標的型メール攻撃に注意

奈　良　県　警　察
令和元年７月１日

あなたの会社は大丈夫ですか？？

標的型メール攻撃とは？

特定の組織や人物を狙って、受信者が思わず開いてしまいそうになる送信元、件名、本文によりメールの開封を誘い、**メールに添付したファイルからコンピュータウイルスを感染**させたり、**感染させるウェブサイトに誘導**して、情報を盗み出す手法です。

標的型メール攻撃対策チェックリスト

☑ 送信元を確認する

- ☐ 今までにメールのやりとりがない相手、存在しない組織からのメール
- ☐ メールアドレスに不審点がある（フリーのメールアドレスを使用している、送信元とメール本文の署名に記載されたメールアドレスが異なる等）

☑ メール本文を確認する

- ☐ 業務上、自分宛に届くべきメールではない
- ☐ 日本語（文法や漢字）に不自然な点がある
- ☐ 緊急の対応の要求、添付ファイルを開かざるを得ない、または、開きたくなるような興味を引く内容

（災害情報、製品に関する問い合わせ、クレーム、取材の申し込み、人事情報等）

☑ その他

- ☐ 添付ファイルが実行形式の【exe、scr】、圧縮ファイルの【zip】
  ※　これらのファイルに限らず、ワード、エクセル形式のファイルの場合もあるので注意が必要

１つでもチェックがつけば、標的型メール攻撃の可能性があります！！絶対にファイルを開かないで下さい。

従業員の皆さんのセキュリティ意識を高めることが重要です！

被害に遭わないように気をつけましょう

サイバーセキュリティに関する対応方法等が載っていますので、参考にして下さい。
【（ここからセキュリティ）　https://www.ipa.go.jp/security/kokokara/】