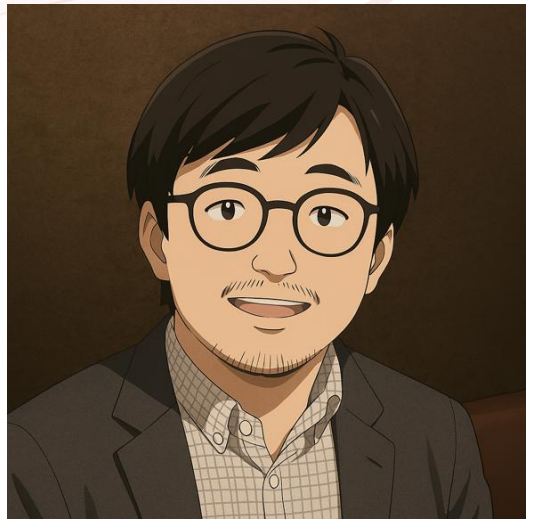
メールサービスの運用・開発こぼれ話。権威の盲信には気をつけよう。

JPAAWG 8th General Meeting – IIJ Sponsor session

2025年11月04日

株式会社インターネットイニシアティブ
今村 侑輔

自己紹介



なまえ: 今村 侑輔

けいれき:
- 2015 IIJ 新卒入社, 現在の部署に配属される
  - はじめてのサーバ構築/運用を経験
- 2018 IIJ Europe に海外赴任
  - パソコンなんでも屋さんを経験
- 2020 IIJ に帰任、古巣へ帰ってくる
- 2025 担当サービスがセキュアMXからxSPプラットフォームサービス/Mailへ

なにやってるの?
- IIJメールサービスのあれこれ(ベンダ/顧客対応/メンテナンス対応などなど)
- 外部への情報発信/情報収集始めました
  - M3AAWG メンバー(数年参加出来てません)
  - JPAAWG 運営委員
  - IIJ engineer blog 執筆

本日のおしながき

昨今の迷惑メール対策のご紹介
総務省からの要請について
- DMARC
- BIMI

ARC 苦労話その1 (IIJ 山下より)
ARC 苦労話その2 (IIJ 清水より)

IIJ メールサービスについて

日本のインターネットを「ゼロ」から作り上げ、国内で初めて本格商用インターネット接続サービスを提供

- **Emailビジネスの歴史も長く、様々なサービス展開を実現**
- **多くの方に長年ご利用していただいております**　（※法人、個人含む）

IIJmio

SecureMX

法人向けメールサービス

・IIJ セキュアMXサービス
業界・規模を問わず多くのお客様に導入いただいているクラウド上でメールセキュリティを強化する統合メールセキュリティサービス
フィッシングなどの脅威メール対策、情報漏えい対策、内部不正対策など、メールの受信・送信のセキュリティ対策をワンストップで実現

コンシューマ向けメールサービス

・ IIJ mioセーフティメール
ウィルス駆除・SSL・SMTP認証・なりすましメール対策フィルタ・送信ドメイン認証など、これからのスタンダードとなる安全対策を標準で備えており好評を得てます。

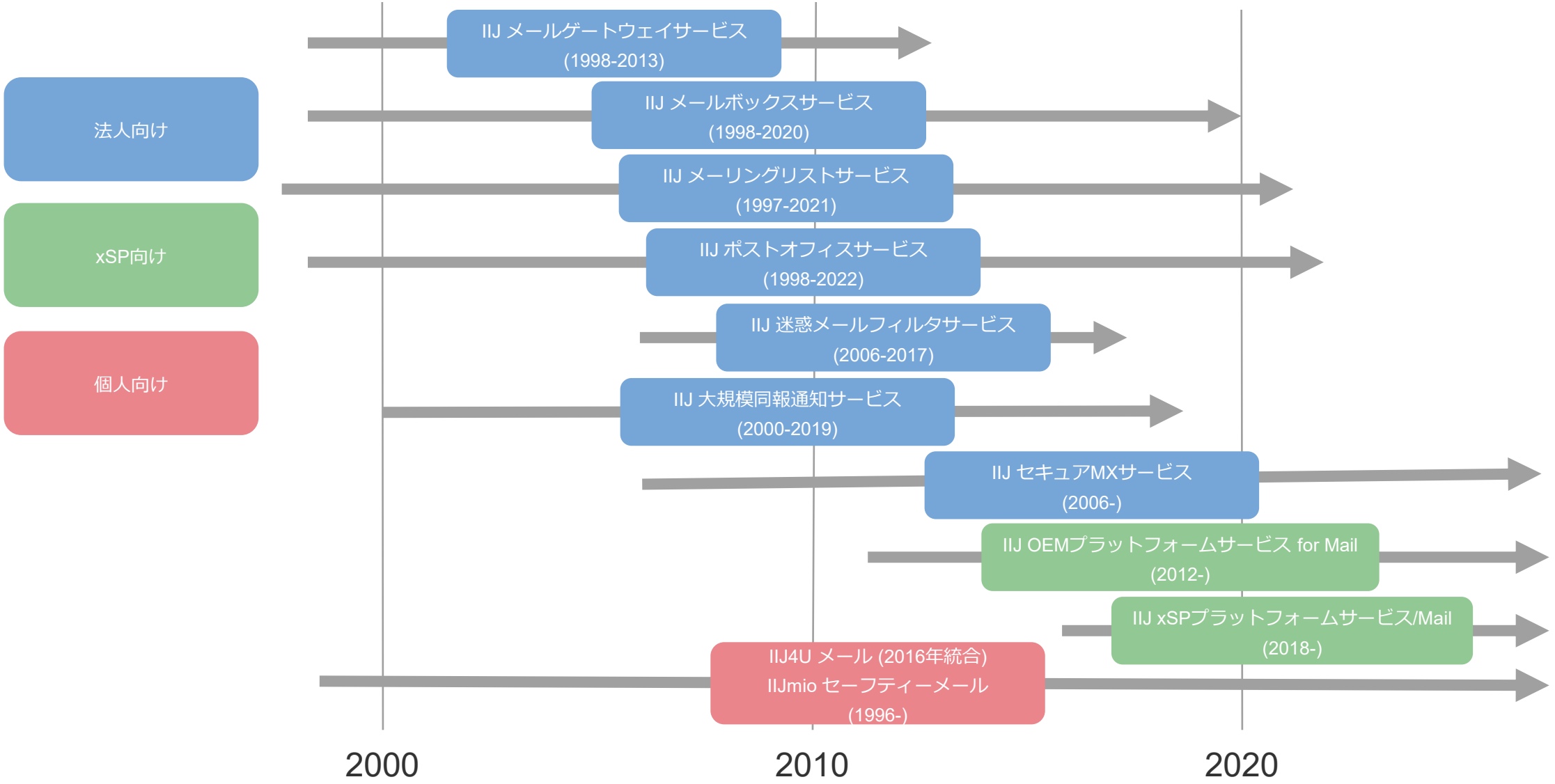
コンシューマ向け OEMプラットフォームサービス

・IIJ xSPプラットフォームサービス/Mail
ISPやCATV事業者など、数百万を超える規模のユーザを抱えるサービス事業者向けに、メールシステムをクラウドサービスとして提供するサービス

大規模メールシステム インテグレーションおよび運用サービス

様々なOSSおよび商用パッケージ導入実績を持ち、お客様システムに最適な形でのシステム導入を実現します。
コードベースでのカスタマイズを行うことで事業者毎のニーズの違いを吸収することが可能です。

多くのメールサービスを運用してきました



昨今の迷惑メール対策について

逆引きレコードのないMTAからの送信の取り扱い

フィッシング対策協議会月次報告書縦読み

直近数ヶ月の月次報告書に記載のある “逆引きレコードがない送信サーバからの迷惑メール率” を見てみると常に半数以上~9割近い値となっている

月	迷惑メール率
4月	83.5%
5月	74.2%
6月	91.0%
7月	87.7%
8月	81.4%

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

M3AAWG Sender Best Common Practices v3.0 (2015)

3.3 Technical IP Details

2. 逆引きDNS（Reverse DNS）

a. メール送信サーバーのIPアドレスには、**逆引きDNS（PTRレコードまたはIN-ADDR）**が設定されていなければなりません。

b. 各IPアドレスには、**1つの逆引きDNS名のみ**が設定されている必要があります。

c. その逆引きDNS名は、上記(1a)で選定された**主要な名前と完全に一致**していなければなりません。

(1a) 名前の選定について

責任主体のドメインを**明確に識別できる名前**を選定しなければなりません。

IPアドレスが共有されている場合は、通常その提供者（プロバイダーやESP）のドメイン名を使用します。

専用IPの場合は、通常その顧客や広告主のドメイン名を使用します。

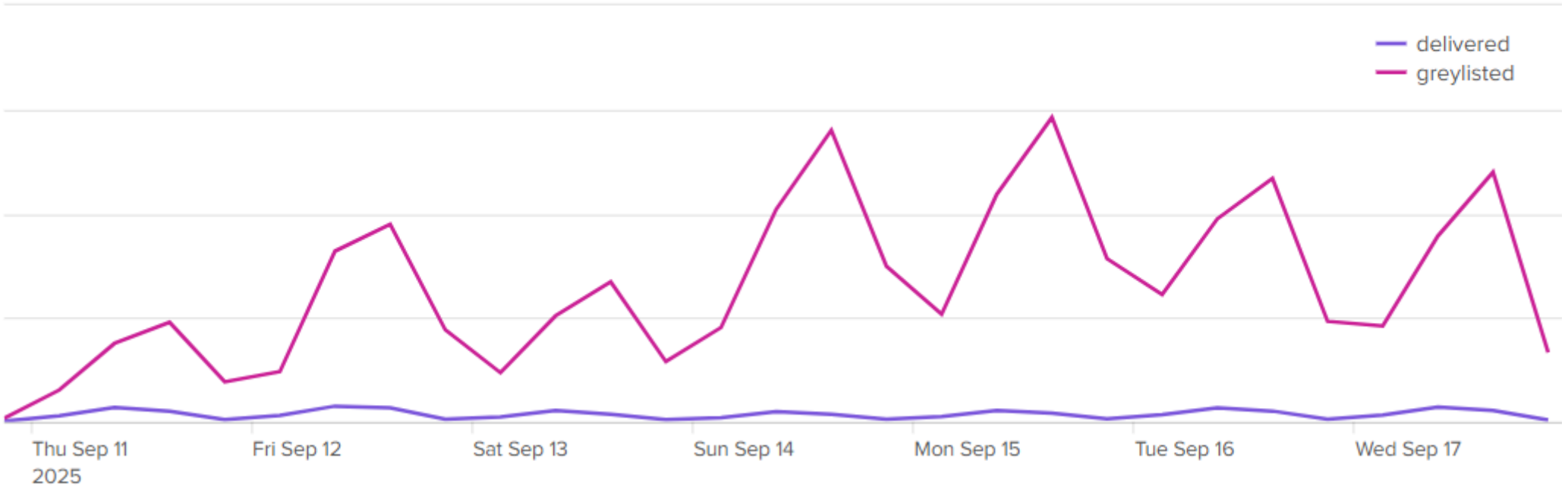
なお、後者（顧客や広告主のドメイン名を使用する場合）では、**正引きDNS（Aレコードなど）の設定は、そのドメインの管理者の責任**となります。

https://www.m3aawg.org/sites/default/files/document/M3AAWG_Senders_BCP_Ver3-2015-02.pdf

実際のところどうなの？

実際に調べてみた

弊社 某サービス宛に来ている逆引きレコードがないメール通数とそうじゃないメールの通数を6時間ごとに1週間分集計



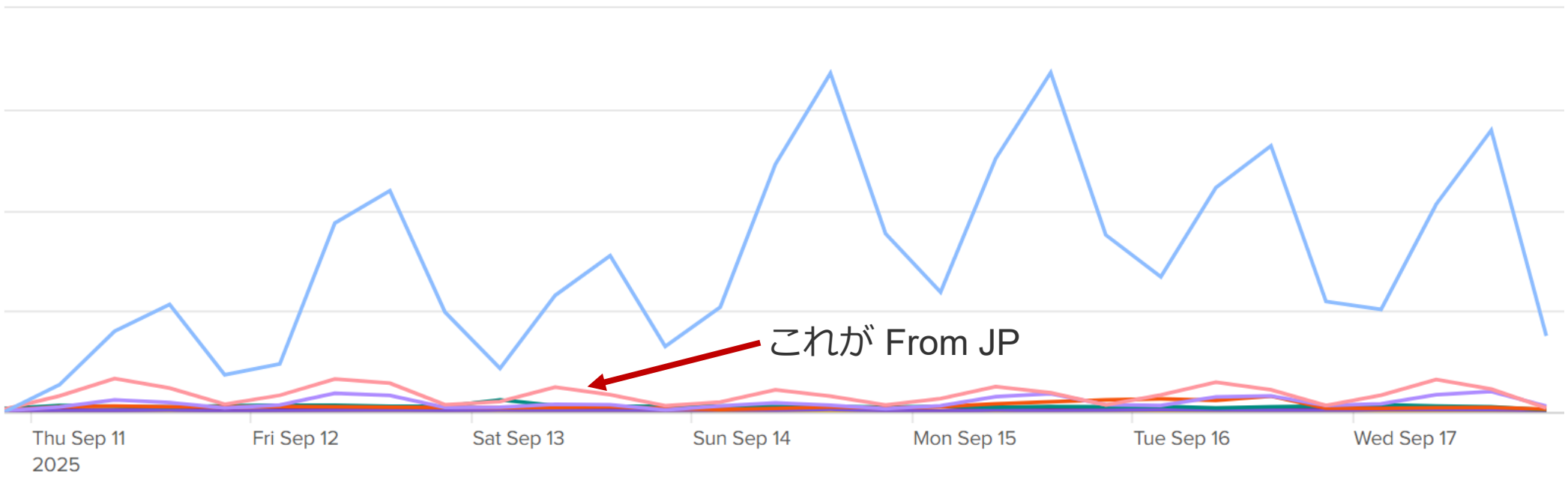
delivered: 逆引きレコードがあるMTAから受信したメール通数

greylisted: 逆引きレコードがないMTAから受信したメール通数

これは止めてもいいのでは…

念のためもうちょっと調べてみた

弊社 某サービス宛にメール送信しているMTAの国別IPアドレス分類集計

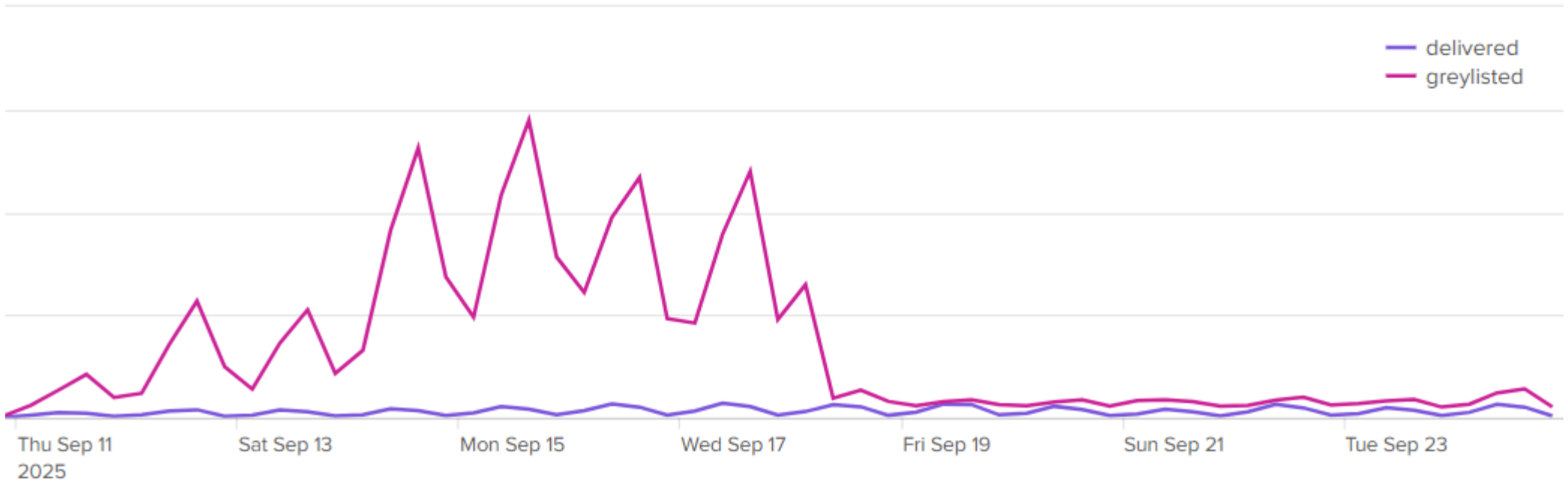


やはり

これは止めてもいいのでは…

実際に弾いてみた

実際に受信しないよう設定変更をした前後の前述のメール通数を2週間分集計



これは大勝利では…みなさまもご検討ください

ユーザーからの問い合わせもなし！

各事業者への総務省からの要請について

フィッシングメール対策の強化について（総務省からの要請）- 2025/09/01

AI 活用

フィルタリングの判定技術の向上や迷惑メール判定における AI の活用等、メールの フィルタリングの精度の一層の向上を積極的に図ること。また、迷惑メールのフィルタリ ング強度を適切に設定するなどして、高度化するフィッシングメールに対応可能なメール フィルタリングを目指すこと。

なりすまし対策

なりすましメール対策として有効な DMARC の導入や DMARC ポリシーの設定（隔離、拒否）を行うこと。送信側だけでなく受信側についても、適切な DMARC ポリシーに基づく処 理やレポート送信を設定すること。また、ドメインレピュテーション、BIMI、踏み台送信 対策等の更なる対策の導入を積極的に検討していくこと。

情報発信

提供しているフィッシングメール対策サービスについて、様々な利用者層に向けた一 層の周知・啓発を行うこと。

1. DMARC の有効活用

DMARCはなりすましメールの受信を送信者、受信者の双方の協力によって防ぐための仕組みメールボックスプロバイダーのみが対応しても、メール送信を実施するドメイン所有者が対応をしないと結果として作用しない

2. BIMI の有効活用

BIMI も DMARC と同様、送信者と受信者双方の対応が必要

もともとはブランド保護を目的とした仕組みであり、結果としてなりすましメールを視覚的にわかりやすく判別できるという副作用がある

3. 踏み台送信対策

踏み台とされたアカウントやサーバーに対する事後対応については、これまでも各所で議論ならびに対策が講じられているが、その根本対策には至っていない

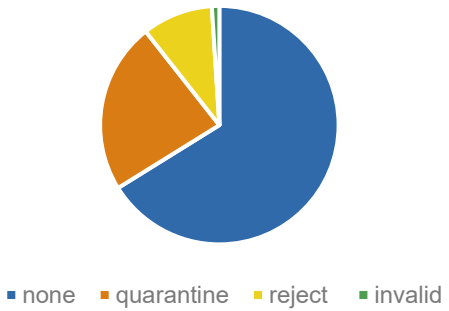
メールで利用される SMTP, POP3, IMAP4 における多要素認証との非親和性に起因する障壁が大きい

DMARC

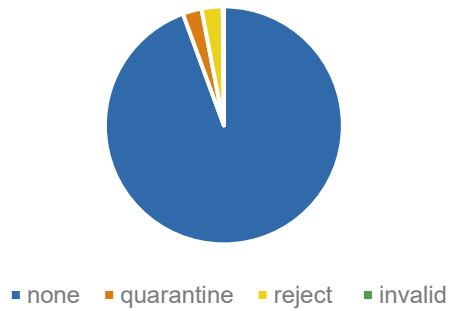
日本の DMARC ポリシー quarantine/reject 率はまだまだ低い

一部分野別にDMARCポリシー分類を調査 (2025/10/28 現在)

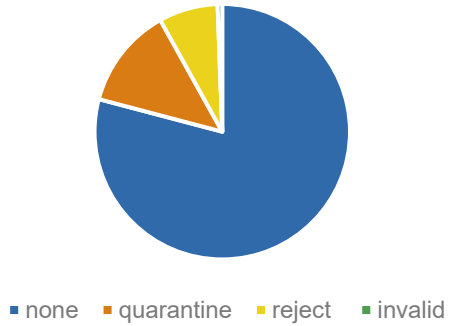
日本政府



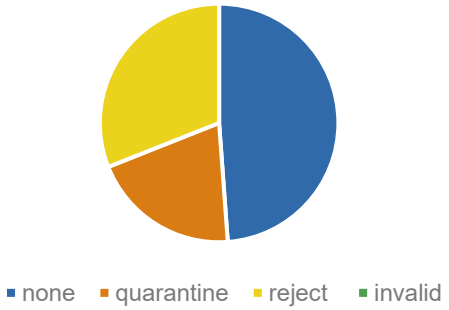
地方公共団体



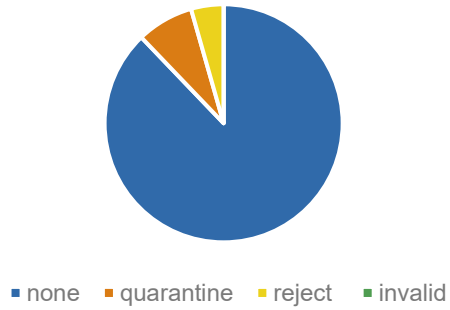
TOPIX



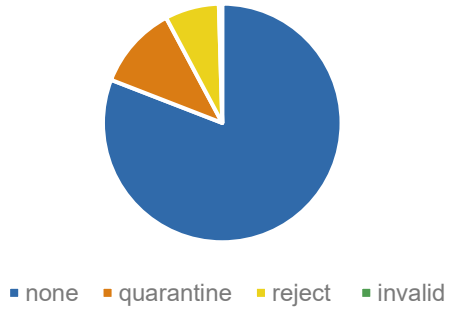
金融機関



教育機関



計



https://stats.dnsops.jp/ より

DMARC ポリシー強化の必要性

そもそも quarantine/reject にする必要あるの？

ドメイン管理者目線

1. 自組織ドメインの信頼性向上

DMARCポリシーを宣言することで自組織が管理するドメインを用いたメールの信頼性が向上する

メール送信先システムがDMARC評価している場合、なりすましメールの防止につながり自組織ならびにブランドの信頼性が向上する

2. BIMI の利用

DMARCポリシーを宣言することでBIMIを活用した自組織のブランド保護が可能

DMARCポリシーの quarantine/reject が増えるとどうなるの？

DMARC ポリシーが厳格化された後の世界線

1. フィッシングメール被害の大幅な減少

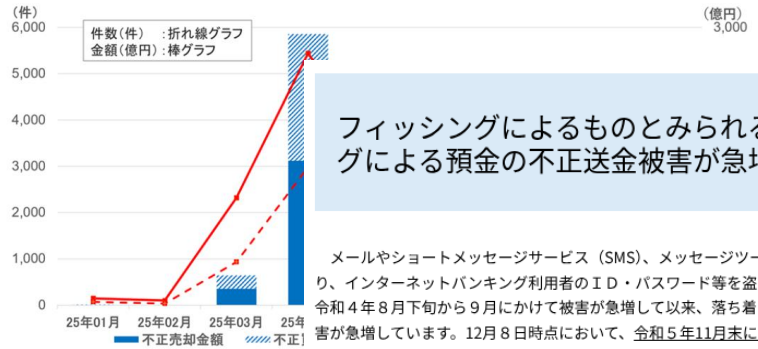
全ての正規メールが DMARC 評価を pass するため、多くのなりすましメールがなくなる

…それだけ?

フィッシングメールの被害が急増しています

インターネット取引サービスへの不正アクセス・不正取引による被害が急増しています

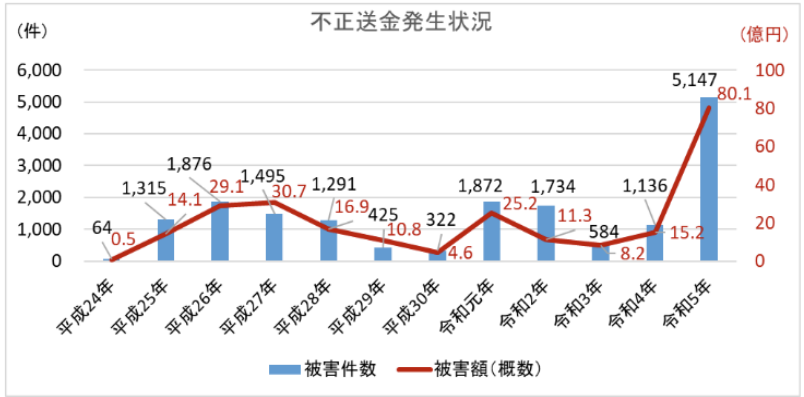
○　実在する証券会社のウェブサイトを装った偽のウェブサイト（フィッシングサイト）等で窃取した顧客情報（ログインIDやパスワード等）によるインターネット取引サービスでの不正アクセス・不正取引（第三者による取引）の被害が急増しています。



フィッシングによるものとみられるインターネットバンキングによる預金の不正送金被害が急増しています。

メールやショートメッセージサービス（SMS）、メッセージツール等を用いたフィッシングと推察される手口により、インターネットバンキング利用者のＩＤ・パスワード等を盗み、預金を不正に送金する事案が多発しています。令和４年８月下旬から９月にかけて被害が急増して以来、落ち着きを見せていましたが、令和５年２月以降、再度被害が急増しています。12月８日時点において、令和５年11月末における被害件数は5,147件、被害額は約80.1億円となり、いずれも過去最多を更新しています。

不正取			
25年1月	25年2月	25年3月	25
2	2	5	



※ 平成24年から令和４年の数値は確定値、令和５年の数値は、同年12月８日時点における暫定値

https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html
https://www.fsa.go.jp/ordinary/internet-bank_2.html

なりすましメールを防ぐのはもはや企業の責任

これまでのホームページに注意喚起を掲載するような対応では防ぎきれない

今後どのような種類のなりすましメールが増えるか、なりすましメールの流量が急増するのかもわからない

事前の対策ができるのはドメイン所有者のみ

なりすまし被害の責任は消費者ではなくそれを許した企業にもある

ITシステムで止めないといつ何があるかわからない

フィッシングメールの被害が、急増しています！！！！！

電気通信事業者としてできること

ではメールサービス提供している事業者の立場で何ができるのか

1. DMARCに対応したメールシステムを提供すること

なりすましメールではない、と宣言できるためのメール送信システムを提供する

なりすましメールを防ぐことができるようにDMARC評価ならびに評価結果に基づいてフィルタリングできるメール受信システムを提供する

DMARCポリシー強化の普及のためにDMARC 集計レポート(rua) を受信して解析するシステムならびに rua を送信するシステムを提供する

2. 啓蒙活動

とにかく広めていくしかない

DMARC検証結果によるフィルタリングの見解

総務省のドキュメントをみてみましょう

（3） フィルタリング行為に関する「通信の秘密」侵害行為の該当性

送信ドメイン認証の結果のラベリング等に基づき、受信した電子メールについてフィルタリングを行うことが、電気通信事業法との関係で問題が生じないか。

具体的には、上記行為が、
電気通信事業法第4条に規定する「通信の秘密」を「侵害する行為」に該当するか
が問題となる。

・「通信の秘密」「侵害行為」該当性

フィルタリングを行い、あらかじめ設定した条件に該当する特定の通信に係る通信の秘密を検知し、通信当事者の意思に反して処理する（例：ブロックしたり、廃棄したりする）行為は、**通信の秘密を「発信者又は受信者の意思に反して利用する」ことに当たり、通信の秘密の窃用（侵害）に当たる**と考えられる。

→ **当事者の同意がない限り、「通信の秘密」を「侵す行為」に該当する。**

フィルタリングは、受信者のために行う行為であるから、受信者の意思に関わらず実施する正当業務行為等の違法性阻却事由には原則として該当しない。
したがって、当事者の有効な同意を取得する必要がある。

7

https://www.soumu.go.jp/main_content/000499986.pdf

DMARC 検証結果によるメールフィルタリングは "侵害行為"

通信の秘密を侵害する行為となるため、当事者(メールサービス利用者)の同意が必要

B to B 事業者の場合

- 利用者が企業、団体であるため実質的に情報システム管理部門が Go を出せるので導入障壁はほぼなし

B to C 事業者の場合

- 当事者の同意を得る必要があり、ここがとても大変そう

フィルタリング導入にあたっての同意について

ではメールサービス提供している事業者の立場で何ができるのか

フィルタリング導入にあたっての当事者の同意について

(1) 初期設定オフで、利用者から申込みを受けて提供する場合
一般的に、利用者の有効な同意があると考えられる。

(2) 初期設定オンで提供する場合
約款等による事前の包括的合意により、通信の秘密の利益を放棄させることは、

① 約款の性質になじまないこと
② 同意の対象が不明確であること

から、原則として**許されない（有効な同意とは解されない）**

※ ただし、以下の条件を満たす場合には、「初期設定オン」で提供したとしても、利用者の有効な同意を取得したものと考えることができる。

① 同意後も、随時、利用者が任意に設定変更できること
② 同意の有無に関わらず、その他の提供条件が同一であること(※1)
③ 同意の対象・範囲が明確に限定されていること
④ 平均的利用者であれば同意することが合理的に推定されること（信用できるデータ(※2)による裏付けが必要）
⑤ フィルタリングサービスの内容について、事前の十分な説明を行うこと（電気通信事業法第26条に規定する重要事項説明に準じた手続によること）

※1 フィルタリングサービスを合理的な料金により提供することは問題ない。
※2 利用者を対象に無作為抽出によるアンケートを実施することなどが考えられる。

8

https://www.soumu.go.jp/main_content/000499986.pdf

いろいろな解釈ができるが…

④ 平均的利用者であれば同意することが合理的に推定されること

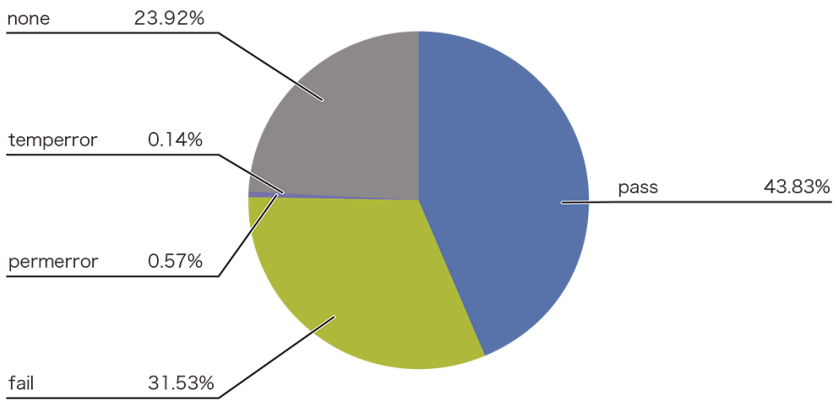
昨今の情勢であれば利用者の多くがなりすましメールを拒否することに同意してくれるのではないか

⑤ フィルタリングサービスの内容について、事前の十分な説明を行うこと

（提供条件の説明）
第２６条
電気通信事業者及び電気通信事業者の電気通信役務の提供に関する契約の締結の媒介、取次ぎ又は代理を 業として行う者は、電気通信役務の提供を受けようとする者（中略）と国民の日常生活に係るものとして総務省令 で定める電気通信役務の提供に関する契約の締結又はその媒介、取次ぎ若しくは代理をしようとするときは、総務 省令で定めるところにより、当該電気通信役務に関する料金その他の提供条件の概要について、その者に説明しな ければならない。

フィルタリング導入の効果測定

ではメールサービス提供している事業者の立場で何ができるのか



弊社環境で観測されている受信メールのDMARC評価の割合

https://www.iij.ad.jp/dev/report/iir/067/02.html

DMARCフィルタリングの是非

DMARC評価結果によるフィルタリングを一括導入すると、3割強のメールを受信しなくなることになる

もし、p=none なメールも受信しない、という今後 Google と同じような対応をすると半分以上のメールが受信拒否対象に

事件は会議室で起きてるんじゃない、現場で起きてるんだ！

BIMI

Brand Indicators for Message Identification (BIMI)

メッセージ識別のためのブランドインジケーター（BIMI）は、ドメイン所有者がメールユーザーエージェント（MUA）と連携し、適切に認証されたメッセージの横にブランド固有のインジケーターを表示できるようにします。BIMIの連携には2つの側面があります。ドメイン所有者が希望するインジケーターを公開するためのスケーラブルなメカニズムと、メール転送エージェント（MTA）がインジケーターの真正性を検証するためのメカニズムです。

https://datatracker.ietf.org/doc/draft-brand-indicators-for-message-identification/

なんのためにBIMIを使うのか

■ブランドの保護

MUA にブランドロゴを表示することで、そのメールが正規なメールであることを認識してもらうための手段の一つ

昨今、迷惑メール対策の一環として BIMI の利用が推奨されているが主目的は “ブランドの保護”

IIJmio　SMX Secure　IIJiD　wizSafe　IIJ Omnibus　IIJ GIO

ドメイン所有者の対応

■専用証明書の取得

■ブランドロゴの作成、登録、公開

メール受信事業者(webメール提供事業者)の対応

■BIMI 検証

■検証結果に基づいたブランドロゴの表示機構実装

コモンマーク証明書(CMC) への対応

2024年12月よりCMCが登場し、BIMIへの対応のハードルが一段下がりました

コモンマーク証明書(CMC) の利点

■従来の 企業マーク証明書(VMC) と異なり、**商標登録がなくてもブランドロゴをメールに表示できるように**

■過去12か月以上のロゴ使用実績があればよい

項目	VMC	CMC
ロゴの要件	商標登録済みロゴが必須	商標登録不要。過去の使用実績で可
認証機関の審査	厳格（商標・法人・ドメインなど）	比較的緩やか（ロゴ使用実績の確認）
取得難易度	高い（審査期間：数週間～1ヶ月）	低め（数日～数週間）
ロゴ加工	不可（登録ロゴそのまま）	一部加工可（配置変更など）

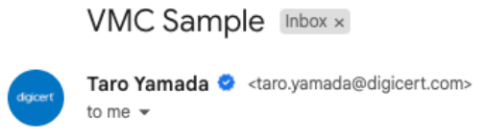
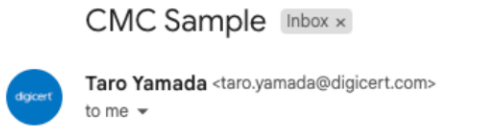
コモンマーク証明書(CMC) への対応

2024年12月よりCMCが登場し、BIMIへの対応のハードルが一段下がりました

事業者としての CMC への対応

■Google に続いて VMC/CMC に対応するか

■対応する場合、どういう表示にするか

受診トレイの表示	顧客の受信トレイの「送信者」フィールドの横に、Google の青いチェックマークとともに自社のブランドロゴが表示される 	顧客の受信トレイの「送信者」フィールドの横に、自社のブランドロゴのみが表示される (青いチェックマークは**表示されない**) 
備考	Gmail 以外のメーラーでもサポートされている	2024年10月現在、サポートの表明は Google のみ

https://www.digicert.com/jp/tls-ssl/verified-mark-certificates

本講演のまとめ

逆引きレコードがないMTAからのメールは止めよう

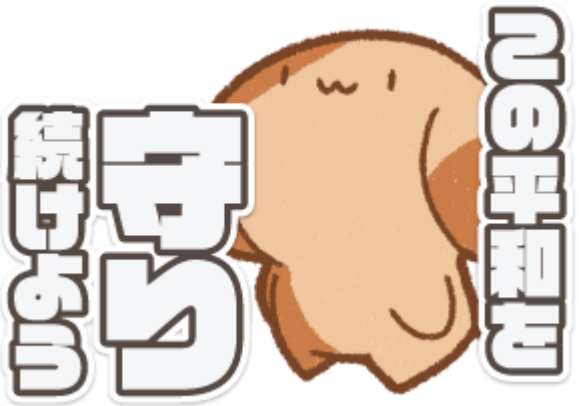
■迷惑メールの可能性がとても高いです

DMARC、BIMI はブランド保護のため

■結果的に迷惑メール対策となるが、自社ブランドの保護のために対応を進めましょう

■送信者だけでなく、受信システム側での対応も急務

そして話はARCへ...



日本のインターネットは1992年、IIJとともにはじまりました。以来、IIJグループはネットワーク社会の基盤をつくり、技術力でその発展を支えてきました。インターネットの未来を想い、新たなイノベーションに挑戦し続けていく。それは、つねに先駆者としてインターネットの可能性を切り拓いてきたIIJの、これからも変わることのない姿勢です。IIJの真ん中のIはイニシアティブ――IIJはいつもはじまりであり、未来です。