【参考資料】

IQYファイル(※)を悪用する攻撃手口に関する注意点（第二版）

2018年 7月 初版公開
2018年 8月 第二版公開

独立行政法人情報処理推進機構
セキュリティセンター

※ Internet Query ファイル ：Microsoft Excel に関するファイル。

はじめに

Microsoft ExcelのIQY（Internet Query）ファイルを悪用する攻撃手口の情報が、2018年5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】

- IQY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、「.iqy」です。

※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

- 標的を絞った攻撃であるのか、無作為にばらまかれたものであるのかは不明ですが、悪意のあるIQY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。

  メールに添付されたIQYファイルを開くと、悪意のあるサーバからウイルスがダウンロードされて、パソコンに感染させられます。

- 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」を有効にしていても防御できず、表示される警告画面で攻撃を回避する操作をしなければ、ウイルスに感染させられてしまいます。

IQYファイルを悪用する攻撃の観測状況

- 2018年8月、日本語の件名・内容で、この手口による攻撃メールが国内に広くばらまかれたことを確認しています。今後も繰り返し攻撃に悪用される可能性があり、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。

特徴と対応方法

- 現時点で確認している「IQYファイルを悪用する攻撃手口」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IQY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、**ウイルスに感染させられてしまう。**

対応方法

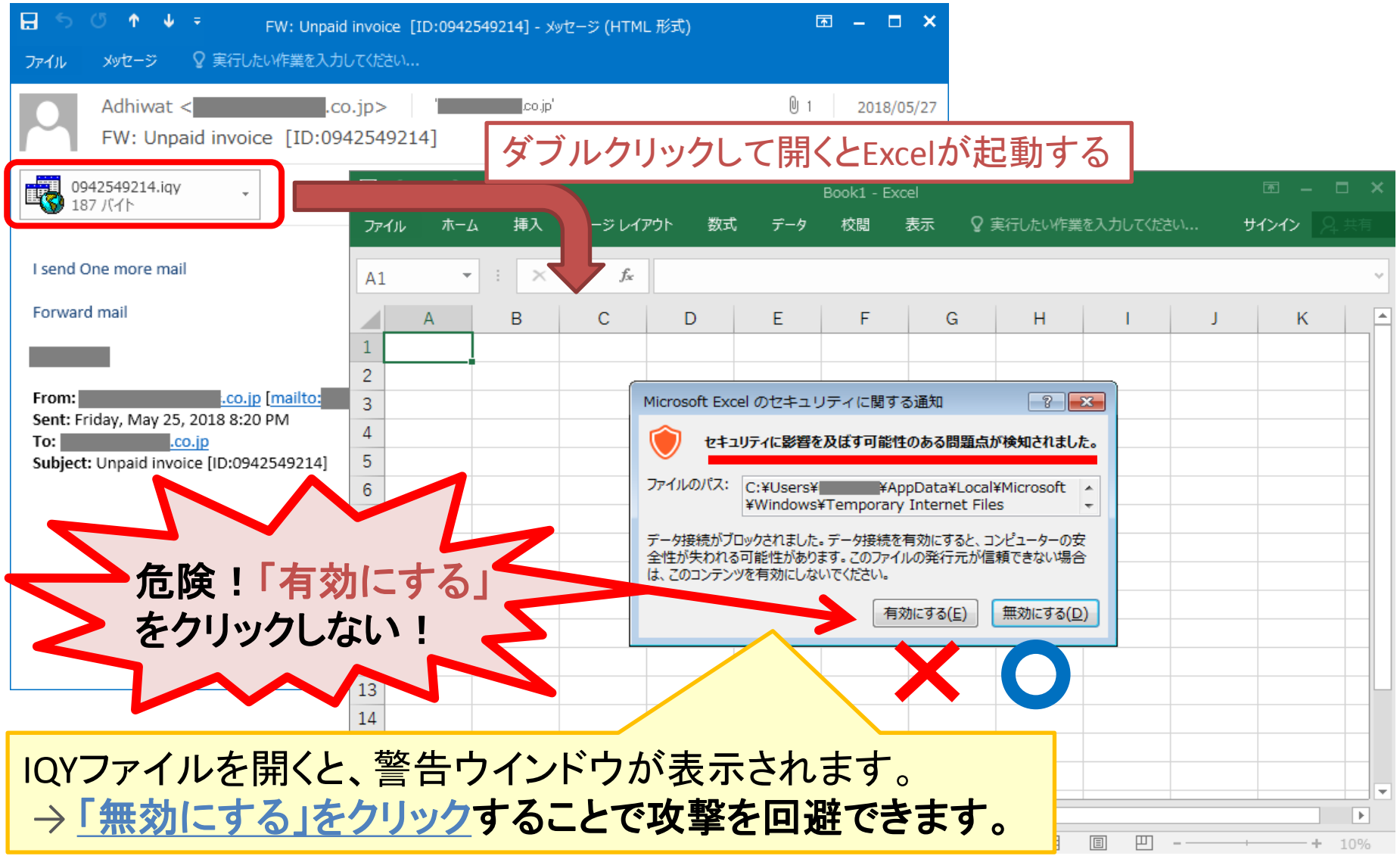
上記の特徴にあてはまる、身に覚えのないメールを受信した場合、IQYファイルを開かないよう注意するとともに、**システム管理部門等へ連絡**してください。
（なお、IQYファイルを開いただけではウイルスには感染しません）

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（2018年8月、日本語の攻撃メール）

事例紹介

- メールで送られた、罠が仕込まれたIQYファイルを開いた場合



【参考情報】この攻撃手口の防止策

- Microsoft Excelの次の設定を行うことで、IQYファイルをExcelで開かないようにすることができます。

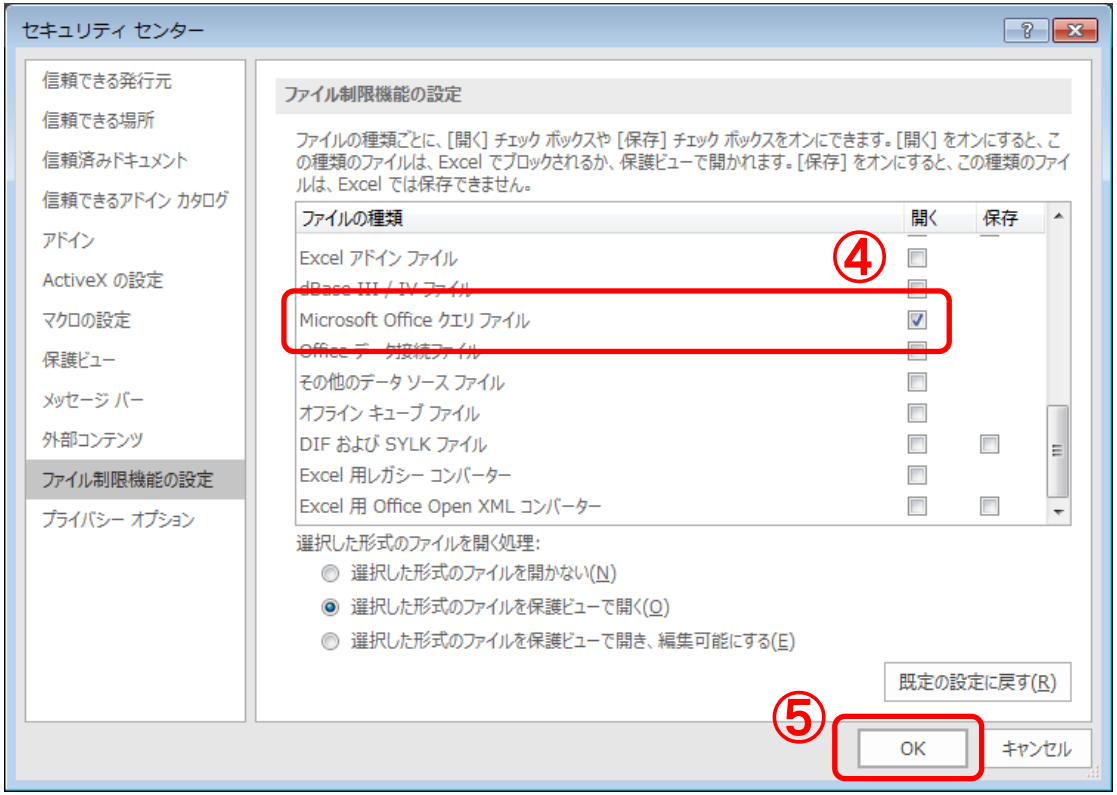
① Microsoft Excelを起動する

② メニューから、[ファイル]-[オプション]を選択する

③ Excelのオプションから、[セキュリティセンター]-[セキュリティセンターの設定]ボタンをクリックする

④ セキュリティセンターの[ファイル制限機能の設定]から、[Microsoft Office クエリファイル]の[開く]のチェックボックスにチェックを入れる

⑤ OKボタンをクリックする



※ 正規の目的で本機能を使用していないか、業務影響の有無を確認してから実施してください。

※ この他、.iqy 拡張子の関連付けをExcelからメモ帳に変更するといった方法でも対策できます。

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」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、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。**