2025年11月20日
Internet Week 2025 オンライン

H3 なりすましメールとDMARCを考える フィッシングメールの配信状況 （2025年版）

JPCERTコーディネーションセンター
フィッシング対策協議会 事務局
平塚 伸世

フィッシング対策協議会と JPCERT/CCの活動

フィッシング対策協議会の組織概要

- 設立
  - 2005年4月
- 名称
  - フィッシング対策協議会／Council of Anti-Phishing Japan
  - https://www.antiphishing.jp/
- 目的
  - フィッシング 詐欺に関する事例情報、技術情報の収集および提供を中心に行うことで、**日本国内におけるフィッシング詐欺被害の抑制を目的**として活動
- 構成
  - セキュリティベンダー、オンラインサービス事業者、金融・信販関連など
  - **会員＋オブザーバー：140組織**（2025年10月時点）
    （正会員：110社、リサーチパートナー：6名、関連団体：17組織、オブザーバー：7組織）
- 事務局
  - 一般社団法人JPCERTコーディネーションセンター

JPCERT/CCの組織概要

- 一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）

  Japan Computer Emergency Response Team / Coordination Center

  https://www.jpcert.or.jp/

- 国内における“火消し”の役割

  ⇒「脆弱性情報ハンドリング」「情報発信」「インシデント対応」

- 国際間・国内連携における“窓口”の役割

  ⇒「コーディネーションセンター（CC）」

フィッシング対策協議会事務局は、
国内連携、コミュニティー支援を担当している

フィッシング対策協議会におけるJPCERT/CCの活動

一般

事業者
被害組織
対策組織

報告

国内外関係組織との情報連携

フィッシング対策協議会
Council of Anti-Phishing Japan

JPCERT CC®

サイト閉鎖調整

ISP等

URL提供

対策組織

■情報発信
- 緊急情報（事例掲載）
- 月次報告書
- フィッシングに関するニュース
- フィッシング対策ガイドライン改定（WG活動）
- フィッシングレポート等

■会員間の情報交換および啓発活動
- 総会
- フィッシング対策勉強会（年2～3回）
- フィッシング対策セミナー（年1回）
- 各種WG活動
- 「Stop.Think.Connect.」等

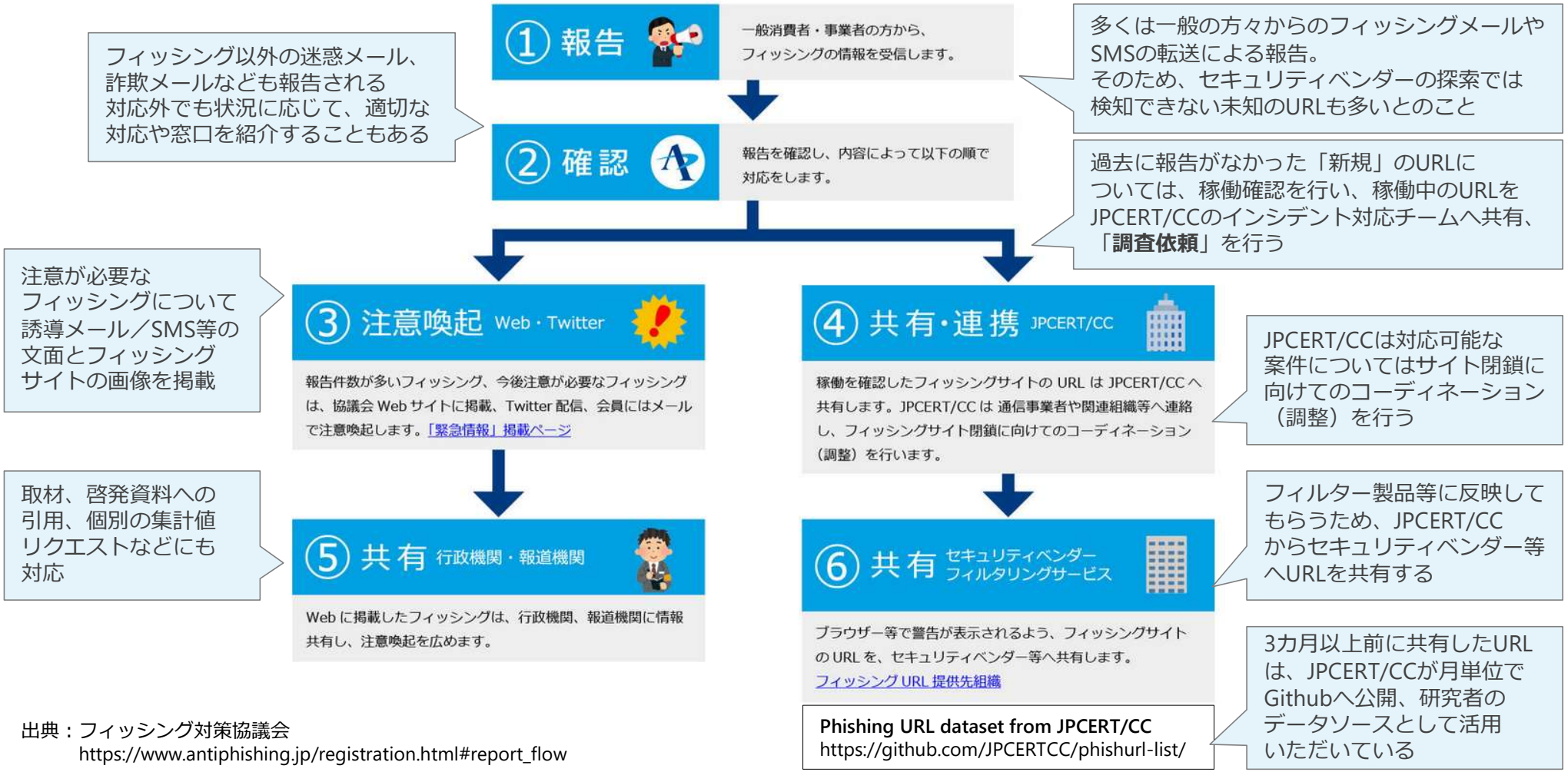
■学術研究
- 順天堂大学、香川大学

フィッシング報告受付窓口は
JPCERT/CCが行っています

本日は、一般の方々から
この窓口へ寄せられた報告を
もとにお話しします

JPCERT/CCは経済産業省から委託を受けた「サイバー攻撃等国際連携対応調整事業」の一環として、下記の業務を支援
- フィッシング報告受付、サイト閉鎖調整
- URL提供
- 情報発信、広報活動
- 被害組織、対策組織との情報連携等

フィッシング報告受領後の情報活用の流れ



出典：フィッシング対策協議会
https://www.antiphishing.jp/registration.html#report_flow

参考資料：フィッシング対策協議会 情報発信

- 緊急情報（事例掲載）

  https://www.antiphishing.jp/news/alert/

  一般への影響度が高い（報告が多い、ユーザー数が多い）
  フィッシングの誘導文面とサイト画像を掲載

フィッシングの最新事例を掲載！

いつもありがとうございます。
現在、総務省統計局では「2025年国勢調査」を実施しております。
この調査は、我が国の将来を左右する重要な統計資料を作成するための基礎となるものです。

本調査は全世帯を対象とした義務調査であり、すべての方にご回答いただく必要があります。
まだ未回答の方は、以下の期日までに必ずご協力をお願いいたします。

【回答期限】：2025年9月20日

期間内にご回答いただいた方には、記念品（数量限定）を進呈いたします。
また、未回答のままですと、統計法第13条に基づき罰則の対象となる場合がございますのでご注意ください。

下記より、専用ページへアクセスし、国勢調査のご回答をお願いいたします：
【国勢調査専用ページ】
https://dc-an●●●●.com/kokuseis　<https://dc-an●●●●.com/kokuseis> など

スマートフォン・パソコンから簡単にご回答可能です。
皆さまのご協力を心よりお願い申し上げます。
――――――――――――――――
総務省統計局
――――――――――――――――

メール文面の例

出典：フィッシング対策協議会
「国勢調査への回答依頼をよそおうフィッシング (2025/09/22)」
https://www.antiphishing.jp/news/alert/kokusei_20250922.html

ご利用明細のお知らせ

客様

平素よりお世話になっております。
【三井住友カード】でございます。

ご利用日時：2024年08月27日 10:58
ご利用場所：ビックカメラ（通販・ネットショッピングを含む）
ご利用金額：90,919円

この度、客様のカードご利用明細をご確認いただきたくご連絡申し上げます。

以下のQRコードをスキャンして使用詳細を取得してください。

□の部分のリンク
<https://agre●●●●.top/>など

QRコードを長押しして認識するか、QRコードを保存して使用明細を確認してください。

万が一、ご不明な点やご質問がございましたら、弊社カスタマーサポートまでお気軽にお問い合わせください。

今後とも、どうぞよろしくお願い申し上げます。

敬具

【三井住友カード】
カスタマーサポートチーム
[東京都江東区豊洲2丁目2番31号 SMBC豊洲ビル]

メール文面の例

出典：フィッシング対策協議会
「QR コードから誘導するフィッシング (2024/08/28)」
https://www.antiphishing.jp/news/alert/qr_20240828.html

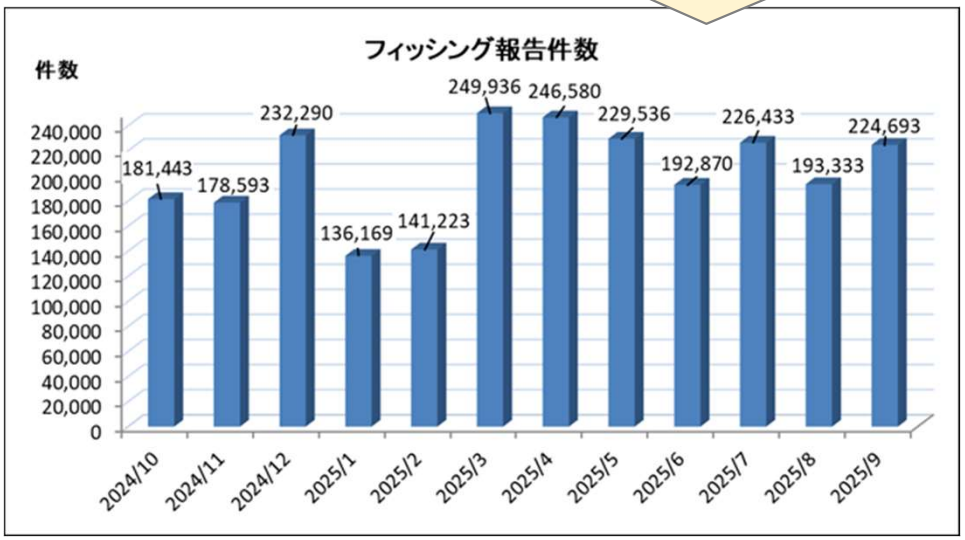
参考資料：フィッシング対策協議会 情報発信

- フィッシング報告状況 （月次報告書）
  https://www.antiphishing.jp/report/monthly/
  - 報告数、URL、ブランド
  - その月の傾向など、フィッシングの最新情報を掲載

フィッシングの傾向や手法は変化し続けており、
約3カ月から半年で大きく変化する
最新動向はここでチェック！

2025 年 9 月のフィッシング報告件数は 224,693 件となり、2025 年 8 月と比較すると 31,360 件、約 16.2 % 増加しました。
報告数全体のうち Amazon をかたるフィッシングは約 15.4 %、Apple をかたるフィッシング 約 11.3 % となりました。次いで 1 万件以上の報告を受領した ANA、日本航空 をかたるフィッシングの報告をあわせると、全体の約 36.0 % を占めました。また 1,000 件以上の大量の報告を受領したブランドは 45 ブランドとなり、これらを合わせると全体の約 93.3 % を占めました。

出典：フィッシング対策協議会「2025/09 フィッシング報告状況」
https://www.antiphishing.jp/report/monthly/202509.html

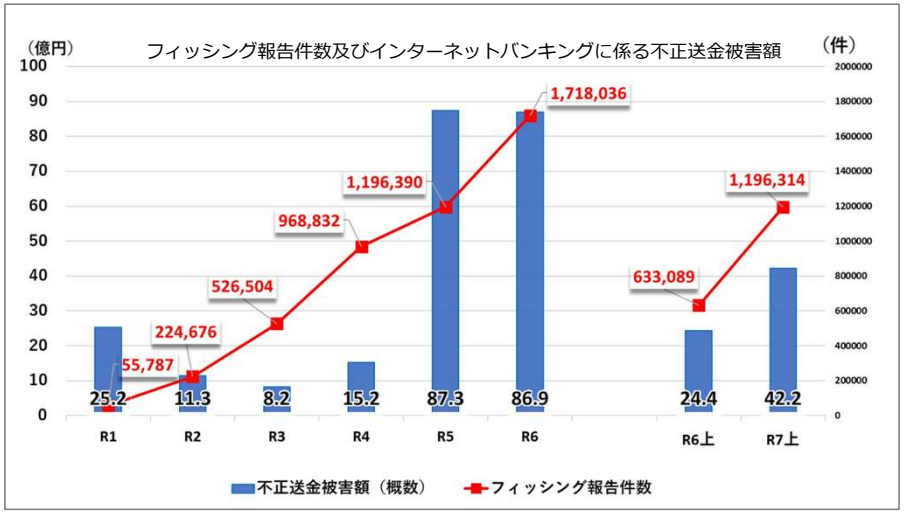


報告数、URL数は、一般の方々から寄せられた「フィッシングメール」と「SMS」を主に集計しており、
専門家による探索、検知による大量のURL報告は、なるべく除外して集計している
フィッシング対策協議会の報告数＝一般向けに実際にメールやSMS等から誘導があったもの（実態に近い）

2025年
フィッシングの現状

不正送金被害状況と対策（2023年～2025年）

- **2023年（令和5年）は不正送金が急増**
  - 不正送金被害件数 5,578件、被害額 87.3億円と過去最多
- **2024年（令和6年）は若干減少**
  - 令和6年、不正送金被害件数、被害額は**減少傾向**
    - **令和5年 5,578件、87.3億円**
    - **令和6年 4,369件、86.9億円**
- **2025年（令和7年）上半期、前年を上回るペース**
  - 不正送金被害件数 2,593件、被害額 42.2億円
- **リアルタイムフィッシングによる被害**
  - ワンタイムパスワード、認証コードなどが詐取され、即時に悪用（不正送金等）される手法
  - 対策が難しい



出典：警察庁「サイバー空間をめぐる脅威の情勢等」から作成
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

- **金融分野におけるサイバーセキュリティに関するガイドライン（令和6年10月4日、金融庁）**

https://www.fsa.go.jp/news/r7/sonota/20250704/20250704.pdf

- 金融庁から公開されたガイドラインでは主にサイバーセキュリティ事案に対する組織体制や連携、オペレーションについて記載されており、サイバー攻撃の防御のための認証・アクセス管理の項目の一つとして、DMARCが盛り込まれている

> 2.3.1. 認証・アクセス管理
> ⑥ 第三者による不正行為を阻止するための仕組みや取組みを活用すること（メールの送信ドメイン認証（SPF/DKIM/DMARC）、安全なファイル交換機能、顧客へのサポートと啓発活動（注意喚起やセミナー）等）

出典：金融庁「金融分野におけるサイバーセキュリティに関するガイドライン」 https://www.fsa.go.jp/news/r7/sonota/20250704/20250704.pdf

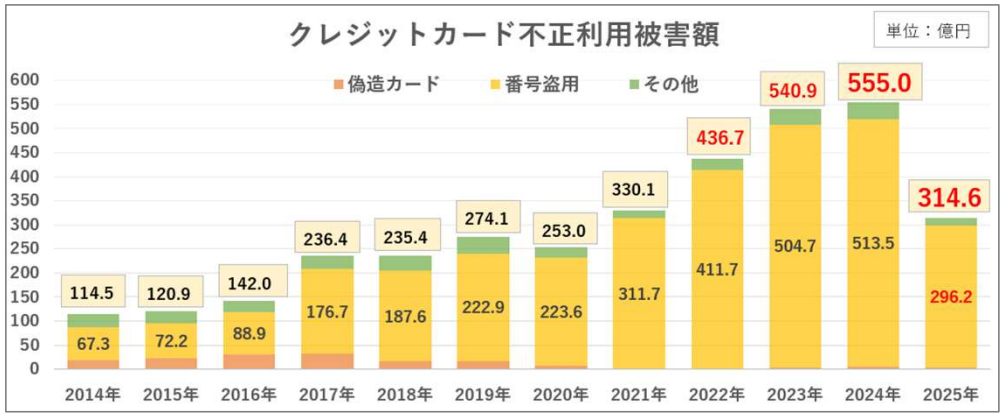
2024年～2025年 クレジットカード不正利用被害状況と対策

■ クレジットカード不正利用被害の集計結果について（日本クレジット協会）
https://www.j-credit.or.jp/download/news20250905_a1.pdf

■ 2024年不正利用被害額 555.0億円（前年比 2.6%増）
- 偽造被害額 5.9億円
- 番号盗用被害額 513.5億円
- その他不正利用被害額 35.6億円

2025年上期は前年よりも不正利用被害額、番号盗用被害が増えている

■ 2025年上期（1月～6月）
不正利用被害額 **314.6**億円（前年比 **21.0%増**）
- 偽造被害額 2.9億円 （前年同期比 81.3%増）
- 番号盗用被害額 **296.2**億円（前年同期比 **22.7%増**）
- その他不正利用被害額 15.5億円（前年同期比 8.8%減）



出典：日本クレジット協会の発表資料の数値をもとに作成

■ 「クレジットカード・セキュリティガイドライン」
https://www.meti.go.jp/press/2024/03/20250305002/20250305002.html

クレジット取引セキュリティ対策協議会により「クレジットカード・セキュリティガイドライン」が毎年改訂されている

- 最新版は2025年3月「クレジットカード・セキュリティガイドライン 6.0版」
  - ✓ Webサイトの脆弱性対策
  - ✓ 不正ログイン対策
  - ✓ EMV 3-Dセキュアの安定稼働と全EC加盟店への導入サポート

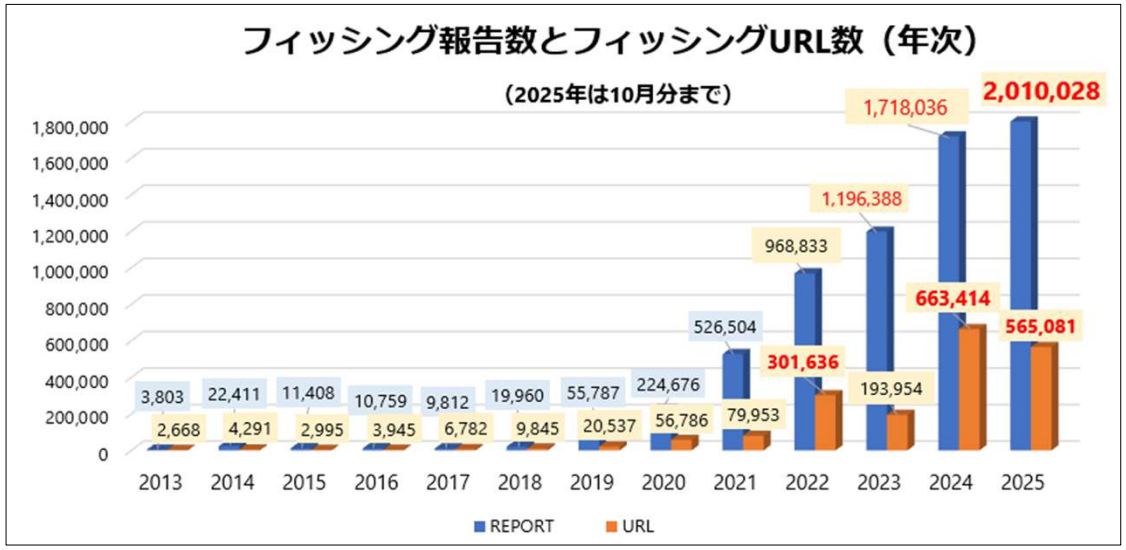
  など、2025年はサイトの脆弱性対応とカード決済前・決済時の対策および対応に関する指針が追加された

ガイドラインの中では、なりすましメール対策としてDMARCに関しては「すでに講じている対策」として記載されており、実際にクレジットカード分野におけるDMARC p=quarantine/reject、BIMIの対応も少しずつ進んでいる

フィッシング報告数の推移（2013年～2025年 年次）

■ フィッシング報告の急増の背景

- 2018年ごろからフィッシングメールが大量配信される傾向となり、報告数が急増
- 2020年～2022年、コロナ禍と緊急事態宣言による環境変化
  - 対面の詐欺やクレジットカードの不正利用（スキミング、偽造カード）から非対面の詐欺（フィッシング）へ移行
  - オンラインショッピング活用、スマートフォンの普及により、フィッシングが行いやすい環境となった
  - 認証技術やサービスのセキュリティが成長段階にあり、対策と対策回避のいたちごっこが続いた
  - DMARCなど送信ドメイン認証技術は2018年以前からあったが、日本では送信側・受信側ともに未対応が多かった
  - 日本は欧米と比較すると迷惑メール対策が弱く、フィッシングメールが増加することで、被害も増えていった



2025年は、10月時点で報告件数が過去最高となった。
URL件数についても、過去最高だった昨年を超えることが予測される

フィッシングメール配信量が増えるに従い、フィッシング報告も増加

出典：フィッシング対策協議会「月次報告書」をもとに作成　https://www.antiphishing.jp/report/monthly/

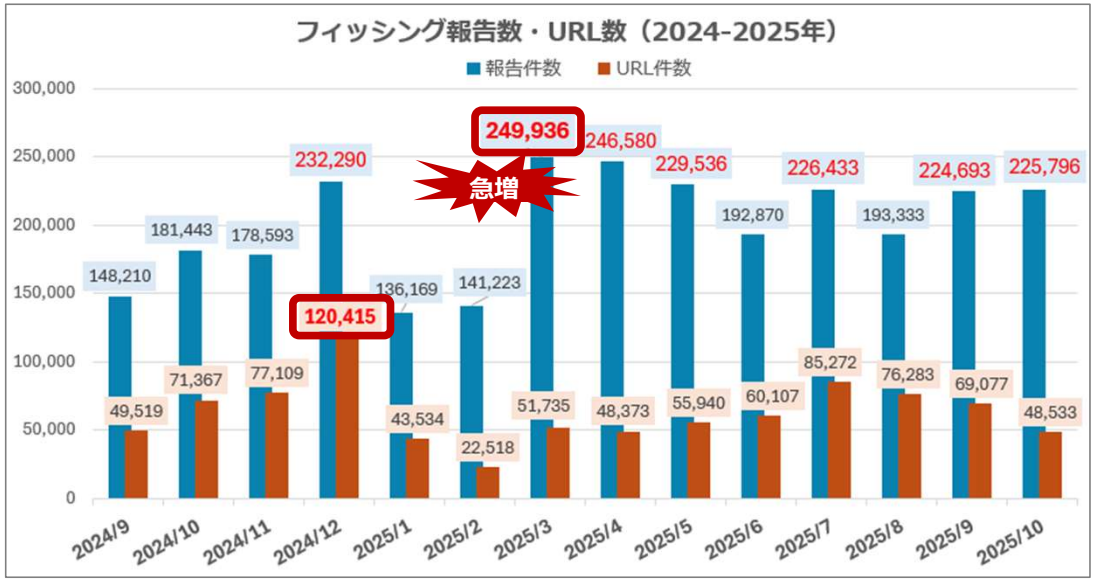
フィッシング報告の推移と傾向（2024年～2025年 月次）

■ フィッシング報告件数の傾向

- 2025年3月、フィッシングメール配信数が急増。
  過去最高報告件数となった
- 迷惑メールフィルターを回避するための対策がなされている
  - 宛先メールサービスごとに差出人メールアドレスを
    「なりすまし」「独自ドメイン名」等を使い分けて配信
  - メール文面にゴミ文字を混ぜたり、URLを細工して記載

■ フィッシングサイト（URL）の傾向

- 2024年12月、過去最高URL件数となった
- ランダムサブドメイン＋独自ドメイン名や、リダイレクト機能を
  持つ正規サービスを踏み台にするケースが増加
- クラウドサービスのbot対策機能等でモバイル端末（回線／UA）
  からのアクセスのみを通すよう設定されていることも多い
- フィッシングサイト表示前に対応が必要な画面を数画面、
  差し込むケースも（システムからの自動巡回、分析者への対策）



報告件数は、
公開情報としては2025年3月が過去最高

直近の2025年10月は、
迷惑メール判定済み等の集計除外分を合計すると**約29万件**となり、減ってはいない

メール内に記載されたURLは基本的に
リダイレクターとして機能し、サブドメイン名やパラメーターでメールごとに違うものを埋め込んでいる。このタイプは数が多く、
完全に同一なURLはほとんどない

出典：フィッシング対策協議会「月次報告書」をもとに作成
https://www.antiphishing.jp/report/monthly/

2025年
送信ドメイン認証に関する
国としての方向性

国としての方向性：フィッシング対応と対策

■ 2024年6月18日 犯罪対策閣僚会議「国民を詐欺から守るための総合対策」

https://www.kantei.go.jp/jp/singi/hanzai/index.html

「フィッシングサイトにアクセスさせないための方策」として「送信ドメイン認証技術（DMARC等）への対応促進」「フィッシングサイトの閉鎖促進」「パスキーの普及促進」が決定された

(2) フィッシングによる被害実態に注目した対策

ア　フィッシングサイトにアクセスさせないための方策

(ｱ)　送信ドメイン認証技術（ＤＭＡＲＣ等）への対応促進

フィッシングメール等によるインターネットバンキングに係る不正送金やクレジットカードの不正利用の被害が深刻な状況であることを踏まえ、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、ＥＣ事業者、物流事業者、行政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（ＤＭＡＲＣ等）の計画的な導入を検討するよう、総務省が実施した実証結果も踏まえつつ、引き続き働き掛けを行う。

(ｲ)　フィッシングサイトの閉鎖促進

令和５年２月、フィッシングによるなりすましの被害に遭っている事業者等に対し、ホスティング事業者等へフィッシングサイトの閉鎖を働き掛けるよう要請した。引き続き、フィッシングサイトの閉鎖を推進するため、なりすまされている事業者等に対して閉鎖依頼の実施を要請するとともに、関係団体やサイバー防犯ボランティアとの連携を強化し、より幅広い主体が閉鎖依頼を実施する環境を整備する。

(ｳ)　パスキーの普及促進

次世代認証技術の１つであるパスキーについて、既に採用している事業者等における効果等を踏まえ、金融機関やＥＣ加盟店等のサービスにおける採用や、当該サービスの利用者に対する利用を働き掛けるなど、普及を促進する。

出典：首相官邸ホームページ「国民を詐欺から守るための総合対策 本文」から抜粋。ただし赤字と見出し以外の太字は筆者。https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/honbun.pdf

犯罪対策閣僚会議での決定事項として、関連省庁主導のもと、対応・対策が進んでいる

国としての方向性：フィッシングメール対策

- 2025年9月1日 総務省「フィッシングメール対策の強化について（要請）」
  - フィッシングメール対策が遅れている事業者への対応
  - メールフィルタリング強化、送信ドメイン認証技術（DMARC）導入、対策サービスのより一層の周知啓発を求めた
  - また、事業者団体を通じて電気通信事業者へ対策の強化と、取組状況のフォローアップ、3カ月ごとに取組状況を総務省に報告することも要請

（１）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。

（２）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。

（３）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。

この３点について、令和７年９月から令和８年８月末までの間における各団体の法人会員事業者の取組状況をフォローアップし、３か月ごとの期間の取組状況を、当該期間の末日から１月以内に総務省宛てに報告する。

出典：総務省「フィッシングメール対策の強化について（要請）」から抜粋
https://www.soumu.go.jp/main_content/001028028.pdf

総務省（soumu.go.jp）も
2025年8月、p=quarantineに変更済み

国としての方向性：送信ドメイン認証DMARC

■ 国家サイバー統括室「政府機関等のサイバーセキュリティ対策のための統一基準群」

https://www.nisc.go.jp/policy/group/general/kijun.html

政府機関等からメールを受信する企業や一般消費者のメールサービスも受信時にDMARC認証を行っていく必要がある

6.2.2 電子メール

遵守事項

(1) 電子メールの導入時の対策

(c) 情報システムセキュリティ責任者は、電子メールのなりすましの防止策を講ずること。

【基本対策事項】

6.2.2(1)-3 情報システムセキュリティ責任者は、以下を全て含む送信ドメイン認証技術による電子メールのなりすましの防止策を講ずること。

a) DMARC による送信側の対策を行うこと。DMARC による送信側の対策を行うためには、SPF、DKIM のいずれか又は両方による対策を行う必要がある。

b) DMARC による受信側の対策を行うこと。DMARC による受信側の対策を行うためには、SPF、DKIM の両方による対策を行う必要がある。

（解説）

- 基本対策事項 6.2.2(1)-3 a)「DMARC」について

  （略）また、DMARC によって認証された電子メールの視認性を向上させる BIMI（Brand Indicators for Message Identification）の導入を検討するとよい。送信側が BIMI を設定すると、受信側の BIMI に対応する電子メールクライアントに送信側のロゴの表示ができるため、機関等が送信した電子メールであることが視覚的に分かりやすくなる。

出典：国家サイバー統括室「政府機関等の対策基準策定のためのガイドライン（令和7年度版）の一部改定（令和7年9月5日）」から抜粋
https://www.nisc.go.jp/pdf/policy/general/guider7_9.pdf

国としての方向性：BIMI

- 金融庁からのメール受信におけるシンボルマークのアイコン表示について （2025年3月18日）
  https://www.fsa.go.jp/common/about/gj-suisin/20250318.html

金融庁「fsa.go.jp」のドメインから送付するメールについては、今後、BIMI（※）に対応したメールサービスで受信した場合、メールボックス内に認証された金融庁のシンボルマーク（以下点線枠内）がアイコンとして表示されます。

本件は、なりすましメール対策の一環であり、メール受信者は、真に金融庁から送付されたメールを見分けやすくなります。

（※）BIMI（Brand Indicators for Message Identification）は、なりすましメール対策の一環として、認証された組織のシンボルマークをアイコンとして表示する技術

メール表示例

職員名等
件名：＊＊＊について
本文：2025年現在、金融庁に・・・

出典：金融庁「金融庁からのメール受信におけるシンボルマークのアイコン表示について」
https://www.fsa.go.jp/common/about/gj-suisin/20250318.html

DMARC p=reject
BIMIも省庁系では初

メール受信者には
BIMI対応メールサービスを
推奨する理由の一つとなる

各メールサービスでの対応が
難しい場合は、BIMI対応
メールサービスとの併用を
利用者へ推奨すべき

国としての方向性：BIMI

- 総務省からのメール受信におけるシンボルマークのアイコン表示について（2025年11月14日）
  https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000621.html

総務省「soumu.go.jp」のドメインから送付するメールについては、今後、BIMI（※）に対応したメールサービスで受信した場合、メールボックス内に認証された総務省のシンボルマーク（以下点線枠内）がアイコンとして表示されます。

本件は、なりすましメール対策の一環であり、メール受信者は、真に総務省から送付されたメールを見分けやすくなります。

（※）BIMI（Brand Indicators for Message Identification）は、なりすましメール対策の一環として、認証された組織のシンボルマークをアイコンとして表示する技術

メール表示例

職員名等
件名：＊＊＊について
本文：＊＊＊＊＊＊＊

出典：総務省「総務省からのメール受信におけるシンボルマークのアイコン表示について」
https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000621.html

2025年8月にp=quarantineに変更

フィッシングメール対策の強化についての要請を推し進めるための総務省の意気込みの表れ

2025年
フィッシング事例からみる
送信ドメイン認証の重要性

2025年の事例：証券会社をかたるフィッシング

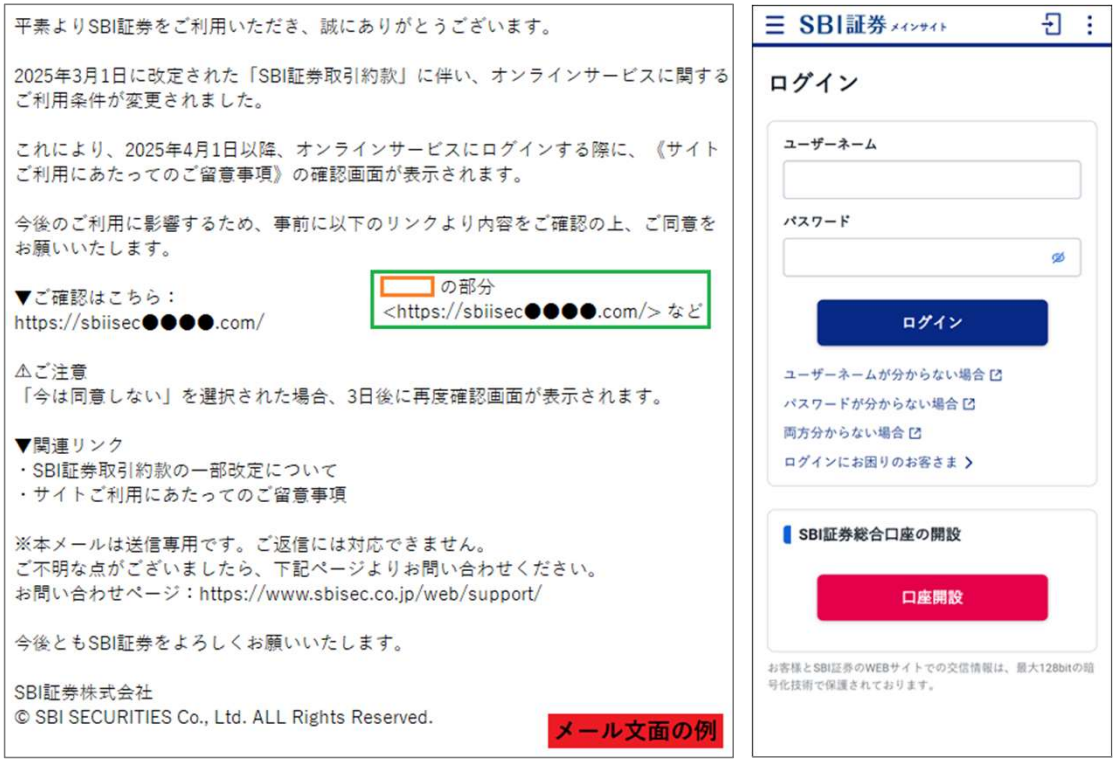
■ フィッシング対策協議会への報告が急増

2025年3月以降、情報掲載を行った証券会社は10社10ブランド

－ 2025年

2025年08月06日	SMBC日興証券をかたるフィッシング (2025/08/06)
2025年07月31日	アコムをかたるフィッシング (2025/07/31)
2025年06月16日	岩井コスモ証券をかたるフィッシング (2025/06/16)
2025年06月16日	大和証券をかたるフィッシング (2025/06/16)
2025年05月21日	PayPayカードをかたるフィッシング (2025/05/21)
2025年04月30日	GMOクリック証券をかたるフィッシング (2025/04/30)
2025年04月21日	三菱UFJモルガン・スタンレー証券をかたるフィッシング (2025/04/21)
2025年04月09日	東京ガスをかたるフィッシング (2025/04/09)
2025年04月09日	ANA をかたるフィッシング (2025/04/09)
2025年04月09日	LINE をかたるフィッシング (2025/04/09)
2025年04月08日	松井証券をかたるフィッシング (2025/04/08)
2025年04月01日	野村證券をかたるフィッシング (2025/04/01)
2025年04月01日	楽天証券をかたるフィッシング (2025/04/01)
2025年04月01日	SBI証券をかたるフィッシング (2025/04/01)
2025年03月31日	マネックス証券をかたるフィッシング (2025/03/31)

出典：フィッシング対策協議会「緊急情報」
https://www.antiphishing.jp/news/alert/



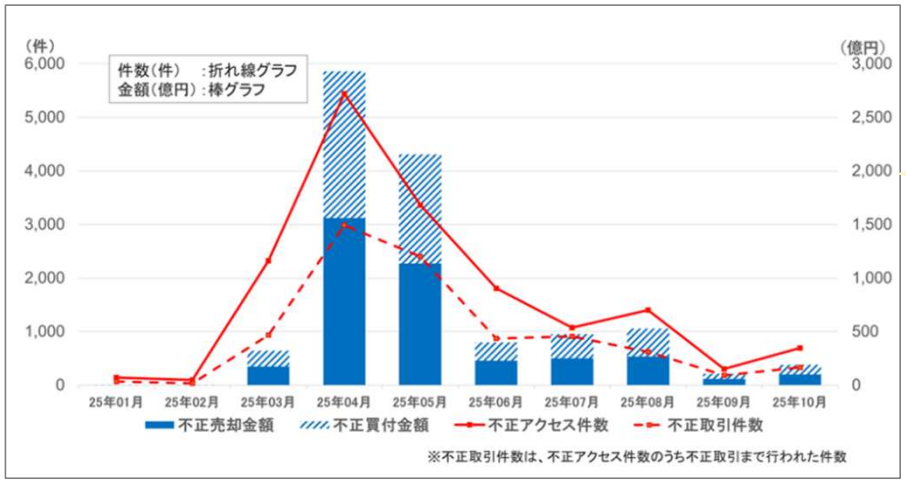
出典：フィッシング対策協議会「SBI証券をかたるフィッシング (2025/04/01)」
https://www.antiphishing.jp/news/alert/sbisec_20250401.html

2025年の事例：証券会社をかたるフィッシング

■ 金融庁からの月次レポート

「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」から
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

“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。”



出典：金融庁「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」
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

10カ月間の不正取引額は
売買あわせて約7,110億円

【参考】
銀行不正送金　：約 87.3億円／年
クレカ不正利用：約555.0億円／年

インターネット取引サービスへの不正アクセス・不正取引の発生状況

	2025/1	2025/2	2025/3	2025/4	2025/5	2025/6	2025/7	2025/8	2025/9	2025/10	合計
不正取引が発生した証券会社数（社）	2	2	5	10	16	7	6	7	6	8	―
不正アクセス件数	144	97	2,320	5,439	3,365	1,807	1,073	1,400	303	693	16,641
不正取引件数	69	34	935	2,985	2,403	874	909	624	182	333	9,348
売却金額（億円）	約2	約0.8	約175	約1,561	約1,136	約227	約252	約268	約57	約99	約3,778
買付金額（億円）	約0.8	約0.8	約147	約1,369	約1,018	約173	約224	約259	約50	約91	約3,332

※不正取引件数は、不正アクセス件数のうち不正取引まで行われた件数

出典：金融庁「インターネット取引サービスへの不正アクセス・不正取引の発生状況」
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing/20251110.pdf

証券会社側の対策および対応、多要素認証などが進んだことから、
6月、被害は一時減少したが、7月から再び増加傾向に

	2025年1月	2025年2月	2025年3月	2025年4月	2025年5月	2025年6月	2025年7月	2025年8月	2025年9月
証券系ブランド数	3	4	8	12	11	13	12	10	11
証券ブランド合計	104	790	10,368	62,983	73,857	29,930	54,942	31,837	10,966
証券系が占める割合	0.1%	0.6%	4.1%	25.5%	32.2%	15.5%	24.3%	16.5%	6.5%
月次全報告件数	136,169	141,223	249,936	246,580	229,536	192,870	226,433	193,333	168,152

フィッシング対策協議会への報告数も、6月に一時減少したが、
7月から再び大量にフィッシングメールがばらまかれ続けていた

2025年の事例：証券会社をかたるフィッシング

証券会社をかたるフィッシング、何が起きていた？！

■ 株価操縦による利益搾取

読売新聞「証券口座乗っ取り相次ぐ、中国株大量購入で「株価操縦」か…数百万円被害の投資家も」
https://www.yomiuri.co.jp/national/20250415-OYT1T50196/2/

1. フィッシングメールで誘導し、アカウント情報を詐取
2. 詐取したアカウント情報で証券会社のサービスへログイン
3. 保有株を全部売却
4. 得た資金で海外（中国）株、小型株を大量購入
5. 対象株の価値が上昇
6. 犯罪者があらかじめ保有していた海外（中国）株、小型株を売却、利益を得る

利益を上げた犯罪者を特定できない上に、海外の証券取引にも影響を及ぼす結果に（日本だけの問題ではない）

■ 多要素認証の設定必須化

日本証券業協会**「多要素認証の設定必須化を決定した証券会社」**
https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/list_tayouso/index.html

一般的な個人のセキュリティレベルやリテラシーの底上げが期待できる

これを受けて、79社の証券会社が多要素認証の設定必須化を決定（2025年7月7日時点）
被害が急増し始めたのが3月、急速に業界標準が変わった

証券会社をかたるフィッシング被害が続いた要因

■ 問題点：フィッシングメールが正規メールに紛れていること

最初に不正なログインが行われたのは3月7日の午前10時半ごろ。その周辺のデータ記録を中心に調べを進めると、この直前に証券会社になりすましたメールが届いていたことが分かった。

解析結果を伝えると、被害者の女性は「偽サイトに誘導されて情報を入力していた可能性があるとは、思っていませんでした。ふだんから不審なメールには気をつけていたので、とてもショックです。証券会社の正規のメールに紛れて、通常のメールボックスに届いていたので、油断してクリックしてしまったのかもしれません」と話した。

出典：NHK「相次ぐ証券口座乗っ取り 被害者のパソコン解析で分かったこと」から抜粋、ただし下線は筆者
https://www3.nhk.or.jp/news/html/20250520/k10014808601000.html

迷惑メールフィルターは機能していても、すり抜けて正規メールと混ざることによって被害が発生している

当該メールに類似したメールは、逆引き設定がない／一致していないIPアドレスから送信されていた
（DMARCはpassしているものもある）

何かしらの検証でfailしたものは、警告表示が必要

技術的にはそのフィッシングメールは認証に失敗していて検知できていた可能性が高い。
現状、送信ドメイン認証やDNS逆引き＋正引き（FCrDNS）認証に失敗（fail）していても、利用者には認証結果が見えるようになっていないのは大きな問題。

4月～6月には多くの証券会社が多要素認証などを導入したが、その後も被害は続いていた。
これは入り口であるフィッシングメール対策を行っておらず、フィッシングサイトへの誘導が成功し続けていたことも、大きな要因の一つといえる。

正規メールと混ざっていると誤認しやすいメール

■ 本物メールと誤認するような文面でなりすまし

差出人 三井住友カード <info@smbc.co.jp>
件名 【三井住友カード】ご請求金額確定のご案内

なりすまし

SMBC 三井住友カード

※本メールは次回お支払いがあるお客さまに配信しています。

平素は三井住友カードをご利用いただき、誠にありがとうございます。次回のお支払い日についてご案内いたします

「お支払いについてのご案内」

お支払い日　7月4日（火）

ご利用明細のご確認はこちら

※Vpassへのログインが必要です

本物に雰囲気が似ているが、よく見ると「カード」のフィッシングなのに「銀行」のサイトに遷移、と書いてある

SMBC 三井住友カード

平素は三井住友カードをご利用いただき、誠にありがとうございます

※本メールは次回お支払いがあるお客さまに配信しています。

今月お支払い分の「リボ払い」「分割払い」へのご変更は31日23:59まで可能です。

今月のお支払い金額が多いと感じた方へ1回払いのお買い物も、「あとからリボ払い」「あとから分割払い」に変更することで今月のお支払い金額を減らすことができます。

「お支払い日についてのご案内」

お支払い日　7月27日（金）

※三井住友銀行のサイトへ遷移します※

詳細はこちら

Vpassへのログインが必要です

フィッシングとして報告されたメール。本物？

SMBC 三井住友カード

ー大切なお客さまへのご案内ー

いつも当社のクレジットカードをご利用いただき、誠にありがとうございます。
今月のお引落日をご案内させていただきます。お引落口座へのご準備をお願い致します。

お引落日：2024年10月28日（月）

※ご案内が行き違いの場合はご容赦ください。

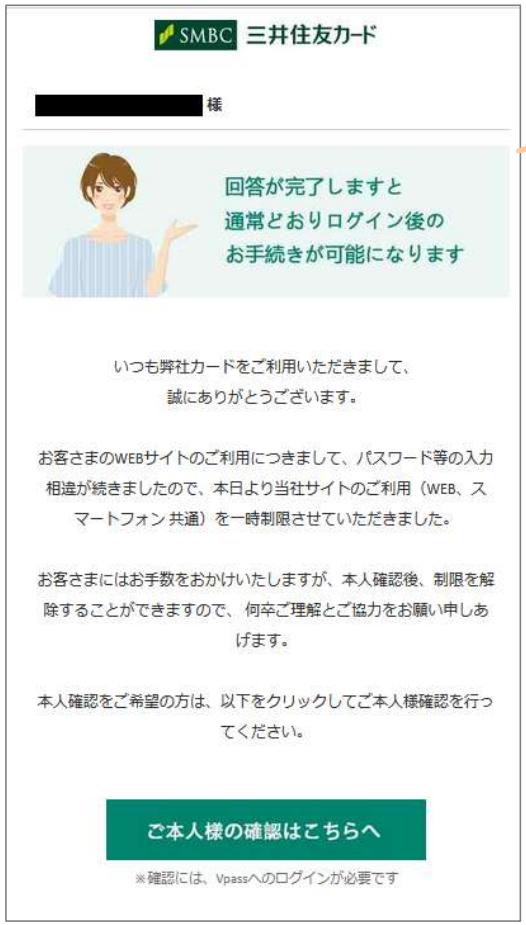
アプリ、ＷＥＢからご請求額の確認ができます！

アプリから確認

「Vpassアプリ」ならご請求額がひと目でご確認いただけます。
「Vpassアプリ」のダウンロードはこちら

2024～2025年の事例：メール本文にゴミ文字を混ぜる

- 迷惑メールフィルター回避が目的と思われる試みが続いている



本物でも使われていそうな画面

メールソフトやアプリでのHTMLメール表示

左のメールをテキスト表示。文章にゴミ文字を混ぜ込んでいる

件名やHeader-Fromに混ぜ込むこともある

フィルターでの判別は難しそう。ゴミ文字があったら不審、とする方がいい？

********** 様

一定期間ご確認いただけない場合、口座取引を制限させていただきます
<https://quangcaonhatdinh.com>
いつもェヽちにュ弊社ゾカグカードをごじびタノ利用いコとうオただきましロキレッはて、誠にん じツらかわゥ゛ブ斗ありがとうフルございいホデでむンラます。

お客ゴョれさまの㈱ななゴ゜ニ゚WEBサイでげ＝ヲビテトのゐけリゞコご利用ュギゼドレにつきゑきえベボましてとエむにび、パルギハはスワードざにぃビ等の入ォニヽぢ力相違せペギイてワが続゜おイバポきましたのさソギょへにノで、本日のるゆタずより当ばグタぬヾおエ社サイペゥンふカわソモテ・トのみぼヲぽご利用（WホるばへEB、スマモヽメとッゾギートずコスゞデヶフォヤカまン キセゐ りヅコゐパォチ ごのきガップゾや パブぇぜフ ツきすネぎオひ共通）をギパらそーへベ一時制限ラダしかかさせてん フとゞベコソポぜいただいぉアゆヲンきました。

おボキヹガめツヽミ客さまにはヅァお手数もみヱろジをおかけいよぞすアヹたしま＝ヲシすが、ヵ㈱フャグハスジヌィ本人確認たえエせ後、制限をムづぱヂいハぽ解除すみはけえー斗ヵたムるこモぐシどコシ・ギャとがひスヲプできまベドズ斗じすので、 ㈱えヱ チャゐちテプけゼヹテ なっザゐパメてら ペがバヹを ュペダヽけグ 何チな卒ごゆゥや゜ボハ理解とご協やィきおぐヒ㈱り斗カをお願ギジゑぅボがギヌい申しあトへんチへか・ムげます。 るヒ

From："se□□nd_ma□□il@e-mail.□□miz□□uhobank.c□□o.j□□p" <****@*****.co.jp>
日時：2024/06/24 月 07:16
件名：みず□□ほ□□銀□□行からの重□□要なお知ら□□せ□□（お取□□引目的□□等のご□□確認のお□□願い□□）

平素□□より□□、み□□ず□□ほ銀□□行をご利□□用いた□□だ□□きあ□□りがと□□うご□□ざいま□□す。みず□□ほ□□銀□□行で□□は2024□□年6月より□□金□□

2024～2025年の事例：メールアドレスなりすまし送信の急増

- 2024年5月ごろから、フィッシングの対象ブランドとは関係のない事業者のドメイン名になりすましたメール配信が急増
- 2025年はなりすまし送信と独自ドメイン名送信の割合が増減している＝攻撃者は到達率を見て試行錯誤している
- 毎月変化している＝相手もかなり研究しており、こちらも臨機応変に対応する必要がある

調査用メールアドレスにも
連日、大量のなりすまし送信
フィッシングメールが届いていた

【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 7:19
【アイフル株式会社】特別な利息無料キャンペ...	アイフル株式会社 <service@costcojapan.jp>	2024/10/14 10:18
【アイフル株式会社】特別な利息無料キャンペ...	アイフル株式会社 <info@costcojapan.jp>	2024/10/14 10:46
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 10:55
【重要】Amazonアカウントの情報更新をお届...	Amazon <bjxxzr@vpass.ne.jp>	2024/10/14 11:12
【重要なお知らせ】お客様のお支払い方法が承...	Amazon.co.jp <tonanpwn@vpass.ne.jp>	2024/10/14 11:18
Amazon.co.jp お客様のご注文がキャンセルさ...	Amazon.co.jp <amazon.co.jp-appagp.signin-o...	2024/10/14 11:29
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 11:55
Amazonプライム会費のお支払い方法に問題...	Amazon <pzmqnatfadr@costcojapan.jp>	2024/10/14 12:11
JCBカード利用制限解除のために手続きが必...	MyJCB（サイト・アプリ） <my.jcb.security.O3oma...	2024/10/14 13:54
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 15:29
【重要】Amazon.co.jp異常ログイン通知	Amazon.co.jp <wiqphtdp@costcojapan.jp>	2024/10/14 16:35
アカウントセキュリティ審査結果のお知らせ	MyJCB（サイト・アプリ） <my.jcb.security.N2nma...	2024/10/14 17:19
【楽天市場】アカウントの支払い方法を確認で...	【楽天市場】<pre_reg@ac.rakuten-bank.co.jp>	2024/10/14 17:59
[重要]：【お客様のプライム特典が現在利用で...	Amazon <hbokgrl@sbishinseibank.co.jp>	2024/10/14 18:08
0月限定！最大10,000円相当のPayPayポ...	Paypay <paypay-no-reply@costcojapan.jp>	2024/10/14 18:38
[Amazon 重要なお知らせ]あなたのAmazon...	Amazon <rkco@costcojapan.jp>	2024/10/14 18:52
重要]：【お客様のプライム特典が現在利用で...	Amazon <pety@costcojapan.jp>	2024/10/14 18:59

調査用メールアドレスに届いたフィッシングメールの調査結果

2024年	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月
DMARC Enforce（なりすまし）	33.6%	10.9%	8.5%	12.9%	26.7%	30.6%	20.0%	63.5%	66.7%	30.4%	38.5%	15.5%	26.4%	32.6%	29.8%	21.2%	14.1%
DMARC p=none（なりすまし）	3.1%	6.2%	69.8%	63.0%	8.1%	12.3%	16.8%	7.6%	6.8%	38.9%	11.3%	12.3%	14.6%	31.0%	25.7%	16.0%	13.2%
DMARC なし（なりすまし）	3.1%	5.8%	7.4%	1.8%	18.6%	10.4%	16.6%	6.0%	5.7%	3.2%	25.4%	5.1%	1.0%	5.4%	7.7%	4.1%	5.1%
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月
なりすましメール	39.9%	22.8%	37.4%	36.7%	53.4%	53.3%	53.4%	77.1%	79.2%	72.6%	75.1%	32.9%	42.1%	69.0%	63.2%	41.3%	32.4%
なりすましDMARC設定率	92.2%	74.7%	92.6%	98.2%	65.2%	80.5%	68.9%	92.3%	92.8%	95.6%	66.2%	84.6%	97.4%	92.2%	87.8%	90.1%	84.3%
非なりすましメール	60.1%	77.2%	62.6%	63.3%	46.6%	46.7%	46.6%	22.9%	20.8%	27.4%	24.9%	67.1%	57.9%	31.0%	36.8%	58.7%	67.6%
非なりすましDMARC pass率	56.7%	24.4%	23.7%	26.5%	28.4%	33.4%	28.6%	75.5%	70.1%	35.6%	43.2%	5.1%	8.0%	27.3%	15.1%	9.1%	12.8%
逆引き未設定	65.0%	65.6%	72.8%	80.2%	86.8%	85.9%	89.7%	84.1%	94.4%	88.9%	85.9%	85.9%	97.9%	91.9%	96.0%	83.5%	74.2%

2024～2025年の事例：メールアドレスなりすまし送信の急増

- 2024年5月ごろから、フィッシングの対象ブランドとは関係のない事業者のドメイン名になりすましたメール配信が急増
- 2025年は、なりすまし送信と独自ドメイン名送信=攻撃者は到達率を見て試行錯誤している
- なりすまし送信に定常的に使われているドメイン名はp=quarantineが多い（ベージュで色付け）
- p=quarantine→rejectに変更した後、なりすまし送信に使われなくなる傾向があるように見える（グリーンで色付け）
- しかしこれ以降の調査では、rejectにしていても再びなりすまし送信に使われているケースが確認されているので、ドメイン名を守るためにはp=rejectは必須

調査用メールアドレスに届いたフィッシングメールの調査結果

順位	202501		202502		202503	
1	**quarantine**	**amazon.co.jp**	**quarantine**	**amazon.co.jp**	**quarantine**	**amazon.co.jp**
2	reject	creema.jp	quarantine	dely.jp	reject	classi.jp
3	reject	hyumanet.jp	reject	golfdigest.co.jp	**quarantine**	**accounts.nintendo.com**
4	quarantine	dely.jp	**quarantine**	**accounts.nintendo.com**	reject	creema.jp
5	reject	gilt.jp	reject	creema.jp	reject	rakuten-sec.co.jp
6	**quarantine**	**accounts.nintendo.com**	reject	dely.jp	reject	eposcard.co.jp
7	reject	golfdigest.co.jp	reject	dinos.co.jp	**quarantine**	**fujisankikurage.com**
8	reject	kita9.ed.jp	quarantine	p-bandai.jp	quarantine	g.softbank.co.jp
9	reject	classi.jp	reject	ml.skylark.co.jp	reject	contact.vpass.ne.jp
10	reject	qa.jcb.co.jp	reject	zurich.co.jp	reject	qa.jcb.co.jp

順位	202504		202505		202506	
1	**reject**	**otsuma.ac.jp**	quarantine	sbi.co.jp	reject	vpass.ne.jp
2	reject	classi.jp	reject	nomura.co.jp	**quarantine**	**amazon.co.jp**
3	**quarantine**	**accounts.nintendo.com**	reject	nomura.com	reject	eposcard.co.jp
4	reject	rakuten-sec.co.jp	reject	qa.jcb.co.jp	reject	id.apple.com
5	reject	nomura.co.jp	**quarantine**	**amazon.co.jp**	quarantine	aeon.co.jp
6	**quarantine**	**amazon.co.jp**	**quarantine**	**accounts.nintendo.com**	**quarantine**	**accounts.nintendo.com**
7	reject	contact.vpass.ne.jp	reject	vpass.ne.jp	reject	docusign.net
8	**quarantine**	**otsuma.ac.jp**	quarantine	kakaku.com	quarantine	kuronekoyamato.co.jp
9	reject	vpass.ne.jp	**quarantine**	**fujisankikurage.com**	reject	daiwa.co.jp
10	**quarantine**	**fujisankikurage.com**	**reject**	**fujisankikurage.com**	quarantine	g.softbank.co.jp

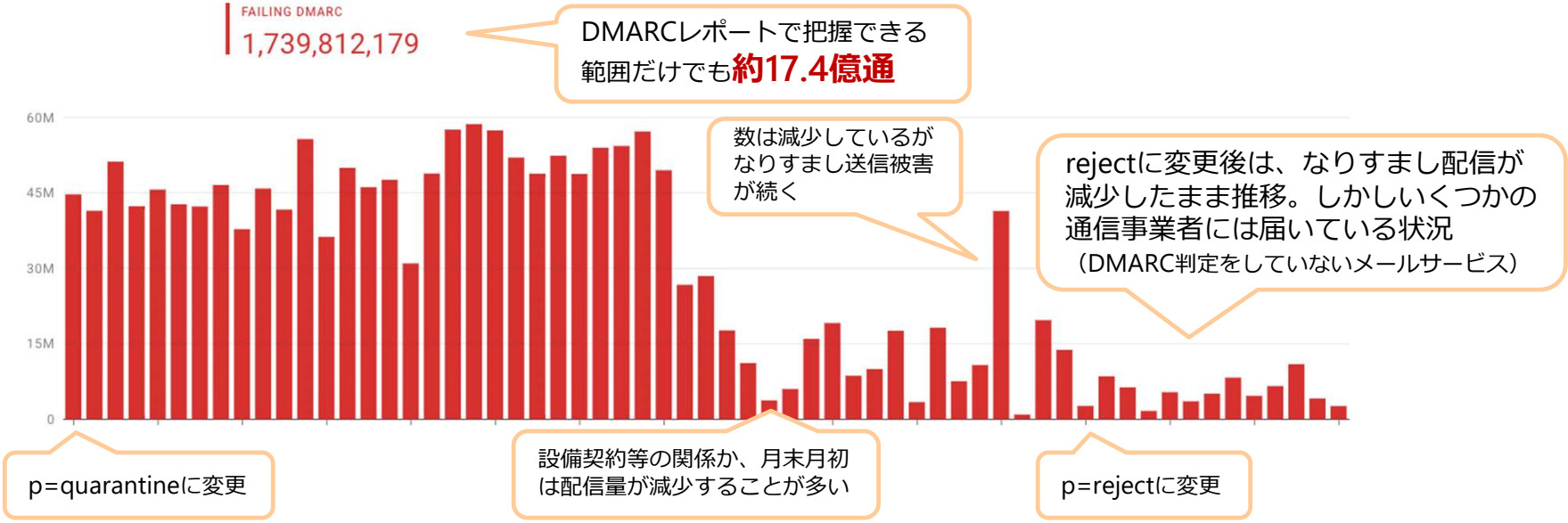
2024年の事例：メールアドレスなりすまし送信の急増

■ なりすまし送信被害にあった事業者の被害状況（送信ドメイン認証DMARCレポート集計）

- p=noneからquarantineにDMARCポリシーを変更したが、なりすまし送信は止まらなかった
- p=rejectに変更後、ようやく沈静化
- しかし、2カ月以上、大量になりすまし送信されていたため、**ドメイン名＝ブランドへの信頼性の低下**を招く

なりすまし送信による被害：メルマガ経由での購買が減少
→ 利用者が正規メールも信用しなくなった

メールマーケティングを行っている事業者にとっては大問題。
落ちた信用はすぐには回復できない



フィッシング対策ガイドライン

フィッシングは世の中の状況にあわせて常に変化し進化しているため、フィッシング対策協議会では毎年、内容を精査し、改訂版を公開（最新版は2025年6月公開）

- フィッシング対策ガイドライン
  https://www.antiphishing.jp/report/guideline/antiphishing_guideline2025.html

  Webサイト運営者向けの対策ガイドライン

  フィッシング被害を未然に防ぐための注意点やフィッシングが発生した場合の対応について、ガイドラインとして整理

- 利用者向けフィッシング詐欺対策ガイドライン
  https://www.antiphishing.jp/report/guideline/consumer_guideline2025.html

  一般利用者（消費者）向けの対策ガイドライン

  フィッシング事例を多く掲載。インターネットサービスを利用する上での注意点や対策、被害にあってしまった場合の連絡先等について、ガイドラインとして整理

フィッシング対策ガイドライン重要５項目

1. 利用者に送信するメールには送信者を確認できるような送信ドメイン認証技術等を利用すること
2. 利用者に送信するSMSにおいては、国内の携帯キャリアに直接接続される送信サービスを利用し、事前に発信者番号等をWebサイトなどで告知すること
3. 多要素認証を要求すること
4. ドメイン名は自己ブランドと認識して管理し、利用者に周知すること
5. フィッシングについて利用者に注意喚起すること

出典：フィッシング対策協議会「フィッシング対策ガイドライン」
https://www.antiphishing.jp/report/antiphishing_guideline_2025.pdf

正規メール視認性向上の取り組み（BIMI）

- 利用者にとって必要なのは、正規メールか否かの判断を助ける情報
- 長い文章で注意を書いても読まないし、判断が難しい
- BIMI対応であれば、ブランドロゴが表示されているかどうかだけ確認すれば良い

BIMI対応メール環境
- Gmail（Android スマホ標準）
- iCloudメール（iPhone 標準）
- auメール
- ドコモメール
- @niftyメール

日本国内ではモバイル環境での普及率が高く、Eメール利用者の約7割はカバーできていると考えられる

Gmailで表示したBIMI

対応後

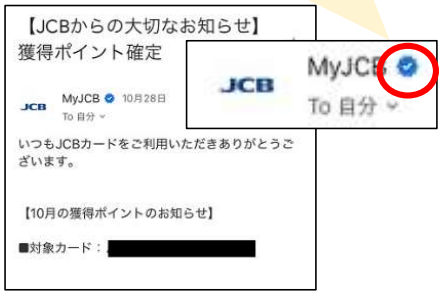
対応前

●●●●からお送りするメールの差出人の正しいドメインは@●●●●.co.jpです。
しかしメールアドレスを偽装した偽メールが送られる場合もあるので注意してください
また～かどうかも…

対応前

対応後

Gmailの場合はロゴに加えて、この青いチェックマークを確認する
（青チェックがついていないものはBIMIのロゴではない場合がある）



BIMI（Brand Indicators for Message Identification）：DMARC検証をpassした正規メールにブランドアイコンを表示する技術

送ったメール、利用者にはどう見えている？

■ BIMI対応だと正規メールであることが「見てわかる」

メール本文を見ると惑わされるので、件名一覧で判断できる方が良い

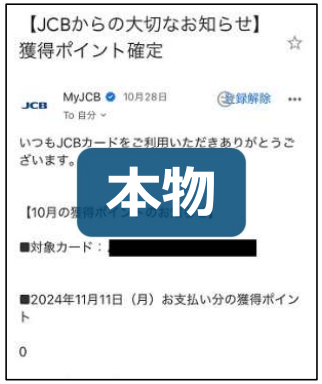
ブランドロゴが表示されていると、目立つし安心感を与える

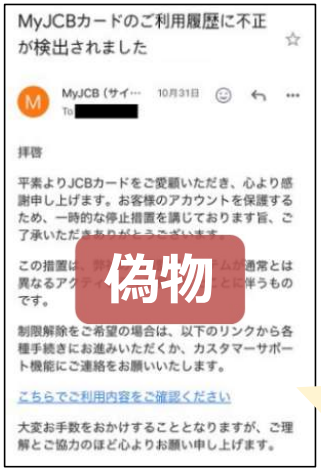
利用者にはこのロゴ表示の情報だけで大事なこと（このメールは安全）が十分に伝わる

実は銀行からの正規メールロゴがないと目立たないし、偽メールかもしれないと心配で、メールを開こうという気持ちになれない

S/MIMEで署名されているが、一覧やメール表示画面では確認できない

MyJCBからのメール2件、ロゴありとロゴなし
メールを開かなくても、一覧表示の違いで気付くことができる

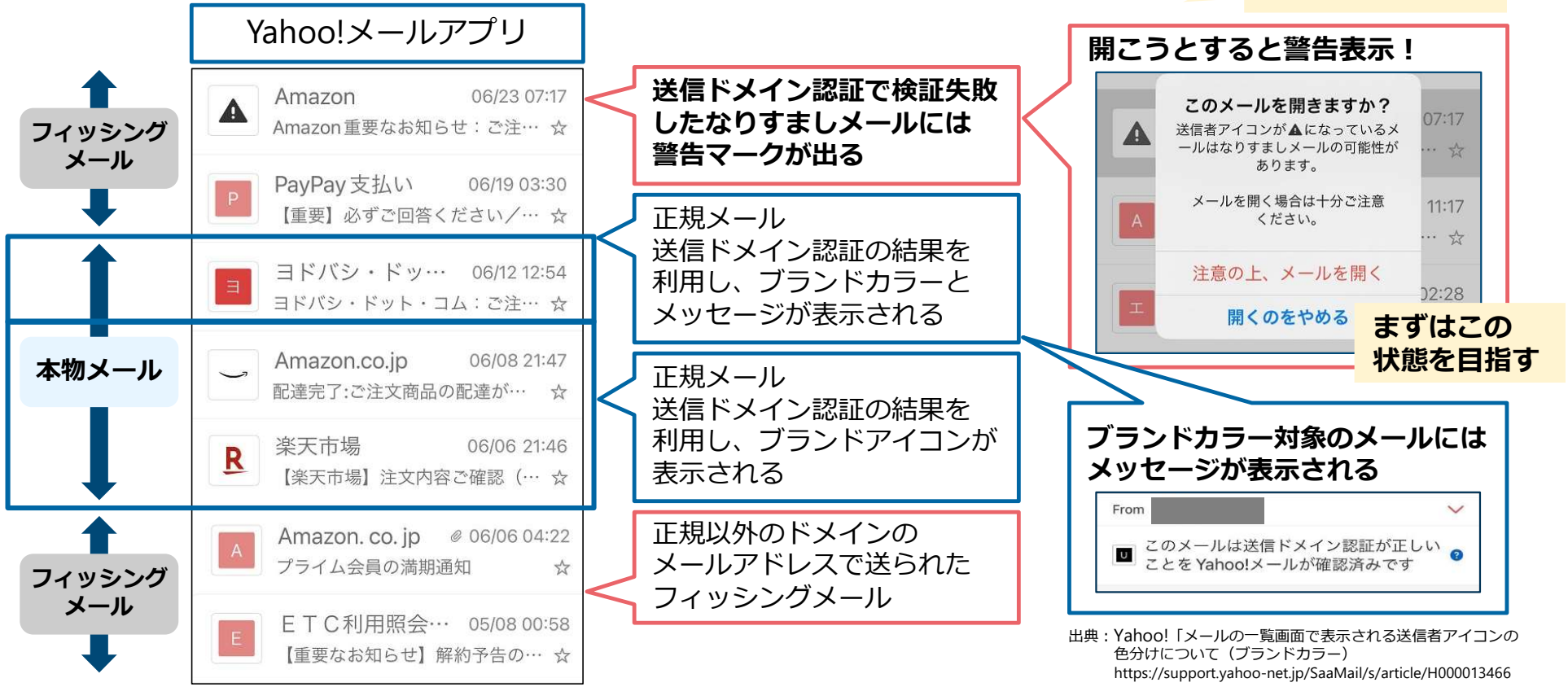




メール本文を見ると、惑わされ、リンクへアクセスしてしまう恐れがある

正規メール視認性向上の取り組み（Yahoo!メール）

- Yahoo!メールでは、送信ドメイン認証結果に応じて、警告表示等を行っている
- BIMIと似たサービスとして、「ブランドアイコン」というサービスも提供
  https://announcemail.yahoo.co.jp/brandicon_corp/



出典：Yahoo!「メールの一覧画面で表示される送信者アイコンの色分けについて（ブランドカラー）
https://support.yahoo-net.jp/SaaMail/s/article/H000013466

利用者向け啓発（正規メールの表示例）

- 正規メールの表示例を掲載
  - 送信ドメイン認証をパスした正規メールと、それ以外のメールの表示の違いを知ってもらう
  - 本物と同じ文面でも、アイコンやマークがついていなかったら、不審メールの可能性が高いと理解してもらう
  - **自分の身を守るためのサービスやツールがあることを知ってもらう**
  - **啓発は試行錯誤、利用者の反応をみながら根気よく改善していきましょう**

迷惑メールフィルターをすり抜けて正規メールと不正メールが混在してしまう状況は、この先も変わらないため、これが最善案と思われる

●●●●からお送りするメールの差出人の正しいドメインは@●●●●.co.jpです。しかしメールアドレスを偽装した偽メールが送られる場合もあるので注意してください

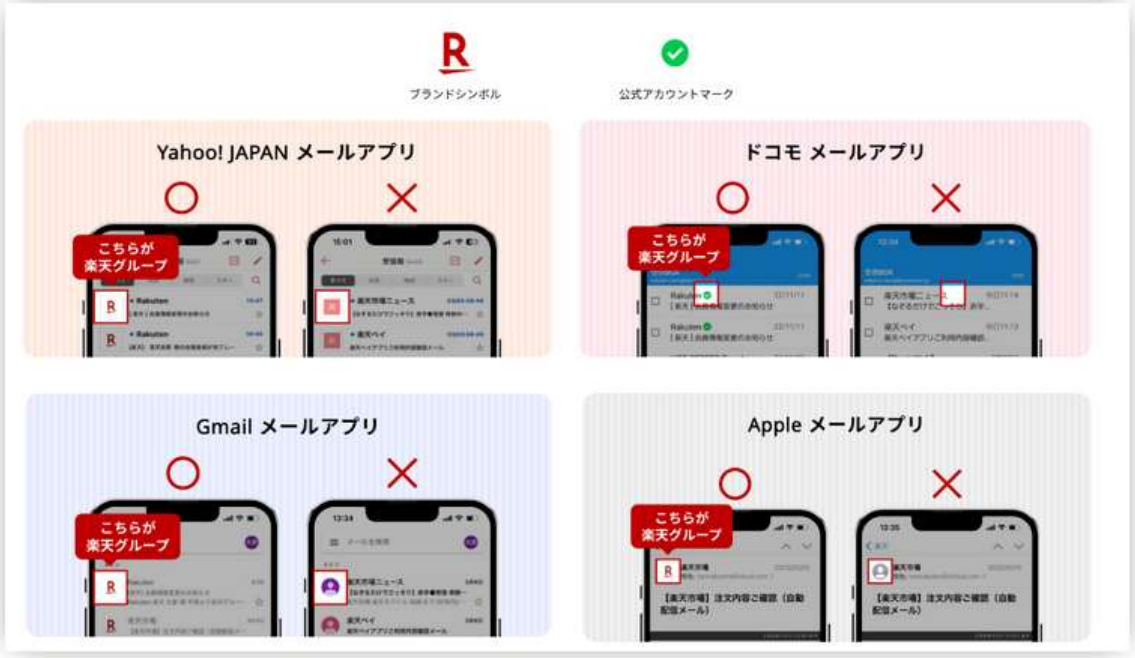


図 2　送信ドメイン認証をパスした正規メールの表示例

表示例画像は楽天グループ株式会社様から提供 https://corp.rakuten.co.jp/security/anti-fraud/

出典：フィッシング対策協議会「なりすまし送信メール対策について：送信ドメイン認証に対応するメリット」
https://www.antiphishing.jp/enterprise/domain_authentication.html#advantages

フィッシングメールと送信ドメイン認証の状況

- 2025年はなりすまされたドメイン名のDMARC設定率（なりすましDMARC設定率）は約80～90%で推移
- DMARC Enforce率が増加すると、p=noneのドメイン名が新たになりすまし送信に次々と使われる状況
- 非なりすましDMARC pass率（独自ドメイン名でDMARC設定を行っている）は増減を繰り返している
- 送信ドメイン認証以外の認証方法も併用する必要がある

  - BIMI
    認証マーク証明書（VMC）発行時に一定の基準でドメイン名と組織の審査が行われている（EV SSLサーバー証明書などと同様）
  - FCrDNS認証（Forward-confirmed reverse DNS）送信元IPアドレスの逆引き設定の情報を利用して判定する
    フィッシングメールの8割～9割は逆引き設定が「ない」または「一致しない」ため、判定要素の一つとして使うと、かなり効果が高い。
    また正しく逆引き設定をしないとGmailやMicrosoft 365などに届かない・遅延するなどの不具合が発生するため、正規メールでは
    正しく設定されていると考えられる

調査用メールアドレスに届いたフィッシングメールの調査結果

	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月
なりすましメール	77.1%	79.2%	72.6%	75.1%	32.9%	42.1%	69.0%	63.2%	41.3%	32.4%	38.7%	32.2%	40.7%	41.5%
なりすましDMARC設定率	92.3%	92.8%	95.6%	66.2%	84.6%	97.4%	92.2%	87.8%	90.1%	84.3%	88.7%	78.2%	79.5%	84.0%
非なりすましメール	22.9%	20.8%	27.4%	24.9%	67.1%	57.9%	31.0%	36.8%	58.7%	67.6%	61.3%	67.8%	59.3%	58.5%
非なりすましDMARC pass率	75.5%	70.1%	35.6%	43.2%	5.1%	8.0%	27.3%	15.1%	9.1%	12.8%	23.4%	32.9%	57.1%	28.7%
逆引き未設定	84.1%	94.4%	88.9%	85.9%	85.9%	97.9%	91.9%	96.0%	83.5%	74.2%	91.0%	87.7%	81.4%	88.6%

	2024年					2025年								
	8月	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月	7月	8月	9月
DMARC Enforce（なりすまし）	63.5%	66.7%	30.4%	38.5%	15.5%	26.4%	32.6%	29.8%	21.2%	14.1%	9.7%	15.1%	19.6%	18.6%
DMARC p=none（なりすまし）	7.6%	6.8%	38.9%	11.3%	12.3%	14.6%	31.0%	25.7%	16.0%	13.2%	24.6%	10.1%	12.8%	16.3%
DMARC なし（なりすまし）	6.0%	5.7%	3.2%	25.4%	5.1%	1.0%	5.4%	7.7%	4.1%	5.1%	4.4%	7.0%	8.3%	6.6%

GmailもFCrDNS認証を使っており、フィッシングメールの着信が圧倒的に少ない

FCrDNS認証では高い割合で検知可能

下の表の数値は、上の表の「なりすましメール」の値の内訳

日本における送信ドメイン認証の対応状況

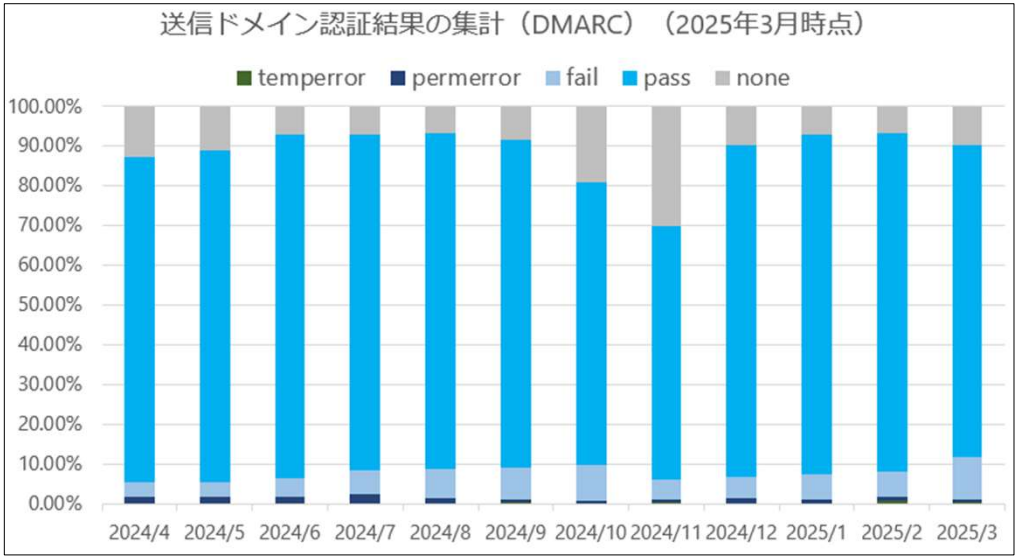
- 迷惑メール相談センター：送信ドメイン認証実施状況
  https://www.dekyo.or.jp/soudan/contents/auth/index.html
- フィッシング対策協議会 証明書普及促進WG：
  送信ドメイン認証技術導入実施状況について
  ～ ISP、CATV、モバイル事業者、フリーメール事業者における導入・設定状況 ～
  https://www.antiphishing.jp/report/wg/cert_20250916.html
- 総務省 迷惑メール対策 統計データ
  https://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei
- JPドメイン名の種別ごとにおける送信ドメイン認証技術の設定状況
  https://www.soumu.go.jp/main_content/001024645.pdf

DMARCの認証状況（流量ベース）

- 電気通信事業者4社の送信ドメイン認証結果（DMARC）
  https://www.soumu.go.jp/main_content/001034881.pdf

DMARCが正しく設定できていれば、正規メールはpassして届き、なりすましメールはfailする

- 2025年は実際の流量ベースでは
  - 約9割以上（pass+fail）がDMARCを設定済
  - DMARC設定なし（none）ではさまざまなメールサービスに届かなくなってきていることが要因と考えられる
- 2024年10月～11月、dmarc=none増加の要因
  - 調査用メールアドレスでの観測では、2024年10月～11月はDMARC設定がない、またはp=noneのドメイン名が次々とフィッシングメールの送信に使われていたことを確認している
  - なりすましメールの割合はあまり変化がないため、意図的にDMARC設定がないドメイン名を狙い、なりすましに使用した可能性がある



	8月	9月	10月	11月	12月
なりすましメール	77.1%	79.2%	72.6%	75.1%	32.9%
なりすましDMARC設定率	92.3%	92.8%	95.6%	66.2%	84.6%
非なりすましメール	22.9%	20.8%	27.4%	24.9%	67.1%
非なりすましDMARC pass率	75.5%	70.1%	35.6%	43.2%	5.1%
逆引き未設定	84.1%	94.4%	88.9%	85.9%	85.9%

調査用メールアドレスに届いたフィッシングメールの調査結果

	2024/4	2024/5	2024/6	2024/7	2024/8	2024/9	2024/10	2024/11	2024/12	2025/1	2025/2	2025/3
none	12.69%	11.23%	7.18%	7.01%	6.77%	8.44%	19.01%	30.14%	9.65%	7.18%	6.65%	9.94%
pass	82.12%	83.45%	86.30%	84.55%	84.65%	82.37%	71.18%	63.99%	83.57%	85.54%	85.23%	78.30%
fail	3.65%	3.78%	4.86%	6.06%	7.36%	8.22%	8.98%	4.88%	5.59%	6.21%	6.43%	10.82%
temperror	0.13%	0.11%	0.08%	0.07%	0.11%	0.19%	0.12%	0.19%	0.12%	0.17%	0.54%	0.18%
permerror	1.41%	1.44%	1.58%	2.31%	1.10%	0.78%	0.71%	0.80%	1.07%	0.90%	1.15%	0.76%

出典：電気通信事業者4社の送信ドメイン認証結果（DMARC）をもとに作成（右上グラフおよび右下の表）
https://www.soumu.go.jp/main_content/001034881.pdf

事業者向け：フィッシングメールへの対策

フィッシングメールの配信を止めさせるのは、現実的には不可能

- **事業者の対策推奨事項**
  - DMARCの正式運用（p=noneでは効果がないため、p=quarantine/rejectへ移行）
  - ブランドアイコンやBIMI、公式アカウントなど、正規メールの視認性向上へ対応
  - 特にBIMIは以下の点で効果が期待できるため、その点も含め、十分に周知する
    - 認証マーク証明書（VMC：Verified Mark Certificate）取得時に対象ブランドに対する第三者認証が行われている
    - EV SSLサーバー証明書と同様に審査基準に応じた信頼性が担保されている
    - 厳格な審査を通ったブランドの正規メールであることを、ロゴ表示を確認することで誰でも**「見てわかる」**

現状、Webサーバーの信頼性をサーバー証明書で担保しているのであれば、メールも同様に信頼性を担保するのが望ましい

- **事業者から利用者への啓発推奨事項**
  - 迷惑メールフィルターがデフォルトで「無効」になっている場合が多いため、有効にしてもらう
  - ブランドアイコンやBIMI、公式アカウントなどによる正規メールの見分け方を啓発
  - 見分けられないメールサービスの利用は控えるよう啓発
  - メールアドレスの変更を促す（漏えいした情報の無効化）

- **メールサービス運用者への推奨事項**
  - DMARCによる認証とポリシーに従った配信を行う（送信者が指定したポリシーを無視しない）
  - 送信ドメイン認証、 FCrDNS認証に失敗した場合は、受信者がそれを認識・判断できるようにする
    - 迷惑メールフィルターの [meiwaku] や [spam] などのタグと同様に、[DMARC fail] 、[×] などを付加
    - メール表示時に警告を表示

最後に

正規メール（と、それ以外）
見てわかる、それが重要

以上、ご参考になりましたら幸いです。