新連載
第１回

こんなときどうしたら?
インターネットのセキュリティガイド

偽警告

独立行政法人 情報処理推進機構（IPA） 技術本部 セキュリティセンター

インターネットは急速な発展を遂げ、今では誰もがパソコン・スマートフォンなどで利用できる時代となりました。インターネットを通じた情報のやり取りを、私たちは当たり前のように行っています。便利な一方、サイバー空間上で行われる攻撃は遠い世界の話ではなく、私たちの身近で起こり得るものとなりました。

本連載では、情報処理推進機構（IPA）に寄せられた相談や事例の手口について、対策とともに解説していきます。第1回目では、最近被害が多く確認されている、偽の警告画面を表示させる手口について解説します。

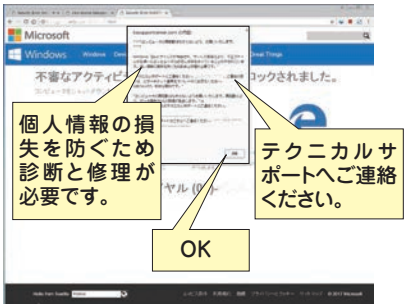
偽の警告画面を表示させる手口

パソコンやスマートフォンでウェブサイトを閲覧していると、突然音声案内や警告音とともに「ウイルスが検出された」「システムが破損している」といった文言で偽の警告画面が表示されます。これらの警告画面には何の根拠もありませんが、動揺した人が慌てて行動することにより次のような被害にあいます。

●偽警告（別名：サポート詐欺）

表示されている電話番号に電話をかけると、パソコンを遠隔操作され、修復や保守と称して高額の契約をさせられる（図 1）。

図 1 偽警告の画面例



●偽対策ソフト（別名：偽セキュリティソフト）

セキュリティ対策と称して必要のないソフトウェアを購入させられる（図 2）。

図 2 偽対策ソフトの購入画面例

●アプリ誘導（スマートフォン）

セキュリティ対策と称して必要のない無料アプリをインストールさせられる（図 3）。

図 3 アプリ誘導の画面例

画面例から分かるように、実在する企業名や企業ロゴを見せることで、あたかも本物であるかのように思わせています。ただし、画面内のメッセージをよく読むと日本語が不自然です。

ここで、2018年5月に確認された実例を見ていきましょう。

［パソコンの事例］

①偽の警告画面が表示される

インターネットを見ていたら、突然、警告画面がポップアップ*1として表示された（図1）。画面には警告メッセージや「OK」などのボタンがある。「×」ボタンで画面を閉じたくても、なぜかボタンが押せない。

しくみとしてポップアップが表示されると、画面の「×」ボタンなどは押せなくなります。先にポップアップを閉じると、「×」ボタンが押せるようになりますが、一度閉じても、再度表

＊1 ウェブサイトなどで自動的に表示される最前面の画面のこと。または、そのしくみのこと。

示させるしくみにすることで、ポップアップ自体が閉じられなくなった、と思わせます。

②無償のソフトウェアをインストール*2

パソコンを修復するように、という画面表示に促され、無償のソフトウェアをダウンロード*3して、インストールした。ソフトウェアを実行すると、スキャン結果が表示された。

実際にスキャンしているかどうかは不明で、スキャンしているかのようなアニメーションを見せているだけかもしれません。

③有償のソフトウェアを購入

スキャン結果の画面に、問題を解消するためには有償のソフトウェアの購入が必要だと書かれていたので、クレジットカードで購入した。

購入画面ではクレジットカード決済だけに限定され、他の決済方法が選択できないようになっていることが多いです。

④電話をかけさせる

クレジットカード決済完了後、購入したソフトウェアをアクティベート*4するよう電話番号が表示されたので、電話をかけた。

⑤電話で遠隔操作

サポート業者は「より詳しくパソコン内を調べるため」と言って遠隔操作の実施を提案してきた。提案を受諾すると、遠隔操作用のソフトウェアをインストールするよう指示された。そして、遠隔操作でさまざまな画面を表示し、パソコンが危険な状態だと伝えてきた。

遠隔操作用のソフトウェア自体は一般的に使われていて、不正なソフトウェアではありません。業者は遠隔操作を通して、次のような操作をします。

・コマンドプロンプト*5から「netstat」などを実行する（**図4**）。
・イベントビューアーの管理イベントを表示して、エラーログを見せる（**図5**）。

技術的な操作内容のため、知識のない消費者は専門的な調査をしていると思い込んでしまいます。例えば、サポート業者はコマンドプロンプトの実行結果で表れた数値を「ウイルスが発見された数」と言って、次にイベントビューアーのエラーログを見せて「だから、こんなにエラーが出ている」と言います。しかし、これらの操作はウイルスを発見する方法ではありません。「netstat」などのコマンドはパソコン環境の状態を表示するものであり、数値もウイルスを示していません。エラーログについても、パソコンを使用するうえで気にする必要がないほど影響の小さいエラーです。

⑥サポート契約を持ちかけられる

サポート業者は遠隔操作を一通り終えると、1年間で何万円といった内容の保守サポート契約を持ちかけます。

図4 「netstat」コマンドの実行結果例*6

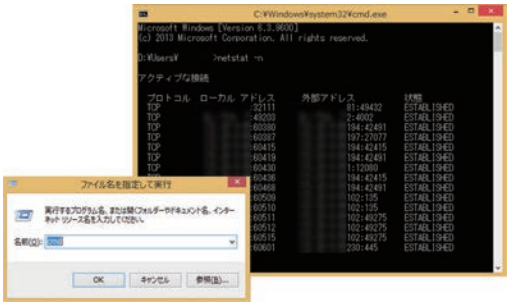
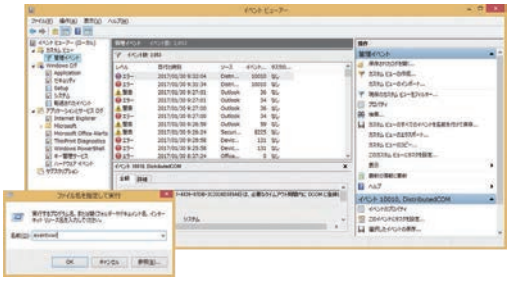


図5 イベントビューアー画面例



[スマートフォンの事例]

①偽の警告画面が表示される

図3のような画面が表示されたので、「修復」「OK」などのボタンを押した。

*2 データやプログラムをパソコンに取り込むこと。反対の言葉は「アンインストール」となる。
*3 サイト上にあるデータやプログラムを手元のパソコン内に転送すること。日本語で「落とす」と表現することもある。反対の言葉は「アップロード」となる。
*4 「有効化」を意味する英語。正規の購入者であることを認識させるため、ライセンスキーなどを入力する操作のこと。
*5 英語ベースの命令文（コマンド）を直接入力することで、Windowsを操作できるツールのこと。
*6 「IPA 情報セキュリティ安心相談窓口に寄せられた相談の分析（2016年）」報告書
https://www.ipa.go.jp/security/anshin/info/2016soudan-analysis-report.html

②アプリをインストール

「App Store」や「Google Play」といった公式マーケットに並ぶアプリのインストール画面に移動し、無償アプリをインストールした。

この手口では、アプリは公式マーケット上にあり、無償であることが確認されています。これらのアプリが実際にどのような仕様で、本当にスマートフォン上の問題を解消するのかどうか不明です。

パソコン・スマートフォンの手口に共通して考えられる相手側の目的は金銭です。ソフトウェアの販売、サポート契約など最終的にお金を得ることが目的と考えられます。アプリ誘導についても、アプリ自体は無償ですが、アプリ内で広告が表示されるため、インストール数稼ぎ＝広告収入になることが推測できます。

偽の警告画面が表示される原因

偽の警告画面は、ウェブサイトの閲覧をきっかけに表示されます。これは迷惑な広告のようなものであり、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ます。実際に、偽の警告画面が表示された時に閲覧していたウェブサイトには広告バナーがあった、という事例も確認されています。

一方で、広告バナーがないサイトでも自動的に偽の警告画面に移動した[*7]という事例もありました。これは正規のサイトが改ざんされた可能性が考えられます。

偽の警告画面を表示する手口への対策

偽の警告画面はウイルス感染ではないため、正規のセキュリティソフトを導入していても、検知されないこともあります。そのため、偽の警告画面が出ないようにする事前対策は困難です。しかし、偽の警告画面が出たとしても、無視して閉じれば問題ありません。音声案内や警告音もBGMとして流しているだけです。ウェブページを表示しているブラウザ[*8]の閉じ方はいくつかありますが、汎用(はんよう)的なものを紹介しますので、いずれかの操作を試してください。

・パソコンを再起動する。
・タスクマネージャー[*9]からタスクを終了する。
・キーボードの「Alt」と「F4」を同時に押す[*10]。

もし、サポート業者に電話をして遠隔操作された場合は、遠隔操作用ソフトウェアのアンインストール[*11]を推奨します。遠隔操作された際、パソコン内に保存しているデータを読まれてしまう可能性は否定できません。ただし、これまでに個人情報を悪用された、またはパソコンにウイルスを仕込まれたといった報告はありません。遠隔操作は画面上に見える範囲でしか操作できないため、その遠隔操作の内容を一部始終目視していて、不審な操作をしていなかったら問題ないといえるでしょう。

また、偽対策ソフトやアプリを入れてしまった場合も、アンインストールの実施を推奨します。しかし、特に偽対策ソフトにおいては、詳細な動作が把握されておらず、パソコンにどのような影響を及ぼしたのか分かりません。そのため、より安全な策として、「システムの復元[*12]」によってパソコンを前の日付の状態に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[*13]をするといいでしょう。

この手口に対して重要なことは偽の警告画面にだまされないことです。表示されるメッセージには、どこか不自然な点があります。警告画面を決してうのみにせず、メッセージの内容をよく確認するといいでしょう。

---

*7 ウェブサイトを閲覧したとき、自動的にページが移動するしくみをリダイレクトと言う。
*8 インターネットを見るためのソフトウェア。例：Internet Explorer、Google Chrome、Firefox
*9 パソコンで動いているプログラムなどをリアルタイムで確認できる管理機能のこと。
*10 Windows のショートカットキーで「強制終了」を意味する。
*11 意図せず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 https://www.ipa.go.jp/files/000054281.pdf
*12 Windows の機能でバックアップから復元するもの。
*13 初期化を実施する場合、パソコン内のデータはすべて消えるため、通常の操作が可能であれば、データのバックアップを行う。初期化の方法は、マニュアルを参照するか、メーカーのサポート窓口へ問い合わせる。