JP AAWG Japan Anti-Abuse Working Group

通信キャリアが考えるDMARCを活用したなりすましメール対策

株式会社NTTドコモ　正見　健一朗
KDDI株式会社　中島　直規
ソフトバンク株式会社　熊沢　明生

登壇者紹介

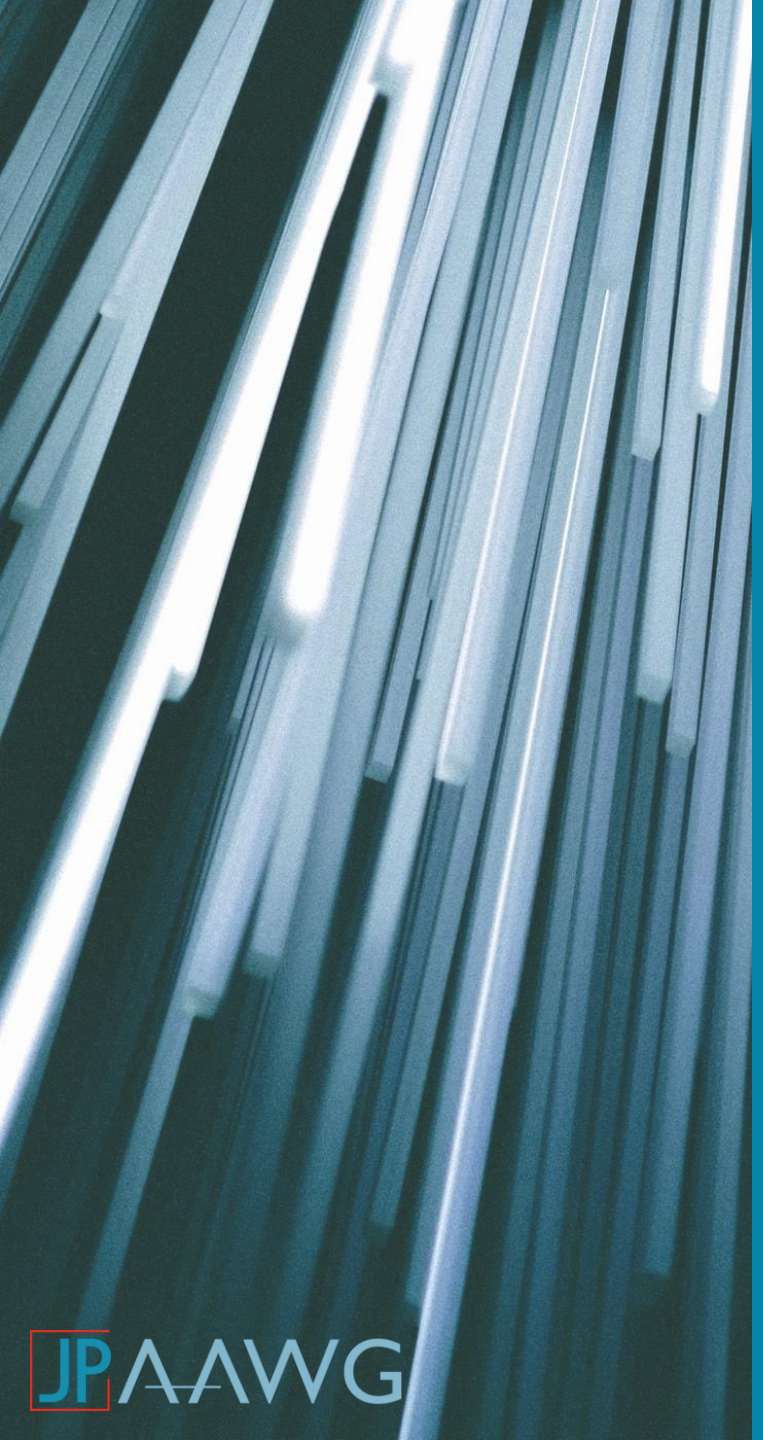
櫻庭 秀次
JPAAWG会長

正見 健一朗
株式会社NTTドコモ

中島 直規
KDDI株式会社

熊沢 明生
ソフトバンク株式会社

DMARC普及活動にご協力を！



DMARCの日本国内の現状、そして今後

正見　健一朗
株式会社NTTドコモ

JP AAWG

昨年度までのNTTドコモからの発信

これからは**２種類の対策が必要**と言い続けてきました

docomo

2軸の対策

①偽物メールを止める

詐欺/ウイルスメール拒否（DMARCフィルタリングを新たに機能追加）

②正規メールを正しく認知する

ドコモメール　公式アカウント

公式アカウントマーク

19

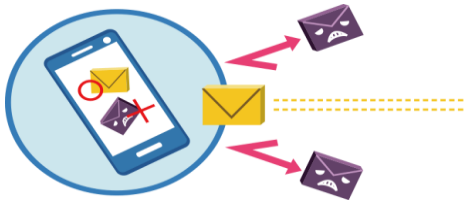
過去のJPAAWG資料から抜粋

NTTドコモの今後の取り組み

2025年1月ごろに、**２つの取り組みをさらに進化**をさせます

①怪しいメールの対処強化

・DMARCポリシーのフィルタリング
・**DMARC失敗、未導入時の警告表示**



②正規メールの保護強化

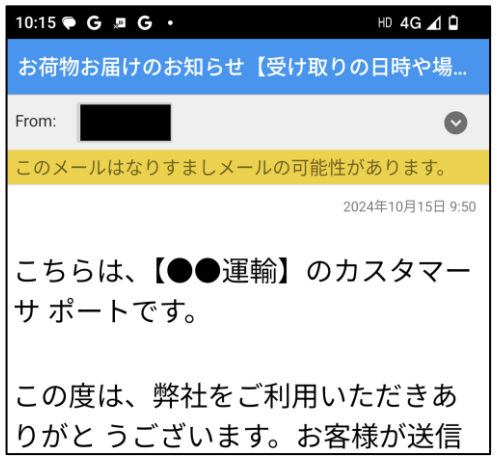
・**公式アカウントの改善**
・**BIMI**

目指す世界

DMARCを活用し、あんしん・安全な環境を作っていきます

警告

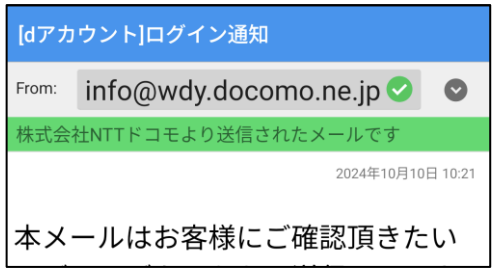
WARNING



なりすましメールが存在しない世界へ

・DMARCがFail、または未導入の場合に警告する
・ポリシーが**noneのドメインを含め**、警告することで幅広くフィッシング詐欺への対策が可能に
・未導入がなくなり、全ての正規メールがDMARCによって認証される環境へ！

公式アカウントマーク



しっかり取組んだ**企業にメリット**を

・取組み済のメールを閲覧するユーザにはあんしん・安全を
・開封率が上がる仕掛けにより、企業にもビジネス価値を

BIMI

JP AAWG

なりすましメールへの警告表示機能の導入

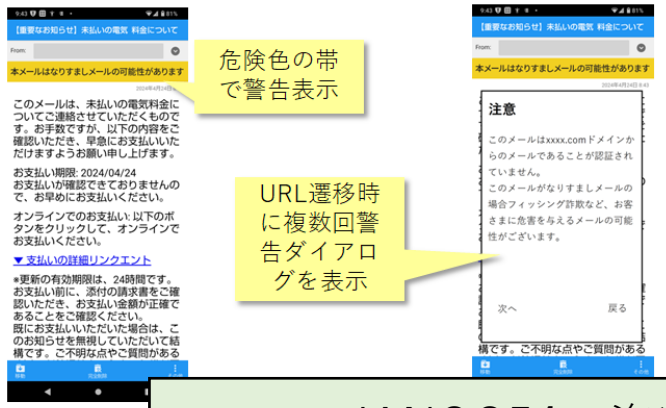
DMARC未導入だとドコモメールでは必ず**警告**を出します
（2025年1月ごろより）

docomo

NTTドコモもDMARCが当たり前になるよう、新たな対策を開始します

DMARCを用いた警告表示機能の概要

身元確認（ドメイン認証）ができていないメールは**一律警告を表示**



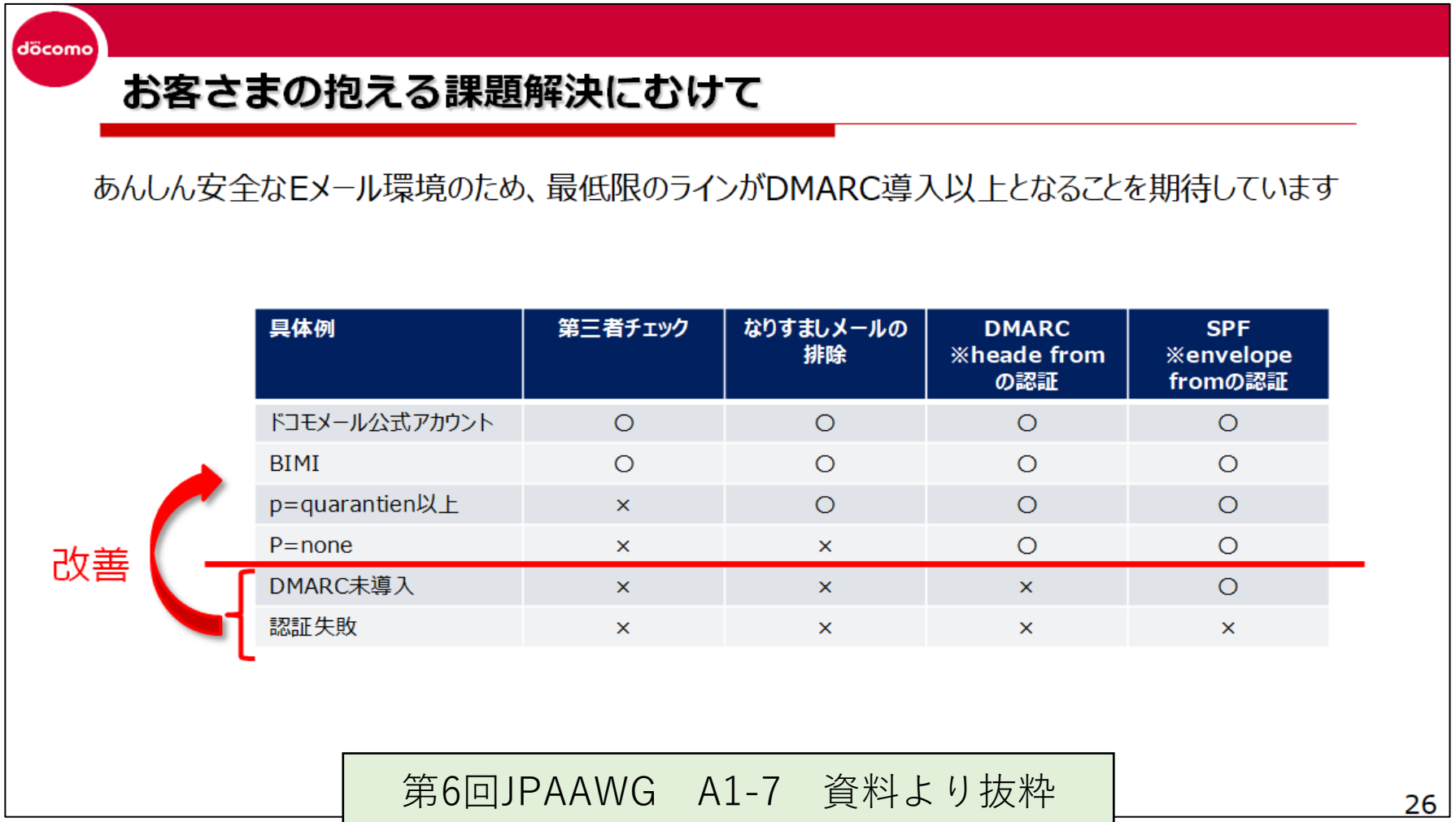
目的

・**基準レベルをDMARC導入済**に引き上げる
・基準を満たしたメールはドメインなりすましはないので、**ドメイン単位でレピュテーション**を行う
・基準未達、またはレピュテーションの結果に従い、ユーザが**視覚的にわかりやすい警告**を行い詐欺を**未然に防止**する

JANOG54　資料より抜粋

Eメールを送信する側に期待する水準

昨年弊社より**せめてp=noneを！**とご説明しました



docomo

お客さまの抱える課題解決にむけて

あんしん安全なEメール環境のため、最低限のラインがDMARC導入以上となることを期待しています

具体例	第三者チェック	なりすましメールの排除	DMARC ※heade fromの認証	SPF ※envelope fromの認証
ドコモメール公式アカウント	○	○	○	○
BIMI	○	○	○	○
p=quarantien以上	×	○	○	○
P=none	×	×	○	○
DMARC未導入	×	×	×	○
認証失敗	×	×	×	×

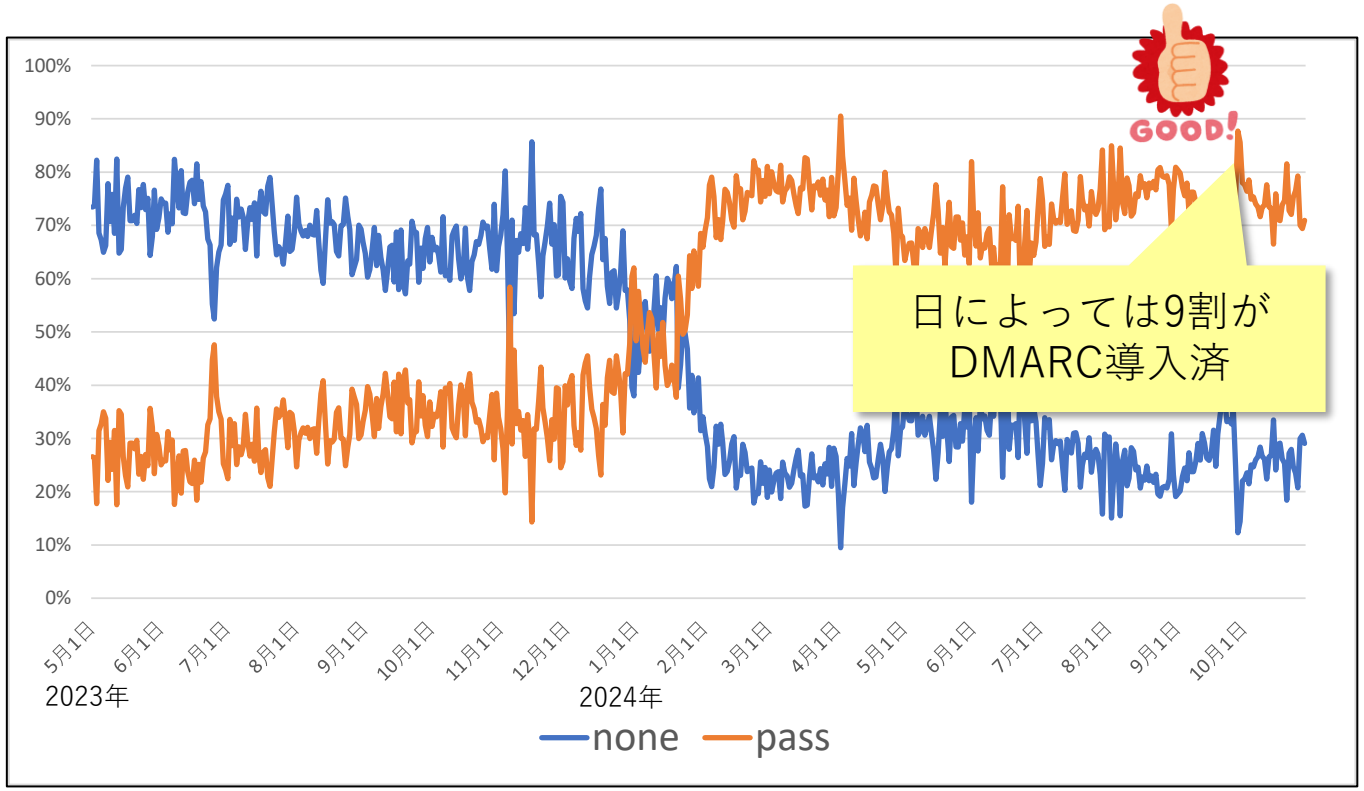
改善

26

第6回JPAAWG　A1-7　資料より抜粋

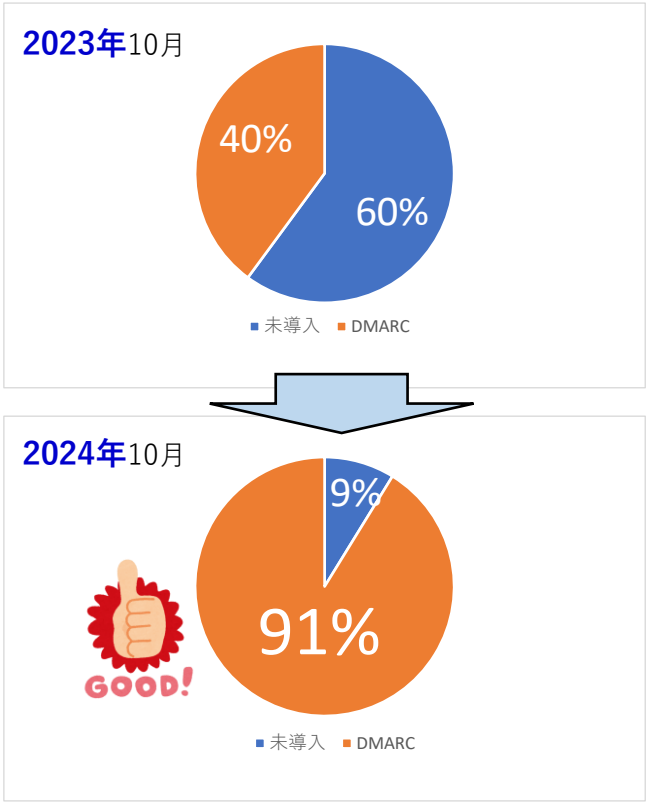
日本国内のDMARC認証率の現状

日本国内も、ついにDMARCの導入が**ほぼ完了**



NTTドコモによせられた偽陽性報告(FP申告)のDMARC認証状況

FP申告から、spamによる偽報告を除去



昨年度と比較して**DMARCの設定率が大幅に上昇**しました。

一部未導入の送信元企業、団体さまへ

一部**自治体さま**のドメインにて未導入があります。
ぜひDMARCの導入をお願いします

迷惑メール対策協議会 技術WG資料より引用

地方自治体の SPF, DMARC 設定状況
(2024.10.01)

全国での SPF レコード宣言率: 99.8% (98.7%)
全国での DMARC レコード宣言率: 36.5% (35.2%)

	SPF* (%)	DMARC* (%)
北海道	100.0 [180/180]	100.0 [180/180]
東北	99.6 [232/233]	16.7 [39/233]
関東	100.0 [323/323]	46.7 [151/323]
中部	100.0 [325/325]	31.1 [101/325]

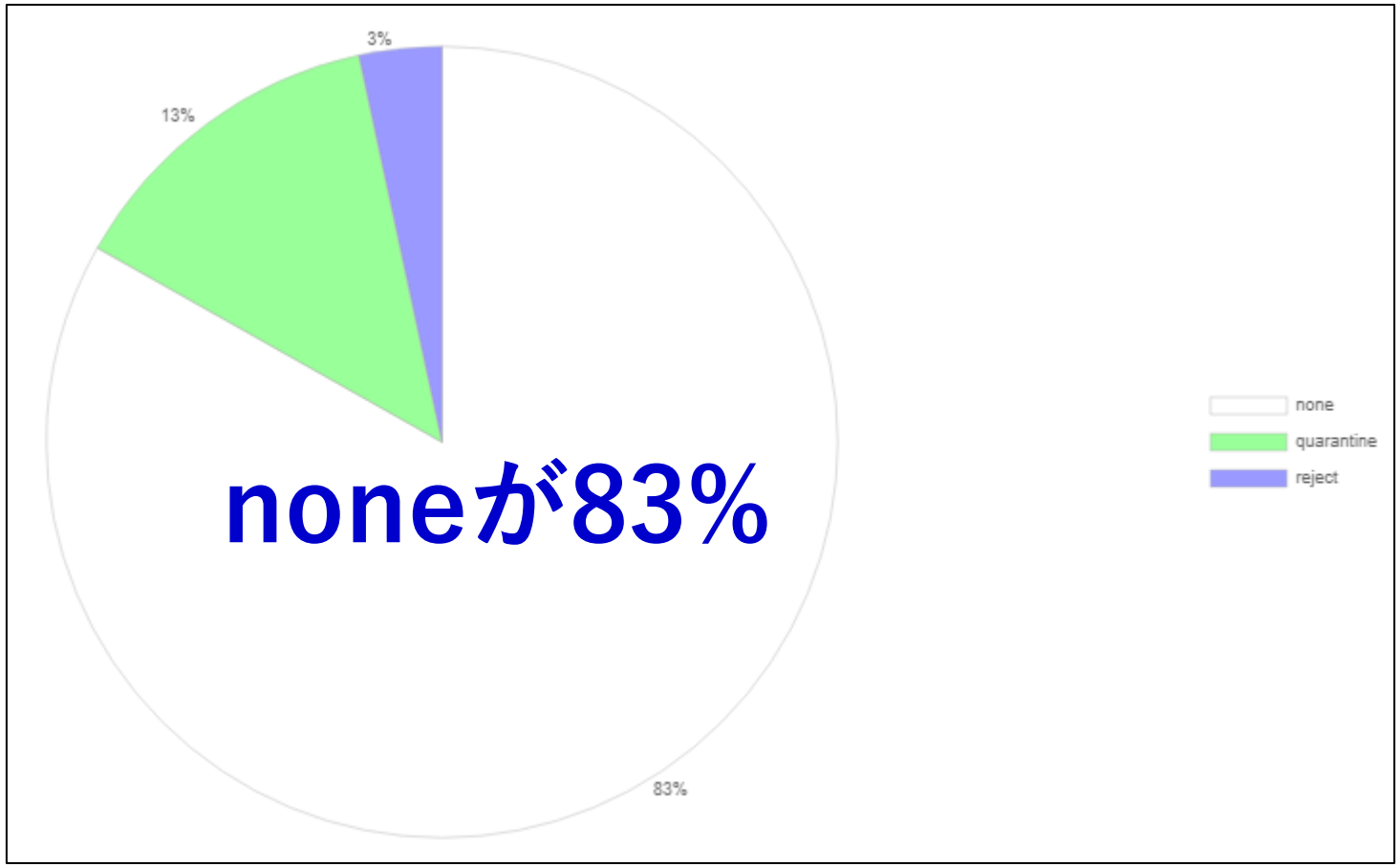
	SPF* (%)	DMARC* (%)
近畿	99.6 [233/234]	48.3 [113/234]
中国	99.1 [111/112]	18.8 [21/112]
四国	100.0 [99/99]	14.1 [14/99]
九州沖縄	100.0 [282/282]	12.1 [34/282]

- 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
- 全国の括弧内割合は前回調査 (2024.04.22)

JPAAWG

しかし、DMARCポリシーの状況では

現状**p=noneのドメインが圧倒的に多い**状況です



とある1日のドコモメール宛のメールのDMARC宣言の分布

次のSTEPであるなりすましメールの排除へ

p=quarantine/rejectへ進む時です

具体例	第三者チェック	なりすましメールの排除	DMARC ※header fromの認証	SPF ※envelope fromの認証
ドコモメール公式アカウント	○	○	○	○
BIMI	○	○	○	○
p=quarantine/reject	×	○	○	○
p=none	×	×	○	○
DMARC未導入	×	×	×	○
認証失敗	×	×	×	×

新しい基準

古い基準

p=quarantine/rejectが必要な理由

p=noneのドメインは攻撃者の踏み台にされます

Point①：ドメイン固定で複数の攻撃の踏み台に

From:xx@crXXXX.jp
【重要なお知らせ】お客様のお支払い方法が承認されません

残念ながら、Amazon のアカウントを更新できませんでした。
今回は、カードが期限切れになってるか、請求先住所が変更されたなど、さまざまな理由でカードの情報を更新できませんでした。
お客様のアカウントを維持するため Amazon アカウントの 情報を確認する必要があります。下からアカウントをログインし、情報を更新してください。
■ご利用確認はこちら

From:xx@crXXXX.jp
今すぐ受け取れる！5000円分のPayPayボーナスとお得なキャンペーン情報

PayPayをご利用いただきありがとうございます。
すぐに5000円分のPayPayボーナスを受け取ることができます。
■ 詳しくはこちらをご覧ください。
ウエルシアグループアプリから
PayPayで支払うと最大全額戻ってくる！
開催期間：2021/8/13（火） ～ 9/9（月）
付与上限：100,000ポイント／回および期間

Point②：対策されたらすぐに次のドメインへ移行

From:xx@myXXXXmo.com
Amazonプライム会員様への重要なお知らせ

お客様、

Amazon.co.jpをご利用いただきありがとうございます。最近、お客様のアカウント情報が第三者によって変更された可能性があります。アカウントの安全を確保するため、下記のリンクをクリックしてアカウントを検証してください。

hxxps://xxx.html
Amazon セキュリティチーム

From:xx@account.XXXXendo.com
【緊急】dカードが利用停止のお知らせ

ご利用いただき、誠にありがとうございます。このたび、お客様のdカードアカウントで不審なアクティビティが検出されたため、ご利用を一時的に制限させていただきました。

つきましては、以下のリンクからアカウントの確認と利用再開手続きを行ってください。
hxxps://xxx.cc。

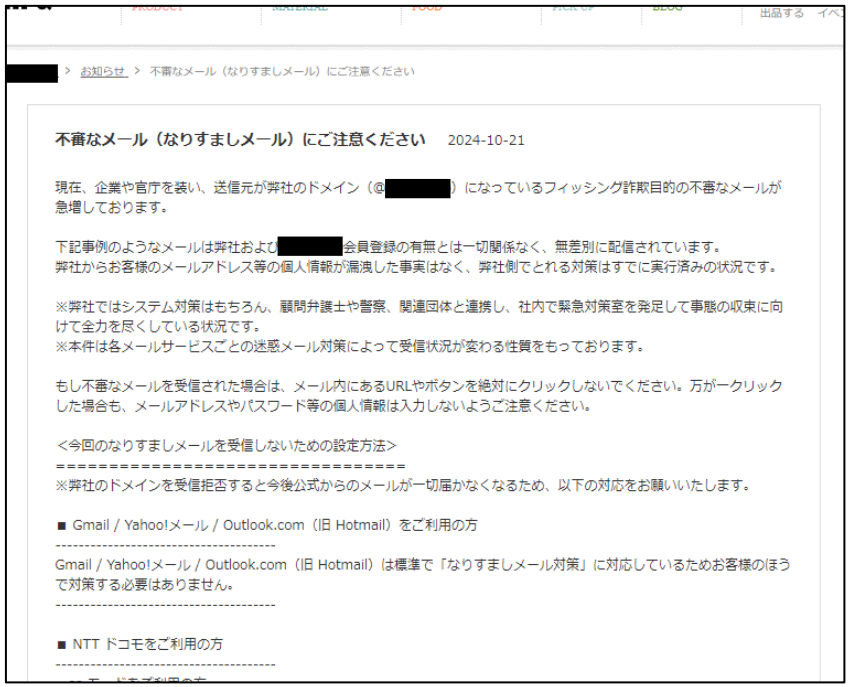
いずれもDMARCの宣言は
「none」の日本企業の実在ドメイン

⇒無関係のドメインがいきなり利用されるため、**全ての企業が被害者に**

p=quarantine/rejectが必要な理由

p=noneでは**自社の顧客の信頼度低下**を招きます

なりすまし対策をしておかないと、踏み台にされ、自社の顧客が困ることになります



不審なメール（なりすましメール）にご注意ください　2024-10-21

現在、企業や官庁を装い、送信元が弊社のドメイン（@[redacted]）になっているフィッシング詐欺目的の不審なメールが急増しております。

下記事例のようなメールは弊社および[redacted]会員登録の有無とは一切関係なく、無差別に配信されています。
弊社からお客様のメールアドレス等の個人情報が漏洩した事実はなく、弊社側でとれる対策はすでに実行済みの状況です。

※弊社ではシステム対策はもちろん、顧問弁護士や警察、関連団体と連携し、社内で緊急対策室を発足して事態の収束に向けて全力を尽くしている状況です。
※本件は各メールサービスごとの迷惑メール対策によって受信状況が変わる性質をもっております。

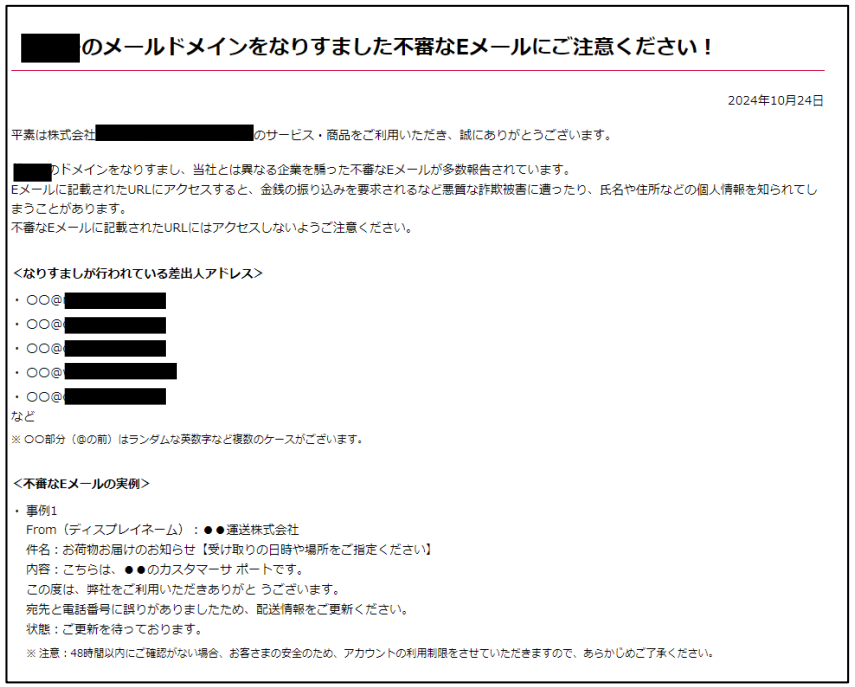
もし不審なメールを受信された場合は、メール内にあるURLやボタンを絶対にクリックしないでください。万が一クリックした場合も、メールアドレスやパスワード等の個人情報は入力しないようご注意ください。

<今回のなりすましメールを受信しないための設定方法>
==========
※弊社のドメインを受信拒否すると今後公式からのメールが一切届かなくなるため、以下の対応をお願いいたします。

■ Gmail / Yahoo!メール / Outlook.com（旧 Hotmail）をご利用の方

Gmail / Yahoo!メール / Outlook.com（旧 Hotmail）は標準で「なりすましメール対策」に対応しているためお客様のほうで対策する必要はありません。

■ NTT ドコモをご利用の方



[redacted]のメールドメインをなりすました不審なEメールにご注意ください！

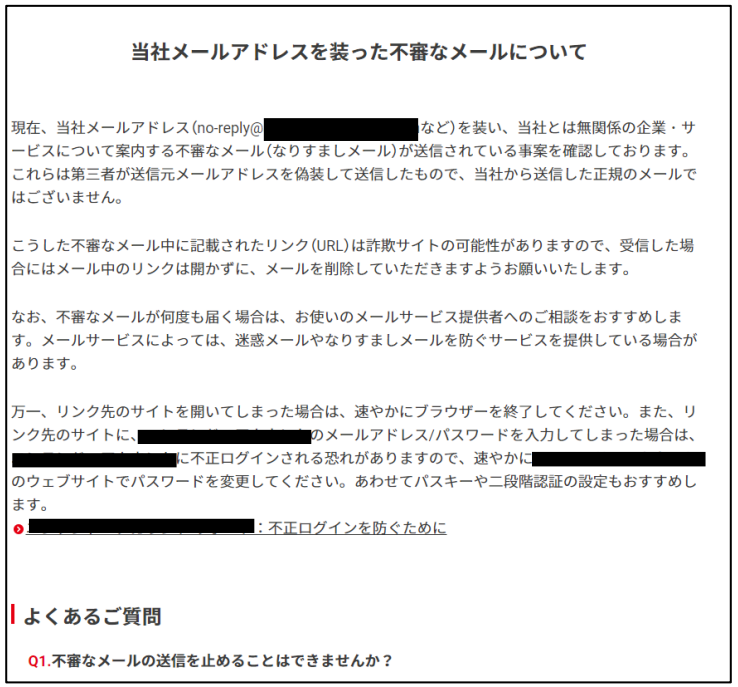
2024年10月24日

平素は株式会社[redacted]のサービス・商品をご利用いただき、誠にありがとうございます。

[redacted]のドメインをなりすまし、当社とは異なる企業を騙った不審なEメールが多数報告されています。
Eメールに記載されたURLにアクセスすると、金銭の振り込みを要求されるなど悪質な詐欺被害に遭ったり、氏名や住所などの個人情報を知られてしまうことがあります。
不審なEメールに記載されたURLにはアクセスしないようご注意ください。

<なりすましが行われている差出人アドレス>
・○○@[redacted]
・○○@[redacted]
・○○@[redacted]
・○○@[redacted]
・○○@[redacted]
など
※○○部分（@の前）はランダムな英数字など複数のケースがございます。

<不審なEメールの実例>
・事例1
From（ディスプレイネーム）：●●運送株式会社
件名：お荷物お届けのお知らせ【受け取りの日時や場所をご指定ください】
内容：こちらは、●●のカスタマーサ ポートです。
この度は、弊社をご利用いただきありがと うございます。
宛先と電話番号に誤りがありましたため、配送情報をご更新ください。
状態：ご更新を待っております。
※注意：48時間以内にご確認がない場合、お客さまの安全のため、アカウントの利用制限をさせていただきますので、あらかじめご了承ください。



当社メールアドレスを装った不審なメールについて

現在、当社メールアドレス(no-reply@[redacted]など)を装い、当社とは無関係の企業・サービスについて案内する不審なメール(なりすましメール)が送信されている事案を確認しております。これらは第三者が送信元メールアドレスを偽装して送信したもので、当社から送信した正規のメールではございません。

こうした不審なメール中に記載されたリンク(URL)は詐欺サイトの可能性がありますので、受信した場合にはメール中のリンクは開かずに、メールを削除していただきますようお願いいたします。

なお、不審なメールが何度も届く場合は、お使いのメールサービス提供者へのご相談をおすすめします。メールサービスによっては、迷惑メールやなりすましメールを防ぐサービスを提供している場合があります。

万一、リンク先のサイトを開いてしまった場合は、速やかにブラウザーを終了してください。また、リンク先のサイトに、[redacted]のメールアドレス/パスワードを入力してしまった場合は、[redacted]に不正ログインされる恐れがありますので、速やかに[redacted]のウェブサイトでパスワードを変更してください。あわせてパスキーや二段階認証の設定もおすすめします。
[redacted]：不正ログインを防ぐために

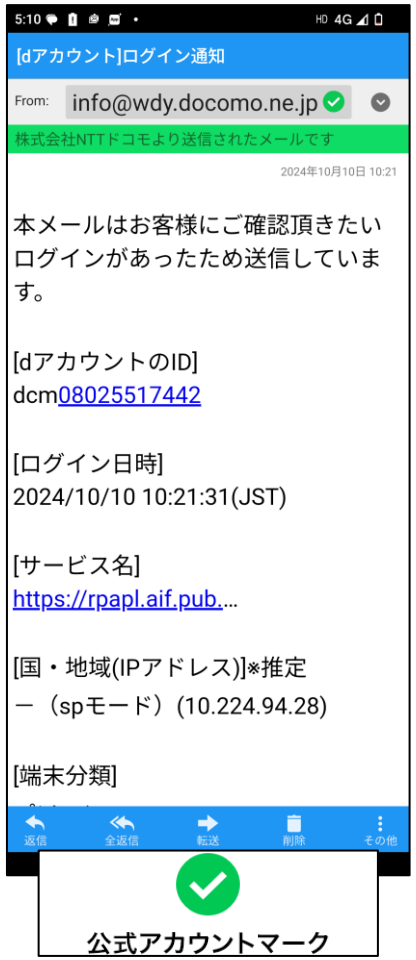
よくあるご質問

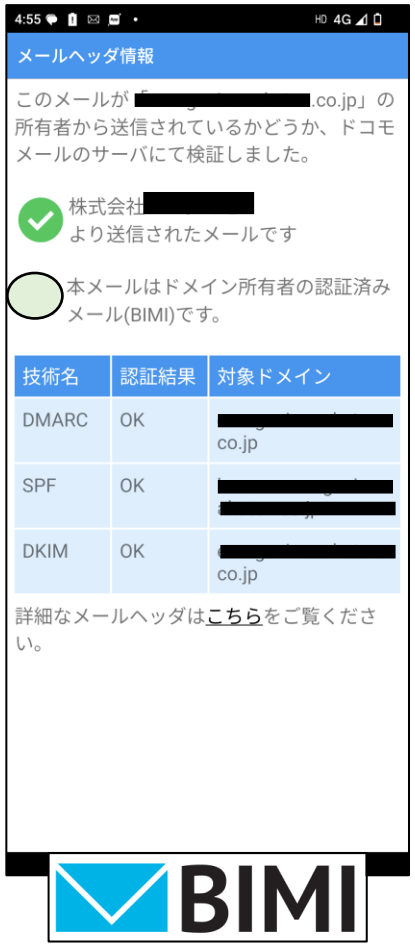
Q1.不審なメールの送信を止めることはできませんか？

踏み台をされた企業における広報の例

p=quarantine/rejectと併せて

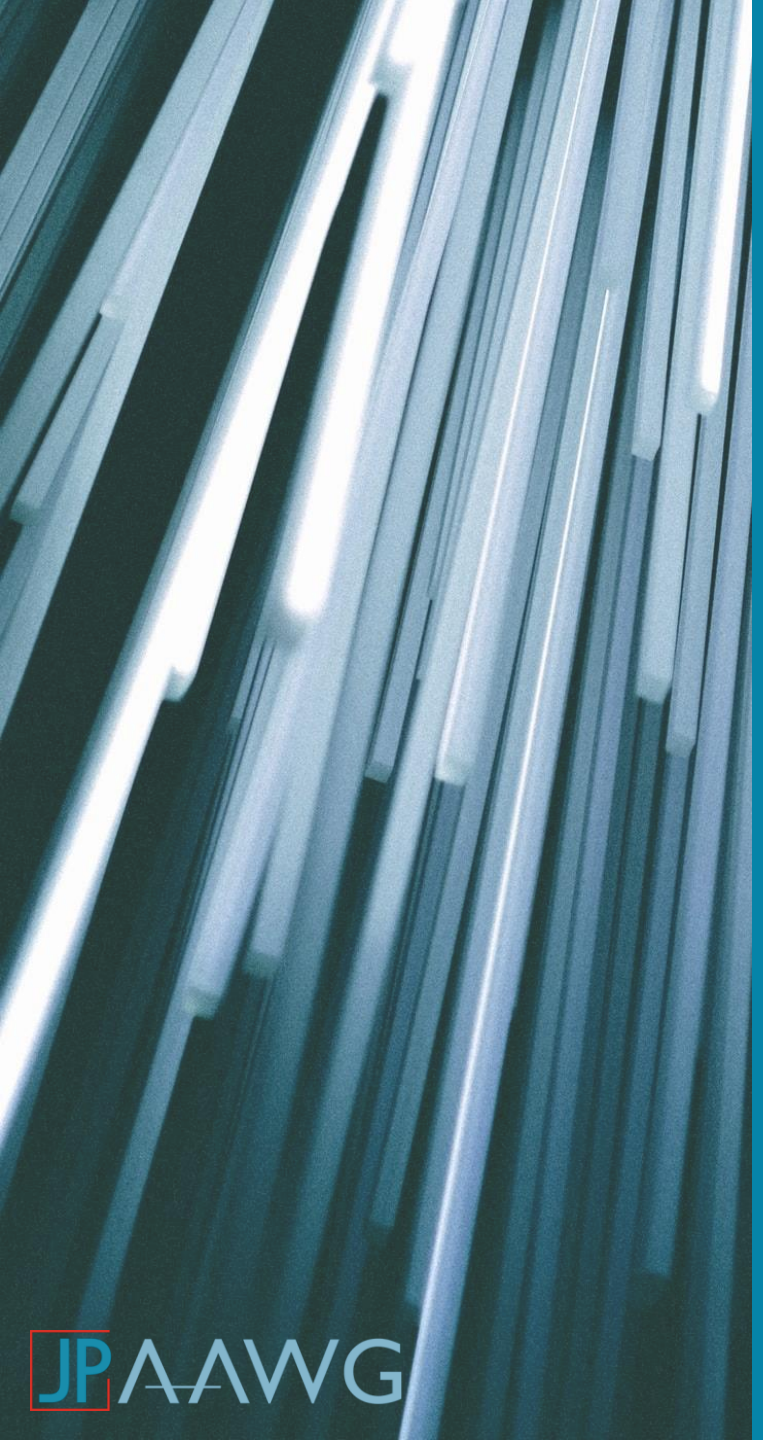
正規メールのPRを行い、**あんしん・安全の訴求**を！





まとめ

- DMARCの**p=noneは順調**に普及！
- **次はp=quarantine/reject**を導入すべき！
- 並行して、**正規メールのPR**も！



キャリアメールのDMARC 発信者としてのDMARC

中島 直規

KDDI株式会社

JP AAWG

日本におけるキャリアメールとは

キャリアメールの価値とは？

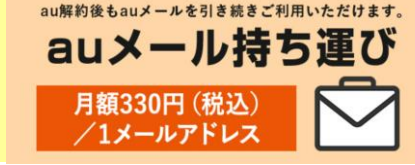
「一番長く使っている個人メアド」

⇒　キャリアメールアドレスしか知らない旧知の間柄の唯一の連絡手段

「フリーメールにはない、“保証されているメアド”である価値」

⇒　“有料契約に紐づくメアド”としては国内随一

【3キャリア通信端末契約数】
約9,800万回線
（2023年12月末現在／廉価プラン・MVNOを除く）



【キャリアメールの利用用途の中心は “CtoC” から”BtoC” へ】

個人間コミュニケーションはOTTやプラスメッセージに移行が進む

しかし、登録しているECサイトや保険会社、銀行・・・からの「BtoC」用途は継続

BtoCがメインになってきた今だからこそ、
発信者の皆様のメールを、すべてのお客様へ安全に届けることが必要

JPAAWG

auメールの迷惑メール対策の歩み

迷惑メール社会問題化以降、SPFを始めとした機能を順次強化
2013年に「迷惑メールおまかせ規制」としてデフォルトONへ
2023年12月、DMARC・BIMIの導入によりフィッシング対策をさらに強化

2000年頃～

拒否機能を順次強化

サーバ対応
- 各種拒否機能（指定拒否等）
  SPF／SenderID認証

キャリアメールはSPF/SenderIDを武器に迷惑メール対策を強化

アプリ対応
- メーラでの拒否登録簡素化

手動拒否登録をワンタッチで可能に

2013年～

全てのお客様に自動検知

- 迷惑メールおまかせ規制
  デフォルトON

ほぼすべてのお客様で
迷惑メール対策機能を使って頂けるように

- 迷惑メール報告機能リリース

申告頂いたメールを迷惑メール対策に
利用し、迷惑メール対策ループを構築

迷惑メール申告機能（auメールアプリ）

2023年～

本格的なフィッシング対策

- 受信DMARC/BIMI対応

受信側対策としてDMARC/BIMI対応
送信側対策と合わせてよりセキュアへ！

- BIMIロゴ表示対応

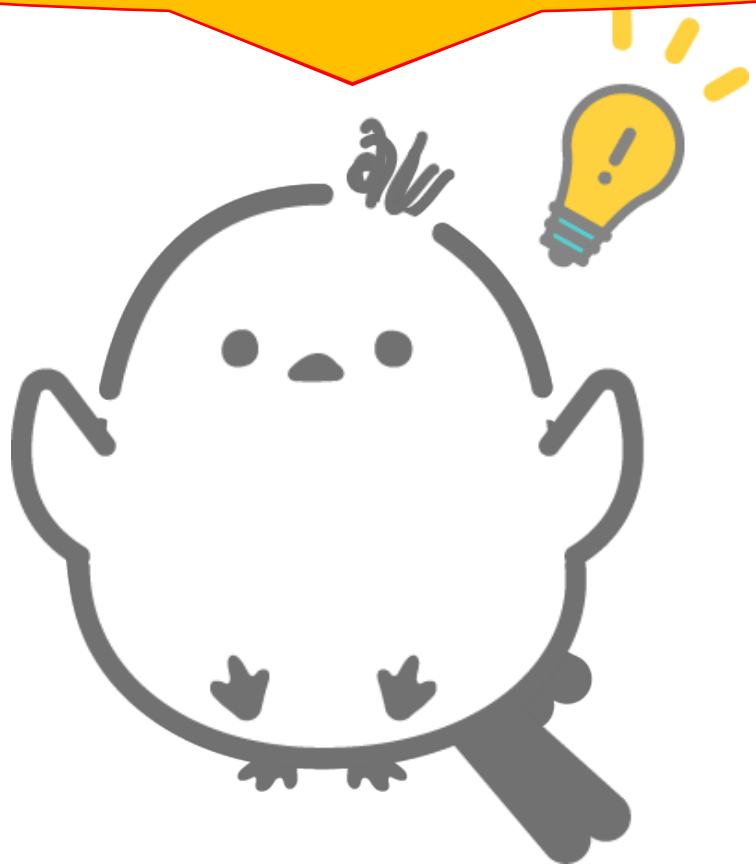
Android auメールアプリ

iPhone／iPadメールアプリ

JPAAWG

受信側としてだけではなく・・・

そうか！
たくさんのメールを「お届けする」立場としても、
しっかり取り組みを進めなければいけないんだ！



JPAAWG

auが発信するメールへのDMARC対応

au系ドメイン：通信／金融／各種サービスのサブドメイン多数

2023/10　全社横断でDMARC(p=reject)推進で方針決定
2024/02　p=reject化完遂へ

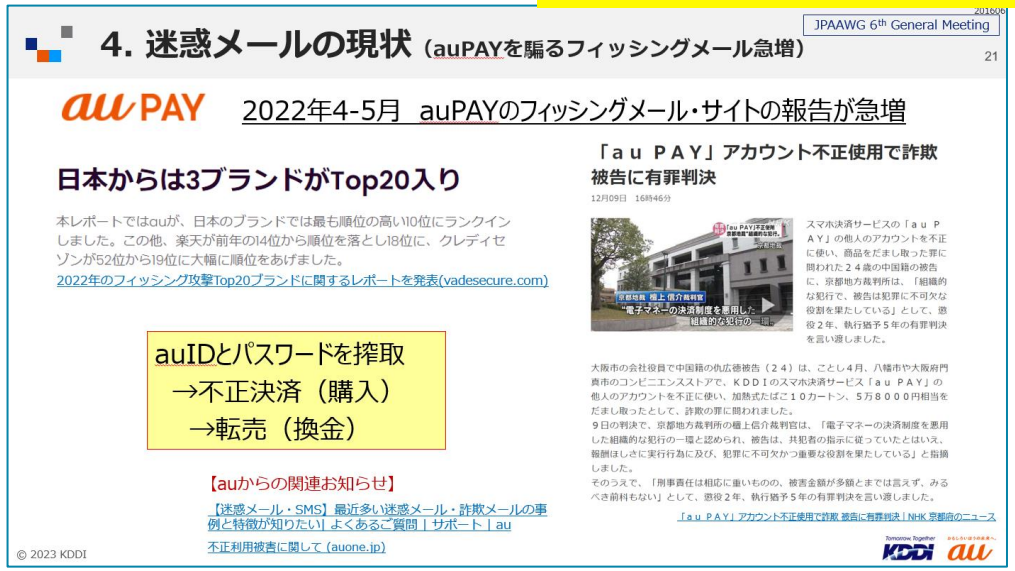
DMARC導入の背景と課題

DMARCレポート分析	お客様からの迷惑メール情報分析
詐称ドメイン多数・・・	**DMARCすり抜けメール増加傾向**

DMARC(p=reject)／BIMI導入

au主要ドメイン：au.com/ezweb.ne.jp/auone.jp
サブドメインを含め、全ドメインでDMARC reject化完了！

6th General-Meeting資料抜粋



金融やEC系業界等を中心にフィッシング被害が拡大
当社のau PAYなどもフィッシング詐欺の標的となった

p=reject完遂までの道のり（実態把握）

スタートライン（p=none）に立ったら、DMARCレポートを分析！
noneからquarantine/rejectへのポリシー強化を進めていく

スタートライン
p=none

まずは
実態を把握

社内布教活動
Let'sDMARC！

ML管理者への
OJT+設定変更

ポリシー強化
フェーズ

要対処ドメイン/ホスト
IP抽出

管理者
教育活動

メール配信設備
DMARC適切な設定へ

順次強化＆DMARC
レポート分析

DMARC設定
p=none

DAMRC設定
p=quarantine/reject
pct=XX 順次上げていく

まずは
実態を把握

【どれだけ悪用されてるの？緊急性と必要性を確認】
各ISPより届く「DMARC集約レポート」を収集・分析
①自社ドメインのなりすまし実態（通数等）を把握
②ドメインごとの対応要否／優先度を決定

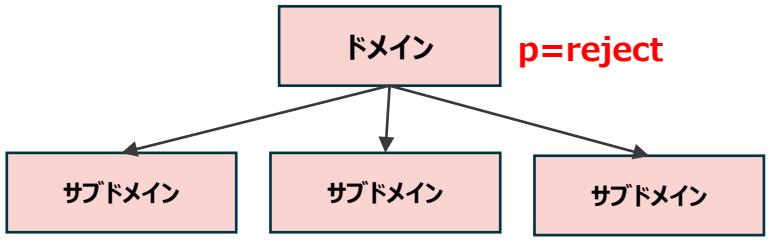
JPAAWG

サブドメインごとに進め方をコントロール

サブドメインごとの対応要否やスケジュールが分かれる場合でも、
細かくポリシー制御を行い着実にreject化を進めていくことが可能！

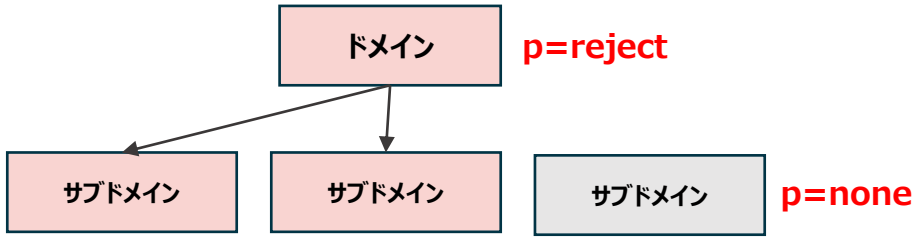
■DMARCポリシー仕様
・組織ドメインのポリシーは、その全てのサブドメインに適用される
・各サブドメインのポリシーが組織ドメインのポリシーよりも優先される

基本）すべてのサブドメインが同一ポリシーに



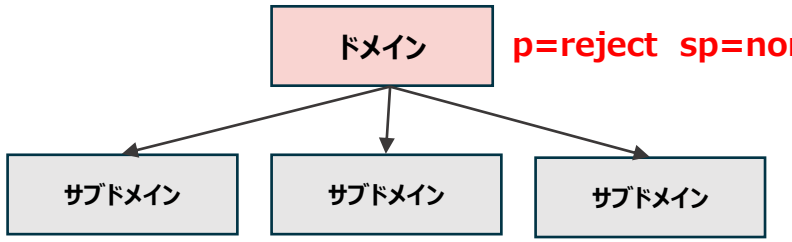
全てのサブドメインにp=rejectが適用される

例１）対処に時間がかかるサブドメインは個別に対処可



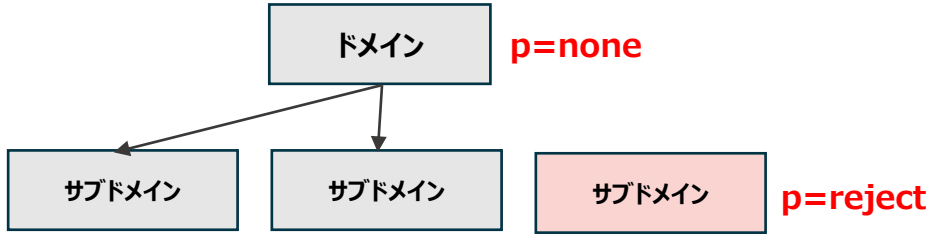
サブドメインにp=reject適用

例２）組織ドメインだけ先行してDMARC化



全てのサブドメインにnoneが適用される

例３）特定のサブドメインのみ先行してDMARC化



JPAAWG

p=reject完遂までの道のり（布教活動）

スタートライン（p=none）に立ったら、DMARCレポートを分析！
noneからquarantine/rejectへのポリシー強化を進めていく

スタートライン
p=none

まずは
実態を把握

社内布教活動
Let'sDMARC！

ML管理者への
OJT+設定変更

ポリシー強化
フェーズ

要対処ドメイン/ホスト IP抽出	管理者 教育活動	メール配信設備 DMARC適切な設定へ	順次強化＆DMARC レポート分析

DMARC設定
p=none

DAMRC設定
p=quarantine/reject
pct=XX 順次上げていく

社内布教活動
Let'sDMARC！

【社内メール管理者整列＆布教活動】
①まず配信メールリストを洗い出す（これが大変
②配信メールごとに管理者を探し出す（これも大変
③DMARCの趣旨を説明して（強制的に）賛同を得る
④DMARCを確実にPassする配信となるよう確認＆設定変更を促す

JPAAWG

p=reject完遂までの道のり（設備対応）

スタートライン（p=none）に立ったら、DMARCレポートを分析！
noneからquarantine/rejectへのポリシー強化を進めていく

スタートライン
p=none

まずは
実態を把握

社内布教活動
Let'sDMARC！

ML管理者への
OJT+設定変更

ポリシー強化
フェーズ

要対処ドメイン/ホスト IP抽出	管理者 教育活動	メール配信設備 DMARC適切な設定へ	順次強化＆DMARC レポート分析

DMARC設定
p=none

DAMRC設定
p=quarantine/reject
pct=XX 順次上げていく

ML管理者への
OJT+設定変更

【配信メールごとの設定変更完遂】
①管理者に対してDMARC Passになるよう設定の勉強会実施
②管理者に責任をもって状況確認＆設定変更依頼、完了まで管理
③（少なくともサブドメインごとに）「完了！」を宣言してもらう

JP AAWG

p=reject完遂までの道のり（ポリシー強化）

スタートライン（p=none）に立ったら、DMARCレポートを分析！
noneからquarantine/rejectへのポリシー強化を進めていく

スタートライン
p=none

まずは
実態を把握

社内布教活動
Let'sDMARC！

ML管理者への
OJT+設定変更

ポリシー強化
フェーズ

要対処ドメイン/ホスト IP抽出	管理者 教育活動	メール配信設備 DMARC適切な設定へ	順次強化＆DMARC レポート分析

DMARC設定
p=none

DAMRC設定
p=quarantine/reject
pct=XX 順次上げていく

ポリシー強化
フェーズ

【順次強化し、最終ゴールへ！】
①管理者による対応完了サブドメインごとにp=quarantine
適用率を「pct=10」⇒「50」⇒「100」等、順次強化していく
DMARC集約レポートで分析を継続しつつ、アクセルを踏む
②完了したら次は「p=reject」 ⇒ 完遂へ！

※DMARC次期ドラフトVerにてpctパラメータ削除の可能性あり
早期のReject化がカギです！

JPAAWG

更なる安心へ：BIMI対応

【BIMI対応の推進】

p=reject化まで完遂したら･･･「BIMI導入」まであと少しです。
BIMI対応をぜひ実現し、安心なメールをお届けして頂きたい！
auメールは2023/12にBIMIを導入済み。
500ドメインを越える送信者のメールでロゴ表示されています！

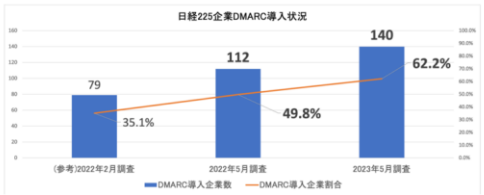
6th General-Meeting資料抜粋

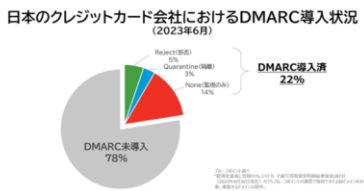
6. auメールの迷惑メール対策まとめ (Let's DMARC/BIMI！)

JPAAWG 6th General Meeting　30

【DMARC/BIMI導入を推進しましょう！】

p=noneを含めても、導入率は日経225企業「62%」、クレカ会社はなんと「22%」
⇒「none定義＋統計レポート受信」 ⇒ 「Ruaレポートから分析」
⇒「quarantine」 ⇒ 「reject」 ⇒ **「BIMIロゴ表示」**
⇒ **安心安全なメール環境の実現へ、皆様のご協力を**





TwoFive、なりすましメール対策実態調査の最新結果を発表 | ニュース＆プレスリリース | TwoFive (twofive25.com)
フループポイントの調査により、日本のクレジットカード会社の７８%がなりすましメール詐欺に有効な対策を取っていないことが判明 | Proofpoint JP

© 2023 KDDI

昨年のJPAAWGでも言っていました･･･

6th General-Meeting資料抜粋

5. auの新たな取り組み(BIMI導入で期待される効果)

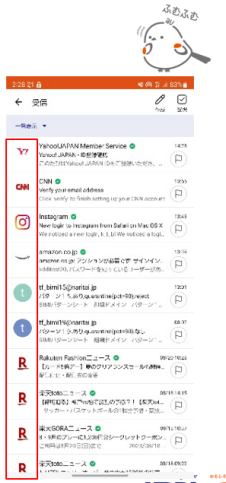
JPAAWG 7th General Meeting　23

BIMIに取り組んでいる（＝DMARCポリシーが強い）
⇒ すなわちフィッシングメール対策に進んで取り組んでる送信者
これら送信元メールの正規メールに「ロゴを表示できる」

BIMI導入効果！

「送信者ロゴ＝メール一覧画面において最初に目に入る情報」
「正しいメール」であると認識率アップが見込まれる ※送信者メリット
(ITリテラシーに依存せず)一律に安全を訴えられる ※受信者メリット

悪意のある攻撃者が「BIMI対応」する障壁の高さ（※）により
BIMI対応事業者はフィッシング送信者からは"避けられる"
（≒BIMI非対応事業者が狙われる確率があがる）
※VMC証明書の発行には厳格な審査＋ロゴ商標登録が必須



© 2023 KDDI

BIMIはセキュリティ対策である「と同時に」
「安心できるメール」として開封率が上がった報告も。
マーケティング対策の側面もあるかもしれません！

JPAAWG

まとめ

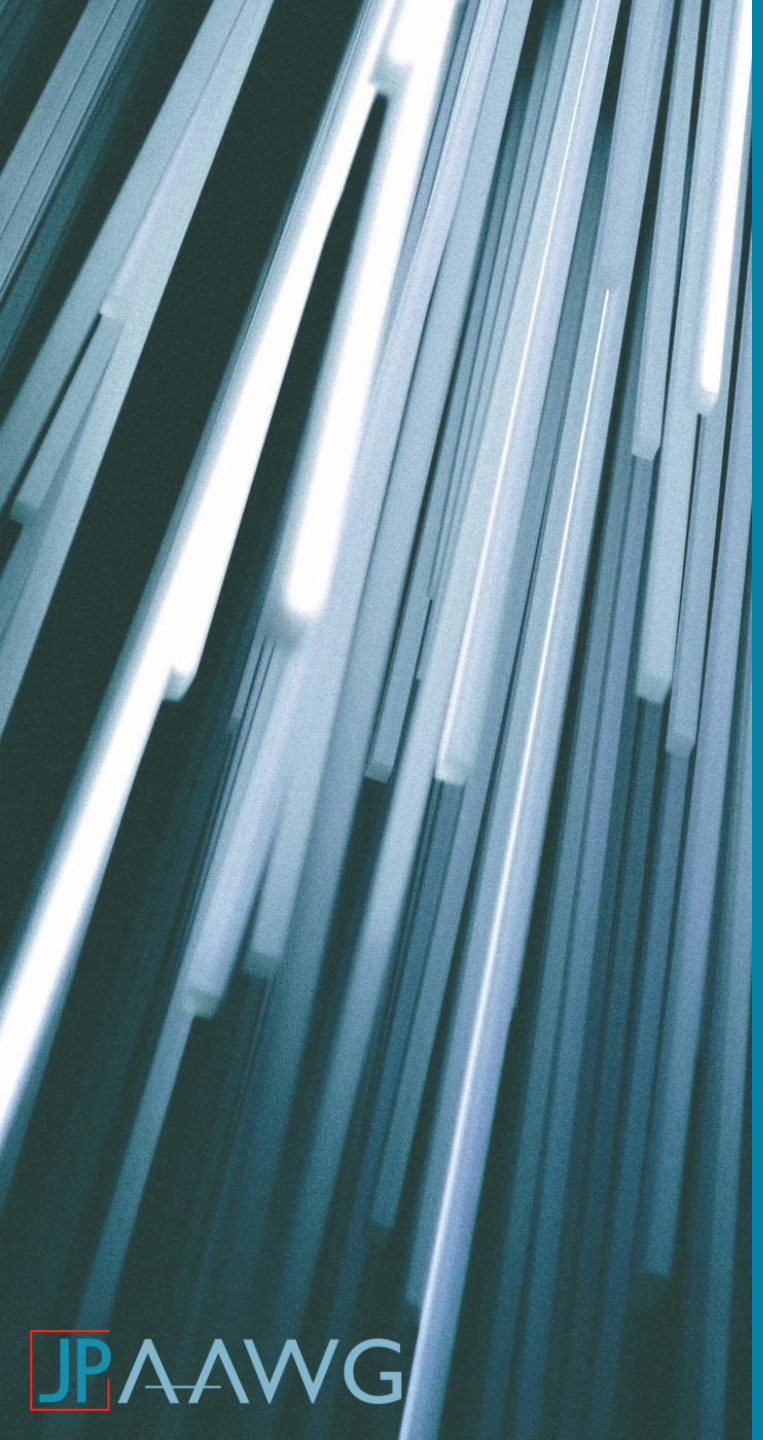
・キャリアメールは国内1億人のDMARC対応メール

・DMARC　みんなでReject　目指しましょう！（字余り

・Reject化は（少し大変だけど）怖くない！
　結構あっさり実現できます！

・Reject化終われば次はBIMIで正規メールアピールを！

by KDDI
（懐かしい



なりすましメールを撲滅

熊沢 明生
ソフトバンク株式会社

JPAAWG

6月フィッシング詐欺被害を減らすために国も動いた！

犯罪対策閣僚会議にて岸田総理から直々に提言

フィッシングを防止するための送信ドメイン認証技術を導入・促進を強力に進める！！

フィッシング対策

- **送信ドメイン認証技術（ＤＭＡＲＣ等）への対応促進**
  - 利用者にフィッシングメールが届かない環境を整備するため、インターネットサービスプロバイダー等のメール受信側事業者や、金融機関等のメール送信側事業者等に対して、送信ドメイン認証技術の計画的な導入を要請
- **フィッシングサイトの閉鎖促進**
- **フィッシングサイトの特性を踏まえた先制的な対策**
  - フィッシングサイトが有する、１つのＩＰアドレス上に複数のサイトが構築されるなどの特性を踏まえ、いまだ通報がなされていないフィッシングサイトを把握して、ウイルス対策ソフトの警告表示等に活用するなどを検討

※出典：首相官邸　令和6年6月18日犯罪対策閣議会議資料

なりすましメール

社会問題となっているフィッシングメール
その多くになりすましメールが悪用**されている**

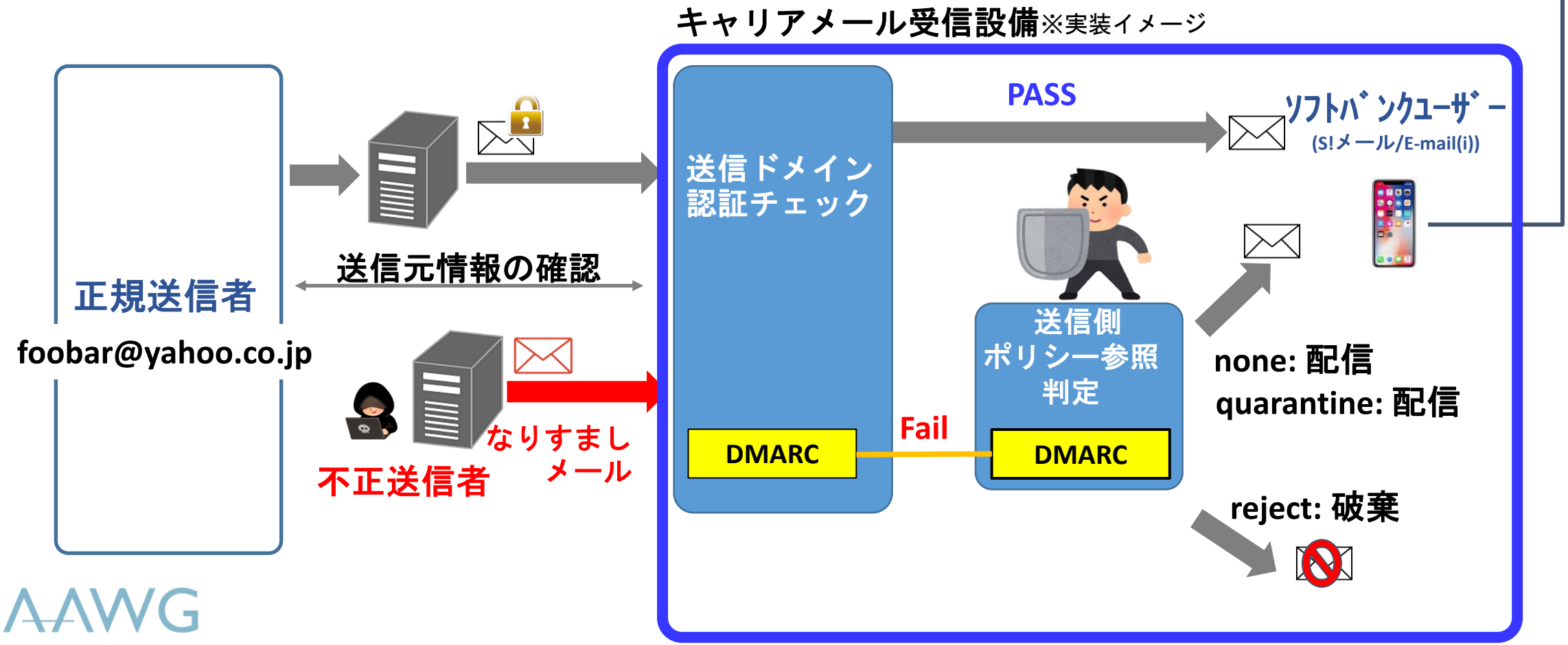
調査用メールアドレス宛に8月に届いたフィッシングメールのうち、
約７７．１%がメール差出人に実在するサービスのメールアドレス(ドメイン名)を使用した「なりすまし」フィッシングメール

※出展：フィッシング協議会 2024/08フィッシング報告状況より抜粋

DMARCフィルタ

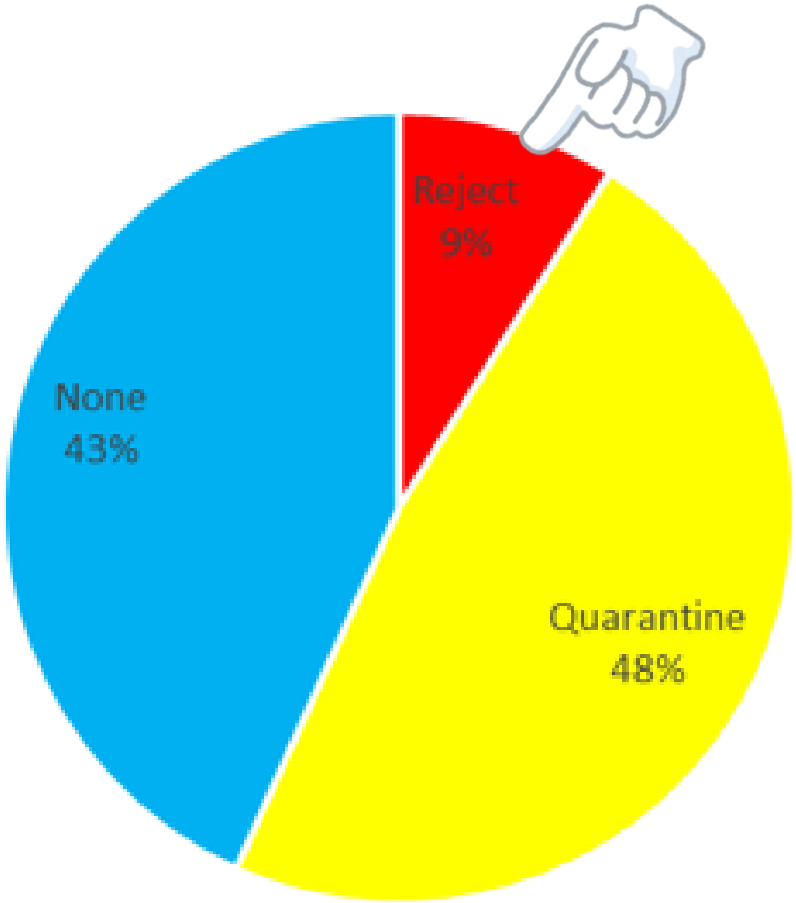
通信キャリアで導入済み
しかもデフォルトON！高設定率！

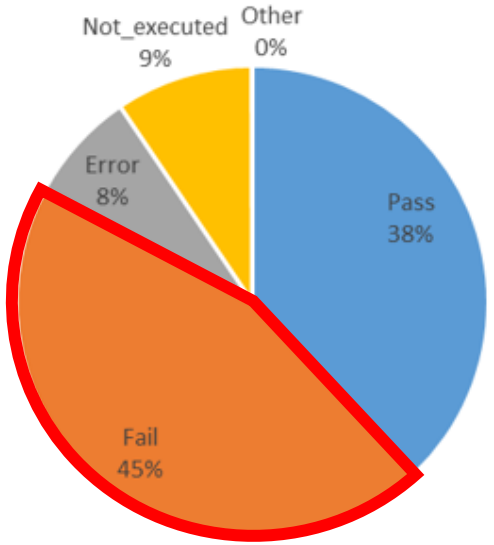
MySoftBank
なりすましメール拒否設定
利用する(初期値)
利用しない



DMARCフィルタ導入完了

reject宣言はまだまだ少ない・・





認証Failの効果が薄い・・

p＝reject

絶大な効果あり！！

DMARCポリシーをrejectに変更したことで
なりすましメールのブロック件数急増！！
さらに、**なりすましメール通数自体が減少！！**

送信DMARC

送信側で何をすればいいの？

【送信DMARCで対応してほしいこと】

・DMARC-SPF or DMARC-DKIMがPassすること

・DKIM対応は必須ではありませんが可能なら署名を推奨

　BIMI表示を希望する方はDKIM署名が必須

・**DMARCポリシーは「reject」**

ここ重要！！

繰り返しますが・・

p＝noneは効果がない

ポリシー変更前はすり抜けていた

DMARCポリシー強化

ソフトバンクもポリシー強化 rejectが目標！！

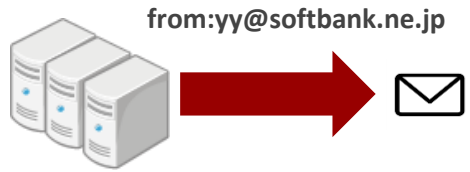
ドメインが多く分析が大変

@softbank.ne.jp
@i.softbank.jp
@t.vodafone.ne.jp
@k.vodafone.ne.jp
:
:
（計31ドメイン）
他社DNS管理のドメインも…

全利用ドメインの洗い出しを忘れずに！

キャリアメール以外でのメール送信

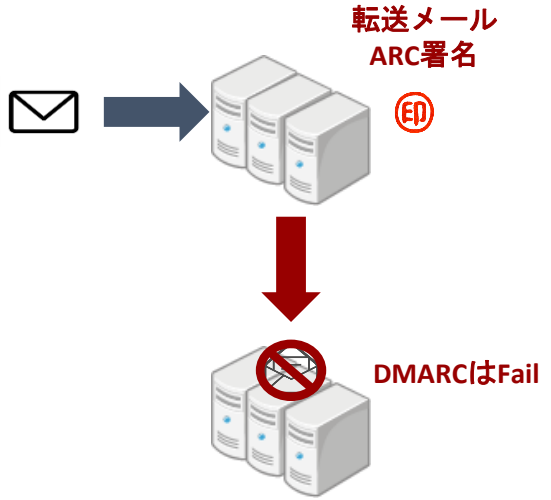
キャリアメールサーバ



他サービスサーバ

他システムでのドメイン利用に注意！

転送メールにはARC署名



転送先でARC対応必要

JPAAWG

まとめ

①なりすましドメインとして実在するサービスのドメインが悪用されている

・金融、宅配、決済可能なキャリアや企業のドメインが悪用されていたが、

フリマ系、某大手倉庫店のドメインを悪用するパターンも増加傾向

②キャリアでDMARCフィルタ導入

・**国内3キャリアはデフォルトON！1億ユーザーが適用中！！**

・**DMARCポリシーを「reject」に変更するだけで大きな効果**

ここ重要！！

③転送メールサービスはARC署名で対策！？

・受信側ARCに対応する企業は増えるのか？

Thank you for your listening!