

サイバー犯罪の「踏み台」にされないために

①「踏み台」とは

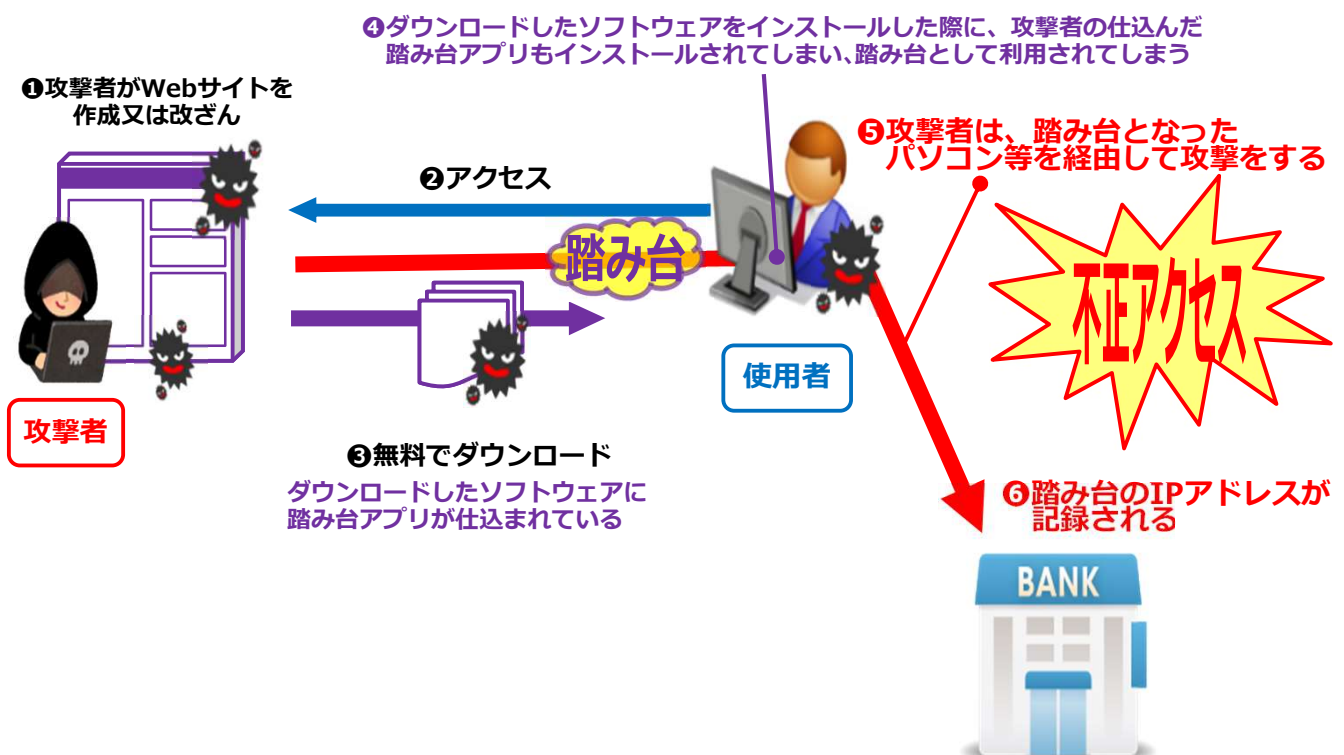
インターネットバンキングの不正送金事犯や不正アクセス事件における発信元パソコンを解析する中で、平成29年から、プロキシサービスのプログラムがインストールされた**踏み台(第三者に乗っ取られた状態のコンピュータ)**の取扱いが増加しています。

これらの踏み台は、「ProxyGate」「MaskVPN」等のプログラムに感染し、不正送金事犯等の被疑者の通信を中継する**サイバー犯罪インフラ**を構成していることが判明しました。

②感染原因

感染の原因は、パソコン使用者が、有料ソフトウェアのライセンス認証の回避を騙るソフトウェアや、無料のライティングソフト等をダウンロードしてインストールした際、同時にProxyGate等の意図しないプログラムがインストールされたことによるものと認められます。

また最近では、主に動画視聴等に利用されるAndroidセットトップボックスにも、踏み台化させるプログラムがインストールされている事例も確認されています。



対処方法 (Windows10の場合)

確認方法

ウイルス対策ソフトウェアでは、検知されない場合があります。



① ウィンドウズボタンをクリック



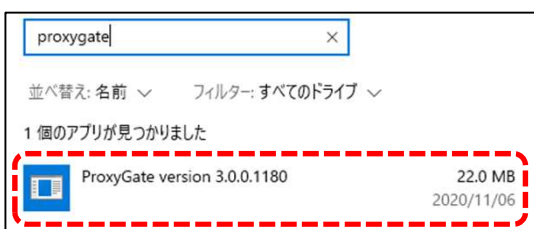
③ 「アプリ」をクリック

④ 「アプリと機能」をクリック

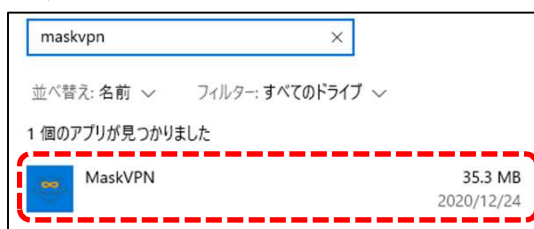


⑤ 入力欄に検索するアプリ名を入力

⑥ インストールされていれば検索結果に表示される



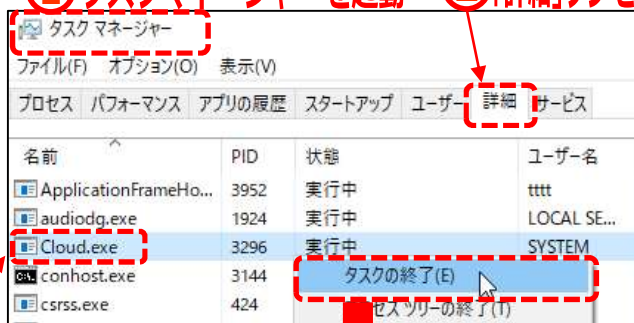
※色々なバージョンがあります



削除方法

【ProxyGate】

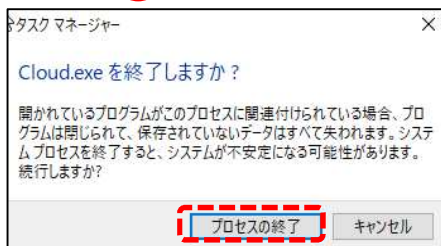
① タスクマネージャーを起動 ② 「詳細」タブをクリック



③ 「Cloud.exe」を右クリック

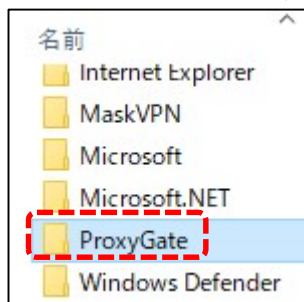
※Cloud.exeはProxyGateの実行ファイルです。
右クリックしてプロパティを表示すると、ファイルの場所が C:¥Program Files¥ProxyGate などとなっていることが確認できます。

④ 「タスクの終了」をクリック

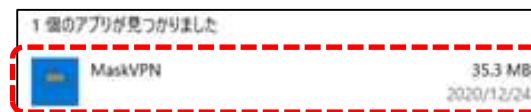


⑤ 「プロセスの終了」をクリック

⑥ ProxyGate フォルダを削除して完了



【MaskVPN】



① 該当のアプリをクリック



② 「アンインストール」をクリック

③ アンインストールが実行され、アプリが削除されていることが確認できれば完了

新潟県警察本部
生活安全部
サイバー犯罪対策課
025 - 285 - 0110

