特別解説

# 私たちは泣きたくはない
## ―ランサムウェア「WannaCry」の騒動―

応用 一般

金岡　晃（東邦大学）

### 大きな騒動となった「WannaCry」

2017年5月12日金曜日，マルウェアの一種であるランサムウェア「WannaCry」が世界的な規模で感染拡大しているという報道が一斉に流れた．WannaCryは脆弱性のあるWindowsマシンを中心に感染し，感染端末からさらに拡大をさせるなど，大きな被害をもたらしている．日本でも週末をはさんだ週明けには地上波テレビの朝の情報番組で特集が組まれるなど大きな話題となっている．被害の広まりは業種業態を問わず，この記事を執筆している時点（5月17日）でも新たな被害情報や亜種の発生などその騒動は収まりを見せていない．

感染先端末のデータを暗号化し利用不可能にした後に復号のための身代金を要求する「ランサムウェア（Ransomware）」は，古くから存在していた．手法もさまざまであったが，数年前よりRevetonやCryptoLockerといったランサムウェアが出現し，（皮肉な言い方であるが）確かな暗号技術と身元特定の難しい支払いシステムを利用した身代金支払いなど，高度化かつ洗練されてきていた．

WannaCryも同様である．感染は脆弱性対策が適用されてないOSに対して行われ，感染後は感染端末上のファイルを暗号化し，身代金を要求する．

### WannaCryは特別なのか

これほどの騒動になったWannaCryの何が特別なのか．拡散にあたって未知の技術や脆弱性が使われたのか？　攻撃対象が非常に限られた場所だったのか？　見たこともない人質の取り方だったのか？要求される身代金に特徴があったのか？　いずれも答えは「否」である．利用された脆弱性は2017年3月に公表され更新プログラムはすでに公開されている．攻撃対象は状況を見る限りランダムに感染拡大がされている．データの「人質化」はRSAとAESを組み合わせた暗号利用であり，身代金はビットコインでの支払いを要求しその額は300米ドル．技術的には目新しいものはないと言ってよいだろう．WannaCryをめぐる周辺の状況がそうさせたと考える．

誰が何のためにやっているかは分からないが，大規模に感染させる活動を始めたことがまずはきっかけであろう．そしてその中で明らかになる事実や被害の特徴，そして規模がWannaCryを際立たせた．英国の国民保健サービス（National Health Service，NHS）が被害を受け，医療行為に影響が出た．「ネットの中の話」と考えがちなマルウェアが，現実世界の，しかも人命にかかわる部分に影響を及ぼした．感染拡大に利用された脆弱性と技

術は，米国の国家安全保障局（National Security Agency，NSA）から流出した技術とツールが基になっている可能性が指摘された．少なくとも今回の感染ターゲットになった Windows OS を提供するマイクロソフト社の Brad Smith 社長は NSA を批判している．日本の小売店端末にも感染しているという画像が出回り，日本を代表する大企業の社内システムに感染し障害を発生させていることが判明した．そして官房長官が会見でコメントをした．

被害範囲の大きさが何よりもポイントだったのではないか．被害範囲が広まれば，さまざまな著名なサービスや企業の多くが被害を受ける可能性も高まり，被害が大きくなればセキュリティ関連組織が注意喚起を導く．被害の中には耳目を引く事例もあり，それがメディアに乗り，専門家以外にも広く共有される．ある情報番組でコメンテーターが「初めてこういうのを知った」と言った．WannaCry が及ぼした最も大きな影響を示す代表的なセリフと言ってよい．

## 騒動は去ったかもしれないが，脅威は去らない

2009 年に大きな感染被害をもたらしたマルウェアである Conficker は，最初の発見から 8 年以上が経た現在でも多くの検出報告がされている．WannaCry の騒動はともすれば本誌が発刊されるときには収まっていることも十分考えられるが，脅威は Conficker 同様に長い期間続くだろう．あらためて，OS やアプリケーションのアップデートやマルウェア対策ツールの適切な利用といったごく基本的なことが重要となる．ランサムウェアにターゲットを絞れば，データは複数個所にバックアップし少なくとも 1 つは端末から切り離して保管することが良いだろう．

## 情報処理学会の一会員として本件から何を見るか

我々研究者がこの一件から学ぶものはなにか．初出からある程度の期間を経てその分野の研究者界隈では常識化したとも思えていた情報は，専門外の人々にとってはまだ見ぬ情報であり，ある発火点をきっかけに急激に広まる．機械学習，VR，枚挙にいとまがない．そしてその急激さを目の当たりにした研究者はさまざまな態度をとる．あるものは「前から言っていた」と胸を張り，あるものは怒り，あるものは「またか」と嘆息する．分野にもよるだろうが，我々セキュリティ研究者は「起きてしまったか」と半ばあきらめ気味で嘆息することも多いのではないだろうか．少なくとも私はそうだ．それで良いのか．研究者が，そして学会が抱える「アウトリーチ」という問題はここにだって存在するのだ．泣いてる暇はないのではないだろうか．

（2017 年 5 月 17 日受付）

**金岡　晃（正会員）　akira.kanaoka@is.sci.toho-u.ac.jp**

2004 年筑波大学大学院博士課程システム情報工学研究科修了．同年セコム（株）入社．筑波大学システム情報工学研究科研究員，同助教を経て，2013 年東邦大学理学部講師．2017 年同准教授．セキュリティとプライバシのユーザビリティ，暗号技術の応用に関する研究に従事．