NRIセキュアテクノロジーズ

Internet Week 2016

【T1】知って納得！企業のDDoS対処戦略～基礎から実践まで～

1.DDoS対処の戦術と戦略

2016年11月29日

NRIセキュアテクノロジーズ株式会社
サイバーセキュリティサービス事業本部

セキュリティコンサルタント　中島　智広

〒100-0004
東京都千代田区大手町一丁目7番2号 東京サンケイビル

目次

1.はじめに

DDoS対策の悩ましい性質

DDoS対策は保険のようなもの、極力コストは掛けずに対策したい

規模、頻度が不定

ニュースメディアは大規模な事例を取り上げるが、自社が遭遇する規模はわからない。

備えても狙われないかもしれない。一度狙われたからと言って再び狙われるわけでもない。

企業やシステムの特性を鑑みて判断

掛け捨て

何かしらの製品やサービスを導入する場合、活用せずとも月額の維持費用が発生し続ける。

費用を抑えられれば、情報漏洩対策など、より喫緊の脅威への施策に費用を回せる。

事業全体の支出入とのバランスで判断

自然復旧

時間がたてば自然復旧する。永続的に続くものではなく、短時間のものが割合的には多い。

事業影響が許容範囲であれば受容することも方法のひとつ。

事業影響と許容時間を鑑みて判断

戦略の選択

中身を知って、システム毎に最適なものを、賢く選ぶ

CDN/
スクラビングサービス
(DDoS対処専門事業者)

＋

有事運用

既存契約
+Mitigationオプション
(ISP/IDC/SI事業者)

＋

自社対策と有事運用

既存契約内での対処
(ISP/IDC/SI事業者)

＋

自社対策と有事運用

本プログラムの焦点

ネットワーク帯域を溢れさせるDDoS攻撃に対し、
既存インフラを前提に各事業者と手を取り合って取り組む対処の「いま」を共有

■アプローチ

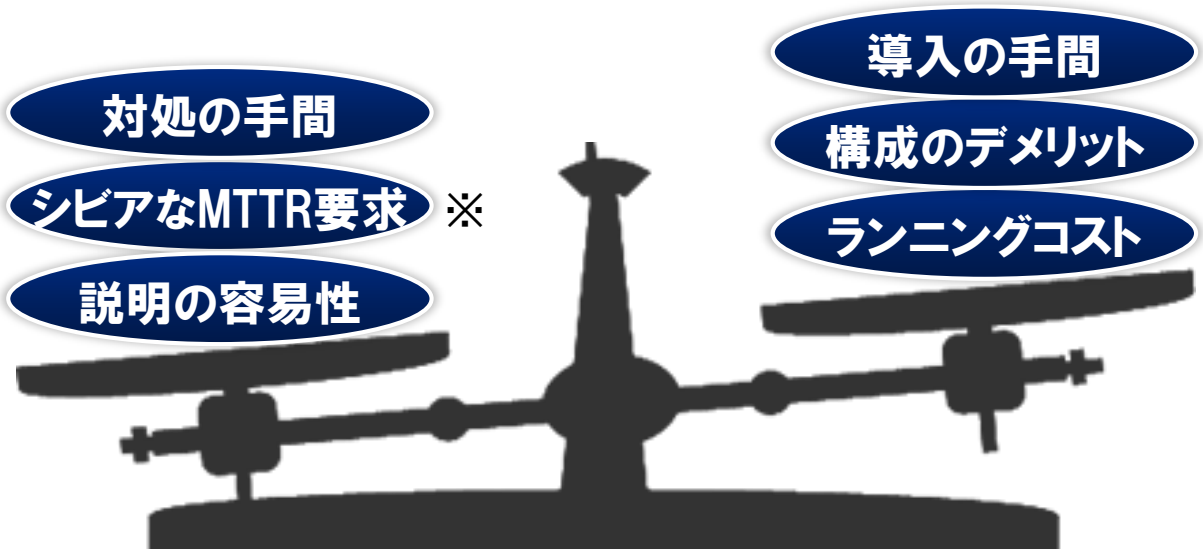
- 対処技術とその適用を知る
- 自らの対処範囲と戦略を見極める
- 自らの現状を確認し必要な備えをとる
- 事業者とのコンセンサスにより効果的に対処する

利用者
（顧客）

各事業者
（ISP、IDC、IXP、SIerなど）

松（CDN、スクラビングサービス）との使い分け

コストやニーズ、構成の制約に合致するなら「松」を利用する方が容易



※MTTR(Mean Time To Repair):障害から復旧までの時間

松への言及（少しだけ）

■CDNは意外と高くない、賢く選んで使えば費用対効果は高い

- World Wideの大規模なものから、国内を中心とした中規模なものまで選択肢がある
- 廉価なものでは月額20万円弱から(トラヒック従量課金※)
  ※一般な95%ルールでは散発的なDDoSトラヒックは課金から外れる
- 規模によらず相応の分散効果は確実に見込め、攻撃しにくく、されにくくなる
- 低コスト化、耐障害性を目的とした複数事業者の組み合わせ（マルチCDN）も選択肢

■スクラビングサービスは万能ではない

- 保有しているサービス資源の限りでの対処、ISPなどの既存事業者と同じベストエフォート
- 構成上、相応のデメリットや懸念がある（特にAlways-On構成）
  - 通信距離増による遅延（レイテンシ）の増加はどうか？
  - インフラを共有する他社への攻撃は本当に無影響か？
  - 障害ポイントの増加、運用トラブルの話はどうか？
- 国外の事業者が多いが意識や文化の壁はないか？
  - 説明責任や情報開示：障害発生時に要求する水準の報告書や是正計画は出てくるか？
  - 借用に対する考え方：日本時間の平日日中にメンテナンスは行われないか？

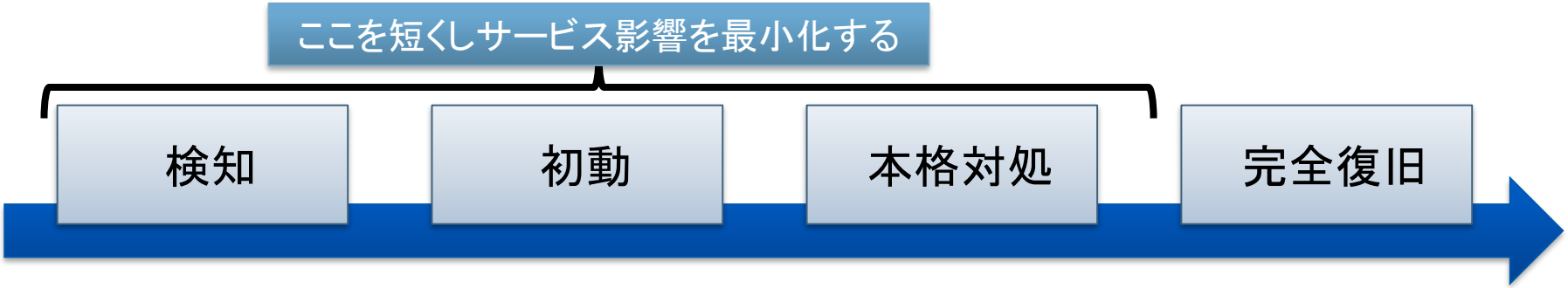
戦術とは？戦略とは？

■戦術

- ●技術を中心とした対処の方法論
  - ▪ 対処する主体とポイント(誰が、どこに)
  - ▪ 対処手法(どのようにして)

■戦略

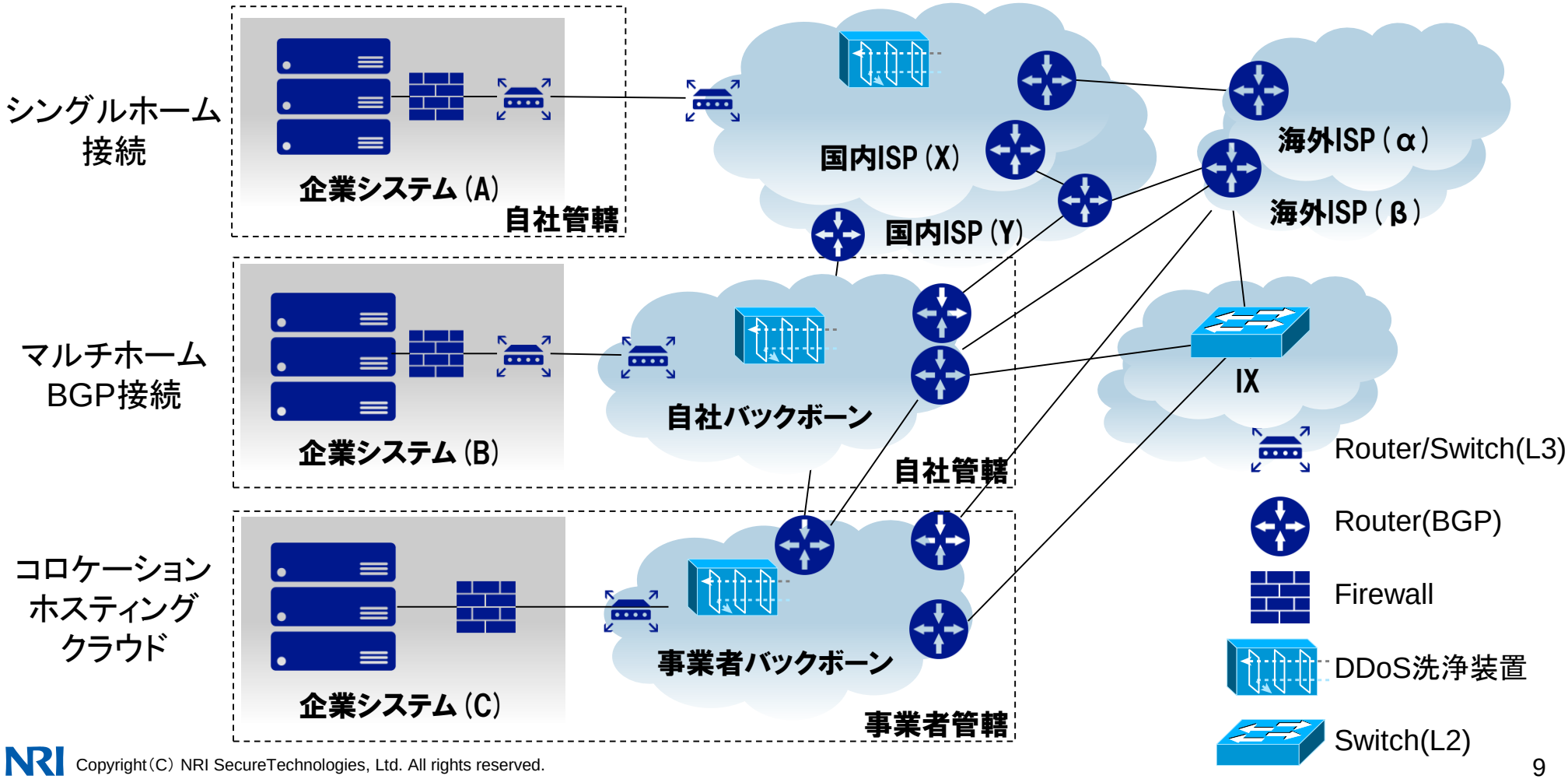
- ●戦術をいかに適用し、サービスを継続するかの方法論
- ●MTTRを最小化するための運用、そのために必要な準備



戦術と戦略を把握し、できることから少しでも対策を進めることがゴール

企業システムのインターネット接続形態

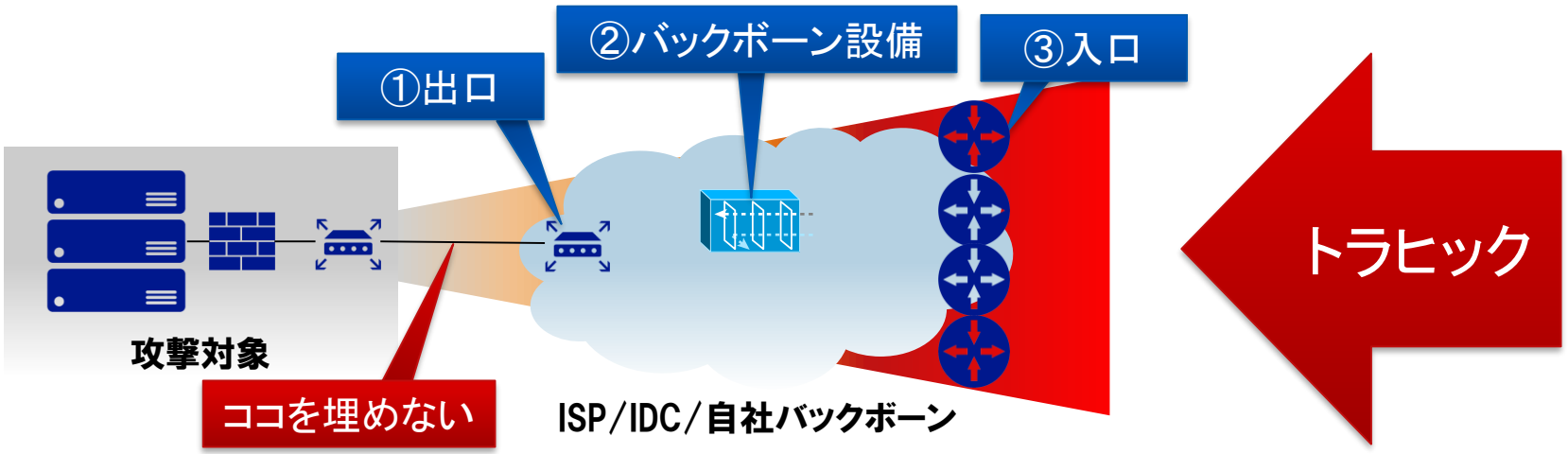
インターネット接続形態により自社と事業者で戦術、戦略の担当範囲が異なる



2.DDoS対処の戦術

対処のポイントと手法

対外接続回線を埋めないため、ひとつ上流のネットワークでの対処が基本となる



①出口(顧客収容口)
収容するインターフェイス毎に適用、性能問題などの影響がない範囲で柔軟に設定しやすい

②バックボーン設備
バックボーン内の専用機器で機械的に対処、処理可能な規模であれば利用しやすい

③入口(対外接続点)
BGPルータのルーティングでの対処が基本、処理性能や運用影響からACLは設定しづらい
ただし今後は・・・(後述)

Network ACLベース ※

アルゴリズムベース

ルーティングベース

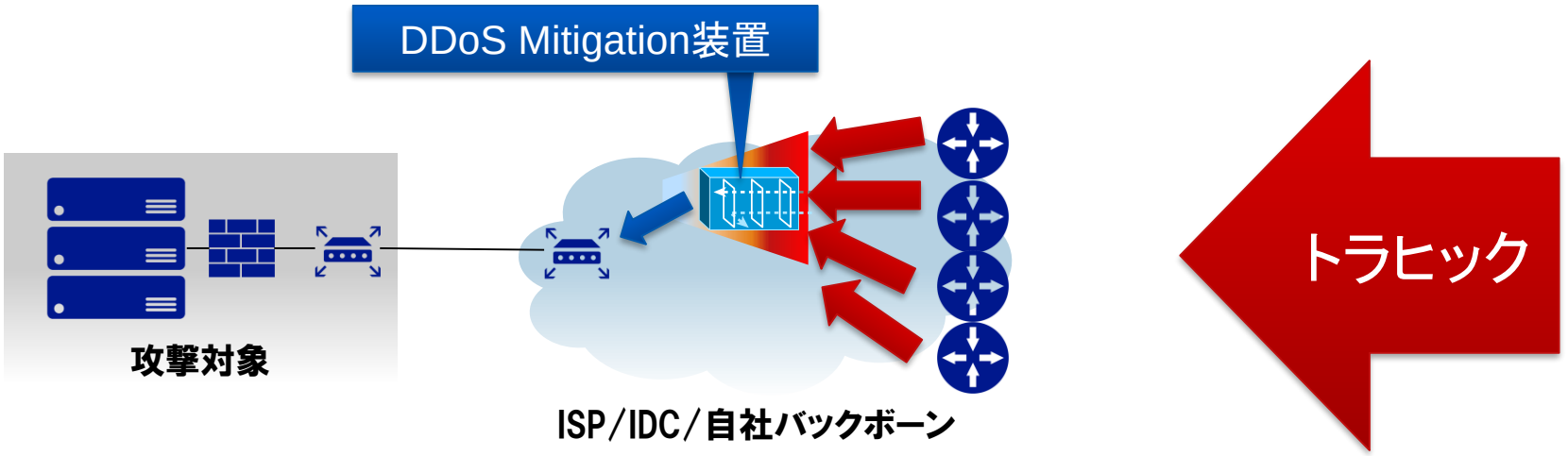
※一般にL3(送信元/宛先IPアドレス)、L4(プロトコル、ポート番号、フラグ)の組み合わせで許可/不許可を定義

機械と人間（アルゴリズムとマニュアル）

	機械(アルゴリズム)	人間(マニュアル)
判定手法	トラヒック解析 レピュレーション 機器毎の独自アルゴリズム	人の目で見て総合的に判断
処理手法	悪性トラヒックを選別して破棄 シェーピング	ACL(IPアドレス、ポート) ルーティング 機械との組み合わせ
対処時間	即時(有効化後)	10分～30分程度
処理可能規模	機器のスペックが性能限界 一般に数Gbps～100Gbps/1台	特になし、ベストエフォート
費用	一般的には要オプション料金	一般的には追加費用無し
前頁との対応	②バックボーン設備	①出口(顧客収容口) ③入口(BGPルータ)

オプション料金は必要なものの、機械による対処にはメリットが多い

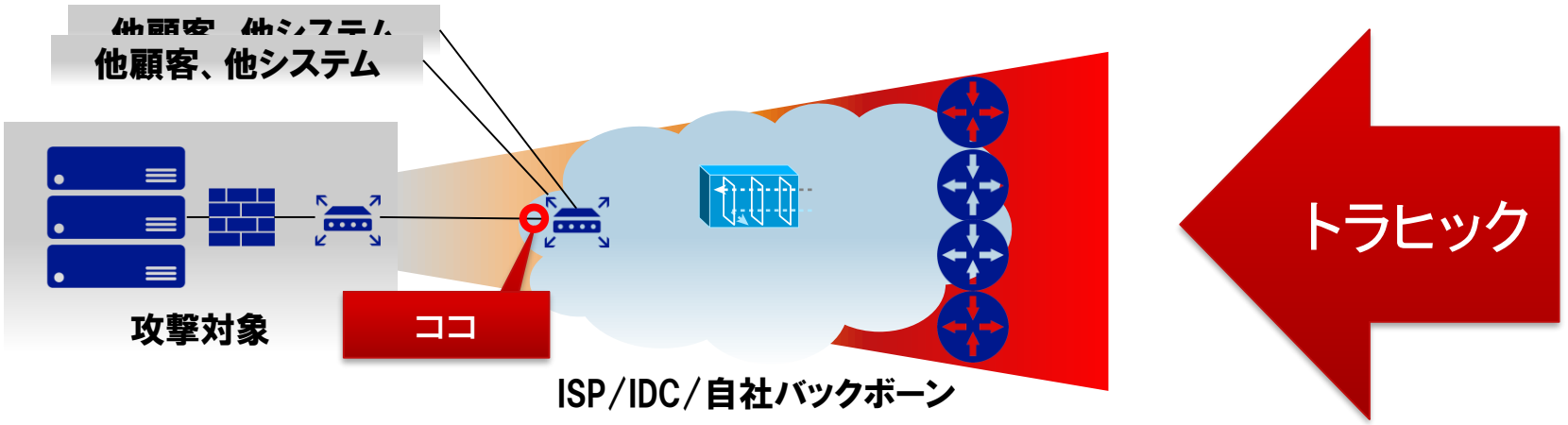
機械で対処：バックボーン設備のDDoS Mitigation 装置



- 専用のアプライアンスを用いてDDoSトラヒックをクリーニングする仕組み
  - 必要なときに機器にトラヒックを引きこんで対処(オフランプ構成)
  - 引き込みにはダイナミックルーティングを用いる

もっとも迅速に影響少なく対処可能な手段、できれば使えるようにしておきたい

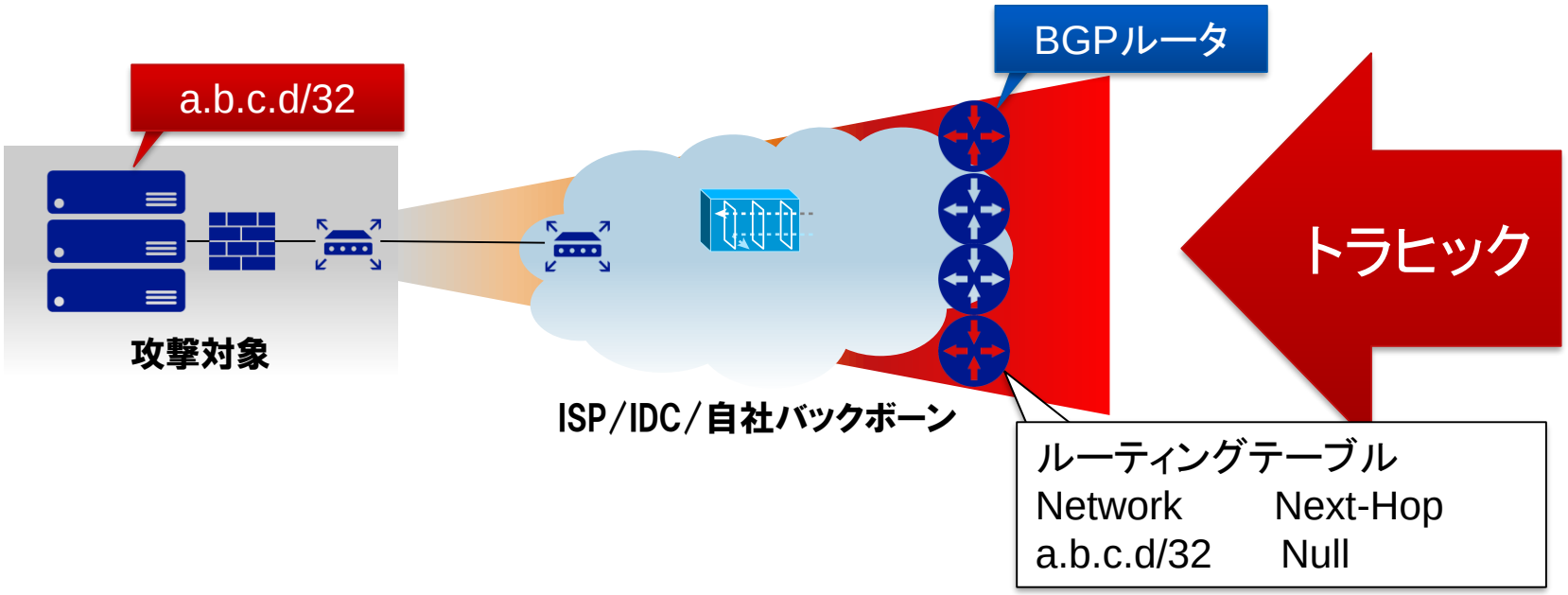
出口で対処：Egress Filtering



- 収容ルータのインターフェイスにNetworkACLを定義してフィルタリング
  - 事業者に依頼、あるいは事業者の提供するWebインターフェイスから設定
  - 契約毎のインターフェイスに設定するため、他顧客、他システムに影響を与えにくい
  - DDoSに悪用されるサービスが不要であれば、予め遮断ACLを設定しておくことも有効

サービスメニュー化されていない場合でも、相談すると受け入れてもらえることは多い

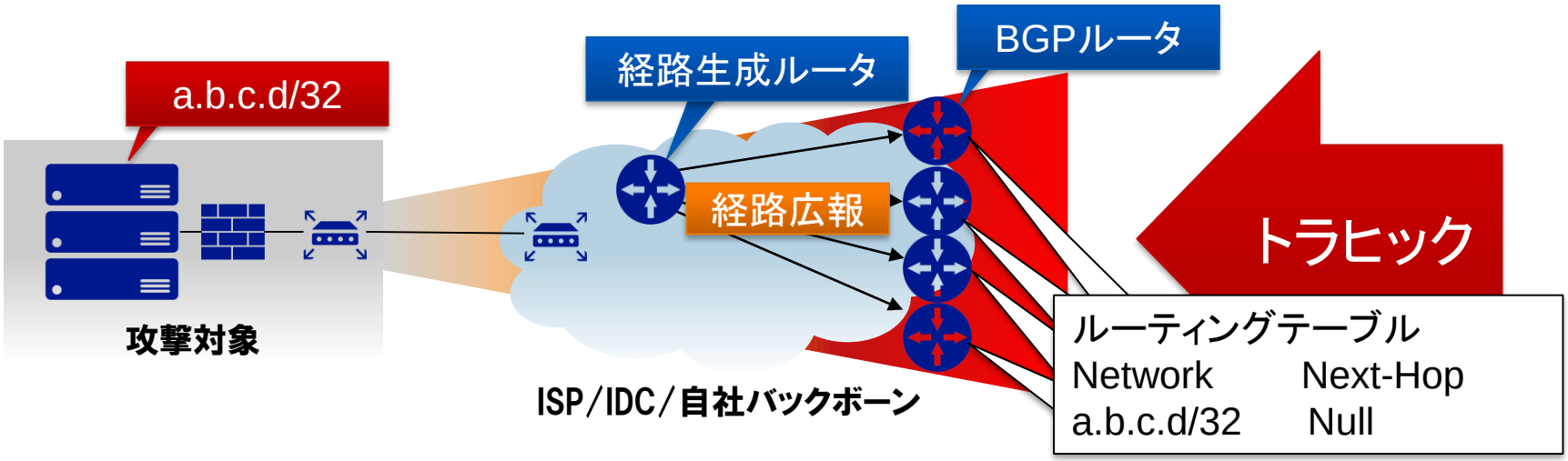
入口で対処：Blackhole Routing



- BGPルータにNext-Hop Nullの経路を設定、トラヒックを破棄する仕組み
  - 純然たるルーティング機能のため、基本的に性能劣化はない
  - 遮断は宛先IPアドレス単位

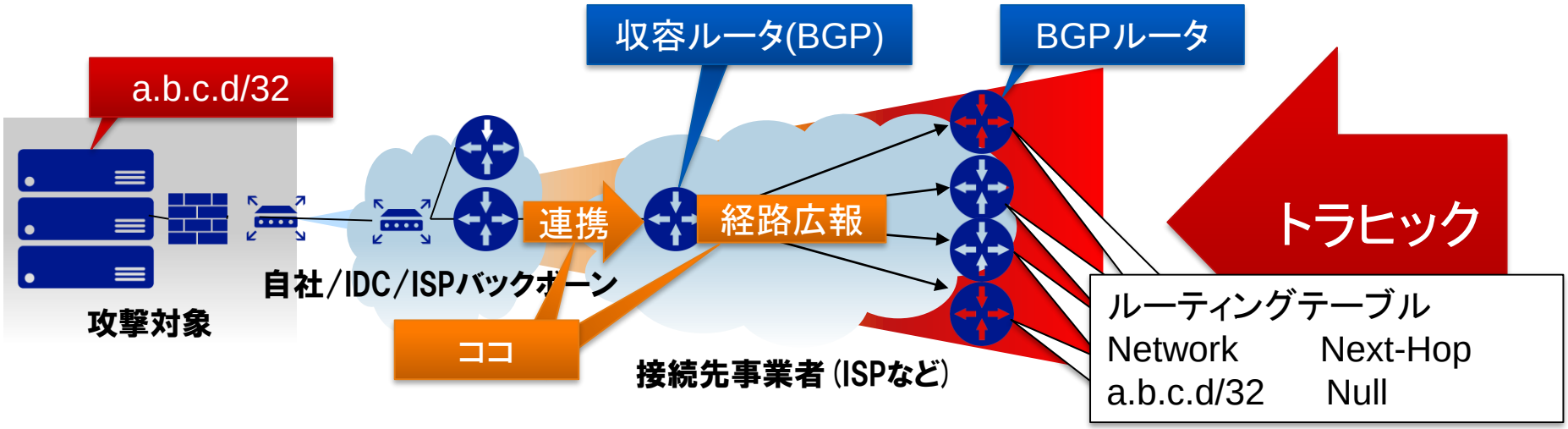
サービス継続の観点では対象とするトラヒックを限定するなど工夫が必要(後述)

Blackhole Routingの応用①：RTBH（Remotely Triggered Black Hole）



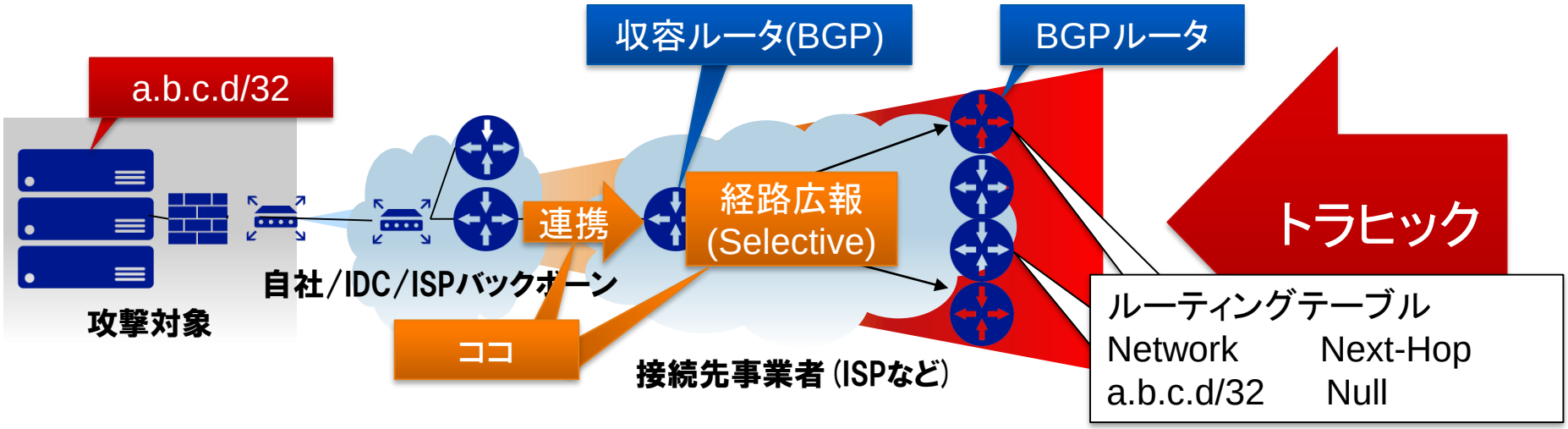
- 経路広報により一斉に全BGPルータにBlackhole Routingを設定する仕組み
  - 1台1台に設定をする手間がなく、迅速に全BGPルータに適用可能
  - 実態はルーティングアップデートのため、設定変更と比べミスオペレーションのリスクが少ない
  - 戻し作業も容易、経路広報を止めるのみ

Blackhole Routingの応用②：Community RTBH



- BGPのCommunity Attributeを利用してBlackhole Routingの設定を伝搬する仕組み
  - ユーザから事業者への連携(依頼)の手間が省け、より迅速に対処が可能
  - 下記の条件が必要
    - マルチホーム環境など事業者とBGPで接続されていること
    - 接続先事業者がCommunity RTBHをサポートしていること
  - 受け取ったCommunity Attributeを他の事業者にまで伝搬させるかは議論がある
    - 情報の信頼性を確認するよい手法がないためその気になれば悪用が可能
    - /32といった細かな経路を受け付けることになるため、経路数問題も懸念される

Blackhole Routingの応用③：Selective RTBH



- 特定のBGPルータにのみBlackhole Routingを設定する
  - 特定の国や地域のISPを収容するルータにのみ設定するといった制御が可能
  - 国や地域もCommunity Attributeによりユーザが制御

活用例
- 利用者のほとんどを占める国内向けトラヒックを守るため、海外ISPから流入するトラヒックを破棄
- DDoSの大部分を占めるA国ISPからのトラヒックを破棄し、トラヒック全体を受容できる量に収める

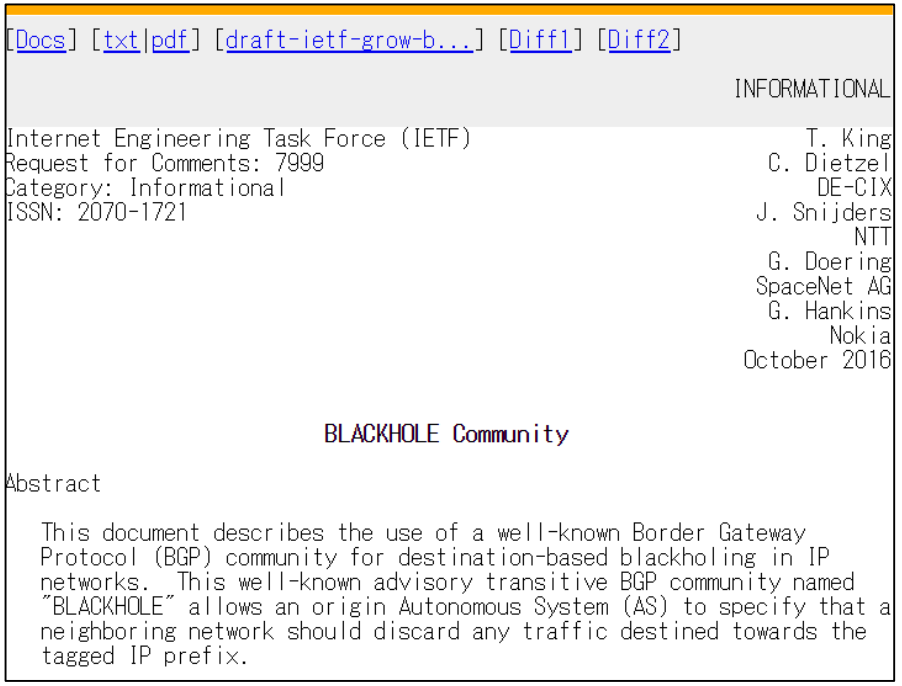
予め守るべきトラヒックの優先順位付けができていれば有効に機能する

Community Attributeの標準化

- RTBHに用いるCommunity Attributeの記述について標準化されておらず、ISP各社が独自に仕様を決めて実装しているのが実情

- IETFにて議論が進行、Informational RFCとして公開(2016/10)
  - 666の利用を示唆

本日11月29日(火)16:15～18:45
「T6 想いが伝わるBGP運用
～経路制御とルーティングセキュリティ最前線～」
にて詳しく取り上げる予定



[Docs] [txt|pdf] [draft-ietf-grow-b...] [Diff1] [Diff2]

INFORMATIONAL

Internet Engineering Task Force (IETF)
Request for Comments: 7999
Category: Informational
ISSN: 2070-1721

T. King
C. Dietzel
DE-CIX
J. Snijders
NTT
G. Doering
SpaceNet AG
G. Hankins
Nokia
October 2016

BLACKHOLE Community

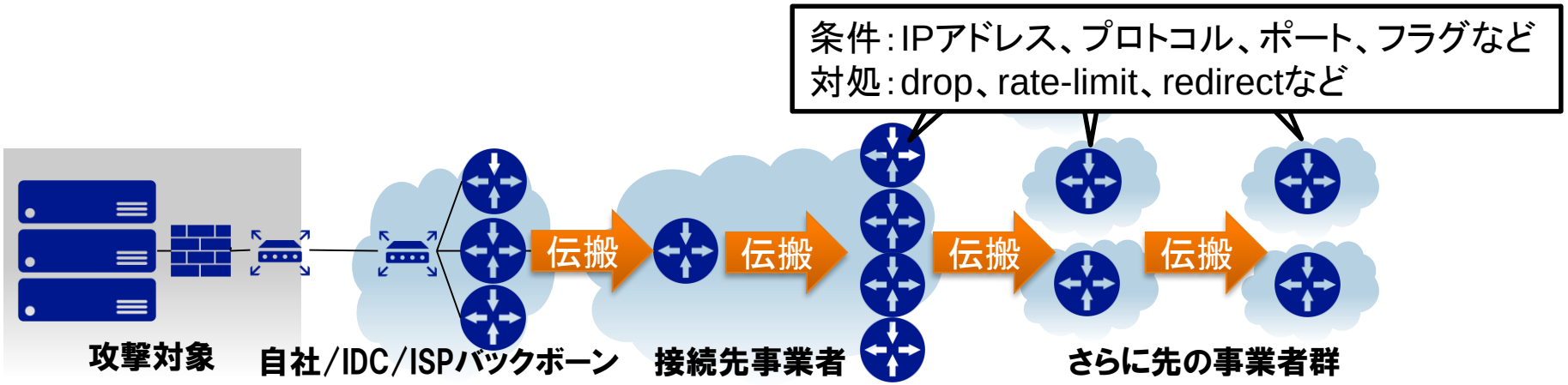
Abstract

This document describes the use of a well-known Border Gateway Protocol (BGP) community for destination-based blackholing in IP networks. This well-known advisory transitive BGP community named "BLACKHOLE" allows an origin Autonomous System (AS) to specify that a neighboring network should discard any traffic destined towards the tagged IP prefix.

https://tools.ietf.org/html/rfc7999

統一されることでより一般化し使いやすくなると期待される

一歩先んじた取り組み：BGP Flowspec

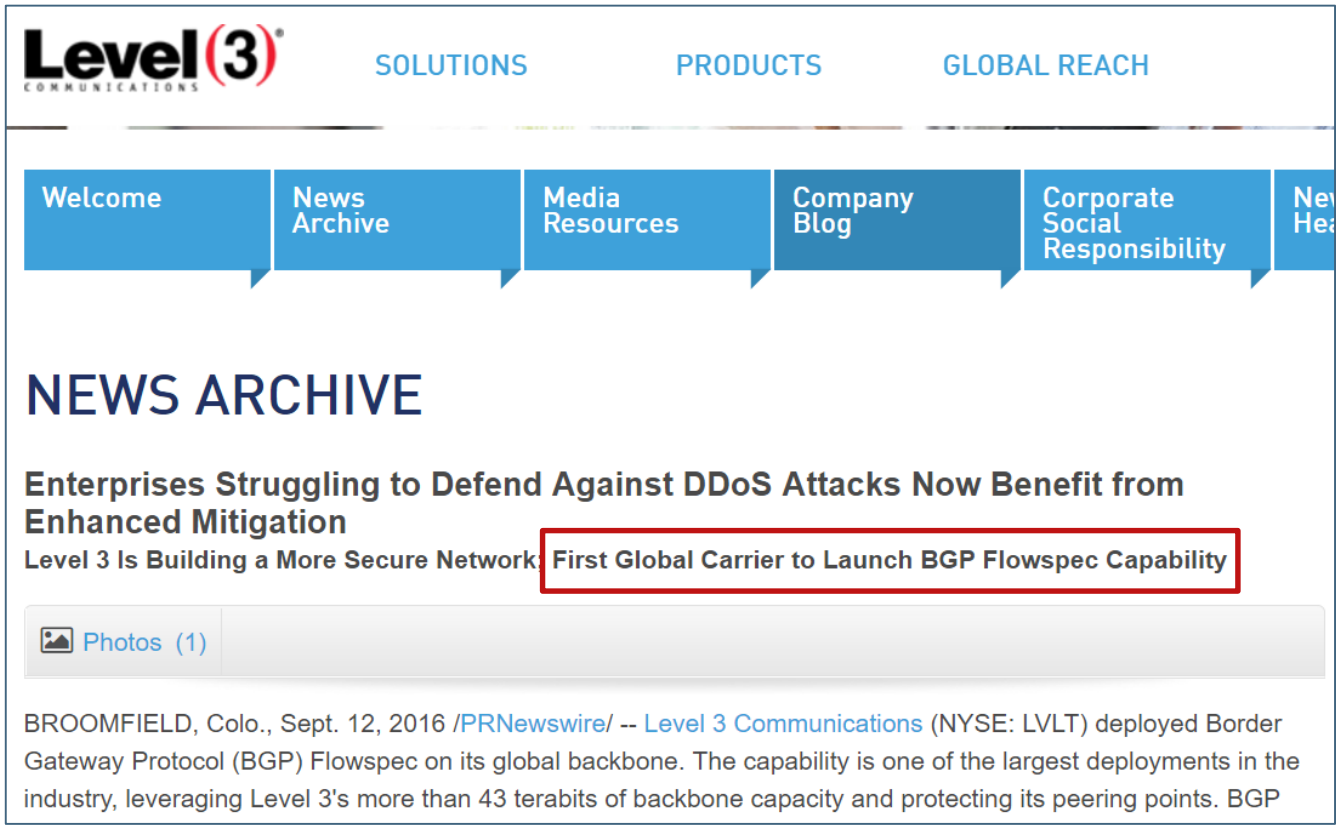


- 自社設備、他社設備を問わず遠方のBGPルータにNetwork ACLを設定する仕組み
  - RFC5575(2009年)として標準化、主要メーカーは実装済み、そろそろこなれてきた頃(?)
  - 大手事業者で実際にDDoS対処に利用(次頁)、国内でも事業者間連携の議論始まる
  - Community RTBHとの比較
    - IPアドレス単位ではなく、Network ACL(L3, L4)レベルのルールを設定可能
    - 遮断(drop)だけでなく、シェイピング(rate-limit)、転送(redirect)などを選択可能
    - eBGPでの伝搬を前提にオリジネータ(発生元)のValidation機能が実装されている

DDoS攻撃を受ける側が発生源近くでトラヒックの制御を可能とする

BGP Flowspecは徐々に実用の段階に

米国のTier1プロバイダLevel 3 Communicationsの事例



Level 3 COMMUNICATIONS

SOLUTIONS PRODUCTS GLOBAL REACH

Welcome | News Archive | Media Resources | Company Blog | Corporate Social Responsibility | New Hea

NEWS ARCHIVE

Enterprises Struggling to Defend Against DDoS Attacks Now Benefit from Enhanced Mitigation

Level 3 Is Building a More Secure Network; First Global Carrier to Launch BGP Flowspec Capability

Photos (1)

BROOMFIELD, Colo., Sept. 12, 2016 /PRNewswire/ -- Level 3 Communications (NYSE: LVLT) deployed Border Gateway Protocol (BGP) Flowspec on its global backbone. The capability is one of the largest deployments in the industry, leveraging Level 3's more than 43 terabits of backbone capacity and protecting its peering points. BGP

http://news.level3.com/2016-09-12-Enterprises-Struggling-to-Defend-Against-DDoS-Attacks-Now-Benefit-from-Enhanced-Mitigation

小まとめ

- DDoS対処のポイントは大きく3つ、手数は多ければ多いほどよい
  - バックボーン設備：DDoS Mitigation 装置
  - 出口：収容インターフェイスのEgress Filtering
  - 入口：RTBHをはじめとするBlackhole Routing、一歩先のBGP Flowspec
- 費用は必要なものの機械（DDoS Mitigation装置）による対処は用意しておきたい
  - 機器性能までは迅速かつ安定的に動作
- インターネット接続形態により、自社と事業者で戦術、戦略の担当範囲が異なる
  - BGP接続では自社コントロールでCommunity AttributeによるRTBHを利用可能
  - それ以外では接続先事業者との連携にどうしても時間がかかる
- ユーザで制御、発生元近くで対処が全世界的な取り組みの方向性
  - BGP Flowspecの足音が少しずつ近くまで
  - みんなの夢、ゆえに議論もまだまだ必要

3.DDoS対処の戦略

インシデント対応フローをふまえた対処

1.準備

- 事前にできるDDoS耐性強化、監視や運用の設備投資
- 運用マニュアル整備、予防訓練
- 事業者とのコンセンサス

2.検知・初動

- 検知後迅速に初動を開始、対処できるものは対処
- 対処しきれないものは影響範囲を局所化、全滅を避ける
- 必要に応じて関係者への連絡

3.本格対処

- 初動で対処しきれなかったものに継続対処
- 徐々に通信を復旧させる

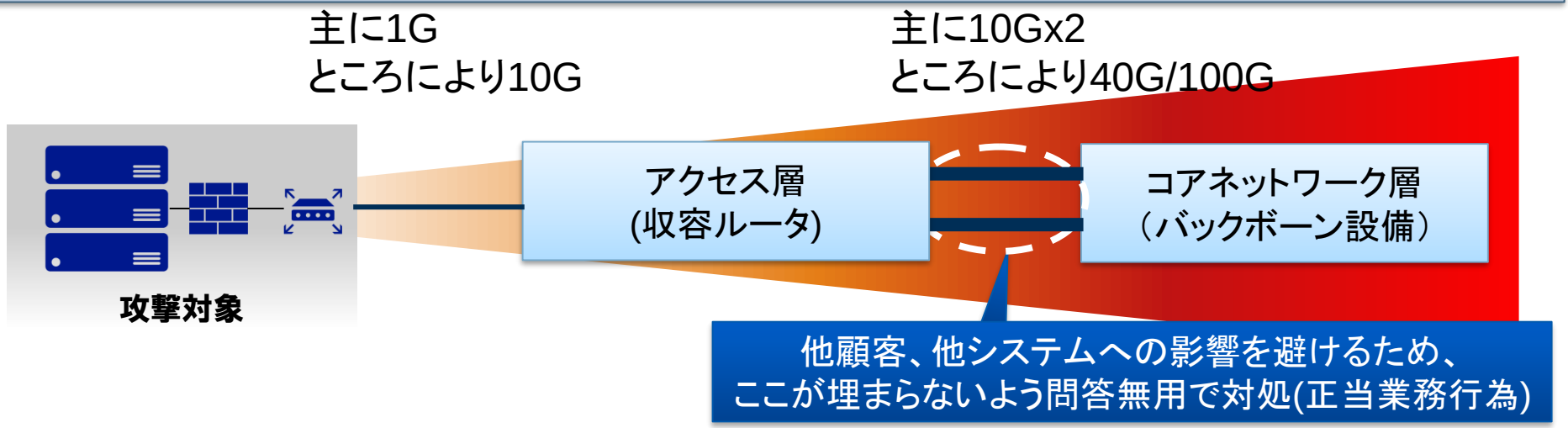
4.完全復旧

- 攻撃の鎮静化を確認
- 各種対処をやめを通常運用状態に戻す

全てのフェーズで備えのない対応はできない、予めの備えが要

まず、10Gbps規模までへの対処を考える

攻撃のトレンド、接続先事業者や自社のバックボーン構成もふまえた想定が必要

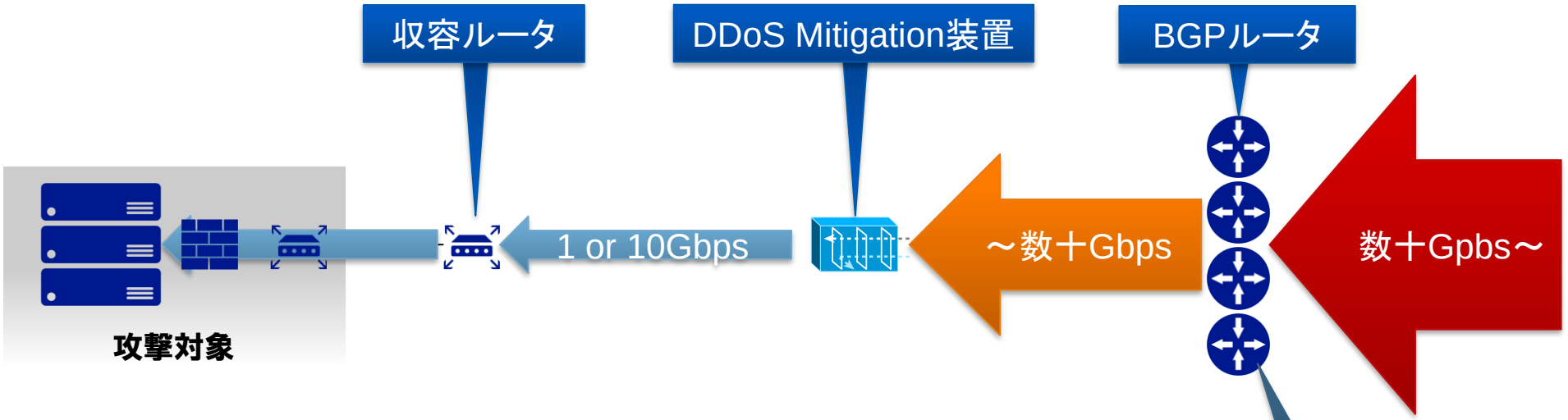


- 規模が大きければ大きいほど、トラヒックの流入元での対処が必要
- 一般に10Gbpsを超えるトラヒックは接続先事業者内で放置されにくい
  DDoS Mitigation装置のオプション契約がなければ無条件に落とさざるを得ないことも
- 一方、契約帯域未満のトラヒックに対しては事業者からの積極的関与はない
- 国内で日々観測されているDDoSの多くはこの規模
- 大規模なDDoSになればなるほど攻撃者の費用負担も大きい(DDoS as a Service)

このあとのBBIX矢萩さまパートにて詳解

次に、大規模DDoSへの対処を考える

トラヒックに優先順位付けをして多段で対処、Mitigation装置はやはりキーパーツ



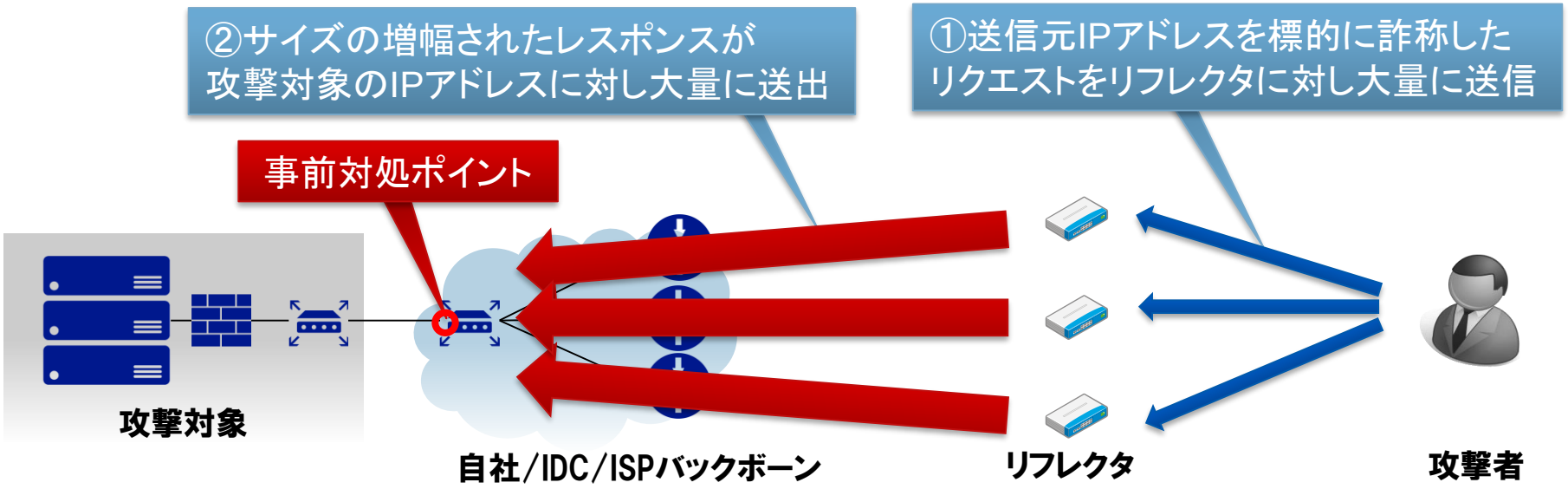
1. 入口となるBGPルータでMitigation装置でまかなえるに帯域に制限
   (Blackhole RoutingやBGP Flowspecの活用)
2. Mitigation装置で悪性トラヒックをクリーニング
3. Mitigation装置がなければどこかのACLで対処

遮断にしろシェーピングにしろ
正常通信に完全無影響とはいかない

準備：事前フィルタリングによるReflection攻撃への耐性強化

既知のUDPサービスをフィルタリングすることでReflection攻撃を未然に防御

- Reflection型攻撃(Amp型攻撃)はパターン化して防御しやすい
  - 現在でも多く観測されているポピュラーな手法
  - UDPかつ送信元ポート番号が固定、悪用されやすいサービスは既知
    収容ルータで予めEgress Filteringすることである程度の規模までは被害を未然に防止
  - 必要なUDPサービスも代替策の検討が可能



準備：Reflection攻撃耐性強化実践

■DNSは自前で運用しない方が有益

- 同一ネットワーク上で運用することは、DDoS発生時の全滅リスクが高まる
- ネームサーバ(権威DNSサーバ)は、事業者ダイバーシティも考慮したい
- フルリゾルバ(キャッシュDNSサーバ)は、ISP提供やpublic DNSなどの選択肢がある

■NTPはデータセンタ提供のものを参照することが定石

- インターネット経由の参照は精度が落ちるため望ましくない

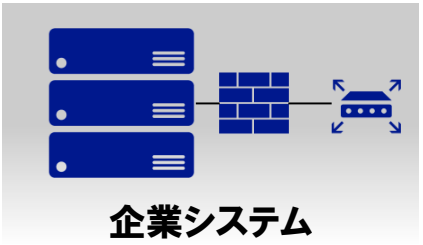
Protocol	Bandwidth Amplification Factor
DNS	28 to 54
NTP	556.9
SNMPv2	6.3
NetBIOS	3.8
SSDP	30.8

代表的なプロトコルを制限するだけでも効果は高い

Reflection攻撃に悪用されやすいUDPサービスの例
[引用元]https://www.us-cert.gov/ncas/alerts/TA14-017A

準備：システム全体の耐性確認、耐性強化

機器のスペックシートを鵜呑みにせず、**実測スペックの把握**が必要



[参考プログラム]
12月1日(木)09:30～12:00
「T12 ネットワーク機器の本当のスペックを見抜く」

- 自社設備は回線帯域ぎりぎりのトラヒックに耐えうるか？
  - Router/Switch/Firewall
    - 正常にパケットを処理し続けられるか
    - 監視やFlowの出力に影響がないか
    - より狭帯域の設備が残っていないか、リンク速度やDuplex設定は適切か
    - オプション処理により高負荷にならないか(例：遮断ログの記録)
  - Server
    - Firewallの保護化にあるか、ない場合Malformedなトラヒックへの耐性があるか

準備：監視と観測、検知の仕組み

■SNMPなどによるリソース監視(MUST)

- ネットワーク帯域、CPU負荷
- 定常トラヒックを踏まえた閾値を設定し検知

<ソリューションの例>

- Cacti、MRTGなどのオープンソース実装

■NetFlow/sFlowなどによるトラヒック解析(SHOULD)

- 送信元AS、国、地域、プロトコルなどトラヒックの傾向を分析
- 帯域が埋まりきってもトラヒック全体の傾向はある程度把握可能

<ソリューションの例>

- FastNetMon：DDoS対処に特化したオープンソース実装
- Flow as a Serviceや接続先事業者のサービス利用

検知の迅速化、対処の戦略を立てやすくするためにぜひ検討したい

準備：マニュアル化

■場合分け
- 規模や特性に応じて

■優先順位付け
- 優先するべきトラヒックは何か？(国内、海外、国、地域)
- 優先するべき対象、サービスは何か？

■権限の委譲
- 都度責任者の承認を得るようでは迅速な対処ができない

■インターネット不通を想定した連絡体制
- 電話、FAX、バックアップ回線

人は予め用意された手順通りにしか動けない、予行演習もあわせて考えたい

準備：事業者とのコンセンサス

- パワーバランスに基づく一方的な要求は下策
- コミットを求められれば求められるほど杓子定規な対応しかできない
- 相互理解による協力的な関係性とコンセンサスの構築がDDoS対処の要

このあとのIIJ原さまパートにて詳解

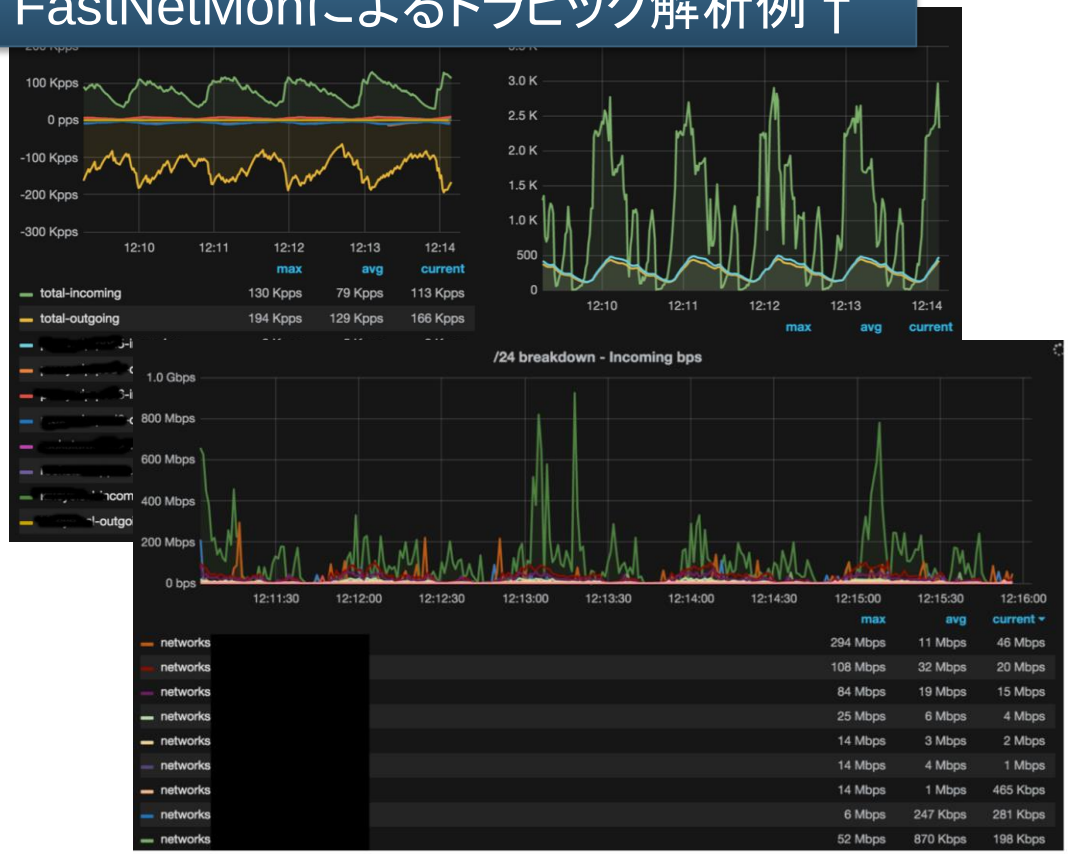
利用者
（顧客）

各事業者
（ISP、IDC、IXP、SIerなど）

準備：やはりトラヒックの解析結果はほしい

- 準備フェーズ
  - 優先順位付けの材料
  - 事業者と円滑に会話するための材料
- 対処フェーズ
  - 実態の把握
    - 攻撃種別の判定
    - 狭義の攻撃対象の把握
  - 対処手法検討の材料
    - どの程度の影響があるのか
    - どの程度の効果が見込めるのか

FastNetMonによるトラヒック解析例 †



† [引用元]https://www.nanog.org/sites/default/files/OpenSource-DDoS.pdf

小まとめ

■戦略は規模に応じて場合分けして考える
- まず、10Gpbs級への対処
- 次に、大規模への対処

■準備が要
- システム全体のボトルネック洗い出し、耐性強化
- 監視、観測、検知の仕組み整備
- 運用手順整備
- トラヒックの優先順位付け
- 権限委譲
- 事業者とのコンセンサス
- 予行演習

何事も備えあれば憂い無し、備えなくして為す術なし

4.おわりに

全体まとめ

DDoSは日常茶飯事、各事業者で対処ノウハウが日々向上

↓

対処の中身を知り、各事業者と手を取り合って、適材適所な選択を

CDN/
スクラビングサービス
(DDoS対処専門事業者)

＋

有事運用

既存契約
+Mitigationオプション
(ISP/IDC事業者)

＋

自社対策と有事運用

既存契約内での対処
(ISP/IDC/SI事業者)

＋

自社対策と有事運用

明日すぐにはじめてほしいこと

1. 事業者へのコンタクト、相談

何事も事業者との良好な関係性が要

2. 不要サービスの事前フィルタリング検討

Reflection(Amp)型攻撃の防御に有効

3. ISP/IDCのMitigationオプション加入の検討

規模によらず影響を最小化するためのキーパーツ

特に頻度の多い小規模DDoSに迅速かつ有効に作用

このあとのお話

1. DDoS対処の戦術と戦略
   中島 智広(NRIセキュアテクノロジーズ株式会社)

2. 顧客と事業者の関係性、契約、コンセンサス
   原 孝至(株式会社インターネットイニシアティブ)

3. 事業者における対処の実際とサービスオペレーション
   湯澤 民浩(さくらインターネット株式会社)

4. DDoS時代のIXとの付き合い方～IXPからみた現状と展望～
   矢萩 茂樹(BBIX株式会社)


NRI
未来創発
Dream up the future.