JP AAWG JAPAN ANTI-ABUSE WORKING GROUP

IPv6 BlockListで困った話

フリービット株式会社 技術本部 クラウドサービス部

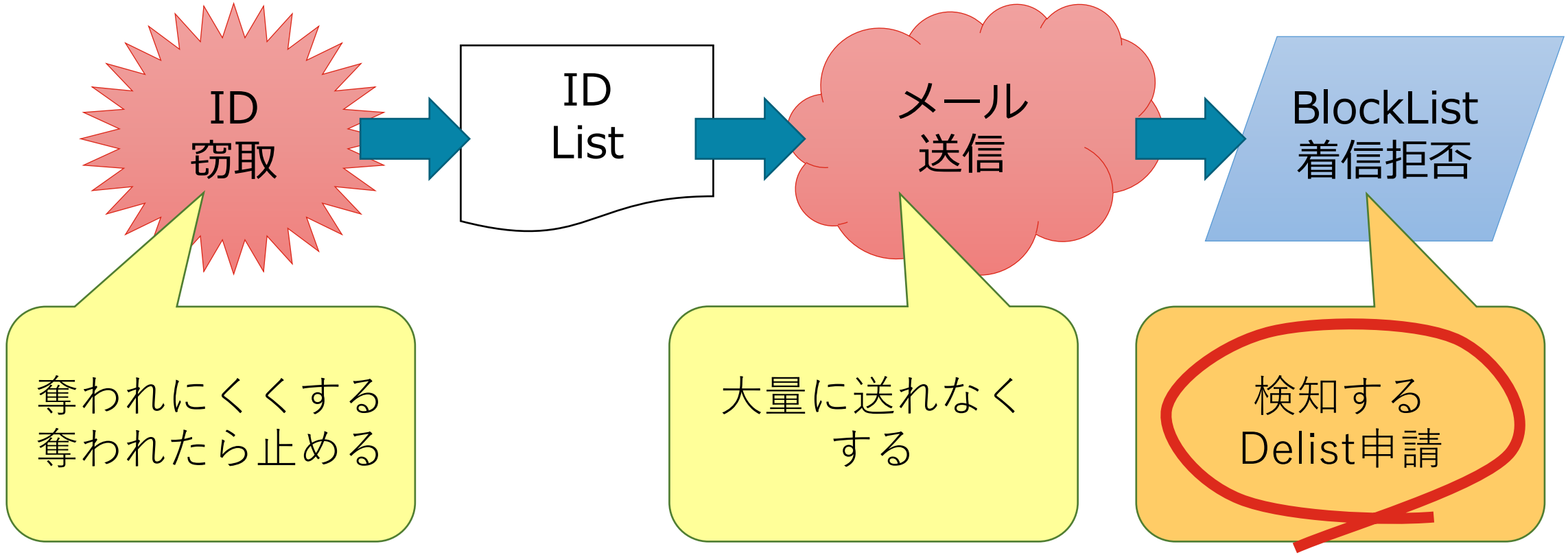
三浦 敏孝

自己紹介

- フリービット株式会社: ISPサービスをOEM提供など
- 割と何でも屋に近い、開発もする運用担当
- 1999/4～ DTI
  - ISPのサーバサービス全般
    - DNS, Radius, WWW, Mail, … (NWと顧客DB以外何でも)
  - 調達関係、対外接触、データセンタ構築運用
- 2007/8～ フリービットに買収され、遊撃隊仕事
  - その中でGmail対抗メールサービスの開発・構築・運用
- 2015/5～ フリービットに転籍
  - 現在はOEM向けメールサービスとDTIのISPサーバサービス運用担当

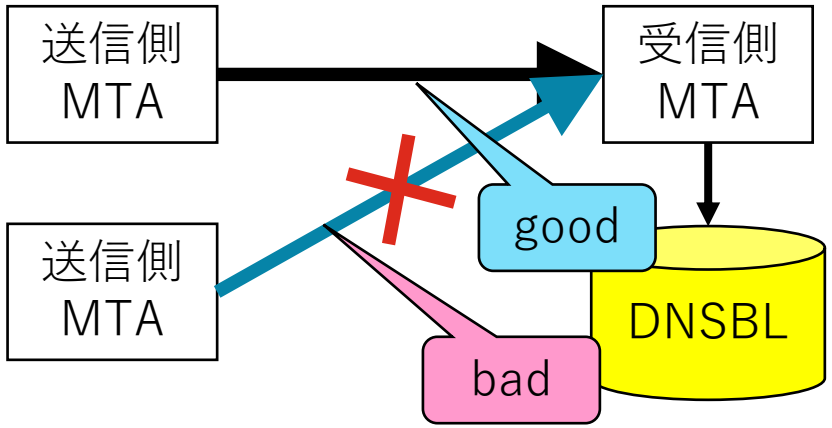
乗っ取りspammer: 積年の課題

- ひとつの対策では効果が低くて、spammerのワークフロー全体に対する打ち手が必要



IP Blocklistとは

- Spam送信実績を収集した「spam送信元IP」のリスト
- 載ると受け取ってもらえなくなる
- DNSをAPIとするのがポピュラー(RFC5782)
- 勝手リストなので世の中に沢山



- OP25Bのない世界では有効
- ISPのMSAで乗っ取りアカウントを使われると善意の送信者も割を食う
- 有名どころ
  - Cisco TALOS、ProofPoint、Barracuda等フィルタ箱ベンダ系
  - McAfee、TrendMicro等セキュリティソフトベンダ系
  - SORBSなど草の根系
  - Spamhaus ←今回の話題

送信側ISPのIP BlockList対策

- 有名どころを定期パトロール
  - DNS公開してたら引けばよい
  - TALOSだけは人力周回
  - MxToolBoxみたいなまとめてチェックサービスも使う
- 載ってたらdelist申請
  - もちろん該当spammerアカウントは止めてから
  - SORBSは「該当IPから申請せよ」なので送信サーバ多数あると大変
- 影響が大きくてdelistに時間がかかる場合はIPつけかえ
- ここまでは普通にやることですが……

IPv6 Blocklist問題

- メールサーバはMXに記載された名前にAとAAAAが両方書かれていたらAAAAを優先する
- SpamhausはIPv6アドレスを64bit prefix単位でブロックする!
  - /64なプライベートクラウドに複数テナントを収容して専用IPを/127とかで割り振っているとサービス全体が一蓮托生に
  - 日本の某政府機関が参照していて、例の調査をする季節になると「届かない」という問い合わせが一度に複数来る
  - 一応、B-Treeベースの格納方式を開発中とWebサイトに書いてあるページのlast updateが2011年……
    - **Spamhaus IPv6 Blocklists Strategy Statement**

検討中の対策案

- 対策1: 顧客割り当てアドレスをリナンバ
  - サービス全体で/48を確保して顧客専用サーバに/64ひとつずつ割り当てる
    - 弊社の顧客数ならアドレス空間は足りるが、さすがに勿体ない
- 対策2: mailertableで宛先ドメインを引っ掛けてv4 staticに流す
  - そもそも動くのか要検証
  - もぐら叩き: 問合せの温度感が高い宛先に限られる
  - 配送先はIPv4アドレス直書き: 相手先のDNS変更に追従する必要
- いずれもそれなりに重たい

どうすれば皆で幸せになれるか

- IP BlockList/IPレピュテーション自体の需要はなくならないだろう
  - DMARC/ARC検証で数を減らしても乗っ取りアカウント発は残る
  - Gmailのポリシー(逆引き+SPF必須)もたびたび変わるということは……
  - そもそも接続させない、というのは見かけのspam着信を減らすのに魅力的
- IPv6対応のBlockListが少ないからSpamhausが使われる
- ならば、DNSBL用のDB込みのDNSサーバを作って配布すれば……
  - 必要なのはポン付けレシピ: dockerfileとか
  - DB部分は、作る技術と時間があれば、の話だが