2023年2月8日
MCPC情報セキュリティセミナー #10

フィッシングの報告状況

一般社団法人JPCERTコーディネーションセンター
エンタープライズサポートグループ リーダー
シニアアナリスト
吉岡 道明,CISSP

JPCERT/CCの紹介

- **一般社団法人JPCERTコーディネーションセンター**
  Japan Computer Emergency Response Team / Coordination Center
  - コンピューターセキュリティインシデントへの対応、国内外にセンサーをおいたインターネット定点観測、ソフトウェアや情報システム・制御システム機器などの脆弱性への対応など国内の「セキュリティ向上を推進する活動」を実施
  - 1995年から活動を実施。現在は経済産業省や内閣官房からの委託予算で活動
  - サービス対象: 国内のインターネット利用者やセキュリティ管理担当者、ソフトウェア製品開発者等のセキュリティに関わる担当者
  - インシデント対応をはじめとする、国際連携が必要なオペレーションや情報連携に関する、**日本の窓口となる「CSIRT」**

  ※各国に同様の窓口CSIRTが存在する（米国のCISA（US-CERT）、韓国のKrCERT/CC、等）
- 経済産業省からの委託事業としてサイバー攻撃等国際連携対応調整事業を実施
- サイバーセキュリティ基本法上の「サイバーセキュリティに関する事象が発生した場合における国内外の関係者との連絡調整を行う関係機関」
- サイバーセキュリティ協議会（2019年発足）の事務局をNISCとともに実施
  （事案対応の相談や情報共有活用の運用面を担当）

JPCERT/CCの果たす役割

- JPCERT/CC

  Japan Computer Emergency Response Team / Coordination Center

- 国内における“火消し”の役割

  ⇒「インシデントレスポンスチーム」

【対策・予防】
脆弱性情報
ハンドリング

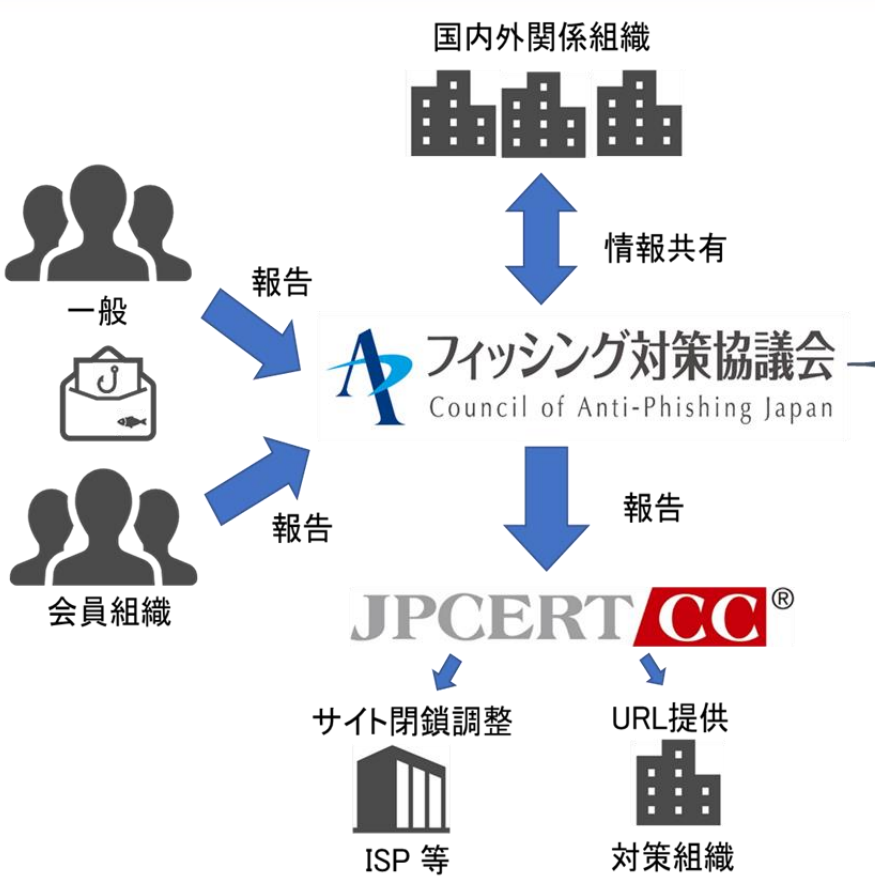
【注意喚起】
情報収集・分析
情報発信

【初動対応】
インシデント対応

- 国際間・国内連携における“窓口”の役割

  ⇒「コーディネーションセンター（CC）」

JPCERTにおけるフィッシング対策の取り組み



■情報発信(事業者／一般向け)
・緊急情報
・フィッシングに関するニュース
・ガイドライン改訂(WG活動)
・フィッシングレポート 等

■会員間の情報交流
・総会／情報交換会
・勉強会
・WG活動　等

■啓発
・フィッシング対策セミナー
・「Stop.Think.Connect.」 等

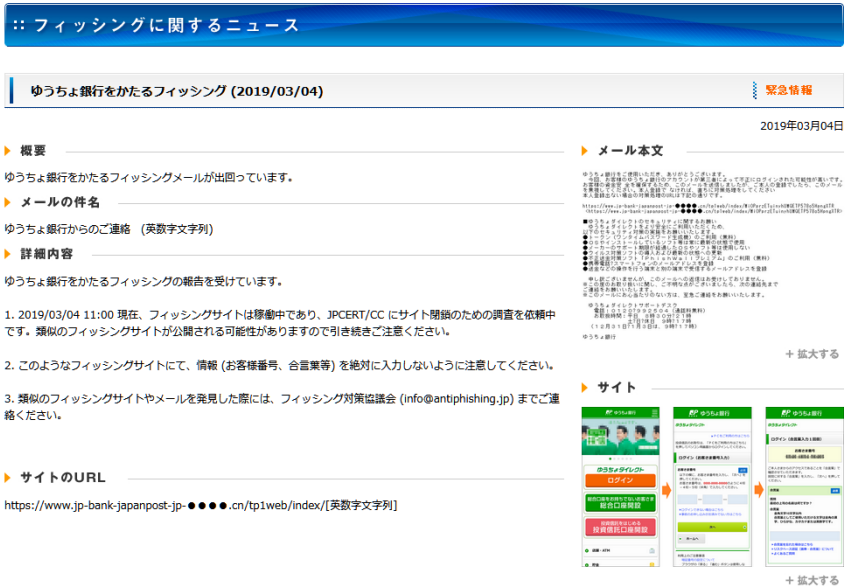
■学術研究
・フィッシングサイト早期検知 等

フィッシング対策協議会 情報発信

■ 緊急情報

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



:: フィッシングに関するニュース

ゆうちょ銀行をかたるフィッシング (2019/03/04)　緊急情報

2019年03月04日

▸ 概要

ゆうちょ銀行をかたるフィッシングメールが出回っています。

▸ メールの件名

ゆうちょ銀行からのご連絡　(英数字文字列)

▸ 詳細内容

ゆうちょ銀行をかたるフィッシングの報告を受けています。

1. 2019/03/04 11:00 現在、フィッシングサイトは稼働中であり、JPCERT/CC にサイト閉鎖のための調査を依頼中です。類似のフィッシングサイトが公開される可能性がありますので引き続きご注意ください。

2. このようなフィッシングサイトにて、情報 (お客様番号、合言葉等) を絶対に入力しないように注意してください。

3. 類似のフィッシングサイトやメールを発見した際には、フィッシング対策協議会 (info@antiphishing.jp) までご連絡ください。

▸ サイトのURL

https://www.jp-bank-japanpost-jp-●●●●.cn/tp1web/index/[英数字文字列]

▸ メール本文

＋拡大する

▸ サイト

＋拡大する

フィッシング対策協議会 情報発信

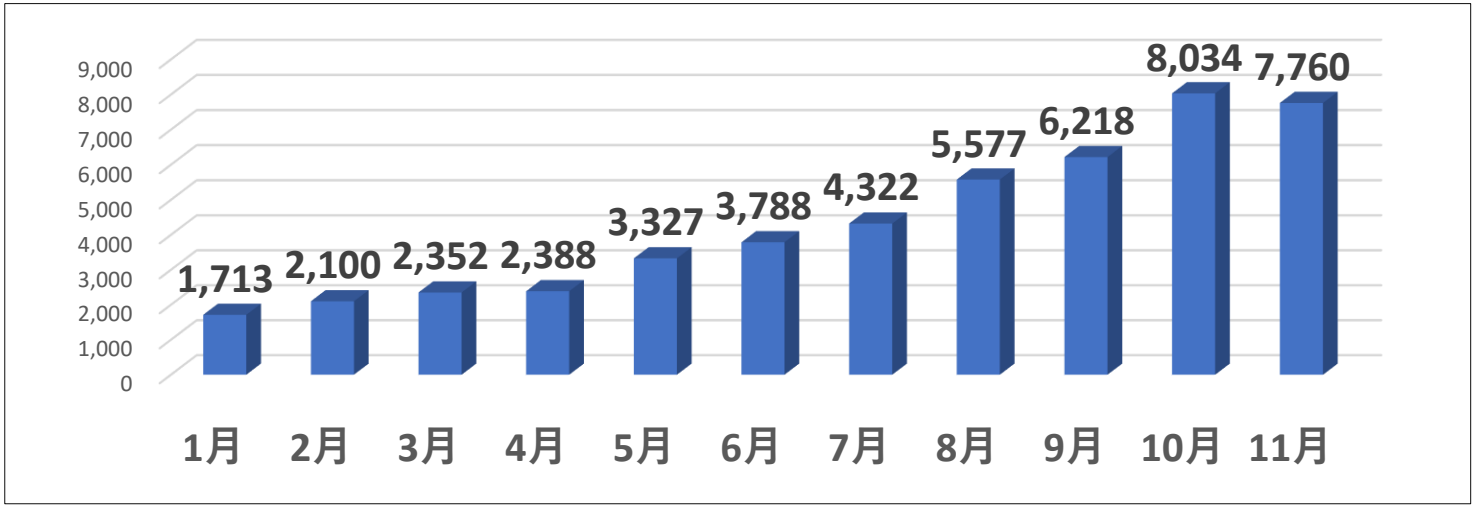
- 月次報告書

  https://www.antiphishing.jp/report/monthly/

  ―フィッシング、URL、ブランドの件数を掲載

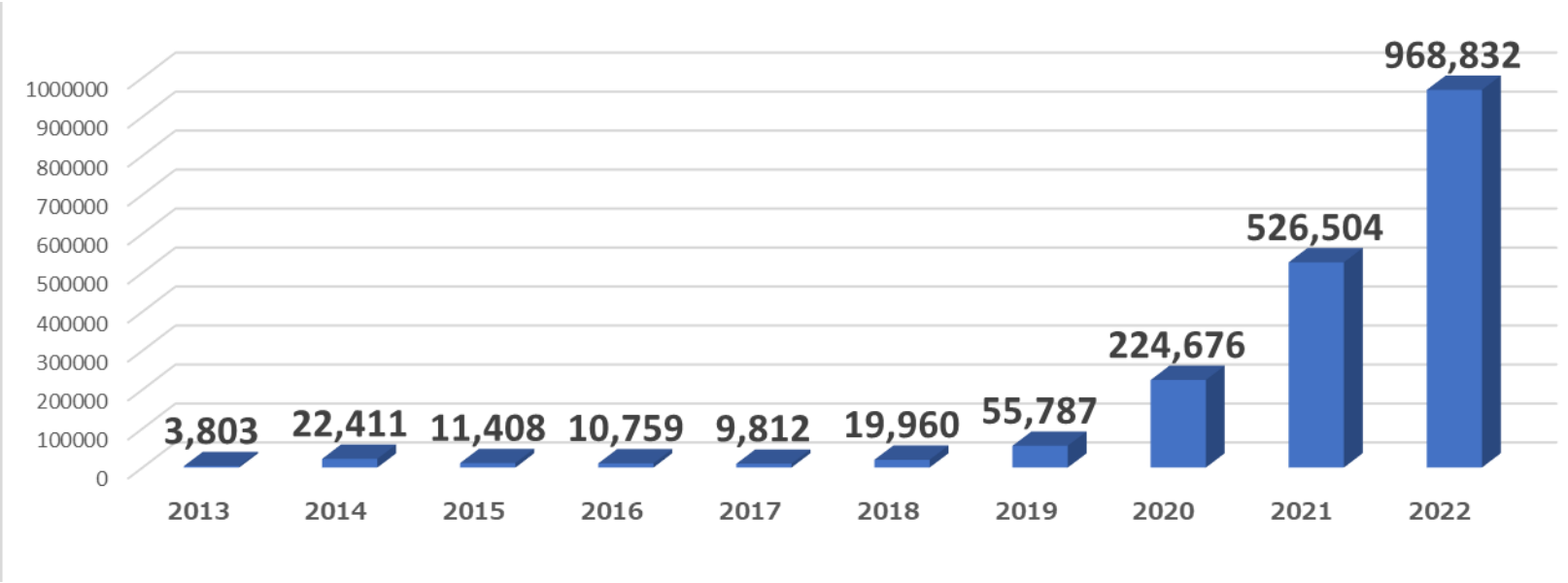
  ―1カ月分のデータを集計

  ―その月の傾向など、最新情報のサマリーを掲載



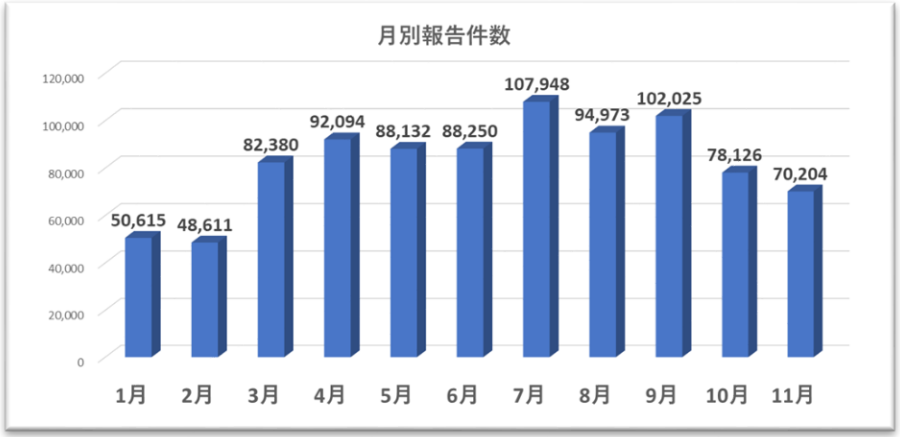
フィッシング報告状況2022

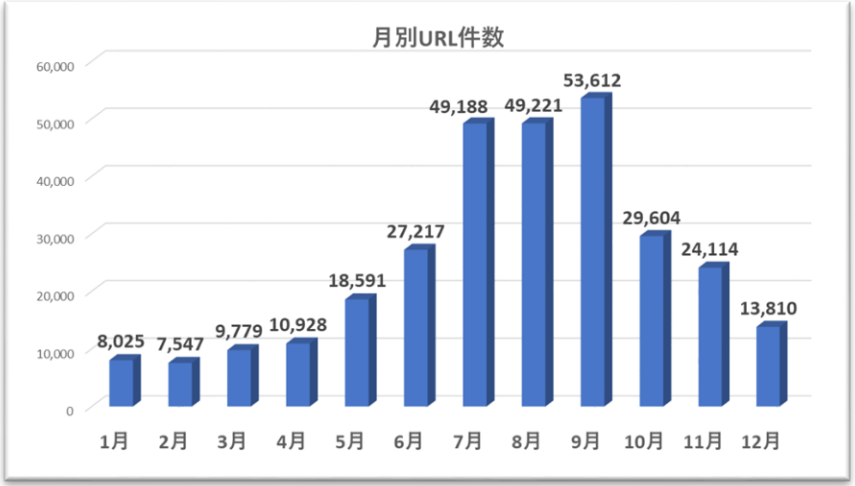
- 報告件数は2020年以降急増
- 過去最高の報告件数を毎年更新



フィッシング報告状況2022

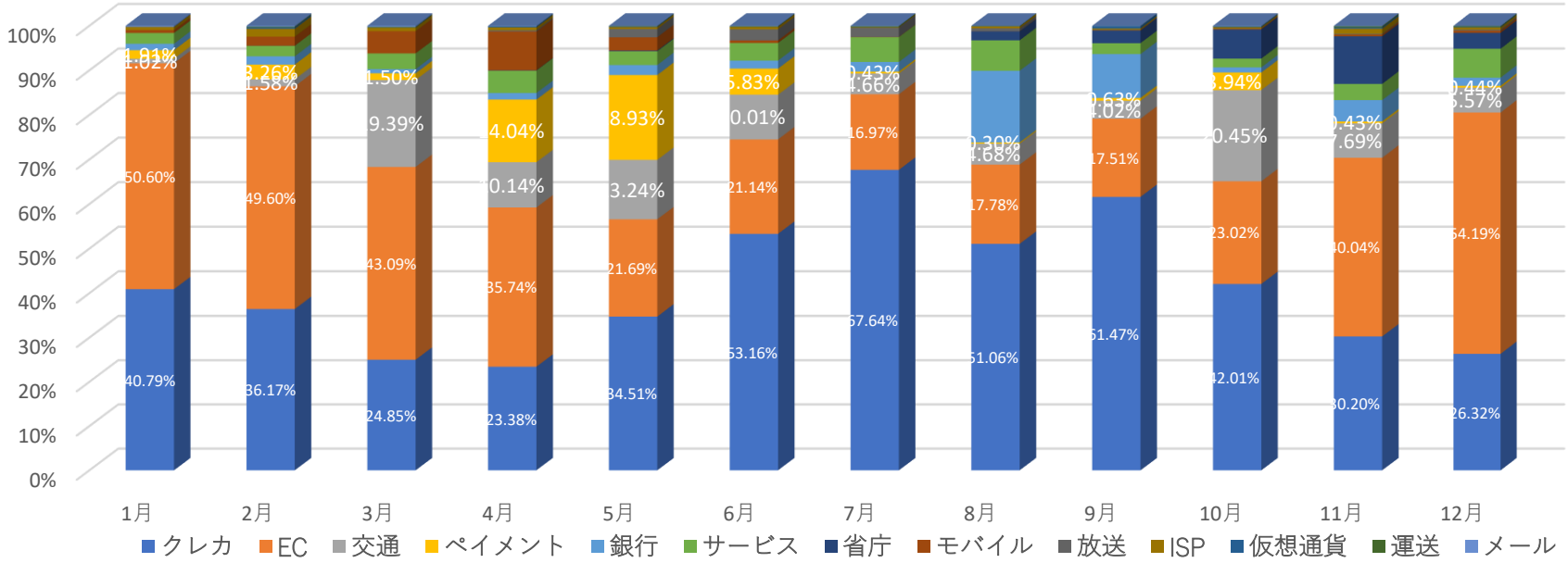
- 2022年7月過去最高の月次報告件数10万件超え
- ドメイン、サブドメインを組み合わせたURL多数観測



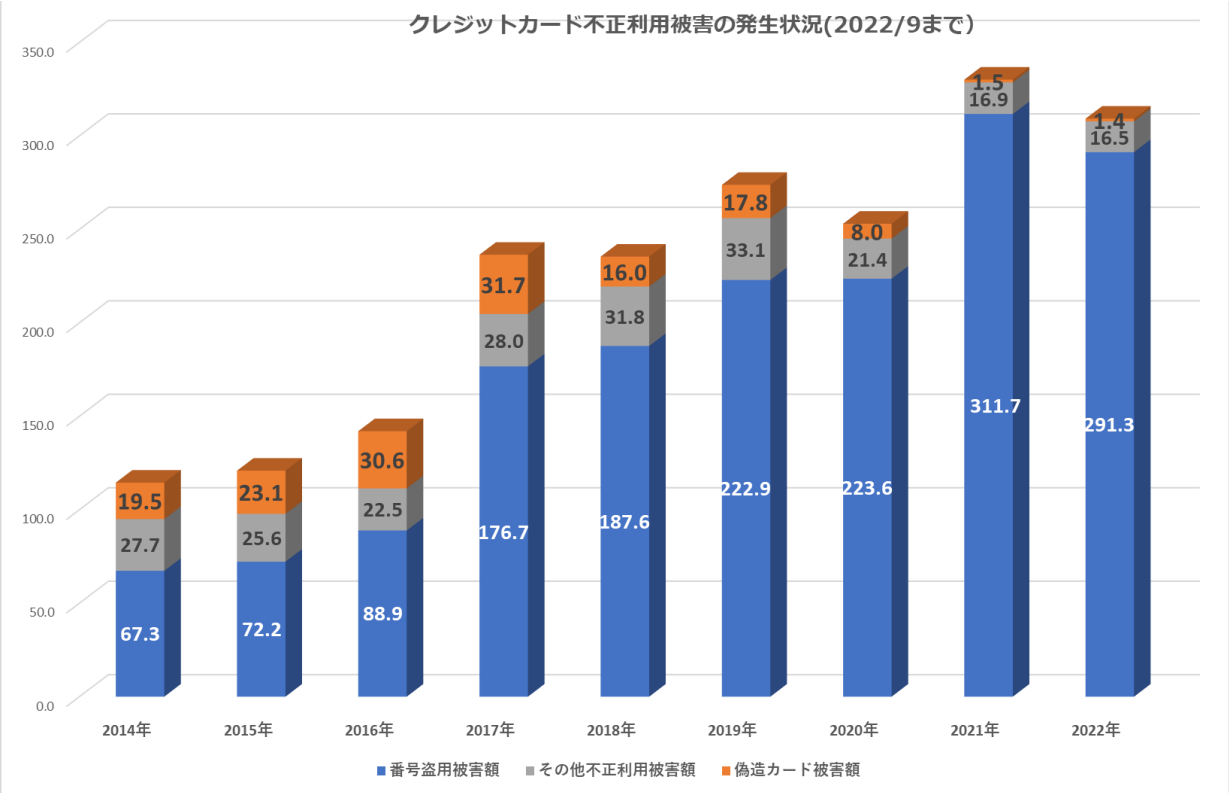


詐称される分野の割合 2022

- クレジットカードを利用できるサービスであり、ユーザーが多ければ狙われる可能性がある。誘導率の高い文面で繰り返し狙われる傾向も。
- フィッシング対応、対策が遅れている分野が狙われている可能。



クレジットカード不正利用被害の発生状況



日本クレジット協会　クレジットカード不正利用被害額の発生状況 をもとにグラフ作成
https://www.j-credit.or.jp/information/statistics/#damage

情報セキュリティ10大脅威2023（個人）

前年順位	脅威	順位
1位	**フィッシングによる個人情報等の詐取**	1位
2位	ネット上の誹謗・中傷・デマ	2位
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	3位
4位	クレジットカード情報の不正利用	4位
5位	スマホ決済の不正利用	5位
7位	不正アプリによるスマートフォン利用者への被害	6位
6位	偽警告によるインターネット詐欺	7位
8位	インターネット上のサービスからの個人情報の窃取	8位
10位	インターネット上のサービスへの不正ログイン	9位
圏外	ワンクリック請求等の不当請求による金銭被害	10位

独立行政法人 情報処理推進機構「情報セキュリティ10大脅威2023」
https://www.ipa.go.jp/security/vuln/10threats2023.html

消費者委員会「フィッシング問題への取組に関する意見」

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

- 2020年12月に消費者委員会から「フィッシング問題への取組に関する意見」として、対策を所管する、警察庁、総務省、経済産業省、消費者庁に対して「早急に取り組むべき事項」として意見が示された。

1．フィッシングメールの受信防止対策の普及促進および効果検証

2．不正アクセス禁止法等に基づく取り締まりの強化

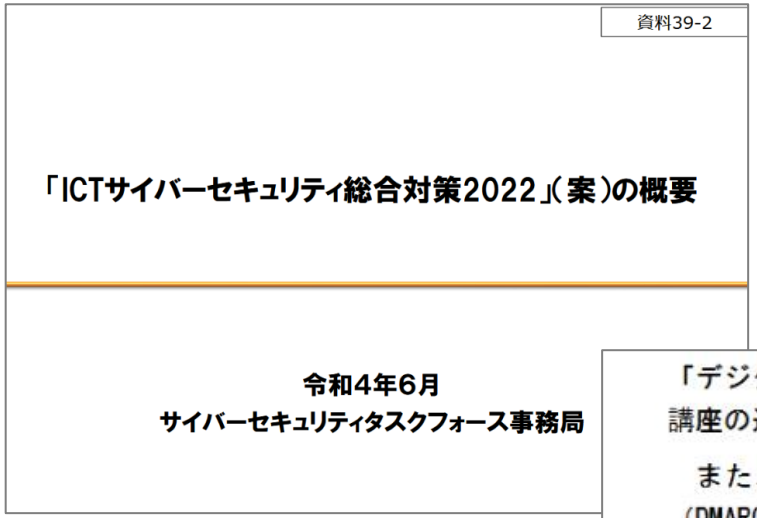
3．消費者への注意喚起の一層の強化

4．関係行政機関の連携強化

消費者委員会「フィッシング問題への取組に関する意見」

- **フィッシングメールの受信防止対策の普及促進および効果検証**
  - （１）フィッシングメールの受信防止対策の普及促進
    - ア 送信ドメイン認証技術の普及促進
    - イ 迷惑メールフィルターの啓発強化
  - （２）フィッシングメールの受信防止対策の効果検証
- **不正アクセス禁止法等に基づく取締りの強化**
- **消費者への注意喚起の一層の強化**
  - （１）消費者に対する注意喚起の強化
  - （２）消費者側の対策に係る周知啓発の強化
  - （３）注意喚起および周知啓発の効果検証
- **関係行政機関の連携強化**

総務省の動き


資料39-2

「ICTサイバーセキュリティ総合対策2022」(案)の概要

令和4年6月
サイバーセキュリティタスクフォース事務局

- 総務省サイバーセキュリティタスクフォースにて、電気通信事業者におけるDMARC等の対策導入推進が議論され「ICTサイバーセキュリティ総合対策2022」に盛り込まれる

「デジタル活用支援推進事業」については、サイバーセキュリティに関する講座の追加に向けて検討する。

また、フィッシングの急拡大を踏まえ、電気通信事業者における対策（DMARC 対応等）を推進するほか、利用者向けには、メールや SMS の送信元やリンク先 URL をよく確認することの重要性を周知するなど、普及啓発の強化を検討する。その際、利用者には真偽の判別がつきづらい、送信元を偽装するなりすまし送信メールが 2020 年６月以降大幅に増加している[49]点についても十分に留意して普及啓発を進めることが必要である。

https://www.soumu.go.jp/main_sosiki/kenkyu/cybersecurity_taskforce/02cyber01_04000001_00215.html

経済産業省の動き


日本経済新聞

朝刊・夕刊　LIVE　Myニュース

トップ　速報　オピニオン　経済　政治　ビジネス　金融　マーケット　マネーのまなび　テック　国際　スポーツ　社会・

この記事は会員限定です

フィッシング検知機能、カード250社に導入要請　経産省

経済　＋フォローする

2023年1月3日 0:00 [有料会員限定]

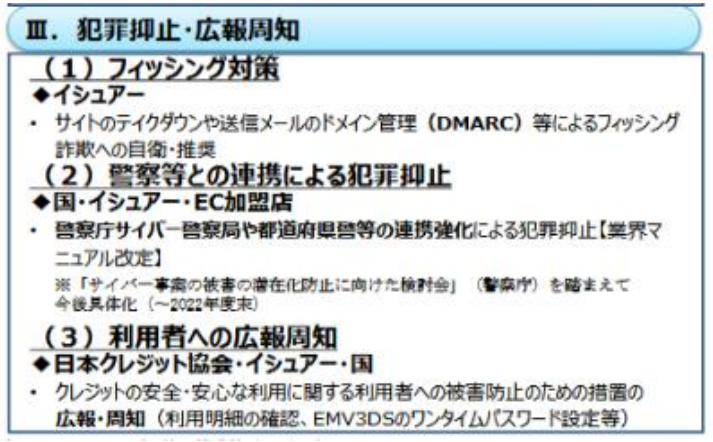
保存

経済産業省はなりすましメールで偽サイトに誘導し、カード番号などを盗み取る「フィッシング」を防ぐための対策強化をクレジットカード各社に求める。警察庁サイバー警察局と連携し、なりすましを検知する機能の導入を要請する。キャッシュレス決済のさらなる普及に向け、安全な利用環境を整える。

送信者情報を偽ったメールを防ぐ「DMARC（ディーマーク）」機能の導入を求める。カード不正利用防止の対策方針を1月中にま...

https://www.nikkei.com/article/DGXZQOUA26C990W2A221C2000000/

- 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検討会における検討結果としてイシュアーにおけるDMARC導入を要請


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）

https://www.meti.go.jp/shingikai/mono_info_service/credit_card_payment/pdf/005_02_00.pdf

フィッシング詐欺とは

- 実在する組織を騙って、ユーザーネーム、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
  （フィッシング対策協議会）

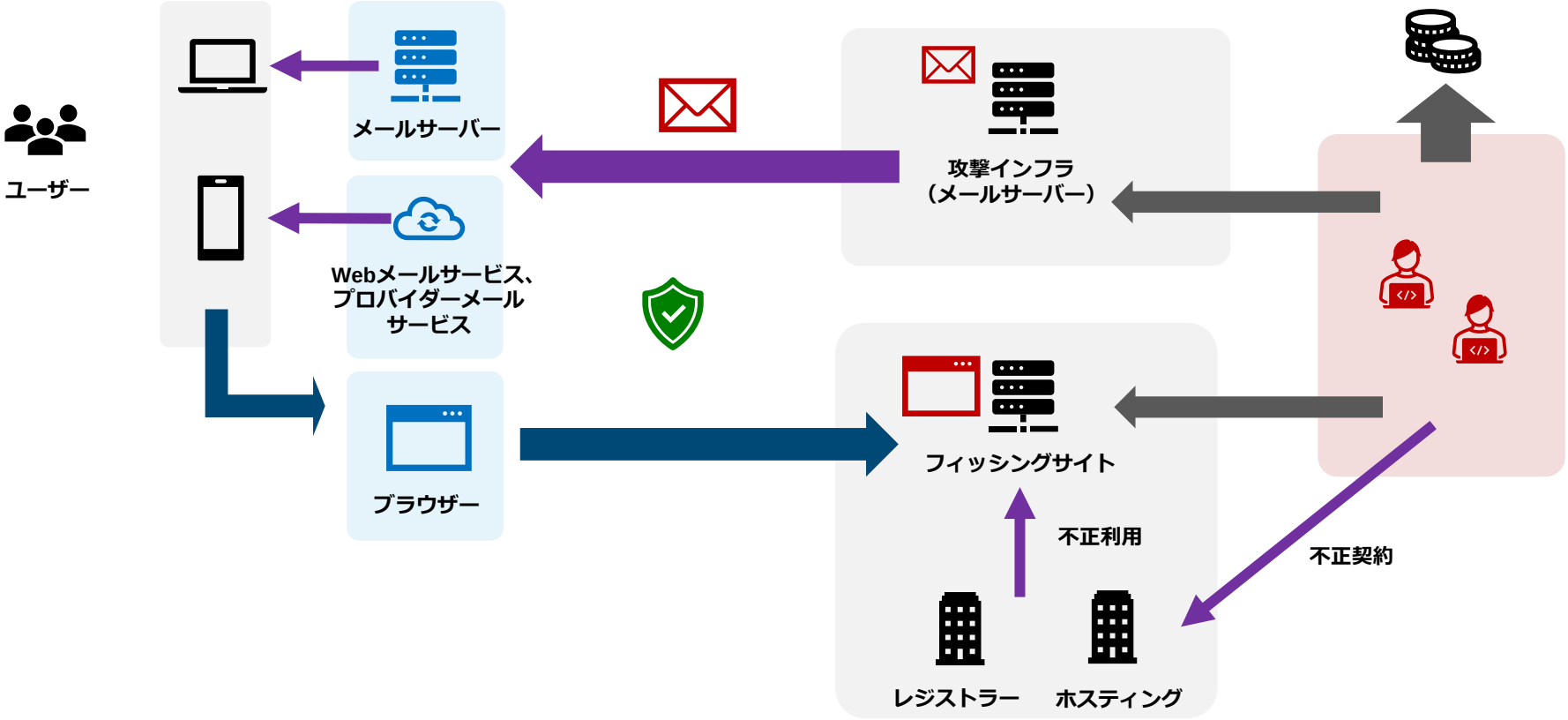
- **不正アクセス禁止法**上における「フィッシング行為」を対象
  - アクセス管理者と誤認させて利用権者に行う行為
  - 「識別符号の入力を求める情報」があるWebサイトを公開すること **（フィッシングサイト公開）**
  - 「識別符号の入力を求める情報」ある電子メールを送信すること **（フィッシングメール送信）**
  - 「識別符号」とは一般的にID・パスワード **（ログイン画面があること）**

フィッシングと扱わないケース

- 迷惑メール（特定電子メール法に違反するもの）
- 当選詐欺（スマフォ当選、100円で安く買えるなど）
- 悪質ECサイト
- 偽ブランド品販売（レイバン、オークリー等）
- セクストーションメール（性的脅迫）
- 出会い系等

捜査機関ではないので捕まえたりすることはできません

フィッシング詐欺の流れ



フィッシング犯罪の特徴

- 目的（認証情報等の詐取）を達成しやすい
  - （他の犯罪と比較した場合）フィッシングサイトに誘導すればよく、個別の被害者ごとにオペレーションを行わなくてよい
- スケールメリット？がある
  - ばらまく件数が増えれば増えるほど、1件あたりの犯罪コストは低くなる
- （他の犯罪に比べて）インフラ／ツール調達コストが低い
  - 使い捨てできるインフラサービスが多数存在している
  - マルウェア開発／調達、C2サーバー等の維持をしなくてよい
- “分業制”により足がつきにくい
  - 詐取した認証情報等を直接使わずに収益を得られる（詐取情報の転売で収益を得られる）
  - 攻撃インフラや送信元メールアドレスリストなどの“道具”を自ら調達しなくてもよい（実際に月額課金制のPhaaSも存在する）

フィッシング詐欺 実例 1

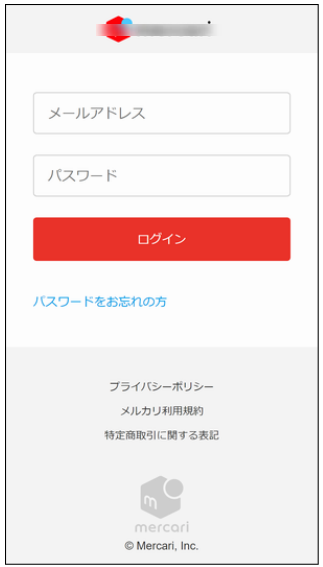
- クレジットカードの利用確認を装うフィッシング
  - 複数ブランドを使用したメール誘導
  - 大量のURLを取得（サーバーは少ない）

【JCBカード】カード年会費のお支払い方法に問題があります
【My Jcb】重要なお知らせ
【VISAカード】お支払い金額確定のご案内
VISAカード 【重要:必ずお読みください】
【Mastercard】カード年会費のお支払い方法に問題があります
【マスターカード 】重要なお知らせ
【イオンカード】カード年会費のお支払い方法に問題があります
【イオンカード】重要:必ずお読みください
【重要】AEON CARD重要なお知らせ
【重要】イオンカード 本人確認のお知らせ [メールコード A●●●●]
【重要なお知らせ】三井住友カード ご利用確認のお願い
【最終警告】三井住友カード からの緊急の連絡 [メールコード S●●●●]
【三井住友カード】事務局からのお知らせ
<緊急!三井住友カード 重要なお知らせ>
【最終警告】au PAY マーケット からの緊急の連絡
【au PAY マーケット】個人情報確認

https://www.antiphishing.jp/news/alert/creditcard_20220624.html

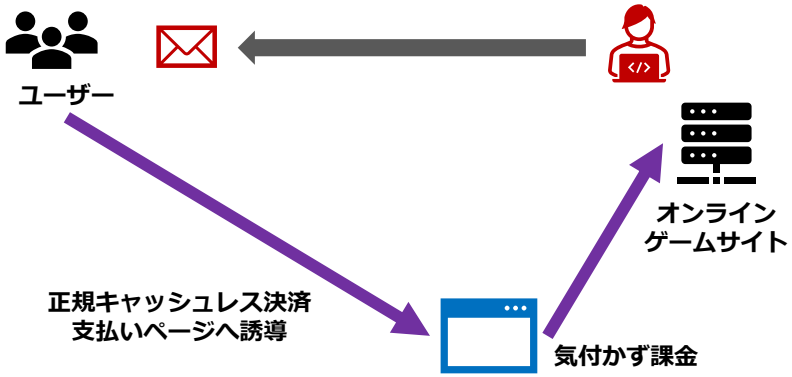
フィッシング詐欺 実例２

- キャッシュレス決済の不正利用を目的としたフィッシング
  - キャッシュレス決済が普及したことによりターゲット
  - コンビニ等での換金に利用し易い



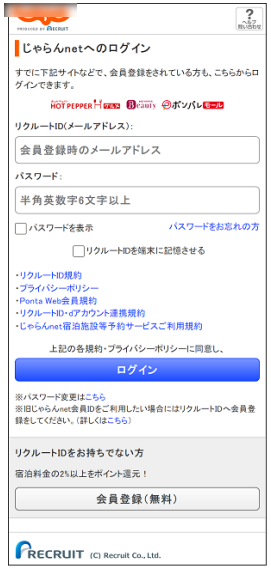
https://www.antiphishing.jp/news/alert/au_20220412_1.html
https://www.antiphishing.jp/news/alert/mercari_20211006.html

※本物の決済サイトへ誘導する手法も発生



フィッシング詐欺 実例３

- コロナ期間を開けての交通往来再開を狙うフィッシング
  - ETC利用紹介サービスをかたるフィッシングは定番化
  - 政府による全国旅行支援発表タイミング
  - リスティング広告を悪用した誘導も発生



https://www.antiphishing.jp/news/alert/etcQR_20221115.html

https://www.antiphishing.jp/news/alert/jalan_20221028.html

https://www.antiphishing.jp/news/alert/ekinet_20220729.html

https://www.antiphishing.jp/news/alert/westjr_20220729.html

フィッシング詐欺 実例４

- フィッシングサイトへの誘導にQRコードを使用
  - URLフィルターを回避するための手法
  - 過去にも発生。誘導率が低いためか短期間で終わることが多い

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。

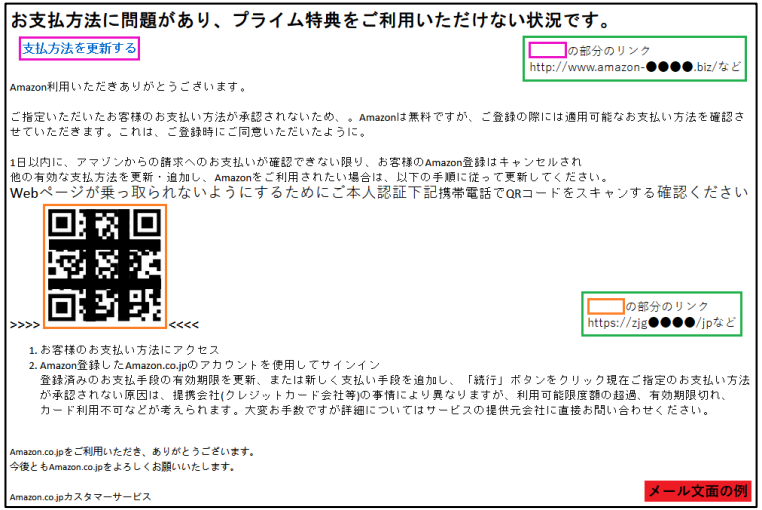
こちらのメールに返信いただいても、返答できませんのでご了承ください。

【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

https://www.antiphishing.jp/news/alert/etcQR_20221115.html



お支払方法に問題があり、プライム特典をご利用いただけない状況です。

支払方法を更新する

□□□の部分のリンク
http://www.amazon-●●●●.biz/など

Amazon利用いただきありがとうございます。

ご指定いただいたお客様のお支払い方法が承認されないため、。Amazonは無料ですが、ご登録の際には適用可能なお支払い方法を確認させていただきます。これは、ご登録時にご同意いただいたように。

1日以内に、アマゾンからの請求へのお支払いが確認できない限り、お客様のAmazon登録はキャンセルされ
他の有効な支払方法を更新・追加し、Amazonをご利用されたい場合は、以下の手順に従って更新してください。
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://zjg●●●●/jpなど

1. お客様のお支払い方法にアクセス
2. Amazon登録したAmazon.co.jpのアカウントを使用してサインイン
   登録済みのお支払手段の有効期限を更新、または新しく支払い手段を追加し、「続行」ボタンをクリック現在ご指定のお支払い方法が承認されない原因は、提携会社(クレジットカード会社等)の事情により異なりますが、利用可能限度額の超過、有効期限切れ、カード利用不可などが考えられます。大変お手数ですが詳細についてはサービスの提供元会社に直接お問い合わせください。

Amazon.co.jpをご利用いただき、ありがとうございます。
今後ともAmazon.co.jpをよろしくお願いいたします。

Amazon.co.jpカスタマーサービス

メール文面の例

https://www.antiphishing.jp/news/alert/amazonQR_20230105.html

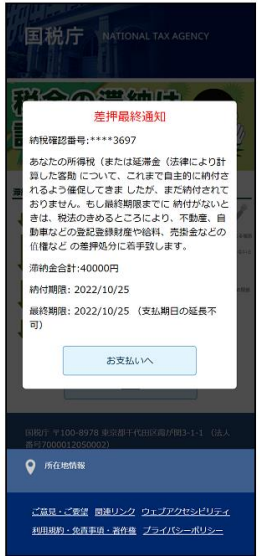
フィッシング詐欺 実例５

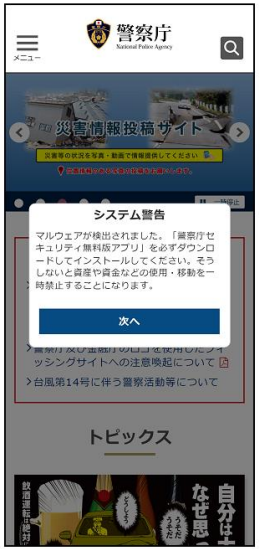
- 国税庁をかたるフィッシングが定番化
  - 金融庁、警察庁、フィッシング対策協議会をかたるものも
  - OS（Android)によっては不正アプリインストール

税金のお支払い方法に問題があります、更新してください：https://www.td[redacted].net/WbqFUa2494

【国税庁８月12日】未払い税金お支払いのお願い。ご確認ください。https://cutt.ly/[redacted]

【警察庁】重要なお知らせ、必ずお読みください。http://[redacted].duckdns.org





https://www.antiphishing.jp/news/alert/nta_20220815.html
https://www.antiphishing.jp/news/alert/npa_20221026.html

フィッシング詐欺 実例６

- フィッシングURL
  - 短縮URL、DDNSサービスを使用したフィッシング
  - Google翻訳を経由してフィッシングサイトへ誘導する手法

例）

- 短縮URL

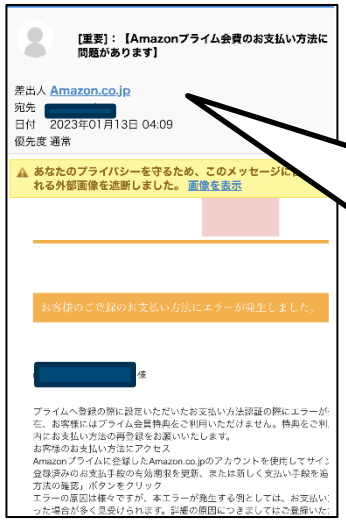
  https://**rebrand.ly**/****
- DDNSサービス

  https://servicecssam86.**duckdns.org**/?*******
- Google翻訳経由

  https://translate.google.com/translate?sl=auto&tl=ja&hl=ja&u=https://ancient-feather-b86e.h0o8rowdum.*******.***/
  ※ページ翻訳機能へフィッシングURLを指定している

スマートフォン普及による影響

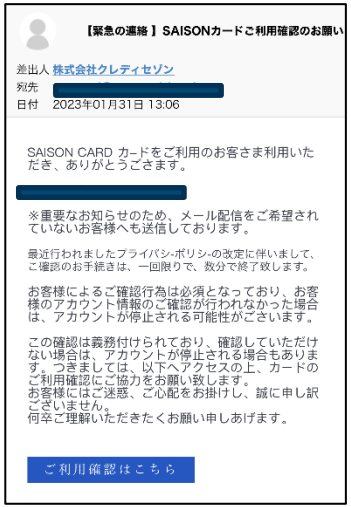
- 幅広い年齢層の方々がメールやインターネットサービスを活用
  - 狭いディスプレイ。見難い小さい文字。簡略化された文字表示。
  - 本物のメールやWebサイトをコピーしたフィッシングに気付けない。
  - 怪しいか調べる方法が難しい（**不審な～は意味がない**）



ディスプレイネームしか表示されない。長押しすると見える。

Amazon.co.jp <news-amazon@rhsvlrv.cn>

赤文字：ディスプレイネーム
青文字：本当のメールアドレス



フィッシングメールなのに差出人メールアドレスが本物の場合も

なりすまし送信メール

メールアドレスを確認しても意味がない

URL偽装

- 良く見ないとわからないURL（見てもわかりづらい）
  - サブドメインとドメインの組み合わせ
  - 大文字、小文字、フォントによっては似たように見える文字を使用
  - タイプミスするとなりそうな文字
  - スマートフォンのブラウザーでは、**ドメイン名の最初の方しか見えない**

本物）https://www.amazon.co.jp/

偽物）https://www.amazon.co.jp.kwmgmt.top/
https://amzanao.co.ip.aerrtyial.shop/
https://www.amazcznn-co-jp.amazczne.eppium.top/
https://amazom.umzasd.top/

URL偽装

2つのURLのうち、違いがわかりますか？

www.yoshioka.com

www.yoshioka.com

「Punycode(ピュニコード)」を悪用した**ホモグラフ攻撃**
「yoshioka」の中に見える「o」(オー)は、ギリシャ文字の「o」(オミクロン)

フィッシング対策ガイドライン

フィッシングは世の中の状況にあわせて、つねに変化し進化しているため、毎年、内容を精査し、改訂版を公開

- **フィッシング対策ガイドライン**
  https://www.antiphishing.jp/report/guideline/antiphishing_guideline2022.html

  Webサイト運営者向けの対策ガイドライン
  フィッシング被害を未然に防ぐための注意点や、フィッシングが発生した場合の対応を、ガイドラインとして整理

- **利用者向けフィッシング詐欺対策ガイドライン**
  https://www.antiphishing.jp/report/guideline/consumer_guideline2022.html

  一般利用者（消費者）向けの対策ガイドライン
  フィッシング事例を多く掲載し、インターネットサービスを利用する上での注意点や対策、被害にあってしまった場合の連絡先等を、ガイドラインとして整理

利用者へのアドバイス

- 急かされるような文面でも慌てない。メール、SMSのリンクからはアクセスしない
- お気に入り（ブックマーク）、正規アプリを利用して、正規サイトにアクセスする
- カード情報、口座情報、暗証番号、認証コード等の入力を求められたら一度立ち止まる
- 怪しいと思ったら「件名」「本文」内の文字列で検索したり、カード会社へ確認
- セキュリティ機能を活用する（迷惑メールフィルター、多要素認証の併用）
- メールアドレス、同一パスワード変更 （漏えい情報の再利用防止、配信リスト無効化）

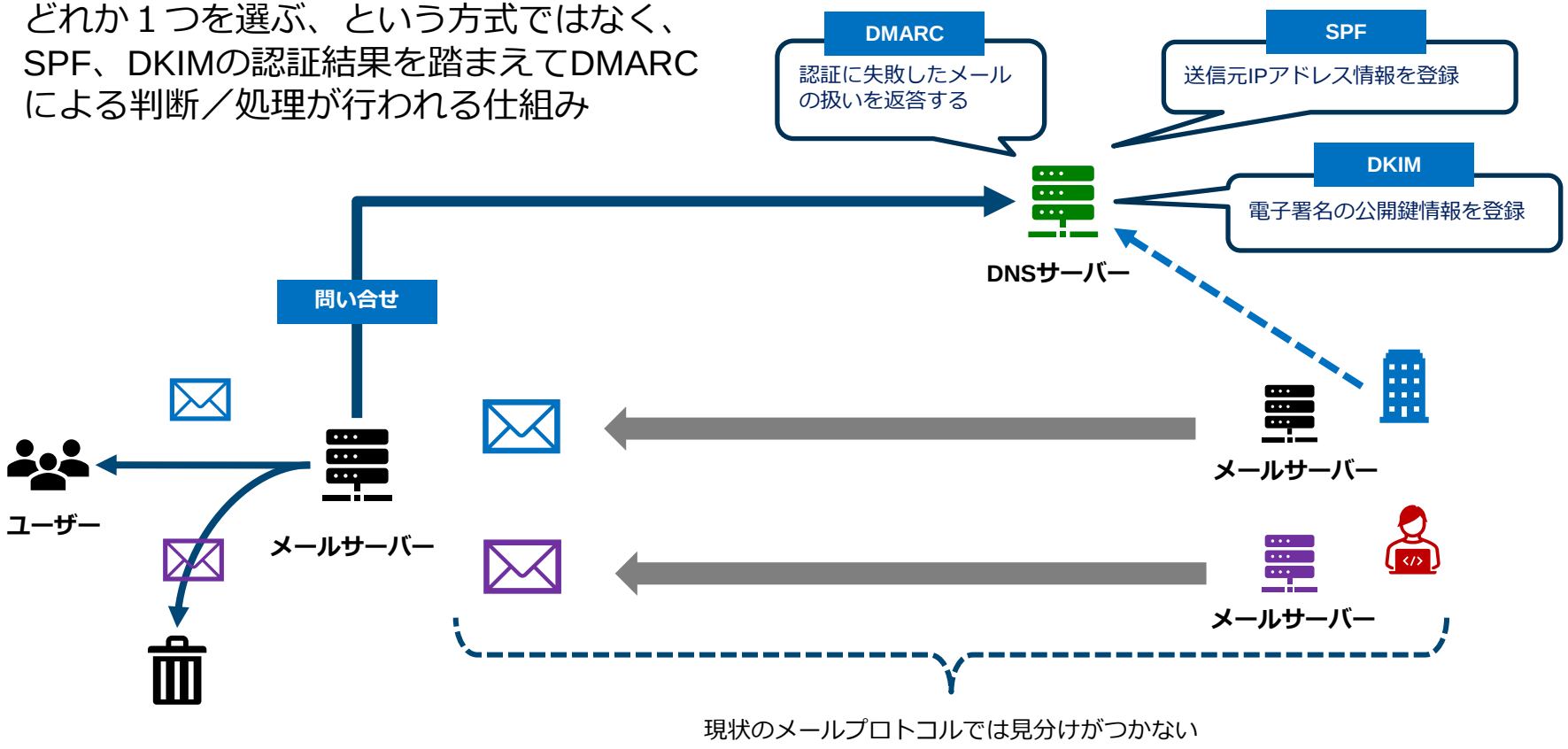
事業者の対策

フィッシング対策ガイドライン重要５項目

1. 利用者に送信するメールには「なりすましメール対策」を施すこと
2. 複数要素認証を要求すること
3. ドメインは自己ブランドと認識して管理し、利用者に周知すること
4. すべてのページにサーバー証明書を導入すること
5. フィッシング詐欺について利用者に注意喚起すること

なりすまし送信メール対策：送信ドメイン認証

- どれか１つを選ぶ、という方式ではなく、SPF、DKIMの認証結果を踏まえてDMARCによる判断／処理が行われる仕組み



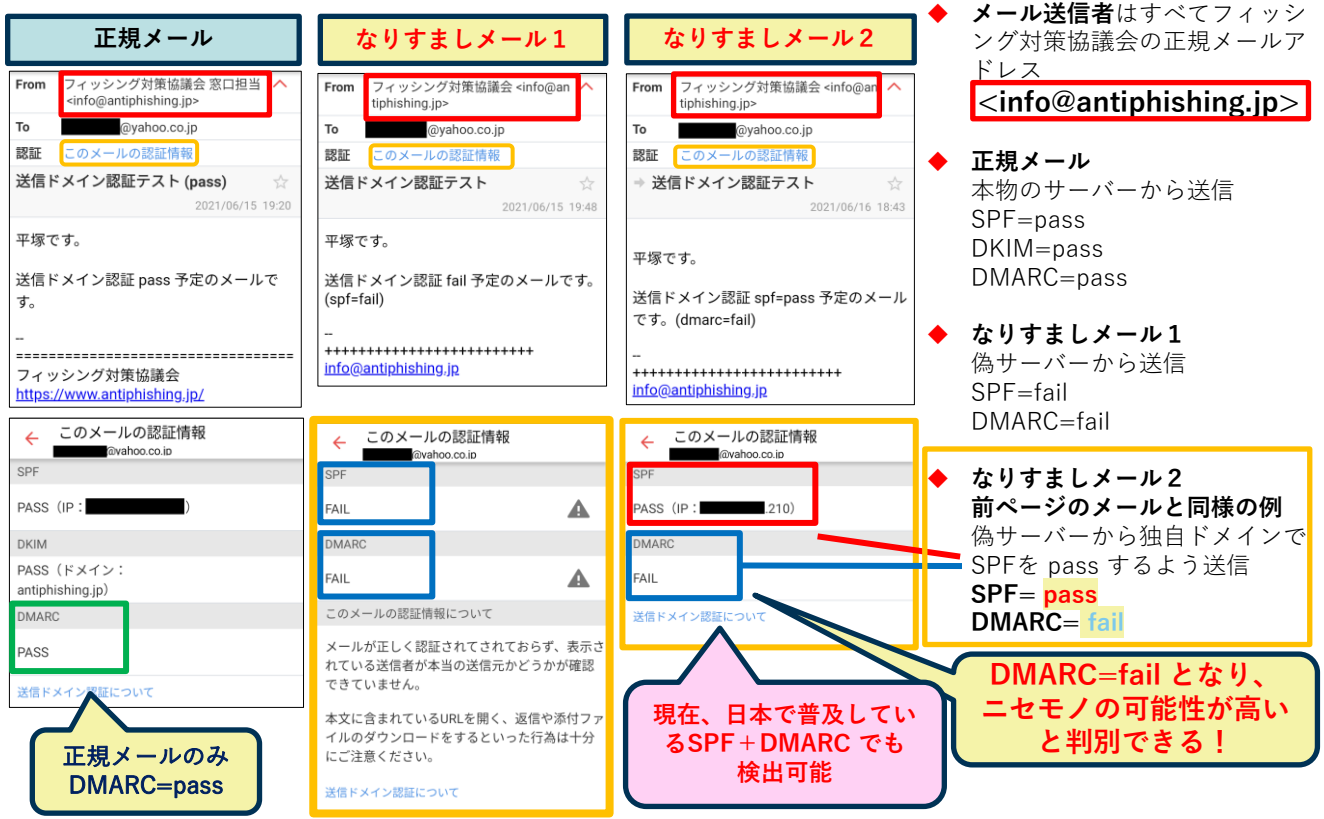
送信ドメイン認証方式の比較

	SPF	DKIM	DMARC
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	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	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ないほうのメールアドレス（エンベロープ From ）	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）	**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	送信側の設定は SPF レコードを DNS へ登録するだけで容易	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	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	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 しても素通し）	メールを転送されても検証可能	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、検証結果や効果を確認できる。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。
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	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	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

https://www.antiphishing.jp/enterprise/domain_authentication.html から筆者作成

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



◆ **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**
前ページのメールと同様の例
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

送信ドメイン認証結果の表示例（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/
- 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 は、正規メールの視認性向上のため、ブランドアイコン表示に対応している

ユーザーには、**本物メールがひとめでわかる効果**がある

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

ユーザービリティーを大きく向上！

BIMI 対応後は
本物のメールに
アイコン表示

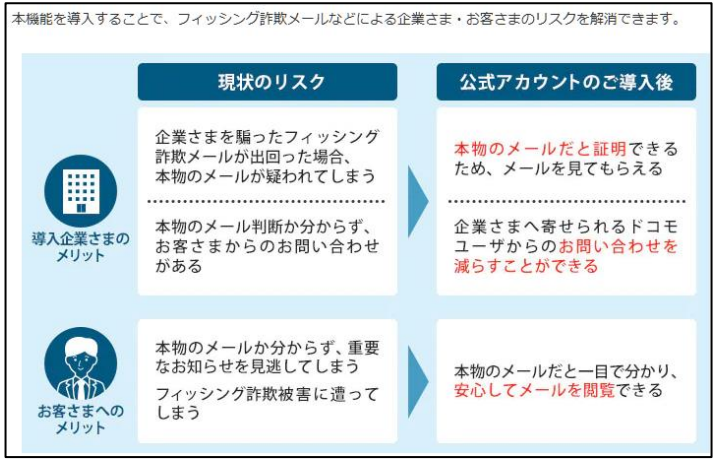
BIMI対応前は
ブランドアイコン
表示なし

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

送信ドメイン認証結果の表示例（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

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

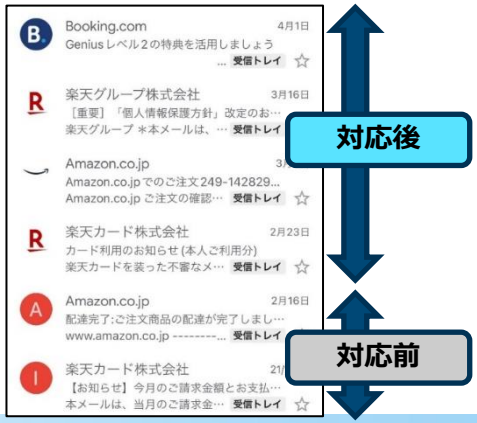


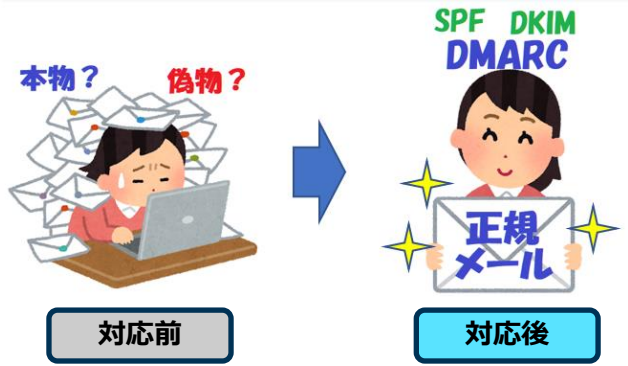
ドコモメールアプリ、Web メールで表示対応（標準機能）
銀行、クレジットカード系などを中心に、フィッシング対策に力を入れている事業者（サービス）が主に対応している

フィッシング対策 (メール関連)

- 被害ブランドへの推奨事項
  - なりすましメール対策技術 (DMARC) への対応、ポリシーの強化
  - DMARC レポートによるフィッシングメール配信検知と規模の把握
  - 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

- 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 (DMARCポリシーによるフィルタリング)
  - ブランドアイコンや BIMI、公式アカウントなど、正規メールの見分け方を知る
  - 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





関係省庁フィッシング対策の強化を要請

- 2023年2月1日 経済産業省、警察庁および総務省が連名で、クレジットカード会社等に対し、送信ドメイン認証技術（DMARC)の導入をはじめとするフィッシング対策の強化を要請。

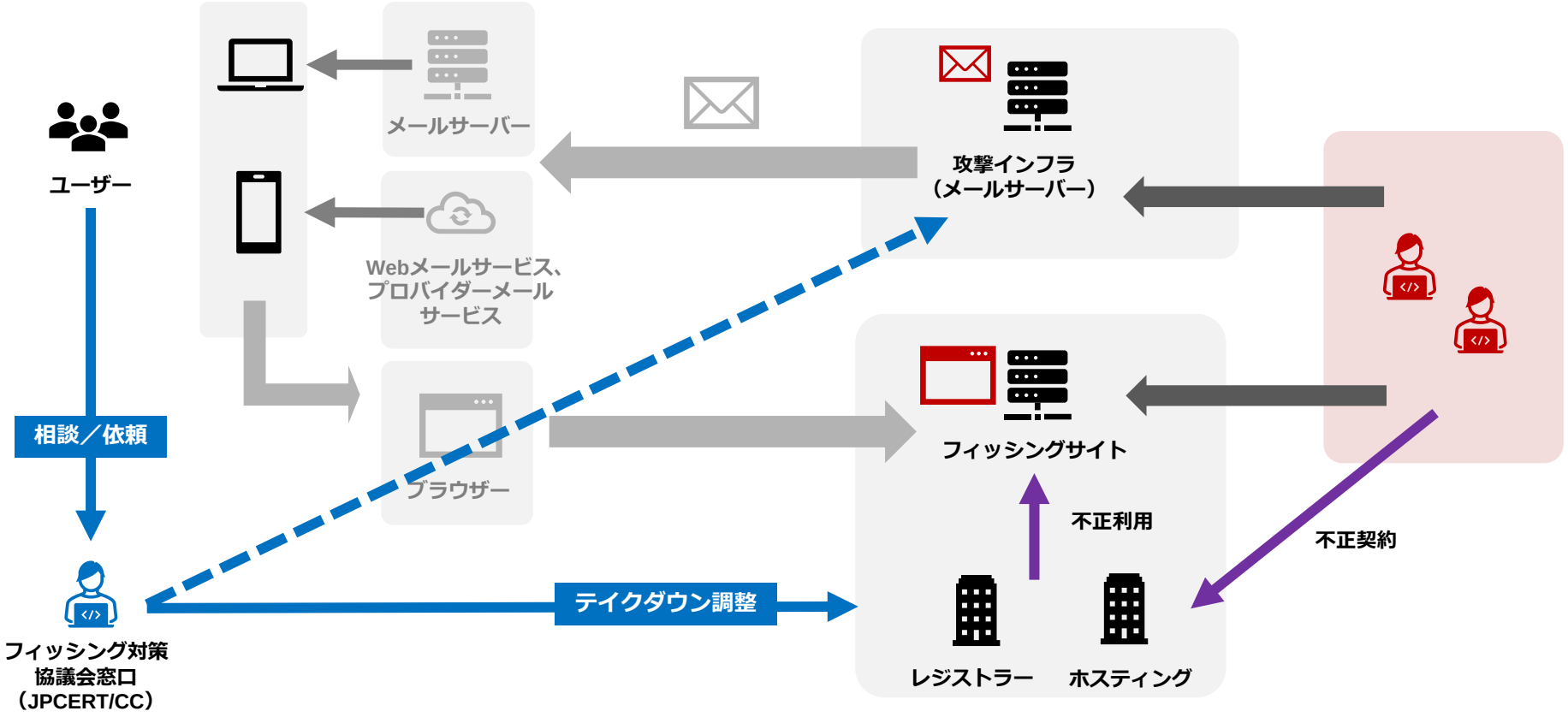
- フィッシング対策協議会が公開する「フィッシング対策ガイドライン」にフィッシング対策の実施も要請対象

https://www.meti.go.jp/press/2022/02/20230201001/20230201001.html

フィッシングサイト対応

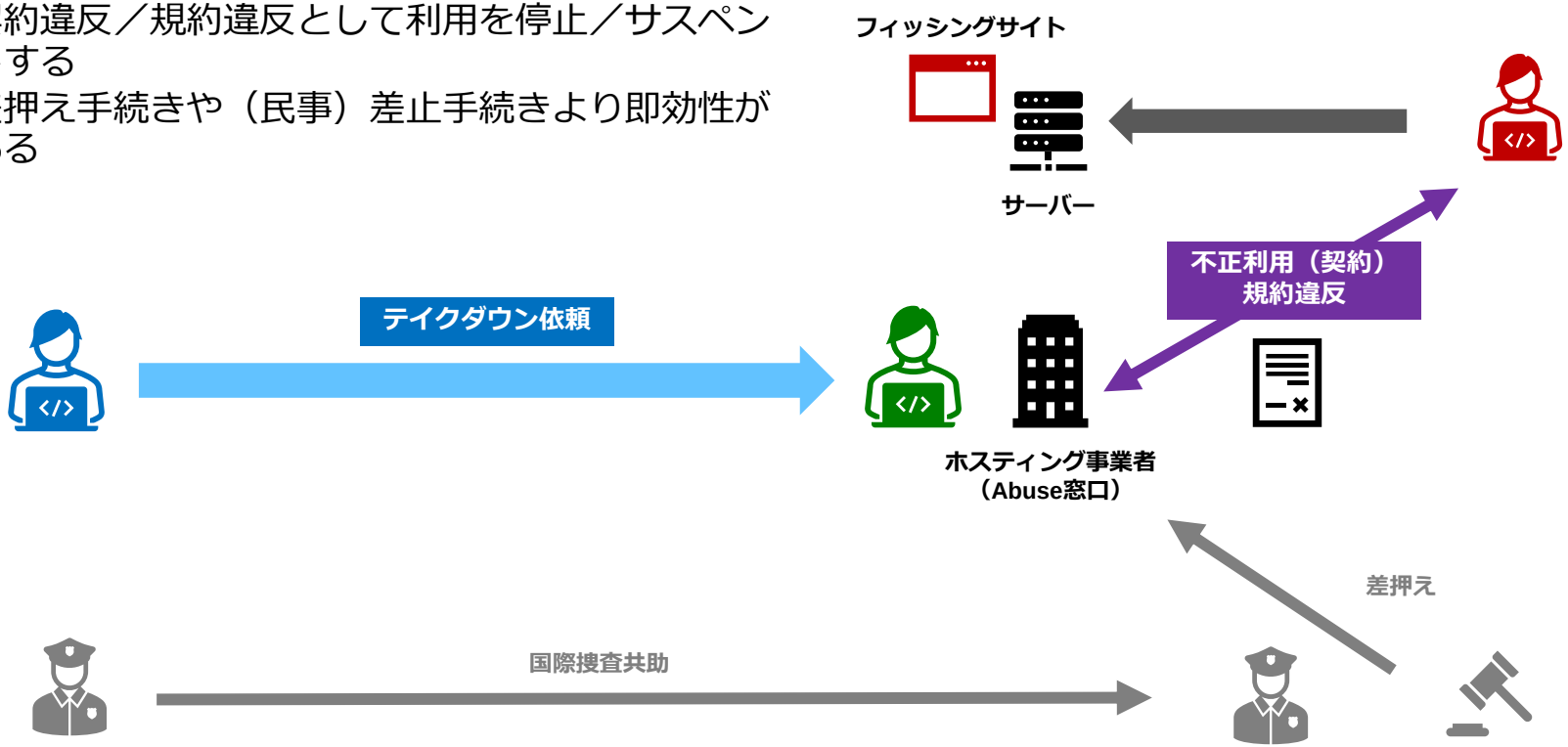
- フィッシングサイトの検知
  - Twitter等のSNSからの情報収集
  - ユーザーからの報告
- フィッシングサイトの閉鎖調整（テイクダウン）
  - ホスティング事業者等へのサイト閉鎖依頼
  - JPCERT/CCや該当事業者（推奨）が実施
- URLフィルタリング
  - フィッシングサイト閉鎖までの利用者保護のため
  - Google Safebrowsing等へのURL登録

対策：テイクダウン

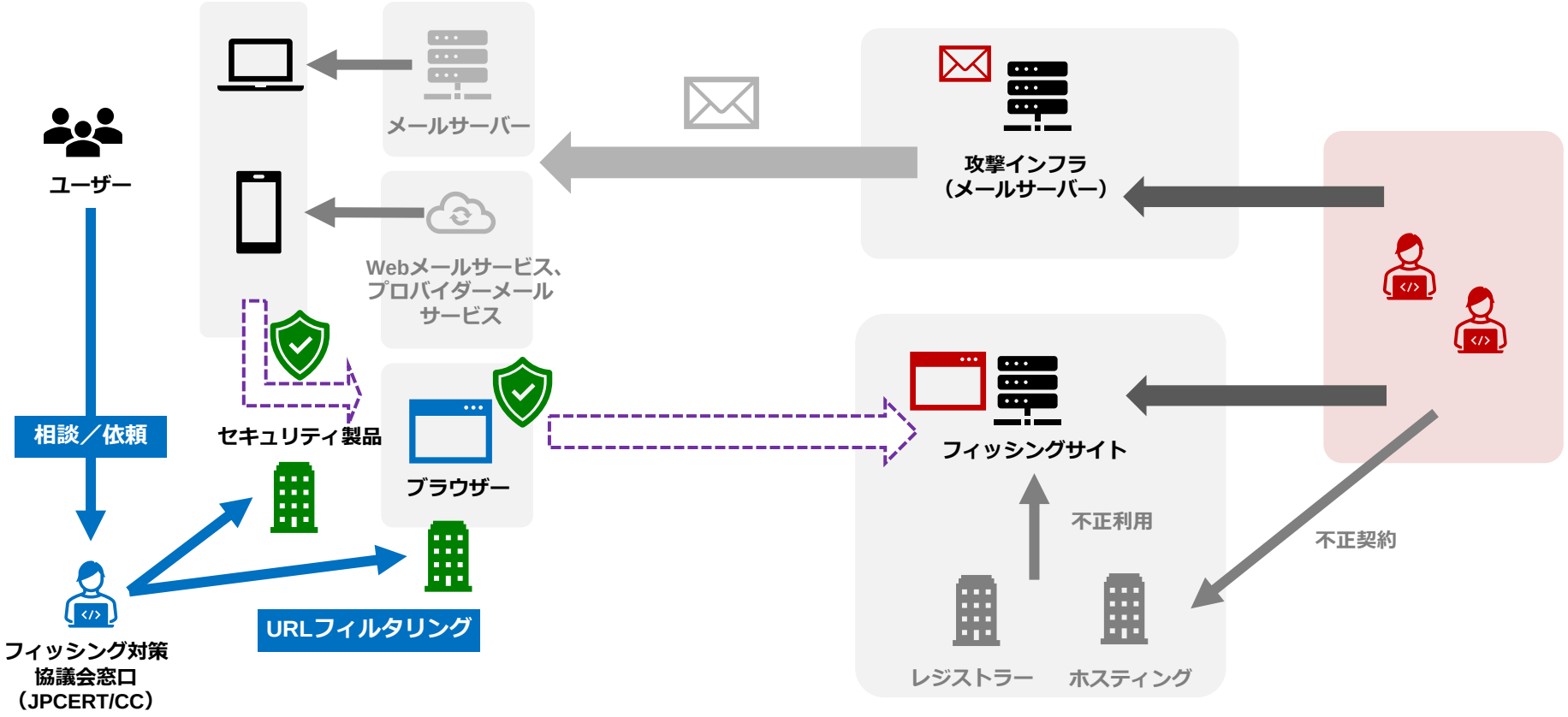


テイクダウンオペレーション

- あくまで任意の依頼
- 契約違反／規約違反として利用を停止／サスペンドする
- 差押え手続きや（民事）差止手続きより即効性がある



対策：フィルタリング



検知サービスの活用

- 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
- 組織内に専門の人員や設備がなくても、迅速な対応が可能
- 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

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守るための基本的なセキュリティ対策と考える
　　送信ドメイン認証、正規メールの視認性向上

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。検知サービスの活用。

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完全に行わない限り、狙われ続けることを認識する（対策をすると減る傾向あり）

自己紹介

一般社団法人JPCERTコーディネーションセンター
エンタープライズサポートグループ　リーダー、シニアアナリスト

吉岡 道明（よしおか みちあき）, CISSP

◆経歴

1993年　システム開発、情報セキュリティ会社 入社
システム開発事業部門にてSE/DBA/PMとして開発プロジェクトに従事
DBセキュリティ対策やDB監視システム開発支援に携わった後、2007年データベースセキュリティ研究所の上級研究員として、セキュリティ事業部門に異動。インシデント対応支援、WAF導入支援などの業務に従事する傍ら、執筆や講演活動も行う。2011年からは、セキュリティコンサルティング部門の部門長。その後、セキュリティコンサルタントとして、インシデント対応支援、情報セキュリティアドバイザー、CSIRT構築支援などに従事

2018年　一般社団法人 JPCERTコーディネーションセンター 着任（現職）
フィッシング対策協議会における、フィッシング報告受付業務、および事務局担当として従事する傍ら、執筆および講演活動を行っている。

◆業界団体での活動

・データベース・セキュリティ・コンソーシアム(DBSC)運営委員

◆講演活動

・Webセキュリティ、フィッシング詐欺に関するセミナー講演
－セキュリティ・ワークショップ in 越後湯沢
－千葉インターネット防犯協会
－フィッシング対策セミナー（フィッシング対策協議会）
－日本クレジット協会
－埼玉県クレジットカード犯罪対策連絡協議会 など多数

◆執筆活動

・専門誌・サイトへの寄稿
ーDBマガジン、gihyo.jp、bizgate など
・『情シス担当者のための絵で見てわかる情報セキュリティ（DB MagazineSELECTION）』(共著)

お問い合わせ、インシデント対応のご依頼は

JPCERTコーディネーションセンター

- Email：pr@jpcert.or.jp
- https://www.jpcert.or.jp/

インシデント報告

- Email：info@jpcert.or.jp
- https://www.jpcert.or.jp/form/

制御システムインシデントの報告

- Email：icsr-ir@jpcert.or.jp
- https://www.jpcert.or.jp/ics/ics-form.html

脆弱性に関するお問い合わせ

- Email：vultures@jpcert.or.jp
- https://jvn.jp/

ご清聴ありがとうございました