ONE STOP

標的型攻撃メール対応訓練サービス

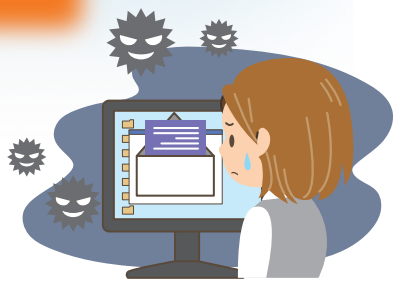
メールによる標的型攻撃※を擬似体験することで、
不審メールの対処を学んでいただくサービスです

※標的型攻撃:特定の企業などの組織、サービスに対して行われるサイバー攻撃のこと。
一般的な攻撃手法として、添付ファイルやURL付きの電子メールが用いられる。

こんなお悩み解決します!

標的型攻撃メールと気付けずに開いてしまわないか心配…

普通のメールと区別がつきにくい巧妙なメール。
見抜けるか不安…



不審メールが届いた場合の連絡ルートは本当に機能する?

有事の際の対処ルールが正しく理解・浸透しているかを確認したい。

知識だけではなく、不審メールの対処を身につけるには?

セキュリティ教育のみでは不十分。実際の対処方法を着実に身に付けたい。

こんな効果が期待できます!

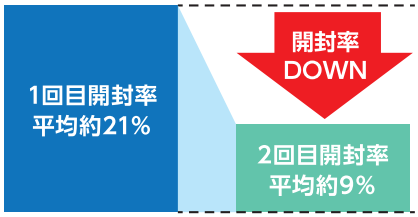
実際に不審メールを擬似体験することで、攻撃手法やその対処方法を習得できます。
また、一人ひとりの情報セキュリティ意識向上につながり、ウイルス感染のリスクを確実に低減することができます。

ONE STOP

訓練導入の結果

セキュリティ意識を高めましょう!

1回の訓練で効果あり!



出典:ITセキュリティ予防接種調査報告書2009年版

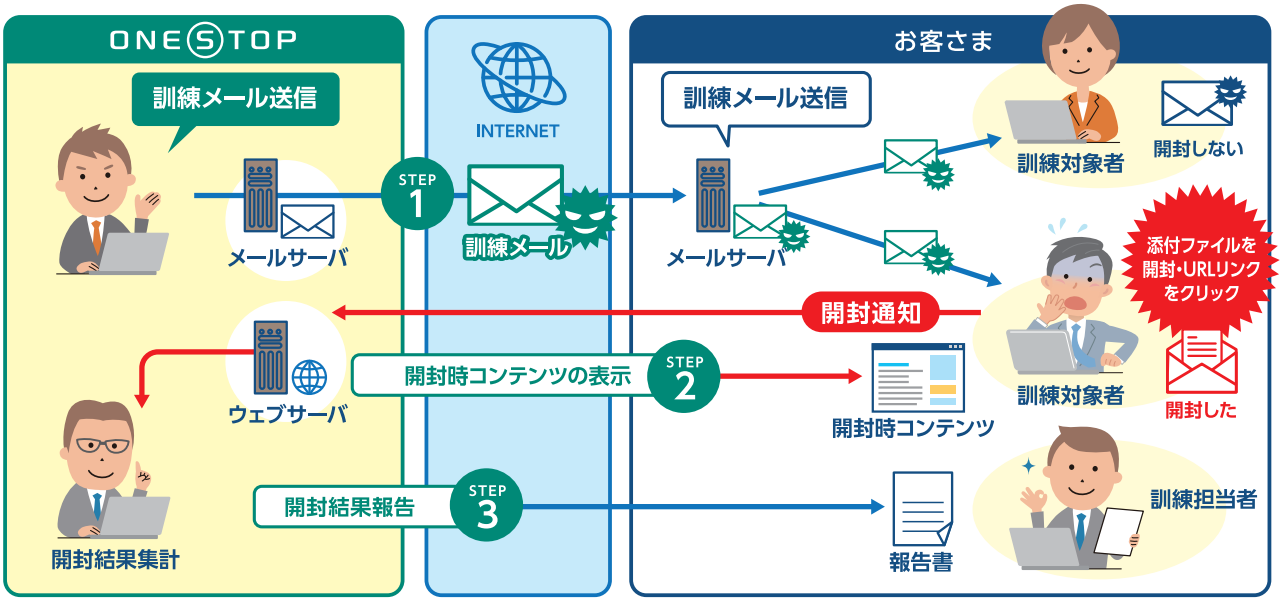
これまでに訓練を実施した企業・団体の効果を調査。訓練2回目では、1回目よりも添付ファイル開封率が減少することが確認できました。

さまざまな状況に対応!

インターネット接続環境だけでなく、クローズドネットワーク環境にも対応。添付ファイル型の訓練では、添付するファイル形式も豊富に取り揃えています。

導入訓練イメージ

「基本メニュー」訓練イメージ



STEP 1 訓練メール送信

訓練メール(擬似攻撃メール)を送信します。訓練メールの形式は「URLリンク型」と「添付ファイル型」から選択できます。

STEP 2 開封時コンテンツの表示

訓練メールのURLリンクをクリックした、もしくは添付ファイルを開いてしまった訓練対象者(開封者)には、標的型攻撃メールへの注意を促すコンテンツ(開封時コンテンツ)が表示されます。

STEP 3 開封結果報告

訓練メールの開封者の割合(開封率)をお知らせします。

ほくでん情報テクノロジー株式会社

〒060-0041 札幌市中央区大通東3丁目4番地e・i大通東ビル
デジタルソリューション部
TEL:011-330-7612　E-mail:staff-sales@hokuden-it.co.jp
URL:https://www.hokuden-it.co.jp/