

# 運用者の集い2024秋 (Part 1)


## -fail2ban導入について-



Internet Initiative Japan

株式会社インターネットイニシアティブ  
ネットワーク本部 アプリケーションサービス部 メールサービス運営課  
芹澤駿人

Ongoing Innovation

A red curved underline graphic under the text 'Ongoing Innovation'.

## 自己紹介

---

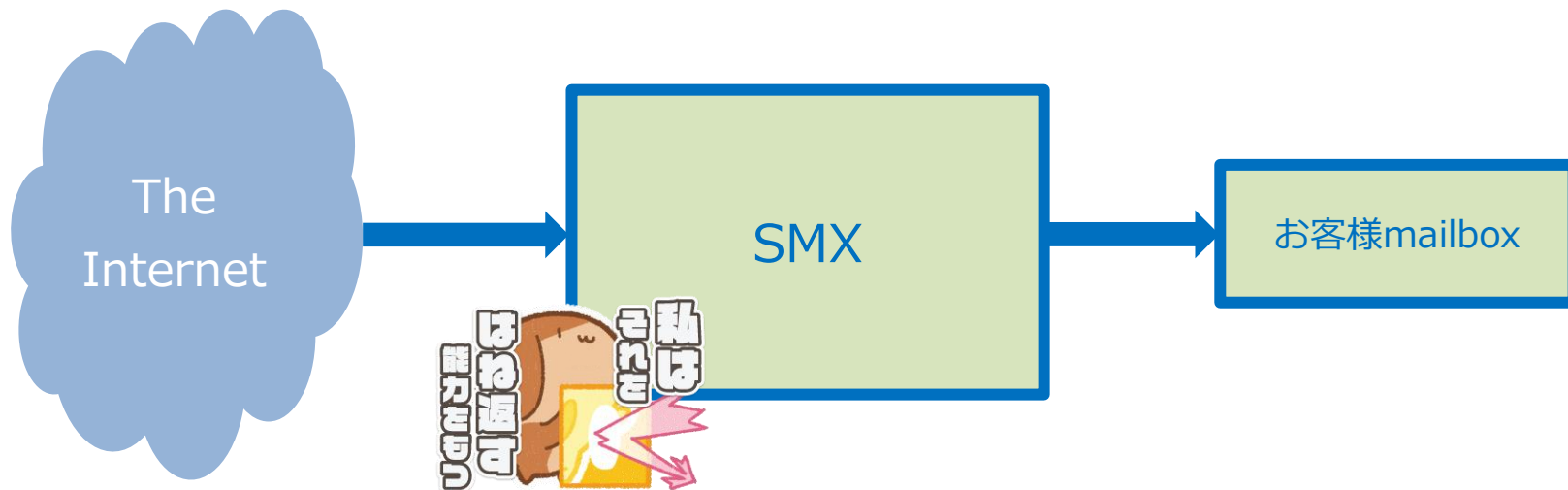
芹澤駿人(せりざわ はやと)

- 2023年 IIJ新卒入社
- 2000年生まれの24歳
  - SMX運用メンバーで一番若い
- メールには配属されてから触れる
  - 日々勉強の身
  - メンテナンス準備と遂行
  - 設備運用/サポート対応
- 趣味
  - 音楽(聴く専)
  - プラモデルを買って満足



## IIJセキュアMXとは

# IIJセキュアMX: ゲートウェイ型メールセキュリティサービス



お客様ドメイン宛のメールに対して  
ウイルス・スパム等検査し、配送・隔離 を実施

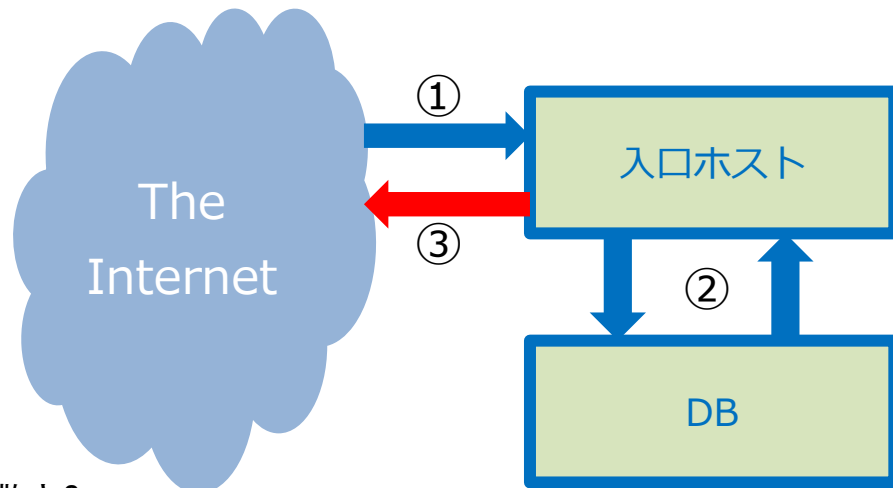
## SMXの困りごと

# 大量に届く User unknown メール

存在しない宛先への

1. 着弾
2. ユーザが存在するか(等)DBへ問い合わせ
3. 存在しない場合、User unknown (5xx応答)

上記処理が着弾のたび発生



送信側のミス or ハーベスティング or ばら撒き?

→ 迷惑行為のため、続くようなら着弾前にブロックしたい

お客様と設備を守るために

## fail2banの導入

fail2banとは

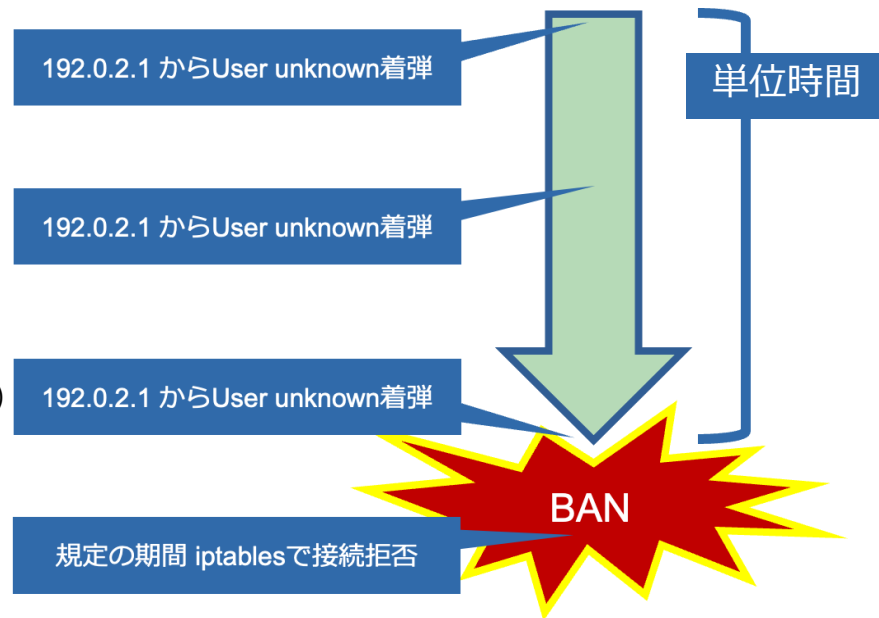
- ログファイルを監視
- 不審な通信をIPアドレスごとに自動ブロック可能
- <https://github.com/fail2ban>

SMXでは

User unknownな着弾をIPアドレスごとに集計

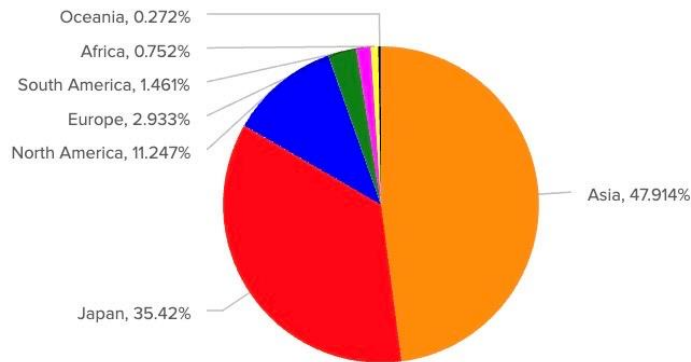
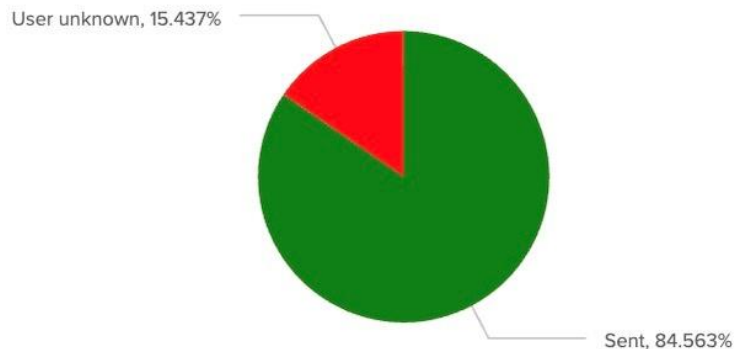
単位時間内に閾値を超えたらBAN (iptablesで拒否)

規定の時間経過後、BAN解除



## SMXでの例

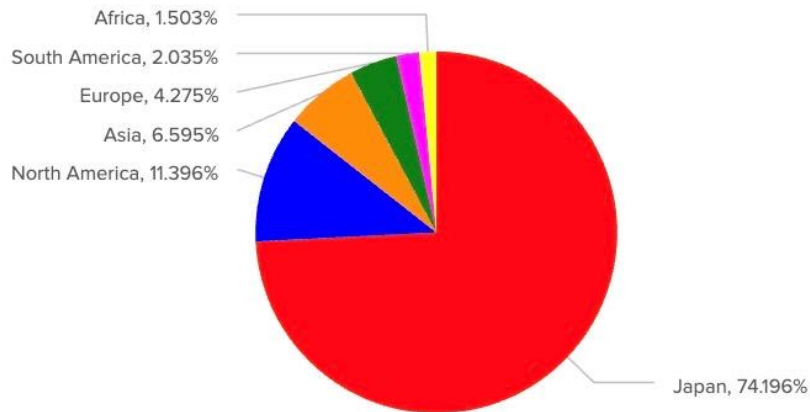
## 一ヶ月間のUser unknown率と国(地域)別割合



- User unknownは受信全体の約15%
- User unknownのうち、日本を除くアジアが約50%
  - ハーベスティングorばら撒き?
- 日本国内からは35%
  - 悪意があるかは不明

## SMXでの例と気づいたこと

### 一ヶ月間のBan件数 国(地域)別割合



- 日本国内のIPアドレスが約75%
  - fail2ban起因の問い合わせはなし。Banしても問題ない。
- 日本を除いたアジアの割合は約6.5%
  - 悪意のある送信と仮定して、閾値を超える前にIPアドレスを変えているのでは?
  - そもそもアジアのIPレンジが日本と比較して広いのでは?

## まとめ

---

### まとめとこれから

初期は閾値を緩く設定していました

- 誤BAN発生を防ぐため
- BAN設定投入前に検知ログのみ出すdry-runを実施

段階を踏んで厳しくしている最中

- 分析の結果、更に閾値の最適化の余地あり

**閾値の最適化等, お客様と設備を守る行動を続けていきます**



Ongoing Innovation

IIJ Internet Initiative Japan

**ご清聴ありがとうございました。**

本書には、株式会社インターネットイニシアティブに権利の帰属する秘密情報が含まれています。本書の著作権は、当社に帰属し、日本の著作権法及び国際条約により保護されており、著作権者の事前の書面による許諾がなければ、複製・翻案・公衆送信等できません。IIJ、Internet Initiative Japanは、株式会社インターネットイニシアティブの商標または登録商標です。その他、本書に掲載されている商品名、会社名等は各会社の商号、商標または登録商標です。本文中では™、®マークは表示していません。

© Internet Initiative Japan Inc. All rights reserved. 本サービスの仕様、及び本書に記載されている事柄は、将来予告なしに変更することがあります。