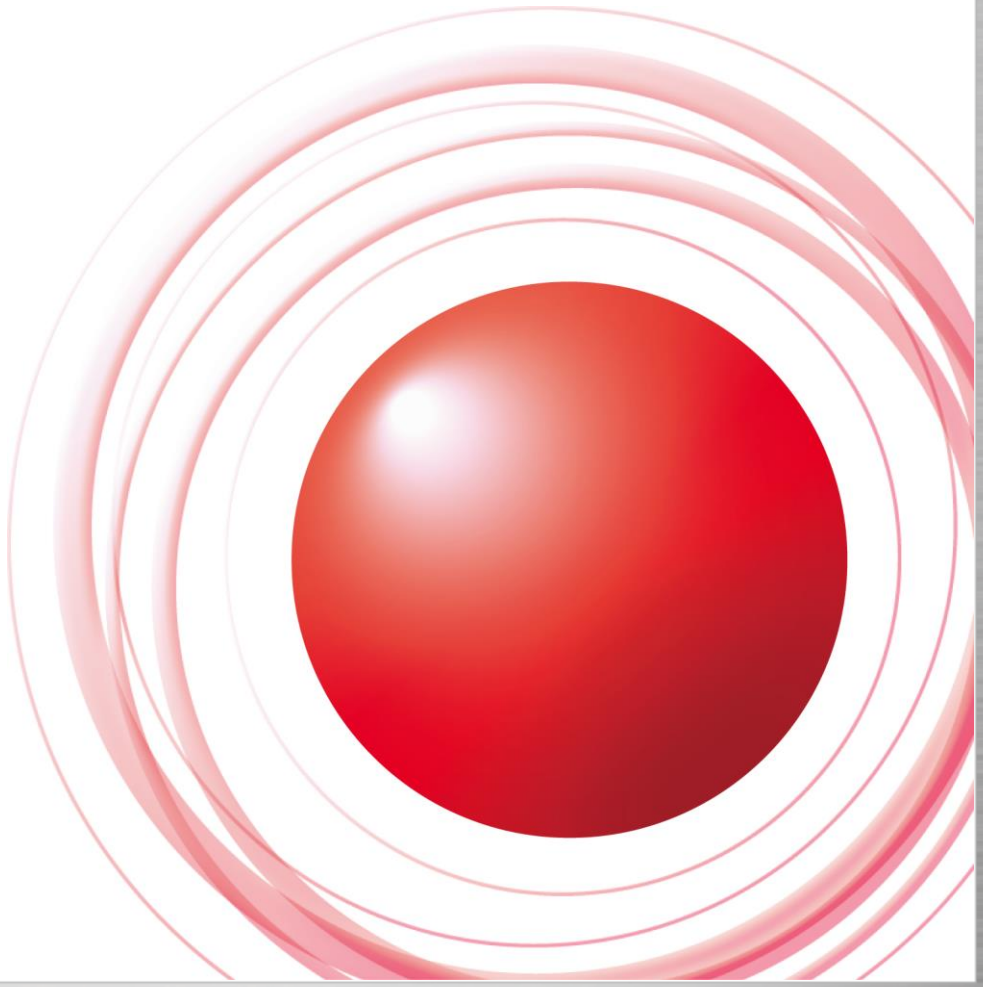
Internet Week ショーケース in 名古屋
企業のDDoS対処戦略 Reloaded
事業者にいま求められる取り組み
～技術、運用、考え方～

IIJ
Internet Initiative Japan



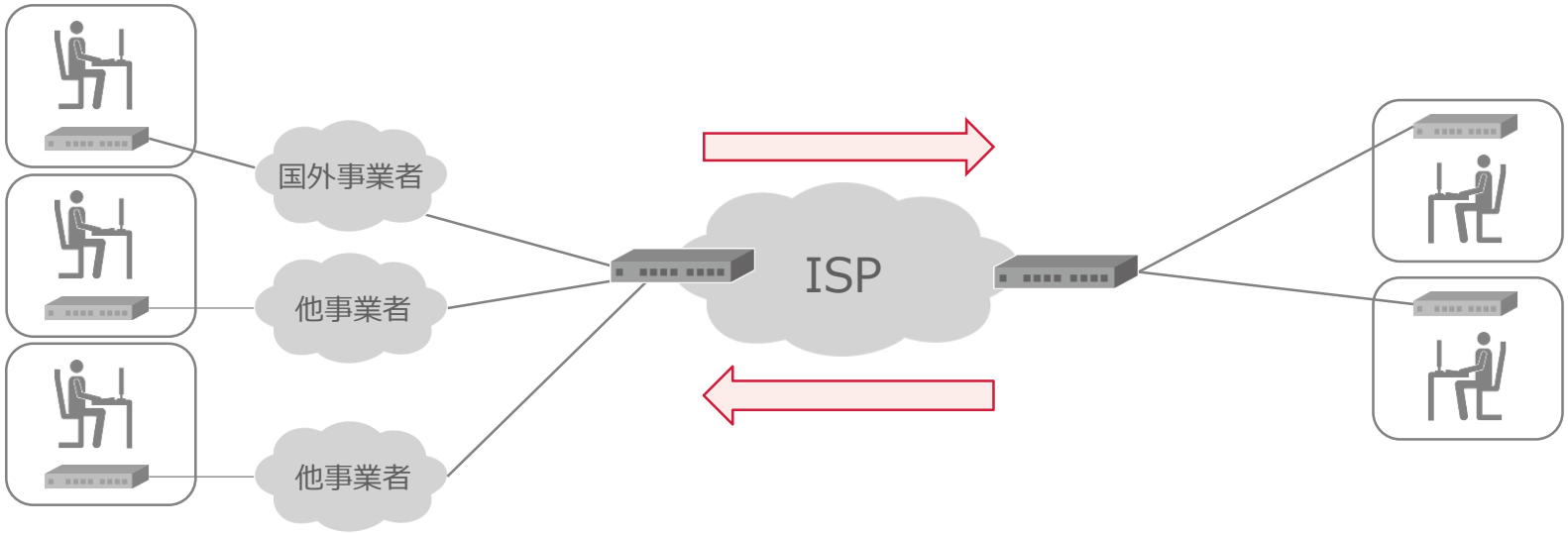
株式会社インターネットイニシアティブ
原 孝至 hara@iij.ad.jp

Ongoing Innovation

事業者(ISP)の考えを知る

事業者のビジネス(収益)

顧客の通信をたくさん運ぶことにより、収益を上げる



事業者(ISP)は通信を運ぶことが本業

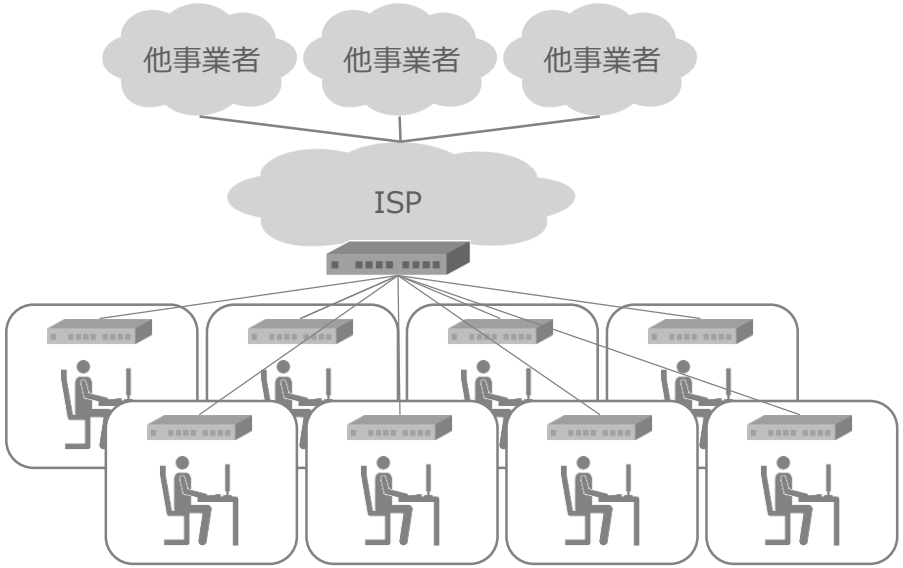
- 郵便会社がたくさんの郵便物を取り扱う
- 運送会社がたくさんの荷物を取り扱う
- 鉄道会社が乗客荷物を電車で大量に遠くまで運ぶ
- 航空会社が乗客荷物を飛行機で遠くまで運ぶ

通信に善悪はなく、とにかく運ぶことで事業者はご飯が食べられる
通信を運ぶのを止めるのは、事業者にとってはイレギュラー

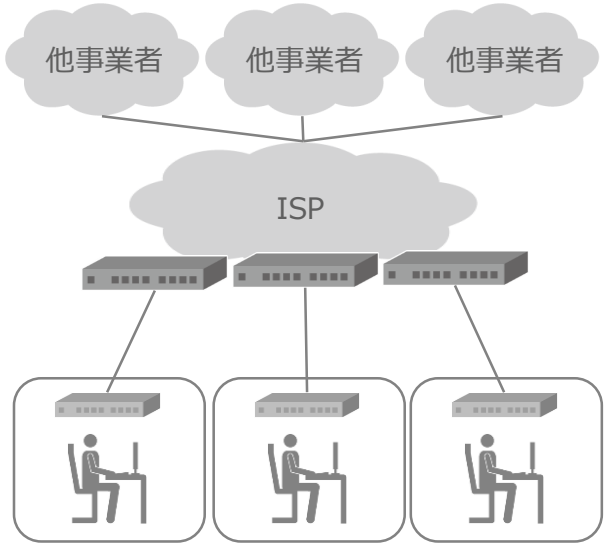
通信に何らかの作用をするには、ユーザの意志や同意が必ず必要

事業者のビジネス(利益)

限りなく少ない設備とコストでたくさんの顧客を収容する、
いわゆるベストエフォート回線サービスやそれに準ずるサービス



潤沢な設備に収容し、顧客からそれなりに費用をいただく
いわゆる専用線系サービス



集約をするほどコストは下げられるが問題が発生すると手がつけられない
大人の事情から対応するモチベーションは低い

分割をするほどコストは上がるが問題が発生しても切り分けやすい
空気を読んで対応するモチベーションは高くなる

コストは問題発生から解決までの重要な要素となり得る

最近のDoS

気軽に実行される
- 10Gbps超の攻撃でなくとも、数Gbps程度の攻撃であれば日常的に発生する

普段さほど通信がない箇所でも何かの拍子で攻撃が流入するので
キャパシティ設計や増強計画、設備の隔離が難しい
おそらく攻撃理由もあまりなく、突拍子もない
- 人の失言
- 企業のサービス内容への不満
- OpKillingBayのような厨房/キッズの遊び

攻撃がしつこい
- 攻撃者はSNSで反応を伺えるので面白がってエスカレートする
- 被害者がSNSで対策を即時公表できるので、攻撃者が追従してくる

顧客の温度感は上がるばかりなので、攻撃対策の準備は必須

出来ることをやるために必要なこと

対策をする前に準備すること

通信の秘密と適法性

お客様は正常な通信を復旧させたい不要な通信を止めてくれと依頼がある
必要な通信と不要な通信の確認をする必要がある
通信の秘密があるから何でもかんでもできるわけではない

顧客との合意形成
　　事業者は通信の秘密により、
　　ある程度制限をされ、
　　それを言い訳にしてしまうことがあるが
　　やらなければいけないことはしっかりやらなければいけない

顧客との事前コンセンサス

何が対応できるのか、何が起きるのか、顧客に説明できるよう準備する
顧客は何ができるのか確認する
人と人のコミュニケーションは大切

通信に対する考え(前提)

「通信の秘密」

憲法
第21条　集会、結社及び言論、出版その他一切の表現の自由は、これを保障する。
２　検閲は、これをしてはならない。通信の秘密は、これを侵してはならない。

電気通信事業法
（検閲の禁止）
第3条　電気通信事業者の取扱中に係る通信は、検閲してはならない。
（秘密の保護）
第4条　電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。
2　電気通信事業に従事する者は、在職中電気通信事業者の取扱中に係る通信に関して知り得た他人の秘密を守らなければならない。その職を退いた後においても、同様とする。

→「侵してはならない」とは以下の行為の禁止のこと

知得(ちとく)	積極的に知ろうとすること、知ること
漏洩(ろうえい)	他人が知り得る状態にすること
窃用(せつよう)	自己又は他人の利益のために用いること

→事業者が把握し提供するものは大抵が通信の秘密に該当
　ログ、個人情報、ルーティング自体?

→顧客の通信に対して事業者が能動的にアクションを起こすのは基本的にマズい

※検閲は国や公的機関など公権力が行うものなのでここでは対象外
→あくまでも「通信の秘密」の問題

通信に対する考え(実際の運用)

正当業務行為
事業者が、電気通信事業を遂行するために必要かつ正当な行為

正当防衛/緊急避難
現在発生している危機から、自社設備、顧客、自社と関係ないインターネット利用者を守るために、自社のユーザ等の通信の秘密を侵害する行為

- 攻撃と思われる通信の内容を調査(知得)すること
  →通信の送信者に悪意があれば正当防衛、悪意がなければ緊急避難
- 攻撃と思われる通信から自社設備を守るためサービスを停止(窃用)すること
  →通信の送信者に悪意があれば正当防衛、悪意がなければ緊急避難
- 攻撃と思われる通信をフィルタなどで破棄(窃用)すること
  →通信の送信者に悪意があれば正当防衛、悪意がなければ緊急避難

※ルーティング自体は正当業務行為

影響が生じる攻撃が発生している場合、
ユーザの同意がなく事業者がアクションを起こしても通信の秘密の侵害にはならない

おそらくほとんどの事業者の規約や約款で(直接的な形でないにしろ)謳われていると思われる
事業者は正当業務行為を行う必要があり、合わせて正当な理由の準備が必要
顧客は規約や約款の同意が必要

参考:電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン
https://www.jaipa.or.jp/other/mtcs/

顧客と事業者の事前コンセンサス

事業者が何が出来るのか確認する、また出来ることを用意する

- 調査はできるのか、手段を用意しているか
- フィルタ手段はどのようなものを用意しているのか、できるのか、どう利用するのか
- 対応目標時間はあるのか
- RTBHなどリスクある機能の利用は念入りに説明する、程度により別途覚書を交わしておく
- いざという時に実行できるのか

顧客自身もコンセンサスを準備してもらう

- そもそもそんなに止めてはいけないシステムなのか
- どのシステムの通信がどこの事業者のどの契約の回線を通っているのか
- どこまで停止は許容されるのか
- 停止できる時間帯はあるのか
- どれだけ止まるとどれだけ被害が出るのか(影響利用者数、金額、社会的影響)
- 調査できる情報は何か
- 事業者に開示できる情報はどこまでか
- 遮断と解除を判断する人は誰か
    - 発見/対応した担当者か、特定の上長か、事業者におまかせか
    - 24時間いつでも判断できるか、判断できなかったらどうするか

事業者にいま求められる取り組み

攻撃による顧客の巻き添え防止

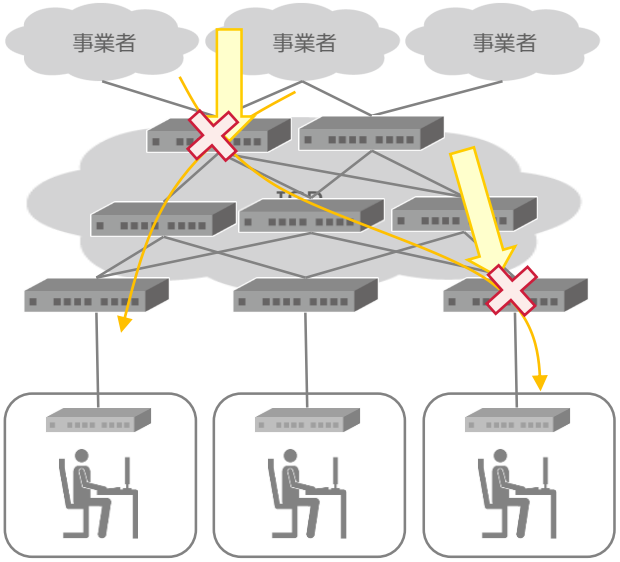
DDoS攻撃を受けやすい顧客の隔離
同質の客層を集めて隔離する
強力な機器/設備で耐える
集めすぎるとメンテナンスなどができなくなるので程度を見極める

DDoS攻撃にシビアな顧客の分離
それなりの費用をいただいて専用設備を用意する
それなりの専用設備には付加価値を用意し、顧客の納得感を引き出す

取捨選択/ダメージコントロール
インシデントが起こった際の素早い判断と顧客への案内
各種遮断時の影響と把握と顧客への案内

- エッジで対処は事業者ネットワーク内が苦しい
- コアで対処すればするほど影響は大きい

最悪の場合に設備/通信/顧客を切り捨てる決断
正当防衛なのか緊急避難なのか説明できるように



安定性向上の取り組み

常に新しい機器への対応
古い機器や低性能機器では攻撃に耐えられないかもしれない
- フルルートが保持できないクラスの機器の駆逐
- メーカーEoS/EoLが到来する/している機器の破棄

定期的にメンテナンスを行う
機器のバグや脆弱性を排除しておく
Flow情報やBGP FlowSpecなど機能拡張、新しい機能の追加を確認する
動いているからOKでは済まされない

検証と動作確認
機器のスペック、挙動を把握する
不具合は潰しておく、もしくは回避オペレーションを把握しておく

オペレーション訓練と業務フローレビュー
来るべきときに備え、オペレーション経験を積んでおく
やっぱり経験が物を言う
顧客とのコミュニケーション、各種報告、クローズまで何をするか合意形成をしておく

事業者(ISP)が対応できること

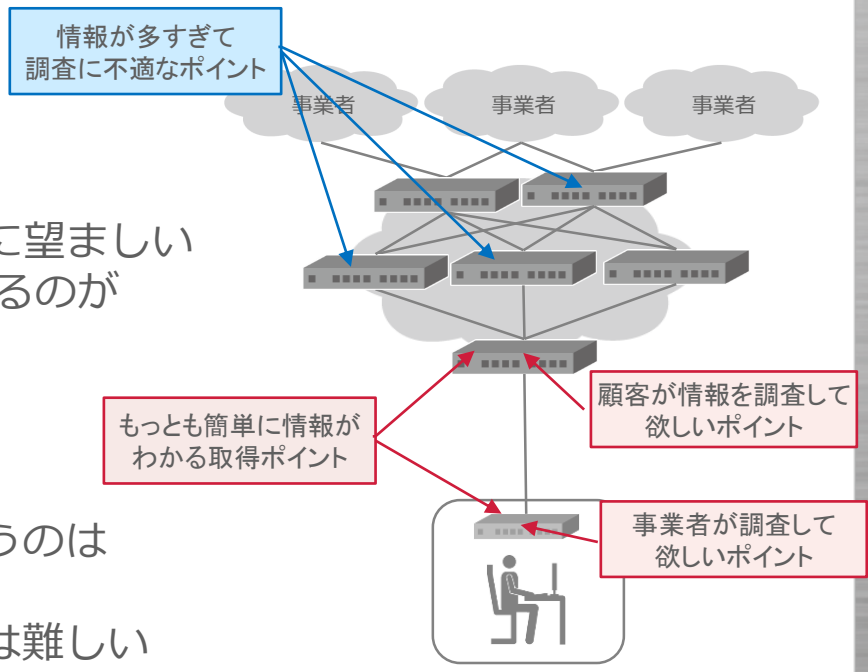
攻撃と思われる通信を調査する

アラートから調査する
- PING監視、syslog監視、SNMP trap監視、トラフィックしきい値監視

SNMPから調査する
- トラフィックグラフ、CPU load、I/Fエラーカウンター

Flow情報から調査する
- NetFlow、sFlow、IPFIXなど

顧客機器のアクセスログから調査する
- Webサーバ、FWなど



誰が調査するのか

顧客機器のログから調査するのが通信の秘密的に望ましい
現実的には事業者側のFlow情報などから調査するのが
一番手っ取り早いと思われる

事業者としては

「通信の中身を探れる手法を持っている」というのは
顧客に対して説明が難しい…
コア部分で情報を取得するほど情報過多で絞込は難しい

顧客としては

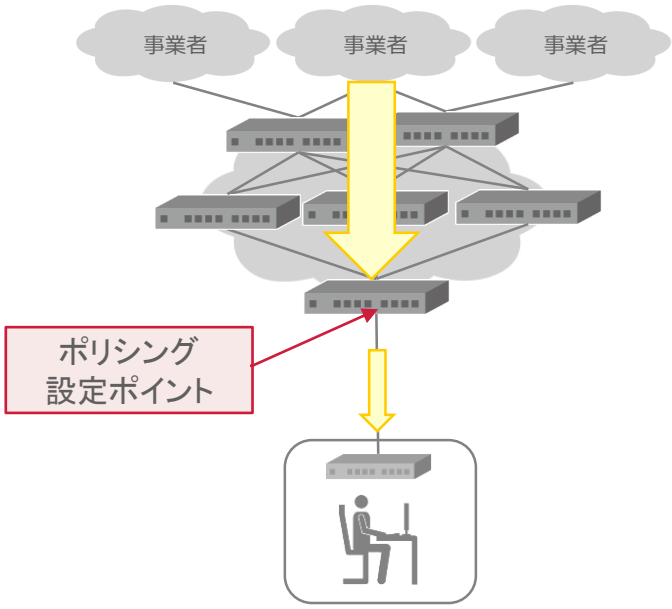
探れる手法を持っていない、ログが多すぎてわからない
そもそもテンパっていてほとんど対応できない

攻撃と思われる通信を遮断する方法 その1

絞り設定、ポリシング

- そもそも攻撃は止まらないが被害は最小化できる
- ちょっとでも通信をとめたくないという貴方へ
  (すでに攻撃で止まってるけど…)

遮断ではなく、緩和や軽減
攻撃されているホスト以外を救うという考え方
攻撃を緩和してなにを守るのかの決断が重要



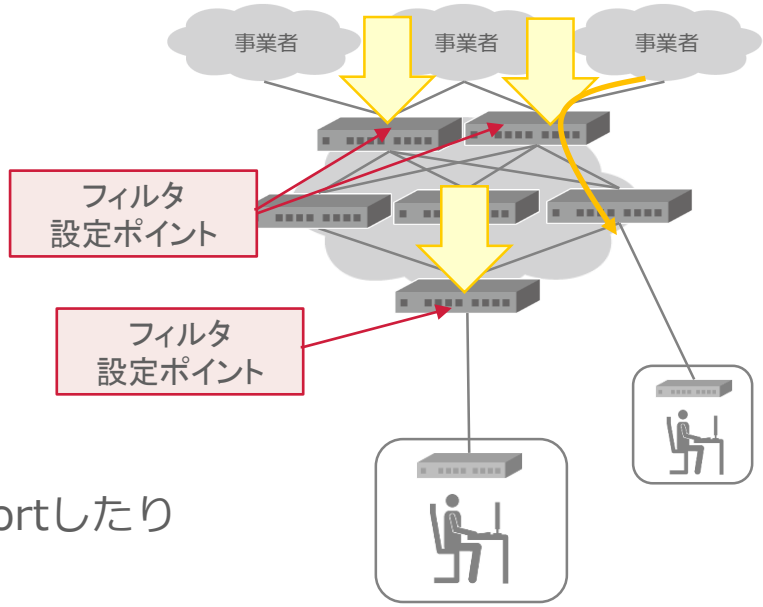
攻撃を耐えているだけで終息していない
そもそも攻撃されているホストは攻撃されたままなので
早めにフィルタに移行すべき
事業者も自ネットワーク内で攻撃を運んでしまっている
のできつい

攻撃と思われる通信を遮断する方法 その2

Access Control List(ACL)

- もっとも手法として考えられる
- 詳細にフィルタできる一方、DDoS攻撃に対してはすべて遮断が前提

- 超めんどい！適用まで時間かかる！



準備が大変、設定適用時も気が抜けない
変換スクリプトやツールなどで省力化はできるが
やっぱり最後に判断するのは人
→フィルタ依頼を読み違えてたら？
→そもそも依頼が間違ってたら？

そもそもそんなにACL設定してルータは耐えられる？
→数10Gbpsフォワーディングして、Flow情報をexportしたり
SNMP GETしながら耐えられる？
→ACLって何行まで設定できるの？
→限界越えたらそのルータに収容されている顧客全てを巻き込んでしまう！
→攻撃を現在進行形で

事業者ネットワークのよりコア側で設定するほど粗く、影響が大きい設定になる
→顧客アドレスを守るフィルタ設定はコア側で設定するほどすり抜けが大きくなる
→攻撃元を制限するフィルタ設定は他顧客も巻き込むのでより顧客収容側で設定するべき

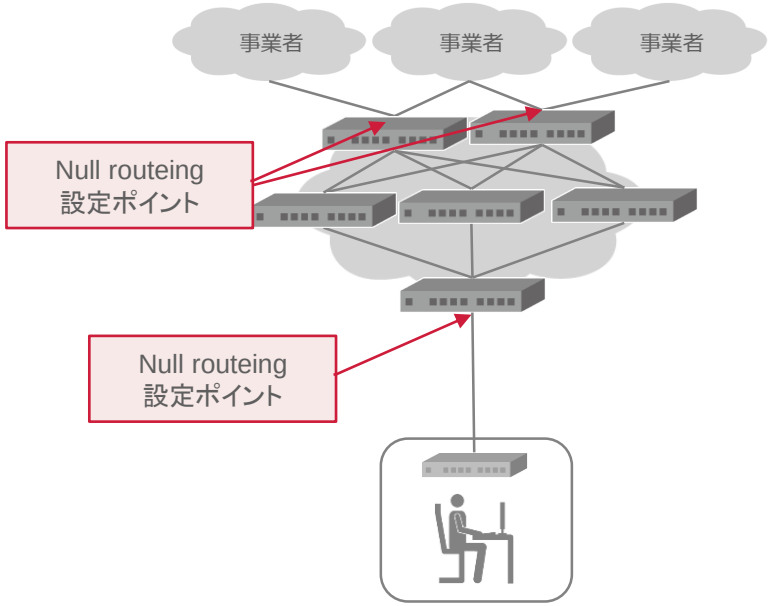
攻撃と思われる通信を遮断する方法 その3

Null routing

- ACLよりはコンフィグが容易
- ルータへの負荷はたぶん一番低い

送信元アドレスやポート番号を指定してのフィルタではない
結局防御アドレスはサービスが利用できなくなるのである意味DoSが成功している
Null設定はFlowなど各種情報がとれなくなるなど影響が大きい場合がある
ルータ負荷を除くリスクはACLとだいたい同じ感じ

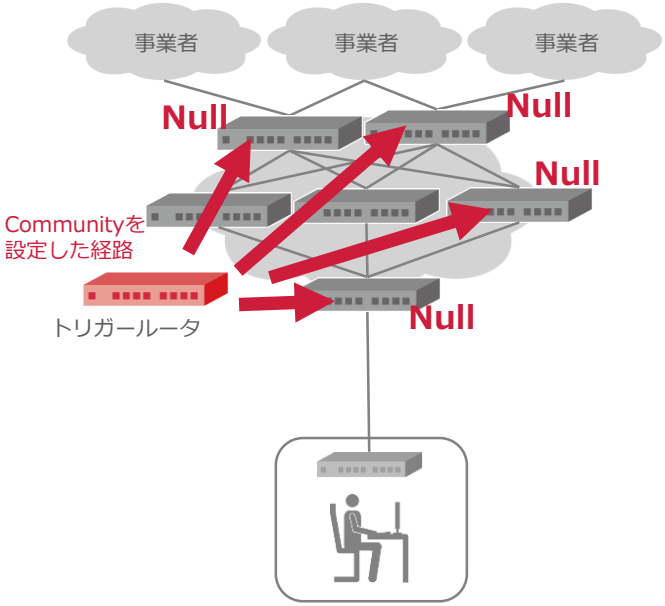
事業者としてはまず初めに発動させたい
設定が容易で迅速な対応が可能なので
フィルタやポリシングの前にまず設定し影響を
最小化してから対応準備したい



攻撃と思われる通信を遮断する方法 その4

- Remote Triggered Black Hole filtering/routing
- BGP Flowspec
  - BGP communityを設定した経路に対してNull routingやACLを発動する
  - 事業者から仕組みを提供してもらえば顧客自身で
    フィルタができるのでより素早い対応が可能
  - 動作の理解が難しい、上級者向け

難しい
設定によってどうやって動作するか把握が大変
少なからずBGP設定が必要なのでオペレーション
攻撃発生時にどのようなBGP communityを設定すれば
よいか落ち着いて判断できるか



設定時の責任問題
ACLは事業者の責任で実施されるが顧客自身の責任で実施される
→設定ミスしたら誰の責任になるのか
→設定と期待する動作に違いがあった場合は誰の責任なのか

入念な準備
オペレーション簡素化のためのシステム作り込みは十分か
機器の動作検証は十分か
準備ができれば最速の対応が可能だが影響範囲も大きかもしれない

今後どうやって取り組んでいくのか

自動化とニーズの複雑化

手動運用では顧客ニーズ/スピード感に耐えられない
- 早急な対応をしたいので顧客自身で事業者のバックボーンをいじってフィルタを実施したい
- **有償も含めて、サービス機能の拡充**や出来る限りの自動化

常に複雑化する顧客ニーズにいかに対処するか
- 一度決めた仕様でシステムを作ってもそれを超える要望は常にある
- システムやオペレーターの**柔軟な対応**

対応要求の高頻度化
- 一度DDoSが発生すると顧客の要求レベルは一気に上昇する
- そもそも昨今のDDoSは気軽に実行されるので顧客も事業者も休めない
  - 体制の強化、スクリプトやツールでの**省力化**

DDoS Mitigation機器やサービスの活用

運用でカバーの脱却

前述の対応は業界でいうところの「運用でカバー」
苦しいならMitigation機器やサービスを検討するべき

保護する対象

- 自社の設備を保護するのか
- 顧客向けに DDoS 対策機能を提供するのか

規模感があっているか

- 自社で実施するべき内容なのか
- 他社サービスを使う規模なのか

本当に停めてはいけないサービスなのか、ある程度許容されるのか

- 多額のお金が関わるもの
- メンツや体裁が必要なもの
- 人の人生や命が関わるもの

攻撃の対応コスト

人が対応するコストが安いか、機械/サービスに任せる方が安いか
対応が可能な設備/システム/スキルがなければサービスに任せる

責任の所在

サービスを購入すれば、サービス提供者が攻撃に対する責任を負ってくれる
(ただし規約や約款の確認は入念に)

DDoS Mitigation機器やサービスの注意事項

自社で実施する＝自前で機器を購入する
機器はそれなりに高額だけど、自分で納得できるコントロールはしやすい
プロ向けすぎてUIを始め操作はあまりユーザフレンドリーじゃない
導入するにはそれなりに自ネットワークの構成変更が必要

- 攻撃引き込み型ならトンネル、ルーティングなどでの複雑な制御
- ネットワークインライン型なら、全外部接続部分への導入

他社サービスを導入する
それなりに高額だけど、責任を押し付けられるのは魅力
外資系事業者さんを利用する場合は「癖」に注意
日本の事業者さんは高いけど真面目にやってくれるので無茶苦茶言える気がする
運用でカバーしているともいう

一分一秒を止めないように防御は無理
Mitigation機器は動作を始めるまで、それなりにタイムラグがある

- しきい値までの時間
- 攻撃を引き込むまでのルーティングなどの動作

ある程度の攻撃を許容しなければいけないコンセンサスは必須

まとめ

事業者の考え

トラフィックを運ぶことが仕事で、落とすことはイレギュラー
コストと顧客対応は大きく関係する
攻撃は気軽にやってくる、対策は必須と意識する

出来ることをする前に

何ができるか顧客と合意形成をする
対策を実施する/しないを説明できる理由を用意する

事業者が対応できること

攻撃を調査できる設備/システム/人員を用意する
フィルタやNull routingなど設定できることを把握しておく
設定できる内容のリスク管理も合わせて把握

事業者に求められること

攻撃に対するサービス機能拡充や自動化、本気でやるなら相応の有償でもいいのでは
定期的なメンテナンスやオペレーターの訓練、柔軟な対応、体制強化と省力化…

本当に大切なものであればMitigation機器や他社サービスも検討するべき
導入するのに必要なことはもう一度確認