Ksisnetだより
発行:Ksisnet事務局
平成29年10月18日
Vol.36

油断していませんか？ メールに添付のPDFファイル

PDFファイル（拡張子「.pdf」）とは、印刷したときの状態をデータでそのまま保存することができるファイル形式です。

誤操作などによる意図しない編集を避けることができ、見やすく扱いやすいことから、ワードやエクセル、パワーポイントの資料をPDFファイルに変換して使っている方も多くいます。

標的型攻撃メールや無差別型攻撃メールの多くは、実行ファイル（拡張子「.exe」など）が添付されていたり、ワードやエクセルのマクロ機能を悪用した不正なプログラムが仕込まれている危険性があることは今は多くの方が認識し注意を払っていますが、PDFファイルの場合はどうでしょうか？

「PDFファイルだから安全」と油断したりしていないでしょうか？

本当にPDFファイルって安全なのかな？？

CAUTION PDFファイルを利用したサイバー攻撃は可能です！

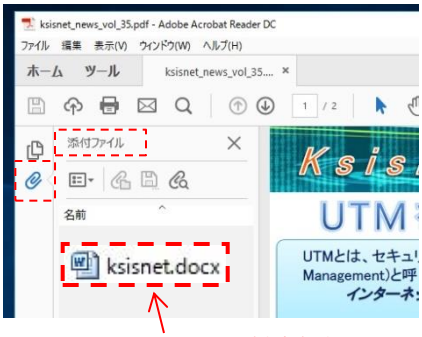
PDFファイルを利用したサイバー攻撃例

1　アイコン・拡張子の偽装

アイコンをPDFファイルのものに差し替え、拡張子の偽装や大量のスペース挿入などにより一見すると拡張子が「.pdf」のように見せかけることにより不正プログラムを開かせます。

2　不正プログラムの埋め込み

PDF編集ソフトにより不正なプログラム（JavaScript）を埋め込んだり、不正なマクロ付きのワードファイルを添付することが可能です。この埋め込まれたファイルを開くとウイルスなどの不正なプログラムがダウンロードされたりします。



3　閲覧ソフトの脆弱性を利用

閲覧ソフトの脆弱性を利用する不正なコードを埋め込むことで、PDFファイルを開いたときに閲覧ソフトがその不正なコードを読み込み、ウイルスなどの不正なプログラムを開かせます。

被害に遭わないために

- ✓　添付ファイルの形式をプロパティ等でしっかり確認する
- ✓　「Acrobat　Reader」などの閲覧ソフトはJavaScriptの実行時に警告画面が出るので、必要がなければ実行をブロックする
- ✓　閲覧ソフトの脆弱性が利用されないように、ソフトは最新の状態に保つ
- ✓　不正プログラムを検知できるようにウイルス対策ソフトを導入し最新の状態に保つ