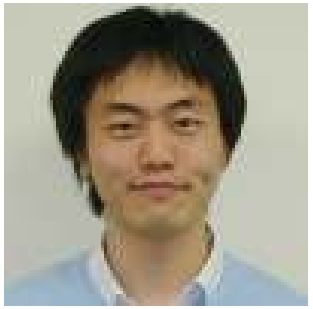
Internet Week 2015
セキュアルーティング時代の
DDoS対策テクニック

2015.11.18 16:15～18:45
[s12]垣根を越える！インターネットルーティングセキュリティ

Kaname Nishizuka@NTT Communications

自己紹介

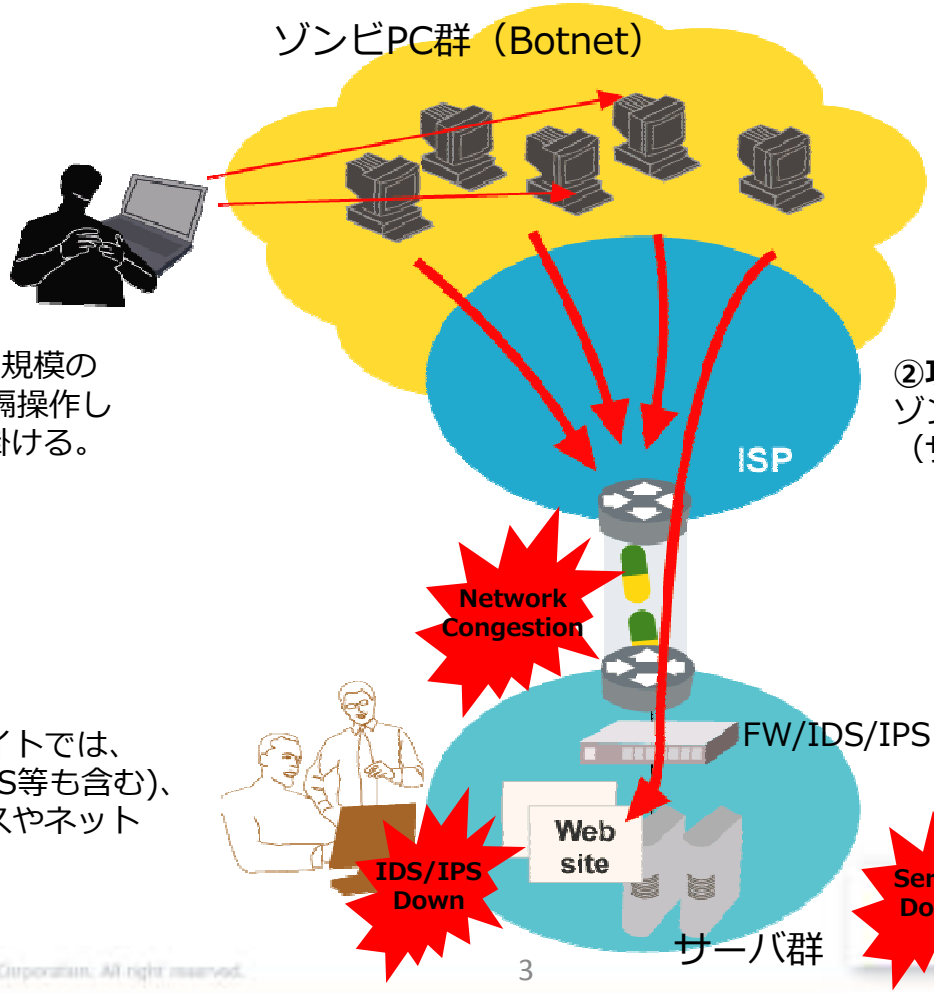
- 2006年 NTTコミュニケーションズ入社
- OCNアクセス系ネットワークの設計に従事した後、
  大規模ISP向けのトータル保守運用サービスを担当
- 現在、DDoS対策ソリューション/CGN関連技術の開発
  および、IETFにおける提案活動に従事
- ISOC-JP プログラムチェア



DDoS攻撃とは

DDoS攻撃とは

DDoS（Distributed Denial of Service：分散サービス妨害）攻撃は、インターネット上に存在する大量のコンピュータから一斉に特定サイト（WEBサーバなど）や企業のネットワークへ不正パケットを送出し、サーバ/システム負荷、ネットワーク輻輳を招き、サービスを停止させてしまう攻撃です。
ここ数年でDDoS攻撃が大規模化・複雑化しており、事前のセキュリティ対策が不可欠になりつつあります。



①攻撃命令
インターネット上の数十万規模のゾンビPC（Botnet）を遠隔操作しWEBサーバ等に攻撃を仕掛ける。

②攻撃パケット送信
ゾンビPC（Botnet）から、特定サイト（サーバ）への大量のパケット送信。

③DDoS被害の発生
DDoS攻撃対象となったサイトでは、サーバ高負荷（FW/IDS/IPS等も含む）、NW輻輳が発生してサービスやネットワークがダウン。

脅威を増すDDoS攻撃の傾向

日時	継続時間	攻撃対象	影響内容
2013年3月	4日間	Spamhaus/Cloudflare	300Gbps以上の攻撃 3月22日には、ロンドン、アムステルダム、フランクフルト、香港のIXがトラヒック輻輳が発生、欧州全体に影響
2014年2月	不明	Cloudflareの顧客	NTP増幅攻撃により、400Gbps弱の攻撃
2014年5～6月	14日間	K-optcom社 eo光　DNSサーバ	Web閲覧、メール送受信などに時間がかかる、または表示不可
2014年7月	5日間以上	K-optcom社 eo光　DNSサーバ	Web閲覧、メール送受信などに時間がかかる、または表示不可
2014年6～7月	28日間	セガ 「ファンタシースターオンライン2」サービス	当該期間は、サービス停止 6月27日から、一次サービスを再開
2014年6月	数時間	Evernote	400Gbps以上のDDoS攻撃を受け、サービスに支障が出た 金銭要求
2014年6月	半日	Feedly	Evernoteとほぼ同時にDDoS攻撃を受け、サービス停止 金銭要求。米国ISP等の協力により、サービス復旧
2014年8月	数時間	PlayStation Network (PSN)	ネットワークに接続障害。サービス利用停止
2014年12月	不明	北朝鮮（STAR-KP）	9時間半にわたり北朝鮮がインターネットから孤立(※原因がDDoS攻撃かどうかは定かではない)

DDoS攻撃の規模・頻度の増加原因

- UDP リフレクションアタック
  - DNSだけでなく、NTPやChargenなど、UDPパケットを利用したリフレクション攻撃が増加
  - ブロードバンドルータなどの一般ユーザの機器の脆弱性を利用し、攻撃者は少ないリソースでも、ごく簡単に大規模トラフィックを生成することが可能

- DDoS攻撃を”買える”サービス
  - DDoS攻撃のコモディティ化

Booter	Attack Types	Cost
ANO	DNS	$6.60
BOO	NTP,Chargen	$2.50
CRA	DNS,SSDP	£10.99
GRI	NTP,SSDP	$5.00
HOR	NTP,SSDP	$6.99
INB	DNS,NTP,SSDP	$11.99
IPS	NTP,SSDP,Chargen	$5.00
K-S	SSDP,Chargen	$3.00
POW	SSDP	$14.99
QUA	DNS,SSDP	$10.00
RES	DNS,NTP	$10.00
SPE	DNS,NTP,SSDP,Chargen	$12.00
STR	DNS,SSDP	$3.00
VDO	DNS,NTP,SSDP	$18.99
XR8	DNS	$10.00

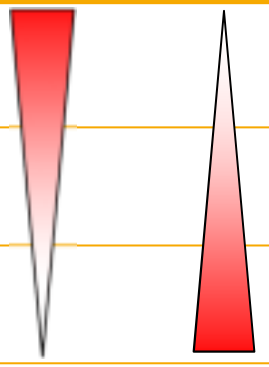
Table 3: *List of booter services we measured, which of the four attack types included in our measurements each booter offered and cost of cheapest one month subscription.*

Stress Testing the Booters: Understanding and Undermining the Business of DDoS Services
http://arxiv.org/abs/1508.03410

DDoS防御のトレードオフ

- DDoS対策において、精度-費用間のトレードオフが存在する
- DDoS防御の精度
  - False positive：通常トラフィックを誤って攻撃トラフィックと判断して遮断してしまうこと
  - False negative：攻撃トラフィックを誤って通常トラフィックと判断して通してしまうこと

	手法	特徴	巻込	費用
①	ブラックホールルーティング	大規模アタックに対する対処。特定IP宛の全てのトラフィックを全て破棄		
②	アクセス制御設定	ルータ等におけるACL設定にてIP+Portの組み合わせでパケットを破棄		
③	DDoS軽減専用装置	きめ細やかなDDoS対処が可能。DDoS軽減専用装置にトラフィックを通して防御実施		

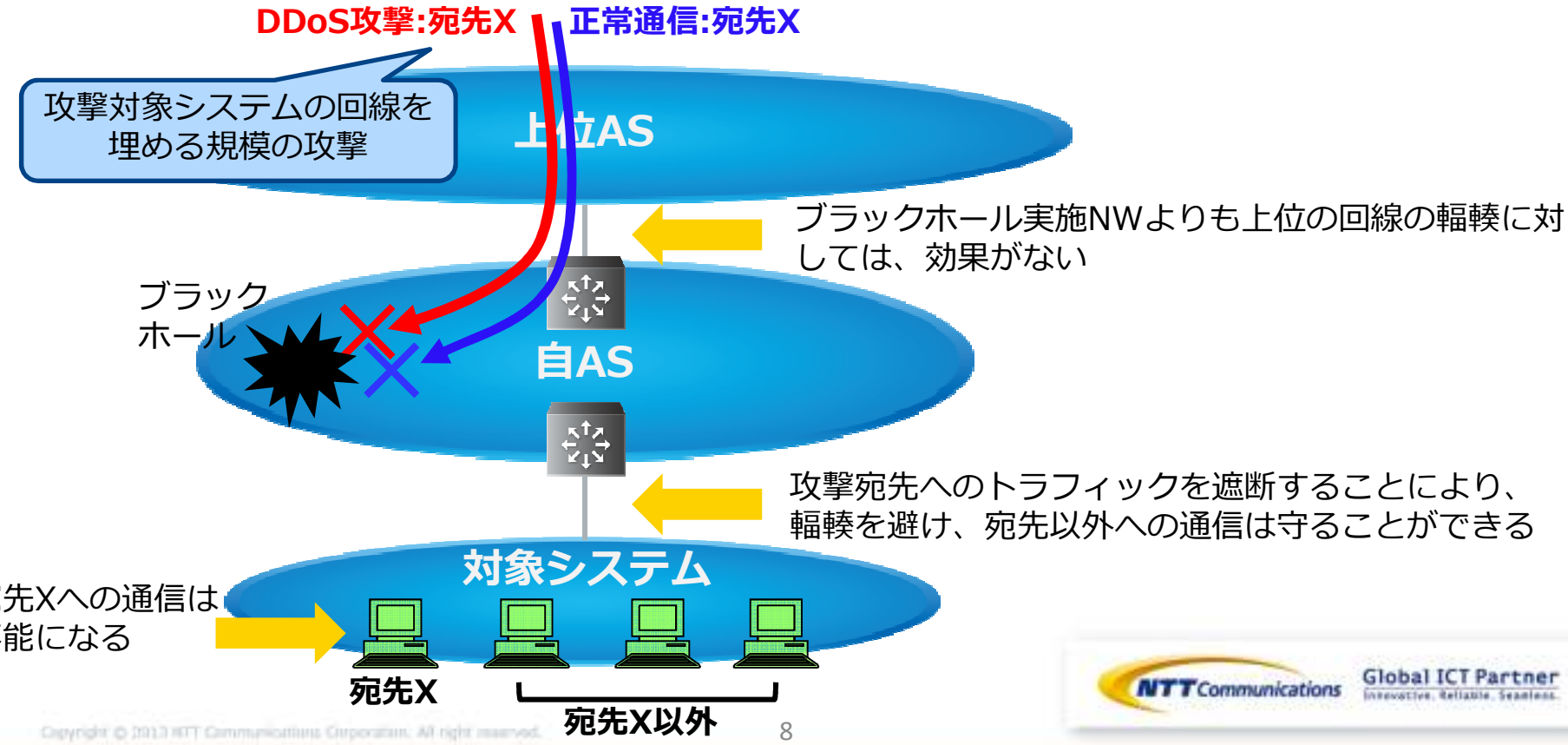


防御手法の具体例

- ブラックホールルーティング
- DDoS軽減専用装置を利用した防御
- Flowspec

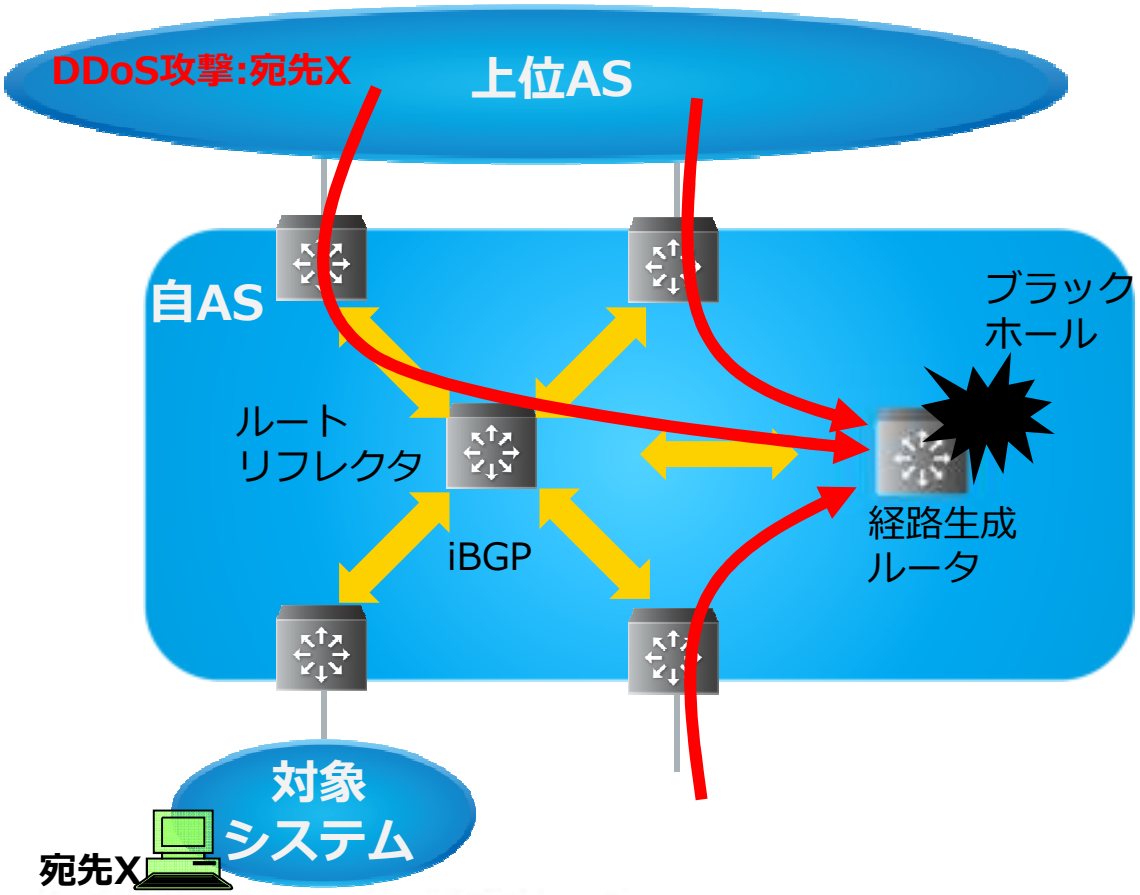
ブラックホールルーティング

- ブラックホールルーティングの特徴
  - 攻撃のターゲットとなったIPアドレス宛の通信を遮断
  - 配下の回線の輻輳を避けることができるが、ターゲットに対する全てのトラフィックが遮断されるため、攻撃自体は成立



自ASにおけるブラックホールルーティング手法の例(1)

- ブラックホールルーティング
  - 宛先に到達不能なルータ(ゴミ箱ルータ)を用意して、到達不能経路をiBGPで網内に広報する



経路生成ルータ：

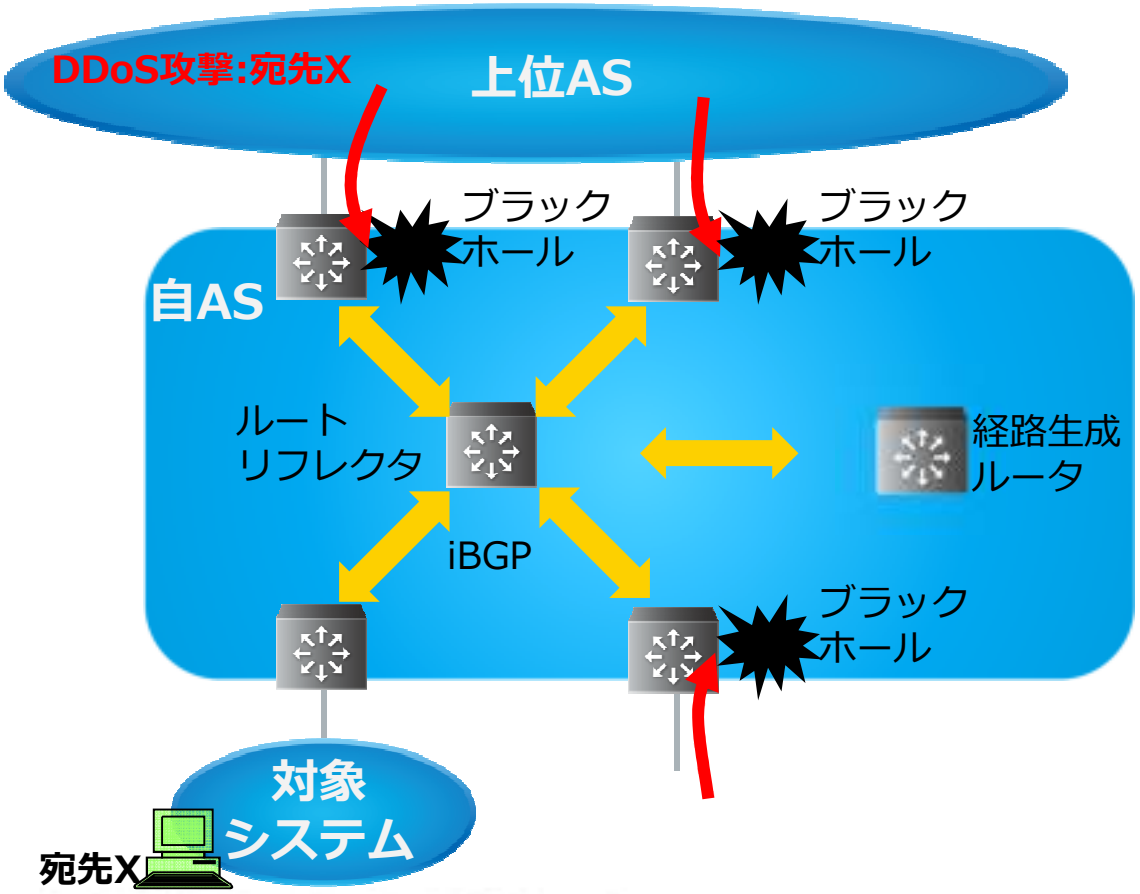
経路生成：
ip route X.X.X.X/32 null0
static-to-BGP

経路広報：
iBGP
next-hop-self
community no-export

※ルートリフレクタ自身を経路生成ルータとしてもよい

自ASにおけるブラックホールルーティング手法の例(2)

- RTBH:Remotely Triggered Black Hole Filtering
  - 特定のCommunityを用意して、Communityが付与されている経路は、各ルータでNull0にルーティングする



経路生成ルータ：

経路生成：
ip route X.X.X.X/32 null0
static-to-BGP

経路広報：
iBGP
community <AS>:666
community no-export

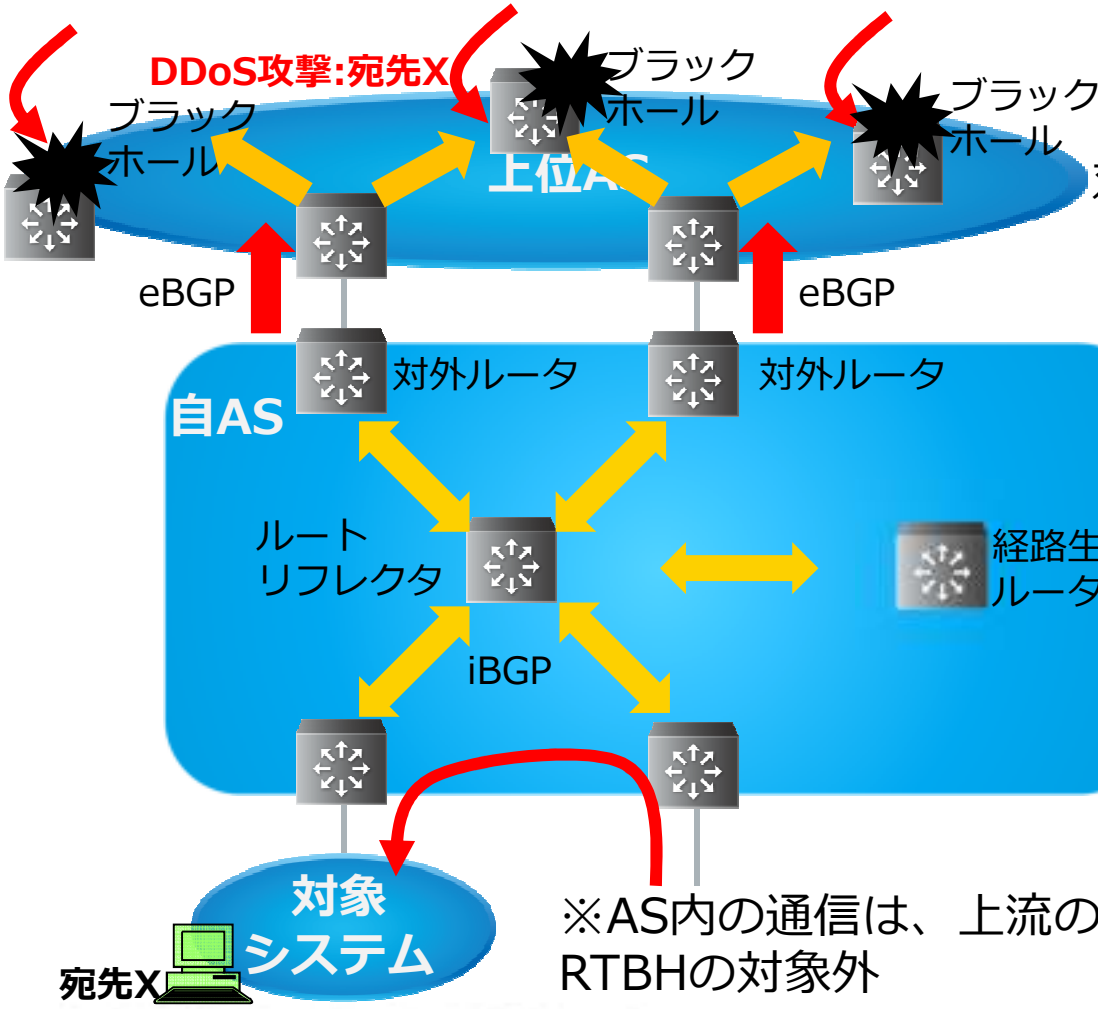
網内ルータ：

static：
ip route 192.0.2.1/32 null0

経路受信：
match community <AS>:666
then next-hop 192.0.2.1

上流ASにおけるブラックホールサービス

- 一部のトランジットASやIX事業者は、顧客からのRTBH経路を受け入れている



対外ルータ：

経路広告：
eBGP
match community <AS>:666
then set community 65535:666

経路生成ルータ：

経路生成：
ip route X.X.X.X/32 null0
static-to-BGP

経路広報：
iBGP
community <AS>:666
community no-export

上流AS/IXによるRTBH

- メリット
  - 自ASに攻撃が入ってくる前に攻撃を止められるため、上流回線の輻輳を避けることができる
  - 自ASのRTBHと組み合わせて利用できる
  - 自動化が容易である
- デメリット
  - 攻撃が止まったかどうかの判断ができない

- 注意点
  - 対応していない事業者もある
    - ✓ 選定の時の考慮事項にいれましょう☺
  - RTBH用の広告経路(/32, /128)を受け入れてもらえるようフィルタを空けてもらうことを忘れないように

RTBH用のcommunity

- IETF grow(Global Routing Operations) WGにて、Communityの共通化の提案がされている
  - 65535:666 になる見込み

Motivation: Different Triggers for Blackholing

- Different triggers for Blackholing at IXPs (selection):
  - DE-CIX Apollon — Blackhole IP Address: FRA: 80.81.193.66, NY: 206.130.10.66
  - Netix — Blackhole Community: 65499:999
  - MSK-IX.ru — Blackhole Community: *0:666*
  - NIX.CZ — Fenix: RTBH
  - TPIX.pl — Blackhole Community: *29535:666*

  Policy control at route servers

- Different triggers for Blackholing at ISPs (selection):
  - Init7: Blackhole Community: *65000:666*
  - Team Cymru: Blackhole Community: *64496: 666*
  - Hurrican Electric: Blackhole Community: *6939:666*
  - NTT: Blackhole Community: *2914:666*
- Proposal: One commonly agreed way to trigger Blackholing at IXPs and ISPs -> Internet Draft

https://tools.ietf.org/html/draft-ymbk-grow-blackholing-00

(参考)Selective RTBH

- 全網内でブラックホール化するのではなく、地域ごとや国ごとなどの特定エリアのルータでのみパケットを破棄する
  - 自国内の折り返しについてはブラックホールさせたくない場合などの利用方法が考えられる

- 例：AS2914

Selective Blackhole communities	
2914:661	only blackhole inside the region the announcement originated
2914:663	only blackhole inside the country the announcement originated
2914:660	only blackhole outside the region the announcement originated
2914:664	only blackhole outside the country the announcement originated

https://www.us.ntt.net/support/policy/routing.cfm

ブラックホールルーティングまとめ

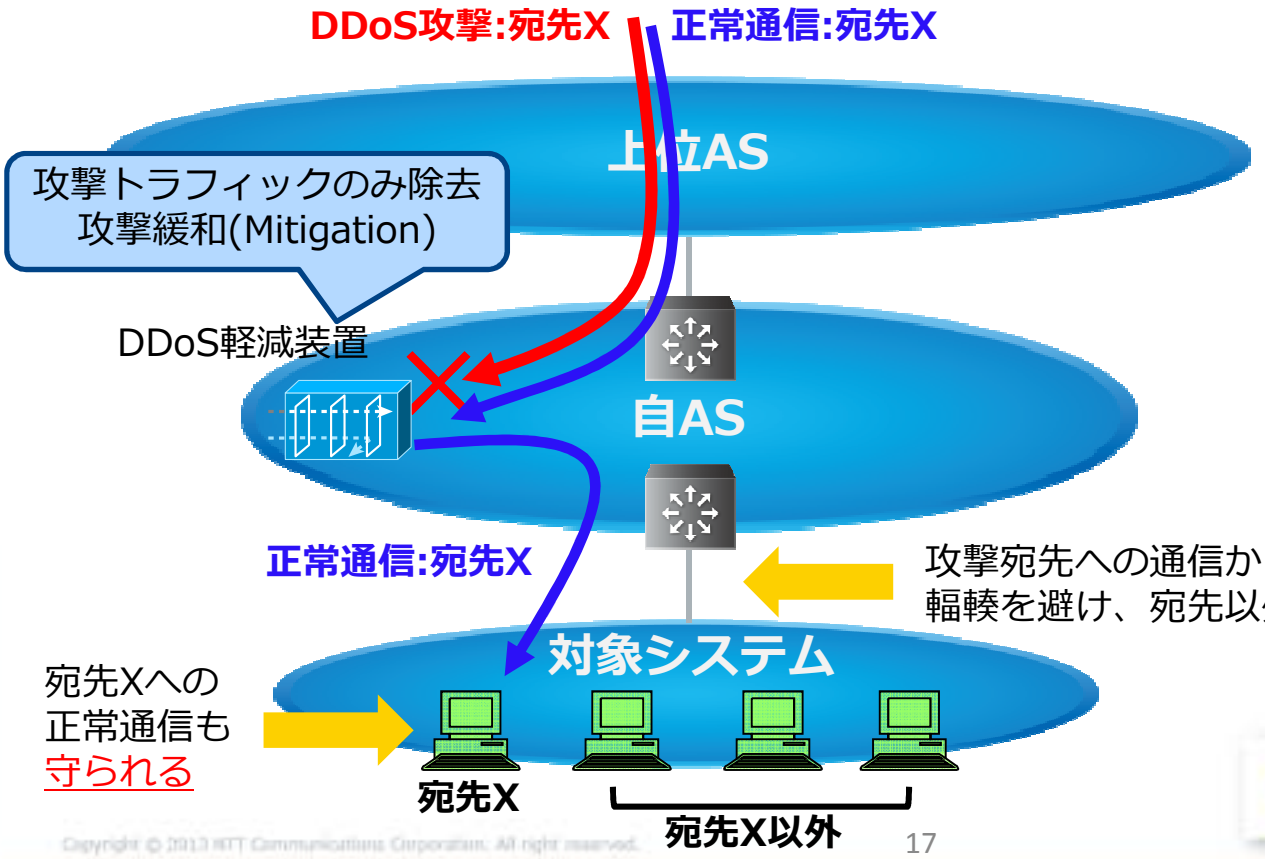
- すでに多くのISPで利用されている
- 対象のトラフィックを全て止めてしまう
  - そのため、効果は限定的
- より上流で止めるために、blackhole communityを受け入れている事業者がある
- selective blackhole などの新しい技術もある
  - 他にも、RTBH with uRPF など
- community 制御が重要

防御手法の具体例

- ブラックホールルーティング
- DDoS軽減専用装置を利用した防御
- Flowspec

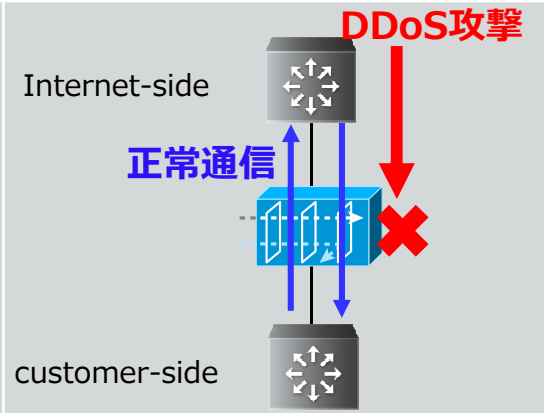
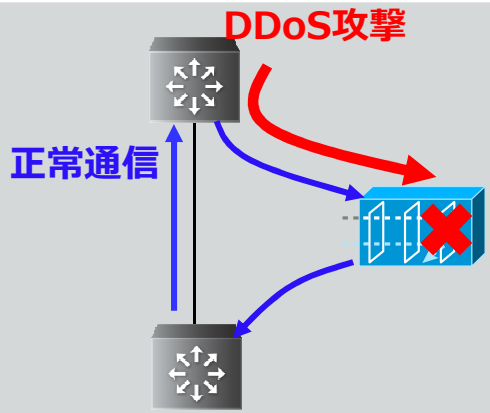
DDoS軽減専用装置を利用した防御

- DDoS軽減専用装置を利用した防御の特徴
  - DPIによりきめ細やかに攻撃だけを遮断
    - ✓ 精度はメーカのシグネチャに依存⇒誤検知との戦いの始まり
  - サービスを継続することができる(ただし高価)



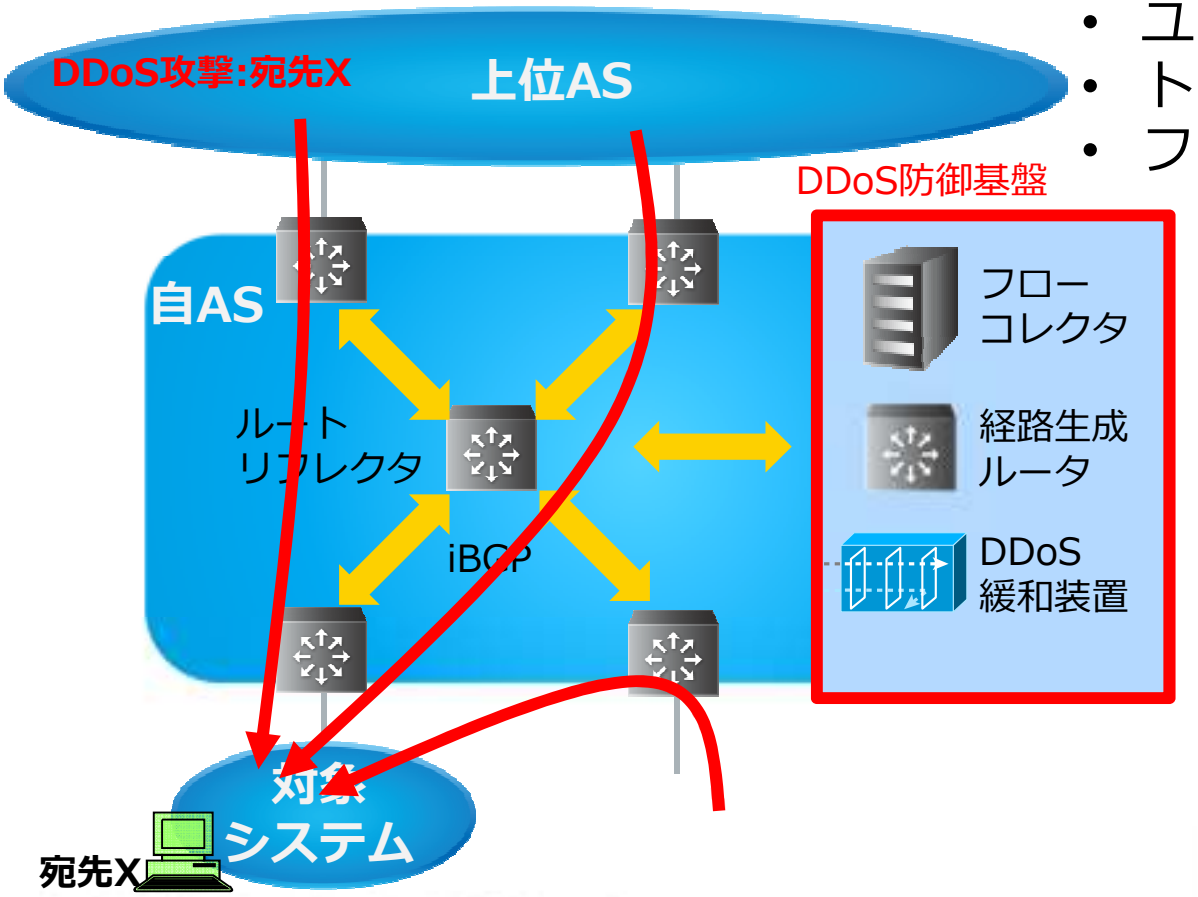
DDoS軽減専用装置を利用した防御

■ 主な構成

	インライン構成	オフランプ構成
構成		
防御期間	常時	flow情報などにより検知をし、一時的にトラフィックを引き込んでいる間のみ
トラフィック制御	特になし	BGP等を用いてトラフィックを引き込むGREトンネル等を利用して、元のNWに戻す
検知	DDoS軽減専用装置	flow技術による検知やユーザ申告など
防御	DDoS軽減専用装置	DDoS軽減専用装置
収容可能ユーザ	少ない	多い

オフランプ型DDoS緩和の例

- オフランプ型DDoS緩和
  - ①検知　②トラフィック迂回　③除去　④トラフィック戻しの4技術の組み合わせ

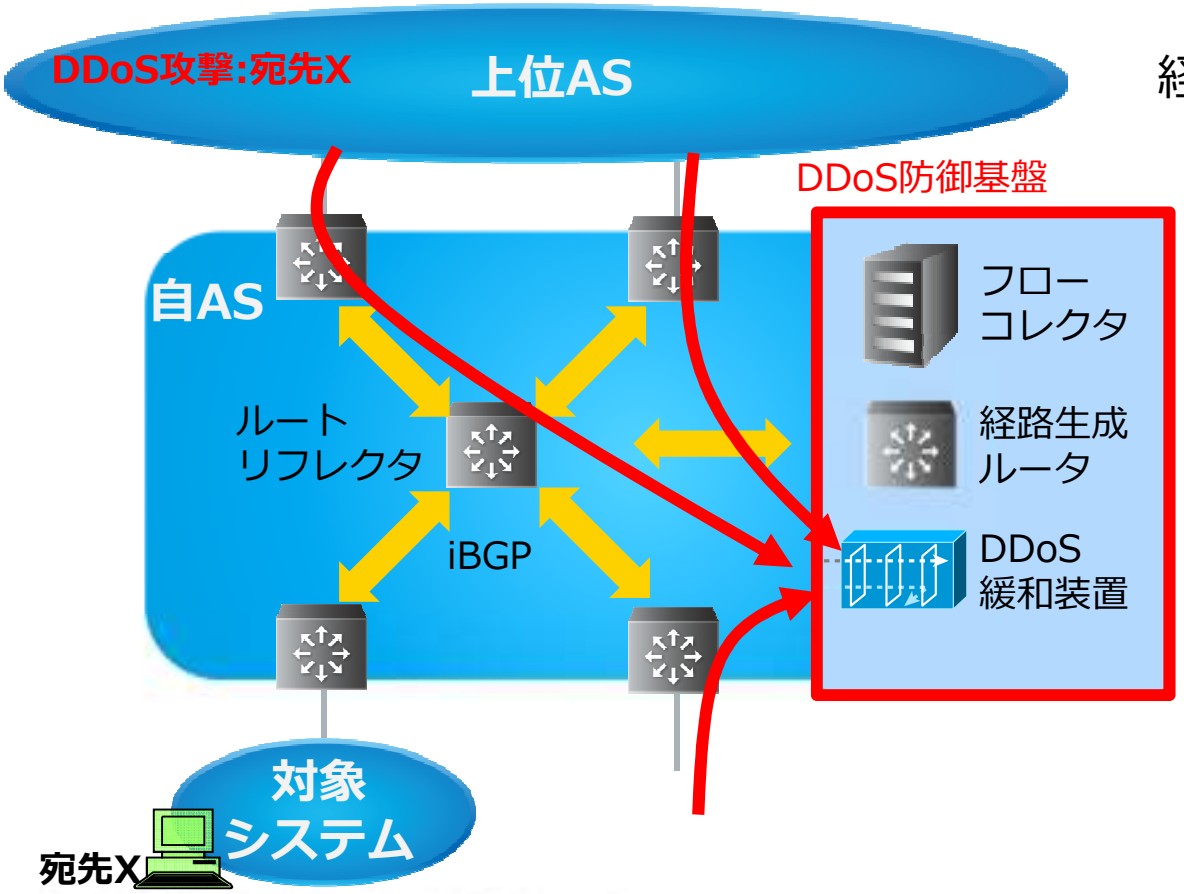


①検知
- ユーザからの申告
- トラフィック閾値監視
- フローコレクタによる検知

オフランプ型DDoS緩和の例

②トラフィック迂回

- 検知情報を元にトラフィックをDDoS緩和装置に引き込む
  - ✓ フローコレクタが経路生成する機能を持つ場合もある
  - ✓ DDoS緩和装置が経路生成する機能を持つ場合もある



経路生成ルータ：

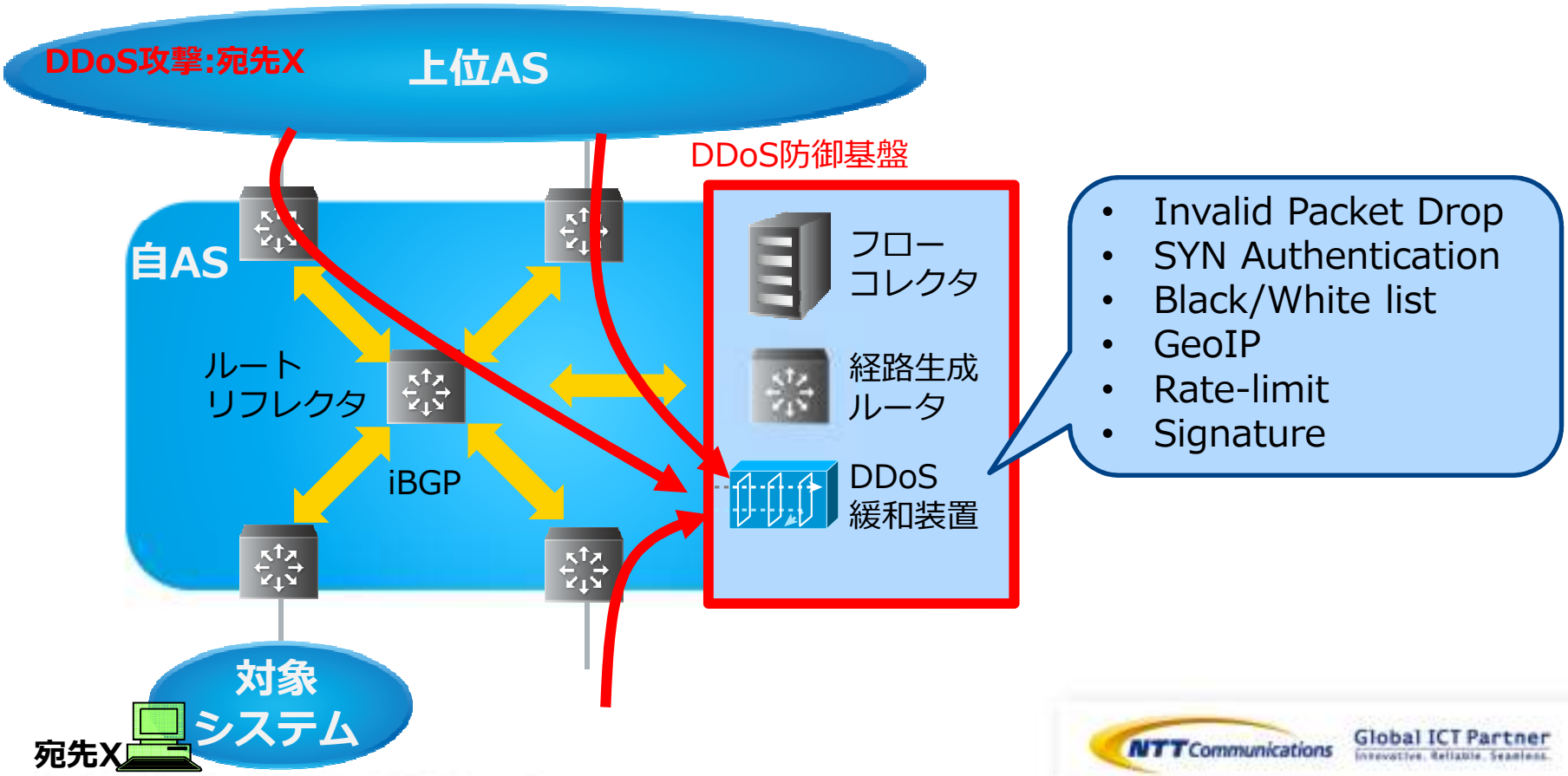
経路生成：
ip route X.X.X.X/32 null0
static-to-BGP

経路広報：
iBGP
next-hop <DDoS緩和装置>
community no-export

オフランプ型DDoS緩和の例

③除去

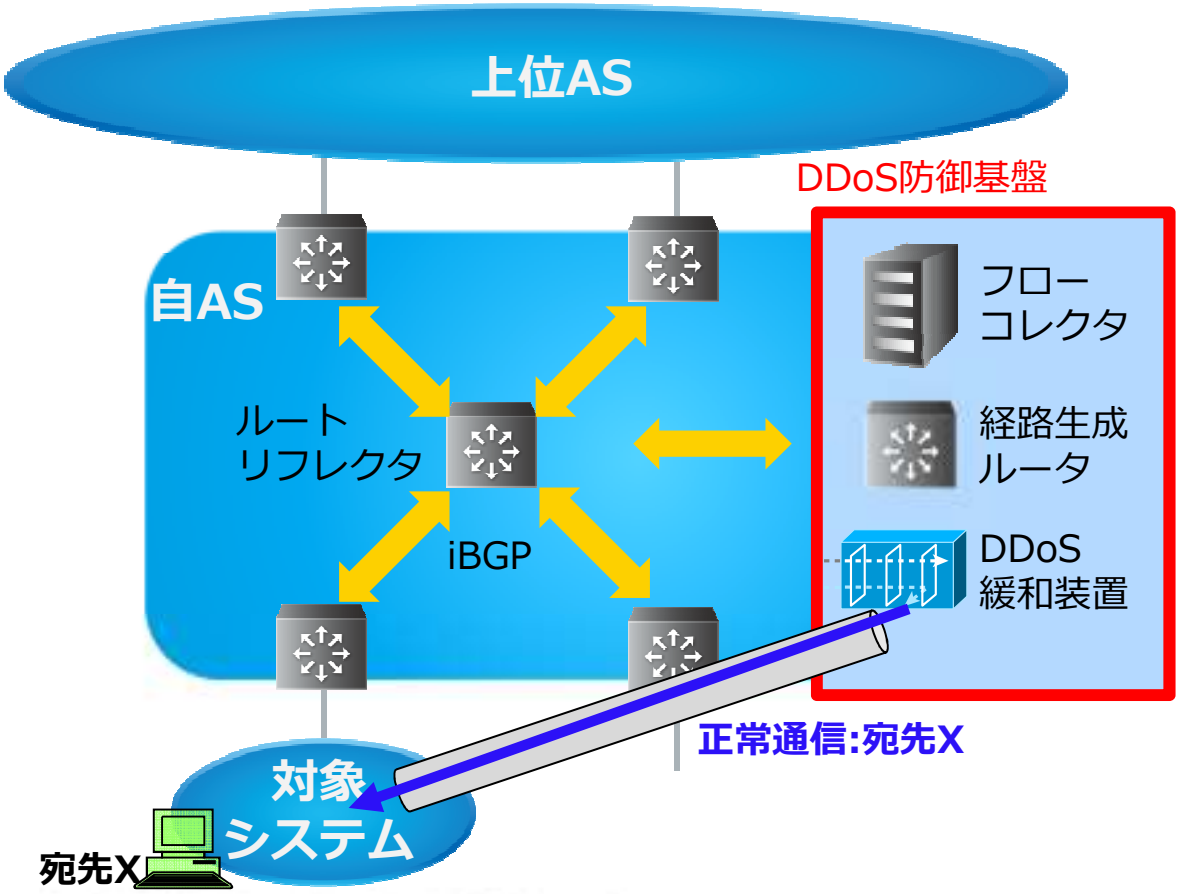
- DDoS緩和装置の機能により、攻撃トラフィックを除去



オフランプ型DDoS緩和の例

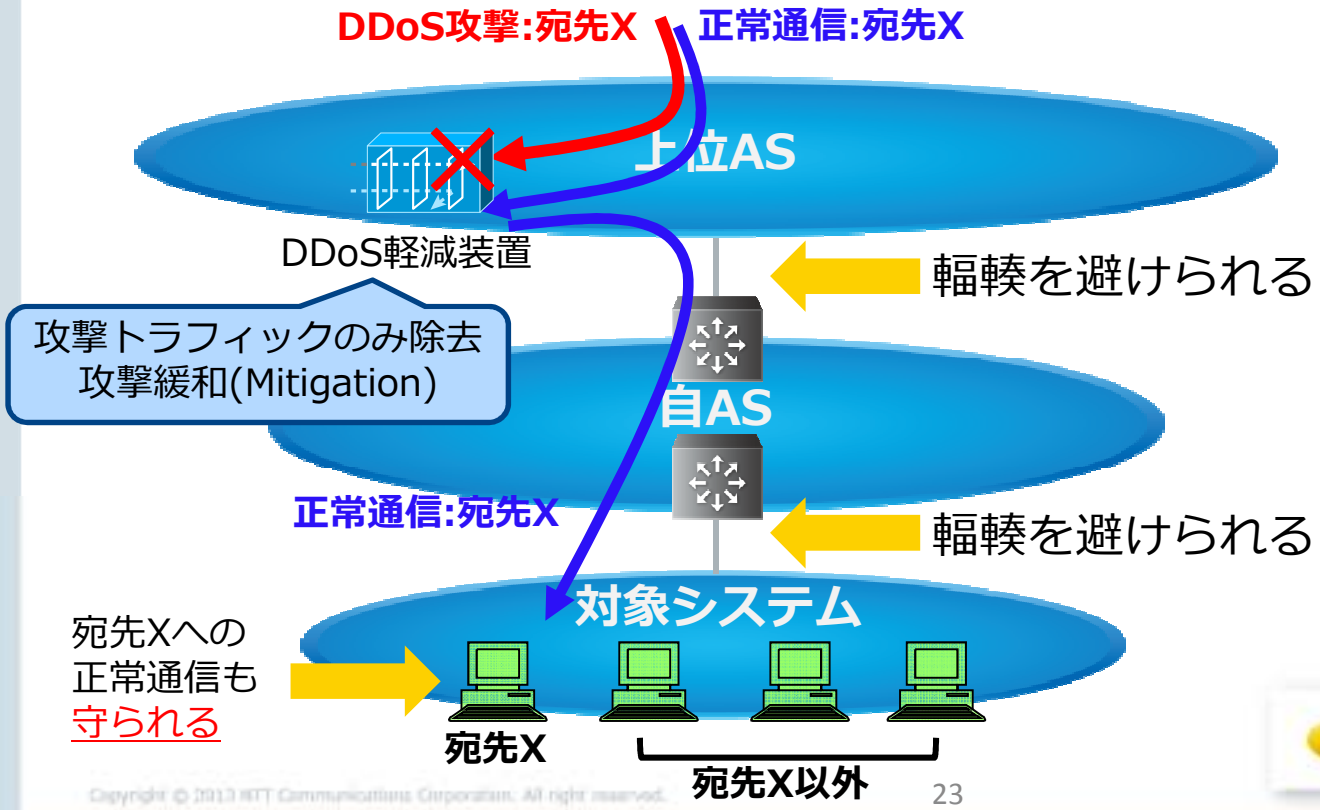
④トラフィック戻し

- ループにならないように、トラフィック引き込み範囲よりも、外側にトラフィックを返す
  - ✓ 専用線、トンネル(GRE)



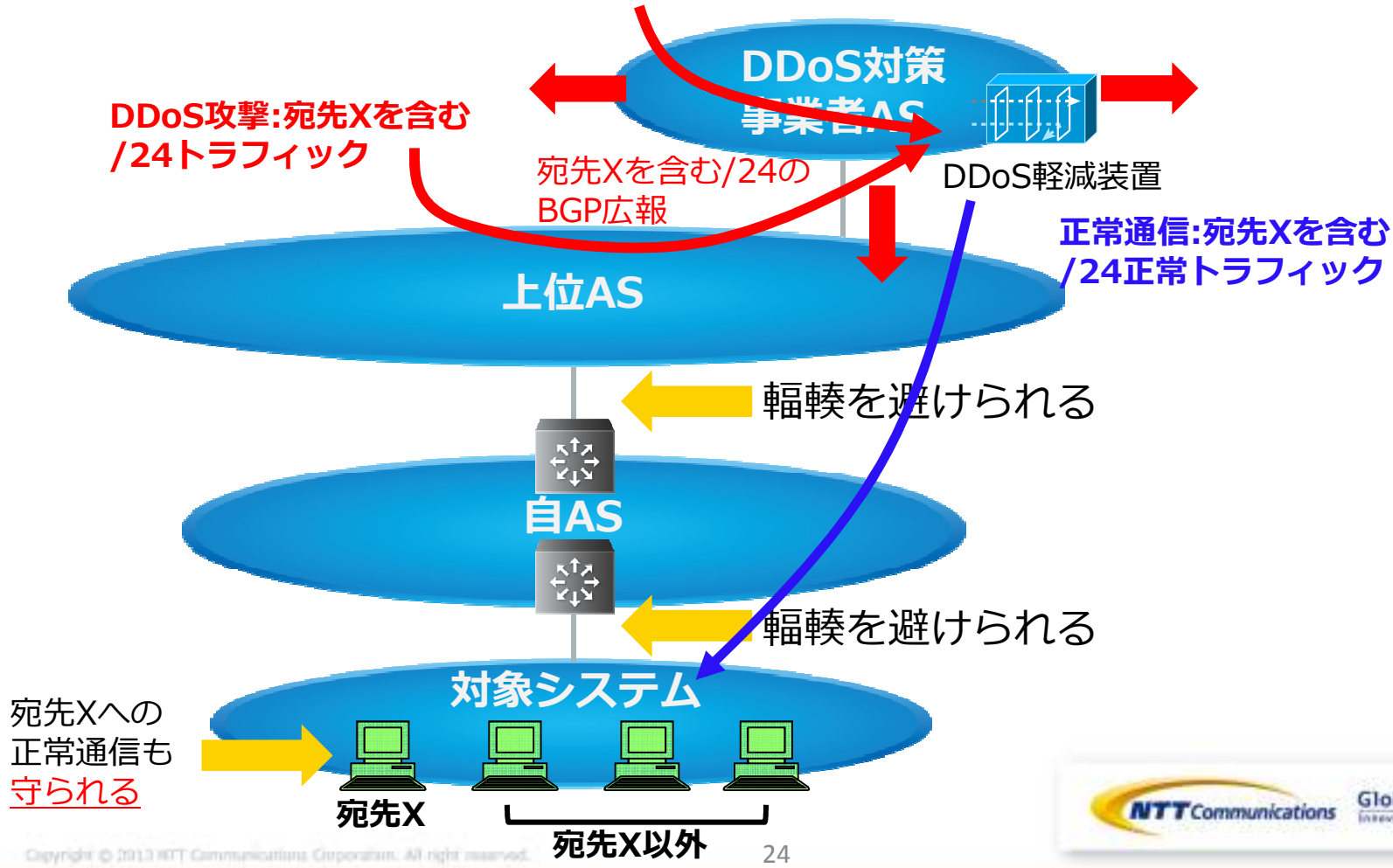
上流ASにおけるDDoS軽減サービス

- トランジット回線に付随するDDoS軽減サービス
  - インライン型
  - オフライン型
    - ✓ ①検知　②トラフィック迂回　③除去　④トラフィック戻しの4技術の組み合わせである点は同じ



クラウド型DDoS対策事業者におけるDDoS軽減サービス

- トランジット回線に依存しないDDoS軽減サービス
  - BGPを用いて/24単位のトラフィックの迂回を行う



クラウド型DDoS対策事業者におけるDDoS軽減サービス

トラフィック迂回手法

- 自ASの経路を、 DDoS対策事業者が代わりに広報する
- ASが異なるため、
  - DDoS対策事業者のASのIRR登録に、自ASの経路を追加する必要がある
    - ✓ 上記のIRR登録がないと、インターネット上に伝播しない、経路奉行がアラートを出す、という事象が予想される
  - DDoS対策事業者のASのRPKI登録に、自ASの経路を追加する必要がある
    - ✓ 複数のOriginで同一のprefixを登録することは可能
    - ✓ 広報単位が/24になるため、 maxlen=24で登録するとよい
  - 自ASがその経路を受け取らないようにする
    - ✓ 自経路を受け取らない経路フィルタ
    - ✓ トラフィック戻し後のトラフィックが再度インターネット上に流れてループするのを防ぐため
- 同一ASで経路広報する場合もある

クラウド型DDoS対策事業者におけるDDoS軽減サービス

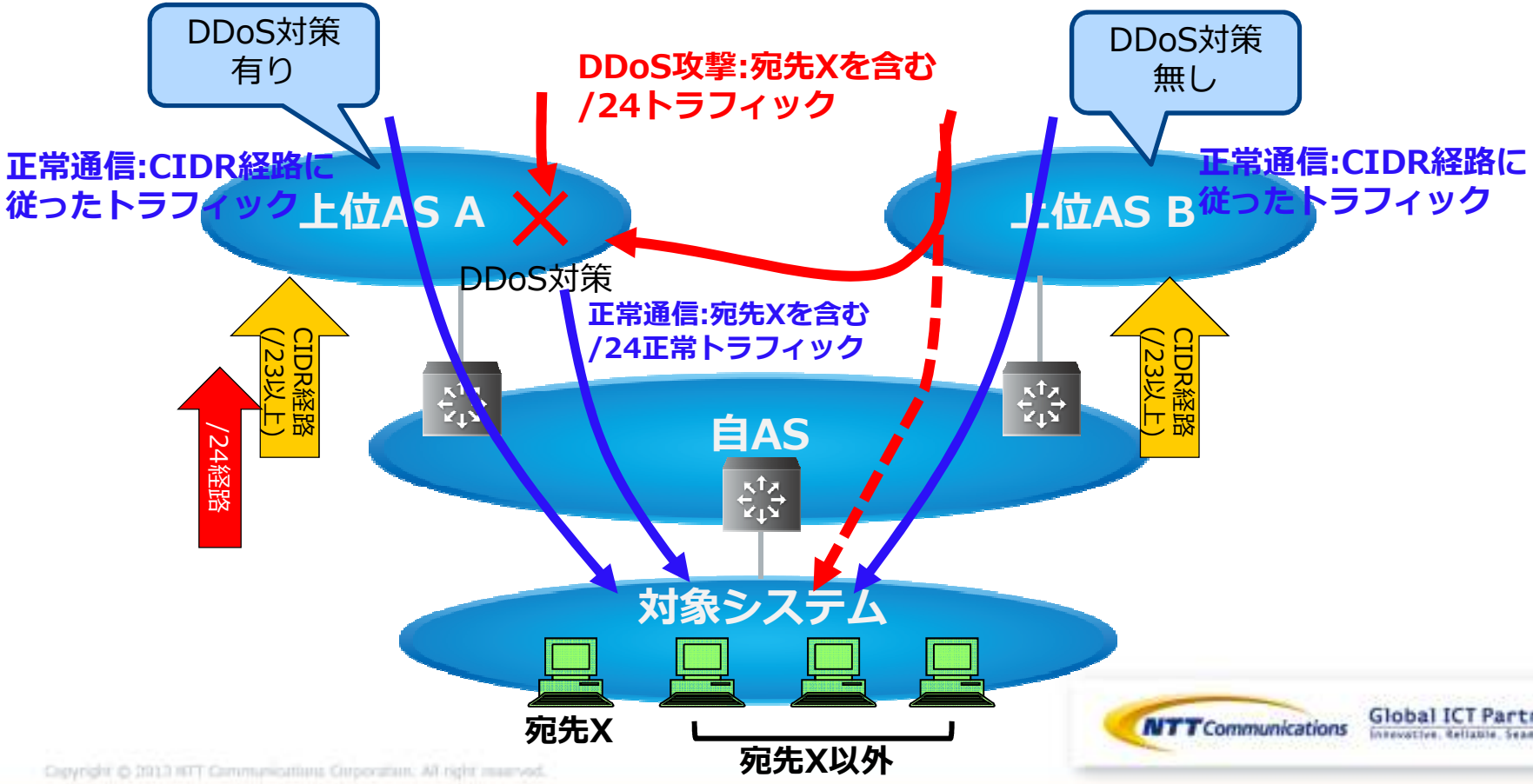
■ クラウド型DDoS対策の特徴
- トランジット回線に依存しない
- 上流回線の輻輳も避けることができる
- 経路制御を伴うため、セキュアに代理広報してもらう仕組みが重要
- トラフィック戻し
  - ✓ インターネット上で返すため、トンネル技術を用いる必要がある
  - ✓ あるいはトラフィック戻し専用の回線を用意する必要がある

■ デメリット
- /24単位での引き込みになるため、攻撃宛先(/32)以外のトラフィックに影響がある
  - ✓ 遅延が付加される
  - ✓ トンネルを通るため、フラグメントする可能性がある

マルチホーム環境におけるDDoS対策

マルチホーム環境

- DDoS対策が無いトランジットから攻撃が流入してしまう
- より細かい(/24)経路広告によって、DDoS対策があるトランジットにトラフィックを寄せて対応することができる



マルチホーム環境におけるDDoS対策

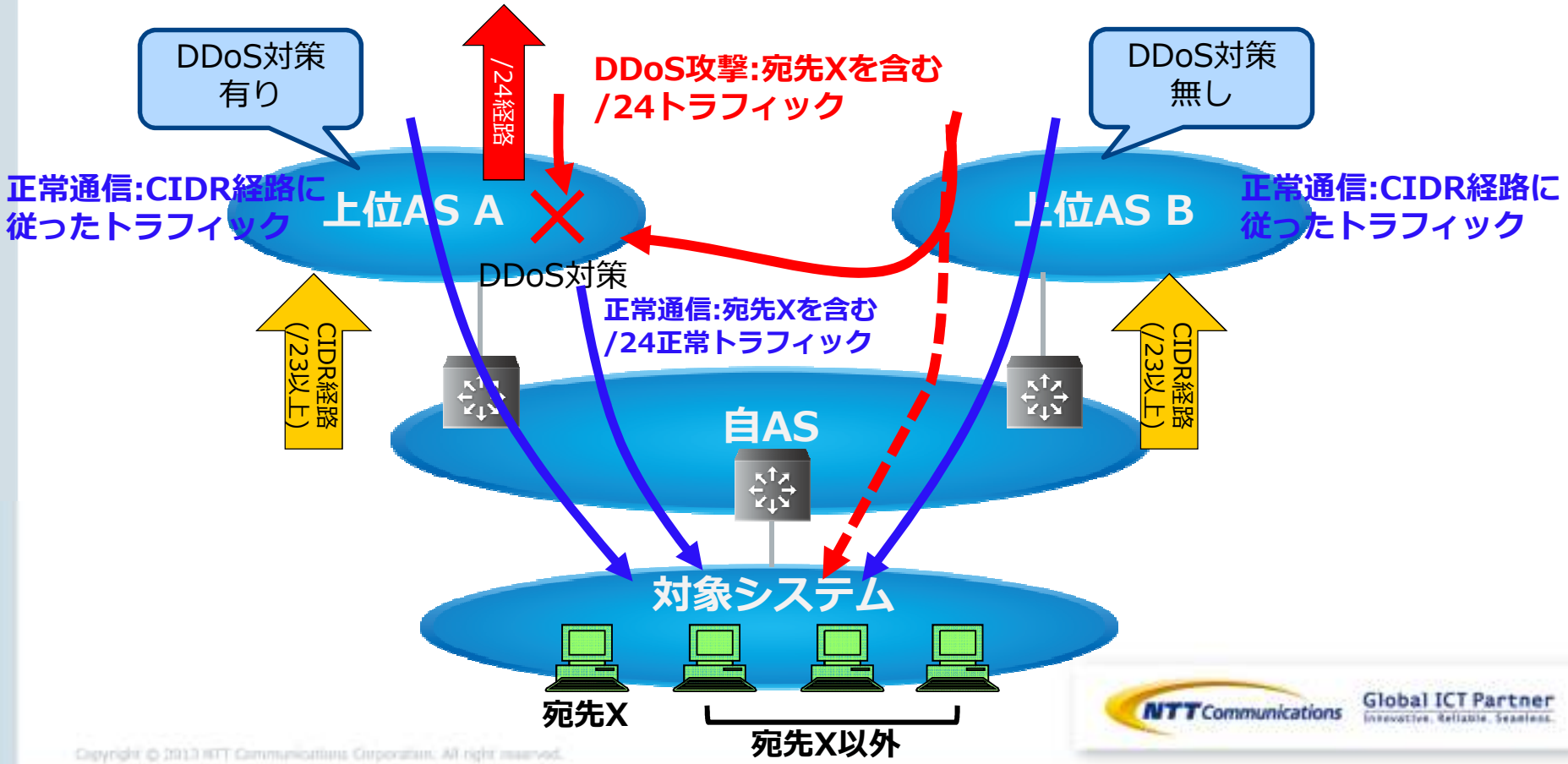
- 自ASの細切れ(/24)経路を、DDoS対策があるトランジットに広報する
  - 準備をせずにいきなりはできない

POINT:

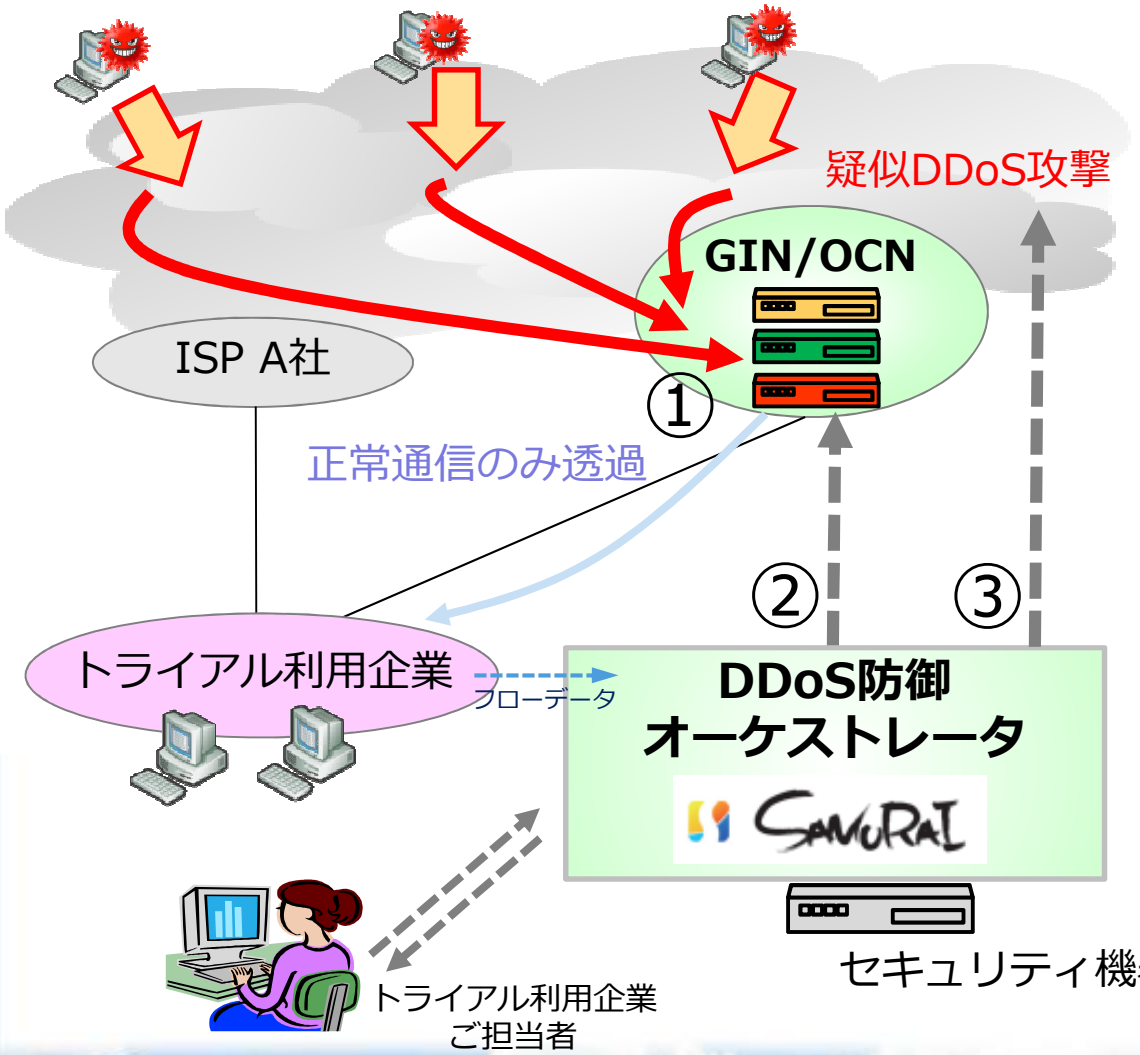
- トランジット側で、経路を受け入れること
  - exact ではなく or longer での経路フィルタが可能なことが望ましい
- RPKI登録
  - 広報単位を細切れにするため maxlen=24とすることを推奨
- 自動化
  - 攻撃検知後の細切れ経路の広報を自動化し、できるだけ短時間で対策実施できること

マルチホーム環境におけるDDoS対策

- 細切れ(/24)経路の経路広告について、上流ASで代理で実施することができないか？



DDoSテストベッド トライアルを開始



■３つの特徴

①NTT Com独自の経路制御技術

- DDoS攻撃をGIN/OCNに引き込み一元的に防御

②適切な防御手段の選択

・マネジメントポータルから状況に応じた防御手段を選択

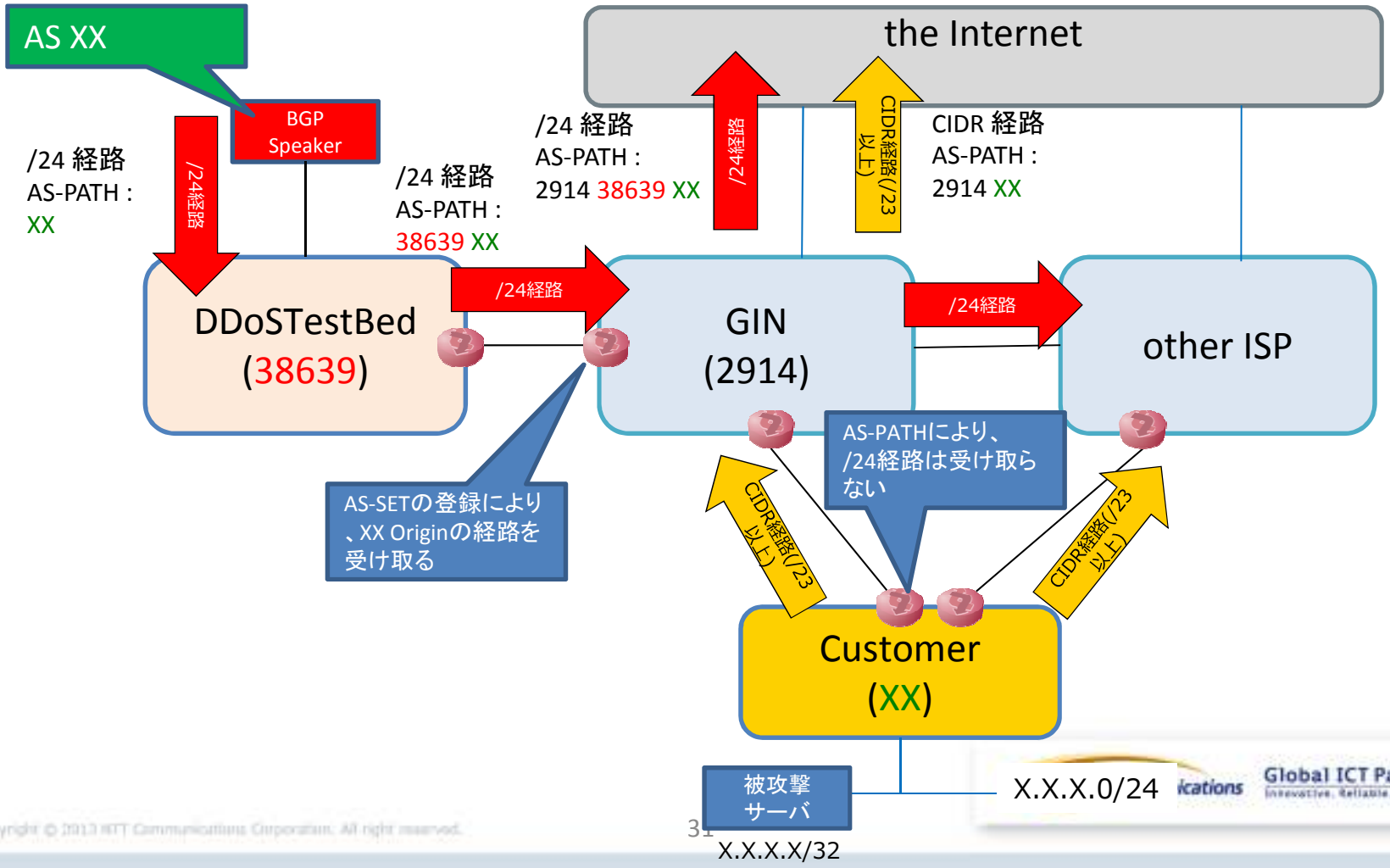
③擬似攻撃発生による試験実施

・トライアル利用企業が自社への擬似DDoS攻撃が可能
・利用企業が自ら試験シナリオを作成・実行し有効性を評価

セキュリティ機器ベンダ提供のDDoS緩和装置

同一Origin ASによる代理広告

- Origin ASを同一にするメリット：
  - /24経路をCustomerに受け取らせない
  - AS-SETの登録によりGINに経路を受け取らせる

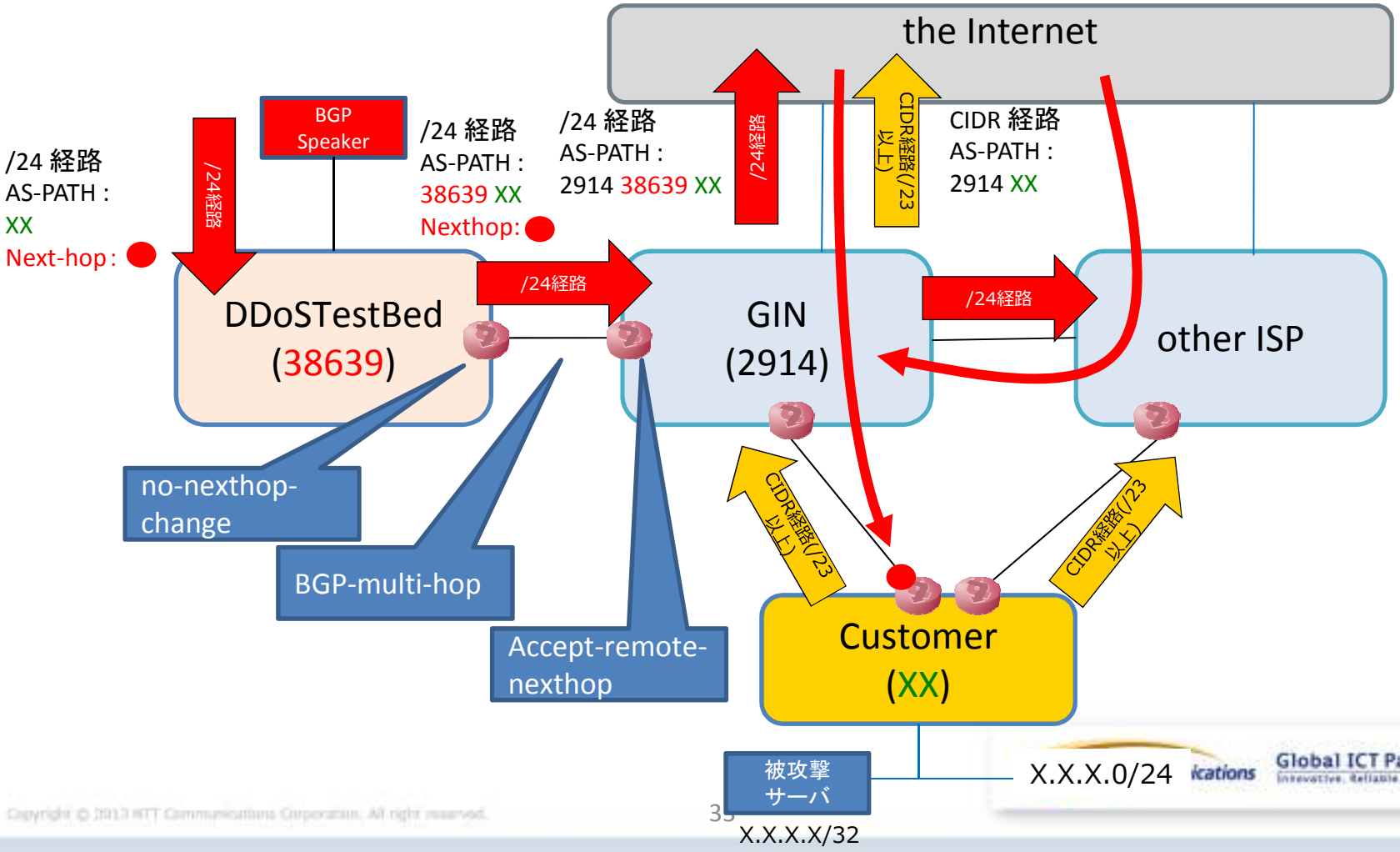


同一Origin ASによる代理広告

- DDoSテストベッドからの広報をGINはなぜ受け取るのか？
  - AS-SETにCustomerのASを登録することにより、配下にCustomer ASがあるように見せかけます。IRRへの登録により、経路フィルターが動的に更新されます。
- /24の細切れをIRRに登録していなくてもOKなのか
  - /24のlonger経路を受け取るようにGIN側で設定しています。
  - また/32のlonger経路も受け取るようにしています。
- 経路奉行はアラートを出すのか？
  - OriginASで評価しているようなのでアラートはでませんでした。
- RPKIを導入したらValidationでNGになるのか？
  - Origin Validation：Originが一致しているので、validになると思われます(exactで書いている場合はinvalidになる可能性があります。Maxlen=24の場合はOKと思われます)
  - Path Validation：AS-Pathが変わるのでinvalidになると思われます(代理広報用に登録いただければOKです)

Next-hopの代理の工夫

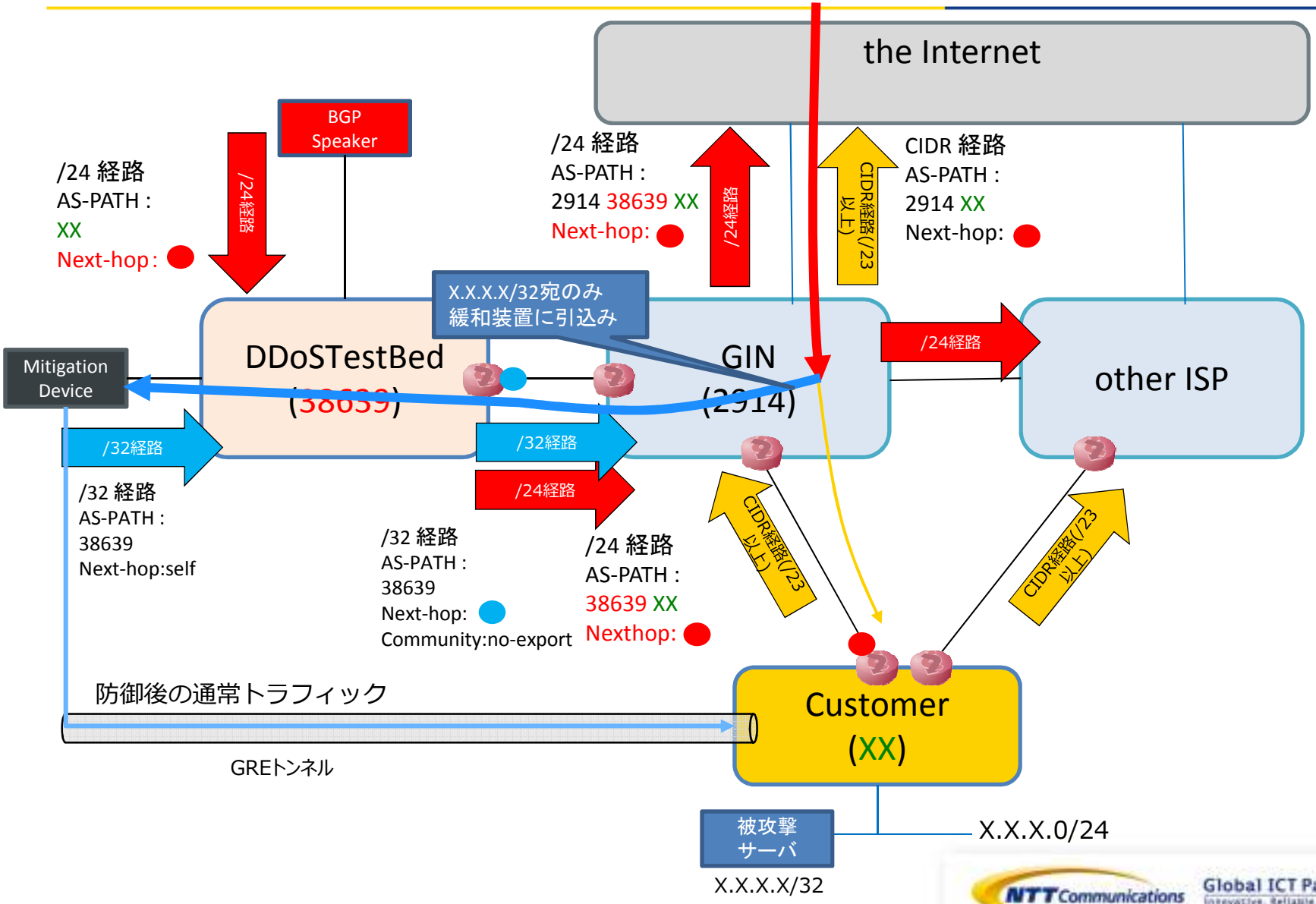
- Next-hopを代理するメリット
  - 引き込んだ/24トラフィックがそのまま顧客とのトランジットへ流れる(遅延への影響を最小化)



Next-hopの代理の工夫

- なぜNexthopの代理が必要なのか？
  - 通常のeBGPでは、ピアアドレスがNext-hopになるため、そのままではトラフィックを引き込んでしまう。
  - 一度引き込んでから返す方式だと遅延時間の増加が問題となるため、直接トランジットを通すようにした。

/24引き込み後の動作(/32引き込み)



DDoS軽減専用装置を利用した防御まとめ

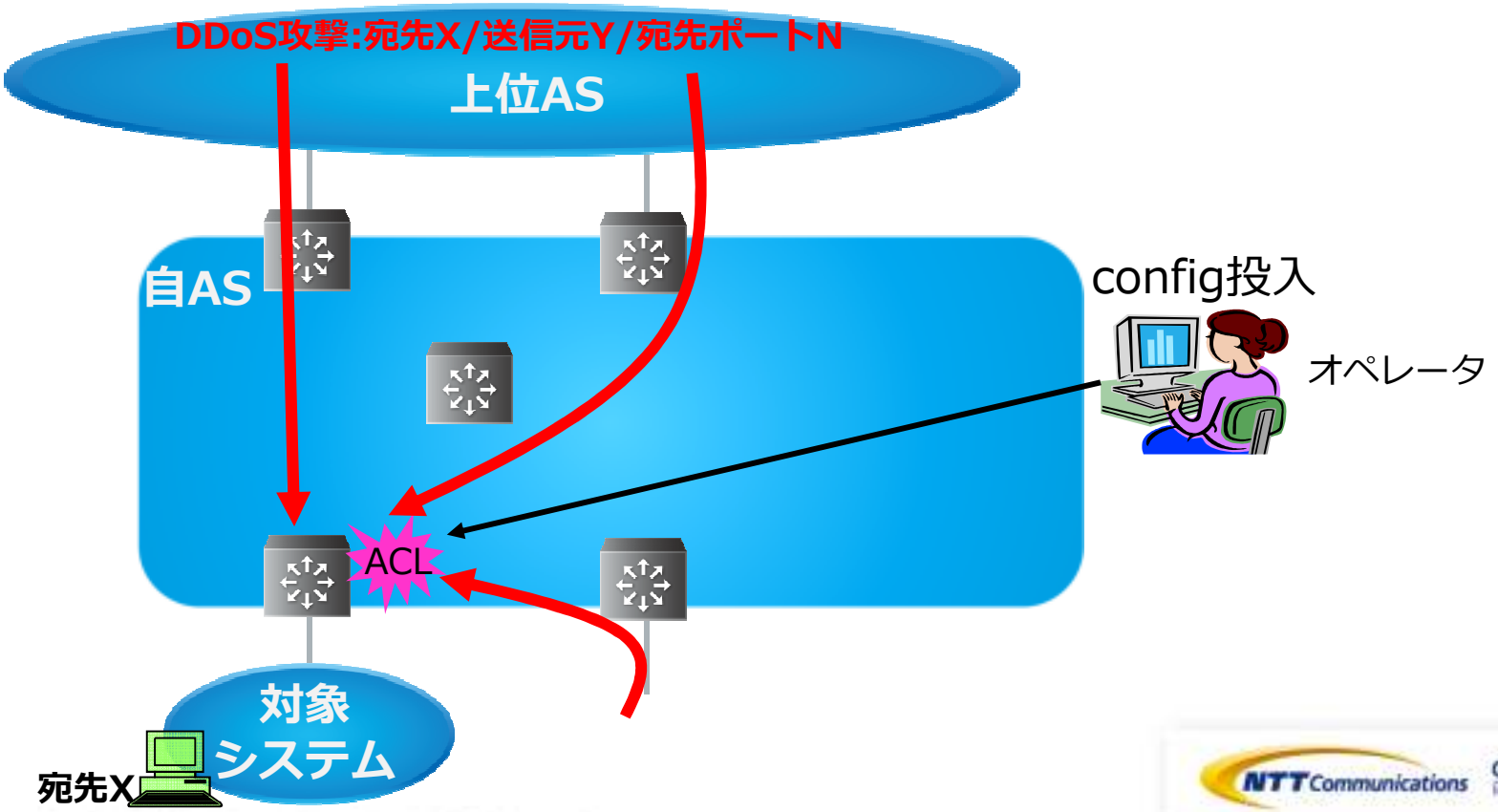
- オフランプ構成が一般的
  - ① 検知
  - ② トラフィック迂回→セキュアルーティングが重要
  - ③ 除去
  - ④ トラフィック戻し
- より上流において対策をする要望が強い
- トラフィック迂回における経路広告については、IRR登録や経路フィルターに要注意
- RPKIを導入しても、クラウド型・マルチホーム型のDDoS対策は可能
  - 同一Originの場合と異なるOriginの場合いずれにしても、適切にRPKI登録することで、広告することが可能

防御手法の具体例

- ブラックホールルーティング
- DDoS軽減専用装置を利用した防御
- Flowspec

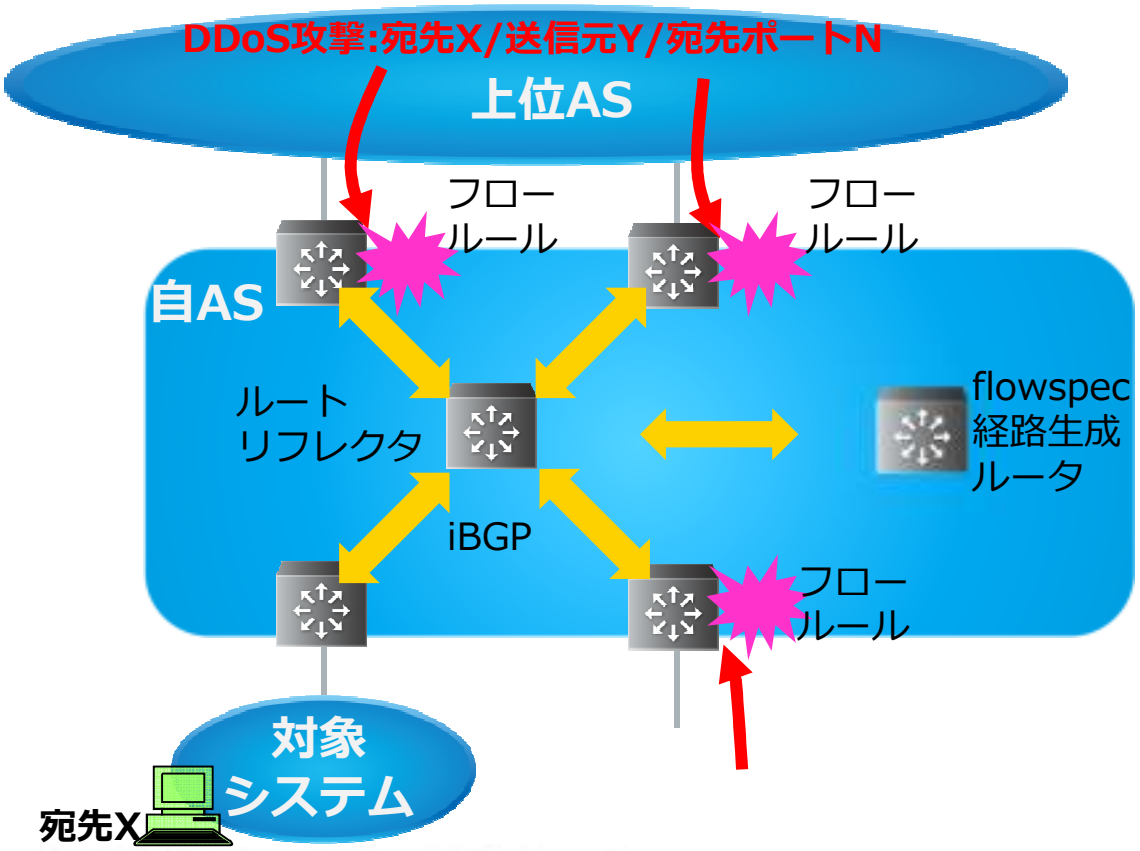
ACL:Access Control Listによる防御

- ACL:Access Control Listによる防御の特徴
  - 5tupleをベースとして、攻撃トラフィックだけを除去
  - オペレータが手動で投入する場合、攻撃の変化に動的に追従することが困難



BGP flowspecによる防御

- BGP flowspecによる防御の特徴
  - 5tupleをベースとした制御ルールを動的に配信可能
  - 対応ルータが限られている



flowspec経路生成ルータ：

```
routing-options {
    flow {
        route example {
            match {
                destination X.X.X.X/32;
                source Y.Y.Y.Y/32;
                destination-port N;
            }
            then discard;
        }
    }
}
```

網内ルータ：

```
protocols {
    bgp {
        group iBGP {
            type internal;
            family inet {
                flow {
                    no-validate;
                }
            }
} } }
```

BGP flowspecによる防御

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

```
+---------------------------------------------------------+
|                AFI(2 octets)  1 and 2                   |
+---------------------------------------------------------+
|             SAFI (1 octet) 133 and 134                  |
+---------------------------------------------------------+
| Length of Next Hop Network Address (1 octet)            |
+---------------------------------------------------------+
| Network Address of Next Hop (variable)                  |
+---------------------------------------------------------+
| Reserved (1 octet)                                      |
+---------------------------------------------------------+
| Network Layer Reachability Information (variable)       |
+---------------------------------------------------------+
```

SAFI
133 Dissemination of flow specification rules
134 L3VPN dissemination of flow specification rules

JANOG35: BGP Flowspec(RFC5575)
https://www.janog.gr.jp/meeting/janog35/program/bgpfs/

BGP flowspecへの期待

- 現状手動で行っているACLによる対策を自動化できる
- インタードメインでのBGP flowspecの利用
  - フロールールをフィルタする/信頼する仕組みは？

まとめ

セキュアルーティング時代のDDoS対策テクニック

- DDoS攻撃の頻度・ボリュームの増加
  - 自動化による短期間での対処
  - より上流での対策

- DDoS対策のためのBGP制御
  - 自動化のために以下を適切に設定する
    - ✓ community制御
    - ✓ 経路フィルタ
    - ✓ IRR登録
    - ✓ RPKI登録

- DDoS対策とセキュアルーティングは「手を取り合って」
  - DDoS対策≠経路ハイジャック