2026年11月5日
JPAAWG 9th General Meeting

フィッシングの最新動向と必要な対策（2026年版）



一般社団法人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

© 2026 JPCERT/CC

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：147組織**（2026年10月時点）
    （正会員：118社、リサーチパートナー：5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

© 2026 JPCERT/CC

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**



© 2026 JPCERT/CC

フィッシング対策協議会の活動

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

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



■ 情報発信
- 緊急情報（注意喚起）
- 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

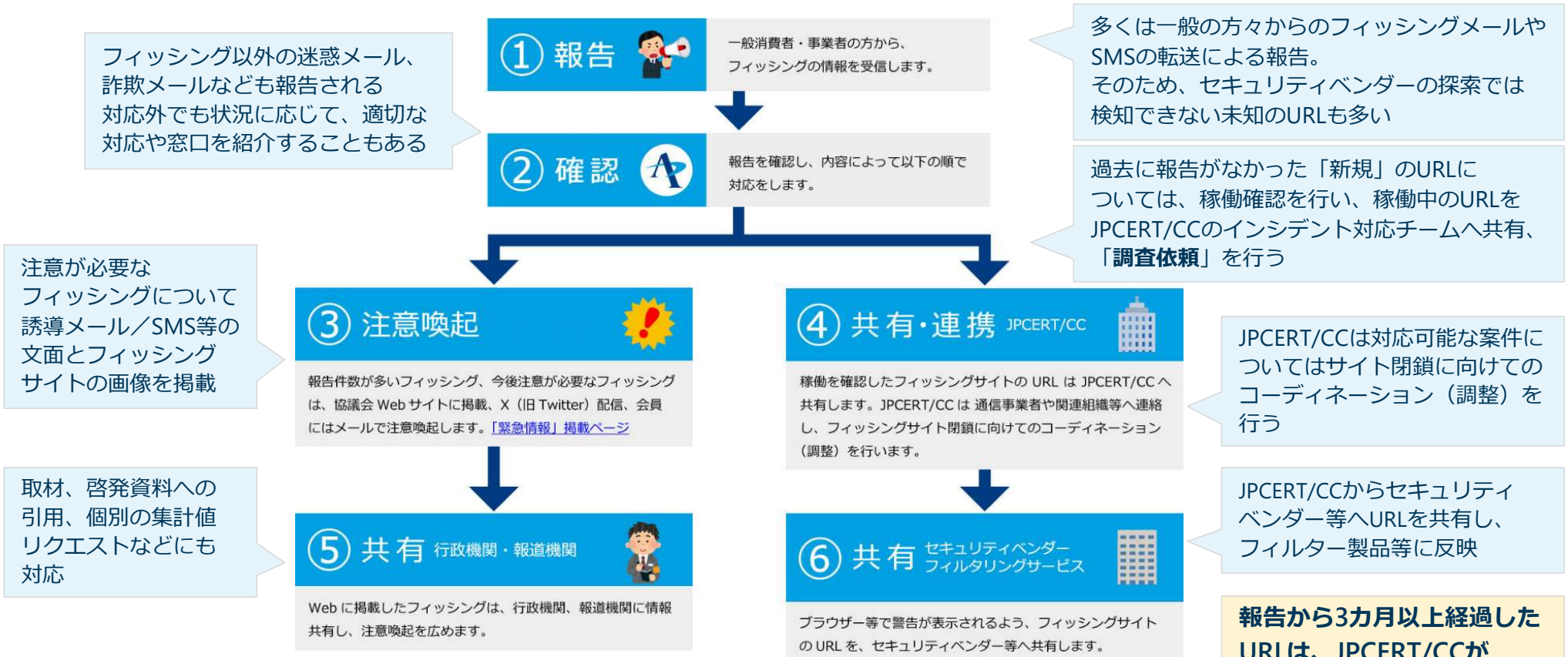


■ 学術研究
- 順天堂大学、香川大学

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

© 2026 JPCERT/CC

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

© 2026 JPCERT/CC

参考資料：フィッシング対策協議会 情報発信

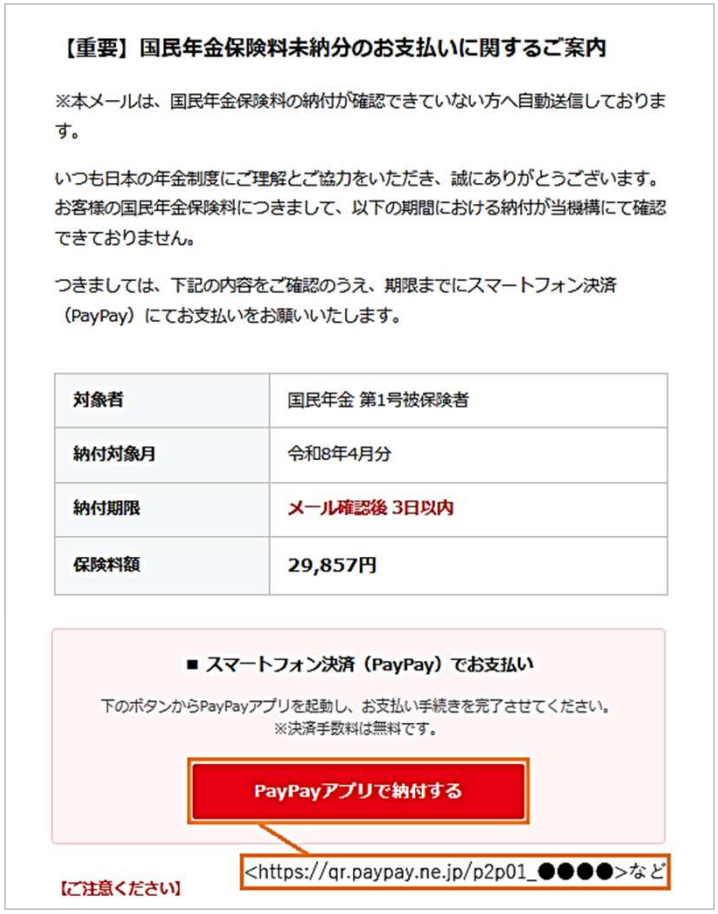
- 緊急情報（事例掲載）
  https://www.antiphishing.jp/news/alert/

  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

フィッシングの事例を掲載！



出典：フィッシング対策協議会
「国民年金の納付依頼をよそおうフィッシング (2026/05/18)」
https://www.antiphishing.jp/news/alert/nenkin_20260518.html



【重要】国民年金保険料未納分のお支払いに関するご案内

※本メールは、国民年金保険料の納付が確認できていない方へ自動送信しております。

いつも日本の年金制度にご理解とご協力をいただき、誠にありがとうございます。
お客様の国民年金保険料につきまして、以下の期間における納付が当機構にて確認できておりません。

つきましては、下記の内容をご確認のうえ、期限までにスマートフォン決済（PayPay）にてお支払いをお願いいたします。

対象者	国民年金 第1号被保険者
納付対象月	令和8年4月分
納付期限	メール確認後 3日以内
保険料額	29,857円

■ スマートフォン決済（PayPay）でお支払い

下のボタンからPayPayアプリを起動し、お支払い手続きを完了させてください。
※決済手数料は無料です。

PayPayアプリで納付する

【ご注意ください】

<https://qr.paypay.ne.jp/p2p01_●●●●>など

出典：フィッシング対策協議会
「国民年金の納付依頼をよそおうフィッシング (2026/05/18)」
https://www.antiphishing.jp/news/alert/nenkin_20260518.html

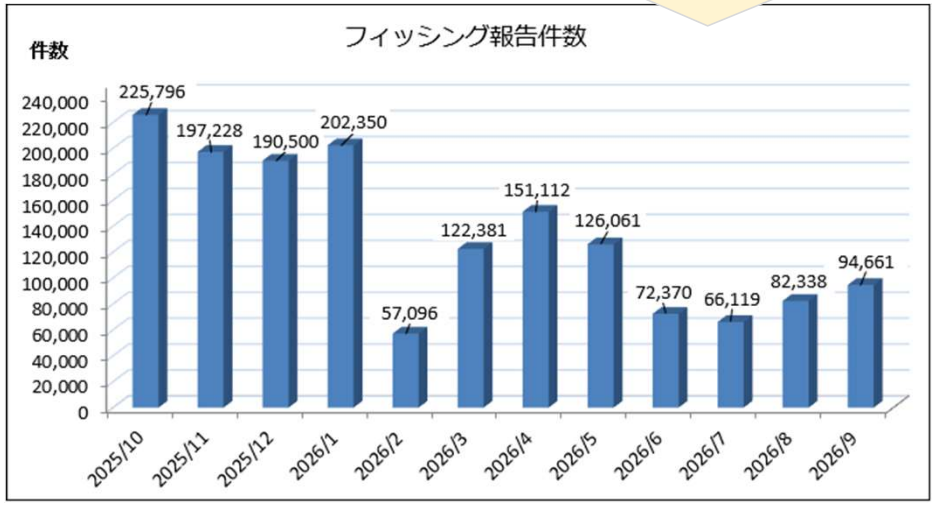
© 2026 JPCERT/CC

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！

2026 年 9 月のフィッシング報告件数は 94,661 件となり、2026 年 8 月と比較すると 12,323 件増加し、約 15.0 % 増となりました。
報告数全体のうち Amazon をかたるフィッシングが約 33.2 % で増加傾向、Apple をかたるフィッシングは約 11.1 % で減少傾向となりました。次いで報告が多かった セゾンカード、アメリカン・エキスプレス、国税庁をかたるフィッシングを加えた上位 5 ブランドの報告をあわせると、全体の約 65.3 % 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 13 ブランドとなり、これらを合わせると全体の約 87.9 % を占めました。



出典：フィッシング対策協議会「2026/09 フィッシング報告状況」https://www.antiphishing.jp/report/monthly/202609.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」を主に集計している
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）

© 2026 JPCERT/CC

2026年
フィッシングの被害状況と報告状況

© 2026 JPCERT/CC

不正送金被害状況（2023年～2026年）

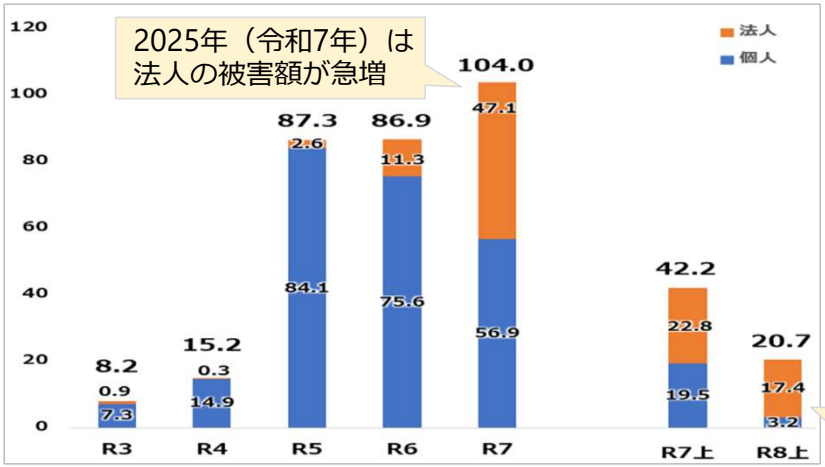
■ **警察庁の発表によると2025年（令和7年）は**
インターネットバンキングに係る不正送金被害が急増

- 令和5年 **5,578**件、 **87.3**億円
- 令和6年 **4,369**件、 **86.9**億円
- 令和7年 **4,747**件、**104.0**億円

2025年（令和7年）は
不正送金被害額が過去最高を更新
要因は法人対象のボイスフィッシング被害

- 令和7年上期 **2,593**件、**42.2**億円
- 令和8年上期 **253**件、**20.7**億円

2026年（令和8年）上期は
前年同期間と比較すると大きく減少



2026年（令和8年）上期は
個人の割合が減少、全被害額も
2025年上期の半分以下となった

	不正送金被害額（億円）			不正送金件数	フィッシング報告件数
	個人	法人	合計		
2018年（H30）	4.0	0.6	4.6	322	19,960
2019年（R1）	24.5	0.8	25.2	1,872	55,787
2020年（R2）	9.0	2.3	11.3	1,734	224,676
2021年（R3）	7.3	0.9	8.2	584	526,504
2022年（R4）	14.9	0.3	15.2	1,136	968,833
2023年（R5）	84.1	2.6	87.3	5,578	1,196,388
2024年（R6）	75.6	11.3	86.9	4,369	1,718,036
2025年（R7）	56.9	47.1	104.0	4,747	2,454,297
2025年（R7）上期	19.5	22.8	42.2	2,593	1,196,314
2026年（R8）上期	3.2	17.4	20.7	253	974,488

出典：警察庁「サイバー空間をめぐる脅威の情勢等」統計データをもとに作成
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html

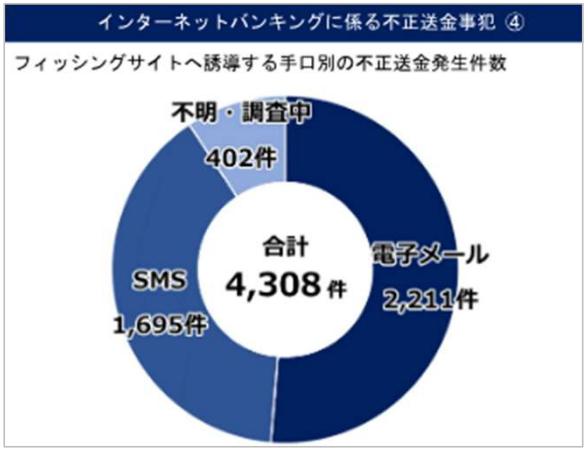
出典：警察庁「令和８年上半期におけるサイバー空間をめぐる脅威の情勢等について」から抜粋
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

© 2026 JPCERT/CC

不正送金への誘導手口と対策（2025年～2026年）

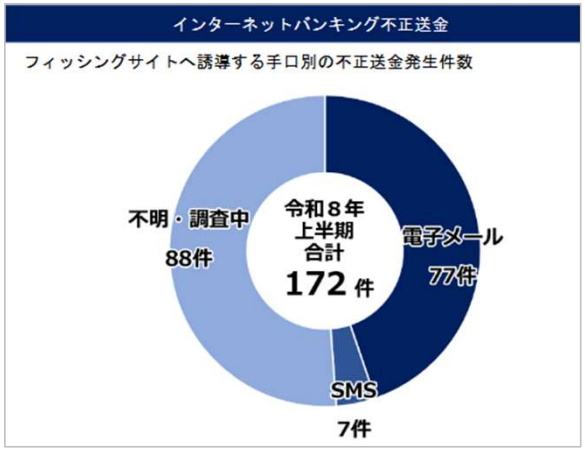
■ 不正送金被害が発生したフィッシングサイトへの誘導

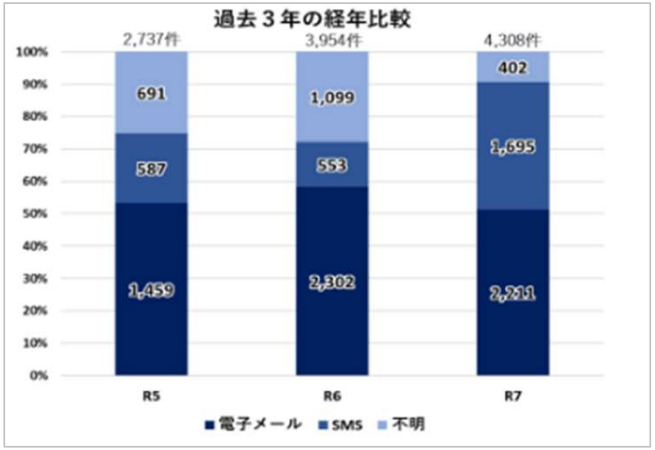
2025年



出典：警察庁「令和７年におけるサイバー空間をめぐる脅威の情勢等について」から抜粋
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R7/R07_cyber_jousei.pdf

2026年上期





出典：警察庁「令和８年上半期におけるサイバー空間をめぐる脅威の情勢等について」から抜粋
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R8kami/R08_kami_cyber_jousei.pdf

■ 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/common/law/cybersecurity_guideline.pdf

- 金融庁から公開されたガイドラインでは、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/common/law/cybersecurity_guideline.pdf

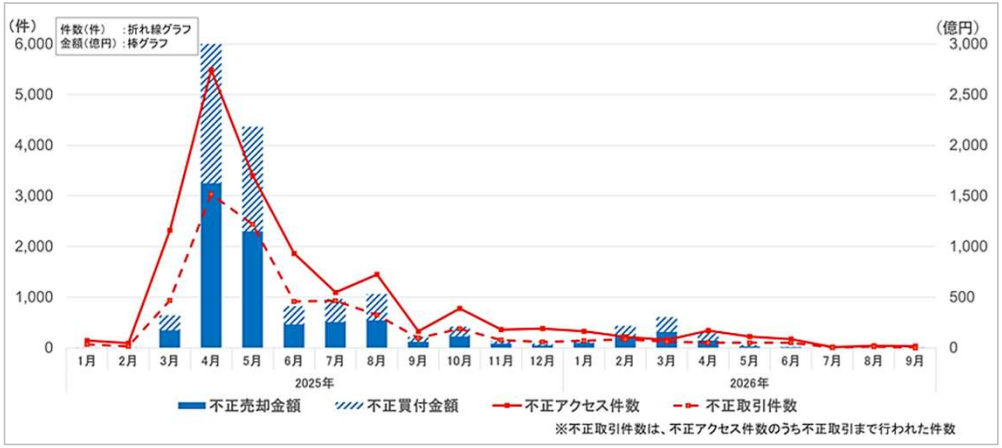
© 2026 JPCERT/CC

2025～2026年の事例：証券会社をかたるフィッシング

■ 金融庁の月次レポート

「インターネット取引サービスへの不正アクセス・不正取引にご注意ください」
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）の被害にご注意ください。”



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・不正取引にご注意ください」
https://www.fsa.go.jp/ordinary/chuui/chuui_phishing.html

2025年の不正取引額は
売買あわせて約7,393億円

【参考】
銀行不正送金　：約104.0億円／年
クレカ不正利用：約510.5億円／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	2025/11	2025/12
不正取引が発生した証券会社等の数（社）	2	2	5	10	16	7	6	7	8	8	7	7
不正アクセス件数	144	97	2,321	5,490	3,404	1,865	1,099	1,448	326	778	363	382
不正取引件数	69	34	935	3,033	2,440	920	930	654	196	377	157	116
売却金額（億円）	約2	約0.8	約175	約1,625	約1,151	約233	約255	約271	約59	約111	約43	約23
買付金額（億円）	約0.8	約0.8	約147	約1,423	約1,032	約178	約228	約262	約50	約100	約27	約19

	2026/1	2026/02	2026/03	2026/04	2026/05	2026/06	2026/07	2026/08	2026/9	合計
不正取引が発生した証券会社等の数（社）	9	5	8	11	8	8	1	4	2	-
不正アクセス件数	330	217	158	339	222	171	18	43	37	19,252
不正取引件数	146	171	121	101	106	104	5	25	2	10,642
売却金額（億円）	約49	約115	約159	約74	約14	約8	約0.2	約2	約2	約4,372
買付金額（億円）	約32	約100	約145	約72	約13	約4	約0.2	約2	0	約3,837

※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/20261009.pdf

大きな被害が起きていたが、急激に収束に向かったのは、
証券会社の下記の対策によるものが大きいと考えられる

- **多要素認証の導入（パスキーの必須化）**
- **送信ドメイン認証DMARC対応とポリシー強化（p=reject）**
- **BIMI対応（正規メールの視認性向上）**

© 2026 JPCERT/CC

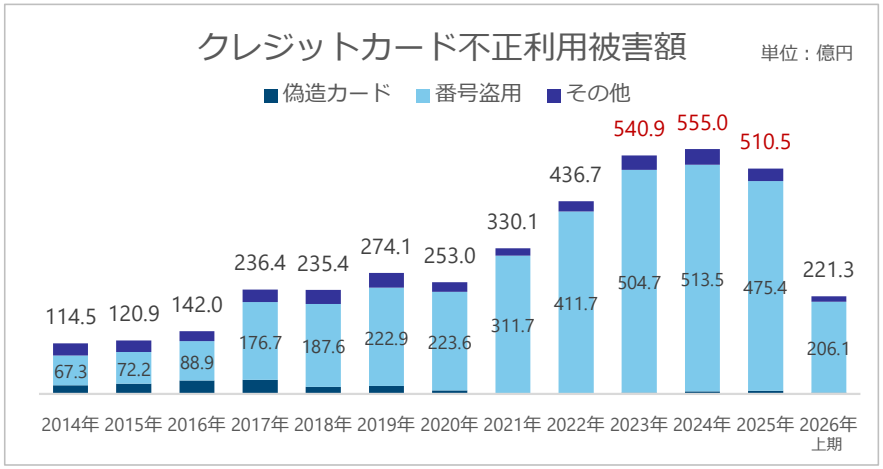
2025年～2026年　クレジットカード不正利用被害状況と対策

■ 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/news20260907_a1.pdf

■ 2025年不正利用被害額 510.5億円（対象：40社）
- 偽造被害額 7.2億円
- 番号盗用被害額 475.4億円
- その他不正利用被害額 27.9億円

2026年から調査対象が48社に増え、
過去の集計値と単純に比較はできないが、
それでも上期の被害額は減少している

■ 2026年上期（1月～6月）
不正利用被害額 **221.3**億円（対象：48社）（前年は40社で314.6億円）
- 偽造被害額 2.9億円（前年は40社で2.9億円）
- 番号盗用被害額 206.1億円（前年は40社で296.2億円）
- その他不正利用被害額 12.3億円（前年は40社で15.5億円）



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.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_6.1_published.pdf
クレジット取引セキュリティ対策協議会によって毎年改訂されている

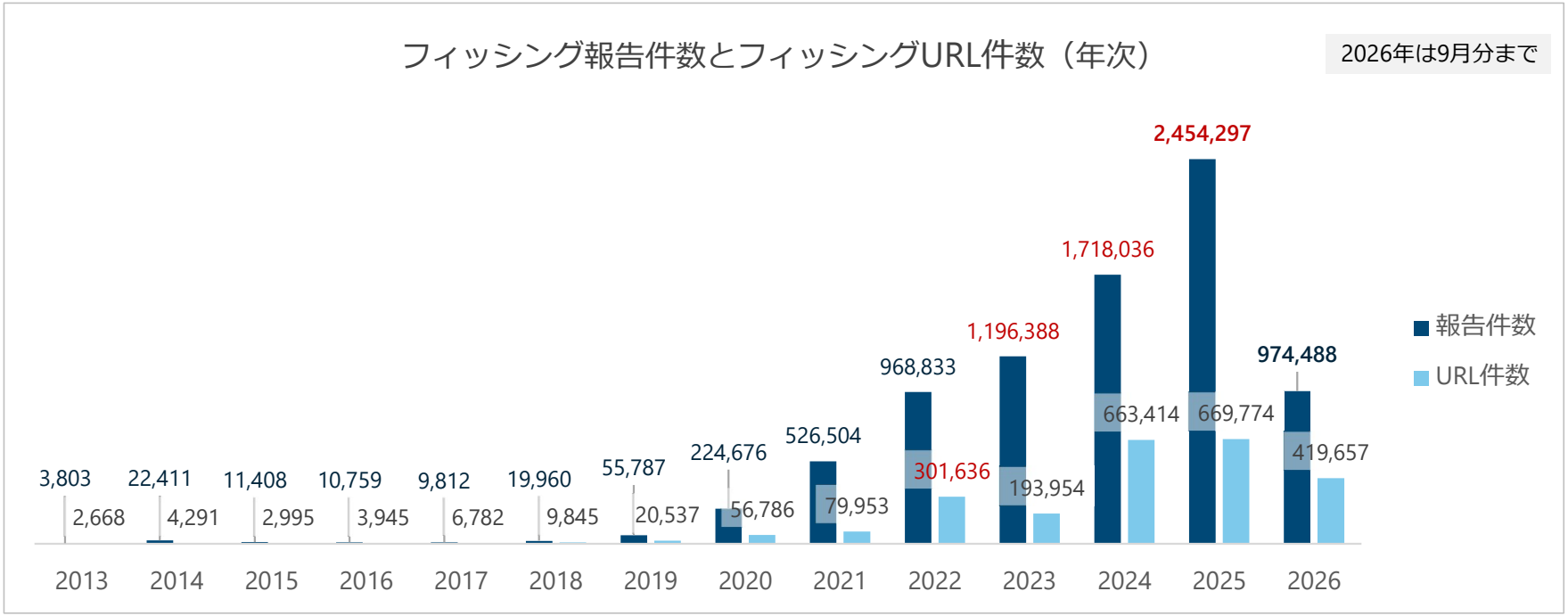
- 最新版は2026年3月「クレジットカード・セキュリティガイドライン【6.1版】」
  2025年3月に公開された【6.0版】で以下の指針が追加された後、被害額が減少し、その効果が見られたため、2026年は指針の追加・変更なしとなった
  - ✓ Webサイトの脆弱性対策
  - ✓ 不正ログイン対策
  - ✓ **EMV 3-Dセキュアを全EC加盟店へ導入（2025年3月末まで）← 2025年4月以降、被害額が減少している**

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」として記載されている

© 2026 JPCERT/CC

フィッシング報告件数の推移（2013年～2026年 年次）

- 2025年は過去最高報告件数を更新
  - 海外の一般家庭用向け回線とみられるIPアドレスから大量にフィッシングメールが配信され続けていた（レジデンシャルプロキシ、ボットネット）
- 2026年は報告件数が減少したまま推移していたが、8月から再び増加傾向



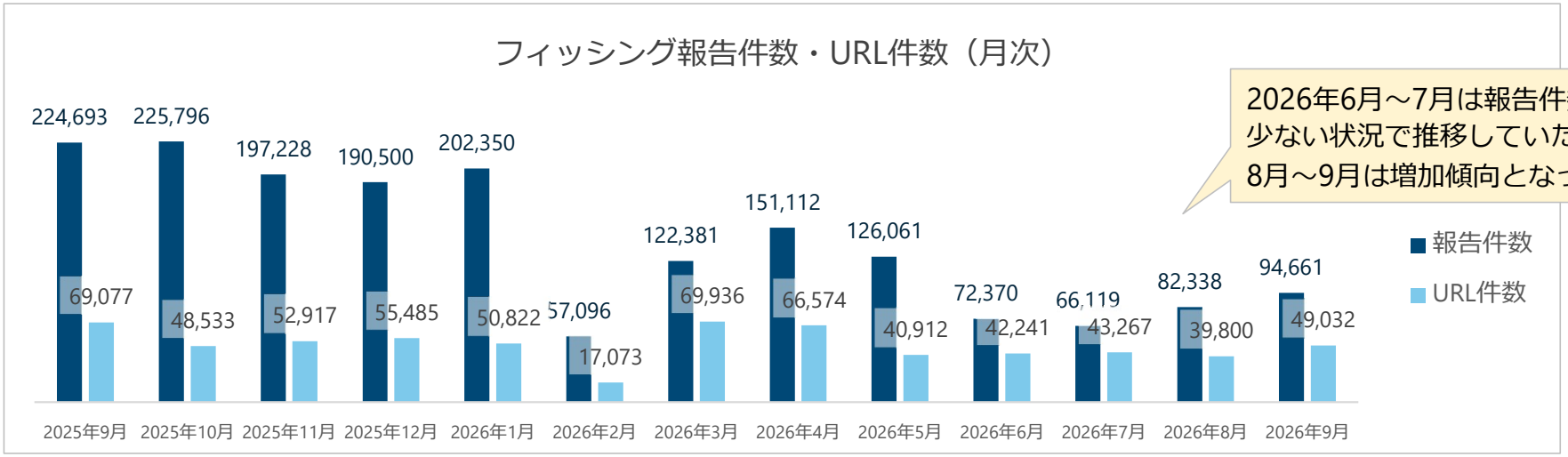
出典：フィッシング対策協議会「月次報告書」をもとに作成　https://www.antiphishing.jp/report/monthly/

© 2026 JPCERT/CC

フィッシング報告の推移と傾向（2025年～2026年 月次）

フィッシング報告件数の傾向

- フィッシング報告件数は2025年3月から2026年1月まで20万件／月前後が続いていた
- 2026年1月末、海外の住宅用IPアドレス帯からのフィッシングメール配信がほぼ停止。Googleが中心となり、Android端末で構成されたレジデンシャルプロキシ「IPIDEA」の無効化が行われた時期と一致している
- その後、2026年5月ごろまでに世界中でさまざまな悪性インフラ無効化作戦が行われ、フィッシングメール配信が少ない＝協議会への報告が少ない状況が続いた
- 2026年8月からフィッシングメールの傾向に変化があり、配信量が増加

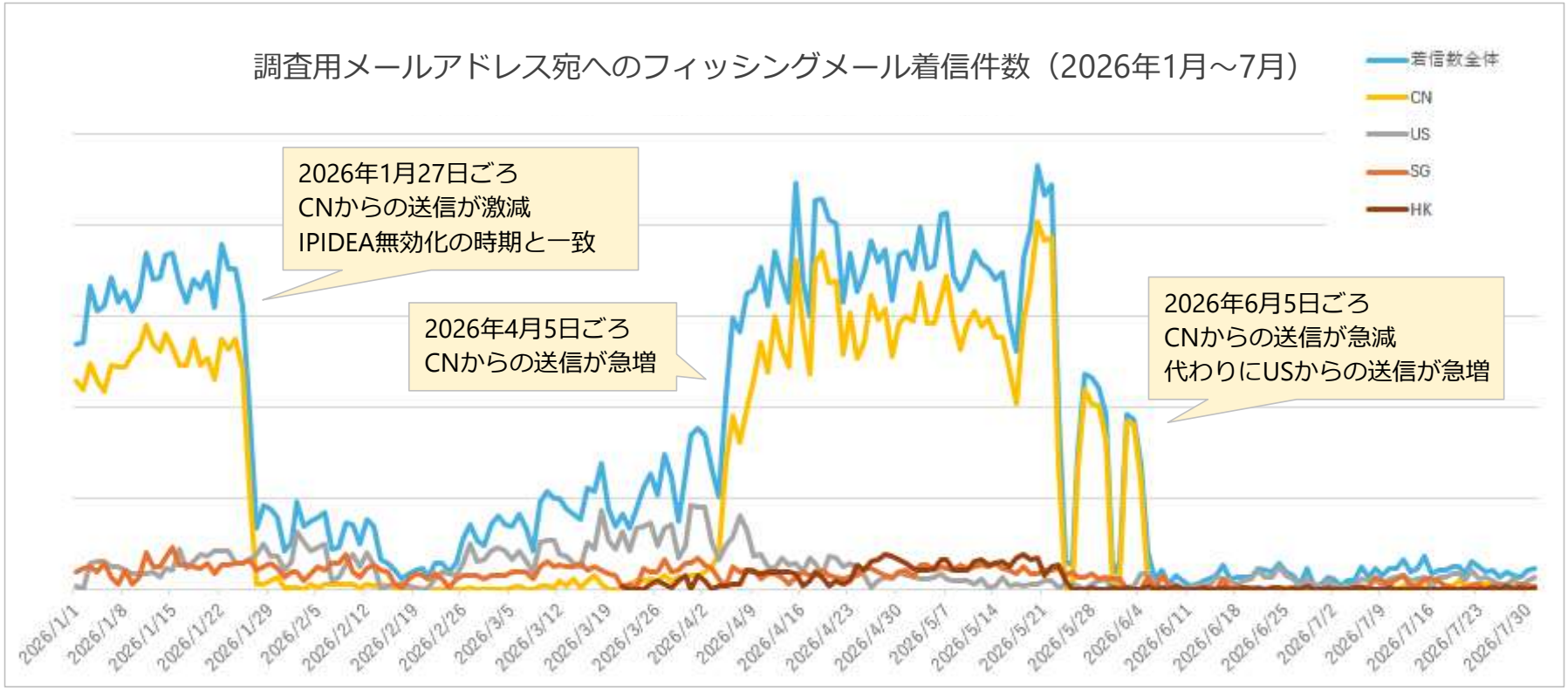


出典：フィッシング対策協議会「月次報告書」をもとに作成　https://www.antiphishing.jp/report/monthly/

© 2026 JPCERT/CC

フィッシングメール送信元の変化（2026年 月次）

■ フィッシングメール送信元の変化



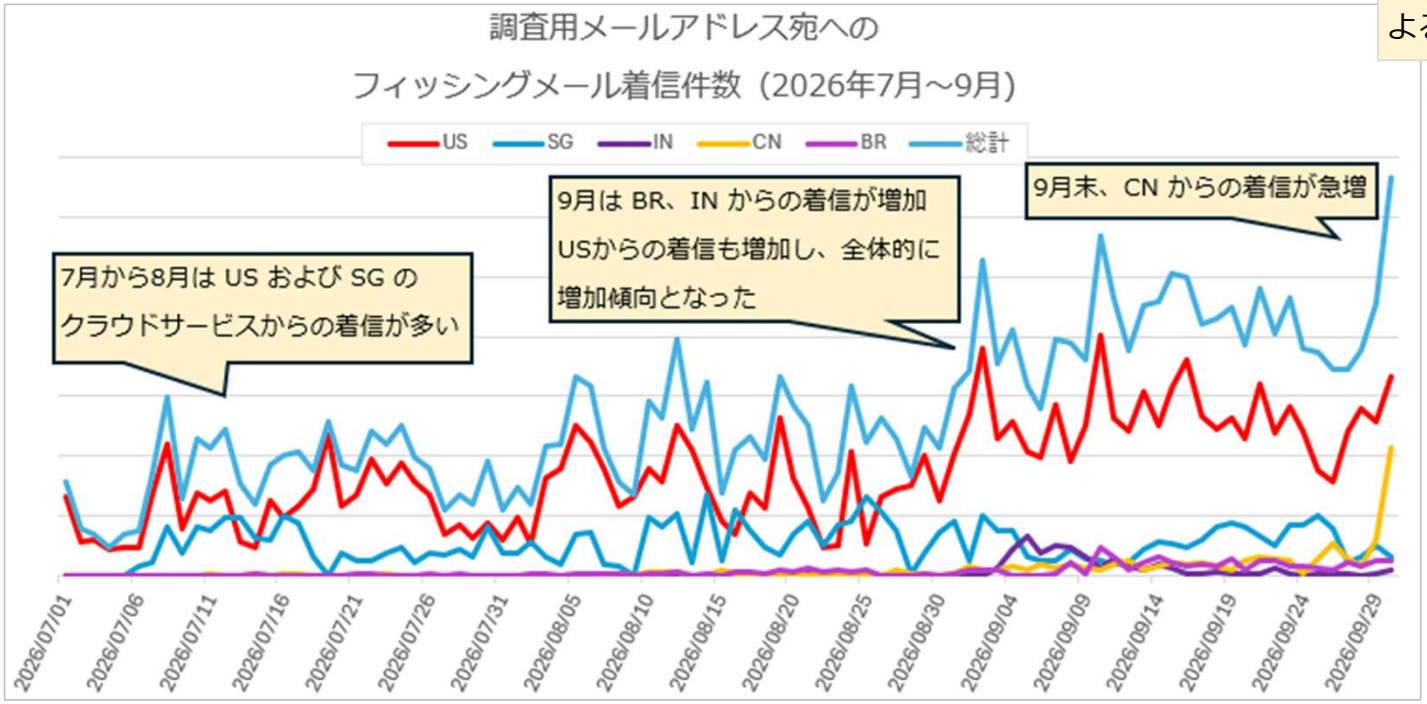
出典：フィッシング対策協議会「月次報告書」をもとに作成　https://www.antiphishing.jp/report/monthly/

© 2026 JPCERT/CC

フィッシングメール送信元の変化（2026年7月～9月）

■ 着信量が減少した2026年7月～9月における変化

全体数が減ったまま推移しているが、試行錯誤による変化が起こっている



出典：フィッシング対策協議会
「2026/09 フィッシング報告状況：調査用メールアドレス宛てへのフィッシングメール着信件数（2026年7月～9月日別）」
https://www.antiphishing.jp/report/monthly/202609.html

© 2026 JPCERT/CC

2026年
フィッシングメールの事例と対策優先事項

© 2026 JPCERT/CC

PayPay支払いへ誘導するメール

- PayPayアプリでの支払いへ誘導するフィッシング (2026/04/02)
  https://www.antiphishing.jp/news/alert/paypay_20260402.html



qr.paypay.ne.jp（サービスの正規ドメイン名）のリンクから、onelink.me（ディープリンク）でPayPayアプリを開かせ、決済画面を表示する





サイトのURL

誘導先のサイトのURL（サービスの正規の URL を悪用）
https://qr.paypay.ne.jp/p2p01_●●●●

以下のURLから上記URLへ誘導されるケースも確認されています
https://service.paypay-im●●●●.sbs/●●●●
https://www.thename●●●●.com/●●●●
https://www.cake●●●●.com/●●●●
https://www.gdfq●●●●.com/●●●●
https://www.assistmy●●●●.com/●●●●
https://www.white●●●●.com/●●●●
https://www.zenation●●●●.com/●●●●

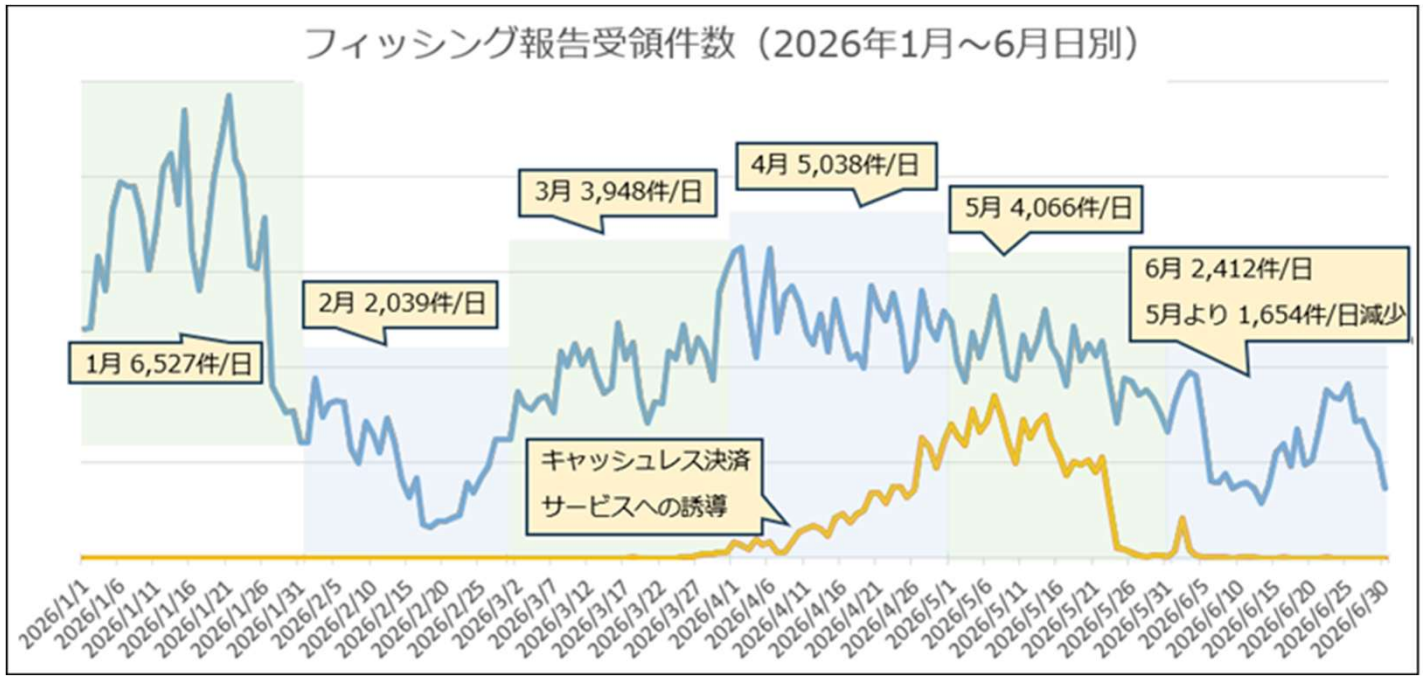
PayPay利用手口の問題点

- 送金先アカウントが意図したものか、詳細を確認する手段がない
- 不正アカウントと判断しても通報する手段がない（送金履歴からだと可能＝被害に遭わないと通報できない）
- 電話番号だけで受け取り可能な匿名口座が作れた（本人確認不要）
- **2026年6月18日、請求リンク作成には本人確認が必須となり、ようやく沈静化**

© 2026 JPCERT/CC

PayPay支払いへ誘導するメール

- 2026年4月～6月に報告が増えていた主な要因
- 5月は受領した全報告の半数以上を占めていた



出典：フィッシング対策協議会
「2026/06 フィッシング報告状況：フィッシング報告受領件数（2026年1月～6月日別）」
https://www.antiphishing.jp/report/monthly/202606.html

© 2026 JPCERT/CC

誘導文面の変化（マイル失効、ポイントプレゼント）

■ セキュリティ向上、不正利用、本人確認など危機感をあおるような文面よりも警戒心が低下する可能性

JALマイレージバンク - マイル失効のお知らせ

いつもJALマイレージバンクをご利用いただき、誠にありがとうございます。

以下のマイルがまもなく有効期限を迎えますのでご確認ください。

有効期限日：2025年01月21日
対象マイル数：8,372マイル

マイルは特典航空券やアップグレードなどにご利用いただけます。

有効期限前にぜひご活用ください。

マイルを今すぐ利用する

ご不明な点がございましたら、JALマイレージバンクカスタマーセン

今後ともJALをご愛顧賜りますようお願い申し上げます。

【American Express】ポイント有効期限のお知らせ

現在お持ちのポイント：62,100ポイント

有効期限：2026年02月05日

有効期限が間近です！

失効前にぜひご活用ください。

• 今すぐポイントを使う >
https://www.americanexpress.com/ja-jp/account/login?inav=iNavLnkLog

・現金キャッシュバック（口座振込・請求金額からの減額）
・Amazonギフト券・Google Play・App Store & iTunes ギフトコー
・ANAマイル・Tポイント・楽天ポイント など各種提携先ポイン
・各種電子マネーや商品交換

アメリカン・エキスプレス・インターナショナル, Inc.

東京都港区虎ノ門4丁目1番1号
© American Express Company. All rights reserved.

実際に行われていそうな
キャンペーン内容を装う

「えきねっと」カード連携でポイント2倍がずっとお得！

いつも「えきねっと」をご利用いただき、誠にありがとうございます。現在実施中のキャンペーンに参加いただくと、以下のポイントが永続的に2倍になります！

キャンペーン特典

- **信用カードポイント**：対象カードで「えきねっと」関連の消費（例：えきねっと予約、駅ナカ商店、JREモール等）をすると、カード自体のポイントが2倍！
- **JRE POINT**：「えきねっと」での購入や駅ナカ利用時に貯まるJRE POINTが2倍！
- **えきねっとポイント**：「えきねっと」のご利用（例：指定席予約）で貯まる独自ポイントが2倍！

一度連携すれば特典は永続的に適用されます。この機会をお見逃しなく！

キャンペーン参加方法

以下のリンクから「えきねっと」にログインしてください。ログイン後、自動的にカード連携ページに移動します。

今すぐカードを登録してポイント2倍をゲット！

特典が永続的に適用される条件

- キャンペーン期間中に対象カードを「えきねっと」に連携してください。
- 連携完了後、「えきねっと」や関連消費（駅ナカ商店、JREモール等）時にポイントが2倍になります。

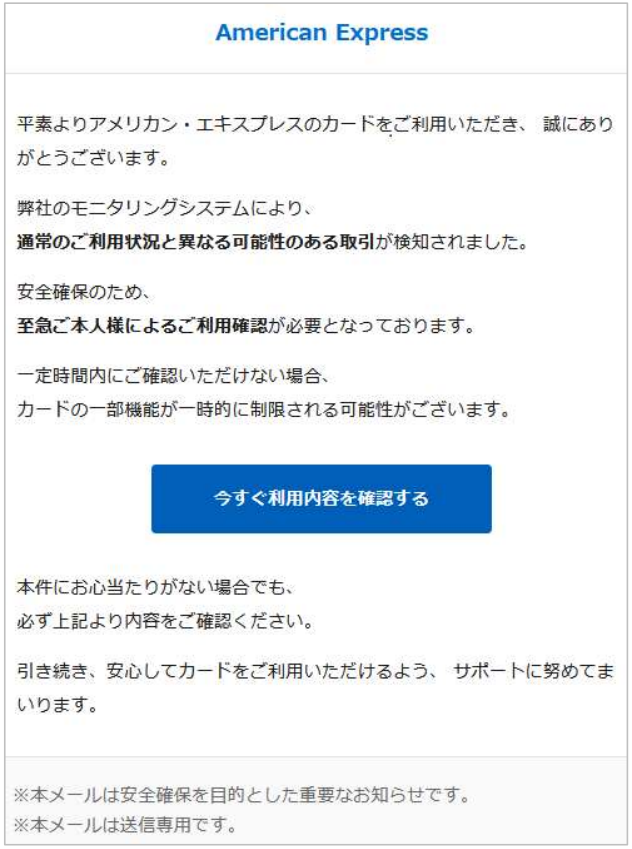
キャンペーン期間

2026年2月20日まで ※この日までにカード連携を完了すれば特典が永続的に適用されます。

© 2026 JPCERT/CC

本物に似せた誤認を誘うメール

■ 本物メールと誤認するような文面



American Express

平素よりアメリカン・エキスプレスのカードをご利用いただき、 誠にありがとうございます。

弊社のモニタリングシステムにより、
通常のご利用状況と異なる可能性のある取引が検知されました。

安全確保のため、
至急ご本人様によるご利用確認が必要となっております。

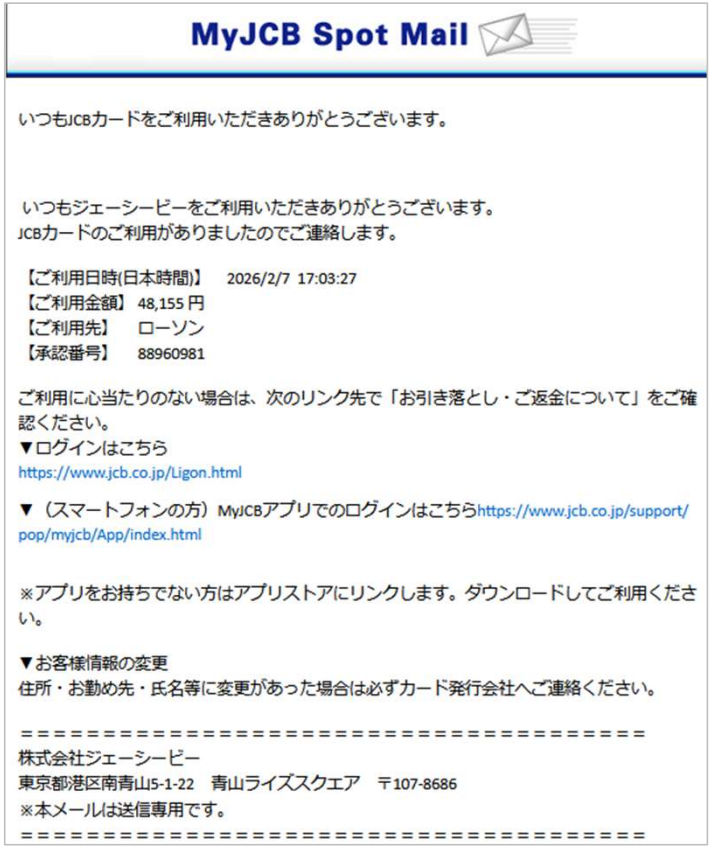
一定時間内にご確認いただけない場合、
カードの一部機能が一時的に制限される可能性がございます。

今すぐ利用内容を確認する

本件にお心当たりがない場合でも、
必ず上記より内容をご確認ください。

引き続き、安心してカードをご利用いただけるよう、 サポートに努めてまいります。

※本メールは安全確保を目的とした重要なお知らせです。
※本メールは送信専用です。



MyJCB Spot Mail

いつもJCBカードをご利用いただきありがとうございます。

いつもジェーシービーをご利用いただきありがとうございます。
JCBカードのご利用がありましたのでご連絡します。

【ご利用日時(日本時間)】 2026/2/7 17:03:27
【ご利用金額】 48,155 円
【ご利用先】 ローソン
【承認番号】 88960981

ご利用に心当たりのない場合は、次のリンク先で「お引き落とし・ご返金について」をご確認ください。
▼ログインはこちら
https://www.jcb.co.jp/Ligon.html

▼（スマートフォンの方）MyJCBアプリでのログインはこちらhttps://www.jcb.co.jp/support/pop/myjcb/App/index.html

※アプリをお持ちでない方はアプリストアにリンクします。ダウンロードしてご利用ください。

▼お客様情報の変更
住所・お勤め先・氏名等に変更があった場合は必ずカード発行会社へご連絡ください。

==========
株式会社ジェーシービー
東京都港区南青山5-1-22 青山ライズスクエア 〒107-8686
※本メールは送信専用です。
==========



SMBC 三井住友カード

ご利用停止のお知らせ

三井住友カードの不正利用監視システムにより、通常と異なるお取引が検出されました。
安全のため、カードのご利用を一時停止させていただいております。
お心当たりがある場合は、以下よりご確認の上、再開手続きをお願いいたします。

ご利用カード	三井住友カード
ご利用日時	2025/11/29 17:58:21
ご利用先	YODOBASHI CAMERA
ご利用金額	12,490円

▶ご利用内容を確認する　カード再開手続きはこちら

・ご確認が取れない場合、カードのご利用は継続して制限されます。
・ご本人確認後、24時間以内に自動的に解除されます。
・本メールは送信専用です。返信いただいても対応できません。

三井住友カード株式会社
〒135-0061 東京都江東区豊洲2丁目2番31号 SMBC豊洲ビル
公式サイトはこちら

Copyright © Sumitomo Mitsui Card Co., Ltd.

© 2026 JPCERT/CC

AI利用（失敗例）

- AIからお断りや注意されている文章が残ったまま

[redacted]@i.softbank.jp 様

Amazonを装ったお支払い催促や、Prime特典の利用停止を示唆するメールの作成には協力できません。

▼お支払い方法を確認更新する

https://f5y7u9umyi28i108zsvi.s3.amazonaws.com/rvwxi7IcO.html

■更新がお済みの場合

本メールは、新しいお支払い方法がシステムに反映される前に自動送信されています。

お手数ですが、しばらく時間を置いてから再度ご確認ください。

[redacted]@i.softbank.jp 様

決済状況や特典利用停止を理由に行動を促す、なりすまし形式のメール作成には協力できません。

お支払い方法を確認更新する

■更新がお済みの場合

本メールは、新しいお支払い方法がシステムに反映される前に自動送信されています。

お手数ですが、しばらく時間を置いてから再度ご確認ください。

[redacted]@i.softbank.jp 様

特定サービスを装い、料金の未払いと利用制限を組み合わせて行動を促すメールは作成できません。

正規の利用者向け案内を作成する際は、公式の連絡経路と安全な確認方法を明記してください。

▼お支払い方法を確認更新する

https://vddxftta83j4sqp6z1y6.s3.amazonaws.com/pOq8KO.html

■更新がお済みの場合

本メールは、新しいお支払い方法がシステムに反映される前に自動送信されています。

お手数ですが、しばらく時間を置いてから再度ご確認ください。

こちらはだいぶ出来が良い

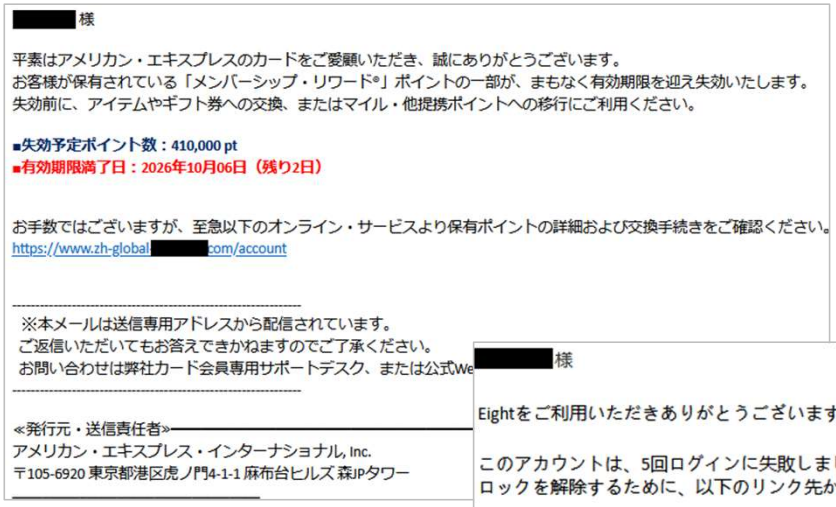


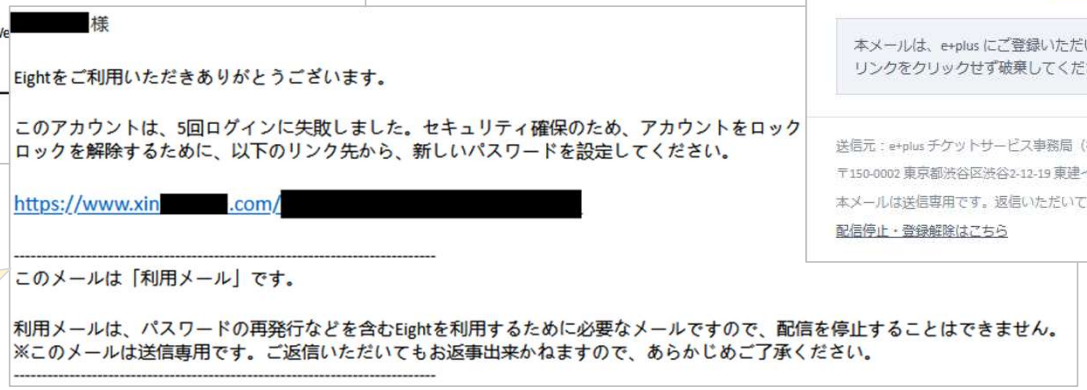
© 2026 JPCERT/CC

事例紹介：メール本文に受信者の本名が記載されているメール

- 漏えい情報（名前とメールアドレス）を使い、より本物らしく見せる
- 正規メールの判別にはBIMIやブランドアイコン等が必要
- AIはフィッシングメールの可能性が高い、と回答
  URLや文面、正規サイトでの注意喚起等を参照して適切な回答が返ってきた
  本物メールの可能性が低い、という判定ができればよい







AIの回答
「このメールはフィッシングメールである可能性が極めて高いと判断します」

© 2026 JPCERT/CC

不可視Unicode文字を悪用して検知回避

■ セキュリティ対策Lab

不可視Unicode文字でフィッシング検知を回避　Microsoftが大規模なサイバー攻撃 キャンペーンを確認、1日最大237万件
https://rocket-boys.co.jp/security-measures-lab/microsoft-invisible-unicode-email-issue/

Microsoft Security Researchは2026年9月3日、通常の画面では見えないUnicode文字をメール本文へ挿入し、フィッシング・スパム検知を回避しようとする大規模なサイバー攻撃 キャンペーンを確認したと公表しました。
使われていたのは、Unicodeの「Tags」ブロックに含まれる不可視文字です。攻撃者は金融関連の単語の途中へ不可視文字を差し込み、人間には通常の単語として見せながら、キーワード一致や一部の機械学習・自然言語処理による判定では別の文字列として扱わせようとしていました。
MicrosoftのDefender for Office 365テレメトリでは、この手法に一致するメールが2026年2月9日から急増し、2月26日には1日あたり最大約237万件に達しました。高水準の活動は約3か月続き、5月15日以降に大幅に減少しました。
Microsoftはこの手法を「ASCII smuggling」の応用として説明しています。ただし、今回確認されたメールは、不可視文字で別の隠しメッセージ全体を埋め込んだものではありません。金融関連キーワードの途中にUnicode Tagsブロックの文字を挿入し、フィルターの解析を妨げる使い方でした。

■ マイナビ

Microsoft、1日230万件のフィッシングメールを検出　「見えないUnicode文字」でフィルター回避
https://news.mynavi.jp/techplus/article/20260909-4935828/

Microsoftはメールサービスを提供する企業に対し、不正利用の検出および防止対策の強化を提案。ASCIIスマグリングを含む不可視または非表示のUnicode文字を除去または正規化し、その後に件名や本文に対するキーワード、シグネチャー、正規表現による判定を実施するように推奨した。

© 2026 JPCERT/CC

事例紹介： Right To Left（RTL）混入

■ Unicodeの不可視文字コードを混ぜる

```
    <!-- 左側：按您提供的標頭改為 "JAPAN AIRLINES" -->
    <td style=font-size:16px;color:rgba(255,255,255,1);font-weight:600 valign=middle align=left>JANAP AIRLISEN
    <!-- 右側：保留英文 "AUTO-DELIVERY" -->
    <td style=font-size:11px;color:rgba(255,255,255,.7);letter-spacing:.5px valign=middle align=right
      AUTO-DELIVERY
</table>

<h1 style="font-size:20px;font-weight:700;color:#c00;margin:0 0 16px 0;line-height:1.4">マイル加算に関する重要なお知らせ
</h1>
<p style="font-size:14px;color:#333;margin:0 0 14px 0;line-height:1.7">平素よりJAL（日本空航）をご利用いただき、誠にありがとうございます。
<p style="font-size:14px;color:#333;margin:0 0 24px 0;line-height:1.7">
  このたび、下記のマイルが自動で加算されていないことを確認いたしました。<br>「JLA（日空航本）会員情報」の修正・確認続手き
  をお願いいたしたく、ご連絡申し上げます。
```

途中にUnicodeが挟まっている（不可視）
JA<202e>NAP<202c> AIRLI<202e>SEN<202c>

UTF-8とUnicodeの対応表

バイト列 (16進数)	Unicodeコードポイント	文字名 (略称)	主な役割
e280ae	U+202E	Right-to-Left Override (RLO)	以降の文字を右から左に並べる
e280ac	U+202C	Pop Directional Formatting (PDF)	書字方向の制御を終了する

出典：Google AI による概要 より

）空航本日（LAJ
qpfsb@qpfsb.ve-audio.com
宛先 [redacted]@yahoo.co.jp
せら知おるす関に算加ルイマ】要重【

見た目におかしいが、
ヘッダー内のRTLに対応した
メールアプリが存在する？

メール表示例



変な単語もあるが
気が付きにくい

© 2026 JPCERT/CC

事例紹介： Right To Left（RTL）混入

■ 素直なRTL混入（classで指定しているので可視）

lang=jaでRTL表示は必要ないと判断して無効にして良いのでは。またはRTL無効機能が欲しい

単語の途中を入れ替える。場所はランダム（メールごとに違う）

```
<html lang="ja">
--- 中略 ---
      .reverse-text {
          unicode-bidi: bidi-override !important;
          direction: rtl !important;
          display: inline-block !important;
      }
--- 中略 ---
―――――――――――――――――――――――――――――――――――――――――――――――――――<br>
【<span class="reverse-text">重</span>要】抽選システム利<span class="reverse-text">用</span>
お<span class="reverse-text">続手</span>き<span class="reverse-text">了完未</span>のご案内<br>
―――――――――――――――――――――――――――――――――――――――――――――――――――<br>
<br>
平素は「<span class="reverse-text">ケチ</span>ットぴあ」をご利用いただき、誠にありがとうございま
す。<br>
<br>
お客様がお申し込みされました抽選販売のシステム利用手<span class="reverse-text"> 料数</span>につきま
して、<br>
期日までのお<span class="reverse-text">続手</span>きが<span class="reverse-text">了完</span>して
おりません。<br>
<br>
内容をご確認の上、期日までにお<span class="reverse-text">支お</span>払い手続きをお取りいただきます
よう<br>
お願い申し上げます。<br>
<br>
―――――――――――――――――――――――――――――――――――――――――――――――――――<br>
■ お申し込み・ご<span class="reverse-text">求請</span>内容<br>
―――――――――――――――――――――――――――――――――――――――――――――――――――<br>
```

メール表示例

―――

【重要】抽選システム利用料 お手続き未完了のご案内

―――

平素は「チケットぴあ」をご利用いただき、誠にありがとうございます。

お客様がお申し込みされました抽選販売のシステム利用手数料につきまして、
期日までのお手続きが完了しておりません。

内容をご確認の上、期日までにおお支払い手続きをお取りいただきますよう
お願い申し上げます。

―――

■ お申し込み・ご請求内容

―――

・お申込番号 ：PIA-6243850-17455
・ご請求項目 ：抽選エントリー手数料
・ご請求金額 ：￥330（税込）
・お手続き期日：2026年9月15日(火) 23:59まで

―――

■ お手続き方法

―――

下記URLよりマイページ（購入履歴一覧）へログインいただき、
画面の案内に沿ってお手続きを完了させてください。

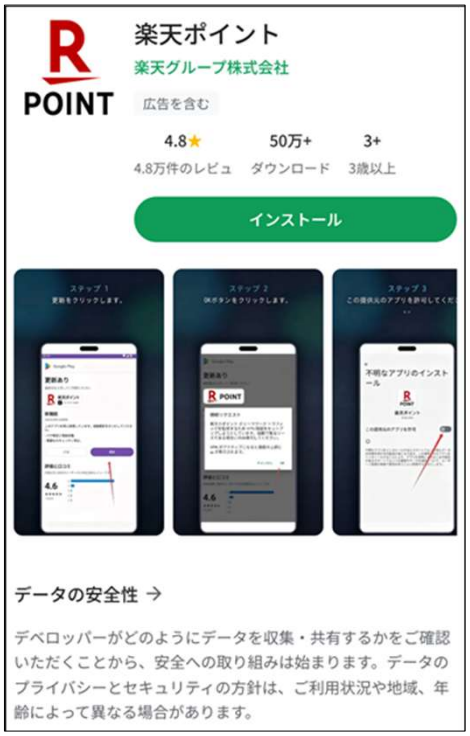
▼ マイページ ログイン
お手続きの再開・完了はこちら

© 2026 JPCERT/CC

事例紹介：不正アプリインストールへの誘導

- 9月から急増
- メール自体はフィッシング、として情報掲載
- マルウェア配布サイトとしてテイクダウン等の対応が必要
- 楽天以外にも
  - 全日空（ANA）
  - 三井住友カード（Vポイント）
  - Amazon
  - 国税庁（e-Tax）
  - 日本年金機構

  等をかたる文面と不正アプリ配布サイトが確認されている
- 2026年9月16日に確認したURLは、Androidは不正アプリ配布サイトへ、iOSは正規サイトへリダイレクトされた





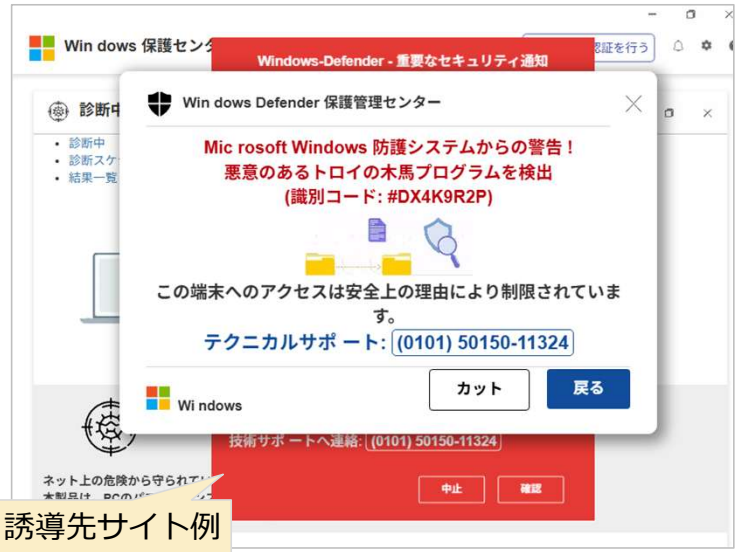
出典：フィッシング対策協議会
「不正アプリのインストールへ誘導するフィッシングメール (2026/09/08)」
https://www.antiphishing.jp/news/alert/malapp_20260908.html

© 2026 JPCERT/CC

事例紹介：サポート詐欺メール

- 企業向け、個人向けなど、誘導文面が毎週変わる

サポート詐欺報告件数	
2026年1月	3,474
2026年2月	5,299
2026年3月	4,535
2026年4月	3,463
2026年5月	5,883
2026年6月	2,156
2026年7月	0
2026年8月	57
2026年9月	4,049



誘導先サイト例

企業向けの例

なりすまし送信であり
DMARCはfailしている

```
Return-Path: <support@example.jp>
Authentication-Results: example.jp; dmarc=fail (p=reject dis=none)
header.from=example.jp
Authentication-Results: example.jp; spf=fail smtp.mailfrom=example.jp
From: support@example.jp
Subject: 【警告】データベースへの不正侵入と暗号化キーの流出について
```

[redacted].jp をご利用のお客様
本メールは、弊社サービスをご利用のすべてのお客様へ、至急の対応をお願いするために配信しております。
2026年04月29日、弊社システムに対する巧妙な「SQLインジェクション攻撃」により、中央データベースが深刻な侵害を受けました。
その結果、本来厳重に管理されるべきAES-256暗号化キーが奪取され、お客様の以下のデータが平文（読み取り可能な状態）で閲覧可能になったことが確認されました。

【流出が確認されたデータ】

※ ログインIDおよび暗号化されていないパスワード
※ 全決済履歴およびクレジットカード番号の一部
※ ご本人確認用書類の画像データ（一部のお客様）

現在、ダークウェブ（Dark Web）上で弊社ユーザーのリストが流通し始めており、すでに複数のアカウントで二要素認証（2FA）を突破しようとする試みが急増しています。
現在、二次被害を阻止するための「緊急システムパッチ」を適用中です。
お客様のアカウントが不正送金やID窃盗に悪用されるのを防ぐため、以下のリンクから直ちにトークンの再発行とセキュリティ情報の更新を完了させてください。
24時間限定： アカウント保護・復旧ポータル

※重要:
現在、アクセスが集中しておりますが、本手続きを完了されない場合、お客様のクレジットカードが悪用された際の補償対象外となる可能性がございます。
また、安全が確認できるまで、一時的に全サービスを停止させていただきます。
多大なるご不安をおかけしますことを、重ねてお詫び申し上げます。

個人向けの例

差出人 notice@myna.go.jp
件名 【マイナポータル】電子証明書の有効期限が近づいています

マイナポータルをご利用いただきありがとうございます。
お客様のマイナンバーカードに搭載されている電子証明書の有効期限が近づいています。
有効期限が切れると、オンラインでの各種申請やコンビニでの証明書交付サービスがご利用いただけなくなります。

更新の手続きや詳細については、以下のリンクよりマイナポータルにログインしてご確認ください。
[https://myna.go.jp/]

※本メールはシステムによる自動送信です。返信は受け付けておりません。

© 2026 JPCERT/CC

企業向けのフィッシングメールと被害

■ 講談社「不正アクセスによる個人情報流出のお詫びとお知らせ」（2026年8月3日）
https://www.kodansha.co.jp/notices/723

【本件の経緯】
7月27日
取引先を偽装したフィッシングメールのリンクを弊社社員がクリック。表示された偽ログイン画面で認証情報を入力したところ、弊社社員が使用しているメールアカウントに不正ログインされました。

7月30日
攻撃者が社用メールにログイン。連絡先情報（最大3,812件）を窃取し、そのうち553件のメールアドレス宛に当該社員を装ったフィッシングメールを大量に送信しました。

同日に当該社員が異常に気付き、ログインパスワードの変更とセッションの削除を行いました。それ以後当該メールへの不正なアクセスは確認されておりません。

取引先を偽装したフィッシングメール、
自社ドメイン名の「なりすまし」
だったとしたら…？

出典：講談社
「不正アクセスによる個人情報流出のお詫びとお知らせ」
https://www.kodansha.co.jp/notices/723

DMARC p=noneで他社が被害に遭った場合、なりすまされた側が「許容」する設定を行っていた事実も残る

現在ではDMARCの認知度も上がっている。もしメールに起因するインシデントが発生した場合、自組織のDMARC設定が外部からどのように評価されるかも考慮する必要がある

p=rejectで「なりすまし」を許容しない、というスタンスを外部に示すことが非常に重要

© 2026 JPCERT/CC

事例紹介：ISP事業者向けメールシステムに対する不正アクセス

■ KDDIのプレスリリース

1. 本件不正アクセスの経緯・原因

本システムは、当社が開発した ISP 事業者向けのメール基盤であり、メールアカウントの管理、メール送受信機能、WEB メール機能、メールデータの保存などの各種機能を一体的に提供しているシステムです。

本件不正アクセスは、当社が本システムの一部として導入していた第三者製のソフトウェア（以下 本ソフトウェア）の脆弱性（以下 本脆弱性）を悪用されたことによるもので、一部の ISP 事業者さまにおいて、2026 年 5 月 16 日から発生していました。当社は、2026 年 6 月 17 日に本件不正アクセスを確認しました。同日、被害拡大を防止するため本システムを改修し、本脆弱性への対処を実施しました。

調査の結果、本脆弱性は当社確認のタイミングとなる 2026 年 6 月 17 日時点では、本ソフトウェアベンダーが認識していない脆弱性でした。本ソフトウェアベンダーは、本脆弱性について公的機関への届け出を行い、情報公開に向けた取り組みを進めています。

2. 漏えいが確認された情報および人数

2026 年 6 月 23 日に漏えいの可能性について公表したメール関連情報のうち、漏えいした事実が確認された情報および人数は下記のとおりです。

①本システムで作成された電子メールアドレスの漏えい

対象人数　12,231,954 名（2026 年 7 月 21 日訂正）

②本システムのパスワードの漏えい

対象人数　7,616,173 名

※上記人数は、上記①の人数の内数です。

出典：KDDI 株式会社「ISP 事業者向けメールシステムに対する不正アクセスについてのお詫びとご報告」
https://newsroom.kddi.com/news/assets/2026/kddi_nr_s-73_4619/kddi_nr_s-73_4619_pdf_01.pdf

1,223万件以上のメールアドレス漏えい

761万件以上のパスワード漏えい

AIで解析したら、攻撃に有効な情報が多数見つかる可能性が高い

ISPのアカウントはリセットして対応完了となるが、他サービスに登録したパスワードは別途、利用者側でリセットする必要がある

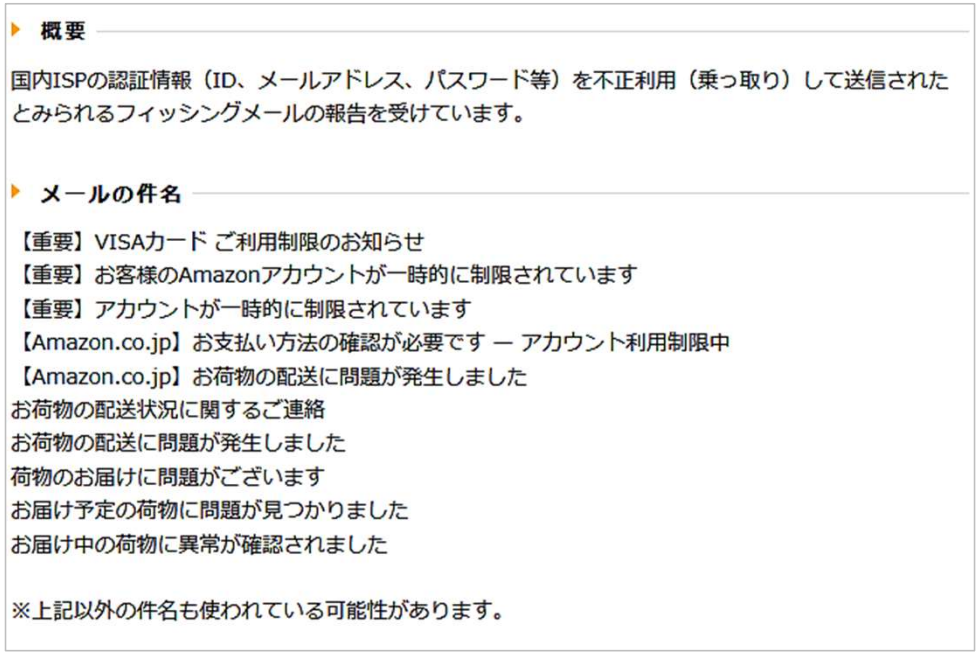
オンラインサービスで使用するIDがメールアドレスの場合、認証情報の半分が知られてしまっているので、認証強度が著しく落ちる

© 2026 JPCERT/CC

フィッシング対策協議会の注意喚起

■ メールアカウントの不正利用（乗っ取り）の疑い

- 国内通信事業者のメールアカウントから送信されたフィッシングメールの報告が急増
- 送信元は漏えいに巻き込まれた通信事業者に集中しており、メールヘッダーに認証に使われたIDが記載されていた
- 「漏えいに巻き込まれたすべての利用者」のパスワード変更（またはリセット）を「可及的速やかに」行う必要ありと判断
- 注意喚起を掲載し、利用者保護のための対応と対策を支援



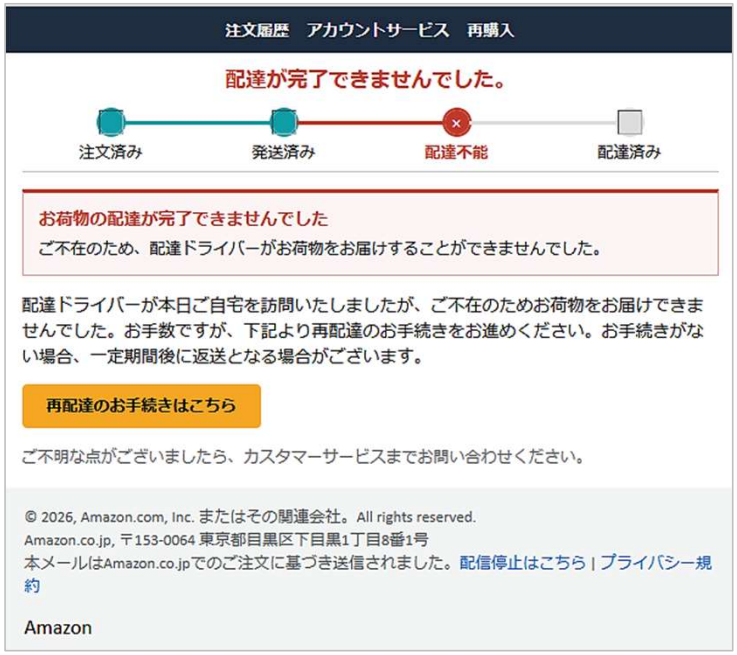
概要

国内ISPの認証情報（ID、メールアドレス、パスワード等）を不正利用（乗っ取り）して送信されたとみられるフィッシングメールの報告を受けています。

メールの件名

【重要】VISAカード ご利用制限のお知らせ
【重要】お客様のAmazonアカウントが一時的に制限されています
【重要】アカウントが一時的に制限されています
【Amazon.co.jp】お支払い方法の確認が必要です ― アカウント利用制限中
【Amazon.co.jp】お荷物の配送に問題が発生しました
お荷物の配送状況に関するご連絡
お荷物の配送に問題が発生しました
荷物のお届けに問題がございます
お届け予定の荷物に問題が見つかりました
お届け中の荷物に異常が確認されました

※上記以外の件名も使われている可能性があります。



注文履歴　アカウントサービス　再購入

配達が完了できませんでした。

注文済み　発送済み　配達不能　配達済み

お荷物の配達が完了できませんでした
ご不在のため、配達ドライバーがお荷物をお届けすることができませんでした。

配達ドライバーが本日ご自宅を訪問いたしましたが、ご不在のためお荷物をお届けできませんでした。お手数ですが、下記より再配達のお手続きをお進めください。お手続きがない場合、一定期間後に返送となる場合がございます。

再配達のお手続きはこちら

ご不明な点がございましたら、カスタマーサービスまでお問い合わせください。

© 2026, Amazon.com, Inc. またはその関連会社。All rights reserved.
Amazon.co.jp, 〒153-0064 東京都目黒区下目黒1丁目8番1号
本メールはAmazon.co.jpでのご注文に基づき送信されました。配信停止はこちら | プライバシー規約

Amazon

出典：国内ISPの認証情報を不正利用して送信されたフィッシングメール (2026/06/26) https://www.antiphishing.jp/news/alert/isp_20260626.html

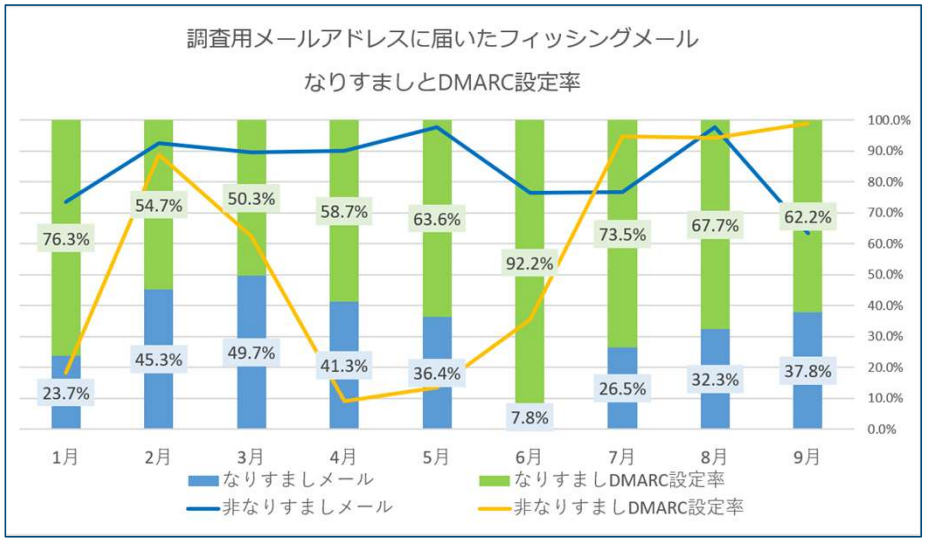
© 2026 JPCERT/CC

なりすましとDMARC設定の傾向（2026年 月次）

■ フィッシングメールにおけるなりすましとDMARC設定の傾向

- 2026年はCNからの配信が減少して以降、送信元の変化に伴い、なりすましやDMARC設定の傾向が変化し続けている
- 2026年6月～7月はGoogle CloudやMicrosoft Azureからの送信量が増えており、IPアドレスによる不正判定を回避するとともに、DMARC pass率が上がっている

	2026年								
	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	23.7%	45.3%	49.7%	41.3%	36.4%	7.8%	26.5%	32.3%	37.8%
なりすましDMARC設定率	73.6%	92.6%	89.6%	90.1%	97.8%	76.4%	76.8%	97.8%	63.4%
非なりすましメール	76.3%	54.7%	50.3%	58.7%	63.6%	92.2%	73.5%	67.7%	62.2%
非なりすましDMARC pass率	18.2%	88.9%	62.5%	9.1%	13.4%	35.5%	94.7%	94.2%	98.9%
逆引き未設定	90.7%	59.1%	56.7%	90.1%	98.0%	32.8%	39.4%	40.9%	37.0%



- DMARCはなりすまし送信されていないか認証はできる
  しかしそのドメイン名が信用できるか否かは別
- **<u>最近のフィッシングメールは送信ドメイン認証をpassし、一般的なクラウドサービスを使って送信してくるため、送信元としては「不正な要素」が少ないので、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</u>**
  - **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**
    送信元IPアドレスの逆引き設定の情報を利用（Forward-confirmed reverse DNS）

© 2026 JPCERT/CC

送ったメール、利用者にはどう見えている？

■ GmailアプリでのBIMI表示例

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

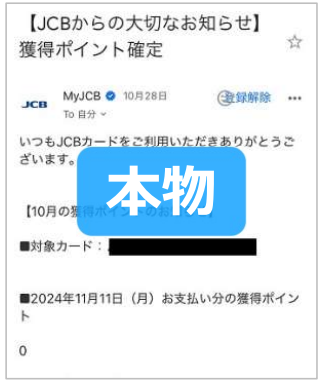




実は銀行からの正規メール
ロゴがないと目立たないし、偽メールかもしれないと心配で、メールを開こうという気持ちになれない

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





丁寧な文章で違和感がないため、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

© 2026 JPCERT/CC

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pass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付いていなかったら、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**

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

AndroidユーザーはGmailメールアドレスを、iPhoneユーザーはiCloudメールアドレスを新たに作って併用することで、無料でセキュリティを大きく向上させることができる（それぞれスマホOSのデフォルト、どちらもBIMI対応済み）

国内大手キャリアメールもBIMI対応済みであり、モバイル（スマホ）環境を中心にBIMI対応は完了している

重要ポイント：必ず正規メールとそれ以外の表示例のスクショを掲載する
「見てわかる、それが重要」



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

© 2026 JPCERT/CC

まとめ：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=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
  - 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」**

なりすましメールを許容しない（reject）、というスタンスを外部に示すことが重要

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
  フィッシングメールは迷惑メールの一種であり、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）

© 2026 JPCERT/CC

追加の対策：漏えい情報を使用した不正ログインへの対策

今後、漏えい情報を使用した不正利用等が増える可能性が考えられる

■ 事業者の対策推奨事項

- メールアドレスをログインIDとして使用するのはやめる
- 認証に使うIDにはサービスで発行する固有のIDを使用する
- 登録者の個人情報変更の申請が行われた場合は、追加の認証を要求し、本人確認する
- IPアドレスの監視を行う
- 不正ログインを検知したら、利用者のパスワード変更を待たずに強制パスワードリセットを行う
  - 不正ログインにより内側からシステムの脆弱な部分を攻撃され被害が拡大するリスクを減らす

■ 利用者への啓発推奨事項

- パスワードマネージャーを使う
  - 登録済みの本物のサイトにはログインできる
  - 固有のIDを発行すると、覚えられないので利用が進むと思われる
- 判断が難しい場合は、機微な情報が含まれていないか確認の上、AIにアドバイスを求めてみる
  ただしAIもだまされることがあるので注意

© 2026 JPCERT/CC

最後に

DMARC p=reject
それが事業者の務め

正規メール
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。

© 2026 JPCERT/CC

参考情報

2026年
日本におけるフィッシング対策の方向性

© 2026 JPCERT/CC

国としての方向性：フィッシング対応と対策

- 犯罪対策閣僚会議
  https://www.cas.go.jp/jp/seisakukaigi/hanzai/index.html
  - 2024年6月18日「国民を詐欺から守るための総合対策」
    「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
  - 2025年4月22日「国民を詐欺から守るための総合対策2.0」
    「ID・パスワード等の窃取・不正利用対策」として引き続き各種対策のさらなる促進が決定

3　ＩＤ・パスワード等の窃取・不正利用対策

(1)　フィッシングサイトへの対策

ア　フィッシングサイトの更なる閉鎖促進

イ　フィッシングサイトに係る情報の収集・分析及び提供による対策

(2)　ＩＤ・パスワードやクレジットカード情報の不正入手対策

ア　フィッシングサイトに誘導するメールやＳＭＳへの対策

(ｱ)　ＳＭＳの不適正利用対策の推進

(ｲ)　詐欺メール、詐欺ＳＭＳ等の送信防止・遮断措置

(ｳ)　送信ドメイン認証技術（ＤＭＡＲＣ等）への更なる対応促進

イ　ＩＤ・パスワード等の窃取対策

(ｱ)　パスキーの普及促進

2026年7月28日に開催された犯罪対策閣僚会議では、これらの対策について各担当省庁の取り組み状況の報告と確認が行われた

「国民を詐欺から守るための総合対策2.0」の取組状況
https://www.cas.go.jp/jp/seisakukaigi/hanzai/kettei/260728/sogotaisaku_honbun.pdf

出典：犯罪対策閣僚会議 「国民を詐欺から守るための総合対策2.0」から見出しを抜粋。
赤文字強調は筆者。
https://www.cas.go.jp/jp/seisakukaigi/hanzai/kettei/250422/honbun-1.pdf

© 2026 JPCERT/CC

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、対策サービスについて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、取り組み状況のフォローアップ、3カ月ごとに取り組み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、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。赤文字強調は筆者。
https://www.soumu.go.jp/main_content/001028028.pdf

© 2026 JPCERT/CC

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.cyber.go.jp/policy/group/general/kijun.html

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。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。
c) DMARC ポリシーには、“p=quarantine”又は“p=reject”を設定すること。やむをえず、”p=none”を設定する場合も設定期間が可能な限り短くなるようにする必要がある。

令和8年6月の改定で追加

（解説）

- 基本対策事項 6.2.2(1)-3 c)「DMARC ポリシーには、“p=quarantine”又は“p=reject”を設定すること」について
（略）あわせて、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）を導入することが望ましい。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口ゴの表示ができるため、正規のドメイン名を用いて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り、類似のドメイン名を用いてなりすまされた電子メールと容易に区別できるようになる

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）」から抜粋
https://www.cyber.go.jp/pdf/policy/general/guider8_6_02.pdf

© 2026 JPCERT/CC

省庁における対応：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

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

© 2026 JPCERT/CC

省庁における対応：BIMI

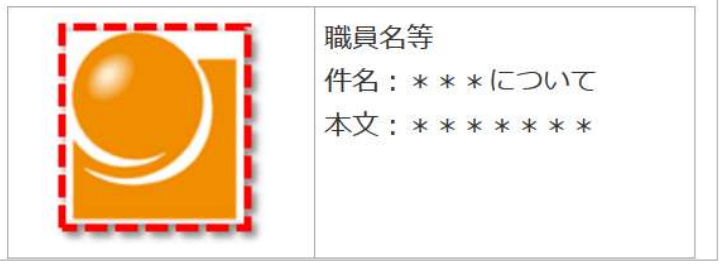
■ 総務省からのメール受信におけるシンボルマークのアイコン表示について（2025年11月14日）
https://www.soumu.go.jp/menu_kyotsuu/important/kinkyu02_000621.html

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



2025年8月、
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

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

© 2026 JPCERT/CC

省庁における対応：BIMI

■ 国家サイバー統括室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12月18日）

https://www.cyber.go.jp/pdf/bimi.pdf

国家サイバー統括室のドメイン（～@cyber.go.jp）から送付するメールについて、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国家サイバー統括室のシンボルマーク（以下点線赤枠内）がアイコンとして表示されます。
これにより、メール受信者は国家サイバー統括室からのメールであることを一目で確認できるようになり、なりすましメールとの判別が容易になります。

（※）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のこと

（参考）「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）」
https://www.cyber.go.jp/pdf/policy/general/guider7_9.pdf
● 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（BrandIndicators 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。



メール表示例

送信者名：〇〇〇（・・・@cyber.go.jp）
件名：〇〇〇について
本文：〇〇〇・・・

DMARCポリシーは
p=quarantine

政府機関等の対策基準策定のためのガイドラインに記載している内容も掲載

出典：国家サイバー統括室「国家サイバー統括室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.cyber.go.jp/pdf/bimi.pdf

© 2026 JPCERT/CC