TOKIO MARINE
リスクマネジメント最前線
2024 | No.12

急速に深刻化するサポート詐欺の最新動向

サイバーセキュリティ事業部　主任研究員（専門分野：クラウドセキュリティ、インシデントレスポンス）
荒川 琴恵

近年急速に増加しているサイバー犯罪の一つとして「サポート詐欺」がある。かつては「パソコンに疎い人だけがターゲットになる」または「怪しいサイトにアクセスしなければ被害に遭わない」といったイメージを持たれることも多かった。しかし、犯罪者の手口は刻々と進化し続けており、今はより身近で悪質な詐欺に変化している。当社が提供する企業向けのサイバーインシデント相談窓口「緊急時ホットライン」にも、サポート詐欺の被害相談は多く寄せられており、企業にとっても憂慮すべきサイバー攻撃となりつつある。

本稿では、当社に寄せられた相談から実際の事例も交えつつ、諸機関の報告を踏まえてサポート詐欺の最新の手口と被害動向を考察し、企業が取るべき対策について解説する。

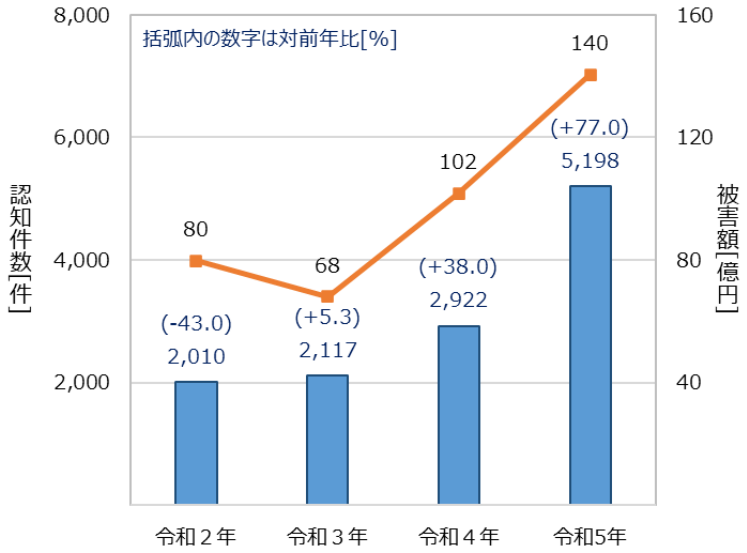
1. サポート詐欺の動向

(1) サポート詐欺の被害額・件数が大幅に増加

サポート詐欺とは、インターネットを通じて個人に対して行われる詐欺の一つであり、「偽セキュリティ警告」等とも呼ばれる。代表的な手口は、WEB サイト上に「コンピュータがウイルスに感染した」などの偽の警告メッセージを表示し、有名な IT 企業の窓口を騙る電話番号に電話させ、そこからサポート料金として高額な費用を請求するものである。

警視庁の報告[1]によれば、2023 年（令和 5 年）におけるサポート詐欺を含む架空料金請求詐欺の認知件数は前年比 1.8 倍の 5,198 件に増加し、被害額は前年比 1.4 倍の 140.4 億円に上った（図 1）。特殊詐欺の被害全体から見ても、架空料金請求詐欺の占める割合は前年の 16.6%から 10.7 ポイント増の 27.3 %となり、急速な増加傾向にある。

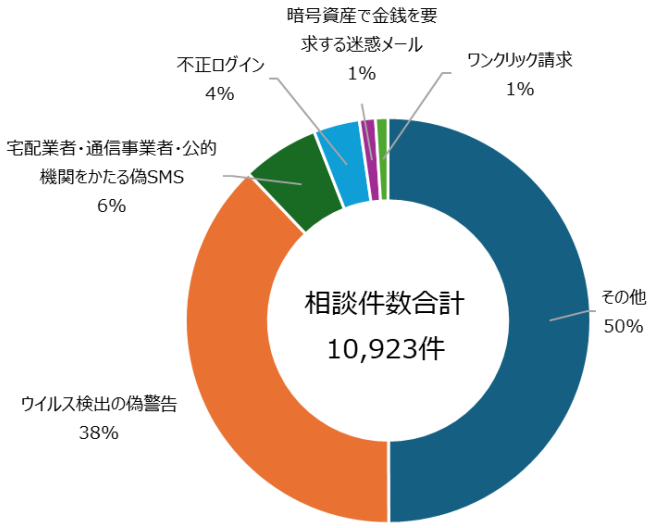
図１　架空料金請求詐欺（サポート詐欺を含む）の認知件数と被害額の推移



出典：警察庁「令和 5 年における特殊詐欺の認知・検挙状況等について（確定値版）[1]」をもとに当社作成

IPA（情報処理推進機構）が運営する、主に個人からの相談を受け付けている「情報セキュリティ安心相談窓口」では、2023 年に寄せられた 10,923 件の相談のうち、サポート詐欺を指す「ウイルス検出の偽警告」は 4,145 件であった[2]。これは「その他」を除けば最も高い 38%を占めており（図 2）、サポート詐欺は個人を標的としたサイバー犯罪において今や最も身近なものとなっている。

■　図２　2023 年に「情報セキュリティ安心相談窓口」に寄せられた相談の手口別相談件数



出典：IPA「情報セキュリティ安心相談窓口の相談状況［2023 年第 4 四半期（10 月～12 月）］[2]」をもとに当社作成

(2) 一件あたりの被害額が大幅に増加

一件あたりの被害額では、2023 年を境に大きな変化が見られる。ウイルス対策ソフト「ウイルスバスター」を提供するトレンドマイクロ社は、同社のサポート窓口に寄せられる相談において、2023 年に初めてインターネットバンキングを通じて 100 万円以上の金額を支払ってしまった事例を報告している[3]。

当社に寄せられた相談においても、今年度に入ってからサポート詐欺によってインターネットバンキングを侵害される事例が数件確認され、いずれも被害額は一件あたり 300 万円～500 万円と非常に高額であった。

従来のサポート詐欺において、金銭の要求は銀行への振り込みやプリペイドカードが使われることが多く、被害額は 10 万円～数十万円程度であった。インターネットバンキングが侵害されると被害額は 100 万円を超え、手口の変化が被害の高額化に大きな影響を与えていることがわかる。

(3) 企業におけるサポート詐欺

企業の従業員もサポート詐欺の標的となる可能性がある。当社がサイバー保険の加入企業向けに提供している「緊急時ホットライン」においても、実際に企業の従業員や委託先の職員がサポート詐欺の被害に遭ったという相談が多く寄せられている。

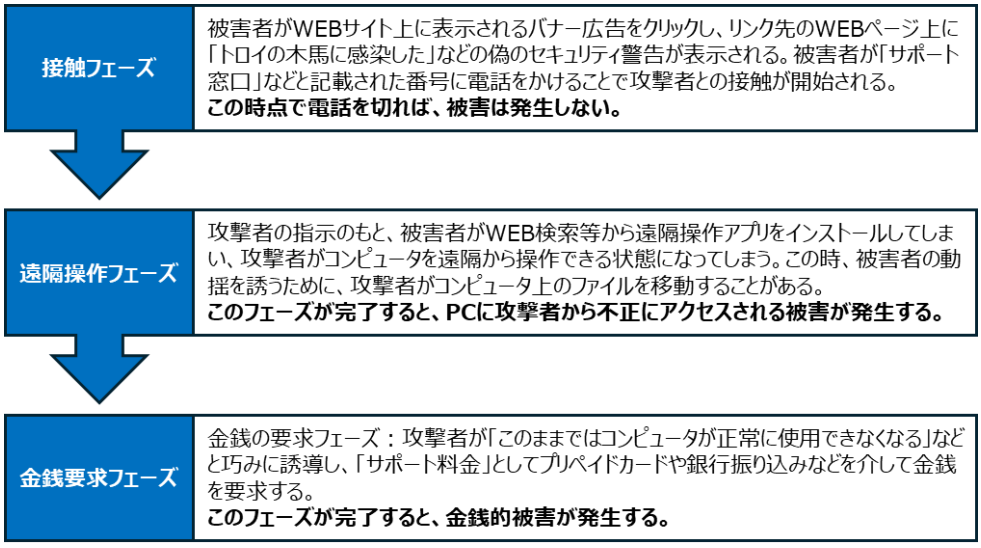
企業の従業員がサポート詐欺の被害に遭った場合、機密文書を PC 端末上に保存しており、攻撃者にファイルの中身を見られてしまう、攻撃者によって社外に不正に送信されるといった、情報漏えいリスクが問題とされやすい。また、最近ではインターネットバンキングの口座が標的とされるケースが増えており、企業の口座は個人の口座よりも多額の送金が可能であることから、攻撃者にとってはより効率的な、「コストパフォーマンスが高い」標的となっていると言える。

こうした動向の変化の中、企業で実施しているセキュリティ教育において、最新のサポート詐欺に関する啓発は十分にできているだろうか。企業で取るべき対策については、本稿の後段で詳しく述べていく。

2. サポート詐欺における手口の変化

こうした被害件数と被害額の飛躍的な増加の背景には、攻撃者グループが手口を次々に変化させており、サポート詐欺が急速に悪質化している状況があると考えられる。本章では、従来のサポート詐欺の典型的な手口を、被害の進行度から「接触フェーズ」、「遠隔操作フェーズ」、「金銭要求フェーズ」の 3 つに分類する。図 3 に各フェーズにおいてしばしば行われる内容と、そのフェーズが完了した時点での被害の進行度を整理する。

■ 図 3 従来のサポート詐欺における典型的な手口の流れ



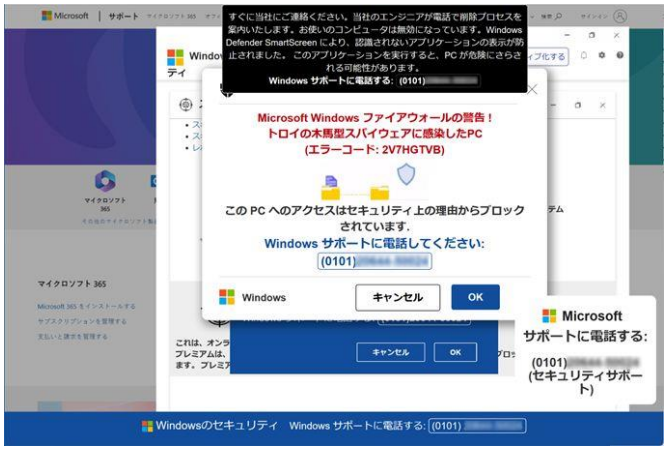
出典：当社作成

(1) 接触フェーズにおける変化

サポート詐欺は、WEB サイト上に表示されるバナー広告等から詐欺サイトに誘導され、誘導先で「トロイの木馬に感染した」などの偽のセキュリティ警告が表示されることから始まる。偽のセキュリティ警告には Microsoft 等の有名な IT 企業を騙ったサポート窓口の電話番号が表示されており、動揺した被害者が番号にかけることで攻撃者との会話が開始される。この「被害者が攻撃者に電話をかける」ことで開始される性質上、被害件数の増加はこの接触フェーズにおける変化が大きく影響していると考えられる。

また、手口の変化ではないものの、詐欺サイトに誘導するバナー広告が、企業が運営する WEB サイト上に表示される事例が報告されている。今年の 7 月、読売新聞社が提供する「読売新聞オンライン」を閲覧中に上に偽セキュリティ警告が表示されたとの報告を受け、同社が注意喚起を出す事態となった[4]。これは詐欺広告が配信元の審査機能をすり抜けて表示されているものと見られ、企業が運営するサイトだからといって安心できない状況となってきている。

■ 図 4 詐欺サイト上に表示される偽のセキュリティ警告の例



出典：IPA「サポート詐欺の偽セキュリティ警告はどんなときに出るのか？[5]」

□ 操作不能に「見せかける」のではなく、実際に操作不能になる詐欺サイトが出現

サポート詐欺の偽警告には多くのバリエーションがあり、その中には被害者の PC を操作不能にすることで動揺を誘うものがよく見られる。しかしこれらはマウスカーソルを非表示にする、ブラウザを全画面表示にして画面を閉じられなくするなど、あくまでも操作ができなくなったように「見せかける」ものであり、実際にはキーボード操作等で対処可能なケースがほとんどであった。

しかし、今年の 6 月以降、キーボードやマウスの操作を一切受け付けず、電源を入れなおし再起動しても状況が変わらないという、実際に操作不能になってしまう手口が IPA から報告された。

■ 図 5 2024 年 8 月に確認された、画面がロックされ操作不能となった状態の画面

出典：IPA「パソコンの画面全体に偽のメッセージが表示され操作不能になる手口が増加中[6]」

この手口についてトレンドマイクロ社は、以下の流れによってなされたものと分析している[7]。

1. WEB ブラウザから不審なファイルがダウンロードされる
2. 不審なファイルが実行されることで、遠隔操作ソフトや、画面をロックするソフトが PC にインストールされる
3. インストールされたソフトによって偽警告が表示され、画面がロックされることで操作が不能になる

すなわち、この手口では被害者は偽警告画面が表示される前に、WEB ブラウザから何らかの形で不審な実行ファイルをダウンロードしてしまっている。従って、ブラウザから不用意にファイルをダウンロードしないブラウザ設定や、不審なファイルダウンロードを検知するセキュリティソフト等で対策が可能である。一方で、従来の手口では単に WEB ブラウザ上の表示を変更する程度だったものが、知らぬ間にファイルをインストールさせ、PC を操作不能にする手口に変わっていることは、犯罪が高度化していることを強く感じさせる。

(2) 遠隔操作フェーズにおける変化

攻撃者は被害者からの電話を受けると、正規のサポート窓口を装って、被害者が使う PC に遠隔操作ソフトをインストールするよう誘導する。遠隔操作ソフトが実行されると、インターネットを通じて攻撃者が被害者の PC を遠隔操作できる状態となる。この際従来の手口では、電話に対応する被害者をより動揺させるために、攻撃者がデスクトップ上のファイルを全て移動するなどファイルの移動を行い、「パソコンが壊れてしまった。直すにはサポート料金の支払いが必要。」などと言って、金銭を要求するケースが多く見られた。

□「ファイルの移動」から「ファイルの削除」へ

当社に寄せられたサポート詐欺の相談では、今年に入ってから更に深刻な、ファイルの削除が行われるケースを確認している。一部のファイルがゴミ箱に移動されるという軽微なものは以前から見られていたものの、新たに確認されたケースでは、ディスクドライブがフォーマット（初期化）されることでドライブ上のデータが全て削除され、「消失したファイルを元に戻すため」という名目で金銭を要求された。なお、こうしたケースでは仮に金銭を支払ったとしても必ず攻撃者がファイルを元に戻してくれるとは限らない。金銭の支払いを確認したところで電話を切られることも十分考えられる。

業務に使用する PC でこのような深刻な被害に遭った場合、業務上重要なデータが直接削除される危険に晒される可能性もあり、企業においてはこうした手口の登場によって警戒度を上げる必要がある。

(3) 金銭要求フェーズにおける変化

従来の手口では、攻撃者が要求するサポート料金の支払いは「プリペイドカードを購入させる」、「攻撃者が指定する銀行に振り込ませる」のいずれかで、この支払要求における被害額は 10 万円～数十万円であった。

□ インターネットバンキングにログインさせることで数百万円を送金

2023 年以降、インターネットバンキングを侵害し、数百万円を攻撃者の口座に振り込ませる手口が報告されている。当社に寄せられた相談でも実際に数百万円を送金させられたケースを確認している。電話口でインターネットバンキングの認証情報（アカウントの ID やパスワード等）を聞き出す、被害者にインターネットバンキングにログインさせて送金させるなど、具体的な手口は異なっていた。また、前述のようにサポート詐欺では攻撃者が被害者の PC を遠隔操作できる状態にあり、被害者がインターネットバンキングにログインするように誘導され、ログインしたところで攻撃者の遠隔操作によって多額の送金がなされたケースも見られた。

インターネットバンキングを侵害されるケースでは攻撃者が送金操作を行える状態になっていることもあり、被害額が高額になりやすい傾向にある。対策としては、認証機能を強化することが有効である。たとえばインターネットバンキングサービスが、ログインの認証に ID、パスワードに加え SMS の認証や生体認証を要求する「多要素認証」を提供していれば、そうしたものを利用することが望ましい。

一方で、当社に寄せられた相談の中にはワンタイムパスワードを電話口で攻撃者から要求されて伝えてしまったというケースも見られ、「ワンタイムパスワードは家族を含め自分以外の人間に教えない」などの基本的なことも含め、改めてインターネットバンキングの利用のあり方を意識または注意喚起する必要がある。

(4) 考察

サポート詐欺に近い手口は 2010 年代初頭から継続して見られてきたが、2022 年から 2023 年にかけて昨年比 1.8 倍の認知件数という拡大ペースは目覚ましく、その背景には犯罪ビジネスの成熟化があるのではないかと考える。

IPA が毎年発表している「情報セキュリティ 10 大脅威（組織）」において、「犯罪のビジネス化（アンダーグラウンドビジネス）」が 2 年連続で 10 位にランクインする[8]など、サイバーセキュリティの分野では、犯罪者グループがサイバー攻撃を組織的に行っていることは、既に常識となっている。代表的なのは「ランサムウェア」と呼ばれる暗号化マルウェアで、このツール自体はダークウェブ上で定額課金サービスとして提供されていることが知られている。このように、犯罪者グループが犯罪ツールを販売することによって、技術的な知識がない者でもサイバー攻撃が可能になり敷居が下がってしまう。また、犯罪者グループは販売可能なビジネスとして犯罪ツールを開発しており、これが犯罪ツールの開発スピードを促進し、手口の多様化・悪質化に繋がっている。サポート詐欺においても同様に、偽サイトや侵害ツールのソースコード、またはオペレーションのノウハウ等が組織的にやり取りされ、それが本稿で見てきたような手口の変化に繋がったことが推測される。

一方、これだけ被害が拡大しているのは、組織や個人において未だ啓発や対策が十分でないということでもある。警察や IPA 等の諸機関による啓発活動もあり、「サポート詐欺」という言葉自体は浸透してきている。それでも被害に遭ってしまうのは、具体的な詐欺の手口と、それらに遭遇した時にどうすればよいかを一人ひとりが認識できていないということである。また、適切なセキュリティ対策を導入できていないという問題もある。これには費用が高額であること、セキュリティの専門知識が不足していること等が原因として考えられる。これまで見てきたように攻撃の手口が刻々と変化していることも、よりいっそう啓発や対策を難しくしている。

犯罪者グループはあたかも彼らのビジネスを改善させるように新たな手口を「改善」し続けており、今後更なる手口の悪質化や巧妙化も予期される。より大きな利益を求めて企業の口座やデータを標的とした攻撃にシフトしていく可能性も考えられ、企業においては以降に挙げるようなガバナンスと技術の両面から対策を講じることを強く推奨する。

3. 企業における対策

ガバナンス面の対策

□ 具体的な手口情報の共有

前述の考察で述べた通り、詐欺の具体的な手口と、遭遇時のアクションを個人に認識させることが啓発活動のゴールである。当社に寄せられた相談においては、金銭を窃取される前の段階でおかしいと気付き電話を切ったというケースも多く、どれだけ前の段階で、被害が進行する前に気づかせるかといったところで、具体的な手口情報の共有が肝要となる。諸機関が提供している下記のような啓発コンテンツも、積極的に従業員啓発等に活用されたい。

・IPA「偽セキュリティ警告（サポート詐欺）画面の閉じ方体験サイト」
https://www.ipa.go.jp/security/anshin/measures/fakealert.html
・日本サイバー犯罪対策センター「サポート詐欺の手口について（動画解説）」
https://www.jc3.or.jp/threats/examples/article-356.html

□ 事案発生時の連絡・対応体制の構築

遭遇時のアクションを認識させるという点においては発生時の連絡・対応体制の構築が重要となる。サポート詐欺に限らず、セキュリティ事案が発生した際の連絡体制や、対応体制を整備し、事態に遭遇した時にどのように行動するかを一人ひとりが認識できていることが重要である。

技術面の対策

□ インストールするソフトウェアの制限

サポート詐欺では、攻撃者が被害者の PC に遠隔操作ソフトをインストールさせる。また、接触フェーズにおける変化で触れたように、WEB ブラウザから知らずに不審な実行ファイルをインストールしてしまうことから攻撃に発展するケースもあり、業務 PC へインストールできるソフトウェアを制限することは、有効な対策である。

□ WEB ブラウザで閲覧可能な URL の制限

接触フェーズで紹介した通り、企業の運営する WEB サイト上でも詐欺サイトに誘導する広告が表示されることが報告されているものの、やはり海外のサイトやあまり管理されていないサイト、アダルトサイト等に表示された広告から詐欺サイトに誘導されるケースが依然多くなっている。アクセス可能な URL を制限することは事前対策として一定の有効性があると言える。

□ PC の中に機密情報を持たない環境を作る

遠隔操作フェーズにおいて、PC 上の情報を攻撃者に閲覧される、ファイルを操作・削除される懸念があることについて触れた。こうしたリスクの低減のために、従業員が PC 上に会社の機密情報を持たないような環境づくりが有効である。具体的には、機密情報を含んだファイルをクラウドストレージ上で管理するとし、個人が PC 上に保存することを禁止するなどが考えられる。

4. おわりに

本稿では、サポート詐欺の被害動向や最新の手口について考察し、企業において発生する情報漏えいや損失のリスク、企業がとるべき対策について述べた。

本稿では企業がリスクとして意識しにくいサイバー攻撃としてサポート詐欺を取り上げたが、サポート詐欺という一つの攻撃の種類に限らず、企業がサイバー攻撃のリスクを認識し、発生しうる被害を想定しそれに備えることが重要である。サイバー攻撃は、火事と同様に、どんな組織であっても何かのきっかけで巻き込まれてしまう可能性がある。サポート詐欺においても、「こんな詐欺に引っかかるわけがない」といった先入観を持たず、身近に起こりうる現実的な脅威として認識し、何かが起こった時に一人ひとりが冷静に対処できるよう、事前の対策を講じてほしい。

本稿が、貴社における社内での注意喚起や情報共有に役立てられ、リスクマネジメントへの意識を高めることに繋がれば幸いである。

[1] 警視庁「令和 5 年における特殊詐欺の認知・検挙状況等について（確定値版）」
https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2023.pdf （2024 年 2 月）
[2] IPA「情報セキュリティ安心相談窓口の相談状況［2023 年第 4 四半期（10 月～12 月）］」
https://www.ipa.go.jp/security/anshin/reports/2023q4outline.html（2024 年 6 月）
[3] トレンドマイクロ株式会社「「国内サポート詐欺レポート 2024 年版」を公開 ～2023 年は、100 万円を超える高額な金銭被害が複数発生～」https://www.trendmicro.com/ja_jp/about/press-release/2024/pr-20240425-01.html (2024 年 4 月)
[4] 読売新聞社 「サポートを装った怪しい警告にご注意を」https://www.yomiuri.co.jp/topics/20240719-SYT8T5591569/ (2024 年 7 月)
[5] IPA「サポート詐欺の偽セキュリティ警告はどんなときに出るのか？」
https://www.ipa.go.jp/security/anshin/attention/2023/mgdayori20240227.html (2024 年 3 月)
[6] IPA 「パソコンの画面全体に偽のメッセージが表示され操作不能になる手口が増加中」
https://www.ipa.go.jp/security/anshin/attention/2024/mgdayori20240917.html（2024 年 9 月)
[7] トレンドマイクロ株式会社「正規ツールを悪用し PC を操作不能にさせるサポート詐欺の新手口を解説」
https://www.trendmicro.com/ja_jp/research/24/j/support-fraud-new-technique.html （2024 年 10 月)
[8] IPA「情報セキュリティ 10 大脅威 2024」 https://www.ipa.go.jp/security/10threats/10threats2024.html (2024 年 7 月)

[2024 年 11 月 28 日発行]

東京海上ディーアール株式会社
サイバーセキュリティ事業部 主任研究員（専門分野：クラウドセキュリティ、インシデントレスポンス）
荒川 琴恵
〒100-0004 東京都千代田区大手町 1-5-1 大手町ファーストスクエア ウエストタワー23F
Tel. 03-5288-6580 Fax. 03-5288-6590 https://www.tokio-dr.jp/