【参考資料】

ヘルプファイルを悪用した攻撃
メールの攻撃手口と注意点

2022年4月

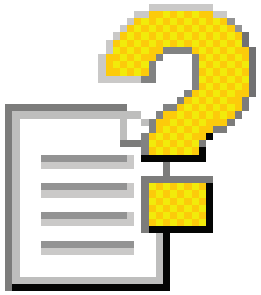
IPA 独立行政法人情報処理推進機構
セキュリティセンター

はじめに

Microsoftの**コンパイルされた HTML ヘルプ ファイル（以降、ヘルプファイル）を悪用した攻撃**が行われていることを公開情報より確認しました。
本資料は、この攻撃手口について紹介し、注意点を説明するものです。

【参考情報】

- コンパイルされた HTML ヘルプ ファイル とは
  Windows環境において、HTML形式で表示されるヘルプに用いられるファイルのことです。
  ファイルを開くとヘルプ情報を表示します。ファイルの拡張子は、「.chm」であり、次のようなアイコンのファイルです。



※本資料では、Windows 10の画面で説明しています。
バージョンにより、表示されるアイコン等は異なる場合があります。

本資料をもとに、攻撃の手口について知っていただくとともに、不審なメールや、
不審な添付ファイルに対して警戒いただくようお願いいたします。

攻撃手口

攻撃手口

- 現在までに公開されている情報および観測状況より、「圧縮形式のファイル」を添付した攻撃メールの存在を確認しています。圧縮形式のファイルには、悪意のある仕掛けが組み込まれたヘルプファイルが格納されています。
- メールに添付された圧縮形式のファイルを解凍し、中にあるヘルプファイルを開くと、端末の情報が盗まれたり、ウイルス感染が目的と思われる通信が発生することを確認しています。
- このヘルプファイルは、**開くだけで悪意のある動作を開始する**ため、不審なメールに添付されたファイルは開かないように注意することが重要です。

本手口による攻撃の観測状況

- 2022年3月時点において、日本語のメールで攻撃が行われた可能性を示す情報は確認しておりません。ただし、今後、日本語のメールで攻撃が行われる可能性もあるため、不審なメールに注意してください。

⇒ 本資料にて、攻撃の特徴と注意点について説明します。

特徴と対応

- 現時点で確認している、ヘルプファイルを悪用した攻撃メールには次のような特徴があります。

特徴

① メールにはRAR形式やZIP形式、7Z形式といった、いくつかのパターンの圧縮形式のファイルが添付されている。
② 圧縮形式のファイルには、ヘルプファイルやWord文書ファイル等が格納されている。

対応方法

上記の特徴にあてはまる、身に覚えのないメールを受信した場合、圧縮形式のファイルや、ヘルプファイルを開かないよう注意するとともに、**システム管理部門等へ連絡**してください。
（なお、圧縮形式のファイルを解凍しただけでは、悪意のある動作は行われません）

次のページからは、実際の悪意のあるメールを例にして説明します。

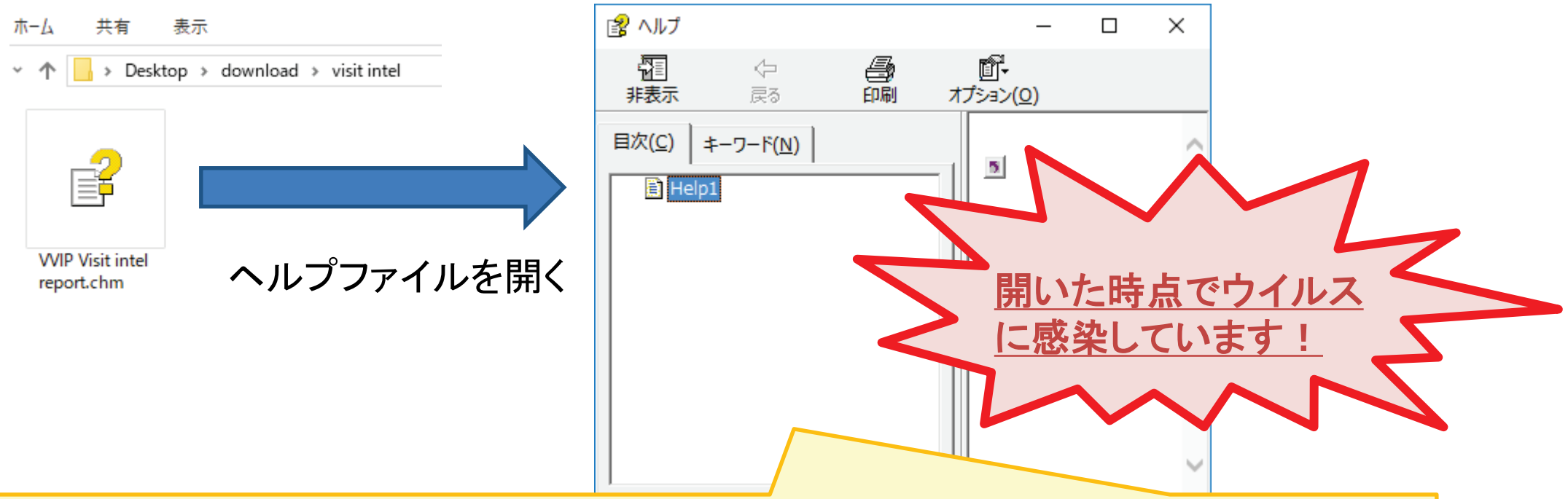
事例紹介1―(1)

- メールに添付されている圧縮形式のファイルに、ヘルプファイルが格納されている場合。

[次ページへ続く]

事例紹介1―(2)

- ヘルプファイルを開くだけで、ウイルスに感染します。

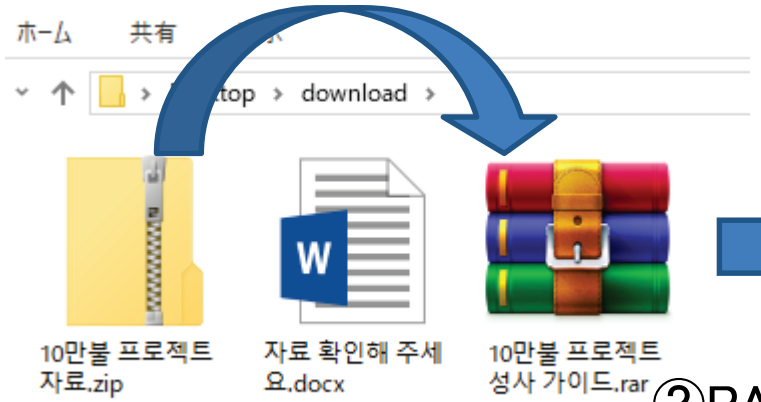


ヘルプファイルを開くと、ヘルプウィンドウが表示されます。
警告画面等は表示されませんが、このとき**悪意のある動作(ウイルス感染等)が実行されています**。

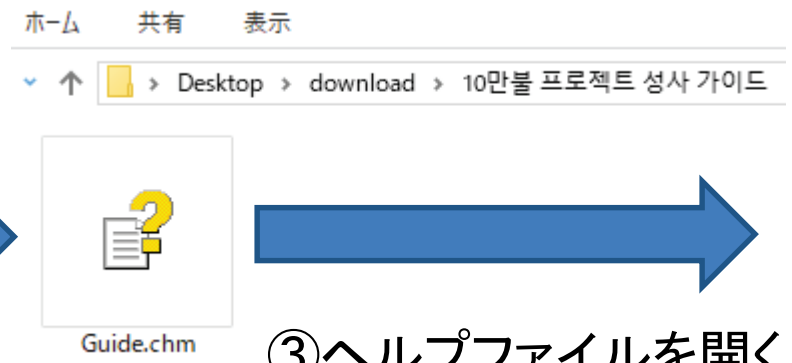
事例紹介2

- メールに添付されている圧縮形式のファイルに、ヘルプファイルだけでなく、Word文書ファイルも格納されている場合。

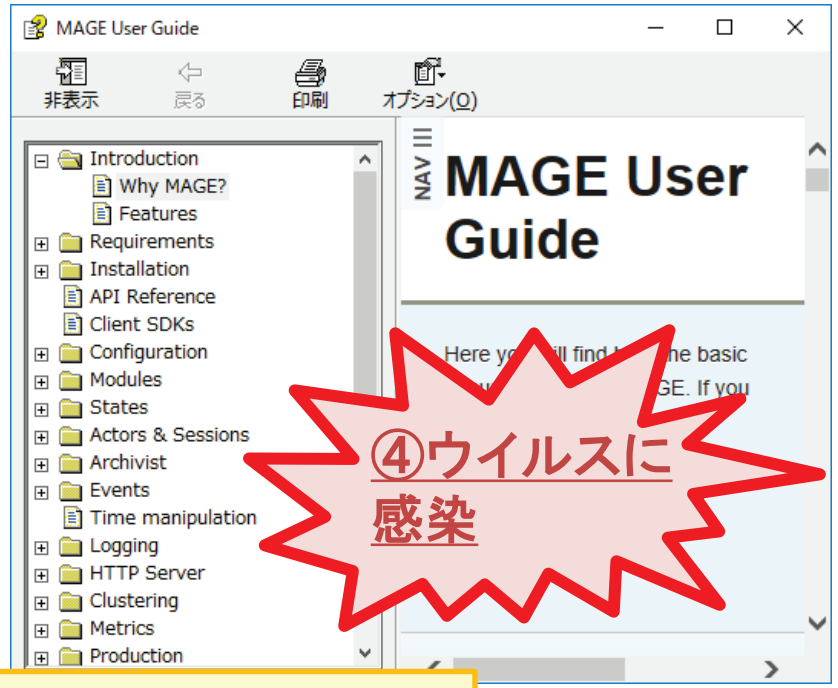
①ZIPファイルを解凍する



②RARファイルを解凍する



③ヘルプファイルを開く



ZIPファイルに格納されているWord文書ファイルはパスワードがかかっており、閲覧できません。メール受信者に、RARファイル内にパスワードがあると思わせ、ファイルを開かせようとしているものと思われます。

【参考情報】この攻撃手口の緩和策

- ヘルプファイルを「Microsoft HTML ヘルプの実行可能ファイル」で実行しないようにすることで、悪意のあるコードが実行されないようにすることができます。
- ただし、WindowsOSを操作する上でヘルプファイルを用いたヘルプ参照は通常業務の操作でも起こりうるため、**業務影響が大きくなる可能性があります。**
- 業務影響を加味した上で、実施を検討してください。

■緩和策の一例

おわりに

身に覚えのないメールや添付ファイルを**開いてしまった**場合は、すぐにシステム管理部門等へ連絡してください。
また、安全であると判断できない限り、不用意に不審なメールの添付ファイルは開かないように注意してください。

本資料で説明したタイプの「悪意のあるヘルプファイル」のほかにも、文書ファイルの機能を悪用したウイルスが存在します。
これらのウイルスに感染しないよう、次のような基本的なウイルス対策を行ってください。

- ✓ **不審なメールのURLリンクはクリックしない。**
- ✓ **OSやアプリケーション、セキュリティソフトを常に最新の状態にする。**
- ✓ **信頼できないメールに添付されたWord文書やExcelファイルを開いた際、マクロに関する警告が表示された場合、「マクロを有効にする」「コンテンツの有効化」というボタンはクリックしない。**
- ✓ **メールや文書ファイルの閲覧中、身に覚えのない警告ウインドウが表示された際、警告の意味が分からない場合は操作を中断する。**