2025年フィッシングの動向と対策&
最新メールセキュリティ

JANOG 56 Meeting in Matsue

2025.07.30

SAKURABA Shuji

Agenda

- 送信ドメイン認証技術の導入状況
  - DMARCの普及状況調査
  - 地方自治体の普及状況調査
- 技術仕様動向
  - DMARCの仕様改定
  - BIMI
  - DKIM2

DMARCの普及状況調査

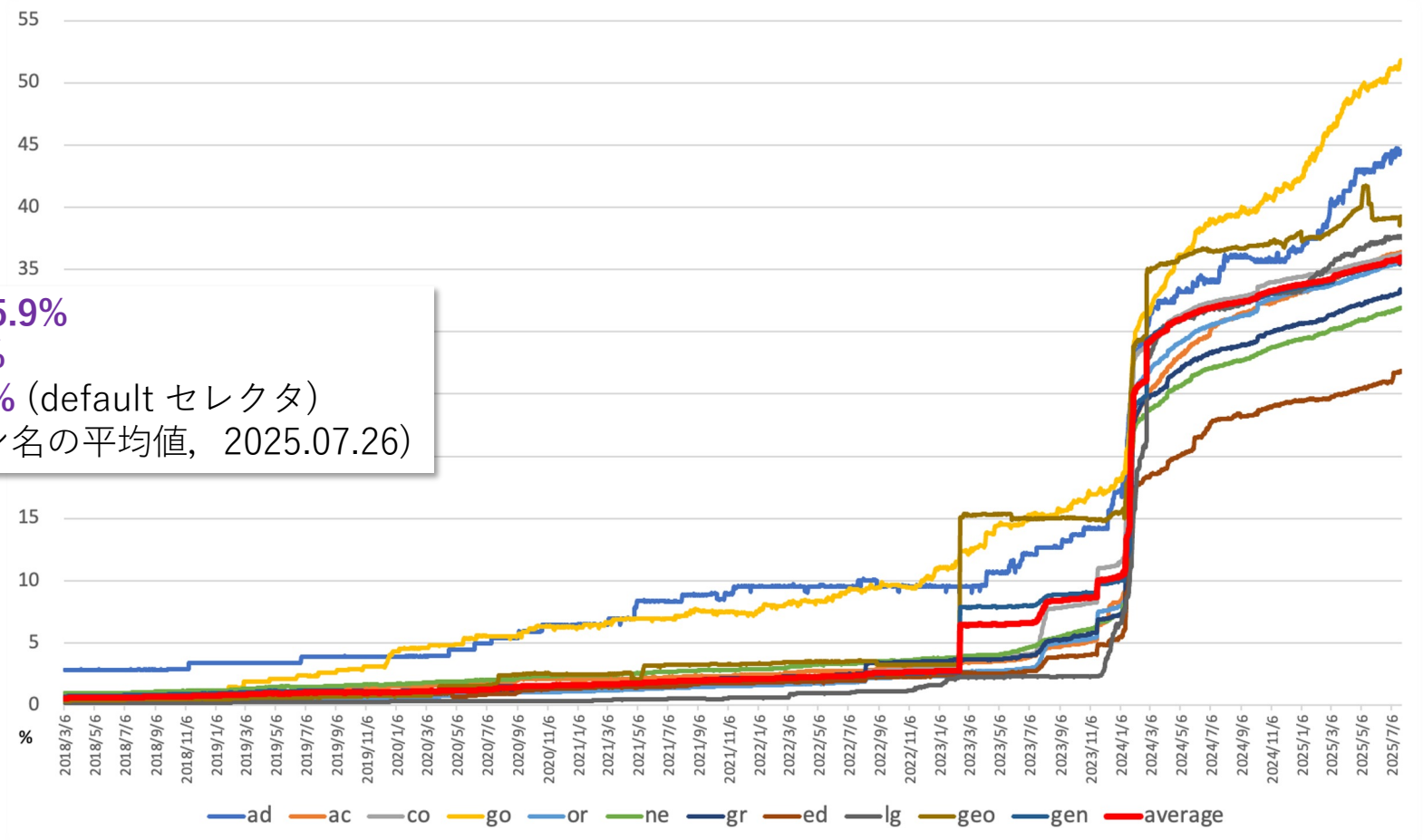
- JPドメイン名の調査
  - JPRS (Japan Registry Services) と IAjapan (インターネット協会) の共同研究契約[*1]に基づいて実施 (2018.03.16～現在)
  - 調査結果は総務省の Web Site で定期的に更新され公開中

    https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei
  - 登録JPドメイン名に対して，MXレコードが設定されている場合，SPFレコードやDMARCレコード，関連技術の設定状況を継続調査
  - DKIM鍵レコードの調査は，セレクタ名が必要[*2]となるため，存在可能性[*3]のみを参考調査 (非公開)

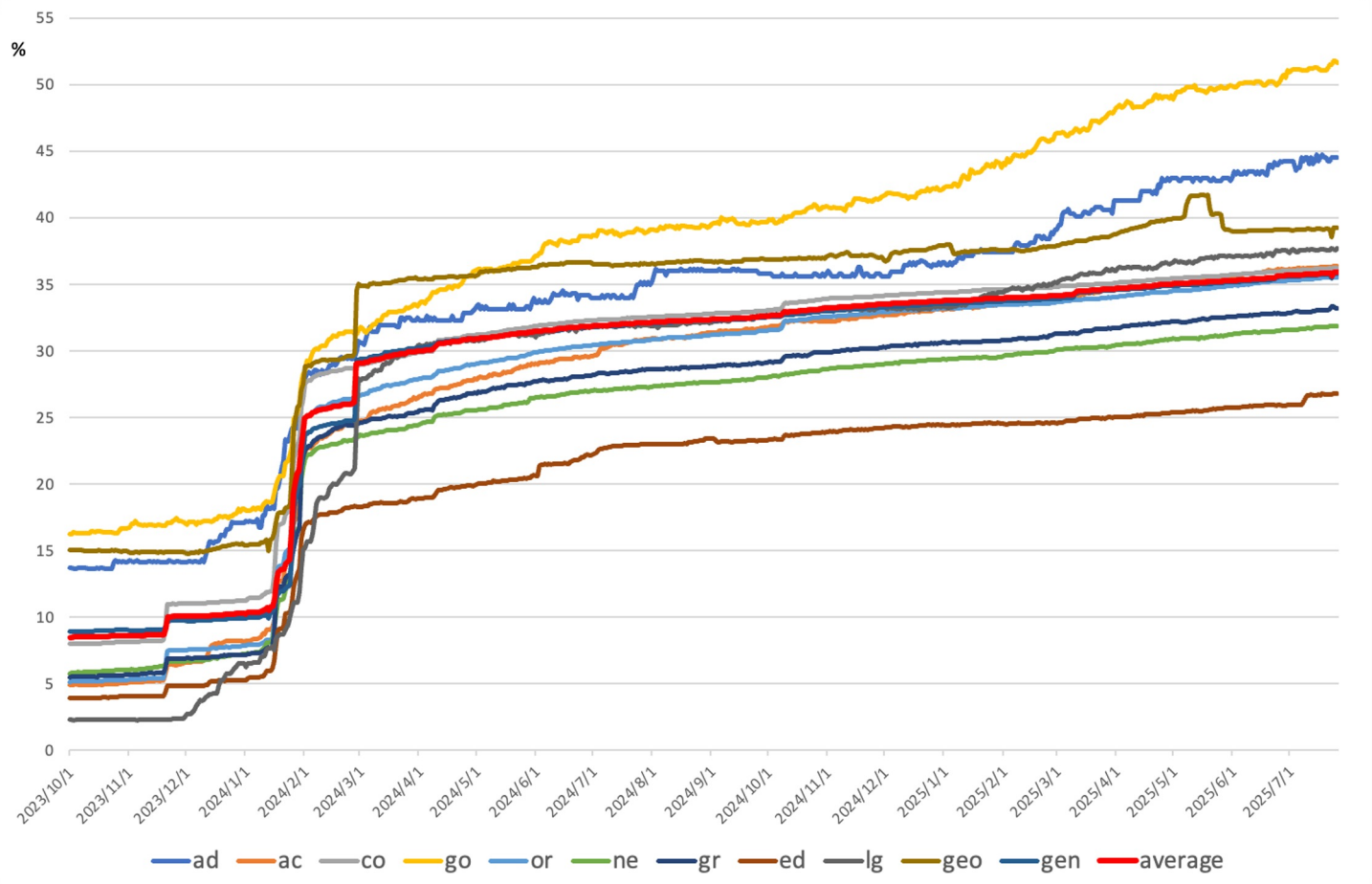
*1 2018年度～2019年度までは(一財)日本データ通信協会との共同研究契約として実施
*2 DKIM-Signature: ヘッダに記載されている
*3 http://member.wide.ad.jp/wg/antispam/stats/measure.html.ja
https://eng-blog.iij.ad.jp/archives/1234

DMARCの普及状況調査 (2018.03.18〜)

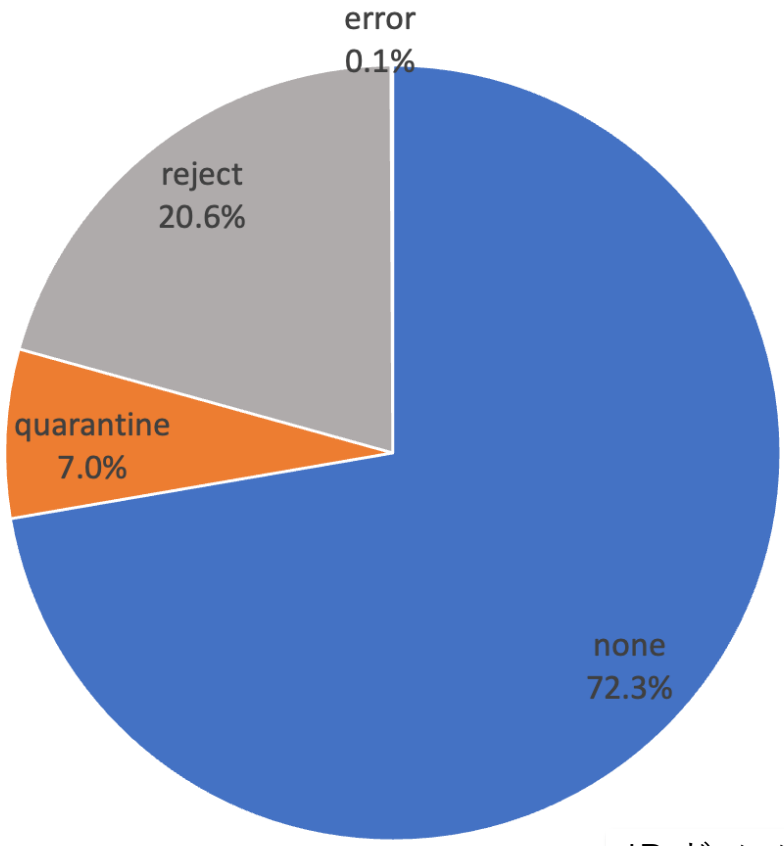
DMARC : **35.9%**
SPF : **89.4%**
BIMI : **0.03%** (default セレクタ)
(JP ドメイン名の平均値，2025.07.26)



DMARCの普及状況調査 (2023.10.01～)

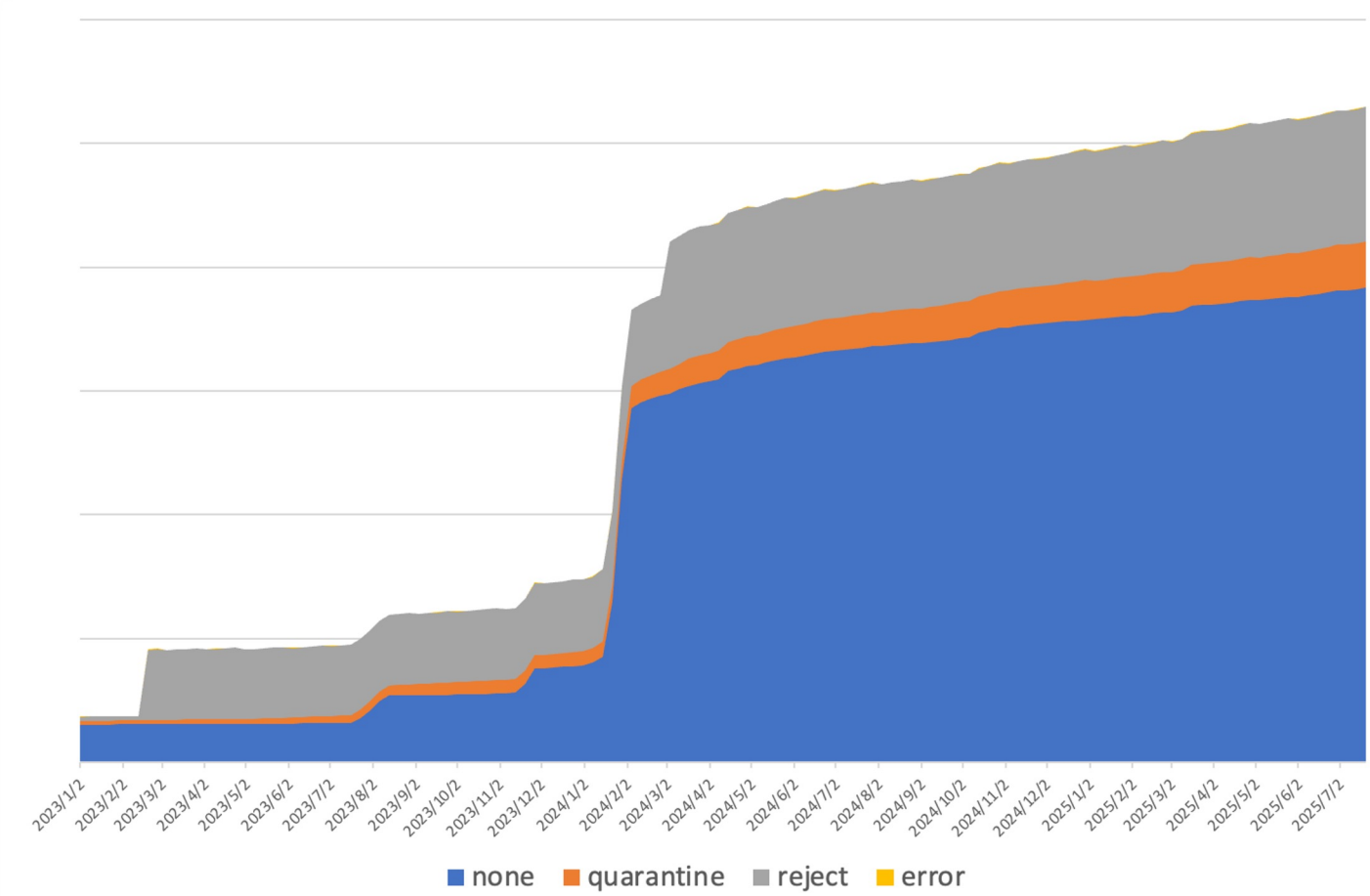


DMARCのpolicy設定状況調査



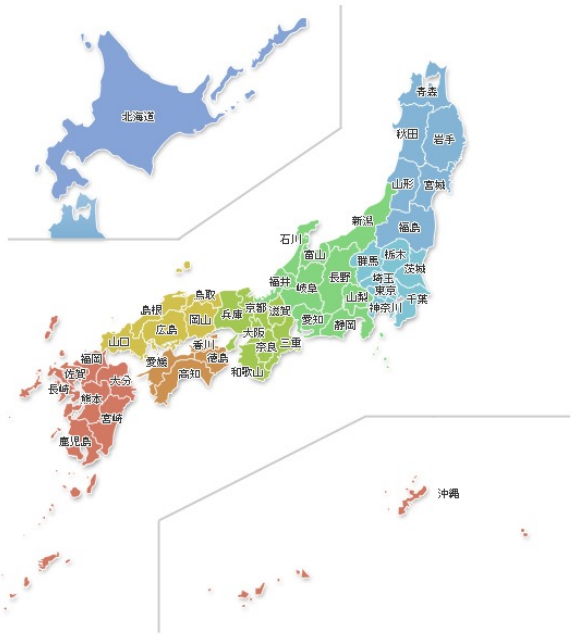
JP ドメメイン名の設定 policy，2025.07.26

DMARCのpolicy設定状況調査



地方自治体のSPF, DMARC設定状況

- 自治体ドメイン名の調査
  - 1,718 (市町村) + 23 (東京23区) + 47 (都道府県) = 1,788
  - JIPDEC 調査のドメイン名から独自調査を加えたドメイン名
  - 調査前に対象のドメイン名に MX レコードが設定されていることを確認済み
  - 調査は J-LIS (地方公共団体情報システム機構) による各自治体の Web サイト情報などを活用



地方自治体のSPF, DMARC設定状況
(2025.07.28)

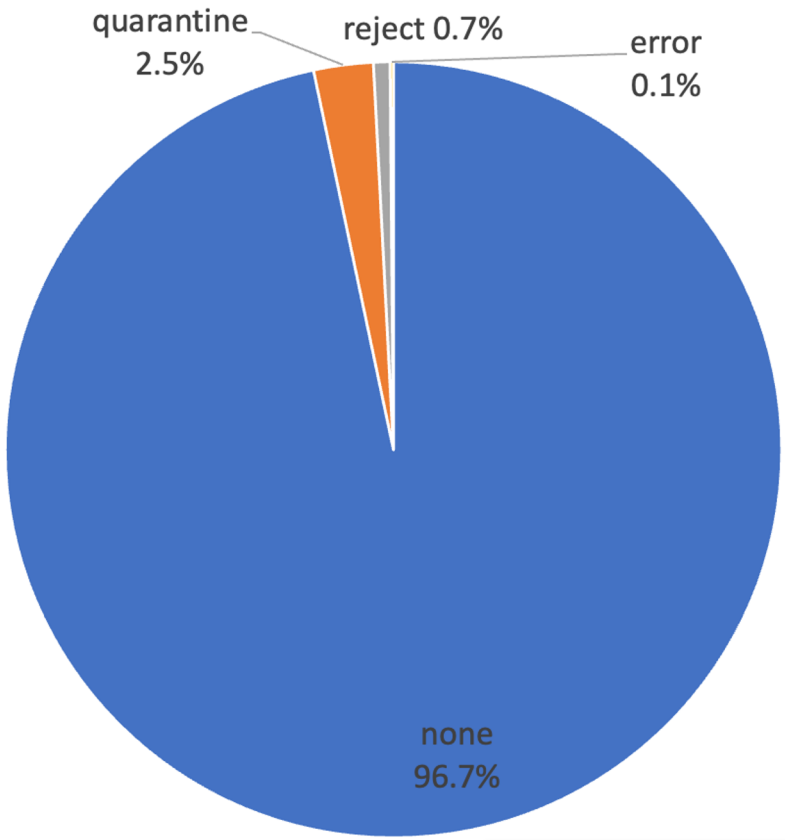
全国での SPF レコード宣言率: 99.8%
全国での DMARC レコード宣言率: 40.6%

	SPF* (%)	DMARC* (%)
北海道	100.0 [180/180]	100.0 [180/180]
東北	99.6 [232/233]	19.7 [46/233]
関東	100.0 [323/323]	57.0 [184/323]
中部	100.0 [325/325]	35.7 [116/325]

	SPF* (%)	DMARC* (%)
近畿	99.6 [233/234]	51.3 [120/234]
中国	99.1 [111/112]	20.5 [23/112]
四国	100.0 [99/99]	16.2 [16/99]
九州沖縄	100.0 [282/282]	14.5 [41/282]

- BIMI レコード設定ドメイン数は 0 (2025.07.28)

地方自治体のDMARC policy設定状況



地方自治体ドメメイン名の設定 policy，2025.07.28

DMARCの仕様改定

- 背景
  - DMARCの仕様 (RFC7489, 2015.03) が IETF (Internet Engineering Task Force) で改定作業が行われている
  - 目的は Informational カテゴリから Standard Track (標準化) へ
- 現在の状況
  - IETFでのDMARC WGは一旦close，しかしfailure reportの取り扱いが未定
  - aggregate report は別 RFC として発行予定
  - failure report については承認されていない，且つ本体に記述 (参照) が残っている状態
  - failure reportの取り扱いを決めるためだけに，再度DMARC WGを立ち上げ
    - failure report に関する Internet-Draft を完成させる
    - DMARCの仕様からfailure reportに関する記述を完全に削除
    - のいずれかを判断 (年内予定)

DMARCの仕様改定

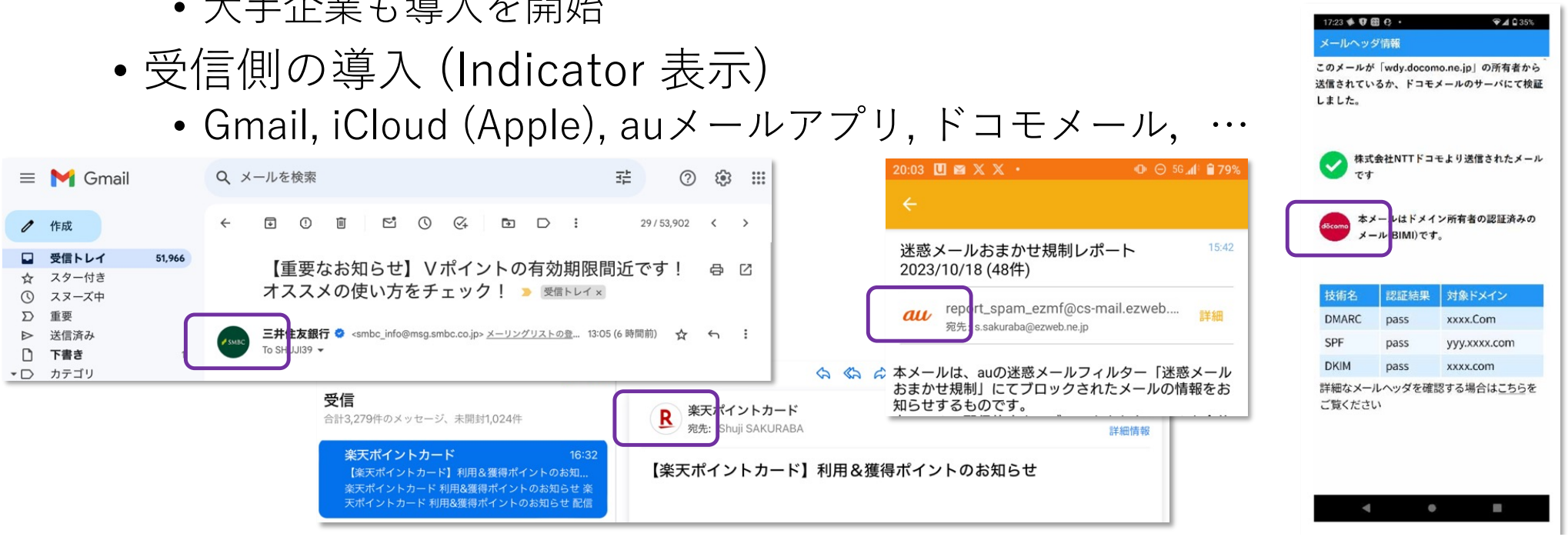
- 主な変更点
  - レポート (aggregate, failure) の仕様を分離 (別 I-D)
  - 組織ドメイン名の決定方法を Public Suffix List を利用する方式から DNS Tree Walk 方式へ変更
  - DNS レコードのパラメータの変更
    - 削除: **pct** (ポリシー適用割合), **rf** (failure report形式), **ri** (aggregate 送信間隔)
    - 追加: **np** (存在しないドメイン名のポリシ), **psd** (PSDかどうか), **t** (テストモード指定)
- DNS Tree Walk 方式
  - 送信者(著者)ドメイン名にDMARCレコードがあれば参照
  - 無い場合 (組織ドメイン名の探索方法)
    - ドメイン名のラベルが 8以上 → 7に縮退してDMARCレコードを参照
    - DMARC レコードが取得できるまで上位ドメイン名を参照 (最大 8回)

BIMI (Brand Indicators for Message Identification)

- 概要
  - DMARC 認証 (**p=quarantine** 以上) されたメールに対して，ロゴ (Brand Identification) を表示する仕組み
  - VMC (Verified Mark Certificate) は MVA (Mark Verifying Authority) が発行した MC (Mark Certificate)
  - メール受信側は VMC を検証してロゴを表示
  - 仕様はまだ Internet Draft 段階
- 普及状況
  - 証明書やロゴの情報は DNS 上に設定
  - DKIM と同様にセレクタによって場所を変えられる
  - デフォルトセレクタが決められている (**default**)
  - jp ドメイン名の 0.03% が BIMI レコードを設定

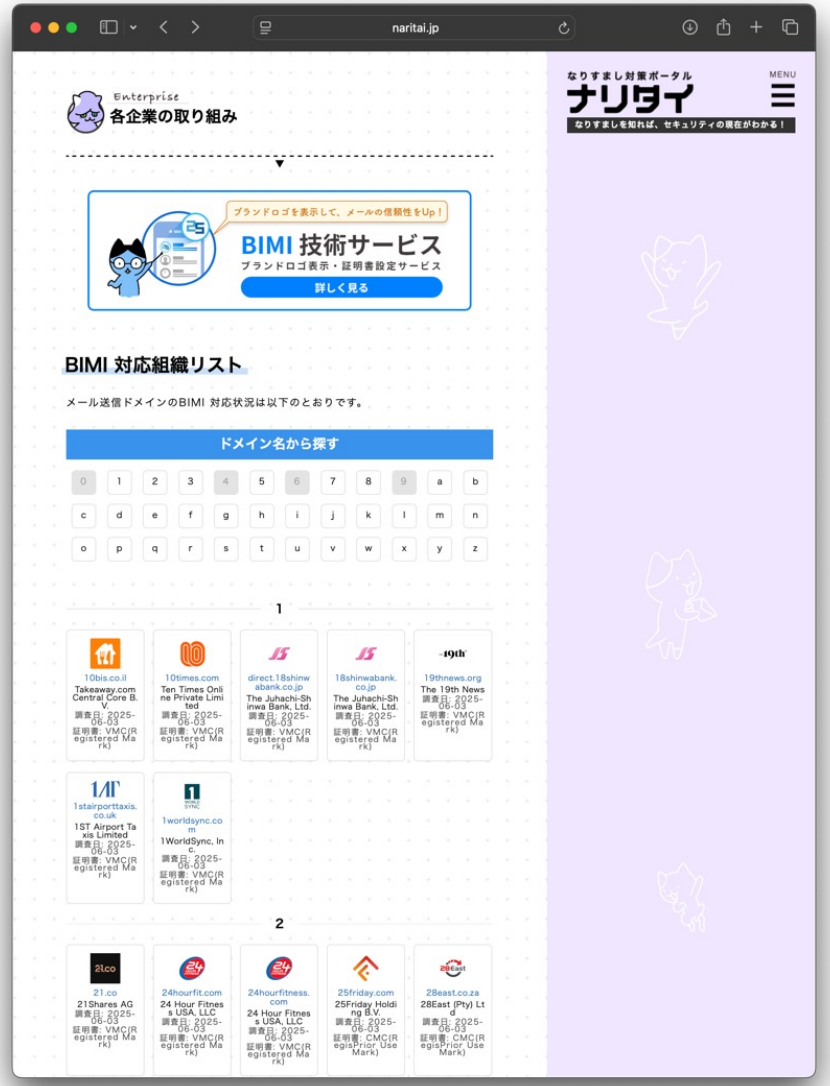
BIMI (Brand Indicators for Message Identification)

- 送信側の導入
  - jp ドメイン名の 0.03% に BIMI Assertion Record が設定 (default)
  - 大手企業も導入を開始
- 受信側の導入 (Indicator 表示)
  - Gmail, iCloud (Apple), auメールアプリ, ドコモメール, …

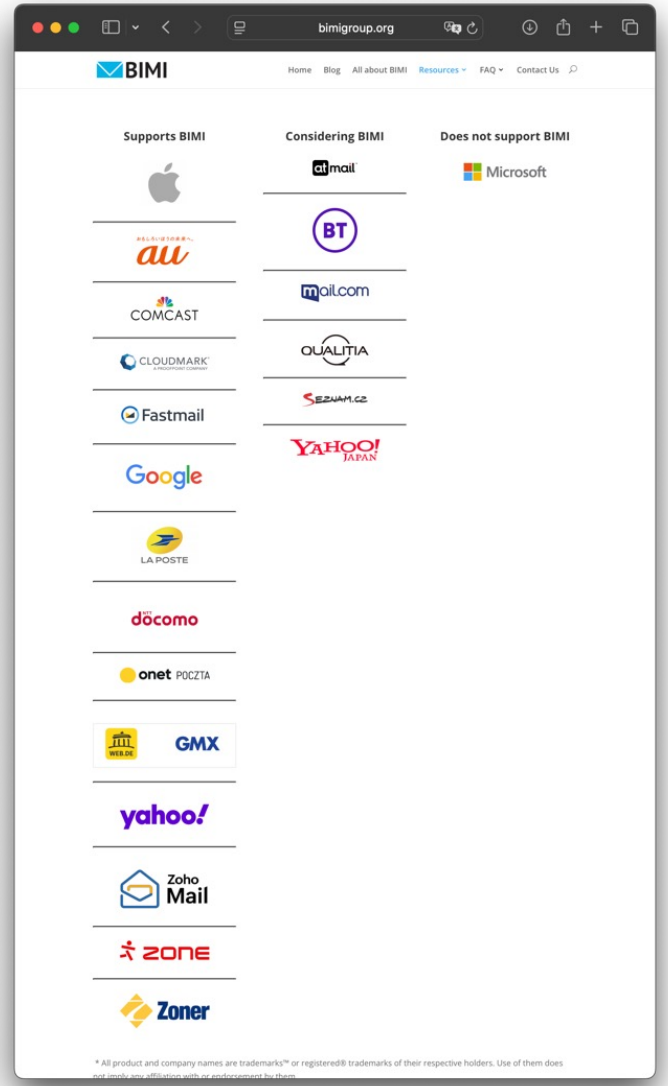


BIMI

- 普及状況



https://www.naritai.jp/enterprise_bimilist.html



https://bimigroup.org/bimi-infographic/

DKIM2

- 状況
  - IETF 122 meeting (2025.03) で最初の meeting,　I-D は 2024.10 から
  - Fastmail, Yahoo, Google が提案
- 送信ドメイン認証に関わる課題の解決を目指している
  - DKIM replay 攻撃
    - 正しく署名されたメールを再利用可能 (Bcc などを装う)
    - DKIM2 ではタイムスタンプを記載，宛先を 1つに限定して宛先アドレスを記載
  - バックスキャッター問題
    - エラーメールが詐称された第三者に送信されてしまう問題
    - バウンスアドレスを署名ドメインと一致させ，署名対象情報とする
    - これにより転送メールのエラーメール送信先も適切なものとなる
  - 暗号関連問題
    - RSA と楕円曲線暗号 (EC) が仕様化されているが，EC がほぼ使われていない
    - 耐量子計算機暗号 (PQC) 方式への対応
    - 現状は記載されている全ての DKIM 署名の検証が必要なため，計算負荷が発生するが，DKIM2 ではこれを削減