2022年11月７日
JPAAWG 5th General Meeting

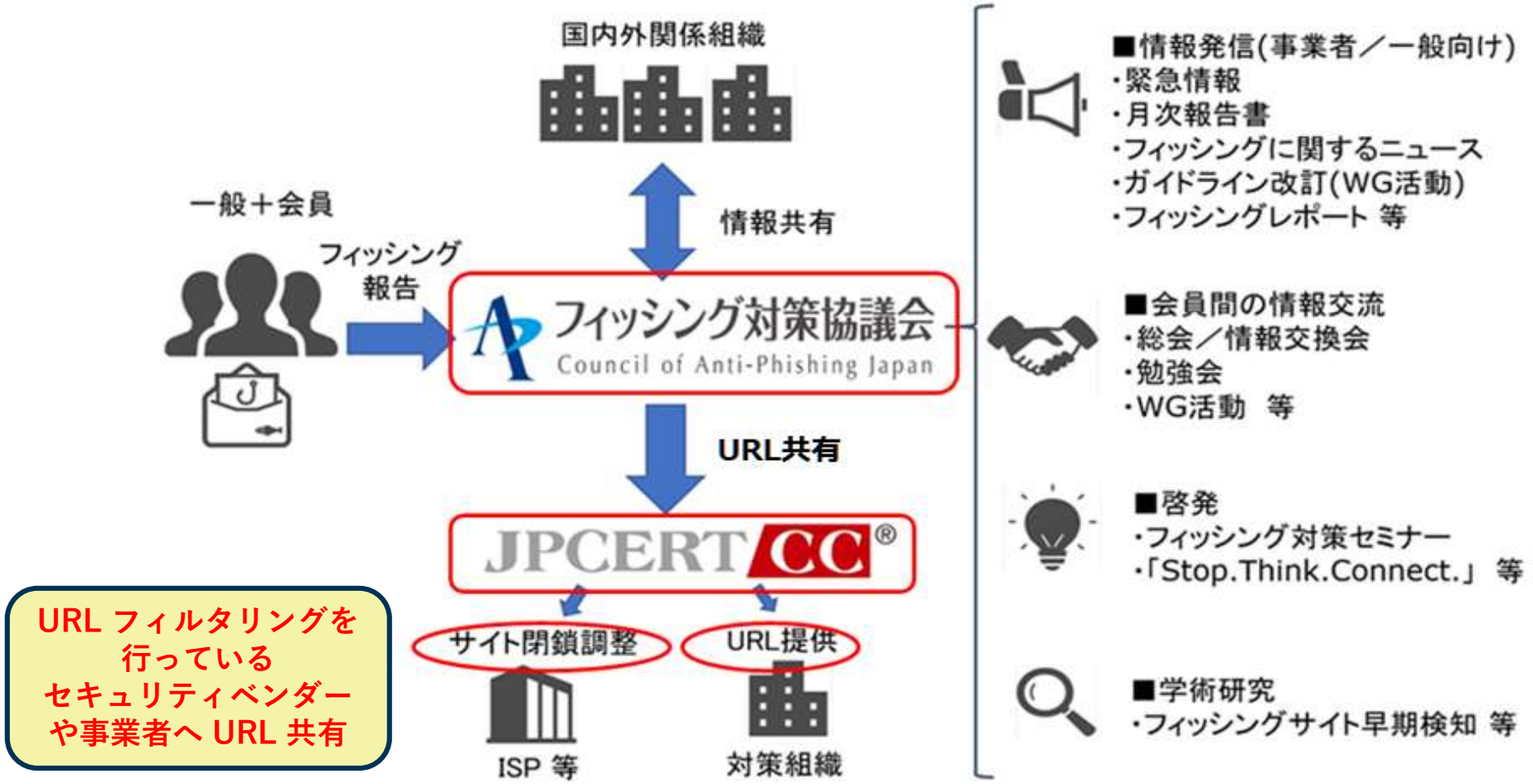
2022年版
フィッシング報告状況と対策

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・クレジットカード関連など
  - 会員+オブザーバー 118 組織 （2022 年 10 月時点）
    正会員： 91 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)
- 事務局およびフィッシング報告受付窓口
  - 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 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）フィッシングのメール文面とサイト画像を掲載

フィッシング対策協議会「緊急情報」より

フィッシング対策協議会 情報発信

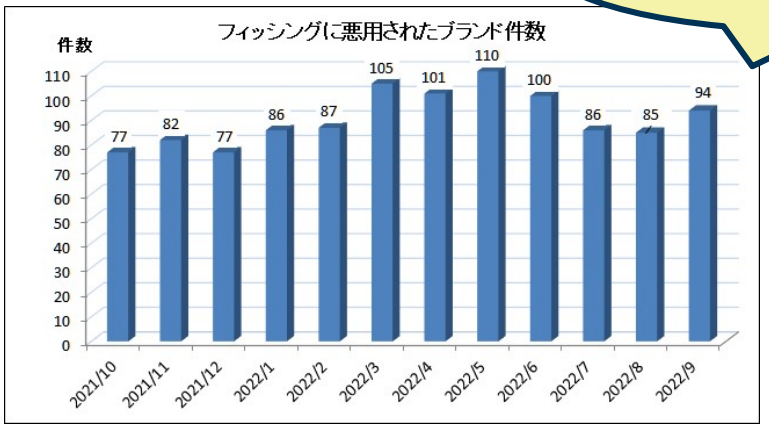
- フィッシング報告状況 （月次報告書）
  https://www.antiphishing.jp/report/monthly/

受領した報告をもとに分析し、

- 報告数、URL、ブランド
- その月の傾向、分析
- 有効な対策

など、フィッシングの最新情報を掲載

フィッシングの最新動向がわかる！



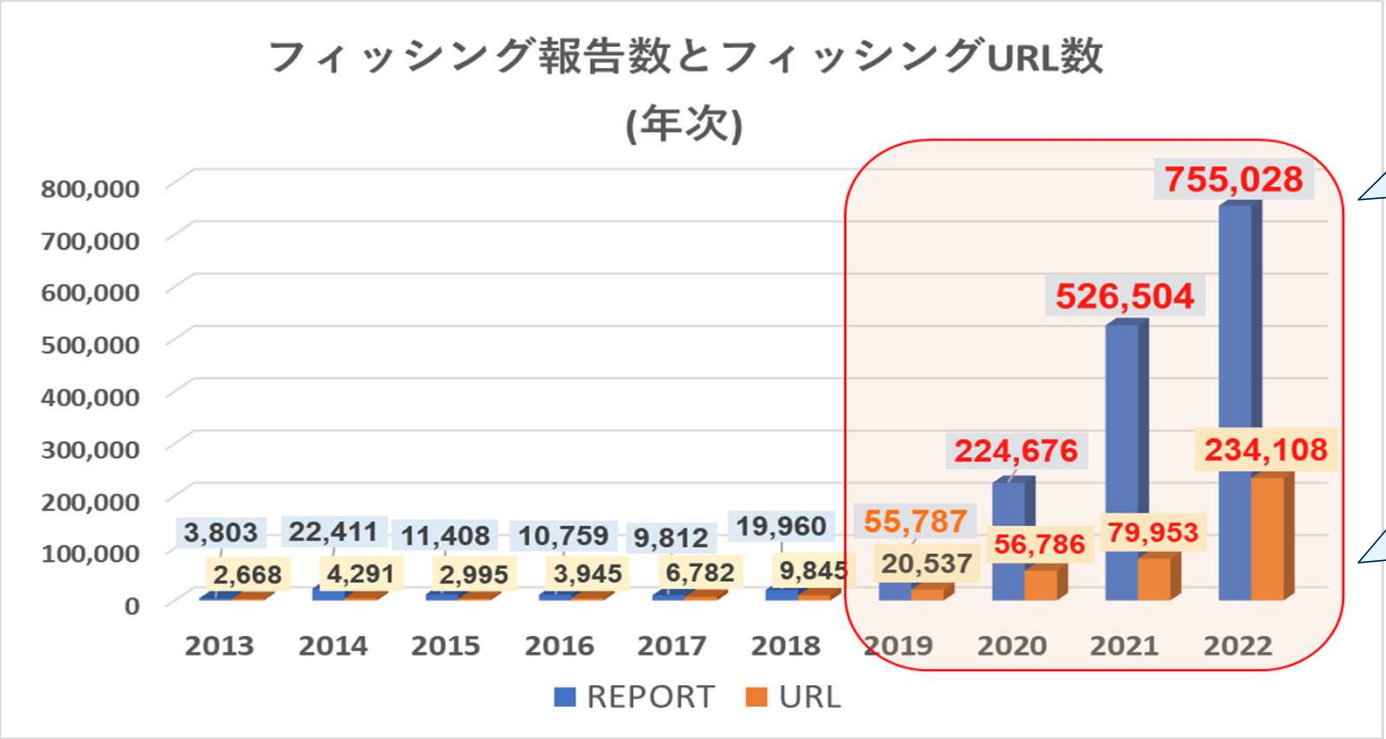
2022 年 9 月のフィッシング報告件数は 102,025 件となり、2022 年 8 月と比較すると 7,052 件増加しました。
6 月に緊急情報を掲載した「クレジットカードの利用確認を装うフィッシング」の報告が引き続き多く、報告数全体の約 38.7 % となり、誘導元フィッシングメールが確認された 8 ブランドのうち、特に VISA、セゾンカード、JCB をかたるメール文面が多く報告されました。次いで報告が多かった Amazon、三井住友銀行、イオンカードをかたるフィッシングの報告をあわせると、全体の約 68.8 % を占めました。また、1,000 件以上の大量の報告を受領したブランドは 15 ブランドあり、これらで全体の約 90.2 % を占めました。
分野別では、クレジット・信販系は報告数全体の約 61.4 %、EC 系 約 17.5 %、金融系 約 9.9 %、交通系 約 4.0 %、省庁 約 2.9 %、オンラインサービス系 約 2.5 % となりました。

フィッシング対策協議会 「2022/9 フィッシング報告状況」より

2022年フィッシング報告状況

フィッシング報告件数の推移 (年別)

- ここ2-3年で報告が急増、**2021年には「社会問題」と言われるようになる**
  - 報告数は **2022 年 9 月末時点で、2019年 (3 年前) の約 13.5 倍**。
  - URL件数は **2022 年 9 月末時点で、2019 年の約 11.4 倍。**
  - 各事業者、利用者ともにフィッシングへの対応コストが増加



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、踏み台送信が多かった

2020 年頃からホスティング事業者発のフィッシングメール配信が増える。同時になりすまし送信も増え始めた

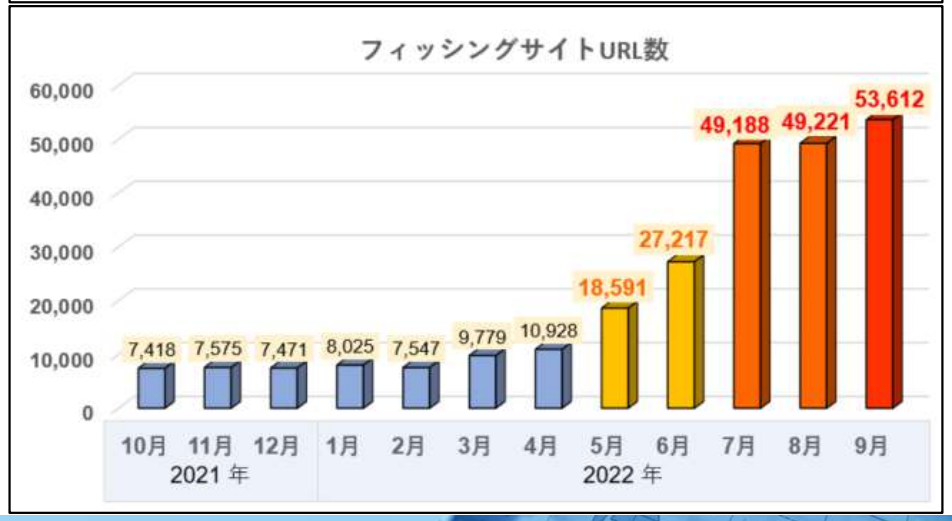
フィッシング報告の推移 (2022年 月別)

■ フィッシング報告件数の傾向

- **2022年3月以降、急増。7月には 10 万件突破**
- 報告数は昨年同時期の倍以上となっている
- メール配信規模が非常に大きくなってきている
- **あるブランドは 1カ月に数億通以上のなりすましフィッシングメールを配信されたことが、DMARCレポートから確認**された
- 漏えいデータ等から配信先メールアドレスを収集しており、**配信範囲が広がっている**

■ フィッシングサイト (URL) 件数の傾向

- **2022年5月以降、急増。9月には 5 万件突破**
- 大量のドメイン、サブドメインを組みあわせて、大量にURLを生成。(**全体の7-8割以上を占める**)
- **同一のURLが少なく、ブラウザーのURLフィルターが有効に機能しない**
- 日本以外からアクセスするとフィッシングサイトが見れない、同じIPアドレスから１度しか見れない等、**テイクダウンされづらい仕組みが実装されている**

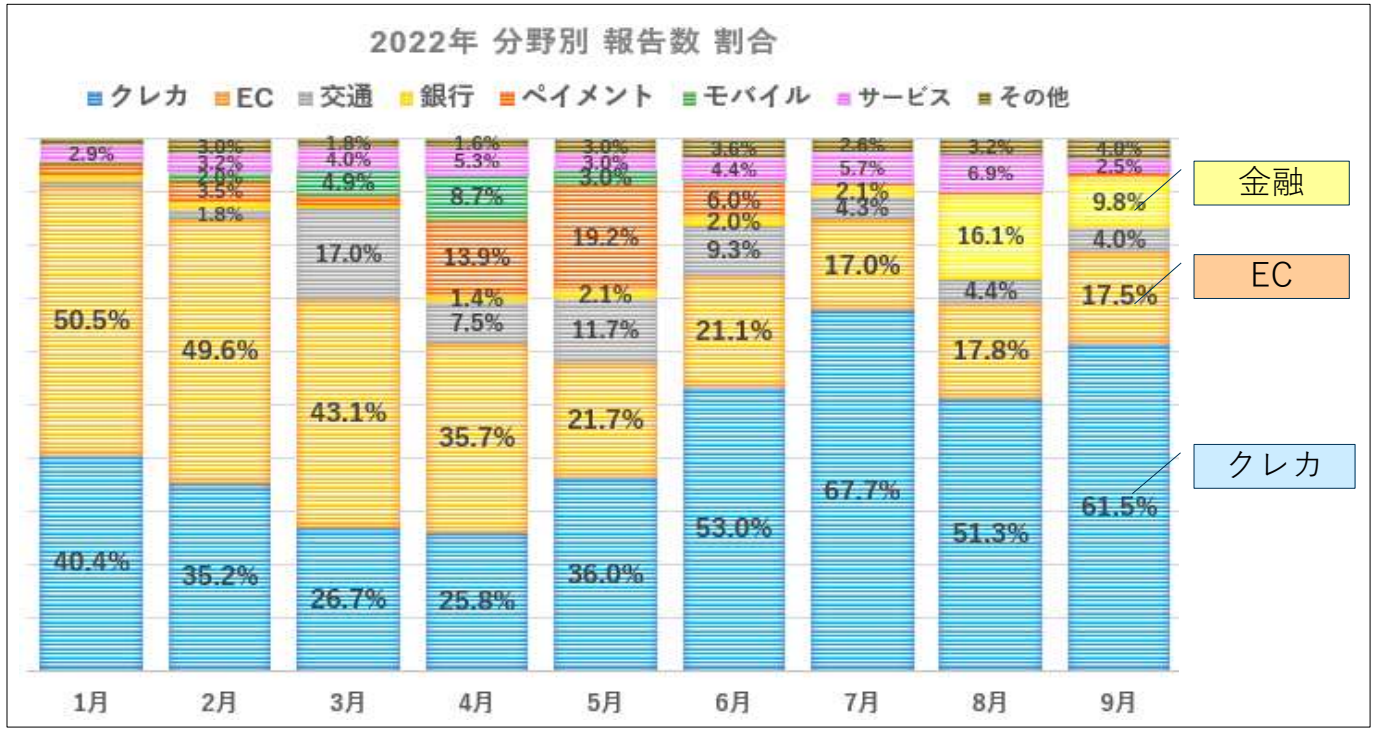


分野別報告数の割合 (2022年 9月末まで)

- クレジットカードを利用できるサービスであれば、特に分野は限らず、ユーザー数が多いブランドを中心に、成功率が高かった誘導メール文面で繰り返し狙う
- 2021年後半からキャッシュレス決済の不正利用目的のフィッシングが増え始め、4月～6月頃、特に増えた
- 4月頃から金融機関をかたるフィッシングの報告が増え始め、8月～9月頃、特に増えた
- 8月国税庁をかたるフィッシング（メール、SMS）が発生し、以降、定番入りし続いている

- 2022年報告数TOP3

2022年月次順位			
	1位	2位	3位
1月	Amazon	メルカリ	JCB
2月	Amazon	メルカリ	JCB
3月	Amazon	メルカリ	えきねっと
4月	au (PAY)	Amazon	メルカリ
5月	au (PAY)	Amazon	えきねっと
6月	Amazon	イオンカード	えきねっと
7月	クレカ	Amazon	三井住友カード
8月	クレカ	Amazon	三井住友銀行
9月	クレカ	Amazon	三井住友銀行

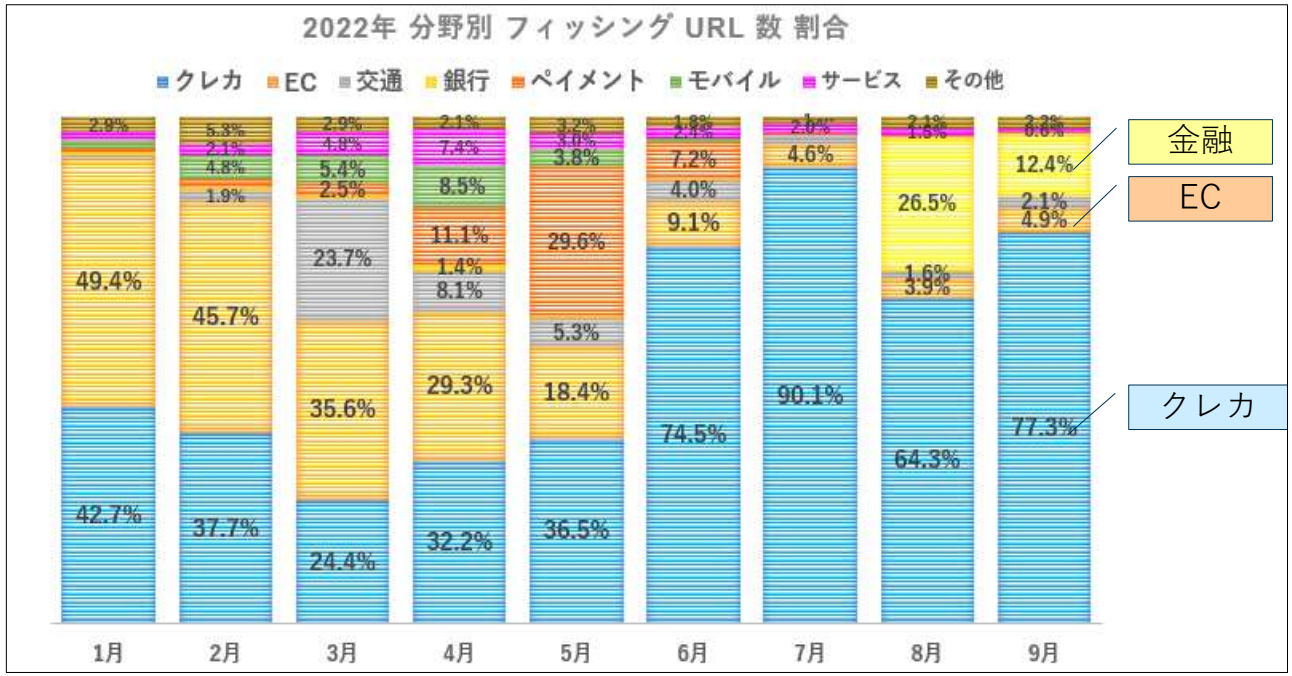


分野別 URL 数の割合 (2022年 9月末まで)

- 6月～9月、クレジットカードブランドのフィッシングサイトのURLが大量に報告される
- フィッシングサイトのデザインは同じだが、誘導メールは多数のブランドが使われた

- 2022年URL数TOP3

2022年月次順位（URL）	1位	2位	3位
1月	Amazon	三井住友カード	メルカリ
2月	Amazon	MICARD	メルカリ
3月	えきねっと	Amazon	メルカリ
4月	Amazon	au (PAY)	三井住友カード
5月	au (PAY)	Amazon	VISA
6月	クレカ	au (PAY)	Amazon
7月	クレカ	Amazon	ETCサービス
8月	クレカ	三井住友銀行	Amazon
9月	クレカ	三井住友銀行	Amazon



メールによるフィッシングへの誘導

【VISAカード】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.●●●●.com.cn/ic6oXx7P3s/page1.php> 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■
VISAカード
東京都中野区中野4-3-2

メール文面の例

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

- 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
  - 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 など
    （順不同）

- このタイプは配信量が非常に多く、報告が多い
- 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6月以降に増えた大量のURLを使用した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月以降)
  - 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

今まで主流だったURLフィルタリングによる対策で効果が出にくい状況
誘導元となるフィッシングメールへの対策を行うことが、ますます重要となる

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

2022年報告からみる
効果的なフィッシング対策
「なりすましメール対策」

なりすまし送信とは

- 「なりすまし」送信とは
  - **実在するメールアドレスをかたり、偽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**
    （メールアドレスの@より後ろの部分＝ドメインが本物と同じ）
  - **最近はDMARC対応していない他事業者のメールアドレスを使うケースもよく見られる**

- 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（見分けがつかず、フィッシング成功率が高い）**
  - 迷惑メールフィルター等でブロックされづらい（届きやすい）
  - メールを送るためにドメインを取らなくて良い（コストがかからない）

なりすまし送信メール メールソフトでの表示例

フィッシングを行う側にとっては成功率が高くなり、コストもかからない
でも**なりすまし対策技術を行えば、メール着信率 (成功率) を下げられる**

なりすまし送信メールの例（フィッシング）

- 国税庁のドメイン（e-tax.nta.go.jp）を使ったなりすまし送信（2022/9/19 配信）

差出人：e-Tax（国税電子申告・納税システム） <info@e-tax.nta.go.jp>
件名：税務署からの【未払い税金のお知らせ】
日付：2022年9月19日 18:06:33 JST

e-Taxをご利用いただきありがとうございます。

あなたの所得税（または延滞金（法律により計算した客観 について、これまで自主的に納付されるよう催促してきま したが、まだ納付されておりません。
もし最終期限までに 納付がないときは、税法のきめるところにより、不動産、自動車などの登記登録財産や給料、売掛金などの債権など の差押処分に着手致します。

納税確認番号:****0936

滞納金合計:10119円

納付期限：2022/09/19

最終期限：2022/09/19 （支払期日の延長不可）

お支払いへ→ https://nta[redacted].com

※ 本メールは、【e-Tax】国税電子申告?納税システム(イータックス)にメールアドレスを登録いただいた方へ配信しております。

なお、本メールアドレスは送信専用のため、返信を受け付けておりません。ご了承ください。

発行元：国税庁 〒100-8978 東京都千代田区霞が関3-1-1 （法人番号7000012050002）

e-Tax（国税電子申告・納税システム） <info@e-tax.nta.go.jp>
本物メールにも使われている差出人

e-Tax を利用して納税している利用者は、
差出人が本物と同じであるため、
ついアクセスしてしまう

クレジットカード情報の詐取を狙った
フィッシングサイトなどへ誘導する

なりすまし送信メールの例（マルウェア）

- 厚生労働省のドメイン（mhlw.go.jp）を使ったなりすまし送信（2021/12/4 配信）
  マルウェアのインストールへ誘導

From: 厚生労働省 <hjhvs@mhlw.go.jp>
Sent: Saturday, December 4, 2021 8:45 AM
Subject: 【緊急】新型コロナウイルスの変種のため、15日以内の個人情報を報告してください

2021年12月4日現在、新型コロナウイルスには再び変種が出現しています。

新型コロナウイルスの最新の変種Omicronは南アフリカで発見された。

社会秩序および住民の健康を維持するため、15日間の個人情報を報告してください。

厚生労働省としては、引き続き、各国政府やＷＨＯ、専門家等とも連携しつつ、諸外国の感染状況を注視しながら、機動的な感染拡大防止対策に努めてまいります。

URLからフォームをダウンロードして個人情報を記入し、このメールに返信してください。

https://iab●●.com/

（表はエクセル形式です,開くことができない場合は、ウイルス対策ソフトを閉じるか、ホワイトリストにフォームを追加してみてください。）

緊急事態ですので、住民の皆さんも協力して行動してください。ありがとうございます。

【配信元】
厚生労働省 https://www.mhlw.go.jp/

〒100-8916 東京都千代田区霞が関1-2-2

電話番号 03-5253-1111（代表）

Copyright © Ministry of Health, Labour and Welfare, All Rights reserved.

厚生労働省 <hjhvs@mhlw.go.jp>

変種のオミクロン株が発見された、と
時事ネタを入れて誘導

Excel ファイルを装い、ウイルス対策ソフトを
閉じるよう誘導

それはなりすましメールです！
弊社は送っておりません！と言ってるだけでは被害は減らず、なんの効果もない。
なりすましメール対策を行い、正規メールを証明する手段を提供することが、サービス提供者としての最低限の義務と考える。

またドメイン=ブランドを不正利用から保護することは、現代のセキュリティの基本と心得る

なりすましメール対策

■ 送信ドメイン認証

メールが正規の送信元から送られてきたか、検証できる技術。現状、SPF、DKIM、DMARC の 3 種類ある

SPF	Sender Policy Framework
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
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）**
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。
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 も素通し）
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**

DKIM	DomainKeys identified mail
検証方法	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
検証対象	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）
導入	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
利点	メールを転送されても検証可能
欠点	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

なりすましメール対策

■ 送信ドメイン認証 DMARC
SPFとDKIMの欠点を補い、有用な機能を実現

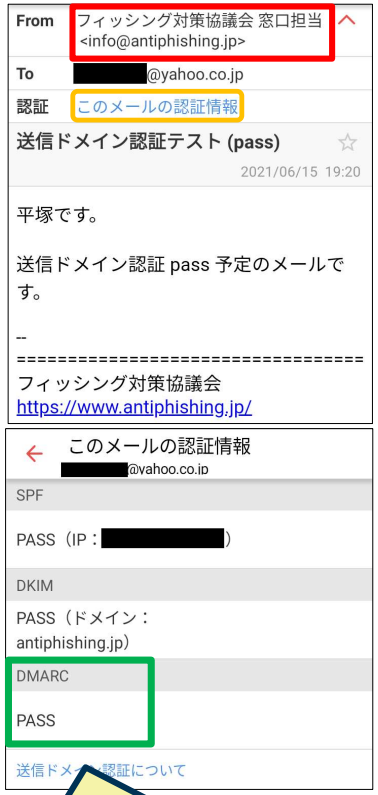
DMARC	Domain-based Message Authentication, Reporting, and Conformance
検証方法	SPFとDKIMの検証結果を使って検証。**SPF＋DMARCなど、片方だけでも可**
検証対象	**メールソフトで表示されるほうのメールアドレス**で検証
導入	すでにSPFまたはDKIMが設定されていれば、送信側の設定はDMARCレコードをDNSへ登録するだけで**容易**。
利点	**SPF のみでは正規メールとして誤判定される なりすまし送信を検出できる**
	ドメイン管理者側が、検証失敗したメールの扱いを指定できる none: モニタリングのみ (何も効果なし)、quarantine: 隔離 (迷惑メールフォルダーへ配信)、reject: 拒否
	迷惑メールフィルターも送信ドメイン認証結果を利用するため、組み合わせることで、より効果が高くなる
	受信側から送られるDMARCレポートで、検証結果を確認できる。 正規メールの検証成功数、なりすまし送信の検知、配信規模の把握など。
	国内でユーザー数が多い大手のメールサービスや大手企業は対応しており、特に**モバイルユーザーのカバー率はこの１年で上がっている**
欠点	国内 ISP のメールサービスでは対応が遅れている

SPFだけでは検出できない なりすまし送信メールが検出できるようになる

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

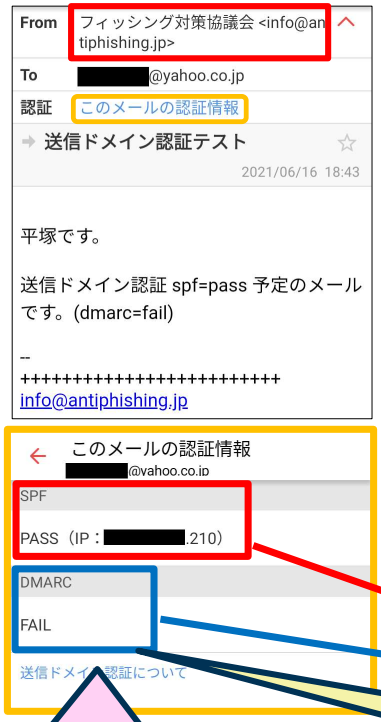
正規メール



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）

- Yahoo!メールブランドアイコン
  https://announcemail.yahoo.co.jp/brandicon_corp/
- 迷惑メール、なりすまし、フィッシングを Gmail 認証で防止する
  https://cloud.google.com/blog/ja/products/identity-security/bringing-bimi-to-gmail-in-google-workspace
- Apple メールの BIMI サポートについて
  https://support.apple.com/ja-jp/HT213155

ユーザビリティーを大きく向上！

正規メールの視認性向上のため、Yahoo! メール はブランドアイコン、Gmail と Apple iCloudメールは BIMI を使いブランドロゴ表示に対応している。

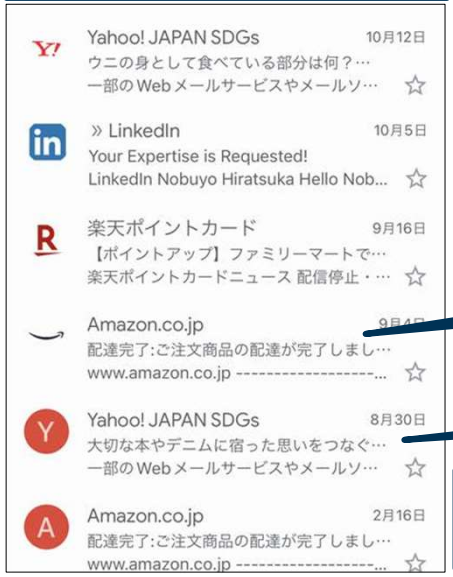
ユーザーには、**正規メールがひとめでわかる効果**がある

また、なりすまし対策を行っている**安全なメールサービス、安全なブランド**をユーザーに認識してもらえる

Yahoo！メール
ブランドアイコン

SPFまたはDKIMの検証をPassした
本物のメールにアイコン表示

Gmail で表示した BIMI



BIMI 対応後は**本物のメールにロゴ表示**

BIMI対応前はロゴ表示なし

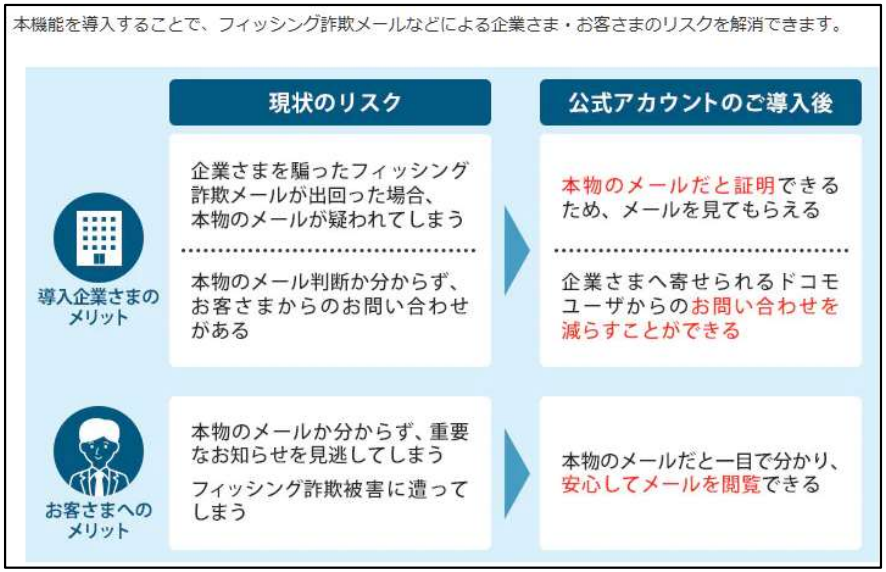
BIMI (Brand Indicators for Message Identification)
DMARC検証をpassした正規メールにブランドロゴを表示する技術

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

併せて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

フィッシングメールに対するDMARCの効果

- あるメールアドレス着フィッシングメールを2021年の1年分調査

なりすましメールと dmarc=fail 数												
	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	199	182	198	264	359	221	272	423	389	363	363	442
なりすましメール	100	64	124	202	291	148	186	308	244	267	238	272
なりすまし率	50.3%	35.2%	62.6%	**76.5%**	**81.1%**	67.0%	68.4%	**72.8%**	62.7%	**73.6%**	65.6%	61.5%
dmarc=fail	39	27	82	159	223	87	98	74	132	217	200	223
dmarcでの検知率	39.0%	42.2%	66.1%	**78.7%**	**76.6%**	58.8%	52.7%	24.0%	54.1%	**81.3%**	**84.0%**	**82.0%**

なりすましメールの 80% 以上が DMARC で検出可能

- 2020年からフィッシングメールの半数以上がなりすましメール。
  なりすまし送信被害ブランドが DMARC 対応すると、検知率が上がる
- DMARC p=reject 対応したブランドを避け、DMARC 対応を行っていないブランドが次々と狙われる
- 現在は **p=none のまま運用中のブランドが集中的に狙われ続ける傾向がある**
  迷惑メールフィルターを素通りし、フィッシングメール到達率、成功率が高いからと思われる

現在もフィッシングメールの半数以上がなりすましメール
DMARC ポリシー p=quarantine/reject で運用することで排除できる
しかし、DMARC p=none では効果がないため、狙われ続ける

2022年報告からみる
効果的なフィッシング対策
まとめ

フィッシング対策 (フィッシングサイト対応)

- **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
- **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
- **情報収集: フィッシング報告受付窓口設置**
  - 一般からのフィッシングメールの報告が、一番早い検知となることは多い
  - メールで報告できる窓口を作る
    情報収集目的と明記し、返信しない。大量報告の場合、返信は逆に報告者にとって迷惑となる
    返信が必要な場合は、従来通りのサポート窓口へ問い合わせるよう案内する

フィッシング対策協議会ホームページにも記載することで、より情報が集まる

フィッシング報告受付メールアドレス
info@antiphishing.jp

以下のフィッシングの報告は、事業者へも直接、ご報告ください。

Amazon	stop-spoofing@amazon.com
メルカリ	phish@mercari.com

- **検知サービス**
  - 組織内に専門の人員や設備がなくても、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
  - 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

2022年3月、フィッシング対策協議会に報告された (実際にフィッシングサイトへの誘導が行われた) URL と、検知サービスで検知した URL とのデータ突合を実施。
検知率良は良好だった。

検知率 (2022年3月分)	
カードブランドA	80.10%
カードブランドB	97.10%
カードブランドC	88.80%
カードブランドD	78.80%
ECブランドA	90.60%

フィッシング対策（メール関連）

- **被害ブランドへの推奨事項**
  - DMARC 未対応の場合は、テスト運用開始（p=none モニタリングモード）
  - DMARC レポートの定常監視、異常時のフィッシングメール配信検知と規模の把握
  - DMARC 正式運用を開始する（p=quarantine または reject へ変更）
  - 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
    （フィッシングメールの見破り方を説明しても効果は期待できない）

重要！ p=none では効果なし！

- **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、認証情報の確認など、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

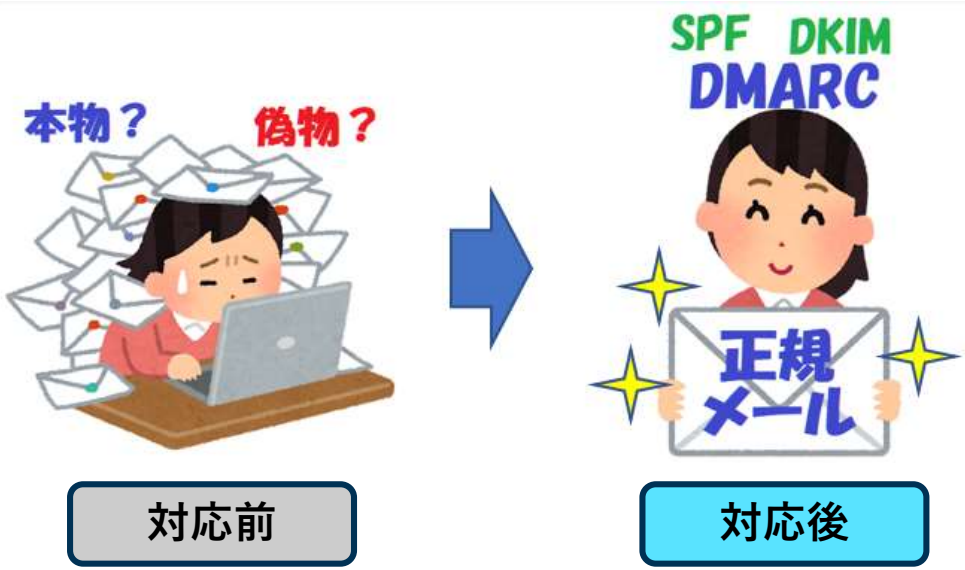
DMARC ポリシーに従い、なりすましメールを隔離、拒否する主なメールサービス
- **Gmail（BIMI に対応）**
- **iCloud.com（BIMI に対応）**
- **Yahoo! メール（ブランドアイコン）**
- **ドコモ（ドコモ公式アカウント）**
- **NIFTY**
- **楽メール**

日本国内では利用者が多く、カバー率が高いため十分に効果が見込まれる

DMARC 正式運用前のオンラインサービス事業者は、これらのメールアドレスを使っている利用者数を確認すると、期待できる効果の測定を行うことができる

フィッシング対策（メール関連）

DMARC は p=reject がゴールです



なりすまし送信メール対策について
https://www.antiphishing.jp/enterprise/domain_authentication.html

フィッシング対策 まとめ

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

システム部門と連携し、平常時のログや DMARC レポートの分析を行っておき、異常の発見や、フィッシング対応の効果測定を行う

フィッシングサイトへの対応（発見、URLフィルター登録、テイクダウンなど）は、早期に行うほど効果が高い。自社内で対応が難しければ、検知サービスを利用することも検討する

URLフィルターやテイクダウンは、被害抑制に効果が出にくい状況もあるため、一定の効果がある正規メールの視認性向上を検討する

フィッシング手法は日々進化しているため、他ブランドのフィッシング事例を収集し、自ブランドでの対応方法を検討しておく

一度フィッシングの標的になると、なりすましメール対策を行わない限り、狙われ続けることを認識する（DMARC p=reject にするとフィッシングメールが届かなくなるので減る）

以上、ご参考になりましたら幸いです

参考資料
（今回、説明できなかった資料）

DMARC レポートによる正規メール配信状況の確認

- DMARCレポートの例
  フィッシング対策協議会 (@antiphishing.jp) が差出人になっているメールの判定例

[ ]がフィッシング対策協議会の正規サーバから Gmail へ直配送されたメール
それ以外は別のメールアドレスに配送したものがGmailに転送されたもの

送信元サーバのIPアドレス

転送によりSPF判定はfail でも、DKIM判定でpassで検証可能

全て正規メールなので、DMARC判定もpass

org_name	domain	source_ip	count	dkim	spf	header_from	selector	result
google.com	antiphishing.jp	202.*.*.*	1	pass	fail	antiphishing.jp	apcdkim01	pass
google.com	antiphishing.jp	101.*.*.*	1	pass	fail	antiphishing.jp	apcdkim01	pass
google.com	antiphishing.jp	210.●.●.●	15	pass	pass	antiphishing.jp	apcdkim01	pass
google.com	antiphishing.jp	218.*.*.*	2	pass	fail	antiphishing.jp	apcdkim01	pass
google.com	antiphishing.jp	2001:*:*:*::*	2	pass	fail	antiphishing.jp	apcdkim01	pass
google.com	antiphishing.jp	202.*.*.*	1	pass	fail	antiphishing.jp	apcdkim01	pass
google.com	antiphishing.jp	175.*.*.*	1	pass	fail	antiphishing.jp	apcdkim01	pass
google.com	antiphishing.jp	202.*.*.*	1	pass	fail	antiphishing.jp	apcdkim01	pass

spf が fail しているのは、どこかへ配送したメールが Gmail のアカウントへ転送されているため

DMARC レポートは xml 形式で1日1回くらいの頻度で届く。
Excel で開くと、上記のように表で見られるが、定常的な監視には向かない。
配信の異常を検知するには、DMARCレポート分析ツールを使うことを検討する

DMARCレポートの活用

- **フィッシング対策協議会をかたるフィッシング (2022/05/06)**
  https://www.antiphishing.jp/news/alert/apc_20220506.html

～ フィッシングとは実在する組織を騙って、ユーザネーム、パスワード、アカウントID、ATMの暗証番号、クレジットカード番号といった個人情報を詐取する行為です ～
フィッシング対策協議会 Council of Anti-Phishing Japan
ネットショッピング認証サー(3-D Secure)とは何ですか？
インターネットショッピングをご利用の際、悪用防止のために、パスワードによるカード利用者のご本人確認を行い、より安全なお取り引きを提供するサービスです。
Visaでは「Visa Secure」、Mastercardでは「Mastercard® SecureCode™（マスターカード・セキュアコード）」の名称でサービスを提供しています。不正利用防止の観点からご導入をおすすめしております。

「Visa Secure」/「Mastercard® SecureCode™（マスターカード・セキュアコード）」の使い方を教えてください。
今回は、フィッシング対策協議会を通じて日本の大手銀行と提携し、お客様が持っているすべてのVISA/Mastercardクレジットカードを簡単に登録することができます。メールの下の専用リンクをクリックして登録すればいいです。複数のカードを登録したいユーザーは、カードごとに1回設定してください。

このサービスにログインしたら、私に何のメリットがありますか?
不正利用の抑止:第三者によるカードの不正利用を抑止します。
信頼性のアップ:お客さまにより安心してご利用いただけるため、貴店サイトの信頼性が向上し、利用促進につながります。

債権買戻しリスクの軽減:お客さまが利用否認しても、貴店にご負担していただく必要がなくなります。

登録「Visa Secure」/「Mastercard® SecureCode™（マスターカード・セキュアコード）」サービスの専用リンク:
「Visa Secure」
https://www.antiphishing.jp/visa-service
リンク１
<http://antiphishing-jp.●●●●/update/upvisa.php> など
「Mastercard® SecureCode™（マスターカード・セキュアコード）」
https://www.antiphishing.jp/ms-service
リンク２
<http://antiphishing-jp.●●●●/update/upmatser.php> など

発行者
名称
フィッシング対策協議会 / Council of Anti-Phishing Japan
事務局
一般社団法人 JPCERTコーディネーションセンター (事務局長：村上憲二)
〒103-0023 東京都中央区日本橋本町 4-4-2 東山ビルディング 8 階
TEL: 03-6271-8905
FAX: 03-6271-8908

メール文面の例

メール文面やサイトの作りが雑であり、嫌がらせが目的の可能性が高いと判断

DMARCレポートの活用

DMARCレポートによるフィッシングメール送信元の検知

- メール配信は 2022年 5月 4日の 2:55am 頃～4:00am 頃。協議会への報告数は 7 件のみ
- 差出人は ****@antiphishing.jp というメールアドレス（なりすまし）
- DMARCレポートを Yahoo.com、Google、Outlook.com、NIFTY 等から受領
- 全2,453 通分のレポートを受領し、うち216 通についてはフィッシングメールの転送と判断（5月4日は祝日なので、正規メールは送られていない）
- 特定の IP アドレスから数十通～数百通単位のなりすまし送信を検知
  報告されたフィッシングメールの送信元 IPアドレスとも一致

source_ip	Reverse_DNS	whois	count	Report_from
[redacted].78.43	[redacted]	[redacted]	39	Yahoo.com, Google, NIFTY
[redacted]52.90			256	Outlook
[redacted]231.116			989	Yahoo.com, Google, NIFTY など
[redacted]118.139			953	Yahoo.com, Google, NIFTY など
合計			2,237	

DMARCレポートにより、なりすまし送信の検知、
送信元事業者の特定、配信規模の把握ができる

DMARCレポートの活用

- DMARCレポート(xml)を Excel で開いて編集して集計するとこのような感じ

送信元	送信数	DMARC 的検証結果		見えないメアド	見えるメアド	SPF検証に使ったドメイン	SPF判定結果
source_ip	count	dkim	spf	envelope_from	header_from	spf_domain	spf_result
[redacted]91.2	1	fail	fail	[redacted]	antiphishing.jp	[redacted]	pass
[redacted]17.6	1	fail	fail	[redacted]	antiphishing.jp	[redacted]	pass
[redacted]1.116	2	fail	fail	[redacted]	antiphishing.jp	[redacted]o	pass
[redacted]90	101	fail	fail	[redacted]p	antiphishing.jp	[redacted].jp	pass
[redacted]4.182	1	fail	fail	[redacted]	antiphishing.jp	[redacted]o	softfail
[redacted]8.139	61	fail	fail	[redacted]	antiphishing.jp	[redacted]o	pass
[redacted]1.116	13	fail	fail	[redacted]	antiphishing.jp	[redacted]o	pass
[redacted]1.116	1	fail	fail	[redacted]	antiphishing.jp	[redacted]o	temperror
[redacted]90	1	fail	fail	[redacted]p	antiphishing.jp	[redacted].jp	pass
[redacted]8.139	390	fail	fail	[redacted]	antiphishing.jp	[redacted]o	pass
[redacted]90	81	fail	fail	[redacted]p	antiphishing.jp	[redacted].jp	pass
[redacted]1.116	431	fail	fail	[redacted]	antiphishing.jp	[redacted]o	pass
[redacted]90	27	fail	fail	[redacted]p	antiphishing.jp	[redacted].jp	pass

今回のケースでは通数が少なく envelope-from が国内ISPなどの場合は転送と判断

envelope-from は SPF 単体での検証を pass するドメインを使って送信設定

大量にメールを送っている IP アドレスを中心に調査

DMARCは header-from のドメイン (antiphishing.jp) で検証するので SPF fail する DKIM 署名もついてないので fail する

結果、送信数が多かったのが前ページの 4 IPアドレス

毎日こういう手作業は大変なので、DMARC レポート分析ツールをお使いになることをお勧めします。

DMARCレポートの活用

■ 大量配信の検知、規模の把握

集計日時範囲	Count数	合計
2022-05-28T09:00:00+09:00	55574860	122,436,773
2022-05-27T09:00:00+09:00	41124956	
2022-05-14T09:00:00+09:00	14170438	
2022-05-24T09:00:00+09:00	4918972	
2022-05-25T09:00:00+09:00	2882092	
2022-05-30T09:00:00+09:00	1369633	
2022-05-23T09:00:00+09:00	1124614	

Begin Time	Count	Source IP	Reverse Lookup Name
2022-05-28	62385	58.171	.jp
2022-05-28	62775	77.116	.jp
2022-05-28	64418	77.61	.jp
2022-05-28	64992	72.224	.jp
2022-05-28	68182	70.153	.jp
2022-05-28	72607	51.236	.jp
2022-05-28	75896	36.106	.jp
2022-05-28	76667	44.183	.jp
中略			
2022-05-28	413393	35.178	.jp
2022-05-28	415079	36.243	.jp
2022-05-28	417882	9.155	.jp
2022-05-28	418318	1.170	.jp
2022-05-28	423519	73.22	.jp
2022-05-28	424124	50.219	.jp
2022-05-28	425535	64.45	.jp
2022-05-28	426400	47.21	.jp
2022-05-28	428396	32.59	.jp
2022-05-28	429021	42.105	.jp
2022-05-28	432560	38.111	.jp

- 2022年5月になりすまし送信被害にあった
  ブランドへDMARCレポートによる情報提供を依頼
- 結果、特定の国内ホスティング事業者から

5 月だけで約1億2,243万通以上の
なりすましメールが発信されていることを確認

- 1日多い日で5,000万通以上、メール送信
- 649 台のサーバーを使い、1 台当たり数万通 ～ 約 43 万通の配信を行っていた

DMARC ポリシーを p=reject にすると、この「1 億通以上の不正メールから受信者を守る」ことができる

しかし、DMARC p=none では不正メールは素通し、受信者へ届いてしまうので効果がない

DMARC の段階的導入

- **DMARC ポリシー宣言**
  DMARCレポートを取得して状況を把握するため、モニタリングモードで始める。
  - **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 、Outlook など）
  - 実際にレポートを受け取り、**正規メールが正常に配送されていることを確認**する
  - 管理できていない**「未承認」「野良」メールサーバーがいないか、確認**する
- **ポリシー変更**
  - **レポートを確認しながら、問題点を解決する**
  - **正規メールが配信できていることを確認できたら、p=reject または quarantine に変更し、正式運用を開始する。**
    (pct パラメータで適用割合を指定できる)
- **【推奨】メールを送信しないドメインへのポリシー宣言**
  - ポリシーを宣言してい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

BIMI 対応手順

- 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
- Google: Add a brand logo to your email with BIMI
  https://support.google.com/a/topic/10911234?hl=ja&ref_topic=9061731

BIMI 対応手順の例	
1. DMARC 対応 (p=quarantine or reject)	BIMI では DMARC 設定は以下の制限があるため、メール環境を整備していく ➢ **DMARC ポリシーは p=reject または p=quarantine pct=100** ➢ サブドメインのポリシーで sp=none は指定不可
2. ロゴ準備	BIMIではロゴは複数切り替えて指定可能なため、必要なロゴを準備 ➢ **正方形や円に表示されても視認可能なロゴか確認** ➢ **ロゴの商標登録** ➢ SVG 形式ロゴファイル作成 ➢ HTTPS ウェブサーバー上にロゴファイルを配置
3. VMC 取得	Verified Mark Certificate の略。日本語では「認証マーク証明書」 BIMI 仕様上は必須ではないが、Gmail でロゴ表示するには VMC が必要 ➢ 取得には商標登録されたロゴが必要 ➢ ロゴごとに VMC が必要。(1ドメインで複数ロゴ申請、利用可能) ➢ HTTPS ウェブサーバー上に VMC ファイルを配置
4. BIMI 対応開始	➢ BIMI レコードを DNS に登録、公開 ➢ 1ドメインで複数のロゴを BIMI-selecor で切り替えることも可能 ➢ チェックサイトで確認 BIMI Group : BIMI Lookup & Generator https://bimigroup.org/bimi-generator/

DNSからわかるドメインセキュリティ対策状況

- ドメイン名に対するセキュリティ対策状況
  - 統計情報
    https://dnsops.jp/stats/
    - 日本の政府関連ドメイン名のDNSSECステータス
    - 日本の地方公共団体関連ドメイン名のDNSSECステータス
    - 日本の高等教育機関のドメイン名のDNSSECステータス
    - 日本の金融機関のドメイン名のDNSSECステータス
    - TOPIX銘柄企業ドメイン名のDNSSECステータス

    上記のDNSSECだけでなく、SPF、DKIM、DMARC 等への対応状況もわかる
  - どのような情報が外部から判別可能か、把握することは重要
  - **DNSは公開情報。隠すことはできない**
    なりすましメール対策を行っていないことは、外部から丸見えとなっていることを認識する