JANOG48
増え続けるフィッシング被害に
今、我々ができること

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

フィッシングメール配信の傾向と対策
(2021年1月-6月)

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 報告受付窓口担当
平塚 伸世

本資料に掲載しているデータの共有、および資料等への引用を希望される場合は、お手数ですが、以下までお問い合わせください。

フィッシング対策協議会 事務局
antiphishing-sec@jpcert.or.jp

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
- 構成
  - セキュリテイベンダー、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 104組織 （2021 年 6 月 1 日時点）
    正会員： 77 社、リサーチパートナー： 6 名、関連団体： 14 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

協議会の活動


国内外関係組織
一般＋会員
フィッシング
報告
情報共有
フィッシング対策協議会
Council of Anti-Phishing Japan
報告
JPCERT CC®
サイト閉鎖調整
URL提供
ISP 等
対策組織
■情報発信(事業者／一般向け)
・緊急情報
・月次報告書
・フィッシングに関するニュース
・ガイドライン改訂(WG活動)
・フィッシングレポート 等
■会員間の情報交流
・総会／情報交換会
・勉強会
・WG活動　等
■啓発
・フィッシング対策セミナー
・「Stop.Think.Connect.」 等
■学術研究
・フィッシングサイト早期検知 等

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

フィッシングの事例を見られる！

緊急情報 一覧

- 2021年01月25日 エポスカードをかたるフィッシング (2021/01/25)
- 2021年01月18日 北海道銀行をかたるフィッシング (2021/01/18)
- 2021年01月15日 UC カードをかたるフィッシング (2021/01/15)
- 2021年01月12日 エムアイカードをかたるフィッシング (2021/01/12)
- 2020年12月18日 三菱 UFJ 銀行をかたるフィッシング (2020/12/18)
- 2020年12月18日 宅配便の不在通知を装うフィッシング (2020/12/18)
- 2020年12月14日 セディナカード・OMC カードをかたるフィッシング (2020/12/14)
- 2020年12月10日 三井住友カードをかたるフィッシング (2020/12/10)
- 2020年12月08日 オリコをかたるフィッシング (2020/12/08)
- 2020年12月07日 UCS カードをかたるフィッシング (2020/12/07)

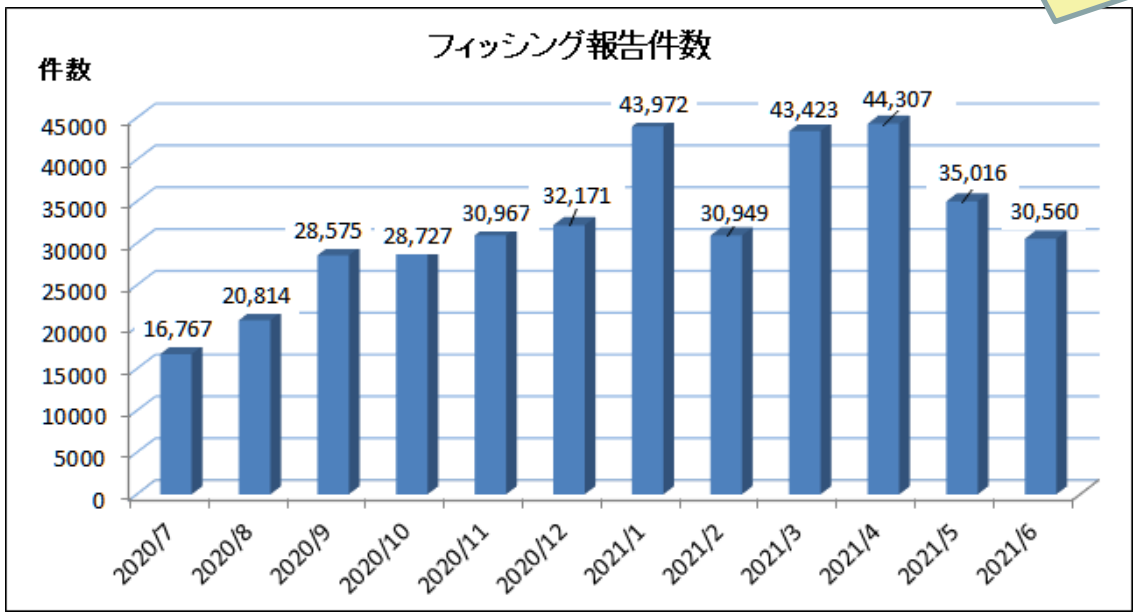
(特別定額給付金に関する通知を装うフィッシング (2020/10/15) より)

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

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、ブランドの件数を掲載
  - その月の傾向など、フィッシングの最新情報を掲載

フィッシングの動向がリアルに判る！



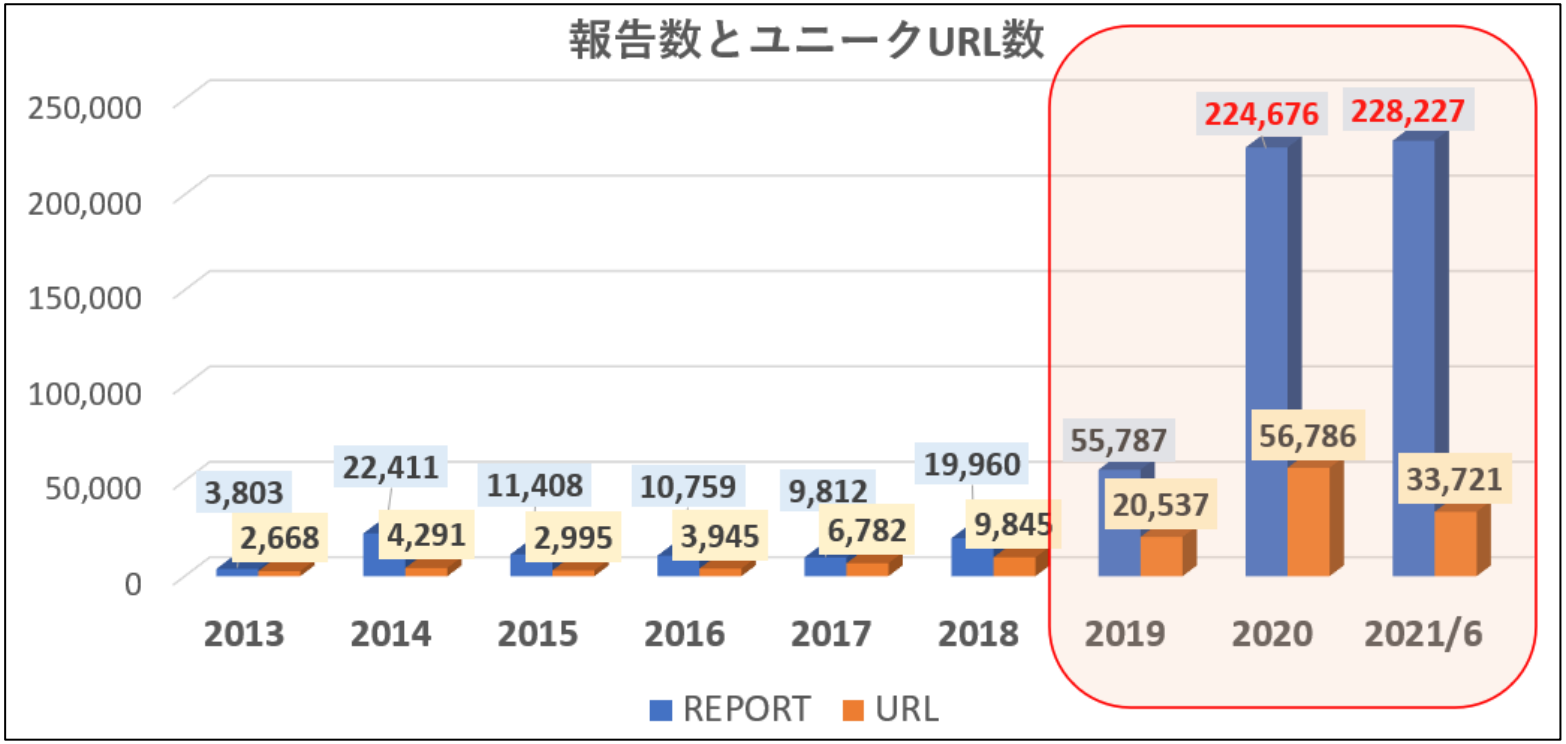
2021 年 6 月のフィッシング報告件数は 30,560 件となり、5 月と比較すると 4,456 件減少しました。
Amazon をかたるフィッシングは報告数全体の約 35.8 % を占めており、引き続き多い状況ではあるものの、前月より約 33.1 % 報告数が減少しました。次いで楽天、エムアイカード、三井住友カード、エポスカードをかたるフィッシングの報告も含めた上位 5 ブランドで、報告数全体の約 71.4 % を占めました。

（2021/06 フィッシング報告状況 より）

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

フィッシング報告数の推移 （年別）

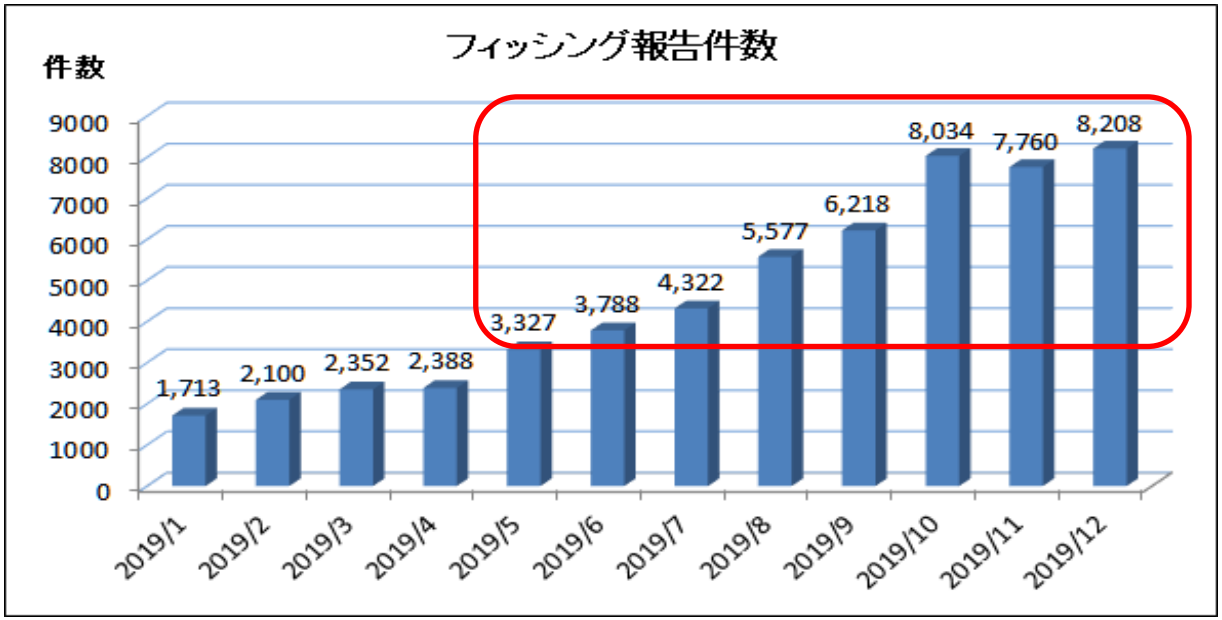
- 2020年以降、報告が激増
  - 2019年から2020年は 約22.4万件と約4倍に
  - 2021年も6月末時点で、既に2020年を上回っている
  - フィッシングメールは詐欺への誘導が行われる危険なメール
  - さらに、受信者のメールボックスを埋め尽くす、非常に迷惑な存在
    正当なメール、普通の迷惑メールより、フィッシングメールのほうが多い人も…



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

フィッシング報告数の推移（2019年）

- 2019年後半から、急激に増加。

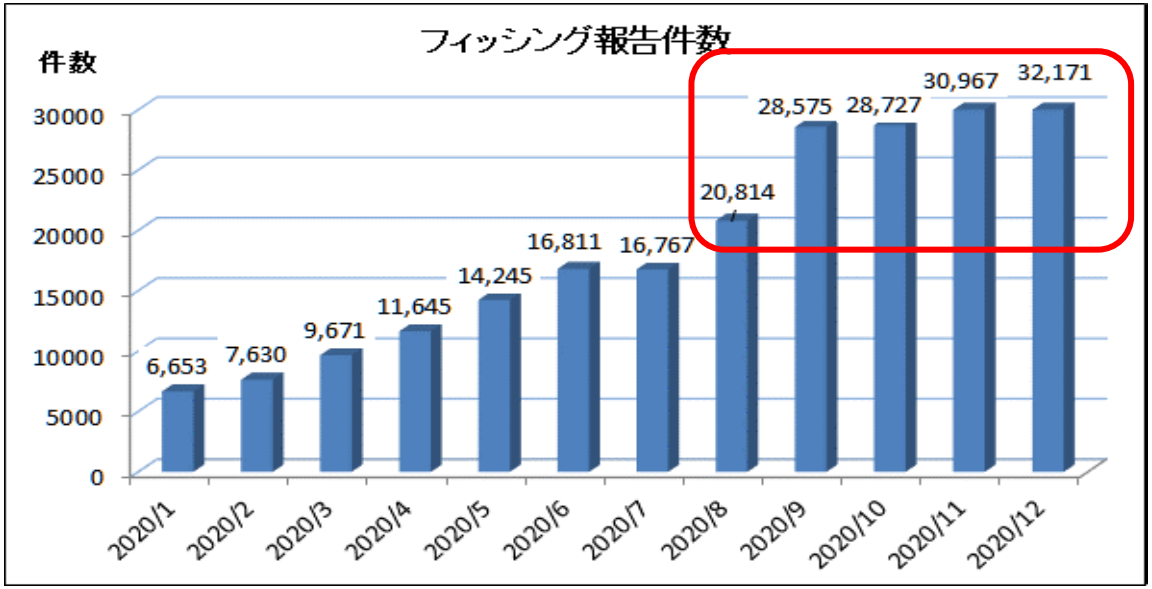


- 2019年主な増加の原因と傾向
  - **スパムボットを使った大量メール配信**（週１配信 → 週数回配信）
  - 特定の海外事業者からの大量メール配信
  - 国内ISPユーザのアカウントを不正利用した踏み台メール送信
  - 国内ホスティング事業者を踏み台にした大量メール配信

これらの大量配信系だけで全体の90%以上を占めていた

フィッシング報告数の推移（2020年）

- 2020年、フィッシング報告数が急激に増加
  - **1万件以下から、3万件超**へ
  - 特に配信インフラが変わった8月以降、大量に配信

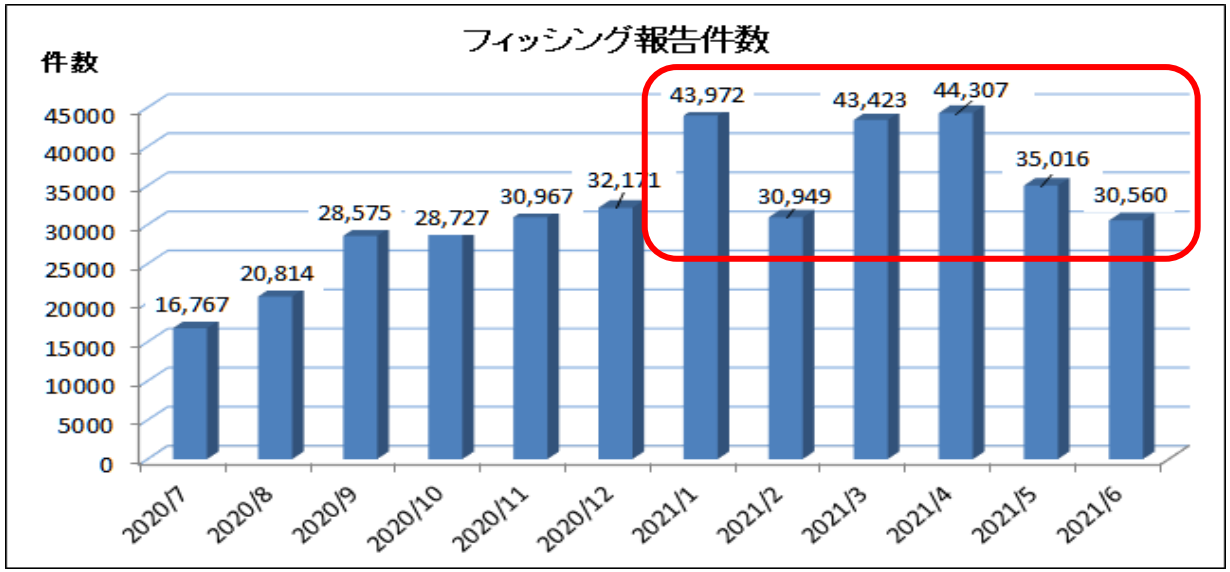


- 2020年主な増加の原因と傾向
  - PC (botnet) → サーバを使うようになり、配信リソースが増強
    大量配信の頻度と量の増加（1日4-5通、多い人で数十通 同じメールを毎日受信）
  - 本物と同じドメインを使った、**なりすまし送信**の増加
  - 特定の国内ホスティング事業者設備からの大量メール配信

2020年も大量配信系は 80-90% を占めていた。

フィッシング報告数の推移 （2021年）

- 2021年、更にフィッシング報告数が増加したが…
  - 1月年明けとともに、報告数は4万件を突破
    国内事業者からのなりすまし送信メールと、CN の事業者からの大量配信が続く



- **2021年は増加の一途だった状況に変化が起きている**
  - 2月は中国春節休暇期間の報告が激減、3万件にとどまる
  - 3月、4月は、1月と同じ傾向で、ふたたび4万件超へ
  - 5月、突然 CN からの大量配信が停止。3万件台となる
  - 6月、大量のなりすましメール送信を行っていた、国内事業者設備からの配信が減る。
    DMARC対応した組織は効果があらわれはじめ、全体で3万件台前半に戻る。

2020年 なりすまし送信メールの急増

なりすまし送信状況

- 2020年6月頃から Amazon、クレジットカードブランドの、なりすまし送信が増える
  多くの利用者は差出人メールアドレスを確認し、本物かと困惑
- この頃は、スマートフォンでは、なりすましメールは確認するすべがなかった

送信ドメイン認証 DMARC を使えば全体の **約 60%以上** 検出可能な状況

- 窓口の対応負荷が増大し、DMARC普及啓発の必要性
- 内閣府 消費者委員会の「フィッシング問題への取組に関する意見」(2020年12月発行)
  に DMARC 対応が盛り込まれる (22ページ以降参照)
  消費者保護の面でも、DMARC の有効性、必要性が認められた

なりすまし合計	4月	5月	6月	7月	8月	9月	10月	11月	12月
Amazonなりすまし合計	575	1,156	3,394	5,420	7,564	10,737	8,598	12,096	9,594
国内ECサイトなりすまし合計		51	124	470	512	1,059	789	625	1,046
クレカブランドなりすまし合計			191	310	153	1,648	2,757	4,431	6,857
二回目特別定額給付金(soumu.go.jp)							522	82	
なりすまし合計	575	1,207	3,709	6,200	8,229	13,444	12,666	17,234	17,497
フィッシング報告メール 件数	11,755	12,665	15,113	15,135	17,414	24,315	22,777	25,021	26,328
なりすまし全体に対する割合	5%	10%	25%	41%	47%	55%	56%	69%	66%

各なりすましの割合	4月	5月	6月	7月	8月	9月	10月	11月	12月
Amazon	12%	16%	36%	52%	54%	62%	58%	63%	60%
国内ECサイト	0%	3%	7%	17%	14%	20%	17%	25%	29%
クレジットカードブランド			39%	52%	14%	41%	38%	56%	61%

2021年 なりすまし送信メールの状況

■ 2021年なりすまし送信状況

	2021年					
	1月	2月	3月	4月	5月	6月
Amazonなりすまし合計	7,293	2,904	3,081	6,027	5,975	3,165
クレカブランドなりすまし合計	6,339	4,263	6,797	6,688	5,794	7,090
国内ECサイトなりすまし合計	584	616	784	1,747	2,538	2,399
なりすまし合計	14,216	7,783	10,662	14,462	14,307	12,654
フィッシング報告メール 件数	30,534	21,250	29,566	29,059	25,532	22,634
なりすまし全体に対する割合	46.6%	36.6%	36.1%	49.8%	56.0%	55.9%

- Amazon は SPF の宣言に不備があり、検証エラーで実質、SPFもDMARCも判定エラー（無効と同じ）となる状況だったが、 3月初めに修正された
- 4月、なりすまし送信されるブランドが増える。（クレジットカードブランド、国内ECサイトなど）
- 5月、4月と傾向は変わらないが、全体の報告数が減ったため、なりすまし割合が増加
- 6月、Amazon のなりすましは減少（独自ドメインに移行）、クレカブランドでDMARC対応していないブランドが集中的に狙われる

■ 現状でも、送信ドメイン認証で全体の **約 56 %以上** 検出できる可能性がある

非常に大きな効果が見込まれる！

2021年 クレカブランド報告状況

- 特に目立つクレカブランドのなりすましフィッシングメール
  - ブランドを日ごと週ごとに変えて、大量配信し、反応をみている
  - 部分的なDMARC対応すると、サブドメインや他の所有ドメインで大量配信
  - DMARC完全対応すると、他のDMARC対応していないクレカブランドを狙う

- DMARC対応しているか否かが、各ブランドの報告数にも表れている
  （以下は、なりすまし＋非なりすまし両方含む）

		2020年			2021年						
ブランド	DMARC	10月	11月	12月	1月	2月	3月	4月	5月	6月	7/14
Amazon	3月済	14,930	19,305	16,084	26,999	18,684	22,547	22,479	16,334	10,926	5,213
A社	済	946	1,808	1,411	1,381	820	3,486	1,702	1,102	452	15
B社	一部	4,968	2,859	4,130	5,768	4,345	3,039	2,099	2,633	2,646	1,584
C社	一部	224	282	346	1,149	936	1,269	2,389	665	818	696
D社	6月済	6	61	2	611	60	441	348	652	2,971	123
E社	未					1			1,725	1,145	593
F社	未	259	193	224	820	404	1,904	1,434	904	1,211	43
G社	未		1,438	2,496	250	582	1,125	322	213	58	64
H社	未				384	27	542	907	224	187	547
I社	未								235	143	1561
J社	未		8		28	2			416	146	297

フィッシングを行う側は、ブランド側の対応をよく見ており、DMARC対応ができない組織（ドメイン）を集中的に狙ってくる

DMARCレポートからわかる、なりすまし状況と効果

- A社のDMARCレポート集計結果
  - なりすまし送信被害状況、DMARCの効果を見える化

	9月	10月	11月	12月	1月	2月	3月	4月	5月	6月
DMARC失敗数		172,276	6,882,083	1,890,838	256,249	7,046	4,443,915	4,891,654	3,260,605	935,283
なりすましメール		130,192	6,806,484	1,875,150	244,336	6,101	4,438,635	4,887,186	3,256,502	931,745
フィッシング報告受領数	245	946	1,808	1,411	1,381	820	3,486	1,702	1,102	452

  - 2020年、モニタリングモード（p=none）でDMARC対応開始
  - 2020年11月に大量のなりすましフィッシングメールを配信される
    1か月で 680 万通以上のなりすましメールを dmarc=fail で検出
  - 2021年3月、他の所有ドメインでなりすましフィッシングメールを大量配信される
  - 6月、他の所有ドメインにもDMARC設定完了
    報告数、コールセンターへの問い合わせ数、減少＝フィッシング減少

- なりすまし被害が多かった D社もDMARC対応
  - 6月、集中的に狙われる。SPF で –all 指定をしていても効果が見えない
  - DMARC対応を提案し、6月中旬に p=none で運用開始
  - ある土日、Gmail 宛てだけで 24 万通以上を dmarc=fail で検出
  - p=quarantine にすれば、この 24万通 は迷惑メールフォルダ行きにできる

現状、対応している事業者宛てだけでも、利用者が多いため、
数十万、数百万のフィッシングメールを検出し、排除できるのは
フィッシング対策において、非常に効果があると言える

なりすまし送信メールの例

- 送信ドメイン認証をかいくぐろうとするメール
  Envelope-From 独自ドメインでSPF や DKIM を pass、Header-From 正規サービスのドメイン
  - ✓ SPF：**pass （ama001.com で判定するため、pass、偽物と判定できない）**
  - ✓ DKIM：独自ドメインの正規署名をつけられると **pass（偽物と判定できない）**
  - ✓ DMARC：**fail (amazon.comで判定をするため、検出可能)**

```
Return-Path: <istrator@ama001.com>
Delivered-To: example@antiphishing.jp
Received: from hwsrv-817213.****.com (hwsrv-817213.****.com [***.***.***.***])
        by antiphishing.jp with ESMTPS id 06FD66068F77
        for <example@antiphishing.jp>; Mon, 28 Dec 2020 17:59:12 +0900 (JST)
Authentication-Results: antiphishing.jp; dmarc=fail (p=quarantine dis=none) header.from=amazon.com
Authentication-Results: antiphishing.jp; spf=pass smtp.mailfrom=istrator@ama001.com
From: "Amazon.co.jp" <account-update@amazon.com>
To: <example@antiphishing.jp>
Subject: Amazonプライム会員登録キャンセルのお知らせ
Date: Mon, 28 Dec 2020 16:59:05 +0800
```

SPF=passするために使われたメールアドレス

SPFとDMARCでは判定に使うドメインが違う

メールソフトで見える部分

SPFとDKIMは、検証対象のドメインを独自ドメインにされると効果がない（SPFのみの対応だと、上記の不正メールは正規メールと判定される）

DMARCを組み合わせなければなりすまし検出は不可能

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

なりすまし送信メールの例

普通のなりすまし送信

差出人: "Amazon.co.jp" <account-update@amazon.co.jp>
日時: 2021年7月8日 9:44:47 JST
件名: 【アマゾン】注文状況が変更されました

お客様の注文とアマゾン アカウントを変更させていただいております。請求先住所が変更されたなど、理由で発生する可能性があります。アカウントにログインして画面の指示に従うことで、アカウントの停止状態を解除していただけます。

下記にあるタブをクリックしていただき、注文情報をご確認または変更。

他組織のドメインを使ってなりすまし送信

自分関係ない、と思っていても巻き込まれる

From: 楽天市場 <admini@rakuten.co.jp>
日付: 2021/07/07 5:28
件名: Amazon.co.jp アカウントの支払い方法を確認できず、注文を出荷できません.

amazon.co.jp プライム

Amazon お客様 [redacted]

Amazon に登録いただいたお客様に、Amazon アカウントの情報更新をお届けします。
残念ながら、Amazon のアカウントを更新できませんでした。

受信者のメールアドレスや他人のメールアドレスを使って送信

自分関係ない、と思っていても巻き込まれる

差出人: [redacted]@k6.dion.ne.jp <[redacted]@[redacted]com>
日時: 2021年7月8日 7:56:55 JST
宛先: [redacted] <[redacted]@k6.dion.ne.jp>
件名: **Rakuten.cojp**にご登録のアカウント(名前、パスワード、その他個人情報)の確認
CID:856734

Rakuten Card

本メールはお客様によるお楽天アカウントのご更新が必要な場合にお知らせする

[redacted]@k6.dion.ne.jp様

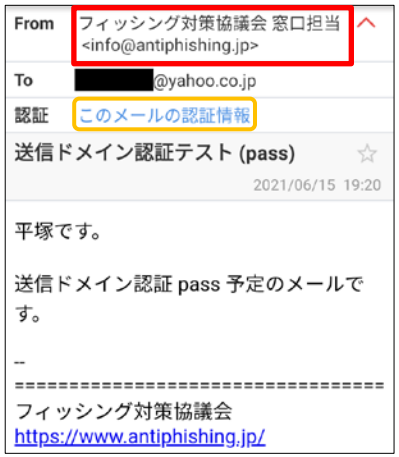
お客様の注文と楽天アカウントを停止させていただいております。請求先住所が変更されたなど、理由で発生する可能性があります。アカウントにログインして画面の指示に従うことで、アカウントの停止状態を解除していただけます。

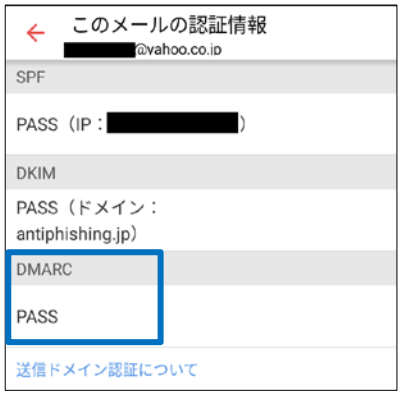
下記にあるタブをクリックしていただき、注文情報をご確認または変更。

なりすまし送信メール、ユーザ側での確認例

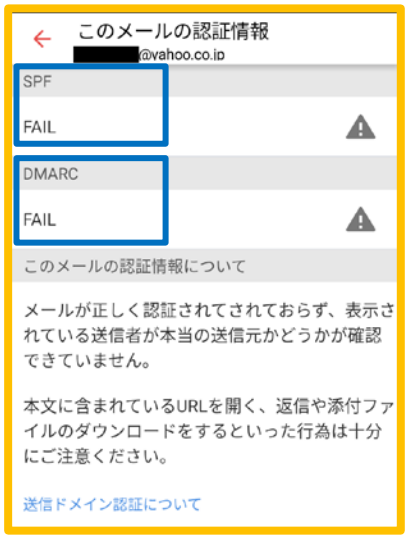
■ Yahoo! メール スマホアプリでの表示例

正規メール

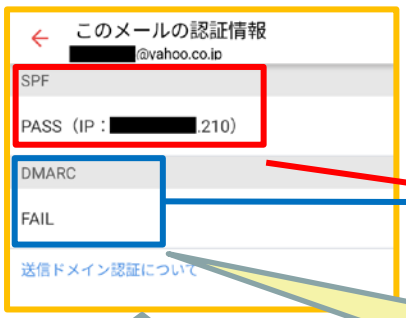




なりすましメール１



なりすましメール２



◆ **メール送信者**は全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**
本物のサーバから送信
SPF=pass
DKIM=pass
DMARC=pass

◆ **なりすましメール１**
偽サーバから送信
SPF=fail
DMARC=fail

◆ **なりすましメール２**
偽サーバから独自ドメインで SPFを pass するよう送信
SPF= pass
DMARC= fail

DMARC=fail となり、ニセモノの可能性が高いと判別できる！

現在、日本で普及している SPF＋DMARCでも検出可能（DKIM 無しでも可能）

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

まとめ

- 現在、フィッシング対応のメインとなっているURLフィルタリングやテイクダウンによる対応は今後も必要だが、動きの速いフィッシングサイトへの対応としては限界がきている

- 2020年は特に正規のドメインを使用した 「なりすまし送信」 が急増し、2021年現時点でも、フィッシングメール報告全体の 半分以上 を占めるため、送信ドメイン認証による対策が有効である

- 被害ブランドと関係のないドメインでも送信メールアドレスに使われると「なりすまし送信」 被害に巻き込まれるため、いかなる組織、企業にも DMARC 対応を推奨する

- 送信ドメイン認証 SPF/DKIM だけでは、昨今の 「なりすまし送信」 フィッシングメールを防げないため、DMARC に対応する必要がある。

- SPF対応済であれば、DMARCはすぐに対応可能
  自社ドメインのなりすましメール送信の検知、規模の把握、コントロールが可能
  正規メールが届いている (dmarc=pass) かどうかも把握することが可能

DMARC はフィッシング対策・対応にも有効です。SPFだけでもOK！
まずはモニタリングモードで「見える化」してみましょう！

以降、参考資料

DMARCレポートの例

- クレカブランドA社のDMARCレポート集計結果
  - 2020/11/1 - 11/10 までの 10日間分
  - 自社ドメインのなりすましメールが、クラウド事業者から大量に送信されている
  - なりすまし送信の実態が把握できる
  - 正規メールの配信は dmarc=pass で把握できる

1サーバあたり数万通～数十万通の dmarc=fail するメール＝なりすましメールが配信

送信元のIPアドレス

Sender	Domain	RDNS	Mail Cour	DMARC %	SPF Pass
[redacted]223.202	[redacted].co.jp	[redacted]23-202.1gal.sta[redacted]	219993	0.14	0.14
[redacted]72.157	[redacted].co.jp	[redacted]2-157.thcj.stati[redacted]	122228	0.15	0.15
[redacted]74.164	[redacted].co.jp	[redacted]4-164.eqwx.sta[redacted]	121453	0.26	0.26
[redacted]220.36	[redacted].co.jp	[redacted]20-36.0tbu.stat[redacted]	93397	0.23	0.23
[redacted].0.240	[redacted].co.jp	[redacted]0-240.5t62.stati[redacted]	77424	0.09	0.09
[redacted]75.2	[redacted].co.jp	[redacted]5-2.h9iy.static.[redacted]	73397	0.39	0.39
[redacted].2.90	[redacted].co.jp	[redacted]2-90.mwqa.stat[redacted]	69964	0.26	0.26
[redacted].3.69	[redacted].co.jp	[redacted]3-69.busz.stati[redacted]	67752	0.4	0.4
[redacted]77.228	[redacted].co.jp	[redacted]7-228.wj1b.stat[redacted]	60230	0.42	0.42

なりすまし送信時に使われたドメイン

DMARC 段階的導入

- **DMARC ポリシー宣言**
  ポリシーを宣言し、なりすまし状況レポートを取得するだけなら、メールが届かなくなることもなく、今までと変わりません。まずは状況を把握しましょう。
  - Google：チュートリアル:DMARCおすすめのロールアウト方法
    https://support.google.com/a/answer/10032473?hl=ja
  - **設定例**

```
_dmarc.●●●●.jp.  IN  TXT  “v=DMARC1; p=none; rua=mailto:レポート受信用メールアドレス"
```

- **レポート確認**
  いくつかのメールサービスはDMARC検証結果レポートを送信してくれる（Gmail など）
  - 実際にレポートを受け取り、きちんと配送されていることを確認する
  - 届かなくなることを心配する以前に、まず届いていることを確認しましょう
    （現状、本当にメールが届いているか、回答できますか？）

- **【推奨】メールを送信しないドメインへのポリシー宣言**
  - ポリシーを宣言しないサブドメインやドメインを使って、なりすまし送信されるケースも非常に多くみられるため、メール送信しないドメインにもポリシーを宣言する
  - 取得済で未使用の Parked domain も忘れずに（自組織が保有するドメインを確認）
  - M3AAWG パークドメインを保護するベストコモンプラクティス
    https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12-japanese.pdf

DMARC 参考資料

- DMARC 導入
  - Google：DMARC について
    https://support.google.com/a/answer/2466580?hl=ja
  - Google：チュートリアル:DMARCおすすめのロールアウト方法
    https://support.google.com/a/answer/10032473?hl=ja
  - M3AAWG パークドメインを保護するベストコモンプラクティス
    https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12-japanese.pdf
  - なりすまし対策ポータル「ナリタイ」
    https://www.naritai.jp/

内閣府 消費者委員会の意見書

■ フィッシング問題への取組に関する意見（2020年12月3日）
https://www.cao.go.jp/consumer/iinkaikouhyou/2020/1203_iken.html

消費者の安全・安心を守る観点から、本件問題に係る関係行政機関における取組を一層促進する必要があると考え、早急に取り組むべき事項として、警察庁、総務省、経済産業省及び消費者庁に対して、下記第２のとおり意見を述べる。

…（中略）

なお、消費者委員会としても、**今後の状況を注視し、必要に応じ更に調査審議を行う**こととする。

■ 内閣府 消費者委員会とは

独立した第三者機関として、主に以下の機能を果たすことを目的としている

- 各種の消費者問題について、自ら調査・審議を行い、消費者庁を含む関係省庁の消費者行政全般に対して意見表明（建議等）を行う
- 内閣総理大臣、関係各大臣又は消費者庁長官の諮問に応じて調査・審議を実施

内閣府 消費者委員会の意見書

１ **フィッシングメールの受信防止対策の普及促進及び効果検証**

（１）フィッシングメールの受信防止対策の普及促進

総務省は、関係行政機関と連携しつつ、フィッシング対策にも有効な技術的対策（以下「本件技術的対策」という。）を普及、促進及び啓発すること。特に、当該対策の一つである下記技術を重点的に普及、促進及び啓発すること。

ア **送信ドメイン認証技術の普及促進**

関係事業者等における送信側及び受信側双方に係る送信ドメイン認証技術（SPF、DKIM及びDMARC）の導入を普及促進すること。当該技術のうち特に、DMARCの普及率が伸びない原因及び当該原因を踏まえた改善策等を調査検討し、同普及率を伸ばすように努めること。

イ **迷惑メールフィルターの啓発強化**

消費者に対する迷惑メールフィルターに係る啓発を強化すること。

当該普及啓発に当たっては、**若年層から高齢者までのあらゆる消費者**が、当該機能及び効果（長所だけでなく短所も含む。）を理解し、これらを総合的に勘案した上で適切に当該機能を設定ないし選択できるように、**サービスプロバイダー等の関係事業者等による消費者への適時適切な情報提供等を促すこと**。

（２）**フィッシングメールの受信防止対策の効果検証**

総務省は、関係行政機関と連携しつつ、**送信ドメイン認証技術や迷惑メールフィルター等**、本件技術的対策の**効果検証を適時適切に行い**、**当該結果を踏まえ、必要に応じて**その**普及促進方法や本件技術的対策等を改善**すること。

内閣府 消費者委員会の意見書

3 消費者への注意喚起の一層の強化

警察庁、総務省、経済産業省及び消費者庁は、各々及び必要に応じて連携して、以下の取組を行うこと。

（1）消費者に対する注意喚起の強化

常に変化していくフィッシングの手口の傾向等について、消費者に対して迅速に情報提供し、注意喚起を強化すること。

（2）消費者側の対策に係る周知啓発の強化

消費者側において講じるべき対策の周知啓発を強化すること。特に、当該対策として、例えば以下の点が基本的かつ重要であることが個々の消費者に伝わるように、周知啓発の方法を更に工夫すること。

④ フィッシングの被害に遭った場合は、**直ちに銀行やクレジットカード会社等に連絡**し、必要な手続を行うこと。

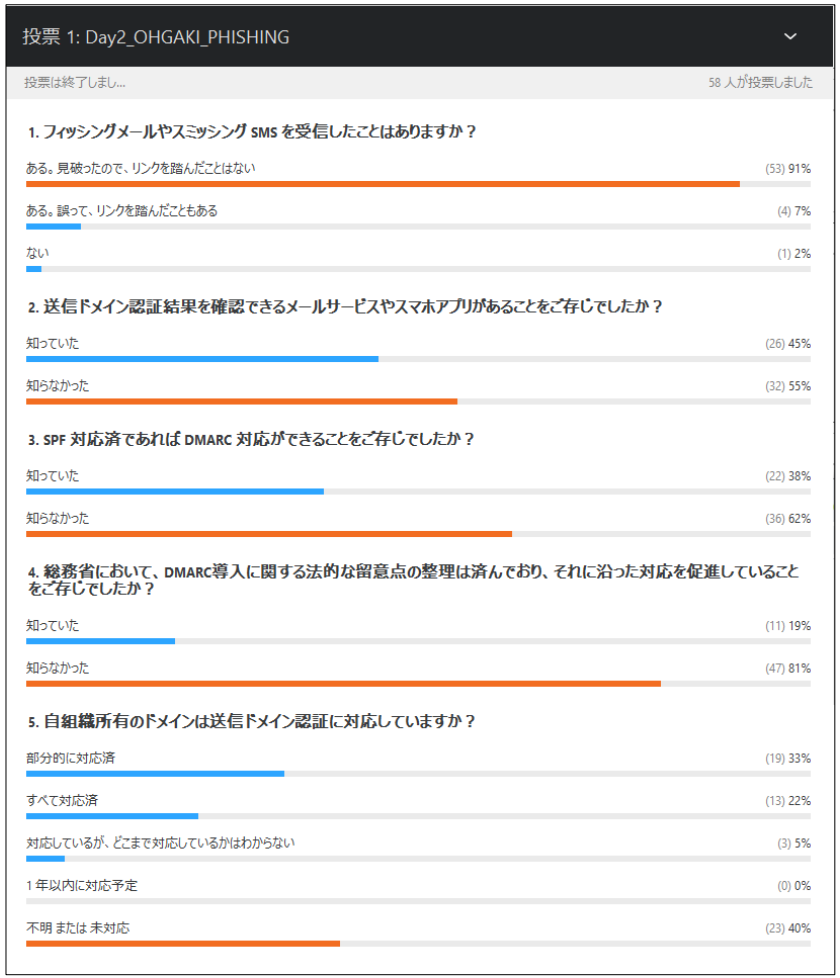
なお、上記第２の３（２）④を周知啓発するに当たっては、消費者が相談し得る窓口等が複数にわたる現状を踏まえ、**消費者が第一次的にどこに相談すればよいのかを直ちに判断し得るようにするための方策等を検討**することが望ましい。

（3）注意喚起及び周知啓発の効果検証

上記第２の３（１）の注意喚起及び同（２）の周知啓発の取組につき、**適時適切に効果検証を行い、当該結果を踏まえ、必要に応じてその方法等を改善すること**。

フィッシング被害に遭った時の連絡窓口の明記（24時間対応）
どこに連絡すれば、不正送金を止められるか？
どこに連絡すれば、カードを停止できるか？

JANOG48 発表後のアンケート結果



投票 1: Day2_OHGAKI_PHISHING

投票は終了しまし... 58 人が投票しました

1. フィッシングメールやスミッシング SMS を受信したことはありますか？

ある。見破ったので、リンクを踏んだことはない	(53) 91%
ある。誤って、リンクを踏んだこともある	(4) 7%
ない	(1) 2%

2. 送信ドメイン認証結果を確認できるメールサービスやスマホアプリがあることをご存じでしたか？

知っていた	(26) 45%
知らなかった	(32) 55%

3. SPF 対応済であれば DMARC 対応ができることをご存じでしたか？

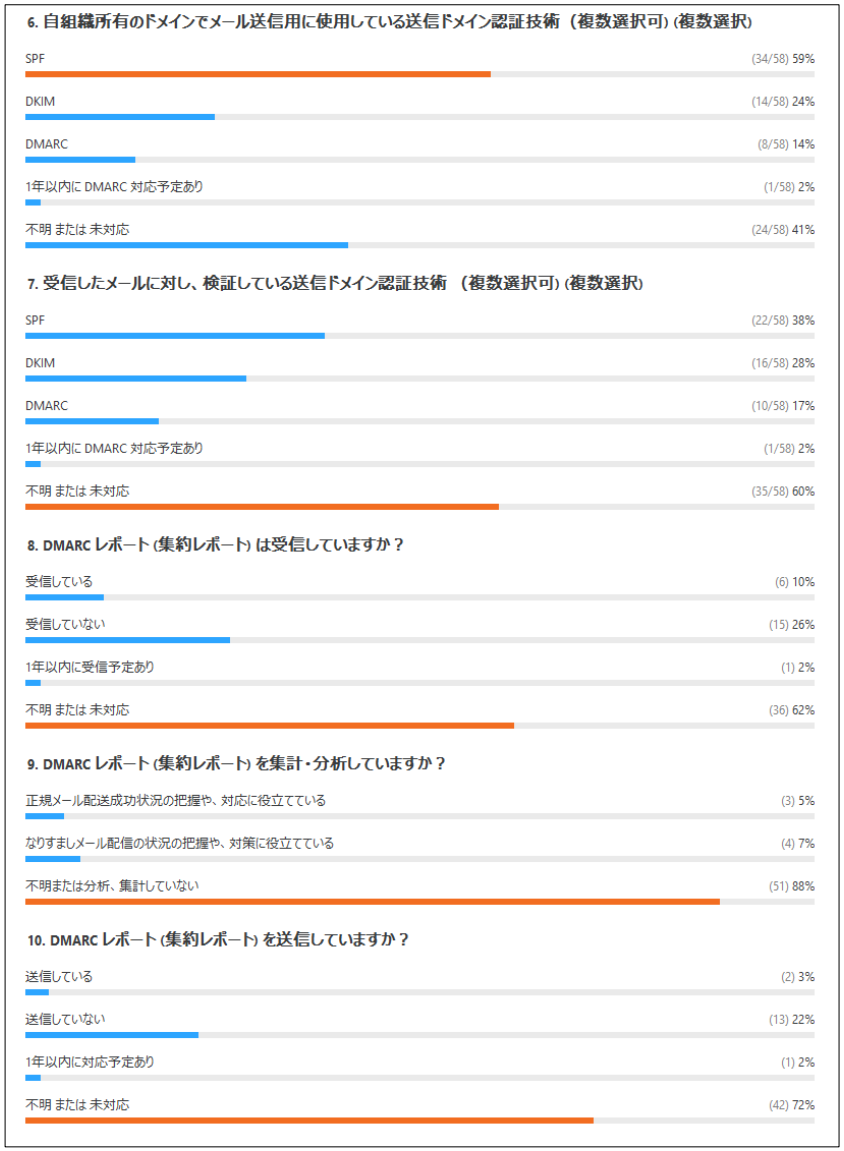
知っていた	(22) 38%
知らなかった	(36) 62%

4. 総務省において、DMARC導入に関する法的な留意点の整理は済んでおり、それに沿った対応を促進していることをご存じでしたか？

知っていた	(11) 19%
知らなかった	(47) 81%

5. 自組織所有のドメインは送信ドメイン認証に対応していますか？

部分的に対応済	(19) 33%
すべて対応済	(13) 22%
対応しているが、どこまで対応しているかはわからない	(3) 5%
1 年以内に対応予定	(0) 0%
不明 または 未対応	(23) 40%



6. 自組織所有のドメインでメール送信用に使用している送信ドメイン認証技術（複数選択可）(複数選択)

SPF	(34/58) 59%
DKIM	(14/58) 24%
DMARC	(8/58) 14%
1年以内に DMARC 対応予定あり	(1/58) 2%
不明 または 未対応	(24/58) 41%

7. 受信したメールに対し、検証している送信ドメイン認証技術 （複数選択可）(複数選択)

SPF	(22/58) 38%
DKIM	(16/58) 28%
DMARC	(10/58) 17%
1年以内に DMARC 対応予定あり	(1/58) 2%
不明 または 未対応	(35/58) 60%

8. DMARC レポート (集約レポート) は受信していますか？

受信している	(6) 10%
受信していない	(15) 26%
1年以内に受信予定あり	(1) 2%
不明 または 未対応	(36) 62%

9. DMARC レポート (集約レポート) を集計・分析していますか？

正規メール配送成功状況の把握や、対応に役立てている	(3) 5%
なりすましメール配信の状況の把握や、対策に役立てている	(4) 7%
不明または分析、集計していない	(51) 88%

10. DMARC レポート (集約レポート) を送信していますか？

送信している	(2) 3%
送信していない	(13) 22%
1年以内に対応予定あり	(1) 2%
不明 または 未対応	(42) 72%

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

フィッシング被害を減らすため、
皆さまのご協力が必要です。
どうか、よろしくお願いいたします