2017
5
Vol8-2
獨協医科大学　情報基盤センターニュース
CiCT News
Center for Information & Communication Technology News
オンライン版 :http://infoed.dokkyomed.ac.jp/news/news_index.html

ランサムウェア「WannaCry」にご注意ください！

５月中旬より、国内外でランサムウェア（身代金要求型ウイルス）によるサイバー攻撃が起きています。「WannaCry」などと呼ばれるこのランサムウェアによって、英国の医療機関や国内のインフラ企業等でも被害が発生したことが確認されています。

ランサムウェアとは？

コンピューターに感染すると、ファイルを勝手に暗号化するとともに、ファイルの暗号化を解くための「身代金」の支払いを要求してきます。
ランサムウェアに感染するとコンピューターのデータを事実上読み出せなくなってしまうため、重要な情報が失われる危険があります。

写真：ランサムウェアに感染した PC 画面の一例

原 因

2017年3月に修正された Windows の脆弱性（SMB v1 の脆弱性 ）への対応がなされていない Windows 7 などの Windows PC への感染が確認されています。
メールの添付ファイルに仕組まれたウイルスによる感染の場合と、感染した PC からネットワーク越しに脆弱性への対応ができていない PC への感染が起きていると報告されています。

対 策

第一に、普段からファイルのバックアップをしっかりと取っておくことが必要です。特に重要なデータの場合は安易にデータを書き換えられない方法（DVD-R など ）でバックアップを残しておくなどの工夫が必要です。なお、ランサムウェアに感染したコンピューターでは、バックアップからファイルを復元しようとした際に再度暗号化される危険性が考えられます。そのため、ファイルの復元は、ランサムウェアを完全に取り除いた後に行う必要があります。
また、コンピューターへの基本的なセキュリティ対策も重要です。WannaCry は、上にも書きましたように、Windows の既知の脆弱性を狙ったものです。そのため、Windows のアップデートを行うことが予防につながります。
加えて、ウイルス対策ソフトで定義ファイルを更新しておくことも重要です。ウイルスは、メールの添付ファイル等からも侵入します。メールに添付されたファイルが一見 Office や PDF のファイルに見える場合でも、実際にはウイルスである場合があります。少しでも怪しいと感じたら添付ファイルは開かないようにしてください。
このようなウイルスやサイバー攻撃に対しては、普段からの個人および組織のセキュリティ対策や情報リテラシーが問われます。
ご不明な点や、ご相談は、情報基盤センターまでご連絡ください。

【連絡先】
情報基盤センター
壬生内線：2241
直通：0282-87-2136（越谷・日光・三郷からはこちら）