— AUS（アルテミス・ユーザ・サポート）便り 2017/05/15(号外)号 —
http://www.artemis-jp.com

ここで紹介するニュースは、ほとんどの場合、日頃からOS・アプリケーション・アンチウイルスのデータベース等を常に最新の状態に保つこと、併せて、UTM導入等によるネットワーク全体の防御を行うことで対策できます。

●【緊急】Windowsの脆弱性を突くランサムウェア「WannaCrypt」が世界中で猛威…XP等にも特例でパッチリリース

http://www3.nhk.or.jp/news/html/20170513/k10010980311000.html
http://pc.watch.impress.co.jp/docs/news/1059552.html
https://www.ipa.go.jp/security/ciadr/vul/20170514-ransomware.html
https://www.jpcert.or.jp/at/2017/at170020.html
https://blogs.technet.microsoft.com/jpsecurity/2017/05/14/ransomware-wannacrypt-customer-guidance/
http://blog.trendmicro.co.jp/archives/14884
https://www.symantec.com/connect/ja/blogs/wannacry-1

このニュースをザックリ言うと・・・

- 5月12日（米国時間）以降、ランサムウェア「ワナクリプト(WannaCrypt, WannaCry, Wcry)」への感染被害が日本を含む全世界で報告されており、セキュリティベンダーやIPA・JPCERT/CCといった専門機関等から警告が相次いでいます。

- WannaCryptは、3月15日にパッチがリリースされたWindowsの古いファイル共有機能（SMBv1）の脆弱性「MS17-010」を突いて感染し、PC上のファイルの暗号化と身代金の要求を行います。MS17-010の発表時点でサポートが終了していたWindows XPやWindows 8を使用しているPCにおいて、主に被害が出ているとされており、Microsoftでは、WannaCryptによる顧客への影響の大きさを鑑み、XPや8に対しても、特例としてセキュリティパッチを公開しています。

AUS便りからの所感等

- NSAから流出したハッキングツール（AUS便り 2017/4/24号 参照）にMS17-010の脆弱性を悪用する攻撃コードが含まれており、WannaCryptはその攻撃コードを流用したものとみられています。

- 感染経路の大多数は「あるPCに感染し、そこから社内LAN上で他のPCに拡散する」ケースと考えられます。一方で、メールの添付ファイル等からの感染の可能性も少なからずあり、またランサムウェアへの警告文をかたり添付ファイルからマルウェアに感染させようとする動きも確認されています。

- 現在サポートが続いているWindows 10, 8.1, 7およびサポート終了までにパッチが公開されていたVistaについては、Windows Updateによる更新を確実に実施しているか、必ず確認を行ってください（当然ながら、アンチウイルスのパターンファイルが最新のバージョンかの確認も欠かせません）。一方、XPや8に対して特例で公開されたパッチは、各OSに対応する実行ファイルを「Microsoft Update Catalog」からダウンロードし、手動で適用する必要があることに注意してください。

- UTMを用い、適宜LANの分割を行う等により、感染の拡大を食い止められるネットワーク構成とすることが重要です。特に、XP等サポートが終了したOSを使用し続けているPCについては、他のPCから隔離を行い、一刻も早いアップグレードの実施を検討すべきです。