IPA Better Life with IT 情報処理推進機構

世界中で感染が拡大中のランサムウェアに悪用されているMicrosoft製品の脆弱性対策について

最終更新日：2017年5月15日

※追記すべき情報がある場合には、その都度このページを更新する予定です。

概要

2017年3月15日(日本時間)にMicrosoft製品に関する脆弱性の修正プログラム MS17-010が公表されました。
この脆弱性がランサムウェアの感染に悪用され国内を含め世界各国で被害が確認され、英国では医療機関において業務に支障が出るなどの深刻な影響が発生しています。
ランサムウェアに感染するとコンピュータのファイルが暗号化され、コンピュータが使用できない被害が発生する可能性があります。

今回観測されているランサムウェアはWanna Cryptor と呼ばれるマルウェア (WannaCrypt, WannaCry, WannaCryptor, Wcry 等とも呼ばれる) の亜種であると考えられます。

※ランサムウェアとは、「Ransom(身代金)」と「Software(ソフトウェア)」を組み合わせた造語です。感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求する挙動から、このような不正プログラムをランサムウェアと呼んでいます。

対策

週明け(5月15日)には業務開始前に下記対策の実施を推奨します。

1.不審なメールの添付ファイルの開封やリンクへのアクセスをしない

今回のランサムウェアの感染には細工したメールの添付ファイルを開封させる等の方法が用いられていると報道されています。
メールの確認作業をする前に必ず以下の「2.」「3.」の対策を実施してください。
また、不審なメールを確認した場合はシステム管理者等に問題ないか確認してください。

2.脆弱性の解消 - 修正プログラムの適用

Microsoft 社から提供されている修正プログラムを適用して下さい。Windows Update の利用方法については以下のサイトを参照してください。

Windows 10 の Windows Update については以下のサイトを参照してください。
- Windows 10、Microsoft Edge、初めての月例セキュリティ リリース - 読み解き
  https://blogs.technet.microsoft.com/jpsecurity/2015/08/11/windows-10microsoft-edge-3529/

Windows 10 以外の Windows Update の利用方法については以下のサイトを参照してください。
- Windows 10 以外の Windows Update 利用の手順
  https://www.microsoft.com/ja-jp/safety/pc-security/j_musteps.aspx

Windows 7 / 8.1に対する月例パッチの利用方法については以下のサイトを参照してください。

- Windows 7 および Windows 8.1 のサービス モデル変更についての追加情報
https://blogs.technet.microsoft.com/jpsecurity/2016/10/11/more-on-windows-7-and-windows-8-1-servicing-changes/

Windows XP / 8および Windows Server 2003 に対するパッチの利用方法については以下のサイトを参照してください。

- ランサムウェア WannaCrypt 攻撃に関するお客様ガイダンス
https://blogs.technet.microsoft.com/jpsecurity/2017/05/14/ransomware-wannacrypt-customer-guidance/

※Windows XP / 8および Windows Server 2003は既にサポートが終了しています。今回は影響を考慮し例外的にパッチが公開されました。
このパッチの公開は非常に例外的な対応のため、Windows XP / 8および Windows Server 2003を使用している方は早急にサポート中の製品に移行してください。

3.ウイルス対策ソフトの定義ファイルを更新する

各ウイルス対策ソフトをアップデートしてください。
ご利用されているウイルス対策ソフトが今回のランサムウェアを検知するかについては各ベンダにご確認ください。

感染した場合の対応

感染してしまった場合、以下の窓口へご相談ください。
－ IPA
情報セキュリティ安心相談窓口
https://www.ipa.go.jp/security/anshin/

Tel: 03-5978-7509
(なお、受付時間は平日の10:00～12:00および13:30～17:00とさせていただいています。)
E-mail: anshin@ipa.go.jp

－ JPCERT/CC
JPCERT コーディネーションセンター インシデント対応依頼
https://www.jpcert.or.jp/form/#report
Tel: 03-3518-4600
Email:info@jpcert.or.jp

参考情報

- ランサムウエア "WannaCrypt" に関する注意喚起(JPCERT/CC)
https://www.jpcert.or.jp/at/2017/at170020.html

脆弱性情報

- マイクロソフト セキュリティ情報 MS17-010 - 緊急
https://technet.microsoft.com/ja-jp/library/security/ms17-010.aspx
- ランサムウェア WannaCrypt 攻撃に関するお客様ガイダンス - 日本のセキュリティチーム
https://blogs.technet.microsoft.com/jpsecurity/2017/05/14/ransomware-wannacrypt-customer-guidance/

脆弱性検証報告

- Microsoft Windows 製品のSMBv1 サーバーの脆弱性により、リモートから任意のコードが実行可能な脆弱性(MS17-010)に関する調査レポート | ソフトバンク・テクノロジー
https://www.softbanktech.jp/information/2017/20170508-01/

感染状況の報告

- Statement on reported NHS cyber attack - NHS Digital
https://digital.nhs.uk/article/1491/Statement-on-reported-NHS-cyber-attack

ランサムウェアの検証報告

- Cisco's Talos Intelligence Group Blog: Player 3 Has Entered the Game: Say Hello to 'WannaCry'
http://blog.talosintelligence.com/2017/05/wannacry.html
- How to Accidentally Stop a Global Cyber Attacks | MalwareTech
https://www.malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html

- WannaCry ransomware used in widespread attacks all over the world – Securelist
  https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
- Wanna Decryptor (WNCRY) Ransomware Explained | Rapid7 Community and Blog
  https://community.rapid7.com/community/infosec/blog/2017/05/12/wanna-decryptor-wncry-ransomware-explained

ランサムウェアの対策資料

- IPAテクニカルウォッチ「ランサムウェアの脅威と対策」
  https://www.ipa.go.jp/security/technicalwatch/20170123.html

脅威情報早期入手サービス

- サイバーセキュリティ注意喚起サービスicat
  https://www.ipa.go.jp/security/vuln/icat.html

本件に関するお問い合わせ先

IPA　技術本部　セキュリティセンター

E-mail：vuln-inq@ipa.go.jp

※個別の環境に関するご質問を頂いても回答ができない場合があります。詳しくは製品ベンダなどにお問合せください。

更新履歴

2017年5月15日	対策：リンク情報の訂正
2017年5月14日	掲載