標的型攻撃メール訓練

標的型攻撃メールを疑似体験する訓練サービス

情報セキュリティ意識の向上＆可視化を実現！

標的型攻撃メールって、知っていますか？

特定の組織や社員を狙ってウイルスを仕込んだメールを送り、添付ファイルやURLを開いてしまうことで個人情報や取引先情報が盗まれるサイバー攻撃の手口です。
取引先の企業などを装い、攻撃メールであると気が付きにくいのが特徴です。

2018年の組織に対する情報セキュリティ脅威No.1となっています！※
※独立行政法人 情報処理推進機構セキュリティセンター(IPA)「情報セキュリティ10大脅威2018」より

効果的な対策とは？

従業員一人ひとりが攻撃メールであると「気づけること」が最も有効な対策です。
昨今サイバー攻撃のリスクは高まる一方であり、意識の向上が不可欠です。

メール訓練の流れ

お客様には訓練メール送信の宛先をご準備頂くだけ！

❶ 訓練準備

■訓練計画の打ち合わせ
■訓練用メールを作成
■対象者のメールアドレス登録
■訓練スケジュール設定

❷ 訓練メール送信

■指定した日時に対象者へ自動配信
■添付ファイルやURLを開くと警告メッセージが表示
■訓練後のWeb教育コンテンツでの学習、アンケート実施

❸ 結果報告

■部署別、役職別などの開封結果を報告書にて提供
（開封率のグラフ化や他社との比較を含む）

FIC
株式会社 福島情報処理センター

株式会社 福島情報処理センター

価格

（税抜）

	基本料金 （打ち合わせ、設定と送信、訓練結果報告）	1メール送信あたりの単価 （1ID=1メール送信）
提供料金	30,000円	500円／ＩＤ

訓練後のフォロー

開封率が高く、全組織的な教育が必要！

→各社様に合ったオリジナルシナリオでの集合セミナーを開催可能です

ソフトやハード面でのメールセキュリティ強化製品を導入したい！

→サンドボックスやメール無害化製品等、お客様に最適な製品をご紹介します

ご利用にあたっての注意事項

- Webサイトの閲覧に制限をかけている場合や、メーラーの設定などによっては正常に訓練が行えない場合があります。ご契約前に、訓練用メールサーバからお客様側メールサーバとの間で正常にメールの送信、開封ログの収集が行えるか、サービス提供可否確認を実施します。

お問い合わせ

株式会社 福島情報処理センター 情報セキュリティ事業部
〒963-8025 福島県郡山市桑野三丁目18-24
Mail: security@fic.co.jp TEL:024-923-2116／FAX:024-938-6762

※この資料に記載の内容は平成30年12月時点の情報になります。