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

フィッシング対策セミナー2024
最近のフィッシング報告動向

フィッシング対策協議会事務局（JPCERT/CC)
事務局長 吉岡道明, CISSP

フィッシング対策協議会について

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

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
目的として活動している任意団体です。

名称	フィッシング対策協議会／Council of Anti-Phishing Japan	
設立年月日	2005年4月28日	
会長	岡村 久道	
運営委員長	加藤 孝浩（TOPPANエッジ株式会社）	
運営副委員長	唐沢 勇輔（Japan Digital Design 株式会社／ソースネクスト株式会社）	
会員数	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
		全134組織
		（2024年10月時点）
事務局	一般社団法人JPCERTコーディネーションセンター	

協議会の活動

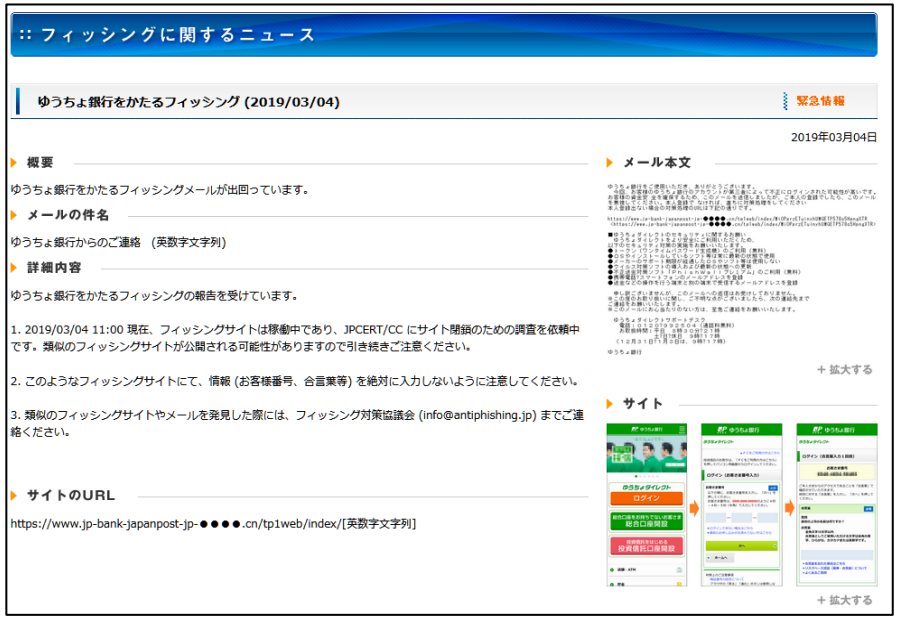
URLフィルタリングを行っている
セキュリティベンダー、事業者へURL共有

フィッシング対策協議会 情報発信

■緊急情報

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

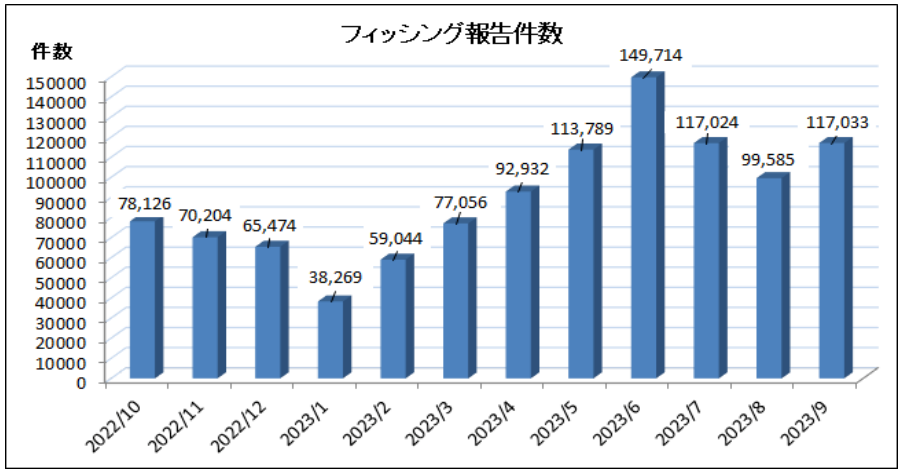
一般への影響度が高い（報告が多い、ユーザー数が多い）フィッシングのメール文面とサイト画像を掲載



■月次報告書

https://www.antiphishing.jp/report/monthly/

—フィッシング、URL、ブランドの件数を掲載
—1カ月分のデータを集計
—その月の傾向など、最新情報のサマリーを掲載

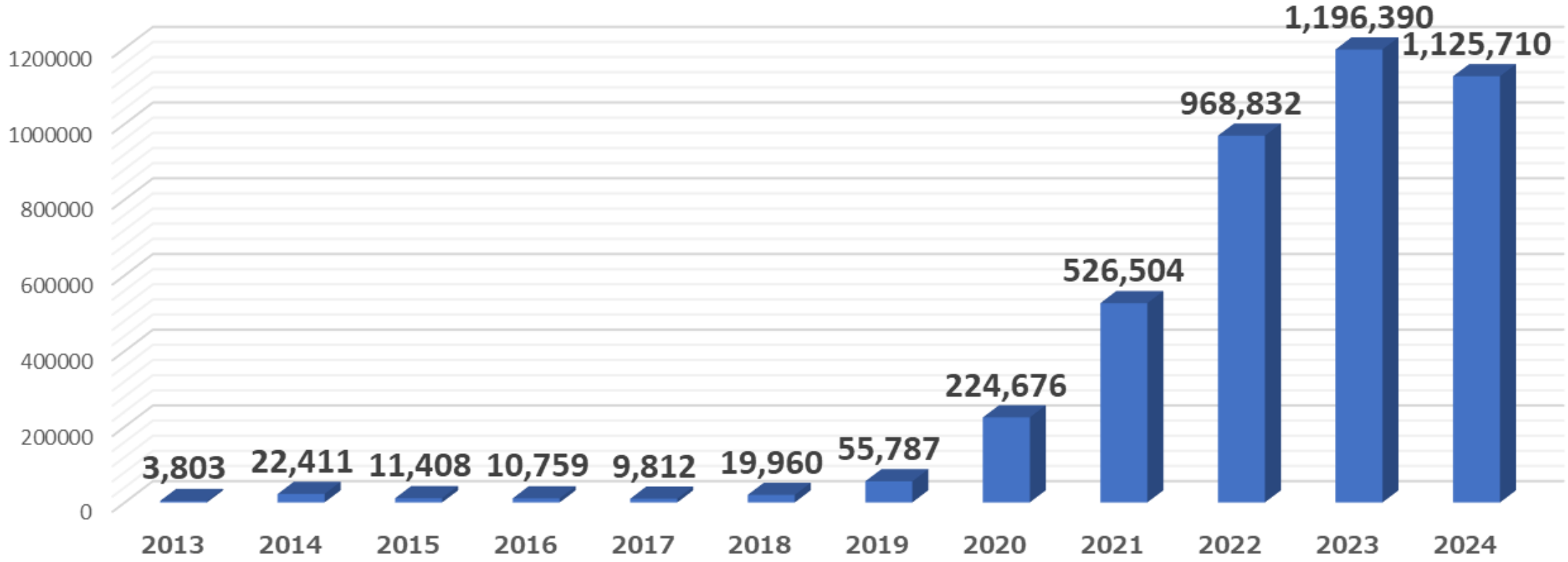


フィッシング対策協議会
Council of Anti-Phishing Japan

フィッシング報告受付状況

フィッシング報告状況（年別）

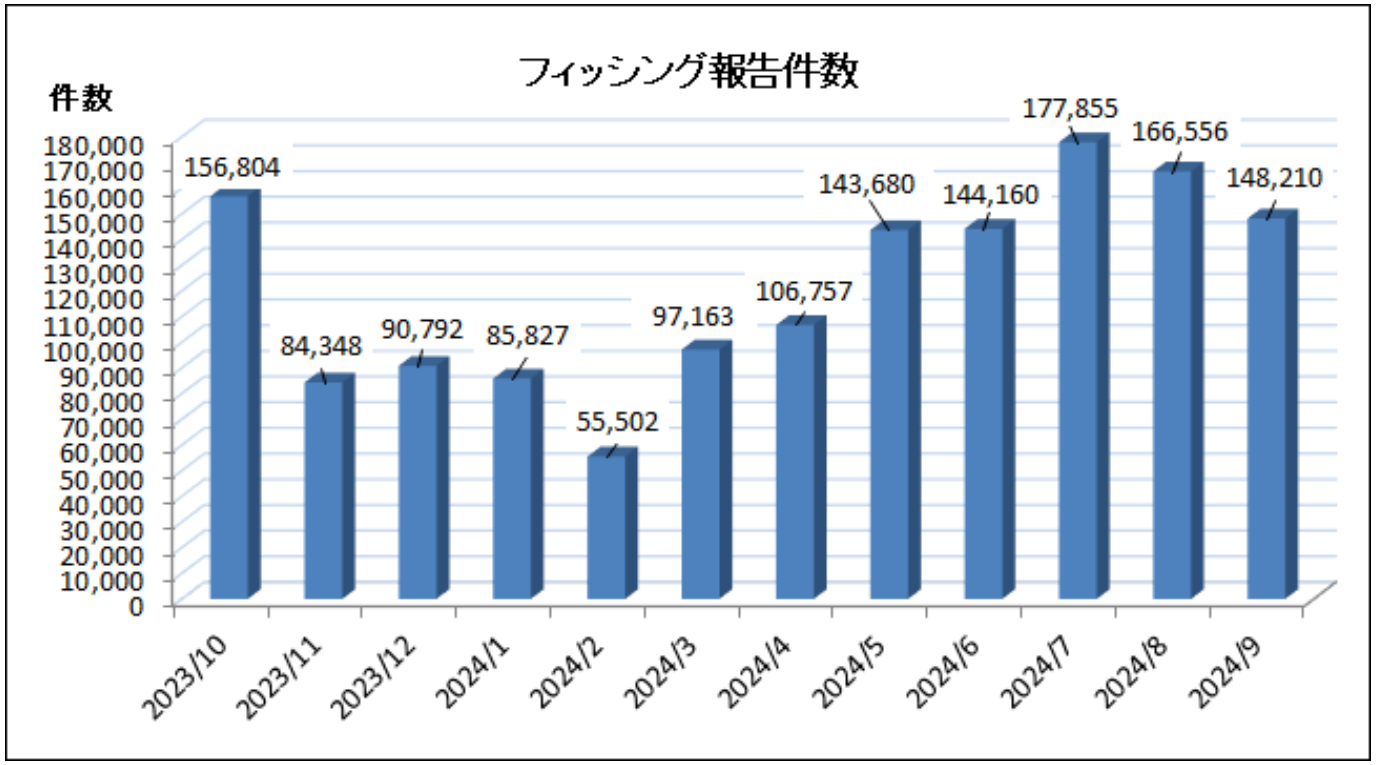
- 報告件数は2020年以降急増
- 過去最高の報告件数を毎年更新。2024年も引き続き多い（2024年9月時点）
- フィッシング詐欺の認知度向上も影響



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

フィッシング報告状況2024

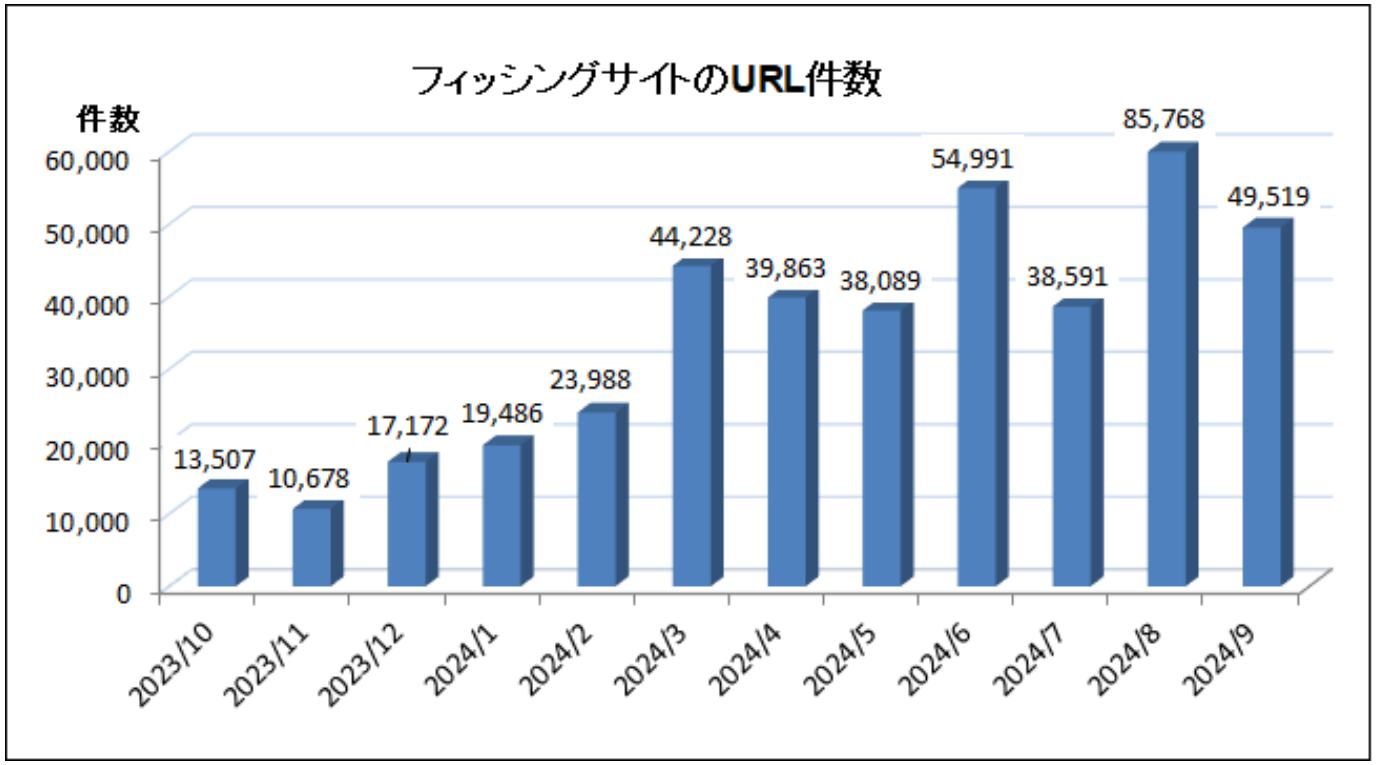
- 5月以降、フィッシングメール配信数が急増
- 連動して報告件数も急増し、7月には過去最高値
- 宛先メールサービスごとに発信元メールアドレスを「なりすまし」「独自ドメイン名」で使い分け、フィルター条件をすりぬけて大量に着信している



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

フィッシング報告状況2024

- 3月から6月はURL件数が急増、8月は過去最高値
- 6月から8月はランダムサブドメイン名＋独自ドメイン名、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
- 大量配信系のフィッシングサイトはクラウドサービスの bot 対策機能でモバイル回線、モバイル端末（UA）からのアクセスのみを通すよう設定

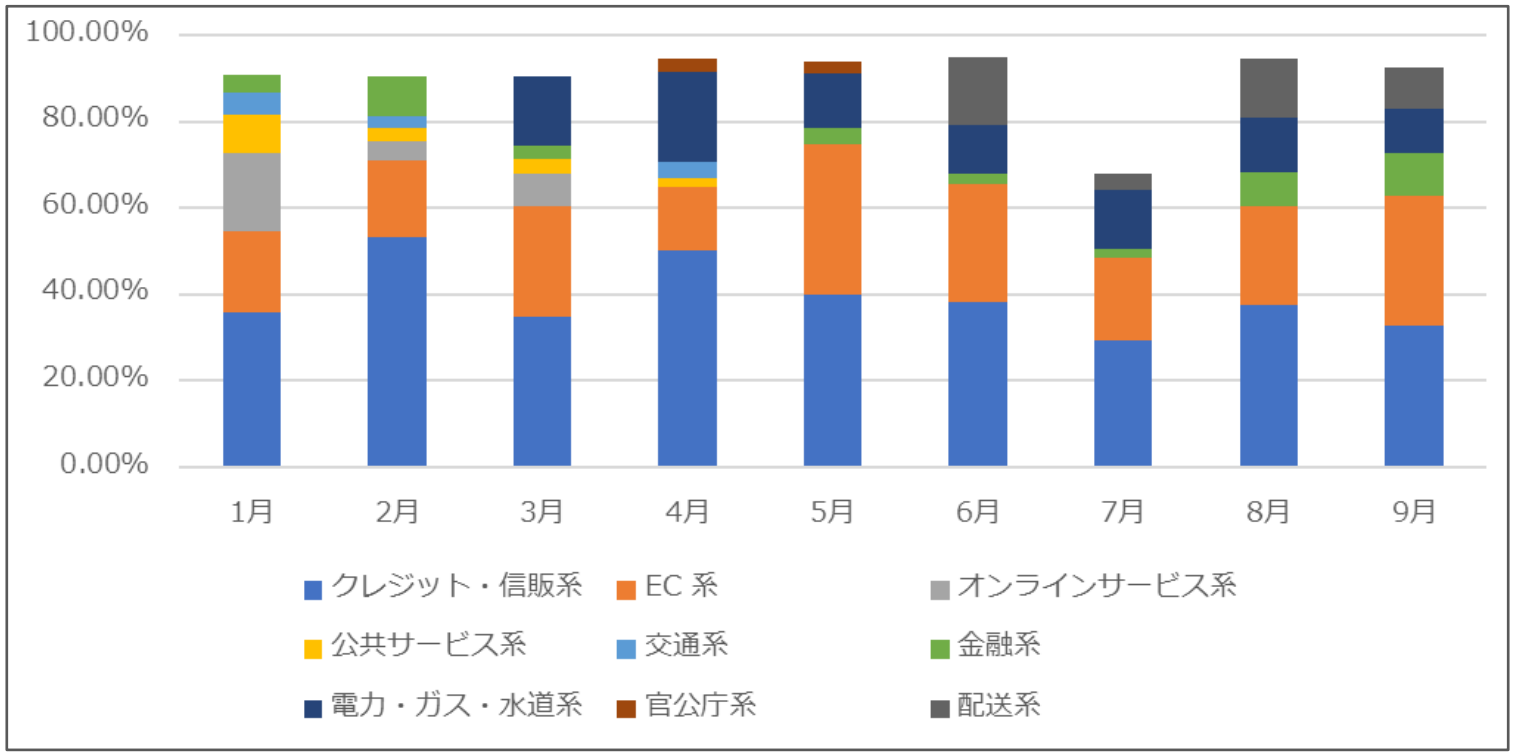


出典：フィッシング対策協議会「2024/09 フィッシング報告状況」https://www.antiphishing.jp/report/monthly/202409.html

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

フィッシング報告の推移（分野別）

- クレジットカードを利用できるサービスであり、ユーザーが多ければ狙われる可能性がある
- 引き続きさまざまなブランドが使用されている
- メガバンク⇒インターネットバンキング⇒地銀⇒労金と幅広くかたられている



出典：フィッシング対策協議会「月次報告書」からグラフ化　https://www.antiphishing.jp/report/monthly/

フィッシングの事例

2023年～2024年の事例：URLに飾り文字などが含まれたフィッシング

本日、お客様宛にお荷物のお届けにお伺いいたしましたが、
ご不在のため配達を完了することができませんでした。
誠に申し訳ございません。

【お荷物情報】

＊お問い合わせ番号：2462-4625-1542
＊サービス名：宅急便
＊保管営業所：ヤマト運輸センター
＊保管期限：10/14/2024まで

【ご対応のお願い】

以下の方法で再配達のご依頼をお願いいたします。

オンラインで再配達を依頼する
<https://zrxkadimsrje.com/POKJOWLREZjxIQDTvP/KPxqVcDDLReWJVgSjDdAjCM/mEMFbDBlTyEoCHUpBaLKvsE@zrxkadimsrje.qijitu.cn/caonima=XhHGLvPxbceCffnaFTPHDLxE.co.jp/>

また、玄関先などでの「置き配」も承っております。
再配達のご依頼時にお申し付けください。

お客様のご都合の良い時間帯に、確実にお届けできるよう
努めてまいります。

- 2023年10月末頃から、迷惑メールフィルター回避が目的と思われる、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として認識され、アクセスできてしまう
- 単純にフィルターだけが目的なら、Unicodeが含まれたURLは不正である可能性が高い、というスコアリングをすれば良さそう

2024年10月12日配信のメール

メール内に記載されたURL

<https://zrxkadimsrje.com/POKJOWLREZjxIQDTvP/KPxqVcDDLReWJVgSjDdAjCM/mEMFbDBlTyEoCHUpBaLKvsE@zrxkadimsrje.qijitu.cn/caonima=XhHGLvPxbceCfaFTPHDLxE.co.jp/>

ブラウザーに認識されるURL

https://zrxkadimsrje.qijitu.cn/caonima=XhHGLvPxbceCfaFTPHDLxE.co.jp/

2024年10月現在も、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：メール本文やURLに、ゴミ文字やUnicode文字を混ぜる

■ 2024年10月現在も、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

メール内の表記

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

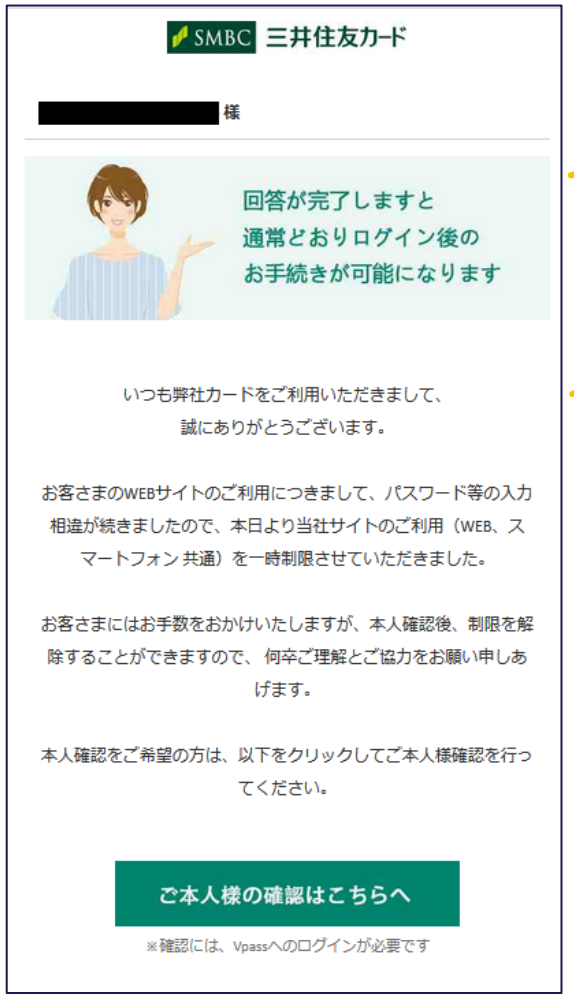
メーラーの認識

- **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
- 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：メール本文やURLに、ゴミ文字やUnicode文字を混ぜる

■ 2024年10月現在も、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



出典：フィッシング対策協議会

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


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

メールアドレスなりすまし送信の現状

- **2024年6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**
- **送信元のIPアドレスは以下が多い**
  - **China Telecom**
  - **China Unicom**
  - **IPアドレス貸し事業者**
- 同じドメイン名のメールアドレスになりすまし、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
- 同じドメイン名のメールアドレスになりすまし、迷惑メールも送信されている
- 「なりすまし」「非なりすまし」「送信元事業者」「IPv4/IPv6」を切り替えながら、到達率の良い方法で送ってくる

「URLパターンや文面の特徴がいくつかに分かれる」「迷惑メールも配信している」などから、到達率を調査し高めている不正メール配信専門サービスがあると考えられる。各犯罪者（グループ）はメール配信にそういったサービスを使うようになってきている可能性がある。

件名	通信相手	送信日時
【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

フィッシング対策について

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、毎年内容を精査し、改訂版を公開（最新版は2024年6月8日公開）

■改訂内容
使いやすさや読みやすさを向上させ、より役立つものになるように全体的な更新を行いました
◇ コンテンツへの動線の見直し。基本的な概念の説明や用語集を付録に移動
◇ 情勢の変化を受けた項目削除
◇ 要件を示す内容とその実施方法を示す内容とを分別
◇ 付録にフィッシング対策チェックリストの追加
◇ その他、最新情報へのアップデート

■ フィッシング対策ガイドライン

https://www.antiphishing.jp/report/guideline/antiphishing_guideline2023.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を、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_guideline2023.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し、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を、ガイドラインとして整理

フィッシング対策ガイドライン重要5項目

1. 利用者に送信するメールでは送信者を確認できるような送信ドメイン認証技術等を利用すること

2. 利用者に送信する SMS においてはなりすましが起きにくいサービス（国内で直接接続される送信サービス）を利用し、発信者番号を利用者に告知すること

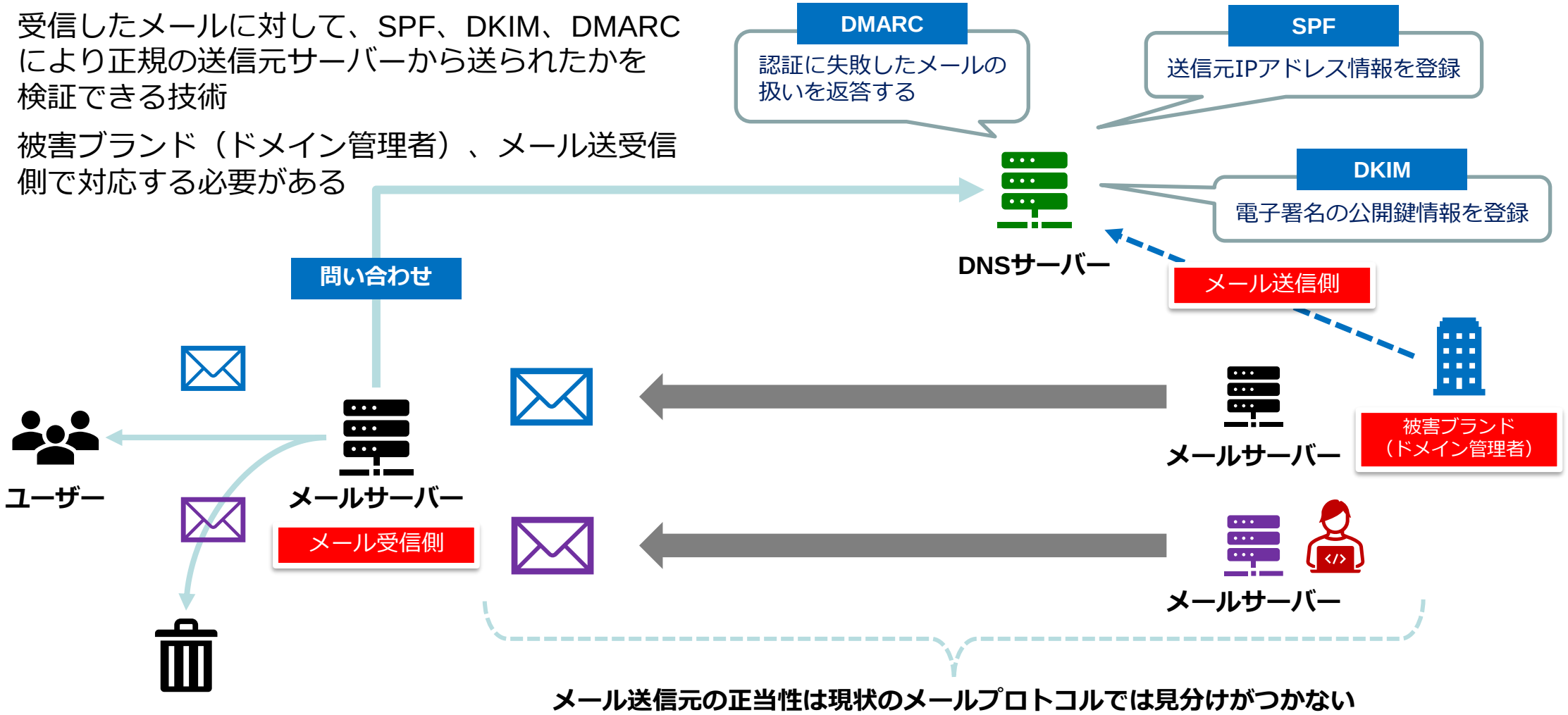
3. 複数要素認証を要求すること

4. ドメイン名は自己ブランドと認識して管理し、利用者に周知すること

5. フィッシング詐欺について利用者に注意喚起すること

なりすまし送信メール対策：送信ドメイン認証

- **正規ドメインの差出人メールアドレスで詐称したなりすまし送信メールに有効**
- 受信したメールに対して、SPF、DKIM、DMARCにより正規の送信元サーバーから送られたかを検証できる技術
- 被害ブランド（ドメイン管理者）、メール送受信側で対応する必要がある

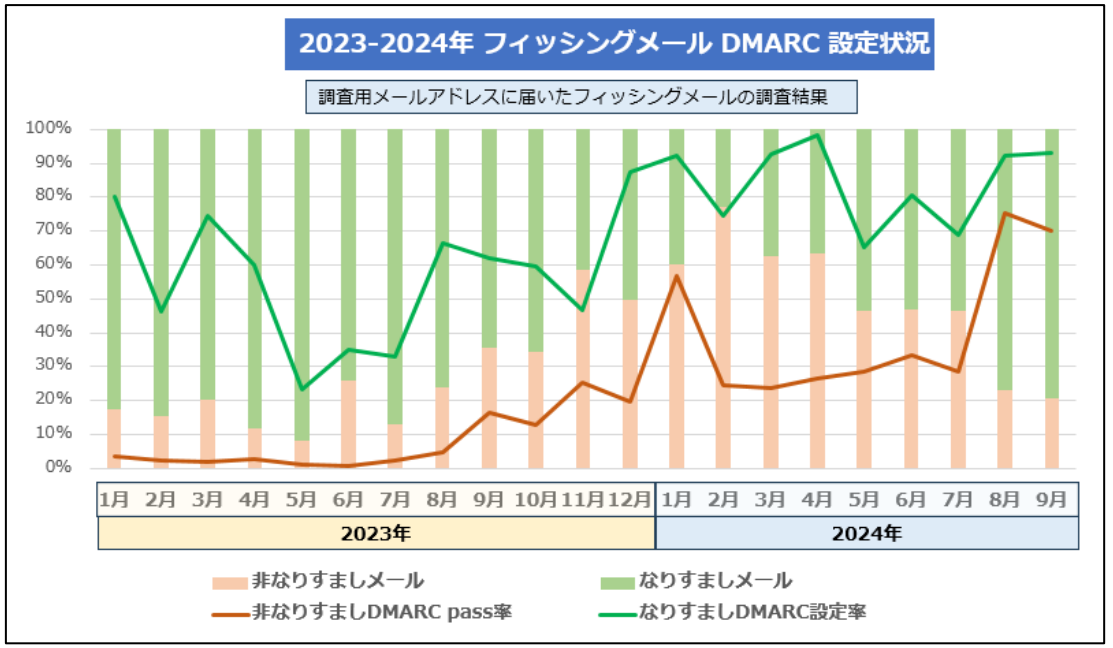


なりすましフィッシングメールとDMARC対応状況

報告が多いメールサービスと少ないメールサービスには差がある

- **2024年5月以降、なりすましメールが増加。不正メール配信量も激増**
  迷惑メールフィルター機能が弱い国内事業者メールサービス利用者からの報告が増える
  → なりすましメールが素通りすることが判り、迷惑メールフィルター回避率が高いと認識された？
- **2024年7月以降、なりすましが急増、素通りするメールサービス利用者からの報告割合が増えた（要改善）**
- **宛先メールサービスごとに送信元メールアドレスを「なりすまし」「独自ドメイン名」で使い分け、フィルター条件をすりぬけて大量に着信している（ホワイトドメインではなく、DMARCの結果を優先すべき）**

2024年	1月	2月	3月	4月	5月	6月	7月	8月	9月
DMARC Enforce	33.6%	10.9%	8.5%	12.9%	26.7%	30.6%	20.0%	63.5%	66.7%
DMARC p=none	3.1%	6.2%	69.8%	63.0%	8.1%	12.3%	16.8%	7.6%	6.8%
DMARC なし	3.1%	5.8%	7.4%	1.8%	18.6%	10.4%	16.6%	6.0%	5.7%
	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	39.9%	22.8%	37.4%	36.7%	53.4%	53.3%	53.4%	77.1%	79.2%
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%
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%
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%



報告が多いメールサービスの特徴

- **DMARC受信側検証をしていない（p=rejectでも素通し）**
- **迷惑メールフィルター判定条件を読まれ、回避されて素通り**
- **フィードバックを受けていない（機能が強化されない）**
- **特定のドメイン名は無条件に素通し（ホワイトリスト）**

DMARC普及における課題

- Gmail送信者ガイドライン等のおかげで送信者側のDMARC普及率は上がったが、フィッシングメール（迷惑メール）はまったく減っておらず、さらに、**なりすまし送信が増加**している状況
- **正規メールの不達**を気にするあまり、受信側で正しく検証、ポリシーに従った処理をしていないメールサービスがある（これでは意味がない）
- 受信側で正規メールの検証失敗やエラーを考慮して、**メールを素通し**してしまう
  - 意図しない結果になるのは、通常、送信側の設定に問題が発生しているケースが多い
  - 検証失敗は問題を明確にする効果があり、送信側にとっても誤設定の早期発見に役立つ
  - 重要なメールであれば、送信側が再送信すれば済む話
  - 問題があるメールを素通しするほうが大問題
- 検証結果を利用者に通知できていないため、**p=none/quarantineで受信したメールを確認できない**

・DMARCの普及が目的（ゴール）ではない。「効果を出す」ことが目的

・p=none/quarantineでは効果はないので、p=rejectでの運用の必要性を十分に啓発する

・受信側でポリシーに従った配送、および認証結果の表示が必要

送信ドメイン認証技術による認証結果の表示

- 正規のものと判定されたメールをBIMIやブランドアイコン表示することで通知
- BIMI等に対応できなくても、件名に[DMARC fail]などを追記することでも良い
- 重要なのは、**利用者が判断するための情報を提供**すること

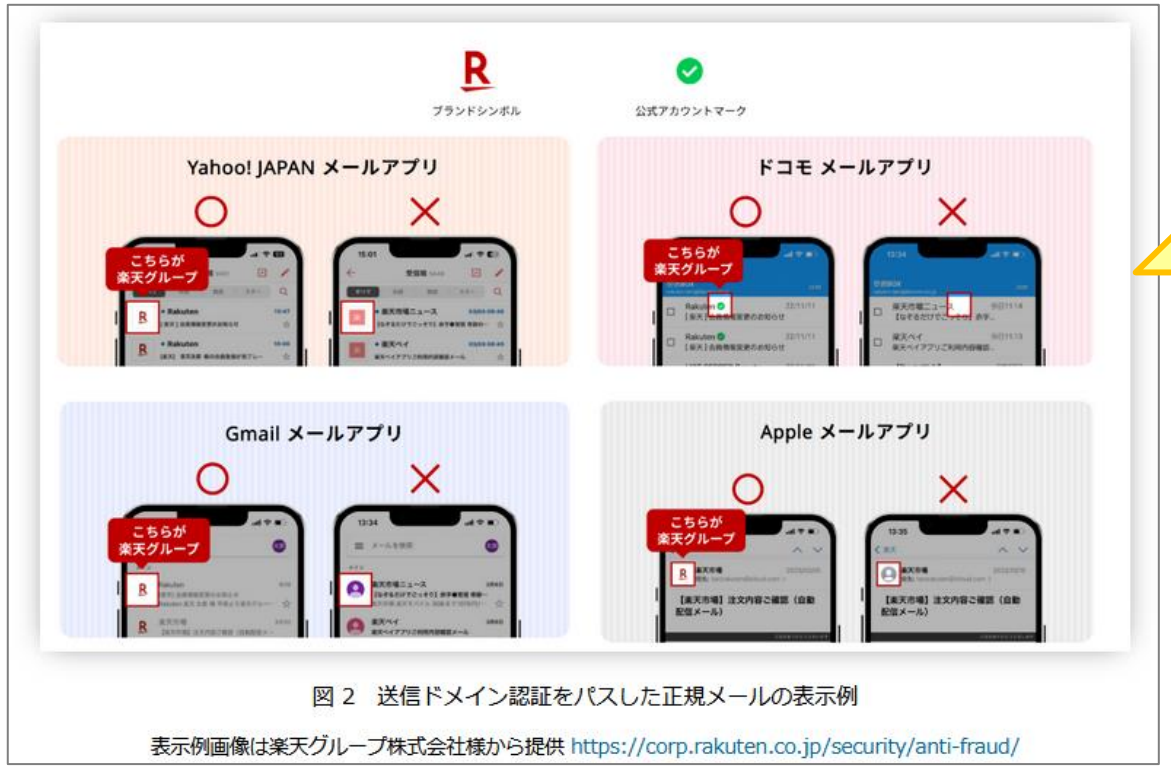


図 2　送信ドメイン認証をパスした正規メールの表示例

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/

とにもかくにも正規メールである と利用者が判別できるかが重要

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

DMARC対応 日本の国としての方向性

- 犯罪対策閣僚会議
  - 令和6年6月18日 決定事項
    https://www.kantei.go.jp/jp/singi/hanzai/index.html

受信側の対応も求められている
届かない＝rejectは受信者へ配信しない！

(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。

- 犯罪対策閣僚会議における決定事項は、非常に重要であり、実施を行ったかどうかを求められる。
  総務省主導で国内通信事業者のメールサービスは、このリクエストに応えてくれていくと期待

利用者へのアドバイス

- 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）
- 迷惑メールフィルターが強力、送信ドメイン認証技術に対応しているメールサービスを選択する

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、再利用を防ぐため、利用者側で行える対策

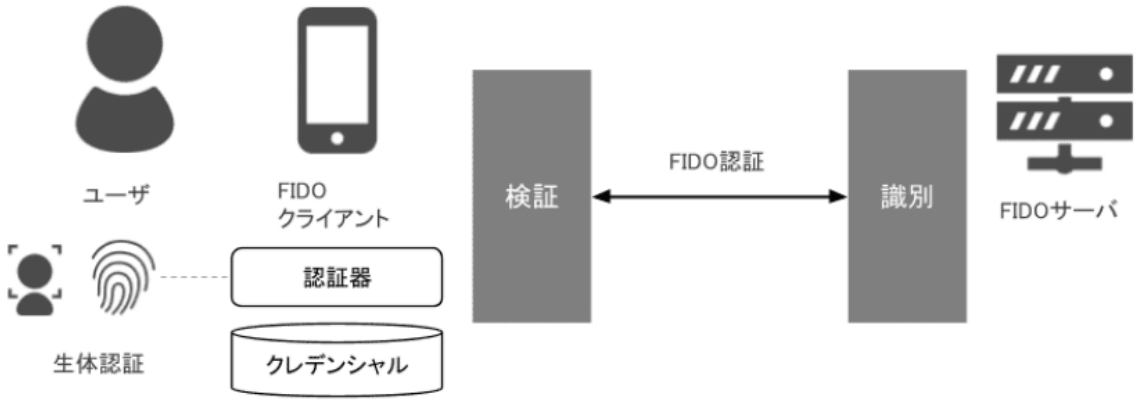
その他の対策について FIDO／Passkey

これまでクレジットカード情報の保護対策

- PCI-DSS準拠
- 加盟店サイトでは決済代行システムを利用　**フィッシング詐欺による不正ログイン**
- 3Dセキュアの普及　**リアルタイムフィッシングによる被害**

FIDO/Passkey

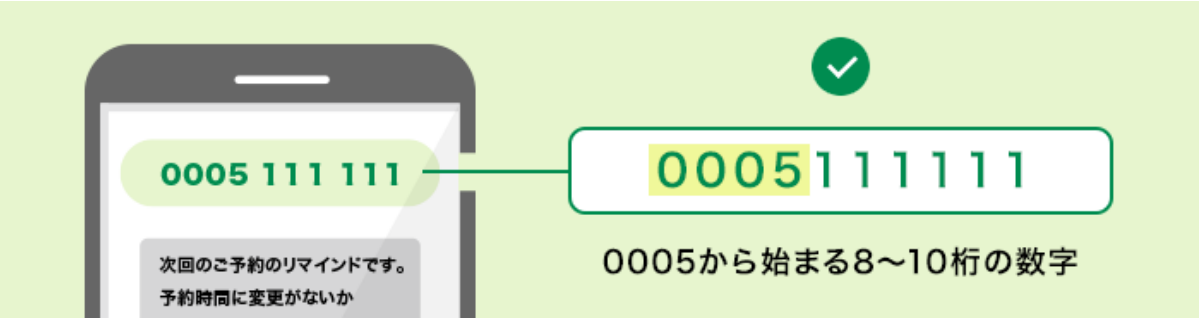
- 認証にパスワードを使用しないパスワードレスの技術
- パスキーと呼ばれるオンライン認証の仕組みで、スマートフォンなどの生体認証を使用して個人認証が可能
- 公開鍵方式を採用し、認証情報であるクレデンシャル端末内で安全に管理され、セキュリティリスクを低減
- 正規ドメインでないサイトからのアクセスを防ぐことが可能となり、パスワードに起因するフィッシング被害を防ぐ



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

その他の対策について SMS送信元表示名 共通番号

- ドコモ、KDDI、ソフトバンク、楽天モバイルの携帯キャリア4社が企業単位で審査・発行する「0005」から始まる8～10桁
- 重複のない番号で**なりすまし防止**
- 携帯キャリア4社で共通の番号のため**正規メッセージを判別し易い**



出典：NTTドコモ「携帯キャリア4社が発行しているSMSの送信元表示名」
https://www.docomo.ne.jp/service/sms/displayname/

ご清聴ありがとうございました

フィッシング対策協議会
@antiphishing_jp
フィッシング対策協議会は2005年4月に発足いたしました。海外、特に米国を中心として大きな被害を生んでいるフィッシング詐欺に関する事例情報、技術情報の収集及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しております。
http://www.antiphishing.jp/

- フィッシング対策協議会 事務局（JPCERT/CC内）
  - Email：antiphishing-sec@jpcert.or.jp