2025年11月5日
JPAAWG 8th General Meeting in 高知

フィッシングの現状と対策 2025

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 **C**omputer **E**mergency **R**esponse **T**eam / **C**oordination **C**enter

  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」

【対策・予防】脆弱性情報ハンドリング → **【注意喚起】情報収集・分析情報発信** → **【初動対応】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

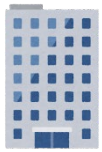
報告

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

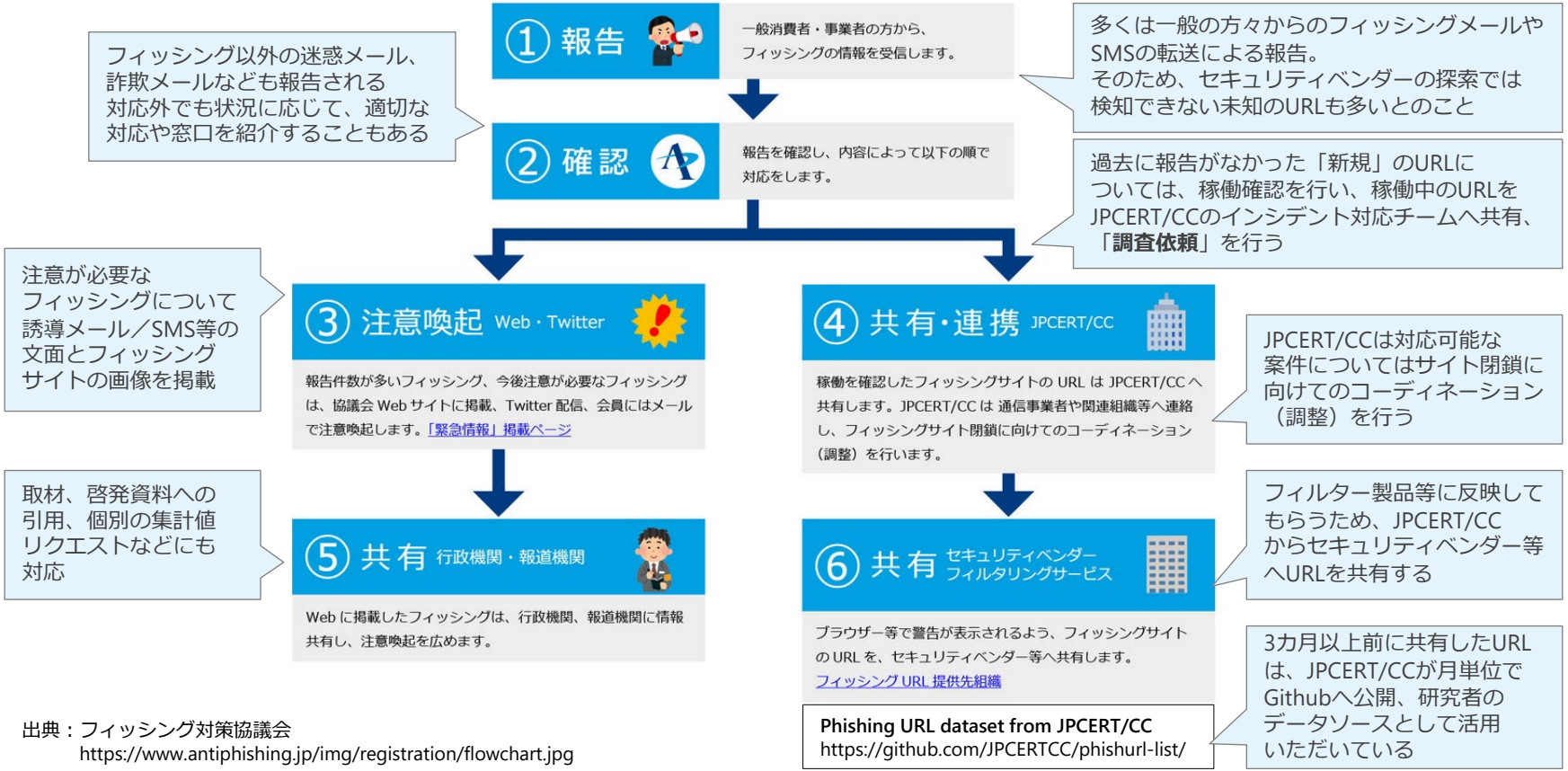
■学術研究
- 順天堂大学、香川大学

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/img/registration/flowchart.jpg

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

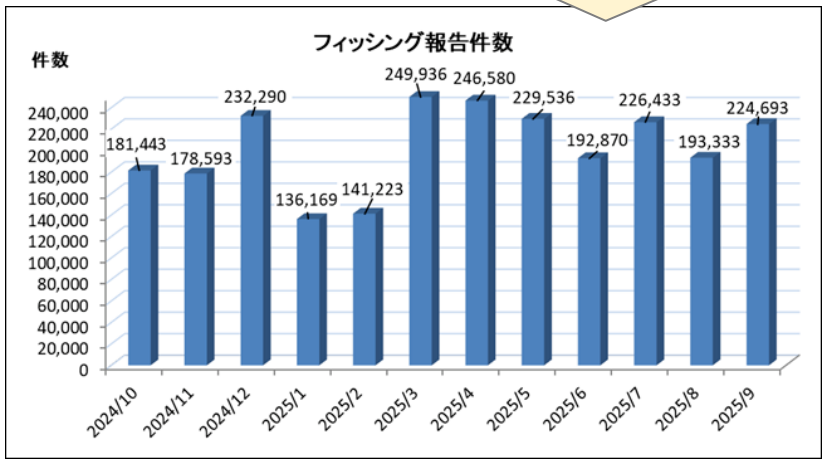
参考資料：フィッシング対策協議会 情報発信

- 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と報告状況

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

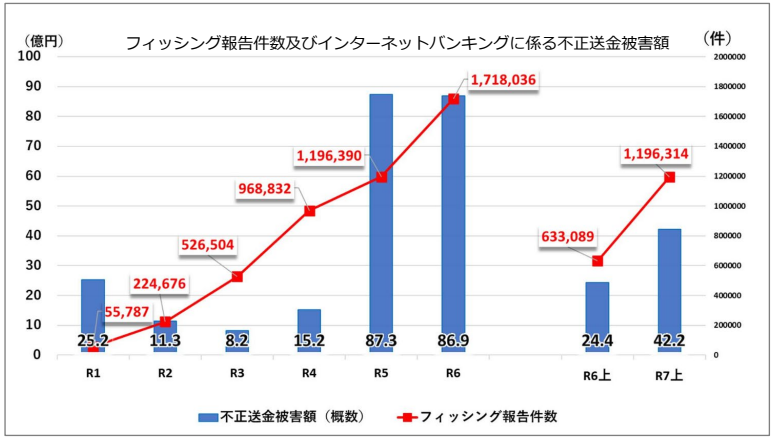
- 令和6年、不正送金被害件数、被害額は**減少傾向**
  - **令和5年 5,578件、87.3億円**
  - **令和6年 4,369件、86.9億円**

■ 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/r6/sonota/20241004/18.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が盛り込まれた

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/r6/sonota/20241004/18.pdf

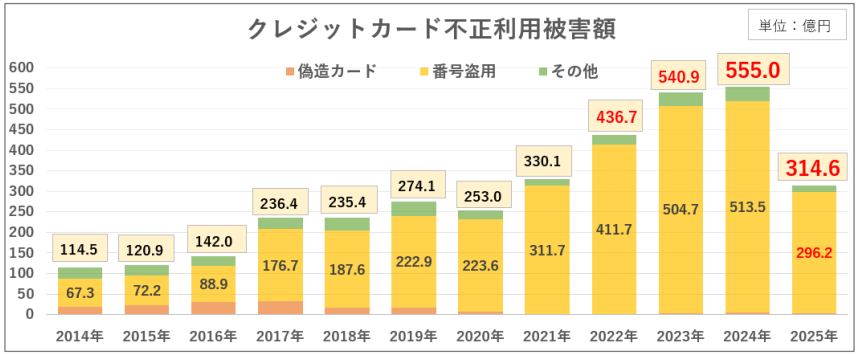
2024年～2025年 クレジットカード不正利用被害状況と対策

■ 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/news20250624_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、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

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
  - 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
  - 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

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

（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。

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

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

金融庁（fsa.go.jp）も2025年3月、p=rejectに変更

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

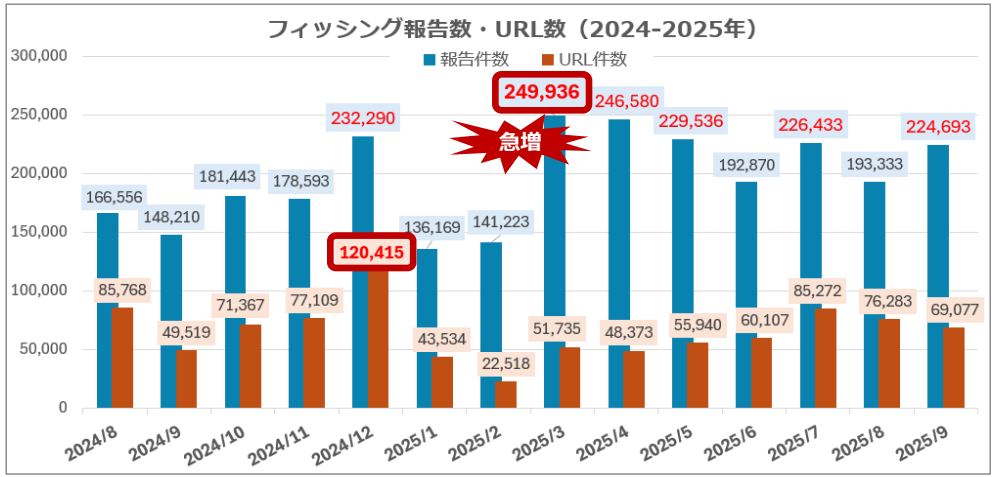
フィッシング報告の推移と傾向（2024年～2025年 月次）

■ 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）



報告数は、
公開情報としては2025年3月が過去最高

直近の2025年9月は、
迷惑メール判定済み等が約7万件、合わせると
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はほとんど無い

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
フィッシング事例と不正利用対策

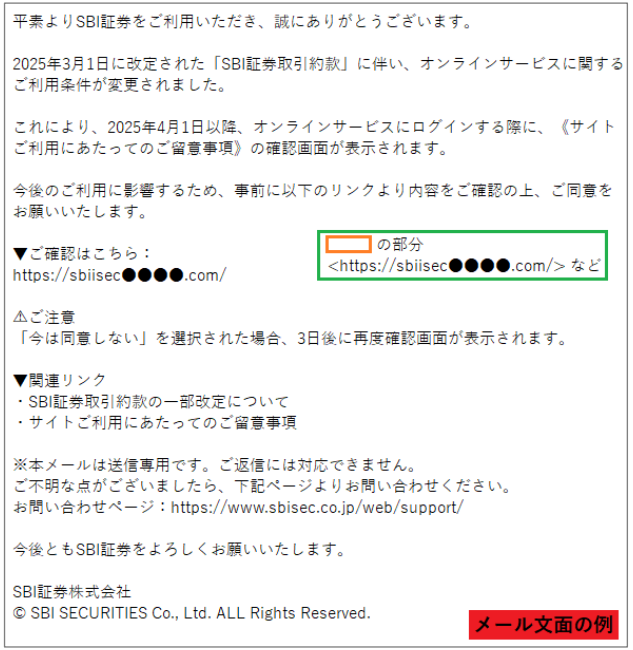
2025年の事例：証券会社をかたるフィッシング

■ 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/



平素よりSBI証券をご利用いただき、誠にありがとうございます。

2025年3月1日に改定された「SBI証券取引約款」に伴い、オンラインサービスに関するご利用条件が変更されました。

これにより、2025年4月1日以降、オンラインサービスにログインする際に、《サイトご利用にあたってのご留意事項》の確認画面が表示されます。

今後のご利用に影響するため、事前に以下のリンクより内容をご確認の上、ご同意をお願いいたします。

▼ご確認はこちら：
https://sbiisec●●●●.com/

□の部分
<https://sbiisec●●●●.com/> など

⚠ご注意
「今は同意しない」を選択された場合、3日後に再度確認画面が表示されます。

▼関連リンク
・SBI証券取引約款の一部改定について
・サイトご利用にあたってのご留意事項

※本メールは送信専用です。ご返信には対応できません。
ご不明な点がございましたら、下記ページよりお問い合わせください。
お問い合わせページ：https://www.sbisec.co.jp/web/support/

今後ともSBI証券をよろしくお願いいたします。

SBI証券株式会社
© SBI SECURITIES Co., Ltd. ALL Rights Reserved.

メール文面の例

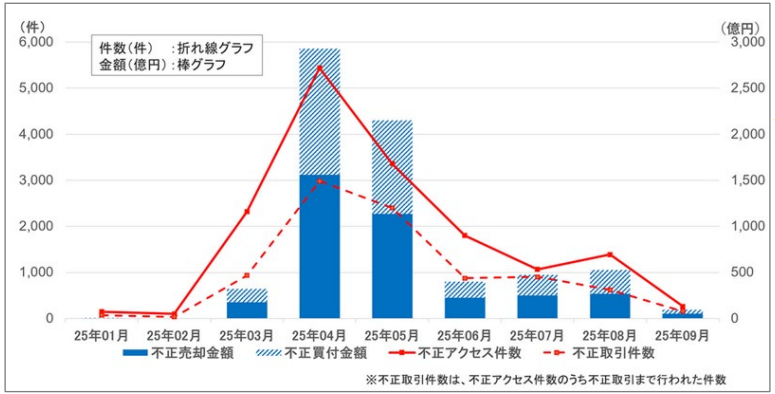
出典：フィッシング対策協議会「SBI証券をかたるフィッシング (2025/04/01)」
https://www.antiphishing.jp/news/alert/sbisec_20250401.html

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

9カ月間の不正取引額は
売買合わせて約6,903億円

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	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	5	–
不正アクセス件数	144	97	2,320	5,438	3,359	1,802	1,065	1,386	262	15,873
不正取引件数	69	34	935	2,984	2,398	873	903	618	156	8,970
売却金額（億円）	約2	約0.8	約175	約1,561	約1,135	約227	約251	約267	約51	約3,670
買付金額（億円）	約0.8	約0.8	約147	約1,369	約1,017	約173	約223	約259	約44	約3,233

※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/20250908.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

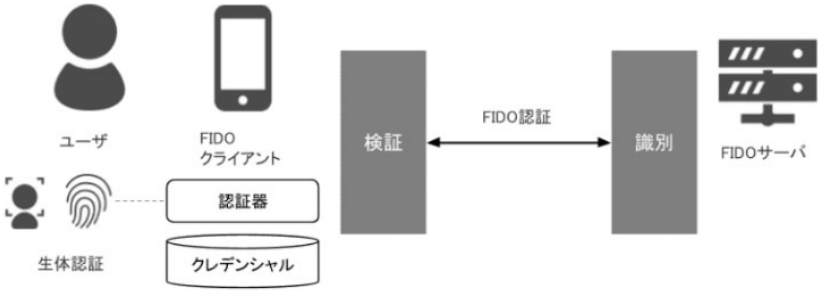
日本証券業協会**「多要素認証の設定必須化を決定した証券会社」**
https://www.jsda.or.jp/about/hatten/inv_alerts/alearts04/list_tayouso/index.html

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

不正利用対策：認証強化（パスキー）

- **FIDO認証／Passkey（FIDO2）**
  - 認証にパスワードを使用しないパスワードレスの技術
  - パスキーと呼ばれるオンライン認証の仕組みで、スマートフォンなどの生体認証を使用して個人認証が可能
  - 公開鍵方式を採用し、認証情報である秘密鍵が端末内で安全に管理され、セキュリティリスクを低減
  - 正規でないサイトへのアクセスを防ぐことが可能となり、パスワードに起因するフィッシング被害を防ぐ
  - SMS／メール認証を置き換えることで、リアルタイムフィッシングへの対策効果が期待できる



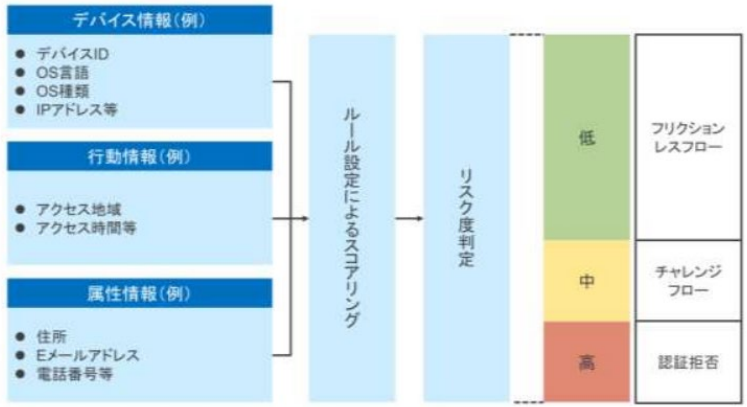
出典：フィッシング対策協議会「フィッシングレポート2024」https://www.antiphishing.jp/report/phishing_report_2024.pdf

不正利用対策：認証強化（リスクベース認証）

■ リスクベース認証とは

- クレジットカード決済（EMV 3Dセキュア）で使用
- さまざまなデータを使い、本人の利用か確認を行い認証する仕組み
- 判定に使う情報例
  - 利用者が決済に使用するデバイス情報
  - 利用者から提供される個人情報
  - アクセス地域や時間
- 判定されたリスク度に応じて、追加の認証を要求する
- リアルタイムフィッシング被害が多い
  オンラインバンキングや証券サービスの分野でも普及が進みつつある

図 2 【リスクベース認証のイメージ】



① フリクションレスフローとチャレンジフロー

リスクベース認証で判定されたリスク度合いに応じて、認証処理は下記の通りフローが異なる。

・低：フリクションレスフローとして動的（ワンタイム）パスワードの入力等なしに認証が完結する。

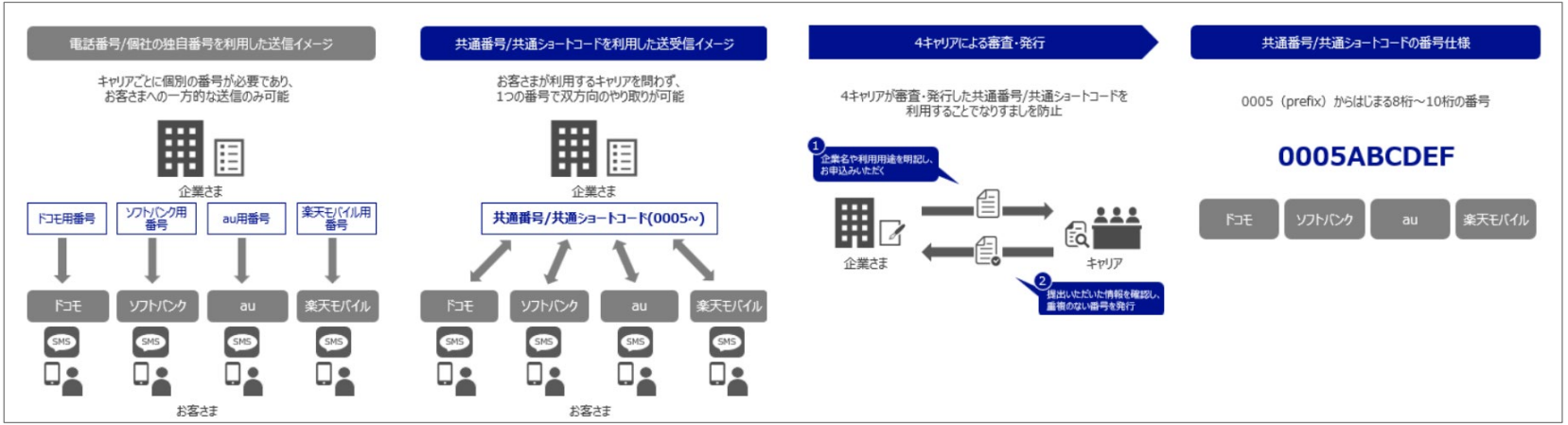
・中：チャレンジフローとして会員に対して追加の認証（動的（ワンタイム）パスワードの入力等）を要求する。

・高：認証拒否

出典：クレジット取引セキュリティ対策協議会「EMV 3-D セキュア導入ガイド 2.0版」
https://www.j-credit.or.jp/security/pdf/secure_installation_guide.pdf

スミッシングへの対策：SMS送信元表示名 共通番号

- ドコモ、KDDI、ソフトバンク、楽天モバイルの携帯キャリア4社が企業単位で審査・発行する「0005」から始まる8～10桁の表示名
- 重複のない番号で**なりすまし防止**
- 携帯キャリア4社で共通の番号のため**正規メッセージを判別可能**
  - 審査済み番号は以下のサイトで調べることができる
    「SMS共通番号/共通ショートコード情報」https://japansms.com/

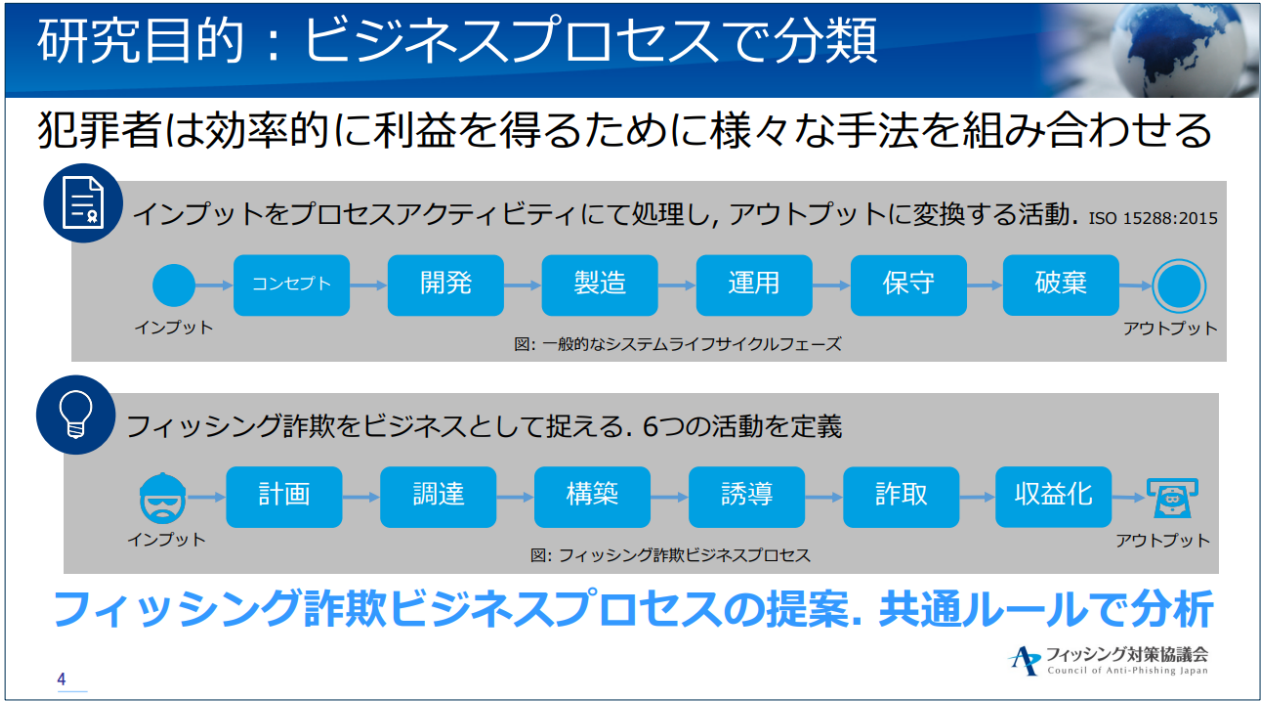


出典：「SMS共通番号/共通ショートコード情報」https://japansms.com/

2025年
フィッシング報告からみる
フィッシングサイトへ
アクセスさせないための対策

「対応」と「対策」

■ フィッシング詐欺のビジネスプロセス分類
https://www.antiphishing.jp/news/collabo_20210316_CSEC.pdf



発生したフィッシング行為には「対応」（事後）
例）テイクダウン、
問い合わせ・被害への対応

以後、フィッシング行為の発生や被害を防ぐのは「対策」（事前）
例）フィッシングメール対策、SMSやWebサイトアクセスに対するフィルター、認証強化など

「対応」＝「対策」ではない。両方必要であり、それが「対応」なのか「対策」なのかを分類し、隙のないよう実施することで、全体として「被害抑制」などの効果が出る

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。

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

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。

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

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

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いなかったことが、大きな要因の一つといえる。

正規メール視認性向上の取り組み（BIMI）

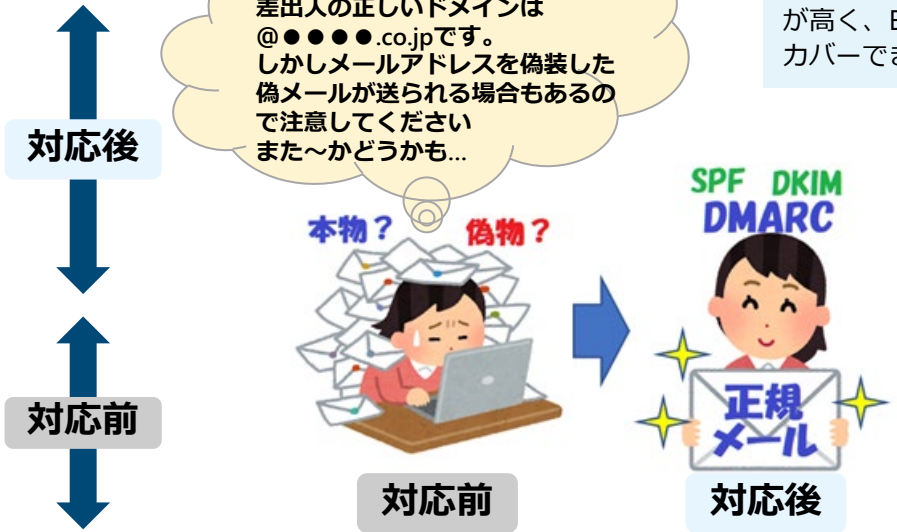
- 利用者にとって必要なのは、正規メールか否かの判断を助ける情報
- 長い文章で注意を書いても読まないし、判断が難しい
- BIMI対応であれば、ブランドロゴが表示されているかどうかだけ確認すれば良い

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



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？

このスライドも長らく使い回していますが今一度おさらい

■ BIMI対応ブランド、増えています！

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

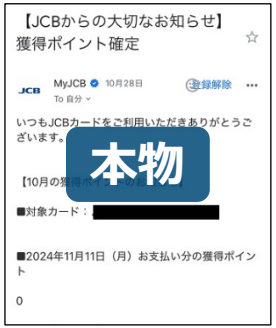
ブランドロゴが表示されていると、目立つし安心感を与える

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らない

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

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

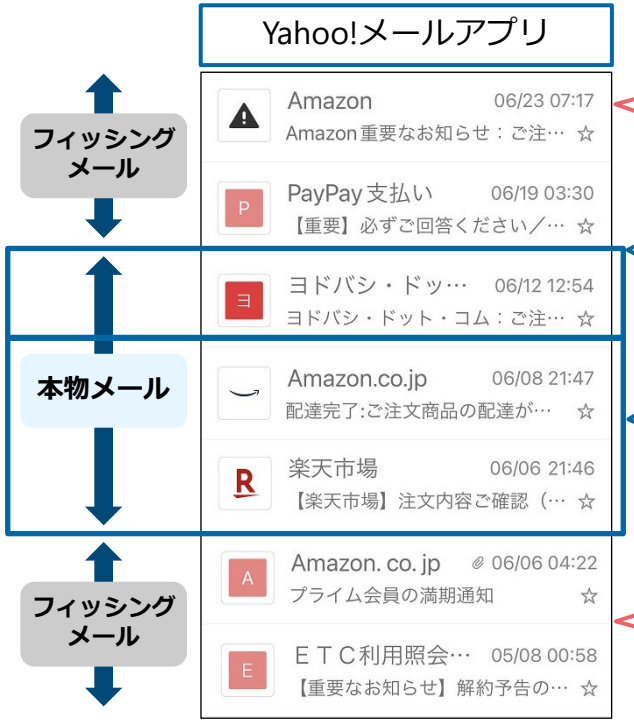
各メールサービスでの対応が
難しい場合は、BIMI対応
メールサービスとの併用を
利用者へ推奨すべき

正規メール視認性向上の取り組み（Yahoo!メール）

このスライドも長らく使い回していますが今一度おさらい

- 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/

この表示の違いを十分に周知する！



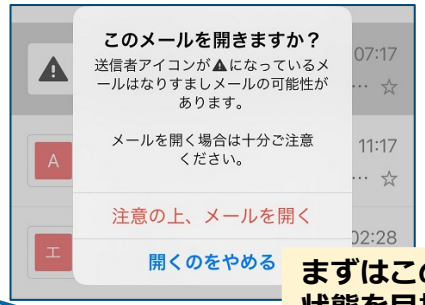
送信ドメイン認証で検証失敗したなりすましメールには警告マークが出る

正規メール
送信ドメイン認証の結果を利用し、ブランドカラーとメッセージが表示される

正規メール
送信ドメイン認証の結果を利用し、ブランドアイコンが表示される

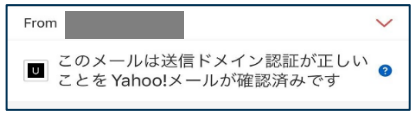
正規以外のドメインのメールアドレスで送られたフィッシングメール

開こうとすると警告表示！



まずはこの状態を目指す

ブランドカラー対象のメールにはメッセージが表示される



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）

このスライドも長らく使い回していますが今一度おさらい

- 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

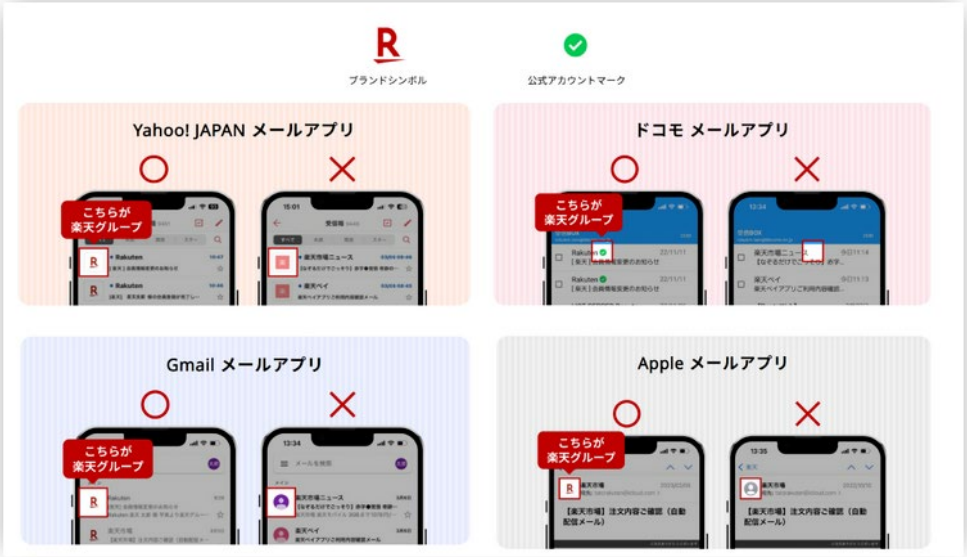


図 2　送信ドメイン認証をパスした正規メールの表示例

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

- なりすまされたドメイン名のDMARC設定率は増加
  なりすましに使われることへの対策として、DMARCはかなり普及してきた
  DMARC Enforce率も増加しているが、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
- 直近では非なりすましDMARC pass率（独自ドメイン名でDMARC設定を行っている）が増加傾向となっている
- 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）
  - 送信元IPアドレスの逆引き設定の情報を利用したFCrDNS認証（Forward-confirmed reverse DNS）
    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

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

下の表の数値は、上の表の「なりすましメール」の値の内訳

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（モニタリングモードから始め、p=quarantineそして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、可能であれば対応を検討
    - 認証マーク証明書（VMC：Verified Mark Certificates）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（入口対策）**
  - 迷惑メールフィルターの利用
    国内ISPのメールサービスでは、迷惑メールフィルターがデフォルトで「無効」になっているので、有効にする
  - 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（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（入口対策）**
  - DMARCによる認証を行い、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）
  - FCrDNS認証、送信ドメイン認証に失敗した場合は、受信者にそれを判断できるようにする
    例）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

最後に

弱い認証のままでは狙われます
認証強化を！

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。

以降、参考資料
(時間がなく、会場でお話できなかった分)

2025年
フィッシング事例・手法

2025年の事例：正規のキャッシュレス決済画面で送金させる

- クレジットカードの月額請求をかたる文面でキャッシュレス決済画面に誘導する
- キャッシュレス決済の認証情報を入力すると不正送金される
- 2023年にも発生しており、ISP月額料金の請求を装い、ISPのアカウント情報を詐取した後、キャッシュレス決済の本物の決済画面に誘導していた

出典：フィッシング対策協議会「PayPayカードをかたるフィッシング (2025/05/21)」
https://www.antiphishing.jp/news/alert/paypay_20250521.html

出典：フィッシング対策協議会
「OCN をかたるフィッシング (2023/01/04)」
https://www.antiphishing.jp/news/alert/ocn_20230104.html

PayPayでは
- 利用可能額の設定
- 端末認証

等を推奨しているが、本物と信じて操作しているので、
- リンクから決済画面に誘導されたら一度操作を中断
- メールの認証情報や請求元サービスのアプリで確認

を心がける必要がある。

2025年の事例：大量に生成されたフィッシングURL

- ランダム文字列サブドメイン名＋独自ドメイン名で大量生成
  - ワイルドカードでネームサーバーに登録されているので、
    サブドメインは何を指定しても同じIPアドレスが返ってくる
  - 最近はIPv6アドレスも振られている　あるクラウド発のフィッシングメールも IPv6で配信されてくる

□ メール内のURL表記

マイル加算
<https://zhjinghua.com%E2%88%95bknTOWs%E2%88%95onAwEItKWU%E2%88%95hLFzbZQBV@rgam.sinoroad.me/wgpp.co.jp>

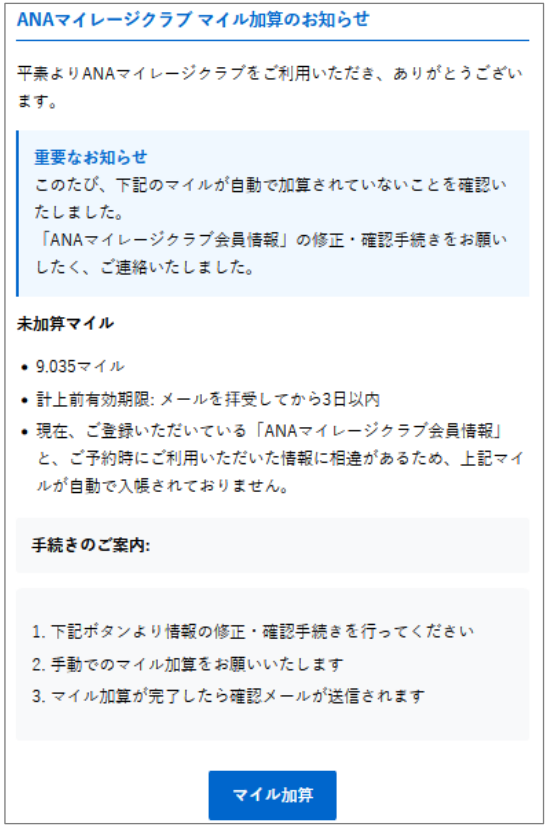
□ ブラウザーに認識されるURL

https://rgam.sinoroad.me/wgpp.co.jp　Basic認証表記なので@以降の文字列のみ認識

□ ワイルドカードで登録されており、IPv6 Ready

```
$ host *.sinoroad.me
*.sinoroad.me has address 104.21.68.224
*.sinoroad.me has address 172.67.199.50
*.sinoroad.me has IPv6 address 2606:4700:3033::ac43:c732
*.sinoroad.me has IPv6 address 2606:4700:3030::6815:44e0
```

フィッシングに使われたドメイン名がワイルドカードで登録されているか確認できた場合は、ドメイン名ごとにフィルター登録等の処理が必要。また、複数IPv4／IPv6アドレスの割り当てがされているケースがあることを認識しておく。



2025年の事例：Google翻訳の悪用

- 2025年2月以降、Google翻訳URLの悪用が急増する
  translate.google.*（com、jp、その他のccTLD）
- 正規のURLを（動作には関係ない）パラメーターに埋め込んで、無害を装うものもある（正規利用のGoogle翻訳ではパラメーターに翻訳元のURLが入る）
- 2022年にもGoogle翻訳のURL悪用が増えており、このような手法は対策の隙を狙って周期的に発生すると考えられる。

参考: Google 翻訳の正規 URL から誘導されるフィッシング (2022/08/09)
https://www.antiphishing.jp/news/alert/googletranslate_20220809.html

2025/5/19	19:38:31	松井証券	https://h85nnsbv3ypjv-pages-dev.translate.goog/www.matsui.co.jp.html?_x_tr_sch=&_x_tr_
2025/5/19	19:39:01	Apple	https://lyct7sxa2y491-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_s
2025/5/19	19:39:14	Apple	https://ygaop0gw76plh-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr
2025/5/19	19:40:44	松井証券	https://nzznakhin0a8-pages-dev.translate.goog/www.matsui.co.jp.html?_x_tr_sch=&_x_tr_s
2025/5/19	19:40:51	ANA	https://runy2xdxsjpz5-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex
2025/5/19	19:44:30	SBI証券	https://bxlblwyeq1byb-pages-dev.translate.goog/site4.sbisec.co.jp.html?_x_tr_sch=&_x_tr_s
2025/5/19	19:44:51	Apple	https://tuvmo3xuymgqz-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_t
2025/5/19	19:45:33	ANA	https://dpq0ndtsul3yf-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex
2025/5/19	19:45:34	ANA	https://expuz3tq6uvfg-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex
2025/5/19	19:45:58	Apple	https://d5eq5ylun65tg-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_
2025/5/19	19:46:26	ANA	https://expuz3tq6uvfg-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex
2025/5/19	19:47:13	Apple	https://kg4sbfqxzwlbu-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_
2025/5/19	19:47:33	SBI証券	https://540qkoz4qdqpx-pages-dev.translate.goog/site4.sbisec.co.jp.html?_x_tr_sch=&_x_tr_
2025/5/19	19:49:54	Amazon	https://rapid--boat--bcb9-shaoye5625-workers-dev.translate.goog/amazon?_x_tr_sl=monex
2025/5/19	19:50:24	Apple	https://ygaop0gw76plh-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr
2025/5/19	19:50:24	松井証券	https://vr0wmt7puh0uf-pages-dev.translate.goog/www.matsui.co.jp.html?_x_tr_sch=&_x_tr_
2025/5/19	19:50:24	SBI証券	https://p2h6zjz3uyvbk-pages-dev.translate.goog/site4.sbisec.co.jp.html?_x_tr_sch=&_x_tr_s

分野	1月	2月	3月	4月	5月	6月	7月	8月	9月	合計
EC	384	8,737	17,114	6,071	18,225	6,527	3,476	667	35	61,236
証券			104	5,942	34,484	1,301	1,360	43		43,234
クレカ	2,744	3,063	3,066	7,847	5,552	2,656	1,717	595	35	27,275
航空		8	103	833	3,608	1,412	835	99	7	6,905
決済	344		2,901	31	129	67	10	19		3,501
銀行	212	559	1,147	418	337	32	437	284	1	3,427
配送	236	553	122	705	813	32	192	16		2,669
電力・ガス・水道			25	224	1,183	453	410	193	2	2,490
交通	361			1	1,152	447	342	3		2,306
サービス			21	144	1,243	14	9			1,431
放送					590	1		1		592
官公庁		62	15	280	60		115	1		533
モバイル				18	93	141	139			391
貸金	306									306
SNS				191						191
小売							89	75	1	165
メール				47		1				48
旅行				8						8
仮想通貨							1	2		3
合計	4,587	12,982	24,618	22,760	67,469	13,084	9,132	1,998	81	156,711

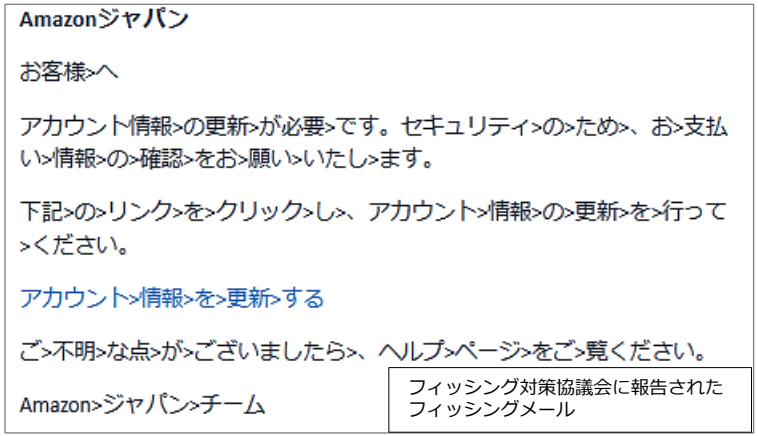
対象ブランド・分野を問わず、一般的なフィッシング対応／対策回避の手法としてGoogle翻訳URLが悪用されており、ブランドによっては、月次報告の半数近くを占めていたが、2025年8月以降、いったん沈静化。

正規サービスのURLの悪用については、フィッシングメールが配信された時点では悪性か否かを判断するのが難しいため、今までと同じ判定基準の迷惑メールフィルターでは効果が出るまでに時間がかかる＝すり抜けしやすいように見える

2025年の事例：font-size:0pxでゴミ混ぜ

- HTMLメールで非表示となるゴミ文字列を混ぜて、フィルターの判定を回避しようとする試み
- メールをテキストで処理していると判定ができない

font style="font-size:0px; color:transparent;">ふへほ&#8203>願いまみむ&#8203>いたしめもや&#8203>ます。 下記ゆよら&#8203>のりるれ&#8203>リンクろわが&#8203>をぎぐげ&#8203>クリックござじ&#8203>しずぜぞ&#8203>、アカウントだぢづ&#8203>情報でどば&#8203> のびぶべ&#8203>更新ぼぱぴ&#8203>をぷぺぽ&#8203>行ってぁぃぅ&#8203>ください。



Amazonジャパン

お客様へ

アカウント情報の更新が必要です。セキュリティのため、お支払い情報のご確認をお願いいたします。

下記のリンクをクリックし、アカウント情報のご更新を行ってください。

アカウント情報を更新する

ご不明な点がございましたら、ヘルプページをご覧ください。

Amazonジャパンチーム

フィッシング対策協議会に報告されたフィッシングメール

font-size:0pxは実質的に表示されないにも関わらず多くの文字列を混ぜているということは、よからぬことを企んでいるメールとして、迷惑メール判定してよいと思われる

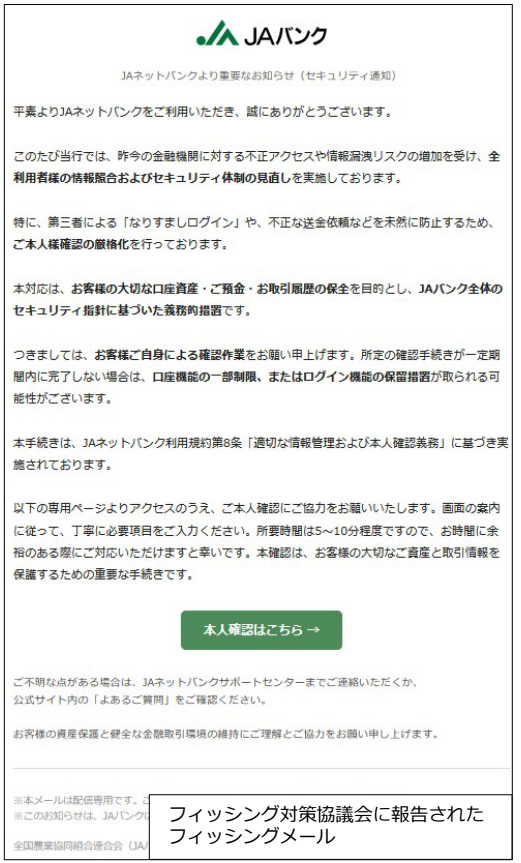
2025年の事例：<FONT style=“display:none”>でゴミ混ぜ

- HTMLメールで非表示となるゴミ文字列を混ぜて、フィルターの判定を回避しようとする試み
- メールをテキストで処理していると判定ができない

J<FONT style="display:none;">wahmyzy</FONT>A<FONT style="display:none;">
lafuh</FONT>ネ<FONT style="display:none;">tvtiaajv</FONT>
FONT style="display:none;">yvyrt</FONT>ト<FONT style="display:none;">mydigctc</FONT>
バ<FONT style="display:none;">xvosg</FONT>ンク<FONT
style="display:none;">kpuaib</FONT>よ<FONT style="display:none;">kdjck</FONT>り
<FONT style="display:none;">bgmyy</FONT>重<FONT style="display:none;">rtscqo</FONT>
要<FONT style="display:none;">hcpq</FONT>な<FONT
style="display:none;">sgdtav</FONT>お<FONT style="display:none;">ehbj</FONT>知<FONT
style="display:none;">mvurgwyv</FONT>ら<FONT style
="display:none;">rvpc</FONT>せ（<FONT style="display:none;">cuwjl</FONT>セキ<FONT
style="display:none;">bsldefxj</FONT>ユリ<FONT style="display:none;">tifqc</FONT>テ<FO
NT style=“display:none;”>bpsdtq</FONT>イ<FONT style=“display:none;”>npjxkrs</FONT>通
<FONT style=“display:none;”>iqprx</FONT>知<FONT
style=“display:none;”>wmiwm</FONT>） </p>

1行目の“JAネットバンクより重要なお知らせ（セキュリティ通知）”の部分のもとの表記は=E3=83=8Dなど
URLエンコードされているので、上記はわかりやすいようにデコードしている

特定のMSPユーザーからのみ報告がきている（狙って送信していると考えられる）。
<FONT style=“display:none”>は実質的に表示されないので、よからぬことを企んでいるメールとして、迷惑メール判定してよいと思われる


JAバンク

JAネットバンクより重要なお知らせ（セキュリティ通知）

平素よりJAネットバンクをご利用いただき、誠にありがとうございます。

このたび当行では、昨今の金融機関に対する不正アクセスや情報漏洩リスクの増加を受け、全**利用者様の情報照合およびセキュリティ体制の見直し**を実施しております。

特に、第三者による「なりすましログイン」や、不正な送金依頼などを未然に防止するため、**ご本人様確認の厳格化**を行っております。

本対応は、**お客様の大切な口座資産・ご預金・お取引履歴の保全**を目的とし、**JAバンク全体のセキュリティ指針に基づいた義務的措置**です。

つきましては、**お客様ご自身による確認作業**をお願い申上げます。所定の確認手続きが一定期間内に完了しない場合は、**口座機能の一部制限、またはログイン機能の保留措置**が取られる可能性がございます。

本手続きは、JAネットバンク利用規約第8条「適切な情報管理および本人確認義務」に基づき実施されております。

以下の専用ページよりアクセスのうえ、ご本人確認にご協力をお願いいたします。画面の案内に従って、丁寧に必要項目をご入力ください。所要時間は5〜10分程度ですので、お時間に余裕のある際にご対応いただけますと幸いです。本確認は、お客様の大切なご資産と取引情報を保護するための重要な手続きです。

本人確認はこちら →

ご不明な点がある場合は、JAネットバンクサポートセンターまでご連絡いただくか、
公式サイト内の「よあるご質問」をご確認ください。

お客様の資産保護と健全な金融取引環境の維持にご理解とご協力をお願い申し上げます。

※本メールは配信専用です。ご
※このお知らせは、JAバンク

全国農業協同組合連合会（JA

フィッシング対策協議会に報告されたフィッシングメール

2025年の事例：不完全なURLがリンクとして機能する問題

■ お支払い手順

1. 下記ボタンよりお支払いサイトにアクセス
2. お客様番号とお名前を入力
3. 表示される手順に従いお支払いを完了

お支払いサイトへアクセス

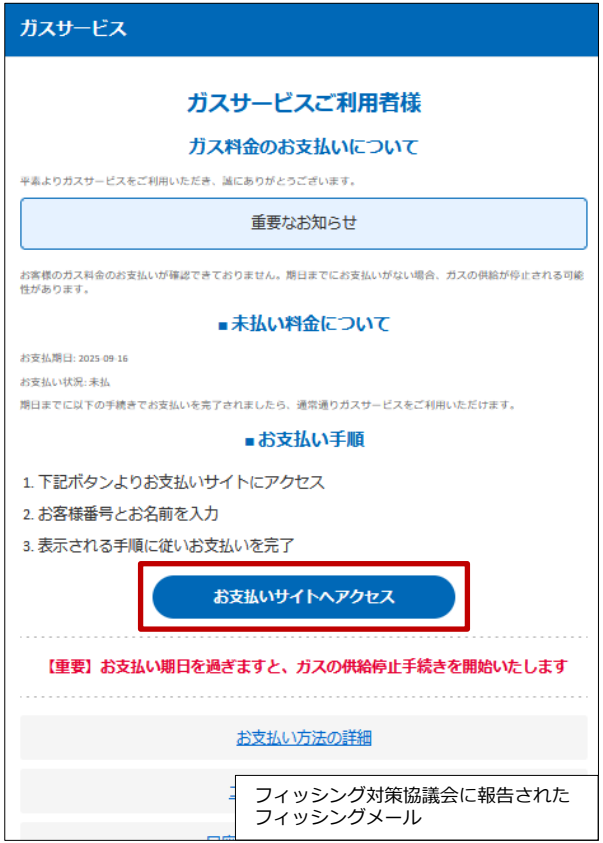
https://artthszga.wmotl.com/

<https:s[redacted].co.jp%2Fushio_atsuo_star%2Fvaehw%2Fhvzlvlty%2Foqfjl%2398186$2Ffzzkbunu%2Fyzgrlm@artthszga.wmotl.com>

【重要】お支払い期日を過ぎますと、ガスの供給停止手続きを開始いたします

お支払い方法の詳細 <https://www.[redacted].co.jp/payment/methods/> コンビニでのお支払い <https://www.[redacted].co.jp/payment/convenience/> 口座自動引き落としのご案内 <https://www.[redacted].co.jp/payment/automatic/> お問い合わせ <https://www.[redacted].co.jp/contact/>

.co.jpのURLはランダム文字列のドメイン名で、いくつか調べたが実在していない。
迷惑メール判定を緩和する目的と思われる



フィッシング対策協議会に報告された
フィッシングメール

- 一部のメールアプリではhttps:やホスト名だけでもリンクになる
- BASIC認証表記部分は捨てられるので、ゴミをたくさん混ぜる
  最近よく使われるゴミは%2F（スラッシュ）
- このような細工をされた不完全なURL表記はアクセスできない方が安全
- 脆弱性と言っていいレベルの危険な実装であり、Webメールやアプリでリンクにしている場合は要修正（「親切な実装」は現代では不要）

2025年の事例：不完全なURLがリンクとして機能する問題

■ マイル利用手順

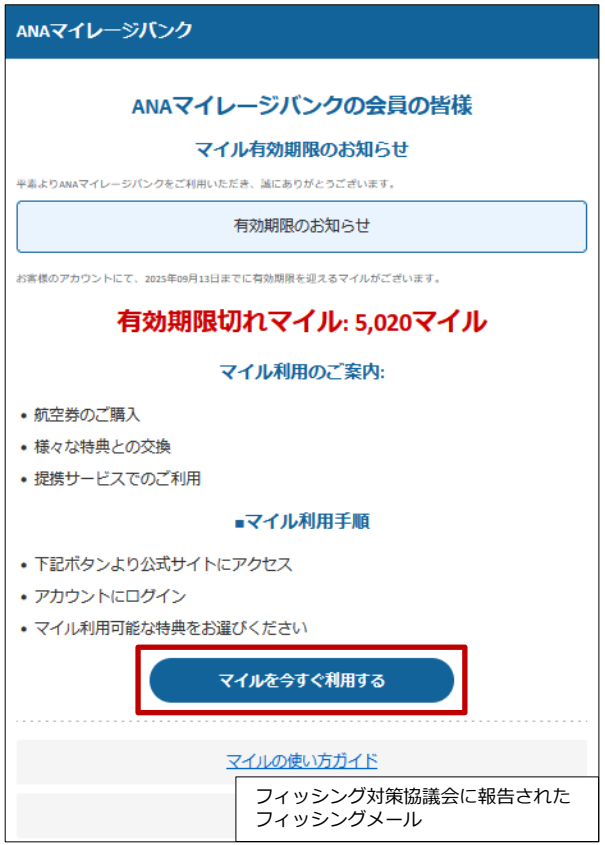
* 下記ボタンより公式サイトにアクセス
* アカウントにログイン
* マイル利用可能な特典をお選びください

マイルを今すぐ利用する
<https:/example@[redacted].ne.jp%2Fkpogw%2FXqtfb%23jtysls@jmnbfr.com>
マイルの使い方ガイド <https://[redacted].co.jp/jp/ja/jmb/guide/use/>提携サービス一覧 <https://[redacted].co.jp/jp/ja/jmb/partner/>航空券特典
<https://[redacted].co.jp/jp/ja/jmb/travel/award-ticket/>有効期限について
<https://[redacted].co.jp/jp/ja/jmb/guide/expiration/>

https://jmnbfr.com/

こちらも前ページと同様。迷惑メール評価を避ける目的と思われる

- 前ページの例の派生版で/が一つ（https:/）となっている
- 受信者のメールアドレスがURLに含まれているが、評価がホスト部において最右最短一致となっており、最初の@は無視されている
- メールアドレスをBASIC認証のIDとして使う場合は@を%40に変換するルールとなっており、実際に%40に変換するメールアプリがあった
- このような細工をされた不完全なURL表記はアクセスできない方が安全
- 脆弱性と言っていいレベルの危険な実装であり、Webメールやアプリでリンクにしている場合は要修正（「親切な実装」は現代では不要）
- 現代の一般的なWebブラウザーでは無効にされる部分なので%40変換も不要



フィッシング対策協議会に報告されたフィッシングメール

2025年の事例：電話番号認証を装ったフィッシング

- 電話番号と認証コードを盗み、アカウントの本人認証に不正利用する
- さまざまなブランド、メール文面があるが、現在のところ、特定のオンラインサービスからのみ認証コードが届いている

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

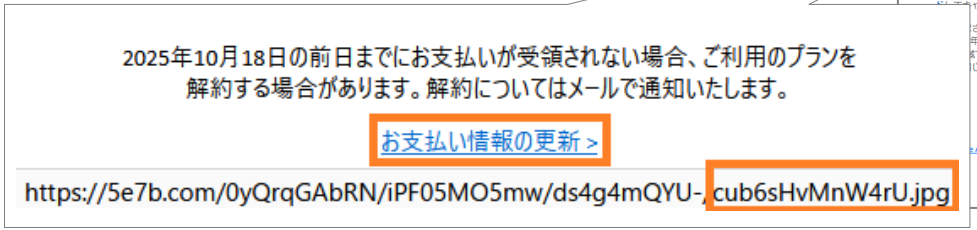
フィッシング対策協議会に報告された
フィッシングメールおよびフィッシングサイトより

2025年の事例：画像等のリンクを装ったURL

- 2025年7月、フィッシングサイトのURLで.jpg（通常は画像ファイル）などの拡張子で終わるものが確認される
- その後、さまざまな拡張子が報告される
  - .jpg
  - .gif
  - .zip
  - .pdf
  - .png
  - .mp4
  - .webp
  - .json
- 2025年7月はworkers.devにホスティングされていた

```
hxxps://dlpj-m5s9ez.pokejunct.workers.dev/{中略}gMB3jbGFK_wQc.gif
hxxps://3ac6-eew5q.ninocar795.workers.dev/{中略}zgC_BnBZjKg.png
hxxps://lis9-8tjl1.ninocar795.workers.dev/{中略}BxGaHP2S_gbGA.jpg
```

- 基本的にこれらはリダイレクターとして機能しており、拡張子での判定では迷惑メールフィルターおよびURLフィルターのチェックから除外される可能性もある
- 2025年7月以降、あまり見かけなくなったが、10月にふたたび同様のケースが発生（右のメール）
- 拡張子が.jpgでも人が見てクリックしようと判断するリンクにひも付いていないか確認する必要がある



フィッシング対策協議会に報告されたフィッシングメールおよび誘導先のフィッシングサイト

正引き／逆引きとは

- DNSの正引き／逆引きとは

DNS(*1)の主なサービスはホスト名（ドメイン名）とIPアドレスを対応づけることです。DNSを用いて、www.nic.ad.jpのように表されるホスト名から、202.12.30.144のように表されるIPアドレスを解決することを正引きと呼んでいます。インターネットに接続されているコンピュータ同士は、IPアドレスを使って通信をしていますが、この正引きの仕組みによって、ユーザはIPアドレスを意識することなく、より覚えやすいホスト名によって、インターネット上の各サービスを利用することができます。
正引きとは反対に、202.12.30.144で表されるIPアドレスから、www.nic.ad.jpというホスト名を解決することを逆引きと呼びます。逆引きは、正引きとの組み合わせによってデータ送信者の識別の正確性を高める働きをもっています。

出典：JPNIC「正引き/逆引きとは」https://www.nic.ad.jp/ja/basics/terms/seibiki-gyakubiki.html

- 正引き（ホスト名からIPアドレスを得る）
  - ・ドメイン名の管理者（登録者）が自由に任意に設定可能
  - ・ホスト名に対してAレコードを登録

```
■mailserv.example.co.jpを正引き
mailserv.example.co.jp.  IN  A  192.0.2.1
```

- 逆引き（IPアドレスからホスト名を得る）
  - ・IPアドレスを管理している事業者（ホスティング事業者・ISP等）が逆引きを登録・管理する
  - ・IPアドレスに対応したin-addr.arpaという特別なドメイン名空間に対してPTRレコード登録
  - ・IPアドレス利用者が任意のホスト名を登録したい場合は、基本的にはホスティング事業者へ登録を依頼する

```
■IPアドレス 192.168.1.1を逆引き
1.2.0.192.in-addr.arpa.  IN  PTR  mailserv.example.co.jp.
```

- 契約してすぐ仮想サーバーを大量に作成し、フィッシングメールを送り終わったらサーバーを消す、という、今までの「送り逃げ」のような送信がやりづらくなる
- 不正利用されるホスティング事業者側は、逆引き設定の手続きを行う契約者を検知できるため、事前の対処がしやすくなる＝攻撃者にとっては足がつきやすい
- 攻撃者の特定および攻撃抑制効果が期待できる

正引きはドメイン名の管理者が任意のタイミングで登録・有効化・削除することができるが、逆引きは使用するIPアドレスを管理している事業者でなければ登録・有効化・削除できない。そのため逆引き登録は利用形態に制限（無料枠では設定できない、固定的に割り当てられたIPアドレスにしか設定できない等）が発生すると考えられる

逆引きを利用した認証（FCrDNS認証）とは

- FCrDNS（Forward-confirmed reverse DNS）

特定のIPアドレスが前方（名前からアドレスへ）と後方（アドレスから名前へ）の両方向のドメイン名システム（DNS）エントリーを持ち、お互いに一致している状態を指す。

出典：WikiPedia「正引きで確認された逆引きDNSエントリ」https://ja.wikipedia.org/wiki/正引きで確認された逆引きDNSエントリ

1. IPアドレス 192.0.2.1を逆引き
   1.2.0.192.in-addr.arpa. IN PTR mailserv.example.co.jp.
2. mailserv.example.co.jpを正引き
   mailserv.example.co.jp. IN A 192.0.2.1
3. IPアドレスが一致しているか確認

逆引き（PTRレコード）が存在するかのみ認証しても効果はあるが、FCrDNS認証による正逆一致まで行うと、多くのフィッシングメールは判定・検知できる

- Gmail「メール送信者のガイドライン」での要件

重要: 送信元 IP アドレスは、ポインタ（PTR）レコードで指定されたホスト名の IP アドレスと一致している必要があります。

送信元 SMTP サーバーのパブリック IP アドレスには、対応するホスト名を参照する PTR レコードが必要です。これは、リバース DNS ルックアップと呼ばれます。このホスト名には、送信元サーバーと同じパブリック IP アドレスを参照する A レコード（IPv4 の場合）または AAAA レコード（IPv6 の場合）も必要です。これは、フォワード DNS ルックアップと呼ばれます。

出典：Google「メール送信者のガイドライン」インフラストラクチャ設定の要件とガイドライン：IP アドレス
https://support.google.com/a/answer/81126?&p=sender-guidelines-ip&rd=1#ip

・リバース DNS ルックアップ＝rDNS＝逆引き
・フォワード DNS ルックアップ＝fDNS＝正引き

- 「どのようなエラーコードが送信されますか」

エラーコード 4.7.23	このメールの送信元 IP アドレスに PTR レコードがないか、PTR レコードの前方DNS エントリが送信元 IP アドレスと一致しません。迷惑メールからユーザーを保護するため、この送信者からのメールに対して一時的にレート制限が適用されます。
エラーコード 5.7.25	このメールは送信元 IP アドレスに PTR レコードがないか、転送 DNS エントリが送信元 IP アドレスを参照していないため、ブロックされました。Gmail では、送信元 IP アドレスに PTR レコードが必要です。

出典：Google「メール送信者のガイドラインに関するよくある質問」メール送信者のガイドラインの適用：どのようなエラーコードが送信されますか？
https://support.google.com/a/answer/14229414?hl=ja#zippy=%2Cどのようなエラーコードが送信されますか