JPAAWG Japan Anti-Abuse Working Group

増え続けるフィッシング被害に今，我々ができること

JANOG 48 meeting @ Online & Ogaki, Gifu

2021.07.15

JPAAWG / Internet Initiative Japan Inc. (IIJ)

Shuji SAKURABA

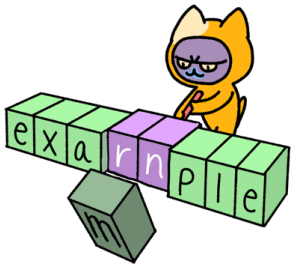
JPAAWG について

- 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)
  - IAjapan 主催，迷惑メール対策カンファレンスと併催 (第18, 19, 20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
Web: 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
    → 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
- 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
  - 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



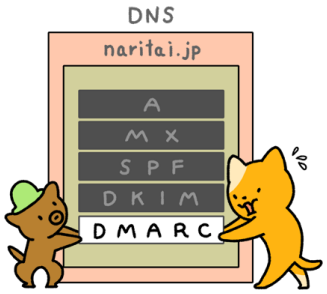
ナリタイ <naritai.jp>

前回 (janog45-47) までのおさらい

- 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) の受信と対策
  - 送信ドメイン認証技術の導入
- 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>

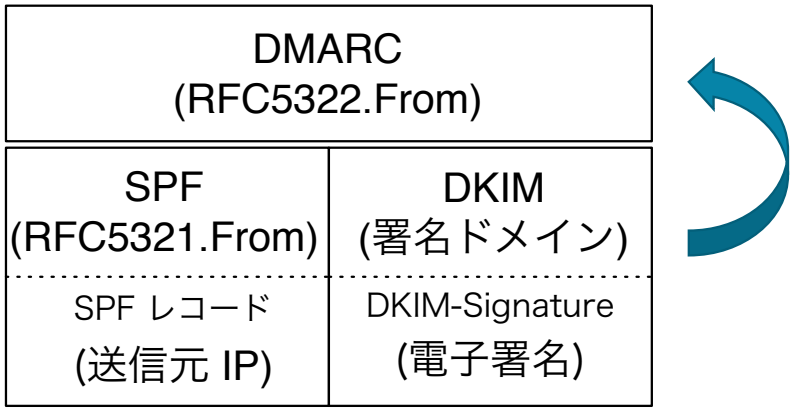
	SPF	DKIM	DMARC
名称	Sender Policy Framework RFC 7208	DomainKeys Identified Mail STD 76, RFC 6376	Domain-based Message Authentication, Reporting, and Conformance RFC 7489
特徴	送信元をネットワーク的に判断 （送信元のIPアドレスにより確認）	送信時に電子署名をメールに付加 （電子署名の検証により判断）	SPFあるいはDKIMの認証結果を利用 （送信側でポリシーを設定、認証結果のレポート機能）
導入コスト	送信側はほぼ皆無（DNSの記述のみで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

近日 update 予定

JPAAWG

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

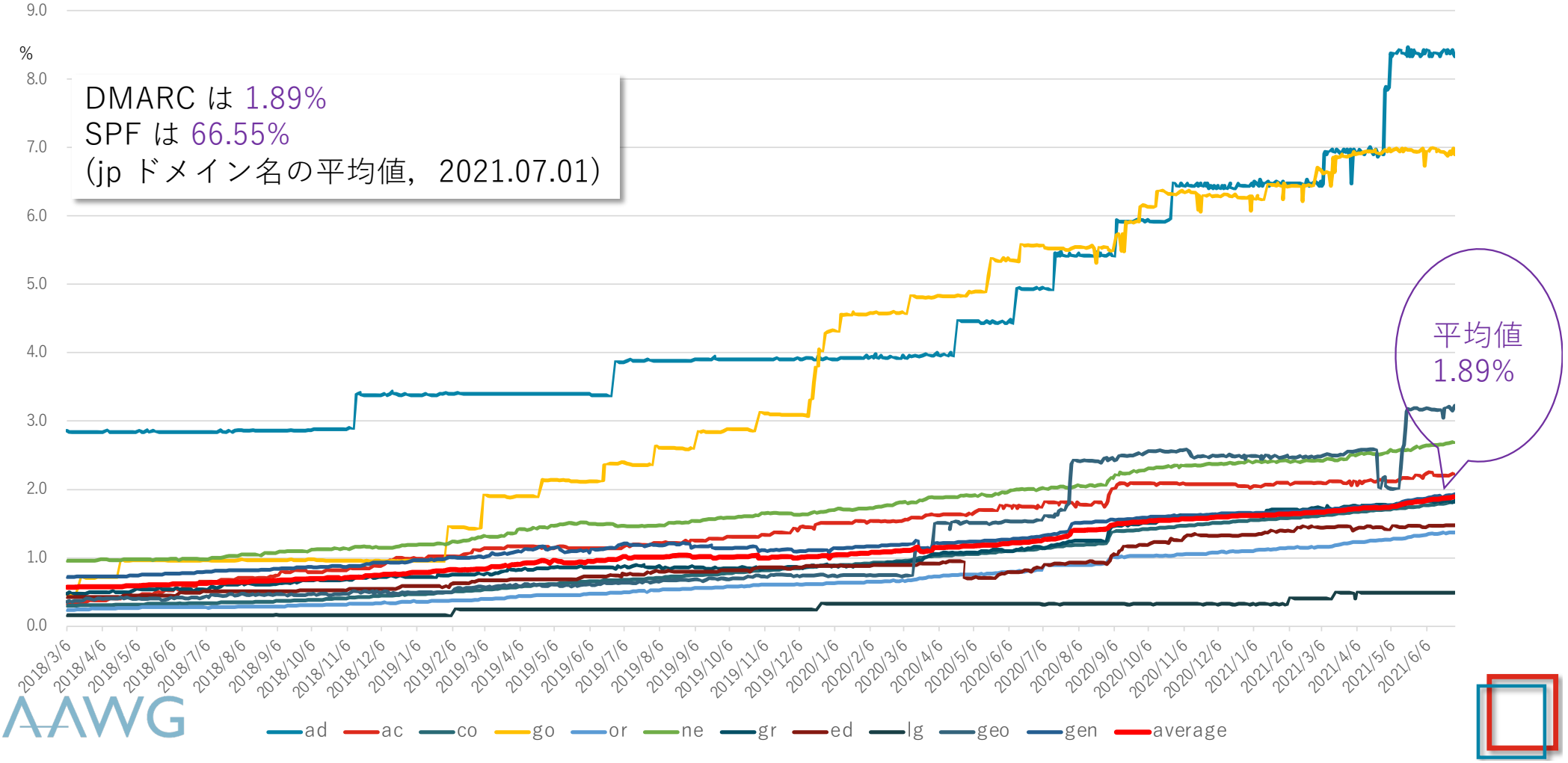
- 詐称元をそのまま利用
  - SPF, DKIM (none が多い) 詐称は少ない (最近は堂々と詐称する場合も)
  - DMARC の詐称多い → 認証結果の確認と DMARC 設定を
  - SPF の設定ミスを悪用 (permerror になる) → pass 以外の認証結果は信用しない
- 独自ドメインを利用
  - 認証結果が none → pass しないメールの検討要 (ex. No Auth, No Entry)
  - 認証結果が pass → 認証したドメインの確認 (ex. domain reputation)
- 不正な形式の利用で認証回避
  - RFC5322.From (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

正しい送信ドメイン認証技術設定

- SPF レコード
  - include 先のドメイン名の SPF レコード (TXT RR) も存在していること
  - 評価中の DNS lookup 回数 (10回) の上限を超えていないこと
    - a mx などは lookup 回数が増える記述
    - 深い include 先まで確認が必要
    - メールサービス提供元が提供する SPF レコードの設定の配慮が必要 (IP, network アドレスのみを記述，が理想)
  - 複数の SPF レコードを設定 (“v=spf1” で始まる TXT RR は一つだけ)
- DMARC レコード
  - 組織ドメインへの DMARC レコード記述でデフォルトの設定を
  - 詐称されて困るドメイン (サブドメイン) 名には，より厳しい (enforced) policy (p=quarantine, p=reject) の設定を
  - 正しい判定処理結果となることが前提 (現時点では RFC7489 が仕様)
- 再配送メールに対する対応
  - メール転送，メーリングリストなど，それぞれの対応も可能であれば

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)



JPAAWG

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, 2021.07.01)

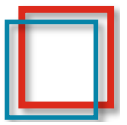
全国での SPF レコード宣言率: 84.6% (1513 / 1788)
全国での DMARC レコード宣言率: 0.9% (16 / 1788)

	SPF* (%)	DMARC* (%)
北海道	76.7 (138/180)	1.7 (3/180)
東北	86.7 (202/233)	0.4 (1/233)
関東	88.5 (286/323)	1.9 (6/323)
中部	81.2 (264/325)	0.6 (2/325)

	SPF* (%)	DMARC* (%)
近畿	88.5 (207/234)	0.4 (1/234)
中国	78.6 (88/112)	0.0 (0/112)
四国	83.8 (83/99)	2.0 (2/99)
九州沖縄	86.9 (245/282)	0.4 (1/283)

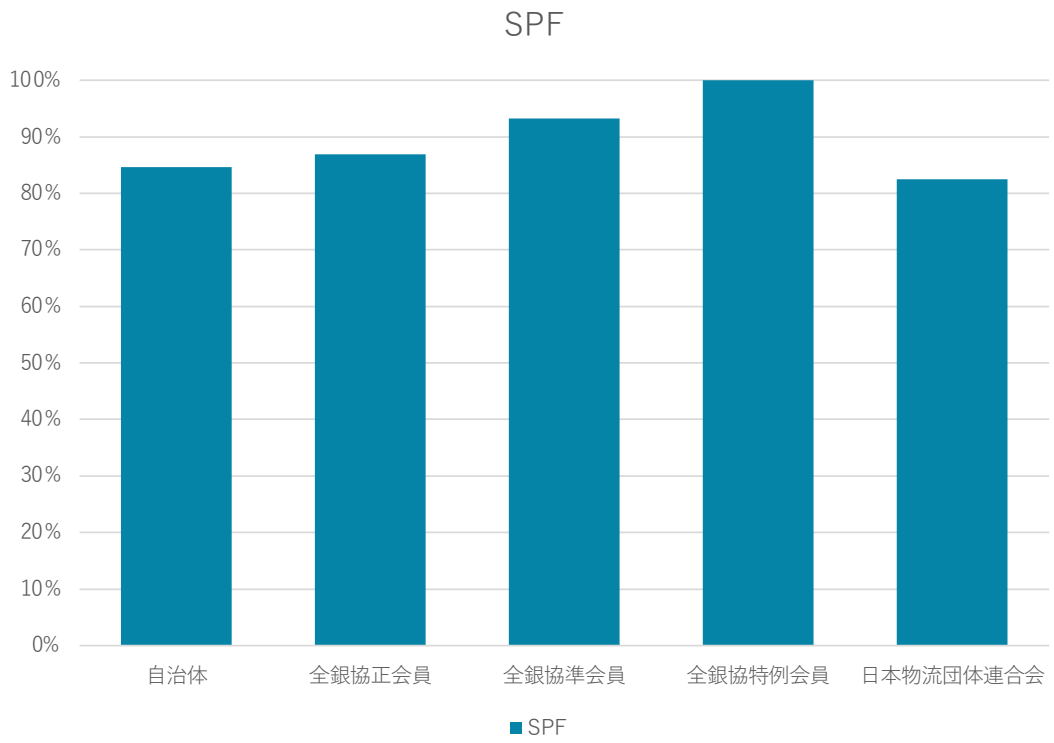
JPAAWG

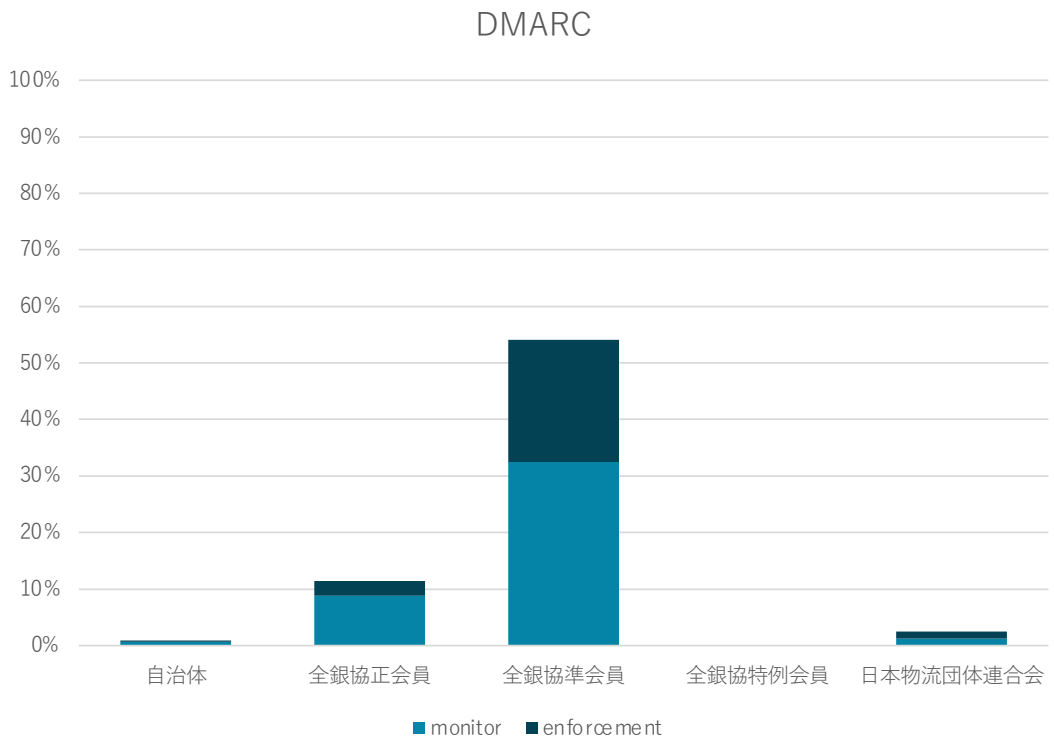
* 全ての対象ドメインに MX レコードが設定されていることを確認済み
* 岐阜県大垣市は city.ogaki.lg.jp を調査



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, 2021.07.01)

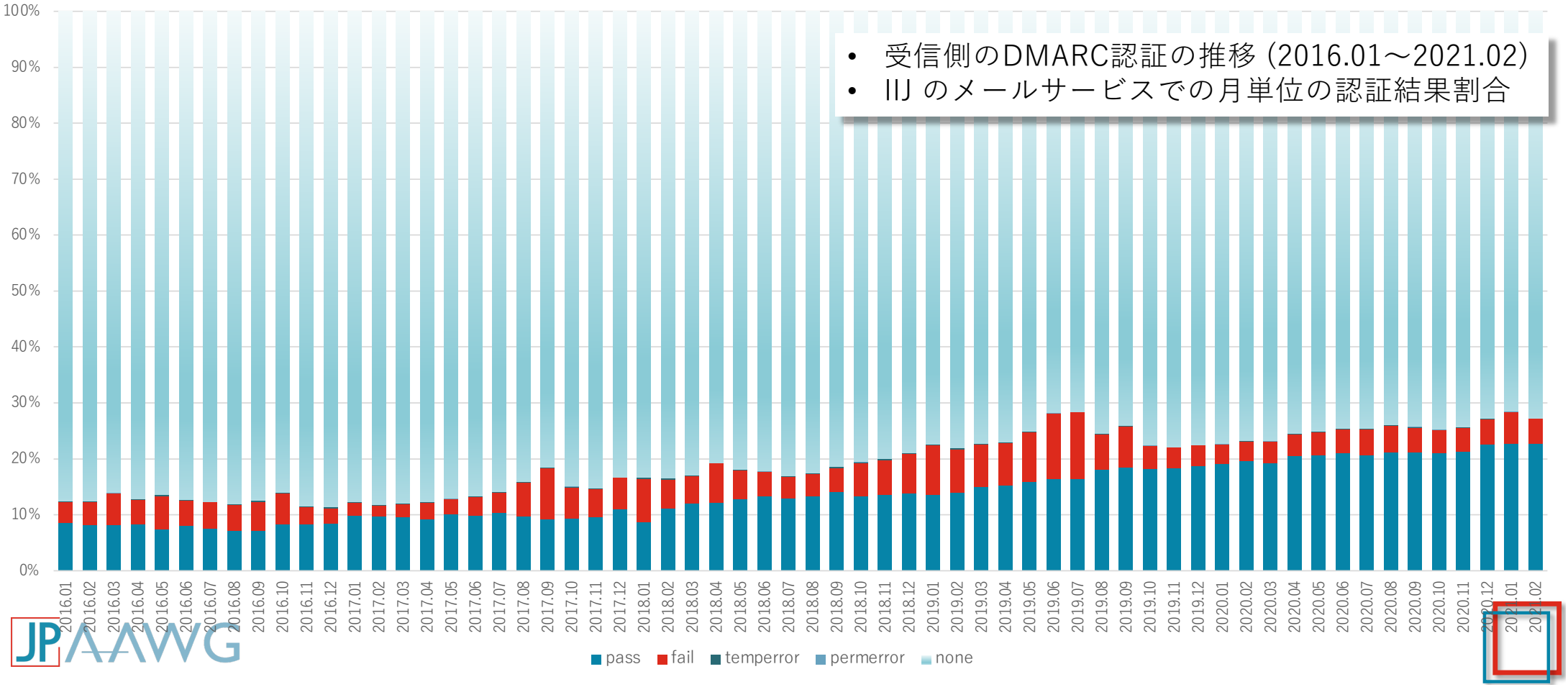




JP AAWG

DMARC の認証結果割合の推移

transition of DMARC authentication results rate



送信ドメイン認証技術の応用

- メールに利用しないドメイン名の設定
  - ドメイン名が DNS 参照できるだけで悪用される恐れあり (親ドメイン等)
  - メールに利用しないことを示す設定方法 (Null MX および SPF, DMARC)

```
example.com.          IN MX  0  .                          ← Null MX
example.com.          IN TXT "v=spf1 -all"                ← fail SPF
_dmarc.example.com.IN TXT "v=DMARC1; p=reject"  ← enforced DMARC policy
```

  - jp ドメイン名で設定されているMXレコードの 0.03% が Null MX
  - Null MX の 48.8% のSPFレコードが “v=spf1 –all” ← ドメイン名の詐称防御
  - fail SPF の 55.1% のDMARCレコードが “v=DMARC1; p=reject” ← 受信拒否可
- エラーとなる SPF レコードに注意
  - チェックサイト等を利用して設定内容，フォーマットの確認を

送信ドメイン認証技術の応用

信頼できるメールの表示方法

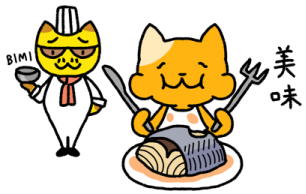
- Yahoo!メール (DKIM)
  - ブランドアイコン表示
  - Yahoo!メールアプリによるブランドカラー表示

Y!

- ドコモメール (SPF)
  - 公式アカウントマーク

公式アカウントマーク

- BIMI (DMARC)
  - Brand Indicators for Message Identification
  - Google: Advancing email security for Gmail and beyond with BIMI



ナリタイ <naritai.jp>

https://cloud.google.com/blog/products/identity-security/bringing-bimi-to-gmail-in-google-workspace

JPAAWG

BIMI

Brand Indicators for Message Identification

- 標準化動向
  - Internet Draft (Active): draft-blank-ietf-bimi-02 & related documents
- 仕組み
  - 送信側 (ドメイン管理者)
    - DMARCを完全に実装 (enforcement policy)，BIMI(Assertion)レコードをDNS上に公開(TXT RR)

default._bimi.example.jp IN TXT “v=BIMI1; l=https://image.example.jp/bimi/logo/example-bimi.svg”

    - 形式的には <selector>._bimi.<domain> の TXT 資源レコード
    - <selector> のデフォルト値は “default”，変更する場合は BIMI-Selector: ヘッダに記載

BIMI-Selector: v=DMARC1; s=myselector;

  - 受信側
    - DMARC 認証を実施，DMARC policy などを確認
    - BIMI レコードを取得し Indicator を取得 (場合によっては evidence document を検証)
    - 結果をメールヘッダに記述

Authentication-Results: serv-id; bimi=pass header.d=example.jp selector=default;
BIMI-Location: v=BIMI1; l=https://image.example.jp/bimi/logo/example-bimi.svg
BIMI-Indicator: PD94bW...8L3N2Zz4K

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 の正しい設定，できれば DKIM 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可能
- メールが悪用されない対策を
  - SPF, DKIM, DMARC を正しく設定する，メールに使わないドメイン名についても
  - 認証結果と認証ドメインを評価 (確認) する
- 受信したメールの結果をわかりやすく提示
  - 類似サービスは是非 BIMI に移行していきましょう
  - BIMI の今後の動向を把握しましょう

議論のポイント

- DMARC が日本で普及しない理由 (続)
- DMARC の policy に沿った受信処理は可能か
- 正しい送信ドメイン認証 (処理手順) の確認方法，認証結果の利用方法など
- BIMI は普及していくか