

標的型攻撃メール予防訓練サービスのご案内

- 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
- 感染元調査の金銭的被害
- 個人情報の流出と改ざん

約7割の中小企業が「自社のサイバーインシデントが取引先事業に影響を与えた」と回答

- サービスの障害、遅延、停止による逸失利益
- 個人顧客への賠償や法人取引先への補償負担
- 原因調査・復旧にかかわる人件費等の経費負担

標的型攻撃メールに気が付かず被害者のアナタが加害者になる事も…

独立行政法人情報処理推進機構「2024年度中小企業における情報セキュリティ対策の実態調査報告書」より引用

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！

擬似環境

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文

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疑似的に体験していただき、攻撃メールに対する注意力の向上を目的としております。そのため、実際に本訓練の内容等を悪用してはなりません。
実際の標的型攻撃メールでは、添付ファイルの疑念や本文に記載されている宛先へのアクセスから情報漏洩に繋がると可能性があります。
また、標的型攻撃メールは日々増加しているため、以下の情報も確認し、メールの取り扱いには細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
・ 弊会の企業情報や個人情報を悪用した攻撃である。
・ 開封しただけで悪用される内容のメールを送り付けてくる。
・ 社セキュリティシステムでの対策が難しい攻撃である。
不要なメールを「開けようとしたら開いてしまった」場合は、上層または関係部署に速やかにエスカレーションしてください。

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！

◆2026年度標的攻撃メール予防訓練スケジュール◆

	第1回	第2回	第3回	第4回	第5回	第6回	第7回	第8回	第9回	第10回	第11回
受付/申込期間	4/10 ~25	5/10 ~25	6/10 ~25	7/10 ~25	8/10 ~25	9/10 ~25	10/10 ~25	11/5 ~20	12/10 ~25	1/10 ~25	2/10 ~25
訓練実施時期	5/下旬頃	6/下旬頃	7/下旬頃	8/下旬頃	9/下旬頃	10/下旬頃	11/下旬頃	12/下旬頃	1/下旬頃	2/下旬頃	3/下旬頃

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

