

機構内パーソナルコンピュータのマルウェア（不正プログラム）感染
の可能性及び外部サイトとの意図しない通信について（続報）

平成 24 年 6 月 11 日
独立行政法人
原子力安全基盤機構

1. 独立行政法人 原子力安全基盤機構では、外部機関からの連絡により、5 台のパーソナルコンピュータ（以下、「PC」という。）がマルウェアに感染した可能性があり、これらが外部のサイトと意図しない通信を行っていることが5月1日に判明しました（既報）。
2. その後、外部専門業者とともに詳細な調査を進めた結果、以下のことが判明しました。
 - （1）ウイルスに感染している疑いのあった5台のPCについては、全て新種のマルウェアにより感染していることが確定しました。
 - （2）感染したPCを介して、機構のファイルサーバに格納されていた電子ファイル（紙媒体をPDF化したもの）が、平成23年3月から7月の間において、外部に送信され流出した可能性が高いことが確認されました。また、これらのファイルの一部に個人情報が含まれていることを確認しました。ただし、流出した可能性が高い情報には、核物質防護情報等の機微な情報は含まれていません。
 - （3）機構の他のPCも調査したところ、新種のマルウェアにより、合計19台（当初判明した5台を含む。）が意図しない通信をしていることが分かりました。これらのPCについては、直ちにネットワークからの切り離しを行いました。
3. 機構では、今回の事案を踏まえ再発防止策として、以下の対策を実施することとしました。
 - （1）機構から外部に発信される通信について、24時間365日の監視・運用体制を構築。（5月31日実施済）
 - （2）複数のウイルス対策用ソフトを用いて、定期的な全PCスキャンを実施。（5月31日実施済）
4. このような事態となりましたことについて、深くお詫び申し上げます。
今後更なる調査を進めるとともに、今回の事態を重く受け止め、情報セキュリティ対策の一層の強化に取り組んでまいります。

（問い合わせ先）独立行政法人原子力安全基盤機構
企画部情報システムグループ 足立、佐野、長澤
電話 03-4511-1212、03-4511-1217（直通）
（ホームページ）www.jnes.go.jp