資料４
情報セキュリティ担当者向け資料

Antinny への感染が疑われる場合の対応方法

Antinny 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、Antinny 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。

（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

Antinny 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。（情報の抽出方法は資料５）

(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。Antinny 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 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 Antinny 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 Antinny 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。

※　Antinny 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。その場合、資料６、７、８を参考に Antinny 被害によるものであるか否かについて検討してください。

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ね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。