2025年7月30日
JANOG56 in 松江
配布用資料

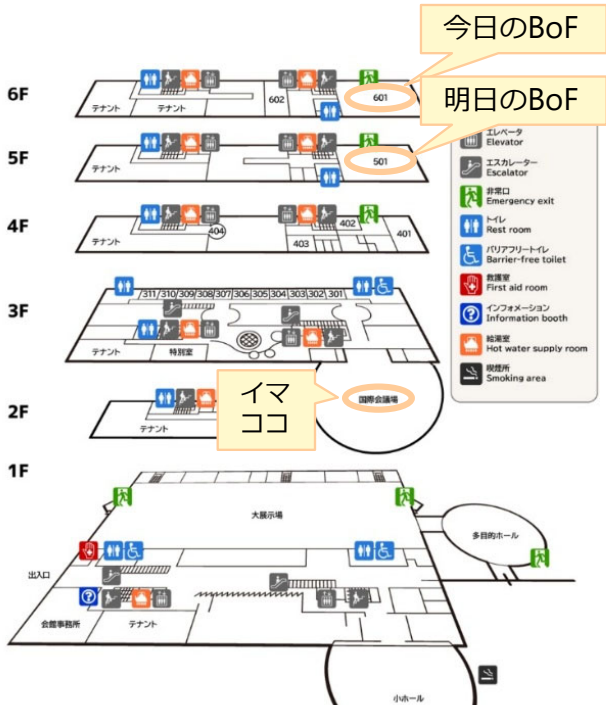
2025年フィッシングの動向と対策 ＆最新メールセキュリティ

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

本プログラムの内容

- 平塚 伸世（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）
  - 2025年フィッシングの状況
  - 事例紹介、有効と思われる対策
- 加瀬 正樹さん（株式会社TwoFive／JPAAWG）
  - メール送信者ガイドラインと逆引きDNS設定
  - 逆引きDNS（rDNS）がないサーバーに対する対策
- 櫻庭 秀次さん（一般社団法人メッセージング研究所／JPAAWG）
  - 国内の送信ドメイン認証普及状況
  - 最新のメールセキュリティーの動向について（DMARCの改訂、DKIM2.0）
- 末政 延浩さん（株式会社TwoFive／JPAAWG）
  - 海外の動向（M3AAWGでのGmailガイドラインに関する議論など）
- 本プログラムに関連するBoF
  - フィッシング＋メールセキュリティ対策BoF
    Day1：7月30日 17:00～18:00、601大会議室（126席）（このあとすぐ！）
  - JPAAWG BoF
    Day2：7月31日 14:30～15:30、501大会議室（126席）

- ぜひアンケートにもご協力ください！（事後でも可）
  フィッシング＋メールセキュリティ対策アンケート
  https://forms.gle/g4E8rYTqhuy1MJCQ7



出典：くにびきメッセ「施設案内」を基に加筆
https://www.kunibikimesse.jp/organizer/facility/

フィッシング対策協議会とJPCERT/CCの活動

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からURLフィルタリングを行っている セキュリティベンダー、事業者へURL共有

2025年
フィッシングの被害状況と報告状況

不正送金被害状況と対策（2023年～2024年）

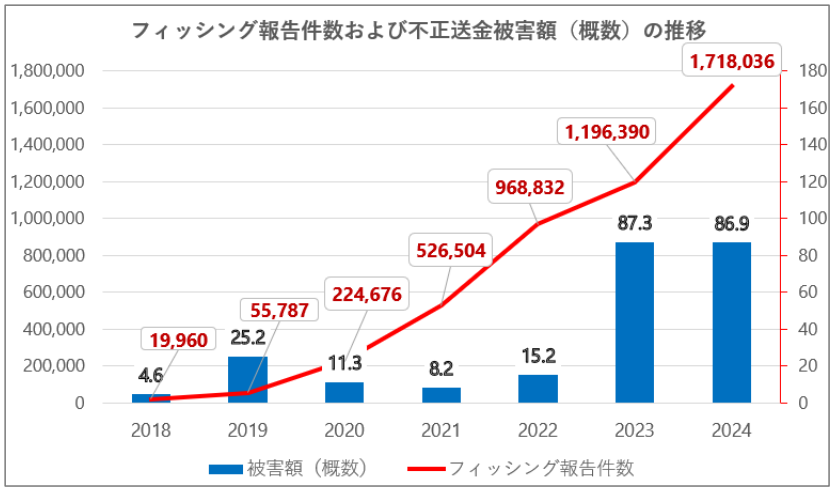
■ 2023年（令和5年）は不正送金が急増

- 令和5年、不正送金被害件数 5,578件、被害額 87.3億円と過去最多となった

■ 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**

年	総件数	被害額（概数）	被害額（億円）	フィッシング報告件数
2018	322	約4億6,100万円	4.6	19,960
2019	1,872	約25億2,100万円	25.2	55,787
2020	1,734	約11億3,300万円	11.3	224,676
2021	584	約8億2,000万円	8.2	526,504
2022	1,136	約15億1,900万円	15.2	968,832
2023	5,578	約87億3,100万円	87.3	1,196,390
2024	4,369	約86億8,900万円	86.9	1,718,036



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

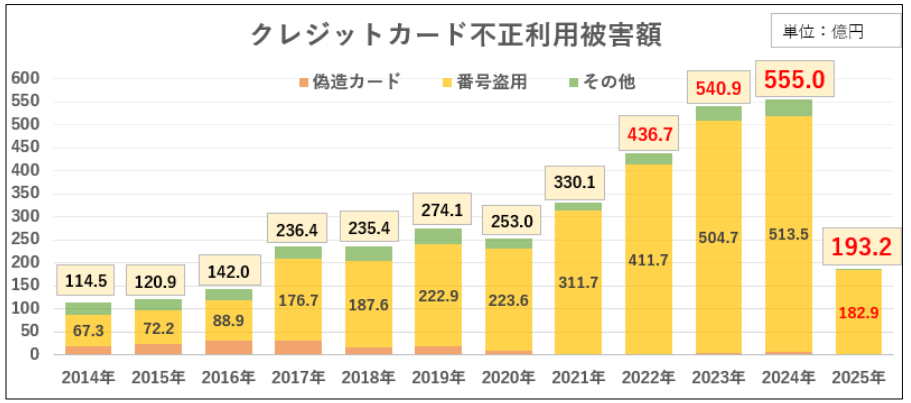
2024年～2025年　クレジットカード不正利用被害状況と対策

■ 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年第1四半期（1月～3月）
不正利用被害額 **193.2**億円（前年比 **19.0%増**）
- 偽造被害額 1.8億円（前年同期比 18.2%減）
- 番号盗用被害額 182.9億円（前年同期比 **21.4%増**）
- その他不正利用被害額 8.5億円（前年同期比 9.6%減）

2025年第1四半期は前年よりも不正利用被害額、特に番号盗用被害が増えている



出典：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セキュアを全EC加盟店へ導入（2025年3月末まで）

  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

「2025年3月末まで」という期限があるため、カード会社やECサイトからEMV 3-Dセキュアへの対応依頼が利用者へ送られていたが、当然のようにその依頼を模したフィッシングメールがばらまかれていた。
正規メールであると認証されたメール以外は信用しない、という認識を持つ必要がある。
（なお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）

国としての方向性：フィッシング対応と対策

■ 令和6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：送信ドメイン認証DMARC

■ 内閣サイバーセキュリティセンター「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。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。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。

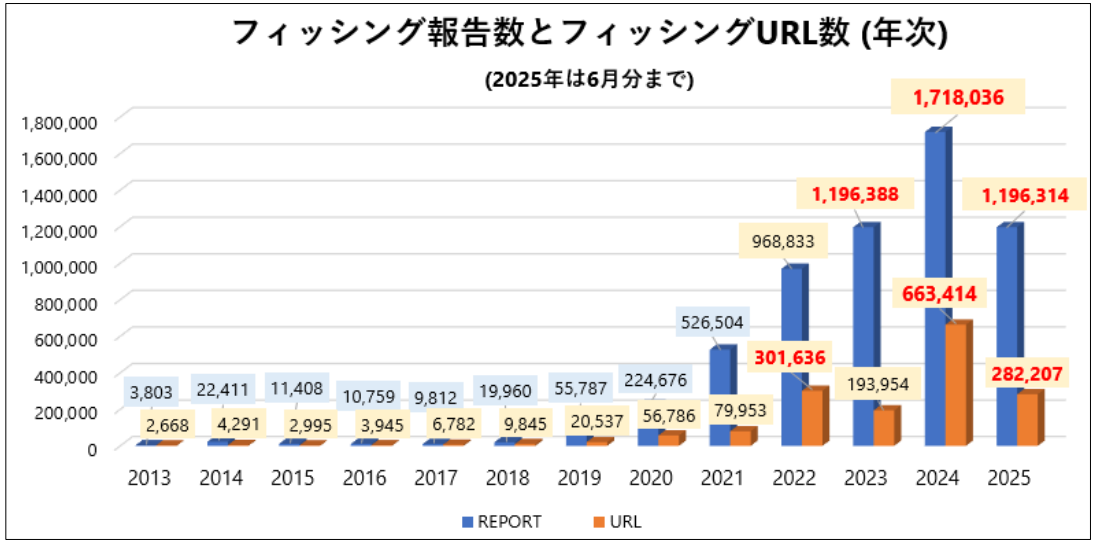
（解説）
- 基本対策事項 6.2.2(1)-3 a)「DMARC」について
（略）また、DMARC によって認証された電子メールの視認性を向上させる BIMI（Brand Indicators for Message Identification）の導入を検討するとよい。送信側が BIMI を設定すると、受信側の BIMI に対応する電子メールクライアントに送信側の口ゴの表示ができるため、機関等が送信した電子メールであることが視覚的に分かりやすくなる。

出典：内閣サイバーセキュリティセンター「政府機関等の対策基準策定のためのガイドライン（令和５年度版）の一部改定（令和６年７月）」から抜粋
https://www.nisc.go.jp/pdf/policy/general/guider6.pdf

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＝フィッシングが増加
  - 対面（店舗）からオンラインへ、生活に必要なサービスが変わり、フィッシングが行いやすい環境となった
  - スマートフォンの普及によりオンラインサービスを24時間いつでも使えるようになった
  - 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年以前から存在したが、日本では送信側・受信側ともに未対応が多かった
  - 国内メールサービスの多くがフィッシングメールを素通しし、受信者が判別できない状況のため、被害が発生、狙われ続けている



2024年は、報告数、URL数ともに過去最高となった

2025年は、6月末時点ですでに2024年の報告数の半数を超えており、このままでは過去最高値を更新する

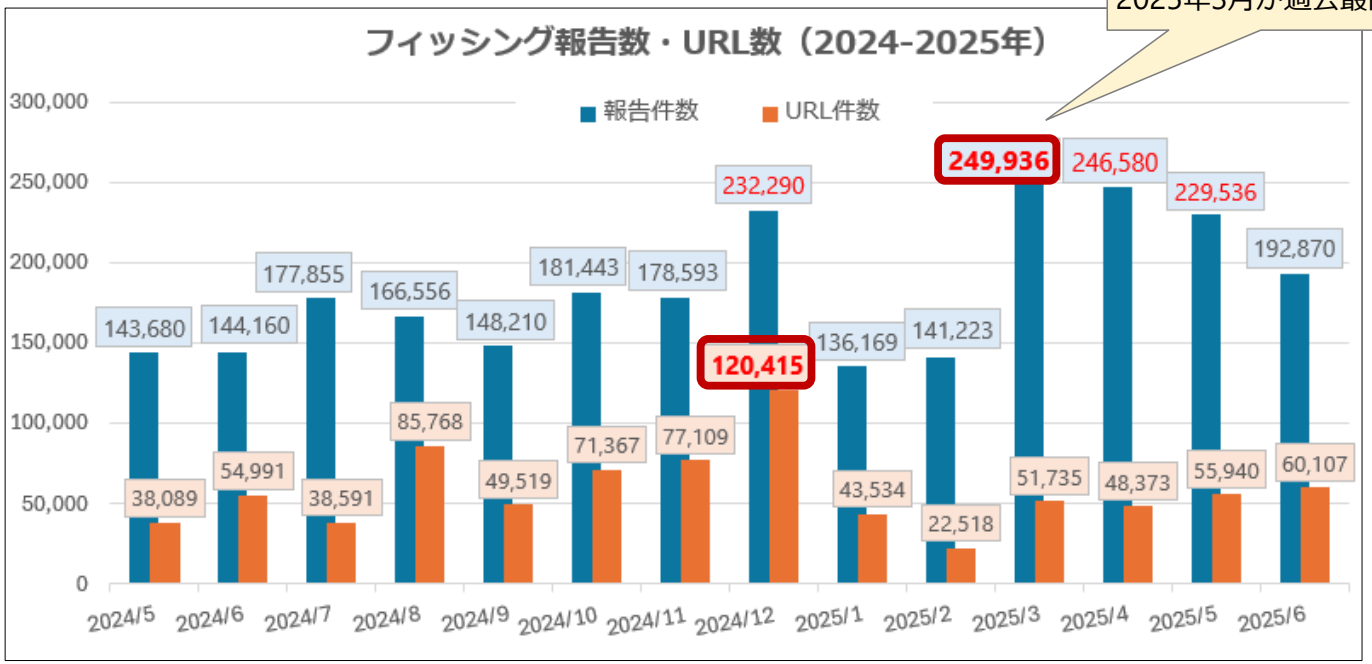
フィッシングメール配信量が増えるに従い、フィッシング報告も増加

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

- 2024年12月以降、フィッシングメール配信数が急増しており、2025年3月は報告数が過去最高となった
- 2025年4月からは迷惑メール判定済み（件名に[meiwaku]や[SPAM]などがついている）を除外しており、それらを含める（2025年3月以前と同じ集計方法）と35万件以上となった



報告数は公開情報としては2025年3月が過去最高

急増

2025年4月から迷惑メール判定済みは報告数から除外。
その除外分を含めると**35万件以上**

2025年5月は、
迷惑メール判定済み等も含めると
約32万件

2025年6月は、
迷惑メール判定済み等も含めると
約26万件
各方面の対策が効いてきたか、減少傾向となったが、それでも実質的には2025年3月の約25万件よりも多い

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・手法

2025年上期の事例：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

- メール内のURL表記

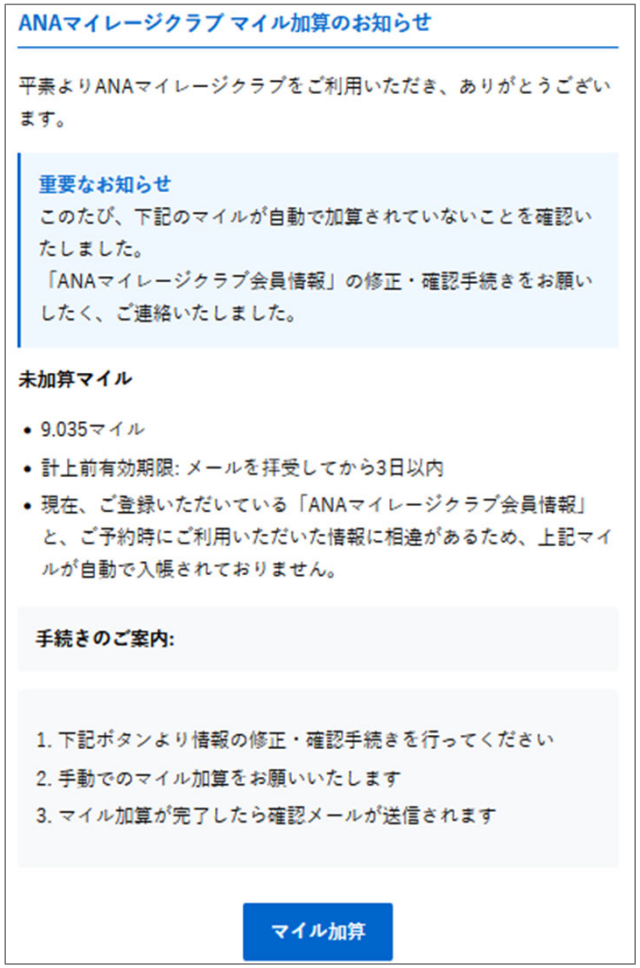
```
マイル加算
 <https://zhjinghua.com%E2%88%95bknTOWs%E2%88%95onAwEItKWU%E2%88%
95hLFzbZQBV@rgam.sinoroad.me/wgpp.co.jp>
```

- 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）とtranslate.goog
- 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）
- 3月からUnicode文字列も混ぜ始める
- さまざまなブランドをかたるフィッシングでこの手法が採られる

2025/5/19	19:37:22	SBI証券	https://p2h6zjz3uyvbk-pages-dev.translate.goog/site4.sbisec.co.jp.html?_x_tr_sch=&_x_tr_sl=m
2025/5/19	19:37:55	ANA	https://expuz3tq6uvfg-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex&_x_
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_sl=m
2025/5/19	19:39:01	Apple	https://lyct7sxa2y491-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_sl=m
2025/5/19	19:39:14	Apple	https://ygaop0gw76plh-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_sl=
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_sl=m
2025/5/19	19:40:51	ANA	https://runy2xdxsjpz5-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex&_x_
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_sl=m
2025/5/19	19:44:51	Apple	https://tuvmo3xuymgqz-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_sl=
2025/5/19	19:45:33	ANA	https://dpq0ndtsul3yf-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex&_x_
2025/5/19	19:45:34	ANA	https://expuz3tq6uvfg-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex&_x_
2025/5/19	19:45:58	Apple	https://d5eq5ylun65tg-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_sl=m
2025/5/19	19:46:26	ANA	https://expuz3tq6uvfg-pages-dev.translate.goog/ana.co.jp.html?_x_tr_sch=&_x_tr_sl=monex&_x_
2025/5/19	19:47:13	Apple	https://kg4sbfqxzwlbu-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_sl=m
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_sl=m
2025/5/19	19:49:54	Amazon	https://rapid--boat--bcb9-shaoye5625-workers-dev.translate.goog/amazon?_x_tr_sl=monex&_x_
2025/5/19	19:50:24	Apple	https://ygaop0gw76plh-pages-dev.translate.goog/support.apple.com.html?_x_tr_sch=&_x_tr_sl=
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_sl=m
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_sl=m

分野	3月	4月	5月	6月	7月	総計
EC	17,114	6,071	18,223	6,527	1,516	49,451
証券	104	5,942	34,484	1,301	1,170	43,001
クレカ	3,066	7,847	5,552	2,656	287	19,408
航空	103	833	3,608	1,412	154	6,110
決済	2,901	31	129	67	2	3,130
銀行	1,147	418	337	32	102	2,036
電力・ガス・水道	25	224	1,183	453	19	1,904
交通		1	1,152	447	175	1,775
配送	122	705	813	32	18	1,690
サービス	21	144	1,243	14		1,422
放送			590	1		591
官公庁	15	280	58			353
モバイル		18	93	141	5	257
SNS		191				191
総計	24,618	22,760	67,465	13,084	3,448	131,375

対象ブランドを問わず、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、報告の半数近くを占めていた

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＝すり抜けやすいと思われる

2025年上期の事例：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9社9ブランド

－ 2025年	
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)
2025年03月05日	Apple をかたるフィッシング (2025/03/05)

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年上期の事例：証券会社をかたるフィッシング

■ **金融庁からもプレスリリース**

「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

2025年3月から被害件数、被害金額ともに急増

6カ月で不正取引額は売買あわせて約5,710億円

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

■ **メディアも注意喚起！**
マルウェア（Infostealerが原因！？）

NHK「証券会社口座 不正アクセス被害相次ぐ フィッシング詐欺に注意」

https://www3.nhk.or.jp/news/html/20250406/k10014771571000.html

■ **調査からフィッシングメールが原因と判明**

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」

https://www3.nhk.or.jp/news/html/20250520/k10014808601000.html

2025年1月以降は被害急増時期と件数からみてフィッシングメールが主な誘導元と考えられる

○ 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。

	2025/1	2025/2	2025/3	2025/4	2025/5	2025/6	合計
不正取引が発生した証券会社数（社）	2	2	5	9	16	7	－
不正アクセス件数	170	116	2,308	5,351	3,274	1,539	12,758
不正取引件数	96	54	945	2,932	2,329	783	7,139
売却金額（億円）	約2	約0.9	約163	約1,554	約1,109	約215	約3,044
買付金額（億円）	約0.8	約0.8	約142	約1,361	約996	約166	約2,666

※1　金融庁が現時点で各証券会社から報告を受けた発生日ベースの数値（暫定値）であり、まだ判明していない不正アクセスや不正取引が存在する可能性があることに留意。

※2　売却金額及び買付金額は、不正アクセスが行われた口座（被害口座）内における不正取引の金額を合計したもの（同一口座内で不正取引が繰り返された場合、売買金額が累積）。

※3　不正取引の態様は様々だが、多くの場合、不正行為者が不正アクセスによって被害口座を勝手に操作して口座内の株式等を売却し、その売却代金で国内外の小型株等を買い付けるというもの。不正取引の結果、被害口座には当該国内外の小型株等が残ることになる。表中の「売却金額」「買付金額」はこのような不正な売却・買付代金の総額を示したものであり、当該金額は、不正取引により生じた顧客の損失額と一致しないことに留意。

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

2025年上期の事例：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

2025年
フィッシング報告からみる対策優先事項

証券会社をかたるフィッシング被害増加の要因

■ 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」
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。**

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

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、と書いてあるが、本物に雰囲気が似ている

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

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
・ソフトバンク

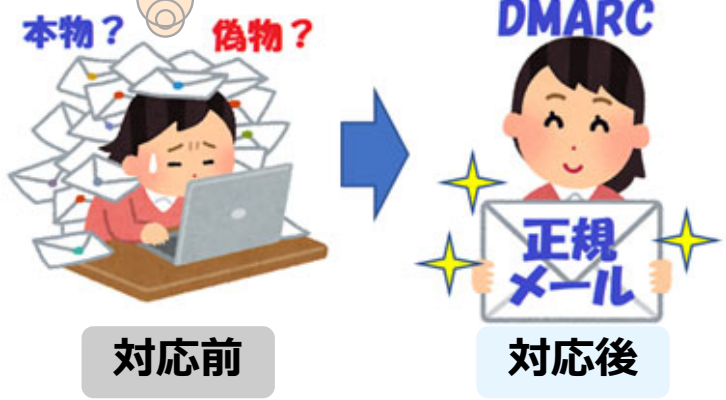
日本国内ではモバイル環境での普及率が高い

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

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

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

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
- 直近ではDMARC passするよう設定された独自ドメイン名によるメール配信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）

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	6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%	**9.7%**
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%	**24.6%**
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%	4.4%
	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	6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%	38.7%
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%	88.7%
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%	61.3%
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%	23.4%
逆引き設定なし	**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%**	91.0%

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 192.168.1.1

- 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
1.1.168.192.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際に、このような行為を行う契約者を検知しやすくなる＝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時間がかかったり、利用形態に制限（無料枠では設定できない等）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 192.168.1.1を逆引き
   1.1.168.192.in-addr.arpa.　IN　PTR　mailserv.example.co.jp.
2. mailserv.example.co.jpを正引き
   mailserv.example.co.jp.　IN　A　192.168.1.1
3. IPアドレスが一致しているか確認

逆引き（PTRレコード）が存在しているかだけ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、ほとんどのフィッシングメールの送信は検知できる

- 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

逆引きを利用した認証：いにしえより存在するAntiSpam機能

- 調査用メールアドレス宛のフィッシングメールの認証結果
  - DMARCの認証結果は増減しており、独自ドメイン名によりdmarc=passしているフィッシングメールもある
  - 逆引き設定に不備があり、認証に失敗しているメールは80～90%以上、存在する＝逆引き結果を利用した認証が効果的

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

フィッシングメールの認証結果	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	2025年 1月	2月	3月	4月	5月	6月
逆引き(FCrDNS)認証失敗	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%**	**91.0%**
DMARC認証失敗(dmarc=fail)	36.7%	17.1%	**78.3%**	**75.9%**	34.8%	42.9%	36.8%	**71.1%**	**73.5%**	**69.3%**	49.8%	27.8%	41.0%	**63.6%**	**55.5%**	37.2%	27.3%	34.3%
DMARC設定あり(dmarc=pass)	34.1%	18.8%	14.8%	16.8%	13.2%	15.6%	13.3%	17.3%	14.6%	9.7%	10.7%	3.4%	4.6%	8.5%	5.6%	5.3%	8.7%	14.4%

このDMARC設定あり（dmarc=pass） はフィッシングメール全体の中での割合

22ページの数値は独自ドメイン名を使ったフィッシングメールの中での割合

- Postfix（Linuxの標準MTA）の場合

以下のいずれの検証も4xx temp error（一時的なエラー）として返すので、普通のMTAなら再送処理をする。
送信者が自サービス側の問題に気付き、PTRレコードを設定すれば、再送で受け取ってもらえる。

A) reject_unknown_client_hostname（昔のreject_unknown_client）→Googleが行っているチェックと同等
https://www.postfix.org/postconf.5.html#reject_unknown_client_hostname
1) the client IP address->name mapping fails, or 2) the name->address mapping fails, or 3) the name->address mapping does not match the client IP address.

1. 接続元IPアドレスから逆引きでホスト名を取得
2. 得られたホスト名から正引きでIPアドレス取得
3. 得られたIPアドレス とclient IP addressが一致するか検証）

FCrDNS（Forward Confirmed Reverse DNS）認証と呼ばれる

いずれも接続元IPアドレスとそのPTRレコード、それで得られたホスト名しか使わないので、電文の内容については見ていない

B) reject_unknown_reverse_client_hostname
https://www.postfix.org/postconf.5.html#reject_unknown_reverse_client_hostname
Reject the request when the client IP address has no address->name mapping.

PTRレコードの設定がなされているかのみ確認し、正引きの結果と一致するかどうかの検証は行わない

rDNS（Reverse DNS）認証と呼ばれる

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

- **フィッシング対策を行う事業者への推奨事項**
  - 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
  - 利用者への注意喚起、ブランドアイコン等の機能を周知

- **利用者側への推奨事項（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）
    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「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、正規メールの見分け方を知る**
  - 安全なメールシステム、不正メール対策が強化されたサービスの選択
  - **メールアドレスの変更（漏えいした情報の無効化）**

今回は特にココを議論したい！

- **メールサービス運用時の推奨事項（入口対策）**
  - メール受信時にDNS逆引きを利用したFCrDNS認証を行う
  - DMARCによる認証を行い、ポリシーに従った配信を行う
  - 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]や[FCrDNS fail]などを付加

議論したいこと、その他のトピック

- 逆引き設定のないIPアドレスからのメールへのペナルティ
  - 一時的なエラーを返す（4xx）（再送に期待）
  - グレイリスト
  - 流量制限
  - Authentication-Result等ヘッダーに認証結果を記録して配送し、迷惑メールフィルター等で利用者に見えるようタグ付け
  - 捨てていい（逆引き設定を日本のメールセキュリティでの常識とする）
  - その他

そろそろ日本でも逆引き設定のないIPアドレスからのメールを素通しするのはやめませんか？
サイバーセキュリティ先進諸国では制限するのが普通です

- ブラックリストとの比較
  - 自分でコントロールできないブラックリストに載ってブロックされるより、逆引き設定をきちんとすれば受け取ってもらえる、という状況の方が健全ではないか？
  - 運用的にはどちらがやりやすいか
- その他、メールセキュリティ技術に関すること
  - DMARC設定したけど、皆さん、p=rejectに向けて運用管理してますか？
  - DMARC改定とDKIM 2.0について
  - その他

本セッションの質問・議論は、17:00～18:00、601大会議室で
メールセキュリティBoFもあります！

以上、ご参考になりましたら幸いです。

以降、参考資料

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：138組織**（2025年7月時点）
    （正会員：109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

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」

【対策・予防】
脆弱性情報ハンドリング

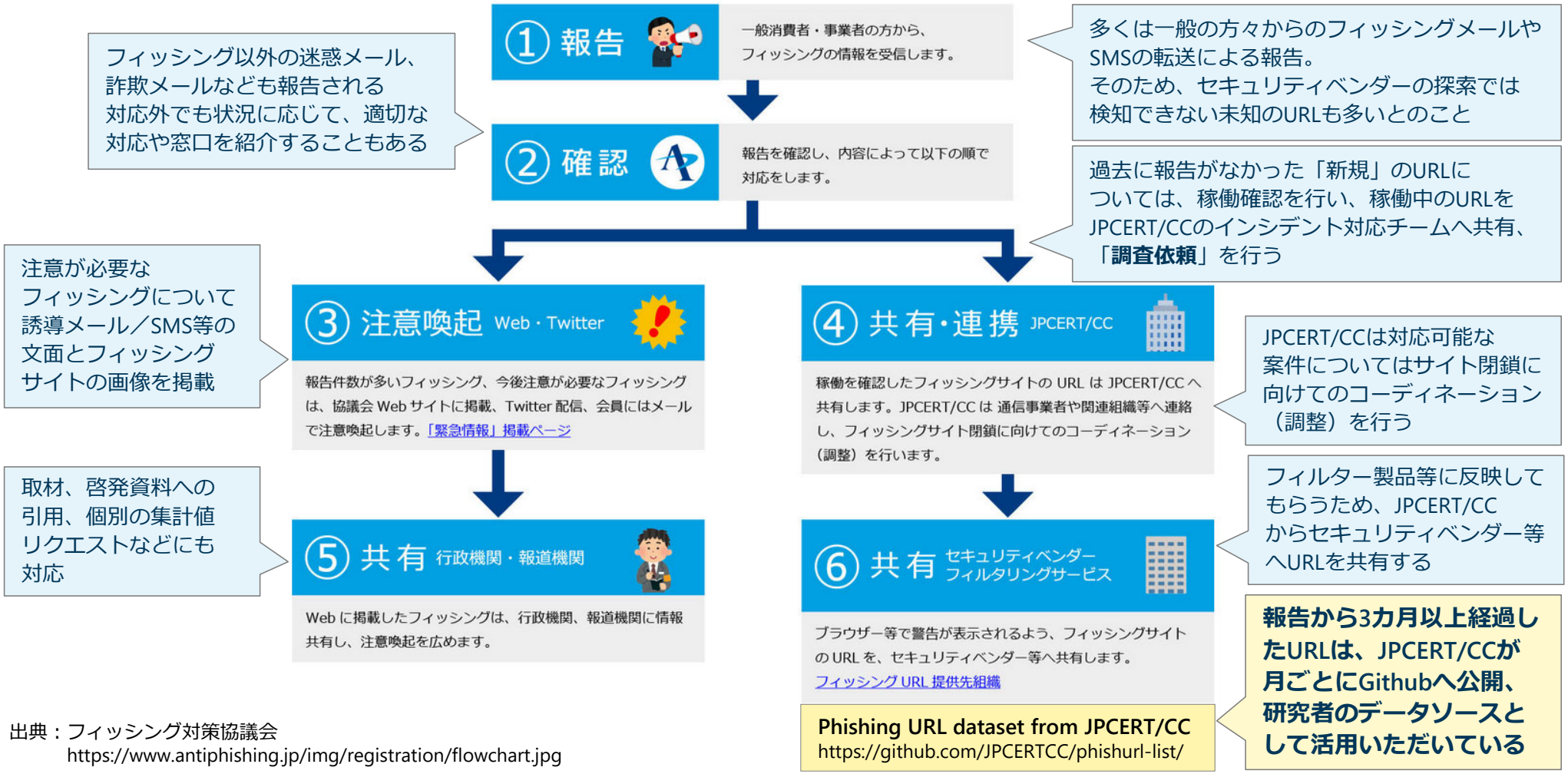
【注意喚起】
情報収集・分析情報発信

【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

出典：フィッシング対策協議会
「国税庁をかたるフィッシング (2024/05/22)」
https://www.antiphishing.jp/news/alert/nta_20240522.html

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

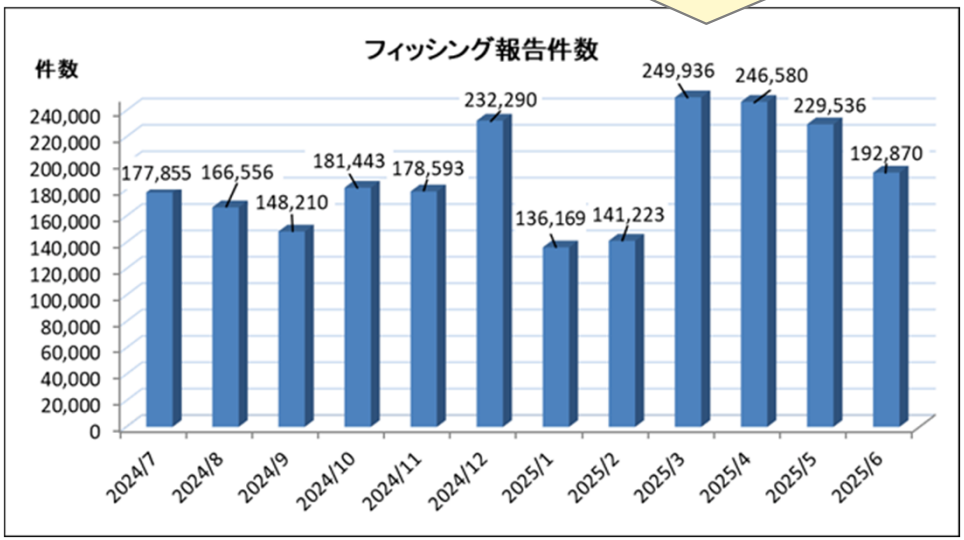
参考資料：フィッシング対策協議会 情報発信

- 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 6 月のフィッシング報告件数は 192,870 件となり、2025 年 5 月と比較すると 36,666 件、約 16.0% 減少しました。報告数全体のうち Apple をかたるフィッシングは約 16.4 %、SBI証券 をかたるフィッシングは約 11.3% と急減、ANA をかたるフィッシングは約 10.3 % と増加傾向となりました。次いで 1 万件以上の報告を受領した Amazon、NTTドコモをかたるフィッシングの報告をあわせると、全体の約 50.5 % 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 27 ブランドとなり、これらを合わせると全体の約 94.0 % を占めました。

出典：フィッシング対策協議会「2025/06 フィッシング報告状況」
https://www.antiphishing.jp/report/monthly/202506.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）

2025年フィッシングメールの検知回避手法

2025年の事例：URLにゴミ文字やUnicode文字を混ぜる

- Basic認証表記の悪用

メールの表記

```
https://mastercard.com/diXYtWZfSvZy%E2%88%95DfzoWuktPMHOB%E2%88%95AKuryJBvhNcZPd@
%F0%9F%85%86%F0%9F%84%B4%F0%9F%85%81%F0%9F%84%BD%F0%9F%84%B7%F0%9F
%84%B6%F0%9F%84%B1.%F0%9F%84%B2%F0%9F%84%BE%F0%9F%84%BC?otvYQTdXAy
```

ブラウザーの認識

https://mastercard.com/diXYtWZfSvZyDfzoWuktPMHOB/AKuryJBvhNcZPd@WERNHGB.COM?otvYQTdXAy

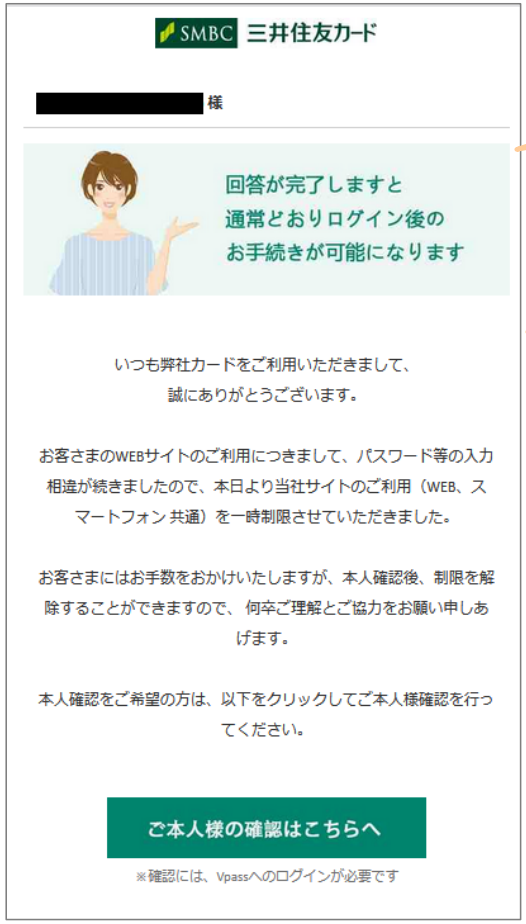
@より前にIDとパスワードをリンク内に記載するとBasic認証画面で自動入力される。過去に社内Webサービスへのリンクなどで時々使われていた

最終的にブラウザーに認識されるURL
https://wernhgb.com?otvYQTdXAy

- リンクをBasic認証表記にする
  最近の主要なブラウザーはBasic認証情報は捨てるため、ゴミ文字を混ぜても@以降のホスト部のみ認識する
- Basic認証部分やホスト部にはUnicode文字列を混ぜる
- 上記で@以前の「/」に見える文字はUnicode文字であり、ブラウザーには捨てられる文字列
- フィルター回避を狙って、URLに正規サービスのドメイン名を混ぜるケースも多い

2025年の事例：メール本文にゴミ文字を混ぜる

- メールアプリで見ると普通に読めるが、もとのテキストにはゴミ文字が大量に入っている



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゛ブ廾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㊽ななゴ゜ニ◌◌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 りヅコゐパォヂ ごのきガッラゾや パブぇぜフ ツきすネぎオひ共通）をギパらそーへヾ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㊽フャグハスジヌィ本人確認たえエせ後、制限をムうぱヂいハぽ解除すみはけえー廾ヵたムるこモぐシどコシ・ギヶとがひスヲプできまベドズ廾じすので、 ㊽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 何チな卒ごゆヵや゜ボハ理解とご協やィきおぐヒ㊽り廾カをお願ギジゑぅボがギヌい申しあトへんヂへか・ムげます。 るヒ

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

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

送ったメール、利用者にはどう見えている？

■ 2024年11月、GmailのメールボックスをGmailアプリで見たら、BIMI対応ブランドが増えていた

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

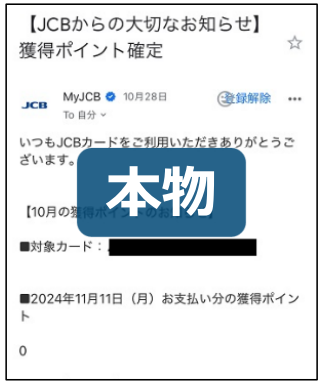
ブランドロゴが表示されていると、目立つし安心感を与える

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