JAPAN ANTI-ABUSE WORKING GROUP

フィッシングメールの現状と対策 (2020年前半版) ~ 技術的対策 ~

JPAAWG / Internet Initiative Japan Inc. (IIJ)

Shuji SAKURABA

JPAAWG について

- Japan Anti-Abuse Working Group
  - グローバルなセキュリティ組織 M³AAWG (Messaging, Malware and Mobile Anti-Abuse Working Group) と連携した国内唯一の組織
  - メッセージングセキュリティを中心に関連技術も含めた対策を検討する Working Group
  - 2018.03 の pre-meeting を経て 2019.05 正式発足 (現在 13社のメンバ)

- General Meeting
  - 2020.11.11[Wed] & 12[Thu] 3rd General Meeting 開催予定
  - Online Meeting
  - 第20回迷惑メール対策カンファレンスと併催 (IAjapan 主催)

フィッシング対策の課題

- メール送信側
  - ISPs 等のメールサーバの悪用 (感染元 PC や搾取した認証 ID/Password の悪用)
    → 踏み台送信
  - 固定 IP やクラウドサービス (ホスティング) の悪用
    → 対応するまでの時間で大量送信，短時間での回収
  - 高速化 (通信環境) し便利 (ホスト利用環境) になる各種インフラの悪用

- メール受信側
  - 受信メールへの不正アクセス対策 ← BEC へと発展
  - 巧妙化する送信手法，コンテンツ，添付ファイルの対策
  - 法的な制限 (いわゆる通信の秘密)
    - フィルタ等を後から導入するのが難しい (同意を後付けでとることの難しさ)

前回 (janog45) のおさらい

- メール送信側
  - 踏み台問題対策
    - 送信者認証
    - 国内以外からの投稿抑制
    - FBL (Feedback Loop)
  - 送信ドメイン認証技術

- メール受信側
  - 迷惑メールフィルタ
  - 送信ドメイン認証技術 (SPF, DKIM, DMARC, BIMI)
  - メール配送経路の暗号化 (STARTTLS, MTA-STS, TLSRPT, DANE)

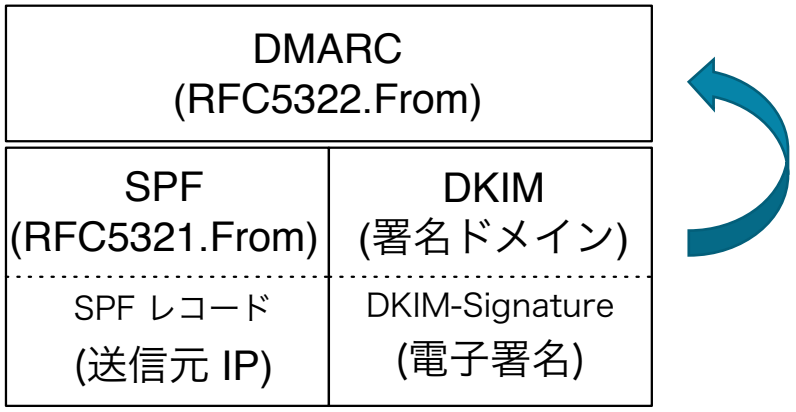
送信ドメイン認証技術

- 概要
  - 送信者をドメイン名単位で認証する仕組み
  - 仕組みの違いで 2つの方式と 3つの認証ドメイン
    - SPF (Sender Policy Framework): RFC5321.From ドメイン
    - DKIM (DomainKeys Identified Mail): 署名ドメイン
    - DMARC (Domain-based Message Authentication, Reporting, and Conformance): RFC5322.From ドメイン

	SPF	DKIM	DMARC
名称	Sender Policy Framework RFC 7208	DomainKeys Identified Mail STD 76, RFC 6376	Domain-based Message Authentication, Reporting, and Conformance RFC 7489
特徴	送信元をネットワーク的に判断 （送信元のIPアドレスにより確認）	送信時に電子署名をメールに付加 （電子署名の検証により判断）	SPFあるいはDKIMの認証結果を利用 （送信側でポリシーを設定、認証結果のレポート機能）
導入コスト	送信側はほぼ皆無（DNSの記述のみで１通ずつの処理は不要） 受信側では一定の処理が必要	送信側は相対的に高め （１通ずつ署名作成・付加が必要） 受信側では一定の処理が必要	既にSPF, DKIMを導入していれば送信側はほぼ皆無 （DNSの記述のみ） 受信側では一定の処理が必要
長所	送信側の導入の容易さ（特にコスト面） 普及が進んでいる	メール本文の改ざんも検知 メールの配送経路に影響されない	送信側の導入の容易さ 認証失敗時のふるまいをポリシー指定可能
短所	メール転送時に認証失敗する場合がある	配送経路上でメール内容が変更されると認証失敗 第三者署名ではDMARC認証に失敗する場合がある（DNS設定の工夫で回避できる場合がある）	SPFとDKIM双方が失敗する場合には認証が失敗する

DMARC の特徴

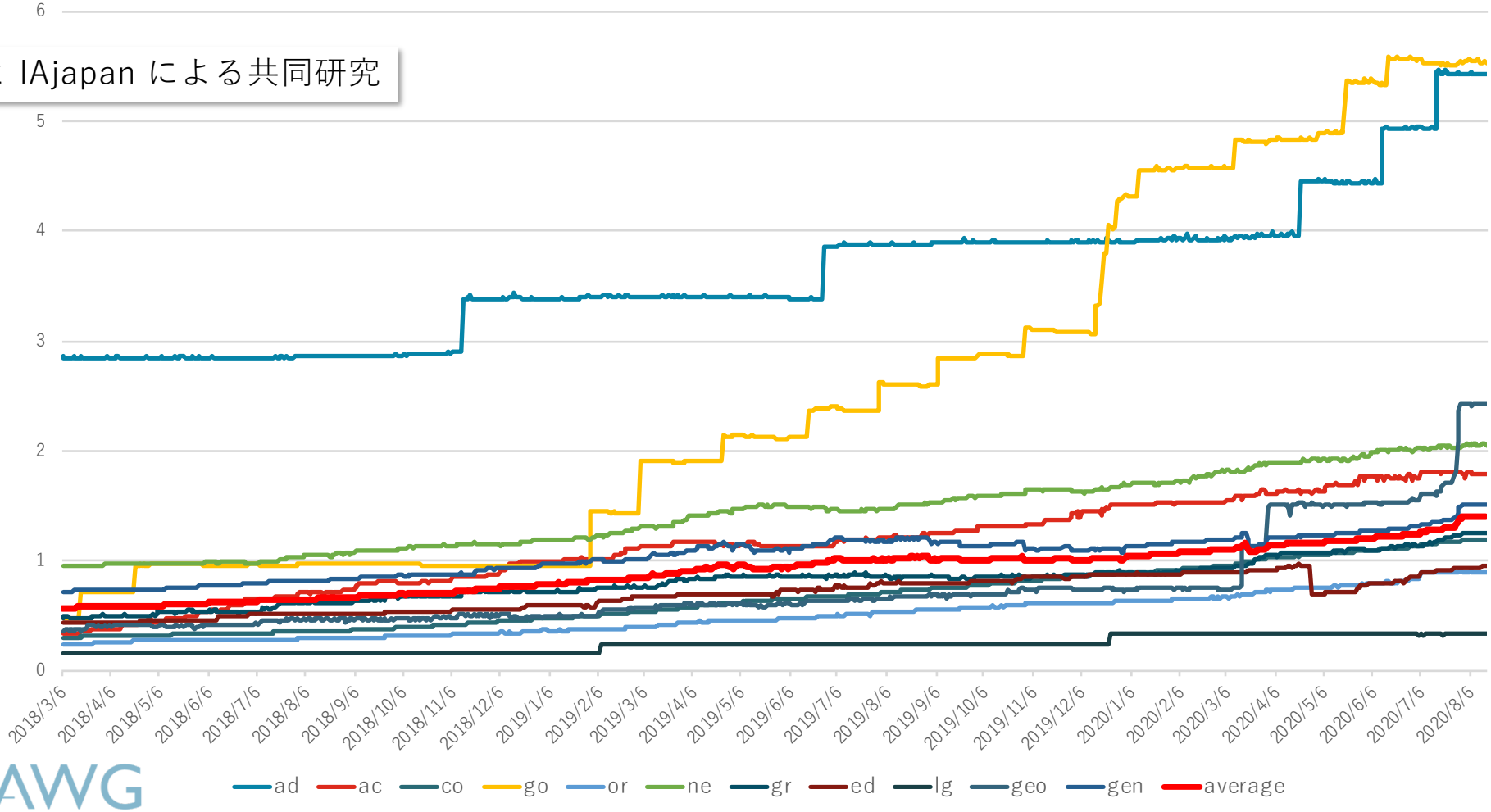
- 認証方式
  - SPF and/or DKIM で認証されたドメインと RFC5322.From
- 特徴
  - ドメイン管理側 (メール送信者) が認証失敗時の取り扱いを policy 宣言
    - none (何もしない), quarantine (隔離), reject (受信拒否)
  - ドメイン管理側に認証結果の report 送信
    - Aggregate Report (rua) と Failure Report (ruf) の 2種類
    - Report 送信先を委譲可能
      - DNS に委譲関係を設定
  - 組織ドメイン (上位ドメイン)
    - サブドメインまで影響させることが可能



JP ドメイン名の DMARC 設定率

2018.03.06 ～ 2020.08.16

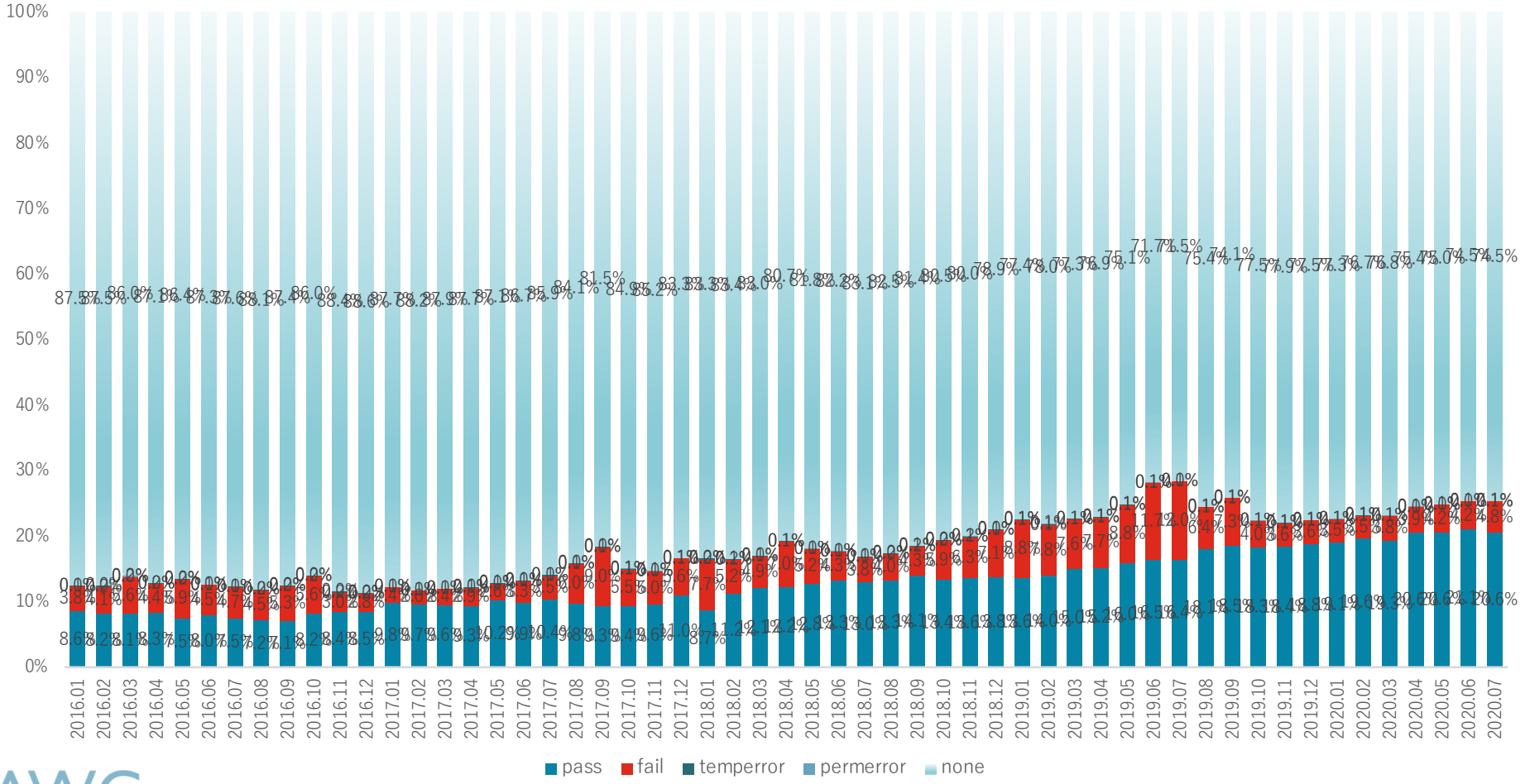
JPRS と IAjapan による共同研究



JPAAWG

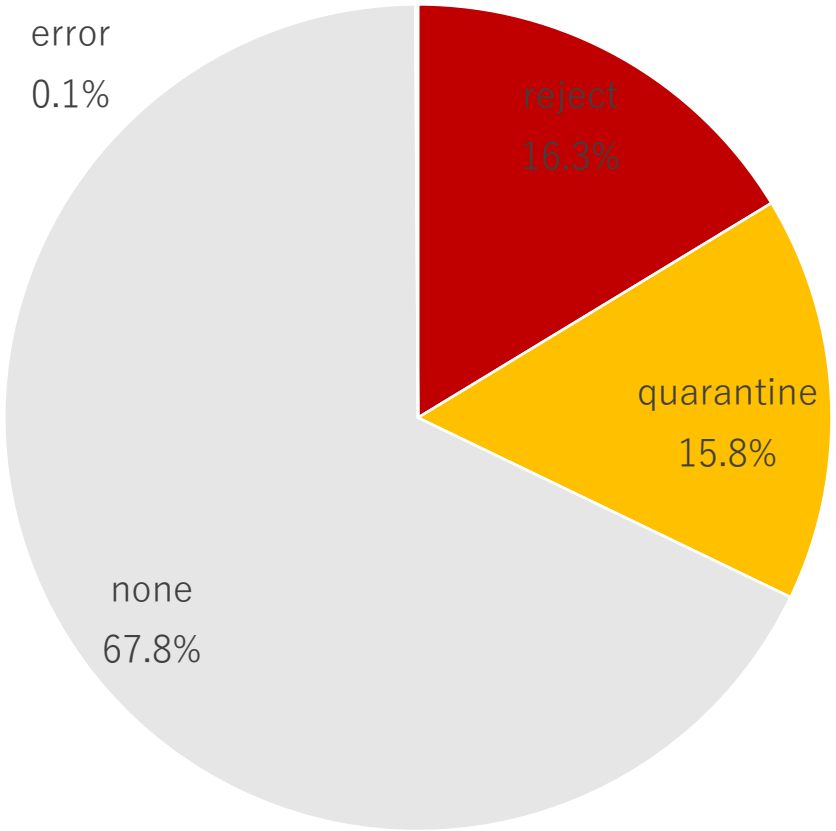
受信メールの DMARC 認証割合

2016.01 ～ 2020.07



DMARC 設定ポリシー割合

2020.07



JPAAWG

DMARC の活用
BIMI

- 概要
  - Brand Indicators for Message Identification
  - DMARC 認証されたドメイン名に対してロゴを表示する仕組み
- 対応状況
  - Google が対応を表明
    - Support for the BIMI standard in Gmail (2020.07.21)
  - 受信メールで DMARC 対応ドメイン
    - 523 ドメインが default のレコード設定
  - 標準化動向
    - I-D (draft-blank-ietf-bimi-01)