まず報告！
あなたは、不審なメールへの
不適切な操作をしました！

・“標的型攻撃メール”に対する適切な対応力の強化を目的として、訓練用のメールを送信しました。

・本メールは訓練用であるため、添付ファイルを開いたり、リンクをクリックすることによる危険性はありません。

・このメールが実際の“標的型メール”であった場合、ウィルスの感染・拡散など非常に危険な状態となります。

不審なメールを受信した際の対応方法は？

・業務に無関係なメール(不審なメール)を受信したら、添付ファイルを開いたり、メール本文にあるリンクをクリックしたりしないこと。

・不審なメールに気づいたら、**まずは上長に報告**し、指示を仰ぐこと。

・万が一不審メールの添付ファイルを開いたり、リンクをクリックしたら、**速やかに上長へ報告**し、上長から「**経営企画部　村田（1106）または　竪山（1104）**」へ連絡し、指示を仰ぐこと。

“標的型攻撃メール” かもしれない 「ポイント」

① 差出人が、見知らぬドメインやフリーメールアドレスからになっている
② 件名や本文で日本語らしくない言い回しになっていたり、日本語では使用されない漢字（繁体字、簡体字）が使用されている
③ 会社や組織が実在しない
④ 添付ファイルの拡張子が実行ファイル形式（exe/scr/jar/cpl など）やショートカットファイル（lnk/pif/url）
⑤ 表示されている URL と実際のリンク先の URL が異なる　など

※今回は①に該当。標的型攻撃では、本物と見分けのつかないような内容のメールがありえます！