増加する偽警告の脅威と対策について

はじめに

日本国内での被害が増加している偽警告について、脅威と対策をご説明します。

偽警告について

偽警告は、Web サイトを閲覧中に「ウイルスに感染しています」「Windows のセキュリティシステムが破損しています」などと突然表示される偽物の警告メッセージです。

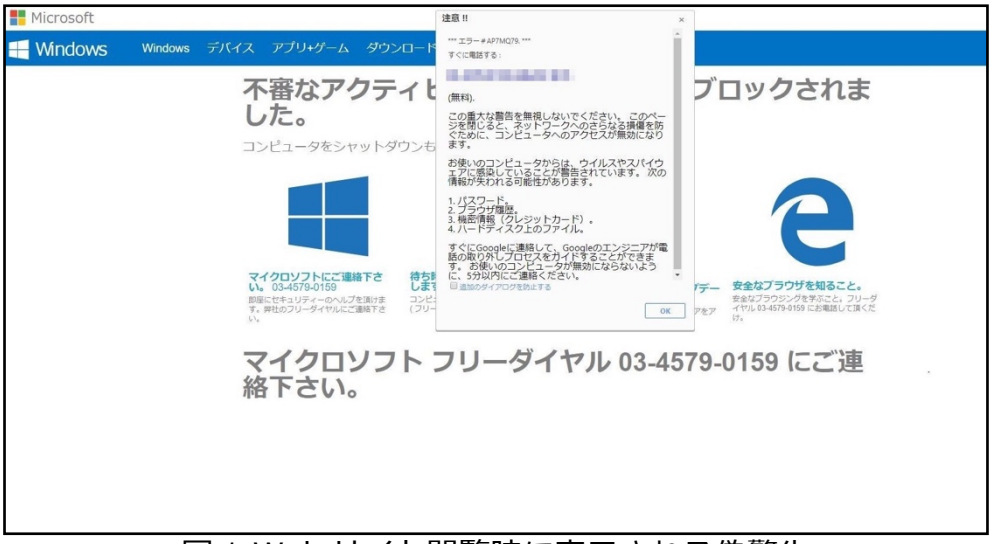

図 1.Web サイト閲覧時に表示される偽警告

偽警告の中には表示されると同時に「ピー」のような大きな警告音や不安を与えるような音声を鳴らすものが存在しています。※1

偽警告が表示されると下記手順で作業をするよう促してきます。
例）

① 不安を与えるような音声が流れ、サポートセンターに電話するように誘導される
② 電話をかけるとリモートアクセスツールをインストールするように指示される
③ インストールするとパソコンを遠隔操作され、偽のセキュリティ対策ソフトをインストールするよう指示される

④ サポートの作業費の請求や年間のサポート料金の契約を持ちかけてくる
クレジットカードや電子マネー決済などで支払いを要求される

現在、偽警告が表示されたことによる相談が相次いでおり、実際に金銭を支払った被害が増加してきています。

偽警告が表示される理由として、「ウイルスに感染しています」などの画面はWeb ページの広告の仕組みを利用して表示されるため、パソコン側に不正なソフトがインストールされた可能性は低いと考えられます。
不安を煽るメッセージを表示するだけのものがほとんどです。

表示された際の対処

- 画面内のボタンなどはクリックせず、ブラウザの「X」ボタンで閉じる
- Windows のタスクマネージャーを利用してブラウザを強制終了させる

<手順>
(1)「Ctrl + Shift + Esc」を同時に押してタスクマネージャーを起動させる
(2) 図 2 ①～③の手順でプロセスを終了する

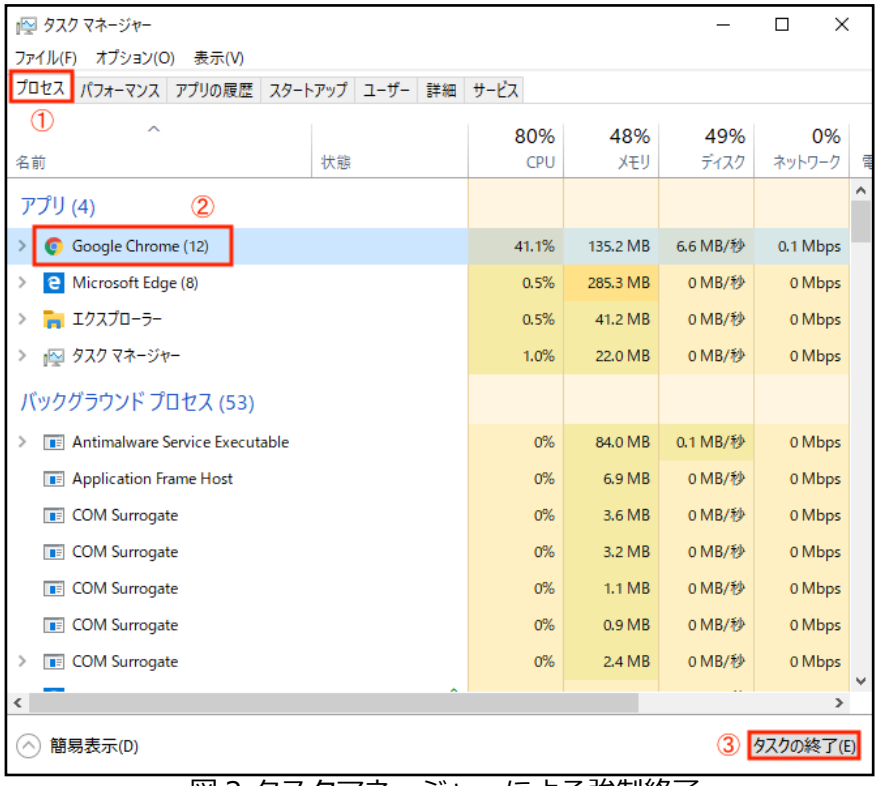

図 2.タスクマネージャーによる強制終了

- 上記の方法でも閉じない場合、パソコン自体を再起動する

NetStable での検知

NetStable では、偽警告に関連する通信を検出するシグネチャをリリースしています。

1. 偽警告を表示されるサイトへのアクセス遮断

- 2001059 Fake Windows Error Msg
- 2001086 Fake Microsoft error page
- 2001484 Fake Alert Redirect site access 5

送信元 IP アドレスの端末で偽警告画面が表示された際の通信を検知するシグネチャです。
端末上で警告画面が繰り返し表示されていないか確認してください。

2. 電話した際にインストールされるリモートアクセスツールの通信検知

- 1003283 - 1003284 TeamViewer 1～2
- 1003245 LogMeIn
- 2001487 GoToAssist Download Request
- 2001488 GoToAssist Login Detect

インストールされることが報告されているリモートアクセスツール(TeamViewer, LogMeIn, GoToAssist)の通信を検知するシグネチャです。
利用していない場合は、アンインストールを行ってください。

3. 電話した際にインストールされる偽セキュリティソフトの通信遮断

- 3000081 RegClean Pro Connection
- 3000339 Reimage Connection
- 2001485 OneSafe PC Cleaner download Detect
- 2001486 OneSafe PC Cleaner site Detect
- 2001491 Advanced Identity Protector Dtect

偽セキュリティソフトのダウンロード、ソフト起動時の通信を遮断するシグネチャです。
送信元 IP アドレスの端末で偽セキュリティソフトのダウンロードまたはソフトを起動した可能性があります。見覚えのないソフトがある場合は、アンイントールを行ってください。

まとめ

- Web 閲覧中に「ウイルスに感染しています」などと表示される画面は偽物の警告画面
- 表示された際は、ブラウザの「X」ボタンまたはタスクマネージャーを利用して強制終了して閉じる
- NetStable で検知された場合は、「NetStable での検知」を参考にして対処する

<参考>
※1 サポート詐欺や iPhone 当選詐欺の手口 – 日本サイバー犯罪対策センター
https://www.jc3.or.jp/topics/support_iphone_fraud.html