警察庁におけるフィッシング対策について

2022年11月７日
警察庁サイバー警察局
サイバー企画課
清川　敏幸

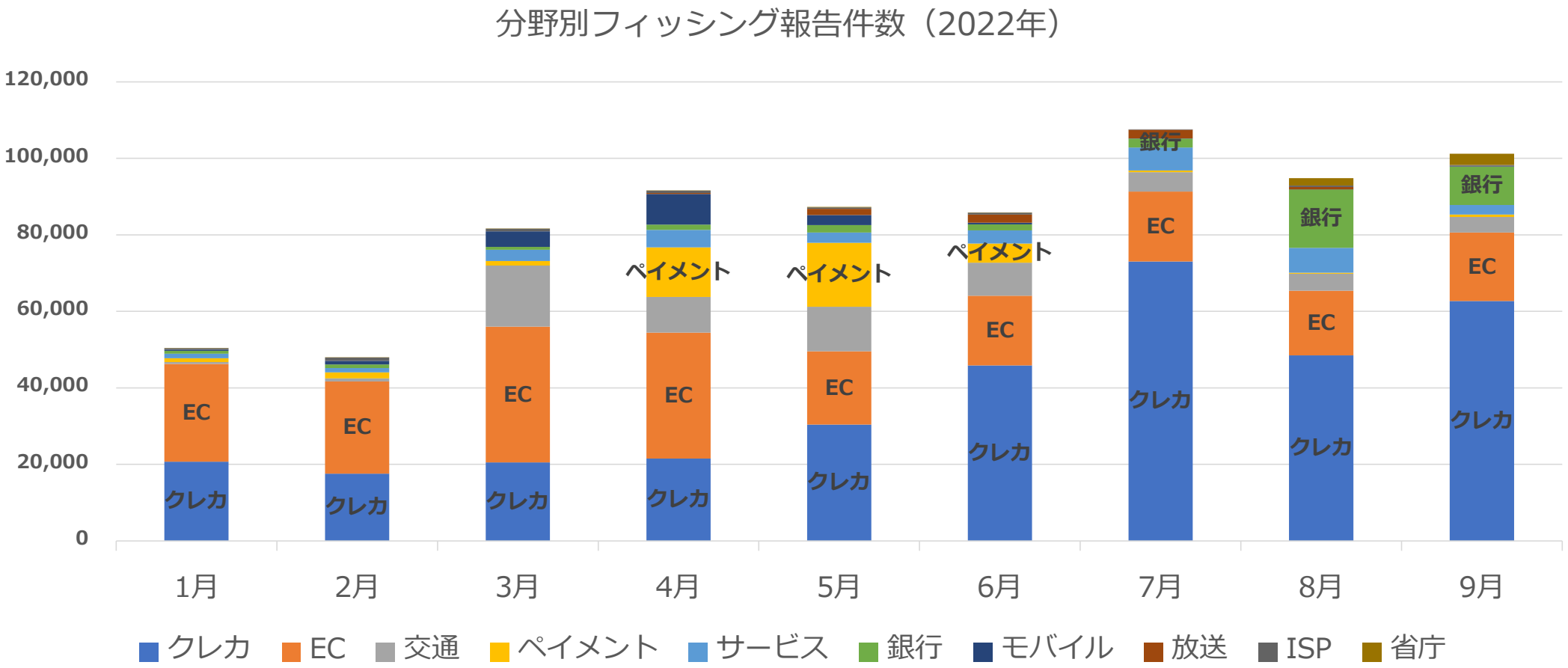
本日のアジェンダ

- フィッシングに起因する犯罪の検挙事例
- フィッシングの最新情勢
- 警察庁のフィッシング対策

フィッシングの最新情勢

分野別フィッシング報告件数

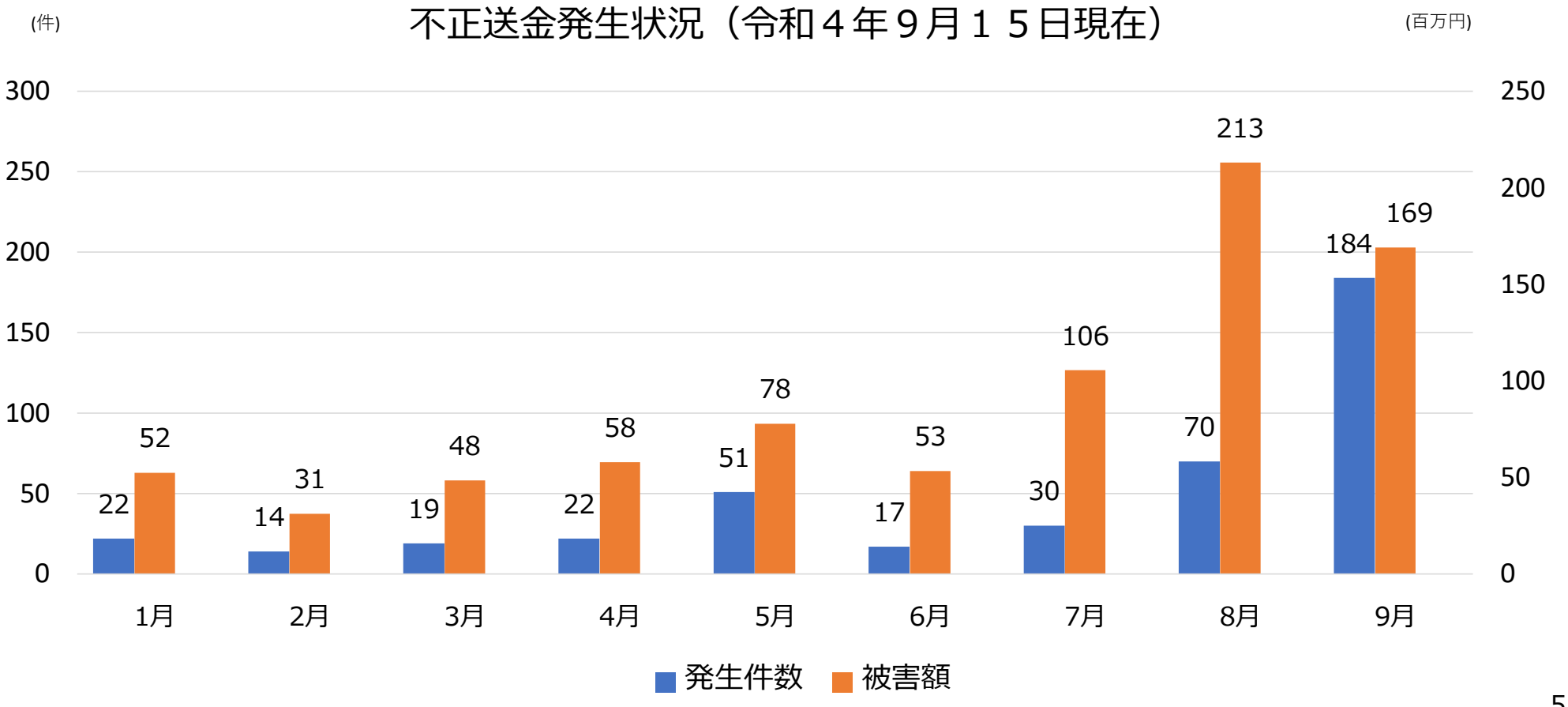
令和４年８月、９月に銀行系フィッシングが急増



※フィッシング対策協議会提供情報（上位１０分類を抜粋）

インターネットバンキング不正送金被害状況

令和４年８月、９月に被害額、発生件数が急増



ブランド別フィッシングサイト件数

２０２０年

順位	ブランド名	URL数
1	Amazon	3,707
2	楽天	3,081
3	三井住友カード	980
4	Microsoft	680
5	Apple ID	437
6	JCB	250
7	au	197
8	LINE	181
9	三井住友銀行	143
10	TS CUBIC CARD_MY TS3	111

２０２１年

順位	ブランド名	URL数
1	Amazon	6,038
2	三井住友カード	3,760
3	au	3,056
4	楽天	1,912
5	メルカリ	1,481
6	ETC利用照会サービス	1,016
7	Apple ID	901
8	NTT docomo	842
9	MICARD	790
10	Vpass	744

２０２２年上期

順位	ブランド名	URL数
1	au	5,490
2	三菱UFJニコス	4,385
3	メルカリ	4,373
4	Amazon	2,103
5	三井住友カード	1,836
6	SAISON CARD	1,698
7	えきねっと	1,359
8	イオンカード	1,156
9	JCB	1,096
10	エポスカード	1,040

※JPCERT/CCの公開情報を元に集計

警察庁のフィッシング対策

フィッシング対策のイメージ

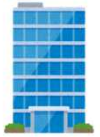
ブラウザ事業者
警告表示

セーフブラウジング警告

不正SMS遮断

携帯事業者

フィルタリング事業者



SMSHUB事業者
SMSプロバイダ

SMS

フィッシングサイト

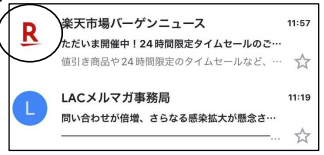
ホスティング
サーバ

メール配信サーバ

ホスティング・
レジストラ事業者
サイト削除
メール不正送信対策
不正ドメイン排除
不正契約排除

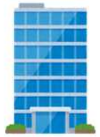
BIMI

ウイルス対策ソフト等



電子メール

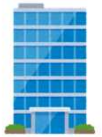
なりすまし防止対策普及啓発
(DMARC,SPF,BIMI)



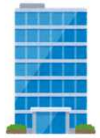
メールサービス
事業者

企業
(カード会社等)

契約



フィッシング
対策事業者
フィッシング検知
テイクダウン



セキュリティ
事業者

情報提供

事件捜査、通報受理、分析
削除要請、広報、働きかけ

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

通報受理、分析、広報

働きかけ
(国内)

一般財団法人 日本データ通信協会
(迷惑メール相談センター)
相談受理、分析

送信ドメイン認証
導入マニュアル

情報収集、分析、広報
テイクダウン

JPCERT CC®

テイクダウン（海外含む）

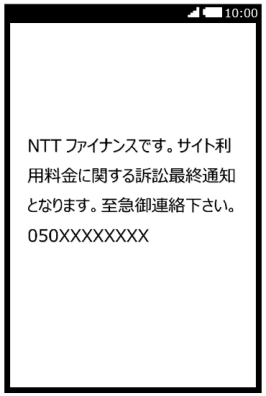
不正SMS対策

フィッシング詐欺

スミッシングSMS

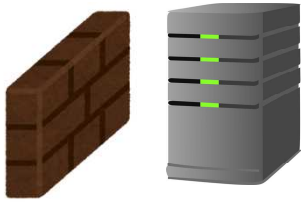
架空請求SMS

特殊詐欺



NTTドコモ

【危険SMS拒否設定】R4.3.24開始



フィッシングサイトのアドレス等

遮断

NTTドコモ利用者

分析

報道発表資料

2022 年 1 月 13 日
株式会社 NTT ドコモ

フィッシング詐欺を未然に防ぐ「危険 SMS 拒否設定」の提供を開始

株式会社 NTT ドコモ（以下、ドコモ）は、ショートメッセージ（以下、SMS）を悪用したフィッシング詐欺への対策を目的に、危険なサイトの URL などが含まれる SMS を自動で拒否※1 する「危険 SMS 拒否設定」（以下、本機能）を、2022 年 3 月中旬（予定）から提供いたします。

本機能は、不正なアプリをインストールするよう誘導したり、個人情報を盗み出そうとするサイトへ誘導したりする SMS を判定し、お客さまが受信しないようにするものです。お客さまが SMS を受信する前に、送信元情報や本文内容に基づいてドコモのネットワーク上でフィッシング SMS を自動判定します。

本機能は提供開始後、お申込み不要で自動で適用され※2※3、お客さまは無料でご利用いただけます。

セキュリティソフトにおける警告表示

偽サイト
詐欺サイト
偽ブランド品販売サイト等

インターネット利用者

相談
被害届

集約・確認

都道府県警察

報告

集約

情報
提供

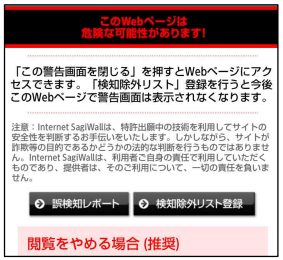
- 消費者庁
- 日本通信販売協会
- ブランド団体

JC3 日本サイバー犯罪対策センター
JC3 : Japan Cybercrime Control Center

提供件数
2021年12月現在　累計105,807件
（2021年中29,475件）

情報提供

- ウイルス対策ソフトで警告表示
- フィルタリングアプリでフィルタ
- ルータ等通信機器でフィルタ
- ブラウザ機能で警告表示
- 検索結果に注意喚起表示　等



ウイルス対策ソフト事業者　11社

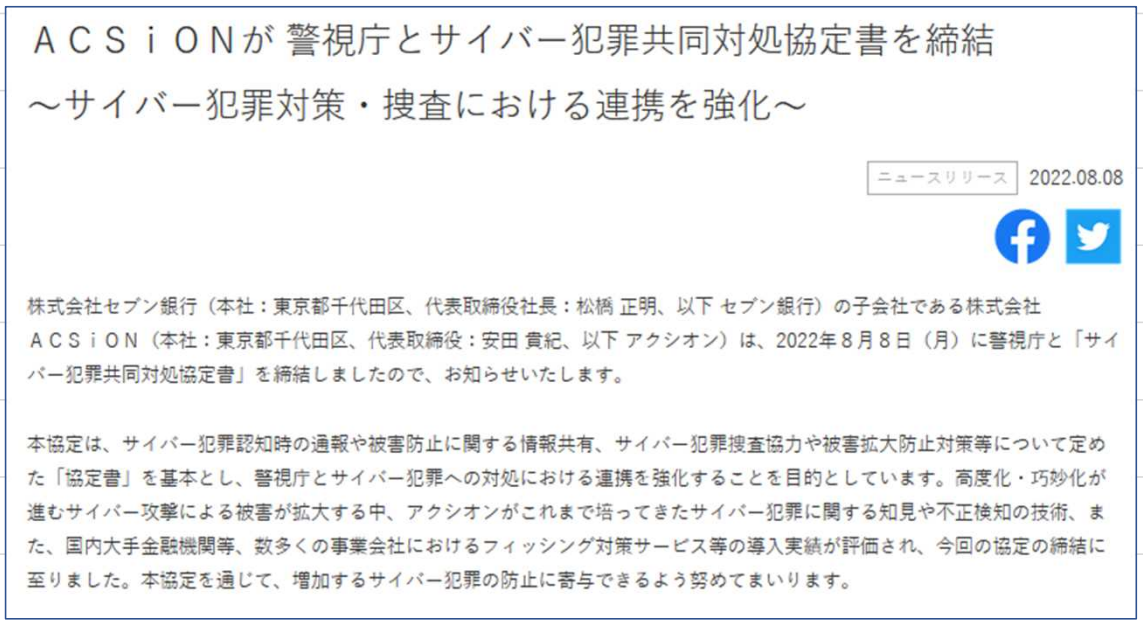
フィルタリング事業者　４社

APWG(Anti-Phishing Working Group)
全世界2,000以上の組織や企業で構成される
米国に本拠地を置くフィッシング対策等を推進する非営利団体

警察からの情報提供を増やそう

警察庁からのフィッシングURL提供件数

引用元：https://www.acsion.co.jp/news/113/



ＡＣＳｉＯＮが 警視庁とサイバー犯罪共同対処協定書を締結

～サイバー犯罪対策・捜査における連携を強化～

ニュースリリース 2022.08.08

株式会社セブン銀行（本社：東京都千代田区、代表取締役社長：松橋 正明、以下 セブン銀行）の子会社である株式会社ＡＣＳｉＯＮ（本社：東京都千代田区、代表取締役：安田 貴紀、以下 アクシオン）は、2022年８月８日（月）に警視庁と「サイバー犯罪共同対処協定書」を締結しましたので、お知らせいたします。

本協定は、サイバー犯罪認知時の通報や被害防止に関する情報共有、サイバー犯罪捜査協力や被害拡大防止対策等について定めた「協定書」を基本とし、警視庁とサイバー犯罪への対処における連携を強化することを目的としています。高度化・巧妙化が進むサイバー攻撃による被害が拡大する中、アクシオンがこれまで培ってきたサイバー犯罪に関する知見や不正検知の技術、また、国内大手金融機関等、数多くの事業会社におけるフィッシング対策サービス等の導入実績が評価され、今回の協定の締結に至りました。本協定を通じて、増加するサイバー犯罪の防止に寄与できるよう努めてまいります。

DMARCの推進

フィッシング問題への取組に関する意見

令和２年１２月３日　消費者委員会

（抜粋）

フィッシング問題への取組に関する意見

令和２年12月３日
消費者委員会

第１　背景

金融機関やECサイト等、一般消費者の認知度の高い企業やブランドを装った電子メールやSMS[1]（以下「フィッシングメール」という。）を送り、ログインID、パスワード、口座番号、
下、「フィッシング」と
ンキングに係る不正送金
いる。

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[10]（SPF[11]、DKIM[12]及びDMARC[13]）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。

https://www.cao.go.jp/consumer/iinkaikouhyou/2020/1203_iken.html

ブランド別フィッシングサイト件数

２０２０年

順位	ブランド名	URL数
1	Amazon	3,707
2	楽天	3,081
3	三井住友カード	980
4	Microsoft	680
5	Apple ID	437
6	JCB	250
7	au	197
8	LINE	181
9	三井住友銀行	143
10	TS CUBIC CARD_MY TS3	111

２０２１年

順位	ブランド名	URL数
1	Amazon	6,038
2	三井住友カード	3,760
3	au	3,056
4	楽天	1,912
5	メルカリ	1,481
6	ETC利用照会サービス	1,016
7	Apple ID	901
8	NTT docomo	842
9	MICARD	790
10	Vpass	744

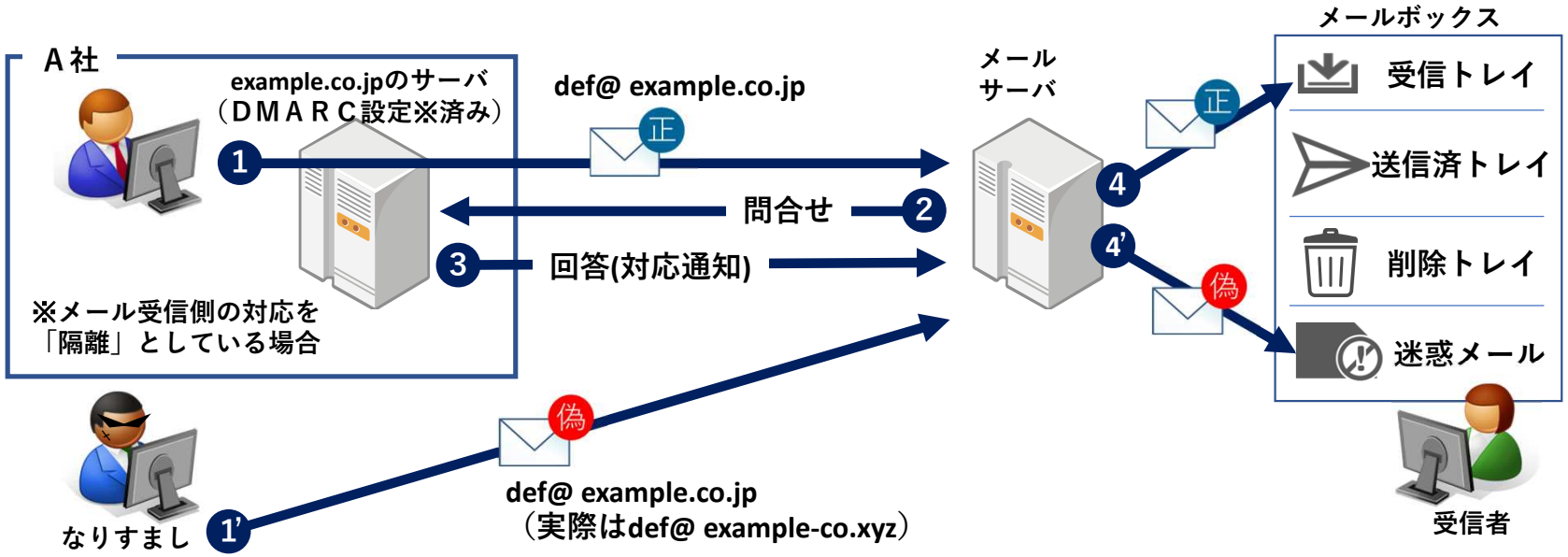
２０２２年上期

順位	ブランド名	URL数
1	au	5,490
2	三菱UFJニコス	4,385
3	メルカリ	4,373
4	Amazon	2,103
5	三井住友カード	1,836
6	SAISON CARD	1,698
7	えきねっと	1,359
8	イオンカード	1,156
9	JCB	1,096
10	エポスカード	1,040

※JPCERT/CCの公開情報を元に集計

ＤＭＡＲＣの仕組みの概要

DMARCを導入することにより、なりすましメールを迷惑メールフォルダに隔離（quarantine）したり、メールボックスに到達させない（reject）ようにすることができます。
下図は、隔離の際の仕組みの概要について説明しています。



正規メール の場合

1. 正規のメール を送信
2. Ａ社のサーバに問合せ
3. Ａ社のサーバが回答
4. は受信トレイに

なりすましメール の場合

1’ なりすましメール を送信
2. Ａ社のサーバに問合せ
3. Ａ社のサーバが回答
4’ **は迷惑メールフォルダに**（隔離）

ＤＭＡＲＣの導入手順概要

１　ＳＰＦ、ＤＫＩＭの設定

送信元メールサーバ認証（ＳＰＦ）及び電子署名の付与（ＤＫＩＭ）を設定

⚠ ＳＰＦのみを設定している場合は、ＤＭＡＲＣの導入を慎重に検討（後述）

２　自社内のドメインの見直し

自社で使用するメールのドメイン、送信メールサーバ情報の棚卸し

３　ＤＭＡＲＣの導入（試行）

受信側の振る舞い（DMARCポリシー）を【none（何もしない）】として運用開始

４　ＤＭＡＲＣのレポート確認

自社からの正規なメールが認証失敗になっていないか確認

５　ＤＭＡＲＣの本格運用

DMARCポリシーを【reject（拒否）】に設定し、なりすましメールを排除

（参考）送信ドメイン認証技術導入マニュアル【第３版】

DMARCを含めた送信ドメイン認証に関する技術的な導入マニュアルが、迷惑メール対策推進協議会から公表されています。

https://www.dekyo.or.jp/soudan/aspc/report.html

DMARC導入事例（とある企業）

ＤＭＡＲＣの運用

- 企業内で使用しているメールの棚卸し
- 最初はp=none（隔離も拒絶もしない）で情報収集
- 送られてくるレポート情報を分析
  【社内から送信している正規なメールがFailになっていないか確認】
- Failになっている社内メールの設定を改善【ＳＰＦ、ＤＫＩＭ設定の改善】
- 社内メールの設定改善が終了した時点でp=reject（破棄）設定
- 企業内で使用するメールに関する継続的なガバナンスが必要
- レポート情報を分析するには、ＤＭＡＲＣを理解する人員の確保が必要

これが重要
しかし大変

ＤＭＡＲＣの効果

- なりすましメールが減少【３か月後に８割減少、最大時は９割以上減少】
- コールセンターへの顧客からの問合せが減少【３か月後に８割減少】

なりすまし
が多い企業
ほど効果大

DMARCは万能か？

ＤＭＡＲＣを勧めると聞こえてくる声

なりすまし以外のメールには効果がない

- 類似ドメインを用いたメール
- 全く無関係なドメインを用いたメール

公式ブランドマーク等への対応

メーリングリスト等転送メールが届かない可能性ある

- 送信メールサーバが送信者と異なるケースがある
- 件名などヘッダ情報の書き換えに対応しきれないケースがある

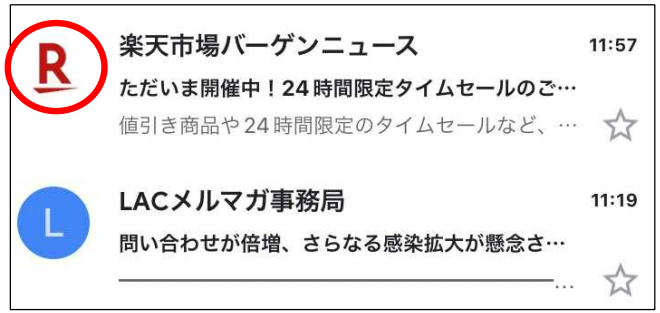
ＤＫＩＭで対応

エモテットには効果がない

- 正規サーバが乗っ取られて送信されるのでＤＭＡＲＣはＰＡＳＳ
- そもそもＤＭＡＲＣはエモテット対策の技術ではありません

ＤＭＡＲＣはフィッシング対策の一つです

公式ブランドマークについて

	ヤフーブランドアイコン	ドコモメール公式アカウント	BIMI (Brand Indecators for Message Identification)	
				
提供元	**ヤフー株式会社**	**株式会社NTTドコモ**	**Google**	**Apple**
対応ソフト	Yahoo!メール	ドコモメール	Gmail	iOSメールアプリ
判定	SPF又はDKIM	SPF又はDMARC	DMARC	DMARC
提供開始	2022/1	2021/5	2021/7	2022/9
登録料金	無料	無料	ドメインごとに VMC（認証マーク証明書）登録料	

これからの対策

公式アプリや「お気に入り」機能を利用する

これまでの警察における対策
主に注意喚起広報

電子メールにあるリンクは安易にクリックしない

＋

送信側、受信側
双方のDMARC対応

そもそも利用者に届かせない対策

今ここ

でも、DMARCも万能ではないので・・・

BIMIを含めた
公式ブランドマーク対応
アプリへの移行
メール内のURLなし・・・

正規なものが分かりやすくなる対策

ご清聴ありがとうございました