S6 今を知り今後に備える！　ルーティングセキュリティ

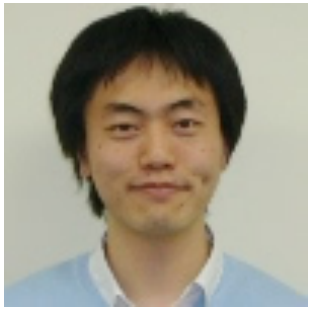
DDoS対策最新動向

Internet Week 2017
2017年11月28日

NTT Communications Global ICT Partner
Innovative. Reliable. Seamless.

自己紹介

- 西塚要(にしづか かなめ)
  - 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の運用サービスを担当。現在は研究開発組織にて、トラフィック分析などISPの課題に関する研究開発に従事。
- メインフィールド
  - トラフィック分析
  - DDoS対策
  - IPv4枯渇対策関連技術
- 社外活動
  - IETF標準化 DOTS WG
  - JPNIC「IPv6教育専門家チーム」



1. DDoS攻撃の傾向

“DDoS”の文字がニュース誌面にも登場

- ○○銀行のネットバンキングが使えない
- ○○オンラインのゲームができない
- 攻撃を止めて欲しければ金を払え

DDoS攻撃の停止と引き換えに金銭を要求する脅迫メール、JPCERT/CCが注意喚起

山崎 洋一＝ITpro　2017/09/21

目次一覧

シェア 67　B!ブックマーク 14　Pocket　ツイート　保存する

JPCERTコーディネーションセンター（JPCERT/CC）は2017年9月21日、DDoS（分散型サービス妨害）攻撃の停止と引き換えに金銭を要求する脅迫メールを受け取ったとする報告が複数出ていると公表した。脅迫メールは9月19日頃から確認されており、送信者は「Phantom Squad」を名乗っているという。ただ、「9月14日頃から国内の複数の組織で発生したと報じられているDDoS攻撃の犯人がPhantom Squadであるという情報はなく、関連性は不明」（JPCERT/CC）としている。

JPCERT/CCが提供を受けた情報によると、脅迫メールは2017年6月20日頃に「Armada Collective」を名乗る攻撃グループが発信した脅迫メールの文面と類似点があるという。一方、文中では宛先や対象を直接指定しておらず、国内外の広範囲に送付されているという相違点も確認されている。

JPCERT/CCは、ネットワークやサーバーにおけるDDoS攻撃発生時の対応体制を平時から点検することを勧めている。また、管理下にあるサーバーやルーターなどがDDoS攻撃の踏み台とならないよう適切に設定することを呼びかけている。

Android端末を踏み台にしたDDoS攻撃発生 Google Playに300本の不正アプリ

マルウェアを仕込んだアプリがGoogle Playで配信され、世界100カ国以上のAndroid端末が関わる大規模DDoS攻撃が発生した。

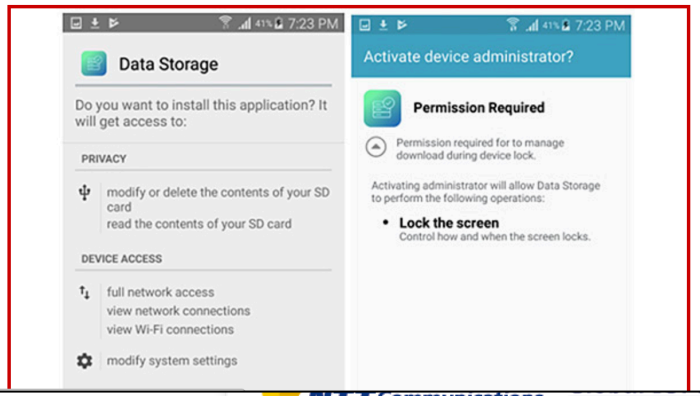
[鈴木聖子，ITmedia]

印刷／PDF　172 ツイート　231 いいね！　231 シェア　16 B! Bookmark　24 Pocket　G+　通知

PR 大手銀行がアジャイル開発、セキュアなAPI開発で変わる！

PR 煩雑化する顧客接点に対応できるデジタル化導入と付加価値

Android端末を踏み台にして、分散型サービス妨害（DDoS）攻撃を仕掛ける悪質なアプリが、公式アプリストアのGoogle Playで配信され、世界100カ国以上のAndroid端末がかかわる大規模攻撃が発生した。対策に協力した各社が8月28日のブログで明らかにした。Googleは既に、不正なアプリ約300本を削除するなどの対策を講じているという。

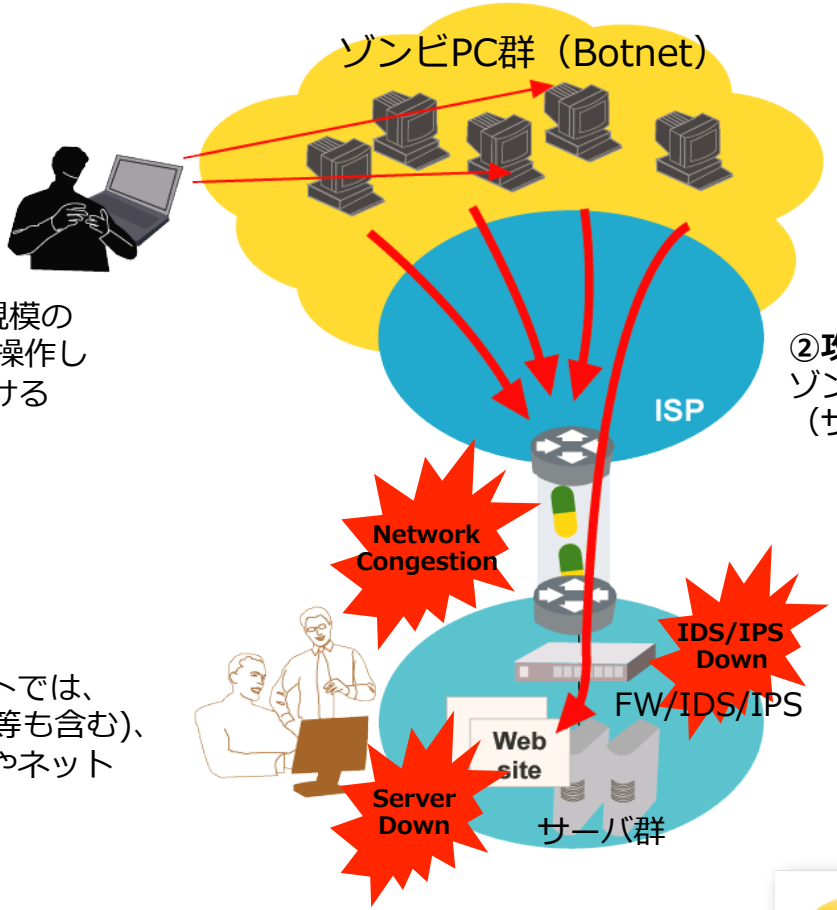


大規模DDoS攻撃の事例

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	ネットバンキングに接続しつらい状況。金銭要求。
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)。
2016年10月	約6時間	Dyn (Managed DNS基盤)	IoT機器向けマルウェア「Mirai」によるDDoS攻撃により、Amazon, PayPal, Twitterなど多くののサービスに支障。(1.2Tbps)
2017年6月	3日間(断続的)	Final Fantasy XIV 北米サーバ	FF14の北米サーバがDDoS攻撃を受け、6月17、19、21日にネットワーク障害が発生。
2017年10月	2日間	スウェーデンの複数の交通機関	列車運行を管理するTrafikverket（スウェーデン産業省交通局）のITシステムが麻痺し、列車の運行停止や遅延が発生。

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。ここ数年でDDoS攻撃も深刻化・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る。



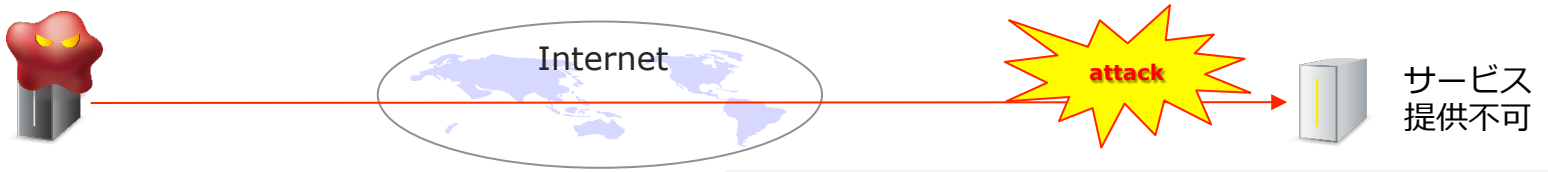
①攻撃命令
インターネット上の数十万規模のゾンビPC（Botnet）を遠隔操作しWEBサーバ等に攻撃を仕掛ける

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

DoS攻撃/DDoS攻撃

- DoS（Denial of Service）攻撃

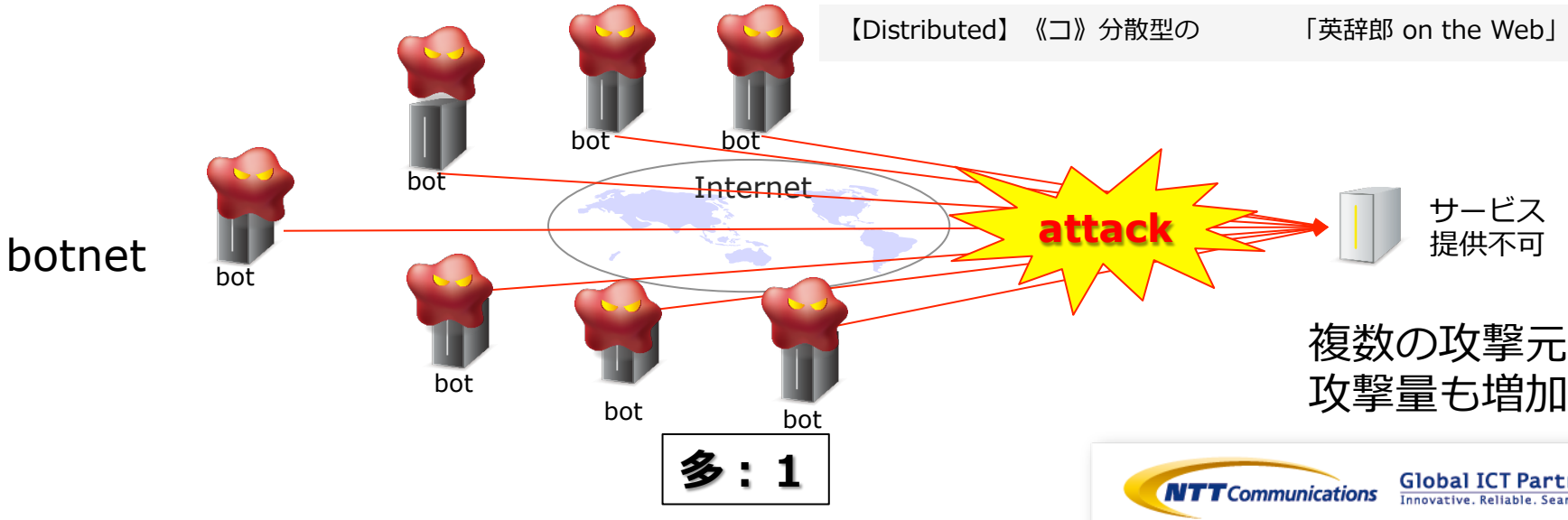


1 : 1

【Denial-of-Service attack】
《イ》サービス妨害攻撃
（悪意のある人が）企業のウェブサイトに大量のデータを
送信して、そのサーバーが正常に機能しなくなるようにして、
（その企業の）顧客またはユーザーがアクセス不可能な状態にすること

- DDoS(Distributed Denial of Service）攻撃

【Distributed】《コ》分散型の　　「英辞郎 on the Web」より

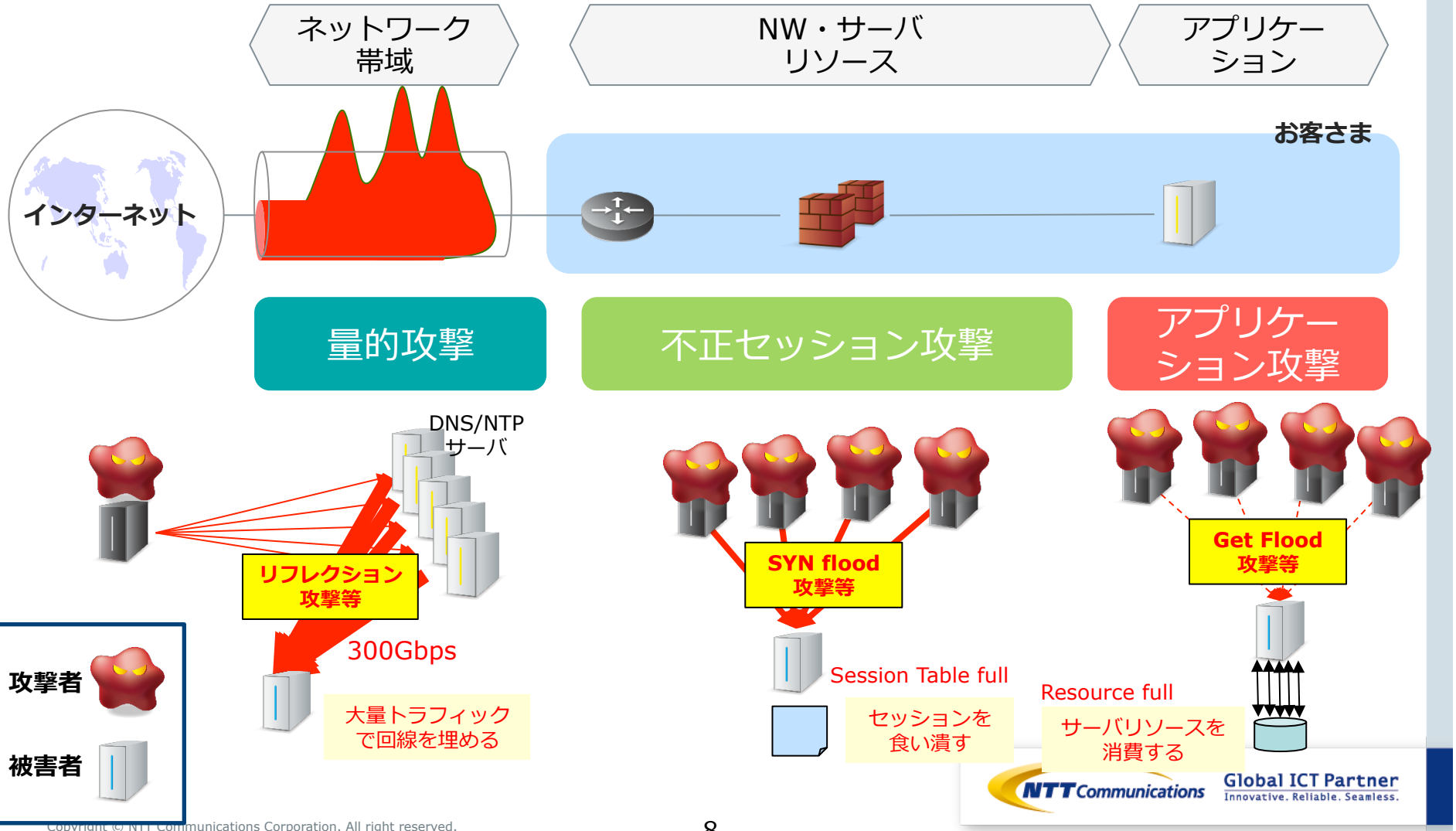


複数の攻撃元
攻撃量も増加

多 : 1

DDoS攻撃の種類と影響範囲

- 攻撃手法により、影響箇所は異なる



DDoS攻撃手法

✓ 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

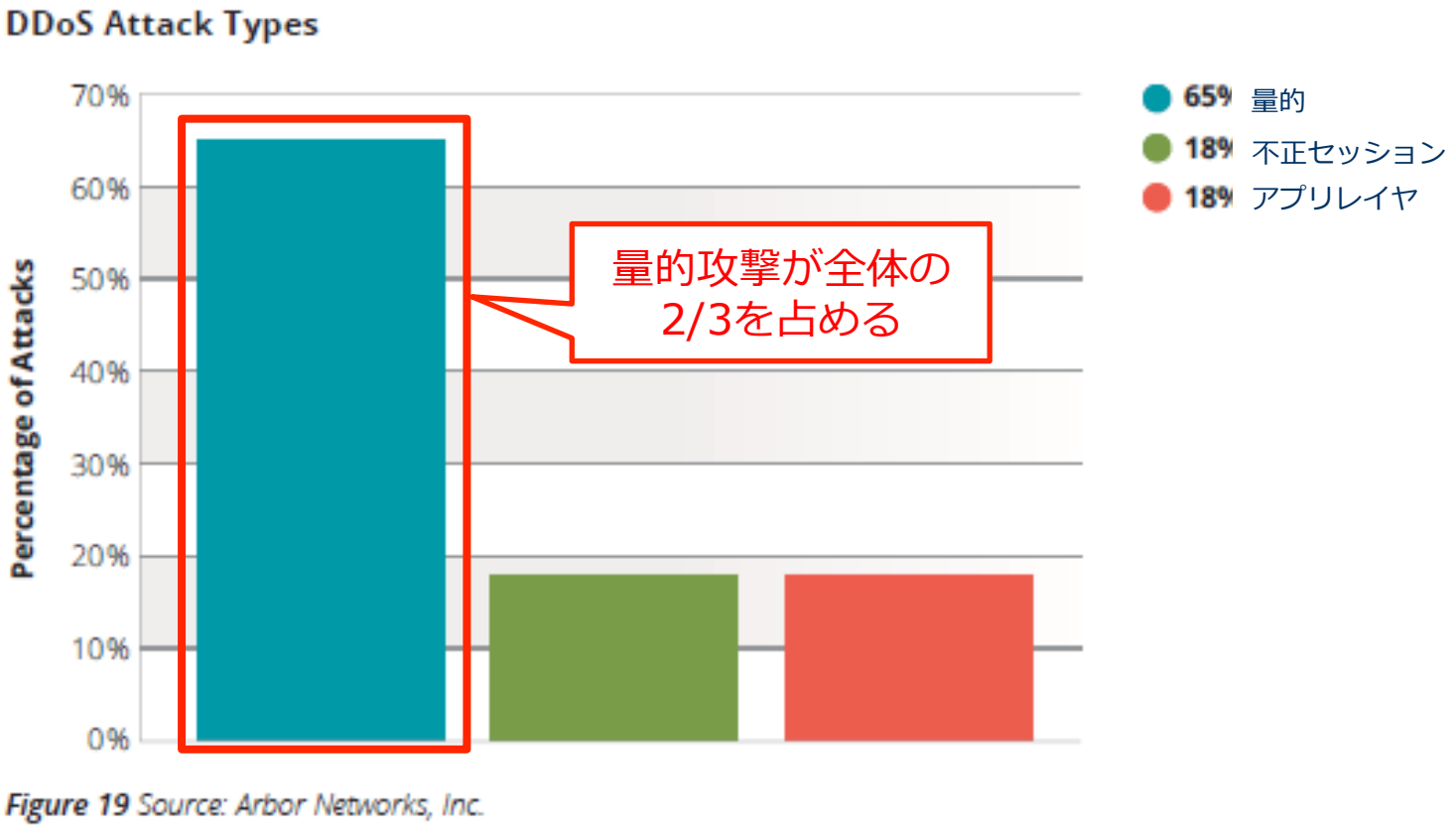


Figure 19 Source: Arbor Networks, Inc.

※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

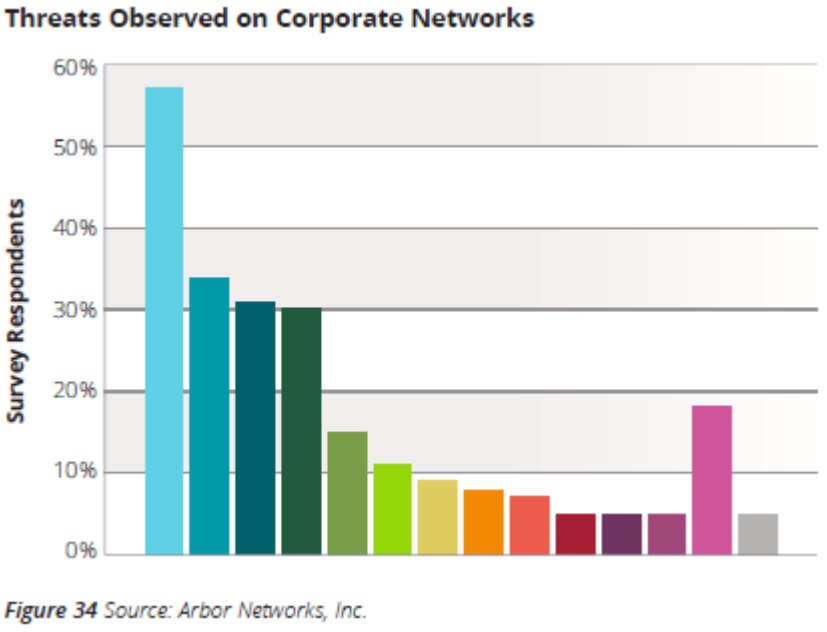
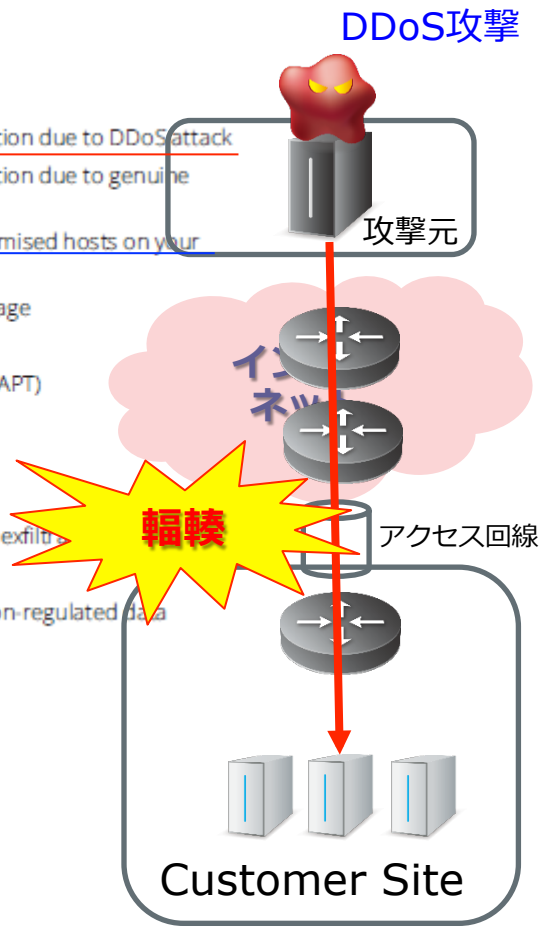
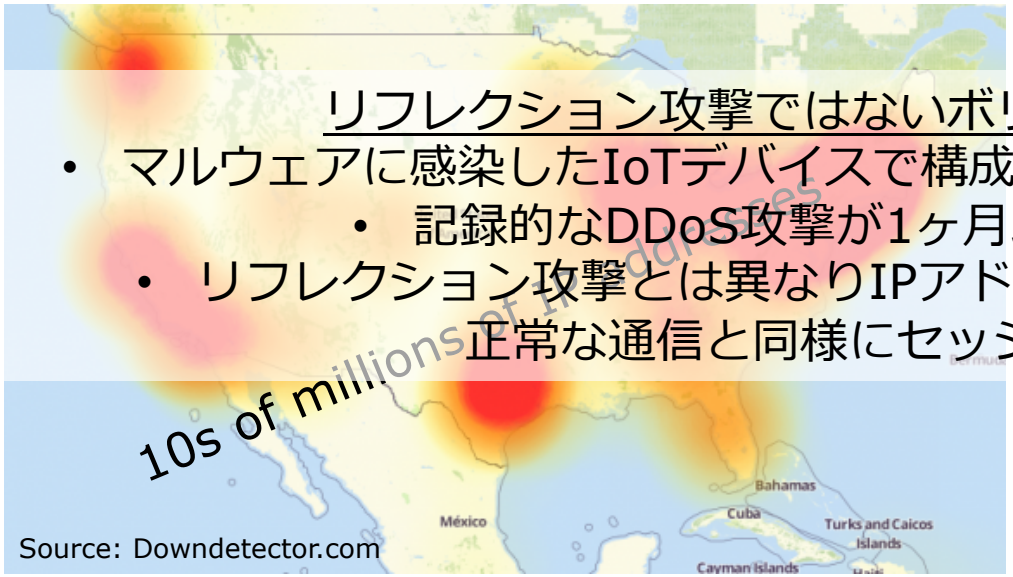


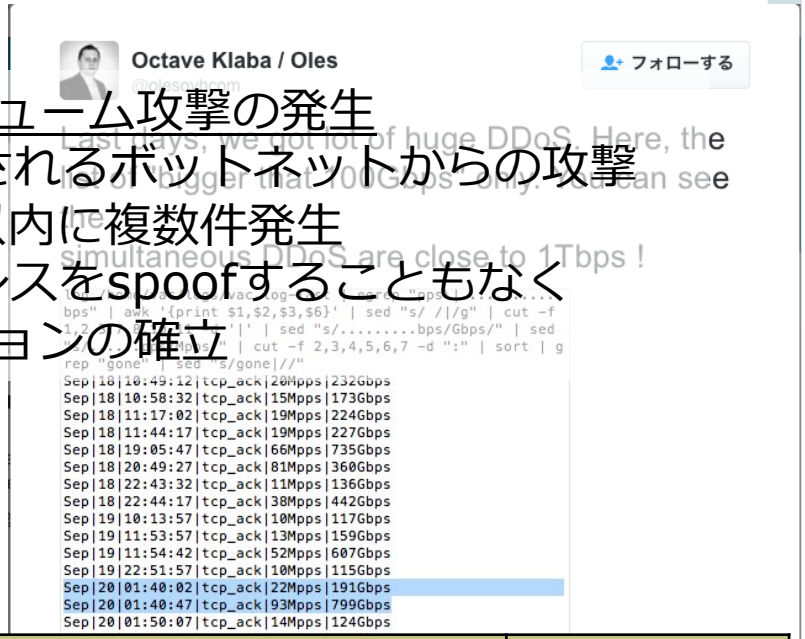
Figure 34 Source: Arbor Networks, Inc.

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



IoTデバイスを利用したボリューム攻撃





リフレクション攻撃ではないボリューム攻撃の発生

- マルウェアに感染したIoTデバイスで構成されるボットネットからの攻撃
  - 記録的なDDoS攻撃が1ヶ月以内に複数件発生
- リフレクション攻撃とは異なりIPアドレスをspoofすることもなく正常な通信と同様にセッションの確立

発生日時	攻撃対象		攻撃帯域	攻撃元			攻撃手法
2016/9/20	KrebsOnSecurity.com	web	625Gbps	router, DVR, IP camera	BASHLITE Mirai		o SYN/GET/ POST flood o GRE
2016/9/20	OVH	hosting	1Tbs+	DVR IP camera		145,607 IP	o TCP/ack oTCP/ack+psh o TCP/syn
2016/10/21	Dyn	Managed DNS基盤	1Tbs+		Mirai	10s of millions of IP	o Pseudo Random Subdomain Attack

2. DDoS対策手法

DDoS対策の流れ

検知

- フロー監視
- パケット監視
- サービス監視
- 申告

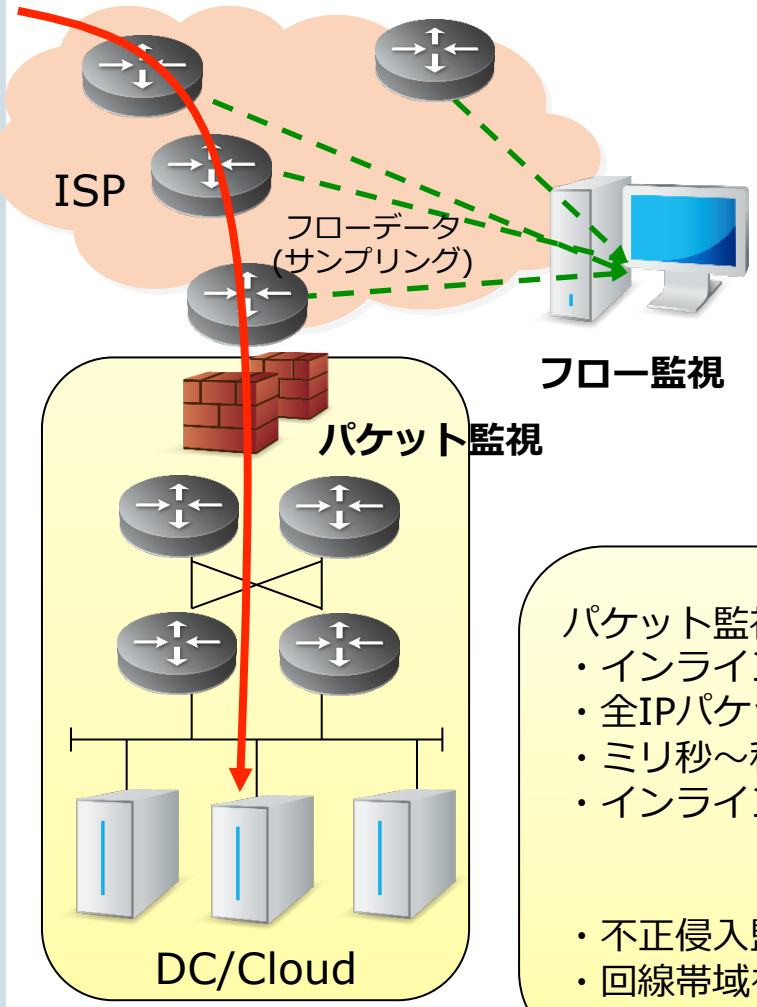
防御

- 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対策手法
～ 検知 ～

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

DDoS検知方法

- Netflow、Firewall logs、SNMPが上位
- Netflow は昨年より 11% 増、Firewall logs は 8% 減

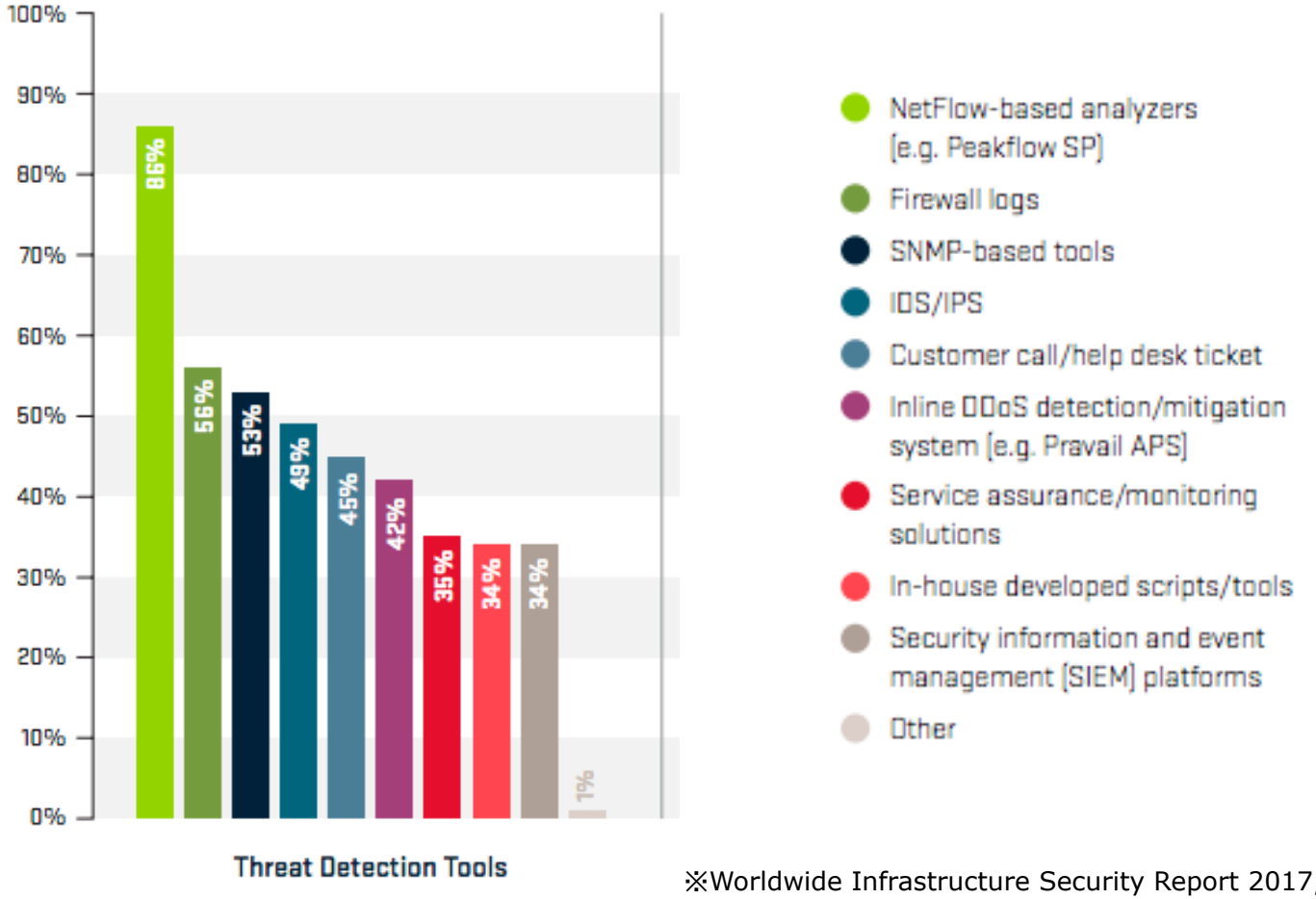


Figure 7 Threat Detection Tools and Threat Tool Effectiveness

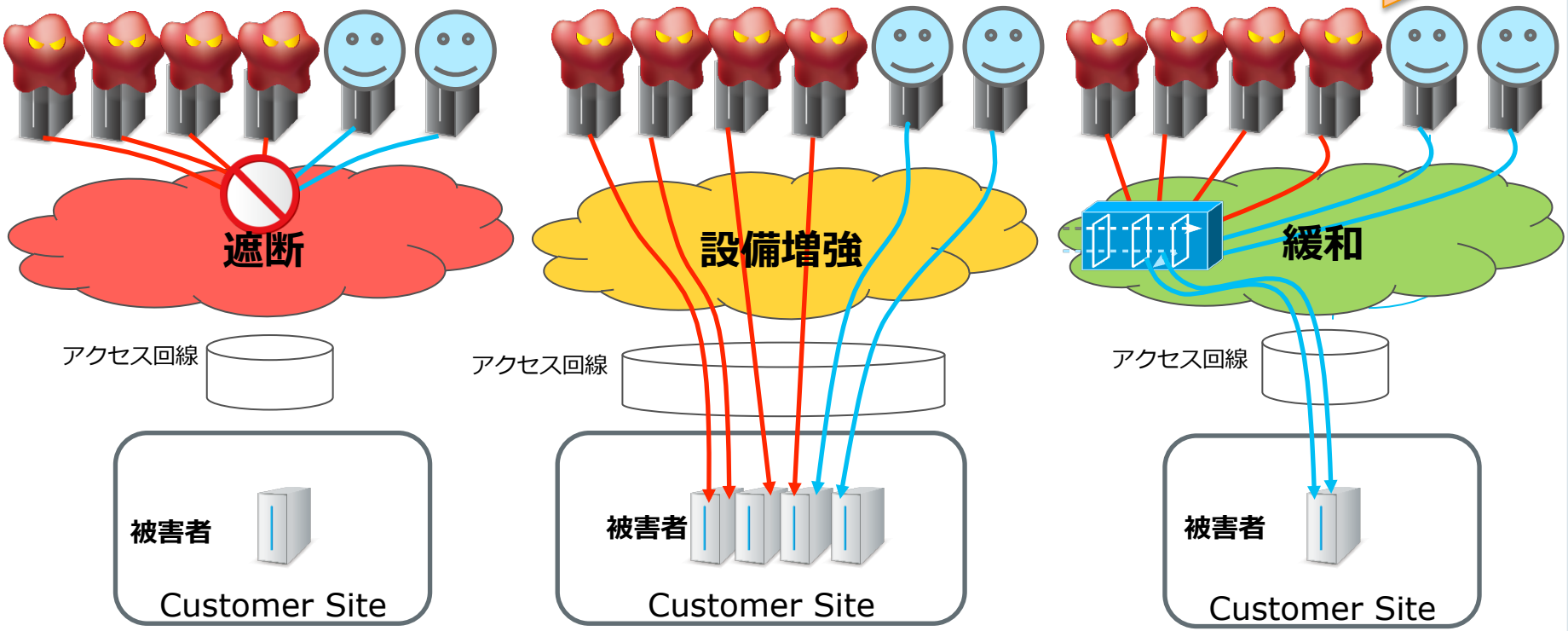
※Worldwide Infrastructure Security Report 2017, Arbornetworks

DDoS対策手法
~ 防御 ~

防御方法の違い

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

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

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

DDoS防御方法

・DDoS Mitigation装置、Blackhole Routing 、ACLが中心
・増減が目立つのは、IDMS 73% → 83%，ACL 70% → 52%

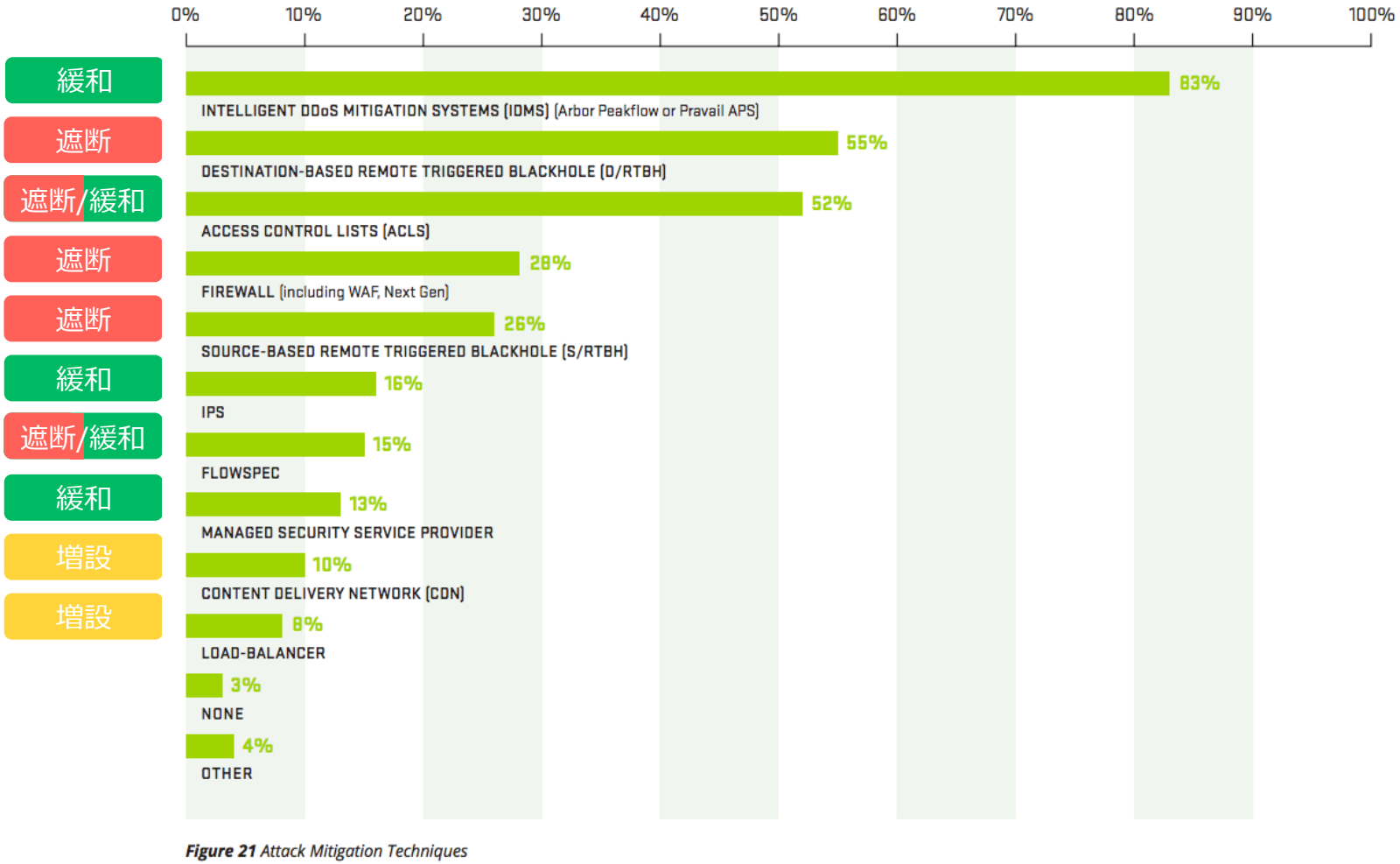
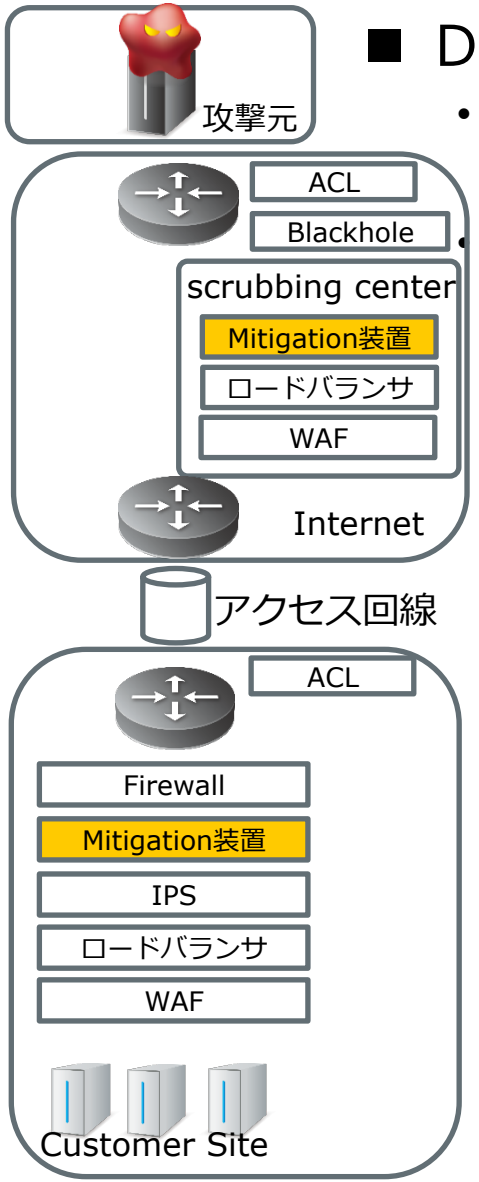


***Figure 21** Attack Mitigation Techniques*

※Worldwide Infrastructure Security Report 2017, Arbornetworks

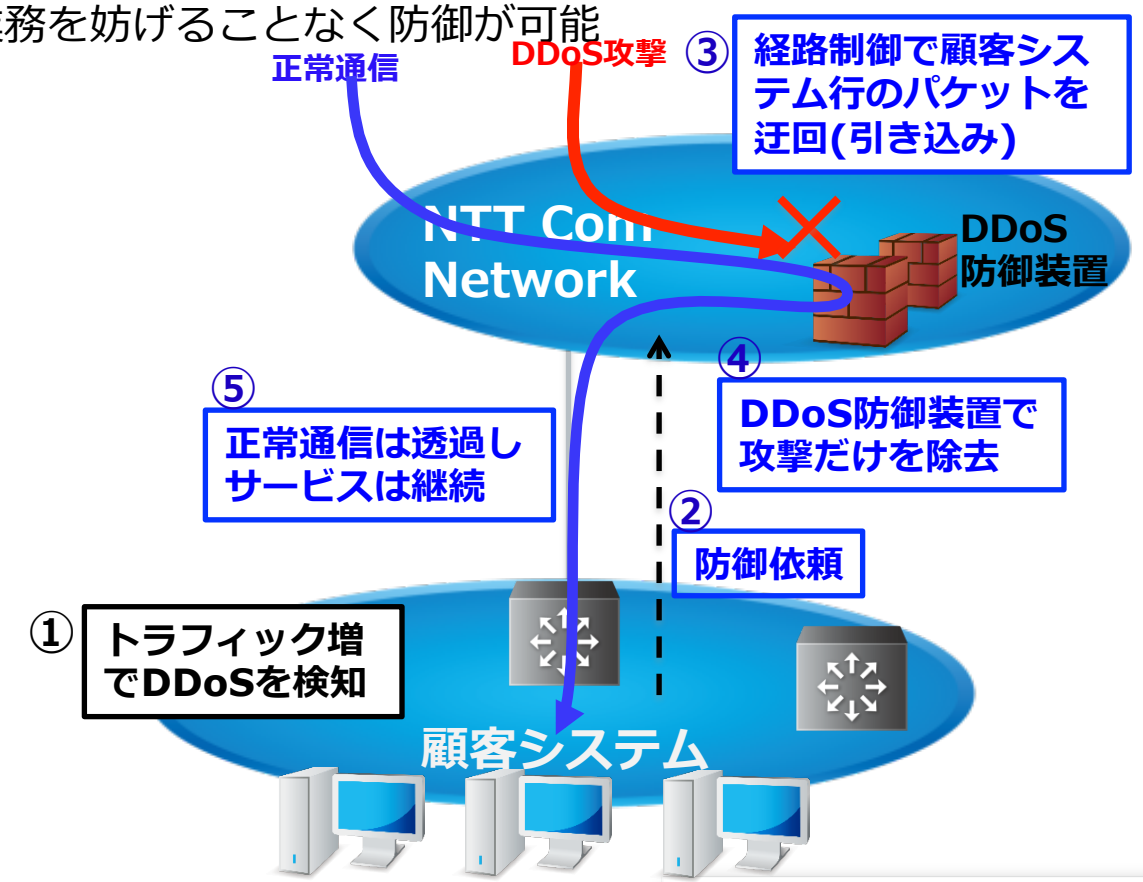
DDoS防御方法 -Mitigation装置-

遮断 増設 緩和



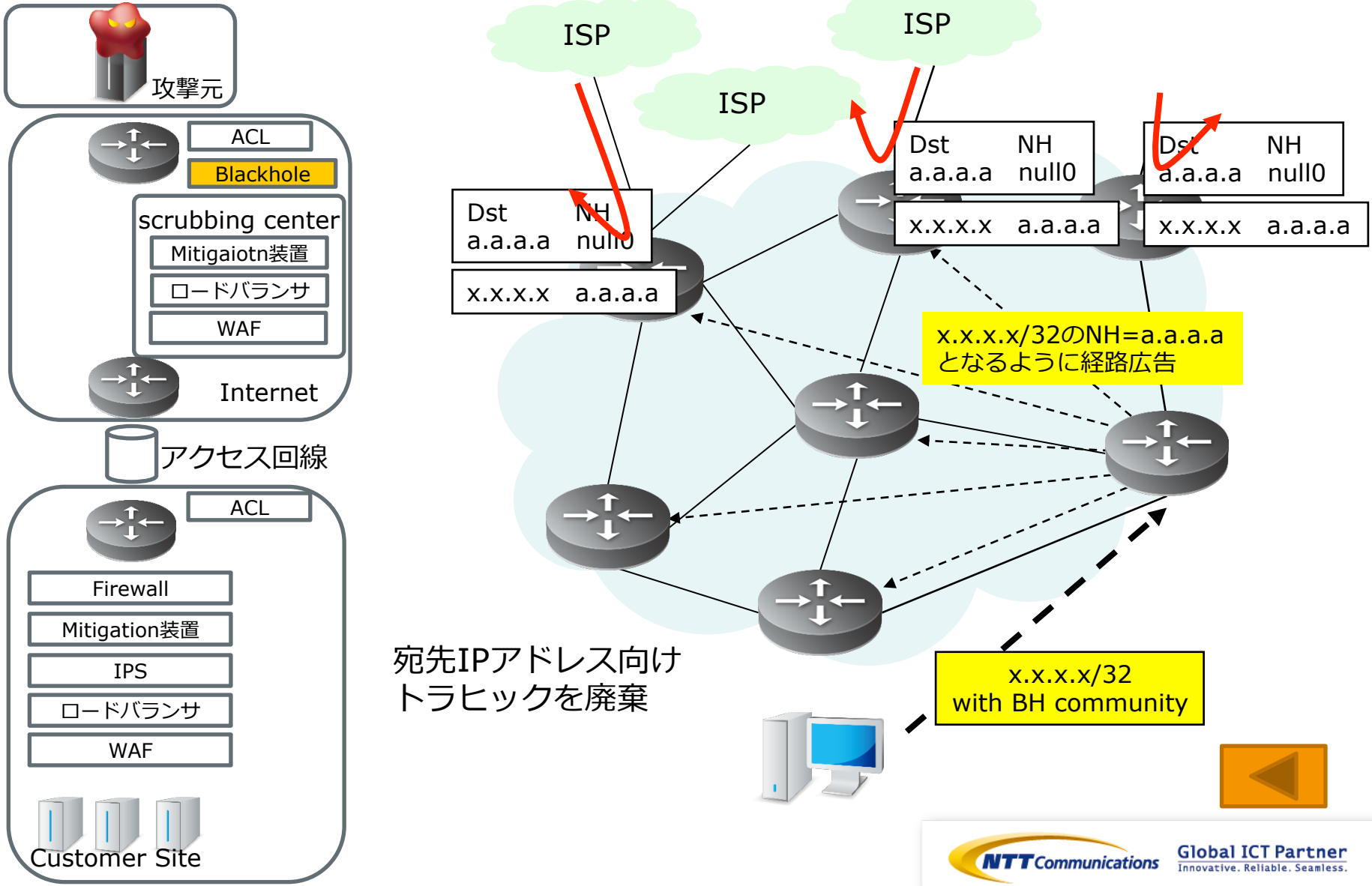
■ DDoS攻撃緩和装置

- 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



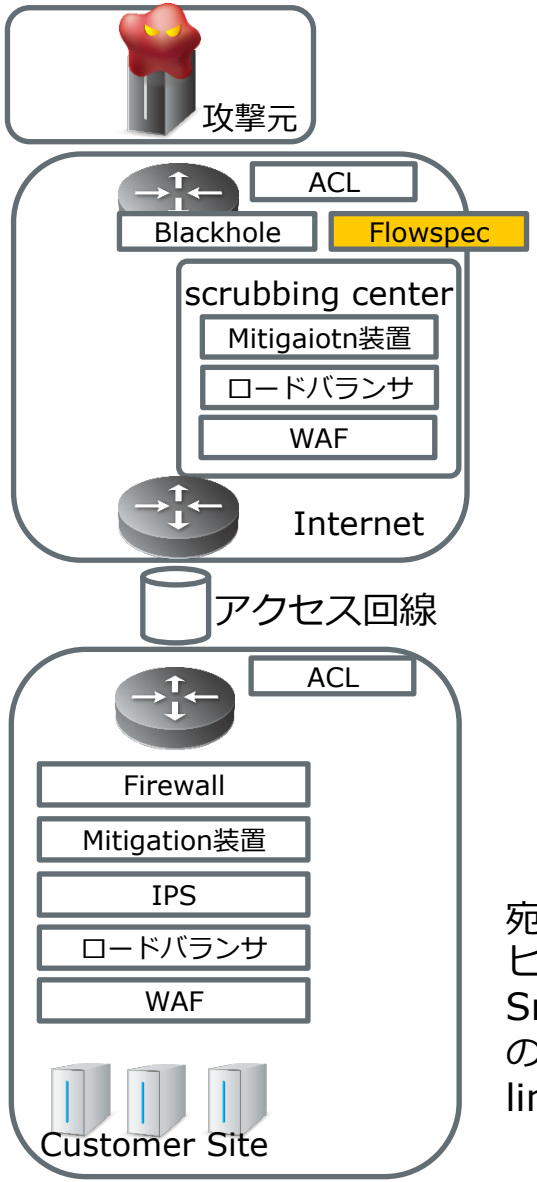
DDoS防御方法-Blackhole Routing-

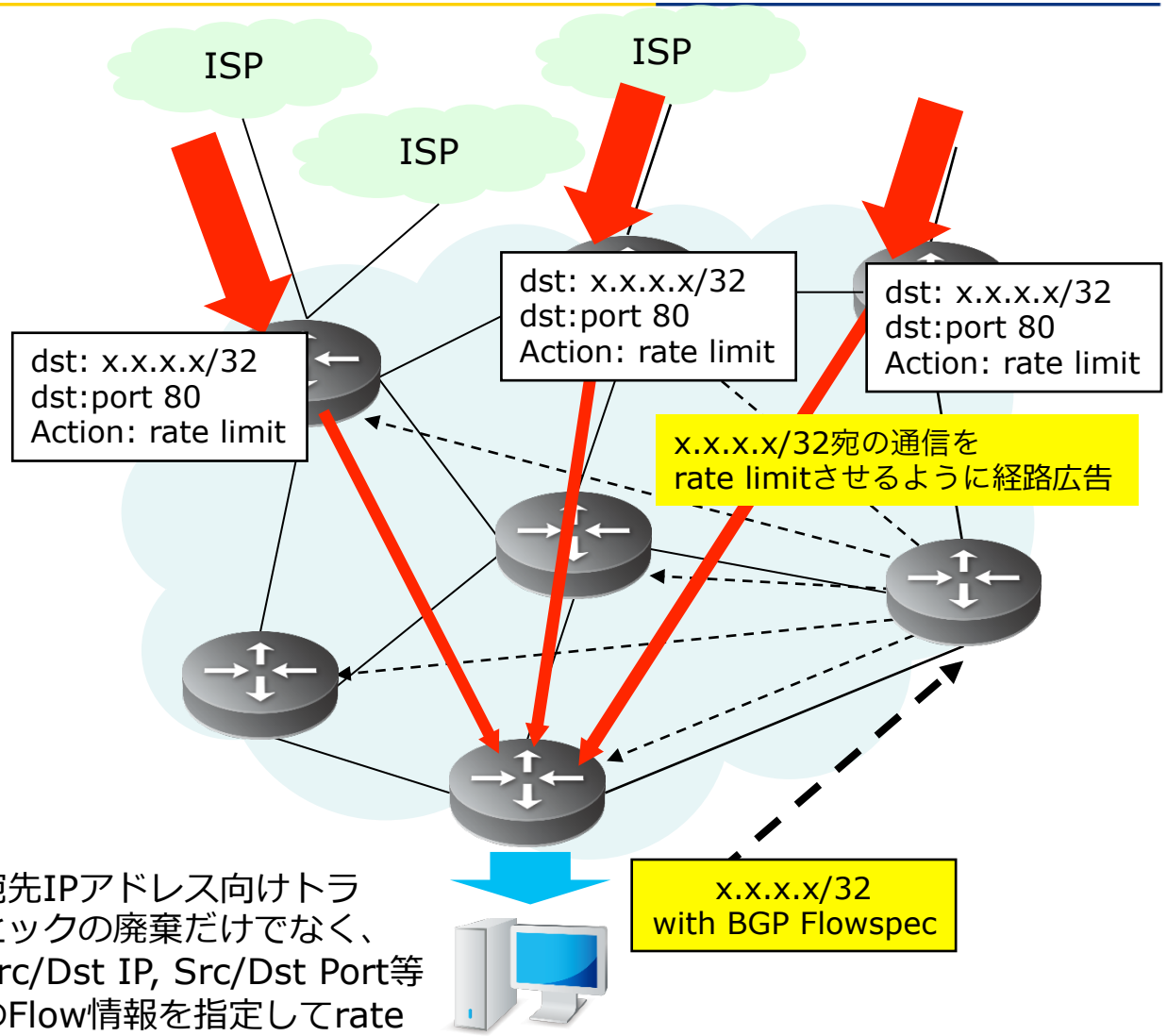
遮断 | 増設 | 緩和



DDoS防御方法-BGP Flowspec-

遮断 増設 緩和



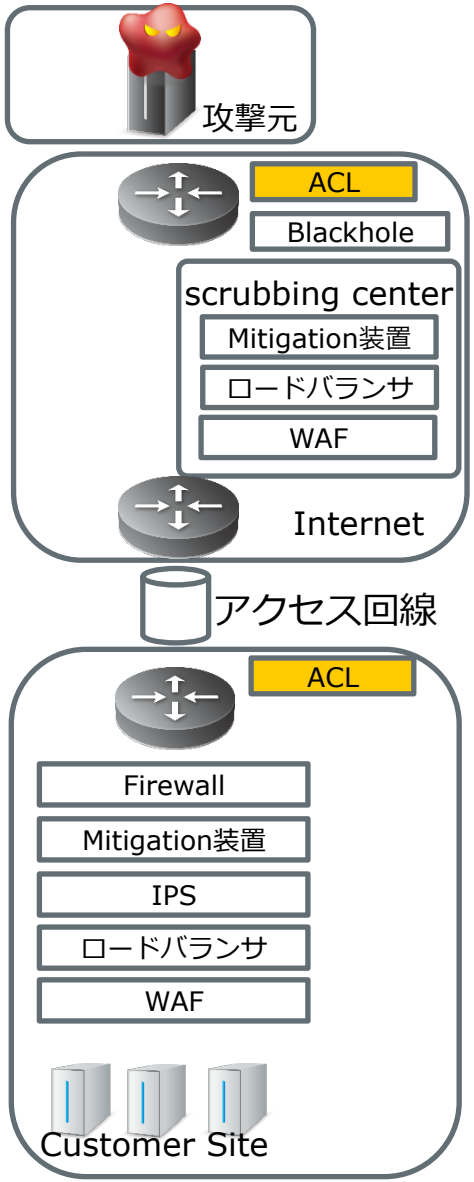


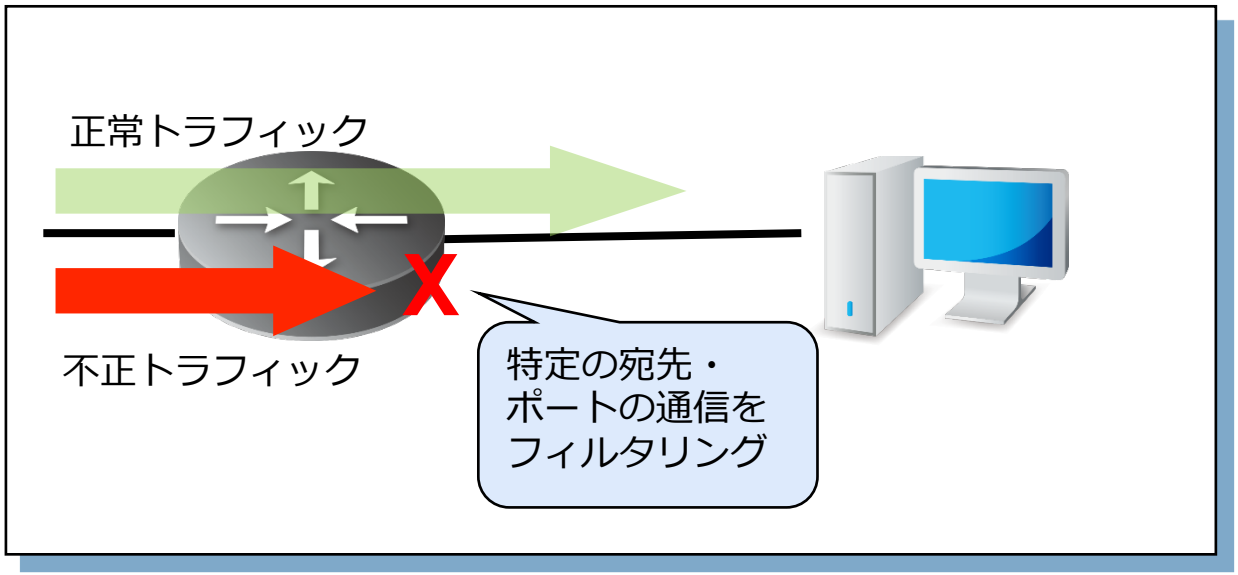
宛先IPアドレス向けトラヒックの廃棄だけでなく、Src/Dst IP, Src/Dst Port等のFlow情報を指定してrate limitやリダイレクトが可能

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

DDoS防御方法-ACL-

遮断 増設 緩和

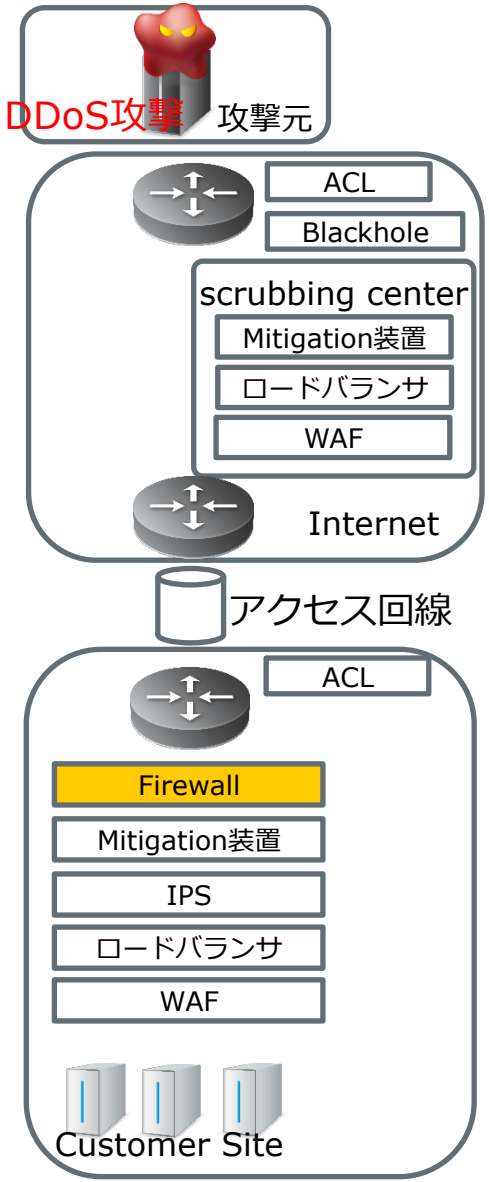




- 設定が比較的容易
- 攻撃者のフィルタリングができない場合は
  正常トラフィックも遮断

DDoS防御方法-Firewall-

緩和 | 増設 | 遮断



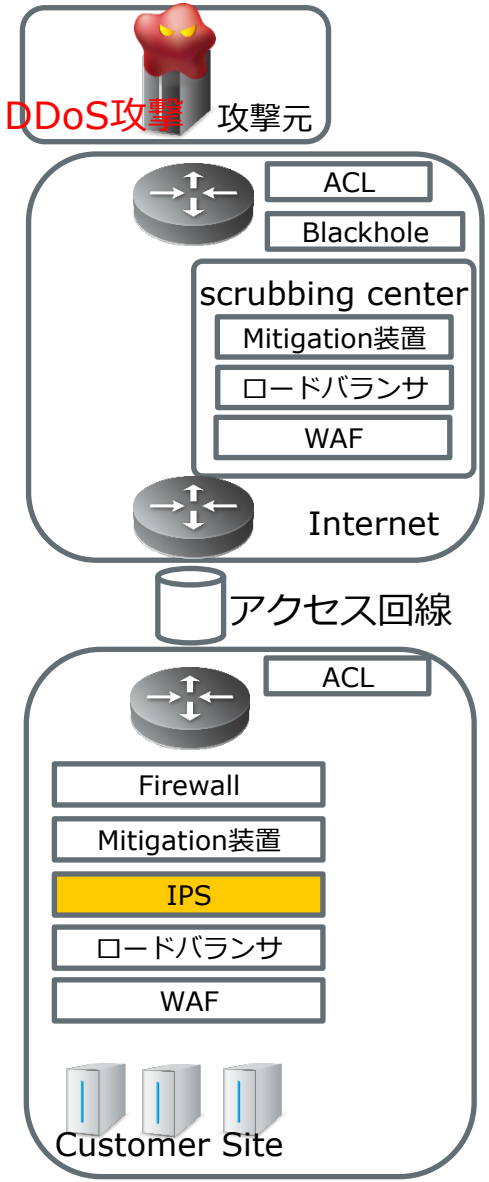
- 通常のFirewallはDDoS攻撃防御には不十分
- DDoS攻撃はFirewallで許可されたプロトコル・ポート番号を用いて実行される

- 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

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

DDoS防御方法-IPS-

緩和 | 増設 | 遮断



- IPS: Intrusion Prevention System (侵入防止システム)
- 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

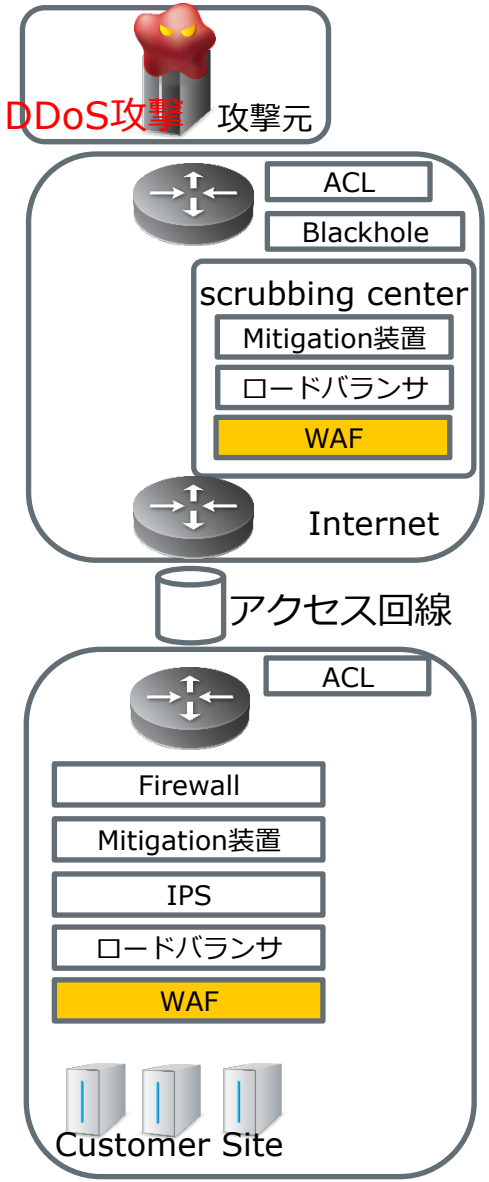
- IPSにはTCP SYN Flood攻撃などの一部のDoS攻撃手法を検出し廃棄する機能を持つ製品がある

- 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

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

DDoS防御方法-WAF-

緩和 | 増設 | 遮断



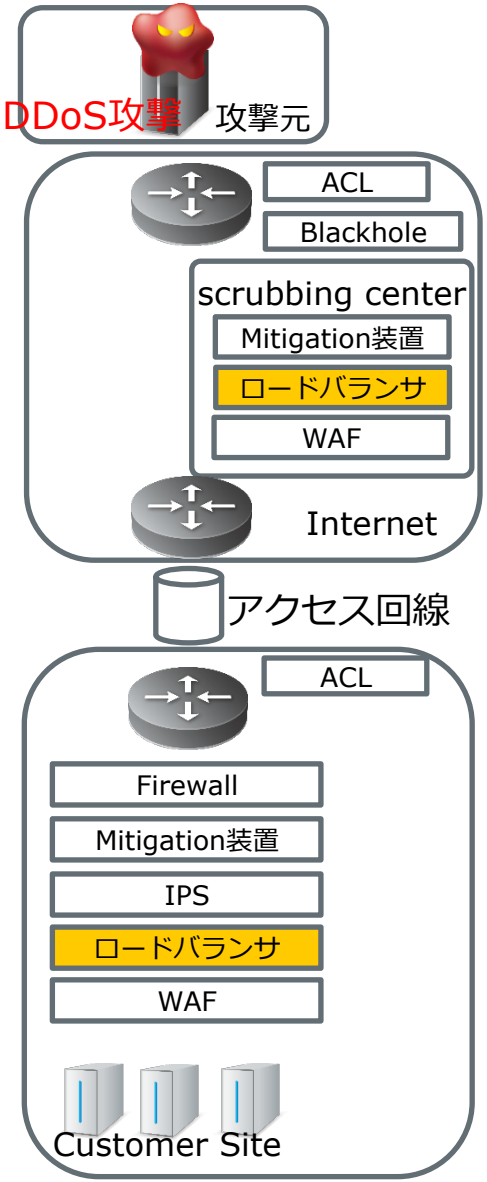
- WAF: Web Application Firewall
- 対処箇所は、クラウドおよびオンプレミス
  ＃大量攻撃時にはボトルネックになる

- 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

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

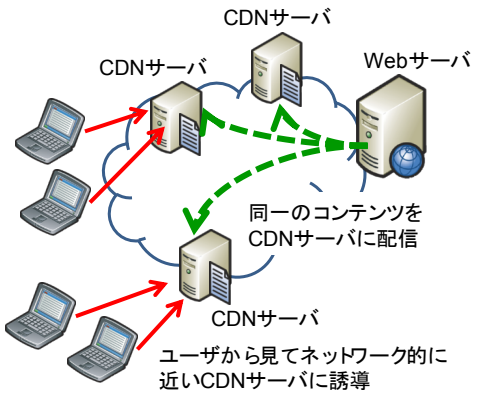
DDoS防御方法-ロードバランサ-

遮断 | 増設 | 緩和

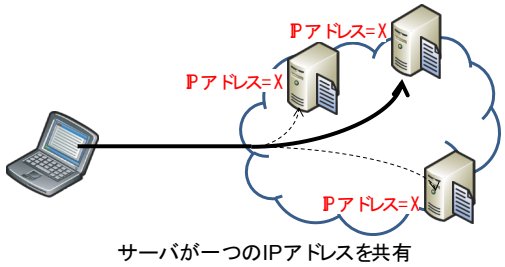


・トラフィックを負荷分散させることで、不正パケットに対するサーバ負荷を分散し、サービスの継続が可能
＃攻撃を止める訳ではなく、力技！！

・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

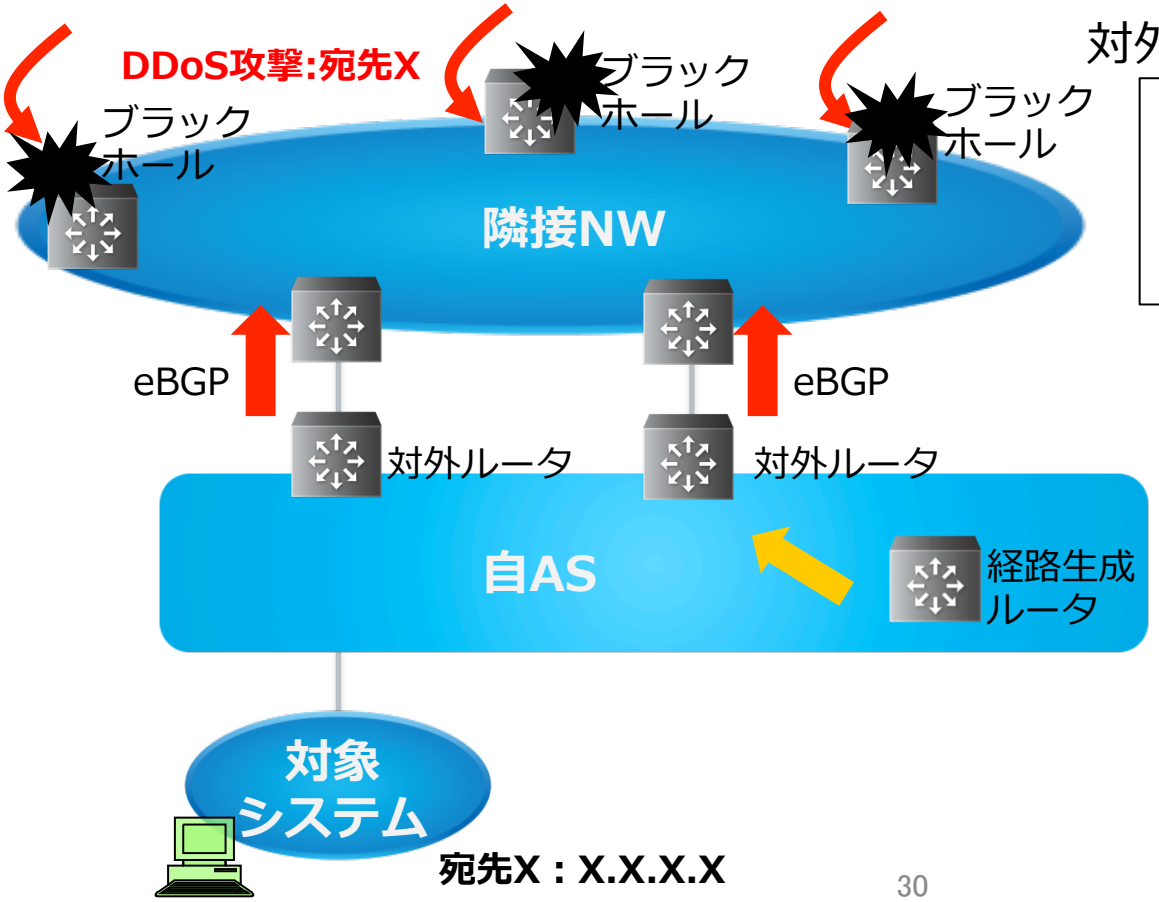
3.BGPを利用したDDoS対策

BGPを利用したDDoS対策

- BGPを利用したDDoS対策手法
  1. RTBH(Remotely Triggered Black-Hole Routing)
  2. BGP Flowspec
  3. (BGPを利用したトラフィック引き込み)
     - 直接の防御手法ではなく、クラウドタイプの防御手法で組み合わせて使われる
- なぜBGPを使うのか
  - 隣接ASへ防御を依頼するため

隣接NWにおけるRTBH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

隣接するNW(ISP/IXP)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
  - RTBH用の広告経路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

Selective RTBH

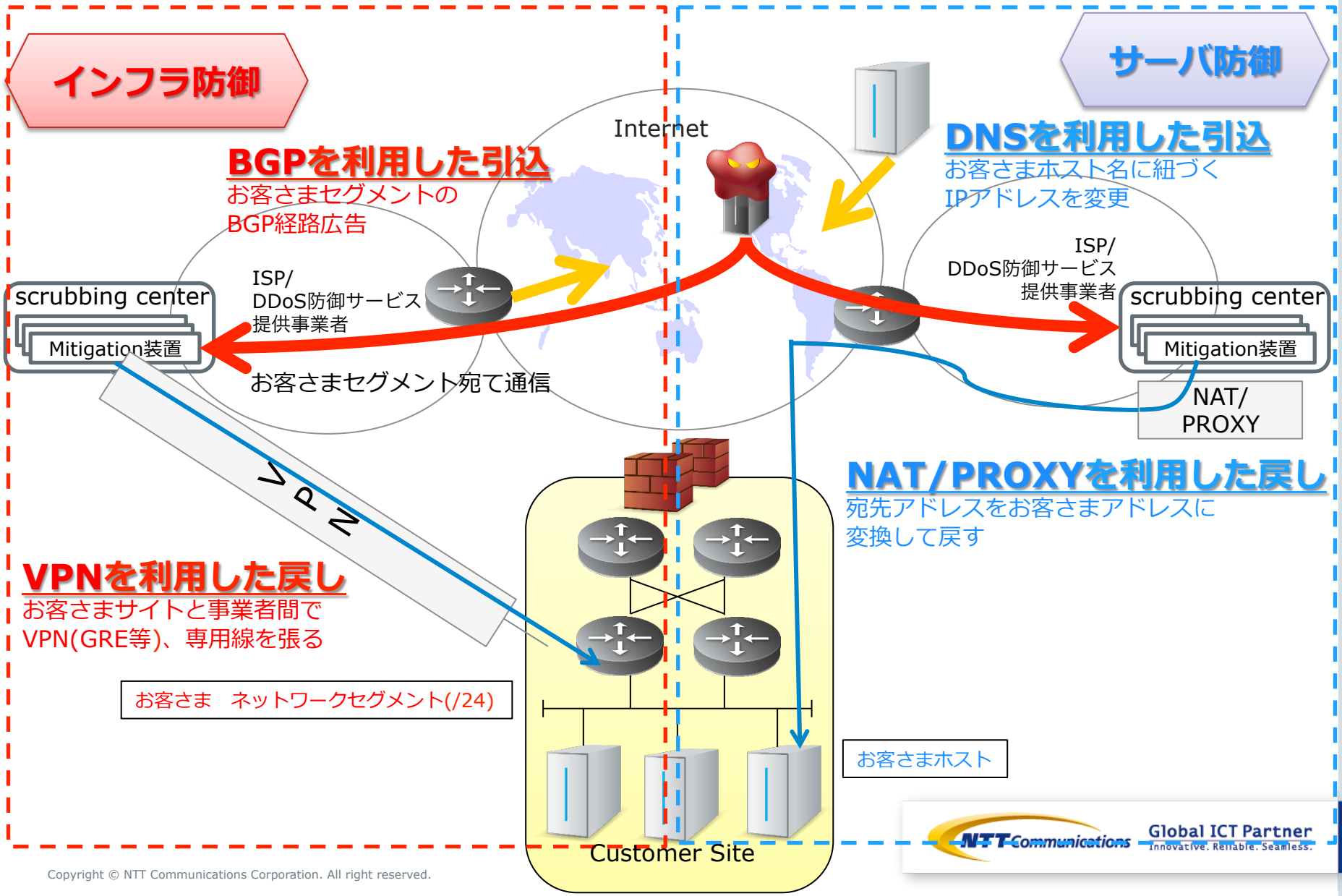
- 全網内でブラックホール化するのではなく、地域ごとや国ごとなどの特定エリアのルータでのみパケットを破棄する
- 自国内の折り返しについてはブラックホールさせたくない場合などの利用方法が考えられる
- 例 : AS2914

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

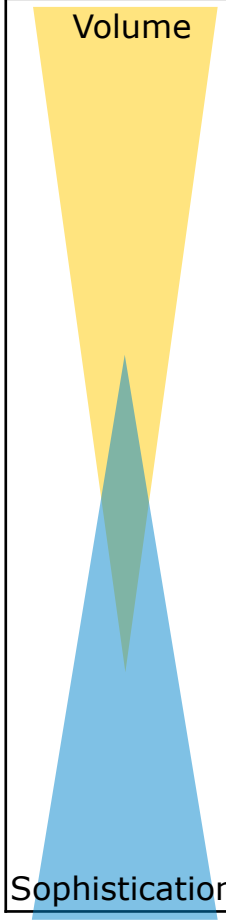
4. DDoS対策サービス

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.

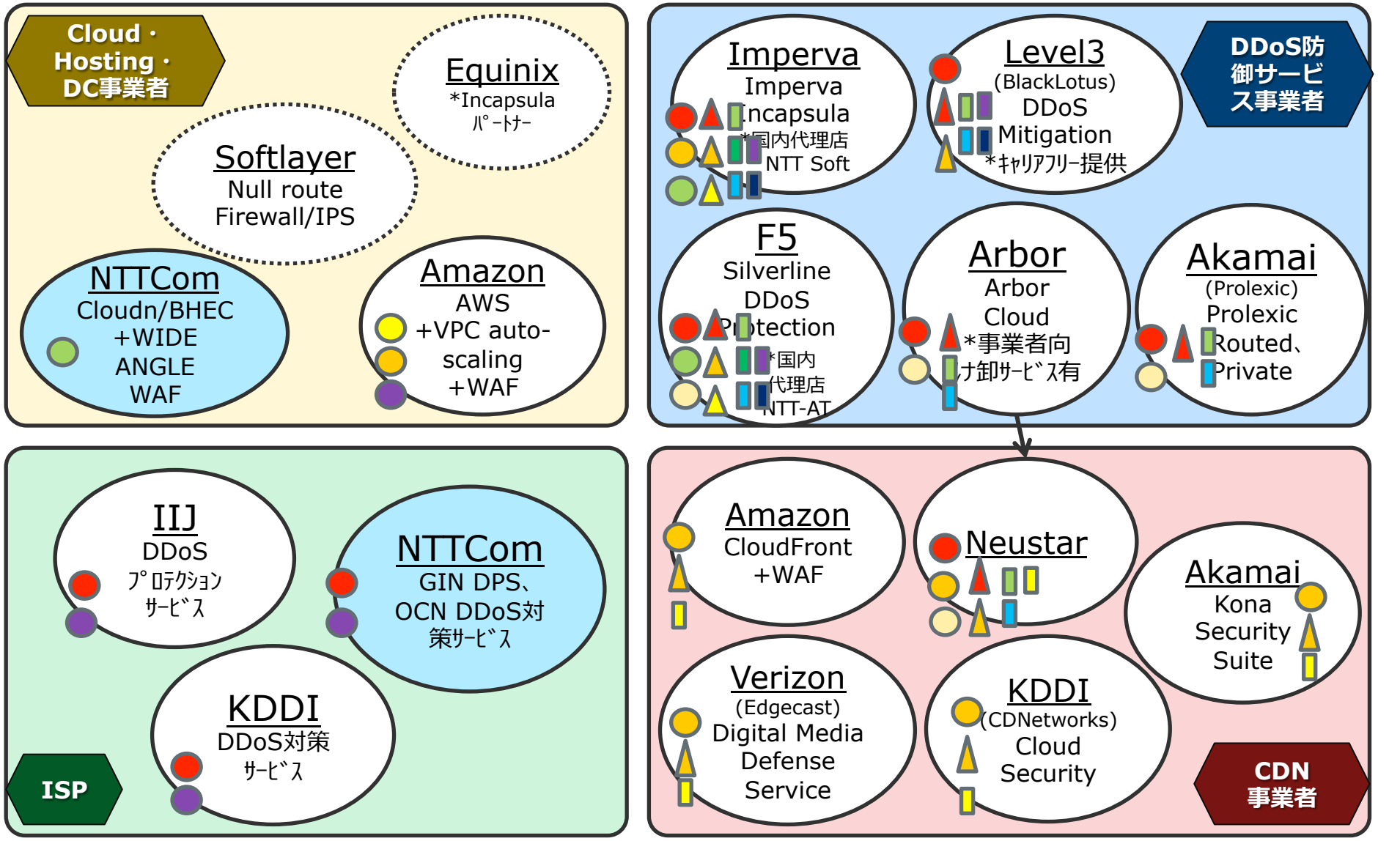
DDoS防御サービス 選択のポイント

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

NTT Communications Global ICT Partner Innovative. Reliable. Seamless.

DDoS対策サービス・提供事業者分類



防御手法

- Cloud型ｽｸﾗﾋﾞﾝｸﾞｾﾝﾀｰ
- Cloud型WAF
- auto-scaling(VM,CDN,DI
- acl/null-route
- ｵﾝﾌﾟﾚWAF
- ｵﾝﾌﾟﾚmitigation装置

引込手法

- BGP
- DNS
- IP割当

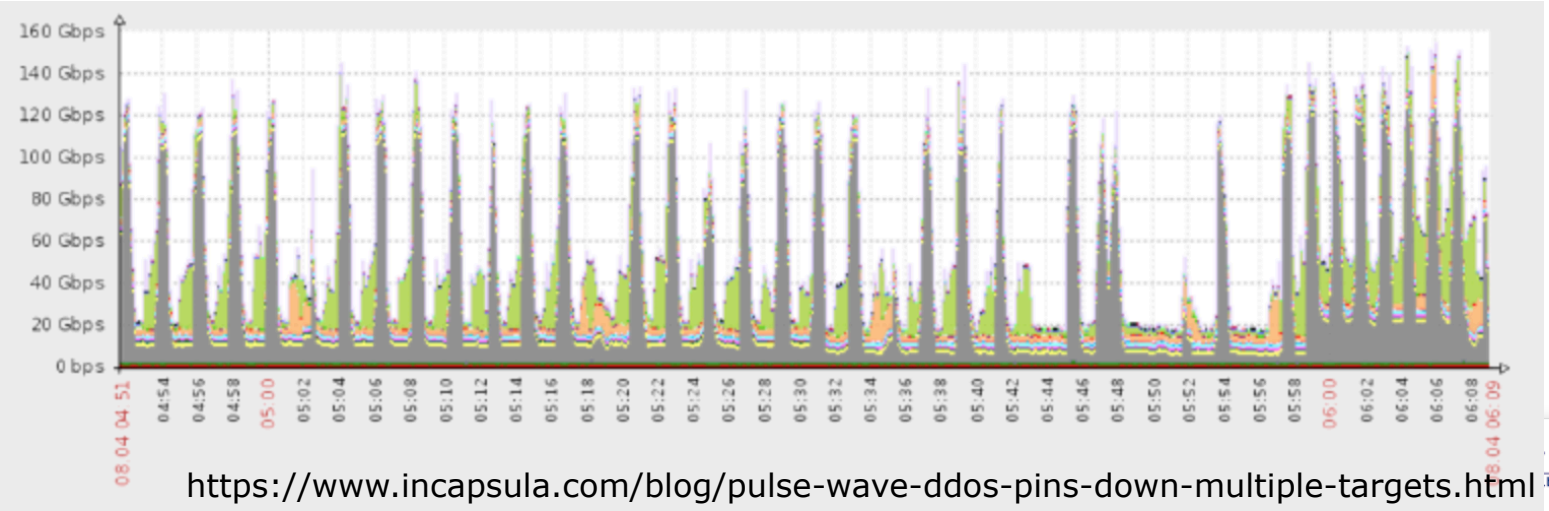
戻し手法

- GRE
- CDN
- NAT
- PROXY
- 専用線
- X-conne

5. これからのDDoS対策サービス

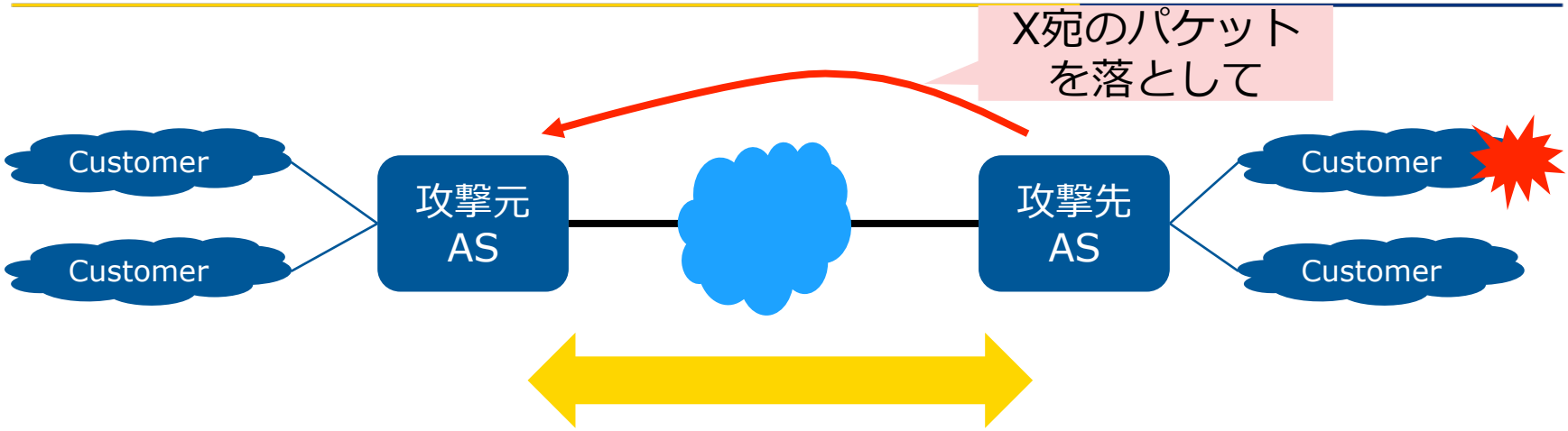
これからのDDoS対策

- パケットフィルタリングアウトソーシング
  - 1つのNWのキャパシティを超える攻撃
  - 別のNWに防御を依頼する
  - 例: NANOG71 (2017/10) における、AT&TとCenturyLinkのDDoS Peering(flowspecルールの相互流通)の発表
- セキュリティオートメーション(自動化)
  - Pulse wave DDoS
  - 人手での対策は困難



https://www.incapsula.com/blog/pulse-wave-ddos-pins-down-multiple-targets.html

防御依頼と相互信頼



- セキュリティオートメーションと相互信頼を実現する技術として、IETF にて　DOTSプロトコルが検討されている

DOTSプロトコルとは

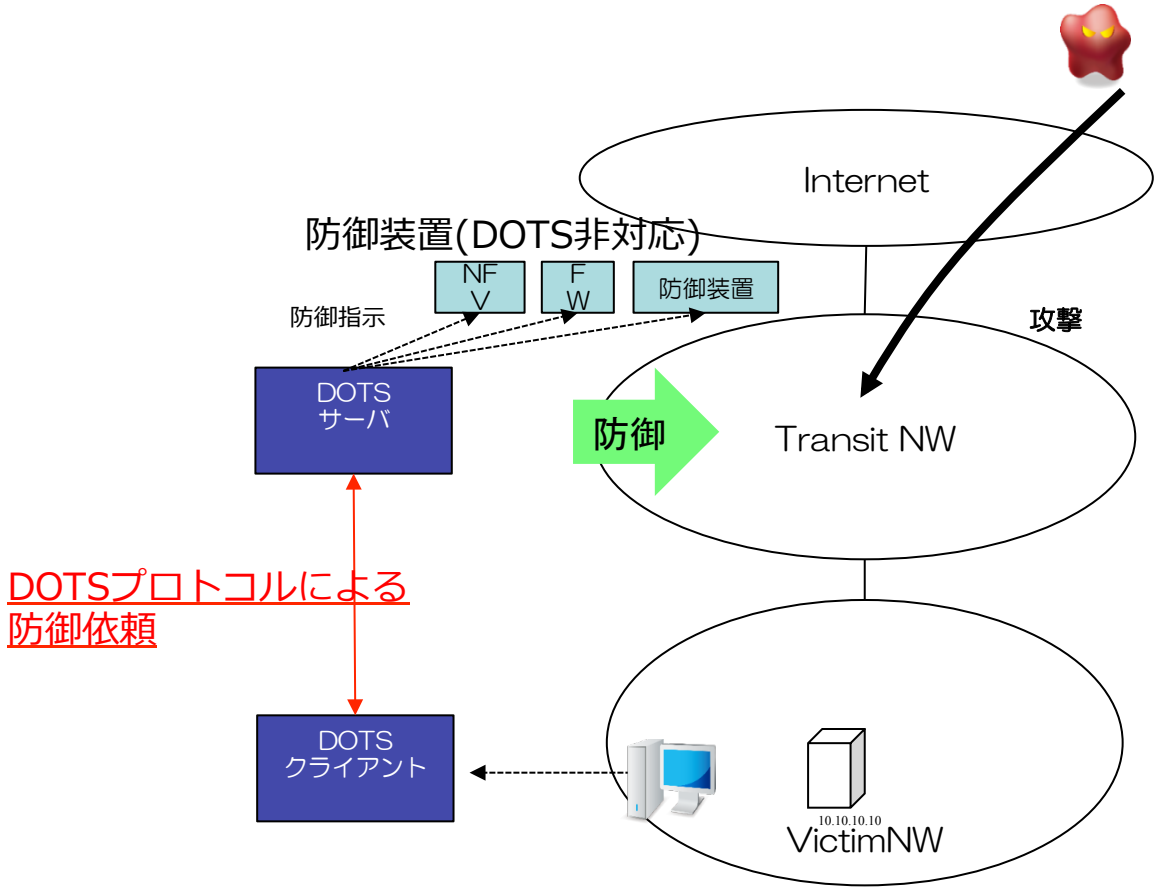
- DOTSプロトコル
  - DDoS Open Threat Signalingの略称
  - DDoS対策における組織内/間の防御依頼の標準化をめざして、DOTS WGが2015年にIETFで発足
- 既存のDDoS対策の問題点
  - インターネットへつながる回線が輻輳させられてしまうほどの大規模な攻撃であった場合には、上流のサービスプロバイダや専門のDDoS対策事業者に防御(ミチゲーション(緩和)やスクラビング(除去)と呼ばれます)を依頼する他に、回線の輻輳を避ける方法がない
  - しかし、防御依頼を受け付ける機械的な窓口がなく、人間がメールあるいは電話対処するため、防御を発動するまでの時間がかかり、その間は攻撃が成立し続けてしまう

DOTSプロトコルの動き

- DOTSプロトコルの動き方
  - 利用者側のDOTSクライアントから提供者側のDOTSサーバに対して、攻撃を受けているIPアドレスなどの情報とともに防御を依頼
  - 依頼を受けたDOTSサーバ側は、認証および防御依頼のバリデーションを実施した上で、DDoS対策を実施
- DOTSプロトコルのメリット
  1. 人間を介さない防御受付のインタフェースが規定されることで、DDoS対策の自動化が可能になる
  2. 複数の対策事業者に対して共通のプロトコルで防御依頼をすることができるようになる
  3. 別の対策事業者に防御依頼をするような事業者間連携を実現できる

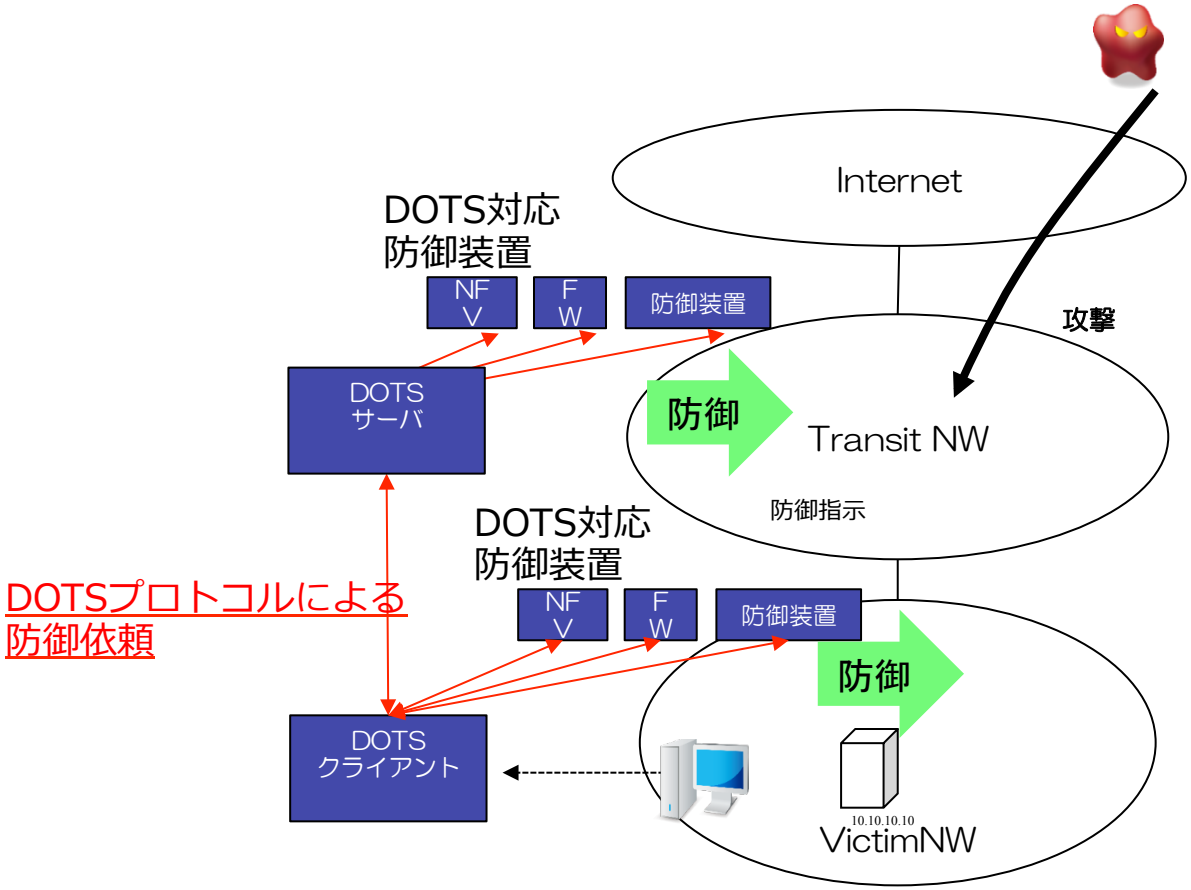
DOTS利用シーン その1

■ 人間を介さない防御受付インタフェースによるDDoS対策自動化



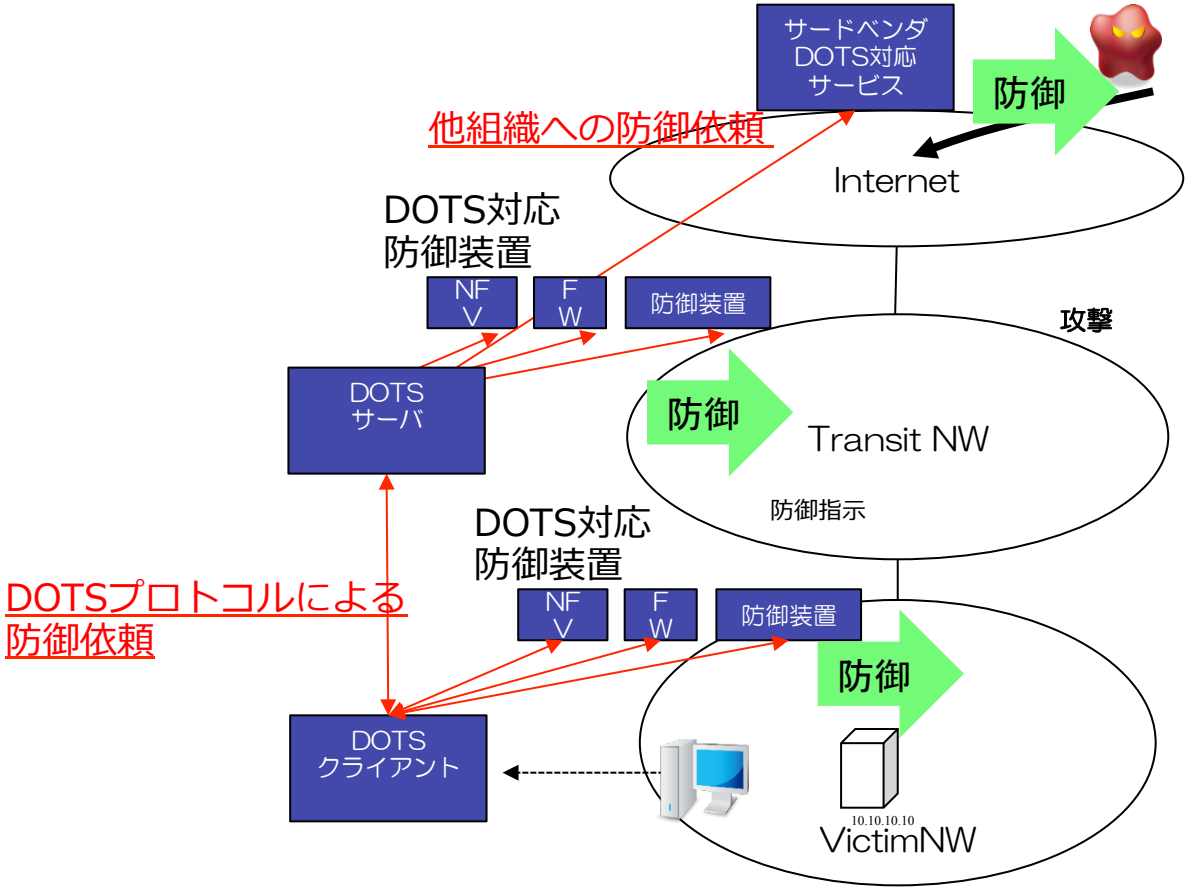
DOTS利用シーン その2

■ 防御装置(DOTS対応)への防御依頼の共通化



DOTS利用シーン その3

■ キャパシティオーバの際に別の対策事業者に防御依頼をするような事業者間連携が実現できる

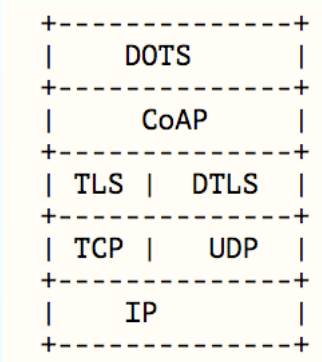
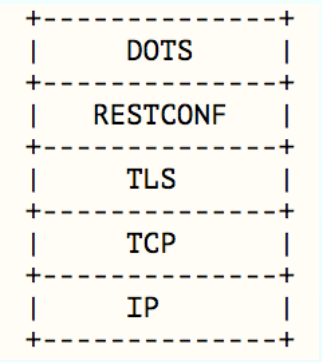


業界動向

■ (私見です)

Arbor	2016年9月に観測された1Tbps規模のDDoS攻撃を背景に、他のDDoS対策事業者(AKAMAI/Prolexic)との連携を模索している。WGにて精力的に活動
AKAMAI/ Prolexic	早期のdots プロトコル仕様確定に期待 「DOTS対応をDDoS対策サービスの選び方に加えるべき」
Radware	自社サイトにて、dots プロトコルへの対応を明言
Verisign	DDoS対策サービスを提供。Arborとの連携を想定に、WGにて精力的に活動
Cisco	Cisco の NW機器に dots のクライアント機能を入れる狙い。CPEやIoTデバイスの防御がメインのユースケースか。WGにて精力的に活動
Orange	キャリアの視点で、各DDoS対策サービスを利用したい考え。Ciscoと共に、マネージドCPEを出す狙いか

DOTS プロトコルスタック

	Signal Channel	Data Channel
スタック		
アプリケーション	CoAP	RESTCONF
セキュリティ	TLS/DTLS	TLS
トランスポート	TCP/UDP	TCP
目的	(攻撃を受けているときに)防御を依頼するチャンネル	(攻撃を受けていないときに)防御をセットアップするチャンネル
クライアント→サーバ	・防御依頼(開始/停止) ・攻撃を受けているIPアドレス・プレフィックス ・防御状況の確認	・ネットワーク情報の登録 ・テレメトリ情報
サーバ→クライアント	・防御状況の報告	・テレメトリ情報

Go implementation of DOTS

Demo scenario:
Enabling DDoS Protection in an upstream network by DOTS protocol

https://github.com/nttdots/go-dots

DOTS is:

- **D**DoS **O**pen **T**hreat **S**ignaling
- Automation and Standardization of signaling for DDoS protection
- “ask for help!” from a victim to an upstream provider
  - inter-organization / including authN and authX in spec

What you can see in this demo:

- A DOTS client sends a mitigation request to a DOTS server over DOTS signal channel.
- The DOTS server receives and validates the request, then starts mitigation by kicking a blocker
- In this demo, the blocker is a gobgp server which triggers “blackhole routing” in a service operator's network

Signal Channel

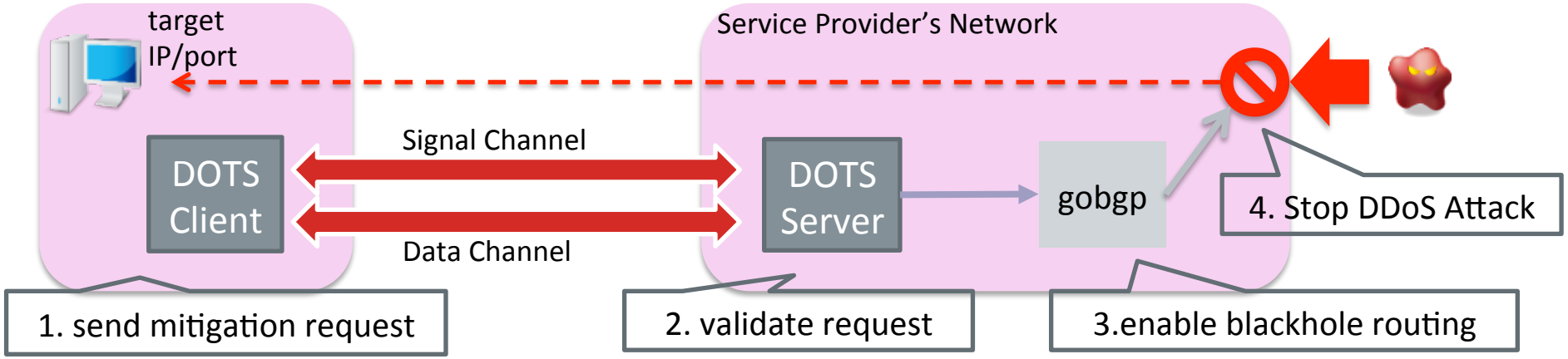
```
+--------------+
|     DOTS     |
+--------------+
|     CoAP     |
+--------------+
| TLS |  DTLS  |
+--------------+
| TCP |   UDP  |
+--------------+
|     IP       |
+--------------+
```

Data Channel

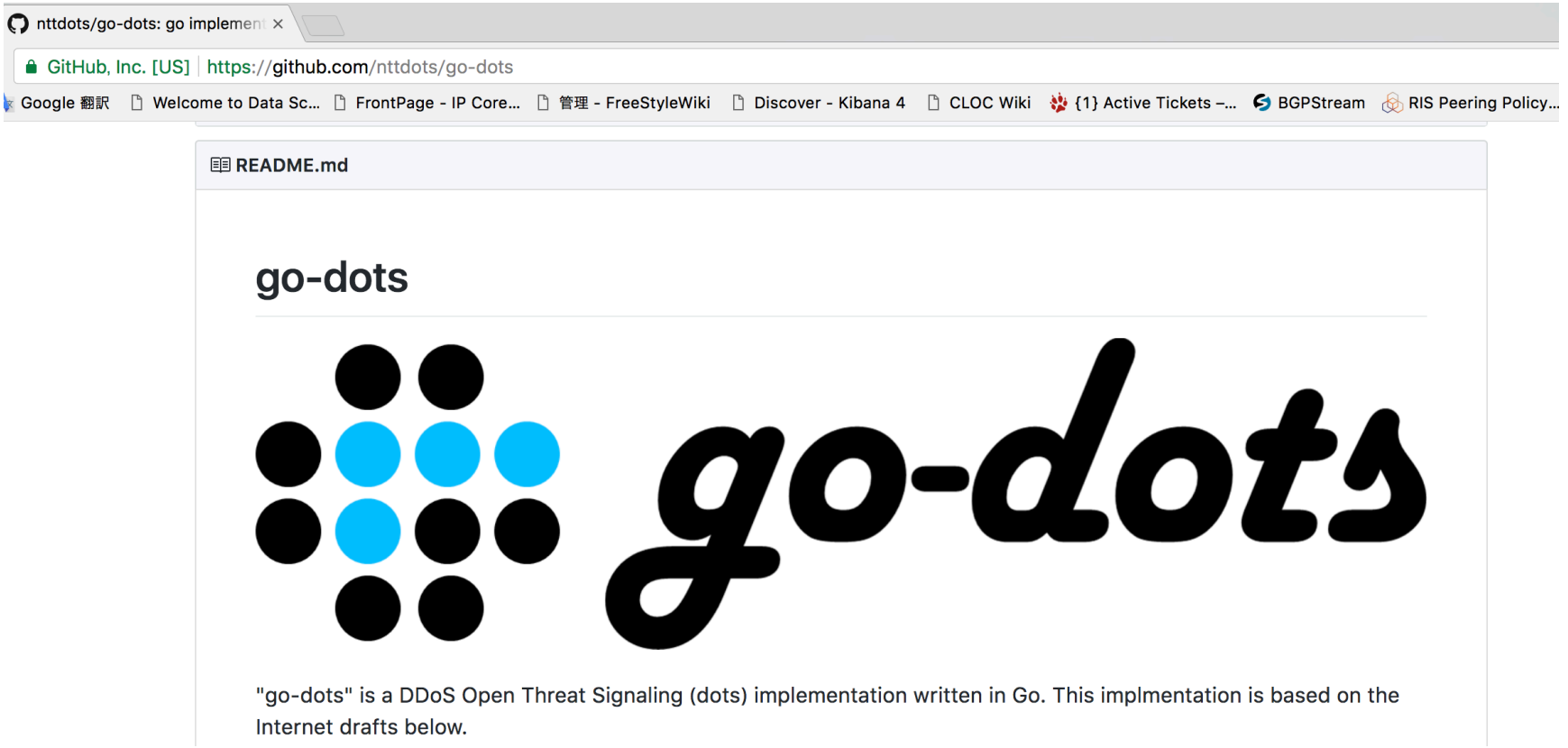
```
+--------------+
|     DOTS     |
+--------------+
|   RESTCONF   |
+--------------+
|     TLS      |
+--------------+
|     TCP      |
+--------------+
|     IP       |
+--------------+
```

Mitigation Request Model

```
module: ietf-dots-signal
    +--rw mitigation-scope
       +--rw scope* [mitigation-id]
          +--rw mitigation-id          int32
          +--rw target-ip*             inet:ip-address
          +--rw target-prefix*         inet:ip-prefix
          +--rw target-port-range* [lower-port upper-port]
          |  +--rw lower-port     inet:port-number
          |  +--rw upper-port     inet:port-number
          +--rw target-protocol*       uint8
          +--rw fqdn*                  inet:domain-name
          +--rw uri*                   inet:uri
          +--rw alias*                 string
          +--rw lifetime?              int32
```



オープンソース実装(世界初)



IETF ハッカソン

- IETF99 プラハ (2017年7月)
  - オープンソース実装の改善を実施
  - Best Name Awardを受賞

- IETF100 シンガポール (2017年11月)
  - NCC Groupの実装と相互接続試験を実施
  - Best Open Source Award を受賞

まとめ

- DDoS対策もルーティングセキュリティも、事業者間での合意や連携が重要
- 新しい提案が次々と出てきていますが、一緒に試していきましょう