おさえておきたい基本や、
最新動向を解説するコーナーです。

No.86号 10:00 min.

01 不正送金の発生状況

不正送金被害額が過去最多を更新

2023年12月8日時点において、令和5年（2023年）11月末における不正送金被害件数は5,147件、被害額は約80.1億円となり、いずれも過去最多を更新しています。

金融機関を騙るメールを送信し、フィッシングサイトに誘導、IDやパスワードを窃取する従来型の手口が大半ですが、なりすましメールの内容が精巧になっていることも被害額増加の一因になっています。

なお、特殊詐欺（振り込め詐欺）とは異なり、被害者が高齢者のみに偏ることはなく、スマートフォンやパソコンを日常的使っている幅広い年齢層で被害が発生している状況です。

● 不正送金発生状況 ●

※平成24年から令和４年の数値は確定値、令和５年の数値は、同年12月８日時点における暫定値

出典：
警察庁「フィッシングによるものとみられるインターネットバンキングに係る不正送金被害の急増について（注意喚起）（R5.12.25）」
https://www.npa.go.jp/bureau/cyber/pdf/20231225_press.pdf

02 攻撃手口について

❶フィッシング

銀行を装ったフィッシングメールとしては、「送金失敗」や「継続的顧客管理（取引目的の確認）」などの内容で、
・送金時に必要な認証情報を窃取して、裏で待ち受けている犯罪者がリアルタイムに不正送金を実行
・ソフトウェアトークンの不正紐付けを狙い、その後不正送金を実行

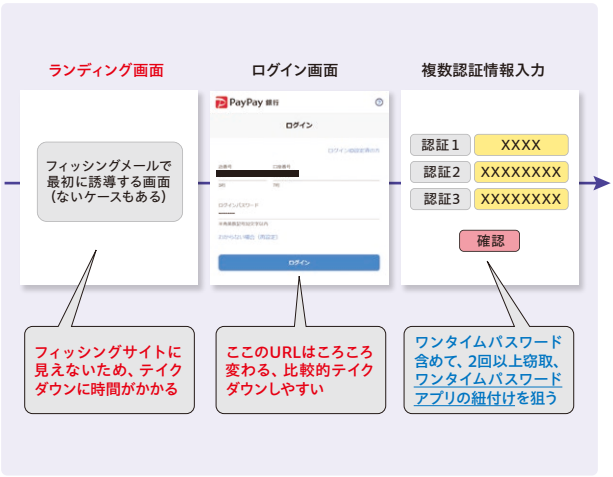
といった攻撃手口が継続しています。

なお、メールの件名や内容は多岐にわたり、1日に10種類以上のフィッシングメールが送信されることもあり（件名や本文をランダムに送信している印象）、利用者に対して、この件名のメールに注意してください、と伝えるだけでは注意喚起としては不十分な状況です。

● ある銀行の1日のフィッシングメールの件名 ●

[redacted]
銀行 アカウントセキュリティ通知.msg
銀行 アカウントの安全性に関するお知らせ.msg
銀行 お客様の口座について.msg
銀行：ログイン通知.msg
銀行：口座アクセス確認のご連絡.msg
銀行：新サービスのご紹介.msg
銀行：新しいモバイルアプリのご紹介.msg
銀行：特別キャンペーンのお知らせ.msg
銀行：年間取引サマリーのお知らせ.msg

フィッシングサイトの中には、ログイン画面や認証情報を窃取する画面の前に、ランディングページを挟むものがあります。利用者が最初にアクセスするそのページは、ただの誘導ページでフィッシング（情報窃取する）サイトそのものではないため、テイクダウンが困難だったり、テイクダウンされるまでに時間がかかったりするケースが見受けられます。



また、ランディングページに使われるURLには、メールアドレスを含むこと等により、誰が（どのメールアドレスから）フィッシングサイトに遷移してきたかをトラッキングし、騙されやすいメールアドレスを一覧として蓄積しているのではないかと推測しています。

［ テーマ ］

不正送金の脅威、その攻撃手口とリスク軽減策

▶▶▶ 2023年11月時点の速報情報において、不正送金の年間被害額が過去最多を更新しています。フィッシング等以前からある攻撃が多いにも関わらず、不正送金被害が止まらないのは、犯罪者が利用者の心理を巧妙についているからです。具体的にどのような攻撃手口があるのか、またそのリスク軽減策について、利用者、および企業（金融機関等）ができる対策の両面から解説します。

・誘導用（ランディングページ）
hxxps://*u340***22[.]ct.sendgrid.net/ls/click?upn=lQZbb09d4O-2FMJ***JjAkiX-2FEjZqXFsI-2F4gSWB19xdZQWPU9pwJRxpSXN-2Bmq3U3cfPxWw_pceu5zy8Ep4BYXT3jWd20Lszd6pWhj6FG1fzZG***U5b7Ad-2FPghCcwEeMtqRbK-2BbnnLWysvO***l4uSNdhDLIZ1oQ5
・実際のフィッシングサイト
hxxps://*new***s-url[.]is/all/answer3.php?ilfa=fiejflafei1245e4faeg55af***egrewgeegaegt***hrt26556

フィッシングサイトでは、ログイン情報（ID、パスワード）や送金時に直接必要な認証情報に限らず、暗証番号、カード番号、生年月日、電話番号等、本人を特定するための基礎的な情報は、根こそぎ窃取されているケースも多いため、フィッシング発生時は、企業（銀行）はその前提での対応が必要となります。

❷スミッシング（SMSフィッシング）

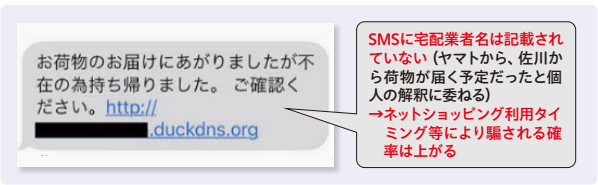
○銀行を騙るSMS

利用者の『銀行口座に不正アクセスがあった』、『銀行口座の一時利用停止』などを装ったSMSを送信し、フィッシングサイトに遷移させる手口です。送金時に必要な認証情報を直接窃取するオーソドックスなタイプや、ソフトウェアトークンの不正紐付けに必要な認証情報の窃取を狙うタイプが多い印象です。

フィッシングメールと異なり、スマートフォンにポップアップ表示されるため、視認性が高く、開封率・クリック率が高くなりやすいことが多いです。

○宅配業者の不在通知を騙るSMS

宅配業者やECサイト・通信キャリアを騙り、アクセスしたスマートフォンのOSやブラウザにより、その後の不正処理を分岐させる手口です。



（Androidの場合）
『MoqHao（モクハオ）』等のウイルス感染を狙い、偽のChromeをインストールさせ、偽Chrome「Chrome.」起動時に、インストール済みの銀行アプリを判定し、当該銀行の不正アクセスを騙った偽画面を表示し、認証情報を窃取します。ウイルスに感染したスマートフォン端末は、その後、SMSの送信元としても悪用されるなど、犯罪者の攻撃基盤の一つになり得るリスクを抱えています。

（iOSの場合）
JailBreak等していないiOS端末をウイルス感染させることは難しいため、フィッシングサイトに遷移させ、認証情報を直接窃取します。

○正規SMSに割り込むタイプ

送信元を偽装して送信されたSMSをチャット形式で受信・表示する場合、正規SMSと同じスレッド内（画面）に偽SMSが表示されるため、正規SMSか偽SMSかを判別することは困難です。その特性を活用し、SMS本文に記載されたURLをクリックさせて、フィッシングサイトに誘導しています。

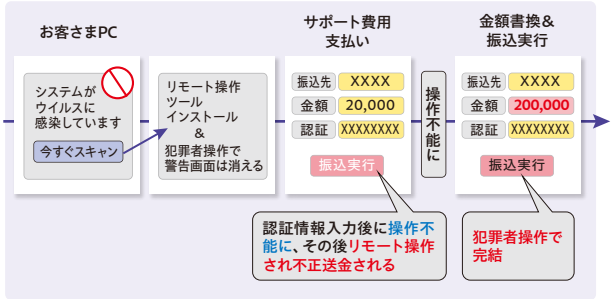
❸その他の攻撃手口（特殊詐欺含む）

○PCサポート詐欺

<攻撃手口>
パソコンがウイルス感染したと偽の警告画面を表示し、ウイルス駆除に

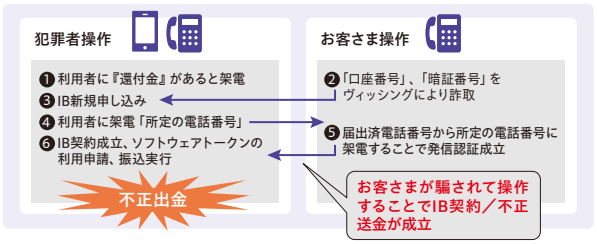
は専用ツールのインストールが必要、その駆除対応にはサポート費用が必要と利用者を騙す手口です。ここまでは古典的な手口ですが、利用者がサポート費用「X万円」をインターネットバンキングで送金を行う際に、犯罪者がインストールさせた専用ツール、実際にはリモート操作ツールで、利用者の送金額を「XX万円」に書き換えて（桁数を増やすなどして）送金を実行するものです。

<状況>
多数の銀行の利用者において当該事案を認識しています。利用者が自分の端末を（一部）操作していることもあり、特殊詐欺（振り込め詐欺）の一種として扱われます。犯罪者がリモート操作しているだけで、アクセス元の利用環境（デバイス、OS、ブラウザ）は、利用者が普段から使っている環境のため、銀行側でなりすましログインや不正送金されたことに気づきにくいという特徴があります。



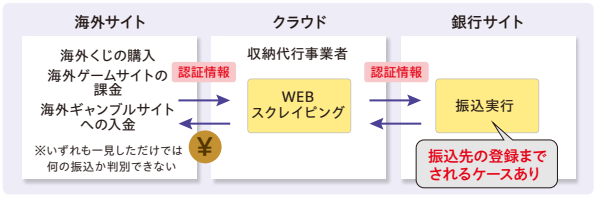
○ヴィッシング／インターネット版振り込め詐欺
<攻撃手口>
銀行員等を装い『還付金』の返還があると連絡し、「口座番号」「暗証番号」等を窃取、犯罪者が新規にインターネットバンキングを契約し、ソフトウェアトークンの利用申請や不正紐付けを実施する手口です。

インターネットバンキング契約時に、届出済電話番号による発信認証を採用している銀行でも、利用者が犯罪者に騙されて、所定の電話番号に自ら架電してしまうため、インターネットバンキング契約が成立してしまいます。
※高額預金者には、還付金返還の手数料が無料と言って騙す手口も確認されています。



○オンラインカジノ
<攻撃ではありませんが>
一部の銀行口座利用者がオンラインカジノを利用していると推測しており、海外のサイトから銀行サイトをスクレイピングすることで、送金を行っているものと考えています。送金先は、オンラインカジノの事業者名やサービス名ではなく、間に収納代行業者が入っていることから、実態が見えづらく対応が難しい状況にあります。

なお、利用者は海外のオンラインカジノサイトに、口座情報や送金時に必要な認証情報を入力してしまっている状況のため、悪用された場合、なりすましログインや不正送金も可能な状況です。



収納代行業者のアクセス元は、クラウドやVPSサービス等であることが多く、IPアドレスも頻繁に変更されるため、なりすましログイン等のリスクベース検知精度の阻害要因にもなっています。

<オンラインカジノは犯罪>
海外オンラインカジノの取り扱いはグレーだと記載しているサイトもありますが、警察庁のホームページには、明確に犯罪です、と記載されていますので、注意が必要です。

出典：（警察庁ホームページ）「オンラインカジノを利用した賭博は犯罪です！」
https://www.npa.go.jp/bureau/safetylife/hoan/onlinecasino/onlinecasino.html

03 リスク軽減策について

❶利用者ができるリスク軽減策

被害に遭わないために

・偽サイト（フィッシングサイト）を見分けようとしない
本物のサイトをコピーして作成されることが多く、偽サイトを見分けることは困難です。

・不審に感じたらアクセスしない
受信したメール・SMSにおいて、少しでも不審、不安に感じたら、本文のURLにはアクセスしないことが必要です。

・SMSの迷惑メール設定を利用する
利用している通信キャリアによっては、迷惑SMSブロック機能を提供していることがあります。ぜひ活用しましょう。

SoftBank	https://www.softbank.jp/support/faq/view/11600
docomo	https://www.docomo.ne.jp/info/spam_mail/spmode/sms/
au	https://www.au.com/mobile/service/sms/filter/

・常に公式アプリからログイン
常に公式アプリやお気に入り（ブックマーク）からログインすることをお奨めします。真に必要な連絡事項は、メールでの連絡だけでなく、ログイン後のお知らせ欄や通知欄などに掲載されていることも多いため、ログイン後の画面も確認してみると良いと思います。

受信したメール・SMSのリンクは、正規のものであってもクリックしない、このくらいの慎重さが必要です。

被害時のリスクを低減するために

・1日当たりの振込限度額を低くする
被害に遭われる方は、意外と振込限度額が高い状態のまま放置していることが多いです。セキュリティに意識を配っている方は、送金時に振込限度額を引き上げ、送金後は低い金額に戻す、または0円にしているケースが多いです。

普段からそういう操作をされている方は、フィッシングなどで認証情報を窃取されたということもほとんど発生していません。

❷企業（金融機関等）ができる軽減策

・利用者への注意喚起
フィッシングサイトや偽メールが出回っていることの注意喚起も必要ですが、それ以上に公式アプリの利用促進を推奨します。利用者が偽サイト（フィッシングサイト）を見分ける必要がないため、フィッシングによる不正送金が発生せず、利用者の資産保護に繋がることや金融機関

のセキュリティサイドから見ても、不正対応にかかるリソースを削減できること、加えて営業サイドから見ても取引の活性化に繋がるケースが多いため、良いこと尽くめです。

・モニタリング

犯罪者は、フィッシング一つとっても手を変え、品を変え攻撃してきます。日々のモニタリングにより、通常時の取引ぶりを知ることにより、異常時の取引に違和感を覚える嗅覚のようなものを養うことができます。平時にいろいろな角度からモニタリングしておくことで、有事に備えることが可能になります。

・重要操作のディレイ（遅らせる）

認証方式の切り替え、各種限度額の変更など、重要操作を一律即時反映させるのではなく、リスクベース判定で一定時間ディレイさせる（遅らせる）ことにより、金融機関のモニタリングや取引制限をかける時間を稼ぐなども有用な対策になります。利用者の利便性とセキュリティ（利用者の資産保護）との兼ね合いになりますので、バランスを見ながら、リスクベースの判定ロジックやディレイ時間をチューニングしていくことが重要です。

・なりすましメール対策（DMARC、BIMI）

送信ドメイン認証の一つであるDMARC※1対応を推進することも必要です。

ただし、銀行業においては必ずしもなりすましメールがドメイン詐称されているケースは多くないため、ブランドアイコン表示等（BIMI※2対応等）、正規メールの視認性向上を行うのが良いと思われます。2024年2月時点で、PayPay銀行においても取り組み中です。

❸業界団体における取り組み

・金融ISACの組成、取り組みについて

不正送金やサイバー攻撃は、常に犯罪者が有利です。その理由としては以下などが挙げられます。

・特定企業が攻撃を防御しても、犯罪者は攻撃対象を変えれば良いだけだから
  - 大手企業が常に新しい攻撃を受けているわけではありません（攻撃手口を知らない可能性もあります）
  - 関連／取引先企業から狙うと攻撃成功の確率は高くなります
・企業だけでは防御しきれない攻撃が増加しているから
  - 利用者／従業員が騙されるから（フィッシング、ビジネスEメール詐欺）
・1万人に攻撃して、仮に1人だけ騙されたとしても儲かるから
  - 犯罪者は不正に得た資金で、攻撃手口の高度化や攻撃手口を変えるためのシステム投資が可能です

不正送金や金融機関を狙ったDDoS攻撃／サイバー攻撃の発生から、情報共有の重要性を認識し、2014年に金融ISACを設立しています。PayPay銀行は、2012年4月に設置した前身組織から、その活動に参加しています。

・不正送金対策ワーキンググループの取り組みについて

約200社800名超のメンバーで活動しています。不正送金の新しい攻撃手口、モニタリング手法や効果的な対策などを情報共有しています。

『各銀行での対策（自助）』は前提として、『警察等組織との連携（公助）』だけでなく、『銀行間での協力（共助）』が重要になると考えています。

リソースシェアリング／情報シェアリングの実効性を高めるためにも、顔の見えるネットワークを構築し、信頼関係を築くことが必要だと考えています。

・利用者への注意喚起について

各銀行においてフィッシング等による不正送金への注意喚起は、当然実施していますが、必ずしも利用者の目に触れるとも限りません。そのため同一日に多数の銀行から注意喚起を実施することで、その取り組みをメディアにも取り上げてもらい（金融ISACとしてメディアへの働きかけ含む）、注意喚起の拡散を狙いました。

これらの取り組みを1社で行うには、リソース制約もあるため、なかなか難しいところですが、不正送金対策ワーキンググループのメンバーで役割／作業分担することにより、対応することができました。

・アクター（攻撃者）分析

各銀行でアクターを分析することは、リソースのみならず、スキル的にも難しいところですが、JC3※3と連携し、警察組織やセキュリティベンダの力を借りることで、それを実現しています。

アクターの分析結果を使いこなせているのは、一部の銀行に限定されますが、それでも攻撃手口の予測や対策を考える上では役に立ちます。1歩ずつにはなりますが、不正送金対策／セキュリティ対策の高度化を進めています。

※1 DMARC（Domain-based Message Authentication, Reporting and Conformance）
※2 BIMI（Brand Indicators for Message Identification）
※3 JC3：Japan Cybercrime Control Center（一般財団法人日本サイバー犯罪対策センター）

04 最後に

❶不正送金はアナログな攻撃手口が続く

現在、発生しているフィッシング等は、攻撃対象（デバイス、人、地域）を変えるだけで、同じ攻撃手口が通用します。これは犯罪者から見ると攻撃対象ごとにかかるコストが大きく抑えられることになるため、同じような攻撃手口は続くと考えられます。

これに対抗する企業の側から見ても、フィッシング等に対する知見やスキルがあっても、短い期間で大量にフィッシングサイトを立てられると目の前のテイクダウン対応や利用者への対応に追われ、根本的な対策が後手に回る（実際には企業として総力を挙げて対応していたとしても対応が追い付かない）こともありえます。そうならないためにも、他の企業で発生している事案を確認し、事前に対策を進めていくことが必要です。

❷特殊詐欺との境界があいまいに

不正送金も特殊詐欺（振り込め詐欺他）もクレジットカード不正も、犯罪者から見れば資金を窃取するための手段に過ぎません。コストパフォーマンスが良ければ、攻撃手口は問わないのだと思います。その意味では、これまで以上に不正送金と特殊詐欺の境界はなくなっていくと考えられます。

❸企業（金融機関）は、人が一番脆弱であることを改めて認識すべき

企業（金融機関）は、利用者が騙される前提でシステム制御を実施していく必要あります。偽サイト（フィッシングサイト）に騙される人は限定的だ、犯罪者（企業や警察を装った）に認証情報を伝えてしまう人は限定される、などと考えるのは非常に危険です。利用者が置かれている状況やタイミングにより、騙される確率は大きく変わると認識する必要があります。

当社が受けた攻撃を考慮すると、『これまでと攻撃レベルが異なる』と認識の上、対策を推進する必要があります。また、根本対策が進むまで、一時的なサービスレベル低下も視野に入れて対応を検討する必要がありそうです。

PayPay銀行株式会社
IT本部副本部長 PayPay Bank CSIRTリーダー
岩本俊二