【参考資料】

OLE(※)機能を悪用した文書ファイルの手口に関する注意点（第二版）

2019年 7月 初版公開
2020年 1月 第二版公開

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

※ OLE : Object Linking and Embedding

はじめに

Microsoft WordのOLE（Object Linking and Embedding）という機能を悪用し、悪意のあるマクロを埋め込んだWord文書ファイルを使っ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（手口自体は、従来より多く観測されている、マクロ機能を悪用したものです）。

【参考情報】

- OLE機能とは

  OLEはWindows環境において、複数のソフトウェアが連携したり、データを共有するための技術です。

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。

※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、表示されるアイコン等は異なる場合があります。

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、「OLE機能を悪用し、悪意のあるマクロを埋め込んだWord文書ファイル」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Word文書ファイルを開くと、ウイルスがダウンロードされ、端末がウイルスに感染させられることを確認しています。

- メールに添付された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。本攻撃手口でも「保護ビュー」を有効にしている状態では、ウイルスに感染しません。

本手口による攻撃の観測状況

- **2019年11月に、件名・本文が日本語で書かれたメールで、この手口による攻撃メールを確認しております。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

- 現時点で確認している、「OLE機能を悪用した文書ファイル」による攻撃には次のような特徴があります。

特徴

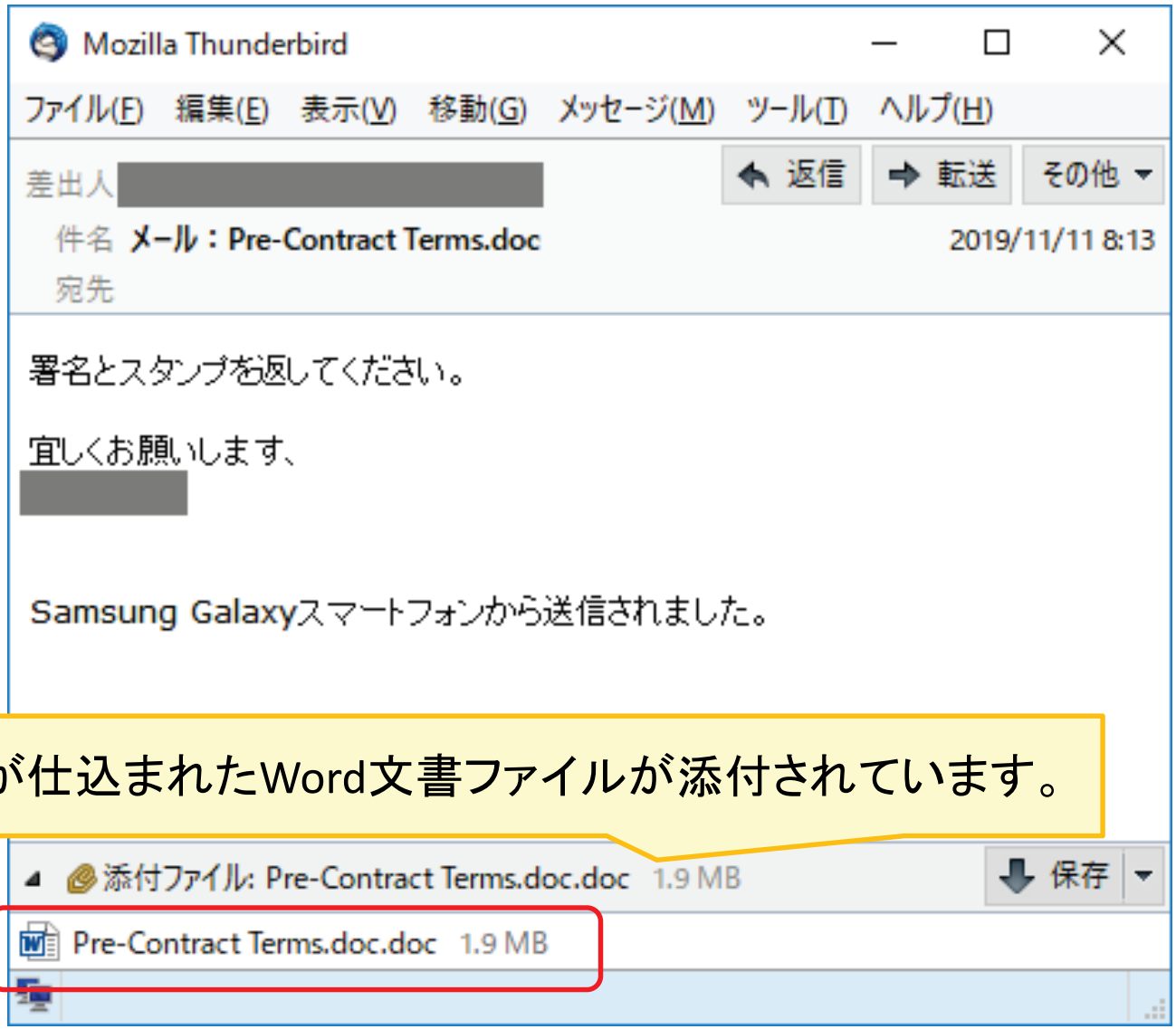
① Word文書ファイルを開くと、セキュリティの警告ウインドウが表示される。
② セキュリティの警告ウインドウの「マクロを無効にする」ボタンをクリックしても、同様の警告ウインドウが**何度も表示される。**
⇒ １回でも警告ウインドウで「マクロを有効にする」ボタンをクリックすると、**ウイルスに感染させられてしまう。**

対応方法

外部から入手したファイルなどについて、安全であると判断できない限り、上記のような動作をしても、「マクロを無効にする」ボタンをクリックし続けてください（「マクロを有効にする」ボタンはクリックしないでください）。併せて**システム管理部門等へ連絡**してください。

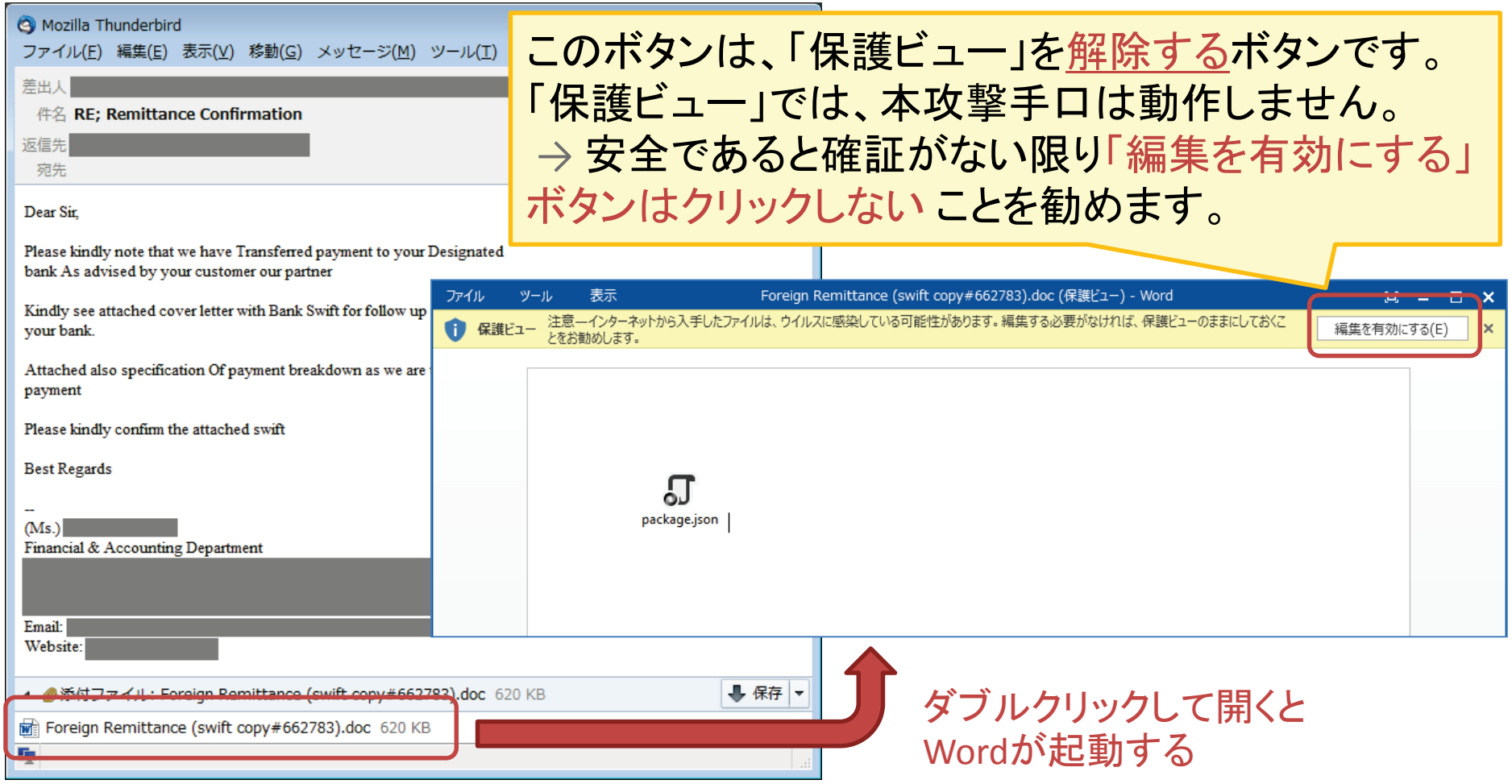
次のページからは、実際に確認した悪意のあるメールやファイルを例にして説明します。

事例紹介（2019年11月、日本語の攻撃メール）



事例紹介1

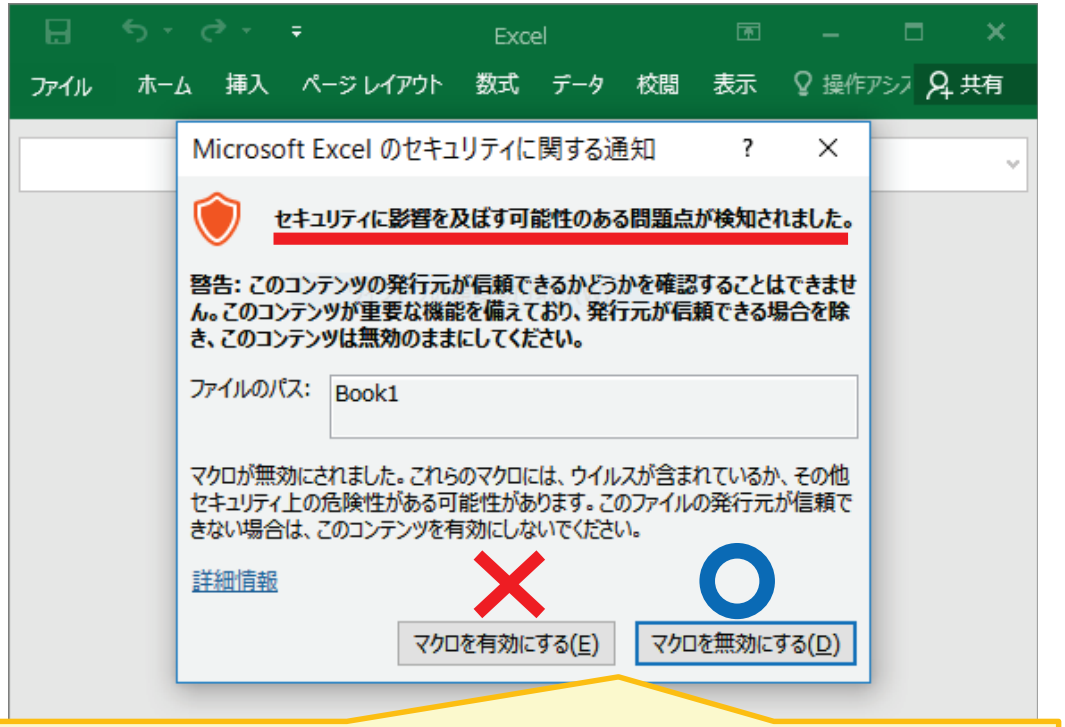
- メールに添付されている状態から、添付ファイルを開いた場合



事例紹介２－（１）

- メール等で送られた、罠が仕込まれたWord文書ファイルを開いた場合

ファイルを開く

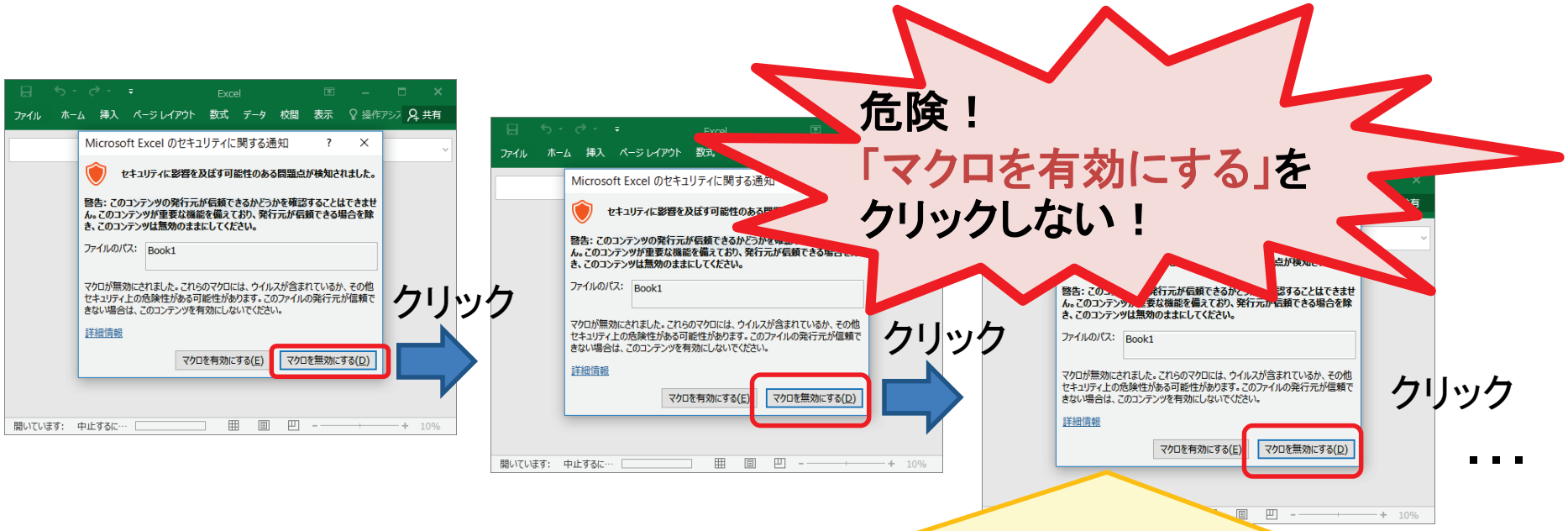


Word文書ファイルを開くと、警告ウインドウが表示されます。
（この事例では、Word文書であるにも関わらず、Excelの警告ウインドウが表示されるよう仕掛けが施されており、判断しにくくなっています。）
→ **マクロの実行を防ぐため、「マクロを無効にする」をクリックしてください。**
※「マクロを有効にする」をクリックするとウイルスに感染してしまいます

［次ページへ続く］

事例紹介2－(2)

- セキュリティの警告ウインドウは、何度も表示する仕掛けが施されており、「マクロを無効にする」ボタンをクリックしても複数回表示されます。



「マクロを無効にする」ボタンをクリックしても、同じ画面が何度も表示されますが、**「マクロを有効にする」はクリックしないでください**。
1回でも「マクロを有効にする」ボタンをクリックするとウイルスに感染させられてしまいます。
→ **「マクロを無効にする」を選択し続けることで攻撃を回避できます。**

【参考情報】この攻撃手口の緩和策

- 本攻撃手口では、「保護ビュー」を有効にしている状態だと、マクロ入りExcelオブジェクトが動作しないため、ウイルス感染を防ぐことができます。
- 現在、RTFファイルによる攻撃を確認しており、Microsoft Wordの次の設定を行うことで、RTFファイルを常に保護ビューで開くようにすることができます。
  - 利用者が保護ビューを無効にする操作を行った場合は、マクロ入りExcelオブジェクトが動作し、マクロの警告ウインドウが表示されます。その状態でマクロを有効化すると、ウイルスに感染させられてしまいます。

① Microsoft Wordを起動する
② [ファイル]-[オプション]を選択する
③ 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、[RTF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

※ 業務影響の有無を確認してから実施してください。

おわりに

マクロに関する警告が表示された場合、安全であると判断できない限り、**「マクロを有効にする」というボタンはクリックしない**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。**