

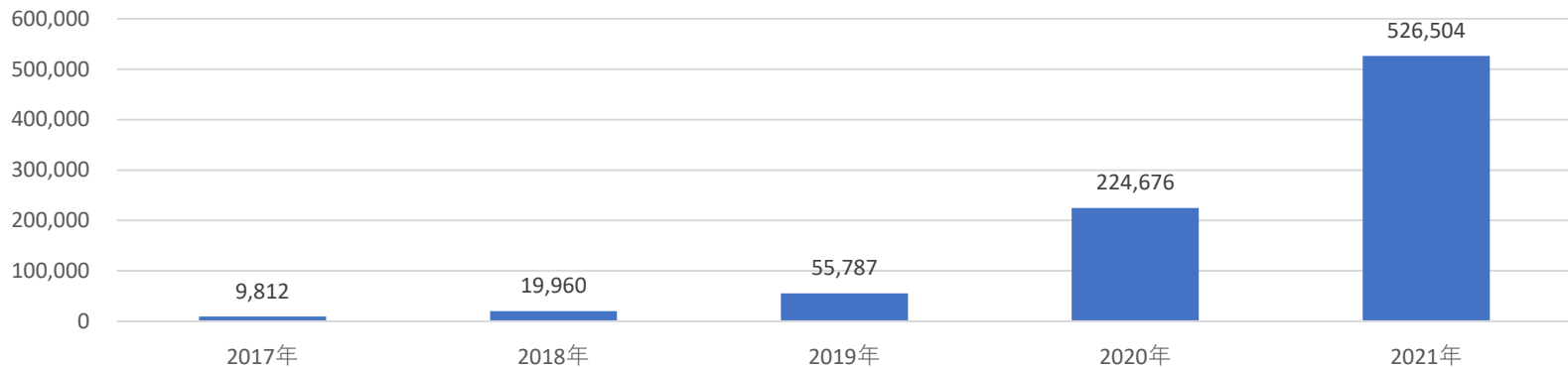
フィッシング対策への取組

警察庁サイバー警察局
サイバー企画課
令和4年11月15日

D M A R Cの導入背景

1 フィッシングの増加

フィッシング報告件数の推移



フィッシング対策協議会(<https://www.antiphishing.jp/>)月次報告書より作成

2 フィッシングによる被害例

- ◆ キャッシュレスサービス運営会社を装ったメールにより偽サイトに誘導されてID・パスワード等が盗み取られ、不正な決済が行われた。(令和3年9月)
- ◆ メモアプリの運営者を装ったメールにより偽サイトに誘導されてID・パスワードが盗み取られ、メモアプリ内に記録していたインターネットバンキングのID・パスワードを悪用されて不正送金された。(令和3年5月)
- ◆ 大手通販サイトを装ったメールにより偽サイトに誘導されてクレジットカード情報等が盗み取られ、ECサイトで不正決済が行われた。(令和3年5月)

民間事業者、関係機関等と連携したフィッシング対策

1 フィッシング問題への取組に関する意見

- ◆ 金融機関やE Cサイト等を装った電子メールやS M Sを送り、ログインID、パスワード、クレジットカード番号等の個人情報を詐取する行為が増加
- ◆ 令和2年12月3日消費者委員会「フィッシング問題への取組に関する意見」
 - 1 フィッシングメールの受信防止対策の普及促進及び効果検証
 - 2 不正アクセス禁止法等に基づく取締りの強化
 - 3 消費者への注意喚起の一層の強化

2 民間事業者、関係機関等と連携した対策の推進

- ◆ 警察が把握したフィッシングサイト等に関する情報をウイルス対策ソフト事業者等に提供するほか、関係団体等と連携し、民間事業者に対して、送信ドメイン認証技術（DMARC等）の導入等のなりすましメール対策を講じるよう働き掛ける。

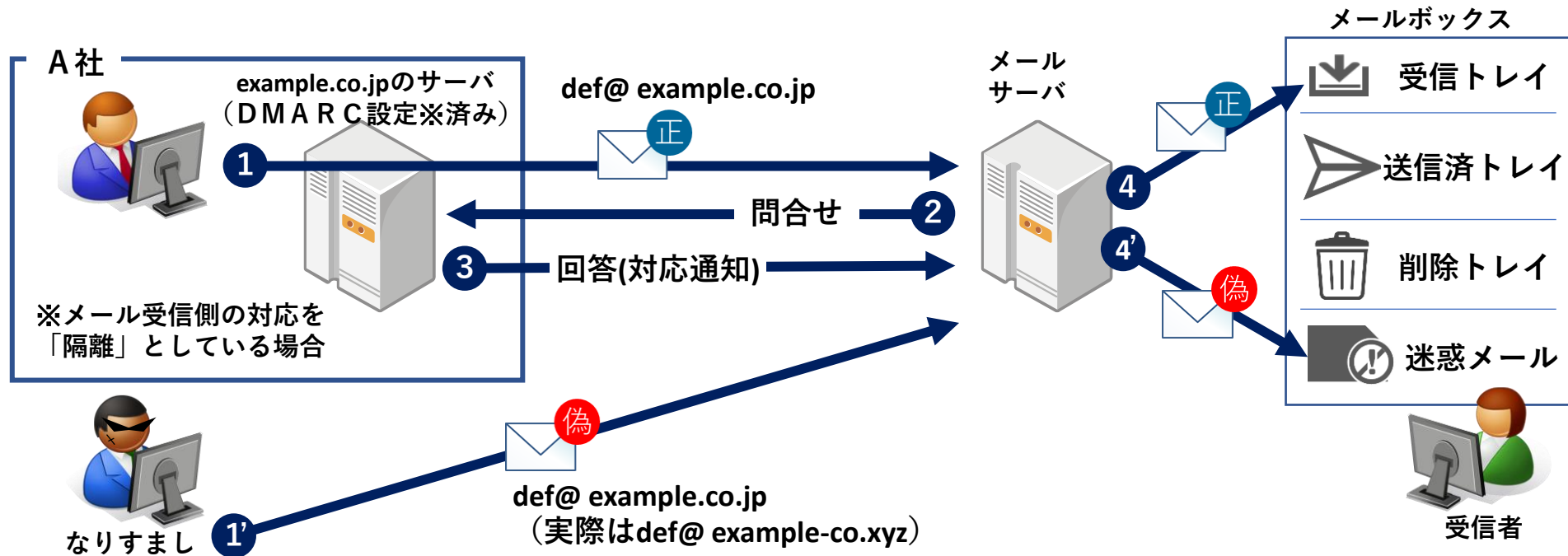
【具体的事例】

- 令和4年9月 金融庁と連携して銀行関連団体へ働き掛け
- 令和4年10月 総務省と連携して通信事業者へ働き掛け

DMARCの仕組みの概要

DMARCを導入することにより、なりすましメールを迷惑メールフォルダに隔離（quarantine）したり、メールボックスに到達させない（reject）ようにすることができます。

下図は、隔離の際の仕組みの概要について説明しています。



正規メール の場合

- 1 正規のメール を送信
- 2 A社のサーバに問合せ
- 3 A社のサーバが回答
- 4 は受信トレイに

なりすましメール の場合

- 1' なりすましメール を送信
- 2 A社のサーバに問合せ
- 3 A社のサーバが回答
- 4' は迷惑メールフォルダに (隔離)

導入の経緯

- 2017年頃、同社を騙ったフィッシングメールを認知
- ホームページでの注意喚起とともに抜本的な対策としてD M A R C 対応を検討

事前準備

- 企業内で使用しているメール棚卸し【使用ドメイン、送信サーバ情報】

D M A R C の運用

- 最初はp=none（隔離も拒絶もしない）で情報収集
- 送られてくるレポート情報を分析
【社内から送信している正規なメールがFailになっていないか確認】
- Failになっている社内メールの設定を改善【S P F、D K I M設定の改善】
- 社内メールの設定改善が終了した時点でp=reject（破棄）設定

D M A R C の効果

- なりすましメールが減少【3 か月後に 8 割減少、最大時は 9 割以上減少】
- コールセンターへの顧客からの問合せが減少【3 か月後に 8 割減少】

D M A R C について

- 顧客を守るための企業の責任、姿勢を示す意味でもD M A R C 対策は必要
- 企業内で使用するメールに関する継続的なガバナンスが必要

導入の経緯

- 2018年頃、同社サービスを騙ったなりすましメールを認知
- 送信ドメイン認証とブランドマーク表示サービスへの対応を開始

対応の状況

- 2018年4月 D M A R C / D K I M対応開始（p=none）
- 2018年10月 ヤフーメールのブランドアイコン表示に対応
- 2021年5月 ドコモメール公式アカウントに対応
- 2021年8月 D M A R C破棄設定対応（p=reject）
- 2021年12月 B I M I（ブランドロゴ表示・証明書設定サービス）対応開始

D M A R Cの運用

- 最初はp=none（隔離も拒絶もしない）で情報収集
- 【社内から送信している正規なメールがFailになっていないか確認】
- Failになっている社内メールの設定を改善【S P F、D K I M設定の改善】
- 社内メールの設定改善が終了した時点でp=reject（破棄）設定
- D M A R Cレポートの分析は、エクセルからクラウドサービス利用に移行

導入に係る苦労点

- Rejectによる被害抑止のメリットとメール不達（可能性）によるデメリットを比較して事業判断を下すのが難しい
- レポートを分析するには、D M A R Cを理解する人員の確保が必要

DMARCの効果

- コールセンターへの顧客からの問合せが最大9割減少
問合せの内8割がメール関連だったが、少ない月は2割未満まで減少
- なりすましメール総数が少ない月は前年比9割減少

DMARCについて

- DMARCを導入してもなりすましメールの全てがなくなるわけではない
無関係なドメインを使ったなりすましメールはDMARCでは防げない
→ 併せてブランドマーク表示サービス（BIMI）への対応も重要
- 社内で顧客向けのメールを使っている部署が多い場合、経営層の理解と会社としての方向性を示す必要がある

DMARCの導入手順概要

1 SPF、DKIMの設定

送信元メールサーバ認証（SPF）及び電子署名の付与（DKIM）を設定

⚠ SPFのみを設定している場合は、DMARCの導入を慎重に検討（後述）

2 自社内のドメインの見直し

自社で使用するメールのドメイン、送信メールサーバ情報の棚卸し

3 DMARCの導入（試行）

受信側の振る舞い（DMARCポリシー）を【none（何もしない）】として運用開始

4 DMARCのレポート確認

自社からの正規なメールが認証失敗になっていないか確認

5 DMARCの本格運用

DMARCポリシーを【reject（拒否）】に設定し、なりすましメールを排除

（参考）送信ドメイン認証技術導入マニュアル【第3版】

DMARCを含めた送信ドメイン認証に関する技術的な導入マニュアルが、迷惑メール対策推進協議会から公表されています。

<https://www.dekyo.or.jp/soudan/aspc/report.html>



送信ドメイン認証技術
導入マニュアル

第3版 2021年9月
迷惑メール対策推進協議会



DMARCの導入に関する留意事項

1 法的な整理

【電子メールの受信サーバにおいて、電子メールの送信ドメインを認証し、認証できない場合は一定の措置を講ずる行為】は電気通信事業法第4条に規定する「通信の秘密」を「侵害する行為」に該当する。

しかし

メールサービス提供者において

フィルタリングサービスが顧客の有効な同意に基づいて提供される場合、ドメイン認証は正当業務行為に該当し、このことは、DMARC実施のために行われるドメイン認証行為においても同様である。

※顧客の有効な同意 ～ 以下の条件を満たす場合、約款等による包括同意が有効

- ・利用者が、随時、任意に設定変更できること
- ・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
- ・同意の対象・範囲が明確にされていること
- ・レポートを送信する場合、レポートの内容に本文及び件名が含まれないこと
- ・DMARCの内容について、事前の十分な説明を行うこと

総務省「送信ドメイン認証技術等の導入に関する法的解釈について」
(https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail/legal.html)

D M A R Cの導入に関する留意事項

2 受信側の転送設定時の動作

D K I Mを導入していない場合、受信者がメール転送設定をすると「なりすましメール」と判定される。したがって、S P Fのみを設定している場合には、D M A R Cの導入を慎重に検討する必要がある。

A 社

example.co.jpのサーバ
(D K I M設定なし)

1



転送設定

2



メール
サーバ



メールボックス



受信トレイ



送信済トレイ



削除トレイ



迷惑メール

※メール受信側の対応を
「隔離」としている場合

転送メール



の場合

1

正規のメール



を送信

2

正規のメール



を転送

3'

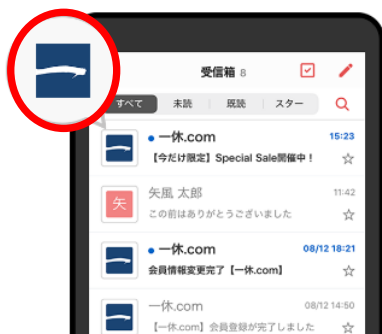


送信元が異なるのでなりすましと判定



【参考】公式ブランドマークについて

ヤフーブランドアイコン

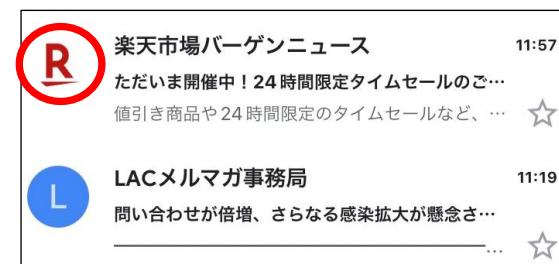


ドコモメール公式アカウント



BIMI

(Brand Indicators for Message Identification)



提供元	ヤフー株式会社	株式会社NTTドコモ	Google	Apple
対応ソフト	Yahoo!メール	ドコモメール	Gmail	iOSメールアプリ
判定	SPF又はDKIM	SPF又はDMARC	DMARC	DMARC
提供開始	2022/1	2021/5	2021/7	2022/9
登録料金	無料	無料	ドメインごとに VMC（認証マーク証明書）登録料	