SMB 1.0 の影響と無効化について

SMB とは

SMB とは、Windows のファイル共有に利用されるプロトコルで、
現在は OS を問わず一般的なファイル共有で利用される共有の仕組みとして
利用されています。

SMB にもいくつかのバージョンがあり、
Windows 2000 や XP で利用された「SMB 1.0」、
Windows Vista で導入され、高速化された「SMB 2.0」、
Windows 7 からの「SMB 2.1」、Windows 10 からの「SMB3.11」
などがあります。

このうち、既にサポートが終了している Windows 2000 や XP で利用された
SMB 1.0 は、脆弱性が多く報告されているため、無効化が推奨されています。

※ SMB 1.0 は、SMBv1 や CIFS などと呼ばれることもあります。

SMB 1.0 の影響

SMB 1.0 を利用して共有サーバに接続した場合、以下の影響があります。

- SMB 2.0 以降を利用した場合と比べて、接続速度や通信速度が遅い
- 古い方式で脆弱性が修正されないので、SMB 1.0 の脆弱性を狙った攻撃の影響を受ける可能性がある

2017 年に流行したランサムウェア WannaCry も、この SMB 1.0 の脆弱性を悪用して感染を拡大することが知られています。

脆弱性の影響を防ぐために、Windows Update を実行して最新の更新プログラムを適用することに加え、SMB 1.0 を無効化することをご検討ください。

SMB 1.0 通信の検知

NetStable では、以下の SMB 1.0 通信を検知するシグネチャをリリースしています。

- 3000205 Global SMB1 Trans Command
  外部(グローバル IP)から、SMB 1.0 の接続を開始しようとした通信を検知するシグネチャです。外部から共有ファイルを閲覧されたり、
  脆弱性を攻撃され、マルウェアに感染する恐れがあります。

SMB 1.0 の無効化

利用中のサーバや NAS 等の設定を確認し、SMB 2.0 以降が利用できる場合、
以下の手順にてパソコン側の SMB 1.0 を無効化されることをご検討ください。

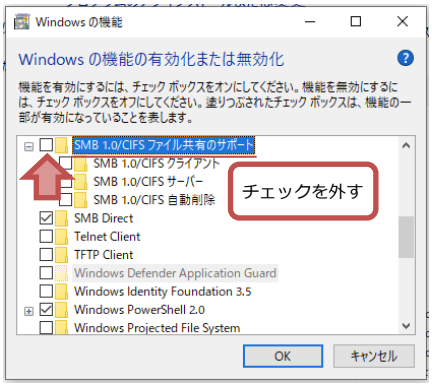
- Windows 7
  コマンドやレジストリを操作する必要があります

  以下の Microsoft 技術情報を参照してください。

  Windows と Windows Server で SMBv1、SMBv2、SMBv3 を検出する方法と有効または無効にする方法
  https://support.microsoft.com/ja-jp/help/2696547/detect-enable-disable-smbv1-smbv2-smbv3-in-windows-and-windows-server

- Windows 10 / 8.1
  プログラムの追加と削除 内の Windows の機能の有効化または無効化 より SMB 1.0 を無効化することが出来ます

  「SMB 1.0/CIFS ファイル共有のサポート」のチェックを外します
  ※ 詳細は上記の Microsoft 技術情報を参照してください



まとめ

- SMB 1.0 は古いファイル共有方式であり、脆弱性がある
- WannaCry 等のランサムウェアもこの脆弱性を悪用している
- 確認の上、必要が無ければ SMB 1.0 を無効化する