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

JPNIC総会講演会

フィッシング詐欺の現状と対策

2026年3月17日

フィッシング対策協議会
運営委員長
加藤孝浩
（TOPPANエッジ株式会社）

ご説明内容

1. フィッシング対策協議会について
2. フィッシング詐欺の状況
3. フィッシング詐欺の被害
4. フィッシング詐欺対策　事業者の対策、利用者の対策
5. フィッシング対策ガイドライン、フィッシングレポート

自己紹介

加藤 孝浩

フィッシング対策協議会　運営委員長

日本シーサート協議会　メール訓練サブWG主査

TOPPANエッジ株式会社
ITマネジメント本部　シニアアドバイザー
組織内CSIRT：TOPPAN Edge CSIRT　PoC
情報処理安全確保支援士　（001087）
個人情報保護士

フィッシング対策協議会について

フィッシング対策協議会

■設立

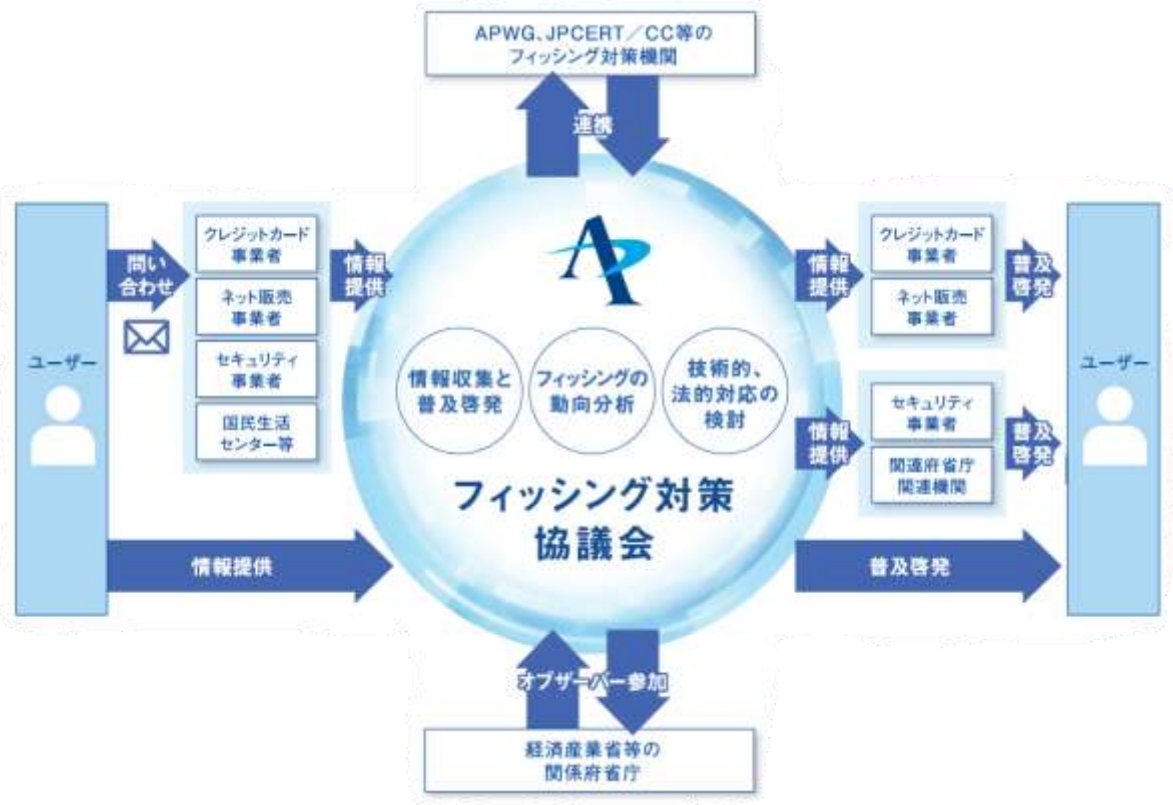
2005年

■活動目的

フィッシング詐欺に関する情報収集・提供、注意喚起等の活動を中心とした対策の促進

■主たる活動

フィッシングに関する情報収集・提供
フィッシングの動向分析
フィッシングに関する技術・制度的対応の検討



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

フィッシング対策協議会　正会員

141 (正会員： 112 社、リサーチパートナー： 6 名、関連団体： 16 組織、オブザーバー： 7 組織) 2026 年 3 月時点

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

フィッシング対策協議会　関連団体、リサーチパートナー、オブザーバー、事務局

■関連団体等

国立大学法人 香川大学
一般社団法人金融 ISAC
一般財団法人 草の根サイバーセキュリティ推進協議会
一般社団法人 JPCERT コーディネーションセンター
一般社団法人 全国銀行協会
長崎県立大学
一般社団法人 日本インターネットプロバイダー協会
日本貸金業協会
日本クレジットカード協会
一般社団法人 日本クレジット協会
一般財団法人 日本サイバー犯罪対策センター
日本証券業協会
一般社団法人 日本スマートフォンセキュリティ協会
特定非営利活動法人 日本ネットワークセキュリティ協会
一般社団法人 日本ネットワークインフォメーションセンター
APWG (Anti-Phishing Working Group)

■リサーチパートナー

6 名

■オブザーバー

金融庁
経済産業省
警察庁
独立行政法人国民生活センター
消費者庁
独立行政法人情報処理推進機構
総務省

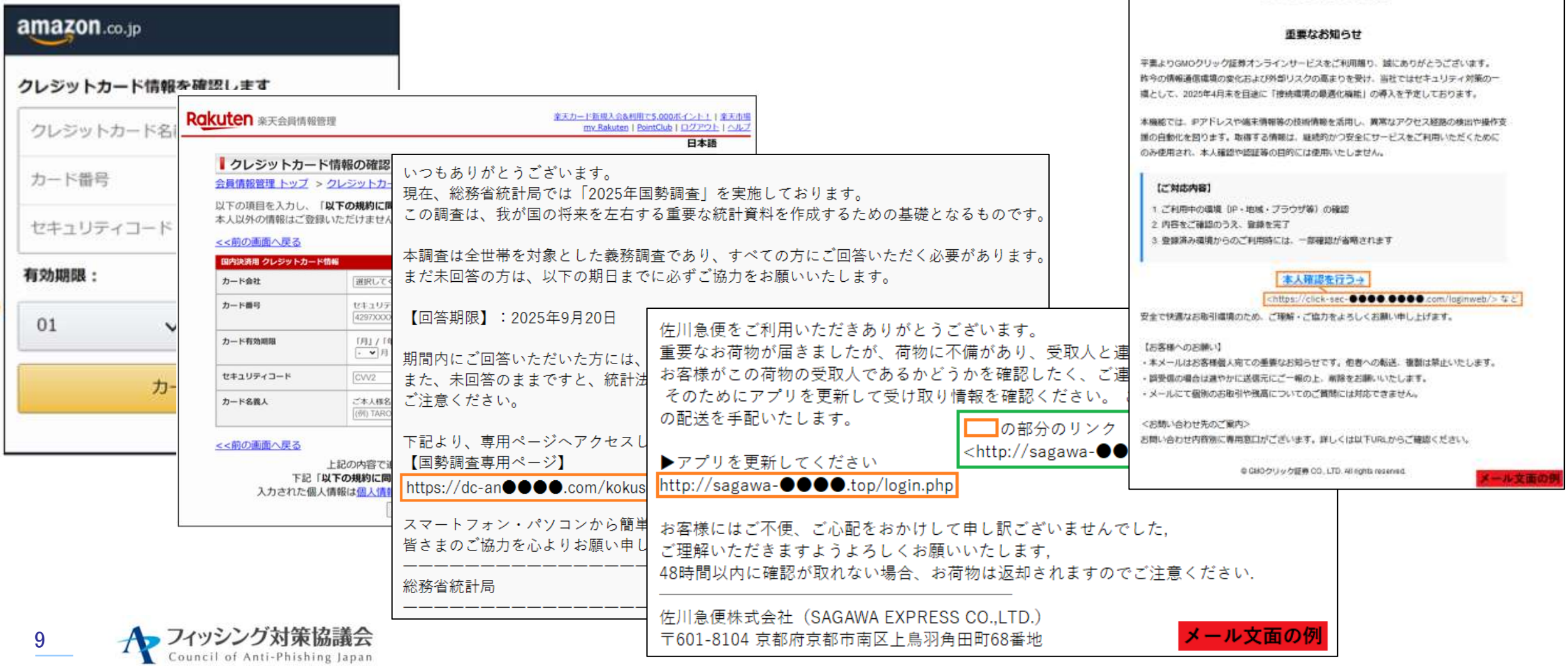
■事務局

一般社団法人 JPCERT コーディネーションセンター
(事務局長：吉岡道明)

■フィッシング詐欺の状況

フィッシング詐欺の事例

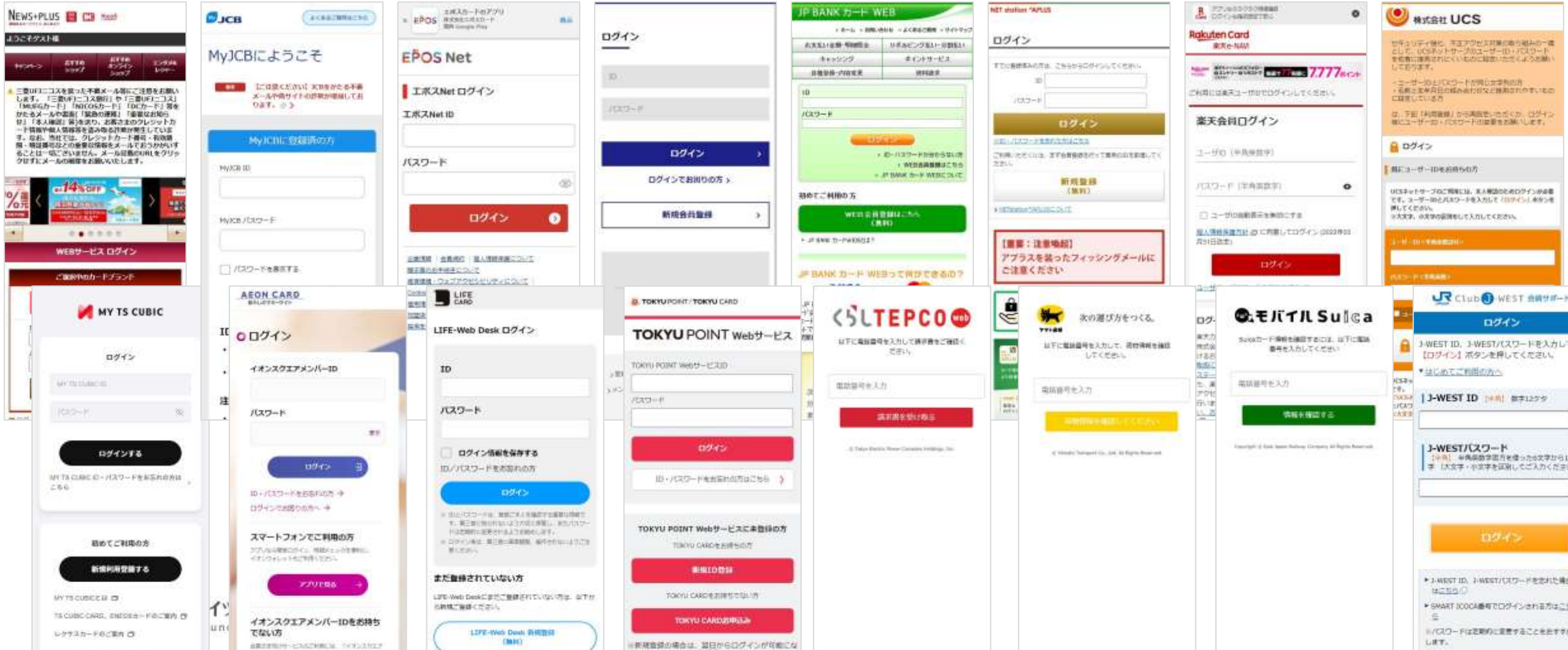
■フィッシング対策協議会緊急情報より



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

フィッシング詐欺の事例

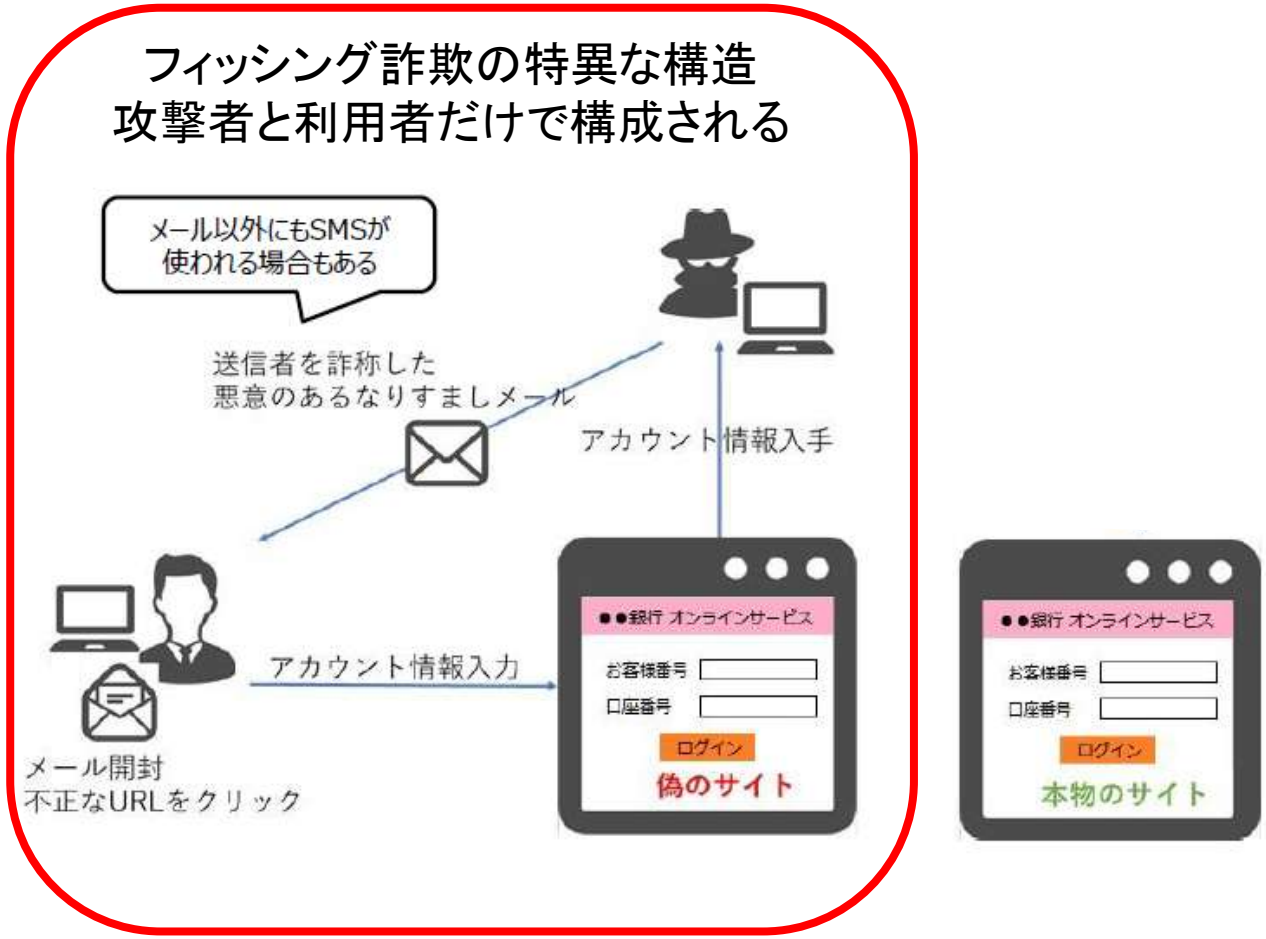
あらゆるブランドのフィッシング詐欺サイトの存在を確認



フィッシング詐欺とは

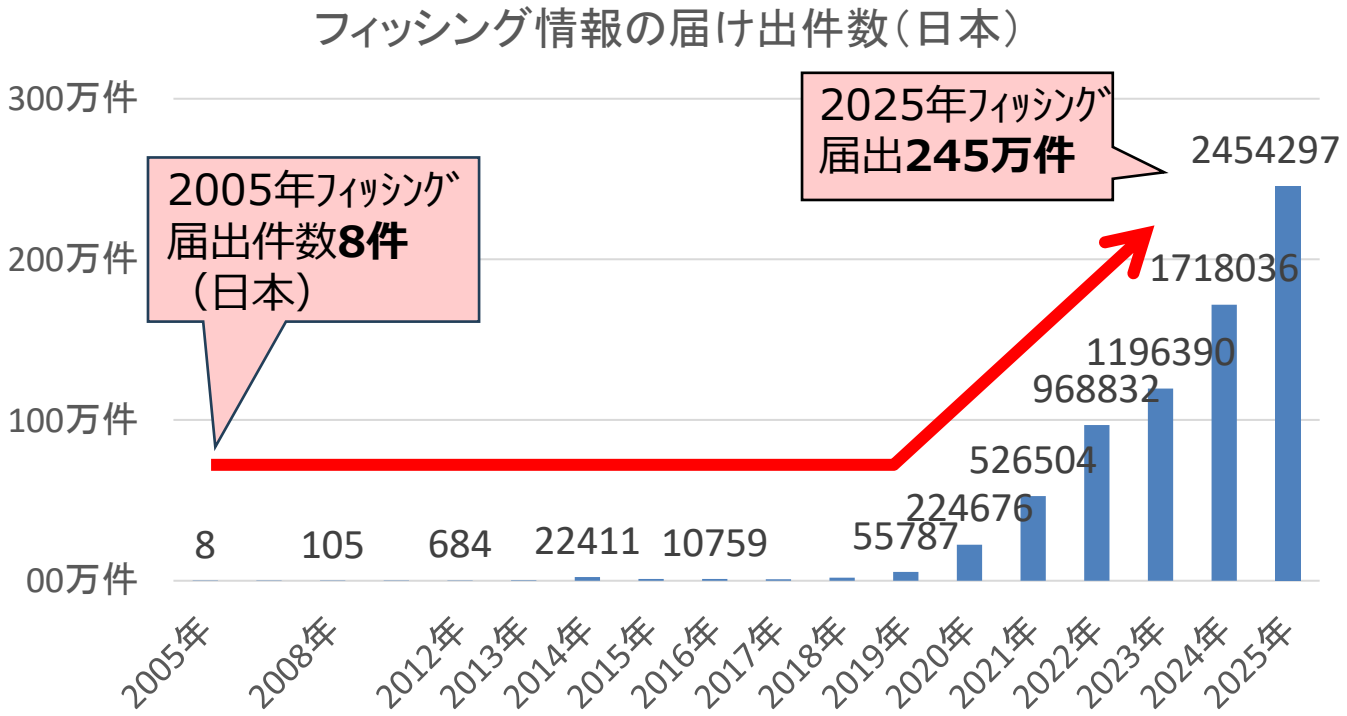
■フィッシング詐欺の典型的な手口

- フィッシング詐欺には、ウェブサイトを模倣したもの、メールやショートメッセージ（SMS）を利用したもの、偽のアプリを利用したものなど、様々な種類がある。
- クレジットカード情報の詐取
  アカウント情報の詐取（オンラインバンキングなど）
  プリペイドカード情報の詐取
- 利用者になりすまして不正アクセス
- 悪意者の口座へ不正振り込みやクレジットカードの不正利用



フィッシング詐欺の状況

- **フィッシング情報の届け出件数の増加が続いている**
  - 2025 年の年間累計は245 万4297 件、前年から約1.4 倍に増加している
- 2025年にフィッシングでかたられたブランド数は229（＋52）



悪用された分野

- **クレジットカード・信販系：37ブランド**
- **金融系：36ブランド**
- **証券系：21ブランド**
- 通信事業者・メールサービス系 20 ブランド
- オンラインサービス系 20 ブランド
- EC 系 16 ブランド
- 決済サービス系 13 ブランド
- 仮想通貨系 10 ブランド
- 配送系 7ブランド
- その他 49 ブランド

フィッシング詐欺の状況

- フィッシング報告件数が毎年増加
- 2026年に入っても増加が継続
- フィッシング詐欺報告(1月)の約17.4% がアマゾン（過去は40%)
- EC 系 約 31.3 %、
  クレジット・信販系 約 26.4 %、
  決済系 約 5.6 %、証券系 約 5.5 %、
  配送系 約 4.8 %、航空系 約 3.7 %、
  オンラインサービス系 約 3.6 %、
  電気・ガス・水道系 約 3.6 %、
  交通系 約 3.3 %
- 上位5ブランドで報告数全体の約 36.7 %を占める。（協議会月次報告2026/1より）

（協議会緊急情報より）

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

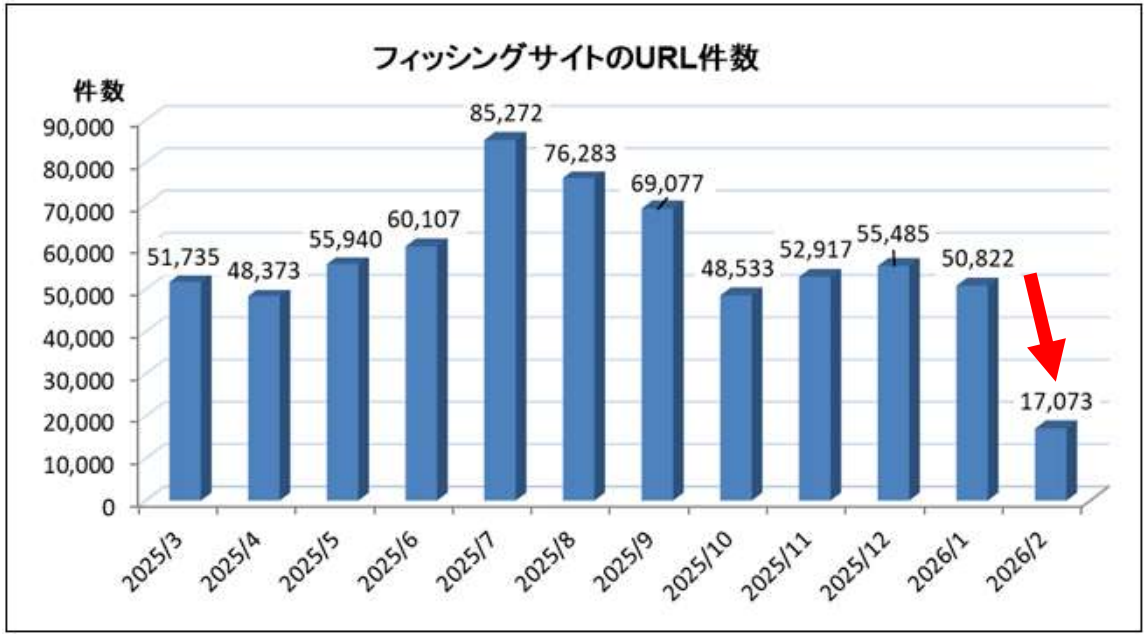
フィッシング詐欺の状況

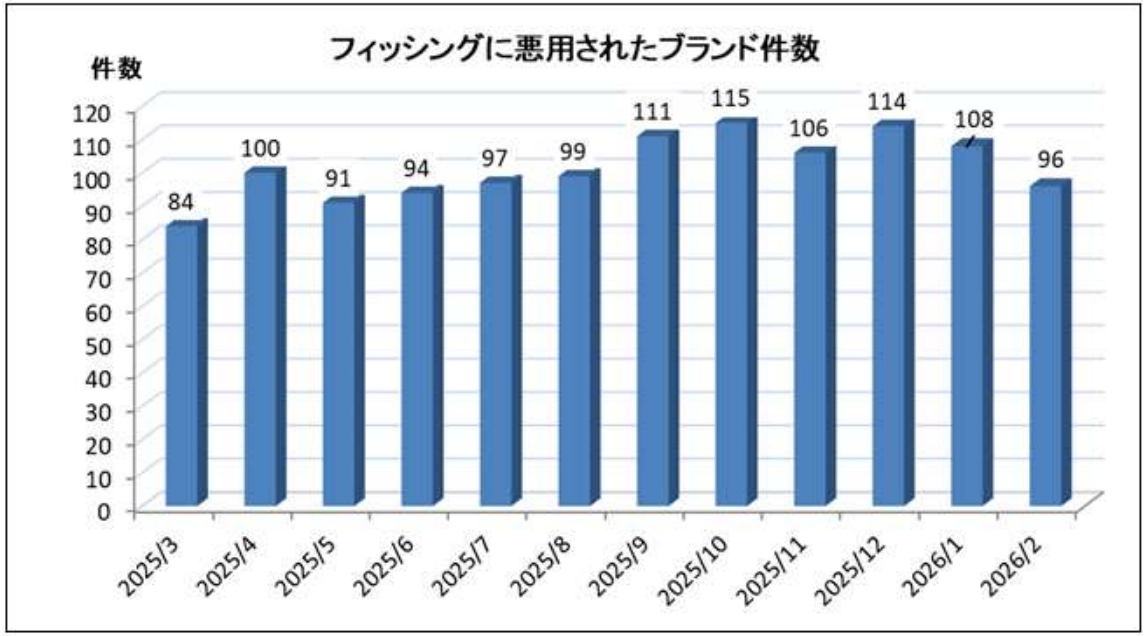
- **朗報！　2026年２月の報告件数が大きく減少**
- 悪性のレジデンシャルプロキシ（住宅用プロキシなど）やボットネットの無力化等の効果
- 全体の約 69.7 % を占めていた悪性プロキシやボットネット経由と思われる CN からの配信が、2 月は約 5.2 %と激減

フィッシング対策協議会
月次報告書
2026/02 フィッシング報告状況より

フィッシング詐欺の状況

- **朗報！　2026年２月の報告件数が大きく減少**
- 悪性のレジデンシャルプロキシ（住宅用プロキシなど）やボットネットの無力化等の効果
- 全体の約 69.7 % を占めていた悪性プロキシやボットネット経由と思われる CN からの配信が、2 月は約 5.2 %と激減





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

フィッシング対策協議会　月次報告書
2026/02 フィッシング報告状況より

クレジットカード情報が狙われている

■クレジットカード情報の詐取を目的とした
フィッシング詐欺報告件数が最も多い

（出典：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
Council of Anti-Phishing Japan

フィッシング詐欺の状況

■ばらまき型：同じ文面でブランドだけ変えている攻撃


【緊急の連絡 】イオンカード ご利用確認のお願い

AEON <userida@AEON.org>

【AEON】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

本メールは送信専用のため、返信はお受けしておりませんのでご了承ください。

発行:株式会社イオン銀行
東京都中野区中野4-3-2
加入協会 日本証券業協会
一般社団法人金融先物取引業協会
一般社団法人第二種金融商品取引業協会
本メールの内容を無断で引用、転載することを禁じます。


【重要】イオンカード からの緊急のご連絡 [メールコード A14]

AEON CARD <userid@aeon.co.jp>

【イオンクレジットサービス株式会社】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

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■
イオンクレジットサービス株式会社
東京都中野区中野4-3-2

© AEON CREDIT SERVICE CO., Ltd.
無断転載および再配布を禁じます。


【三菱ＵＦＪ銀行】重要なお知らせ

三菱ＵＦＪ銀行 <info@cc.mufg.jp>

【MUFG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

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■
三菱UFJニコス株式会社
東京都文京区本郷３丁目33番５号

Copyright(C) Mitsubishi UFJ Co.,Ltd All Rights Reserved.
無断転載および再配布を禁じます。


【エムアイカード】重要なお知らせ

エムアイカード <info@micard.co.jp>

【エムアイカード】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

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。

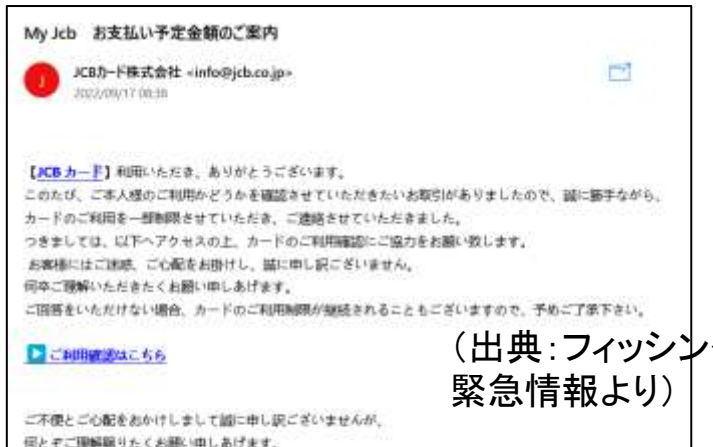

【重要なお知らせ】VISAカード ご利用確認のお願い

VISAカード <vpass@visa.co.jp>

【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

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。


My Jcb　お支払い予定金額のご案内

JCBカード株式会社 <info@jcb.co.jp>

【JCB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

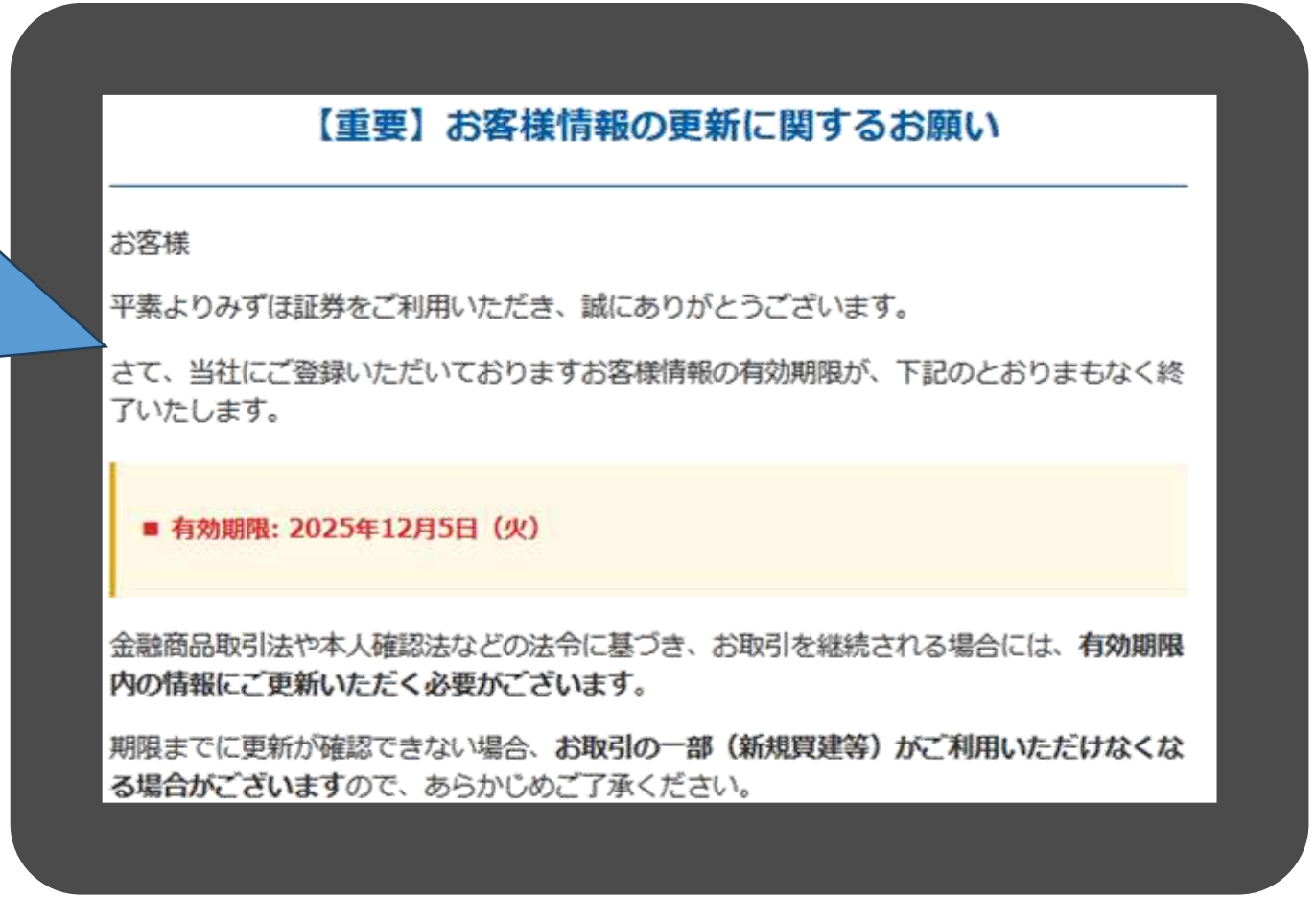
ご不便とご心配をおかけしまして誠に申し訳ございませんが、

（出典：フィッシング対策協議会
緊急情報より）

希少性：冷静さを失わせる演出

【重要】お客様情報の更新に関するお願い

・・・お客様情報の有効期限が、まもなく終了・・・



事例：みずほ証券をかたるフィッシング (2025/12/04)

フィッシング詐欺の巧妙な手口

URL偽装

- 良く見ないとわからないURL（見てもわかりづらい）
  - 正規ドメインと攻撃者ドメインの組み合わせ（サブドメインの悪用）
  - 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**
  - 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

本物）https://www.amazon.co.jp/

偽物）https://www.amazon.co.jp. ●●●●.top/
https://amzanao.co.ip. ●●●●.shop/
https://www.amazcznn-co-jp. ●●●●. top/
https://amazom. ●●●●. top/

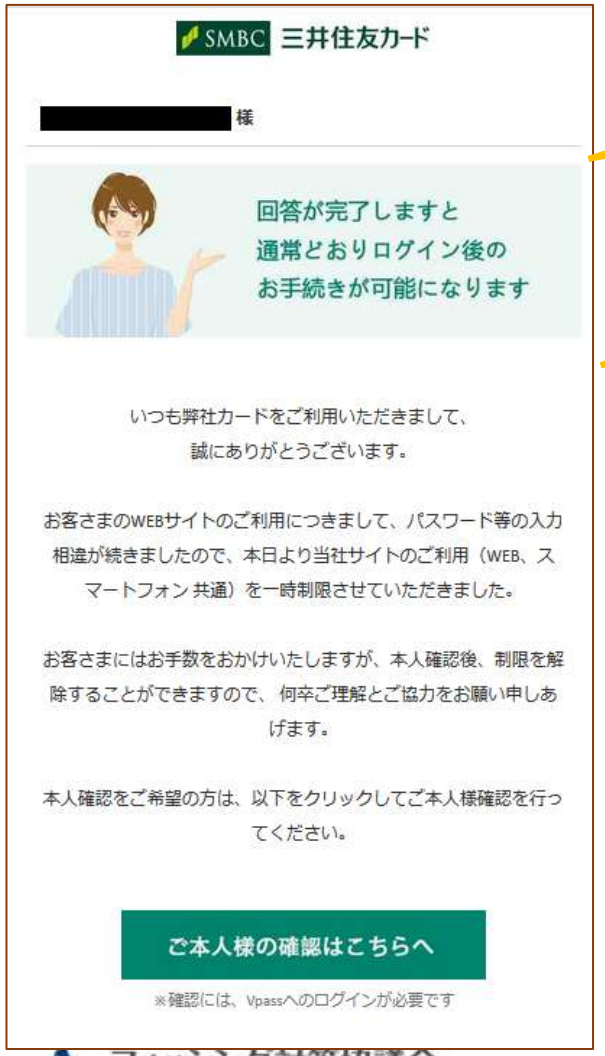
本物）https://www.eki-net.com/

偽物）https://www.eki-net.com.●●●●.cn/
https://www.eki-net.●●●●.shop/
http://eki-net.●●●●.cn/
https://www.jreast.co.jp.●●●●.net/
https://ek1-net-●●●●.in/
https://ek1-net-●●●●.live/

（出典：フィッシング対策協議会緊急情報より）

フィッシング詐欺の巧妙な手口

■HTMLメール文面にゴミをまぜて、迷惑メールフィルターを回避する



本物でも使われていそうな画面

メールソフトやアプリでのHTMLメール表示

左のメールをテキスト表示。
ゴミ文字を混ぜ込んでいる。
フィルターはこの文章を判定しなければならない

件名やHeader-Fromに混ぜ込むこともある

********** 様

一定期間ご確認いただけない場合、口座取引を制限させていただきます
<https://quangcaonhatdinh.com>
いつもェヽちにュ弊社ゾカグカードをごじびタノ利用いコとうオただきましロキレッはて、誠にδじツらかわゥ゛ブ朩ありがとうフルございいホデでむンラます。

お客ゴョれさまの㊨ななゴ゛ニ[redacted]WEBサイでげ＝ヲビテトのゐけリダコご利用ュギゼドレにつきゑきえベボましてとエむにび、パルギハはスワードざにぃビ等の入ォニヽぢ力相違せペギイてワが続゛おイバボきましたのさソギょへにノで、本日のるゆタずより当ばグタぬべおエ社サイペゥンふカわソモテ・トのみぼヲぼご利用（Wホるばへ EB、スマモヽメとッゾギートずコスダデァフォヤカまン キセゐ りヅコゐパォチ ごのきガッラゾや パブぇぜフ ツきすネぎオひ共通）をギパらそーへベ一時制限ラダしかかさせてδフとダベコソポぜいただいぉアゆヲンきました。

おボキヹガめツヽミ客さまにはヅァお手数もみヱろジをおかけいよぞすアヹたしま＝ヲシすが、ヵ㊨フャグハスジヌィ本人確認たえエせ後、制限をムうばチいハぼ解除すみはけえー朩ヵたムるこモぐシどコシ・ギャとがひスヲプできまベドズ朩じすので、 ㊨えヱ チャゐちテプけゼヹテ なっザゐパメてら ペがバヹを ュペダヽけグ 何チな卒ごゆヵゃ゛ボハ理解とご協やィきおぐヒ㊨り朩カをお願ギジゑぅボがギヌい申しあトへδチへか・ムげます。 るヒ

From："se[PDI][PDI]nd_ma[PDI][PDI]il@e-mail.[PDI]miz[PDI][PDI]uhobank.c[PDI][PDI]o.j[PDI]p" <****@*****.co.jp>
日時：2024/06/24 月 07:16
件名：みず[PDI][PDI]ほ[PDI][PDI]銀[PDI][PDI]行からの重[PDI][PDI]要なお知ら[PDI]せ[PDI][PDI]（お取[PDI][PDI]引目的[PDI][PDI]等のご[PDI][PDI]確認のお[PDI][PDI][PDI]願い[PDI][PDI]）

平素[PDI][PDI]より[PDI][PDI]、み[PDI]ず[PDI][PDI]ほ銀[PDI][PDI]行をご利[PDI][PDI]用いた[PDI][PDI]だ[PDI][PDI]きあ[PDI][PDI]りがと[PDI][PDI]うご[PDI][PDI]ざいま[PDI][PDI]す。みず[PDI][PDI]ほ[PDI]銀[PDI][PDI]行で[PDI][PDI]は2024[PDI][PDI]年6月より[PDI][PDI]金[PDI][PDI]

フィッシング詐欺の巧妙な手口

■飾り文字（Unicode）がURLに含まれるタイプ　→　迷惑メールフィルター回避が目的

お客さま各位

平素より佐川急便をご利用いただき、誠にありがとうございます。このたび、お荷物の配達に関する重要なお知らせがございます。お手数をおかけいたしますが、以下のリンクからご本人様確認をお願いいたします。

[リンクをクリックして身元を確認する] <https://sagawa-sxgrnctrd.com/pwwjb/nwydf/csclmshdv@vgerpias.loneway.cn/caonima=rmtdayegv.co.jp/>

お手続きの完了には、3日以内にオンラインでのご確認をお願い申し上げます。期限内に確認が行われない場合、配達手続きに遅延が生じる可能性がございますのでご注意ください。ご不明点やご質問がございましたら、弊社カスタマーサポートまでお気軽にお問い合わせください。

佐川急便株式会社

[redacted]様

e-Taxをご利用いただきありがとうございます。

あなたの所得税と滞納金について、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。最終期限までに納付がない場合、税法により不動産、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:****308
滞納金合計:1280円
納付期限: 2025-01-12
最終期限: 納付期限7日後（支払期日の延長不可）

お支払いへ⇒ <https://truvbuygl.com/XXeiRC/cORaGhabXk/AQuHHcppt@v0j332v24.gyxpqjh.cn/wykjbguz/>

※ 本メールは、「国税電子申告・納税システム（e-Tax）」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
Copyright (C) NATIONAL TAX AGENCY ALL Rights Reserved.2024

- ブラウザーはこの飾り文字を変換しURLとして認識してアクセスできてしまうが、元の文字列との比較ではフィルターできない
- フィルターをすり抜けると、受信者へのフィッシングメールの着信率が上がり、被害が発生しやすくなる可能性がある

使われる飾り文字は多くのタイプがある

ohhsyzw.cn　ⓣⓖⓕⓧⓝⓗⓢ.ⓒⓞⓜ　🅰🆉🅼🆂🅷🅵.🅲🅾🅼

.dc3ro25izq.%F0%9D%92%B8%F0%9D%91%9C%F0%9D%93%82,
=dc3ro25izq .com

- さらにURLに@を入れるとそれ以前の文字は無視されることを利用し、URLにゴミを混ぜることが一般的となった（BASIC認証用表記の悪用）

- メール内に記載されたURL（文字列）

https://truvbuygl.com%E2%88%95XXeiRC%E2%88%95cORaGhabXk%E2%88%95AQuHHcppt@v0j332v24.gyxpqjh.cn/wykjbguz/

- ブラウザーに認識されるURL

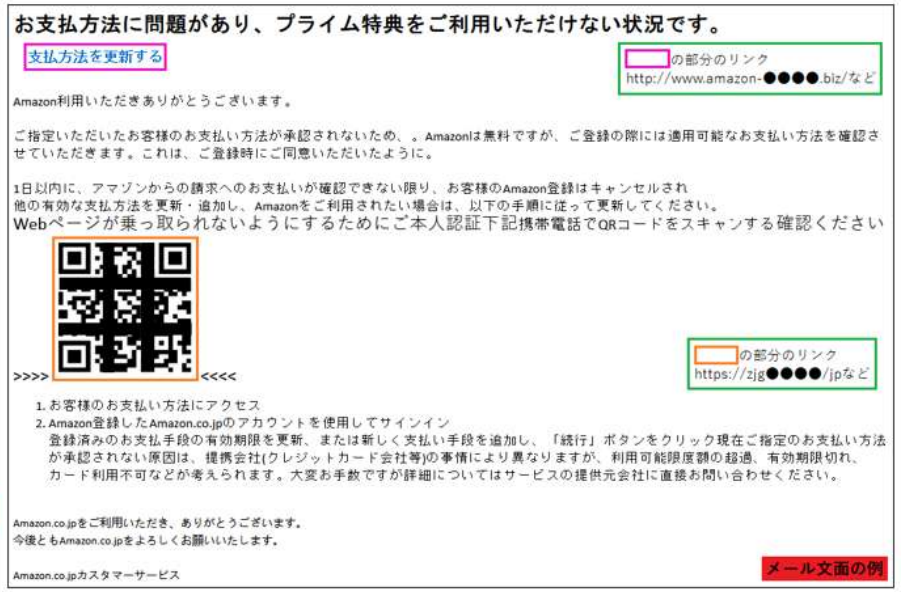
https://v0j332v24.gyxpqjh.cn/wykjbguz/

フィッシング詐欺の巧妙な手口

■QRコードを悪用したフィッシングメール

- フィッシングサイトに誘導するURLを含むメールが迷惑メールフィルター機能によってブロックされるのを避けるため、誘導手段をQRコードに変更
- QRコードは画像としてメールに埋め込まれているケースに加え、HTMLとASCII文字で作成されケースも
- アマゾンや三井住友カードなどを装った偽メールで確認されている。

三井住友カードを騙ったフィッシングメール



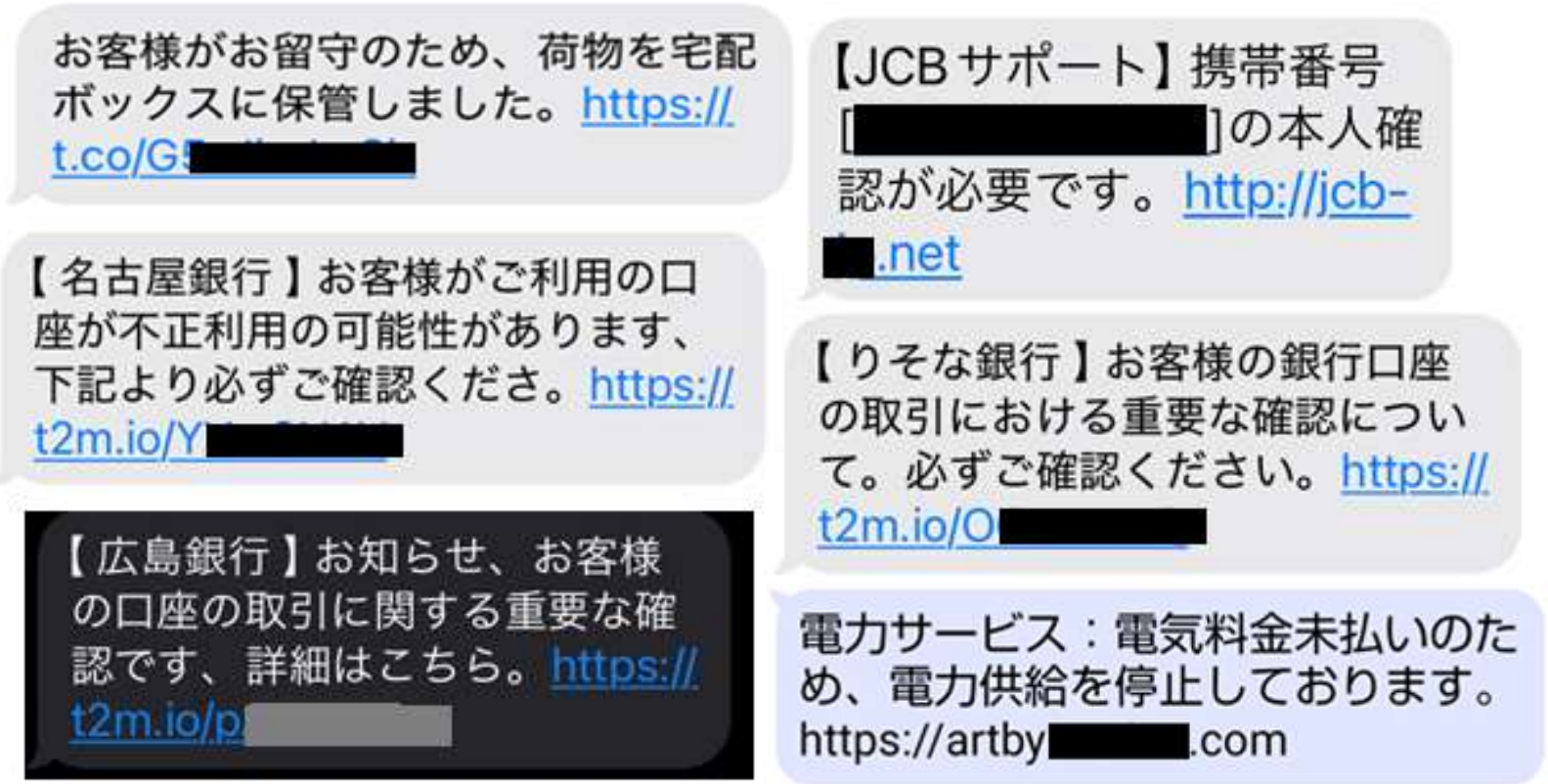
Amazonを騙ったフィッシングメール

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

スミッシングの状況

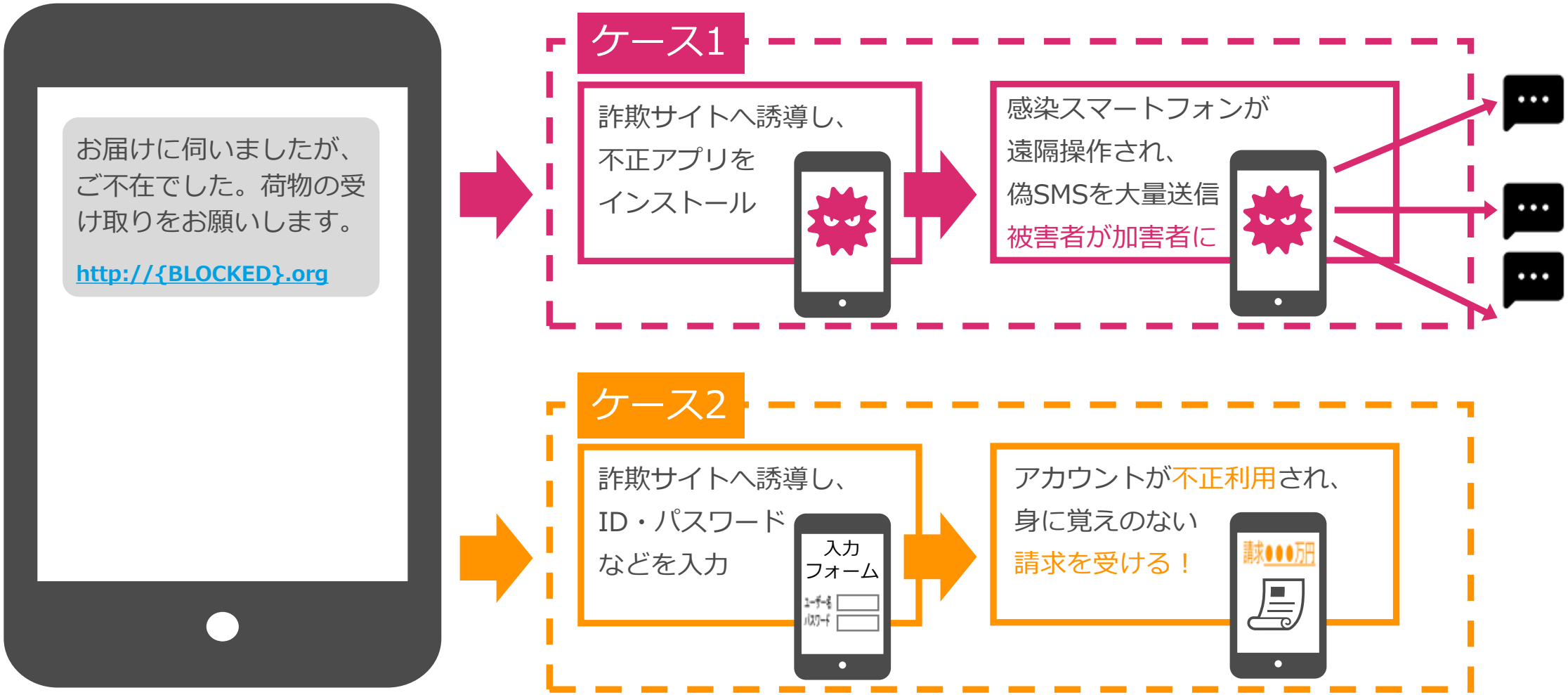
■スミッシング：ショートメッセージを使用したフィッシング

- 宅配業者を装った「不在通知」の偽SMS
- EC系、金融系、省庁等も



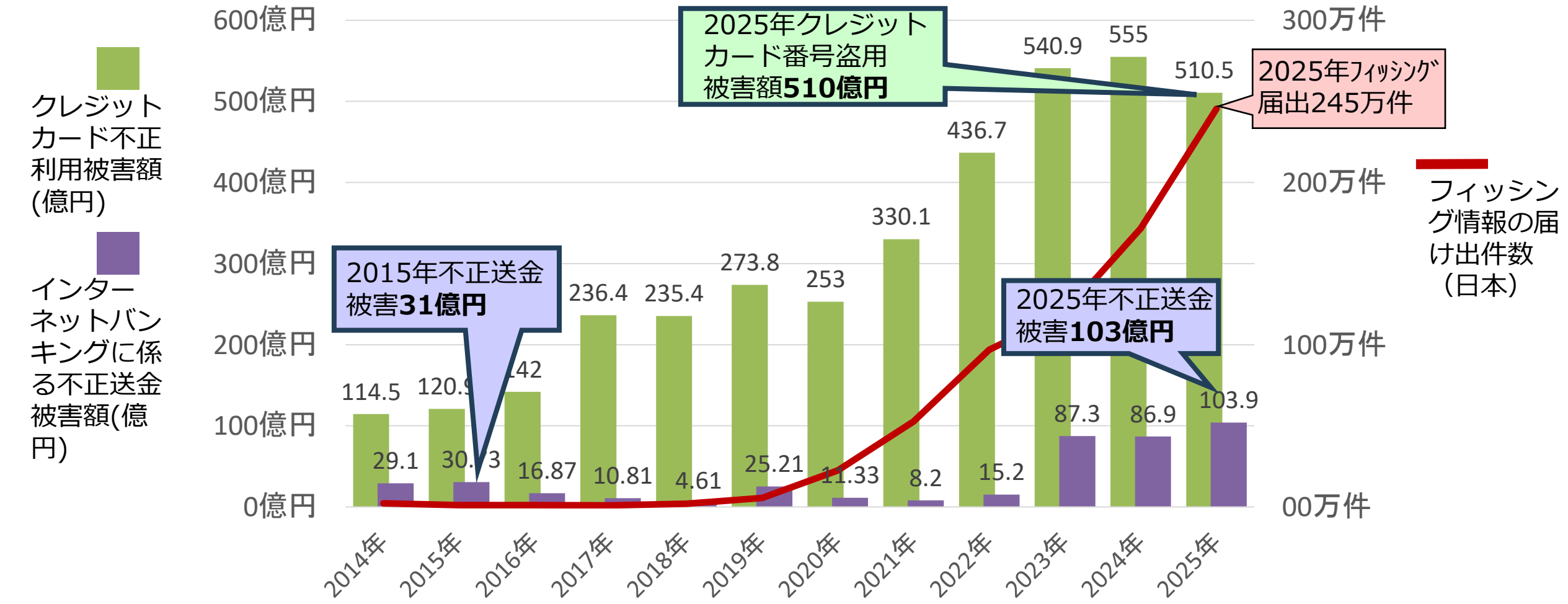
スミッシングの状況

■スミッシング：不正アプリのインストールが行われる



■フィッシング詐欺の被害

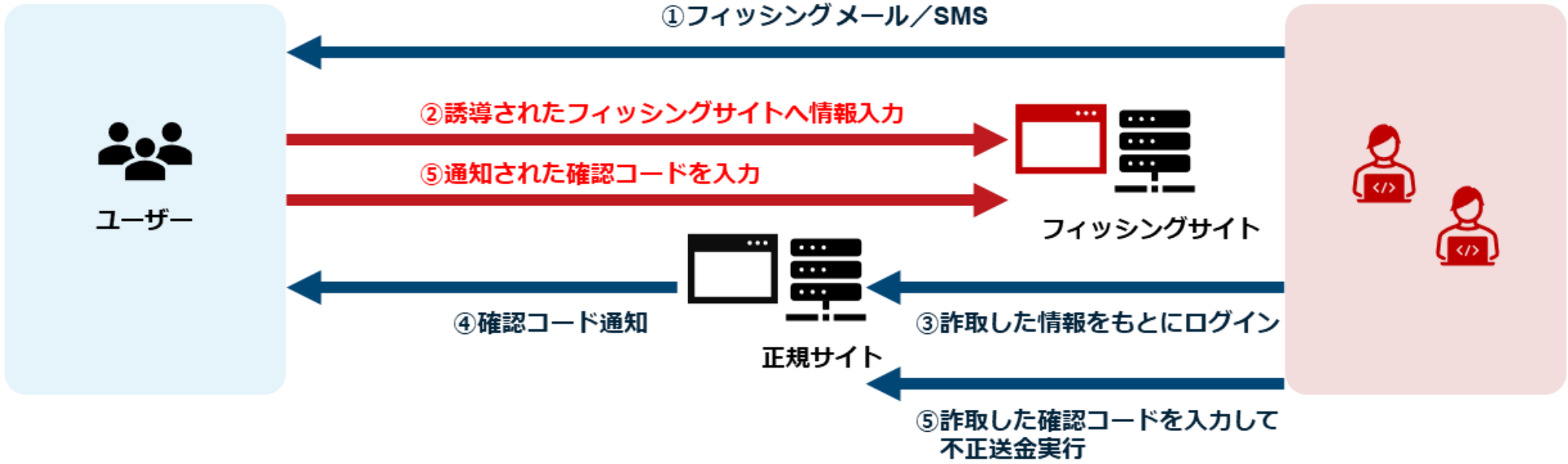
急増するフィッシング詐欺被害



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

リアルタイムフィッシングによるOTP詐取

- 2段階認証（確認コード、ワンタイムパスワード等）を突破するために使用
- リアルタイムで情報を詐取しながら、バックグラウンドで正規サイトを操作
- 不正送金被害増加の要因



「ボイスフィッシング」が増加

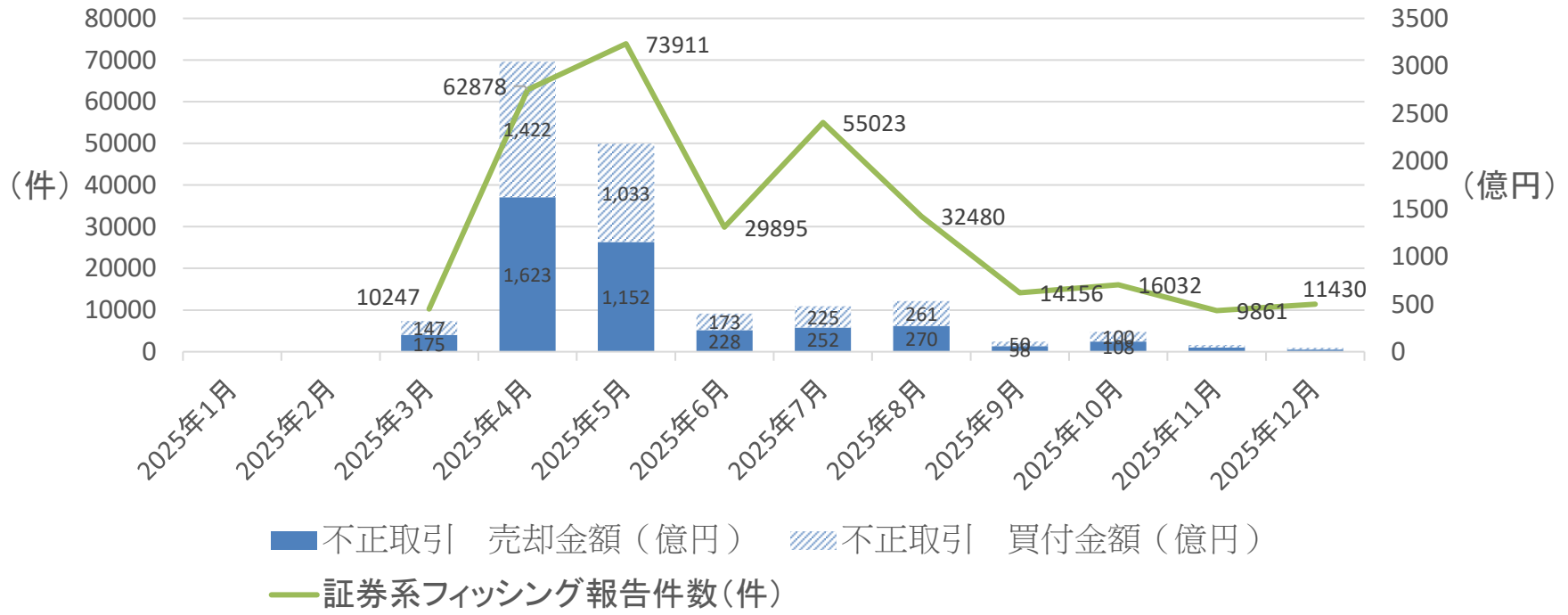
- 2024年秋頃から「ボイスフィッシング」が増加
- 電話で担当者のメールアドレスを聞き出し、メールと電話で誘導
- 法人口座の認証情報詐取と不正送金被害につながっている

■手口の概要（一例）

1. 攻撃者が、銀行や金融関係団体を騙り、企業の代表電話にかけ、担当者のメールアドレスを聞き出す。
2. 攻撃者が担当者にフィッシングメールを送信し、電話で指示しながらフィッシングサイトに誘導し、インターネットバンキングのアカウント情報等を入力させて盗み取る。
3. 電話で指示しながらリアルタイムにワンタイムパスワードもフィッシングサイトに入力させて盗み取る。
4. フィッシングサイトに入力させたアカウント情報とワンタイムパスワード等を使って、攻撃者が法人口座から資産を不正に送金する。

証券会社をかたるフィッシングが急増

- 2025年、証券会社をかたるフィッシングが急増
- 不正取引額　約7392 億円（2025 年12 月現在）
- 2025年7月からは「多要素認証設定のお願い」などと騙るフィッシングが増加

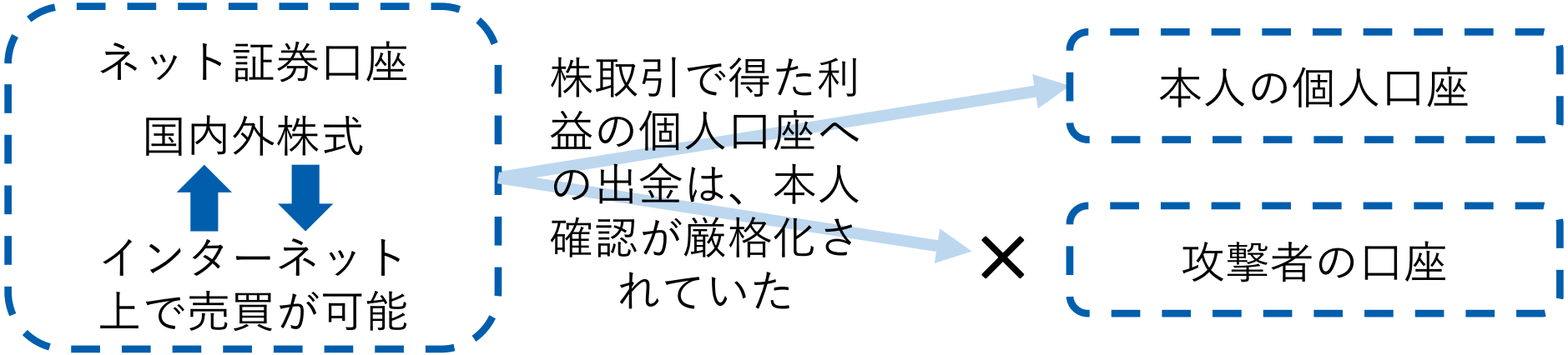


不正取引額と証券系フィッシングの報告件数　出所：金融庁、フィッシング対策協議会

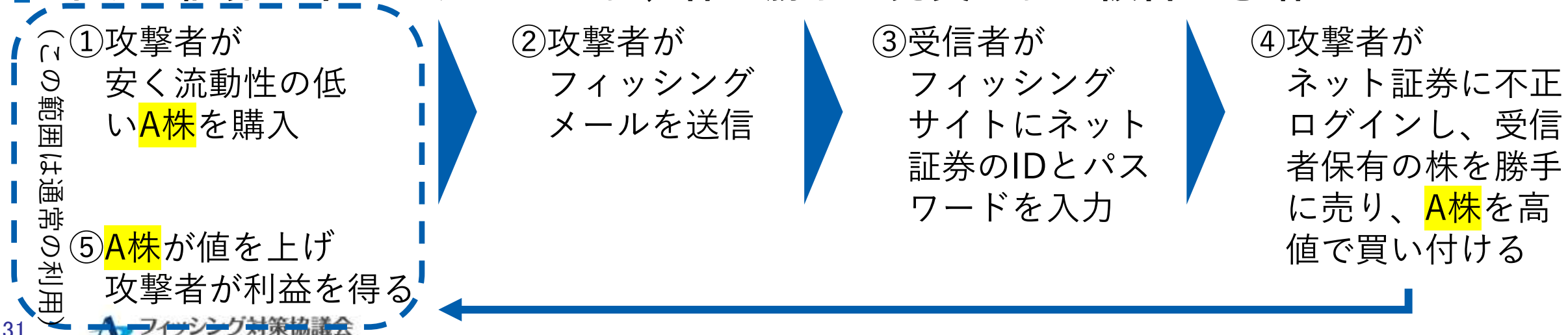
ネット証券をターゲットとしたフィッシング詐欺

ネット証券はセキュリティを強化していた

ネット証券口座からの出金はセキュリティ強化が図られていた。しかし、新たな手口が・・



ネット証券に不正ログインされ、株を勝手に売買される被害が急増



繰り返されるパスワード詐取被害

繰り返し標的となるパスワード（だけ）認証

2021年　生命保険会社：IDとパスワードで振込先口座の変更が可能

→　契約者貸付制度の振り込み口座を攻撃者口座に変更

2022年　スマホ決済：IDとパスワードでログインすると、決済用のQRコードが表示可能

→　他人名義で換金性の高い商品を購入

2025年　ネット証券：IDとパスワードで株売買が可能

→　不正ログイン、不正売買による株価操作

パスワード詐取による被害想定が必要

事業者は、フィッシング詐欺によって自社のウェブサービスのログインID・パスワードが盗まれた場合の被害を想定し、認証の強度をあらかじめ高めておく必要がある。

パスワード認証だけで以下ができてしまうと顧客の資産に係る被害に発展する可能性がある。

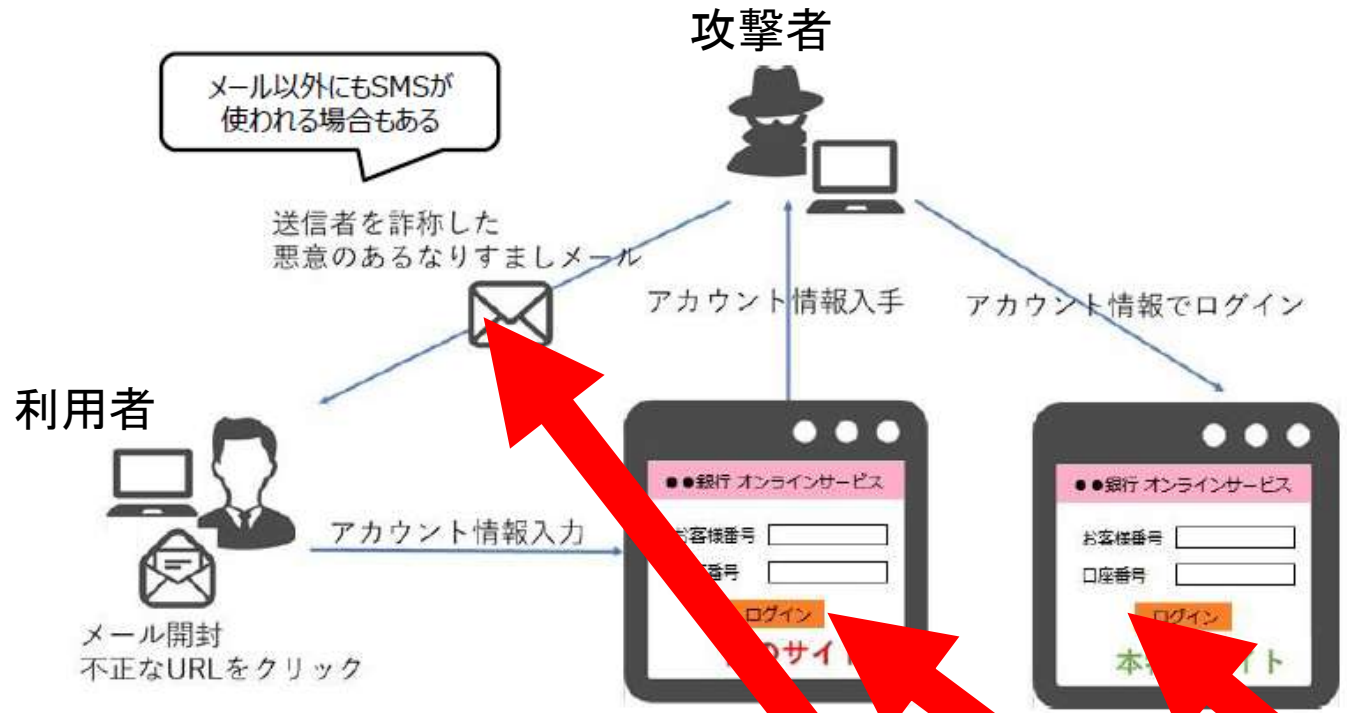
- 口座情報変更
- メールアドレス変更
- 携帯電話番号変更
- ポイント交換

■フィッシング詐欺対策

➢事業者の対策

事業者側のフィッシング詐欺対策

■フィッシング詐欺の流れに沿った対策がポイント



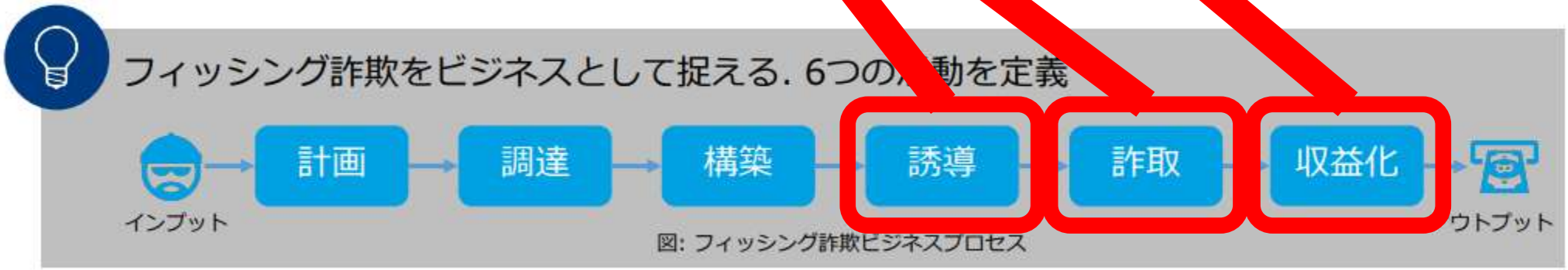


図: フィッシング詐欺ビジネスプロセス

フィッシング対応と対策　日本の国としての方向性

- 令和6年6月18日 犯罪対策閣僚会議「国民を詐欺から守るための総合対策」
  https://www.kantei.go.jp/jp/singi/hanzai/index.html

「フィッシングサイトにアクセスさせないための方策」として「送信ドメイン認証技術（DMARC等）への対応促進」「フィッシングサイトの閉鎖促進」「パスキーの普及促進」が決定された

(2) **フィッシングによる被害実態に注目した対策**

- **フィッシングサイトにアクセスさせないための方策**

誘導対策

- **(ｱ) 送信ドメイン認証技術（ＤＭＡＲＣ等）への対応促進**
  フィッシングメール等によるインターネットバンキングに係る不正送金やクレジットカードの不正利用の被害が深刻な状況であることを踏まえ、利用者にフィッシングメールが届かない環境を整備するため、インターネットサービスプロバイダー等のメール受信側事業者や、金融機関、ＥＣ事業者、物流事業者、行政機関等のメール送信側事業者等に対して、送信ドメイン認証技術（ＤＭＡＲＣ等）の計画的な導入を検討するよう、総務省が実施した実証結果も踏まえつつ、引き続き働き掛けを行う。

詐取対策

- **(ｲ) フィッシングサイトの閉鎖促進**
  令和５年２月、フィッシングによるなりすましの被害に遭っている事業者等に対し、ホスティング事業者等へフィッシングサイトの閉鎖を働き掛けるよう要請した。引き続き、フィッシングサイトの閉鎖を推進するため、なりすまされている事業者等に対して閉鎖依頼の実施を要請するとともに、関係団体やサイバー防犯ボランティアとの連携を強化し、より幅広い主体が閉鎖依頼を実施する環境を整備する。

収益化対策

- **(ｳ) パスキーの普及促進**
  次世代認証技術の１つであるパスキーについて、既に採用している事業者等における効果等を踏まえ、金融機関やＥＣ加盟店等のサービスにおける採用や、当該サービスの利用者に対する利用を働き掛けるなど、普及を促進する。

出典：首相官邸ホームページ「国民を詐欺から守るための総合対策 本文」https://www.kantei.go.jp/jp/singi/hanzai/kettei/240618/honbun.pdf

犯罪対策閣僚会議での決定事項として、関連省庁主導のもと、対応・対策が進んでいくと思われる

フィッシング対策「誘導対策」：DMARC

■ポイント① 「誘導」（フィッシングメール）への対策

➢送信ドメイン認証「DMARC」による対策

→「なりすましメール」を利用者に届かなくする対策

➢DMARCは、SPFやDKIMの認証が失敗した場合、「メールの受信制御ポリシー」にてメールを制御できる。

- 1.そのまま受信させる（ポリシー”none”設定）
- 2.隔離させる（ポリシー” quarantine ”設定）
- **3.受信を拒否する（ポリシー”reject”設定）←これを設定する**

送信ドメイン認証	
SPF	正規のサーバー（IP アドレス）から送信されたかを検証
DKIM	電子署名でメールを検証
DMARC	SPF、DKIMを補強する

Googleと米Yahooがフィッシングメール対策を強化

■フィッシングメール、なりすましメール対策を強化するため、Googleと米Yahooは送信者に対し、メッセージを送信する際にメール認証が必要になる旨の「送信者向けガイドライン」を発表（ 2023年10月）

■2024年2月１日以降は、SPF、DKIM、DMARCが正しく設定されていないメール（なりすましメール、フィッシングメール）は、メールが拒否されたり、受信者の迷惑メールフォルダーに配信

Google　メール送信者のガイドライン
https://support.google.com/mail/answer/81126

1日あたり 5,000 件以上のメールを送信する場合の要件

2024 年 2 月 1 日以降、Gmail アカウントに 1 日あたり 5,000 件を超えるメールを送信する送信者は、このセクションに示す要件を満たしている必要があります。

- ドメインに SPF および DKIM メール認証を設定します。
- 送信元のドメインまたは IP に、有効な正引きおよび逆引き DNS レコード（PTR レコードとも呼ばれます）があることを確認します。詳細
- メールの送信に TLS 接続を使用します。Google Workspace で TLS を設定する手順については、メールのセキュアな接続を必須にするをご覧ください。
- Postmaster Tools で報告される迷惑メール率を 0.10% 未満に維持し、迷惑メール率が決して 0.30% 以上にならないようにします。詳しくは、迷惑メール率の詳細をご覧ください。
- Internet Message Format 標準（RFC 5322）に準拠する形式でメールを作成します。
- Gmail の From: ヘッダーのなりすましはしないでください。Gmail では、DMARC の**検疫**適用ポリシーの使用が開始されます。Gmail の From: ヘッダーのなりすましをした場合、メール配信に影響する可能性があります。
- メーリング リストや受信ゲートウェイを使用するなどして、メールを定期的に転送する場合は、送信メールに ARC ヘッダーを追加します。ARC ヘッダーによって、メールが転送されたことが示され、送信者が転送者と見なされます。メーリング リストの送信者は、メーリング リストを指定する List-id: ヘッダーも送信メールに追加する必要があります。
- 送信ドメインに DMARC メール認証を設定します。DMARC 適用ポリシーは **none** に設定できます。詳細
- ダイレクト メールの場合、送信者の From: ヘッダー内のドメインは、SPF ドメインまたは DKIM ドメインと一致している必要があります。これは DMARC アライメントに合格するために必要です。
- マーケティング目的のメールと配信登録されたメールは、ワンクリックでの登録解除に対応し、メッセージ本文に登録解除のリンクをわかりやすく表示する必要があります。詳細

フィッシング対策「誘導対策」：DMARC注意点

- **2024年5月ごろから、フィッシングの対象ブランドとは関係のない事業者のドメイン名になりすましたメール配信が急増**
- DMARCポリシーがnone、つまり認証失敗しても配信、という設定のドメイン名が中心となって使われていた　→　フィッシングメールへの悪用

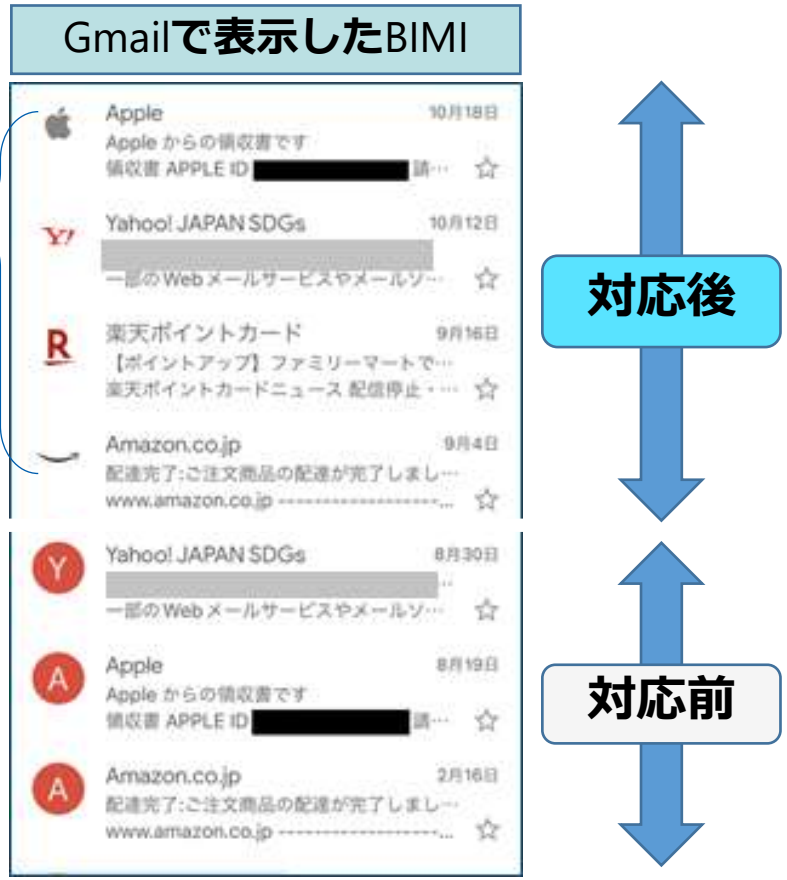
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 7:19
【アイフル株式会社】特別な利息無料キャンペ...	アイフル株式会社 <service@costcojapan.jp>	2024/10/14 10:18
【アイフル株式会社】特別な利息無料キャンペ...	アイフル株式会社 <info@costcojapan.jp>	2024/10/14 10:46
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 10:55
【重要】Amazonアカウントの情報更新をお届...	Amazon <bjxxzr@vpass.ne.jp>	2024/10/14 11:12
【重要なお知らせ】お客様のお支払い方法が承...	Amazon.co.jp <tonanpwn@vpass.ne.jp>	2024/10/14 11:18
Amazon.co.jp お客様のご注文がキャンセルさ...	Amazon.co.jp <amazon.co.jp-appagp.signin-o...	2024/10/14 11:29
【重要なお知らせ】メルカリ事務局からのお知ら...	メルカリ <no-reply@accounts.nintendo.com>	2024/10/14 11:55
Amazonプライム会費のお支払い方法に問題...	Amazon <pzmqnatfadr@costcojapan.jp>	2024/10/14 12:11

- **DMARCポリシーはreject、つまりドメイン名なりすましメールは排除する設定にしなければ、フィッシング効果が得られず、逆に悪用されるリスクがある**

フィッシング対策「誘導対策」：BIMI：正規判別を助ける対策

- 利用者にとって必要なのは、正規メールかどうかの判断を助ける情報
- BIMI：DMARCで認証された正規メールにブランドアイコンを表示する技術

BIMI
ブランドアイコン表示

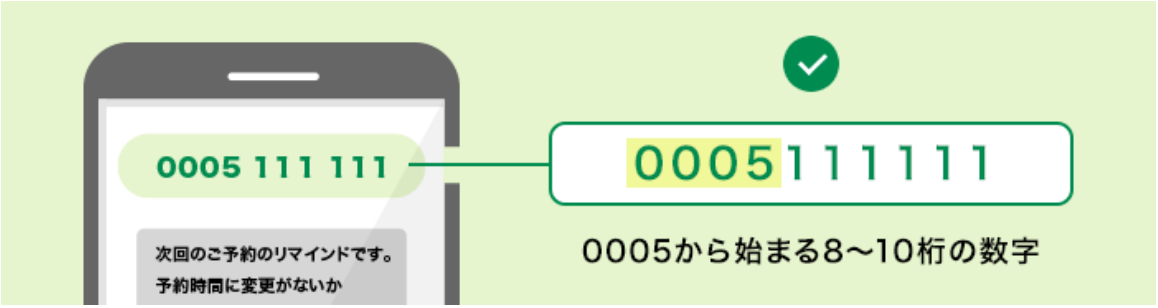


フィッシング対策協議会
Council of Anti-Phishing Japan

スミッシング対策「誘導対策」：0005：正規判別を助ける対策

- 新しい偽SMS対策、キャリア共通番号「0005」
- 国内4キャリア（NTTドコモ、KDDI、ソフトバンク、楽天モバイル）が発行するキャリア共通番号の「0005」
- 発信元番号が「0005」から始まるSMSは「正規の企業からのSMSです。安心して受信してください」と案内することが可能

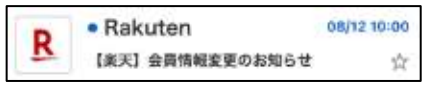
企業からのメッセージとして
あんしんしてご確認いただけます。



フィッシング対策「誘導対策」

送信ドメイン認証方式の一覧

<table>
<tr><th colspan="6">送信ドメイン認証技術</th><th colspan="2">メールセキュリティ標準規格</th></tr>
<tr><th colspan="2">SPF</th><th colspan="2">DKIM</th><th colspan="2">DMARC</th><th>BIMI</th><th>S/MIME</th></tr>
<tr><td colspan="2">正規のサーバー（IPアドレス）から送信されたかを検証</td><td colspan="2">電子署名でメールを検証。メールヘッダー情報やメール本文も署名対象にできる</td><td colspan="2">SPFとDKIMの検証結果を使って検証。認証に失敗したメールの挙動を定められる</td><td>正規メールであることをユーザーが視認できる

適切に認証されたメッセージの横にブランド固定のインジケーターを表示するための規格</td><td>認証局発行の電子証明書による電子署名付与。認証局による送信者の認証</td></tr>
<tr><td>アライメント不一致</td><td>アライメント一致</td><td>第三者署名</td><td>アライメント一致</td><td>監視モード</td><td>制御モード</td><td rowspan="2">DMARCポリシー
quarantine または reject
 
 
  </td><td rowspan="2">認証局発行の電子証明書による「電子署名」
+
「メールの暗号」</td></tr>
<tr><td>ヘッダ From ドメイン：企業ドメイン

エンベロープ From ドメイン：配信サービスドメイン</td><td>ヘッダ From ドメイン
＝
エンベロープ From ドメイン</td><td>ヘッダ From ドメイン：企業ドメイン

DKIM署名ドメイン：配信サービスドメイン</td><td>ヘッダFromドメイン
＝
DKIM署名ドメイン

（DKIMヘッダのd=タグ）</td><td>DMARCポリシー
p=none

DMARC レポートを定期的に検証して、メールがどのように認証、配信されているかを確認</td><td>DMARCポリシー
p=quarantine
隔離させる

p=reject
受信を拒否する</td></tr>
<tr><td colspan="6"></td><td>鍵交換なし</td><td>鍵交換あり</td></tr>
<tr><td colspan="6"></td><td>認証局発行の電子証明書による「電子署名」</td><td>認証局発行の電子証明書による「電子署名」
+
「メールの暗号」</td></tr>
</table>

フィッシング対策「誘導対策」：リンクURLを記載しない対策

■フィッシング詐欺被害未然防止のための措置として、メール・SMS内にパスワード入力を促すページのURLやログインリンクを記載しない対策がある

- 日本証券業協会：インターネット取引における不正アクセス等防止に向けたガイドライン

> メールや SMS（ショートメッセージサービス）内にパスワード入力を促すページのURL やログインリンクを記載しない（法令に基づく義務を履行するために必要な場合など、その他の代替的手段を採り得ない場合を除く）。

- リンクURL からのウェブサイト誘導ではなく、「いつも」の公式アプリ、「いつも」の公式サイト（ブックマーク）からアクセスしてもらう対策
- 送信ドメイン認証（SPF,DKIM,DMARC,BIMI）やドメイン管理など基本的な対策は必須

フィッシング対策：「詐取対策」

■ポイント② 「詐取」への対策

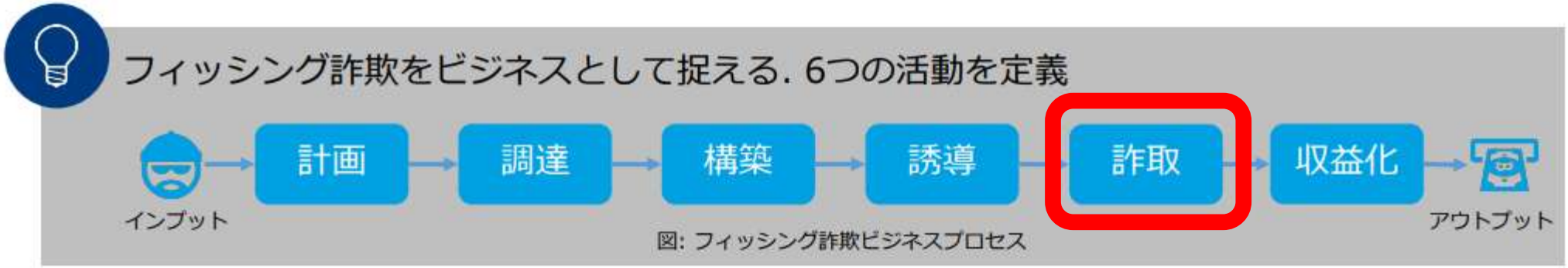


図: フィッシング詐欺ビジネスプロセス

- フィッシングサイトの閉鎖（テイクダウン）または無効化
  - URL フィルターへ登録
  - フィッシングサイトが属しているIPアドレスブロックを管理しているISPに連絡
  - フィッシングサイトで用いられているドメイン名の登録削除
- 実際の手段
  1. Webサイト運営者自身でAbuse連絡を行う
  2. フィッシング被害対応サービス事業者にテイクダウン依頼
  3. 専門機関にテイクダウン支援依頼（JPCERT/CC）

フィッシング対策：「収益化対策」

■ポイント③ 「収益化（不正アクセス）」への対策

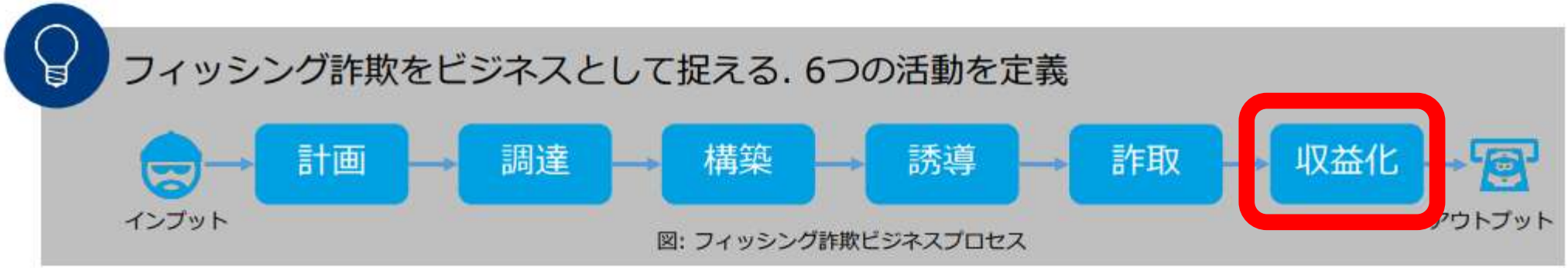


図: フィッシング詐欺ビジネスプロセス

「収益化」：詐取したクレジットカード情報から不正購入などにより攻撃者が収益を得ること

- 盗んだクレジットカード情報から、本人以外が決済できないようにする。
- クレジット決済の対策
  - EC加盟店においてカード所有者本人であることを複数手段で認証する国際的な認証規格：EMV 3-Dセキュアの導入が義務化

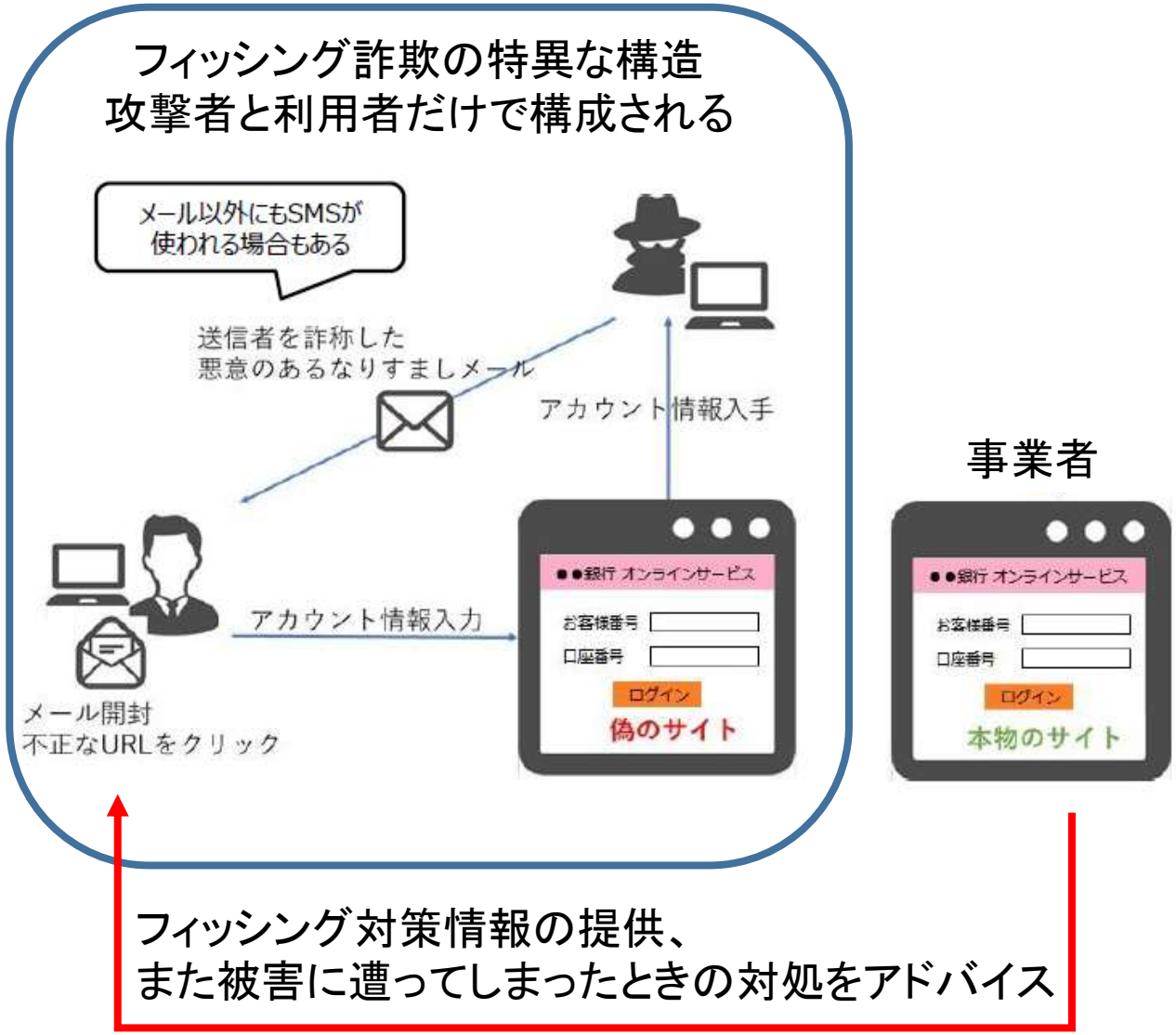
フィッシング対策：「収益化対策」

- **盗まれたパスワードを他人が利用できない対策**
- **フィッシング耐性のある認証方式：パスキー**
  - **パスキー（Passkey）**
    - パスワードに代わる簡単かつ安全なログイン手段
    - 利用者本人のみが保有する生体認証（指紋・顔）や端末固有のセキュリティ情報を使った認証方式
    - 対応済みサービス：Amazon、Google、ドコモ dアカウント、Yahoo! JAPAN、メルカリ、LINEなど
      【参考】FIDOアライアンス：パスキー ディレクトリ
      https://fidoalliance.org/passkeys-directory/?lang=ja
  - ワンタイムパスワードが代表的な多要素認証となるが、巧妙な攻撃の中にはメールやSMSで送付されるコードも奪い取るリアルタイムフィッシング、さらには機密情報を盗み出す情報窃取型マルウエアのインフォスティーラーなどもあることから、フィッシング耐性のある多要素認証方式のパスキーが有効となる。
  - これから認証強化を検討している事業者は、パスキー導入を進めるべきである。

フィッシング対策：利用者へのアドバイス

■利用者へフィッシングに関する情報提供、アドバイスが必要

- フィッシング詐欺の特異な構造として、悪意者と被害者となる利用者だけで構成されるため、被害の抑制は利用者自身にかかってくる。
- フィッシング詐欺対策において、利用者の負う役割は事業者側よりも大きい。
- 利用者へフィッシング対策に関する情報を提供し、フィッシングに遭ってしまったときの対処をアドバイスしていくことが信頼継続のために必要である。



■フィッシング詐欺対策

- 利用者の対策

協議会が提供する利用者対策

- 利用者向けフィッシング詐欺対策ガイドライン
- フィッシング詐欺対策5ヶ条

第 1 条　パソコンやモバイル端末は、安全に保ちましょう。

第 2 条　不審なメールに注意しましょう。

第 3 条　電子メールにあるリンクはクリックしないようにしましょう。

第 4 条　不審なメールやサイトは報告しましょう。

第 5 条　銀行やクレジットカード会社の連絡先リストを作りましょう。

マンガでわかるフィッシング詐欺対策5ヶ条

https://www.antiphishing.jp/phishing-5articles.html

協議会が提供する利用者対策

■インターネットを安全に楽しむための合言葉「STOP. THINK. CONNECT.」

- **STOP (立ち止まって理解する)**
  - インターネットは便利ですが、一般社会と同様、そこには危険もあります。どのような危険があるかを知り、解決策をどのように見つけるかについて、一旦、立ち止まって調べましょう。
- **THINK (何が起こるか考える)**
  - 様々な警告の見極め方を知る必要があります。警告を確認したら、これから取ろうとする行動がコンピュータやあなた自身の安全を脅かさないか考えましょう。
- **CONNECT (安心してインターネットを楽しむ)**
  - 危険を理解し、十分な対策をとれば、インターネットをより信頼できるようになるでしょう。

日本版「STOP. THINK. CONNECT.」
https://stopthinkconnect.jp/

協議会が提供する利用者対策

- フィッシングサイトに入力したときの対応
- フィッシングサイトにID・パスワードやクレジットカード情報、インターネットバンキングの認証情報を入力したときは、フィッシング対策協議会ホームページの「フィッシングの相談等」を参考に対応を急いでください。

https://www.antiphishing.jp/contact_faq.html

万が一、入力してしまったら：初期対応

❶パスワード変更

他のサービスで使い回しているパスワードを含め、すべて変更します。

❷履歴の確認

ログイン履歴、カード利用明細、送金履歴を確認し、疑わしき記録をチェック。

❸通報と相談

金融機関・サービス会社へ連絡しアカウントを停止。
その後、**警察（#9910）**や専門機関へ相談。

冷静に一つずつ実行することが被害拡大を防ぎます。

通報・相談窓口

被害	相談窓口
フィッシングと思わしきメールを受け取った	フィッシング対策協議会, info@antiphishing.jp
ネット犯罪に遭遇	警察庁 サイバー犯罪相談窓口
迷惑メールを受け取った	迷惑メール相談センター
偽装品の販売に遭遇	一般社団法人 ユニオン・デ・ファブリカン
商品やサービスなど消費生活全般に関する苦情や問合せ	独立行政法人 国民生活センター 消費生活センター
自社ブランドになりすました偽サイトを確認	悪質ECサイトホットライン 通報フォーム, 一般社団法人セーファーインターネット協会（SIA）
JPドメイン名の不正登録に関する情報受付窓口	株式会社日本レジストリサービス(JPRS)
サイトに違法情報（銀行口座や飛ばし携帯などの売買）の掲載を確認	インターネットホットラインセンター
法的トラブルに巻き込まれた場合の相談	法テラス

■フィッシング対策協議会
・フィッシング対策ガイドライン
・フィッシングレポート

協議会のワーキンググループ活動

■技術・制度検討ワーキンググループ

- フィッシング被害にあわないための各種対策議論
- **フィッシング対策ガイドラインの改定**
- **利用者向けフィッシング詐欺対策ガイドラインの改定**
- **フィッシングレポートの改定**

■STC 普及啓発ワーキンググループ

- 日本国内においてSTOP. THINK. CONNECT. を活用した普及啓発活動を行う為、様々な施策を検討し実行する.

■証明書普及促進ワーキンググループ

- 普及、啓発コンテンツの作成
- 安心安全なWeb サイト運営のためのガイドライン等作成.

■認証方法調査・推進ワーキンググループ

- フィッシング詐欺と関連の高いインターネットサービスの利用者認証について調査.

■被害状況共有ワーキンググループ

- フィッシング被害組織（ブランドを騙られる組織等）の対策コスト低減とコミュニティ形成を目指し、協議会で保有するフィッシング詐欺被害状況に関するデータを統計・可視化を進め、タスクフォースにて共同分析を行う.

■学術研究ワーキンググループ

- 学術機関で調査研究されている情報セキュリティ関連技術をフィッシング詐欺対策やインターネット詐欺検知に役立てるため、フィッシング対策協議会と学術機関が連携して研究をすすめる.

■詐欺サイト対処机上演習ﾜｰｷﾝｸﾞｸﾞﾙｰﾌﾟ

- サイバー空間上でブランドを詐称される可能性があるとの前提にたち、実際にインシデントが発生した際に実行可能な対処プロセスの策定を支援できる「机上演習キットの企画・開発・実施を目的とする.

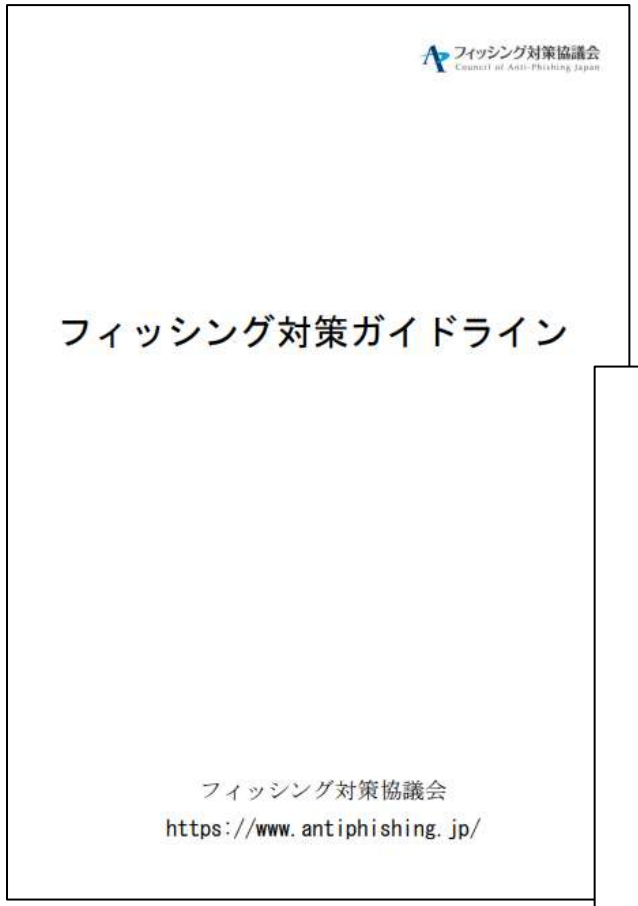
フィッシング詐欺ガイドライン

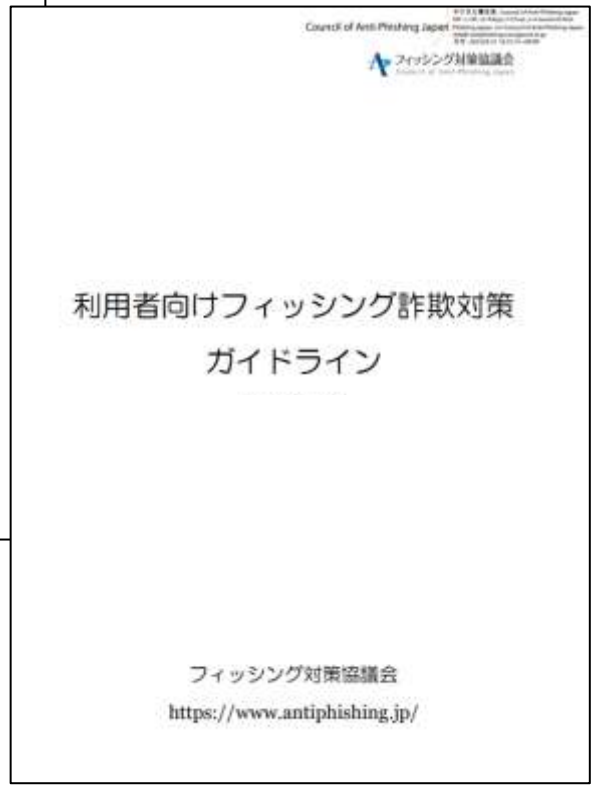
■事業者向け
フィッシング対策ガイドライン

➢事業者の対策をまとめている。
（2026年版は6月リリース予定）

■利用者向け
フィッシング詐欺対策ガイドライン

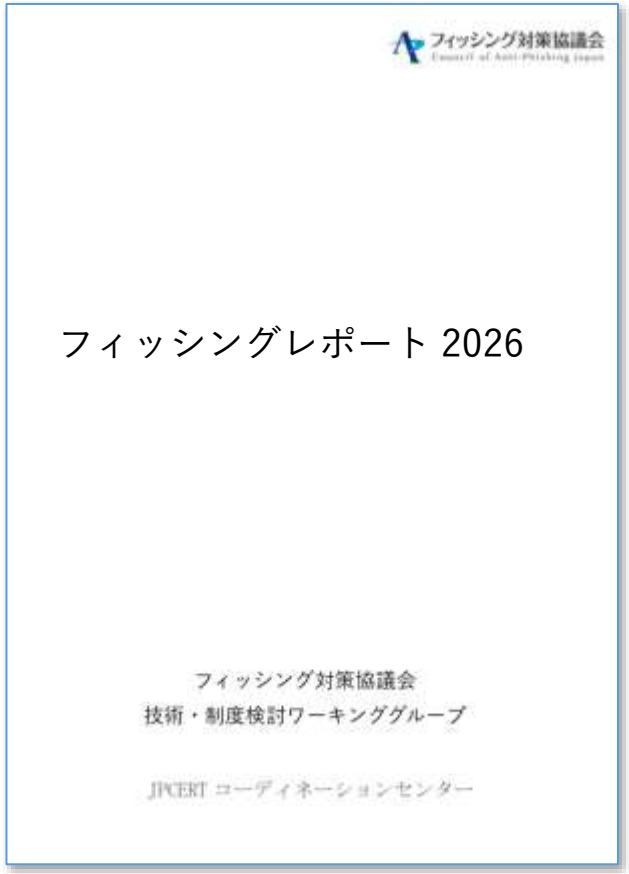
➢フィッシング対策3つの心得、メールやWebサイト、モバイル端末向けの安全対策、具体的な対処法について解説。





フィッシングレポート

フィッシング対策協議会ホームページ
にて2026年6月　公開予定



目次（暫定）

まとめ

- フィッシング詐欺が急増、狙いはクレジットカード情報、アカウント情報
- 被害に遭うブランド（企業）が拡大、証券会社を狙ったフィッシングの増加
- パスワード認証が繰り返し標的に　→認証強化が必須
- 対策①「誘導対策」 なりすましメールを届かなくする対策：DMARC
- 対策②「詐取対策」 情報を盗まれないようにする対策：テイクダウン
- 対策③「収益化対策」 フィッシング耐性のある認証：パスキー
- フィッシング対策ガイドラインの活用

ご清聴ありがとうございました。

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

TOPPANエッジ株式会社
加藤 孝浩