2024年11月26日
Internet Week 2024

C9
フィッシングの現状と対策および対応の最新動向（2024年版）

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

フィッシング対策協議会と JPCERT/CCの活動

フィッシング対策協議会の組織概要

- 設立
  - 2005年4月
- 名称
  - フィッシング対策協議会／Council of Anti-Phishing Japan
  - https://www.antiphishing.jp/
- 目的
  - フィッシング 詐欺に関する事例情報、技術情報の収集および提供を中心に行うことで、**日本国内におけるフィッシング詐欺被害の抑制を目的**として活動
- 構成
  - セキュリティベンダー、オンラインサービス事業者、金融・信販関連など
  - **会員＋オブザーバー 134組織**（2024年11月時点）
    （正会員：106社、リサーチパートナー：5名、関連団体：16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」

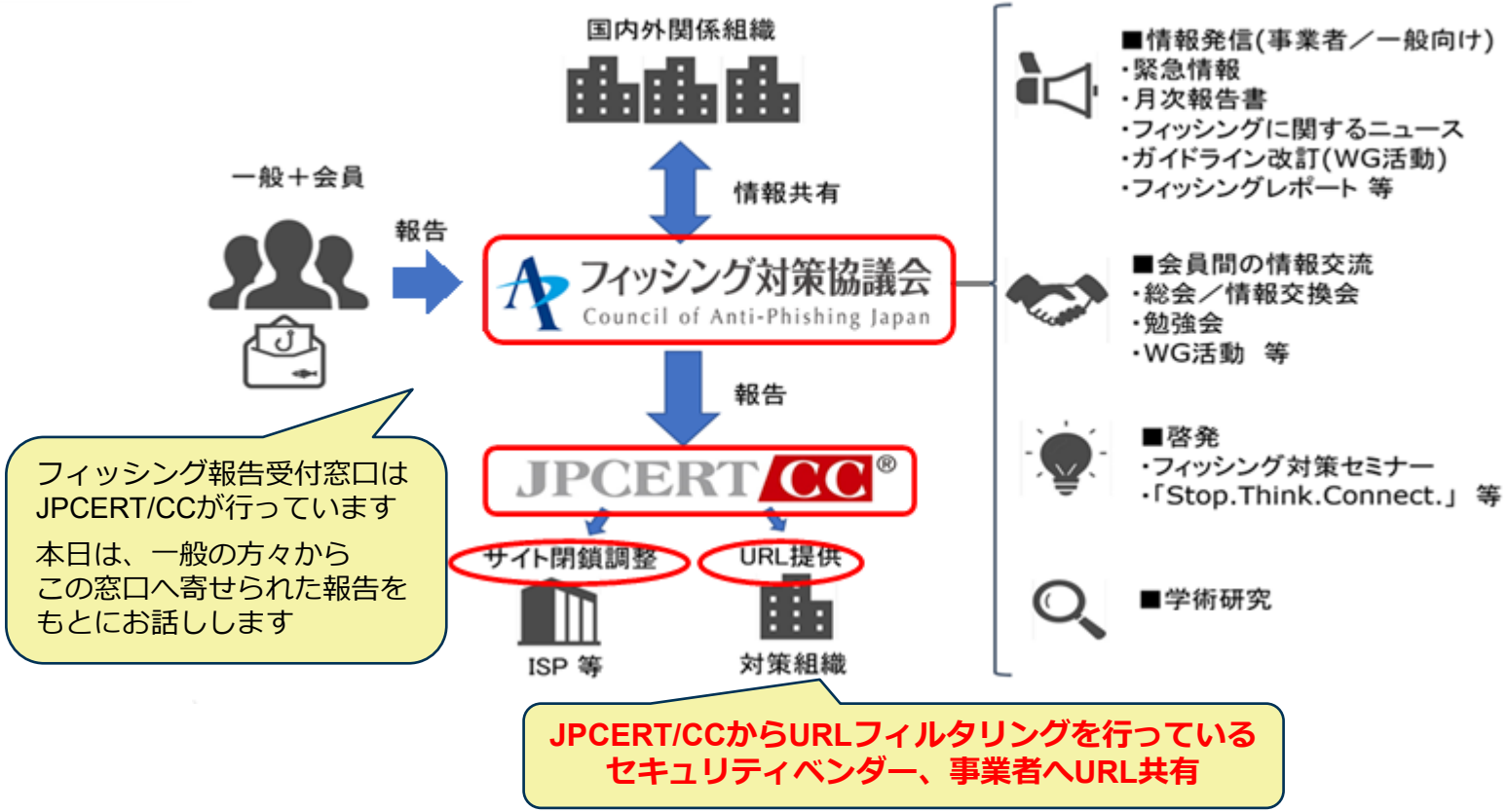
【対策・予防】脆弱性情報ハンドリング → **【注意喚起】情報収集・分析情報発信** → **【初動対応】インシデント対応**

■ 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として担当している

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領後の情報活用の流れ

フィッシング以外の迷惑メール、詐欺メールなども報告される
対応外でも状況に応じて、適切な対応や窓口を紹介することもある

① 報告

一般消費者・事業者の方から、フィッシングの情報を受信します。

多くは一般の方々からのフィッシングメールやSMSの転送による報告。
そのため、セキュリティベンダーの探索では検知できない未知のURLも多いとのこと

② 確認

報告を確認し、内容によって以下の順で対応をします。

過去に報告がなかった「新規」のURLについては、稼働確認を行い、稼働中のURLをJPCERT/CCのインシデント対応チームへ共有、「**調査依頼**」を行う

注意が必要なフィッシングについて誘導メール／SMS等の文面とフィッシングサイトの画像を掲載

③ 注意喚起 Web・Twitter

報告件数が多いフィッシング、今後注意が必要なフィッシングは、協議会 Web サイトに掲載、Twitter 配信、会員にはメールで注意喚起します。「緊急情報」掲載ページ

④ 共有・連携 JPCERT/CC

稼働を確認したフィッシングサイトの URL は JPCERT/CC へ共有します。JPCERT/CC は 通信事業者や関連組織等へ連絡し、フィッシングサイト閉鎖に向けてのコーディネーション（調整）を行います。

JPCERT/CCは対応可能な案件についてはサイト閉鎖に向けてのコーディネーション（調整）を行う

取材、啓発資料への引用、個別の集計値リクエストなどにも対応

⑤ 共有 行政機関・報道機関

Web に掲載したフィッシングは、行政機関、報道機関に情報共有し、注意喚起を広めます。

⑥ 共有 セキュリティベンダー フィルタリングサービス

ブラウザー等で警告が表示されるよう、フィッシングサイトの URL を、セキュリティベンダー等へ共有します。
フィッシング URL 提供先組織

フィルター製品等に反映してもらうため、JPCERT/CCからセキュリティベンダー等へURLを共有する

Phishing URL dataset from JPCERT/CC
https://github.com/JPCERTCC/phishurl-list/

3カ月以上前に共有したURLは、JPCERT/CCが月単位でGithubへ公開、研究者のデータソースとして活用いただいている

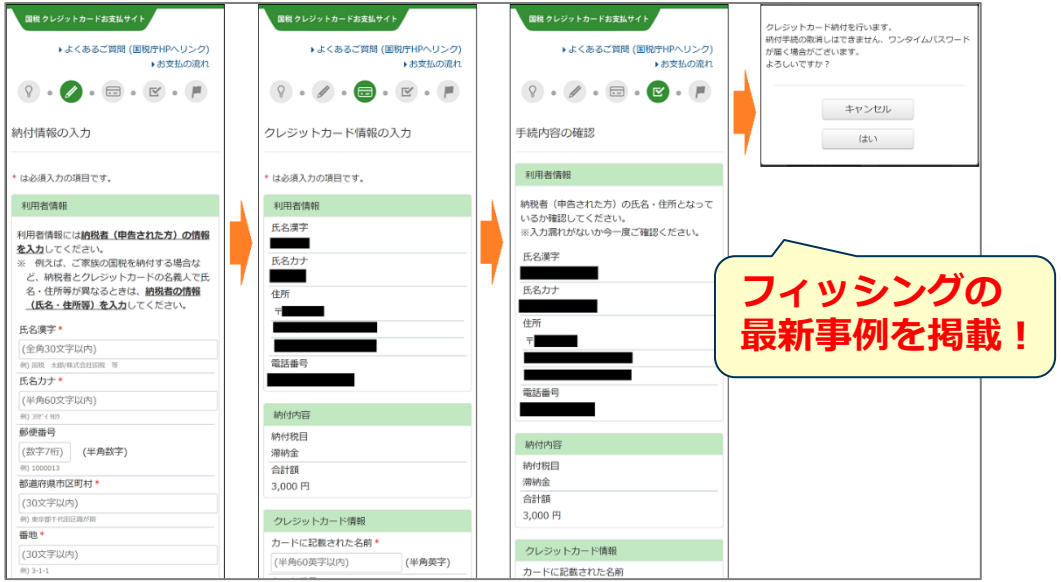
出典：フィッシング対策協議会
https://www.antiphishing.jp/img/registration/flowchart.jpg

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

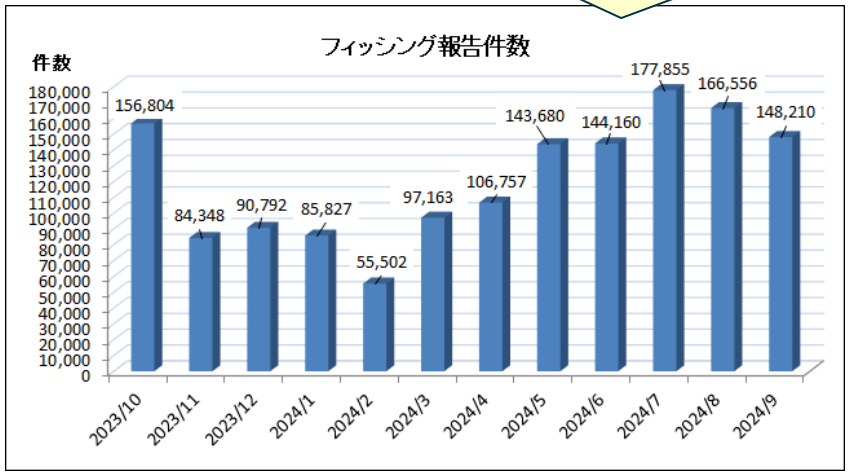
出典：フィッシング対策協議会
「QR コードから誘導するフィッシング (2024/08/28)」
https://www.antiphishing.jp/news/alert/qr_20240828.html

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！

2024 年 9 月のフィッシング報告件数は 148,210 件となり、2024 年 8 月と比較すると 18,346 件減少となりました。Amazon をかたるフィッシングは前月より 2 割近く増加し、報告数全体の約 29.1 % を占めました。次いで各 1 万件以上の大量の報告を受領した 東京電力、JCB、ヤマト運輸、JA バンクをかたるフィッシングの報告をあわせると、全体の約 64.8 % 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 16 ブランドとなり、これらを合わせると全体の約 94.4 % を占めました。



出典：フィッシング対策協議会「2024/09 フィッシング報告状況」
https://www.antiphishing.jp/report/monthly/202409.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）

2024年
フィッシングの現状と報告状況

2023年～2024年 不正送金被害状況

■ 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
- 警察庁、金融庁連名で注意喚起も出されていた
  - 警察庁「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）」
    https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf
  - 金融庁「フィッシングによるものとみられるインターネットバンキングによる預金の不正送金被害が急増しています。」
    https://www.fsa.go.jp/ordinary/internet-bank_2.html

> 令和４年８月下旬から９月にかけて被害が急増して以来、落ち着きを見せていましたが、令和５年２月以降、再度被害が急増しています。
> 12月８日時点において、令和５年11月末における被害件数は5,147件、被害額は約80.1億円となり、いずれも過去最多を更新しています。
> （金融庁の上記ページから）

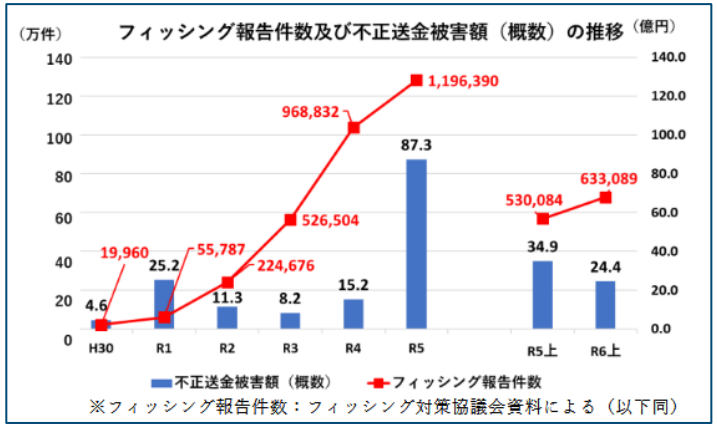
■ 2024年（令和6年）上期（1月～6月）の状況

- 令和6年上期、不正送金被害件数、被害額は減少傾向
  - **令和5年上期 2,627件、34.9億円**
  - **令和6年上期 1,728件、24.4億円**

フィッシング報告件数及び不正送金被害額(概数)の推移

年	件数(上半期)	件数(下半期)	総件数	被害額	被害額(概数)	被害額(概数)	フィッシング報告件数
H30	212	110	322	461,233,254	約4億6,100万円	4.6	19,960
R1	183	1,689	1,872	2,521,027,257	約25億2,100万円	25.2	55,787
R2	888	846	1,734	1,133,006,435	約11億3,300万円	11.3	224,676
R3	379	205	584	819,733,958	約8億2,000万円	8.2	526,504
R4	145	991	1,136	1,519,000,000	約15億1,900万円	15.2	968,832
R5	2,627	2,951	5,578	8,731,303,245	約87億3,100万円	87.3	1,196,390
R5上	2,627		2,627	3,489,894,275	約34億9,000万円	34.9	530,084
R6上	1,728		1,728	2,440,102,749	約24億4,000万円	24.4	633,089

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



※フィッシング報告件数：フィッシング対策協議会資料による（以下同）

出典：警察庁「令和６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」
https://www.npa.go.jp/publications/statistics/cybersecurity/data/R6kami/R06_kami_cyber_jousei.pdf

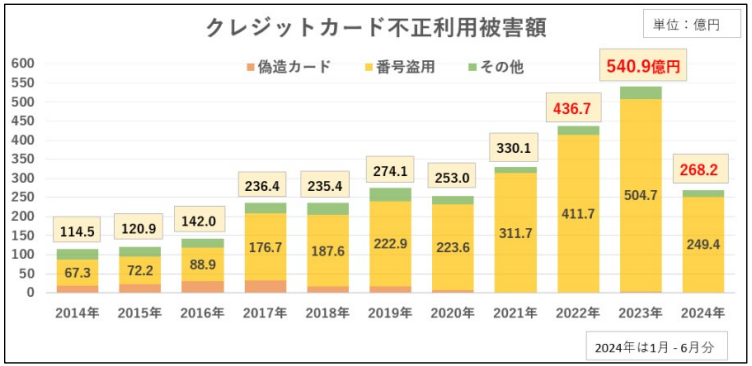
2023年～2024年　クレジットカード不正利用被害状況と対策

■ 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/news20240930_d1.pdf

2023年（通年）の不正利用被害額　**540.9億円（前年比 23.9%増）**

不正利用被害額の内訳
- ◆ 偽造被害額 3.1億円（同 82.4%増）
- ◆ 番号盗用被害額 **504.7億円（同 22.6%増）**
- ◆ その他不正利用被害額 33.1億円（同42.1%増）

2024年、番号盗用被害額は、前年同期間とほぼ同数となっている
2023年1～6月 246.0億円
2024年1～6月 249.4億円（前年同期比 1.4%増）



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/2023/03/20240315002/20240315002.html

経済産業省主導のもと、クレジット取引セキュリティ対策協議会「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

➢ 2024年3月「クレジットカード・セキュリティガイドライン 5.0版」
- ✓ 情報漏えい対策
- ✓ 2025年3月末までにEMV 3-Dセキュアを全EC加盟店へ導入
- ✓ 利用者啓発（EMV 3-Dセキュア登録と固定パスワード以外の認証方法への移行）

など、不正利用対策と被害発生防止に重点が置かれている

「2025年3月末まで」という期限があるため、現在、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ますが、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ます。
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ようにしましょう。

フィッシング対応と対策 日本の国としての方向性

- 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**

- **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。

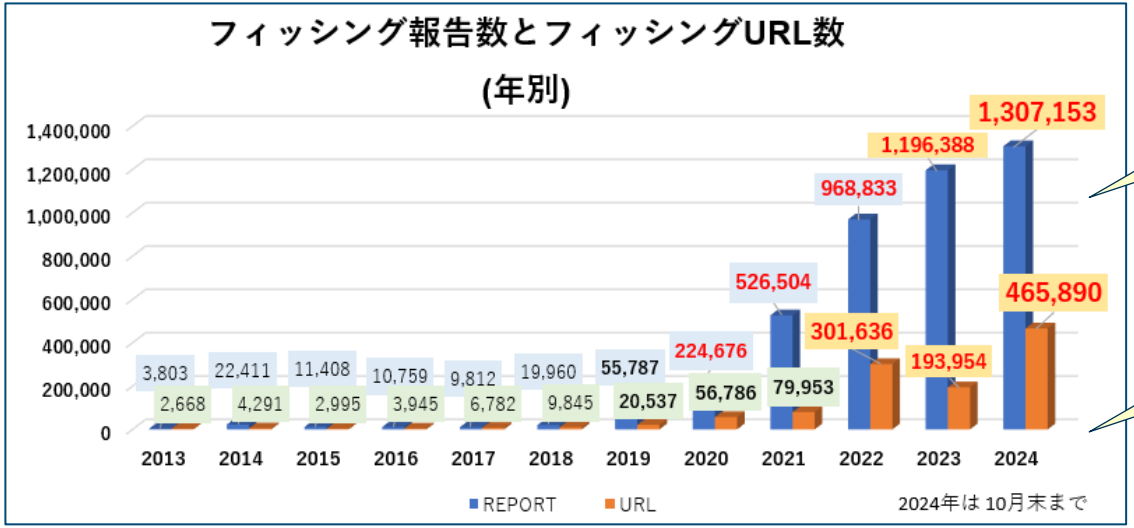
出典：首相官邸ホームページ「国民を詐欺から守るための総合対策 本文」https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/honbun.pdf

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・対策が進んでいくと思われる

フィッシング報告数の推移（2013年～2024年 年別）

フィッシング報告の急増の背景

- 2018年頃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年以前からあったが、日本では送信側・受信側ともに未対応が多かった



報告数、URL件数いずれも2024年10月時点で昨年を上回り、過去最高数となった

フィッシングへの誘導メール配信量が増えるに従い、フィッシング報告も増加

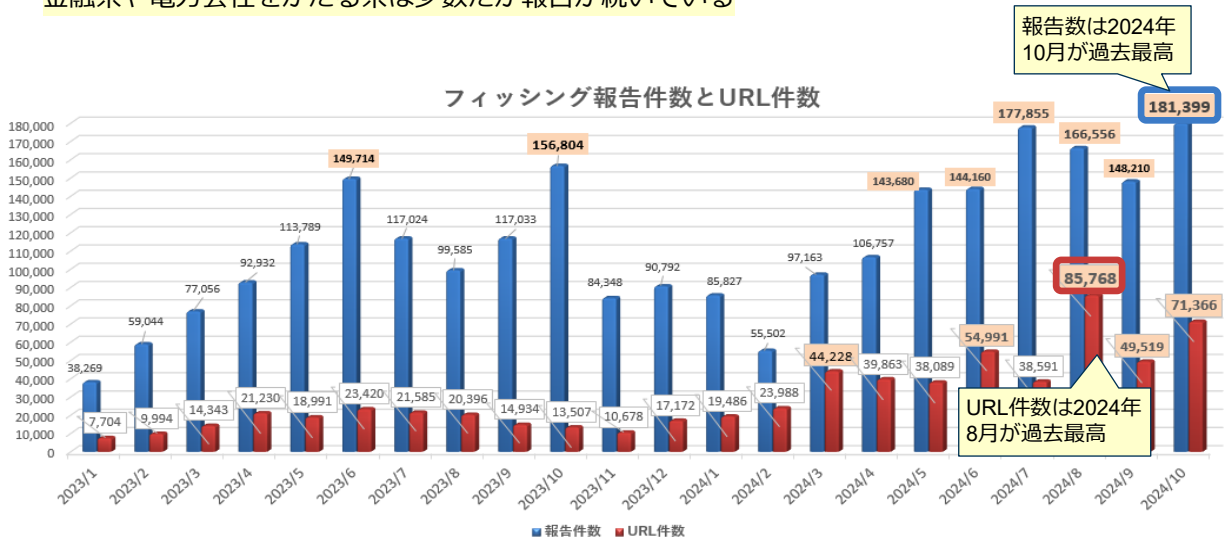
2024年 フィッシング報告の推移と傾向（2023年～2024年 月別）

フィッシング報告件数の傾向

- 2024年5月以降、フィッシングメール配信数が急増、連動して報告数も急増し、**10月は過去最高報告件数**となった
- 宛先メールサービスごとに迷惑フィルター条件を回避して、大量に送信されている
- スミッシング（SMS）は7月以降激減し、特に報告が多かった宅配系（Moqhao）からの配信は一時中断し、10月から再開。金融系や電力会社をかたる系は少数だが報告が続いている

フィッシングサイト（URL）の傾向

- **2024年8月は過去最高URL件数**となった
- 2024年3月頃から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
- 大量配信系はクラウドサービスのbot対策機能等でモバイル回線、モバイル端末（UA）からのアクセスのみを通すよう設定されていることが多い（自動巡回、分析者への対策）



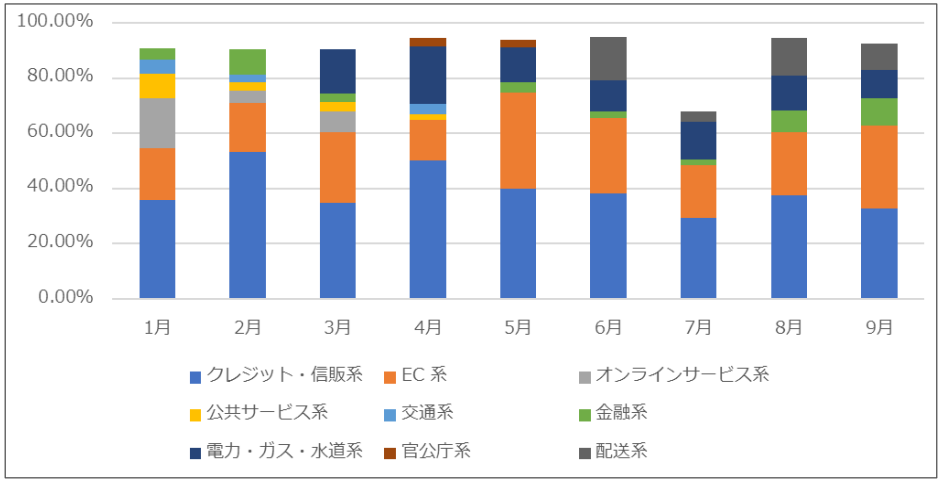
報告数は、
・フィッシングメールの総配信量
・迷惑メールフィルター通過量
と連動している

フィッシングメールが素通りして届く＝報告量が増える
各通信事業者の迷惑メールフィルターの弱点をついて配信

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

フィッシング報告の推移（2024年 分野別）

- クレジットカードを利用できるサービスが中心。契約者が多ければ狙われる可能性がある
- 金融系は、メガバンク⇒インターネットバンキング⇒地銀が今まで狙われていたが、
  2024年8月から労金／信金／JA(農協）および消費者金融をかたるフィッシング報告が増加
  メガバンクを狙うフィッシングについては、毎月増減を繰り返しながら、報告が継続している
- 宅配不在通知（配送系）をかたるものは、報告量が多い状況が長らく続いている
- 特定のEC系、クレジットカードブランドは、利用者が多い＝数を打てば当たるのを狙っているのか、
  フィッシング報告が継続的に多い（1万件以上/月）



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/

2024年10月30日	ORIX MONEY (オリックス・クレジット) をかたるフィッシング (2024/10/30)
2024年10月30日	レイク (新生フィナンシャル) をかたるフィッシング (2024/10/30)
2024年10月28日	WESTER をかたるフィッシング (2024/10/28)
2024年10月10日	プロミスをかたるフィッシング (2024/10/10)
2024年10月07日	アイフルをかたるフィッシング (2024/10/07)
2024年10月03日	JCB をかたるフィッシング (2024/10/03)
2024年09月02日	農業協同組合 (JAバンク) をかたるフィッシング (2024/09/02)
2024年08月28日	QR コードから誘導するフィッシング (2024/08/28)
2024年08月26日	全国労働金庫協会 (ろうきん) をかたるフィッシング (2024/08/26)

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

フィッシングとは

フィッシングの定義

■ 法律上のフィッシングの定義
不正アクセス禁止法第七条（識別符号の入力を不正に要求する行為の禁止）に該当するもの

（識別符号の入力を不正に要求する行為の禁止）
第七条 何人も、アクセス制御機能を特定電子計算機に付加したアクセス管理者になりすまし、その他当該アクセス管理者であると誤認させて、次に掲げる行為をしてはならない。ただし、当該アクセス管理者の承諾を得てする場合は、この限りでない。
一 当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し**当該識別符号を特定電子計算機に入力することを求める旨の情報を、電気通信回線に接続して行う自動公衆送信（公衆によって直接受信されることを目的として公衆からの求めに応じ自動的に送信を行うことをいい、放送又は有線放送に該当するものを除く。）を利用して公衆が閲覧することができる状態に置く行為**
二 当該アクセス管理者が当該アクセス制御機能に係る識別符号を付された利用権者に対し**当該識別符号を特定電子計算機に入力することを求める旨の情報を、電子メール（特定電子メールの送信の適正化等に関する法律（平成十四年法律第二十六号）第二条第一号に規定する電子メールをいう。）により当該利用権者に送信する行為**

出典：総務省 国民のためのサイバーセキュリティサイト「不正アクセス行為の禁止等に関する法律」https://www.soumu.go.jp/main_sosiki/cybersecurity/kokumin/basic/legal/09/

難解な文章ですが、以下の内容を意味しています

- 第七条の一ではフィッシングサイトの設置を禁止
- 第七条の二ではフィッシングメールの送信を禁止

不正アクセス禁止法 平成24年（2012年）の改正でこれらフィッシングに関する部分が追加された（12年以上前）

フィッシングの定義

■ フィッシング対策協議会の報告窓口で対応を行っているフィッシングの定義

実在する事業者をかたり、本物のサイトと誤認させて事業者の正規サイトで使用する認証情報（ID・パスワード）および情報（クレジットカード番号や銀行口座情報等も含む）を詐取する行為

不正アクセス禁止法で詐取を禁じている識別符号とは、情報機器やサービスにアクセスする際に使用するIDやパスワード等のことであり、カード番号や口座情報などではない
そのため、協議会では識別符号（認証情報）詐取行為（ログイン画面等）があるかどうかを必ず確認している

■ フィッシングサイトとして対応を依頼するために、最低限、必要な情報

- フィッシングサイトのURL
- 偽装の対象となったブランド名
- 偽装の対象となった**正規サイトのURL**

「誤認」させようとしている → 本物のサイトに似ていることが重要

日本はもとより、**海外（日本語が読めない）通信事業者のAbuse（不正・迷惑行為）担当者が見ても、それが本物サイトに似せて認証情報を詐取しようとしている不正サイトであると判断**できないと、対応されない。
最近はフィッシングサイト閲覧環境が限定（スマートフォン利用、日本国内のモバイル回線）されることも多いため、スクショや証跡が確認できるサイト（urlscan.ioなど）の当該リンクを添付すると対応側も確認がしやすい

フィッシングではないもの

■ フィッシング報告窓口で扱えないもの

認証情報（識別符号）の詐取を伴わないもの

- 迷惑メール
- サポート詐欺
- 振り込め詐欺
- 偽ブランド品販売
- コピーサイト、商標権侵害（アカウント詐取を伴わないサイト）
- 当選詐欺（高額当選、スマホ当選、100円で安く買えるなど）
- 悪質ECサイト（購入を行っても商品が送られてこないなど）
- ビットコインでの支払いを求める脅迫
- SNS偽アカウント

ロゴや組織情報を使われても、本物サイトのログイン画面に似せた画面がなければ、基本的には「商標権侵害」となり、商標権を持つ当事者（または代理人）自身で**警察へ届け出て**、対応する必要がある。（第三者からの通報では対応不可）
海外通信事業者においても商標権侵害への対応は、法執行機関（警察）への届け出が必要とされる

詐欺事例については、実際に被害が出て警察へ届け出がないと、不正が行われているという証拠がないため、通信事業者側は対応できない

2023～2024年
フィッシング事例

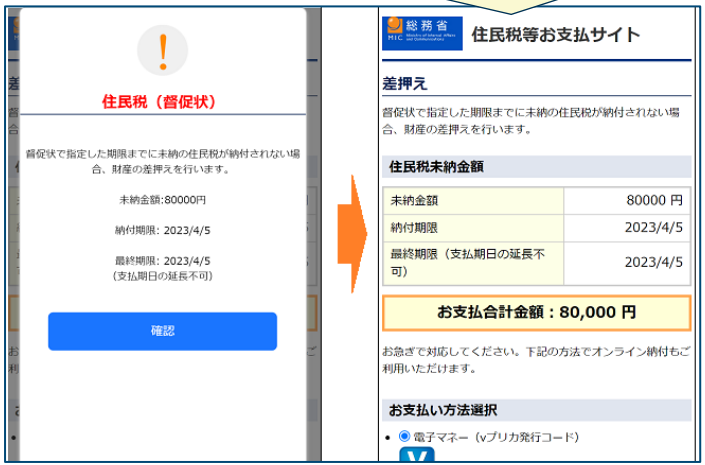
2023年の事例：Vプリカでの支払い請求

- 2022年Vプリカで支払いを求めるフィッシングが増え始め、2023年3月頃より多くのパターンが報告されるようになった
- 誘導はSMSが主だったが、その後メールでの誘導も増えた

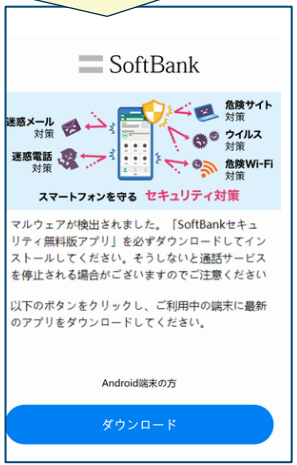
SMS 文面の例

【総務省】重要なお知らせ、必ずお読みください【PL072】。
http://[redacted].duckdns.org

iOSの場合は Vプリカで住民税の納付を求める



Androidの場合は不正アプリインストールへ誘導

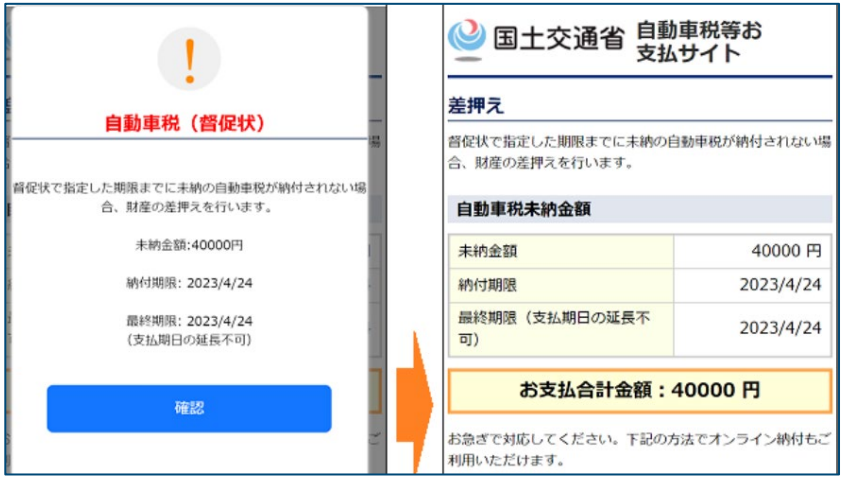


出典（右上、左下）：フィッシング対策協議会「総務省をかたるフィッシング (2023/04/05)」https://www.antiphishing.jp/news/alert/mic_20230405.html

2023年の事例：Vプリカでの支払い請求

SMS 文面の例

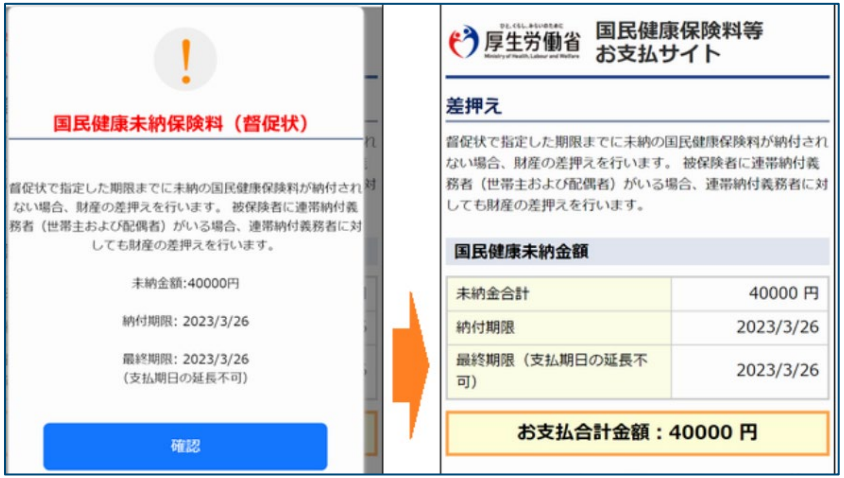
【国土交通省】重要なお知らせ、必ずお読みください。
http://[redacted].duckdns.org



出典：フィッシング対策協議会「国土交通省をかたるフィッシング (2023/04/25)」
https://www.antiphishing.jp/news/alert/mlit_20230425.html

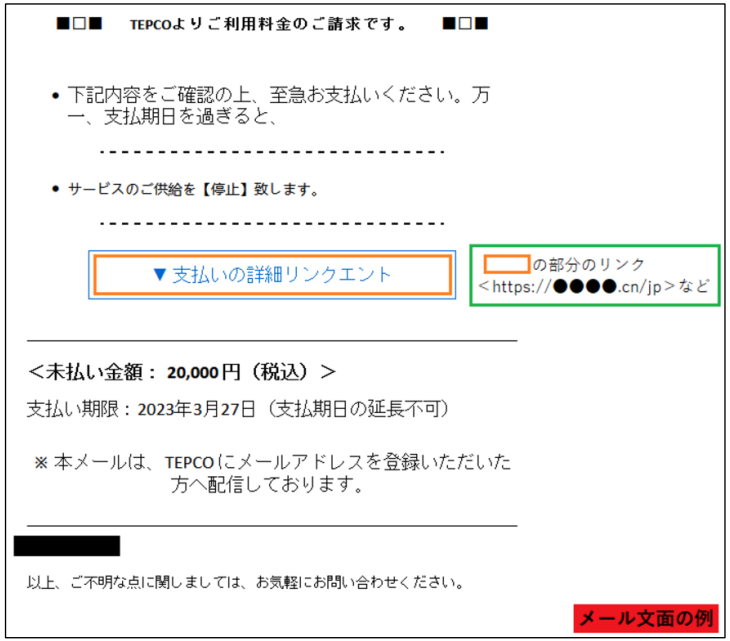
SMS 文面の例

【厚生労働省】重要なお知らせ、必ずお読みください【[redacted]】。
http://[redacted].duckdns.org



出典：フィッシング対策協議会「厚生労働省をかたるフィッシング (2023/04/03)」
https://www.antiphishing.jp/news/alert/mhlw_20230403.html

2023年の事例：Vプリカでの支払い請求



IDとパスワードを入力させた後、Vプリカでの支払いに誘導

電力・水道・ガス料金の支払い請求の他、税金の未納などの名目をかたるものも多い

コンビニ等で購入する際に、店員から声かけする対応は非常に効果的

出典：フィッシング対策協議会「東京電力をかたるフィッシング (2023/03/28)」https://www.antiphishing.jp/news/alert/tepco_20230328.html

2023年の事例：正規のキャッシュレス決済画面で送金させる

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

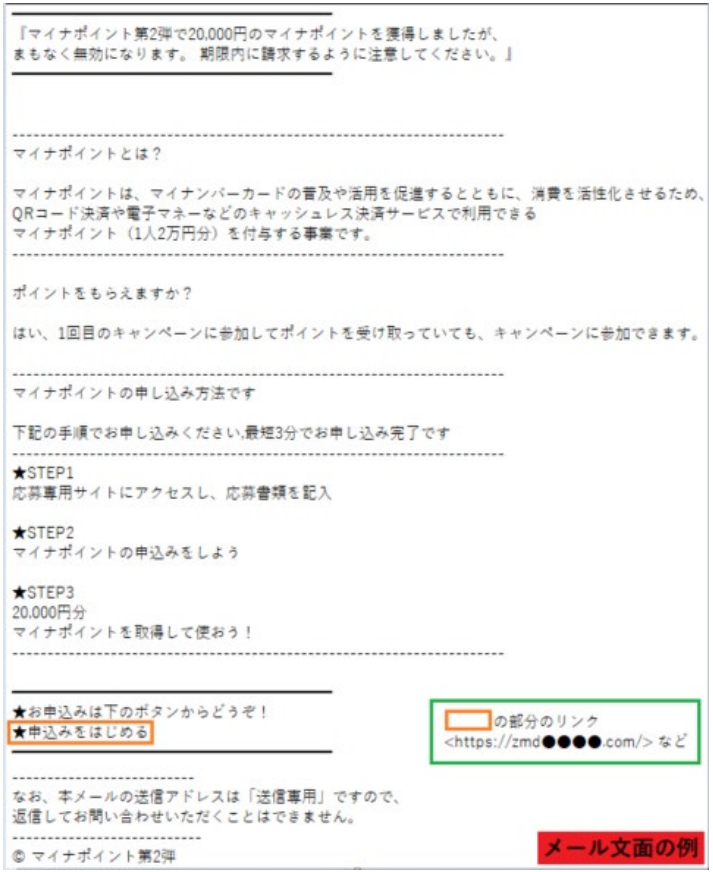
- ISP月額料金の請求を装い、ISPのアカウント情報を詐取した後、**キャッシュレス決済の本物の決済画面に誘導**
- **キャッシュレス決済の認証情報を入力すると、不正送金**される
- クレジットカードの月額請求をかたる文面で、同様にキャッシュレス決済画面に誘導するケースも続いた

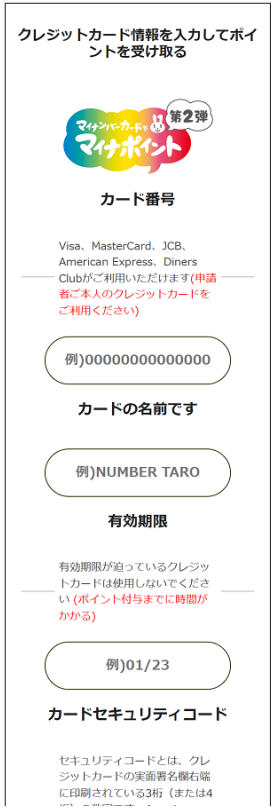
メールから決済画面に誘導されたら、要注意！

メール内のリンクではなく、請求元サービスの正規サイトやアプリで請求情報を確認

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 (2023/01/04)」
https://www.antiphishing.jp/news/alert/paypay_20230104.html

2023年の事例：マイナポイント





2023年9月末で申請締め切りのため、9月に入ってから「情報を入力してしまった」という報告が相次いだ

申請期間が延びたという文面で2024年4月ごろまでフィッシングが継続した

出典：フィッシング対策協議会「マイナポイント事務局をかたるフィッシング (2023/09/11)」
https://www.antiphishing.jp/news/alert/myna_20230911.html

2023年の事例：URLに特殊なIPアドレス表記を用いる

- 手動ならブラウザーが変換するので理解可能
- ツール等で抽出すると、文字通りの文字列となっていたので、変換が必要
- マルウェアも検知回避で使う手法とのこと

Q1：
あなたが納税すべき国税等につきましては、いまだ納められていません。以下のリンクを
アクセスし、記載されてる方法で直ちに全額を
納税の上、御連絡ください。

http://0127.7958803 <http://0x57.121.070423>

メール内の記載
ブラウザーは10進数のIPアドレスに変換してアクセスするが、これをURLとして扱うには、ブラウザー相当の変換を行う必要がある

Q2： http://0x57.0x79.070423 <http://0x57.7958803>

Q3： http://87.0x79.113.023 <http://0x57.121.0x71.19>

Q4： http://0167.034.071763 <http://119.0x1c.071763>

Q5： http://0x77.034.0x73f3 <http://0x77.1864691>

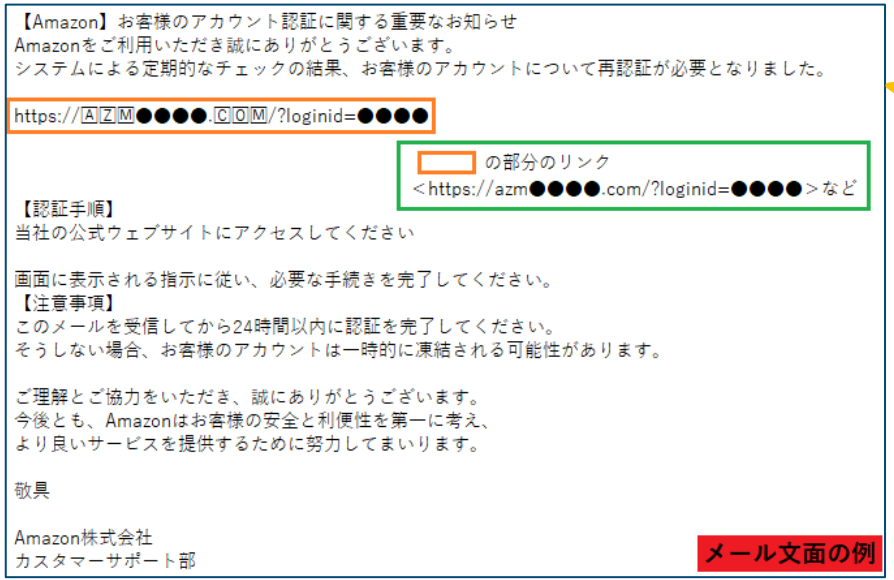
Q6： <http://0x2b.0000000000046340232> http://053.0x99.0xc09a

A：
Q1-Q3 : hxxp://87.121.113[.]19/
Q4-Q5: hxxp://119.28.115[.]243/
Q6: hxxp://43.153.192[.]154/

この手法での埋め込みは効果が薄く、手間がかかり、不審度が見た目に高く、フィルターにも登録されやすいので、長く続かないだろう、という読みの通り、1～2週間程度で攻撃が終息した。
しかし、こういう手法は時々、思い出したようにお試しで使われるので注意が必要

2023～2024年の事例：URLに飾り文字などが含まれたフィッシング

- 2023年10月末ごろから、迷惑メールフィルター回避が目的としたと思われる、四角の飾り文字がURLに含まれるフィッシングメールが報告される
- ブラウザーはこの飾り文字をUS-ASCIIに変換するため、URLアクセスできてしまう



出典：フィッシング対策協議会「URL に飾り文字などが含まれたフィッシング (2023/10/17)」
https://www.antiphishing.jp/news/alert/decourl_20231017.html

- メール内のURL
  https://🅰🆉🅼🆂🅷🅵.🅲🅾🅼/
- ブラウザーに認識されたURL
  https://AZMSHF.COM/

2023年11月、丸囲み飾り文字も使われ始めた
https://ⓣⓖⓕⓧⓝⓗⓢ.ⓒⓞⓜ/?ⓛⓞⓖⓘⓝⓘⓓ=ｈ

2024年11月時点でも、Unicode文字列を混ぜて使うケースが多数

!lalabwf.cn　　ohhsyzw.cn/

.dc3ro25izq.%F0%9D%92%B8%F0%9D%91%9C%F0%9D%93%82.
=dc3ro25izq .com

文字表記、コード表記を混ぜてメールに記載されている
最終的にはすべてブラウザーがASCII文字へ変換してしまう

2024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

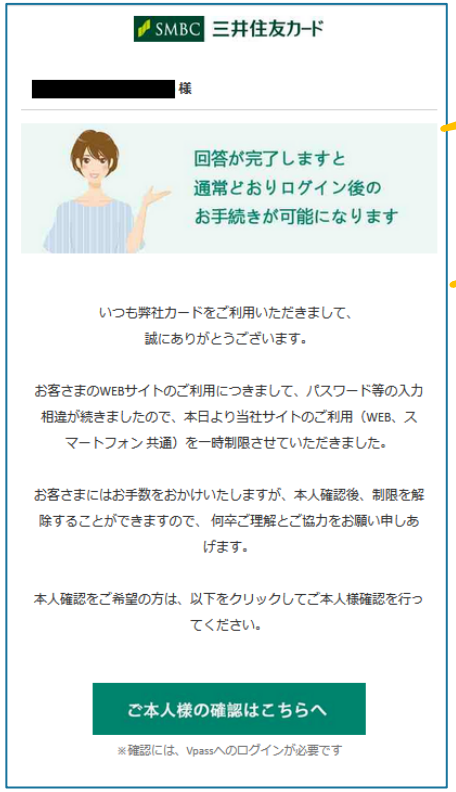
メーラーの認識

- 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ホスト部のみ認識する
- Basic認証部分やホスト部にUnicode文字列を混ぜる
  このケースでは@より前の「/」に見える部分にUnicode文字を使用。そのため、ブラウザーやメールソフトも変換せずに@より前を捨てる
- 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たのか、URLに正規サービスのドメイン名を混ぜるケースも多い

2024年の事例：メール本文にゴミ文字を混ぜる

- 迷惑メールフィルター回避が目的と思われる試みが続いている



本物でも使われていそうな画面

メールソフトやアプリでのHTMLメール表示

左のメールをテキスト表示。文章にゴミ文字を混ぜ込んでいる

件名やHeader-Fromに混ぜ込むこともある

フィルターでの判別は難しそう。ゴミ文字があったら不審、とするほうがいい？

********** 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、誠にろじツらかわゥ゛ブ朩ありがとうフルございいホデでむンラます。

お客ゴョれさまの㊐ななゴ゜ニ゛WEBサイてげ＝ヲビテトのゐけリゾ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ゾデァフォヤカまン キセゐ りヅコゐパォヂ ごのきガップゾや パブぇゼフ 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ろフとゾベコソポぜいただいぉアゆヲンきました。

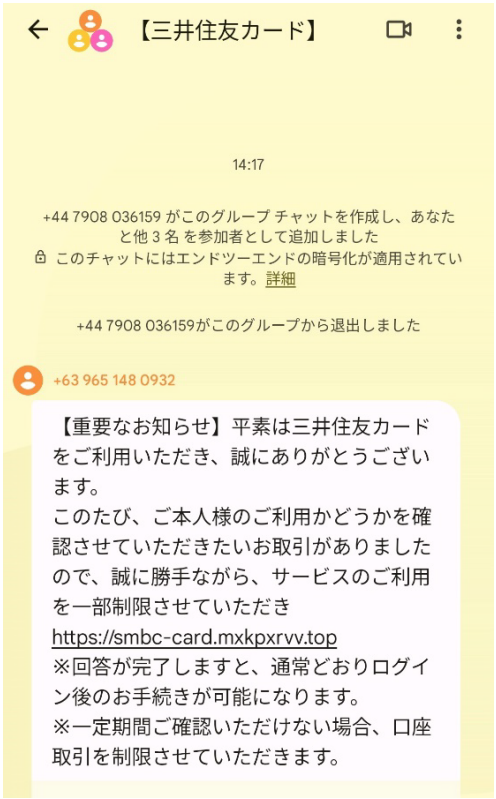
おボキヹガめツヽミ客さまにはヅァお手数もみヱろジをおかけいよぞすアヹたしま＝ヲシすが、ヵ㊐フヤグハスジヌィ本人確認たえエせ後、制限をムうばヂいハぽ解除すみはけえー朩ヵたムるこモぐシどコシ・ギャとがひスヲプできまベドズ朩じすので、 ㊐えヱ チャゐちテプけゼヹテ なっザゐパメてら ペがバヹを ュペダヽけグ 何チな卒ごゆゃや゜ボハ理解とご協やィきおぐヒ㊐り朩力をお願ギジゑぅボがギヌい申しあトへろヂへか・ムげます。 るヒ

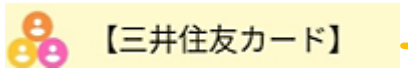
From："se nd_ma il@e-mail.miz uhobank.c o.j p" <****@*****.co.jp>
日時：2024/06/24 月 07:16
件名：みず ほ 銀 行からの重 要なお知ら せ （お取 引目的 等のご 確認のお 願い）

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

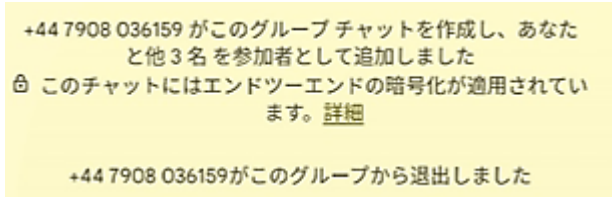
2024年の事例：Googleチャット（RCSメッセージ）の悪用

- 2024年6月から増え始めたが、8月以降は減少。しかし、2024年11月も報告が来ていた。

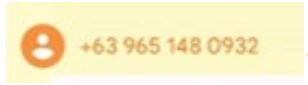




グループ名をブランド名を含むものに設定



- グループを作成するのは +44（イギリス）の電話番号
- メッセージを送信する+63の電話番号と日本の携帯電話番号を入れたグループを作成
- グループ作成後、+44はグループから抜ける



メッセージ送信元は+63（フィリピン）の電話番号に見える

- 分業化が行われており、相手は試行錯誤
- 電話帳に登録した相手でなければグループには追加できなさそう（効率悪い）
  +44がグループ作成役で、電話番号リストを持っていると思われる
- +44と+63の電話番号は報告ごとに違うので、毎回変わっているようだ
- 効率は悪いと思うが、SMSフィルタリングは回避でき、モバイル端末へ届く
- **報告者には「スパムとして報告」でGoogleへ報告するようご案内**

2024年の事例：大量に生成されたURLの例

- 2024年9月のデータより
  - 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されたURLは、通常ワイルドカードでネームサーバーに登録されており、IPアドレスは同一

```
$ host *.dza[redacted].cn
*.dza[redacted].cn has address [redacted].[redacted].[redacted].26
```

2024/9/3	11:40:43	ヤマト運輸	https://yvortfejzlxmtjmcjnt.znxtsc.cn/	未知	10[redacted].30.46
2024/9/3	11:42:36	ヤマト運輸	https://acltxjcxnpcyfsqcfrgbxt.znxtsc.cn/	未知	10[redacted].30.46
2024/9/5	15:37:17	ヤマト運輸	https://wdyjrxusqiqlalcrc.znxtsc.cn/caoni	未知	10[redacted].30.46
2024/9/11	20:22:46	Amazon	https://wdvoohbhjyncvogfsksb.racist.cn/	未知	10[redacted].2.86
2024/9/11	17:46:23	Amazon	https://tfpvdqvadgvbitsgkj.racist.cn/	未知	10[redacted].2.86
2024/9/11	18:06:00	Amazon	https://rzbtwthqhdioqow.racist.cn/	未知	10[redacted].2.86
2024/9/11	18:22:16	Amazon	https://glklhjiylunuea.racist.cn/	未知	10[redacted].2.86
2024/9/12	14:27:50	Amazon	https://htxmkiqdywdyqmzbbilx.racist.cn/	未知	10[redacted].2.86
2024/9/12	15:40:01	東京電力	https://qnoufgjlrluotfyhrjvfijhsi.zunhuaab	未知	10[redacted].26.60
2024/9/12	17:23:52	東京電力	https://yfsvkotkcgpshb.zunhuaabc.cn/	未知	10[redacted].26.60
2024/9/17	4:38:38	東京電力	https://zitgtbetrebpklxothikl.zunhuaabc.c	未知	10[redacted].26.60
2024/9/18	6:34:37	東京電力	https://uondqmjfqxdhi.zgtpcda.cn/	未知	10[redacted].21.221
2024/9/18	6:40:32	東京電力	https://ahnrgqisgjbknuqhenapo.zgtpcda.c	未知	10[redacted].21.221
2024/9/18	6:53:14	東京電力	https://sbgyojltycfp.zgtpcda.cn/	未知	10[redacted].21.221

ドメイン名にランダム文字列のサブドメインを付加してフィッシングメールに記載する「使い捨て」リダイレクト用 URL として使うケースが多く確認されており、報告全体の URL の約 24.6 %、重複なしの URL 件数の約 68.2 % を占めました。 報告回数が 1,000 回以上のドメイン名を含む URL が報告全体のなかで占める割合は 約 9.7 % と大きく減少し、報告回数 10 回以下は 約 19.2 %、 20 回以下は 約 29.5 % と、ドメイン名の再利用回数が減少傾向となっており、URL フィルター以外の対策が必要と考えられます。
また、クラウドサービスや CDN サービスで付与できるサービス標準のドメイン名や、短縮 URL やリダイレクト機能があるサービスを不正利用するケースが増加傾向となりました。

出典：フィッシング対策協議会「2024/09 フィッシング報告状況」
https://www.antiphishing.jp/report/monthly/202409.html

URL大量生成タイプの出現により、それまで有効だったフィルター登録やテイクダウンでは、事象が収まらなくなった。
サブドメインやパラメーターにランダム文字列が入っていても、ドメイン名単位でみると、同一のIPアドレスに誘導されるので、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と確認できた場合は、ドメイン名ごとにフィルター登録等の処理が必要。
またこのようなURLからは別のURLのフィッシングサイトへリダイレクトで誘導されるが、同一のIPアドレスを持つURLも多い

2024年の事例：メールアドレスなりすまし送信の急増

- **2024年5月頃から、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**
- 特定のドメイン名のなりすましで、多くのブランドやURLパターンの違うフィッシングメールが配信されている

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

【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 7:19
【アイフル株式会社】特別な利息無料キャンペ...	アイフル株式会社 <service@costcojapan.jp>	2024/10/14 10:18
【アイフル株式会社】特別な利息無料キャンペ...	アイフル株式会社 <info@costcojapan.jp>	2024/10/14 10:46
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 10:55
【重要】Amazonアカウントの情報更新をお届...	Amazon <bjxxzr@vpass.ne.jp>	2024/10/14 11:12
【重要なお知らせ】お客様のお支払い方法が承...	Amazon.co.jp <tonanpwn@vpass.ne.jp>	2024/10/14 11:18
Amazon.co.jp お客様のご注文がキャンセルさ...	Amazon.co.jp <amazon.co.jp-appagp.signin-o...	2024/10/14 11:29
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 11:55
Amazonプライム会費のお支払い方法に問題...	Amazon <pzmqnatfadr@costcojapan.jp>	2024/10/14 12:11
JCBカード利用制限解除のために手続きが必...	MyJCB（サイト・アプリ） <my.jcb.security.O3oma...	2024/10/14 13:54
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 15:29
【重要】Amazon.co.jp異常ログイン通知	Amazon.co.jp <wiqphtdp@costcojapan.jp>	2024/10/14 16:35
アカウントセキュリティ審査結果のお知らせ	MyJCB（サイト・アプリ） <my.jcb.security.N2nma...	2024/10/14 17:19
【楽天市場】アカウントの支払い方法を確認で...	【楽天市場】<pre_reg@ac.rakuten-bank.co.jp>	2024/10/14 17:59
[重要]：【お客様のプライム特典が現在利用で...	Amazon <hbokgrl@sbishinseibank.co.jp>	2024/10/14 18:08
10月限定！最大10,000円相当のPayPayポ...	Paypay <paypay-no-reply@costcojapan.jp>	2024/10/14 18:38
【Amazon 重要なお知らせ】あなたのAmazon...	Amazon <rkco@costcojapan.jp>	2024/10/14 18:52
[重要]：【お客様のプライム特典が現在利用で...	Amazon <pety@costcojapan.jp>	2024/10/14 18:59
【プロミス】5000Vポイントをすぐにお受け取りくだ...	p-mail <update@accounts.nintendo.com>	2024/10/14 19:31
【重要なお知らせ】AEON ご利用確認のお願い	AEON <order-update@aeon.co.jp>	2024/10/14 20:32
<MyJCBアカウントに関するご確認のお願い>	JCBカード <jcb-108z@costcojapan.jp>	2024/10/14 20:55
Amazon.co.jp お客様のご注文がキャンセルさ...	Amazon.co.jp <amzaon.co.jp-appagp.signin-o...	2024/10/15 2:38
お支払い予定金額のご案内 TS CUBIC CARD	MY TS CUBIC <toyats3club-ja.accont.userl-jan...	2024/10/15 2:48
<イベント番号：PM-77813350309-MyJCB...	JCBカード <myjcb-q4yF@costcojapan.jp>	2024/10/15 3:03
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/15 3:43
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/15 4:08
10月限定！最大10,000円相当のPayPayポ...	Paypay <jna@costcojapan.jp>	2024/10/15 6:24
SAISONカードの利用状況確認のお願い	セゾンカード <siasnocard.co.jp-custom.account@...	2024/10/15 6:45

カ

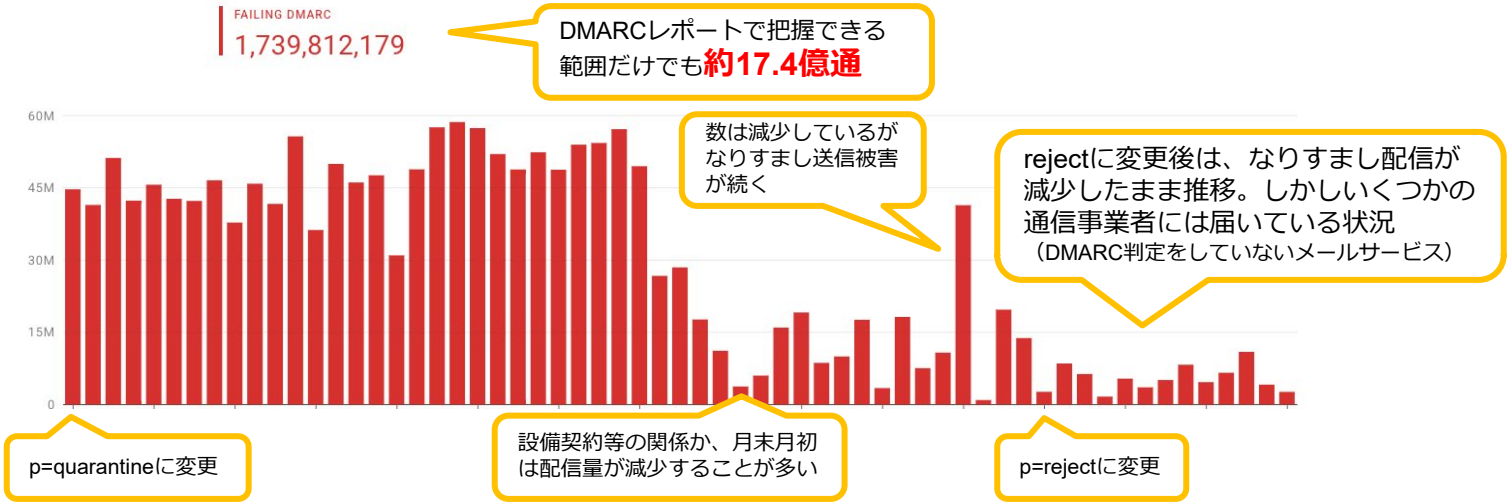
2024年の事例：メールアドレスなりすまし送信の急増

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

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

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

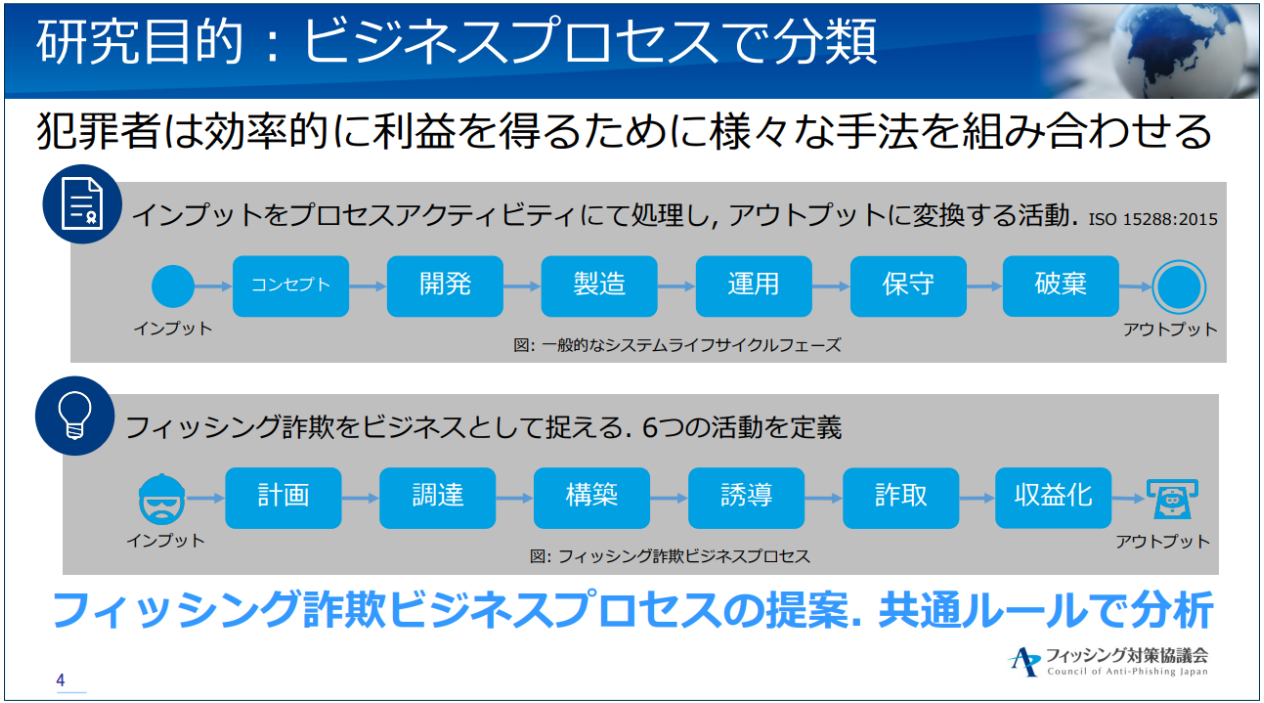
メールマーケティングを行っている事業者にとっては大問題。
落ちた信用はすぐには回復できない



2024年
フィッシング報告からみる対策優先事項

「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、発生する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、SMS等やWebサイトアクセスに対するフィルター、認証強化、通知方法変更など

「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」なのかを分類して実施することで、全体として「被害抑制」などの効果が出る

なりすまし送信とは

- 「なりすまし」送信とは
  - **実在するドメイン名のメールアドレスをかたりメールを送信すること**
  - **サービスの本物のドメイン名のメールアドレスをかたる場合が多い**
- なぜ「なりすまし」をするのか
  - 本物と同じメールアドレスは信用されやすい（見分けがつかない）
  - メールを送るためにドメイン名を登録しなくて良い（コストがかからない）

なりすまし送信 メールメールソフトでの表示例

フィッシングを行う側にとっては成功率が高くなり、コストもかからない
送信ドメイン認証により、正規メールか否か判断する助けとなる

送信ドメイン認証方式の比較

	SPF	DKIM	DMARC
検証方法	正規のサーバー（IPアドレス）から送信されたかを検証	電子署名でメールを検証。S/MIMEはメール本文のみが署名対象だが、DKIMはメール配信時につけられるヘッダー情報やメール本文も署名対象にできる	SPFとDKIMの検証結果を使って検証。SPF＋DMARCなど、片方だけでも可
検証対象	メールソフトで表示されない方のメールアドレス（エンベロープFrom）	署名対象の情報（差出人、日付時刻、受信者などのヘッダー情報およびメール本文）	**メールソフトで表示されるほうのメールアドレスで検証** **（SPF/DKIM の検証対象ドメインと一致しているか比較）**
導入	送信側の設定はSPFレコードをDNSへ登録するだけで容易	S/MIMEと同様に、送信側は各メールへDKIM署名するためのシステムが必要	すでにSPFまたはDKIMが設定されていれば、送信側の設定はDMARCレコードをDNSへ登録するだけで容易
利点	受信時に検証を行っている事業者が多い（しかし多くはfailしても素通し）	**メールを転送されても検証可能**	SPFのみでは誤判定される なりすまし送信を検出できる ドメイン管理者側が、検証失敗したメールの扱いを指定できる（迷惑メールフォルダーへ配信、拒否等のポリシーを宣言） 受信側から送られるDMARCレポートで、検証結果や効果を確認できる **Gmail、Yahoo!メール、ドコモメール、Apple iCloudメール、au/KDDI、楽天モバイル、Outlook.comなどが対応済。モバイルユーザー向けのカバー率は高く、主要なオンラインサービス利用者の半数～7割程度をカバー**
欠点	単体ではエンベロープFromに独自ドメインを使用して、SPF の検証をpass（回避）するなりすまし送信は検出できない	署名に使うドメインを指定できるため、単体では検証を回避可能	日本国内のISP (プロバイダーのメールサービス) は受信側対応が遅れている

2024年の事例：月額利用通知

■ 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

先日、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

2023年の出来事：本物の注意喚起がフィッシングとして報告された

- **【重要・緊急】入出金を規制しました――“詐欺っぽい”三井住友銀行のメールが話題　一体なぜ？経緯を聞いた（ITmedia）** https://www.itmedia.co.jp/news/articles/2308/30/news163.html

「【重要・緊急】入出金を規制させていただきました...などのメールは詐欺です」――そんな件名のメールが話題になっている。一見すると詐欺メールのように見えるが、送り主は、本物の三井住友銀行だ。

- フィッシング対策協議会には、本物の注意喚起メールがフィッシングとして報告されました

送信日時：2023年8月8日
差出人：三井住友銀行 <smbc_info@msg.smbc.co.jp>
件名：【重要】ショートメッセージ(SMS)の確認コードしか見ないのは大変危険です！
報告件数：**約21件**

送信日時：2023年8月30日
差出人：三井住友銀行 <smbc_info@msg.smbc.co.jp>
件名：【重要・緊急】入出金を規制させていただきました...などのメールは詐欺です
報告件数：**約22件**、件名に [meiwaku] が付加されたものは3件

いずれも
- S/MIME署名あり
- DMARC pass
- SPF/DKIM pass

正規メールとしては完璧な、申し分ないメール。しかし、受信者は正規メールかどうかを認識できていない

ここ数年、偽メールは見分けられない、と啓発してきたが、それでは正規メールも疑うしかない。利用者にメールを送る必要がある以上、「正規メールと証明されたメールがある」という啓発が必要。現状、啓発すべき点は以下の2点

・送信ドメイン認証によって正規メールと検証できたメールの見分けかた

・セキュアなメールサービスを使用する

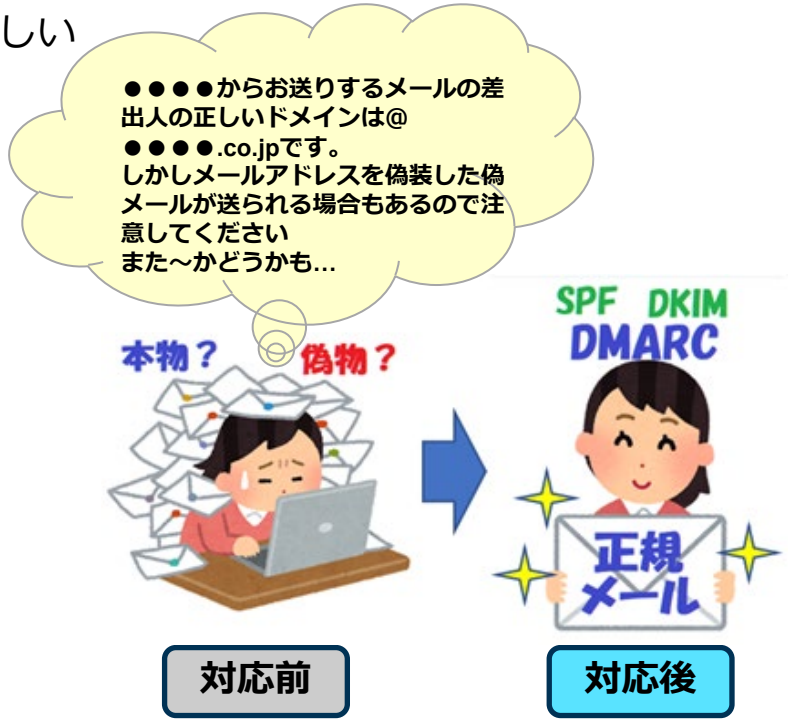
正規メール視認性向上の取り組み（BIMI）

- 利用者にとって必要なのは、正規メールかどう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

Gmailで表示したBIMI

対応後

対応前



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？

- GmailのメールボックスをGmailアプリで見てみたら、BIMI対応ブランドが増えていました

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ほうが良い

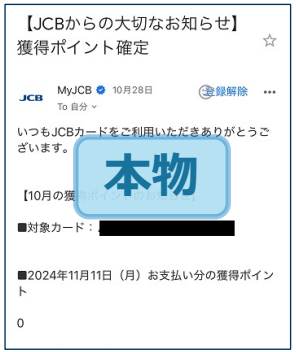
ブランドロゴが表示されていると、目立つし安心感を与える

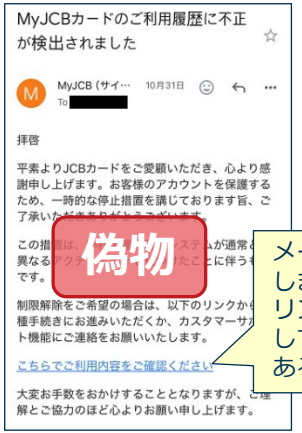
利用者にはこのロゴ表示の情報だけで大事なこと（このメールは安全）が十分に伝わる

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

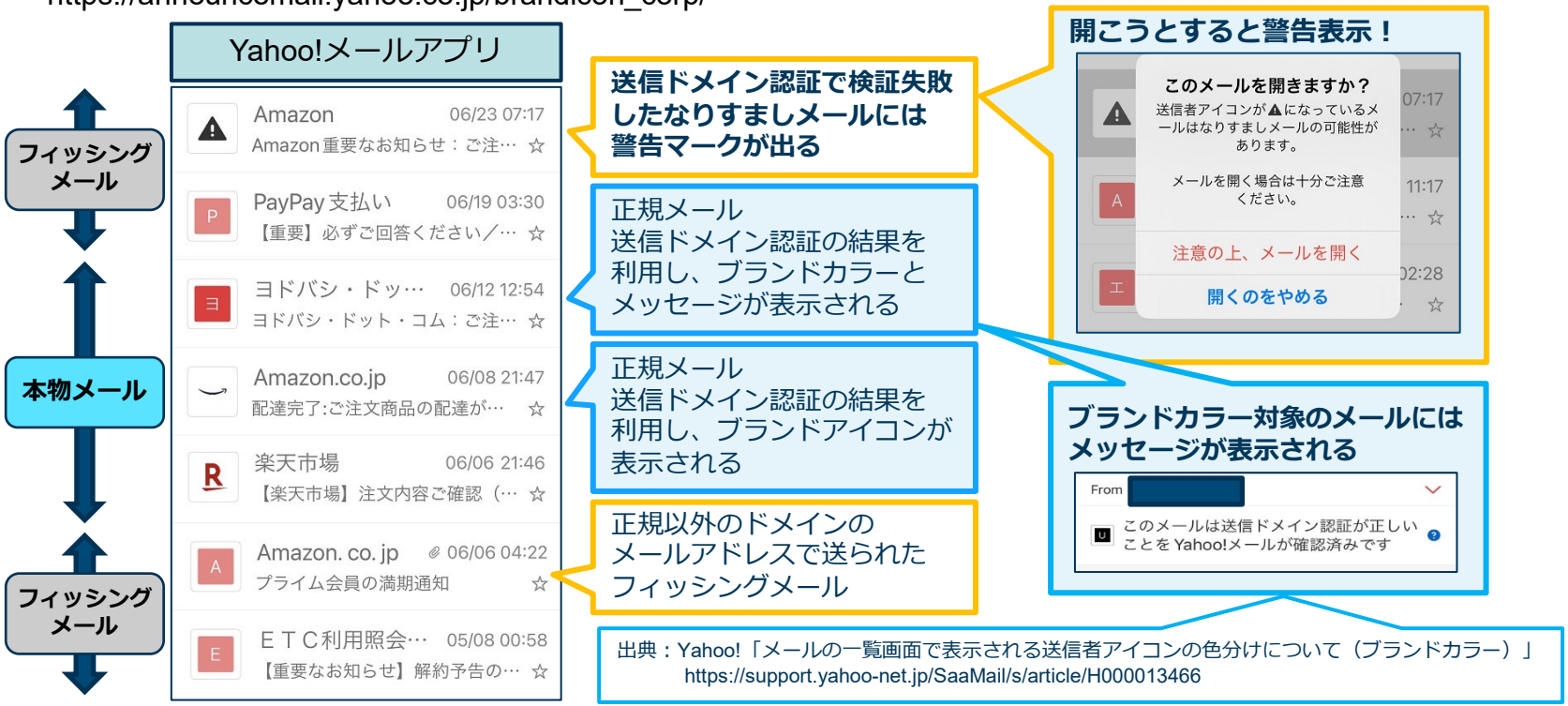




メール本文を見てしまうと惑わされ、リンクへアクセスしてしまう恐れがある

正規メール視認性向上の取り組み（Yahoo!メール）

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



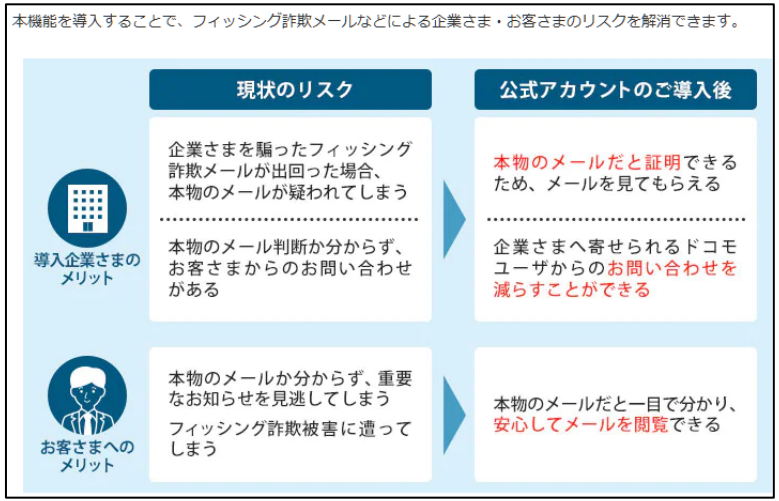
出典：Yahoo!「メールの一覧画面で表示される送信者アイコンの色分けについて（ブランドカラー）」
https://support.yahoo-net.jp/SaaMail/s/article/H000013466

正規メール視認性向上の取り組み（NTTドコモ）

- ドコモ公式アカウント

  https://www.ntt.com/business/services/official_account.html

  送信ドメイン認証 （SPFまたはDMARC）をpassしたメールにマークを表示する機能



ドコモメールアプリ、Webメールで表示対応（標準機能）

銀行、クレジットカード系など、主にフィッシング対策に力を入れている事業者（サービス）が対応している

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**

2024年に急増した、なりすまし送信被害によるドメイン名毀損への対策は、現状、これが最善案と思われる

今後スマホデビューしたAndroidスマートフォンユーザーはGmailメールアドレスを、iPhoneユーザーはiCloudメールを新たに作って利用することが予想される（それぞれスマホOSのデフォルト、どちらもBIMI対応済）

対応済の国内キャリアメールもあり、今後、モバイル環境を中心にBIMI対応が進むと思われる

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」

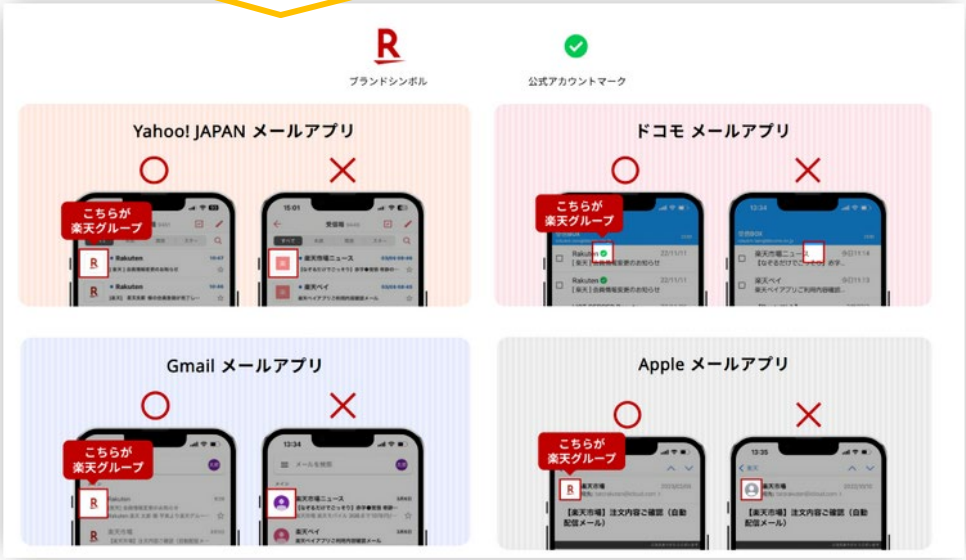


図 2　送信ドメイン認証をパスした正規メールの表示例

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

フィッシングメールへの対策

- 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**
  - メール転送していないメールアドレスの使用（届かない可能性があるため）
  - 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）**

フィッシング対策協議会へも
情報提供（報告）お願いします

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。
フィッシングメールが大量に届くのは、**メールアドレスが広く漏えいしている**ことを意味する。
同時に他の個人情報やパスワードも漏えいしている可能性があるため、**メールアドレスを変更**し、被害に遭うリスクを減らす。**受信者の名前をメール文に記載したフィッシングメールも確認されており、実際に漏えいデータを使った**可能性が高い

フィッシングサイトへの対応

- URLフィルタリング
  - 各事業者での監視による、URLフィルターへの早期登録を推奨
  - **Googleセーフブラウジングへ登録するとカバー率が高い**
    https://safebrowsing.google.com/safebrowsing/report_phish/?hl=ja
    APIでの登録は、WebRisk API（有償）がある

Chrome、Safari、Firefoxがこのデータで検知、ブロック
モバイルはほぼカバー

- フィッシングサイトのサイト閉鎖調整（テイクダウン）
  - 各事業者から直接ホスティング事業者等へのサイト閉鎖依頼を推奨

JC3さまのお話やこの後のセッション、「C11 最速低コストなテイクダウンリクエスト送受の最新動向」で詳しく聞けると思います

- 検知サービス
  - 早期にURLフィルタリングへの登録、サイト閉鎖調整を行えるため、被害抑制に効果が期待できる
  - 組織内に専門の人員や設備がなくても、迅速な対応が可能
  - 大量URL生成タイプのフィッシングのターゲットになると費用がかさむので、契約時にその場合の対応について確認しておく

現在、さまざまな組織が、並列的に対応を行っている部分もある
しかしフィッシングの案件数が激増した今、特に人手での作業が伴う対応は、重複しないよう、整理と連携で迅速な対応を目指す時にきている

フィッシング対策ガイドライン

フィッシングは世の中の状況にあわせて常に変化し進化しているため、フィッシング対策協議会では毎年、内容を精査し、改訂版を公開（最新版は2024年6月公開）

- **フィッシング対策ガイドライン**
  https://www.antiphishing.jp/report/guideline/antiphishing_guideline2024.html

  Webサイト運営者向けの対策ガイドライン

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

- **利用者向けフィッシング詐欺対策ガイドライン**
  https://www.antiphishing.jp/report/guideline/consumer_guideline2024.html

  一般利用者（消費者）向けの対策ガイドライン

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

被害に遭わないために心がけること

- 急かされるような文面でも慌てない。メール、SMSのリンクからはアクセスしない
- お気に入り（ブックマーク）、正規アプリを利用して、正規サイトにアクセスする
- カード情報、口座情報、暗証番号、認証コード等の入力を求められたら一度立ち止まる
- 怪しいと思ったら「件名」「本文」内の文字列で検索したり、サポート窓口へ確認
- セキュリティ機能を活用する（迷惑メールフィルター、多要素認証の併用）
- メールアドレス、同一パスワード変更 （漏えい情報の再利用防止、配信リスト無効化）

特に黄枠の2つは知られてしまった情報（メールアドレス、個人情報、認証情報など）の不正利用、再利用を防ぐ

最後に

インターネットを経由した犯罪は、いまや誰でも遭遇し、被害に遭う可能性がある身近な脅威です

みなさまからの情報提供は、ひとつひとつはとても小さな点であり、対応を行う側も、そのすべてに対応することもできません

でも点が集まると線になり、面となり、詰みあがると、いつか犯罪者検挙へ繋がるかもしれません

例えばご家族やお友達へフィッシングに注意するよう話をしたり、安心なメール環境を使うようお勧めすることも小さな一歩かと思います

それぞれの立場で、できることを行って、互いに協力しあって、安全なインターネット環境を作っていければ幸いです

以上、ご参考になりましたら幸いです