JPAAWG | Japan Anti-Abuse Working Group

増え続けるフィッシング被害を乗り越えるために，我々がすべきこと

JANOG 49 meeting @ Kagoshima & Online

2022.01.28

JPAAWG / Internet Initiative Japan Inc. (IIJ)

SAKURABA Shuji

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各種対策を検討する WG
  - 2018.03 の pre-meeting を経て 2019.05 正式発足
- General Meeting
  - 2018.11.08[Thu] 1st General Meeting 開催 (411名参加)
  - 2019.11.14[Thu], 15[Fri] 2nd General Meeting 開催 (436名参加)
  - 2020.11.11[Wed], 12[Thu] 3rd General Meeting 開催, Online (637名参加登録)
  - 2021.11.11[Thu], 12[Fri] 4th General Meeting 開催, Online (607名参加登録)
  - IAjapan 主催, 迷惑メール対策カンファレンスと併催 (第18, 19, 20, 21回)
- その他カンファレンス
  - 2020.12.15[Tue] SMS フィッシング対策カンファレンス 開催, Online (272名参加登録)
  - 2021.02.25[Thu] パスワード付きzip添付メール問題を考える 開催, Online (411名参加登録)

問い合わせ先: contact@jpaawg.org
https://www.jpaawg.org

フィッシング対策の課題

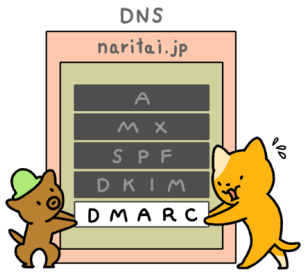
- メール送信側
  - ISPs 等のメールサーバの悪用 (窃取 or 流出した認証 ID/Password の悪用)
    → 踏み台送信
  - 固定 IP やクラウドサービス (ホスティング) の悪用，海外からの送信
    → 検知対応するまでの時間内で大量送信，短時間で撤退
  - 高速化 (通信環境) し便利 (ホスト利用環境) になる各種インフラの悪用
  - 送信元を正しく確認 (送信ドメイン認証) できないような設定
- メール受信側
  - 受信メールへの不正アクセスによる情報漏洩 (認証情報の窃用) ← BEC へと発展
    - Feedback Loop による検知と対策が必要
  - 巧妙化する送信手法，本物と同じコンテンツ，添付ファイル対策の難しさ (PPAP)
  - 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)
  - 受信者にとってわかりやすい結果の提示

前回 (janog45-48) までのおさらいと今回の主題

- 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) の受信と対策
  - 送信ドメイン認証技術の導入，正しい設定方法
- メール受信側
  - 迷惑メールフィルタ (AntiVirus Filter 含む)
  - 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)
  - FBL (Feedback Loop) の通知

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 (詐称されていないことを確認)
  - 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
  - 認証結果は `Authentication-Results` ヘッダに記載



ナリタイ <naritai.jp>

	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

JPAAWG

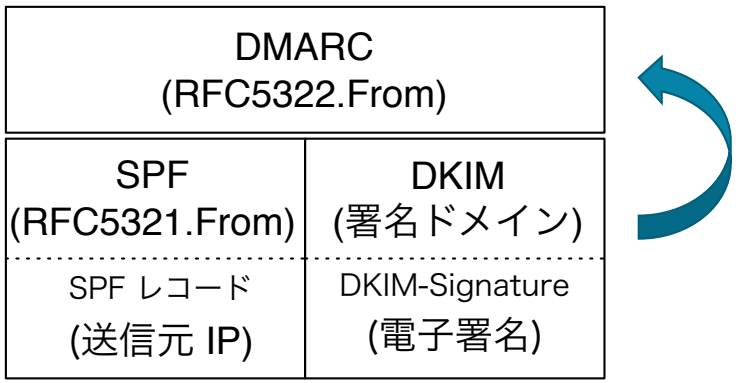
送信ドメイン認証技術導入マニュアル改訂

- 入手方法
  - 迷惑メール対策推進協議会 (事務局: デ協) の Web Site

    https://www.dekyo.or.jp/soudan/aspc/report.html#dam
  - (一財)日本データ通信協会 → 迷惑メール相談 → 迷惑メール対策推進協議会 → 関連資料について → 送信ドメイン認証技術導入マニュアル (深い…)
- 改訂概要
  - 構成を「基礎編」と「応用編」に変更
  - 基礎編
    - メールに関する基本的な解説
    - SPF, DKIM, DMARC についての仕様解説
    - 認証結果ヘッダ (Authentication-Results) の技術仕様解説
  - 応用編
    - DMARC 認証できることを目的に SPF, DKIM を含めた DMARC 運用のための注意点等
    - メールの送信側と受信側で各送信ドメイン技術の導入に際し，気をつけるべき tips 等を解説

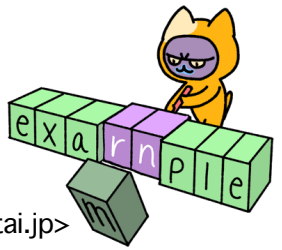
DMARC の特徴

- 認証方式
  - SPF and/or DKIM で認証されたドメインと RFC5322.From との比較
- 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



フィッシング対策と送信ドメイン認証技術

- 詐称元をそのまま利用
  - SPF, DKIM (none が多い) 詐称は少ない (最近は堂々と詐称する場合も)
  - DMARC の詐称多い → 認証結果の確認と DMARC 設定を
  - SPF の設定ミスを悪用 (permerror になる) → pass 以外の認証結果は信用しない
- 独自ドメインを利用
  - 認証結果が none → pass しないメールの検討要 (ex. No Auth, No Entry)
  - 認証結果が pass → 認証したドメインの確認も必要
    紛らわしいドメイン名も増えてきている (ex. smbnc-card.com, amczor.com, etc)
- 不正な形式の利用で認証回避
  - RFC5322.From (ヘッダ From) がドメイン名のみ (メールアドレス形式ではない) → DMARC が none となる, DMARC の普及 & 形式違反に対するチェックを
- display name を悪用
  - 上記不正な形式との組み合わせる場合が多い
  - display name のみあるいは優先表示する MUA (webmail も) に注意

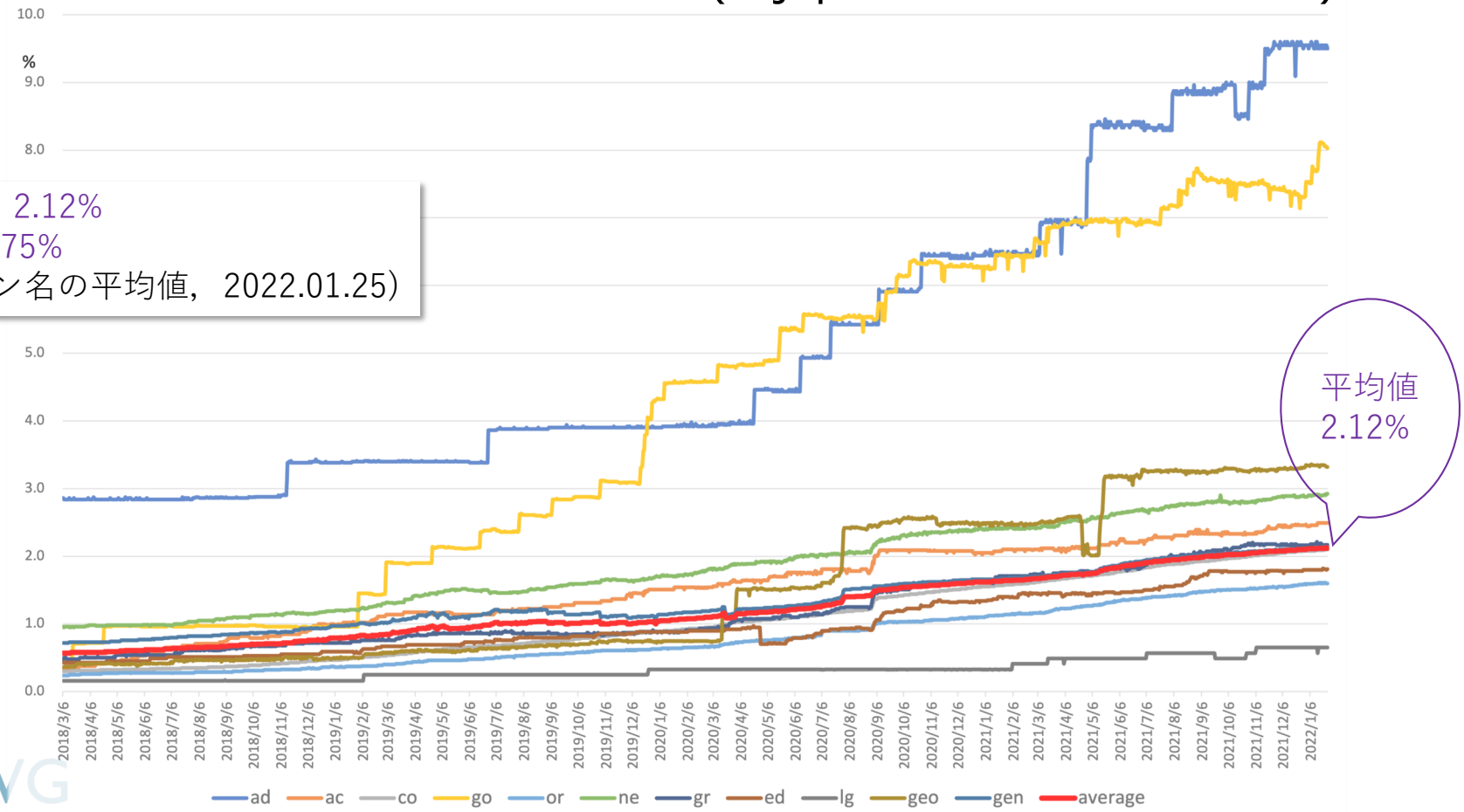


ナリタイ <naritai.jp>

送信ドメイン認証技術の普及状況

JP ドメイン名の DMARC 宣言率推移 (IAjapan & JPRS との共同研究)

DMARC は 2.12%
SPF は 67.75%
(jp ドメイン名の平均値，2022.01.25)



送信ドメイン認証技術の普及状況

地方自治体 (ドメイン名は独自調査, 2022.01.26)

全国での SPF レコード宣言率: 85.2% (1523 / 1788)
全国での DMARC レコード宣言率: 1.0% (18 / 1788)

	SPF* (%)	DMARC* (%)
北海道	77.2 (139/180)	1.7 (3/180)
東北	86.3 (201/233)	0.4 (1/233)
関東	90.1 (291/323)	1.9 (6/323)
中部	81.2 (264/325)	0.9 (3/325)

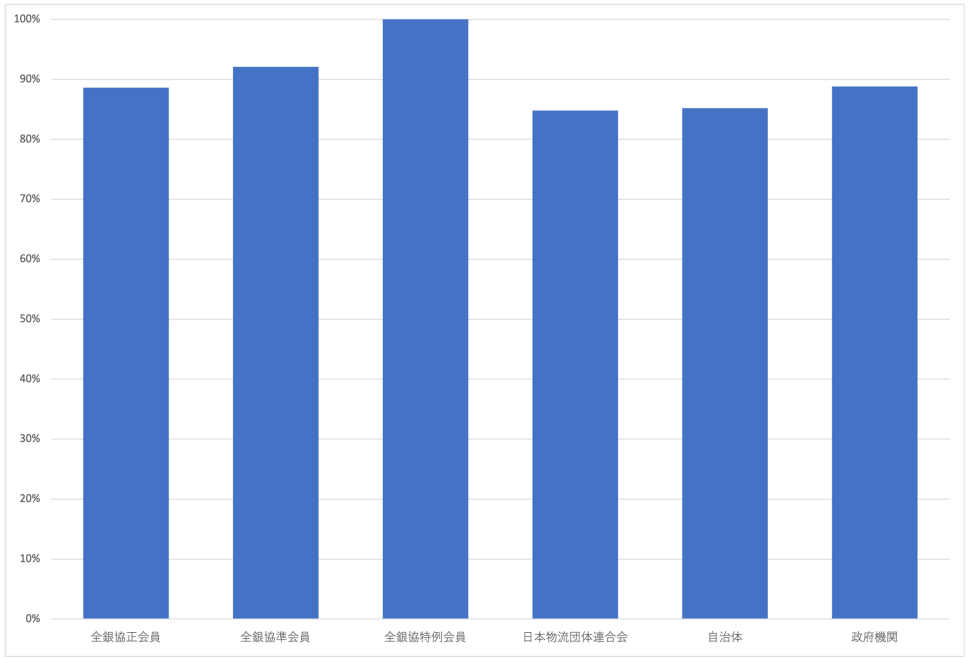
	SPF* (%)	DMARC* (%)
近畿	89.3 (209/234)	0.9 (2/234)
中国	79.5 (89/112)	0.0 (0/112)
四国	83.8 (83/99)	2.0 (2/99)
九州沖縄	87.6 (247/282)	0.4 (1/283)

JPAAWG

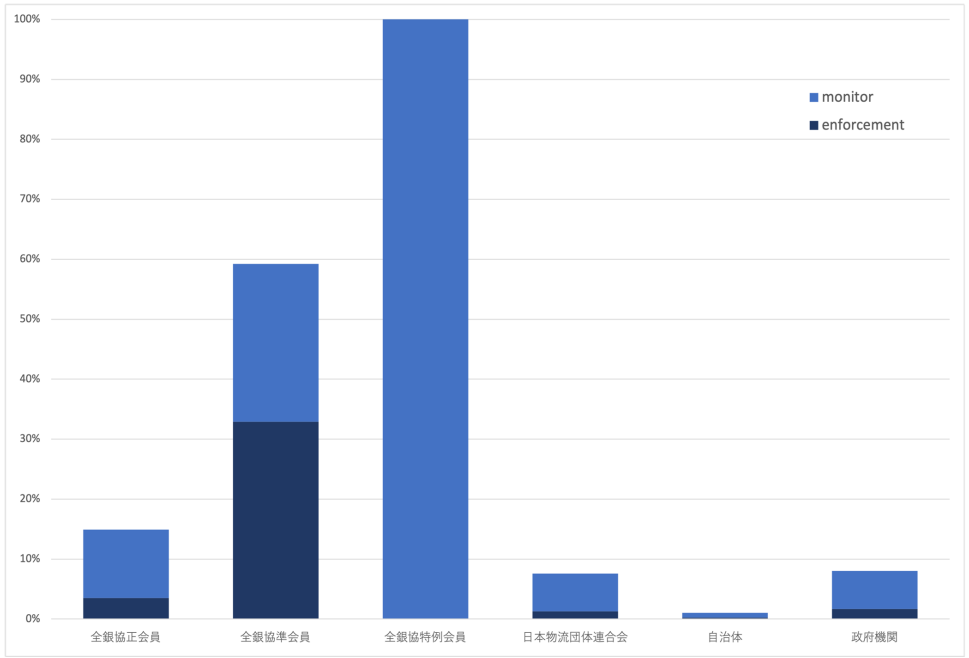
* 全ての対象ドメインに MX レコードが設定されていることを確認済み

送信ドメイン認証技術の普及状況
業界団体の調査(ドメイン名は独自調査, 2022.01.26)

SPF



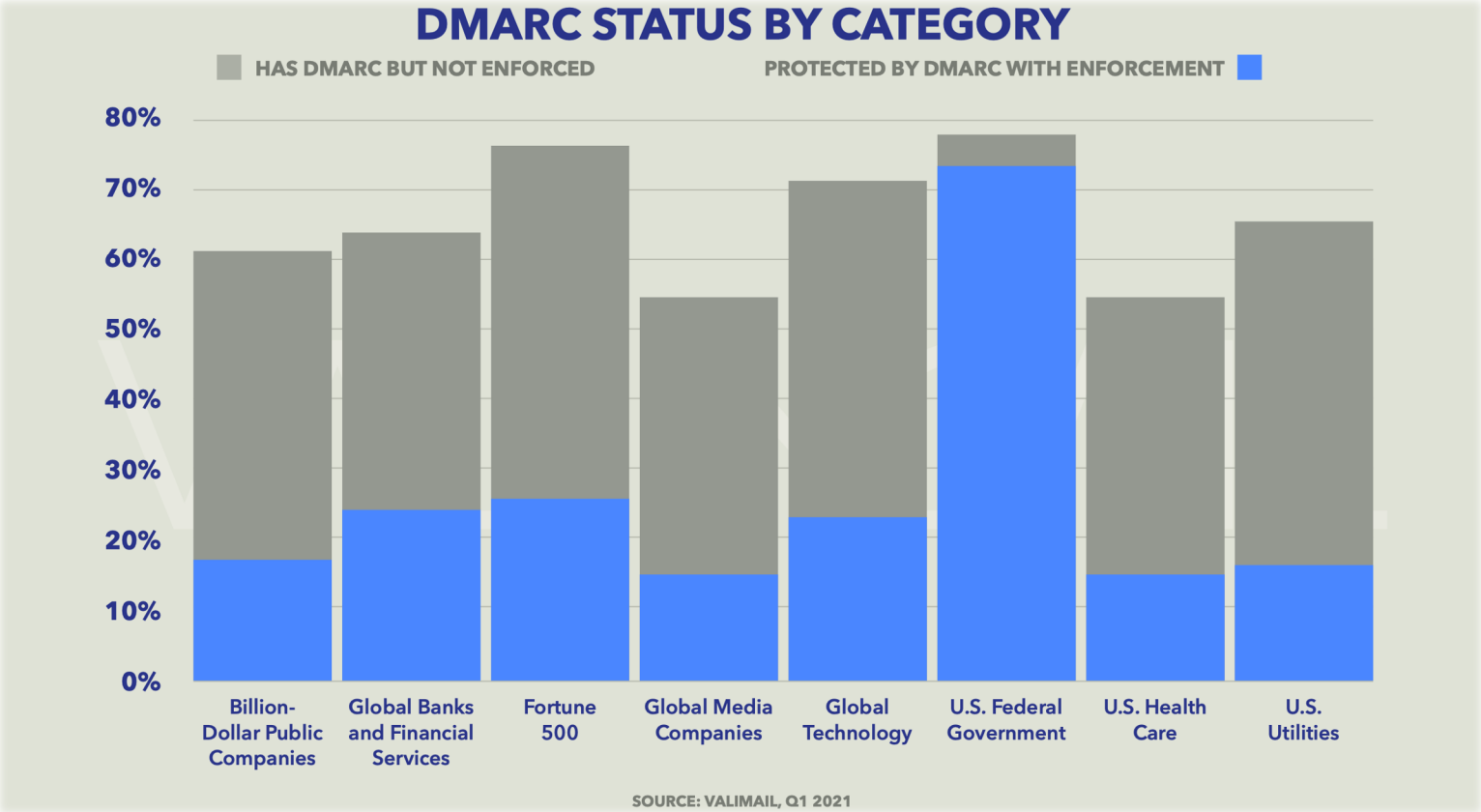
DMARC



- 全てのドメイン名は MX 資源レコードが設定されていることを確認済み
- 自治体のドメイン名は独自調査 (lg.jp 以外も含む)
- 政府機関は go.jp ドメイン名が対象

送信ドメイン認証技術の普及状況

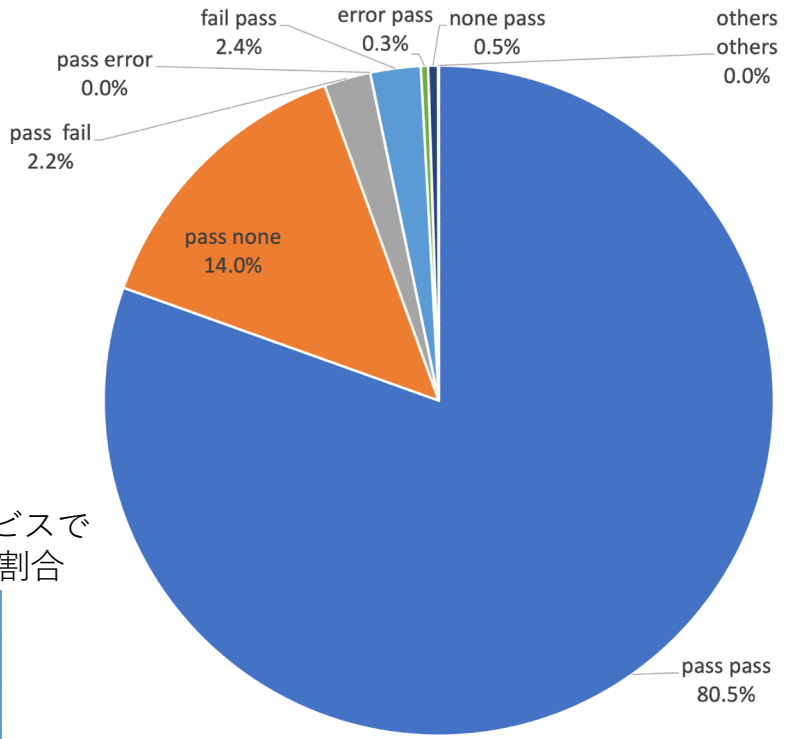
米国 (Valimail 社 Research Report, March 2021)



DMARC 認証の依存度

- DMARC が pass したときの SPF, DKIM それぞれの寄与割合*
  - SPF & DKIM: 80.5%
  - SPF のみ: 2.2%
  - DKIM のみ: 3.2%

- DKIM の導入も重要!



- 2020年に IIJ のメールサービスで受信したメールの認証結果割合

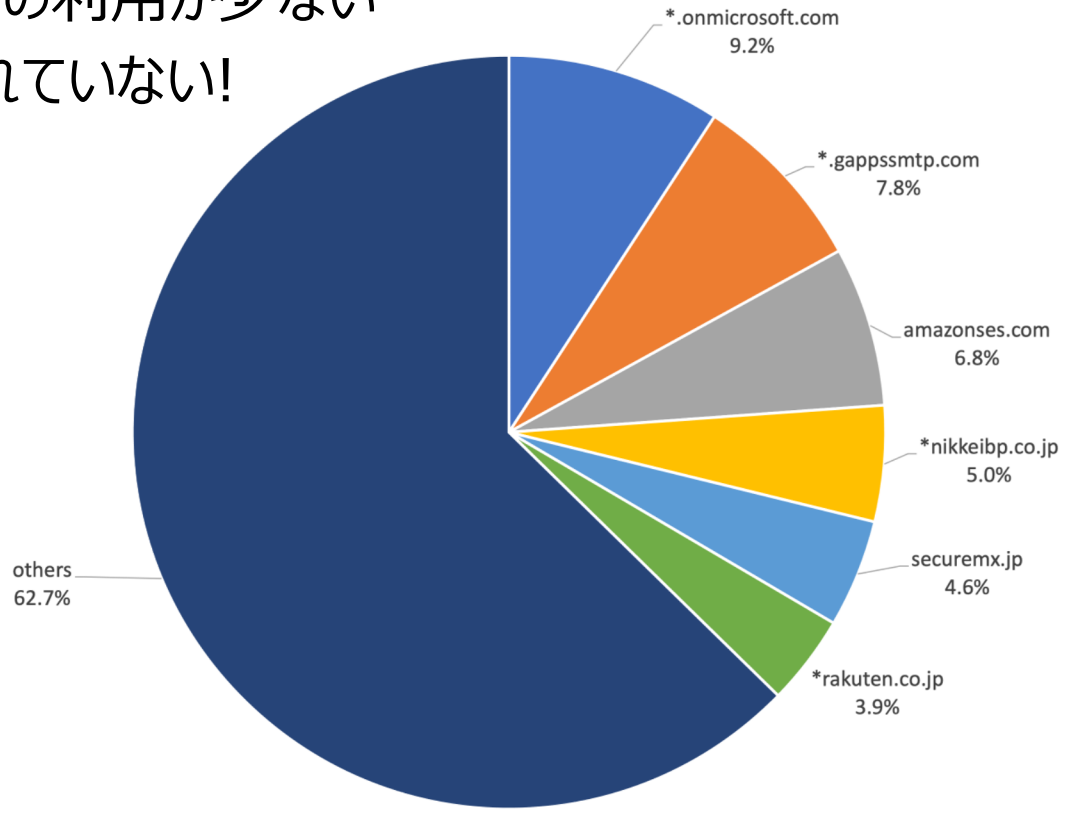
認証割合 (pass)	
SPF	73.0%
DKIM	42.7%
DMARC	19.2%

* 但し認証されたドメイン名まで確認していないので正確にDMARC認証に寄与したかどうかまでは不明

JPAAWG

DKIM の認証ドメイン名

- 自組織ドメイン名の利用が少ない
  → 正しく設定されていない!



クラウドサービスでの DKIM 利用方法

- Microsoft 365
  - 「DKIMを使用して，カスタムドメインから送信される電子メールを検証する」…(若干誤訳な気が)
    - DKIMを構成するドメイン名 → DKIMキーの作成 → 表示されるCNAMEを確認
    - DNSサービスで CNAME を設定 → DKIMページでDKIMを有効に設定
  - 鍵管理は自動，CNAME で実態とリンクをとる
- Google Workspace
  - 「DKIMを使用してメールを認証する」
    - 送信メールのドメイン鍵を生成する → ドメインプロバイダでDKIM鍵を追加する → 管理コンソールでDKIM署名を有効にする
  - 自ドメインに手動で DMARC レコード (公開鍵) を設定
- Amazon SES
  - Route 53 でドメイン名を管理している場合はほぼ自動で設定される
  - それ以外の DNS プロバイダを利用している場合は CNAME で 3つのレコードを設定する (SPF, DMARC の CNAME 用レコードも提供される)

まとめ

- フィッシング対策としての DMARC の導入
  - メール受信者が参照可能なヘッダ From (RFC5322.From) の詐称を防ぐ技術
  - DMARC 導入のためにはまず SPF の設定，DKIM の正しい設定についても
  - DMARC レポートにより，送信側 (ドメイン管理側) が送信ドメイン認証技術の設定状況の確認，詐称メールの状況を把握 → SPF, DKIM の設定確認を
- サービス運用側でも対応しやすい対応を
  - ドメインの運用形態は様々なので，それぞれでの設定例を示すなど工夫を
  - DNS で “_” が利用できないとか，CNAME をTXT RRに設定できないとかはちょっと…
- さらに
  - DMARC 認証後の仕組み (BIMI) も利用が増えてきています
  - より強い (enforced) DMARC ポリシーの設定，そのための設定確認を

議論のポイント

- DKIM 署名を自ドメインで行えない理由は他に何かあるのか
- DMARC を設定できない理由は何か? 知らないだけ?
- DMARC レポートは活用していますか?