令和版 POP before SMTP を作った話

自己紹介



- HN：　まさんき(ma3ki)
- 本業：　インフラエンジニア
- 副業：　メール・DNSの相談対応(ココナラ)
- 趣味：　ジョギング、スクーバダイビング、メールサーバ

JPAAWG 8th でもLTをさせて頂きました

※ 個人参加のため、発表は所属会社とは無関係です

突然ですが

みなさんも経験ありますよね？

不正アクセス

私のメールサーバも
不正アクセスされました

被害状況



- 期間：2026-08-26 ～ 2026-09-05 (※)
- 不正利用されたアカウント数：2個
- 送信試行回数：　約45,000 (総宛先数)
- 送信成功通数：　約19,000
- 接続元IP数：　約13,000
- 接続元国数：　約120

※対応(検知)までに時間がかかった理由はいくつかありますが本発表ではふれません

迷惑メールを
大量に送信してしまい
大変申し訳ありませんでした

なぜ防げなかったのか

メールサーバの防御策



- 特定IP群からのパスワード試行攻撃への対策
  - ブルートフォースアタック
  - ディクショナリアタック

- 認証アカウントとEnvelope Fromの一致必須
  - sender_login_mismatch (postfix)

約8年、この防御策だけで運用し、特に問題は起きなかった

無意味でした

不正アクセスは
初回から正しいパスワードで認証し
普通にメールを送信していました

なんと私のメールサーバは
有効なアカウントで
正しいパスワードで認証されると
いくらでもメールを送信できる
仕様だったのです

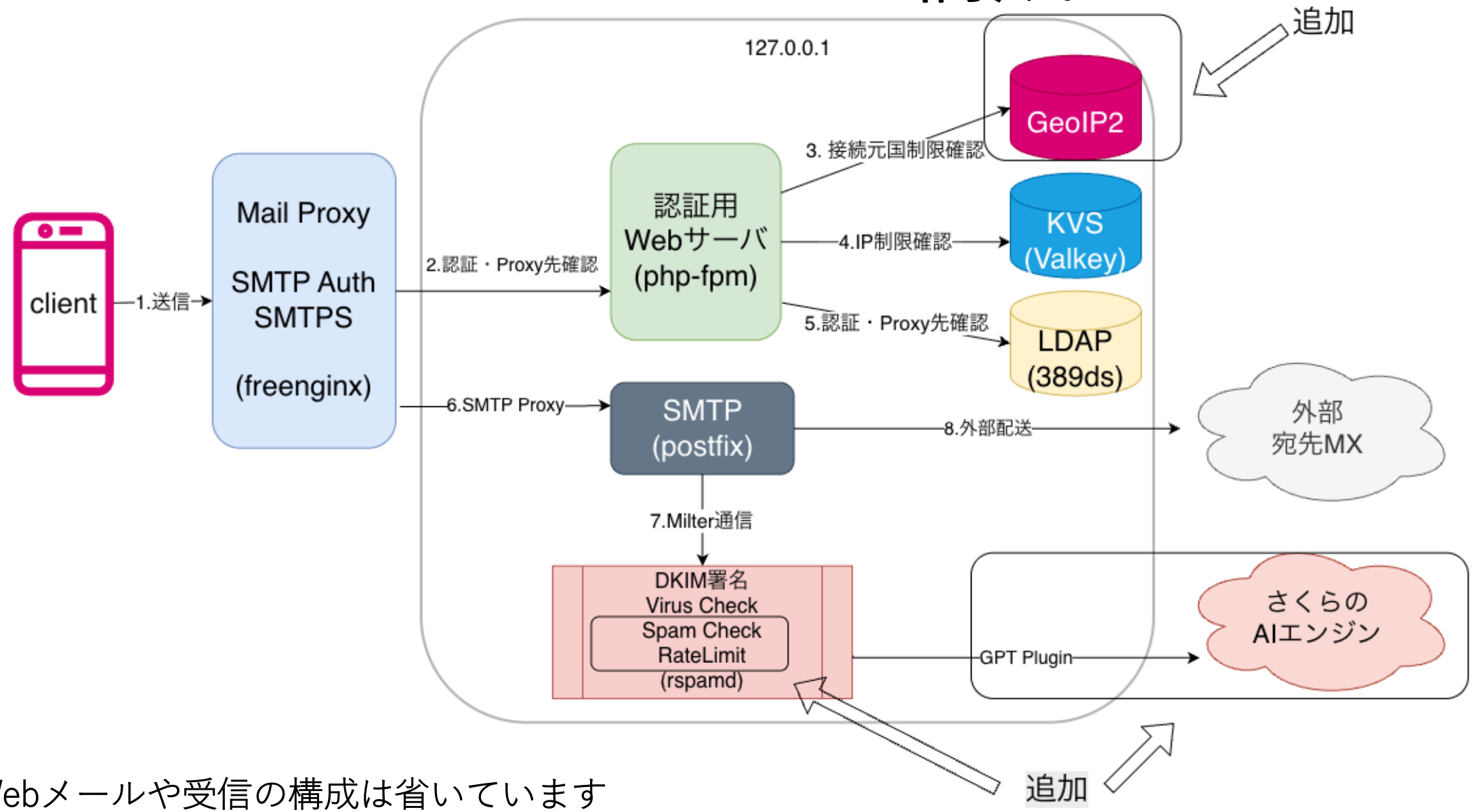
一時対応



- 不正アクセスされないために
  - パスワード変更
  - GeoIP2による国外からの認証拒否(※)
  - Webメールを2要素認証必須化
- 不正アクセスされた時のために
  - 送信時の迷惑メール判定有効化
  - 送信時のRatelimit有効化

※国内からの不正アクセスは 0.2%でした

メールサーバ構成



※Webメールや受信の構成は省いています

一時対応だけでも
今回の不正アクセスは
ほぼ防げました

が

完璧を目指したい

国内からの不正アクセスは
防げていない

もし海外に行ったら…

もし国内として認識されない
IPが割り当てられたら…

Webメールしかログインできない

そんなのやだ！

メーラーからいつもどおり
メールを送受信したい！

私が思う完璧とは



- 外部にメールアカウントとパスワードが漏洩しても認証させない
- 正規利用者は既存のメールクライアントの設定を変更せず、メールの送受信ができる

閃いたこと



1. Autheliaで2要素認証(パスワード/OTP)をする(※)
2. 2要素認証した”IPアドレス”からのアクセスは、SMTP/POP/IMAPでのパスワード認証を短時間許可する
3. 一度認証できた”アカウント+IPアドレス”の組み合わせは、最後の認証成功から長時間パスワード認証を許可する

※私のメールサーバでは以前よりRoundcube + Authelia(IdP)で２要素認証ができる状態でした

認証に成功したIPを
しばらく信用するなんて…

POP before SMTP
みたい！！

って思った人は
たぶん
45歳
超えてます

※私は47歳です

これを
OTP before MailService
と名づけました

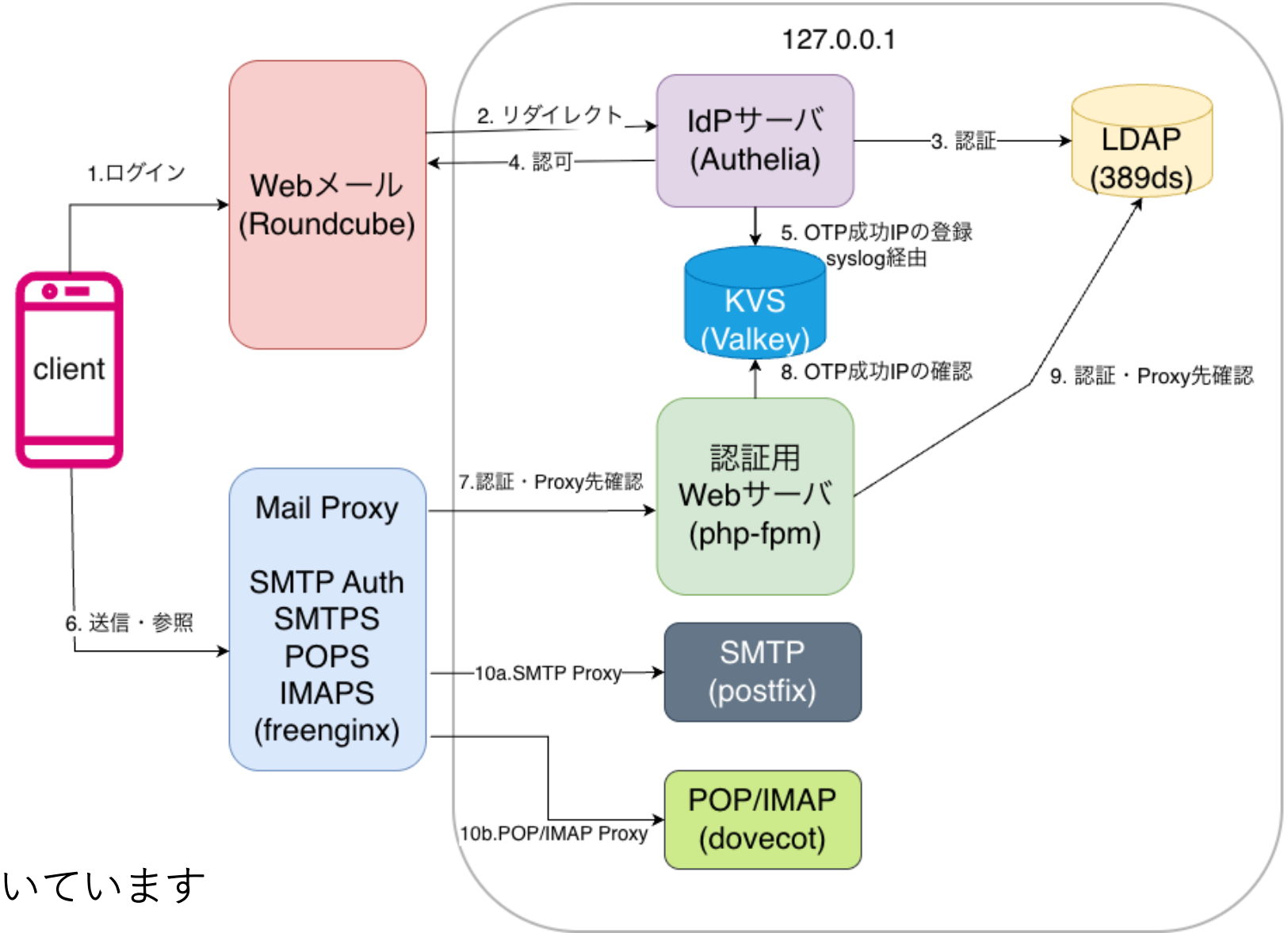
OTP before MailService



- 実装のためにしたこと
  - Autheliaのソースを修正し、2要素認証成功ログをdebugからinfoレベルに変更 (※)
  - rsyslogで上記ログから必要な情報をKVSに登録するスクリプトを作成(※)
  - 認証用phpスクリプトに必要機能追加(※)

(※) 協力者 Gemini

OTP before MailService



※一部構成は省いています

まとめ



- 漏洩したアカウントとパスワードだけでは認証できない仕組みができました
- 導入後は、GeoIP2を無効にしても外部からのアクセスは想定通り制限できています
- 外出するとスマフォからの認証が失敗するのでIIJmioのIPv6帯はホワイトリストにいれてますw
- 複数アカウント利用時の利便性のため、2要素認証時はIP単位で信用しますが、アカウント+IPへの変更も可能です

ご清聴ありがとうございました

補足1

資料作成後にAIで調べたら Zextras Carbonio にも「Trust the IP」というほぼ同じ機能がありました（Webで2FAしたIPを一定時間信頼してSMTP/IMAPを通す）

9月にリリースされた Thunderbird 155 で、独自で構築した OAuth2 サーバを設定できるようになってました
私の環境でもThunderbirdでのxoauth2(※) を使用した認証ができたので、今後モバイル用クライアントへの対応が進めば、OTP before MailServiceは不要になるかもしれません

※freenginxはxoauth2に対応しているので採用してます

補足2

不正利用された2つのアカウントについて

1つはこの発表の迷惑メールの大量送信に使用されました
もう1つは、裏でIMAPアクセスされていました

IMAPアクセスの詳細

1回目: ログインとログアウトのみ
2回目: 1回目の数時間後に再ログインし、仮想通貨取引所の「アカウント登録確認メール(ログのmessageidから予測) 」を1通だけ受信し、そのメールを削除してログアウト
取引所のアカウントがまだ作られていなかったため、使えるアカウントかの下見だったと思われます
Zabbixの通信量グラフやdovecotのログから、その確認メール1通以外は読まれていないと判断してます