

ファイル共有ソフトを悪用して情報流出を引き起こす ウイルスへの感染が疑われる場合の対応方法

ファイル共有ソフトを悪用して情報流出を引き起こすウイルスへの感染が疑われる場合には、以下の措置を講ずる必要があります。なお、この種のウイルスは亜種の発現頻度が極めて高いことから、ウイルスの情報は必要に応じてウイルス対策ソフトウェアベンダ等が提供している情報を確認するようにしてください。

また、流出したファイルを特定できる情報（流出したファイルの名称、サイズ、ハッシュ値等）は第三者が当該ファイルを収集することを容易にし、ファイル共有ソフトウェアのネットワーク等において更に当該ファイルが拡散することを助長するため、以下の措置を行うに当たって、その取り扱いには十分に注意してください。

(注) 情報流出の被害を拡大しないため、①の作業をできるだけ早期に行う必要があります。

① 感染の疑いのあるパーソナルコンピュータ（以下「PC」という）をインターネットから切り離す。

当該PCで現に使用しているインターネット接続を遮断することに加えて、無線LANデバイス等の当該PCが機能として持っているネットワーク接続環境すべてにつき、インターネットへの接続を行えないよう設定します。（特にノートパソコンの場合には直ちにシャットダウンすることをお勧めします。）

(注) ②及び③の作業は、状況に応じて、同時並行で、または逆順で行う必要があります。

② 情報流出の被害範囲を特定する。

(1) PC上で確認できる流出情報

ウイルスの被害により情報が流出した場合、当該PCから流出した情報が残っていることがあります。当該PC中から流出した情報を抽出することにより、確実に流出した情報を特定する一助となります。

(2) (1)以外の流出した可能性のある情報

(1)で抽出できるデータは、現在も当該PCから流出し続けている情報だけです。ウイルスに感染してから①の作業を行うまでの間に当該PCに保存された、または当該PCで扱われた情報は、すべて流出している可能性があります。利用者から当該PCの利用状況を確認する等して、流出した可能性のある情報を特定する必要があります。

※ 流出しているファイルを確認するために、Winny や *Share* 等のファイル共有ソフトのネットワーク上で流出したファイル名をキーとして検索をかける行為は、流出情報の拡散を助長するおそれがありますので、安易に実施しないでください。

③ 流出原因の特定

情報流出の原因はファイル共有ソフトを悪用して情報流出を引き起こすウイルスによるものだけとは限りません。最新のパターンファイルを適用したウイルス対策ソフトウェアによるウイルスの検出や当該PCの利用者からの聴き取りにより、流出原因を特定する必要があります。

※ ファイル共有ソフトを悪用して情報流出を引き起こすウイルスは亜種の発現頻度が非常に高くなっています。そのため、ウイルス対策ソフトウェアでは感染しているウイルスを検知できない場合もあります。

④ 当該PCの安全な環境への復旧

①から③までの作業が完了したら、当該PCを安全な環境へ復旧することとなります。復旧に当たっては当該PCをクリーンインストールしてください。なお、クリーンインストールする場合、当該PC中の必要なデータをバックアップすると思いますが、そのときは、ウイルス対策ソフトウェアでは検知できないウイルスがバックアップデータに混入される可能性が十分にあることを考慮して作業を行ってください。

※ ウイルス対策ソフトウェア等でウイルスを駆除するだけでは、②で特定した情報の流出原因を絶つことはできません。

(注) ①から④までの作業は情報の流出を停止するための最低限の措置です。事案発生時には

①から④の作業の外

- 情報が流出したことにより発生した被害への対策
- 情報が流出するに至った経緯を調査すること等による根本的な情報流出防止対策の検討
- ウイルス被害に関する関係機関への届出
- ウイルス対策ソフトウェアで検知できないウイルス検体を発見した際のウイルス対策ソフトウェアベンダへのウイルス検体の提供

等を状況に応じて実施する必要があります。