事務所News
2024.9
K-061
発行：税理士法人グッドパートナーズ

経営バイタルの強化書 KEIEI VITAL

サポート詐欺の手口と対策について理解しましょう!

サポート詐欺レポート

近年 偽セキュリティ警告（サポート詐欺）の相談事例が増加傾向にあり、その手口も巧妙化してきています。表示された画面を通常の方法（ESCキーの長押し）で消すことのできない事例も増加してきており、被害にあうリスクも増えています。
サポート詐欺の手口と対処方法を理解しておきましょう。

1 サポート詐欺レポート

IPA（独立行政法人情報処理推進機構）は7月31日、情報セキュリティ安心相談窓口に寄せられた、偽セキュリティ警告（サポート詐欺）の相談内容や、独自の調査・検証等により把握した内容をまとめたレポート「サポート詐欺レポート」2024を公開しました※1。

このレポートは、IPA情報セキュリティ安心相談窓口に寄せられた「サポート詐欺」の相談内容や、独自の調査・検証等により把握した内容をまとめたレポートとなっており、主に情報セキュリティ関連の業務に従事されている方等に、サポート詐欺の手口や被害状況の実態を本レポートを通じて共有することで、被害低減や対策推進に資することを目的としたものですが、手口が巧妙になってきている「サポート詐欺」の被害にあわないためにその手口と対処方法を知っておくことが重要です。

このレポートは、

- サポート詐欺の手口
- 安心相談窓口に寄せられている相談件数の推移
- サポート詐欺の手口の実際の流れにおける変化と特徴
  - ・被害者が偽警告画面に接触する段階での変化
  - ・偽警告画面の変化
  - ・偽警告表示画面に施されている細工
  - ・電話番号の変化
  - ・オペレーターの対応
  - ・金銭的被害
- 2024年から急激に増加している、偽警告画面を表示するサイトへ誘導する広告の状況
- IPAの取り組み

の内容となっており、関連情報として

- 偽セキュリティ警告（サポート詐欺）に関する手口や対処、対策
- 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?
- 偽のセキュリティ警告に表示された番号に電話をかけないで!
- 会社や組織のパソコンにセキュリティ警告が出たら、管理者に連絡!
- 遠隔操作を他人に安易に許可しないで
- 偽警告画面を閉じる手順書
- 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

が公表されています。

2 サポート詐欺の手口と相談件数の推移

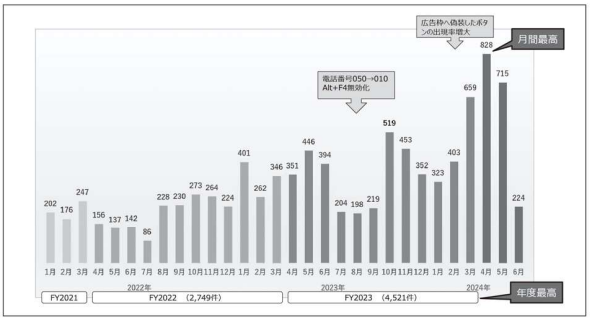
サポート詐欺の手口は、【図1】のようにインターネット閲覧中に偽の警告画面が表示され、画面を閉じるため等に表示されている電話番号へ連絡すると、遠隔操作で偽のサポートを受け、サポート料金を請求されるというものです。

請求金額を支払い、実際に被害にあってしまう事例は多くない状況にはありますが、通常の手段（ESCキー長押しやパソコンの電源OFF）で画面を閉じることができない事例が多くなっており、対処方法について理解しておくことが必要になっています。

サポート詐欺の相談件数は年々増加しており、2023年度は過去最高の4,521件の相談が寄せられており、今年4月には月間過去最高の828件の相談が寄せられています（【図2】）。

【図1】サポート詐欺の手口※2

【図2】サポート詐欺相談件数の推移※2



裏面へ続く→

3 偽のセキュリティ警告が表示される事例と対処方法

偽のセキュリティ警告が表示される主な事例としては、

- アダルトサイトの動画再生ボタンをクリック
- 不審な広告のクリック
- 不審なサイトに誘導する検索結果をクリック
- ブラウザの通知機能を悪用した偽のセキュリティ警告通知をクリック

等がありますが、URLの打ち間違い（タイポスクワッティング）を待ち構えて偽警告サイトへ移動し、アクセスすると、さまざまな詐欺サイトや偽サイトへリダイレクトされ、偽警告サイトへリダイレクトされる場合もあることが報告されています（【図3】）。

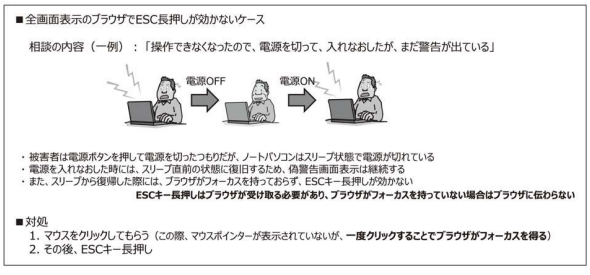
【図3】URLの打ち間違い（タイポスクワッティング）による事例※2

偽警告画面については、2023年～2024年にかけ徐々にその内容が変化していることが確認されており、具体的には画面の構成、視覚的効果、画面の閉じ方、表示される電話番号等が変わってきており、その手口が巧妙になってきているため、最新の情報を確認しておくことが重要となります。

偽警告画面が出てしまい、通常の対処で対応できない場合（[ESC]長押しが効かないケース）の対処方法としては、【図4】のようにマウスをクリックし、その後[ESC]長押しを行う方法や[Ctrl]+[Alt]+[Delete]キーを押して再起動する方法があります。

なお、ブラウザを再起動する際にページの復元を促すメッセージが表示されることがありますが、その場合は、「復元」をクリックしないで右上の「×」をクリックすることが必要となります。「復元」をクリックしてしまうと、ブラウザ終了時にアクセスしていたページを再読み込みしてしまうため、同じ警告画面が表示されてしまうことになってしまいます。

【図4】全画面表示のブラウザへの対処方法※2



4 相談事例と管理者、一般職員向けの対策

企業・組織で偽のセキュリティ警告に遭遇した相談事例と回答

IPAへ寄せられた相談は、企業や組織の場合、パソコン内の情報漏えいの有無を心配した相談が多くなっていますが、相手に電話をかけた後、指示に従い、パソコンを遠隔操作されたかどうかが、情報漏えいの可能性があるかどうかの分かれ目となります。

「電話をしなかった」、「電話をしたが遠隔操作を許可しなかった」事例

偽の警告画面を不審と感じて電話をしなかったため、情報漏えいの被害なし

事例1 会社のパソコンに「トロイの木馬に感染」と出て、ピーピー音がする。どうしたら良いか教えてほしい。

事例2 トロイの木馬に感染しているという警告が表示された。セキュリティソフトや機器も導入しているのに、検知されなかったようだ。電話はかけずに、その後、パソコンの電源は落としているが、パソコンの対処をどうしたら良いか教えてほしい。

回答 相手に電話をしなかったので、情報漏洩につながる懸念はない。

電話をかけてしまったが遠隔操作をされる前に不審と感じ電話を切ったため、情報漏えいの被害がなかった事例

事例3 会社で社員がパソコンを見ていたら、トロイの木馬に感染したと警告が出て電話をしてしまった。直ぐに電話を切ったので、遠隔操作はされていない。パソコンの対処をどうしたら良いか教えてほしい。

事例4 職員がパソコンで画像を取り込んでいる最中に、「ウイルス感染、トロイの木馬に感染しました」という警告とともに大音量の警告がなり、表示された050から始まる電話番号に電話をかけてしまった。電話には片言の日本語を話す外国人が出たので、この時点で職員は不審に思い、システム管理者である私に報告が上がってきたので、詐欺であることを説明し電話をすぐに切るように指示をした。

回答 電話をしても遠隔操作をさせなかったので、情報漏洩につながる懸念はない。

被害にあわないための管理者、一般職員向けの対策

管理者向け対策

- 社内、組織内で偽セキュリティ警告の手口について、周知、研修を行なう。
  周知・研修に際しては、〈IPAからの注意喚起等〉、〈他機関からの注意喚起等〉の情報を活用することが有用です。
- 偽セキュリティ警告に限らず、パソコンに異常があった場合の対応ルールを定めて徹底する。
  特に、テレワーク時に発生した異常の連絡や、管理者の許可なく業務用のパソコンを第三者に遠隔操作をさせないことを徹底することが重要です。

一般社員・職員向け対策

- パソコンにセキュリティ警告が出たら、対処を自分一人で判断せず、会社・組織の対応ルールに従い、落ち着いてシステム管理者（または上司）に連絡してもらう。
  冷静な対処が、職員自身、会社・組織の情報資産を守ることにつながります。
- 画面に表示された電話番号に電話をしない。
  システム管理者（または上司）の許可なく、相手からの遠隔操作の要求を許可しない。特に、パソコンの異常に対処するといったサポート名目の誘いには注意が必要です。

※1 サポート詐欺レポート（IPA）（URL：https://www.ipa.go.jp/security/anshin/measures/supportscam_report.html）
※2 IPA「サポート詐欺レポート」2024（PDF）（URL：https://www.ipa.go.jp/security/anshin/measures/f55m8k00000047km-att/supportscam_report2024.pdf）