

2022年3月24日

第36回サイバーセキュリティタスクフォース
掲載用資料

フィッシングの現状（2021年版）

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
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 105 組織**（2022 年 2 月時点）
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
（経済産業省の委託事業として行っている）

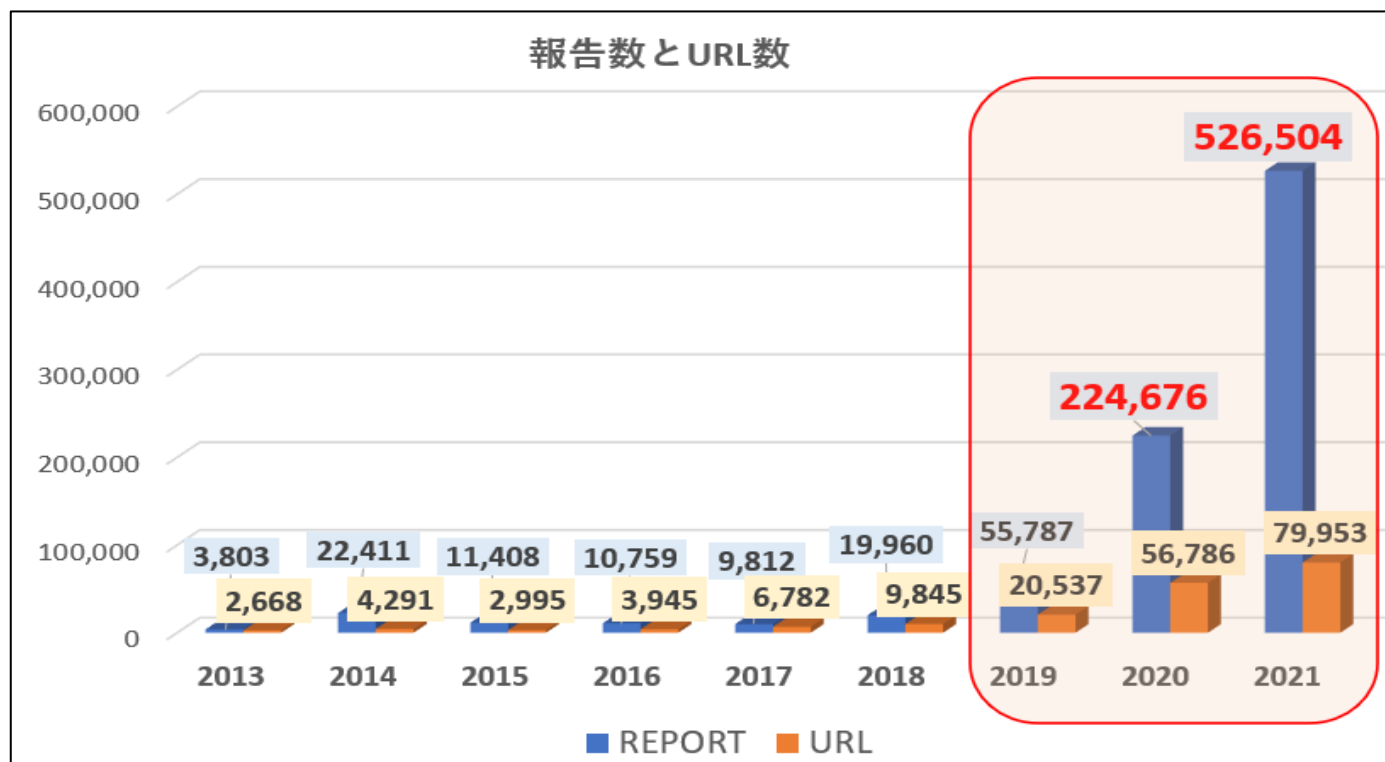


URLフィルタリングを行っている
セキュリティベンダー、事業者へURL共有

フィッシング報告数の推移（年別）★

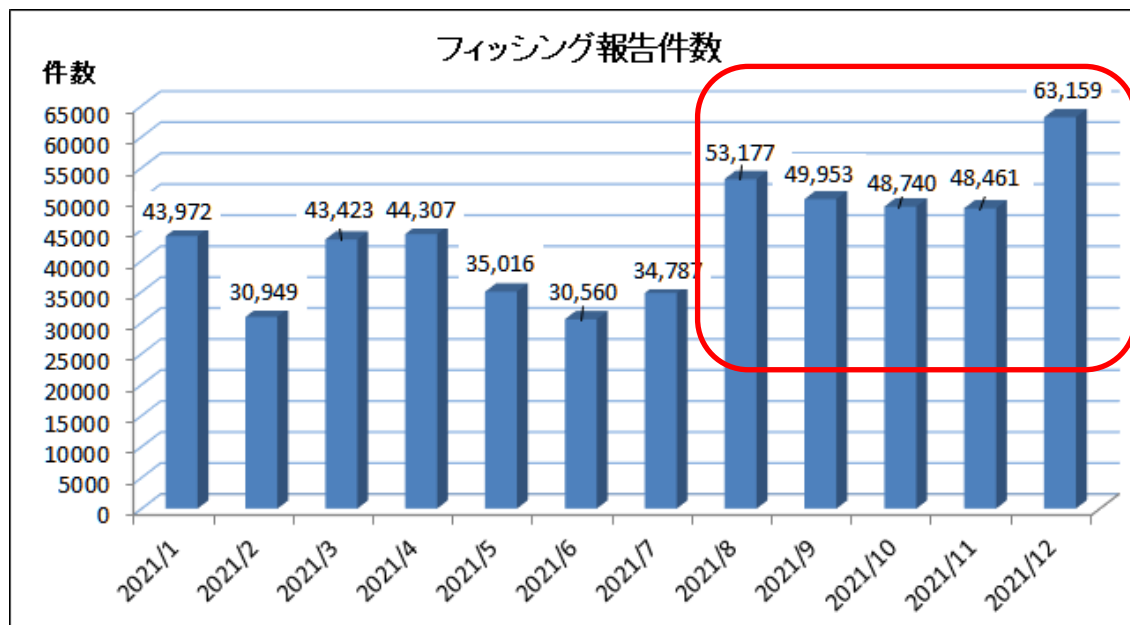
■ 2020年以降、報告が激増

- 報告数は、2年前の2019年と比較して約9.4倍。
この2年で消費者、事業者にとって非常に大きな問題となってきた。
- URL件数は2019年と比較して約3.9倍。
- 百万通単位のフィッシングメール配信が繰り返し行われている



フィッシング報告内容の推移（2021年後半）★

- 2021年後半、フィッシングは「社会問題」と言われるようになる



- 新規ブランド、業種をかたるフィッシングが次々と現れる
日本年金機構（ねんきんネット）、厚生労働省（コロナワクチンナビ）、ホスティング事業者、水道局、生命保険会社、キャッシュレス決済サービスなど
- 2021年末は、フィッシングで入手した携帯電話番号を使って、別サービスへのログイン試行と思われる認証コード通知 SMS の報告が増え始める。
- キャッシュレス決済（●●Pay、キャリア決済）の不正利用を狙うフィッシングが増える
携帯電話番号もクレジットカード番号や口座番号のように決済に結び付く情報となってきた

フィッシングは詐欺なので、手法はいくつもある
対応方法が異なるが、**基本的には誘導元（メール、SMS）への対策がやはり効果的**

メールによるフィッシングへの誘導 ★

■ 同じ文面でブランドだけ変えている例

Mastercard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上げます。
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
<<https://mastercard.co.jp.●●●●.bar/>> 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上げます。

■発行者■
Mastercard
〒150-8512
東京都渋谷区桜丘町26-1 セルリアンタワー16階
TEL: 00531-11-3886 (フリーダイヤル)

メール文面の例

Mastercard をかたるフィッシング (2021/11/18)
https://www.antiphishing.jp/news/alert/mastercard_20211118.html

このタイプは配信量が非常に多く、報告が多い
(多いときは1人数通/日 x 連日、1週間で数十通など)
本物と同じドメインを使ったなりすまし送信率が高い

2020年頃から使われ続けている。

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
- 楽天カード
- VJA
- りそなVISAカード
- ライフカード
- VISA
- Mastercard など (順不同)

なりすまし送信メールの例（番外編マルウェア）★

■ 厚生労働省のドメイン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

厚生労働省 <hjhvs@mhlw.go.jp>

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。

変種のおミクロン株が
発見された、と時事ネタを
入れて誘導

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。

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

<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。

なりすまし送信対策をしていたら

- ・被害を抑えられたのに…
 - ・受信者を守れたのに…
 - ・ブランドイメージ、信用を守れたのに…
- ということが無いよう、備えることが重要

【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 [REDACTED]（代表）

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

なりすまし送信とは ★

- 「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

差出人 株式会社ジェーシービー <info@jcb.co.jp> ☆

件名 【JCBカード】重要なお知らせ

差出人「楽天市場」 <noreply@rakuten.co.jp> ☆

件名 【楽天市場】あなたのアカウントを確認

差出人 エムアイカード <info@micard.co.jp> ☆

件名 【重要】エムアイカードの利用確認

差出人 Amazon.co.jp <account-update@amazon.co.jp> ☆

件名 Amazonプライム会費のお支払い方法に問題があります

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

■ 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	
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
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 hardfail も素通し)
欠点	独自ドメインを使い、SPFを回避するなりすまし送信は検出できない

DKIM	
検証方法	電子署名でメールを検証。S/MIMEはメール本文に対し署名するが、DKIMは主に配信時につけられるヘッダー情報に対し署名する。
検証対象	署名対象の情報 (差出人、日付時刻、受信者など、主にヘッダー中の情報)
導入	送信側は各メールへ署名するためのシステムは必要で、導入コストはかかる
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を補い、有用な機能を実現

DMARC	
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	容易。送信側の設定はDMARCレコードをDNSへ登録するだけ
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 (迷惑メールフォルダーへ配信、拒否等のポリシーを宣言) 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、規模の把握など。
欠点	大手のメールサービスは対応しているが、日本国内の事業者やISP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**

2021年 なりすまし送信メールの増加 ★



- フィッシングメールは増加の一途
 - 2020年6月頃から、本物と同じメールアドレス（ドメイン）を使って送信するなりすまし送信メールが急増
- 多くの利用者が困惑したり、本物と信じて情報を入力
特にスマートフォンユーザーが見分けるのは、ほぼ不可能

	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%

- 送信ドメイン認証 **DMARC** を使えば、フィッシングメールの**半数以上** が偽物として判定可能。
- DMARCの判定結果をもとに迷惑メールフィルターで排除することが可能なため、**利用者に届かなくなる（＝被害抑制効果）**

受信側DMARC検証の効果



■ 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 推移												
	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
dmarc=fail数	39	27	82	159	223	87	98	74	132	217	200	223
なりすまし%	50.3%	35.2%	62.6%	76.5%	81.1%	67.0%	68.4%	72.8%	62.7%	73.6%	65.6%	61.5%
全体dmarc=fail%	19.6%	14.8%	41.4%	60.2%	62.1%	39.4%	36.0%	17.5%	33.9%	59.8%	55.1%	50.5%
fail/なりすまし%	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%	全メール中、なりすましメールが占める割合											
全体dmarc=fail%	全メール中、dmarc=fail でなりすまし検出できた割合											
fail/なりすまし%	なりすましメール中、dmarc=fail で検出できた割合											
	低い → DMARC未対応ブランドが狙われた または エラーで検証できなかった割合が多い											
	高い → DMARC対応ブランドが多く狙われたが、dmarc=failで検出できた割合が多い											

なりすましメール
DMARCで
80%以上検出

- 1月2月、dmarc=failでの検出率は約20%以下。
大手ECブランドドメインのSPFレコード記述ミスによる検証失敗が主な原因
- 3月、大手ECブランドドメインのSPFレコードが修正され、DMARCでの検出率が上がる
- 4月5月、全体の80%前後がなりすましメールだったが、被害ブランド側がDMARC対応し、報告メール全体の60%以上が検出可能。DMARCが効果的に機能し始めた
- 6月7月、全体の配信量、なりすまし送信率が減少し、DMARCでの検出率も下がる
- 8月、DMARC非対応ブランドを狙ったなりすまし送信が急増、DMARCでの検出率が下がる
- 10月-12月、DMARC対応ブランドが増え、報告メール全体の50%以上が検出可能。
なりすましメールは80%以上検出可能。

DMARCレポート活用事例：なりすまし送信検知 ★

■ なりすまし送信の検知

送信元IPアドレス合計		
1	.176	177,127
2	12	149,892
3	170	127,237
4	3.231	125,035
5	2.236	120,789
6	140	120,212
7	2.250	118,259
8	15	115,682
9	237	115,060
10	37	110,487
11	230	110,294
12	.136	108,867
13	229	107,341
14	0.106	101,094
15	185	100,346
16	3.230	98,430
中略		
284	3.44	14,168
285	2.169	13,825
286	253	11,636
287	6.73	7,670
288	.22	7,475
総計		14,251,993

- 被害ブランドに相談し、2021年11月のDMARCレポートの dmarc=fail の検出数を共有いただいた結果…

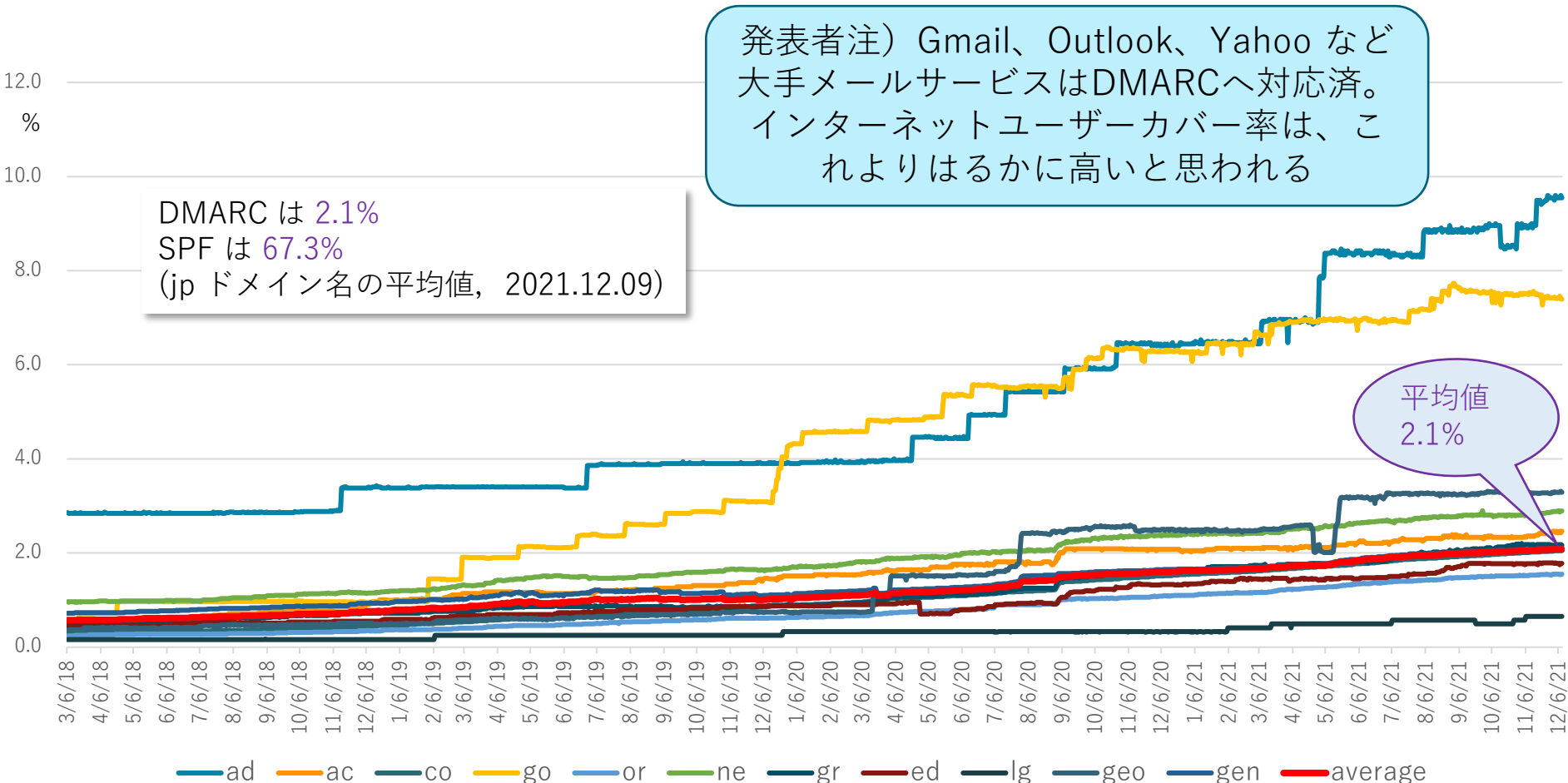
約**1,425万通以上**/月の
なりすましメールが
発信されていることを確認

10万通以上送信しているサーバー: 15台
1万通以上送信しているサーバー: 286台

- 今後の通信事業者との要調整事項
Abuse のエビデンスとしてメールヘッダーではなくDMARCレポート集計結果を使いたい

送信ドメイン認証技術の普及状況

JP ドメイン名の DMARC 宣言率推移 (IAJapan & JPRS との共同研究)



SecurityDay (<https://www.securityday.jp/>)

フィッシング対策技術の適切な導入

(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

正規メールをもっと視認しやすく ★

- Yahoo!メールブランドアイコン
https://announcemail.yahoo.co.jp/brandicon_corp/
- 楽天：楽天サービスに対する不正対策
<https://corp.rakuten.co.jp/security/anti-fraud/>

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



Yahoo および Gmailユーザーは多
いため、効果が期待できる。

また、より安全なメールサービス
がある、とユーザーにも認識して
もらいやすい

ユーザーには、なりすまし対策を
行っている**事業者の本物メー
ル**が一目でわかる効果もある

**ユーザビリティを
大きく向上！**

BIMI 対応後は
本物のメールに
アイコン表示

BIMI対応前は
ブランドアイコン
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アイコンを表示する技術

フィッシング問題への取り組み ★

■ 被害ブランドにおける対策

- なりすましメール対策技術 (DMARC) への対応、ポリシーの強化
- ブランドアイコンやBIMI 等、正規メールの視認性向上
- 利用者への注意喚起、被害者へメールアドレス変更推奨

■ URLフィルタリング

- 各事業者（検知サービス）でのモニタリングによる、URLフィルターへの早期自動登録

■ フィッシングサイトのテイクダウン

- 各事業者自身（サービス利用）による早期テイクダウン依頼実施

■ 利用者側における入口対策（フィッシングメール対策）

- 迷惑メールフィルターの利用を推奨
- 安全なメールシステム、対策を行っているサービスの選択、変更

■ 通信事業者における対策

- なりすましメール対策技術 (DMARC) への受信側検証対応
- メールアカウント不正利用による踏み台送信への対応
- ホスティングサービスの不正契約への対応
 - フィッシングメールを大量配信している契約についてAbuse対応

DMARC普及啓発活動で伝えていること ★



■ 誤解、似たようなものとの違い

- 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、DMARCは署名がついていないメールの判定にも有効です

■ 対策方法についての情報提供

- なりすまし対策技術があることを知らない
→ ユーザーに見分けるのは不可能。結果、本物メールも信用しなくなっている。
→ 偽メールは迷惑メールフォルダーへ配信させることができる。
- 情報を収集できておらず、状況を把握できていない
→ DMARCのモニタリングモードでまず現状把握を（配信には影響ありません）

■ 普及率よりカバー率、安全なものを選ぶ権利

- ユーザーが多いメールサービスはDMARC対応済なので、導入効果はでる
- 主要なクラウドメールサービスやセキュリティGW製品は、DMARC 検証対応済であり、不正メール検出の手段の一つとして、すでに使われ始めている
- ユーザーにも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）



技術でできることは技術で対処し、犯罪者側の
コストを上げ、成功率を下げる

他の先進国では普及、標準化しているDMARCの導入を促し、
対応すべきEメールセキュリティの標準とする

ブランドアイコン表示など、正規メールを判別しやすくする
技術は積極的に対応するようサービス提供事業者へ促す

メールが入り口となるインシデントや攻撃は多いため、
将来的には報告データを各関連組織で共有し、連携して
分析や対応を行えると望ましい