

標的型メール訓練サービス

「標的型メール」は、アンチウイルスなどの技術的な対策を実施しても防ぐことが難しいのが現状です。そのため、**ユーザー一人ひとりが標的型メールに気をつける**ことはもちろん、万が一攻撃メールの添付ファイルなどを開いてしまった場合でも**適切な対処を迅速にできるように訓練**しておくことが重要です。



日立ソリューションズの標的型メール訓練サービスとは

お客さまの会社にて標的型メール攻撃を疑似体験いただきます。誤ってメールを開封したユーザーには教育コンテンツを指示し、適切な研修を実施します。また、メール開封状況など結果を報告書でご提供することで、セキュリティの向上に役立てていただけます。



標的型メール訓練サービスの効果

攻撃メールへのリスクレベルを評価し、把握

実際に、どの程度のユーザーが攻撃メールを開封してしまうか、現状のリスクレベルを調査し、把握できます。



ユーザー端末のマルウェア感染率を大幅低減

継続的に、あるいは複数回メール訓練をすることで、攻撃メールの開封率を下げることで、感染率を低減します。



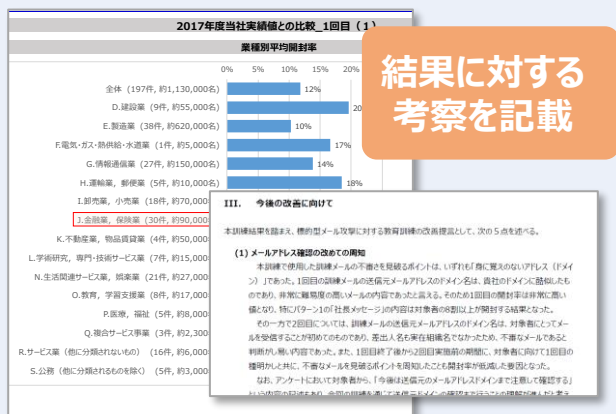
感染時の初動対応を徹底し、被害を最小化

適切な初動対応が取れるよう訓練することで、ユーザーが攻撃メールを誤って開封してしまった場合でも、被害を最小化します。



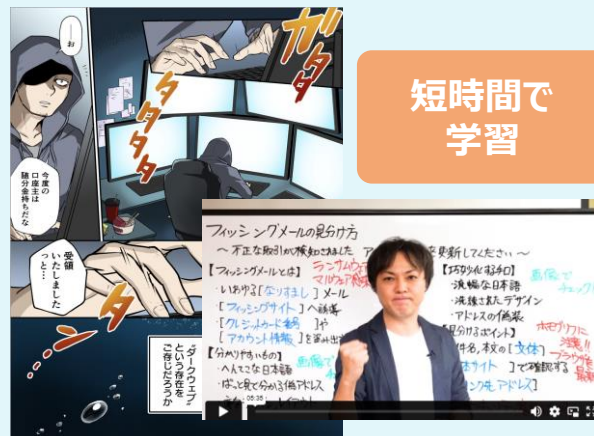
報告書重視タイプ

- 同業他社との開封データの比較や、改善案などを記載した詳細な報告書を提供



学習効果重視タイプ

- 動画、漫画など受講者の記憶に残りやすい教育コンテンツを提供



導入ステップ

調査方法の検討から訓練実施まで、発注後3から4週間。訓練終了後にアンケート実施し、Webアンケート締切後約2週間で報告書をご提供します。



おすすめポイント

- 小規模から大規模ユーザーまで対応**
お客さまのユーザー数に合ったメニューを選択できるので、コストを抑えて、標的型メール訓練を実施することができます。
- 訓練内容をカスタマイズ可能**
訓練メールの分散送信、メールや教育コンテンツの修正、アンケートの未実施など内容をカスタマイズ可能です。
- 未学習のユーザーをフォロー※**
教育コンテンツ未学習のユーザーをお客さまに代わりフォローすることで、運用の手間を軽減します。

※学習効果重視タイプのみフォロー可能です

※本リーフレット中の会社名、商品名は各社の商標、または登録商標です。 ※本文中および図中では、TMマーク、®マークは表記しておりません。 ※製品の仕様は、改良のため、予告なく変更する場合があります。 ※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。 ※本リーフレット中の情報は、作成時点のものです。

