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

フィッシングの現状とその対策

フィッシング対策協議会 報告受付窓口担当
一般社団法人 JPCERTコーディネーションセンター
平塚 伸世

この資料にあるデータは、
フィッシングの報告状況により、
発表時には変更される可能性が
あります

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 102 組織
    正会員：75、リサーチパートナー：６、関連団体：14、オブザーバー：7
- 事務局
  - 一般社団法人JPCERTコーディネーションセンター

協議会の活動

国内外関係組織

情報共有

一般＋会員

フィッシング
報告

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

報告

JPCERT CC®

サイト閉鎖調整

URL提供

ISP 等

対策組織

■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 報告受付 窓口

- 報告受付窓口
  info@antiphishing.jp / 03-6271-8905
- 事業者や一般からの報告メール、電話相談を受け付ける
  - フィッシングメール のみに対応

    それ以外にも以下の報告、相談がくるが、フィッシング以外でも被害者からの相談には返信、適切な窓口をご紹介している
    - マルウエアインストールへの誘導メール
    - 懸賞（当選）詐欺メール
    - 偽ショッピングサイト
    - 偽（模倣）サイト
    - 迷惑メール
    - 詐欺一般相談
- 報告されたURLの確認、テイクダウンの調整
  - フィッシングサイト のみに対応

    サイトを実際に確認した際に、以下のサイトに誘導されることもあり、適切な窓口へ連絡することもある
    - 懸賞（当選）詐欺サイト
    - マルウエアインストールへ誘導する URL
    - フィッシング以外の詐欺サイト
- データ蓄積、分析
  - フィッシングメールデータ
  - 送信日時、ブランド、URL、サーバ証明書など
  - 分析に基づいた、さまざまな情報発信

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

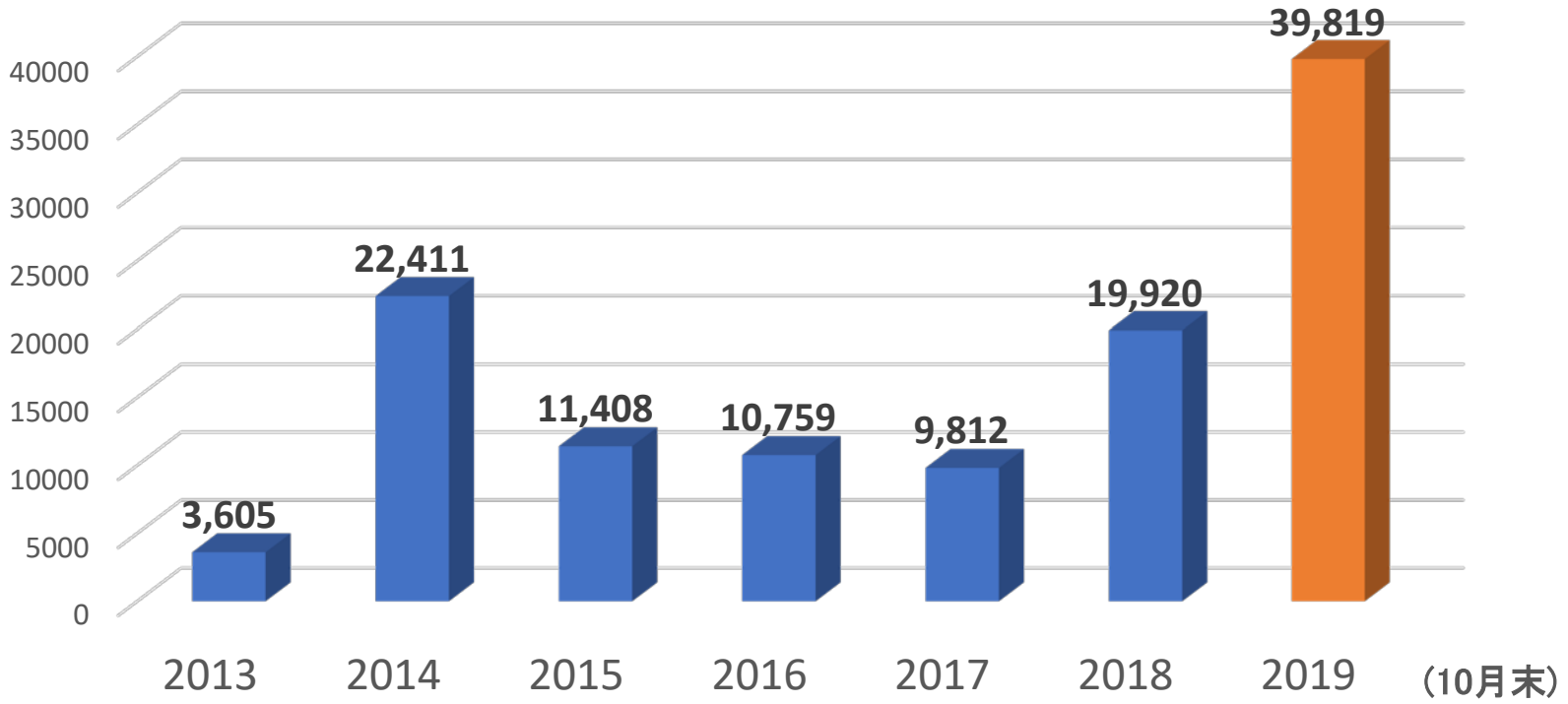
最近のフィッシング事例

当日、会場で

フィッシングの報告受領状況

フィッシング報告件数（年別）

- 2019年1月から10月までで39,819件
- 2018年、フィッシングが増えてます、と言っていたが、2019年はそれをはるかに超える勢い

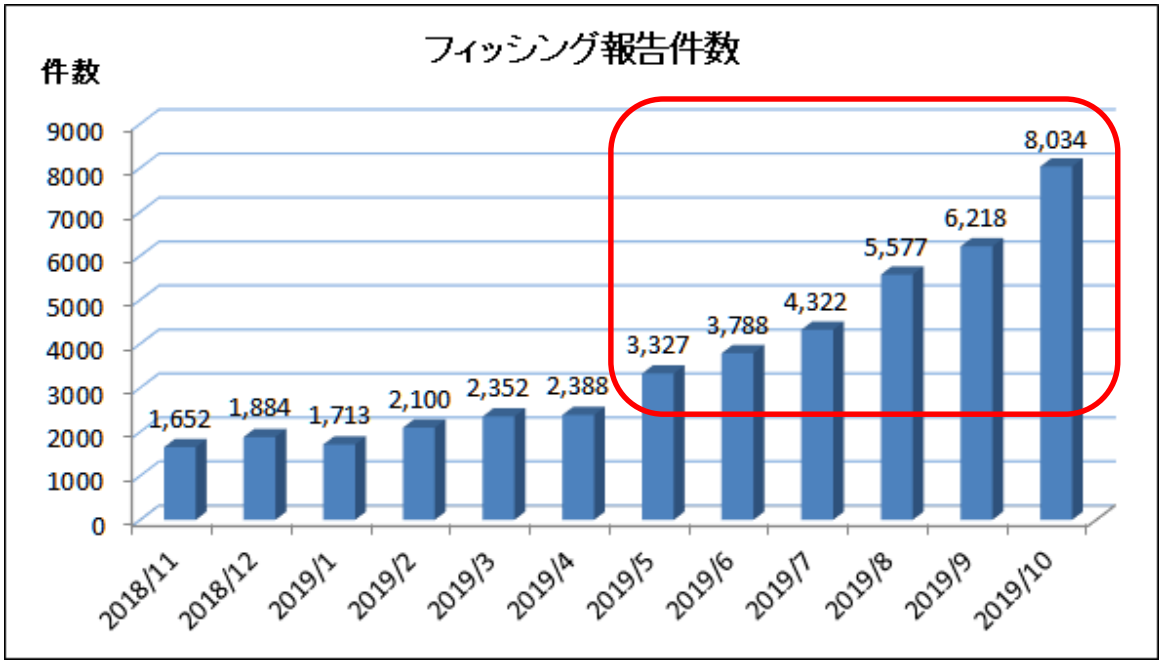


出典：フィッシング対策協議会

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

フィッシング報告数の推移

- 2019年度、急激に増加している。



- 主な増加の原因
  - スパムボットを使った大量配信 （週１配信 → 週数回配信）
  - 特定の海外事業者からの大量配信
  - 国内ISPユーザのアカウントを不正利用した踏み台送信
  - 国内レンタルサーバ事業者を踏み台にした大量配信（10月は激増）

これらの大量配信系フィッシングメールを減らしたい！

大量配信系フィッシングメール

以下のタイプの大量配信が目立っている

- スパムボットを使った配信
  - 国内外のIPアドレスから発信、直配送
  - 差出人のメールアドレスはさまざま（独自ドメイン）
  - 同じ文面、URL で大量の宛先に何度も配信される
  - 宛先には同じドメインの受信者のメールアドレスが列挙される場合が多い
- 国内事業者の設備（サーバ）を経由した配信 （踏み台送信）
  - 差出人のメールアドレスは、なりすましている場合もあるが、独自ドメイン、または事業者のドメインを使っている場合が多い
  - 正規ユーザとしてSMTP認証をパスして送信
  - 事業者に契約を行っているケースと、詐取したアカウントを使用していると思われるケースがある
  - 発信元は調べた範囲では ●●, ▲▲ が多い
- 特定の海外事業者からの直配送
  - 国内事業者の踏み台送信と交互に使うケースも多い
  - 発信元は調べた範囲では ●●, ▲▲ が多い
  - 当該事業者に調査依頼をするのは、現実的ではなさそう（不正送信の常連）

繰り返す国内事業者設備経由の
フィッシングメール配信

【重要：必ずお読みください】フィッシング

- MyJCB
  - MyJCB をかたるフィッシング (2017/02/20)
    件名:【重要：必ずお読みください】 MyJCB ご登録確認 ●●●●
  - 2017年2月、国内ISP6のメールアドレスを使用、発信元 不明
  - **2019年7月、**国内ISP2のメールアドレスを使用、発信元 TW
  - **2019年8月、**国内ISP2のメールアドレスを使用、発信元 CN

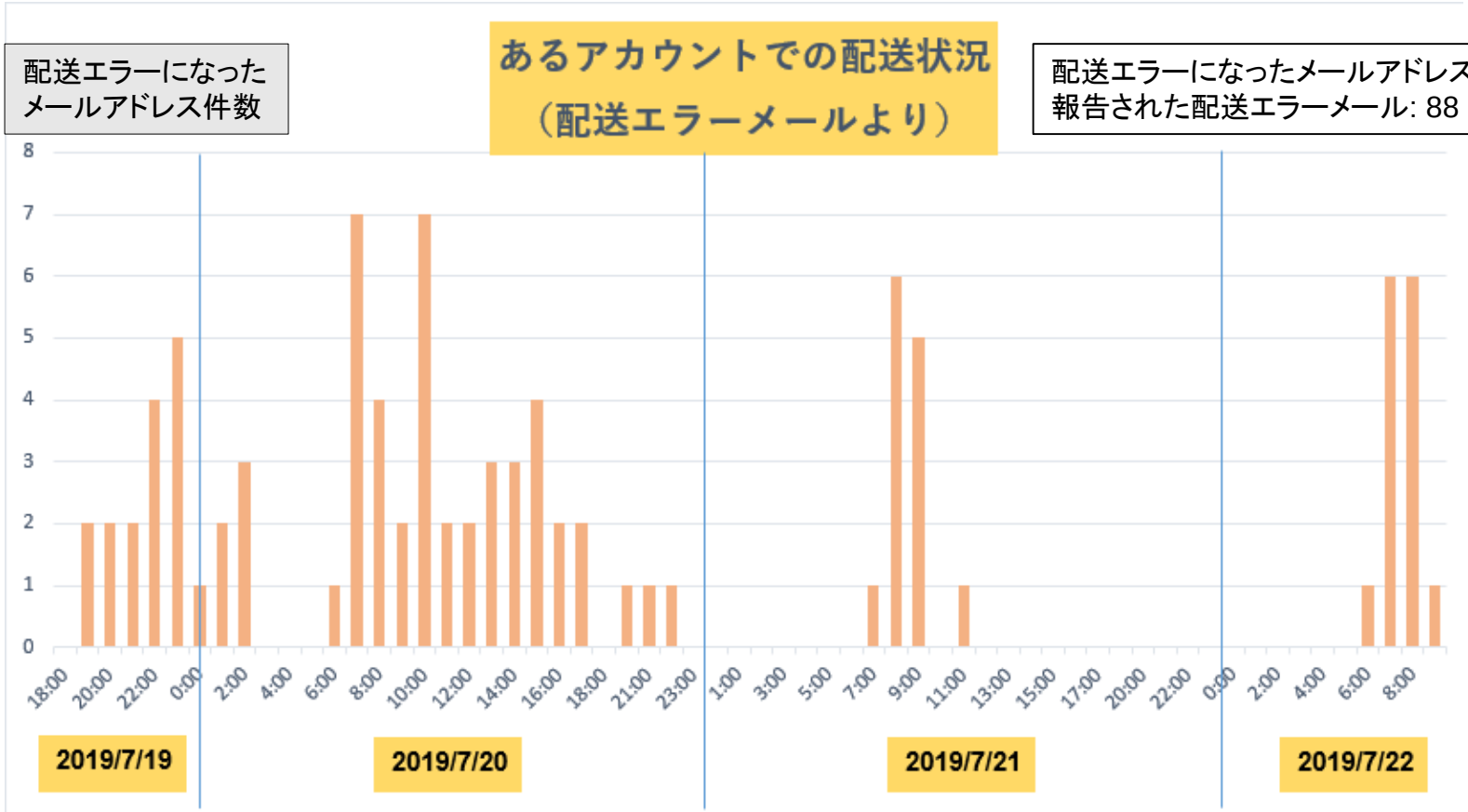
  - **どうみても実在するISPユーザのアカウントから送ってるようにみえる。。。**
  - **と思ったら、7月の配信では、いつもとちょっと違う報告を受領**

メールアカウントを不正利用された本人から
配送エラーメールの報告がきた！！

メール文面は2017年モノと同じ

JCBカードWEBサービスご登録確認
いつも JCBカードWEBサービスをご利用いただき、ありがとうございます。
この度、JCBカードWEBサービスに対し、第三者によるアクセスを確認いたしました。
万全を期すため、本日、お客様のご登録ＩＤを以下のとおり暫定的に変更させていただきました。
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。

配送エラーメールからみる配送状況



- メールアカウントは1回のキャンペーンで数日にわたって、何度も配送に不正利用する
- 通常の送信に紛れるよう、目立たないように送っている
- 送信先メールアドレスは @以前でソートしたリストを使って配送
  今回は、先頭文字が数字と a のメールアドレスに対して送信していた

国内事業者 踏み台送信系まとめ

繰り返し同じ手口で送られ続けている

- 発信元は海外が多いが、時々、国内サービスも発信元として使われる（不正契約？）
- 多数の ISP を渡り歩き、SMTP認証のアカウントを不正利用して配送を行う
  → **数年間、繰り返している**
- 送信者のメールアドレスは判るが、報告時にヘッダ情報がなく、Abuse対応できなかったメールアカウントは、また利用される可能性がある
  → そもそもアカウント情報が漏洩している
  → パスワード変更を促すメールを送るなどの対応をしてほしい
- 配送に使われた事業者のサーバのIPアドレスは、DNSBL に登録され、大手メールサービスに Reject される
  → レピュテーションの低下
  → メールを送れなくなる
  → 他の善良な利用者も巻き込まれる

- クレジットカード情報を入れてしまった被害者も出ています

このままでは、また繰り返す
何か打てる対策はないでしょうか？

不正利用目的のドメイン大量取得

- 不正利用目的でドメイン名を大量取得
  - 1 日朝晩 の 2 回、フィッシングサイトを切り替える
  - URLフィルタへ反映されると、別のドメイン名で稼働開始
  - メール件名、文面は同じことが多い
  - 数か月にわたり、ほぼ毎日新たなフィッシングサイトを立てられ続けるケースも
  - 不正目的利用されたドメイン名と、同一の登録者の残りのドメイン名も順次利用されていく….（判っていても止められない）

利用前に差し止めたい
何か打てる対策はないでしょうか？

今後のフィッシング対策
（迷惑メール含む）

フィッシング対策

- 今までの主なフィッシング対策
  - 一般への普及啓発活動
  - セキュリティ対策事業者・サービスによるURLフィルタリング
    - Safebrowsing に登録されるとフィッシングサイトが止まり、次のサイトが稼働する
  - フィッシングサイトのテイクダウン
    - 被害はメール配信から数時間内に集中して発生し、URLフィルタリングが間に合わない
    - 数時間～数日で停止し、次々と新しいURLで稼働するフィッシングサイトへの対応としては、そろそろ限界が見えている

- 今後、注力していきたいフィッシング対策（例）
  - フィッシングメールを送らせない、受け取らない
    迷惑メール対策技術を使ったフィッシングメール対策
  - 送信ドメイン認証 (DMARC)
  - レピュテーションによる判別、情報共有（ブラックリスト含む）
  - 現状把握のためのメールヘッダ情報収集、分析
  - 対応が難しい原因を明確化し、問題解決に向けた調整
  - **技術でできることは、技術で対応したい**
  - **技術でできないことは、知恵を持ち寄って対応したい**

事業者が正当業務行為として、対策・対応を行うには、どうすればいいのか？

事業者側の対応例

- 事業者の対応の試みを紹介
  → 当日、会場で

対策について

- 実際のところ、効果は？
  - DMARC
    レピュテーションを上げるために必要なケースもある

- 出来る？出来ない？（既にやってる？？）
  - 発信元IPアドレスのレピュテーション
    やはり発信元の情報は判断するうえで重要
    - MXに接続してきたホストまたはSPF 判定に使ったIPアドレスをヘッダに明記
    - SMTP-Auth 時の接続元 IP アドレスまたは地域情報をヘッダに明記
    - ブランド名と発信元IPアドレス情報の組み合わせで、ユーザ側で受け取るべきメールか判断材料の一つにする
    - レピュテーションに基づくレート制限
  - メール送信（SMTP-Auth）利用制限（海外からはデフォルト禁止など）
  - ブラックリスト (DNSBL) への登録
    - 不正送信に使われたサーバのレピュテーションを（一時的に）下げる
  - レジストラのレピュテーション
  - ドメイン名不正利用に基づくドメイン差し止め請求

対策について

- 利用形態の変化への対応
  - スマートフォン・タブレット（のみの）ユーザ増加
    メールヘッダ転送が難しい、表示できる情報が少ない
  - Display Nameを詐称する詐欺メールの増加
    特電法はメールアドレスのみが対象
    スマホだとDisplay Nameしか表示しない場合が多く、見分けがつかない
  - 専用アプリ？法整備？ガイドライン？

- 何のために対策するのか？
  - フィッシング被害に遭う人を減らしたい（自分が、家族が被害に遭ったら？）
  - 事業者も不正送信、不正利用の被害者。運用者や設備を守りたい
    ・Abuse 窓口だけでは対応は難しい。制約があるのは理解してます。
    ・でも目的を明確に、改善に向けて、一緒に前向きに対策を考えていきたい
    ・視点を変えて違う立場からアプローチをすると、解決の糸口が見つかるかも？
    ・通信の内容が見られない → 内容を見る立場側からの情報提供
    ・最初はできないと思っていたことも、実はできるかも（例：OP25Bなど)
    ・正当業務行為として、定常的にできる状態を目指したい

ぜひ意見交換、情報共有させてください！

フィッシングかな？と思ったら

フィッシング対策協議会 報告受付窓口

フィッシングの報告受付

- フィッシングに関する問い合わせが来た場合、ユーザに（なるべくヘッダ付きで）フィッシング対策協議会へ報告をするようにご案内して頂けると助かります

メールの場合

- ブランドをかたっている、本物のサイトで使用する認証情報を入力して、急いでログインするよう促している等、フィッシングの特徴があるか、確認する
- フィッシングメールを以下のメールアドレスに転送する
  info@antiphishing.jp
- メールは可能であれば「添付ファイル形式」で転送する（ヘッダ情報が付く）

ショートメッセージ（SMS）の場合

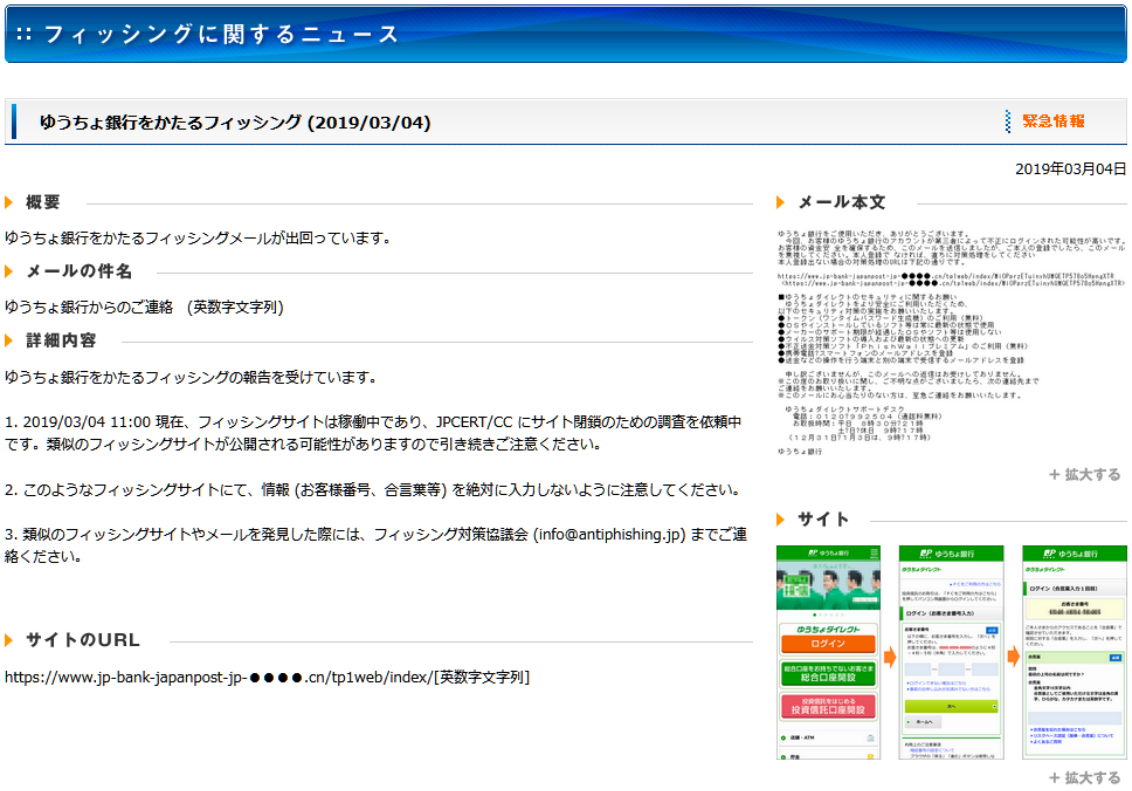
- SMSで来たフィッシングメッセージの、スクリーンショットを撮る
- 先ほど撮った SMS 画像をメールに添付する
  またはSMS の内容を、メール送信画面にコピペする
- 以下のメールアドレス宛に送信する
  info@antiphishing.jp

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

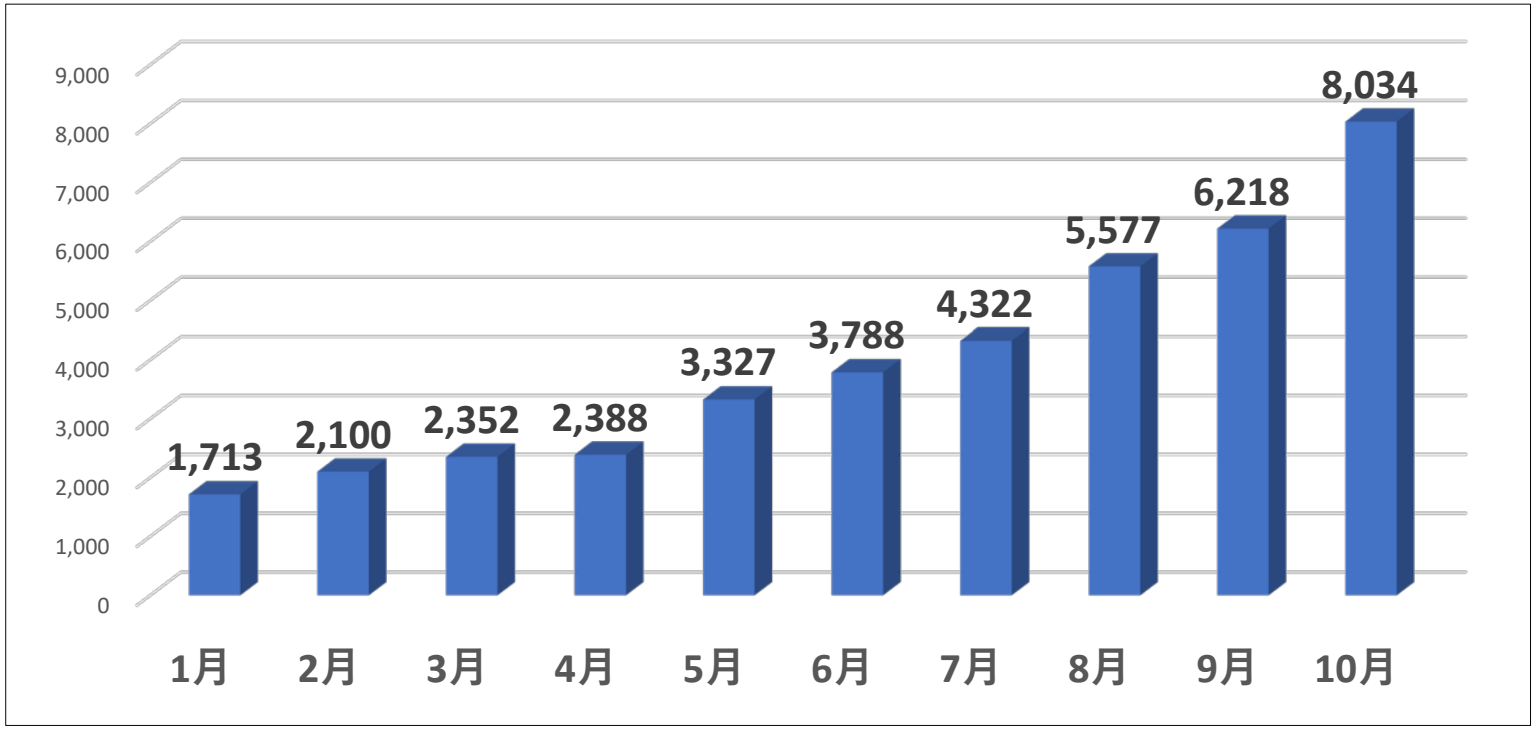
フィッシング対策協議会
Council of Anti-Phishing Japan

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か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



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

会場でお会いしましょう！