NTTコミュニケーションズにおける
マルチホームのお客様向けソリューションのご紹介

2018年02月23日

NTTコミュニケーションズ株式会社
ネットワークサービス部　Nguyen Tuan Duong

Transform your business, transcend expectations with our technologically advanced solutions.

自己紹介

Nguyen Tuan Duong （グエン トウアン　ズオン）

ネットワークサービス部　ネットワークビジネスエキスパート
東京オリンピック・パラリンピック推進室（兼務）
1985年10月1日生まれ　ベトナム出身

NTT ComのインターネットサービスGIN/OCNやNWセキュリティのSE
CiscoのSE最上位資格 CCIE Routing and Switching（#55027）

・2004年～2012年　日本留学
・2012年4月（H24) NTT Com入社
・2012年～2013年　NTT America勤務
・2014年～　　NTT Com勤務

Agenda

第一部：マルチホームのお客様向けDDoS対策ソリューションのご紹介

1．最近のDDoS攻撃を中心としたトピック

2．DDoS攻撃およびDDoS対策手法

3．マルチホームDDoS対策ソリューションのご紹介

第二部：トランジット＋IX接続のお客様向けソリューションのご紹介

4．マルチホームのお客様の現状＆課題

5．JPNAP接続ソリューションのご紹介

Agenda

第一部：マルチホームのお客様向けDDoS対策ソリューションのご紹介

1．最近のDDoS攻撃を中心としたトピック

2．DDoS攻撃およびDDoS対策手法

3．マルチホームDDoS対策ソリューションのご紹介

第二部：トランジット＋IX接続のお客様向けソリューションのご紹介

4．マルチホームのお客様の現状＆課題

5．JPNAP接続ソリューションのご紹介

最近のDDoS攻撃を中心としたトピック

1．DDoS攻撃の大規模化

米セキュリティ情報サイトの「Krebs on Security」が大規模なDDoS攻撃665Gbps

2．日本国内での被害

FXサイトや仮想通貨サイトにDDoS攻撃ーダウン相次ぐ

21 KrebsOnSecurity Hit With Record DDoS

On Tuesday evening, KrebsOnSecurity.com was the target of an extremely large and unusual distributed denial-of-service (DDoS) attack designed to knock the site offline. The attack did not succeed thanks to the hard work of the engineers at Akamai, the company that protects my site from such digital sieges. But according to Akamai, it was nearly double the size of the largest attack they'd seen previously, and was among the biggest assaults the Internet has ever witnessed.

The attack began around 8 p.m. ET on Sept. 20, and initial reports put it at approximately 665 Gigabits of traffic per second. Additional analysis on the attack traffic suggests the assault was closer to 620 Gbps in size, but in any case this is many orders of magnitude more traffic than is typically needed to knock most sites offline.

Martin McKeay, Akamai's senior security advocate, said the largest attack the company had seen previously clocked in earlier this year at 363 Gbps. But he said there was a major difference between last night's DDoS and the previous record holder: The 363 Gpbs attack is thought to have been generated by a botnet of compromised systems using well-known techniques allowing them to "amplify" a relatively small attack into a much larger one.

FXサイトや仮想通貨サイトにDDoS攻撃--ダウン相次ぐ

ZDNet Japan Staff 2017年09月19日 12時36分

国内のFXサイトや仮想通貨取引サイトに対する分散型サービス妨害（DDoS）攻撃が9月14日頃から継続的に発生しているもようだ。19日午前11時半時点でも一部サイトがダウンしている。

マネーパートナーズによると、14日午前9時10分頃にDDoS攻撃が発生し、断続的にアクセスしづらい状況が続いた。テックビューロでは、15日午前9時頃から同日午後7時40分頃まで、ボットネットのDDoS攻撃によるアクセス過多から、取引所内に関わる処理で想定以上に時間がかかる状態になった。

FXトレード・フィナンシャルは16日午前からDDoS攻撃を受け、一部サービスが利用できなくなった。同社は攻撃対象になったデータセンターからウェブサーバを移管し、ウェブサーバにおけるロードバランシングやファイアウォールによる攻撃元からの通信を遮断する対策を講じた。19日午前時点でも一部サービスを中断しており、同日正午以降に復旧する見込みだとしている。

ヒロセ通商は、18日までにDDoS攻撃が原因でウェブサイトや一部のサービスを中断した。サービスへのログインについては部分的に復旧しているものの、19日午前11時半時点もDDoS攻撃による影響を拡大させないための措置として、ウェブサイトへのアクセスを意図的に遮断しているという。

最近のDDoS攻撃を中心としたトピック

3. IoT端末のBot化（ウィルス感染）

「Mirai」による DDoS事例から IoT の「エコシステム」を考察する

投稿日: 2016年10月28日
脅威カテゴリ: 不正プログラム，サイバー攻撃，TrendLabs Report
執筆: Trend Micro

2016年10月21日、DNSサービスプロバ
DDoS）」の大規模な攻撃を受けたことが
機器に感染した不正プログラムが DDo
が、インターネットを支えるインフラスト
用不能となったことは、「モノのインター
告となりました。

IoT機器から600Gbpsを超えるDDoS攻撃

吉岡 克成＝横浜国立大学大学院環境情報研究院/先端科学高等研究院 准教授　2016/12/12　日経NETWORK

出典：日経NETWORK 2016年12月号pp.50-51
（記事は執筆時の情報に基づいており、現在では異なる場合があります）

目次一覧

ツイート　保存する

ラやデジタルビデオレコーダー（DVR）、ルー
ルス（マルウエア）が大きな脅威になってい
染を広げるとともに、サイバー攻撃を実施する。
そこで本記事では、IoTウイルスの現状や感染メカ

IoT機器を踏み台にした史上最大規模のDDoS攻撃が続々発生

2016/09/28

ツイート

Lucian Constantin IDG News Service

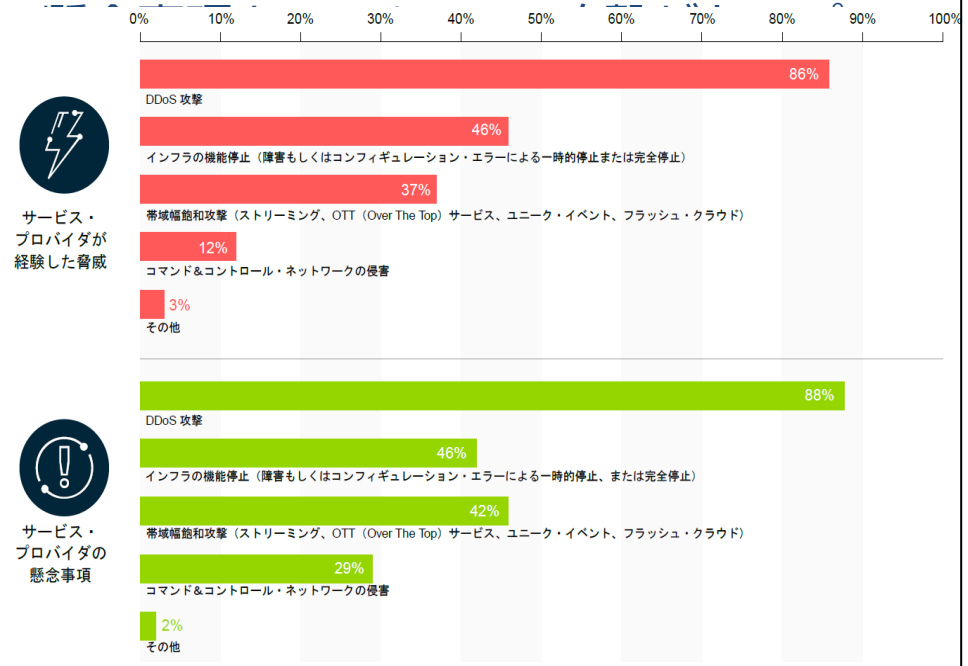
IoT（モノのインターネット）デバイスのセキュリティが貧弱なせいで、重大な事態が引き起こされる可能性があるとして、セキュリティ専門家は数年前から警告を発してきた。そして、今やその警告は現実のものとなった。IoTデバイスをハッキングしてボットネットを形成し、空前の規模で分散型サービス拒否（DDoS）攻撃を仕掛ける事例が相次いで発生している。

（参考）DDoS攻撃の現状（グローバル）

拡大傾向のDDoS攻撃をユーザ側だけで防御するのは限界
ネットワークの利用を継続するには**上流ネットワークでの防御**が不可欠

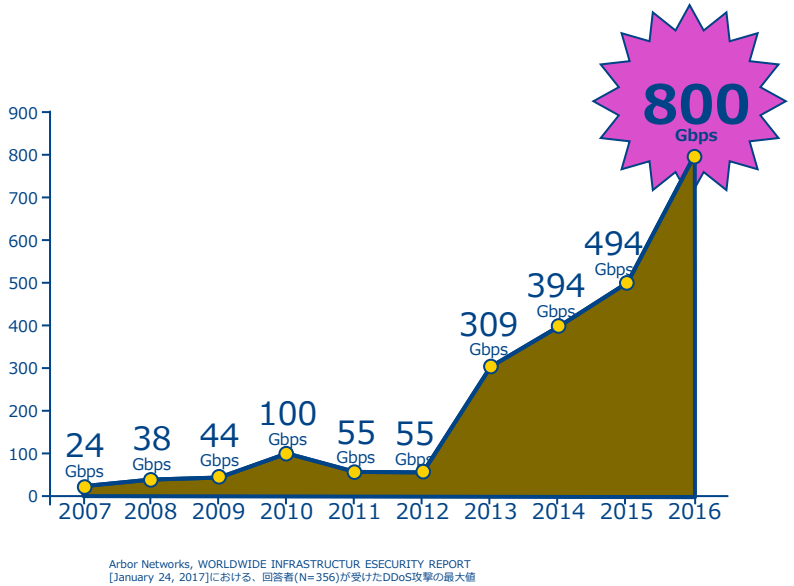
DDoS攻撃のリスクの顕在化

・84%の事業者で、DDoS攻撃をすでに経験



<出展>Arbor Networks

拡大するDDoS攻撃の規模

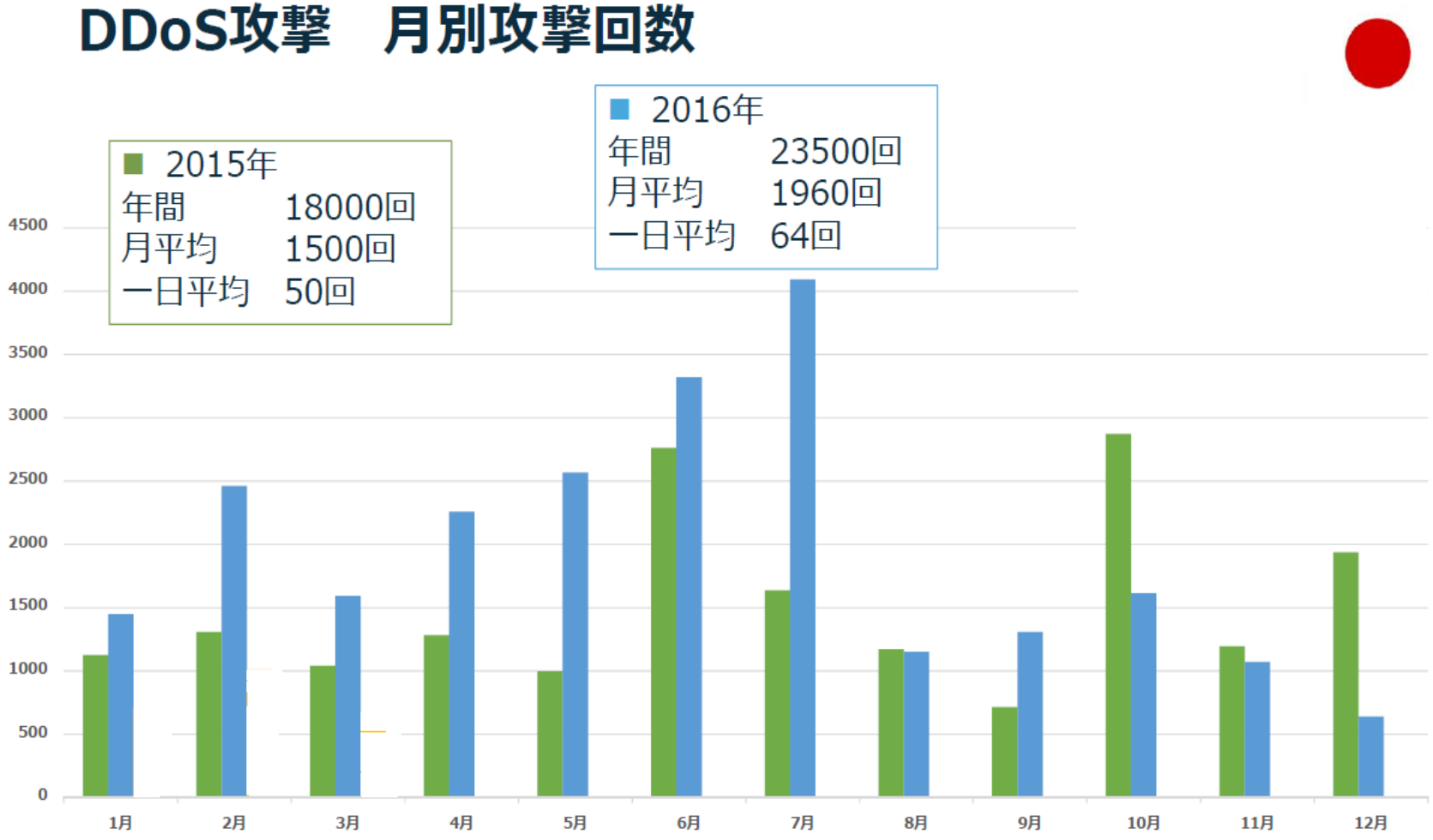


Arbor Networks, WORLDWIDE INFRASTRUCTUR ESECURITY REPORT
[January 24, 2017]における、回答者(N=356)が受けたDDoS攻撃の最大値

- DDoSの攻撃規模も年々拡大
サーバダウンだけでなく、**ネットワークの利用不能**を目的とした攻撃も増加

（参考）DDoS攻撃の現状（日本）

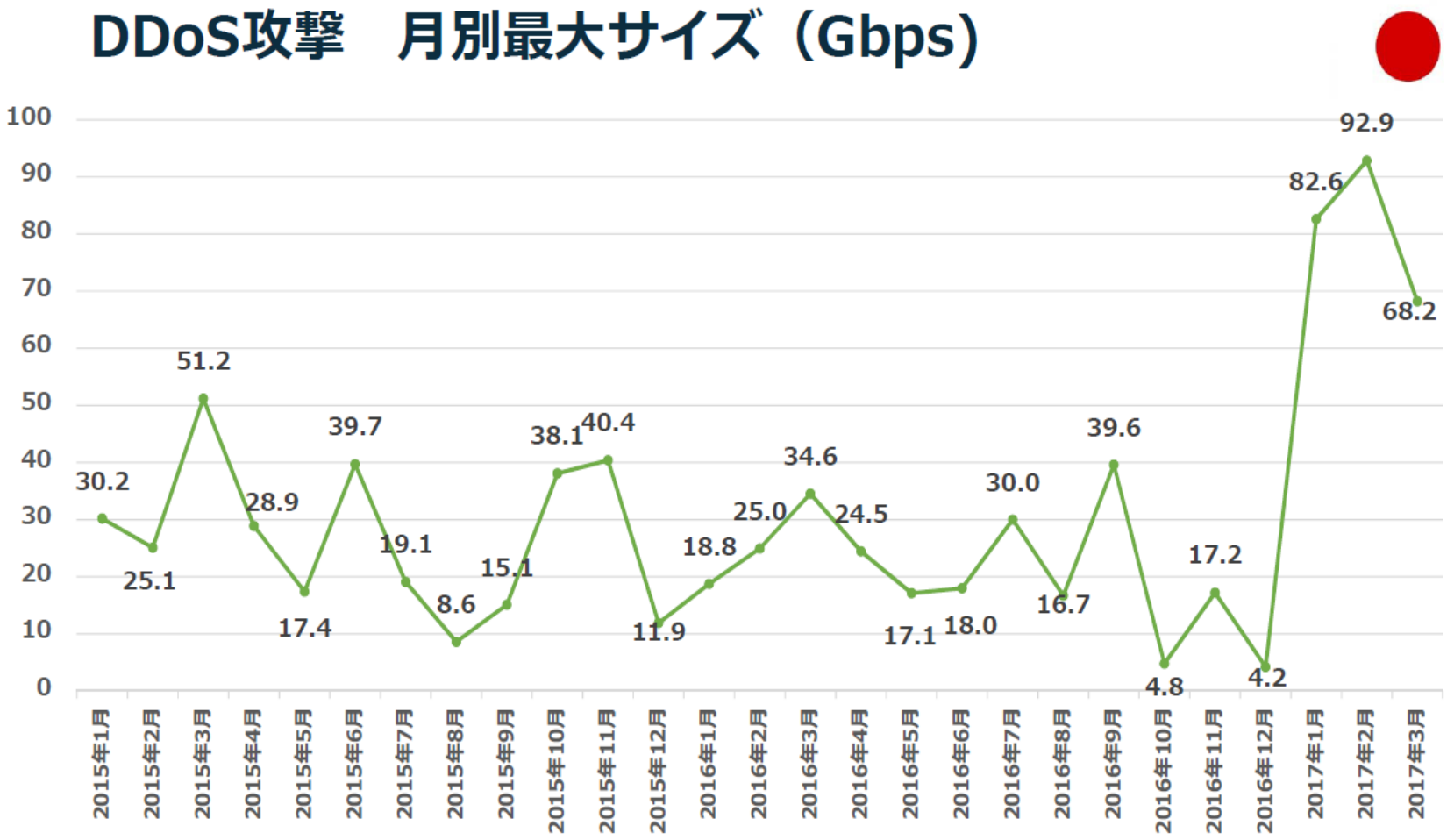
DDoS攻撃　月別攻撃回数



ARBOR NETWORKS

© Arbor Networks 2016

（参考）DDoS攻撃の現状（日本）



ARBOR NETWORKS

Agenda

第一部：マルチホームのお客様向けDDoS対策ソリューションのご紹介

1．最近のDDoS攻撃を中心としたトピック

2．DDoS攻撃およびDDoS対策手法

3．マルチホームDDoS対策ソリューションのご紹介

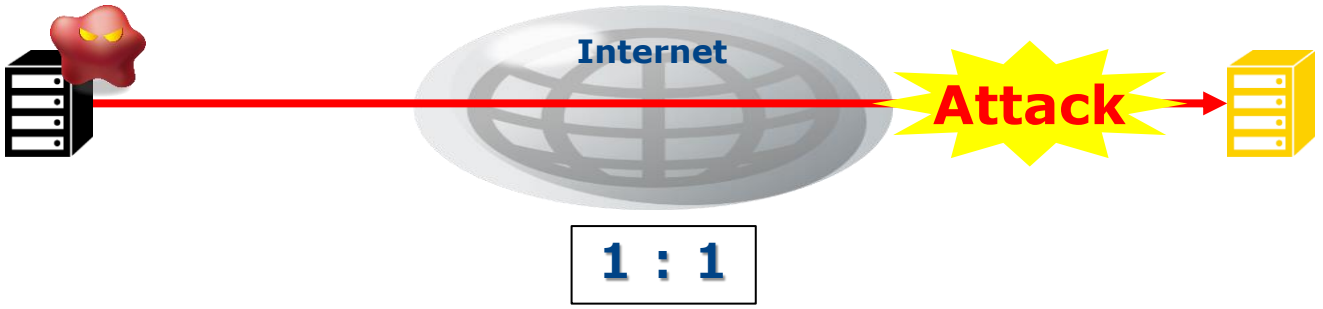
第二部：トランジット＋IX接続のお客様向けソリューションのご紹介

4．マルチホームのお客様の現状＆課題

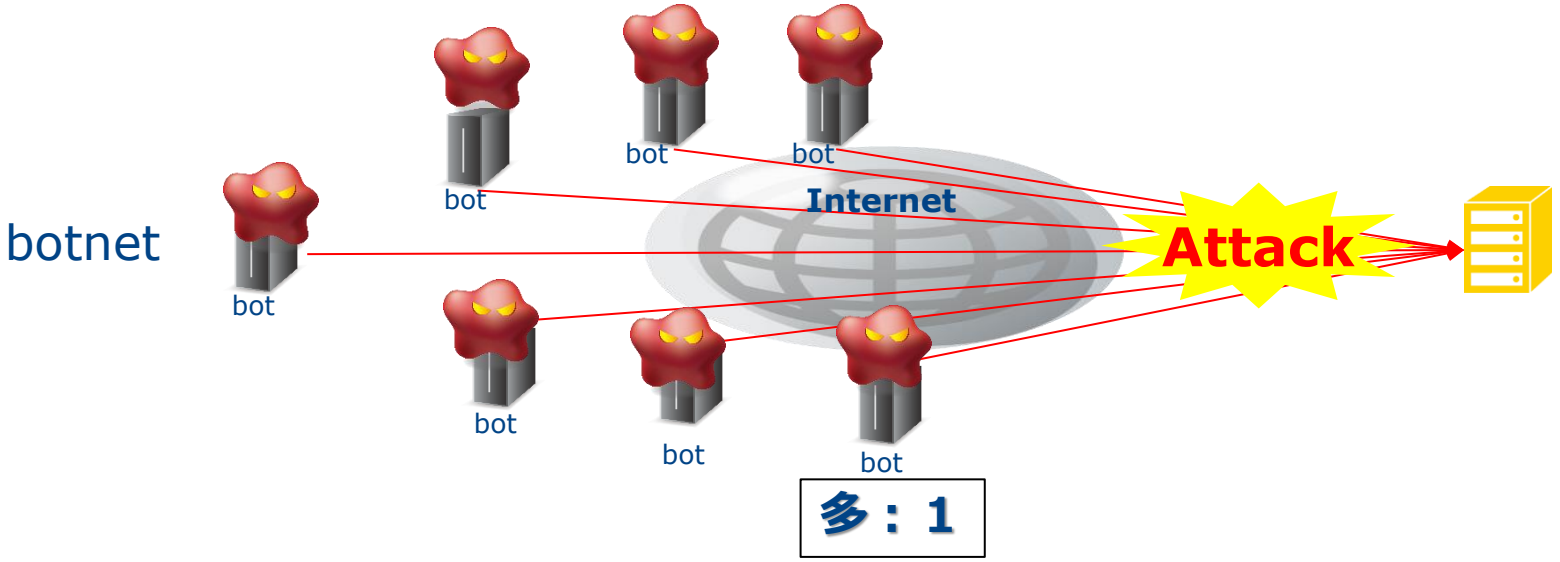
5．JPNAP接続ソリューションのご紹介

DoS/DDoS攻撃とは

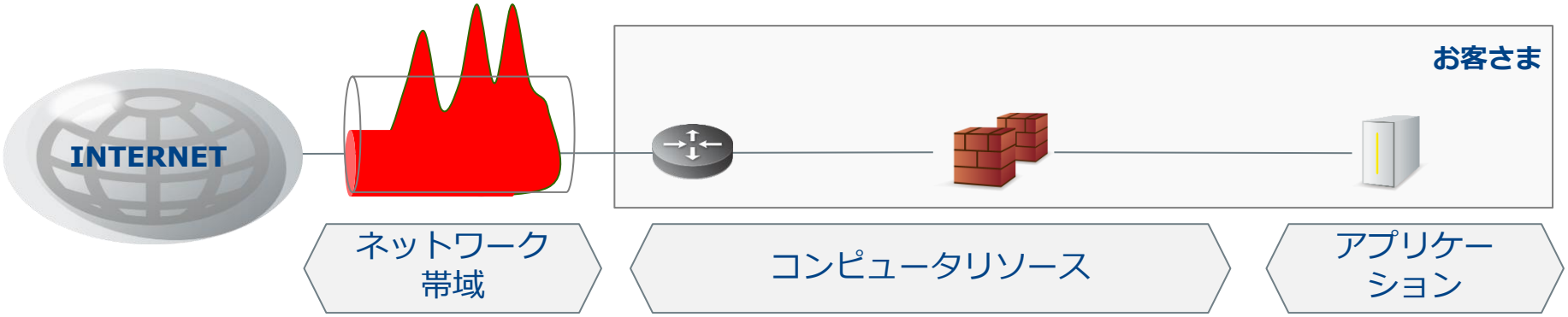
- DoS（Denial of Service）攻撃



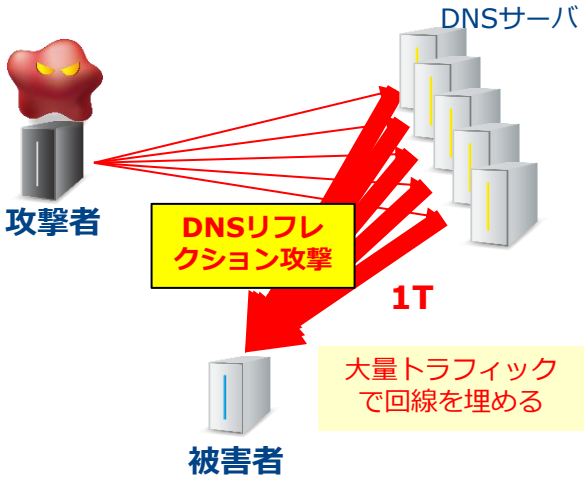
- DDoS(Distributed Denial of Service）攻撃



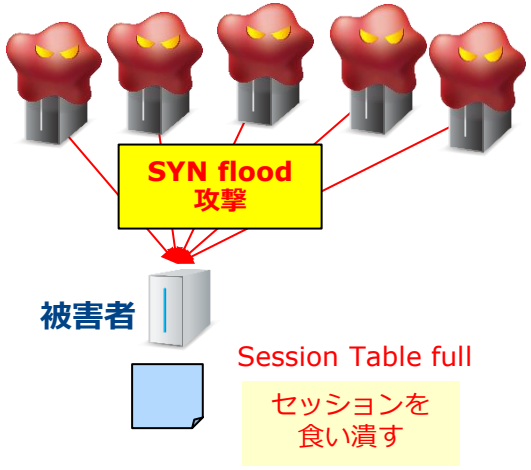
DoS/DDoSの攻撃の種類



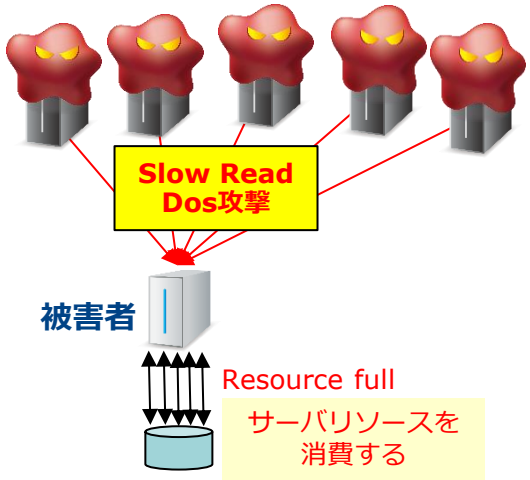
量的攻撃



不正セッション攻撃



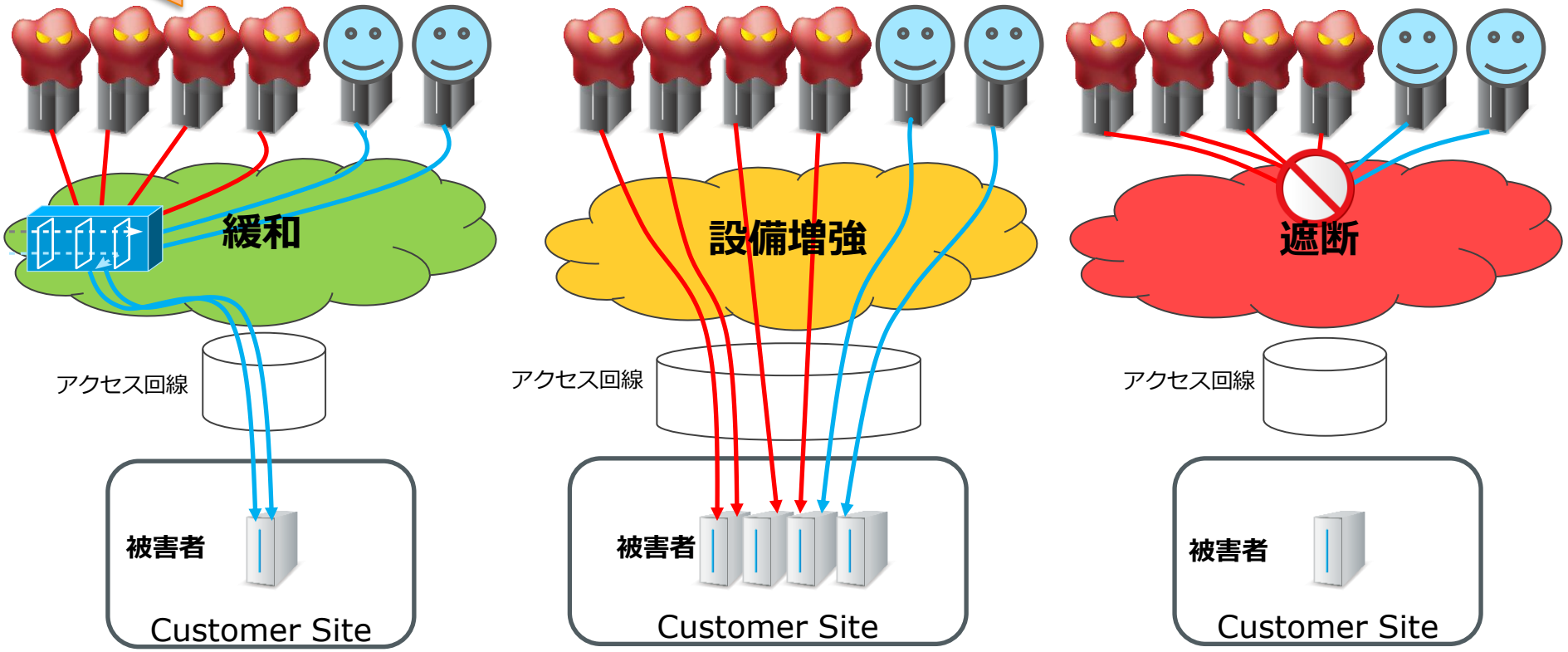
アプリケーションレイヤ攻撃



DDoS攻撃の対策方法

- 緩和　　攻撃のみ遮断、正常通信は通す
- 設備増強　　通信はできるが、攻撃も受け続ける
- 遮断　　正常通信も含めて通信が止まる

より、インテリジェンスな防御



Agenda

第一部：マルチホームのお客様向けDDoS対策ソリューションのご紹介

1．最近のDDoS攻撃を中心としたトピック

2．DDoS攻撃およびDDoS対策手法

3．マルチホームDDoS対策ソリューションのご紹介

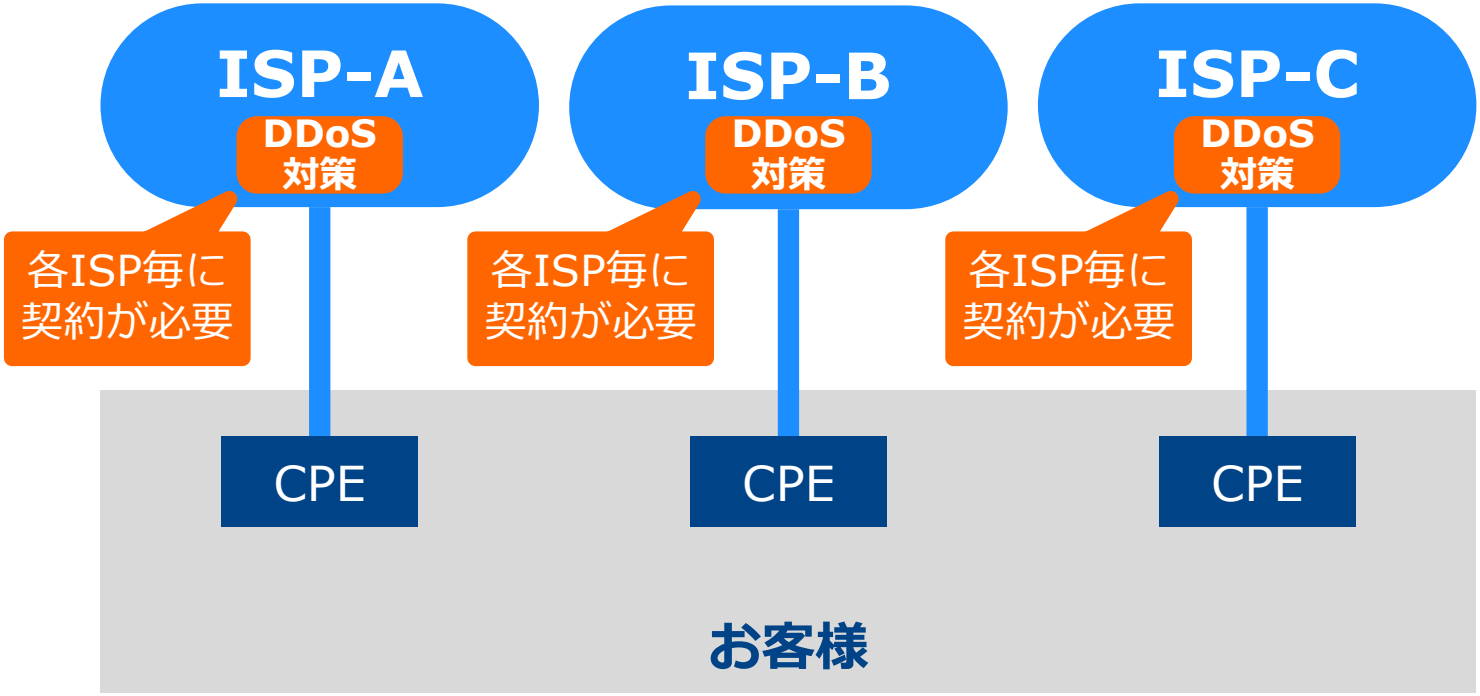
第二部：トランジット＋IX接続のお客様向けソリューションのご紹介

4．マルチホームのお客様の現状＆課題

5．JPNAP接続ソリューションのご紹介

マルチホームでのDDoS対策課題

1．各ISPで提供しているDDoS対策は対策ポリシーがバラバラで運用・管理が大変
2．お客さまが接続しているISP全てにDDoS対策を契約しないといけないため、非常にコストがかかる
3．複数のISPとのDDoS対策の契約をする必要があり、契約の手間や更新などが大変

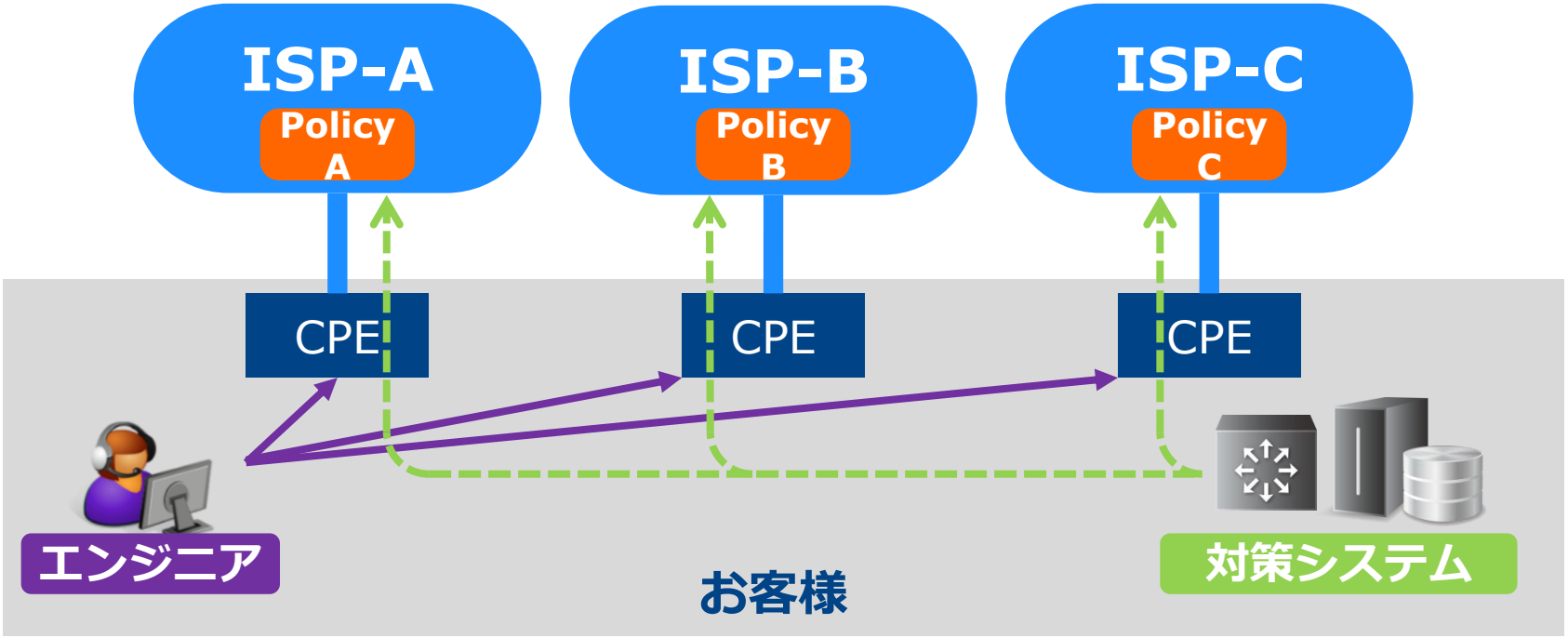


潜在的な問題

マルチホームDDoS対策を行う際の潜在的な問題

1．複数の対策ポリシーでの運用することで高スキルエンジニアの確保が必要。また、いつDDoS攻撃が発生するか分からないため、休日・夜間を含めた24時間365日でのエンジニア体制が必要。

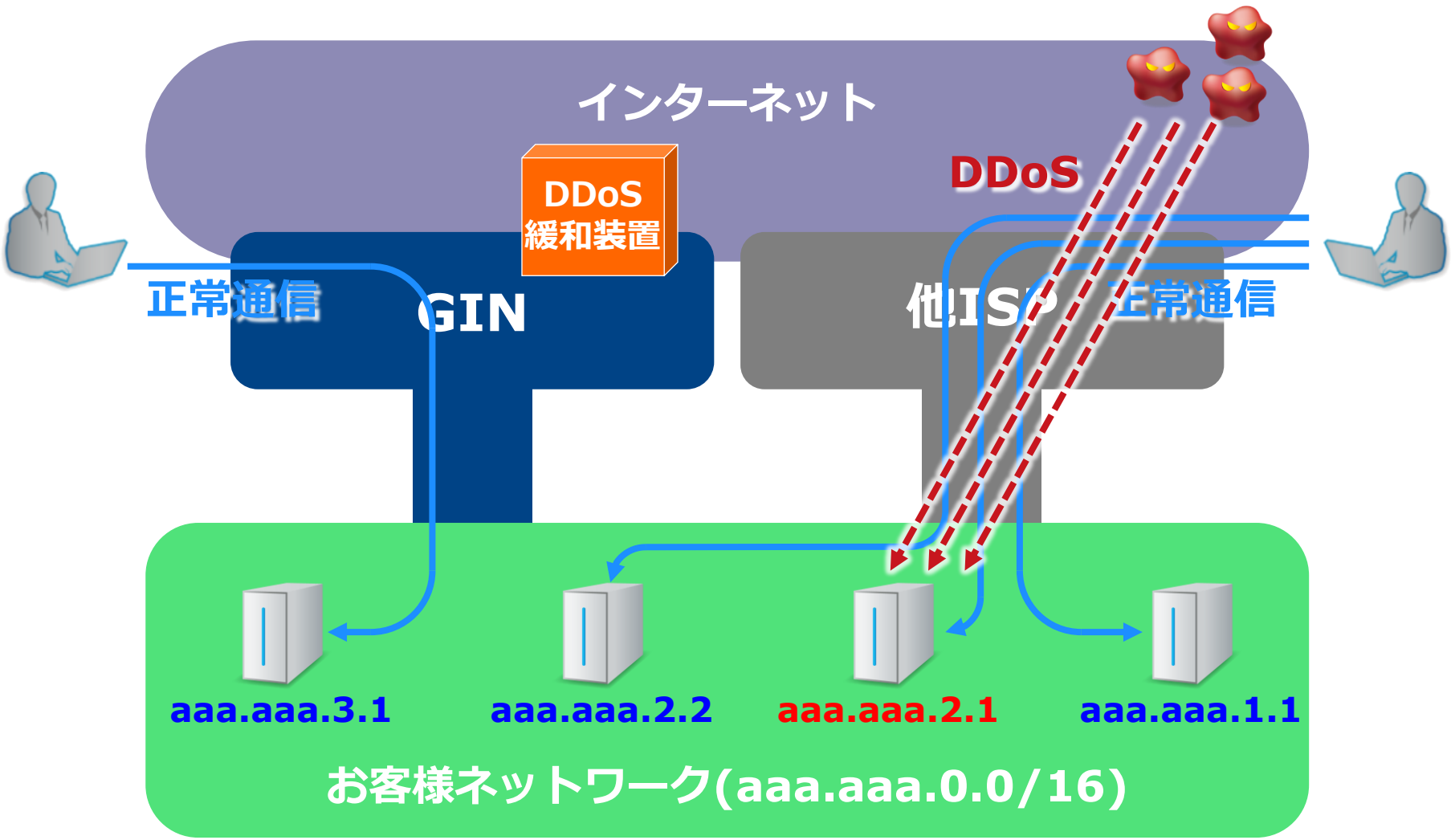
2．運用やエンジニアの稼働削減をさせるのに、設備や仕組みが必要。



マルチホームDDoS対策ソリューション

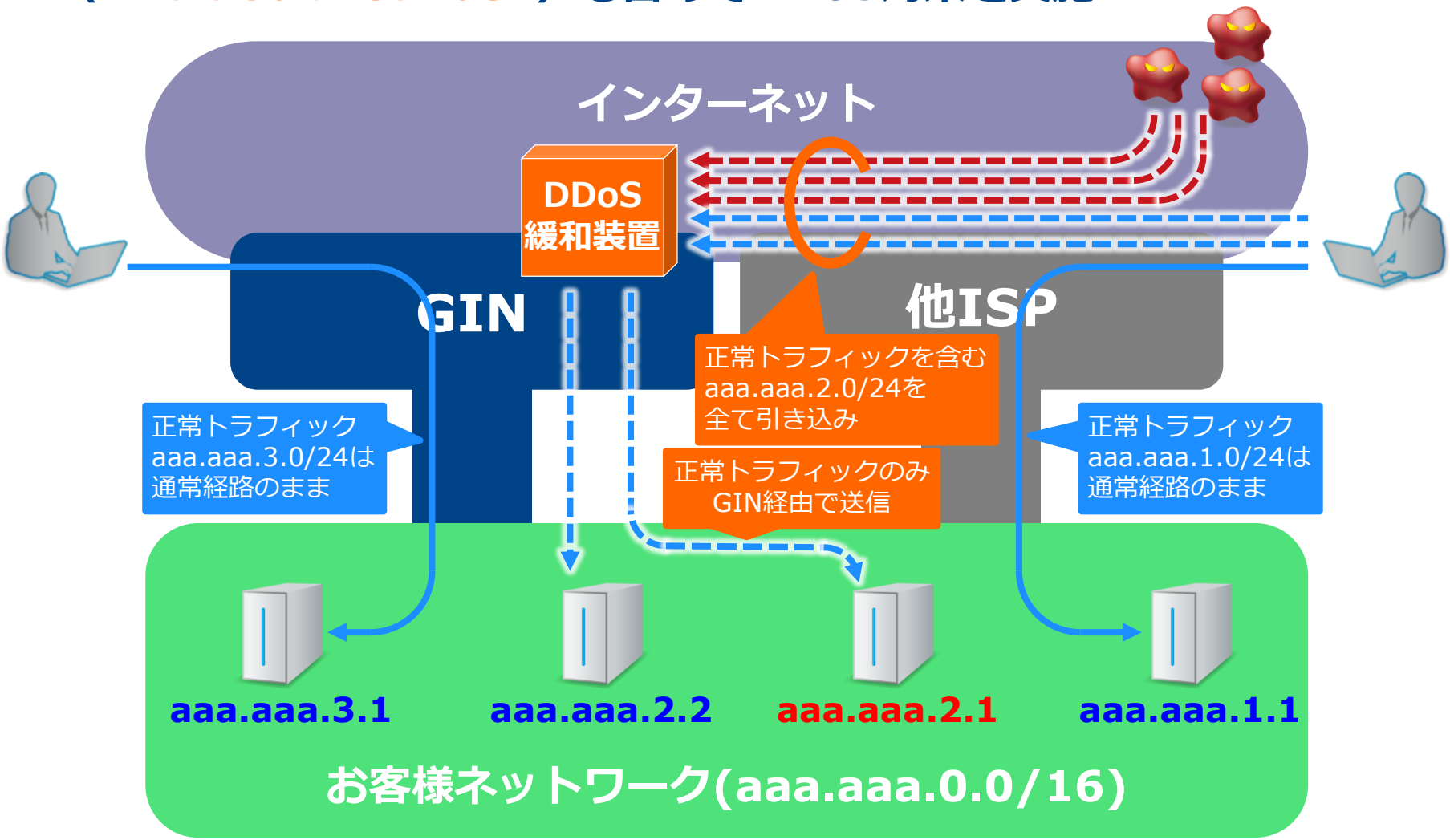
マルチホーム構成でDDoS対策（GINのみでDDoS対策）

DDoS対策を行っていない他ISPでDDoSが発生し通常通信に影響



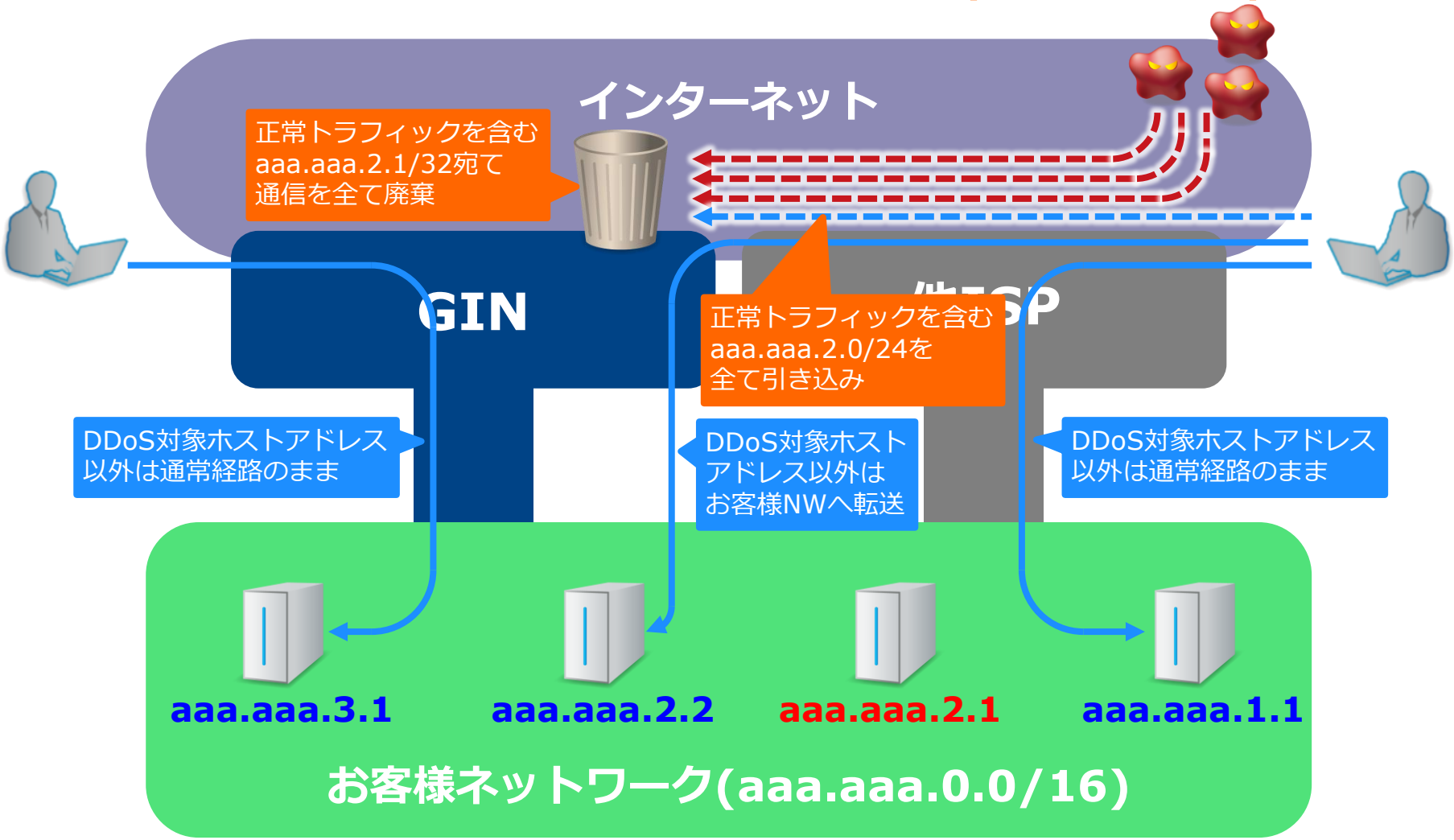
DDoS緩和機能イメージ

他ISPトラフィック（インターネット上に広告可能な最少ブロック（24bit Subnetmask）も含めてDDoS対策を実施

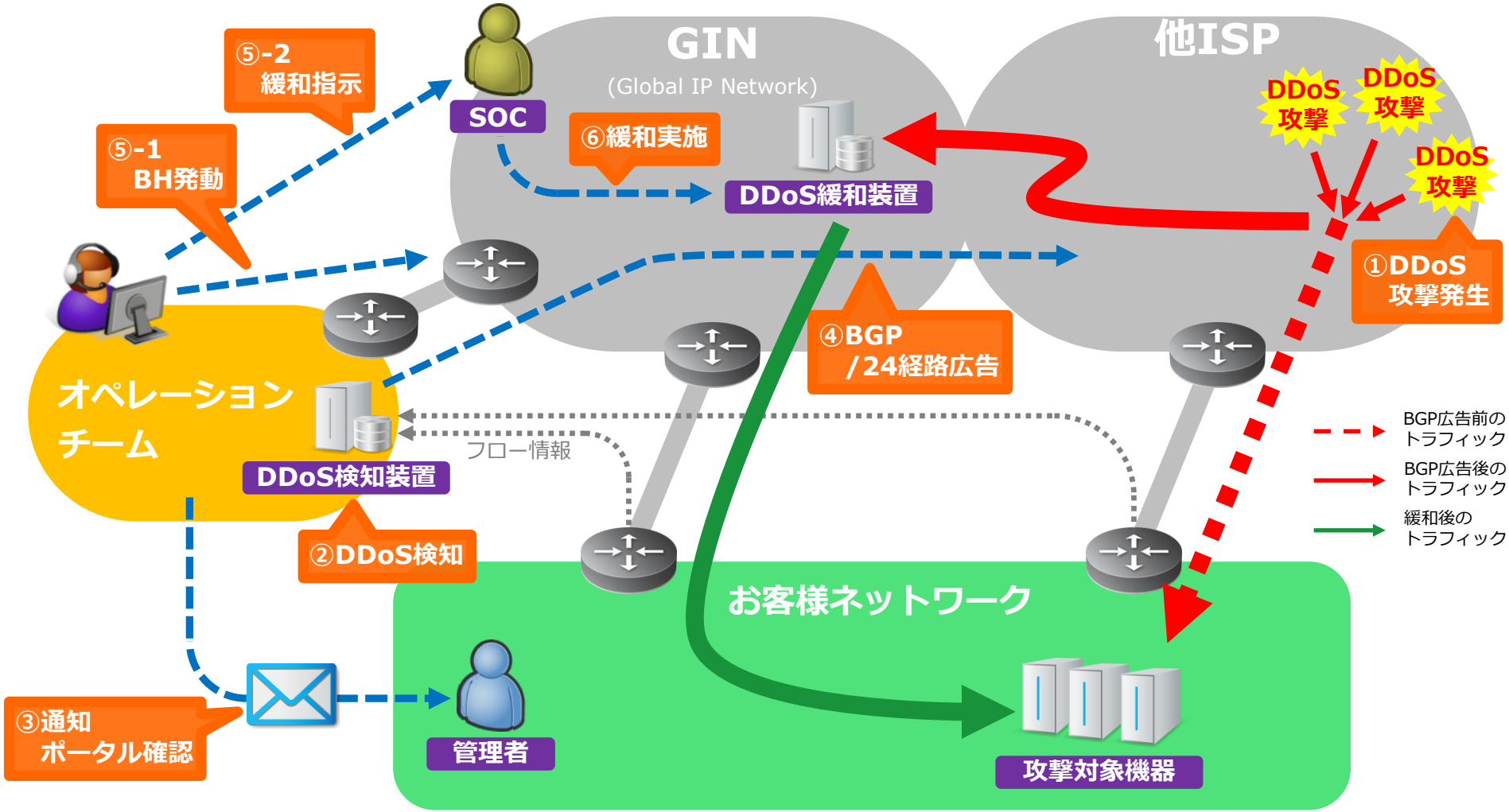


ブラックホール機能イメージ

他ISPトラフィックも含めて、ネットワーク単位（24bit mask）で
トラフィックを引き込んで、ホストアドレス単位（32bit mask）全て廃棄



ソリューションの動作



ソリューションの特徴

1．複数のISPをまとめて対策！！
- 他社回線も含めた１つの運用ポリシーにてDDoS対策が可能。
- ISP毎のDDoS対策が不要となり、コスト削減が可能。

2．DDoS対策の専門部隊にアウトソーシング！！
- 24時間365日体制でオペレーションをアウトソーシング可能。
- 経験豊富なDDoS対策スペシャリストが対応することで弊社のネットワークと同等な高いセキュリティレベルを実現。

3．設備投資不要！！
- 設備はNTTコミュニケーションズ側(全世界）に設置することでお客様の設備投資が不要。

Agenda

第一部：マルチホームのお客様向けDDoS対策ソリューションのご紹介

1．最近のDDoS攻撃を中心としたトピック

2．DDoS攻撃およびDDoS対策手法

3．マルチホームDDoS対策ソリューションのご紹介

第二部：トランジット＋IX接続のお客様向けソリューションのご紹介

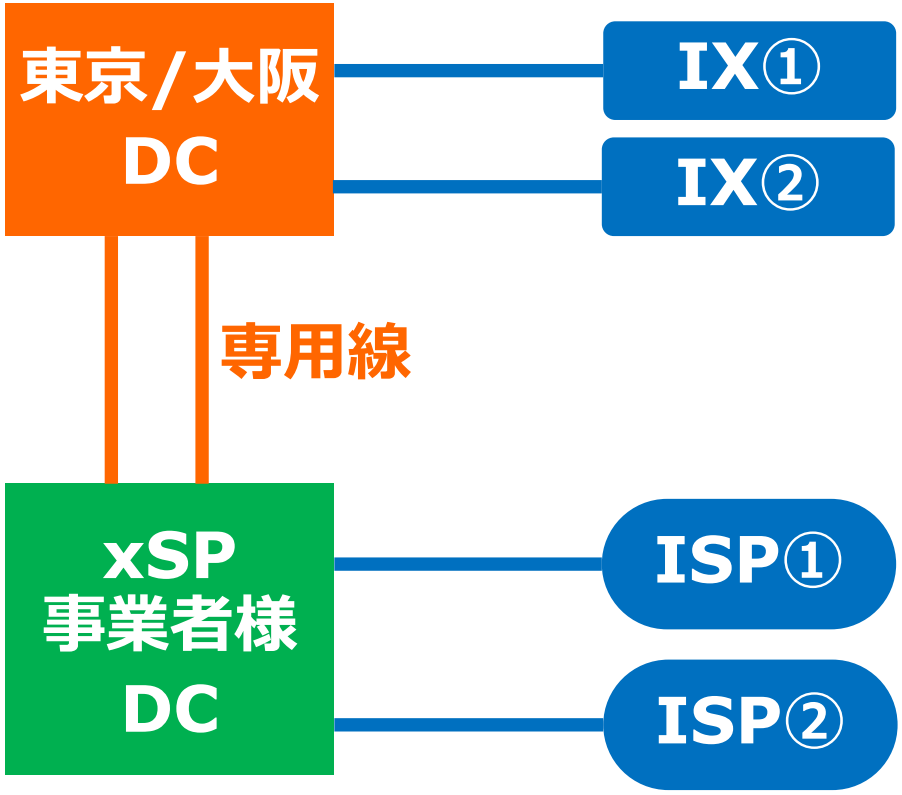
4．マルチホームのお客様の現状＆課題

5．JPNAP接続ソリューションのご紹介

マルチホームのお客様の現状

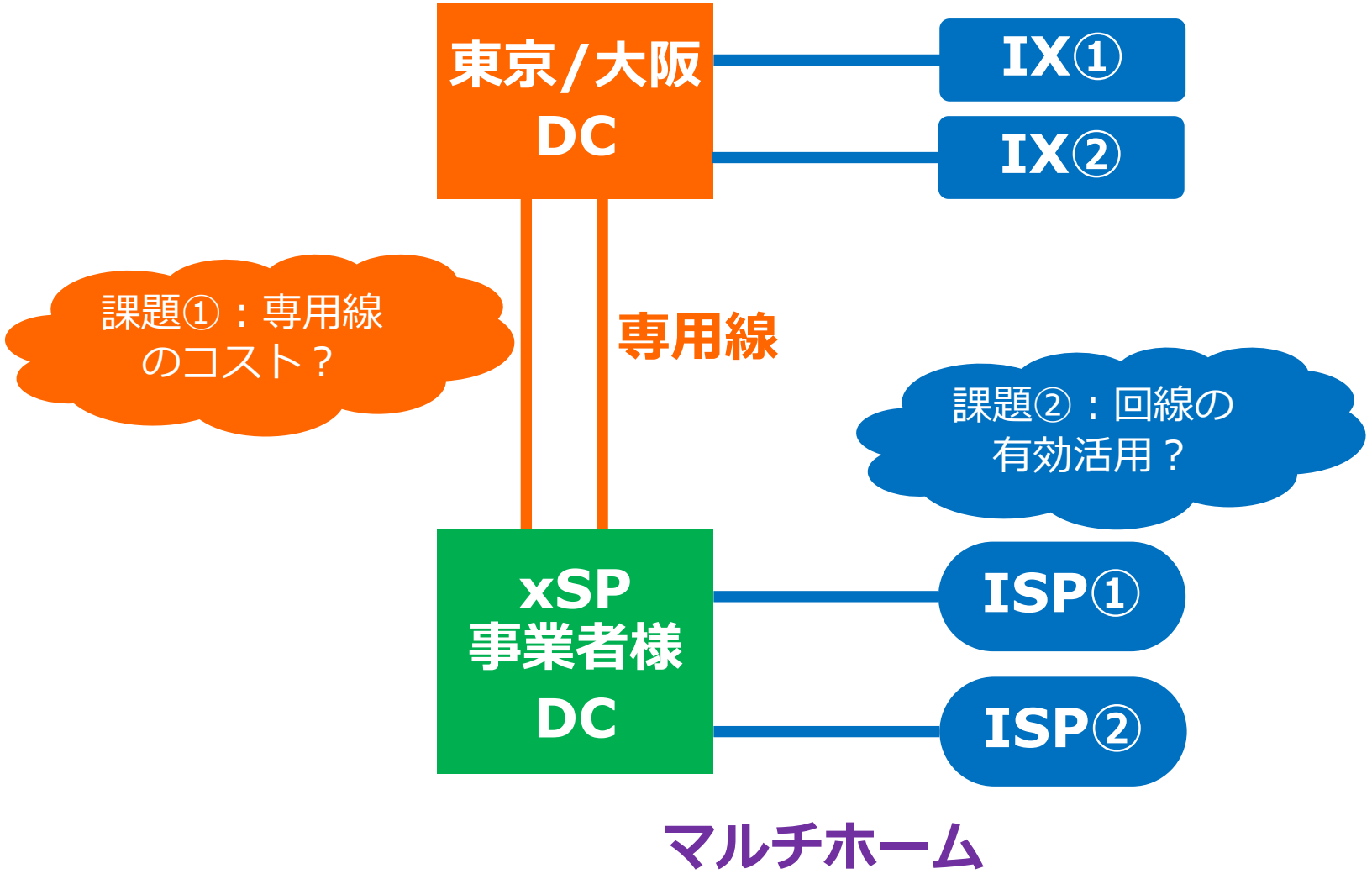
①トランジットは、ローカルで複数のISPと接続⇒マルチホーム構成

②OTTやxSPとはIX経由で接続　⇒　Peering



マルチホーム

マルチホームのお客様の課題



Agenda

第一部：マルチホームのお客様向けDDoS対策ソリューションのご紹介

1．最近のDDoS攻撃を中心としたトピック

2．DDoS攻撃およびDDoS対策手法

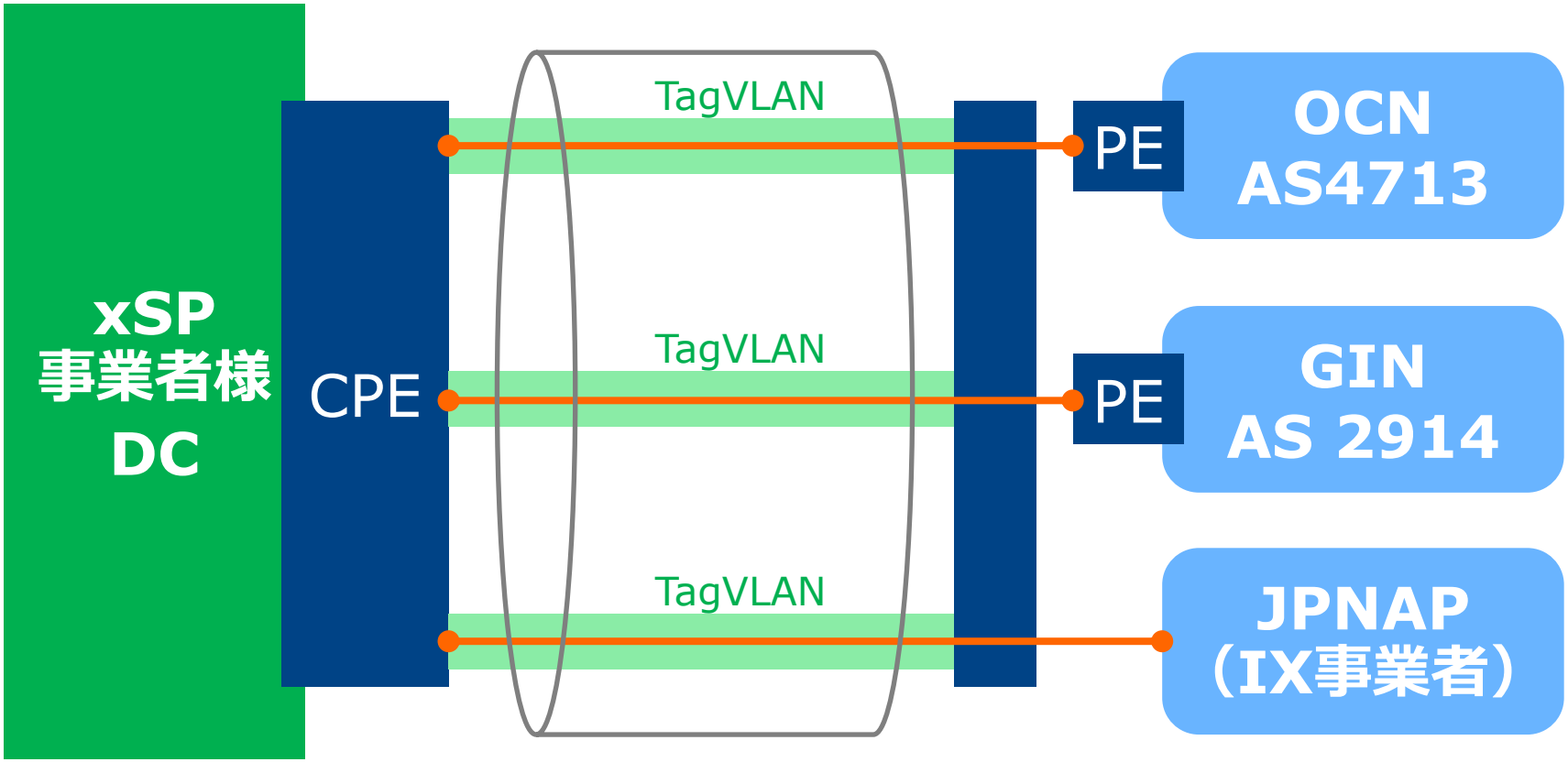
3．マルチホームDDoS対策ソリューションのご紹介

第二部：トランジット＋IX接続のお客様向けソリューションのご紹介

4．マルチホームのお客様の現状＆課題

5．JPNAP接続ソリューションのご紹介

JPNAP接続ソリューションのご紹介



「ご清聴ありがとうございました」

お問い合わせは、
営業担当者または下記へご連絡ください
trahanki-ns@ntt.com