【参考資料】

SLKファイル(※)を悪用した攻撃手口に関する注意点

2018年4月25日

IPA 独立行政法人情報処理推進機構
技術本部 セキュリティセンター

※ Symbolic Link ファイル ：Microsoft Excel に関するファイル。

はじめに

Microsoft ExcelのSLK（Symbolic Link）ファイルを悪用した攻撃手口の情報が、2018年の2月に海外で公開されました。

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。（この攻撃手口は、脆弱性の悪用や、従来より多く観測されているマクロ機能の悪用とは異なるものです）

【参考情報】

- SLKファイルとは
  Microsoft Excelに関連付けされているファイルで、次のようなアイコンのファイルです。
  ファイルを開くと、Microsoft Excelが起動します。ファイルの拡張子は、「.slk」

※本資料では、Microsoft Office 2016 の画面で説明しています。
バージョンにより、表示される警告画面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から、攻撃者から悪意のあるSLKファイルを添付したメールが送られてくるものと考えられます。
  メールに添付されているSLKファイルを開くと、悪意のあるサーバへアクセスし、ウイルスをダウンロードして感染させられることを確認しています。
- メールに添付されるOffice文書ファイルによる攻撃の多くは、Microsoft Officeの「保護ビュー」の機能で防御することが可能ですが、本攻撃手口では「保護ビュー」を有効にしている状態でもウイルスに感染させられてしまいます。

SLKファイルを悪用した攻撃の状況

- 2018年4月時点で、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、同様の攻撃が今後国内で発生する危険性もあり、注意が必要です。

➡ 本資料にて、攻撃の特徴と注意点について説明します。

攻撃の特徴

- 現時点で確認している、「SLKファイルを悪用した攻撃の手口」による攻撃には次のような特徴があります。

特徴

① メールに添付されたSLKファイルを開くと、『セキュリティに影響を及ぼす可能性のある問題点が検知された』旨の警告ウインドウが表示される。

② 上記①の警告ウインドウで「有効にする」を選択すると、『外部データへのアクセスができないため、他のアプリケーションを起動する』旨の警告ウインドウが表示される。

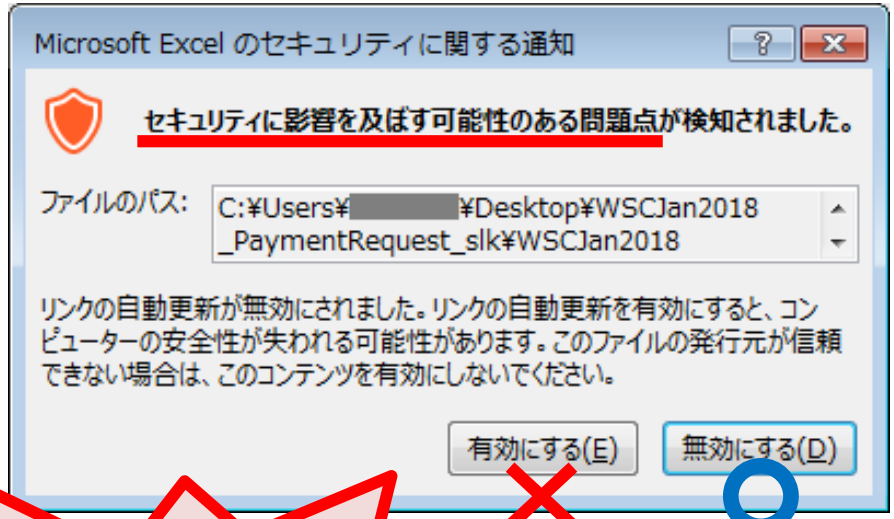
⇒ ②の警告ウインドウで「はい」を選択してしまうと、ウイルスに感染させられてしまう。

次のページに、実際の警告ウインドウを示します。

対応方法

- SLKファイルを開いた際に、次の警告ウインドウが表示された場合、閲覧中のファイルが安全なものであると確証がない限り、「無効にする」・「いいえ」を選択してください。

攻撃メールに添付された .slk という拡張子のファイルを開く

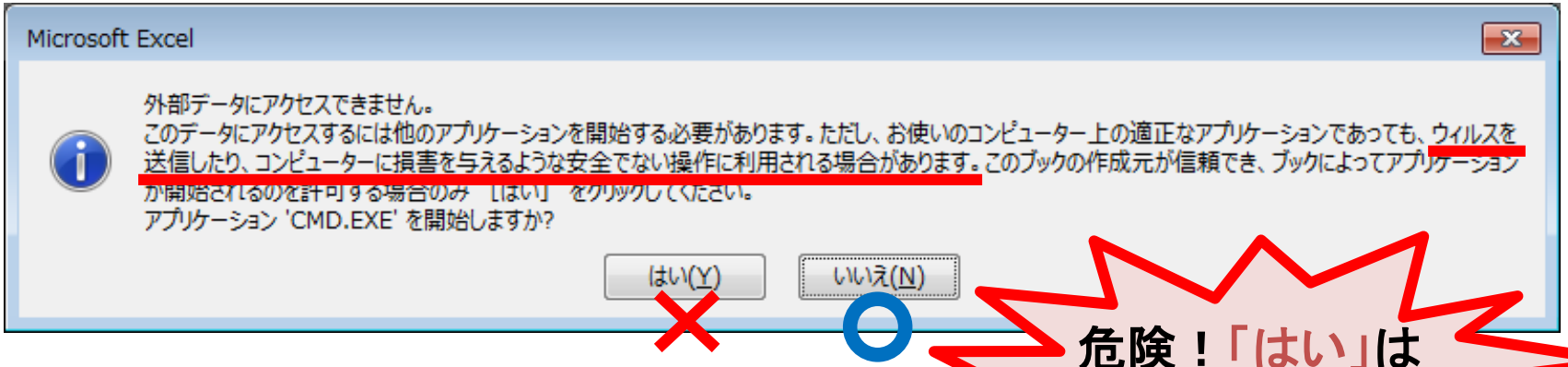


危険！「有効にする」はクリックしない！

[次ページへ続く]

対応方法

- 同様に、次の警告ウインドウが表示された場合、閲覧中のファイルが安全なものであると確証がない限り、**「無効にする」・「いいえ」を選択してください**。



危険！「はい」はクリックしない！

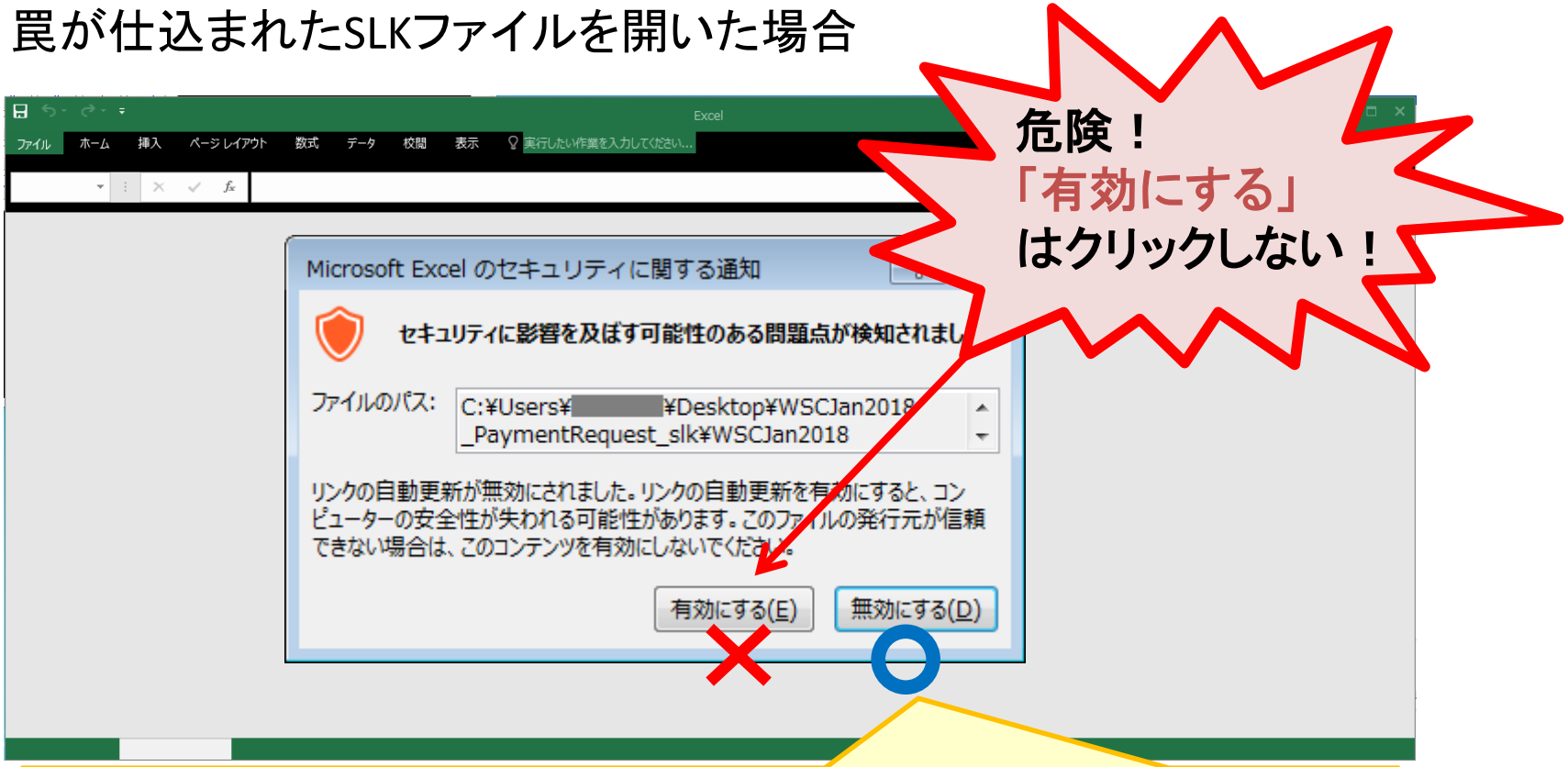
対応方法

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、操作を中断し、**システム管理部門等へ連絡**してください。（警告ウインドウで「無効にする」・「いいえ」を選択した場合は、ウイルスに感染しません）

次のページからは、実際に確認されたウイルスを例にして説明します。

攻撃の画面（1）

- 罠が仕込まれたSLKファイルを開いた場合

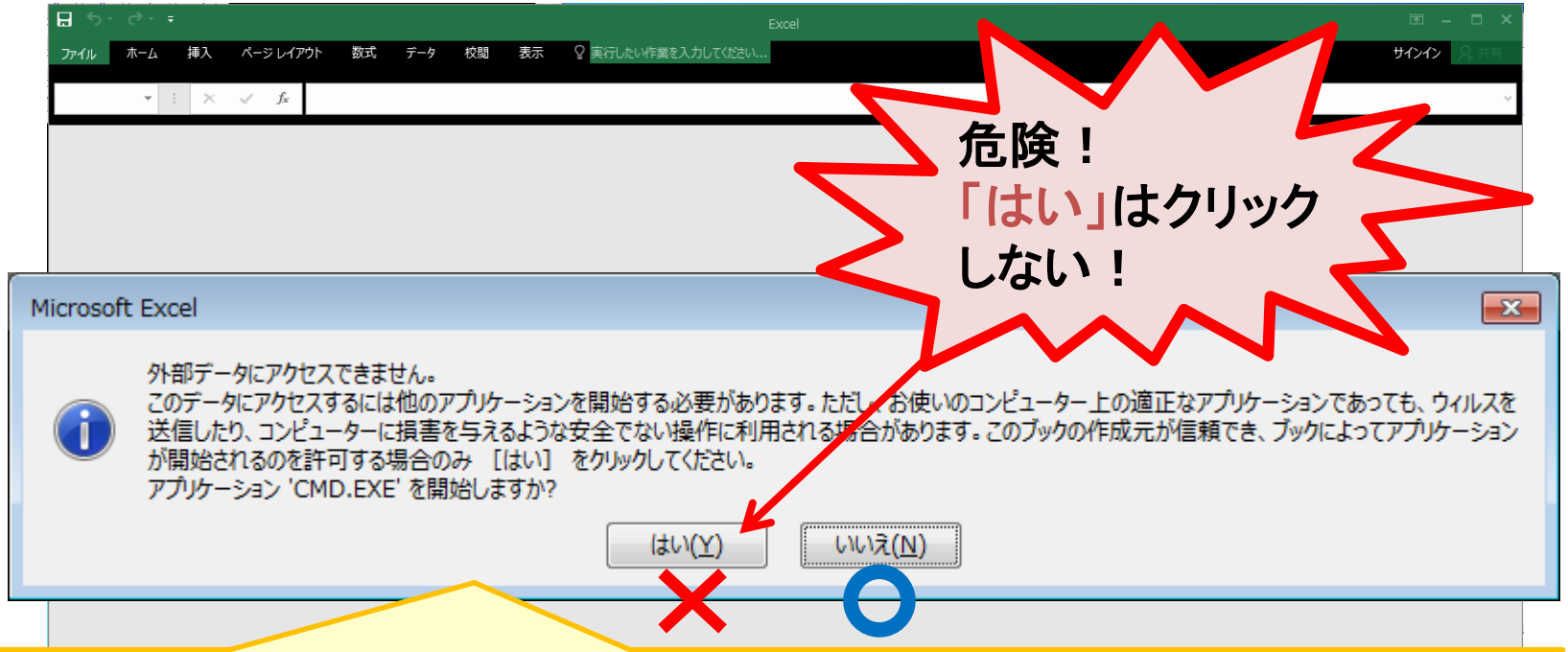


① SLKファイルを開くと、警告ウインドウが表示されます。
→**「無効にする」をクリックすることで攻撃を回避できます。**

[次ページへ続く]

攻撃の画面（2）

- 前ページの警告ウインドウで「有効にする」を選択してしまった場合

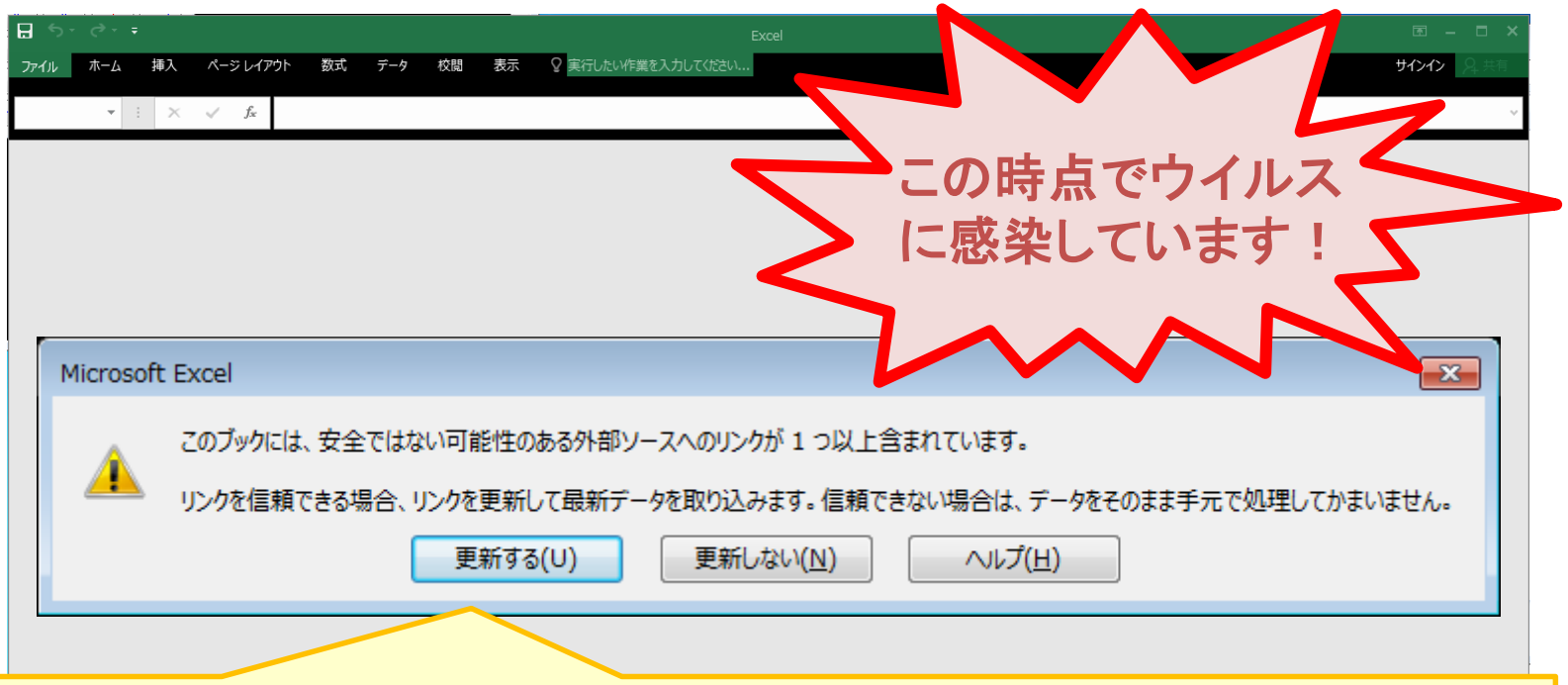


② アプリケーションの起動を確認する警告ウインドウが表示されますが、ここで「はい」をクリックすると、ウイルスがダウンロードされ、感染させられてしまいます。
→**「はい」はクリックしないでください。**

［次ページへ続く］

攻撃の画面（3）

- 前ページの警告ウインドウで「はい」を選択してしまった場合



③ 外部ソースの更新を確認する警告ウインドウが表示されますが、
この時点で<u>ウイルスがダウンロードされ、感染してしまっています</u>。
→ 操作を中断し、<u>**システム管理部門等へ連絡**</u>してください。

おわりに

本資料で説明した警告ウインドウが表示された場合は、安易に「有効にする」や「はい」をクリックしないでください。また、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。

本資料で説明したタイプの攻撃のほかにも、Microsoft Office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。

- ✓ **不審なメールの添付ファイルは開かない。**
- ✓ **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に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。**