これは、標的型メール攻撃の模擬訓練です。

今回メール利用者を対象に、標的型メール攻撃の模擬訓練を実施しました。
情報セキュリティ強化の一環として本訓練を実施しましたことをご理解いただき、ご了承願います。

↓必ずお読み下さい！　★標的型攻撃から身を守るポイント★

1. 差出人名を確認しましょう。見知らぬ差出人やフリーメールアドレスからのメールに添付されているファイルや
   URLにはアクセスしないようにしましょう。
2. 自分に関係があると感じる差出人からのメールでも、差出人アドレスが適切なドメインからのものであるかを確認しましょう。
3. そのメールが自分宛のメールかどうか確認しましょう。直接自分宛のメールでなければ、
   URLアクセスや添付ファイルの開封には注意を払う必要があります。
4. 差出元の組織が実在するのかを確認しましょう。
5. 署名（発信者の記載）に所在地や連絡先がキチンと明記されているかを確認しましょう。
6. 「大至急」などと危機感を煽っている内容になっていないか確認しましょう。
   直接自分宛でないメールで大至急などと言って何らかのアクションを促すのは標的型攻撃の特徴です。
7. 社内メールや、良く利用するサービスを装う攻撃メールも増えています。身に覚えのない内容の場合は、
   URLアクセスや添付ファイルの開封などを行う前に、今一度差出人アドレスやその他ポイントを確認してください。

以上のようなことに注意し、不審だと思われるメールに添付されたファイルの開封やURLアクセスはせず、

メールを削除し、管理部署もしくは上司へ報告する事が適切な対処となります。

★補足事項★

・このURLへのアクセス/添付ファイルの開封によって、パソコンが影響を受けることはありません。
・メールを開封してしまったことを報告する必要はありません。
・訓練精度を保つため、本メールが届いたことを周囲の方に伝えないで下さい。

通信監視強化やウィルス対策徹底等、標的型メール攻撃への対策を継続して実施する事とは別に、

利用者一人ひとりが日頃から標的型メール攻撃に注意すること が重要な予防策となります。

標的型メールのURLへアクセスしたり、添付ファイルを開封すると、当該パソコンがウィルスに感染し、

それが原因で機密情報が 漏洩する可能性もありますので、今後も注意をお願いします。

以上