2023年11月6日
JPAAWG 6th General Meeting

2023年版
フィッシングの現状と対策

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

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 131組織**（2023年10月時点）
    （正会員：103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

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**

参考資料：フィッシング対策協議会 情報発信

- 緊急情報（事例掲載）

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

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

フィッシングの最新事例を掲載！

いつもAmazon.co.jpをご利用いただき、ありがとうございます。
弊社ではお客様のアカウントの安全性を最優先に考え、
アカウント情報の定期的な更新をお願いしております。
ご利用のアカウントについて、更新が必要な情報があります。
アカウント情報を更新しない場合、アカウントの制限がかかる可能性がございます。
下記のリンクより、アカウント情報の更新をお願いいたします。

https://ft3●●●●.NET/?loginid=●●●●

□の部分のリンク
<https://ft3●●●●.net/?loginid=●●●●>など

更新が完了するまで、一部のサービスの利用が制限される場合がございますので、
お早めに更新を行っていただくようお願いいたします。
何かご不明な点がございましたら、Amazonカスタマーサポートまでお問い合わせください。
引き続き、Amazon.co.jpをご利用いただけますよう、心よりお待ちしております。
敬具
Amazonカスタマーサポート

メール文面の例

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

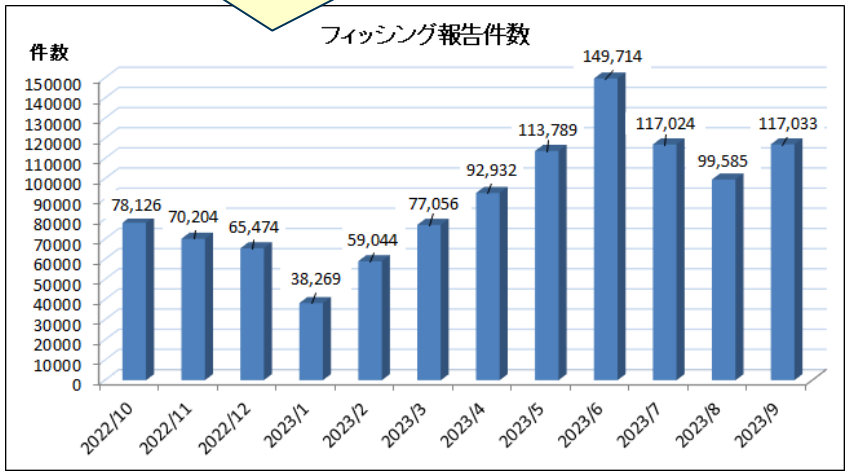
出典：フィッシング対策協議会
マイナポイント事務局をかたるフィッシング (2023/09/11)
https://www.antiphishing.jp/news/alert/myna_20230911.html

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！

2023年9月のフィッシング報告件数は117,033 件となり、2023年8月と比較すると17,448件、約14.9%増加しました。前月に引き続きAmazonをかたるフィッシングの報告が増加しており、報告数全体の約40.8%となりました。次いで報告数が多かったETC利用照会サービス、三井住友カード、Apple、マイナポイント事務局をかたるフィッシングの報告をあわせると、全体の約71.3%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17ブランドあり、これらで全体の約93.8%を占めました。



出典：フィッシング対策協議会「2023/09 フィッシング報告状況」
https://www.antiphishing.jp/report/monthly/202309.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）

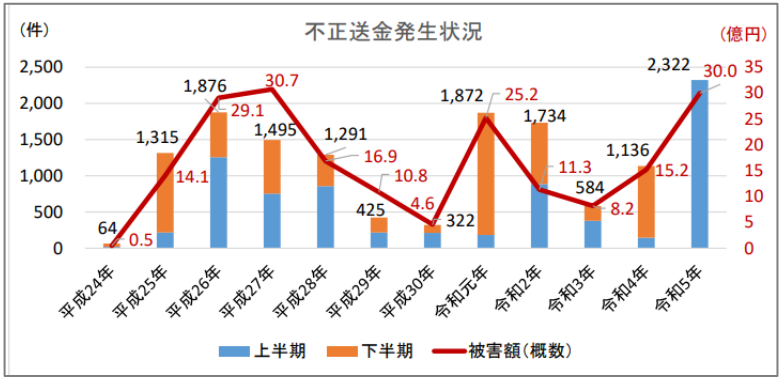
2023年
フィッシングの現状と報告状況

2022年-2023年 不正送金被害増加

■ 2023/08/08：警察庁と金融庁連名の注意喚起

- 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）
  （警察庁）https://www.npa.go.jp/bureau/cyber/pdf/20230808_press.pdf
- 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。
  （金融庁）https://www.fsa.go.jp/ordinary/internet-bank_2.html

令和5年4月にインターネットバンキングに係る不正送金事犯による被害急増に関する注意喚起を実施するとともに、被害金融機関と連携し対策を講じているものの、その後も被害は拡大し続け、8月4日時点において、**令和5年上半期における被害件数は、過去最多の2,322件、被害額も約30.0億円**となっています。
（中略）
被害の多くはフィッシングによるものとみられます。具体的には、**金融機関（銀行）を装ったフィッシングサイト（偽のログインサイト）へ誘導するメールが多数確認**されています。



出典：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）」

2023年1月～8月は、フィッシング対策協議会でも以下の金融系ブランド29件のフィッシング情報を掲載した

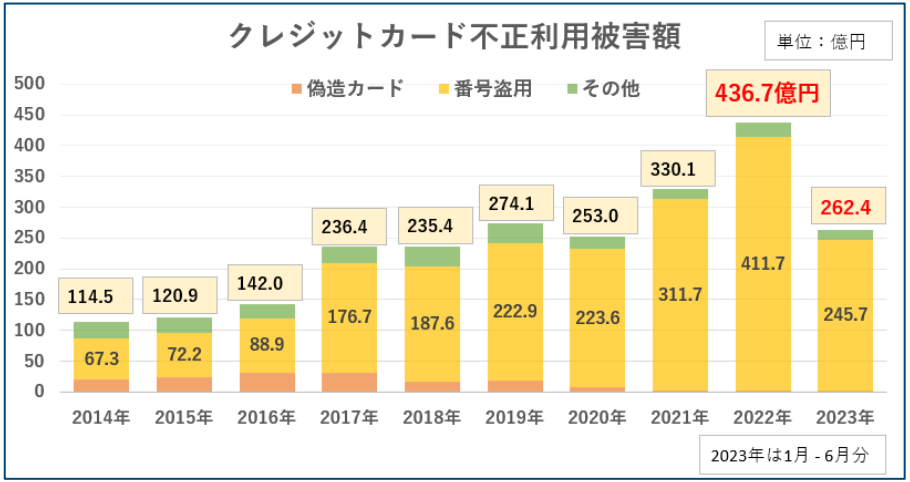
静岡銀行/千葉銀行/イオン銀行/ソニー銀行/SBJ銀行/ローソン銀行/神奈川銀行/GMOあおぞら銀行/三井住友銀行/広島銀行/三井住友信託銀行/PayPay銀行/十八親和銀行/住信SBIネット銀行/三菱UFJ信託銀行/セブン銀行/三井住友信託銀行/auじぶん銀行/大和ネクスト銀行/横浜銀行/りそな銀行/福井銀行/みなと銀行/秋田銀行/北洋銀行/三菱UFJ銀行/西日本シティ銀行/みずほ銀行/楽天銀行

2022年-2023年 クレジットカード不正利用被害額 増加

- クレジットカード不正利用被害額の発生状況（日本クレジット協会)
  https://www.j-credit.or.jp/information/statistics/download/toukei_03_g.pdf
- クレジットカード不正利用被害の集計結果について（ニュースリリース）
  https://www.j-credit.or.jp/information/statistics/download/toukei_03_f.pdf

2022年（通年）の不正利用被害額
436.7億円（前年比32.3%増）
不正利用被害額に占める
◆ 偽造被害額 1.7億円（同13.3%増）
◆ 番号盗用被害額 **411.7億円（同32.1%増）**
◆ その他不正利用被害額 23.3億円（同37.9%増）

2023年の不正利用被害額は、
前年同期間と比較し**27.2%の増加**となっている
2022年1-6月 206.3億円
2023年1-6月 262.4億円
フィッシングメール増加によってカード番号詐取が増加したのが、その主な要因と考えられる



出典：上記発表資料をもとにJPCERT/CCが作成

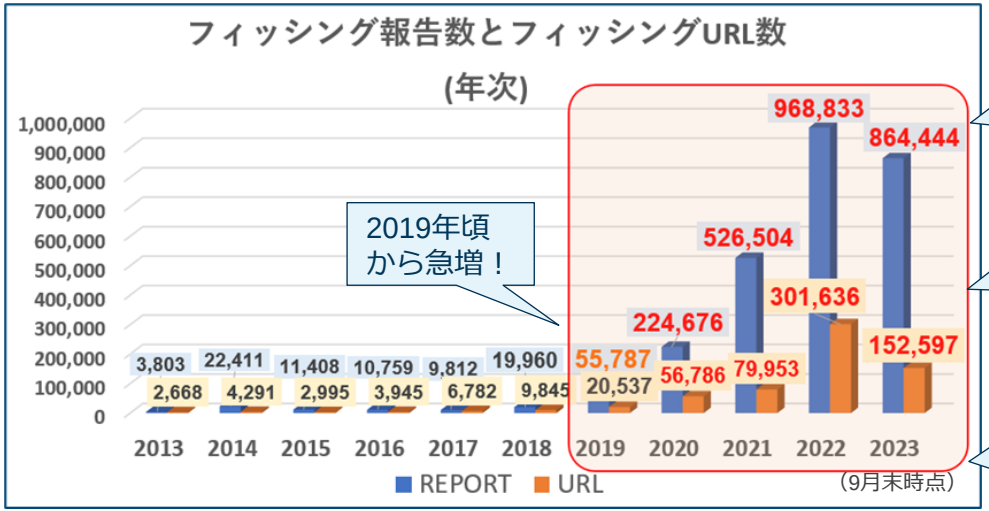
最終的には、EMV 3-Dセキュアなど不正利用防止の対策が重要。
しかし、フィッシングの多くはメールが誘導元となっており、入り口対策として「送信ドメイン認証」と「迷惑メール対策」で利用者を守ることが、被害を減らすことにつながっていく

フィッシング報告件数の推移と傾向（年別）

■ 2022年-2023年のフィッシングメール配信における傾向

- **海外の一般向けサービス回線からのフィッシングメール発信**
  特定の事業者の特定の地域からの配信が多かった（2023年10月時点では減少傾向）
- **海外クラウドサービスからの大量配信**
  サーバーを大量に立ち上げ、フィッシングメールを送信したら停止を繰り返す
  → 現在ではサーバーのテイクダウンではなく、事業者側での不正契約対策が必要（対策が難しい）
  → **送信ドメイン認証によりフィッシングメールが送りづらい・着信しづらい環境づくりが重要**

この2タイプで、全フィッシングメールの 6～8割を占めていたが、2023年10月現在は大量配信はほぼ特定の海外クラウドサービスからとなっている



2019年頃はCutwailなどのマルウェアに感染したPCから成るbotnetからの配信や、アカウント乗っ取り、踏み台送信なども多かった

2020年頃からホスティングサービスのサーバー発のフィッシングメール配信が主流となり、配信量が急増。同時になりすまし送信も増え始めた

2022年後半から海外の一般向けサービス回線のIPアドレスレンジからのメール配信が増えた。現在はIPアドレスが不定のクラウドサービス利用が多い

2023年 フィッシング報告の推移と傾向（2022年-2023年 月別）

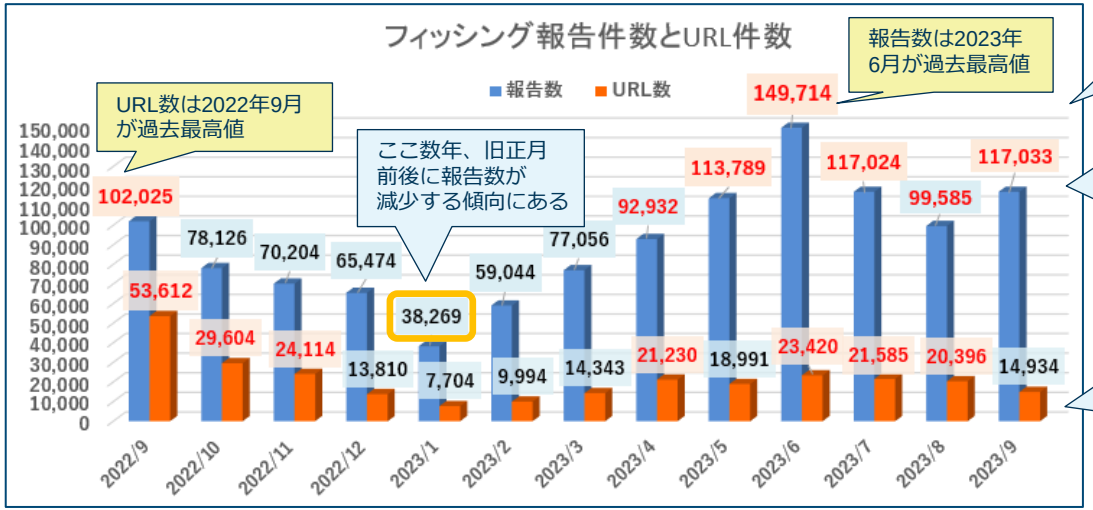
■ フィッシング報告件数の傾向

- 2023年6月、過去最高報告数が更新されたが、URL数は2022年9月が過去最高数となっている
- **DMARC正式運用* していないドメインが、なりすましフィッシングメールの大量配信に不正利用されている**
  * ポリシーがreject/quarantine
- **DMARC受信側検証をしていないメールサービス利用者からの報告の割合が増えている（フィルターを素通りするため）**

■ フィッシングサイト（URL）の傾向

- URLフィルター回避を目的とした、短縮URL、DDNSサービス、事業者の正規サービスの悪用、サブドメインの組み合わせで大量のURLを生成するパターンが主流。
- スマートフォンユーザー狙いが増え、ブラウザー（端末）情報やアクセス回線を見てフィッシングサイトへの誘導をコントロールするものが増えている

稼働確認が難しく、URLフィルター登録、テイクダウンされづらい



報告数増の大きな要因は、なりすましフィッシングメール大量配信

2023年7月9日以降、某海外クラウドサービスからの大量配信が停止。一時的にメール配信量が激減したが、9月からは別の海外クラウドサービスから大量配信が行われている

URL数増加の要因は、URLフィルター回避狙いの大量URL生成。
しかし、同一のIPアドレスへ誘導されるケースも多かった

最近のトピック：国際連携によるフィッシング実行犯逮捕

- **初の国際サイバー捜査、インドネシア人逮捕 世界的詐欺ツールを使用（朝日新聞デジタル）**
  https://www.asahi.com/articles/ASR884RWLR87UTIL040.html

クレジットカードの不正利用で大阪府警がインドネシア人を逮捕した事件をもとに、警察庁とインドネシア国家警察が国際共同捜査を行い、同国警察が7月、共犯などとして在インドネシアのデア・カリスナ容疑者（40）を逮捕したことが、捜査関係者への取材でわかった。警察庁が他国との本格的なサイバー共同捜査で容疑者摘発に至った初のケースという。
（中略）
デア容疑者はフィッシングに「16SHOP」と呼ばれるツールを購入し、使っていた。
16SHOPによる被害は世界中に及び、ICPOが主導した国際共同捜査が展開されてきた。

上記の影響か、7月、8月はフィッシング報告数が少なかった（フィッシングメールが減少）

フィッシングサイトの稼働確認業務をしていると、よくこういう画面が表示されていた（フィッシングサイトのサービス終了画面）

2018/08に撮ったスクリーンショット
メールアドレスが記載されていた

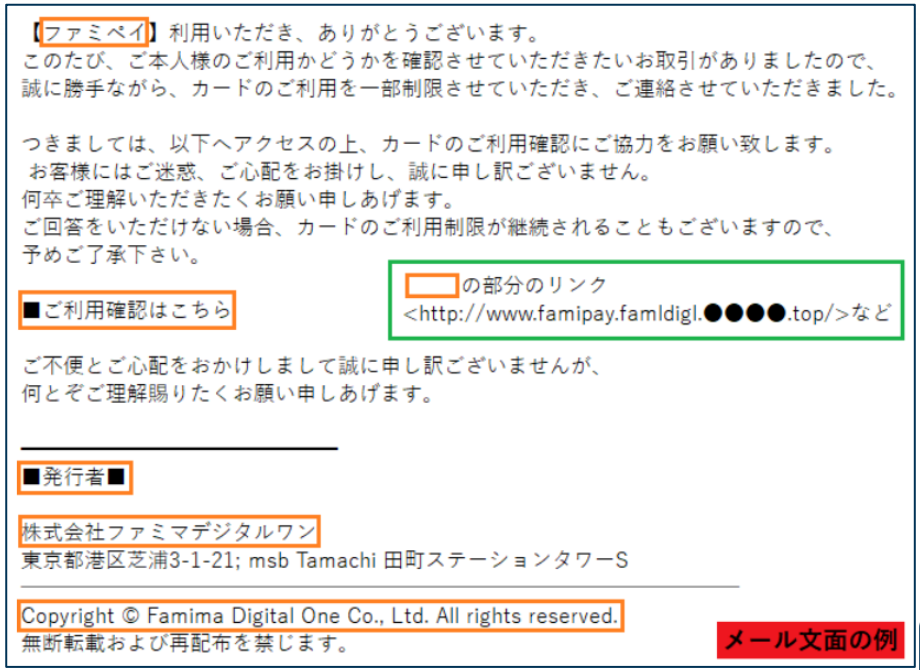
2019/03に撮ったスクリーンショット
メールアドレスの記載がなくなった

2019/04 に撮ったスクリーンショット
Apple をかたるフィッシング

被害者へは必ず警察への情報提供を依頼しましょう！（協議会にも情報提供よろしくお願いします）

フィッシング事例

2022年-2023年の事例：なりすましフィッシングメールの大量配信



【ファミペイ】利用いただき、ありがとうございます。
このたび、ご本人様のご利用かどうかを確認させていただきたいお取引がありましたので、
誠に勝手ながら、カードのご利用を一部制限させていただき、ご連絡させていただきました。

つきましては、以下へアクセスの上、カードのご利用確認にご協力をお願い致します。
お客様にはご迷惑、ご心配をお掛けし、誠に申し訳ございません。
何卒ご理解いただきたくお願い申しあげます。
ご回答をいただけない場合、カードのご利用制限が継続されることもございますので、
予めご了承下さい。

■ご利用確認はこちら

の部分のリンク
<http://www.famipay.famldigl.●●●●.top/>など

ご不便とご心配をおかけしまして誠に申し訳ございませんが、
何とぞご理解賜りたくお願い申しあげます。

■発行者■

株式会社ファミマデジタルワン
東京都港区芝浦3-1-21; msb Tamachi 田町ステーションタワーS

Copyright © Famima Digital One Co., Ltd. All rights reserved.
無断転載および再配布を禁じます。

メール文面の例

出典：フィッシング対策協議会「FamiPay をかたるフィッシング (2023/04/21)」
https://www.antiphishing.jp/news/alert/famipay_20230421.html

- ほぼ同一文面で、ブランド名と署名欄だけ変更
- 2020年頃から使われている。
- 今まで確認されたブランド
  - 三井住友銀行
  - 三菱UFJ銀行
  - PayPay銀行
  - イオン銀行
  - 鹿児島銀行
  - 三井住友カード
  - 三菱UFJニコス
  - JCB
  - JACCS
  - オリコ
  - アプラス
  - エムアイカード
  - セゾンカード
  - アメリカン・エキスプレス
  - エポスカード
  - イオンカード
  - UC カード
  - UCSカード
  - ビューカード
  - 楽天
  - 楽天カード
  - ライフカード
  - VISA
  - Mastercard
  - au PAY
  - えきねっと
  - ファミペイ など（順不同）

- このタイプは**大量配信を行うため、非常に報告数が多い**
- 本物と同じドメインを使った**なりすまし送信率**が高い
- **2022年5月～9月および2023年４月以降、再び増えた**

4月約11,000件、5月約24,000件（月全体の報告数のうち 2割以上）の報告受領

2023年6月は文面は違うが、クレジットカード会社3社が集中的に狙われ、それぞれ1万件～2万件の報告を受領した

大量に生成されたURLの例

- 2023年6月の状況
  - 基本のドメイン＋ブランド名に似せたサブドメインの組み合わせで大量生成
  - 基本のドメイン＋ランダム文字列の組み合わせで大量生成
  - ワイルドカードでネームサーバーに登録されており、IPアドレスは同一

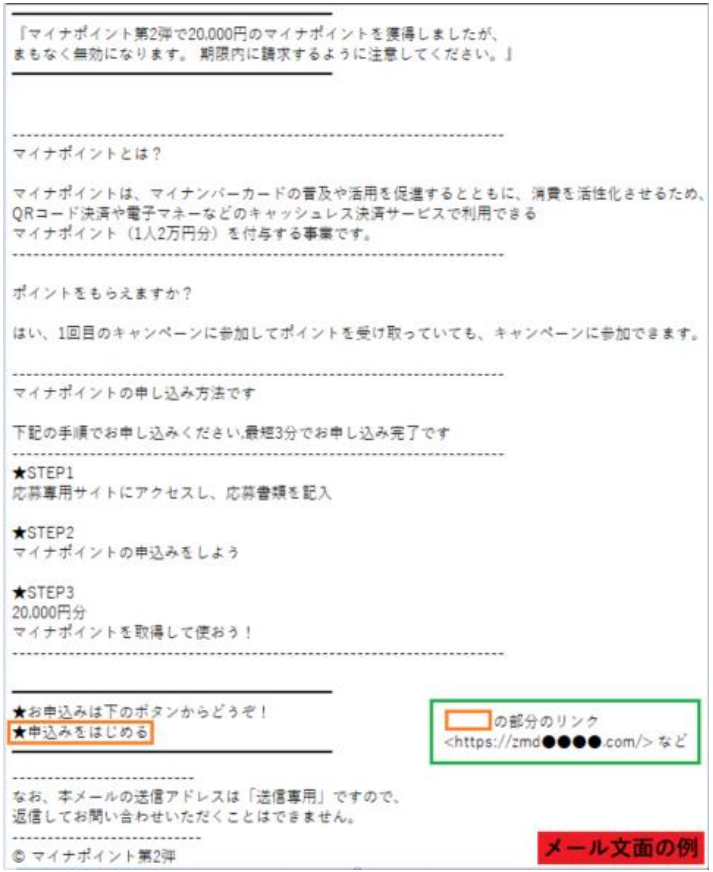
```
$ host *.dza[redacted].cn
*.dza[redacted].cn has address [redacted].26
```

ETCサービス	https://www2.etc-maisaai.jp.191pf.cn/
ETCサービス	https://www2.etc-maisaai.jp.95jd.cn/
ETCサービス	https://www2.etc-maisaai.jp.fc1999.cn/
ETCサービス	https://www2.etc-maisaai.jp.j5608.cn/
ETCサービス	https://www2.etc-maisaai.jp.k3567.cn/
ETCサービス	https://www2.etc-maiseai.jp.191pf.cn/
ETCサービス	https://www2.etc-maiseai.jp.95jd.cn/
ETCサービス	https://www2.etc-maiseai.jp.fc1999.cn/
ETCサービス	https://www2.etc-maiseai.jp.j5608.cn/
ETCサービス	https://www2.etc-maiseai.jp.k3567.cn/

Amazon	https://e1221b4bc06c3ea37d3fc757bb9a3c0f.ktvled.cn/caoni
Amazon	https://6c7ab6baf81a5d0e211449a1fed02aec.51tpsh.cn/caor
Amazon	https://a314a862ba877acfd1fec1b7b1fc0bec.bjsjjldb.cn/caor
Amazon	https://0ef095c75c1fe79b185fa2b6c2de294b.3renwx.cn/caor
Amazon	https://001782eeea49ac4bdc40d8697e5e132c.3renwx.cn/ca
Amazon	https://06a8f23165847bd9f63f3d69a9442da5.dkehmyw.cn/ca
Amazon	https://9cdf92f81a122e36dd77172069de2e9c.51tpsh.cn/caor
Amazon	https://c901a8d52e7f11e8a28d0fc5d2d7a17d.2022qazwsx09
Amazon	https://24feaf4fdda26a5a7eec259b045502d4.yuandongjx.cn/

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ている。フィッシングが成功して悪者が利益を得ている限り、フィッシングで狙われ続ける。また、誘導元メールへの対応状況を相手はよく見ている。フィッシングサイトへの対応で時間を稼いでいる間に、サービス側での不正利用対策を行い、フィッシングを成功しづらくして、被害を抑制する対策が必要となってきた

2023年の事例：マイナポイント



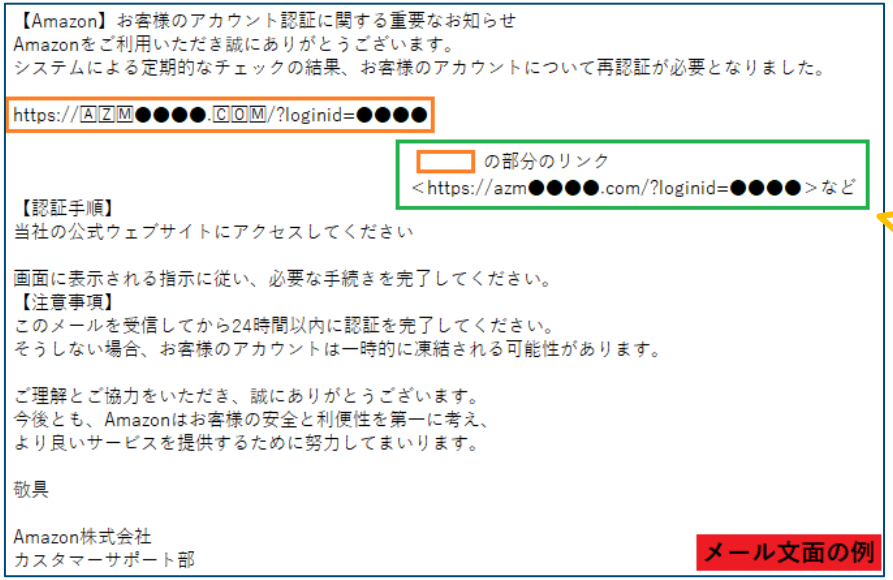
2023年9月末で申請締め切りのため、9月に入ってから情報を入力してしまった、という報告が相次いだ

2023年10月末、2023年11月末、と申請期間が延びたことになってフィッシング継続中

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に飾り文字などが含まれたフィッシング

- 2023年10月末頃から、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



- メール内のURL
  https://AZMSHF.COM/‘
- 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://ⓣⓖⓕⓧⓝⓗⓢ.ⓒⓞⓜ/?ⓛⓞⓖⓘⓝⓘⓓ=ⓡ

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

2023年
報告されたフィッシングメールからみる
今、必要性な対策

なりすましフィッシングメールとDMARC対応状況

- あるメールアドレス宛のフィッシングメールを調査
- 2023年5月～7月は、DMARC未対応ドメインのなりすまし送信メールが多かった

	2023年							
	1月	2月	3月	4月	5月	6月	7月	8月
メール数全体	203	369	307	431	720	989	493	369
なりすましメール	170	312	245	381	662	783	429	281
なりすまし率	83.7%	84.6%	79.8%	88.4%	91.9%	79.2%	87.0%	76.2%
DMARC Enforce	62.9%	30.9%	30.3%	40.6%	14.6%	22.8%	23.5%	43.1%
DMARC p=none	4.5%	8.1%	29.3%	12.3%	6.8%	2.5%	5.1%	7.6%
DMARC なし	16.3%	45.5%	20.2%	35.5%	70.6%	47.0%	58.4%	25.5%

date	time	hFrom2	Subject	dmarc	policy
2023/7/7	14:58:19	ヤマト運輸 <info@kuronek	【ヤマト運輸】お届け先の住所が正	none	none
2023/7/7	15:06:23	ヤマト運輸 <info@kuronek	【ヤマト運輸】重要なお荷物が届き	none	none
2023/7/7	15:06:40	ヤマト運輸 <info@kuronek	【ヤマト運輸】重要なお荷物が届き	none	none
2023/7/7	16:38:41	Amazon <mt@chenduo-grc	【重要なお知らせ】Amazonプライム	none	none
2023/7/7	21:55:53	Amazon <hon@qoo10.jp>	【緊急の連絡】Amazonから情報を更	fail	reject
2023/7/8	11:01:01	Amazon <jq@rakuten.co.jp	【緊急の連絡】Amazonから情報を更	fail	reject
2023/7/8	17:14:16	Amazon <wzbpx@rakuten.c	【緊急の連絡】Amazonから情報を更	fail	reject
2023/7/9	4:48:09	ＥＴＣマイレージサービス事	【重要】ETCサービスご利用者様へ	none	none
2023/7/9	8:45:37	えきねっと <admin@hfd.yt	「新幹線eチケットサービス」えきね	pass	none
2023/7/9	9:08:52	《セゾン》Netアンサー <in	【セゾンカード】お取引目的等の確	none	none
2023/7/9	9:10:31	セゾンカード <info@saisor	＜緊急!セゾンカード 重要なお知らせ	none	none
2023/7/9	10:35:57	クレディセゾン <info@sais	【重要なお知らせ】セゾンカード ご	none	none
2023/7/9	12:48:46	クレディセゾン <info@sais	【重要】セゾンカード からの緊急の	none	none

毎月送られる月額の利用通知や注意喚起、メルマガの文章をコピーし、リンクだけ差し替えたなりすましフィッシングメールも多く送られていた。
この場合、メールに不審な点が少ないため、迷惑フィルターを素通りするケースが多いようだった。

受信側メールサービスで、受信者に届けるべき正規メールかそれ以外かの判定には、DMARCによる検証が必須と思われる

2023年7月の状況

しつこく何度もDMARC未対応ドメインの「なりすまし送信メール」が送られていた。
当該ブランドのなりすましの他、DMARC対応済の他ブランドのドメインでのなりすまし送信も多くみられたが、DMARCで検知できていた

フィッシング報告が多かったブランドのDMARC対応状況

- 毎月のフィッシング報告対象ブランドトップ5を調査
- 2023年5月～7月は、DMARC未対応・正式運用していないドメインを持つブランドをなりすまし送信で狙う傾向があった
- **2023年8月～10月は、DMARC p=quarantine/reject のブランドの報告が増えた**

	2023年4月	2023年5月	2023年6月	2023年7月	2023年8月	2023年9月	2023年10月
1位	Amazon	FamiPay	ヤマト運輸	Amazon	Amazon	Amazon	Amazon
2位	FamiPay	セゾンカード	イオンカード	三井住友カード	三井住友カード	ETC利用照会	ETC利用照会
3位	えきねっと	Amazon	Amazon	イオンカード	ヤマト運輸	三井住友カード	マイナポイント
4位	Uber Eats	イオンカード	セゾンカード	セゾンカード	三井住友銀行	Apple	三井住友カード
5位	ETC利用照会	えきねっと	ジャックス	ヤマト運輸	Apple	マイナポイント	えきねっと
	DMARC	p=quarantine p=reject	p=none	未対応			

調査するとDMARC対応済ブランドの報告は、DMARC受信側検証を行っていないメールサービス利用者からの報告が多い
DMARC検証を行えば、不正であると検出できる「なりすましメール」が素通りして届いている状況で、フィッシング被害が増えているのは、これも要因のひとつと考えられる

2023年Amazonをかたるフィッシングメールのなりすまし状況

Amazonをかたる	7月	8月	9月	10月
フィッシングメール	15,627	16,015	28,423	35,249

Amazonをかたるフィッシングメールで、迷惑メールフィルターで検知されていない（素通りした）と判断されたメールのみを調査・集計対象とした

なりすましドメイン	7月	8月	9月	10月
特定国内通信事業者	0	0	35	12,932
apple.com	2,315	3,935	2,724	1,280
amazon.co.jp	3,997	5,935	16,731	5,529
なりすまし合計	6,312	9,870	19,490	19,741
割合	40.4%	61.6%	68.6%	56.0%

10月以降、DMARC未対応の国内特定通信事業者のメールアドレスをかたり、Amazonブランドのフィッシングメールが大量配信が始まった

DMARC検証対応が進んでいない国内メールサービス利用者からの報告が多く、迷惑メール対策が進んでいる G の利用者からの報告が少ない

報告元	10月
P	3,836
S	3,357
O	3,279
Z	2,592
D	2,127
E	1,548
N	1,237
D	1,055
E	939
D	888
Y	706
S	608
W	604
B	533
P	509
G	10

報告数1位のAmazonをかたるフィッシングは、 p=quarantine の @amazon.co.jp や p=reject の @id.apple.com ドメインで なりすまし送信されたメールが大量に報告されていたが、10月に入り、特定の国内通信事業者のドメインをなりすまして送信するケースが激増した

@id.apple.com、@amazon.co.jp をかたるフィッシングの報告は、DMARC受信側検証未対応のメールサービスから来ている。
なりすまされている国内通信事業者は DMARC未対応なので、<u>その事業者自身は、なりすまし送信されていることに気が付いていない可能性もある</u>

DMARC未対応ドメインは狙われやすい

DMARC検証未対応メールサービス利用者からの報告増加

- 2023年8月～9月、DMARC受信側検証を行っていない、ある特定のメールサービス利用者からのなりすましメール報告の割合が急増
- 多数のブランドをかたっているが、なりすましに使う差出人メールアドレスはほぼすべて@id.apple.comだった

	4月	5月	6月	7月	8月	9月
報告メール件数	73,653	82,268	110,662	92,313	81,291	41,241
某通信事業者	2,362	2,806	9,021	8,878	12,197	5,791
	3.2%	3.4%	8.2%	9.6%	**15.0%**	**14.0%**
メール件数	76,026	88,535	114,226	92,689	84,268	43,030

@id.apple.com（p=quarantine → reject）のなりすましメールが多かった

- 週次でみると、全報告の2割近くを占める週もあった

apple.comドメインはDMARC p=reject/quarantineのため、そのほとんどが**DMARC受信側検証していないメールサービス利用者からの報告**だった。

期間（始め）	7/1	7/8	7/15	7/22	7/29	8/5	8/12	8/19	8/26	9/2	9/9	9/16
期間（終わり）	7/7	7/14	7/21	7/28	8/4	8/11	8/18	8/25	9/1	9/8	9/15	9/22
報告メール件数	23,734	19,554	17,642	20,093	18,104	21,835	19,007	14,787	18,528	17,012	21,825	19,716
某通信事業者	2,431	2,472	895	1,869	1,859	3,165	2,626	2,386	3,628	3,042	2,130	468
	10.2%	**12.6%**	5.1%	9.3%	10.3%	**14.5%**	**13.8%**	**16.1%**	**19.6%**	**17.9%**	9.8%	2.4%

DMARC未検証メールサービスで迷惑メール判定されづらいメールの例

■ 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

smbc.co.jpは DMARC p=reject なのに届いている

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

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

受信者にどうやって見分けてもらうのか

差出人: 三井住友銀行 SMBC_service@dn.smbc.co.jp
件名: 【三井住友銀行】入出金を規制いたしました

重要なお知らせのため、商品・サービス情報の配信を希望されていないお客様にもお送りしております。

平素より、三井住友銀行をご利用いただきありがとうございます。

お客さまのお取引を規制させていただきましたので、お知らせします。

規制内容は下記をご確認ください。

取引規制日時：2023/08/22

取引規制内容
・出金規制
・入金規制

規制解除するには下記へアクセスし、お手続きしてください。

規制解除 <URLはsendgridのもの>

2023/08/22までにご答いただけない場合、
お客様のご答に著しい不足がある場合、もしくは
ご答から当社規約第9条（禁止事項）に抵触すると判断した場合、
やむを得ず、お客様の口座を解約させていただくことがございますので、あらかじめご了承ください。

お客さまにはお手数をおかけいたしますが、何とぞご理解、ご協力のほどお願いいたします。
――――――――――――――――――――――――――――――――――――-
株式会社三井住友銀行
金融機関コード：0009
登録金融機関：関東財務局長（登金）第54号
加入協会：日本証券業協会、一般社団法人金融先物取引業協会

・sendgrid※のURLが貼られている
※メールマーケティングサービス

利用者はメールが送られてくる以上は、
やはり正規メールか否か、判断しなければならない

・啓発内容は適切なのか？
・判断するための情報は誰にでも判りやすいのか？
・簡潔に説明できるのか？
・画面例は載せているか？

これはフィッシングメールです。
正規メールか否か、どうだったら説明しやすいでしょうか？

本当に受信者に望むことは、「正規メールは読んで欲しい」では、どうやって正規メールだと証明すれば良いのか？

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

利用者にはこの情報だけで大事なことが十分に伝わる

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

このゴールに向けてはDMARC正式運用が必須

Gmailで表示したBIMI

対応後

対応前

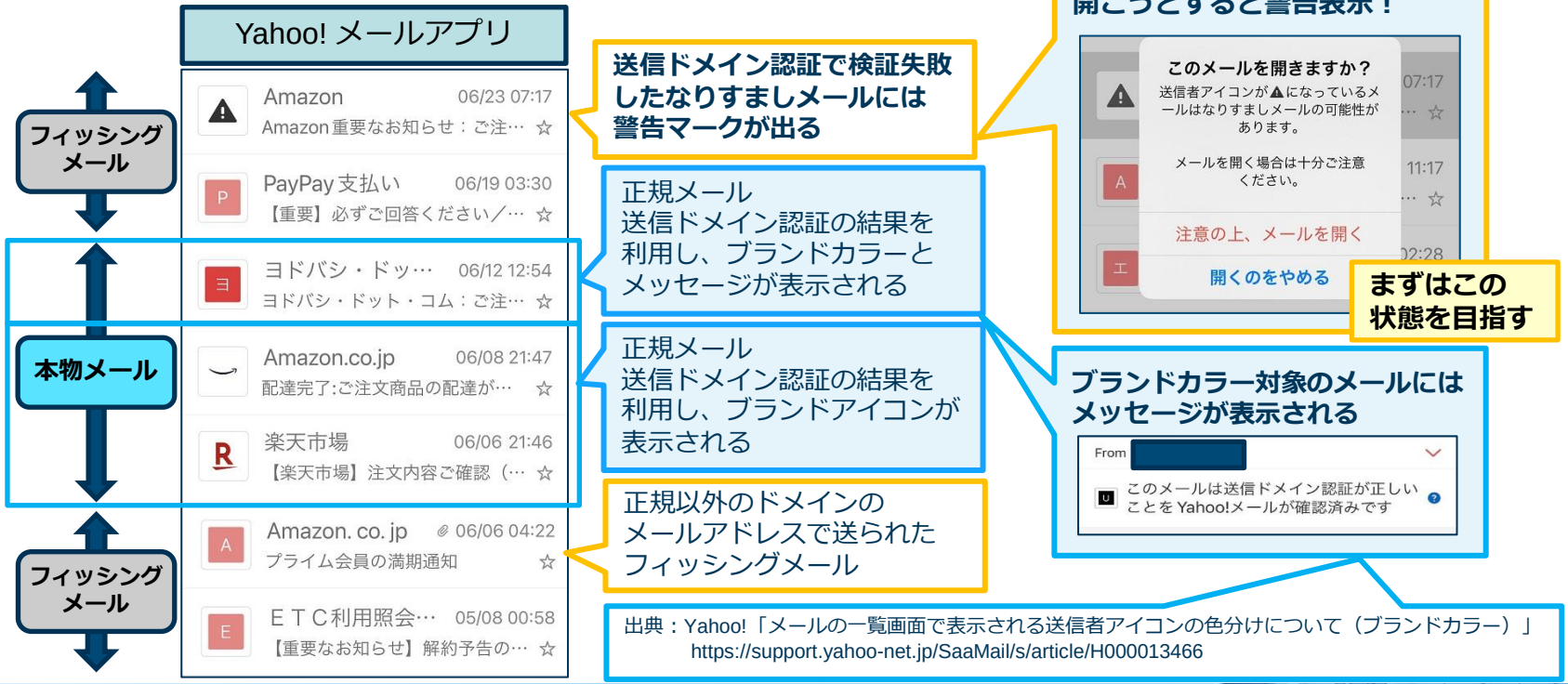
●●●●からお送りするメールの差出人の正しいドメインは@●●●●.co.jpです。
しかしメールアドレスを偽装した偽メールが送られる場合もあるので注意してください
また～かどうかも…

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

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
- 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

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パスした正規メールと、それ以外のメールの表示の違いを知ってもらう
  - 本物のような文面でも、アイコンやマークがついていなかったら、不審メールの可能性が高いと理解してもらう
  - **自分の身を守るためのサービスやツールがあることを知ってもらう**
  - **啓発は試行錯誤、利用者の反応をみながら改善していきましょう**

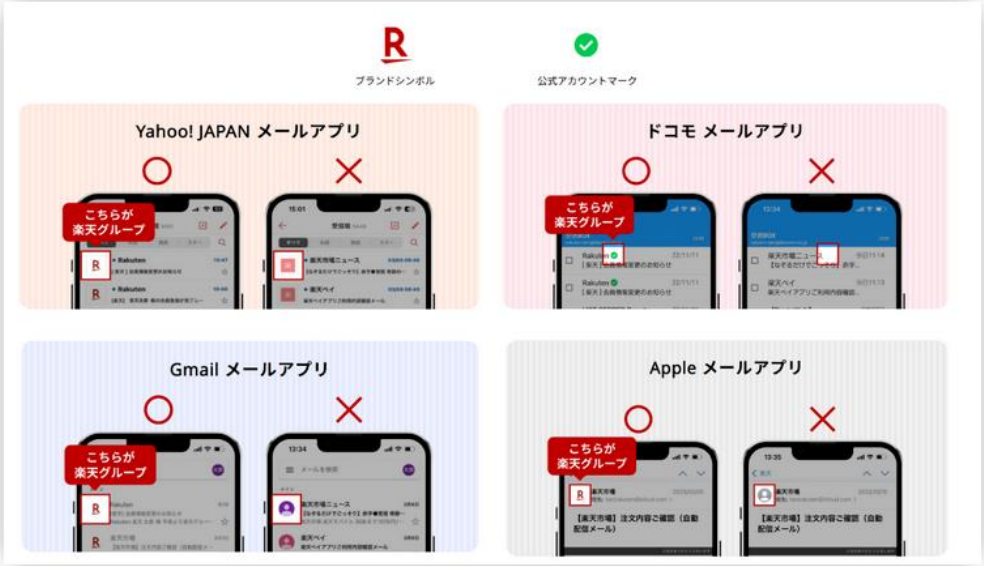


図２　送信ドメイン認証をパスした正規メールの表示例

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

●●●●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

Gmail：メール送信者のガイドライン

このような要件を設定しなければならないほど利用者は危険にさらされ、状況は切迫し厳しい、と理解してください

- Gmail：メール送信者のガイドライン
  https://support.google.com/mail/answer/81126

5,000通／日以上、Gmail宛てにメール送信する場合は、2024年2月1日までに要件を満たす必要がある

- **ドメインにSPFおよびDKIMメール認証を設定します。**
- **送信元のドメインまたはIPに、有効な正引きおよび逆引きDNSレコード（PTRレコードとも呼ばれます）があることを確認します。**
- **Postmaster Tools**で報告される迷惑メール率を0.3%未満に維持します。
- Internet Message Format標準（RFC 5322）に準拠する形式でメールを作成します。
- **GmailのFrom: ヘッダーのなりすましはしないでください。Gmail では、DMARCの検疫適用ポリシーの使用が開始されます。GmailのFrom: ヘッダーのなりすましをした場合、メール配信に影響する可能性があります。**
- メーリング リストや受信ゲートウェイを使用するなどして、メールを定期的に転送する場合は、送信メールに ARCヘッダーを追加します。ARCヘッダーによって、メールが転送されたことが示され、送信者が転送者と見なされます。メーリング リストの送信者は、メーリング リストを指定するList-id: ヘッダーも送信メールに追加する必要があります。
- **送信ドメインにDMARCメール認証を設定します。DMARC適用ポリシーはnoneに設定できます。**
- **ダイレクト メールの場合、送信者のFrom: ヘッダー内のドメインは、SPFドメインまたはDKIMドメインと一致している必要があります。これはDMARCアライメントに合格するために必要です。**
- 配信登録されたメールの場合は、ワンクリックでの登録解除を有効にし、メッセージ本文に登録解除用のリンクをわかりやすく表示します。

まずは DMARC p=none でDMARCレポートを受信し分析するとともに、Postmaster Toolsで送信したメールの判定状況を確認し、改善してください

通信事業者さまへ：現状を改善するために（2023年10月時点）

メールサービスを提供している通信事業者はDMARC受信側検証を行い、ポリシーに沿ったメールの処理を検討してください。迷惑メールフィルターで判別されづらい「なりすましメール」が貴サービスの利用者に届いており、被害が発生しています

利用者に迷惑メールフィルターの利用を強く推奨するとともに、送信ドメイン認証の結果をメールツール（Webメールなど）で表示し、利用者の本物メールか否かを判断を助ける環境を提供してください

素通りしたフィッシングメールの報告窓口を用意し、迷惑メールフィルターへすみやかに反映できるようにしてください（フィルター提供セキュリティベンダーの窓口でも良い）

フィッシングメールは情報漏えいデータをもとに送られており、漏えいしたデータはインターネット上から完全に消すことはできません。フィッシングメールが届いたり、情報を入力してしまった被害者には、今後の安全のため「メールアドレスの変更」を強く推奨してください

フィッシング対策を行う事業者さまへ：現状を改善するために（2023年10月時点）

Gmailのメール送信者のガイドラインは、メールセキュリティの基本的な対策のみを要求しています。DMARC未対応の場合は、p=noneですぐにモニタリングを開始し、Postmaster Tools等で状況を確認して、メールセキュリティ上の脆弱性を排除してください

正規メール視認性向上を行い、それを利用者に十分に啓発してください。また、啓発を行う側が「利用者として」このようなサービスを実際に使って、利用者側の立場で、どのように表示・啓発をしてもらえたら理解しやすいか、考えてください

フィッシングメールは情報漏えいデータをもとに送られており、漏えいしたデータはインターネット上から完全に消すことはできません。フィッシングメールが届いたり、情報を入力してしまった被害者には、今後の安全のため「メールアドレスの変更」を強く推奨してください

現状のメールサービスが要件を満たせない場合は、受信者には身を守るために、DMARC受信側対応済のセキュリティレベルの高いサービスを利用するよう、ご案内してください

見てわかる、それが最善

ご協力、ご検討いただけましたら幸いです

以降、参考資料

送信ドメイン認証に関する省庁・関連団体の動向

クレジットカード会社等に対するDMARC対応の要請

- クレジットカード会社等に対するフィッシング対策の強化を要請しました (2023/02/01)
  https://www.meti.go.jp/press/2022/02/20230201001/20230201001.html
  警察庁、総務省、経済産業省の連名で発表

昨今、悪意のある第三者が、クレジットカード会社等を騙った電子メール等を利用者に送信し、利用者を当該電子メール等のリンクから偽サイトに誘導したうえで、利用者のクレジットカード番号等を詐取する攻撃（いわゆるフィッシング）が多発しています。

フィッシングによるクレジットカード番号等の詐取は、クレジットカード番号等の不正利用の一因となっており、利用者保護の観点から、クレジットカード会社等において適切な対応が取られることが求められます。とりわけ、**フィッシングメールがドメイン名をなりすまして送信されることが多い点に鑑みると、送信ドメイン認証技術のうち、フィッシングメール対策に特に有効とされているDMARCを導入し、ドメイン名のなりすましを検出するとともに、自社を騙るフィッシングメールが利用者に届かなくなるよう利用者の受信を制限することが重要**です。

経済産業省、警察庁及び総務省は、こうした状況を踏まえ、クレジットカード会社等に対してフィッシング対策の強化を要請しました。

クレジットカード・セキュリティガイドライン【4.0版】

- 日本クレジット協会
  クレジットカード・セキュリティガイドライン【4.0版】
  https://www.j-credit.or.jp/security/pdf/Creditcardsecurityguidelines_4.0_published.pdf

１．消費者への周知・啓発（P.46）から引用

> また、昨今では、フィッシングメール等を起因とするカード利用者からのクレジットカード情報窃取等によるクレジットカードの不正利用被害も増加しており、**カード会社をはじめとする関係事業者においては DMARC その他のフィッシング対策を講じている**※ものの、事業者における対策だけでは限界もあることから、消費者であるカード会員自らがフィッシングの被害に遭わないための取組が強く求められるところである。
>
> ※「クレジットカード決済システムのセキュリティ対策強化検討会報告書」（2023年1月20日）において、「フィッシングからの自衛」として、イシュアーに対して、クレジットカード会社をかたるフィッシングサイトの検知・テイクダウンや**クレジットカード会社の送信メールのドメイン管理**等による未然防止による多面的・重層的な自衛措置を講じることが求められている。

政府機関等の対策基準策定のためのガイドライン

■ 内閣サイバーセキュリティセンター（NISC）

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
政府機関等の対策基準策定のためのガイドライン（令和５年度版）
https://www.nisc.go.jp/pdf/policy/general/guider5.pdf

6.2.2(1)-2 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。

6.2.2(1)-3 情報システムセキュリティ責任者は、**必要に応じて、S/MIME 等の電子メールにおける電子署名**の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。

2020年～2022年にかけて、省庁ドメインをかたるなりすましフィッシングメールが多く配信された影響か、**DMARCは「行う必要がある」対策**として記述された

S/MIMEは「必要に応じて」で、DMARCの方がより強く推奨されている