freebit
毎日、発明する会社

IP blocklist戦記 (2023-2024)

2024/11/12 JPAAWG GM7 A2-6/B2-6

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

目次

- 自己紹介
- 枕: Service Update
- IP Blocklistで困った事例

自己紹介

freebit
毎日、発明する会社

- 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

freebit
毎日、発明する会社

枕
Service Update

枕: 乗っ取りspam総合的対策

段階	問題の性質	ありうる対策	項番
ID窃取	弱いパスワード	パス変画面で強さチェック**(済)** **既存の弱いパスワードはロック(レポート)**	(1) (2)
	ID名前空間狭い	認証IDをメールアドレスに	(3)
	リスト攻撃	認証頻度制限、パスワードレス認証	(4)(5)
共通	アクセス元分布	ID数/IP数比ペナルティ、GeoIPで重み付け、国間移動ペナルティ **(→横軸)**	(6)
	ユーザ認知	ログイン事実通知、多要素認証	(7)(8)
送信	送信の量自体	検知してユーザ対応**(済)**、エラー率ペナルティ**(済)**、**ID毎流量制限(展開済)**	(9)(10) (11)
	ブロックリスト	**出口分離(準備中)**、リストチェック**(済)**、IPローテーション	(12)(13) (14)

枕: 乗っ取りspam対策 進捗pickup

- アカウント毎送信流量制限を実装
  - 当座はログ解析ベースのロックと等価な形でリリース
  - SMTPエラーを出すモードは事業者毎に展開できる仕組み
- 既存の弱いパスワード対策
  - 事業者向けに既存脆弱パスワードレポート
  - エンドユーザへの変更働きかけは当座事業者お任せ
- 出口分離は仕組みを準備中
  - 個別合意込みの展開手法については検討中

枕: 2024/02 Gmailポリシー変更対応

- 準備期間3か月の突貫工事: DKIM/ARC対応
  - DNS: OEM先の対応を容易にするミニマムセット
    - ドメイン作成に連動して鍵生成・専用権威サーバに保持
    - 事業者ドメインのゾーンにCNAMEを書いてもらう
  - 送信サーバ: opendkimをmilter接続して署名
  - 転送サーバ: openarcをmilter接続して署名
- その後: opendkim/openarcがあまり安定してない
  - Watchdog/カジュアルに再起動するという運用
  - 風の噂: MTAがpostfixだと落ちないらしい?
  - 風の噂: libmilterをチューンせよ、という情報

freebit
毎日、発明する会社

本題

IPv6 Blocklist問題の続報(2022-)

- 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
  - ちょうど今の時期のとある調査で問合せ増える
- 対策: 顧客割り当てアドレスをリナンバ → 実装し始めた
  - 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(勿体ないけど仕方なし)
- その矢先、Gmailがv6を殆ど吸わなくなった(2023/4-)
  - G Workplaceの独自ドメイン考慮するとmailertableは使えない

  → 出口の**v6トランスポート廃止**で対応(技術的退化)

Blocklist困りごと 考察/頭痛ポイント

- Gmail等はv6を捨ててる?
- ARC署名付けてもIPでブロックされたら効かない
- 送信終息して時間が経ってからブロックされる
- 通報/honeypotに加えてDNSBL経由でトラフィック見てる?
  - 海外Blocklistは日本の通秘知らないことに注意
- 一次対策としては出口分離が必要だが
  - Spam判定の有効性に疑問
    - 計算リソース大量消費
    - MXですり抜け多いので分離しきれるかどうか
  - 個別同意が大変……