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

2021年11月26日 IP Meeting 2021
～明日のカタチ～パネルディスカッション
「～なぜ、普及してしかるべき技術が普及しないのか？ ～」

なりすましフィッシングメール対策技術 DMARCの普及にむけて

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

フィッシング対策協議会の組織概要

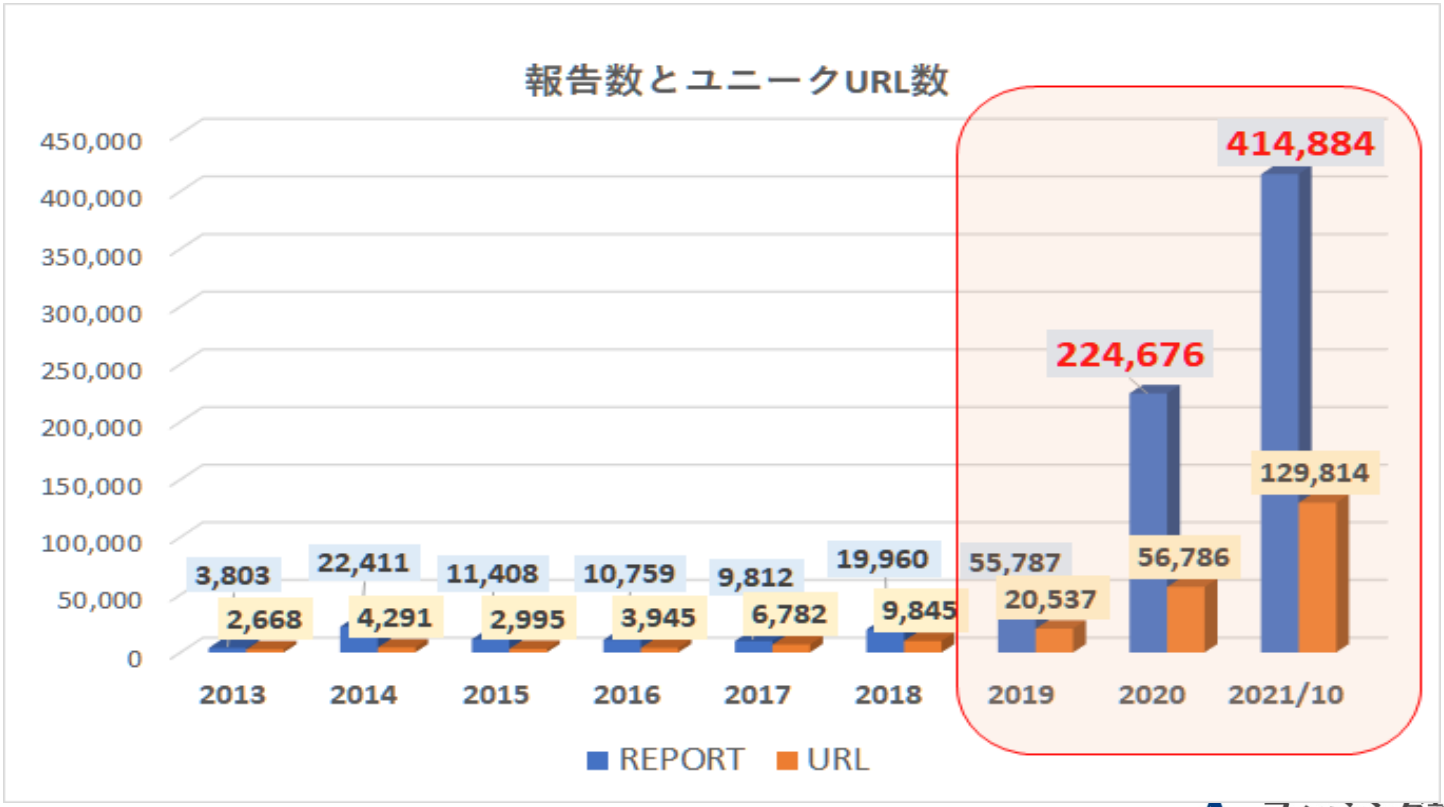
- 設立
  - 2005年4月
- 名称
  - フィッシング対策協議会 / Council of Anti-Phishing Japan
  - https://www.antiphishing.jp/
- 目的
  - フィッシング 詐欺に関する事例情報、技術情報の収集及び提供を中心に行うことで、日本国内におけるフィッシング詐欺被害の抑制を目的として活動
- 構成
  - セキュリテイベンダー、オンラインサービス事業者、金融・信販関連など
  - 会員+オブザーバー 104 組織 （2021 年 6 月 1 日時点）
    正会員： 77 社、リサーチパートナー： 6 名、関連団体： 14 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年は10月末時点で、既に2020年の約２倍の報告を受領
    2年前の 2019年と比較して約 8 倍。ここ 2 年で**非常に大きな問題となってきた**
  - 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**



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

フィッシング問題への取り組み

- 2020年頃までの主なフィッシング対策
  - 一般への普及啓発活動（フィッシングメールを見破る → 無理）
    - 本物のお知らせメールの文面をコピーして作成するので、判別不可
  - URLフィルタリング
    - Google Safebrowsing に登録され各種ブラウザで警告がでるようになると、フィッシングサイトは別の URL で稼働し始める
  - フィッシングサイトのテイクダウン
    - 数時間から1日以内に多くのフィッシングサイトはたたんでしまう
    - 被害はメール配信から数時間内に集中して発生するため、間に合わない
  - 迷惑メール対策
    - 誘導元であるフィッシングメールを減らす
    - スパムボットによる配信 (Cutwail など)
    - メールアカウント不正利用による踏み台送信
    - ホスティングサービスの不正契約
    - 迷惑メールフィルタの利用

2020年 なりすまし送信メールの急増

- 2020年6月頃から、**なりすまし送信メールが急増**
- スマートフォンで見ると、差出人には本物のメールアドレスが表示され、多くの利用者が困惑したり、本物と信じて情報を入力
- 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

	2020年								
	4月	5月	6月	7月	8月	9月	10月	11月	12月
なりすまし合計	575	1,207	3,709	6,200	8,229	13,444	12,666	17,234	17,497
フィッシング報告数	11,755	12,665	15,113	15,135	17,414	24,315	22,777	25,021	26,328
なりすましの全体比	5%	10%	25%	41%	47%	55%	56%	69%	66%

しかしDMARCは日本では普及していない！
どう啓発活動をしていくべきか？

- 内閣府 消費者委員会からフィッシング問題についてヒアリングの依頼
  - なりすまし送信が多い状況と、対策としての DMARCの必要性を説明
  - **「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

内閣府 消費者委員会の意見書

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

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

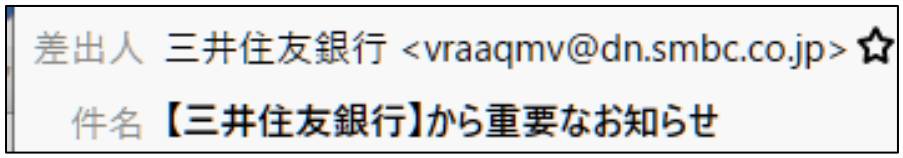
総務省は、関係行政機関と連携しつつ、**送信ドメイン認証技術や迷惑メールフィルター等、**本件技術的対策の**効果検証を適時適切に行い、当該結果を踏まえ、必要に応じてその普及促進方法や本件技術的対策等を改善**すること。

なりすまし送信

- 「なりすまし」送信とは
  - **実在するドメインのメールアドレスをかたりメールを送信すること**
  - **サービスの本物のドメインのメールアドレスをかたる場合が多い**

- なぜ「なりすまし」をするのか
  - 本物と同じメールアドレスは信用されやすい（見分けがつかない）
  - 迷惑メールフィルタ等でブロックされづらい
  - メールを送るためにドメインを取らなくて良い

- なぜ「なりすまし」送信ができるのか
  - メールは仕様上、かんたんになりすまし送信ができる
  - メールソフトで見える差出人メールアドレスは、実はどんな文字列でも自由に設定できる（通信上はメール本文と同等）



なりすまし送信メール
メールソフトでの表示例

なりすまし送信メールの例

- 送信ドメイン認証 DMARC でなければ検出できないメール
  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

新たなフィッシング問題への取り組み

- なりすまし送信メールを減らすための活動として、2021年よりDMARC 普及・啓発活動を始める
  - 月次報告書での毎月のメッセージ
  - JPAAWG、JANOG 等での発表
  - なりすまし送信被害が多いブランド（事業者）への個別対応
  - DMARCやSPFがエラーで無効になっている事業者への連絡
    大手ブランドでもシステム切り替えなどのタイミングで気が付かないうちに定義が無効になっているケースが良く見られる（多いのはspfのinclude指定に問題があるパターン)
  - 各方面の連携組織への説明

消費者委員会の意見書により、対応しなければならない問題として各方面に認識されやすくなった。

また、DMARC 試験運用中だった組織にとっては、本格運用に向けて踏み出すきっかけとなった。

2021年 なりすまし送信メールの状況

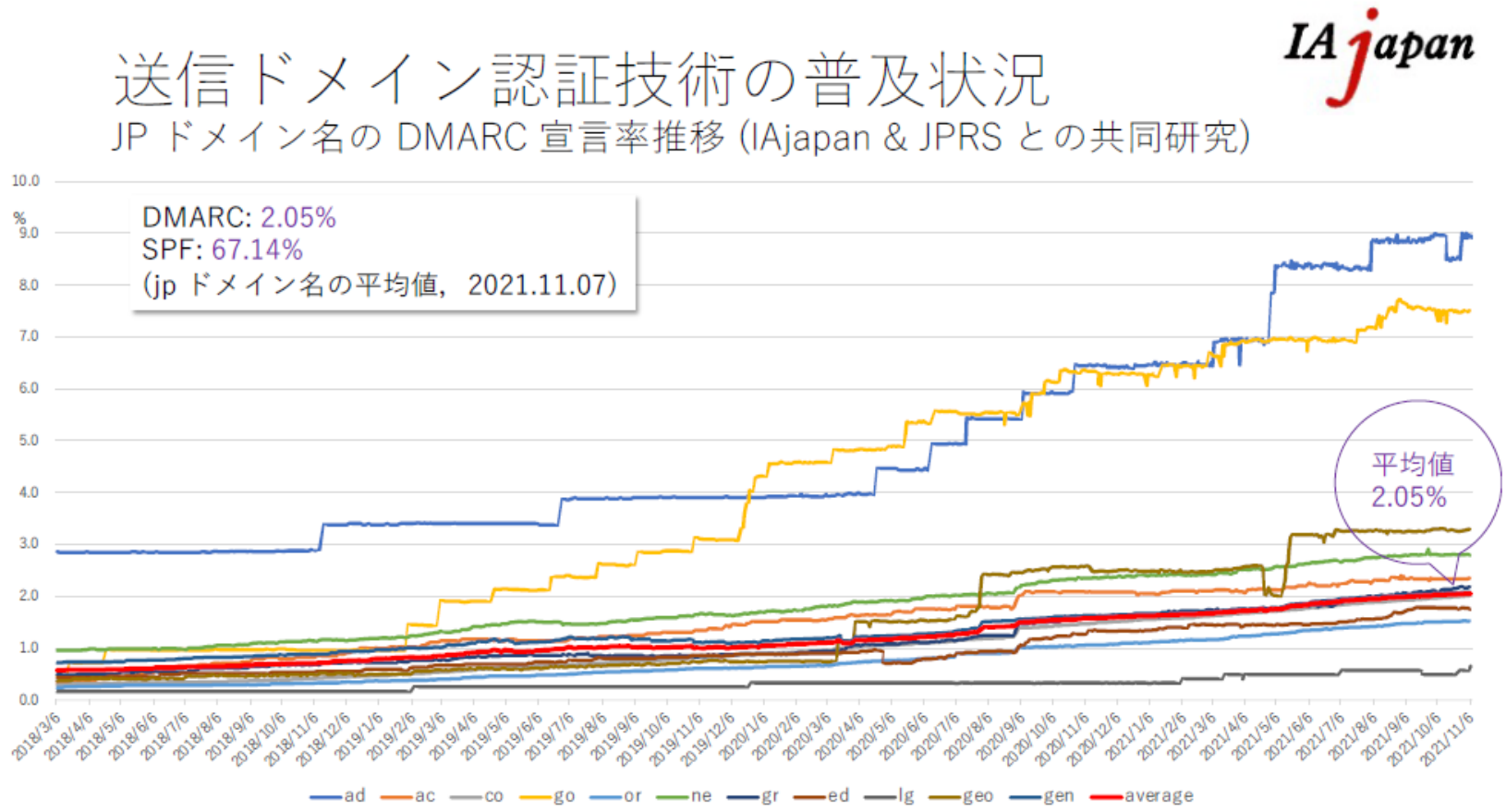
- フィッシングメールは増加の一途
  - DMARC対応ブランドに関しては、なりすまし送信メールが減少傾向
  - しかし、なりすまし送信の割合は減っていない
  - フィッシングで狙われる新規ブランドが次々と出てくる
    （緊急情報参照）

	2021年									
	1月	2月	3月	4月	5月	6月	7月	8月	9月	10月
なりすまし合計	14,216	7,783	10,662	14,462	14,307	16,779	18,784	35,395	29,335	26,469
フィッシング報告数	30,534	21,250	29,566	29,059	25,532	30,560	34,787	53,177	49,953	48,740
なりすましの全体比	46.6%	36.6%	36.1%	49.8%	56.0%	54.9%	54.0%	66.6%	58.7%	54.3%

- 現状見えている問題点
  - DMARC非対応ブランドが、なりすまし送信で狙い撃ちされている
  - 国内 ISP、モバイルのメールサービスは、受信時の送信ドメイン認証の判定を行っていないところが多い。（spf=hardfail 判定でも素通し）
  - 他ブランドのドメインを使ったり、ISPのメールアドレスを使ったなりすまし送信も、よく行われている
    （実在するドメインのチェックを回避するためか？）

まだ DMARC 啓発活動を始めて１年、頑張りどころ

送信ドメイン認証の普及率



JPAAWG 4th General Meeting
B1-5 メール技術のいま (櫻庭 秀次氏 / 株式会社インターネットイニシアティブ) より
https://www.slideshare.net/GeneralMeetingJPAAWG/b15-250681006

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

DMARCレポートからわかる、なりすまし状況と効果

■ クレカブランドA社のDMARCレポート集計結果
- なりすまし送信被害状況や 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、再びなりすましフィッシングメールを大量配信される
  1か月で 443 万通以上のなりすましメールを dmarc=fail で検出
- 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**

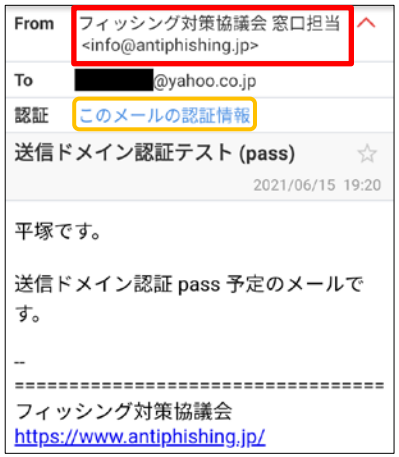
■ なりすまし被害が多かったクレカブランドD社もDMARC対応
- 6月、集中的に狙われる。SPF で –all 指定をしていても効果が見えない
- DMARC対応を提案し、6月中旬に p=none で運用開始
- ある土日、Gmail 宛てだけで 24 万通以上を dmarc=fail で検出
- p=quarantine にすれば、この **24万通 は迷惑メールフォルダ行き**にできる

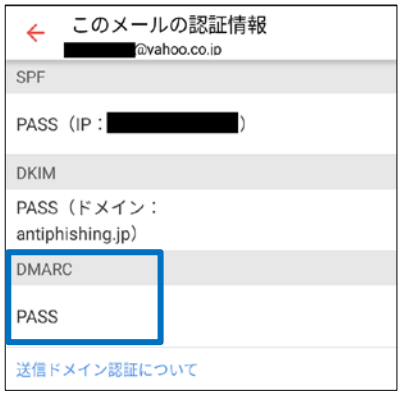
現状、対応している大手事業者宛てだけでも、利用者が多いため、数十万、数百万のフィッシングメールを検出し、排除できるのは フィッシング対策として、非常に効果があると言える

なりすまし送信メール、ユーザ側での確認例

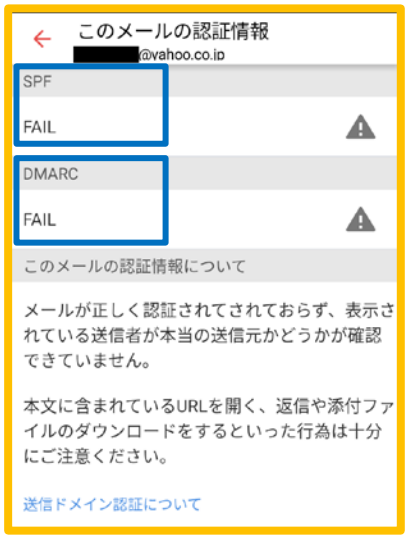
■ Yahoo!メールスマホアプリでの表示例 （Yahooメール、Gmail アカウントに対応）

正規メール

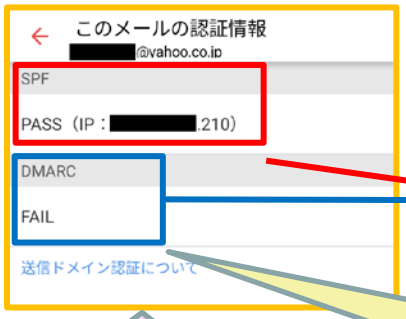




なりすましメール１



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

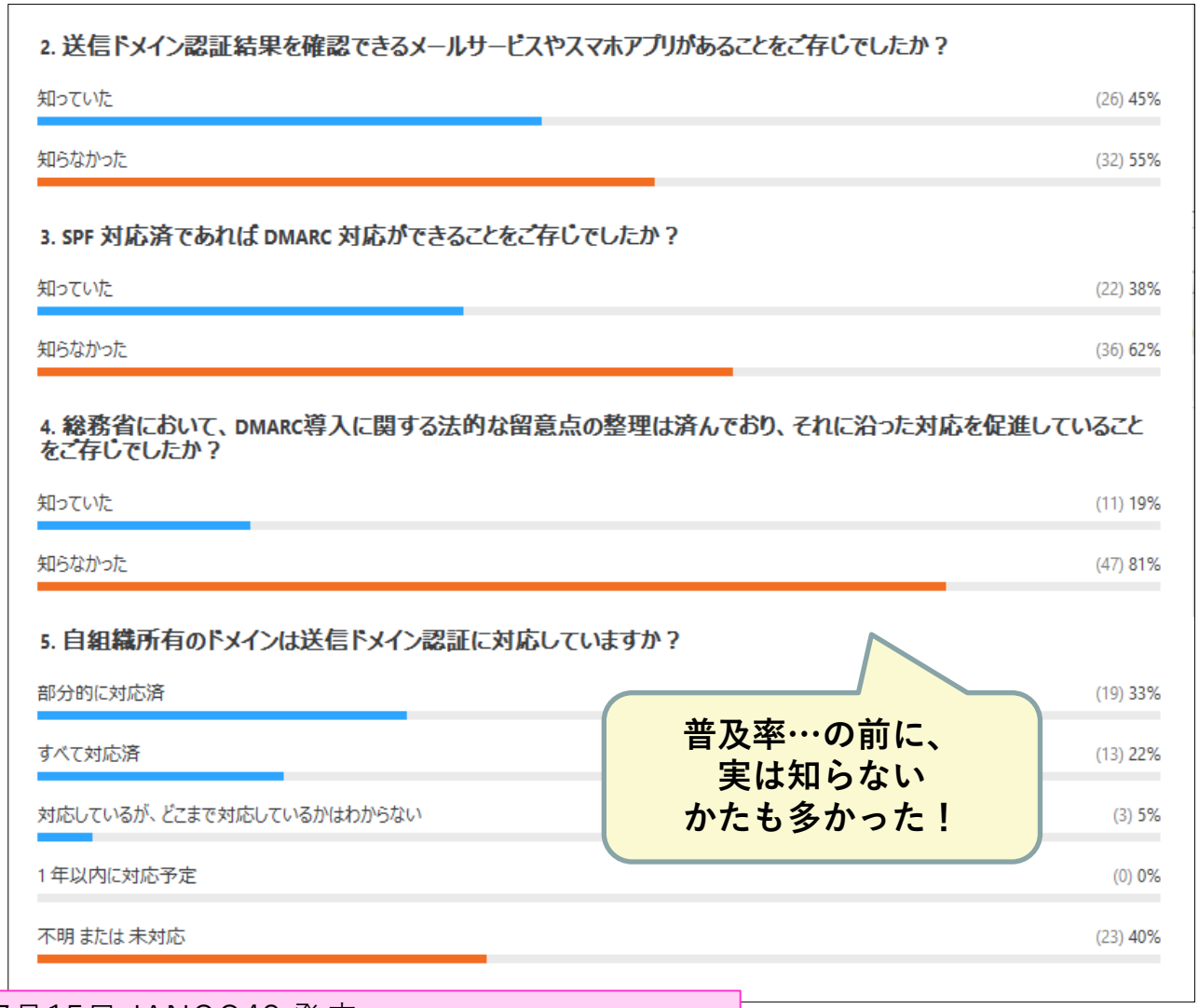
◆ **なりすましメール２**
偽サーバから独自ドメインで SPFを pass するよう送信
SPF= pass
DMARC= fail

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）

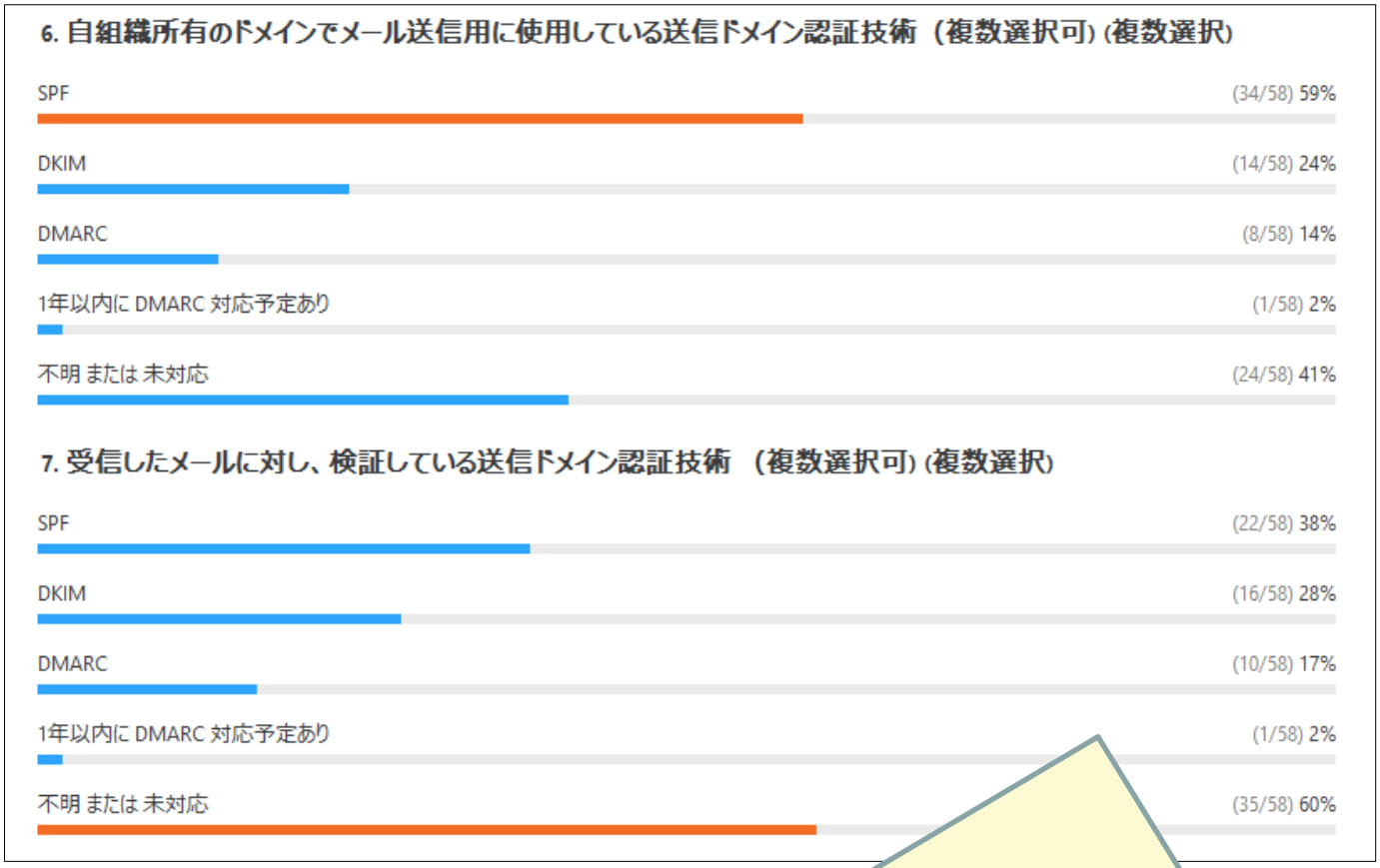
フィッシング対策協議会
Council of Anti-Phishing Japan

JANOG48 発表後のアンケート結果



2021年7月15日 JANOG48 発表
増え続けるフィッシング被害に今、我々ができること
https://www.janog.gr.jp/meeting/janog48/phishing/

JANOG48 発表後のアンケート結果



DKIM, DMARCに関しては、送信側の対応より、受信時に検証しているほうが多い。
企業等で不正メール検出に利用？（セキュリティ製品で自動でやっている）

2021年7月15日 JANOG48 発表
増え続けるフィッシング被害に今、我々ができること
https://www.janog.gr.jp/meeting/janog48/phishing/

啓発活動で伝えること

- 誤解を解く、似たようなものとの違いを説明する
  - DMARCは通秘に触れるのでできない → 法的整理は済んでおり、できます。
  - メールが届かなくなるかもしれない → 到達率には影響なかったそうです。
  - 送信ドメイン認証？SPF対応済です → SPFだけではなりすましは防げません。
  - なりすまし対策？S/MIME使ってます → S/MIMEは本物メールであることを証明できますが、署名がついていないメールの判別には DMARC が有効です
- 最初は個別に説明することも大事
  - 情報を収集できておらず、状況を把握できていない
  - 対策技術があることを知らない
  - メール関連のシステムのことは判らない（担当ではない）
  - 説明して反応が悪ければ、別の窓口からアプローチしてみる。
- 普及率よりカバー率、安全なものを選ぶ権利
  - 利用者が多いメールサービスでは対応済なので、導入効果はでる
  - 主要なメールシステムやセキュリティ対策製品は、DMARC 検証は機能として実装済なので、不正メール検出の手段のひとつとして、すでに使われ始めている
  - 利用者には不正メール対策に力を入れている安全なメールサービスを使う選択の余地があることを知らせる（対応済事業者の努力を汲む）

DMARC 普及に向けて

- 普及していないのは、実は知られていない、という理由もあった
  まずは被害の大きい組織から対応を依頼していく
- まずは p=none のモニタリングモードでDMARCを運用し、状況を把握してみる(p=none はメールの送受信には影響はでません)
- 対応できる事業者からやる
  最終的に p=quarantine/reject にしなければ、効果は出ないです
- 対応できないところは、できない理由があるのでしかたない
  集中的に狙われることも想定し、対策を考えておく

できるところからやりましょう

導入検討のためのデータ、情報、説明が必要であればフィッシング対策協議会へご相談ください

参考資料：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）

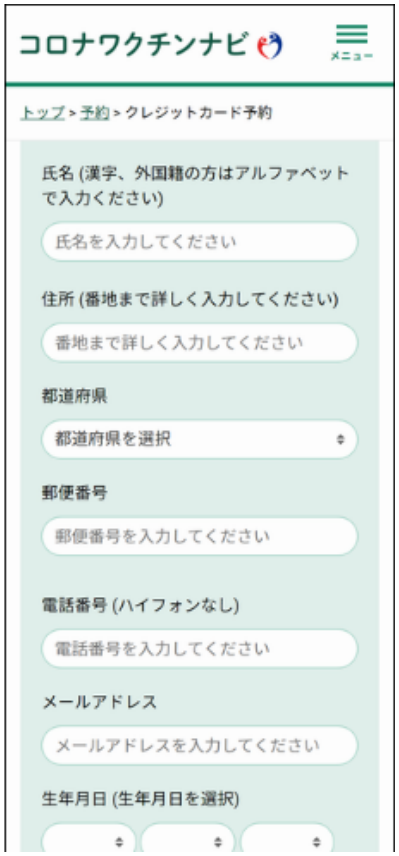
- 実際にレポートを受け取り、きちんと配送されていることを確認する
- 届かなくなることを心配する以前に、まず届いていることを確認しましょう
  （現状、本当にメールが届いているか、回答できますか？）

【推奨】メールを送信しないドメインへのポリシー宣言

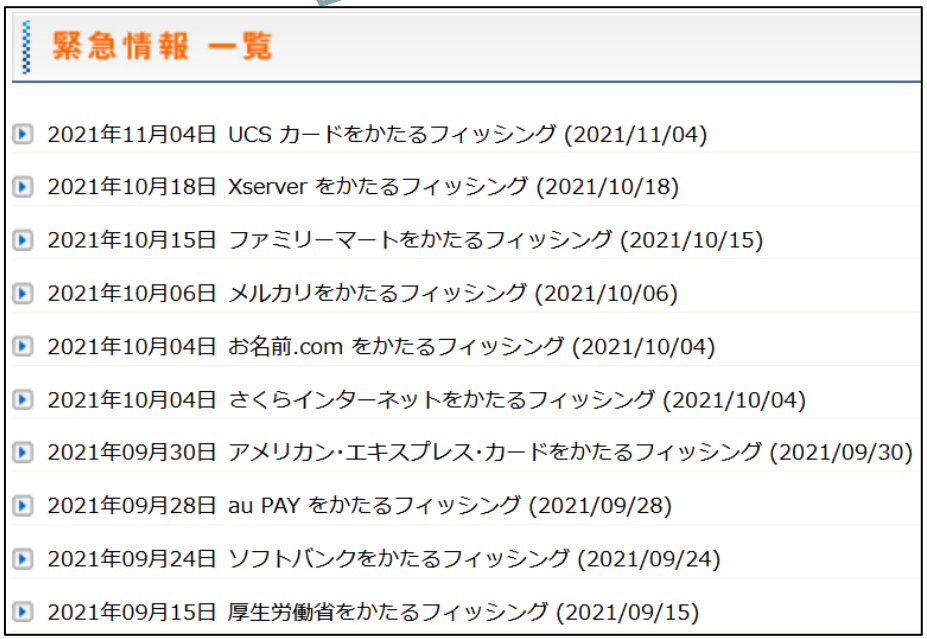
- ポリシーを宣言しないサブドメインやドメインを使って、なりすまし送信されるケースも非常に多くみられるため、メール送信しないドメインにもポリシーを宣言する
- 取得済で未使用の Parked domain も忘れずに（自組織が保有するドメインを確認）
- M3AAWG パークドメインを保護するベストコモンプラクティス
  https://www.m3aawg.org/sites/default/files/m3aawg_parked_domains_bp-2015-12-japanese.pdf

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！

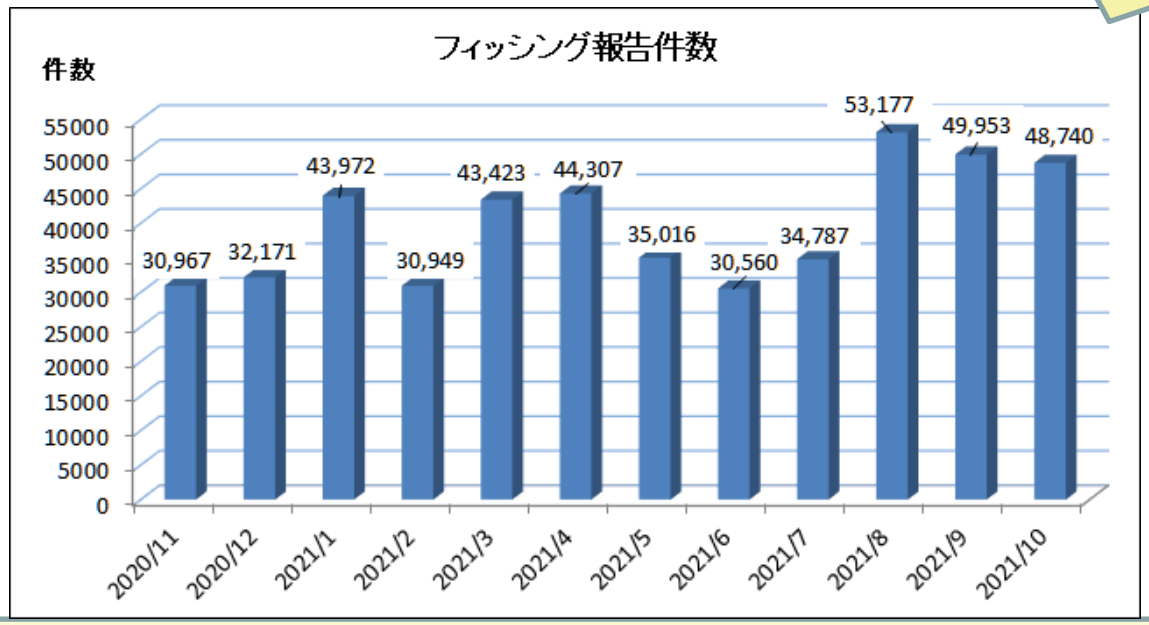


（厚生労働省をかたるフィッシング (2021/08/30)より）

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 10 月のフィッシング報告件数は 48,740 件となり、9 月と比較すると 1,213 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 28.2 % を占めており、次いで メルカリ、三井住友カード、ETC 利用照会サービス、楽天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 66.6 % 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 11 ブランドあり、これら上位 11 ブランドでは全体の約 83.2% を占めました

（2021/10 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

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