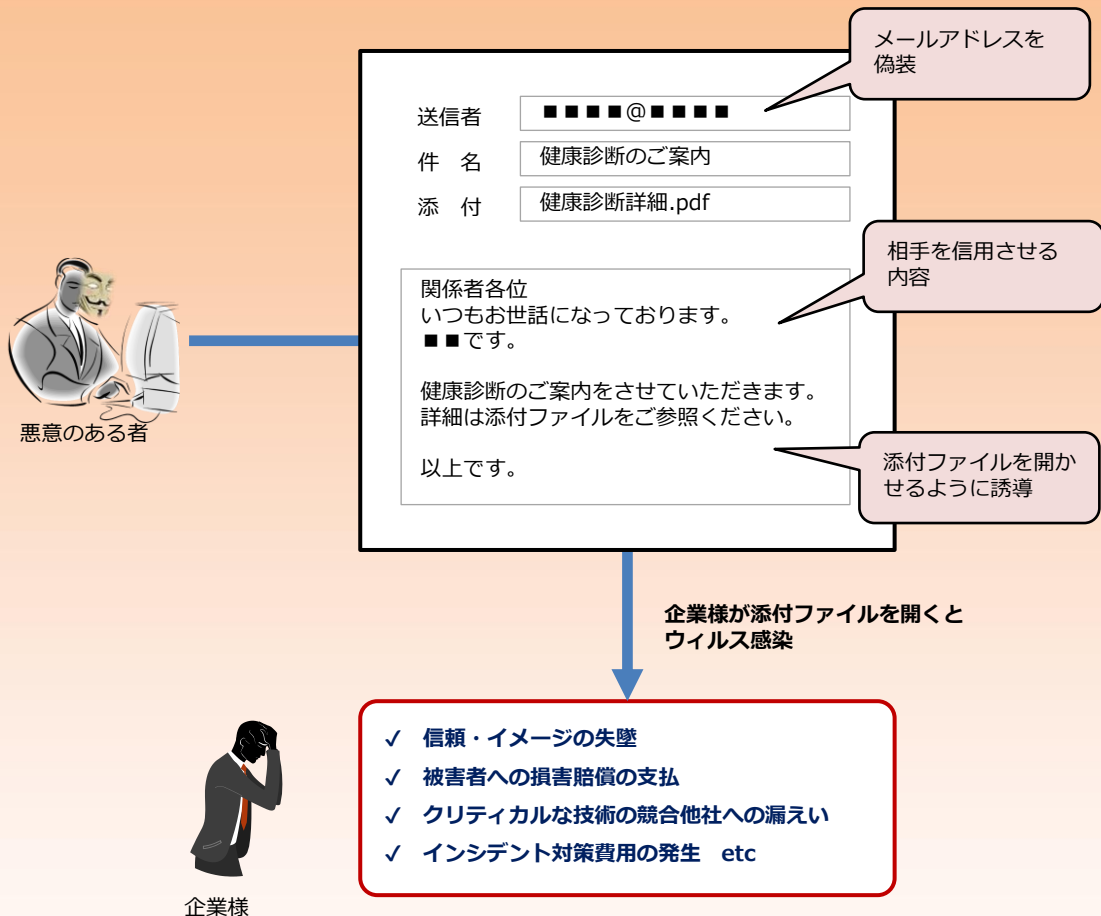


標的型メール攻撃耐性訓練サービス

標的型メールとはサイバー攻撃の一種で、特定の組織内の情報を狙って送りつけられる電子メールです。誤って添付ファイルを開封もしくはURLをクリックすると、クライアント端末がウイルス感染し、内部情報が外部へ漏えいする可能性があります。



標的型メールの特徴

- 特定組織を狙った特製の不正プログラムを使用するため、ウイルス対策ソフトでの検知が困難です。
- 不正プログラムは通常のルートで外部との通信を行うため、ファイアウォールやIDS(不正侵入検知システム)によって異常を検知することが困難です。

このような状況であるため、まずは社員様一人ひとりが、

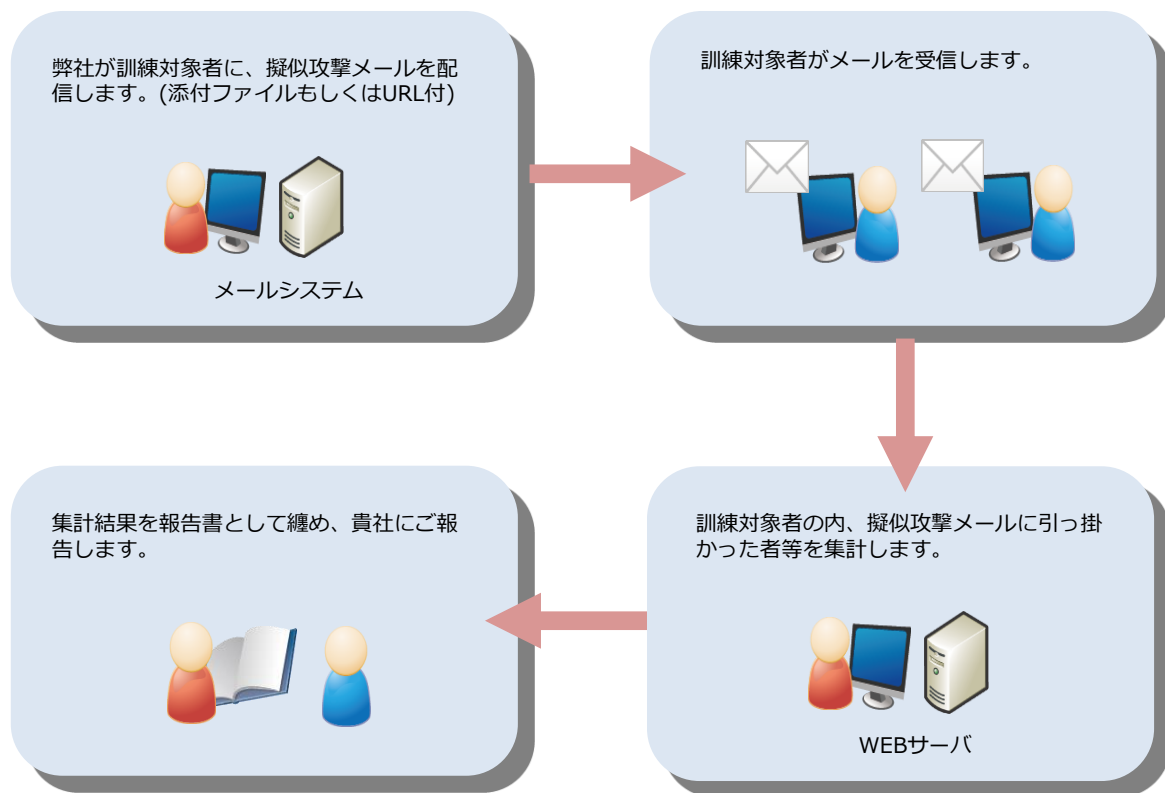
- ① 「標的型メール攻撃」は他人事ではなく、**自分が被害者**になる可能性があることを認識すること
- ② 「標的型メール攻撃」に引っ掛かったとしても、その後の**社内エスカレーション**を理解しておくこと

が非常に重要です。



サービスの概要

本サービスでは、擬似的な標的型攻撃メールを実際に体験していただくことで、社員様のセキュリティ意識の向上や、仮にインシデントが発生した時のエスカレーションについて再確認をしていただくきっかけを作ることができます。



訓練で得られる効果

1. 社員様の注意力の向上

標的型メールの特徴を体験していただくことで、社員様一人ひとりの注意力が向上し、組織がウイルスに感染するリスクが低下します。

2. お客様組織の耐性把握が可能

標的型攻撃メールに対する貴社組織の耐性度合いが数値(開封率)で把握できます。また、定期的に訓練することで、数値の変化という形で訓練の効果を測ることができます。

3. 訓練結果を分析し今後の対策が立てられる

訓練対象者の部署別や職種別に集計して、訓練結果を分析することで、組織や個人毎の耐性が把握できるため、今後の教育方針立案に役立ちます。

お問い合わせ先

TIS株式会社
セキュアワンセンター
東京都新宿区西新宿8-17-1 住友不動産新宿グランドタワー
TEL : 03-5337-5344
E-mail : so_kansa@ml.tis.co.jp



Go Beyond