

メールの添付ファイルに注意してください！

実在する会社名等を装って不正プログラムをメールで送りつける「ばらまき型メール攻撃」による感染被害が後を絶ちません。

不審なメールを開かないために、添付ファイルの不審点を見分けるポイントを紹介します。

～不審な添付ファイルの見分け方～

【注意すべき拡張子】

「.exe」は、パソコン内でプログラムを実行させるファイルの拡張子で、この拡張子を持つファイルがメールで送られてきた場合は、不正プログラムである危険性があります。

右図の拡張子もプログラムを実行させるファイルの拡張子であり注意が必要です。

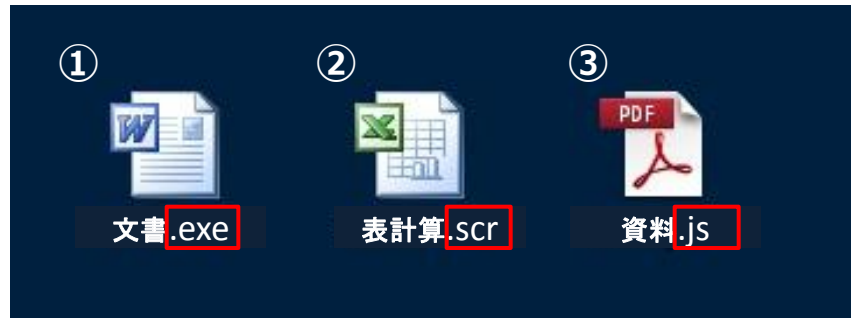
.exe .com .bat .cmd .pif .scr

他にも、「VBS」や「VBE」、「JS」、「JSE」、「WSF」、「WSH」といったスクリプトファイルの拡張子にも注意!!

【アイコンの偽装に注意】

アイコンを偽装して実行プログラムのファイルであることを隠す手口もあります。

- ① アイコンは「Wordファイル」、
実際は「実行形式ファイル」
- ② アイコンは「Excelファイル」、
実際は「スクリーンセーバーファイル」
- ③ アイコンは「PDFファイル」、
実際は「JavaScriptファイル」



※ 「拡張子」とは、ファイルの種類を識別するためにファイルの末尾に付く文字列のことで、Wordであれば「.doc」「.docx」、Excelであれば「.xls」「.xlsx」等となります。

～メール攻撃の対策～

- ◎ 不審なメールは開かず、送信者名や送信者のアドレス、添付されたファイル（拡張子が「.zip」「.exe」等）、添付されたURL、文面を確認してください!!
- ◎ 不審なメールを発見すれば、直ちに社員等に周知することが重要です。
- ◎ ウイルス対策ソフトやソフトウェアを最新の状態に更新してください!!
更新されていない場合は、効果はありません。

京都中小企業情報セキュリティ支援ネットワーク (Ksisnet)

お困りの時は!! IT 相談窓口 (公益財団法人京都産業21 お客様相談室)



相談内容：情報セキュリティ対策、情報漏えい・流出事案等
※毎週月曜日～金曜日の9:00～17:00（祝日を除く）

TEL 075-315-8660 メールアドレス okyaku@ki21.jp



公益財団法人京都産業21 お客様相談室 (〒600-8813 京都市下京区中堂寺南町134 京都府産業支援センター内)