2024~2025年末年始にDDoSと戦った人の交換会リターンズ

田島弘隆(taji)

Akamai Technologies

2025年7月31日@JANOG56

はじめに

2024年〜2025年の年末年始のDDoSは一般の報道でも大きく伝えられました。

ミーはセキュリティサービスを提供する組織にて、インシデントレスポンスのプレイヤーとして対応をしました。

そのあたりのナレッジをシェアしつつ会場の皆さんと議論を深めたいと思います。

このセッションについて

- 基本方針
  - ヘルシーなインターネットを作っていくため、経験や知見を個人の立場で交換します
- お約束
  - いちジャノガーとして話します。
  - 資料は公開します
    - (全部オリジナル。ハンドメイドの温かみのあるスライドです)
  - 撮影禁止でしたが、気が変わったので撮ってよいす。
    - 撮るなら無音(微音)シャッターアプリ推奨
    - ミー自身はフリー素材なんで、ご自由に

進め方

- 皆さんとインタラクティブにすすめたいです。
- マイクにいつでも立ってください。
  - 初マイク・初**JANOG**・学生さんを歓迎します。
  - 話の流れで割り込みたい場合は前の人に断ったうえで発言可。
  - リスペクト!
- 大事なことなのでもう一度
  - 本セッションのすべての発言・内容は個人の意見です。

セットリスト

1. 年末年始の攻撃発生状況サマリー
2. ネットワーク攻撃方面(おもにL4以下の話)
3. Web攻撃方面(おもにL7の話)
4. マネージメント方面(おもにL8以上の話)
5. まとめ

多分おそらく絶対1時間で収まる気がしません。時間が押してきたら、ちっと空気読んでください。

年末年始の攻撃発生状況

サマリー

ChatGPT君に聞いた

2024年末から2025年始に発生したDDoSについて、日本で被害が報告されている状況のサマリーを教えて

- 2024年12月26日：航空会社
  - サイバー攻撃により国内線と国際線あわせて71便に30分以上、最大4時間余りの遅れが発生。航空券の販売も一時停止しました
- 2024年12月26日：金融機関
  - インターネットバンキングで障害が発生し、一時的に利用不可となりました
- 2024年12月29日：金融機関
  - 個人向けインターネットバンキングが攻撃を受け、一部サービスが利用困難となる事態が発生。グループ内の複数銀行にも影響が広がりました
- 2024年12月31日：金融機関
  - ネットバンキングサービスが一時停止し、送金や残高照会などのサービスが利用できなくなりました
- 2025年1月2日：通信会社
  - 複数のサービスが、大規模なDDoS攻撃を受け、アクセスしづらい状況に陥りました
- 2025年1月5日・9日：気象サービス機関
  - DDoS攻撃によりアクセス不能となり、特に雪が多い地域での気象確認が困難となりました。

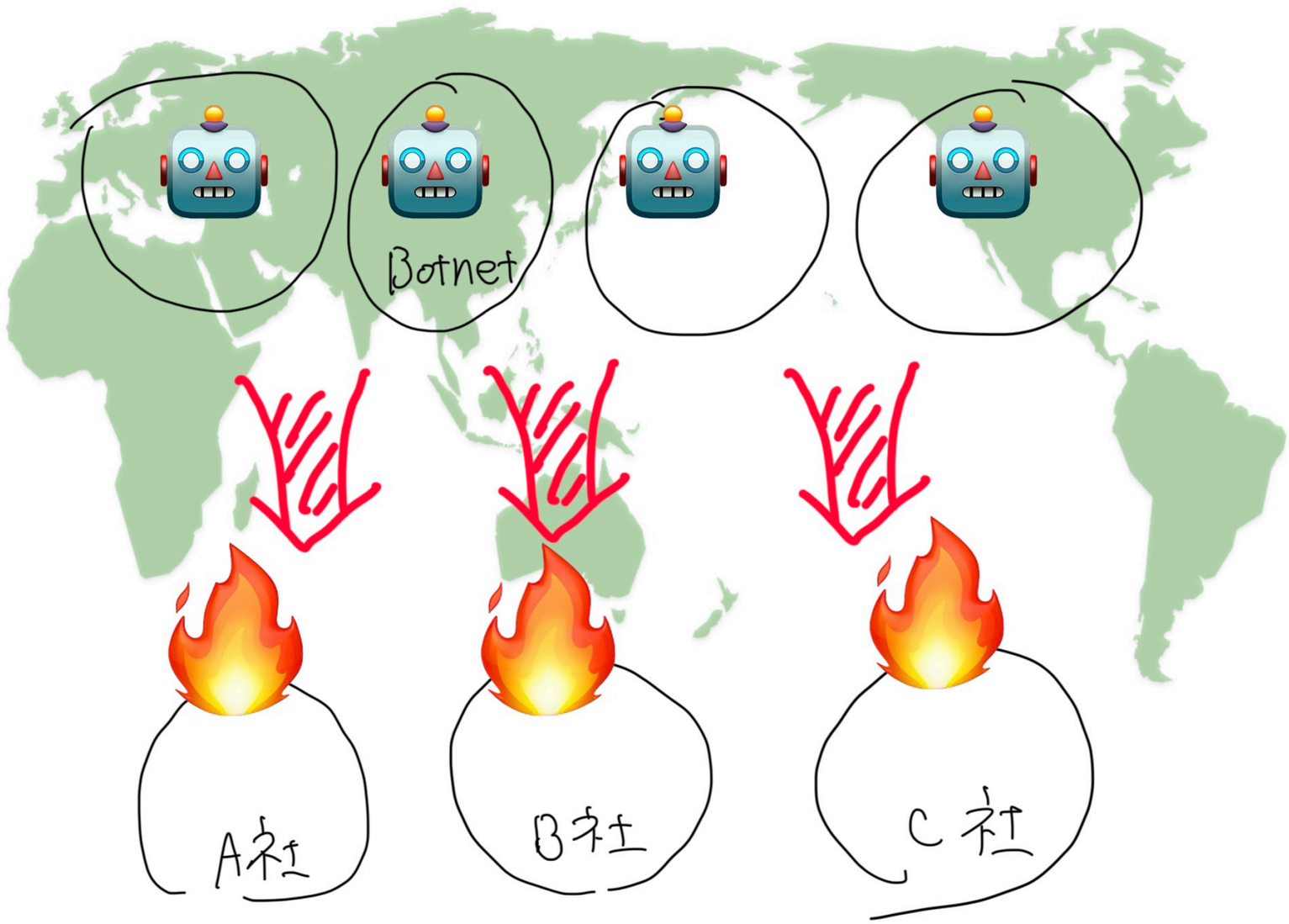
- 🔍 攻撃の特徴と背景
- ターゲットの多様化：金融機関や通信サービスだけでなく、航空業界や気象情報サイトなど、生活インフラに密接なサービスが狙われました。
- 攻撃の目的：金銭要求を伴うランサムDDoS が一般的な動機とされるが、混乱を目的としている可能性が高いと指摘されています。
- 年末年始というタイミング：多くの人がWebサービスを利用する繁忙期を狙った攻撃は、影響範囲を拡大させる意図があったと考えられます。

ネットワーク攻撃方面

(おもにL4以下の話)

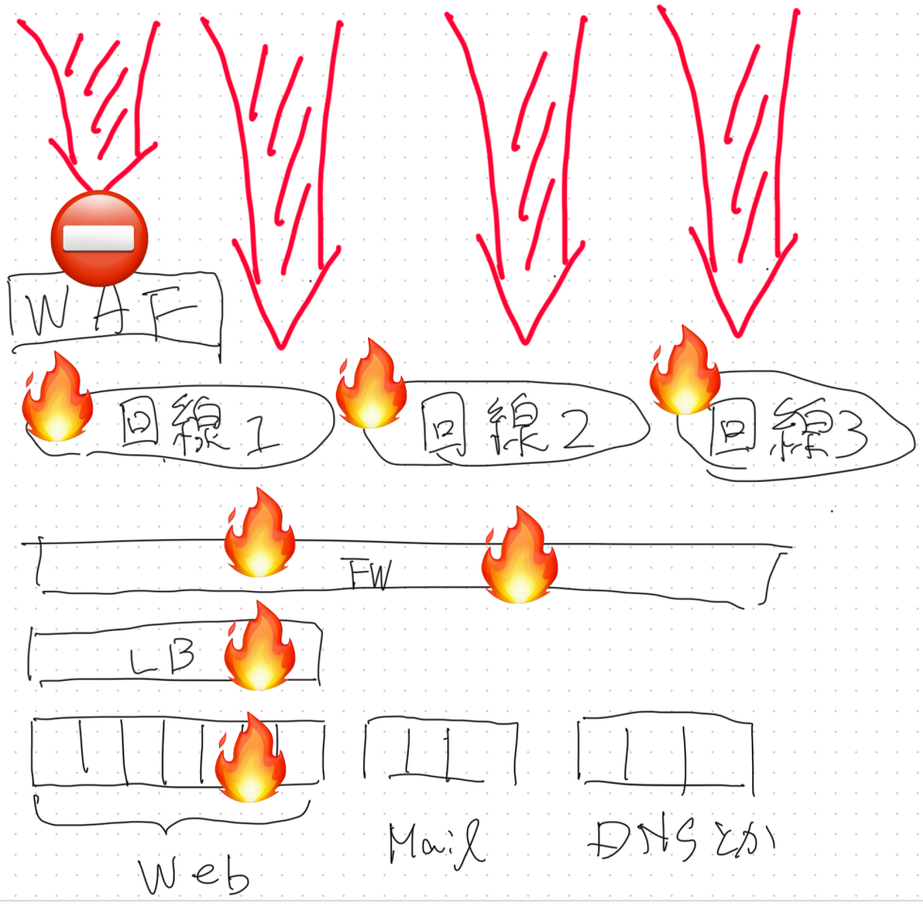
分散度が非常に高い

- 送信元はワールドワイドで非常に分散度の高い攻撃
- 送信先も同時期に多数の社会的影響力にあるサイトを攻撃



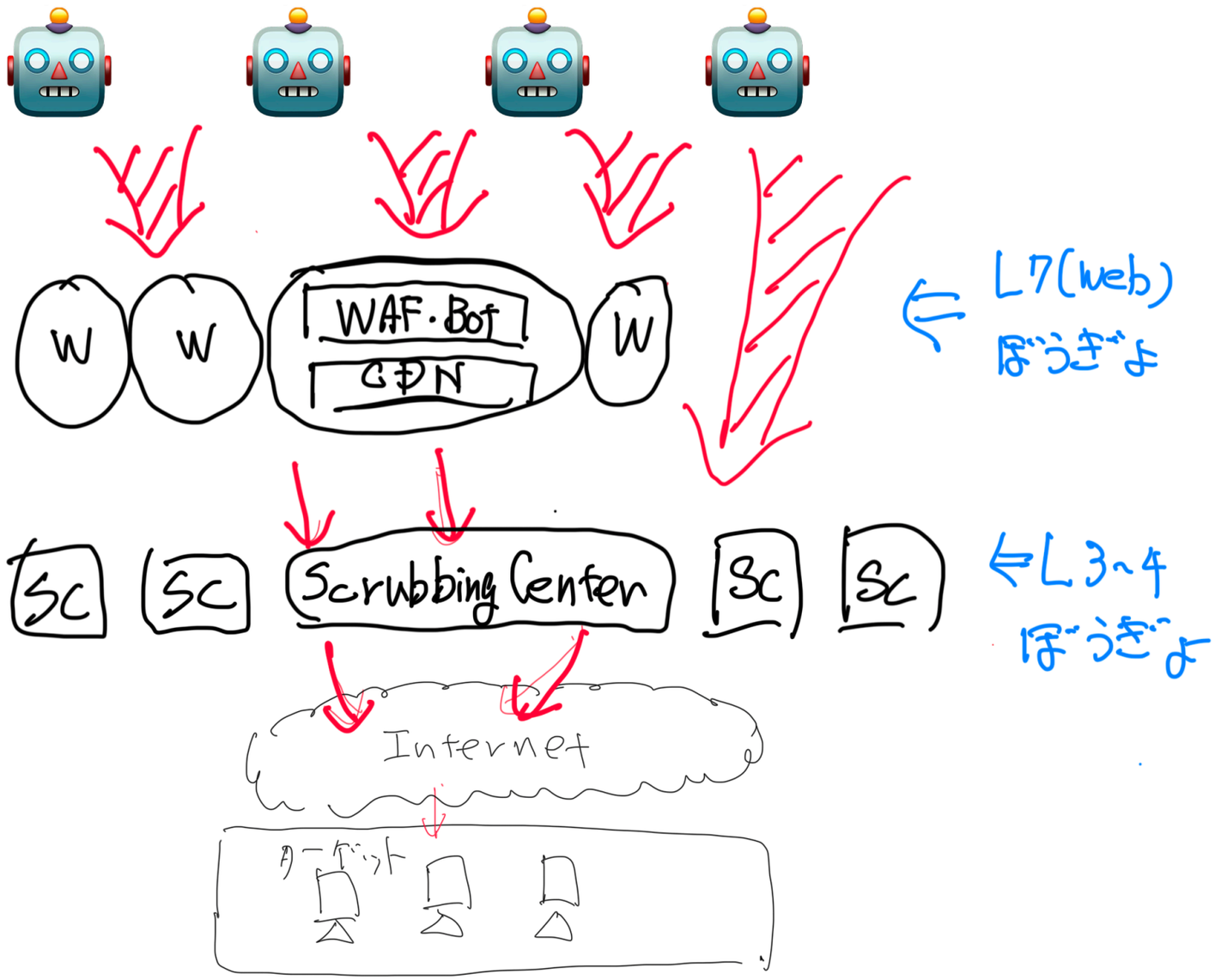
攻撃対象のPrefixを網羅的に攻撃

- WebサービスはWAFで保護されている一方、オリジンサイトを含むPrefixを網羅的に攻撃してきた
  - Webサービスは保護できてもNW帯域とかFW、LB等がキャパオーバーしてしまう



DDoS防御

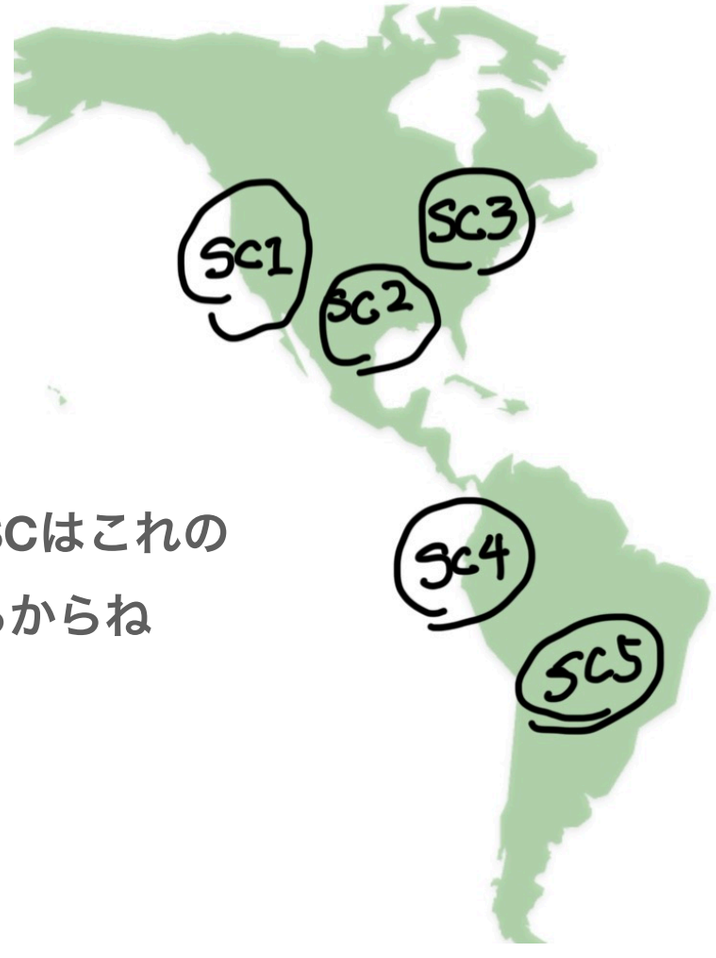
- 世界中に分散されたWAF・CDNエッジ鯖とScrubbing Center(SC)でDDoSを緩和する



「海外IPは遮断していいよ」

- 国内向けサービスだから海外IPは遮断してってよく言われるけど、DDoSの場合、実はこれ結構むずかしい

- 送信元IPがどれほどアテにならないか見てみましょう

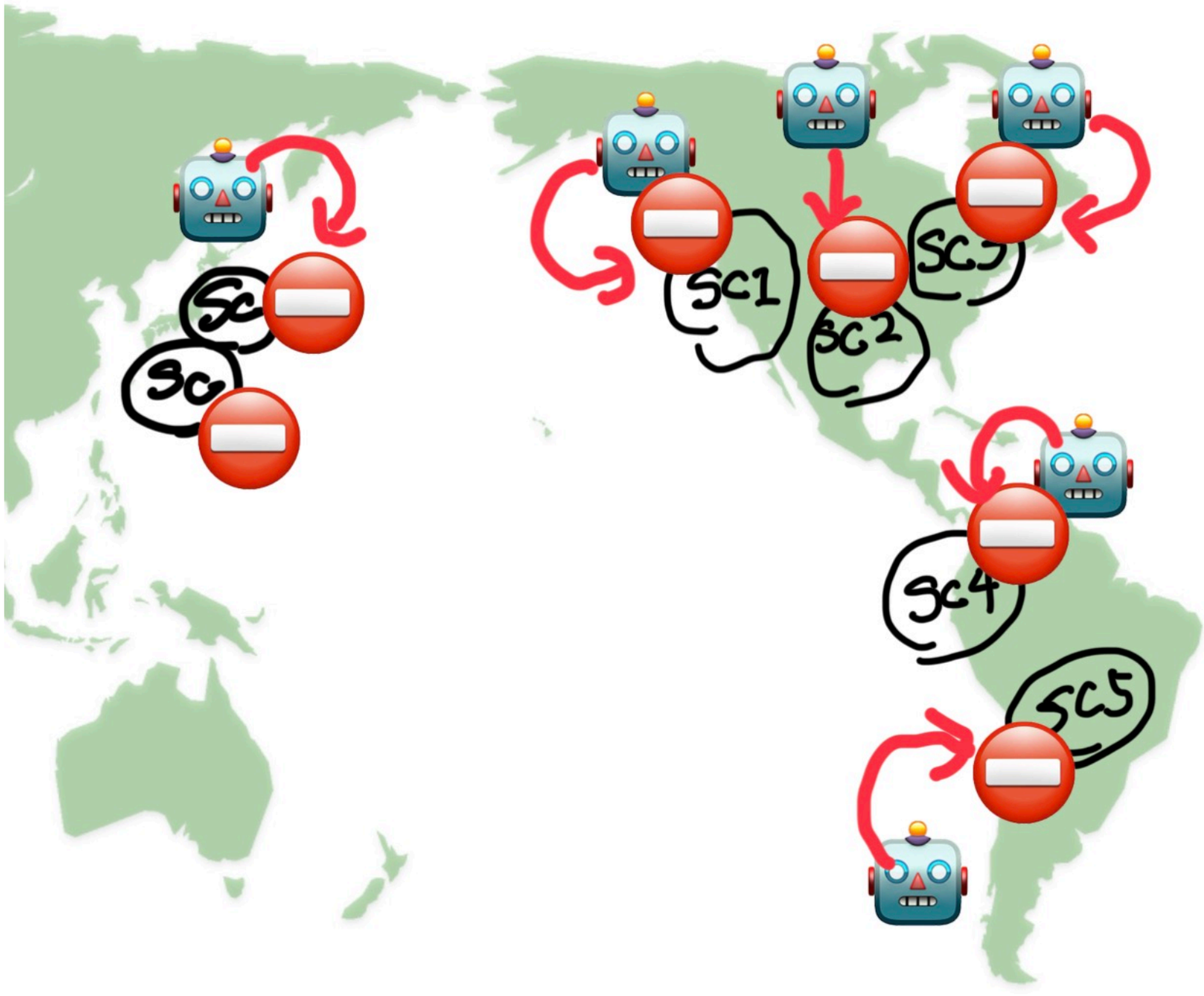


(注)実際のSCはこれの
N倍あるからね

SC1で吸い込んだDDoSの送信元IPのGEO情報

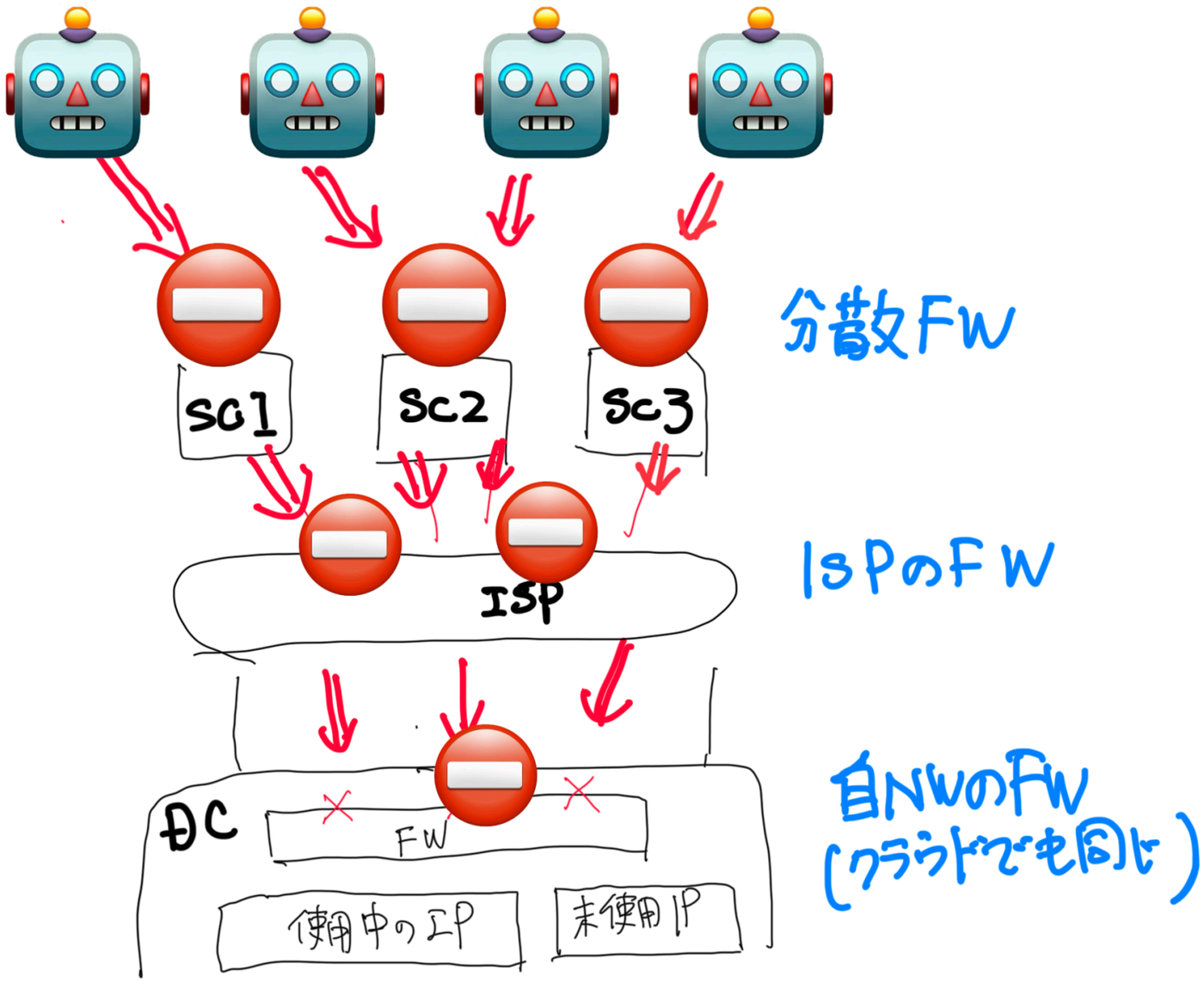
US-CN-JP-KR-DE-BR-GB-FR-IT-AU-CA-NL-RU-TW-IN-ES-SE-ZA-MX-EG-PL-AR-SG-ID-VN-HK-MA-CO-BE-CH-IE-TR-NO-CZ-IR-UA-DK-AT-TH-FI-SA-PK-RO-CL-BG-IL-HU-MY-VE-PT-TN-GR-PE-KE-AE-PH-na-RS-HR-MU-SK-NG-DZ-OM-KZ-LT-EC-LV-UY-NZ-CR-SI-DO-SY-PY-PR-BO-CI-BY-TZ-KW-BA-EE-BD-MO-MD-MT-AO-RE-PA-IQ-NP-CY-TJ-GH-SD-IS-TT-LR-SV-UG-CM-ZM-PS-MW-JO-QA-AF-LK-TG-GE-GT-YT-ME-NA-SZ-BZ-KG-LU-UZ-AG-AD-IM-KH-ET-LY-NE-MG-LS-VG-TL-AM-LA-MK-MM-GI-JE-BH-BW-BS-BQ-GA-

送信元IPに頼らず
できるだけ発信元の近くで叩き落としたい



ネットワーク攻撃方面のベスプラ

- なにはなくとも未使用IP空間と未使用ポートはブロックする
  - ブロックしやすい順: 自NWの入口→上流ISP→分散FWサービス
  - 効果の大きさはこの逆:分散FW→上流IPS→自NWの入口
- Webサービス提供してるならWAFは必須(次の章で話します)

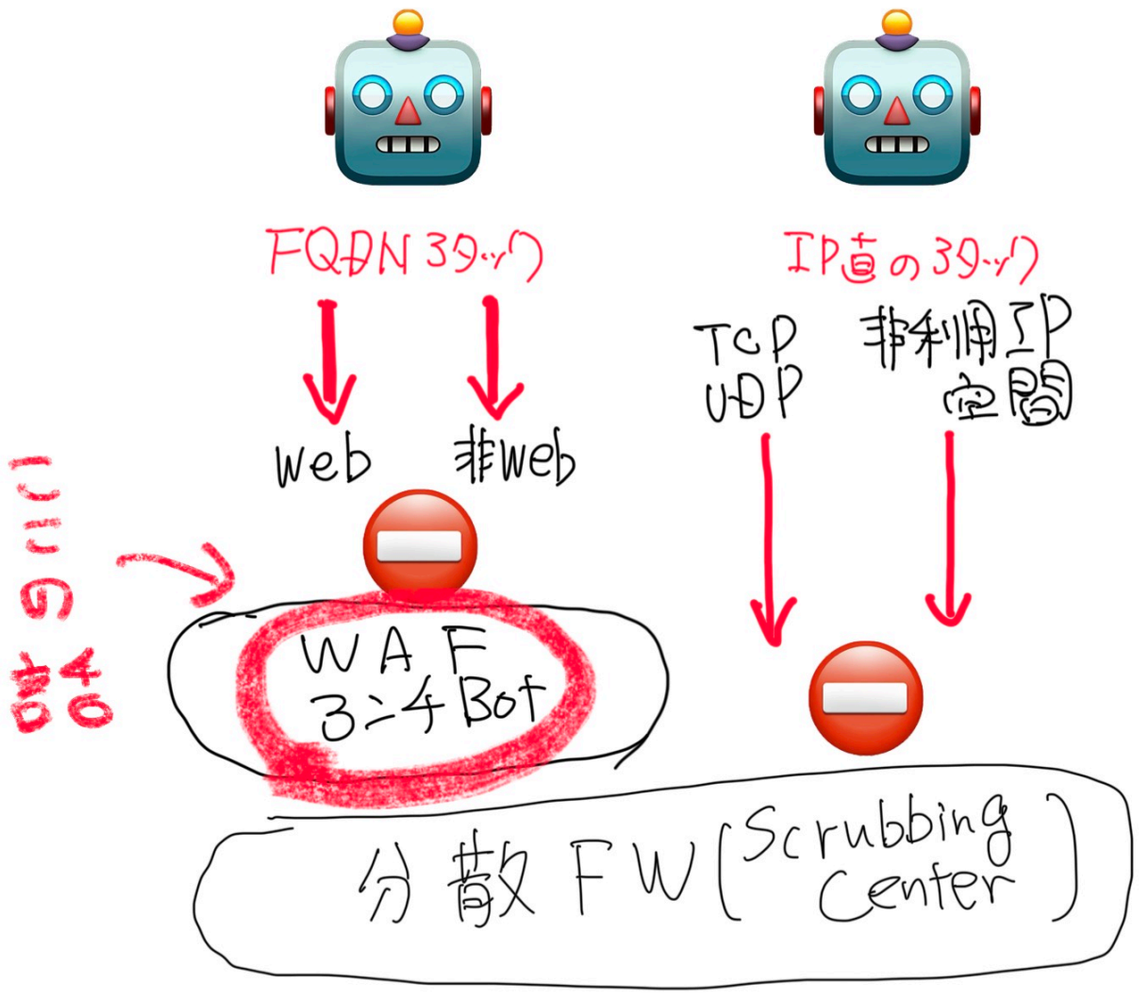


Web攻撃方面

(おもにL7の話)

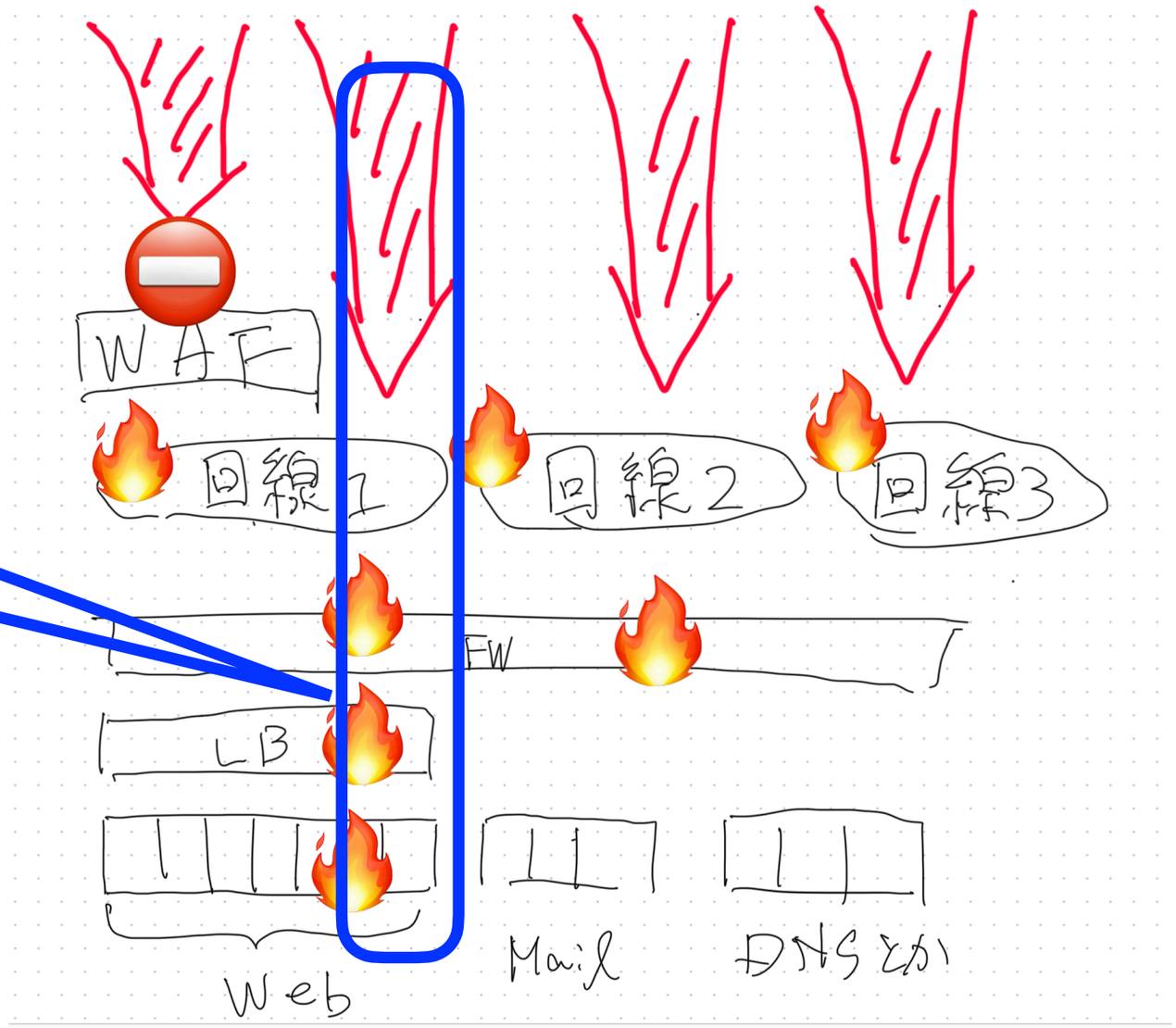
Web攻撃はWAFがないとどうにもならない

- おもにL4以下を防ぐFirewallでは対処困難
- ネットワーク型(L3-4)とアプリケーション型(L7)の複合攻撃



やっぱり怖いボリューム攻撃

- WAFが適用済と未適用が混在してるとどこかが穴になる
  - オリジン側のFWやロードバランサが逝ってしまう
- オリジンがクラウドでも同じだから安心しないこと

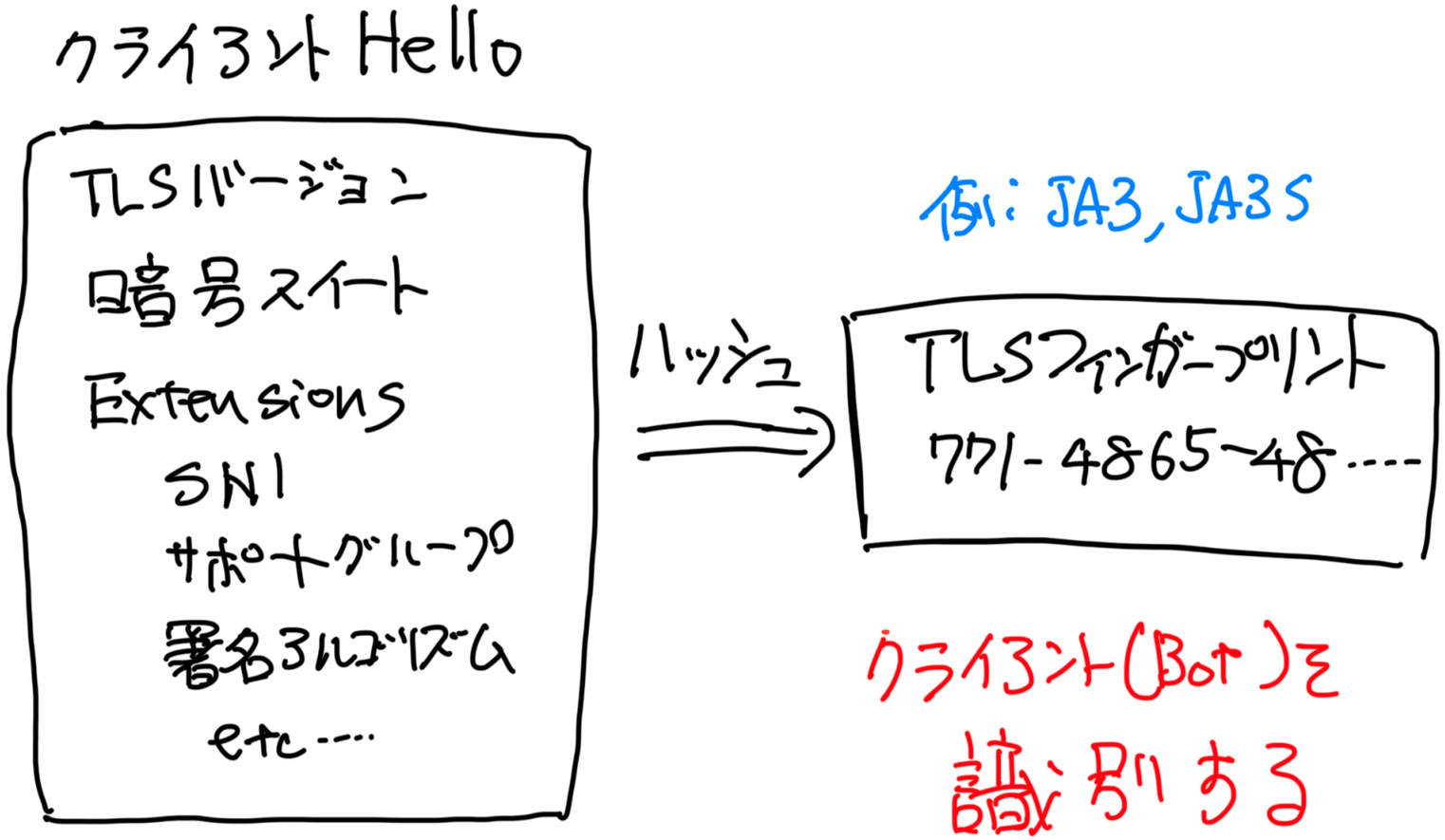


Botnetとの戦い

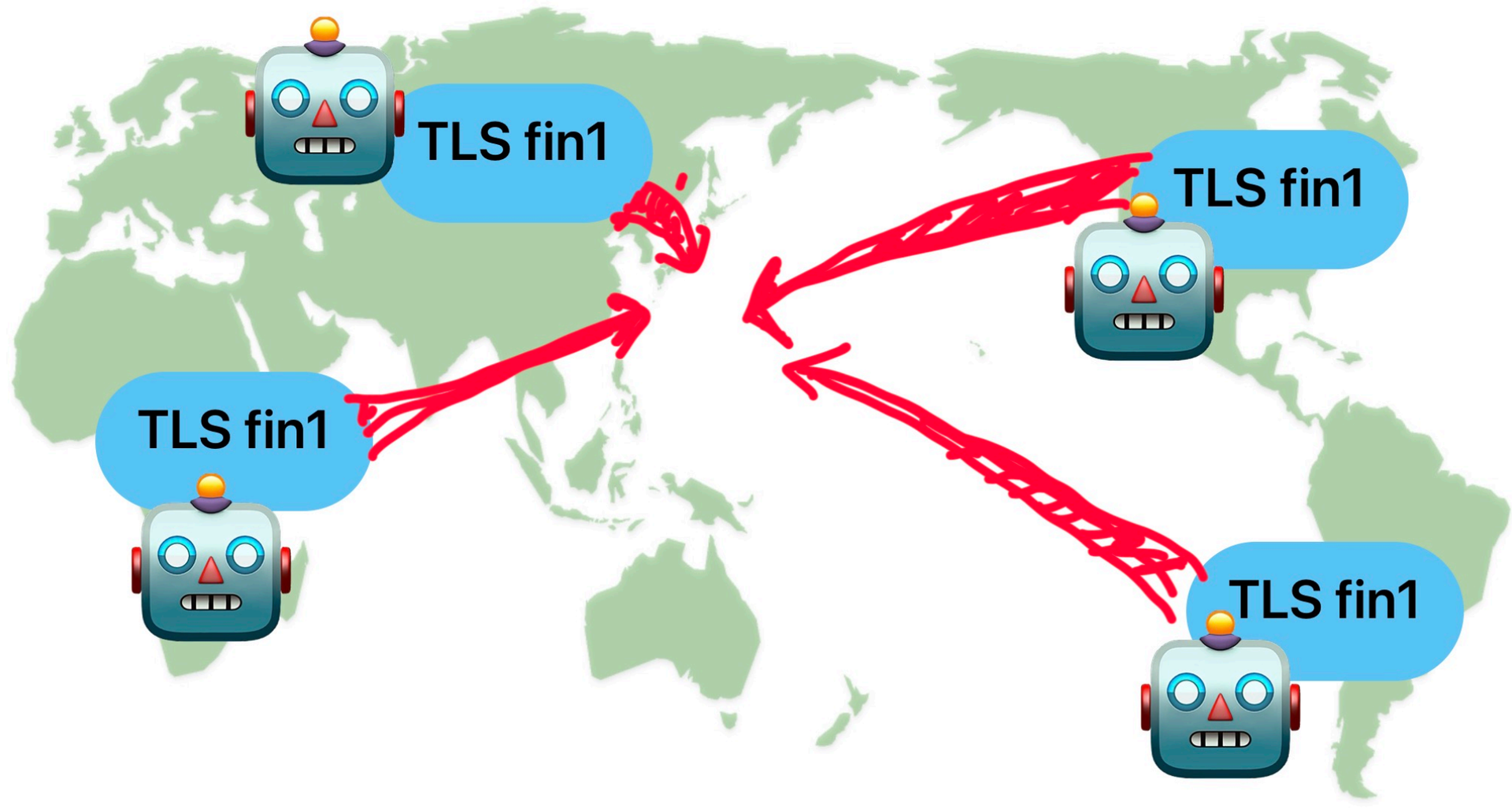
- DDoS攻撃の多くはBotnetからくる
- 特にやっかいなのがクラウドサービスからくる攻撃

Botnetを特定するTLS Fingerprint

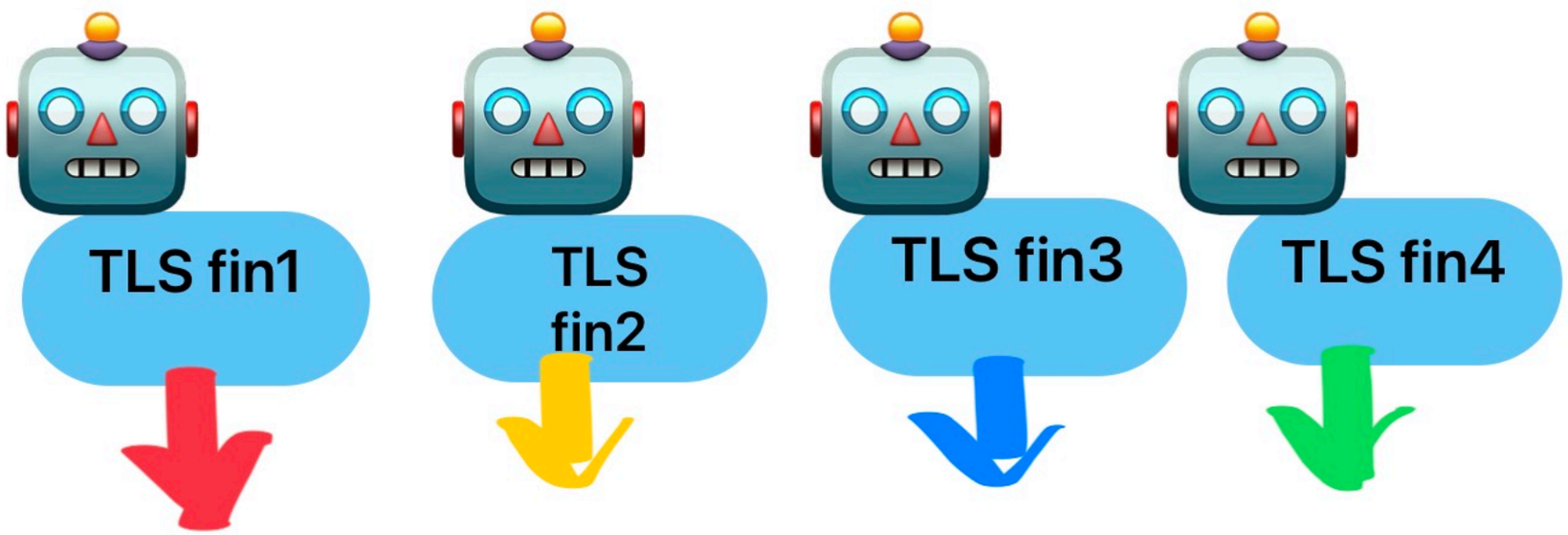
- Botnetを特定する手段の1つがTLS Fingerprint

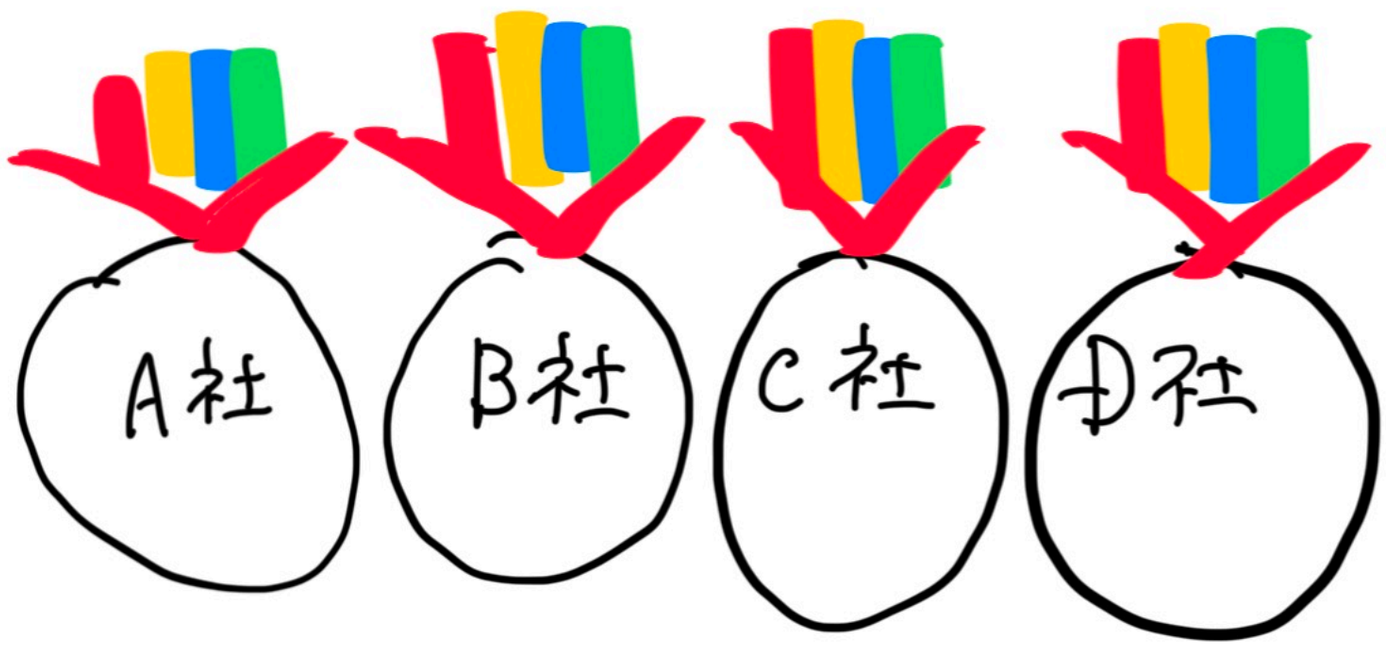


Botnetを特定するTLS Fingerprint(cont.)



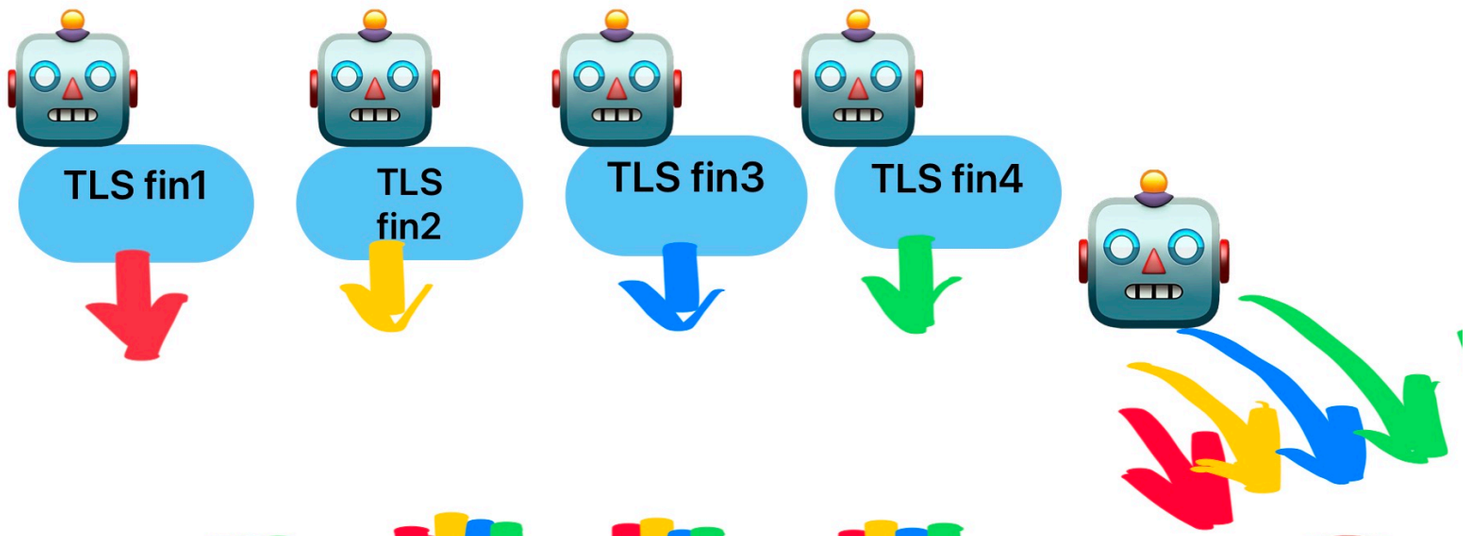
同じTLS FingerprintからのDDoSを観測

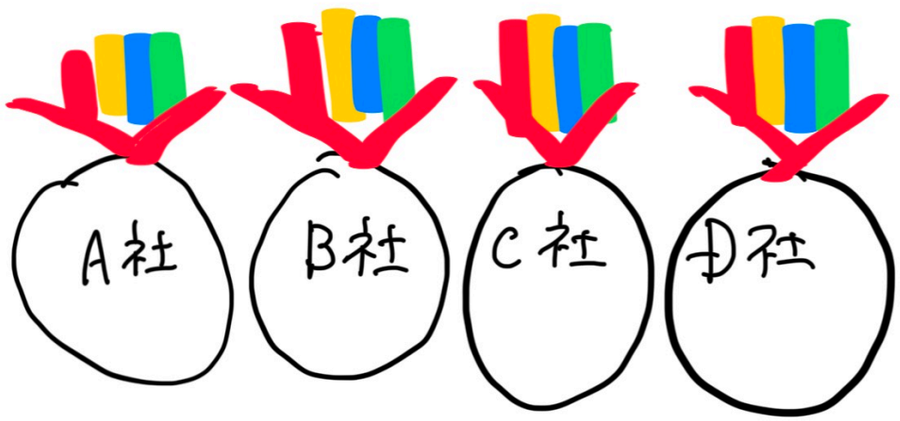




同じTLS Fingerprintを事前遮断する?

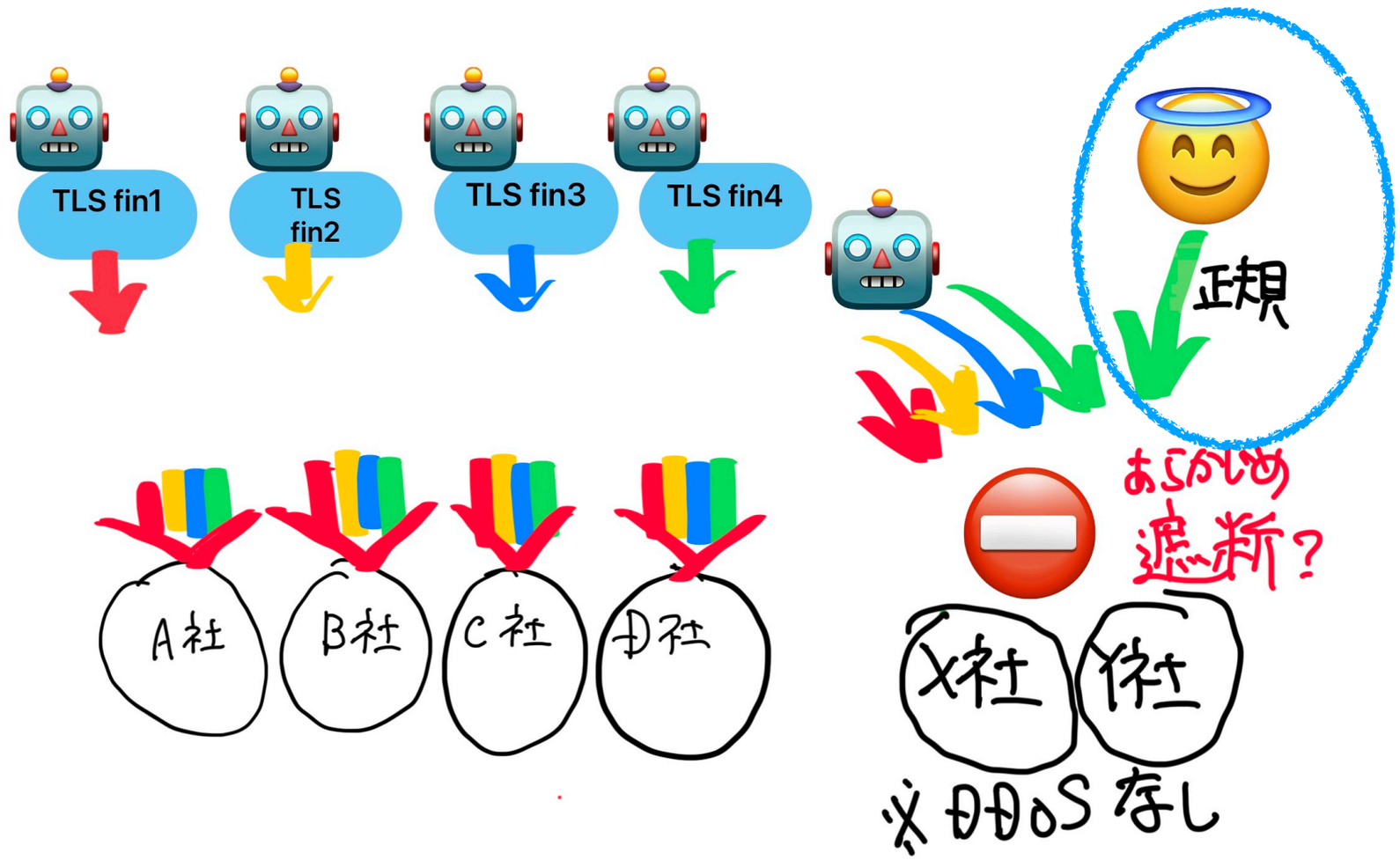
- 「事前対処としてDDoSがきてない他組織についてTLS Finger.を事前に遮断してほしい」





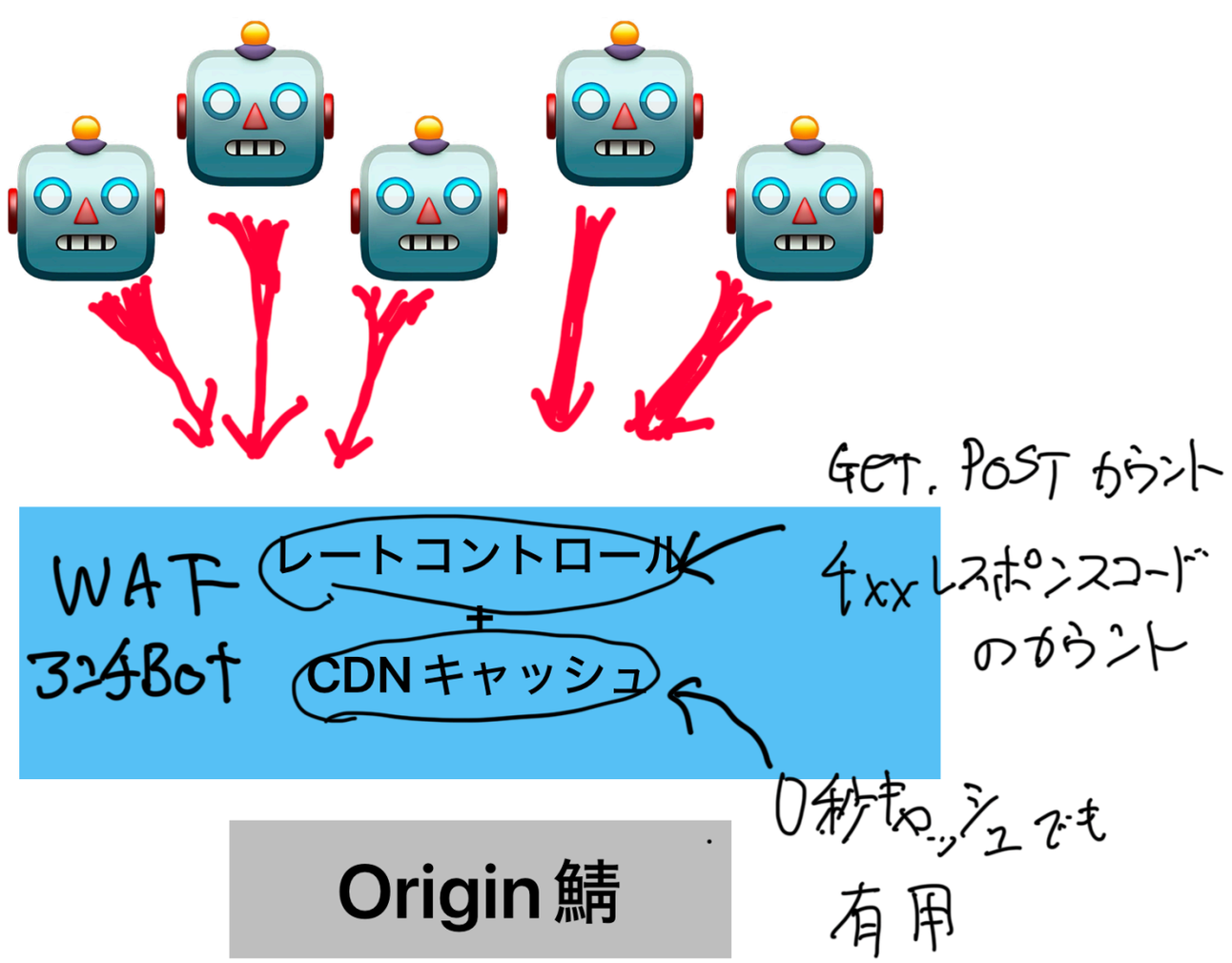
でもTLS Finger. は銀の弾じゃない

- TLS fingerprintではBotnetを特定できる場合もあるが、正規通信も含まれてしまう場合が多い。
- TLS Fingerprintはすぐに遮断せずに必ずアラートモードで検証すること



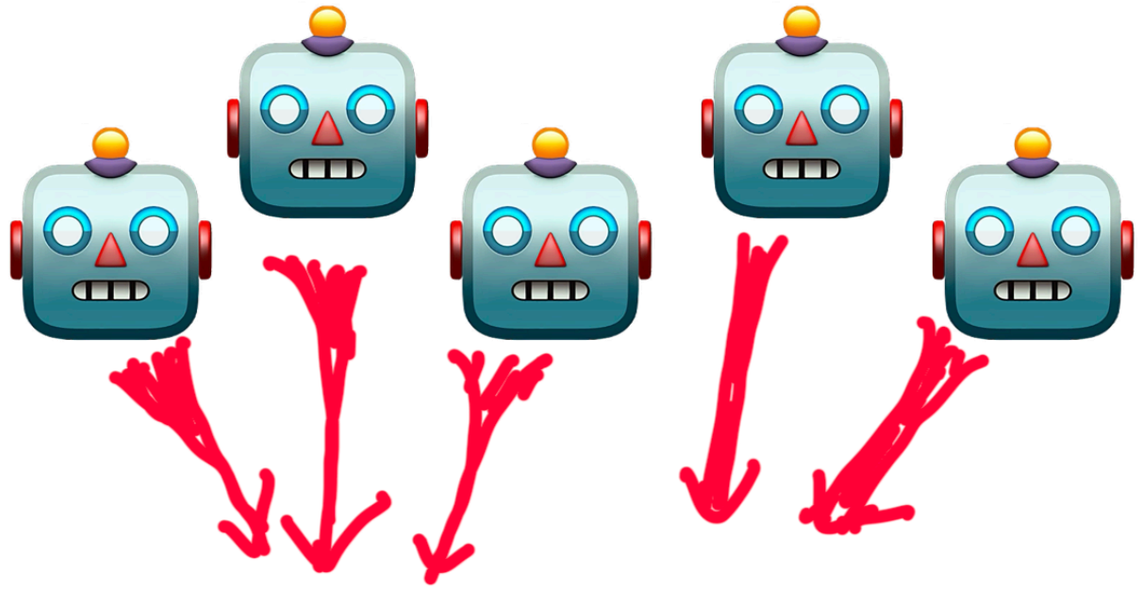
Webボリューム攻撃のベスプラ

- 見落としがちだが、キャッシュは最強の武器(の一つ)
- 通信レートのコントロール
  - ページビュー総数のほかメソッド(POST等)やレスポンスコード(404等)でもカウントする



Webボリューム攻撃のベスプラ(cont.)

- IPアドレスのレピュテーション(悪性度のスコア)はとても有用
  - とくにクラウドの共有IPは警戒する
  - ただしWebフィルタサービス(zscalerとか)のFP(誤検知)注意
- TLS finger.はあくまでも攻撃を受けたあとの事後手段として考えること
  - (重要)メンテナンス超重要‼️



WAF
3rdBot

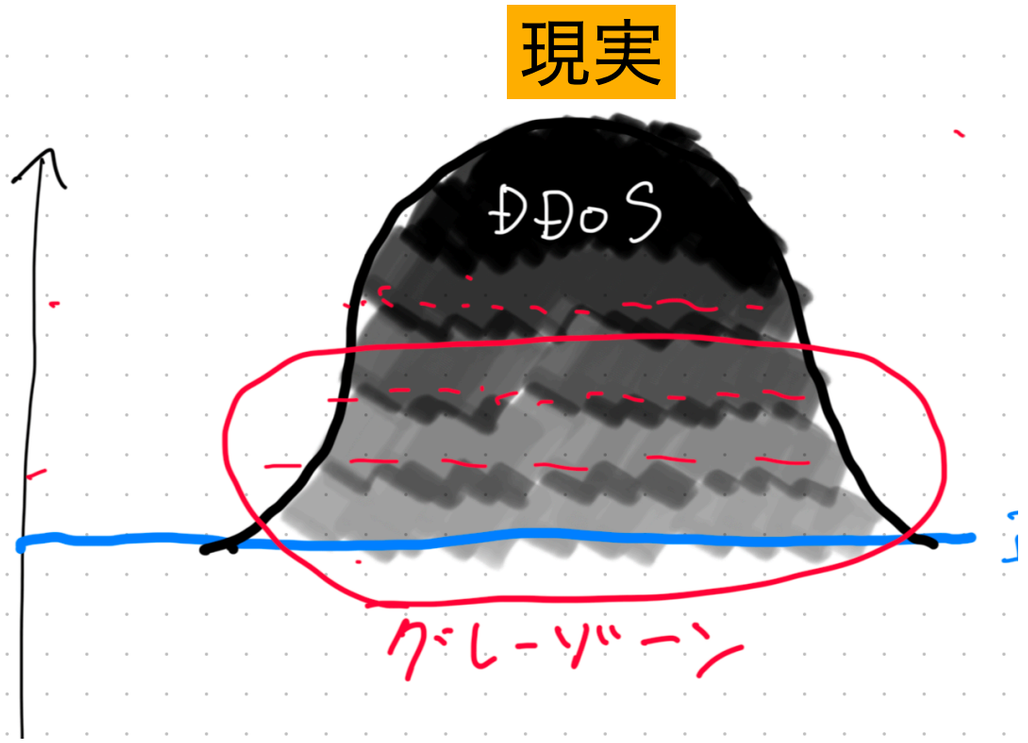
IPレピュテーション
+
TLS Finger(要メンテ)

Origin 鯖

マネージメント方面

DDoSトラヒックの白黒

- DDoSの攻撃通信を見極めるのはとても難しい
- 攻撃と非攻撃がはっきりしないグレーが非常に多い。今回もとても悩んだ



＊注意

このセッションでは 白=正規通信、黒=攻撃通信 の意味で使用しますが、いまどきは別の表現を使います。

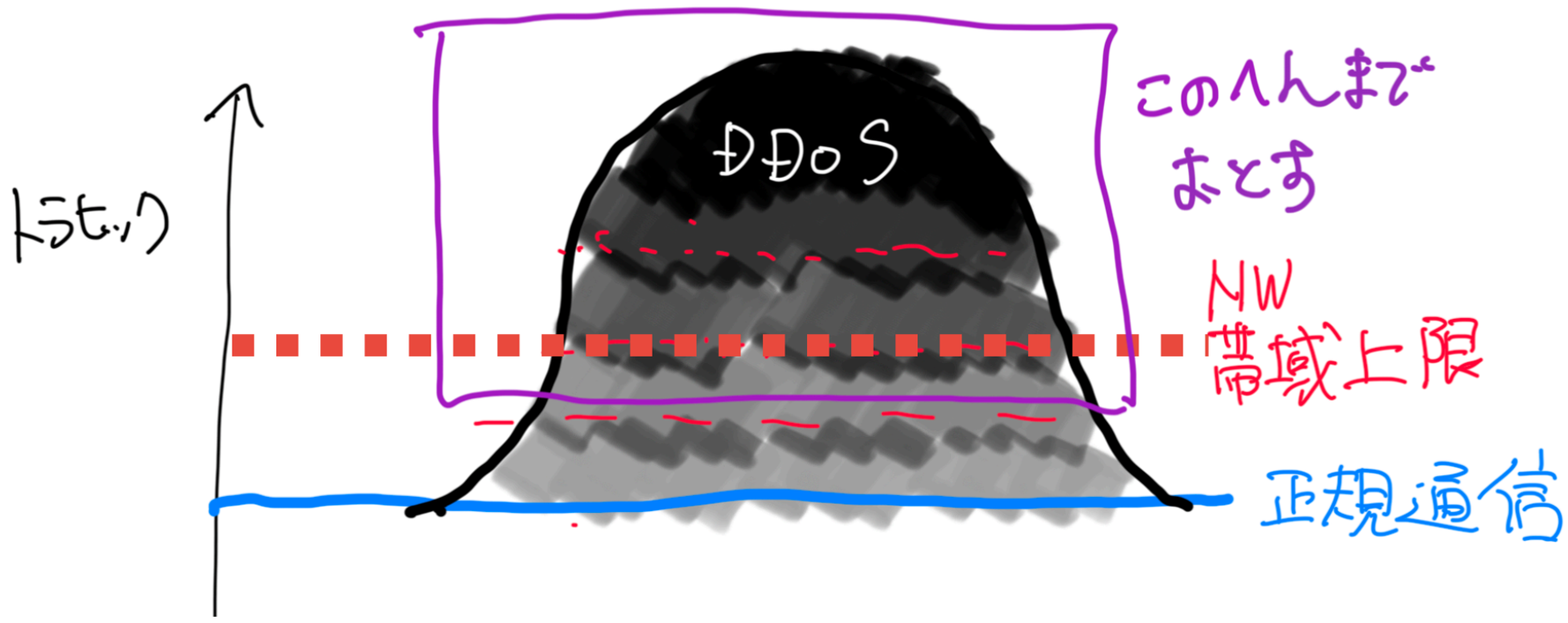
例: ホワイトリスト→許可リスト(allow list)、ブラックリスト→ブロックリスト(block list)

グレートラヒックの対処ポリシー

- グレー部分を許容するか遮断するかは決断するしかない
- 100%遮断と0%遮断(モニターする)だけでなく、一部遮断(たとえば70%遮断)もあり

グレートラヒックの対処ポリシー(cont.)

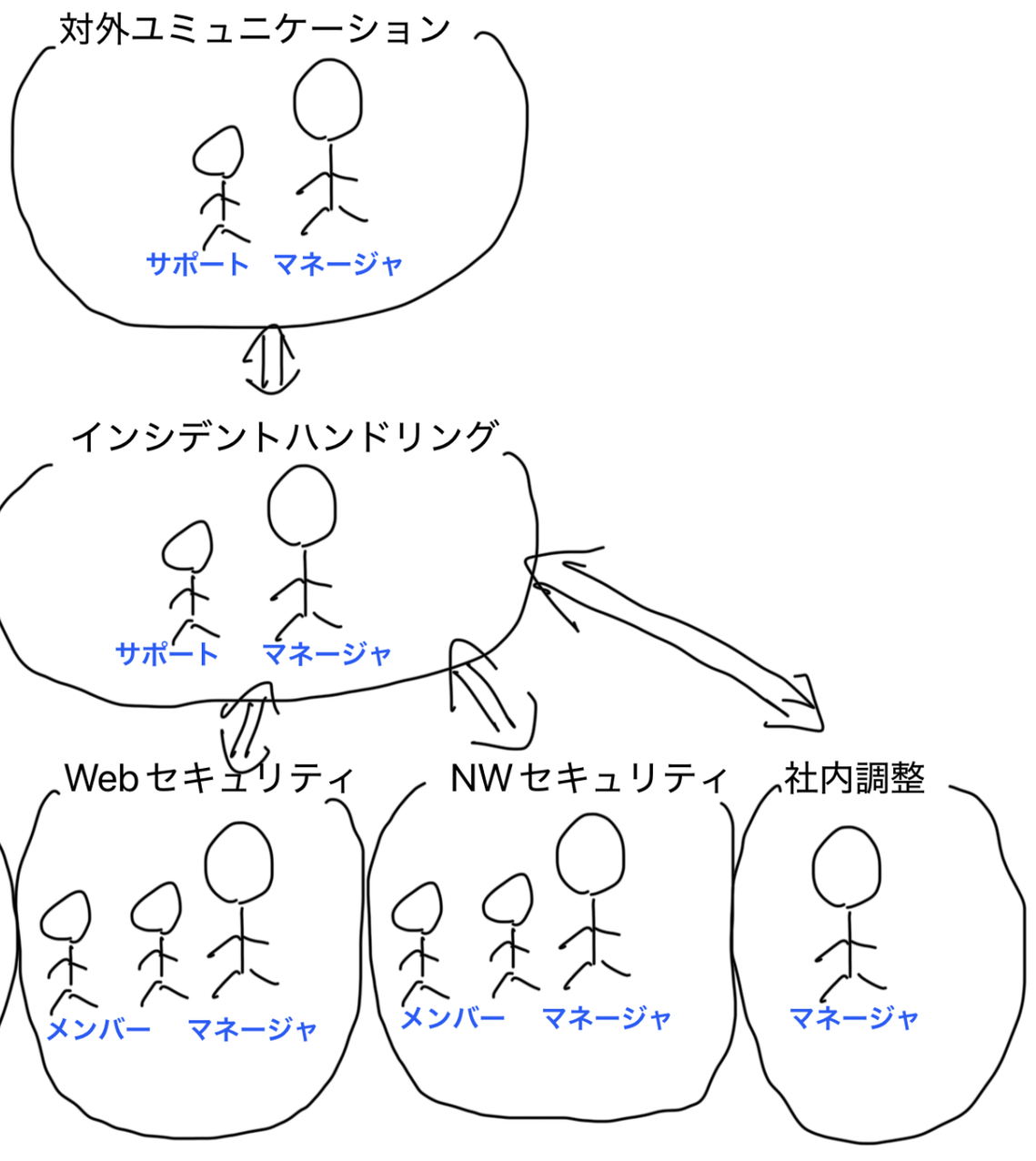
- 通信帯域やシステム負荷的に可能なら一定のグレーを許容する判断も必要
- 余裕の帯域をどのくらい確保するか悩ましいが､バースト対応や従量課金の回線サービスの採用も一案



体制の話

- 理想の障害対応(?)の体制と大規模DDoS対応の違い

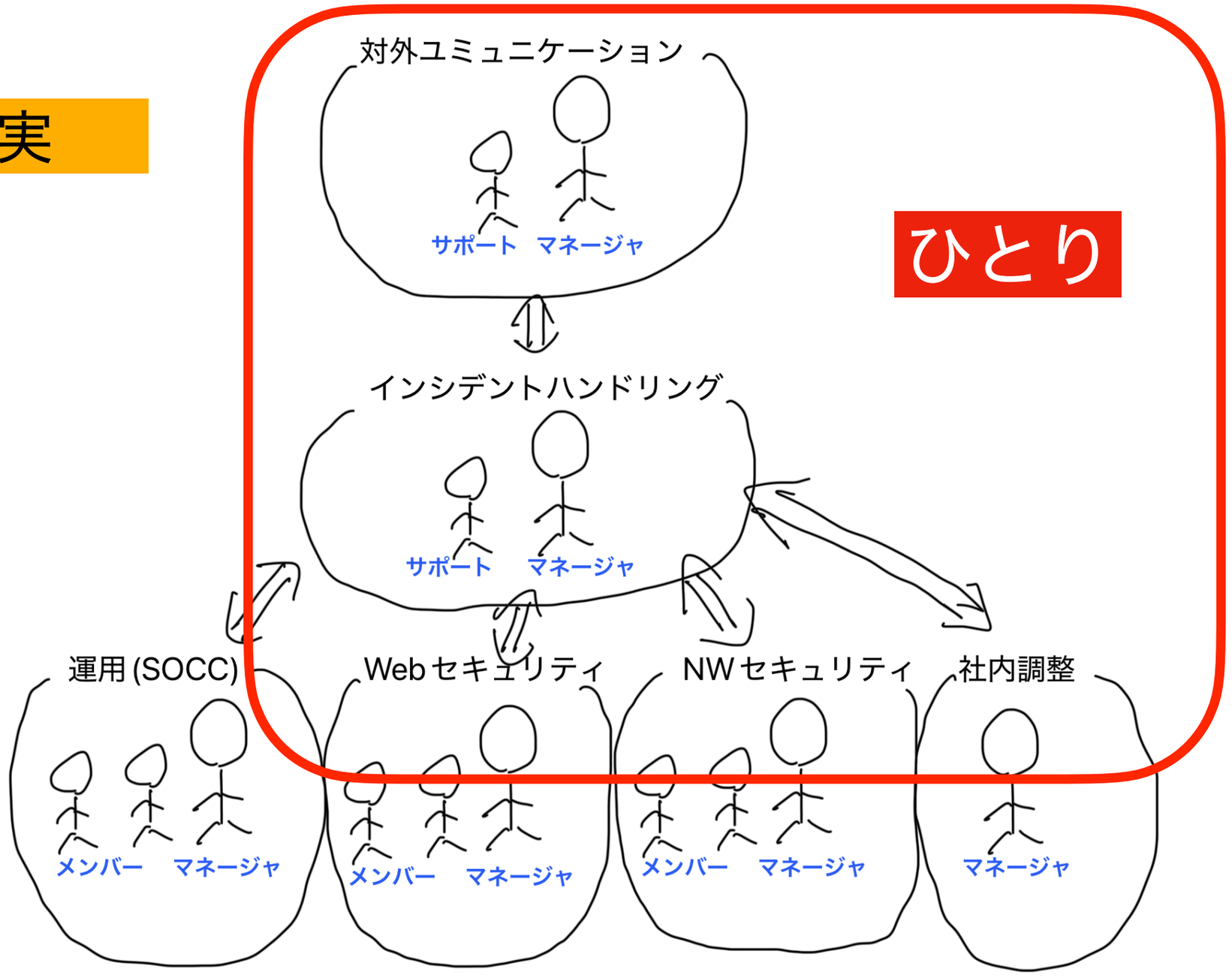
理想



ヤベーとき

- 1秒が惜しい場合はワンオペ最強
  - 負荷分散 <<< 情報の分割損をゼロにする

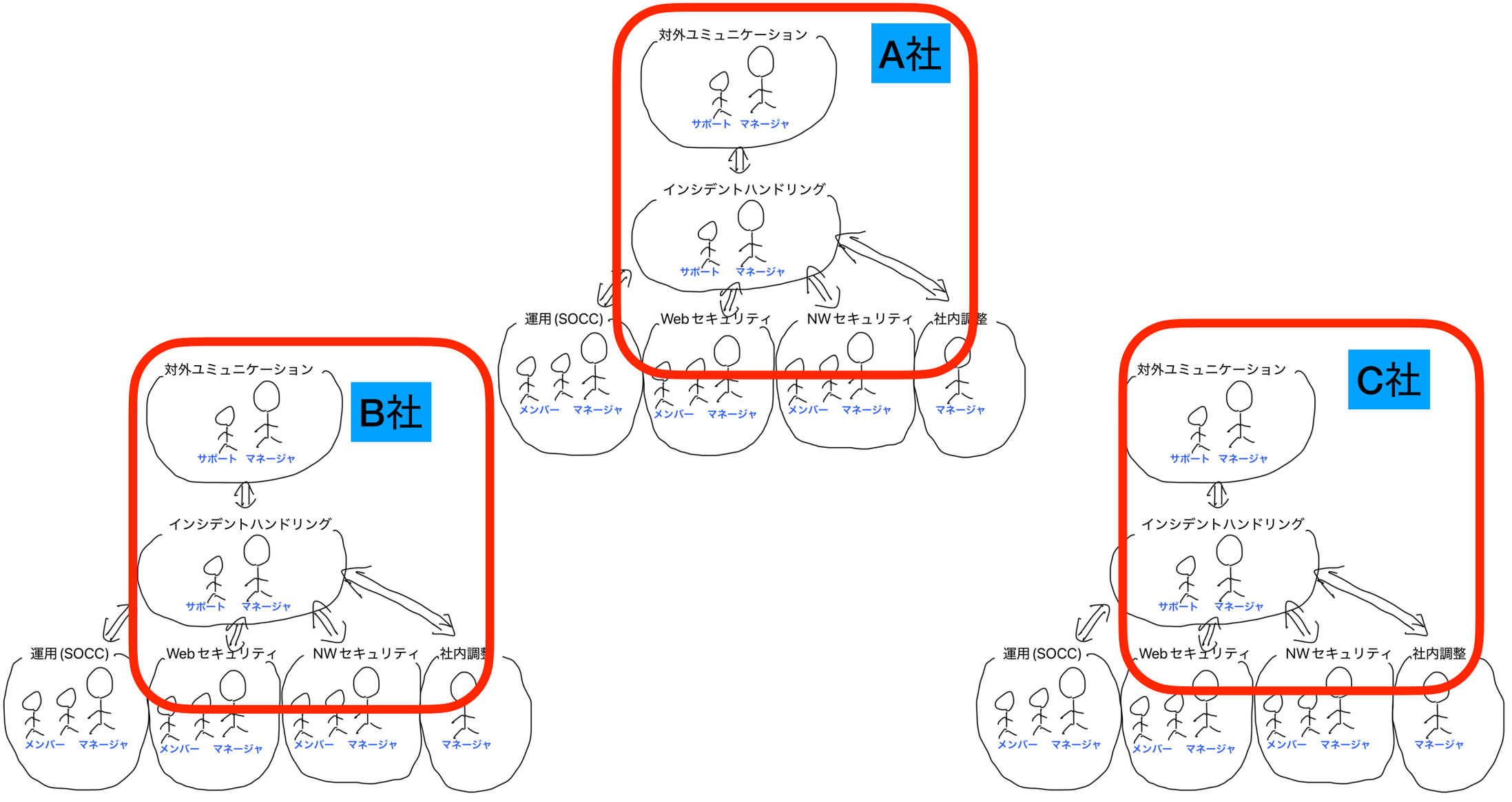
現実



ひとり

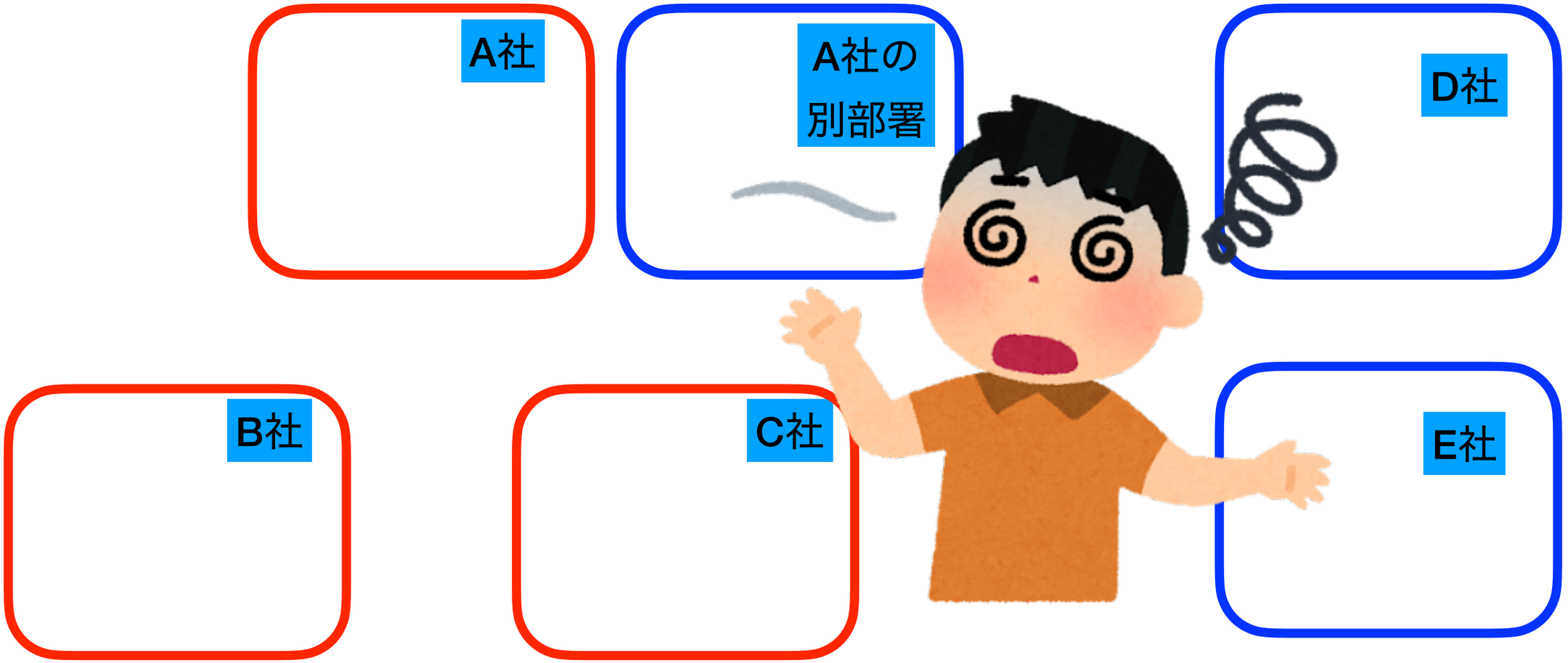
もっとヤベーとき(今回のDDoS)

- DDoSのターゲットが複数組織で同時発生する



別のもっとヤベーとき(今回のDDoSアフター)

- 攻撃対象の組織に加えて、攻撃を受けてない組織(同じ会社の別の部署とか同業種の別会社)からの対処リクエストが殺到

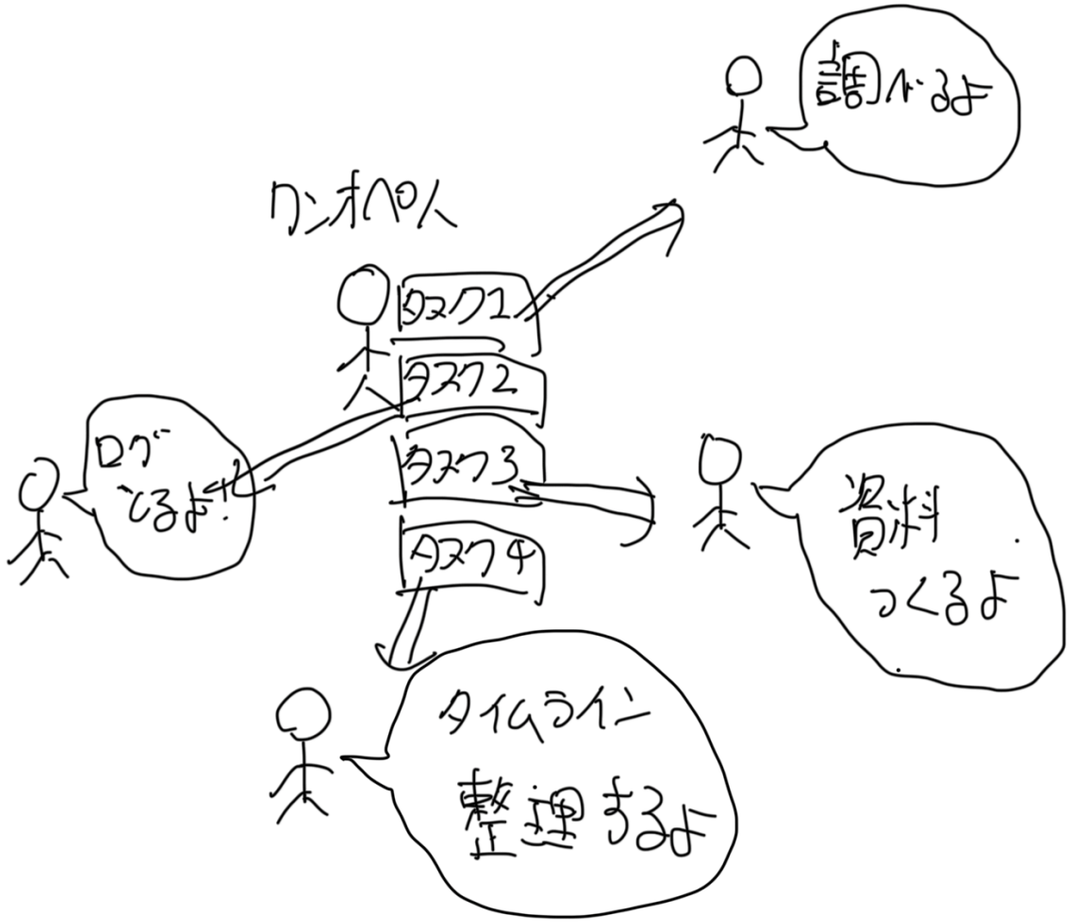


じゃぁどうすればいいのか

- インシデントレスポンスのコア部分は分散なんてできない
  - 1秒を争うときに理想の体制を整えることはかなり困難
  - 休日夜間なんてなおのこと
- 「究極のワンオペ体制」を受け入れるしかないし、そうなったら腹をくくるしかない

周りの人がタスクを奪う

- 重要なのは、ワンオペ人から周りの人がタスクを"奪う" こと
  - ワンオペ人は他者にタスクをアサインする余裕なんて1秒もない(とくに休日夜間)
  - ワンオペ期間を以下に短く&負荷を軽減するか



DDoS対処の「計画」について

- 理想
  - 事前に「対応計画」や「対策」を立てておく
- 現実
  - いわゆる「想定外」事象が高確率で発生する

「想定外」は起こるもの

- どんなに準備してもDDoS発生時の「想定外」は発生する
- システム投資する <<<<< 相談先を確保する
- 「導入して放置」は最悪
  - トラブったとき何もできなくなる
  - メンテナンス必須。「機器保守」だけでは不十分だからね
- DDoS含めてインシデントレスポンスは結局のところ人間が支配していることを理解する

「チーム総力戦」と「ワンオペ」

- 大規模なDDoS対応において、「チーム総力戦」、と「究極のワンオペ」は矛盾しない
    - チームは組織を超える
        - 攻撃を受けた組織、対策サービス、ISP、DC、SIer等
- ワンオペはゼロにできない。ワンオペをいかに短時間に抑えて負荷を軽減するかが勝負
    - ワンオペ人は強烈なストレスに晒され続けます

まとめ

- 低レイヤーDDoSは未使用空間をブロックしておく
- Web DDoS攻撃はWAFやBot対策等が必須。
- 対策デバイス・サービスの放置は悪。メンテナンス超重要。
- 大規模なDDoS対応は自組織だけで対応はかなり困難。組織の内外をふくめた総力戦ができる備えをする。

おしまい