社外秘

サポート詐欺に騙されるな！！

公社における情報システム使用に関する周知事項(令和6年度 その３)

番外編

企画総務課システム担当　広瀬

番外編　サイバー攻撃特集

サポート詐欺に気を付けたい理由

①ネットワーク・セキュリティ環境を問わない攻撃手法

サポート詐欺はネットワーク環境を問わず、いつどこで遭遇するかわかりません。

また、Webブラウザでのサポート詐欺画面表示はウィルス対策製品の守備範囲外であるため、高セキュリティ環境でも被害の抑止・軽減は見込めません。

②被害＝即インシデントな攻撃手法

サポート詐欺ではPCの操作権限をすべて攻撃者に渡すこととなるため、画面上で見える範囲以外にも何かをされている可能性があります。このため、そのPCを起点として考えられる最悪の事態を想定した対応を行う必要があります。

公社でも自宅でも、サポート詐欺は時と場所を選びません

正しい知識と認識で日頃から備えましょう！

社外秘

８月周知の資料より

社外秘

番外編　サイバー攻撃特集

爆増するサポート詐欺

流れのおさらい

サポート詐欺の流れは、概ね次のとおりです。

Webブラウザの画面上に「ウイルス検知」と「サポート窓口の電話番号」が全画面表示される

→ 電話をかけると攻撃者からパソコンにリモート接続できるソフトウェアのインストールを求められる

→ 攻撃者はリモート接続するとウイルスを駆除したフリをする

被害の類型

サポート詐欺による被害は、概ね次のいずれか、または全てです。

①ウイルス駆除の報酬として金銭を要求される

②リモート接続したパソコンまたはネットワークのデータを窃取する

（③リモート接続したパソコンまたはネットワークにマルウェアを感染させる）

社外秘

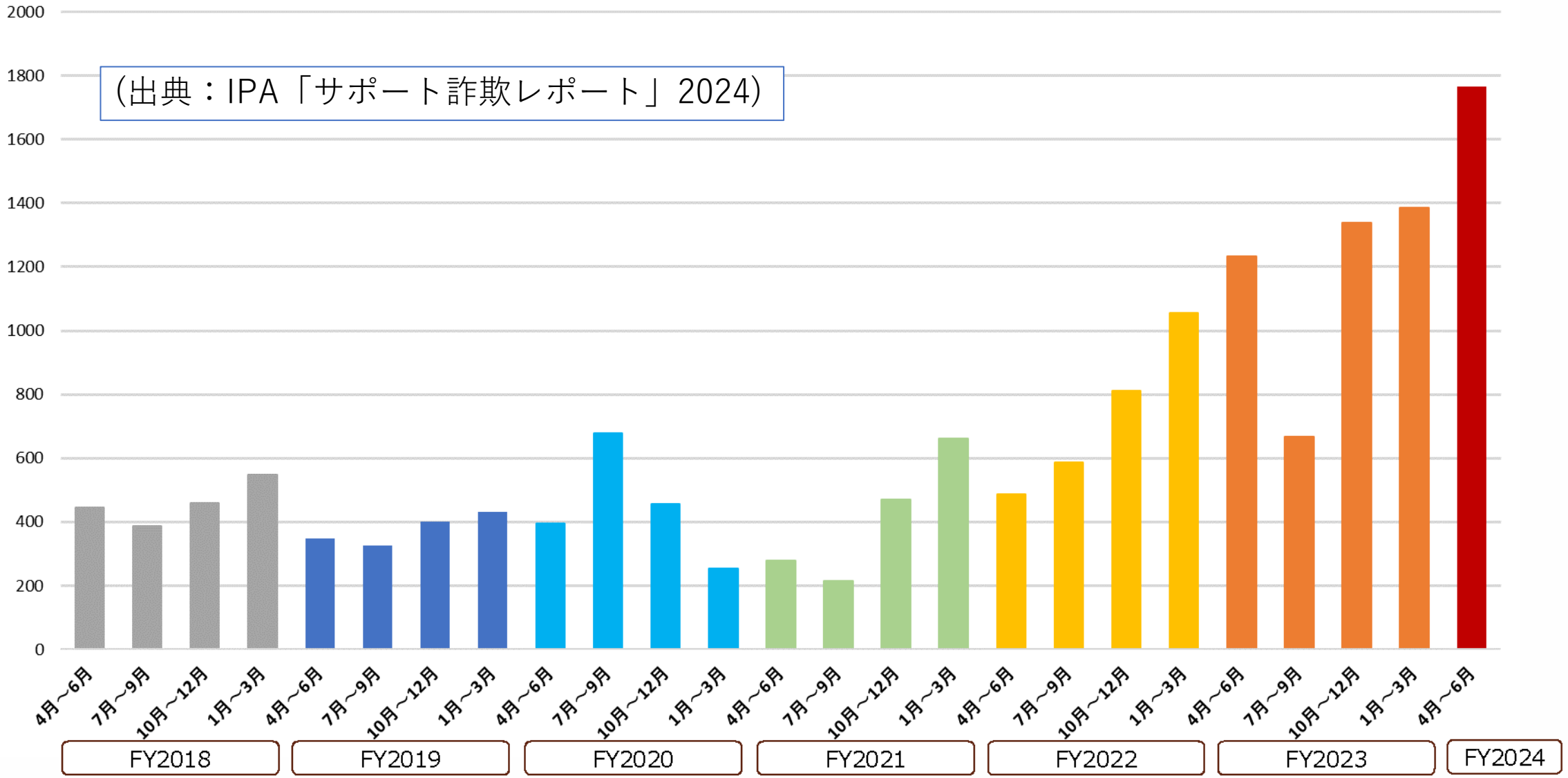
最近の実例


高度なオプ
スタートア
Windowsか
読み込み
スタートア
Windowsの
コマンド
のコマンドプロン
高度なトラブル
より多くの回復オプションを
この PC へのアクセスはセキュリティ上の理由からブロックされています。この PC にアクセスしたり再起動したりしないでく◆ さい。この基本的な警告を見落とすと、このフレー◆ ワークに関する情◆ ◆が失われる可能性があります。できる◆ け早くサポートに連絡してく◆ さい。Microsoft の専門家が電話で調査を案内します。このアプリケーションを実行すると、PC が危険にさらされる可能性があります。
Windows サポート: (050)-5050-1289
Windows ディフェンダー
セキュリティ上の理由により、この PC へのアクセスはブロックされています
スキャン
マイクロソフトディフェンダー
管理者ログイン
異常なアクティビティにより Windows がロックされました。
Microsoft ID とパスワードを使用して再度ログインしてく◆ さい。
サポートが必要な◆ ◆合は、Microsoft サポートにお問い合わせく◆ さい
(050)-5050-1289
ユーザー名
パスワード
ログイン
Windows セキュリティ
今スキャンして
後でスキャンする
Microsoft
Windows テクニカル サポート
(050)-5050-1289
(フリーダイヤル番号)
Windowsのセキュリティ Windows サポート (050)-5050-1289

社外秘

社外秘

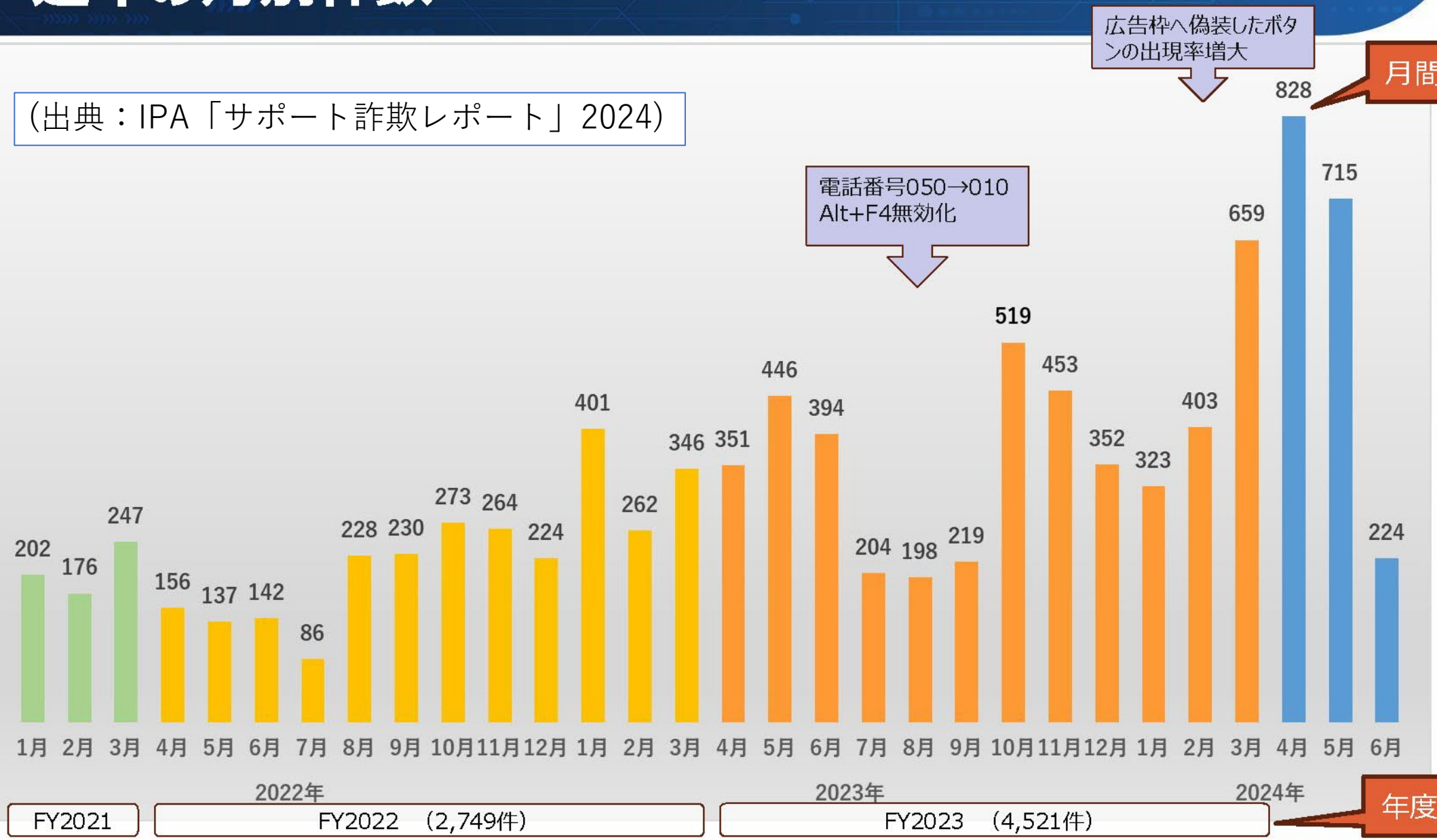
サポート詐欺の相談件数推移



社外秘

近年の月別件数

（出典：IPA「サポート詐欺レポート」2024）



番外編　サイバー攻撃特集

「弱り目に祟り目」な手口

こちらの動揺に付け込むサポート詐欺

サポート詐欺の画面は、被害者の感覚としては突然表示されます。

不意を突かれているうえに、基本的にマウス操作が受け付けられなくなるため、多くの人にとっては画面に表示されるサポート受付の電話番号が唯一の解決策に見えてしまいます。

怪しいはずなのに見抜けない？

偽の電話番号にかけるとあの手この手で不安をあおる相手の口車に乗せられます。

大抵のサポート詐欺はMicrosoft社のサポートスタッフを名乗りますが、偽の社員証などを提示して信じ込ませる手口もあるようです。

偽造社員証の一例
(出典：IPA「サポート詐欺レポート」2024)

社外秘

番外編　サイバー攻撃特集

サポート詐欺はいつ襲ってくる？

サポート詐欺が表示される瞬間

　サポート詐欺の画面は、被害者の感覚としては突然表示されますが、そのトリガーは大体悪意のURLをクリックした瞬間です。

　悪意のURLは多くの場合広告などのバナー画像に偽装して表示されています。

　中でも悪質な偽装バナーは「次へ」ボタンなどに偽装していることもあります。

悪意のURLをクリックしないためには

　まずはシンプルな原則ですが、Webサイトを閲覧する際は目的のページのみとし、広告バナーをたどる“ウィンドウショッピング”的な閲覧を控えることです。

　また、多くのWebブラウザではバナーを含めたリンクにマウスを合わせるとURLが画面左下に表示されるので、あまりに意味不明な文字列には用心しましょう。

よく見るバナー広告

スポンサード リンク

スポンサード リンク

社外秘

社外秘

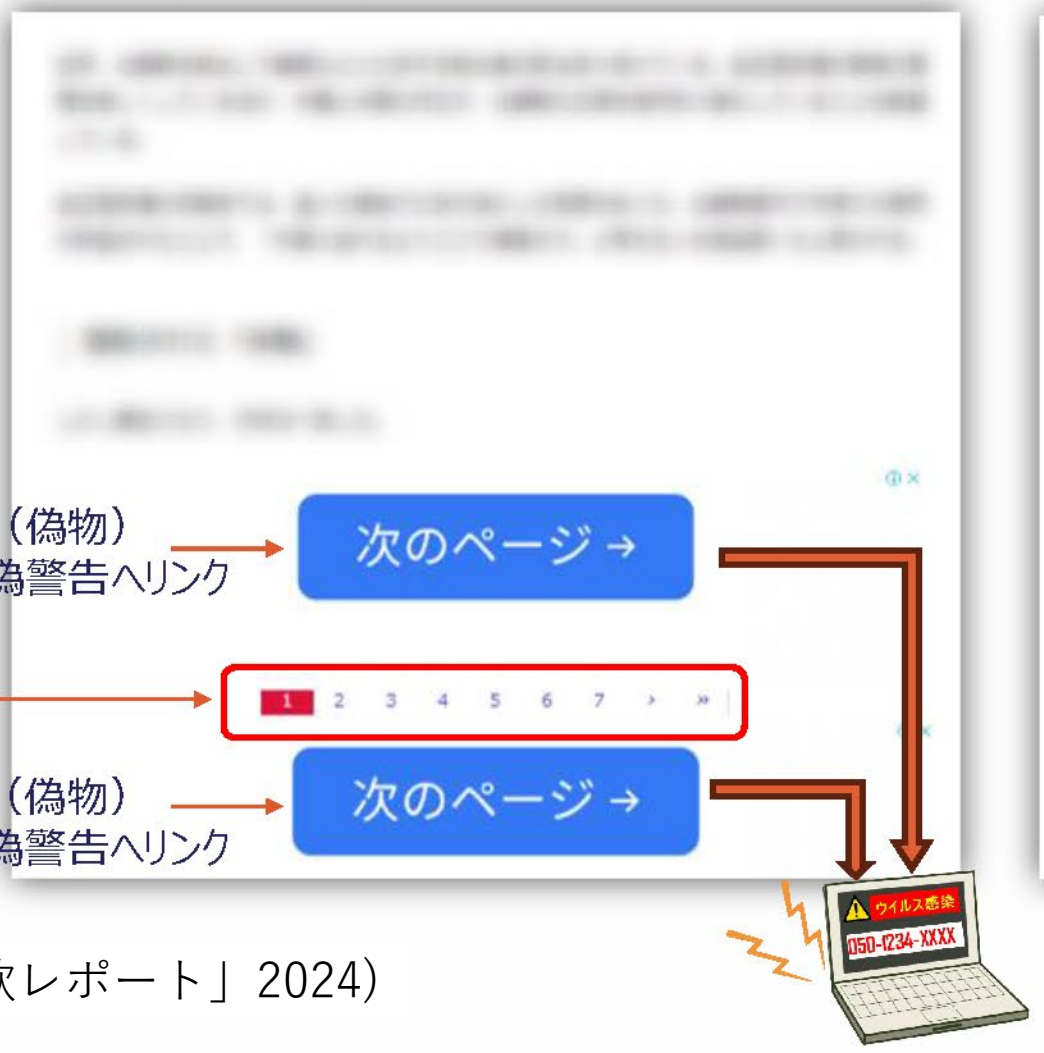
被害者が偽警告に接触する機会のいろいろ 3/7

一般のウェブページの広告枠（広告スペース・アフェリエイト）に
時世の話題や興味を惹くキーワードを画像化して表示

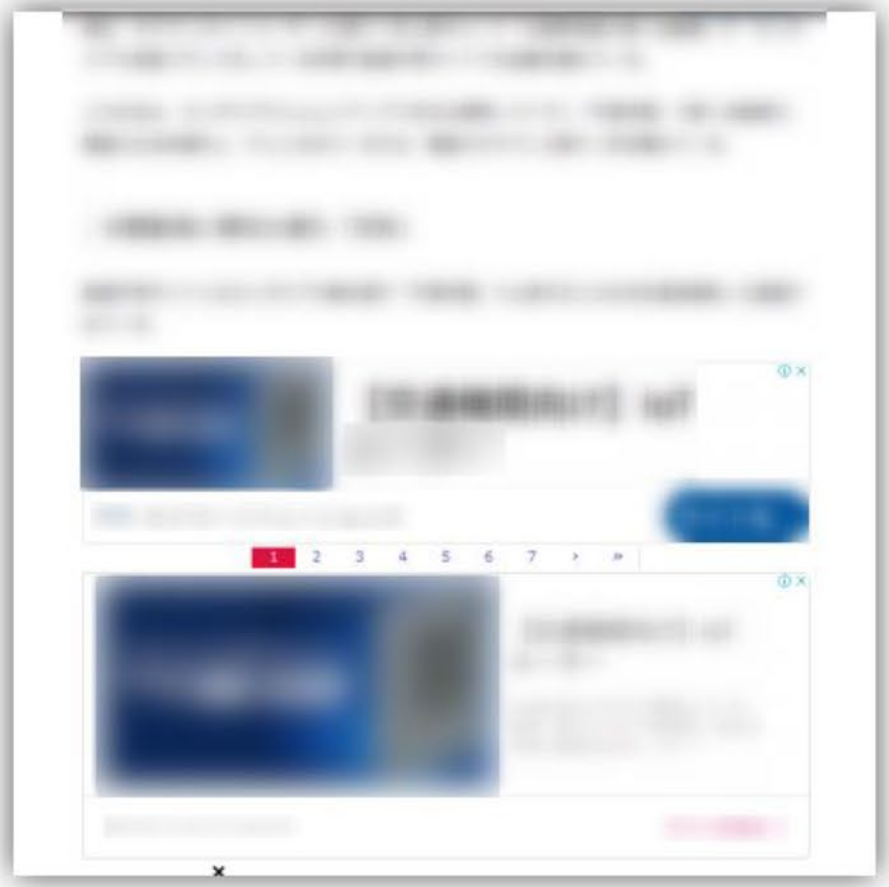
（出典：IPA「サポート詐欺レポート」2024）

被害者が偽警告に接触する機会のいろいろ 4/7

前ページと同じく広告枠に出現するもの。ウェブページの次のページや次のコンテンツへ進むボタンのように見せかけた画像



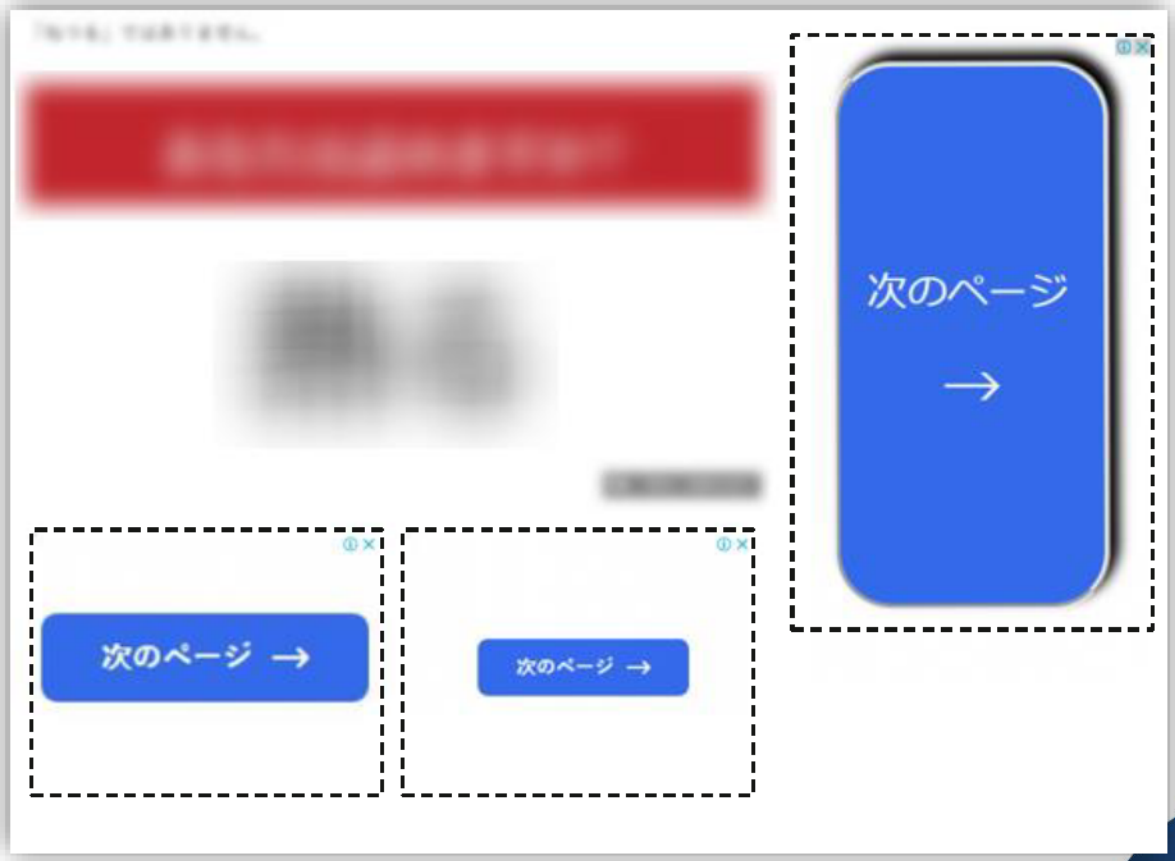
（参考）
同ウェブページで一般的な広告の表示例



（出典：IPA「サポート詐欺レポート」2024）

広告枠の判断

- 広告枠の右上（左下）には ⓘ ✕ の小さなボタンアイコンがある。左が情報ボタン、右が広告を閉じるボタン
- 広告枠の広告画像は矩形型であり、この右上のボタンアイコンが目安になる（右図）
- ボタンに似せた広告画像は、背景色の余白を多めに取ることで右上のアイコンから離れて見え、広告と判断しにくくなっている



(出典：IPA「サポート詐欺レポート」2024)

サポート詐欺による被害の一例

2024年2月

笛吹市商工会でインターネットバンキングを不正操作され約1000万円の被害(個人情報にもアクセス可能なPCだったとのこと)

2024年3月

焼津市の業務委託先事業者で海洋深層水購入者1万5000人分の氏名・住所・電話番号流出のおそれ(加えておよそ32万円も支払ってしまったとのこと)

2024年5月

近畿大学病院で患者約2000人分の氏名・診察情報が流出のおそれ

2024年10月

大手薬局チェーン通販サイトで約４万人分の氏名・住所等が流出のおそれ
→ その後の調査で個人情報が流出した事実はほぼ否定された

2024年11月

浦添市の市立小で約700人分の児童名簿情報が流出したおそれ

2024年12月

広島県の公立大で約3200人分の卒業生含めた生徒氏名が流出したおそれ

社外秘

前回(8月周知資料)**のおさらい**

○サポート詐欺が表示されたら

　サポート詐欺も表示された時点では原則無害です。まずは落ち着いてPCの背面からLANケーブルを抜き、速やかに企画総務課までご報告ください。

　絶対に表示されている電話番号にかけないでください。

○その他に「サイバー攻撃かも」と思ったら

　公社のネットワーク環境下では、サイバー攻撃はLANケーブルでのみ感染拡大が可能です。そのため、何かしらサイバー攻撃が疑われる事象がありましたらまずはLANケーブルを抜き、その後に企画総務課までご報告ください。

引き続きご協力をお願いします。

社外秘

前回いただいたコメントから

ごもっとも！

「LANケーブルは勝手に抜いてはいけないと思っていた」

「LANケーブルは絶対に抜き差しするなと言われたことがある」

なぜ？

某官公庁を例に考えてみます

①重要な業務系のケーブルかもしれないから

同じフロアに職員用PCと業務用PCが混在している場合、誤って業務系のケーブルを抜いてしまうと業務全体がストップする可能性があります。

②違うネットワークに接続するかもしれないから

①に似た内容ですが、異なるネットワークのケーブルが混在している場合、正しいネットワークの装置に接続しないとPCが正しく動作しません。

③ループ配線になるかもしれないから

ループ配線とは「同じLANケーブルの両端が同じスイッチングハブに接続される」ことで、これによって異常なデータ送信が行われ、そのネットワークがダウンする可能性があります。

恐るべき“ループ配線”(イメージ)

社外秘

番外編　サイバー攻撃特集

自宅でサポート詐欺に遭遇したら

サポート詐欺は時と場所を選びません

サポート詐欺による金銭被害の多くは自宅で発生しています。

自宅のパソコンなどで突然ウイルス感染などの画面が表示されたら、まずは落ち着いてサポート詐欺を疑い、次の手順で画面の消去を試みましょう。

【画面消去の方法】

これでダメなら…

① “Esc”キーを長押しする(最低5秒程度)
→画面の最大化が解除されたら問題のタブかブラウザを終了する

② “Ctrl”＋“Alt”＋“Delete”キーを同時押ししてタスクマネージャーを呼び出す
→タスクマネージャーからWebブラウザを終了する

普段から自宅のパソコンにインストールされているソフトウェア(特にセキュリティ関連)を把握しておくことも重要です。

社外秘

番外編　サイバー攻撃特集

自宅でサポート詐欺に遭遇したら

サポート詐欺は時と場所を選びません

サポート詐欺による金銭

ち

らちが明かなければ
警察へ電話しましょう

問題のタブかブラウザを終了する

“Ctrl” + “Alt” + “Delete”キーを同時押ししてタスクマネージャーを呼び出す
→タスクマネージャーからWebブラウザを終了する

普段から自宅のパソコンにインストールされているソフトウェア(特にセキュリティ関連)を把握しておくことも重要です。

社外秘

ついに出た！
これがトレンドマイクロのアラート画面だ！

幸いにして誤検知のアラートでした

社外秘

動画のサポート詐欺対策で使用したWebサイトです。
「サポート詐欺　体験」などで検索すればトップに表示されることと思います。

図3：「ESCキー」を長押しすると、「閉じるボタン」が現れる。「閉じるボタン」で画面を閉じて体験を終了

3. 体験サイトへ移動

下記の「偽セキュリティ警告画面の閉じ方体験サイト」をクリックして、体験サイトへ移動します。

偽セキュリティ警告画面の閉じ方体験サイト

サポート詐欺特有の「全画面化されてマウス操作が受け付けられない」Webページを疑似体験できるサイトです

4. 関連情報

偽セキュリティ警告に関する手口や対処、対策は以下のページをご覧ください。

- パソコンに偽のウイルス感染警告を表示させるサポート詐欺に注意
- 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

ページの先頭に戻る

（出典：IPAホームページ　https://www.ipa.go.jp/security/anshin/measures/fakealert.html）