

静岡県警察からのお知らせ

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】

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。

**.exe .com .bat .cmd .pif .scr
.VBS .VBE .JS .JSE .WSF .WSH**

※ 「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。

【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」



～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。

お問い合わせ先

静岡県警察本部生活安全部サイバー犯罪対策課
企画指導係

TEL：054-271-0110（代表）
711-3496（内線）