JANOG51
最新フィッシング動向とDMARC運用のポイント

JANOG50+
我々の周りで変わり始めたこと ～フィッシングの変化とその対応～

JANOG49
増え続けるフィッシング被害を乗り越えるために、我々がすべきこと

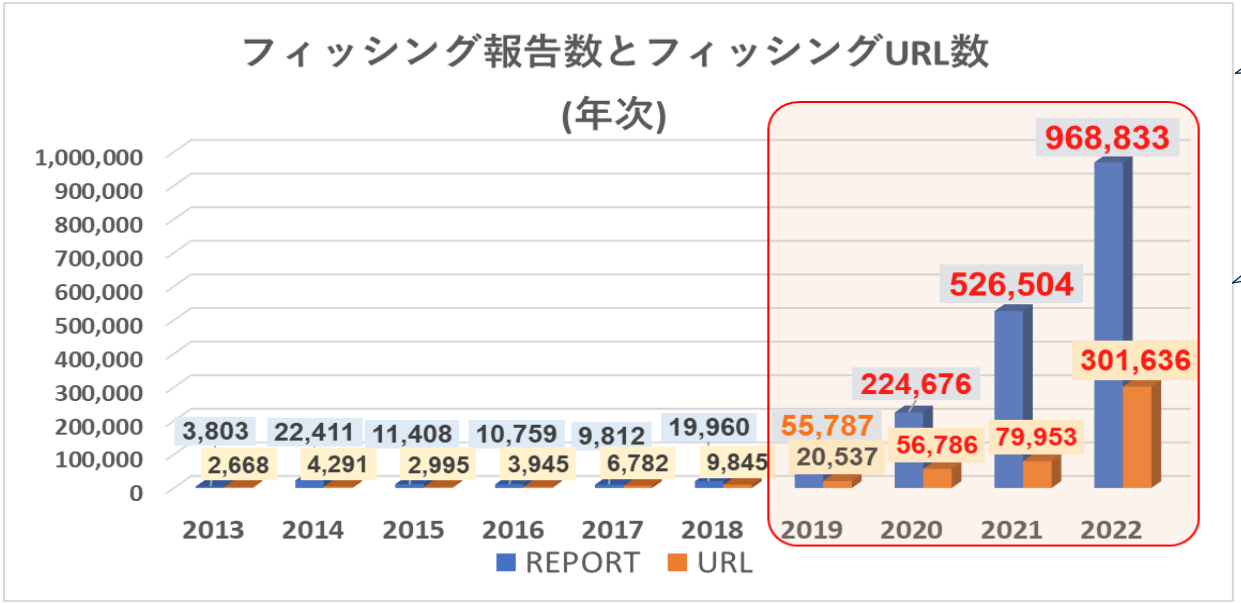
JANOG48
増え続けるフィッシング被害に今、我々ができること

最新フィッシング動向と対策
(2022年10月-2023年1月)

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

フィッシング報告件数の推移 (年別)

- ここ 3 年間で報告が急増、**2021年には「社会問題」と言われるようになる**
  - コロナ渦でオンラインサービス利用者が増えたことも要因
  - 報告数は **2020年と比較し、2年で約 4.3 倍**。
  - URL件数 (=フィッシングサイト件数) は **2020年と比較し、2年で約 5.3 倍。**
  - **各事業者、利用者ともにフィッシングメールが占めるリソースと対応コストが増加**



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

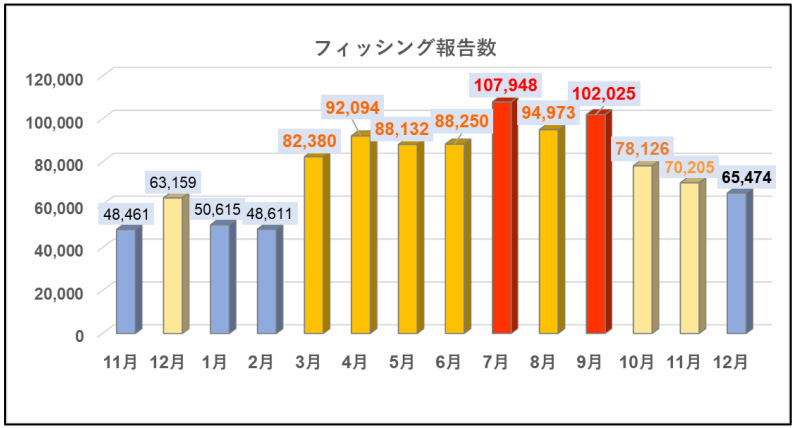
2020 年頃からホスティング事業者発のフィッシングメール配信が増える。同時になりすまし送信も増え始めた

2023 年現在、さまざまなクラウドサービスに大量の契約を持ち、配信インフラを整備して大量配信

フィッシング報告の推移 (2022年 月別)

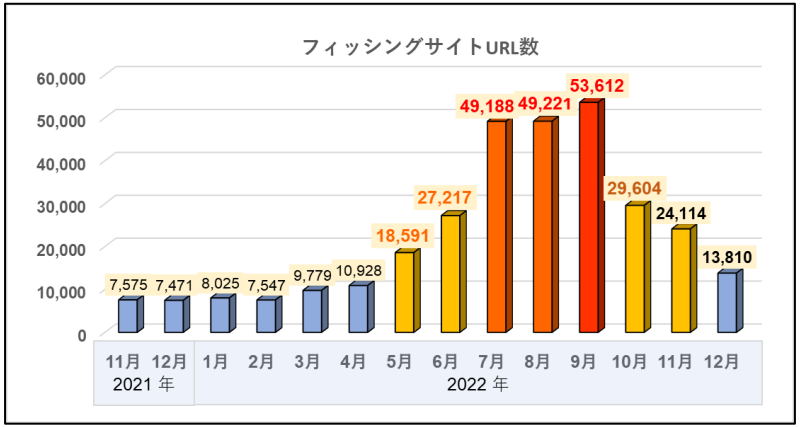
フィッシング報告件数の傾向

- **2022年3月以降、急増し、7月には 10 万件突破**
- **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、**配信範囲は日々、広がっている**
- **受信側 DMARC 対応が進み、2022年11月時点では、利用者の約 7 割がカバーされている（ある大手ECサービス）**
- **残り約 3 割は、DMARC 非対応の国内 ISP/モバイル事業者からのフィッシング報告が多い**



フィッシングサイト (URL) 件数の傾向

- **2022年5月以降、大量のドメイン、サブドメインを組みあわせて、大量にURLを生成するタイプが急増し、全体の7-8割以上を占めていた**
- **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くなる**
- **早期URL検知とURLフィルターへの早期登録など、各方面の尽力により、大量生成系は10月以降、収束に向かった。**
- **短縮URL、Google翻訳など、クロ判定しづらいURLからの誘導が増えた**
- **スマートフォン狙いのものや、テイクダウンされづらい仕組みが実装されているものも増えている**



最近の事例：QRコードで誘導

ETC 総合情報ポータルサイト

ETCサービスをご利用のお客様へ：

インフォメーションMAIL

平素よりＥＴＣ利用照会サービスをご利用いただき、誠にありがとうございます

今日、ETCに支払情報が変更されたことが発見しました

本人操作確認するため為、一時使用制限をしております

お早めに当社までご連絡くださいませ、ご容赦のほど宜しくお願い致します。お忙しい中お邪魔して申し訳ませんでした

本人認証の手続きが完了してから、ＥＴＣサービス制限が解除。

Webページが乗っ取られないようにするためにご本人認証下記携帯電話でQRコードをスキャンする確認ください

>>>　<<<

[　　]の部分のリンク
＜https://www.etc.co-●●●●.●●●●.com.cn/＞など

弊社は、インターネット上の不正行為の防止･抑制の観点からサイトとしての信頼性･正当性を高めるため、

==========

･ご案内している内容について、お持ちのカードによっては一部利用できない場合があります。

＊こちらのメールは送信専用メールアドレスから配信されております。

==========

こちらのメールに返信いただいても、返答できませんのでご了承ください。

【配信元】

発行者ETC利用照会サービス事務局East Nippon Expressway Company Limited,Metropolitan Expressway Company Limited

メール文面の例

フィッシング対策協議会
ETC 利用照会サービスをかたるフィッシング (2022/11/15)
https://www.antiphishing.jp/news/alert/etcQR_20221115.html

- 2022年11月～2023年1月、継続中
  上記期間中、確認されたブランド
  - ETC利用サービス
  - Amazon
  - えきねっと
  - ソフトバンク

  2023年1月初めは、そこそこ報告がきていた

QRコード	2022年		2023年
ブランド	11月	12月	1月
Amazon			96
ETCサービス	59	96	926
えきねっと			23
ソフトバンク		13	7

- 迷惑メールフィルターを回避する目的
  とはいえ、どうやってアクセスすれば
  いいのか判らない人が多いので、効果は
  薄そう…

おまけ：
QRコードでの誘導は、
フィッシング対策協議会
で情報掲載した中では
2019/08/19 が最古でした

フィッシング対策協議会
MyEtherWallet をかたるフィッシング(2019/08/09)
https://www.antiphishing.jp/news/alert/myetherwallet_20190809.html

最近の事例：正規のキャッシュレス決済画面で送金させる

フィッシング対策協議会
OCN をかたるフィッシング (2023/01/04)
https://www.antiphishing.jp/news/alert/ocn_20230104.html

- ISP月額料金の請求を装い、ISPのアカウント情報を詐取した後、キャッシュレス決済の本物の決済画面に誘導。
- ここでキャッシュレス決済の認証情報を入力すると、不正送金されてしまう
- クレジットカードの月額請求をかたる文面で、同様にキャッシュレス決済画面に誘導するケースも続いている

メールから決済画面に誘導されたら、要注意！

メール内のリンクではなく、請求元サービスの正規サイトやアプリで請求情報を確認しましょう

フィッシング対策協議会
PayPay カードをかたるフィッシング (2023/01/04)
https://www.antiphishing.jp/news/alert/paypay_20230104.html

事例：国税庁をかたるフィッシング

- 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

事例: なりすましフィッシングメールの大量配信

【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

- 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）

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

- 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5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**

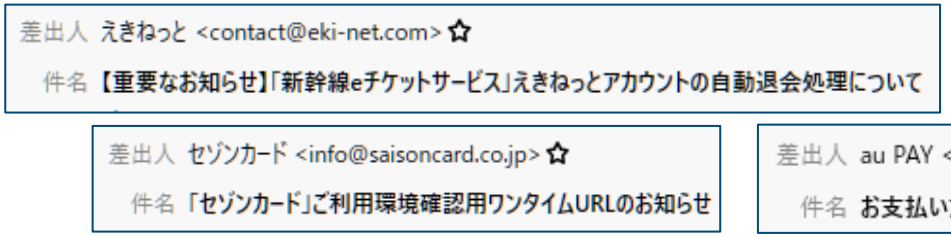
なりすまし送信とは

- 「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）
  - **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）

2022年10月ー11月に来た
フィッシングメールの例

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（送信ドメイン認証）により、メール着信率 (成功率) を下げられる**

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
	一般的には迷惑メールフィルター機能の一部として利用者へ提供し、同意を取る
	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 **特にモバイルユーザーのカバー率はこの１年で上昇！** **Gmail、Yahoo!メールに加え、ドコモ、Apple iCloud メールが対応開始** **主要なオンラインサービス利用者の半数～7 割程度をカバー**）
課題点	**国内 ISP のメールサービスでは対応が遅れている** **DMARCレポートの分析にはメールに関する専門知識が必要**

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 1 年分調査

		2022年											
		1月	2月	3月	4月	5月	6月	7月	8月	9月	10月	11月	12月
調査メール総数		391	369	631	809	510	635	608	496	367	351	466	512
なりすまし割合		43.7%	42.0%	47.9%	60.8%	37.6%	43.3%	60.2%	56.7%	60.8%	57.3%	66.1%	57.0%
独自ドメイン割合		49.9%	49.3%	43.4%	29.4%	52.9%	42.8%	29.8%	27.4%	33.5%	33.9%	30.9%	38.1%
dmarc	fail	36.3%	32.0%	33.4%	51.7%	27.3%	34.5%	45.1%	47.4%	45.2%	55.6%	51.5%	49.4%
	none	34.3%	37.4%	37.9%	32.8%	51.2%	48.0%	40.6%	41.3%	36.8%	20.8%	36.1%	37.3%
	pass	27.6%	28.7%	24.4%	10.6%	16.7%	13.5%	11.3%	7.5%	16.6%	19.1%	10.1%	11.1%
	error	1.8%	1.9%	4.3%	4.9%	4.9%	3.9%	3.0%	3.8%	1.4%	4.3%	2.4%	2.1%

フィッシングメールの約半数がなりすまし

DMARC でフィッシングメールの約半数を検出できている

- DMARC 設定率は上がり、fail するようになってきたが…
  - モニタリングモード(p=none)のドメイン（ブランド）は、なりすましで狙われ続ける
  - DMARC enforcement (p=reject/quarantine)にしたドメイン（ブランド）は攻撃が減少し、その後も狙われづらくなる （一部を除く）

DMARC で検出できているのに、フィッシングメールの着信（報告）が多い原因

- ISP のメールサービスなど、受信側の対応が必要
  - DMARC ポリシーに沿った配信（DMARC enforcement）していない ISP メールサービス利用者からのフィッシング報告が多い。（フィッシングメールを排除できていない）
  - DMARC enforcement 済のメールサービスには、そもそも届かないので報告が少ない

フィッシングメールに対するDMARCの効果

- 報告状況からみえる DMARC の効果
  - フィッシングメールの報告受領数の変化に現れる
    DMARC Enforcement 後、メール着信率が下がった？報告数が減る

1月は20日頃までの数値

		2022年									2023年
分野	Enforcement	4月	5月	6月	7月	8月	9月	10月	11月	12月	1月
EC	2021年3月	11,317	14,995	14,968	15,697	14,452	14,502	15,065	23,651	30,112	6,170
サービス	2022年9月	1,861	1,276	585	338	233	87	67	68	41	0
クレカ	2021年？月	521	2,648	3,429	4,924	7,787	4,167	782	48	19	0
クレカ	2022年10月	360	2,122	4,626	4,471	1,889	1,363	1,630	57	54	1
クレカ	2022年11月	854	2,386	1,732	778	609	837	974	1,051	157	428
クレカ	2022年12月	1,320	2,192	6,504	2,342	3,056	6,755	9,621	243	5,258	410

■ フィッシング報告種別の違い

- **フィッシングメールや SMS の転送**
  実際にフィッシングサイトへの誘導が行われたメールやSMSの報告
  どのくらいの規模で配信され、受信者に届いたのかが把握できる
- **URL のみの報告**
  パブモニや報告、探索で見つけたURLも含まれる
  誘導の規模は判らないが、誘導が行われる前のフィッシングURLなども把握できる

DMARCレポートでわかること

■ 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

■ 多い日で5,000万通/日以上、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

「1 億通以上の不正メールから受信者を守る」には？

DMARC Enforcement (p=reject/quarantine) の必要性

- **送信側: ポリシーを none から reject/quarantine へ変更**
- **受信側: 国内ISPメールサービス等で DMARC ポリシーに沿った配信を行う（迷惑メールフィルターを使ってフィルタリング）**

DMARC 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ーから 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

送信元サーバーの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

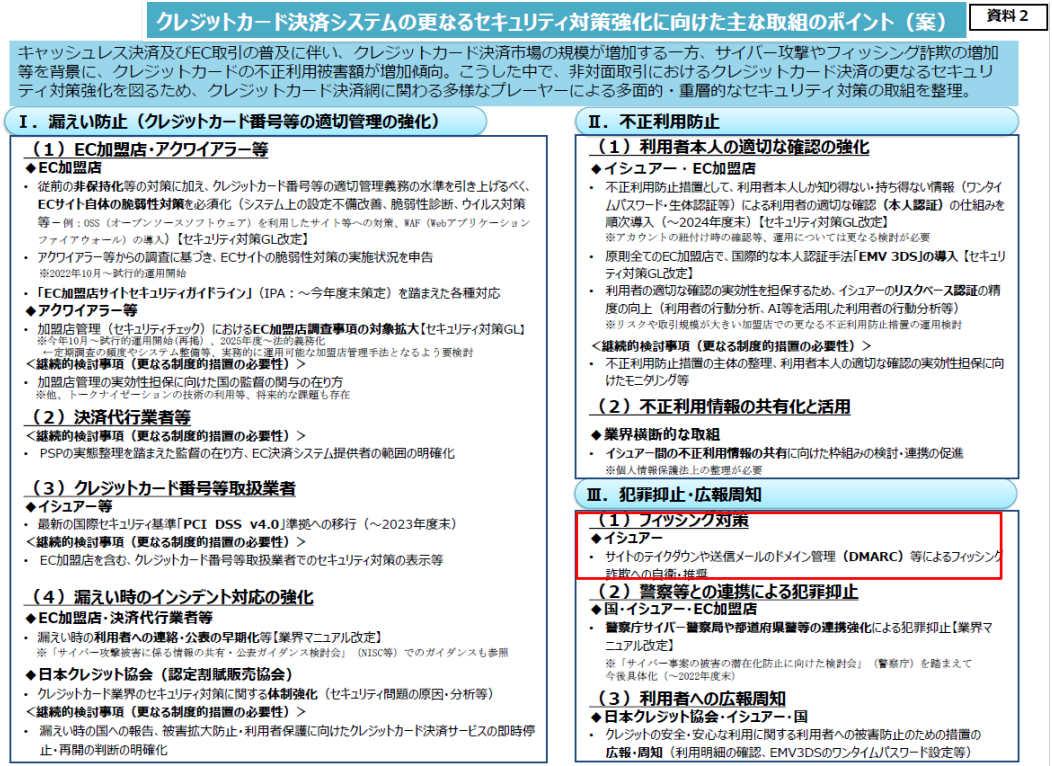
すべて正規メールなので、
DMARC判定もpass

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

経済産業省：令和4年 (2022年) クレジットカード決済システムのセキュリティ対策強化検討会



クレジットカード決済システムの更なるセキュリティ対策強化に向けた主な取組のポイント（案）

資料２

キャッシュレス決済及びEC取引の普及に伴い、クレジットカード決済市場の規模が増加する一方、サイバー攻撃やフィッシング詐欺の増加等を背景に、クレジットカードの不正利用被害額が増加傾向。こうした中で、非対面取引におけるクレジットカード決済の更なるセキュリティ対策強化を図るため、クレジットカード決済網に関わる多様なプレーヤーによる多面的・重層的なセキュリティ対策の取組を整理。

Ⅰ．漏えい防止（クレジットカード番号等の適切管理の強化）

（１）EC加盟店・アクワイアラー等

◆EC加盟店

- 従前の**非保持化**等の対策に加え、クレジットカード番号等の適切管理義務の水準を引き上げるべく、**ECサイト自体の脆弱性対策**を必須化（システム上の設定不備改善、脆弱性診断、ウイルス対策等－例：OSS（オープンソースソフトウェア）を利用したサイト等への対策、WAF（Webアプリケーションファイアウォール）の導入）【セキュリティ対策GL改定】
- アクワイアラー等からの調査に基づき、ECサイトの脆弱性対策の実施状況を申告
  ※2022年10月～試行的運用開始
- 「EC加盟店サイトセキュリティガイドライン」（IPA：～今年度末策定）を踏まえた各種対応

◆アクワイアラー等

- 加盟店管理（セキュリティチェック）における**EC加盟店調査事項の対象拡大**【セキュリティ対策GL】
  ※今年10月～試行的運用開始（再掲）、2025年度～法的義務化
  －定期調査の頻度やシステム監査等、実務的に運用可能な加盟店管理手法となるよう要検討

＜継続的検討事項（更なる制度的措置の必要性）＞

- 加盟店管理の実効性担保に向けた国の監督の関与の在り方
  ※他、トークナイゼーションの技術の利用等、将来的な課題も存在

（２）決済代行業者等

＜継続的検討事項（更なる制度的措置の必要性）＞

- PSPの実態整理を踏まえた監督の在り方、EC決済システム提供者の範囲の明確化

（３）クレジットカード番号等取扱業者

◆イシュアー等

- 最新の国際セキュリティ基準「PCI DSS v4.0」準拠への移行（～2023年度末）

＜継続的検討事項（更なる制度的措置の必要性）＞

- EC加盟店を含む、クレジットカード番号等取扱業者でのセキュリティ対策の表示等

（４）漏えい時のインシデント対応の強化

◆EC加盟店・決済代行業者等

- 漏えい時の**利用者への連絡・公表の早期化**等【業界マニュアル改定】
  ※「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」（NISC等）でのガイダンスも参照

◆日本クレジット協会（認定割賦販売協会）

- クレジットカード業界のセキュリティ対策に関する**体制強化**（セキュリティ問題の原因・分析等）

＜継続的検討事項（更なる制度的措置の必要性）＞

- 漏えい時の国への報告、被害拡大防止・利用者保護に向けたクレジットカード決済サービスの即時停止・再開の判断の明確化

Ⅱ．不正利用防止

（１）利用者本人の適切な確認の強化

◆イシュアー・EC加盟店

- 不正利用防止措置として、利用者本人しか知り得ない・持ち得ない情報（ワンタイムパスワード・生体認証等）による利用者の適切な確認（**本人認証**）の仕組みを順次導入（～2024年度末）【セキュリティ対策GL改定】
  ※アカウントの紐付け時の確認等、運用については更なる検討が必要
- 原則全てのEC加盟店で、国際的な本人認証手法「**EMV 3DS**」の**導入**【セキュリティ対策GL改定】
- 利用者の適切な確認の実効性を担保するため、イシュアーの**リスクベース認証**の精度の向上（利用者の行動分析、AI等を活用した利用者の行動分析等）
  ※リスクや取引規模が大きい加盟店での更なる不正利用防止措置の運用検討

＜継続的検討事項（更なる制度的措置の必要性）＞

- 不正利用防止措置の主体の整理、利用者本人の適切な確認の実効性担保に向けたモニタリング等

（２）不正利用情報の共有化と活用

◆業界横断的な取組

- **イシュアー間の不正利用情報の共有**に向けた枠組みの検討・連携の促進
  ※個人情報保護法上の整理が必要

Ⅲ．犯罪抑止・広報周知

（１）フィッシング対策

◆イシュアー

- サイトのテイクダウンや送信メールのドメイン管理（**DMARC**）等によるフィッシング詐欺への自衛・推奨

（２）警察等との連携による犯罪抑止

◆国・イシュアー・EC加盟店

- **警察庁サイバー警察局や都道府県警等の連携強化**による犯罪抑止【業界マニュアル改定】
  ※「サイバー事案の被害の潜在化防止に向けた検討会」（警察庁）を踏まえて今後具体化（～2022年度末）

（３）利用者への広報周知

◆日本クレジット協会・イシュアー・国

- クレジットの安全・安心な利用に関する利用者への被害防止のための措置の**広報・周知**（利用明細の確認、EMV3DSのワンタイムパスワード設定等）

※「世界一安全な日本」創造戦略（2022年12月改定）においても、クレジットカード等の決済の本人認証や不正検知の強化、フィッシング対策の推進等が必要とされている。
※セキュリティ対策GL：クレジットカード・セキュリティガイドライン（クレジット取引セキュリティ対策協議会）

経済産業省：2022年12月23日 第5回 クレジットカード決済システムのセキュリティ対策強化検討会
資料2　クレジットカード決済システムのセキュリティ対策強化に向けた主な取組のポイント（案）
https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/005_02_00.pdf

■ 経済産業省「クレジットカード決済システムのセキュリティ対策強化に向けた主な取組」の中で、今後、**クレジットカード発行事業者に対し、DMARCへの対応を求めていく**こととなった。

（１）フィッシング対策

◆イシュアー

- サイトのテイクダウンや送信メールのドメイン管理（DMARC）等によるフィッシング詐欺への自衛・推奨

- 2022年度に DMARC モニタリング (p=none) を開始した事業者は増えた
- 2023年、送信側の対応がますます進む可能性が高い
- DMARC対応済サービスへのニーズが高まる

みなさん、準備できてますか？

DMARCレコードを設定したけれど…

- DMARC p=none で運用中の組織のお悩み

DMARCレポートの集計結果の項目の意味が判らない

dmarc=fail が多すぎて、異変を見つけられない

どうやったら fail が減るのか判らない

メール届かなくなるんじゃないの？と言われて p=reject に踏み出せない。どう言えばいい？

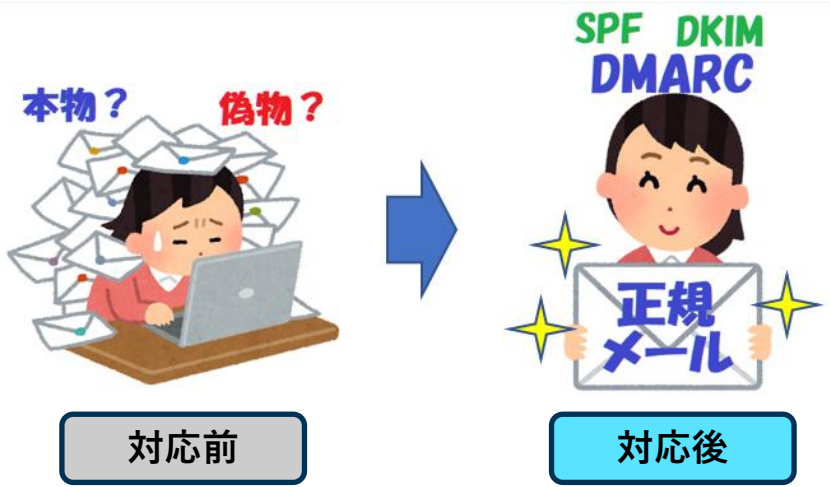
p=reject に変更する見極めポイントは？

なりすましじゃないフィッシングメール対策は、どうしたらいい？

p=none で停滞している組織、なりすまし送信され続けてる組織が動き出し、一歩踏み出すため 、そしてその先に続くお話は、このあとすぐ！

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

以後、参考資料

おさらい: DMARC の段階的導入

1. **DMARC ポリシー宣言**
   DMARCレポートを取得するだけなら、モニタリングモードで始める。メールが届かなくなることもなく、今までと変わらない。まずはレポートから状況を把握しする。
   - **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"

2. **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、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

3. **ポリシー変更**
   - **p=reject または quarantine に変更し、不正メールを排除する（pct パラメーターで適用割合を指定できる）**

4. **【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

チェックサイトの活用

- BIMI Group：BIMI Inspector
  https://bimigroup.org/bimi-generator/

- なんだか判らないけど、うまく判定されない！という場合は、DMARC SPF check などのキーワードで検索すると、チェックサイトがいろいろ出てきます。
- DMARC関連サービスを提供しているセキュリティベンダーが運用しているサイトが多い
- トラブルシューティングに役立つ詳細な情報を出してくれるサイトもある

- The AuthIndicators Working Group (bimigroup.org) は BIMI の標準化と実装を行っているベンダー等からなるグループで、BIMI のチェックできるツールを提供している
- BIMI は DMARC が正常に設定されていないとロゴが出ないので、DMARCやSPFのチェックにも使える

フィッシング対策協議会のドメイン
SPF/DMARC関連でエラーは出ていないが、
BIMI未対応なのでロゴが出ない

チェックサイトの活用

BIMI Audit Report For rakuten.co.jp

MX Record

[redacted]

MX record found for rakuten.co.jp, and is BIMI compliant

SPF Record

v=spf1 include:[redacted]
include:[redacted]
include:[redacted]

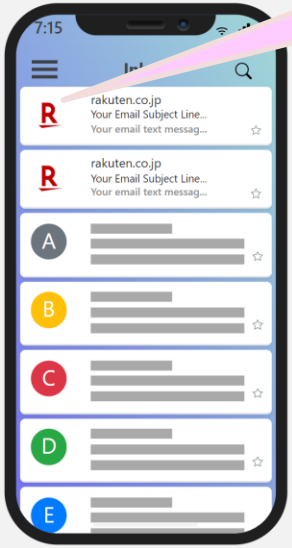
SPF record found for rakuten.co.jp, and is BIMI compliant

DMARC Record

v=DMARC1; p=reject; rua=mailto:[redacted]

DMARC record found for rakuten.co.jp, and is BIMI compliant

Your Logo Might Appear Like This



楽天さんはBIMI対応しているので、ロゴが表示される
SPF/DMARC、BIMI 関連もエラーが無いことが確認できる

BIMI SVG Image

We found the following SVG image in your BIMI record. Your SVG image is as per BIMI compliance.

https://[redacted].svg

View in Dark Mode

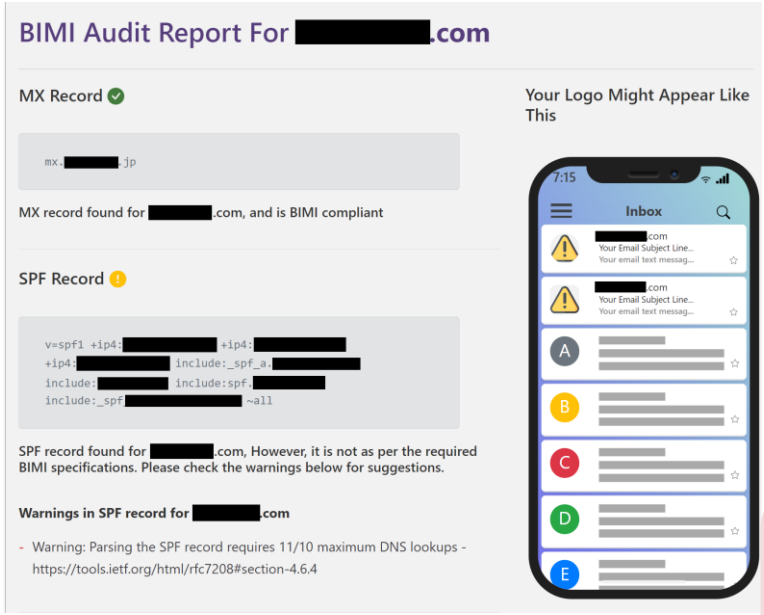
VMC Certificate

We found the following vmc certificate in your BIMI record. Your vmc certificate is as per the BIMI compliance.

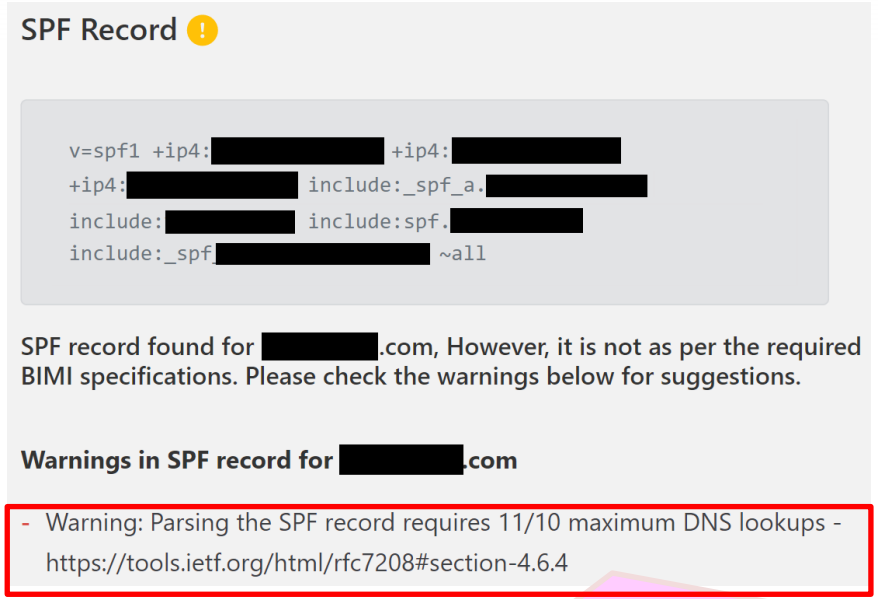
SVG Image のチェック、見え方の確認、VMC 証明書のチェックなどもできる

チェックサイトの活用

フィッシングメールを調査していると、ときどき検証エラーになっているメールを発見する



気が付かないうちにSPF検証エラーになっているパターン



SPF レコードは DNS Lookups 10回までの制限がある
メール配信サービスを次々にSPFレコードに追加していった結果、この制限値を超えているドメインがよく見られる。
include 先も Lookup 回数にカウントされるので、**include 先で include が増えると自ドメインで変更していなくとも、突然エラーになる（月1度は SPFレコードを確認することをお勧め！）**