広告ウィルス除去マニュアル(案)(rev.1)

2014.10.29 大越 健児

ウィルス (マルウェア)ではないが、「スパイウェアが検出されました」「お使いの PC がクラッシュ寸前です」 「お使いの PC の性能がダウンしています」「コンピュータが遅いですか?」などと、恐怖、注意を喚起して、対 策用ソフトを売り込もうとする、詐欺まがいのソフトが横行しています。ここでは「広告ウィルス」と呼ぶこと にします。

この「広告ウィルス」の除去法について下記します。

1. 広告ウィルスの種類

次の2種類に分かれると考えられる。

(1) Windows が起動状態および何らかのアプリケーションが動作状態に、随時警告画面等が現れるもの これは通常のアプリケーションソフトと同じように、Windows にインストールされ、レジストリの書き込み に従って随時現れると考えらえる。

【例】

・Systweak RegClean Pro ・Uniblue SpeedUpMyPC ・Advanced System Protector ・Reimage Repair (2) ブラウザが起動したときに警告画面等が現れるもの

これはブラウザのアドオンに、不正なものが追加され、意図しない形で現れると考えられる。

【例】

·yontoo · babylon · webcake · Browser2save · TubeSaver · ad.yieldmanager

- 2. インストールソフトの除去法
- (1) 手動で除去する
 - (a) 問題の広告ウィルスが稼働した画面で、そのソフト名を調べる(ソフト名が判らないと以下の操作ができない)。
 - (b) 「スタート」「すべてのプログラム」画面で、上のソフト名を探す。見つかって、そこに「uninstaller」 があれば、それをクリックしソフトをアンインストールする。
 - (c) 「uninstaller」が見つからない場合は、「コントロールパネル」「プログラムと機能」(または「プログラ ムのアンインストール」) 画面で、上記ソフト名を捜し、見つかったらアンインストールする。
 - (d) Program Files フォルダの中に、上記ソフト名のフォルダが残っていないか確認、残っていた場合はその 中のファイルごと削除する。
- (2) フリーソフトを使う

次のフリーソフトを使ってアンインストールする。

IObit Uninstaller

通常のアンインストールでは残ってしまうファイルやフォルダ、レジストリキーといった"ゴミ"を同時 に削除可能な、多機能アンインストール支援ソフト。下記よりダウンロードする。

http://www.forest.impress.co.jp/library/software/iobituninst/

怪しいソフトとして、1.(1)【例】の外に次のようなものがあると言われる。

yontoo babylon delta webcake Lyrics Browser my pc backup QuickShare DealPly Tuto4PC Sing Along Lyr Mix Video Saver Tube Karaoke Youtube Flags EasyLife PriceGong PassWidget Media view luck leap

IObit Uninstaller を起動し、検索バー(IObit Uninstaller の右上の所)に上記キーワード入力し、一つひ とつ検索し、それが含まれるソフトが見つかった場合は削除する。

3. アドオンの除去法

- (1) 手動で除去する
 - (a) Internet Explorer の設定

IE を起動し、「ツール」「インターネットオプション」「プライバシー」を選択する。「プライバシー」の画 面で「詳細設定」をクリックする。「プライバシーの詳細設定」画面で、Cookie 欄の「自動 Cookie 処理 を上書きする」をチェックし、「サードパーティーの Cookie」欄で「ブロックする」を選択する。

インターネット オプション	(下図参照)				
全般 セキュリティ プライバシー コンテンツ 接続 プログラム 詳細設定 設定 カスタム設定を使用しないで、標準のプライバシーのレベルを設定する場 今付 「既定1 ボタッをグリック」 てください	プライバシーの詳細設定 ※ インターネット ゾーンでの Cookie の処理方法を選択できます。これは自動 Cookie 処理を上書きします。				
日は、[LULE] バランをクラックしてくことい。 カスタム - 詳細またはインボートされた設定	Cookie 「回動 Cookie 処理を上書きする(<u>O</u>)				
サイト(<u>S</u>) インボート(<u>I</u>) 詳細設定(⊻) 既定(<u>D</u>) 位置情報 Web サイトによる物理的な位置情報の要求を許可しない(<u>L</u>) サイトのクリア(<u>C</u>)	ファースト パーティの Cookie サード パーティの Cookie ● 承諾する(A) ● 承諾する(C) ● ブロックする(B) ● ブロックする(L) ● ダイアログを表示する(P) ● ダイアログを表示する(R) ■ 常にセッション Cookie を許可する(W) OK				
ボップアップ プロック ■ ボップアップ プロックを有効にする(<u>B</u>) InPrivate ■ InPrivate プラウズの開始時に、ツール バーと拡張機能を無効にする(<u>I</u>) OK キャンセル 適用(<u>A</u>)					

(b) アドオンの削除

「ツール」「インターネットオプション」「アドオンの管理」を選択する。次のような画面が出る。

アドオンの管理			-	X	2
Internet Explorer アドオンの表示。	と管理				
アドオンの種類	名前	発行元	状態	アーキテ	*
 ◇ ツールパーと拡張機能(I) ◇ 検索プロパイダー(S) ◇ アクセラレータ(A) ◇ 追跡防止(K) ◇ えペルの修正(C) 表示: 現在読み込まれているアドオン ◆ Advanced SystemCare Browser P IObit Information Technology 	Google Inc Google Toolbar Google Toolbar Helper ChromeFrame BHO IObit Information Technology Advanced SystemCare Browser Protection JUSTSYSTEMS CORPORATION	Google Inc Google Inc Google Inc IObit Information Tec	有効 有効 無効 無効	32 ビット 32 ビット 32 ビット 32 ビット 32 ビット	III .
パージョン: 7.0.0.0 ファイル日付: 2014年2月20日、1 詳細情報(氏)	種類: ブラウ 10:44 既定の検索プロバイダー	ザー ヘルパー オブジェクト -でこのアドオンを検索(<u>C</u>)		有効にする(<u>E</u>)	
追加のツール バーと拡張機能を検索 ツール バーと拡張機能の詳細(<u>N</u>)	ξ(<u>Ε</u>)			閉じる(L)	

前頁画面で、「名前」欄に不審なアドエア、例えば1.(2)【例】記載のものが見つかった場合は、それ を無効に設定する(該当アドエアを選択し、画面右下の「無効にする」ボタンをクリックするか、該当ア ドエア上で右クリックし「無効にする」を選択する)。

- (c) 不審なアドエアが見つかった場合は、「コントロールパネル」「プログラムと機能」(または「プログラムのアンインストール」) 画面で、同じ名前のソフトがないかチェックする。見つかった場合はアンインストールする。
- (2) フリーソフトを使う

次のようなフリーソフトを使う。

・AdwCleaner ・Malwarebytes Anti-Malware ・RogueKiller ・Junkware Removal Tool 【参考】

AdwCleaner のダウンロード先

https://toolslib.net/downloads/finish/1/get/eIeV/

AdwCleaner の利用の仕方(下記サイトを参照)

http://www.japan-secure.com/entry/blog-entry-213.html

「追記」

広告ウィルスではないが、知らない間に入り込み既定ソフトを変更したり、IEのホームページを自分のページ に変えてしまうソフトがある。既存ソフトのアップロード時に不用意にインストールされないよう注意が必要と 考える。

【例】

• Hao123 • Ask.com

以上