ランサムウェア WannaCrypt 対策まとめ

対応のポイント

WannaCrypt の感染原因は、メールの添付ファイルではなく、SMB の脆弱性悪用ツールを利用したものである可能性が高い―このため、対策は Windows Update をこまめに行って Windows OS のセキュリティホールを無くすことが重要である

メールの添付ファイルをクリックやダブルクリックで開かない―特に不信なメール、
　疑わしいメール―偽装しているメールにも注意すること

セキュリティ更新プログラム「4013389」を Windows Update で適用する
Windows OS のファイル共有サービス(SMB v1)を無効化する

Windows 8 以前が攻撃対象となっている(2017/5 時点)
今後、Windows 10 も攻撃される可能性があるので注意―Windows Update を適用

5 月 15 日月曜日は特に厳重注意! - ランサムウェア「WannaCrypt」の攻撃

マイナビニュース / 2017 年 5 月 14 日 18 時 33 分

すでに何らかの報道で目にしている人は多いと思うが、ランサムウェア「WannaCrypt」が世界各国で大きな被害をもたらしている。主に法人を対象に大規模な攻撃が行われており(もちろん個人にも)、約 80%がメールと添付ファイルによって拡散中だ。日本でも多数の検出報告があるため、メールチェックが急増する週明けの 5 月 15 日月曜日は特に注意してほしい。

WannaCrypt は、感染した PC のファイルを暗号化し、解除のために身代金を要求するランサムウェアだ。トレンドマイクロのセキュリティブログによると、WannaCrypt は 2017 年 4 月に、

Dropbox の URL を悪用して拡散する暗号化型ランサムウェアとして確認されたとのこと。

今回の世界的な被害は、Windows OS のファイル共有サービス(SMB v1)が抱える脆弱性「CVE-2017-0145」を悪用し、感染を広げている。1 台の PC に感染すると、Windows OS のファイル共有機能を介して、ネットワーク内の PC にも次々と感染するからタチが悪い。身代金を要求する画面上のメッセージは、日本語にも対応している。

ただしこの脆弱性は、Microsoft が 2017 年 3 月にリリースしたセキュリティ情報「MS17-010」、およびセキュリティ更新プログラム「4013389」にて対策済みだ。また、5 月 14 日に投稿された日本マイクロソフト「TechNet 日本のセキュリティチーム」ブログでは、「現時点では WannaCrypt で使用されている悪用コードは Windows 10 には無効であることを確認しています」とされている。あくまで「現時点」なので、油断禁物なのは言うまでもない。

従って脅威にさらされるのは、
・Windows 8.1 以前の Windows OS(サーバーOS については割愛)
・セキュリティ更新プログラム「4013389」を未適用
・「SMB v1」が有効
という環境だ。

WannaCrypt が進化し、Windows 10 をターゲットにするようになれば、当然だが Windows 10 環境でも対策を講じる必要がある。

○まずはセキュリティ更新プログラム。例外的に「Windows XP」用を配布中

ではどんな対策をすればいいのか。

とにもかくにも、セキュリティ更新プログラム「4013389」の適用が第一だ。すぐに Windows Update を実行してほしい。Microsoft は影響の大きさ考慮し、すでにサポートが終了した Windows XP、Windows 8、Windows Server 2003 についても、例外的にセキュリティ更新プログラムをリリースした。

・セキュリティ対策ソフトウェアを最新の状態にする。
・SMB v1 を無効化する。方法については「マイクロソフト サポート技術情報 2696547」を参照のこと。
・外部ネットワークからのアクセスに対して、SMB が標準で利用する「TCP 445」ポートをルータやファイアウォールでブロック(遮断)する。

参考までに、Windows 10 において SMB v1 を無効化する方法は、別記事「Windows 10 ミニ Tips 第 153 回 セキュリティレベルを高めるために、SMB バージョン 1 を無効化する」を参照してほしい。

○メールの添付ファイルを開かない、クリック/ダブルクリックしない

上記の対策は根本的なものだが、企業では一個人ユーザーが実行できない場合も多いだろう(セキュリティ管理者のみ実行可能)。

オフィスの一個人としてできるのは、メールの添付ファイルをクリック/ダブルクリックしないこと、クラウドストレージやファイル転送サービスで送られてくるファイルをクリック/ダブルクリックしないことだ。まずはシステム管理者に問い合わせ、オフィスの PC 環境が対策済みであることを確認したうえで、上記のようなファイルを開くようにしてほしい。

システム管理者がいない場合、さらにセキュリティ更新プログラムの適用も個人ベースで運用しているような場合は、真っ先に Windows Update を実行する。次に、セキュリティ対策ソフトウェアを起動して、マルウェア定義ファイルなどを手動で更新しておこう。

余談だが、この記事を読んでくださった読者諸氏の多くは、セキュリティに関する情報感度と知識をお持ちだと思う。ぜひ、周りの人たちにも注意を促してもらえるようお願いしたい。
（林利明）

https://news.infoseek.co.jp/article/mynavi_1626815/?p=1

Windows 10 ミニ Tips

153 セキュリティレベルを高めるために、SMB バージョン 1 を無効化する

阿久津良和

[2017/01/27]

「Windows 10 ミニ Tips」は各回の作成時点で最新の Windows 10 環境を使用しています。

Windows OS で長年にわたって使われ続けてきた SMB(Server Message Block)だが、今回はセキュリティを優先するため、SMB バージョン 1 を無効化する手順を紹介する。

30 年以上前のプロトコルに潜む脆弱性

以前から Microsoft は、Windows OS のファイル共有時などに用いられる SMB(Server Message Block)プロトコル バージョン 1 の無効化を呼び掛けている。Windows Vista の時点で SMB バージョン 2 を実装し、Windows 8 では SMB バージョン 3。そして現在の Windows 10 では SMB バージョン 3.1.1 が利用可能だ。

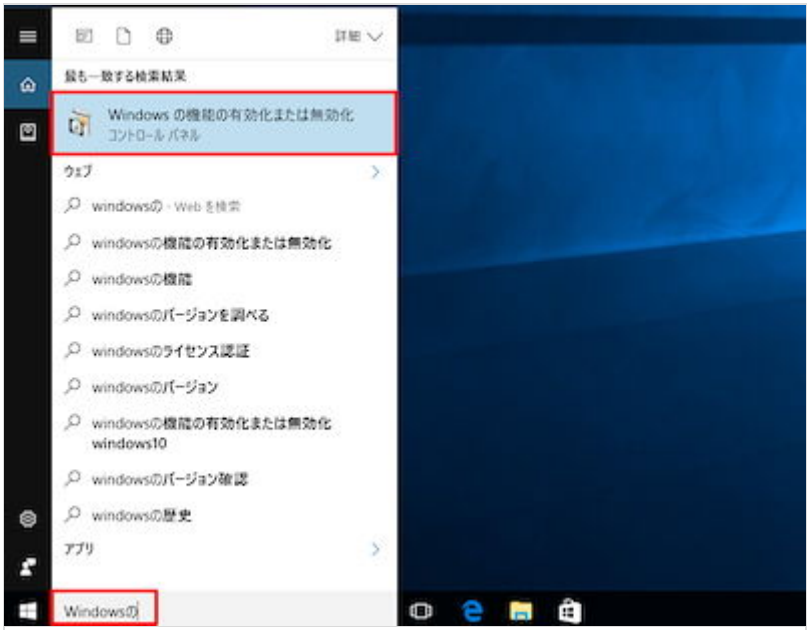
不要な機能は無効にすれば済む話だが、ここには互換性問題が関わってくる。例えば古い NAS は、OS として Linux を利用し、Windows 互換のファイル共有に「Samba」というパッケージを用いてきた。

現在の Samba は SMB バージョン 2 およびバージョン 3 をサポートしているものの、古い NAS のファームウェア(パッケージ)が更新されていない場合、SMB バージョン 1 で通信を試みてしまう。ネットワーク周りのトラブルを減らすため、Windows 10 でも SMB バージョン 1 はサポートされている。

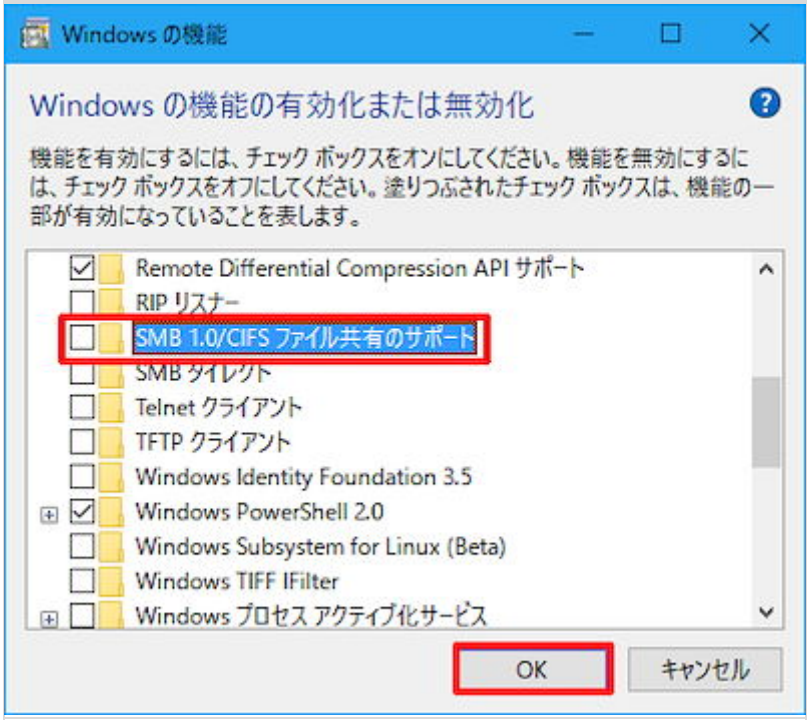
30 年以上も経過している SMB バージョン 1 だが、米国コンピューター緊急事態対策チーム(US-CERT)も、SMB バージョン 1 の利用中止を広く呼び掛けた。LAN 内に Windows XP や Windows Server 2003 など古い OS を搭載した PC が存在せず、および同じ時期に導入した NAS を既に使っていないのであれば、SMB バージョン 1 は即座に無効化すべきだ。

GUI/CUI から SMB バージョン 1 を無効にする

Windows 10 で SMB バージョン 1 を無効化するには、2 種類の手順がある。ひとつは、コントロールパネルなどから呼び出せる「Windows の機能」だ。ここで「SMB 1.0/CIFS ファイル共有のサポート」を無効にすればよい。設定後は PC の再起動を求められるので、編集中のファイルは事前に保存しておこう。



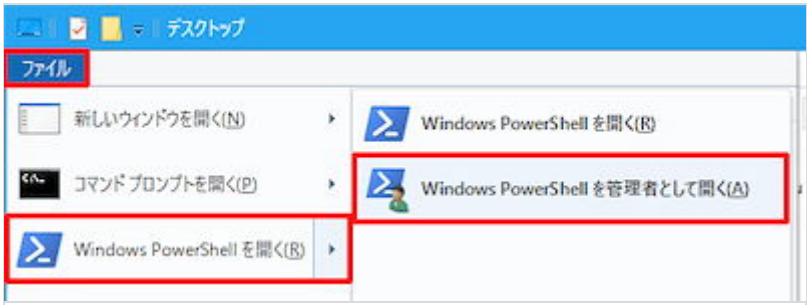
検索ボックスに「Windows の」と入力し、検索結果の「Windows の機能の有効化または無効化」をクリック/タップ



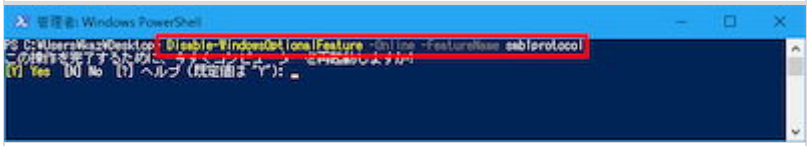
一覧から「SMB 1.0/CIFS ファイル共有のサポート」をクリック/タップしてチェックを外し、「OK」ボタンをクリック/タップ

処理実行後は PC の再起動をうながすメッセージが現れるので、「今すぐ再起動」ボタンをクリック/タップ

もうひとつは、PowerShell を使う方法だ。コマンドラインからの操作に慣れたユーザーなら、PowerShell のほうが簡単だろう。「Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol」を実行するだけで、SMB v1 の無効化が可能だ。ただし、GUI 操作時と同じく、PC の再起動は必要となる。



「エクスプローラー」の「ファイル」タブ→「Windows PowerShell を開く」→「Windows PowerShell を管理者として開く」と順にクリック/タップ



プロンプトに「Disable-WindowsOptionalFeature -Online -FeatureName smb1protocol」と入力して[Enter]キーを押す。処理終了後は「Y」キー→[Enter]キーを押して、PC を再起動しよう

阿久津良和(Cactus)

http://news.mynavi.jp/column/win10tips/153/