これからのメールセキュリティ

Internet Week 2020

2020.10.08

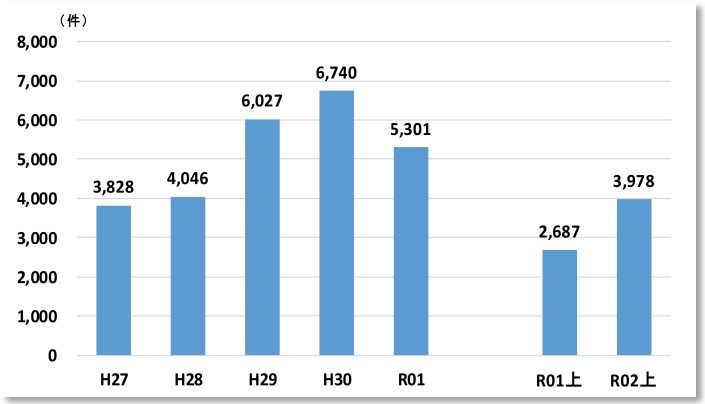
Shuji SAKURABA

JPAAWG / Internet Association Japan /

Internet Initiative Japan Inc.

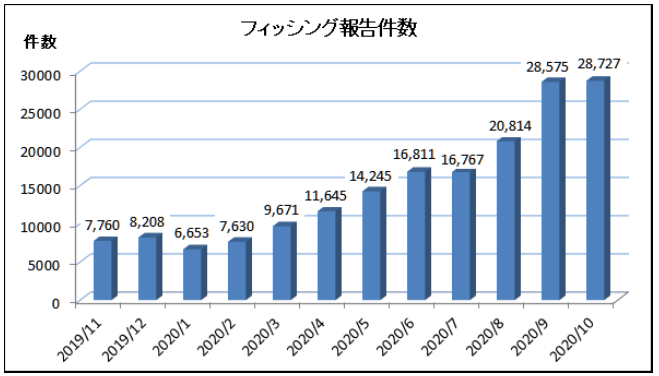
最近の迷惑メール状況

- 令和2年上半期におけるサイバー空間をめぐる脅威の情勢等について *(2020.10.01 警察庁)*
  - 令和2年上半期にサイバーインテリジェンス情報共有ネットワークを通じて把握した標的型メール攻撃の件数は3,978件
  - 送信元メールアドレスが偽装されていると考えられるものが全体の98%



https://www.npa.go.jp/publications/statistics/cybersecurity/data/R02_kami_cyber_jousei.pdf

- フィッシング報告件数 *(2020.11.04 フィッシング対策協議会)*
  - 2020年10月にフィッシング対策協議会に寄せられたフィッシング報告件数（海外含む）は、前月より152 件増加し、28,727 件



https://www.antiphishing.jp/report/monthly/202010.html

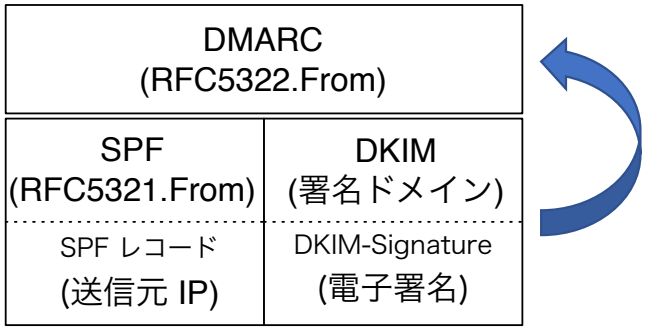
送信ドメイン認証技術

- 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 (smtp.mailfrom)
  - DKIM (DomainKeys Identified Mail): 署名ドメイン
  - DMARC (Domain-based Message Authentication, Reporting, and Conformance): RFC5322.From ドメイン (ヘッダ From)

	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

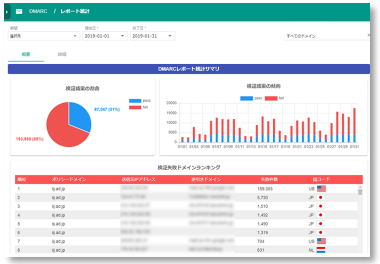
DMARC の特徴

- 認証方式
  - SPF and/or DKIM で認証されたドメインと RFC5322.From (ヘッダ 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を 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) での設定
    - サブドメインまで影響させることが可能



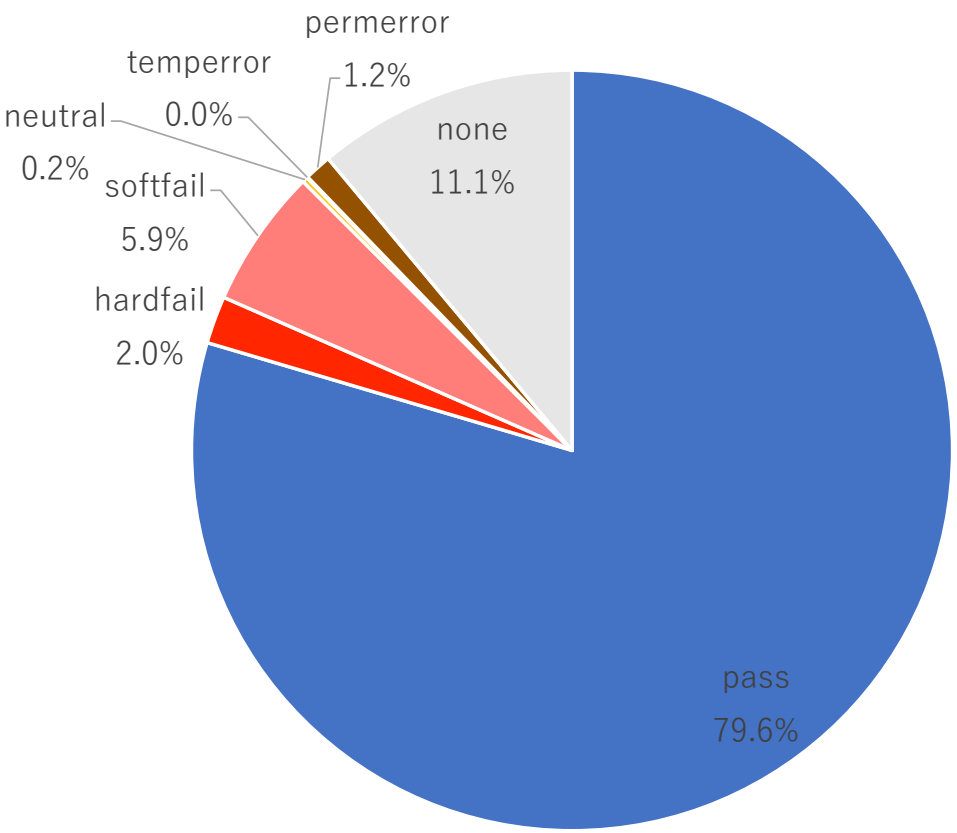
DMARC レコードの設定例:

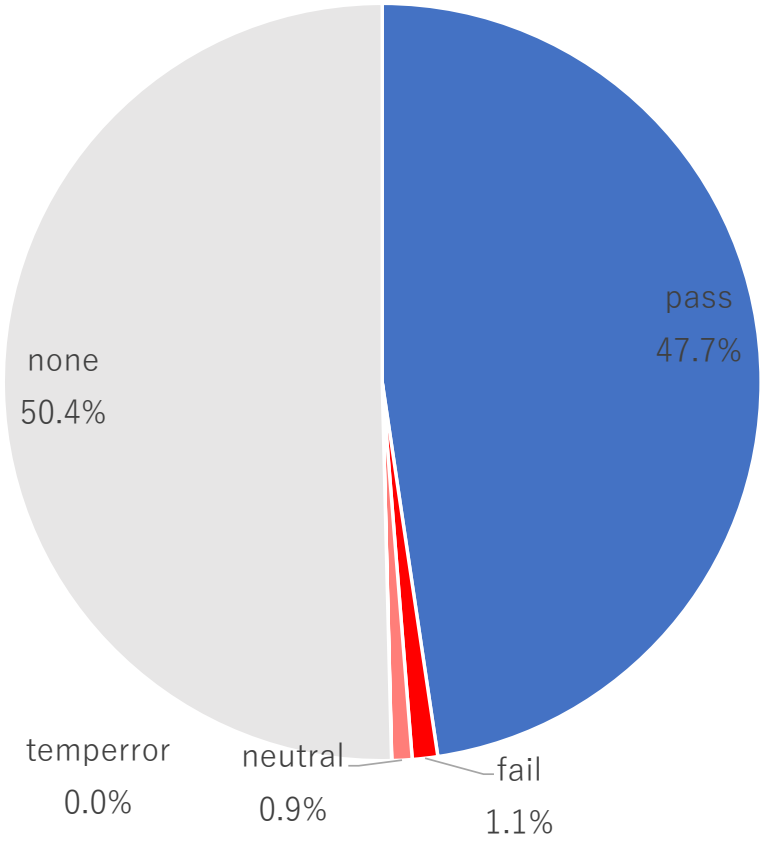
_dmarc.example.jp IN TXT "v=DMARC1; p=none"



SPF/DKIM 認証結果割合

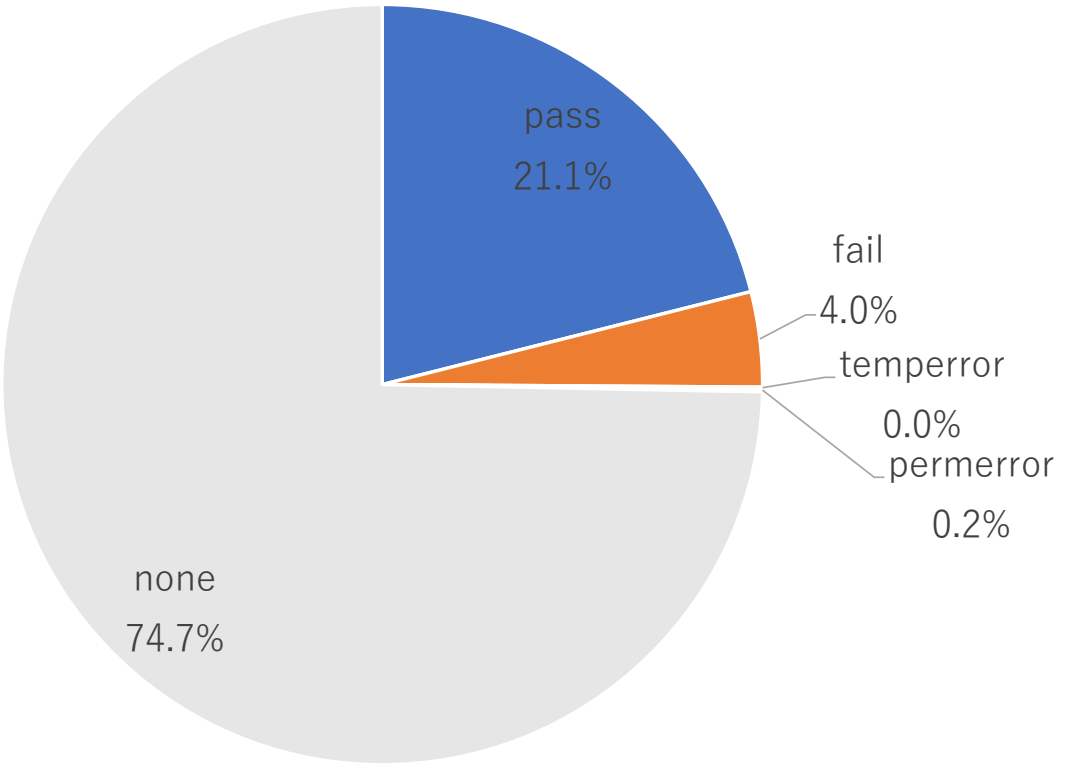
2020.10 IIJ 受信メール

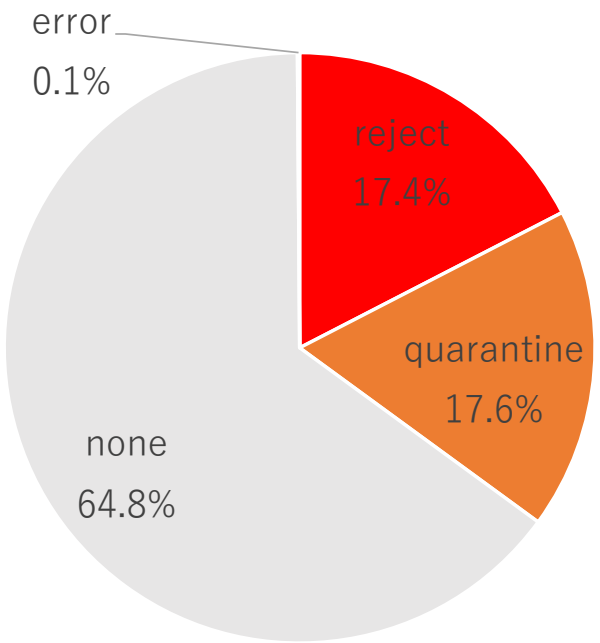




DMARC 認証結果割合

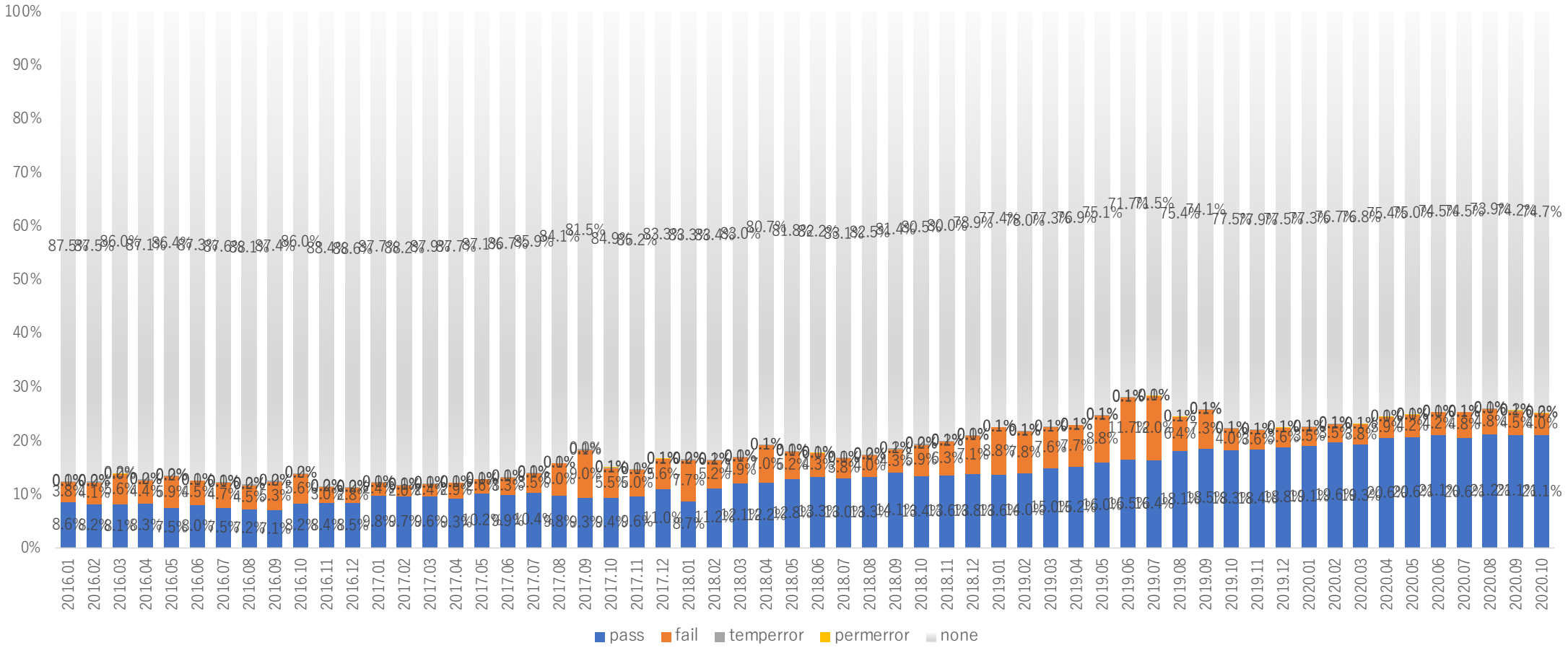
2020.09 IIJ 受信メール





DMARC 認証結果割合の推移

2016.06 – 2020.10 IIJ 受信メール



送信ドメイン認証技術の普及状況

JP ドメイン (JPRS と IAjapan の共同研究) 2020.11.16

全体に対する MX レコード宣言率: 80.72% (1279284 / 1584745)
MXドメインに対する SPF レコード宣言率: 65.73% (840814 / 1279284)
MXドメインに対する DMARC レコード宣言率: 1.58% (20164 / 1279284)

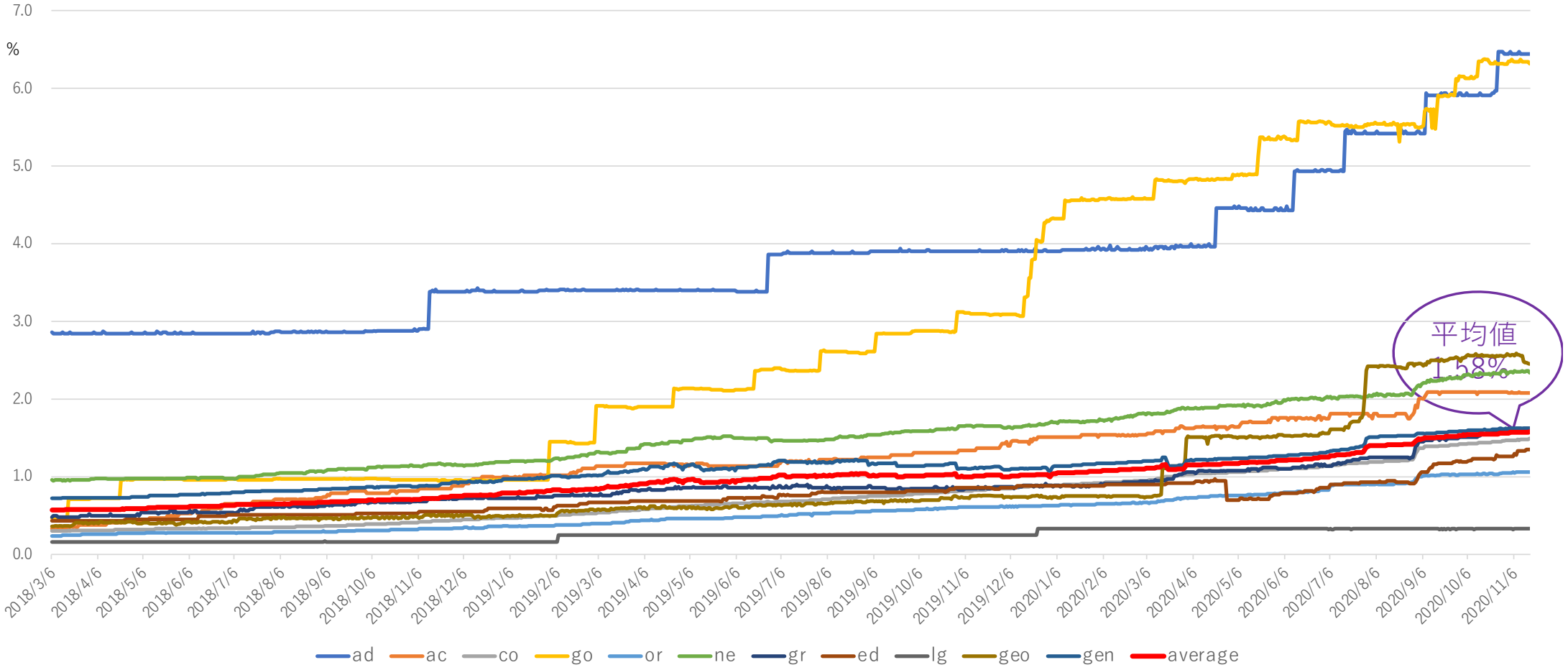
登録型	MX (%)	SPF (%)	DMARC (%)
AD	81.1	72.3	6.4
AC	94.6	71.9	2.1
CO	93.9	74.7	1.5
GO	70.2	92.5	6.3
OR	93.6	73.4	1.1
NE	81.4	61.9	2.3
GR	88.9	63.5	1.6
ED	89.9	70.6	1.4
LG	73.7	81.2	0.3
地域型*1	62.7	60.4	2.5
汎用	74.9	60.8	1.6

JPRS: (株)日本レジストリサービス
(Japan Registry Service)
IAjapan: (一財)インターネット協会
(Internet Association Japan)

*1 地域型は新規受付停止
数値は都道府県型を含む

DMARC の設定割合の推移

JP ドメイン (JPRS と IAjapan の共同研究) 2018.03 – 2020.11



送信ドメイン認証技術の普及状況

自治体ドメイン 2020.11.17

全国での SPF レコード宣言率: 84.2% (1505 / 1788)
全国での DMARC レコード宣言率: 0.7% (13 / 1788)

	SPF (%)	DMARC (%)
北海道	75.0 (135/180)	1.7 (3/180)
東北	85.8 (200/233)	0.4 (1/233)
関東	88.2 (285/323)	1.6 (5/323)
中部	80.6 (262/325)	0.3 (1/325)

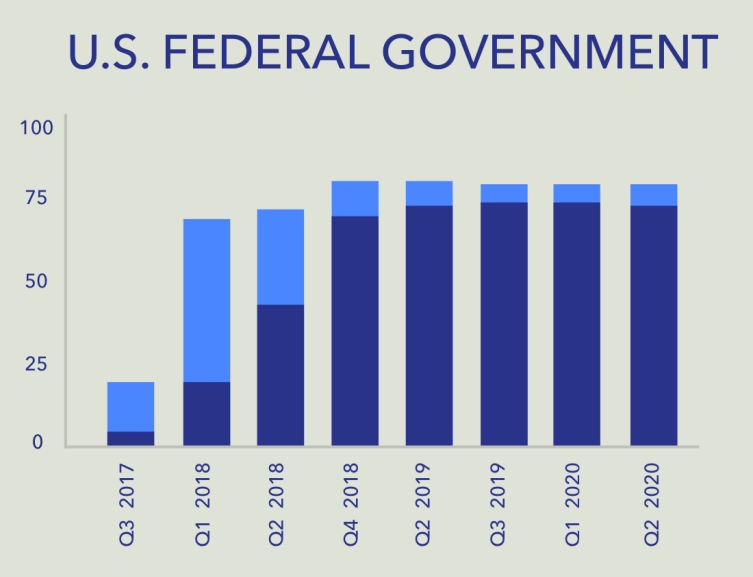
	SPF (%)	DMARC (%)
近畿	88.5 (207/234)	0.4 (1/234)
中国	78.6 (88/112)	0.0 (0/112)
四国	83.8 (83/99)	1.0 (1/99)
九州沖縄	86.9 (245/282)	0.4 (1/282)

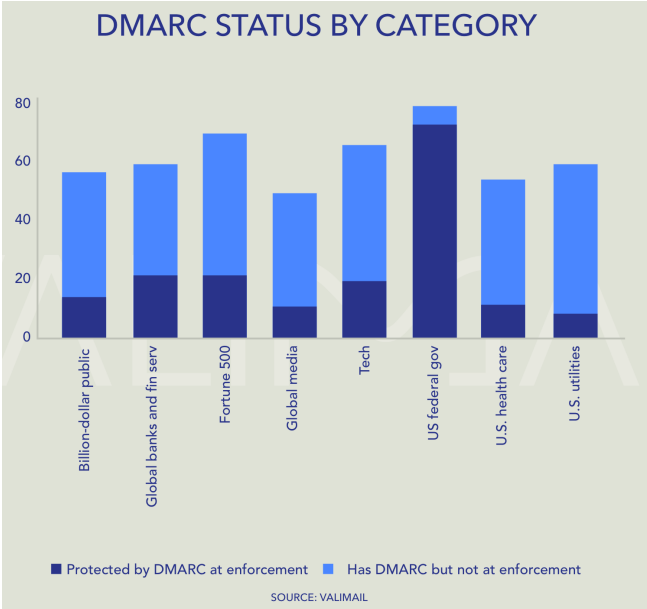
* ドメイン名は独自調査，全ての対象ドメインに MX レコードが設定されていることを確認済み

米国の DMARC 普及率

- 政府機関の取り組み
  - BOD 18-01 by Department of Homeland Security (DHS) (Oct.16 2017)
    - A. Email Security
      - STARTTLS
      - Email Authentication
        - All second-level agency domains to have valid SPF/DMARC records, with at minimum a DMARC policy of “p=none” and at least one address defined as a recipient of aggregate and/or failure reports. (within 90 days)
        - setting a DMARC policy of “reject” for all second-level domains and mail-sending hosts. (within one year after)

https://cyber.dhs.gov/bod/18-01/

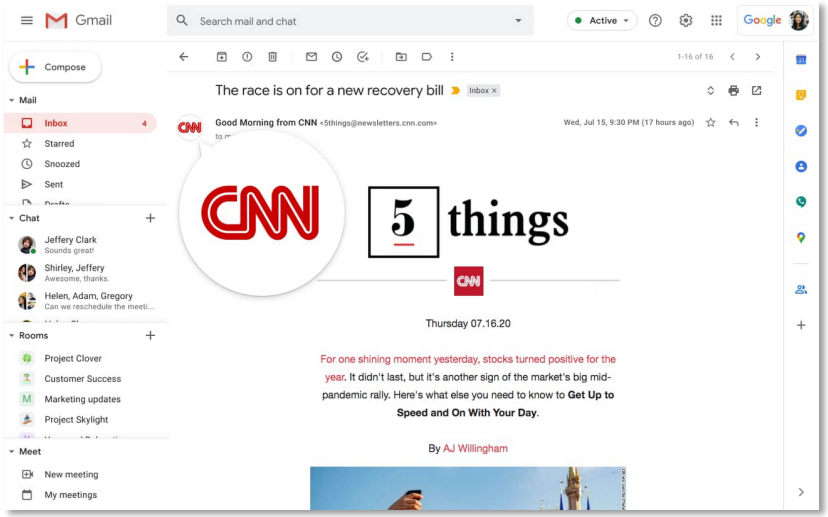




Email fraud landscape, Summer 2020
by Valimail

DMARC の応用
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)
  - BIMI レコード設定ドメイン数 (default 位置)
    - 受信メールの DMARC 対応ドメイン: 632
    - JP ドメイン名: 26
  - 標準化動向
    - I-D (draft-blank-ietf-bimi-01)



https://cloud.google.com/blog/products/g-suite/gsuite-security-updates-for-gmail-meet-chat-and-admin

BIMI Assertion レコードの設定例:

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

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.jp.              IN MX 0 .
example.jp.              IN TXT “v=spf1 –all”
_dmarc.example.jp.       IN TXT “v=DMARC1; p=reject”
```

  - 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 34.8% のSPFレコードが “v=spf1; – all”
- 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の確認を

送信ドメイン認証技術のまとめ

- DMARC の導入のすすめ
  - 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 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
  - 送信側ドメインが SPF + DMARC (DNS TXT レコードに記述するだけ) でも技術的には DMARC 認証可能
- なりすましメール対策
  - 現時点では認証結果と認証ドメイン名を参照すれば詐称メールが判別可能
  - ドメインレピュテーション (評価) による紛らわしいドメイン名の対策も
  - なりすまされないための設定も必要 (メールに利用しないドメインについても)
- 技術的な注意点
  - メール転送されるメールを送信する場合は DKIM の導入を推奨
  - DKIM の署名ドメインに注意 (ヘッダ From と同じ or 上位ドメインを利用)
  - クラウド型メールサービスの DKIM 署名に注意 (CNAME 等で自ドメイン署名に)