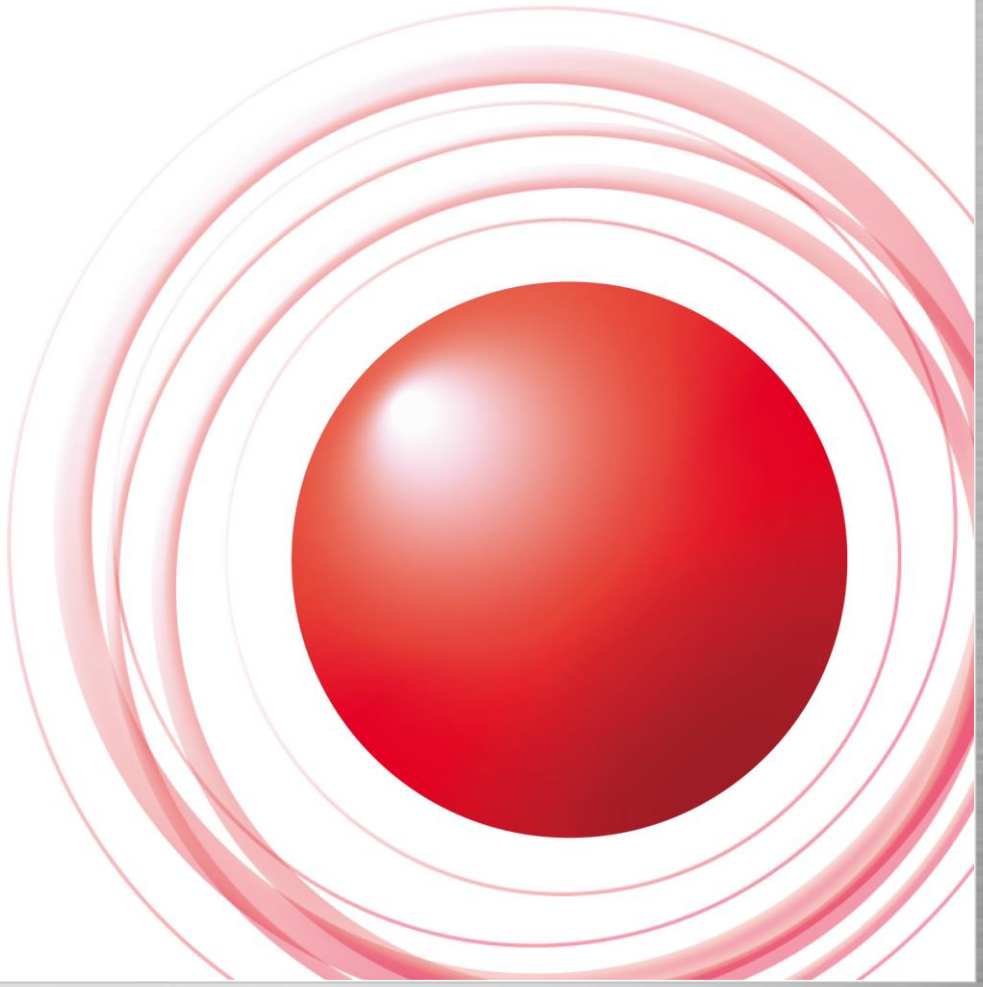
# 顧客と事業者の関係性、契約、コンセンサス

IIJ
Internet Initiative Japan



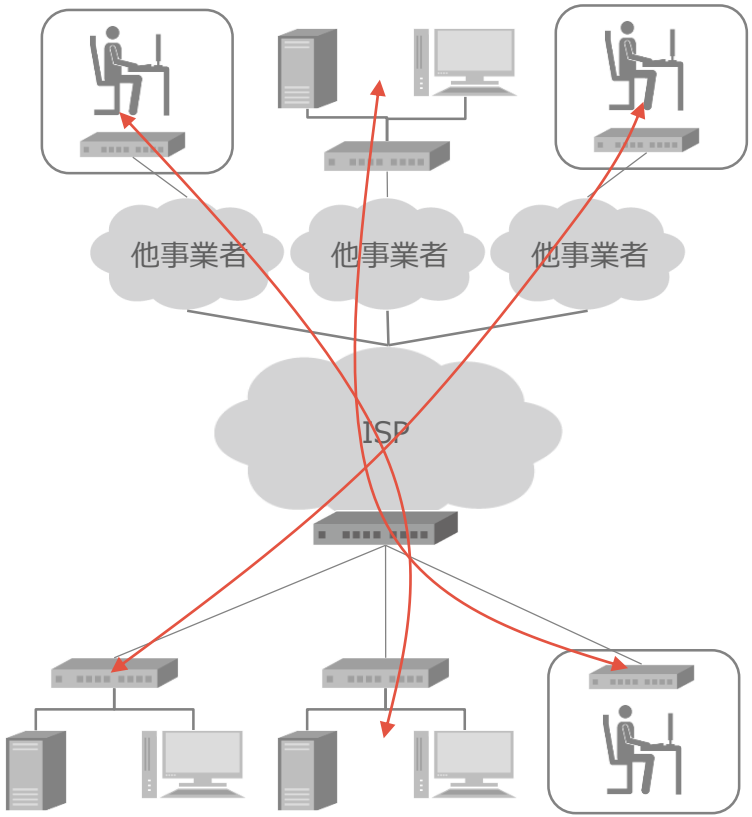
株式会社インターネットイニシアティブ
原 孝至 hara@iij.ad.jp

Ongoing Innovation

# 事業者(ISP)のビジネスを知る

# 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

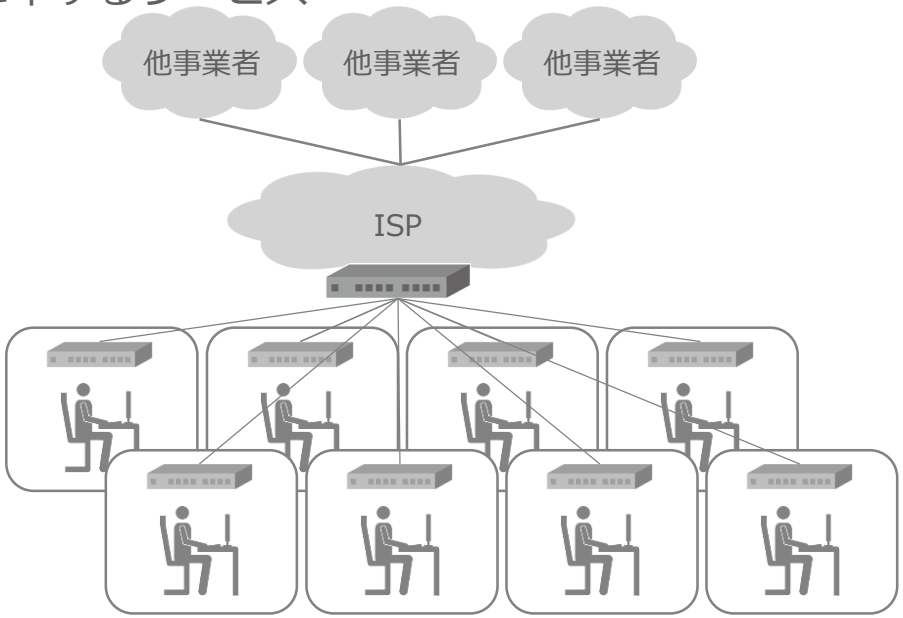



- 郵便会社がたくさんの郵便物を取り扱う
- 運送会社がたくさんの荷物を取り扱う
- 鉄道会社が乗客を電車で大量に遠くまで運ぶ
- 航空会社が乗客を飛行機で遠くまで運ぶ

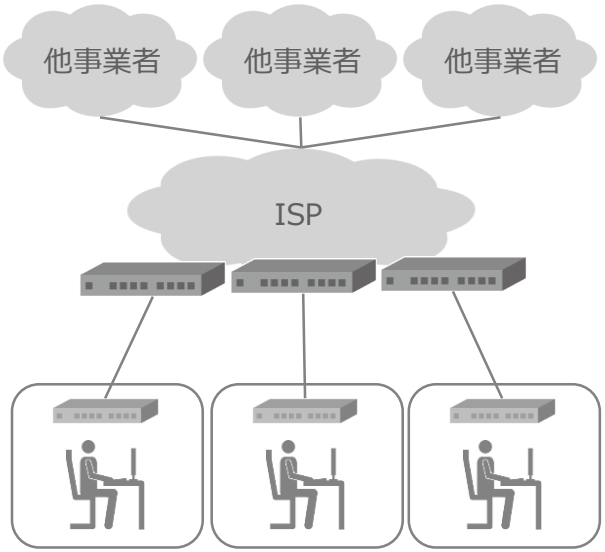
トラフィックを運ぶことが本業で、止めることは本来の事業ではない

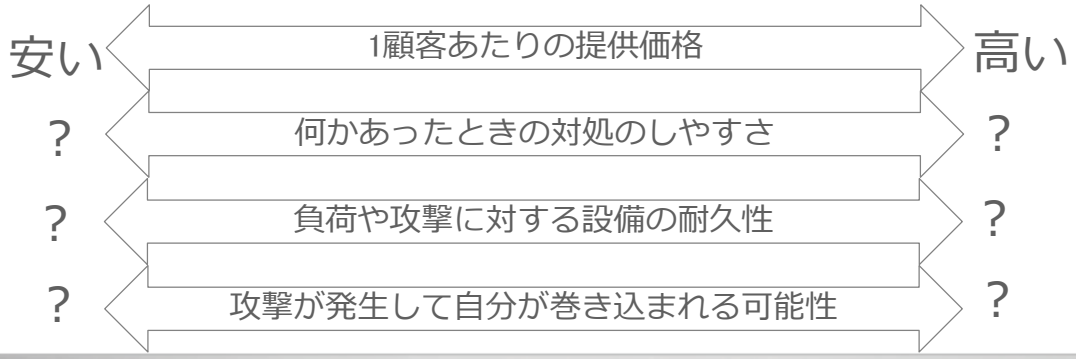
# 事業者のビジネス(利益)

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



# 事業者(ISP)の考えを知る

# 事業者の通信に対する考え(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」とは以下の行為が禁止される
①知得(ちとく)　積極的に知ろうとすること、知ること
②漏洩(ろうえい) 他人が知り得る状態にすること
③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事業者は対象外
→あくまでも「通信の秘密」の問題

# 事業者の通信に対する考え(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

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/

# 実際の運用例(IIJ約款)

http://www.iij.ad.jp/svcsol/agreement/regulation/

## 通信の秘密について

第9章 契約者情報
第37条（通信の秘密）
当社は、通信の秘密に係る契約者の情報について、電気通信事業法（昭和59年法律第86号）第4条を遵守した取り扱いを行うものとします。

2 前項のもとに、当社は、契約者の同意がある場合、第41条（業務委託）に基づき業務委託を行う際に必要がある等正当な業務行為である場合並びに法令の定め（当社の事業を管轄する監督官庁が示す指針又はガイドラインを含む。）に基づいて許容される場合に限り、前項に定める通信の秘密を知得、利用（当社の電気通信設備及び契約者の通信の安全性確保の観点から、通信記録を統計処理すること、及び、その処理結果によって得られた知見について個別通信の特定を不可能とした上で契約者に情報提供すること又は公開することを含む。）、又は第三者に開示する場合があり、契約者はあらかじめこれらについて同意するものとします。

## サービス提供停止について

第6章 利用の制限、中止及び停止並びにサービスの廃止
第23条（利用の制限）
(前略)非常事態が発生し、若しくは発生するおそれがあるときは、(中略)、IIJインターネットサービスの利用を制限する措置を採ることがあります。

第24条（利用の中止）
(2) 当社が設置する電気通信設備の障害等やむを得ない事由があるとき

第25条（利用の停止等）
(3) 第19条（禁止事項）の規定に違反したとき

第19条（禁止事項）
(1) 違法、不当、公序良俗に反する態様(略)
(2) 当社又は当社のサービスの信用を毀損するおそれがある態様(略)
(3) 当社のサービスを直接又は間接に利用する者の当該利用に対し支障を与える態様(略)

# 実際の運用例(IIJのabuse説明)

http://www.iij.ad.jp/svcsol/agreement/regulation/info.html

## abuse行為

2 abuse行為が確認された場合の対応手順
当社においてabuse行為を確認した場合、または、当社においてabuse行為が行われたと信じるに足る合理的な理由がある場合で、サービスを停止する必要があると当社が判断するときには、ご契約のサービスを停止します。

3 行為者の責任の帰属
ご契約サービスを使用してabuse行為が行われた場合は、その実際の行為者の如何などに関わらずお客様の責任となります。

別記
15. 伝送速度の高い回線を利用している場合において、大規模なトラヒック量の通信をすることにより、複数ユーザで共有される通信帯域の多くを専有する行為
19. 上記の他、当社の設備に著しく負荷を及ぼす態様でサービスを利用する行為

**攻撃を受けている場合でも他顧客から見ればabuse行為を行っている行為者になる**

- 攻撃をされているのは自分だけではない
- 攻撃を行ってしまっている側であれば言うに及ばず

# 事業者の通信に対する考え(本音)

サービス規約や約款を持ち出して正論を吐くのは簡単だが、ビジネス的には…

- のちほど「必要性」「妥当性」の検証は必要になると思われる
  とくに日本人相手には
- 攻撃発生中に顧客(とその後ろにいるであろう上席)に、これまでのことを
  「すばやく」「簡潔に」「誤解なく」伝えるのは非常に困難と思われる
  とくに日本人相手には
- 攻撃でいっぱいいっぱいの顧客に規約や約款とか言った瞬間、顧客は**大爆発**するよ？

やっぱり、通信の秘密に関わることには触れたくないな！！
フィルタもやろうと思えばできるけど実施の一線を超えるのは怖い！！

事業者自身の設備に影響が起きている状態でないと能動的には動けない
(事業者が自衛のための正当防衛、緊急避難)

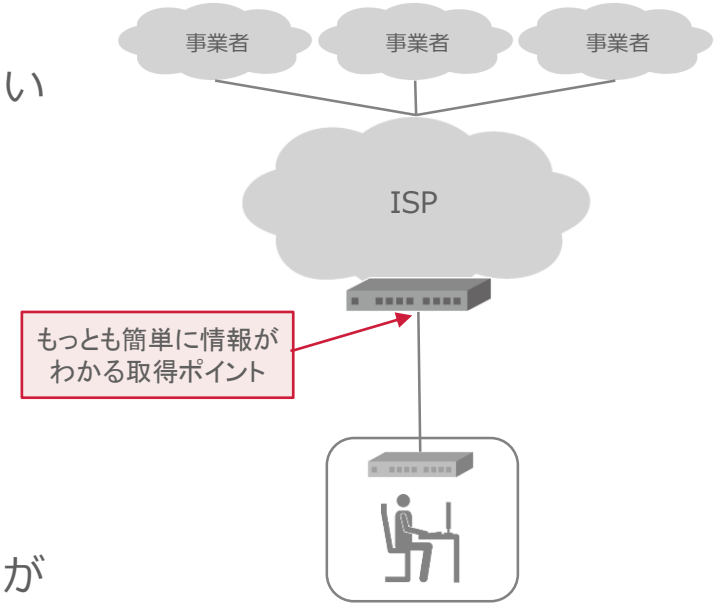
顧客からの申告ベースでの対応が望ましい！
(顧客依頼の正当業務行為)

# 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

顧客側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情報から調査するのが
一番手っ取り早いと思われる



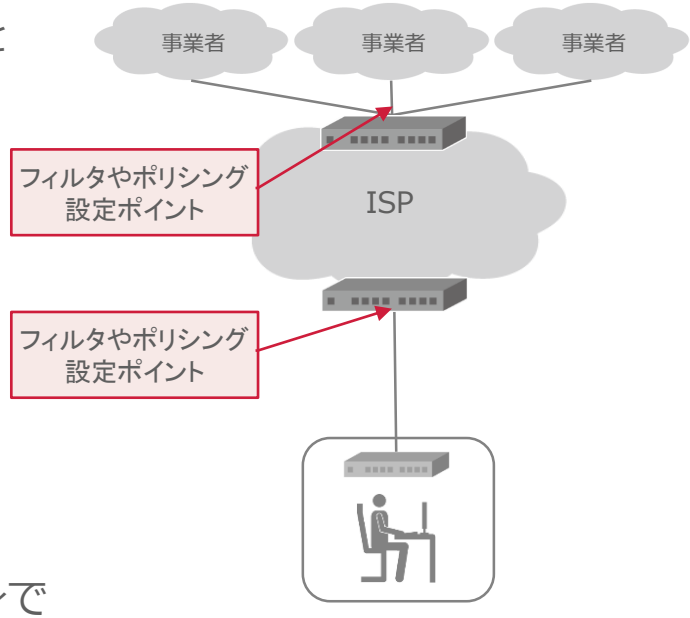

Flow解析機器やソフトウェアは
ほとんどの事業者は手段として持っていると思われるが
通信の中身を探れる手法を持っているというのは前述の通り
顧客に対して説明が難しいので存在は隠したい…

# 攻撃と思われる通信を遮断する方法

- 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(そもそも攻撃で止まってるけど…)

- 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

- Null routing
  - ルーティングは宛先しかみないため、送信元を判断しては遮断できないが効果は絶大
  - 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
  - 結局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




- 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

# 各手段に思うこと

# 通信を調査することの注意点

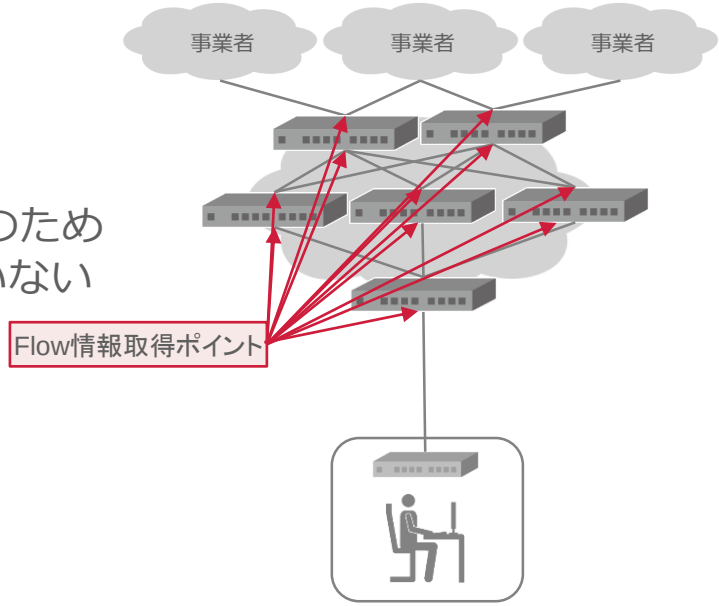
**Flow情報はあくまでもサンプリング結果**

通信のおおよその傾向をつかむことはできるが、通信の中身自体をそのまま取得しているわけではない

→宛先アドレス、送信元アドレス、ポート番号、プロトコルなど最も多い傾向のものから探し出すことになる

→攻撃の通信を見つけるのは比較的容易だが、本来あるべきだった正しい通信は少数派のはずなので、調べるのは骨が折れる

→保存期間やデータの完全性などはあまり期待しないでもらえると…




**やっぱり「通信の秘密」**

攻撃以前からFlow情報を取得、保存することは万一のための正当業務行為と主張できるが顧客に同意を取っていないことは説明が難しい

→保存されている情報の安全は大丈夫？漏洩しない？

→適正に利用されている？

他の用途(マーケティングとか)に流用されてない？

→説明する？できる？

→同意できる？できなかったらどうする？

# 通信を遮断することの注意点(ACL)

- Access Control List(ACL)
  - 超めんどい！適用まで時間かかる！そもそも通信を止めるのは仕事じゃないから怖い！

**依頼とコンフィグ**

対応中どこかの部分でどうしても適用まで時間がかかる
コンフィグを直接いただければ一番適用まで速いが…

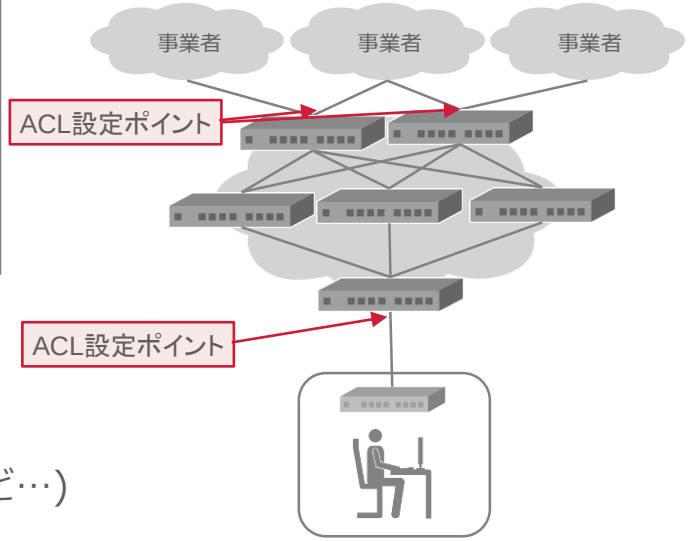
宛先アドレス
192.0.0.0～192.0.224.255
198.51.229.0～198.51.250.255
203.0.254.0～203.0.255.255

ポート/プロトコル
53/UDP
80/TCP,UDP

を遮断してください

```
!
ip access-list extended DOS-FILTER
 deny udp any 192.0.0.0 0.0.127.255 eq 53
 deny udp any 192.0.128.0 0.0.63.255 eq 53
 deny udp any 192.0.192.0 0.0.31.255 eq 53
 deny udp any 192.0.224.0 0.0.0.255 eq 53
 deny udp any 198.51.229.0 0.0.0.255 eq 53
 deny udp any 198.51.230.0 0.0.1.255 eq 53
 deny udp any 198.51.232.0 0.0.7.255 eq 53
 deny udp any 198.51.240.0 0.0.7.255 eq 53
 deny udp any 198.51.248.0 0.0.1.255 eq 53
 deny udp any 198.51.250.0 0.0.0.255 eq 53
 deny udp any 203.0.254.0 0.0.1.255 eq 53
 deny ip any 192.0.0.0 0.0.127.255 eq 80
 deny ip any 192.0.128.0 0.0.63.255 eq 80
 deny ip any 192.0.192.0 0.0.31.255 eq 80
 deny ip any 192.0.224.0 0.0.0.255 eq 80
 deny ip any 198.51.229.0 0.0.0.255 eq 80
 deny ip any 198.51.230.0 0.0.1.255 eq 80
 deny ip any 198.51.232.0 0.0.7.255 eq 80
 deny ip any 198.51.240.0 0.0.7.255 eq 80
 deny ip any 198.51.248.0 0.0.1.255 eq 80
 deny ip any 198.51.250.0 0.0.0.255 eq 80
 deny ip any 203.0.254.0 0.0.1.255 eq 80
 permit ip any any
!
interface Gi1/0/1
 ip access-group DOS-FILTER out
!
```

フィルタは顧客に最も近い位置で設定するが
影響が酷ければより上流で設定




**準備がツライ、適用時は緊張の瞬間**

変換スクリプトなどで省力化はできるが
やっぱり最後に適用するのは人、それはもう必死！
→読み違えてたら？
→そもそも依頼が間違ってたら？(確認はやれる範囲でやるけど…)

**そもそもそんなにACL設定してルータは耐えられるの？**

→数10GbpsフォワーディングしてFlowをexportやらSNMP GETしてても耐えられる？
→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部巻き込んでしまう！

# 通信を遮断することの注意点(RTBH、Flowspec)

- Remote Triggered Black Hole(RTBH) filtering/routing
- BGP Flowspec

**難しい**

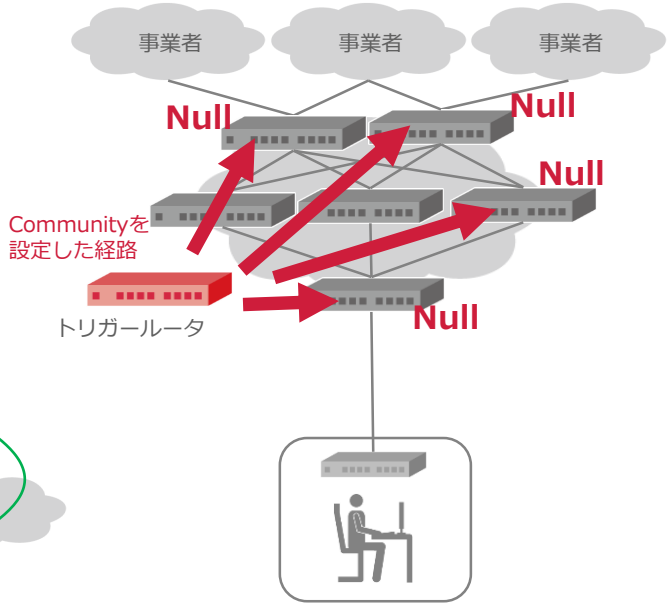
設定によってどうやって動作するか把握は大丈夫？
少なからずBGP設定が必要なのでオペレーションは大丈夫？
どのようなBGP communityを設定すればよいか攻撃時に確認するのは大丈夫？

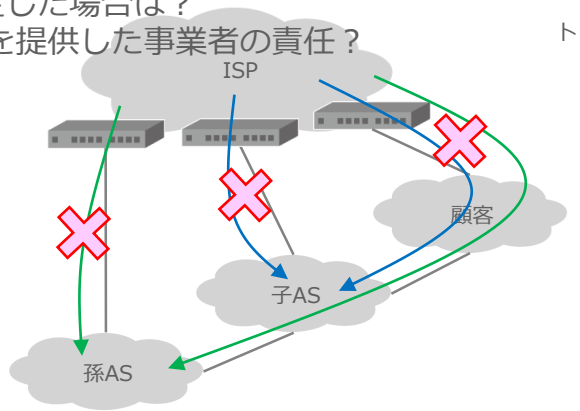
**設定時の責任問題**

ACLは事業者の責任で実施されるが顧客自身での責任で
実施される
→もし設定ミスしたら誰のせい？
→設定と期待する動作に違いがあった場合は？

**子AS孫AS問題 (IIJ用語)**

事業者と顧客に接続しているAS(子AS、孫AS)があった場合、
顧客が子ASや孫ASの経路についてRTBHなどを発動させた場合、
事業者に接続する通信がすべて遮断されてしまう問題
→どうやって防ぐ？顧客が意図して設定した場合は？
→子ASが遮断された場合、それは方法を提供した事業者の責任？
→さらにその先の孫ASがいたら？



# 実際に攻撃が来た！

## 事業者に連絡しようの前に

**連絡するその前に伝える必要があるかもしれない情報を可能な限り収集しよう**

- ホストに設定されているIPアドレス
- ホストで動いているサービスはなにか？
  - Web、DNS、Mail、VPN、SSH、NTP
  - ECサイト、匿名掲示板、動画サイト、オンラインバンキング、コーポレートサイト、
    ゲーム配信サイト、インターネットゲートウェイ用FW
- ホストはなに？
  - ルータ、スイッチ、サーバ、アプライアンス機器…
- ホストへのアクセスログ
  - IPアドレス
  - TCP、UDP、GREなどプロトコル

**サポート窓口も人間**なのでいかにヤバイものが停止に
追い込まれているかを伝えれば
ちょっとでも迅速な対応を引き出すことが出来るかもしれない！

状況確認
連絡
遮断対応
復旧対応

# 事業者に連絡しよう

**サポート窓口に連絡する**

- 電話
  - 電話番号は確認OK？
  - 電話口で伝える内容は確認できてる？
    - 会社名
    - 担当者名
    - サービス識別子、回線IDなど
  - 問い合わせ担当者としての事前登録
    - コールバック認証など
- メール
  - メールアドレスは確認OK？
  - メール本文中に何を書くか
    - 会社名
    - 担当者名
    - サービス識別子、回線IDなど
    - なにが問題か、なにを対応してほしいか
  - 電話で確認入れるものやはり必要
  - 問い合わせ担当者としての事前登録
- Web窓口、チケットシステムなど
  - URLは確認OK？
  - ログインID、パスワード、認証システム
  - 選択画面
    - サービス識別子、回線IDなど
    - なにが問題か、なにを対応してほしいか
  - 事前にログインして操作感を確認
  - インターネットの障害だけどアクセスは確保できてる？

**本当にヤバイなら担当営業さんに連絡する裏技も**(このための法人契約！)

- 連絡先知ってる？
- 話しやすい？
- 対応してくれそう？

状況確認
連絡
遮断対応
復旧対応

## 事業者とやり取り

**まずは落ち着く**
焦る気持ちはわかるけどサポート窓口を怒鳴りつけても攻撃は収まらない

- わかっている情報はすべて伝える
- 自前で調査が不可能であれば、事業者にお任せしてしまう

**「攻撃が来ていて困っているが、状況が確認できないので、調査して遮断してほしい」**
(通信の秘密をクリアする正当業務行為の依頼)

遮断時は、事業者から確認が入るはずなのですぐに連絡を受け取れる状態にいること
- 上長への報告、エンドユーザへの報告は別のメンバへおねがいして、
  復旧対応に集中する
  - 上長やエンドユーザへの連絡しながら、復旧にむけての対応をするのは
    相当の熟練職人でないと無理
- 対応中はある程度人数の確保は必要

状況確認
連絡
遮断対応
復旧対応

## 事業者が困る対応とその対策

### 複雑なルールを伴うフィルタ

- SRCポート、DSTポートの組み合わせなどルールが多数になるもの
  - 急ぎで設定するのでは…
  - フィルタルールは可能な限り簡易に
  - 複雑なルールにしなければいけないのであれば、Cisco ACL形式で作成して連絡してしまう(おそらく業界共通言語…)

### 一般的な答えがない依頼

- ○○国からの通信を遮断してほしいなど
  - ○○国とはなにか
    - ISP、IPアドレス、地域、人、接続点
- 海外からの通信を遮断してほしいなど
  - 海外とは何か
    - ISP、IPアドレス、人、接続点
- 復旧最優先なので、あまり細かく考えずバッサリ落として少しずつ開けていく対応の検討を

### 連絡がつかないこと

- フィルタ設定前後の連絡がつかない
  - 事業者に指示を出せる体制づくりを

状況確認
連絡
遮断対応
復旧対応

## 遮断対応が終わったら

**何をもって対応の終わりとするかを事業者に伝えよう**

- 期間
  - 翌営業日まで様子見をして解除する
  - 一週間様子見をして解除する
  - 特定の国の長期休暇以降に解除する
- 対策の実施
  - アクセスログ取得の準備
  - 絞り設定、アクセス制限設定
  - ホストの強化、移設
  - 攻撃対策サービスの検討導入

**遮断解除時の対応は**

- 攻撃が来ていないことを確認して解除
  - 事業者に確認してもらう
  - 解除したらホスト側でもアクセス確認
- 事前事後連絡をする、もらう

**フィルタはある程度のタイミングで解除しないとトラブルのもと**

- 事業者側で設定されているフィルタは確認が面倒
- フィルタ依頼をした自社担当が異動になったら…
- ある日エンドユーザからアクセスが出来ないと問い合わせがあったら

状況確認
連絡
遮断対応
復旧対応

# 対応してわかること

# 事前準備は対応の9割

## 契約している事業者が何が出来るのか確認しておく

- 調査はしてもらえるのか、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相談をする、程度により別途覚書を交わしておく

## 社内でもコンセンサスを準備しておこう

- 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把握しておく
- 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)
- 事業者に開示できる情報はどこまでか
  - そもそも信用できない事業者を使っているのは…
- 遮断と解除を判断する人は誰か
  - 発見した担当者？特定の上長？事業者におまかせ？
  - 24時間いつでも判断できる？判断できなかったらどうする？

## 事業者にも定期的にコミュニケーションをとっておくのをオススメ

- 日本の事業者さんはとっても真面目
- 担当営業さんに相談しておくといい対応を提案してもらえるかも
- やっぱり人間が対応しているので「あの人(会社)だったら対応しようか」はある！

# 覚書とは

**一般に通常サービスにおいて提供されていない機能を提供する/受ける場合に交わすもの**

- サービス規約や約款で謳われている機能の提供であればそもそも覚書は必要ない
- リスク対応など程度に応じて双方の法務的な部署へ相談する

**覚書の例**

- 提供するもの
  - 乙(事業者)は甲(顧客)に対し、○○の機能を提供する。
- 費用
  - 別途提示する見積による。
  - 無償で提供する。
- 注意事項、免責事項
  - 機能の仕様や完全性、保証、対応時間など。
  - 利用により発生した事象による不利益や損害についての責任。
- 提供の一時停止、恒久停止、禁止事項。
  - メンテナンスの取扱
  - 解約や不具合などに伴う、提供の終了。
  - Acceptable Use Policy(AUP)
    - 違法に、または公序良俗に反する態様での利用の禁止
    - 利用に対し、重大な支障を与える態様でのサービス利用の禁止
      - 規約、約款にあるから改めて書かないかも

**あまりガチガチに決めてしまうとやりづらいので適度な落とし所の相談を**

→覚書に書いてないからやらない、書いてある事以上はやらない、など…

# まとめ

**契約している事業者の考えを把握しておこう**
- 事業者は運ぶことが本業
  - フィルタなどに積極的でないこともあるかもしれない
  - そもそもフィルタができるかどうか

**契約している事業者の対応方法を把握しておこう**
- 手段、契約、費用
- 仕様、注意事項、免責事項
- 窓口の対応
- 連絡先

**事業者を動かそう**
- 「攻撃が来ていて困っているが、状況が確認できないので、調査して遮断してほしい」
  - 事業者の正当業務行為へ！

**自システムの対応を決めておこう**
- 遮断の判断、解除の判断
- 攻撃発生時の対応フロー、連絡フロー
- 対応に納得できなければDoS/DDoS対策サービスを使うかどうか

**事業者とコミュニケーションを取っておこう**
- ICTは大事