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

フィッシングの現状と対策（2020年後半版）

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について

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 105組織 （2020 年 11 月 10 日時点）
    正会員： 78 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

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

- 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

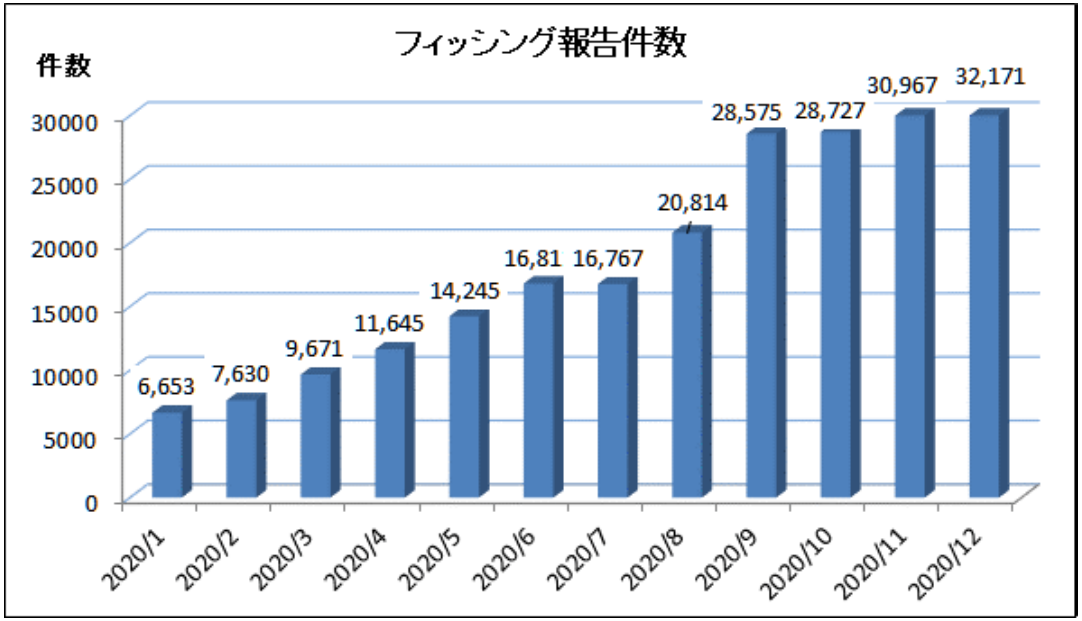
- 2021年01月25日 エポスカードをかたるフィッシング (2021/01/25)
- 2021年01月18日 北海道銀行をかたるフィッシング (2021/01/18)
- 2021年01月15日 UC カードをかたるフィッシング (2021/01/15)
- 2021年01月12日 エムアイカードをかたるフィッシング (2021/01/12)
- 2020年12月18日 三菱 UFJ 銀行をかたるフィッシング (2020/12/18)
- 2020年12月18日 宅配便の不在通知を装うフィッシング (2020/12/18)
- 2020年12月14日 セディナカード・OMC カードをかた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



2020 年 12 月のフィッシング報告件数は 32,171 件となり、11 月と比較すると 1,204 件増加となりました。
Amazon をかたるフィッシングの報告が多く、全体の約 50.0% を占めており、次いで三井住友カード、楽天、アプラス (新生銀行カード)、MyJCB 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 86.0 % を占めました。

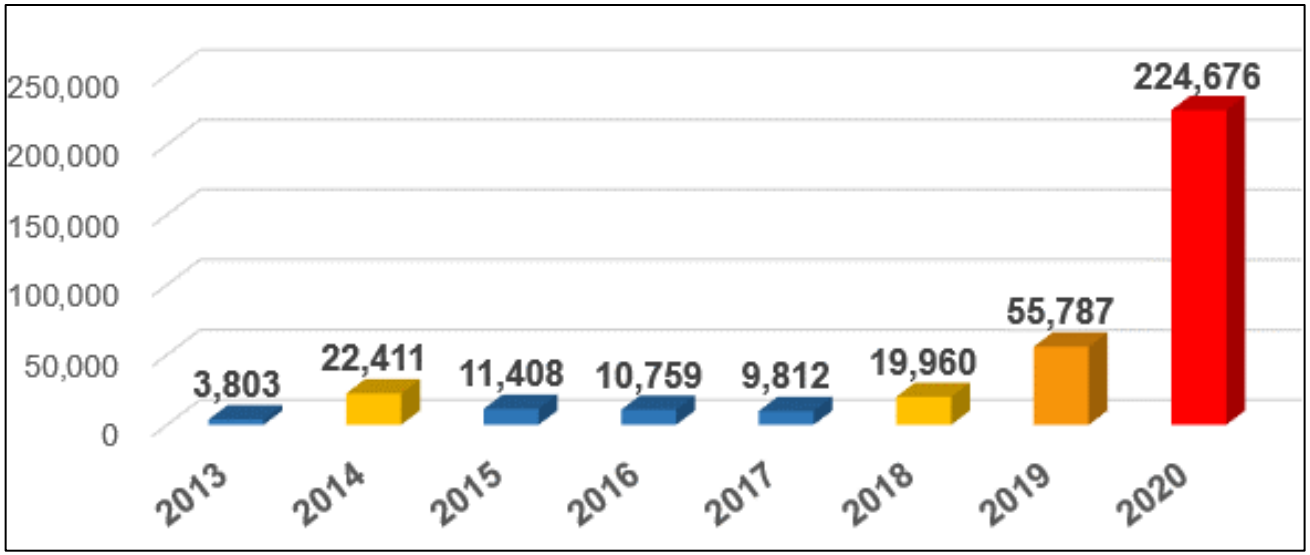
（2020/12 フィッシング報告状況 より）

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

フィッシング報告受領状況

フィッシング報告数の推移 （年別）

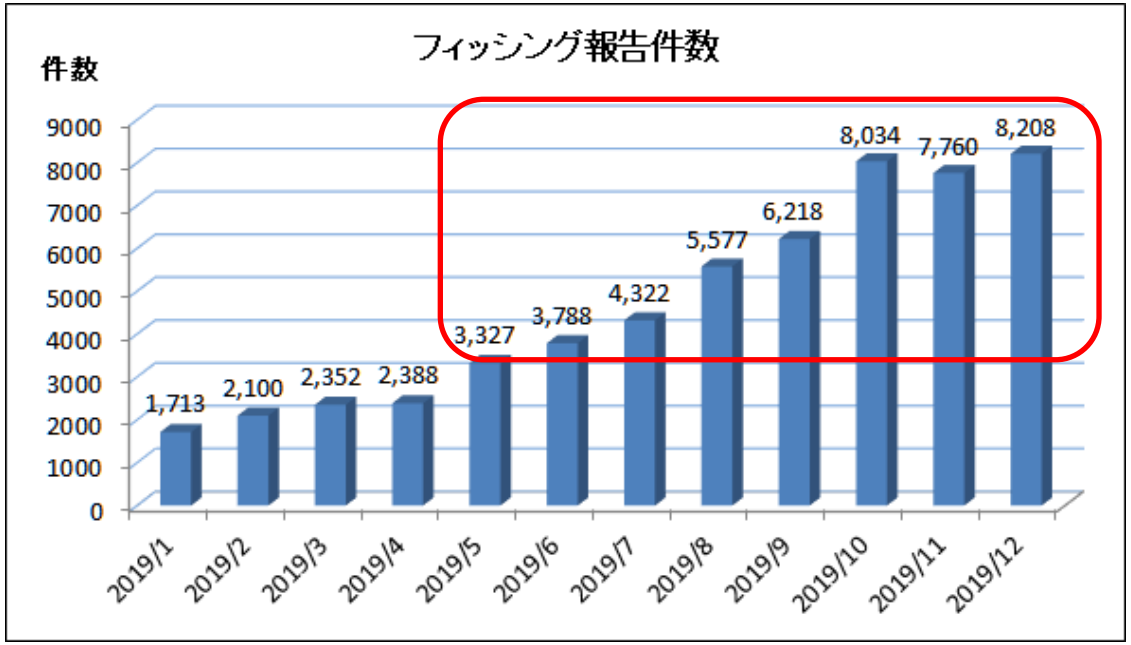
- 2020年は報告が激増。いまだ報告増加中
  2019年度の約4倍！22万4千超え！



- 目的はクレジットカード情報（世界中、どこでも簡単に使える）が主
- 2019年から2020年にかけては、不正送金目的のものも増加
  不正送金被害件数および被害額が急激に増えた
- SMSによるフィッシング（スミッシング）の報告も2019年以降、増加中
  不正アプリのインストールや銀行等のフィッシングサイトへ誘導

フィッシング報告数（2019年）

- 2019年後半から、急激に増加。

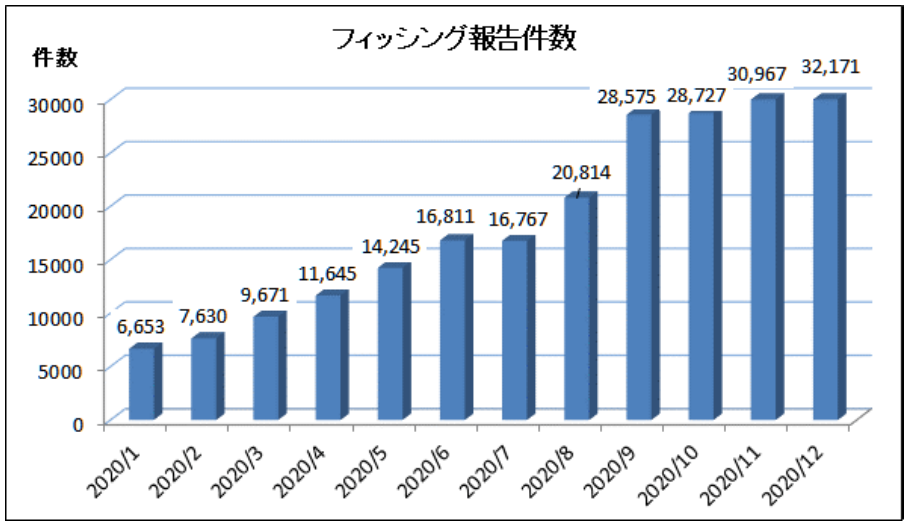


- 2019年主な増加の原因と傾向
  - スパムボットを使った大量メール配信　（週１配信 → 週数回配信）
  - 特定の海外事業者からの大量メール配信
  - 国内ISPユーザのアカウントを不正利用した踏み台メール送信
  - 国内ホスティング事業者を踏み台にした大量メール配信

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。
  - 12月には１月の約５倍の３万２千件！
  - 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
  - 大量配信される頻度と量の増加（1日4-5通、多い人で数十通 同じメールを毎日受信）
    PC (botnet) → サーバを使うようになり、配信リソースが増強
  - 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

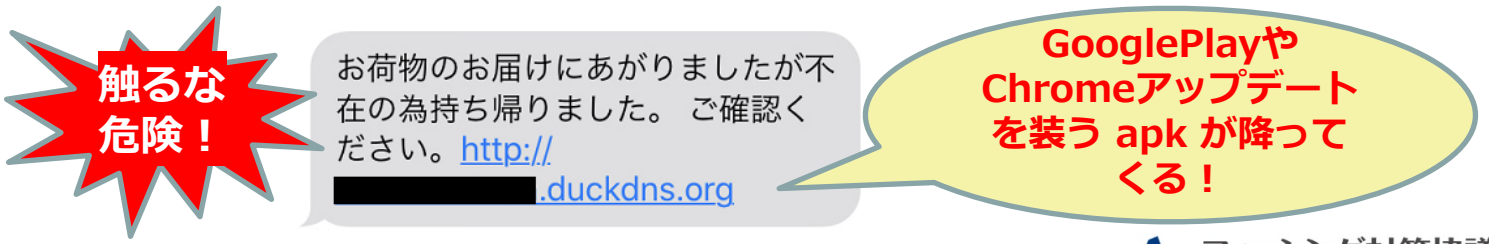
2020年も大量配信系は 80–90% を占めていた。
これらのフィッシングメールを減らしたい！

大量配信系フィッシングメール その１

- スパムボット経由での配信
  - マルウエア (Cutwail など) に感染した国内外の PC 等から直配送 (SMTP)
    - Amazon, Apple, 楽天をかたるフィッシングメールなど
    - 宛先には同じドメインの受信者のメールアドレスが列挙される場合が多い
    - 2020年6月まで週数回配信だったが、7月から減り始め、8月は数回配信のみ

大量配信系フィッシングメール その２

- 国内外事業者の設備（サーバ）を経由した配信
  - Amazon、楽天、クレジットカードブランドをかたるフィッシングメール
  - 正規サービスのドメインを使って、なりすまし送信するものも多数
  - 送信ドメイン認証や、迷惑メールフィルタを使えばブロックできるものも多い
- 特定の海外事業者からの直配送
  - CN 系が依然として多い
  - 一時期多かった TW 系は昨年 10月くらいから減った
    （特定ブランドのフィッシングメール配信に使われていたが、報告数ゼロになった）
- 正規のメール配信サービスを使った配信
  - 2020年前半は多かったが、後半はあまり見かけなくなった
  - sendgrid などのマーケティング用配信ツールを悪用
  - URL がメールごとでユニークで、正規サービスなので、URLフィルタが適用できない
- スマートフォンによるフィッシングSMS（スミッシング）配信
  - だまされてアクセスし、不正アプリ (遠隔操作マルウェア）をインストールしてしまった Android スマートフォンよる配信が非常に多い



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

迷惑メールフィルタの効果

- spam, meiwaku が件名についたメールも多数、報告される
- タグ付きメールを報告してくる方の他のメールも、ほとんどタグつき
  つまり**迷惑メールフィルタで、多くのフィッシングメールが検知できている**
- しかし、タグつきメールの割合は、報告全体の約18%
- 残り 82% は
  - 迷惑メールフィルタを使っていない？
  - X-ヘッダがついて、迷惑メールフォルダに振り分けられている場合もある

件名タグ	4月	5月	6月	7月	8月	9月	10月	11月	12月
spam	863	1,264	1,202	1,332	1,220	1,718	1,911	1,702	2,389
meiwaku	889	988	867	998	3,238	2,108	2,145	2,235	2,394
spam+meiwaku	1,752	2,252	2,069	2,330	4,458	3,826	4,056	3,937	4,783
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
検知割合	15%	18%	14%	15%	26%	16%	18%	16%	18%

- SPAM 判定されていることが、ヘッダを見ないと判らないメールの扱い
  - スマートフォンのみで、ヘッダでの振り分け設定をするのは厳しそう
  - 件名に [spam] をつけたほうが良いかも

利用者に迷惑メール検知・振り分けONの設定を用意し、
フィッシングメールが多い今こそ、利用者を守るために同意を得るとき！
＝ 事業者自身も守られます！

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月頃から増え始めた
  - Amazon のなりすまし送信メールはかなり多い
  - クレジットカードブランドも、なりすまし送信が増えている
    そして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
  - スマートフォンではヘッダなどの付加情報も、見るすべがない

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%
楽天	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%

- 送信ドメイン認証を使えば全体の **約 60%以上** 検出できる可能性がある

	4月	5月	6月	7月	8月	9月	10月	11月	12月
Amazonなりすまし	575	1,156	3,394	5,420	7,564	10,737	8,598	12,096	9,594
楽天なりすまし		51	124	470	512	1,059	789	625	1,046
クレカブランドなりすまし			191	310	153	1,648	2,757	4,431	6,857
二回目特別定額給付金							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%

なりすまし送信メールの例

- 普通のなりすましメール
  Envelope-From、Header-From ともに正規サービスのドメイン
  - ✓ SPF：**fail で検出可能**
  - ✓ DKIM：かならず fail
  - ✓ DMARC：**fail で検出可能**

```
Return-Path: <server@amazon.co.jp>
Authentication-Results: example.jp; dmarc=fail (p=quarantine dis=none) header.from=amazon.co.jp
Authentication-Results: example.jp; spf=fail smtp.mailfrom=server@amazon.co.jp
From:          Amazon.co.jp <server@amazon.co.jp>
Subject:       【重要】カード情報更新のお知らせ
```

- 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 で検出不可**
  - ✓ DKIM：独自ドメインの正規署名をつけられると **pass で検出不可**
  - ✓ DMARC：**fail で検出可能**

```
Return-Path:    <no-reply@amauon-****.jp>
Authentication-Results: example.jp; dmarc=fail (p=quarantine dis=none) header.from=amazon.co.jp
Authentication-Results: example.jp; spf=pass smtp.mailfrom=no-reply@amauon-****.jp
Authentication-Results: example.jp; dkim=pass (1024-bit key) header.d=amauon-****.jp
                header.i=no-reply@amauon-****.jp header.b="bFg1iNWO"
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=default; d=amauon-****.jp; h=略;
                i=no-reply@amauon-****.jp;  （以下、略）
From:           Amazon.co.jp <account@amazon.co.jp>
Subject:        あなたのAmazonアカウントはセキュリティ上の理由で中
```

SPFとDKIMは、検証につかうドメイン名を独自ドメインにされると効果がない

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

- Envelope-From、Header-From ともにランダムな値（ドメイン）
  2-8文字+TLDで実在する/しない関係なく使用。
  2-3文字+TLDは、ほぼ実在するドメイン（結果、なりすましとなる）
  - ✓ SPF：**fail で検出可能**
  - ✓ DKIM：署名がついていない または fail
  - ✓ DMARC：**fail で検出可能**

使っていないドメイン でも送信ドメイン認証 関連の宣言する

検出不可 ✖

■SPF/DMARCの宣言なしのパターン

Return-Path: <hxsmhdyke@***.net>
Authentication-Results: example.jp; **spf=none** smtp.mailfrom=hxsmhdyke@***.net; dkim=none;
dmarc=none header.from=hxsmhdyke@***.net
From: amazon <hxsmhdyke@***.net>
Subject: お支払い方法の情報を更新

検出可能 ○

■SPF/DMARCも宣言しているパターン

Return-Path: <ynxxud@**.org>
Received-SPF: **fail** (**.org: domain of ynxxud@**.org does not designate ***.***.***.*** as permitted sender)
receiver=**.org; client-ip= ***.***.***.***; envelope-from=ynxxud@**.org;
Authentication-Results: example.jp from=**.org; domainkeys=neutral (no sig); dkim=neutral (no sig); header.i=@**.org;
dmarc=fail (p=NONE,sp=NONE,pct=100,domain=**.org); header.from=**.org
From: amazon <ynxxud@**.org>
Subject: お支払い方法の情報を更新

検出不可 ✖

■未登録ドメインのパターン （受信拒否して良いと思う）

Return-Path: <zav@drw****.net>
Received-SPF: **none** (drw****.net: domain of zav@drw****.net does not designate permitted sender hosts)
Authentication-Results: example.jp from=drw****.net; domainkeys=neutral (no sig);
dkim=neutral (no sig); header.i=@drw****.net; dmarc=none; header.from=drw****.net
From: amazon <zav@drw****.net>
Subject: お支払い方法の情報を更新

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

送信ドメイン認証の問題点：判定の相違

- SPFで検証失敗するケース
  SPF の RR で include 指定されているが、include 先のドメインで当該 RR が登録されていない
  - ある実装では
    - ✓ SPF：**permerror or unknown で検出不可**
    - ✓ DMARC：**permerror で検出不可**

PermError
(Permanent Error)
認証情報の記述ミス
定義なしと同じ扱いとなる

```
Return-Path: <mym@amazon.co.jp>
Received-SPF: unknown (amazon.co.jp: domain of mym@amazon.co.jp
              encountered an error while parsing (check SPF record amazon.co.jp for errors))
Authentication-Results: example.jp from=amazon.co.jp; domainkeys=neutral (no sig);
              dkim=neutral (no sig); header.i=@amazon.co.jp; dmarc=permerror; header.from=amazon.co.jp
From:         Amazon <mym@amazon.co.jp>
Subject:      Amazonプライムの自動更新設定を解除いたしました！
```

  - DMARC fail 判定する実装もある

```
Authentication-Results: example.jp; dmarc=fail (p=quarantine dis=none) header.from=amazon.co.jp
Authentication-Results: example.jp; spf=fail smtp.mailfrom=dldlnnxyoc@amazon.co.jp
From: Amazon <dldlnnxyoc@amazon.co.jp>
```

```
Authentication-Results: example.jp; spf=permerror smtp.mailfrom=xzcymube@amazon.co.jp; dkim=none
header.d=amazon.co.jp header.b=; dmarc=fail header.from=amazon.co.jp
From:         Amazon <xzcymube@amazon.co.jp>
```

    - ➢ include 先で RR がない場合のDMARC判定結果が、事業者（実装）によって違う
    - ➢ 参照先のドメインの RR がきちんと管理されているか、実際にはあまり確認されていない permerror では気が付かないので、fail がさせることが、望ましいと思われる

送信ドメイン認証の問題点：判定の相違

- DKIMで検証失敗するケース
  - Envelope-From は SPF 宣言していない独自ドメイン（未登録含む）のメールアドレス
  - Header-From は DMARC 対応済の実在するドメイン
  - DKIM 署名は、DKIM 対応しているドメインの偽署名（正規メールからコピー？）
  - ある実装では
    - ✓ SPF：**none**
    - ✓ DKIM：**permerror （bad sig）**
    - ✓ DMARC：**permerror (fail しない)**

```
Return-Path:    <oanq02@vemanch****.com>
Received-SPF:  none (mail-.google.com: domain of oanq02@vemanch****.com does not designate permitted  sender hosts)
Authentication-Results: example.jp from=vemanch****.com; domainkeys=neutral (no sig);
                        dkim=permerror (bad sig);  header.i=@societyforscience-***.com;
                        dmarc=permerror  (p=REJECT,sp=REJECT,pct=100,domain=accounts.google.com);
                        header.from=accounts.google.com
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=200608; d=societyforscience-***.com;
                        h=From:To:Subject:Date:List-Unsubscribe:MIME-Version:Reply-To:List-ID:
                        X-CSA-Complaints:Message-ID:Content-Type; i=reply@societyforscience-***.com; (以下、略)
From: Amazon.co.jp <no-reply@accounts.google.com>
Subject: 【重要】Amazon.co.jpアカウントが停止されました、再度アクティブにしてください
```

```
Authentication-Results: example.jp from=google.com; domainkeys=neutral (no sig);
                        dkim=permerror (bad sig); header.i=@accounts.google.com;
                        dmarc=permerror (p=REJECT,sp=REJECT,pct=100,domain=google.com); header.from=google.com
```

  - dmarc=fail する事業者（実装）もある（こちらのほうが望ましい）
    - ✓ **permerror 判定されると DMARC 無効と同じ**
    - ✓ **DMARC を優先し、SPF/DKIM の permerror = 検証失敗 (fail) が妥当と思われる**

不完全なメールアドレス

- DMARC が使えないパターン
  - Envelope-From 独自ドメイン、Header-From 不完全なメールアドレス
    - ✓ SPF：**pass で検出不可**
    - ✓ DKIM：独自ドメインの正規署名をつけると **pass で検出不可**
    - ✓ DMARC：**none で検出不可**（**迷惑メールフィルタでは容易に検出可能**）

```
Return-Path: <kefu@xtr****.cn>
Received-SPF: PASS identity=mailfrom; envelope-from="kefu@xtr****.cn"
Authentication-Results: example.net; dmarc=none (could not find any valid author domain)
From:          rakuten.co.jp <Rakuten>
Subject:       【楽天市場】お支払い方法を更新してください知らせ
```

- ✓ **スマートフォンだとメール受信者に見えるのは、Display Name だけで気が付かない**
- ✓ **PC ユーザでも通常 Header-From しか見ない**
- ✓ **Outlook 系はヘッダを書き換えて Envelope-From を表示する**
  スマホユーザも「これはおかしい！」と気がつくことができる

```
From: "rakuten.co.jp" <Rakuten>
Subject: 【重要】カード情報更新のお知らせ

From: noreply@gtt****.cn <noreply@gtt****.cn> On Behalf Of rakuten.co.jp
Subject: 【重要】カード情報更新のお知らせ
```

Envelope-From に書き換える

- ✓ **内部 Relay 時に問題が発生する可能性もあるので、Header-From はチェックしてはどうか？（次のページにつづく！）**

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

なりすまし？（不完全なメールアドレス）

- @以降に受信組織のホスト名がついた なりすましメール（？）
  - From: "Amazon.co.jp" <Amazon@host1.example.jp>
  - 当該ホスト名のサーバを経由している (Postfixらしい)
    - local_header_rewrite_clients
    - remote_header_rewrite_domain
  - @以降がないHeader-Fromに自身のホスト名を追加してしまっている
    - 元は From: "Amazon.co.jp" <Amazon>
  - 送信ドメイン認証の検証サーバがその後方だと、自ドメイン（ホスト名）でDMARC検証してしまう場合も…

```
Authentication-Results:  host2.example.jp; dmarc=none (p=none dis=none) header.from=host1.example.jp
Authentication-Results:  host2.example.jp; spf=fail smtp.mailfrom=bgwsbx@amazon.co.jp
Received:       from host0.example.jp by host1.example.jp (Postfix) with ESMTP id 40923DC00EE for
                <hogehoge@example.jp>; Mon, 24 Aug 2020 14:13:07 +0900 (JST)
Received:       from amazon.co.jp (unknown [***.***.***.***]) by host0.example.jp (Postfix) with ESMTP id
                78D6117C1E3 for <hogehoge@example.jp>; Mon, 24 Aug 2020 14:13:06 +0900 (JST)
Sender:         bgwsbx@amazon.co.jp
From:           Amazon.co.jp <Amazon@host1.example.jp>
```

  - フィッシング（迷惑）メールが自組織ドメインのメールアドレスでエンドユーザに着信するので混乱を誘発
  - 内部配送でいくつも **Postfix の Relayサーバ**を経由するところは、**要確認**！
  - 前回も言いましたが、いまだに直ってない and 大手や老舗が多い
    （設備拡充、サーバ追加の際に、こういう設定が混ざったと思われる）

フィッシングメールの送信ドメイン認証対応例

- 送信ドメイン認証をきっちり pass するメール
  - Envelope-From、Header-From ともに独自ドメインを使う
    - ✓ SPF：**pass !**
    - ✓ DKIM：**pass !**
    - ✓ DMARC：**pass !** しかも **p=QUARANTINE !**

```
Return-Path:    <contact@paypal ****.cf>
Received-SPF: pass (mta0.paypal ****.cf: domain of contact@paypal **** .cf designates ***.***.**.* as permitted sender)
                receiver=mta0.paypal ****.cf; client-ip= ***.***.**.*; envelope-from=contact@paypal ****.cf;
Authentication-Results: example.jp from=paypal **** .cf; domainkeys=neutral (no sig); dkim=pass (ok);
                header.i=@paypal ****.cf; dmarc=pass (p=QUARANTINE,sp=NONE,pct=100,domain=paypal ****.cf);
                header.from=paypal ****.cf
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; s=default; d=paypal ****.cf; h=From:To:Subject:Date:Message-
                ID:MIME-Version:Content-Type; i=contact@paypal **** .cf;....(以下、略)
Subject:        【重要】PayPalカスタマーサービス (2021/1/11 18:17)
```

国内正規サービス、負けてます…．
がんばりましょう

今後の対策

フィッシング 対応の限界

- 今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 → **困難**）
  - セキュリティ対策事業者・サービスによるURLフィルタリング → **限界**
    - Safebrowsingに登録されるとフィッシングサイトが止まり、次のサイトが稼働する
    - 短時間で自主的に停止してしまうものも多い
  - フィッシングサイトのテイクダウン → **限界**
    - 停止調整は（頑張っているけれど）それなりに時間がかかる
    - 被害者はメールを送ってから２－３時間以内にアクセスしている

- これからのフィッシング対策
  - フィッシングメールを送らせない、受け取らない
    迷惑メール対策技術を使ったフィッシングメール対策
  - 不正なメールが届かなければ、被害は減るはず

  - **技術でできることは、技術で対応したい**
  - **技術でできないことは、データを積み重ね、解決策を模索したい**

でも、送信ドメイン認証も、やれば効果あるのに
全然導入が進まない…

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。

なりすましメール 防御側の対応

- 送信ドメイン認証への対応
  - まずはSPFとDMARCで、p=none で調査をスタートしましょう
    それだけでも、受信側は検証結果が使えるので利益があります
  - メール送信に使わないドメインは「明確に送信しない設定」をする
    メールにしか作用しないので、いますぐ設定！

- 送信ドメイン認証はセキュリティ対策の一環
  - DMARCレポートで、なりすましメールを送られてる状況を可視化できます
  - なりすましフィッシングメール送信を容認しているのは組織として問題
  - 何もしない＝正規のメールが不正なメールと同じでは、もう信用されません
    - 利用者を危険にさらし続けているのは問題
    - 正規メールも迷惑メールとして利用者に分別され、読んでもらえない
  - メール環境を整理、管理し、正規のメールを届ける努力をする

自組織のドメインを使ったなりすましメールから
自組織とユーザを守りましょう

現状、フィッシングメールを送る側のほうがSPF、DKIM、
DMARCを駆使してメールを届ける努力をしています

なりすましメール 受信側の対応

- DMARC 受信側の対応
  - DMARCレポート (集約レポート、Aggregate report) の生成、送信
  - p=none なら迷惑メールフィルタの判定の一要素として検証結果を使用
  - p=quarantine なら検証が fail した場合、迷惑メールボックス等へ振り分ける
  - p=reject なら検証が fail した場合、ブロックまたは迷惑メールボックス等へ振り分けする
  - 検証が fail した場合、件名にタグを追加する
    スマートフォンユーザ向けの対応 [spam]? [fake]? [偽]?

- 迷惑メールフィルタ利用への誘導
  - 送信ドメイン認証結果によるフィルタリング＝迷惑メールフィルタを使うこと
    利用者の同意を得られる

送信ドメイン認証のテスト

- 送信ドメイン認証の判定結果の検証
  - 正常パターンはテストされているが、細工されたメールの判定結果は利用する実装によって相違がある
    - Permerror or fail?
      fail してほしいのに permerror だと SPF/DMARC を宣言していても無効となってしまう
    - 検証用メール（細工されたメール）のテストが必要
    - フィッシング対策協議会に寄せられた膨大な報告メールから permerror のパターンを抽出し、各実装でテストを行ってもらう、等

それ以外の技術的対策

- 送信制限
  - メール送信（SMTP-Auth）利用制限
    （Submission Port への接続は海外からはデフォルト禁止など）
  - 不審な認証パターンが見られるアカウントの自動停止
  - 動的IPアドレスレンジ、モバイル系アドレスレンジからの SMTP 直配送を制限

- 送信制限の例 （前回も記載）
  - **イッツコム：海外からのメール送信仕様の変更について**
    https://www.itscom.co.jp/support/userinfo/20190918_gjslkq0000008td2.html

    マイページより「海外からのメール送信」をONにすることで、1週間（設定後マイページに表示）海外からメールを送信することが可能になります。

  - **OCN: 単位時間移動量によるSMTP認証アカウントの自動停止**
    https://internet.watch.impress.co.jp/img/iw/docs/1219/335/html/03a_o.jpg.html

    条件：単位時間当たりにX力国以上のIPアドレスからSMTP認証要求を発信した
    対象：SMTP認証アカウント
    方法：ログから条件合致の対象を抽出、認証不可のフラグを立てる

事業者各社さまの努力で、2020年は、SMTP認証不正利用の送信は減っています

それ以外の技術的対策 （案）

- 発信元IPアドレス/ドメインのレピュテーションなど
  やはり発信元の情報は判断するうえで重要
  - SMTP-Auth 時の接続元 IP アドレスまたは地域情報をヘッダに明記
  - MXへのSMTP 接続元 IP アドレスまたは地域情報をヘッダに明記
    - Yahoo のX-Originating-IP
    - NIFTY のX-Nifty-SrcIP
  - ブランド名と発信元IPアドレス情報の組み合わせによる判断
    - Amazon 等のキーワード＋CN から着弾したメールなど
  - レピュテーションに基づくレート制限
  - 送信ドメイン認証の検証時、未登録ドメインであれば受信しない
    （SOAを見る？）

現在の配信は国内クラウド経由も増えており、
継続してIPレピュテーションは必要ではあるが、
正規契約のAbuseに関しては、判断が難しい

そもそも、送信は完全には止められない
送信側を止められないなら、
受信側で判断

まとめ

- フィッシング報告は2020年は 2019年の約4倍になり、今後も増える予想
- 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
- 被害ブランドと関係のないドメイン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
- 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 はすぐ対応できる。

まずは自組織のドメインにDMARCを宣言しましょう

今後の議論

- 議論の場
  同業同士の情報交換も大事
  でも他の立場からの意見を聞くのは、とても参考になります
  - フィッシング対策協議会 被害状況共有WG
    協議会会員のみ参加可能ですが、フィッシング対策を行う組織やベンダーが集まり、対策について議論や情報共有を行っています
  - 迷惑メール対策推進協議会 技術WG
    フィッシングメール配信の状況について、共有しています
    迷惑メール対策も含め、前向きな議論をしましょう
  - JPAAWG
    このあと、櫻庭氏より説明

対策のために必要な情報は可能な限り共有します
一緒に考えて行きましょう！

ご視聴ありがとうございました