【参考資料】

文書ファイルの新たな悪用手口に関する注意点

2017年7月27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**

はじめに

ウイルスに感染させるための罠が仕掛けられた悪意のある文書ファイルは、これまでにもOfficeの脆弱性の悪用や、マクロ機能を悪用する手口のものがありました。

昨今、それらとは異なる新たな攻撃手口を使ったものが出てきています。

本資料は、新たな攻撃手口について紹介し、注意点を説明するものです。

本資料では、次の3つの攻撃手口を紹介します。

① アイコンのような画像が埋め込まれた文書ファイル
② Word文書ファイルが埋め込まれたPDFファイル
③ 細工されたスライドショー形式PowerPointファイル

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、添付された不審な文書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 2010、Adobe Reader XI 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。

① アイコンのような画像が埋め込まれた文書ファイル

特徴

特徴①：Word、Excel等のOffice文書ファイル。
特徴②：文書ファイルを開くと、**アイコンのような画像**がある。
⇒ この画像をクリックすると、更に**警告ウインドウが表示される**が、
そこで「OK」をクリックすると、**ウイルスに感染させられてしまう。**

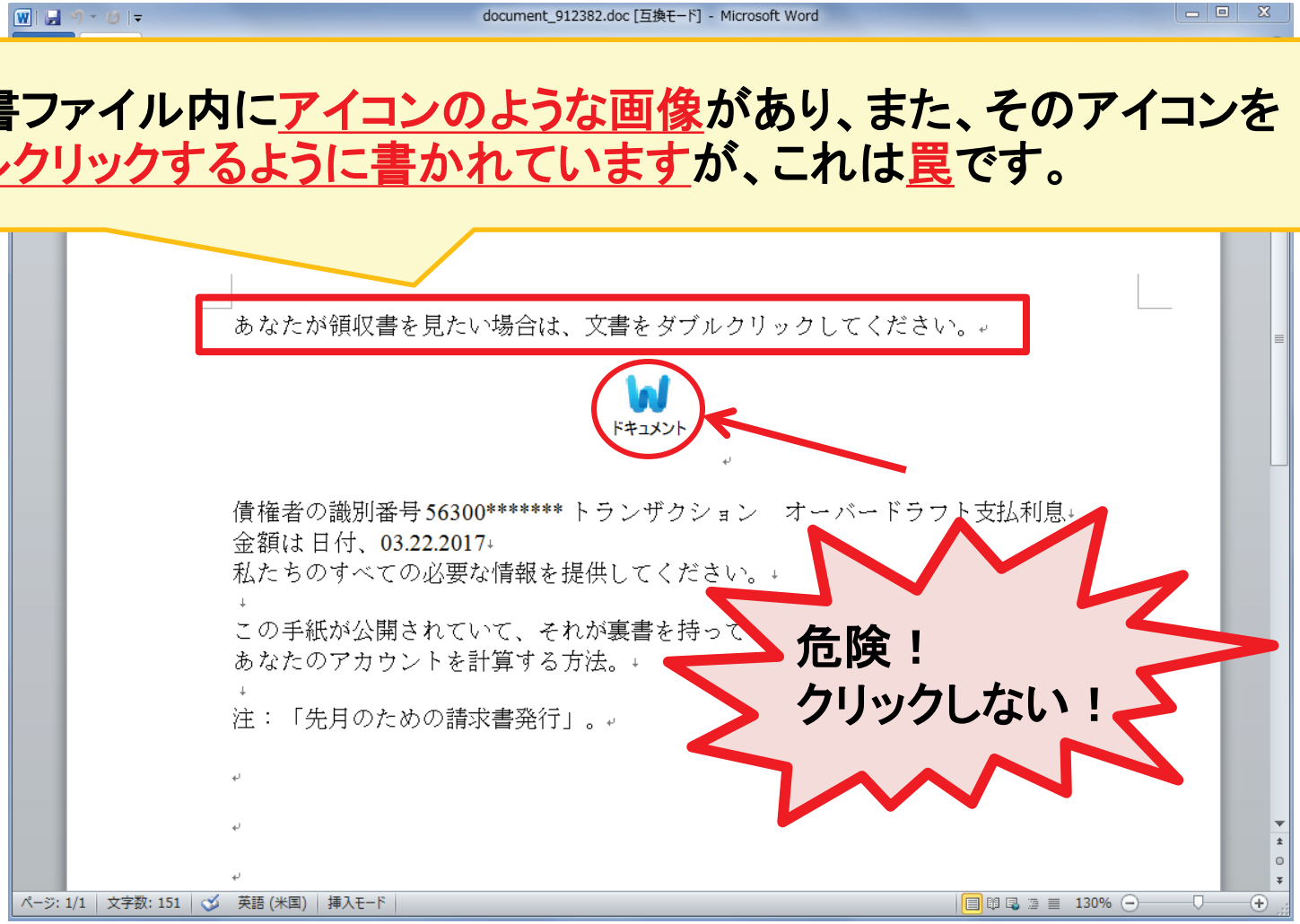
対応方法

身に覚えのないWord等の文書ファイルを開かないよう注意するとともに、ここで説明する特徴が見られた場合、**システム管理部門等へ連絡**してください。
（なお、文書ファイルを開いただけではウイルス感染しません）

次のページからは、公開情報から得られた実際のWord文書ファイルを例にして説明します。

① アイコンのような画像が埋め込まれた文書ファイル

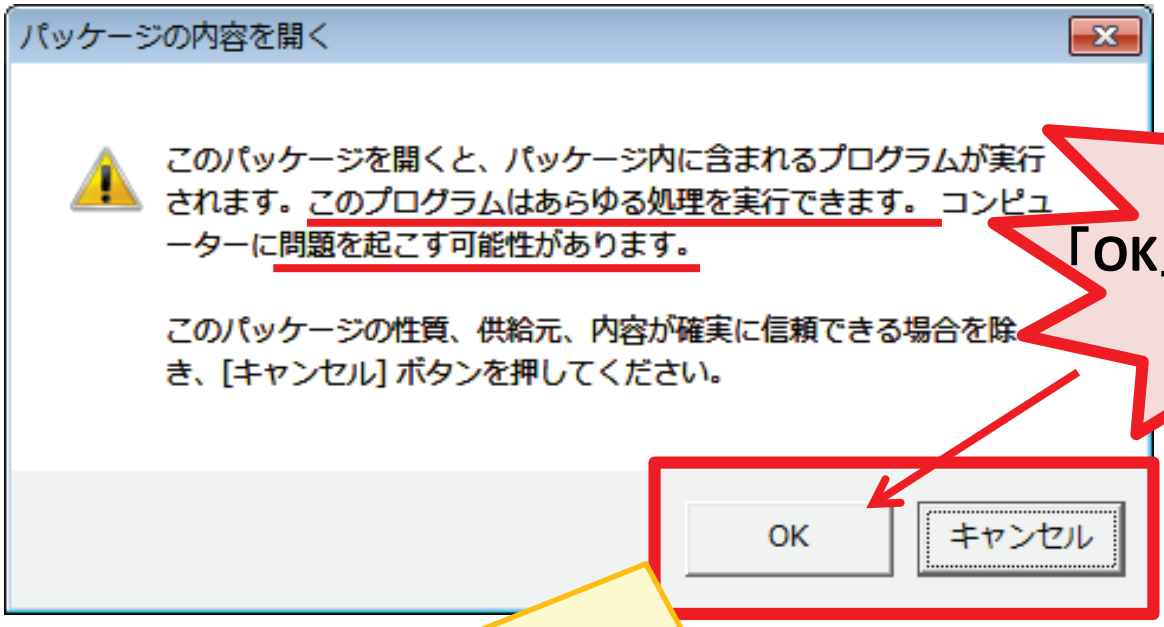
ファイル動作（事例1）



[次ページへ続く]

① アイコンのような画像が埋め込まれた文書ファイル

ファイル動作（事例1）

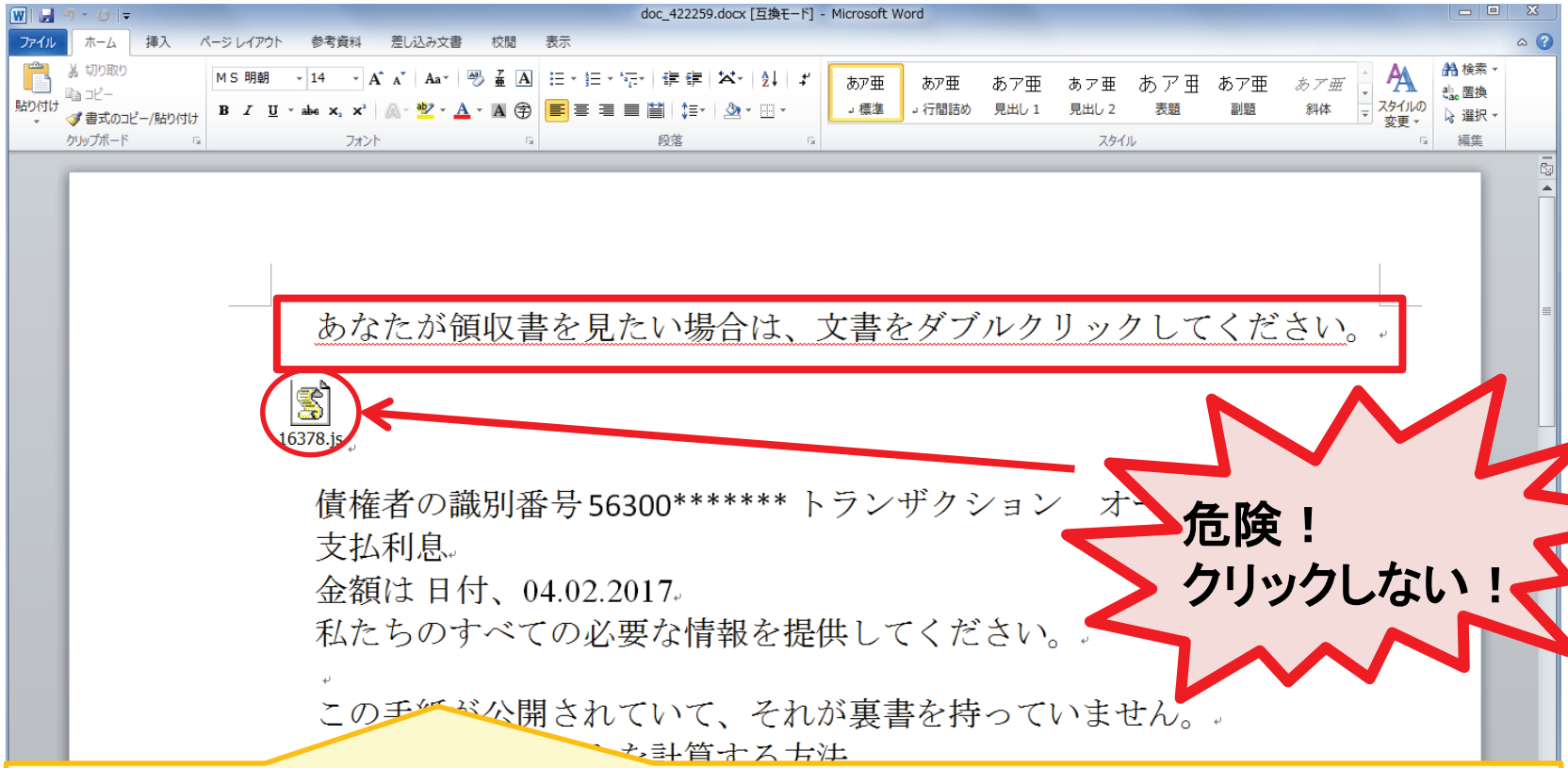


危険！！
「OK」はクリックしない！

②前ページの罠のアイコン画像をクリックした場合、このような警告ウインドウが開きます。ここで「OK」ボタンをクリックすると、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。 → 「キャンセル」をクリックしてください。

① アイコンのような画像が埋め込まれた文書ファイル

ファイル動作（事例2）



事例1のファイルと同じく、アイコン画像をクリックした場合、警告ウインドウが開きます。「OK」ボタンをクリックすると、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。

② Word文書ファイルが埋め込まれたPDFファイル

特徴

特徴：PDFファイルを開くと、Word文書ファイルを開く旨の**警告ウインドウ**が表示される。

⇒ Word文書ファイルを開くことを選択すると、Word文書ファイルが開く。
Word文書ファイルにはマクロ機能を有効にするように記載されている。
マクロ機能を有効にする操作を行うと、**ウイルスに感染させられてしまう。**

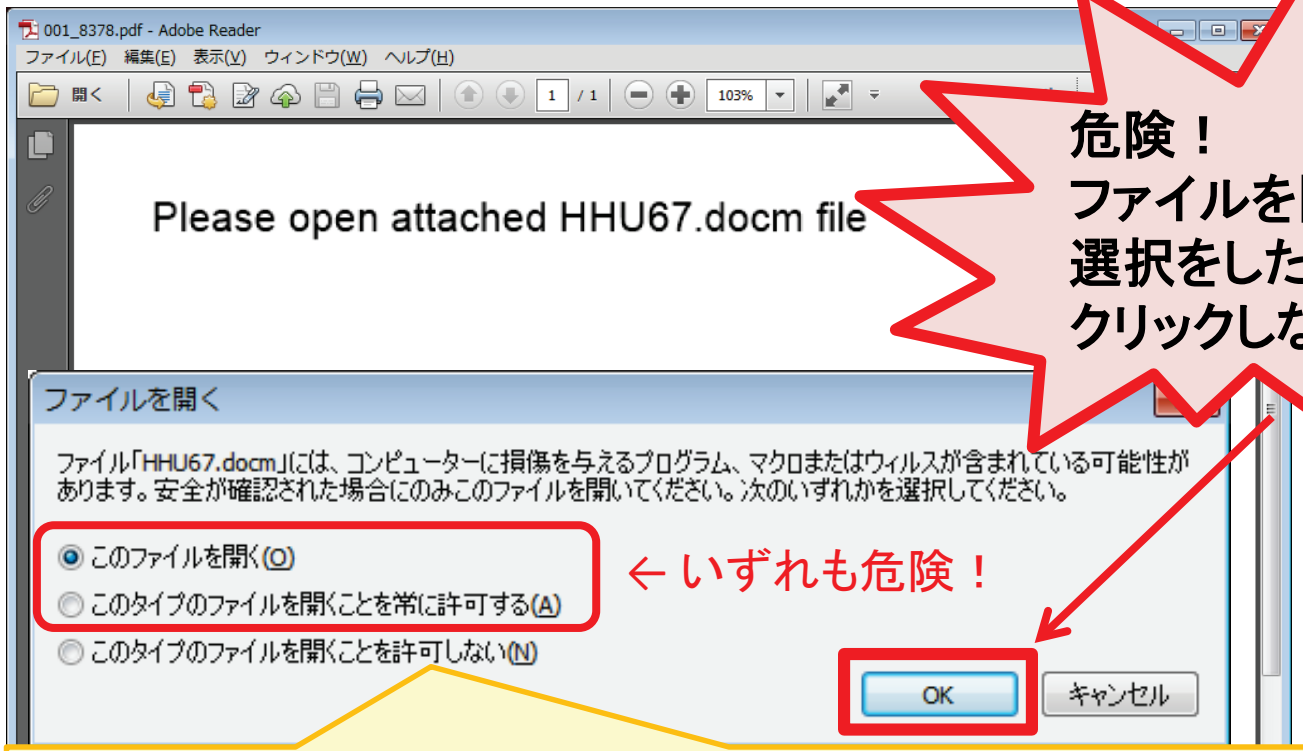
対応方法

身に覚えのないPDFファイルを開かないよう注意するとともに、ここで説明する特徴が見られた場合、**システム管理部門等へ連絡**してください。
（なお、PDF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、公開情報から得られた実際のPDFファイルを例にして説明します。

② Word文書ファイルが埋め込まれたPDFファイル

ファイル動作



危険！
ファイルを開くという
選択をした状態で
クリックしない！

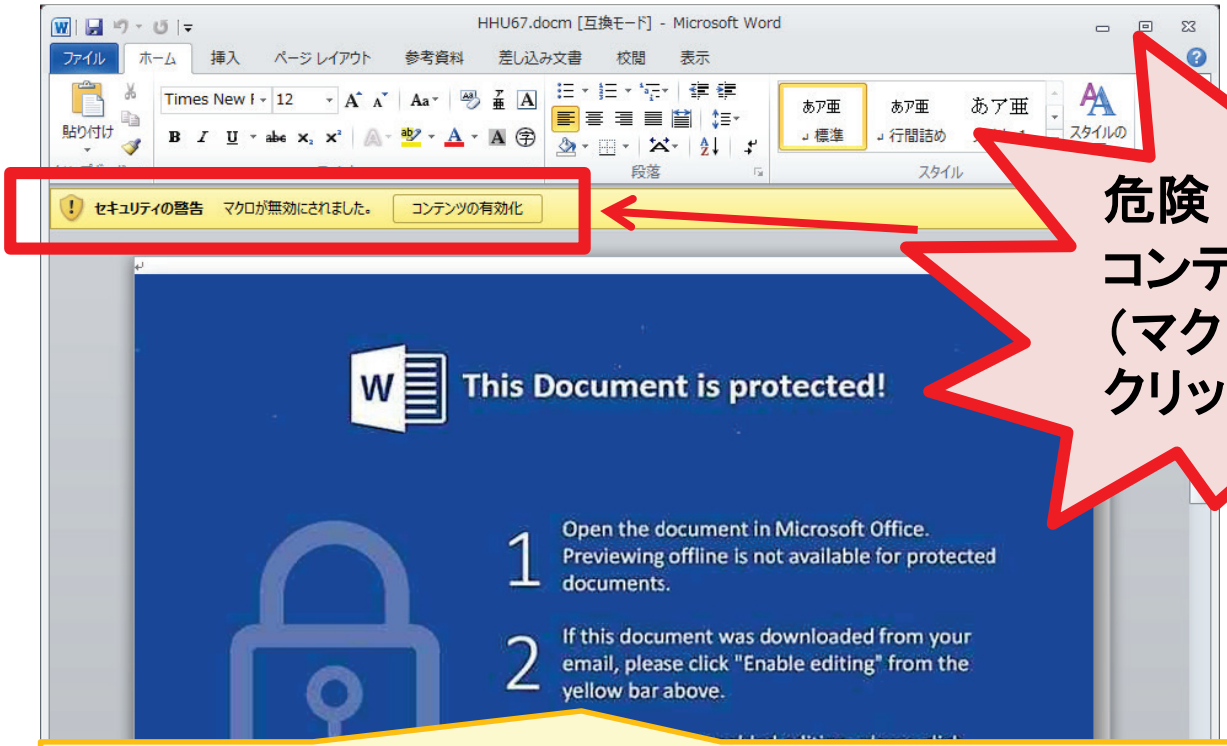
← いずれも危険！

① PDFファイルを開くと、このような警告ウインドウが開きます。ここで「このファイルを開く」または「このタイプのファイルを開くことを常に許可する」を選択した状態で「OK」ボタンをクリックすると、悪意のあるWord文書ファイルが開きます。 →**「キャンセル」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]

② Word文書ファイルが埋め込まれたPDFファイル

ファイル動作



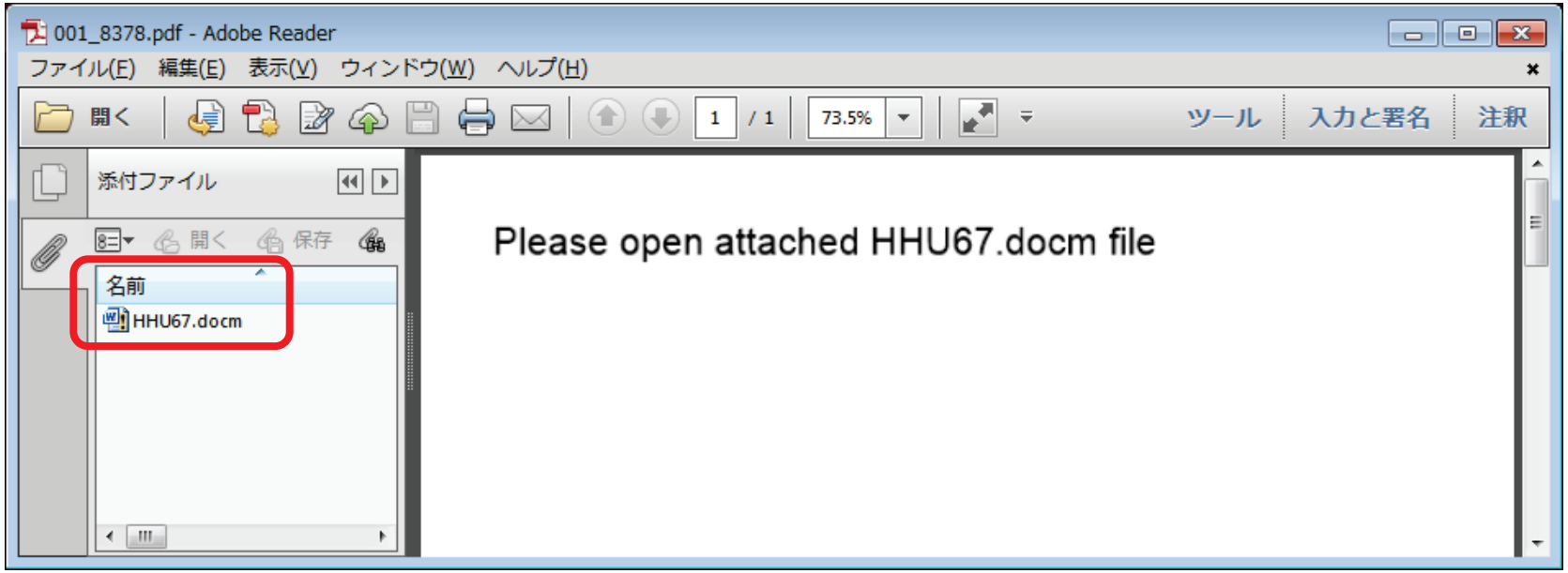
危険！
コンテンツの有効化（マクロの有効化）はクリックしない！

② Word文書ファイルが開くと、マクロの有効化を促す内容が記載されていますが、**これは罠です**。ここで「コンテンツの有効化」（マクロの有効化）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。→**「コンテンツの有効化」はクリックしないでください。**

② Word文書ファイルが埋め込まれたPDFファイル

攻撃の仕組み

- PDFファイルが自動的にWord文書ファイルを開こうとする動作は、Adobe Acrobat/Adobe Readerの標準機能であるPDFにファイルを添付する機能を悪用することで発生しています。
- 具体的には、本件のPDFファイルには、次のように攻撃者によってWord文書ファイルが添付されています。これにより、この悪意のあるWord文書ファイルが開かれるように細工されています。



② Word文書ファイルが埋め込まれたPDFファイル

防止策

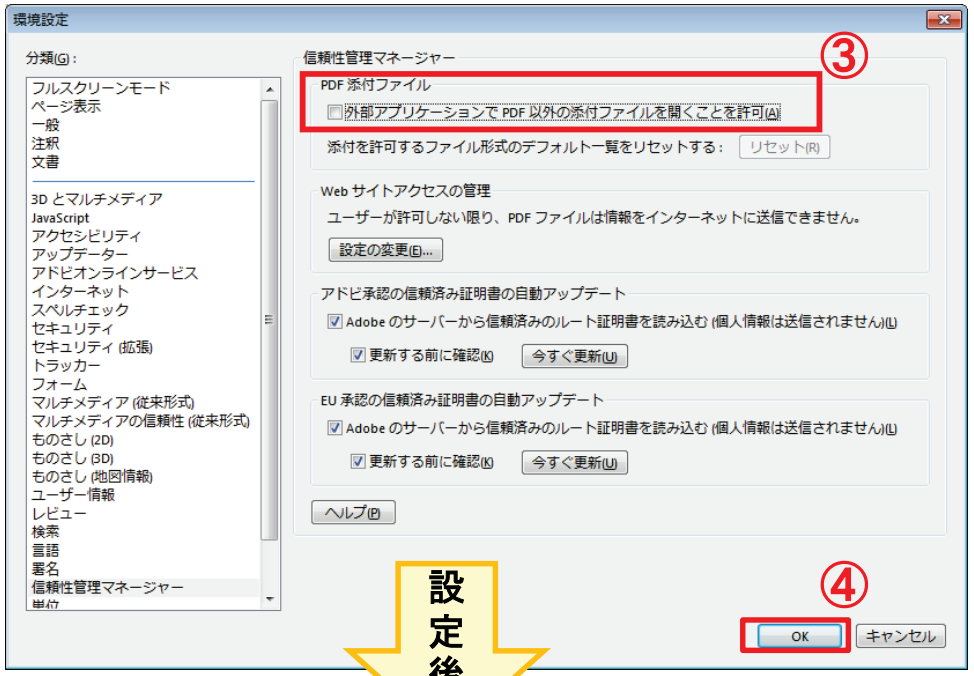
次の設定を行うことで、PDFファイルに添付されているファイルを実行したり開かないようにできます。

① Adobe Acrobat/Adobe Readerを起動する

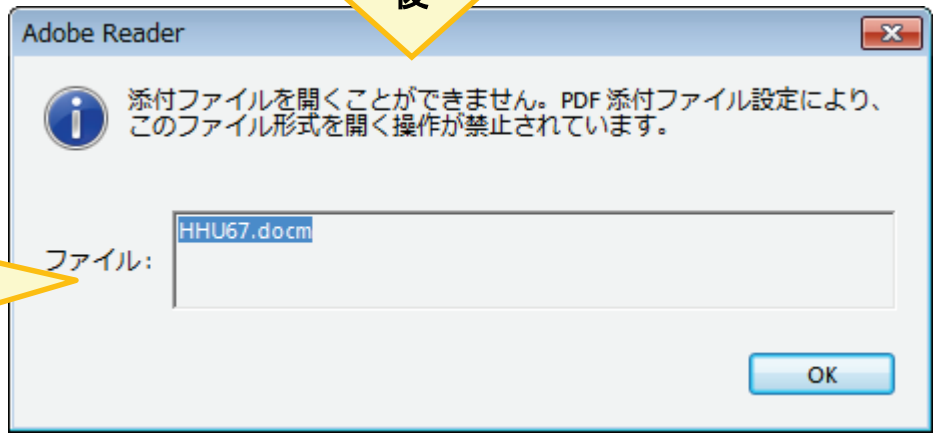
② メニューから、[編集]-[環境設定]を選択する

③ [分類]-[信頼性管理マネージャー]を選択し、「外部アプリケーションでPDF以外の添付ファイルを開くことを許可」のチェックボックスの**チェックを外す**

④ OKボタンをクリックする



設定後



本防止策を設定後、本件のPDFを開くと、このような警告ウインドウが表示され、Word文書ファイルが開かれなくなります。

※ 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。

③ 細工されたスライドショー形式PowerPointファイル

特徴

特徴①：PowerPointスライドショーファイル形式 (.ppsx) ※である。
特徴②：ファイルを開くとスライドショーが表示される。罠が仕掛けられたエリアにマウスカーソルが触れると警告ウィンドウが表示される。
⇒「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。

※PowerPointスライドショーを直接表示するファイル形式で、通常のPowerPointファイル(拡張子：ppt、pptx)とは異なり、スライド編集画面が表示されません

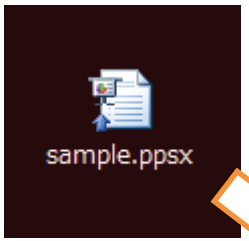
対応方法

身に覚えのないPowerPointファイルを開かないよう注意するとともに、ここで説明する特徴が見られた場合、**システム管理部門等へ連絡**してください。
（なお、PowerPointファイルを開いただけではウイルス感染しません）

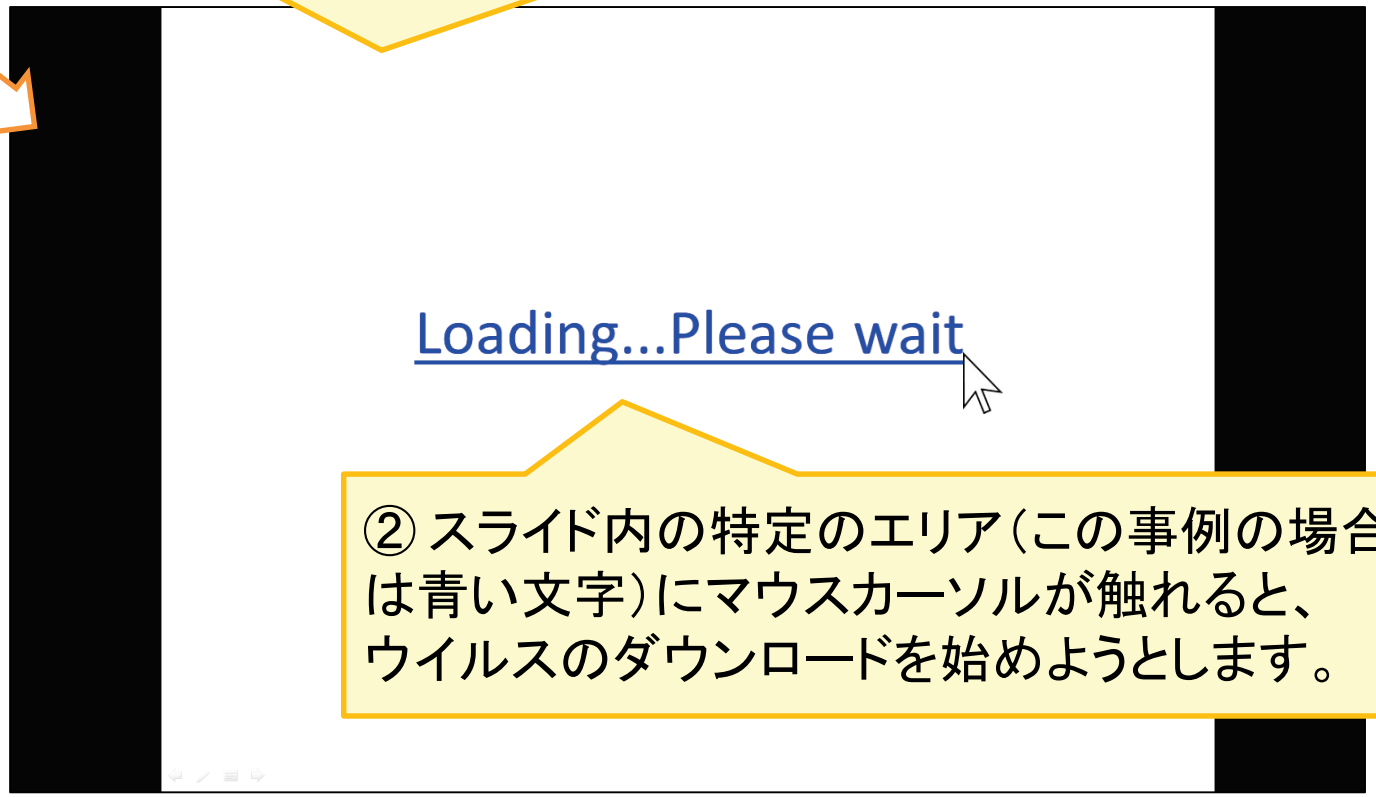
次のページからは、公開情報から得られた実際のPowerPointファイルを例にして説明します。

③ 細工されたスライドショー形式PowerPointファイル

ファイル動作



① ファイルを開くとスライドショーが表示されます。



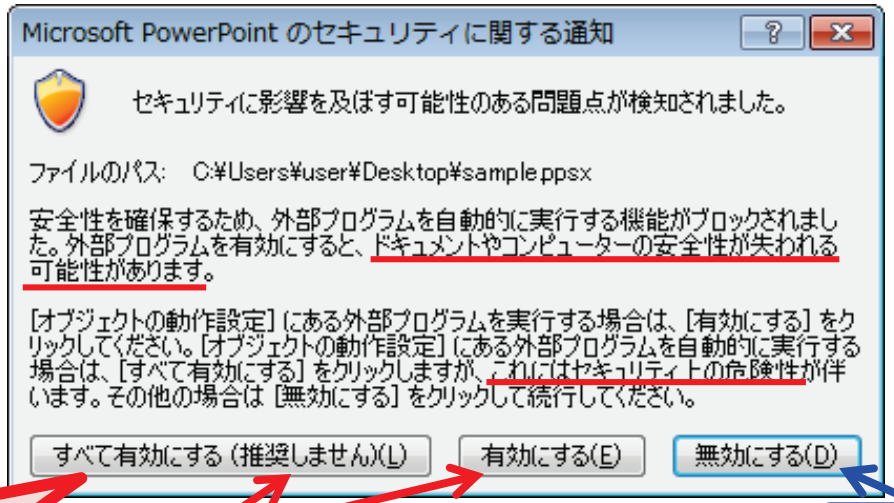
② スライド内の特定のエリア（この事例の場合は青い文字）にマウスカーソルが触れると、ウイルスのダウンロードを始めようとします。

［ 次ページへ続く ］

③ 細工されたスライドショー形式PowerPointファイル

ファイル動作

③ マウスカーソルが文字に触れると、この警告ウインドウが表示されます。
ここで「すべて有効にする」または「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。
⇒**「無効にする」をクリック**することで攻撃を回避できます。



危険！！
クリックしない！

「無効にする」を
クリックする！

おわりに

本資料で説明した悪用手口のほかにも、文書ファイルの機能を悪用してウイルスに感染させようとする手口や、文書ファイルの脆弱性を悪用する手口が存在します。

ウイルスに感染させられないようにするため、次のような基本的なウイルス対策を心掛けてください。

- ✓ **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文書ファイル等を開き、警告ダイアログ等が表示された場合、警告の内容をよく確認し、むやみに「OK」や「有効にする」といったボタンをクリックしない。**