JANOG52
フィッシングとメールセキュリティの現在と未来

Let’s eXchange!

2023年前半版
フィッシング対策の現在と未来

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、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 126 組織**（2023 年 6 月時点）
    正会員： 99 社、リサーチパートナー： 5 名、関連団体： 15 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

協議会とJPCERT/CC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

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

（厚生労働省をかたるフィッシング (2021/08/30)より）

フィッシングの最新事例を掲載！

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いる。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 6 月のフィッシング報告件数は 149,714 件となり、2023 年 5 月と比較すると 35,925 件、約 31.6 % 増加しました。
ヤマト運輸をかたるフィッシングの報告は報告数全体の約 18.1 % となり、次いで各 1 万件以上の報告を受領した イオンカード、Amazon、セゾンカード、ジャックスをかたるフィッシングの報告をあわせると、全体の約 60.2 % 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 20 ブランドあり、これらで全体の約 91.6 % を占めました。

フィッシング対策協議会
2023/06 フィッシング報告状況
https://www.antiphishing.jp/report/monthly/202306.html

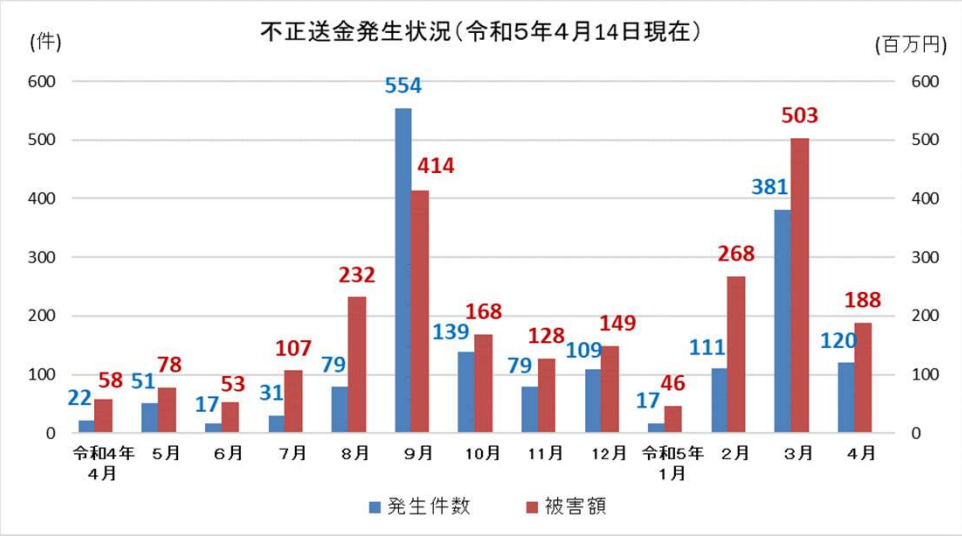
報告数、URL数は、一般の方々から寄せられた「フィッシングメール」と「SMS」を主に集計している。
専門家による探索、検知による大量のURL報告は、なるべく除外して集計している。
フィッシング対策協議会の報告数＝一般向けに実際にメールやSMS等から誘導があったもの。（実態に近い）

2022年-2023年 不正送金被害増加

- 2023/04/24 : 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/20230424_press3.pdf
  - インターネットバンキングによる預金の不正送金事案が多発しています。（金融庁）https://www.fsa.go.jp/ordinary/internet-bank_2.html

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。(警察庁の発表資料より)

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、一旦被害件数は減少傾向となりましたが、令和5年2月以降、再度、被害が急増しています。（金融庁の発表資料より)



2023年1月～6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 27 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

2022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/download/news_202300000195.pdf

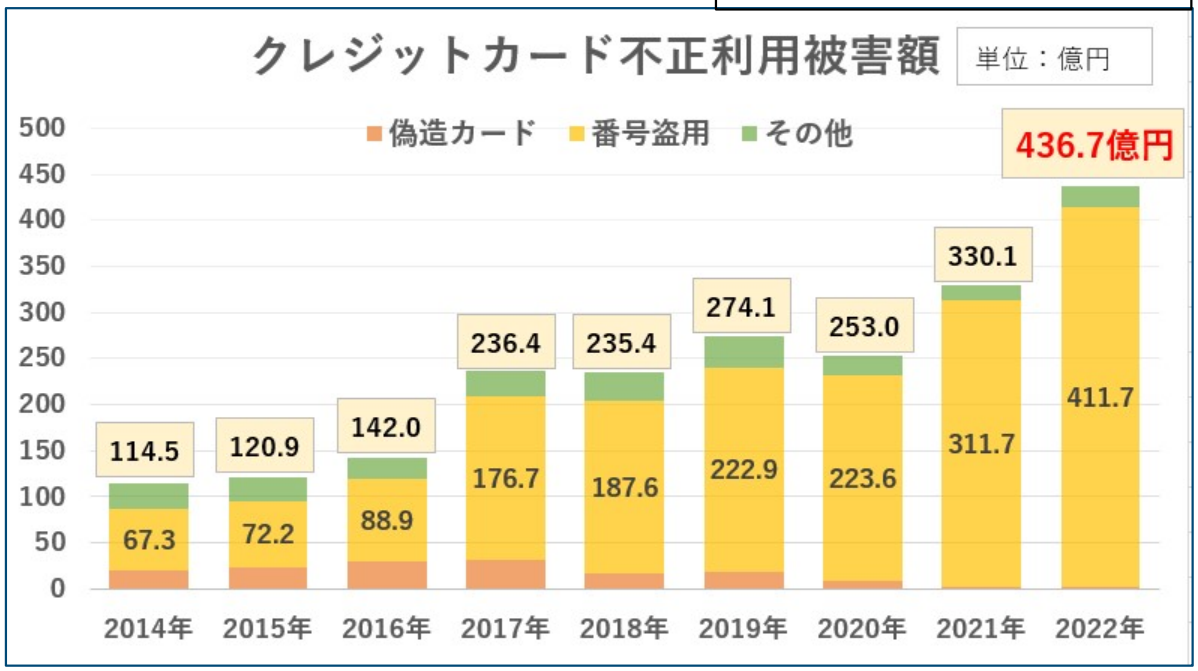
上記資料の数値をもとに作成

2022 年通年の不正利用被害額
436.7 億円（前年比 32.3 %の増加）

不正利用被害額に占める
◆ 偽造被害額 1.7 億円（13.3 % 増）
◆ 番号盗用被害額 **411.7 億円（32.1 % 増）**
◆ その他不正利用被害額 23.3 億円（37.9 % 増）

番号盗用被害額が占める割合
◆ 2021年 **94.4 %**
◆ 2022年 **94.3 %**

不正利用のほとんどが番号盗用被害。
フィッシングメール増加によるカード番号詐取が増加したのも、その主な要因と考えられる



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、フィッシングはその多くがメールとSMSが誘導元となっており、メールについては入り口対策として「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

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。

フィッシング対策協議会での緊急情報掲載数（年別）

- 2023年6月末時点ですで に2022年の掲載数を超えている
- 緊急情報掲載の条件
  - 新たなブランド
  - 報告数が多い、急増
  - 影響度が大きい　等

2023年	72件
2022年	68件
2021年	84件
2020年	46件
2019年	46件
2018年	48件

6月	14件
5月	11件
4月	14件
3月	17件
2月	9件
1月	7件

2023年06月30日ANA をかたるフィッシング (2023/06/30)
2023年06月30日エポスカードをかたるフィッシング (2023/06/30)
2023年06月27日ジャックスをかたるフィッシング (2023/06/27)
2023年06月21日西日本シティ銀行をかたるフィッシング (2023/06/21)
2023年06月19日日本航空をかたるフィッシング (2023/06/19)
2023年06月16日三菱UFJ銀行をかたるフィッシング (2023/06/16)
2023年06月14日北洋銀行をかたるフィッシング (2023/06/14)
2023年06月13日総務省をかたるフィッシング (2023/06/13)
2023年06月13日沖縄電力をかたるフィッシング (2023/06/13)
2023年06月13日北海道電力をかたるフィッシング (2023/06/13)
2023年06月12日チューリッヒ保険会社をかたるフィッシング (2023/06/12)
2023年06月05日Apple をかたるフィッシング (2023/06/05)
2023年06月05日じゃらんをかたるフィッシング (2023/06/05)
2023年06月01日エムアイカードをかたるフィッシング (2023/06/01)

3月末の移動シーズンには電力・ガス会社をかたるフィッシングが発生したり、アフターコロナで人々の移動が増え始めた6月は旅行関連（予約サイト、航空会社）をかたるフィッシングが発生。
納税シーズンには省庁をかたり、住民税、自動車税などの支払いを求めるなどの手口も発生。
注意深い人でも、思い当たるタイミングでこのようなフィッシングメールがくると、反応してしまう可能性がある

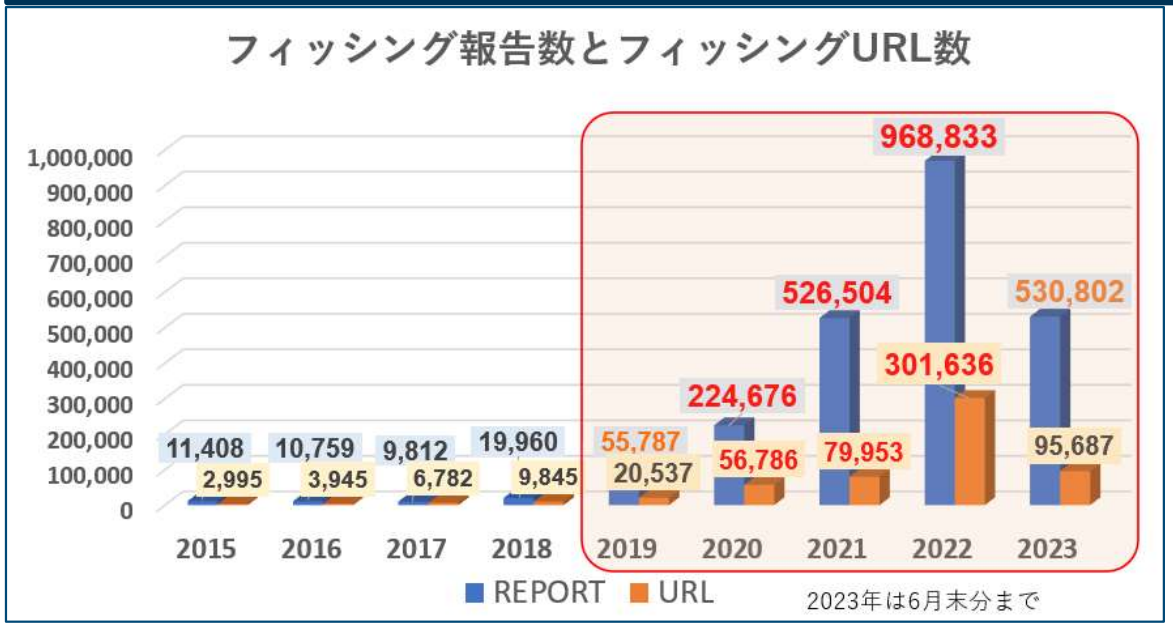
フィッシング報告件数の推移と傾向（年別）

■ 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が多くなった**
  特定の事業者の特定の地域からの配信が多い（bot? VPN? その地域に設置された何かの機器?）
- **海外のクラウドサービス利用のメール配信が増える。おそらくサーバーのテイクダウン（停止）より、不正契約アカウントまるごと契約解除の対応が必要**

この2つで、全フィッシングメールの6〜8割は占める状況

過去、国内事業者からの発信については、迷惑メール相談センターさまと各通信事業者さまのご協力で、不正契約への対応および対策が行われてきたが、海外の対応については、難航している状況



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。
IPアドレスが不定のクラウドサービス利用も多い

フィッシング報告の推移と傾向（2022年-2023年 月別）

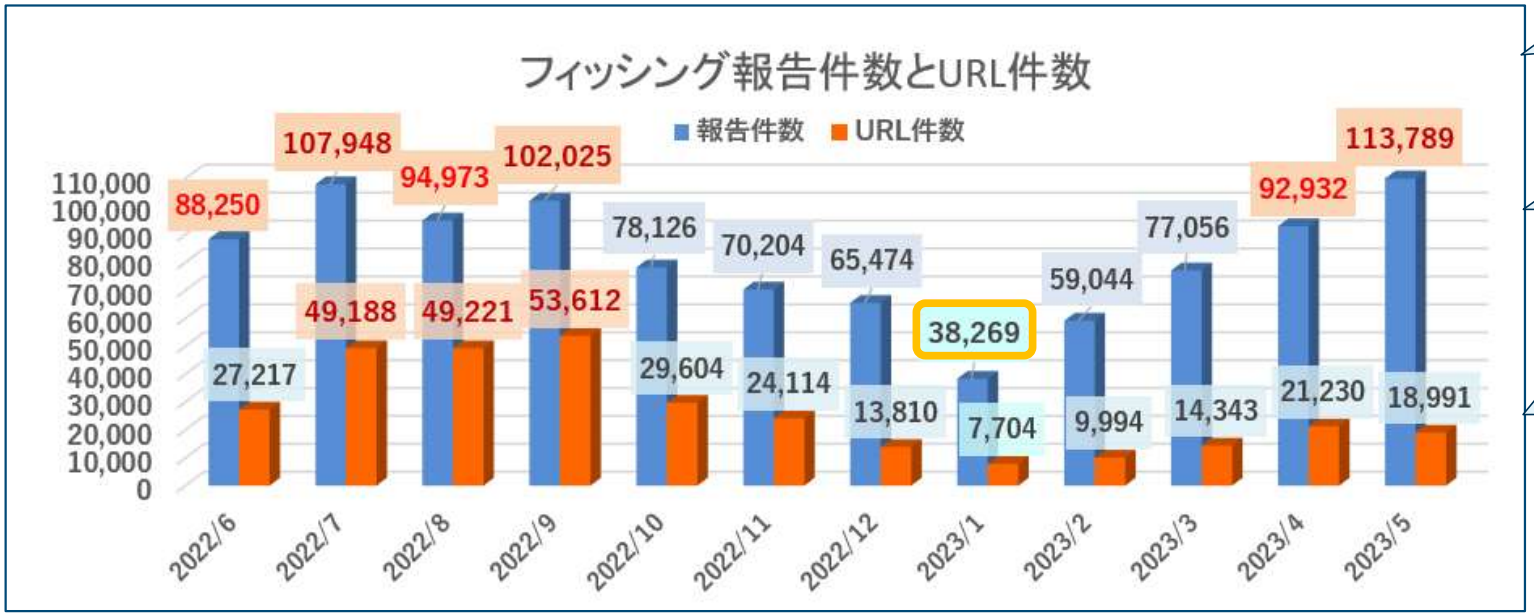
■ フィッシング報告件数の傾向

- 2023年1月は報告数（メール配信数）が激減。ここ数年、旧正月の前後は減る傾向がある
- **DMARC正式運用(*)していないブランドは狙われ、なりすましフィッシングメールの大量配信が続いている。（フィッシングメールが利用者に届きやすい＝成功しやすい）**

(* DMARC正式運用 = ポリシーがreject/quarantine)

■ 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増えた。
- **スマートフォンユーザー狙いが増え、UA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、テイクダウンしづらい）**

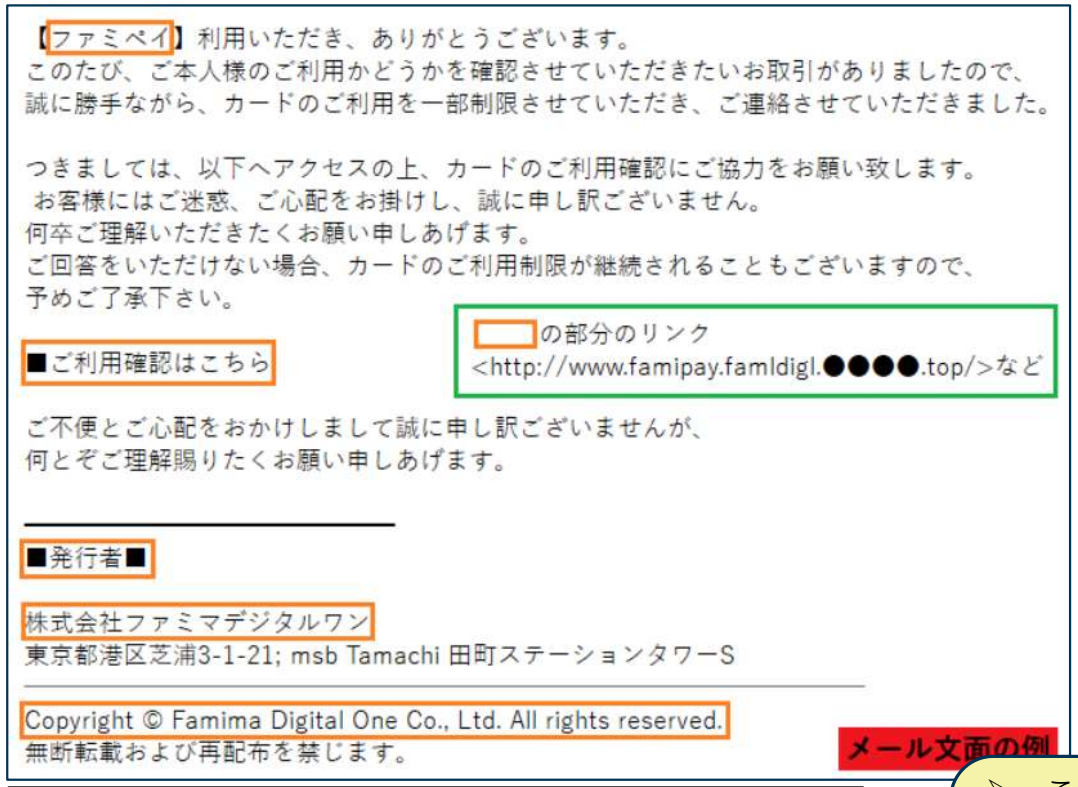


報告数増の大きな要因は、フィッシングメール大量配信

大量配信系を抑えることができれば、1月くらいの量となるはず

URL数増加の要因は、URLフィルター回避を狙った大量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い

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

- 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）

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

4月約11,000件、5月約24,000件(月全体の2割以上を占める)の報告受領

- このタイプは**国内外のクラウドサービスを使って、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、再び増えたサブドメインで大量のURLを生成するフィッシングもこのタイプ**

大量に生成されたURLの例

- 確認された誘導元フィッシングメールのブランドの例 (2022年6月～9月頃)
  - 三井住友カード
  - 三菱UFJニコス
  - JCB
  - エポスカード
  - イオンカード
  - セゾンカード
  - エムアイカード
  - 楽天カード
  - VISA
  - Mastercard
  - au PAY
  - えきねっと など
- クレカブランドのケースでは誘導元メール文面でかたるブランドに関係なく、同一デザインのフィッシングサイトへ誘導された
- URL 内の文字列もメール文面でかたるブランドではないブランドの文字列が含まれる

2022/9/2	13:18:36	VISA	http://www.vieivsaves.visasaneeie.rfqbpz.id/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:19:44	VISA	http://www.vivccaees.visveaaaser.gtfvze.top/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:20:32	VISA	http://www.viecvaeaees.viscaasneeire.xtkiwg.top/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:24:18	VISA	http://www.vieivsaves.visasaneeie.ulcodn.za.com/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:25:27	MyJCB	http://www.vsacvaeaei.visacaasaosr.nidat1.icu/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:26:47	MyJCB	http://www.vsacveoaei.visaccasaos.qlpyab.cyou/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:30:18	VISA	http://www.vivacaces.visceacaie.qlndwb.id/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:36:56	VISA	http://www.vieivsaaees.visccaaneaie.vnlzsn.za.com/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:37:16	MyJCB	http://www.vsaccaeaei.visacaasaosr.jxsfsm.top/k7OIMyJhEU/page1.php	稼働中	未知
2022/9/2	13:37:35	MyJCB	http://www.vsacveosi.visavvsaos.yhcwiu.cyou/k7OIMyJhEU/page1.php	稼働中	未知

それまで主流だったURLフィルタリングによる対策で効果が出にくい状況となった。IPアドレスは同一の場合が多いため、テイクダウンが効果的だが、落ちるまでに数十万通のメール配信による誘導が行われている状況

フィッシング対策協議会
クレジットカードの利用確認を装うフィッシング (2022/06/24)
https://www.antiphishing.jp/news/alert/creditcard_20220624.html

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].[redacted].[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/

現状、IPアドレスでのブロック（フィルタリング）は積極的に行われていないという認識だが、じきに必要な状況がくるのは明確。IPアドレスのブラックリスト(DNSBL/RBL) 登録と解除について、IPアドレスホルダー側とセキュリティベンダー側との I/F が必要になってくると思われる。（迷惑メール対策界隈では昔からあった）
別案として、悪性判定されたドメインのワイルドカード登録をチェックツールで可視化したり、キャッシュDNSサーバーやProxyで上書きして応答など、利用者側の合意を得たセキュリティサービスなどでは可能？

フィッシングサイトへの対応と対策：現状と課題

- **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

今後は、ワイルドカード登録についても効果的な対応を考えていく必要がある

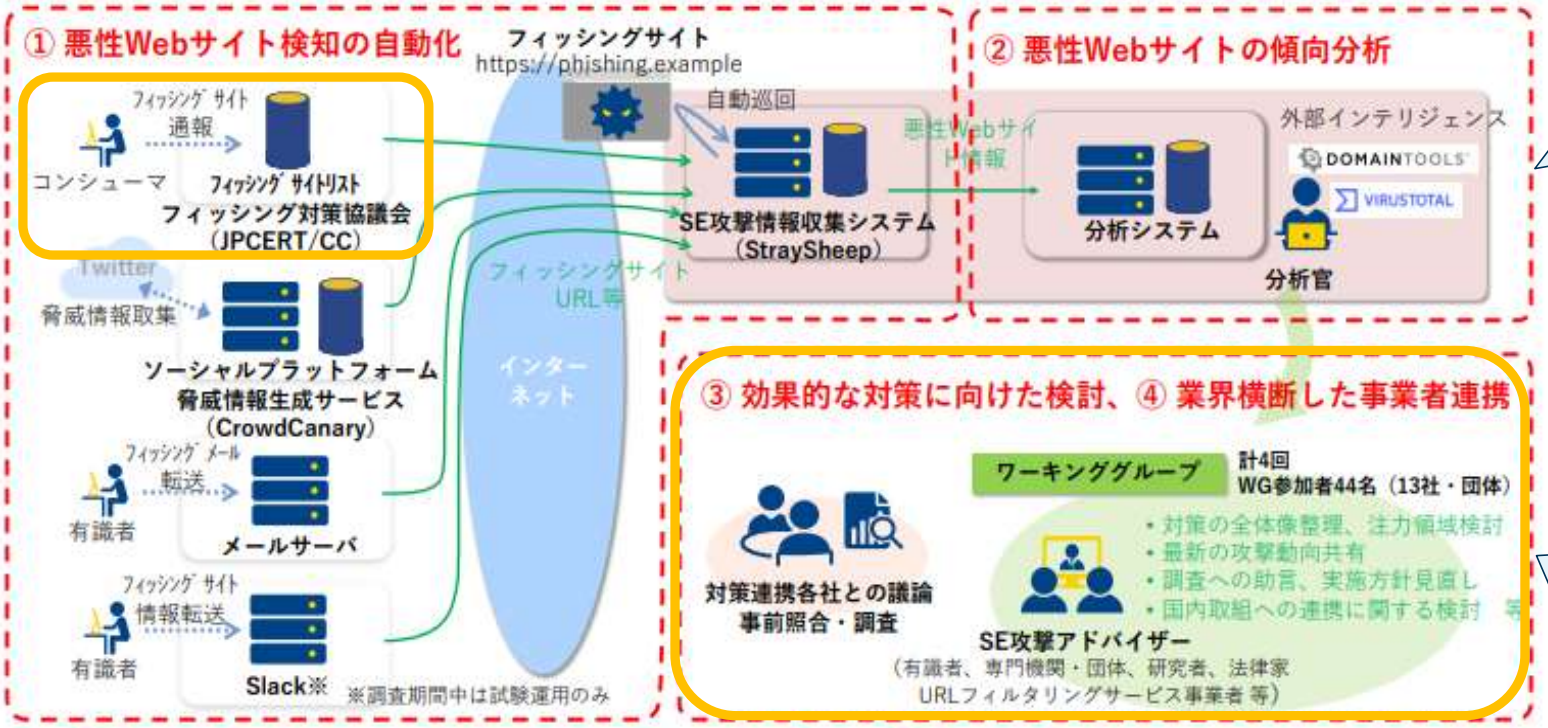
- **フィッシングサイトのサイト閉鎖調整（テイクダウン）**
  - 各事業者から直接ホスティング事業者等へのサイト閉鎖依頼を推奨
- **検知サービス**
  - 早期に URL フィルタリングへの登録、サイト閉鎖調整を行えるため、被害抑制に効果が期待できる
  - 組織内に専門の人員や設備がなくても、迅速な対応が可能
  - 2022 年度版の「フィッシング対策ガイドライン」で検知サービスの利用を「必要に応じて」から「推奨」へ変更
  - 大量URL生成タイプのフィッシングのターゲットになると、費用がかさむので、契約時にその場合の対応について、確認しておく。

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現在では、各所でリソース不足と遅延が発生している。
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めざす時にきている

フィッシングサイトの検知、共有に係る調査 （総務省）

■ 総務省 サイバーセキュリティタスクフォース（第43回）
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00237.html

➢ 資料43－1－2：
悪性Webサイトの検知技術・共有手法の実装可能性検証に係る調査ご報告（NTTコミュニケーションズ）
https://www.soumu.go.jp/main_content/000878674.pdf （5ページ目、調査の全体像 より抜粋）



フィッシングサイトの検知から共有、対応までをいかに効果的に行うか、を試行し調査する

JPCERT/CC (フィッシング対策協議会) は
①フィッシングサイトリスト提供
③効果的な対策に向けた検討
④業界横断した事業者連携について、参加、協力している

フィッシング対策：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、つね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 2023年6月1日公開）

- **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

事業者側での対策

- フィッシング対策ガイドライン重要５項目

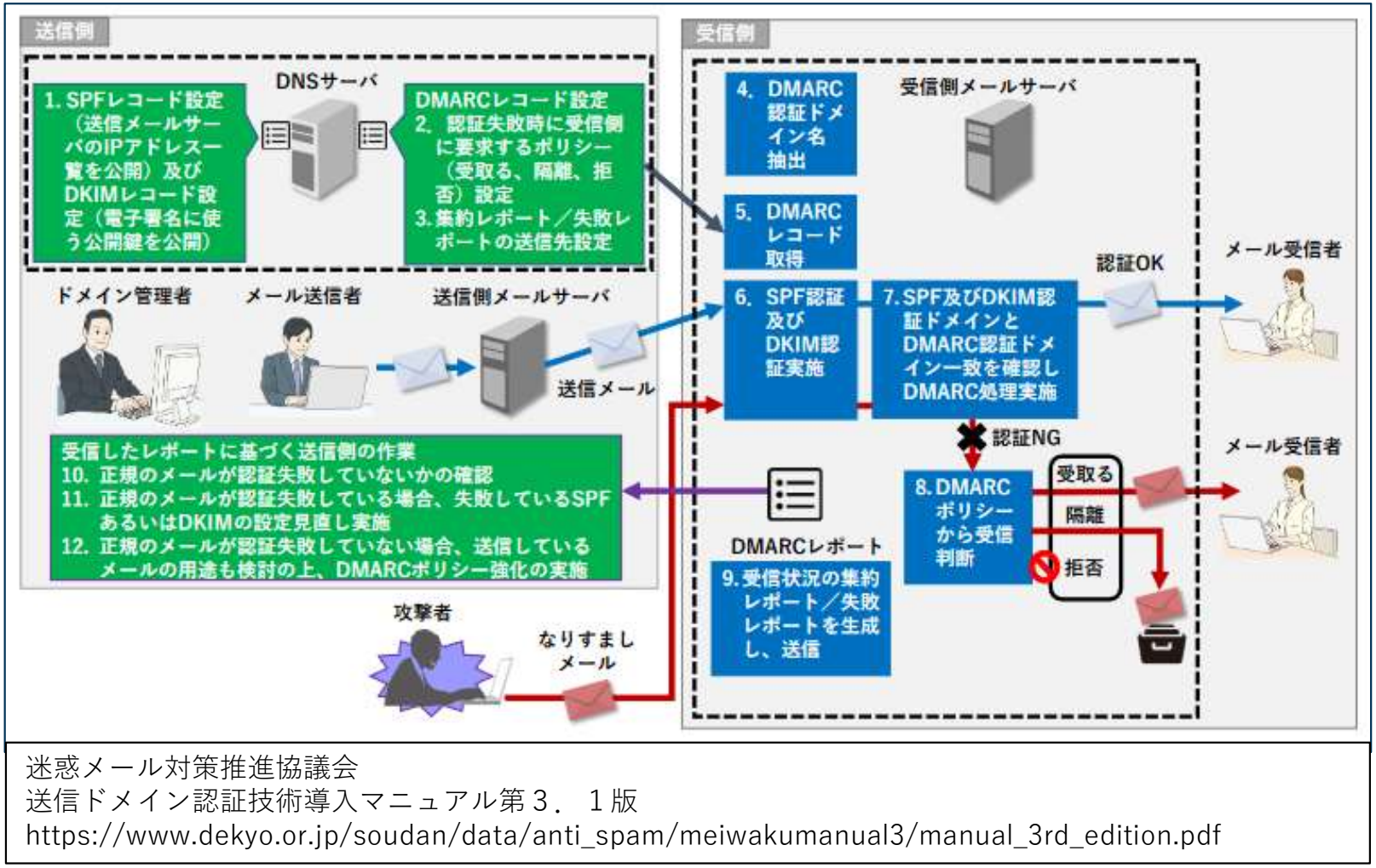
1. **利用者に送信するメールには「なりすましメール対策」を施すこと**
2. 複数要素認証を要求すること
3. ドメインは自己ブランドと認識して管理し、利用者に周知すること
4. すべてのページにサーバー証明書を導入すること
5. フィッシング詐欺について利用者に注意喚起すること

なりすましメール対策：送信ドメイン認証

送信ドメイン認証技術は現在、
・SPF
・DKIM
・DMARC
の3種類ある。

DMARCはSPFやDKIM単体で使用した場合の欠点を補い、有用な機能が追加されている

DMARCで正規メールであると認証（検証）できたメールの視認性を向上するBIMIという技術もある



迷惑メール対策推進協議会
送信ドメイン認証技術導入マニュアル第３．１版
https://www.dekyo.or.jp/soudan/data/anti_spam/meiwakumanual3/manual_3rd_edition.pdf

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ほうのメールアドレス（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 メールが対応済** **モバイルユーザー向けのカバー率は高い** **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	日本国内の事業者や ISP (プロバイダーのメールサービス) は対応が遅れている

2022年1月～2023年5月 なりすまし送信メール割合

- あるメールアドレス宛のフィッシングメールを集計
- **送信ドメイン認証技術DMARCを使用すると、フィッシングメールの約 50 ～ 90% を占める「なりすまし送信メール」が技術的に排除できる**

	2022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
メール数全体	126	177	315	537	364	364	316	258	202	287	318	392
なりすましメール	96	97	181	421	253	220	196	139	167	251	287	357
なりすまし率	76.2%	54.8%	57.5%	78.4%	69.5%	60.4%	62.0%	53.9%	82.7%	87.5%	89.90%	91.1%
CN 発	87.3%	85.9%	84.4%	91.1%	90.1%	96.4%	92.1%	91.9%	98.0%	94.8%	95.3%	88.0%

	2023年				
	1月	2月	3月	4月	5月
メール数全体	203	369	307	431	720
なりすましメール	170	312	245	381	662
なりすまし率	83.7%	84.6%	79.8%	88.4%	91.9%
CN 発	75.9%	85.9%	74.6%	88.3%	94.6%

フィッシングメールが増え続けている現在、DMARCで技術的に不正送信されたメールを検知・排除することで、被害抑制に大きな効果が期待できる。

2023年5月の状況
しつこく何度も「なりすまし送信メール」が送られていた。gmail.com や yahoo.com、その他の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

2023/5/7	1:17:20	アマゾン <wznkhsgy@yahoo.com>	Amazonプライムの自動更新設定を解除し
2023/5/7	11:00:14	ファミペイ <info@family.co.jp>	【ファミペイ】個人情報確認
2023/5/7	11:10:22	FamiPay <info@family.co.jp>	【ファミペイ】ご注文内容の確認 [メール
2023/5/7	11:42:26	アマゾン <ez@gmail.com>	Amazonプライムの自動更新設定を解除し
2023/5/7	12:36:40	ファミペイ <info@family.co.jp>	【最終警告】ファミペイ からの緊急の連
2023/5/7	21:30:29	大和ネクスト銀行 <llv@yahoo.com>	【大和ネクスト銀行】お客様の直近の取
2023/5/7	23:25:04	AEON株式会社 <yioa@AEON.com>	イオンカード会員 緊急のご連絡.！！！！
2023/5/8	5:35:35	横浜銀行 <info@boy.co.jp>	横浜銀行の重要なお知らせ（必ずご確認
2023/5/8	9:08:28	ファミペイ <info@family.co.jp>	【重要】ファミペイ重要なお知らせ

なりすまし送信の例

- 2023年7月、モバイル系メールアドレスへの配信では特徴的な傾向
  - フィッシングの標的とならなくてもドメインは不正利用されるため、対策が必要
  - 通信事業者側も、DMARCポリシー等に沿ったメールの扱いが必要

ソフトバンク宛て info@id.apple.com を使ってなりすまし送信	**au 宛て** ******@ponta.jp を使ってなりすまし送信**
差出人: メルカリ <info@id.apple.com> **日時:** 2023年7月3日 4:43:57 JST **宛先:** [redacted]@i.softbank.jp **件名: 【メルカリ】お客様のアカウント認証に関するお知らせ**	**差出人:** メルカリ <rakuten@ponta.jp> **日時:** 2023年7月3日 0:09:40 JST **宛先:** [redacted]@ezweb.ne.jp **件名: 【メルカリ】お客様のアカウント認証に関するお知らせ**
差出人: 三井住友銀行 <info@id.apple.com> **日時:** 2023年7月4日 8:26:53 JST **宛先:** [redacted]@i.softbank.jp **件名: 【重要】三井住友銀行アカウントの異常通知**	**差出人:** 三井住友銀行 <smbc@ponta.jp> **日時:** 2023年7月3日 7:19:11 JST **宛先:** [redacted]@ezweb.ne.jp **件名: 【重要】三井住友銀行アカウントの異常通知**
差出人: icloud <info@id.apple.com> **日時:** 2023年7月3日 8:45:44 JST **宛先:** [redacted]@i.softbank.jp **件名: Apple お客様のアカウント認証に関する重要なお知らせ**	**差出人:** icloud <apple@ponta.jp> **日時:** 2023年7月3日 2:46:21 JST **宛先:** [redacted]@ezweb.ne.jp **件名: Apple お客様のアカウント認証に関する重要なお知らせ**
差出人: ペいペい <info@id.apple.com> **日時:** 2023年7月3日 2:11:18 JST **宛先:** [redacted]@i.softbank.jp **件名: PayPayお客様のアカウント認証に関するお知らせ**	**差出人:** ペいペい <epos@ponta.jp> **日時:** 2023年7月3日 9:20:00 JST **宛先:** [redacted]@ezweb.ne.jp **件名: PayPayお客様のアカウント認証に関するお知らせ**

2023年1月～6月 差出人メールアドレスドメインの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集計
- 多い月では半数以上を排除することができるが、2023年5月以降、DMARC 対応していないドメインを持つブランドを集中的になりすまし送信で狙う傾向がある
- DMARC 受信側検証はモバイルユーザーのカバー率は高いが、PC ユーザーはDMARC未対応のメールサービスを使っている割合が多いので、メールアドレスの移行を促進していくことも重要

DMARCは偽メールを検出するための技術ではない

DMARCはメールが正規の送信元から送られたかを検証できる技術

利用通知や注意喚起、メルマガの文章をコピーした なりすましメールは、迷惑フィルターを素通りして届くケースが多い。

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

2023年5月-6月の状況
DMARC登録なしのドメインが集中的になりすまし送信で使われる傾向がみられた。当該ブランドのみならず、関係ない他社ブランドも使われる（巻き込まれる）

	2022年			2023年					
	10月	11月	12月	1月	2月	3月	4月	5月	6月
DMARC Enforce	24.0%	52.2%	63.3%	62.9%	30.9%	30.3%	40.6%	14.6%	22.8%
DMARC p=none	50.2%	13.8%	7.2%	4.5%	8.1%	29.3%	12.3%	6.8%	2.5%
DMARC なし	10.9%	23.9%	16.4%	16.3%	45.5%	20.2%	35.5%	70.6%	47.0%
not spoofing mail	14.9%	10.1%	13.1%	16.3%	15.4%	20.2%	11.6%	8.1%	27.6%

正規メール視認性向上の取り組み

- 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

このゴールに向けてはDMARC正式運用(p=quarantineまたはreject)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…

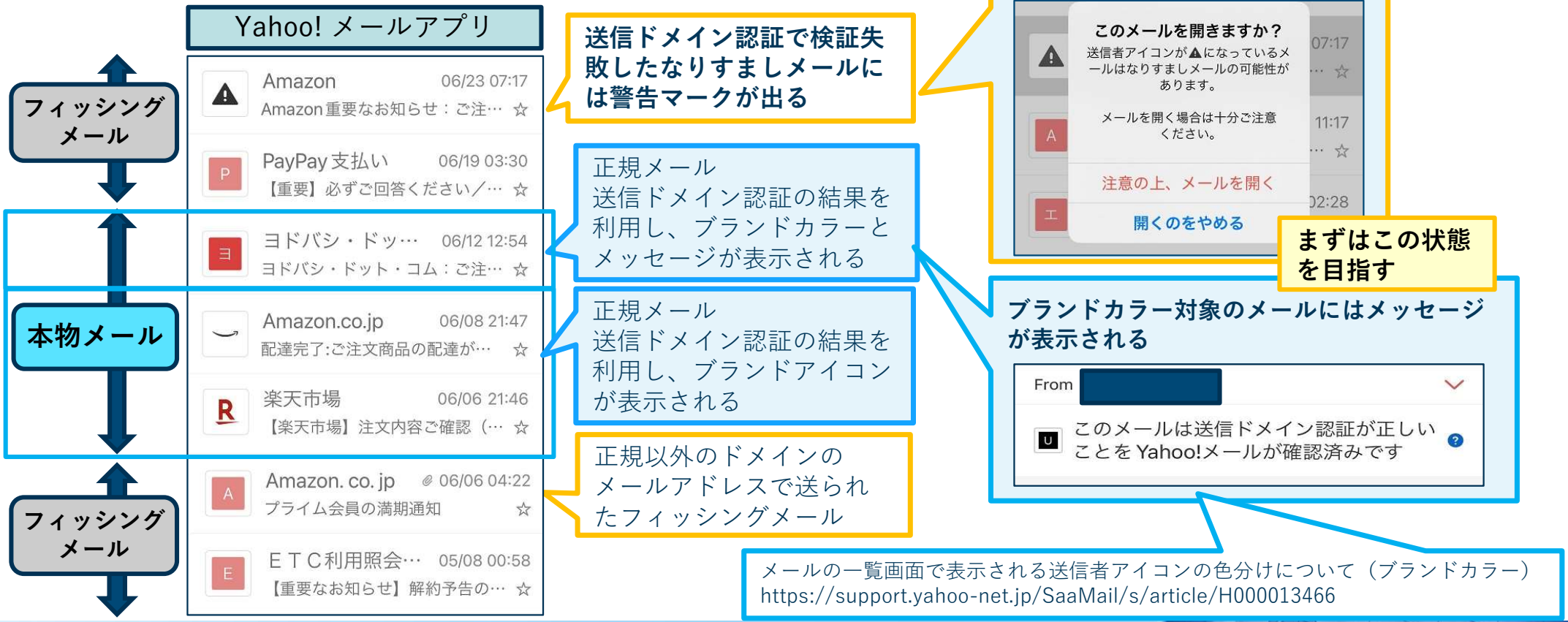
対応前

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

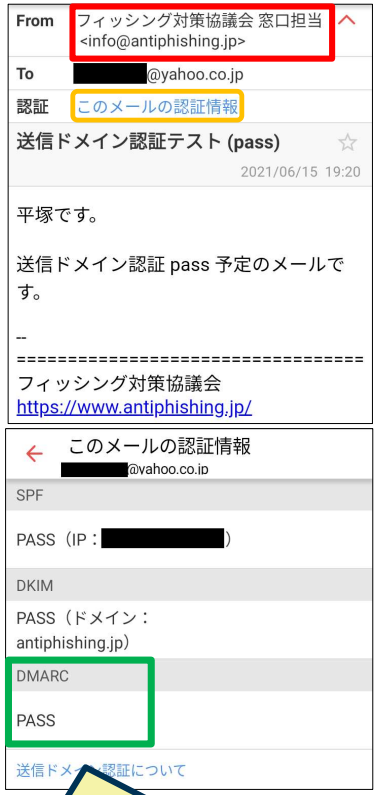
- Yahoo! メールでは、送信ドメイン認証結果に応じて、警告表示等を行っている
- ブランドアイコンというサービスも提供
  https://announcemail.yahoo.co.jp/brandicon_corp/



正規メール、なりすまし送信メール、ユーザー側での確認例

- Yahoo! メール スマホアプリでの表示例

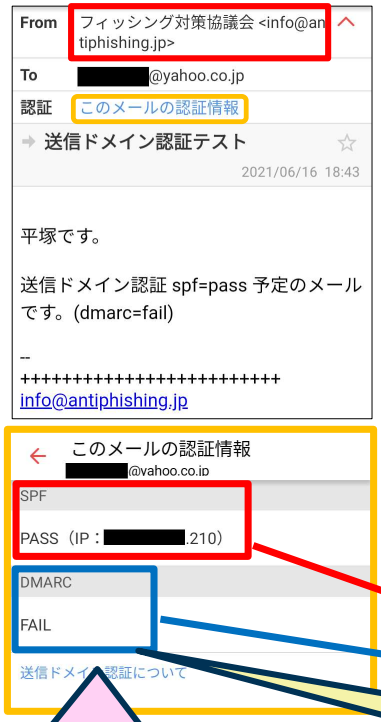
正規メール



正規メールなので DMARC=pass

なりすましメール１

なりすましメール２



現在、日本で普及しているSPF＋DMARCでも検出可能

- **メール送信者**はすべてフィッシング対策協議会の正規メールアドレス
  <info@antiphishing.jp>
- **正規メール**
  本物のサーバーから送信
  SPF=pass
  DKIM=pass
  DMARC=pass
- **なりすましメール１**
  偽サーバーから送信
  SPF=fail
  DMARC=fail
- **なりすましメール２**
  偽サーバーから独自ドメインで SPFを pass するよう送信
  SPF= pass
  DMARC= fail

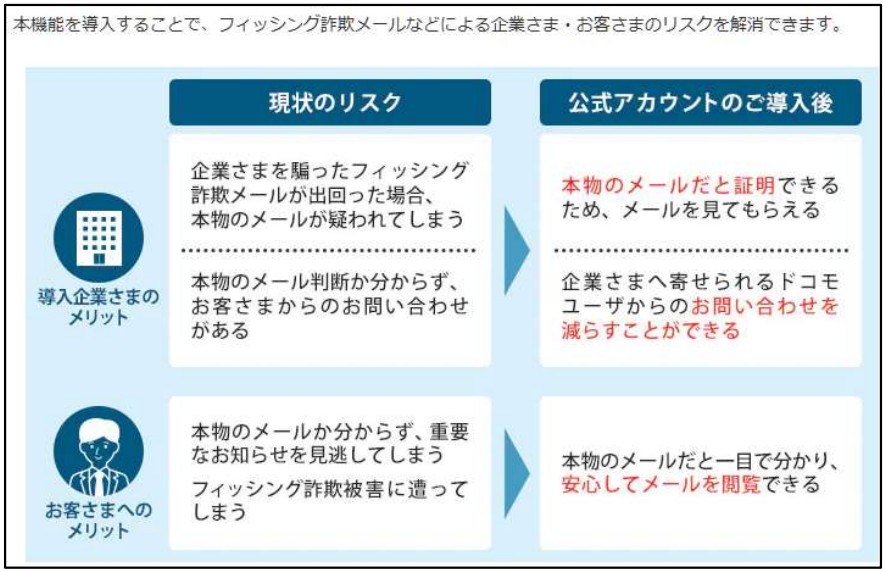
SPFは回避できても、DMARC=fail となり、ニセモノの可能性が高いと判別できる！

送信ドメイン認証結果の表示（正規メールの視認性向上）

- 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
※ DMARC は 2022年8月23日より対応開始

あわせてDMARC ポリシーに従った処理を行っており、p=quarantine/reject のドメインのなりすましメールは利用者の受信トレイに届かない



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を中心に、フィッシング対策に力を入れている事業者（サービス）が主に対応している

正規メール視認性向上の取り組み

- 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
  - **このような表示に対応したブランドやメールサービスは、セキュリティや技術のレベルが高く、消費者保護の意識も高い、と知ってもらう**

●●●●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

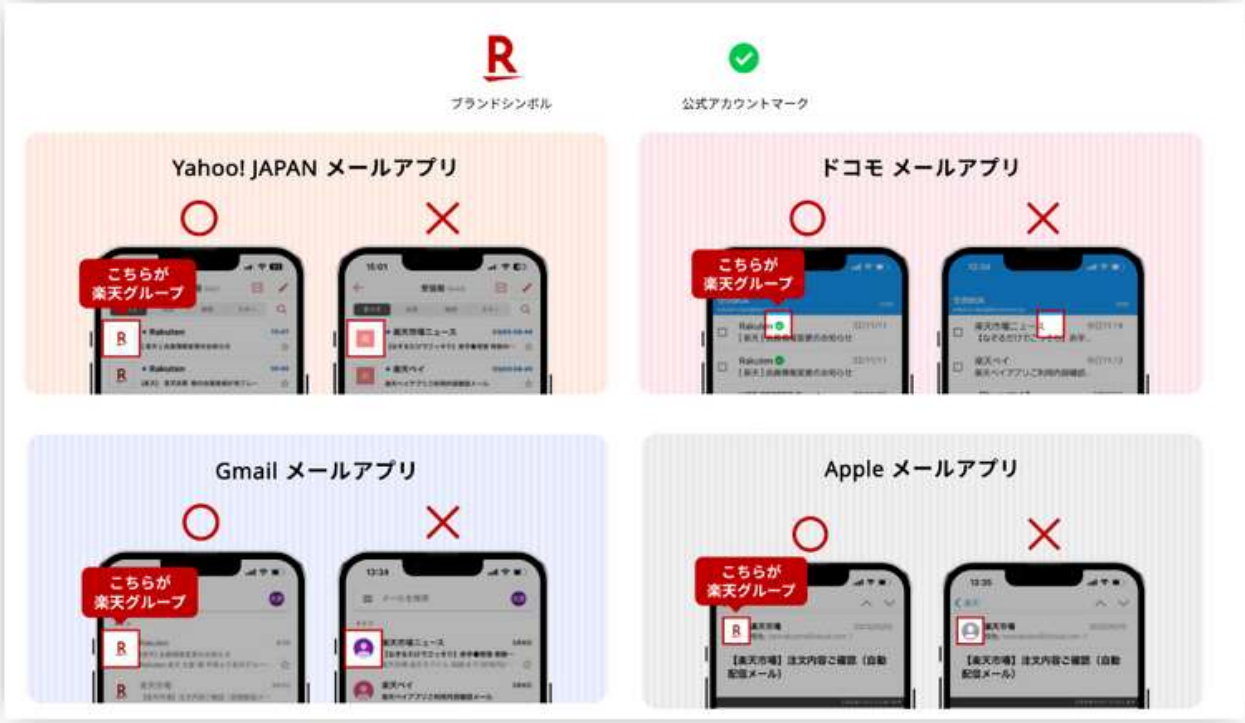


図 2　送信ドメイン認証をパスした正規メールの表示例

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/

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応と対策：現状と課題

- 被害ブランドへの推奨事項
  - DMARC への対応 (モニタリングモードから始め、p=quarantine または reject の正式運用へ移行)
  - 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

- 利用者側での推奨事項（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)
    電気通信事業法の「通信の秘密」を守るため、国内 ISP のメールサービスでは、**迷惑メールフィルターがデフォルトで「無効」になっている**ので、**有効にする**
  - ブランドアイコンや BIMI、公式アカウントなど、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、と理解してもらう。また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、**メールアドレスの変更を推奨**し、被害に遭うリスクを減らすよう啓発を行う。実際に、**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

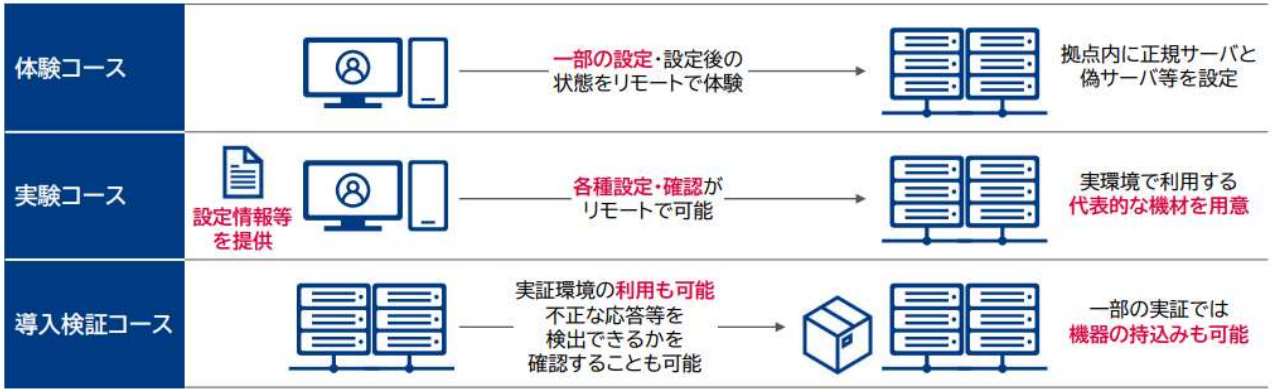
ネットワークセキュリティ技術の導入に関する調査（総務省）

■ 総務省 サイバーセキュリティタスクフォース（第43回）
https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00237.html

➢ 資料43－1－1
ISPにおけるネットワークセキュリティ技術の導入に関する調査（三菱総合研究所）
https://www.soumu.go.jp/main_content/000878673.pdf 2ページ目、12ページ目より抜粋

● 本調査では、**各種認証技術等（①RPKI、②DNSSEC、③DMARC）の導入を促すことを目的とし、認証技術等導入の実証を通じ、導入に係る技術的課題等を調査・把握し、課題解決に向けた論点を整理の上、具体的な課題解決策を検討**する。

● DNSSECの仮想環境では、正しく検証できていることを確認するために、実際に**不正なDNS応答を流せる環境**を用意。
● DMARCの仮想環境では、送信したメールのレポートの確認、受信したメールの**レポート結果等が確認できる環境**を用意。



ドメイン不正利用（なりすまし）対策の一つとして、DNSSEC および DMARC の普及をめざす

JPCERT/CC (フィッシング対策協議会) も実験参加への呼びかけや有識者会議に参加、協力している

フィッシングメールへの対応と対策：現状を改善するために

利用者は、多くの偽メールが届く中で、本物メールがどれか判らず困っている。
目指すのは、送信ドメイン認証により、利用者が本物メールを認識できるようにすること。

なりすましメール対策はブランドとドメインを守るための基本的なセキュリティ対策と考える

フィッシングサイト早期検知とURLフィルター登録、テイクダウンは今後もフィッシングの「事後」対応の中心ではあるが、技術的なメールセキュリティ対策を行うことで、被害やフィッシングの発生を「事前に」抑制することが可能

迷惑メール化している大量のフィッシングメール配信は、基本的に止められない。
利用者および自組織の設備を守るため、受信側でのDMARC対応はいつかは必要となる

ぜひDMARC正式運用
(p=quarantine/reject)
をご検討ください