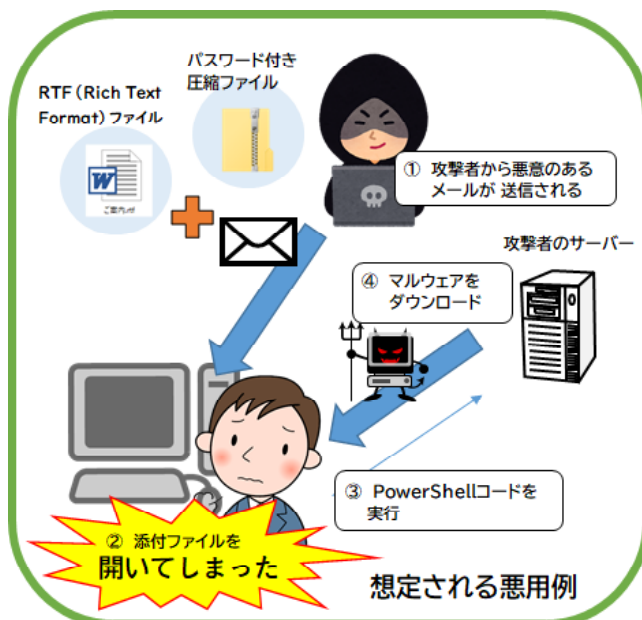




Microsoft社のサポート診断ツールのぜい弱性について

本年5月末、Windowsに標準搭載されているMicrosoftサポート診断ツール(Microsoft Support Diagnostic Tool,MSDT)にリモートコード実行が可能となるぜい弱性(CVE-2022-30190)が存在するという情報が開示されました。

このぜい弱性を悪用することで、不正なプログラムのインストール、内部データの閲覧・変更・削除、アカウントの新規作成などを行なわれる危険性があります。



通常、安全でない場所のファイルは、「保護ビュー」によって読み取り専用で開かれる設定になっているため、すぐにこのぜい弱性を突いた攻撃を受けることはありません。

しかし、保護ビューが無効になっている場合や、保護ビューが効かない

「パスワード付き圧縮ファイル内から解凍されたofficeファイル」

「RTF(Rich Text Format)ファイル」

については、**ファイルを開くと即座に実行されてしまう**可能性があります。

また、このぜい弱性は、**マクロを無効化していても影響を受けます。**

現在も十分注意していただいているとは思いますが、引き続き

- 不審なメールの添付ファイルは開かない
- メール添付ファイルを開く際は、信頼できる者以外電話などで一度相手に確認する

などの対策について、徹底していただくようお願いします。

<Microsoft社が公表したガイダンス>

参照先URL <https://msrc-blog.microsoft.com/2022/05/30/guidance-for-cve-2022-30190-microsoft-support-diagnostic-tool-vulnerability-jp/>

長崎県警察本部サイバー犯罪対策課
095-820-0110 (3451・3452)
メールアドレス e103107@police.pref.nagasaki.jp

サイバー犯罪対策課
公式LINEアカウントで
情報配信中！

@387ojopi

