（資料１）

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

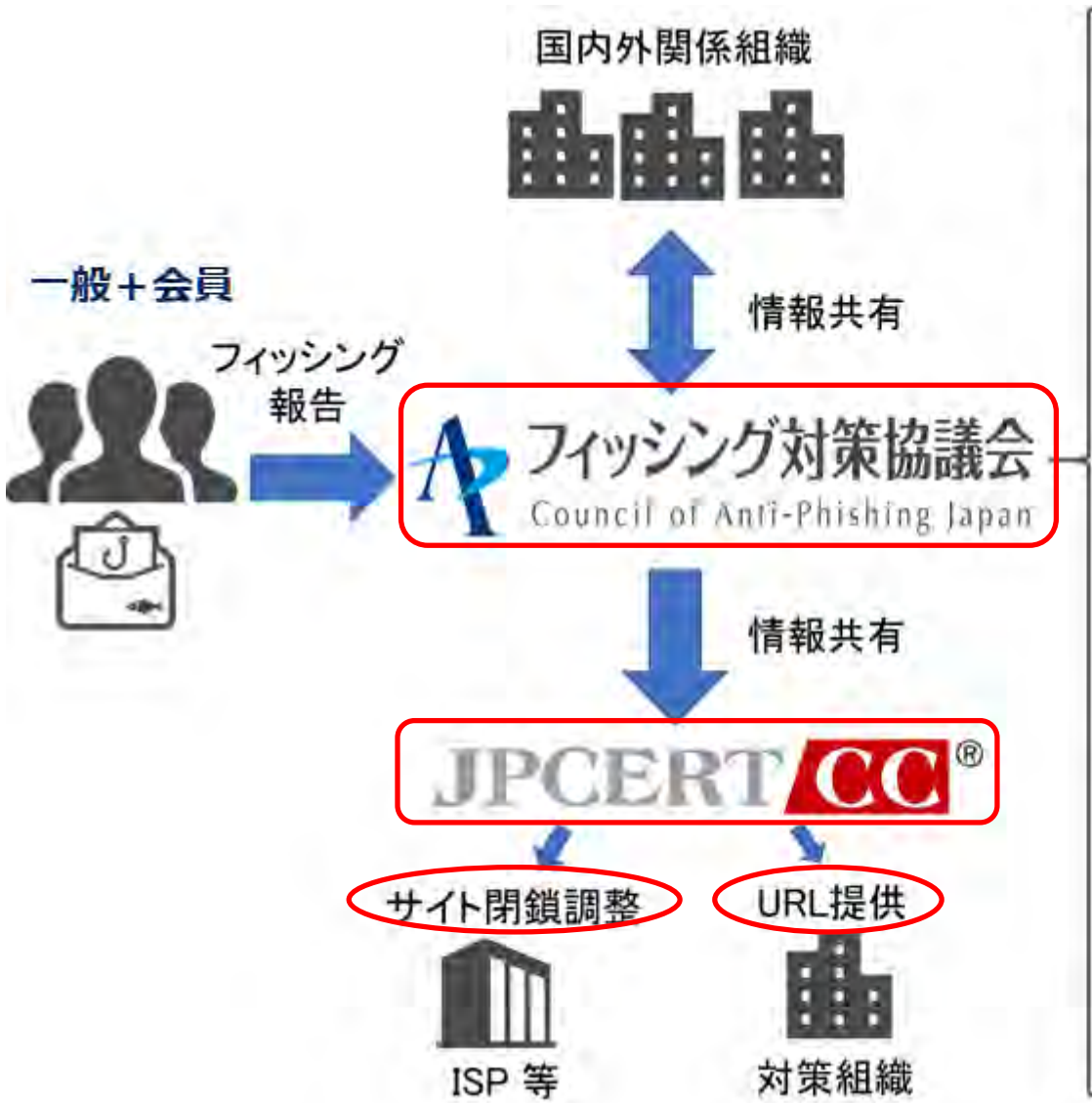
フィッシング対策協議会
消費者委員会 本会議 資料

フィッシング対策協議会 事務局

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
  - セキュリテイベンダー、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 104組織 （2020 年 9 月 17 日時点）
    正会員： 77 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
  - 一般社団法人JPCERTコーディネーションセンター
    - サイバー攻撃の初動対応支援やサイバー攻撃停止のための国内・国際間調整を担う中立的な専門機関
    - 1995年から活動し、経済産業省、内閣官房からの予算で活動

協議会の活動 ★



■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
Council of Anti-Phishing Japan

フィッシングとは ★

- フィッシング報告窓口で対応を行っているフィッシングの定義
  - 実在する事業者をかたり、本物のサイトと誤認させて事業者の正規サイトで使用する認証情報 (ID・パスワード) および個人情報 (クレジットカード番号や銀行口座情報等も含む) を詐取する行為
  - 不正アクセス禁止法第7条（識別符号の入力を不正に要求する行為の禁止）に該当するもの

- フィッシング報告窓口で扱っていないもの

  認証情報（識別符号）の窃取を伴わないもの

  ー 迷惑メール

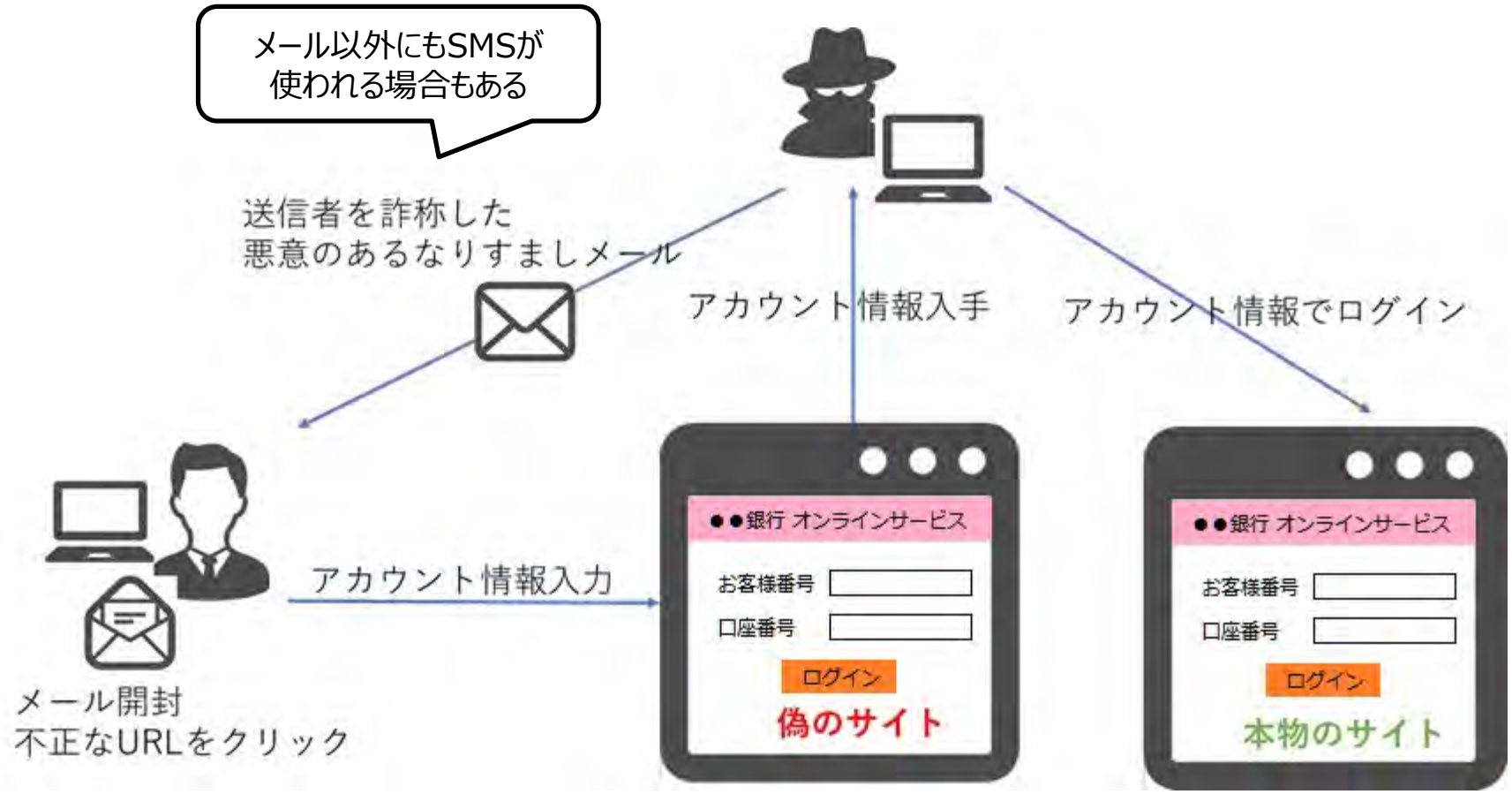
  – 当選詐欺（スマフォ当選、100円で安く買えるなど）

  – 悪質ECサイト

  – 偽ブランド品販売（レイバン、オークリー。。。）

  – セクストーション（性的脅迫）

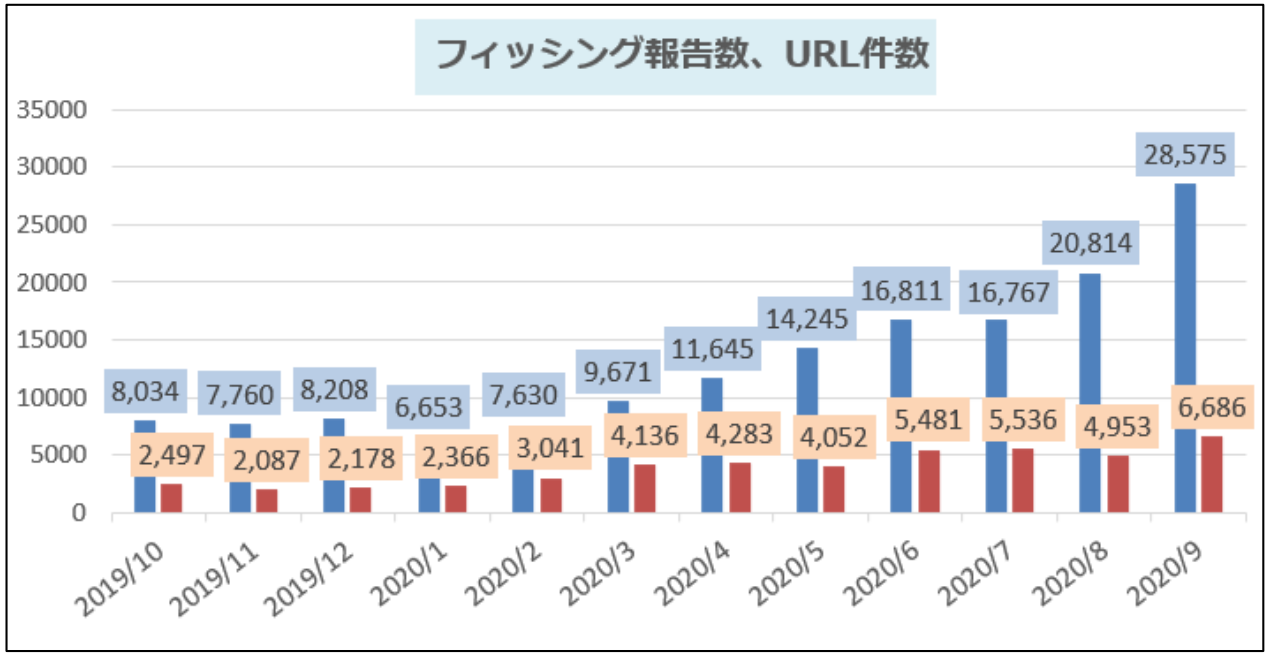
フィッシングとは（典型例）★



出典：フィッシング対策協議会

被害事案等の件数・具体的事例等 ★

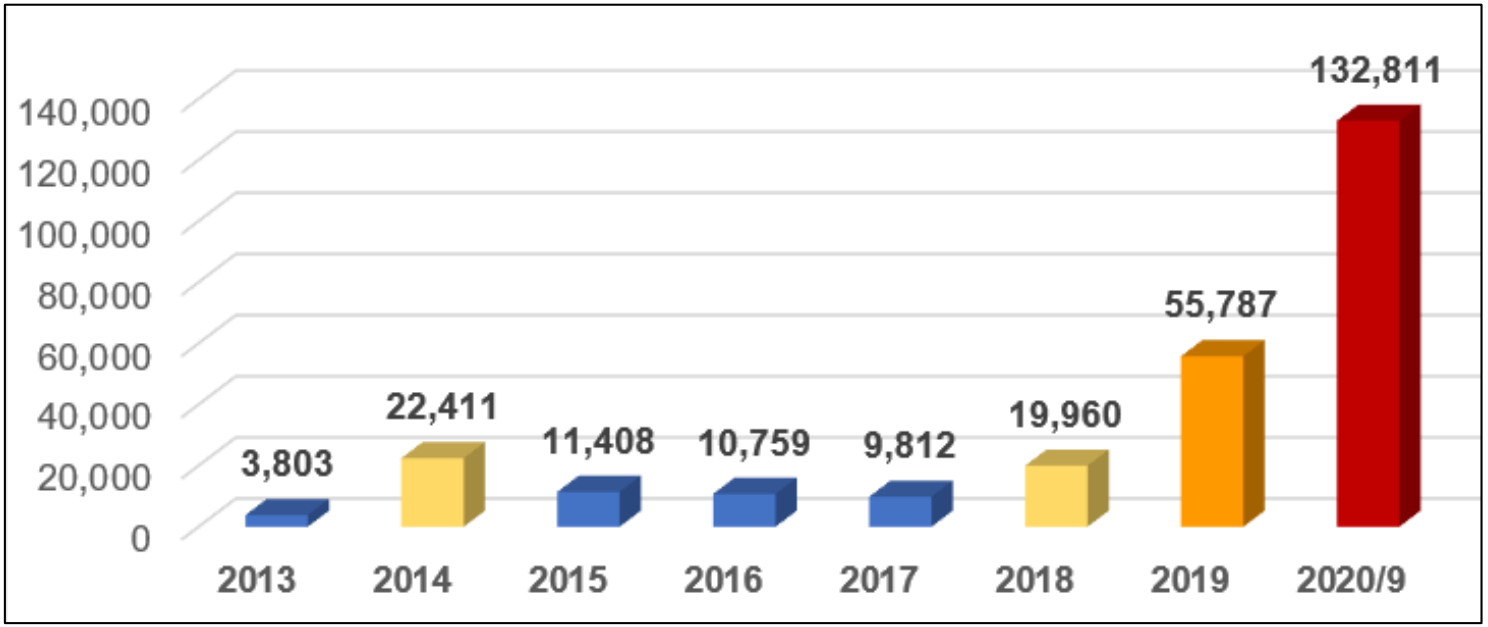
- フィッシング報告件数、URL (フィッシングサイト) 数の推移



- 2020年前半、報告数増加の要因、特徴
  - フィッシングメールの大量配信頻度の増加（1日20-30通 同じメールを受信）
  - 本物と同じドメインを使った、なりすまし送信の増加
  - 新たなユーザ層をターゲットとしたフィッシング攻撃（ブランドの多様化）
    - 国内EC サイト、フリーマーケットサービス、行政サービス等

被害事案等の件数・具体的事例等 ★

- フィッシング報告件数（年別）



- 2014年頃は不正送金目的、オンラインゲームの認証情報詐取目的のフィッシングが増加（事業者側の対策により、翌年以降は減少）
- 2016年頃よりクレジットカード情報を狙ったフィッシングが増加
- 2018年頃より、フィッシングメールが大量配信されるようになる
- 2019年ー2020年にかけて、不正送金目的のものが増加
  不正送金被害件数および被害額が急激に増えた
- 2020年10月現在では90%以上がクレジットカード情報を狙うフィッシング

被害事案等の件数･具体的事例等 ★

事務局におけるフィッシング報告の集計方法および対応内容

報告者

- ほとんどが当該メールや不審サイトを発見した「一般（ユーザー）」からの報告（約98%）
  他は警察、被害ブランド組織、組織のシステム部門等からの報告・相談

カウント方法

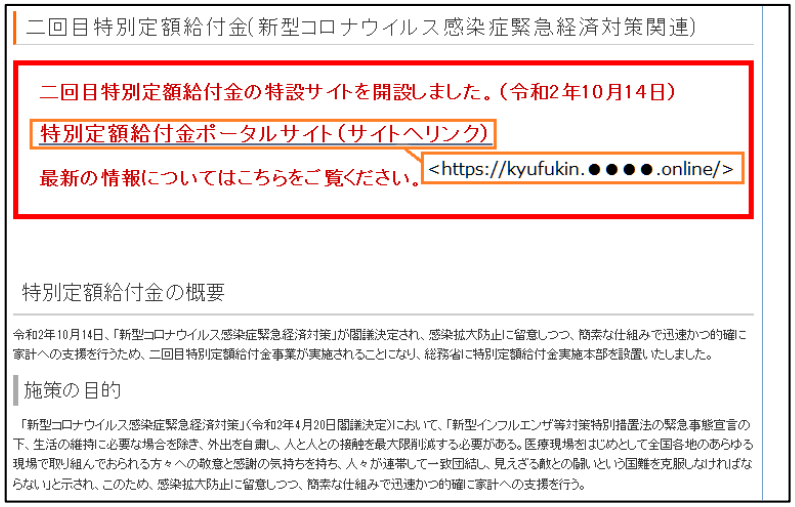
- 基本は報告URL 1件につき、1件と数えている
- フィッシングメール1通につき、1件とカウント
- 1通の報告メールに 3 通添付されていたら、3 件とカウント
- 1通の報告メールに URL だけ 3 件記載されていたら、3件とカウント

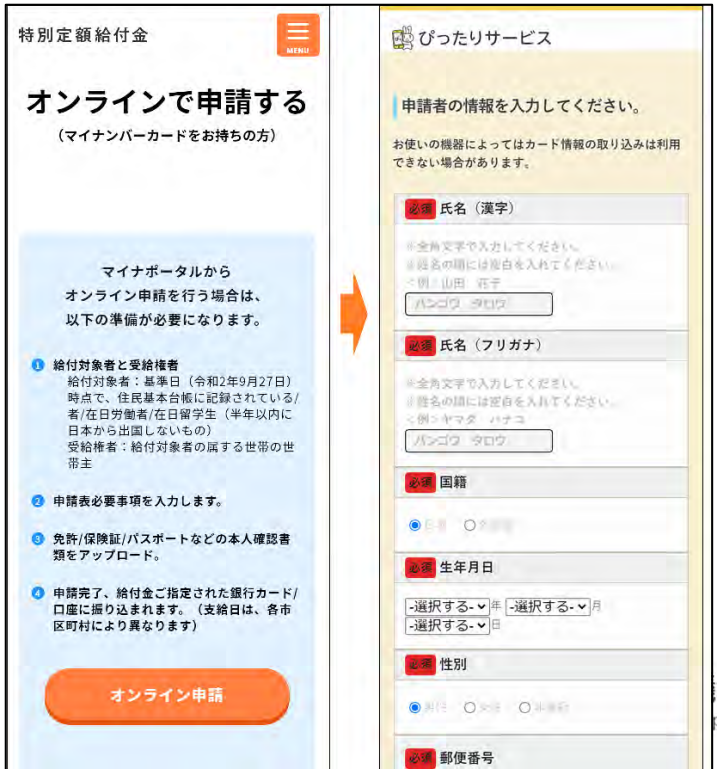
対応

- 毎日1,200 通前後の報告メールを分類（フィッシングとそれ以外）
- フィッシングメール内の URL へアクセスし、稼働状況を確認
- 報告者には受領返信、被害者・相談者には個別で返信
- 稼働中の未知のフィッシングURLを JPCERTコーディネーションセンターへ共有し、セキュリティベンダー等へのURL共有と不正サイトのテイクダウン調整を依頼
  （JPCERT/CCから国内外の事業者へサイト停止依頼を行う）

被害事案等の件数･具体的事例等 ★

- 特別定額給付金に関する通知を装うフィッシング (2020/10/15)
  https://www.antiphishing.jp/news/alert/kyufukin_20201015.html
  - ✓ 10/14、2回目の特別定額給付金の可能性に関するニュースが報道された、その翌日にフィッシングが発生
  - ✓ メールの差出人は 「総務省 <info●soumu.go.jp>」となっており、総務省の正規ドメインのメールアドレスをかたっている（なりすましメール）
  - ✓ 総務省は送信ドメイン認証（DMARC）に対応しており、DMARC検証を行っている受信側組織、サービスでは、このなりすましメールは検出できる
  - ✓ 連日のように新たなフィッシングサイトが次々に稼働し、フィッシングメールが配信され続けた。(10/15-10/30で720 件の報告受領)





問題の所在・課題

- フィッシング対応における問題点
  - 日本国内の一般ユーザー向けのフィッシング（当協議会で報告を受領しているもの）は、ほとんどが海外のクラウド事業者等でサーバが稼働している
  - メール発信元も、ほとんどが海外だが、日本国内の事業者のサーバを踏み台として経由したり、日本国内のISPユーザーのアカウントを不正利用してメール送信するケースも多い
  - フィッシングのほとんどはメールによる誘導
    - 9月の上位4ブランドは、繰り返し大量配信されており、報告数全体の約93.2 %であり、これらを無くすだけで、被害も減ると考えられる
    - フィッシングメールを送信させない（送信ドメイン認証など）
    - フィッシングメールを受信させない（ブラックリスト、送信ドメイン認証、迷惑メールフィルタ）
  - 海外では大手企業、オンラインサービスは 送信ドメイン認証に対応しているため、海外メールサービス事業者も送信ドメイン認証に基づくフィルタリングやブロックを実施しているが、日本のサービスは導入に遅れを取っているため、それを狙ったなりすましメールによるフィッシングが増えている

次ページへ続く

問題の所在・課題

フィッシング対応における問題点（続き）

- ドメイン、ホスティングの契約段階での検知に関する課題
  ⇒いわゆる「不正契約者情報」の共有が必要になるが、個人情報保護法や通信の秘密との関係で整理が必要

- 不正ドメインの利用停止における課題
  ⇒不正ドメインについて速やかに使用を停止させる方法が現時点でない
  レジストラでの対応が難しい。民事手続きやUDRPは時間がかかるため、一般的なフィッシングサイトの生存時間（12-48時間）にまったく追いつかない

- フィッシングサイトのテイクダウン（停止）における課題
  ホスティング事業者へ連絡して調査を依頼するも、特に海外は時差があり時間がかかるため、被害抑制の効果が薄い。また、現状は報告量が増える一方で、今後も継続して、すべてのフィッシングについて、関連組織への連絡を行うことが難しい状況となりつつある

- 不審なメールに関する報告・対応窓口の分散
  警察、迷惑メール相談センター、消費生活センター、フィッシング対策協議会…
  どこに報告・相談すれば良いのか判りづらい。

次ページへ続く

問題の所在・課題

- フィッシング対応における問題点（続き）
  - URLフィルタを利用したアクセスブロックによる被害抑制に関する課題
    - 迅速に URL をレポートすることが重要 (PhishTank, APWG eCX, Google Safebrowsing など) 。安定的に行えるような枠組みが必要
    - URL フィルタリングサービスは海外サービスであるため、国内ブランドのフィッシングは登録されづらいケースもある
  - 緊急対応窓口が不明
    フィッシングの被害に遭った（情報を入力してしまった）場合の対応窓口や、対応方法を記載していないところが多く、詐取された情報の不正利用被害を迅速に食い止められない
  - スマートフォン側での対応に関する問題
    現在ではオンラインサービスの利用者のほとんどがスマートフォンユーザであり、PC で可能だったメールセキュリティ対策が、スマートフォンでは様々な制限があり難しい。（S/MIME 等の電子署名、差出人メールアドレスの表示、端末側でのセキュリティソフトによる迷惑メールフィルタリングなど）

問題の所在・課題★

【対策】
不正サイトのテイクダウン
⇒【課題】攻撃のスピードに追い付いていない

【対策】
不正サーバ契約やアカウントの不正利用
⇒【課題】不正な契約をいかに防止するか

攻撃インフラ

海外の不正契約サーバやドメイン

国内の不正契約サーバやドメイン

国内の不正契約サーバやメールアカウントの不正利用

ボットネット

途中経路

【対策】
ブラウザやセキュリティソフトによるフィルタリング
⇒【課題】いかに早くURL情報を共有できるか

不正コンテンツへの誘導

メールの大量配信

【対策1】
通信事業者によるフィルタリング
【対策2】
DMARC対応によるなりすましメール検出
⇒【課題】利用者の同意、対応リソース、設備更新にかかる費用等

利用者

【対策】
不正行為に気付いた際や二次被害拡大防止
⇒【課題】サービス側の案内方法

取り組み・対策 ★

■ 事業者側での対策

【全体】

- DMARC推進、普及（なりすましフィッシングメール対策）
- URLフィルタサービスへの迅速な情報共有（フィッシングサイト発見したらすぐ登録する）

【メールサービスを提供する事業者】

- DMARC検証結果による なりすましメール判定
- 迷惑メールフィルタなど、各種メールセキュリティ対策の実装

【オンラインサービス提供事業者】

- 本物のサイトに常にアクセスさせるための技術や手法の導入
  スマートフォン アプリ、ブラウザのセキュリティ機能による警告
- 利用者がフィッシングメールやサイト判別のための情報を確認しやすくする
  サービス側から送信したメールを、正規サイトで確認可能とする等

■ 消費者側での対策

- 迷惑メールフィルタの利用
- 正規アプリ、正規サイトからの利用を行う（SMS、メールからのリンクばかり使わない）

■ 攻撃しづらくさせる取り組み

- メール配信に用いられる国内インフラ（サーバ、メールアカウント）の不正利用への対処
- URLフィルタサービスへの迅速な情報共有（再掲）
- フィッシングにより認証情報が窃取されても二次被害へ拡大させない取り組み（消費者が相談・報告しやすい総合窓口、各サービスにおける緊急相談窓口の案内など）

参考情報

- なりすまし対策ポータル「ナリタイ」
  https://www.naritai.jp/index.html
  - 電子メールの仕組み
    https://www.naritai.jp/introduction_mechanism.html
  - DMARC とその有効性
    https://www.naritai.jp/dmarc_effectiveness.html
  - DMARC 実例
    https://www.naritai.jp/dmarc_example.html
  - 法整備の状況、具体例-1
    https://www.naritai.jp/technology_compliance1.html
  - 法整備の状況、具体例-2
    https://www.naritai.jp/technology_compliance2.html

- フィッシング対策協議会
  https://www.antiphishing.jp/
  - 緊急情報・事例公開
    https://www.antiphishing.jp/news/database/
  - 月次レポート
    https://www.antiphishing.jp/report/monthly/
  - ガイドライン
    https://www.antiphishing.jp/report/guideline/

以上