

標的型攻撃メールを気付かないで 開封してしまうと **社会的信用を失う事も...**

- マルウェア感染により機材の買い替え**
- 取引先の信用を失い取引停止に**
- 感染元調査の金銭的被害**
- 個人情報の流出と改ざん**

2021年に発生したセキュリティインシデント1,451件のうち

49.2%がメールとWEBアクセス

に起因がある※といわれ、特定の企業や組織を狙った**標的型攻撃メール**により、情報を盗み出すウイルスに感染し機密情報が漏洩する事態に陥る被害が近年増加しています。

※デジタルアーツ(株)「国内企業・団体の情報セキュリティ対策の実態を調査」より引用

人的ミスは研修で減らすことができます！

標的型攻撃メールへの備えのために擬似環境で訓練をしましょう！

システムから疑似攻撃メール

誤ってクリックすると注意

これは標的型攻撃メールの訓練です。
本訓練は標的型攻撃メールを模擬的に体験していただき、攻撃メールに対する注意の向上を目的としております。そのため、用途に本訓練の登録を推奨してまいります。

実際の標的型攻撃メールでは、添付ファイルの開封や本文に記載されているURLへのアクセスから情報漏洩のリスクが生じることがあります。

また、標的型攻撃メールは必ず開封しているため、以下の情報を隠し、メールの取り扱いは極心の注意を払ってください。

【標的型攻撃メールの主な特徴】

- 特定の企業や組織内の構成員を狙った攻撃である。
- 開封しただけでは必ずしも被害が発生するわけではない。
- 仕事先のITシステム上で何らかの被害が引き起こされる。

不要なメールを「開けなかった」という場合は、上長または関係部署に通知してエクスポートしていただく。

メール開封状況のレポートで結果も見える

会員様は**10ID/年 無料で利用可能!**

訓練を受けた企業の声

三島商工会議所 様

申込みの手続きが簡単で負担が少なく訓練実施後に教育コンテンツの提供があったのがよかったです。

株式会社ダイワ・エム・ティ 様

セキュリティの専門家がない企業にとってメール予防訓練は非常にありがたいと思います。

くわしくはこちら <https://www.jtua.or.jp/ict/shindan/benefit/targeted-attack/>

