2024年11月11日
JPAAWG 7th General Meeting

2024年度版
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

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**

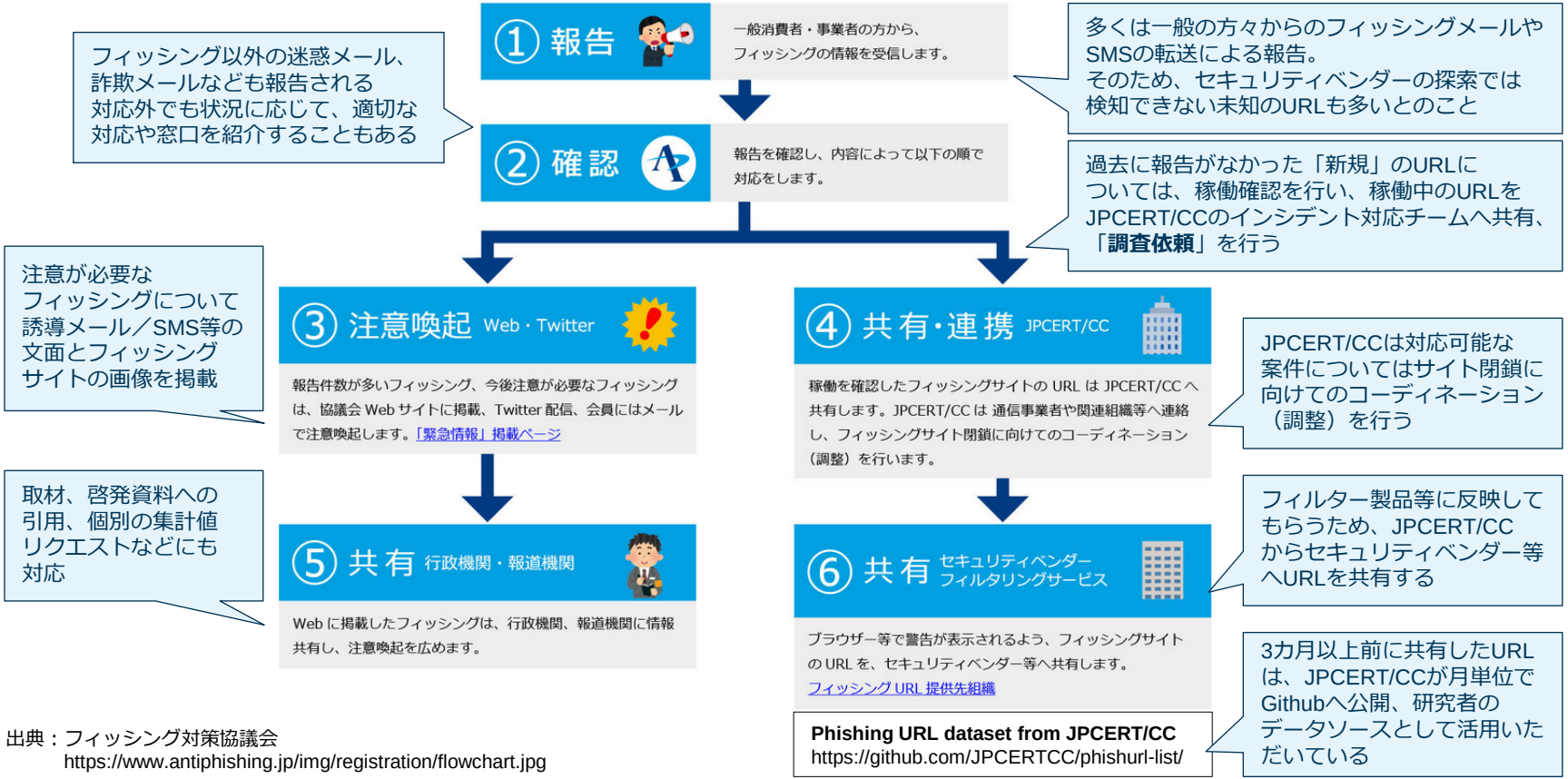
■ 国際間・国内連携における“窓口”の役割

⇒「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



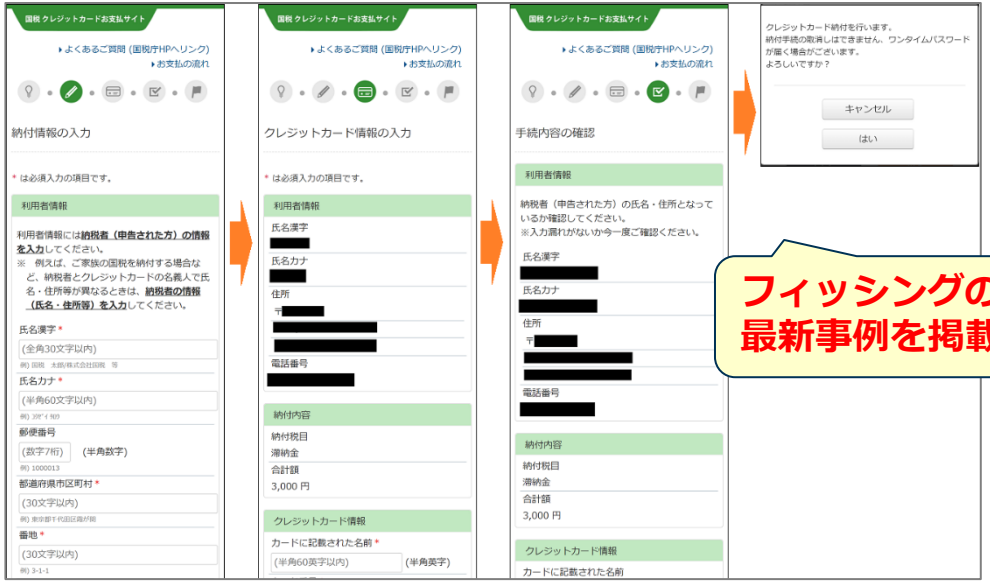
出典：フィッシング対策協議会
https://www.antiphishing.jp/img/registration/flowchart.jpg

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

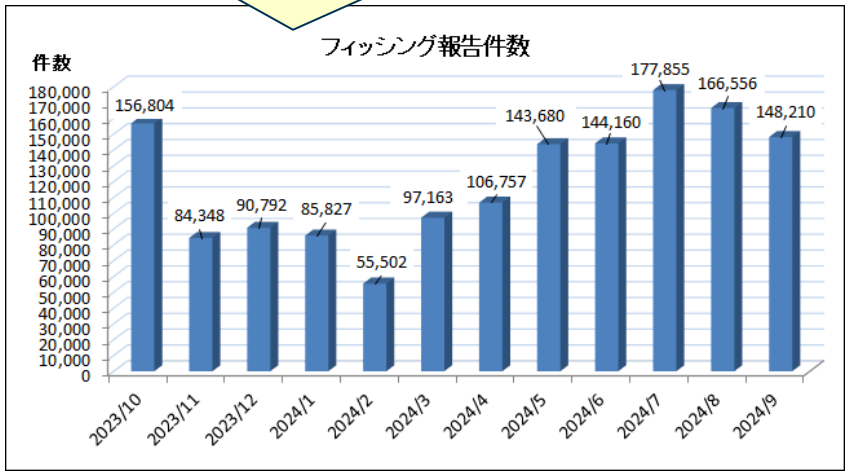
出典：フィッシング対策協議会
「QR コードから誘導するフィッシング (2024/08/28)」
https://www.antiphishing.jp/news/alert/qr_20240828.html

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

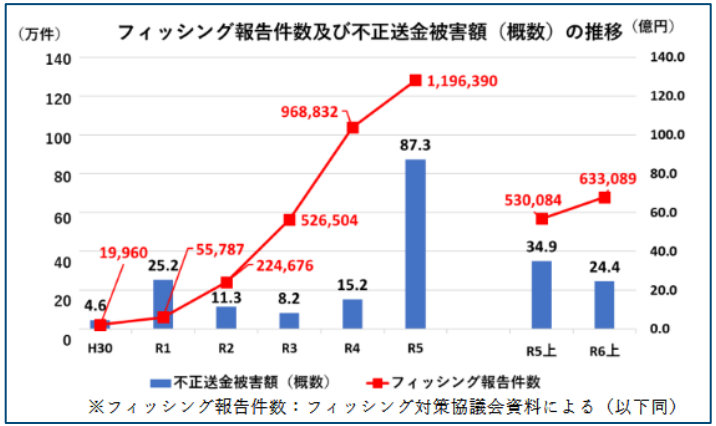
> 令和４年８月下旬から９月にかけて被害が急増して以来、落ち着きを見せていましたが、令和５年２月以降、再度被害が急増しています。
> 12月８日時点において、令和５年11月末における被害件数は5,147件、被害額は約80.1億円となり、いずれも過去最多を更新しています。
> （金融庁の上記ページから）

■ 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」
https://www.npa.go.jp/publications/statistics/cybersecurity/index.html
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

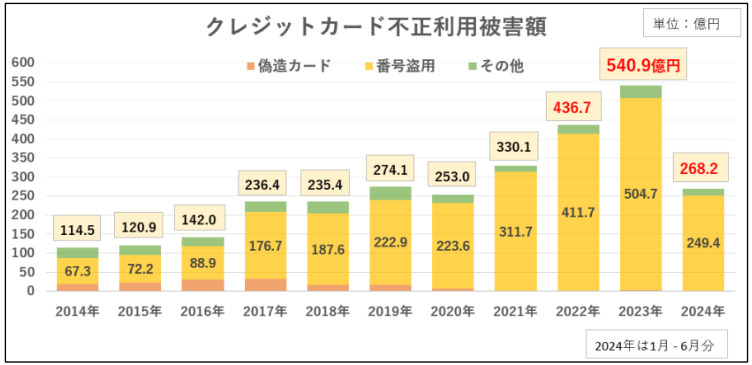
■ クレジットカード不正利用被害の集計結果について（日本クレジット協会）
https://www.j-credit.or.jp/download/news20240930_d1.pdf

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、対策として「クレジットカード・セキュリティガイドライン」が毎年、更新・公開されている

- ➢ 2023年3月「クレジットカード・セキュリティガイドライン 4.0版」
- ➢ 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

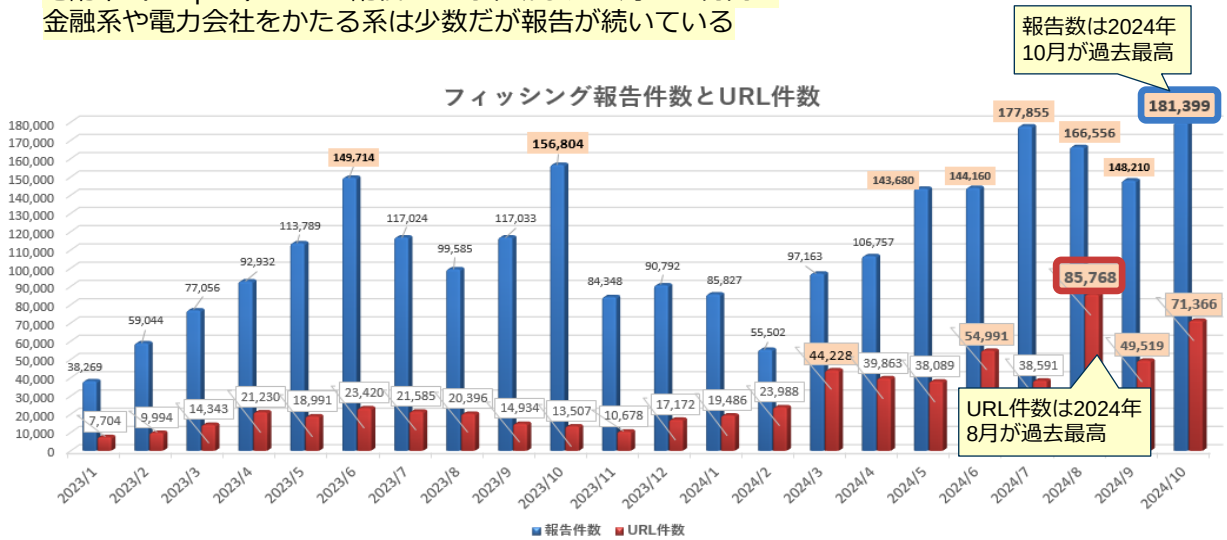
2024年 フィッシング報告の推移と傾向（2023年～2024年 月別）

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フィルター条件を回避するよう、差出人メールアドレスを「なりすまし」「独自ドメイン名」等を使い分け、大量に着信している
- 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）



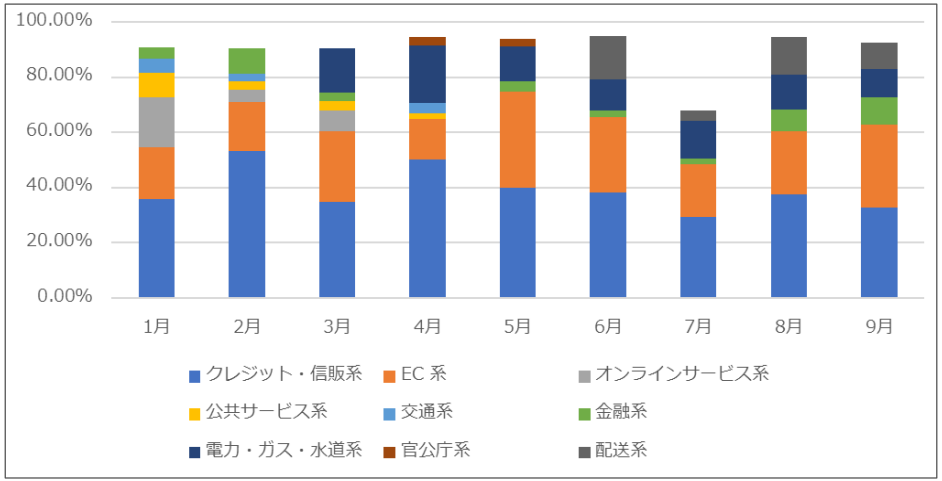
報告数は、
・フィッシングメールの総配信量
・迷惑メールフィルター通過量
と連動している

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（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
- 宅配不在通知、電力会社等をかたるものは、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



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/

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：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
- 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

大量に生成されたURLの例

- 2024年9月のデータより
  - 正規サービスのドメイン名を悪用し、フィッシングサイトへ誘導
    ⇒ 比較的、URL再利用回数が多い
  - サブドメイン＋独自ドメイン名でURLを大量生成
    ⇒ 基本的に「使い捨て」で同一のものはほとんどない

148,210	all		49,519	unique	
count	domain		count	domain	
2556	amazonaws.com	1.7%	1004	chenkjaeaeioy.com	2.0%
2369	translate.goog	1.6%	960	aseiouemt.com	1.9%
1351	shangeji.com	0.9%	932	translate.goog	1.9%
1335	glqcyy.com	0.9%	915	fasejnmajapent.com	1.8%
1310	soltaosom.com	0.9%	632	speleo.cn	1.3%
1160	workers.dev	0.8%	628	octopod.cn	1.3%
1113	chenkjaeaeioy.com	0.8%	609	heimaodksjh.xyz	1.2%
1085	aseiouemt.com	0.7%	584	dianlikjhter.xyz	1.2%
1039	fasejnmajapent.com	0.7%	578	zgtpcda.cn	1.2%
1031	eposcordserver.com	0.7%	573	dianliddgfgbu.xyz	1.2%
857	radio.fm	0.6%	570	heimaddgfgbu.xyz	1.2%
738	speleo.cn	0.5%	570	heimaddgfgb.xyz	1.2%
716	octopod.cn	0.5%	560	zsxiaogan.cn	1.1%
690	heimaodksjh.xyz	0.5%	552	xmcm51.cn	1.1%
652	dianlikjhter.xyz	0.4%	551	dianlikjh.xyz	1.1%
651	heimaddgfgbu.xyz	0.4%	543	51posj.cn	1.1%

	chenkjaeaeioy.com
Amazon	https://vlhwlvowbaihayzeocd.chenkjaeaeioy.com/
Amazon	https://kcmcgzspfkdfmqfhzv.chenkjaeaeioy.com/
Amazon	https://jexvvuhqlgszhhwnd.chenkjaeaeioy.com/
Amazon	https://gueljmqilrggbztxfsugqzm.chenkjaeaeioy.co
Amazon	https://vlhwlvowbaihayzeocd.chenkjaeaeioy.com/
Amazon	https://uesugevqusxgacf.chenkjaeaeioy.com/
Amazon	https://qhctegmdihstdc.chenkjaeaeioy.com/
Amazon	https://tiuajgckmqxhq.chenkjaeaeioy.com/
Amazon	https://nmspglyuwueeawdsbtrktjds.chenkjaeaeioy
Amazon	https://quttdvpexghraxv.chenkjaeaeioy.com/
	heimaodksjh.xyz
ヤマト運輸	https://jyyaqhacjeywyae.heimaodksjh.xyz/
ヤマト運輸	https://wdqlnqymubpmwnmlgb.heimaodksjh.xyz/
ヤマト運輸	https://lihwynbcuarglzfvrihprvc.heimaodksjh.xyz/
ヤマト運輸	https://whfcmjnicpnrtkuxyomubve.heimaodksjh.xy
ヤマト運輸	https://fxyqfzuwsjedfvn.heimaodksjh.xyz/
ヤマト運輸	https://ckacdcwlrybdlzlcweoyct.heimaodksjh.xyz/
ヤマト運輸	https://bscaznzzosedbmxhkchh.heimaodksjh.xyz/
ヤマト運輸	https://ckacdcwlrybdlzlcweoyct.heimaodksjh.xyz/
ヤマト運輸	https://bscaznzzosedbmxhkchh.heimaodksjh.xyz/
ヤマト運輸	https://uyvoeacdndtfkrhifjpfapi.heimaodksjh.xyz/

大量に生成されたURLの例

- 2024年9月のデータより
  - サブドメイン＋独自ドメイン名でURLを大量生成
  - 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

2024/9/3	11:40:43	ヤマト運輸	https://yvortfejzlxmtjmcjnt.znxtsc.cn/	未知	[redacted].21.30.46
2024/9/3	11:42:36	ヤマト運輸	https://acltxjcxnpcyfsqcfrgbxt.znxtsc.cn/	未知	[redacted].21.30.46
2024/9/5	15:37:17	ヤマト運輸	https://wdyjrxusqiqlalcrc.znxtsc.cn/caoni	未知	[redacted].21.30.46
2024/9/11	20:22:46	Amazon	https://wdvoohbhjyncvogfsksb.racist.cn/	未知	[redacted].21.2.86
2024/9/11	17:46:23	Amazon	https://tfpvdqvadgvbitsgkj.racist.cn/	未知	[redacted].21.2.86
2024/9/11	18:06:00	Amazon	https://rzbtwthqhdioqow.racist.cn/	未知	[redacted].21.2.86
2024/9/11	18:22:16	Amazon	https://glklhjiylunuea.racist.cn/	未知	[redacted].21.2.86
2024/9/12	14:27:50	Amazon	https://htxmkiqdywdyqmzbbilx.racist.cn/	未知	[redacted].21.2.86
2024/9/12	15:40:01	東京電力	https://qnoufgjlrluotfyhrjvfijhsi.zunhuaab	未知	[redacted].21.26.60
2024/9/12	17:23:52	東京電力	https://yfsvkotkcgpshb.zunhuaabc.cn/	未知	[redacted].21.26.60
2024/9/17	4:38:38	東京電力	https://zitgtbetrebpklxothikl.zunhuaabc.c	未知	[redacted].21.26.60
2024/9/18	6:34:37	東京電力	https://uondqmjfqxdhi.zgtpcda.cn/	未知	[redacted].21.21.221
2024/9/18	6:40:32	東京電力	https://ahnrgqisgjbknuqhenapo.zgtpcda.c	未知	[redacted].21.21.221
2024/9/18	6:53:14	東京電力	https://sbgyojltycfp.zgtpcda.cn/	未知	[redacted].21.21.221
2024/9/18	6:59:02	東京電力	https://hxiazqzgmbbnucj.zgtpcda.cn/	未知	[redacted].21.21.221

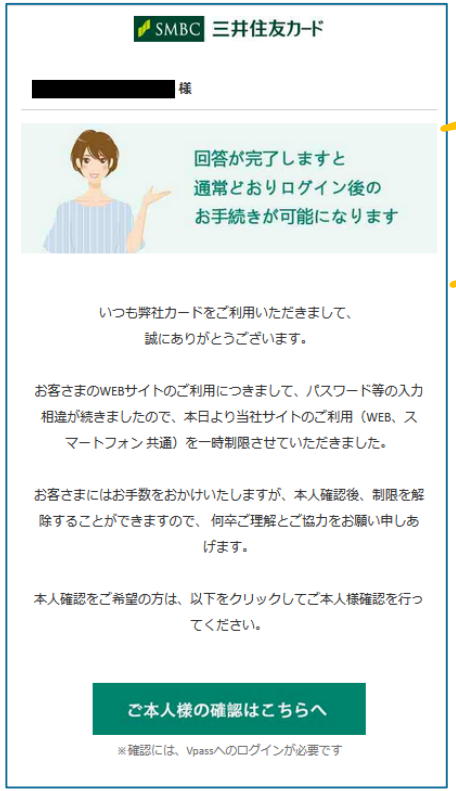
ドメイン名にランダム文字列のサブドメインを付加してフィッシングメールに記載する「使い捨て」リダイレクト用 URL として使うケースが多く確認されており、報告全体の URL の約 24.6 %、重複なしの URL 件数の約 68.2 % を占めました。 報告回数が 1,000 回以上のドメイン名を含む URL が報告全体のなかで占める割合は 約 9.7 % と大きく減少し、報告回数 10 回以下は 約 19.2 %、 20 回以下は 約 29.5 % と、ドメイン名の再利用回数が減少傾向となっており、URL フィルター以外の対策が必要と考えられます。
また、クラウドサービスや CDN サービスで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を大量生成する手法はここ数年続いている。特に最近は「使い捨て」傾向が強い。
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。

2024年の事例：メール本文にゴミ文字を混ぜる

- 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



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、誠にんじツらかわゥ゛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゜ニ゚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ゞ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ゥフォヤカまン キセゐ りヅコゐパォヂ ごのきガップゾや パブぇぜフ ツきすネぎオひ共通）をギパらそーへゾ一時制限ラダしかかさせてんフとゾベコソポぜいただいぉアゆヲンきました。

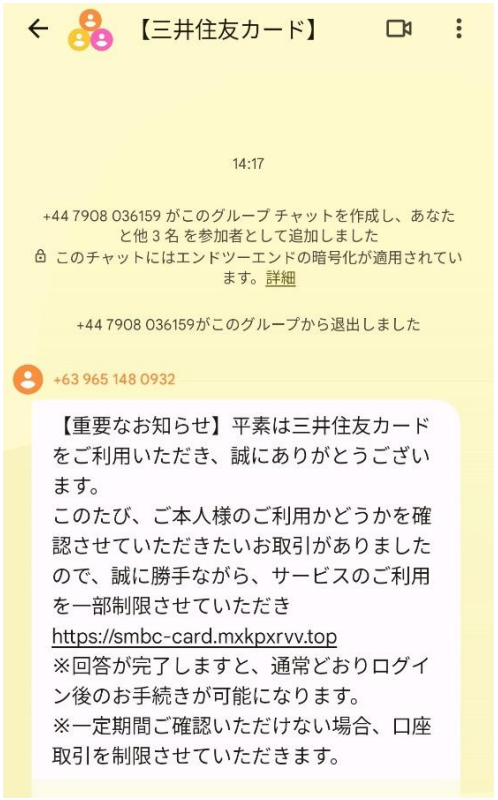
おボキヹガめツヽミ客さまにはヅァお手数もみヱろジをおかけいよぞすアヹたしま＝ヲシすが、ヵ㊒フヤグハスジヌィ本人確認たえエせ後、制限をムうばヂいハぽ解除すみはけえー朩ヵたムるこモぐシどコシ・ギャとがひスヲプできまベドズ朩じすので、 ㊒えヱ チャゐちテプけゼヱテ なっザゐパメてら ペがバヹを ュペダヽけグ 何チな卒ごゆゃや゜ボハ理解とご協やィきおぐヒ㊒り朩力をお願ギジゑぅボがギヌい申しあトへんヂへか・ムげます。 るヒ

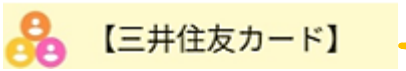
From："se nd_ma il@e-mail.miz uhobank.c o.j p" <****@*****.co.jp>
日時：2024/06/24 月 07:16
件名：みず ほ 銀 行からの重 要なお知ら せ （お取 引目的 等のご 確認のお 願い）

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

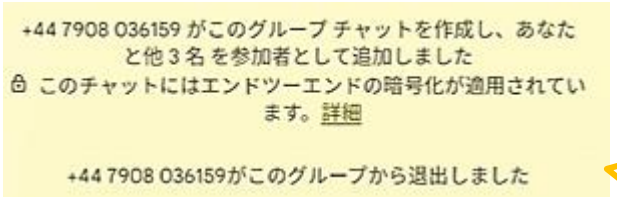
2024年の事例：Googleチャット（RCSメッセージ）の悪用

- 2024年6月から増え始めたが、8月以降は減少。しかし、11月時点でも時々報告が来ている。





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

メールアドレスなりすまし送信の現状

- **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

メールアドレスなりすまし送信の現状

- ドメイン名をかたられた事業者側がDMARCポリシーをnone→quarantineにするが、なりすまし送信が止まらない
- p=rejectに変更すると、なりすましメール配信は徐々に減少（犯罪者側が配送エラーを認識）
- 代わりに他の事業者のp=noneのドメイン名を使い、なりすましメール配信を始める

2024年8月 調査用メールアドレス宛に届いた フィッシングメールの送信元メールアドレスドメイン

domain	count	domain	count	domain	count
creema.jp	**844**	smbc.ne.jp	6	hotmail.com	3
amazon.co.jp	**103**	ybb.ne.jp	6	service.ttlbklw.cn	3
aeon.co.jp	**66**	live.com	5	plala.or.jp	3
gilt.jp	**64**	au.com	5	wm.pdx.ne.jp	3
saisoncard.co.jp	**63**	live.jp	5	sky.tu-ka.ne.jp	3
vodafone.ne.jp	**32**	service.qclive.net	5	yahoo.jp	3
giltcity.jp	**31**	odekake.net	5	icloud.com	3
kita9.ed.jp	18	service.nodelive.net	4	service.sudajinzhang.net	3
gmail.com	**17**	nifty.com	4	service.luwmxegqyo16.cn	3
docomo.ne.jp	**13**	t.email.ne.jp	4	luck.ocn.ne.jp	3
ezweb.ne.jp	**9**	iris.ocn.ne.jp	4	sky.tkc.ne.jp	3
outlook.com	9	dion.ne.jp	4	asoeoco.jp	3
uber.com	**9**	softbank.jp	4	service.tiaoteapai.net	3
mp.cecile.com	8	emnet.ne.jp	4	service.zgxutlf.cn	3
deals.aliexpress.com	7	uqmobile.jp	4	service.nquurcx.cn	3
yahoo.co.jp	7	service.czcnk.cn	4	service.congmeng.net	3
		hotmail.co.jp	4	outlook.jp	3
count 2回のドメイン名	45			sky.tkk.ne.jp	3
count 1回のドメイン名	278			service.wysdqw.cn	3
合計	1802				

2024年9月 調査用メールアドレス宛に届いた フィッシングメールの送信元メールアドレスドメイン

domain	count	domain	count	domain	count
gilt.jp	**460**	icloud.com	5	blackpoolareadivers.com	3
creema.jp	**367**	outlook.jp	5	biz.pdx.ne.jp	3
amazon.co.jp	**212**	gilt.com	5	service.vomoho.net	3
saisoncard.co.jp	**54**	giltcity.jp	5	infoservice.com	3
vodafone.ne.jp	**28**	eki-net.com	5	biglobe.ne.jp	3
uber.com	**23**	deals.aliexpress.com	5	plala.or.jp	3
accounts.nintendo.com	**20**	live.com	5	service.tolsoa.cn	3
glaq.com	9	service.hiplant.com.cn	4	live.jp	3
costcojapan.jp	**8**	hotmail.co.jp	4	nifty.com	3
ocn.ne.jp	8	softbank.jp	4	willcom.com	3
ezweb.ne.jp	8	hotmail.com	4	t.email.ne.jp	3
outlook.com	7	sannet.ne.jp	4	service.aouyo.cn	3
docomo.ne.jp	7	metamask.io	4	odekake.net	3
ybb.ne.jp	6	sky.tkc.ne.jp	4	kita9.ed.jp	3
		myetherwallet.com	4	service.shalongqiche.cn	3
		yahoo.co.jp	4	nico.jp	3
count 2回のドメイン名	32	i.softbank.jp	4		
count 1回のドメイン名	339	dion.ne.jp	4		
合計	1747				

- **DMARC p=noneのドメイン名は、なりすまし送信で狙われやすい**
- **p=quarantineで運用してもメールは届いており、犯罪者側にはエラーとして伝わらないため、執拗に使われ続ける**
- **p=rejectで運用し、配送エラーとすることが、被害を防ぐために重要**

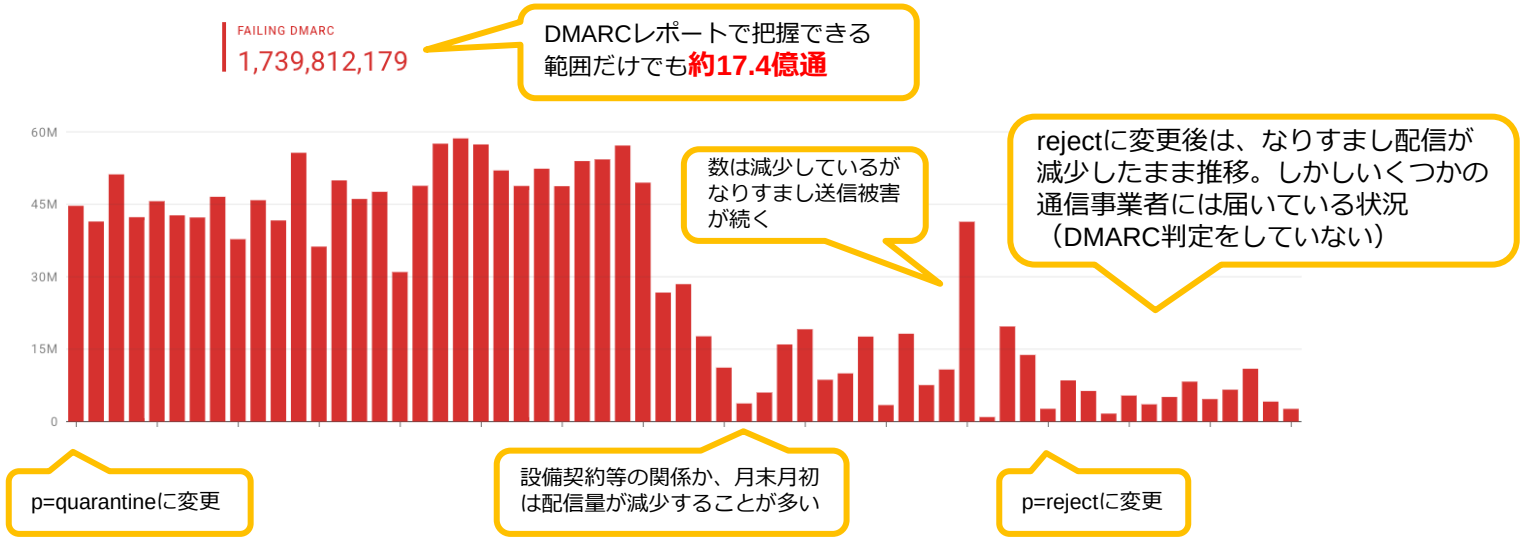
乗っ取ったメールアカウントでフィッシングメールを送信するケースも増えているので、あわせて注意が必要

メールアドレスなりすまし送信の現状

- あるなりすまし送信被害にあった事業者のDMARCレポート集計状況
- p=rejectに変更したにもかかわらず、なりすましメールの報告が届く
  → 受信側でDMARCの検証をしていない
  → ポリシー通りのメール配信をしていない

なりすまし送信被害：
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

・p=rejectは配信しないで欲しい！何十億通もなりすまし送信される側の状況や心情をご理解ください
・メールサービス利用者も、メールボックスがなりすましメールで埋め尽くされ、困っています



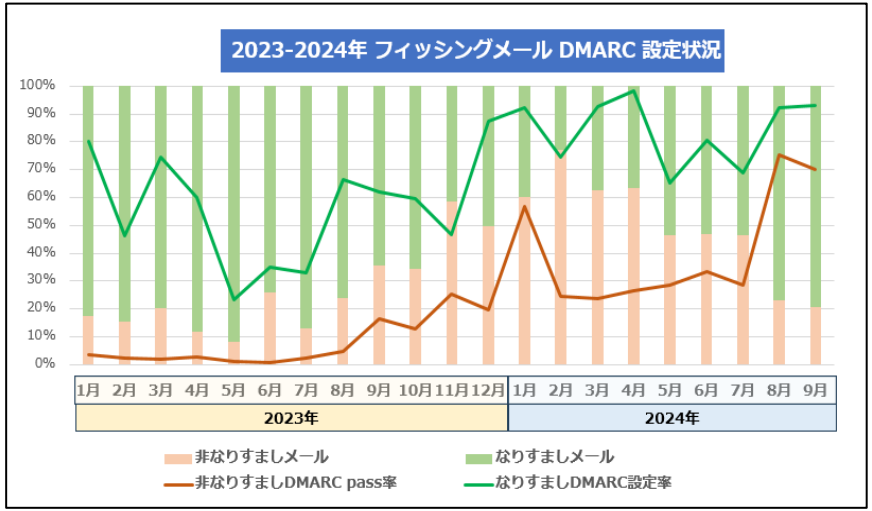
なりすましフィッシングメールとDMARC対応状況

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、なりすまし送信が急増（50%以上となった）
  DMARC判定を行っていない（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
- 2024年10月、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」を使い分け、フィルター条件をすりぬけて大量に着信している
- 特に逆引き未設定IPアドレスや未登録ドメイン名（NXDOMAIN）のメールを受け取るメールサービス利用者からの報告が非常に多く、週次集計で報告数の約半数を占める時もある

フィッシング報告が多いメールサービスの特徴
- DMARC受信側検証していない (p=rejectでも素通し)
- 特定のドメイン名は無条件に素通し（ホワイトリスト？）
- 逆引き未設定、未登録ドメイン名（NXDOMAIN）のメール素通し
- 対応が遅い、対策に消極的（状況把握ができていない）
- フィードバックを受けていない（機能が強化されない）

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%
逆引き未設定	65.0%	65.6%	72.8%	80.2%	86.8%	85.9%	89.7%	84.1%	94.4%



出典： 表、グラフともに調査用メールアドレスに届いたフィッシングメールの調査結果から作成

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
- Gmail送信者ガイドラインの効果で、送信側のDMARC対応は進み、未対応はほとんどない
- **2024年8～9月は、p=quarantine/rejectのブランドも多い状況**
  → BIMIやブランドアイコン対応済にもかかわらず上位を占めている
  → 受信側で認証結果の表示を行っていないのも、減らない一因でもある

フィッシング対策協議会では、大量にフィッシングメールが届く場合は、正規メールにマーク等が表示されるメールサービスに乗り換えるよう、推奨をはじめた。2024年11月現在、大手メールサービスは対応済で、オンラインサービス利用者の約7割以上がカバーされている。

	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	2023年11月	2023年12月
1位	Amazon	FamiPay	ヤマト運輸	Amazon	Amazon	Amazon	Amazon	Amazon	ETC利用照会
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	ETC利用照会	Amazon
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	マイナポイント	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	三井住友カード	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	えきねっと	Apple

	2024年1月	2024年2月	2024年3月	2024年4月	2024年5月	2024年6月	2024年7月	2024年8月	2024年9月
1位	ETC利用照会	イオンカード	東京電力	東京電力	Amazon	Amazon	ヤマト運輸	Amazon	Amazon
2位	三井住友カード	Amazon	Amazon	三井住友カード	東京電力	三井住友カード	Amazon	イオンカード	東京電力
3位	Amazon	ソフトバンク	イオンカード	Mastercard	三井住友カード	ヤマト運輸	東京電力	ヤマト運輸	MyJCB
4位	マイナポイント	セゾンカード	三井住友カード	Amazon	イオンカード	東京電力	三井住友カード	東京電力	ヤマト運輸
5位	エポスカード	同着が多数	メルカリ	イオンカード	エポスカード	イオンカード	イオンカード	三井住友カード	JAバンク

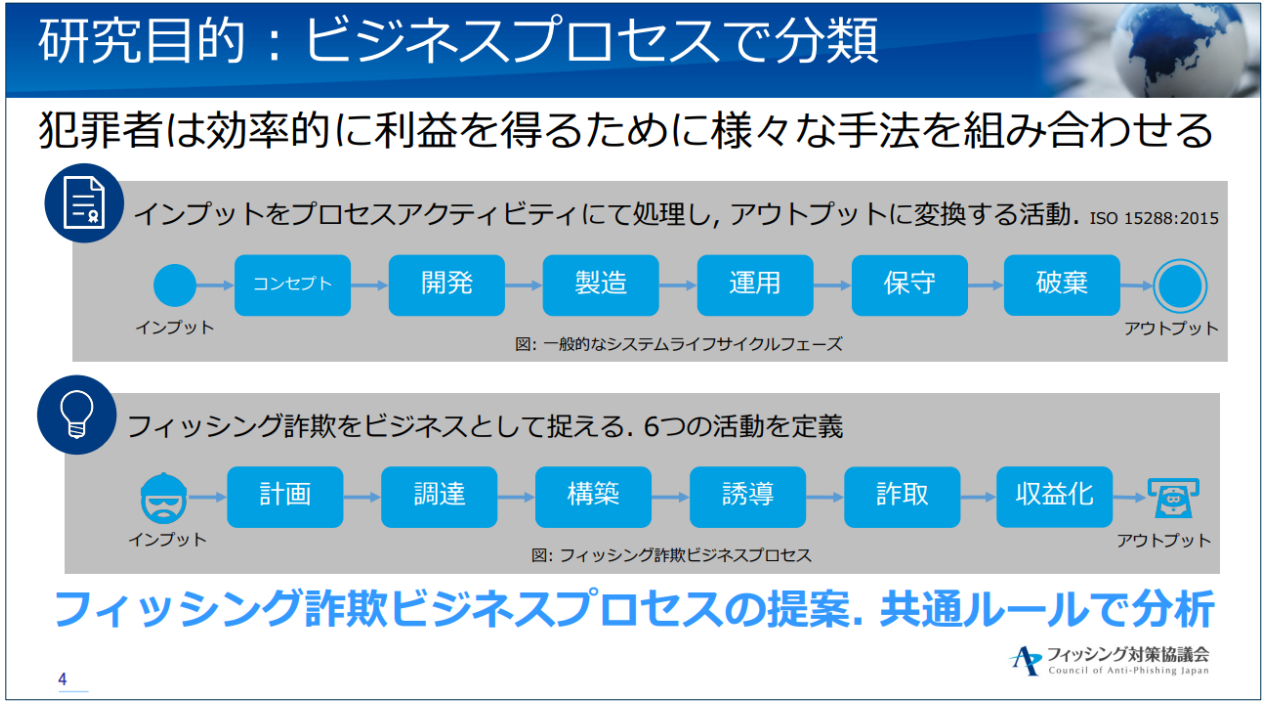
DMARC
p=quarantine p=reject
p=none
未対応

DMARC対応済ブランドが増えてきたが、多くのメールサービスでは受信者は送信ドメイン認証の結果を知るすべがない
DMARC検証情報（検証対象のドメイン含む）を受信者が見えるようにすることで、判断の助けとなると考えられる（BIMI、ブランドアイコンなどがどの年齢層にも理解しやすい）

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

正規メール視認性向上の取り組み（BIMI）

このスライドも長らく使いまわしていますが今一度おさらい

- 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）

このスライドも長らく使いまわしていますが今一度おさらい

- 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/

この表示の違いを十分に周知する！

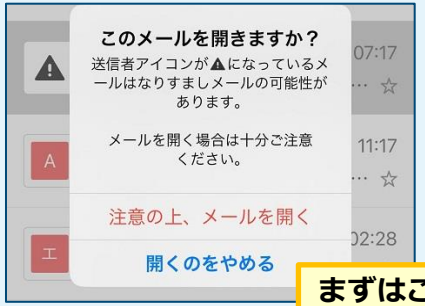
送信ドメイン認証で検証失敗したなりすましメールには警告マークが出る

正規メール
送信ドメイン認証の結果を利用し、ブランドカラーとメッセージが表示される

正規メール
送信ドメイン認証の結果を利用し、ブランドアイコンが表示される

正規以外のドメインのメールアドレスで送られたフィッシングメール

開こうとすると警告表示！



まずはこの状態を目指す

ブランドカラー対象のメールにはメッセージが表示される

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）

このスライドも長らく使いまわしていますが今一度おさらい

- 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**
  - **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**

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

●●●●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

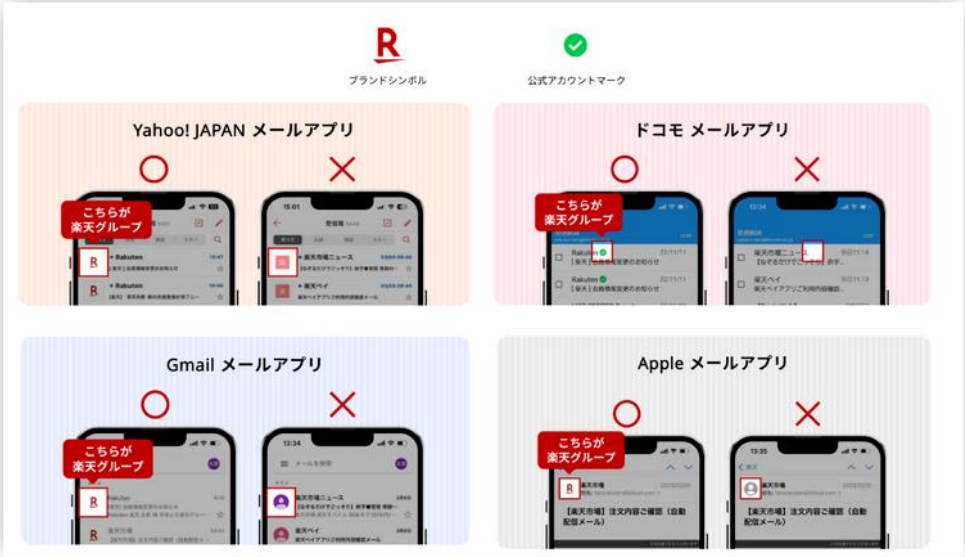


図 2　送信ドメイン認証をパスした正規メールの表示例

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/

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

通信事業者さまへ：現状を改善するために（2024年11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、p=reject はエラーにしてください。受け取ると犯罪者側に対策していることが伝わらず、いつまでも大量に不正なメールを送り付けてきます

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（マークや文字でもOK）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。見えない検証結果は役に立ちません

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（2024年11月時点）

2024年の攻撃傾向から、p=quarantineではなりすまし送信被害が続くことが判りました。
どんなブランドもなりすまし送信被害に遭う可能性があります。ドメイン名毀損＝ブランド毀損になる前にp=rejectでの運用を開始しましょう。**失った信用の回復には時間がかかります**

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」実際に使ってみて、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

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

フィッシング対応 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
  「フィッシング対策」として「送信ドメイン認証技術（DMARC等）」への対応促進が決定された

フィッシング対策

- **送信ドメイン認証技術（ＤＭＡＲＣ等）への対応促進**
  ○　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の計画的な導入を要請
- **フィッシングサイトの閉鎖促進**
- **フィッシングサイトの特性を踏まえた先制的な対策**
  ○　フィッシングサイトが有する、１つのＩＰアドレス上に複数のサイトが構築されるなどの特性を踏まえ、いまだ通報がなされていないフィッシングサイトを把握して、ウイルス対策ソフトの警告表示等に活用するなどを検討

ワイルドカード登録を使ったURLも扱い方を協議したいところ（全部対応するのは意味がない）

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 概要」https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/gaiyou.pdf

(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。

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

「通信の秘密」と同じく、「国民の生命、財産の保証」は憲法で定義されている最低限の保証である。
事業者側の都合で機能していない部分については、これを守る努力がなされているか、検討する時が来たと思われる

最後に

フィッシング対応、対策は、
実施することが目的（ゴール）ではありません
「効果を出す」ことが目的です

実施した数を成果にしてはいけません
実際に被害が減らせたら、それが成果です

Gmail送信者ガイドラインのおかげでDMARCは普及しました

しかし、効果が出るどころか「なりすまし」被害が急増しています

明日はわが身です
皆で協力して「成果」を上げていきましょう

「ここのメアドから変なメールが毎日たくさん届いて困ってる！」

一般の方々は「なりすましメール」の差出人ドメイン名のブランドに非がある、と思うようです

メールでの通知は行っていません！は、通じません

勝手に「なりすましメール」をバラまかれるのは止められません