これからのメールセキュリティ

Internet Week Show Case Online 2021

2021.07.09

Shuji SAKURABA

JPAAWG / Internet Association Japan /

Internet Initiative Japan Inc.

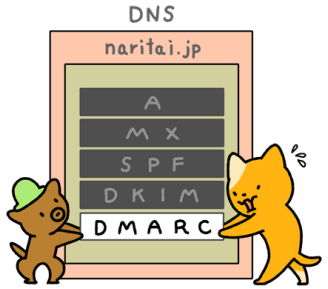
最近の迷惑メール関連情報

- Internet Crime Report 2020 (FBI IC3, Internet Crime Complaint Center)
  - 2020年に報告された苦情は 791,790 件
  - そのうち BEC (Business Email Compromise) は 19,369件 (2.4%)，被害額は $1.8 billion (1,980億円) 以上
  - フィシング詐欺は 241,342件 (30.5%)，被害額は $54 million (59.4億円)以上
  - ランサムウェアは 2,474件，被害額は $29.1 million (32億円) 以上
- 令和2年におけるサイバー空間をめぐる脅威の情勢等について (警察庁, 令和3年3月4日)
  - インターネットバンキングにかかる不正送金被害は 1,734件 (92.6%)，被害額が 11.3億円 (44.9%)，SMS や電子メールを用いて金融機関を装ったフィッシングサイトへ誘導する手口
  - 不正アクセス禁止法の違反件数は 609件，そのうち識別符号窃用型が 576件 (94.6%)，手口としてフィッシングサイトによる入手が 172件 (29.9%)

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)

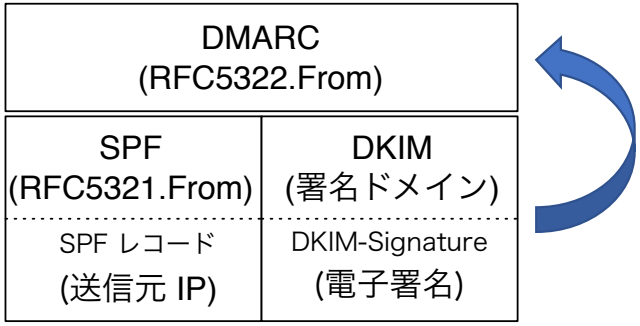
	SPF	DKIM	DMARC
名称	Sender Policy Framework RFC 7208	DomainKeys Identified Mail STD 76, RFC 6376	Domain-based Message Authentication, Reporting, and Conformance RFC 7489
特徴	送信元をネットワーク的に判断 （送信元のIPアドレスにより確認）	送信時に電子署名をメールに付加 （電子署名の検証により判断）	SPFあるいはDKIMの認証結果を利用 （送信側でポリシーを設定、認証結果のレポート機能）
導入コスト	送信側はほぼ皆無（DNSの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

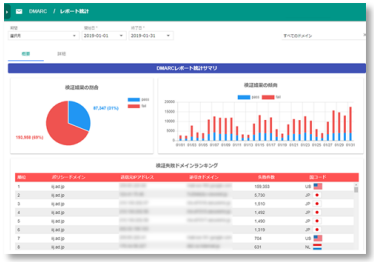


ナリタイ <naritai.jp>

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



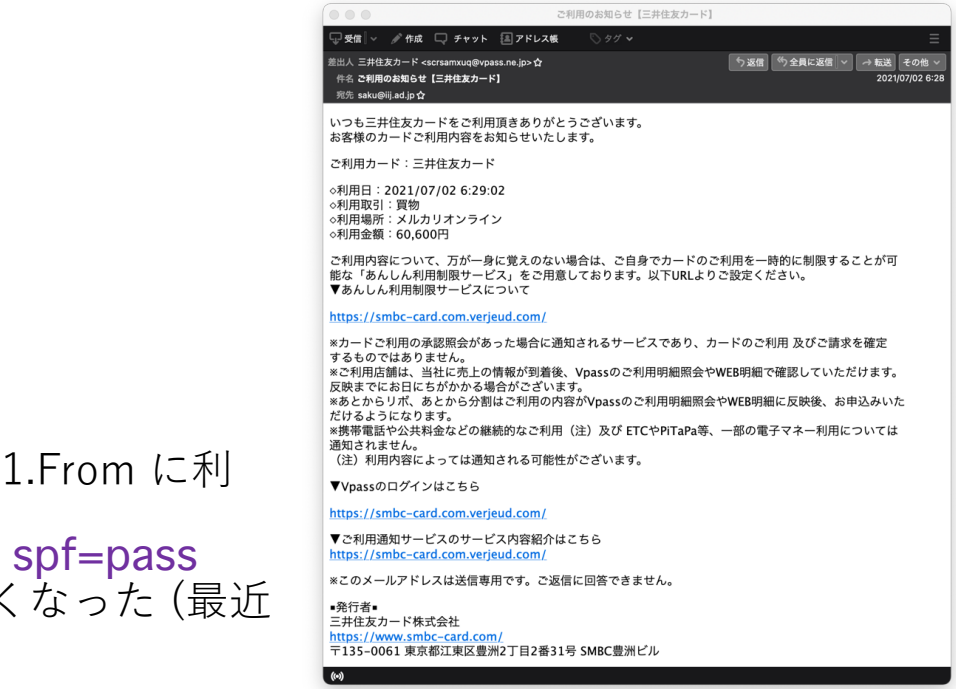


DMARC レコードの設定例:

_dmarc.example.jp IN TXT "v=DMARC1; p=reject; rua=mailto:r@example.jp"

フィシングと DMARC

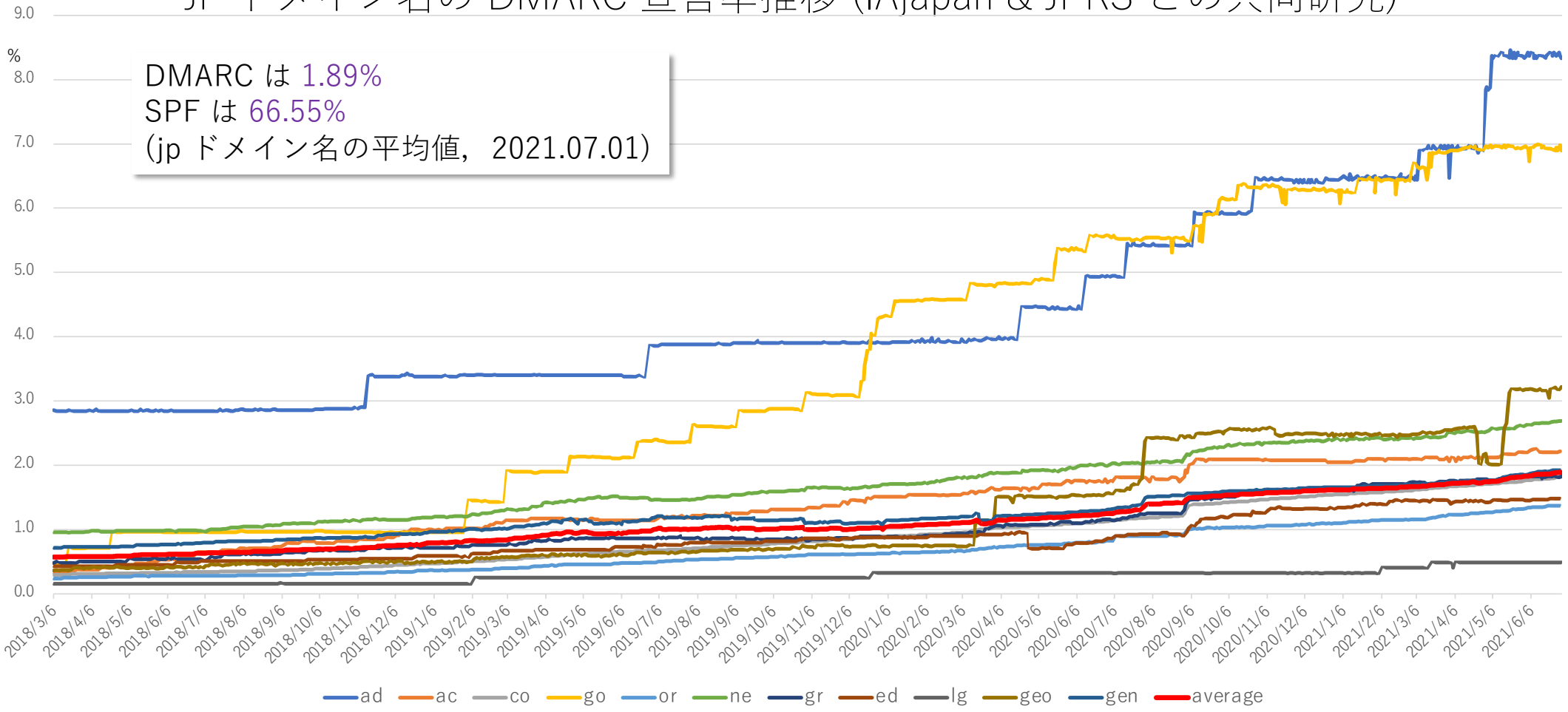
- SPF なりすましのパターン
  - RFC5321.From を堂々となりすます, spf=softfail/fail/neutral
  - SPF が設定されていないドメイン名を RFC5321.From に利用, spf=none
  - 無関係なドメイン名を RFC5321.From に利用, spf=pass
  - どこからでも pass するドメイン名の利用は無くなった (最近の傾向)
- DMARC の状況
  - 多くは DMARC レコードが設定されていない, dmarc=none
  - 不正な RFC5322.From を利用 (ドメイン名のみ), dmarc=none
  - 無関係なドメイン名を RFC5322.From に利用, dmarc=pass (display-name にはそれらしい名称を利用)
  - 存在しないドメイン名を RFC5322.From に利用, dmarc=none (cousin domain 名などを利用)



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)



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)

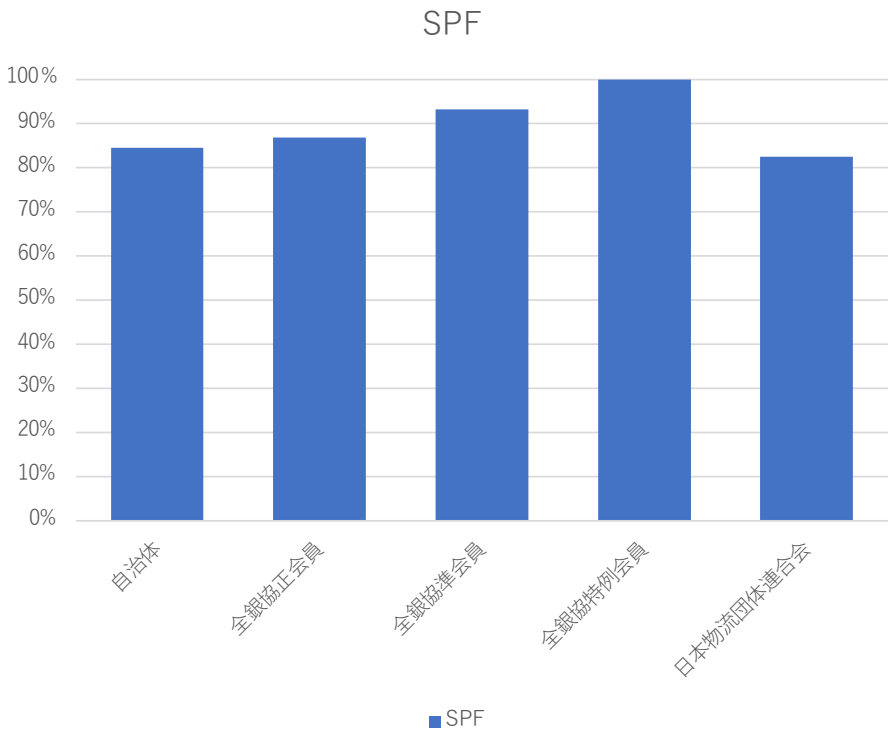
	SPF*2 (%)	DMARC*2 (%)
北海道	76.7 (138/180)	1.7 (3/180)
東北	86.7 (202/233)	0.4 (1/233)
関東	88.5 (286/323)	1.9 (6/323)
中部	81.2 (264/325)	0.6 (2/325)

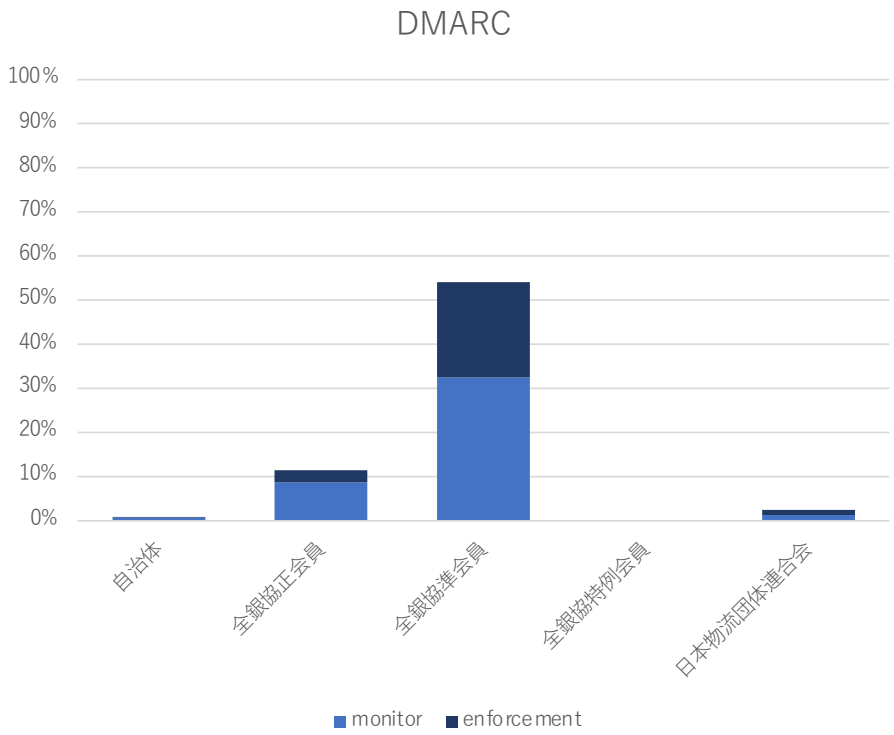
	SPF*2 (%)	DMARC*2 (%)
近畿	88.5 (207/234)	0.4 (1/234)
中国	78.6 (88/112)	0.0 (0/112)
四国	83.8 (83/99)	2.0 (2/99)
九州沖縄	86.9 (245/282)	0.4 (1/283)

* 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

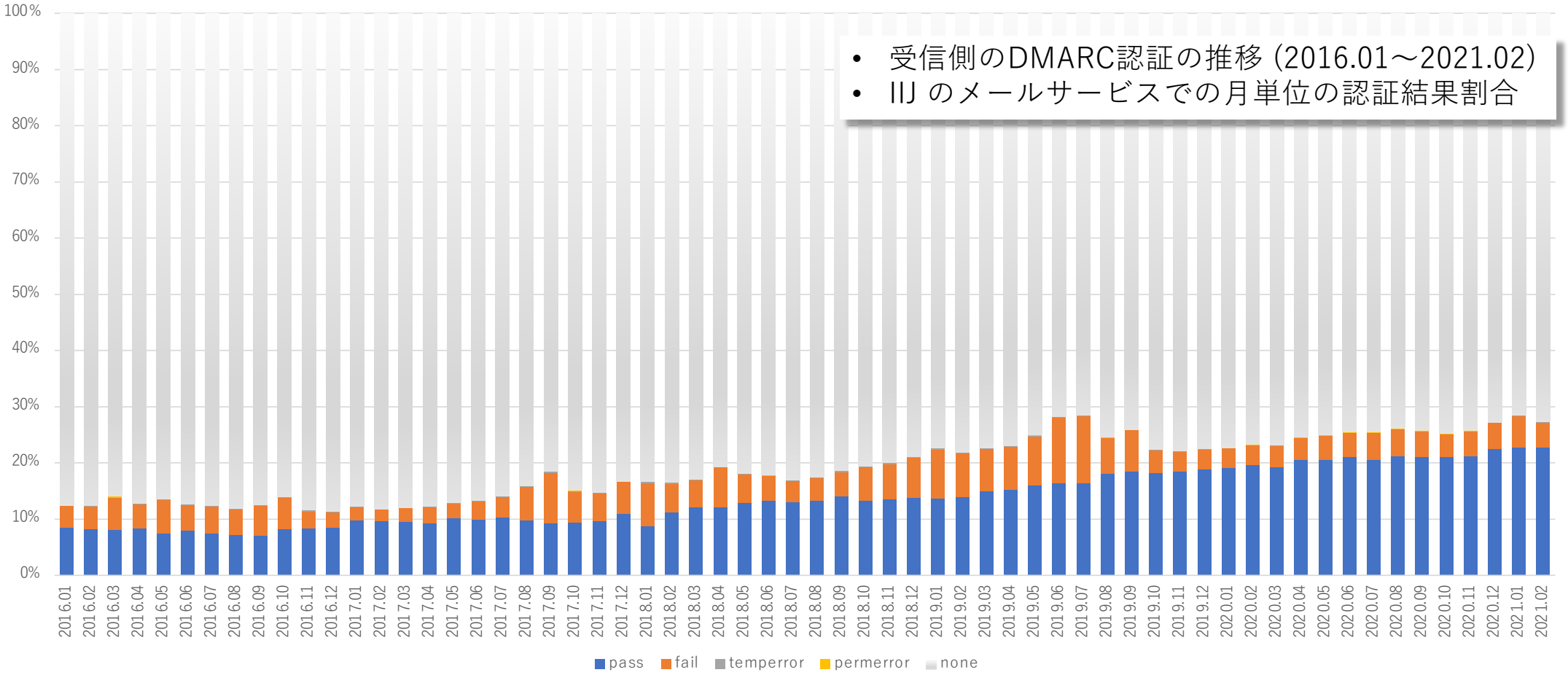
業界団体の調査(ドメイン名は独自調査, 2021.07.01)





DMARC の認証結果割合の推移

transition of DMARC authentication results rate



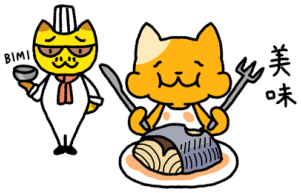
- 受信側のDMARC認証の推移 (2016.01～2021.02)
- IIJ のメールサービスでの月単位の認証結果割合

DMARC の応用

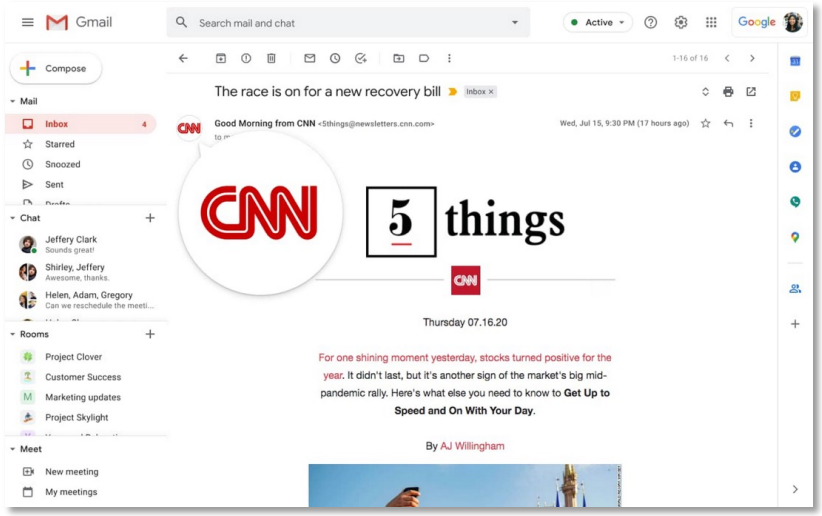
信頼できるメールの表示方法

- Yahoo!メール
  - 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
- ドコモメール
  - 公式アカウントマーク
- BIMI
  - 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
  - 標準化動向
    - I-D (draft-blank-ietf-bimi-02)

公式アカウントマーク



ナリタイ <naritai.jp>



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.com IN TXT "v=BIMI1; l=https://image.example.com/bimi/logo/example-bimi.svg"

送信ドメイン認証技術の応用

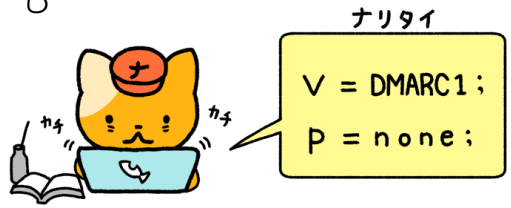
- メールに利用しないドメイン名の設定
  - ドメイン名が DNS 参照できるだけで悪用される恐れあり (親ドメイン等)
  - メールに利用しないことを示す設定方法 (Null MX および SPF, DMARC)

```
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 48.8% のSPFレコードが “v=spf1; –all”
  - 上記の 55.1% の DMARC レコードが “v=DMARC1; p=reject”
- エラーとなる SPF レコードに注意
  - 複数の SPF レコードの設定 (“v=spf1” で始まる TXT RR が複数存在)
  - include 先の SPF レコードが参照できない, etc
  - 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，できれば DKIM も導入を
- 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 同じ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)
  - DKIM の普及が十分でない状況を考えると ARC の普及はまだ難しいかも
  - せめて設定した SPF レコードの確認を忘れずに



ナリタイ <naritai.jp>