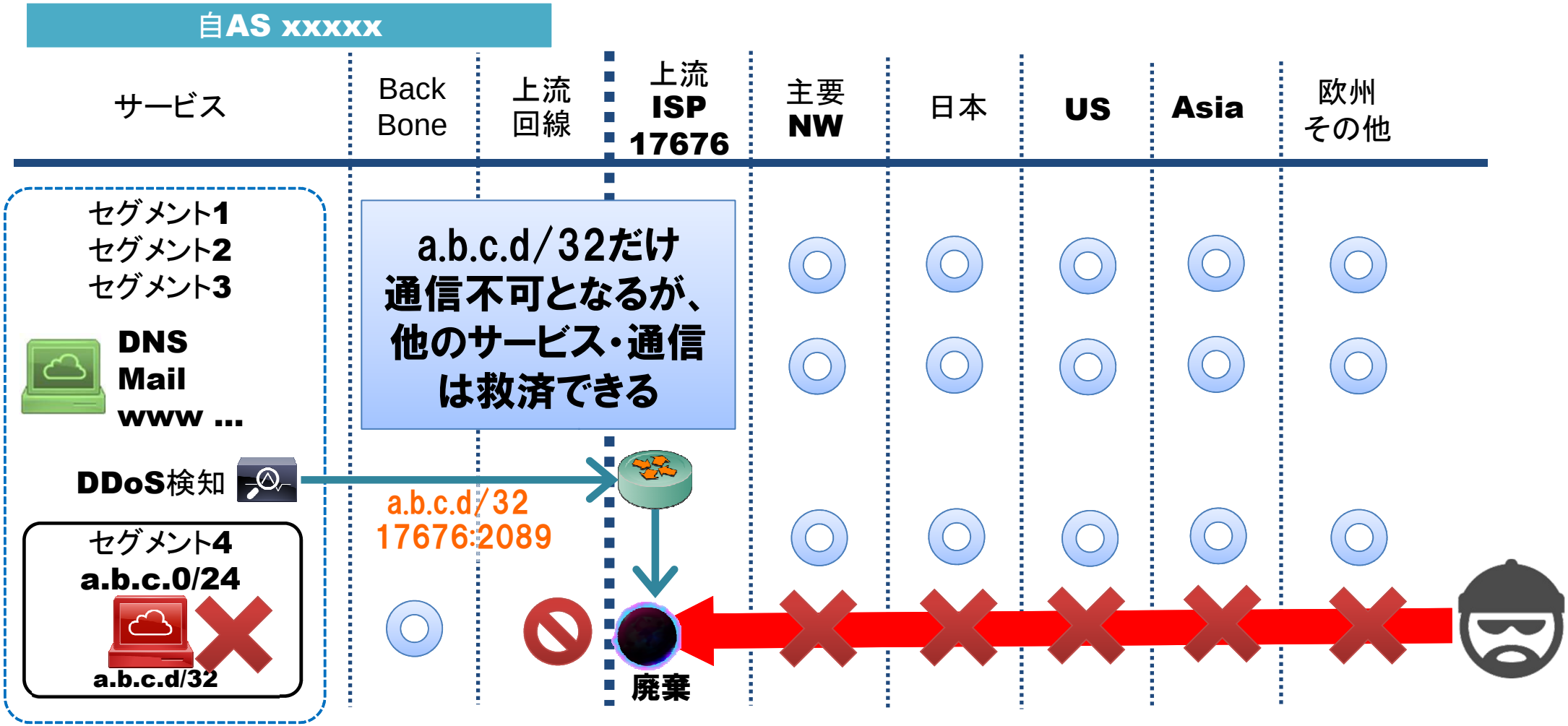
1. お客様 CPEにてwwwアドレス（10.0.0.1/32）に対しcommunity 17676:2089 を付与し広報する
2. PEでは受け取った /32 経路にLOCAL-AS を 付加し, Local Preferenceを強く17676網内に広報
3. 対外接続用ルータでは community 17676:2089がついている経路へのトラフィックを破棄する
4. US ISP軽油だけでなく、wwwアドレス（10.0.0.1/32）に対する全パケットを破棄する。



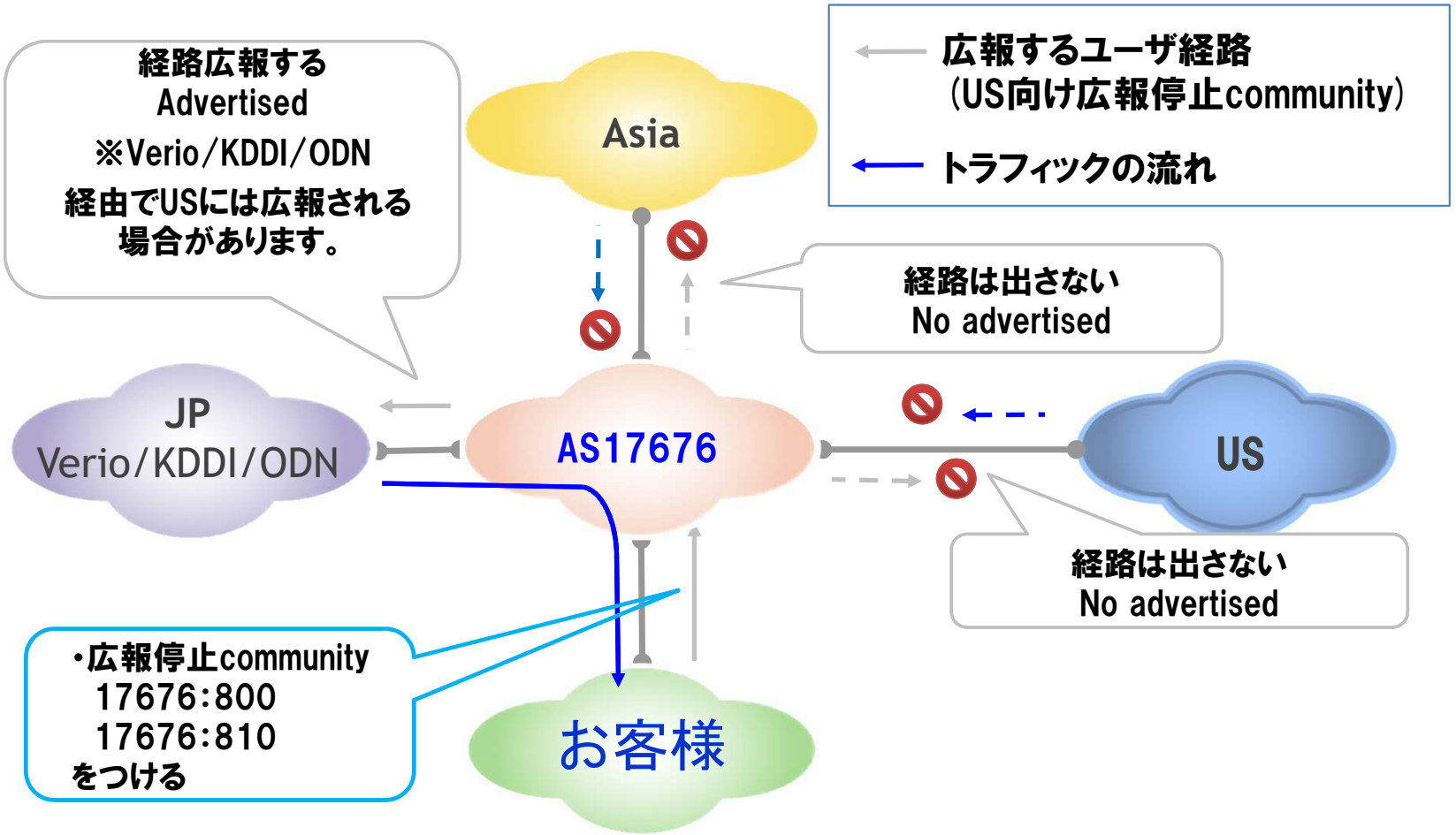
Blackhole対処



Blackhole対処：サービス影響



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りますので、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。

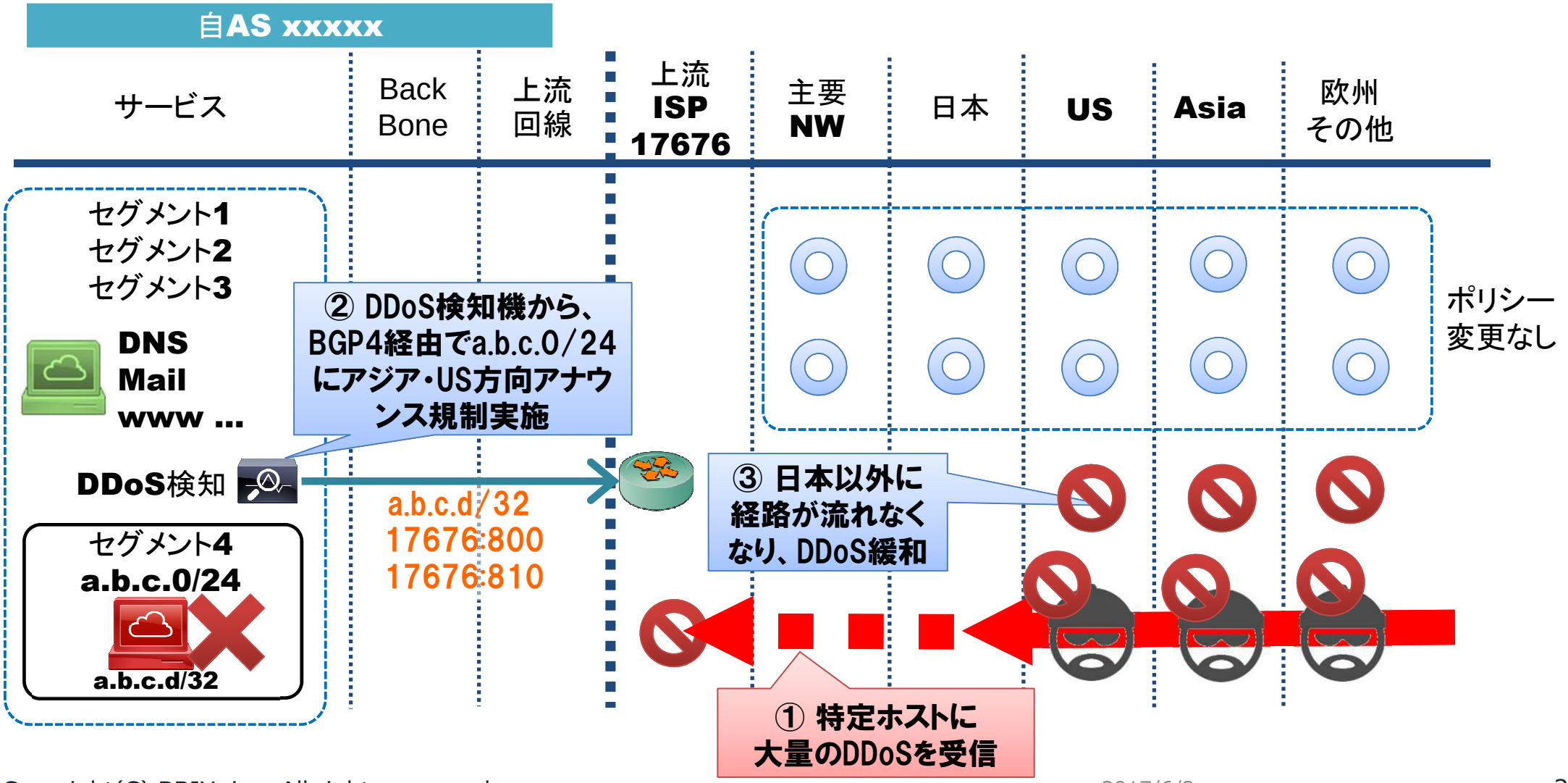
総合的対策:トランジットでの対策例

② 流入経路規制

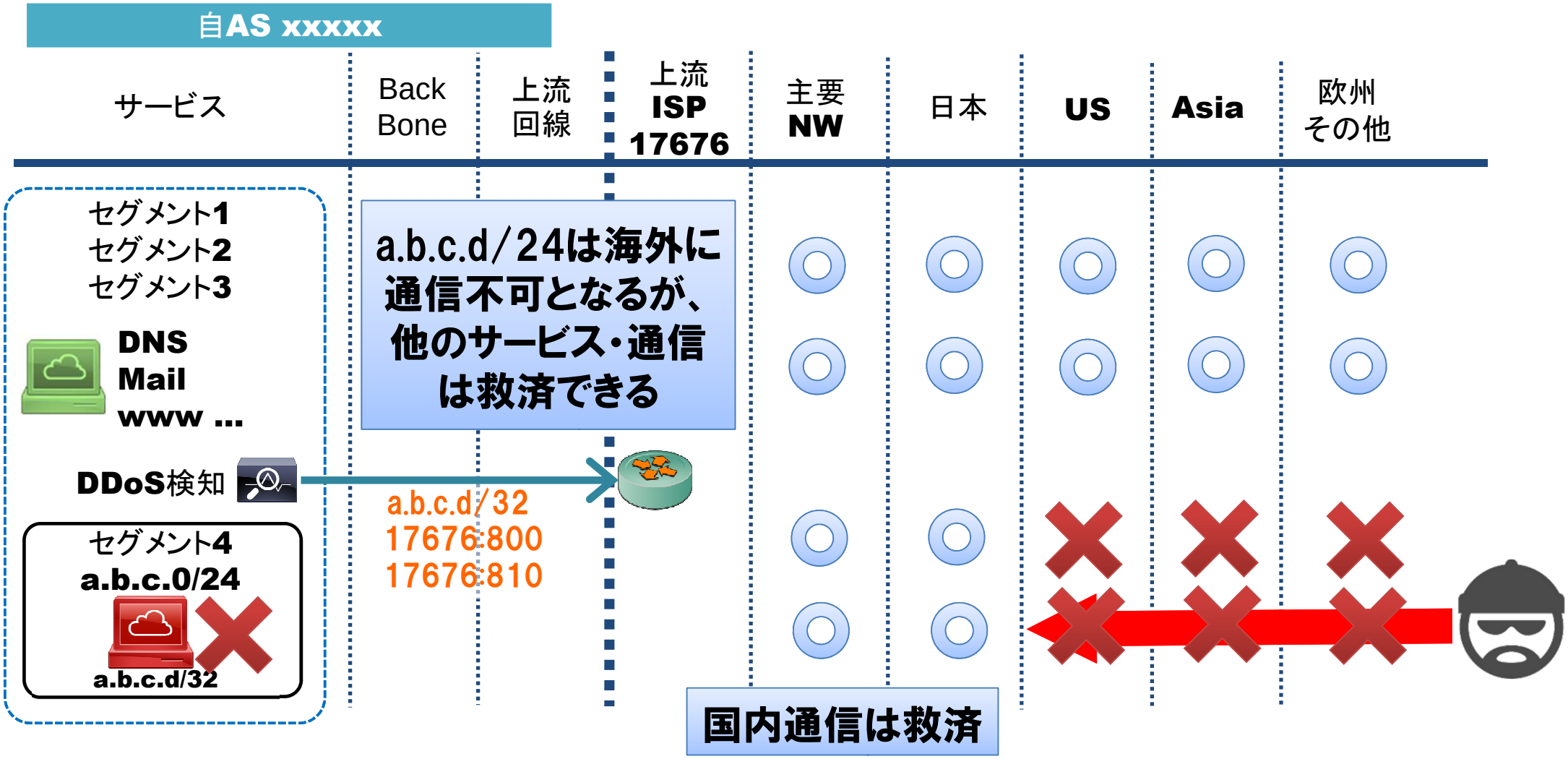
規制方法	Community	制御内容
流入経路規制	**17676:800**	**AS17676**から米国向けに広報しない
流入経路規制	**17676:810**	**AS17676**からアジア向けに広報しない
流入経路規制	**17676:820**	**AS17676**から国内向けに広報しない

規制方法	Community	制御内容
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

流入経路規制



流入経路規制：サービス影響

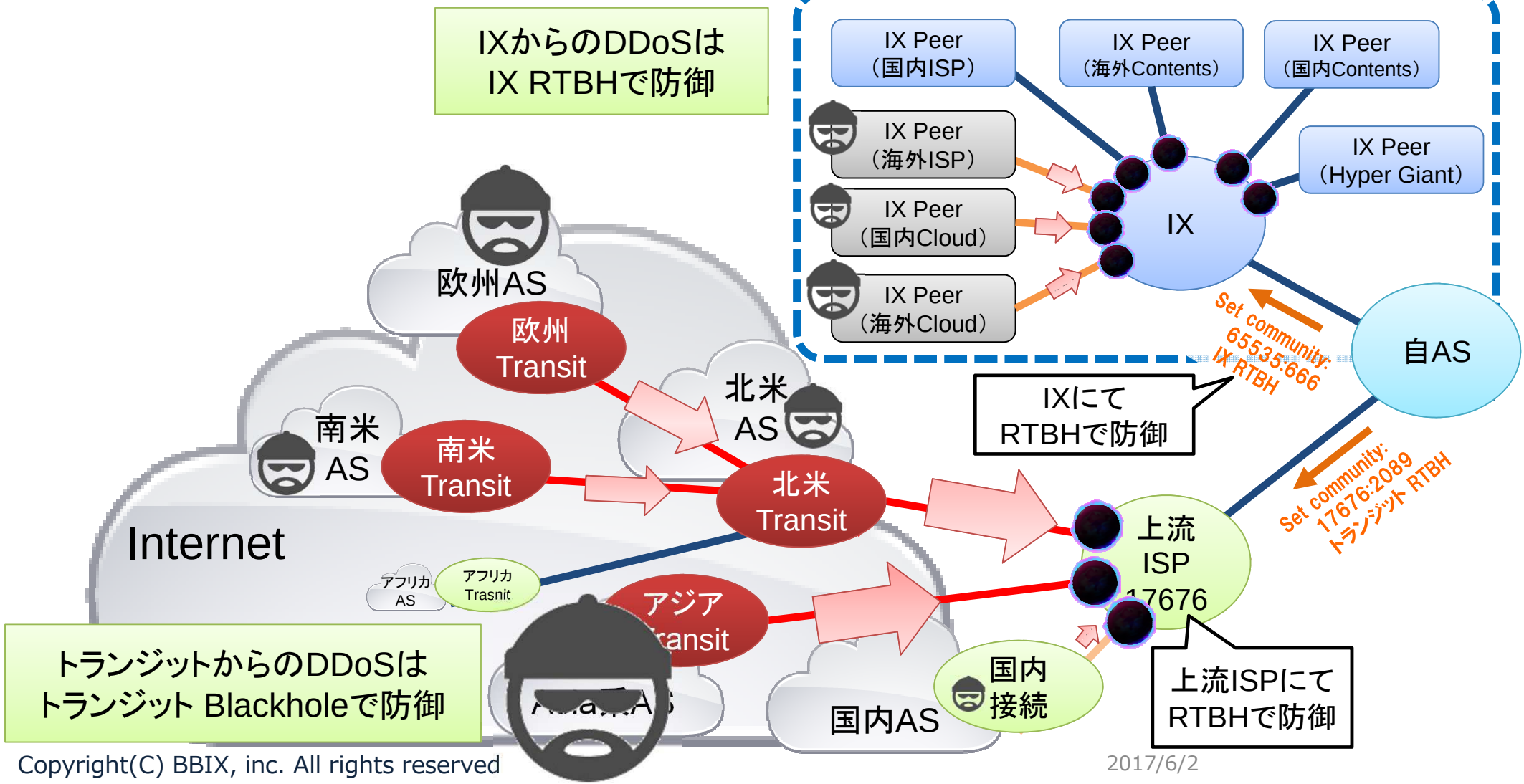


総合的対策：IXでの対応

- 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

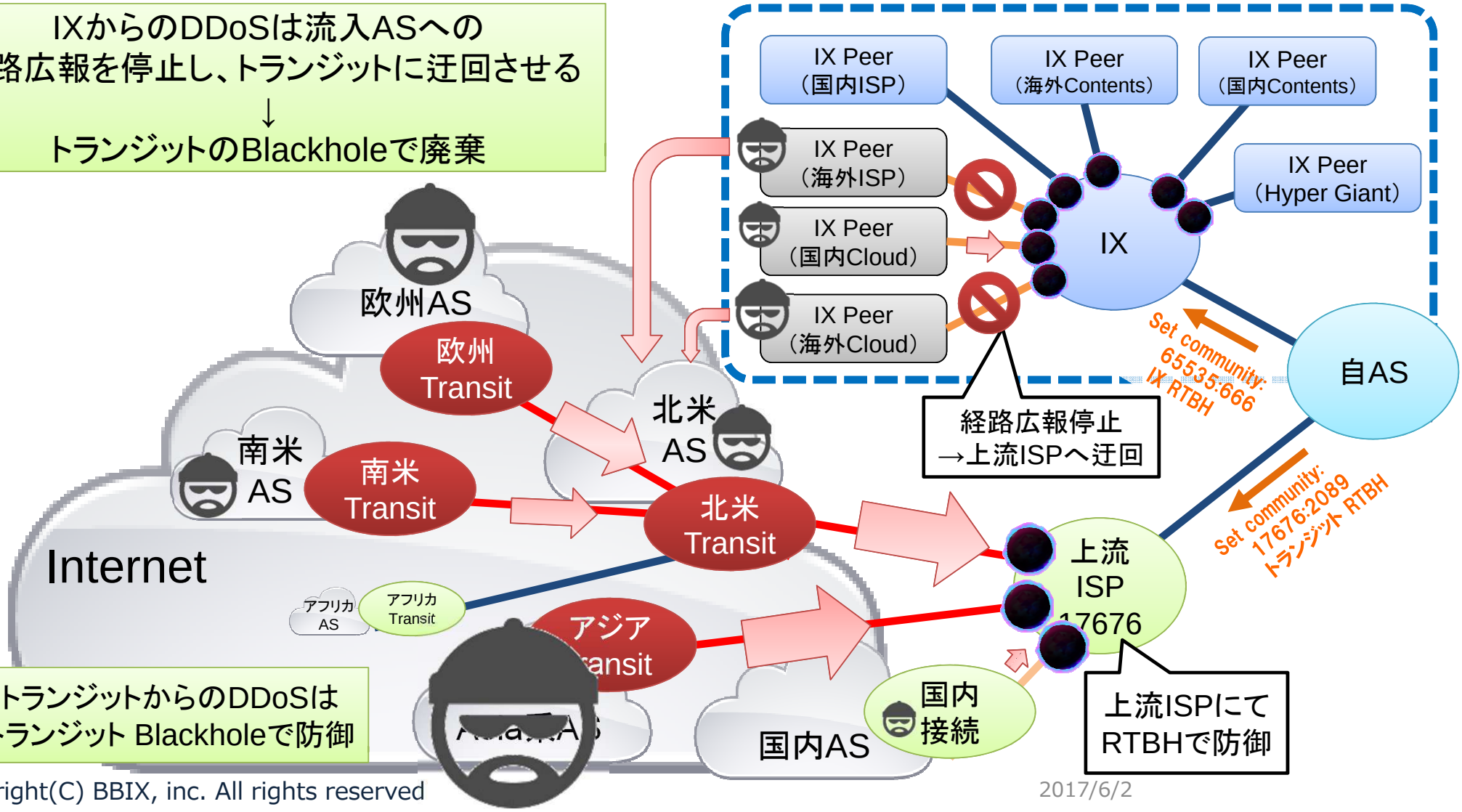
- IXのPeerが受け入れてくれるもの
  - ① 広報経路による制御：BGPのattribute制御でトランジットなど他経路を優先させる
    → 通常のトラフィック流量制限で利用。非常時は使えない！
  - ② IX RTBH：攻撃されているホスト経路にBlackhole指定でアナウンス → IXで廃棄
    - 利点：IXで接続している全ASに対して、廃棄するIP範囲を限定してDDoS対処可能。対象の判定不要！
    - 欠点：受付プリフィクス長制限があり、実際に効果があるのは/24単位でのRTBH（悪影響の懸念）
  - ③ 保守目的での経路広報停止 → トランジットに回してトランジットで廃棄
    - 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

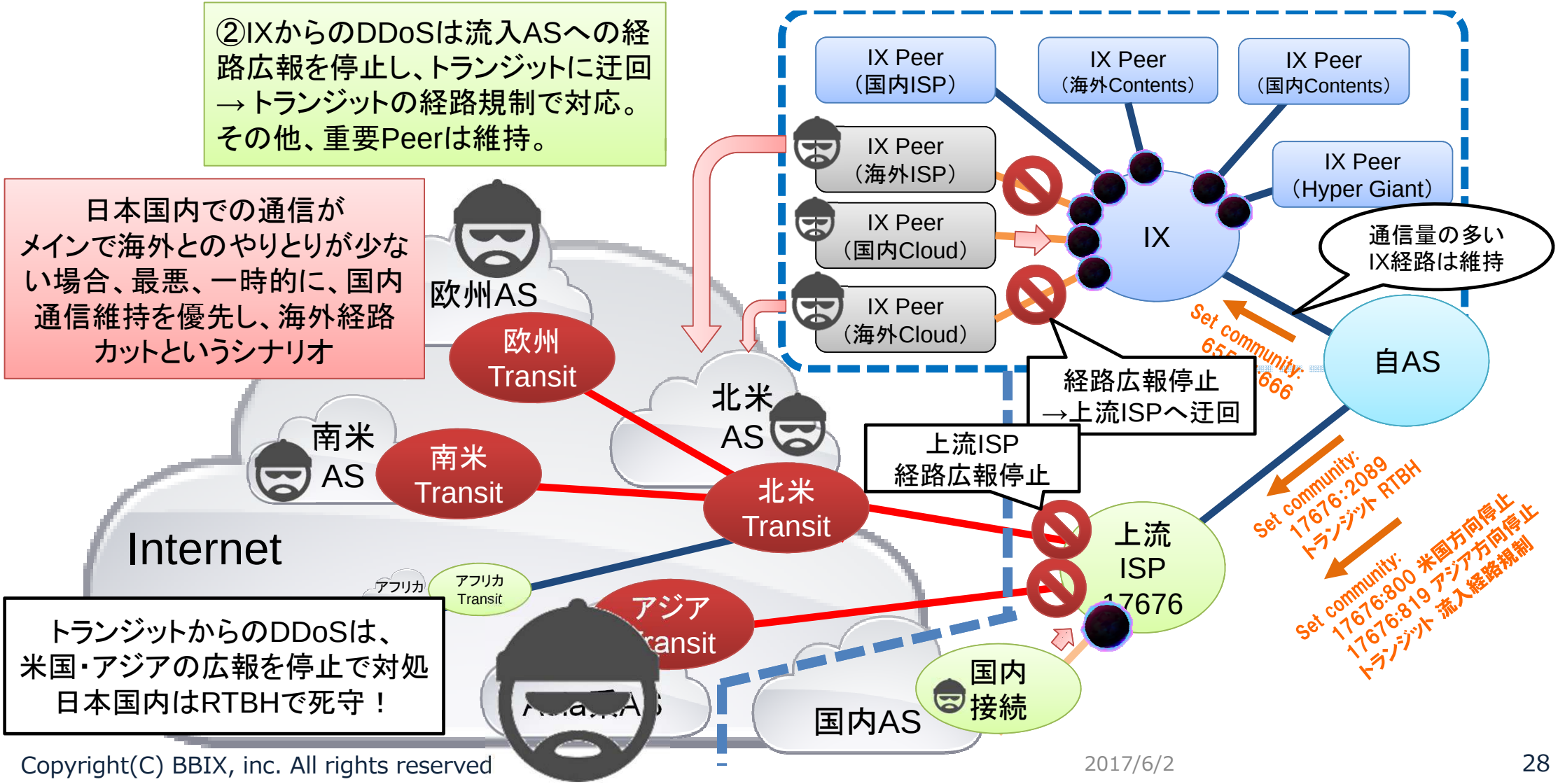
IXからのDDoSは流入ASへの
経路広報を停止し、トランジットに迂回させる
↓
トランジットのBlackholeで廃棄



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
  - まずは検知と発動の環境整備が重要

No Peering, No Internet!