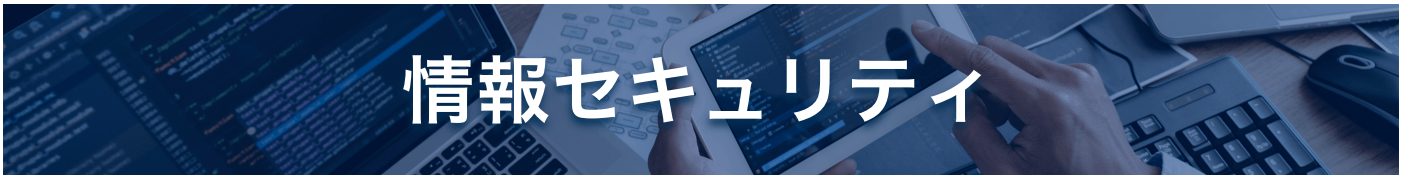

偽のセキュリティ警告によって有償の「ソフトウエア購入」や「サポート契約」をしてしまう相談が増加中

公開日：2018年7月18日
最終更新日：2023年11月21日
独立行政法人情報処理推進機構
セキュリティセンター

偽のセキュリティ警告によって有償の「ソフトウエア購入」や「サポート契約」をしてしまう相談が増加中
- インターネット利用中に表示される偽の警告画面にだまされないで！-

注釈：2021年11月16日追記

本手口については、下記の安心相談窓口だよりが最新となりますので、そちらもあわせてご確認ください。

2021年11月16日：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！

IPAでは2006年5月に「偽セキュリティソフト」の手口について初めて注意喚起を行いました。（脚注1）この手口は「パソコンがウイルスに感染している」等、偽の警告画面をパソコンに表示させ、最終的に有償ソフトウエアの購入に誘導するものです。その相談件数に増減はあるものの、現在も継続して相談が寄せられています。

（有償ソフトウエアの購入に誘導）

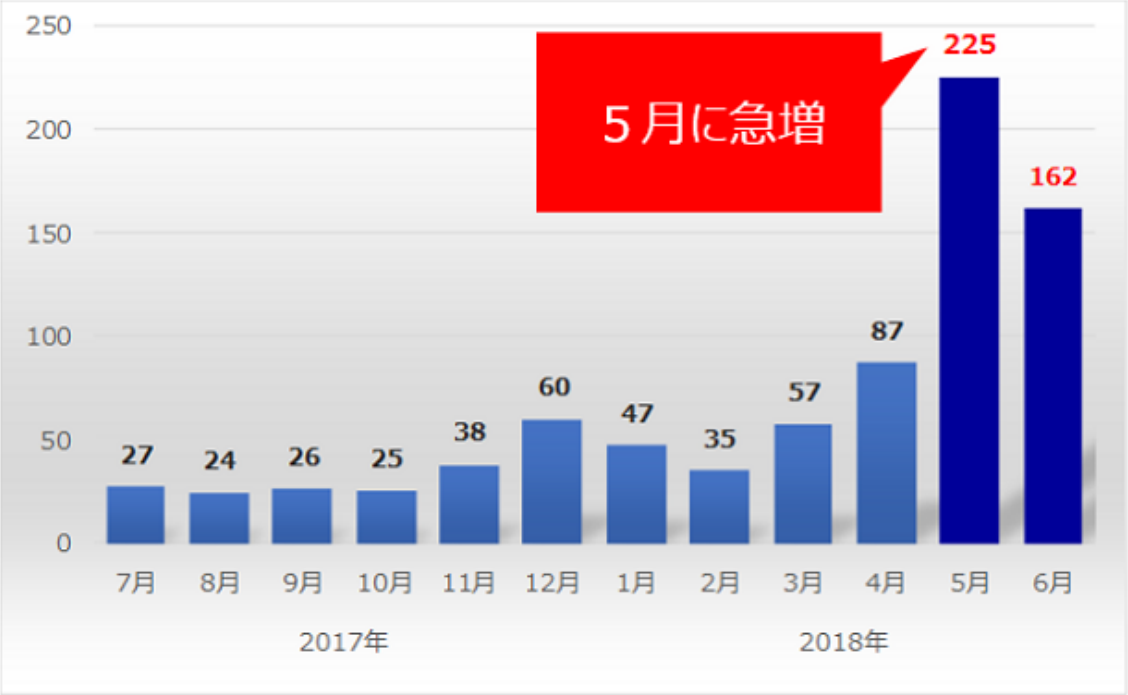

図1.IPAに寄せられた偽セキュリティソフトに関する相談件数の推移

また、2016年6月には同様に偽の警告画面をパソコンに表示させ、画面に記載されている連絡先に電話をかけさせ、オペレーターの遠隔操作による有償サポート契約へ誘導する、「偽警告」の手口について注意喚起を行いました。（脚注2）この手口に関しても、継続して相談が寄せられています。

（有償サポート契約へ誘導）

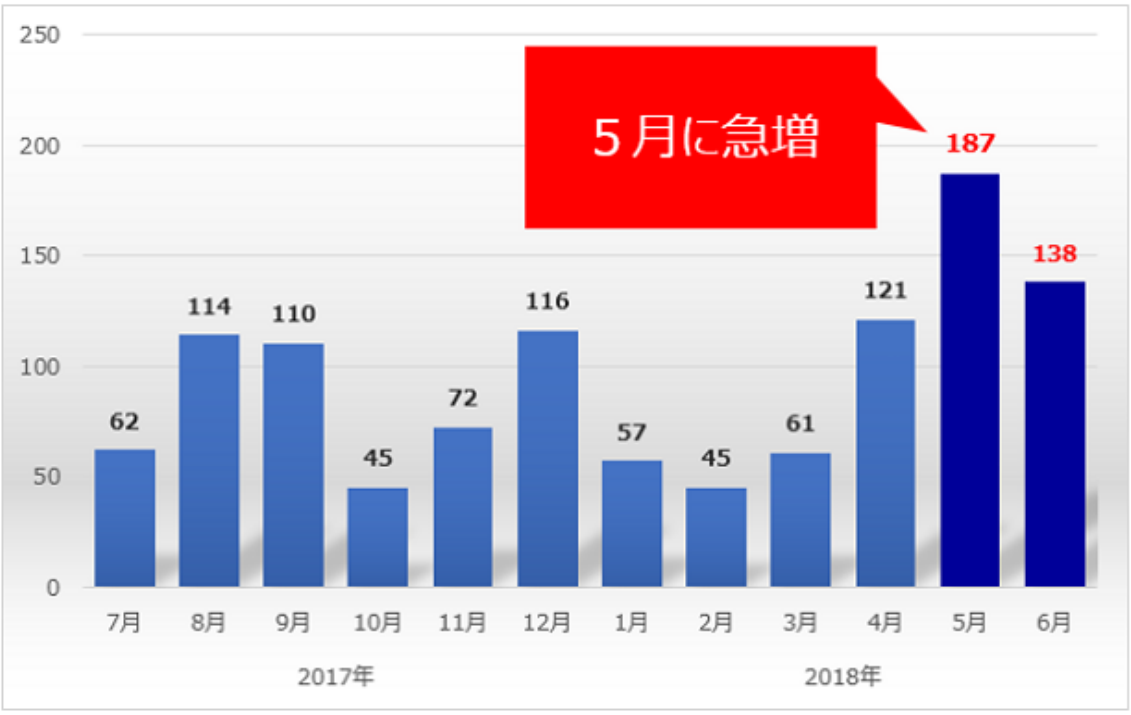

図2:IPAに寄せられた偽警告に関する相談件数の推移

両手口の相談件数は、2018年5月に急増し、6月も引き続き多い状況です。

(脚注1)「セキュリティ対策ソフトウエアの押し売りに注意！！」
「その警告表示はソフトウエア購入へ誘導されるかも知れません」

(脚注2) 「偽警告で、また新たな手口が出現」

手口の複合化
2017年の年末頃より、上記の二つの手口が複合化された相談が確認されるようになりました。

「パソコンがウイルスに感染している」等、偽の警告画面から有償ソフトウエアの購入に誘導し、さらに電話をかけさせたうえで、遠隔操作による有償サポート契約の誘導も併せて用いるなど、です。

そこであらためて、これらの手口と、被害にあわないための対策について、実際の画面例を交えて紹介します。

1．両手口における警告画面の表示例とその対処

突然表示される警告画面

両手口は、ウェブサイトの閲覧中に突然「お使いのコンピューターはウイルスに感染しています」「Windowsのシステムが破損します」「～個のシステムの問題が見つかりました」「～秒以内に対応しないとデータが全部削除される」等というようなポップアップやサイトの警告画面が表示されることからはじまります。（図3）

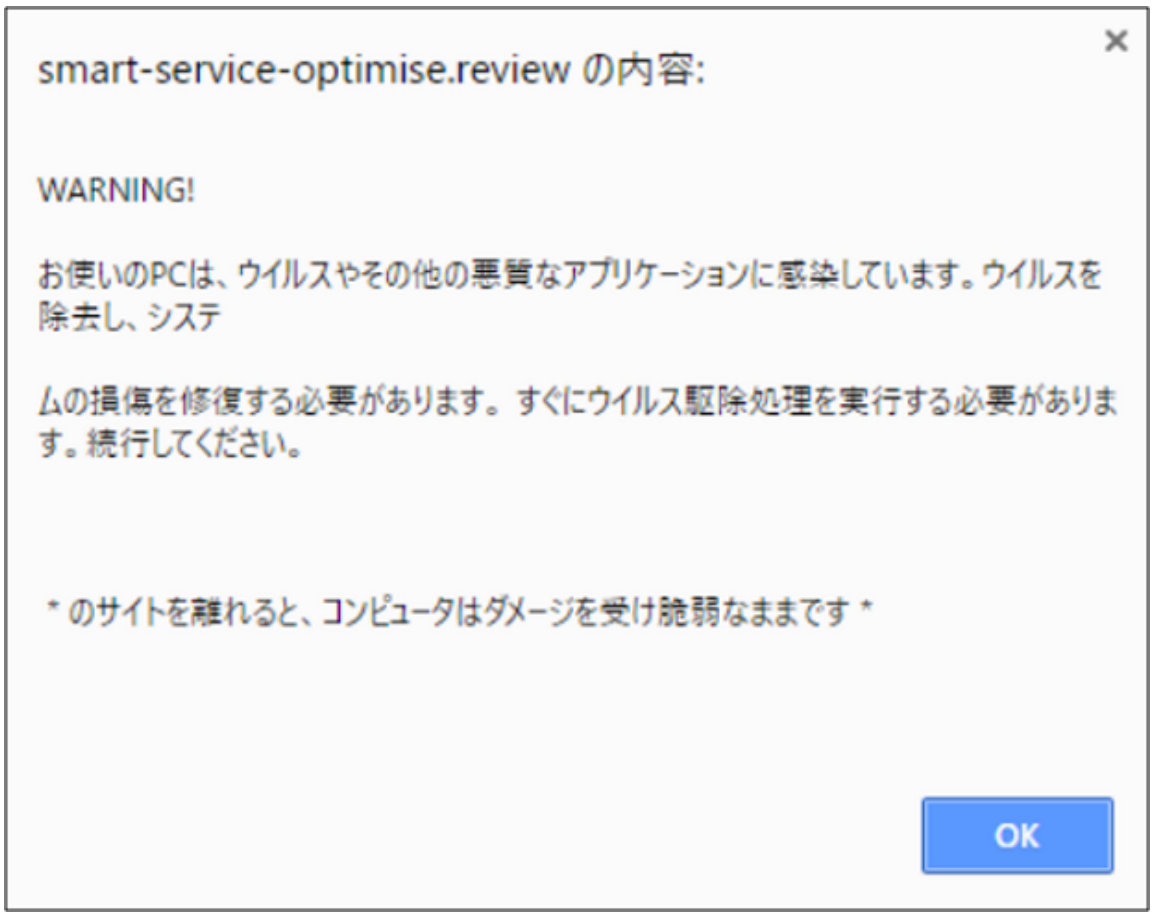

図3.偽警告のポップアップ画面例

また、その際には警告音や警告メッセージを音声で流して不安をあおることが確認されています。さらに、相手を信用させるため、その画面に実在の企業のロゴが使われていることも確認しています。（図4）

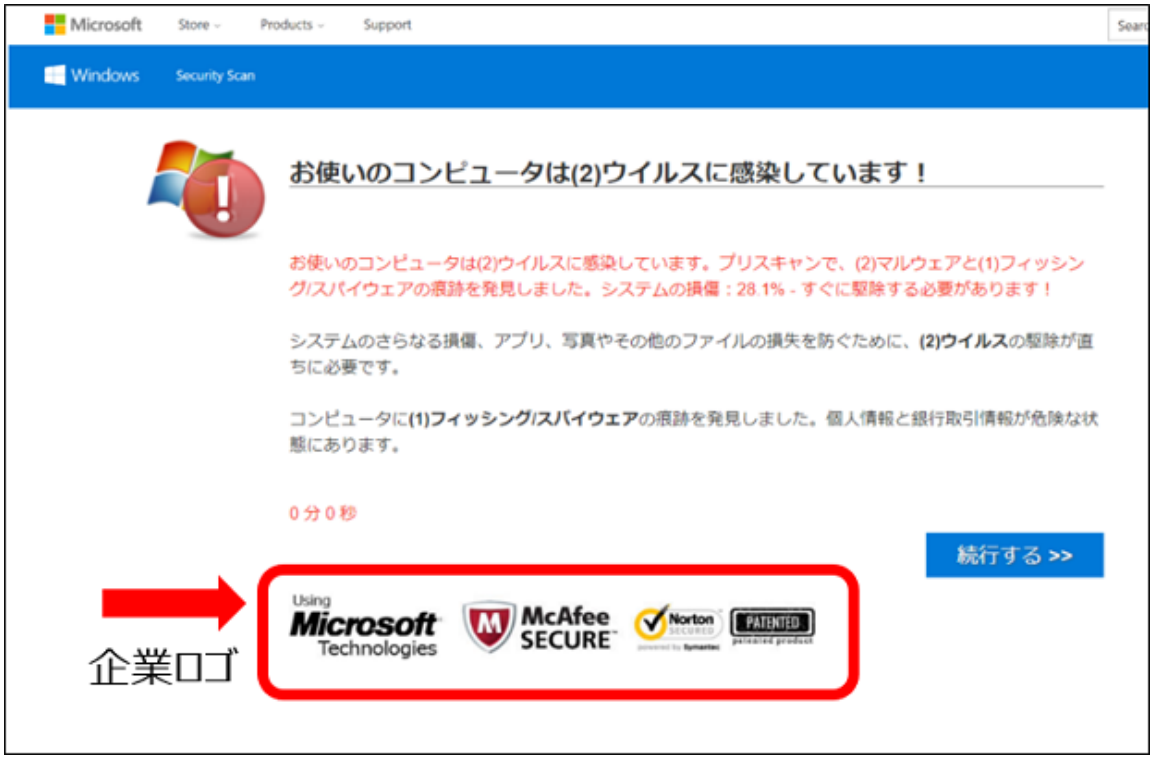

図4：ロゴの無断使用例

このような警告表示や本物と見まちがう画面により、パソコンの修復が必要と思わせ、セキュリティソフトをダウンロードするように仕向けます。

IPAが確認した限り、これらのセキュリティ警告ではいずれも実際のウイルス感染はなく、ポップアップメッセージ等を偽の警告画面として繰り返し表示させているに過ぎないことが分かっています。また、マイクロソフト社等のロゴマークが表示されていますが、この場合それら企業とは関係がありません。当該企業が提供する正規のサービスとみせかけるために、実在の企業のロゴが使われ、もっともらしく見せかけていると思われます。

誰でも偽の警告画面に遭遇する可能性

この手口は、ウェブサイトで広告が表示される仕組みを用いて、偽の警告画面を広告として仕込むことにより表示させていると考えられます。よって、インターネットでウェブサイトを閲覧していれば誰でも遭遇する可能性があり、事前に仕込まれているウェブサイトを判別することは困難です。

対処は画面を閉じるだけ

この現象は実際のウイルス感染によるものではありません。偽の警告画面を閉じるだけで問題は解消されます。画面が消せない場合は、ブラウザを強制終了するか、パソコンを再起動してください。

偽警告画面を閉じる手順書(PDF:833 KB)

2. 警告画面を信じて操作を進めてしまった場合に出現する画面例

偽の警告画面を信じてしまい、操作を進めてしまった場合に出現する画面例(一部)とその順番を解説します。なお、これらの画面例や順番は一例であり、実際には、類似した複数の異なる手順、画面が存在します。

(1) 無料セキュリティソフトのインストールに誘導される

警告に対する解決方法として、無料のセキュリティソフトをインストールするよう誘導されます。ソフトウエアをインストールすると、ここでもパソコンに問題が見つかった（ウイルス感染等）という診断結果が表示されます。（図5）しかしこのソフトウエアが実際にパソコン内を適切に検査（スキャン）しているかは不明です。

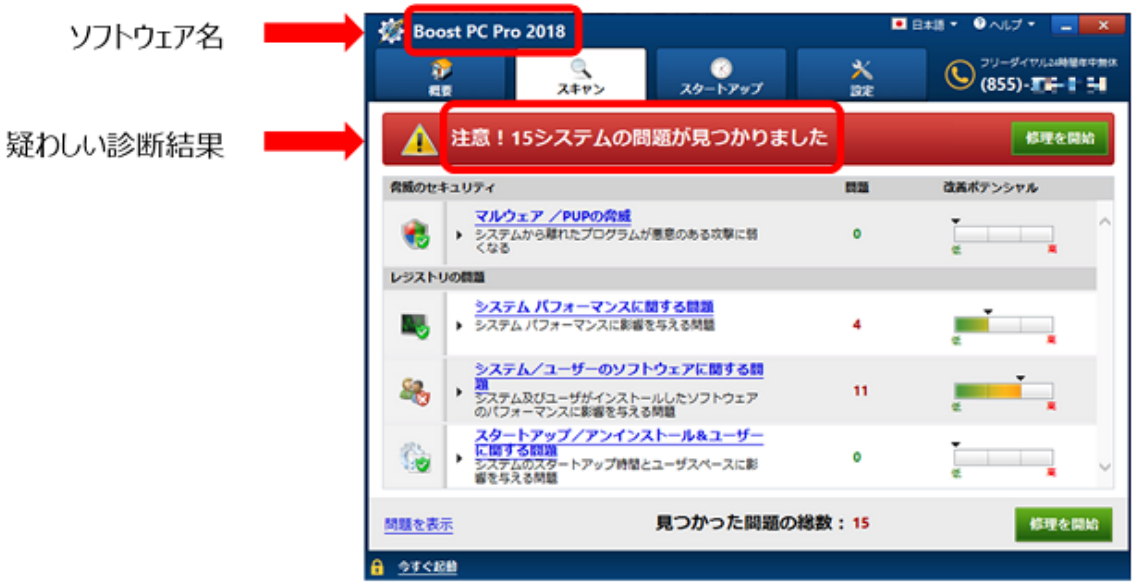

図5：検査（スキャン）結果表示の画面例

2018年7月5日時点で相談の多いセキュリティソフト等の名称は下記の通りです。

・Auto Fixer Pro 2018（Windows）
・Auto Mechanic 2018（Windows）
・Speedy PC Pro 2018（Windows）
・Boost PC Pro 2018（Windows）
・Identity Protector（Windows）
・Smart PC Care（Windows）
・Advanced Mac Cleaner（Mac）
・Mac Keeper（Mac）

(2) 有償版セキュリティソフトの購入とインストールを誘導される

スキャン結果の問題を解決するためとして、クレジットカード支払いによる有償のセキュリティソフトの購入へと誘導されます。この時、氏名、電話番号、メールアドレスなどの個人情報の入力も求められる場合が多いことが確認されています。（図6）

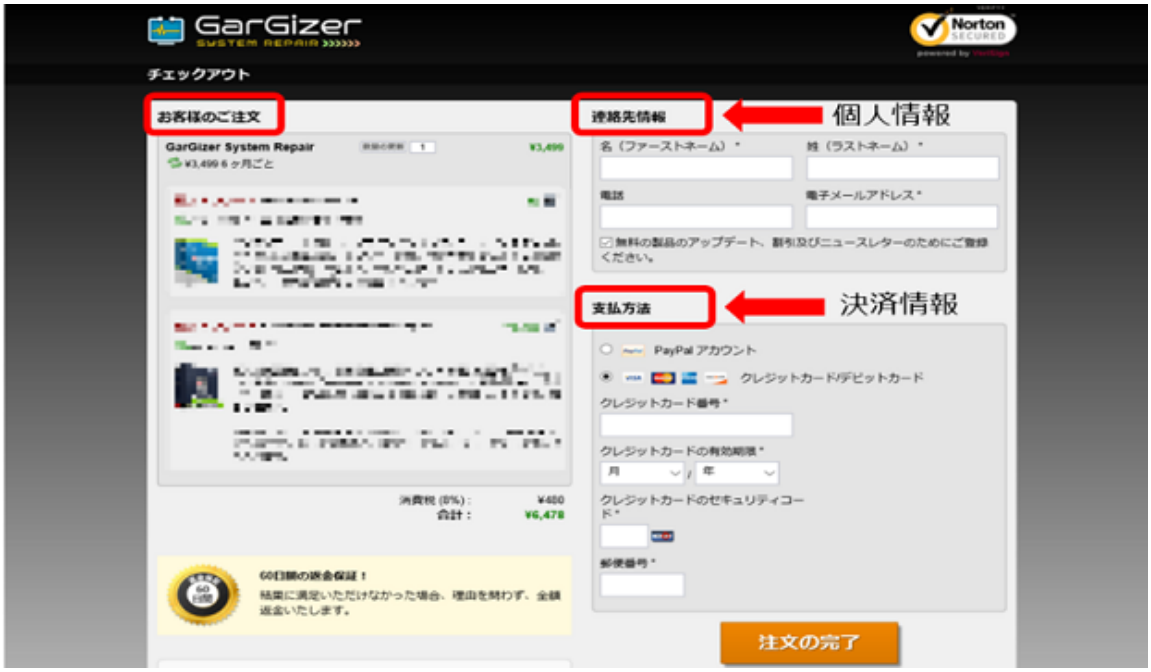

図6：クレジットカード決済の画面例

(3) 購入したセキュリティソフトウエアの使用を可能にする操作（有効化）のために電話をかけるよう誘導される

購入した有償版セキュリティソフトをインストールすると、“ソフトウエアの使用のため、アクティベート（有効化）が必要”と電話番号と共に表示され、電話をかけるように仕向けられます。（図7）

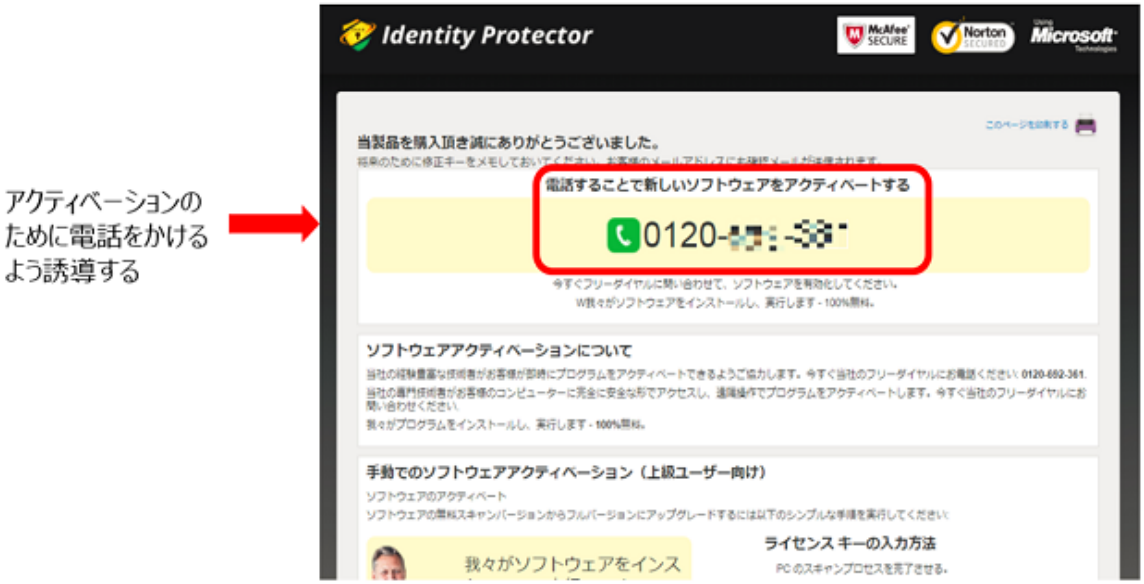

図7：電話番号表示の画面例

(4) 遠隔操作によるサポート作業を誘導される

記載の番号へ電話をかけると、サポート業者を名乗る外国人オペレーターが出て、片言の日本語で「あなたのパソコンには問題があるので、より詳しく調べるために遠隔操作でのサポートが至急必要」等の説明を行います。そして遠隔操作ソフトのインストールへと誘導し、そのソフトウエアを使って、1、2時間程度遠隔操作によるサポートと称する作業を行います。その際に別のソフトウエアをインストールするようなケースも確認されています。なお、この遠隔操作によるサポートにおいて、パソコンに問題がある証拠として、いくつかの画面が示されることがあります。しかし、その画面はパソコンのウイルス感染等とは無関係と考えられます。あたかも問題があるように見せかけ

る材料に過ぎません。

(5) 有償サポート契約を交わすように誘導される

サポート業者は遠隔操作でパソコンの操作を行ったあと、その場で実施したサポートの作業費や、その後の年間サポート料金（1年から3年程度）の契約を持ちかけてきます。金額は数万円で、支払い手段はクレジットカード決済やコンビニ決済です。また、サポート対応中に電話を一度切って、数時間後に再度電話をかけてきて契約を持ち掛けるケースも確認されています。

3. 被害に遭わないための対策

偽の警告画面のメッセージを見極める

・自分が普段から利用しているセキュリティソフトによる警告ではない場合、特にインターネット利用中にブラウザ画面上に表示される警告は偽である可能性が高いと考えられます。このような場合、画面の指示に安易に従わないようにしてください。
・偽と思われる警告画面が表示された場合は、画面を閉じてください。
・偽警告画面かどうかの判断が難しい場合は、画面をそのままの状態にしてIPAの安心相談窓口へご相談ください。

セキュリティソフトはダウンロードもインストールもNG

・インストールしてしまった場合の対処は「4. セキュリティソフト等をインストールしてしまった場合の対処」を参照してください。

電話をかけない

・表示された電話番号に電話をかけてはいけません。一度でもかけてしまうと、電話番号が相手に伝わってしまい、後で相手からかかってくる場合があります。その電話には出ないようにしてください。

購入・契約しない

・セキュリティソフトやサポート業者の信頼性が判断できない場合は、購入や契約は行わず、IPAの安心相談窓口や消費生活センターに相談して下さい。

4. セキュリティソフト等をインストールしてしまった場合の対処

もし、セキュリティソフト等をインストールしてしまった場合は、ソフトウエアのアンインストールが必要です。しかし、それらのソフトウエアを一旦インストールしてしまった場合の、パソコンへの影響の有無は不明です。よって、より安全な対策として、「システムの復元 」を行い、ソフトウエアをインストールする前の状態にパソコンを戻すことを推奨します。「システムの復元」が実行できないなどの場合はパソコンの初期化を推奨します。

「システムの復元」の実施手順書(PDF:525 KB)

5. その他のよくある質問

本手口において、上記以外のよくある質問は次のとおりです。

質問(1)

遠隔操作をされてしまったが、情報漏えいした可能性はないか。	パソコン内の情報を盗み見られてしまった可能性は考えられます。ただし、遠隔操作内容は、マウスのポインタの移動をはじめ、ファイルやフォルダのクリックなど目の前のパソコン上でリアルタイムに表示されます。そのため、遠隔操作中のパソコンの動きが目に見えて特に不審でなかったのであれば問題はないと言えます。

質問(2)

言われるがまま遠隔操作ソフトをインストールしてしまったが、今後も遠隔操作されてしまうことはないか。	遠隔操作ソフトを用いてパソコンの遠隔操作を成立させるためには、下記の3つの条件を満たす必要があり、知らないうちに遠隔操作されてしまうということはありません。 1. 「操作される側」のパソコンに遠隔操作ソフトがインストールされ、サービスが有効（ソフトが起動していて遠隔操作可能状態）となっている 2. 「操作される側」のパソコンがネットワークに接続され、通信が可能となっている 3. 「操作される側」のパソコンのIPアドレスや遠隔操作ソフトを利用する際のアカウント情報（ID、パスワードなど）を「操作する側」が知っていて、操作時に、操作される側が操作を許可した場合 不安を感じるようであれば、遠隔操作ソフトをアンインストール（条件1.の排除）することを推奨します。 （ご参考） 意図せずにインストールしてしまったプログラムをアンインストールする際の手順(PDF:560 KB)

質問(3)

ソフトの購入やサポート契約は取り消しできるのか。	最寄りの消費生活センターに相談してください。 （ご参考） ・全国の消費生活センター等（電話：局番なしの188）

お問い合わせ先

IPAセキュリティセンター 情報セキュリティ安心相談窓口

E-mail　anshin@ipa.go.jp
URL　情報セキュリティ安心相談窓口

記載されている製品名、サービス名等は、各社の商標もしくは登録商標です。

更新履歴

2023年11月21日	『「ウイルスを検出した」という旨の警告が表示されてブラウザを終了させることができない場合の対応手順』を『偽警告画面を閉じる手順書』に改訂
2021年11月16日	最新の安心相談窓口だよりの案内を追記
2018年7月18日	掲載