

# 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に
- 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

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

標的型攻撃メールに気が付かず被害者のアナタが加害者になる事も...

## 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伝えないでください。  
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隠蔽されているURLへのアクセスから情報漏洩しにつなげる可能性があります。  
また、標的型攻撃メールは悪意を持って送信されているため、以下の被害を招き、メールの取り扱い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」  
・特定の企業や組織内の構成員を標的とした攻撃である。  
・開封しただけで被害を受ける可能性のある内容のメールが送られてくる。  
・社員がスマートフォンなどで開封しやすい攻撃である。  
不要なメールを「開けなかったら開いてしまった」場合は、上表または関係部署に連絡がベストレーションとしてください。

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！

### 標的型攻撃メールの流れ

攻撃者 → 指令 → C&Cサーバ → 標的型メール → ① 受信 → ② 開封 → ③ 感染 → ④ 攻撃者のターゲット

特定の組織内の情報を狙って行われるサイバー攻撃の一種。特定の会社の社員宛てに、ウイルスが添付された電子メールを送ることをきっかけに、その会社のみならず関連の会社の情報が狙われることも

※C&Cサーバ（Command and Control Serverの略称） 攻撃者が用意した指令サーバでPC内部に潜伏したウイルスとバックドア通信を行う。

■ 1回のお申込みで10名様まで可能です (年度内1回のみです)  
申込方法、スケジュールは、裏面をご確認願います

# 標的型攻撃メール予防訓練サービス 申込方法等

■お申込みは日本電信電話ユーザ協会青森支部ホームページから

<https://www.pi.jtua.or.jp/aomori/>



- ①画面左の“イベント情報”の「標的型攻撃メール予防訓練」をクリック
- ②「標的型攻撃メール予防訓練」ページの「イベント申込み」ボタンをクリック
- ③標的型攻撃メール予防訓練サービスお申込みフォームが開きますので、必要事項を入力いただき、**確認画面へ**ボタンをクリック



## ■2026年度のスケジュール

	申込受付期間	実施時期
第1回	4月10日(金)～4月25日(土)	5月下旬
第2回	5月10日(日)～5月25日(月)	6月下旬
第3回	6月10日(水)～6月25日(木)	7月下旬
第4回	7月10日(金)～7月25日(土)	8月下旬
第5回	8月10日(月)～8月25日(火)	9月下旬
第6回	9月10日(木)～9月25日(金)	10月下旬
第7回	10月10日(土)～10月25日(日)	11月下旬
第8回	11月5日(木)～11月20日(金)	12月下旬
第9回	12月10日(木)～12月25日(金)	1月下旬
第10回	1月10日(日)～1月25日(月)	2月下旬
第11回	2月10日(水)～2月25日(木)	3月下旬

- 申込受付終了後、2週間程度で責任者様へ通知メールを送信させていただきます
- ご登録者様へ訓練メールを送信させていただき、開封状況の監視を行います
- 開封状況の監視終了後、教育コンテンツ案内メールを送信させていただきます
- メール開封状況を記載したレポートを責任者様へ郵送させていただきます

## お申込・お問合せ

お申込は青森支部ホームページから <https://www.pi.jtua.or.jp/aomori/>

お問合せは青森支部事務局へ (017) 731-3140 e-mail:ao-sibu@jtua.or.jp