フィッシングメールの対策

2020.01.23

Japan Anti-Abuse Working Group (JPAAWG)

Internet Initative Japan Inc. (IIJ)

櫻庭 秀次

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 12社のメンバ)
- General Meeting
  - 第1回 JPAAWG General Meeting (IAjapan 第18回迷惑メール対策カンファレンスと併催)
    - 2018.11.08 @ 赤坂インターシティ，来場者数 411名
  - 第2回 JPAAWG General Meeting (IAjapan 第19回迷惑メール対策カンファレンスと併催)
    - 2019.11.14-15 (二日間) @ ベルサール飯田橋ファースト, 来場者数 436名

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 (ホスト) の悪用 → 対応までの時間で大量送信
  - 高速化 (通信環境) し便利 (ホスト利用環境) になるインフラの悪用
- メール受信側
  - 巧妙化する送信手法，コンテンツ，添付ファイル
  - 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)
    - 緊急避難ではなく恒久対策が必要 (正当業務行為としての導入)

事業者として考えられる対応
メール送信側

- 踏み台送信問題対策
  - SMTP AUTH により個々の送信者を特定
    - 報告があればログ等から調査し該当アカウントを利用停止
    - 利用者のパスワード変更やウイルスチェック等の実施を依頼
  - 海外からのメール投稿を原則禁止する施策導入の検討
    - 海外からの投稿か可能にするインタフェース (Web) を提供し個別に opt-out
    - 包括同意により実施するためには，法的整理が必要という認識
    - 海外からの投稿ができなくなっても国内からに代わるだけという指摘
- まずは送信元が身元を明らかにする
  - 送信するメールの送信ドメインは事業者側のドメインに限定
    - これまでの利用規約との関係整理，検知や対応の仕組みの導入，サポート体制の検討等が必要
  - 送信ドメイン認証技術 (SPF, DKIM, DMARC) を導入
    - 不正な送信ドメインの利用を禁止
    - 事業者のドメインを利用したなりすましメールを抑制する
    - DMARC および DMARC レポートの利用

事業者として考えられる対応
メール受信側

- 迷惑メールフィルタの提供
  - フィッシングメールが迷惑メールフィルタで検知されることを期待
  - URL フィルタリングの導入
    - コンテンツ (本文，添付ファイル) 中の URL を精査し判定する URL フィルタリングの導入 (URL の形式等も含め)
    - コンテンツ中の URL ドメインに対する評価の導入
- 送信ドメイン認証の導入
  - なりすましメールに対しては送信ドメイン認証で検知
    → No Auth, No Entry
  - 独自ドメイン等による認証が通るメール (なりすまさないメール)
    - 認証したドメインに対するドメインレピュテーション (評価) の導入
    - White List としての利用が進む可能性あり
      - 受信フィルタをより強化，その一方で必要なメールを受け取るための仕組みとして
      - 踏み台利用された場合は送信側に通知する仕組み (フィードバックループ) を検討
- メールの盗聴対策
  - 特に BEC (Business Email Compromise) では，送信側あるいは受信側のメールを事前に把握していた可能性があると言われている
    - メール作成時 (Web メール等) やメール配送時あるいはメールスプールに対する盗聴対策が必要
    - メール利用者の利用環境 (PC等) に不正なものが含まれていないか等 (事業者としては対象外かもしれないが)

メールの安全性を高める技術
メール配送の暗号化

- 課題
  - TLS downgrade 問題
  - MitM 等による内部情報搾取 → より高度なフィッシング (BEC 等) への発展
  - 証明書の信頼性への不安
- DNS を利用した配送の暗号化通信
  - DANE (DNS-based Authentication of Named Entities, RFC6698) の利用
    - DNSSEC を利用し DNS の信頼性を高める
    - 既存 CA (Certificate Authority) を使わない暗号化通信
  - MTA-STS (SMTP MTA Strict Transport Security, RFC8461) の利用
    - 事前に TLS (STARTTLS) の対応状況や TLS 接続ポリシーを受信側が表明
    - これにより TLS downgrade 問題への対応を期待
  - TLSRPT (SMTP TLS Reporting, RFC8460) の利用
    - TLS (DANE 含む) 接続状況に関する情報共有の仕組み ← TLS 版 DMARC レポート

メールの安全性を高める技術

利用者の利便性向上

- BIMI
  - Brand Indicators for Message Identification
  - 送信ドメイン認証 (DMARC) されたメールに対して，Brand Indicators (アイコン等) を受信者に提示する仕組み
  - 受信側で認証されたドメインを適切に評価し Brand Indicators を提示できれば，メール利用者にとって視覚的に安全なメールであることが判断可能
  - これにより DMARC の導入 (より強いポリシーでの) が進むことも期待される
- 類似の仕組み
  - Yahoo! メールでのブランドアイコンの表示
  - 利用する送信ドメイン認証技術は DKIM
  - 表示する送信者 の選択は Yahoo! Japan

参照: https://about.yahoo.co.jp/pr/release/2018/10/30b/

送信ドメイン認証技術等の導入状況

- メールサービスからみた調査
  - 受信メール対する各認証結果

- JP ドメイン名の調査
  - JPRS と日本データ通信協会との共同研究契約に基づく JP ドメイン名の調査 (総務省の web site* で定期的に公開)
  - 独自調査のドメイン名(地方自治体) 調査
  - SPF, DMARC, MTA-STS の各レコードの設定状況を調査

* https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei

JP ドメイン名の DMARC 普及率
2020.01.18

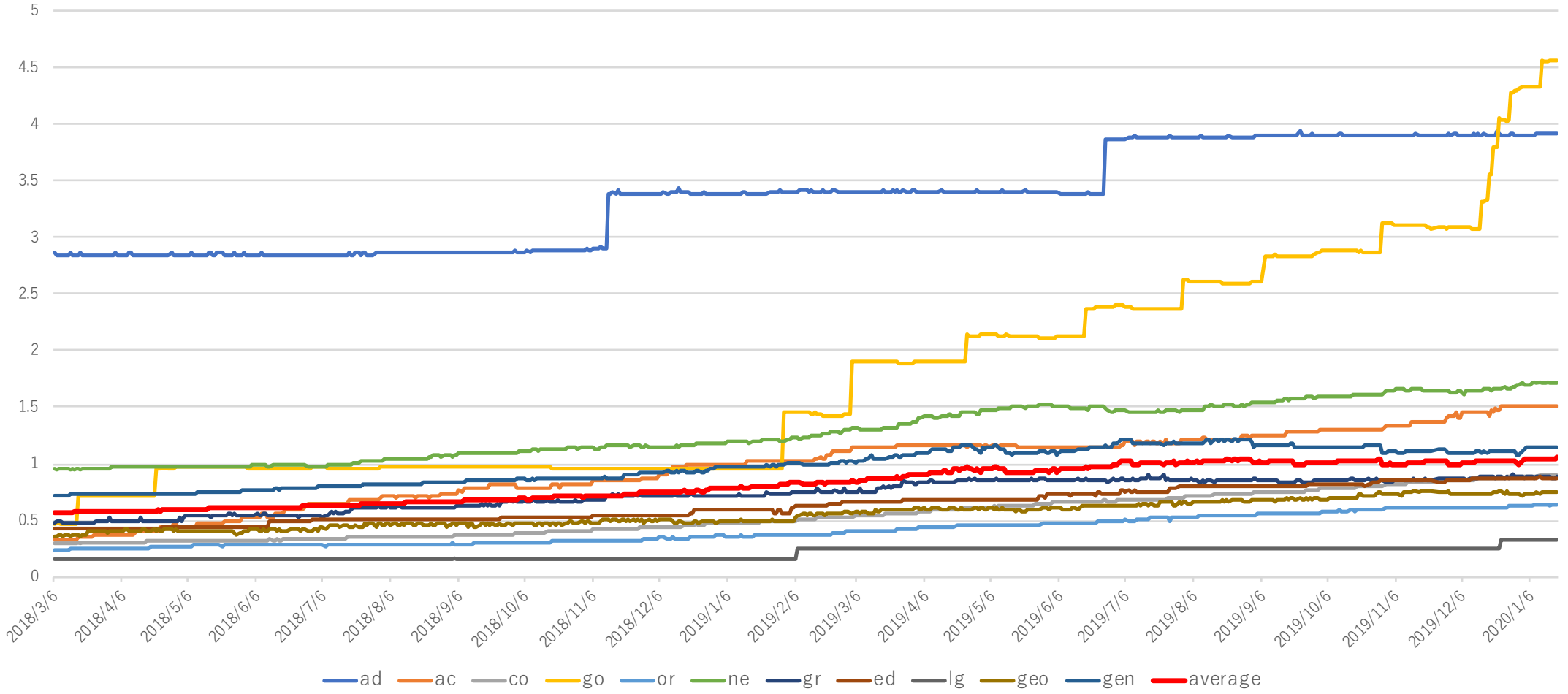
JP ドメイン名全体に対する MX レコードの宣言割合: 81.1%
MX設定ドメイン名に対する SPF レコード宣言割合: 63.9%
MX設定ドメイン名に対する DMARC レコード宣言割合: 1.06%

登録型	MX (%)	SPF (%)	DMARC (%)
AD	81.9%	70.6%	3.9%
AC	94.4%	70.5%	1.5%
CO	94.0%	73.3%	0.9%
GO	72.2%	93.1%	4.6%
OR	93.8%	71.5%	0.6%
NE	81.6%	60.3%	1.7%
GR	89.3%	61.2%	0.9%
ED	93.0%	68.2%	0.9%
LG	73.6%	79.8%	0.3%
地域型*1	61.4%	56.5%	0.8%
汎用	75.5%	58.8%	1.2%

*1 地域型は新規受付停止
数値は都道府県型を含む

JP ドメイン名の DMARC 普及率の推移

2018.03.06 ～ 2020.01.18



自治体の SPF / DMARC 普及率
2020.01.19

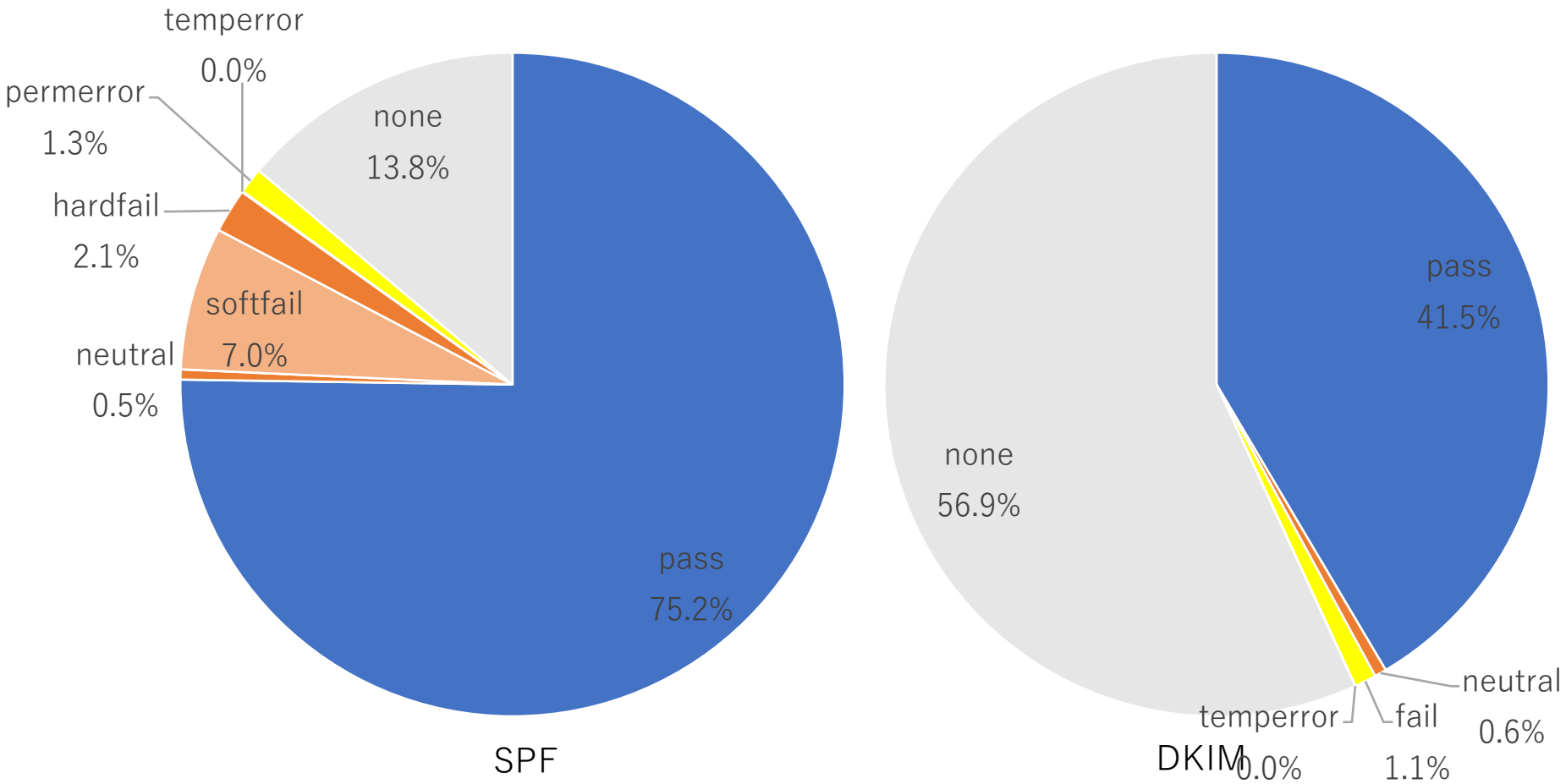
全国での SPF レコード宣言率: 83.1% (1485 / 1788)
全国での DMARC レコード宣言率: 0.7% (13 / 1788)

	SPF (%)	DMARC (%)
北海道	72.2 (130/180)	1.7 (3/180)
東北	85.4 (199/233)	0.4 (1/233)
関東	86.7 (280/323)	1.6 (5/323)
中部	79.4 (258/325)	0.3 (1/325)

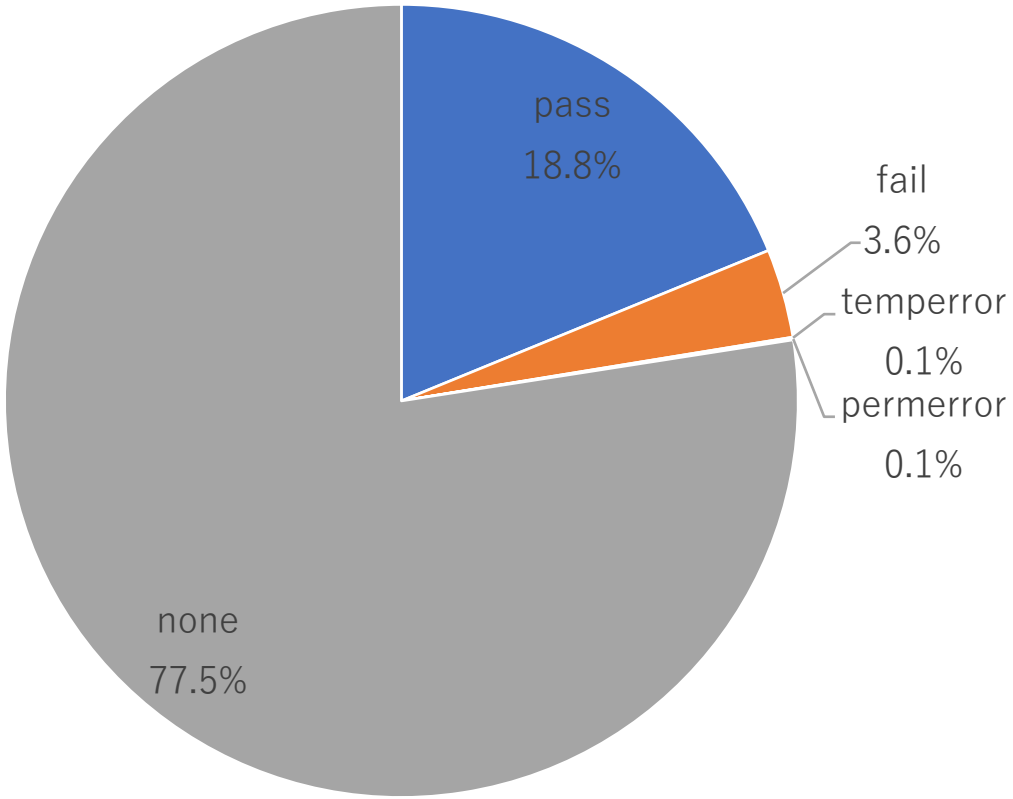
	SPF (%)	DMARC (%)
近畿	88.0 (206/234)	0.4 (1/234)
中国	79.5 (89/112)	0.0 (0/112)
四国	82.8 (82/99)	1.0 (1/99)
九州沖縄	85.5 (241/282)	0.4 (1/282)

注: 全ての対象ドメインに MX レコードが設定されていることを確認済み

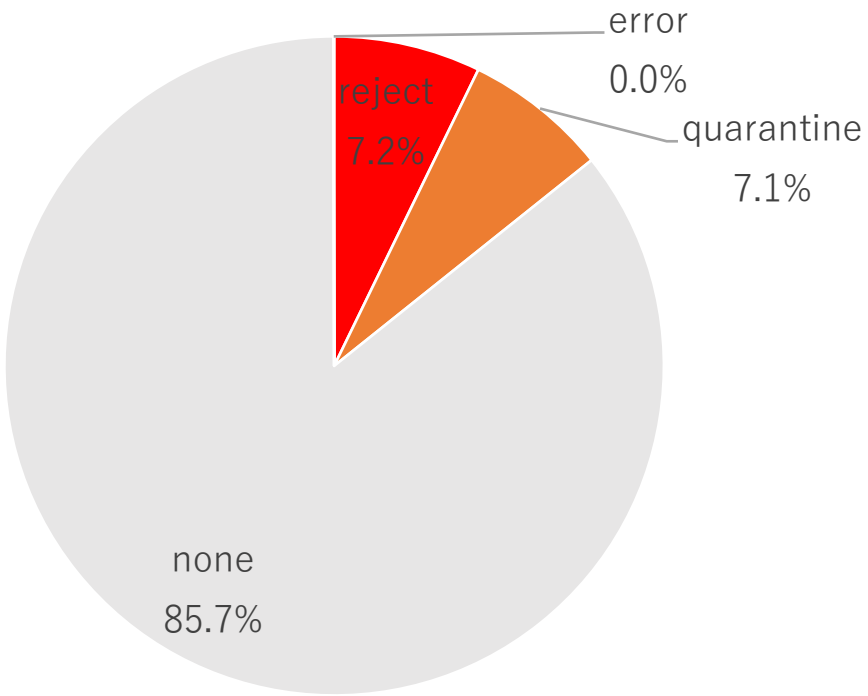
メール受信での送信ドメイン認証技術普及率 2019.12



メール受信での DMARC 普及率
2019.12

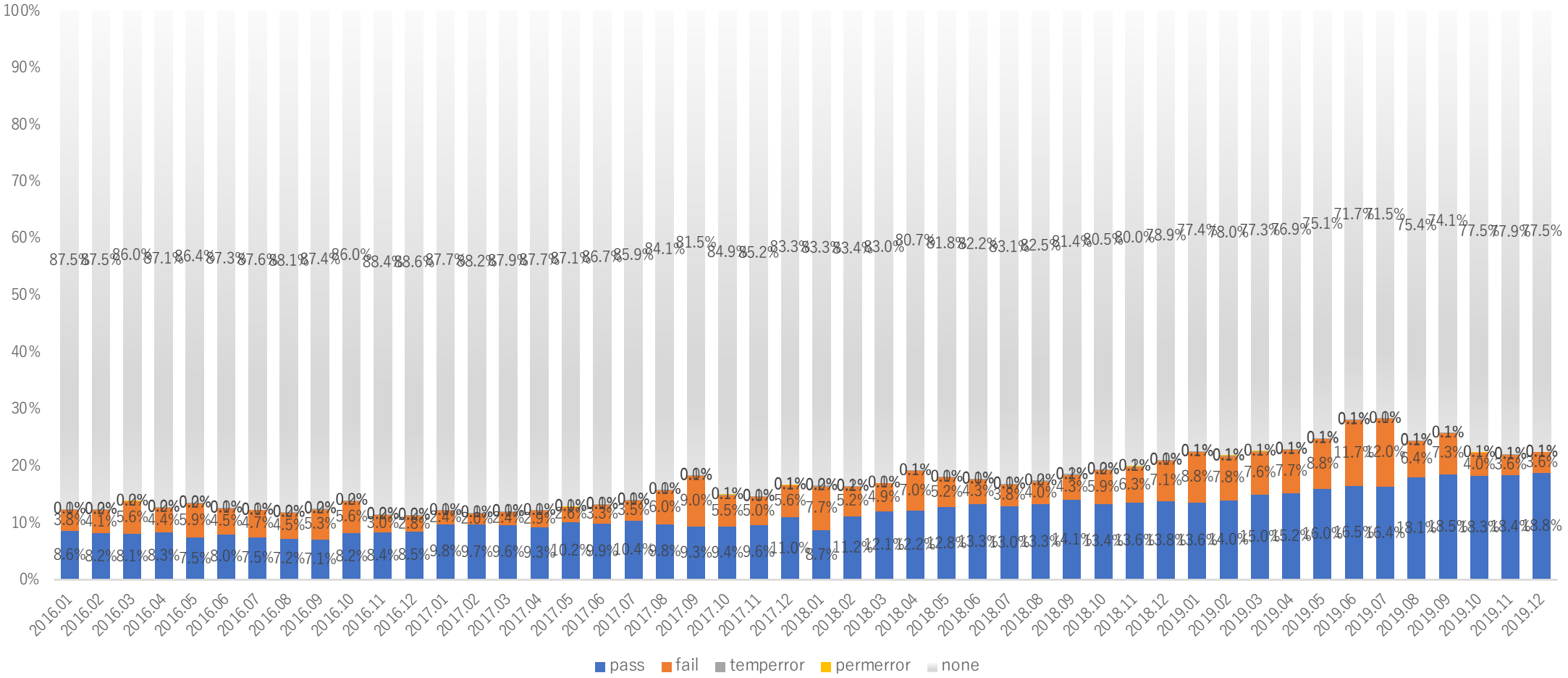


DMARC Results



DMARC Domain Policies

メール受信での DMARC 普及率推移
2016.01～2019.12



議論のポイント

- 技術的な対策や仕組みが日本であまり進んでいない
  - 送信ドメイン認証技術やそれらの応用技術（ドメインレピュテーション，フィードバックループ等を含む）が欧米に比べて導入が遅れている原因は
  - これらの技術が正しく理解され，その効果を示すにはどうすれば良いか
  - 法的な制限（通信の秘密）が技術の普及を阻害しているのか
- メール利用者を守るために必要なこと
  - 既に情報漏洩や金銭的被害等が発生している状況で，メールサービス事業者はどう対応していくべきか
  - 既に利用されているメールサービスに対し，新しい技術対策を導入する際には個別同意が必要だがそうした状況をどう考えるか

    → あるいはこれまでの法的整理のやり方を見直すべきか等