情報セキュリティ最新事情
－ランサムウェアの脅威－

電気電子・情報系技術班　宮田 晃

1. はじめに

ネットワークの世界的な普及に伴い，個人や組織のコンピュータに攻撃を加え，運用の停止や情報の盗み出しを試みる悪意あるアクセスも増加の一途をたどっている．なかでも最近爆発的に流行したのが「ランサムウェア」と呼ばれる不正プログラムである．本稿ではランサムウェアの概要と，その対処法などにつきまとめる．

2. ランサムウェアについて

ランサムウェアとは，メール添付ファイルや Web ページを利用してコンピュータに潜入し，内部のファイルを暗号化して読み書きできなくしたうえで，暗号化の解除を名目に身代金（ransom）を要求するコンピュータウイルスの一種である．

2000 年初頭ごろから存在は確認されていたが，2017 年 5 月に‘WannaCry’と名付けられたランサムウェアが世界的に猛威を振るい，英国では国民保健サービスや医療機関が攻撃を受け，医療機器が使えなくなったり，患者の情報にアクセスできなくなるなど深刻な被害が発生した．また，自動車生産工場でも操業が停止するなどの被害があった．日本でも日立製作所や JR 東日本などいくつかの組織が影響を受けた．

図－１　WannaCry の身代金要求画面
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html より

図－１に，WannaCry に感染した際に表示される身代金要求画面を示す．日本語のメッセージも用意されていたり，画面左に支払期限までのカウントダウンタイマーを表示し，不安感をあおって支払いに応じさせようとするなど，周到さがうかがわれる．

また，6 月下旬にも亜種と思われる別のランサムウェア‘Petya’が拡散しているとの報告がある．

3. 傾向と対策

3.1 WannaCry の傾向

ランサムウェアは，Windows OS の脆弱性を利用して感染，拡散する．今回 WannaCry が利用したファイル共有サービスの脆弱性は，2017 年 3 月の Windows アップデートで修正されていたが，これほどの世界的流行を見せた背景には，アップデートが適切に施されていないコンピュータがまだまだ多数存在していることを物語っている．

セキュリティの確保において，OS のアップデートは基本中の基本，最低限の対策であり，常に最新の状態を保つように心掛けたい．また今回，Microsoft は既にサポートの終了した OS（Windows Vista, XP, 8, WindowsServer 2003 等）に対しても，この脆弱性に対する修正プログラムを配布した．配布ページの URI を以下に示す．

http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598

これらを適切に利用し，悪意ある攻撃からコンピュータシステムをしっかり保護する必要がある．

WannaCry の感染経路については，未だ確定していない部分もあるが，一般的なメール添付や不正 Web サイトへの誘導等ではなく，OS の脆弱性を利用して，インターネットからターゲットの PC に直接アクセスする方法が多くとられたとみられる．

3.2 ランサムウェア全般への対策

万が一，不幸にして感染してしまった場合，仮に身代金を支払ってもデータが元に戻る保証はない．特に WannaCry は，「支払って復元できた例は確認されていない」という情報もある．感染後システムを終了・再起動しておらず，かつ身代金支払期限前であれば，メインメモリ上に残されたデータ復号用キーの情報を探してデータ復旧を試みるツールも存在するが，これも確実ではない．

ほとんど唯一の確実なデータ復旧手段は，感染したコンピュータを直ちにネットワークから切り離し，ディスクドライブの初期化後，バックアップデータからの復旧である．ネットワーク共有ディスクはウイルスからアクセスされる可能性があるため，バックアップには必ず取り外し可能な記録メディア（USB 接続のハードディスクやメモリデバイス等）を利用すべきである．

また，情報処理推進機構（IPA）や JPCERT コーディネーションセンター，また OS やセキュリティソフトのベンダー等から発信されるセキュリティ情報にも注意しておく必要がある．

4. メール添付ウイルスの傾向

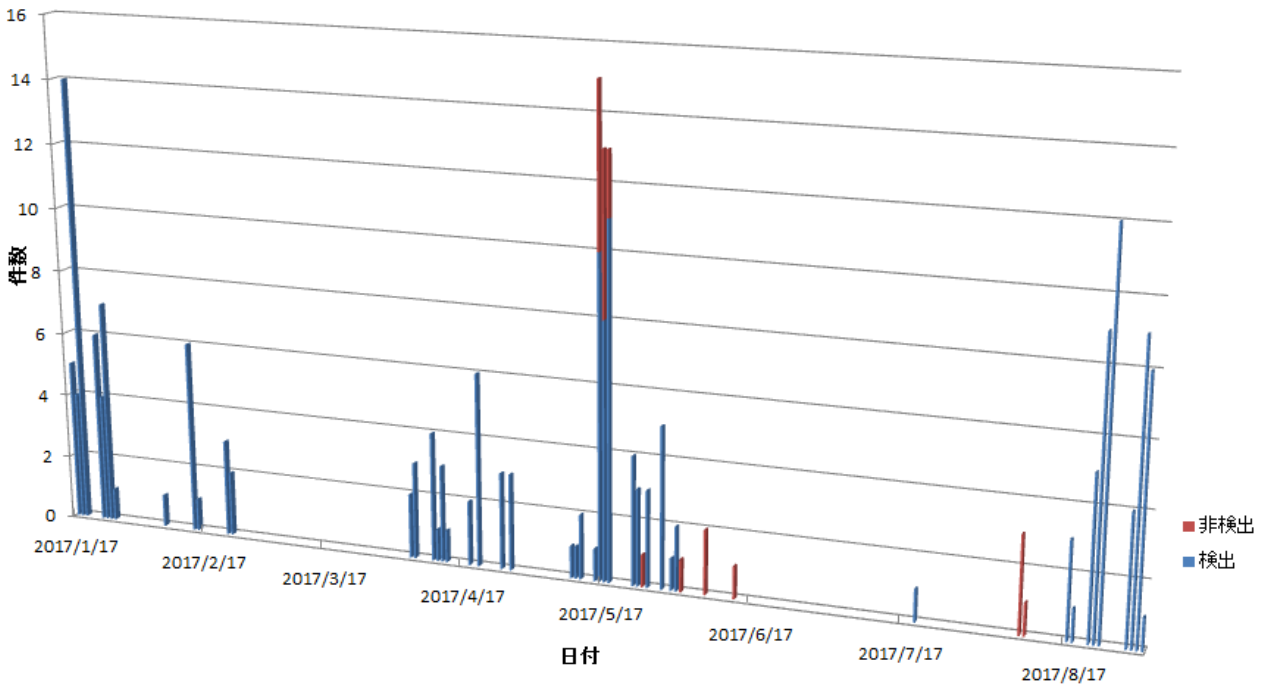
本章では，2017 年 1 月から 8 月までの間に筆者のアカウントに送り付けられた SPAM（迷惑メール）に添付されていたコンピュータウイルスの傾向について報告する．

上記期間中に届いた迷惑メール 4,749 通中，ウイルスとみられるファイルが添付されていたメールは 208 通であった．図－２にその分布図を示す．

これより，メール添付ウイルスは常に一定数が届いているわけではなく，周期的な受信数の変化がみられる．また，新年 1 月や新年度 4 月初頭，5 月の連休あけ等，業務の区切りとなる時期に集中して送り付けられる傾向がうかがえる．

ここで注意しなければならないことは，愛媛大学ではメール送受信サーバによって添付ファイルのウイルスチェックが行われており，ウイルスが検出されたファイルは削除したうえでユーザーに送られているが，一部のウイルスはこのチェックをすり抜けてそのまま届けられていることである．図中赤棒で示した件数がそれにあたり，全部で 21 件あった．

その原因としては，新種もしくは一部改変された亜種のウイルスであり，サーバのチェックパターンの更新が間に合わなかった可能性があげられる．ただしそのいずれも，PC のローカルディスクに保存した時点でセキュリティソフトの検疫に引っかかり，削除された．ただローカルのチェックパターン更新も間に合わない可能性もあるので，セキュリティソフトのみに頼りきるのは危険である．



図－２　メール添付ウイルスの受信件数分布 (2017/1/1～8/31)

5. 各種 OS のセキュリティ

本章では，PC やスマートデバイス用の各種 OS についてのセキュリティ事情をまとめる．

5.1 Microsoft Windows

Windows OS には，ベンダー各社から多くの種類のセキュリティソフトが供給されているが，OS に標準装備されているセキュリティソフトが 2 種存在する．ここではその内容を紹介する．

5.1.1 Microsoft Security Essentials

Microsoft Security Essentials は，Windows7 に装備されているセキュリティソフトである．ローカルディスクに保存されているファイルのウイルスチェックや，リアルタイムに不正な通信を監視するスパイウェア検出機能を持つ．ただし，メールソフトと連携してのメール添付ファイルのウイルスチェック機能はない．

5.1.2 Windows Defender

Windows Defender は，Windows7 以降に装備されているセキュリティソフトである．ただし Windows7 と，それ以降の OS では機能の異なる別のソフトであることに注意が必要である．

Windows7 用 Defender は，スパイウェア検出機能のみを持つ．Windows8 以降の Defender は，ファイルのチェックとスパイウェア検出，加えてメール添付ファイルのチェック機能もある．

結論として，Windows7 では Microsoft Security Essentials，Windows8 以降では Windows Defender を利用することが望ましい．

5.2 MacOS

Apple 社のパソコン用 OS，MacOS は，世界全体のシェアで 8%弱程度であり，Windows と比べて出回っているウイルスの数は少ない．しかしランサムウェア等の存在は確認されているので，OS やアプリケーションのアップデートや添付ファイルの取り扱い，フィッシングへの対策等，Windows と同様の心構えは必要である．Windows と同様のセキュリティソフトも各種供給されている．

5.3 Linux

Unix 系 OS の Linux は，個人用パソコンの OS としては使われている絶対数が少なく，ウイルスもあまり確認されていない．しかし Linux はもともとサーバ用途を目的としており，万が一不正プログラムに感染した場合の被害は甚大となることが予想される．

各ディストリビュータやサーバプログラムの開発元からアップデートが定期的に提供されており，それらを的確に利用することが重要である．

5.4 スマートデバイスのセキュリティ

スマートフォンやタブレット端末等，いわゆるスマートデバイス用 OS として現在主流のものに，Android OS と iOS の 2 種がある．

5.4.1 Android OS

Google によって開発され，Apple 社を除く多くのメーカーのスマートデバイスに搭載されている OS が，Android OS である．

セキュリティの観点からみると，Windows 等と違い，メールに添付されている実行ファイルやスクリプトを自動的に実行してしまう機能はなく，アプリをインストールするには必ずユーザーによる操作が必要になるため，その点ではパソコンより安全である．

しかし，Android OS を狙ったウイルスは既に存在しており，加えて OS の仕様上，Google 社の正規サイト‘Google Play’以外からでもアプリをインストールすることが可能であるため，アプリに仕込まれたウイルスをつかまされてしまう危険は常にはらんでいる．信頼性の低いサイト等からのアプリの入手は避けるべきである．

また，Android OS 用にも Windows と同様に，スパイウェア検出やファイルのウイルスチェック機能を備えたセキュリティソフトが各種提供されているので，それらの導入も有効である．

他の注意点として，スマートメディア用 Web サイトの中には，偽の「ウイルス検知」画面を表示させ，セキュリティソフトへのリンクと偽ってウイルスや架空請求サイトに誘導しようとする悪質なものが存在する．むやみにその指示に従わず，疑わしい時はネット検索等を利用して同様の事例がないかどうか調査すべきである．

5.4.2 iOS

iOS は，Apple 社のスマートデバイス（iPad，iPhone 等）用 OS である．

iOS の場合，アプリのインストールは Apple 社の正規サイト‘Apple Store’からしかできず，そこにおかれるアプリに対してはウイルスの有無も含めて厳重な審査が行われている．加えて iOS の仕様では，個々のアプリが実行中の他のアプリから隔離されたメモリ空間で実行される‘Sandbox’と呼ばれる仕組みがあるため，ウイルスがインストールされたとしても他のアプリのデータにアクセスすることが困難となり，安全性はかなり高い．

しかし，前述の偽画面による誘導には Android 同様に注意が必要である．

6. まとめ

個人や組織のコンピュータに対する悪意ある攻撃は，新たな手口を次々に生み出しつつ，とどまるところを知らない．しかしながらその対策は，どのような脅威に対してもおおよそ同じ内容となる．

- OS やアプリケーションのアップデートを的確に実施する．
- 不審なメール添付ファイルや Web サイトに注意する．
- 重要なデータのバックアップを常に心がける．
- セキュリティ情報に常に注意を払う．

以上のような基本的な対策で，多くの攻撃は回避することが可能であり，そのことを常に意識してコンピュータを利用することが大切であるといえる．