増え続けるDDoS攻撃に対抗するために事業者間で協力してできること(公開版)

JANOG38 Day1 BoF
2016年7月6日

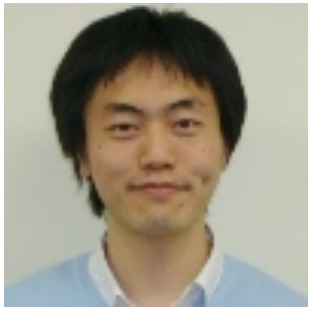
自己紹介

■ 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
- 大規模ISP保守運用サービス担当

■ 現在、研究開発部門にてDDoS対策ソリューション関連技術およびデータ解析技術開発とIETF提案活動に従事

■ 2015～ ISOC-JP プログラムチェア

【JANOG活動履歴】
- JANOG28 実行委員長
- JANOG30 会場運営委員長
- JANOG32 「HTTP 2.0のインパクト」登壇

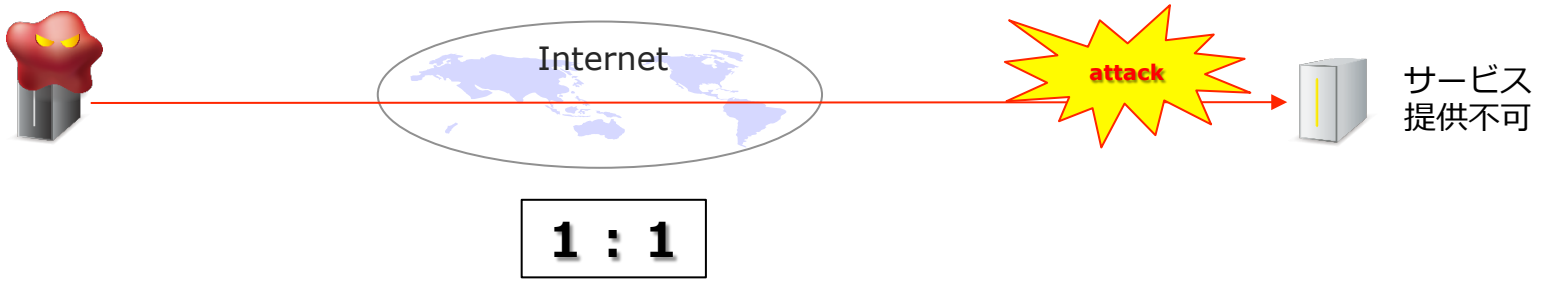


NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

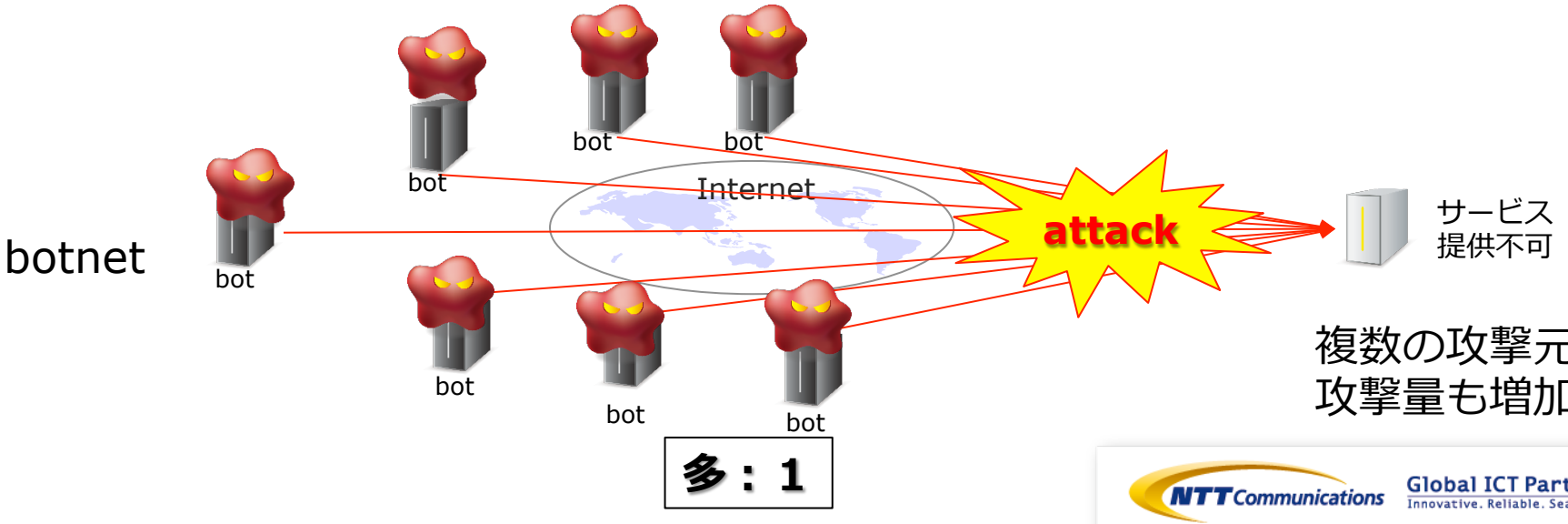
はじめに

DoS攻撃/DDoS攻撃

- DoS（Denial of Service）攻撃

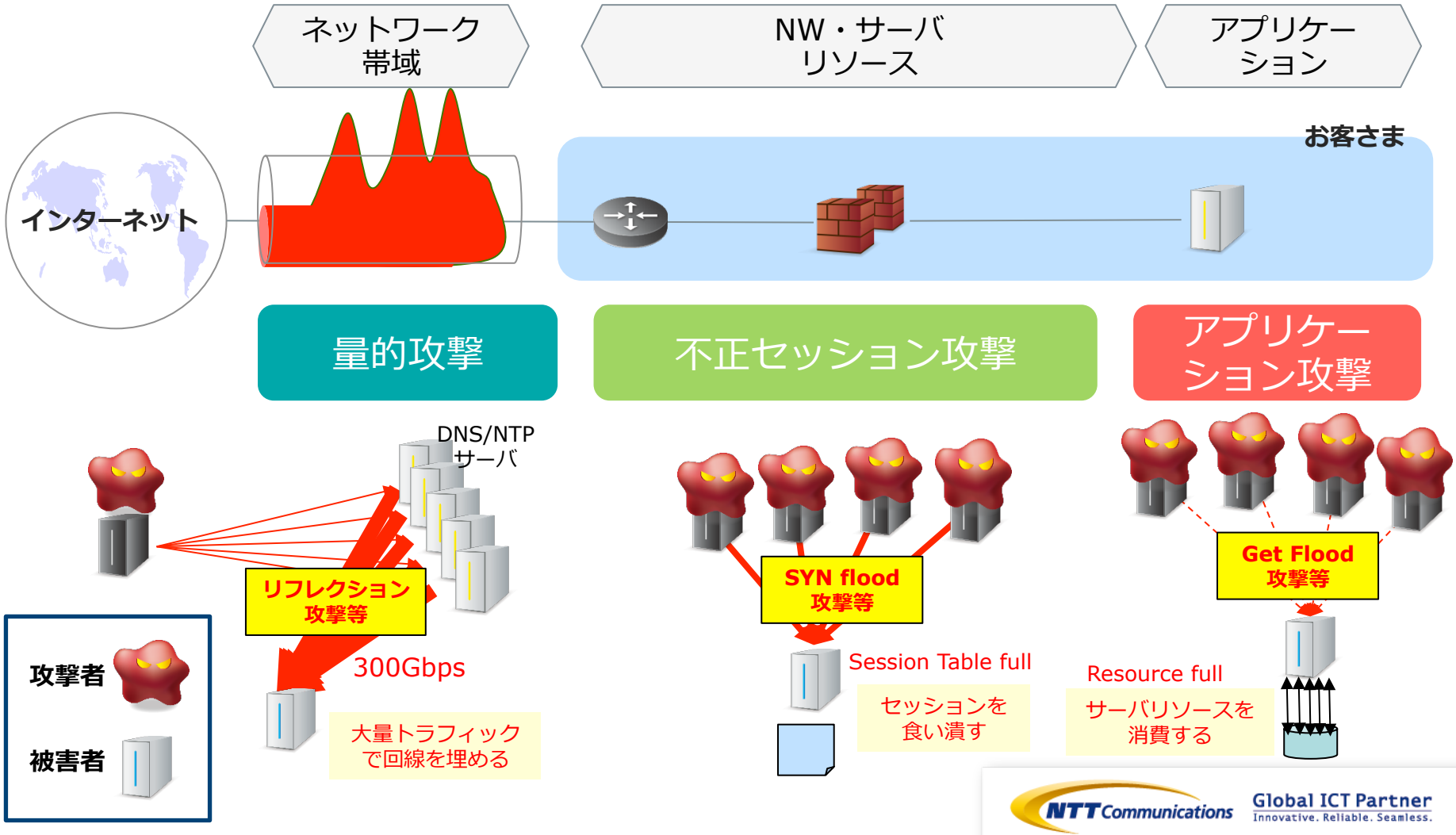


- DDoS(Distributed Denial of Service）攻撃



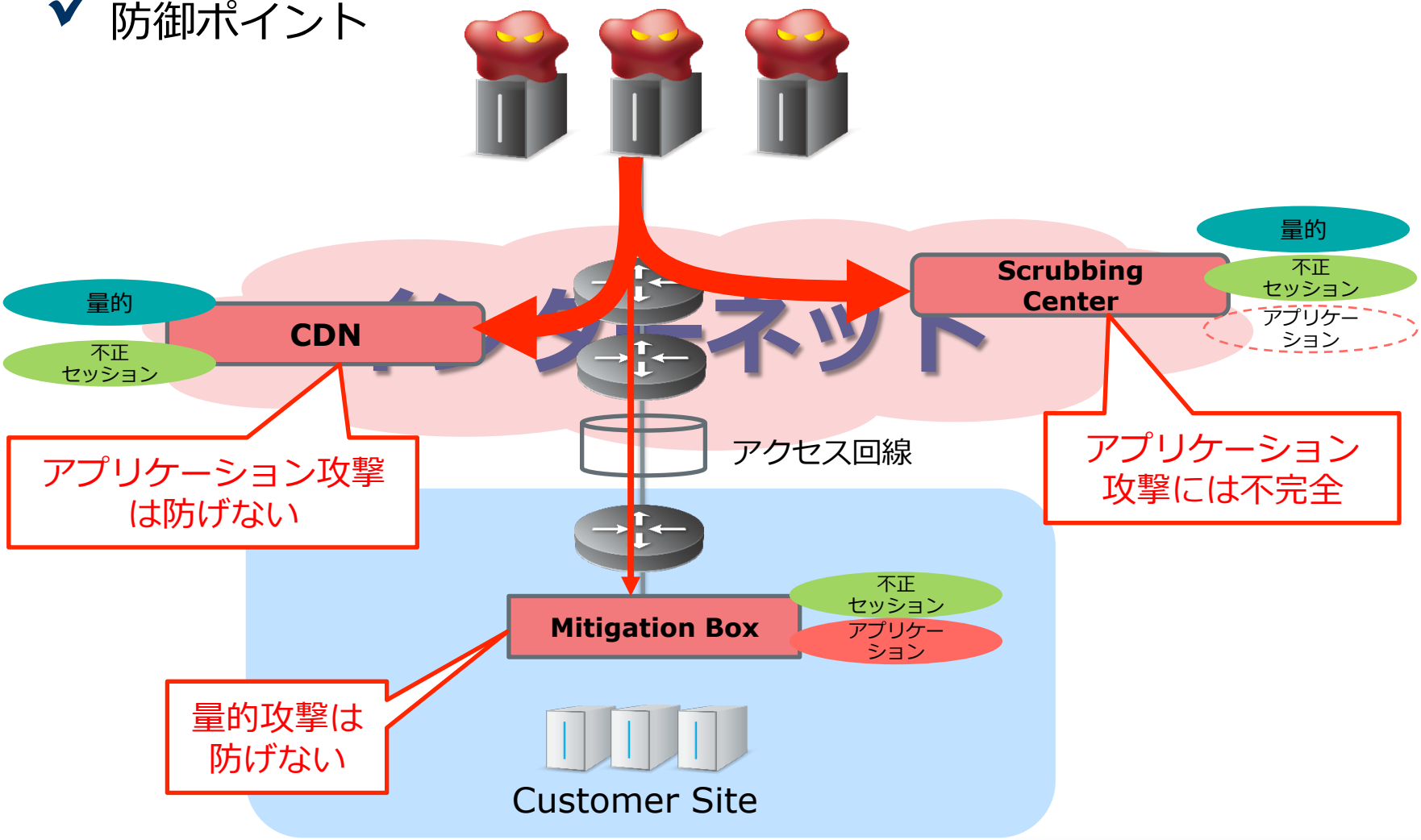
攻撃手法と影響

- 攻撃手法により、影響箇所は異なる



DDoS防御手法と効果

✓ 防御ポイント



大規模DDoS攻撃の事例

日時	継続時間	攻撃対象	影響内容
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」	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などの協力により、サービス復旧
2014年8月	数時間	PlayStation Network	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
2015年3月	6日間以上	Greatfire.org	2.6B/h（通常の2500倍）の接続要求が発生。サービス停止。
2015年3月	4日以上	Github	改竄された第三者Webサイトから2秒毎にGithubへ大量アクセスが発生。攻撃が繰り返され、都度対策を実施。
2015年5月	1時間	FXプライム by GMO	ネットバンキングに接続しつらい状況。金銭要求。
2015年6月	約2時間	セブン銀行	DD4BCから攻撃を受けダイレクトバンキングサービスの利用が困難に。ビットコインでの支払い要求あり。
2015年8月	約3時間	ゲーム「Dota2」の世界大会	賞金総額1800万ドルの世界大会「The International 2015」二日目にDDoS攻撃が発生。約3時間試合中止。
2016年1月	5日間以上	日産自動車	国際的ハッカー集団アノニマスによるDDoS攻撃により、Webサイトが全面停止(捕鯨への抗議のため)。

(公開情報からNTTコム調べ)

DDoS攻撃の傾向

DDoS攻撃対象

企業ネットワークにおける脅威として、Internet接続部の輻輳が1位

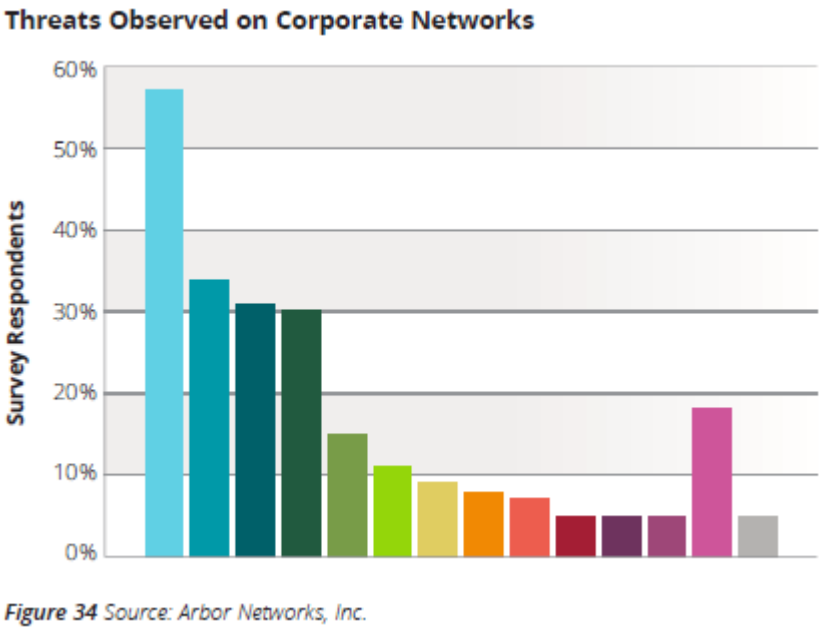
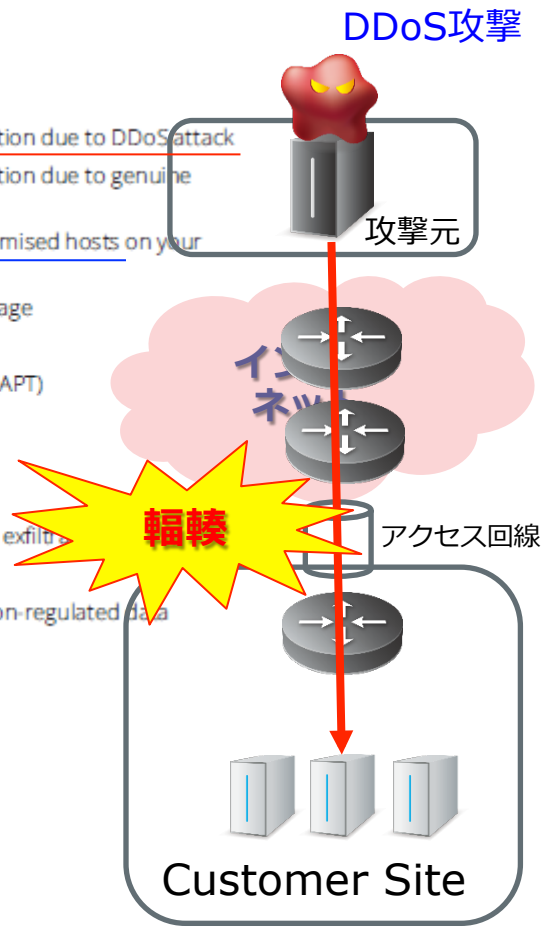


Figure 34 Source: Arbor Networks, Inc.

- **57%** Internet connectivity congestion due to DDoS attack
- **34%** Internet connectivity congestion due to genuine traffic growth/spike
- **31%** Botted or otherwise compromised hosts on your corporate network
- **30%** Accidental major service outage
- **15%** Accidental data loss
- **11%** Advanced persistent threat (APT)
- **9%** Theft
- **8%** Web defacement
- **7%** Malicious insider
- **5%** Industrial espionage or data exfiltration
- **5%** Exposure of regulated data
- **5%** Exposure of sensitive, but non-regulated data
- **18%** None of the above
- **5%** Other

※Worldwide Infrastructure Security Report 2016, Arbornetworks
based on a survey comprised of 172 free-form and multiple choice questions



NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

DDoS攻撃手法の傾向　1/2

✓ 攻撃タイプ毎の割合

アクセス回線を埋めるため、上流ISPでの対策が必要

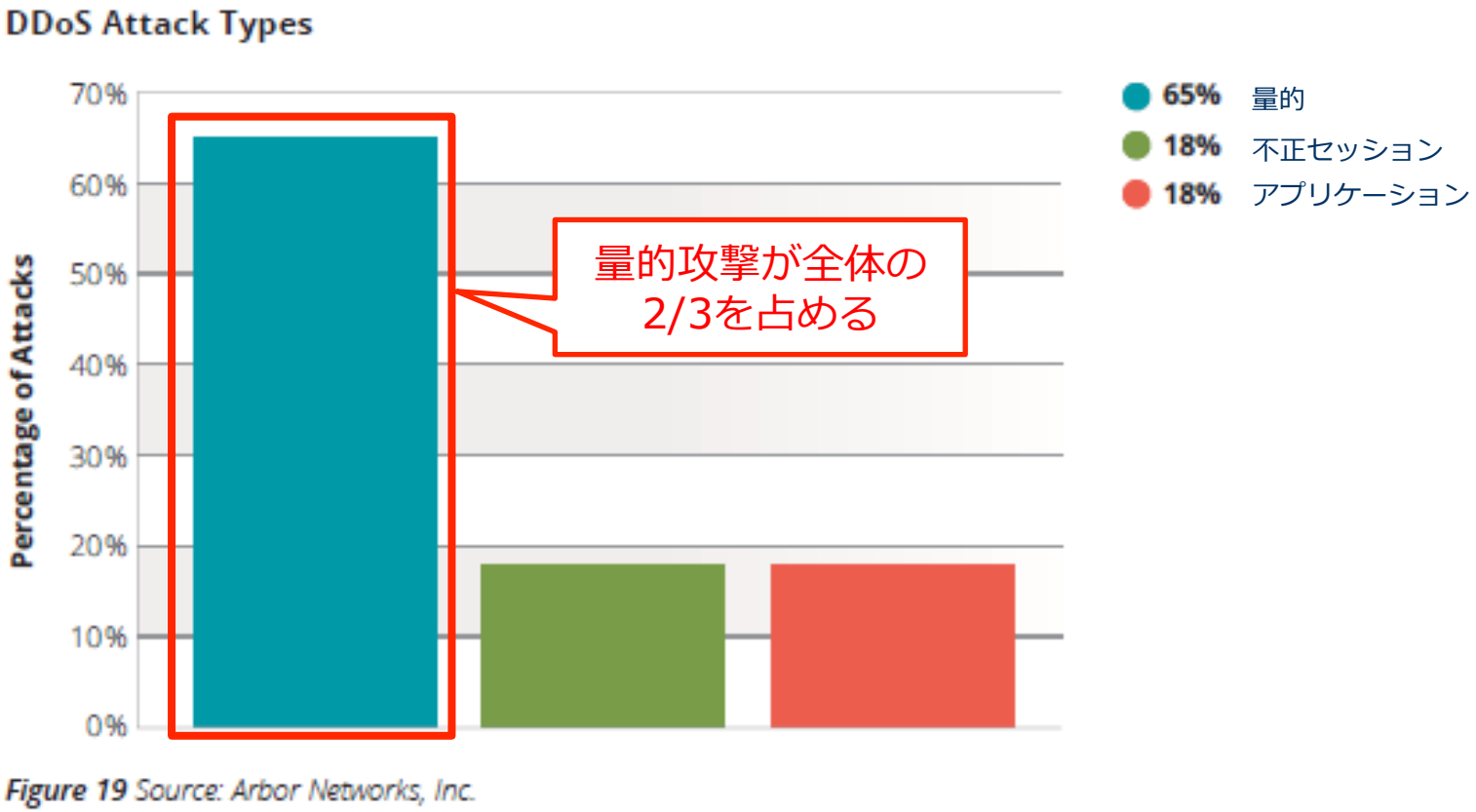


Figure 19 Source: Arbor Networks, Inc.

※Worldwide Infrastructure Security Report 2016, Arbornetworks
based on a survey comprised of 172 free-form and multiple choice questions

DDoS攻撃手法の傾向　2/2

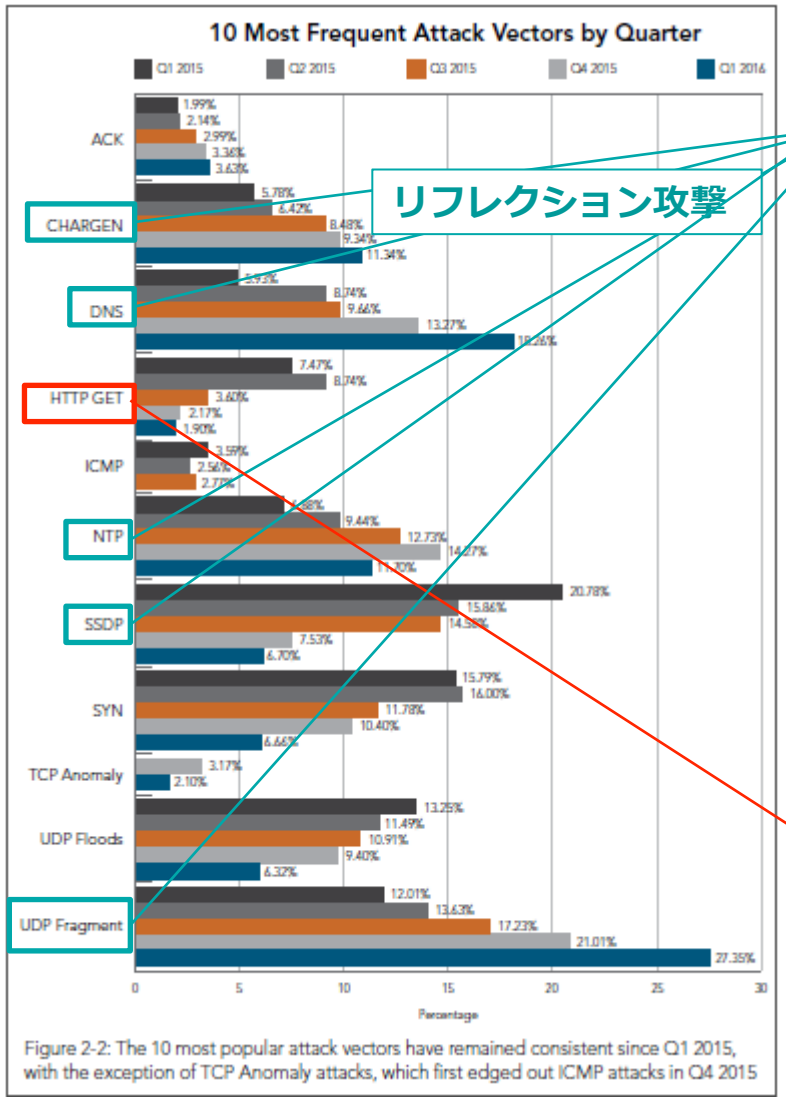


Figure 2-2: The 10 most popular attack vectors have remained consistent since Q1 2015, with the exception of TCP Anomaly attacks, which first edged out ICMP attacks in Q4 2015

※akamai's [state of the internet]/ security Q1 2016 report

よく用いられている攻撃手法

- 量的攻撃

CHARGET,DNS,NTP,SSDP等使われるプロトコル間での増減があるが、リフレクション攻撃は増加傾向にある

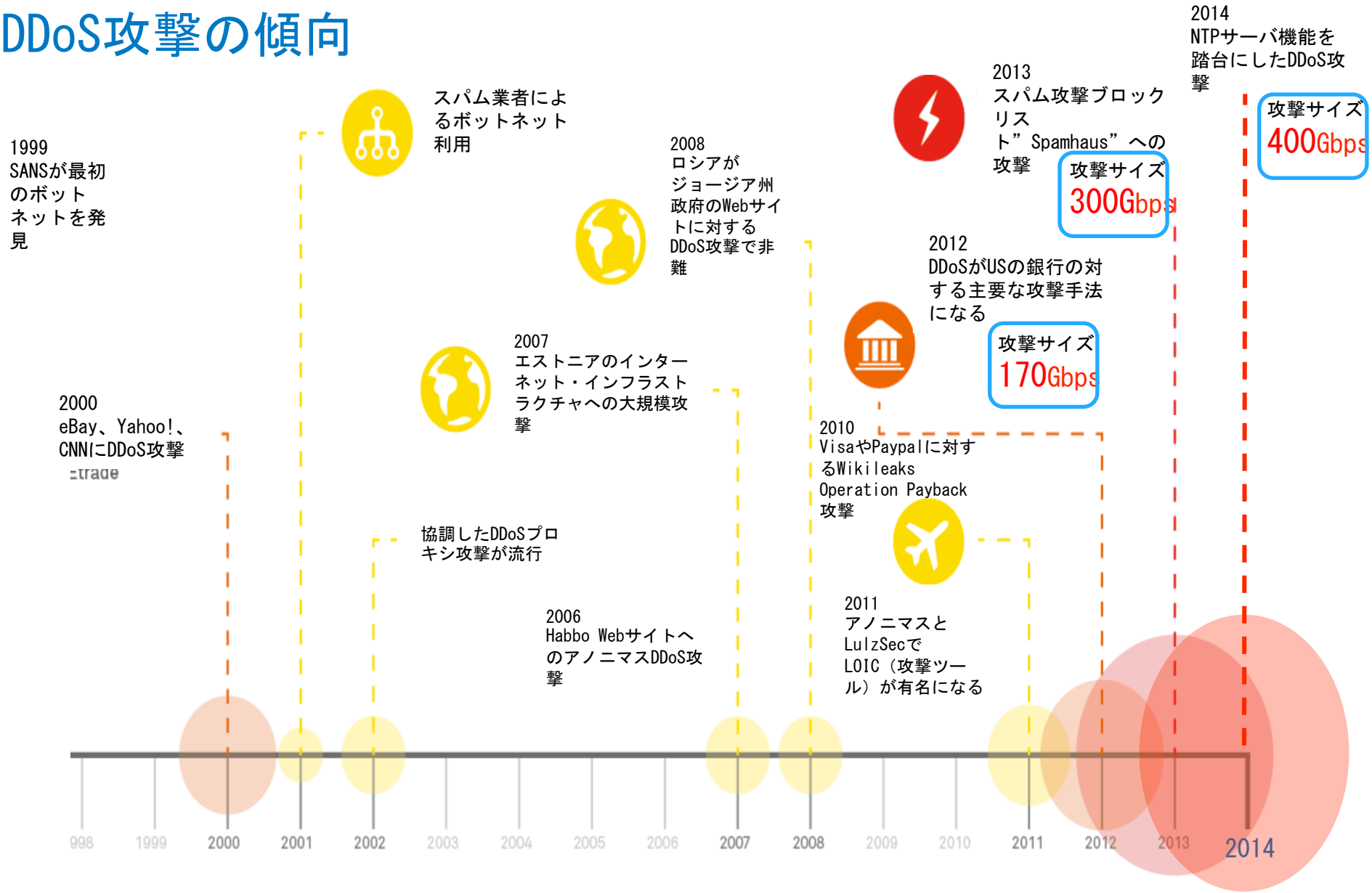
セキュリティ対策が弱い傾向にあるIoTデバイスの増加もリフレクション攻撃増加の一因

UDP fragmentがUDP Floodより多いが、UDPベースのDNS、CHARGENの攻撃による（ペイロードサイズが1500byte以上）と考えられる

- アプリケーションレイヤ攻撃

HTTP GETが引き続き主要な攻撃手法として利用されている

DDoS攻撃の傾向



より大容量化するDDoS攻撃：　最大400Gbps

マルチベクタ化するDDoS攻撃

- 攻撃者は、攻撃対象サーバをモニタリングし、攻撃の有効性を常時確認
- 攻撃対策によりサーバが復活すると、攻撃種類を変える
- 対策不能な攻撃が1種類でもあると、サーバのサービス不能状態が続く

DDoS攻撃の目的

・攻撃の理由は、恐喝が上位

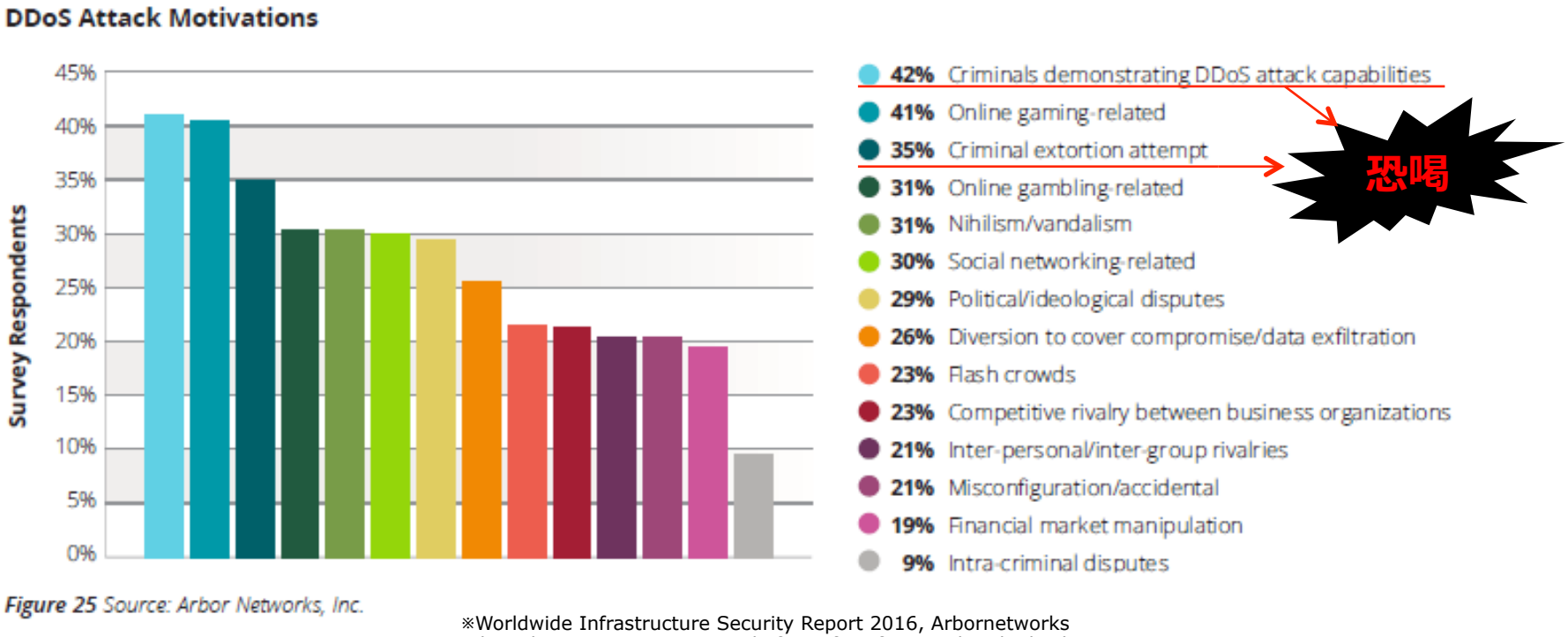
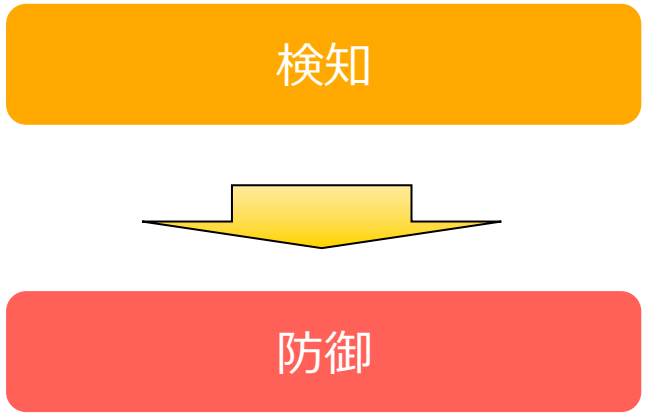


Figure 25 Source: Arbor Networks, Inc.

※Worldwide Infrastructure Security Report 2016, Arbornetworks
based on a survey comprised of 172 free-form and multiple choice questions

DDoS対策手法

DDoS対策



・フロー監視
・インライン監視
・サービス監視
・申告

・遮断
・設備増強
・緩和

・検知と防御でそれぞれの手法があり、どのように組み合わせるかが重要

DDoS検知方法

・Netflow、Firewall Log、SNMPが継続的に上位に位置
・DPIが増加し、SNMPと同率

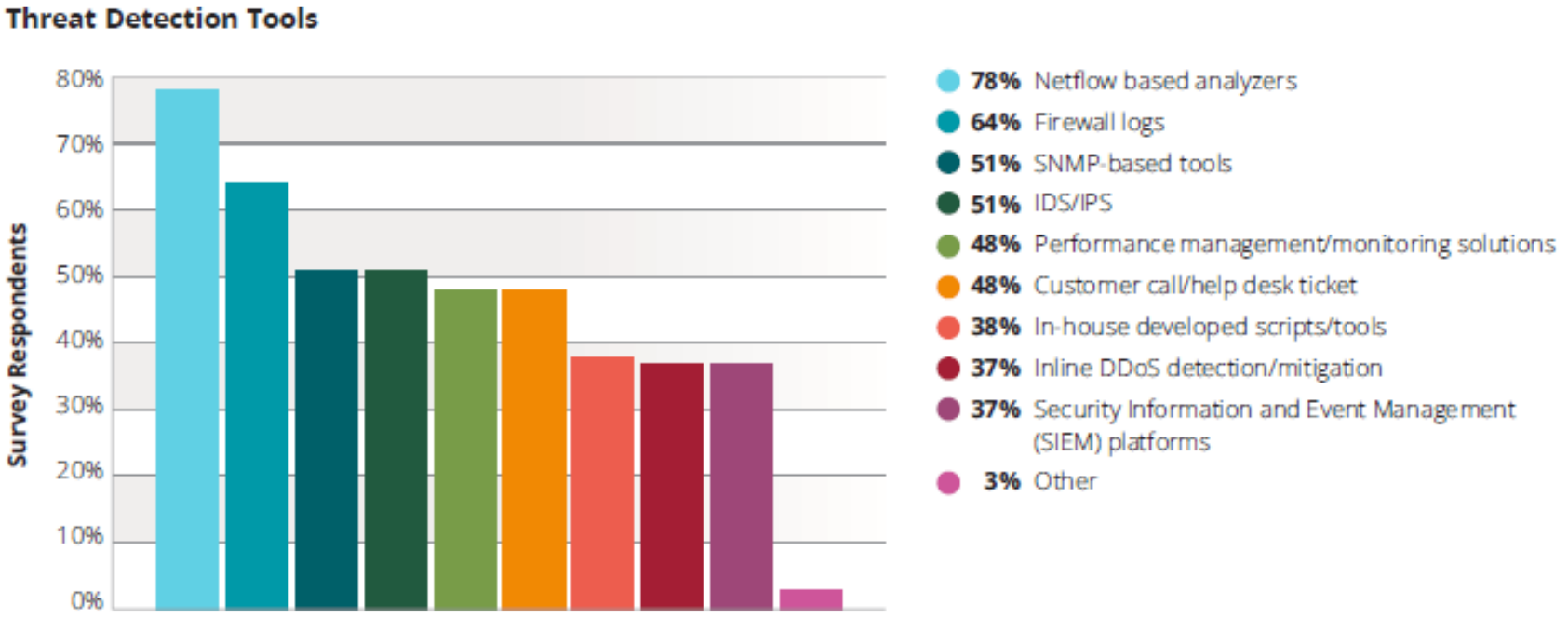
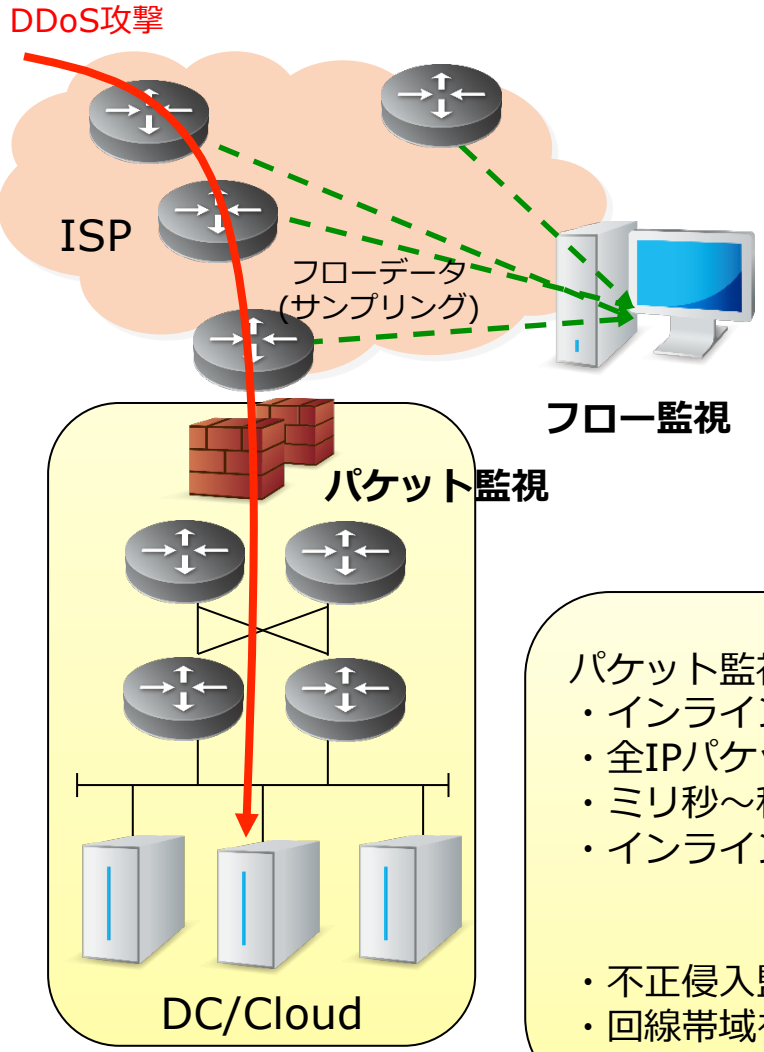


Figure 9 Source: Arbor Networks, Inc.

※Worldwide Infrastructure Security Report 2016, Arbornetworks
based on a survey comprised of 172 free-form and multiple choice questions

検知方法　フロー監視 vs パケット監視



フロー監視（Netflow/sFlow）
・ルータから受信したフローデータを用いて異常監視
・アウトラインに設置、網全体のトラフィックを集中監視
・フローデータは送受信IPアドレス、プロトコルなど
IPヘッダ内の情報

・不正侵入監視・ウイルス監視等には向かない
・大量トラフィックのDDoS攻撃を集中監視し、網全体の
分析・対策に有効

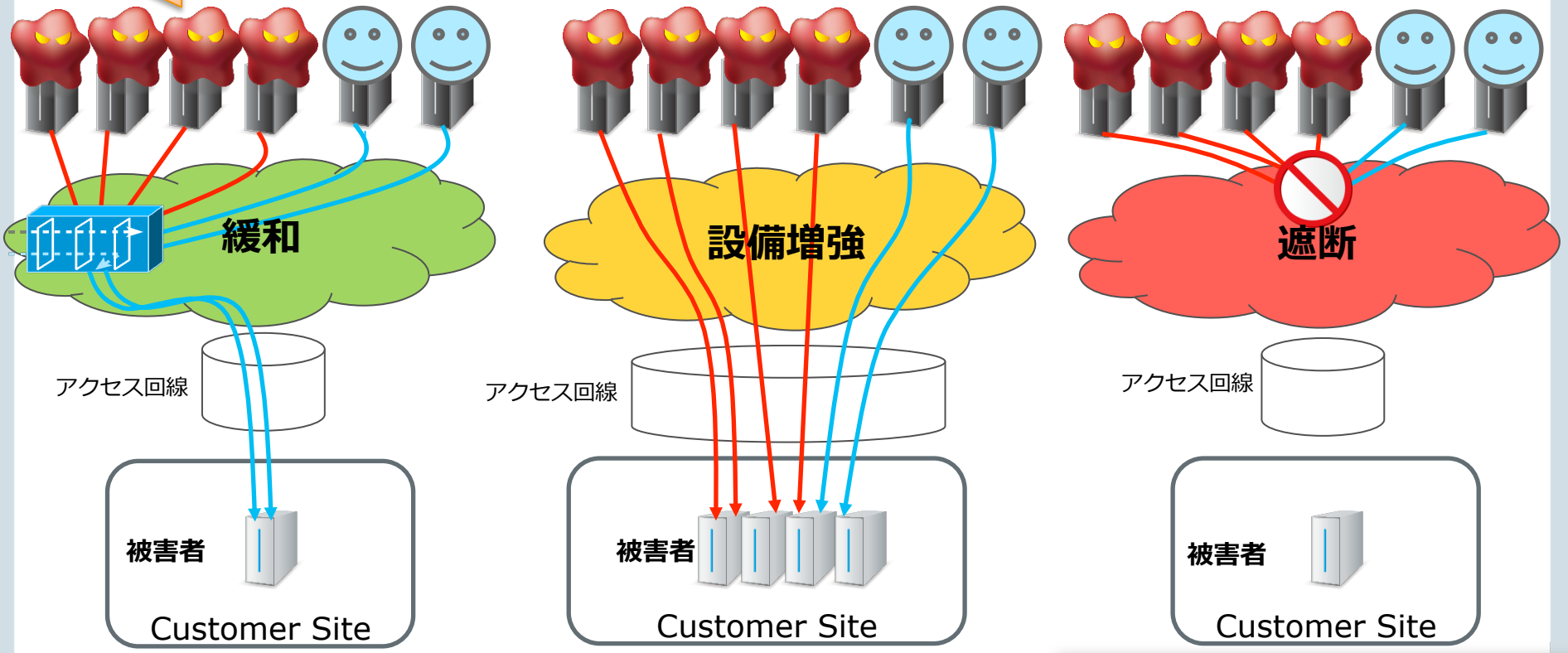
パケット監視（DPI）
・インラインに設置
・全IPパケットの内容(ペイロード)を見てウイルス等を監視
・ミリ秒～秒単位で検知・対策
・インラインなので、装置の信頼性が必要

・不正侵入監視、小規模DDoS攻撃、セッション占有攻撃監視に有効
・回線帯域を埋められる攻撃には対処不能、大規模攻撃で全断

防御方法の違い

- 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　　正常通信も含めて全ての通信が止まる

より、インテリジェンスな防御



正規ユーザに対するサーバの可用性を確保

DDoS防御方法

・DDoS Mitigation装置、ACL、Firewall、Blackhole Routingが中心
・増加が目立つ方法としてはBGPFlowSpec（9%→19%)

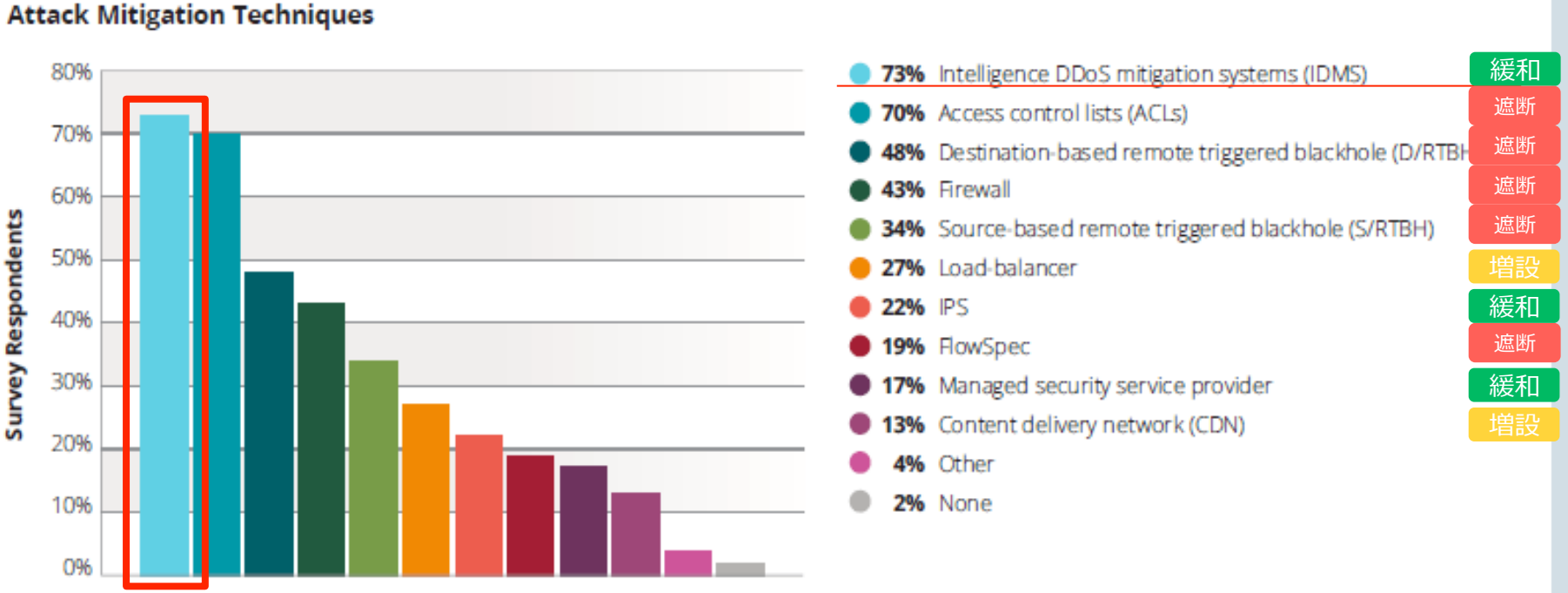
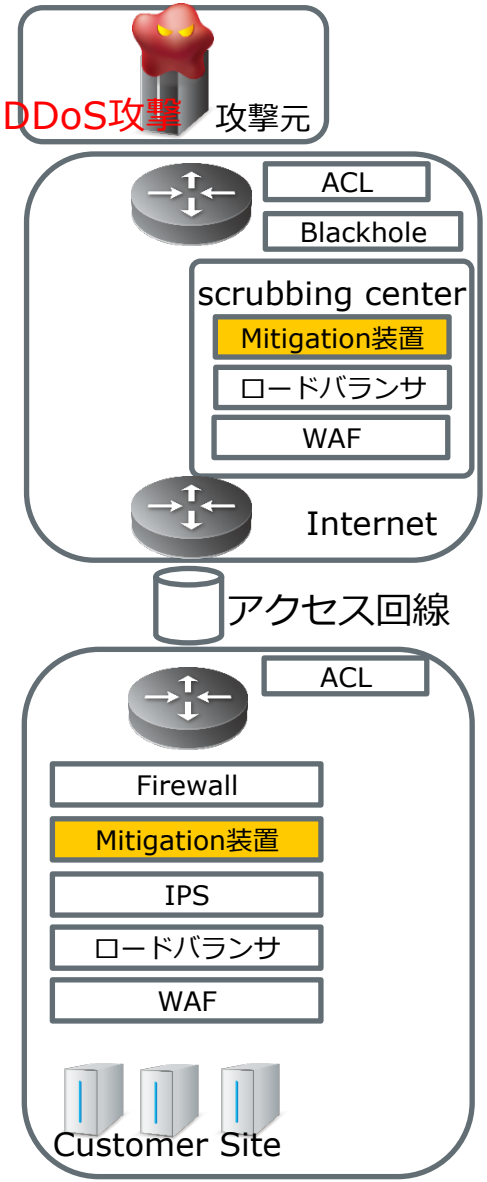


Figure 27 Source: Arbor Networks, Inc.

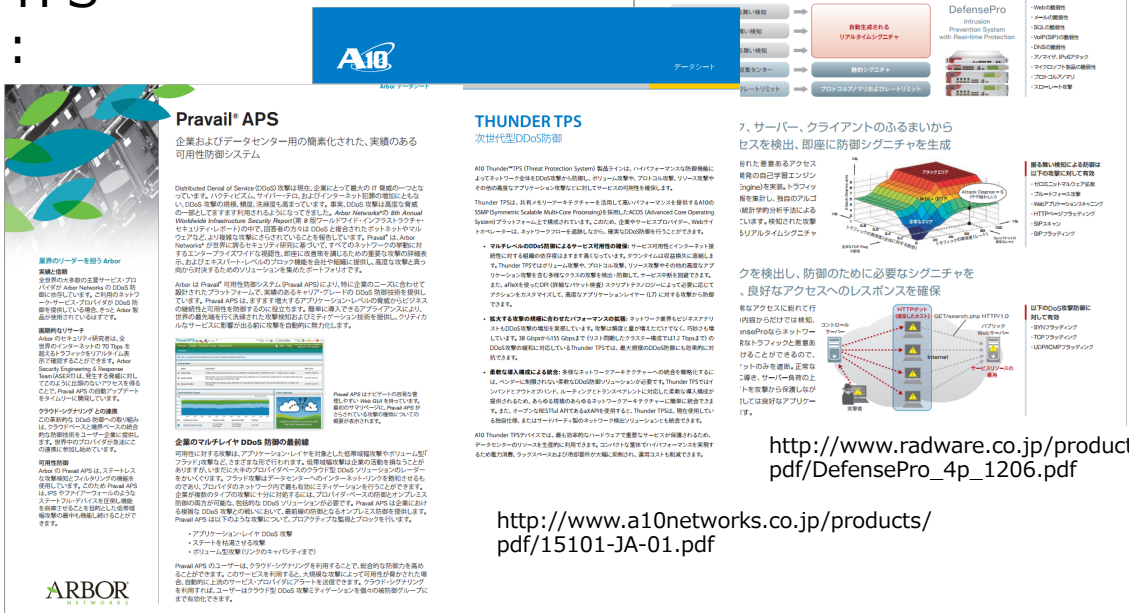
※Worldwide Infrastructure Security Report 2016, Arbornetworks
based on a survey comprised of 172 free-form and multiple choice questions

DDoS防御方法-Mitigation装置-

緩和 | 増設 | 遮断



- Arbor TMS/APS
- Radware Defense Pro
- A10 TPS
- ：



https://www.arbornetworks.com/jp/images/dm_documents/DS_Pravail_JA.pdf

http://www.a10networks.co.jp/products/pdf/15101-JA-01.pdf

http://www.radware.co.jp/product/pdf/DefensePro_4p_1206.pdf

- 対処箇所は、クラウドおよびオンプレミス
  オンプレミスの場合、大量攻撃時に効果が期待できない
- Akamai(Prolexic)等が提供しているDDoS防御サービスも同様なDDoS防御手法と見なせる

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

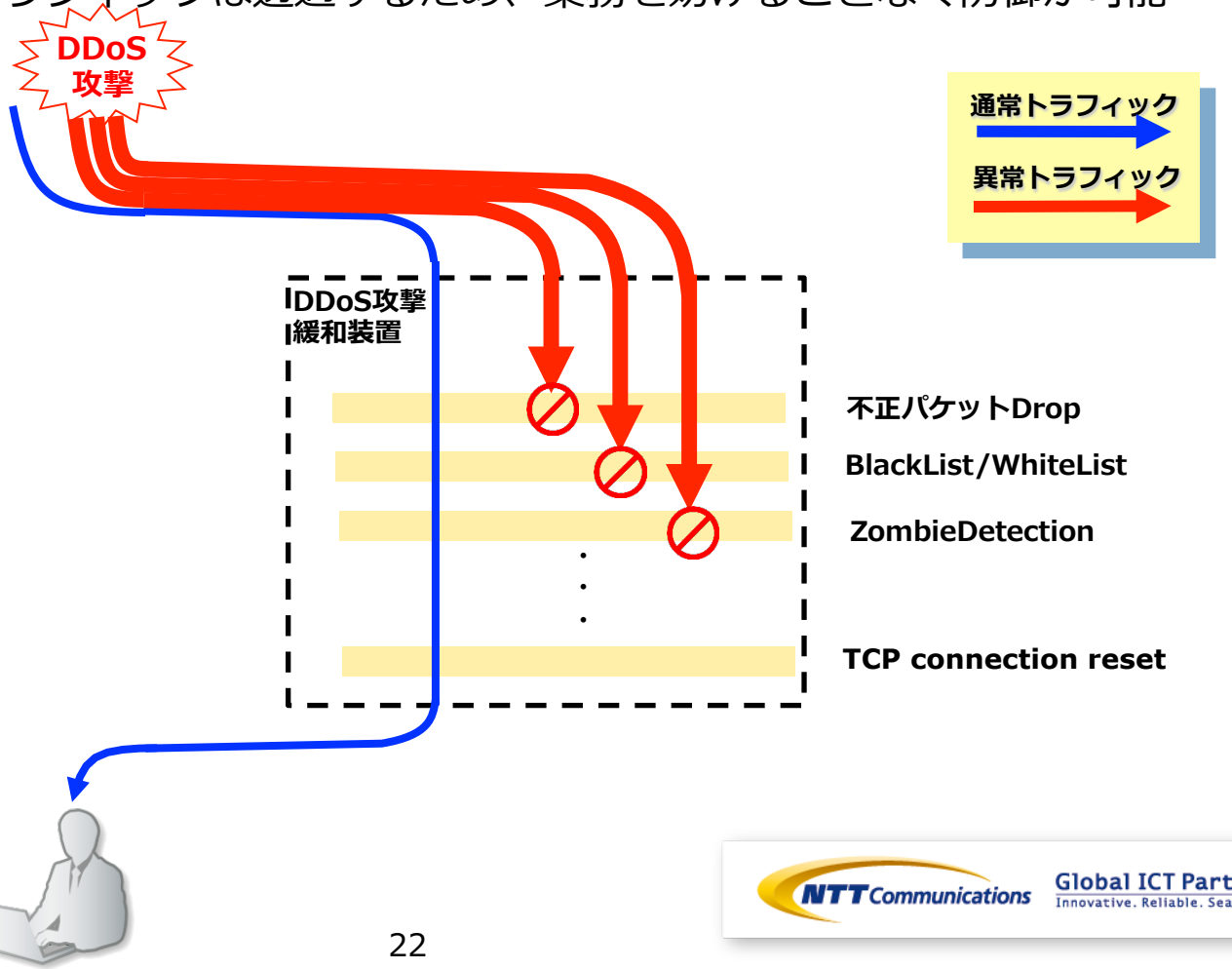
DDoS防御方法-Mitigation装置-2

緩和 | 増設 | 遮断

■ DDoS攻撃緩和装置

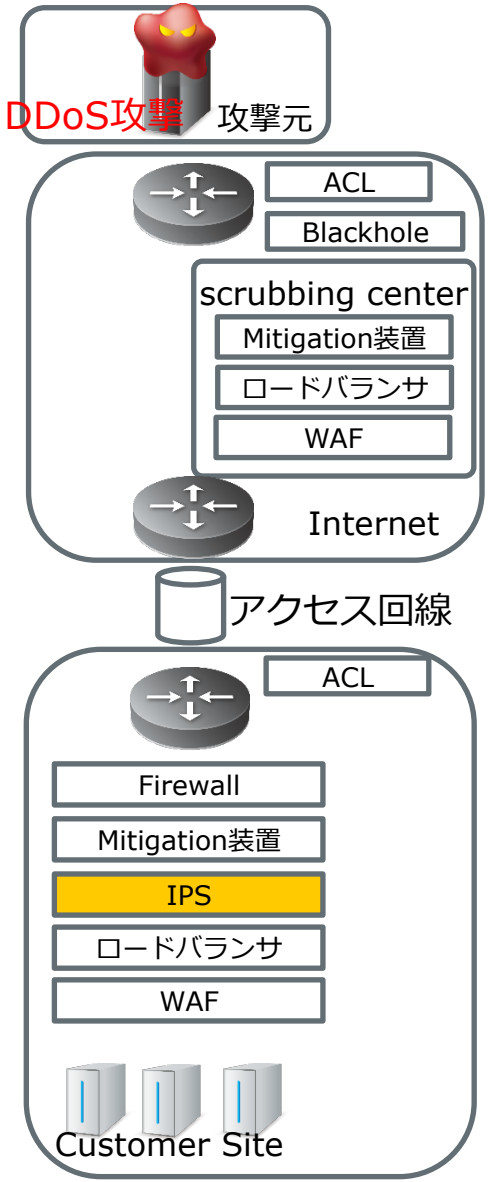
- パケットレベルの解析により、攻撃トラフィックのみを識別して阻止する一方で、正常な業務トラフィックは透過するため、業務を妨げることなく防御が可能

<イメージ図>



DDoS防御方法-IPS-

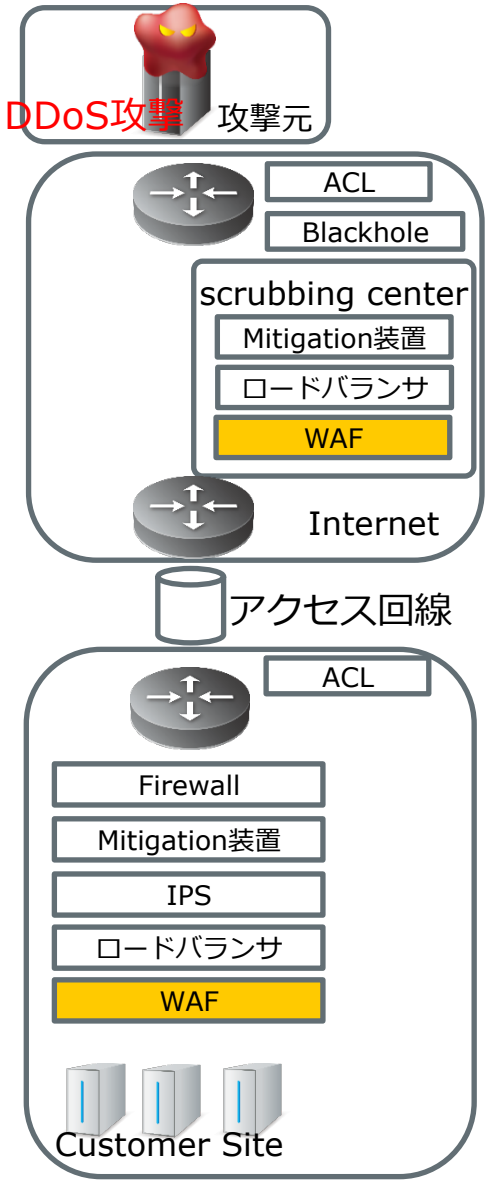
緩和 | 増設 | 遮断



- 対処箇所は、オンプレミス
  ＃大量攻撃時にはボトルネックになる
- IPSにはTCP SYN Flood攻撃などの一部のDoS攻撃手法を検出し廃棄する機能を持つ製品がある
- 使用しているIPSが検出可能な攻撃で、パケット数やセッション数等で機器性能内であれば、IPSで不正パケットを廃棄することでサービスの継続が可能

DDoS防御方法-WAF-

緩和 | 増設 | 遮断

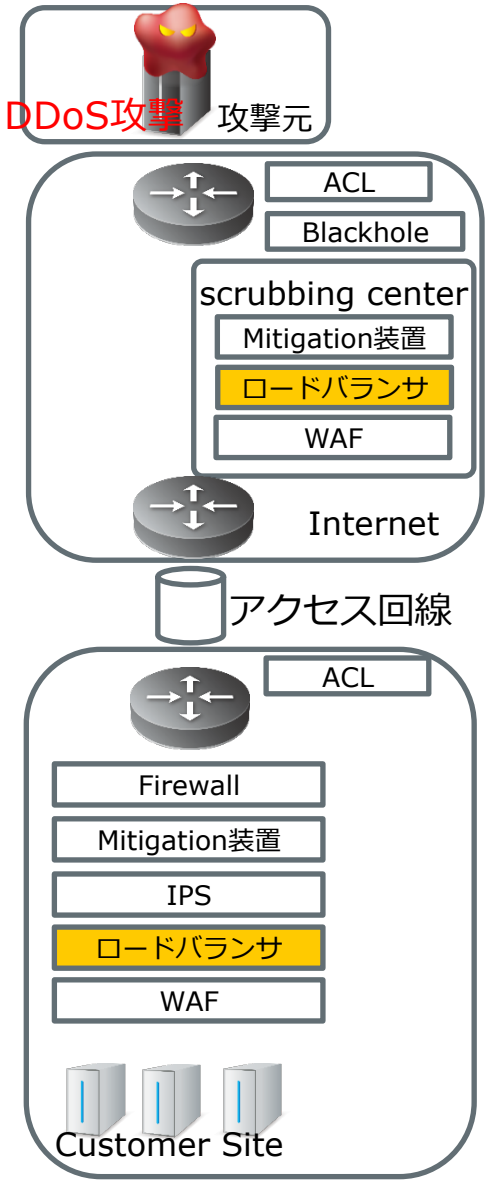


・対処箇所は、クラウドおよびオンプレミス
＃大量攻撃時にはボトルネックになる

・Webサーバに特化したDoS攻撃も出現していることから、TCP SYN Flood攻撃から、Slow DoS攻撃のようなTCPコネクションに関わるリソースを占有する攻撃に対策可能な製品が存在

DDoS防御方法-ロードバランサ-

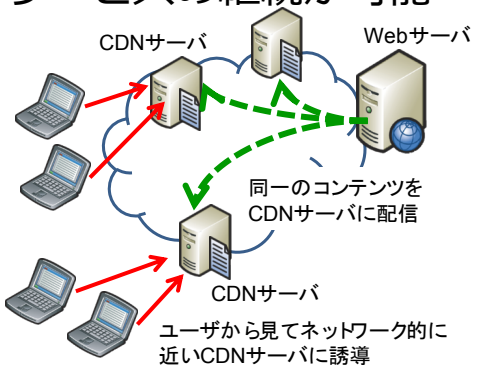
緩和 | 増設 | 遮断



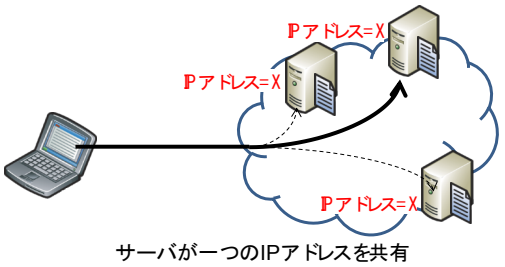
・対処箇所は、クラウドおよびオンプレミス

・トラフィックを負荷分散させることで、不正パケットに対するサーバ負荷を分散し、サービスの継続が可能
＃攻撃を止める訳ではなく、力技！！

・負荷分散の手段としては、
・CDN(Content Delivery Network)
・IP Anycast
も同様に、不正パケットに対するサーバ負荷を分散し、サービスの継続が可能



CDNによるトラフィック分散

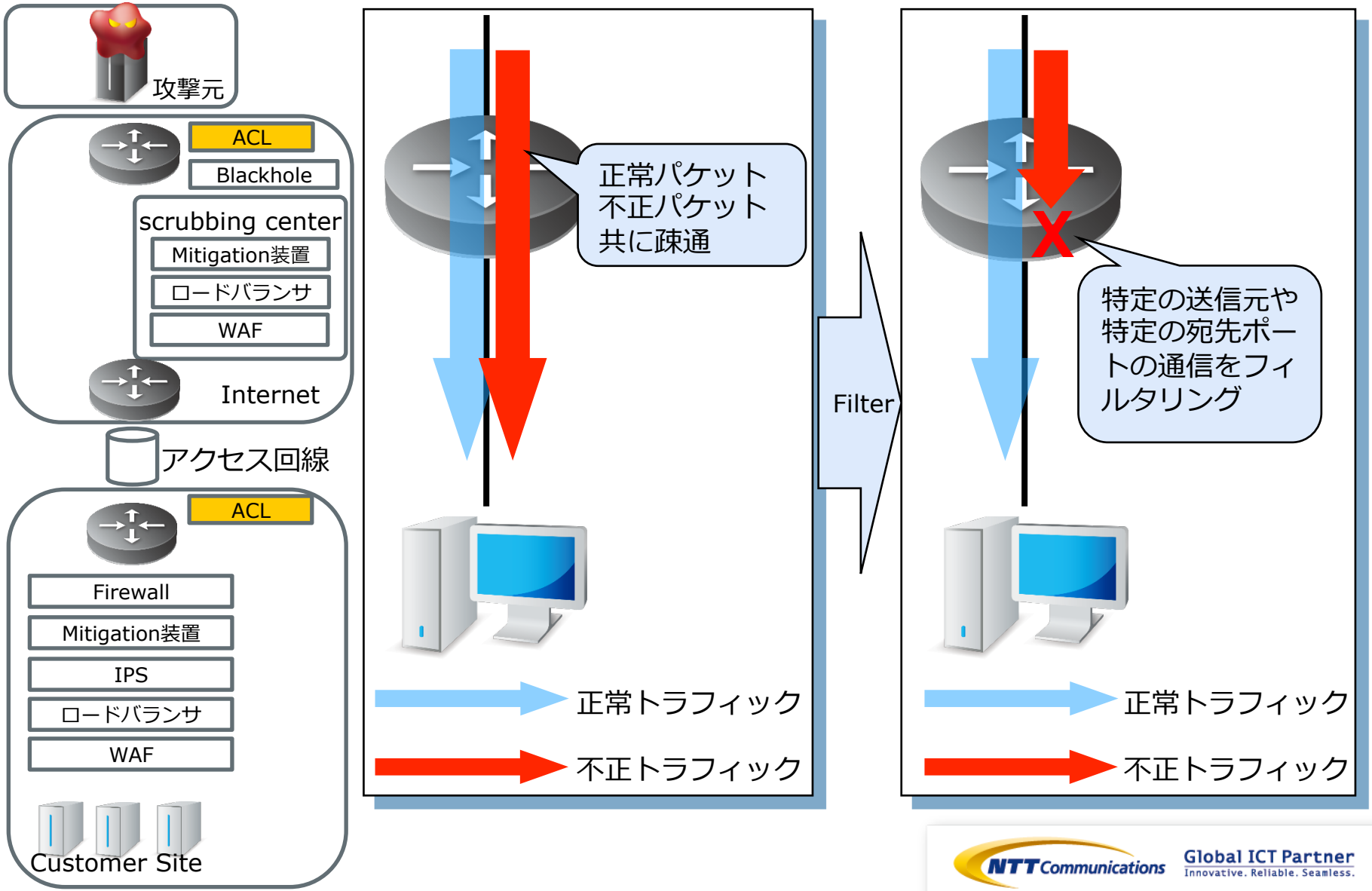


IP Anycastによるトラフィック誘導

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

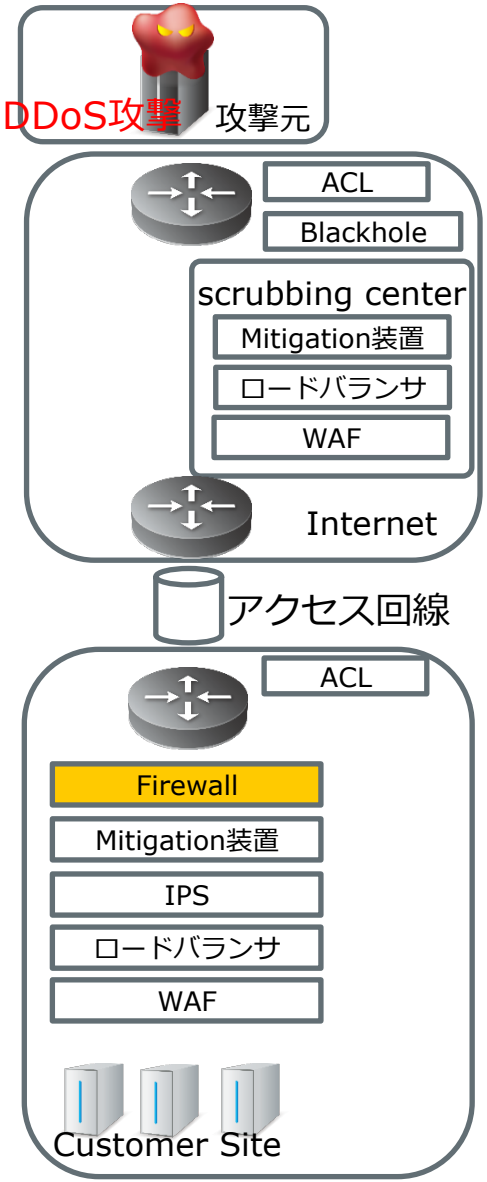
DDoS防御方法-ACL-

緩和 | 増設 | 遮断



DDoS防御方法-Firewall-

緩和 | 増設 | 遮断



・通常のFirewallはDDoS攻撃防御には不十分
・DDoS攻撃はFirewallで許可されたプロトコル・ポート番号を用いて実行される

・さらに、下図で示すように、サーバやアクセス回線と同様にFirewall自体がDDoS攻撃対象になっている
・DDoS攻撃パケットでFirewallのフィルター処理負荷を上げられ、Firewallダウンによりサイト全断する事例が発生している

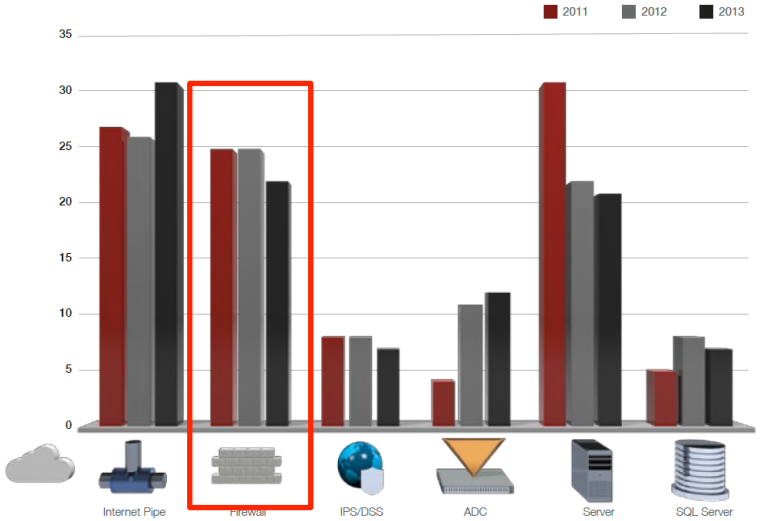


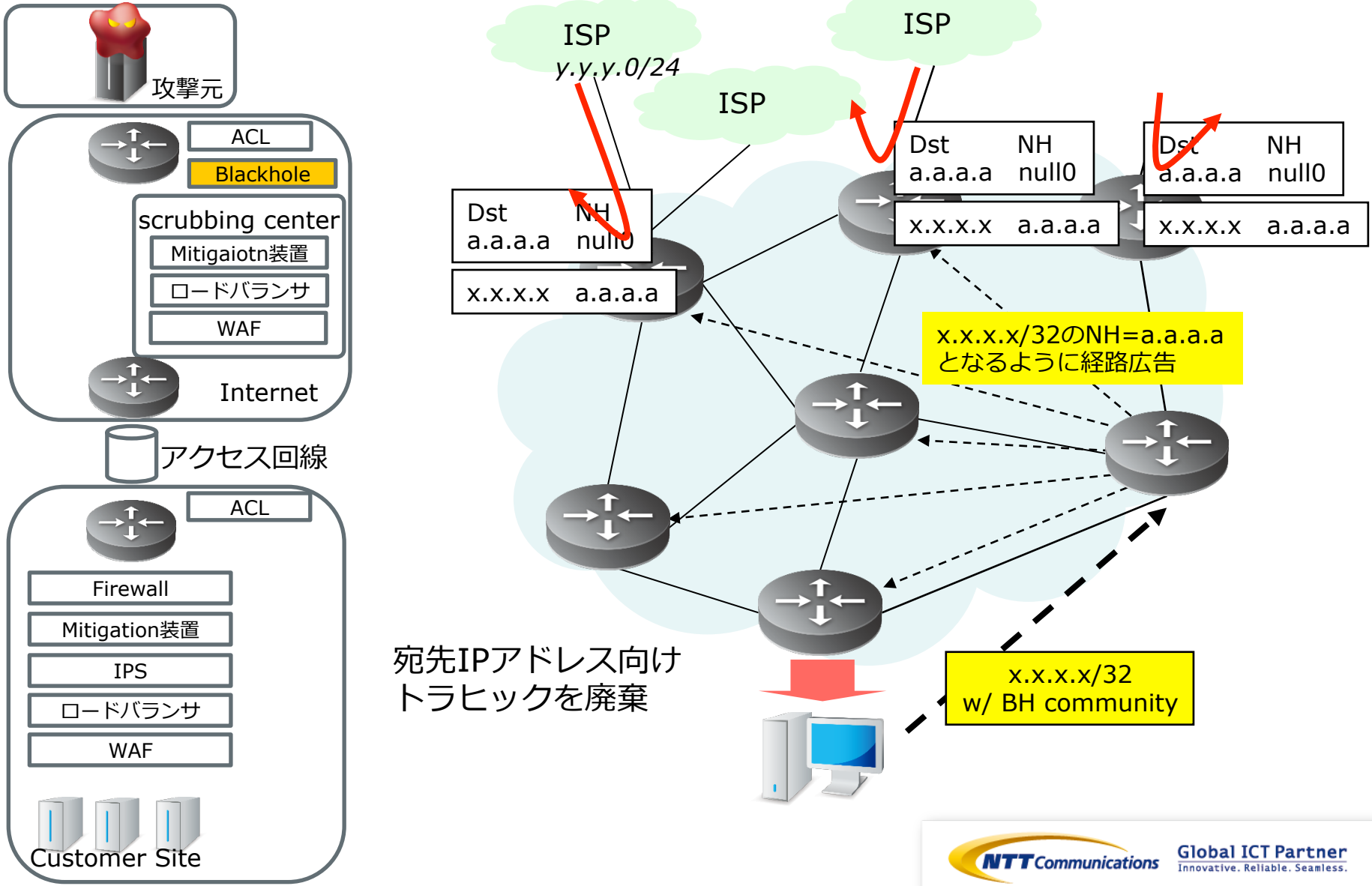
図12：攻撃対象となるネットワークコンポーネント

※2013 Global Application and Network Security Report, Radware

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

DDoS防御方法-Blackhole Routing-

緩和 | 増設 | 遮断



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

- 海外からのトラフィックのみブラックホールしたい場合などの利用方法が考えられる

例) ntt.net

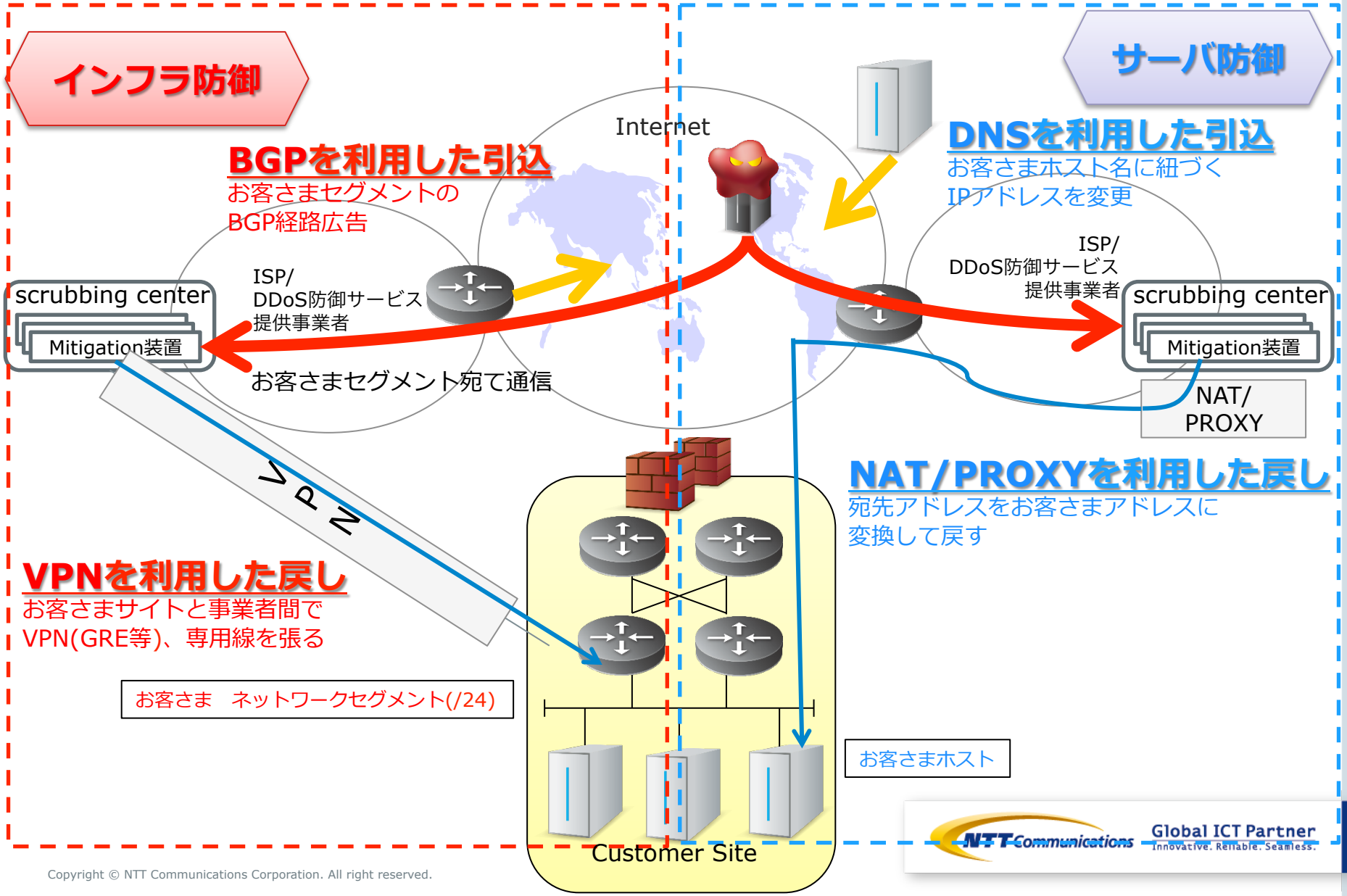
Selective Blackhole communities	
2914:661	only blackhole inside the region the announcement originated
2914:663	only blackhole inside the country the announcement originated
2914:660	only blackhole outside the region the announcement originated
2914:664	only blackhole outside the country the announcement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

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

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

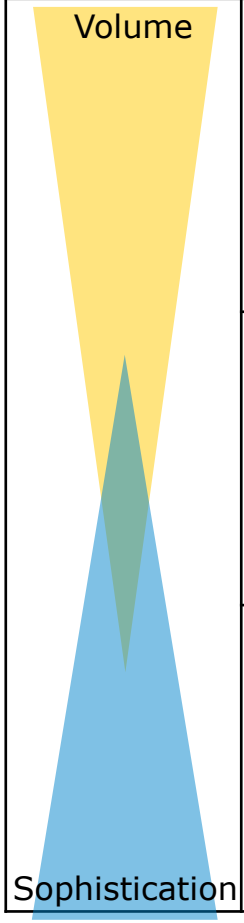
DDoS対策サービス

Cloud型DDoS防御サービス引込＋戻し一般的な手法



NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

DDoS防御サービスのいろいろ

Type of Attacks		攻撃対象	攻撃例	防御ｻｰﾋﾞｽ		事業者NW引込・戻し手法
				防御ﾎﾟｲﾝﾄ	防御提供方式	
	量的攻撃	ネットワーク帯域 Saturate Bandwidth	UDP floods, ICMP floods Spoofed packet floods	事業者NW	・Cloud型mitigation ・Cloud型WAF ・auto-scaling (CDN,VM,DNS) ・acl/null-route	引込 ・BGP ・DNS ・IP割当 戻し ・GRE ・NAT ・Proxy ・CDN ・専用線 ・x-connect
				顧客Site	*顧客ｻｲﾄでの防御困難	
	不正ｾｯｼｮﾝ攻撃	サーバー群（ｻｰﾊﾞｰ、Fireawall、LoadBlancer等)	SYN floods, fragmented packet attack, Ping of Death, SmurfDDoS	事業者NW	・Cloud型mitigation ・Cloud型WAF	
				顧客Site	・ｵﾝﾌﾟﾚWAF・IPS ・ｵﾝﾌﾟﾚMitigation	
	ｱﾌﾟﾘｹｰｼｮﾝﾚｲﾔ攻撃	サーバーアプリケーション	Slowloris, HTTP flood, DNS dictionary, Zero-day DDoS	事業者NW	・Cloud型*mitigation ・Cloud側*WAF *非対称ﾙｰﾄ環境下で、ｼｸﾞﾈﾁｬﾍﾞｰｽ対応に制限有	
				顧客Site	・ｵﾝﾌﾟﾚWAF・IPS ・ｵﾝﾌﾟﾚMitigation装置	

※ｸﾗｳﾄﾞ型：ﾕｰｻﾞｵﾝﾌﾟﾚではなく、ISP、DDoS防御ｻｰﾋﾞｽ事業者等の事業者ﾈｯﾄﾜｰｸ内に配置した設備で防御を提供するｻｰﾋﾞｽ形態

ディスカッションパート

アイスブレイク

- **BoFに参加いただきありがとうございます**
- **DDoS対策を提供している？**
- **DDoS対策を利用している？**

1. 今あるサービスについて

今あるサービスについて

1. RTBH(Remote Triggered blackhole)
2. ACL
3. 増設による対策(CDN等)
4. クラウド型DDoS対策(緩和サービス)

提供者側から見て、利用者から見て、メリット/デメリットや要望についてのコメントはありますか？

2. 事業者間の連携について

How Can You Ask for Help Today?

Technology pioneered by Robert Hooke in 1667, only slightly improved!

IETF93 DOTS WG
https://www.ietf.org/proceedings/93/slides/slides-93-dots-3.pdf

IETFにおける標準化の営み

- **DDoS Open Threat Signaling (dots) WG**

- DDoS対策を効率的に実現するために、DDoSに関連した情報のリアルタイムでのシグナリングを規格化する

- 目的
  - DDoS対策の自動化
  - ベンダ独自なソリューションからの開放
  - 防御システム同士の連携による対策の大規模化

セキュリティオートメーション技術概観

IETFにおけるセキュリティオートメーション技術 (DOTS, I2NSF, MILE, SACM WG)

4つのWGのトピック概要

セキュリティオートメーションに関し、IETFでは4つのWGにて検討

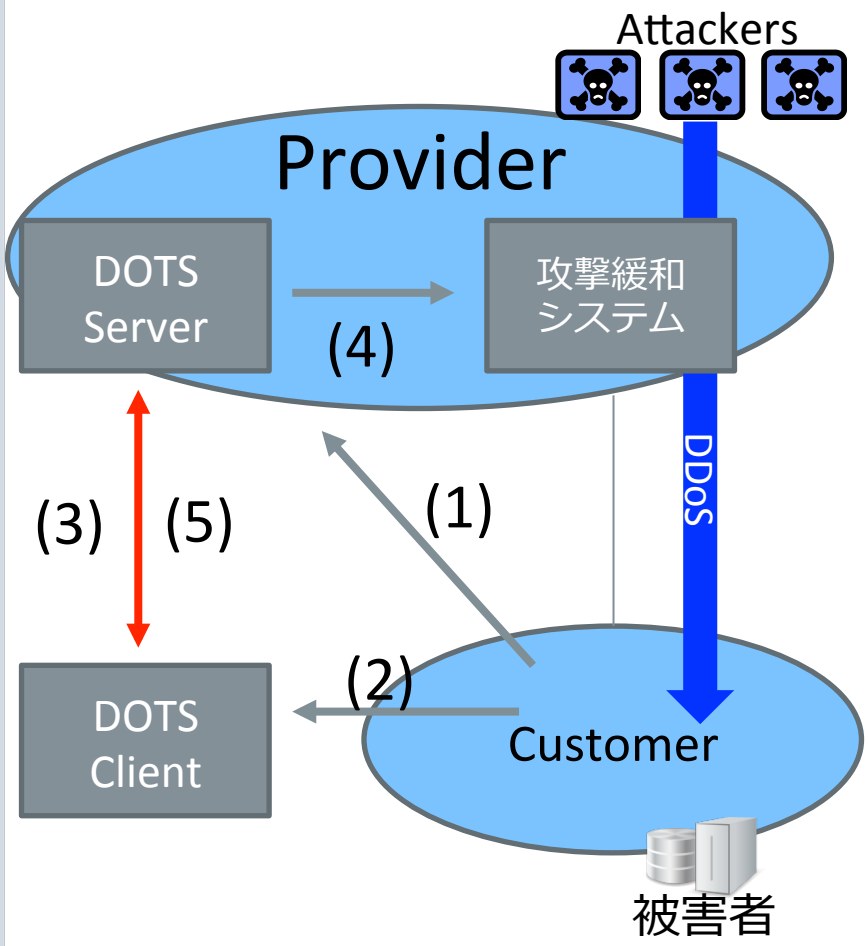
Security Automation

MILE : Managed Incident Lightweight Exchange	*IETF 82 ～*	インシデント情報の交換技術を検討
SACM : Security Automation and Continuous Monitoring	*IETF 85 ～*	Endpointのセキュリティ状態の監視・評価技術を検討
DOTS : DDoS Open Threat Signaling	*IETF 93 ～*	DDoS対策のための機器へのSignaling技術を検討
I2NSF : Interface to Network Security Functions	*IETF 94 ～*	機器のセキュリティ設定・制御のためのSignaling技術を検討

2015/10/6 5

第２回IETF勉強会https://www.isoc.jp/wiki.cgi?page=PreIETF94
NICT 高橋健志氏 スライドより

DOTSプロトコルの基本構成



1) DDoS防御サービスへの登録

2) 攻撃検知

DOTSプロトコル

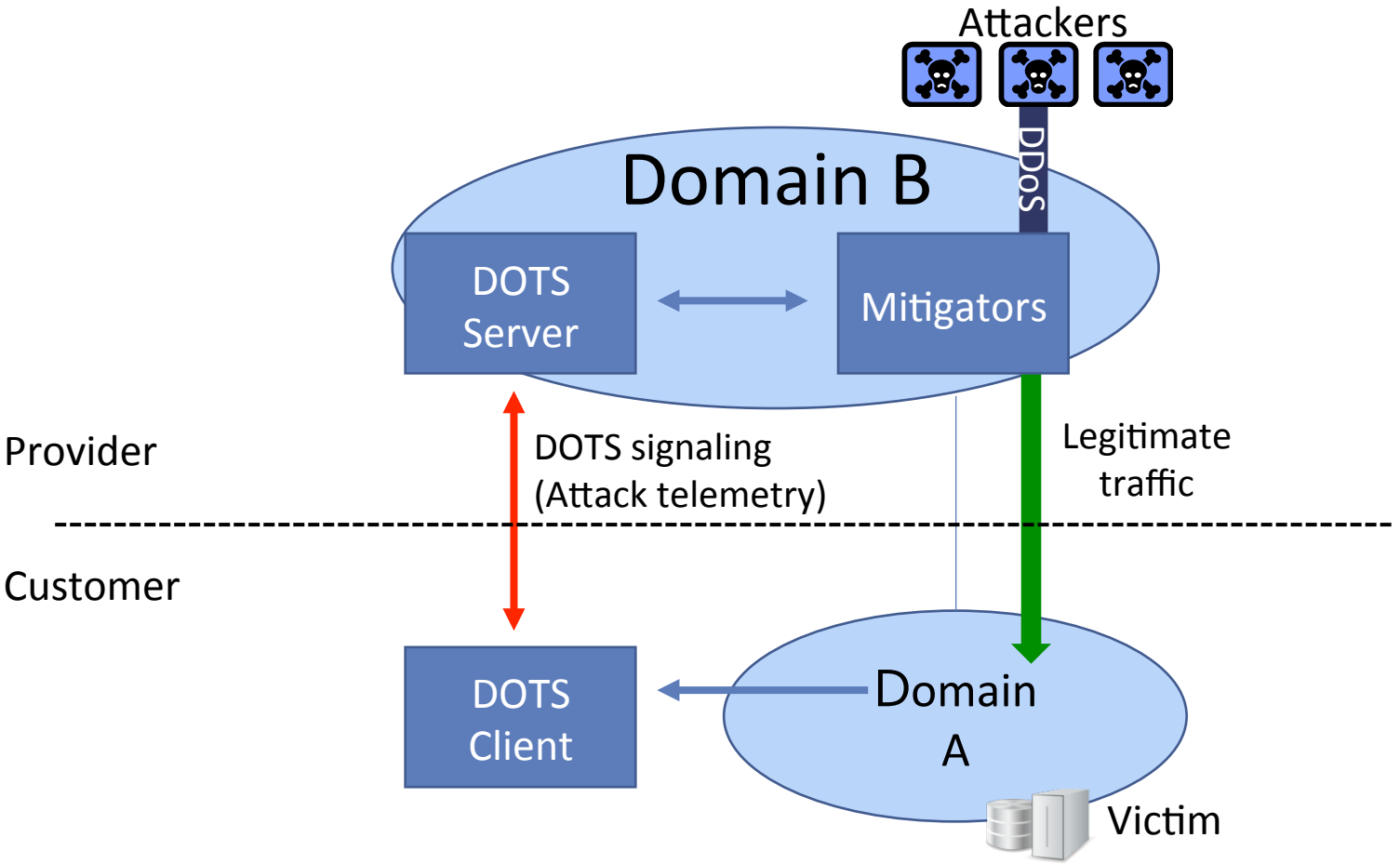
3) DOTS Signaling
DOTSクライアントからDOTSサーバへのシグナリングにより、攻撃情報を提供者に通知し防御を依頼

4) DDoS攻撃緩和

5) DOTS Signaling
DOTSサーバからDOTSクライアントへの攻撃/対策状況の通知

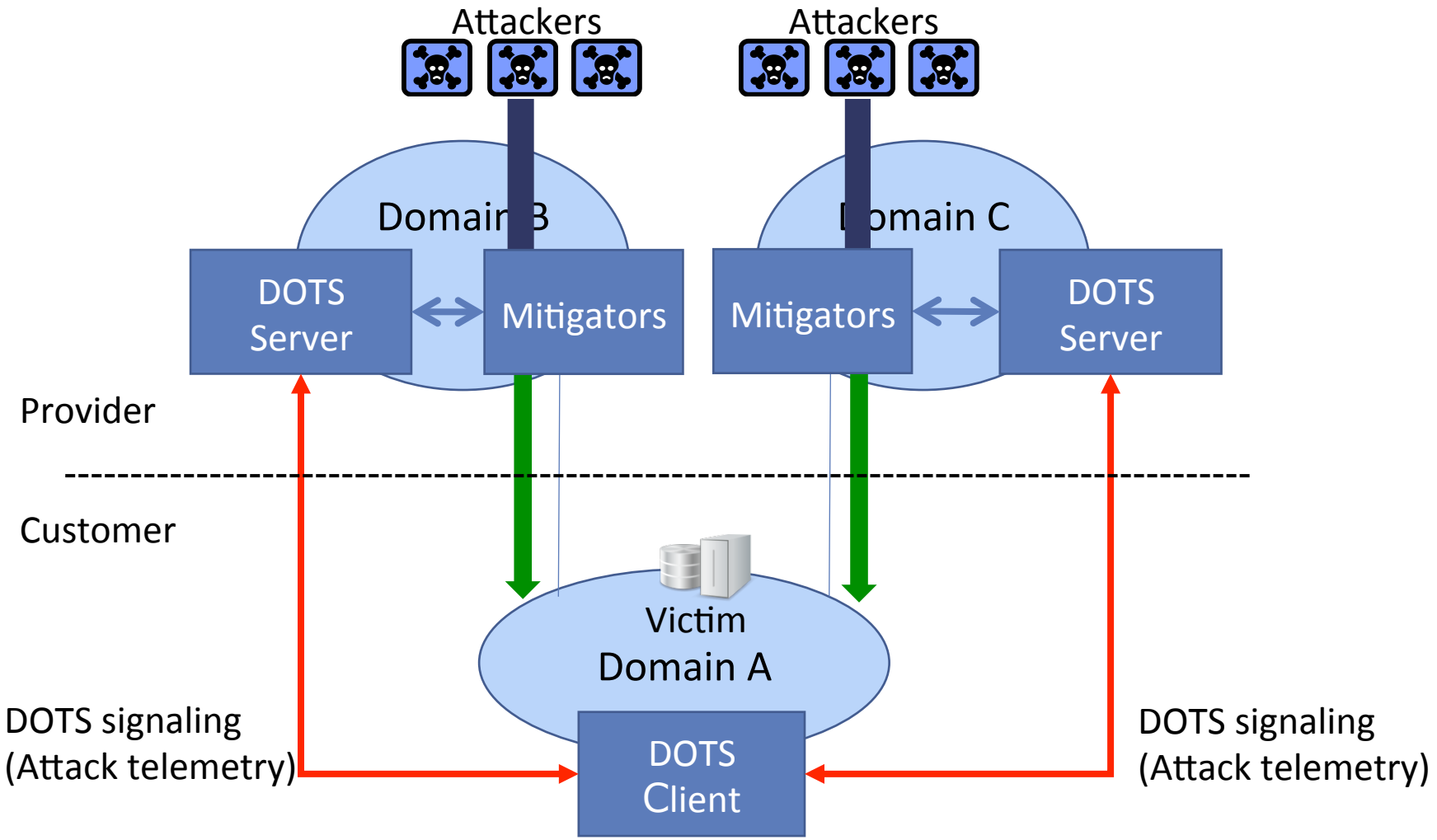
発表時スライド

Inter-domain usecase1: Single-home model



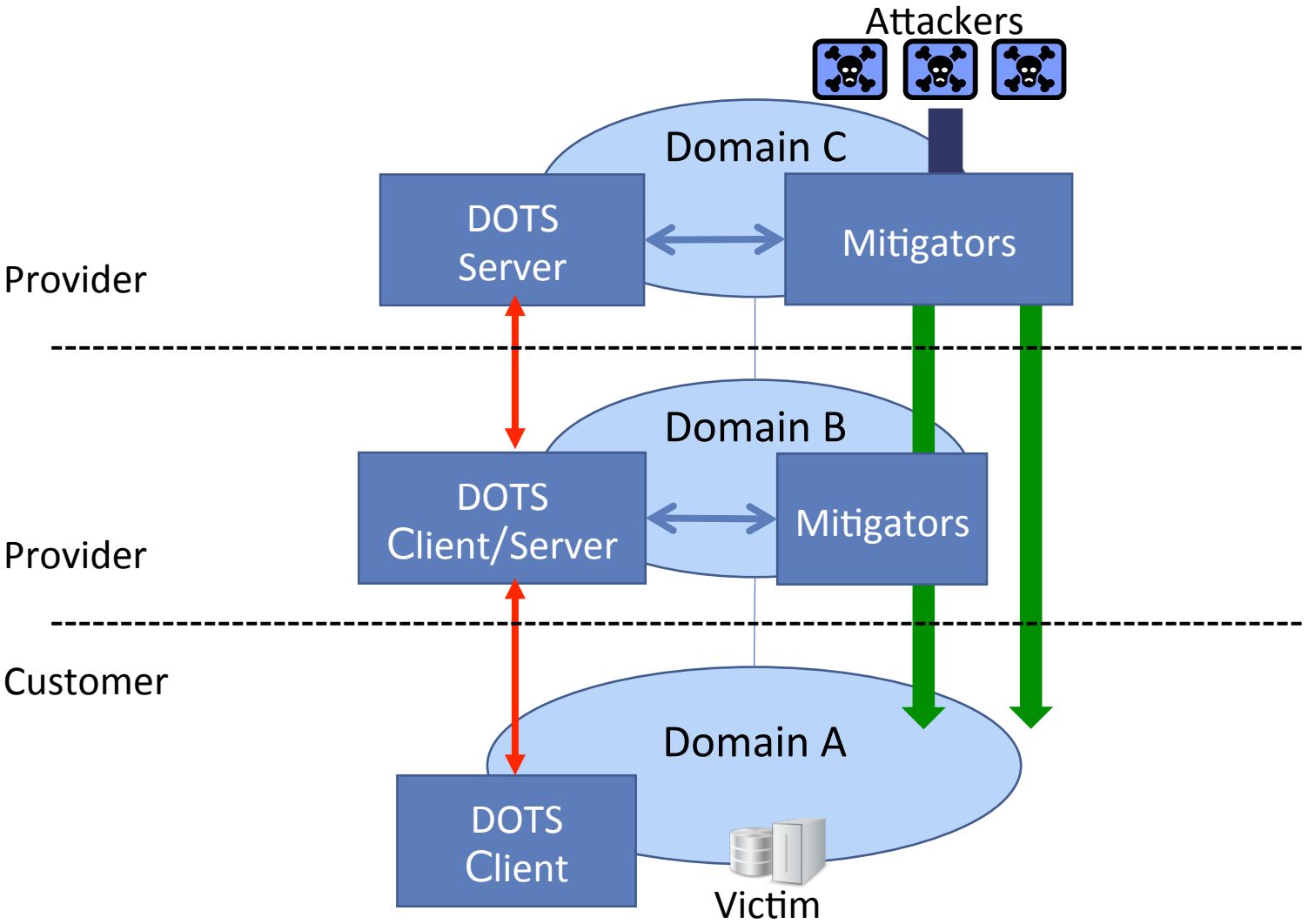
発表時スライド

Inter-domain usecase2: Multi-home model



発表時スライド

Inter-domain usecase3: Delegation model



事業者間の連携について

1. 利用者と提供者の連携(customer-to-provider)
   - 仕様の統一は必要だと思いますか
   - どのようにしたらより上手く連携できますか

2. 提供者間の連携 (provider-to-provider)
   - 必要だと思いますか
   - 必要だとしたらどのような形が考えられますか

3. DDoS攻撃/対策の今後について

DDoS攻撃/対策の今後について

1. DDoS攻撃はいつまで続くのか
   - 防御側不利の状況はいつまで

2. 今後のあるべき対策
   - 対策手法への理解は十分か
   - DDoS対策のコストと仕様は見合っているのか

3. DDoS対策事業者への期待
   - SOCなどマネジメントの充実
   - コスト/競合環境
   - Scrubbing centerの場所
   - 仕様の統一

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.